Trend Micro Cloud One Workload Security™
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）

本資料は
2020年8月現在の情報となります

ダイワボウ情報システム株式会社

はじめに

- このたびは、Trend Micro Cloud One – Workload Security™ (以下、C1WS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、C1WS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C1WSをご利用ください。

- 本資料は、C1WS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りません。詳細については、以下のオンラインヘルプセンターをご確認ください。
  https://cloudone.trendmicro.com/docs/jp/workload-security/

- C1WS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。
  https://www.trendmicro.com/ja_jp/partners/security-as-a-service.html

本資料における言葉の定義

略語	定義
C1WS	Trend Micro Cloud One – Workload Securityの略称です。 C1WS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。
C1WSコンソール	C1WS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。
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、以下AC）です。

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）

**C1WS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。**

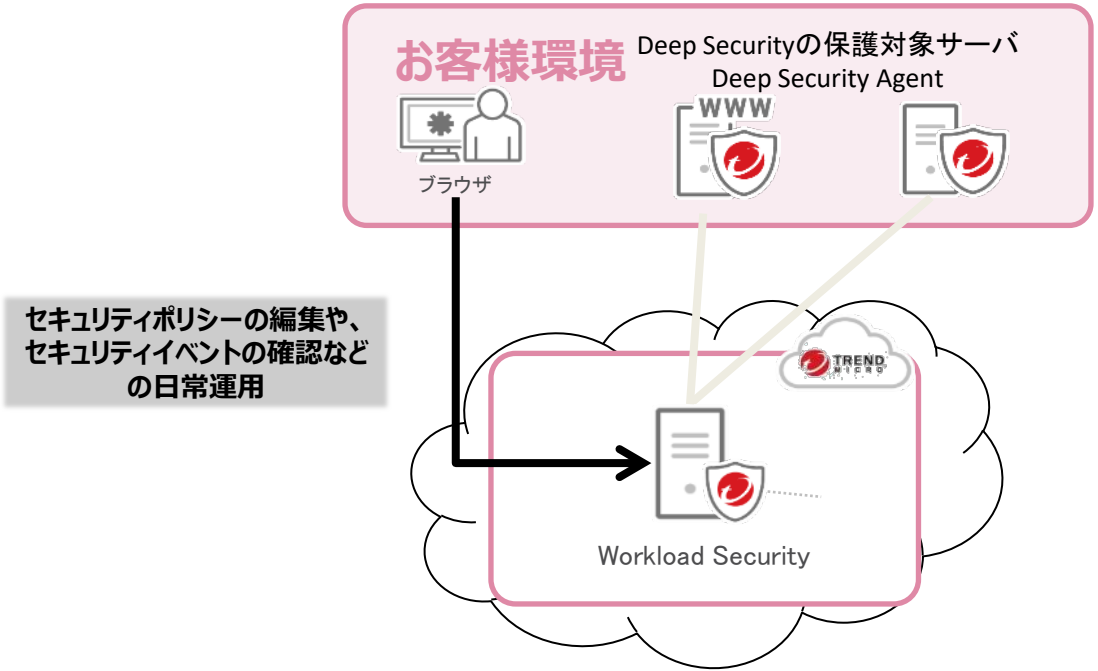
- C1WSで提供しているDSAのシステム要件は、こちらを参照してください
  https://www.go-tm.jp/tmdsaas/req
- DSAをインストールするサーバから、C1WSにアクセスできることを確認してください
  https://cloudone.trendmicro.com/docs/jp/workload-security/communication-ports-urls-ip/
- プロキシサーバを経由する場合は、こちらを参照してください-
  https://cloudone.trendmicro.com/docs/jp/workload-security/proxy-set-up/
- DSAをインストールするサーバにおいて、お使いのDSAバージョンによって、ネットワークの瞬断や、ドライバーのインストールにより、OS再起動が必要となる場合があります。
- C1WS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）
- C1WS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. C1WS アカウントの作成
2. C1WS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）

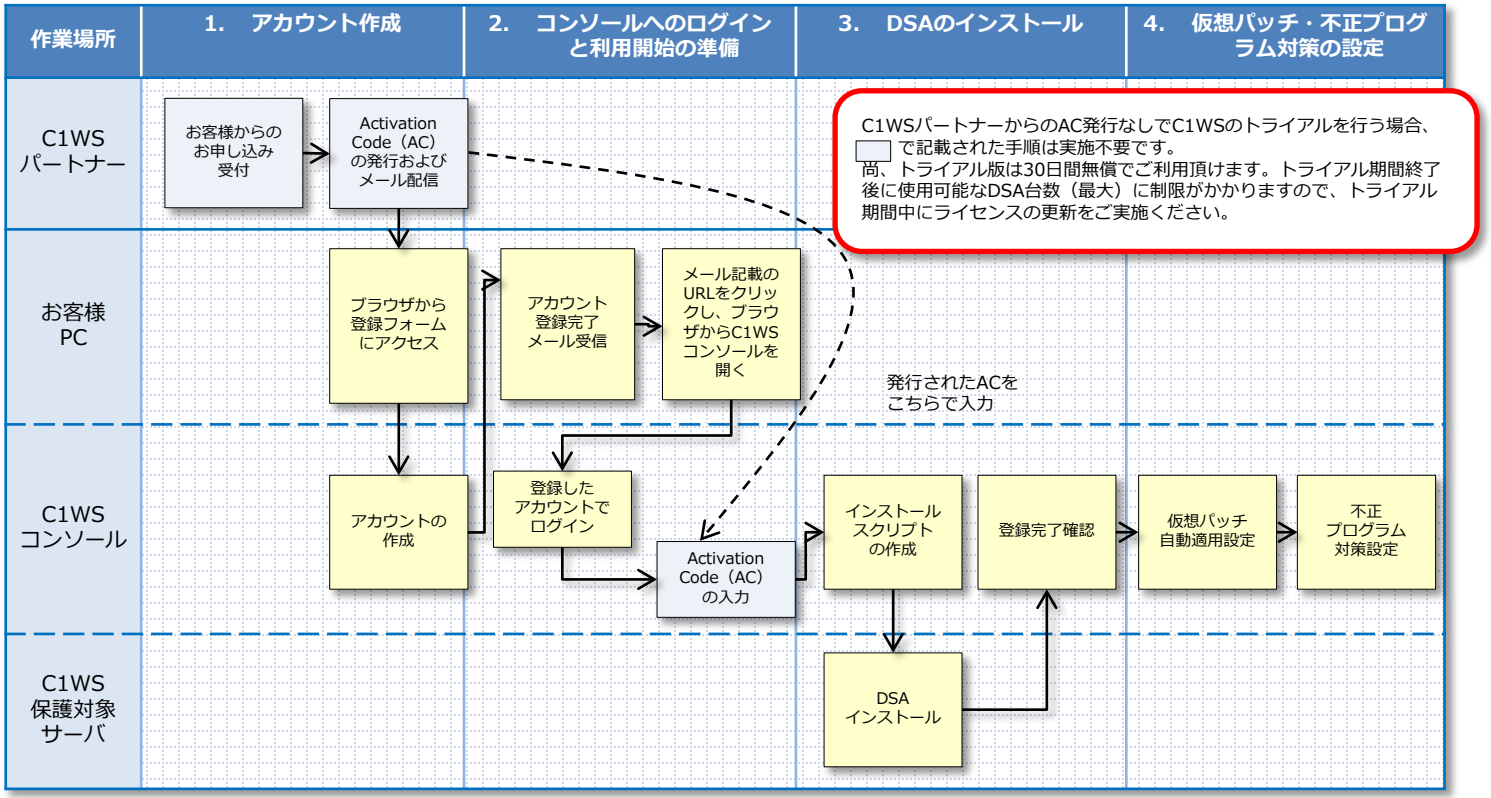
Cloud One Workload Security構成概要

C1WS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C1WSコンソールにログインして行います。
但し、インストール作業時はC1WS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。



