



Dr.Web Enterprise Security Suite Ver.10 簡易構築ガイド -Linux 用-

株式会社 Doctor Web Pacific

初版 : 2014/09/19

改訂 : 2017/04/18



目次

1. はじめに.....	4
1.1 ライセンス証書の受領.....	4
1.2 ライセンス証書に含まれる内容.....	4
2. 環境前提条件.....	4
3. 準備.....	5
3.1 インストール環境の確認.....	5
3.2 ファイル.....	5
4. インストール.....	6
4.1 インストーラのパーミッションの変更.....	6
4.2 インストーラの実行.....	6
4.3 キーファイルの登録.....	7
5. Control Center の設定.....	10
5.1 ESS サーバの更新.....	10
5.2 「Dr.Web Server の設定」の変更(1).....	10
5.3 「Dr.Web Server の設定」の変更(2).....	10
5.4 「Web Server の設定」の変更.....	10
5.5 「通知設定」の変更.....	11
5.6 Dr.Web for MS Outlook の設定変更.....	11
5.7 hosts の除外設定.....	12
5.8 Windows8 使用時の設定変更.....	12
6. Agent のインストール.....	13
6.1 Agent のインストールの前に.....	13
6.1.1 導入するコンポーネントの選択.....	13
6.1.2 その他注意事項等.....	14
6.2 Agent のインストーラの配布とインストール、承認.....	15
6.2.1 Agent のインストーラの配布.....	15
6.2.2 Agent のインストール、承認.....	15
6.3 その他の Agent のインストール方法.....	20
6.3.1 端末毎の専用インストーラ.....	20
6.3.2 フルパッケージインストーラ.....	22
7. ケーススタディ.....	24
7.1 パスワードの変更.....	24
7.2 ライセンスの更新.....	25



7.3	CC の表示言語の変更.....	29
7.4	Agent のインストールに失敗する.....	29
7.5	端末の追加に失敗する.....	30
7.6	リポジトリの更新による PC の再起動を止めたい.....	30
7.7	PC のクローニングについて.....	31
7.7.1	構築済みの ESS サーバがあり、イメージ展開時に通信が可能な場合.....	31
7.7.2	構築済みの ESS サーバがあり、イメージ展開時に通信が不可能.....	32
7.8	InternetExplorer11 での CC の利用について.....	32
7.9	業務用のアプリケーションが脅威として検知された場合の対処.....	33
7.10	業務用のアプリケーションの起動等が遅くなった場合の対処.....	34
7.11	統計情報.....	35
7.11.1	スキャン統計情報.....	35
7.11.2	脅威.....	36
7.12	クローズドネットワークでの定義ファイル等の更新.....	37



この度は、株式会社 DoctorWebPacific の製品をご購入いただき、誠にありがとうございます。本ガイドは、初めて弊社製品をご利用いただくお客様向けに、弊社集中管理ツール(Enterprise Security Suite/Control Center)を簡潔に構築いただくための手順を説明する資料となります。なお、詳細な機能や操作の説明に関しましては、製品マニュアルをご参照ください。

1. はじめに

1.1 ライセンス証書の受領

ライセンス証書は、Doctor Web Pacific(以下、DWP)または、DWP パートナー企業より、電子メールか郵送もしくはその両方の方法で、お客様へ送付いたします。

1.2 ライセンス証書に含まれる内容

ライセンス証書には、以下のライセンスに関する情報が記載されておりますので、大切に保管してください。

- custmer(お客様情報)
- product(購入製品名)
- serial number(製品用キーコード)
- license term(ライセンス期間)
- protected objects (購入ライセンス数)

※ “My Dr.Web”につきましては、日本ではご利用できません。

2. 環境前提条件

本書は、下記の環境で動作確認の上作成しております。

- Cent OS 6.5 (64bit)
- Enterprise Security Suite (以降、ESS)を新規インストール
- 内部 DB(SQLite3)を使用



3. 準備

3.1 インストール環境の確認

➤ 通信ポート

以下のポートの通信が可能であるか確認してください。

TCP : 2193,139,445

UDP : 2193,139,445

http : 9080

https : 9081

➤ モジュール

lsb : v.3 以降

glibc : v.2.7 以降

※ メモリ、HDD 容量等については、インストールマニュアルを参照してください。

3.2 ファイル

以下のファイルを用意してください。インストーラおよび agent.key の入手方法については、「Dr.Web ダウンロード & アクティベーションガイド」を参照してください。

➤ インストーラ

インストール対象の Linux のディストリビューションにあった.run ファイルを用意し、インストール対象のサーバにコピーしてください。

➤ agent.key



4. インストール

4.1 インストーラのパーミッションの変更

インストーラ(.run ファイル)パーミッションを変更し、実行権を付与する。

```
# chmod +x <インストーラ名>
```

4.2 インストーラの実行

- 1) 以下のコマンドを実行する。

```
# ./<インストーラ名>
```

※ ファイルの解凍が始まります。

- 2) 「END USER LICENSE AGREEMENT」が表示されたら、内容をよく確認する。

※ 次のページの内容を参照する場合は、スペースキーを押してください。

- 3) 「Do you agree with the terms of this license?」と確認が表示されるので、「yes」と入力し、Enter キーを押す。

※ 何も入力せずに Enter キーを押した場合は、インストールが終了します。

- 4) 「Please enter the path to your ES backup data」と表示されたら、「0」を入力し、Enter キーを押す。

※ ユーザ、グループの作成、ファイルのコピー等が始まります。

- 5) 以下のメッセージが表示された後、プロンプトに戻ったことを確認する。

```
.....+++
.....+++
writing new private key to '/var/opt/drwcs/etc/private-key.pem'
-----
Initializing new database ...
Making initial product revision ...
chkconfig setup...
#
```

- 6) 以下のコマンドを実行し、drwcsd のプロセスが開始していることを確認する。

```
# /etc/init.d/drwcsd status
Dr.Web Server is started
#
```


4.3 キーファイルの登録

- 1) ブラウザから以下の URL にアクセスする。

http://<ESS サーバの IP アドレス or DNS 名>:9080/

※ SSL でアクセスする場合は、https://<ESS サーバの IP アドレス or DNS 名>:9081/

- 2) ID と Password を入力し、ControlCenter(以降、CC)ログインする。



LOGIN

PASSWORD

OK

ID : admin

Password : root

※ 上記のパスワードは、初期パスワードのため、必ず変更を行なってください。

- 3) 「管理」メニューに移動する。



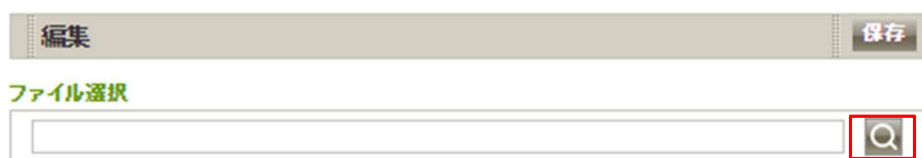
- 4) 画面左側の[管理]-[ライセンスマネージャー]をクリックする。



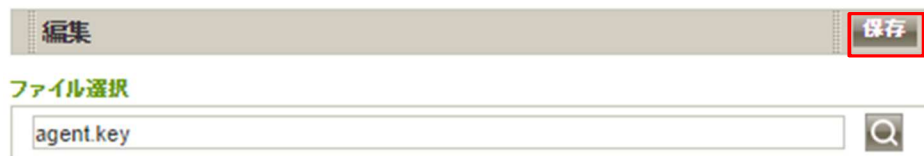
- 5) 画面中央の「キー」と書かれたツリーの上にある「キーの追加」アイコンをクリックする。



- 6) 画面右側に表示された虫眼鏡のアイコンをクリックする。



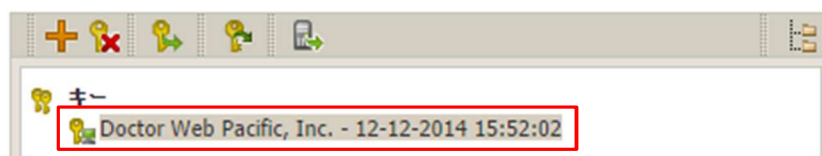
- 7) 予め用意してある agent.key を指定し、「開く」をクリックする。
- 8) 「保存」ボタンをクリックする。



