



Dr.WEB

Enterprise Security Suite

付録



© Doctor Web, 2021無断複写・転載を禁じます。

本マニュアルは特定のDr.Webソフトウェアの使用に関する情報を提供し、参照目的で用いられることを意図したものです。Dr.Webソフトウェアに特定の機能や技術仕様が備わっているかどうかを評価する際の根拠となるものではなく、また、Dr.Webソフトウェアが特定の要件や技術的タスク/パラメータ、サードパーティのマニュアルに合致するかどうかを判断するために使用するものではありません。

本マニュアルの著作権はDoctor Webが有します。本マニュアルのどの部分も、いかなる形式、方法、および購入者が個人で利用する以外のいかなる目的においても、無断で複写、出版、転載することを禁じます。

商標

Dr.Web、SpIDer Mail、SpIDer Guard、CureIt!、CureNet!、AV-Desk、KATANA、Dr.WEBロゴは、ロシアおよびその他の国におけるDoctor Webの商標および登録商標です。本マニュアルに記載されているその他の商標、登録商標、および会社名の著作権はそれぞれの所有者が有します。

免責事項

Doctor Webおよびそのリセラー、ディストリビューターは、過失または損失、このマニュアルによって直接、または間接的に引き起こされた、または引き起こされたと考えられるいかなる損害、および本マニュアルに含まれる情報の利用、または利用できないことに対する責任を負わないものとします。

Dr.Web Enterprise Security Suite

バージョン12.0

付録

2021/02/20

Doctor Webロシア本社

2-12A, 3rd str. Yamskogo polya, Moscow, Russia, 125124

ウェブサイト: <https://www.drweb.com/>

電話番号: +7 (495) 789-45-87

支社および海外オフィスについては、Doctor Web公式サイトをご覧ください。

Doctor Web

Doctor Web は、悪意のあるソフトウェアやスパムからの効果的な保護を提供するDr.Web情報セキュリティソリューションの開発および販売を行っています。

Doctor Web のカスタマーは、世界中のホームユーザーから政府機関、小規模な会社、大企業にまで広がっています。

Dr.Web アンチウイルスソリューションは、マルウェア検出における継続的な卓越性と国際情報セキュリティ基準への遵守によって1992年よりその名を広く知られています。

Dr.Web ソリューションに与えられたロシア連邦による認定や数々の賞、そして世界中に広がるそのユーザーが、製品に対する並外れた信頼の何よりの証です。

Dr.Web 製品に対するサポートについて、すべてのカスタマーに対して厚く御礼申し上げます。



目次

第1章:はじめに	7
マニュアルについて	7
表記規則および略語	8
第2章:付録	10
付録A. 対応OSバージョンコンプリートリスト	10
付録B. DBMSの設定とDBMSドライバのパラメータ	14
B1. ODBCドライバのセットアップ	16
B2. Oracleデータベースドライバのセットアップ	17
B3. PostgreSQL DBMSの使用	20
B4. MySQL DBMSの使用	22
付録C. 管理者の認証	24
C1. Active Directory認証	24
C2. LDAP認証	25
C3. LDAP/AD認証	26
C4. パーミッションセクション	29
付録D. 通知システムの設定	35
D1. 通知システムパラメータの記述	35
D2. 通知テンプレートのパラメータ	37
付録E. ネットワークアドレスの指定	68
E1. アドレスの一般フォーマット	68
E2. Dr.Web Agent/Installerのアドレス	70
付録F. リポジトリの管理	71
F1. 全般設定ファイル	71
F2. 製品設定ファイル	73
付録G. 設定ファイルフォーマット	78
G1. Dr.Web Server設定ファイル	78
G2. Dr.Web Security Control Center設定ファイル	100
G3. download.conf設定ファイル	104
G4. Dr.Web Proxy Server設定ファイル	105
G5. Repository Loader設定ファイル	111
付録H. Dr.Web Enterprise Security Suite に含まれるプログラムのコマンドラインパラメータ	116
H1. ネットワークインストーラ	117
H2. Dr.Web Agent for Windows	119



H3. Dr.Web Server	121
H4. Dr.Web Scanner for Windows	132
H5. Dr.Web Proxy Server	132
H6. UNIX系OS向けDr.Web Serverインストーラ	136
H7. ユーティリティ	138
付録I. Dr.Web Serverによってエクスポートされる環境変数	156
付録J. Dr.Web Enterprise Security Suiteで使用される正規表現	157
J1. PCRE正規表現で使用されるオプション	157
J2. PCRE正規表現の特性	158
付録K. ログファイルフォーマット	160
付録L. Web APIとDr.Web Enterprise Security Suiteの連携	162
付録M. ライセンス	163
M1. Boost	165
M2. C-ares	166
M3. Curl	166
M4. ICU	166
M5. GCC runtime libraries - 例外	167
M6. Jemalloc	169
M7. Leaflet	169
M8. Libpng	170
M9. Libradius	172
M10. Libssh2	172
M11. Linenoise NG	173
M12. Net-snmp	174
M13. Noto Sans CJK	178
M14. OpenLDAP	179
M15. OpenSSL	180
M16. Oracle Instant Client	182
M17. ParaType Free Font	186
M18. PCRE	186
M19. Script.aculo.us	188
M20. Zlib	188
第3章: よくある質問	190
他のコンピューターに Dr.Web Server を移動する(Windows OS環境)	190
Dr.Web Agent を他の Dr.Web Server に接続する	192
Dr.Web Enterprise Security Suite の DBMS の種類の変更	194



Dr.Web Enterprise Security Suite のデータベースの復元	197
LANサーバー上の Dr.Web Agent のアップグレード	201
Dr.Web Enterprise Security Suite 管理者のパスワードの復元	202
Active Directory 経由での Agent インストールにおける DFS の使用	204
Dr.Web Server 故障後のアンチウイルスネットワークの復元	205
Dr.Web Serverのバックアップから復元する	205
Dr.Web Serverのバックアップが無い状態での復元	207
Dr.Web Server for Windows OS のロギングレベルの管理	209
Android OS 搭載端末の自動位置情報	209
Dr.Web Server データベースへのアクセス例	211
機能分析の基準	214
第4章：トラブルシューティング	218
リモートインストールにおけるトラブルシューティング	218
Dr.Web Agent for Windows のインストール中の BFE エラーの解決	221
テクニカルサポート	222



第1章: はじめに

マニュアルについて

Dr.Web Enterprise Security Suiteアンチウイルスネットワーク管理者マニュアルは、一般的な機能の紹介と、Dr.Web Enterprise Security Suiteを使用した企業コンピューターへの包括的なアンチウイルス保護の構築に関する詳細情報の提供を目的としています。

Dr.Webアンチウイルスネットワーク管理者マニュアルには、次のドキュメントが含まれています。

1. インストールマニュアル([drweb-12.0-esuite-install-manual-ja.pdf](#))

インストールマニュアルは、包括的なアンチウイルス保護の購入およびインストールについての検討、決定を行う企業のマネージャーにとって便利な内容になっています。

インストールマニュアルでは、アンチウイルスネットワークを構築し、その主要コンポーネントをインストールする方法について説明しています。

2. 管理者マニュアル([drweb-12.0-esuite-admin-manual-ja.pdf](#))

管理者マニュアルはアンチウイルスネットワーク管理者(インターネットサービスを提供するネットワーク内のコンピューター(ワークステーションやサーバー)に対するアンチウイルス保護を担当する

アンチウイルスネットワーク管理者は、システム管理者権限を持っているか、ローカルネットワーク管理者と緊密に連携し、アンチウイルス保護戦略に精通し、さらにネットワーク内で使用される全てのOS用のDr.Webアンチウイルスパッケージの詳細を把握している必要があります。

3. 付録([drweb-12.0-esuite-appendices-ja.pdf](#))

付録では、アンチウイルスコンポーネントの設定パラメータと、これらのモジュールの操作に使用される命令の構文と値を説明する技術情報について説明しています。



上記のドキュメントには、相互参照機能があります。これらのドキュメントをローカルコンピューターにダウンロードすると、ドキュメントが同じフォルダに初期名で配置されている限り、相互参照が機能します。

また、次のマニュアルが用意されています。

1. アンチウイルスネットワーク・クイックインストールガイド

アンチウイルスネットワークコンポーネントのインストールと初期設定の概略が記載されています。詳細については、管理者ガイドを参照してください。

2. ワークステーションの管理に関するマニュアル

Dr.Web Security Control Center経由でアンチウイルスネットワーク管理者によって提供される、端末上のアンチウイルスソフトウェアの集中管理での設定に関する情報が記載されています。

3. ユーザーマニュアル

保護された端末上でのDr.Webアンチウイルスソフトウェアの設定に関する情報が記載されています。

4. Web APIマニュアル

Dr.Web Enterprise Security Suite とサードパーティソフトウェアをWeb API経由で統合する際の技術的詳細について記載されています。

5. Dr.Web Serverデータベースマニュアル



Dr.Web Serverデータベースの内部構造の説明とその使用例が記載されています。

リストにあげた全てのマニュアルは、Dr.Web Enterprise Security Suite製品の一部としても提供されており、Dr.Web Security Control Centerから開くことができます。

これらのドキュメントをお読みになる前に、それがお使いの製品バージョンに対応する最新のバージョンであることを確認してください。マニュアルは随時更新されています。最新版はDoctor Webの公式サイト <https://download.drweb.com/doc/> でいつでも確認できます。

表記規則および略語

表記規則

本マニュアルでは、以下の文字・記号を使用しています。

文字・記号	説明
	重要な部分や指示
	重要な注釈、またはエラーを引き起こす可能性のある状況に関する警告
アンチウイルスネットワーク	新しい用語、または強調したい用語
<IP-address>	プレースホルダー
保存	ボタン、ウィンドウ、メニューアイテム、および他のプログラムインターフェースエレメントの名称
CTRL	キーボードのキー名称
C:\Windows\	ファイルやフォルダの名前、コード例
付録 A	本書の他のページや外部Webページへのリンク

略語

以下の略語は本マニュアル内では次の意味でのみ使われます。

- ACL - Access Control List(アクセス制御リスト)
- CDN - Content Delivery network(コンテンツデリバリーネットワーク)
- DFS - Distributed File System(分散ファイルシステム)
- DNS - Domain Name System(ドメインネームシステム)
- FQDN - Fully Qualified Domain Name(完全修飾ドメイン名)
- GUI - Graphical User Interface(グラフィカルユーザーインターフェース、プログラムのGUIバージョン - GUIを使ったバージョン)
- MIB - 管理情報ベース



- MTU - Maximum Transmission Unit(最大転送ユニット)
- NAP - Network Access Protection(ネットワークアクセス保護)
- TTL - Time To Live(タイムツーリーブ: パケットの有効期間)
- UDS - UNIX Domain Socket(UNIXドメインソケット)
- DB、DBMS - Database(データベース)、Database Management System(データベース管理システム)
- Dr.Web GUS - Dr.Web Global Update System
- LAN - Local Area Network(ローカルエリアネットワーク)
- OS - Operating System(オペレーティングシステム)



第2章: 付録

付録A. 対応OSバージョンコンプリートリスト

Dr.Web Server

UNIX系OS

ライブラリglibc2.13以降(ALT Linux 5.0以降、Astra Linux Special Edition 1.3以降を含む)を使用したLinux

FreeBSD 10.3以降

Windows OS

- 32ビット:

Windows 7

Windows 8

Windows 8.1

Windows 10

- 64ビット:

Windows Server 2008 R2

Windows 7

Windows Server 2012

Windows Server 2012 R2

Windows 8

Windows 8.1

Windows 10

Windows Server 2016

Windows Server 2019

Dr.Web Agentおよびアンチウイルスパッケージ

UNIX系OS

カーネル2.6.37以降(プラットフォームx86/amd64/arm64)、PAMおよびライブラリglibc 2.13以降を使用したLinux



SpIDer Gateを正常に動作させるには、次のアイテムを含めてOSカーネルをコンパイルする必要があります。

- CONFIG_NETLINK_DIAG, CONFIG_INET_TCP_DIAG
- CONFIG_NF_CONNTRACK_IPV4, CONFIG_NF_CONNTRACK_IPV6, CONFIG_NF_CONNTRACK_EVENTS
- CONFIG_NETFILTER_NETLINK_QUEUE, CONFIG_NETFILTER_NETLINK_QUEUE_CT, CONFIG_NETFILTER_XT_MARK



64ビットプラットフォームでは、32ビットアプリケーションのサポートが有効になっている必要があります。

以下のLinuxディストリビューション(32ビットおよび64ビット)上での動作が確認されています。

Linuxディストリビューション名	バージョン	64ビットバージョン向けの追加のライブラリが必要です
ALT Linux Server	9	ARM64
ALT Linux Workstation	9	ARM64
Astra Linux Special Edition (Smolensk)	1.4、1.5、1.6	x86_64
CentOS	6.9、7.4	x86、x86_64、ARM64
Debian	7.11、8.10、9.3	x86_64
Fedora	27、28、29	x86、x86_64
Red Hat Enterprise Linux	7.4	x86_64
SUSE Linux Enterprise Server	11 SP4、12 SP3	x86_64
Ubuntu	14.04、16.04、18.04	x86_64、ARM64

ARM64プラットフォームでは、Ubuntu 18.04、CentOS 7.7、ALT Linux Workstation 9、ALT Linux Server9のディストリビューションとの互換性が確認されています。

上の要件を満たすその他のLinuxディストリビューションについては、Dr.Web for Linuxとの互換性テストは行われていませんが、対応している場合があります。互換性の問題が発生した場合は、公式サイト <https://support.drweb.com> のテクニカルサポートまでご連絡ください。



バージョン6のコンポーネントがDr.Web Enterprise Security Suiteと一緒に使用されている場合、そのシステム要件については、該当するコンポーネントのマニュアルを確認してください。



Windows OS

- 32ビット:

Windows XP SP2

Windows Server 2003 (SP1以降)

Windows Vista (SP2)

Windows Server 2008 (SP2以降)

Windows 7 (SP1)

Windows 8

Windows 8.1

Windows 10

- 64ビット:

Windows Vista (SP2以降)

Windows Server 2008 (SP2以降)

Windows Server 2008 R2 (SP1)

Windows 7 (SP1)

Windows Server 2012

Windows Server 2012 R2

Windows 8

Windows 8.1

Windows 10

Windows Server 2016

Windows Server 2019



MicrosoftによるSHA-1ハッシュアルゴリズムのサポートが終了しています。Windows Vista、Windows 7、Windows Server 2008、またはWindows Server 2008 R2にDr.Web Agentをインストールする場合は、オペレーティングシステムがSHA-256ハッシュアルゴリズムをサポートしていることを事前に確認するようにしてください。これを行うには、Windows Updateにリストされているすべての推奨更新プログラムをインストールします。詳細については[Doctor Web公式ウェブサイト](#)をご確認ください。



WindowsのStarterエディションおよびHomeエディションではDr.Web Agentのリモートインストールはできません。

macOS

OS X 10.10 (Yosemite)

OS X Server 10.10 (Yosemiteサーバー)

OS X 10.11 (El Capitan)

OS X Server 10.11 (El Capitanサーバー)



macOS 10.12 (Sierra)
macOS Server 10.12 (Sierra)
macOS 10.13 (High Sierra)
macOS Server 10.13 (High Sierra)
macOS 10.14 (Mojave)
macOS Server 10.14 (Mojave)
macOS 10.15 (Catalina)

Android OS

Android 4.4
Android 5.0
Android 5.1
Android 6.0
Android 7.0
Android 7.1
Android 8.0
Android 8.1
Android 9.0
Android 10.0



付録B. DBMSの設定とDBMSドライバのパラメータ



Dr.Web Serverインストールフォルダのetcサブフォルダ内にあるinit.sqlスクリプトを利用してDr.Web ServerのDB構成を確認できます。

Dr.Web Serverのデータベースとして以下の2種類を使用できます。

- 内部DBMS
- 外部DBMS

内部DBMS

データを保管および処理するためにDBMSへのアクセスを設定する際には、内部DBMSに表B-1のパラメータを使用します。

表B-1内部DBMS

名前	デフォルト値	説明
DBFILE	database.sqlite	データベースファイルへのパス
CACHESIZE	2000	ページ内のデータベースキャッシュサイズ
SYNCHRONOUS	FULL	データベース内の変更のロギングをディスクと同期するモード <ul style="list-style-type: none">• FULL - ロギングをディスクと完全に同期• NORMAL - 重要なデータのロギングを同期• OFF - ロギングを同期しない

バージョン10以降のServerでサポートされる内部DBMSとして、SQLite3 DBMSが使用されます。

外部DBMS

Dr.Web Serverの外部データベースを調整するために、以下のデータベース管理システムを使用します。

- Oracle: 設定については、[付録B2. Oracleデータベースドライバをセットアップする](#)をご覧ください。
- PostgreSQL: PostgreSQL で必要な設定については、[付録B3. PostgreSQL DBMSの使用](#)をご覧ください。
- Microsoft SQL Server/Microsoft SQL Server Express: これらのDBMSへのアクセスには、ODBCドライバを使用します (WindowsでのODBCドライバのパラメータ設定については、[付録B1. ODBCドライバのセットアップ](#)をご覧ください)。



Microsoft SQL Server 2008以降が、サポートされています。Microsoft SQL Server 2014以降の使用を推奨します。



Microsoft SQL Server Expressの使用は、端末数の多い(100台以上)アンチウイルスネットワークでは推奨されません。

UNIX系OS環境のServerに対する外部DBとしてMicrosoft SQL Serverを使用する場合、FreeTDSを用いたODBC経由での動作は保証していません。

ODBC経由でのDr.Web ServerとMicrosoft SQL Server DBMSとの連携中に警告またはエラーが発生した場合、このエディション向けのDBMSの最新バージョンを使用していることを確認します。

バージョンについては、マイクロソフト社のページ(<https://docs.microsoft.com/en-us/troubleshoot/sql/general/determine-version-edition-update-level>)で確認してください。



Microsoft SQL Server DBMSをデフォルトのトランザクション分離レベル(READ COMMITTED)で使用している場合にデッドロックの発生を減らすには、次のSQLコマンドを実行してREAD_COMMITTED_SNAPSHOTオプションを有効にすることをお勧めします。

```
ALTER DATABASE <database_name>  
SET READ_COMMITTED_SNAPSHOT ON;
```

上記のコマンドは、暗黙的なトランザクションモードで、データベースへの既存の単一接続を使用して実行する必要があります。

特徴比較



Dr.Web Serverのあるコンピューターのハードウェアコンフィギュレーションで許可されており、実行中の他のプロセスの負荷レベルが許容範囲内である場合は端末を1000台まで接続できます。Serverに接続された端末が200~300台よりも少ない場合は組み込みDBの使用が可能です。

それ以外の場合は外部DBを使用します。

外部DBを使用していて10,000台を超える端末がServerに接続されている場合、以下の最小要件を満たすことを推奨します。

- 3 GHzプロセッサCPU
- Dr.Web Serverに4 GB以上、DBサーバーに8 GB以上のRAM
- UNIX系OS

内部データベースか外部データベースかを選択する際には、DBMSの以下の特徴を考慮してください。

- 大規模なアンチウイルスネットワーク(200~300台を超える端末)では、内部DBよりも耐障害性のある外部DBの使用を推奨します。
- 内部DBを使用する場合、サードパーティソフトウェアのコンポーネントをインストールする必要はありません。データベースの一般的な使用として推奨されます。
- 内部データベースはDBMS管理スキルを必要とせず、中小規模のアンチウイルスネットワークに適しています。
- DBMSを通じて作業をする場合や、DBに直接アクセスする必要がある場合は、外部データベースを使用できます。OLE DB、ADO.NET、ODBCなどの標準APIを使用してアクセスを簡単にできます。



B1. ODBCドライバのセットアップ

データを保管および処理するためにDBMSへのアクセスを設定する際には、外部DBMSに表 B-2のパラメータを使用します。

表B-2ODBC接続用のパラメータ

名前	値	説明
DSN	drwcs	データセット名
USER	drwcs	ユーザー名
PASS	fUqRbrmlvI	パスワード
TRANSACTION	DEFAULT	TRANSACTIONパラメータに使用可能な値 <ul style="list-style-type: none">• SERIALIZABLE• READ_UNCOMMITTED• READ_COMMITTED• REPEATABLE_READ• DEFAULT DEFAULT値は「SQL Serverのデフォルトを使用する」という意味です。詳細については、該当するDBMSのマニュアルを参照してください。



エンコードの問題を回避するため、ODBCドライバの以下のパラメータを無効にする必要があります。

- **Use regional settings when outputting currency, numbers, dates and times** - 数値パラメータのフォーマット中にエラーを引き起こす可能性があります。
- **文字データの変換を実行する** - Dr.Web Security Control Center内で、DBのパラメータに誤った記号を表示させる可能性があります。このパラメータはUnicodeを使用しないプログラムの言語パラメータに応じて記号を表示させます。

Microsoft SQL DBMSで新しいデータベースを作成する際には、大文字と小文字が区別され（_CSサフィックスの付いた）、アクセント記号が区別される（_ASの付いた）照合順序を指定する必要があります。

データベースは、最初に上記のパラメータを使用してSQL Server上に作成されます。

Dr.Web ServerがインストールされているコンピューターでODBCドライバのパラメータも設定する必要があります。



UNIX系OS上でのODBCの設定に関する情報は<http://www.unixodbc.org/>の**Manuals**セクションを確認してください。

WindowsでのODBCドライバの設定

ODBCドライバのパラメータを設定するには

1. Windows OSのコントロールパネルで **管理ツール** を選択します。開いたウィンドウで **データソース (ODBC)** をクリックします。**ODBC データソースの管理者** ウィンドウが開きます。システム **DSN** タブに移動します。
2. **追加** をクリックします。ドライバを選択するウィンドウが開きます。
3. リスト内で、使用するDB向けの該当するODBCドライバを選択し、**完了** をクリックします。DB Serverへのアクセスを設定する最初のウィンドウが開きます。



外部DBMSを使用する場合、そのDBMSと一緒に提供されるODBCドライバの最新バージョンをインストールする必要があります。WindowsのOSと一緒に提供されるODBCの使用は推奨できません (MicrosoftによってODBCドライバなしで提供されるデータベースは除く)。

4. データソースへのアクセスパラメータを入力します (Dr.Web Serverの設定と同じ)。DBサーバーがDr.Web Serverと同じコンピューターにインストールされていない場合、**サーバーフィールド**でDBサーバーのIPアドレスか名前を指定します。**次へ** をクリックします。
5. **SQL Server**認証オプションを選択し、DBへのアクセスに必要なユーザー認証を指定します。**次へ** をクリックします。
6. **既定のデータベースを以下に変更する** ドロップダウンリストで、Dr.Web Serverの使用するデータベースを選択します。その際、サーバーデータベース名は必ず指定する必要がありますが、デフォルト値は必須ではありません。

ANSIの引用符付き識別子を使用する および **ANSIのNULL**、**埋め込み文字**および**警告を使用する** にチェックが入っていることを確認します。**次へ** をクリックします。



ODBCドライバ設定でSQL Serverシステムメッセージの言語の変更が可能になっている場合は **English** を選択します。

7. 設定が終了したら **完了** をクリックします。指定したパラメータのサマリーを表示するウィンドウが開きます。
8. 指定した設定をテストするには、**データソースのテスト** をクリックします。テスト成功の通知を確認した後 **OK** をクリックします。

B2. Oracleデータベースドライバのセットアップ

概要

Oracleデータベース (Oracle DBMS) はオブジェクトリレーショナルDBMSです。OracleはDr.Web Enterprise Security Suiteの外部DBとして使用できます。



Dr.Web Serverは、FreeBSDを除く全てのプラットフォーム上で外部データベースとしてOracle DBMSを使うことができます ([インストールと対応バージョン](#) 参照)。



Oracle DBMSを使用するには

1. Oracle DBのインスタンスをインストールし、AL32UTF8エンコーディングをセットアップします。AL32UTF8エンコーディングを使用するために設定された既存のインスタンスを使うこともできます。
2. それぞれの外部データベースを使用するようデータベースドライバをセットアップします。この操作は[設定ファイル](#)内、またはDr.Web Security Control Center経由(**Dr.Web Server**設定→データベース タブ)で行うことができます。



Oracle DBをODBC接続経由で外部データベースとして使用する場合、Dr.Web Serverインストール(またはアップグレード)中に、インストーラ設定内でビルトインOracle DBMSクライアントのインストールを無効にします(データベースのサポート - **Oracle**データベースドライバ セクション)。

この操作を行わない場合、ライブラリの競合により、ODBC経由でOracle DBと連携できません。

SYSユーザーおよびSYSTEMユーザーとしてOracleデータベースに接続することはできません。また、SYSDBA管理者権限およびSYSOPER管理者権限を持った接続も禁止されています。

インストールと対応バージョン

外部DBとしてOracleを使用する場合、Oracle DBのインスタンスをインストールし、AL32UTF8(C`CHARACTER SET AL32UTF8 / NATIONAL CHARACTER SET AL16UTF16`)エンコーディングをセットアップする必要があります。この操作は以下のいずれかの方法で行うことができます。

1. Oracleインストーラを使用して(インスタンスインストールおよび設定の外部モードを使用)
2. `CREATE DATABASE` SQLコマンドを使用して

Oracleインスタンスの作成および設定に関する詳細については、Oracleドキュメンテーションを参照してください。



異なるエンコーディングを使用する場合、アルファベット以外の文字は正常に表示されない場合があります。

データベースにアクセスするためのクライアント(Oracle Instant Client)は、Dr.Web Enterprise Security Suiteのインストールパッケージに含まれています。

Oracle DBMSが対応しているプラットフォームのリストは、ベンダーの[Webサイト](#)を参照してください。

Oracle Clientが対応しているプラットフォームのリストは、ベンダーの[Webサイト](#)を参照してください。

Dr.Web Enterprise Security Suiteでは、Oracle DBMSバージョン11以降をサポートします。

また、Oracle外部データベースを操作する際のDr.Web Serverのシステム要件に注意してください(インストールマニュアルの [システム要件](#)を参照)。

パラメータ

Oracle DBMSへのアクセスを調整するには、表B-3のパラメータを使用します。



表B - 3。Oracle DBMSのパラメータ

パラメータ	説明
drworacle	ドライバ名
User	データベースユーザー名(必須)
パスワード	ユーザーパスワード(必須)
ConnectionString	データベース接続文字列(必須)
Prefetch-rows	データベースへのクエリを実行する際にプリフェッチされる行数
Prefetch-mem	データベースへのクエリを実行する際にプリフェッチされる行に割り当てられるメモリ

Oracle DBMSの接続文字列のフォーマットは以下のとおりです。

```
// <host>: <port>/ <service name>
```

ここで:

- <host>- Oracle Serverの名前またはIPアドレス
- <port> - Oracleがリッスンしているポート
- <service name> - 接続するDBの名前

例:

```
//myserver111:1521/bjava21
```

ここで:

- myserver111 - Oracle Serverの名前
- 1521 - Oracleがリッスンしているポート
- bjava21 - 接続するDBの名前

Oracle DBMS Driverの設定

Oracleを使用する場合、データベースドライバの設定を以下のいずれかの方法で変更する必要があります。

- Control Center内で: メインメニューの→管理 → コントロールメニュー内の**Dr. Web Server**設定→ データベース タブ → データベース ドロップダウンリストから **Oracle** を選択し、以下のフォーマットに従ってパラメータを設定します。
- サーバー設定ファイル内。



B3. PostgreSQL DBMSの使用

概要

Oracle Database、Microsoft SQL Serverなどの商用DBMSとは異なり、PostgreSQLはフリーウェアとして流通するオブジェクトリレーショナルDBMSです。大規模なアンチウイルスネットワーク内でDr.Web Enterprise Security Suiteの外部DBとしてPostgreSQL DBMSを使用できます。

PostgreSQLを外部データベースとして使用するには

1. PostgreSQLサーバーまたはPostgres Proサーバーをインストールします。
2. それぞれの外部データベースを使用するようDr.Web Serverをセットアップします。この操作は[設定ファイル](#)内、またはDr.Web Security Control Center経由(**Dr.Web Server**設定→データベース タブ)で行うことができます。



PostgreSQL DBとの接続には、信頼認証、パスワード認証、およびMD5認証のみが使用できます。

インストールと対応バージョン

1. このフリーPostgreSQL製品 (PostgreSQLサーバーおよび対応するODBCドライバ)の最新のバージョンをダウンロードするようにしてください。それ以外の場合でも、**8.4**(Postgres Proでは11.4.1)よりも古いバージョンは使用しないでください。
2. 以下のうちいずれかの方法でPostgreSQLデータベースを作成します。
 - a) pgAdminグラフィカルインターフェースを使用して
 - b) CREATE DATABASE SQLコマンドを使用して



データベースはUTF8エンコーディングで作成する必要があります。

外部データベースへの変換の詳細については、[Dr.Web Enterprise Security SuiteのDBMSの種類の変更](#)を参照してください。

また、PostgreSQL外部データベースを操作する際のDr.Web Serverのシステム要件に注意してください(インストールマニュアルの[システム要件](#)を参照)。

パラメータ

PostgreSQLデータベースの設定には表B-4に記載されたパラメータを使用します。



表B-4 PostgreSQLのパラメータ

名前	デフォルト値	説明
host	<UNIX domain socket>	PostgreSQL Serverホスト
port		PostgreSQL Serverポート、またはソケットファイル名の拡張子
dbname	drwcs	データベース名
user	drwcs	ユーザー名
password	drwcs	パスワード
options		サーバーに送信するためのデバッグ/トレース オプション
requiressl		<ul style="list-style-type: none">• 1: SSL接続をリクエストする• 0: リクエストしない
temp_tablespaces		一時テーブル空間名
default_transaction_isolation		トランザクション分離レベル(PostgreSQLのマニュアルを参照してください)

詳細については、<https://www.postgresql.org/docs/>を参照してください。

UDS経由でのDr.Web ServerとPostgreSQL DBの連携

Dr.Web ServerとPostgreSQL DBが同一のコンピューターにインストールされている場合、UDS (UNIXドメインソケット) 経由でその連携を設定できます。

UDS経由で連携を設定するには

1. PostgreSQL設定ファイル(`postgresql.conf`)内で、UDSに以下のディレクトリを指定します。

```
unix_socket_directory = '/var/run/postgresql'
```
2. PostgreSQLを再起動させてください。

PostgreSQLデータベースの設定

PostgreSQLデータベースとのインタラクション時にパフォーマンスを向上させるには、このデータベースの公式ドキュメントの情報に従って設定を行うことを推奨します。



大規模なデータベースを使用して適切なコンピューティングリソースを費やす場合は、`postgresql.conf`設定ファイルで、次のパラメータを設定することを推奨します。

最小構成:

```
shared_buffers = 256MB  
temp_buffers = 64MB  
work_mem = 16MB
```

拡張設定:

```
shared_buffers = 1GB  
temp_buffers = 128MB  
work_mem = 32MB  
fsync = off  
synchronous_commit = off  
wal_sync_method = fdatasync  
commit_delay = 1000  
max_locks_per_transaction = 256  
max_pred_locks_per_transaction = 256
```



`fsync = off`パラメータはパフォーマンスを大幅に向上させますが、停電やシステムクラッシュの場合にはデータが完全に消失する可能性があります。`fsync`パラメータを「off」にするのは、データベースを完全に復元できるバックアップがある場合に限定されます。

`max_locks_per_transaction`パラメータの設定は、データベーステーブルの操作をなじみやすくスムーズなものにすることができ、特にデータベースを新しいバージョンにアップグレードするときに便利です。

B4. MySQL DBMSの使用

概要

MySQL - クロスプラットフォームのリレーショナルデータベース管理システムです。MySQL DBMSはDr.Web Enterprise Security Suiteの外部DBとして使用できます。



MySQLを外部データベースとして使用するには

1. MySQLサーバーをインストールします。
2. それぞれの外部データベースを使用するようDr.Web Serverをセットアップします。この操作は設定ファイル内、またはDr.Web Security Control Center経由(**Dr.Web Server**設定→データベース タブ)で行うことができます。

インストールと対応バージョン

Dr.Web Enterprise Security Suite は、次のバージョンのMySQL DBMSに対応しています。

- MySQL—5.5.14から5.7および8.0.12以降、
- MariaDB—10.0、10.1、10.2.

DBMSのインストール後、新しいデータベースを作成する前に設定ファイル内で以下の設定を指定する必要があります(詳細はDBMSドキュメントを参照)。

バージョン5.XのMySQLの場合:

```
[mysqld]
innodb_large_prefix = true
innodb_file_format = barracuda
innodb_file_per_table = true
max_allowed_packet = 64M
```

バージョン8.XのMySQLの場合:

```
[mysqld]
innodb_file_per_table = true
max_allowed_packet = 64M
```

使用するMariaDBのバージョンが10.2.4より前の場合は、設定ファイルで次のように設定する必要があります。

```
binlog_format = mixed
```

付録C. 管理者の認証



Dr.Web Serverでの管理者の認証に関する一般的な情報は、[管理者マニュアルの管理者の認証](#)を参照してください。

C1. Active Directory認証

認証方法の使用の有効化、および認証者リスト内の順番のみが設定されます(auth-ads.conf設定ファイルの<enabled/>および<order/>タグ内)。

動作原理:

1. 管理者は以下のいずれかのフォーマットでユーザー名およびパスワードを指定します。
 - username
 - domain\username
 - username@domain
 - ユーザーのLDAP DN
2. Serverはそれらのユーザー名およびパスワードをデフォルトのドメインコントローラ(またはユーザー名内で指定されたドメインに一致するドメインコントローラ)に登録します。
3. 登録に失敗した場合、次の認証メカニズムに移行します。
4. 登録されたユーザーのLDAP DNが識別されます。
5. 識別されたDNのオブジェクトについては、DrWebAdmin属性が読み込まれます。FALSE値を持っていた場合、認証は失敗と見なされ次の認証メカニズムに移行します。
6. この段階で、定義されていない属性があった場合、ユーザーが含まれているグループ内でそれらの属性を検索します。各グループに対しそれぞれの親グループもチェックされます(外から内へ)。



エラーが発生した場合は、次の認証メカニズムに移行します。

drweb-12.00.0-<build>-esuite-modify-ad-schema-<OS_version>.exeユーティリティ(Serverディストリビューションキットに含まれています)はActive Directory内に新しいオブジェクトクラスDrWebEnterpriseUserを作成し、このクラスに対して新しい属性を定義します。

属性はEnterprisespace内に以下のOIDを持っています。

```
DrWeb_enterprise_OID "1.3.6.1.4.1" // iso.org.dod.internet.private.enterprise
DrWeb_DrWeb_OID DrWeb_enterprise_OID ".29690" // DrWeb
DrWeb_EnterpriseSuite_OID DrWeb_DrWeb_OID ".1" // EnterpriseSuite
DrWeb_Alerts_OID DrWeb_EnterpriseSuite_OID ".1" // Alerts
DrWeb_Vars_OID DrWeb_EnterpriseSuite_OID ".2" // Vars
DrWeb_AdminAttrs_OID DrWeb_EnterpriseSuite_OID ".3" // AdminAttrs

// 1.3.6.1.4.1.29690.1.3.1 (AKA
iso.org.dod.internet.private.enterprise.DrWeb.EnterpriseSuite.AdminAttrs.Admin)

DrWeb_Admin_OID DrWeb_AdminAttrs_OID ".1" // R/W admin
```



```
DrWeb_AdminReadOnly_OID DrWeb_AdminAttrs_OID ".2" // R/O admin
DrWeb_AdminGroupOnly_OID DrWeb_AdminAttrs_OID ".3" // Group admin
DrWeb_AdminGroup_OID DrWeb_AdminAttrs_OID ".4" // Admin's group
DrWeb_Admin_AttrName "DrWebAdmin"
DrWeb_AdminReadOnly_AttrName "DrWebAdminReadOnly"
DrWeb_AdminGroupOnly_AttrName "DrWebAdminGroupOnly"
DrWeb_AdminGroup_AttrName "DrWebAdminGroup"
```

Active Directoryユーザーの設定は、Active Directory Serverにおいて手動で変更できます(管理者マニュアルの[管理者の認証](#)を参照)。

管理者に対するパーミッションは、その管理者が含まれているグループの階層ツリー内における全般的な継承の原則に従って割り当てられます。

C2. LDAP認証

設定はauth-ldap.conf設定ファイル内にあります。

設定ファイルの一般的なタグは以下のとおりです。

- `<enabled/>`および`<order/>` - Active Directoryと同様。
- `<server/>` - LDAP Serverアドレスを指定します。異なるLDAPサーバーアドレスの複数の`<server/>`タグを追加できます。これにより、認証に使用するサーバーのリストが作成されます。主に負荷を受けるメインサーバーを最初に指定し、残りのバックアップサーバーのアドレスをその後指定します。管理者が接続する際は、最初に使用可能なLDAPサーバーが使用されます。認証に失敗した場合、設定ファイル内にリストアップされているLDAPサーバーアドレスの順番に従って、次のサーバーで順次再試行されます。
- `<user-dn/>` - DOS同様のマスクを使用して名前をDN(Distinguished Name: 識別名)に変換する際のルールを定義します。

`<user-dn/>`タグ内では、以下のワイルドカードの使用が可能です。

- *は、. , = @ \ および空白を除く任意の記号のシーケンスと置き換えられます。
- #は、任意の記号のシーケンスと置き換えられます。

- `<user-dn-expr/>` - 正規表現を使用して名前をDNに変換する際のルールを定義します。

以下の2つは同じルールです。

```
<user-dn user="*@example.com" dn="CN=\1,DC=example,DC=com"/>
<user-dn-expr user="(.*@example.com" dn="CN=\1,DC=example,DC=com"/>
```

`\1 .. \9`は * 記号の値を置き換える場所、またはテンプレートでの角括弧内の表現を定義します。

この原理により、ユーザー名がlogin@example.comと指定されていた場合、変換後のDNは"CN=login,DC=example,DC=com"になります。

- `<user-dn-extension-enabled/>`では、ユーザー名のDNへの変換にldap-user-dn-translate.ds (プラグインフォルダから)のLUAスクリプトの実行が許容されます。このスクリプトは、適切なルールがない場合に、user-dn、user-dn-exprルールの使用が試行された後で実行されます。スクリプトのパラメータは1つです(ユーザー名の指定)。スクリプトからはDNを含む文字列が返されるか、何も返されません。適切なルールがなく、スクリプトが無効になっているか、結果を何も返さない場合には、指定したユーザー名がそのまま使用されます。
- 変換の結果定められたDNに対するLDAPオブジェクトの属性およびその可能な値はタグによって定義されます(デフォルト値が提示されます)。

```
<!-- DrWebAdmin attribute equivalent (OID 1.3.6.1.4.1.29690.1.3.1) -->
<admin-attribute-name value="DrWebAdmin" true-value="^TRUE$" false-
value="^FALSE$"/>
```



`true-value/false-value`パラメータの値として、正規表現が指定されます。

- 定義されていない管理者属性の値が存在し、設定ファイル内で`<group-reference-attribute-name value="memberOf"/>`タグが設定されている場合、`memberOf`属性の値はこの管理者が含まれているDNグループのリストであると見なされ、必要な属性の検索はActive Directoryの場合と同様にそのグループ内で実行されます。

C3. LDAP/AD認証

設定ファイル

設定は`auth-ldap-rfc4515.conf`設定ファイル内にあります。

標準的な設定の設定ファイルも用意されています。

- `auth-ldap-rfc4515-check-group.conf` - Active Directoryグループに属しているかどうかを確認して簡易スキーマを使うLDAPによる、管理者の外部認証用設定ファイルテンプレート。
- `auth-ldap-rfc4515-check-group-novar.conf` - Active Directoryグループに属しているかどうかを確認して簡易スキーマを使い、変数を用いるLDAPによる、管理者の外部認証用設定ファイルテンプレート。
- `auth-ldap-rfc4515-simple-login.conf` - 簡易スキーマを使うLDAPによる、管理者の外部認証用設定ファイルテンプレート。

`auth-ldap-rfc4515.conf`設定ファイルの一般的なタグは以下のとおりです。

- `<server />` - LDAPサーバー定義。

属性	説明	デフォルト値
<code>base-dn</code>	検索が実行されるオブジェクトエントリの相対DN。	Root DSEオブジェクトの <code>rootDomainNamingContext</code> 属性値
<code>cacertfile</code>	ルート証明書ファイル(UNIXのみ)。	-
<code>host</code>	LDAPサーバーのアドレス。	<ul style="list-style-type: none"> • Windows OSのサーバーのドメインコントローラー。 • UNIX系OS環境のサーバーの場合は127.0.0.1。 • 異なるLDAPサーバーアドレスの複数の<code><server/></code>タグを追加できます。主に負荷を受けるメインサーバーを最初に指定します。認証に失敗した場合、指定された順番に従って、次のサーバーで順次再試行されます。
<code>scope</code>	検索範囲。可能な値は次のとおりです。 <ul style="list-style-type: none"> • <code>sub-tree</code> - ベースDN以下のサブツリー全体 • <code>one-level</code> - ベースDN直下 • <code>base</code> - ベースDN。 	<code>sub-tree</code>



属性	説明	デフォルト値
tls	LDAPへの接続でTLSを確立。	no
ssl	LDAPへの接続時にLDAPSプロトコルを使用。	no

- `<set />` - LDAP検索によって設定される変数。

属性	説明	デフォルト値
attribute	変数に値が割り当てられている属性名。省くことはできません。	-
filter	LDAPのRFC4515検索フィルター。	-
scope	検索範囲。可能な値は次のとおりです。 <ul style="list-style-type: none"> • sub-tree - ベースDN以下のサブツリー全体 • one-level - ベースDN直下 • base - ベースDN。 	sub-tree
search	検索が実行されるオブジェクトエントリの相対DN。	存在しない場合、 <code><server /></code> タグのbase-dnが使用されます。
variable	変数名。文字で始まり、文字と数字のみで構成される必要があります。省くことはできません。	-

変数は`<mask />`と`<expr />`タグのadd属性の値、`<filter />`タグのvalue属性の値で`\varname`として使用できます。`<set />`タグのsearch属性の値でも使用できます。変数で許可される再帰レベルは16です。検索で見つかった複数のオブジェクトが返された場合は、最初のものだけが使用されます。

- `<mask />` - ユーザー名のテンプレート。

属性	説明
add	置換要素とAND演算を使用して検索フィルターに追加される文字列。
user	DOSのようなメタシンボル(*と#)を使用するユーザー名マスク。省くことはできません。

例:

```
<mask user="*@#" add="sAMAccountName=\1" />
<mask user="*\*" add="sAMAccountName=\2" />
```

\1と\2は、user属性の一致するマスクのリンクです。

- `<expr />` - 正規表現を使用したユーザー名テンプレート(属性は`<mask />`の場合と同じ)。

例:

```
<expr user="^(.*)@([\^.,=@\s\\]+)$" add="sAMAccountName=\1" />
```



```
<expr user="^(.*)\\(.*)" add="sAMAccountName=\2" />
```

マスクと正規表現の対応は次のとおり。

マスク	正規表現
*	.*
#	[^.,=@\s\\]+

- `<filter />` - LDAP検索フィルター。

属性	説明
value	置換要素とAND演算を使用して検索フィルターに追加される文字列。

フィルターの連結

```
<set variable="admingrp" filter="& (objectclass=group) (cn=ESuite Admin)"
attribute="dn" />
<mask user="*\*" add="sAMAccountName=\2" />
<filter value="& (objectClass=user) (memberOf=\admingrp)" />
```

検索後にadmingrpが"CN=ESuite Admins,OU=some name,DC=example,DC=com"値を取得し、ユーザー入力はdomain\userだった場合、結果のフィルターは次のとおりです。

```
" (& (sAMAccountName=user) (& (objectClass=user) (memberOf=CN=ESuite
Admins,OU=some name,DC=example,DC=com))) "
```

LDAP/AD認証の設定例

次に、LDAPを使用した認証の一般的な設定例を示します。設定は、Control Centerの **管理** → **認証** → **LDAP/AD認証** セクション(アドバンス設定)で行います。

認証が必要な管理者の初期パラメータは次のとおりです。

- ドメイン: dc.test.local
- Active Directoryグループ: DrWeb_Admins

Control Centerの設定:

設定	値	
サーバーのタイプ	Microsoft Active Directory	
サーバーアドレス	dc.test.local	
認証するユーザーのログインプレート	アカウントマスク	test*または*@test.local
	ログイン	\1



設定	値	
認証するユーザーのメンバーシップ	名前	DrWeb_Admins
	ジョブの種類	グループ

C4. パーミッションセクション

表C-1 管理者権限とその機能一覧

コード	パーミッション	説明	Control Centerのセクション
端末グループを管理			
1*	端末グループのプロパティを確認	管理者がアンチウイルスネットワーク内で見ることのできるユーザーグループのリストです。アンチウイルスネットワークツリーには全てのシステムグループも表示されますが、その中で見ることができるのは指定されたグループリストに含まれている端末のみです。	アンチウイルスネットワーク アンチウイルスネットワーク → 全般 → プロパティ
2*	端末グループのプロパティを編集	管理者がプロパティを編集することのできるユーザーグループのリストです。 パーミッション1のリストにあるグループを含んでいる必要があります。	アンチウイルスネットワーク → 全般 → プロパティ
3	端末グループの設定を確認	管理者が設定を確認することのできるユーザーグループのリストです。また、管理者は、リストにあるグループをプライマリとする端末の設定も確認できます。 パーミッション1のリストにあるグループを含んでいる必要があります。	アンチウイルスネットワーク アンチウイルスネットワーク → 全般 → 実行中のコンポーネント
4	端末グループの設定を編集	パーミッション3に加え、編集が許可されています。 パーミッション3のリストにあるグループを含んでいる必要があります。	アンチウイルスネットワーク → 全般 → 隔離 設定 セクション内
5	端末プロパティを確認	管理者がプロパティを確認することのできる端末のプライマリであるユーザーグループのリストです。 パーミッション1のリストにあるグループを含んでいる必要があります。	アンチウイルスネットワーク アンチウイルスネットワーク → 全般 → プロパティ
6	端末プロパティを編集	ACL、拒否、許可などを含みます。	



コード	パーミッション	説明	Control Centerのセクション
		<p>パーミッション5に加え、編集が許可されています。</p> <p>パーミッション5のリストにあるグループを含んでいる必要があります。</p>	
8*	端末をグループに追加、または端末をグループから削除	<p>ユーザーグループのリストです。</p> <p>パーミッション1のリストにあるグループを含んでいる必要があります。</p>	
9	端末を削除	<p>管理者が削除することのできる端末のプライマリであるユーザーグループのリストです。</p> <p>パーミッション1のリストにあるグループを含んでいる必要があります。</p>	
10	リモートでのAgentのインストールとアンインストール	<p>選択されたIDを持つAgentのリモートインストールを行うことを管理者が許可されている端末が含まれたユーザーグループのリストです。</p> <p>パーミッション1のリストにあるグループを含んでいる必要があります。</p> <p>禁止されているオブジェクトがある場合、メニュー項目は表示されません。</p> <p>ネットワークインストールは、パーミッション16が許可されている場合にのみ、/esuite/network/index.dsから行うことができます。</p>	アンチウイルスネットワーク
11	端末の結合	<p>結合することのできる端末のユーザーグループのリストです。これらのグループは端末に対してプライマリである必要があります。端末を結合するためのアイコンはツールバーにあります。</p> <p>パーミッション1のリストにあるグループを含んでいる必要があります。</p>	
12*	統計一覧を確認	<p>管理者が統計を見ることのできるユーザーグループのリストです。</p> <p>このパーミッションでは、定期的にレポートを受信できるようServerスケジュールでタスクを作成できます。管理者がタスクに指定できるユーザーグループのリストがセットされます(レポートを受信する端末のグループ)。Everyoneが設定されている場合、リストの全てのグループについてレポートが受信されます。</p>	アンチウイルスネットワーク 統計 セクション内



コード	パーミッション	説明	Control Centerのセクション
		パーミッション1のリストにあるグループを含んでいる必要があります。	
23	ライセンスキーを変更	管理者がライセンスキーを追加／変更／削除することができるユーザーグループのリストです。これらのグループは端末にとってプライマリである必要があります。 パーミッション1のリストにあるグループを含んでいる必要があります。	
管理者を管理			
25	管理者、管理者グループを作成	ツールバー上の該当するアイコンは表示されません。	管理 → 設定 → 管理者
26	管理者アカウントを編集	新規端末 グループの管理者には、ルートノードがその管理者のグループである管理者ツリーのみ、すなわち、自身のグループとそのサブグループの管理者のみ表示されます。管理者グループの管理者には、所属グループに関わりなく他の全ての管理者が表示されます。 管理者は指定されたグループの管理アカウントを編集できます。その際、該当するアイコンがツールバーで使用可能になります。	
27	管理者アカウントを削除	パーミッション26と同じです。管理者は指定されたグループの管理アカウントを削除できます。	
28	管理者グループのプロパティと設定を確認	グループおよびサブグループ内の管理者を含みます。 管理者は、親グループのサブグループからのみ選択できます。	
39	「Newbies」管理者グループを表示	プリインストールされた Newbies (新規端末) グループを管理者ツリー内で確認することを管理者に対して許可します。 管理者が Newbies (新規端末) グループを表示するパーミッションを持っていない場合や、管理者がこのグループに属している場合、管理者には自分のアカウントのみが表示されます。	
29	管理者グループのプロパティと設定を編集	グループおよびサブグループ内の管理者を含みます。	



コード	パーミッション	説明	Control Centerのセクション
		<p>管理者は、親グループのサブグループからのみ選択できます。</p> <p>このパーミッションが拒否されている場合、このグループに対してパーミッション26が許可されている場合であっても、管理者は同グループ内の管理者に対するパーミッションの継承または追加を無効にすることはできません。</p>	
追加設定			
7	端末を作成	<p>端末作成時には、パーミッション8を持ったグループ(端末が含まれるグループはこのパーミッションを持っている必要があります)のリストのみ利用可能になります。</p> <p>端末の作成時には、利用可能なユーザーグループのうちの1つをプライマリにする必要があります。</p>	アンチウイルスネットワーク
13	監査ログを確認	監査ログは全権管理者のみ、およびパーミッション4を持ったオブジェクトに対してのみ使用可能です。	管理 → 統計 → 監査ログ
16	Network Scannerを起動	パーミッションが許可されなかった場合、/esuite/network/index.dsからのネットワークインストールは行うことができません。	アンチウイルスネットワーク 管理 → Network Scanner
17	新規端末を承認	<p>パーミッション8のグループリストを使用できます。</p> <p>管理者が一部のグループの管理のみ許可され、全てのアンチウイルスネットワークオブジェクトの管理は許可されていない場合には、このパーミッションは付与できません。このため、パーミッション1(端末グループのプロパティを確認)に対するグループセットが指定されます。</p>	アンチウイルスネットワーク
18	Serverスケジュールを確認	<p>タスク実行ログの表を表示します。</p> <p>パーミッション12および18が許可されていない場合、Serverスケジュールページを見ることはできません。</p> <p>パーミッション12が許可されており、パーミッション18が許可されていない場合、統計スケジュールを見ることができます。</p> <p>特定の管理者に対してレポートを送信するジョブは、パーミッション18が許可されていない</p>	管理 → 設定 → Dr.Web Server Task Scheduler 管理 → 統計 → タスク実行ログ



