Orchestrating a brighter world

NEC

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 (※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	【Windows】 Windows Server 2003 SP2 (32/64bit) Windows Server 2003 R2 SP2 (32/64bit) Windows Server 2008 (32/64bit) Windows Server 2008 R2 (64bit) Windows Server 2008 R2 Hyper-V Windows Server 2012 (64bit) Windows Server 2012 R2 (64bit) Windows Server 2012 R2 Hyper-V Windows Server Core 2012 (64bit) Windows Server Core 2012 R2 (64bit) Windows Server 2016 (64bit)Windows 10 (32/64bit) Windows XP (32/64bit) Windows Vista (32/64bit) Windows 7 (32/64bit) Windows 8 (32/64bit) Windows 8.1 (32/64bit) Windows 10 (32/64bit)	【Linux】 Red Hat 5、6、7 (32/64 bit) CentOS 5、6、7 (32/64 bit) SUSE 10 SP3、SP4 (32/64bit) SUSE 11 SP1、SP2、SP3 (32/64bit) SUSE 12 (64bit) Ubuntu Linux 10.04、12.04、14.04、16.04 (64bit) Oracle Linux 5 RedHat/Unbreakable Kernel (32/64 bit) Oracle Linux 6 RedHat/Unbreakable Kernel (32/64 bit) Oracle Linux 7 RedHat/Unbreakable Kernel (64 bit) CloudLinux 5 (32/64bit) CloudLinux 6 (32/64bit) CloudLinux 7 (64bit) Debian 6 (64bit) Debian 7 (64bit) Amazon Red Hat 6 EC2 (32/64bit) Amazon Red Hat 7 EC2 (64bit) Amazon SUSE 11 EC2 (32/64bit) Amazon SUSE 12 EC2 (64bit) Amazon Ubuntu 12 EC2 (64bit) Amazon Ubuntu 14.04 LTS (64bit) Amazon Ubuntu 16.04 LTS (64bit) Amazon AMI Linux (32/64bit) Amazon Debian 7 (64bit)
Webブラウザ （管理コンソール）	Internet Explorer 9, 10,11 (Cookie を有効にする) 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ございます。

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	
reray.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。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		

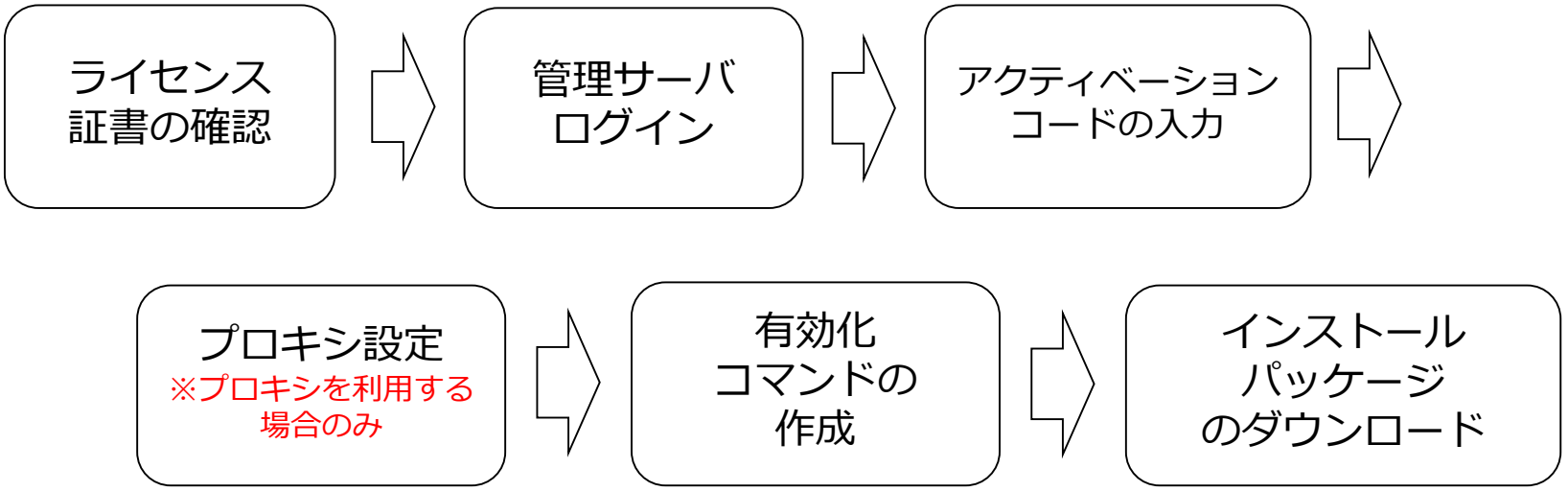
目次

事前準備　（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。

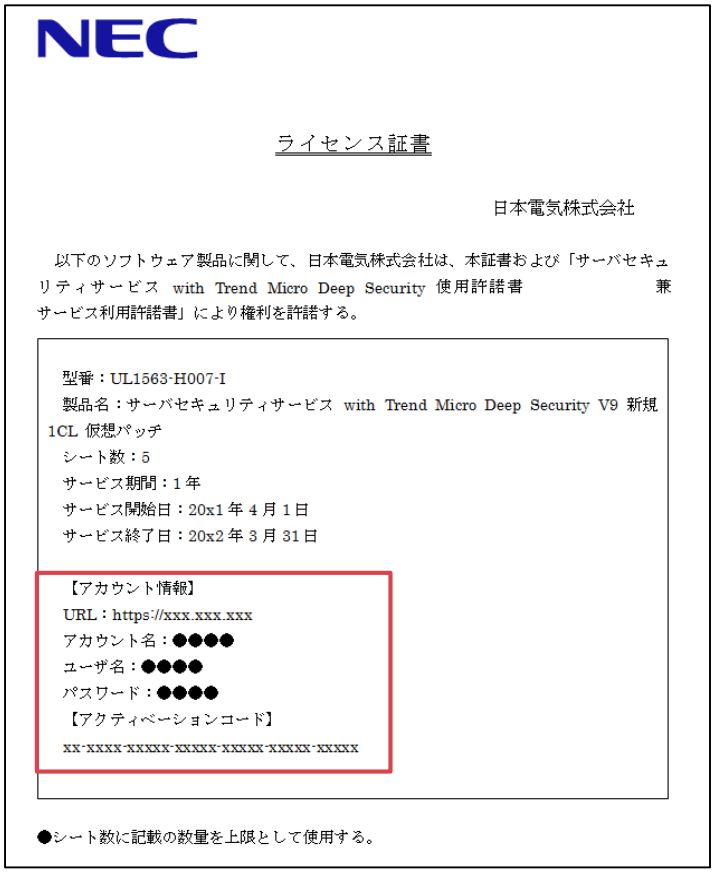
注意事項

- 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-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx

●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

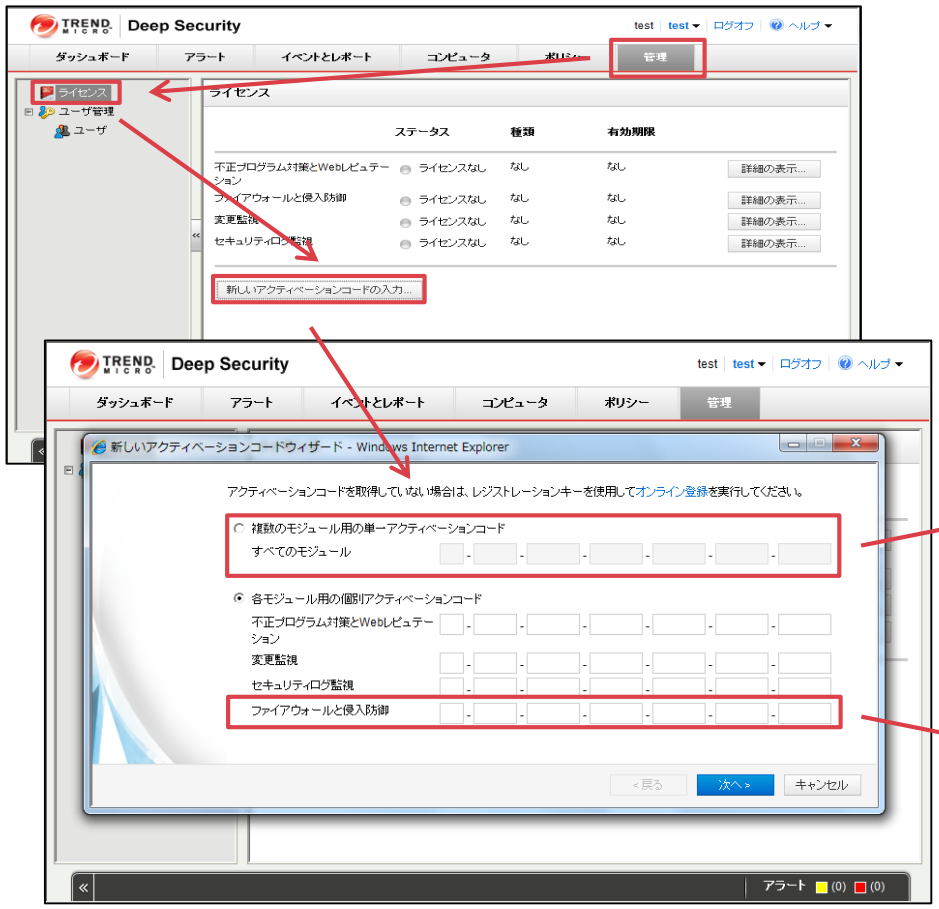
② ライセンス証書のアカウント情報 > アカウント名/ユーザ名/パスワードを入力してログイン