- 9) 画面中央の「キー」ツリーに追加した agent.key の「登録名」と「ライセンス終了日」が表示されたことを確認する。



- 10) 追加されたキーをクリックする。



※ クリックすると背景がグレーに変わります。

- 11) 「端末およびグループにキーを配信する」アイコンをクリックする。

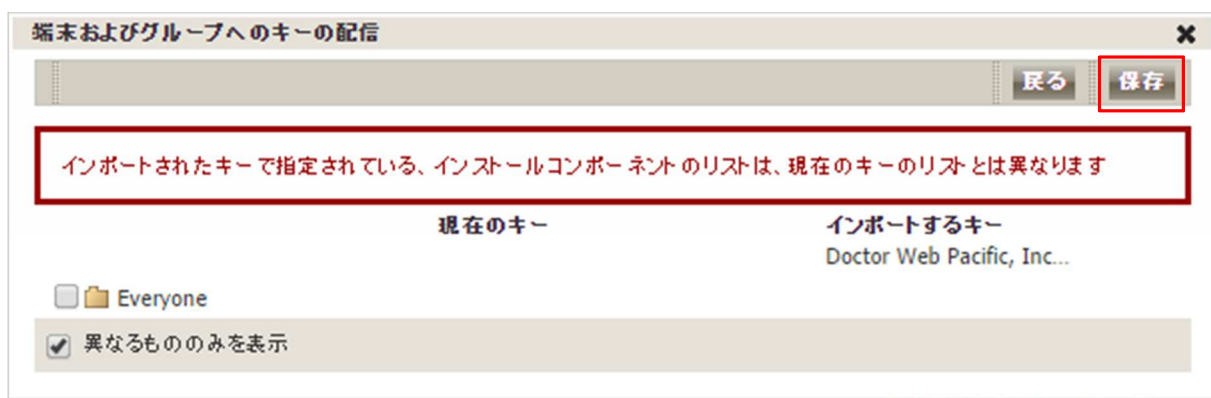


- 12) 「Everyone」を選択し、「キーの追加」ボタンをクリックする。



※ クリックすると背景がグレーに変わります。

- 13) 以下のような画面が表示された場合は、「保存」ボタンをクリックする。



- 14) 画面中央の「キー」ツリーに、「Everyone」が表示されたことを確認する。





5. Control Center の設定

ESS サーバを使用するにあたっての設定を行いません。

5.1 ESS サーバの更新

ESS サーバのアップデートの有無を確認し、アップデートがある場合、更新を行いません。

- 1) CC にログインし、「管理」メニューを開き、「リポジトリの状態」をクリックする。
- 2) 「更新情報のチェック」ボタンをクリックし、最新のリポジトリを取得する。
- 3) リポジトリの更新完了後、「Dr.Web Server」をクリックし、「バージョンリスト」ボタンをクリックする。
- 4) アップデートがある場合、「全てのバージョン」の箇所に適用可能なものの一覧から、最新のものを選択し、「保存」ボタンをクリックする。
 - ※ バージョン表記は、dd-mm-yyyy HH:mm:ss の形式です。
 - ※ バージョンアップは、環境によって異なりますが、数分～数十分かかります。
- 5) バージョンアップ完了後、再度 CC にログインし、「管理」メニューで表示されている「Dr.Web Server のバージョン」が更新されたことを確認する。

5.2 「Dr.Web Server の設定」の変更(1)

- 1) CC にログインし、「管理」メニューを開き、「Dr.Web Server の設定」をクリックする。
- 2) 「ダウンロード」タブをクリックする。
- 3) 「サーバー」欄に、当該サーバの IP アドレスか DNS 名を入力する。
- 4) 「保存」をクリックし、設定を保存する。
- 5) 再起動要求が表示された場合、再起動ボタンをクリックして再起動する。

5.3 「Dr.Web Server の設定」の変更(2)

管理対象に Android 端末がある場合、以下の設定を行なってください。

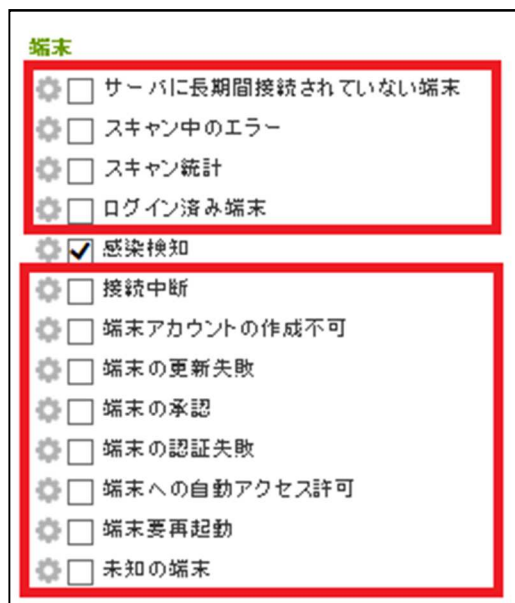
- 1) CC にログインし、「管理」メニューを開き、「Dr.Web Server の設定」をクリックする。
- 2) 「全般」タブをクリックする。
- 3) 「暗号化」の設定を、「はい」から「**可能であれば**」(もしくは、「いいえ」)に変更する。
- 4) 「保存」をクリックし、設定を保存する。
- 5) 再起動要求が表示された場合、再起動ボタンをクリックして再起動する。

5.4 「Web Server の設定」の変更

- 1) CC にログインし、「管理」メニューを開き、「Web Server の設定」をクリックする。
- 2) 「全般」タブをクリックする。
- 3) 「サーバー」欄に、当該サーバの IP アドレスか DNS 名を入力する。
- 4) 「保存」をクリックし、設定を保存する。
- 5) 再起動要求が表示された場合、再起動ボタンをクリックして再起動する。

5.5 「通知設定」の変更

初期状態では、管理者宛に多くの通知内容行われ、その内容は DB 内に保存されます。これによりデータベースの肥大化が生じることもある為、端末に関する通知項目を以下のように、「感染検知」のみに変更してください。



端末

- サーバに長期間接続されていない端末
- スキャン中のエラー
- スキャン統計
- ログイン済み端末
- 感染検知
- 接続中断
- 端末アカウントの作成不可
- 端末の更新失敗
- 端末の承認
- 端末の認証失敗
- 端末への自動アクセス許可
- 端末要再起動
- 未知の端末

※ 赤枠内の項目については、チェックを外してください。

5.6 Dr.Web for MS Outlook の設定変更

MS Outlook 使用時に、メールに添付されているパスワードが設定された ZIP ファイル等が隔離されてしまうことを防止するため、以下の設定を行なってください。

- 1) CC にログインし、「アンチウイルスネットワーク」を開く。
- 2) 画面中央のツリーから、「Everyone」グループを選択する。
- 3) 「Dr.Web for MS Outlook」をクリックする。
- 4) 「アクション」タブ内の「未検査のファイル」の設定を「隔離」から「無視」に変更する。
- 5) 「保存」ボタンをクリックする。



5.7 hosts の除外設定

hosts の変更を行なっている環境において、Dr.Web により hosts が初期化される場合がありますので、これを防止するため、以下の設定を行なってください。

※ 入力された文字コードによっては、適切に動作しない場合があるため、本書記載の内容をコピーするのではなく、直接キーボードより入力してください。

- 1) CC にログインし、「アンチウイルスネットワーク」を開く。
- 2) 画面中央のツリーから、「Everyone」グループを選択する。
- 3) 「Scanner」をクリックする。
- 4) 「除外」タブ内の「除外するパスとファイル」に以下を追加し、「保存」をクリックする。

C:\¥windows¥system32¥drivers¥etc¥hosts

- 5) 「SpIDer Guard for workstations」をクリックする。
- 6) 「除外」タブ内の「除外するパスとファイル」に以下を追加し、「保存」をクリックする。

C:\¥windows¥system32¥drivers¥etc¥hosts

- 7) 「SpIDer Guard for servers」をクリックする。
- 8) 「除外」タブ内の「除外するパスとファイル」に以下を追加し、「保存」をクリックする。

C:\¥windows¥system32¥drivers¥etc¥hosts

5.8 Windows8 使用時の設定変更

Windows8 を使用している場合、Dr.Web からの通知(再起動要求、脅威の検出等)が一切表示されない場合があります。その場合、以下の設定を行なってください。

- 1) CC にログインし、「アンチウイルスネットワーク」を開く。
- 2) 画面中央のツリーから、「Everyone」グループを選択する。
- 3) 「Dr.Web Agent」をクリックする。
- 4) 「インターフェース」タブ内の「フルスクリーンモードの時には通知を表示しない」のチェックを外す。
- 5) 「保存」ボタンをクリックする。



6. Agent のインストール

Windows PC に Agent をインストールする場合、コンポーネントの選択の後、本項の手順にて配布、インストール、承認を行なってください。

6.1 Agent のインストールの前に

6.1.1 導入するコンポーネントの選択

Agent は複数のコンポーネントから構成され、コンポーネント単位で導入するか否かを選択できます。

必要に応じて、CC 上で[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]から導入するコンポーネントを選択してください。