コード	パーミッション	説明	Control Centerのセクション
		場合であっても、パーミッション12および通知の定期レポートに応じて表示されます。	
19	Serverスケジュールを編集		管理 → 設定 → Dr.Web Server Task Scheduler
20	Server設定とリポジトリ設定を確認		管理 → 設定 → Web server設定
21	Server設定とリポジトリ設定を編集		管理 → リポジトリ → リポジトリの状態 管理 → リポジトリ → 更新の保留 管理 → リポジトリ → リポジトリ一般設定 管理 → リポジトリ → リポジトリの詳細な設定 管理 → リポジトリ → リポジトリコンテンツ 管理 → ログ → リポジトリ更新ログ 管理 → 設定 → ユーザーフック 管理 → Dr.Web Server → バージョンリスト
22	ライセンス情報を確認		管理 → 管理 → ライセンスマネージャー
24	通知設定を編集		管理 → 通知 → 通知設定 管理 → 通知 → 未送信通知 管理 → 通知 → Webコンソール通知
30	XML API経由で操作		-
31	隣接ネットワーク接続を確認		Neighbors
32	隣接ネットワーク接続を編集		Neighbors



コード	パーミッション	説明	Control Centerのセクション
33	追加機能を使用	常に使用可能であるユーティリティサブセクションを除く、追加機能セクションに含まれる全ての項目へのアクセスを制限します。	管理 → 追加の機能
34	リポジトリの更新	ServerリポジトリをGUSから更新します。	リポジトリの状態 セクションの リポジトリの更新 ボタン
42	自身の設定を編集するには	自身の管理者アカウントの設定を編集することを許可するパーミッションです。	管理 → 設定 → 管理者

*パーミッション1、2、8、12は端末のプライマリグループではなく、端末が含まれているグループのリストによって端末に対して定義されます。

これらパーミッションの一部が許可されているグループに端末が含まれている場合、管理者はグループが端末のプライマリであるかどうかに関係なく、これらのパーミッションに対応する機能にアクセスできるようになります。その際、許可が優先されます。すなわち、端末が許可されたグループと拒否されたグループの両方に含まれていた場合、管理者は許可されたグループのパーミッションに対応する機能に対してアクセスできるようになります。



付録D. 通知システムの設定



管理者通知の設定に関する基本的な情報については、[管理者マニュアルの通知設定](#)を参照してください。

D1. 通知システムパラメータの記述

アンチウイルスネットワークコンポーネントの動作に関連したイベントについての通知には以下の種類があります。

- Eメール通知
- Webコンソール経由での通知
- SNMP経由での通知
- Agentプロトコル経由での通知
- プッシュ通知

通知の送信方法によって、key -> value形式でのパラメータが必要です。送信方法ごとに以下のパラメータを設定します。

表D-1. 全般的パラメータ

パラメータ	説明	デフォルト値	必須
TO	通知の受信者。" "を区切り文字として使用することにより、複数の受信者を指定できます。		yes
ENABLED	通知の送信の有効または無効	trueまたはfalse	yes
_TIME_TO_LIVE	通知送信に失敗した場合の再試行回数	10回	no
_TRY_PERIOD	通知の再送信を試行する間隔(秒)	300秒(300秒に1回以上の頻度で送ることはできません)	no

送信方法ごとのパラメータは以下のとおりです。

表D-2. Eメール通知

パラメータ	説明	デフォルト値
FROM	Eメール送信者のアドレス	drwcsd@\${host name}
TO	Eメール受信者のアドレス	-
HOST	SMTP Serverのアドレス	127.0.0.1



パラメータ	説明	デフォルト値
PORT	SMTP Serverのポート番号	<ul style="list-style-type: none">• SSLパラメータがnoの場合は25• SSLパラメータがyesの場合は465
USER	SMTP Serverユーザー	"" ※未設定 ユーザーが指定された場合、少なくとも1つの認証方法が有効になっている必要があります。そうでない場合、メールは送信されません。
PASS	SMTP Serverユーザーのパスワード	"" ※未設定
STARTTLS	データ転送を暗号化します。その際、STARTTLSコマンドを使用して安全な接続への切り替えが実行されます。接続にはデフォルトで25番ポートが使用されます。	yes
SSL	データ転送を暗号化します。その際、安全なTLS接続が新たに確立されます。接続にはデフォルトで465番ポートが使用されます。	no
AUTH-CRAM-MD5	CRAM-MD5認証を使用	no
AUTH-PLAIN	PLAIN認証を使用	no
AUTH-LOGIN	LOGIN認証を使用	no
AUTH-NTLM	NTLM認証を使用	no
SSL-VERIFYCERT	SSL証明書を検証	no
DEBUG	デバッグモードを有効化(認証失敗時に問題を解決するためなどに使用)	-

表D-3. Webコンソール経由での通知

パラメータ	説明	デフォルト値
TO	通知の送信先となる管理者のUUID	-
SHOW_PERIOD	受信時から数えて、メッセージを保存しておく期間(秒)	86400秒(1日)

表D-4. SNMP経由での通知

パラメータ	説明	デフォルト値
TO	SNMP受信者(IPアドレスなど)	-



パラメータ	説明	デフォルト値
DOMAIN	ドメイン	<ul style="list-style-type: none">Windows OSでは localhostUNIX系OSでは""
COMMUNITY	SNMPコミュニティまたはコンテキスト	public
RETRIES	APIによる通知の再送信試行回数	5回
TIMEOUT	APIが通知の再試行を実行するまでの間隔(秒)	5秒

表D-5. Agentプロトコル経由での通知

パラメータ	説明	デフォルト値
TO	受信する端末のUUID	-
SHOW_PERIOD	受信時から数えて、メッセージを保存しておく期間(秒)	86400秒(1日)

表D-6. プッシュ通知

パラメータ	説明	デフォルト値
TO	ベンダー(Appleなど)のサーバーへの登録後にアプリケーションが取得するデバイストークン	-
SERVER_URL	ベンダーサーバーへの通知の送信に使用する、サーバーのURLリレー	-

D2. 通知テンプレートのパラメータ

メッセージのテキストは、テンプレートファイルに基づいてテンプレートプロセッサとサーバーコンポーネントによって作成されます。



Windowsネットワークメッセージシステムは、Windows Messenger(Net Send)サービスをサポートしているWindows環境でのみ使用できます。

Windows Vista以降のOSではWindows Messengerサービスをサポートしていません。

テンプレートファイルは中括弧で囲まれたテキストと変数から成っています。テンプレートファイルを編集するには以下の変数を使用できます。

変数:

- { <VAR> } - <VAR>変数の現在の値の代わりになります。



- { <VAR>: <N> } - <VAR>変数の最初から<N>文字の指定です。
- { <VAR>: <first>: <N> } - <VAR> 変数の最初の文字から<first>キャラクタ (<first>+1 字目)以降の <N>文字の指定です。残りがそれよりも少ない場合、右側に空白を置いて補います。
- { <VAR>: <first>:- <N> } - <VAR> 変数の最初の文字から<first>キャラクタ (<first>+1 字目)以降の <N>文字の指定です。残りがそれよりも少ない場合、左側に空白を置いて補います。
- { <VAR>/ <original1>/ <replace1>[/ <original2>/ <replace2>] } - <VAR>変数の指定されたキャラクタを別のキャラクタに置き換えます。<original1>は <replace1>に置き換えられ、<original2>は <replace2>に置き換えられます。
置換ペアの数には制限はありません。
- { <VAR>/ <original1>/ <replace1>[{ <SUB_VAR> }] [/ <original2>/ <replace2>] } - 上記と同様に指定された値に置換されますが、<SUB_VAR>のネストされた変数が使用されます。ネストされた変数を持つアクションは、親変数を持つアクションと同じです。
再帰的置換のネストレベルには制限はありません。
- { <VAR>/ <original1>/ <replace1>/ <original2>/ <replace2>/ * / <replace3> } - 上記と同様に指定された値に置換されますが、リストにあげたoriginalの値と一致しない場合は、<replace3>からの値にも置換できます。また、<VAR>に<original1>または<original2>のいずれかが見つからなかった場合は、すべての値が<replace3>に置き換えられます。

表D-7変数の表記

変数	値	表現	結果
SYS.TIME	10:35:17:456	{SYS.TIME:5}	10:35
SYS.TIME	10:35:17:456	{SYS.TIME:3:5}	35:17
SYS.TIME	10:35:17:456	{SYS.TIME:3:-12}	°°35:17:456
SYS.TIME	10:35:17:456	{SYS.TIME:3:12}	35:17:456°°
SYS.TIME	10:35:17:456	{SYS.TIME/10/99/35/77}	99:77:17.456

表記規則

° - 空白

環境変数

メッセージテキストの作成にサーバープロセスの環境変数を使用できます(**System**ユーザー)。

環境変数はControl Centerメッセージエディタ内の **ENV** ドロップダウンリストから使用できます。変数はENV.プレフィックスを用いて指定する必要があります(プレフィックスの終わりにはピリオドが付きます)。

システム変数

- SYS.BRANCH - システムバージョン(サーバーおよびAgent)
- SYS.BUILD - サーバーがビルドされた日付



- `SYS.DATE` - システムの現在の日付
- `SYS.DATETIME` - システムの現在の日時
- `SYS.HOST` - ServerのDNS名
- `SYS.MACHINE` - Serverがインストールされているコンピューターのネットワークアドレス。
- `SYS.OS` - Serverがインストールされているコンピューターのオペレーティングシステム名。
- `SYS.PLATFORM` - Serverプラットフォーム
- `SYS.PLATFORM.SHORT` - `SYS.PLATFORM`の短い変数
- `SYS.SERVER` - 製品名 (Dr.Web Server)
- `SYS.TIME` - システムの現在の時間
- `SYS.VERSION` - Serverバージョン

端末の共通変数

- `GEN.LoginTime` - 端末のログイン時間
- `GEN.StationAddress` - 端末のアドレス
- `GEN.StationDescription` - 端末の説明
- `GEN.StationID` - 端末固有の識別子
- `GEN.StationLDAPDN` - Windows OSの端末の識別名。ADS/LDAPドメインに含まれる端末に関連します。
- `GEN.StationMAC` - 端末のMACアドレス
- `GEN.StationName` - 端末名
- `GEN.StationPrimaryGroupID` - 端末のプライマリグループのID
- `GEN.StationPrimaryGroupName` - 端末のプライマリグループ名
- `GEN.StationSID` - 端末のセキュリティID

リポジトリの共通変数

- `GEN.CurrentRevision` - 現在のバージョンの識別子
- `GEN.Folder` - 製品のあるフォルダ
- `GEN.NextRevision` - 更新したバージョンの識別子
- `GEN.Product` - 製品名



種類別の通知パラメータと変数

管理者

管理者認証に失敗しました

パラメータ	値	
通知の送信理由	Control Centerでの管理者認証時にエラーが発生した場合に送信されます。通知には認証失敗の理由が記載されています。	
通知設定	必要ありません。	
変数	MSG.Login	ログイン
	MSG.Address	Control Centerのネットワークアドレス
	MSG.LoginErrorCode	数値のエラーコード

未知の管理者

パラメータ	値	
通知の送信理由	Control Centerで、未知のログインを使用した管理者による認証の試みが行われた場合に送信されます。	
通知設定	必要ありません。	
変数	MSG.Login	ログイン
	MSG.Address	Dr.Web Security Control Centerのネットワークアドレス

インストール

このグループのメッセージには、[上](#)の端末の共通変数を使用することもできます。

端末でのインストールに失敗しました

パラメータ	値	
通知の送信理由	端末上でのAgentのインストール中にエラーが発生した場合に送信されます。通知にはエラーの理由が記載されています。	
通知設定	必要ありません。	
変数	MSG.Error	エラーメッセージ



端末上でのインストールが完了しました

パラメータ	値
通知の送信理由	端末上でのAgentのインストールが成功した場合に送信されます。
通知設定	必要ありません。
変数	ありません。

ライセンス

グループ内の端末数がライセンスで指定された上限に近づいています

パラメータ	値	
通知の送信理由	グループ内の端末数が、そのグループに割り当てられたキーで指定されたライセンスの上限に近づいている場合に送信されます。	
通知設定	キー内で使用可能なライセンスの残り数が3つ未満、またはライセンス合計数の5%未満になった場合に通知が送信されます。	
変数	MSG.Free	残っている空きライセンスの数
	MSG.Licensed	このグループのライセンスを使用している端末の数
	MSG.Total	グループに割り当てられているすべてのキー内のライセンス合計数 注意: グループのライセンスキーは他のライセンスするオブジェクトにも割り当てることができます。
	GEN.StationPrimaryGroupID	プライマリグループID
	GEN.StationPrimaryGroupName	プライマリグループ名

オンライン端末数の上限を超えています

パラメータ	値
通知の送信理由	端末からServerへの接続中に、その端末が含まれているグループ内の端末数が、ライセンスキーによって割り当てられている上限に達している場合に送信されます。 新しい端末をServerに登録することはできません。
通知設定	必要ありません。



パラメータ	値	
変数	MSG.ID	端末UUID
	MSG.StationName	端末名
	上 の端末の共通変数を使用することもできます。	

ライセンスキーを自動で更新できません

パラメータ	値	
通知の送信理由	現在のキーと新しいキーとでライセンスされるコンポーネントが異なるために、ライセンスキーを自動的に更新できない場合に送信されます。この場合、新しいキーは正常にダウンロードされますが、古いライセンスキーの全てのオブジェクトに対しては配信されません。手動でライセンスキーを置き換える必要があります。	
通知設定	ライセンスの自動更新の詳細については、「管理者マニュアル」のp. 「ライセンスの自動更新」 を参照してください。	
変数	MSG.ExpirationDate	ライセンスの期限が切れる日付
	MSG.Expired	<ul style="list-style-type: none">1 - 期限が切れている0 - 期限が切れていない
	MSG.KeyDifference	自動更新が不可能な理由: <ul style="list-style-type: none">現在のライセンスキーと新しいライセンスキーで、ライセンスされるコンポーネントの組み合わせが異なる新しいライセンスキーのライセンス数が現在のライセンスキーよりも少ない
	MSG.KeyId	古いライセンスキーの識別子
	MSG.KeyName	古いライセンスキーのユーザー名
	MSG.NewKeyId	新しいライセンスキーの識別子
	MSG.NewKeyName	新しいライセンスキーのユーザー名

ライセンスキーは自動で更新されました

パラメータ	値	
通知の送信理由	ライセンスキーが自動的に更新された場合に送信されます。その場合、新しいキーがダウンロードされ、古いライセンスキーの全てのオブジェクト上に配信されています。	
通知設定	ライセンスの自動更新の詳細については、「管理者マニュアル」のp. 「ライセンスの自動更新」 を参照してください。	



パラメータ	値	
変数	MSG.KeyId	古いライセンスキーの識別子
	MSG.KeyName	古いライセンスキーのユーザー名
	MSG.NewKeyId	新しいライセンスキーの識別子
	MSG.NewKeyName	新しいライセンスキーのユーザー名

ライセンスキーがブロックされています

パラメータ	値	
通知の送信理由	Dr.Web Global Update Systemからの更新中に、ライセンスキーのブロックに関する情報が受信された場合に送信されます。これ以降、このキーは使用できません。	
通知設定	ブロックの詳しい理由については、テクニカルサポートサービスにお問い合わせください。	
変数	MSG.KeyId	ライセンスキーのID
	MSG.KeyName	ライセンスキーのユーザー名

提供するライセンスの数が上限に達しました

パラメータ	値	
通知の送信理由	隣接Serverに提供するためにリクエストされたライセンスの数が、そのライセンスキーで使用可能なライセンスの数を超過している場合に送信されます。	
通知設定	必要ありません。	
変数	MSG.ObjId	ライセンスキーID

ライセンス提供期限が切れています

パラメータ	値	
通知の送信理由	このServerのライセンスキーから隣接Serverへのライセンス提供の期限が切れている場合に送信されます。	
通知設定	隣接Serverへのライセンス提供の期限は 管理 → Dr.Web Serverの設定 → ライセンス セクション内で指定します。	
変数	MSG.ObjId	ライセンスキーID
	MSG.Server	隣接Server名



ライセンスキー内のライセンス数の制限

パラメータ	値	
通知の送信理由	Serverの起動中に、グループ内の端末数がライセンスキーによって割り当てられている上限に達していることが判明した場合に送信されます。	
通知設定	必要ありません。	
変数	MSG.KeyId	ライセンスキーのID
	MSG.KeyName	ライセンスキーユーザー名
	MSG.Licensed	許可されるライセンスの数
	MSG.LicenseLimit	ライセンスの状態: <ul style="list-style-type: none">• 1 - ライセンスキー内の空きライセンスの数がなくなりかけています。• 2 - ライセンスキー内の空きライセンスの数がなくなりました。• 3 - ライセンスキーを割り当てられたオブジェクトの数が、このキーで許可されている数を超過しています。
	MSG.Licensed	キーが割り当てられているオブジェクトの数
	MSG.Total	キー内のライセンス数

ライセンスキーの有効期限切れ

パラメータ	値	
通知の送信理由	ライセンスキーの有効期限切れが近づいていて、ライセンスの自動更新を使用できない場合に送信されます。	
通知設定	必要ありません。	
変数	MSG.ExpirationDate	ライセンスの期限が切れる日付
	MSG.Expired	<ul style="list-style-type: none">• 1 - 期限が切れている• 0 - 期限が切れていない
	MSG.KeyId	ライセンスキーの識別子
	MSG.KeyName	ライセンスキーのユーザー名



新規端末

このグループのメッセージには、[上](#)の端末の共通変数を使用することもできます。

端末は承認待ちです

パラメータ	値
通知の送信理由	新規端末がServerとの接続を要求していて、管理者によって手動で承認または拒否を行う必要がある場合に送信されます。
通知設定	これは、 管理 → Dr.Web Server設定 → 全般 セクション内で 新規端末登録モード オプションに 手動でアクセスを承認する の値が設定されている場合に起こる可能性があります。
変数	ありません。

端末は自動的に拒否されました

パラメータ	値
通知の送信理由	新規端末がServerとの接続を要求し、それがServerによって自動的に拒否された場合に送信されます。
通知設定	これは、 管理 → Dr.Web Server設定 → 全般 セクション内で 新規端末登録モード オプションに 常にアクセスを拒否する が設定されている場合に起こる可能性があります。
変数	ありません。

端末は管理者によって拒否されました

パラメータ	値	
通知の送信理由	新規端末がServerとの接続を要求し、それが管理者によって手動で拒否された場合に送信されます。	
通知設定	これは、 管理 → Dr.Web Server設定 → 全般 セクション内で 新規端末登録モード オプションに 手動でアクセスを承認する の値が設定されていて、管理者が該当する端末に対して アンチウイルスネットワーク → 未承認端末 → 選択した端末を拒否 オプションを指定していた場合に起こる可能性があります。	
変数	MSG.AdminAddress	Control Centerのネットワークアドレス
	MSG.AdminName	管理者名



リポジトリ

このグループのメッセージには、[上](#)のリポジトリの共通変数を使用することもできます。

リポジトリ製品の更新は「凍結」状態です

パラメータ	値
通知の送信理由	リポジトリ製品の状態が管理者によって凍結状態にされている場合に送信されます。その場合、この製品に対するGUSからの更新は実行されません。
通知設定	管理 → リポジトリの詳細な設定 セクション内でリポジトリ製品を凍結または凍結解除の状態に設定できます。
変数	ありません。

リポジトリ製品の更新を開始しました

パラメータ	値
通知の送信理由	リポジトリの更新確認中に、該当する製品の更新が必要であると判断された場合に送信されます。その場合、GUSからの更新が開始されます。
通知設定	必要ありません。
変数	ありません。

リポジトリの更新は既に実行中です

パラメータ	値
通知の送信理由	Serverの更新中に他の更新が開始された場合に送信されます。
通知設定	必要ありません。
変数	ありません。

リポジトリを更新することができません

パラメータ	値	
通知の送信理由	GUSからのリポジトリまたはリポジトリ製品の更新中にエラーが発生した場合に送信されます。通知には、更新エラーの理由と製品名が記載されています。	
通知設定	必要ありません。	
変数	MSG.Error	エラーメッセージ



パラメータ	値	
	MSG.ExtendedError	エラーの詳細

リポジトリ製品は最新の状態で

パラメータ	値
通知の送信理由	リポジトリの更新確認中に、該当する製品が最新であると判断された場合に送信されます。その場合、この製品に対するGUSからの更新は必要ありません。
通知設定	必要ありません。
変数	ありません。



リポジトリ製品は最新の状態で テンプレートの変数には、設定ファイルで「**not to be notified of (通知しません)**」とマークされたファイルは含まれません。詳細については、[F1.設定ファイル .config の構文](#)を参照してください。

リポジトリ製品が更新されました

パラメータ	値	
通知の送信理由	GUSからのリポジトリ更新が正常に完了した場合に送信されます。	
通知設定	必要ありません。	
変数	MSG.Added	追加されたファイルのリスト(名前は一行ずつ)
	MSG.AddedCount	追加されたファイルの数
	MSG.Deleted	削除されたファイルのリスト(名前は一行ずつ)
	MSG.DeletedCount	削除されたファイルの数
	MSG.Replaced	置き換えられたファイルのリスト(名前は一行ずつ)
	MSG.ReplacedCount	置き換えられたファイルの数

ディスク空き容量が足りません

パラメータ	値
通知の送信理由	var フォルダの置かれているディスクの空き容量が足りなくなっている場合に送信されます。



パラメータ	値	
通知設定	ディスクの空き容量不足は、環境変数によって再定義されない限り、残り315 MB未満または1000 inode未満 (UNIX系OSの場合)と定義されます。	
変数	<u>上</u> のリポジトリの共通変数は使用することができません。	
	MSG.FreeInodes	空きinodeファイルディスクリプタの数 (一部のUNIX系OSにのみ該当)
	MSG.FreeSpace	空き容量 (バイト)
	MSG.Path	空き容量の少ないフォルダへのパス
	MSG.RequiredInodes	動作に必要な空きinode数 (一部のUNIX系OSにのみ該当)
	MSG.RequiredSpace	動作に必要な空き容量

その他

Application Controlによる多数のブロックが検出されました

パラメータ	値	
通知の送信理由	Application Controlによって端末上で多数のアプリケーションがブロックされた場合に送信されます。	
通知設定	多数のブロックされたアプリケーションに関する通知の送信を有効にするには、 管理 → Dr.Web Serverの設定 → 統計 セクション内で Application Controlによる複数のブロック にチェックを入れ、同じセクション内で該当するパラメータを設定してください。	
変数	MSG.Total	ブロックの合計数
	MSG.Profile	ブロックに最も多く使用されているプロファイル (それによってブロックが実行されたプロファイル) の数

異常終了した接続が多数検出されました

パラメータ	値
通知の送信理由	クライアント (端末、Agentインストーラ、隣接Server、Proxy Server) との接続が多数異常終了した場合に送信されます。
通知設定	多数の異常終了した接続に関する通知の送信を有効にするには、 管理 → Dr.Web Serverの設定 → 統計 セクション内で 異常終了した接続 にチェックを入れ、同じセクション内で該当するパラメータを設定してください。



パラメータ	値	
変数	MSG.Total	終了した接続の数
	MSG.AddrCount	切断されたアドレスの数

Serverログローテーションエラー

パラメータ	値	
通知の送信理由	Server動作ログのローテーション中にエラーが発生した場合に送信されます。通知にはエラーの理由が記載されています。	
通知設定	必要ありません。	
変数	MSG.Error	メッセージテキスト

Serverログ書き込みエラー

パラメータ	値	
通知の送信理由	Server動作ログへの情報の書き込み中にエラーが発生した場合に送信されません。通知にはエラーの理由が記載されています。	
通知設定	必要ありません。	
変数	MSG.Error	メッセージテキスト

ネットワーク内で感染拡大が検出されました

パラメータ	値	
通知の送信理由	アンチウイルスネットワーク内で大規模感染が確認された場合に送信されます。これは、指定された期間に、指定された数を超える脅威がネットワーク内で検出された場合を意味します。	
通知設定	感染拡大に関する通知の送信を有効にするには、 管理 → Dr.Web Serverの設定 → 統計 セクション内で 感染拡大の追跡 にチェックを入れてください。同じセクション内で、感染拡大の検出に関するパラメータを指定することができます。	
変数	MSG.Infected	検出された脅威の総数
	MSG.Virus	最も多く検出された脅威



隣接Serverは長い間接続していません

パラメータ	値	
通知の送信理由	Serverスケジュール内のタスクに応じて送信されます。隣接Serverが長い間このServerに接続されていないという情報のほか、最後に接続された日付が記載されています。	
通知設定	隣接Serverが長期間接続されていないと見なされる期間は、 管理 → Dr.Web Server Task Schedule 内にあるServerスケジュールの 隣接Serverは長い間接続していません タスクで設定します。	
変数	MSG.LastDisconnectTime	Serverが最後に接続された時間
	MSG.StationName	隣接Server名

統計情報レポートの作成

パラメータ	値	
通知の送信理由	Serverスケジュール内のタスクに従って定期レポートが生成された後に送信されます。また、通知にはレポートファイルをダウンロードするためのパスが含まれています。	
通知設定	レポートは 管理 → Dr.Web Server Task Schedule 内で設定されるServerスケジュールの 統計情報レポート タスクに従って生成されます。	
変数	MSG.Attachment	レポートへのパス
	MSG.AttachmentType	MIMEの種類
	GEN.File	レポートファイル名

予防的保護のサマリーレポート

パラメータ	値	
通知の送信理由	ネットワーク端末の予防的保護コンポーネントから多数のレポートを受信した際に送信されます。	
通知設定	予防的保護のレポートに関する1件の通知を送信するには、 管理 → Dr.Web Serverの設定 → 統計 セクションで、 予防的保護のグループレポート フラグ を設定する必要があります。同じセクション内で、レポートのグループ化に関するパラメータを指定できます。	
変数	MSG.AutoBlockedActCount	自動的にブロックされた疑わしいアクティビティを持つプロセスの数
	MSG.AutoBlockedProc	自動的にブロックされた疑わしいアクティビティを持つプロセス



パラメータ	値																										
	<table border="1"><tr><td>MSG.HipsType</td><td>保護するオブジェクトのタイプ</td></tr><tr><td>MSG.IsShellGuard</td><td>自動ブロック時の予防的保護反応のタイプは次のとおりです。<ul style="list-style-type: none">• 認証されていないコードのブロック• 保護するオブジェクトへのアクセスを確認</td></tr><tr><td>MSG.ShellGuardType</td><td>自動イベントブロックでの認証されていないコード実行のブロックのうち最も一般的な原因</td></tr><tr><td>MSG.Total</td><td>ネットワークで検出された予防的保護イベントの総数</td></tr><tr><td>MSG.UserAllowedActCount</td><td>ユーザーが許可した疑わしいアクティビティを持つプロセスの数</td></tr><tr><td>MSG.UserAllowedHipsType</td><td>ユーザーがアクセスを許可した保護するオブジェクトの最も一般的なタイプ</td></tr><tr><td>MSG.UserAllowedIsShellGuard</td><td>ユーザーがアクセスを許可した場合、予防的保護反応のタイプは次のとおりです。<ul style="list-style-type: none">• 認証されていないコードのブロック• 保護するオブジェクトへのアクセスを確認</td></tr><tr><td>MSG.UserAllowedProc</td><td>ユーザーが許可した疑わしいアクティビティを持つプロセス</td></tr><tr><td>MSG.UserAllowedShellGuard</td><td>ユーザーが許可した認証されていないコード実行をブロックする最も一般的な理由</td></tr><tr><td>MSG.UserBlockedActCount</td><td>ユーザーがブロックした疑わしいアクティビティを持つプロセスの数</td></tr><tr><td>MSG.UserBlockedHipsType</td><td>ユーザーがブロックした保護するオブジェクトの最も一般的なタイプ</td></tr><tr><td>MSG.UserBlockedIsShellGuard</td><td>ユーザーがアクセスをブロックした場合、予防的保護反応のタイプは次のとおりです。<ul style="list-style-type: none">• 認証されていないコードのブロック• 保護するオブジェクトへのアクセスを確認</td></tr><tr><td>MSG.UserBlockedProc</td><td>ユーザーがブロックした疑わしいアクティビティのプロセス</td></tr></table>	MSG.HipsType	保護するオブジェクトのタイプ	MSG.IsShellGuard	自動ブロック時の予防的保護反応のタイプは次のとおりです。 <ul style="list-style-type: none">• 認証されていないコードのブロック• 保護するオブジェクトへのアクセスを確認	MSG.ShellGuardType	自動イベントブロックでの認証されていないコード実行のブロックのうち最も一般的な原因	MSG.Total	ネットワークで検出された予防的保護イベントの総数	MSG.UserAllowedActCount	ユーザーが許可した疑わしいアクティビティを持つプロセスの数	MSG.UserAllowedHipsType	ユーザーがアクセスを許可した保護するオブジェクトの最も一般的なタイプ	MSG.UserAllowedIsShellGuard	ユーザーがアクセスを許可した場合、予防的保護反応のタイプは次のとおりです。 <ul style="list-style-type: none">• 認証されていないコードのブロック• 保護するオブジェクトへのアクセスを確認	MSG.UserAllowedProc	ユーザーが許可した疑わしいアクティビティを持つプロセス	MSG.UserAllowedShellGuard	ユーザーが許可した認証されていないコード実行をブロックする最も一般的な理由	MSG.UserBlockedActCount	ユーザーがブロックした疑わしいアクティビティを持つプロセスの数	MSG.UserBlockedHipsType	ユーザーがブロックした保護するオブジェクトの最も一般的なタイプ	MSG.UserBlockedIsShellGuard	ユーザーがアクセスをブロックした場合、予防的保護反応のタイプは次のとおりです。 <ul style="list-style-type: none">• 認証されていないコードのブロック• 保護するオブジェクトへのアクセスを確認	MSG.UserBlockedProc	ユーザーがブロックした疑わしいアクティビティのプロセス
MSG.HipsType	保護するオブジェクトのタイプ																										
MSG.IsShellGuard	自動ブロック時の予防的保護反応のタイプは次のとおりです。 <ul style="list-style-type: none">• 認証されていないコードのブロック• 保護するオブジェクトへのアクセスを確認																										
MSG.ShellGuardType	自動イベントブロックでの認証されていないコード実行のブロックのうち最も一般的な原因																										
MSG.Total	ネットワークで検出された予防的保護イベントの総数																										
MSG.UserAllowedActCount	ユーザーが許可した疑わしいアクティビティを持つプロセスの数																										
MSG.UserAllowedHipsType	ユーザーがアクセスを許可した保護するオブジェクトの最も一般的なタイプ																										
MSG.UserAllowedIsShellGuard	ユーザーがアクセスを許可した場合、予防的保護反応のタイプは次のとおりです。 <ul style="list-style-type: none">• 認証されていないコードのブロック• 保護するオブジェクトへのアクセスを確認																										
MSG.UserAllowedProc	ユーザーが許可した疑わしいアクティビティを持つプロセス																										
MSG.UserAllowedShellGuard	ユーザーが許可した認証されていないコード実行をブロックする最も一般的な理由																										
MSG.UserBlockedActCount	ユーザーがブロックした疑わしいアクティビティを持つプロセスの数																										
MSG.UserBlockedHipsType	ユーザーがブロックした保護するオブジェクトの最も一般的なタイプ																										
MSG.UserBlockedIsShellGuard	ユーザーがアクセスをブロックした場合、予防的保護反応のタイプは次のとおりです。 <ul style="list-style-type: none">• 認証されていないコードのブロック• 保護するオブジェクトへのアクセスを確認																										
MSG.UserBlockedProc	ユーザーがブロックした疑わしいアクティビティのプロセス																										



パラメータ	値
	MSG.UserBlockedShellGuard ユーザーがブロックした認証されていないコード実行をブロックする最も一般的な原因

端末

このグループのメッセージには、[上](#)の端末の共通変数を使用することもできます。



マルチサーバーネットワークでは、隣接Serverの端末のイベントに関する通知を受信することができます。隣接するServerの接続を設定する場合にこのオプションを有効にできます(管理者マニュアルの[複数のDr.Web Server間の接続設定](#)セクションを参照)。

次の通知を使用して隣接Serverでイベントを受信できます。セキュリティに対する脅威が検出されました、予防的保護のレポート、スキャン中のエラー、スキャン統計情報。

予防的保護のレポート

パラメータ	値												
通知の送信理由	端末またはその隣接Serverの端末の予防的保護コンポーネントからレポートを受信した際に送信されます。												
通知設定	必要ありません。												
変数	<table border="1"><tbody><tr><td>MSG.AdminName</td><td>疑わしいプロセスでアクションを開始した管理者</td></tr><tr><td>MSG.Denied</td><td>疑わしいプロセスに対するアクションは次のとおりです。<ul style="list-style-type: none">拒否許可</td></tr><tr><td>MSG.HipsType</td><td>保護するオブジェクトのタイプ</td></tr><tr><td>MSG.IsShellGuard</td><td>予防的保護反応のタイプは次のとおりです。<ul style="list-style-type: none">認証されていないコードのブロック保護するオブジェクトへのアクセスを確認</td></tr><tr><td>MSG.Path</td><td>疑わしいアクティビティを持つプロセスへのパス</td></tr><tr><td>MSG.Pid</td><td>疑わしいアクティビティを持つプロセスのID</td></tr></tbody></table>	MSG.AdminName	疑わしいプロセスでアクションを開始した管理者	MSG.Denied	疑わしいプロセスに対するアクションは次のとおりです。 <ul style="list-style-type: none">拒否許可	MSG.HipsType	保護するオブジェクトのタイプ	MSG.IsShellGuard	予防的保護反応のタイプは次のとおりです。 <ul style="list-style-type: none">認証されていないコードのブロック保護するオブジェクトへのアクセスを確認	MSG.Path	疑わしいアクティビティを持つプロセスへのパス	MSG.Pid	疑わしいアクティビティを持つプロセスのID
MSG.AdminName	疑わしいプロセスでアクションを開始した管理者												
MSG.Denied	疑わしいプロセスに対するアクションは次のとおりです。 <ul style="list-style-type: none">拒否許可												
MSG.HipsType	保護するオブジェクトのタイプ												
MSG.IsShellGuard	予防的保護反応のタイプは次のとおりです。 <ul style="list-style-type: none">認証されていないコードのブロック保護するオブジェクトへのアクセスを確認												
MSG.Path	疑わしいアクティビティを持つプロセスへのパス												
MSG.Pid	疑わしいアクティビティを持つプロセスのID												



パラメータ	値																				
	<table border="1"><tr><td>MSG.ShellGuardType</td><td>認証されていないコードのブロック実行の原因</td></tr><tr><td>MSG.StationTime</td><td>端末でのイベント発生時間</td></tr><tr><td>MSG.Target</td><td>アクセス試行が行われた保護するオブジェクトへのパス</td></tr><tr><td>MSG.Total</td><td>予防的保護の自動反応時の拒否数</td></tr><tr><td>MSG.User</td><td>疑わしいプロセスを開始したユーザー</td></tr><tr><td>MSG.UserAction</td><td>疑わしいプロセスのアクションの実行者 <ul style="list-style-type: none">• user• 予防的保護の自動反応</td></tr><tr><td>GEN.ServerRecvLinkID</td><td>接続された端末の予防的保護レポートを送信した最後の隣接ServerのUUID (このServerに接続されている端末についてのレポートが受信された場合は空の値)</td></tr><tr><td>GEN.ServerRecvLinkName</td><td>接続された端末の予防的保護レポートを送信した最後の隣接Serverの名前 (このServerに接続されている端末についてのレポートが受信された場合は空の値)</td></tr><tr><td>GEN.ServerOriginatorID</td><td>予防的保護レポートを送信し、端末が接続されているServerのUUID</td></tr><tr><td>GEN.ServerOriginatorName</td><td>予防的保護レポートを送信し、端末が接続されているServerの名前</td></tr></table>	MSG.ShellGuardType	認証されていないコードのブロック実行の原因	MSG.StationTime	端末でのイベント発生時間	MSG.Target	アクセス試行が行われた保護するオブジェクトへのパス	MSG.Total	予防的保護の自動反応時の拒否数	MSG.User	疑わしいプロセスを開始したユーザー	MSG.UserAction	疑わしいプロセスのアクションの実行者 <ul style="list-style-type: none">• user• 予防的保護の自動反応	GEN.ServerRecvLinkID	接続された端末の予防的保護レポートを送信した最後の隣接ServerのUUID (このServerに接続されている端末についてのレポートが受信された場合は空の値)	GEN.ServerRecvLinkName	接続された端末の予防的保護レポートを送信した最後の隣接Serverの名前 (このServerに接続されている端末についてのレポートが受信された場合は空の値)	GEN.ServerOriginatorID	予防的保護レポートを送信し、端末が接続されているServerのUUID	GEN.ServerOriginatorName	予防的保護レポートを送信し、端末が接続されているServerの名前
MSG.ShellGuardType	認証されていないコードのブロック実行の原因																				
MSG.StationTime	端末でのイベント発生時間																				
MSG.Target	アクセス試行が行われた保護するオブジェクトへのパス																				
MSG.Total	予防的保護の自動反応時の拒否数																				
MSG.User	疑わしいプロセスを開始したユーザー																				
MSG.UserAction	疑わしいプロセスのアクションの実行者 <ul style="list-style-type: none">• user• 予防的保護の自動反応																				
GEN.ServerRecvLinkID	接続された端末の予防的保護レポートを送信した最後の隣接ServerのUUID (このServerに接続されている端末についてのレポートが受信された場合は空の値)																				
GEN.ServerRecvLinkName	接続された端末の予防的保護レポートを送信した最後の隣接Serverの名前 (このServerに接続されている端末についてのレポートが受信された場合は空の値)																				
GEN.ServerOriginatorID	予防的保護レポートを送信し、端末が接続されているServerのUUID																				
GEN.ServerOriginatorName	予防的保護レポートを送信し、端末が接続されているServerの名前																				

既知の脅威のハッシュによる脅威検出に関する予防的保護のレポート

パラメータ	値
通知の送信理由	既知の脅威のハッシュのリストからの脅威の検出で、端末またはその隣接Serverの端末の予防的保護コンポーネントからレポートを受信した際に送信されます。
通知設定	既知のハッシュのリストによる検出に関する通知は、既知の脅威のHash Bulletinの使用がライセンスされている場合 (Serverが使用するライセンスキーの1つ以上のライセンス) に限り可能です。 ライセンスマネージャー のセクションにある 許可されるHash Bulletinのリスト のパラメータで確認できるライセンスキーの情報から、ライセンスを確認できません (Hash Bulletinがライセンスされていない場合はこのパラメータは表示されません)。



パラメータ	値	
変数	MSG.AdminName	疑わしいプロセスでアクションを開始した管理者
	MSG.Denied	疑わしいプロセスに対するアクションは次のとおりです。 <ul style="list-style-type: none">• 拒否• 許可
	MSG.Document	検出された脅威のハッシュを含むBulletin
	MSG.HipsType	保護するオブジェクトのタイプ
	MSG.IsShellGuard	予防的保護反応のタイプは次のとおりです。 <ul style="list-style-type: none">• 認証されていないコードのブロック• 保護するオブジェクトへのアクセスを確認
	MSG.Path	疑わしいアクティビティを持つプロセスへのパス
	MSG.Pid	疑わしいアクティビティを持つプロセスのID
	MSG.SHA1	検出されたオブジェクトのSHA-1ハッシュ
	MSG.SHA256	検出されたオブジェクトのSHA-256ハッシュ
	MSG.ShellGuardType	認証されていないコードのブロック実行の原因
	MSG.StationTime	端末でのイベント発生時間
	MSG.Target	アクセス試行が行われた保護するオブジェクトへのパス
	MSG.Total	予防的保護の自動反応時の拒否数
	MSG.User	疑わしいプロセスを開始したユーザー
	MSG.UserAction	疑わしいプロセスのアクションの実行者 <ul style="list-style-type: none">• user• 予防的保護の自動反応
GEN.ServerRecvLinkID	接続された端末の予防的保護レポートを送信した最後の隣接ServerのUUID (このServerに接続されている端末についてのレポートが受信された場合は空の	



パラメータ	値	
		値)
	GEN.ServerRecvLinkName	接続された端末の予防的保護レポートを送信した最後の隣接Serverの名前 (このServerに接続されている端末についてのレポートが受信された場合は空の値)
	GEN.ServerOriginatorID	予防的保護レポートを送信し、端末が接続されているServerのUUID
	GEN.ServerOriginatorName	予防的保護レポートを送信し、端末が接続されているServerの名前

デバイスがブロックされました

パラメータ	値	
通知の送信理由	Dr.Webアンチウイルスコンポーネントによって端末デバイスへの接続がブロックされたらと端末から通知を受け取った場合に送信されます。	
通知設定	必要ありません。	
変数	MSG.Capabilities	デバイスの特性
	MSG.Class	デバイスのクラス(親グループの名前)
	MSG.Description	デバイスの説明
	MSG.FriendlyName	デバイスのユーザーフレンドリ名
	MSG.InstanceId	デバイスインスタンスの識別子
	MSG.User	ユーザー名

Application Controlが既知の脅威のハッシュリストにあるプロセスをブロックしました

パラメータ	値	
通知の送信理由	既知の脅威のハッシュリストに含まれているアプリケーションがApplication Controlコンポーネントによって端末上でブロックされた場合に送信されます。	
通知設定	<p>既知のハッシュのリストによる検出に関する通知は、既知の脅威のHash Bulletinの使用がライセンスされている場合 (Serverが使用するライセンスキーの1つ以上のライセンス) に限り可能です。</p> <p>ライセンスマネージャー のセクションにある 許可されるHash Bulletinのリスト のパラメータで確認できるライセンスキーの情報から、ライセンスを確認できません (Hash Bulletinがライセンスされていない場合はこのパラメータは表示されま</p>	



パラメータ	値	
	せん)。	
変数	MSG.AppCtlAction	適用されたアクション: <ul style="list-style-type: none">• 0 - 不明• 2 - ブロック• 3 - ブロック(信頼できるアプリケーションの一覧にない)• 5 - 拒否ルールによりブロック• 7 - ポリシー設定によりブロック
	MSG.AppCtlType	イベントタイプ: <ul style="list-style-type: none">• 0 - 不明• 1 - プロセスの起動• 2 - ホストプロセスの起動• 3 - スクリプトインタプリタの起動• 4 - モジュールのロード• 5 - ドライバのロード• 6 - MSIセットアップの起動• 7 - 新しい実行ファイルのディスクへのドロップ• 8 - ディスク上での実行ファイルの変更
	MSG.Document	ハッシュが含まれているBulletin
	MSG.Path	ブロックされたプロセスへのパス
	MSG.Profile	ブロックに使用されたプロファイル(それに従ってブロックが実行されたプロファイル)の名前
	MSG.Rule	ブロックに使用されたルール(それに従ってブロックが実行されたルール)の名前
	MSG.SHA256	ブロックされたプロセスのハッシュ(SHA-256)
	MSG.StationTime	プロセスがブロックされた際の端末の時刻
	MSG.Target	ホストプロセスの場合、ブロックされたスクリプトへのパス
	MSG.TargetSHA256	ホストプロセスの場合、ブロックされたスクリプトのハッシュ(SHA-256)
MSG.TestMode	テストモードがオンになっているかどうか	



パラメータ	値	
	MSG.User	ブロックされたオブジェクトを起動したユーザー

Application Controlがプロセスをブロックしました

パラメータ	値	
通知の送信理由	Application Controlによって端末上でアプリケーションがブロックされた場合に送信されます。	
通知設定	必要ありません。	
変数	MSG.AppCtlAction	適用されたアクション: <ul style="list-style-type: none">• 0 - 不明• 2 - ブロック• 3 - ブロック(信頼できるアプリケーションの一覧にない)• 5 - 拒否ルールによりブロック• 7 - ポリシー設定によりブロック
	MSG.AppCtlType	イベントタイプ: <ul style="list-style-type: none">• 0 - 不明• 1 - プロセスの起動• 2 - ホストプロセスの起動• 3 - スクリプトインタプリタの起動• 4 - モジュールのロード• 5 - ドライバのロード• 6 - MSIセットアップの起動• 7 - 新しい実行ファイルのディスクへのドロップ• 8 - ディスク上での実行ファイルの変更
	MSG.Path	ブロックされたプロセスへのパス
	MSG.Profile	ブロックに使用されたプロファイル(それに従ってブロックが実行されたプロファイル)の名前
	MSG.Rule	ブロックに使用されたルール(それに従ってブロックが実行されたルール)の名前
	MSG.SHA256	ブロックされたプロセスのハッシュ(SHA-256)



パラメータ	値	
	MSG.StationTime	プロセスがブロックされた際の端末の時刻
	MSG.Target	ホストプロセスの場合、ブロックされたスクリプトへのパス
	MSG.TargetSHA256	ホストプロセスの場合、ブロックされたスクリプトのハッシュ(SHA-256)
	MSG.TestMode	テストモードがオンになっているかどうか
	MSG.User	ブロックされたオブジェクトを起動したユーザー

セキュリティに対する脅威が検出されました

パラメータ	値	
通知の送信理由	端末から受け取った通知内に、感染が検出されたという報告があった場合に送信されます。管理通知には、検出された脅威に関する詳細な情報も含まれています。	
通知設定	必要ありません。	
変数	MSG.Action	検出時のアクション
	MSG.Component	コンポーネント名
	MSG.InfectionType	脅威の種類
	MSG.ObjectName	感染したオブジェクトの名前
	MSG.ObjectOwner	感染したオブジェクトのオーナー
	MSG.RunBy	コンポーネントを起動したユーザー
	MSG.ServerTime	イベントを受け取った時間(グリニッジ標準時)
	MSG.Virus	脅威名
	GEN.ServerRecvLinkID	接続された端末の予防的保護レポートを送信した最後の隣接ServerのUUID (このServerに接続されている端末についてのレポートが受信された場合は空の値)
	GEN.ServerRecvLinkName	接続された端末の予防的保護レポートを送信した最後の隣接Serverの名前 (このServerに接続されている端末につ



パラメータ	値	
		いてのレポートが受信された場合は空の値)
	GEN.ServerOriginatorID	予防的保護レポートを送信し、端末が接続されているServerのUUID
	GEN.ServerOriginatorName	予防的保護レポートを送信し、端末が接続されているServerの名前

既知の脅威のハッシュによって検出されたセキュリティ脅威

パラメータ	値	
通知の送信理由	端末からの通知で既知の脅威のハッシュのリストからの脅威検出が報告された場合に送信されます。管理通知には、検出された脅威に関する詳細情報も含まれています。	
通知設定	既知のハッシュのリストによる検出に関する通知は、既知の脅威のHash Bulletinの使用がライセンスされている場合 (Serverが使用するライセンスキーの1つ以上のライセンス) に限り可能です。 ライセンスマネージャー のセクションにある 許可されるHash Bulletinのリスト のパラメータで確認できるライセンスキーの情報から、ライセンスを確認できます (Hash Bulletinがライセンスされていない場合はこのパラメータは表示されません)。	
変数	MSG.Action	検出時のアクション
	MSG.Component	コンポーネント名
	MSG.Document	検出された脅威のハッシュを含むBulletin
	MSG.InfectionType	脅威の種類
	MSG.ObjectName	感染したオブジェクトの名前
	MSG.ObjectOwner	感染したオブジェクトのオーナー
	MSG.RunBy	コンポーネントを起動したユーザー
	MSG.SHA1	検出されたオブジェクトのSHA-1ハッシュ
	MSG.SHA256	検出されたオブジェクトのSHA-256ハッシュ
	MSG.ServerTime	イベントを受け取った時間 (グリニッジ標準時)
MSG.Virus	脅威名	



パラメータ	値	
	GEN.ServerRecvLinkID	接続された端末の予防的保護レポートを送信した最後の隣接ServerのUUID (このServerに接続されている端末についてのレポートが受信された場合は空の値)
	GEN.ServerRecvLinkName	接続された端末の予防的保護レポートを送信した最後の隣接Serverの名前 (このServerに接続されている端末についてのレポートが受信された場合は空の値)
	GEN.ServerOriginatorID	予防的保護レポートを送信し、端末が接続されているServerのUUID
	GEN.ServerOriginatorName	予防的保護レポートを送信し、端末が接続されているServerの名前

端末の認証に失敗しました

パラメータ	値	
通知の送信理由	Serverとの接続試行時に、端末から誤った認証情報が提供された場合に送信されます。通知には、端末の承認ポリシーに応じた、その後のアクションについても記載されています。	
通知設定	端末の承認ポリシーは、管理 → Dr.Web Server 設定 → 全般 セクションの 新規端末登録モード オプション内で設定します。	
変数	MSG.ID	端末UUID
	MSG.Rejected	値: <ul style="list-style-type: none">rejected - 端末へのアクセスは拒否されますnewbie - 端末に「新規端末 (newbie)」ステータスの割り当てを試みました
	MSG.StationName	端末名

端末アカウントを作成できません

パラメータ	値	
通知の送信理由	Server上で新規端末のアカウントを作成することができない場合に送信されます。エラーの詳細はServerログファイル内で確認できます。	
通知設定	必要ありません。	



パラメータ	値	
変数	MSG.ID	端末UUID
	MSG.StationName	端末名

スキャン中のエラー

パラメータ	値	
通知の送信理由	端末から受け取った通知内でスキャン中のエラーについて報告があった場合に送信されます。	
通知設定	必要ありません。	
変数	MSG.Component	コンポーネント名
	MSG.Error	エラーメッセージ
	MSG.ObjectName	オブジェクト名
	MSG.ObjectOwner	オブジェクトの所有者
	MSG.RunBy	コンポーネントを起動したユーザー
	MSG.ServerTime	イベントを受け取った時間(グリニッジ標準時)
	GEN.ServerRecvLinkID	接続された端末の予防的保護レポートを送信した最後の隣接ServerのUUID (このServerに接続されている端末についてのレポートが受信された場合は空の値)
	GEN.ServerRecvLinkName	接続された端末の予防的保護レポートを送信した最後の隣接Serverの名前 (このServerに接続されている端末についてのレポートが受信された場合は空の値)
	GEN.ServerOriginatorID	予防的保護レポートを送信し、端末が接続されているServerのUUID
GEN.ServerOriginatorName	予防的保護レポートを送信し、端末が接続されているServerの名前	

