

# サーバセキュリティサービス 新規導入手順書 Deep Security 9.6SP1 (Linux)

NEC

第2版 2017/08/29

# 本資料に関して

■ 本資料は「サーバセキュリティサービス with Trend Micro Deep Security」をご利用頂くお客様向けの資料です。

■ Linux 環境に「Deep Security Agent 9.6SP1」を導入する方法を記載しています。  
Windows OS 環境の場合、別途、以下Webページよりお客様環境に適した導入手順書をご参照ください。

サーバセキュリティサービス with Trend Micro Deep Security - ドキュメント  
<http://jpn.nec.com/soft/trendmicro/sssw/document.html>

■ Linux版Deep Security Agent は、次ページの動作環境に加えて、OSのカーネルがサポート対象である必要が御座います。  
サポート対象であるかの確認は以下Webページをご参照ください

## [Deep Security 9.6 SP1 Supported Linux Kernels](#)

1. 目次（Table of Contents）よりご利用のLinuxOSを選択ください
2. 一覧の中にご利用のカーネルが含まれていることをご確認ください

※ご不明点がある場合は販売窓口（購入前）、  
またはPP・サポートサービス（購入後）までお問合せください。

■ Ver.9.5ではプロキシの有無により手順が異なっておりましたが、Ver.9.6より手順の共通化を行いました

# 動作環境（１）

サーバセキュリティサービスは以下の動作環境を満たしている必要があります。

|                      |   |   |
|----------------------|---|---|
| メモリ                  | ・ 512MB   |   |
| ハードディスク              | ・ 500MB以上の空き容量<br>(※アンチウイルス機能も動作させる場合は1GB以上を推奨)   |   |
| OS                   | <p>【Windows】</p> <p>Windows Server 2003 SP2 (32/64bit)<br/>Windows Server 2003 R2 SP2 (32/64bit)<br/>Windows Server 2008 (32/64bit)<br/>Windows Server 2008 R2 (64bit)<br/>Windows Server 2008 R2 Hyper-V<br/>Windows Server 2012 (64bit)<br/>Windows Server 2012 R2 (64bit)<br/>Windows Server 2012 R2 Hyper-V<br/>Windows Server Core 2012 (64bit)<br/>Windows Server Core 2012 R2 (64bit)<br/>Windows Server 2016 (64bit)Windows 10 (32/64bit)<br/>Windows XP (32/64bit)<br/>Windows Vista (32/64bit)<br/>Windows 7 (32/64bit)<br/>Windows 8 (32/64bit)<br/>Windows 8.1 (32/64bit)<br/>Windows 10 (32/64bit)</p> | <p>【Linux】</p> <p>Red Hat 5、6、7 (32/64 bit)<br/>CentOS 5、6、7 (32/64 bit)<br/>SUSE 10 SP3、SP4 (32/64bit)<br/>SUSE 11 SP1、SP2、SP3 (32/64bit)<br/>SUSE 12 (64bit)<br/>Ubuntu Linux 10.04、12.04、14.04、16.04 (64bit)<br/>Oracle Linux 5 RedHat/Unbreakable Kernel (32/64 bit)<br/>Oracle Linux 6 RedHat/Unbreakable Kernel (32/64 bit)<br/>Oracle Linux 7 RedHat/Unbreakable Kernel (64 bit)<br/>CloudLinux 5 (32/64bit)<br/>CloudLinux 6 (32/64bit)<br/>CloudLinux 7 (64bit)<br/>Debian 6 (64bit)<br/>Debian 7 (64bit)<br/>Amazon Red Hat 6 EC2 (32/64bit)<br/>Amazon Red Hat 7 EC2 (64bit)<br/>Amazon SUSE 11 EC2 (32/64bit)<br/>Amazon SUSE 12 EC2 (64bit)<br/>Amazon Ubuntu 12 EC2 (64bit)<br/>Amazon Ubuntu 14.04 LTS (64bit)<br/>Amazon Ubuntu 16.04 LTS (64bit)<br/>Amazon AMI Linux (32/64bit)<br/>Amazon Debian 7 (64bit)</p> |
| Webブラウザ<br>(管理コンソール) | Internet Explorer 9, 10,11 (Cookie を有効にする)<br>Mozilla Firefox (Cookie を有効にする)   |   |

※ エディションが指定されていないWindows 製品は、エディションに関係なく動作を保証いたします。

※ システム要件に記載されていないService Pack 等でも、要件に記載されているものより新しいバージョンはサポート対象となります。詳細は [こちら](#) をご確認ください。

※ Linux 版Agent では、ご利用のカーネルもサポート対象である必要があります。サポートするカーネルバージョンについては、以下製品Q&A をご参照ください。

<http://esupport.trendmicro.com/solution/ja-JP/1098600.aspx>

## 動作環境（２）

■ 本製品の利用には下記の要件を満たす必要があります。

1. インターネット接続が可能
2. TCP443で通信が可能
3. プロキシ経由する場合は、プロキシの認証無し、もしくは基本認証で通信が可能  
(プロキシの認証は基本認証のみ。Digest認証とNTLM認証は未サポート。)

■ 保護対象サーバが以下のURLにアクセスできる必要があります。

| URL                                  | 用途                      | 補足   |
|--------------------------------------|-------------------------|--|
| serversecurity-nec.jp:443            | 管理コンソールURL              | 保護対象サーバ上で管理コンソールにアクセスしない場合は不要です。   |
| hb.serversecurity-nec.jp:443         | 管理サーバとの疎通確認、イベントログの送信等  |  |
| rera.y.serversecurity-nec.jp:443     | セキュリティアップデート(インターネット直結) | プロキシを経由する場合利用しません。   |
| iaus.trendmicro.com:443              | セキュリティアップデート(プロキシ環境)    | Trend Micro社 Active Update サーバ。<br>プロキシを経由しない場合でも、アクセス可能にすることで可用性が向上します。 |
| iaus.activeupdate.trendmicro.com 443 |                         |  |

# 目次

## 事前準備

1. ライセンス証書の確認
2. 管理サーバログイン
3. アクティベーションコードの入力
  - a. 侵入防御のみの場合
  - b. アンチウイルス有りの場合
4. プロキシ登録
5. 有効化コマンドの作成
6. アップグレード媒体・カーネル  
サポートパッケージ（KSP）の入手

## サーバへ Agent を導入する手順

7. パッケージの展開
8. 不要なモジュールの削除
  - a. 侵入防御のみの場合
  - b. アンチウイルス有りの場合
9. インストールディレクトリ作成
10. KSPのインポート

11. インストール
12. 有効化/有効化の確認
13. 推奨スキャンの実施

14. 補足
15. 注意事項

## 参考情報 Appendix

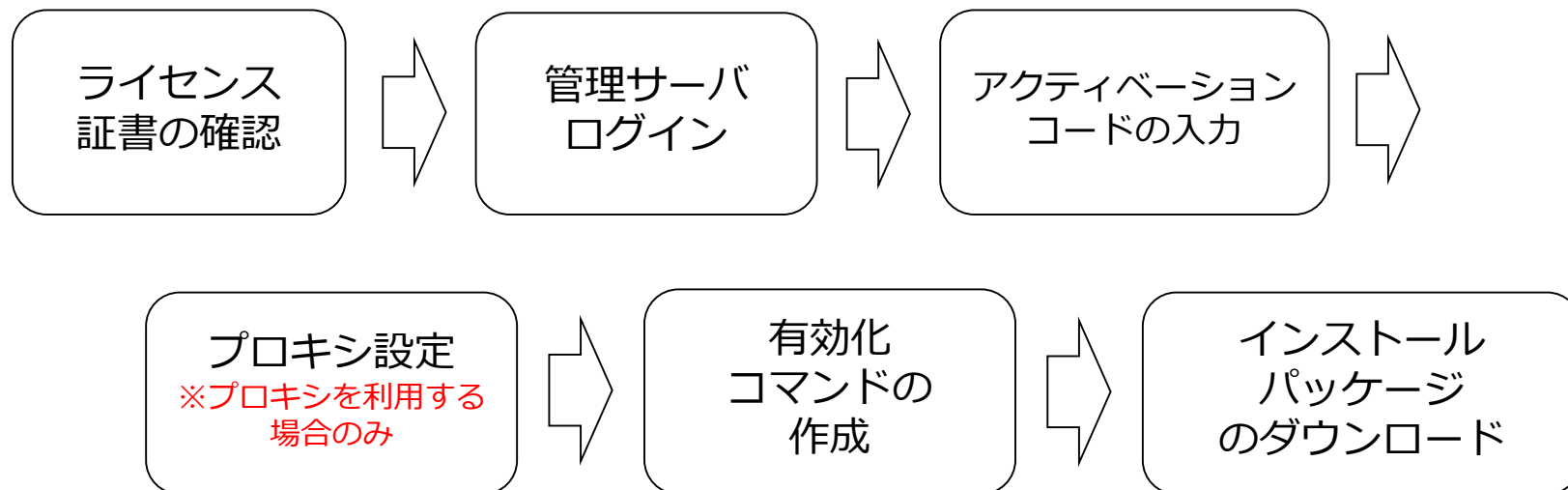
## 更新履歴

# 事前準備（保護対象サーバ外で実施可能）

Agent 導入前にManagerコンソール上で、  
ライセンスの確認やアクティベーション、プロキシ設定を行います。

## 注意事項

- ライセンス証書は外部に公開しない様、慎重にお取扱いください。



# 1. ライセンス証書の確認

別途送付したライセンス証書より、  
アカウント情報・アクティベーションコード（赤枠部分）を確認して下さい。

**NEC**

ライセンス証書

日本電気株式会社

以下のソフトウェア製品に関して、日本電気株式会社は、本証書および「サーバセキュリティサービス with Trend Micro Deep Security 使用許諾書 兼 サービス利用許諾書」により権利を許諾する。

