

サーバセキュリティサービス アップグレード手順書 Deep Security 9.6SP1 (Windows)

NEC

第1版 2017/08/23

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」をご利用中のお客様向けの資料です。

■ サーバセキュリティサービスでは2017/7/30付で提供サービス基盤の Deep Securityのバージョンを9.5 Sp1から9.6 Sp1へとアップグレードを行いました

■ 当該手順書ではWindows 環境において「Deep Security Agent 9.5 Sp1」をご利用のお客様が「Deep Security Agent 9.6SP1」へのバージョンアップを行う方法を記載しています。

Linux OS 環境の場合、別途お客様環境に適した導入手順書をご参照ください。

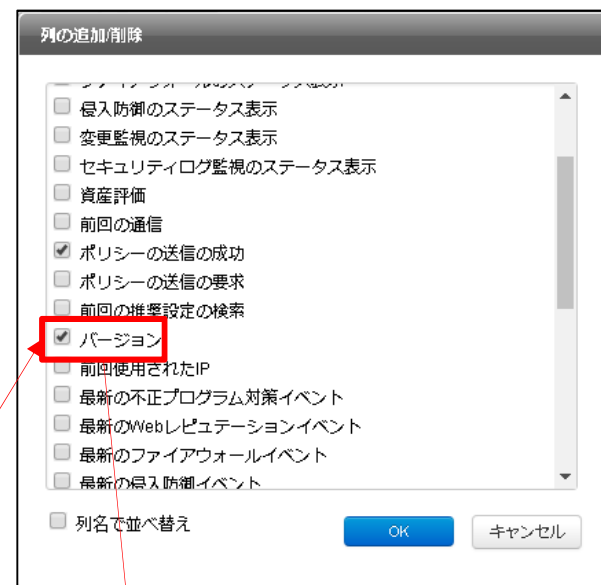
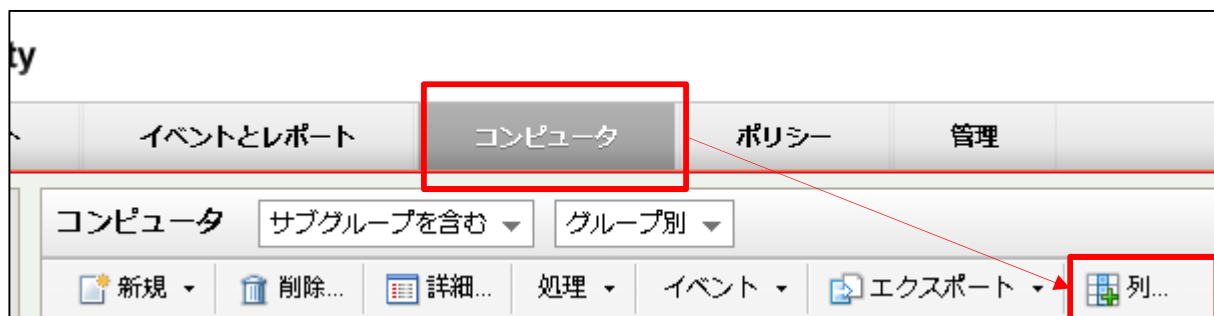
サーバセキュリティサービス with Trend Micro Deep Security - ドキュメント
<http://jpn.nec.com/soft/trendmicro/sssw/document.html>

■ Deep Security Agent 9.5 Sp1につきましては2020/1/7でサポート終了いたします。それまでにバージョンアップをご検討ください

現行のご利用バージョンの確認方法

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 [コンピュータ]を選択
- ③ [列]を選択
- ④ 「バージョン」にチェックボックスを入れ、「OK」を選択
- ⑤ バージョン列の情報を確認



The screenshot shows the console interface with the 'バージョン' (Version) column selected. The 'バージョン' column is highlighted with a red box. The table shows two rows of data:

ステータス	ポリシー	ポリシーの送信の成功	セキュリティアップデート...	バージョン
管理対象 (オンライン)	サーバセキュリティサービス_ポリシー	7 時間 前	NECイントラ	9.6.2.8065
推奨設定の検索の保留...	サーバセキュリティサービス_ポリシー	21 時間 前	NECイントラ	9.5.3.2754