端末更新のクリティカルエラー

パラメータ	値
通知の送信理由	端末から受け取った通知内で、Serverからのアンチウイルスコンポーネントの更



パラメータ	値	
	新中にエラーが発生した旨の報告があった場合に送信されます。	
通知設定	必要ありません。	
変数	MSG.Product	更新された製品
	MSG.ServerTime	Serverがメッセージを受信した時間(ローカル)

既知の脅威のハッシュによる脅威検出時のスキャンエラー

パラメータ	値	
通知の送信理由	既知の脅威のハッシュのリストからの脅威検出でスキャンエラーが発生した場合に送信されます。	
通知設定	既知のハッシュのリストによる検出に関する通知は、既知の脅威のHash Bulletinの使用がライセンスされている場合 (Serverが使用するライセンスキーの1つ以上のライセンス) に限り可能です。 ライセンスマネージャー のセクションにある 許可される Hash Bulletin のリスト のパラメータで確認できるライセンスキーの情報から、ライセンスを確認できません (Hash Bulletinがライセンスされていない場合はこのパラメータは表示されません)。	
変数	MSG.Component	コンポーネント名
	MSG.Document	検出された脅威のハッシュを含む Bulletin
	MSG.Error	エラーメッセージ
	MSG.ObjectName	オブジェクト名
	MSG.ObjectOwner	オブジェクトの所有者
	MSG.RunBy	コンポーネントを起動したユーザー
	MSG.SHA1	検出されたオブジェクトのSHA-1ハッシュ
	MSG.SHA256	検出されたオブジェクトのSHA-256ハッシュ
	MSG.ServerTime	イベントを受け取った時間(グリニッジ標準時)
GEN.ServerRecvLinkID	接続された端末の予防的保護レポートを送信した最後の隣接ServerのUUID (このServerに接続されている端末についてのレポートが受信された場合は空の値)	



パラメータ	値						
	<table border="1"><tr><td>GEN.ServerRecvLinkName</td><td>接続された端末の予防的保護レポートを送信した最後の隣接Serverの名前 (このServerに接続されている端末についてのレポートが受信された場合は空の値)</td></tr><tr><td>GEN.ServerOriginatorID</td><td>予防的保護レポートを送信し、端末が接続されているServerのUUID</td></tr><tr><td>GEN.ServerOriginatorName</td><td>予防的保護レポートを送信し、端末が接続されているServerの名前</td></tr></table>	GEN.ServerRecvLinkName	接続された端末の予防的保護レポートを送信した最後の隣接Serverの名前 (このServerに接続されている端末についてのレポートが受信された場合は空の値)	GEN.ServerOriginatorID	予防的保護レポートを送信し、端末が接続されているServerのUUID	GEN.ServerOriginatorName	予防的保護レポートを送信し、端末が接続されているServerの名前
GEN.ServerRecvLinkName	接続された端末の予防的保護レポートを送信した最後の隣接Serverの名前 (このServerに接続されている端末についてのレポートが受信された場合は空の値)						
GEN.ServerOriginatorID	予防的保護レポートを送信し、端末が接続されているServerのUUID						
GEN.ServerOriginatorName	予防的保護レポートを送信し、端末が接続されているServerの名前						

スキャン統計情報

パラメータ	値																												
通知の送信理由	端末から受け取った通知内で、スキャンの完了について報告があった場合に送信されます。管理通知には、簡単なスキャンの統計情報も含まれています。																												
通知設定	必要ありません。																												
変数	<table border="1"><tr><td>MSG.Component</td><td>コンポーネント名</td></tr><tr><td>MSG.Cured</td><td>修復されたオブジェクトの数</td></tr><tr><td>MSG.DeletedObjs</td><td>削除されたオブジェクトの数</td></tr><tr><td>MSG.Errors</td><td>スキャンエラーの数</td></tr><tr><td>MSG.Infected</td><td>感染したオブジェクトの数</td></tr><tr><td>MSG.Locked</td><td>ブロックされたオブジェクトの数</td></tr><tr><td>MSG.Modifications</td><td>ウイルスの既知の亜種に感染したオブジェクトの数</td></tr><tr><td>MSG.Moved</td><td>隔離に移動したオブジェクトの数</td></tr><tr><td>MSG.Renamed</td><td>名前を変更されたオブジェクトの数</td></tr><tr><td>MSG.RunBy</td><td>コンポーネントを起動したユーザー</td></tr><tr><td>MSG.Scanned</td><td>スキャンしたオブジェクトの数</td></tr><tr><td>MSG.ServerTime</td><td>イベントを受け取った時間(グリニッジ標準時)</td></tr><tr><td>MSG.Speed</td><td>処理速度(KB/s)</td></tr><tr><td>MSG.Suspicious</td><td>疑わしいオブジェクトの数</td></tr></table>	MSG.Component	コンポーネント名	MSG.Cured	修復されたオブジェクトの数	MSG.DeletedObjs	削除されたオブジェクトの数	MSG.Errors	スキャンエラーの数	MSG.Infected	感染したオブジェクトの数	MSG.Locked	ブロックされたオブジェクトの数	MSG.Modifications	ウイルスの既知の亜種に感染したオブジェクトの数	MSG.Moved	隔離に移動したオブジェクトの数	MSG.Renamed	名前を変更されたオブジェクトの数	MSG.RunBy	コンポーネントを起動したユーザー	MSG.Scanned	スキャンしたオブジェクトの数	MSG.ServerTime	イベントを受け取った時間(グリニッジ標準時)	MSG.Speed	処理速度(KB/s)	MSG.Suspicious	疑わしいオブジェクトの数
MSG.Component	コンポーネント名																												
MSG.Cured	修復されたオブジェクトの数																												
MSG.DeletedObjs	削除されたオブジェクトの数																												
MSG.Errors	スキャンエラーの数																												
MSG.Infected	感染したオブジェクトの数																												
MSG.Locked	ブロックされたオブジェクトの数																												
MSG.Modifications	ウイルスの既知の亜種に感染したオブジェクトの数																												
MSG.Moved	隔離に移動したオブジェクトの数																												
MSG.Renamed	名前を変更されたオブジェクトの数																												
MSG.RunBy	コンポーネントを起動したユーザー																												
MSG.Scanned	スキャンしたオブジェクトの数																												
MSG.ServerTime	イベントを受け取った時間(グリニッジ標準時)																												
MSG.Speed	処理速度(KB/s)																												
MSG.Suspicious	疑わしいオブジェクトの数																												



パラメータ	値	
	MSG.VirusActivity	
	GEN.ServerRecvLinkID	接続された端末の予防的保護レポートを送信した最後の隣接ServerのUUID (このServerに接続されている端末についてのレポートが受信された場合は空の値)
	GEN.ServerRecvLinkName	接続された端末の予防的保護レポートを送信した最後の隣接Serverの名前 (このServerに接続されている端末についてのレポートが受信された場合は空の値)
	GEN.ServerOriginatorID	予防的保護レポートを送信し、端末が接続されているServerのUUID
	GEN.ServerOriginatorName	予防的保護レポートを送信し、端末が接続されているServerの名前

未知の端末

パラメータ	値	
通知の送信理由	新規端末がServerとの接続を要求しているが、登録の承認または拒否について確認することを許可されていない場合に送信されます。	
通知設定	必要ありません。	
変数	MSG.ID	未知の端末のUUID
	MSG.Rejected	値: <ul style="list-style-type: none">rejected - 端末へのアクセスは拒否されますnewbie - 端末に「新規端末 (newbie)」ステータスの割り当てを試みました
	MSG.StationName	端末名

接続が異常終了しました

パラメータ	値
通知の送信理由	クライアント(端末、Agentインストーラ、隣接Server、Proxy Server)との接続が異常終了した場合に送信されます。
通知設定	異常終了した接続に関する通知の送信を有効にするには、 管理 → Dr.Web



パラメータ	値	
	Serverの設定 → 統計 セクション内で 異常終了した接続 にチェックを入れ、同じセクション内で該当するパラメータを設定してください。	
変数	MSG.Total	終了した接続の数
	MSG.Type	クライアントの種類

端末はすでにログインしています

パラメータ	値	
通知の送信理由	Serverへの接続を試行した端末のIDが、すでにServerに接続されている端末のIDと同一であった場合に送信されます。	
通知設定	必要ありません。	
変数	MSG.ID	端末UUID
	MSG.Server	端末が登録されているServerのID
	MSG.StationName	端末名

端末は長い間Serverに接続されていません

パラメータ	値	
通知の送信理由	Serverスケジュール内のタスクに応じて送信されます。端末が長い間このServerに接続されていないという情報のほか、最後に接続された日付が記載されています。	
通知設定	端末が長期間接続されていないと見なされる期間は、 管理 → Dr.Web Server Task Schedule 内にあるServerスケジュールの 長期間Serverに接続していない端末 タスクで設定します。	
変数	<u>上</u> の端末の共通変数は使用できません。	
	MSG.DaysAgo	最後に訪問してから経過した日数
	MSG.LastSeenFrom	Serverに最後に訪問した端末のアドレス
	MSG.StationDescription	端末の説明
	MSG.StationID	端末UUID
	MSG.StationMAC	端末MACアドレス
	MSG.StationName	端末名
	MSG.StationSID	端末のセキュリティID



端末の再起動が必要です

パラメータ	値	
通知の送信理由	次のいずれかの理由により、端末の再起動が必要な場合に送信されます。 <ul style="list-style-type: none">• 修復を完了する• 更新を適用する• ハードウェアの仮想化のステータスを変更する• 修復を完了し、更新を適用する• 修復を完了し、ハードウェアの仮想化のステータスを変更する• 更新を適用し、ハードウェアの仮想化のステータスを変更する• 修復を完了し、更新を適用し、ハードウェアの仮想化のステータスを変更する	
通知設定	必要ありません。	
変数	MSG.Reason	再起動理由 起こりうる再起動の理由のリストについては既定のテンプレートを参照してください

端末は自動的に承認されました

パラメータ	値	
通知の送信理由	新規端末がServerとの接続を要求し、それがServerによって自動的に許可された場合に送信されます。	
通知設定	これは、 管理 → Dr.Web Server設定 → 全般 セクション内で 新規端末登録モード オプション に 自動でアクセスを承認する の値が設定されている場合に起こる可能性があります。	
変数	ありません。	

端末は管理者によって承認されました

パラメータ	値	
通知の送信理由	新規端末がServerとの接続を要求し、それが管理者によって手動で承認された場合に送信されます。	
通知設定	これは、 管理 → Dr.Web Server設定 → 全般 セクション内で 新規端末登録モード オプション に 手動でアクセスを承認する の値が設定されていて、管理者が該当する端末に対して アンチウイルスネットワーク → 未承認端末 → 選択された端末を承認し、プライマリグループを設定する オプションを指定していた場合に起こる可能性があります。	
変数	MSG.AdminAddress	Control Centerのネットワークアドレス



パラメータ	値	
	MSG.AdminName	管理者名

更新を適用するには端末の再起動が必要です

パラメータ	値	
通知の送信理由	端末から受け取った通知内で、製品がインストールまたは更新され、端末の再起動が必要である旨の報告があった場合に送信されます。	
通知設定	必要ありません。	
変数	MSG.Product	更新された製品
	MSG.ServerTime	Serverがメッセージを受信した時間(ローカル)



付録E. ネットワークアドレスの指定

指定の際の決まりは以下のとおりです。

- 変数(明確な値に置き換えられるフィールド)は山括弧で囲まれイタリック体で書かれます。
- パーマネントテキスト(置き換え後も残る)は太字で書かれます。
- オプションル元素は角括弧で囲まれます。
- 定義されているものは::=の左側に置きます。定義は右側に置きます(バックス・ナウア記法)。

E1. アドレスの一般フォーマット

ネットワークアドレスは以下のようになります。

[<protocol>: //] [<protocol-specific-part>]

デフォルトでは、<protocol>はTCP値を持ちます。<protocol-specific-part>のデフォルト値はアプリケーションによって決まります。



次の古くなったアドレス形式も許可されています。

[<protocol>/] [<protocol-specific-part>]。

IPアドレス

- <interface>: := <ip-address>
<ip-address>はピリオドで分けられたDNS名、またはIPアドレスのいずれかになります(例:127.0.0.1)。
- <socket-address>: := <interface>: <port-number>
<port-number>は10進数で指定します。

サーバーまたはAgentのアドレスを指定する場合、使用するプロトコルのバージョンを設定できます。以下が利用できます。

- <protocol>: // <interface>: <port-number> - IPv4およびIPv6を使用。
- <protocol>: // (<interface>) : <port-number> - IPv4のみを使用。
- <protocol>: // [<interface>] : <port-number> - IPv6のみを使用。

例:

1. tcp://127.0.0.1:2193

TCPプロトコル、インターフェース127.0.0.1上のポート2193を意味します。

2. tcp://(example.com):2193

TCPプロトコル、IPv4インターフェースexample.com上のポート2193を意味します。

3. tcp://[::]:2193

TCPプロトコル、IPv6インターフェース0000.0000.0000.0000.0000.0000.0000.0000上のポート2193を意味します。

4. localhost:2193



同上。

5. tcp://:9999

サーバーの値: アプリケーションに依存したデフォルトのインターフェース(通常、使用可能なインターフェース全て)、ポート9999、クライアントの値: アプリケーションに依存したホストへのデフォルト接続(通常はlocalhost)、ポート 9999。

6. tcp://

TCPプロトコル、デフォルトポート。

接続指向プロトコル

`<protocol>/ <socket-address>`

`<socket-address>`でサーバーのソケット、またはクライアントのリモートサーバーのローカルアドレスを設定します。

データグラム指向プロトコル

`<protocol>:// <endpoint-socket-address>[- <interface>]`

例:

1. udp://231.0.0.1:2193

デフォルトでアプリケーションに依存しているインターフェース上で、マルチキャストグループ231.0.0.1:2193を使用することを意味します。

2. udp://[ff18::231.0.0.1]:2193

デフォルトでアプリケーションに依存しているインターフェース上で、マルチキャストグループ[ff18::231.0.0.1]を使用することを意味します。

3. udp://

アプリケーション依存のインターフェースおよびエンドポイントです。

4. udp://255.255.255.255:9999-myhost1

myhost1インターフェース上のポート9999のプロードキャストメッセージを使用します。

UDSアドレス

- 接続指向プロトコル:

`unx:// <file_name>`

- データグラム指向プロトコル:

`udx:// <file_name>`

例:

1. unx://tmp/drwcd:stream

2. unx://tmp/drwcd:datagram

SRVアドレス

`srv:// [<server name>] [@ <domain name/dot address>]`



E2.Dr.Web Agent/Installerのアドレス

Dr.Web Serverへの直接接続

[<connection-protocol>]://[<remote-socket-address>]

デフォルトでは<connection-protocol>に依存します。

- tcp://127.0.0.1:2193
ループバックポート2193を意味します。
- tcp://[::]:2193
IPv6のループバックポート2193を意味します。

<drwcs-name>プロトコルのファミリーとエンドポイントを使用したDr.Web Server口 ケーション

[<drwcs-name>]@<datagram-protocol>://[<endpoint-socket-address>[-<interface>]]

デフォルトでは<datagram-protocol>に依存します。

- drwcs@udp://231.0.0.1:2193-0.0.0.0
全てのインターフェースにマルチキャストグループ231.0.0.1:2193を使用するTCP接続に対するdrwcs名を持ったServerの口ケーション。

付録F. リポジトリの管理



リポジトリの管理はControl Centerの該当する設定から行うことが推奨されます。詳細については、管理者マニュアルの [Dr.Web Serverリポジトリの管理](#) を参照してください。

リポジトリ設定は以下のリポジトリ設定ファイルに保存されます。

- **全般設定ファイル**はリポジトリのルートフォルダ内にあり、更新サーバーのパラメータを指定します。
- **製品設定ファイル**は該当するリポジトリ製品のルートフォルダ内にあり、その製品のファイルセットと更新設定を指定します。



設定ファイルを編集した後はサーバーを再起動させてください。



製品ミラーリングのためにインターサーバーリンクをセットアップする際は(管理者マニュアルの [複数の Dr.Web Serverを持つネットワークの特性](#) 参照)、設定ファイルは製品の一部ではないため、ミラーシステムでは正常に操作できないという点にご注意ください。更新中のエラーを防ぐための注意事項は以下のとおりです。

- ピアサーバーには同じ設定を使用します。
- 下位サーバーではHTTPプロトコル経由でのコンポーネントの同期を無効にするか、設定を同一のままにしてください。

F1. 全般設定ファイル

.servers

.serversファイルには、Dr.Web Serverリポジトリ内でGUS サーバーからDr.Web Enterprise Security Suiteコンポーネントを更新するサーバーのリストが含まれています。

その結果、リストにあるServerはポーリングされ、更新が成功するとポーリングは中断されます。

例:

```
esuite.geo.drweb.com
esuite.msk3.drweb.com
esuite.msk4.drweb.com
esuite.msk.drweb.com
esuite.us.drweb.com
esuite.jp.drweb.com
```



.url

.urlファイルには、更新ゾーン - 特定のDr.Web 製品の更新が含まれている、更新サーバー上のフォルダ - のベースURIが含まれています。

例:

```
update
```

.proto

.protoファイルには、更新サーバーから更新を受け取る際に使用されるプロトコル名が含まれています。

次の値を使用できます: http | https | ftp | ftps | sftp | scp | smb | smbs | file



smbおよびsmbsプロトコルはUNIX系OSのサーバーでのみ使用できます。

例:

```
https
```

.auth

.authファイルには、更新サーバー上でのユーザー認証のパラメータが含まれています。

次のフォーマットで指定します。

```
<user name>
```

```
<password>
```

ユーザー名は必須ですが、パスワードは任意です。

例:

```
admin
```

```
root
```

.delivery

.deliveryファイルには、GUSサーバーから更新を配信する際の設定が含まれています。



パラメータ	可能な値	説明
cdn	on off	リポジトリのロード中にContent Delivery Network を使用: <ul style="list-style-type: none">• on – CDNを使用• off – CDNを使用しない
cert	drweb valid any custom	自動的に承認される、更新サーバーのSSL証明書を許可: <ul style="list-style-type: none">• drweb – Doctor WebのSSL証明書のみを許可• valid – 有効な証明書のみを許可• any – あらゆる証明書を許可• custom – ユーザーによって指定された証明書を許可
cert-path		cert パラメータに custom モードが設定された場合の、ユーザー定義へのパスです。
ssh-mode	pwd pubkey	scpおよびsftpプロトコル(ssh2に基づく)を使用する場合の認証モード: <ul style="list-style-type: none">• pwd – ユーザーログインおよびパスワードによる認証• pubkey – 暗号化キーによる認証
ssh-pubkey		更新サーバーのパブリックsshキーへのパス
ssh-prikey		更新サーバーのプライベートsshキーへのパス

F2. 製品設定ファイル

.description

.descriptionファイルは製品名を設定します。ファイルが存在しない場合、製品の各フォルダの名前が製品名として使用されます。

例:

```
Dr.Web Server
```

.sync-off

このファイルは製品更新を無効にします。コンテンツは関係ありません。



GUSからのサーバーリポジトリ更新時における除外を設定するファイル

.sync-only

.sync-onlyファイルには、GUSからのリポジトリ更新中に同期されるリポジトリファイルのリストを定義する正規表現が含まれています。.sync-only内で指定されなかったリポジトリファイルは同期されません。.sync-onlyファイルが存在しない場合、.sync-ignoreファイル内の設定によって除外されているものを除く、全てのリポジトリファイルが同期されます。

.sync-ignore

.sync-ignoreファイルには、GUSからのリポジトリ更新中に同期しないリポジトリファイルのリストを定義する正規表現が含まれています。

除外されるファイルの例:

```
^windows-nt-x64/  
  
^windows-nt/  
  
^windows/
```

設定ファイルを適用する順番

製品が.sync-onlyファイルと.sync-ignoreファイルを持っている場合、以下のルールが使用されます。

1. まず初めに.sync-onlyが適用されます。.sync-onlyファイル内にはないファイルは処理されません。
2. 残りのファイルに対して.sync-ignoreが適用されます。

サーバーからのAgent更新時における除外を設定するファイル

.state-only

.state-onlyファイルには、サーバーからのAgent更新中に同期されるリポジトリファイルのリストを定義する正規表現が含まれています。state-only内で指定されなかったリポジトリファイルは同期されません。state-onlyファイルが存在しない場合、.state-ignoreファイル内の設定によって除外されているものを除く、全てのリポジトリファイルが同期されます。

.state-ignore

.state-ignoreファイルには、サーバーからのAgent更新中に同期しないリポジトリファイルのリストを定義する正規表現が含まれています。

例:

- ドイツ語、中国語、スペイン語のインターフェース言語は受け取りません(その他の言語は受け取ります)。



- 64ビット版Windows用のコンポーネントは受け取りません。

```
;^common/ru-.*\.dwl$ this will be updated  
  
^common/de-.*\.dwl$  
  
^common/cn-.*\.dwl$  
  
^common/es-.*\.dwl$  
  
^win/de-.*  
  
^win/cn-.*  
  
^windows-nt-x64\.*
```

.state-onlyファイルと.state-ignoreファイルが適用される順番は.sync-onlyファイルと.sync-ignoreファイルの場合と同じです。

通知の送信設定

notifyグループのファイルによって、個別の製品の更新完了についての通知システムを設定できます。



これらの設定は 製品が更新されました 通知でのみ使用できます。その他の通知については、除外は適用されません。

通知システムに関する基本的な情報については、管理者マニュアルページの[通知設定](#)を参照してください。

.notify-only

.notify-onlyファイルには、変更されると通知が送信されるリポジトリファイルのリストが含まれています。

.notify-ignore

.notify-ignoreファイルには、変更されても通知を送信しないリポジトリファイルのリストが含まれています。

設定ファイルを適用する順番

製品が.notify-onlyファイルと.notify-ignoreファイルを持っている場合、以下のルールが使用されます。

1. 製品更新時に、GUS から更新されるファイルが除外リスト内にあるファイルと比較されます。
2. .notify-ignoreリストに含まれているファイルが最初に除外されます。
3. 残りのファイルについては、.notify-onlyリストに含まれていないファイルが除外されます。
4. これまでのステップで除外されなかったファイルが残っていた場合、通知が送信されます。



.notify-onlyファイルと.notify-ignoreファイルが存在しない場合、常に通知が送信されます(Control Centerの通知設定ページで有効になっていた場合)。

例:

.notify-ignoreファイル内で^.vdb.lzma\$の除外が設定されていて、ウイルスデータベースのみが更新された場合、通知は送信されません。データベースと一緒にdrweb32.dllエンジンも更新された場合は通知が送信されます。

凍結設定

.delay-config

.delay-configファイルには、製品を新しいリビジョンに切り替えることを無効にする設定が含まれています。リポジトリは古いバージョンを配信し続け、同期は行われなくなります(製品の状態が「凍結」されます)。このリビジョンを配信してもいいと管理者が判断した場合、Control Center 内で配信を有効にします(管理者マニュアルの[Dr.Web Serverリポジトリの管理](#)参照)。

ファイルには、セミコロンで区切られた大文字小文字を区別しない2つのパラメータが含まれています。

ファイルフォーマット:

```
Delay [ON|OFF]; UseFilter [YES|NO]
```

パラメータ	可能な値	説明
Delay	ON OFF	<ul style="list-style-type: none">ON - 製品更新の凍結が有効です。OFF - 製品更新の凍結が無効です。
UseFilter	YES NO	<ul style="list-style-type: none">Yes - .delay-onlyファイル内の除外リストに含まれるファイルに対する更新のみを凍結します。No - 全ての更新を凍結します。

例:

```
Delay ON; UseFilter NO
```

.delay-only

.delay-onlyファイルには、それを変更することで製品の新しいリビジョンへの切り替えを無効にする、ファイルのリストが含まれています。ファイルのリストは正規表現のフォーマットで書かれています。

リポジトリ更新のファイルが指定されたマスクに合致し、.sync-onlyファイル内の UseFilter 設定が有効になっていた場合、リビジョンは凍結されます。

.rev-to-keep

.rev-to-keepファイルには、保存される製品リビジョンの数が含まれています。



例:

3



付録G. 設定ファイルフォーマット

このセクションでは以下のファイルのフォーマットについて説明します。

ファイル	説明
drwcsd.conf	Dr.Web Server設定ファイル
webmin.conf	Dr.Web Security Control Center設定ファイル
download.conf	データのダウンロードに関する設定ファイル
drwcsd-proxy.conf	Dr.Web Proxy Server設定ファイル
drwreloader.conf	Repository Loader設定ファイル



該当するコンポーネントのあるコンピューターに、セルフプロテクションが有効になった Agent がインストールされている場合、設定ファイルを編集する前に Agent 設定経由で Dr.Web Self-protection コンポーネントを無効にします。

変更を全て保存した後は、Dr.Web Self-protection コンポーネントを有効にしておくことを推奨します。

G1. Dr.Web Server設定ファイル

`drwcsd.conf`サーバー設定ファイルは、デフォルトではサーバーインストール フォルダの `etc` サブフォルダ内にあります。サーバーがコマンドラインパラメータで動作している場合、設定ファイルの標準以外のロケーション、および名前を設定できます(詳細は付録H3. [Dr.Web Server](#)を参照してください)。

Dr.Web Server設定ファイルを手動で管理するには次を行います。

1. サーバーを停止します(管理者マニュアルの [Dr.Web Serverの起動と停止](#)参照)。
2. Self-Protectionを無効にします(Self-ProtectionがアクティブなAgentをインストールした場合 - Agentのコンテキストメニュー内)。
3. サーバー設定ファイルを編集します。
4. サーバーを起動します(管理者マニュアルの [Dr.Web Serverの起動と停止](#)参照)。

Dr.Web Server設定ファイルフォーマット

サーバー設定ファイルはXMLフォーマットです。

Dr.Web Server設定ファイルパラメータ:

- `<version value=''>`
設定ファイルの現在のバージョンです。
- `<name value=''/>`



Dr.Web ServerまたはDr.Web Serverのクラスタの名前。これは、Agent、Agentインストーラ、Control Centerによって検索される場合に使用されます。Dr.Web Serverソフトウェアがインストールされているコンピューター名を使用するには、値を空白のままにします(デフォルトでは""が使用されます)。

- `<id value="" />`

サーバーの一意的識別子です。これまでのバージョンではサーバーライセンスキー内に置かれていましたが、バージョン10以降ではサーバー設定ファイル内に保存されています。

- `<location city="" country="" department="" floor="" latitude="" longitude="" organization="" province="" room="" street="" />`

サーバーの地理的位置です。

属性の説明:

属性	説明
city	都市名
country	国
department	部署名
floor	所在階
latitude	緯度
longitude	経度
organization	組織名
province	県名
room	部屋番号
street	番地

- `<threads count='' />`

Agentからのデータを処理するスレッドの数です。最小値は5で、デフォルトでは5になっています。このパラメータはサーバーのパフォーマンスに影響します。テクニカルサポートからの指示がない限り、変更しないことを推奨します。

- `<newbie approve-to-group='' default-rate='' mode='' />`

新規端末のアクセスモードです。

属性の説明:

属性	可能な値	説明	デフォルト
approve-to-group	-	アクセスを自動的に許可するモード (<code>mode='open'</code>) で、新しい端末に対してデフォルトでプライマリに設定されているグループです。	値が空の場合、 Everyone グループがプライマリとして割り当てられます。
default-rate	-	AV-Desk向けアクセスを自動的に許可するモード (<code>mode='open'</code>) で、新	値が空の場合、 Dr.Web Premium グループが課金



属性	可能な値	説明	デフォルト
		しい端末に対してデフォルトで課金プランに設定されているグループです。	プランとして割り当てられません。
mode	<ul style="list-style-type: none"> open - アクセスを自動的に許可する closed - 常にアクセスを拒否する approval - 手動でアクセスを承認する 	新しい端末の承認ポリシーです。	-

詳細については、管理者マニュアルの [新しい端末の承認ポリシー](#) を参照してください。

- `<emplace-auto enabled="" />`

すでにインストールされているアカウントが足りない場合に、グループインストールパッケージを使用してAgentをインストールする際にControl Center内で端末アカウントを作成するモードです。

属性	可能な値	デフォルト
enabled	<ul style="list-style-type: none"> yes - 足りない端末アカウントを自動的に作成します。 no - インストールは、グループ内にすでに作成されている未使用のアカウントの数量内で可能で、その端末用のインストールパッケージが起動されます。 	yes

- `<unauthorized-to-newbie enabled="" />`

未承認端末に対するアクションのポリシーです。enabledに使用できる値は以下のとおりです。

- yes - 承認に失敗した端末(データベースの破損時など)は自動的に新規端末にリセットされます。
- no(デフォルト)- 通常の動作モードです。

- `<maximum-authorization-queue size="" />`

サーバー上での承認待ちキュー内の端末数上限です。デフォルト設定の変更は、テクニカルサポートによる指示があった場合のみ行うようにしてください。

- `<reverse-resolve enabled="" />`

IPアドレスをDr.Web Serverログファイル内の DNS 名で置き換えます。enabledに使用できる値は以下のとおりです。

- yes - DNS名を表示します。
- no(デフォルト)- IPアドレスを表示します。

- `<replace-netbios-names enabled="" />`

コンピューターのNetBIOS名をDNS名で置き換えます。enabledに使用できる値は以下のとおりです。

- yes - DNS名を表示します。
- no(デフォルト)- NetBIOS名を表示します。

- `<dns>`

DNS設定です。

`<timeout value="" />`

DNS正引き・逆引きのタイムアウト(秒)です。解決するまでの待ち時間に制限を設けない場合は値を0に設定します。



```
<retry value="" />
```

DNSクエリの解決に失敗した場合に、クエリを繰り返す回数の上限です。

```
<cache enabled="" negative-ttl="" positive-ttl="" />
```

DNSサーバーの応答をキャッシュに保存する時間(TTL)を設定します。

属性の説明:

属性	可能な値	説明
enabled	<ul style="list-style-type: none">• yes - 応答をキャッシュに保存します。• no - 応答をキャッシュに保存しません。	応答をキャッシュに保存するモードです。
negative-ttl	-	DNSサーバーからのネガティブな応答をキャッシュに保存(TTL)する時間(分)です。
positive-ttl	-	DNSサーバーからのポジティブな応答をキャッシュに保存(TTL)する時間(分)です。

```
<servers>
```

デフォルトのシステムリストに置き換わるDNSサーバーリストです。1つ以上の`<server address="" />`子エレメントを持ち、そのaddressパラメータがサーバーのIPアドレスを定義します。

```
<domains>
```

デフォルトのシステムリストに置き換わるDNSドメインリストです。1つ以上の`<domain name="" />`子エレメントを持ち、そのnameパラメータがドメイン名を定義します。

- `<cache>`

キャッシュの設定です。

`<cache>`エレメントには以下の子エレメントが含まれます。

- `<interval value="" />`

全てのキャッシュをフラッシュする間隔(秒)です。

- `<quarantine ttl="" />`

サーバー隔離ファイルをクリーンアップする間隔(秒)です。デフォルトでは604800(1週間)になっています。

- `<download ttl="" />`

個人のインストールパッケージをクリーンアップする間隔(秒)です。デフォルトでは604800(1週間)になっています。

- `<repository ttl="" />`

サーバーリポジトリ内のファイルをクリーンアップする間隔(秒)です。

- `<file ttl="" />`

ファイルキャッシュをクリーンアップする間隔(秒)です。デフォルトでは604800(1週間)になっています。

- `<replace-station-description enabled="" />`

Dr.Web Server上の端末の説明と、端末上のシステムプロパティページの `コンピューターの説明` フィールドを同期させます。enabledに使用できる値は以下のとおりです。

- yes - サーバー上の説明を端末上の説明と置き換えます。

- no(デフォルト) - 端末上の説明を無視します。



- `<time-discrepancy value="" />`

Dr.Web ServerとDr.Web Agent間のシステム時間の許容する差異(分単位)を指定します。指定値よりも差が大きい場合はDr.Web Serverの端末ステータスにその旨が表示されます。デフォルトでは3分に指定されています。値が空の場合、または0が指定されている場合、システム時間の違いはチェックされません。

- `<encryption mode="" />`

トラフィックの暗号化モードです。modeに使用できる値は以下のとおりです。

- yes - 暗号化を使用します。
- no - 暗号化を使用しません。
- possible - 暗号化が可能です。

デフォルトはyesです。

詳細については、管理者マニュアルの [トラフィックの暗号化と圧縮](#)を参照してください。

- `<compression level="" mode="" />`

トラフィック圧縮モードです。

属性の説明:

属性	可能な値	説明
level	1~9の整数です。	圧縮レベルです。
mode	<ul style="list-style-type: none">• yes - 圧縮を使用します。• no - 圧縮を使用しません。• possible - 圧縮が可能です。	圧縮モードです。

詳細については、管理者マニュアルの [トラフィックの暗号化と圧縮](#)を参照してください。

- `<track-agent-jobs enabled="" />`

ワークステーション上で実行されたタスクの結果をモニタリングし、サーバーデータベース内に保存します。enabledの値にはyesまたはnoを使用できます。

- `<track-agent-status enabled="" />`

端末の状態における変更をモニタリングし、情報をサーバーデータベース内に保存します。enabledの値にはyesまたはnoを使用できます。

- `<track-virus-bases enabled="" />`

端末上のウイルスデータベースの状態の変更(構成、変更)をモニタリングし、情報をサーバーデータベース内に保存します。enabledの値にはyesまたはnoを使用できます。`<track-agent-status enabled="no" />`の場合、このパラメータは無視されます。

- `<track-agent-modules enabled="" />`

端末上のモジュールのバージョンをモニタリングし、情報をサーバーデータベース内に保存します。enabledの値にはyesまたはnoを使用できます。

- `<track-agent-components enabled="" />`

端末上のインストールされたコンポーネントリストをモニタリングし、情報をサーバーデータベース内に保存します。enabledの値にはyesまたはnoを使用できます。

- `<track-agent-userlogon enabled="" />`

端末上のユーザーセッションをモニタリングし、情報をサーバーデータベース内に保存します。enabledの値にはyesまたはnoを使用できます。



- `<track-agent-environment enabled="" />`
端末上のハードウェアとソフトウェアの構成をモニタリングし、情報をサーバーデータベース内に保存します。
enabledの値にはyesまたはnoを使用できます。
- `<keep-run-information enabled="" />`
端末上で動作するアンチウイルスコンポーネントの開始と停止に関する情報をモニタリングし、それらの情報をサーバーデータベース内に保存します。enabledの値にはyesまたはnoを使用できます。
- `<keep-infection enabled="" />`
端末上の脅威検出をモニタリングし、情報をサーバーデータベース内に保存します。enabledの値にはyesまたはnoを使用できます。
- `<keep-scan-errors enabled="" />`
端末上のスキャンエラーをモニタリングし、情報をサーバーデータベース内に保存します。enabledの値にはyesまたはnoを使用できます。
- `<keep-scan-statistics enabled="" />`
端末上のスキャン統計をモニタリングし、情報をサーバーデータベース内に保存します。enabledの値にはyesまたはnoを使用できます。
- `<keep-installation enabled="" />`
端末上でのAgentのインストールに関する情報をモニタリングし、それらの情報をサーバーデータベース内に保存します。enabledの値にはyesまたはnoを使用できます。
- `<keep-blocked-devices enabled="" />`
Office Control コンポーネントによってブロックされたデバイスに関する情報をモニタリングし、その情報をServerデータベースに保存します。enabledの値にはyesまたはnoを使用できます。
- `<keep-appcontrol-activity enabled="" />`
Application Controlによって検出された端末でのプロセスアクティビティをモニタリングし (Applicationsカタログにファイリングするため)、その情報をServerデータベースに保存します。enabledの値にはyesまたはnoを使用できます。
- `<keep-appcontrol-block enabled="" />`
Application Controlによる端末でのプロセスのブロックをモニタリングし、その情報をServerデータベースに保存します。enabledの値にはyesまたはnoを使用できます。
- `<quarantine enabled="" />`
端末上での隔離の状態に関する情報をモニタリングし、それらの情報をサーバーデータベース内に保存します。enabledの値にはyesまたはnoを使用できます。
- `<update-bandwidth queue-size="" value="" />`
サーバーからAgentに対して更新を配信する際の、ネットワークトラフィック帯域幅の上限 (KB/秒) です。

属性の説明:

属性	可能な値	説明	デフォルト
queue-size	<ul style="list-style-type: none">• 正の整数• 無制限	同時に実行することのできるサーバーからの更新配信セッションの上限です。上限に達した場合、Agentのリクエストは実行待ちのキューに置かれます。キューのサイズに上限はありません。	無制限
value	<ul style="list-style-type: none">• 上限 (KB/秒)• 無制限	更新配信の最大速度です。	無制限



- `<install-bandwidth queue-size="" value="" />`

端末上でのDr.Web Agentインストール中にデータをやり取りする際のネットワークトラフィック帯域幅の上限です (KB/秒)。

属性の説明:

属性	可能な値	説明	デフォルト
queue-size	<ul style="list-style-type: none"> • 正の整数 • 無制限 	キューのサイズに上限はありません。サーバーから同時に実行することのできるAgentインストールセッション数の上限です。上限に達した場合、Agentのリクエストは実行待ちのキューに置かれます。	無制限
value	<ul style="list-style-type: none"> • 上限 (KB/秒) • 無制限 	Agentインストール中のデータ配信の最大速度です。	無制限

- `<geolocation enabled="" startup-sync="" />`

Dr.Web Server間の位置情報の同期を有効にします。

属性の説明:

属性	可能な値	説明
enabled	<ul style="list-style-type: none"> • yes - 同期を許可します。 • no - 同期を無効にします。 	同期モード
startup-sync	正の整数	Dr.Web Server間の接続を確立する際にリクエストされた情報と位置情報のない端末の数です。

- `<audit enabled="" />`

Dr.Web Security Control Center での管理者による操作をモニタリングし、情報をサーバーデータベース内に保存します。enabledの値にはyesまたはnoを使用できます。

- `<audit-internals enabled="" />`

Dr.Web Serverの内部動作をモニタリングし、情報をサーバーデータベース内に保存します。enabledの値にはyesまたはnoを使用できます。

- `<audit-xml-api enabled="" />`

Web API経由でのDr.Web Serverの動作をモニタリングし、情報をサーバーデータベース内に保存します。enabledの値にはyesまたはnoを使用できます。

- `<proxy auth-list="" enabled="" host="" password="" user="" />`

HTTPプロキシサーバー経由でのDr.Web Serverとの接続パラメータです。

属性の説明:

属性	可能な値	説明
auth-list	<ul style="list-style-type: none"> • none - 認証を使用しません • any - サポートされているあらゆる方式 • safe - サポートされているあらゆる安全な方式 	プロキシサーバー認証の種類です。デフォルトは「any」です。



属性	可能な値	説明
	<ul style="list-style-type: none"> 以下の方式については、複数ある場合、スペースで区切って必要な全ての方式を設定します。 <ul style="list-style-type: none"> basic digest digestie ntlmwb ntlm negotiate 	
enabled	<ul style="list-style-type: none"> yes - プロキシサーバーを使用します。 no - プロキシサーバーを使用しません。 	HTTPプロキシサーバー経由でのDr.Web Serverとの接続モードです。
host	-	プロキシサーバーアドレスです。
password	-	プロキシサーバーが認証を必要とする場合のプロキシサーバーのユーザーパスワードです。
user	-	プロキシサーバーが認証を必要とする場合のプロキシサーバーのユーザー名です。



プロキシサーバーの許可する認証方式のリストを設定する場合、only マーク(リストの最後にスペースを空けて追加します)を使用して認証方式選択のアルゴリズムを変更できます。

詳細については、https://curl.se/libcurl/c/CURLOPT_HTTPAUTH.html を参照してください。

- `<statistics enabled="" id="" interval="" />`

ウイルスイベントに関する統計をDoctor Webの<https://stat.drweb.com/>に送信するパラメータです。

属性の説明:

属性	可能な値	説明	デフォルト
enabled	<ul style="list-style-type: none"> yes - 統計を送信します。 no - 統計を送信しません。 	Doctor Webへの統計送信モードです。	-
ID	-	AgentライセンスキーのMD5です。	-
interval	正の整数	統計を送信する間隔(分)です。	30

- `<cluster>`

マルチサーバーアンチウイルスネットワーク設定内でデータをやり取りする際のDr.Web Serverクラスタのパラメータです。

1つまたは複数の`<on multicast-group="" port="" interface="" />` 子エレメントが含まれます。

属性の説明:



属性	説明
multicast-group	サーバー間でデータのやり取りを行う際に経由するマルチキャストグループのIPアドレスです。
port	マルチキャストグループ内へデータを配信する際にトランスポートプロトコルが使用するネットワークインターフェースのポート番号です。
インターフェース	マルチキャストグループ内に情報を送信するための、転送プロトコルが設定されているネットワークインターフェースのIPアドレスです。

- `<multicast-updates enabled="" />`

マルチキャストプロトコルを介したワークステーションへのアップデート送信の設定を許可します。enabledの値にはyesまたはnoを使用できます。

`<multicast-updates>`には、複数の子エレメントと属性が含まれます。

子エレメント	属性	説明	デフォルト
port <code><port value="" /></code>	value	トランスポートマルチキャストプロトコルが更新を送信するために使用するDr.Web Serverのネットワークインターフェースポート番号。このポートは、全てのマルチキャストグループが使用します。 マルチキャスト更新の場合、サーバーのトランスポートプロトコル設定で指定されているポートとは異なる未使用のポートを指定する必要があります。	2197
tTl <code><tTl value="" /></code>	value	転送されたUDPデータグラムの存続可能時間。この値は、全てのマルチキャストグループが使用します。	8
グループ <code><group address="" /></code>	アドレス	端末がマルチキャスト更新を受信するマルチキャストグループのIPアドレス。	233.192.86.0 (IPv4の場合) FF0E::176 (IPv6の場合)
on <code><on interface="" ttl="" /></code>	インターフェース	更新を送信する際にマルチキャストトランスポートプロトコルによって使用される、Dr.Web ServerネットワークインターフェースのIPアドレスです。	—
	tTl	指定されたネットワークインターフェースを介して転送されるUDPデータグラムの存続可能時間。一般的な <code><tTl value="" /></code> 子エレメントよりも優先されます。	8
転送 <code><transfer datagram-size="" assembly-timeout="" updates-interval="" /></code>	datagram-size	UDPデータグラムサイズ(バイト) - UDPデータグラムサイズをバイト単位で指定します。 許容範囲は512~8192です。断片化を避けるために、ネットワークのMTU(最大転送単位)より小さい値を設定することを推奨します。	1400



子エレメント	属性	説明	デフォルト
<pre>chunks- interval="" resend- interval="" silence- interval="" accumulate- interval="" announce-send- times="" /></pre>	assembly- timeout	ファイル送信時間(分) - 1つの更新ファイルを送信する時間を指定します。指定された時間が経過した後、サーバーは次のファイルの配信を開始します。 マルチキャストプロトコル更新の一部として送信に失敗した全てのファイルは、TCPプロトコルを介した標準更新プロセスの一部として送信されます。	180000
	updates- interval	マルチキャスト更新間隔(分) - マルチキャストプロトコル経由での更新間隔です。 マルチキャストプロトコルを介した更新の段階で送信に失敗した全てのファイルは、TCPプロトコルを介した標準の更新の一部として送信されます。	600000
	chunks- interval	パッケージ送信間隔(ミリ秒) - マルチキャストグループへのパッケージ送信間隔です。 間隔の値が小さいと、パッケージの転送中に重大な損失が発生し、ネットワークが過負荷になる可能性があります。このパラメータの変更は推奨されません。	14
	resend- interval	再送信要求の間隔(ミリ秒) - この間隔で、消失したパッケージの再送信要求をAgentが送信する間隔です。 Dr.Web Serverはこれらのリクエストを蓄積し、その後、全ての消失したブロックを送信します。	1000
	silence- interval	送信“待ち”間隔(ミリ秒) - 許容時間内にファイルの送信が終了し、かつ指定された“待ち”時間内に消失したパッケージの再送信要求をAgentから受信しなかった場合、Dr.Web Serverは全てのAgentが更新ファイルを受信したと判断し、次のファイルの送信を開始します。	10000
	accumulate- interval	再送リクエスト蓄積期間(分) - 指定された期間、サーバーは、Agentから受信した消失パッケージの再送信要求を蓄積します。 Agentは消失パッケージを要求します。サーバーは、指定された時間にわたってこれらの要求を蓄積し、その後、全ての消失したブロックを送信します。	2000
	announce- send-times	ファイル送信アナウンスの数 - 更新送信が開始する前に、サーバーがマルチキャストグループへのファイル送信をアナウンスする回数。 アナウンスとは、マルチキャストグループに送信されるファイルメタデータを含むUDPデータグラムを意味します。アナウンスの数を増やすと、送信の信頼性が向	3



子エレメント	属性	説明	デフォルト
		上する可能性があります。同時に、許容時間内にマルチキャストプロトコルを介して送信できるデータ量が減少する可能性があります。	

オプションで、`<multicast-updates>`には、ACLリストの作成に使用される`<acl>`子エレメントを含めることもできます。これにより、現在のサーバーからマルチキャストプロトコルを介してマルチキャスト更新を受信することを許可されているワークステーションのTCPアドレスの範囲を制限できます。`<acl>`は当初は存在しません。つまり、デフォルトでは制限は適用されません。

`<acl>`には次の子エレメントが含まれます。

- `<priority mode="" />`

リストの優先度を設定します。modeに使用できる値は、allowまたはdenyです。`<priority mode="deny"/>`値では、`<deny>`リストが`<allow>`リストよりも優先度が高くなります。いずれのリストにも含まれていないアドレス、または両方のリストに含まれているアドレスは拒否されます。許可されるのは、`<allow>`リストに含まれ、`<deny>`リストには含まれていないアドレスのみです。

- `<allow>`

マルチキャストプロトコルを介した更新の受信が許可されたTCPアドレスのリスト。`<allow>`エレメントには1つまたは複数の、IPv4フォーマットで許可されたアドレスを指定する`<ip address="" />`子エレメント、および、IPv6フォーマットで許可されたアドレスを指定する`<ip6 address="" />`が含まれます。address属性は、ネットワークアドレスを`<IP address>/ [<prefix>]`のフォーマットで定義します。

- `<deny>`

マルチキャストプロトコルを介した更新の受信を許可されていないTCPアドレスのリスト。`<deny>`エレメントには1つまたは複数の、IPv4フォーマットで拒否されたアドレスを指定する`<ip address="" />`子エレメント、および、IPv6フォーマットで拒否されたアドレスを指定する`<ip6 address="" />`が含まれます。address属性は、ネットワークアドレスを`<IP address>/ [<prefix>]`のフォーマットで定義します。

- `<database connections="" />`

データベースの定義です。

属性の説明:

属性	可能な値	説明	デフォルト
接続	正の整数	データベースのサーバー接続数を入力します。デフォルト値を変更する場合は、テクニカルサポートに相談した後に変更することを推奨します。	2
speedup	yes no	データベースの初期化、アップグレード、インポート後に、遅らせていたデータベースのページを自動的に実行します(管理者マニュアルの データベース 参照)。	yes

`<database />`エレメントには以下の子エレメントが含まれます。



`<database />`には特定のデータベースを定義する1つの子エレメントのみを含めることができます。

設定ファイルテンプレート内にあるデータベース属性のうち、ここに記載されていないものはDoctor Web テクニカルサポートサービスからの承諾なしに変更しないようお勧めします。



- ```
<sqlite dbfile="" cache="" cachesize="" readuncommitted="" precompiledcache="" synchronous="" openmutex="" checkintegrity="" autorepair="" mmapsize="" wal="" wal-max-pages="" wal-max-seconds="" />
```

SQLite(組み込みデータベース)を定義します。

属性の説明:

属性	可能な値	説明	デフォルト
dbfile		データベース名	database.sqlite
cache	SHARED   PRIVATE	キャッシングモードです。	SHARED
cachesize	正の整数	データベースキャッシュサイズです(1.5Kb ページ)	2048
precompiledcache	正の整数	プリコンパイルされたSQL演算子のキャッシュサイズです(キロバイト)。	1024
synchronous	<ul style="list-style-type: none"> <li>• TRUEまたはFULL - 同期</li> <li>• FALSEまたはNORMAL - 通常</li> <li>• OFF - 非同期</li> </ul>	データ書き込みモードです。	FULL
checkintegrity	quick   full   no	Dr.Web Server起動時にデータベースイメージの整合性を検証します。	quick
autorepair	yes   no	Dr.Web Server起動時に、破損したデータベースイメージを自動で修復します。	no
mmapsize	正の整数	プロセスのアドレス空間に一度にマップすることのできるデータベースファイルの最大サイズ(バイト)です。	<ul style="list-style-type: none"> <li>• UNIX系OS - 10485760</li> <li>• Windows - 0</li> </ul>
wal	yes   no	ログ先行書き込みを使用します。	yes
wal-max-pages		そこへのアクセスをディスク上に書き込む「ダーティな」ページ数の上限です。	1000
wal-max-seconds		ディスク上へのページの書き込みを遅らせることのできる時間の上限です(秒)。	30

- ```
<pgsql dbname="drwcs" host="localhost" port="5432" options="" requiressl="" user="" password="" temp_tablespaces="" default_transaction_isolation="" debugproto="yes" />
```

PostgreSQL外部データベースを定義します。

属性の説明:

属性	可能な値	説明	デフォルト
dbname		データベース名です。	



属性	可能な値	説明	デフォルト
host		PostgreSQLサーバーのホストまたはUnixドメインソケットへのパスです。	
port		PostgreSQLサーバーポートまたはUnixドメインソケットファイルの拡張子です。	
options		データベースサーバーに送信するコマンドラインパラメータです。 詳細については、 https://www.postgresql.org/docs/9.1/libpq-connect.html の第18章を確認してください。	
requiressl	<ul style="list-style-type: none"> • 1 0 (Control Center経由) • y n • yes no • on off 	SSL接続のみ許可します。	<ul style="list-style-type: none"> • 0 • y • yes • on
user		データベースユーザー名です。	
password		データベースユーザーのパスワードです。	
temp_tablespaces		一時テーブルのネームスペースです。	
default_transaction_isolation	<ul style="list-style-type: none"> • read uncommitted (確定していないデータまで読み取る) • read committed (確定したデータを読み取る) • repeatable read (読み取り対象のデータを常に読み取る) • serializable 	トランザクションの分離レベルです。	read committed (確定したデータを読み取る)