型番：UL1563-H007-I  
製品名：サーバセキュリティサービス with Trend Micro Deep Security V9 新規  
1CL 仮想パッチ  
シート数：5  
サービス期間：1年  
サービス開始日：20x1年4月1日  
サービス終了日：20x2年3月31日

【アカウント情報】  
URL：https://xxx.xxx.xxx  
アカウント名：●●●●●  
ユーザ名：●●●●●  
パスワード：●●●●●

【アクティベーションコード】  
XX-XXXX-XXXXXX-XXXXXX-XXXXXX-XXXXXX

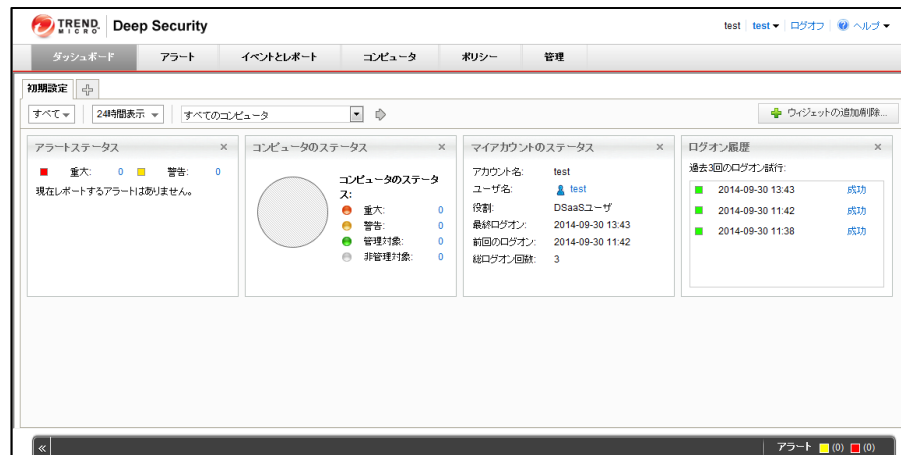
●シート数に記載の数量を上限として使用する。

この情報は、管理サーバログイン等に使用します。  
再発行は致しかねますので大切に保管ください。  
また、外部に公開しない様、慎重にお取り扱いください。

## 2. 管理サーバログイン

### 手順

- ① ライセンス証書のアカウント情報 > URL に記載してあるURLにアクセス
- ② ライセンス証書のアカウント情報 > アカウント名/ユーザ名/パスワードを入力してログイン

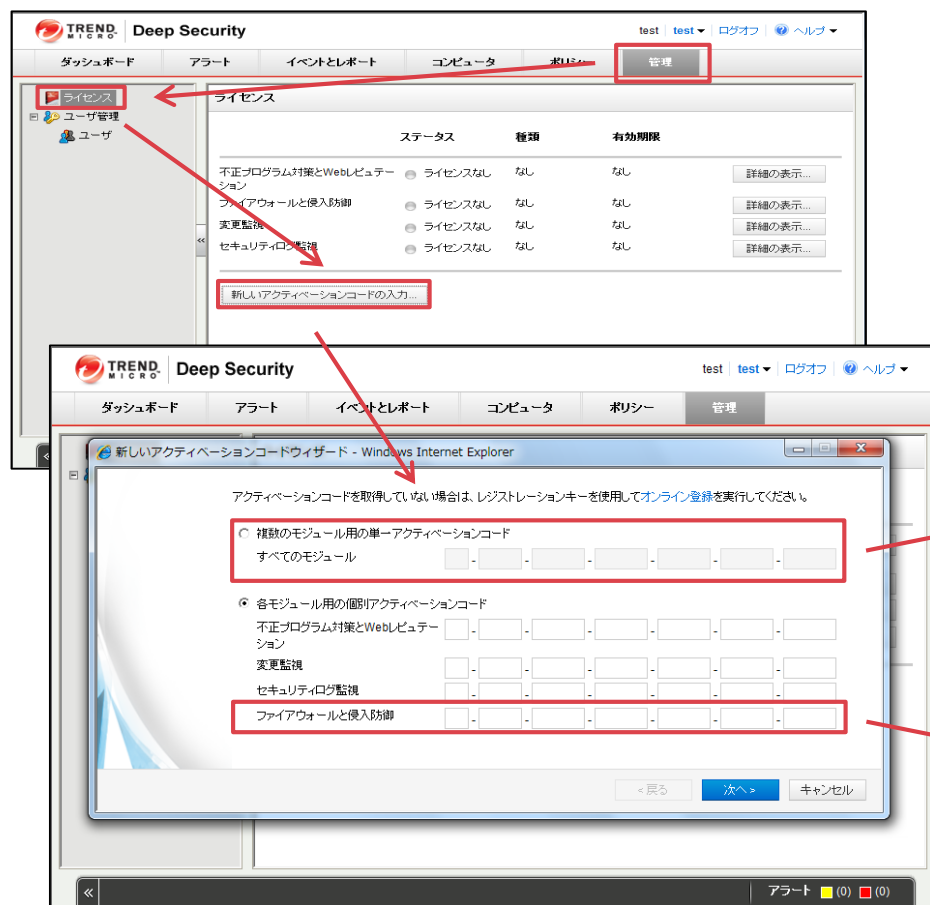




# 3. アクティベーションコードの入力(1)

## 手順

- ① [管理] > [ライセンス] > [新しいアクティベーションコードの入力]をクリック
- ② お客様のご契約内容に合わせて、アクティベーションコードを入力



・ アンチウィルスを含む場合  
→すべてのモジュール

・ 侵入防御(仮想パッチ)のみの場合  
→ファイアウォールと侵入防御

### 3. アクティベーションコードの入力(2a) 侵入防御のみ

仮想パッチ（侵入防御）ライセンスでご購入のお客様はこちらをご参照ください ※仮想パッチ&アンチウイルスライセンスでご購入のお客様は次頁をご参照ください。

#### ③ アクティベートを完了させて、有効なライセンスを確認

ライセンスの内容をご確認下さい。

「ファイアウォールと侵入防御」のアクティベートが完了

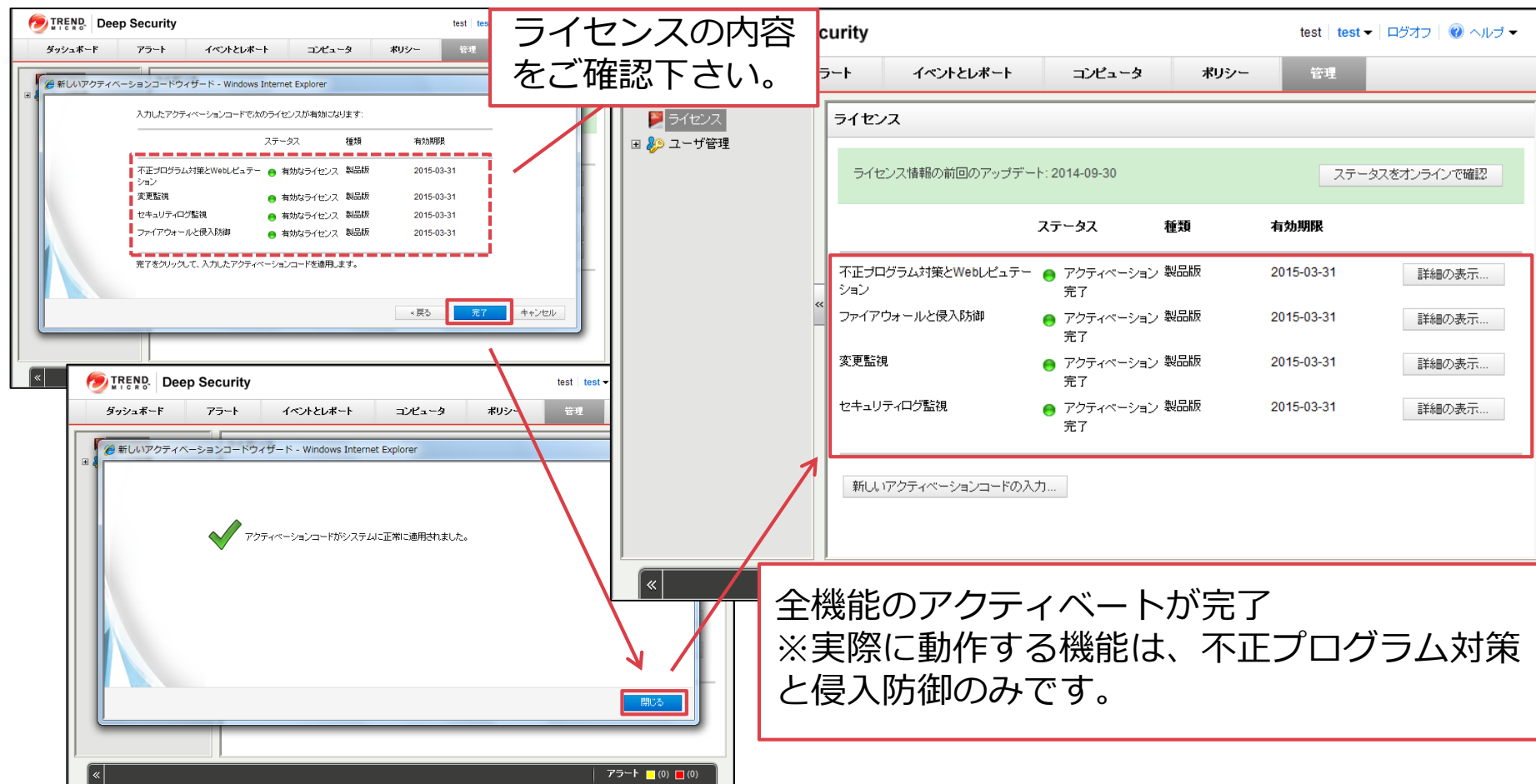
| ステータス         | 種類           | 有効期限       |
|---------------|--------------|------------|
| ファイアウォールと侵入防御 | 有効なライセンス 製品版 | 2015-03-31 |

| ステータス                | 種類          | 有効期限       |
|----------------------|-------------|------------|
| 不正プログラム対策とWebレピューション | ライセンスなし     | なし         |
| ファイアウォールと侵入防御        | アクティベーション完了 | 2015-03-31 |
| 変更監視                 | ライセンスなし     | なし         |
| セキュリティログ監視           | ライセンスなし     | なし         |

