

# Trend Micro Deep Security™ as a Service インストールガイド (仮想パッチ、不正プログラム対策初期設定指南付き)

トレンドマイクロ株式会社

Last Update : 2017/3/3



当資料は  
2017年3月3日現在の情報となります

# はじめに

- このたびは、Trend Micro Deep Security™ as a Service (以下、DSaaSと言います)をご検討頂きまして、誠にありがとうございます。
- 本資料は、DSaaSのインストール手順および、仮想パッチ自動適用設定・不正プログラム対策設定の手順を記載しております。記載内容に沿ってぜひDSaaSをご利用ください。
- 本資料は、DSaaSのインストールを行って頂くための手引書となります。そのため、設定については初期段階の説明までとなり、全ての機能詳細について記載されておられません。詳細はDSaaS管理コンソールのヘルプおよび、別資料「Trend Micro Deep Security as a Service レビューアーズガイド」をご参照ください。(別資料はDSaaSパートナーまたは当社までお申し付けください。)
- DSaaSは、弊社クラウド側セキュリティサービス「Trend Micro Security as a Service」として、弊社サービス提供パートナーから提供されます。サービス提供パートナーは、以下Webページからご確認ください。

<http://www.trendmicro.co.jp/jp/business/solutions/saas/#>

# 本資料における言葉の定義

DSaaS	Trend Micro Deep Security™ as a Serviceの略称です。
DSaaSコンソール	DSaaSの各種設定を行うためのコンソールです。 お客さまのPCからWebブラウザ経由でログインいただきます。
DSaaS管理マネージャ (DSM)	DSAを管理する管理サーバです (DSM) DSaaSでは、トレンドマイクロがクラウド上でホストしています。
DSA	Deep Security エージェントの略称です。 DSAは保護対象のサーバOSにインストールします。
AC (アクティベーションコード)	製品機能を有効化するActivation Code (アクティベーションコード) です。ACは、DSaaS提供パートナーから発行されます。

# 作業を始める前にご確認ください (ご利用における留意点)

DSaaSは、クラウド型のセキュリティサービスです。  
インターネット側への接続確保が必須になるなど、一部パッケージ版  
Deep Securityとはシステム要件が異なります。詳細は以下をご確認ください。

- DSaaSで提供しているDSAのシステム要件は、こちらを参照してください
  - <http://www.trendmicro.co.jp/jp/business/products/tmdsaas/index.html#requirement>
- DSAをインストールするサーバから、DSaaS管理マネージャにアクセスできることをご確認ください
  - agents.deepsecurity.trendmicro.com:443
  - relay.deepsecurity.trendmicro.com:443
  - FAQ : (<http://esupport.trendmicro.com/solution/ja-JP/1104586.aspx>)
- プロキシサーバを経由する際の認証は、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。
- プロキシサーバを経由する場合など、設定の詳細についてはDSaaSコンソール上のオンラインヘルプをご参照ください
- DSAをインストールするサーバにおいて、ネットワークの一時的な切断、またはOSのNWドライバーが他のプログラムによってロックされている場合、OSの再起動が求められる場合があります
- DSaaSのUIの一部、通知メールなどが英語で表記されております、ご了承ください (詳細はこのあとのスライドでご説明いたします)
- DSaaSで提供される機能の一部は日本ではサポートされないものが含まれております、ご了承ください (詳細はこのあとのスライドでご説明いたします)

# 本資料の構成

1. DSaaS アカウントの作成
2. DSaaSコンソールへのログインと利用開始の準備
3. DSAのインストール
4. 仮想パッチ自動適用設定
5. 不正プログラム対策設定
6. 参考資料
7. よくあるご質問と回答集 (FAQ)

# DSaaS構成概要

トレンドマイクロ データセンタ

Deep Security Manager (DSM)

➢ DSaaS管理マネージャ



トレンドマイクロがホストする  
DSaaS管理用サーバ

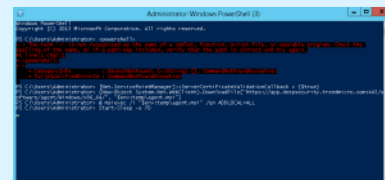
お客さま環境

Deep Security Agent (DSA)

➢ Deep Security エージェント



インストール作業時、  
DSaaS保護対象サーバ側の  
作業が発生します。



お客さま(運用管理者)

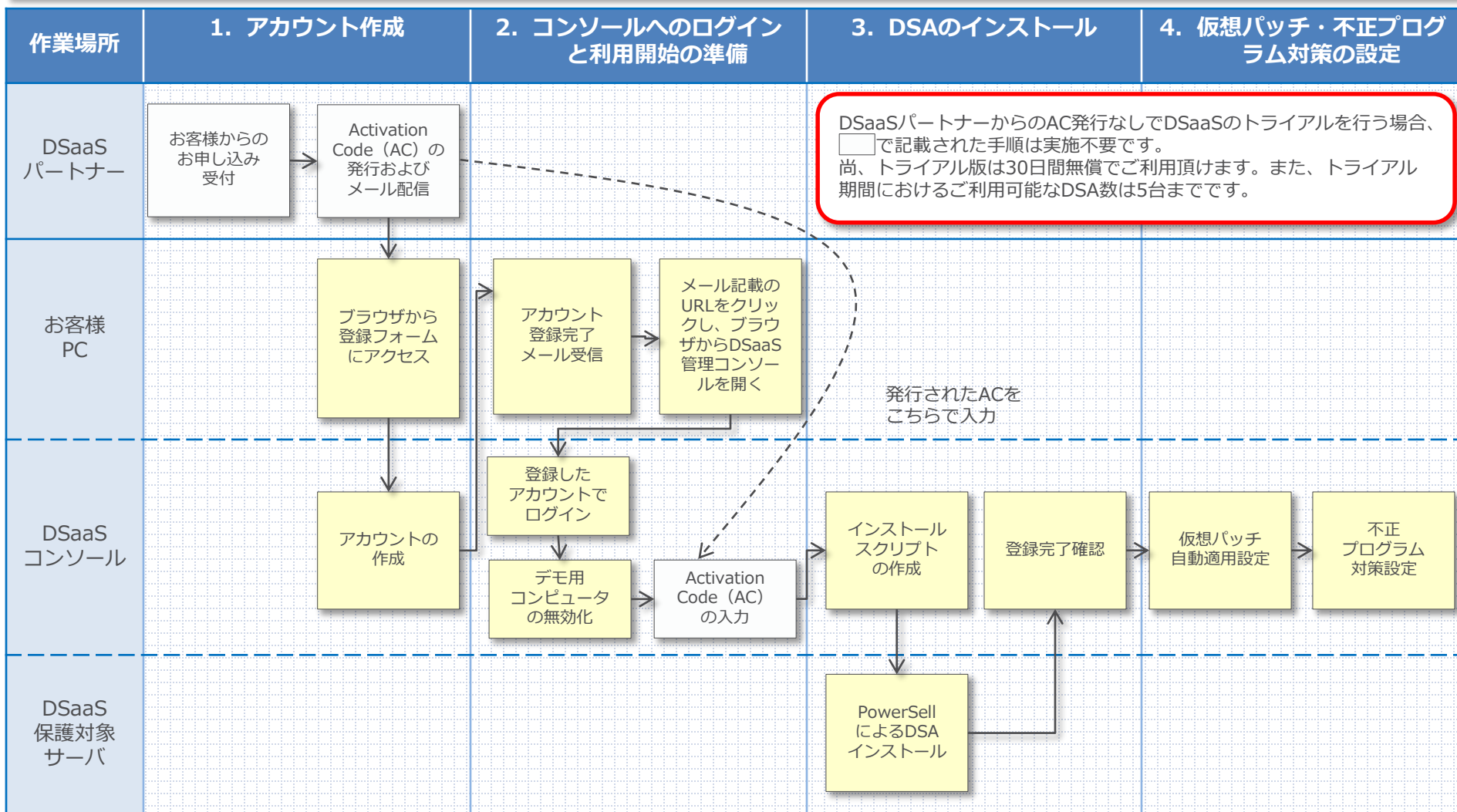
エージェントの死活監視、  
ログの確認等の日常運用

DSaaSの各種設定および日常の運用は、  
トレンドマイクロがホストするDSaaS  
管理マネージャにログインして行います。

但し、インストール作業時はDSaaS保  
護対象サーバ側での作業が発生します。

# インストール作業の全体像

本資料でご紹介しておりますインストール作業の全体像を以下に記載します。  
各作業の詳細内容は次ページ以降をご参照ください。



# 1. DSaaS アカウントの作成

- ①登録フォームへのアクセス
  - ②アカウントの作成
-



# AC (アクティベーションコード)の取得

ライセンス追加時にライセンス担当者様宛にメールが届きます。  
本メールに記載されたAC (アクティベーションコード) は今後の作業で使用しますので、大切に保管してください。

件名

[Deep Security as a Service (各DSaaSパートナーごとのサービス名)] - ライセンス追加のご連絡

メール本文

#Customer company name#様

この度は、「Deep Security as a Service (各DSaaSパートナーごとのサービス名)」のお申込みを頂きましてありがとうございます。

サービスプラン： Deep Security as a Service (各DSaaSパートナーごとのサービス名) のご契約ライセンスが新規追加されましたのでお知らせいたします。

ライセンス数： ライセンス数

アクティベーションコード： **○x-○○x△-△○x○□-xx□△○-△□x☆x-△○□xx-△□☆x○**

製品またはサービスの管理コンソールにアクティベーションコードを入力し、アクティブ化の手続きを完了してください。

# ①登録フォームへのアクセス

登録ページは、以下URLとなり、  
こちらが登録フォームとなっており、  
まず、こちらからアクセスいただきます。

<https://app.deepsecurity.trendmicro.com/SignIn.screen>

こちらの  
“Create an Account”  
をクリックいただき、  
登録フォームを開いてくださ  
い。

## ② トライアル版アカウントの作成

“Create an Account”をクリックすると、トライアル版登録フォーム(Free Trial)が開きますので、必要事項を入力しアカウントを作成してください。

First Name:

← アカウント作成者の名を入力してください。  
半角英数字で登録されることを推奨いたします。

Last Name:

← アカウント作成者の姓を入力してください。  
半角英数字で登録されることを推奨いたします。

Company/Account:

← DSaaS管理コンソールへの**Account Name(ログインID)**となります。  
半角英数字で登録されることを推奨いたします。なお、アカウント登録後に変更することはできません。

Email:

← お客様の連絡先用emailアドレスを入力ください。これが管理コンソールへの**Username**となります。  
なお、DSaaS管理コンソールログイン後に変更可能です。

Password:

← DSaaS管理コンソール用**パスワード**(英数字、大文字小文字の組み合わせ)を設定し、入力してください。設定したパスワードが条件を満たしている場合**“Acceptable”**と表示されます。※1

Confirm Password:

Password Strength:

No Password

Country:

← “Japan”を選択してください。

Language:

← “Japanese”を選択してください。

Time Zone:

← “(UTC+9.00) Japan Standard Time”を選択してください。

Sign Up

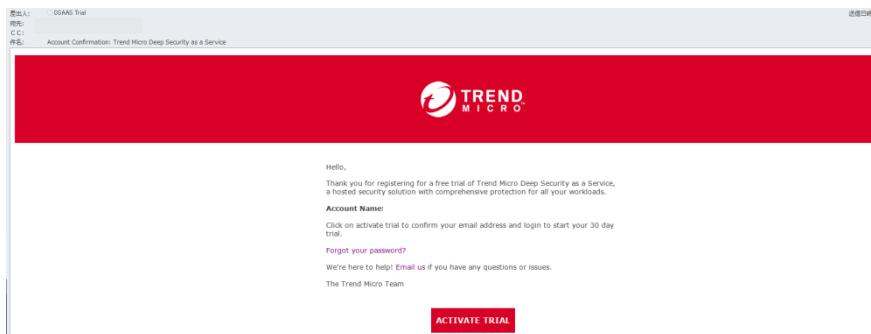
← 必要事項を入力したら、  
**“Sing Up”**をクリックしてください。

※1 “Password Strength” その他の表示

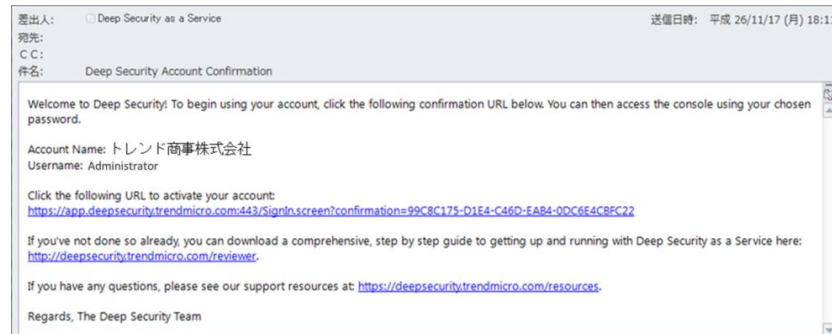
- No Password : パスワードが入力されていない
- Weak : 設定したパスワードが条件を満たしていない
- Password Mismatch : 確認用パスワードが一致しない

# アカウント登録完了メールが届く

15分ほどでアカウント登録完了メールが届きます。  
メール本文のURLからアカウントのアクティベーションを行ってください。



or



メールタイトル	配信時期(目安)	説明
Account Confirmation: Trend Micro Deep Security as a Service	アカウント作成後、 <b>約15分後</b>	メール下部の“ACTIVATE TRIAL”をクリックしてDSaaS管理コンソールにログインしてください。 メール送信元 : <a href="mailto:dsaas_trial@trendmicro.com">dsaas_trial@trendmicro.com</a>

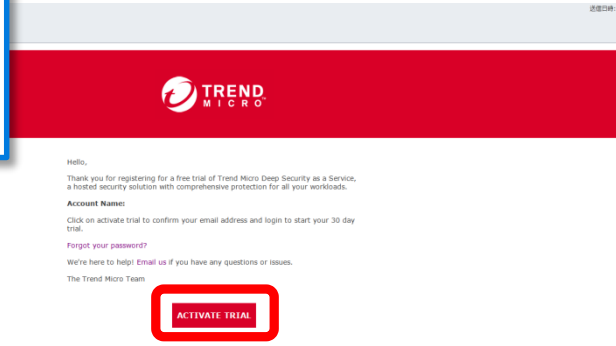
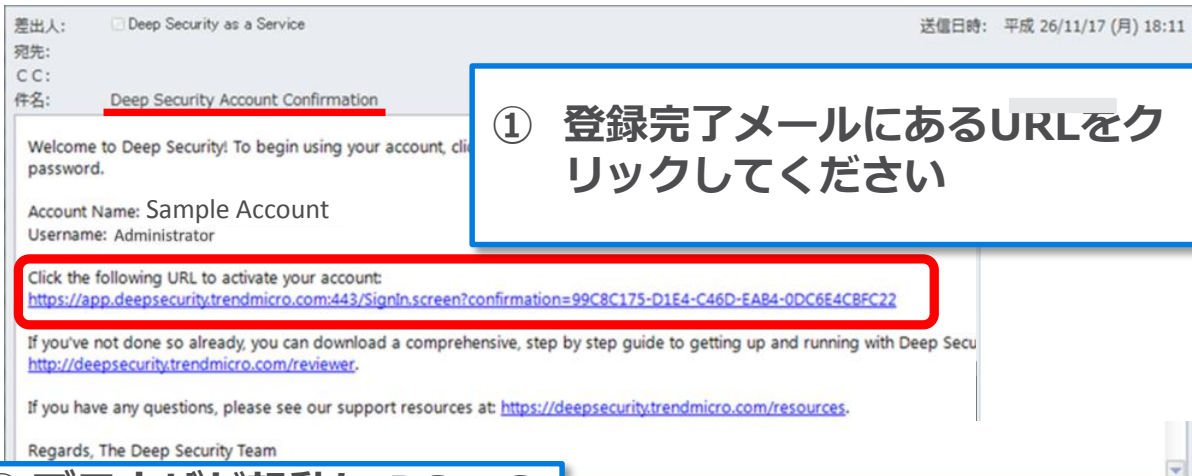


それではDSaaSにログインしてみましょう！

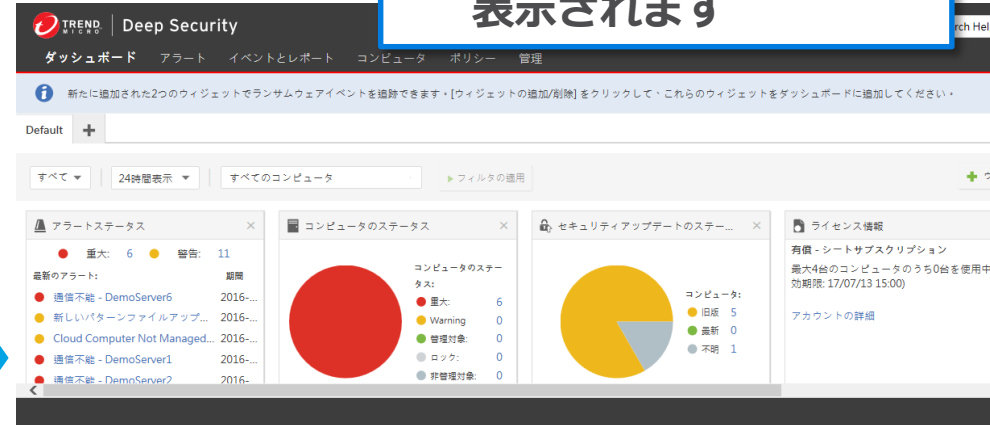
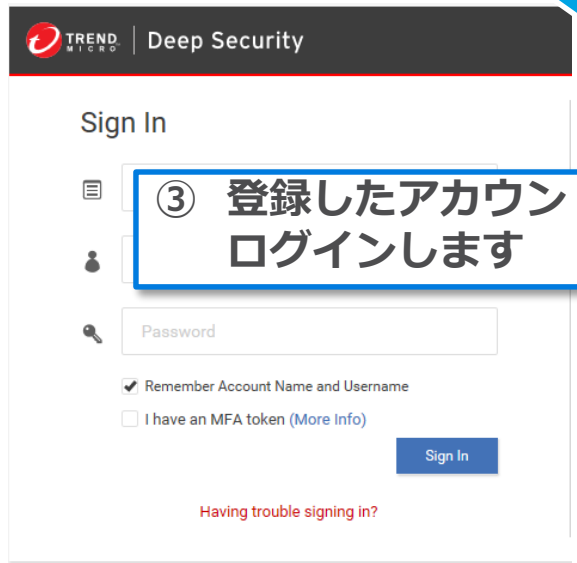
## 2. DSaaSコンソールへのログインと 利用開始の準備

- ①DSaaSコンソールへのログイン
  - ②デモ用コンピュータの無効化および削除
  - ③Activation Code (AC) の入力
-

# ① DSaaSにログインする



② ブラウザが起動し DSaaS  
コンソールが開きます



## ログインできましたか？

## ② デモ用コンピュータの無効化および削除

新規登録をすると、DSaaSのデモ用コンピュータが用意されています。本トライアルでは使用しませんので、ご利用いただく前にデモ用コンピュータの無効化をお願いいたします。

1. コンピュータタブに移動

2. 対象サーバを右クリック

3. ステータスが「非管理対象」になっていれば無効化完了

4. 対象サーバを右クリック

↑ [処理]を選択

↑ [無効化]を選択

↑ 実利用時は[削除]を選択

### 無効化の手順

1. “コンピュータ”タブに移動する
2. 対象のサーバを選択し、右クリック-[処理]-[無効化]を選択する
3. “ステータス”の部分が“非管理対象”となっていたら無効化完了です
4. 本デモコンピュータも1台とカウントされますので、実際の利用時には対象サーバを選択し右クリック[削除]を選択しコンピュータを削除して下さい。

デモ用コンピュータの詳細は、本資料“参考資料”内の「DSaaS: デモコンピュータの紹介」をご参照ください。

# ③ Activation Code (AC) の入力

DSaaSパートナーから発行されるActivation Code (AC) を入力します。

1. Activation Code (AC) が記載されたメールが届きます。次の作業で使用しますので、アクティベーションコードをコピーしてください。

件名: [Deep Security as a Service (各DSaaSパートナーごとのサービス名)] - ライセンス追加のご連絡

メール本文:  
#Customer company name#様

この度は、「Deep Security as a Service (各DSaaSパートナーごとのサービス名)」のお申込みを頂きましてありがとうございます。

サービスプラン: Deep Security as a Service (各DSaaSパートナーごとのサービス名) のご契約ライセンスが新規追加されましたのでお知らせいたします。

ライセンス数: ライセンス数

アクティベーションコード: ○×-○○×△-△○×○□-××□△○-△□×☆×-△○□××-△□☆×○

製品またはサービスの管理コンソールにアクティベーションコードを入力し、アクティブ化の手続きを完了してください。



2. DSaaSコンソールから[アカウント名]→[アカウントの詳細]をクリックします。



3. [アカウントの詳細]が開きますので、[有償版にアップグレード]をクリックします。



4. [有償版のDeep Security as a Service にアップグレード]が開きますので、[アクティベーションコードの入力]欄に上記1.でコピーしたアクティベーションコードをペーストして[OK]を押します。