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



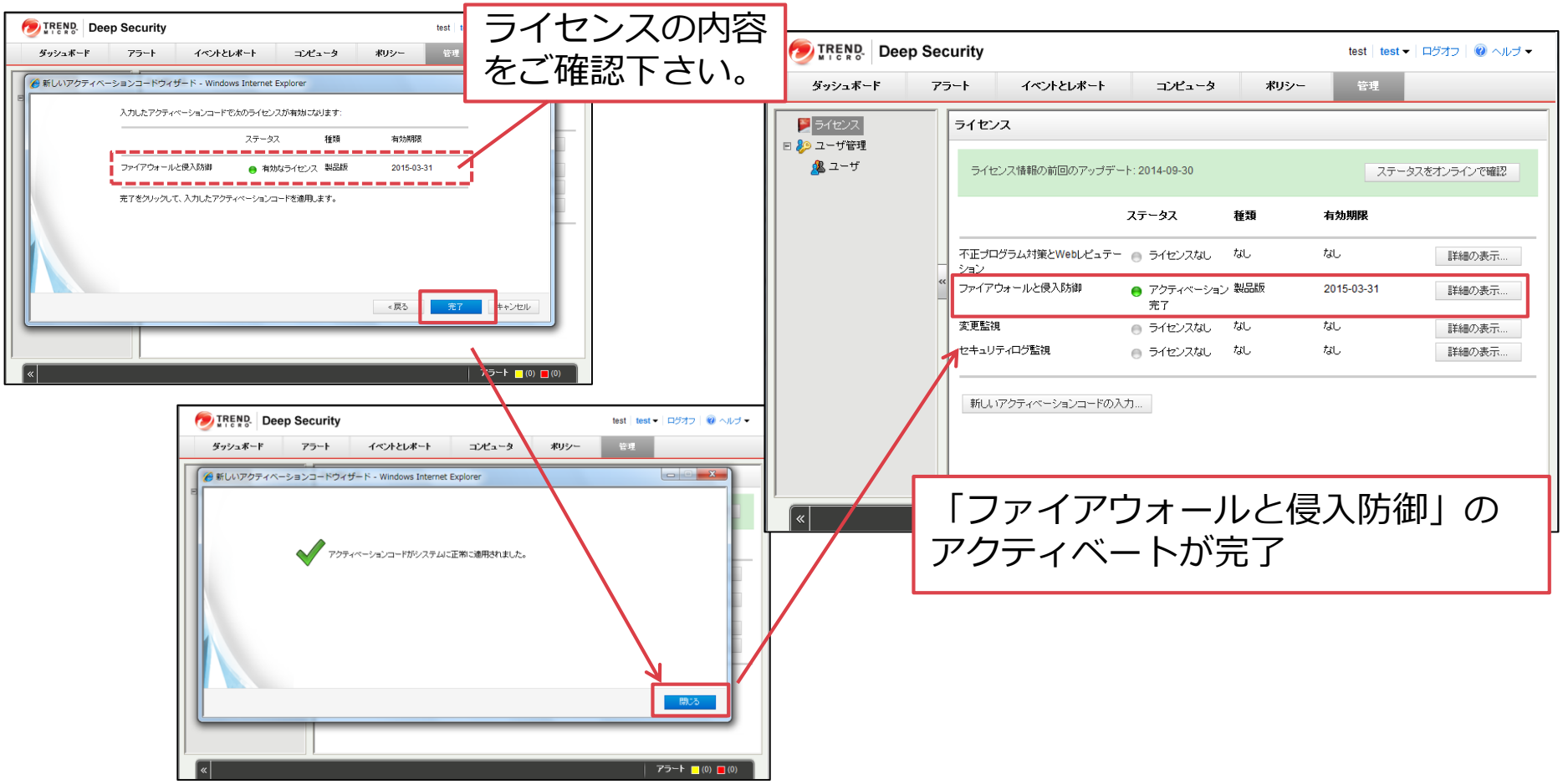
・アンチウィルスを含む場合
→すべてのモジュール

・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。

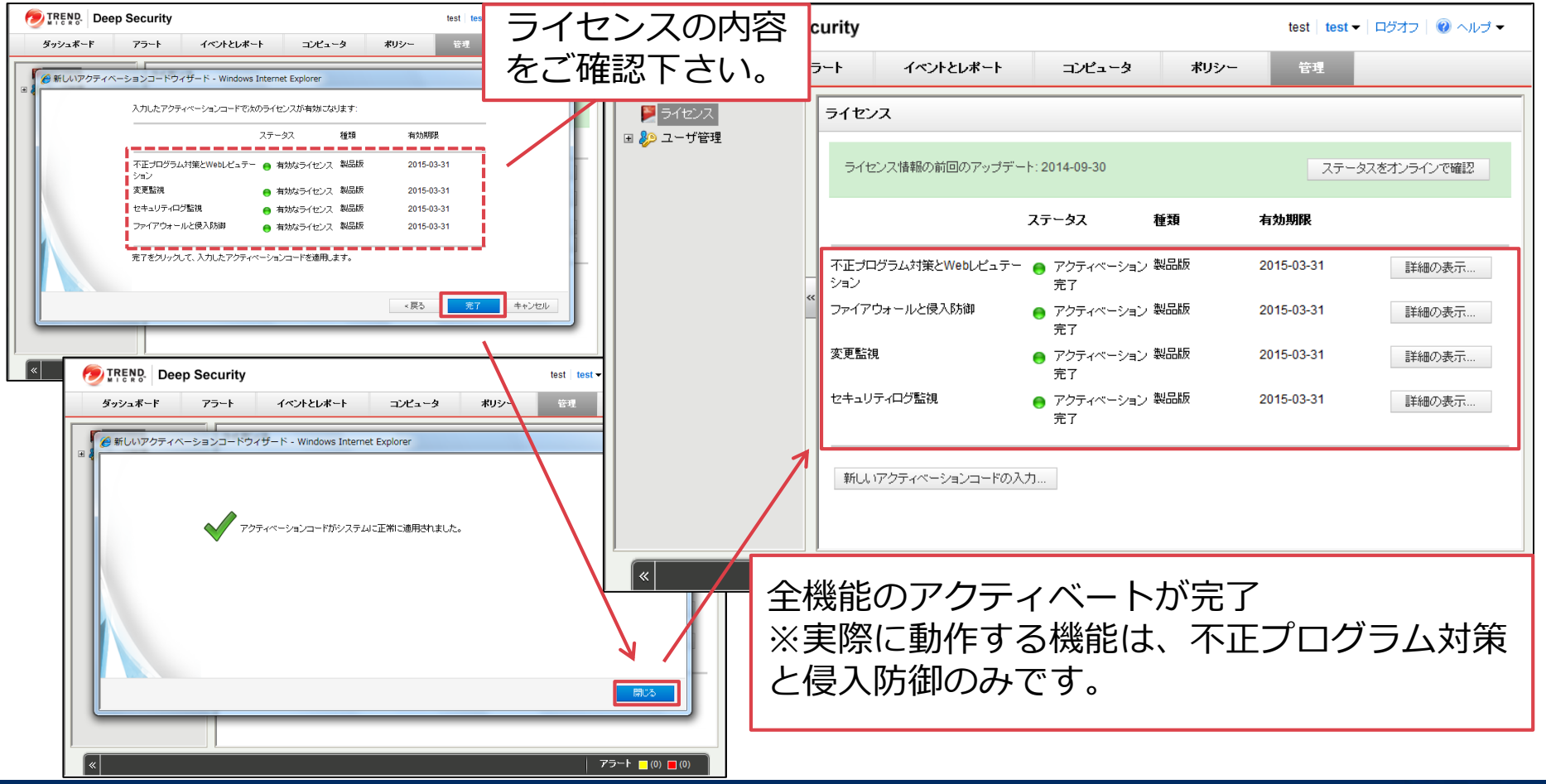
③ アクティベートを完了させて、有効なライセンスを確認



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



4. プロキシ登録

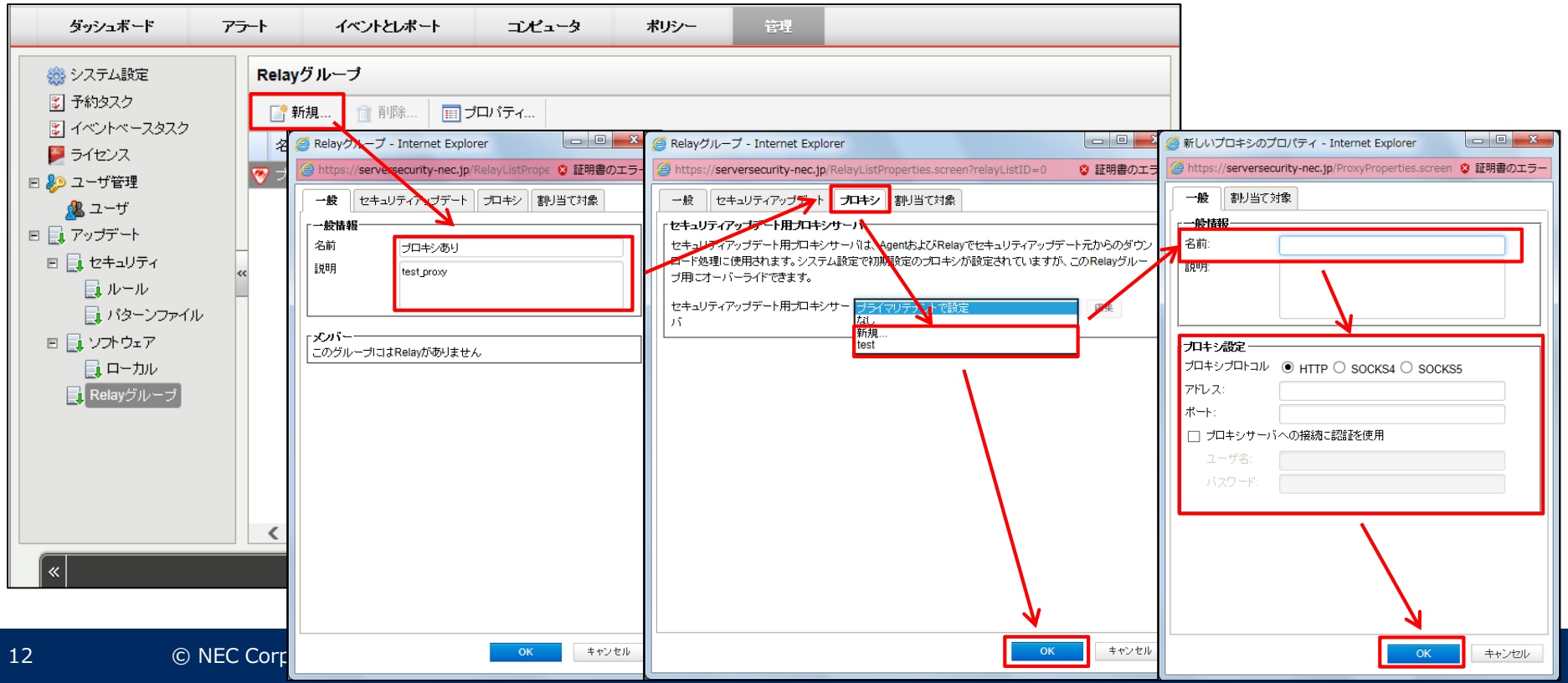