### 3. アクティベーションコードの入力(2b) アンチウイルス有り

仮想パッチ&アンチウイルスライセンスでご購入のお客様はこちらをご参照ください ※仮想パッチライセンスでご購入のお客様は前頁をご参照ください。

#### ③ アクティベートを完了させて、有効なライセンスを確認



ライセンスの内容をご確認下さい。

| ステータス                | 種類           | 有効期限       |
|----------------------|--------------|------------|
| 不正プログラム対策とWebレピューション | 有効なライセンス 製品版 | 2015-03-31 |
| 変更監視                 | 有効なライセンス 製品版 | 2015-03-31 |
| セキュリティログ監視           | 有効なライセンス 製品版 | 2015-03-31 |
| ファイアウォールと侵入防御        | 有効なライセンス 製品版 | 2015-03-31 |

完了をクリックして、入力したアクティベーションコードを適用します。

完了

アクティベーションコードがシステムに正常に適用されました。

閉じる

ライセンス

ライセンス情報の前回のアップデート: 2014-09-30

ステータスをオンラインで確認

| ステータス                | 種類               | 有効期限       |
|----------------------|------------------|------------|
| 不正プログラム対策とWebレピューション | アクティベーション 完了 製品版 | 2015-03-31 |
| ファイアウォールと侵入防御        | アクティベーション 完了 製品版 | 2015-03-31 |
| 変更監視                 | アクティベーション 完了 製品版 | 2015-03-31 |
| セキュリティログ監視           | アクティベーション 完了 製品版 | 2015-03-31 |

詳細の表示...

新しいアクティベーションコードの入力...

全機能のアクティベートが完了  
※実際に動作する機能は、不正プログラム対策と侵入防御のみです。

## 4. プロキシ登録

プロキシをご利用でない環境の場合、本手順は不要です

### 手順

- ① [管理] > [アップデート] > [Relayグループ] > [新規...] を選択
- ② 任意の一般情報を入力し、[プロキシ]タブで新規にプロキシを登録するか既存のプロキシ設定を選択
- ③ [OK]をクリックしプロキシ情報を登録

The screenshot illustrates the process of registering a proxy in the NEC security management system. It shows three overlapping windows:

- Relayグループ (Relay Group) - Internet Explorer:** The '新規...' (New...) button is highlighted with a red box. The '一般' (General) tab is active, showing fields for '名前' (Name) and '説明' (Description). The 'プロキシ' (Proxy) tab is also visible.
- Relayグループ - Internet Explorer:** The 'プロキシ' (Proxy) tab is active. A dropdown menu is open, showing '新規...' (New...) as the selected option. The 'OK' button is highlighted with a red box.
- 新しいプロキシのプロパティ (New Proxy Properties) - Internet Explorer:** The '一般' (General) tab is active. The '名前' (Name) field is highlighted with a red box. The 'プロキシ設定' (Proxy Settings) section shows the 'プロキシプロトコル' (Proxy Protocol) set to 'HTTP'. The 'OK' button is highlighted with a red box.

Red arrows indicate the flow of the process: from the '新規...' button in the first window to the 'プロキシ' tab in the second, then to the '新規...' option in the dropdown, and finally to the 'OK' button in the third window.

## 5. 有効化コマンドの作成(1)

### 手順

- ① [サポート情報] > [インストールスクリプト]より、スクリプト作成ウィンドウを起動
- ② プラットフォームを導入環境に合わせて選択



※注

管理コンソールは以下のWebブラウザで動作を保証します。

- ・ Mozilla Firefox (Cookie を有効にする)
- ・ Internet Explorer 9, 10, 11 (Cookie を有効にする)

Internet Explorer 8 ではプラットフォームが表示されません。

Deep Security AgentはRightScale、Chef、Puppet、SSHなどのツールを使用してインストールできます。このインストールスクリプトジェネレータを使用して、必要なスクリプトを生成します。

プラットフォーム:

Linux Agent環境

☐ インストール後にAgentを自動的に有効化 (セキュリティポリシーを割り当てる場合はチェックボックスをオンにします)

```
#/bin/bash
# This script detects platform and architecture, download and install matching Deep Security Agent package
if ! (type curl &>/dev/null); then echo Please install CURL before running this script;
  logger -t Please install CURL before running this script; exit 1;
fi;
SOURCEURL='https://serversecurity-nec.jp:443'
curl $SOURCEURL/software/deploymentscript/platform/linux/ -o /tmp/DownloadInstallAgentPackage --insecure --silent

if [ -s /tmp/DownloadInstallAgentPackage ]; then ./tmp/DownloadInstallAgentPackage
  Download_Install_Agent;
else echo "fail to download agent installation script";
  logger -t Fail to download Deep Security Agent installation script
```

クリップボードにコピー

閉じる

## 5. 有効化コマンドの作成(2)

- ③ [インストール後にAgentを自動的に有効化（セキュリティポリシーを割り当てる場合はチェックボックスをオンにします）]にチェックを入れる
- ④ セキュリティポリシーを選択。※後ほど適用することも可能
- ⑤ コンピュータグループを選択。※後ほど作成、グループ分けすることも可能
- ⑥ **（プロキシをご利用の場合）** P.12で作成したRelayグループ、およびプロキシを選択
- ⑦ 表示されるスクリプトのうち、「/opt/ds\_agent/dsa\_control -r」以降をコピーし、テキストエディタ等に貼り付け

インストールスクリプト

Deep Security AgentはRightScale、Chef、Puppet、SSHなどのツールを使用してインストールできます。このインストールスクリプトジェネレータを使用して、必要なスクリプトを生成します。

プラットフォーム: Linux Agent環境

☒ インストール後にAgentを自動的に有効化（セキュリティポリシーを割り当てる場合はチェックボックスをオンにします）

セキュリティポリシー: サーバセキュリティサービスポリシー

コンピュータグループ: コンピュータ

Relayグループ: プライマリテナントのRelayグループ

Deep Security Managerとの接続に使用するプロキシ: test

Agentからのリモート有効化では、ホスト名、説明、一意のID、およびその他のプロパティも設定できます。詳細にコマンドラインの手順ページを参照してください。

```
if [ -s /tmp/DownloadInstallAgentPackage ]; then ./tmp/DownloadInstallAgentPackage
Download_Install_Agent;
else echo "fail to download agent installation script";
logger -t Fail to download Deep Security Agent installation script
fi

sleep 15

/opt/ds_agent/dsa_control -r
/opt/ds_agent/dsa_control -x dsm_proxy://test.xxx.jp:808/
/opt/ds_agent/dsa_control -a dsm://hb.serversecurity-nec.jp:443/ "tenantID: [redacted]" "tenantPassword: [redacted]" "policyid:18"
```

プロキシで認証を行う場合

「/opt/ds\_agent/dsa\_control -x "dsm\_proxy://プロキシサーバのURL:ポート/"」行の次行に

「/opt/ds\_agent/dsa\_control -u "ユーザ名:パスワード"」

と入力してください。

例) 「ユーザ名: root、パスワード: Password」の場合

/opt/ds\_agent/dsa\_control -u "root:Password"

※認証は基本認証のみ対応しています

無題 - メモ帳

ファイル(F) 編集(E) 書式(O) 表示(V) ヘルプ(H)

```
/opt/ds_agent/dsa_control -r
/opt/ds_agent/dsa_control -x dsm_proxy://test.xxx.jp:808/
/opt/ds_agent/dsa_control -a dsm://hb.serversecurity-nec.jp:443/ "tenantID: [redacted]" "tenantPassword: [redacted]" "policyid:18"
```

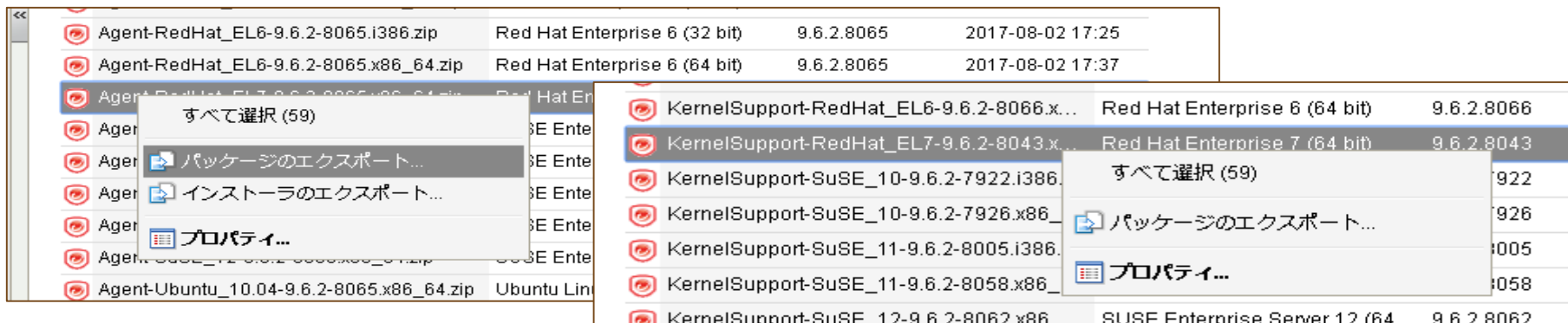
## 6.アップグレード媒体・カーネルサポートパッケージ (KSP)の入手

### 手順

- ① サーバセキュリティサービスのコンソールにログイン
- ② [管理]→[ソフトウェア]→[ローカル]を選択
- ③ 「バージョン」でグループ化
- ④ 9.6.2グループの中からご利用の環境のプラットフォームのAgentモジュール（ファイル名の先頭が"Agent"から始まるもので、ファイル名に含まれる[9.6.2-]に続く4桁の数値が一番大きなファイル）を右クリック

