リコージャパン株式会社

クラウドサービス　ｆｏｒ　サーバーセキュリティ

導入手順書

3.0 版

2022/01/17

※　本ソフトウェアの導入時に、OS 上のネットワークドライバの導入が行われる為、ネットワークの瞬断が発生する場合があります。導入作業前の注意事項としてお伝えください。

※　画面表示は 2015 年 8 月時点の画面であり、本手順書の画面と実機が異なる場合があります。

※　ログオン手順の画面表示は 2022 年 1 月時点の画面であり、本手順書の画面と実機が異なる場合があります。

※　本サービスで提供する製品名称が『Trend Micro Deep Security™ as a Service』から『Trend Micro Cloud One™ Workload Security』へ変更となりました。本手順書内・画面にて、新旧の製品名称が混在しておりますことをご了承願います。

※　上記注意事項については、2 章注意事項に説明があります。

文書変更履歴

版数	発行日	改定履歴
0.2 版	2015/8/18	初版発行
1.0 版	2015/8/31	リリース版発行
1.6 版	2015/12/08	修正版発行 プロキシの登録手順修正
1.7 版	2016/01/25	修正版発行 注意事項追加 プロキシ経由接続のエージェントのインストール手順修正
1.8 版	2016/2/10	P.14　項目 22 修正
1.9 版	2016/11/9	・P.18　項目 3　画像修正 ・P.39　項目 12 画像修正
2.0 版	2017/7/21	・P.8 Feature Pack と通常モジュールに関する注意事項を追加 ・P.9(旧 P.8)の Agent のダウンロード画面を差し替え
3.0 版	2022/1/17	・ログオン手順変更を反映（URL・認証情報） ・製品名称変更について記載（Deep Security as a Service ⇒ Trend Micro Cloud One Workload Security） ・Trend Micro 社の参照 URL 変更を反映

目次

1. 作業前に確認する項目

- お客様のテナント情報（ユーザーポータルへのサインイン情報）を『ご契約内容のご案内』メールと『Cloud One への招待』メールより入手してください。
  ※『ご契約内容のご案内』メールと『Cloud One への招待』メールは、サービスご利用開始時に、申込書に記載いただいたお客様メールアドレスへ送付いたします。メールが届かない場合は、弊社担当営業までお問合せください。
  - メールアドレス
  - Password
    ※Password は『Cloud One への招待』メール本文記載の URL よりお客様にて初期設定が必要です。手順については、下記のサポートサイト掲載の『ユーザーガイド』をご参照ください。
    https://itkeeper.service.ricoh.co.jp/isp2/cs_svsec/usermanual.html

- インストールするサーバの OS バージョンを確認してください。

- お客様環境のインターネット接続情報のうち、プロキシ経由にてインターネットへ接続している場合は、プロキシサーバの以下の情報を確認してください。
  （申込時にご提出いただいた[申込詳細情報シート]の[５．プロキシサーバー情報]でも確認可能です。）
  - IP アドレス
  - ポート番号
  - 認証ユーザー名（※プロキシ認証有りの場合）
  - パスワード（※プロキシ認証有りの場合）

- クラウドサービス for サーバーセキュリティ エージェントをインストールするサーバの Web ブラウザ(※)から、管理画面にアクセスできることを確認する。
  https://cloudone.trendmicro.com/

※ 管理画面にアクセスする Web ブラウザの動作要件がありますので、注意事項の⑥を確認してください。

2. 注意事項

① ネットワークの瞬断が発生する

[重要事項確認書 記載内容]にも記載しております。

アプリケーションの仕様となりますので、作業前の注意事項としてご確認ください。

＜重要事項確認書 記載内容＞ ・本ソフトウェアの導入時に、OS上のネットワークドライバの導入が行われる為、ネットワークの瞬断が発生します。 必要に応じて、サーバーの関係部署などへシステムメンテナンスの調整を行ってください。

＜参考＞

【Deep Security Agent のインストール時のネットワーク瞬断について】

https://success.trendmicro.com/jp/solution/1106385

従来は、Web レピュテーション、ファイアウォール、侵入防御の機能をご利用の場合 DSA にネットワークドライバがインストールされるため瞬断が発生しました。

Deep Security Agent バージョン 9.5 より無瞬断ネットワークドライバーが導入されました。

これらのバージョンを使用した新規インストール、アンインストールまたは、アップグレードでは瞬断が発生しなくなります。

② インターネット接続環境により作業手順が異なる

インストール対象サーバがインターネットに直接接続をする場合と、接続にプロキシを経由する場合とで、手順が異なります。

プロキシ接続せず、インターネットに直接接続するサーバは 3 章、プロキシ経由で接続するサーバは 4 章の手順を実施してください。

③ プロキシ認証の方式に制限がある

インターネット接続にプロキシサーバを経由し、プロキシ認証を行っている場合、認証方式は、Basic 認証のみ利用できます。Digest 認証と NTLM 認証はサポートしていません。

④ 他のウイルス対策ソフトウェアとの併用はできない

導入されている場合、クラウドサービス ｆｏｒ サーバーセキュリティの導入失敗や稼働障害の原因となりますので、導入前に他のウイルス対策ソフトウェアのアンインストールを行ってください。

[重要事項確認書 記載内容]の P.2 “■クラウドサービス for サーバーセキュリティ 動作要件”のその他①欄にてご案内しています。

⑤ ServerProtect が過去に導入されていた環境でのインストール不具合事例

ServerProtect をアンインストール後のサーバでエージェントのインストールに失敗することがあります。

該当環境でインストールに失敗した場合、以下文章の“SPNT アンインストール後に Deep Security Agent 等の”で始まる文章をご確認いただき、手順に従いServerProtectの手動アンインストールを実施してください。

【ServerProtect のアンインストール手順】

https://success.trendmicro.com/jp/solution/1313920

＜文章抜粋＞

SPNT アンインストール後に Deep Security Agent 等の弊社別製品をインストール頂く場合は、ドライバ等の競合により正常にインストールが出来ない場合ございます為、手動にてドライバの情報を削除する必要がございます。

⑥ Web ブラウザの動作要件

管理画面にアクセスする Web ブラウザに動作要件があります。

[重要事項確認書 記載内容]の P.2 “■クラウドサービス for サーバーセキュリティ 動作要件”の Web ブラウザ欄にて、以下を記載しています。

- Firefox
- Microsoft Internet Explorer 11、Edge
- Google Chrome

※ Cookie を有効にする必要があります。

※ 各 Web ブラウザの最新版のご使用を推奨します。

※ Javascript を有効にする必要があります。（注）

※ ファイルのダウンロードを有効にする必要があります。（注）

（注）リモート導入オプション提供時に必要となる動作要件です。

⑦ 管理画面の表示

SaaS のため、管理、操作画面の変更は予告なく発生します。

本手順書は 2015 年 8 月時点の画面であり、本手順書で記載する画面と実機が異なる場合は、実機とマニュアルを読み比べ、用語が同じ、もしくは近い画面、メニューを開いてください。

3. 直接接続のエージェントのインストール

インターネットに直接接続するサーバにエージェントをインストールする手順です。

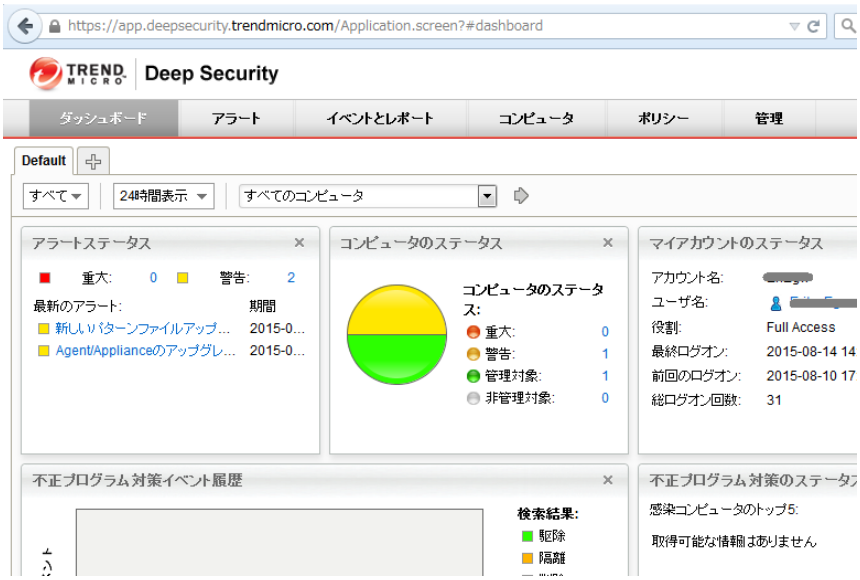
1. Deep Security Manager（クラウドサービス for サーバーセキュリティの Web 管理画面）に、お客様のテナント認証情報でサインインします。

   ※ URL は、[https://cloudone.trendmicro.com/]です

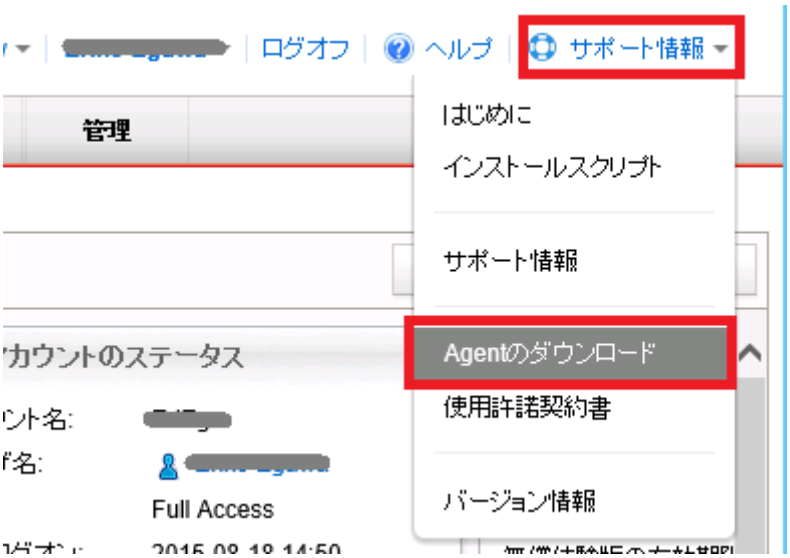
   ※ 認証情報として、[メールアドレス]、[パスワード]の二点を入力し、[ログオン]をクリックします。

2. ［Workload Security］をクリックします。

3. サインイン後の Deep Security Manager 画面です。



4. Deep Security Manager 画面の右上にある［サポート情報］をクリックし、表示されるメニューから［Agent のダウンロード］をクリックします。



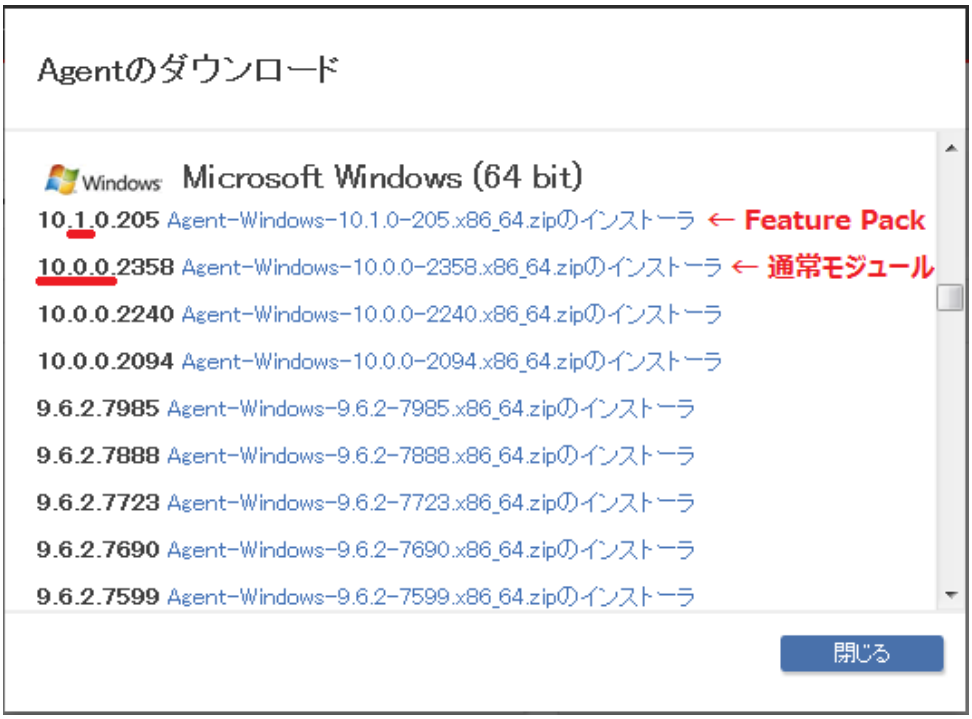
5. エージェントをインストールするサーバの OS の該当するプラットフォームの最新バージョンのエージェントをクリックし、ダウンロードが開始することを確認します。

