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

2017 年 11 月 1 日

【第 2.1 版】

日本電気株式会社

更新履歴

項番	版数	更新日	更新内容	更新箇所	更新区分	備考
1	1.0	2017/08/23	―	―	新規	
2	2.0	2017/09/15	「3.5 レジストリの登録」を追加	3-10～12 ページ	変更	
3	2.1	2017/11/01	ドキュメントのフォーマット変更	全ページ	変更	

目 次

1 はじめに

1.1 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。

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

［参照先］
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）

なお、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 より手順を共通化いたしました。

1.2 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

<table>
<tr><td>メモリ</td><td colspan="2">512MB</td></tr>
<tr><td>ハードディスク</td><td colspan="2">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)</td></tr>
<tr><td>OS</td><td>【Windows】
Windows Server 2003 SP2 (32/64bit)※1
Windows Server 2003 R2 SP2 (32/64bit)※1
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 XP (32/64bit)※1
Windows Vista (32/64bit)
Windows 7 (32/64bit)
Windows 8 (32/64bit)
Windows 8.1 (32/64bit)
Windows 10 (32/64bit)

※1 2017 年 12 月末サポート終了</td><td>【Linux】
Red Hat 5 (32/64 bit)※2
Red Hat 6 (32/64 bit)
Red Hat 7 (32/64 bit)
CentOS 5 (32/64 bit)
CentOS 6 (32/64 bit)
CentOS 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)

※2 2020 年 11 月末サポート終了</td></tr>
<tr><td>Web ブラウザ（管理コンソール）</td><td colspan="2">Internet Explorer 9, 10, 11 (Cookie を有効にする)
Mozilla Firefox (Cookie を有効にする)</td></tr>
</table>

※ OS サポート期間は、基本的にベンダー各社における OS・ミドルウェアおよび Service Pack 等のサポート期間に準拠します。

（例）

・Microsoft: サポートライフサイクル

Microsoft 社製品は全て、「延長サポート終了日」に準拠します。

・Red Hat: Red Hat Enterprise Linux Life Cycle

Red Hat Enterprise Linux では、「End of Production 3」に準拠します。

※ 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、以下の製品 Q&A をご参照ください。

（http://esupport.trendmicro.com/solution/ja-JP/1098600.aspx）

(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。

- インターネット接続が可能
- TCP443 で通信が可能
- 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。

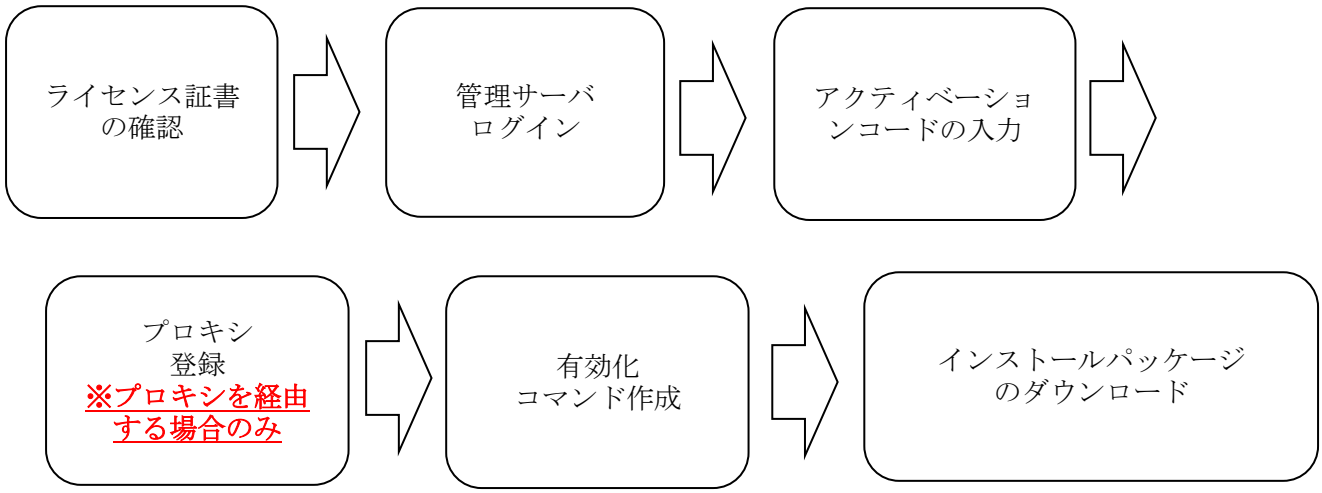
URL	用途	補足
serversecurity-nec.jp:443	管理コンソール URL	保護対象サーバ上で管理コンソールに アクセスしない場合は不要です。
hb.serversecurity-nec.jp:443	管理サーバとの疎通確認、イベントログの送信等	
reray.serversecurity-nec.jp:443	セキュリティアップデート(インターネット直結)	プロキシ経由の場合利用しません。
iaus.trendmicro.com:443	セキュリティアップデート(プロキシ環境)	Trend Micro 社 Active Update サーバ。 プロキシを経由しない場合でも、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		

2 事前準備

2.1 事前準備

【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。
・事前準備作業は、保護対象サーバ以外のお客様のクライアント PC や端末機でも実施可能です。

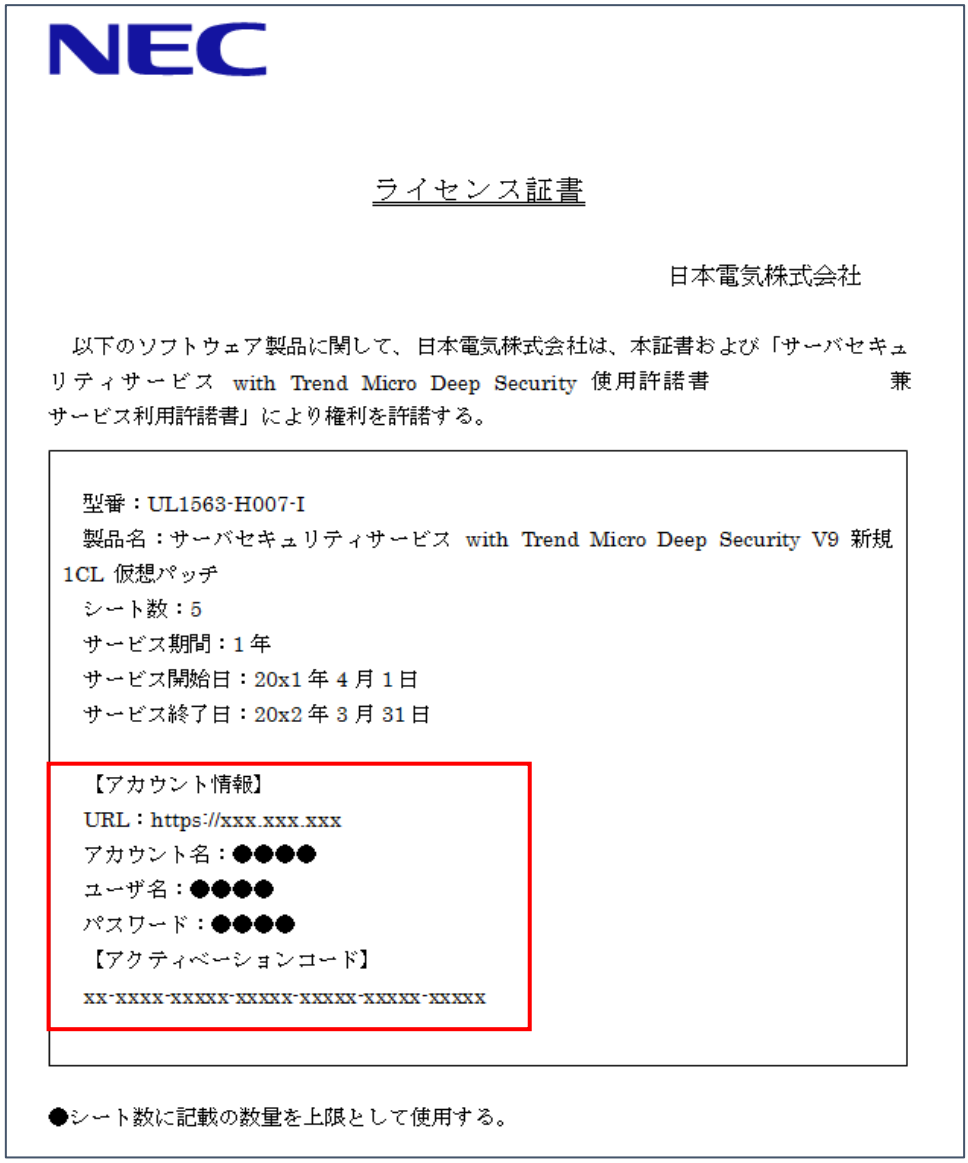
Agent 導入前に Manager コンソール上で、ライセンスの確認やアクティベーション、プロキシ設定を行います。



2.2 ライセンス証書の確認

【注意事項】
・この情報は、管理サーバログイン等に使用します。
・外部に公開しない様、慎重にお取り扱いください。

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）を確認してください。



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。

2.3 管理サーバログイン

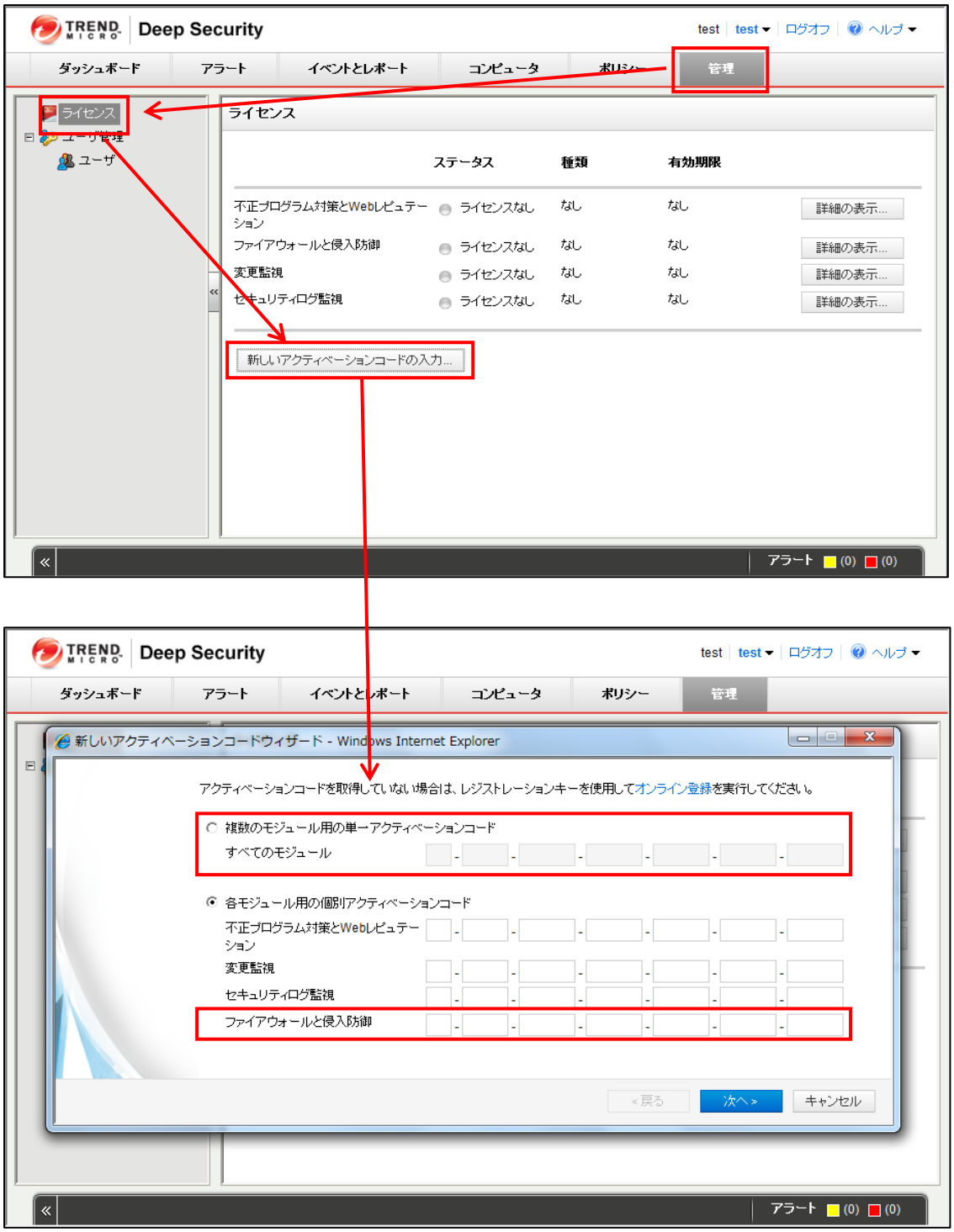
(1) ライセンス証書のアカウント情報 > URL に記載してある URL にアクセス