※該当のグループが見つからない場合は次のページを参照してください

- ⑤ [パッケージのエクスポート]を選択
- ⑥ ④同様に9.6.2グループの、カーネルサポートパッケージ（ファイル名の先頭が"KernelSupport"から始まるもので、ファイル名に含まれる[9.6.2-]に続く4桁の数値が一番大きなファイル）を右クリック
- ⑦ [パッケージのエクスポート]を選択



## (参考) 9.6.2のグループが見つからない場合

■ 複数のコンポーネントがインポートされているため、複数のページに分かれています

■ 以下キャプチャに従い2ページ目を参照してください。

The screenshot shows the NEC management console interface. The top navigation bar includes 'アラート' (Alerts), 'イベントとレポート' (Events and Reports), 'コンピュータ' (Computers), 'ポリシー' (Policies), and '管理' (Management). The main content area is divided into two sections. The left section, titled 'ローカルソフトウェア' (Local Software), shows a table with columns '名前' (Name), 'プラットフォーム' (Platform), 'バージョン' (Version), and 'インポート済み' (Imported). The right section, titled 'ポリシー' (Policies), shows a table with columns 'プラットフォーム' (Platform), 'バージョン' (Version), and 'インポート済み' (Imported). Both tables are paginated. The first page of the left table shows '9.5.3 (373)'. The first page of the right table shows 'Linux AMI (32 bit)', 'Linux AMI (64 bit)', 'Linux 5 (32 bit)', 'Linux 5 (64 bit)', 'CloudLinux 6 (32 bit)', 'CloudLinux 6 (64 bit)', 'CloudLinux 7 (64 bit)', 'Debian 6 (64 bit)', 'Debian 7 (64 bit)', 'Oracle Linux Release 5 (32 bit)', 'Oracle Linux Release 5 (64 bit)', 'Oracle Linux Release 6 (32 bit)', 'Oracle Linux Release 6 (64 bit)', 'Oracle Linux Release 7 (64 bit)', and 'Red Hat Enterprise 5 (32 bit)'. Red boxes and arrows highlight the pagination controls. The first page of the left table has a 'ページ 1 / 2' (Page 1 / 2) control. The first page of the right table has a 'ページ 1 / 2' (Page 1 / 2) control. The second page of the right table has a 'ページ 2 / 2' (Page 2 / 2) control. A red arrow points from the 'ページ 1 / 2' control of the left table to the 'ページ 2 / 2' control of the right table.

| 名前          | プラットフォーム | バージョン | インポート済み |
|-------------|----------|-------|---------|
| 9.5.3 (373) |          |       |         |

| プラットフォーム                        | バージョン      | インポート済み          |
|---------------------------------|------------|------------------|
| Linux AMI (32 bit)              | 9.6.2.8065 | 2017-08-02 17:27 |
| Linux AMI (64 bit)              | 9.6.2.8065 | 2017-08-02 17:28 |
| Linux 5 (32 bit)                | 9.6.2.8065 | 2017-08-02 17:35 |
| Linux 5 (64 bit)                | 9.6.2.8065 | 2017-08-02 17:29 |
| CloudLinux 6 (32 bit)           | 9.6.2.8065 | 2017-08-02 17:28 |
| CloudLinux 6 (64 bit)           | 9.6.2.8065 | 2017-08-02 17:30 |
| CloudLinux 7 (64 bit)           | 9.6.2.8065 | 2017-08-02 17:33 |
| Debian 6 (64 bit)               | 9.6.2.8065 | 2017-08-02 17:33 |
| Debian 7 (64 bit)               | 9.6.2.8065 | 2017-08-02 17:25 |
| Oracle Linux Release 5 (32 bit) | 9.6.2.8065 | 2017-08-02 17:33 |
| Oracle Linux Release 5 (64 bit) | 9.6.2.8065 | 2017-08-02 17:27 |
| Oracle Linux Release 6 (32 bit) | 9.6.2.8065 | 2017-08-02 17:34 |
| Oracle Linux Release 6 (64 bit) | 9.6.2.8065 | 2017-08-02 17:30 |
| Oracle Linux Release 7 (64 bit) | 9.6.2.8065 | 2017-08-02 17:33 |
| Red Hat Enterprise 5 (32 bit)   | 9.6.2.8065 | 2017-08-02 17:32 |

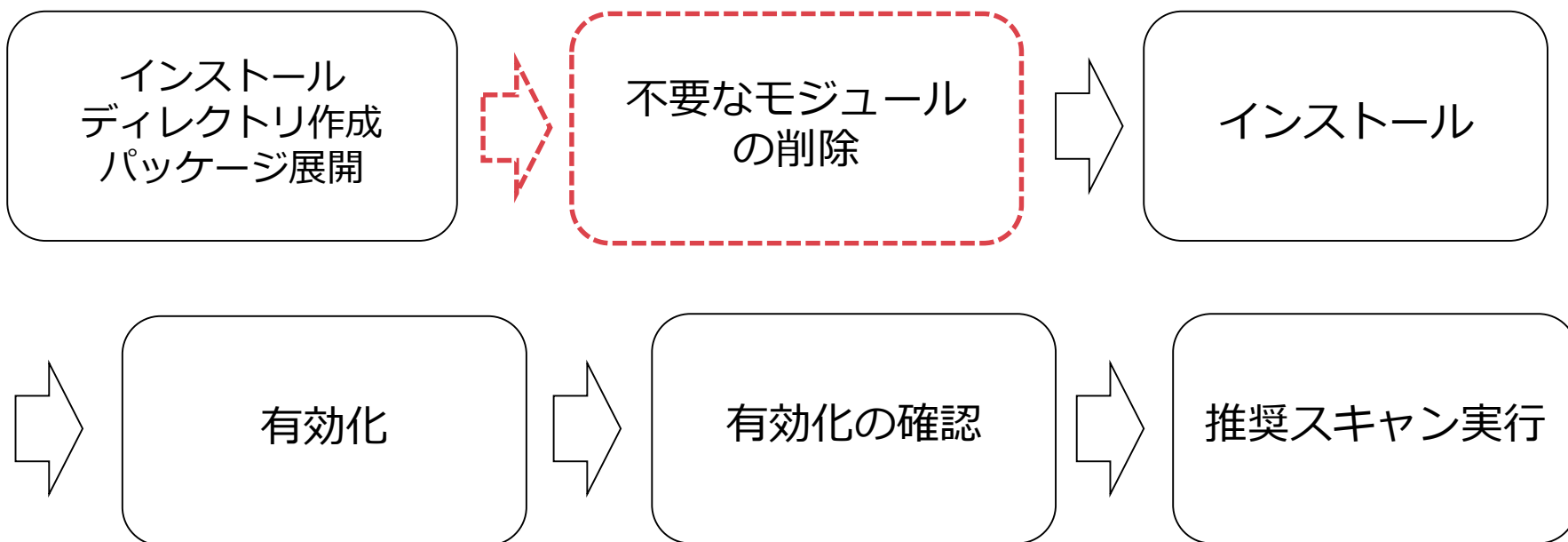


# サーバへ Agent を導入する手順

Agentをインストール後、コマンドラインで有効化を行います。

## 注意事項

- 必ず「Deep Security Agent 9.6 SP1」をダウンロードしてご利用下さい。  
※ Deep Security Agent 10など、9.6 Sp1より後のリリースバージョンはサポート対象外です
- 手順は管理者権限もしくは「sudo」コマンドにて実施して下さい。



## 7. パッケージ展開

■ 手順 ※手順は管理者権限もしくは「sudo」 コマンドで実施して下さい。

- ① インストールパッケージ、カーネルサポートパッケージを任意のディレクトリに格納
- ② インストールパッケージ、カーネルサポートパッケージを展開

※上書きを確認された場合はA（ALL-すべて上書き）を選択。

```
versions.txt  
[root@DSCentOS64 ds_agent]# unzip KernelSupport-RedHat_EL6-9.6.2-8066.x86_64.zip  
Archive:  KernelSupport-RedHat_EL6-9.6.2-8066.x86_64.zip  
replace META-INF/MANIFEST.MF? [y]es, [n]o, [A]ll, [N]one, [r]ename: A
```

## 8. 不要なモジュールの削除(a) 侵入防御のみ

仮想パッチ（侵入防御）ライセンスでご購入のお客様はこちらをご参照ください ※仮想パッチ&アンチウイルスライセンスでご購入のお客様は次頁をご参照ください

■ 仮想パッチのみをご利用(アンチウイルスを利用しない)のお客様は**以下の必要なモジュールを残し、その他の拡張子.dspのファイルを削除**してください。

※削除しない場合、予期せぬ問題が発生する事例が確認されております

- 侵入防御機能
  - Feature-DPI-\*.dsp
  - Plugin-FWDPI-\*.dsp
  - Plugin-Filter\*.dsp

※ \*にはバージョンに応じた英数字文字列が入ります

## 8. 不要なモジュールの削除(b) アンチウイルス含むアンチウイルス含む

仮想パッチ&アンチウイルスライセンスでご購入のお客様はこちらをご参照ください ※仮想パッチライセンスでご購入のお客様は前頁をご参照ください

■ 仮想パッチ&アンチウイルスをご利用のお客様は**以下の必要なモジュールを残し、その他の拡張子.dspのファイルを削除**してください。

※削除しない場合、予期せぬ問題が発生する事例が確認されております

- 不正プログラム対策機能
  - Feature-AM-\*.dsp
  - Plugin-UPDATE-\*.dsp
  - Plugin-VFS\_Filter-\*.dsp (Red Hat/SuSEのみ)
- 侵入防御機能
  - Feature-DPI-\*.dsp
  - Plugin-FWDPI-\*.dsp
  - Plugin-Filter\*.dsp