※ [Microsoft Windows]は、リストを下に 1/3 程度スクロールした位置にあります。
※ 最新バージョンは、プラットフォーム内で一番上に表示されます。
※ Windows Server 2008 R2 以降の OS は 64 bit のみです。

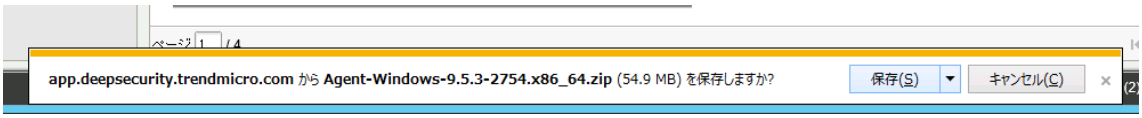
※ 2017 年 7 月 15 日以降、「Feature Pack」バージョンがリリースされますが、Feature Pack には制限事項があるため使用できませんので、最新バージョンに Feature Pack が表示されている場合は、その下の**通常モジュールをダウンロードしてください**。

※ 通常モジュールは、バージョン番号の二桁目が「0」であり、それ以外は Feature Pack です。

例:
10.2.X.XXXX: Feature Pack
10.1.X.XXXX: Feature Pack
10.**0**.X.XXXX: **通常モジュール**

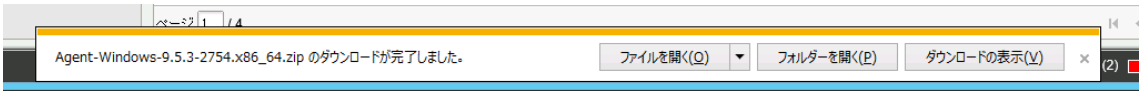


6. Internet Explorer で操作をしている場合、下部に出てくるバーで[保存]、もしくはポップアップウィンドウで[ファイルを保存]をクリックします。



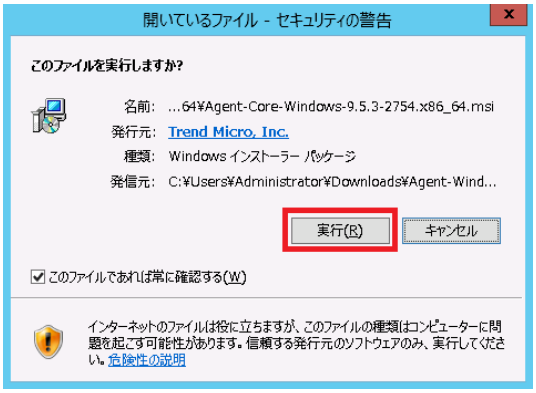
※ ブラウザのバージョンにより、画面やメッセージが異なります。

7. 保存が終わったら、[ファイルを開く]をクリック、もしくは保存先フォルダを開いてファイルをダブルクリックします。

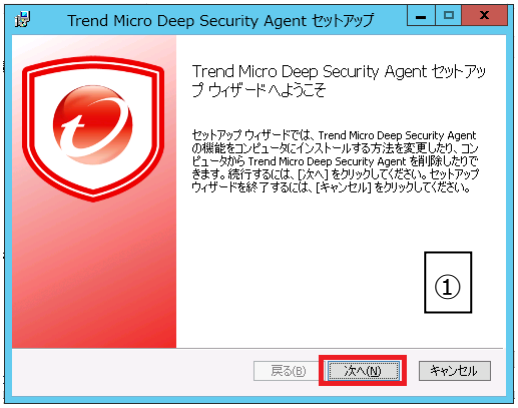


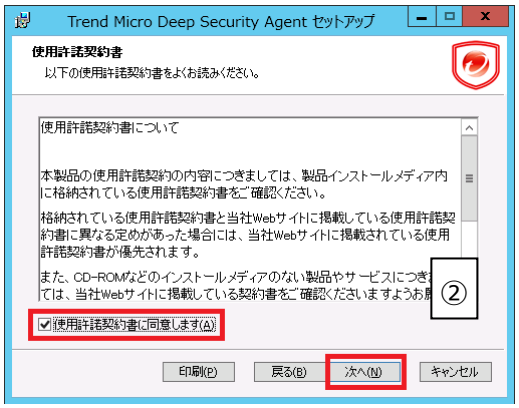
※ ブラウザのバージョンにより、画面やメッセージが異なります。

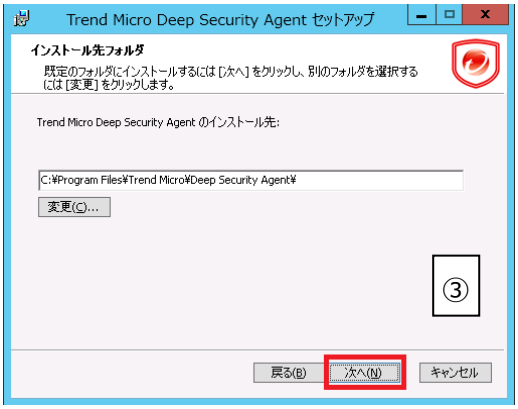
8. セキュリティの警告が出た場合、[実行]をクリックします。

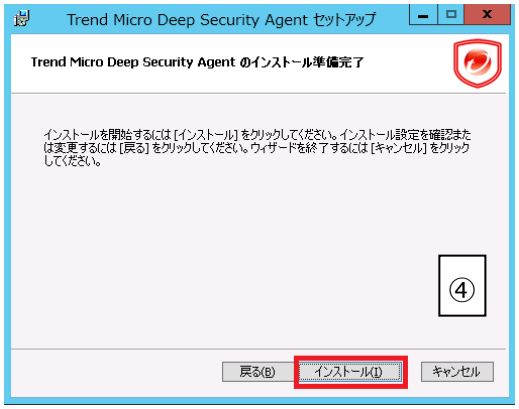


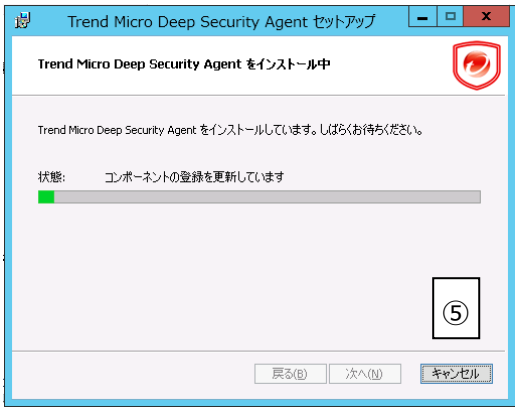
9. インストールが始まります。設定は初期値で進めます。







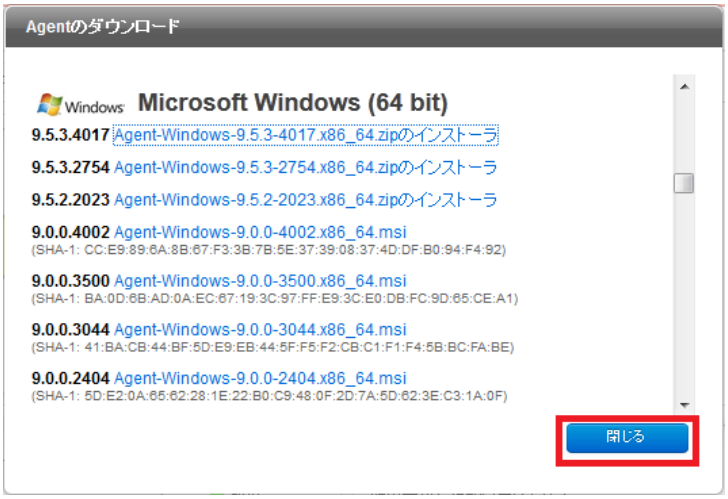




10. タスクバーに[Trend Micro Deep Security]のアイコンが表示されたことを確認します。

11. Deep Security Manager 画面に戻り、手順 4 から 5 で使用した[Agent のダウンロード]画面がまだ表示されている場合は、[閉じる]で閉じます。

※ Deep Security Manager 画面を自動サインアウトされた場合は、サインインしてください。

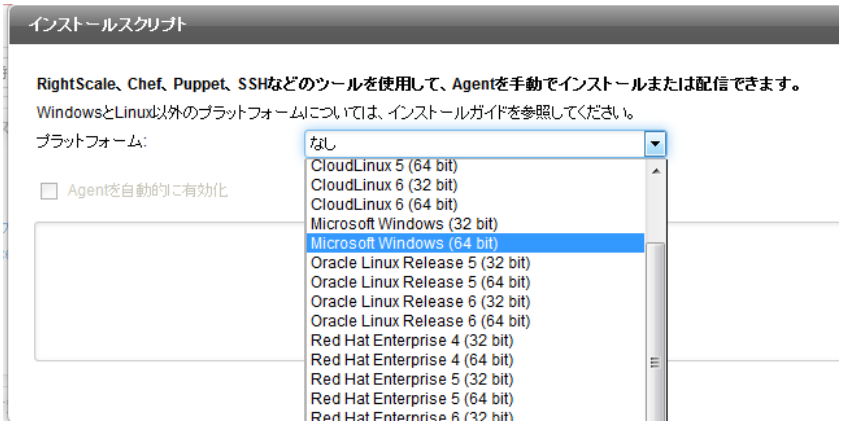


12. エージェント有効化のため、コマンドプロンプトを起動します。

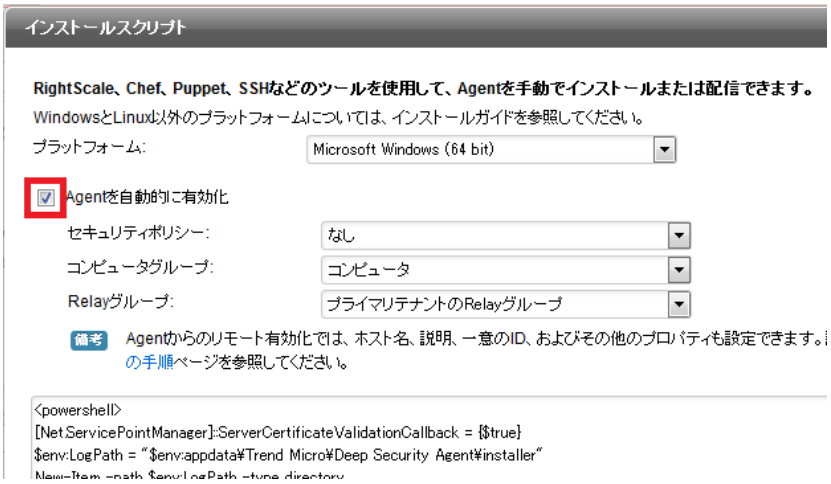
※ コマンドプロンプトをメニューやタスクバーから見つけにくい場合、[Windows]+[R]キーを押し、[ファイル名を指定して実行]画面で、[名前]に[cmd]と入力して[OK]で呼び出すのが便利です。

13. Deep Security Manager でクラウドサービス for サーバーセキュリティ エージェントの有効化スクリプトを作成します。
    Deep Security Manager 画面の右上にある [サポート] をクリックし、表示されるメニューから [インストールスクリプト] をクリックして、インストールスクリプトジェネレータを起動します。

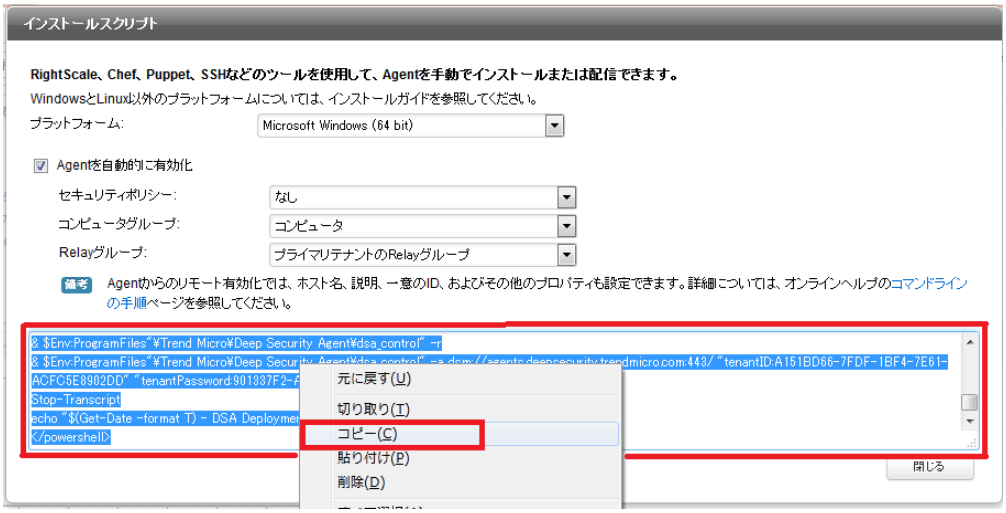
14. [プラットフォーム:]のリストダウンボックスで、エージェントをインストールするサーバの OS に該当するプラットフォームを選択します
    ※ Windows Server 2008 R2 以降の OS は 64 bit のみです。
    ※ プラットフォームが[なし]しか出ない場合、システム要件にあっていない Web ブラウザを使用していないか確認してください。