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
[Cloud One - Workload Security （各C1WS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、「 Cloud One - Workload Security （各C1WS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。

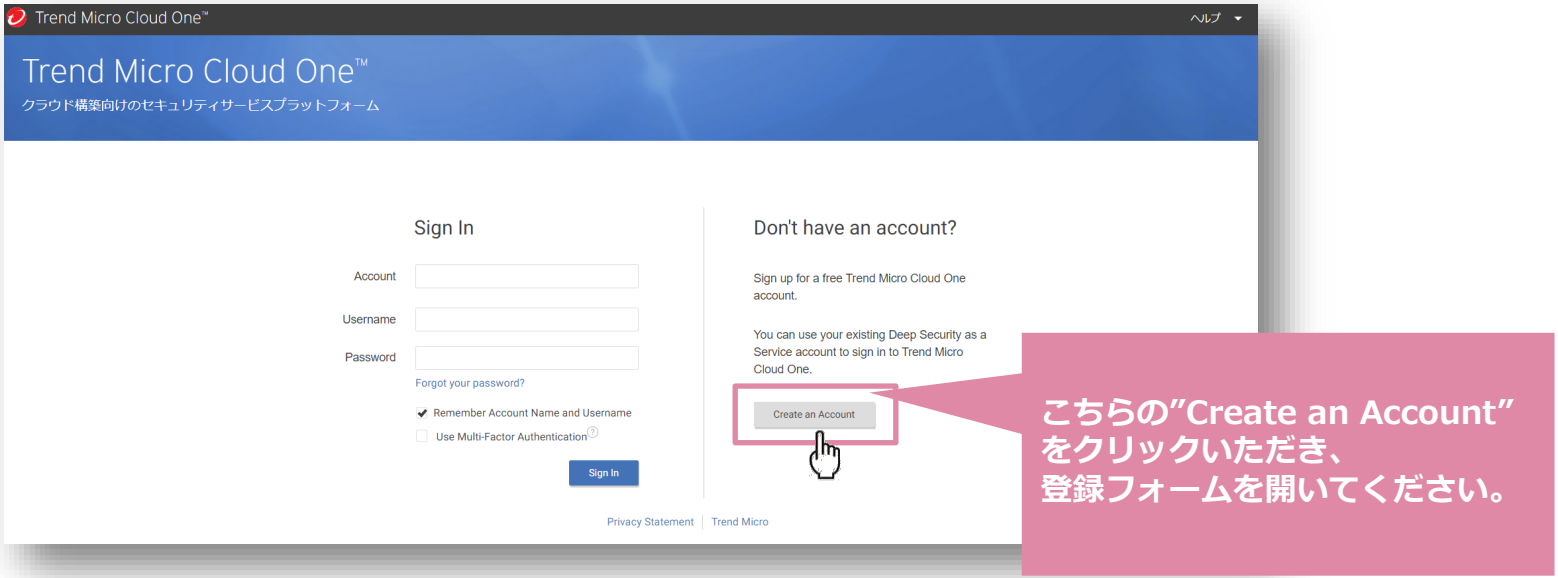
サービスプラン： Cloud One - Workload Security （各C1WSパートナーごとのサービス名）の
ご契約ライセンスが新規追加されましたのでお知らせいたします。

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C1WS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。