プロキシをご利用でない環境の場合、本手順は不要です

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



5. 有効化コマンドの作成(1)

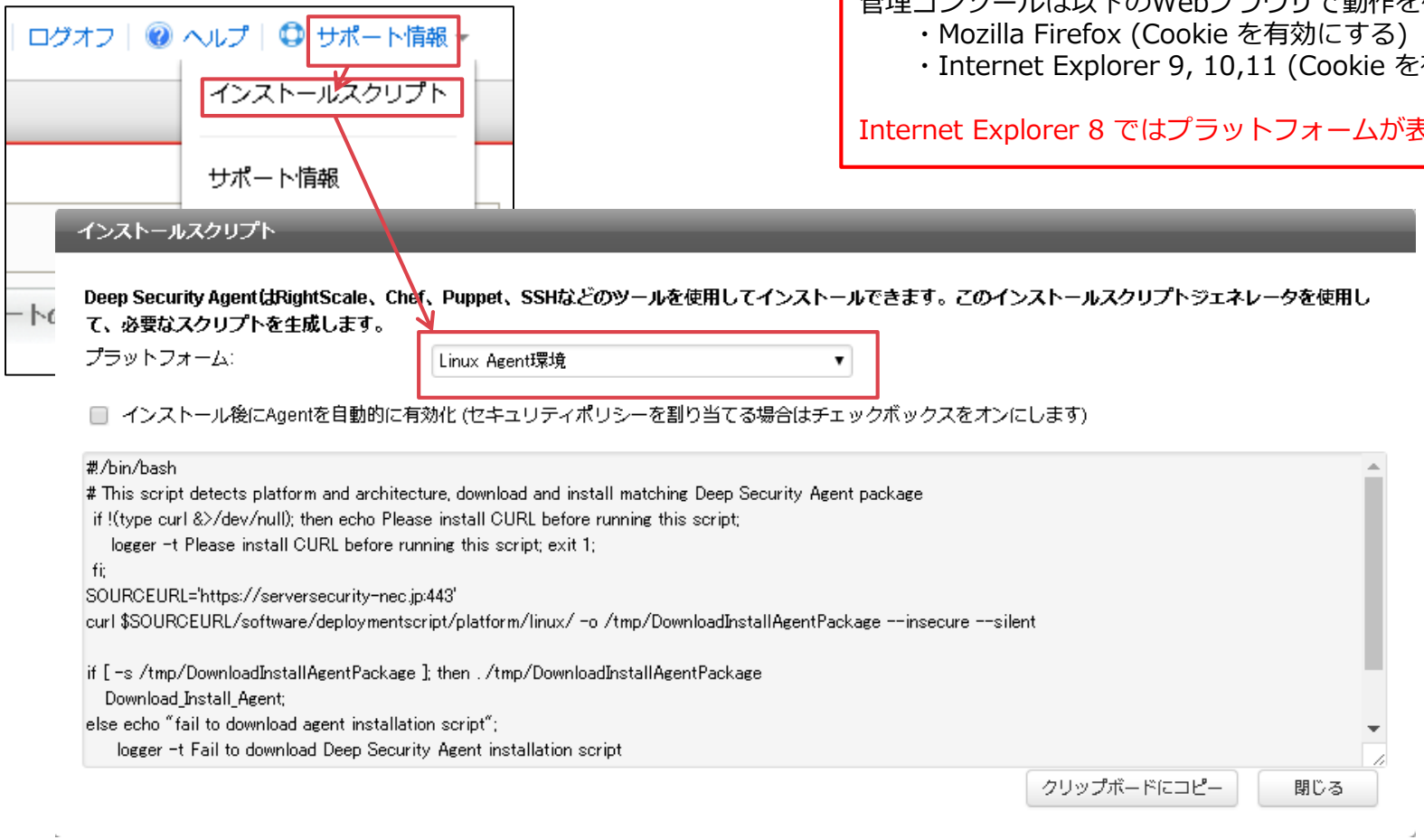
手順

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。



5. 有効化コマンドの作成(2)

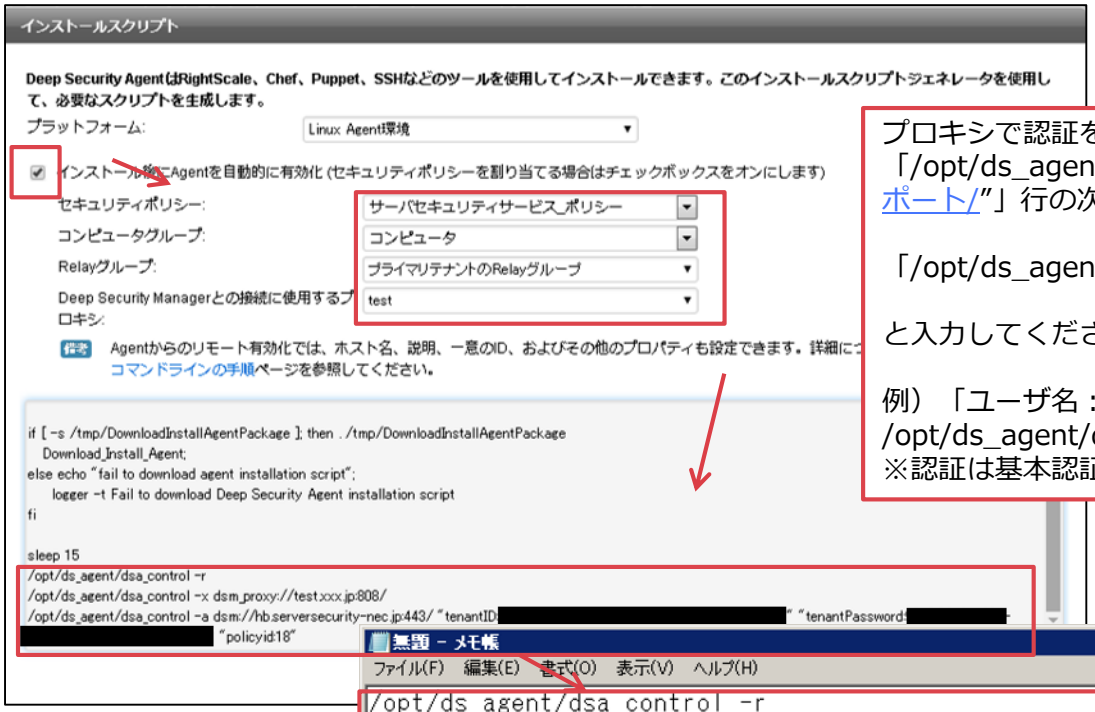
③ [インストール後にAgentを自動的に有効化（セキュリティポリシーを割り当てる場合はチェックボックスをオンにします）]にチェックを入れる