初期状態では、以下となっており、“Dr.Web Firewall”以外がインストールされます。

Everyone. 個人設定が作成されました

Dr.Web Agent for Windows	インストール必須	▼
Dr.Web Scanner	インストール必須	▼

Dr.Web Agent for UNIX	インストール必須	▼

Dr.Web Scanner for Windows	インストール可能	▼
SpIDer Guard for Windows workstations	インストール可能	▼
SpIDer Guard for Windows Servers	インストール可能	▼
SpIDer Mail for Windows workstations	インストール可能	▼
SpIDer Gate for Windows workstations	インストール可能	▼
Dr.Web Office Control	インストール可能	▼
Dr.Web for Microsoft Outlook	インストール可能	▼
Dr.Web Anti-spam	インストール可能	▼
Dr.Web Firewall	インストール可能	▼

※ “SpIDer Guard for Windows workstations”と”SpIDer Guard for Windows Servers”につきましては、OS の種類(クライアント OS かサーバ OS)により、どちらかがインストールされます。

※ Windows OS に対しては、“Dr.Web Agent for UNIX”はインストールされません。

また、**Windows Server に対しては、以下のコンポーネント以外は導入しないでください。**

- Dr.Web Agent for Windows
- Dr.Web Scanner
- Dr.Web Scanner for Windows
- SpIDer Guard for Windows Servers



6.1.2 その他注意事項等

➤ 環境復元ソフトがインストールされている場合

環境復元ソフトがインストールされている場合、環境復元ソフトを停止した状態(復元機能が実行されない状態)でインストールを実施してください。また、予め ControlCenter の更新の設定を「データベースのみ」に変更してください。

また、正常に定義ファイルの更新が行われている状況においても「Dr.Web ウィルスデータベースが最新ではありません」、「コンピューターが脅威に晒される可能性があります」等のメッセージが表示されることがありますが、実際にはディスク内の定義ファイルが読み込まれております。

ディスク内の定義ファイルの状態につきましては、[ツール]-[サポート]-[詳細]から「プログラムについて」ウィンドウに表示された「ウィルスデータベース」よりご確認ください。

※ drwtoday.vdb の日付をご確認ください。

➤ URL フィルタリングソフトがインストールされている場合

URL フィルタリングソフトがインストールされている場合、ホームページの閲覧等ができなくなる場合があります。その際は、SpIDer Mail、SpIDer Gate、Dr.Web for MS Outlook をアンインストールしてください。

6.2 Agent のインストーラの配布とインストール、承認

6.2.1 Agent のインストーラの配布

Agent のインストーラと暗号化キーを、以下の URL よりダウンロードし、Dr.Web をインストールする端末に配布してください。また、Agent インストーラと暗号化キーは、インストールする端末上の同じフォルダに保存してください。

➤ Agent のインストーラ

URL : <http://<ESS サーバの IP アドレス or DNS 名>:9080/install/windows>
<https://<ESS サーバの IP アドレス or DNS 名>:9081/install/windows>

ファイル名 : drwinst.exe

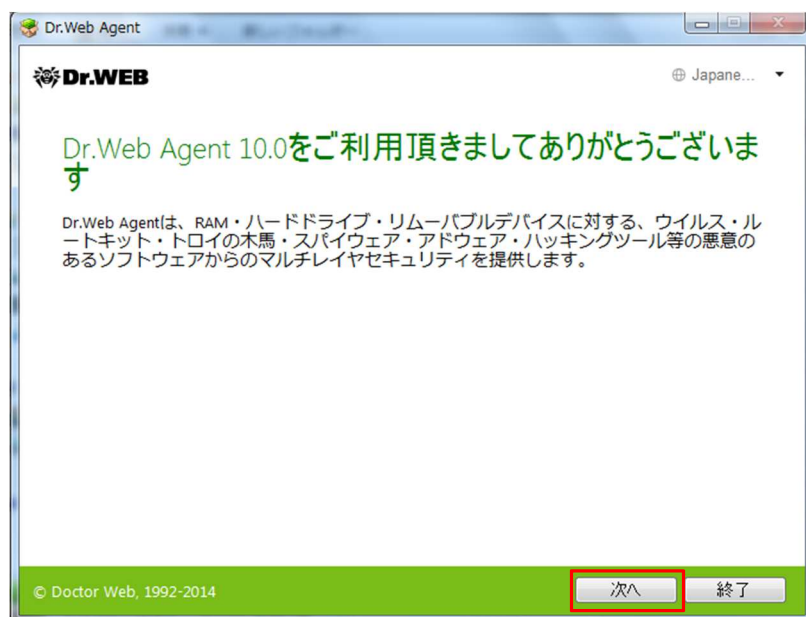
➤ 暗号化キー

URL : <http://<ESS サーバの IP アドレス or DNS 名>:9080/install/>
<https://<ESS サーバの IP アドレス or DNS 名>:9081/install/>

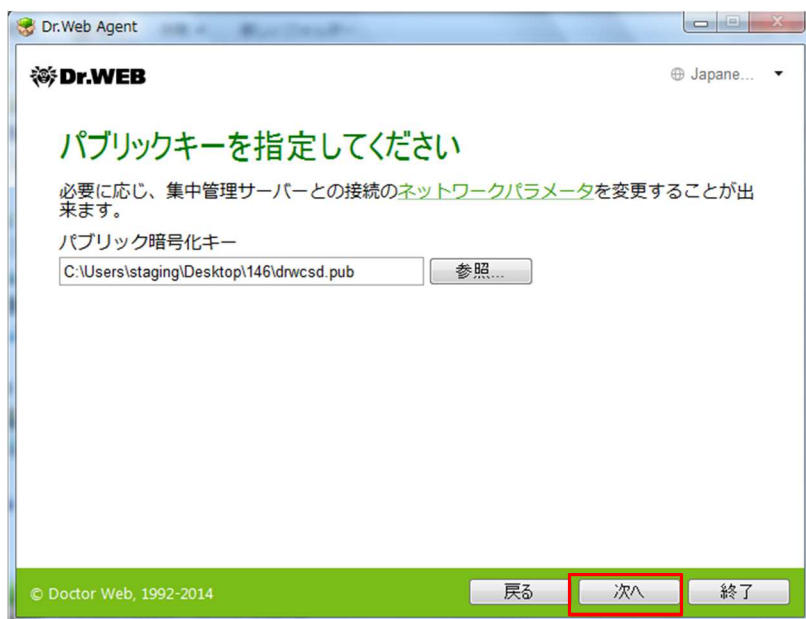
ファイル名 : drwcsd.pub

6.2.2 Agent のインストール、承認

- 1) 端末上に保存した Agent のインストーラ(drwinst.exe)を実行する。
- 2) 以下の画面が表示されたら、「次へ」をクリックする。



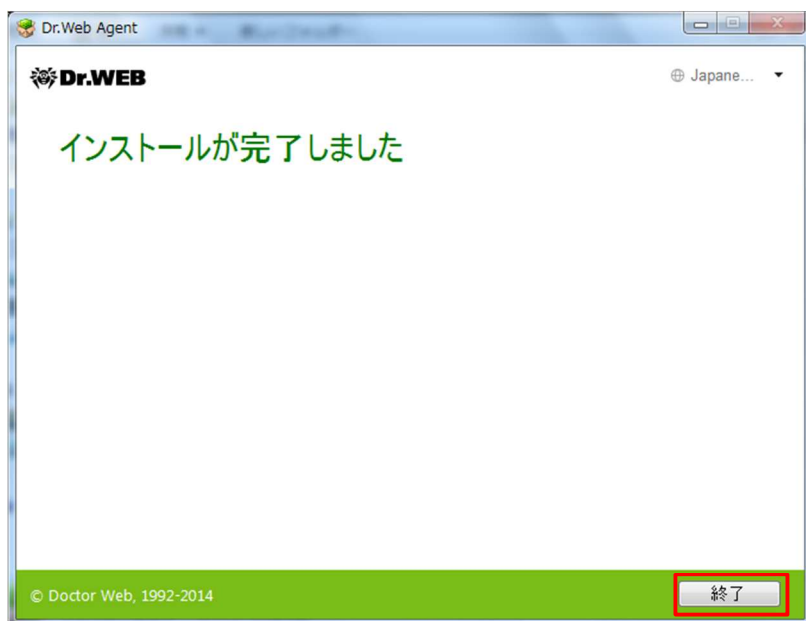
- 3) 以下の画面で暗号化キーが指定されていることを確認して、「次へ」をクリックする。