(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

2.4 アクティベーションコードの入力

(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

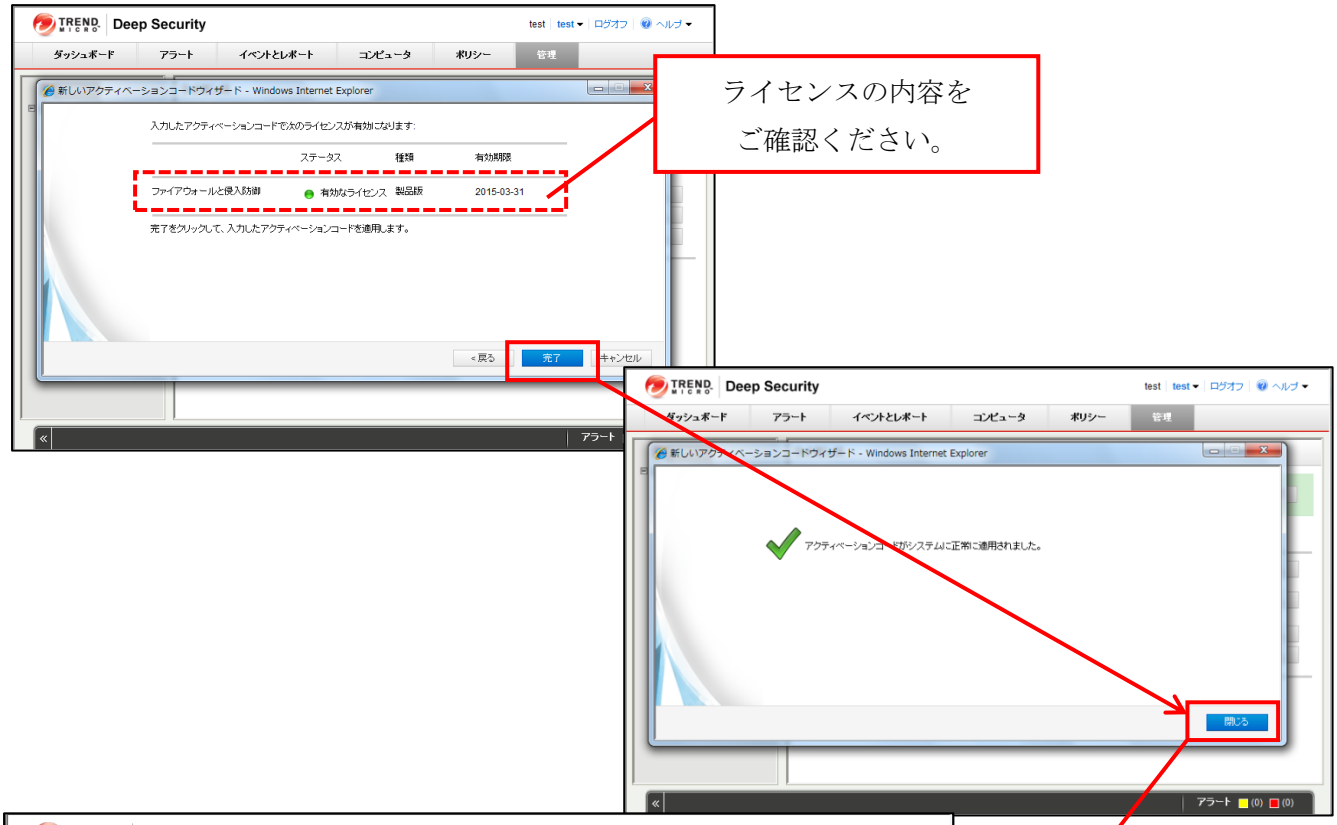
(2) お客様のご契約内容に合わせて、アクティベーションコードを入力



(3) 「仮想パッチ（侵入防御）ライセンス」の場合

(A) 以下の手順で、アクティベートを完了させて、有効なライセンスを確認

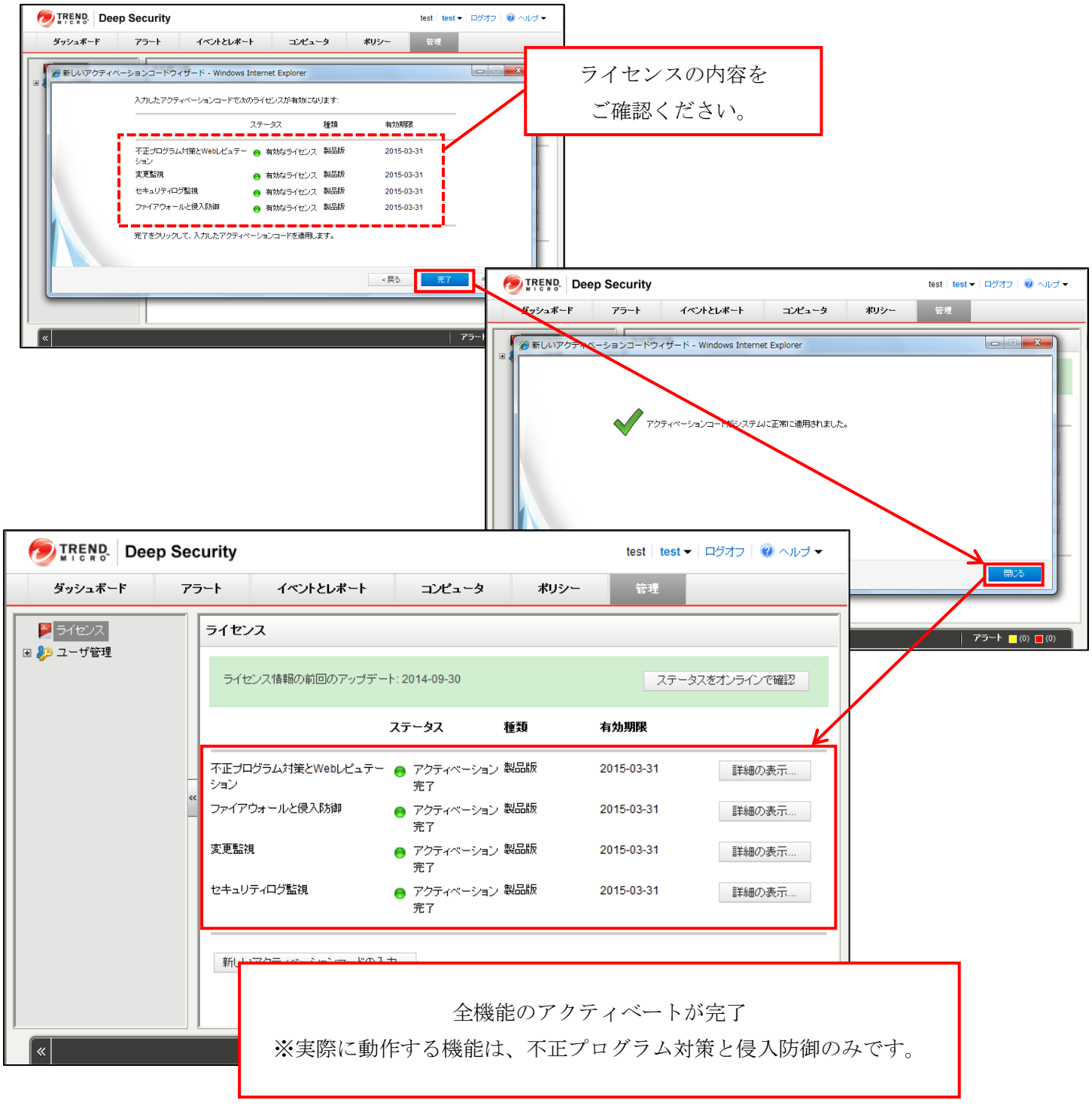
【注意事項】※侵入防御のみ※
仮想パッチ（侵入防御）ライセンスでご購入のお客様は、こちらをご参照ください
※仮想パッチ&アンチウイルスライセンスでご購入のお客様は次頁をご参照ください