Activation Codeはコピー・アンド・ペーストで入力することが可能です。

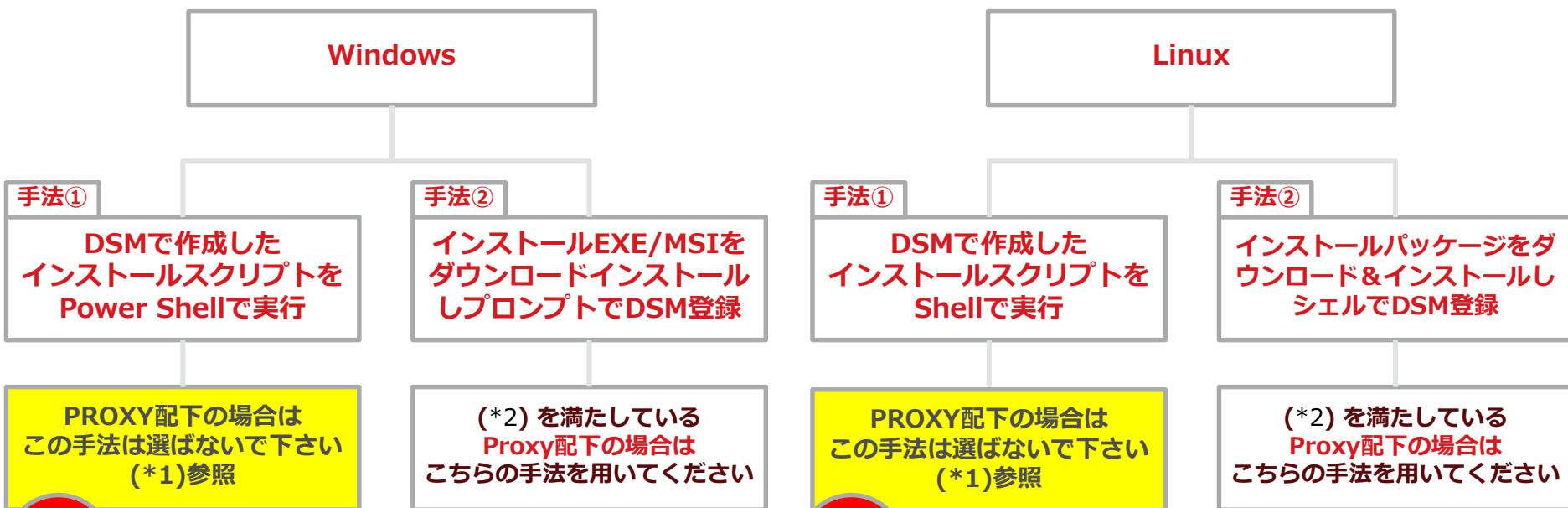


# 3. DSAインストール

---

# インストール手法の選択肢

保護対象サーバがWindows/Linuxの場合、それぞれ2種類のインストール&DSM登録手法があります。



(\*1): Deep Security Agent(以下、DSA)9.5がDeep Security Relayに接続する際にProxyを必須とする環境での問題点について

<http://esupport.trendmicro.com/solution/ja-jp/1110288.aspx>

(\*2): プロキシの認証で使えるのはBasic認証のみです。

Digest認証とNTLM認証はサポートされておりません。

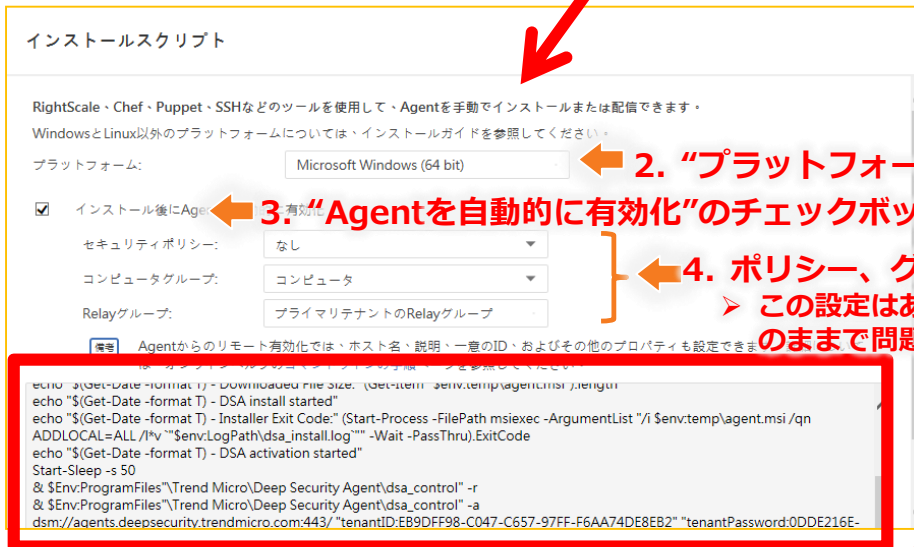
## Windows 手法① DSMで作成したインストールスクリプトをPower Shellで実行

# ① インストールスクリプトの作成

保護対象サーバにDSAをインストールするための、インストールスクリプトを作成します。(インストールスクリプトは、PowerShell上で使用します。)



1. 管理コンソールにログインし、右上の[サポート情報]-[インストールスクリプト]を選択します。



2. "プラットフォーム"から、インストール対象のOSを選択します。

3. "Agentを自動的に有効化"のチェックボックスをオンにします。

4. ポリシー、グループ、Relay、それぞれに左記のとおり選択します。  
➤ この設定はあとから再設定できます。すでに設定済みの設定が無い場合には初期設定のままでも問題ありません。

5. 赤枠に表示されたスクリプトをコピーします。  
➤ コピーしたスクリプトは、次ページの「② PowerShellによるDSAインストール」でペーストして実施させます。



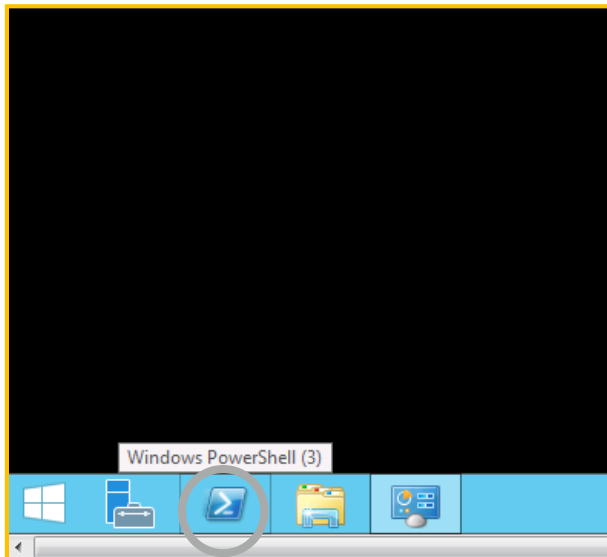
スクリプトが改行された状態でペーストすると、PowerShellで実行されない場合がありますのでご注意ください。

## ② PowerShellによるDSAインストール

本作業は保護対象サーバ上での作業となります。

作成したインストールスクリプトを保護対象サーバのPowerShell上で実施し、保護対象サーバにDSAをインストールします。

1. DSAをインストールする保護対象サーバにアクセスし、タスクトレイからPowerShellを起動します。
2. PowerShellコンソール上で、前ページ「①インストールスクリプトの作成」で作成し、インストールスクリプトを1行ずつペーストします。
3. スクリプトが起動してインストールが始まります
4. このスクリプトは、DSAのインストールビルドモジュールのダウンロード、インストール、管理サーバへの登録までを自動で行います、インストールが完了したらDSaaS管理サーバに対象サーバが登録されているか確認を行います



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.

PS C:\Users\DSaaS> $env:LogPath = "$env:appdata\Trend Micro\Deep Security Agent\installer"
PS C:\Users\DSaaS> New-Item -path $env:LogPath -type directory

Directory: C:\Users\DSaaS\AppData\Roaming\Trend Micro\Deep Security Agent

Mode                LastWriteTime         Length Name
----                -
d----             2/18/2016   6:04 AM             installer