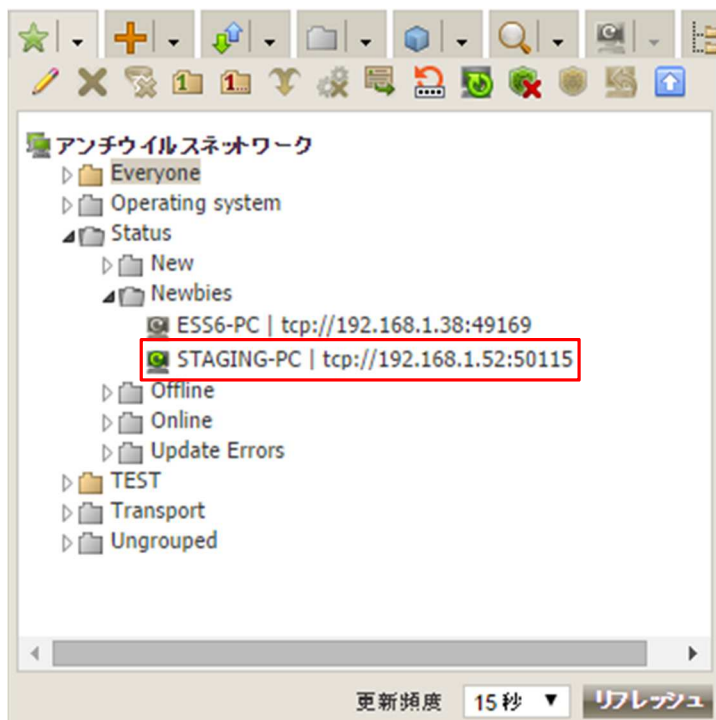
- 4) しばらくすると、以下の画面が表示されるので、「インストール」をクリックする。



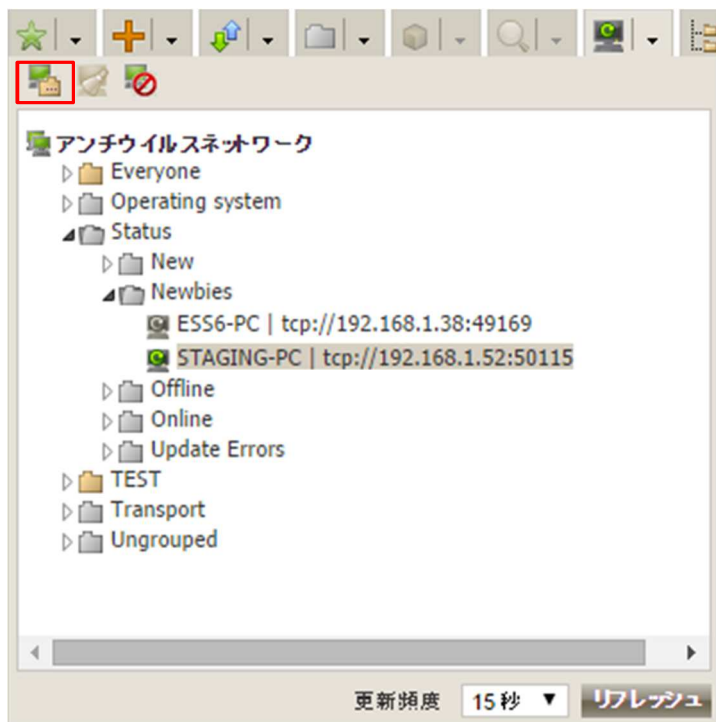
- 5) 以下の画面が表示されたら、「終了」をクリックする。



- 6) CC にログインし、「アンチウイルスネットワーク」メニューを開く。
- 7) 画面中央のツリーから、[Status]-[Newbies]を開き、インストールした端末が表示されていることを確認する。



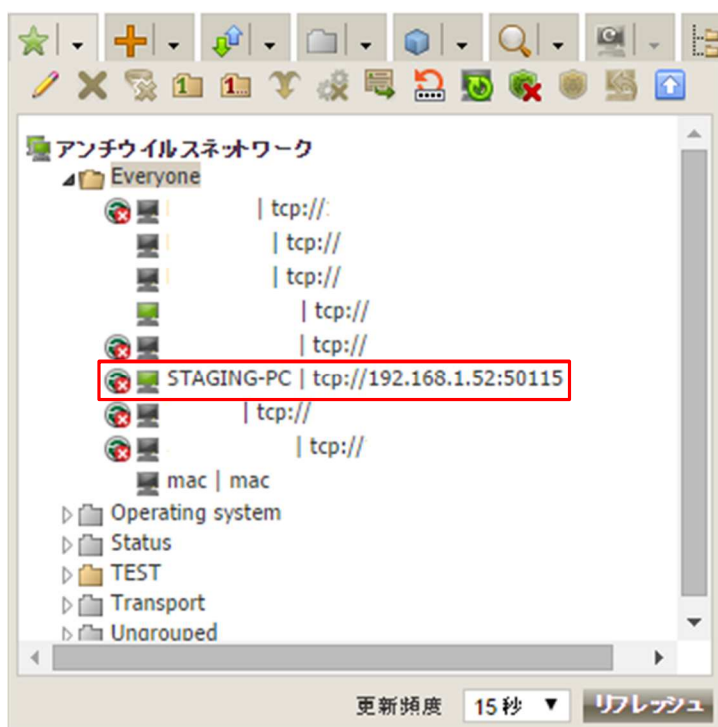
- 8) インストールした端末(以下の図では、STAGING-PC)を選択し、「選択した端末を承認し、プライマリグループに設定」ボタンをクリックする。



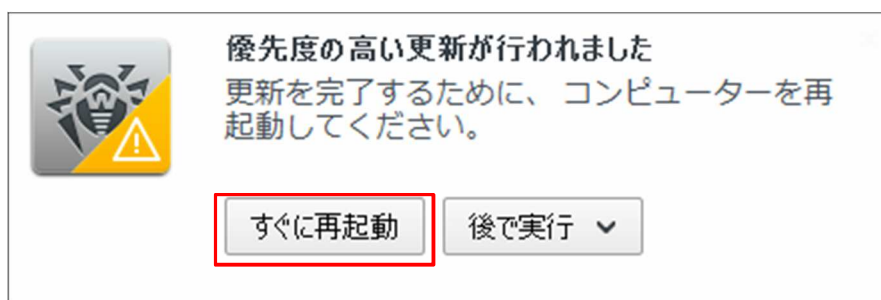
- 9) 画面右側から「プライマリグループ」を選択し、「保存」ボタンをクリックする。



- 10) 画面中央のツリーの「Everyone」グループに承認した端末が表示されたことを確認する。



- 11) 端末を承認した後、しばらくすると Agent をインストールした端末上に以下のメッセージが表示されるので、「すぐに再起動」をクリックする。



6.3 その他の Agent のインストール方法

Agent のインストールは、上記 6-1 の方法以外に、端末毎の専用インストーラ、フルパッケージインストーラ、Active Directory によるログオンスクリプト等の様々な方法で実施することができます。

6.3.1 端末毎の専用インストーラ

端末(Agent)毎に専用のインストーラを作成しますので、これを用いると、サーバ上での承認が不要となります。また、インストール完了時には、再起動要求が表示されます。

※ インストーラには、端末 ID(Agent ID)等が含まれる為、インストール時の承認は不要ですが、端末 ID が重複する為、異なる PC に対して同じインストーラを使用することはできません。

- 1) CC にログインし、「アンチウイルスネットワーク」メニューを開きます。
- 2) 中央のツリーの「+」のボタンをクリックする。



- 3) 次にモニタのアイコンをクリックする。



- 4) 「新規端末」の箇所、パスワードを入力し、「保存」をクリックする。

新規端末 保存

全般

ナンバー*	1
ID*	479400b1-a4fb-409b-9716-fc7c3cfdd0d2
名称*	新規端末
パスワード	<input type="password"/>
パスワードを再度入力してください	<input type="password"/>
説明	<input type="text"/>

グループ

所属グループ

-
-
-
- Everyone
-
-
-

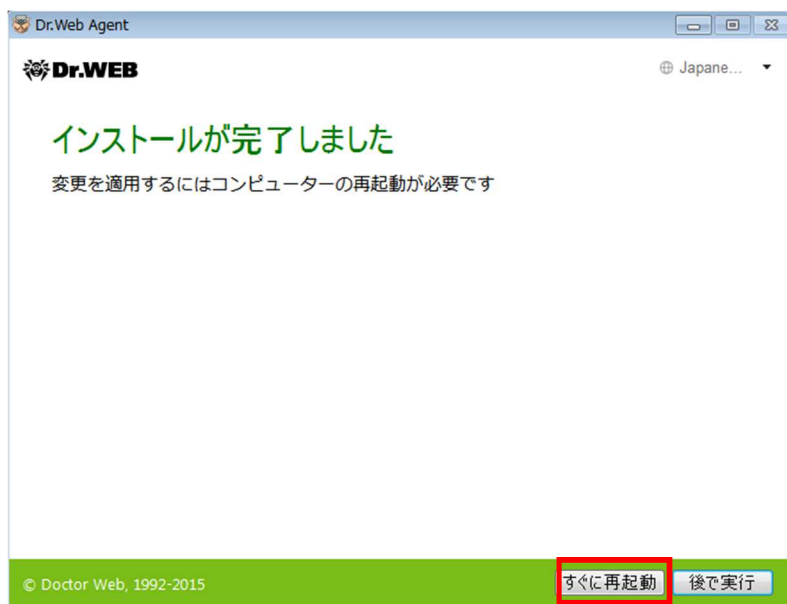
※ 必要に応じてプライマリグループの設定を行なってください。

- 5) 「インストールファイル」の”Windows”をクリックし、専用インストーラをダウンロードする。

端末を作成 インストール

479400b1-a4fb-409b-9716-fc7c3cfdd0d2	端末 479400b1-a4fb-409b-9716-fc7c3cfdd0d2 は正常に作成されました
インストールファイル	Windows , Linux x86_64, Linux x86, MacOS X, Android
設定ファイル	MacOS X & Android & Linux
パスワード	●●●●●●●●●●