※ \*にはバージョンに応じた英数字文字列が入ります

## 9. インストールディレクトリ作成

■ 手順 ※手順は管理者権限もしくは「sudo」 コマンドで実施して下さい。

- ① 以下コマンドでインストールディレクトリを作成  
# mkdir /opt/ds\_agent
- ② ディレクトリ権限を変更  
# chmod 777 /opt/ds\_agent
- ③ インストールディレクトリに移動  
# cd /opt/ds\_agent
- ④ P.18-20の処理後のファイルをインストールディレクトリにコピー

(実行例)

```
[root@localhost administrator]# mkdir /opt/ds_agent
[root@localhost administrator]# chmod 777 /opt/ds_agent
[root@localhost administrator]# cd /opt/ds_agent
[root@localhost ds_agent]# ls
Agent-RedHat_EL7-9.5.3-2754.x86_64.zip
[root@localhost ds_agent]# unzip Agent-RedHat_EL7-9.5.3-2754.x86_64.zip
```

# 10.KSPのインポート

## 手順

- ① インストールディレクトリ配下に以下コマンドでdownloadsディレクトリを作成  
# mkdir -p /var/opt/ds\_agent/downloads
- ② P.21 の④を処理後のインストールディレクトリ以下のファイルをdownloadsディレクトリにコピー  
# cp -r /opt/ds\_agent/\* /var/opt/ds\_agent/downloads

```
[root@DSCentOS64 ds_agent]#  
[root@DSCentOS64 ds_agent]# mkdir -p /var/opt/ds_agent/downloads  
[root@DSCentOS64 ds_agent]# cp -r /opt/ds_agent/* /var/opt/ds_agent/downloads  
[root@DSCentOS64 ds_agent]#
```

# 11. インストール

## 手順

### ① 以下のコマンドでインストールを実行

※利用するAgentによって、ファイル名が異なります。異なる部分は「xxxxxxx」と記載しています。

(Red Hat系)

```
# rpm -i Agent-Core-xxxxxxx.rpm
```

(Debian系)

```
# dpkg -i Agent-Core-xxxxxxx.deb
```

```
[root@localhost ds_agent]# rpm -i Agent-Core-RedHat_EL7-9.5.3-2754.x86_64.rpm
Starting ds_agent (via systemctl): [ OK ]
```

```
[root@localhost ds_agent]# ls
Agent-Core-RedHat_EL7-9.5.3-2754.x86_64.rpm
Agent-RedHat_EL7-9.5.3-2754.x86_64.zip
Feature-DPI-RedHat_EL7-9.5.3-2754.x86_64.dsp
Feature-FW-RedHat_EL7-9.5.3-2754.x86_64.dsp
Feature-IM-RedHat_EL7-9.5.3-2754.x86_64.dsp
Feature-LI-RedHat_EL7-9.5.3-2754.x86_64.dsp
Feature-RELAY-RedHat_EL7-9.5.3-2754.x86_64.dsp
Feature-WRS-RedHat_EL7-9.5.3-2754.x86_64.dsp
META-INF
Plugin-FWDPI-RedHat_EL7-9.5.3-2754.x86_64.dsp
Plugin-Filter-RedHat_EL7-9.5.3-2754.x86_64.dsp
Plugin-Filter_3_10_0_123_13_1_el7_x86_64-RedHat_EL7-9.5.3-2754.x86_64.dsp
Plugin-Filter_3_10_0_123_13_2_el7_x86_64-RedHat_EL7-9.5.3-2754.x86_64.dsp
Plugin-Filter_3_10_0_123_1_2_el7_x86_64-RedHat_EL7-9.5.3-2754.x86_64.dsp
Plugin-Filter_3_10_0_123_4_2_el7_x86_64-RedHat_EL7-9.5.3-2754.x86_64.dsp
Plugin-Filter_3_10_0_123_4_4_el7_x86_64-RedHat_EL7-9.5.3-2754.x86_64.dsp
Plugin-Filter_3_10_0_123_6_3_el7_x86_64-RedHat_EL7-9.5.3-2754.x86_64.dsp
Plugin-Filter_3_10_0_123_8_1_el7_x86_64-RedHat_EL7-9.5.3-2754.x86_64.dsp
Plugin-Filter_3_10_0_123_9_2_el7_x86_64-RedHat_EL7-9.5.3-2754.x86_64.dsp
```

インストールパッケージはP.21でコピーしたファイルに含まれます。

インストール中にネットワークの瞬断が発生します。





## 12. 有効化/有効化の確認

### 手順

[コンピュータ]タブより、対象のコンピュータが追加されていることを確認

※Agent有効化後、Agentに対して自動でセキュリティアップデートが行われます。



The screenshot shows the Trend Micro Deep Security interface. The 'コンピュータ' (Computers) tab is selected. A table displays the following information:

| 名前              | プラットフォーム          | セキュリティアップデートのダウンロード... | ポリシー          | ステータス        |
|-----------------|-------------------|------------------------|---------------|--------------|
| コンピュータ (1)      |                   |                        |               |              |
| WIN-1CL0R0GI3Q8 | Microsoft Wind... | 初期設定のRelayグループ         | サーバセキュリティサ... | 管理対象 (オンライン) |

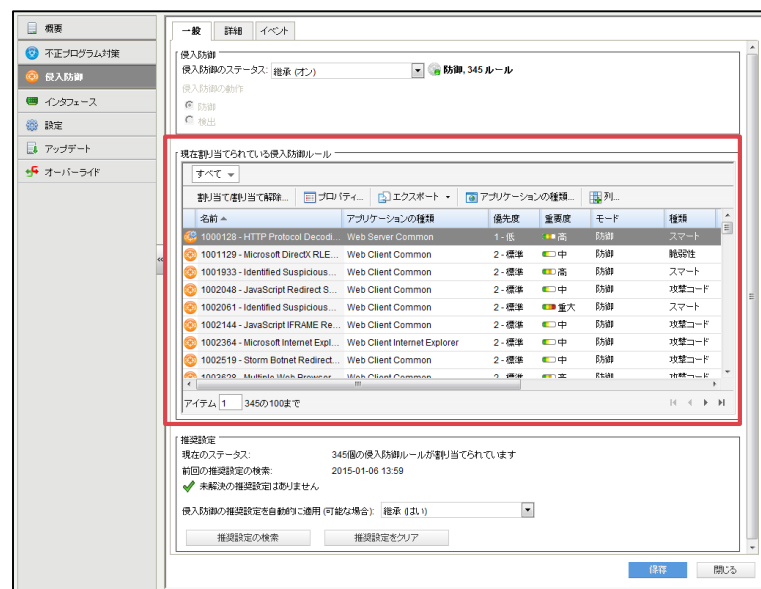
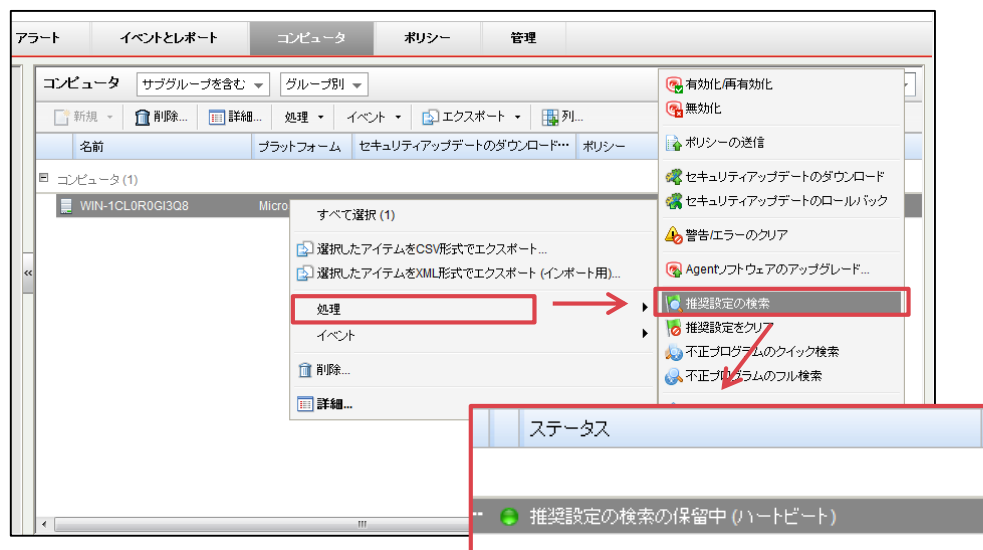
A red box highlights the status '管理対象 (オンライン)' in the table. A red callout box contains the text: 管理対象（オンライン）を表示していれば、有効化されています。

# 13. 推奨スキャンの実施(1)

仮想パッチルールを適用する為に有効化完了後、推奨スキャンを実行する必要があります。

## 手順

- ① [コンピュータ]タブより、対象クライアントを右クリック
- ② [処理] > [推奨設定の検索] をクリックし推奨スキャンをクリック
- ③ ステータス列に「推奨設定の検索の保留中(ハートビート)」が表示され、数分後に推奨設定が実行
- ④ 推奨スキャン実施後、対象コンピュータをダブルクリックし、[侵入防御]を選択。  
[一般]タブにて割り当てられている仮想パッチを確認可能



## 13. 推奨スキャンの実施(2)

推奨スキャン完了後、「未解決の推奨設定」がある場合は下記の手順でルール割り当てが可能です。※自動的に適用できないルールがあるため、下記の手順が必要となります。

### 手順

- ① [割り当て/割り当て解除...]をクリック
- ② IPSルールの中央のボックスから[割り当てを推奨 or 割り当て解除を推奨]を選択
- ③ ルールを割り当てる場合、表示されたルールの左側のチェックボックスをチェック、割り当て解除する場合。チェックを外し、[OK]ボタンを押下

The screenshot displays the '現在割り当てられている侵入防御ルール' (Currently Assigned Intrusion Defense Rules) window. The main table lists rules with columns for Name, Application Type, Priority, Importance, and Mode. A red box highlights the '割り当て/割り当て解除...' button in the top toolbar. Another red box highlights the '割り当てを推奨' (Recommend Assignment) button in the context menu. A third red box highlights the 'OK' button at the bottom right. A red arrow points from the '割り当てを推奨' button to the 'OK' button.