- `<oracle connectionstring="" user="" password="" client="" prefetch-rows="0" prefetch-mem="0" />`

Oracle外部データベースを定義します。

属性の説明:

属性	可能な値	説明	デフォルト
connectionstring		Oracle SQL ConnectのURL文字列またはOracle Netのキーワードと値のペアです。	



属性	可能な値	説明	デフォルト
user		データベースユーザーの登録名です。	
password		データベースユーザーのパスワードです。	
client		Oracle DBにアクセスするOracleインスタントクライアントのパスです。Dr.Web ServerにはOracle Instant Clientバージョン11が付属しています。Oracleドライバがエラーを出力する場合や、新しいバージョンのOracleサーバーに対しては、Oracleサイトから対応するドライバをダウンロードし、この欄にドライバのパスを指定します。	
prefetch-rows	0-65535	データベースへのクエリを実行する際にプリフェッチする行数です。	0 - 値=1を使用 (データベースのデフォルト)
prefetch-mem	0-65535	データベースへのクエリを実行する際にプリフェッチする行に対して割り当てられるメモリです。	0 - 無制限

- `<odbc dsn="drwcs" user="" pass="" transaction="DEFAULT" />`

ODBC経由での外部データベースへの接続を定義します。

属性の説明:

属性	可能な値	説明	デフォルト
dsn		ODBCデータソース名です。	drwcs
user		データベースユーザーの登録名です。	drwcs
pass		データベースユーザーのパスワードです。	drwcs
limit	正の整数	指定された回数のトランザクションが行われた後、DBMSに再接続します。	0 - 再接続しません
transaction	<ul style="list-style-type: none"> • SERIALIZABLE - serializable (シリアライズ可能) • READ_UNCOMMITTED - read uncommitted data (確定していないデータまで読み取る) • READ_COMMITTED - read committed data (確定したデータを読み取る) • REPEATABLE_READ - repeatable read (読み取り対象のデータを常に読み取る) • DEFAULT - equal "" - DBMSによる 	トランザクションの分離レベルです。 一部のDBMSは READ_COMMITTED のみに対応しています。	DEFAULT



- `<mysql dbname="drwcs" host="localhost" port="3306" user="" password="" ssl="no" debug="no" />`

MySQL/MariaDB内部データベースを定義します。

属性の説明:

属性	可能な値	説明	デフォルト
dbname		データベース名	drwcs
host	2つのうちいずれか	TCP/IP接続のデータベースサーバーアドレスです。	localhost
		UDSを使用する場合のUNIXソケットファイルへのパスです。設定されていない場合、Serverは標準のmysqldディレクトリの1つでファイルを見つけようとします。	/var/run/mysql d/
port	2つのうちいずれか	TCP/IP経由でデータベースに接続する際のポート番号です。	3306
		UDSを使用する場合のUNIXソケットファイル名です。	mysqld.sock
user		データベースユーザーの登録名です。	""
password		データベースユーザーのパスワードです。	""
ssl	yes その他文字列	SSL接続のみ許可します。	no
precompiledcache	正の整数	プリコンパイルされたSQL演算子のキャッシュサイズです(キロバイト)。	1024

- `<acl>`

アクセス制限リストです。セキュリティ タブで、Agent、ネットワークインストーラ、他の(隣接の)Dr.Web Serverがサーバーにアクセスできるネットワークアドレスに対する制限を設定できます。

`<acl>`エレメントには、該当する接続の種類に対する制限を設定する以下の子エレメントが含まれます。

- `<install>` - Dr.Web AgentのインストーラがServerに接続することのできるIPアドレス制限のリストです。
- `<agent>` - Dr.Web AgentがServerに接続することのできるIPアドレス制限のリストです。
- `<links>` - 隣接するDr.Web ServerがServerに接続することのできるIPアドレス制限のリストです。
- `<discovery>` - Server検索サービスがブロードキャストクエリを受け取るIPアドレス制限のリストです。

全ての子エレメントは、以下の制限を定義するネストされたエレメントの同じ構造を持っています。

- `<priority mode="" />`

リストの優先順位です。modeに使用できる値は、allowまたはdenyです。`<priority mode="deny" />`値では、`<deny>`リストが`<allow>`リストよりも高い優先度を持ちます。いずれのリストにも含まれていないアドレス、または両方のリストに含まれているアドレスは拒否されます。`<allow>`リストに含まれており、`<deny>`リストには含まれていないアドレスのみが許可されます。

- `<allow>`



アクセスが許可されるTCPアドレスのリストです。<allow />エレメントには1つまたは複数の<ip address="" />と<ip6 address="" />子エレメントが含まれます。前者はIPv4フォーマットで許可するアドレスを指定し、後者はIPv6フォーマットで許可するアドレスを指定します。address属性は<IP address>/ [<prefix>] フォーマットでネットワークアドレスを定義します。

▫ <deny>

アクセスが拒否されるTCPアドレスのリストです。<deny /> エレメントには1つまたは複数の<ip address="" />と<ip6 address="" />子エレメントが含まれます。前者はIPv4フォーマットで拒否するアドレスを指定し、後者はIPv6フォーマットで拒否するアドレスを指定します。address属性は<IP address>/ [<prefix>] フォーマットでネットワークアドレスを定義します。

● <scripts profile="" stack="" trace="" />

スクリプトプロファイリングパラメータ設定です。

属性の説明:

属性	可能な値	説明	デフォルト
profile		必要のない限り、このパラメータは変更しないことを推奨します。サーバースクリプト実行プロファイリングに関する情報をログに記録します。このパラメータはテクニカルサポートやデベロッパーによって使用されます。	no
stack	<ul style="list-style-type: none"> • yes • no 	コールスタックからのサーバースクリプト実行に関する情報をログに記録します。このパラメータはテクニカルサポートやデベロッパーによって使用されます。必要のない限り、このパラメータは変更しないことを推奨します。	
trace		サーバースクリプト実行トレーシングに関する情報をログに記録します。このパラメータはテクニカルサポートやデベロッパーによって使用されます。必要のない限り、このパラメータは変更しないことを推奨します。	

● <lua-module-path>

Luaインタプリタのパスです。



パスの順番が重要です。

<lua-module-path>エレメントには以下の子エレメントが含まれます。

- <cpath root="" /> - バイナリモジュールフォルダへのパスです。rootに使用できる値: home(デフォルト)、var、bin、lib
- <path value="" /> - スクリプトフォルダへのパスです。<jobs />または<hooks />エレメントの子ではない場合、両方で使用されます。value属性で指定されたパスは<cpath>エレメントのroot属性内のパスからの相対になります。
- <jobs> - Serverスケジュールのタスクに対するパスです。

<jobs> エレメントには、スクリプトフォルダへのパスを指定する1つまたは複数の<path value="" />子エレメントが含まれます。

- <hooks> - Serverのユーザーフックに対するパスです。

<hooks> エレメントには、スクリプトフォルダへのパスを指定する1つまたは複数の<path value="" />子エレメントが含まれます。



- **< transports >**

クライアントと接続するためにServerが使用するトランスポートプロトコルパラメータの設定です。1つまたは複数の `<transport discovery="" ip="" name="" multicast="" multicast-group="" port="" />` 子エレメントが含まれます。

属性の説明:

属性	説明	必須	可能な値	デフォルト
discovery	サーバー検出サービスを使用するかどうかを定義します。	no、ip属性のみで指定します。	yes、no	no
<ul style="list-style-type: none"> • ip • unix 	使用するプロトコルのファミリーを定義し、インターフェースアドレスを指定します。	yes	-	<ul style="list-style-type: none"> • 0.0.0.0 • -
name	サーバー検出サービスのためのサーバー名を指定します。	no	-	drwcs
multicast	サーバーがマルチキャストグループに含まれているかどうかを定義します。	no、ip属性のみで指定します。	yes、no	no
multicast-group	サーバーが登録されているマルチキャストグループのアドレスを指定します。	no、ip属性のみで指定します。	-	<ul style="list-style-type: none"> • 231.0.0.1 • [ff18::231.0.0.1]
port	待ち受けるポートです。	no、ip属性のみで指定します。	-	2193

- **< protocols >**

無効なプロトコルのリストです。1つまたは複数の `<protocol enabled="" name="" />` 子エレメントが含まれます。

属性の説明:

属性	可能な値	説明	デフォルト
enabled	<ul style="list-style-type: none"> • yes - プロトコルは有効です。 • no - プロトコルは無効です。 	プロトコルの使用モードです。	no
name	<ul style="list-style-type: none"> • AGENT - サーバーとDr.Web Agentとの連携を可能にするプロトコルです。 • MSNAPSHV - サーバーとシステムの正常性を検証するコンポーネントであるMicrosoft NAP Validatorとの連携を可能にするプロトコルです。 • INSTALL - サーバーとDr.Web Agentインストーラとの連携を可能にするプロトコルです。 • CLUSTER - クラスタシステム内での複数のサーバー間の連携のためのプロトコルです。 • SERVER - Dr.Web Serverとその他のDr.Web Serverとの連携を可能にするプロトコルです。 	プロトコル名です。	-

- **< plugins >**



無効なプラグインのリストです。1つまたは複数の<plugin enabled="" name="" />子エレメントが含まれます。

属性の説明:

属性	可能な値	説明	デフォルト
enabled	<ul style="list-style-type: none"> yes - プラグインは有効です。 no - プラグインは無効です。 	プラグインの使用モードです。	no
name	<ul style="list-style-type: none"> WEBMIN - サーバーおよびアンチウイルスネットワークをControl Centerから管理するためのDr.Web Security Control Centerプラグインです。 FrontDoor - サーバーリモート診断ユーティリティに接続するためのDr.Web Server FrontDoorプラグインです。 	プラグイン名	-

● <license>

ライセンスの設定です。

<license>エレメントには以下の子エレメントが含まれます。

□ <limit-notify min-count="" min-percent="" />

ライセンスキー内のライセンス数の制限に関する通知のためのオプションです。

属性の説明:

属性	説明	デフォルト
min-count	ライセンスキー内のライセンス数の制限 通知が送信される、残りのライセンスの最大数です。	3
min-percent	ライセンスキー内のライセンス数の制限 通知が送信される、残りのライセンスの最大割合です。	5

□ <license-report report-period="" active-stations-period="" />

ライセンス使用状況に関するレポートのオプションです。

属性の説明:

属性	説明	デフォルト
report-period	<p>使用するライセンスキーに関するレポートをServerが作成する期間です。</p> <p>ライセンス使用状況に関するレポートが子Serverによって作成される場合、作成後にそのレポートがメインServerに送信されます。</p> <p>作成されたレポートは、Serverが接続される度(再起動を含む)に、また、メインServerで提供されるライセンスの数が変更された際にも送信されます。</p>	1440
active-stations-period	ライセンスの使用状況に関するレポートを作成するためにアクティブな端末数を数える期間です。値が0の場合は、そのアクティビティステータスに関係なくすべての端末をレポート内に含めます。	0

□ <exchange>

Dr.Web Server間のライセンス伝播の設定です。



`<exchange>` エlementには以下の子Elementが含まれます。

- `<expiration-interval value="" />`
- `<prolong-preact value="" />`
- `<check-interval value="" />`

Elementの説明:

Element	説明	value属性のデフォルト値です(分)。
expiration-interval	提供されたライセンスの有効期限 - 親サーバー上のキーから提供されるライセンスの有効期限です。この設定は親サーバーから隣接サーバーにライセンスが提供される場合に使用します。	1440
prolong-preact	受け取ったライセンスの有効期限 - ライセンスの期限が切れるまでの期間です。これに従ってサーバーは隣接サーバーから受け取ったライセンスの更新を開始します。この設定はサーバーが隣接サーバーからライセンスを受け取る場合に使用します。	60
check-interval	ライセンス同期間隔 - サーバー間でのライセンス提供に関する情報を同期する間隔です。	1440

- `<email from="" debug="" />`

Control CenterからEメールを送信(管理者への通知として、または端末のインストールパッケージを送信する場合など)するためのパラメータです。

属性の説明:

属性	可能な値	説明	デフォルト
from	-	メールの送信者として設定されるメールアドレスです。	drwcs@localhost
debug	<ul style="list-style-type: none"> • yes - デバッグモードを使用します。 • no - デバッグモードを使用しません。 	SMTPセッションの詳細なログを取得するには、デバッグモードを使用します。	no

`<email>` Elementには以下の子Elementが含まれます。

- `<smtp server="" user="" pass="" port="" start_tls="" auth_plain="" auth_login="" auth_cram_md5="" auth_digest_md5="" auth_ntlm="" conn_timeout="" />`

メールを送信するためのSMTPサーバーのパラメータ設定です。

属性の説明:

属性	可能な値	説明	デフォルト
server	-	メールの送信に使用するSMTPサーバーのアドレスです。	127.0.0.1
user	-	SMTPサーバーが認証を必要としている場合の、SMTPサーバーユーザー名です。	-



属性	可能な値	説明	デフォルト
pass	-	SMTPサーバーが認証を必要としている場合の、SMTPサーバーユーザーのパスワードです。	-
port	正の整数	メールの送信に使用するSMTPサーバーのポートです。	25
start_tls	<ul style="list-style-type: none"> • yes - この認証タイプを使用します。 • no - この認証タイプを使用しません。 	データ転送を暗号化します。その際、STARTTLSコマンドを使用して安全な接続への切り替えが実行されます。接続にはデフォルトで25番ポートが使用されます。	yes
auth_plain		メールサーバー上でプレーンテキスト認証を使用します。	no
auth_login		メールサーバー上でLOGIN認証を使用します。	no
auth_cram_md5		メールサーバー上でCRAM-MD5認証を使用します。	no
auth_digest_md5		メールサーバー上でDIGEST-MD5認証を使用します。	no
auth_ntlm	メールサーバー上でAUTH-NTLM認証を使用します。	no	
conn_timeout	正の整数	SMTPサーバーの接続タイムアウトです。	180

▪ `<ssl enabled="" verify_cert="" ca_certs="" />`

メール送信のためのSSLトラフィック暗号化パラメータです。

属性の説明:

属性	可能な値	説明	デフォルト
enabled	<ul style="list-style-type: none"> • yes - SSLを使用します。 • no - SSLを使用しません。 	SSL暗号化使用モードです。	no
verify_cert	<ul style="list-style-type: none"> • yes - SSL証明書をチェックします。 • no - SSL証明書をチェックしません。 	メールサーバーのSSL証明書を検証します。	no
ca_certs	-	Dr.Web ServerのルートSSL証明書へのパスです。	-

• `<track-epidemic enabled="" aggregation-period="" check-period="" threshold="" most-active="" />`

ネットワーク内での大規模感染トラッキングのパラメータ設定です。



属性の説明:

属性	可能な値	説明	デフォルト
enabled	yes no	感染している端末の複数のイベントをモニタリングすることを可能にし、サマリー通知を管理者に送信することができます。	yes
aggregation-period	正の整数	感染拡大に関する通知を送信した後の、個々の感染した端末に関する通知を送信しない期間(秒単位)です。	300
check-period		一定の数の感染した端末に関する通知を受け取った場合に感染拡大に関する通知を送信する期間(秒単位)です。	3600
threshold		指定された期間に受け取る感染通知の数を指定します。この数の感染通知を指定された期間に受け取ると、Dr.Web Serverは全ての感染のケースが含まれた感染拡大に関する通知を1通のみ管理者に対して送信します(ネットワーク内で感染拡大が検出されました 通知)。	100
most-active		感染拡大レポートに含める必要がある、最も多く検出されている脅威の数です。	5

- `<track-hips-storm enabled="" aggregation-period="" check-period="" threshold="" most-active="" />`

予防的保護コンポーネントの複数のイベントを追跡するためのパラメータの設定です。

属性の説明:

属性	可能な値	説明	デフォルト
enabled	yes no	予防的保護の複数のイベントをモニタリングすることを可能にし、サマリー通知を管理者に送信することができます。	yes
aggregation-period	正の整数	予防的保護イベントに関するサマリーレポートを送信した後の、個々のイベントに関する通知を送信しない期間(秒単位)です。	300
check-period		一定の数の予防的保護イベントに関する通知を受け取った場合にサマリーレポートを送信する期間(秒単位)です。	3600
threshold		指定された期間に受け取る必要のある予防的保護イベントの数です。指定された数のイベントを受け取ると、Dr.Web Serverはこれらのイベントに関する1通のサマリーレポートを管理者に送信します(予防的保護のサマリーレポート 通知)。	100
most-active		予防的保護レポートに含める必要がある、最も多く検出された、疑わしいアクションを実行するプロセスの数です。	5

- `<track-appctl-storm enabled="" aggregation-period="" check-period="" threshold="" most-active="" />`

Application Controllコンポーネントの複数のイベントを追跡するためのパラメータの設定です。



属性の説明:

属性	可能な値	説明	デフォルト
enabled	yes no	Application Controlの複数のイベントをモニタリングすることを可能にし、サマリー通知を管理者に送信することができます。	yes
aggregation-period	正の整数	Application Controlによってブロックされたプロセスに関するサマリーレポートを送信した後の、個々のブロックに関する通知を送信しない期間(秒単位)です。	300
check-period		一定の数のプロセスがブロックされた場合にサマリーレポートを送信する期間(秒単位)です。	3600
threshold		指定された期間に受け取る必要のある、Application Controlによってブロックされたプロセスに関するイベントの数です。指定された数のイベントを受け取ると、Dr.Web Serverはこれらのイベントに関する1通のサマリーレポートを管理者に送信します(Application Controlによる多数のブロックが検出されました 通知)。	100
most-active		複数ブロックのレポートに含める必要がある、ブロックに最も多く使用されているプロファイル(それに従ってブロックが実行されたプロファイル)の数です。	5

- `<track-disconnect enabled="" aggregation-period="" check-period="" single-alert-threshold="" summary-alert-threshold="" min-session-duration="" />`

クライアントとの複数の異常終了した接続を追跡するためのパラメータの設定です。

属性の説明:

属性	可能な値	説明	デフォルト
enabled	yes no	クライアントとの異常終了した接続のモニタリングを可能にし、対応する通知を管理者に送信することができます。	yes
aggregation-period	正の整数	複数の接続終了に関する通知を送信した後の、個々の接続終了に関する通知を送信しない期間(秒単位)です。	300
check-period		一定の数のクライアントとの接続が終了した場合に該当する通知を送信する期間(秒単位)です。	3600
single-alert-threshold		1つの異常終了した接続に関する通知を送信するために、カウント期間中に終了する必要がある1つのアドレスとの最低限の接続数です(接続が異常終了しました 通知)。	10
summary-alert-threshold		複数の異常終了した接続に関する共通の通知を送信するために、カウント期間中に終了する必要がある最低限の接続数です(異常終了した接続が多数検出されました 通知)。	1000



属性	可能な値	説明	デフォルト
min-session-duration		終了したクライアントとの接続の持続時間が指定された値よりも短い場合、カウント期間に関係なく、接続数が指定された数に達した際に1つの終了した接続に関する通知(接続が異常終了しました 通知)が送信されず。短い接続とは、それよりも長い接続によって中断されておらず、それらの接続終了について1つの共通の通知が送信されていないものを指します(異常終了した接続が多数検出されました 通知)。	300

- `<default-lang value="" />`

サーバーデータベースから言語設定を受け取ることができなかった場合に、コンポーネントおよびDr.Web Serverシステムによってデフォルトで使用される言語です。特に、データベースが破損して言語設定を取得することができない場合にDr.Web Security Control Centerおよび管理者通知システムで使用されます。

G2. Dr.Web Security Control Center設定ファイル

webmin.conf(Dr.Web Security Control Center設定ファイル)はXMLフォーマットで、サーバーインストールフォルダの `etc` サブフォルダ内にあります。

Dr.Web Security Control Center設定ファイルのパラメータ:

- `<version value="">`

Dr.Web Serverの現在のバージョンです。

- `<server-name value="" />`

Dr.Web Serverの名前です。

次のフォーマットで指定します。

`<ServerのIPアドレスまたはDNS名>[: <port>]`

サーバーアドレスが指定されなかった場合、OSによって返されたコンピューター名、またはサーバーネットワークアドレス(使用可能な場合はDNS名、それ以外の場合はIPアドレス)が使用されます。

ポート番号が指定されなかった場合、リクエスト内で指定されたポート(Control Centerからの、または**Web API**経由でのサーバーへのリクエストなど)が使用されます。特に、Control CenterからのリクエストではControl Centerをサーバーに接続するためのアドレスフィールド内で指定されたポートが使用されます。

- `<document-root value="" />`

Webページのルートフォルダのパスです。デフォルトは`value="webmin"`になります。

- `<ds-modules value="" />`

モジュールフォルダのパスです。デフォルトは`value="ds-modules"`になります。

- `<threads value="" />`

Webサーバーによって同時に処理されるリクエスト数です。このパラメータはサーバーのパフォーマンスに影響します。必要のない限り変更しないことを推奨します。

- `<io-threads value="" />`

ネットワーク上でやり取りされるデータの処理を行うスレッドの数です。このパラメータはサーバーのパフォーマンスに影響します。必要のない限り変更しないことを推奨します。

- `<compression value="" max-size="" min-size="" />`



Webサーバーとの通信チャンネル上でのHTTP / HTTPS経由でのデータ送受信の圧縮設定です。

属性の説明:

属性	説明	デフォルト
value	データ圧縮レベルは1~9です(1が最小、9が最大)。	9
max-size	圧縮されるHTTPからの応答の最大サイズです。0を指定すると無制限になります。	51200 KB
min-size	圧縮されるHTTPからの応答の最小サイズです。0を指定すると無制限になります。	32 bytes

- `<keep-alive timeout="" send-rate="" receive-rate=""/>`

HTTPセッションをアクティブな状態に保ちます。HTTP v 1.X.経由でのリクエストに対する接続の確立を恒久的に維持します。

属性の説明:

属性	説明	デフォルト
timeout	HTTPセッションのタイムアウトです。指定された時間内にクライアントからのリクエストを受信しなかった場合、サーバーはセッションを切断します。	15 sec.
send-rate	許容する最小送信データレートです。データ送信速度がこの値よりも小さい場合、接続は拒否されます。この制限を無視する場合は0を設定します。	1024 Bps
receive-rate	許容する最小受信データレートです。データ受信速度がこの値よりも小さい場合、接続は拒否されます。この制限を無視する場合は0を設定します。	1024 Bps

- `<buffers-size send="" receive=""/>`

データ送受信のバッファサイズを設定します。

属性の説明:

属性	説明	デフォルト
send	データ送信時に使用するバッファのサイズです。このパラメータはサーバーのパフォーマンスに影響します。必要のない限り変更しないことを推奨します。	8192 bytes
receive	データ受信時に使用するバッファのサイズです。このパラメータはサーバーのパフォーマンスに影響します。必要のない限り変更しないことを推奨します。	2048 bytes

- `<max-request-length value=""/>`

HTTPリクエストの最大許容サイズ(KB)です。

- `<reverse-resolve enabled=""/>`

サーバーログファイル内のIPアドレスをDNS名に置き換えます。enabledの値にはyesまたはnoを使用できます。

- `<script-errors-to-browser enabled=""/>`

スクリプトエラーをブラウザ内に表示します(error 500)。このパラメータはテクニカルサポートやデベロッパーによって使用されます。必要のない限り変更しないことを推奨します。

- `<trace-scripts enabled=""/>`



スクリプトのトレースを有効にします。このパラメータはテクニカルサポートと開発者が使用します。必要ない限りは変更しないことを推奨します。`enabled`の値には`yes`または`no`を使用できます。

- `<profile-scripts enabled="" stack="" />`

プロファイリング設定です。パフォーマンス測定 - Webサーバーの関数およびスクリプトの実行時間です。このパラメータはテクニカルサポートやデベロッパーによって使用されます。必要のない限り変更しないことを推奨します。

属性の説明:

属性	可能な値	説明
<code>enabled</code>	<ul style="list-style-type: none"> ● <code>yes</code> - プロファイリングを有効にします。 ● <code>no</code> - プロファイリングを無効にします。 	スクリプトのプロファイリングモードです。
<code>stack</code>	<ul style="list-style-type: none"> ● <code>yes</code> - データをログに記録します。 ● <code>no</code> - データをログに記録しません。 	プロファイリング(関数パラメータおよび戻り値)に関する情報のサーバーログへのロギングモードです。

- `<abort-scripts enabled="" />`

接続がクライアントによって切断された場合にスクリプトの実行を中断します。このパラメータはテクニカルサポートと開発者が使用します。必要ない限りは変更しないことを推奨します。`enabled`の値には`yes`または`no`を使用できます。

- `<search-localized-index enabled="" />`

ローカライズされたページを使用します。このフラグがセットされている場合、サーバーは、クライアントのヘッダーの`Accept-Language`フィールドで設定されている優先言語に従って、指定されたページのローカライズされたバージョンを検索します。`enabled`の値には`yes`または`no`を使用できます。

- `<default-lang value="" />`

HTTPリクエストの`Accept-Language`ヘッダーが存在しない場合に、Webサーバーから返されるドキュメントの言語`value`属性は、ISO言語コードです。デフォルトは`ru`です。

- `<ssl certificate="" private-key="" keep-alive="" />`

SSL証明書の設定です。

属性の説明:

属性	説明	可能な値	デフォルト
<code>certificate</code>	SSL証明書ファイルへのパスです。	-	<code>certificate.pem</code>
<code>private-key</code>	SSLプライベートキーファイルへのパスです。	-	<code>private-key.pem</code>
<code>keep-alive</code>	SSL接続のキープアライブを使用します。古いブラウザでは持続的なSSL接続が正しく動作しない場合があります。SSLプロトコルに問題がある場合は、このパラメータを無効にします。	<ul style="list-style-type: none"> ● <code>yes</code> ● <code>no</code> 	<code>yes</code>

- `<listen>`

ネットワーク接続を待ち受けるパラメータを設定します。

`<listen />` エlementには以下の子Elementが含まれます。

- `<insecure />`



HTTPプロトコル経由での安全でない接続を許可するための、待ち受けるインターフェースのリストです。デフォルトでのポートは9080です。

`<insecure />` エlementには、許可するアドレスをIPv4またはIPv6フォーマットで指定する1つまたは複数の`<endpoint address="" />`子Elementが含まれます。`address`属性では、`<Protocol>:// <IP address>`の形式でネットワークアドレスが指定されます。

□ `<secure />`

HTTPプロトコル経由での安全な接続を許可するための、待ち受けるインターフェースのリストです。デフォルトでのポートは9081です。

`<secure />` Elementには、許可するアドレスをIPv4またはIPv6フォーマットで指定する1つまたは複数の`<endpoint address="" />`子Elementが含まれます。`address`属性では、`<Protocol>:// <IP address>`の形式でネットワークアドレスが指定されます。

- `<access>`

アクセス制御リストです。WebサーバーによるHTTPおよびHTTPSリクエストの受信を許可するために、待ち受けるネットワークアドレスに対して制限を設定できます。

`<access>`Elementには、該当する接続の種類に対する制限を設定する以下の子Elementが含まれます。

□ `<secure priority="">`

HTTPSプロトコル経由での安全な接続を許可するための、待ち受けるインターフェースのリストです。デフォルトでのポートは9081です。

属性の説明:

属性	可能な値	説明	デフォルト
priority	allow	HTTPSの許可プライオリティ - いずれのリストにも含まれていない(または両方に含まれている)アドレスは許可されます。	deny
	deny	HTTPSの拒否プライオリティ - いずれのリストにも含まれていない(または両方に含まれている)アドレスは拒否されます。	

`<secure />`Elementには1つまたは複数の`<allow address="" />`および`<deny address="" />`子Elementが含まれます。

Elementの説明:

Element	説明	<code>address</code> 属性のデフォルト値
allow	安全な接続のHTTPSプロトコル経由でのアクセスを許可するアドレスです。	tcp://127.0.0.1
deny	安全な接続のHTTPSプロトコル経由でのアクセスを拒否するアドレスです。	-

□ `<insecure priority="">`

HTTPプロトコル経由での安全でない接続を許可するための、待ち受けるインターフェースのリストです。デフォルトでのポートは9080です。

属性の説明:



属性	可能な値	説明	デフォルト
priority	allow	HTTPの許可プライオリティ - いずれのリストにも含まれていない(または両方に含まれている)アドレスは許可されます。	deny
	deny	HTTPの拒否プライオリティ - いずれのリストにも含まれていない(または両方に含まれている)アドレスは拒否されます。	

`<insecure />` エレメントには1つまたは複数の`<allow address="" />`および`<deny address="" />`子エレメントが含まれます。

エレメントの説明:

エレメント	説明	address属性のデフォルト値
allow	安全でない接続のHTTPプロトコル経由でのアクセスを許可するアドレスです。	tcp://127.0.0.1
deny	安全でない接続のHTTPSプロトコル経由でのアクセスを拒否するアドレスです。	-

G3. download.conf設定ファイル

download.confファイルによって:

1. Dr.Web Serverクラスタシステムの作成中および操作中に、多数の新規端末に接続する場合、クラスタのサーバー間で負荷を分散できます。
2. Dr.Web Serverでカスタムポートを使用している場合、Agentのインストールファイル作成中にそのポートを指定できます。

download.confファイルは、アンチウイルスネットワークの新規端末に対するインストールファイルの作成時に使用されます。このファイルのパラメータによって、Agentインストーラをサーバーに接続するためのサーバーアドレスおよびポート番号を以下のフォーマットで指定できます。

```
download = { server = '<Server_Address>'; port = <port_number> }
```

ここで:

- `<Server_Address>` - サーバーのIPアドレスまたはDNS名
Agentインストールファイルの作成時、まず最初にdownload.confファイルのサーバーアドレスが使用されます。download.confファイル内にサーバーアドレスが指定されていない場合、webmin.confファイルのServerNameパラメータ値が使用されます。それ以外の場合は、OSによって返されるコンピューター名が使用されます。
- `<port_number>` - Agentインストーラをサーバーに接続するためのポート
download.confファイル内でポートが指定されていない場合、デフォルトで2193ポートが使用されます(Control Centerの 管理 → Dr.Web Server設定 → ネットワーク タブ → トランスポート タブで設定)。



デフォルトでは、download.confファイルのdownloadパラメータは無効になっています。download.confファイルを使用するには、ラインの初めにある"--"を削除することでこのパラメータをアンコメントし、該当するアドレスの値およびサーバーのポートを指定します。

G4. Dr.Web Proxy Server設定ファイル

Proxy Serverのdrwcsd-proxy.conf設定ファイルはXMLフォーマットで、以下の場所にあります。

- Windows OS: C:\ProgramData\Doctor Web\drwcs\etc
- Linux OS: /var/opt/drwcs/etc
- FreeBSD OS: /var/drwcs/etc

Dr.Web Server設定ファイルパラメータ:

- `<listen spec="">`
`<drwcsd-proxy />`ルートエレメントは、プロキシサーバーの受信接続の基本設定を定義する必須の`<listen />`エレメントを1つまたは複数含んでいます。
`<listen />`エレメントは1つの必須属性specを含み、その属性はクライアント接続の着信を「リッスン」するためのインターフェース、およびそのインターフェース上でdiscoveryモードが有効かどうかを定義します。

specエレメントの属性:

属性	必須	可能な値	説明	デフォルト
ip unix	yes	—	接続の着信を受信するプロトコルのタイプ。Proxy Serverがリッスンするアドレスが属性として設定されます。	0.0.0.0 -
port	no	—	Proxy Serverがリッスンするポート。	2193
discovery	no	yes、no	Serverイミテーションのモード。ネットワークスキャナがProxy ServerをDr.Web Serverとして検出できるモードです。	yes
multicast	no	yes、no	Proxy Serverによるマルチキャストリクエストを受信するためのネットワーク「リッスン(待機中)」モード。	yes
multicast-group	no	—	Proxy Serverがあるマルチキャストグループ。	231.0.0.1 [ff18::231.0.0.1]

spec属性内の必須でないプロパティのリストは、プロトコルによって異なる場合があります。

プロトコルに応じて、spec属性内で設定可能(+)、または設定不可能(-)な必須でないプロパティのリストです。

プロトコル	属性内での可否			
	port	discovery	multicast	multicast-group
ip	+	+	+	+



プロトコル	属性内での可否			
	port	discovery	multicast	multicast-group
unix	+	-	-	-



discoveryモードは、**multicast**モードが有効になっている場合であっても、直接有効にする必要があります。

Dr.Web Serverのリストを転送するアルゴリズムについては管理者マニュアルに記載されています。

□ `<compression mode="" level="">`

`<compression />`エレメントは`<listen/>`エレメントの子エレメントで、クライアント - Proxy Server間の通信の圧縮パラメータを定義します。

属性の説明:

属性	可能な値	説明	デフォルト
mode	yes	圧縮が有効	possible
	no	圧縮が無効	
	possible	圧縮が可能	
level	1~9の整数	圧縮レベル。クライアント - Proxy Server間の通信の場合のみ。	8

□ `<encryption mode="">`

`<encryption />`エレメントは`<listen/>`エレメントの子エレメントで、クライアント - Proxy Server間の通信の暗号化パラメータを定義します。

属性の説明:

属性	可能な値	説明	デフォルト
mode	yes	暗号化が有効	possible
	no	暗号化が無効	
	possible	暗号化可能	

□ `<forward to="" master="">`

着信接続をリダイレクトする設定を指定します。`<forward />`エレメントは必須です。複数の`<forward />`エレメントは、異なる属性値で設定できます。

属性の説明:

属性	可能な値	説明	必須
to	アドレスはネットワークアドレスの指定に従って、特に	接続をリダイレクトするDr.Web Serverのアドレスです。	yes



属性	可能な値	説明	必須
	tcp/ <DNS_name>: <port> の形式で指定されます。		
master	<ul style="list-style-type: none"> • yes - Serverは無条件に管理されます。 • no - Serverはどんな条件下でも管理されません。 • possible - Serverは明示的に管理するServer (master属性にYes値を持つServer)がない場合のみ管理します。 	<p>この属性はto属性で指定されたDr.Web ServerのControl Centerから、Proxy Serverの設定をリモートで編集できるかどうかを定義します。</p> <p>任意の数のServerに管理を割り当てることができます (master="yes"に設定)。Proxy Serverは、最初の有効な(空ではない)設定が見つかるまで、設定内の全ての管理Serverに順番に接続します。</p> <p>また、どのServerにも管理を割り当てない設定も可能です (master="no"に設定)。この場合、Proxy Serverのパラメータ(管理Serverの割り当てを含む)は、Proxy Serverの設定ファイルを使用してローカルでのみ設定できます。</p>	no



Serverにmaster属性がない場合、デフォルトはmaster="possible"と同じです。

Proxy Serverのインストール中にインストーラによって作成された設定ファイルでは、どのServerにもmaster属性は定義されていません。

- `<compression mode="" level="">`

`<compression/>`エレメントは`<forward/>`エレメントの子エレメントである場合、Server - Proxy Server間の通信の圧縮パラメータを定義します。属性は前述のとおりです。

- `<encryption mode="">`

`<encryption />`エレメントは`<forward/>`エレメントの子エレメントである場合、Server - Proxy Server間の通信の暗号化パラメータを定義します。属性は前述のとおりです。

- `<update-bandwidth value="" queue-size="">`

`<update-bandwidth/>`エレメントによって、Serverからクライアントへの更新の配信速度上限と、更新を同時にダウンロードするクライアントの数を設定できます。

属性の説明:

属性	可能な値	説明	デフォルト
value	<ul style="list-style-type: none"> • KB/秒 • 無制限 	更新配信の最大速度	無制限
queue-size	<ul style="list-style-type: none"> • 正の整数 • 無制限 	同時に実行することのできるServerからの更新配信セッションの上限です。上限に達した場合、Agentのリクエストは実行待ちのキューに置かれます。キューのサイズに上限はありません。	無制限

- `<bandwidth value="" time-map="" />`

`<update-bandwidth/>`エレメントは、1つまたは複数の`<bandwidth />`子エレメントを持つことができます。このエレメントは指定された期間におけるデータ転送の速度に上限を設定します。

属性の説明:



属性	可能な値	説明	デフォルト
value	<ul style="list-style-type: none"> KB/秒 無制限 	Agent更新時のデータ転送速度の上限	無制限
time-map	—	上限を適用する期間を指定するマスク	—



time-mapの値にはServer設定のトラフィック更新スケジュールのものと同一ものが指定されます。time-mapの手動での設定は現時点ではサポートされていません。

□ `<install-bandwidth value="" queue-size="">`

`<install-bandwidth>`エレメントはAgentインストール中のデータ転送速度の上限と、インストールデータを同時にダウンロードするクライアントの数を設定します。

属性の説明:

属性	可能な値	説明	デフォルト
value	<ul style="list-style-type: none"> KB/秒 無制限 	Agentインストール中のデータ転送速度の上限	無制限
queue-size	<ul style="list-style-type: none"> 正の整数 無制限 	キューのサイズに上限はありません。Serverから同時に実行することのできるAgentインストールセッション数の上限です。上限に達した場合、Agentのリクエストは実行待ちのキューに置かれます。	無制限

▪ `<bandwidth value="" time-map="">`

`<install-bandwidth />`エレメントは、1つまたは複数の`<bandwidth/>`子エレメントを持つことができます。このエレメントは指定された期間におけるデータ転送の速度に上限を設定します。

属性の説明:

属性	可能な値	説明	デフォルト
value	<ul style="list-style-type: none"> KB/秒 無制限 	Agentインストール時のデータ転送速度の上限	無制限
time-map	—	上限を適用する期間を指定するマスク	—



time-mapの値にはServer設定のトラフィック更新スケジュールのものと同一ものが指定されます。time-mapの手動での設定は現時点ではサポートされていません。

● `<cache enabled="">`

Proxy Serverのリポジトリキャッシュの設定を行います。

属性の説明:

属性	可能な値	説明	デフォルト
enabled	yes no	キャッシングが有効かどうかを定義します。	yes

`<cache>`エレメントには以下の子エレメントが含まれます。



エレメント	可能な値	説明	デフォルト
<code><clean-interval value=""></code>	正の整数	保存するリビジョンの数。	3
<code><unload-interval value=""></code>	正の整数	古くなったリビジョンを削除する間隔(分単位)。	60
<code><repo-check mode=""></code>	正の整数	使用されていないファイルをメモリからアンロードする間隔(分単位)。	10
<code><repo-check /></code>	idle sync	起動時(時間がかかることがあります)に、またはバックグラウンドで行うキャッシュの整合性チェック。	idle

□ `<synchronize enabled="" schedule="">`

Proxy ServerとDr.Web Serverリポジトリとの同期の設定。

属性の説明:

属性	可能な値	説明	デフォルト
enabled	yes no	リポジトリの同期が有効になっているかどうかを定義します。	yes
schedule	—	指定された製品の同期のスケジュール。	—



scheduleパラメータには、Control Centerの設定の同期スケジュールと同じ値が設定されます。scheduleの手動での設定は現時点ではサポートされていません。

`<product name="" />`子エレメントは、同期する製品のリストを生成します。

- 10-drwbases - ウイルスデータベース
 - 10-drwgatedb - SpIDer Gateデータベース
 - 10-drwspamdb - AntiSpamデータベース
 - 10-drwupgrade - Dr.Web Updater
 - 15-drwappcntrl - Application Controlコンポーネントの信頼できるアプリケーション
 - 15-drwhashdb - 既知の脅威のハッシュ
 - 20-drwagent - Dr.Web Agent for Windows
 - 20-drwandroid11 - Dr.Web Agent for Android
 - 20-drwunix - Dr.Web Agent for UNIX
 - 40-drwproxy - Dr.Web Proxy Server
 - 70-drwextra - Dr.Webエンタープライズ製品
 - 70-drwutils - Dr.Web管理ユーティリティ
- `<events enabled="" schedule="">`

Agentから受信したイベントをキャッシュするための設定。

属性の説明:

属性	可能な値	説明	デフォルト
enabled	yes no	キャッシングが有効かどうかを定義します。	yes



属性	可能な値	説明	デフォルト
		有効の場合、イベントはタイムテーブルに従ってServerに送信されます。キャッシュが無効になっている場合、イベントはDr.Web Proxy Serverによって受信された直後に、Serverに送信されます。	
schedule	—	Agentからイベントを送信するためのタイムテーブル。	—



scheduleパラメータには、Control Centerの設定のイベント送信スケジュールと同じ値が設定されます。scheduleの手動での設定は現時点ではサポートされていません。

- `<update enabled="" schedule="">`

Proxy Serverの自動更新の設定。

自動更新では、同期が有効になっている場合、Proxy Serverの更新は、(上の)同期タイムテーブルに従ってServerからダウンロードされ、更新タイムテーブル(デフォルトでは時間による制約なし)に従ってインストールされます。同期が無効になっている場合は、更新タイムテーブル(デフォルトでは時間による制約なし)に従って更新がダウンロードされ、インストールされます。

属性の説明:

属性	可能な値	説明	デフォルト
enabled	yes no	自動更新が有効かどうかを定義します。	yes
schedule	—	これに従って更新がダウンロードされ(同期が設定されていない場合)、インストールされるタイムテーブル。	—



scheduleの手動での設定は現時点ではサポートされていません。デフォルトでは、自動更新は時間による制約なしで許可されます。

- `<core-dump enabled="" maximum="">`

SEH例外が発生した場合の収集モードとメモリダンプ数。



メモリダンプの設定はWindows環境でのみ可能です。

メモリダンプを収集するには、OSにdbghelp.dllライブラリが含まれている必要があります。

ダンプは次のフォルダに出力されます: %All Users\Application Data%\Doctor Web\drwcsd-proxy-dump\
 \

属性の説明:

属性	可能な値	説明	デフォルト
enabled	yes no	ダンプの収集が有効かどうかを定義します。	yes
maximum	正の整数	ダンプ数の上限。最も古いダンプから削除されます。	10

- `<dns>`



DNS設定です。

```
<timeout value="">
```

DNS正引き・逆引きのタイムアウト(秒)です。解決するまでの待ち時間に制限を設けない場合は値を0に設定します。

```
<retry value="">
```

DNSクエリの解決に失敗した場合に、クエリを繰り返す回数の上限です。

```
<cache enabled="" negative-ttl="" positive-ttl="">
```

DNSサーバーの応答をキャッシュに保存する時間(TTL)を設定します。

属性の説明:

属性	可能な値	説明
enabled	<ul style="list-style-type: none">• yes - 応答をキャッシュに保存します。• no - 応答をキャッシュに保存しません。	応答をキャッシュに保存するモードです。
negative-ttl	—	DNSサーバーからのネガティブな応答をキャッシュに保存(TTL)する時間(分)です。
positive-ttl	—	DNSサーバーからのポジティブな応答をキャッシュに保存(TTL)する時間(分)です。

```
<servers>
```

デフォルトのシステムリストに置き換わるDNSサーバーリストです。1つ以上の<server address="">子エレメントを持ち、そのaddressパラメータがサーバーのIPアドレスを定義します。

```
<domains>
```

デフォルトのシステムリストに置き換わるDNSドメインリストです。1つ以上の<domain name="">子エレメントを持ち、そのnameパラメータがドメイン名を定義します。

G5. Repository Loader設定ファイル

drwreploder.conf Repository Loader設定ファイルはXMLフォーマットで、Serverインストールフォルダのetcサブフォルダ内にあります。

設定ファイルを使用するには

- コンソールユーティリティの場合、ファイルへのパスは--config **スイッチ**で指定する必要があります。
- グラフィカルユーティリティの場合、ファイルはユーティリティフォルダに存在する必要があります。ユーティリティが設定ファイルなしで実行されると、ユーティリティフォルダに設定ファイルが作成され、次の起動時に使用されます。

Repository Loader設定ファイルパラメータの説明:

- <mode value="" path="" archive="" key="">

属性の説明:



属性	説明	可能な値
value	ローディングモードを更新します。 <ul style="list-style-type: none"> repository - リポジトリがサーバーリポジトリフォーマットでダウンロードされます。ロードされたファイルはServerリポジトリの更新と同時にControl Center経由で直接インポートできます。 mirror - リポジトリがGUS更新ゾーンフォーマットでダウンロードされます。ロードされたファイルはローカルネットワークの更新ミラーに置くことができます。以後、GUS サーバーからではなく、リポジトリの最新バージョンを含んだこの更新ミラーから直接更新を受け取るようServerを設定できます。 	repository mirror
path	リポジトリをダウンロードするフォルダ。	-
archive	ダウンロードしたリポジトリを自動的にzipファイル形式でアーカイブします。これにより、ダウンロードしたリポジトリアーカイブをControl Centerの 管理 → リポジトリコンテンツ セクションにインポートできるようになります。	yes no
key	Dr.Webライセンスキーファイル。ユーザーは、ライセンスキーの代わりにライセンスキーのMD5ハッシュのみ指定できます。MD5ハッシュはControl Centerの 管理 → ライセンスマネージャー セクションで確認できます。	-

- `<log path="" verbosity="" rotate="">`

Repository Loaderログの設定。

属性の説明:

属性	説明	可能な値
path	ログファイルへのパス。	-
verbosity	ログの詳細レベル。デフォルトはTRACE3です。	ALL、DEBUG3、DEBUG2、DEBUG1、DEBUG、TRACE3、TRACE2、TRACE1、TRACE、INFO、NOTICE、WARNING、ERROR、CRIT。ALL値とDEBUG3値はシノニムです。
rotate	<code><N><f></code> , <code><M><u></code> フォーマットのRepository Loaderログローテーションモード。 サーバーログローテーション と同じです。 デフォルトでは10, 10mで、圧縮を使ってそれぞれ10メガバイトのファイルを10個保存するという意味になります。	-

- `<update url="" proto="" cdn="" update-key="" version="">`

リポジトリの一般的なローディング設定。

属性の説明:

属性	説明	可能な値
.url	Dr.Web製品の更新を含むGUSサーバーのフォルダ。	-



属性	説明	可能な値
proto	更新サーバーから更新を受信するプロトコルのタイプ。全てのプロトコルで、更新はGUSサーバーリストの設定に沿ってダウンロードされます。	http https ftp ftps sftp scp file
cdn	Content Delivery Networkを使用してGUSからリポジトリをダウンロードすることを許可します。	yes no
update-key	GUSからロードされた更新の署名を検証するためのパブリックキーまたはパブリックキーのフォルダへのパス。更新を検証するためのupdate-key-* .upubパブリックキーは、Dr.Web Serverのetc フォルダにあります。	-
version	更新をロードする必要のあるServerのバージョン。	-

□ `<servers>`

サーバーリストを更新します。GUSサーバーのリストでの順番は、リポジトリのダウンロード時にユーティリティと接続される順番になります。

更新サーバーを定義する`<server>`子エレメントを含みます。

□ `<auth user="" password="">`

更新サーバーで認証が必要な場合のユーザー認証情報。

属性の説明:

属性	説明
user	更新サーバーのユーザー名。
password	更新サーバーのパスワード。

□ `<proxy host="" port="" user="" password="" />`

プロキシサーバー経由でGUSに接続するためのパラメータ。

属性の説明:

属性	説明
host	プロキシサーバーのネットワークアドレス。
port	プロキシサーバーのポート番号。デフォルトは3128です。
user	使用するプロキシサーバーで認証が要求される場合のユーザー名。
password	使用するプロキシサーバーで認証が要求される場合のパスワード。

□ `<ssl cert-mode="" cert-file="">`

自動的に承認されるSSL証明書のタイプ。このオプションは、暗号化をサポートする安全なプロトコルにのみ使用されます。

属性の説明:



属性	説明	可能な値
cert-mode	証明書を自動的に許可します。	<ul style="list-style-type: none"> □ any - 全ての証明書を許可 □ valid - 有効な証明書のみを許可 □ drweb - Dr.Web証明書のみを許可 □ custom - ユーザー指定の証明書を許可。
cert-file	証明書ファイルへのパス。	-

□ `<ssh mode="" pubkey="" prikey="">`

SCP/SFTPによるアクセス時の更新サーバー上の認証種別。

属性の説明:

属性	説明	可能な値
mode	認証種別。	<ul style="list-style-type: none"> □ pwd - パスワードを使用する認証。パスワードは<auth/>タグに設定されています。 □ pubkey - パブリックキーを使用する認証。パブリックキーは、pubkey属性に設定されているか、prikeyで指定されたプライベートキーから抽出されます。
pubkey	パブリックSSHキー	-
prikey	プライベートSSHキー	-

● **<products>**

製品の設定をロードします。

□ `<product name="" update="">`

各製品の個別設定。

属性の説明:

属性	説明	可能な値
name	製品名。	<ul style="list-style-type: none"> ● 05-drwmeta - Dr.Web Serverセキュリティデータ ● 10-drwbases - ウイルスデータベース ● 10-drwgatedb - SpIDer Gateデータベース ● 10-drwspamdb - アンチスパムデータベース ● 10-drwupgrade - Dr.Web Updater ● 20-drwagent - Dr.Web Agent for Windows ● 20-drwandroid11 - Dr.Web Agent for Android ● 20-drwcs - Dr.Web Server ● 20-drwunix - Dr.Web Agent for UNIX ● 40-drwproxy - Dr.Web Proxy Server ● 80-drwnews - Doctor Web ニュース
update	この製品のダウンロードを有効にします。	yes no



- **<schedule>**

定期的に更新を受信するスケジュール。この場合ユーザーはユーティリティを手動で起動する必要がなく、レポートのダウンロードは、指定した時間帯に合わせて自動実行されます。

□ `<job period="" enabled="" min="" hour="" day="" />`

ロード実行スケジュールの設定。

属性	説明	可能な値
period	ロードタスク実行の周期。	<ul style="list-style-type: none">• every_n_min - N分毎• hourly - 毎時• daily - 24時間毎• weekly - 毎週
enabled	ダウンロードタスクが有効。	yes no
min	タスクを実行するまでの分。	0~59の整数
hour	タスクを実行するまでの時間。dailyとweeklyに関連。	0~23の整数
day	タスクを実行するまでの日数。weeklyに関連。	<ul style="list-style-type: none">• mon - 月曜日• tue - 火曜日• wed - 水曜日• thu - 木曜日• fri - 金曜日• sat - 土曜日• sun - 日曜日

付録H. Dr.Web Enterprise Security Suite に含まれるプログラムのコマンドラインパラメータ

コマンドラインパラメータはデフォルト設定やその他の設定 (Server設定ファイル、Windowsレジストリ内などの設定) よりも高い優先度を持っています。起動時に指定されたパラメータがあらかじめ定数パラメータも決定する場合があります。そのような場合を以下で説明します。