15. [Agent を自動的に有効化] をチェックします。
    ※ その下にある、[セキュリティポリシー]、[コンピュータグループ]、[Relay グループ]の設定は変更不要です。

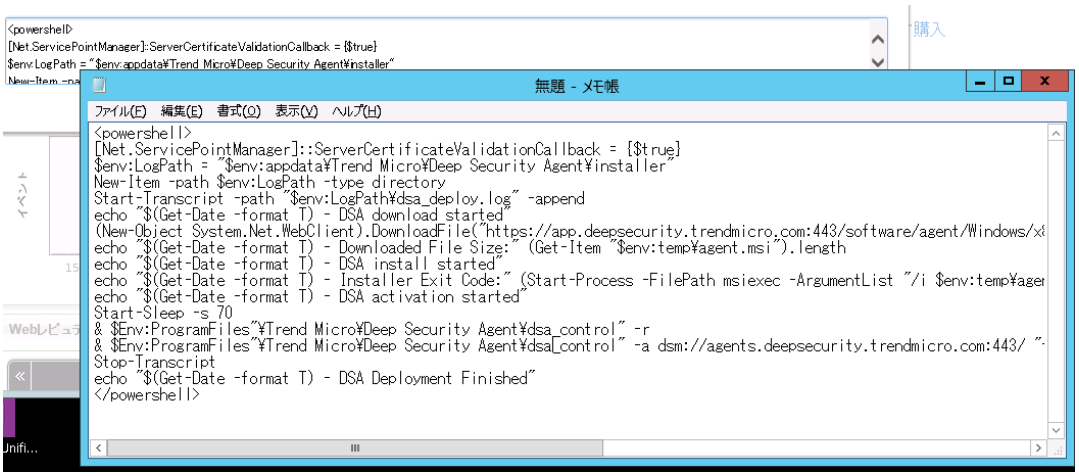


16. 枠内のスクリプトを全て選択し、右クリックのメニューから[コピー]します。



17. メモ帳を起動し、手順 16 でコピーしたスクリプトを貼り付けます。

※ メモ帳をメニューやタスクバーから見つけにくい場合、[Windows]+[R]キーを押し、[ファイル名を指定して実行]画面で、[名前]に[notepad]と入力して[OK]で呼び出すのが便利です。



18. 下から４行目の、[dsa_control" -a]の行を選択します

※ 行番号は実機では異なる可能性があります

※ この行には、お客様固有の[tenantID]、[tenantPassword]が記載されています

選択箇所は[dsa_control" -a dsm://agents.deepsecurity.trendmicro.com:443/ "tenantID:********** " "tenantPassword: **********"]です。

※ 画面の右側表示が切れた場合、[書式]→[右端で折り返す]にチェックを入れて、メモ帳を折り返し表示してください。

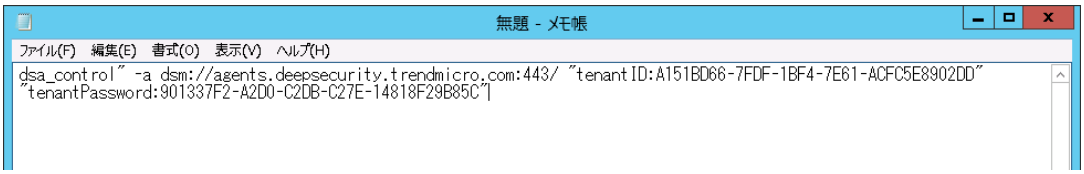
※ 画面は折り返し表示をしているメモ帳です。

19. 選択した行を、コピーします([Ctrl]+[C])。

20. [ファイル]→[新規]で、新規メモ帳画面を表示します。

※ [無題への変更内容を保存しますか？]とでたら、[保存しない]を選択します。

21. コピー内容を貼り付けます([Ctrl]+[V])。



22. 張り付けた行を、メモ帳上で以下のように加工します。
    △は半角スペース 1 つを意味します。

変更前

dsa_control" △ -a △ dsm://agents.deepsecurity.trendmicro.com:443/ △ "tenantID:[お客様のテナント ID]"△"tenantPassword:[お客様のテナントパスワード]"

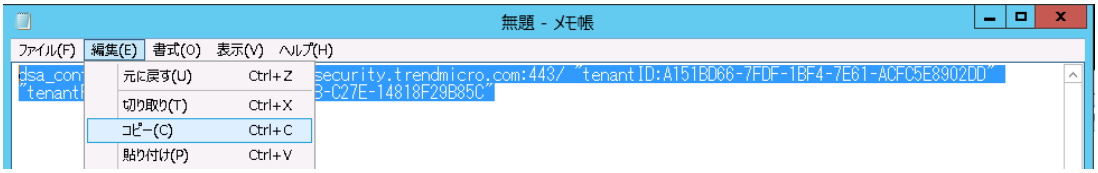
変更後(dsa_control の後のダブルクォーテーションマーク(")1 つを取りました)

dsa_control△-a△dsm://agents.deepsecurity.trendmicro.com:443/△"tenantID:[お客様のテナント ID]"△"tenantPassword:[お客様のテナントパスワード]"

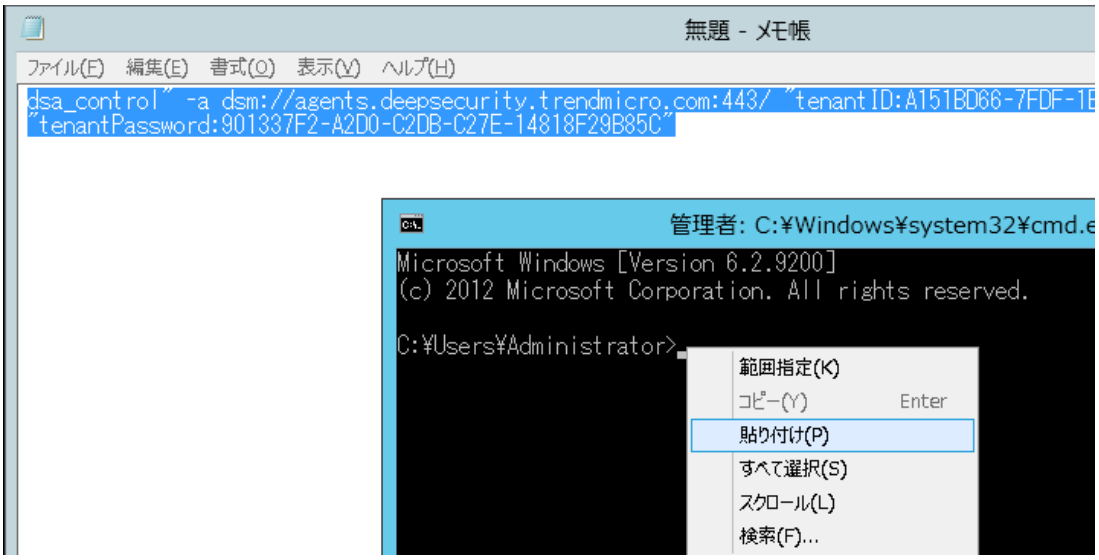
23. コマンドプロンプト画面でクラウドサービス for サーバーセキュリティエージェントのインストールフォルダに移動します。

cd△"C:¥Program△Files¥Trend△Micro¥Deep△Security△Agent"

24. 手順 22 で加工した行を、選択しコピーします。



25. コマンドプロンプト画面上で右クリックし、メニューから[貼り付け]を選択します。



26. 貼り付けた行の最後にカーソルがあることを確認して、Enter キーを押します。

27. 実行結果を確認します。

以下のような画面出力で、「Command session completed.」で終われば完了です。

```
HTTP Status: 200 - OK
Response:
Attempting to connect to https://agents.deepsecurity.trendmicro.com:443/
SSL handshake completed successfully - initiating command session.
Connected with AES256-SHA to peer at agents.deepsecurity.trendmicro.com
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.
Received a 'GetAgentStatus' command from the manager.
Received a 'GetAgentEvents' command from the manager.
Received a 'SetSecurityConfiguration' command from the manager.
Received a 'GetAgentEvents' command from the manager.
Received a 'GetAgentStatus' command from the manager.
Command session completed.
```

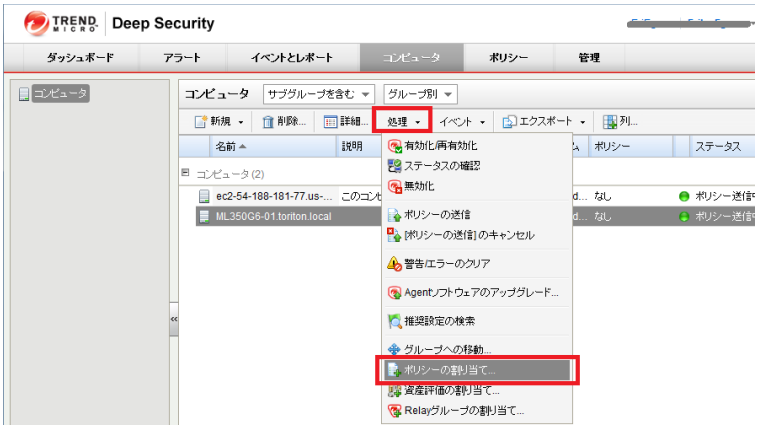
✓ 本作業にて、 クラウドサービス for サーバーセキュリティのエージェントインストールが正常に終了しました。

28. 以上でインストールは完了です。インストールの正常終了を確認するため、次章の手順を実施します。

3.1. インストール正常終了の確認

1. Deep Security Managerの[コンピュータ]タブを開き、エージェントをインストールしたサーバが “管理対象(オンライン)”と表示されることを確認します。

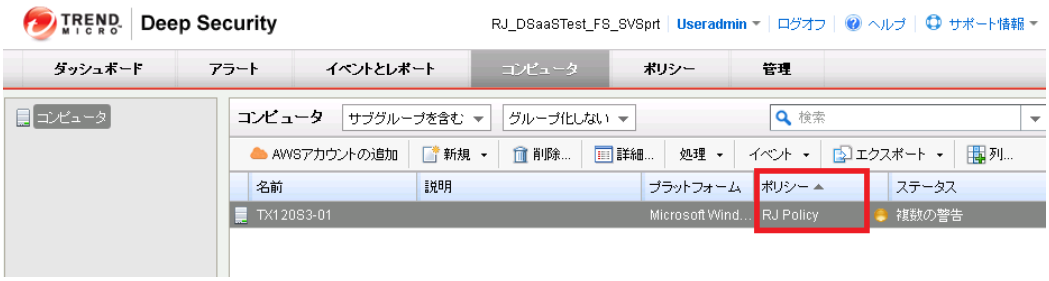
2. ポリシーを変更します。
登録したサーバを選択し反転している状態で、[処理]→[ポリシーの割り当て]をクリックし、表示されるポリシー一覧からポリシー(※)を選択し[OK]をクリックします。



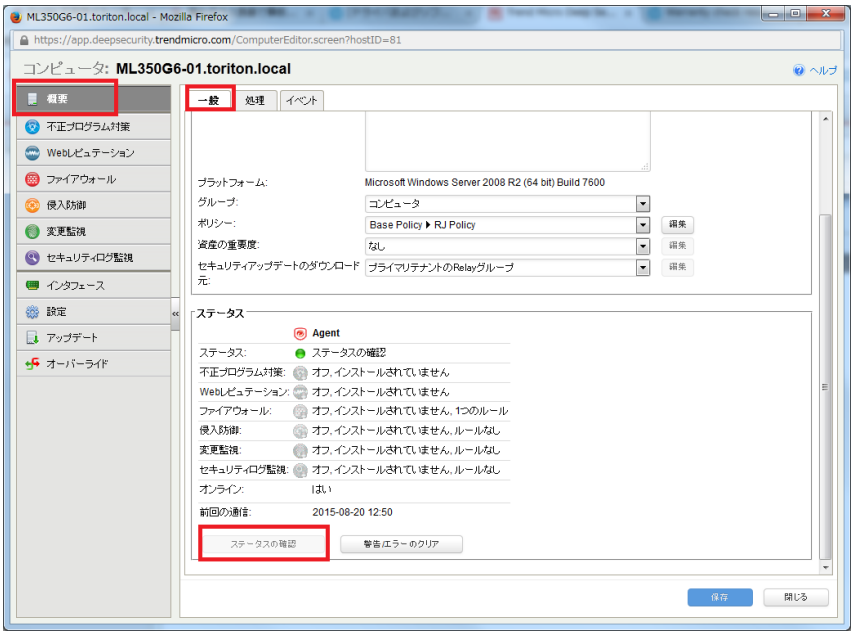
※ 適用するポリシーは、以下のように OS により異なります。

- OS が【Windows Server 2003 32bit **以外**】の場合は、**【RJ Policy】**を選択します。
- OS が【Windows Server 2003 32bit】の場合は、**【RJ Policy(2K3_32bit)】**を選択します。