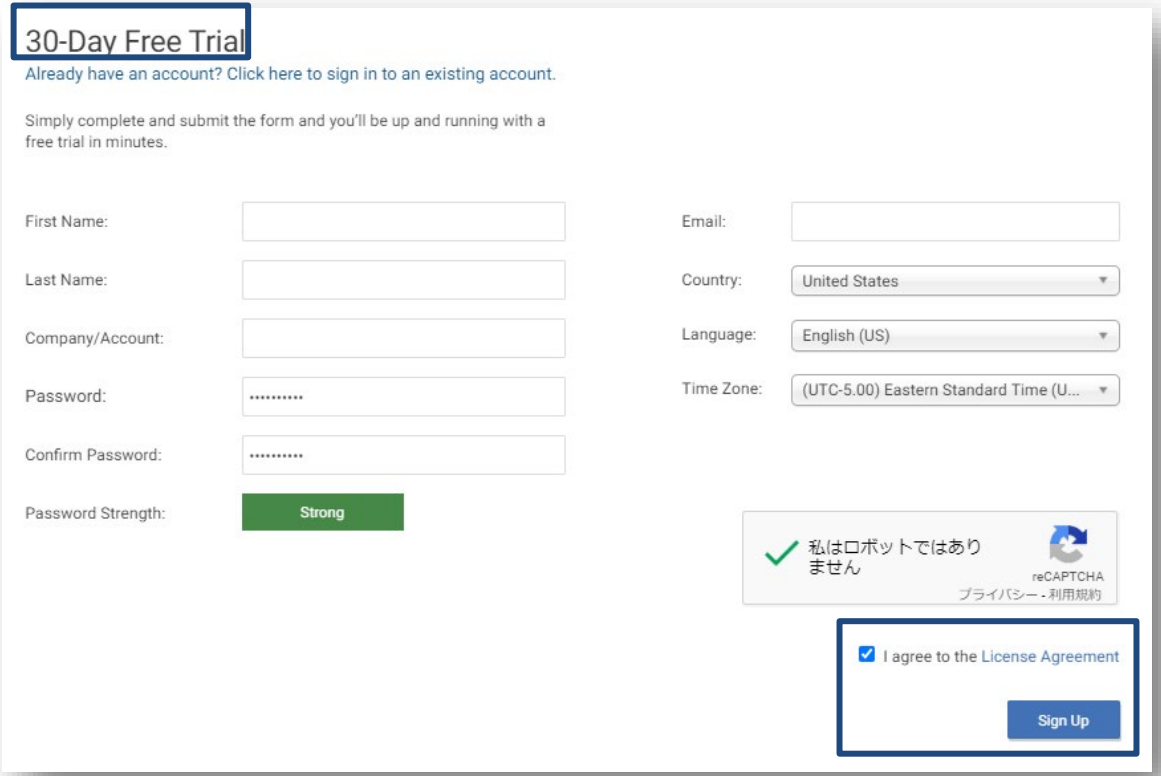
https://cloudone.trendmicro.com/



②アカウントの作成

必要事項を入力しアカウントを作成してください。
※各項目の説明は次のページを確認してください。

どのアカウントも、初めはトライアルアカウントとして作成します。
ACを入力することで製品版となります。



すべての項目をご記入し、License Agreementを確認し、Sign Upします。

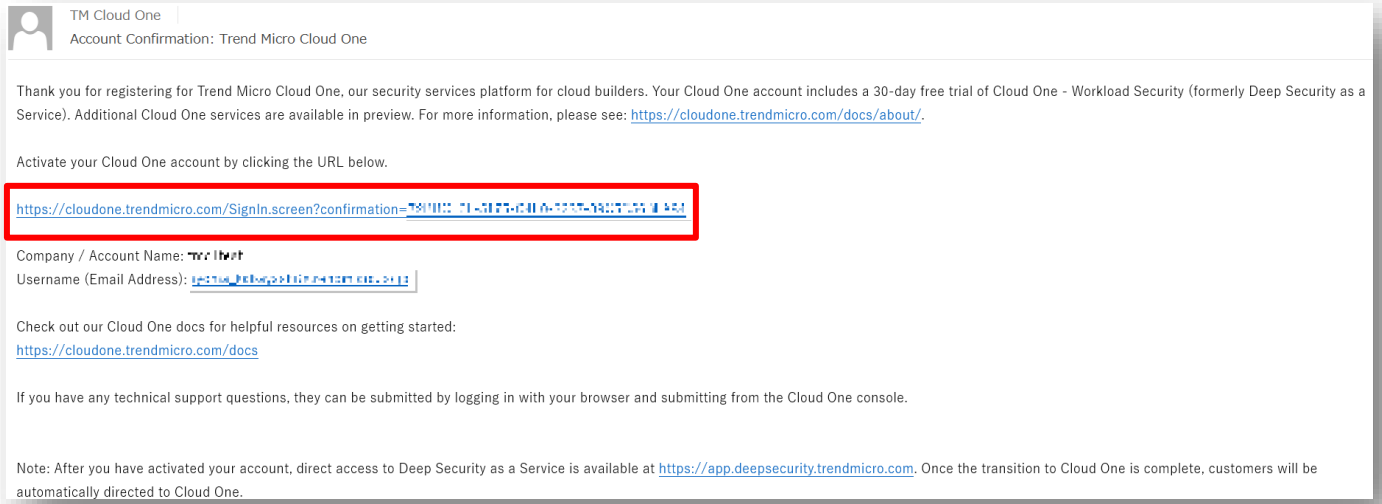
②アカウントの作成

必要事項を入力しアカウントを作成してください。

項目	説明
First Name/Last Name	ご自身の氏名
Company/Account	DIS Cloud Trend Micro Family アカウントのご連絡メール記載のアカウントID ※C1WSコンソールへのログインIDとなります。 ※他アカウントとの重複不可
Password/Confirm Password	任意のパスワード ※英数字大文字小文字の組み合わせ ※設定したパスワードが条件を満たしている場合、Strongと表示されます。
Email	※C1WSコンソールへのUsernameとなります。 ※C1WSコンソールログイン後に変更可能です
Country/Language/Time Zone	Country　：**[Japan]** Language　：**[Japanese]** Time Zone：**[Japan Standard Time(Asia/Tokyo)]**

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。



TM Cloud One
Account Confirmation: Trend Micro Cloud One

Thank you for registering for Trend Micro Cloud One, our security services platform for cloud builders. Your Cloud One account includes a 30-day free trial of Cloud One - Workload Security (formerly Deep Security as a Service). Additional Cloud One services are available in preview. For more information, please see: https://cloudone.trendmicro.com/docs/about/.

Activate your Cloud One account by clicking the URL below.

https://cloudone.trendmicro.com/SignIn.screen?confirmation=

Company / Account Name:
Username (Email Address):

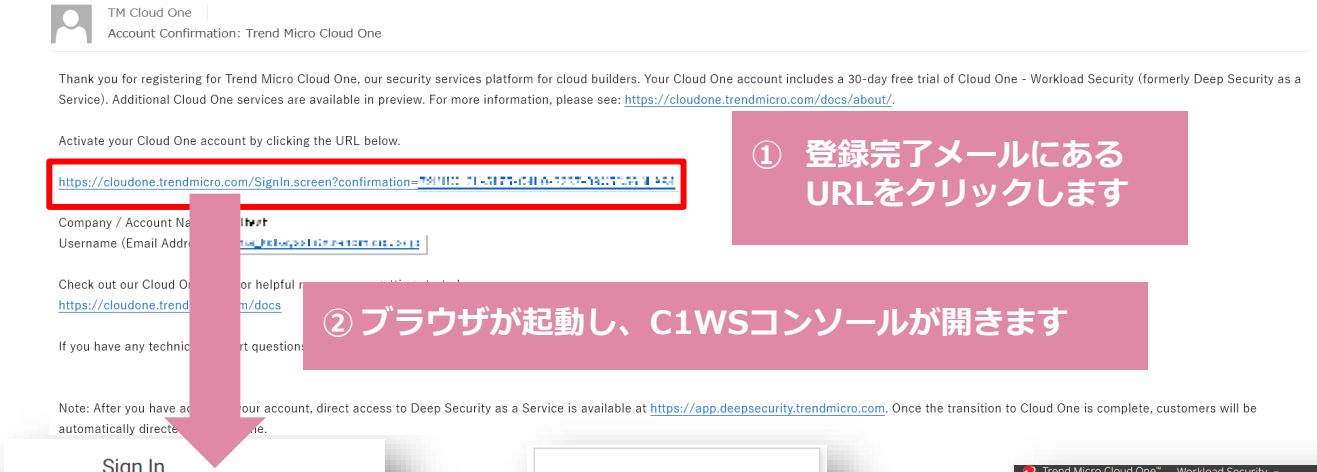
Check out our Cloud One docs for helpful resources on getting started:
https://cloudone.trendmicro.com/docs

If you have any technical support questions, they can be submitted by logging in with your browser and submitting from the Cloud One console.

Note: After you have activated your account, direct access to Deep Security as a Service is available at https://app.deepsecurity.trendmicro.com. Once the transition to Cloud One is complete, customers will be automatically directed to Cloud One.

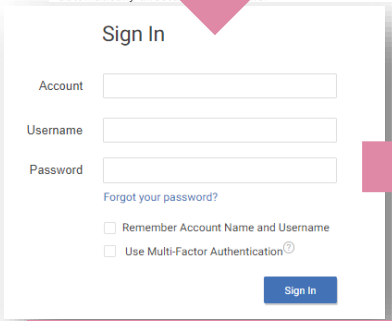
メールタイトル	配信時期(目安)	説明
Account Confirmation: Trend Micro Cloud One	アカウント作成後、**数分後（1分から15分後）**に配信されます。	URLをクリックすることでアカウントが有効化されます。 URLをクリックし、C1WSコンソールにログインしてください。 メール送信元：no-reply-cloudone@trendmicro.com