現在割り当てられている侵入防御ルール

| 名前                                  | アプリケーションの種類       | 優先度    | 重要度 | モード |
|-------------------------------------|-------------------|--------|-----|-----|
| 1000128 - HTTP Protocol Decod...    | Web Server Common | 1 - 低  | 高   | 防御  |
| 1001129 - Microsoft DirectX RLE...  | Web Client Common | 2 - 標準 | 中   | 防御  |
| 1001933 - Identified Suspicious ... | Web Client Common | 2 - 標準 | 高   | 防御  |
| 1002048 - JavaScript Redirect S...  | Web Client Common | 2 - 標準 | 中   | 防御  |

アイテム 1 107の100まで

推奨設定

現在のステータス: 107個の侵入防御ルールが割り当てられています

前回の推奨設定の検索: 2015-01-06 14:03

未解決の推奨設定: 1個の追加ルールの割り当て

侵入防御の推奨設定を自動的に適用 (可能な場合): 継承 (いい)

誤検知のリスクが高い等の理由で一部の推奨されたルールが自動割り当てされない仕様になっています。詳細は以下のURLをご参照ください。

<http://esupport.trendmicro.com/solution/ja-JP/1311156.aspx>

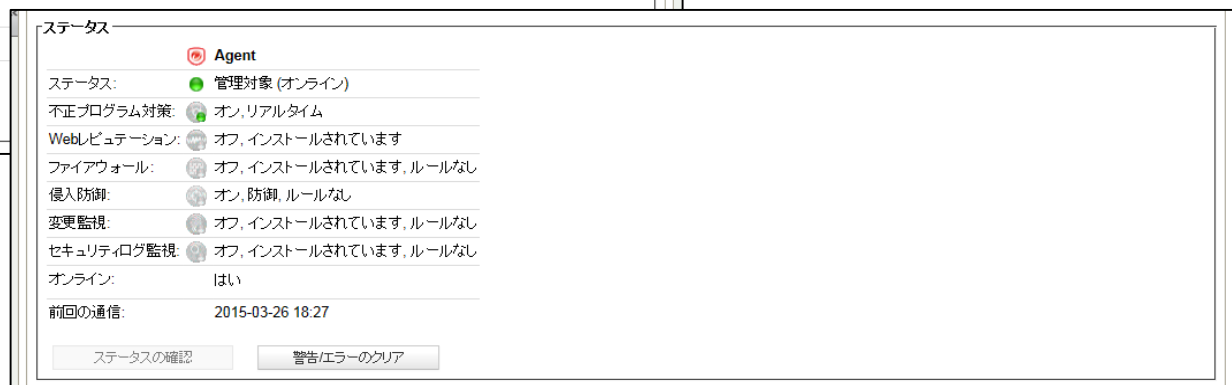
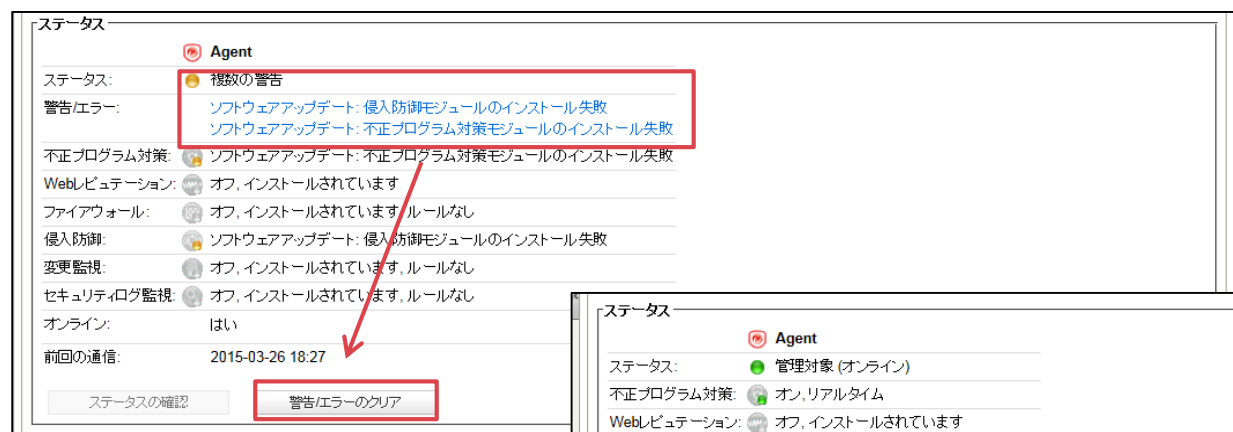
# 14. 補足 (1)

「ソフトウェアアップデート: ○○○モジュールのインストール失敗」アラートが表示された場合の対処方法。

※ソフトウェアの仕様上、導入後に上記のアラートが表示される可能性があります、

## 手順

- ① 対象のコンピュータをダブルクリックし、[警告/エラーのクリア]をクリック
- ② ステータスに「インストールされていません」と表示されていない事を確認

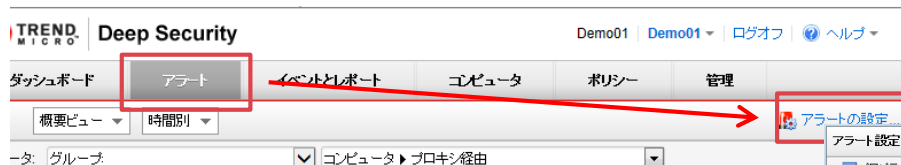


## 14. 補足 (2)

製品仕様により、「空のRelayグループが割り当てられています。」とアラートが表示されます。**※動作に影響はありません**  
アラートを非表示にする場合は、以下の手順に従い設定して下さい。

### 手順

- ① [アラート]→[アラートの設定]を選択
- ② 「空のRelayグループの割り当て」を選択
- ③ 「オフ」を選択し、OKを押下

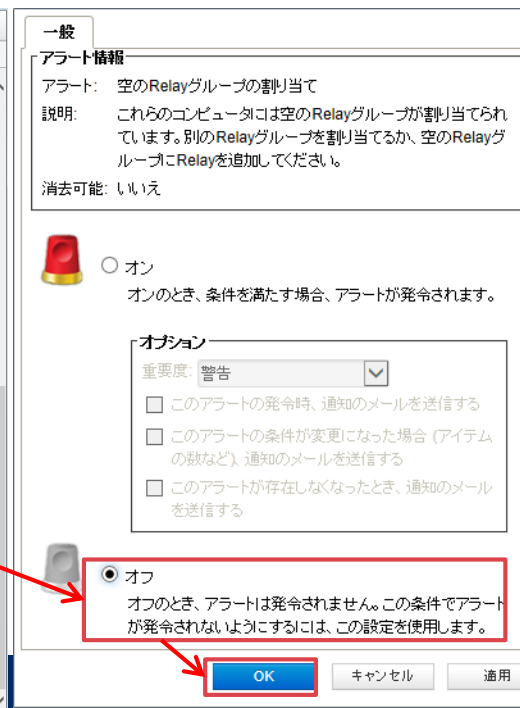
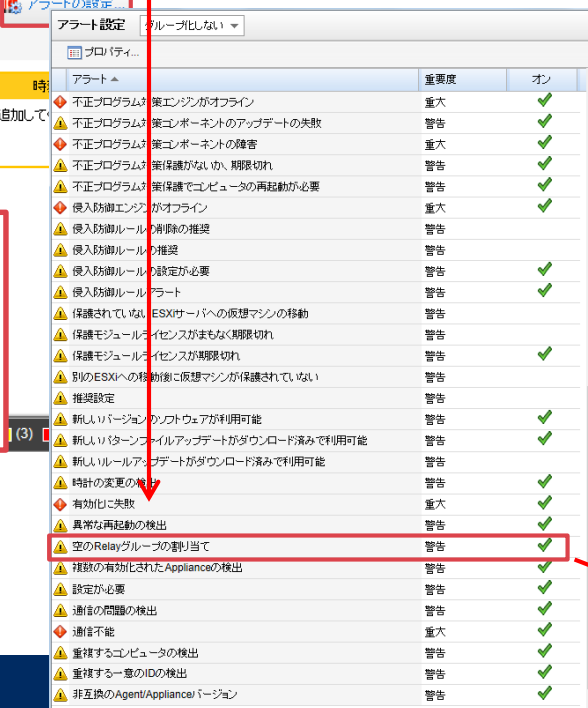


コンピュータに空のRelayグループが割り当てられています  
のコンピュータは空のRelayグループが割り当てられています。別のRelayグループを割り当てるか、空のRelayグループにRelayを追加して

細い表示

仕様上、プロキシを経由する場合はRelayに接続せず、Trend Micro Active Update サーバより直接アップデートを行います。

よってRelayをRelayグループに割り当てる必要は無く、上記のアラートをオフにしても問題ございません。



## 14. 補足 (3)

初期設定では、侵入防御イベントがアラートに上がらない設定になっています。

検知した侵入防御イベントをアラートに上げ、アラートメールを送信させるには下記の手順を実施して下さい。

### 手順

- ① [アラート]タブより、[アラートの設定]をクリック
- ② [侵入防御ルールアラート]をダブルクリック
- ③ [(ルール設定に関係なく) すべてのルールでアラート]をチェックし[OK]をクリック

The screenshot shows the Trend Micro Deep Security console. The 'Alerts' tab is selected, and the 'Alert Settings' dialog is open. The 'Alert Information' section shows the alert name 'Intrusion Defense Rule Alert' and its description. The 'Options' section shows the 'Alert Severity' set to 'Warning' and the 'Alert Action' set to 'Send email notification'. The 'Alert Action' section shows the 'Alert Action' set to 'Send email notification' and the 'Alert Action' set to 'Send email notification'.