3. ポリシー欄で割り当てたポリシー名が表示されたことを確認します。



4. サーバをダブルクリックし詳細画面を開き、[概要]-[一般]タブの[ステータスの確認]をクリックし、ステータスを更新します。



※ ステータスに警告やエラーが出た場合、[警告/エラーのクリア]をクリックし、再度[ステータスの確認]をクリックしてください。

※ ステータスの確認中は、[ステータスの確認]はグレーアウトしクリックできません。

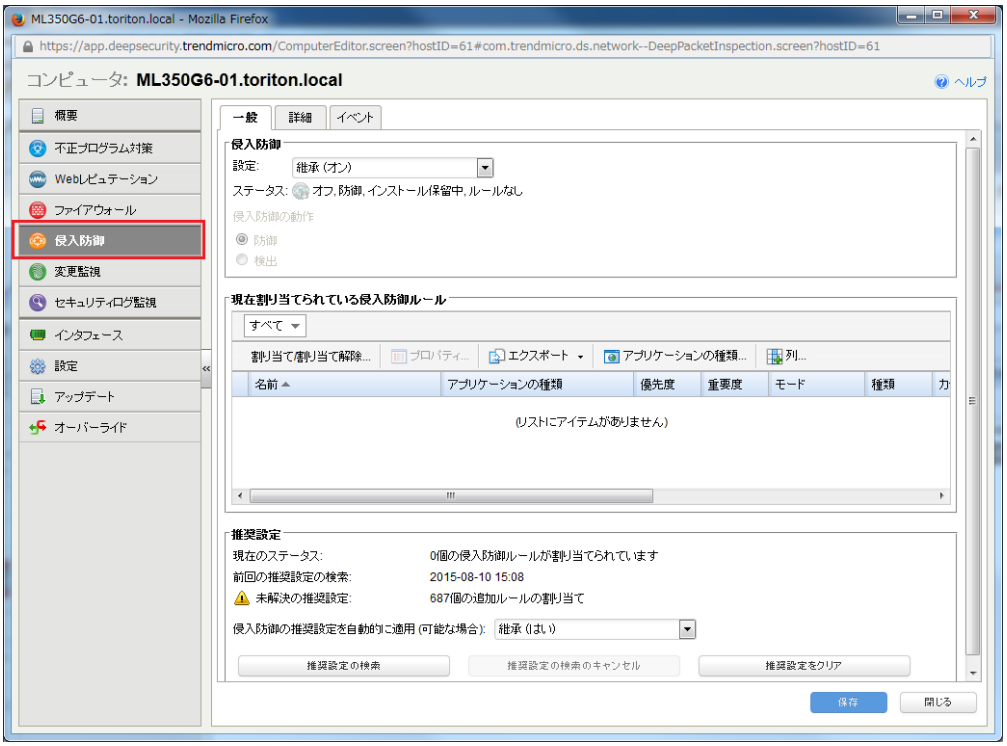
5. ステータスが[管理対象(オンライン)]となれば、インストール正常終了の確認が完了です。

6. 以上で正常終了の確認は完了です。初回手動検索を開始するため、次章の手順を実施します。

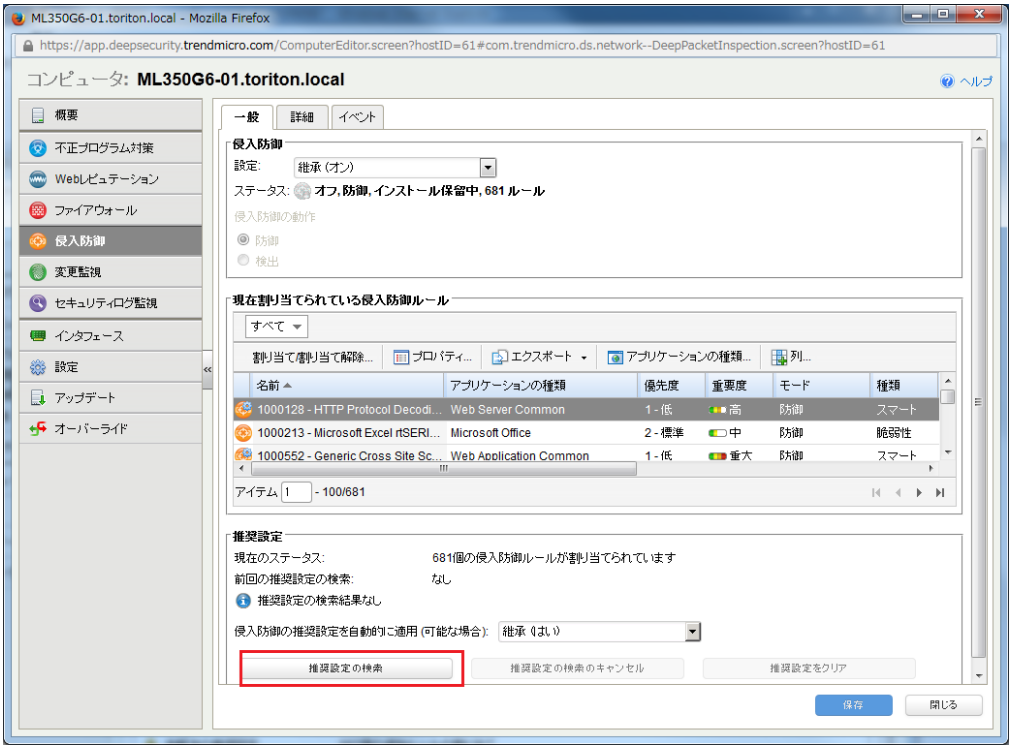
3.2. 手動検索の実施

1. Deep Security Managerの[コンピュータ]タブを開き、登録したコンピュータをダブルクリック、または右クリックからのメニューで[詳細]を開きます。

2. [侵入防御]をクリックします。

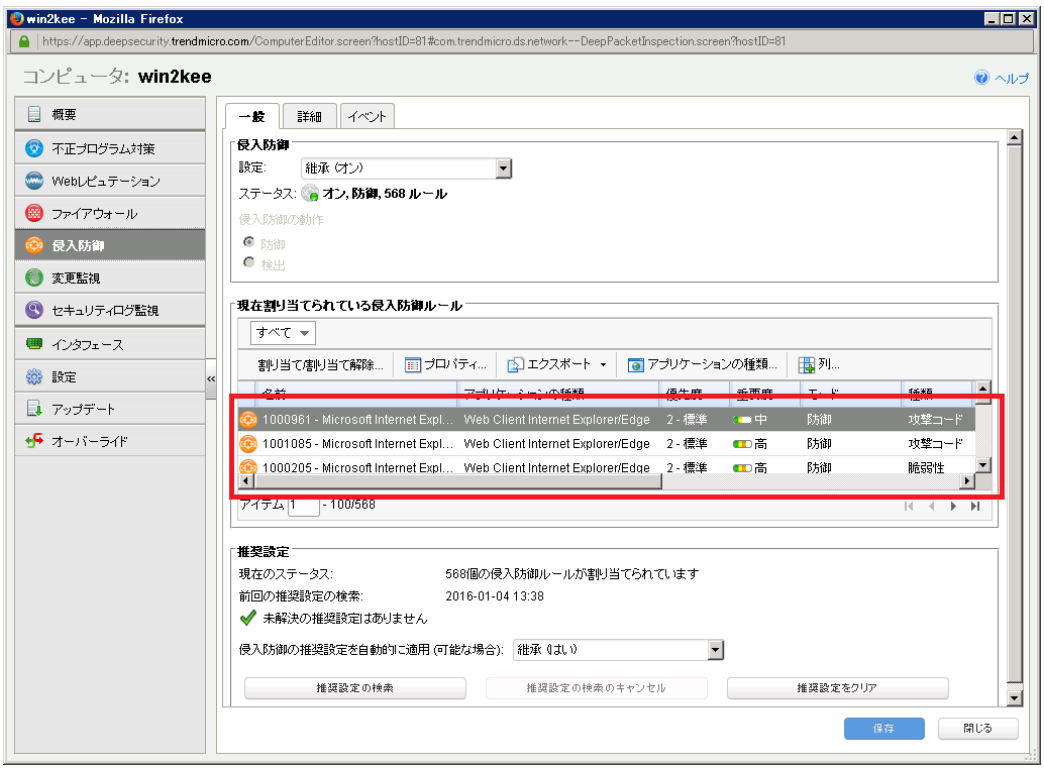


3. [推奨設定の検索]をクリックします。

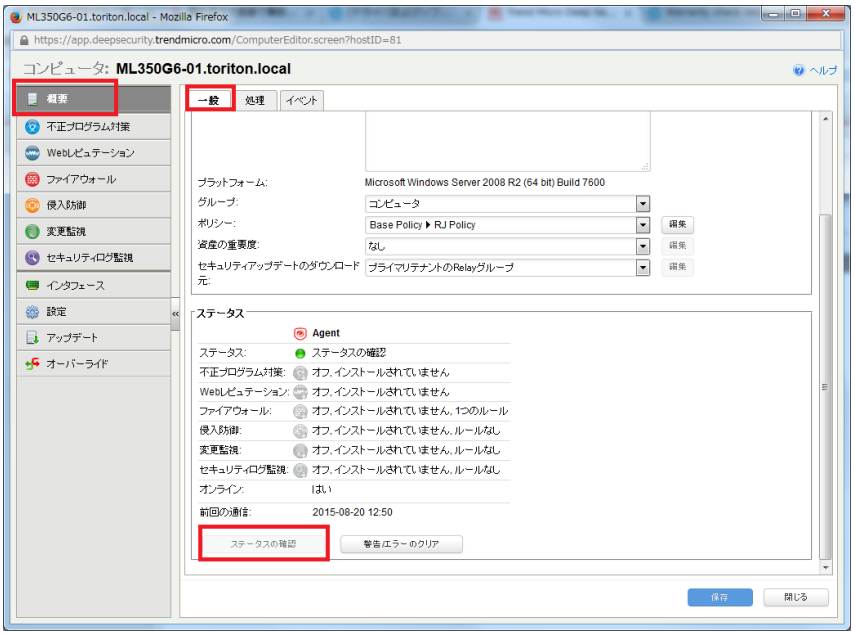


※ 環境により割り当てられるルールが多くなり、検索に 10 分以上がかかる場合があります。

4. 現在割り当てられている侵入防御ルールのリストにルールが追加されたことを確認します。



5. [概要]-[一般]タブの[ステータスの確認]をクリックし、ステータスを更新します。



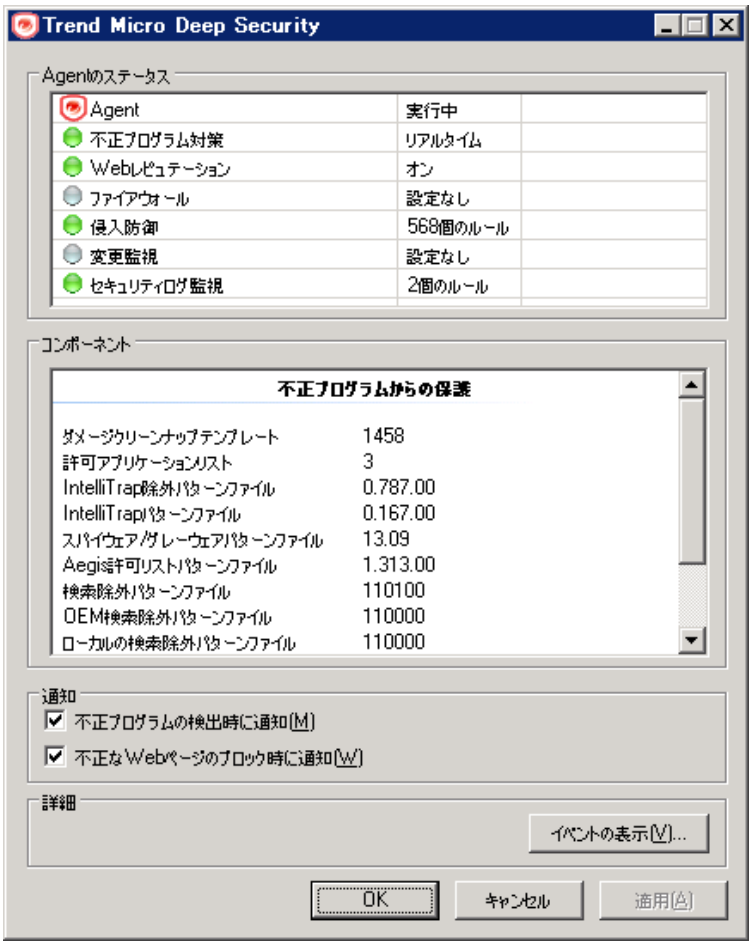
※ ステータスに警告やエラーが出た場合、[警告/エラーのクリア]をクリックし、再度[ステータスの確認]をクリックしてください。

