文書管理番号：SND-SEC-MI-21001-1.84

Deep Security Agent 20.0
導入手順書
(Windows)

2025 年 11 月 12 日

【第 1.84 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	2021/09/27	―	―	新規	
2	1.1	2022/03/23	特定の更新プログラムの適用が必要な OS があることを追記	1.2 動作環境	更新	
3	1.1	2022/03/23	インストーラーは管理者権限で実行する必要があることを追記	3.3 インストーラの実行	更新	
4	1.2	2022/10/13	ハートビート間隔の変更は推奨しないため「5.3 ハートビート待ちの時間が長い」の内容を削除	5.3 ハートビート待ちの時間が長い	削除	
5	1.2	2022/10/13	ハートビート間隔の記載を 10 分から現在の 30 分に修正	4.1 コマンドラインの利用	更新	
6	1.3	2023/01/17	対応 OS を更新 Windows の最小バージョン要件について追記	1.2 動作環境	更新	
7	1.4	2023/10/10	サポート期間が終了した OS の Deep Security Agent 20.0 でのサポート内容が変更されます	1.2 動作環境	更新	
8	1.4	2023/10/10	サポート対象の Web ブラウザを更新	2.3, 5.1	更新	Internet Explorer がサポート対象外になりました
9	1.5	2024/01/23	"https://success.trendmicro.com/jp/" で始まる URL を最新のものに変更	1.2, 3.6.2, 3.7.3	更新	
10	1.5	2024/01/23	以下の内容を追記 ※Deep Security Agent 20.0 未満はサポート対象外です。	1.2 動作環境	更新	
11	1.6	2024/06/25	限定サポート対象 OS の制限事項について記載	1.2 動作環境	更新	
12	1.7	2024/08/14	製品 Q&A の URL を更新	1.2, 3.6.2, 3.7.3, 4	更新	
13	1.8	2024/10/21	記載内容を修正	1.2, 3, 3.1, 4.1	更新	
14	1.81	2025/03/18	記載内容を修正	3.1 インストールパッケージのダウンロード	更新	Agent モジュールのバージョンを 20.0.1 から 20.0.x に変更しました
15	1.82	2025/04/16	他製品との同居について追記	1.2 動作環境	更新	
16	1.83	2025/09/08	システム要件の更新 サポート OS の追記	1.2 動作環境	更新	追加された OS Windows Server 2025 (LTSC, version 24H2) (64 bit)
17	1.83	2025/09/08	DSA のサポート条件について追記	3.3 インストーラの実行	更新	
18	1.84	2025/11/12	特定のビルドで発生する問題を追記	3.1 インストールパッケージの展開	更新	

目 次

1 はじめに

1.1 本資料に関して

本資料は、「Windows 環境」に「Deep Security Agent 20.0」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。

【注意事項】
※本導入作業後に再起動を求められる場合があります。事後に再起動が可能な状況での実施を推奨します。

1.2 動作環境

（1）Deep Security Agent 20.0 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	最小 RAM 2GB ※4GB 以上を推奨
ハードディスク	1GB 以上を推奨
CPU	物理サーバ：Intel Pentium デュアルコアまたは同等以上の CPU、4 コア以上を推奨 仮想マシン：4vCPU 以上を推奨
OS	Windows 7 (32- and 64-bit) Windows 7 Embedded (32-bit) Windows 8 (32- and 64-bit) Windows 8.1 (32- and 64-bit) Windows 8.1 Embedded (32-bit) Windows 10 (32- and 64-bit) Windows 10 IoT Enterprise 2019 LTSC (32- and 64-bit) Windows 10 IoT Enterprise 2021 LTSC (64-bit) Windows 10 Enterprise multi-session (64-bit) Windows 11 (64-bit) Windows Server 2008 (32- and 64-bit) Windows Server 2008 R2 (64-bit) Windows Server 2012 (64-bit) Windows Server 2012 R2 (64-bit) Windows Server 2016 (LTSC, version 1607) (64-bit) Windows Server Core (SAC, version 1709) (64-bit) Windows Server 2019 (LTSC, version 1809) (64-bit) Windows Server 2022 (LTSC, version 21H2) (64-bit) Windows Server 2025 (LTSC, version 24H2) (64-bit)

※　**下記リンク先に記載の各 OS に対応したマイクロソフト社の更新プログラムを適用してください**

Windows の最小バージョン要件に記載のセキュリティパッチが適用されていない場合、2023 年 2 月中旬以降にリリースされる ACS で署名された Deep Security Agent を適用した後、**正常に動作しません**。

2023 年 2 月以降に公開されるトレンドマイクロのサーバおよびエンドポイント製品、および関連モジュールに関する Windows の最小バージョン要件について

[参照先]：https://success.trendmicro.com/ja-JP/solution/KA-0013632

リリース日は以下の URL から確認ください

[参照先]：https://help.deepsecurity.trendmicro.com/ja-jp/software.html

※　「長期サポート（LTS)」タブには 2 世代分しか表示されないので「長期サポート（LTS)」タブに記載がない場合は「以前のバージョン」タブをご確認ください

※ 2024 年 1 月 1 日より OS ベンダーが定めるサポート終了後、原則 1 年間の通常サポートを提供した上で、「限定サポート」の提供へと移行します。詳細は以下の製品 Q&A をご参照ください。
[参照先]：https://success.trendmicro.com/ja-JP/solution/KA-0014849

※ 限定サポート対象 OS の制限事項
限定サポート対象となっているレガシーOS は、次回の改訂した新しい DSA 20.0.x から
システム要件外になります。

例)
2024 年 1 月以降にリリースされた DSA 20.0.1-xxx は、2023/12/31 時点での
限定サポート OS 上では、ご利用いただけません。(システム要件外となります。)
※誤ってアップグレードおよび新規インストールを行った場合は、不可である旨のエラー/警告
が出力されます。

現在の限定サポート対象 OS は以下の製品 Q&A をご参照ください。
[参照先]：https://success.trendmicro.com/ja-JP/solution/KA-0015528

※ 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。

※ Deep Security Agent 20.0 未満はサポート対象外です。

※ 下記の OS については、各 OS に対応したマイクロソフト社の更新プログラムを適用してください。

- Windows 7 SP1　　KB3033929 / KB4490628
- Windows Server 2008 SP2　　KB2763674 / KB4474419
- Windows Server 2008 R2 SP1　　KB3033929 / KB4490628

参考情報
コードサイニング証明書(コード署名証明書)における対応方針について
https://success.trendmicro.com/ja-JP/solution/KA-0006042

（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 Basic 認証で通信が可能（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。
- 保護対象サーバから対象 URL への通信経路に FW やロードバランサなどの通信機器が存在する場合は、SSL を含む送信、受信が共に可能な設定となっていることをご確認ください。
- 「仮想パッチ&アンチウイルスライセンス」のライセンスをご利用で、機械学習型検索をご利用の場合は以下 URL の「Smart Protection Network -Global Census サービス」「Smart Protection Network - Good File Reputation サービス」「Smart Protection Network -機械学習型検索」の項目に記載の URL にアクセスできる必要があります。(https://help.deepsecurity.trendmicro.com/20_0/on-premise/ja-jp/communication-ports-urls-ip.html)

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 ソフトウェアアップデート	
iaus.trendmicro.com:443	セキュリティアップデート	Trend Micro 社 Active Update サーバ。 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		
ipv6-iaus.trendmicro.com:443		
ipv6-iaus.activeupdate.trendmicro.com:443		

（3）他製品との同居について

他ウイルス対策製品との同居は不可、あるいは、制限があります。「ウイルス対策」が必要な場合は「**仮想パッチ＆アンチウイルス**」を選定ください。

◆ 他社製品との同居について

Deep Security では他社製品との競合テストなどを含めた動作テストは行っていないため、個別のソフトウェアとの共存については、導入前にお客様ご自身で十分な動作確認を行っていただきますようお願いいたします。

◆ 他の Trend 製品との同居について

DSA 20.0 以降では、有効化する機能にかかわらず同居はサポートしておりません。

[ご参考]：トレンドマイクロ製品・他社製品と共存した場合の動作について

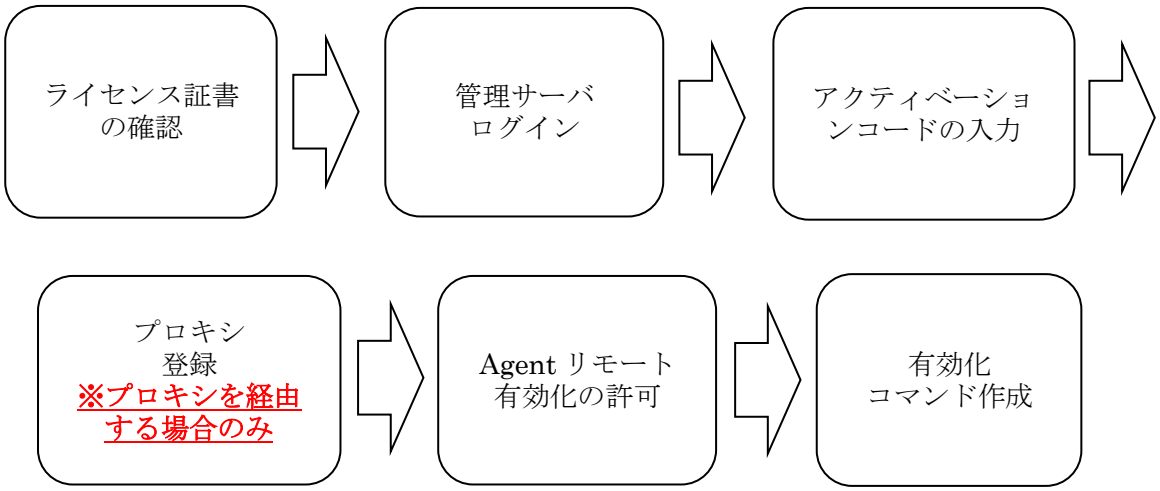
https://success.trendmicro.com/ja-JP/solution/KA-0001417