Deep Security Agent 9.6 Sp1 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	<p>【Windows】</p> <p>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)</p>	<p>【Linux】</p> <p>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)</p>
Webブラウザ (管理コンソール)	<p>Internet Explorer 9, 10,11 (Cookie を有効にする) Mozilla Firefox (Cookie を有効にする)</p>	

※ 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>

Deep Security Agent 9.6 Sp1 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	
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。 プロキシを利用しない場合でも、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

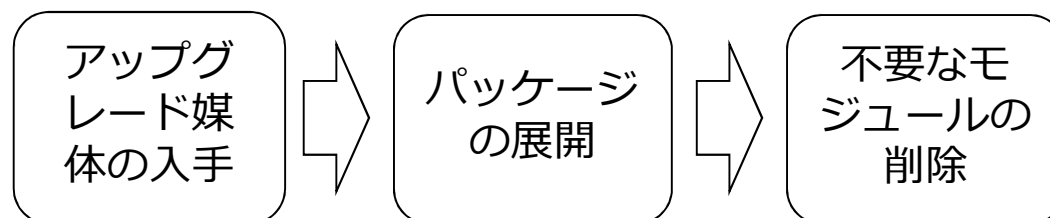
1. アップグレード媒体の入手
(参考) 9.6.2のグループが見つからない場合
2. パッケージの展開
3. 不要なモジュールの削除
 - a. 侵入防御のみの場合
 - b. アンチウイルス有りの場合

アップグレード手順

4. インストーラ実行
5. バージョンアップの確認
(参考) モジュールのインストール失敗のエラーが発生した場合

事前準備

- アップグレード媒体をコンソールから入手し、不要なモジュールの削除を行います



1. アップグレード媒体の入手

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

ダッシュボード | アラート | イベントとレポート | コンピュータ | ポリシー | 管理

ローカルソフトウェア | バージョン ▾

インポート... | 削除... | プロパティ... | エクスポート... | インストールスクリプトの生成...

名前 ▲	プラットフォーム	バージョン	インポート済み
Agent-RedHat_EL7-9.6.2-8065.x86_64.zip	Red Hat Enterprise 7 (64 bit)	9.6.2.8065	2017-08-02 17:35
Agent-SuSE_10-9.6.2-8065.i386.zip	SUSE Enterprise Server 10 (32...	9.6.2.8065	2017-08-02 17:36
Agent-SuSE_10-9.6.2-8065.x86_64.zip	SUSE Enterprise Server 10 (64...	9.6.2.8065	2017-08-02 17:33
Agent-SuSE_11-9.6.2-8065.i386.zip	SUSE Enterprise Server 11 (32...	9.6.2.8065	2017-08-02 17:36
Agent-SuSE_11-9.6.2-8065.x86_64.zip	SUSE Enterprise Server 11 (64...	9.6.2.8065	2017-08-02 17:26
Agent-SuSE_12-9.6.2-8065.x86_64.zip	SUSE Enterprise Server 12 (64...	9.6.2.8065	2017-08-02 17:32
Agent-Ubuntu_10.04-9.6.2-8065.x86_64.zip	Ubuntu Linux 10 (64 bit)	9.6.2.8065	2017-08-02 17:34
Agent-Ubuntu_12.04-9.6.2-8065.x86_64.zip	Ubuntu Linux 12 (64 bit)	9.6.2.8065	2017-08-02 17:27
Agent-Ubuntu_14.04-9.6.2-8065.x86_64.zip	Ubuntu Linux 14 (64 bit)	9.6.2.8065	2017-08-02 17:28
Agent-Ubuntu_16.04-9.6.2-8065.x86_64.zip	Ubuntu Linux 16 (64 bit)	9.6.2.8065	2017-08-02 17:27
Agent-Windows-9.6.2-8065.i386.zip	Microsoft Windows (32 bit)	9.6.2.8065	2017-08-02 17:30
Agent-Windows-9.6.2-8065.x86_64.zip	Microsoft Windows (64 bit)	9.6.2.8065	2017-08-02 17:36
KernelSupport-amzn1-9.6.2.8052	Amazon Linux 1 (64 bit)	9.6.2.8052	2017-08-02 17:30
KernelSupport-amzn1-9.6.2.8053	Amazon Linux 1 (64 bit)	9.6.2.8053	2017-08-02 17:37
KernelSupport-CloudLinux-9.6.2.7923	CloudLinux 6 (64 bit)	9.6.2.7923	2017-08-02 17:23
KernelSupport-CloudLinux-9.6.2.7927	CloudLinux 6 (64 bit)	9.6.2.7927	2017-08-02 17:31
KernelSupport-CloudLinux-9.6.2.8036	CloudLinux 6 (64 bit)	9.6.2.8036	2017-08-02 17:36
KernelSupport-CloudLinux-9.6.2.8040	CloudLinux 6 (64 bit)	9.6.2.8040	2017-08-02 17:30