（4）「仮想パッチ&アンチウイルスライセンス」の場合

（A）以下の手順で、アクティベートを完了させて、有効なライセンスを確認

【注意事項】※アンチウイルスあり※
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



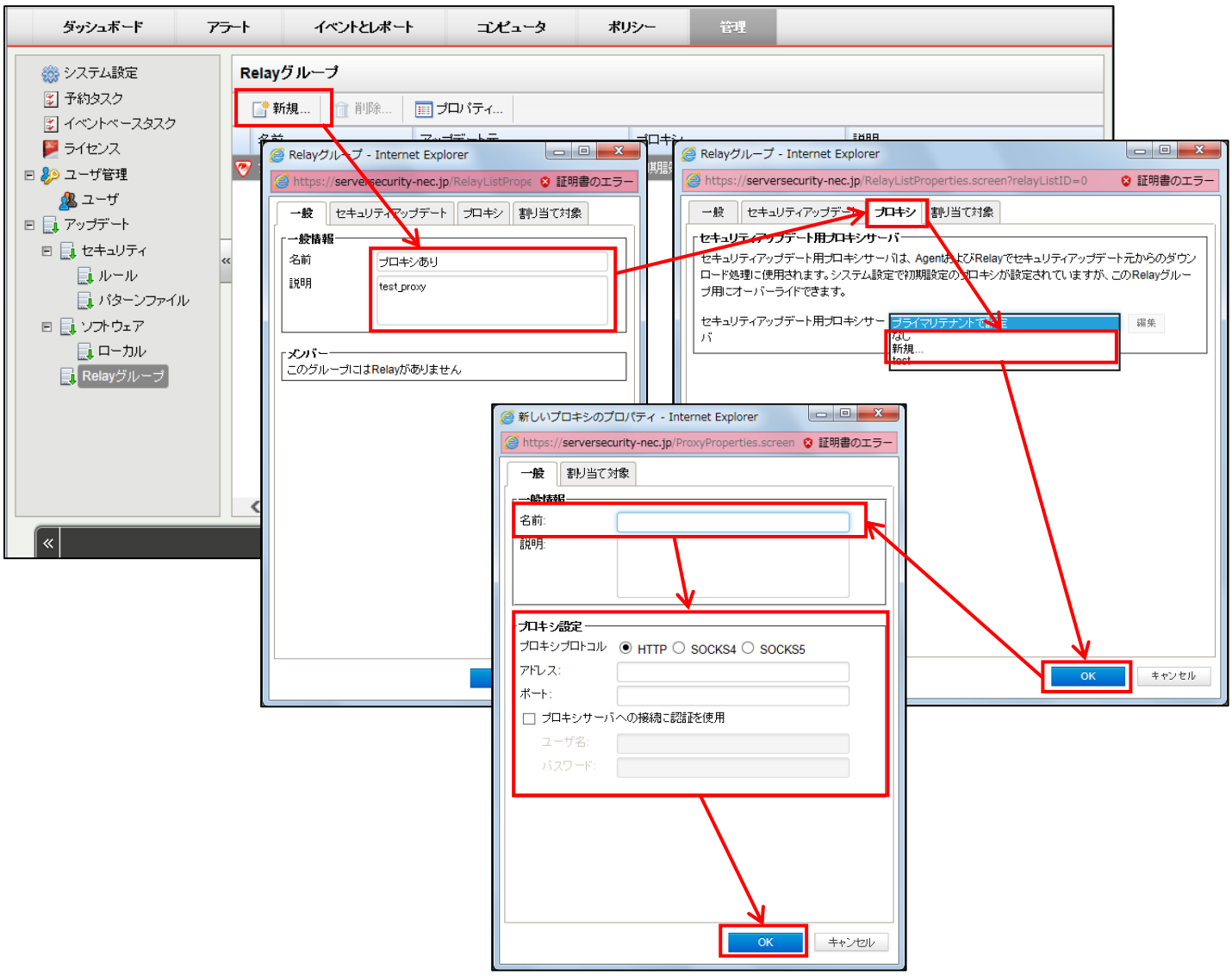
2.5 プロキシ登録

【注意事項】
プロキシを経由しない環境の場合、本手順は不要です

(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

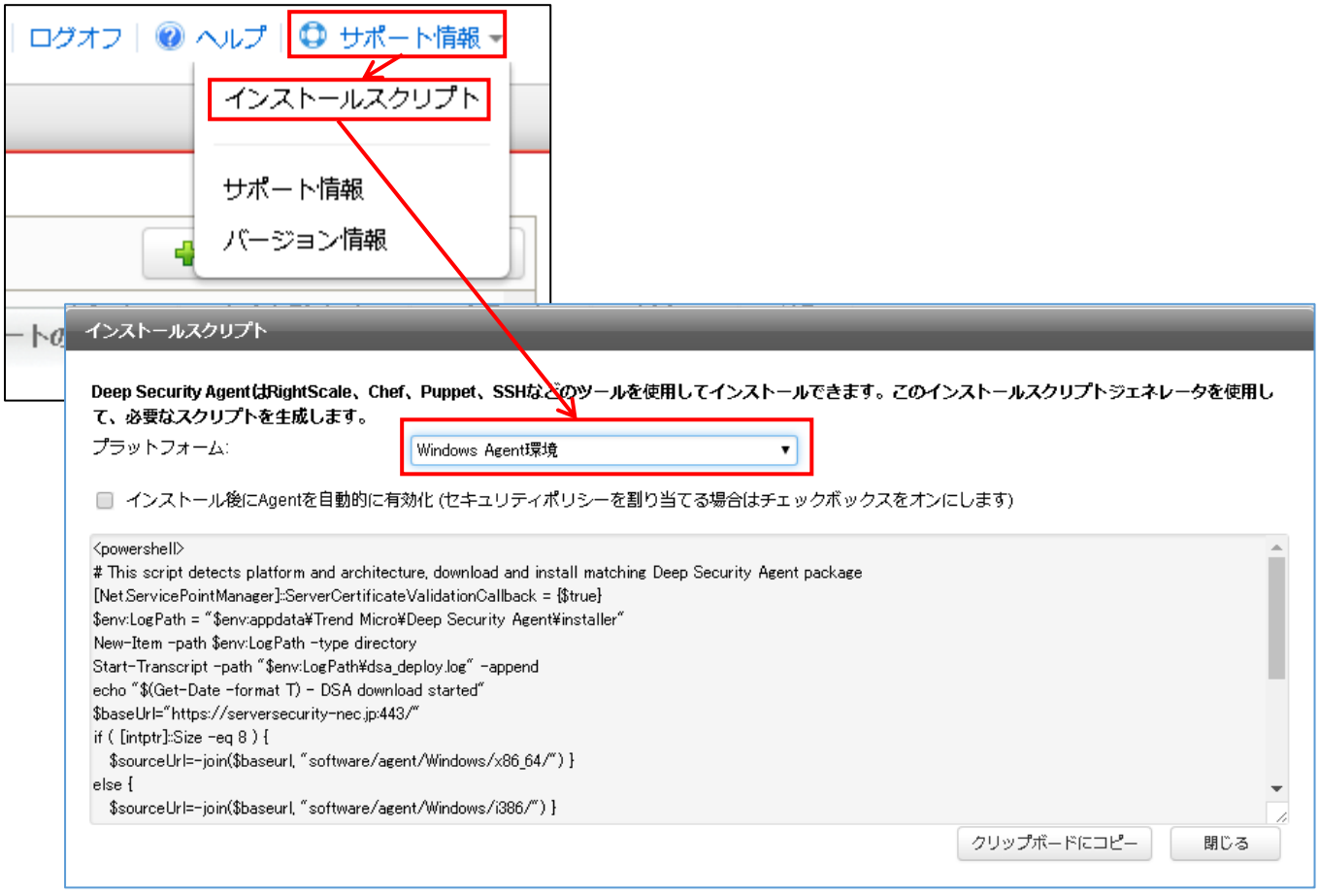


2.6 有効化コマンドの作成

【注意事項】
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。

(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

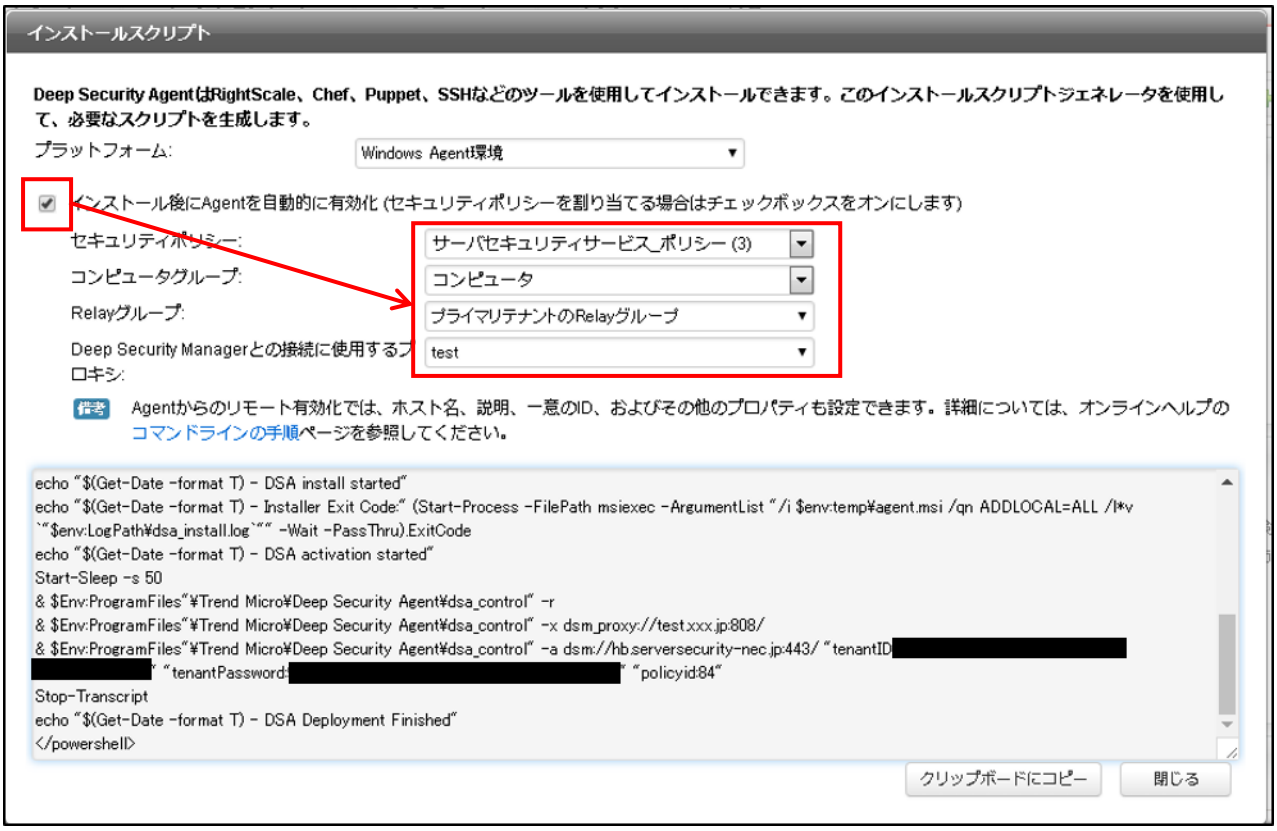


(3) [インストール後に Agent を自動的に有効化（セキュリティポリシーを割り当てる場合はチェックボックスをオンにします）]にチェックを入れる

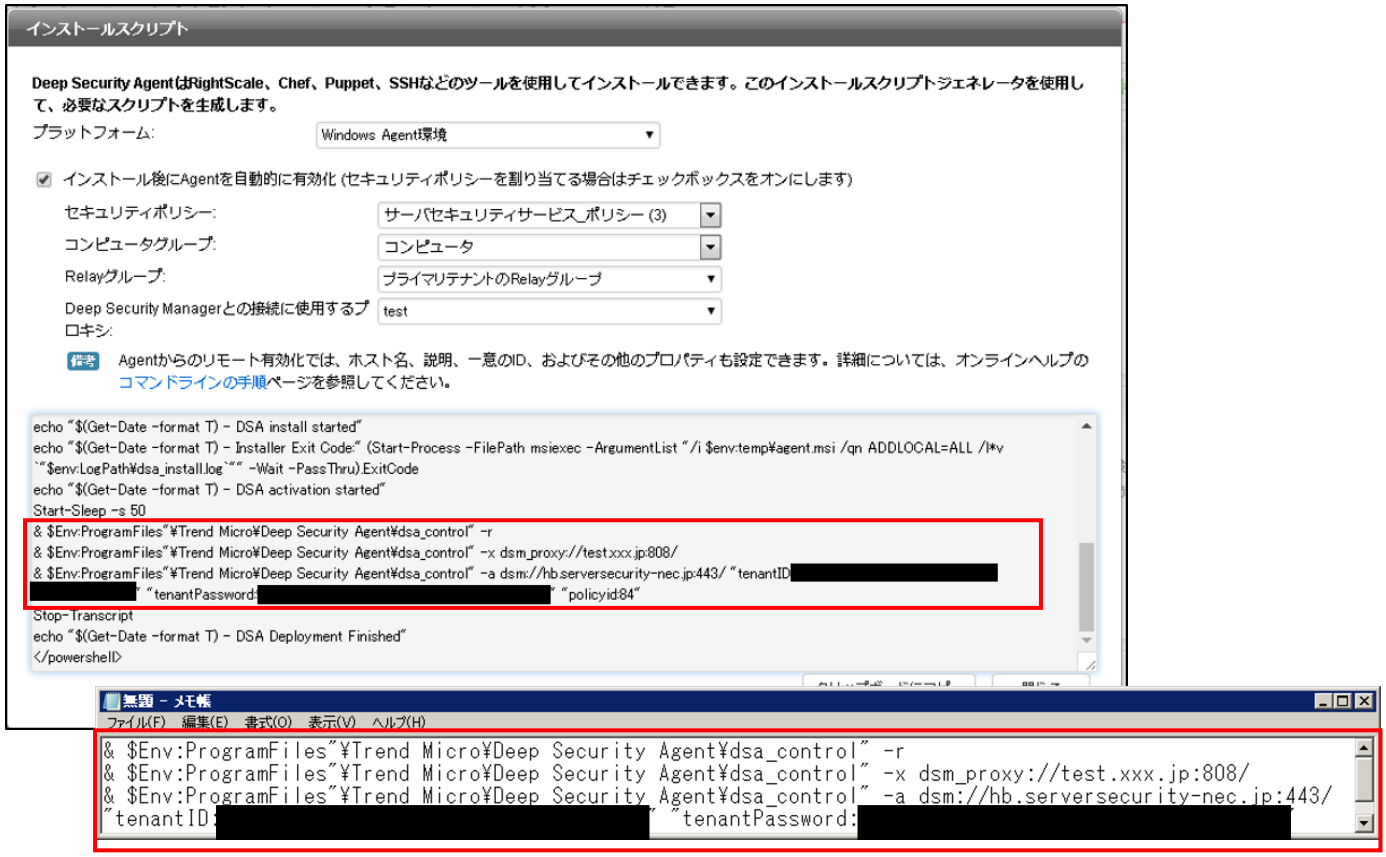
(4) セキュリティポリシーを選択 ※後ほど適用することも可能

(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）「2.5 プロキシ登録」で作成した Relay グループ、およびプロキシを選択

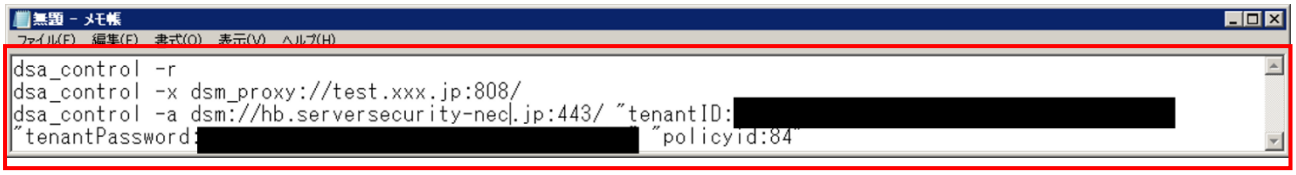


（7）「& $Env:ProgramFiles“¥Trend Micro¥Deep Security Agent¥dsa_control” -r」から「& $Env:ProgramFiles “ ¥Trend Micro¥Deep Security Agent¥dsa_control ” -a dsm://hb.serversecurity-nec.jp:443/ “tenantID:<英数字文字列>” “tenantPassword:<英数字文字列>” “policyid:<数字>” “relaygroupid:<数字>”」をコピーし、テキストエディタ等に貼り付け



（8）すべての行で「& $Env:ProgramFiles“¥Trend Micro¥Deep Security Agent¥」を削除

（9）すべての行で「dsa_control “」の「”」を削除



プロキシで認証（基本認証のみ対応）を行う場合、
「dsa_control -x “dsm_proxy://*プロキシサーバの URL:ポート*/”」行の次行に、

「dsa_control –u “*ユーザ名:パスワード*”」

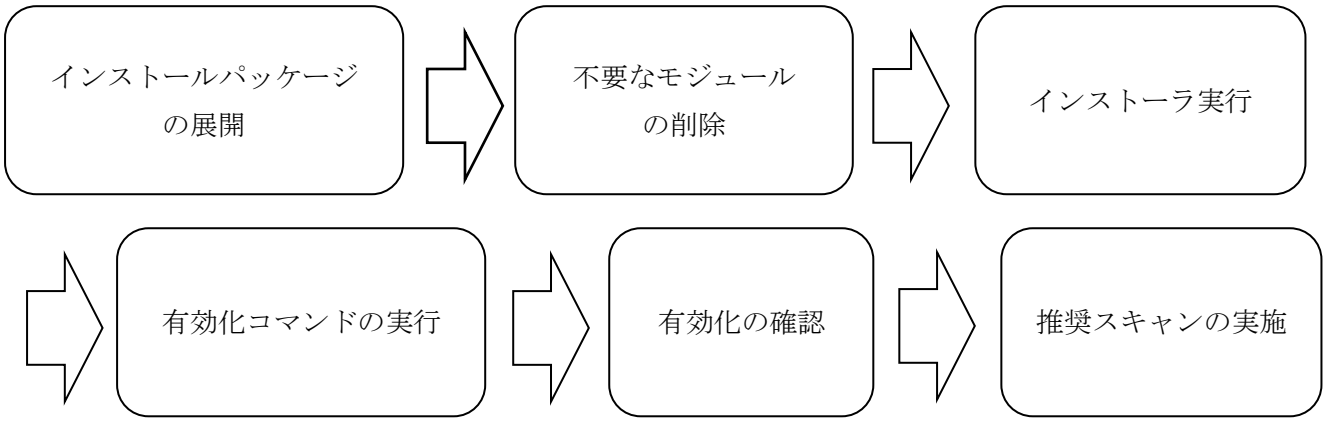
と入力してください。

例）「ユーザ名：root、パスワード：Password」の場合、以下のように入力
dsa_control –u "root:Password "

3 サーバへ Agent を導入する手順

【注意事項】
・必ず「Deep Security Agent 9.6 SP1」をダウンロードしてご利用ください。
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。
・インストール時にネットワークの瞬断が発生します。

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。



3.1 アップグレード媒体のダウンロード

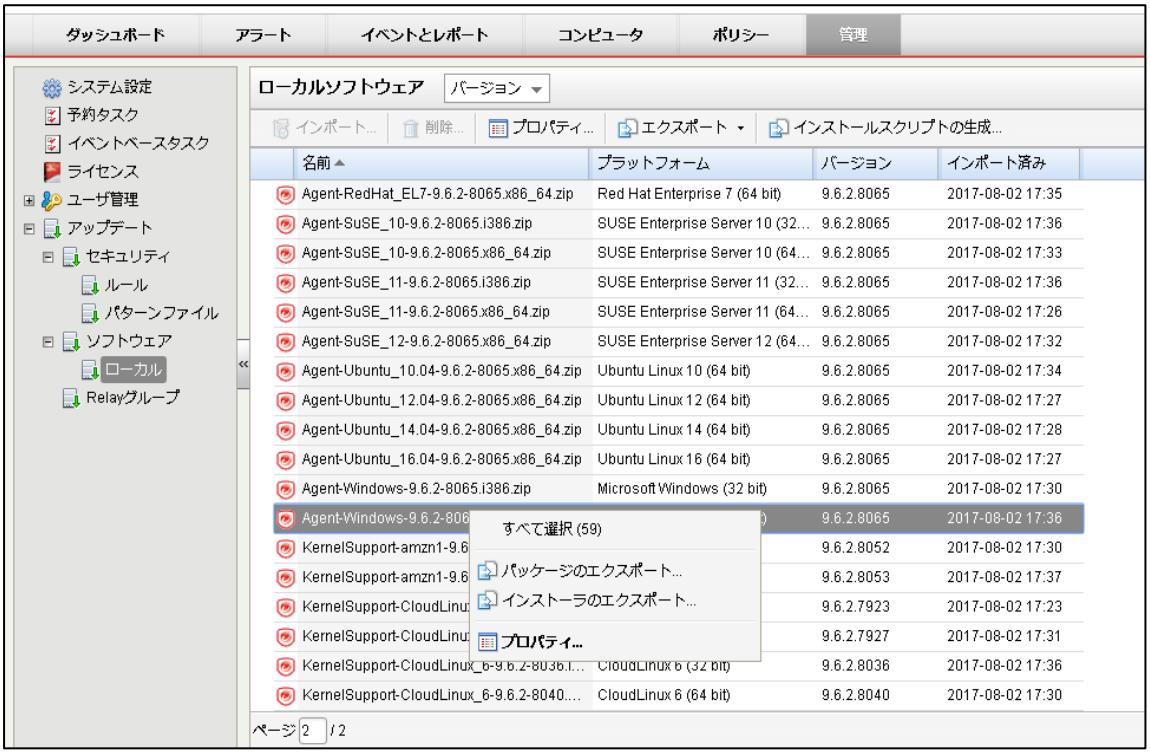
(1) サーバセキュリティサービスのコンソールにログイン

(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モジュールを右クリック
※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