2 事前準備

2.1 事前準備

【注意事項】
・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。

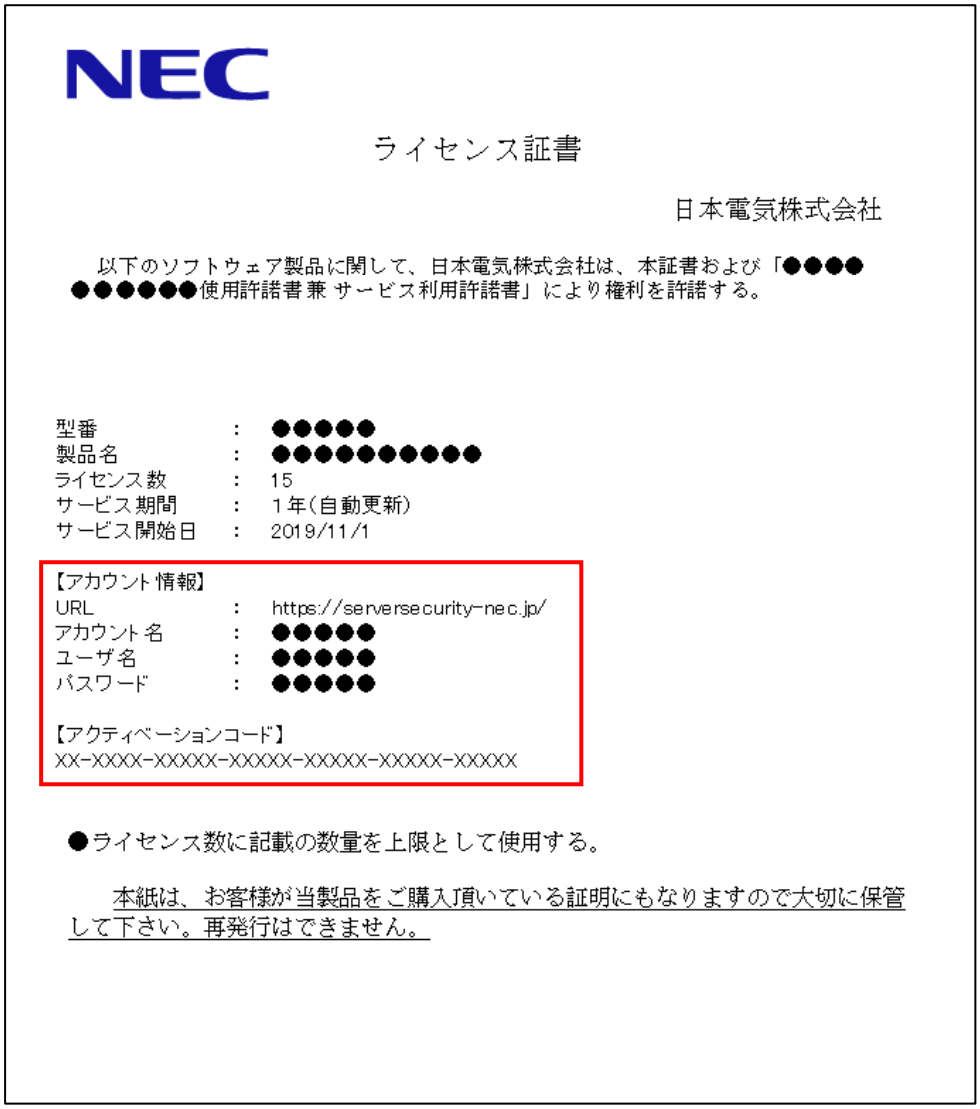
Agent 導入前に管理コンソール上で、ライセンスの確認やアクティベーション、プロキシの設定など Agent インストールの事前準備を行います。



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「●●●●●●●●●●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　：　●●●●●
製品名　：　●●●●●●●●●●
ライセンス数　：　15
サービス期間　：　1年(自動更新)
サービス開始日　：　2019/11/1

【アカウント情報】
URL　：　https://serversecurity-nec.jp/
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

●ライセンス数に記載の数量を上限として使用する。

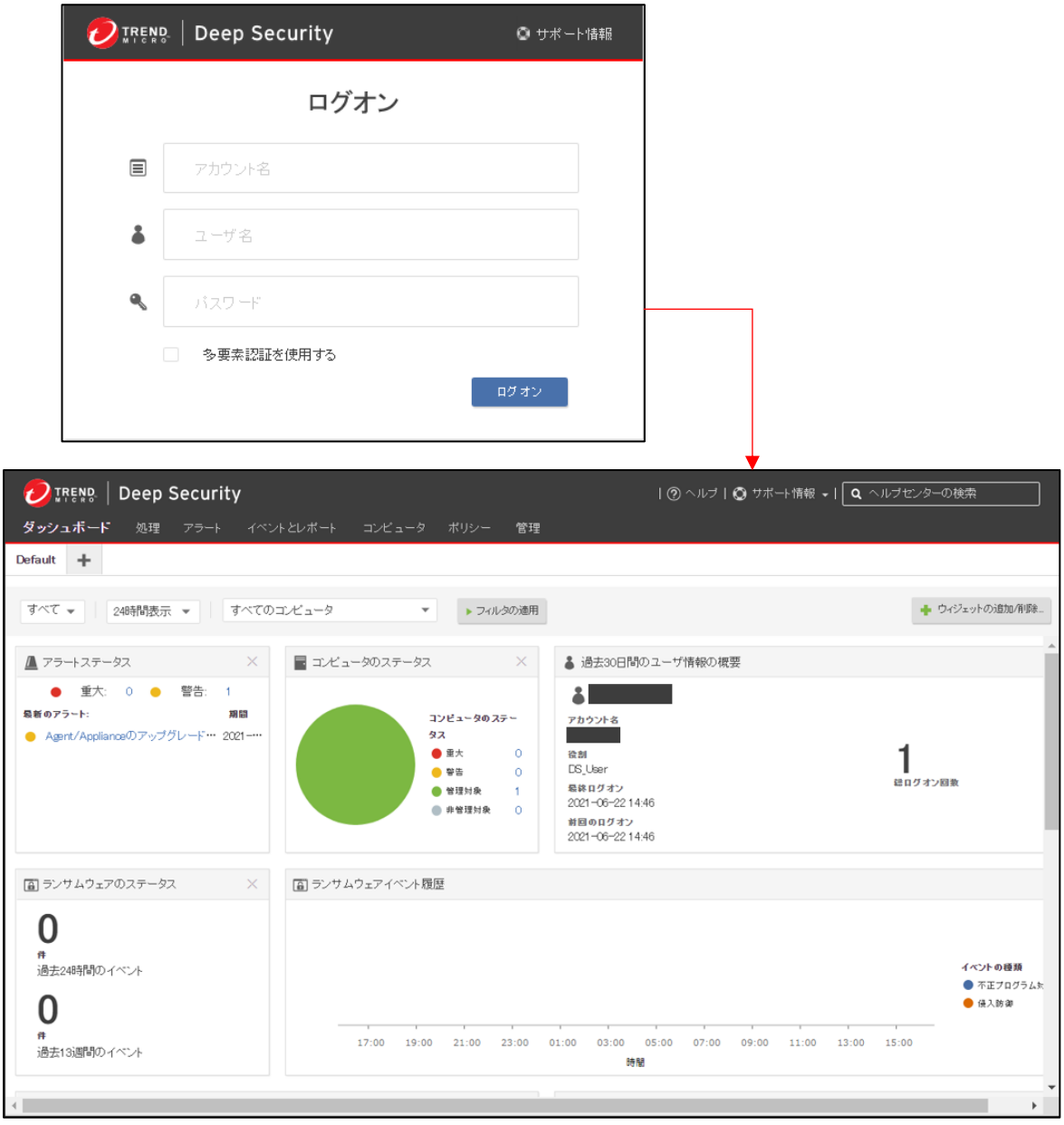
本紙は、お客様が当製品をご購入頂いている証明にもなりますので大切に保管して下さい。再発行はできません。

2.3 管理サーバログイン

【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)
・Microsoft Edge (Cookie を有効にする)
・Google Chrome (Cookie を有効にする)
・Safari (Cookie を有効にする)

（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

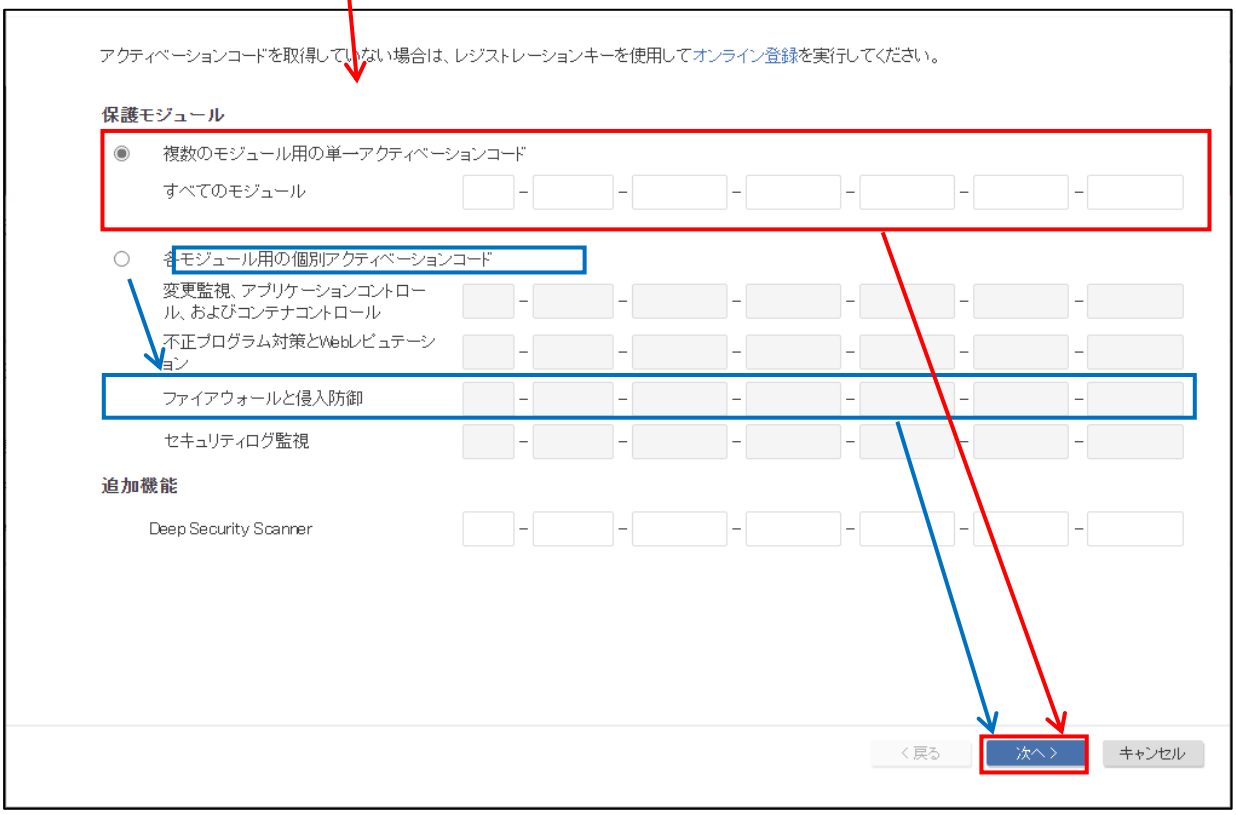
【注意事項】
複数のアカウントをお持ちの場合、誤って違うアカウントのアクティベーションコードを設定すると正しいアクティベーションコードを再設定することができなくなる場合があります。
対処としては、アカウントの再作成となりますので、入力誤りのないようご注意ください。