※ ステータスの確認中は、[ステータスの確認]はグレーアウトしクリックできません。

6. ステータスが以下状態になったことを確認します。
   - ステータスが[管理対象(オンライン)]である
   - 以下 4 つの項目が[オン]である
     ① 不正プログラム対策
     ② Web レピュテーション
     ③ 侵入防御
     ④ セキュリティログ監視

7. [閉じる]ボタンで詳細画面を閉じます。

8. サーバの画面右下のタスクバーで[Trend Micro Deep Security]アイコンをダブルクリックし、開いた画面で Agent が[実行中]であり、以下 4 つの項目に緑の丸がついていることを確認します。
   ① 不正プログラム対策
   ② Web レピュテーション
   ③ 侵入防御
   ④ セキュリティログ監視



9. 管理画面とエージェント画面を閉じて、初回の手動検索は完了です。
※管理画面は Web ブラウザの×で閉じて問題ありません。

✓ 本作業にて Deep Security マネージャ画面にて対象コンピューターが管理対象であることの確認が取れました。

4. プロキシ経由接続のエージェントのインストール

インターネットにプロキシ経由で接続するサーバにエージェントをインストールする手順です。

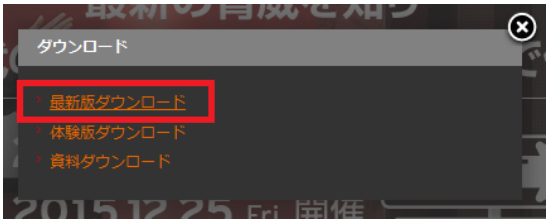
1. エージェントのダウンロードページにアクセスします。

   直接 URL にアクセスする場合は、以下 URL をサーバの Web ブラウザのアドレスバーに入力します。

   http://downloadcenter.trendmicro.com/index.php?regs=jp&cm_sp=Header-_-Download-_-dc

   Trend Micro ホームページからリンクをたどる場合、以下のように開きます。

   http://www.trendmicro.co.jp/⇒ [ダウンロード]⇒[最新版ダウンロード]



2. エージェントのダウンロードリンクをクリックします。

   最新版ダウンロードの一覧から、[統合サーバセキュリティ対策]欄の

   [Windows 版 Deep Security Agent / Relay / Notifier]をクリックします。

(拡大)

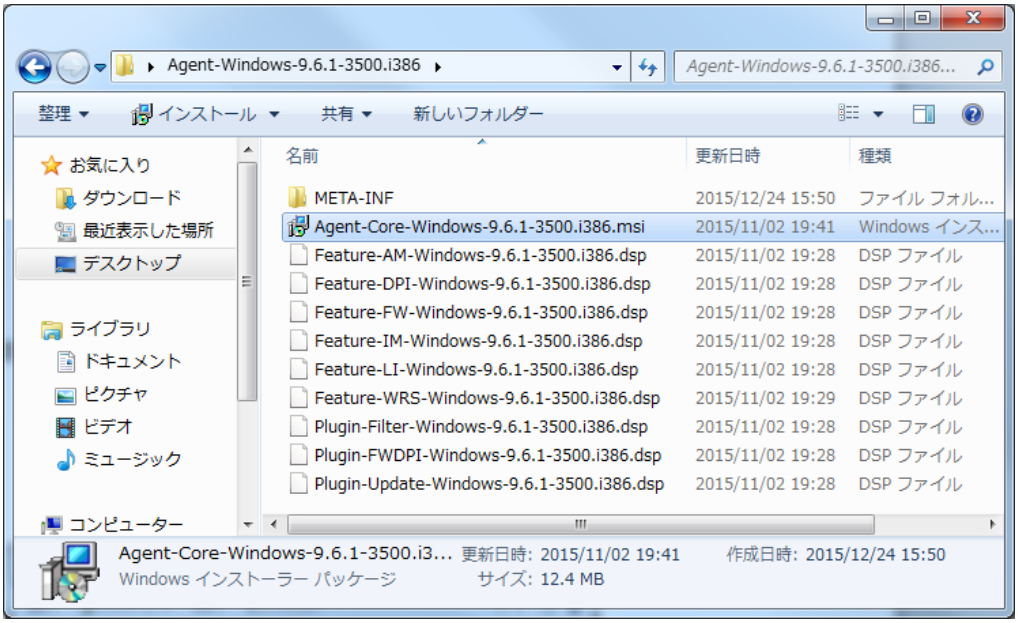
3. 拡張子が zip のインストールプログラムをダウンロードします。
拡張子が zip で、OS の bit にあったインストールプログラムをダウンロードします。
拡張子が msi のインストールプログラムは使用しません。

画面には、zip、msi の両方のインストールプログラムが出ますので、ダウンロードするファイルの拡張子が**.zip であることを**確認してください。

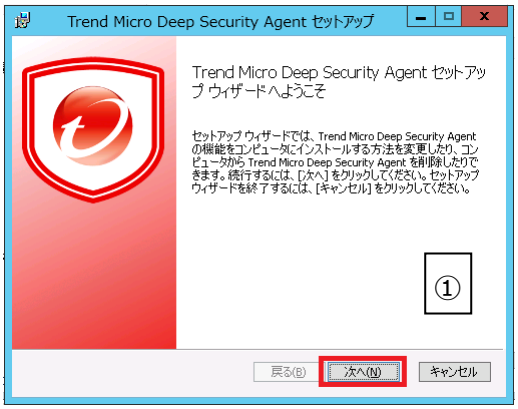
※ ダウンロード時の最新版が出てくるため、ファイル名の拡張子以外の文字は異なる可能性があります。
※ OS の bit により、64bit、32bit のいずれかを選んでください。
※ ファイルのダウンロードでは、実行ではなく[保存]を選んでください。

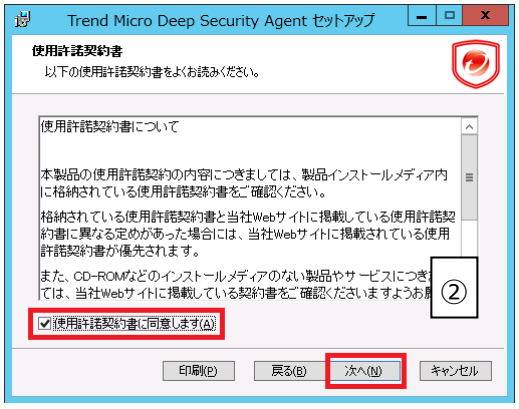
4. ダウンロード、した zip ファイルをサーバ上で解凍します。
※ ZIP ファイルを解凍せずダブルクリックでに開いて次の手順に進むとインストールが不完全になりますので、**必ず解凍してから次の手順に進んでください。**

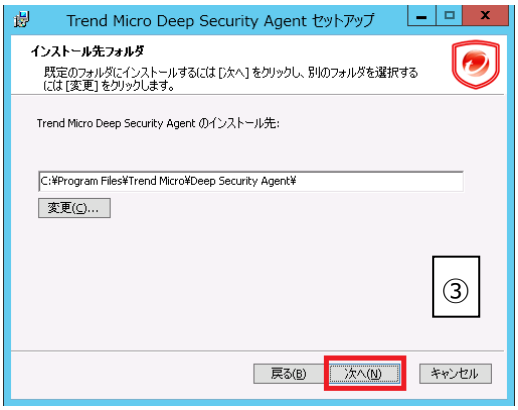
5. 解凍するとフォルダができるので、フォルダ内の Windows インストーラパッケージ(ここでは拡張子が msi)をダブルクリックします。

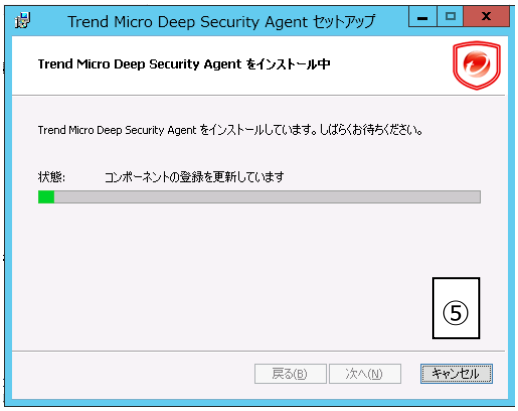


6. インストールが始まります。設定は初期値で進めます。



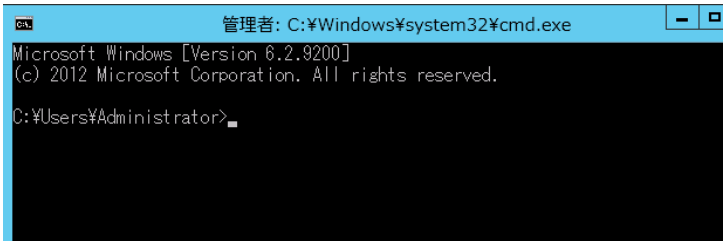






7. タスクバーに[Trend Micro Deep Security]のアイコンが表示されたことを確認します。

8. プロキシサーバ登録、エージェント有効化のため、コマンドプロンプトを起動します。
   ※ コマンドプロンプトをメニューやタスクバーから見つけにくい場合、[Windows]+[R]キーを押し、[ファイル名を指定して実行]画面で、[名前]に[cmd]と入力して[OK]で呼び出すのが便利です。



9. 以下の手順を実施し、プロキシサーバを登録します。
   △は、半角スペース 1 つを意味します。

   (ア) クラウドサービス for サーバーセキュリティエージェントのインストールフォルダに移動します。

   ```
   cd△"C:¥Program△Files¥Trend△Micro¥Deep△Security△Agent"
   ```

   (イ) プロキシサーバの登録を、以下の形式のコマンドで実行します。

   ```
   dsa_control△-x△"dsm_proxy://[プロキシ IP アドレス又はホスト名]:[ポート番号]"
   ```

※　プロキシサーバの IP アドレスが[192.168.10.100]、ポートが[8080]の場合、コマンドは以下になります。

dsa_control –x "dsm_proxy://192.168.10.100:8080/"

※　プロキシサーバのホスト名が[proxy.example.co.jp]、ポートが[8888]の場合、コマンドは以下になります。

dsa_control –x "dsm_proxy://proxy. example.co.jp:8888/"

(ウ) 以下のメッセージが返ってくれば、プロキシサーバの登録は成功です。

HTTP Status: 200 - OK

Response:Add proxy-address:[dsm_proxy] with value:[192.168.10.100:8080/]

プロキシサーバのホスト名、IP アドレスを間違った場合、以下のコマンドでプロキシサーバ設定をクリアしてから、再設定してください。

dsa_control△-x△""

プロキシで認証を行っている場合は、次に進みます。
認証がない場合、手順 10 に進みます。

(エ) プロキシ認証有の場合、認証情報を以下形式でコマンド登録します。

dsa_control△-u△"[認証ユーザ名]:[認証パスワード]"

※　プロキシ認証情報がユーザ名[user01]、パスワードが[pass01]の場合、コマンドは以下になります。

dsa_control –u "user01:pass01"

プロキシ認証は、Basic 認証のみ利用できます。
Digest 認証と NTLM 認証はサポートしていません。

(オ) 認証情報の登録コマンドの結果は出力されないので、プロンプトが返れば登録完了です。

登録を間違った場合、以下コマンドで認証設定をクリアしてから、再設定してください。

dsa_control△-u△""

※　コマンドプロンプトは次の手順で使用するため、まだ閉じません。

10. Deep Security Manager（クラウドサービス for サーバーセキュリティの Web 管理画面）に、お客様のテナント認証情報でサインインします。

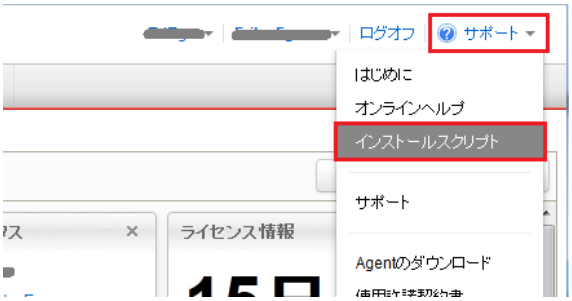
※ URL は、[https://cloudone.trendmicro.com/]です