異なるプログラムの、パラメータ構文を記述する際には追加部分を角括弧 [...] で囲みます。



以下の付録 H セクションに記載されている事項はAgentネットワークインストーラには当てはまりません。

コマンドラインパラメータのいくつかはスイッチの形をしています (ハイフンで始まります)。そのようなパラメータはスイッチ、またはオプションとも呼ばれます。

多くの場合、同じ意味を持つさまざまな形式でスイッチを表現できます。このため、ある論理値 (yes/no、有効/無効) を示唆するスイッチには、逆の意味を持つスイッチがあります。例えば、`-admin-rights` スwitch に対してはちょうど反対の意味を持つ対のスイッチ `-no-admin-rights` があります。このようなスイッチでは明示的な値で指定することもできます。例えば、`-admin-rights=yes` と `-admin-rights=no` です。



yesと同様の意味を持つ表現には `on`、`true`、`OK` があります。noと同様の意味を持つ表現には `off`、`false` があります。

スイッチの値にスペース、またはタブが含まれている場合、パラメータ全体が引用符内に置かれている必要があります。例えば、次のようになります。

```
"-home=c:\Program Files\DrWeb Server"
```



スイッチの名前は短縮できます (末尾の文字を省略して) が、短縮された名前が他のスイッチの始まりと一致しない場合に限られます。

コマンドライン引数がハイフンで始まる場合は、「-」(二重マイナス) 記号を使用してスイッチリストと追加の引数を区切ります。以下はそのような例です。

```
[--] initdb D:\Keys\agent.key - - <password>
```

- [--] - 分離記号です。スイッチリストの終わりであることを示し、スイッチリストと追加の引数リストを分離します。
- <password> - 追加の引数です

WindowsファミリーのOSで管理者としてコマンドを強制的に実行するには、`elevate` パラメータを使用できます。この場合、他の全てのスイッチとパラメータの前に配置する必要があります。例: `drwcsd elevate start`。



H1. ネットワークインストーラ

スタート命令フォーマット

```
drwinst.exe [<switches>]
```

スイッチ



コマンドラインスイッチは全ての種類のAgentインストールファイルの起動に使用できます。

Agentネットワークインストーラを起動するスイッチは / <switch> <parameter> のフォーマットで指定します。

パラメータ値は全てスペースの後ろに指定します。例えば、次のようになります。

```
/silent yes
```

スイッチの値にスペース、タブ、または / 記号が含まれている場合、パラメータ全体を引用符で囲ってください。例えば、次のようになります。

```
/pubkey "C:\my folder\drwcsd-certificate.pem"
```

使用可能なスイッチ

- /compression <mode> - サーバートラフィックの圧縮モードです。<mode>パラメータには次の値を指定できます。
 - yes - 圧縮を使用します。
 - no - 圧縮を使用しません。
 - possible - 圧縮を使用することが可能です。使用については、サーバー側の設定に応じて決定されます。

スイッチが指定されなかった場合、デフォルトでpossibleが使用されます。

- /encryption <mode> - サーバートラフィックの暗号化モードです。<mode>パラメータには次の値を指定できます。
 - yes - 暗号化を使用します。
 - no - 暗号化を使用しません。
 - possible - 暗号化を使用することが可能です。使用については、サーバー側の設定に応じて決定されます。

スイッチが指定されなかった場合、デフォルトでpossibleが使用されます。

- /excludeFeatures <components> - 端末上へのインストールから除外するコンポーネントのリストです。複数のコンポーネントを指定する場合は、" ,"記号を使用して区切ってください。使用可能なコンポーネントは、次のとおりです。
 - scanner - Dr.Web Scanner
 - spider-mail - SpIDer Mail



- spider-g3 – SpIDer Guard
- outlook-plugin – Dr.Web for Microsoft Outlook
- firewall – Dr.Web Firewall
- spider-gate – SpIDer Gate
- parental-control – Office Control
- antispam-outlook – Dr.Web for Microsoft OutlookコンポーネントのDr.Web Anti-spam
- antispam-spidermail – SpIDer MailコンポーネントのDr.Web Anti-spam

手動で指定されなかったコンポーネントについては、デフォルトの状態が維持されます。

- /id <station_id> – Agentがインストールされる端末の識別子を指定します。
サーバーでの自動認証を行うには、/pwd スイッチと共にパラメータを指定します。認証パラメータが設定されなかった場合、認証の決定はサーバー側で行われます。
- /includeFeatures <components> - 端末上にインストールする必要があるコンポーネントのリストです。複数のコンポーネントを指定する場合は、", "記号を使用して区切ってください。使用可能なコンポーネントは、次のとおりです。

- scanner – Dr.Web Scanner
- spider-mail – SpIDer Mail
- spider-g3 – SpIDer Guard
- outlook-plugin – Dr.Web for Microsoft Outlook
- firewall – Dr.Web Firewall
- spider-gate – SpIDer Gate
- parental-control – Office Control
- antispam-outlook – Dr.Web for Microsoft OutlookコンポーネントのDr.Web Anti-spam
- antispam-spidermail – SpIDer MailコンポーネントのDr.Web Anti-spam

手動で指定されなかったコンポーネントについては、デフォルトの状態が維持されます。

- /installdir <folder> – インストールフォルダです。
スイッチが指定されなかった場合、デフォルトでシステムドライブ上のProgram Files\DrWebフォルダにインストールされます。
- /installtimeout <time> – Control Centerから実行されたリモートインストールの際に、端末からの応答を待つ時間の上限です(秒)。
指定されなかった場合、デフォルトで300 秒になります。
- /instMode <mode> - インストーラ起動モードです。<mode>パラメータには次の値を指定できます。
 - remove – インストールされた製品を削除します。スイッチが指定されなかった場合、起動モードはデフォルトでインストーラが自動的に決定します。
- /lang <language_code> – インストーラの言語です。言語コードはISO-639-1形式で指定します。
指定されなかった場合、デフォルトでシステム言語が使用されます。
- /pubkey <certificate> - サーバー証明書へのフルパスです。
証明書が設定されなかった場合、ローカルインストールの実行後、インストーラは自動でインストーラ起動フォルダの*.pem証明書を使用します。証明書ファイルがインストーラ起動フォルダ以外にある場合は、証明書ファイルへのフルパスを手動で指定する必要があります。



Control Center内で生成されたインストールパッケージを実行する場合、証明書はインストールパッケージに含まれています。コマンドラインパラメータで証明書ファイルを指定する必要はありません。

- `/pwd <password>` – Agentがサーバーにアクセスするためのパスワード
サーバーでの自動認証を行うには、`/id`スイッチと共にパラメータを指定します。認証パラメータが設定されなかった場合、認証の決定はサーバー側で行われます。
- `/regagent <mode>` – インストールされたプログラムのリスト内にAgentを登録するかどうかを指定します。
`<mode>`パラメータには次の値を指定できます。
 - `yes` – リスト内にAgentを登録します。
 - `no` – リスト内にAgentを登録しません。スイッチが指定されなかった場合、デフォルトで`no`が使用されます。
- `/retry <number>` – マルチキャストリクエストを送信してサーバーの検索を試行する回数の上限です。指定された回数内にサーバーから応答がなかった場合、サーバーは見つからなかったと判断されます。
スイッチが指定されなかった場合、サーバーの検索試行は3回まで行われます。
- `/server [<protocol>/] <server_address>[: <port>]` – Agentのインストールが開始されるサーバーであり、インストール後にAgentが接続されるサーバーのアドレスです。
スイッチが指定されなかった場合、デフォルトでマルチキャストリクエストの送信によってサーバーを検索します。
- `/silent <mode>` – インストーラをバックグラウンドモードで実行するかどうかを指定します。`<mode>`パラメータには次の値を指定できます。
 - `yes` – インストーラをバックグラウンドモードで起動します。
 - `no` – インストーラをグラフィカルモードで起動します。スイッチが指定されなかった場合、デフォルト設定のインストーラのグラフィカルモードでAgentのインストールが実行されます(インストールマニュアルの[インストーラ経由でのDr.Web Agentのインストール](#)参照)。
- `/timeout <time>` – サーバー検索の際に応答を待つ時間の上限です(秒)。指定された値を超えるまでの時間は応答メッセージの受信を続けます。
指定されなかった場合、デフォルトで3 秒になります。

H2.Dr.Web Agent for Windows

スタート命令フォーマット

```
es-service.exe [ <switches> ]
```

スイッチ

各スイッチは以下の内いずれか1つのフォーマットで設定できます(フォーマットは同じです)。

```
- <short_switch> [ <argument> ]
```

または

```
-- <long_switch> [= <argument> ]
```

短いバージョンと長いバージョンを含み、複数のスイッチを同時に使用できます。



引数にスペースが含まれている場合は引用符で囲む必要があります。

全てのスイッチはServer上で端末に対して許可されたパーミッションに関係なく実行できます。Agent設定を変更するパーミッションがServerで拒否されている場合でも、コマンドラインスイッチを使用してそれらの設定を変更できます。

使用可能なスイッチ

- ヘルプを表示:
 - -?
 - --help
- Agentが接続するServerのアドレスを変更:
 - -e <Server>
 - --esserver=<Server>

複数のServerを同時に設定するには、スペースを使用してアドレスごとに-eスイッチを繰り返して指定します。例えば、次のようになります。

```
es-service -e 192.168.1.1:12345 -e 192.168.1.2:12345 -e 10.10.1.1:1223
```

または

```
es-service --esserver=10.3.1.1:123 --esserver=10.3.1.2:123 --  
esserver=10.10.1.1:123
```

- パブリック暗号化キーを追加:
 - -p <key>
 - --addpubkey=<key>

引数として指定されたパブリックキーはAgentフォルダ(デフォルトでは %ProgramFiles%\DrWeb フォルダ)にコピーされ、drwcsd.pub という名前に変更されて(名前が異なる場合)サービスによって再読み込みされます。この場合、既存のパブリックキーファイル(存在する場合は drwcsd.pub.old という名前に変更されません。

以前に使用されていた全てのパブリックキー(Serverから配信されてレジストリ内に保存されているもの)はそのまま使用されます。

- Server証明書を追加:
 - -c <certificate>
 - --addcert=<certificate>

引数として指定されたServer証明書ファイルはAgentフォルダ(デフォルトでは %ProgramFiles%\DrWeb フォルダ)にコピーされ、drwcsd-certificate.pem という名前に変更されて(名前が異なる場合)サービスによって再読み込みされます。この場合、既存の証明書ファイル(存在する場合は drwcsd-certificate.pem.old という名前に変更され、使用されなくなります。

以前に使用されていた全ての証明書(サーバーから配信されてレジストリ内に保存されているもの)はそのまま使用されます。



H3. Dr.Web Server

サーバーを起動するには、いくつかの方法があります。それらを別々に説明します。

[H3.1. Dr.Web Serverの管理](#)～[H3.5. Dr.Web Serverの重要なデータのバックアップ](#)に記載されているコマンドはクロスプラットフォームであり、特に別の指定がない限り、Windows OSおよびUNIX系OSのどちらでも使用できます。



サーバー管理コマンドの起動中にエラーが発生する場合は、サーバーログファイルを参照して考えられる原因を確認してください(管理者マニュアルの[Dr.Web Serverログ](#)を参照)。

H3.1. Dr.Web Serverの管理

`drwcsd [<switches>]` - サーバー操作のためのパラメータを設定します(スイッチについては以下で詳しく説明します)。

H3.2. 基本的なコマンド

- `drwcsd restart` - Serverを再起動します(`stop`、`start`のペアとして実行されます)。
- `drwcsd start` - Serverを起動します。
- `drwcsd stop` - Serverを停止します。
- `drwcsd stat` - 統計のログをファイルに記録します(CPU時間、メモリ使用量など)。UNIX系OSの場合は `send_signal WINCH`または`kill SIGWINCH`コマンドと同じです。
- `drwcsd verifykey <full_key_filename>` - ライセンスキーファイルを検証します(`agent.key`)。
- `drwcsd verifyekey <full_key_filename>` - Serverのライセンスキーファイル(`enterprise.key`)を検証します。Serverのライセンスキーファイルは、バージョン10以降は使用されません。
- `drwcsd verifyconfig <full_config_filename>` - Serverの設定ファイルのシンタックスを検証します(`drwcsd.conf`)。
- `drwcsd verifycache` - サーバーのファイルキャッシュの内容を検証します。

H3.3. データベースコマンド

データベースの初期化



初期化を実行するには、データベースが存在しない、または空である必要があります。

`drwcsd [<switches>] initdb [<license_key>|- [<sql_script>|- [<ini_file>|- [<password> [<lua_script>|-]]]]]` - データベースの初期化。

- `<license_key>` - Dr.Webのライセンスキーファイル`agent.key`へのパスです。ライセンスキーが指定されていない場合は、後でControl Centerから追加するか、サーバー間接続を介して隣接サーバーから取得する必要があります。
- `<sql_script>` - DB物理構造を初期化するSQLスクリプトへのパス。



- `<ini_file>` - 前回作成された`drweb32.ini`フォーマットのファイルで、Dr.Webソフトウェアコンポーネントの初期設定を行います(**Everyone**グループに対して)。
- `<password>` - サーバー管理者のオリジナルパスワードです(名前は**admin**)。デフォルトでは**root**です。
- `<lua_script>` - DBを初期化するLUAスクリプトへのパス(デフォルトでベースを埋める)。



「-」(マイナス)が指定された値は、このパラメータを使わないことを意味します。

続くパラメータがない場合、マイナスは省略できます。

データベース初期化のパラメータの調整

組み込みデータベースが使用されている場合、外部ファイル経由で初期化パラメータを設定できます。以下のコマンドを使用します。

```
drwcsd.exe initdbex <response-file>
```

`<response-file>` - `initdb`パラメータと同じ順序で一行ずつ記述された初期化パラメータのファイルです。

ファイルフォーマット:

```
<full_license_key_filename>
```

```
<full_sql_script_filename>
```

```
<full_ini_file_filename>
```

```
<administrator_password>
```



レスポンスファイルをWindows OS上で使用する場合は、いずれの記号も管理者パスワードに使うことができます。

特定の場合に必要なパラメータの後に続く文字列は任意になります。マイナス記号(-)のみで構成される文字列の場合、デフォルト値が使用されます(`initdb`などの場合)。

データベースの更新

`drwcsd [<switches>] updatedb <script>` - 指定されたファイルからのSQLスクリプトまたはLUAスクリプトを実行することによって、データベースのあらゆるアクション(新しいバージョンへの更新など)を実行します。

データベースのアップグレード

`drwcsd upgradedb [<folder>]` - 指定されたフォルダ(`update-db`フォルダを参照)から、または内部スクリプトを使用してデータベースの構造を新しいバージョンにアップグレードするためにサーバーを起動します。



データベースのエクスポート

- a) `drwcsd exportdb <file>` - 指定したファイルにデータベースをエクスポートします。

Windows OSの例:

```
C:\Program Files\DrWeb Server\bin\drwcsd.exe -home="C:\Program Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -verbosity=all exportdb "C:\Program Files\DrWeb Server\esbase.es"
```

UNIX系OSでは、このアクションは `drwcs:drwcs` ユーザーの代わりにディレクトリ `$DRWCS_VAR` に対して実行されます (**FreeBSD** OS以外。FreeBSDでは、デフォルトで、スクリプトが実行されたディレクトリにファイルを保存します。パスが明示的に指定されている場合、ディレクトリはインストールの際に作成された `<user>: <group>` に対して記録する権限を持つ必要があります。デフォルトでは `drwcs:drwcs` です)。

- b) `drwcsd xmlexportdb <xml_file>` - 指定したxmlファイルにデータベースをエクスポートします。

`gz` ファイル拡張子を指定した場合、エクスポート中にデータベースファイルは `gzip` アーカイブに圧縮されます。いずれの拡張子も指定しなかった場合または `gz` 以外の拡張子を指定した場合、エクスポートされたファイルはアーカイブされません。

Windows OSの例:

- データベースを圧縮せずにxmlファイルにエクスポートするには

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" "-home=C:\Program Files\DrWeb Server" "-bin-root=C:\Program Files\DrWeb Server" "-var-root=C:\Program Files\DrWeb Server\var" -verbosity=ALL -rotate=10,10m -log=export.log xmlexportdb database.db
```

- データベースをアーカイブに圧縮してxmlファイルにエクスポートするには

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" "-home=C:\Program Files\DrWeb Server" "-bin-root=C:\Program Files\DrWeb Server" "-var-root=C:\Program Files\DrWeb Server\var" -verbosity=ALL -rotate=10,10m -log=export.log xmlexportdb database.gz
```

UNIX系OSの例:

- データベースを圧縮せずにxmlファイルにエクスポートするには

```
/etc/init.d/drwcsd xmlexportdb /test/database.db
```

- データベースをアーカイブに圧縮してxmlファイルにエクスポートするには

```
/etc/init.d/drwcsd xmlexportdb /es/database.gz
```

データベースのインポート

- a) `drwcsd importdb <file>` - 指定したファイルからデータベースをインポートします (データベース内にある以前のコンテンツは削除されます)。

- b) `drwcsd upimportdb <file> [<folder>]` - 以前のバージョンのサーバーからエクスポートしたデータベースをインポートし、アップグレードします (データベース内にある以前のコンテンツは削除されます)。スクリプトでフォルダへのパスを指定して、データベースの構造を新しいバージョンにアップグレードすることもできます (`upgradedb` コマンドと同じ)。



- c) `drwcsd xmlimportdb <xml_file>` - 指定したxmlファイルからデータベースをインポートします。
- d) `drwcsd xmlupimportdb <xml_file>` - 以前のバージョンのサーバーからxml形式でエクスポートしたデータベースをインポートし、アップグレードします。スクリプトでフォルダへのパスを指定して、データベースの構造を新しいバージョンにアップグレードすることもできます(`upgradedb`コマンドと同じ)。
- e) `drwcsd xmlimportdbnh <xml_file>` - ハッシュ値を考慮せず、指定したxmlファイルからデータベースをインポートします。例えばデータベースのxmlファイルが手動で編集されている場合や、エクスポート時に自動的に書き込まれたファイルのハッシュ値が有効ではなくなった場合などに使用できます。



`upimportdb`や`xmlupimportdb`コマンドを使用する前に、データベースのバックアップを作成します。

これらコマンドの実行中に何らかの問題が発生した場合、データベースから全ての情報が削除されてしまう場合があります。

同じDBMSのみで、`upimportdb`や`xmlupimportdb`コマンドを使用してデータベースのバージョンを更新したりインポートできます。

データベースダンプのエクスポート

`drwcsd [<switches>] dumpimportdb <DB_file> [<SQL_file> [<tables_filter>]]` - 組み込みまたは外部データベースに関する詳細な情報をサーバーログファイルまたはSQLファイルに記録します。



`dumpimportdb`コマンドの実行中にはデータベースのインポートとエクスポートは行われません。

- `<DB_file>` - データベースのエクスポートファイルです。そこに格納される情報は、サーバーログファイルや`<SQL_file>`に書き込まれます。エクスポートファイルは、`exportdb`コマンドを介して取得できます。また、データベースのバックアップコピーからファイルを使用できます。`xmlexportdb`コマンド後のXMLファイルは許可されません。
- `<SQL_file>` - `<DB_file>`で指定したファイルからデータベースをインポートする間に実行される全てのSQLクエリを書き込むファイルです。SQLファイルが指定されない場合、データは(テーブルとそのフィールドのリストとして)サーバーのログファイルに書き込まれます。ファイルが指定される場合、SQLファイルへのクエリのみが書き込まれます。
- `<tables_filter>` - `<SQL_file>`に書き込まれるデータベーステーブルのリストや情報です。リスト内のテーブルは、カンマで区切る必要があります。名前は、データベーステーブルの名前に対応する必要があります。例: `admins, groups, stations`。テーブルフィルターは、SQLファイルの出力のみに適用されます。テーブルリストが指定されていない場合は、すべてのテーブルが書き込まれます。

データベースの検証

`drwcsd verifydb` - サーバーを稼働させてデータベースを確認します。結果をログファイルに記録するには、コマンドの後に`-log`キーを付ける必要があります。キーの使用の詳細は、「[H3.8. スイッチについての説明](#)」で説明されています。



データベースの動作速度の向上

`drwcsd [<switches>] speedupdb` - DBの動作速度を向上させるために、`VACUUM`、`CLUSTER`、`ANALYZE`コマンドを実行します。

データベースの修復

`drwcsd repairdb` - **SQLite3**内部データベースの破損したディスクイメージ、または**MySQL**外部データベースの破損したテーブルを修復します。

Control Centerの**SQLite3**データベース設定内で破損したイメージを自動的に修復にチェックが入っている場合、**SQLite3**はサーバーの起動時に自動的に修復される場合があります(管理者マニュアルの[データベースの復元](#)参照)。

データベースのクリーンアップ

`drwcsd cleandb` - 全てのテーブルを削除することでサーバーのデータベースをクリーンアップします。

H3.4. リポジトリコマンド



`syncrepository`、`restorerepo`、`saverepo`コマンドを実行する前にサーバーを停止する必要があります。

- `drwcsd syncrepository` - リポジトリをDr.Web GUSと同期させます。このコマンドはサーバープロセスを開始します。その際、GUSが呼び出され、更新があった場合はリポジトリ更新が行われます。
- `drwcsd rerepository` - ドライブからリポジトリを再読み込みします。UNIX系OSでは、`readrepo`コマンドに似ています。
- `drwcsd updrepository` - Dr.Web GUSからリポジトリを更新します。このコマンドは作動しているServerプロセスに信号を送ってGUSを呼び出し、更新がある場合は、次のリポジトリの更新を実行します。Serverが稼働していない場合、リポジトリの更新は行われません。
- `drwcsd [<switches>] restorerepo <full_archive_name>` - `saverepo` コマンドを使用して作成された、指定されたzipアーカイブからServerのリポジトリを復元します。
- `drwcsd [<switches>] saverepo <full_archive_name>` - Serverの全てのリポジトリを指定したzipアーカイブに保存します。作成されたアーカイブは`restorerepo`コマンドを経由してServerにインポートできます。



`restorerepo`および`saverepo`コマンドによって使用されるアーカイブは、Control Centerからのリポジトリのエクスポートとインポートに使用されるアーカイブとは異なります。



H3.5. Dr.Web Serverの重要なデータのバックアップ

以下のコマンドはクリティカルなサーバーデータのバックアップコピーを作成します(データベースコンテンツ、ライセンスキーファイル、暗号化プライベートキー、サーバー設定ファイル、Dr.Web Security Control Center設定ファイル)。

```
drwcsd -home=<path> backup [ <directory> [ <quantity> ] ]
```

- クリティカルなサーバーデータを指定された<ディレクトリ>にコピーします。
- -homeスイッチはサーバーのインストールフォルダを指定します。
- <quantity>はそれぞれのファイルのコピーの数です。

Windows OSの例:

```
C:\Program Files\DrWeb Server\bin>drwcsd -home="C:\Program Files\DrWeb Server" backup C:\a
```

データベースのコンテンツを除くバックアップの全てのファイルは、すぐに使用できます。データベースバックアップのコピーはgzipやその他のアーカイバで解凍可能な.gzフォーマットで保存されます。データベースのコンテンツはバックアップのコピーから、サーバーの別のデータベースにコピーできるので、データは復元できます([Dr.Web Enterprise Security Suiteのデータベースの復元](#)ページを参照してください)。

操作の実行中に、Dr.Web Serverは重要な情報のバックアップコピーを以下のフォルダ内に定期的に保存します。

- **Windows OS**の場合: <installation_drive>:\DrWeb Backup
- **Linux OS**の場合: /var/opt/drwcs/backup
- **FreeBSD OS**の場合: /var/drwcs/backup

バックアップを実行するために、daily taskがサーバスケジュールに含まれています。このようなタスクがスケジュールにない場合は、作成することを強く推奨します。

H3.6. Windows OS専用のコマンド

- `drwcsd [<switches>] install [<service_name>]` - サーバースerviceをシステムにインストールし、このserviceを起動するswitchを指定して割り当てます。
<service_name>は、serviceのデフォルト名の後に付けられるサフィックスです。この場合、serviceの完全な名称は「DrWebES-<service_name>」になります。installコマンドは指定された名前でserviceを作成(編集)し、自動的に-`service=<service_name>` switchをその引数に追加します。この場合、既存のserviceは変更されません。
- `drwcsd uninstall [<service_name>]` - サーバースerviceをシステムからアンインストールします。
<service_name>は、serviceのデフォルト名の後に付けられるサフィックスです。この場合、serviceの完全な名称は「DrWebES-<service_name>」になります。
- `drwcsd kill` - サーバースerviceの緊急シャットダウンを実行します(正常に終了できなかった場合)。この命令は緊急時以外には使用しないでください。
- `drwcsd reconfigure` - 設定ファイルの再読み込みと再起動を行います(新しいプロセスを開始することなく、より早く実行できます)。
- `drwcsd silent [<options>] <command>` - <command>を起動する際にサーバーからのメッセージを無効にします。特に、サーバーとの双方向性を無効にするためにコマンドファイル内で使用されます。



- `drwcsd syncads` - ネットワーク構造を同期します。コンピューターが含まれるActive Directoryコンテナが、ワークステーションの置かれるアンチウイルスネットワークグループになります。

H3.7. UNIX系OS専用のコマンド

- `drwcsd config - reconfigure`、`kill SIGHUP`コマンド同様、サーバーを再起動します。
- `drwcsd interactive` - サーバーを起動しますが、コントロールは実行しません。
- `drwcsd newkey` - 新しい暗号化キー`drwcsd.pri`と`drwcsd.pub`と`drwcsd-certificate.pem`証明書を生成します。
- `drwcsd readrepo` - ドライブからリポジトリを再読み込みします。`rerepository`コマンドと同じです。
- `drwcsd selfcert [<hostname>]` - 新しいSSL証明書(`certificate.pem`)とRSAプライベートキー(`private-key.pem`)を生成します。パラメータでは、ファイルが生成されるインストール済みのサーバーのホスト名を指定します。名前が指定されない場合、システム機能によって自動的に取得されます。
- `drwcsd shell <file_name>` - スクリプトファイルを実行します。このコマンドは`$SHELL`または`/bin/sh`を実行し、指定されたファイルに渡します。
- `drwcsd showpath` - システムに登録された全てのプログラムパスを表示します。
- `drwcsd status` - サーバーの現在の状態(起動中、停止)を表示します。

H3.8. スイッチについての説明

クロスプラットフォームなスイッチ

- `-activation-key=<license_key>` - Serverのライセンスキーです。デフォルトではルートフォルダの`etc`サブフォルダ内にある`enterprise.key`ファイルです。
Serverのライセンスキーファイルは、バージョン10以降は使用されません。`-activation-key`スイッチは以前のバージョンからのServerアップグレード中またはデータベース初期化の際に使用される場合があります。Server IDは指定されたライセンスキーから取得されます。
- `-bin-root=<folder>` - 実行ファイルへのパスです。デフォルトはルートフォルダの`bin`サブフォルダです。
- `-conf=<folder>` - Server設定ファイルの名前と場所です。デフォルトはルートフォルダの`etc`サブフォルダ内にある`drwcsd.conf`ファイルです。
- `-daemon` - Windowsプラットフォームではサービスとしての起動を意味し、UNIXプラットフォームでは「プロセスをデーモンにする」(ルートフォルダに行くために、ターミナルとの接続を切りバックグラウンドで動作します)を意味します。
- `-db-verify=on` - Server起動時にデータベースの整合性をチェックします。これはデフォルトの値です。データベースを`drwcsd verifydb`命令によってチェックした直後に起動する場合を除いては、このデフォルト値の明示的な逆の値で起動することは推奨できません。上を参照してください。
- `-help` - ヘルプを表示します。上のプログラムと同じです。
- `-hooks` - Serverに対し、Serverインストールフォルダの以下のサブフォルダにあるユーザー拡張子スクリプトの使用を許可します。
 - Windows OS: `var\extensions`
 - FreeBSD OS: `/var/drwcs/extensions`
 - Linux OS: `/var/opt/drwcs/extensions`

Serverインストールフォルダのサブフォルダに置かれています。これらのスクリプトは管理者の作業を自動化し、タスクをより速く実行できるようにします。デフォルトでは全てのスクリプトは無効です。



- `-home=<folder>` - サーバーインストールフォルダ(ルートフォルダ)。このフォルダの構造については『インストールマニュアル』の「[Dr.Web Server for Windows OSをインストールする](#)」を参照してください。デフォルトでは、起動時の現在のフォルダです。
- `-log=<log_file>` - 指定したパスのファイルへのロギングを有効にします。
UNIX系OSのServerでは、ファイル名の代わりに「-(マイナス)」記号を使用できます。これにより、ログの標準出力を指示します。
デフォルト: Windows OSでは`-var-root`スイッチにより指定されるフォルダ内の`drwcsd.log`、UNIX系OSでは、`-syslog=user`により設定されます(以下参照)。
- `-private-key=<private_key>` - Serverのプライベート暗号化キーです。デフォルトは、ルートフォルダの`etc`サブフォルダにある`drwcsd.pri`です。
- `-rotate=<N><f>, <M><u>` - Serverのログローテーションモードです。

パラメータ	説明
<code><N></code>	ログファイルの合計数(カレントログファイルおよびアーカイブを含む)
<code><f></code>	ログファイルの保存フォーマット。可能な値は次のとおりです。 <ul style="list-style-type: none"> • <code>z</code> (gzip) - ファイルを圧縮します。デフォルトで使用されます。 • <code>p</code> (plain) - ファイルを圧縮しません。
<code><M></code>	<code><u></code> 値に応じて、ログファイルのサイズまたはローテーション時間
<code><u></code>	単位、可能な値: <ul style="list-style-type: none"> • ログファイルサイズに応じてローテーションを設定する場合: <ul style="list-style-type: none"> ▫ <code>k</code> - Kb ▫ <code>m</code> - Mb ▫ <code>g</code> - Gb • 時間に応じてローテーションを設定する場合: <ul style="list-style-type: none"> ▫ <code>H</code> - 時間 ▫ <code>D</code> - 日 ▫ <code>W</code> - 週



時間に応じたローテーションが設定されている場合、同期はコマンド実行時間とは関係なく行われます。同期は、値に`H`が指定されている場合は1時間の初めに、`D`が指定されている場合は1日の初めに、`W`が指定されている場合は1週間の初め(月曜日の00:00)に、`<u>`パラメータで指定された頻度で実行されます。

基準となる日時は1年1月1日UTC+0です。

デフォルトでは`10, 10m`で、圧縮を使ってそれぞれ10メガバイトのファイルを10個保存するという意味になります。または、「ローテーションを使用しません。常に、サイズに制限のない同じファイルに書き込みます」という意味の`none`フォーマット(`-rotate=none`)を使うこともできます。

ローテーションモードではログファイルの名前は`file.<N>.log` or `file.<N>.log.dz` のようになります。`<N>`は1, 2などの連続する数です。

例として、ログファイルの名前が`file.log`(上の`-log`スイッチ参照)に設定されているとします。



- `file.log` - 現在のログファイル
- `file.1.log` - 前回のログファイル
- `file.2.log`等 - 数字が大きいほど古いバージョンのファイルです。
- `-trace` - エラーが発生した場所を特定するためのログを作成します。
- `-var-root=<folder>` - Serverが書き込み権限を持ち、変更されたファイル(ログやリポジトリファイルなど)の保存場所として指定されたフォルダへのパスです。デフォルトではルートフォルダの`var`サブフォルダです。
- `-verbosity=<level>` - ログの詳細レベルです。デフォルトはWARNINGです。許可された値は、ALL、DEBUG3、DEBUG2、DEBUG1、DEBUG、TRACE3、TRACE2、TRACE1、TRACE、INFO、NOTICE、WARNING、ERROR、CRIT です。ALL値とDEBUG3値はシノニムです。

必要に応じて、次のフォーマットで複数のメッセージソースに対して特定の詳細レベルを一度に設定することが可能です:

```
verbosity=<message_source1>
:<level1>,<message_source2>:<level2>,<message_source3>:<level3> など。この場合、
<level> は一般的な原則で継承されます(指定された詳細レベルを持つ、最も近い親ソースを探します)。
```

`-verbosity=all:all` スイッチは `-verbosity=all` スイッチと同じです ([付録K, ログファイルフォーマット](#)も参照)。



このキーは、続く`-log`キー(上参照)によって設定されるログの詳細レベルを定義します。1つの命令にこの種類のスイッチを複数含むことができます。

`-verbosity`および`-log`スイッチは相対配置です。

これらのパラメータを同時に使う場合、`-verbosity`スイッチを`-log`スイッチの前に設定します。`-verbosity`スイッチは、フォルダ内にあり次のスイッチ内で指定されるログの詳細レベルを再定義します。

Windows OSでのみ使用可能なスイッチ

- `-minimized` - (サービスとしてではなく、インタラクティブモードで起動している場合はWindowsのみ) - ウィンドウを最小化します。
- `-service=<service_name>` - このスイッチは、Serverサービスのレジストリ部のSelf-Protectionを自己識別して有効にするために、実行中のサービスプロセスにより使われます。`<service_name>`はサービスのデフォルト名の後に付けられるサフィックスです。この場合、サービスの完全な名前は「DrWebES-`<service_name>`」になります。
このスイッチは`install`コマンドで使われます。単独では使用できません。
- `-screen-size=<size>` - (サービスとしてではなく、インタラクティブモードで起動している場合はWindowsのみ) - Serverスクリーンに表示されるログの、ラインでのサイズ。デフォルトの値は1000です。

UNIX系OSでのみ使用可能なスイッチ

- `-etc=<path>` - `etc`ディレクトリへのパスです(`<var>/etc`)。
- `-keep` - Serverのインストール後に一時ディレクトリを削除しません。
- `-pid=<file>` - Serverがそのプロセス識別子を書き込むファイルです。



- `-syslog=<mode>` - システムログへのロギングを命令します。可能なモード: `auth`、`cron`、`daemon`、`kern`、`lpr`、`mail`、`news`、`syslog`、`user`、`uucp`、`local0` - `local7` (および、いくつかのプラットフォームには `ftp`、`authpriv`)



`-syslog` および `-log` キーは一緒に使用されます。Server を `-syslog` キー (例: `service drwcsd start -syslog=user`) で起動する場合、その Server は `-syslog` キーの指定された値、および `-log` キーのデフォルト値で動作します。

- `-user=<user>`、`-group=<group>` - ルートユーザーによって起動している場合に、UNIX OS でのみ使用可能です。プロセスのユーザーまたはグループを変更し、指定されたユーザー (またはグループ) のパーミッションで実行することを意味します。

H3.9. UNIX系OS専用の変数

UNIX系OSのServer管理を簡易化するために、管理者は次のフォルダのスクリプトファイル内にある変数を使用できます。

- Linux OSの場合: `/etc/init.d/drwcsd`
- FreeBSD OSの場合: `/usr/local/etc/rc.d/drwcsd`
(`/usr/local/etc/drweb.com/software/init.d/drwcsd`へのシンボリックリンク)。

表H-1は `drwcsd` の変数とそれに対応する [コマンドスイッチ](#) です。

表H-1

スイッチ	変数	デフォルトのパラメータ
<code>-home</code>	<code>DRWCS_HOME</code>	<ul style="list-style-type: none"> • FreeBSDの場合: <code>/usr/local/drwcs</code> • Linux OSの場合の場合: <code>/opt/drwcs</code>
<code>-var-root</code>	<code>DRWCS_VAR</code>	<ul style="list-style-type: none"> • FreeBSDの場合: <code>/var/drwcs</code> • Linux OSの場合の場合: <code>/var/opt/drwcs</code>
<code>-etc</code>	<code>DRWCS_ETC</code>	<code>\$DRWCS_VAR/etc</code>
<code>-rotate</code>	<code>DRWCS_ROT</code>	<code>10,10m</code>
<code>-verbosity</code>	<code>DRWCS_LEV</code>	<code>info</code>
<code>-log</code>	<code>DRWCS_LOG</code>	<code>\$DRWCS_VAR/log/drwcsd.log</code>
<code>-conf</code>	<code>DRWCS_CFG</code>	<code>\$DRWCS_ETC/drwcsd.conf</code>
<code>-pid</code>	<code>DRWCS_PID</code>	
<code>-user</code>	<code>DRWCS_USER</code>	
<code>-group</code>	<code>DRWCS_GROUP</code>	
<code>-hooks</code>	<code>DRWCS_HOOKS</code>	

スイッチ	変数	デフォルトのパラメータ
-trace	DRWCS_TRACE	



DRWCS_HOOKSおよびDRWCS_TRACEの変数にはパラメータはありません。変数が定義されている場合は、スクリプト実行時に相当するスイッチが追加されます。変数が定義されていない場合、スイッチは追加されません。

表H-2はその他の変数です。

表H-2

変数	デフォルトのパラメータ	説明
DRWCS_ADDOPT		起動時にdrwcsdに対して送られる追加のコマンドライン命令
DRWCS_CORE	無制限	コアファイルの最大サイズ
DRWCS_FILES	131170	Serverが開くことのできるファイル記述子の最大数
DRWCS_BIN	\$DRWCS_HOME/bin	drwcsdを起動するディレクトリ
DRWCS_LIB	\$DRWCS_HOME/lib	Serverライブラリのあるディレクトリ

drwcsdスクリプト内でこれらの変数が設定されていない場合は、パラメータのデフォルト値が使われます。



DRWCS_HOME、DRWCS_VAR、DRWCS_ETC、DRWCS_USER、DRWCS_GROUP、DRWCS_HOOKS変数はすでにdrwcsdスクリプトファイル内で定義されています。

/var/opt/drwcs/etc/common.conf ファイルが存在する場合、このファイルはdrwcsdに含まれ、いくつかの変数を再定義できます。ただし、それらがエクスポートされていない場合 (exportコマンドを使用して) は、何の影響も与えません。

変数を設定するには

1. drwcsdスクリプトファイルに変数の定義を追加します。
2. exportコマンドを使用して、この変数をエクスポートします (同じ場所)。
3. このスクリプトからもう1つのプロセスを実行する際、そのプロセスは設定された値を読み込みます。

H3.10. UNIX OS向けDr.Web Serverの、kill命令を使用した管理

UNIX向けServerはkillユーティリティがServerプロセッサに送るシグナルによって管理されます。



killユーティリティに関するヘルプを受け取るには`man kill`命令を使用します。

以下はユーティリティシグナルと、それによって実行されるアクションのリストです。

- SIGWINCH - 統計のログをファイルに作成 (CPU時間、メモリの使用量など) します。
- SIGUSR1 - ドライブからリポジトリを再読み込みします。
- SIGUSR2 - ドライブからテンプレートを再読み込みします。
- SIGHUP - Serverを再起動します。
- SIGTERM - Serverをシャットダウンします。
- SIGQUIT - Serverをシャットダウンします。
- SIGINT - Serverをシャットダウンします。

WindowsバージョンのServerに対する`drwcsd`命令のスイッチによっても同様のアクションが実行されます。付録 [H3.3. データベースコマンド](#)を参照してください。

H4. Dr.Web Scanner for Windows

ワークステーションソフトウェアのこのコンポーネントには、『**Dr.Web Agent for Windows**ユーザーマニュアル』に記載されているコマンドラインパラメータがあります。唯一違う点として、ScannerがAgentによって実行される場合、`/go /st`パラメータは失敗することなく自動的にサーバーに送信されます。

H5. Dr.Web Proxy Server

Proxy Serverのパラメータを設定するには、Proxy Serverインストールディレクトリの`bin`サブディレクトリにある`drwcsd-proxy`実行ファイルを該当するスイッチで実行してください。

スタート命令フォーマット

```
drwcsd-proxy [ <switches> ] [ <commands> [ <command_arguments> ] ]
```

使用可能なスイッチ

クロスプラットフォームなスイッチ

- `--console=yes|no` - Proxy Serverをインタラクティブモードで実行します。このとき、Proxy Serverの動作ログがコンソールに書き込まれます。
デフォルト: `no`
- `--etc-root=<path>` - 設定ファイルディレクトリへのパス (`drwcsd-proxy.conf` `drwcsd.proxy.auth` など) です。
デフォルト: `$var/etc`
- `--home=<path>` - Proxy Serverインストールディレクトリへのパスです。
デフォルト: `$exe-dir/`



- `--log-root=<path>` - Proxy Server動作ログファイルが置かれているディレクトリへのパスです。
デフォルト:`$var/log`
- `--pool-size <N>` - クライアント接続のプールサイズです。
デフォルト: Proxy Serverがインストールされているコンピューターのコア数(2未満にはなりません)。
- `--rotate=<N><f>, <M><u>` - Proxy Serverのログローテーションモードです。

パラメータ	説明
<code><N></code>	ログファイルの合計数(カレントログファイルおよびアーカイブを含む)
<code><f></code>	ログファイルの保存フォーマット。可能な値は次のとおりです。 <ul style="list-style-type: none"> • z (gzip) - ファイルを圧縮します。デフォルトで使用されます。 • p (plain) - ファイルを圧縮しません。
<code><M></code>	<code><u></code> 値に応じて、ログファイルのサイズまたはローテーション時間
<code><u></code>	単位、可能な値: <ul style="list-style-type: none"> • ログファイルサイズに応じてローテーションを設定する場合: <ul style="list-style-type: none"> ▫ k - Kb ▫ m - Mb ▫ g - Gb • 時間に応じてローテーションを設定する場合: <ul style="list-style-type: none"> ▫ H - 時間 ▫ D - 日 ▫ W - 週



時間に応じたローテーションが設定されている場合、同期はコマンド実行時間とは関係なく行われます。同期は、値にHが指定されている場合は1時間の初めに、Dが指定されている場合は1日の初めに、Wが指定されている場合は1週間の初め(月曜日の00:00)に、`<u>`パラメータで指定された頻度で実行されます。

基準となる日時は1年1月1日UTC+0です。

デフォルトは10,10mで、圧縮を使ってそれぞれ10メガバイトのファイルを10個保存するという意味になります。

- `--trace=[yes/no]` - Proxy Server呼び出しの詳細なロギングを有効にします。Proxy Serverがコールスタックのトレースをサポートしている場合にのみ利用できます(例外が発生した場合は、スタックがログに書き込まれます)。
デフォルト:`no`
- `--tmp-root=<path>` - 一時ファイルディレクトリへのパスです。Proxy Serverの自動更新で使用されます。
デフォルト:`$var/tmp`
- `--var-root=<path>` - キャッシュとデータベースを格納するためのProxy Serverの作業ディレクトリへのパスです。
デフォルト:
 - Windows OSの場合:`%ALLUSERSPROFILE%\Doctor Web\drwcs`



- Linux OSの場合: /var/opt/drwcs
- FreeBSD OSの場合: /var/drwcs
- `--verbosity=<details_level>` - ログの詳細レベルです。デフォルトはTRACEです。可能な値は、ALL、DEBUG3、DEBUG2、DEBUG1、DEBUG、TRACE3、TRACE2、TRACE1、TRACE、INFO、NOTICE、WARNING、ERROR、CRITです。ALL値とDEBUG3値はシノニムです。

必要に応じて、次のフォーマットで複数のメッセージソースに対して特定の詳細レベルを一度に設定することが可能です:

```
verbosity=<message_source1>
: <level1>, <message_source2>: <level2>, <message_source3>: <level3> など。この場合、
<level> は一般的な原則で継承されます(指定された詳細レベルを持つ、最も近い親ソースを探します)。-
verbosity=all:all スイッチは -verbosity=all スイッチと同じです(付録K. ログファイルフォーマット
も参照)。
```



Proxy Serverのパラメータを設定するためのスイッチは全て、同時にセットすることが可能です。

UNIX系OSで使用可能なスイッチ

- `--user` - ユーザーIDを設定します。このスイッチは通常モードとデーモンモードの両方に関連します。
- `--group` - グループIDを設定します。このスイッチは通常モードとデーモンモードの両方に関連します。
- `--pid=<path>` - プロセス識別子のあるディレクトリへのパスです。

デフォルト: /var/opt/drwcs/run/drwcsd-proxy.pid

使用可能なコマンドと引数



コマンドが指定されていない場合は、runコマンドが使用されます。

- `import <path> [<revision>] [<products>]` - Dr.Web ServerリポジトリからProxy Serverのキャッシュファイルをインポートします。
 - `<path>` - Dr.Web Serverリポジトリが入ったディレクトリへのパスです。Serverリポジトリは、Proxy Serverがインストールされたコンピューターに事前にダウンロードしておく必要があります。
 - `<revision>` - インポートするリビジョンの最大数。値が設定されていない場合は、全てのリビジョンがインポートされます。
 - `<products>` - スペースで区切られた、インポートする製品のリスト。デフォルトではリストは空です。つまり、Dr.Web Serverを除く全てのリポジトリ製品をインポートします。リストが設定されている場合は、リストの製品のみがインポートされます。
- `help` - Proxy Server設定のスイッチに関するヘルプメッセージを表示します。
- `run` - Proxy Serverを通常モードで開始します。

Windows OSのみ

- `install` - サービスをインストールします。



- `start` - インストールされているサービスを開始します。
- `stop` - 開始されたサービスを停止します。
- `uninstall` - サービスをアンインストールします。

UNIX系OSでのみ使用可能なコマンド:

- `daemon` - Proxy Serverをデーモンとして実行します ([UNIX系OSで使用可能なスイッチ](#)も参照してください)。

UNIX系OSで使用可能なプロキシサーバー制御スクリプトと変数

UNIX系OSのProxy Server管理を簡易化するために、管理者は次のフォルダの`drwcsd-proxy.sh`スクリプトファイル内にある変数を使用できます。

- **Linux**: `/etc/init.d/dwcp_proxy`
- **FreeBSD**: `/usr/local/etc/rc.d/dwcp_proxy`

スクリプトには次のコマンドを使用することができます。

- `import <path> [<revision>] [<products>]` - Dr.Web ServerリポジトリからProxy Serverのキャッシュファイルをインポートします (Proxy Serverのコマンドと同様。上記参照)。
- `interactive` - Proxy Serverをインタラクティブモードで実行します。この場合、Proxy Serverの動作ログがコンソールに書き込まれます。
- `start` - Proxy Serverをデーモンとして実行します。
- `status` - デーモンが起動されているかどうかをチェックします。
- `stop` - 起動されたデーモンを停止します。

表H-3は`drwcsd-proxy`の変数とそれに対応するコマンドスイッチです。

表H-3

スイッチ	変数	デフォルトのパラメータ
<code>--home=<path></code>	<code>\$DRWCS_PROXY_HOME</code>	<code>\$exe-dir/</code>
<code>--var-root=<path></code>	<code>\$DRWCS_PROXY_VAR</code>	<ul style="list-style-type: none"> • Linux OSの場合: <code>/var/opt/drwcs</code> • FreeBSD OSの場合: <code>/var/drwcs</code>
<code>--etc-root=<path></code>	<code>\$DRWCS_PROXY_ETC</code>	<code>\$var/etc</code>
<code>--tmp-root=<path></code>	<code>\$DRWCS_PROXY_TMP</code>	<code>\$var/tmp</code>
<code>--log-root=<path></code>	<code>\$DRWCS_PROXY_LOG</code>	<code>\$var/log</code>
-	<code>\$DRWCS_PROXY_LIB</code>	<code>\$DRWCS_PROXY_HOME/lib</code>
-	<code>\$DRWCS_PROXY_BIN</code>	<code>\$DRWCS_PROXY_HOME/bin</code>
<code>--verbosity=<details_level></code>	<code>\$DRWCS_PROXY_VERBOSITY</code>	INFO



スイッチ	変数	デフォルトのパラメータ
>		
--rotate=<N><f>,<M><u>	\$DRWCS_PROXY_ROTATE	10,10m
--pid	\$DRWCS_PROXY_PID	/var/opt/drwcs/run/drwcsd-proxy.pid
-	\$NO_DRWCS_PROXY_USER	値が割り当てられている場合、\$DRWCS_PROXY_USERは無視されます。
-user	\$DRWCS_PROXY_USER	-
-	\$NO_DRWCS_PROXY_GROUP	値が割り当てられている場合、\$DRWCS_PROXY_GROUPは無視されます。
--group	\$DRWCS_PROXY_GROUP	-
-	\$DRWCS_PROXY_FILES	131170(現在の制限以上)

H6.UNIX系OS向けDr.Web Serverインストーラ

スタート命令フォーマット

```
<package_name>.run [ <switches> ] [--] [ <arguments> ]
```

ここで:

- [--] - オプションの区切り記号で、スイッチリストの終わりを決定し、スイッチリストと追加の引数リストを区切ります。
- [<arguments>] - 追加の引数または埋め込まれたスクリプト

パッケージに関するヘルプまたは情報を取得するスイッチ

- --help - スイッチに関するヘルプを表示します。
- --info - パッケージに関する詳細な情報を表示します(名前、保存先フォルダ、解凍後のサイズ、圧縮アルゴリズム、圧縮日付、パッキングに使用されたmakeselfのバージョン、パッキングのコマンドユーザー、解凍後に実行されるスクリプト、アーカイブのコンテンツが一時フォルダにコピーされるかどうか(コピーされない場合は何も表示されません)、保存先フォルダがスクリプト実行後も保存されるかまたは削除されるか)。
- --list - インストールパッケージ内のファイルのリストを表示します。
- --check - インストールパッケージの整合性をチェックします。

パッケージを実行するスイッチ

- --confirm - 埋め込まれたスクリプトを実行する前に尋ねます。



- `--noexec` - 埋め込まれたスクリプトを実行しません。
- `--target <folder>` - インストールパッケージを指定されたフォルダに抽出します。
- `--tar <argument_1> [<argument_2> ...]` - tarコマンド経由でインストールパッケージのコンテンツにアクセスします。

追加の引数

- `--help` - 追加の引数に関するヘルプを表示します。
- `--quiet` - インストーラをバックグラウンドモードで起動します。インストーラの以下の全ての質問に対して肯定的な回答が使用されます。
 - 使用許諾契約に同意する
 - バックアップをデフォルトフォルダ内に設定する
 - システム内にインストールされたエクストラ・ディストリビューションキットが削除される場合にインストールを続行する
- `--clean` - 前回のインストールで使用した設定をバックアップから復元せずに、パッケージをサーバーのデフォルト設定でインストールします。
- `--preseed <path>` - インストール中にインストーラによって表示される質問に対するあらかじめ設定された回答が含まれた設定ファイルへのパスです。

設定ファイル内のあらかじめ設定された回答を指定する変数:

- `DEFAULT_BACKUP_DIR=<path>` - 前回のバージョンでの設定を復元する際に使用するバックアップへのパスです(バックアップからの復元を適用せずにインストールを行うよう設定した場合は使用されません)。
- `QUIET_INSTALL=[0|1]` - インストーラのバックグラウンドモードの使用を定義します。
 - 0 - インストーラをバックグラウンドモードで起動します。
 - 1 - インストーラを通常モードで起動します。
- `CLEAN_INSTALL=[0|1]` - インストール中のバックアップの使用を定義します。
 - 0 - バックアップを適用せずにインストールを行います。
 - 1 - `DEFAULT_BACKUP_DIR`変数のフォルダにあるバックアップからリストアを適用してインストールを行います。`DEFAULT_BACKUP_DIR`変数が指定されていない場合、`/var/tmp/drwcs`からのバックアップとなります。
- `ADMIN_PASSWORD=<password>` - デフォルト管理者アカウント(**admin**)のパスワードです。
 - ファイル内で`ADMIN_PASSWORD`変数が指定されている場合は、その値が管理者パスワードとして使用され、インストールの最後に次のメッセージが表示されます。
デフォルト管理者(admin)の設定ファイルで指定されたパスワード: `<password>`
 - ファイル内で`ADMIN_PASSWORD`変数が指定されていない場合は、パスワードが自動的に生成され、インストールの最後に次のメッセージが表示されます。
自動的に生成されたデフォルト管理者(admin)のパスワード: `<password>`



`--preseed`引数を使用し、設定ファイル内で`QUIET_INSTALL=0`変数を使用してインストーラのバックグラウンドモードを定義しない場合、設定ファイルの別の変数の値がインストール中にユーザーによって再定義されます。



H7. ユーティリティ

H7.1. デジタルキーおよび証明書生成ユーティリティ

次のコンソールバージョンのデジタルキーおよび証明書生成ユーティリティが提供されています。

実行ファイル	位置情報	説明
<code>drweb-sign-<i><OS></i>-<i><bitness></i></code>	Control Center、管理 → ユーティリティ セクション webmin/utilities Serverディレクトリ	個々のバージョンのユーティリティ。任意のディレクトリから、または対応するオペレーティングシステムが搭載されたコンピュータで起動できます。
<code>drwsign</code>	bin Serverディレクトリ	ユーティリティのバージョンはサーバーのライブラリに依存します。保存先のディレクトリからのみ起動できます。



`drweb-sign-<OS>-<bitness>`と`drwsign`のバージョンのユーティリティは機能が似ています。さらにこのセクションでは、`drwsign`のバージョンが示されていますが、全ての例が両バージョンに関連しています。

スタート命令フォーマット

- `drwsign check [-public-key=<public_key>] <file>`

このファイルに署名をした人物のパブリックキーとして使用し、特定のファイル署名をチェックします。

スイッチパラメータ	デフォルト値
<code><i><public_key></i></code>	<code>drwcsd.pub</code>

- `drwsign extract [-private-key=<private_key>] [-cert=<Server_certificate>] <public_key>`

プライベートキーファイルまたは証明書からパブリックキーを抽出し、指定したファイルにパブリックキーを書き込みます。

`-private-key`スイッチと`-cert`スイッチはどちらか1つのスイッチのみしか指定できず、互いに排他的なものになっており、両方のスイッチが同時に指定される場合、コマンドは実行に失敗します。

スイッチパラメータは、必ず指定する必要があります。

いずれのスイッチも設定されない場合、`drwcsd.pri`プライベートキーのパブリックキーの抽出には`-private-key=drwcsd.pri`が使用されます。

スイッチパラメータ	デフォルト値
<code><i><private_key></i></code>	<code>drwcsd.pri</code>

- `drwsign genkey [<private_key>] [<public_key>]`



パブリックキーとプライベートキーのペアを作成し、該当するファイルにそれらの記録を作成します。

スイッチパラメータ	デフォルト値
<private_key>	drwcsd.pri
<public_key>	drwcsd.pub



Windowsプラットフォーム向けバージョンのユーティリティでは (UNIXバージョンと異なり)、プライベートキーのコピーは防止されません。

- `drwsign gencert [-private-key=<private_key>] [-subj=<subject_fields>] [-days=<validity_period>] [<self_signed_certificate>]`

Serverのプライベートキーを使用して自己署名済みの証明書を生成し、対応するファイルに書き込みます。

スイッチパラメータ	デフォルト値
<private_key>	drwcsd.pri
<subject_fields>	/CN=<hostname>
<validity_period>	3560
<self_signed_certificate>	drwcsd-certificate.pem

- `drwsign gencsr [-private-key=<private_key>] [-subj=<subject_fields>] [<certificate_sign_request>]`

プライベートキーに基づいた証明書の署名へのリクエストを生成し、そのリクエストを対応するファイルに書き込みます。

例えば、Dr.Web ServerキーでDr.Web Proxy Server証明書に署名するなど、別のServerの証明書への署名に使用できます。

そのようなリクエストに署名するには、`signcsr`スイッチを使用します。

スイッチパラメータ	デフォルト値
<private_key>	drwcsd.pri
<subject_fields>	/CN=<hostname>
<certificate_sign_request>	drwcsd-certificate-sign-request.pem

- `drwsign genselfsign [-show] [-subj=<subject_fields>] [-days=<validity_period>] [<private_key> [<self_signed_certificate>]]`

Webサーバー用の自己署名済みRSA証明書とRSAプライベートキーを生成し、対応するファイルに書き込みます。

`-show`スイッチでは、読み取り可能な表示で証明書の内容を印刷します。



スイッチパラメータ	デフォルト値
<subject_fields>	/CN=<hostname>
<validity_period>	3560
<private_key>	private-key.pem
<self_signed_certificate>	certificate.pem

- `drwsign hash-check [-public-key=<public_key>] <hash_file> <sign_file>`

クライアントサーバーの Protokol 形式で指定された256ビットの数値の署名を確認します。

<hash-file>では、署名する256ビットの数値のファイルが指定されます。<sign_file>は署名結果になります (256ビットの数値 x 2)

スイッチパラメータ	デフォルト値
<public_key>	drwcsd.pub

- `drwsign hash-sign [-private-key=<private_key>] <hash_file> <sign_file>`

クライアントサーバーの Protokol 形式で指定された256ビットの数値に署名します。

<hash-file>では、署名する256ビットの数値のファイルが指定されます。<sign_file>は署名結果になります (256ビットの数値 x 2)

スイッチパラメータ	デフォルト値
<private_key>	drwcsd.pri

- `drwsign help [<comand>]`

プログラムまたはコマンドラインフォーマットの特定のコマンドに関する簡単なヘルプ。

- `drwsign sign [-private-key=<private_key>] <file>`

プライベートキーを使用して、<file>に署名します。

スイッチパラメータ	デフォルト値
<private_key>	drwcsd.pri

- `drwsign signcert [-ca-key=<private_key>] [-ca-cert=<Server_certificate>] [-cert=<certificate_to_sign>] [-days=<validity_period>] [<signed_certificate>]`

Serverのプライベートキーと証明書で既存の<certificate_to_sign>に署名します。署名した証明書は別のファイルに保存されます。

Dr.Web ServerキーによるDr.Web Proxy Server証明書への署名に使用できます。

スイッチパラメータ	デフォルト値
<private_key>	drwcsd.pri
<Server_certificate>	drwcsd-ca-cerificate.pem



スイッチパラメータ	デフォルト値
<certificate_to_sign>	drwcsd-certificate.pem
<validity_period>	3560
<signed_certificate>	drwcsd-signed-certificate.pem

- `drwsign signcsr [-ca-key=<private_key>] [-ca-cert=<Server_certificate>] [-csr=<certificate_sign_request>] [-days=<validity_period>] [<signed_certificate>]`

Serverプライベートキーと証明書を使用して、`genscr`コマンドで生成された<certificate_sign_request>に署名します。署名した証明書は別のファイルに保存されます。

例えば、Dr.Web ServerキーでDr.Web Proxy Server証明書に署名するなど、別のServerの証明書への署名に使用できます。

スイッチパラメータ	デフォルト値
<private_key>	drwcsd.pri
<Server_certificate>	drwcsd-certificate.pem
<certificate_sign_request>	drwcsd-certificate-sign-request.pem
<validity_period>	3560
<signed_certificate>	drwcsd-signed-certificate.pem

- `drwsign tlsticketkey [<TLS_ticket>]`

TLS_ticket を生成します。

共有TLSセッションのServerクラスタで使用できます。

スイッチパラメータ	デフォルト値
<TLS_ticket>	tickets-key.bin

- `drwsign verify [-ss-cert] [-CAfile=<Server_certificate>] [<certificate_to_check>]`

信頼できるServer証明書によって証明書を検証します。

-ss-certスイッチでは、信頼できる証明書を無視し、自己署名した証明書のみを検証します。

スイッチパラメータ	デフォルト値
<Server_certificate>	drwcsd-certificate.pem
<certificate_to_check>	drwcsd-signed-certificate.pem

- `drwsign x509dump [<certificate_to_print>]`

任意のx509証明書のダンプを印刷します。



スイッチパラメータ	デフォルト値
<code><certificate_to_print></code>	<code>drwcsd-certificate.pem</code>

H7.2. 内部データベースの管理ユーティリティ

次の内部DBの管理ユーティリティが提供されています。

- `drwidbsh` - IntDBデータベース用
- `drwidbsh3` - SQLite3データベース用

内部DBの管理ユーティリティは以下のフォルダ内にあります。

- **Linux OS:** `/opt/drwcs/bin`
- **FreeBSD OS:** `/usr/local/drwcs/bin`
- **Windows OS:** `<Server_installation_folder>\bin`
(デフォルトでは、Serverのインストールフォルダは `C:\Program Files\DrWeb Server` です)。

スタート命令フォーマット

```
drwidbsh <full_DB_filename>
```

または

```
drwidbsh3 <full_DB_filename>
```

このプログラムはテキストダイアログモードで動作し、ユーザーからの命令を待ちます(命令はピリオドで始まります)。

他の命令に関するヘルプを受け取る場合は `.help` と入力します。

詳細については、SQL言語についてのリファレンスマニュアルを参照してください。

H7.3. Dr.Web Serverリモート診断ユーティリティ

Dr.Web Serverリモート診断ユーティリティを使うと、動作に関する統計を管理・確認するためにリモートでDr.Web Serverに接続できます。ユーティリティのグラフィカルバージョンはWindows OSでのみ使用可能です。

このユーティリティはControl Center経由でダウンロードできます。メインメニューで **管理** を選択し、コントロールメニューで **ユーティリティ** を選択してください。

- Windows OSの場合 - グラフィカルバージョン。
- UNIX系OSの場合 - コンソールバージョン。

次のバージョンのDr.Web Serverリモート診断ユーティリティが提供されています。

実行ファイル	位置情報	説明
<code>drweb-cntl-<OS>-<bitness></code>	Control Center、管理 → ユーティリティ セクション	個々のバージョンのユーティリティ。任意のディレクトリから、または対応するオペレーティング



実行ファイル	位置情報	説明
	webmin/utilities Serverディレクトリ	システムが搭載されたコンピューターで起動できます。
drwcntl	bin Serverディレクトリ	ユーティリティのバージョンはサーバーのライブラリに依存します。保存先のディレクトリからのみ起動できます。



drweb-cntl- <OS>-<bitness>とdrwcntlのバージョンのユーティリティは機能が似ています。さらにこのセクションでは、drwcntlのバージョンが示されていますが、全ての例が両バージョンに関連しています。



Serverリモート診断ユーティリティに接続するには、Dr.Web Server FrontDoorプラグインを有効にする必要があります。これを行うには、**Dr.Web Server設定** セクションの **モジュール** タブで、**Dr.Web Server FrontDoorプラグイン** フラグを設定します。

Serverリモート診断ユーティリティに接続するには、ユーティリティ経由で接続する管理者が **追加機能を使用** 権限を持っている必要があります。そうでない場合、リモート診断ユーティリティ経由でServerにアクセスすることはできません。

TLSを使用したユーティリティの接続では(グラフィカルとコンソールの両方)、Serverアドレスを設定するときに次のようにプロトコルを直接指定する必要があります: `ssl:// <IPアドレスまたはDNS名>`。

Dr.Web Serverリモート診断ユーティリティへのServerの接続設定については、[管理者マニュアルのDr.Web Serverのリモートアクセス](#)を参照してください。

ユーティリティのコンソールバージョン

スタート命令フォーマット

```
drwcntl [-?|-h|--help] [+<log_file>] [<server> [<login> [<password>]]]
```

ここで:

- `-? -h --help` - ユーティリティ使用のコマンドに関するヘルプを表示します。
- `<log_file>` - ユーティリティの全ての動作を指定されたパスにあるログファイル内に記録します。
- `<server>` - ユーティリティが接続するServerのアドレスの文字列を `[(tcp|ssl)://] <IP address or DNS name>[: <port>]` のフォーマットで指定します。

サポートされているいずれかのプロトコルを介して接続するには、以下の条件を満たしている必要があります。

- a) `ssl` を介して接続する場合、`frontdoor.conf` 設定ファイル内で `<ssl />` タグを設定する必要があります。このとき、接続は `ssl` のみを介して確立できます。
- b) `tcp` を介して接続する場合、`frontdoor.conf` 設定ファイル内で `<ssl />` タグが無効(コメント)になっている必要があります。このとき、接続は `tcp` のみを介して確立できます。

サーバーアドレスの文字列内で接続パラメータが設定されていない場合、以下の値が使用されます。

パラメータ	デフォルト値
接続プロトコル	tcp  TCP接続では、Control Centerの管理 → Dr.Web Server へのリモートアクセス セクション内で TLS を使用 フラグのチェックが外れている必要があります。これにより、 <code>frontdoor.conf</code> 設定ファイル内の <code><ssl /></code> タグが無効になります。
ServerのIPアドレス またはDNS名	Serverアドレスを該当するフォーマットで指定するようユーティリティによって促されます。
ポート	10101  Serverでは、許可されたポートは、 Dr.Web Server リモートアクセス セクションで設定され、 <code>frontdoor.conf</code> 設定ファイルに保存されます。このセクションで別のポートが使用される場合、ユーティリティを接続する際にこのポートを直接設定する必要があります。

- `<login>` - Server管理者のログインです。
- `<password>` - Serverにアクセスするための管理者パスワードです。

接続文字列内で管理者のログインとパスワードが指定されていない場合、該当する認証情報を指定するようユーティリティによって要求されます。

可能なコマンド

- `cache <operation>` - ファイルキャッシュに対する操作です。特定の操作を行うには以下のコマンドを使用します。
 - `clear` - ファイルキャッシュをクリアします。
 - `list` - 全てのファイルキャッシュの内容を表示します。
 - `matched <regular expression>` - 指定された正規表現に合致するファイルキャッシュの内容を表示します。
 - `maxfilesize [<size>]` - プリロードされたファイルオブジェクトの最大サイズを表示、設定します。追加のパラメータなしで実行された場合は現在のサイズが表示されます。サイズを設定するには、コマンド名の後に必要なサイズをバイト単位で指定します。
 - `statistics` - ファイルキャッシュの使用に関する統計を表示します。
- `calculate <function>` - 指定されたシーケンスを計算します。特定のシーケンスを計算するには、以下のコマンドを使用します。
 - `hash [<standard>] [<string>]` - 指定された文字列のハッシュを計算します。特定の規格を設定するには以下のコマンドを使用します。
 - `gost` - 指定された文字列のハッシュをGHOST規格に従って計算します。
 - `md5` - 指定された文字列のmd5ハッシュを計算します。
 - `sha` - 指定された文字列のハッシュをSHA規格に従って計算します。



- SHA1 - 指定された文字列のハッシュをSHA1規格に従って計算します。
- sha224 - 指定された文字列のハッシュをSHA224規格に従って計算します。
- sha256 - 指定された文字列のハッシュをSHA256規格に従って計算します。
- sha384 - 指定された文字列のハッシュをSHA384規格に従って計算します。
- sha512 - 指定された文字列のハッシュをSHA512規格に従って計算します。
- hmac [*<standard>*] [*<string>*] - 指定された文字列のHMACを計算します。特定の規格を設定するには、以下のコマンドを使用します。
 - md5 - 指定された文字列をHMAC-MD5で計算します。
 - sha256 - 指定された文字列をHMAC-SHA256で計算します。
- random - ランダムな数値を生成します。
- uuid - 一意の識別子を算出します。
- clients *<operation>* - 情報を取得し、Serverに接続されたクライアントを管理します。特定の機能についての情報を取得するには、以下のコマンドを使用します。
 - addresses [*<regular expression>*] - 指定された正規表現に合致する端末のネットワークアドレスを表示します。正規表現が指定されていない場合は全ての端末のアドレスが表示されます。
 - caddresses [*<regular expression>*] - 指定された正規表現に合致する端末のIPアドレス数を表示します。正規表現が指定されていない場合は全ての端末の数が表示されます。
 - chosts [*<regular expression>*] - 指定された正規表現に合致する端末のコンピューター名の数を表示します。正規表現が指定されていない場合は全ての端末の数が表示されます。
 - cids [*<regular expression>*] - 指定された正規表現に合致する端末識別子の数を表示します。正規表現が指定されていない場合は全ての端末の数が表示されます。
 - cnames [*<regular expression>*] - 指定された正規表現に合致する端末名の数を表示します。正規表現が指定されていない場合は全ての端末の数が表示されます。
 - disconnect [*<regular expression>*] - 指定された正規表現に合致する識別子を持つ端末とのアクティブな接続を切断します。正規表現が指定されていない場合は、接続されている全ての端末との接続が切断されます。
 - enable [*<mode>*] - Serverでのクライアントの接続許可モードを表示、設定します。モードを設定するには、次のコマンドを使用します。追加のパラメータなしに実行された場合、現在のモードが表示されます。
 - on - 全てのクライアント接続を許可します。
 - off - 全てのクライアント接続を拒否します。
 - hosts *<regular expression>* - 指定された正規表現に合致する端末のコンピューター名の数を表示します。
 - ids *<regular expression>* - 指定された正規表現に合致する端末識別子を表示します。
 - names *<regular expression>* - 指定された正規表現に合致する端末名を表示します。
 - online *<regular expression>* - 指定された正規表現に合致する識別子、名前、またはアドレスを持った端末のオンライン時間を表示します。オンライン時間は最後に端末がServerに接続された瞬間から開始されます。
 - statistics *<regular expression>* - 指定された正規表現に合致するクライアントの数に関する統計を表示します。
 - traffic *<regular expression>* - 現在接続されている、指定された正規表現に合致するクライアントのトラフィック情報を表示します。
- core - Serverプロセスダンプを書き込みます。



- `cpu <parameter>` - ServerがインストールされているコンピューターのCPU使用率に関する統計を表示します。特定のパラメータを要求するには以下のコマンドを使用します。
 - `clear` - 蓄積された統計データを全て削除します。
 - `day` - 当日のCPU使用率のグラフを表示します。
 - `disable` - CPU使用率のモニタリングを無効にします。
 - `enable` - CPU使用率のモニタリングを有効にします。
 - `hour` - 現在の時間のCPU使用率のグラフを表示します。
 - `load` - 平均CPU使用率を表示します。
 - `minute` - 過去1分間のCPU使用率のグラフを表示します。
 - `rawd` - 当日のCPU使用率に関する統計値を表示します。
 - `rawh` - 過去1時間のCPU使用率に関する統計値を表示します。
 - `rawl` - 平均CPU使用率に関する統計値を表示します。
 - `rawm` - 過去1分間のCPU使用率に関する統計値を表示します。
 - `status` - CPU使用率のモニタリング状況を表示します。
- `debug <parameter>` - 設定をデバッグします。特定のパラメータを設定するには、追加コマンドを使用します。追加コマンドのリストを絞り込むには、? `debug`コマンドでヘルプを呼び出すことができます。



`debug signal`コマンドはUNIX系OS環境のServerでのみ使用可能です。

- `die` - Serverを停止し、Serverプロセスダンプを書き込みます。



`die`コマンドはUNIX系OS環境のServerでのみ使用可能です。

- `dwcp <parameter>` - Dr.Web Control Protocol (Server、Agent、Agentインストーラプロトコルを含む) オプションを設定、表示します。可能なパラメータは次のとおりです。
 - `compression <mode>` - 次の内いずれかのトラフィック圧縮モードを設定します。
 - `on` - 圧縮が有効です。
 - `off` - 圧縮が無効です。
 - `possible` - 圧縮が可能です。
 - `encryption <mode>` - 次の内いずれかのトラフィック暗号化モードを設定します。
 - `on` - 暗号化が有効です。
 - `off` - 暗号化が無効です。
 - `possible` - 暗号化が可能です。
 - `show` - 現在のDr.Web Control Protocolのオプションを表示します。
- `io <parameter>` - Serverプロセスの入力／出力統計を表示します。特定のパラメータを要求するには以下のコマンドを使用します。
 - `clear` - 蓄積された統計データを全て削除します。
 - `disable` - 統計のモニタリングを無効にします。



- `enable` - 統計のモニタリングを有効にします。
- `rawdr` - 当日の読み込まれたデータに関する統計値を表示します。
- `rawd` - 当日の書き込まれたデータに関する統計値を表示します。
- `rawh` - 過去1時間の統計値を表示します。
- `rawm` - 過去1分間の統計値を表示します。
- `rday` - 当日のデータ読み込みのグラフを表示します。
- `rhour` - 過去1時間のデータ読み込みのグラフを表示します。
- `rminute` - 過去1分間のデータ読み込みのグラフを表示します。
- `status` - 統計のモニタリング状況を表示します。
- `wday` - 当日のデータ書き込みのグラフを表示します。
- `whour` - 過去1時間のデータ書き込みのグラフを表示します。
- `wminute` - 過去1分間のデータ書き込みのグラフを表示します。
- `log <parameter>` - Serverログファイルに文字列を書き込む、またはログの詳細レベルを設定、表示します。指定されたパラメータに応じて、以下のアクションが実行されます。
 - `log <string>` - 指定された文字列をNOTICEの詳細レベルでServerログファイルに書き込みます。
 - `log \s [<level/>]` - ログの詳細レベルを設定、表示します。コマンドが`\s`コマンドで、レベルが指定されずに起動した場合、現在の詳細レベルが表示されます。利用可能なログの詳細レベルの値: ALL、DEBUG3、DEBUG2、DEBUG1、DEBUG、TRACE3、TRACE2、TRACE1、TRACE、INFO、NOTICE、WARNING、ERROR、CRIT
- `lua` - LUAスクリプトを実行します。
- `mallopt <parameter>` - メモリ割り当てのパラメータを設定します。特定のパラメータを設定するには、追加コマンドを使用します。追加コマンドのリストを絞り込むには、`? mallopt`コマンドでヘルプを呼び出すことができます。



`mallopt`コマンドはUNIX系OS環境のServerでのみ使用可能です。

コマンドパラメータに関するさらなる詳細については、`glibc`ライブラリの`mallopt()`関数に関する記述を参照してください。この関数に関するヘルプを見るには`man mallopt`コマンドを使用します。

- `memory <parameter>` - Serverがインストールされているコンピューターのメモリ使用率に関する統計を表示します。特定のパラメータを要求するには、以下のコマンドを使用します。
 - `all` - 全ての情報と統計データを表示します。
 - `heap` - ダイナミックメモリに関する情報を表示します。
 - `malloc` - メモリ割り当てに関する統計を表示します。
 - `sizes` - 割り当てられたメモリ量に関する統計を表示します。
 - `system` - システムメモリに関する情報を表示します。



`memory`コマンドは、Windows環境、Linux系OS環境、FreeBSD系OS環境のServerのみで利用可能です。ここでは、`memory`コマンドの追加パラメータについて以下の制限があります。

- `system` - Windows OS、Linux系OS環境のServerのみ



- heap - Windows OS、Linux系OS環境のServerのみ
 - malloc - Linux系OS、FreeBSD OS環境のServerのみ
 - sizes - Linux系OS、FreeBSD OS環境のServerのみ
- monitoring *<mode>* - Serverプロセスによって使用されるCPU(*cpu <parameter>*コマンド)およびI/O(*io <parameter>*コマンド)リソースのモニタリングモードを設定、表示します。可能なパラメータは次のとおりです。
 - disable - モニタリングを無効にします。
 - enable - モニタリングを有効にします。
 - show - 現在のモードを表示します。
 - printstat - Server動作の統計をログに記録します。
 - reload - Dr.Web Server FrontDoorプラグインをリロードします。
 - repository *<parameter>* - リポジトリの管理です。特定の機能を要求するには、以下のコマンドを使用します。
 - all - 全てのリポジトリ製品のリストおよび製品ごとの全てのファイルの数を表示します。
 - clear - キャッシュ内のオブジェクトのTTL値に関係なく、キャッシュの内容をクリアします。
 - fill - 全てのリポジトリファイルをキャッシュに読み込みます。
 - keep - 現在キャッシュ内にある全てのリポジトリファイルをTTL値に関係なく永久的に保存します。
 - loaded - 現在キャッシュ内にある全てのリポジトリ製品および製品ごとの全てのファイルの数を表示します。
 - reload - リポジトリをディスクからリロードします。
 - statistics - リポジトリの更新統計を表示します。
 - restart - Serverを再起動します。
 - show *<parameter>* - Serverがインストールされているシステムの情報を表示します。特定のパラメータを設定するには、追加コマンドを使用します。追加コマンドのリストを絞り込むには、? showコマンドでヘルプを呼び出すことができます。



showコマンドの追加コマンドについて以下の制限があります。

- memory - Windows OS、Linux系OS環境のServerのみ
 - mapping - Windows OS、Linux系OS環境のServerのみ
 - limits - UNIX系OS環境のServerのみ
 - processors - Linux系OS環境のServerのみ
- sql - SQLクエリを実行します。
 - stop - Serverを停止します。
 - traffic *<parameter>* - Serverネットワークトラフィックの統計を表示します。特定のパラメータを要求するには、以下のコマンドを使用します。
 - all - Server起動時からの全てのトラフィックを表示します。
 - incremental - 最後にtraffic incrementalコマンドを実行してからのトラフィックの増加分を表示します。
 - last - 最後に保存されたポイントからのトラフィックの増加分を表示します。



- `store - last` コマンドの保存ポイントを作成します。
- `update <parameter>` - 情報を取得し、更新を管理します。特定の機能についての情報を取得するには、以下のコマンドを使用します。
 - `active` - 現在更新が実行されているAgentのリストを表示します。
 - `agent [<mode>]` - ServerからのAgentの更新モードを表示／設定します。追加のパラメータなしに実行された場合、現在のモードが表示されます。モードを設定するには、次の追加コマンドを使用します。
 - `on` - Agentの更新を有効にします。
 - `off` - Agentの更新を無効にします。
 - `gus` - GUSの更新状況を無視してGUSからリポジトリの更新を実行します。
 - `http [<mode>]` - GUSからのServerリポジトリの更新モードを表示／設定します。追加のパラメータなしに実行された場合、現在のモードが表示されます。モードを設定するには、次の追加コマンドを使用します。
 - `on` - GUSからのリポジトリ更新を有効にします。
 - `off` - GUSからのリポジトリ更新を無効にします。
 - `inactive` - 現在更新が実行されていないAgentのリストを表示します。
 - `track [<mode>]` - Agent更新のトラッキングモードを表示／設定します。追加のパラメータなしに実行された場合、現在のモードが表示されます。モードを設定するには、次の追加コマンドを使用します。
 - `on` - Agentの更新トラッキングを有効にします。
 - `off` - Agentの更新トラッキングを無効にします。この場合、`update active` コマンドは現在更新が実行されているAgentのリストを表示しません。

H7.4. Dr.Web Serverリモートスクリプタブル診断ユーティリティ

Dr.Web Serverリモート診断ユーティリティでは、リモートでDr.Web Serverに接続し、基本的な管理と動作の統計表示ができます。[drwcntl](#)とは異なり、`drwcmd`ユーティリティは、スクリプト作成時に使用できます。

次のコンソールバージョンのDr.Web Serverリモートスクリプタブル診断ユーティリティが提供されています。

実行ファイル	位置情報	説明
<code>drweb-cmd- <OS>- <bitness></code>	Control Center、管理 → ユーティリティ セクション	個々のバージョンのユーティリティ。任意のディレクトリから、または対応するオペレーティングシステムが搭載されたコンピューターで起動できます。
	<code>webmin/utilities</code> Serverディレクトリ	
<code>drwcmd</code>	<code>bin</code> Serverディレクトリ	ユーティリティのバージョンはサーバーのライブラリに依存します。保存先のディレクトリからのみ起動できます。



`drweb-cmd- <OS>- <bitness>`と`drwcmd`のバージョンのユーティリティは機能が似ています。さらにこのセクションでは、`drwcmd`のバージョンが示されていますが、全ての例が両バージョンに関連します。



Serverリモート診断ユーティリティに接続するには、Dr.Web Server FrontDoorプラグインを有効にする必要があります。これを行うには、**Dr.Web Server設定** セクションの **モジュール** タブで、**Dr.Web Server FrontDoorプラグイン** フラグを設定します。

Serverリモート診断ユーティリティに接続するには、ユーティリティ経由で接続する管理者が **追加機能を使用** 権限を持っている必要があります。そうでない場合、リモート診断ユーティリティ経由でServerにアクセスすることはできません。

Dr.Web Serverリモート診断ユーティリティへのServerの接続設定については、[管理者マニュアルのDr.Web Serverのリモートアクセス](#)を参照してください。

スタート命令フォーマット

```
drwcmd [ <switches> ] [ <files> ]
```

使用可能なスイッチ



drwcmdユーティリティは[付録H. Dr.Web Enterprise Security Suite](#)に含まれるプログラムの**コマンドラインパラメータ**に記載の一般的な規則に従ってスイッチを使用します。

- `--?` - ユーティリティ使用のスイッチに関するヘルプを表示します。
- `--help` - ユーティリティ使用のコマンドに関するヘルプを表示します。
- `--commands= <commands>` - (`drwcntl`ユーティリティコマンドと同様の) 指定したコマンドを実行します。複数のコマンドを指定するには、「;」記号を区切り文字として使用します。
- `--debug=yes|no` - デバッグモード(`stderr`標準出力ストリーム)でユーティリティ操作をログ記録します。デフォルトは`no`です。
- `--files=yes|no` - 指定したファイルから(`drwcntl`ユーティリティコマンドと同様に) コマンドを実行できます。デフォルトは`yes`です。
コマンドはファイル内で1行に1つずつ設定する必要があります。空行は無視されます。コメントを開始するには「#」記号を使用してください。
- `--keep=yes|no` - 最後のコマンドが実行された後、ユーティリティプロセスが完了するまで、Serverとの接続を維持します。デフォルトは`no`です。
- `--output= <file>` - Server応答の出力ファイル。ファイルが指定されていない場合、デフォルトでは、`stdout`標準出力ストリームが使用されます。
ファイル名が「+」で始まる場合、コマンドの実行結果がファイルの最後に追加されます。そうでない場合はファイルが書き換えられます。
- `--password= <password>` - Serverでの認証用パスワード。`--resource`スイッチのファイルセットで定義できます。
- `--read=yes|no` - リソースファイルからのServer接続パラメータの読み取りを許可します。デフォルトは`yes`です。
- `--resource= <file>` - Server接続パラメータ(Serverのアドレスと、Serverでの認証用の管理者認証情報)のリソースファイル。デフォルトでは、`drwcmdrc`ファイルは以下のディレクトリから使用されます。
 - UNIX系OSの場合: `$HOME`



□ Windows OSの場合: %LOCALAPPDATA%

ファイルの各行は、<Server> <user> <password>のようにスペースで区切られた3つの単語を含む必要があります。

単語の途中でスペースを指定するには、「%S」を使用します。パーセント記号を指定する場合は、「%P」を使用します。

例:

```
ssl://127.0.0.1 user1 password1
ssl://127.0.0.1 user2 password2
ssl://127.0.0.1 user pass%Sword
```



--resourceスイッチを使用する場合は、--serverスイッチも指定する必要があります。ユーティリティは、リソースファイル内のこのServerのアドレスに対応する認証情報に従って、--serverスイッチで指定されたServerに接続します。

- --server=<Server> - Serverのアドレス。デフォルトはssl://127.0.0.1です。--resourceスイッチのファイルセットで定義できます。
- --user=<user> - Serverでの認証用ユーザー名。--resourceスイッチのファイルセットで定義できます。
- --verbose=yes|no - Serverの詳細応答を印刷する(stdout標準出力ストリーム)。デフォルトはnoです。

Serverに接続する手順は次のとおりです。

1. Server接続のデータを定義するとき、--server、--user、--passwordスイッチで指定された値に優先順位が与えられます。
2. --serverスイッチが指定されていない場合は、デフォルト値であるssl://127.0.0.1が使用されます。
3. --userスイッチが指定されていない場合は、.drwcmdrcファイル(--resourceスイッチで再定義可能)で必要なServerが検索され、アルファベット順で最初のユーザー名が使用されます。
4. --passwordスイッチが指定されていない場合は、drwcmdrcファイル(--resourceで再定義可能)でServerとユーザー名の検索が実行されます。



--readで禁止されていない場合、ユーザー名とパスワードはdrwcmdrcファイル(--resourceスイッチで再定義可能)から読み込まれます。

5. ユーザー名とパスワードがスイッチファイルまたはリソースファイルで指定されていない場合、ユーティリティはコンソールで認証情報を入力するよう求めます。

コマンド実行機能は次のとおり。

- ファイルにコマンドで「-」値が設定されている場合、ユーティリティはコンソールで入力されたコマンドを読み取ります。
- --commandsスイッチのコマンドとファイルリストのコマンドの両方が設定されている場合、--commandsスイッチのコマンドが最初に実行されます。
- --commandsスイッチのコマンドのいずれのファイルも指定されていない場合、コンソールから入力されたコマンドが読み込まれます。



例:

--commandスイッチからコマンドを実行してからコンソールコマンドを実行するには、次のように入力します。

```
drwcmd --commands=<commands> -- -
```

完了コード

- 0 - 実行成功。
- 1 - スwitchのヘルプが要求されています。--helpまたは--?。
- 2 - コマンドライン解析エラー。認証パラメータが指定されていない、など。
- 3 - Server応答の出力ファイルを作成できません。
- 4 - Serverの認証エラー。管理者のログイン情報および/またはパスワードが正しくありません。
- 5 - Server接続が異常終了しました。
- 127 - 不明な致命的エラー。

H7.5. Dr.Web Repository Loader



Repository Loaderユーティリティのグラフィカルバージョンについては、管理者マニュアルの[GUIユーティリティ](#)に記載されています。

次のバージョンのDr.Web Repository Loaderコンソールユーティリティが提供されています。

実行ファイル	位置情報	説明
drweb-reploader- <OS>-<bitness>	Control Center、管理 → ユーティリティ セクション	個々のバージョンのユーティリティ。任意のディレクトリから、または対応するオペレーティングシステムが搭載されたコンピューターで起動できます。
	webmin/utilities Serverディレクトリ	
drwreploader	bin Serverディレクトリ	ユーティリティのバージョンはサーバーのライブラリに依存します。保存先のディレクトリからのみ起動できます。



drweb-reploader-<OS>-<bitness>とdrwreploaderのバージョンのユーティリティは機能が似ています。さらにこのセクションでは、drwreploaderのバージョンが示されていますが、全ての例が両バージョンに関連しています。

[Repository Loader設定ファイル](#)を使用すると、コンソールユーティリティを実行するスイッチの指定を簡素化できます。プリインストールされている設定ファイルでは、--ssh-authスイッチを除き、スイッチの値は以下に記載したデフォルト値に対応します。この値は設定ファイルでpubkeyに再定義されます。



使用可能なスイッチ

- `--archive` - リポジトリがアーカイブされます。デフォルトはnoです。
- `--auth <argument>` - `<user>[:<password>]`の形式で更新サーバーの認証の認証情報を入力します。
- `--cert-file <path>` - SSL認証用のルート証明書ストレージへのパス。
- `--cert-mode [<argument>]` - 自動的に承認されるSSL証明書のタイプ。このオプションは、暗号化をサポートする安全なプロトコルにのみ使用されます。
`<argument>`には以下の値を使用できます。
 - `any` - 全ての証明書を許可
 - `valid` - 有効な証明書のみを許可
 - `drweb` - Dr.Web証明書のみに許可
 - `custom` - ユーザー指定の証明書を許可。デフォルトでは`drweb`値が使用されます。
- `--config <path>` - [Repository Loader設定ファイル](#)へのパス。
- `--cwd <path>` - 現在の作業ディレクトリへのパス。
- `--ipc` - 標準出力ストリームへのユーティリティ操作に関するデータ転送を有効にします。デフォルトはnoです。
- `--help` - スイッチに関するヘルプが表示されます。
- `--license-key <path>` - ライセンスキーファイルへのパスです(キーファイルまたはそのMD5ハッシュを指定する必要があります)。
- `--log <path>` - リポジトリダウンロードプロセスに関するログファイルへのパス。
- `--mode <mode>` - 次のようにローディングモードを更新します。
 - `repo` - リポジトリがServerリポジトリフォーマットでダウンロードされます。ロードされたファイルはサーバーリポジトリの更新と同時にControl Center経由で直接インポートできます。値はデフォルトで使用されます。
 - `mirror` - リポジトリがGUS更新ゾーンフォーマットでダウンロードされます。ロードされたファイルはローカルネットワークの更新ミラーに置くことができます。以後、GUS サーバーからではなく、リポジトリの最新バージョンを含んだこの更新ミラーから直接更新を受け取るようサーバーを設定できます。
- `--only-bases` - ウイルスデータベースのみがダウンロードされます。デフォルトはnoです。
- `--path <argument>` - `<argument>`で指定したフォルダに、GUSからリポジトリをダウンロードします。`--archive`スイッチを使用してリポジトリをアーカイブする場合、フォルダ名またはアーカイブファイル名のいずれかへのパスを指定できます。アーカイブ名が指定されていない場合は、`repository.zip`デフォルト名が使用されます。
- `--product <argument>` - 更新された製品。デフォルトではリポジトリ全体がダウンロードされます。
- `--prohibit-cdn` - 更新のダウンロード時にCDNを使用しません。デフォルトではnoとなっているため、CDNを使用できます。
- `--proto <protocol>` - 以下のローディングプロトコルを更新します:`file | ftp | ftps | http | https | scp | sftp | smb | smbs`。デフォルトはhttpsです。
- `--proxy-auth <argument>` - プロキシサーバーでの認証(ユーザーログインとパスワード)に必要な次のフォーマットのデータです:`<login>[:<password>]`。
- `--proxy-host <argument>` - 次のフォーマットで指定されるプロキシサーバーアドレスです:`<server>[:<port>]`。デフォルトでは、portは3128です。



- `--rotate <N><f>, <M><u>` - Repository Loaderのログローテーションモードです。[サーバーログローテーション](#)と同じです。
デフォルトでは10, 10mで、圧縮を使ってそれぞれ10メガバイトのファイルを10個保存するという意味になります。
- `--servers <argument>` - GUSサーバーのアドレスです。次のようにデフォルト値のままにすることをお勧めします: `esuite.geo.drweb.com`。
- `--show-products` - GUS製品のリストが表示されます。デフォルトはnoです。
- `--ssh-auth <type>` - SCP/SFTPによるアクセス時の更新サーバー上の認証タイプです。`<type>`パラメータには、次の値の内の1つが許可されています。
 - `pwd` - パスワードを使用する認証。パスワードは`--auth`スイッチに設定されています。
 - `pubkey` - パブリックキーを使用する認証。対応するパブリックキーを抽出するには、`--ssh-prikey`スイッチでプライベートキーを指定する必要があります。
- `--ssh-prikey <path>` - SSHプライベートキーへのパス。
- `--ssh-pubkey <path>` - SSHパブリックキーへのパス。
- `--strict` - エラーが発生した場合にダウンロードを中止します。デフォルトはnoです。
- `--update-key <path>` - GUSからロードされた更新の署名を検証するためのパブリックキーまたはパブリックキーのあるフォルダへのパス。更新を検証するための`update-key-*.upub`パブリックキーは、Dr.Web Serverの `etc` フォルダにあります。
- `--update-url <argument>` - Dr.Web製品の更新を含むGUSサーバーのフォルダです。次のようにデフォルト値のままにすることをお勧めします: `/update`。
- `--verbosity <details_level>` - ログの詳細レベルです。デフォルトはTRACE3です。可能な値は、ALL、DEBUG3、DEBUG2、DEBUG1、DEBUG、TRACE3、TRACE2、TRACE1、TRACE、INFO、NOTICE、WARNING、ERROR、CRITです。ALL値とDEBUG3値はシノニムです。
- `--version <version>` - 次のフォーマットの場合、更新をロードする必要があるServerバージョンです: `<major_version>.<minor_version>`。たとえば、11バージョンのServerの場合、`<version>` パラメータの値は11.00です。



スイッチの使用機能

Repository Loaderの起動時は、次のルールに注意してください。

スイッチには以下が指定されている必要があります	条件
--license-key	常時
--update-key	
--path	
--cert-file	次のスイッチがいずれかの値をとる場合: <ul style="list-style-type: none">• --cert-mode valid drweb custom• --proto https ftps smbs
--ssh-prikey	次のスイッチがいずれかの値をとる場合: <ul style="list-style-type: none">• --proto sftp scp• --ssh-auth pubkey

使用例

1. 全ての製品を含むインポートされたアーカイブを作成するには

```
drwreploder.exe --path C:\Temp --archive --license-key C:\agent.key --update-key "C:\Program Files\DrWeb Server\etc" --cert-file "C:\Program Files\DrWeb Server\etc"
```

2. ウイルスデータベースのみを含むインポートされたアーカイブを作成するには

```
drwreploder.exe --path C:\Temp --archive --license-key "C:\agent.key" --update-key "C:\Program Files\DrWeb Server\etc" --cert-file "C:\Program Files\DrWeb Server\etc" -only-bases
```

3. Serverのみを含むインポートされたアーカイブを作成する場合:

```
drwreploder.exe --path C:\Temp --archive --license-key "C:\agent.key" --update-key "C:\Program Files\DrWeb Server\etc" --cert-file "C:\Program Files\DrWeb Server\etc" --product=20-drwcs
```



付録I. Dr.Web Serverによってエクスポートされる環境変数

Dr.Web Serverがスケジュールに沿って実行するプロセスの設定を簡易化するために、Serverのカatalogがある場所に関するデータが必要となります。そこでServerは、開始したプロセスの以下の変数を環境にエクスポートします。

- DRWCSD_HOME - ルートフォルダ(インストールフォルダ)へのパスです。スイッチの値は、サーバーの起動時に設定されていた場合は`-home`、それ以外の場合は起動時のカレントフォルダです。
- DRWCSD_BIN - 実行ファイルのあるフォルダへのパスです。スイッチの値は、サーバーの起動時に設定されていた場合は`-bin-root`、それ以外の場合はルートフォルダの`bin`サブフォルダです。
- DRWCSD_VAR - サーバーが書き込み権限を持ち、揮発性ファイル(ログやリポジトリファイルなど)の保存場所に指定されたフォルダへのパスです。スイッチの値は、サーバーの起動時に設定されていた場合は`-var-root`、それ以外の場合はルートフォルダの`var`サブフォルダです。



付録J. Dr.Web Enterprise Security Suiteで使用される正規表現

Dr.Web Enterprise Security Suiteのパラメータのいくつかは以下の種類の正規表現で指定されます。

- Lua言語の正規表現
アンチウイルスネットワーク端末を自動でユーザーグループに含める場合の設定に使用します。
Lua言語の正規表現に関する詳細については、<http://www.lua.org/manual/5.1/manual.html#5.4.1>を確認してください。
- PCREプログラムライブラリの正規表現
PCREライブラリ構文についての詳細については、<http://www.pcre.org/>を確認してください。
この付録ではPCREライブラリの正規表現の最も一般的な使用例のみを簡単に記載します。

J1. PCRE正規表現で使用されるオプション

スキャンの対象から除外されるオブジェクトをScannerの設定内で指定する際、設定ファイル内およびDr.Web Security Control Center内で正規表現が使用されます。

正規表現は次のように表記されます。

```
qr{EXP}options
```

EXPの部分は表現そのもので、optionsは一連のオプション(一連の文字列)、qr{}はリテラルなメタ文字です。全体の構文は次のようになります。

```
qr{pagefile\.sys}i - Windows NTスワップファイル
```

次はオプションと正規表現の説明です。詳細については、<http://www.pcre.org/pcre.txt>を参照してください。

- オプションの'a'はPCRE_ANCHOREDと同じです。
このオプションが設定されている場合、パターンは強制的に固定(anchored)となり、検索される文字列(「対象の文字列」)の先頭でのみマッチするように制限されます。パターン自体の中に適切な指定を行うことでも同じ結果を得ることができます。
- オプションの'i'はPCRE_CASELESSと同じです。
このオプションが設定されている場合、パターン内の文字は大文字・小文字のどちらにもマッチします。このオプションは(?i)オプションの設定によってパターン内で変更できます。
- オプション'x'はPCRE_EXTENDEDと同じです。
このオプションが設定されている場合、パターン内の空白文字は、エスケープされているか文字クラスの中にある場合を除いて完全に無視されます。空白文字はVT文字(コード11)を含みません。さらに、文字クラス外のエスケープされていない#と改行文字の間にある文字は無視されます。このオプションは(?x)オプションを設定することによって、パターン内で変更することが可能です。このオプションによって複雑なパターンの内部にコメントを記述することが可能になります。ただし、適用できるのはデータ文字のみになりますので注意してください。空白文字をパターンの特殊文字の並びの中(条件付きサブパターン内 (? (の内部など)に置くことはできません)。
- オプション'm'はPCRE_MULTILINEと同じです。
デフォルトでは、PCREは対象の文字列を1行の文字の並びとして扱います(実際は改行文字を含んでいても)。「行頭」を表すメタ文字"^"は文字列の先頭でのみマッチし、「行末」を表すメタ文字"\$"は文字列の末尾、または最後の改行の前でのみマッチします(PCRE_DOLLAR_ENDONLYがセットされていない限り)。



PCRE_MULTILINEが設定されている場合、「行頭」および「行末」メタ文字は、文字列の最初と最後に加えて、文字列内でそれらの直前直後にある改行文字にもマッチします。このオプションは(?m)オプション設定によってパターン内で変更できます。対象の文字列に"\n"文字がない場合、またはパターン内に^や\$がない場合にはこのオプションは設定しても意味がありません。

- オプション'u'はPCRE_UNGREEDYと同じです。

このオプションは量指定子の「貪欲さ」を反転させます。量指定子はデフォルトでは貪欲ではなく、後ろに"?"を付けて初めて貪欲になるようになります。パターン内の(?U)オプションでも同じ結果が得られます。

- オプション'd'はPCRE_DOTALLと同じです。

このオプションが設定されている場合、パターン内のドットメタ文字は改行を含む全ての文字にマッチします。設定されていない場合は改行にはマッチしません。このオプションは(?s)オプション設定によってパターン内で変更できます。[^a]のような否定の文字クラスは、このオプションの設定に関係なく常に改行文字にマッチします。

- オプション'e'はPCRE_DOLLAR_ENDONLYと同じです。

このオプションが設定されている場合、パターン内のドルメタ文字は対象文字列の末尾にのみマッチします。このオプションが設定されていない場合には、ドルメタ文字は文字列の最後にある改行の直前(他の改行文字の前にはマッチしません)にもマッチします。PCRE_MULTILINEオプションが設定されている場合PCRE_DOLLAR_ENDONLYオプションは無視されます。

J2. PCRE正規表現の特性

*正規表現*は対象の文字列に対して左から右へマッチするパターンです。ほとんどの文字はパターン内ではその文字自身を意味し、対象内の対応する文字にマッチします。

正規表現の強みは、パターン内に代入と繰り返しを含むことができるという点にあります。それらは、それ自身を意味せずに特殊な解釈をされるメタ文字の使用によって、パターン内にエンコードされます。

メタ文字には2種類あります。角括弧内を除くパターン内のどこでも使用できるものと、角括弧内でのみ使用できるものです。角括弧の外でのメタ文字は以下のとおりです。

表記	値
\	複数の用途を持つ一般的なエスケープ文字
^	検索対象(複数行内では行)の始まりを言明
\$	検索対象(複数行内では行)の終わりを言明
.	改行以外の全ての文字にマッチ(デフォルト)
[文字クラス定義の開始
]	文字クラス定義の終了
	選択枝の開始
(サブパターンの開始
)	サブパターンの終了
?	(の意味を拡張



表記	値
	または量指定子。直前の表現の0回または1回の繰り返し。 または最小量指定子。
*	0 量指定子。直前の表現の0回以上の繰り返し。
+	1 量指定子。直前の表現の0回以上の繰り返し。 または「独占的量指定子」
{	最小／最大を指定する量指定子の開始

角括弧内のパターンの一部は「文字クラス」と呼ばれます。文字クラスの中でメタ文字として扱われるのは以下のものだけです。

表記	値
\	一般的なエスケープ文字
^	先頭にある場合のみ、後に続く文字クラスを否定
-	文字の範囲を指定
[POSIX文字クラス(POSIX構文が後に続いた場合のみ)
]	文字クラスの終了



付録K. ログファイルフォーマット

サーバー(管理者マニュアルのページ[Dr.Web Serverロギング](#)参照)およびAgent上のイベントはテキストファイルにロギングされます。1行につき1つのメッセージになります。

メッセージラインのフォーマットは以下のとおりです。

```
<year><month><day>.<hour><minute><second>.<centisecond> <message_type>
[<process_id>] <thread_name> [<message_source>] <message>
```

ここで:

- `<year><month><date>.<hour><minute><second>.<hundredth_of_second>` - ログファイルにメッセージがエントリされた正確な日時です。
- `<message_type>` - ログの詳細レベルです。
 - **ftl (Fatal error)** - 最も重大なエラーのみ報告します。
 - **err (Error)** - 動作エラーを通知します。
 - **wrn (Warning)** - エラーについて警告します。
 - **ntc (Notice)** - 重要な情報メッセージを表示します。
 - **inf (Info)** - 情報メッセージを表示します。
 - **tr0..3 (trace0..3—tracing)** - 詳細レベルに応じたイベントのトレースを有効にします(**Trace 3**は最も高い詳細レベルでのロギングを命令します)。
 - **db0..3 (debug0..3—debugging)** - 詳細レベルに応じたデバッグイベントのロギングを命令します(**Debug 3**は最も高い詳細レベルでのロギングを命令します)。



tr0..3 (trace)、および**db0..3 (debug)**の詳細レベルは、Dr.Web Enterprise Security Suiteの開発者に対するメッセージにのみ適用できます。

- [`<process_id>`] - ログファイルにメッセージを書き込むスレッドが内部で実行されるプロセスの、独自の数字識別子です。OSによっては[`<process_id>`]が[`<process_id> <thread_id>`]になる場合があります。
- `<thread_name>` - 内部でメッセージのログが作成されたスレッドを表します。
- [`<message_source>`] - メッセージのロギングを開始したシステムの名前です。ソースは存在しないこともあります。
- `<message>` - ログレベルに応じたテキストの記述です。イベントのフォーマルな記述、およびイベントに関連した変数の値の両方が含まれる場合があります。

例:

1. 20081023.171700.74 inf [001316] mth:12 [Sch] Task "Purge unsent IS events" said OK

下記を表しています。

- 20081023—`<year><month><date>`,
- 171700—`<hour><minute><second>`,
- 74—`<hundredth_of_second>`,
- inf—`<message_type>`,
- [001316]—[`<process_id>`],



- mth:12—*<thread_name>*,
 - [Sch]—[*<message_source>*],
 - Task "Purge unsent IS events" said OK - *<message>*未送信イベントの削除イベントタスクが正しく実行されたというメッセージです。
2. 20081028.135755.61 inf [001556] srv:0 tcp/10.3.0.55:3575/025D4F80:2: new connection at tcp/10.3.0.75:2193
- 下記を表しています。
- 20081028—*<year><month><date>*,
 - 135755—*<hour><minute><second>*,
 - 61—*<hundredth_of_second>*,
 - inf—*<message_type>*,
 - [001556]—[*<process_id>*],
 - srv:0—*<thread_name>*,
 - tcp/10.3.0.55:3575/025D4F80:2: new connection at tcp/10.3.0.75:2193 - *<message>* 指定されたソケットを介して新しい接続が確立されたことに関するメッセージです。



付録L. Web APIとDr.Web Enterprise Security Suiteの連携



Web APIについては、『**Web API for Dr.Web Enterprise Security Suite**』マニュアルを参照してください。

アプリケーション

Web APIとDr.Web Enterprise Security Suiteが組み合わせられることで、アカウントのトランザクション操作とユーザー管理サービスの自動化の機能が提供されます。この機能を使用すると、ユーザーからリクエストを受信したり、ユーザーにインストールファイルを送信したりする動的ページを作成できます。

認証

HTTP(S)プロトコルをDr.Web Serverと連携させて使用できます。**Web API**はRESTリクエストを受け取り、XMLで応答します。Web APIへのアクセス時には、ベーシックHTTP認証が使用されます([RFC 2617](#)標準に準拠)。RFC 2617と関連標準に反して、HTTP(S)サーバーは、クライアントからの認証情報報(Dr.Web Enterprise Security Suiteの管理者アカウント名とパスワード)を要求しません。



付録M. ライセンス

このセクションには、Dr.Web Enterprise Security Suiteソフトウェアによって使用されるサードパーティ製ソフトウェアライブラリの一覧、ライセンスに関する情報、および開発プロジェクトのアドレスが含まれています。

サードパーティライブラリ	ライセンス	プロジェクトURL
asio	https://www.boost.org/LICENSE_1_0.txt *	https://think-async.com/Asio/
boost	https://www.boost.org/LICENSE_1_0.txt *	http://www.boost.org/
brotli	MIT License**	https://github.com/google/brotli
bsdifff	Custom	http://www.daemonology.net/bsdifff/
c-ares	https://c-ares.haxx.se/license.html *	https://c-ares.haxx.se/
cairo	Mozilla Public License** GNU Lesser General Public License**	https://www.cairographics.org/
CodeMirror	MIT License**	https://codemirror.net/
curl	https://curl.se/docs/copyright.html *	https://curl.se/libcurl/
ICU	http://www.unicode.org/copyright.html#License *	http://site.icu-project.org/home
fontconfig	Custom	https://www.freedesktop.org/wiki/Software/fontconfig/
freetype	GNU General Public License** FreeType Project License (BSD like)	https://www.freetype.org/
GCC runtime libraries	GNU General Public License**(*の例外を付き)	http://gcc.gnu.org/
HTMLLayout	Custom	https://terrainformatica.com/a-homepage-section/htmlayout/
jemalloc	https://github.com/jemalloc/jemalloc/blob/dev/COPYING *	https://github.com/jemalloc/jemalloc
jQuery	MIT License** GNU General Public License**	https://jquery.com/
JSON4Lua	MIT License**	https://github.com/craigmj/json4lua
Leaflet	BSD License	https://leafletjs.com/



サードパーティライブラリ	ライセンス	プロジェクトURL
	https://github.com/Leaflet/Leaflet/blob/master/LICENSE *	
libpng	http://libpng.org/pub/png/src/libpng-LICENSE.txt *	http://libpng.org/pub/png/libpng.html
libradius	Juniper Networks, Inc.*	https://www.freebsd.org/
libssh2	https://www.libssh2.org/license.html *	https://www.libssh2.org/
libxml2	MIT License**	http://www.xmlsoft.org/
Linenoise NG	BSD license*	https://github.com/arangodb/linenoise-ng
lua	MIT License**	http://www.lua.org/
lua-xmlreader	MIT License**	http://asbradbury.org/projects/lua-xmlreader/
lzma	GNU Lesser General Public License** Common Public License**	https://www.7-zip.org/sdk.html
ncurses	MIT License**	https://invisible-island.net/ncurses/announce.html
Net-snmp	http://www.net-snmp.org/about/license.html *	http://www.net-snmp.org/
nghttp2	MIT License**	https://nghttp2.org/
Noto Sans CJK	https://scripts.sil.org/cms/scripts/render_download.php?format=file&media_id=OFL_plaintext&filename=OFL.txt *	https://www.google.com/get/noto/help/cjk/
OpenLDAP	https://www.openldap.org/software/release/license.html *	https://www.openldap.org/
OpenSSL	https://www.openssl.org/source/license.html *	https://www.openssl.org/
Oracle Instant Client	https://www.oracle.com/downloads/licenses/instant-client-lic.html *	https://www.oracle.com/index.html
ParaType Free Font	https://www.paratype.ru/public/pt_openlicense_eng.asp *	https://www.paratype.ru/
pcre	http://www.pcre.org/licence.txt *	http://www.pcre.org/



サードパーティライブラリ	ライセンス	プロジェクトURL
pixman	MIT License**	http://pixman.org/
Prototype JavaScript framework	MIT License**	http://prototypejs.org/assets/2009/8/31/prototype.js
script.aculo.us scriptaculous.js	http://madrobby.github.io/scriptaculous/license/ *	http://script.aculo.us/
slt	MIT License**	https://code.google.com/archive/p/slt
SQLite	Public Domain https://www.sqlite.org/copyright.html	https://www.sqlite.org/index.html
wtl	Common Public License** Microsoft Public License**	https://sourceforge.net/projects/wtl/
zlib	http://www.zlib.net/zlib_license.html *	http://www.zlib.net/

* - ライセンスのテキストは以下の一覧を確認してください。

** - 次に見つかる基本ライセンスのテキスト:

ライセンス	アドレス
Common Public License	https://opensource.org/licenses/cpl1.0.php
GNU General Public License	https://www.gnu.org/licenses/gpl-3.0.html
GNU Lesser General Public License	https://www.gnu.org/licenses/lgpl-3.0.html
Microsoft Public License	https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff649456(v=pandp.10)
MIT License	https://opensource.org/licenses/mit-license.php
Mozilla Public License	https://www.mozilla.org/en-US/MPL/2.0/

M1. Boost

Boost Software License - Version 1.0 - August 17th, 2003

Permission is hereby granted, free of charge, to any person or organization obtaining a copy of the software and accompanying documentation covered by this license (the "Software") to use, reproduce, display, distribute, execute, and transmit the Software, and to prepare derivative



works of the Software, and to permit third-parties to whom the Software is furnished to do so, all subject to the following:

The copyright notices in the Software and this entire statement, including the above license grant, this restriction and the following disclaimer, must be included in all copies of the Software, in whole or in part, and all derivative works of the Software, unless such copies or derivative works are solely in the form of machine-executable object code generated by a source language processor.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

M2. C-ares

Copyright (c) 2007 - 2018, Daniel Stenberg with many contributors, see AUTHORS file.