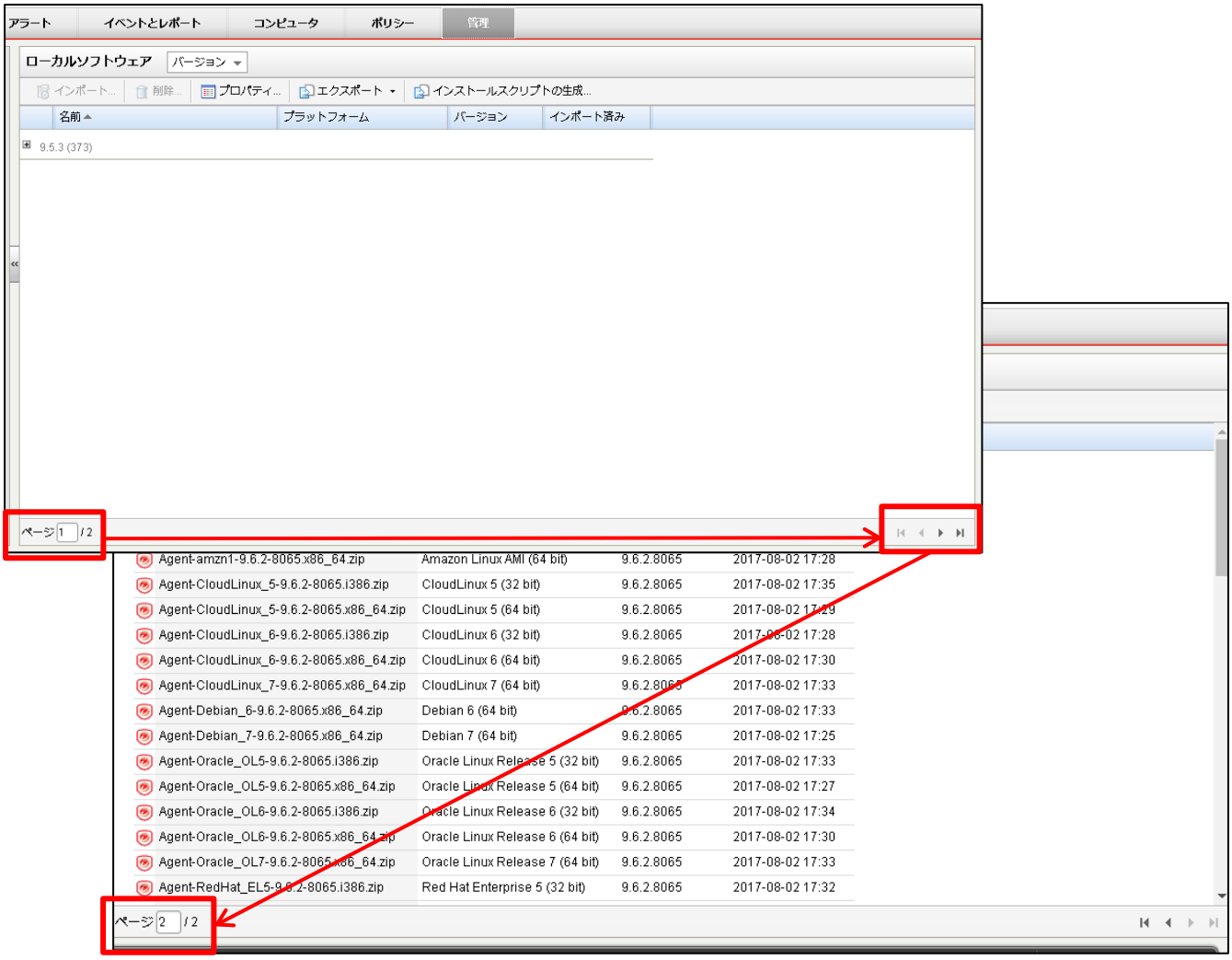
(5) [パッケージのエクスポート]を選択



（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。



3.2 インストールパッケージの展開

(1) ダウンロードしたパッケージをアップグレードするホストに配置

(2) 任意の方法で展開

※下記キャプチャは一例です

3.3 不要なモジュール削除

(1) 「仮想パッチ（侵入防御）ライセンス」の場合

【注意事項】※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

(A) 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

(B) 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

(2) 「仮想パッチ&アンチウイルスライセンス」の場合

【注意事項】※アンチウイルスあり※
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

(A) 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

(B) 不正プログラム対策機能

- Feature-AM-*.dsp
- Plugin-Update-*.dsp

※ *にはバージョンに応じた英数字文字列が入ります

(C) 侵入防御機能

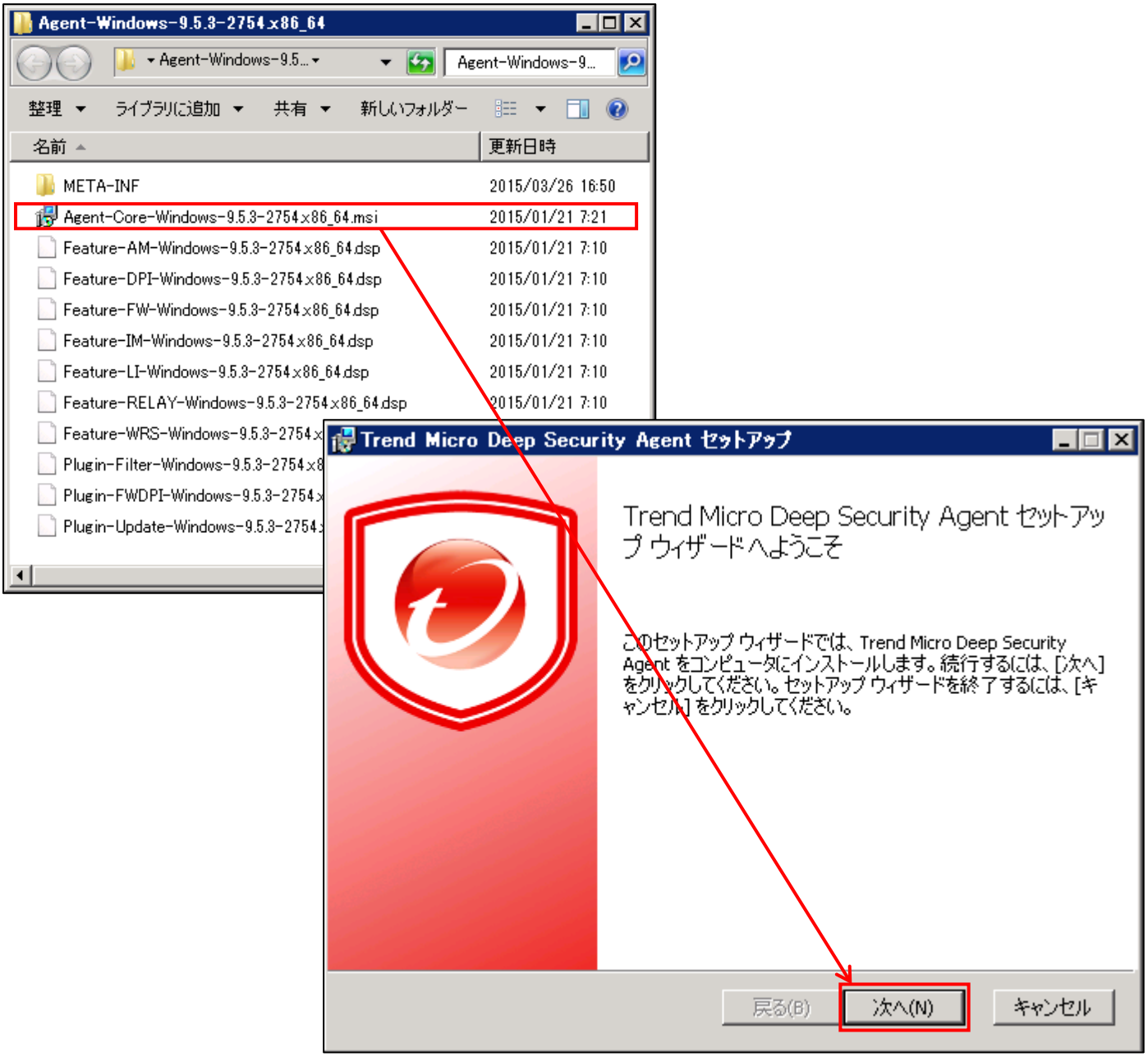
- Feature-DPI-*.dsp
- Plugin-FWDPI-*.dsp
- Plugin-Filter*.dsp