(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し、[次へ]をクリック

(3) ライセンス内容を確認し、[完了]をクリック

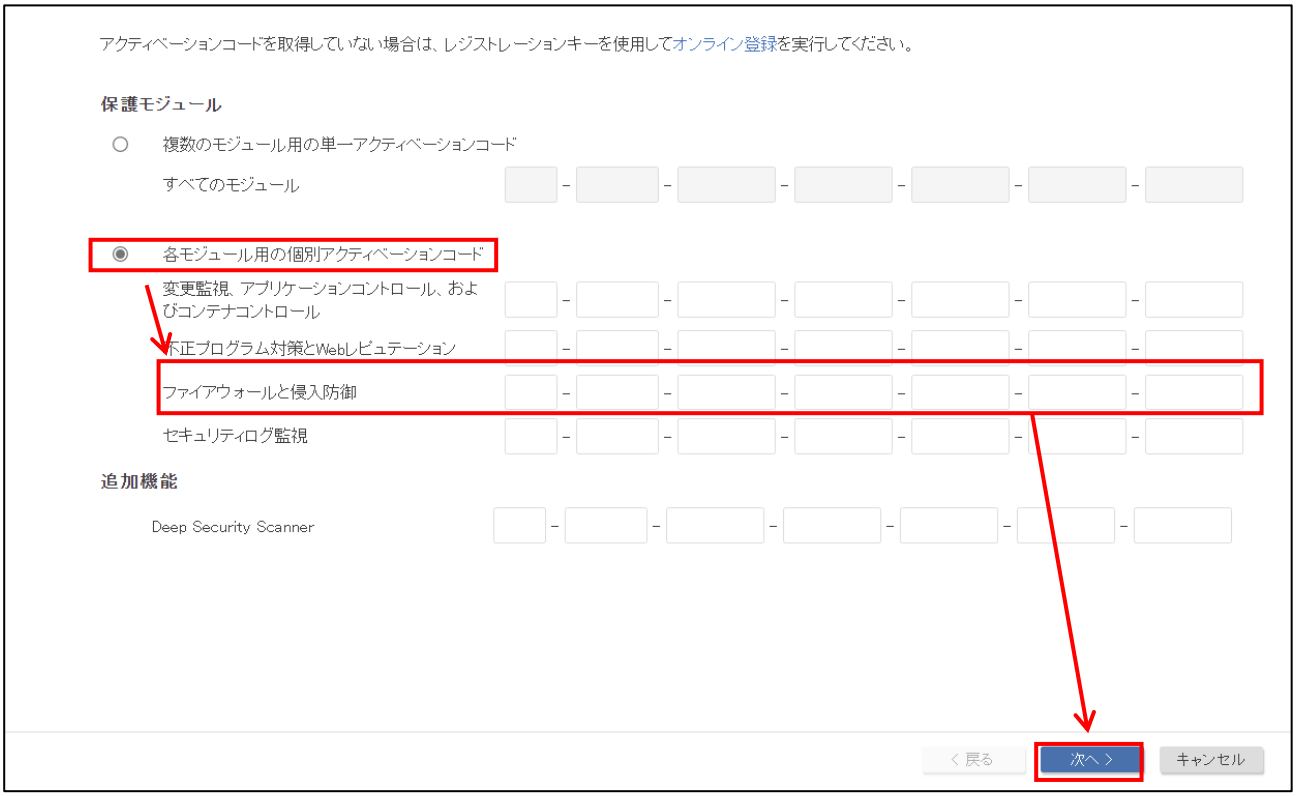
(4) アクティベーションが正常に適用した旨のメッセージ画面で[閉じる]をクリックし、ライセンス画面で内容を確認



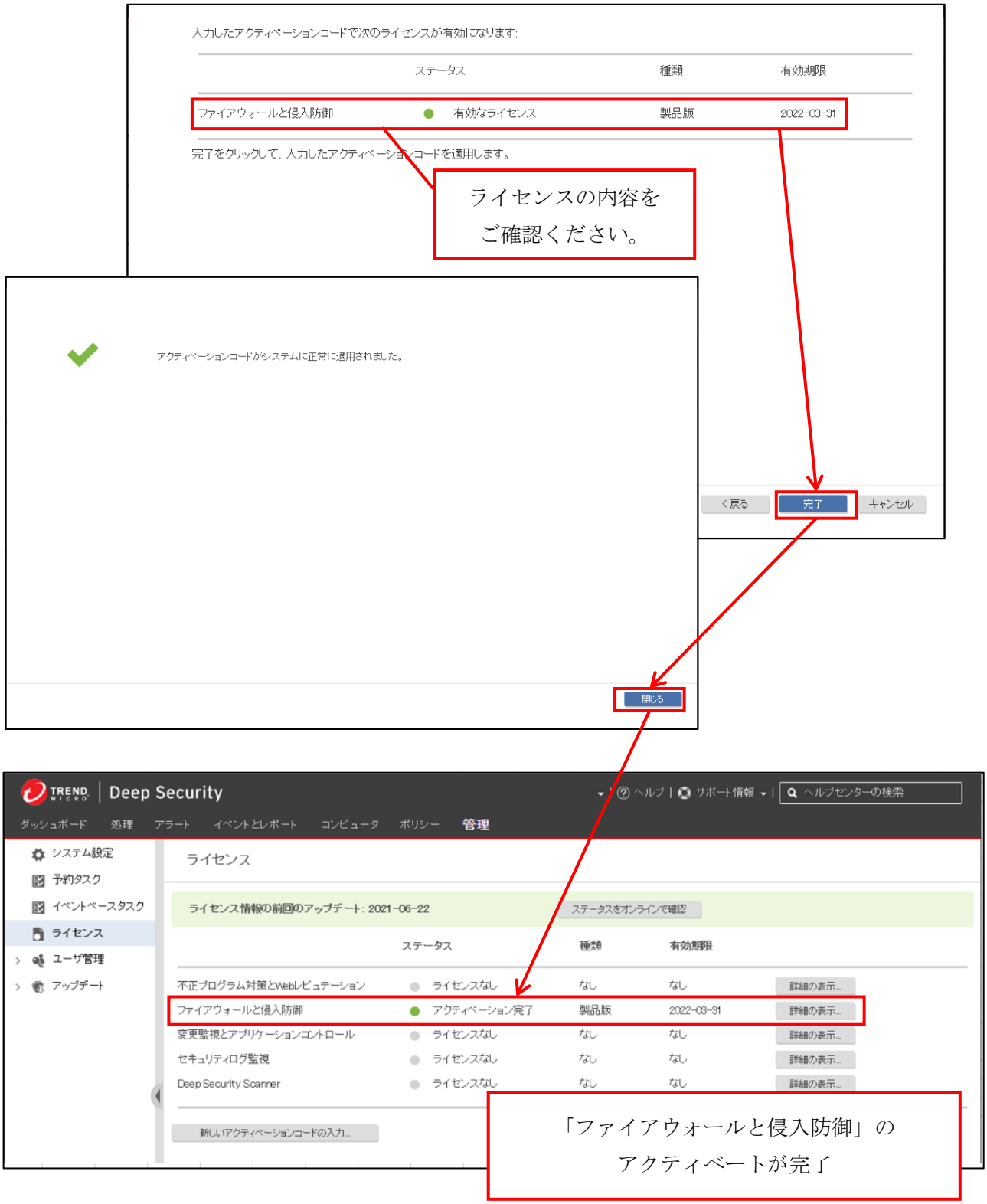
(5) 「仮想パッチ（侵入防御）ライセンス」の場合

【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）アクティベーションコードを以下の箇所に入力し、[次へ]をクリック