ページ 2 / 2

(参考) 9.6.2のグループが見つからない場合

サーバセキュリティサービスの基盤では複数のバージョンがご利用頂けるよう、多数のコンポーネントがインポートされているため、コンソール上のソフトウェアのページが複数に分かれています

9.6.2のグループが見つからない場合、以下画像をご参考にページを切り替えてご確認ください

The screenshot displays two windows from the NEC security management console. The left window, titled 'ローカルソフトウェア' (Local Software), shows a table with columns for '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 window, titled 'ポリシー' (Policy), shows a similar table. Both windows have pagination controls at the bottom. Red boxes highlight the 'ページ 1 / 2' (Page 1 / 2) indicator and the navigation buttons in both windows, indicating that the user should navigate to page 2 to find the 9.6.2 group.

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	
Linux 6 (32 bit)	9.6.2.8065	2017-08-02 17:28	
Linux 6 (64 bit)	9.6.2.8065	2017-08-02 17:30	
Linux 7 (64 bit)	9.6.2.8065	2017-08-02 17:33	
Linux 7 (64 bit)	9.6.2.8065	2017-08-02 17:33	
Linux 7 (64 bit)	9.6.2.8065	2017-08-02 17:33	
Linux 7 (64 bit)	9.6.2.8065	2017-08-02 17:25	
Agent-Debian_7-9.6.2-8065.x86_64.zip	Debian (64 bit)	9.6.2.8065	2017-08-02 17:33
Agent-Oracle_OL5-9.6.2-8065.i386.zip	Oracle Linux Release 5 (32 bit)	9.6.2.8065	2017-08-02 17:27
Agent-Oracle_OL5-9.6.2-8065.x86_64.zip	Oracle Linux Release 5 (64 bit)	9.6.2.8065	2017-08-02 17:27
Agent-Oracle_OL6-9.6.2-8065.i386.zip	Oracle Linux Release 6 (32 bit)	9.6.2.8065	2017-08-02 17:34
Agent-Oracle_OL6-9.6.2-8065.x86_64.zip	Oracle Linux Release 6 (64 bit)	9.6.2.8065	2017-08-02 17:30
Agent-Oracle_OL7-9.6.2-8065.x86_64.zip	Oracle Linux Release 7 (64 bit)	9.6.2.8065	2017-08-02 17:33
Agent-RedHat_EL5-9.6.2-8065.i386.zip	Red Hat Enterprise 5 (32 bit)	9.6.2.8065	2017-08-02 17:32

2.パッケージの展開

手順

- 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.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

3.不要なモジュールの削除(b) 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

■ 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。

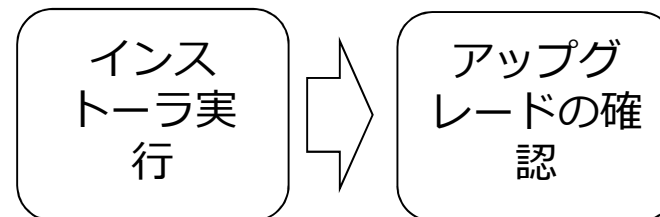
※削除しない場合、予期せぬ問題が発生する事例が確認されております

- 不正プログラム対策機能
 - Feature-AM-*.dsp
 - Plugin-Update-*.dsp
- 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