※ 認証情報として、[メールアドレス]、[パスワード]の二点を入力し、[ログオン]をクリックします。

11. ［Workload Security］をクリックします。

12. Deep Security Manager でクラウドサービス for サーバーセキュリティ エージェントの有効化スクリプトを作成します。

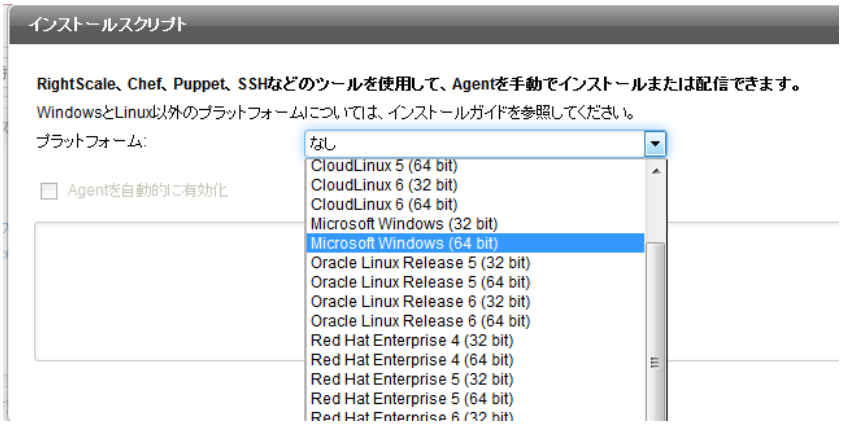
Deep Security Manager 画面の右上にある［サポート］をクリックし、表示されるメニューから［インストールスクリプト］をクリックして、インストールスクリプトジェネレータを起動します。



13. [プラットフォーム:]のリストダウンボックスで、エージェントをインストールするサーバの OS に該当するプラットフォームを選択します

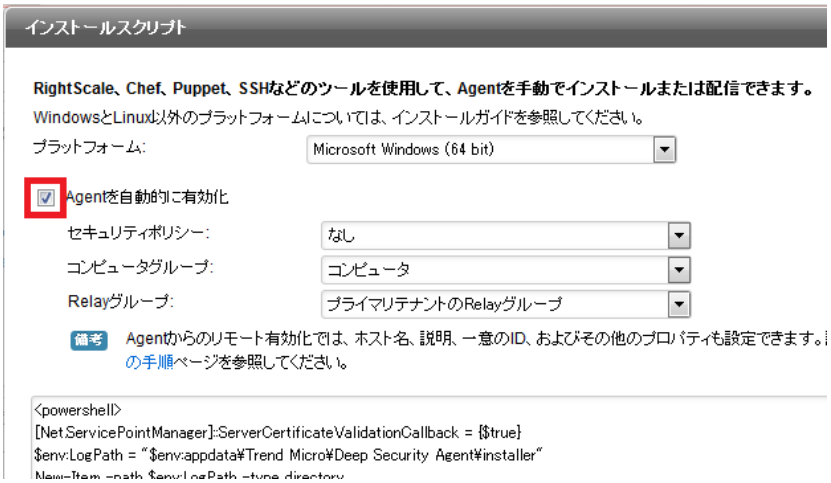
※ Windows Server 2008 R2 以降の OS は 64 bit のみです。

※ プラットフォームが[なし]しか出ない場合、システム要件にあっていない Web ブラウザを使用していないか確認してください。

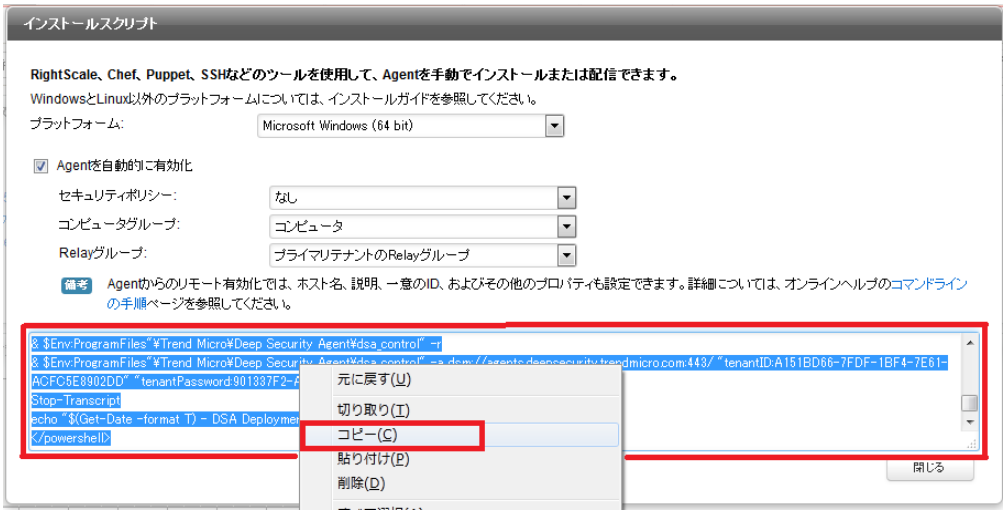


14. [Agent を自動的に有効化] をチェックします。

※ その下にある、[セキュリティポリシー]、[コンピュータグループ]、[Relay グループ]の設定は変更不要です。

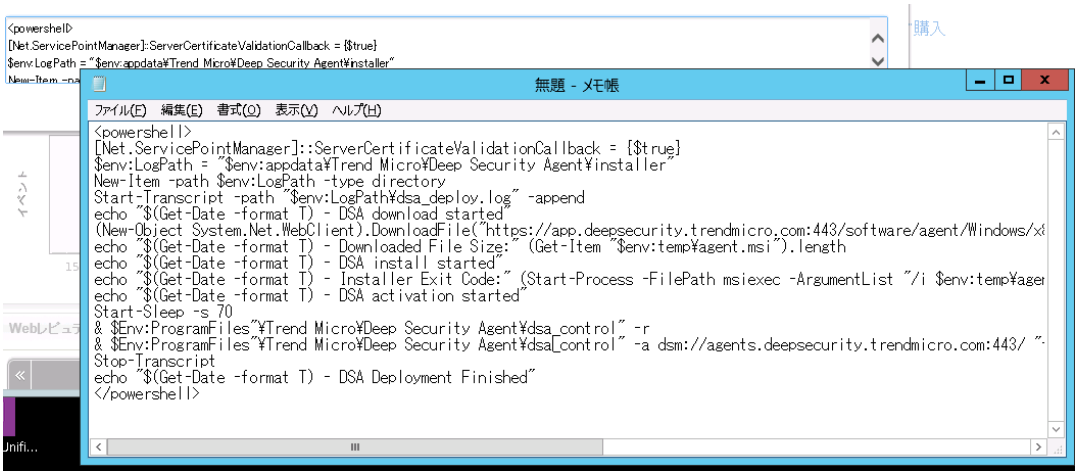


15. 枠内のスクリプトを全て選択し、右クリックのメニューから[コピー]します。



16. メモ帳を起動し、手順 15 でコピーしたスクリプトを貼り付けます。

※ メモ帳をメニューやタスクバーから見つけにくい場合、[Windows]+[R]キーを押し、[ファイル名を指定して実行]画面で、[名前]に[notepad]と入力して[OK]で呼び出すのが便利です。

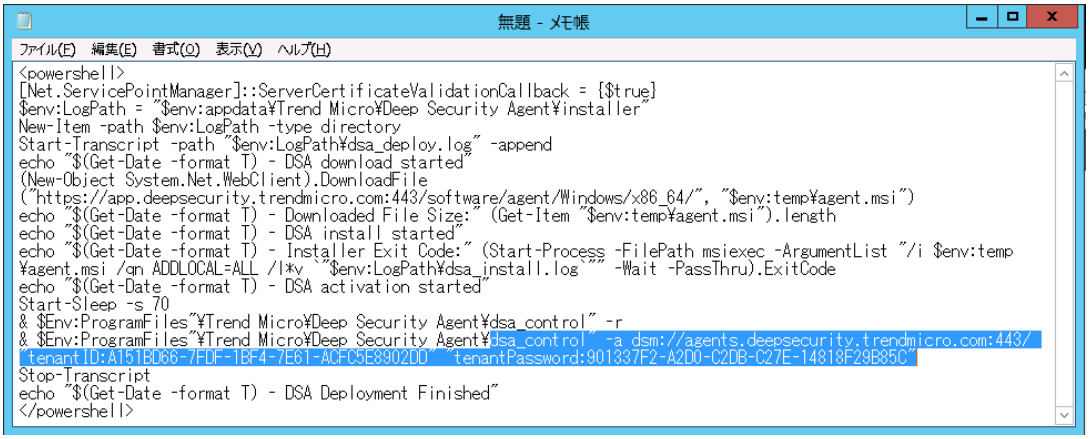


17. 下から 4 行目の、[dsa_control" -a]の行を選択します

※ 行番号は実機では異なる可能性があります

※ この行には、お客様固有の[tenantID]、[tenantPassword]が記載されています

選択箇所は[dsa_control" -a dsm://agents.deepsecurity.trendmicro.com:443/ "tenantID:********** " "tenantPassword: **********"]です。



※ 画面の右側表示が切れた場合、[書式]→[右端で折り返す]にチェックを入れて、メモ帳を折り返し表示してください。

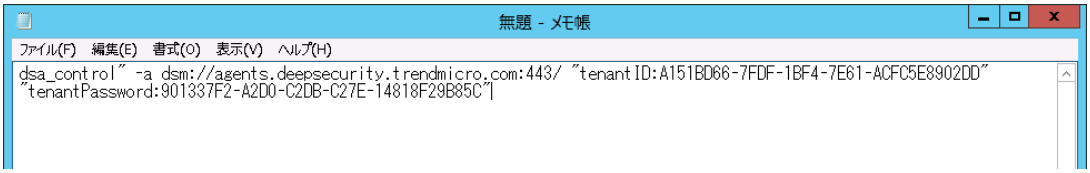
※ 画面は折り返し表示をしているメモ帳です。

18. 選択した行を、コピーします([Ctrl]+[C])。

19. [ファイル]→[新規]で、新規メモ帳画面を表示します。

※ [無題への変更内容を保存しますか？]とでたら、[保存しない]を選択します。

20. コピー内容を貼り付けます([Ctrl]+[V])。



21. 張り付けた行を、メモ帳上で以下のように加工します。

△は半角スペース 1 つを意味します。

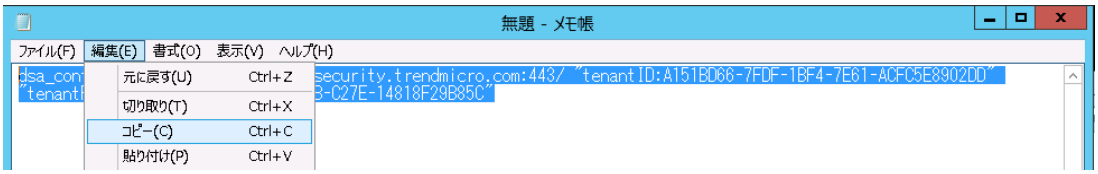
変更前

dsa_control" △ -a △ dsm://agents.deepsecurity.trendmicro.com:443/ △ "tenantID:[お客様のテナント ID]"△"tenantPassword:[お客様のテナントパスワード]"

変更後(dsa_control の後のダブルクォーテーションマーク(")1 つを取りました)

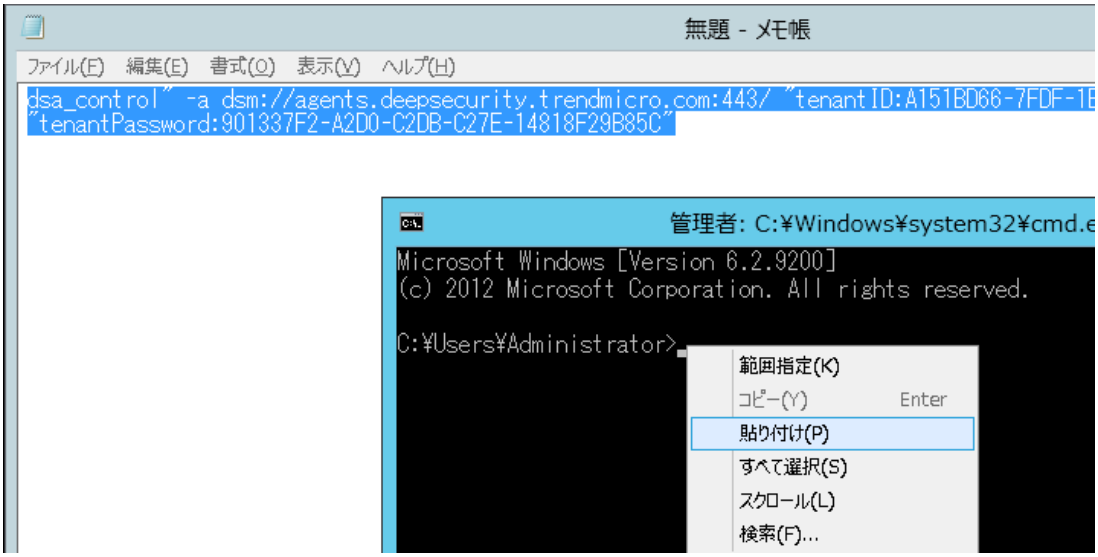
dsa_control△-a△dsm://agents.deepsecurity.trendmicro.com:443/△"tenantID:[お客様のテナント ID]"△"tenantPassword:[お客様のテナントパスワード]"