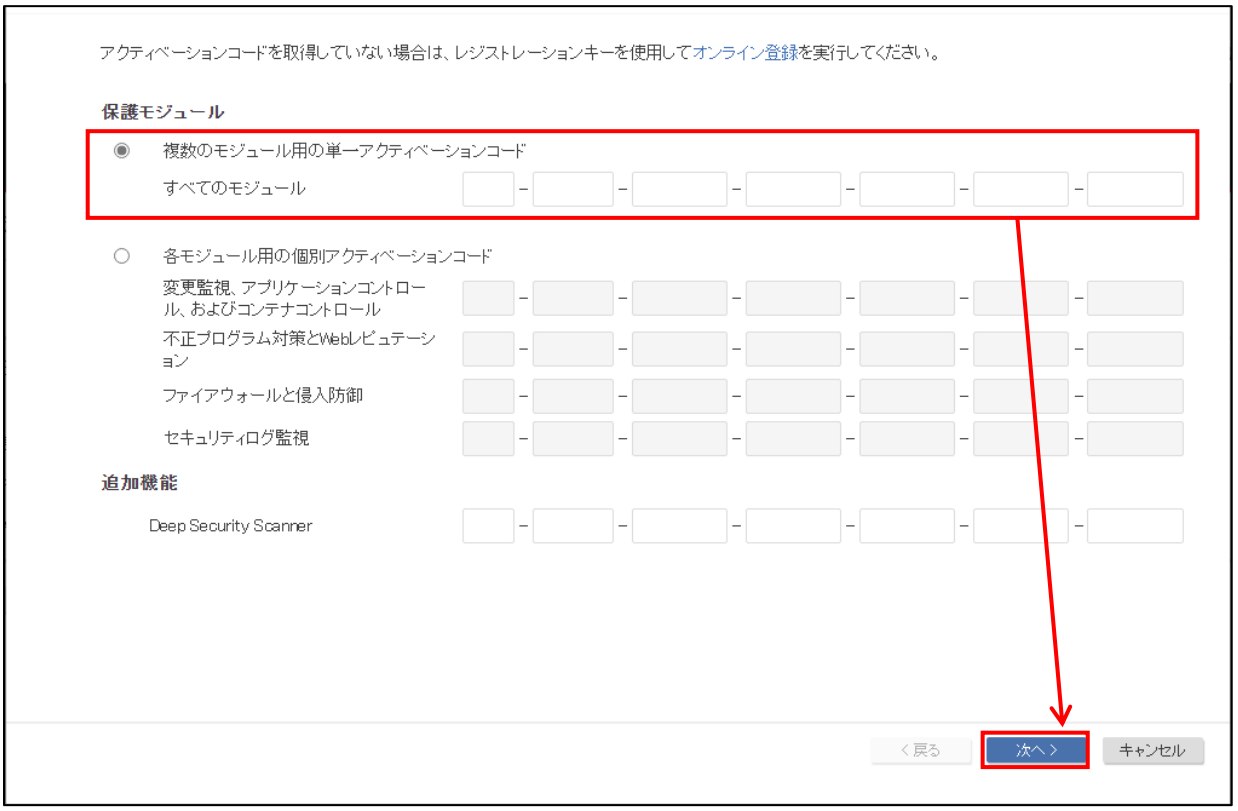
（B）以下の手順で、アクティベートを完了させて、有効なライセンスを確認



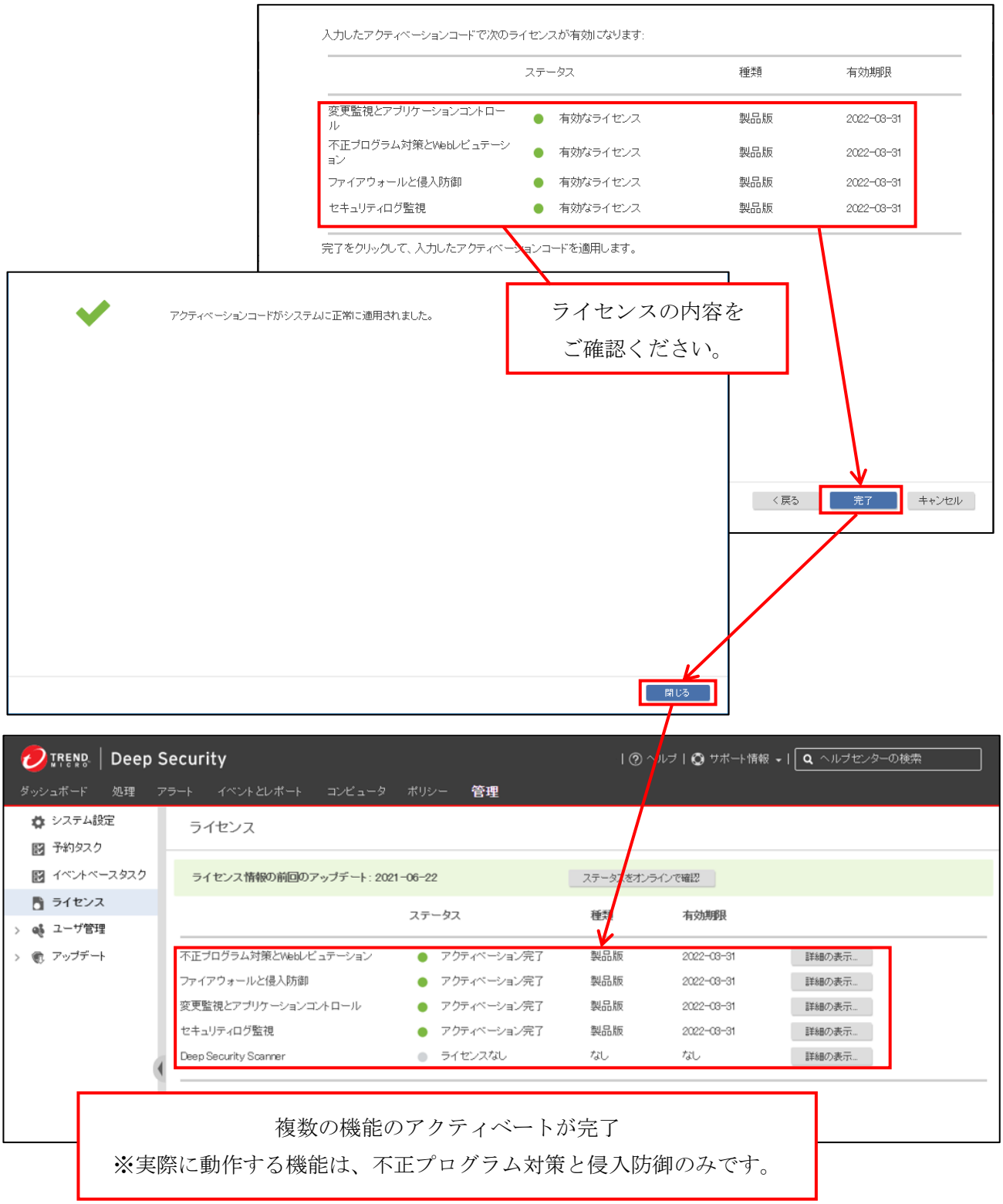
(6) 「仮想パッチ&アンチウイルスライセンス」の場合

【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) アクティベーションコードを以下の箇所に入力し、[次へ]をクリック



（B）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



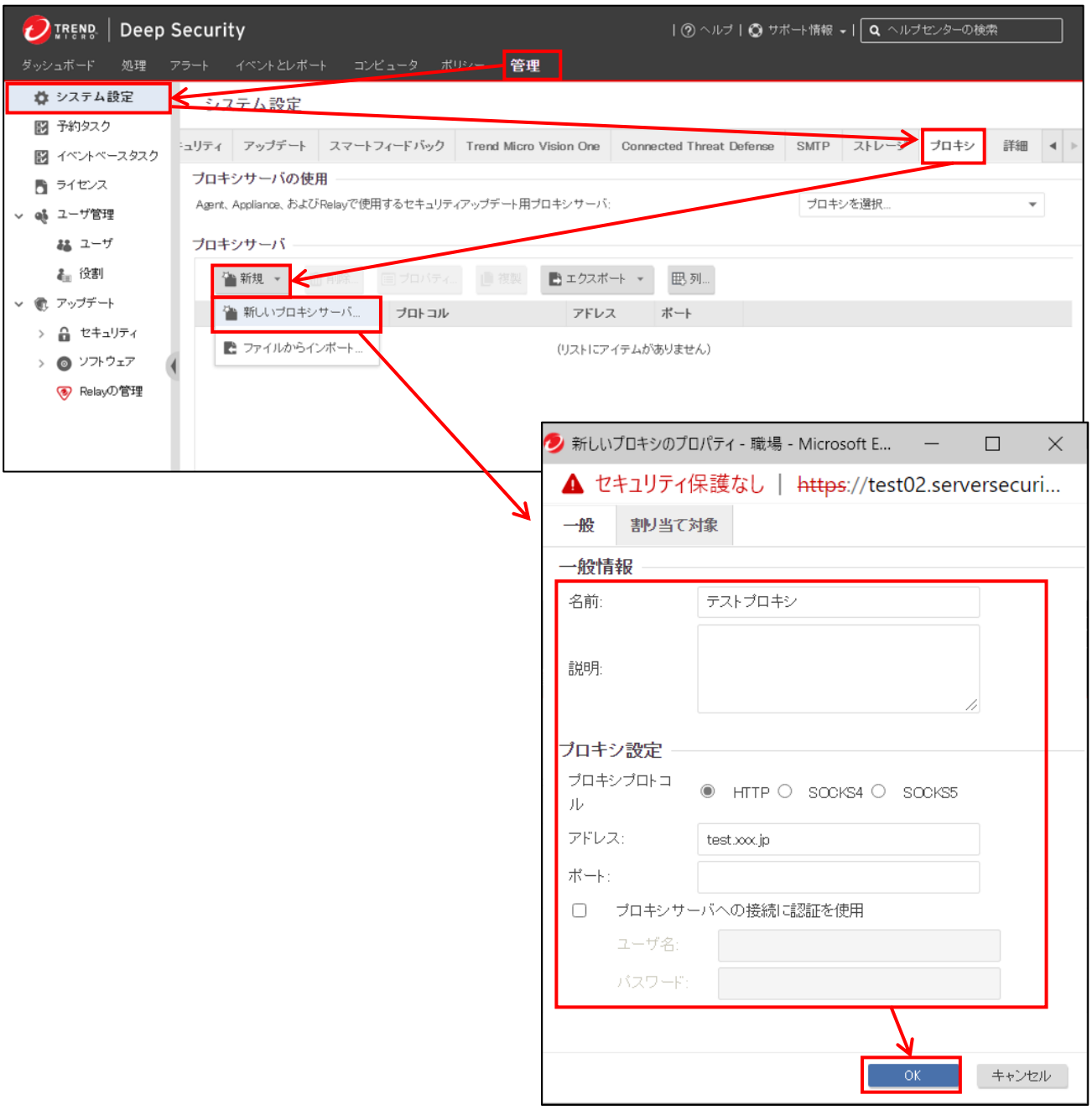
2.5 プロキシ登録

【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] > [システム設定] > [プロキシ] > [新規] > [新しいプロキシサーバ...] を選択

（2）任意の一般情報、プロキシ設定を入力

（3） [OK]ボタンをクリックしプロキシ情報を登録



2.6 Agent リモート有効化の許可

（1） [管理] > [システム設定] > [Agent]を選択

（2）[Agent からのリモート有効化を許可]にチェック

（3）[任意のコンピュータ]を選択し、[保存]をクリック

2.7 有効化コマンドの作成

（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必ず有効化してください)]にチェック
※以下(4)～(7)はこのチェックを入れると出現する項目

(4) [セキュリティポリシー]は[サーバセキュリティサービス_ポリシー]を選択
[サーバセキュリティサービス_ポリシー]を選択することにより、以下の設定になります。

(A) [Deep Security Manager と Agent/Appliance の通信方向]が[Agent/Appliance 開始]となります。※この設定は変更不可