- 6) ダウンロードした専用インストーラ(drweb-ess-installer.exe)をインストール対象に PC にコピーした後、実行する。
 - ※ 暗号化キー(drwcsd.pub)は専用インストーラに含まれるので、別途用意する必要はありません。
 - ※ 以降は画面の表示に従って進めてください。
- 7) 以下の画面が表示されたら、PC の再起動を実施する。



6.3.2 フルパッケージインストーラ

作成日時点での全てのコンポーネントおよび定義ファイルが含まれたインストーラです。これを用いることにより、他の方法と比較して、インストール時の Agent-サーバ間のトラフィックを抑えることができます。

- 1) 弊社ダウンロードサイトよりフルパッケージインストーラをダウンロードする。

Ver	プログラム, ドキュメント				
10.0	<table border="0"><tr><td>Dr.Web Enterprise Security Suite server 選択して下さい ▼</td><td>管理者マニュアル 日本語 ▼ ダウンロード (PDF形式)</td></tr><tr><td>Windows OS向けエージェントインストーラフルパッケージ drweb-esuite-agent-full-10.00.0-201508050-windows.exe</td><td>インストールマニュアル 日本語 ▼ ダウンロード (PDF形式)</td></tr></table>	Dr.Web Enterprise Security Suite server 選択して下さい ▼	管理者マニュアル 日本語 ▼ ダウンロード (PDF形式)	Windows OS向けエージェントインストーラフルパッケージ drweb-esuite-agent-full-10.00.0-201508050-windows.exe	インストールマニュアル 日本語 ▼ ダウンロード (PDF形式)
Dr.Web Enterprise Security Suite server 選択して下さい ▼	管理者マニュアル 日本語 ▼ ダウンロード (PDF形式)				
Windows OS向けエージェントインストーラフルパッケージ drweb-esuite-agent-full-10.00.0-201508050-windows.exe	インストールマニュアル 日本語 ▼ ダウンロード (PDF形式)				

- ダウンロードしたフルパッケージインストーラと暗号化キー(drwesd.pub)をインストールする PC の同じフォルダにコピーした後、実行する。

※ 以降は画面の表示に従って進めてください。

- 以下の画面が表示されたら、PC の再起動を実施する。



- PC の再起動中に 6-1-2 の 6)~10)の手順を実行する。

※ 必ず、端末を CC 上で承認してください。

7. ケーススタディ

7.1 パスワードの変更

- 1) CC にログインする。
- 2) 「管理」メニューに移動する。
- 3) [設定]-[管理者]をクリックする。



- 4) 画面中央のツリーから「Administrators」を展開する。

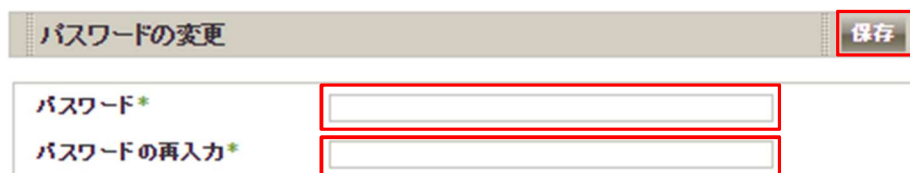


- 5) 「admin」を選択し、「パスワードの変更」アイコンをクリックする。



※ 「admin」を選択した後、「パスワードの変更」アイコンがクリックできるようになります。

- 6) パスワードを入力し、「保存」ボタンをクリックする。



A screenshot of the 'パスワードの変更' (Change Password) form. The form has a title bar with 'パスワードの変更' and a '保存' (Save) button. Below the title bar are two input fields: 'パスワード*' and 'パスワードの再入力*'. Both input fields are highlighted with red boxes.

- 7) 一度ログオフし、変更したパスワードでログインできるか確認する。

7.2 ライセンスの更新

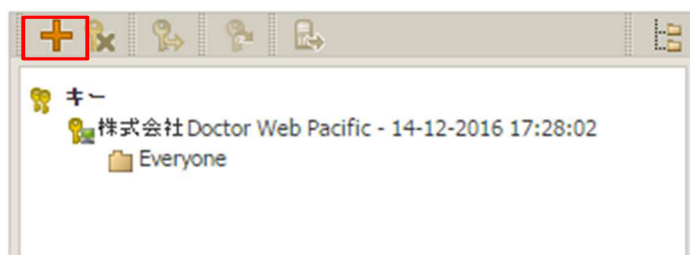
ライセンスキーは、「Everyone」グループに紐づけてください。

※ ESS6 とは異なり、ESS10 では一つのグループに複数のライセンスキーを紐づけたり、逆に一つのライセンスキーに複数のグループを紐づけたりすることが可能です。ライセンスキーとグループは、1対1ではなく、n対nの関係となります。

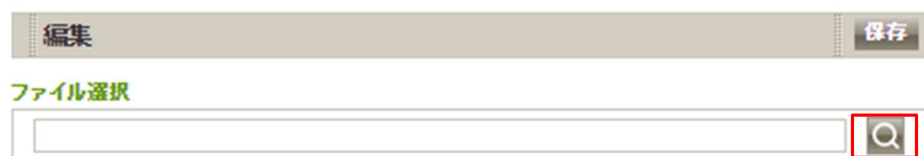
- 1) CC にログインする。
- 2) 「管理」メニューに移動する。
- 3) [設定]-[ライセンスマネージャー]をクリックする。



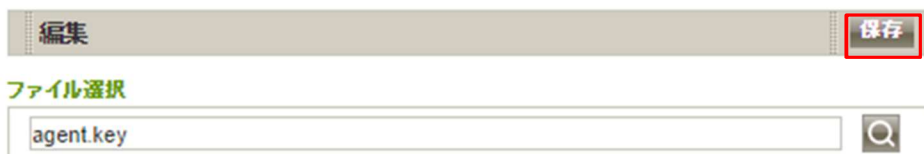
- 4) 画面中央の「キー」と書かれたツリーの上にある「キーの追加」アイコンをクリックする。