※ *にはバージョンに応じた英数字文字列が入ります

3.4 インストーラの実行

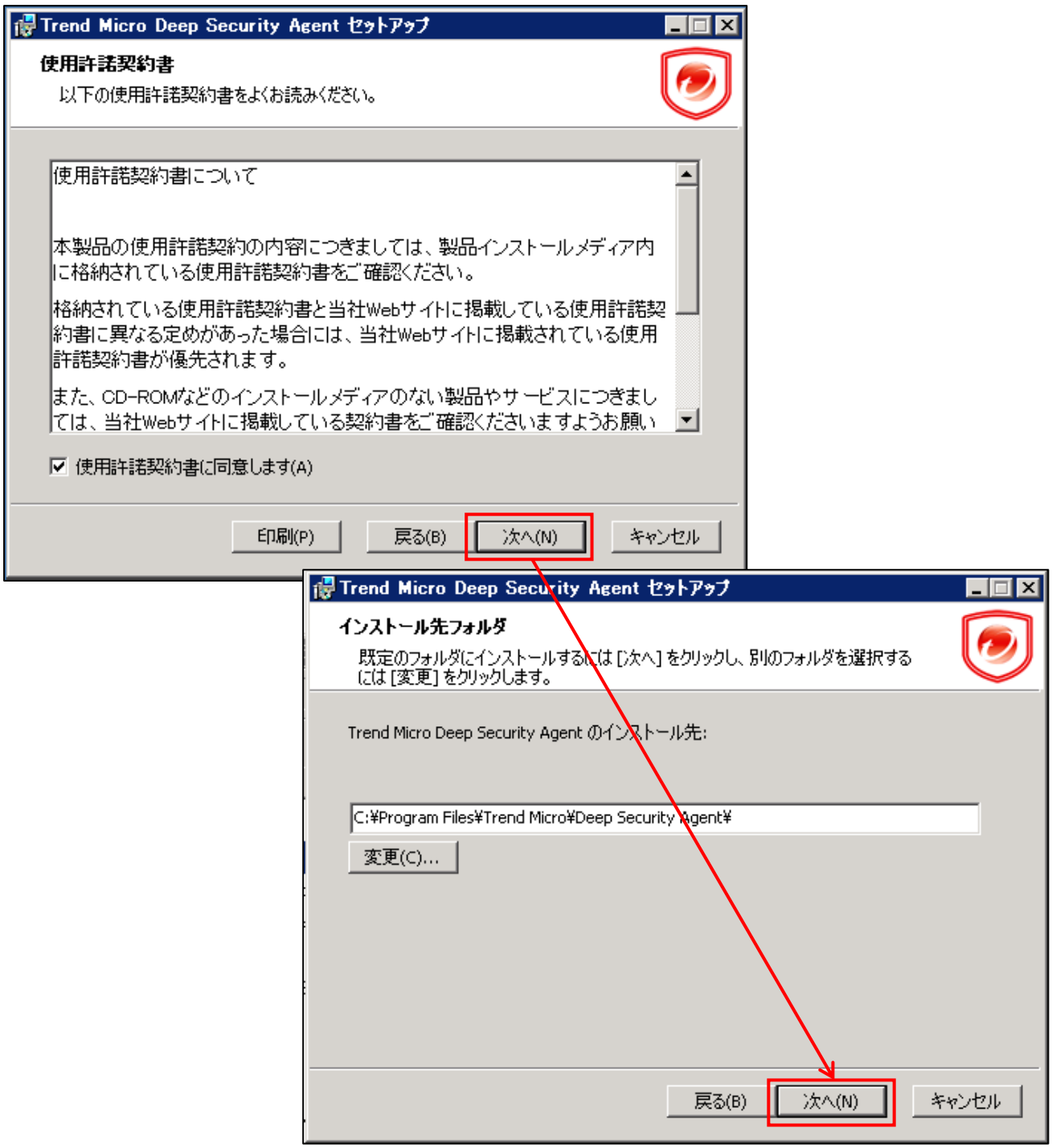
(1) インストーラを実行

(2) セットアップが起動したら［次へ］をクリック



(3) 使用許諾を確認し、問題がない場合は[使用許諾書に同意します(A)] チェックボックスにチェックし、[次へ] をクリック

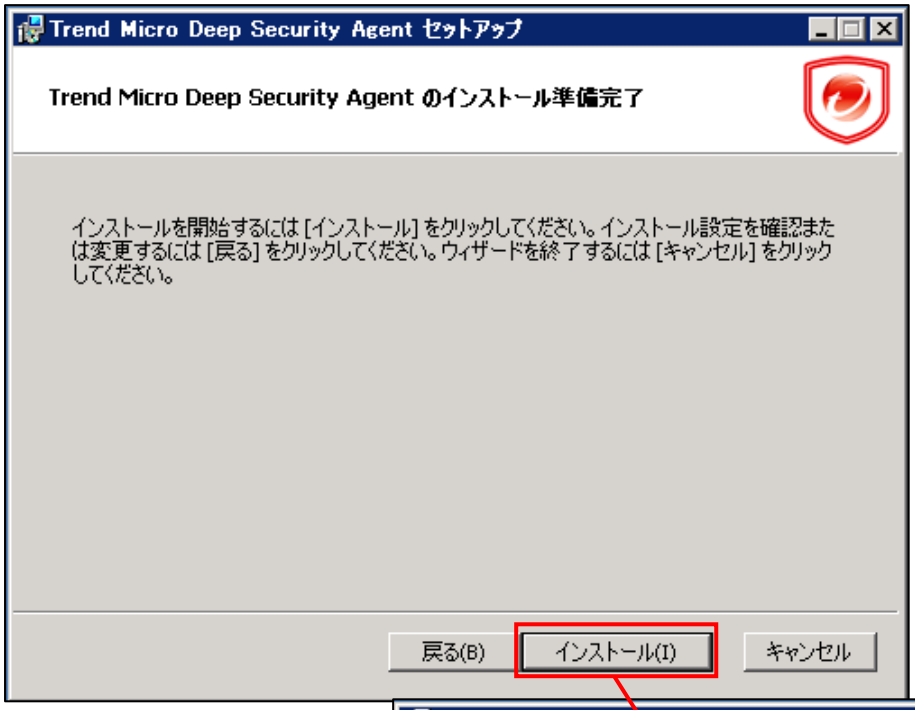
(4) インストール先フォルダを確認し、[次へ] をクリック

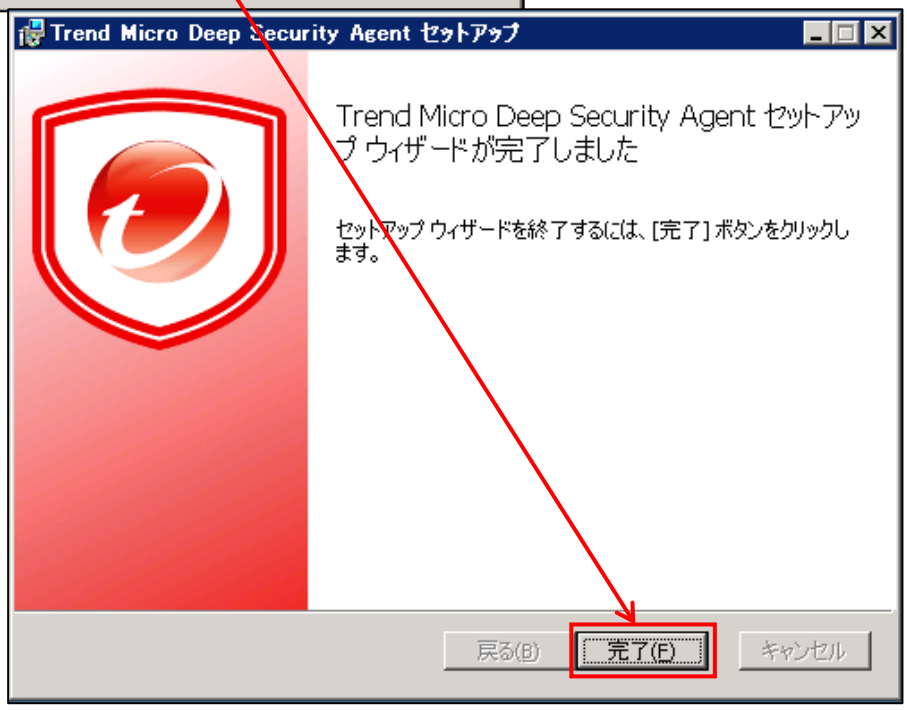


(5) [インストール]をクリック

【注意事項】
※インストール中にネットワークの瞬断が発生します。

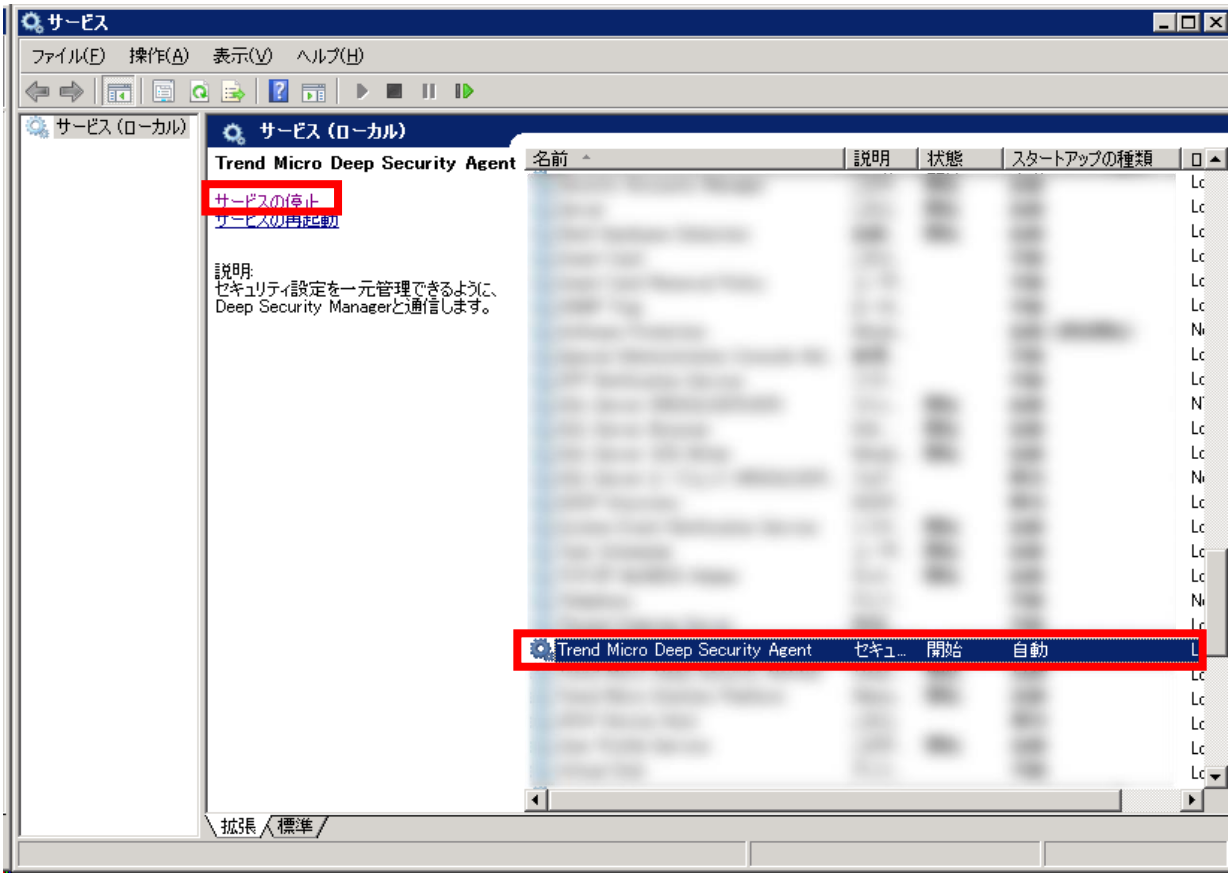
(6) [完了]をクリックしてインストールを完了





3.5 レジストリの登録

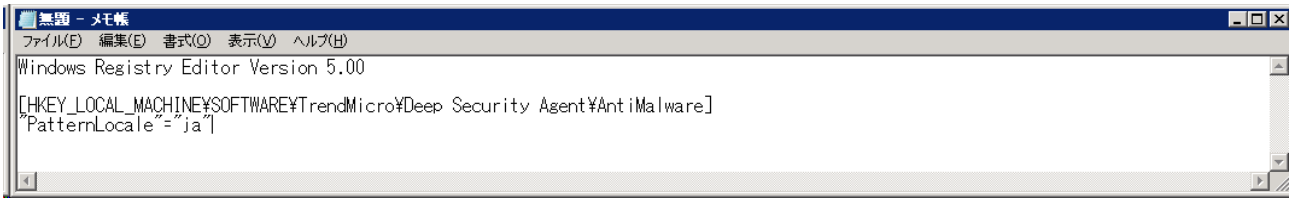
(1) [サービス]より Trend Micro Deep Security Agent サービスを停止します。



(2) Windows の[メモ帳]等のテキストエディタを起動します。

(3) 以下のテキストボックスの内容を貼り付けます。

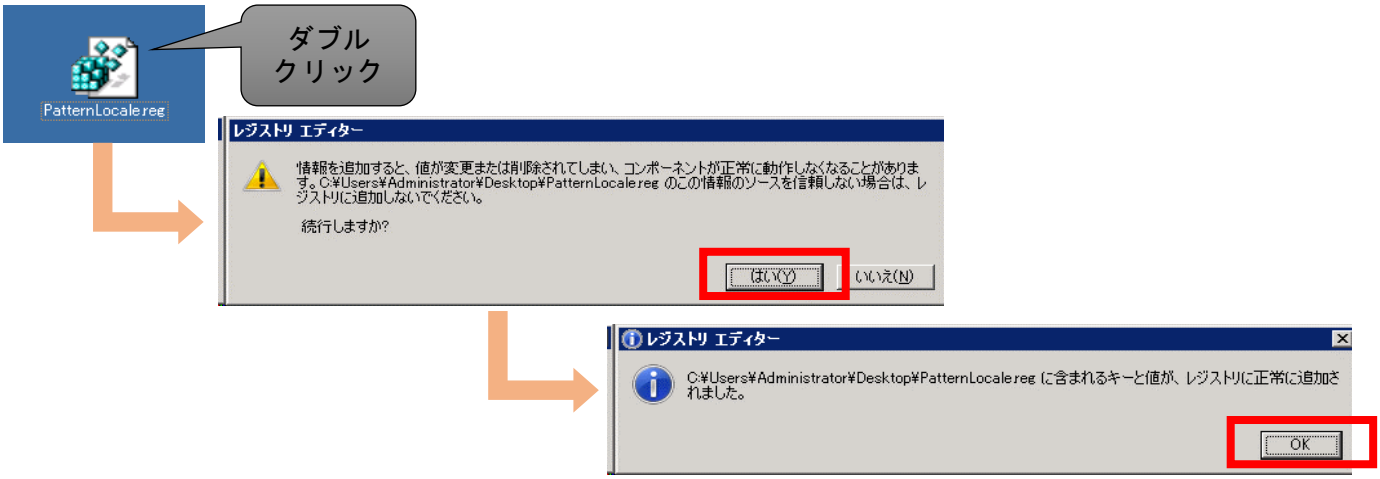
```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE¥SOFTWARE¥TrendMicro¥Deep Security Agent¥AntiMalware]
"PatternLocale"="ja"
```



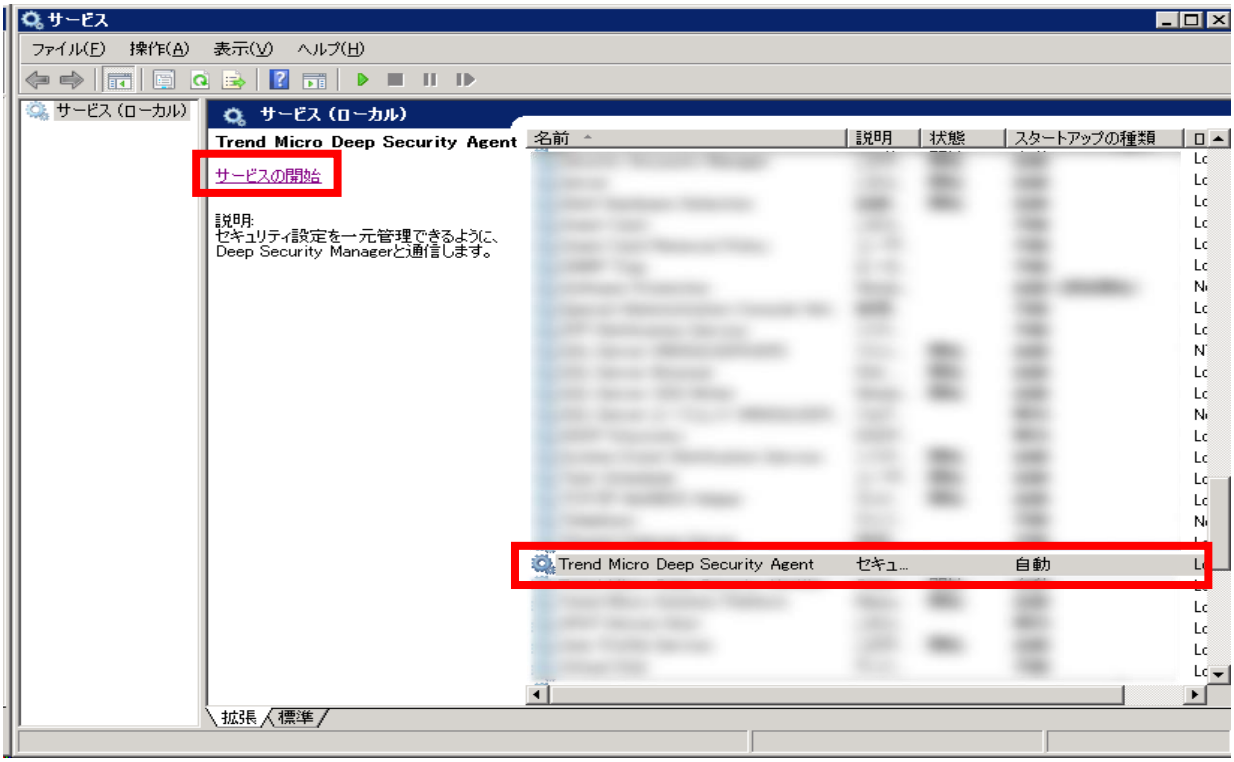
（4）[PatternLocale.reg]の名前で保存します。

（5）DSA を新規インストールしたコンピュータ上で、「3.5 (4)」で作成した[PatternLocale.reg]のファイルをダブルクリックします。

【注意事項】
レジストリの編集内容に問題があると、システムが正常に動作しなくなる場合があります。
そのため、レジストリの編集前に必ずバックアップを作成することを推奨します。
バックアップ方法の詳細は、Windows のヘルプをご参照ください。