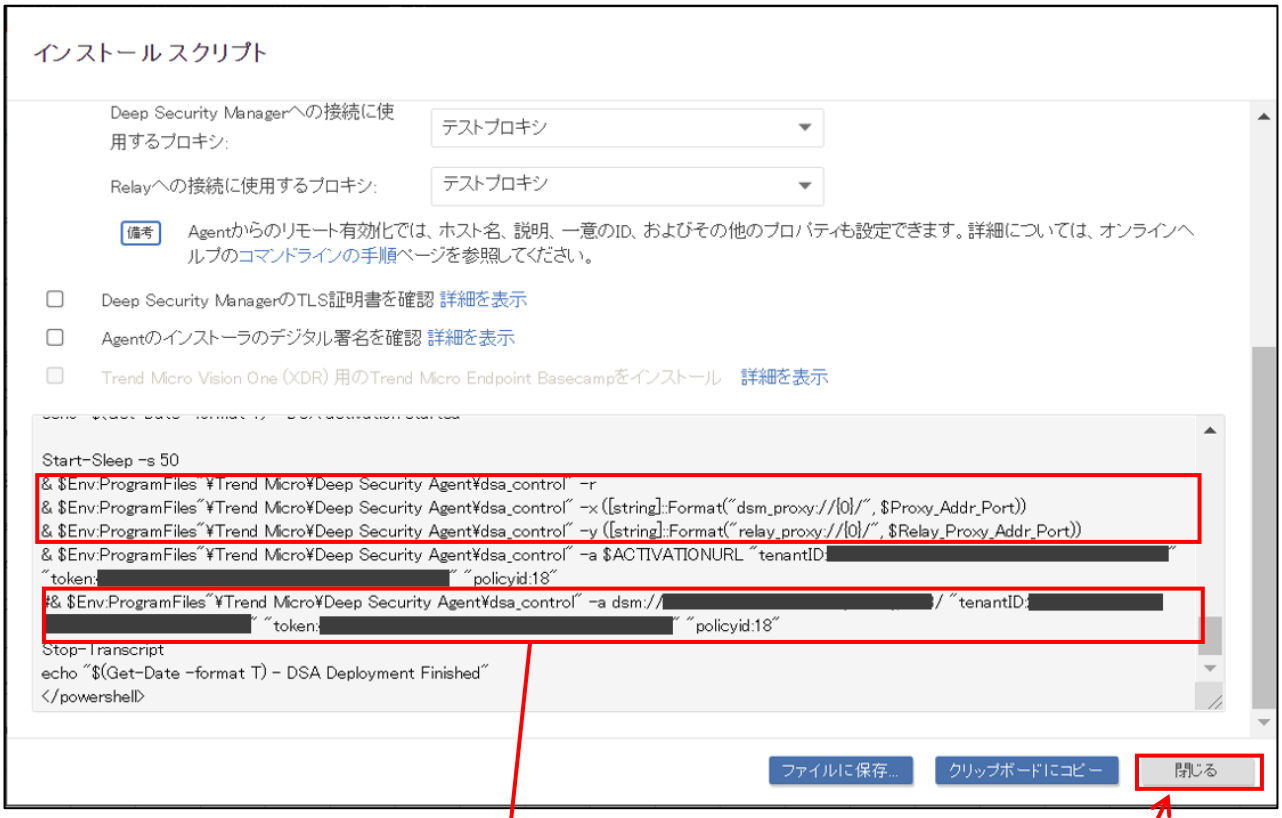
(B) [侵入防御の推奨設定を自動的に適用（可能な場合)]が[はい]になります。
こちらはお客様の運用により変更可能です。
例：検索のみ実施し、適用は手動で行う等。

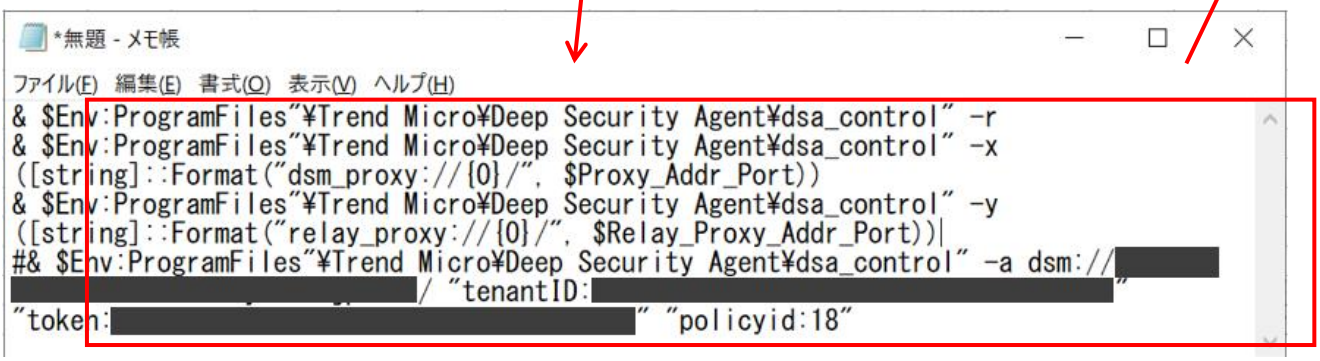
(5) [コンピュータグループ]を選択 ※後ほど作成、グループ分けすることも可能

(6) [Relay グループ]で、[プライマリテナントの Relay グループ]を選択

(7) （プロキシをご利用の場合）「2.5 プロキシ登録」で作成したプロキシを選択

(8) 「& $Env:ProgramFiles“¥Trend Micro¥Deep Security Agent¥dsa_control” -r」から「& $Env:ProgramFiles"¥Trend Micro¥Deep Security Agent¥dsa_control" -y ([string]::Format("relay_proxy://{0}/", $Relay_Proxy_Addr_Port))」までと「#& $Env:ProgramFiles“¥Trend Micro¥Deep Security Agent¥dsa_control” -a dsm://<ホスト名>:<ポート>/ “tenantID:<英数字文字列>” “token:<英数字文字列>” “policyid:<数字>”」をコピーし、テキストエディタ等に貼り付け、[閉じる]をクリック





（9）最後の行の行頭の「#」を削除

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

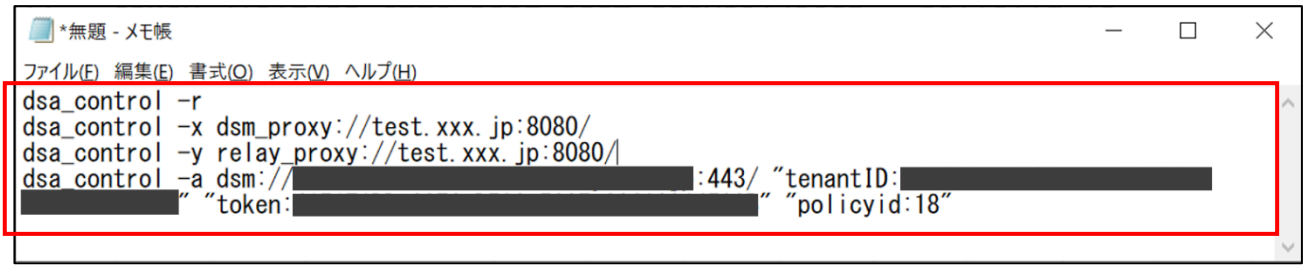
（11）すべての行で「dsa_control “」の「“」を削除

（12）（プロキシをご利用の場合）

” dsa_control -x ([string]::Format("dsm_proxy://{0}/", $Proxy_Addr_Port))”

“dsa_control -y ([string]::Format("relay_proxy://{0}/", $Relay_Proxy_Addr_Port)) “

上記を以下を参考に書き換える



プロキシで認証（Basic 認証のみ対応）を行う場合、
【Deep Security Manager への接続に使用するプロキシ】
「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

【Deep Security Relay への接続に使用するプロキシ】
「dsa_control -y relay_proxy://*プロキシサーバの URL:ポート*」行の次行に、

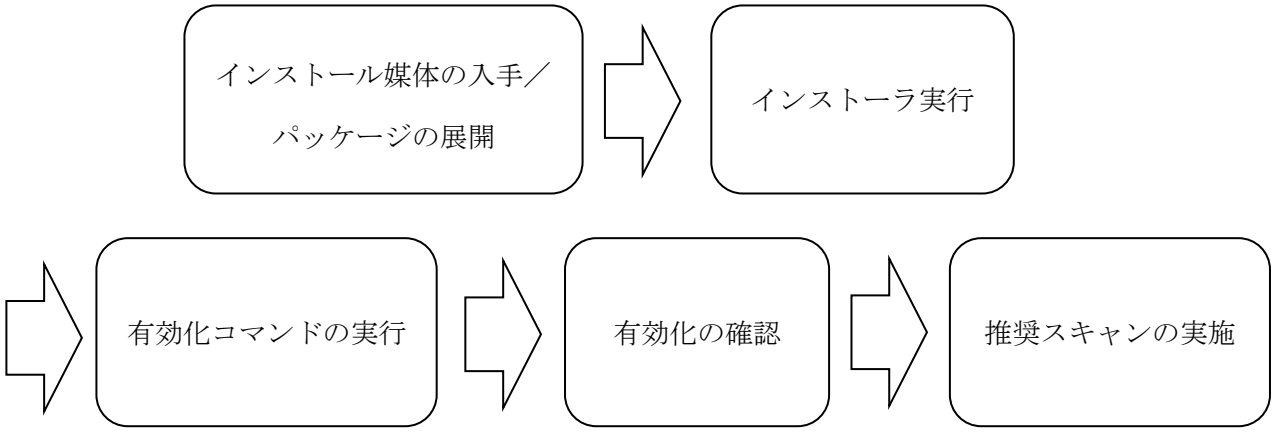
「dsa_control -w *ユーザ名:パスワード*」

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 -w root:Password

3 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。



3.1 インストールパッケージのダウンロード

(1) 管理コンソールにログイン

(2) [管理] > [アップデート] > [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) 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”から始まる最新バージョンのもの）を選択