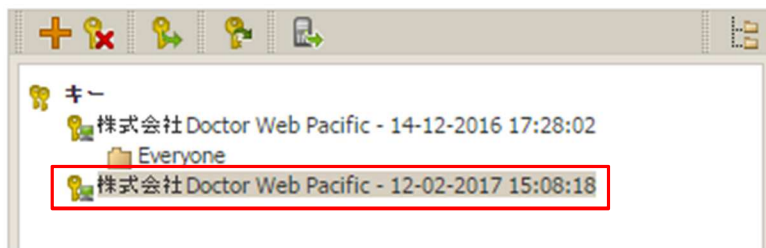
- 5) 画面右側に表示された虫眼鏡のアイコンをクリックする。



- 6) 新しいライセンスの agent.key を指定し、「開く」をクリックする。
- 7) 「保存」ボタンをクリックする。

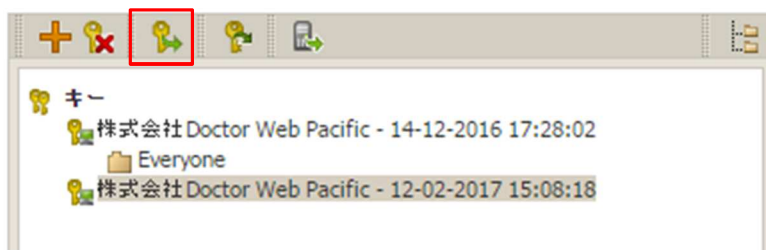


- 8) 画面中央の「キー」ツリーに新しいライセンスの「登録名」と「ライセンス終了日」が表示されたことを確認し、追加したキーをクリックする。



※ クリックすると背景がグレーに変わります。

- 9) 「端末およびグループにキーを配信する」アイコンをクリックする。



- 10) 「Everyone」を選択し、「キーの追加」ボタンをクリックする。



※ クリックすると背景がグレーに変わります。

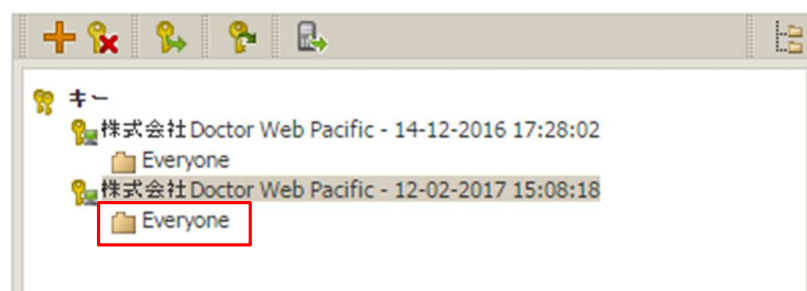
11) 以下のような画面が表示されるので、「保存」ボタンをクリックする。



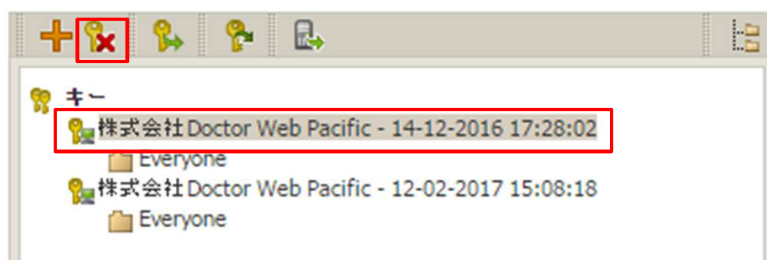
※ 以下のような表示は、現在のライセンスと新しいライセンスで利用可能なコンポーネントが異なることを表しています。



12) 新しいライセンスキーの下に、「Everyone」が表示されたことを確認する。



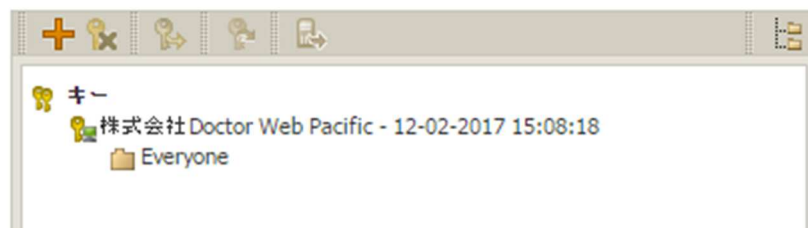
- 13) 以前のライセンスキーを選択し、「選択したオブジェクトの削除」ボタンをクリックする。



- 14) 以下のメッセージが表示されたら、「保存」ボタンをクリックする。

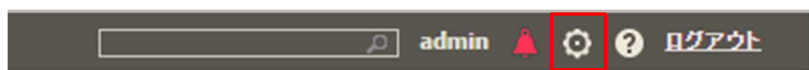


- 15) 以前のライセンスキーが削除されたことを確認する。



7.3 CC の表示言語の変更

- 1) CC にログインする。
- 2) 「環境設定」アイコンをクリックする。



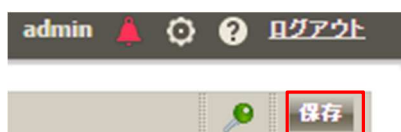
- 3) 「表示言語」を変更する。

管理者アカウントの編集

全般

ログイン*	admin
名前	
ミドルネーム	
名字	
表示言語	日本語 ▼
日付のフォーマット	DD-MM-YYYY HH:MM:SS ▼
最終アドレス	tcp://192.168.1.125:50999
作成日時	2014/09/23 01:05:30

- 4) 「保存」ボタンをクリックする。



7.4 Agent のインストールに失敗する。

Agent のインストールに失敗する場合、下記を確認後、再度実行してください。

- ESS サーバが起動しているか
- インストール時に指定した暗号化キー(drwcsd.pub)が、接続する ESS サーバのものか
- ESS サーバ、Agent をインストールする端末で必要なポートが解放されているか
- ネットワーク機器により、ESS サーバと Agent 間で使用するポートが閉じられていないか

再度実行しても失敗する場合は、以下のようにコマンドラインから接続する ESS サーバを指定して実行してください。

例) drwinst.exe と drwcsd.pub を「C:¥temp」フォルダに保存している場合

```
C:¥temp> drwinst.exe /server <ESS サーバの IP アドレス>
```

7.5 端末の追加に失敗する

CC 上で、「ネットワーク」メニューから端末の追加を行なった際に、下記のようなメッセージが表示される場合があります。



この場合は、次の事項を確認してください。

- Agent.key が登録されているか
- 有効な Agent.key が「Everyone」グループに配信されているか

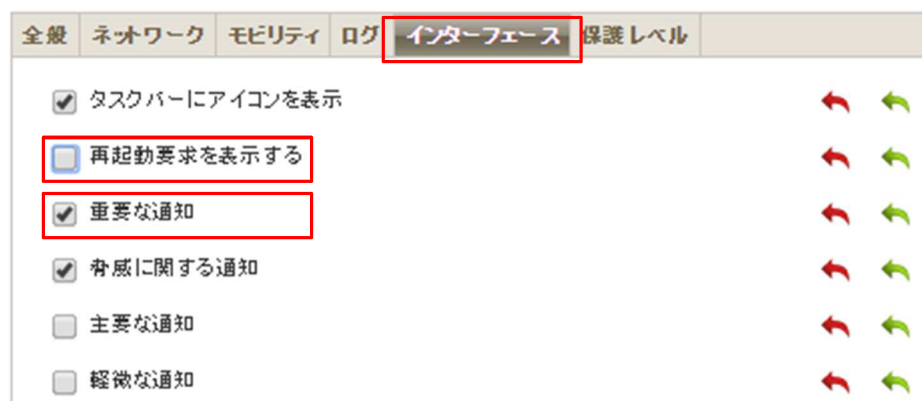
7.6 リポジトリの更新による PC の再起動を止めたい

Agent プログラムの更新により、PC の再起動を要求されることがあります。以下の方法で、再起動要求を表示せず、自動的に再起動がされないようにすることができます。また、この方法では、終業時に PC をシャットダウン、始業時に PC を起動することにより、更新プログラムが適用されます。

- 1) CC にログインする。
- 2) 「アンチウイルスネットワーク」メニューを開く。
- 3) 画面中央のツリーの「Everyone」グループを選択する。
 - ※ 全ての端末ではなく特定の端末や特定のグループに対して設定したい場合は、該当の端末もしくはグループを選択してください。
- 4) 画面右側の「設定」セクションから [Windows]-[Dr.Web Agent] をクリックする。



- 5) 中央に表示されたメニューから、「インターフェース」を選択し、「再起動要求を表示する」と「重要な通知」のチェックを外す。



- 6) 「保存」ボタンをクリックし、設定を保存する。

7.7 PC のクローニングについて

sysprep で作成した OS のマスターイメージをクローニングして展開する場合、構築済み ESS サーバとの通信可否により、手順が異なります。暗号化キーが必要となるため、ESS サーバの構築が完了していない状態では、マスターイメージに含めることはできません。

また、ESS サーバの IP アドレス等は、マスターイメージ作成時とクローニング後で変更がないことが前提となります。

7.7.1 構築済みの ESS サーバがあり、イメージ展開時に通信が可能な場合

マスターイメージに含むことが可能ですが、未承認の端末となる為、ミニセットアップ完了後に CC 上で承認が必要になります。SetupComplete.cmd につきましては、MS 社 HP にてご確認ください。また、本番運用を行なう前に必ず動作検証を行なってください。

7.7.1.1. drwinst.exe を使用する場合

drwinst.exe は最小限のパッケージとなり、ESS サーバにて承認された後、インストールに必要なファイルや定義ファイルをダウンロードしインストールを行います。

- 1) drwinst.exe と drwcds.pub をマスター作成用 PC の同じフォルダに保存する。
- 2) ミニセットアップ完了後に、以下のコマンドが実行されるように SetupComplete.cmd で指定する。
drwinst.exe /silent yes /server <ESS サーバの IP アドレス> /pubkey <drwcds.pub へのパス>

※ “/silent yes”を指定することにより、インストーラ実行中の画面が表示されません。

例) drwinst.exe と drwcds.pub が「C:¥temp」に保存されており、ESS サーバの IP アドレスが 192.168.1.146 の場合

```
C:¥temp¥drwinst.exe /silent yes /server 192.168.1.146 /pubkey C:¥temp¥drwcds.pub
```