Copyright 1998 by the Massachusetts Institute of Technology.

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of M.I.T. not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. M.I.T. makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

M3. Curl

Copyright (c) 1996 - 2013, Daniel Stenberg, <daniel@haxx.se>.

All rights reserved.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

M4. ICU

Copyright © 1991-2018 Unicode, Inc. All rights reserved.



Distributed under the Terms of Use in <http://www.unicode.org/copyright.html>.

Permission is hereby granted, free of charge, to any person obtaining a copy of the Unicode data files and any associated documentation (the "Data Files") or Unicode software and any associated documentation (the "Software") to deal in the Data Files or Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Data Files or Software, and to permit persons to whom the Data Files or Software are furnished to do so, provided that either (a) this copyright and permission notice appear with all copies of the Data Files or Software, or (b) this copyright and permission notice appear in associated Documentation.

THE DATA FILES AND SOFTWARE ARE PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THE DATA FILES OR SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in these Data Files or Software without prior written authorization of the copyright holder.

M5. GCC runtime libraries - 例外

GCC is Copyright (C) 1986, 1987, 1988, 1989, 1990, 1991, 1992, 1993, 1994, 1995, 1996, 1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008 Free Software Foundation, Inc.

GCC is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 3, or (at your option) any later version.

GCC is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

Files that have exception clauses are licensed under the terms of the GNU General Public License; either version 3, or (at your option) any later version.

The following runtime libraries are licensed under the terms of the GNU General Public License (v3 or later) with version 3.1 of the GCC Runtime Library Exception (included in this file):

- libgcc (libgcc/, gcc/libgcc2.[ch], gcc/unwind*, gcc/gthr*, gcc/coretypes.h, gcc/crtstuff.c, gcc/defaults.h, gcc/dwarf2.h, gcc/emults.c, gcc/gbl-ctors.h, gcc/gcov-io.h, gcc/libgcov.c, gcc/tsystem.h, gcc/typeclass.h).

- libdecnumber

- libgomp

- libssp

- libstdc++-v3

- libobjc

- libmudflap

- libgfortran

- The libgnat-4.4 Ada support library and libgnatvsn library.



- Various config files in gcc/config/ used in runtime libraries.

GCC RUNTIME LIBRARY EXCEPTION

Version 3.1, 31 March 2009

Copyright (C) 2009 Free Software Foundation, Inc. <<http://fsf.org/>>

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

This GCC Runtime Library Exception ("Exception") is an additional permission under section 7 of the GNU General Public License, version 3 ("GPLv3"). It applies to a given file (the "Runtime Library") that bears a notice placed by the copyright holder of the file stating that the file is governed by GPLv3 along with this Exception.

When you use GCC to compile a program, GCC may combine portions of certain GCC header files and runtime libraries with the compiled program. The purpose of this Exception is to allow compilation of non-GPL (including proprietary) programs to use, in this way, the header files and runtime libraries covered by this Exception.

0. Definitions.

A file is an "Independent Module" if it either requires the Runtime Library for execution after a Compilation Process, or makes use of an interface provided by the Runtime Library, but is not otherwise based on the Runtime Library.

"GCC" means a version of the GNU Compiler Collection, with or without modifications, governed by version 3 (or a specified later version) of the GNU General Public License (GPL) with the option of using any subsequent versions published by the FSF.

"GPL-compatible Software" is software whose conditions of propagation, modification and use would permit combination with GCC in accord with the license of GCC.

"Target Code" refers to output from any compiler for a real or virtual target processor architecture, in executable form or suitable for input to an assembler, loader, linker and/or execution phase. Notwithstanding that, Target Code does not include data in any format that is used as a compiler intermediate representation, or used for producing a compiler intermediate representation.

The "Compilation Process" transforms code entirely represented in non-intermediate languages designed for human-written code, and/or in Java Virtual Machine byte code, into Target Code. Thus, for example, use of source code generators and preprocessors need not be considered part of the Compilation Process, since the Compilation Process can be understood as starting with the output of the generators or preprocessors.

A Compilation Process is "Eligible" if it is done using GCC, alone or with other GPL-compatible software, or if it is done without using any work based on GCC. For example, using non-GPL-compatible Software to optimize any GCC intermediate representations would not qualify as an Eligible Compilation Process.

1. Grant of Additional Permission.

You have permission to propagate a work of Target Code formed by combining the Runtime Library with Independent Modules, even if such propagation would otherwise violate the terms of GPLv3, provided that all Target Code was generated by Eligible Compilation Processes. You may then convey such a combination under terms of your choice, consistent with the licensing of the Independent Modules.

2. No Weakening of GCC Copyleft.

The availability of this Exception does not imply any general presumption that third-party software is unaffected by the copyleft requirements of the license of GCC.



M6. Jemalloc

Unless otherwise specified, files in the jemalloc source distribution are subject to the following license:

Copyright (C) 2002-2018 Jason Evans <jasone@canonware.com>.

All rights reserved.

Copyright (C) 2007-2012 Mozilla Foundation. All rights reserved.

Copyright (C) 2009-2018 Facebook, Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice(s), this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice(s), this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER(S) ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER(S) BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

M7. Leaflet

Copyright (c) 2010-2018, Vladimir Agafonkin

Copyright (c) 2010-2011, CloudMade

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY



THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

M8. Libpng

If you modify libpng you may insert additional notices immediately following this sentence.

This code is released under the libpng license.

libpng versions 1.0.7, July 1, 2000 through 1.6.32, August 24, 2017 are Copyright (c) 2000-2002, 2004, 2006-2017 Glenn Randers-Pehrson, are derived from libpng-1.0.6, and are distributed according to the same disclaimer and license as libpng-1.0.6 with the following individuals added to the list of Contributing Authors:

Simon-Pierre Cadieux

Eric S. Raymond

Mans Rullgard

Cosmin Truta

Gilles Vollant

James Yu

Mandar Sahastrabuddhe

Google Inc.

Vadim Barkov

and with the following additions to the disclaimer:

There is no warranty against interference with your enjoyment of the library or against infringement. There is no warranty that our efforts or the library will fulfill any of your particular purposes or needs. This library is provided with all faults, and the entire risk of satisfactory quality, performance, accuracy, and effort is with the user.

Some files in the "contrib" directory and some configure-generated files that are distributed with libpng have other copyright owners and are released under other open source licenses.

libpng versions 0.97, January 1998, through 1.0.6, March 20, 2000, are Copyright (c) 1998-2000 Glenn Randers-Pehrson, are derived from libpng-0.96, and are distributed according to the same disclaimer and license as libpng-0.96, with the following individuals added to the list of Contributing Authors:

Tom Lane

Glenn Randers-Pehrson

Willem van Schaik

libpng versions 0.89, June 1996, through 0.96, May 1997, are Copyright (c) 1996-1997 Andreas Dilger, are derived from libpng-0.88, and are distributed according to the same disclaimer and license as libpng-0.88, with the following individuals added to the list of Contributing Authors:

John Bowler



Kevin Bracey

Sam Bushell

Magnus Holmgren

Greg Roelofs

Tom Tanner

Some files in the "scripts" directory have other copyright owners but are released under this license.

libpng versions 0.5, May 1995, through 0.88, January 1996, are Copyright (c) 1995-1996 Guy Eric Schalnat, Group 42, Inc.

For the purposes of this copyright and license, "Contributing Authors" is defined as the following set of individuals:

Andreas Dilger

Dave Martindale

Guy Eric Schalnat

Paul Schmidt

Tim Wegner

The PNG Reference Library is supplied "AS IS". The Contributing Authors and Group 42, Inc. disclaim all warranties, expressed or implied, including, without limitation, the warranties of merchantability and of fitness for any purpose. The Contributing Authors and Group 42, Inc. assume no liability for direct, indirect, incidental, special, exemplary, or consequential damages, which may result from the use of the PNG Reference Library, even if advised of the possibility of such damage.

Permission is hereby granted to use, copy, modify, and distribute this source code, or portions hereof, for any purpose, without fee, subject to the following restrictions:

1. The origin of this source code must not be misrepresented.
2. Altered versions must be plainly marked as such and must not be misrepresented as being the original source.
3. This Copyright notice may not be removed or altered from any source or altered source distribution.

The Contributing Authors and Group 42, Inc. specifically permit, without fee, and encourage the use of this source code as a component to supporting the PNG file format in commercial products. If you use this source code in a product, acknowledgment is not required but would be appreciated.

Glenn Randers-Pehrson

glennrp at users.sourceforge.net

April 1, 2017



M9. Libradius

```
Copyright 1998 Juniper Networks, Inc.
```

```
All rights reserved.
```

```
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
```

```
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
```

```
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
```

```
THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
```

```
$FreeBSD: src/lib/libradius/radlib_private.h,v 1.6.30.3 2012/04/21 18:30:48 melifaro Exp $
```

M10. Libssh2

```
Copyright (c) 2004-2007 Sara Golemon <sarag@libssh2.org>
```

```
Copyright (c) 2005,2006 Mikhail Gusarov <dottedmag@dottedmag.net>
```

```
Copyright (c) 2006-2007 The Written Word, Inc.
```

```
Copyright (c) 2007 Eli Fant <elifantu@mail.ru>
```

```
Copyright (c) 2009-2014 Daniel Stenberg
```

```
Copyright (C) 2008, 2009 Simon Josefsson
```

```
All rights reserved.
```

```
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
```

```
Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
```

```
Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
```

```
Neither the name of the copyright holder nor the names of any other contributors may be used to endorse or promote products derived from this software without specific prior written permission.
```

```
THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR
```



```
CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR  
CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR  
SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY  
THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR  
OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE  
POSSIBILITY OF SUCH DAMAGE.
```

M11. Linenoise NG

linenoise

```
Copyright (c) 2010, Salvatore Sanfilippo <antirez at gmail dot com>
```

```
Copyright (c) 2010, Pieter Noordhuis <pcnoordhuis at gmail dot com>
```

```
All rights reserved.
```

```
Redistribution and use in source and binary forms, with or without modification, are permitted  
provided that the following conditions are met:
```

```
* Redistributions of source code must retain the above copyright notice, this list of  
conditions and the following disclaimer.
```

```
* Redistributions in binary form must reproduce the above copyright notice, this list of  
conditions and the following disclaimer in the documentation and/or other materials provided  
with the distribution.
```

```
* Neither the name of Redis nor the names of its contributors may be used to endorse or  
promote products derived from this software without specific prior written permission.
```

```
THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR  
IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY  
AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR  
CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR  
CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR  
SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY  
THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR  
OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE  
POSSIBILITY OF SUCH DAMAGE.
```

wcwidth

```
Markus Kuhn -- 2007-05-26 (Unicode 5.0)
```

```
Permission to use, copy, modify, and distribute this software for any purpose and without fee  
is hereby granted. The author disclaims all warranties with regard to this software.
```

ConvertUTF

```
Copyright 2001-2004 Unicode, Inc.
```

```
Disclaimer
```

```
This source code is provided as is by Unicode, Inc. No claims are made as to fitness for any  
particular purpose. No warranties of any kind are expressed or implied. The recipient agrees to  
determine applicability of information provided. If this file has been purchased on magnetic or  
optical media from Unicode, Inc., the sole remedy for any claim will be exchange of defective  
media within 90 days of receipt.
```



Limitations on Rights to Redistribute This Code

Unicode, Inc. hereby grants the right to freely use the information supplied in this file in the creation of products supporting the Unicode Standard, and to make copies of this file in any form for internal or external distribution as long as this notice remains attached.

M12. Net-snmp

Various copyrights apply to this package, listed in various separate parts below. Please make sure that you read all the parts.

---- Part 1: CMU/UCD copyright notice: (BSD like) ----

Copyright 1989, 1991, 1992 by Carnegie Mellon University

Derivative Work - 1996, 1998-2000

Copyright 1996, 1998-2000 The Regents of the University of California

All Rights Reserved

Permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU and The Regents of the University of California not be used in advertising or publicity pertaining to distribution of the software without specific written permission.

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

---- Part 2: Networks Associates Technology, Inc copyright notice (BSD) ----

Copyright (c) 2001-2003, Networks Associates Technology, Inc

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the Networks Associates Technology, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS 'AS IS' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR



OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 3: Cambridge Broadband Ltd. copyright notice (BSD) ----

Portions of this code are copyright (c) 2001-2003, Cambridge Broadband Ltd.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* The name of Cambridge Broadband Ltd. may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER 'AS IS' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 4: Sun Microsystems, Inc. copyright notice (BSD) ----

Copyright © 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara,

California 95054, U.S.A. All rights reserved.

Use is subject to license terms below.

This distribution may include materials developed by third parties.

Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the Sun Microsystems, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS 'AS IS' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR



OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 5: Sparta, Inc copyright notice (BSD) ----

Copyright (c) 2003-2009, Sparta, Inc

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of Sparta, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS 'AS IS' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 6: Cisco/BUPTNIC copyright notice (BSD) ----

Copyright (c) 2004, Cisco, Inc and Information Network

Center of Beijing University of Posts and Telecommunications.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of Cisco, Inc, Beijing University of Posts and Telecommunications, nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS 'AS IS' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 7: Fabasoft R&D Software GmbH & Co KG copyright notice (BSD) ----



Copyright (c) Fabasoft R&D Software GmbH & Co KG, 2003

oss@fabasoft.com

Author: Bernhard Penz

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* The name of Fabasoft R&D Software GmbH & Co KG or any of its subsidiaries, brand or product names may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER 'AS IS' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 8: Apple Inc. copyright notice (BSD) ----

Copyright (c) 2007 Apple Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of Apple Inc. ("Apple") nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY APPLE AND ITS CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL APPLE OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 9: ScienceLogic, LLC copyright notice (BSD) ----

Copyright (c) 2009, ScienceLogic, LLC

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:



* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of ScienceLogic, LLC nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS 'AS IS' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

M13. Noto Sans CJK

Copyright (c) <dates>, <Copyright Holder> (<URL|email>), with Reserved Font Name <Reserved Font Name>.

Copyright (c) <dates>, <additional Copyright Holder> (<URL|email>), with Reserved Font Name <additional Reserved Font Name>.

Copyright (c) <dates>, <additional Copyright Holder> (<URL|email>).

This Font Software is licensed under the SIL Open Font License, Version 1.1.

This license is copied below, and is also available with a FAQ at:

<http://scripts.sil.org/OFL>

SIL OPEN FONT LICENSE Version 1.1 - 26 February 2007

PREAMBLE

The goals of the Open Font License (OFL) are to stimulate worldwide development of collaborative font projects, to support the font creation efforts of academic and linguistic communities, and to provide a free and open framework in which fonts may be shared and improved in partnership with others.

The OFL allows the licensed fonts to be used, studied, modified and redistributed freely as long as they are not sold by themselves. The fonts, including any derivative works, can be bundled, embedded, redistributed and/or sold with any software provided that any reserved names are not used by derivative works. The fonts and derivatives, however, cannot be released under any other type of license. The requirement for fonts to remain under this license does not apply to any document created using the fonts or their derivatives.

DEFINITIONS

"Font Software" refers to the set of files released by the Copyright Holder(s) under this license and clearly marked as such. This may include source files, build scripts and documentation.



"Reserved Font Name" refers to any names specified as such after the copyright statement(s).

"Original Version" refers to the collection of Font Software components as distributed by the Copyright Holder(s).

"Modified Version" refers to any derivative made by adding to, deleting, or substituting -- in part or in whole -- any of the components of the Original Version, by changing formats or by porting the Font Software to a new environment.

"Author" refers to any designer, engineer, programmer, technical writer or other person who contributed to the Font Software.

PERMISSION & CONDITIONS

Permission is hereby granted, free of charge, to any person obtaining a copy of the Font Software, to use, study, copy, merge, embed, modify, redistribute, and sell modified and unmodified copies of the Font Software, subject to the following conditions:

- 1) Neither the Font Software nor any of its individual components, in Original or Modified Versions, may be sold by itself.
- 2) Original or Modified Versions of the Font Software may be bundled, redistributed and/or sold with any software, provided that each copy contains the above copyright notice and this license. These can be included either as stand-alone text files, human-readable headers or in the appropriate machine-readable metadata fields within text or binary files as long as those fields can be easily viewed by the user.
- 3) No Modified Version of the Font Software may use the Reserved Font Name(s) unless explicit written permission is granted by the corresponding Copyright Holder. This restriction only applies to the primary font name as presented to the users.
- 4) The name(s) of the Copyright Holder(s) or the Author(s) of the Font Software shall not be used to promote, endorse or advertise any Modified Version, except to acknowledge the contribution(s) of the Copyright Holder(s) and the Author(s) or with their explicit written permission.
- 5) The Font Software, modified or unmodified, in part or in whole, must be distributed entirely under this license, and must not be distributed under any other license. The requirement for fonts to remain under this license does not apply to any document created using the Font Software.

TERMINATION

This license becomes null and void if any of the above conditions are not met.

DISCLAIMER

THE FONT SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF COPYRIGHT, PATENT, TRADEMARK, OR OTHER RIGHT. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, INCLUDING ANY GENERAL, SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF THE USE OR INABILITY TO USE THE FONT SOFTWARE OR FROM OTHER DEALINGS IN THE FONT SOFTWARE.

M14. OpenLDAP

The OpenLDAP Public License

Version 2.8, 17 August 2003



Redistribution and use of this software and associated documentation ("Software"), with or without modification, are permitted provided that the following conditions are met:

1. Redistributions in source form must retain copyright statements and notices,
2. Redistributions in binary form must reproduce applicable copyright statements and notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution, and
3. Redistributions must contain a verbatim copy of this document.

The OpenLDAP Foundation may revise this license from time to time. Each revision is distinguished by a version number. You may use this Software under terms of this license revision or under the terms of any subsequent revision of the license.

THIS SOFTWARE IS PROVIDED BY THE OPENLDAP FOUNDATION AND ITS CONTRIBUTORS ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OPENLDAP FOUNDATION, ITS CONTRIBUTORS, OR THE AUTHOR(S) OR OWNER(S) OF THE SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The names of the authors and copyright holders must not be used in advertising or otherwise to promote the sale, use or other dealing in this Software without specific, written prior permission. Title to copyright in this Software shall at all times remain with copyright holders.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

Copyright 1999-2003 The OpenLDAP Foundation, Redwood City, California, USA. All Rights Reserved. Permission to copy and distribute verbatim copies of this document is granted.

M15. OpenSSL

Copyright (c) 1998-2018 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.



6. Redistributions of any form whatsoever must retain the following acknowledgment:

```
"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit
(http://www.openssl.org/)"
```

```
THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED
WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND
FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS
CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR
SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY
THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR
OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE
POSSIBILITY OF SUCH DAMAGE.
```

```
=====
```

```
This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This
product includes software written by Tim Hudson (tjh@cryptsoft.com).
```

```
Original SSLeay License
```

```
-----
```

```
Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
```

```
All rights reserved.
```

```
This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).
```

```
The implementation was written so as to conform with Netscapes SSL.
```

```
This library is free for commercial and non-commercial use as long as the following conditions
are aheared to. The following conditions apply to all code found in this distribution, be it
the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included
with this distribution is covered by the same copyright terms except that the holder is Tim
Hudson (tjh@cryptsoft.com).
```

```
Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be
removed.
```

```
If this package is used in a product, Eric Young should be given attribution as the author of
the parts of the library used.
```

```
This can be in the form of a textual message at program startup or in documentation (online or
textual) provided with the package.
```

```
Redistribution and use in source and binary forms, with or without modification, are permitted
provided that the following conditions are met:
```

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

```
"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"
```

```
The word 'cryptographic' can be left out if the rouines from the library being used are not
cryptographic related :-).
```



4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

```
"This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
```

```
THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
```

```
The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]
```

M16. Oracle Instant Client

Export Controls on the Programs

Selecting the "Accept License Agreement" button is a confirmation of your agreement that you comply, now and during the trial term, with each of the following statements:

-You are not a citizen, national, or resident of, and are not under control of, the government of Cuba, Iran, Sudan, Libya, North Korea, Syria, nor any country to which the United States has prohibited export.

-You will not download or otherwise export or re-export the Programs, directly or indirectly, to the above mentioned countries nor to citizens, nationals or residents of those countries.

-You are not listed on the United States Department of Treasury lists of Specially Designated Nationals, Specially Designated Terrorists, and Specially Designated Narcotic Traffickers, nor are you listed on the United States Department of Commerce Table of Denial Orders.

You will not download or otherwise export or re-export the Programs, directly or indirectly, to persons on the above mentioned lists.

You will not use the Programs for, and will not allow the Programs to be used for, any purposes prohibited by United States law, including, without limitation, for the development, design, manufacture or production of nuclear, chemical or biological weapons of mass destruction.

EXPORT RESTRICTIONS

You agree that U.S. export control laws and other applicable export and import laws govern your use of the programs, including technical data; additional information can be found on Oracle's Global Trade Compliance web site (<http://www.oracle.com/products/export>).

You agree that neither the programs nor any direct product thereof will be exported, directly, or indirectly, in violation of these laws, or will be used for any purpose prohibited by these laws including, without limitation, nuclear, chemical, or biological weapons proliferation.

Oracle Employees: Under no circumstances are Oracle Employees authorized to download software for the purpose of distributing it to customers. Oracle products are available to employees for internal use or demonstration purposes only. In keeping with Oracle's trade compliance obligations under U.S. and applicable multilateral law, failure to comply with this policy could result in disciplinary action up to and including termination.

Note: You are bound by the Oracle Technology Network ("OTN") License Agreement terms. The OTN License Agreement terms also apply to all updates you receive under your Technology Track subscription.



The OTN License Agreement terms below supercede any shrinkwrap license on the OTN Technology Track software CDs and previous OTN License terms (including the Oracle Program License as modified by the OTN Program Use Certificate).

Oracle Technology Network Development and Distribution License Agreement for Instant Client

"We," "us," and "our" refers to Oracle America, Inc. "You" and "your" refers to the individual or entity that wishes to use the Programs from Oracle under this Agreement. "Programs" refers to the Software Products referenced below that you wish to download and use and Program documentation. "License" refers to your right to use the Programs and Program documentation under the terms of this Agreement. The substantive and procedural laws of California govern this Agreement. You and Oracle agree to submit to the exclusive jurisdiction of, and venue in, the courts of San Francisco, San Mateo, or Santa Clara counties in California in any dispute arising out of or relating to this Agreement.

We are willing to license the Programs to you only upon the condition that you accept all of the terms contained in this Agreement. Read the terms carefully and select the "Accept" button at the bottom of the page to confirm your acceptance. If you are not willing to be bound by these terms, select the "Do Not Accept" button and the registration process will not continue.

Software Product

- Instant Client

License Rights

License.

We grant you a non-exclusive right and license to use the Programs solely for your business purposes and development and testing purposes, subject to the terms of this Agreement. You may allow third parties to use the Programs, subject to the terms of this Agreement, provided such third party use is for your business operations only.

Distribution License

We grant you a non-exclusive right and license to distribute the Programs, provided that you do not charge your end users for use of the Programs. Your distribution of such Programs shall at a minimum include the following terms in an executed license agreement between you and the end user that: (1) restrict the use of the Programs to the business operations of the end user; (2) prohibit (a) the end user from assigning, giving, or transferring the Programs or an interest in them to another individual or entity (and if your end user grants a security interest in the Programs, the secured party has no right to use or transfer the Programs); (b) make the Programs available in any manner to any third party for use in the third party's business operations (unless such access is expressly permitted for the specific program license or materials from the services you have acquired); and (c) title to the Programs from passing to the end user or any other party; (3) prohibit the reverse engineering (unless required by law for interoperability), disassembly or decompilation of the Programs and prohibit duplication of the Programs except for a sufficient number of copies of each Program for the end user's licensed use and one copy of each Program media; (4) disclaim, to the extent permitted by applicable law, our liability for any damages, whether direct, indirect, incidental, or consequential, arising from the use of the Programs; (5) require the end user at the termination of the Agreement, to discontinue use and destroy or return to you all copies of the Programs and documentation; (6) prohibit publication of any results of benchmark tests run on the Programs; (7) require the end user to comply fully with all relevant export laws and regulations of the United States and other applicable export and import laws to assure that neither the Programs, nor any direct product thereof, are exported, directly or indirectly, in violation of applicable laws; (8) do not require us to perform any obligations or incur any liability not previously agreed to between you and us; (9) permit you to audit your end user's use of the Programs or to assign your right to audit the end user's use of the Programs to us; (10) designate us as a third party beneficiary of the end user license agreement; (11) include terms consistent with those contained in the sections of this Agreement entitled "Disclaimer of Warranties and Exclusive Remedies," "No Technical Support," "End of Agreement," "Relationship Between the Parties," and "Open Source"; and (11) exclude the application of the Uniform Computer Information Transactions Act.

You may allow your end users to permit third parties to use the Programs on such end user's behalf for the purposes set forth in the end user license agreement, subject to the terms of



such agreement. You shall be financially responsible for all claims and damages to us caused by your failure to include the required contractual terms set forth above in each end user license agreement between you and an end user. We are a third party beneficiary of any end user license agreement between you and the end user, but do not assume any of your obligations thereunder, and you agree that you will not enter into any end user license agreement that excludes us as a third party beneficiary and will inform your end users of our rights.

If you want to use the Programs for any purpose other than as expressly permitted under this Agreement you must contact us to obtain the appropriate license. We may audit your use of the Programs. Program documentation is either shipped with the Programs, or documentation may be accessed online at <http://www.oracle.com/technetwork/indexes/documentation/index.html>.

You agree to: (a) defend and indemnify us against all claims and damages caused by your distribution of the Programs in breach of this Agreement and/or failure to include the required contractual provisions in your end user agreement as stated above; (b) keep executed end user agreements and records of end user information including name, address, date of distribution and identity of Programs distributed; (c) allow us to inspect your end user agreements and records upon request; and, (d) enforce the terms of your end user agreements so as to effect a timely cure of any end user breach, and to notify us of any breach of the terms.

Ownership and Restrictions

We retain all ownership and intellectual property rights in the Programs. You may make a sufficient number of copies of the Programs for the licensed use and one copy of the Programs for backup purposes.

You may not:

- use the Programs for any purpose other than as provided above;
- charge your end users for use of the Programs;
- remove or modify any Program markings or any notice of our proprietary rights;
- assign this agreement or give the Programs, Program access or an interest in the Programs to any individual or entity except as provided under this agreement;
- cause or permit reverse engineering (unless required by law for interoperability), disassembly or decompilation of the Programs;
- disclose results of any Program benchmark tests without our prior consent.

Export

You agree that U.S. export control laws and other applicable export and import laws govern your use of the Programs, including technical data; additional information can be found on Oracle's Global Trade Compliance web site located at <http://www.oracle.com/products/export/index.html>. You agree that neither the Programs nor any direct product thereof will be exported, directly, or indirectly, in violation of these laws, or will be used for any purpose prohibited by these laws including, without limitation, nuclear, chemical, or biological weapons proliferation.

Disclaimer of Warranty and Exclusive Remedies

THE PROGRAMS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. WE FURTHER DISCLAIM ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT.

IN NO EVENT SHALL WE BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, PUNITIVE OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR DATA USE, INCURRED BY YOU OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, EVEN IF WE HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. OUR ENTIRE LIABILITY FOR DAMAGES HEREUNDER SHALL IN NO EVENT EXCEED ONE THOUSAND DOLLARS (U.S. \$1,000).

No Technical Support



Our technical support organization will not provide technical support, phone support, or updates to you or end users for the Programs licensed under this agreement.

Restricted Rights

If you distribute a license to the United States government, the Programs, including documentation, shall be considered commercial computer software and you will place a legend, in addition to applicable copyright notices, on the documentation, and on the media label, substantially similar to the following:

NOTICE OF RESTRICTED RIGHTS

"Programs delivered subject to the DOD FAR Supplement are 'commercial computer software' and use, duplication, and disclosure of the programs, including documentation, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement. Otherwise, programs delivered subject to the Federal Acquisition Regulations are 'restricted computer software' and use, duplication, and disclosure of the programs, including documentation, shall be subject to the restrictions in FAR 52.227-19, Commercial Computer Software-Restricted Rights (June 1987). Oracle Corporation, 500 Oracle Parkway, Redwood City, CA 94065."

End of Agreement

You may terminate this Agreement by destroying all copies of the Programs. We have the right to terminate your right to use the Programs if you fail to comply with any of the terms of this Agreement, in which case you shall destroy all copies of the Programs.

Relationship Between the Parties

The relationship between you and us is that of licensee/licensor. Neither party will represent that it has any authority to assume or create any obligation, express or implied, on behalf of the other party, nor to represent the other party as agent, employee, franchisee, or in any other capacity. Nothing in this Agreement shall be construed to limit either party's right to independently develop or distribute software that is functionally similar to the other party's products, so long as proprietary information of the other party is not included in such software.

Open Source

"Open Source" software - software available without charge for use, modification and distribution - is often licensed under terms that require the user to make the user's modifications to the Open Source software or any software that the user 'combines' with the Open Source software freely available in source code form. If you use Open Source software in conjunction with the Programs, you must ensure that your use does not: (i) create, or purport to create, obligations of us with respect to the Oracle Programs; or (ii) grant, or purport to grant, to any third party any rights to or immunities under our intellectual property or proprietary rights in the Oracle Programs. For example, you may not develop a software program using an Oracle Program and an Open Source program where such use results in a program file(s) that contains code from both the Oracle Program and the Open Source program (including without limitation libraries) if the Open Source program is licensed under a license that requires any "modifications" be made freely available. You also may not combine the Oracle Program with programs licensed under the GNU General Public License ("GPL") in any manner that could cause, or could be interpreted or asserted to cause, the Oracle Program or any modifications thereto to become subject to the terms of the GPL.

Entire Agreement

You agree that this Agreement is the complete agreement for the Programs and licenses, and this Agreement supersedes all prior or contemporaneous Agreements or representations. If any term of this Agreement is found to be invalid or unenforceable, the remaining provisions will remain effective.

Last updated: 01/24/08



M17. ParaType Free Font

LICENSING AGREEMENT

for the fonts with Original Name: PT Sans, PT Serif, PT Mono

Version 1.3 - January 20, 2012

GRANT OF LICENSE

ParaType Ltd grants you the right to use, copy, modify the fonts and distribute modified and unmodified copies of the fonts by any means, including placing on Web servers for free downloading, embedding in documents and Web pages, bundling with commercial and non commercial products, if it does not conflict with the conditions listed below:

- You may bundle the fonts with commercial software, but you may not sell the fonts by themselves. They are free.
- You may distribute the fonts in modified or unmodified versions only together with this Licensing Agreement and with above copyright notice. You have no right to modify the text of Licensing Agreement. It can be placed in a separate text file or inserted into the font file, but it must be easily viewed by users.
- You may not distribute modified version of the font under the Original name or a combination of Original name with any other words without explicit written permission from ParaType.

TERMINATION & TERRITORY

This license has no limits on time and territory, but it becomes null and void if any of the above conditions are not met.

DISCLAIMER

THE FONT SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF COPYRIGHT, PATENT, TRADEMARK, OR OTHER RIGHT. IN NO EVENT SHALL PARATYPE BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, INCLUDING ANY GENERAL, SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF THE USE OR INABILITY TO USE THE FONT SOFTWARE OR FROM OTHER DEALINGS IN THE FONT SOFTWARE.

ParaType Ltd

M18. PCRE

PCRE2 is a library of functions to support regular expressions whose syntax and semantics are as close as possible to those of the Perl 5 language.

Release 10 of PCRE2 is distributed under the terms of the "BSD" licence, as specified below, with one exemption for certain binary redistributions. The documentation for PCRE2, supplied in the "doc" directory, is distributed under the same terms as the software itself. The data in the testdata directory is not copyrighted and is in the public domain.

The basic library functions are written in C and are freestanding. Also included in the distribution is a just-in-time compiler that can be used to optimize pattern matching. This is an optional feature that can be omitted when the library is built.

THE BASIC LIBRARY FUNCTIONS



Written by: Philip Hazel
Email local part: ph10
Email domain: cam.ac.uk
University of Cambridge Computing Service,
Cambridge, England.
Copyright (c) 1997-2018 University of Cambridge
All rights reserved.

PCRE2 JUST-IN-TIME COMPILATION SUPPORT

Written by: Zoltan Herczeg
Email local part: hzmester
Email domain: freemail.hu
Copyright (c) 2010-2018 Zoltan Herczeg
All rights reserved.

STACK-LESS JUST-IN-TIME COMPILER

Written by: Zoltan Herczeg
Email local part: hzmester
Email domain: freemail.hu
Copyright (c) 2009-2018 Zoltan Herczeg
All rights reserved.

THE "BSD" LICENCE

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notices, this list of
conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notices, this list of
conditions and the following disclaimer in the documentation and/or other materials provided
with the distribution.

* Neither the name of the University of Cambridge nor the names of any contributors may be
used to endorse or promote products derived from this software without specific prior
written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR
IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY



AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

EXEMPTION FOR BINARY LIBRARY-LIKE PACKAGES

The second condition in the BSD licence (covering binary redistributions) does not apply all the way down a chain of software. If binary package A includes PCRE2, it must respect the condition, but if package B is software that includes package A, the condition is not imposed on package B unless it uses PCRE2 independently.

M19. Script.aculo.us

Copyright © 2005-2008 Thomas Fuchs (<http://script.aculo.us>, <http://mir.aculo.us>)

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

M20. Zlib

zlib.h -- interface of the 'zlib' general purpose compression library

version 1.2.11, January 15th, 2017

Copyright (C) 1995-2017 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.



Jean-loup Gailly

Mark Adler

jloup@gzip.org

madler@alumni.caltech.edu



第3章: よくある質問

他のコンピューターにDr.Web Serverを移動する (Windows OS環境)



サーバーを他のコンピューターに移動した後はトランスポートプロトコル設定を確認してください。必要に応じ、管理 → **Dr.Web Server**の設定 セクションの トランスポート タブで該当する設定を変更します。



Dr.Web Serverを起動、停止する方法は、管理者マニュアルの[Dr.Web Serverの起動と停止](#)に記載されています。

Windows環境のDr.Web Serverを(同じバージョンのDr.Web Serverに)移動するには

1. サーバーを停止します。
2. `exportdb`スイッチを使用して`drwcsd.exe`実行し、データベースの中身をファイルにエクスポートします。コマンドライン(Windows向け)は、次のようになります。

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -log=drwcsd.log exportdb  
<full_filename>
```

3. `C:\Program Files\DrWeb Server\etc`フォルダと`drwcsd.pub`キーを`\Program Files\DrWeb Server\webmin\install`フォルダからバックアップします。
4. Dr.Web Serverソフトウェアを削除します。
5. 必要なコンピューターに新しいサーバー(新しい空のDBを持つ)をインストールします。Windows OSサービスの管理ツール、またはDr.Web Security Control Centerからサーバーを停止します。
6. 自動で保存された`etc`フォルダを`C:\Program Files\DrWeb Server\etc`フォルダに、`drwcsd.pub`キーと`drwcsd-certificate.pem`証明書を`C:\Program Files\DrWeb Server\webmin\install`フォルダにコピーします。
7. `importdb`スイッチを使用して`drwcsd.exe`実行し、ファイルからデータベースのコンテンツをインポートします。コマンドライン(Windows向け)は、次のようになります。

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -log=drwcsd.log importdb  
<full_filename>
```

8. Serverを起動します。



内部DBを使用している場合は、DBのエクスポートおよびインポートは必要ありません。ただ、`database.sqlite`ファイルを保存して、インストールしたサーバーで、前のバージョンのサーバーからの古いDBファイルと新しいDBファイルを置き換えてください。

Windows環境のDr.Web Serverを移動するには(異なるバージョンのDr.Web Serverに)

1. サーバーを停止します。



2. SQL Server ツール経由でデータベースを保存します(内部DBを使用している場合はdatabase.sqlite ファイルの保存のみを行ってください)。
3. C:\Program Files\DrWeb Server\etcフォルダとdrwcsd.pubキーを\Program Files\DrWeb Server\webmin\installフォルダからバックアップします。
4. Dr.Web Serverソフトウェアを削除します。
5. 必要なコンピューターに新しいサーバー(新しい空のDBを持つ)をインストールします。Windows OSサービスの管理ツール、またはDr.Web Security Control Centerからサーバーを停止します。
6. 自動で保存されたetcフォルダをC:\Program Files\DrWeb Server\etcフォルダに、drwcsd.pubキーとdrwcsd-certificate.pem証明書をC:\Program Files\DrWeb Server\webmin\installフォルダにコピーします。
7. 新しいサーバー上でDBを復元し、drwcsd.conf設定ファイル内でDBへのパスを指定します。
8. upgradedbスイッチを使用してdrwcsd.exeを実行し、データベースを更新します。コマンドライン(Windows向け)は、次のようになります。

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -log=drwcsd.log upgradedb  
"C:\Program Files\DrWeb Server\update-db"
```

9. Serverを起動します。

移動中にDr.Web Serverの名前またはIPアドレスが変更された場合:



新しいサーバーのアドレスをControl Center経由で設定し、端末のAgent設定に反映されていないAgentを移動させるには、移動が完了するまで両方のサーバーを動作させたままにしてください。

1. 上の該当する手順に従ってサーバーを移動します。
2. 移動したServerに接続する全てのAgentに対し、新しいServerのアドレスを指定します([Dr.Web Agentを他のDr.Web Serverに接続する参照](#))。
新しいサーバーのアドレスをControl Center経由で設定し、端末のAgent設定に反映されていないAgentを移動する場合、両方のサーバー上のAgent設定内で、新しいサーバーIPアドレスを指定する必要があります。
3. Agentが新しいサーバーに接続されるまで待ちます。その後、古いサーバーを削除できます。



Dr.Web Agentを他のDr.Web Serverに接続する

Agentを他のサーバーに接続するには、次の方法があります。

1. Control Center経由

端末が以前のサーバーに接続されている場合、端末上で直接操作することなくリモートでの管理が可能です。この場合、新しいサーバーと古いサーバーの両方のControl Centerへのアクセスが必要です。

2. 端末上で直接

端末上で直接操作を実行する場合、端末での管理者権限とAgentプロパティを編集する権限(サーバー上で設定)が必要です。これらの権限がない場合、インストールされているAgentを削除し、新しいサーバー設定で新たにAgentをインストールした後でのみ、端末上で直接他のサーバーにローカル接続できるようになります。ローカルでAgentをアンインストールする権限がない場合、端末上でDr.Web Remover ユーティリティを使用するか、Control CenterからAgentを削除します。

Control Center経由でDr.Web Agentを他のDr.Web Serverに再接続する

1. 新しいサーバーで、不正な認証パラメータが設定されている端末が新規端末として新しい認証パラメータを要求できるようにします。これを実行するには、Control Centerで、メインメニューの **管理** → **コントロールメニュー** の **Dr.Web Server設定** → **全般** タブの順に選択します。
 - a) **未承認新規アイテムをリセットする** にチェックを入れます(チェックが入っていない場合)。
 - b) **新規アイテム登録** ドロップダウンリストで **常にアクセスを拒否する** が選択されている場合、**手動でアクセスを承認する** または **自動的にアクセスを許可する** に変更します。
 - c) これらの設定を適用するには **保存** をクリックし、サーバーを再起動します。



手順1の設定変更が企業のポリシーによって許可されていない場合、Control Centerであらかじめ作成されているアカウントに応じて端末上で直接、端末認証のパラメータを設定する必要があります。

2. Agentが接続されている古いサーバーで、新しいサーバーのパラメータを設定します。これを設定するには、Control Centerのメインメニューで、**アンチウイルスネットワーク** → **ネットワークの階層リスト**で使用する端末(またはこのグループのすべての端末を再接続するグループ)を選択 → **コントロールメニュー**で、**接続設定** を選択します。
 - a) 新しいサーバー証明書が、以前のサーバー証明書と一致しない場合は、**証明書** フィールドに新しいサーバー証明書へのパスを設定します。
 - b) **サーバー** フィールドで新しいサーバーのアドレスを指定します。
 - c) **保存** をクリックします。

端末上でDr.Web Agentを直接他のDr.Web Serverに再接続する

1. Agent設定で新しいサーバーのパラメータを設定します。これを設定するには、Agentアイコンのコンテキストメニューで、**設定** → **メイン** タブ → **サーバー** → **接続パラメータセクション** → **設定を変更** ボタンを選択します。
 - a) 新しいサーバー証明書が、以前のサーバー証明書と一致しない場合、**証明書のリスト** ボタンを使用して新しいサーバー証明書へのパスを設定します。
 - b) **追加** ボタンで、該当する新しいサーバーのパラメータを設定します。
2. 端末を新規端末として設定します(サーバーの認証パラメータをリセットします)。これを実行するには、手順1の**接続設定セクション**で、**端末接続パラメータ** ボタン → **パラメータをリセットして新規端末として接続** ボタン → **パラメータをリセット** ボタンの順にクリックします。



すでに新しいサーバーを接続するためのIDとパスワードがわかっている場合は、**端末ID**とパスワードフィールドに入力します。この場合、端末を新規端末にする必要はありません。



Dr.Web Enterprise Security SuiteのDBMSの種類の変更

Windows OSの場合



Dr.Web Serverを起動、停止する方法は、管理者マニュアルの[Dr.Web Serverの起動と停止](#)に記載されています。

1. Dr.Web Serverを停止します。
2. `exportdb`スイッチを使用して`drwcsd.exe`実行し、データベースの中身をファイルにエクスポートします。コマンドライン(Windows向け)は、次のようになります。

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -verbosity=all -log=drwcsd.log exportdb D:\esbase.es
```

上記の例では、Dr.Web Serverは、C:\Program Files\DrWeb Serverフォルダにインストールされ、データベースは、ディスクDのルートにある`esbase.es`ファイルにエクスポートされていると想定しています。

ファイルへのパス(またはファイル名)にスペース、またはアルファベット以外の文字が含まれている場合、パスは引用符で囲まれている必要があります。

```
"D:\<long name>\esbase.es"
```

3. Dr.Web Serverを起動し、Dr.Web Security Control Centerをサーバーに接続します。他のDBMSを使うようにサーバーを設定します。サーバーの再起動をキャンセルします。
4. Dr.Web Serverを停止します。
5. データベースファイルを削除します。
6. `initdb`スイッチを使用して`drwcsd.exe`を実行し、新しいデータベースを初期化します。コマンドラインは次のようになります。

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -verbosity=all -log=drwcsd.log -- initdb D:\Keys\agent.key -- root
```

上の例では、サーバーがC:\Program Files\DrWeb Serverフォルダにインストールされ、`agent.key`はD:\Keysに格納されていると想定しています。

ファイルへのパス(またはファイル名)にスペース、またはアルファベット以外の文字が含まれている場合、キーへのパスは引用符で囲まれている必要があります。

```
"D:\<long name>\agent.key"
```

7. `importdb`スイッチを使用して`drwcsd.exe`を実行し、ファイルからデータベースをインポートします。コマンドラインは次のようになります。

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -verbosity=all -log=drwcsd.log importdb D:\esbase.es
```

8. Dr.Web Serverを起動します。



UNIXの場合

1. スクリプトを使用してDr.Web Serverを停止します。

- **Linux:**

```
/etc/init.d/drwcsd stop
```

- **FreeBSDの場合:**

```
/usr/local/etc/rc.d/drwcsd stop
```

またはDr.Web Security Control Center経由。

2. `exportdb`スイッチを使用してサーバーを起動し、ファイルにデータベースをエクスポートします。サーバーインストールフォルダからのコマンドラインは次のようになります。