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

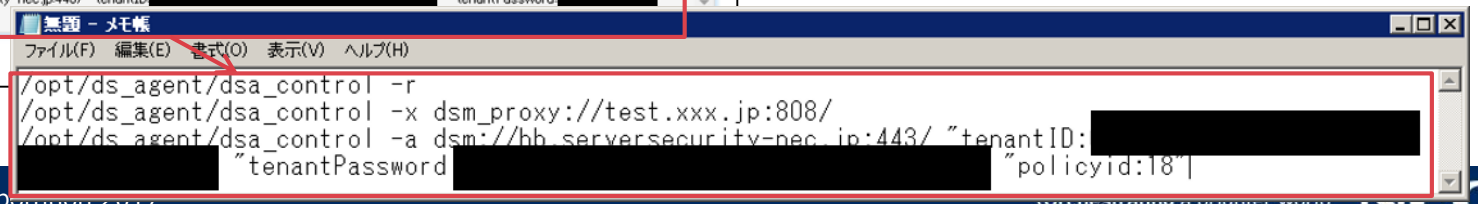


プロキシで認証を行う場合
「/opt/ds_agent/dsa_control -x “dsm_proxy://プロキシサーバのURL:ポート/”」行の次行に

「/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



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

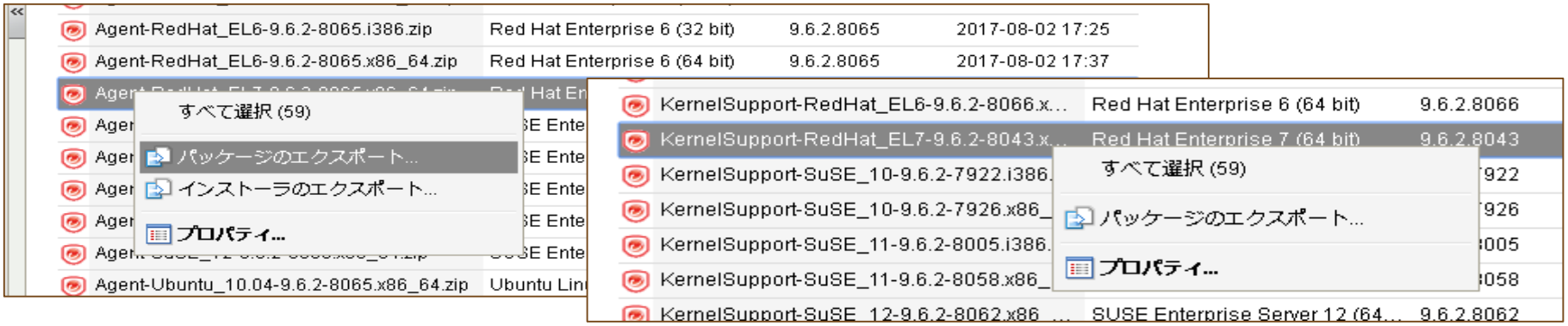
④ 9.6.2グループの中からご利用の環境のプラットフォームのAgentモジュール（ファイル名の先頭が”Agent”から始まるもので、ファイル名に含まれる[9.6.2-]に続く4桁の数値が一番大きなファイル）を右クリック

※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

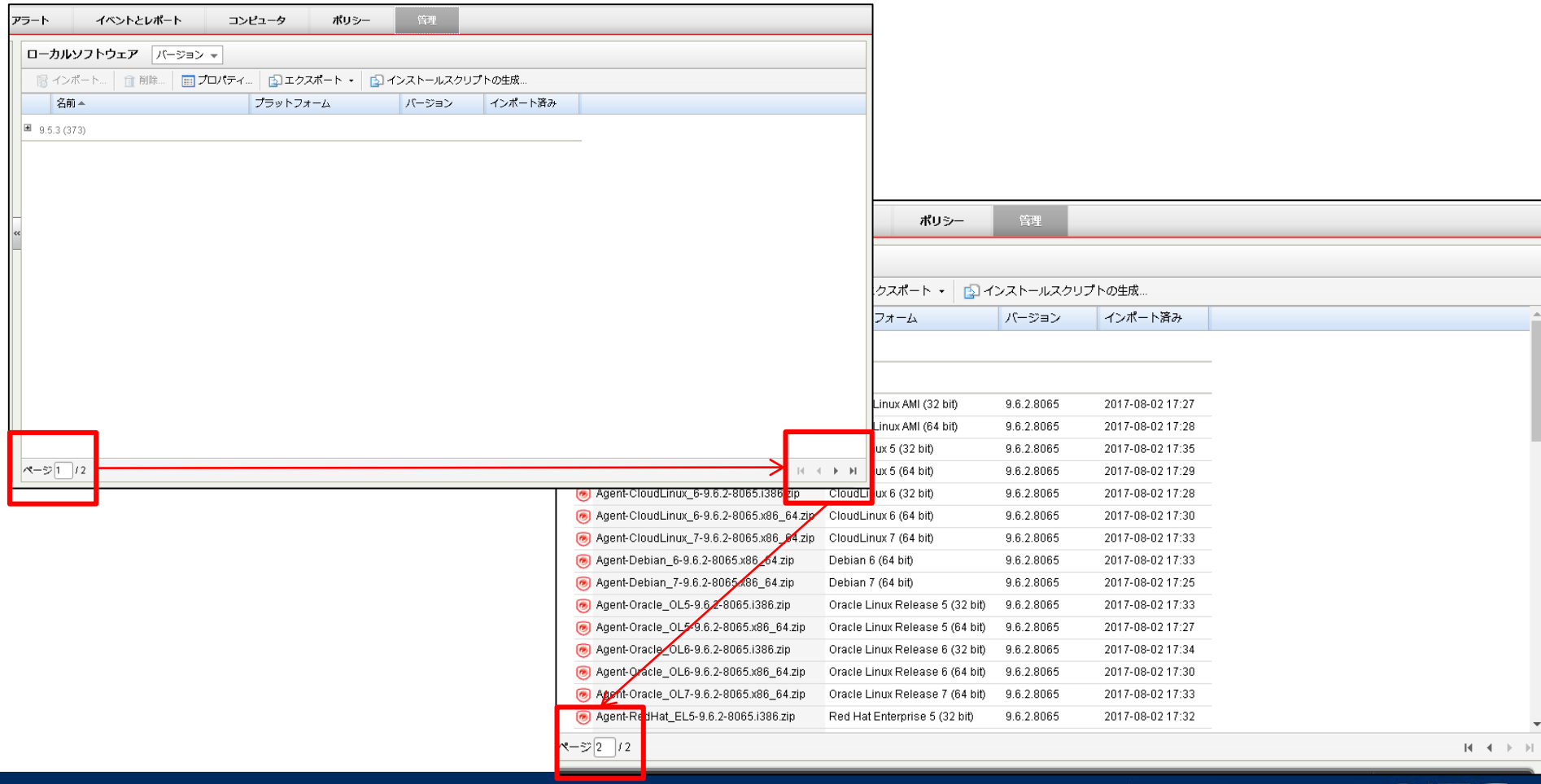
⑥ ④同様に9.6.2グループの、カーネルサポートパッケージ（ファイル名の先頭が”KernelSupport”から始まるもので、ファイル名に含まれる[9.6.2-]に続く4桁の数値が一番大きなファイル）を右クリック