- 3) Sysprep を実行する。



- 4) クローン PC を作成する。
- 5) クローン PC を起動し、ミニセットアップを実行する。
- 6) CC にログインし、「アンチウイルスネットワーク」メニューを開く。
- 7) 画面中央のツリーから、[Status]-[Newbies]を開く。
- 8) 表示されている端末を選択し、「選択した端末を承認し、プライマリーグループに設定」ボタンをクリックする。
- 9) グループを選択し、「保存」ボタンをクリックする。
- 10) クローン PC のタスクトレイ上に、Dr.Web のアイコンが表示されたら、再起動する。

7.7.1.2. “Full anti-virus agent installer for Windows”を使用する場合

“Full anti-virus agent installer for Windows”には、インストールに必要なファイルが全て含まれております。インストール完了後、ESS サーバにて承認された後に定義ファイルをダウンロードします。

- 1) “Full anti-virus agent installer for Windows”を、Dr.Web の HP よりダウンロードする。
- 2) ダウンロードしたインストーラと drwcsd.pub をマスター作成用 PC の同じフォルダに保存する。
- 3) ミニセットアップ完了後に、以下のコマンドが実行されるように SetupComplete.cmd で指定する。

```
drweb-esuite-agent-full-10.00.0-201408070-windows.exe /silent yes /server <ESS サーバの IP アドレス>
```

※ インストーラの数字部分は、異なる場合があります。

※ “/silent yes”を指定することにより、インストーラ実行中の画面は表示されません。

例)インストーラと drwcsd.pub が「C:¥temp」に保存されており、ESS サーバの IP アドレスが 192.168.1.146 の場合

```
C:¥temp¥ drweb-esuite-agent-full-10.00.0-201408070-windows.exe /silent yes /server 192.168.1.146
```

- 4) Sysprep を実行する。
- 5) クローン PC を作成する。
- 6) クローン PC を起動し、ミニセットアップを実行する。
- 7) CC にログインし、「アンチウイルスネットワーク」メニューを開く。
- 8) 画面中央のツリーから、[Status]-[Newbies]を開く。
- 9) 表示されている端末を選択し、「選択した端末を承認し、プライマリーグループに設定」ボタンをクリックする。
- 10) グループを選択し、「保存」ボタンをクリックする。

7.7.2 構築済みの ESS サーバがあり、イメージ展開時に通信が不可能

ESS サーバと通信が可能となった状態で、各 PC から Agent のインストールを実行してください。

構築済みの ESS サーバがあるので、予めインストーラ(drwinst.exe もしくは“Full anti-virus agent installer for Windows”)と暗号化キー(drwcsd.pub)を HDD 内に保存した状態でのマスターイメージの作成は可能です。

7.8 Internet Explorer11 での CC の利用について

Internet Explorer11 で CC にアクセスした際、プラグインのインストールの表示が消えない場合は、CC の URL を「互換表示設定」に追加してください。



7.9 業務用のアプリケーションが脅威として検知された場合の対処

業務用アプリケーションが脅威として検知された場合、検知されたファイルを下記 URL より弊社にご送付ください。弊社にて確認後、誤検知であった場合には、検出されないよう対処します。

https://support.drweb.co.jp/support_wizard/

※ プログラムのバージョン等が変更となった後、再度検出された場合は、当該ファイルをお送りください。

上記の弊社対応には時間をいただきますので、ファイルを弊社にお送りいただくとともに以下の設定を行なっていただけますようお願いいたします。

➤ SpIDer Guard の除外設定

- 1) CC にログインする。
- 2) 「アンチウイルスネットワーク」メニューから、「Everyone」グループを選択する。
- 3) SpIDer Guard for workstations をクリックする。
※ Windows Server に対して設定する場合は、SpIDer Guard for servers をクリックしてください。
- 4) 「除外」をクリックし、「除外するパスとファイル」および「除外するプロセス」に当該ファイルをフルパスで指定する。
- 5) 「保存」をクリックする。

➤ Dr.Web Scanner の除外設定

- 1) CC にログインする。
- 2) 「アンチウイルスネットワーク」メニューから、「Everyone」グループを選択する。
- 3) Scanner をクリックする。
- 4) 「除外」をクリックし、「除外するパスとファイル」に当該ファイルをフルパスで指定する。
- 5) 「保存」をクリックする。



7.10 業務用のアプリケーションの起動等が遅くなった場合の対処

業務用アプリケーションの起動等が明らかに遅くなった場合、SpIDer Guard によるリアルタイムスキャンが影響している可能性があります。

その場合は、以下の設定を行なっていただけますようお願いいたします。

- 1) CC にログインする。
- 2) 「アンチウイルスネットワーク」メニューから、「Everyone」グループを選択する。
- 3) SpIDer Guard for workstations をクリックする。
※ Windows Server に対して設定する場合は、SpIDer Guard for servers をクリックしてください。
- 4) 「除外」をクリックし、該当する実行ファイルやフォルダを指定する。
”除外するプロセス” : 起動等が遅くなったアプリケーションの実行ファイル等を指定
※ 複数ある場合は、複数の実行ファイルをフルパスで指定してください。
”除外するパスとファイル” : 起動等が遅くなったアプリケーションのワークフォルダ、テンポラリフォルダやログファイル等を指定
- 5) 「保存」をクリックする。

《事例》

事 象 : Dr.Web Agent インストール後から、TWAIN ドライバを使用しているスキャナの取り込みが非常に遅くなった。

原 因 : スキャナ取り込み時に TWAIN.LOG ファイルが更新されるが、その更新の都度 SpIDer Guard によるスキャンが実行される為。

対 処 : TWAIN.LOG ファイルを SpIDer Guard の”除外するパスとファイル”に登録する。

登録例 : C:\Users*\AppData\Local\Temp\TWAIN.LOG

※ Windows7 や Windows8 の場合

7.11 統計情報

7.11.1 スキャン統計情報

「スキャン統計情報」から指定した期間における、選択したグループ全体・端末毎の以下の内容を確認することができます。

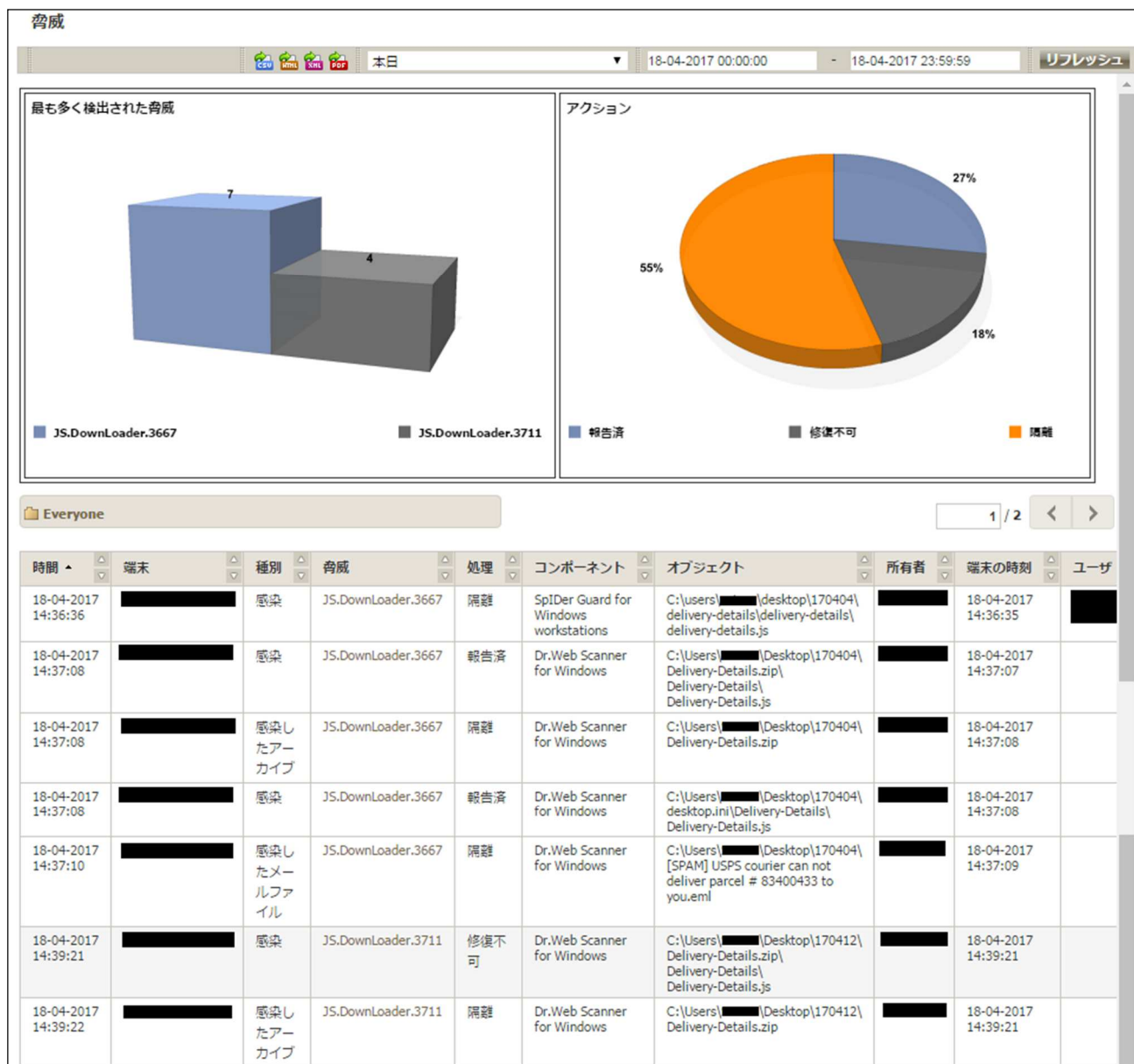
- スキャンしたファイル数 ①の箇所
- 検出された脅威の数 ②の箇所
- 削除された脅威の数 ③の箇所
- 隔離された脅威の数 ④の箇所
- ブロックされた脅威の数 ⑤の箇所
- 平均スキャン速度(Byte/s) ⑥の箇所