※ 下記 x の値が最も大きいものが最新バージョンです。

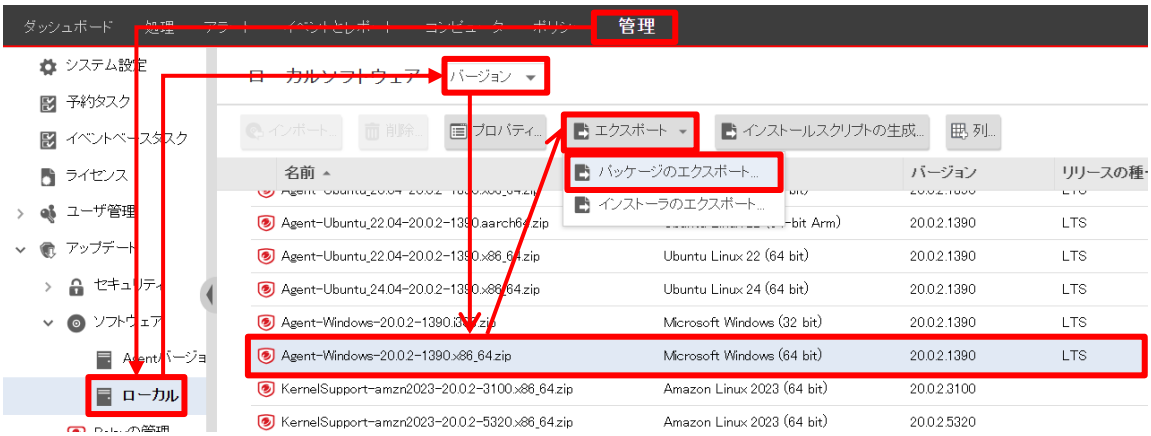
20.0.x-xxxx

※ 任意のビルドを選択される場合であっても、下記ビルドの Agent は他のビルドへのアップグレード時に失敗する可能性がありますので利用しないでください。

- 20.0.0-5995
- 20.0.0-6313
- 20.0.0-6690
- 20.0.0-6860

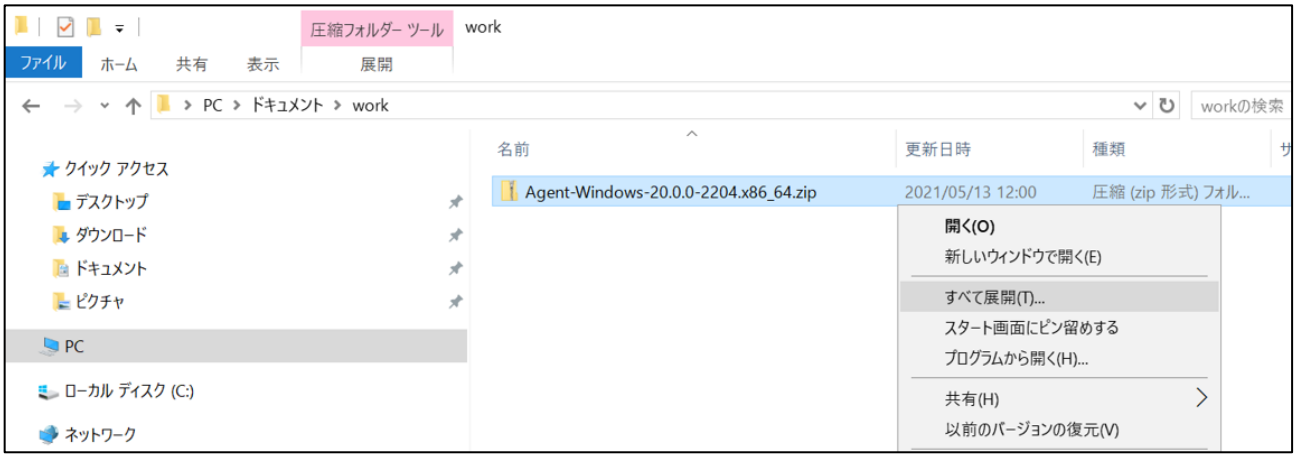
[参照先]：https://success.trendmicro.com/en-US/solution/KA-0014615

(5) [エクスポート] > [パッケージのエクスポート]を選択し、媒体をダウンロード



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インストールするホストの任意の場所に配置
任意の方法で展開
※下記キャプチャは一例です



3.3 インストーラの実行

(1) 解凍したフォルダ内の msi ファイルをダブルクリックしてインストーラパッケージを実行します。

※Windows Server 2012 R2 Server Core の場合は、次のコマンドを使用してインストーラを起動する。

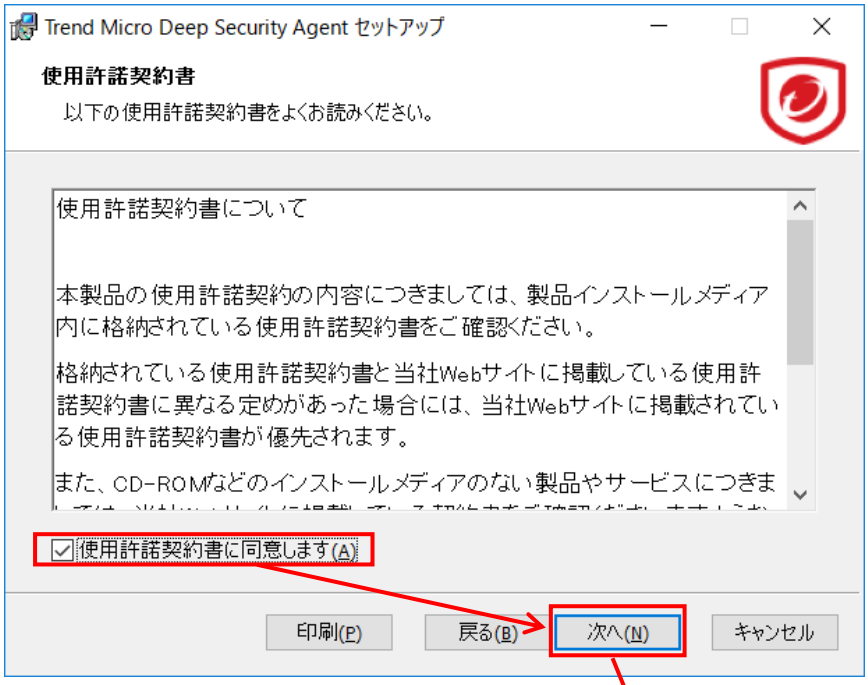
（例）msiexec / i Agent-Core-Windows-20.x-xxxx.x86_64.msi

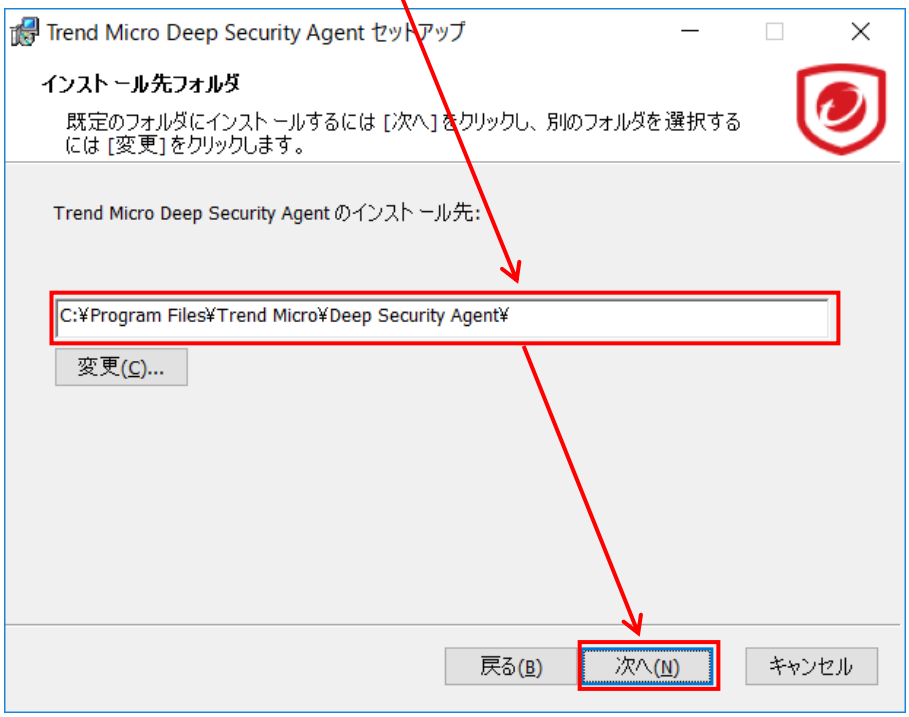
※インストーラの実行には管理者権限が必要です。

(2) 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

(3) インストール先フォルダを確認し、[次へ] をクリック

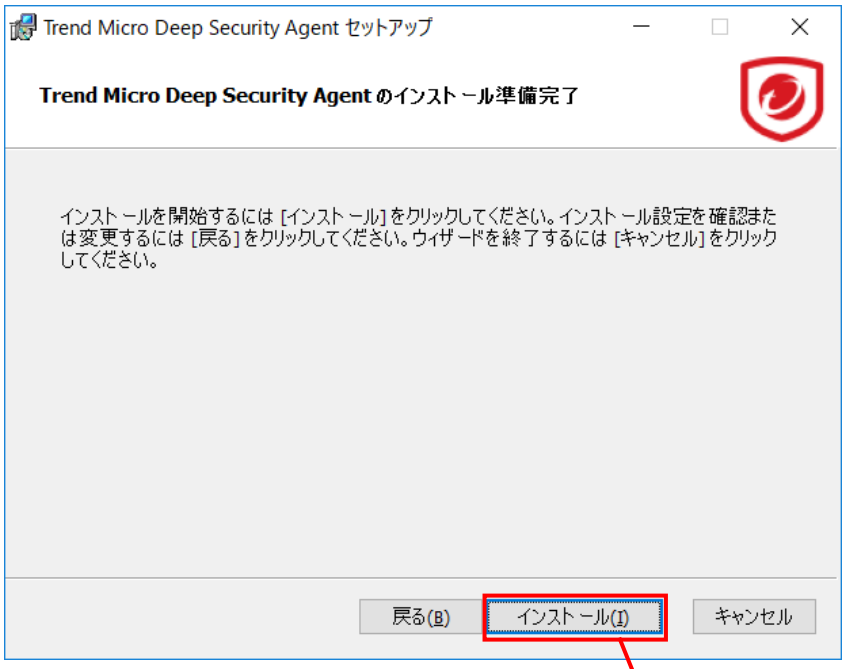
※インストールパスのドライブがシステムドライブ以外の場合サポート対象外となります。