(6) [サービス]より Trend Micro Deep Security Agent サービスを開始します。



3.6 有効化コマンドの実行

(1) コマンドプロンプトを管理者権限で開く

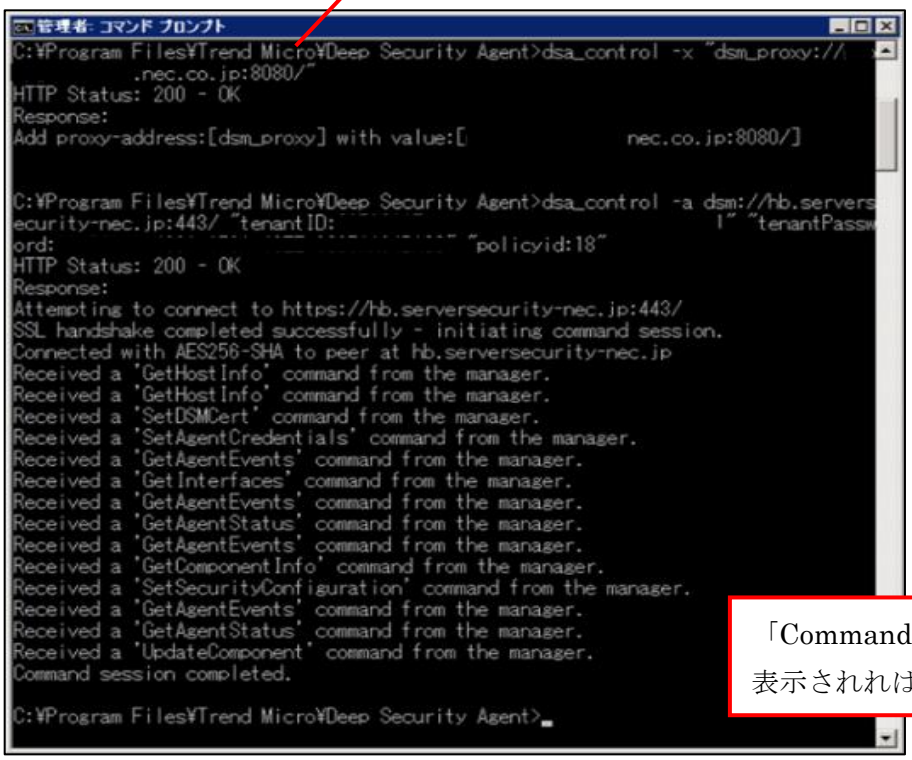
(2) 「cd (DeepSecurityAgent をインストールしたフォルダ)」を入力し[Enter]を押下

【参考】
デフォルト設定の場合は、下記のフォルダ移動コマンドを入力ください。
cd "C:¥Program Files¥Trend Micro¥Deep Security Agent"

(3) フォルダ移動後、「2.6 有効化コマンドの作成」で作成した有効化コマンドを右クリック[貼り付け]を選択し[Enter]を押下

(4) 「Command session completed.」を確認後、コマンドプロンプトを閉じる

【実行例】
dsa_control –x “dsm_proxy://proxy.xxxx.co.jp:808/“
dsa_control -a dsm://hb.serversecurity-nec.jp:443/ "tenantID:xxxx" "tenantPassword:xxxx" "policyid:18"



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

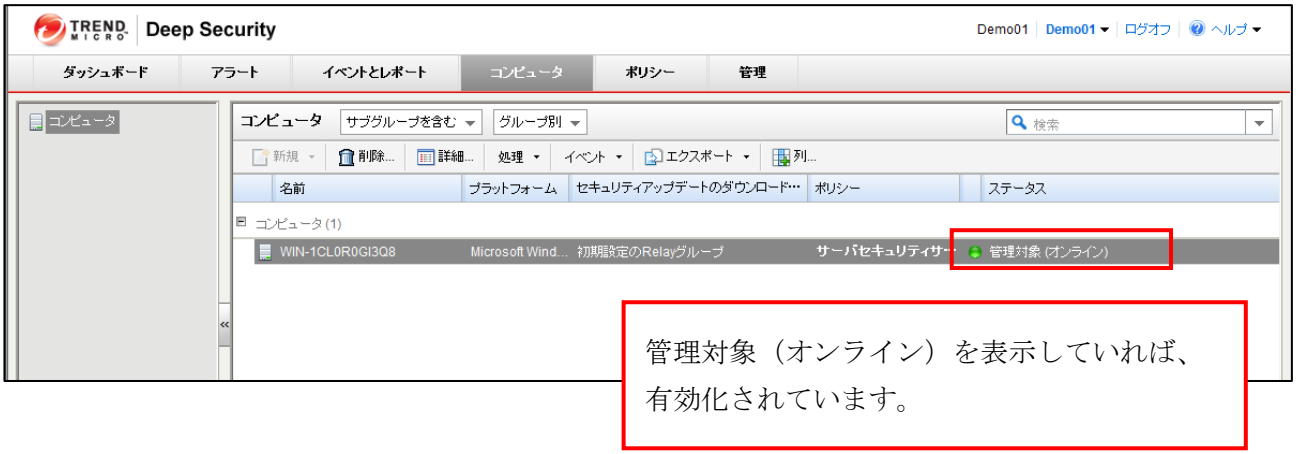
3.7 有効化の確認

(1) [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

(2) 確認後、初回アップデートが完了したのち、OS の再起動を実施

※ 不正プログラム対策機能をご利用の場合、自動アップデート後、「セキュリティアップデート：Agent/Appliance でのパターンファイルのアップデート失敗」、「不正プログラム対策がないか、期限切れ」の警告が出る場合がありますが、OS の再起動により正常に定義ファイルの読み込みが行われます



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。

3.8 推奨スキャンの実施

3.8.1 推奨スキャンの実施（１）

【注意事項】
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。

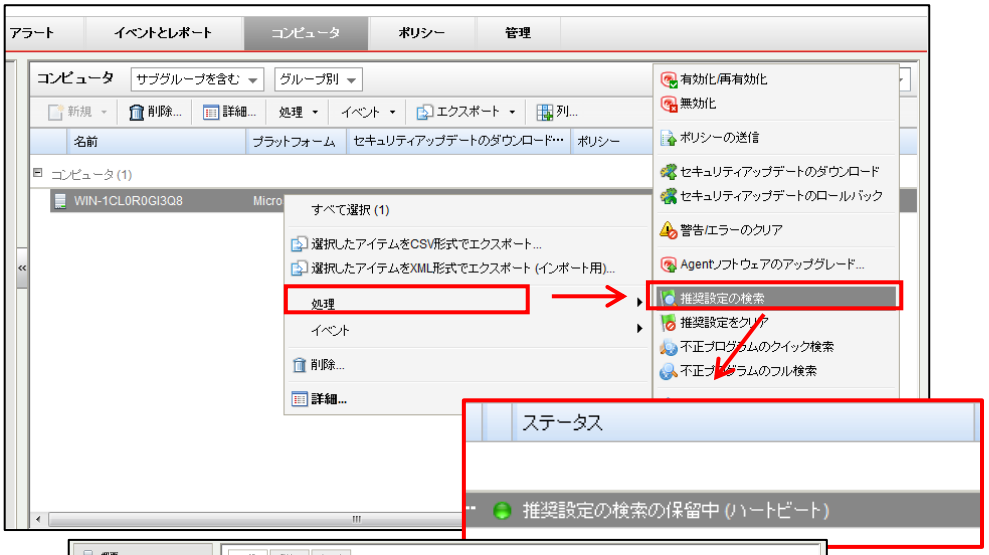
(1) [コンピュータ]タブより、対象クライアントを右クリック

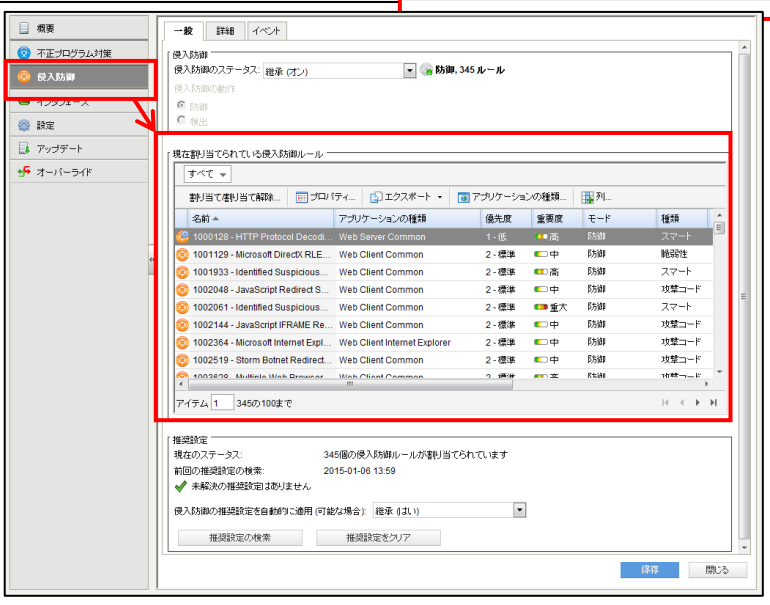
(2) [処理] > [推奨設定の検索] をクリックし推奨スキャンをクリック

(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される

(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

(5) [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





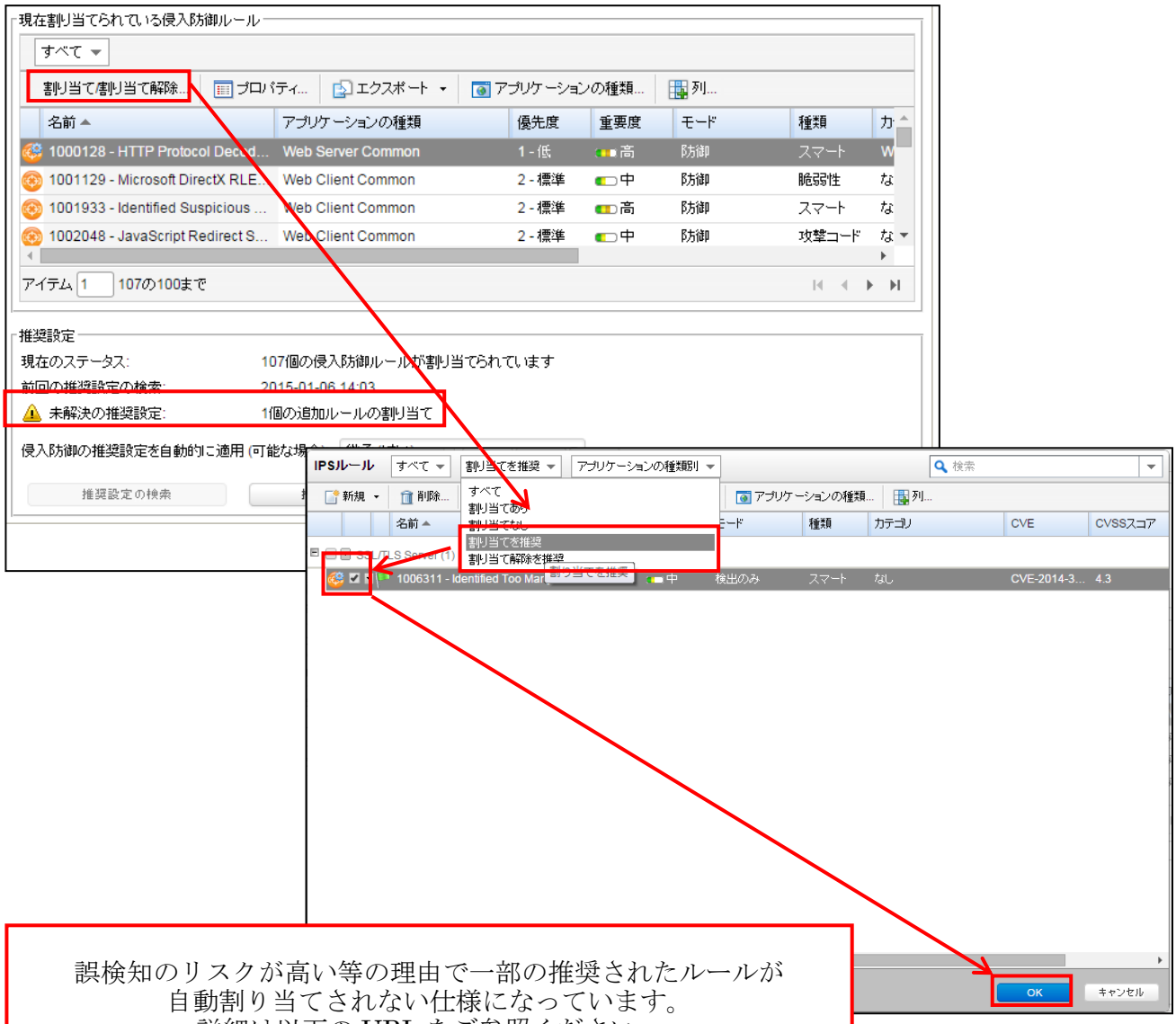
3.8.2 推奨スキャンの実施（２）

【注意事項】
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。

(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）

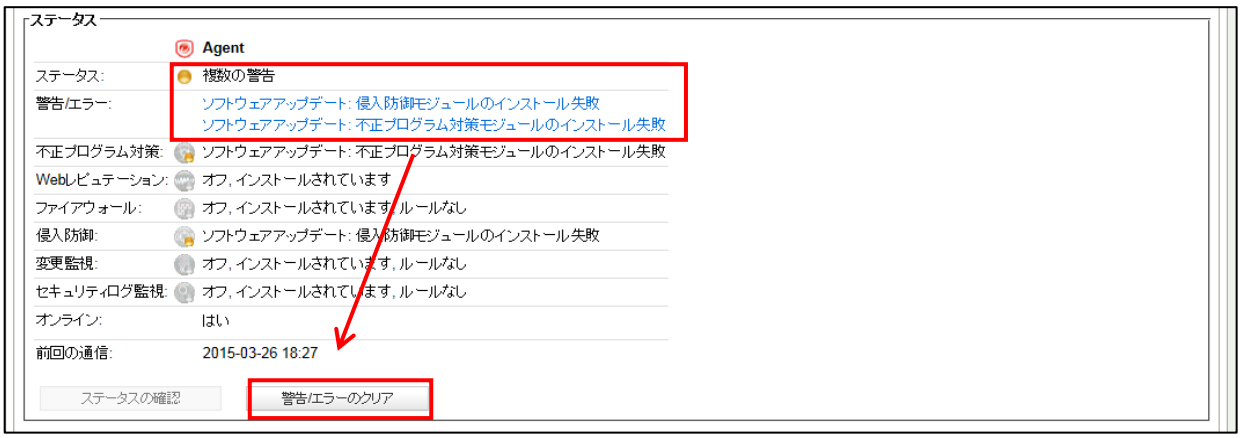
3.9 補足

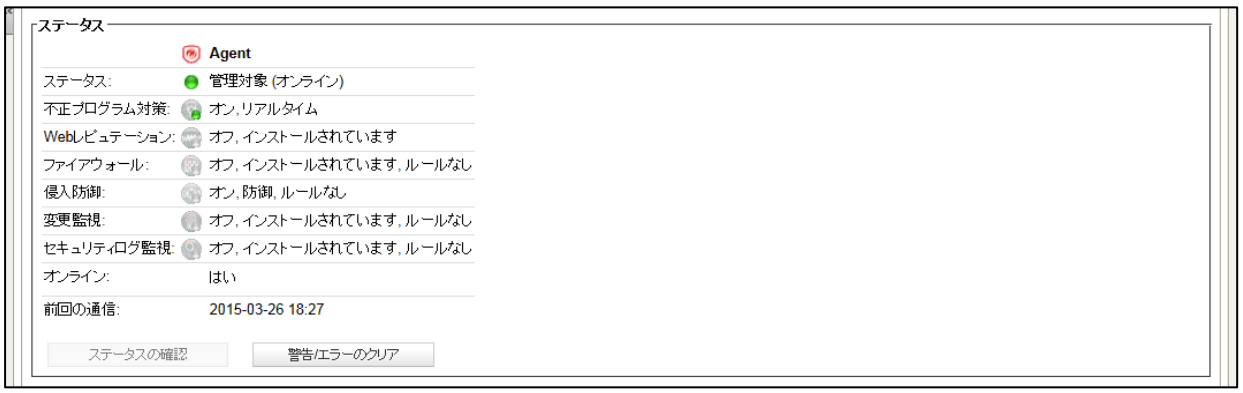
3.9.1 補足（１）「ソフトウェアアップデート：〇〇〇モジュールのインストール失敗」アラートが表示された場合の対処方法