| 時刻               | 重要度 | アラート |
|------------------|-----|------|
| (リストにアイテムがありません) |     |      |

アラート設定 (グループ化しない)

| アラート                        | 重要度 | オン |
|-----------------------------|-----|----|
| ポリシー送信の失敗                   | 重大  | ✓  |
| メモリの書き込み量の超過                | 警告  | ✓  |
| メモリの読み込み量の超過                | 重大  | ✓  |
| ユーザのロックアウト                  | 警告  | ✓  |
| ユーザパスワードがまもなく有効期限切れ         | 警告  | ✓  |
| ルールのアップデートが利用可能             | 警告  | ✓  |
| 不正プログラムの予知検知がスキップされました      | 警告  | ✓  |
| 不正プログラム対策の隔離ファイルがストレージ制限を超過 | 警告  | ✓  |
| 不正プログラム対策アラート               | 警告  | ✓  |
| 不正プログラム対策エンジンがオフライン         | 重大  | ✓  |
| 不正プログラム対策コンポーネントのアップデートの失敗  | 警告  | ✓  |
| 不正プログラム対策コンポーネントの障害         | 重大  | ✓  |
| 不正プログラム対策保護がまもなく期限切れ        | 警告  | ✓  |
| 不正プログラム対策保護でコンピュータの再起動が必要   | 警告  | ✓  |
| 仮想マシンインターフェースの非同期           | 警告  | ✓  |
| 侵入防御エンジンがオフライン              | 重大  | ✓  |
| 侵入防御ルールの削除の権限               | 警告  | ✓  |
| 侵入防御ルールの検出                  | 警告  | ✓  |
| 侵入防御ルールの設定が必要               | 警告  | ✓  |
| 侵入防御ルールアラート                 | 警告  | ✓  |
| 保護されていないESXサーバへの仮想マシンの移動    | 警告  | ✓  |
| 保護モジュールライセンスがまもなく期限切れ       | 警告  | ✓  |
| 保護モジュールライセンスが期限切れ           | 警告  | ✓  |
| 別のESXへの移動前に仮想マシンが保護されていない   | 警告  | ✓  |
| 変更監視のTPMが無効                 | 警告  | ✓  |
| 変更監視のTPMレジスタ値の変更            | 警告  | ✓  |
| 変更監視エンジンがオフライン              | 重大  | ✓  |
| 変更監視ルールのコンパイルエラー            | 重大  | ✓  |
| 変更監視ルールの検出                  | 警告  | ✓  |

アラート情報

アラート: 侵入防御ルールアラート

説明: 1台以上のコンピュータで、アラートを発するように設定されている侵入防御ルールに合致しました。

消去可能: はい

一般

アラート情報

アラート: 侵入防御ルールアラート

説明: 1台以上のコンピュータで、アラートを発するように設定されている侵入防御ルールに合致しました。

消去可能: はい

オプション

重要度: 警告

☒ (ルール設定に関係なく) すべてのルールでアラート

☒ このアラートの発令時、通知のメールを送信する

☒ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☒ このアラートが存在しなくなったとき、通知のメールを送信する

OK

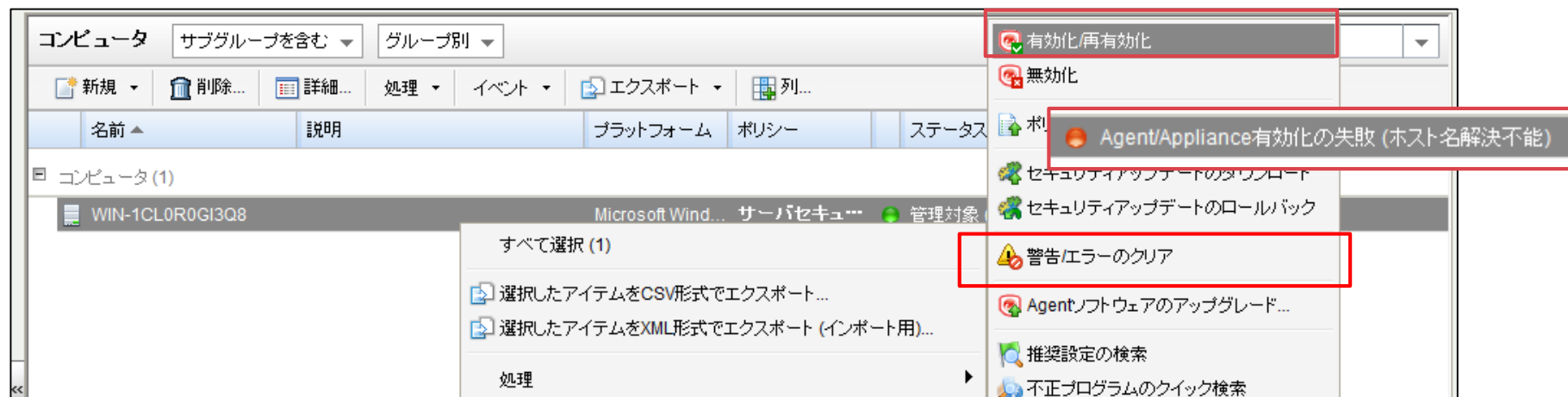
## 14. 補足 (4)

- 仮想パッチで脆弱性対策を行うアプリケーションが使用するポートについて、デフォルト設定から変更をしている場合、追加の設定が必要です
- 設定手順については下記トレンドマイクロ社のQ&Aをご参照ください  
<http://esupport.trendmicro.com/solution/ja-JP/1117498.aspx>

# 15. 注意事項

## 有効化/再有効化

- [コンピュータ] > [処理] > [有効化/再有効化] は実行できません。  
実行した場合、「Agent/Appliance有効化の失敗」のアラートがあがります。  
※アラートが表示されてもコンピュータの保護は正常に実施されています。



## ● アラート解決方法

- ① [処理] > [警告/エラーのクリア] を実行
- ② 「管理対象(オンライン)」もしくは「管理対象(オフライン)」と表示  
※「管理対象(オフライン)」と表示された場合でも、数分以内にオンライン表示になります。



# 参考情報

# Appendix : コマンドラインの利用

■ 本項では、サーバセキュリティサービスで有用なコマンドを紹介します。

※Agentをインストールしたフォルダに「cd」 コマンドで移動してから実行して下さい。

## 1. ハートビートの送信

`dsa_control -m` : 管理サーバにハートビートを送り、通信を確立

※セキュリティアップデート等、管理コンソール上で行った操作はAgentからハートビートが送信された時に実行されます。(初期設定10分毎) 管理コンソール上で行った操作をすぐに実行したい場合は、Agentを導入したサーバで上記のコマンドを実行して下さい。

## 2. Agentの初期化

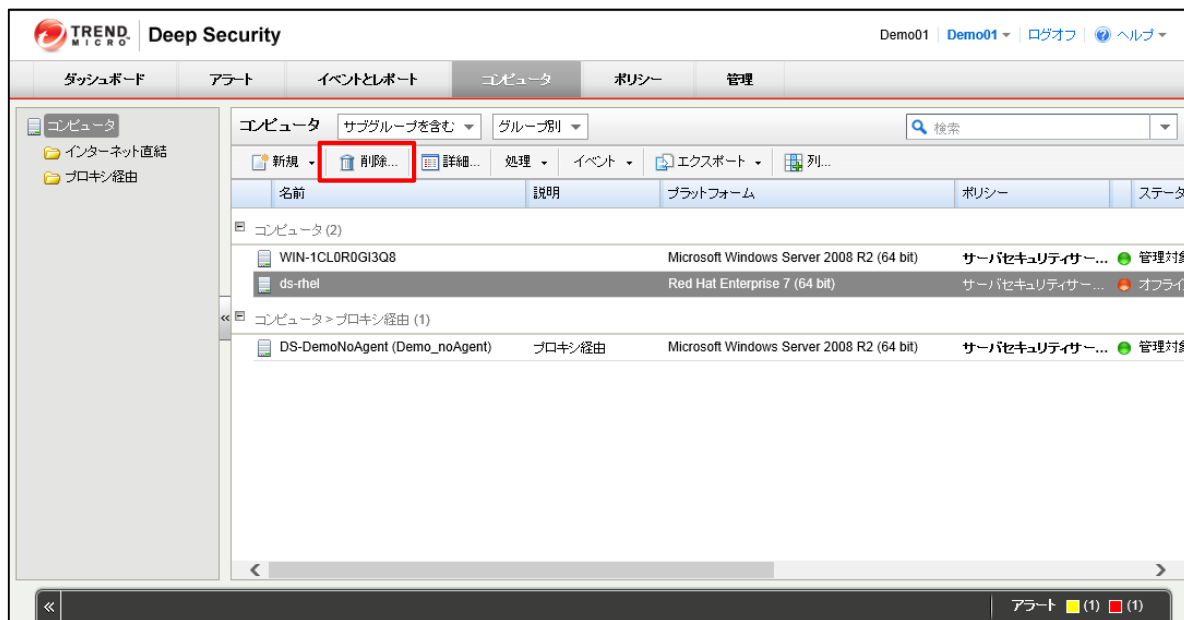
`dsa_control -r` : Agentを初期化

その他のコマンドや詳細につきましては、  
[オンラインヘルプ] > [参照] > [コマンドラインの使用方法]  
をご参照下さい。

# Appendix: アンインストール方法

## 手順

- ① サーバ上の Agent は以下のコマンドでアンインストール。  
(RedHat系)  
# rpm -e ds\_agent  
(Debian系)  
# dpkg --purge ds\_agent
- ② 管理コンソールにログインし対象のコンピュータを削除。