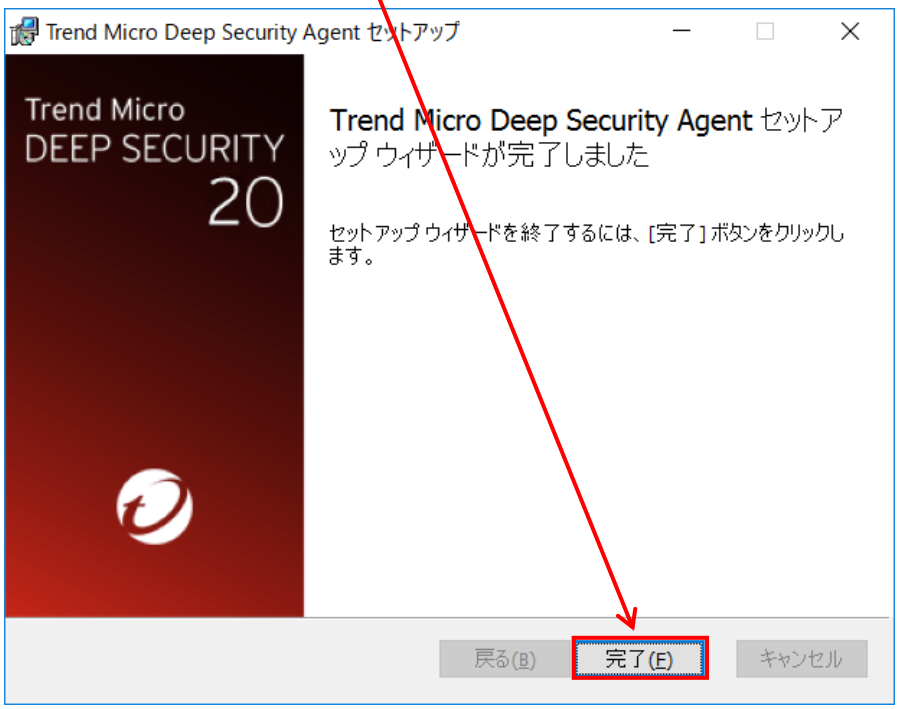




(4) [インストール]をクリック

(5) [完了]をクリックしてインストールを完了



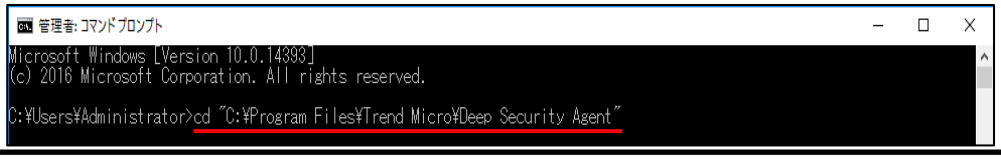


3.4 有効化コマンドの実行

（1）Agent をインストールしたホストで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

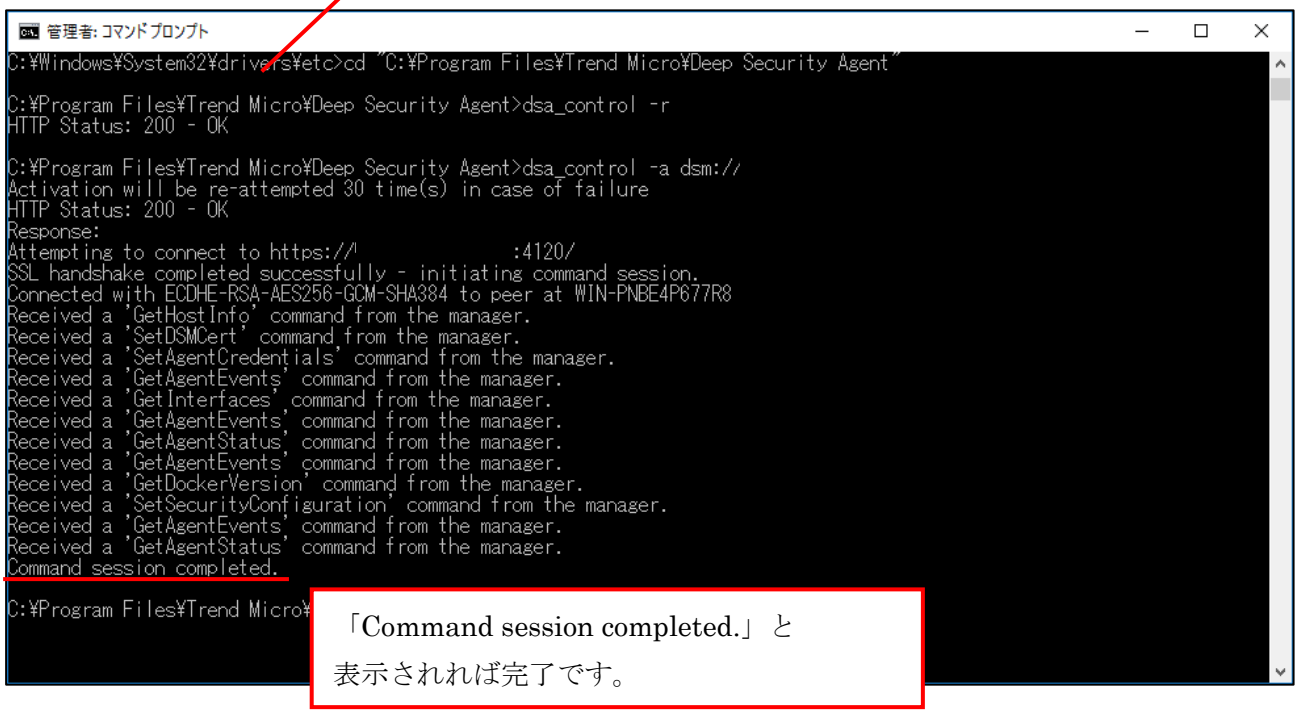
【参考】
デフォルト設定の場合は、下記のフォルダ移動コマンドを入力ください。
cd "C:¥Program Files¥Trend Micro¥Deep Security Agent"



（3）フォルダ移動後、「2.7 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]を押下します。

（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 -r
dsa_control -a dsm://hb.serversecurity-nec.jp:443/ "tenantID:xxxx" "token:xxxx" "policyid:xx" "relaygroupid:1"



「Command session completed.」と
表示されれば完了です。

3.5 有効化の確認

(1) [コンピュータ]タブより、対象サーバ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。
おおよそ 5～10 分程度かかります。あくまで目安であり環境により違いがあります。

(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

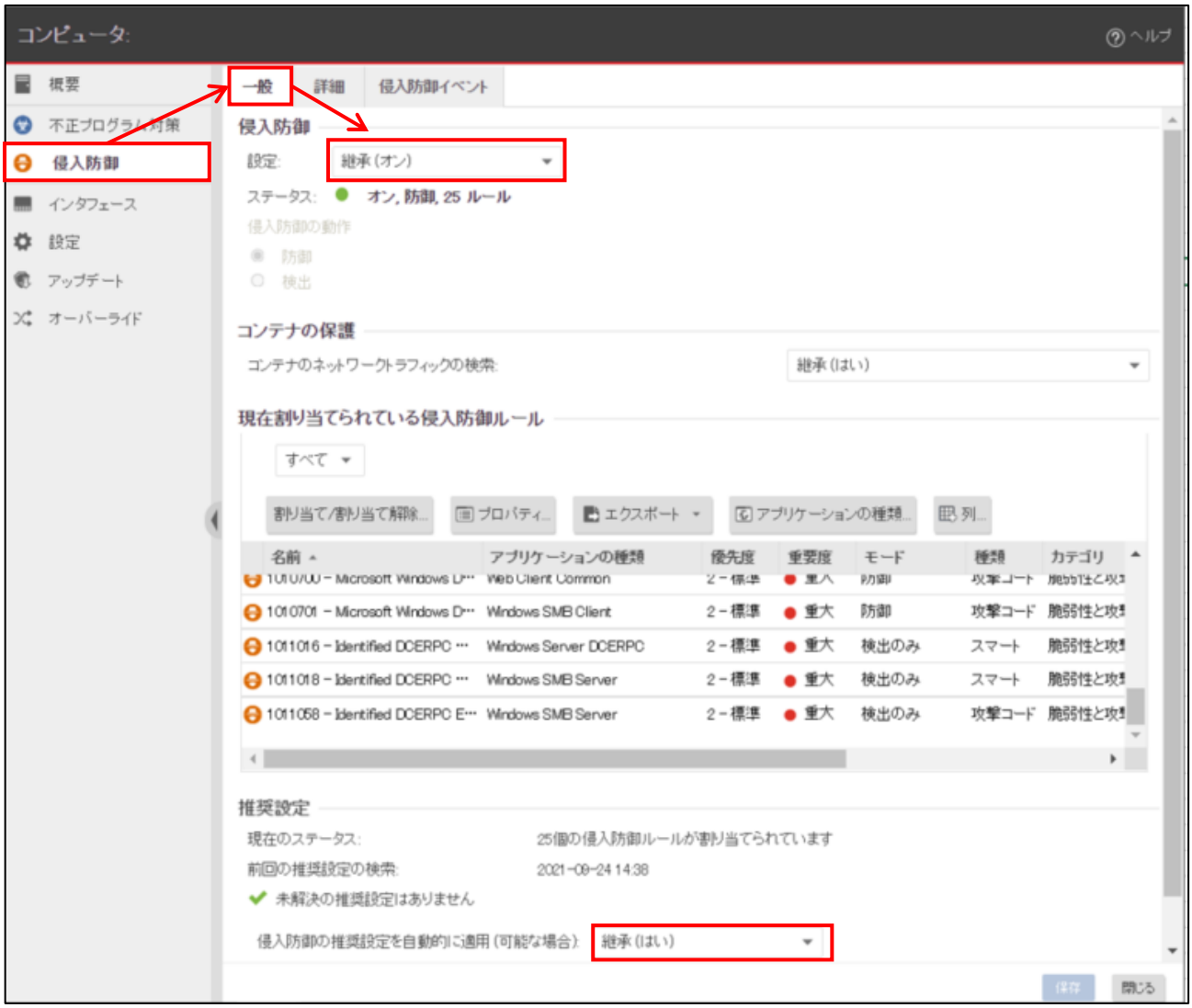
3.6 推奨スキャンの実施

3.6.1 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）対象サーバをダブルクリックし、[侵入防御] > [一般]タブを選択

（2）侵入防御の[設定]が[オン]または[継承（オン）]、推奨設定の[侵入防御の推奨設定を自動的に適用（可能な場合）]が[はい]または[継承（はい）]になっていることを確認