①C1WSコンソールにログインする



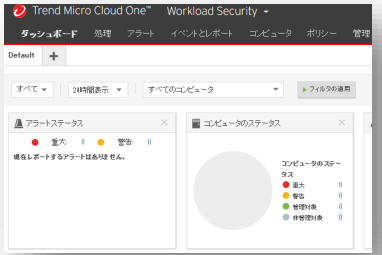
① 登録完了メールにある URLをクリックします

② ブラウザが起動し、C1WSコンソールが開きます



③ 登録したアカウントで ログインします

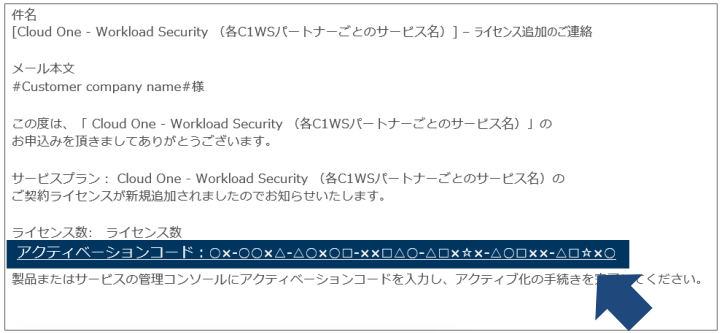
④ Workload Security を選択します



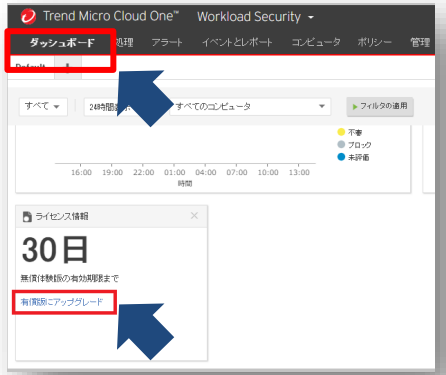
⑤ C1WSコンソールが 表示されます

②Activation Code（AC）の入力

C1WSパートナーから発行されるActivation Code（AC）を入力します。



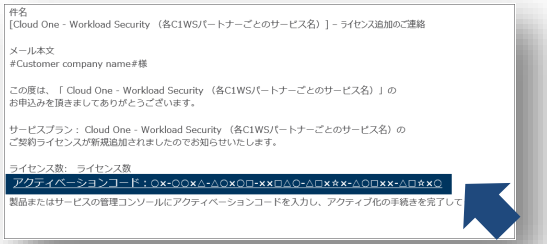
1. Activation Code（AC）が記載されたメールが届きます。
次の作業で使用しますので、アクティベーションコードをコピーしておいてください。



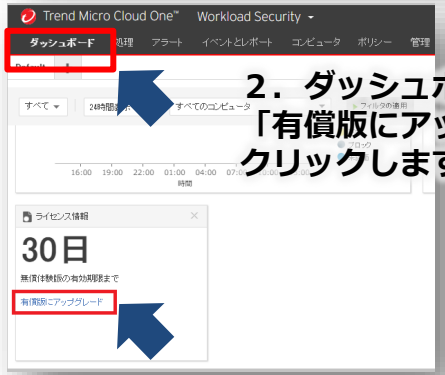
2．ダッシュボード画面の「有償版にアップグレード」をクリックします。

③Activation Code（AC）の入力

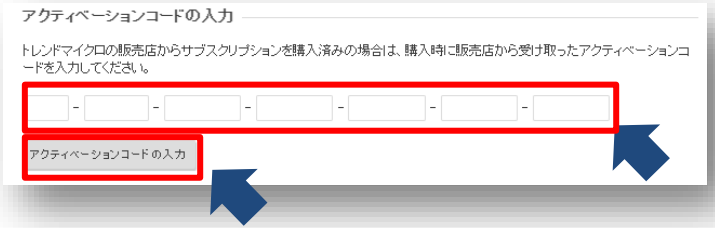
C1WSパートナーから発行されるActivation Code（AC）を入力します。



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おいてください。



2．ダッシュボード画面の「有償版にアップグレード」をクリックします。



3．「有償版のTrend Micro Cloud Oneにアップグレード」画面が表示されますので、手順１でコピーしたACを入力し、「アクティベーションコードの入力」を押します。
（ACはコピー&ペーストでの入力も可能です。）

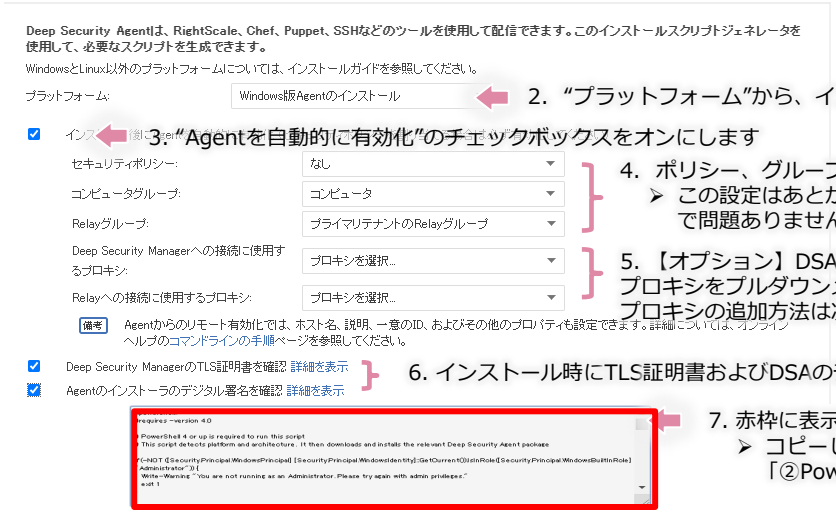
Windows 手法 ①
C1WSで作成したインストールスクリプトを実行

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。)

インストールスクリプト

1. C1WS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問題ありません。

5. 【オプション】DSAがC1WSとの接続でプロキシを経由して接続する場合は、プロキシをプルダウンメニューより選択します。
   プロキシの追加方法は次のページを確認してください。

6. インストール時にTLS証明書およびDSAのデジタル署名を検証する場合は、チェックをつけます。

7. 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「②PowerShellによるDSAインストール」でペーストして実施させます。

【補足】プロキシの追加方法について

DSAがC1WSまたはDSRにアクセスする際にプロキシを経由する場合は、接続先のプロキシを追加することができます。

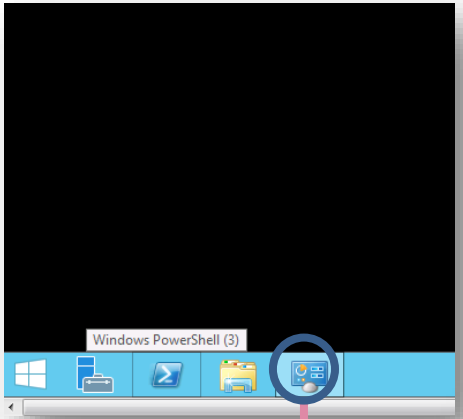
1．C1WSコンソールにログインし、「管理」-「プロキシ」-「新規」でDSAが接続するプロキシを追加することができます。

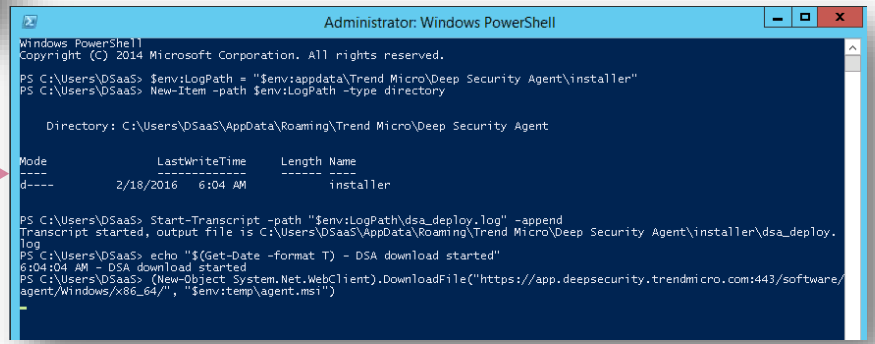
2．アドレス、ポート、プロトコルを入力します。認証が必要な場合は、ユーザ名とパスワードを入力し、「OK」を押します。