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。

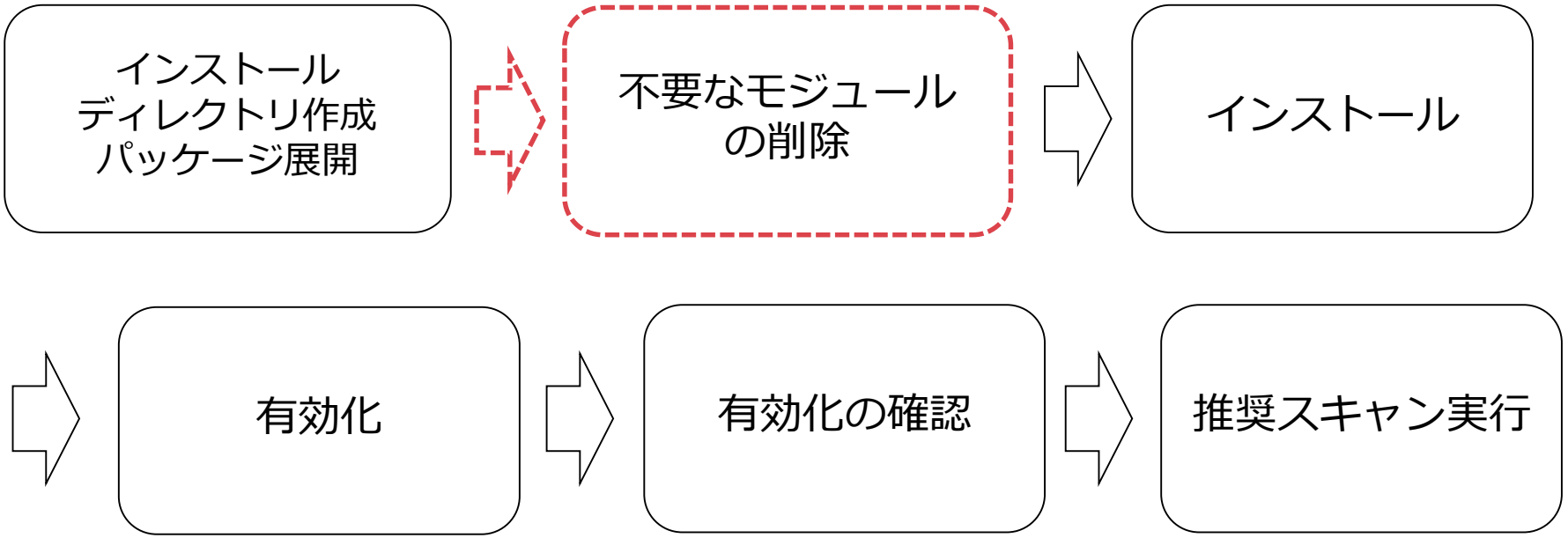


サーバへ Agent を導入する手順

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。

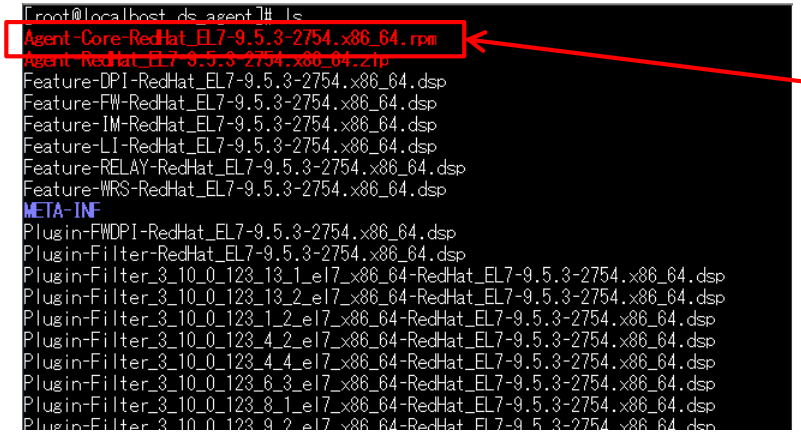
(Red Hat系)

```
# 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  ]
```



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

① P.13-14で作成した、有効化コマンドを実行

② リモート端末にペーストし実行後、Command session completed.の表示を確認

※実行例

```
[root@localhost ds_agent]# /opt/ds_agent/dsa_control -x "dsm_proxy://[redacted]
[redacted].co.jp:[redacted]/"
Starting thread 'CScriptThread' with stack size of 1048576
HTTP Status: 200 - OK
Response:
Add proxy-address:[dsm_proxy] with value:[[redacted]/]

[root@localhost ds_agent]# /opt/ds_agent/dsa_control -a dsm://hb.serversecurity-
nec.jp:443/ "tenantID:[redacted]" "tenantPassword:[redacted]
[redacted]" "policyid:18" "relaygroupid:12"
Starting thread 'CScriptThread' with stack size of 1048576
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.
Received a 'GetHostInfo' command from the manager.
Received a 'SetDSMCert' command from the manager.
Received a 'SetAgentCredentials' command from the manager.
Received a 'GetAgentEvents' command from the manager.
Received a 'GetInterfaces' command from the manager.
Received a 'GetAgentEvents' command from the manager.
[redacted]us' command from the manager.
[redacted]ts' command from the manager.
[redacted]Info' command from the manager.
[redacted]onfiguration' command from the manager.
[redacted]ts' command from the manager.
[redacted]us' command from the manager.
Command session completed.
[root@localhost ds_agent]#
```

「Command session completed.」と表示されれば完了。

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。

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。

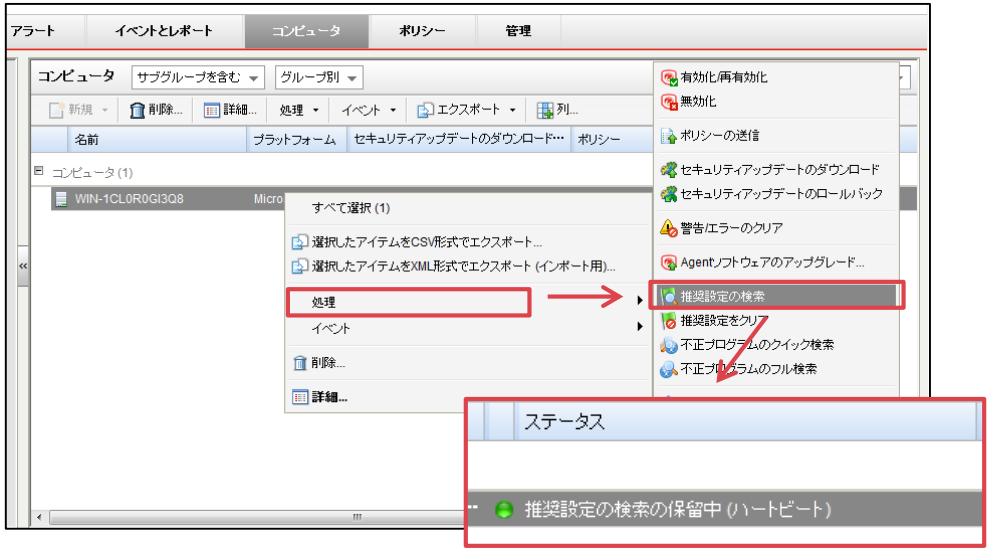
手順

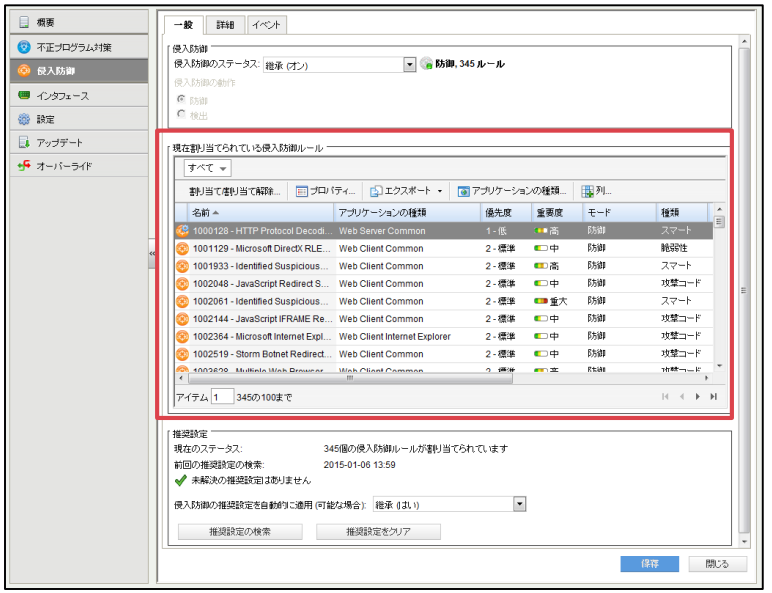
① [コンピュータ]タブより、対象クライアントを右クリック

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)

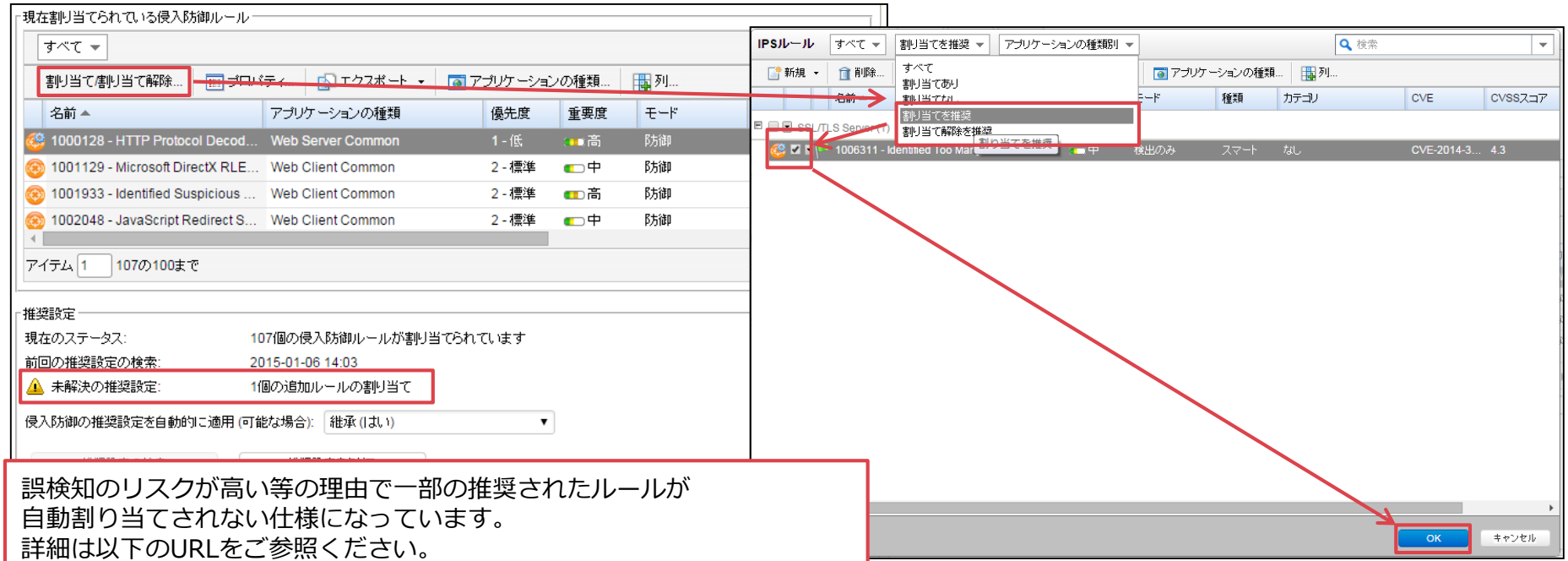
推奨スキャン完了後、「未解決の推奨設定」がある場合は下記の手順でルールの割当てが可能です。※自動的に適用できないルールがあるため、下記の手順が必要となります。