22. 前の手順(手順 22)で加工した行を、選択しコピーします。



23. コマンドプロンプト画面を前面表示します。

24. コマンドプロンプト画面上で右クリックし、メニューから[貼り付け]を選択します。



25. 貼り付けた行の最後にカーソルがあることを確認して、Enter キーを押します。

26. 実行結果を確認します。

以下のような画面出力で、[Command session completed.]で終われば完了です。

```
HTTP Status: 200 - OK
Response:
Attempting to connect to https://agents.deepsecurity.trendmicro.com:443/
SSL handshake completed successfully - initiating command session.
Connected with AES256-SHA to peer at agents.deepsecurity.trendmicro.com
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.
Received a 'GetAgentStatus' command from the manager.
Received a 'GetAgentEvents' command from the manager.
Received a 'SetSecurityConfiguration' command from the manager.
Received a 'GetAgentEvents' command from the manager.
Received a 'GetAgentStatus' command from the manager.
Command session completed.
```

✓ 本作業にてクラウドサービス for サーバーセキュリティのエージェントインストールが正常に終了しました。

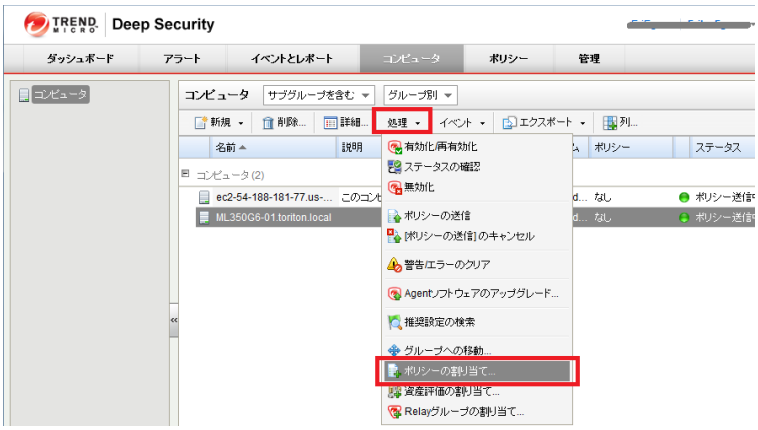
27. 以上でインストールは完了です。インストールの正常終了を確認するため、次章の手順を実施します。

4.1. インストール正常終了の確認

1. Deep Security Manager の[コンピュータ]タブを開き、エージェントをインストールしたサーバのホスト名と表示されることを確認します。

※ ここでステータスにエラーや警告があっても問題はありません。

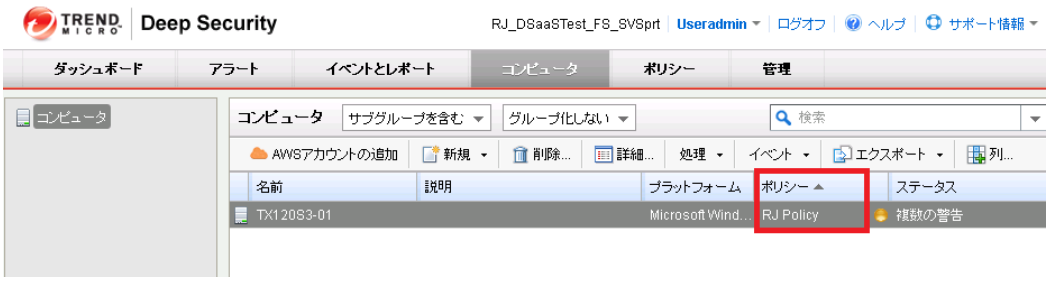
2. ポリシーを変更します。
登録したサーバを選択し反転している状態で、[処理]→[ポリシーの割り当て]をクリックし、表示されるポリシー一覧からポリシー(※)を選択し[OK]をクリックします。



※ 適用するポリシーは、以下のように OS により異なります。

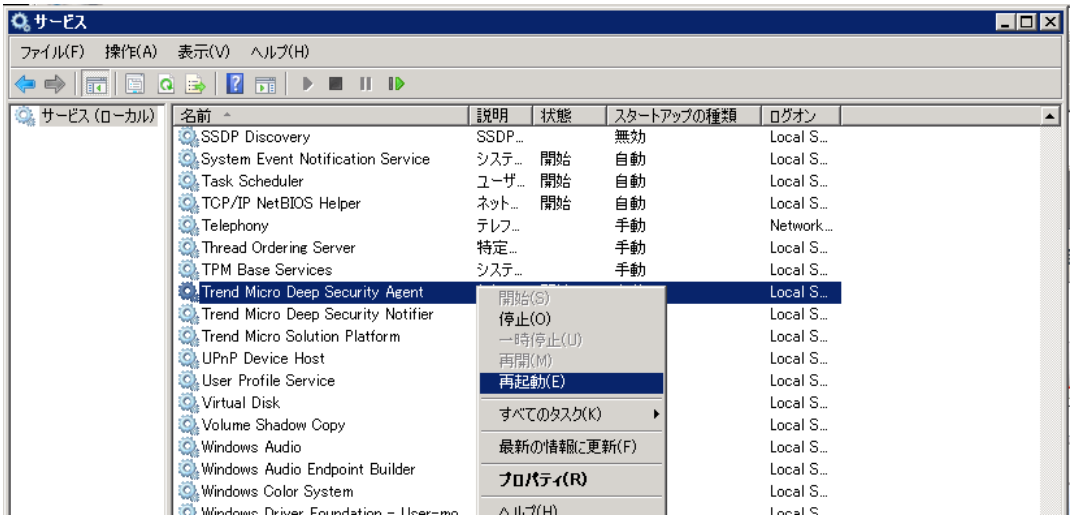
- OS が【Windows Server 2003 32bit **以外**】の場合は、**【RJ Policy】**を選択します。
- OS が【Windows Server 2003 32bit】の場合は、**【RJ Policy(2K3_32bit)】**を選択します。

3. ポリシー欄で割り当てたポリシー名が表示されたことを確認します。

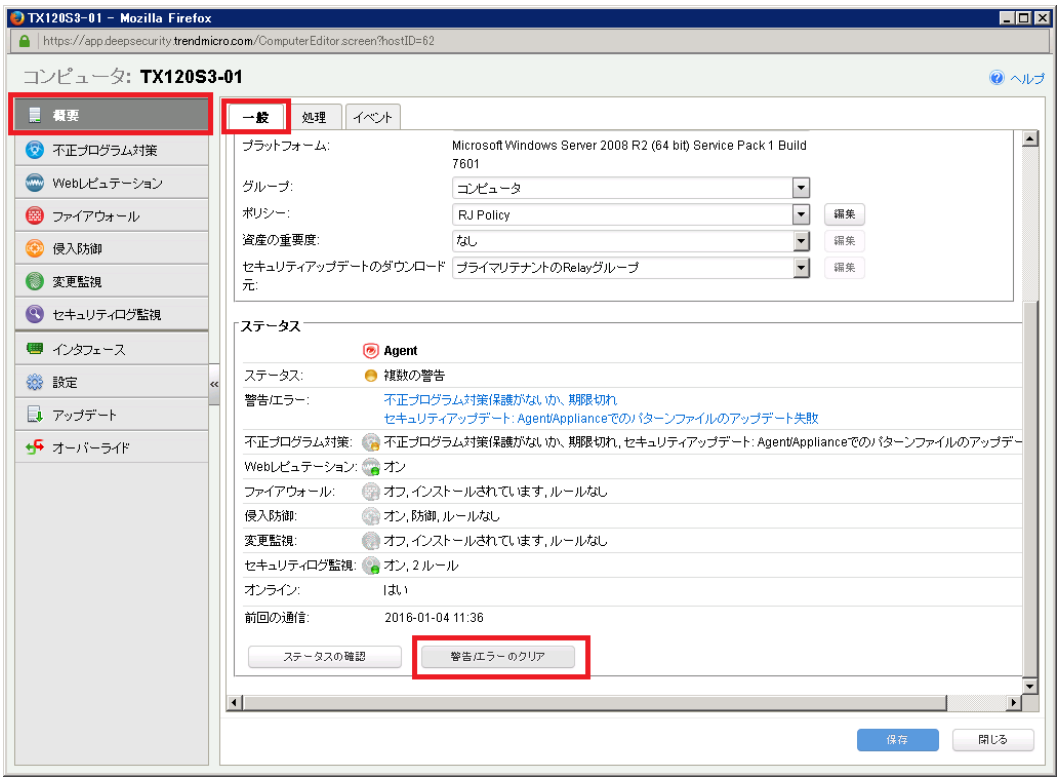


4. Trend Micro Deep Security Agent サービスの再起動を行います。
OS のサービス画面から[Trend Micro Deep Security Agent]サービスを選択し、右クリックのメニューから[再起動]を選択します。

※ サービス画面を見つけにくい場合、[Windows]+[R]キーを押し、[ファイル名を指定して実行]画面で、[名前]に[services.msc]と入力して[OK]で呼び出すのが便利です。



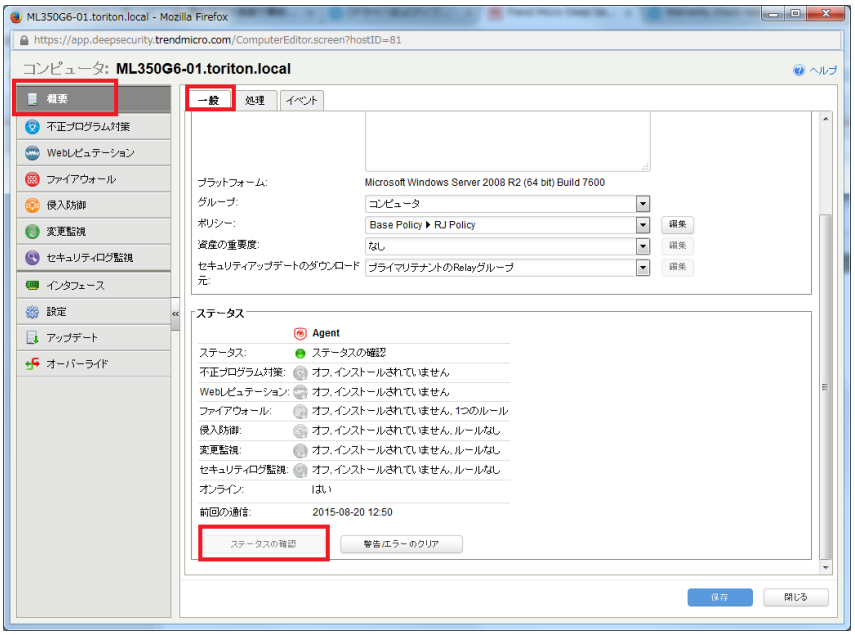
5. Deep Security Manager で[警告/エラーのクリア]を実施します。
[コンピュータ]タブで登録したサーバをダブルクリックし、詳細画面を開き、[概要]-[一般]タブの[警告/エラーのクリア]をクリックします。



6. 画面が更新され、ステータス欄で[ステータス]が管理対象(オンライン)となり、警告/エラーの項目が消えたことを確認します。

7. ステータスが[管理対象(オンライン)]となれば、インストール正常終了の確認が完了です。

※ ステータスが[セキュリティアップデートの実行中]や[管理対象(オフライン)]となった場合、10 分ほどおいてから[ステータスの確認]をクリックし、管理対象(オンライン)となるかを確認してください。