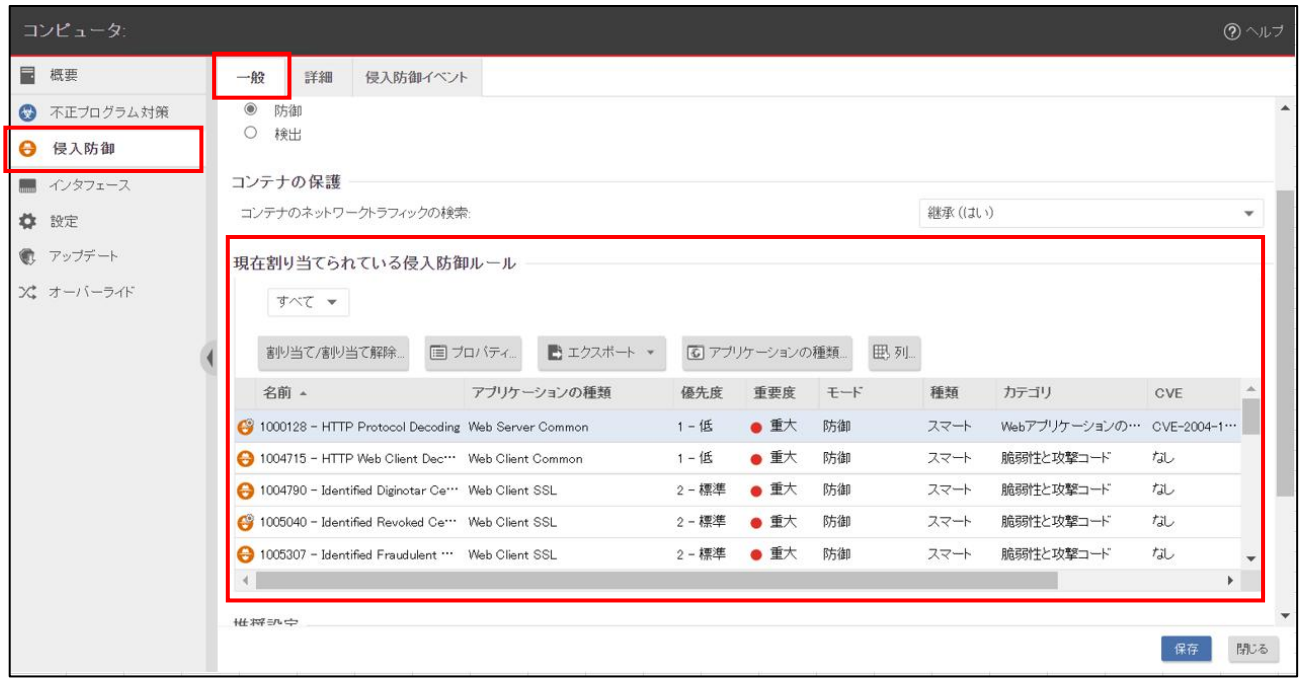
(3) [コンピュータ]タブより、対象サーバを右クリック

(4) [処理] > [推奨設定の検索] をクリック

(5) 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

(6) 推奨スキャン実施後、対象サーバをダブルクリックし、[侵入防御] > [一般]タブを選択

(7) [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



3.6.2 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) [コンピュータ]タブより、対象サーバをダブルクリックし、[侵入防御] > [一般]タブの[割り当て/割り当て解除…]をクリック

(2) 侵入防御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は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はチェックを外し、[OK]ボタンをクリック

3.7 補足

3.7.1 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）対象サーバをダブルクリックし、[概要] > [一般]から[警告/エラーのクリア]をクリック

（2）不正プログラム対策、侵入防御が「オン,XXXXX」になっている事を確認する。

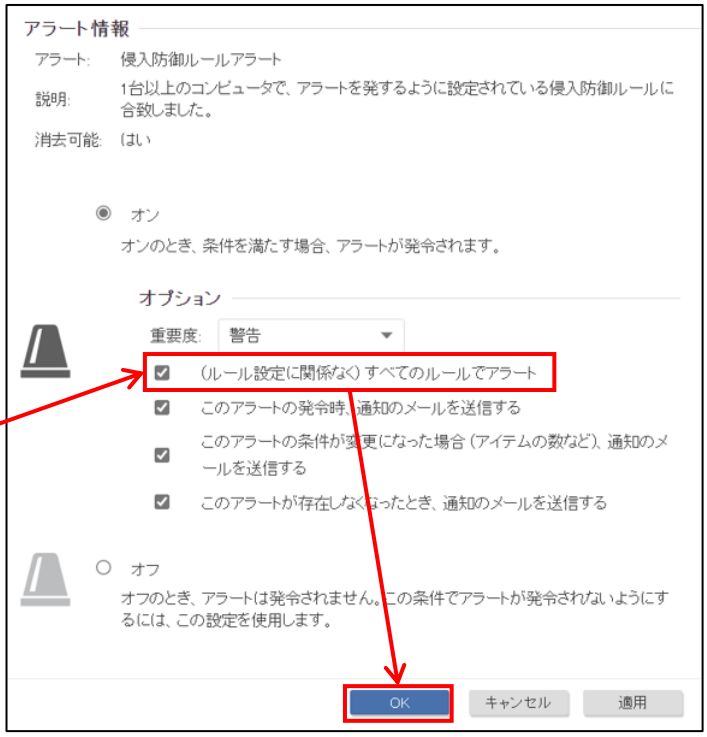
3.7.2 補足（２）検知した侵入防御イベントをアラートメールで送信する方法

【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]ボタンをクリック



3.7.3 補足（３）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
（https://success.trendmicro.com/ja-JP/solution/KA-0007590）

4 参考情報

各機能の詳細については、管理コンソールの[ヘルプセンターの検索]にキーワードを入力し検索することでご確認いただけます。

また、下記の製品 Q&A サイトもあわせてご利用ください。

<https://success.trendmicro.com/ja-JP/>

4.1 コマンドラインの利用

本項では、Deep Security Agent 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直ちに送り、通信を確立する

※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。

※ハートビート間隔は変更しないでください。

（2）Agent の無効化

dsa_control -r　：Agent を無効化

※既に設定済みのプロキシの設定は初期化されません。

（3）プロキシの初期化

dsa_control -x ””　：プロキシを初期化

その他のコマンドや詳細につきましては、管理コンソール右上の[ヘルプセンターの検索] に”コマンドラインの基本”と入力し表示されたクエリから[コマンドラインの基本]をご参照ください。

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 (Cookie を有効にする)
- Microsoft Edge (Cookie を有効にする)
- Google Chrome (Cookie を有効にする)
- Safari (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

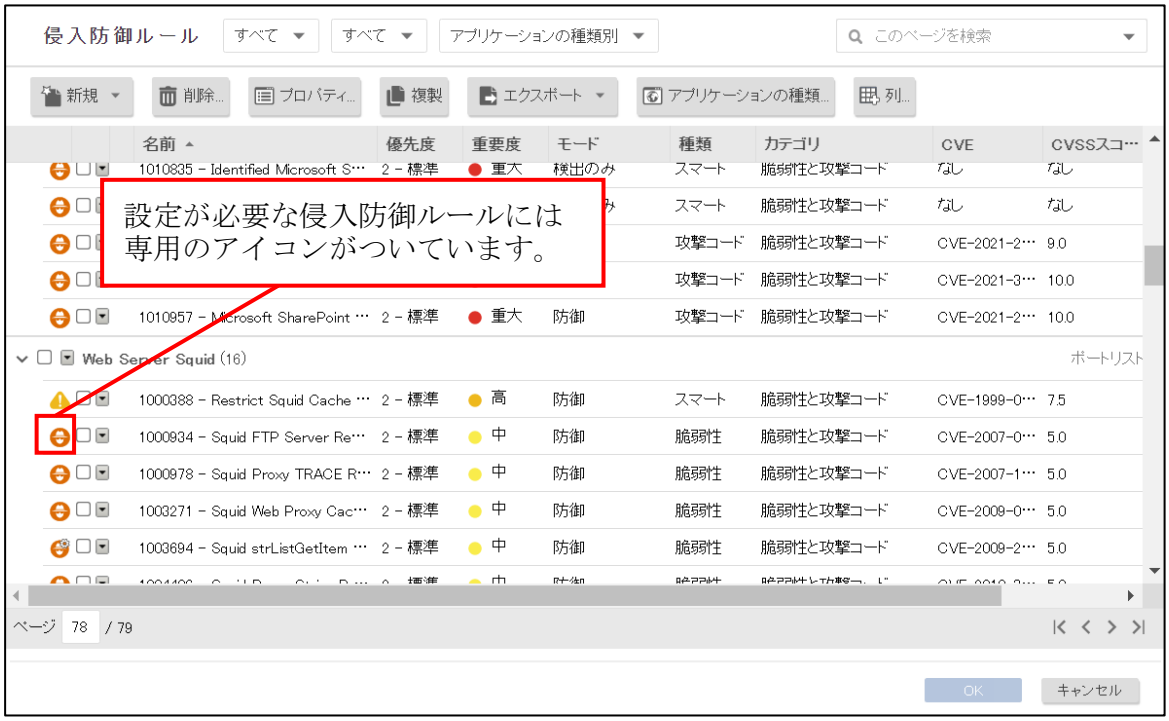
コマンド実行文の「HTTP Status」が 400 番台の場合、管理サーバ-Agent 間の通信に問題がある可能性があります。以下の例をご参照の上、対策が必要になります。

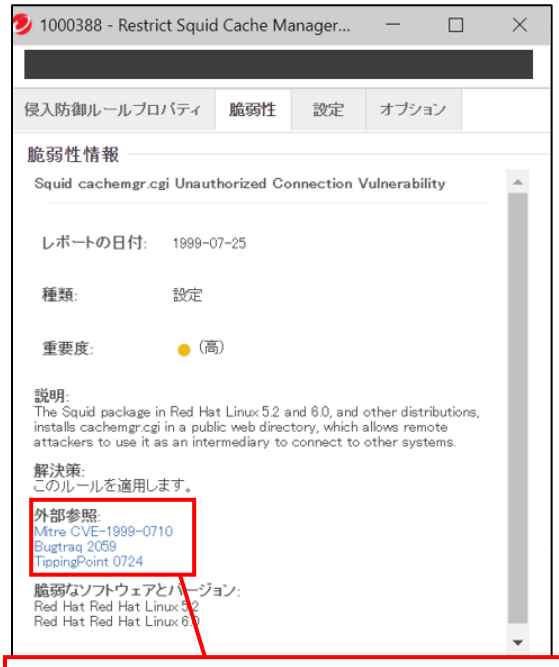
(例)

Code	状態	想定される原因とその対策
400	Bad Request	「2.5 プロキシ登録」で登録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ください。
407	Proxy Authentication Required	プロキシ認証が必要です。「2.5 プロキシ登録」を参考にユーザ名とパスワードを設定してください。
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。

5.3 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。





[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ください。

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。