【注意事項】
※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

(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





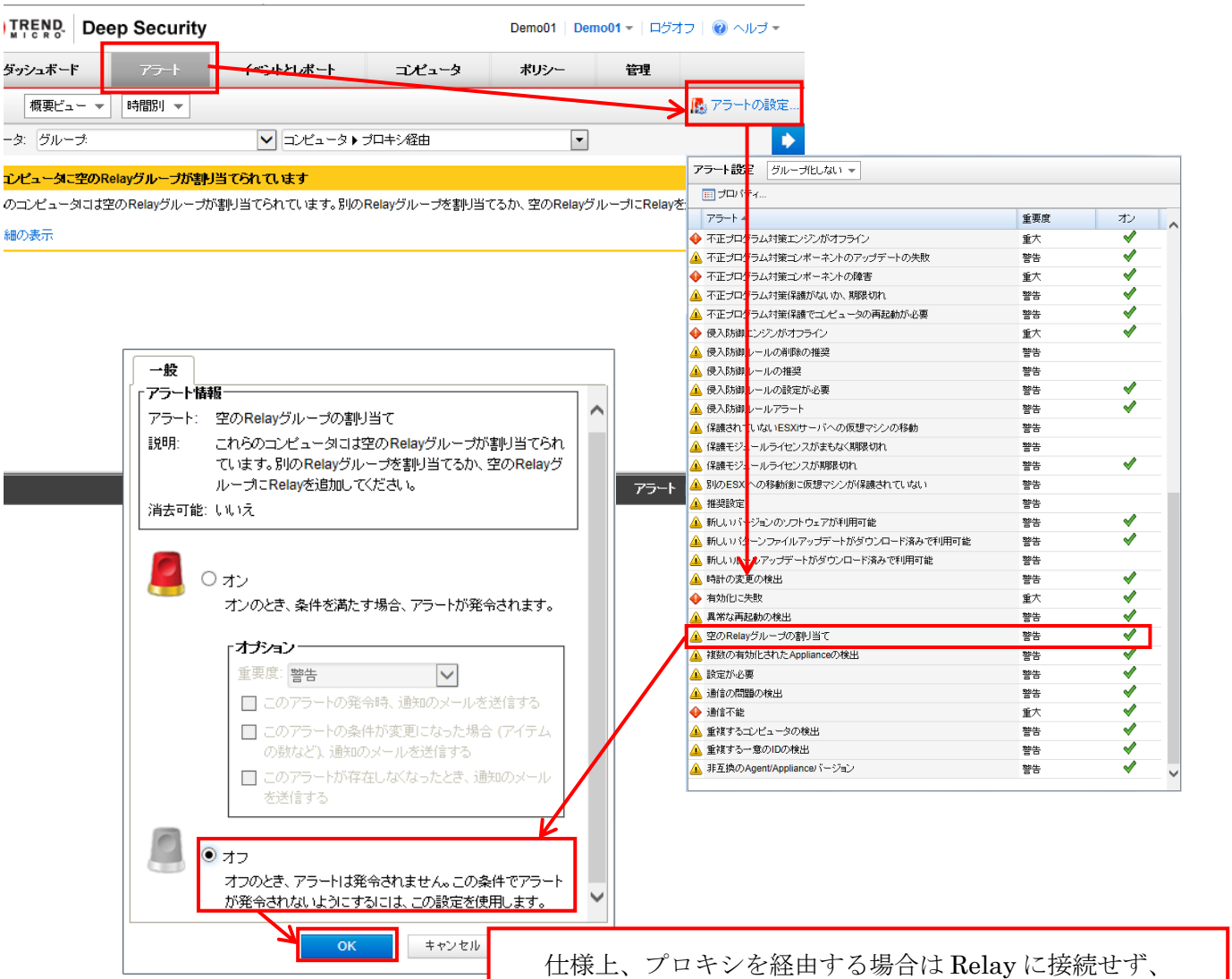
3.9.2 補足（２）「空の Relay グループが割り当てられています。」とアラートが表示された場合の対処方法

【注意事項】
製品仕様により、上記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ください。

（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



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。

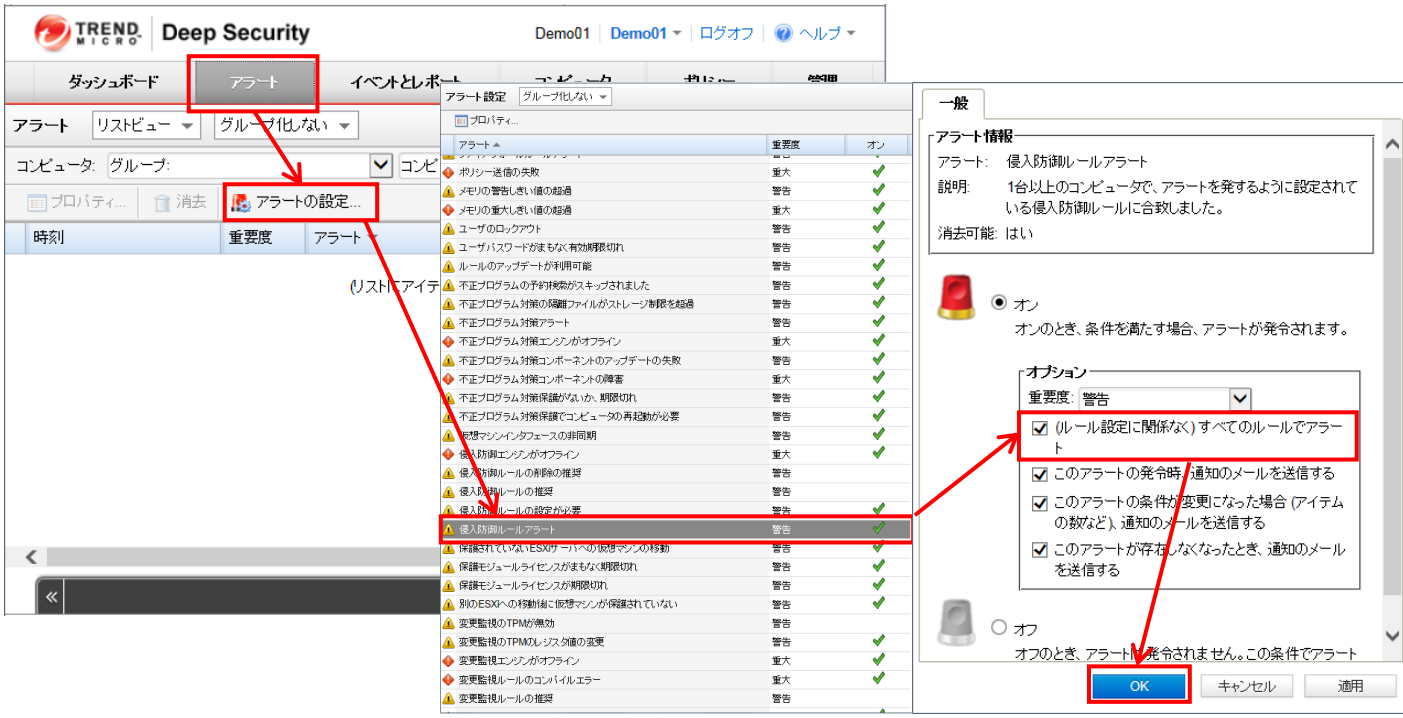
3.9.3 補足（３）検知した侵入防御イベントをアラートメールで送信する方法

【注意事項】
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ください。

(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



3.9.4 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の変更方法

【注意事項】
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）

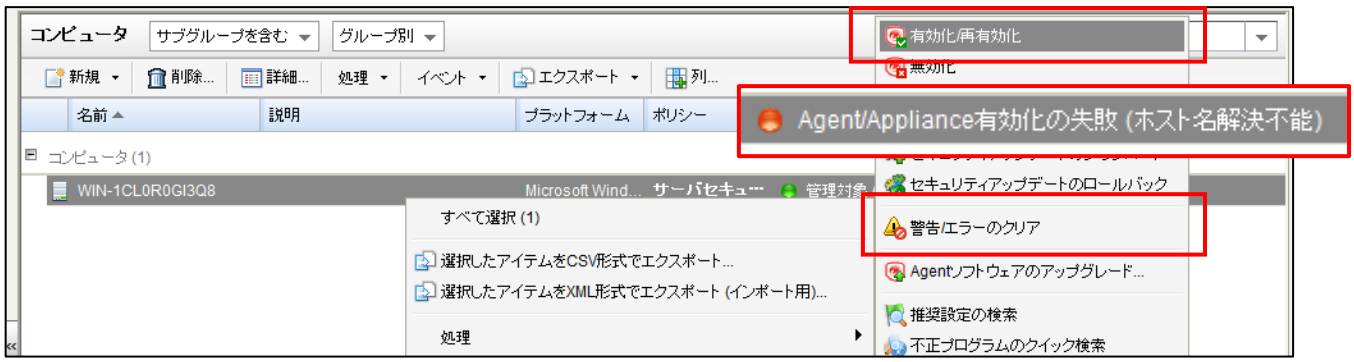
3.10 注意事項

(1) 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。



(2) アラート解決方法

(A) [処理] > [警告/エラーのクリア] を実行

(B) 「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

4 参考情報

4.1 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ください。

(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（初期設定 10 分毎）が送信された時に実行されます。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ください。

(2) Agent の初期化

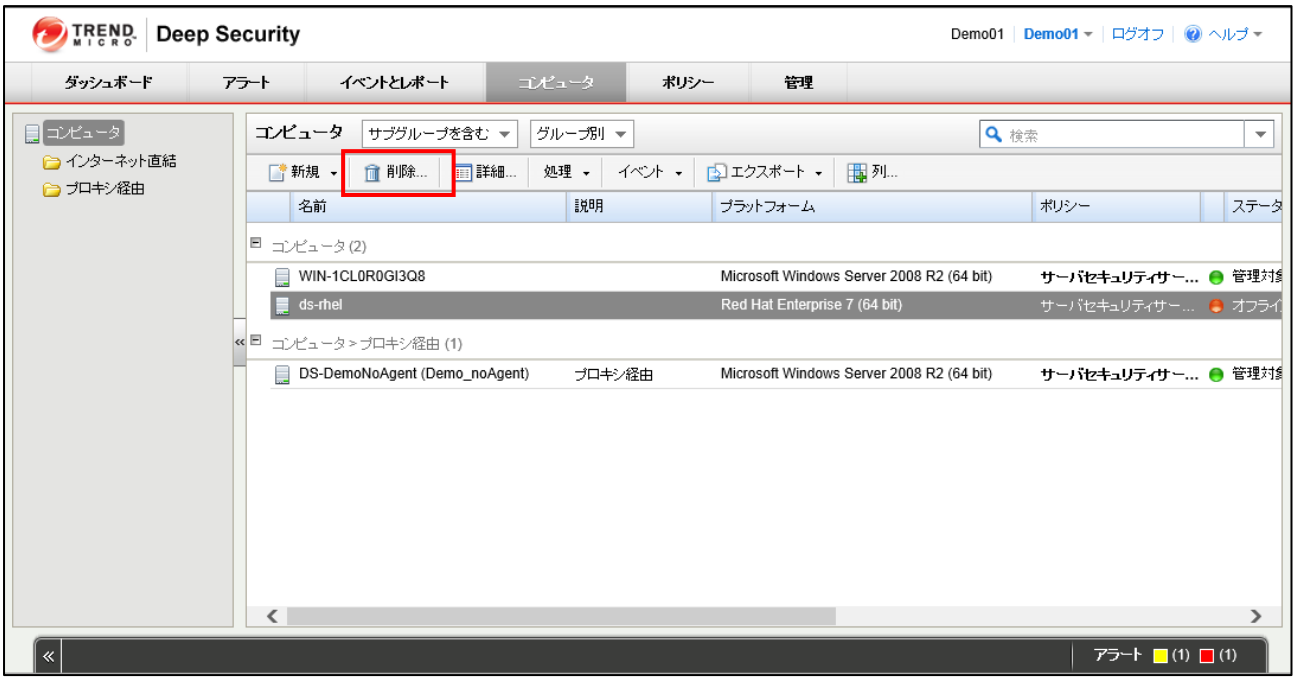
その他のコマンドや詳細につきましては、[オンラインヘルプ] > [参照] > [コマンドラインの使用方法]をご参照ください。

dsa_control -r　：Agent を初期化

4.2 アンインストール方法

(1) サーバ上の Agent は[コントロールパネル] > [プログラムの追加と削除] より、「Trend Micro Deep Security Agent」を削除