②PowerShell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C1WS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

③Deep 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C1WSコンソール上 で“管理対象”と表示されます。

これで、インストール作業は完了です。

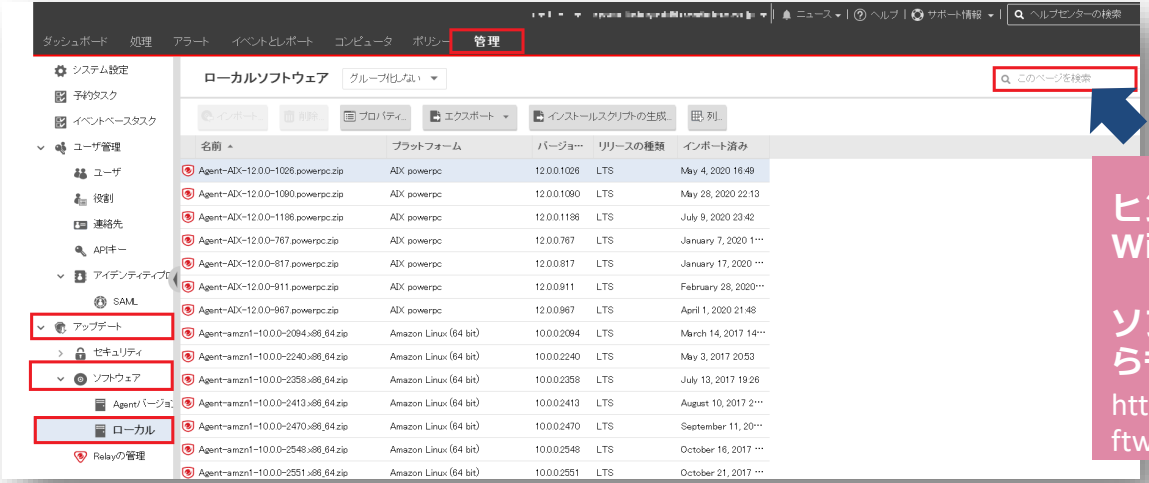
Windows 手法②
インストールEXE/MSIをダウンロードインストールしプロンプトでDSM登録

C1WS / Relayへ接続するためのプロキシの設定方法（コマンドラインでの設定方法）のQ&Aはこちら
https://success.trendmicro.com/jp/solution/1116970

①インストールファイルをダウンロードする

C1WS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.C1WS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



ヒント：
Windowsを入力し、検索できます。

ソフトウェアはダウンロードセンターからも入手できます。
https://help.deepsecurity.trendmicro.com/software.html

2.インストールするパッケージを右クリックし、[インストーラのエクスポート]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Agent-Core-Windows-**.*.*-***.msiファイルをインストール対象マシンにコピーし、

4. Agent-Core-Windows-**.*.*-***.msiをクリックしインストールを実施します。

③インストールスクリプトからテナントIDとテナントパスワードを抜き出し、コマンドを実行する

テナントIDとテナントパスワードを抜き出す

1.C1WSコンソールの右上「サポート情報」から「インストールスクリプト」を開き、プラットフォームの項目にてWindowsを選択する。

2. tenantID: <テナントID>
token: <テナントパスワード>
上記2つをコピーする

※これがプロンプトで実行する、C1WS登録(有効化)のコマンドになります
注意：tenantIDとtokenは、C1WSコンソールから、各アカウント毎に生成してください。

```
Start-Sleep -s 50
& $Env:ProgramFiles"¥Trend Micro¥Deep Security Agent¥dsa_control" -r
& $Env:ProgramFiles"¥Trend Micro¥Deep Security Agent¥dsa_control" -a $ACTIVATIONURL "tenantID:[redacted]
[redacted]" "token:[redacted]"
#& $Env:ProgramFiles"¥Trend Micro¥Deep Security ¥dsa_control" -a dsm://agents.deepsecurity.trendmicro.com:443/ "tenantID:[redacted]
[redacted]" "token:[redacted]"
Stop-Transcript
echo "$(Get-Date -format T) - DSA Deployment Finished"
</powershell>
```

④プロンプトを使って、DSAをDSMに登録する (1)

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.管理者モードで起動したプロンプトより、DSAのフォルダに移動します

2. PROXY配下の場合は下記コマンドを実行してProxyを登録します

```
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
お客さま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C1WS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 -y “relay_proxy://<プロキシサーバのURL>/"	AgentがRelay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 -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ない）。

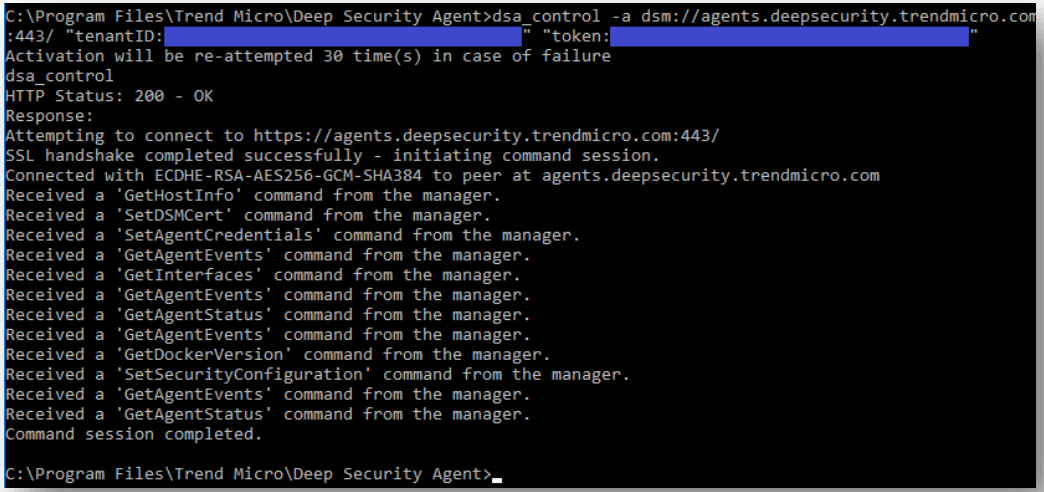
④プロンプトを使って、DSAをDSMに登録する (2)

プロンプトでDSM登録コマンドを実行し登録する (2)

3. 手順２で確認した”テナントID”と”テナントパスワード”を利用して下記のコマンドを実施し、C1WSに登録します。