PS C:\Users\DSaaS> Start-Transcript -path "$env:LogPath\dsa_deploy.log" -append
Transcript started, output file is C:\Users\DSaaS\AppData\Roaming\Trend Micro\Deep Security Agent\installer\dsa_deploy.log
PS C:\Users\DSaaS> echo "$(Get-Date -format T) - DSA download started"
6:04:04 AM - DSA download started
PS C:\Users\DSaaS> (New-Object System.Net.WebClient).DownloadFile("https://app.deepsecurity.trendmicro.com:443/software/agent/windows/x86_64/", "$env:temp\agent.msi")
```

### ③ Deep Securityマネージャへの登録完了確認

正しく有効化が行われれば、DSAがDSaaSコンソール上で“管理対象”と表示されます。

コンピュータ

サブグループを含む ▼ グループ別 ▼

AWSアカウントの追加 新規 ▼ 削除... 詳細... 処理 ▼ イベント ▼ エクスポート ▼

名前 ▲	説明	プラットフ...	ポリシー	ステータス
▼ コンピュータ (1)				
54.70.61.125	このコンピュータは、Deep Se... Amazon Linu... Demo			● セキュリティアップデ... 2
DemoServer1				● 管理対象

↑ 2. DSAをインストールした保護対象サーバが、“管理対象”と表示されていればOK

これで、インストール作業は完了です。



## Windows 手法②

### インストールEXE/MSIをダウンロードインストールしプロンプトでDSM登録

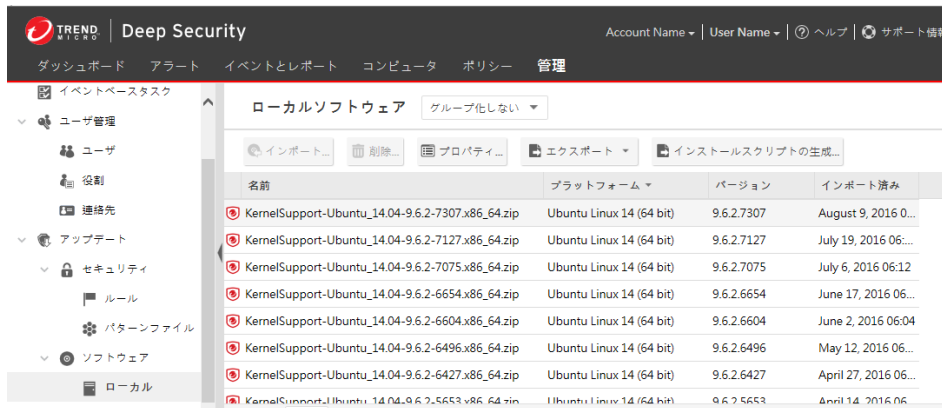
Proxy配下にインストールする場合はこちらの手法を用いてください。

# ①インストールファイルをダウンロードする

DSaaSのDSMコンソールからインストールファイルをダウンロードして下さい

1.管理コンソールで[管理]-[アップデート]-[ソフトウェア]-[ローカル]を開き、該当OSの最新Versionを選択

2.インストールするパッケージを選択し[エクスポート]でファイルをダウンロードしてください





## ② インストールファイルで保護対象OSにインストールする

エクスポート（ダウンロード）したファイルを使って  
DSAをインストールします

3. エクスポートしたzipファイルをインストール対象マシンにコピーし、任意のパスで解凍します。
4. 解凍したフォルダに保存されている "\*\*\*.msi" をクリックしインストールを実施します。

名前	種類	サイズ	更新日時	作成日時
META-INF	ファイルフォル...		2015/08/06 11:24	2015/08/
Agent-Core-Windows-9.5.3-4017.i38...	Windows インス...	12,564 KB	2015/07/30 0:30	2015/07/
Agent-Windows-9.5.3-4017.i386.zip	WinZip File	45,932 KB	2015/08/06 11:23	2015/08/
*+ Feature-AM-Windows-9.5.3-4017.i38...	VC++ 6 Project	28,711 KB	2015/07/30 0:24	2015/07/
*+ Feature-DPI-Windows-9.5.3-4017.i3...	VC++ 6 Project	1 KB	2015/07/30 0:24	2015/07/
*+ Feature-FW-Windows-9.5.3-4017.i38...	VC++ 6 Project	1 KB	2015/07/30 0:24	2015/07/
*+ Feature-IM-Windows-9.5.3-4017.i38...	VC++ 6 Project	257 KB	2015/07/30 0:24	2015/07/
*+ Feature-LI-Windows-9.5.3-4017.i386...	VC++ 6 Project	136 KB	2015/07/30 0:24	2015/07/
*+ Feature-WRS-Windows-9.5.3-4017.i...	VC++ 6 Project	491 KB	2015/07/30 0:24	2015/07/
*+ Plugin-Filter-Windows-9.5.3-4017.i38...	VC++ 6 Project	1,276 KB	2015/07/30 0:24	2015/07/
*+ Plugin-FWDPI-Windows-9.5.3-4017.i...	VC++ 6 Project	138 KB	2015/07/30 0:24	2015/07/
*+ Plugin-Update-Windows-9.5.3-4017.i...	VC++ 6 Project	2,352 KB	2015/07/30 0:24	2015/07/



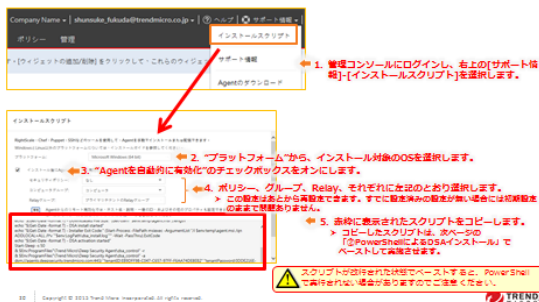
# ③ インストールスクリプトからDSM登録コマンドを抜き出し プロンプトで実行できるように加工する

## プロンプトで実行するスクリプトを作ります

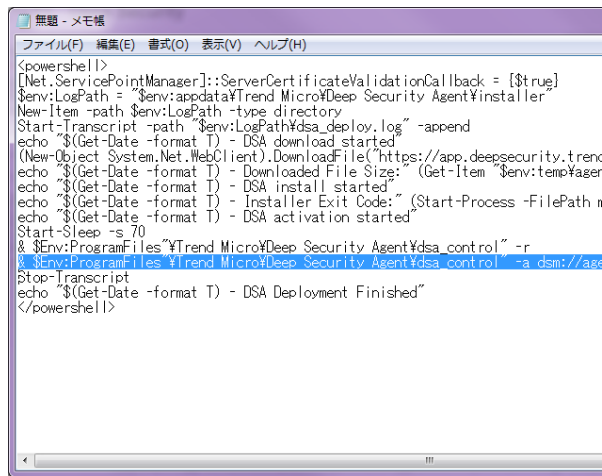
1. Windows 手順①-①でスクリプトを生成し、メモ帳などにコピー＆ペースト

### ①インストールスクリプトの作成

保護対象サーバにDSAをインストールするための、インストールスクリプトを作成します。(インストールスクリプトは、PowerShell上で使用します。)



2. dsa\_constol -aが含まれる行を取り出す



3. 取り出した1行がこちら↓

```
& $env:ProgramFiles%\Trend Micro\Deep Security Agent\dsa_control" -a dsm://agents.deepsecurity.trendmicro.com:443/"tenantID:<テナントのID>" "tenantPassword:<テナントのパスワード>"
```

4. dsa\_controlより先を削除し、control"の"を削除

```
dsa_control -a dsm://agents.deepsecurity.trendmicro.com:443/"tenantID:<テナントのID>" "tenantPassword:<テナントのパスワード>"
```

これがプロンプトで実行する、DSM登録(有効化)のコマンドになります  
注意：dsa\_control -a の間に"がないことを確認してください  
注意：テナントIDとテナントパスワードは、DSaaSのDSMから、各アカウント毎に生成してください。

# ④プロンプトを使って、DSAをDSMに登録する

プロンプトでDSM登録コマンドを実行し登録する  
 ＊Proxy配下の場合は2の手順を実施

1.プロンプトを起動し、DSAのフォルダに移動  
 dsa\_control.cmdを利用します

3. 抽出した1行を実行  
 →DSM登録

```
dsa_control -a
dsm://agents.deepsecurity.trendmicro.com:443/
"tenantID: <テナントのID>" "tenantPassword: <テナントのパスワード>"
```

```
管理者: コマンド プロンプト
c:\Program Files\Trend Micro\Deep Security Agent>dir *cmd
ドライブ C のボリューム ラベルがありません。
ボリューム シリアル番号は F42A-0C8D です

c:\Program Files\Trend Micro\Deep Security Agent のディレクトリ

2014/06/18 12:17          221 dsa_control.cmd
2013/11/12 13:40           92 dsa_query.cmd
2013/11/12 13:39           92 sendCommand.cmd

           3 個のファイル              405 バイト
           0 個のディレクトリ      30,576,906,240 バイトの空き領域
```

```
管理者: コマンド プロンプト
c:\Program Files\Trend Micro\Deep Security Agent>dsa_control -a dsm://agents.deepsecurity.trendmicro.com:443/
tenantPassword:
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 'GetComponentInfo' 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.
Received a 'UpdateComponent' command from the manager.
Command session completed.
```

2. PROXY配下の場合は下記コマンドを実行してProxy

```
を登録
c:\Program Files\Trend Micro\Deep Security Agent>dsa_control -x "dsm_proxy://192.168.2.103:8080/"
HTTP Status: 200 - OK
Response:
Add proxy-address:[dsm_proxy] with value:[192.168.2.103:8080/]
```

**【注意！】このアドレスは例ですので  
 お客様の環境にあわせて入力してください**

構文	備考
dsa_control -x "dsm_proxy://<プロキシサーバのURL>/"	AgentがManagerとの通信に使用するプロキシサーバのアドレスを設定します。
dsa_control -x ""	プロキシサーバのアドレスをクリアします。
dsa_control -u "<ユーザ名:パスワード>"	プロキシサーバのユーザ名とパスワードを設定します。
dsa_control -u ""	プロキシサーバのユーザ名とパスワードをクリアします。

Proxy認証でユーザ/パスワードがある場合は -Uを使って登録してください

＊注意：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**

```
dsa_control -u "root:Passw0rd!"
```

プロキシの認証に、「root」とパスワード「Passw0rd」を使用します（基本認証のみ。Digest認証とNTLM認証はサポートされていません）。

## ⑤ Deep Securityマネージャへの登録完了確認

正しく有効化が行われれば、DSAがDSaaSコンソール上で“管理対象”と表示されます。

コンピュータ ← 1. コンピュータタブに移動

コンピュータ    サブグループを含む    グループ別

AWSアカウントの追加    新規    削除...    詳細...    処理    イベント    エクスポート

名前	説明	プラットフォーム	ポリシー	ステータス
▼ コンピュータ (1)				
54.70.61.125	このコンピュータは、Deep Se... Amazon Linu... Demo			● セキュリティアップデート... 2
DemoServer1				● 管理対象

↑ 2. DSAをインストールした保護対象サーバが、“管理対象”と表示されていればOK

これで、インストール作業は完了です。

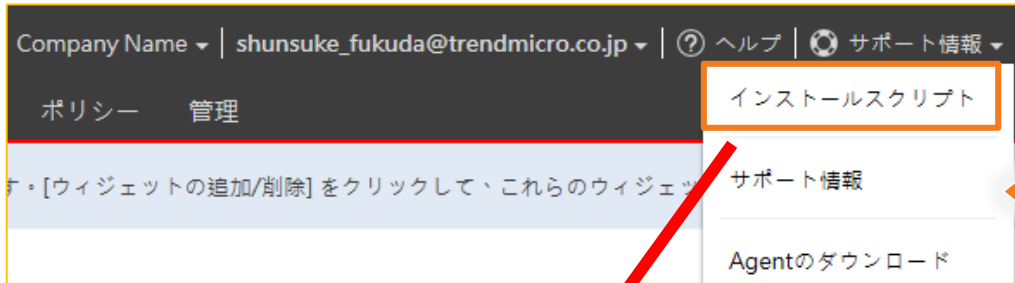


## Linux 手法①

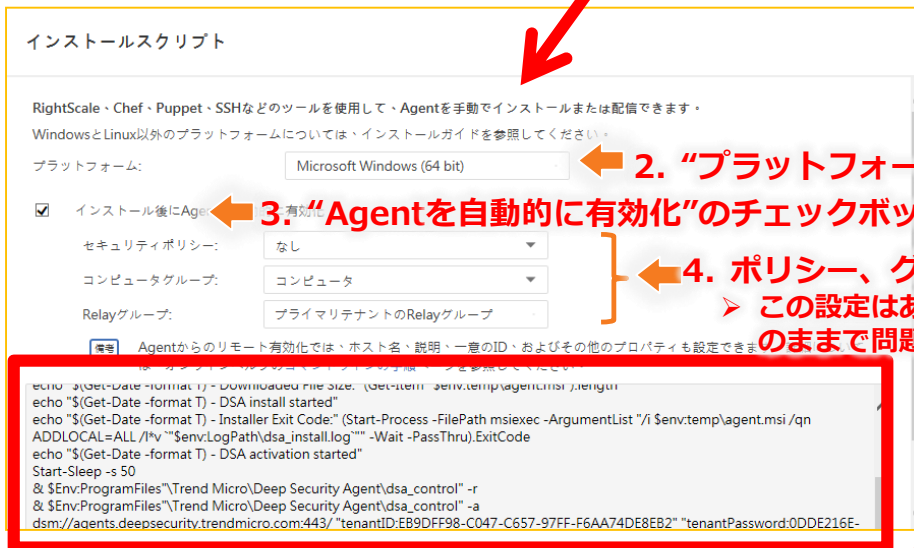
# DSMで作成したインストールスクリプトをShellで実行

# ① インストールスクリプトの作成

保護対象サーバにDSAをインストールするための、インストールスクリプトを作成します。(インストールスクリプトは、Shell上で使用します。)



1. 管理コンソールにログインし、右上の[サポート情報]-[インストールスクリプト]を選択します。



2. "プラットフォーム"から、インストール対象のOSを選択します。

3. "Agentを自動的に有効化"のチェックボックスをオンにします。

4. ポリシー、グループ、Relay、それぞれに左記のとおり選択します。  
➤ この設定はあとから再設定できます。すでに設定済みの設定が無い場合には初期設定のままです。

5. 赤枠に表示されたスクリプトをコピーします。  
➤ コピーしたスクリプトは、次ページの「② PowerShellによるDSAインストール」でペーストして実施させます。



スクリプトが改行された状態でペーストすると、PowerShellで実行されない場合がありますのでご注意ください。

# ① インストールスクリプトの作成

前頁で取得したスクリプトをshell上で実行できるようにする

1. install.sh の所有者に「実行権限」が与えられている必要があります。