(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



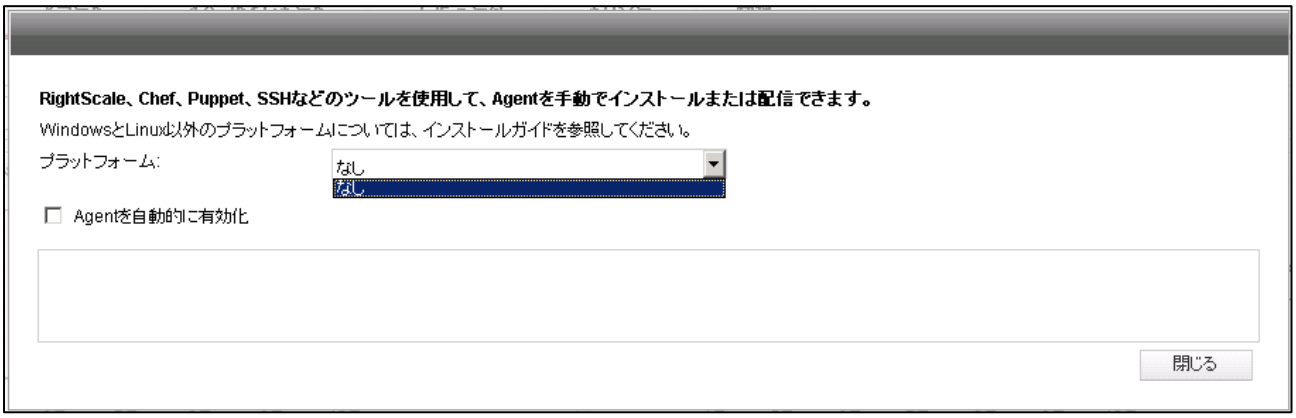
5 導入時のトラブルシューティング

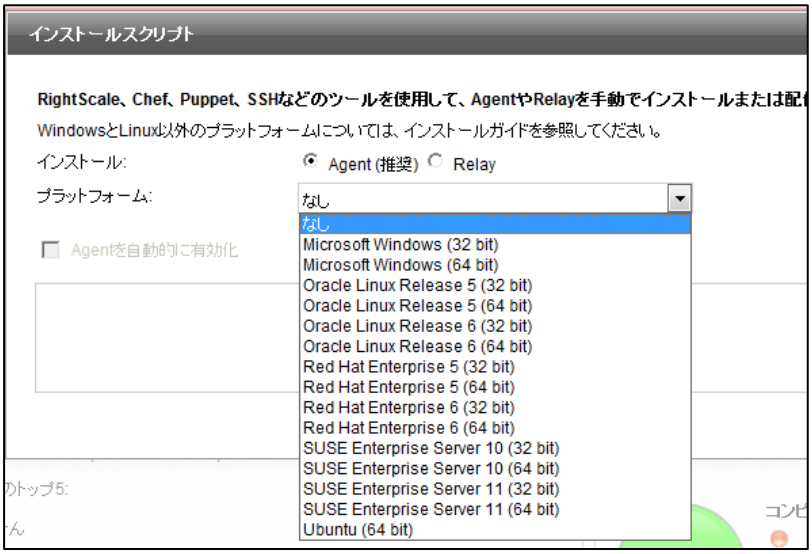
5.1 有効化コマンド作成時にプラットフォームを選択できない

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 24 以上 (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。





5.2 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、対策が必要になります。

有効化に失敗するケースとして下記のケースがあります。

(A) FW 等により、通信が遮断されている。

外向きの通信が TCP/443 ポートで「1.2 動作環境」に記載のホスト名に接続できる設定になっているかご確認ください。

(B) 名前解決に失敗している。

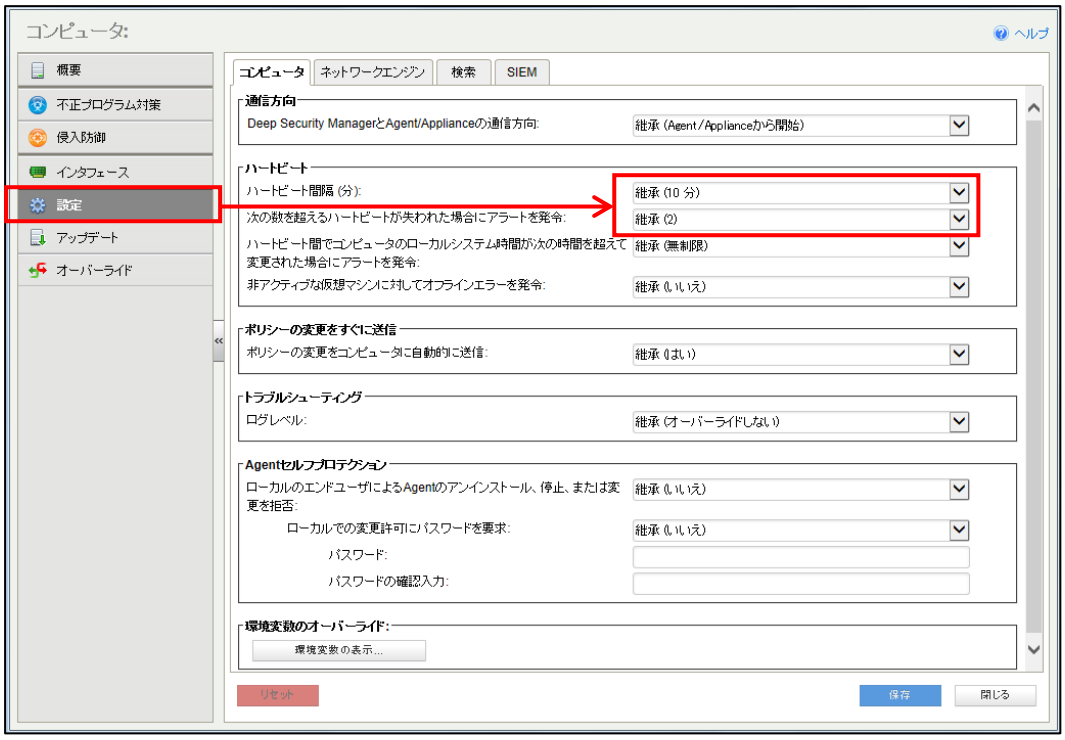
「nslookup hb.serversecurity-nec.jp」コマンドを実行し、名前解決されるかご確認ください。

5.3 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



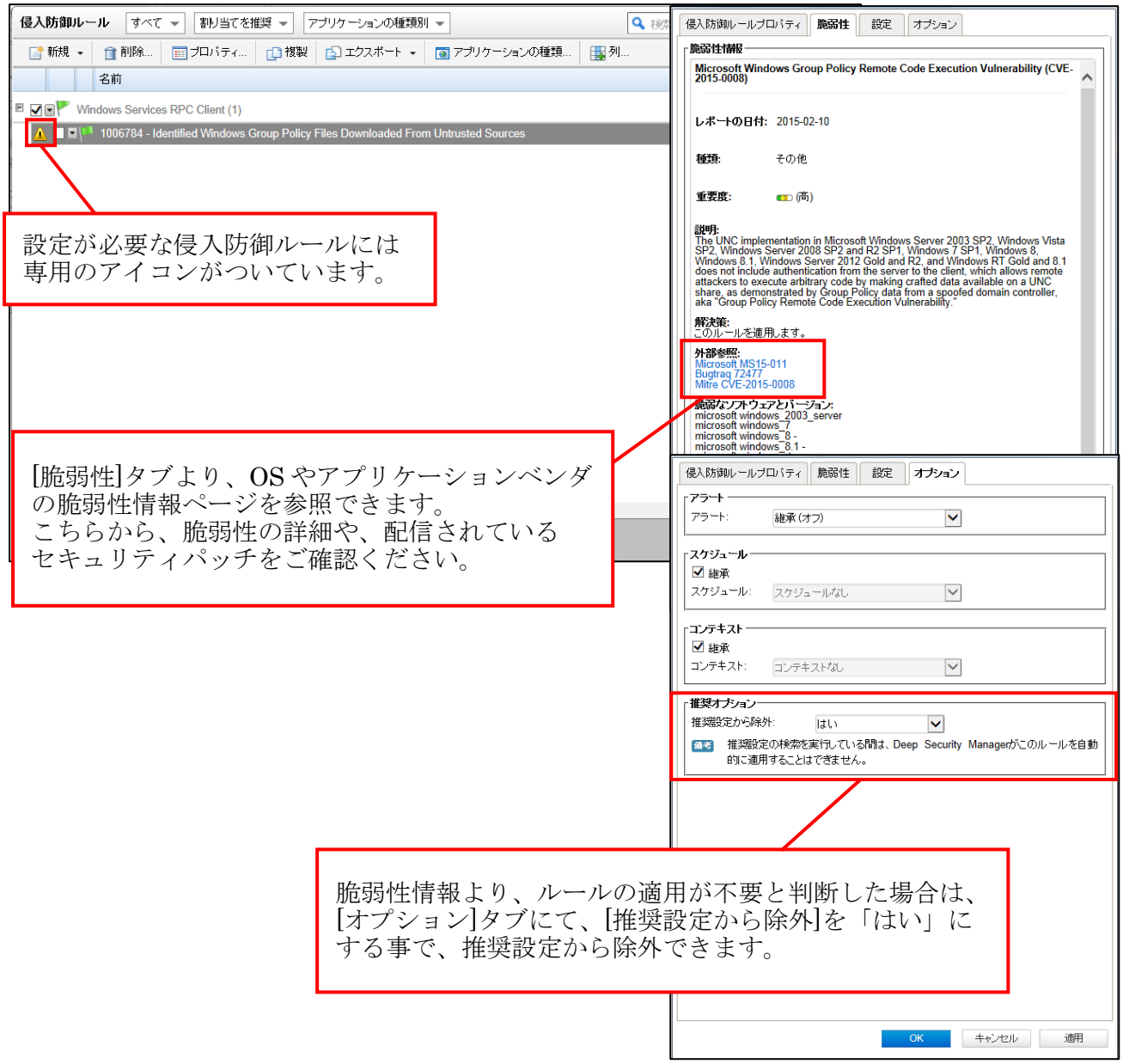
※注
ハートビート間隔を短くすると定期的に発生する通信が増加します。

5.4 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。



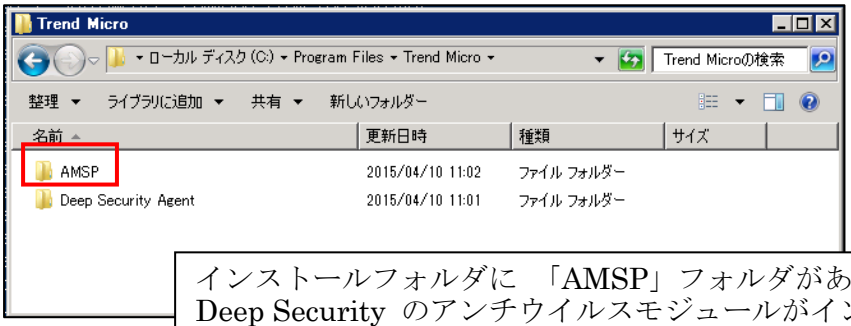
5.5 セキュリティアップデートに失敗する

「3.3 不要なモジュール削除」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ください。

本手順をスキップした場合、以下の現象が発生する可能性があります。

- 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。

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。

5.6 既知の不具合

【概要】

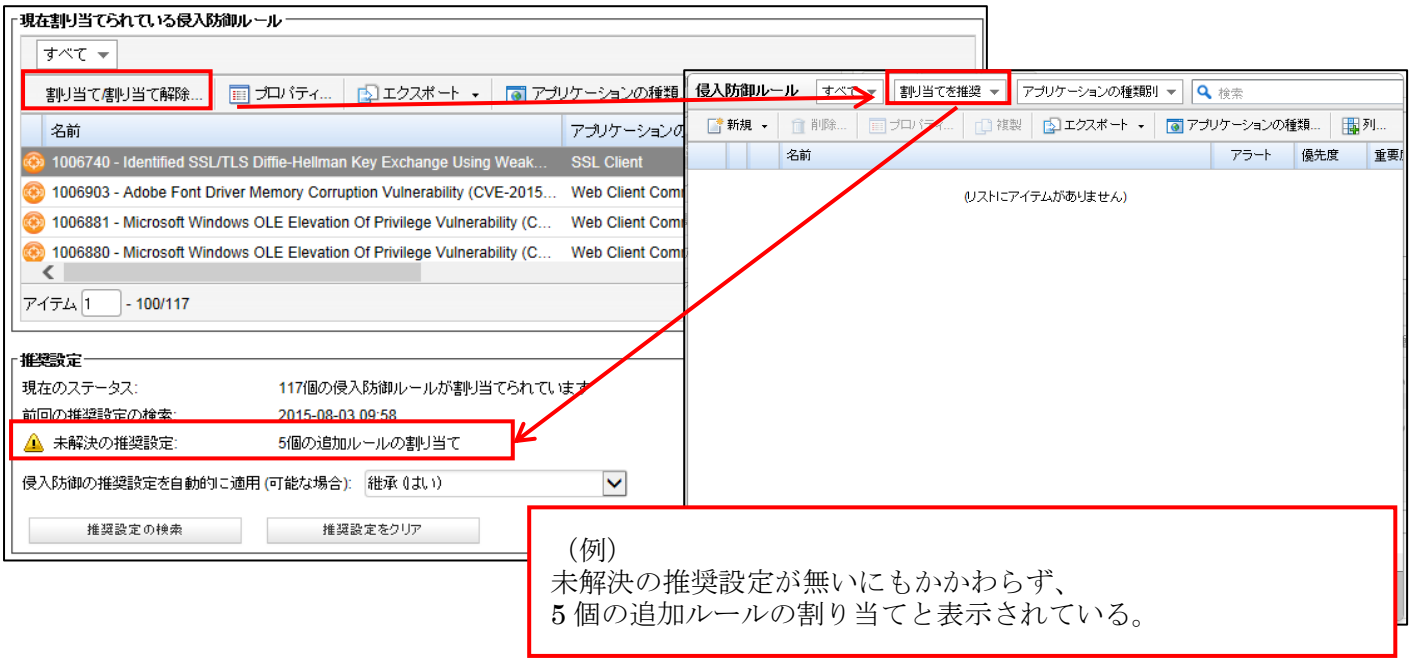
「Windows Server 2003 (32bit) 推奨ポリシー_20150709」をご利用の場合、下記の不具合が発生する可能性があります。

【事象】

「未解決の推奨設定 : x 個の追加ルールの割り当て」 に表示されるルール数が実際のお客様環境における未解決の推奨設定よりも多く表示される。

【影響/回避策】

表示上の問題で実際に[割り当て/割り当て解除…]より表示されるルールに誤りはありません。「3.8.2 推奨スキャンの実施（2）」の手順に従い、[割り当て/割り当て解除…]より割り当てを推奨されるルールで絞り込む事で未解決の推奨設定をすべてご確認頂けます。



（例）
未解決の推奨設定が無いにもかかわらず、
5 個の追加ルールの割り当てと表示されている。