```
dsa_control –a dsm://agents.deepsecurity.trendmicro.com:443/ “tenantID:＜テナントID＞” “token:＜テナントパスワード＞”
```

(出力結果例)



⑤C1WSへの登録完了確認

正しく有効化が行われれば、C1WSコンソール上 で“管理対象”と表示されます。

これで、インストール作業は完了です。

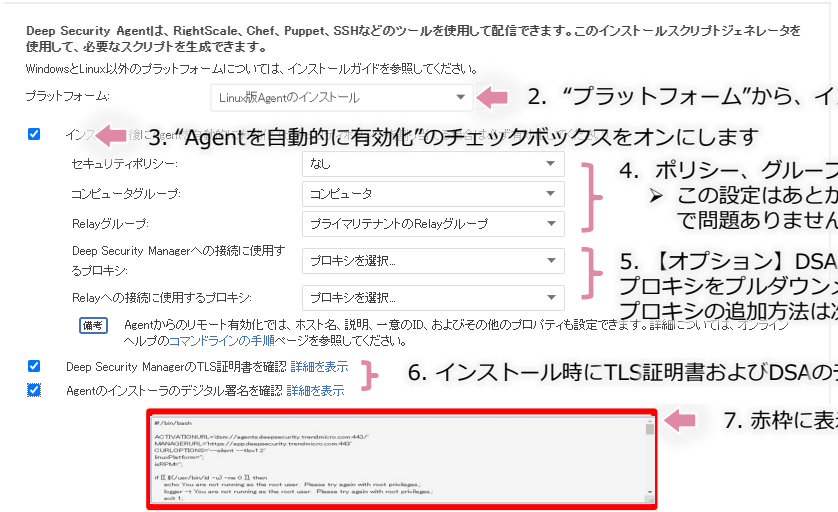
Linux 手法①
C1WSで作成したインストールスクリプトをShellで実行

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、PowerShell上で使用します。)

インストールスクリプト

1. C1WS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問題ありません。

5. 【オプション】DSAがC1WSとの接続でプロキシを経由して接続する場合は、プロキシをプルダウンメニューより選択します。
   プロキシの追加方法は次のページを確認してください。

6. インストール時にTLS証明書およびDSAのデジタル署名を検証する場合は、チェックをつけます。

7. 赤枠に表示されたスクリプトをコピーします。

②インストールスクリプトを実行します

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. C1WSコンソールからインストールスクリプトをコピーし、実行します。 `[root@Linux02 ~]# ./install.sh` で実行

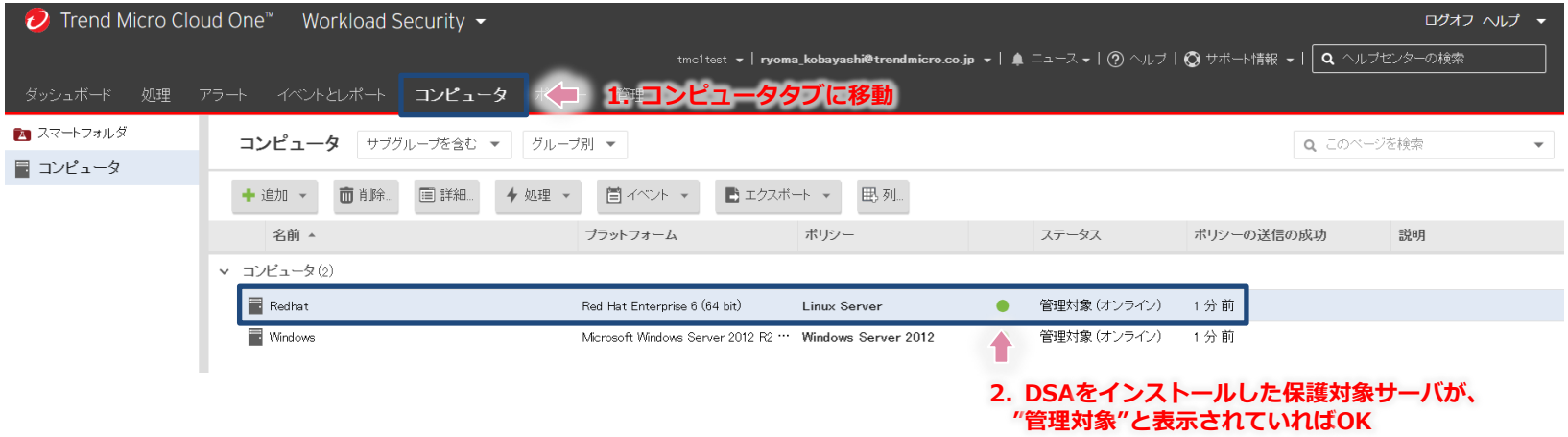
```
#!/bin/bash

ACTIVATIONURL='dsm://agents.deepsecurity.trendmicro.com:443/'
MANAGERURL='https://app.deepsecurity.trendmicro.com:443'
CURLOPTIONS='--silent --tlsv1.2'
linuxPlatform='';
isRPM='';

if [[ $(/usr/bin/id -u) -ne 0 ]]; then
    echo You are not running as the root user.  Please try again with root privileges.;
    logger -t You are not running as the root user.  Please try again with root privileges.;
    exit 1;
```

③C1WSへの登録完了確認

正しく有効化が行われれば、C1WSコンソール上 で“管理対象”と表示されます。



これで、インストール作業は完了です。

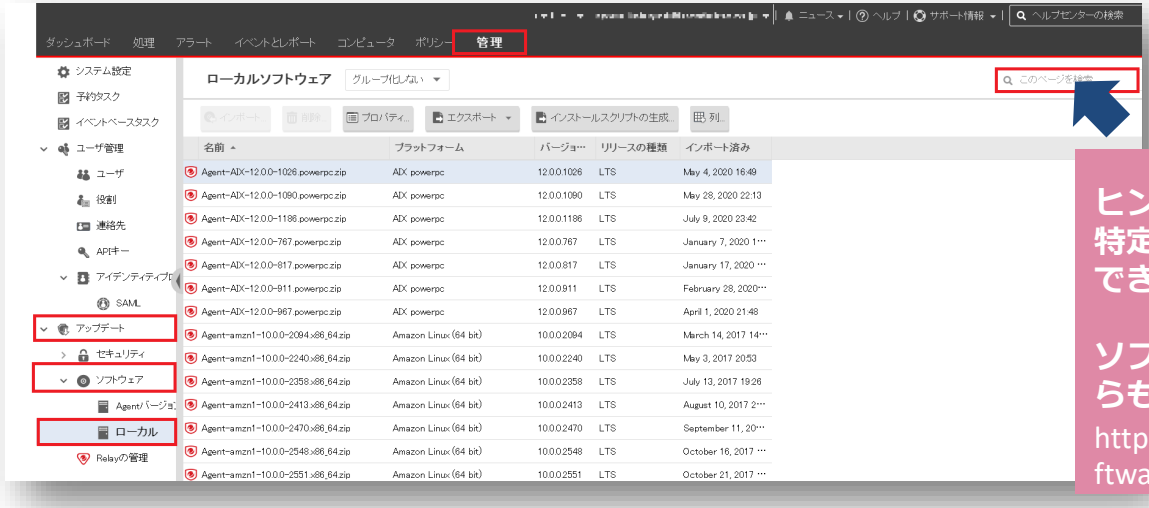
Linux 手法②
インストールパッケージをダウンロード&インストールし
C1WS登録

C1WS / Relayへ接続するためのプロキシの設定方法（コマンドラインでの設定方法）のQ&Aはこちら
https://success.trendmicro.com/jp/solution/1116970

①インストールファイルをダウンロードする

**C1WS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.C1WS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



ヒント：
特定のプラットフォームを入力し、検索できます。（例：RedHat）

ソフトウェアはダウンロードセンターからも入手できます。
https://help.deepsecurity.trendmicro.com/software.html

2.インストールするパッケージを右クリックし、[パッケージのエキスポート]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.前述の手順でダウンロードしたzipファイルを解凍し、rpmパッケージをインストール対象のサーバにコピーします

2.RPMを使ってインストールします