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



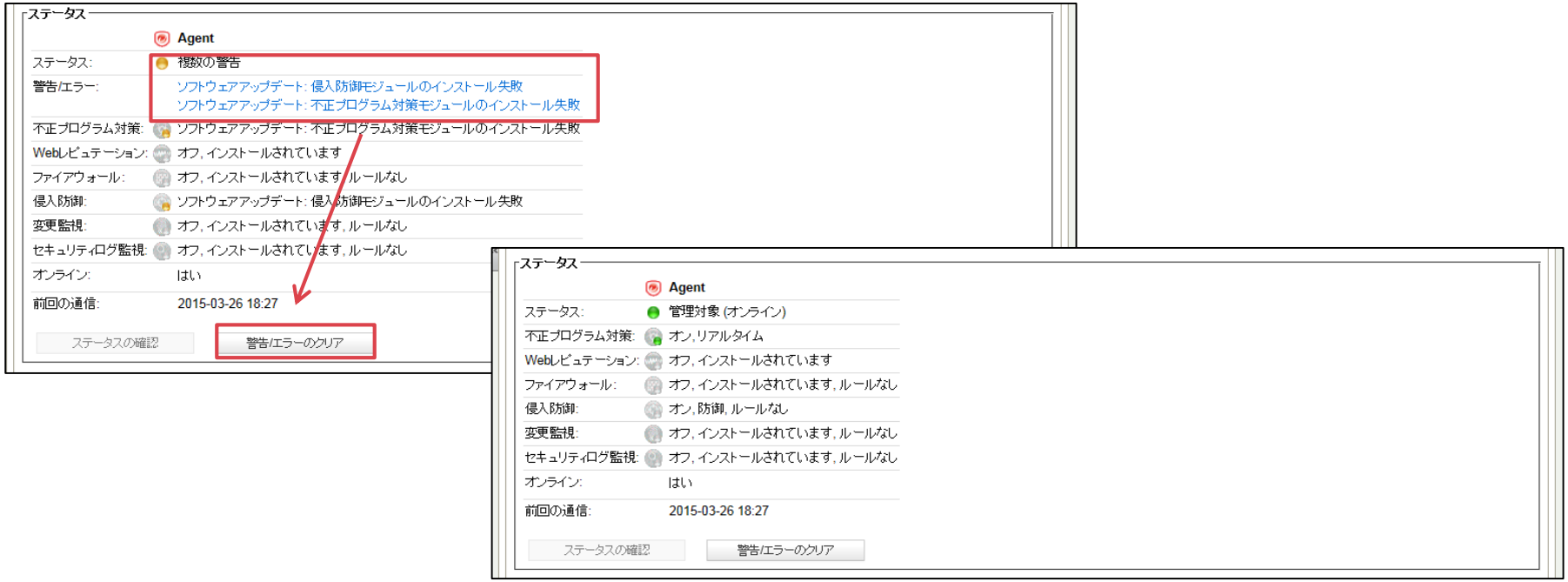
誤検知のリスクが高い等の理由で一部の推奨されたルールが
自動割り当てされない仕様になっています。
詳細は以下のURLをご参照ください。
http://esupport.trendmicro.com/solution/ja-JP/1311156.aspx

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

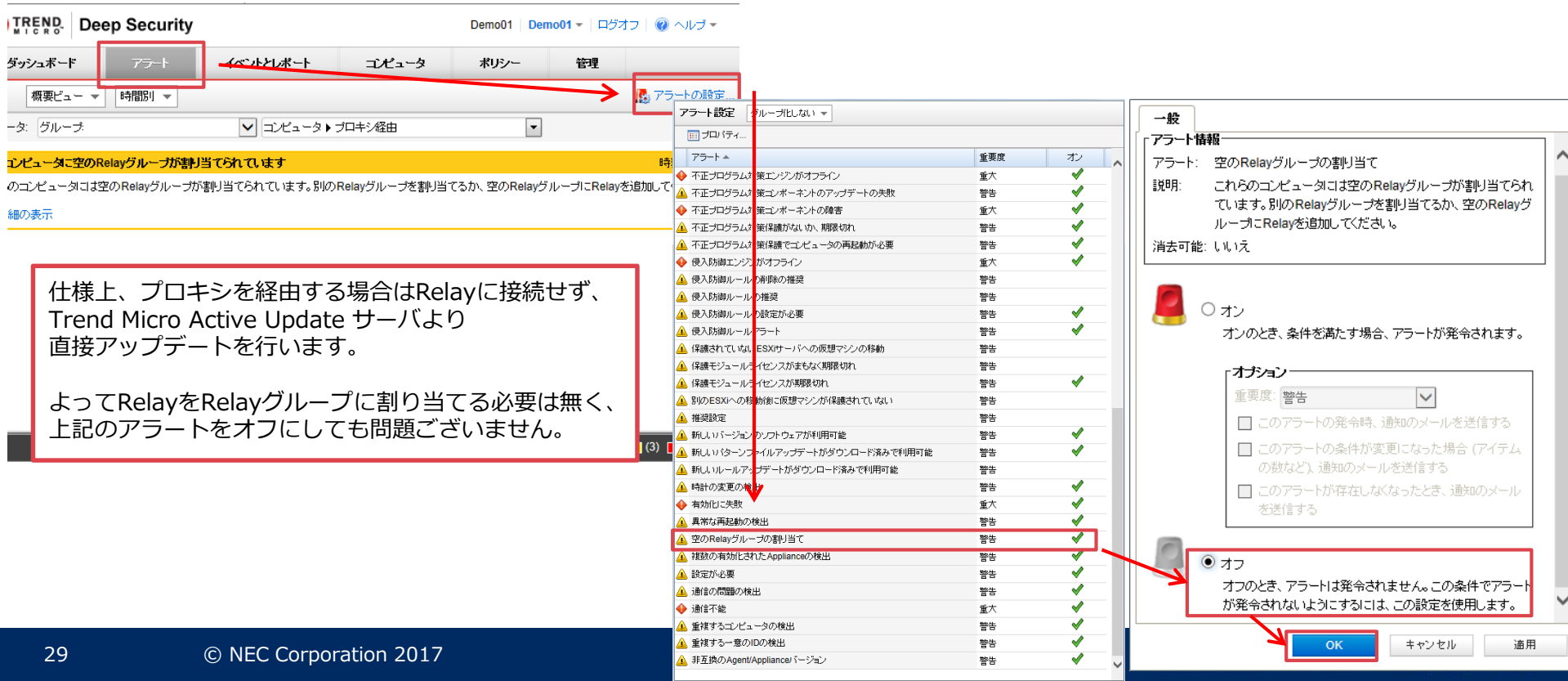


14. 補足 (2)

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

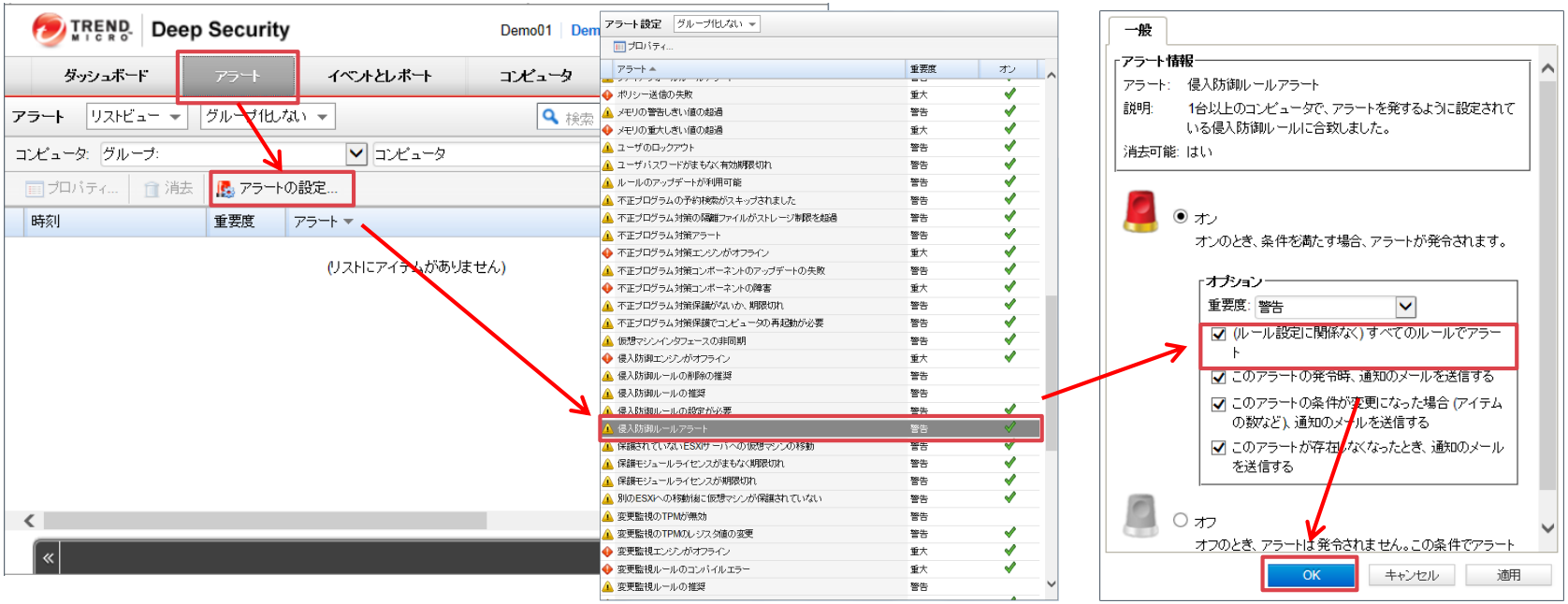


14. 補足 (3)