アップグレード手順

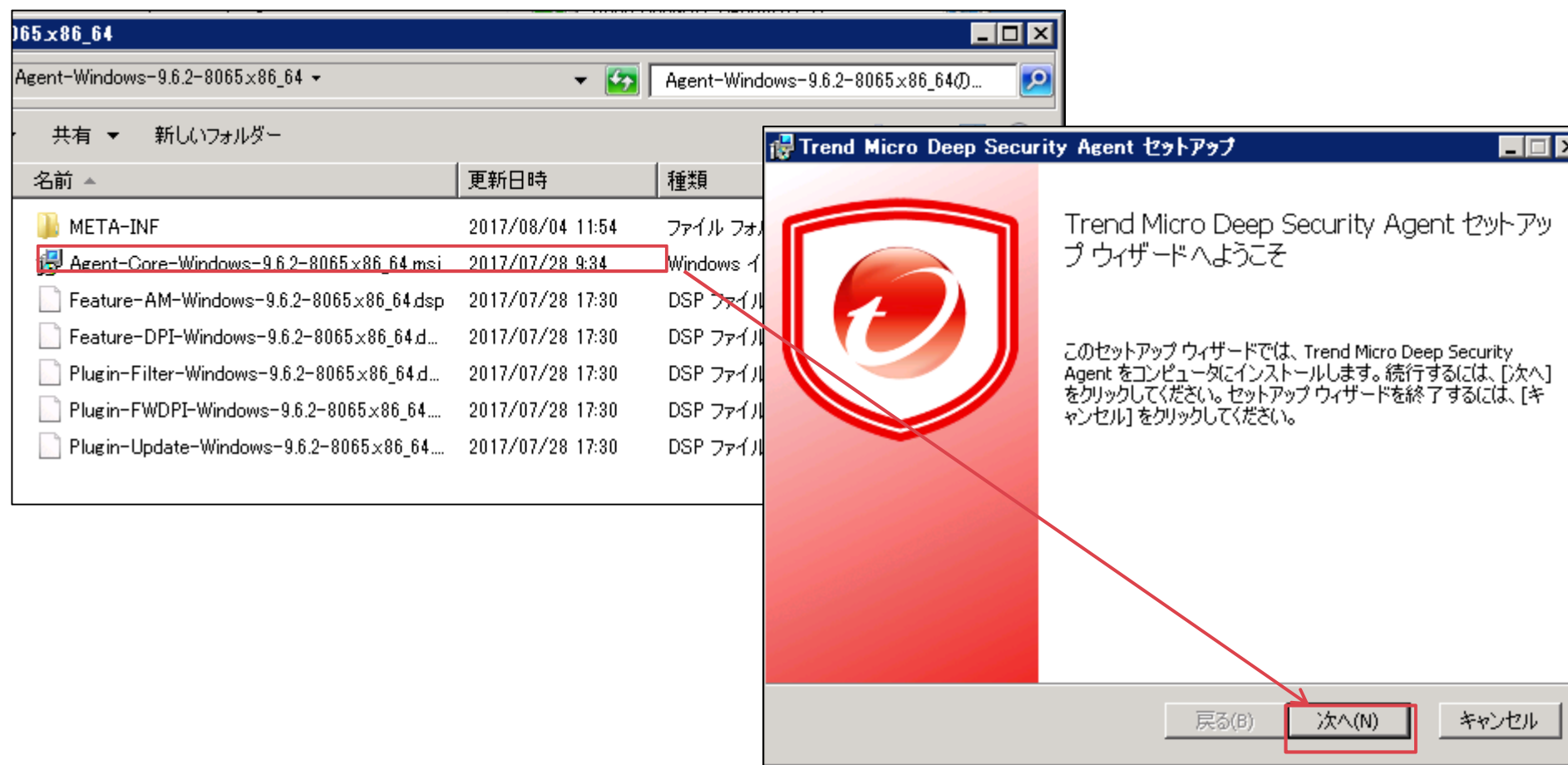
■ 事前準備したモジュールを実行します



4. インストーラ実行 (1)