```
# rpm -i <インストーラ名>
 例
# rpm -i Agent-Core-RedHat_EL6-12.0.0-967.x86_64.
```

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

テナントIDとテナントパスワードを抜き出す

1.C1WSコンソールの右上「サポート情報」から「インストールスクリプト」を開き、
プラットフォームの項目にてLinuxを選択します。

2. tenantID: <テナントID>
token: <テナントパスワード>
上記2つをコピーします

※これがプロンプトで実行する、C1WS登録(有効化)のコマンドになります
注意：tenantIDとtokenは、C1WSコンソールから、各アカウント毎に生成してください。

```
sleep 15
/opt/ds_agent/dsa_control -r
/opt/ds_agent/dsa_control -a $ACTIVATIONURL "tenantID:[redacted]" "token:[redacted]
251F26A026FE"
```

④shellでDSAをDSMに登録する

DSM登録コマンドを実行し登録する
＊Proxy配下の場合は1の手順を実施

1. PROXY配下の場合は下記コマンドを実行します

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

構文	備考
dsa_control -x "dsm_proxy://<プロキシサーバのURL>/"	AgentがC1WS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 -y “relay_proxy://<プロキシサーバのURL>/"	AgentがRelay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 -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。

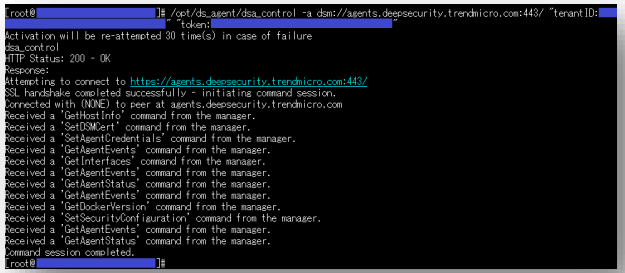
Proxy認証でユーザ/パスワードがある場合は -Uを使って登録してください
＊注意：Basic認証のみ利用できます
Digest認証とNTLM認証はサポートしていません

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ない）。

2. 前のページで確認した“テナントID”と“テナントパスワード”を使用し、下記コマンドを実行します