```
[root@Linux02 ~]# ls -al|grep install.sh  
-rwxr-xr-x 1 root_root    392  8月 14 16:24 install.sh
```

2. 管理コンソールからインストールスクリプトを作成します。



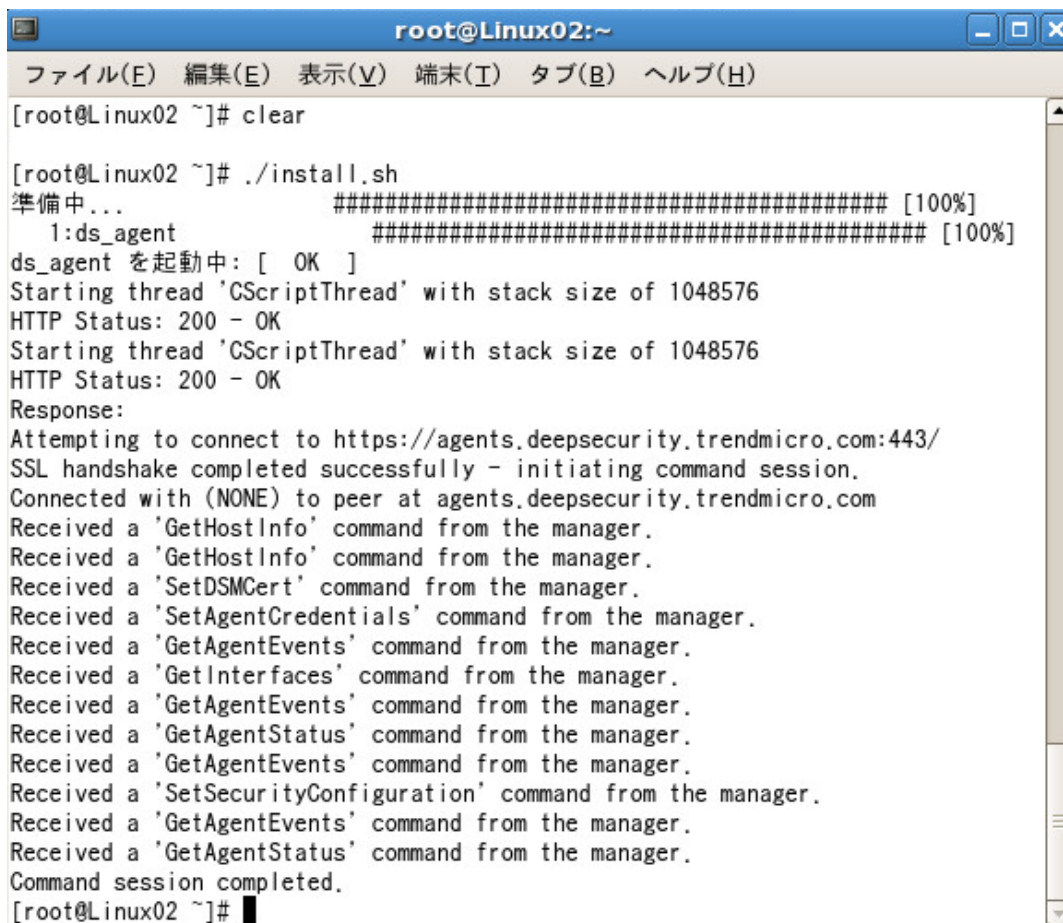
```
root@Linux02:~  
ファイル(E) 編集(E) 表示(V) 端末(T) タブ(B) ヘルプ(H)  
#!/usr/bin/env bash  
wget https://app.deepsecurity.trendmicro.com:443/software/agent/RedHat_EL5/x86_64/ -O /tmp/agent.rpm --no-check-certificate --quiet  
rpm -ihv /tmp/agent.rpm  
sleep 70  
/opt/ds_agent/dsa_control -r  
/opt/ds_agent/dsa_control -a dsm://agents.deepsecurity.trendmicro.com:443/ "tenantID:C6B3C2CC-945A-E709-8A13-81214E791239" "tenantPassword:F6BB2090-7046-1269-3FA2-227B35B34F77"  
~  
~
```

## ② ShellによるDSAインストール

本作業は保護対象サーバ上での作業となります。

作成したインストールスクリプトを保護対象サーバのShell上で実施し、保護対象サーバにDSAをインストール&DSM登録します。

### 1. スクリプトを保護対象サーバ上でroot権限で実行



```
root@Linux02:~
ファイル(E) 編集(E) 表示(V) 端末(T) タブ(B) ヘルプ(H)
[root@Linux02 ~]# clear

[root@Linux02 ~]# ./install.sh
準備中... ##### [100%]
  1:ds_agent ##### [100%]
ds_agent を起動中: [ OK ]
Starting thread 'CScriptThread' with stack size of 1048576
HTTP Status: 200 - OK
Starting thread 'CScriptThread' with stack size of 1048576
HTTP Status: 200 - OK
Response:
Attempting to connect to https://agents.deepsecurity.trendmicro.com:443/
SSL handshake completed successfully - initiating command session.
Connected with (NONE) 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.
[root@Linux02 ~]#
```



### ③ Deep Securityマネージャへの登録完了確認

正しく有効化が行われれば、DSAがDSaaSコンソール上で“管理対象”と表示されます。



1. コンピュータタブに移動

コンピュータ

サブグループを含む ▼ グループ別 ▼

AWSアカウントの追加 新規 ▼ 削除... 詳細... 処理 ▼ イベント ▼ エクスポート ▼

名前 ▲	説明	プラットフ...	ポリシー	ステータス
▼ コンピュータ (1)				
54.70.61.125	このコンピュータは、Deep Se... Amazon Linu...	Demo		● セキュリティアップデ... 2
DemoServer1				● 管理対象

↑ 2. DSAをインストールした保護対象サーバが、“管理対象”と表示されていればOK

これで、インストール作業は完了です。



## Linux 手法② インストールパッケージをダウンロード&インストールし shellでDSM登録

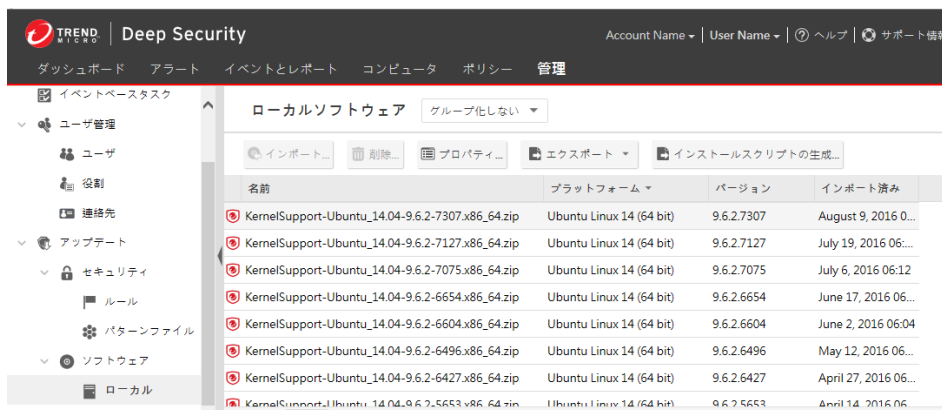
Proxy配下にインストールする場合はこちらの手法を用いてください。

# ① インストールファイルをダウンロードする

DSaaSのDSMコンソールからインストールファイルをダウンロードして下さい

1.管理コンソールで[管理]-[アップデート]-[ソフトウェア]-[ローカル]を開き、該当OSの最新Versionを選択

2.インストールするパッケージを選択し[エクスポート]でファイルをダウンロードしてください



## ② インストールパッケージを保護対象OSにインストールする

エクスポート（ダウンロード）したファイルを使って  
DSAをインストールします

1. パッケージの場合、ダウンロードしたZIPを解凍
2. RPMを使ってインストール  
# rpm -i <インストーラ名>  
例  
# rpm -i Agent-Core-RedHat\_EL5-9.5.3-4017.
3. インストールが完了するとDSAは自動的に起動します

# ③ インストールスクリプトからDSM登録コマンドを抜き出す

## プロンプトで実行するスクリプトを作ります

1. Linux 手法①-①でスクリプトを生成
2. 生成したスクリプトから赤字の部分だけ取り出す

### ①インストールスクリプトの作成

保護対象サーバにDSAをインストールするための、インストールスクリプトを作成します。(インストールスクリプトは、PowerShell上で使用します。)

1. 管理コンソールにログインし、右上の[サポート情報]-[インストールスクリプト]を選択します。

2. "プラットフォーム"から、インストール対象のOSを選択します。

3. "Agentを自動的に有効化"のチェックボックスをオンにします。

4. ポリシー、グループ、Relay、それぞれに必要のとおり選択します。  
> この設定は元々から有効な場合があります。すでに設定済みの設定が無い場合は初期値のままでも問題ありません。

5. 赤枠に表示されたスクリプトをコピーします。  
> コピーしたスクリプトは、次のステップの「PowerShellによるDSMインストール」でペーストして実行されます。

⚠ スクリプトが実行された状態でペーストすると、PowerShellで実行されない場合がありますのでご注意ください。

```
#!/usr/bin/env bash
wget
https://app.deepsecurity.trendmicro.com:443/software/agent/RedHat_EL5/i386/ -O /tmp/agent.rpm --no-check-certificate --quiet
rpm -ihv /tmp/agent.rpm
sleep 70
/opt/ds_agent/dsa_control -r
/opt/ds_agent/dsa_control -a
dsm://agents.deepsecurity.trendmicro.com:443/ "tenantID:<テナントのID>" "tenantPassword:<テナントのパスワード>"
```

# ④ shellでDSAをDSMに登録する

## shellでDSM登録コマンドを実行し登録する \* Proxy配下の場合は2の手順を実施

### 1. PROXY配下の場合は下記コマンドを実行

```
# /opt/ds_agent/dsa_control -x "dsm_proxy://<Proxy>:<port>/"
```

構文	備考
<code>dsa_control -x "dsm_proxy://&lt;プロキシサーバのURL&gt;/"</code>	AgentがManagerとの通信に使用するプロキシサーバのアドレスを設定します。
<code>dsa_control -x ""</code>	プロキシサーバのアドレスをクリアします。
<code>dsa_control -u "&lt;ユーザー名:パスワード&gt;"</code>	プロキシサーバのユーザー名とパスワードを設定します。
<code>dsa_control -u ""</code>	プロキシサーバのユーザー名とパスワードをクリアします。

Proxy認証でユーザ/パスワードがある場合は -U を使って登録してください

\* 注意：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**