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



14. 補足 (4)

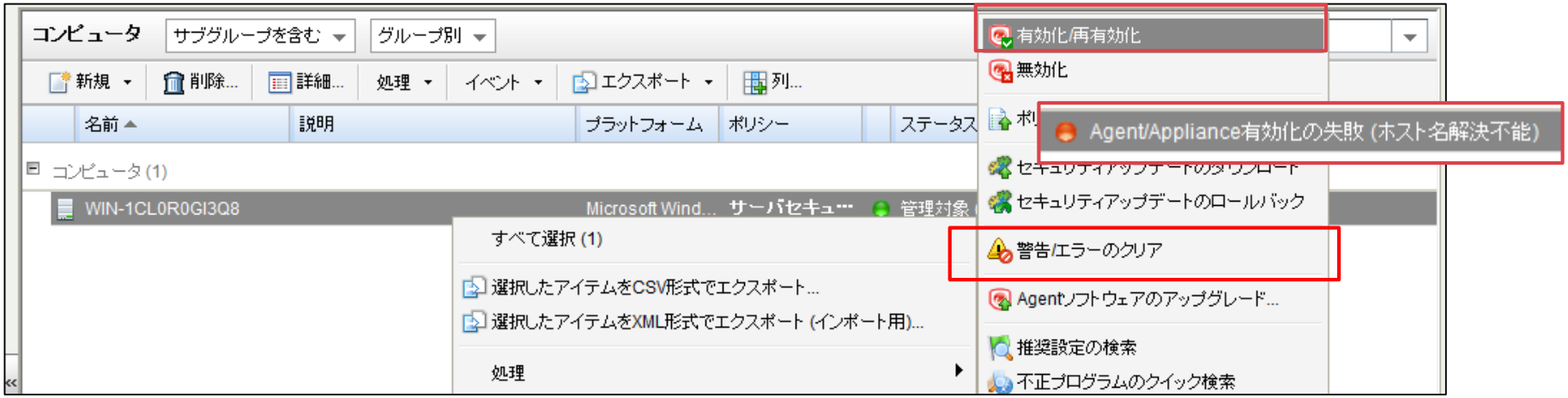
- 仮想パッチで脆弱性対策を行うアプリケーションが使用するポートについて、デフォルト設定から変更をしている場合、追加の設定が必要です