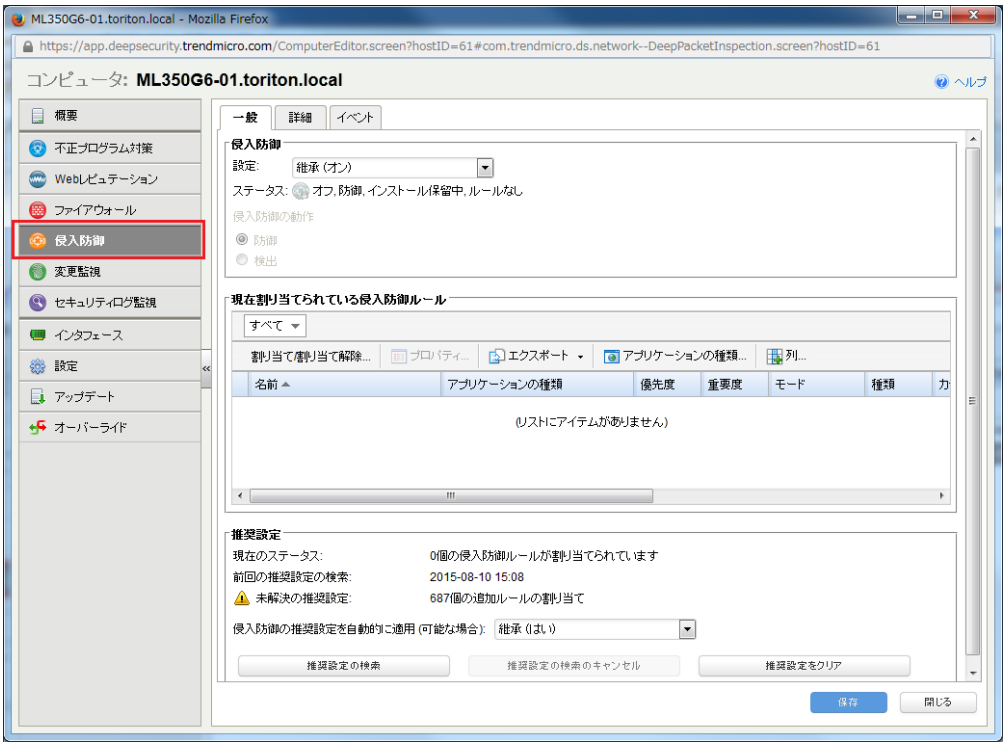


8. 以上で正常終了の確認は完了です。初回手動検索を開始するため、次章の手順を実施します。

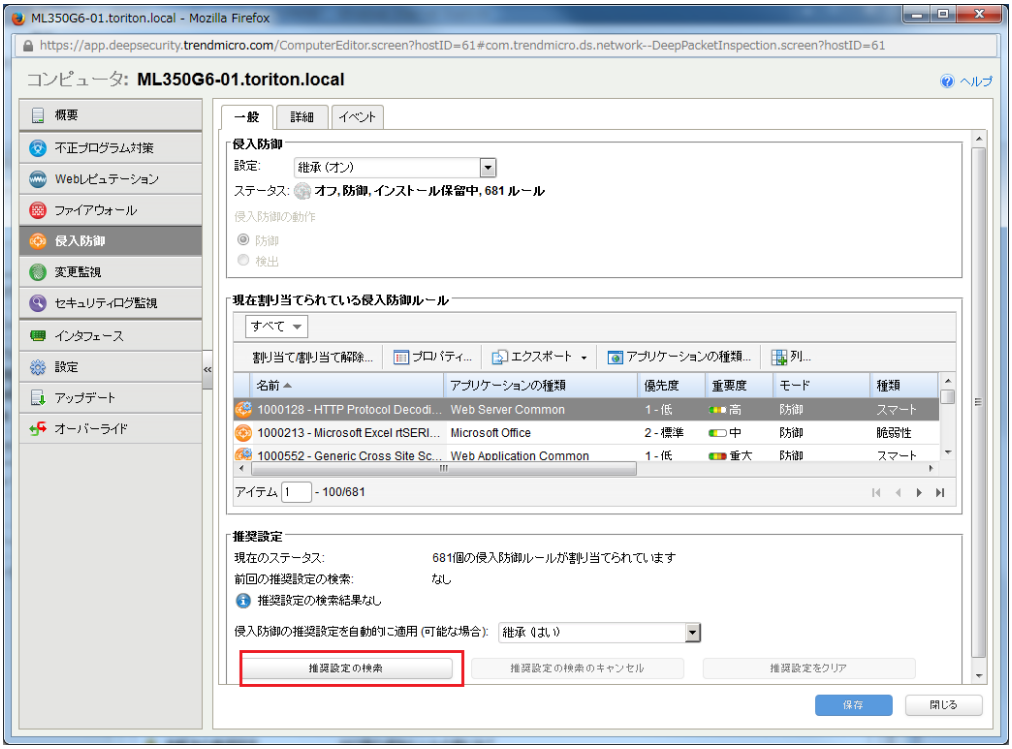
4.2. 手動検索の実施

1. Deep Security Managerの[コンピュータ]タブを開き、登録したコンピュータをダブルクリック、または右クリックからのメニューで[詳細]を開きます。

2. [侵入防御]をクリックします。

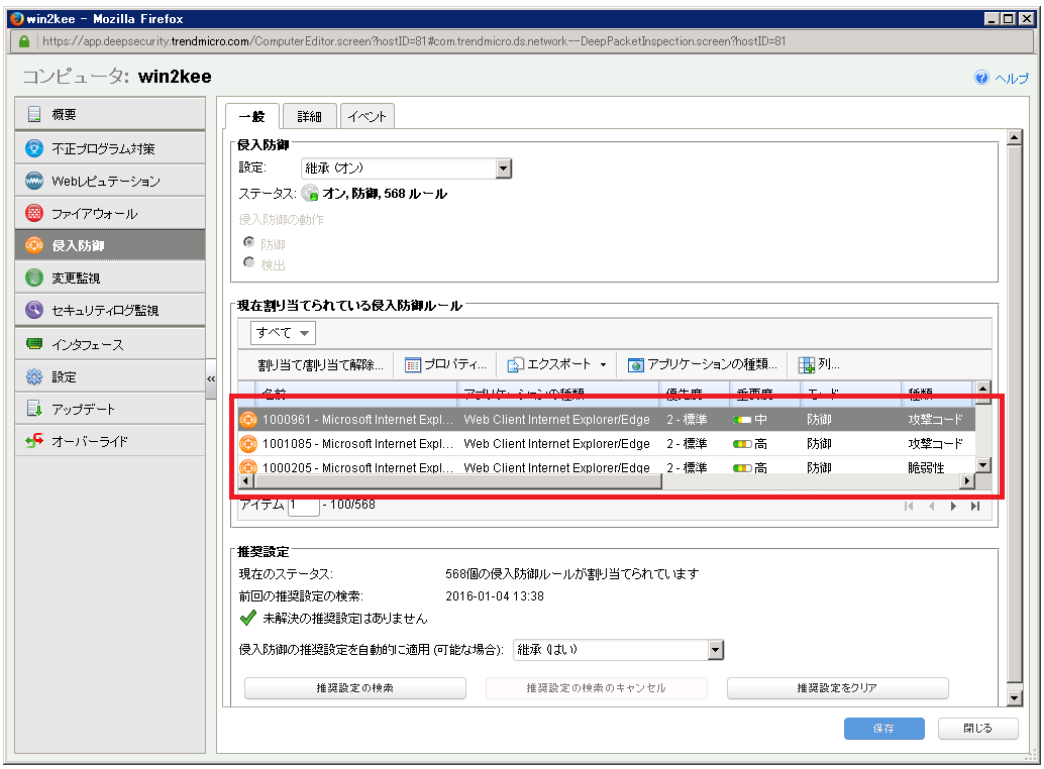


3. [推奨設定の検索]をクリックします。

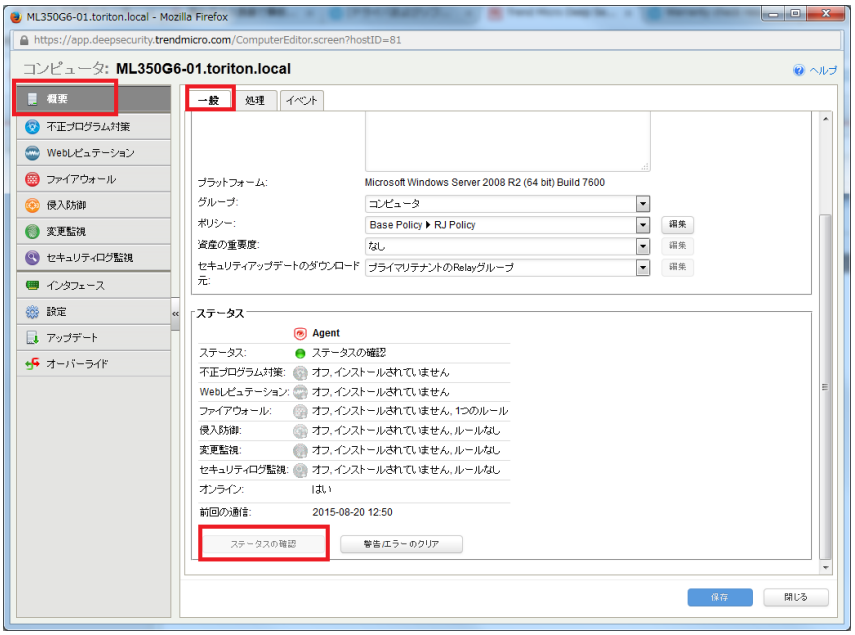


※ 環境により割り当てられるルールが多くなり、検索に 10 分以上がかかる場合があります。

4. 現在割り当てられている侵入防御ルールのリストにルールが追加されたことを確認します。



5. [概要]-[一般]タブの[ステータスの確認]をクリックし、ステータスを更新します。



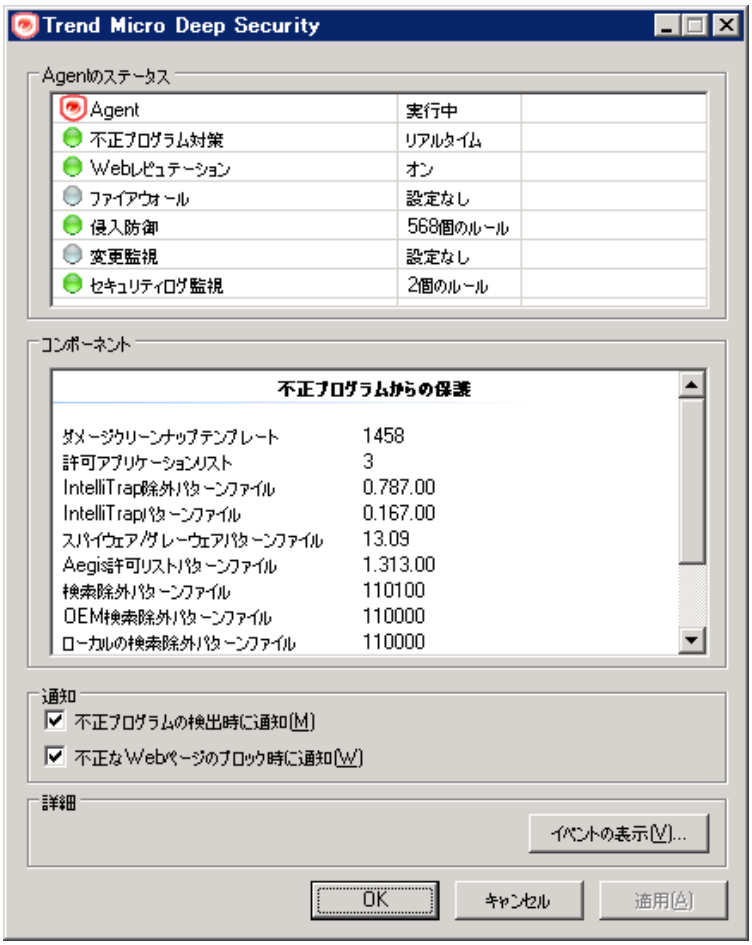
※ ステータスに警告やエラーが出た場合、[警告/エラーのクリア]をクリックし、再度[ステータスの確認]をクリックしてください。

※ ステータスの確認中は、[ステータスの確認]はグレーアウトしクリックできません。

6. ステータスが以下状態になったことを確認します。
   - ステータスが[管理対象(オンライン)]である
   - 以下 4 つの項目が[オン]である
     ① 不正プログラム対策
     ② Web レピュテーション
     ③ 侵入防御
     ④ セキュリティログ監視

7. [閉じる]ボタンで詳細画面を閉じます。

8. サーバの画面右下のタスクバーで[Trend Micro Deep Security]アイコンをダブルクリックし、開いた画面で Agent が[実行中]であり、以下 4 つの項目に緑の丸がついていることを確認します。
   ① 不正プログラム対策
   ② Web レピュテーション
   ③ 侵入防御
   ④ セキュリティログ監視



9. 管理画面とエージェント画面を閉じて、初回の手動検索は完了です。
※管理画面は Web ブラウザの×で閉じて問題ありません。

✓ 本作業にて Deep Security マネージャ画面にて対象コンピューターが管理対象であることの確認が取れました。

以上で、クラウドサービス ｆｏｒ サーバーセキュリティの導入作業は終了です。