```
dsa_control -u "root:Passw0rd!"
```

プロキシの認証に「root」とパスワード「Passw0rd!」を使用します（基本認証のみ。Digest認証とNTLM認証はサポートされていません）。

### 2. 前頁で作成したコマンドを実行する

```
# /opt/ds_agent/dsa_control -a "dsm://agents.deepsecurity.trendmicro.com:443/  
"tenantID:<テナントのID>" "tenantPassword:<テナントのパスワード>"
```

## ⑤ Deep Securityマネージャへの登録完了確認

正しく有効化が行われれば、DSAがDSaaSコンソール上で“管理対象”と表示されます。



1. コンピュータタブに移動

コンピュータ

サブグループを含む ▼ グループ別 ▼

AWSアカウントの追加 新規 ▼ 削除... 詳細... 処理 ▼ イベント ▼ エクスポート ▼

名前 ▲	説明	プラットフ...	ポリシー	ステータス
▼ コンピュータ (1)				
54.70.61.125	このコンピュータは、Deep Se... Amazon Linu...	Demo		● セキュリティアップデ... 2
DemoServer1				● 管理対象

↑ 2. DSAをインストールした保護対象サーバが、“管理対象”と表示されていればOK

これで、インストール作業は完了です。



共通：補足



# 補足：設定前の事前準備

お客さまネットワーク構成によりDSMとDSA間での双方向通信が出来ない場合、DSaaSの通信方向設定を以下の通り変更して下さい。

1. 管理コンソールの[コンピュータ]をクリックします。



2. 該当コンピュータ画面を開きます。



4. [コンピュータ]タブを開き、[通信方向]で"Agent/Applianceから開始"を選択します。

5. [保存]を押してください。

3. [設定]をクリックします。

# ～はじめてのDSaaS①～

初期設定手引きとして、仮想パッチの設定をご紹介します。

## 4. 仮想パッチ自動適用設定

- ① 侵入防御の有効化
  - ② 侵入防御の自動割り当て設定オン
  - ③ 推奨設定のタスク作成
  - ④ 初期設定タスクの削除
  - ⑤ 仮想パッチの適用確認
-

# ① 侵入防御の有効化

仮想パッチ機能を利用するために、最初に侵入防御モジュールを有効にします。仮想パッチを使いたいコンピュータ画面を開き、「侵入防御」のステータスを「オン」、侵入防御の動作を「防御」にします。

1. 管理コンソールの[コンピュータ]をクリックします。



2. 仮想パッチを使いたいコンピュータ画面を開きます。



4. 侵入防御の設定を「オン」にします。

5. 侵入防御の動作を「防御」にします。

3. 侵入防御メニューを開きます。



テスト導入の場合、一定期間「検出」でドライランを行い、問題無い事を確認した上で「防御」に変更することを推奨します。



## ② 侵入防御の自動割り当て設定オン

保護対象サーバにインストールされたDSAが洗い出した仮想パッチルールを、自動的にサーバに割り当てられるように設定します。これにより、推奨設定の検索時に推奨ルールをコンピュータに自動割り当て/割り当て解除します。

1. 侵入防御メニューを開きます。

The screenshot displays the Trend Micro console interface for Intrusion Prevention (IP) settings. On the left, a sidebar menu has '侵入防御' (Intrusion Prevention) selected. The main content area shows a table of rules with columns for '名前' (Name), 'アプリケーションの種類' (Application Type), and '優先度' (Priority). Below the table, the '推奨設定' (Recommended Settings) section is visible, containing status information and a checkbox for '侵入防御の推奨設定を自動的に適用(可能な場合):' (Automatically apply recommended settings (if possible)), which is currently checked. At the bottom, there are buttons for '推奨設定の検索' (Search Recommended Settings), '推奨設定の検索のキャンセル' (Cancel Search Recommended Settings), '推奨設定をクリア' (Clear Recommended Settings), and a '保存' (Save) button.

名前	アプリケーションの種類	優先度
1000128 - HTTP Protocol Decoding	Web Server Common	1 - 低
1001033 - Windows Port Mapper Decoder	Port Mapper Windows	2 - 標準
1004715 - HTTP Web Client Decoding	Web Client Common	1 - 低
1004790 - Identified Diginotar Certificate	Web Client SSL	2 - 標準

推奨設定  
現在のステータス: 203個の侵入防御ルールが割り当てられています  
前回の推奨設定の検索: 2016-07-13 11:12  
未解決の推奨設定: 現在割り当てられている18個のルールの割り当て解除

侵入防御の推奨設定を自動的に適用(可能な場合):

保存 閉じる

2. 「侵入防御の推奨設定を自動的に適用(可能な場合)」を「はい」に設定します。

3. 保存して終了します。

### ③推奨設定のタスク作成-1

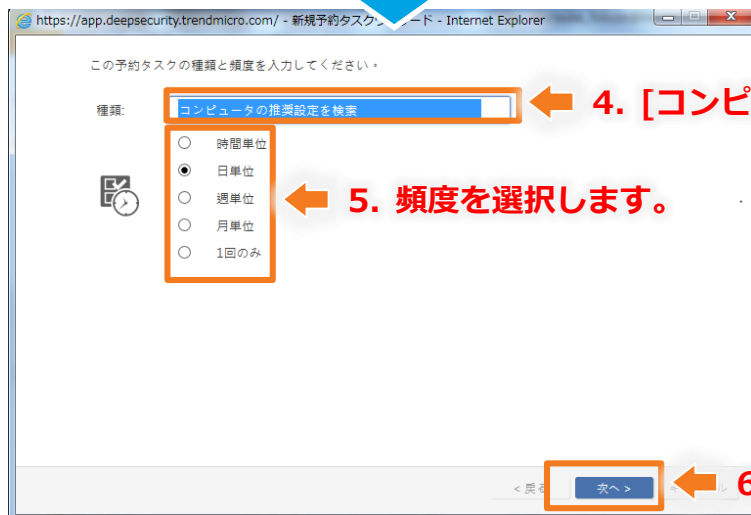
DSAが定期的に仮想パッチルールの洗い出しを実行できるように推奨設定のスケジュール設定を行います。



1. メインメニューの[管理]を開きます。

3. [新規]を開きます。

2. [予約タスク]を開きます。



4. [コンピュータの推奨設定を検索]を開きます。

5. 頻度を選択します。

6. [次へ]をクリックします。

### ③ 推奨設定のタスク作成-2

DSAが定期的に仮想パッチルールの洗い出しを実行できるように推奨設定のスケジュール設定を行います。

この週次タスクのスケジュール詳細を設定してください。

開始時刻: 19:40

1 週ごと

曜日を指定:

- 日曜
- 月曜
- 火曜
- 水曜
- 木曜
- 金曜
- 土曜

< 戻る **次へ** > キャンセル

7. スケジュールの詳細を左記の通り「2週ごと木曜日の0:00」で設定し、[次へ]をクリックします。

推奨設定を検索するコンピュータを指定してください。

すべてのコンピュータ

グループ:

使用ポリシー:

コンピュータ:

コンピュータ

サブグループ:

なし

サブポリシー:

DemoServer1

< 戻る **次へ** > キャンセル

8. 「すべてのコンピュータ」を指定し、[次へ]をクリックします。(個別設定時は適宜コンピュータを指定してください。)

この予約タスクの一意の名前を入力してください。

名前: 週単位コンピュータの推奨設定を検索

種類: コンピュータの推奨設定を検索

スケジュール: 毎週の木曜19:40

次の実行: 2016-08-18 19:40

詳細: すべてのコンピュータ

タスクの有効化

[完了]でタスクを実行

< 戻る **完了** > キャンセル

9. タスク名を入力します。

10. 「[完了]でタスクを実行」にチェックを入れ、[完了]をクリックします。



完了を押すと、一回目の推奨設定の検索が行われます。

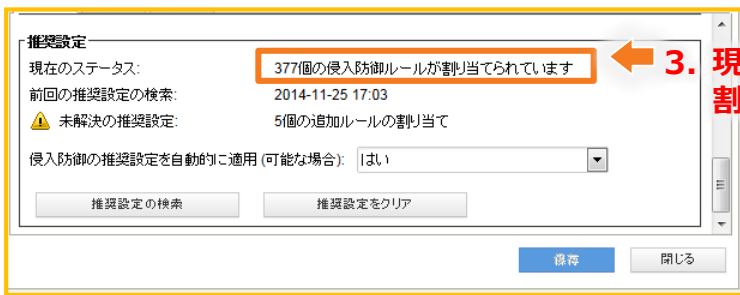
## ④ 仮想パッチの自動適用確認

仮想パッチの推奨設定が実行されていることと、ルールが洗い出されていることを確認します。

1. 管理コンソールの[コンピュータ]をクリックします。

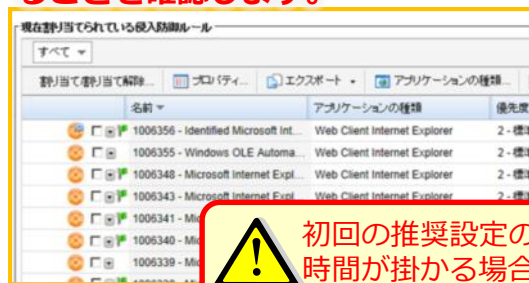


2. 仮想パッチを使いたいコンピュータ画面を開きます。



3. 現在のステータスで侵入防御ルールが割り当てられているか確認します。

4. [現在割り当てられている侵入防御ルール]で自動的に洗い出されたルールが適用されていることを確認します。



初回の推奨設定の検索は少々お時間が掛かる場合がございます。



以上で、仮想パッチの自動適用設定は完了です。

# ～はじめてのDSaaS②～

初期設定手引きとして、不正プログラム対策の設定をご紹介します。

## 5. 不正プログラム対策設定

- ①不正プログラム対策の有効化
  - ②不正プログラム対策・リアルタイム検索の個別設定
  - ③スケジュール設定
-

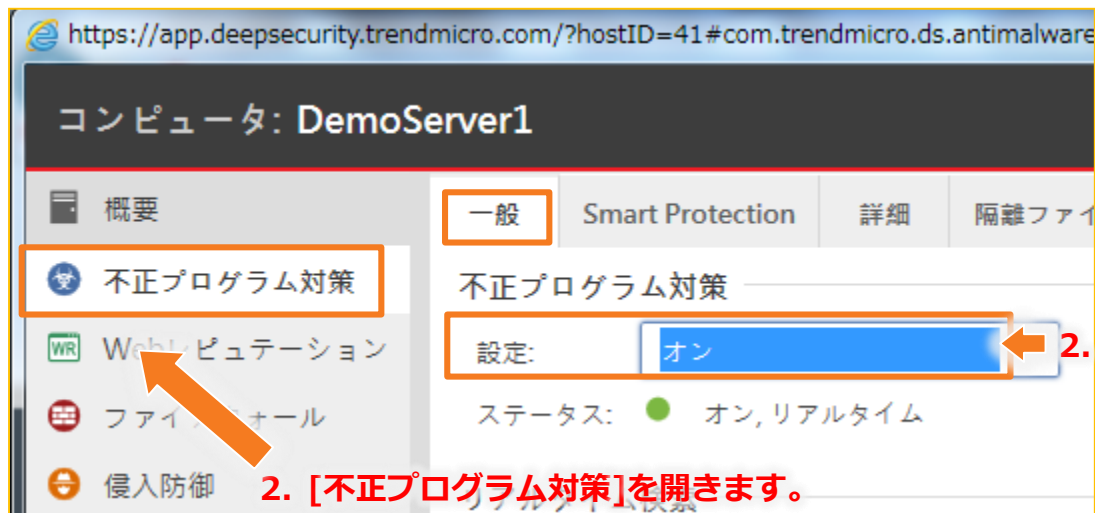


# ①不正プログラム対策の有効化

まず初めに、Deep Securityの不正プログラム対策を有効にします。



2. 不正プログラム対策を使いたいコンピュータ画面を開きます。



2. [一般]タブから、[不正プログラム対策]の設定を[オン]にします。

## ②不正プログラム対策・リアルタイム検索の個別設定

検索除外等の個別設定を行う場合は、初期設定で用意されているポリシーの「継承」を外し、設定画面を開いて各種設定を行います。また、新規ポリシー作成も可能です。

1. 管理コンソールの[コンピュータ]をクリックします。



2. 個別設定を使いたいコンピュータ画面を開きます。

3. [不正プログラム対策] → [一般]を開きます。



3. [継承]のチェックを外します。

4. [Default Real-Time Scan Configuration]を選択し、[編集]をクリックします。



5. 設定画面が開きますので、必要に応じて各種設定を行ってください。



個別設定を行わない場合は、本ページの設定は実施しなくて結構です。

# ③ スケジュール設定

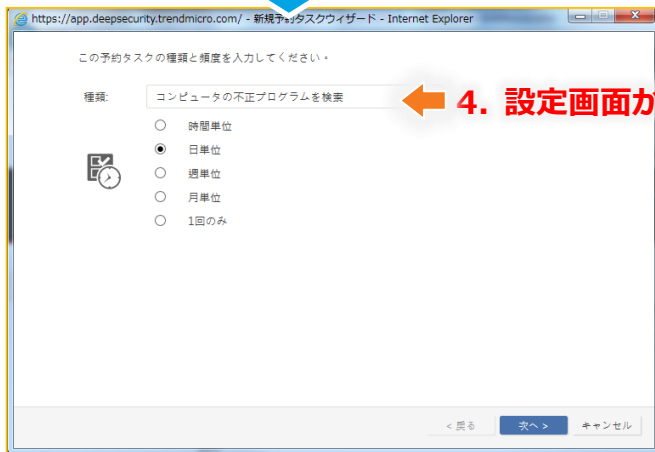
初期設定では、予約タスク「週単位 コンピュータの推奨設定を検索」が毎週水曜日の正午12:00に設定されています。必要に応じて変更して下さい。



← 1. 管理コンソールの[管理]をクリックします。

← 2. [予約タスク]を開きます。

← 3. [新規]をクリックします。



← 4. 設定画面が開きますので、仮想パッチと同様に設定し、完了して下さい。

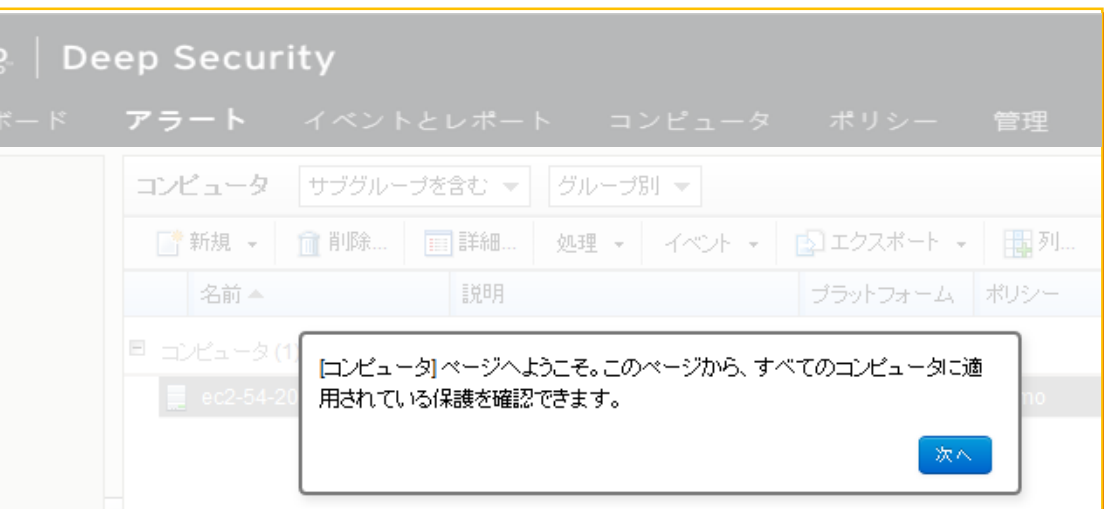