- **Linux:**

```
/etc/init.d/drwcsd -log=drwcsd.log exportdb /var/esbase.es
```

- **FreeBSD:**

```
/usr/local/etc/rc.d/drwcsd -log=drwcsd.log exportdb /var/drwcs/esbase.es
```

上の例では、データベースは指定されたフォルダ内にある`esbase.es`にエクスポートされていると想定しています。

3. スクリプトを使用してDr.Web Serverを起動します。

- **Linux:**

```
/etc/init.d/drwcsd start
```

- **FreeBSD:**

```
/usr/local/etc/rc.d/drwcsd start
```

Dr.Web Security Control Centerをサーバーに接続し、他のデータベースを使用するようDr.Web Security Control Centerからサーバーを設定します。次のようにします: **管理** → **Dr.Web Serverの設定** → **データベース タブ**



また、サーバー設定ファイル`drwcsd.conf`を直接編集して他のデータベース/DBMSを使用するようにサーバーを再設定することもできます。これを行うには、現在のデータベースに関するエントリをコメントにするか削除し、新しいデータベースを入力する必要があります(詳細については、[付録G1. Dr.Web Server設定ファイル](#)を参照)。

サーバーを再起動するよう促されますが、キャンセルします。

4. Dr.Web Serverを停止します(手順1参照)。
5. データベースファイルを削除します。
6. `initdb`スイッチを使用して`drwcsd`を実行し、新しいデータベースを初期化します。コマンドラインは次のようになります。

- **Linux:**



```
/etc/init.d/drwcsd -log=drwcsd.log initdb
```

- **FreeBSD:**

```
/usr/local/etc/rc.d/drwcsd -log=drwcsd.log initdb
```

7. 上の例では、`agent.key`は`/root/keys`フォルダーにあると想定しています。`importdb`スイッチを使用して`drwcsd`を実行し、ファイルからデータベースをインポートします。コマンドラインは次のようになります。

- **Linux:**

```
/etc/init.d/drwcsd -log=drwcsd.log importdb /var/esbase.es
```

- **FreeBSD:**

```
/usr/local/etc/rc.d/drwcsd -log=drwcsd.log importdb /var/esbase.es
```

8. Dr.Web Serverを起動します(手順3参照)。



サーバー起動時にパラメータを変更する場合(サーバーインストールフォルダの指定、ログレベルの変更など)、起動スクリプトを編集する必要があります。

- **FreeBSD:**

```
/usr/local/etc/rc.d/drwcsd
```

- **Linux:**

```
/etc/init.d/drwcsd
```



Dr.Web Enterprise Security Suiteのデータベースの復元

操作の実行中に、Dr.Web Server は重要な情報(ライセンスキー、データベースコンテンツ、プライベート暗号化キー、サーバー設定、Control Center設定)のバックアップコピーを定期的に保存します。

バックアップファイルは以下のフォルダに保存されます。

- **Windows OS**の場合: `<installation_drive>:\DrWeb Backup`
- **Linux OS**の場合: `/var/opt/drwcs/backup`
- **FreeBSD OS**の場合: `/var/drwcs/backup`

バックアップを実行するために、daily taskがサーバースケジュールに含まれています。このようなタスクがスケジュールにない場合は、作成することを強く推奨します。

データベースのコンテンツを除くバックアップの全てのファイルは、すぐに使用できます。データベースバックアップのコピーはgzipやその他のアーカイバで解凍可能な.gzフォーマットで保存されます。データベースのコンテンツは、バックアップのコピーからサーバーの別のデータベースにインポートできます。importdb コマンドを使用すると、データを復元できます。



データベースの復元には、Control Centerの **管理** → **データベースの管理** → **エクスポート** から管理者が手動で作成したバックアップを使用することも可能です(データベース全体をエクスポートモードのみ)。ただし、その場合、バックアップコピーはxml形式で保存され、インポートするにはxmlimportdbコマンドを使用する必要があります。

異なるバージョンのDr.Web ServerのDBの復元



バックアップコピーからDBを復元することができるのは、復元に使用するサーバーのバージョンと同じメジャーバージョンのサーバー経由でコピーが作成された場合のみになります。

例:

- バージョン12のサーバー経由で作成されたバックアップからDBを復元できるのは、バージョン12のサーバーを使用した場合のみです。
- バージョン12のサーバーを使用して、以前のバージョンのサーバー経由で作成されたバックアップからDBを復元することはできません。

以前のバージョンからバージョン12.0へのサーバーのアップグレード中に、何らかの理由でDBが破損した場合は以下の手順を実行します。

1. バージョン12.0のサーバーソフトウェアを削除します。サーバーが使用していたファイルのバックアップコピーは自動的に保存されます。
2. アップグレード前にインストールされており、バックアップコピーの作成に使用されたバージョンのサーバーをインストールします。
一般的なアップグレード手順に従い、DBファイルを除く全ての保存されたサーバーファイルを使用する必要があります。
サーバーインストール中に新しいDBを作成します。
3. 一般的なルールに従ってバックアップからDBを復元します([以下](#)の手順参照)。



4. サーバー設定で、Agent、サーバー、ネットワークインストーラのプロトコルを無効にします。これを行うには、メインメニューの **管理** 項目を選択し、コントロールメニューで **Dr.Web Serverの設定** をクリックし、モジュール タブに移動し、該当する項目のチェックをクリアします。
5. 一般的なルールに従って、サーバーをバージョン12.0にアップグレードします(管理者マニュアルの[Dr.Web Enterprise Security Suite ソフトウェアおよびコンポーネントの更新](#)参照)。
6. 手順4で無効にしたAgent、サーバー、ネットワークインストーラのプロトコルを有効にします。

Windows OSの場合



Dr.Web Serverを起動、停止する方法は、管理者マニュアルの[Dr.Web Serverの起動と停止](#)に記載されています。

DBをバックアップから復元するには

1. Dr.Web Serverが起動している場合は停止します。
2. 該当するバックアップファイルからデータベースのコンテンツをインポートします。コマンドラインは次のようになります。

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -verbosity=all -log=drwcsd.log importdb "<path_to_the_backup_file>\database.gz"
```

コマンドは一行で入力する必要があります。上の例では、Dr.Web ServerがC:\Program Files\DrWeb Serverフォルダにインストールされています。

3. Dr.Web Serverを起動します。

Dr.Web Serverのバージョンを変更した場合、または前のバージョンのDBが破損した場合にバックアップからDBを復元するには

1. Dr.Web Serverが起動している場合は停止します。
2. 現在のDBを削除します。方法は次のとおりです。

2.1. 内部DBの場合:

- a) database.sqliteファイルを削除します。
- b) 新しいデータベースを初期化します。Windowsでは、コマンドラインは次のようになります。

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -verbosity=all -log=drwcsd.log -- initdb D:\Keys\agent.key - -<password>
```

コマンドは一行で入力する必要があります(付録[H3.3. データベースコマンド](#)でinitdbスイッチを使用したdrwcsdコマンドフォーマットを参照してください)。上の例では、Dr.Web ServerがC:\Program Files\DrWeb Serverフォルダにインストールされており、agent.keyライセンスキーはD:\Keys内にあります。

- c) このコマンドが実行されると、Dr.Web Serverインストールフォルダのvarサブフォルダ内に新しいdatabase.sqliteが作成されます。



- 2.2. 外部DBの場合:cleandbコマンド経由でDBをクリーンアップします(付録H3.3. データベースコマンドを参照)。
3. 該当するバックアップファイルからデータベースのコンテンツをインポートします。コマンドラインは次のようになります。

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -verbosity=all -log=drwcsd.log importdb "<path_to_the_backup_file>\database.gz"
```

コマンドは一行で入力する必要があります。上の例では、サーバーはC:\Program Files\DrWeb Serverフォルダにインストールされています。

4. Dr.Web Serverを起動します。

UNIXの場合

1. Dr.Web Serverを停止します(起動している場合)。

- **Linuxの場合:**

```
/etc/init.d/drwcsd stop
```

- **FreeBSDの場合:**

```
/usr/local/etc/rc.d/drwcsd stop
```

2. Dr.Web Serverインストールフォルダの以下のサブフォルダからdatabase.sqlite を削除します。

- **Linux:** /var/opt/drwcs/
- **FreeBSD:** /var/drwcs/



外部DBをクリーンアップするには、cleandbコマンドを使用します(付録H3.3. データベースコマンドを参照)。

3. サーバーデータベースを初期化します。コマンドは次のようになります。

- **Linux:**

```
/etc/init.d/drwcsd -log=drwcsd.log initdb
```

- **FreeBSD:**

```
/usr/local/etc/rc.d/drwcsd -log=drwcsd.log initdb
```

4. このコマンドが実行されると、Dr.Web Serverインストールフォルダのvarサブフォルダ内に新しいdatabase.sqliteデータベースが作成されます。
5. 該当するバックアップファイルからデータベースのコンテンツをインポートします。コマンドラインは次のようになります。

- **Linux:**

```
/etc/init.d/drwcsd -log=drwcsd.log importdb  
"<path_to_the_backup_file>/database.gz"
```



- **FreeBSD:**

```
/usr/local/etc/rc.d/drwcsd -log=drwcsd.log importdb  
"<path_to_the_backup_file>/database.gz"
```

6. Dr.Web Serverを起動します。

- **Linux:**

```
/etc/init.d/drwcsd start
```

- **FreeBSD:**

```
/usr/local/etc/rc.d/drwcsd start
```



パラメータを指定してスクリプトを実行する場合(サーバーインストールディレクトリの設定など)、全ての変更を起動スクリプト内で行う必要があります。

- FreeBSD OSの場合: /usr/local/etc/rc.d/drwcsd
- Linux OSの場合: /etc/init.d/drwcsd

サーバーのログ詳細レベルを変更する必要がある場合は、local.confファイルを使用します。

- Linux OSの場合: /var/opt/drwcs/etc/local.conf
- FreeBSD OSの場合: /var/drwcs/etc/local.conf

最後にバックアップが行われた後にインストールされたAgentは、データベースがバックアップから復元された後、サーバーには接続されません。リモートでAgentを新規端末モードにリセットする必要があります。全般 タブで、管理 → **Dr.Web Server設定** に移動し、未承認の端末を新規端末にリセットにチェックを入れ、新規端末登録モードのドロップダウンリストから、アクセスを自動的に許可する を選択します。保存 をクリックしてサーバーを再起動します。

全ての端末が新しいサーバーに接続された後、これらのサーバー設定をご自身の企業のポリシーに合わせて変更します。

データベースがバックアップから復元されたら、すぐにDr.Web Security Control Centerをサーバーに接続することを推奨します。管理 メニューで、**Dr.Web Server Task Scheduler** を選択し、クリティカルなサーバーデータのバックアップ タスクがリストにあることを確認します。このタスクがスケジュールに存在しない場合は、リストに追加します。



LANサーバー上のDr.Web Agentのアップグレード

LANサーバー上にインストールされたAgentをアップグレードする場合、端末の再起動やそれらの端末上にあるネットワークソフトウェアの停止は望ましくない場合があります。

重要なネットワーク機能を実行する端末の機能のダウンタイムを避けるため、Agentおよびアンチウイルスソフトウェアの次のモードでのアップグレードを推奨します。

1. サーバースケジュール内で標準ジョブを、全てのコンポーネントをアップグレードするものからウイルスベースのみをアップグレードするように変更します。
2. LANサーバーの機能に支障を与えない適切な時間に全てのコンポーネントをアップグレードするという新しいジョブを作成します。

サーバースケジュールのタスクの作成および編集方法は、[管理者マニュアルのDr.Web Serverスケジュールの設定](#)セクションを参照してください。



重要なネットワーク機能を司るサーバー上(ドメインコントローラ、ライセンスサーバーなど)へのSpIDer Gate、SpIDer Mail、Dr.Web Firewallコンポーネントのインストールは、ネットワークサービスとDr.Webアンチウイルス内部コンポーネント間で起こり得る競合を避ける意味で推奨できません。



Dr.Web Enterprise Security Suite 管理者のパスワードの復元

Dr.Web Serverにアクセスするための管理者パスワードを紛失した場合、Server DBに直接アクセスすることで確認または変更を行うことができます。

- a) 内部DB: 管理者パスワードを確認、変更するには、サーバーディストリビューションキットに含まれている drwidbsh3ユーティリティを使用します([H7.2. 内部データベースの管理ユーティリティ](#)を参照)。
- b) 外部DBの場合: 対応するSQLクライアントを使用します。



管理者アカウントのパラメータはadminsテーブル内にあります。

drwidbsh3ユーティリティの使用例:

1. drwidbsh3ユーティリティを実行し、DBファイルへのパスを指定します。

- Linux環境での内部DBの場合:

```
/opt/drwcs/bin/drwidbsh3 /var/opt/drwcs/database.sqlite
```

- Windows OS環境での内部DBの場合:

```
"C:\Program Files\DrWeb Server\bin\drwidbsh3" "C:\Program Files\DrWeb Server\var\database.sqlite"
```



古いIntDBフォーマットの内部データベースを使用する場合(バージョン6からサーバーをアップグレードする場合など)、デフォルトのデータベース名はdbinternal.dbs、データベース管理ユーティリティは drwidbsh になります。

2. adminsテーブルの全てのデータを見るには次のコマンドを実行します。

```
select * from admins;
```

3. 全ての管理アカウントのログインおよびパスワードを見るには次のコマンドを実行します。

```
select login,password from admins;
```

4. adminの名前を持つアカウントが1つのみで、パスワードがrootである場合、結果は以下のようになります。

```
sqlite> select login,password from admins;
admin|root
sqlite> █
```

5. パスワードを変更するには、updateコマンドを使用します。次の例では、コマンドによりadminアカウントのパスワードをqwertyに変更しています。

```
update admins set password='qwerty' where login='admin';
```

6. drwidbsh3ユーティリティを終了するには次のコマンドを実行します。



```
.exit
```

druidbsh3ユーティリティの説明は、付録[H7.2. 内部データベースの管理ユーティリティ](#)に記載されています。



Active Directory経由でのAgentインストールにおけるDFSの使用

Active Directoryサービス経由でのDr.Web Agentインストールの際にDistributed File System (DFS)を使用できます。

LAN内に複数のドメインコントローラがある場合などに便利です。

複数のドメインコントローラを持つLANにDr.Web Agentをインストールする場合

1. 各ドメインコントローラ上に、同じ名前を持つディレクトリを作成します。
2. 作成したディレクトリをDFS経由で1つのルートターゲットディレクトリに統合します。
3. 作成したターゲットディレクトリへの*.msiパッケージの管理インストールを実行します(インストールマニュアルの[Active Directory経由でのDr.Web Agentソフトウェアのインストール](#)を参照)。
4. パッケージ割り当ての際にグループポリシーオブジェクトエディタ内でこのターゲットディレクトリを使用します。
次のようなネットワークアドレスを使用します\\ <domain>\ <folder>
<domain> はドメイン名、<folder> はターゲットディレクトリの名前が入ります。



Dr.Web Server故障後のアンチウイルスネットワークの復元

Dr.Web Serverに重大な障害が発生した場合、端末上にAgentを再インストールすることなく、以下の手順でアンチウイルスネットワークの動作を復元することをお勧めします。



新しいDr.Web Serverは同じIPアドレスとDNS名でコンピューターにインストールされることが前提です。

Dr.Web Serverのバックアップから復元する

操作の実行中に、Dr.Web Serverは重要な情報(ライセンスキー、データベースコンテンツ、プライベート暗号化キー、Server設定、Control Center設定)のバックアップコピーを定期的に保存します。

バックアップファイルは以下のフォルダに保存されます。

- **Windows OS**の場合: `<installation_drive>:\DrWeb Backup`
- **Linux OS**の場合: `/var/opt/drwcs/backup`
- **FreeBSD OS**の場合: `/var/drwcs/backup`

バックアップを実行するために、daily taskがServerスケジュールに含まれています。このようなタスクがスケジュールにない場合は、作成することを強く推奨します。

データベースのコンテンツを除くバックアップの全てのファイルは、すぐに使用できます。データベースバックアップのコピーはgzipやその他のアーカイブで解凍可能な.gzフォーマットで保存されます。upimportdbコマンドを使用して、データベースのコンテンツをバックアップコピーからServerの他のデータベースにインポートし、データを復元できます。



データベースの復元には、Control Centerの **管理** → **データベースの管理** → **エクスポート** から管理者が手動で作成したバックアップを使用することも可能です(データベース全体をエクスポートモードのみ)。ただし、この時にバックアップコピーはXMLフォーマットで保存されるため、インポートするにはxmlupimportdbコマンドを使用する必要があります。

また、作成したバックアップのコピーとその他の重要なファイルを別のコンピューターに保存しておくことをお勧めします。そうすることで、Dr.Web Serverがインストールされているコンピューターが故障した場合に、データを失うことなく、データとServerの機能を完全に復元できます。ライセンスキーを紛失した場合は、再度申請できます。管理者マニュアルの[ライセンス](#)を参照してください。

バックアップが利用可能な場合に、障害発生後にServerを復元する

1. 新しいDr.Web Serverをインストールするコンピューターを選択します。そのコンピューターを動作中のAgentから隔離します(Agentがインストールされているネットワークからそのコンピューターを切断するか、コンピューターのIPアドレスを一時的に変更、またはその他の方法を使用してください)。
2. 新しいDr.Web Serverをインストールします。
3. **管理** → **ライセンスマネージャー** セクションで、前回のServerインストール時のライセンスキーを追加し、該当するグループ、中でも特に**Everyone**グループに対して配信します。ライセンスキーがServerのインストール時に設定されていない場合、この手順は必須です。
4. インストールしたServerのリポジトリをGUSから更新します。
 - a) Control Centerの **管理** → **リポジトリの状態** セクションを開きます。



- b) **更新を確認** ボタンをクリックして、全ての製品に対し、GUSサーバーに利用可能な更新があるかどうかを確認し、更新がある場合には更新をダウンロードします。
5. 新しいバージョンのServerソフトウェアが利用可能な場合は、最新バージョンに更新します。
- a) Control Centerの **管理** → **Dr.Web Server** セクションを開きます。
- b) Serverバージョンのリストを開くには、Serverの現在のバージョンをクリックするか、**バージョンリスト** ボタンをクリックします。利用可能なServerの更新とバックアップのリストが含まれた **Dr.Web Serverの更新** セクションが開きます。
- c) Serverソフトウェアを更新するには、**全てのバージョン** リスト内の最新のバージョンの横にあるオプションを設定します。**保存** をクリックします。
- d) Serverの更新が完了するまで待ちます。
6. Serverを停止します。
7. プライベートキーのバックアップからパブリック暗号化キーを取得するには、Serverインストールフォルダの\binサブフォルダにあるdrwsignユーティリティを使用します。

```
drwsign extract [-private-key=<private_key>] <public_key>
```

<private_key>および<public_key>については、プライベートキーのある場所と作成するパブリックキーを格納する場所へのパスをそれぞれ指定します。

8. Serverのクリティカルなデータをバックアップに保存したものと置き換えます。

OS	パブリック暗号化キー	設定ファイル
Windows	Serverインストールフォルダのwebmin\install	Serverインストールフォルダのetcフォルダ
Linux	/opt/drwcs/webmin/install	/var/opt/drwcs/etc
FreeBSD	/usr/local/drwcs/webmin/install	/var/drwcs/etc

9. データベースの設定を行います。

- a) 外部データベース:

データベースをServerに接続するためのさらなる操作は必要ありません (Serverの設定ファイルが保存されている場合のみ)。

最後の更新時にインストールされたServerのバージョンが故障したServerのものよりも新しい場合、upgradedbコマンドを介して外部データベースを更新します。

- Windows OS:

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -log=drwcsd.log  
upgradedb
```

- Linux OS:

```
/etc/init.d/drwcsd -log=drwcsd.log upgradedb
```

- FreeBSD OS:

```
/usr/local/etc/rc.d/drwcsd -log=drwcsd.log upgradedb
```

- b) 外部または組み込みデータベースのバックアップ:



外部データベースの場合は、cleandbコマンドを使用して、事前にクリーンアップします(付録H3.3. [データベースコマンド](#)を参照)。

upimportdbコマンドを使用して、該当するバックアップファイルから、インストールされたServerのバージョンに更新されたデータベースフォーマットでデータベースのコンテンツをインポートします。

- Windows OS:

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -verbosity=all -log=drwcsd.log upimportdb  
"<path_to_the_backup_file>\database.gz"
```

- Linux OS:

```
/etc/init.d/drwcsd -log=drwcsd.log upimportdb  
"<path_to_the_backup_file>/database.gz"
```

- FreeBSD OS:

```
/usr/local/etc/rc.d/drwcsd -log=drwcsd.log upimportdb  
"<path_to_the_backup_file>/database.gz"
```



置き換えられた全てのファイルには、前回の(故障した)Serverインストール時にセットされたものと同じパーミッションを割り当ててください。

UNIX系OS: drwcs:drwcs:rw

10. Serverを起動します。

11. データベースバックアップからのデータが保存されていて、現在も有効なものであること(Agent設定、アンチウイルスネットワークツリーの状態など)を確認してください。

12. 手順1で選択したServerの隔離方法に応じて、AgentからServerへのアクセスを復元します。



最後にバックアップが行われた後にインストールされたAgentは、データベースがバックアップから復元された後、Serverには接続されません。リモートでAgentを新規端末モードにリセットする必要があります。全般 タブで、管理 → **Dr.Web Server**設定 に移動し、未承認の端末を新規端末にリセットにチェックを入れ、**新規端末登録モード**のドロップダウンリストから、**アクセスを自動的に許可する**を選択します。保存 をクリックしてServerを再起動します。

全ての端末が新しいServerに接続された後、これらのServer設定をご自身の企業のポリシーに合わせて変更します。

Dr.Web Serverのバックアップが無い状態での復元

バックアップが保存されていない場合に、障害発生後にServerを復元する

1. 新しいDr.Web Serverをインストールするコンピューターを選択します。そのコンピューターを動作中のAgentから隔離します(Agentがインストールされているネットワークからそのコンピューターを切断するか、コンピューターのIPアドレスを一時的に変更、またはその他の方法を使用してください)。
2. 新しいDr.Web Serverをインストールします。



3. 管理 → ライセンスマネージャー セクションで、前回のServerインストール時のライセンスキーを追加し、該当するグループ、中でも特に**Everyone**グループに対して配信します。ライセンスキーがServerのインストール時に設定されていない場合、この手順は必須です。
4. インストールしたServerのリポジトリをGUSから更新します。
 - a) Control Centerの **管理** → **リポジトリの状態** セクションを開きます。
 - b) **更新を確認** ボタンをクリックして、全ての製品に対し、GUSサーバーに利用可能な更新があるかどうかを確認し、更新がある場合には更新をダウンロードします。
5. 新しいバージョンのServerソフトウェアが利用可能な場合は、最新バージョンに更新します。
 - a) Control Centerの **管理** → **Dr.Web Server** セクションを開きます。
 - b) Serverバージョンのリストを開くには、Serverの現在のバージョンをクリックするか、**バージョンリスト** ボタンをクリックします。利用可能なServerの更新とバックアップのリストが含まれた **Dr.Web Serverの更新** セクションが開きます。
 - c) Serverソフトウェアを更新するには、**全てのバージョン** リスト内の最新のバージョンの横にあるオプションを設定します。**保存** をクリックします。
 - d) Serverの更新が完了するまで待ちます。
6. Server設定内で端末の接続設定を変更します。
 - a) **管理** → **Dr.Web Serverの設定** を開きます。
 - b) **全般** タブで、**未承認の端末を新規端末にリセット** にチェックを入れます。
 - c) **全般** タブの **新規端末登録モード** ドロップダウンリストから **アクセスを自動的に許可する** を選択します。
 - d) **保存** をクリックしてServerを再起動します。
7. Control Centerの **アンチウイルスネットワーク** セクションで、アンチウイルスネットワークツリーに前回のバージョンと同様のユーザーグループを作成します。必要な場合は、作成したユーザーグループ内の端末に対して自動メンバーシップルールを作成します。
8. 必要な場合は、前回のバージョンと同様に AgentとServerの設定を行ってください(手順5の一時的な設定を除く)。
9. 必要に応じ、**管理** → **リポジトリの詳細設定** セクション内でリポジトリ設定を変更します。
10. 手順1で選択したServerの隔離方法に応じて、AgentからServerへのアクセスを復元します。
11. Serverに接続する予定の、ネットワーク内の全ての端末上のパブリック暗号化キーを置き換えてください。
 - Self-protectionが有効になっている場合、新しいServerのインストール中に作成されたパブリックキーを端末にコピーし、以下のコマンドを実行します。

```
es-service.exe -p <key>
```

または

```
es-service.exe --addpubkey=<key>
```

<key>には、端末にコピーするパブリック暗号化キーへのパスを指定します。
結果として、Agentのインストールフォルダにパブリックキーがコピーされます。デフォルトでは、%ProgramFiles%\DrWebフォルダです(詳しくは、付録[H2.Dr.Web Agent for Windows](#)参照)。
 - 端末上でSelf-protectionが無効になっている場合は、新しいServerのインストール中に作成されたパブリックキーを上で指定したフォルダ内に置いてください。
12. 全ての端末が新しいServerに接続された後、手順5で指定したServer設定をご自身の企業のポリシーに合わせて変更します。



Dr.Web Server for Windows OSのロギングレベルの管理

Windows OSのサーバーの場合、次のいずれかの方法でロギングの詳細レベルを変更できます。

- Control Centerの **Dr.Web Server**の設定 → ログ セクションを利用する。
この方法を推奨します。ログ セクションでは、サーバーのロギングの許可されている詳細レベル全てと、その他の設定の一部を指定できます。
詳細情報は管理者マニュアルの [Dr.Web Serverの設定 → ログ](#) セクションに記載されています。
- 次のコンソールコマンドを使用する:

```
drwcsd [<switches>] install
```

--verbosityスイッチで、サーバーの許可されているロギング詳細を指定できます。

サーバー管理のコマンドラインスイッチの詳細情報については、[H3.8. スイッチについての説明](#) セクションを参照してください。

ロギングの詳細レベルを設定するコマンドの例:

```
drwcsd --daemon "--home=C:\Program Files\DrWeb Server" "--bin-root=C:\Program Files\DrWeb Server" "--var-root=C:\Program Files\DrWeb Server\var" --verbosity=ALL --log=drwcsd.log --rotate=10,50m install
```

サーバーのインストールと作業フォルダの標準パスを再定義した場合は特に、他のスイッチが必須になります。

ログの詳細レベルを変更した後は、サーバーを再起動します。

```
drwcsd restart
```

- Windows OSの スタート メインメニューでコマンドを使用する。
このとき、利用できるロギング詳細レベルは **詳細** または **デフォルト** の2つのみです。
 - a) プログラム → サーバーコントロール → **詳細なロギング**
または
プログラム → サーバーコントロール → **デフォルトのロギング**
 - b) プログラム → サーバーコントロール → **再起動**。

Android OS搭載端末の自動位置情報

Dr.Web Enterprise Security Suiteを使用すると、保護されているAndroid OSモバイルデバイスの位置情報を管理者に自動的に送信できます。

モバイルデバイスを見つけるには

1. 以下の手順で、Dr.Web Serverへのモバイルデバイスの位置情報送信を設定します。
 - a) Dr.Web Security Control Centerの **アンチウイルスネットワーク** セクションにある**アンチウイルスネットワークツリー**で、必要なAndroid OS端末またはAndroid OS端末グループを選択します。
 - b) コントロールメニューで **Dr.Web for Android** を選択します。
 - c) **全般** タブで、**位置情報をトラッキング** フラグを設定します。**位置情報を送信する間隔** ドロップダウンリストで、デバイスの位置情報を更新する間隔の値を選択します。



- d) 変更内容を保存します。
2. 位置情報の自動トラッキングは、次のいずれかの方法で実行されます。
- 位置情報プロバイダ(GPS、モバイルネットワーク)がユーザーデバイスで有効になっていて、信号が安定している場合、位置情報はモバイルデバイス自体によってモニタリングされます。
 - 位置情報プロバイダ(GPS、モバイルネットワーク)がユーザーデバイスで無効になっているか、GPS信号を検知しない場合、Dr.Web Enterprise Security Suiteの拡張機能では、Yandex Locatorを利用してモバイル通信塔(GSM、3D、LTE)とWiFi IDの座標上でモバイルデバイスの位置を特定します。Yandex Locatorを設定するには、**Yandex Locator拡張機能**を有効にし、次の設定を行う必要があります。
 - a) Yandex社のウェブサイト(<https://yandex.ru/dev/locator/keys/get/>)でAPIキーを取得します。
 - b) Dr.Web Security Control Centerの **管理** → **Dr.Web Serverの設定** → **モジュール セクション** で、**Yandex Locator拡張機能** のフラグを設定します。
 - c) **APIキー** フィールドに、手順a)で受信したキーを入力します。
 - d) 変更を保存してDr.Web Serverを再起動します。



WiFi IDはAndroid 5.1以前のモバイルデバイスでのみ使用できます。

3. Dr.Web Security Control Centerで端末位置情報を表示するには、次の手順に従います。
- a) アンチウイルスネットワーク セクションのネットワークツリーで、ステップ 1で対応設定を指定済みの端末を選択します。
 - b) 端末のプロパティでは、**位置情報** セクションに、モバイルデバイスから受信した地理座標が自動的に入力されます。
 - c) **地図で表示** をクリックすると、受信した座標に従って、OpenStreetMapにモバイルデバイスの地理的位置が表示されます。



Dr.Web Serverデータベースへのアクセス例

本章には、PostgreSQLデータベースへのSQLクエリの例が記載されています。他のデータベースへのクエリは、データベース自体の機能とその使用に関する微細な相違により、ある程度異なる場合があります。



ここに記載するクエリは意図的に作成されたものであり、読みやすさを考慮したものではありません。
標準SQLツールの特性により、クエリではグループと端末の階層を考慮しません。

データベースに直接アクセスするには

1. お使いのServerのControl Centerを開きます。
2. 管理 → **SQLコンソール** セクションを開きます。
3. 必要なSQLクエリを入力します。クエリの例は以下に示します。
4. **実行** をクリックします。

SQLクエリの例

1. Windows server OSがインストールされ、ウイルスデータベースが2019.07.04-00:00:00 UTC(12.0)より古い端末を検索します。

```
SELECT
  stations.name Station,
  groups_list.name OS,
  station_products.crev Bases
FROM
  stations
  INNER JOIN groups_list ON groups_list.platform = (
    CAST(stations.lastos AS INTEGER) & ~15728640
  )
  AND (
    (
      CAST(stations.lastos AS INTEGER) & 2130706560
    ) = 33554560
  )
  INNER JOIN station_products ON station_products.id = stations.id
  AND station_products.product = '10-drwbases'
  AND station_products.crev < 12020190704000000;
```

2. アンチウイルスネットワーク → 統計 → ステータスセクションの重要度が高いおよび最大となっているレコードを持つ端末を検索します。

```
SELECT
  stations.name Station
FROM
  stations
WHERE
  id IN (
    SELECT
      DISTINCT id
    FROM
      station_status
    WHERE
      severity >= 1342177280
  );
```

3. 対応するステータスと、これらのステータスを持つ端末の数を取得します。



```
SELECT
  code Code,
  COUNT(code) Num
FROM
  (
    SELECT
      DISTINCT id,
      code
    FROM
      station_status
  ) AS t
GROUP BY
  Code
ORDER BY
  Code;
```

4. 「373a9afb-9c9a-4d4d-b9b1-de817b96bcc5」識別子を持つグループまたはその中にネストされたグループに含まれる端末で、2019.06.01から2019.07.01に検出された脅威の上位10を取得します。

```
SELECT
  cat_virus.str Threat,
  COUNT(cat_virus.str) Num
FROM
  station_infection
  INNER JOIN cat_virus ON cat_virus.id = station_infection.virus
WHERE
  station_infection.infectiontime BETWEEN 20190601000000000
  AND 20190701000000000
  AND station_infection.id IN (
    SELECT
      sid
    FROM
      station_groups
    WHERE
      gid = '373a9afb-9c9a-4d4d-b9b1-de817b96bcc5'
      OR gid IN (
        SELECT
          child
        FROM
          group_children
        WHERE
          id = '373a9afb-9c9a-4d4d-b9b1-de817b96bcc5'
      )
  )
GROUP BY
  cat_virus.str
ORDER BY
  Num DESC
LIMIT
  10;
```

5. 感染した端末の上位10を取得します。

```
SELECT
  Station,
  Grp,
  Num
FROM
  (
    SELECT
      stations.id,
      groups_list.id,
      stations.name Station,
      groups_list.name Grp,
      COUNT(stations.id) Num
    FROM
```



```
station_infection
INNER JOIN stations ON station_infection.id = stations.id
INNER JOIN groups_list ON groups_list.id = stations.gid
GROUP BY
stations.id,
groups_list.id,
stations.name,
groups_list.name
ORDER BY
Num DESC
LIMIT
10
) AS t;
```

6. これらの端末のプライマリではないユーザーグループから、すべての端末のメンバーシップを削除します。

```
DELETE FROM
station_groups;
INSERT INTO station_groups(sid, gid)
SELECT
stations.id,
groups_list.id
FROM
stations
INNER JOIN groups_list ON stations.gid = groups_list.id
AND groups_list.type NOT IN(1, 4);
```

7. SpIDer Gateコンポーネントの個人設定のホワイトリストで指定されたドメインを含むアンチウイルスネットワークのオブジェクトを検索します。

```
SELECT
stations.name Station
FROM
station_cfg
INNER JOIN stations ON stations.id = station_cfg.id
WHERE
station_cfg.component = 38
AND station_cfg.name = 'WhiteVirUrlList'
AND station_cfg.value = 'domain.tld';
SELECT
groups_list.name Grp
FROM
group_cfg
INNER JOIN groups_list ON groups_list.id = group_cfg.id
WHERE
group_cfg.component = 38
AND group_cfg.name = 'WhiteVirUrlList'
AND group_cfg.value = 'domain.tld';
SELECT
policy_list.name Policy
FROM
policy_cfg
INNER JOIN policy_list ON policy_list.id = policy_cfg.id
WHERE
policy_cfg.component = 38
AND policy_cfg.name = 'WhiteVirUrlList'
AND policy_cfg.value = 'domain.tld';
```

8. 管理者のControl Centerへのログイン失敗のイベントを、対応する認証エラーコードとともに取得します。

```
SELECT
admin_activity.login Login,
admin_activity.address Address,
activity_data.value ErrorCode,
admin_activity.createtime EventTimestamp
FROM
admin_activity
```



```
INNER JOIN activity_data ON admin_activity.record = activity_data.record
WHERE
  admin_activity.oper = 10100
  AND admin_activity.status != 1
  AND activity_data.item = 'Error';
```

9. 必要なセキュリティ修正プログラムがインストールされていないWindows端末を検索します。

```
SELECT
  stations.name Station
FROM
  stations
WHERE
  id NOT IN (
    SELECT
      station_env_kb.id
    FROM
      station_env_kb
    INNER JOIN stations ON stations.id = station_env_kb.id
    WHERE
      (
        CAST(stations.lastos AS INTEGER) & 2130706432
      )= 33554432
    AND station_env_kb.name IN (
      SELECT
        id
      FROM
        env_strings
      WHERE
        str IN(
          'KB4012212', 'KB4012213', 'KB4012214',
          'KB4012215', 'KB4012216', 'KB4012217',
          'KB4012598'
        )
    )
  );
```

機能分析の基準

機能分析の設定を行う際は、最大レベルの保護を実現するために機能分析の基準を指定することをお勧めします。

機能分析の基準 セクションには、プロファイルを保護するための、設定可能なカテゴリに関する情報が含まれています。必要な保護レベルに応じてカテゴリを選択することができます。

機能分析基準のカテゴリ

1. アプリケーションの起動

- *Doctor Web*においてアドウェアのものであると知られている証明書によって署名されたアプリケーションの実行を禁止する
広告を配信する可能性のあるアプリケーションの実行をブロックします。
- *Doctor Web*においてグレーとして知られている証明書によって署名されたアプリケーションの実行を禁止する
「グレー」の証明書によって署名されたアプリケーションの実行をブロックします。多くの場合、これらの証明書は安全でないアプリケーションの署名に使用されます。
- *Doctor Web*においてハッキングツールのものであると知られている証明書によって署名されたアプリケーションの実行を禁止する
システムのセキュリティを脅かすアプリケーションの実行をブロックします。この基準を設定することをお勧めします。



- 偽の／不正な証明書によって署名されたアプリケーションの実行を禁止する
無効な証明書によって署名された悪意のあるアプリケーションの実行をブロックします。この基準を設定することをお勧めします。
- Doctor Webにおいてマルウェアのものであると知られている証明書によって署名されたアプリケーションの実行を禁止する
侵害された証明書によって署名されたアプリケーションの実行をブロックします。この基準を設定することをお勧めします。
- 失効した証明書によって署名されたアプリケーションの実行を禁止する
盗まれた証明書または侵害された証明書によって署名されたアプリケーションの実行をブロックします。この基準により、悪意のある可能性のあるアプリケーションの実行を防ぐことができます。この基準を設定することをお勧めします。
- 自己署名証明書によって署名されたアプリケーションの実行を禁止する
悪意のある可能性のある、ライセンスのないソフトウェアをブロックします。
- 未署名のアプリケーションの実行を禁止する
悪意のある可能性がある、提供元が不明な信頼できないアプリケーションの実行をブロックします。
- Sysinternalsユーティリティの実行を禁止する
システムを侵害する目的で使用されることの多いSysinternalsユーティリティの実行をブロックします。



パーミッション セクションで システムアプリケーションとMicrosoft社のアプリケーションの実行を許可する フラグが設定されている場合、Sysinternalsユーティリティは実行が許可されていない場合でも実行されます。

- NTFS(ADS)代替スレッドからのアプリケーションの実行を禁止する
NTFS(ADS)代替スレッドからのアプリケーションは、悪意のあるものである場合があります。この基準を設定することをお勧めします。
- ネットワークや共有からのアプリケーションの実行を禁止する
ネットワークと共有からのアプリケーションの実行は、システムのセキュリティを脅かす可能性があります。この基準を設定することをお勧めします。
- リムーバブルメディアからのアプリケーションの実行を禁止する
リムーバブルメディアからのアプリケーションの実行は、システムのセキュリティを脅かす可能性があります。この基準を設定することをお勧めします。
- 一時フォルダからのアプリケーションの実行を禁止する
一時フォルダからのアプリケーションの実行は、システムのセキュリティを脅かす可能性があります。この基準を設定することをお勧めします。
- Windows／Microsoftストアアプリケーションの実行を禁止する (Windows 8以降のみ)
Windows／Microsoftストアからダウンロードされたアプリケーションの実行をブロックします。
- 二重／非標準的拡張子を持つアプリケーションの実行を禁止する
標準的でない拡張子 (例: *.jpg.exe) を持つ疑わしいファイルの実行をブロックします。
- bashシェルとWSLアプリケーションの実行を禁止する (Windows 10以降のみ)
bashシェルとWSLアプリケーションの実行をブロックします。

2. モジュールのロードと実行 - このカテゴリでは、動作モードを指定できます。

- モジュールのロードと実行をすべて制御する
このモードはリソースを大量に消費します。強化された保護が必要な場合にのみ、このモードを指定することをお勧めします。
- ホストアプリケーションでのモジュールのロードと実行を制御する
このモードは、リソース消費のより少ないモードです。システムを侵害する目的で使用される可能性のあるプロセスでのみ、モジュールの動作を制御します。この場合、システムや信頼できるファイルを装ってマルウェアが



システムに侵入する可能性があります。強化された保護を必要としない場合に、モジュールのロードと実行をすべて制御するモードの代わりにこのモードを使用してください。

モジュールのロードと実行 基準を使用する際の推奨事項は、[アプリケーションの起動](#) 基準を使用する際の推奨事項と同じです。

3. スクリプトインタプリタの起動

- **CMD/BATスクリプトの実行を禁止する**
cmdおよびbatファイルの起動をブロックします。
- **HTAスクリプトの実行を禁止する**
HTAスクリプトの実行をブロックします。このようなスクリプトは、悪意のあるスクリプトを処理し、実行ファイルをコンピューターにダウンロードする可能性があります。
- **VBScript/JavaScriptの実行を禁止する**
VBScriptおよびJavaScript言語で記述されたアプリケーションの実行をブロックします。このようなアプリケーションは、悪意のあるスクリプトを処理し、実行ファイルをコンピューターにダウンロードする可能性があります。
- **PowerShellスクリプトの実行を禁止する**
PowerShellスクリプト言語で記述されたスクリプトの実行をブロックします。このようなスクリプトは、悪意のあるスクリプトを処理し、実行ファイルをコンピューターにダウンロードする可能性があります。
- **REGスクリプトの実行を禁止する**
reg拡張子を持つレジストリスクリプトファイルの起動をブロックします。これらのレジストリスクリプトファイルは、レジストリの値を追加したり変更したりするために使用される可能性があります。
- **NTFS(ADS)代替スレッドからのスクリプトの実行を禁止する**
NTFS(ADS)代替スレッドからのスクリプトは、悪意のあるものである場合があります。この基準を設定することをお勧めします。
- **ネットワークや共有からのスクリプトの実行を禁止する**
ネットワークと共有からのスクリプトの実行は、システムのセキュリティを脅かす可能性があります。この基準を設定することをお勧めします。
- **リムーバブルメディアからのスクリプトの実行を禁止する**
リムーバブルメディアからのスクリプトの実行は、システムのセキュリティを脅かす可能性があります。この基準を設定することをお勧めします。
- **一時フォルダからのスクリプトの実行を禁止する**
一時フォルダからのスクリプトの実行は、システムのセキュリティを脅かす可能性があります。この基準を設定することをお勧めします。

4. ドライバのロード

- **未署名のドライバのロードを禁止する**
ルートキットとブートキットのロードをブロックします。この基準により、システムやソフトウェアの脆弱性の悪用から保護します。
この基準は、64ビット版のOSに対して推奨されます。システムに未署名のドライバがない場合は、32ビット版のOSでもこの基準を使用することができます。
- **一般的なソフトウェアの脆弱性のあるドライババージョンのロードを禁止する**
一般的なソフトウェアの脆弱なドライババージョンのダウンロードをブロックします。



一般的なソフトウェアの脆弱なドライババージョンのダウンロードの禁止は、除外によってブロックすることはできません。

ドライバのロード 基準を使用する際のその他の推奨事項は、[アプリケーションの起動](#) 基準を使用する際の推奨事項と同じです。

5. MSIパッケージのインストール



MSIパッケージのインストール 基準を使用する際の推奨事項は、[アプリケーションの起動](#) 基準を使用する際の推奨事項と同じです。

6. 実行ファイルの整合性

- *新しい実行ファイルの作成を禁止する*
新しい実行ファイルを作成する試みをブロックします。
- *実行ファイルの改変を禁止する*
実行ファイルを改変する試みをブロックします。

実行ファイルの整合性 カテゴリの基準は、信頼できる実行環境で実行されているシステムでのみ使用します。そのようなシステムでは、すべてのプロセスが管理者によって制御されています(ATMやその他のシステムなど)。

それ以外のシステムで **実行ファイルの整合性** カテゴリの基準を使用する場合、予測できない動作をする可能性があります、端末が故障するリスクが高くなります。



実行ファイルの整合性 カテゴリの基準は、ルールによってブロックすることはできません。



第4章: トラブルシューティング

リモートインストールにおけるトラブルシューティング

インストールの原理

1. Dr.Web Serverはリモート端末のADMIN\$リソース(\\ <remote_station>\ADMIN\$\Temp)に接続し、サーバーインストールフォルダのwebmin\install\windowsフォルダにあるネットワークインストーラ drwinst.exeとサーバーインストールフォルダのetcフォルダにあるSSL証明書drwcsd-certificate.pemを\\ <remote_station>\ADMIN\$\Tempフォルダにコピーします。
2. ServerはControl Centerの設定に沿ったコマンドラインスイッチを使用し、リモート端末でdrwinst.exeファイルを実行します。

インストールを成功させるには、インストールを実行するサーバーで以下の条件を満たす必要があります。

1. リモート端末でADMIN\$\Tempリソースが利用可能になっている必要があります。

次の方法で確認できます。

Windows Explorerアプリケーションのアドレスラインで、

\\ <remote_station>\ADMIN\$\Temp

と入力します。このリソースにアクセスするログインとパスワードを入力するよう指示されます。インストールページで指定したアカウントデータを入力します。

ADMIN\$\Tempリソースが利用できない場合、以下の理由が考えられます。

- a) アカウントが管理権限を持っていません。
 - b) 端末の電源が切れているか、455ポートへのアクセスがファイアーウォールにブロックされています。
 - c) 端末がドメインの外部にある場合、Windows Vistaおよびそれ以降のバージョンでは、ADMIN\$\Tempリソースへのリモートアクセスに制限があります。
 - d) フォルダの所有者が存在しないか、フォルダに対するユーザーまたはグループの権限が足りません。
2. drwinst.exeファイルとdrwcsd.pubファイルが利用可能になっている必要があります。

Dr.Web Security Control Centerは、エラーの原因を特定する外部情報(手順およびエラーコード)を表示します。



Dr.Web Agentのリモートインストールエラーの一覧

ステップ	エラー	原因
SMBから <host>端末に接続	<host>端末のアドレスが不正	Agentインストールに指定された端末のIPアドレスが有効なIPv4/IPv6アドレスではないか、DNS名からアドレスへの変換に失敗しました。そのようなDNS名が存在しないか、ネームサーバーの設定が間違っています。
	SMBから <host>端末への接続エラー	SMBから端末に接続できません。次の理由が考えられます。 <ul style="list-style-type: none"> ● 端末のサーバーサービスが無効になっています。 ● リモート端末で445ポートが利用できません。次の理由が考えられます。 <ul style="list-style-type: none"> □ 端末の電源がオフになっています。 □ ファイアウォールが特定のポートをブロックしています。 □ リモート端末のOSがWindows OSではありません。 ● ローカルアカウントの共有とセキュリティのモデルが設定されていません。 ● 認証サーバーを利用できません(ドメインコントローラー)。 ● ユーザー名を認識できないか、パスワードが間違っています。
	<host>端末の <share>共有リソースを開くための権限が不十分	リモート端末にADMIN\$リソースが存在しないか、リソースを開くための必要な権限がありません。
<host>端末にファイルを送信	<share>共有リソースの <path>パスが <host>端末で見つかりません	ADMIN\$/TEMPディレクトリが存在しません。
	<host>端末で <share>共有リソースに <path>一時フォルダを作成できません	必要な書き込み権限がないなどで、ADMIN\$/TEMPに一時ディレクトリを作成できません。
	<host>端末で <share>共有リソースの <path>一時フォルダを削除できません	処理の完了後にADMIN\$/TEMPの一時ディレクトリを削除できません。例えば、サービスが完了しなかったり、このディレクトリのファイルを開いている人がいる場合などです。
	サーバーで <path>ファイルを読み込み用にオープンできません サーバーで <path>ファイルを読み込みできません	サーバーにインストーラファイルが見つからなかったか、インストーラファイルに必要な権限が設定されていません。



ステップ	エラー	原因
	<p><host>端末で <share>共有フォルダの <path>ファイルを書き込み用にオープンできません</p> <p><host>端末で <share>共有フォルダの <path>ファイルに書き込みできません</p>	対象のファイルまたは対象のディレクトリに読み込みまたは書き込みのための必要な権限がありません。
<host>端末でのサービスの作成	<host>端末でサーバーサービス(srvsvc RPC)への接続エラー	サービスのリモート管理は使用できません。
	<p><host>端末でSMCへの接続がエラー</p> <p><host>端末でサービスを作成できません</p> <p><host>端末でサービスを開始できません</p> <p><host>端末でサービスを停止できません</p> <p><host>端末でサービスを削除できません</p>	サービスの管理に必要な権限がありません。
<host>端末でのサービスの実行	<host>端末のサービスの状態を取得できません	考えられるSCMエラー。
	<host>端末でインストールのタイムアウト	指定の時間内にインストーラがAgentをインストールできませんでした。理由として、端末とサーバー間のチャンネル速度が遅い、必要なデータをダウンロードするのに十分な時間がなかった、などが考えられます。
	<host>端末で <share>共有リソースへのローカルパスを取得できません	端末でADMIN\$リソースへのパスが見つかりませんでした。
	<host>端末でエラーによりサービスが停止しました。完了状態: <share>。エラーコード: <rc>。	Agentインストーラのエラー。



Dr.Web Agent for Windowsのインストール中のBFEエラーの解決

Dr.Web Anti-virus for Windowsの一部のコンポーネントでは、ベース・フィルタリング・エンジン(BFE)サービスが実行中であることが動作の必要条件となっています。このサービスが存在していないか破損している場合、Dr.Web Agent for Windowsをインストールできません。また、そのような場合は端末上に脅威が存在している可能性も考えられます。

Dr.Web Agent for Windowsのインストールが失敗し、BFEエラーが出力された場合は、次のアクションを実行する必要があります。

1. Doctor Webの提供するユーティリティのCureNet!を使用して端末のシステムをスキャンしてください。
このユーティリティのデモバージョン(診断は可能ですが、修復はしません)は <https://download.drweb.com/curenet/> でリクエストできます。
ユーティリティのフルバージョンの使用条件と価格については、<https://estore.drweb.com/utilities/> を参照してください。
2. BFEサービスを有効にするか再起動します。BFEサービスを再起動できない場合、またはサービスの一覧に表示されない場合は、[Microsoftテクニカルサポート](#) にお問い合わせください。
3. Dr.Web Agent for Windowsインストーラを実行し、インストールマニュアルに記載された一般的な手順に沿ってインストールを実行します。
問題が解決しない場合は、Doctor Webの[テクニカルサポート](#) サービスにお問い合わせください。



テクニカルサポート

Dr.Web製品のインストールまたは使用中に問題が発生した場合、テクニカルサポートへのお問い合わせの前に以下のオプションをご利用ください:

- <https://download.drweb.com/doc/> から最新のマニュアルやガイドをダウンロードして読む。
- https://support.drweb.com/show_faq/ で「よくあるご質問」を読む。
- <https://forum.drweb.com/> でDr.Webフォーラムを見る。

問題が解決しなかった場合、サポートサイト <https://support.drweb.com/> の該当するセクション内でwebフォームに必要事項を入力し、直接 Doctor Web テクニカルサポートまでお問い合わせください。

企業情報については、Doctor Web 公式サイト <https://company.drweb.com/contacts/offices/> をご覧ください。