## 目次

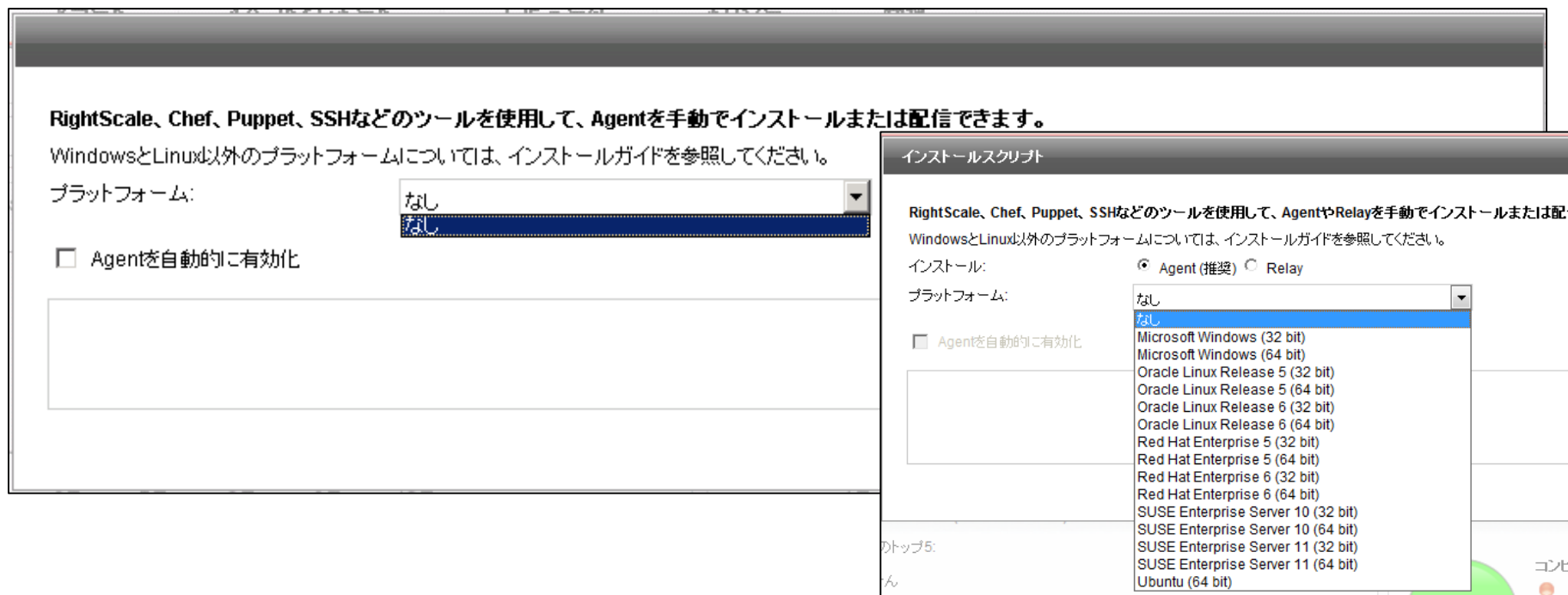
- ① 有効化コマンド作成時にプラットフォームを選択できない。
- ② 有効化に失敗する。
- ③ セキュリティアップデートに失敗する。(仮想パッチのみご利用のお客様)
- ④ ハートビート待ちの時間が長い

# ① 有効化コマンド作成時にプラットフォームを選択できない

管理コンソールは以下のWebブラウザで動作を保証します。

- Mozilla Firefox (Cookie を有効にする)
- Internet Explorer 9, 10, 11 (Cookie を有効にする)

ご利用中のWebブラウザが上記に含まれない場合、サポート対象のWebブラウザをお試ください。



## ② 有効化に失敗する

■ コマンド実行文の「HTTP Status」が400番台の場合、管理サーバ-Agent間の通信に問題がある可能性があります。以下の例をご参照の上、対策を行って下さい。

```
C:\Program Files\Trend Micro\Deep Security Agent>dsa_control -a dsm://hb.serversecurity-nec.jp:443/ "tenantID:
ord:
"policyid:18"
HTTP Status: 200 - OK
Response:
Attempting to connect to https://hb.serversecurity-nec.jp:443/
SSL handshake completed successfully - initiating command session.
Connected with AES256-SHA to peer at hb.serversecurity-nec.jp
Received a 'GetHostInfo' command from the manager.
```

例)

| Code | 状態                            | 想定される原因とその対策   |
|------|-------------------------------|--|
| 400  | Bad Request                   | P.12で作成した、プロキシサーバのURLが間違っている可能性があります。<br>設定したURLが間違っていないかご確認下さい。 |
| 407  | Proxy Authentication Required | プロキシ認証が必要です。P.12を参考にユーザ名とパスワードを設定して下さい。                          |
| 408  | Request Timeout               | 名前解決されない等の理由により、管理サーバと通信に失敗している可能性があります。                         |

### ③ ハートビート待ちの時間が長い

ハートビート(疎通確認)は、初期設定では10分毎に送信されます。  
以下の設定を行う事でハートビート間隔を変更し、リードタイムを1分まで短縮できます。

※ハートビート：管理サーバと同期する為に、定期的にハートビートを飛ばしています。  
推奨設定の検索やポリシーの変更等はハートビート後に適用されます。

#### コンピュータ or ポリシー の詳細

コンピュータ: ヘルプ

概要  
不正プログラム対策  
侵入防御  
インタフェース  
**設定**  
アップデート  
オーバーライド

コンピュータ ネットワークエンジン 検索 SIEM

通信方向  
Deep Security ManagerとAgent/Applianceの通信方向: 継承 (Agent/Applianceから開始)

ハートビート  
ハートビート間隔 (分): 継承 (10 分)  
次の数を超えるハートビートが失われた場合にアラートを発令: 継承 (2)  
ハートビート間でコンピュータのローカルシステム時間が次の時間を超えて変更された場合にアラートを発令: 継承 (無制限)  
非アクティブな仮想マシンに対してオフラインエラーを発令: 継承 (はい)

ポリシーの変更をすぐに送信  
ポリシーの変更をコンピュータに自動的に送信: 継承 (はい)

トラブルシューティング  
ログレベル: 継承 (オーバーライドしない)

Agentセルフプロテクション  
ローカルのエンドユーザによるAgentのアンインストール、停止、または変更を拒否: 継承 (はい)  
ローカルでの変更許可パスワードを要求: 継承 (はい)  
パスワード:   
パスワードの確認入力:

環境実数のオーバーライド:  
環境実数の表示...

リセット 保存 閉じる

※注  
ハートビート間隔を短くすると定期的に発生する通信が増加します。

## ④ 設定が必要な侵入防御ルール

一部の侵入防御ルールは、誤検知を防ぐために設定が必要です。

設定が必要な侵入防御ルールが推奨された場合は、適用の必要性を確認し、設定を行ったうえで適用する必要があります。

詳細はPP・サポートサービスまでお問い合わせください。

※本項に関する問い合わせは体験版期間中に受け付けることができません。

設定が必要な侵入防御ルールには専用のアイコンがついています。

[脆弱性]タブより、OSやアプリケーションベンダの脆弱性情報ページを参照できます。こちらから、脆弱性の詳細や、配信されているセキュリティパッチをご確認下さい。

脆弱性情報より、ルールの適用が不要と判断した場合は、[オプション]タブにて、[推奨設定から除外]を「はい」にする事で、推奨設定から除外できます。



## ⑤ セキュリティアップデートに失敗する

P.21-22の手順を実施して、不要なモジュールがインストールされない様にして下さい。

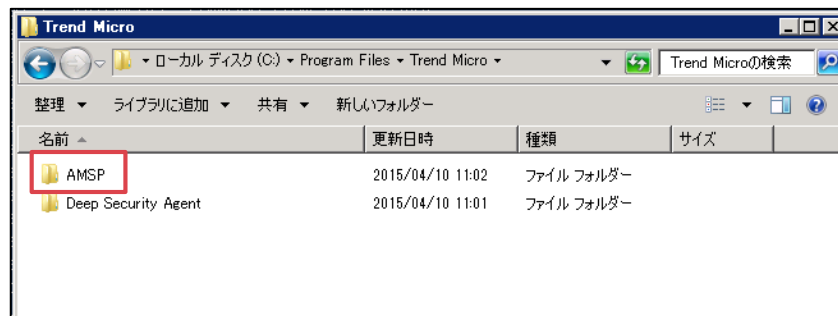
本手順をスキップした場合、

- ・ セキュリティアップデートに失敗する。
- ・ 既存のアンチウイルスと競合し、正常に動作しない。

等の現象が発生する可能性があります。



仮想パッチのみ場合、不正プログラム対策とWebレピュテーションが「ライセンスなし」になっています。



インストールフォルダに「AMSP」フォルダがある場合、Deep Security のアンチウイルスモジュールがインストールされています。

# 更新履歴

| 版数  | 更新日        | 内容        | 備考                  |
|-----|------------|-----------|---------------------|
| 第1版 | 2017/08/23 | 初版        | 前Ver.のプロキシあり・なしをマージ |
| 第2版 | 2017/08/29 | P.15 文言変更 |                     |
|     |            |           |                     |
|     |            |           |                     |
|     |            |           |                     |
|     |            |           |                     |
|     |            |           |                     |
|     |            |           |                     |
|     |            |           |                     |
|     |            |           |                     |
|     |            |           |                     |
|     |            |           |                     |
|     |            |           |                     |
|     |            |           |                     |
|     |            |           |                     |

# Orchestrating a brighter world

未来に向かい、人が生きる、豊かに生きるために欠かせないもの。  
それは「安全」「安心」「効率」「公平」という価値が実現された社会です。

NECは、ネットワーク技術とコンピューティング技術をあわせ持つ  
類のないインテグレーターとしてリーダーシップを発揮し、  
卓越した技術とさまざまな知見やアイデアを融合することで、  
世界の国々や地域の人々と協奏しながら、  
明るく希望に満ちた暮らしと社会を実現し、未来につなげていきます。

 **Orchestrating** a brighter world

**NEC**