これで、インストールおよび不正プログラム対策・仮想パッチの初期段階設定は終了です。お疲れさまでした。  
(詳細設定はDSaaS管理コンソールのヘルプにあるマニュアルをご参照ください。)

# 6. 參考資料

---

# DSaaS: デモコンピュータの紹介



Deep Security

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

コンピュータ サブグループを含む ▼ グループ別 ▼

新規 ▼ 削除... 詳細... 処理 ▼ イベント ▼ エクスポート ▼ 列...


名前 ▲	説明	プラットフォーム	ポリシー
コンピュータ (1)			
ec2-54-203-95-111.us-west-2.compute.amazonaws.com			

[コンピュータ] ページへようこそ。このページから、すべてのコンピュータに適用されている保護を確認できます。

次へ

最初のログイン時に、デモコンピュータの説明をするチュートリアルが表示されます  
このデモコンピュータは30日使えます  
また、各機能のデモも準備されていますので是非お試しください

本デモコンピュータも1台とカウントされますので、  
利用時には削除いただきますようお願いいたします



TREND MICRO | Deep Security

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

コンピュータ サブグループを含む ▼ グループ別 ▼

新規 ▼ 削除... 詳細... 処理 ▼ イベント ▼ エクスポート ▼ 列...

名前 ▲	説明	プラットフォーム	ポリシー
コンピュータ (1)			
ec2-54-203-95-111.us-west-2.compute.amazonaws.com			

Deep Securityについて説明するためのコンピュータが1台作成されています。Deep Securityの機能を試すには、<http://ec2-54-203-95-111.us-west-2.compute.amazonaws.com/>に移動し、インタフェースを使用してさまざまなセキュリティイベントを生成してください。

このコンピュータは、Deep Securityの機能を説明するためのものです。28日以内に削除されます。

次へ

# DSaaS:ヘルプメニュー



インストールスクリプト	インストール用のスクリプトを作成するツールです
サポート情報	(日本では現在この機能を提供しておりません、こちらにフィードバック、質問を記載いただいても対応はできかねますのであらかじめご了承ください)
コメントおよびフィードバック	
Agentのダウンロード	DSAのインストールパッケージをダウンロードできます
使用許諾契約書	(日本では適用されません)
バージョン情報	DSaaSコンソールバージョンを確認できます

# DSaaS:ユーザプロパティ

ユーザ情報、パスワードの変更などの編集が行えます

一般 | 連絡先情報 | 設定

一般情報

ユーザ名:

名前:

説明:

役割:

言語:

タイムゾーン:

時刻の形式:  12時間  24時間

ログオン資格情報

最終変更日: 2016-07-08

パスワードの有効期限なし

ロックアウト (ログオンを拒否)

多要素認証 (MFA)

多要素認証の有効化: いいえ

Account Name | User Name

ユーザプロパティ

パスワードの変更

ログオフ

ユーザ:

現在のパスワード:

新しいパスワード:

新しいパスワードの確認入力:

このシステムのパスワードの条件は次のとおりです:

- 8文字以上であること
- 英字と数字の両方が含まれていること
- 大文字と小文字の両方が含まれていること

# DSaaS : パスワードを忘れたら

- ログインページにある、“Having trouble signing in?”リンクをクリックして、アカウント名、ユーザ名を入力してください
- パスワードリセットのメールが数分で届きますので、メールに記載されたURLからパスワードの再設定を行ってください

TREND MICRO | Deep Security

## Sign In

Account Name  
Account Name

Username  
User Name

Password

Remember Account Name and Username

I have an MFA token ([More Info](#))

Sign In

Having trouble signing in?

### Sign-in troubles?

To reset your password, enter your account details and click **OK**. We will send instructions to the address associated with your account.

Account Name: Account Name ×

Username: User Name

Lost your MFA token? Click **Reset MFA token** below to learn how to reset your account.

Reset MFA token OK Cancel



# 7. よくあるご質問と回答集 (FAQ)

---

# FAQ ～製品仕様関連①～

質問	回答
Auto-Scaling機能に対応していますか？	対応しています。
DSAが攻撃を検知した時や、オフラインになった時等、DSaaS管理マネージャから管理者に通知メールが届きますか？	届きます。
推奨スキャンの実行時間を指定することは可能でしょうか？	可能です。
ルールのチューニングは可能ですか？	可能です。
誤検知が発生した場合はどのような対応になりますか？	誤検知か否かを切り分けた結果、DPIルールの不具合の場合は、ルールの修正を行います。
DSaaS管理マネージャで生成するレポートを定期的に自動送付することは可能ですか？	可能です。
DSaaS管理マネージャが停止した場合、DSAをインストールしているサーバへの影響はどうなりますか？	動作を続けます。管理マネージャが停止した場合、DSAが動作を止めることはありません (参考FAQ: <a href="http://esupport.trendmicro.com/solution/ja-JP/1310095.aspx">http://esupport.trendmicro.com/solution/ja-JP/1310095.aspx</a> )
DSaaS管理マネージャのアカウントがロックされてしまった場合、パスワードを忘れてしまった場合はどうしたらいいですか？	ログインページから再発行する事ができます。
管理マネージャは冗長化されていますか？	はい。冗長化されています。DSAはプライマリの管理マネージャと通信できない場合に、自動でセカンダリに切り替わる仕様になっています。
DSAのバージョンアップが必要な場合、強制アップデートになるのでしょうか？	強制アップデートは実行しません。お客様に告知の上、お客様にてアップデートをして頂きます。
Deep Securityマネージャは日本語対応していますか？	対応しています。アカウント作成の時に“Country = Japan”を選択する、またはDSaaSログイン後に、ユーザープロファイル>一般>言語 = 日本語を選択し適用することで日本語表示になります。しかし、一部の言葉が英語表記のままとなっています、予めご了承ください。今後のアップデートでフルローカライズを予定しています。

# FAQ ～製品仕様関連②～

質問	回答
設定の移行について：既に構築しているDSMから、DSaaSに移行したい場合、DSaaSのDSMに設定を移行することは可能でしょうか？	可能です。設定のExport/Importで移行できます。ただし、ログの移行はできません。
DSMのメンテナンス時の連絡はどうなりますか？定期メンテナンスはありますか？	メンテナンスは不定期です。メンテナンスのアナウンスはDSaaSログイン画面にも表示されます。
DSAのバージョン確認方法を教えてください	DSaaS管理コンソールから、コンピュータ>概要>処理の、[ソフトウェア]でご確認ください。または、DSAがインストールされているコンピュータ上で、タスクトレイ>DSAアイコンをクリックいただくことで確認できます。
DSaaSの製品FAQはどこにありますか？	DSaaSが提供しているDSAはパッケージ版のDSAと同じものです、DSaaSの製品FAQはTMDSのFAQを参照してください。(http://esupport.trendmicro.com/ja-jp/enterprise/ds/top.aspx?cm_re=Sup_-_ds_-_esupporttop_suptop)
トライアルで付いてくるインスタンスはWindowsですか？	はい、Windowsです。但し、トライアルで提供されるサーバは、Deep Securityの設定配信などのテスト用サーバとなります。リモートデスクトップ等でログインし、OSの設定変更やアプリケーションのインストール等は行えません。
トライアルで、他のインスタンスにDSAをインストールしてOKか？	可能です。
DSMのセッションが増えた場合の対処方法は？	ロードバランサーを使って負荷分散を行っています。負荷が増えた場合は、ロードバランサー配下のサーバを増やします。
インストールするDSAのバージョンを常に固定にしておきたい場合のインストール方法は？	インストールスクリプトによるDSAインストールを推奨していますが、お客さま環境によりインストールするDSAのバージョンを常に固定にしておきたい場合は、インストーラーによるDSAインストールを行う事により対応が可能です。この方法では、DSAのインストールとDSAの有効化をそれぞれ実行する必要があります。詳細はお問い合わせください。

# FAQ ～製品仕様関連③～

質問	回答
CentOS上のリアルタイム検索はDSバージョンいくつかから可能ですか？	DS9.5 SP1から可能です。
DSaaSを利用する際、FWにて443を全開放したくないと考えているのですが、DSMを特定する情報（IPアドレス、ドメイン名、ホスト名など）を教えてください。	①内→外の443を開けていただければ片方向通信にて管理可能です ②上記の穴あけも厳しいということであれば、次のFQDNをFWにて設定してください。 agents.deepsecurity.trendmicro.com ⇒ DSAからDSMへのハートビート relay.deepsecurity.trendmicro.com ⇒ DSAとRelayの通信 ※ DSMのIPアドレスは変更する可能性がありますので、お教えすることはできません。
DSaaS利用ユーザはどんなログをどれくらいの期間保持可能ですか？	システムイベントとセキュリティイベントの2つが残ります。DSaaSにおいてはそれぞれ13週間保持されます。 ※2017年5月15日以降は保存期間が4週間（32日）に変更となります。