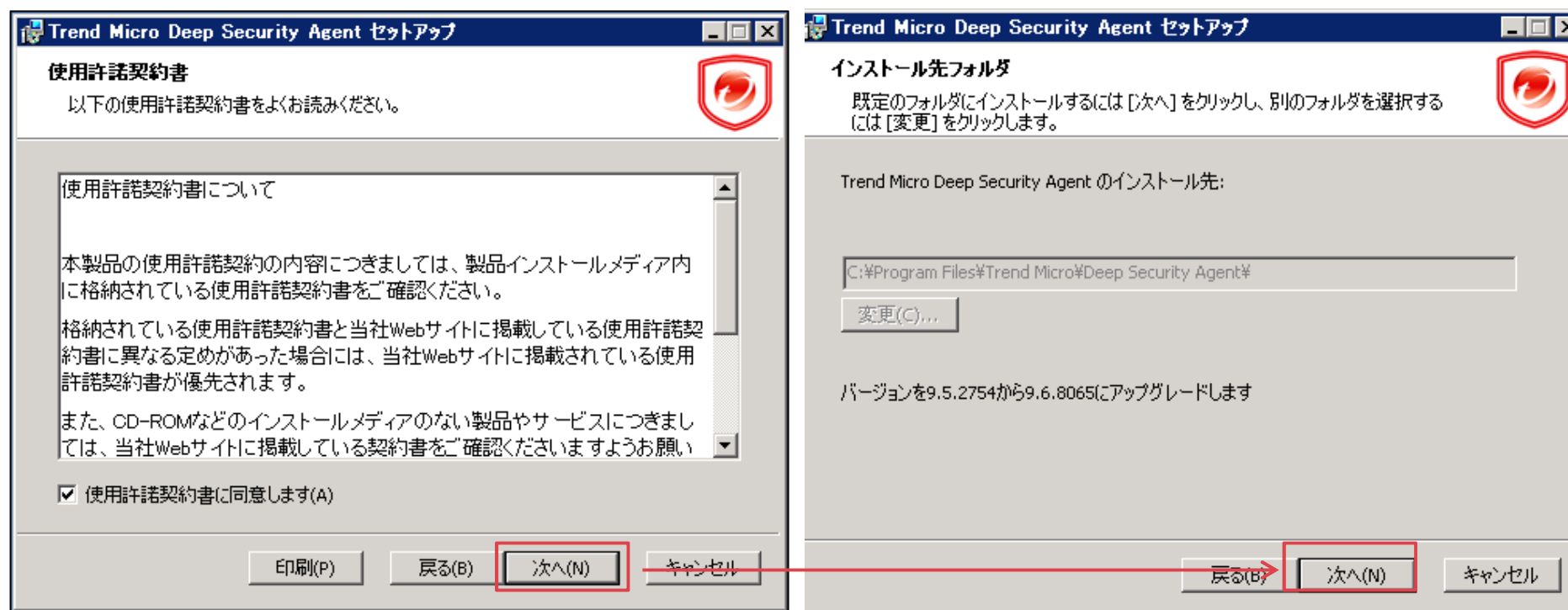
手順

- 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



4. インストーラ実行 (2)

- 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



4. インストーラ実行 (3)

- ⑤ [インストール]をクリック
- ⑥ [完了]をクリックしてインストールを完了




※インストール中にネットワークの瞬断が発生します。

5.アップグレードの確認


手順

- ① ステータスが「管理対象（オンライン）」になっていることを確認
- ② P.3のバージョンを確認頂き、「9.6.2.8065」に更新されていることを確認

ステータス	ポリシーの送信の成功	バージョン
 管理対象 (オンライン)	1 分 前	9.6.2.8065

(参考) モジュールのインストール失敗のエラーが発生した場合

- アップグレード処理時、一時的に「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」のエラーが発生することが確認されています
- 当該エラーはアップグレード処理における一時的なものですので、警告/エラーのクリアを押下し、しばらく後に状況をご確認ください

ステータス	
	 Agent
ステータス:	 複数のエラー
警告/エラー:	ソフトウェアアップデート: 侵入防御モジュールのインストール失敗 ソフトウェアアップデート: 不正プログラム対策モジュールのインストール失敗 不正プログラム対策エンジンがオフライン
不正プログラム対策:	 ソフトウェアアップデート: 不正プログラム対策モジュールのインストール失敗, 不正プログラム対策エンジンがオフ
侵入防御:	 ソフトウェアアップデート: 侵入防御モジュールのインストール失敗
オンライン:	はい
前回の通信:	2017-08-04 12:10
<div>ステータスの確認</div> <div>警告/エラーのクリア</div>	

更新履歷

[illegible]

\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