- 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

Apendix：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。

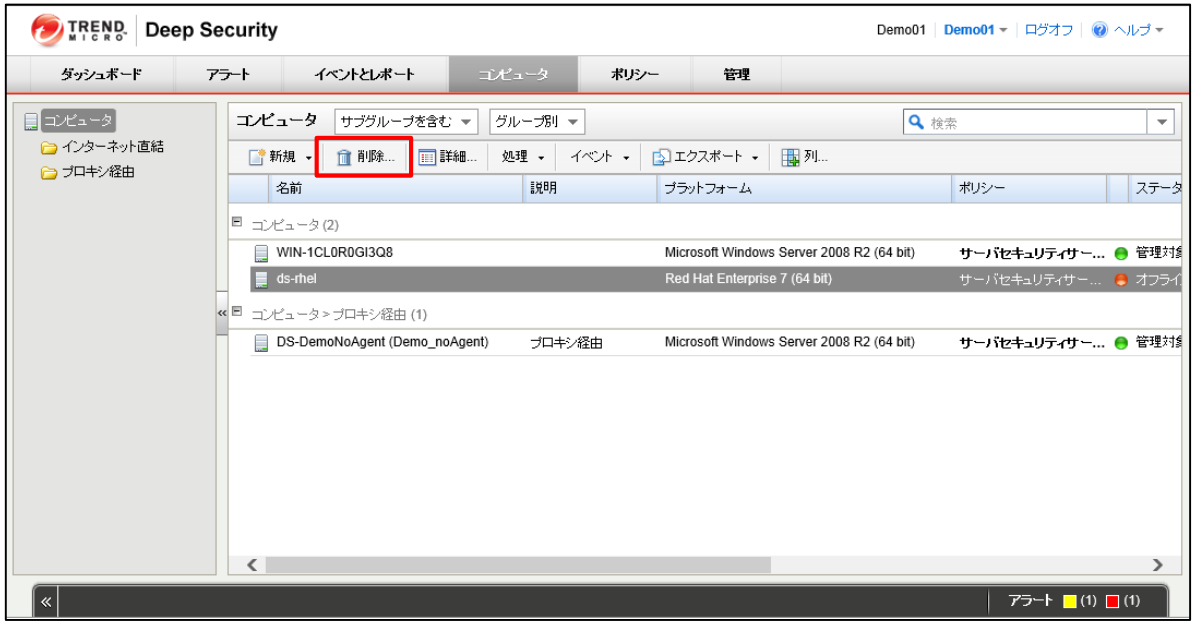
(RedHat系)

```
# 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。



導入時のトラブルシューティング

目次

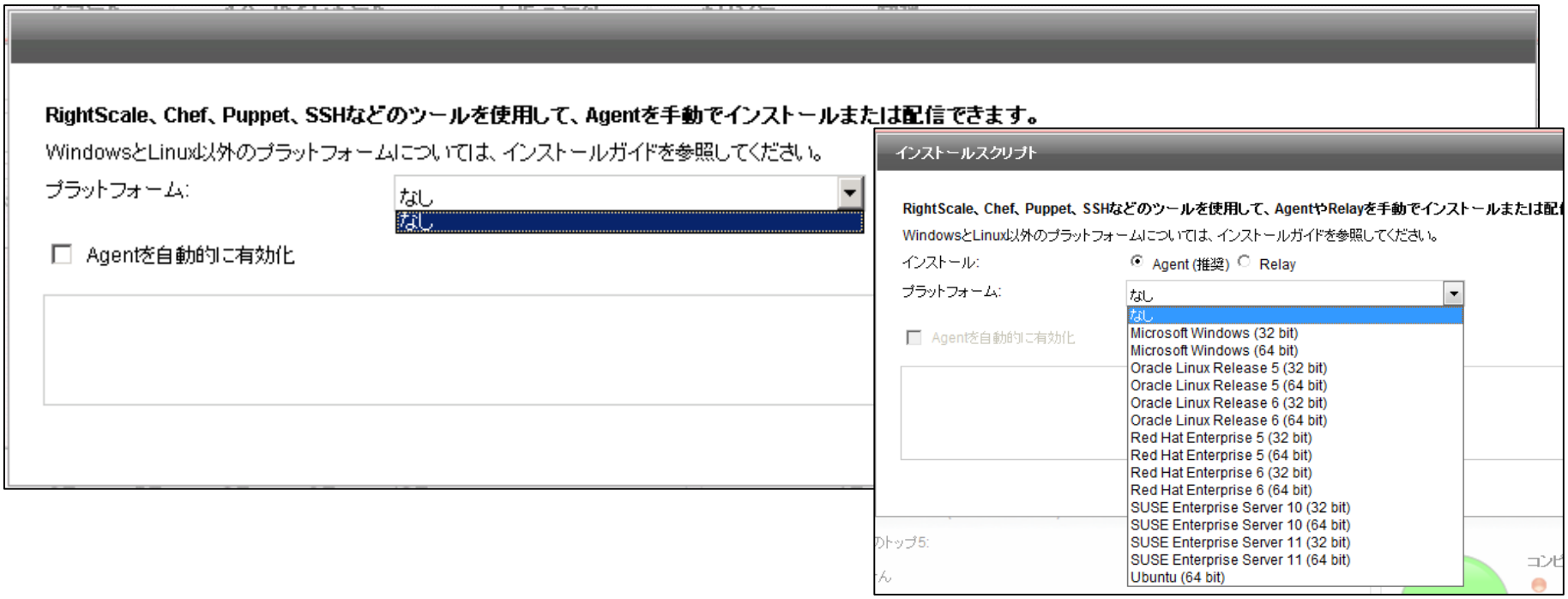
① 有効化コマンド作成時にプラットフォームを選択できない。
② 有効化に失敗する。
③ セキュリティアップデートに失敗する。(仮想パッチのみご利用のお客様)
④ ハートビート待ちの時間が長い

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。

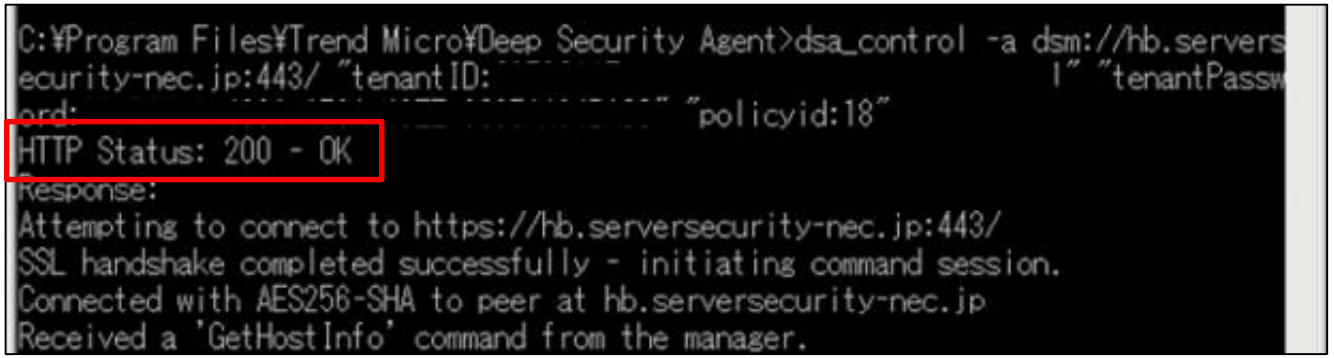
- Mozilla Firefox (Cookie を有効にする)
- Internet Explorer 9, 10,11 (Cookie を有効にする)

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ブラウザをお試しください。



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御座います。
以下の例をご参照の上、対策を行って下さい。



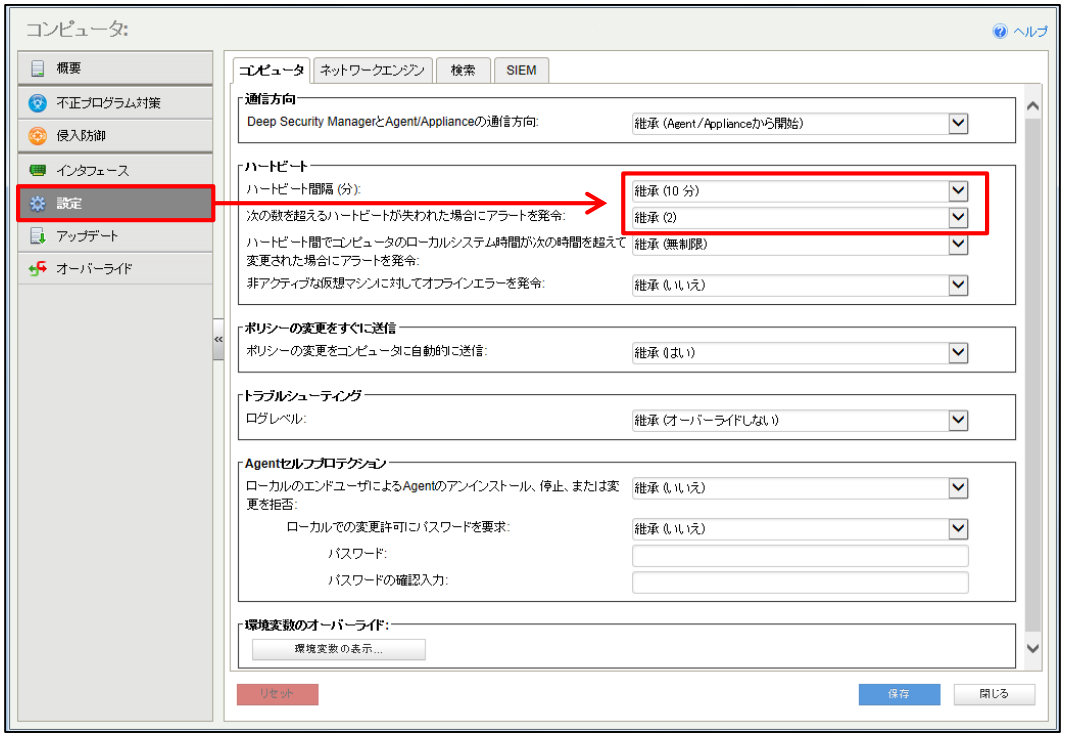
例)

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。 設定したURLが間違って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。

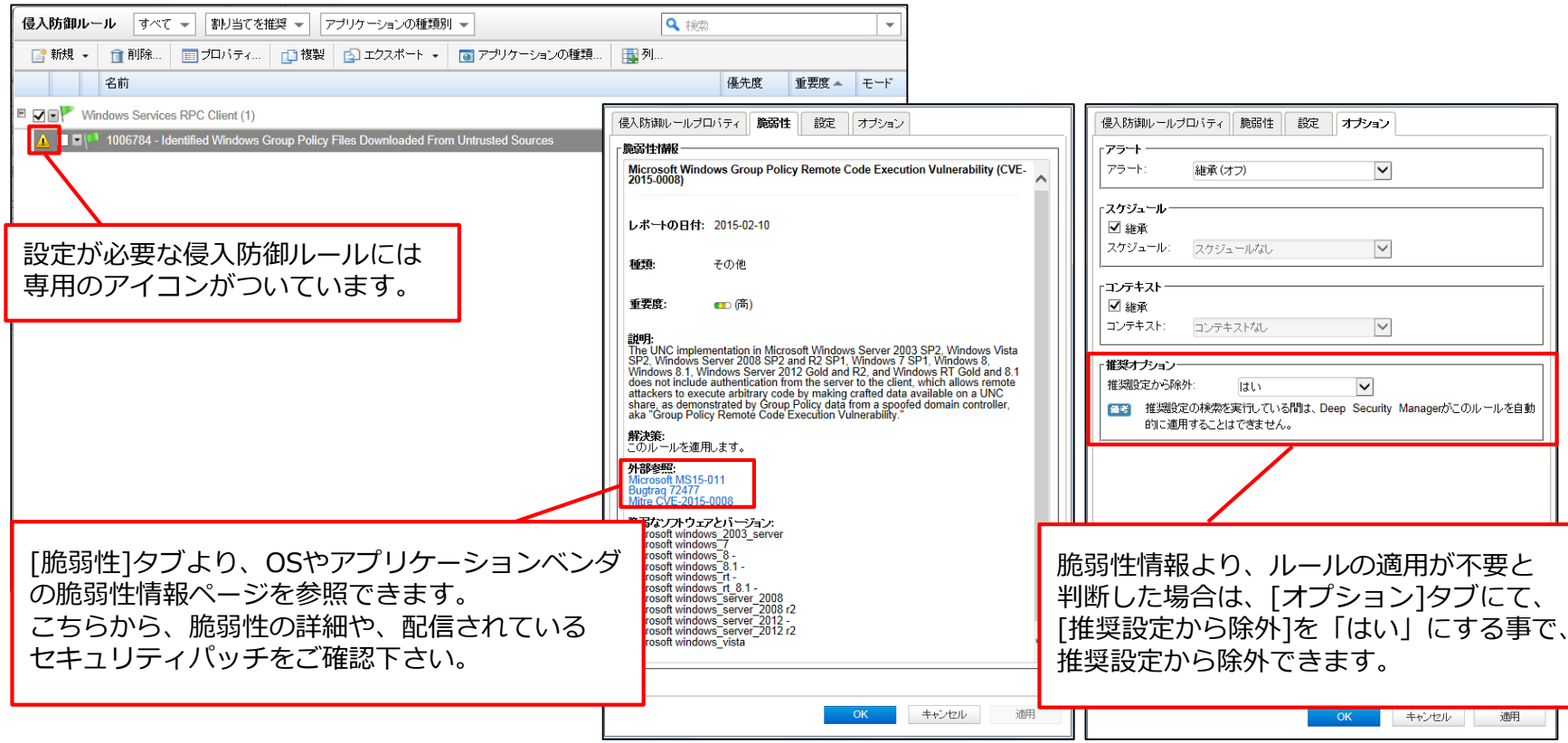
コンピュータ or ポリシー の詳細



※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。



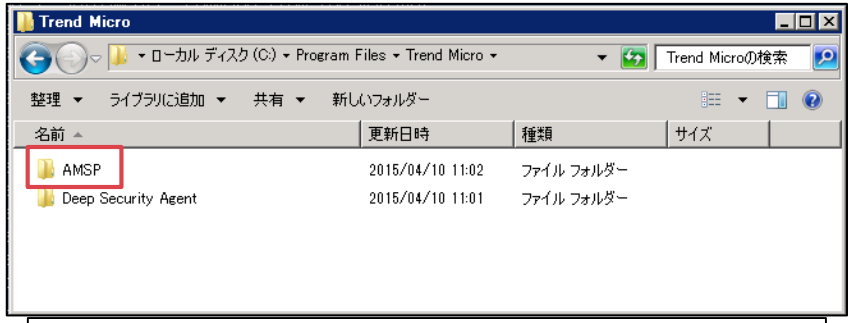
⑤ セキュリティアップデートに失敗する

- 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