DSaaSを使用しているサーバは1台で、ライセンスも1台分購入してあります。管理コンソールのアラートで「最大1台のコンピュータのうち1台を使用中」と表示されるのですが、何かのエラーですか？	エラーではありません。購入いただいたライセンス数の最大値までご利用いただくと表示されるものです。表示が不要であれば下記の手順で当該アラートをオフにしてください。 ①DSaaS管理コンソール画面の「管理」タブを選択 ②「システム設定」の中の「アラート」タブを選択 ③「アラート設定の表示」を選択 ④「ライセンスシート数の上限に達しました」アラートのプロパティを選択し、設定をオフにする
DSaaSにて攻撃（設定したルールに引っかかるもの）を検知した場合は、どのように通知されるのでしょうか？	下記の通りです。 ①DSaaS管理コンソール上の「イベントとレポート」の該当するイベント部分に表示 ②イベントルールに合致した場合にアラートをあげる設定にしていれば、DSaaS管理コンソール上の「アラート」に表示 ③イベントルールアラートをメールで通知する設定にしていれば、メールにて通知 ④不正プログラムの検出、不正サイトのブロック(Webレピュテーション)に関しては、保護対象サーバにてポップアップ通知（保護対象サーバにDeep Security Notifierが入っている必要有）
DSaaSのインストールスクリプトを利用してDSAのインストールを試みたのですが、上手くいきません。他に方法はありますか？	下記A,Bの2通りがあります。 A：管理コンソール右上の「サポート」内の「Agentのダウンロード」からダウンロード B：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]にて、インストール対象のOSに応じたパッケージを選択③その後[エクスポート]⇒[インストーラーのエクスポート]にてエクスポートしたインストーラを実行
DSaaSが実際に攻撃などを検知できるのか試したいのですが何か方法はありますか？	●不正プログラム対策 ⇒ EicarウイルスをDLしてみてください。 ●侵入防御 ⇒ <a href="http://esupport.trendmicro.com/solution/ja-jp/1097204.aspx">http://esupport.trendmicro.com/solution/ja-jp/1097204.aspx</a> を参照ください。 ●変更監視 ⇒ 監視対象のフォルダにファイルを置く、あるいは対象のファイルを編集するなどしてみてください。 ●ログ監視 ⇒ 一例ですが、Windowsログインに失敗した場合の閾値を下げて、わざとログインに失敗をしてアラートをあげてください。

# FAQ ～販売ルール・使用許諾関連～

質問	回答
複数年契約は可能ですか？	SPL販売パートナー様との契約次第となります。
DSライセンス版からDSaaSへの移行は可能でしょうか？	入れ替えになります。それぞれ違うACを使うので、買い替えの際はライセンス期限等に考慮が必要です。
現在取り扱いが決まっているSPLパートナーは？	DSaaSをお取り扱い頂くSPLパートナー様は、以下TMSaaSページに掲載しています。 <a href="http://www.trendmicro.co.jp/jp/business/solutions/saas/">http://www.trendmicro.co.jp/jp/business/solutions/saas/</a>
標準価格はありますか？	ありません。DSaaSに標準価格設定はなく、価格はSPLパートナー側にて決定します。
課金対象について。シート数なのか、サーバ数なのか。	サーバ数です。
Webサーバ等、公開サーバへの導入も可能ですか？	はい。可能です。EA-Packも引き続き併売いたします。
ServerProtectはバンドルされていますか？	いいえ、されていません。
アクティベーションコード入力画面での「AWS Marketplace のサブスクリプション申込み」について	アクティベーションコードは販売店様より入手ください。 「AWSマーケットプレイスからのサブスクリプション申込み」に関して、現在日本においてはサポート管轄外となっております。

## トレンドマイクロ株式会社

[www.trendmicro.co.jp](http://www.trendmicro.co.jp)

本書に関する著作権は、トレンドマイクロ株式会社へ独占的に帰属します。トレンドマイクロ株式会社が書面により事前に承諾している場合を除き、形態および手段を問わず本書またはその一部を複製することは禁じられています。本書の作成にあたっては細心の注意を払っていますが、本書の記述に誤りや欠落があってもトレンドマイクロ株式会社はいかなる責任も負わないものとします。本書およびその記述内容は予告なしに変更される場合があります。

TRENDMICRO、TREND MICRO、ウイルスバスター、ウイルスバスター On-Line Scan、PC-cillin、InterScan、INTERSCAN VIRUSWALL、ISVW、InterScanWebManager、ISWM、InterScan Web Security Suite、IWSS、TRENDMICRO SERVERPROTECT、PortalProtect、Trend Micro Control Manager、Trend Micro MobileSecurity、VSAPI、トレンドマイクロ・プレミアム・サポート・プログラム、License for Enterprise Information Security、LEISec、Trend Park、Trend Labs、InterScan Gateway Security Appliance、Trend Micro Network VirusWall、Network VirusWall Enforcer、Trend Flex Security、LEAKPROOF、Trendプロテクト、Expert on Guard、InterScan Messaging Security Appliance、InterScan Web Security Appliance、InterScan Messaging Hosted Security、DataDNA、Trend Micro Threat Management Solution、Trend Micro Threat Management Services、Trend Micro Threat Management Agent、Trend Micro Threat Mitigator、Trend Micro Threat Discovery Appliance、Trend Micro USB Security、InterScan Web Security Virtual Appliance、InterScan Messaging Security Virtual Appliance、Trend Micro Reliable Security License、TRSL、Trend Micro Smart Protection Network、Smart Protection Network、SPN、SMARTSCAN、Trend Micro Kids Safety、Trend Micro Web Security、Trend Micro IM Security、Trend Micro Email Encryption、Trend Micro Email Encryption Client、Trend Micro Email Encryption Gateway、Trend Micro Collaboration Security、Trend Micro Portable Security、Portable Security、Trend Micro Standard Web Security、トレンドマイクロ アグレッシブスキャナー、Trend Micro Hosted Email Security、Hosted Email Security、Trend Micro Deep Security、ウイルスバスタークラウド、ウイルスバスター CLOUD、Smart Surfing、スマートスキャン、Trend Micro Instant Security、Trend Micro Enterprise Security for Gateways、Enterprise Security for Gateways、Trend Micro Email Security Platform、Trend Smart Protection、Vulnerability Management Services、Trend Micro Vulnerability Management Services、Trend Micro PCI Scanning Service、Trend Micro Titanium、Trend Micro Titanium AntiVirus Plus、Smart Protection Server、Deep Security、Worry Free Remote Manager、ウイルスバスター ビジネスセキュリティサービス、HOUSECALL、SafeSync、トレンドマイクロ オンラインストレージ SafeSync、Trend Micro InterScan WebManager SCC、Trend Micro NAS Security、Trend Micro Data Loss Prevention、TREND MICRO ENDPOINT ENCRYPTION、Securing Your Journey to the Cloud、Trend Micro オンラインスキャン、Trend Micro Deep Security Anti Virus for VDI、Trend Micro Deep Security Virtual Patch、Trend Micro Threat Discovery Software Appliance、SECURE CLOUD、Trend Micro VDIオプション、おまかせ不正請求クリーンナップサービス、Trend Micro Deep Security あんしんバック、こどもモード、Deep Discovery、TCSE、おまかせインストール・バージョンアップ、トレンドマイクロ バッテリーエイド、Trend Micro Safe Lock、トレンドマイクロ セーフバックアップ、Deep Discovery Advisor、Deep Discovery Inspector、Trend Micro Mobile App Reputation、あんしんブラウザ、Jewelry Box、カスタム ディフェンス、InterScan Messaging Security Suite Plus、および おもいでバックアップサービス、トレンドマイクロ サイバー攻撃 対応支援サービスは、トレンドマイクロ株式会社の登録商標です。本書に記載されている各社の社名、製品名、およびサービス名は、各社の商標または登録商標です。

Copyright (c) 2014 Trend Micro Incorporated. All rights reserved.