最初に選択したグループ全体の情報が表示され、その下に端末単位での情報が表示されます。

スキャン統計情報												
統計情報の要約												
グループ	①	②			③			④		⑤		⑥
Everyone	436701	0	0	2	0	0	0	2	0	7559	2611086	
	436701	0	0	2	0	0	0	2	0	7559	2611086	
Everyone												
端末	①	②			③			④		⑤		⑥
ESS10FULL tcp://192.168.1.35:49500	1318	0	0	0	0	0	0	0	0	0	5028633	
ESS10 tcp://192.168.1.52:49648	7	0	0	0	0	0	0	0	0	0	0	
32-PC tcp://192.168.1.49:49388	26070	0	0	0	0	0	0	0	0	0	7451948	
X86US tcp://192.168.1.45:49324	4827	0	0	0	0	0	0	0	0	0	4196963	
OFF tcp://192.168.1.33:49873	494	0	0	0	0	0	0	0	0	0	65775	
X86JP tcp://192.168.1.46:49314	7447	0	0	0	0	0	0	0	0	0	2932884	
dokutauebu-no-MacBook-Air.local tcp://192.168.1.62:53293	55669	0	0	0	0	0	0	0	0	6990	134911	
DWPTASAKI-PC tcp://192.168.1.48:49626	340869	0	0	2	0	0	0	2	0	569	8273792	
	436701	0	0	2	0	0	0	2	0	7559	2611086	

7.11.2 脅威

「脅威」から指定した期間における、選択したグループ全体・端末毎の検出された脅威およびその対処の内容等を確認することができます。画面の上部には、選択したグループ内での検出された脅威とその対処について、グラフ表示されます。



- **コンポーネント** 脅威を検出したコンポーネント名が表示されます。
- **処理** 検出された脅威に対して行われた処理が表示されます。「脅威に対してアクションを自動的に適用」が有効でない場合、Dr.Web Scannerにてファイルのスキャンを実行した場合には、「報告済」が表示されます。

7.12 クローズドネットワークでの定義ファイル等の更新

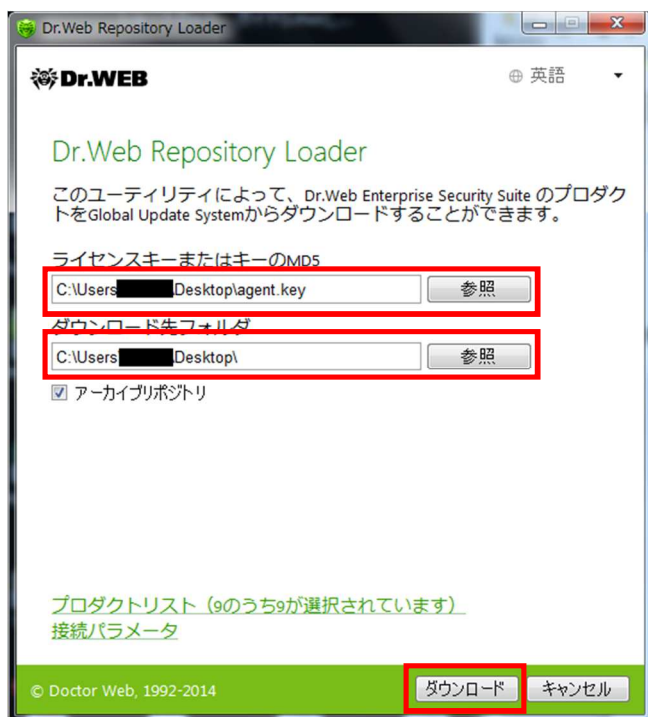
インターネットに接続されていないクローズドネットワーク内で利用される場合、以下の方法で定義ファイル等の更新を行なうことが可能です。

この場合も、クローズドネットワーク内に ESS サーバを用意し、クローズドネットワーク内の他の端末には ESS Agent をインストールしてください。また、定義ファイル等のダウンロードの際には、インターネットに接続可能な Windows 端末が必要となります。

- 1) クローズドネットワーク内の CC にログインします。
- 2) 「管理」メニューから「ユーティリティ」を開きます。
- 3) Dr.Web Repository Loader をダウンロードします。
※ Dr.Web Repository Loader を実行する端末の Windows OS が 32bit の場合は「x86」を、64bit の場合は「x64」を選択してください。
- 4) ダウンロードした Dr.Web Repository Loader を定義ファイル等のダウンロードに用いる Windows 端末にコピーします。
32bit 用 : drwreploder-gui-10.00.0-201507030-x86.exe
64bit 用 : drwreploder-gui-10.00.0-201507030-x64.exe
※ インストーラの数字部分は、異なる場合があります。
- 5) ダウンロードした Dr.Web Repository Loader を定義ファイル等のダウンロードに用いる Windows 端末にコピーします。
- 6) コピーした Dr.Web Repository Loader を実行します。



- 7) Agent.key ファイルとダウンロード先フォルダを指定した後、「ダウンロード」ボタンをクリックします。



※ プロキシ設定が必要な場合は、「接続パラメータ」から設定が可能です。

- 8) リポジトリのダウンロードが開始します。



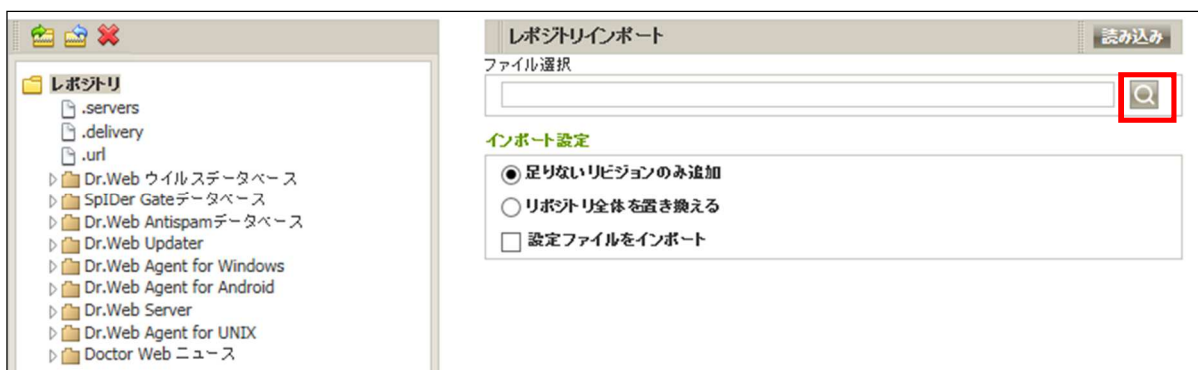
- 9) 下記が表示されたら「OK」ボタンをクリックし、保存された zip ファイルを USB メモリ等にコピーします。



- 10) クローズドネットワーク内の CC にログインします。
11) 「管理」メニューから「レポジトリコンテンツ」を開きます。
12) 「リポジトリファイルを含んだアーカイブをインポート」アイコンをクリックします。



13) 虫眼鏡のアイコンをクリックし、9)で保存した zip ファイルを指定します。



14) 「読み込み」ボタンをクリックすると、リポジトリが取り込まれます。



15) 取り込みが完了した後、「管理」メニューから「リポジトリの状態」を開き、定義ファイル等が更新されたことを確認します。





お使いの製品の詳細な機能の説明や、利用方法は、各製品マニュアルをご参照ください。
また、製品のご利用について、ご質問やトラブル等がありましたら、下記 URL よりお気軽にお問い合わせください。

https://support.drweb.co.jp/support_wizard/

株式会社 Doctor Web Pacific

〒210-0005 神奈川県川崎市川崎区東田町 1-2 いちご川崎ビル 2F

URL: www.drweb.co.jp