```
# /opt/ds_agent/dsa_control -a dsm://agents.deepsecurity.trendmicro.com:443/ ”tenantID:<テナントID>” “token:<テナントパスワード>”
```

(出力結果例)



⑤C1WSへの登録完了確認

正しく有効化が行われれば、C1WSコンソール上 で“管理対象”と表示されます。

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C1WSとDSA間での双方向通信が出来ない場合、C1WSの通信方向設定を以下の通り変更して下さい。

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仮想パッチの自動適用確認

~はじめてのC1WS①~

初期設定手引きとして、仮想パッチの設定をご紹介を致します。

①侵入防御の有効化

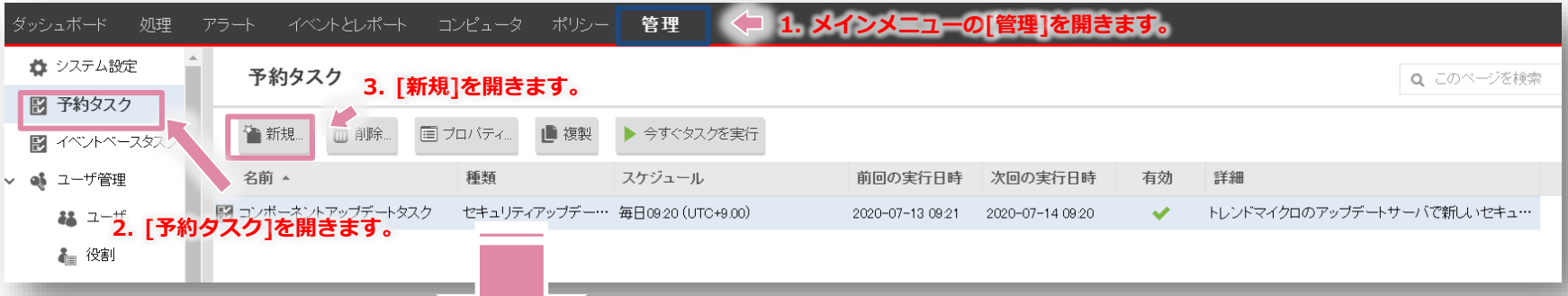
仮想パッチ機能を利用するために、最初に侵入防御モジュールを有効にします。
仮想パッチを使いたいコンピュータ画面を開き、「侵入防御」のステータスを
「オン」、侵入防御の動作を「防御」にします。

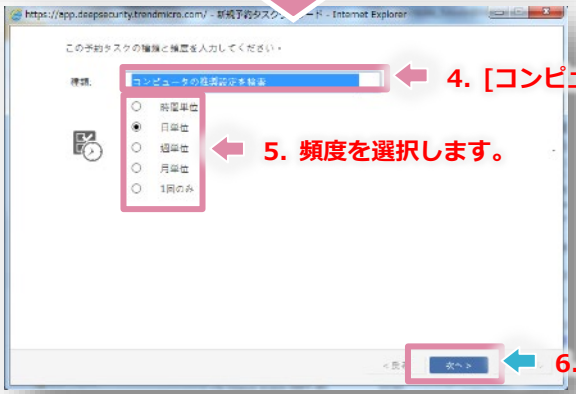
②侵入防御の自動割り当て設定オン

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。

③推奨設定のタスク作成-1

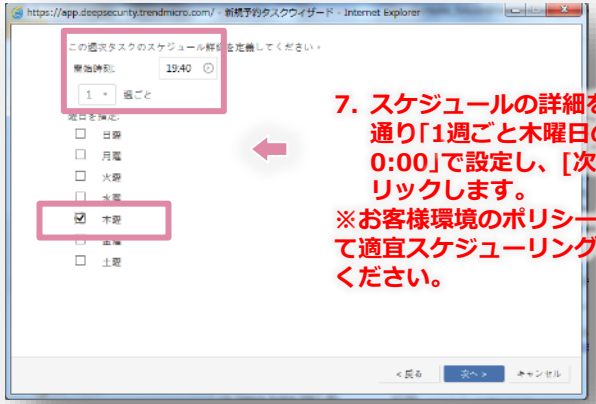
DSAが定期的に仮想パッチルールの洗い出しを実行できるように推奨設定のスケジュール設定を行います。



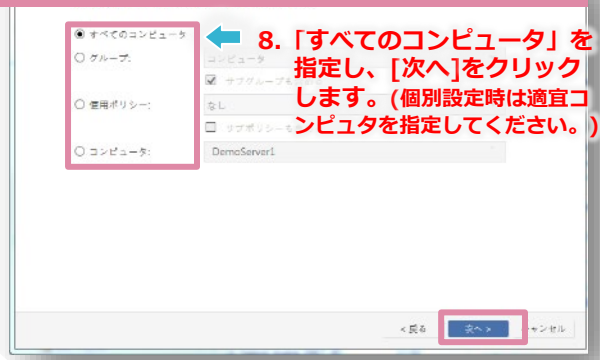


③推奨設定のタスク作成-2

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。



7. スケジュールの詳細を左記の通り「1週ごと木曜日の0:00」で設定し、[次へ]をクリックします。
※お客様環境のポリシーに応じて適宜スケジューリングをしてください。



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。)

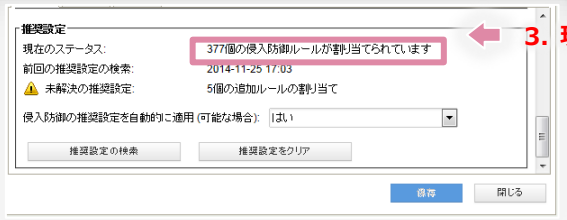
9. タスク名を入力します。

完了を押すと、一回目の推奨設定の検索が行われます。

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。

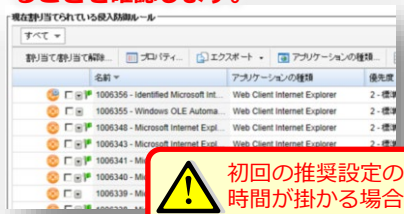
④仮想パッチの自動適用確認

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。



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。

※推奨設定で洗い出されたルールには旗のマークが付きます。

以上で、仮想パッチの推奨設定検索の設定は完了です。

~はじめてのC1WS②~

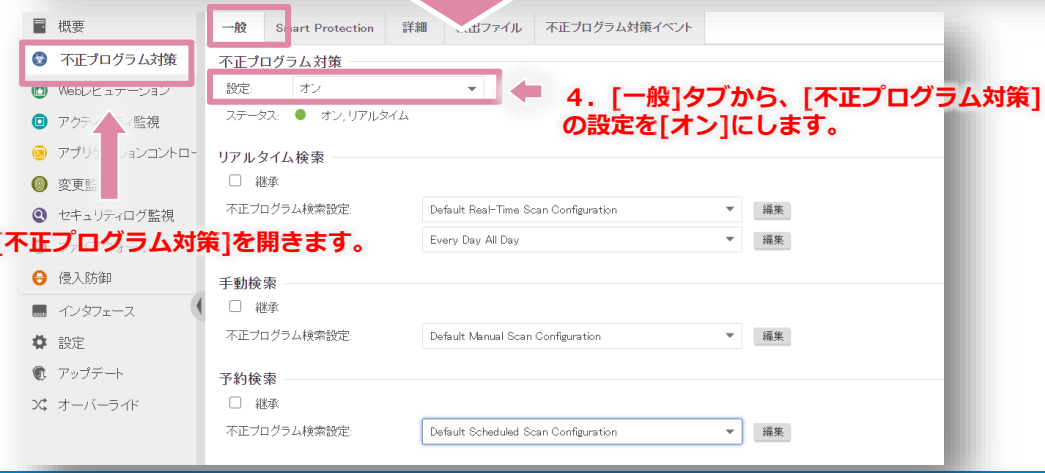
初期設定手引きとして、不正プログラム対策の設定をご紹介を致します。

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。

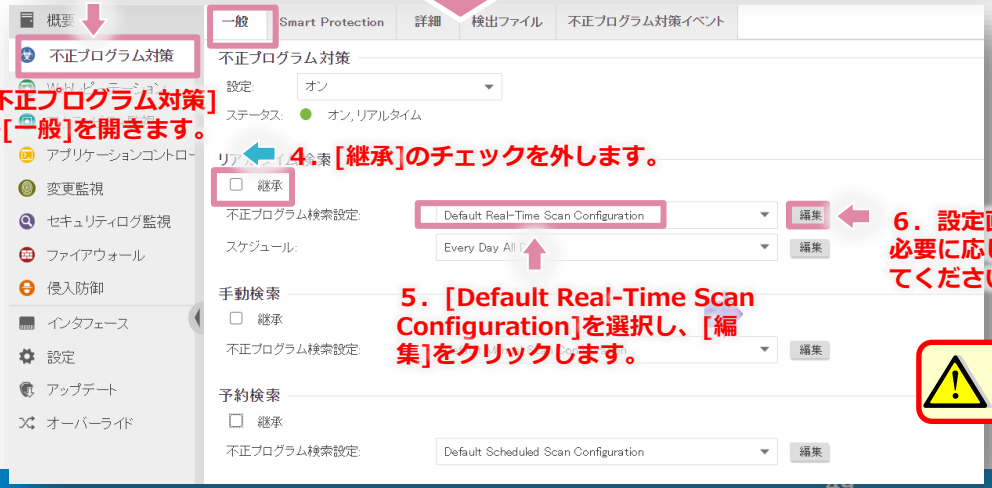


①不正プログラム対策の有効化

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・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。



3. [不正プログラム対策]→[一般]を開きます。

4. [継承]のチェックを外します。

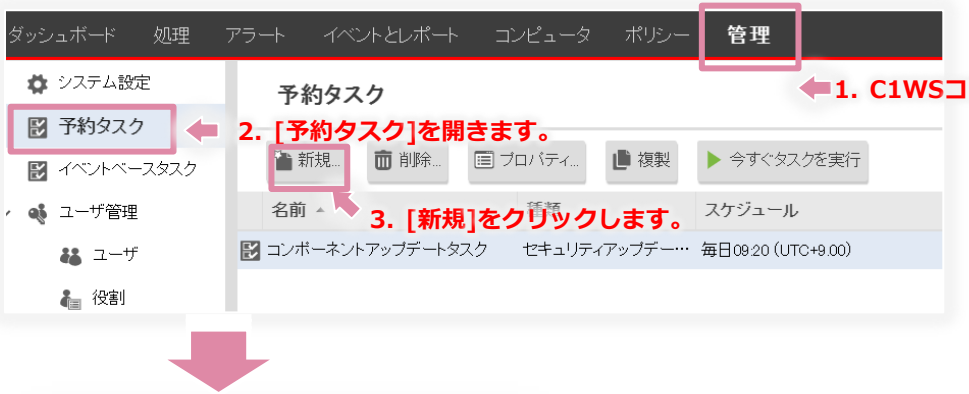
5. [Default Real-Time Scan Configuration]を選択し、[編集]をクリックします。

6. 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

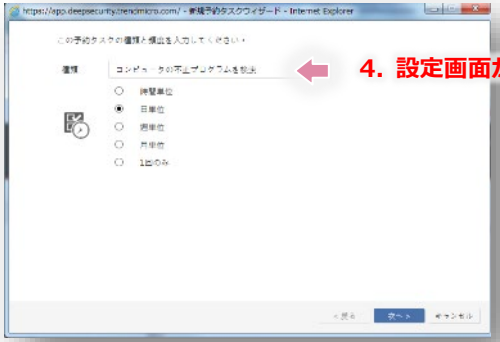
必要に応じてスケジュールを設定し、不正プログラム対策機能の定期スキャンを設定します。



1. C1WS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。

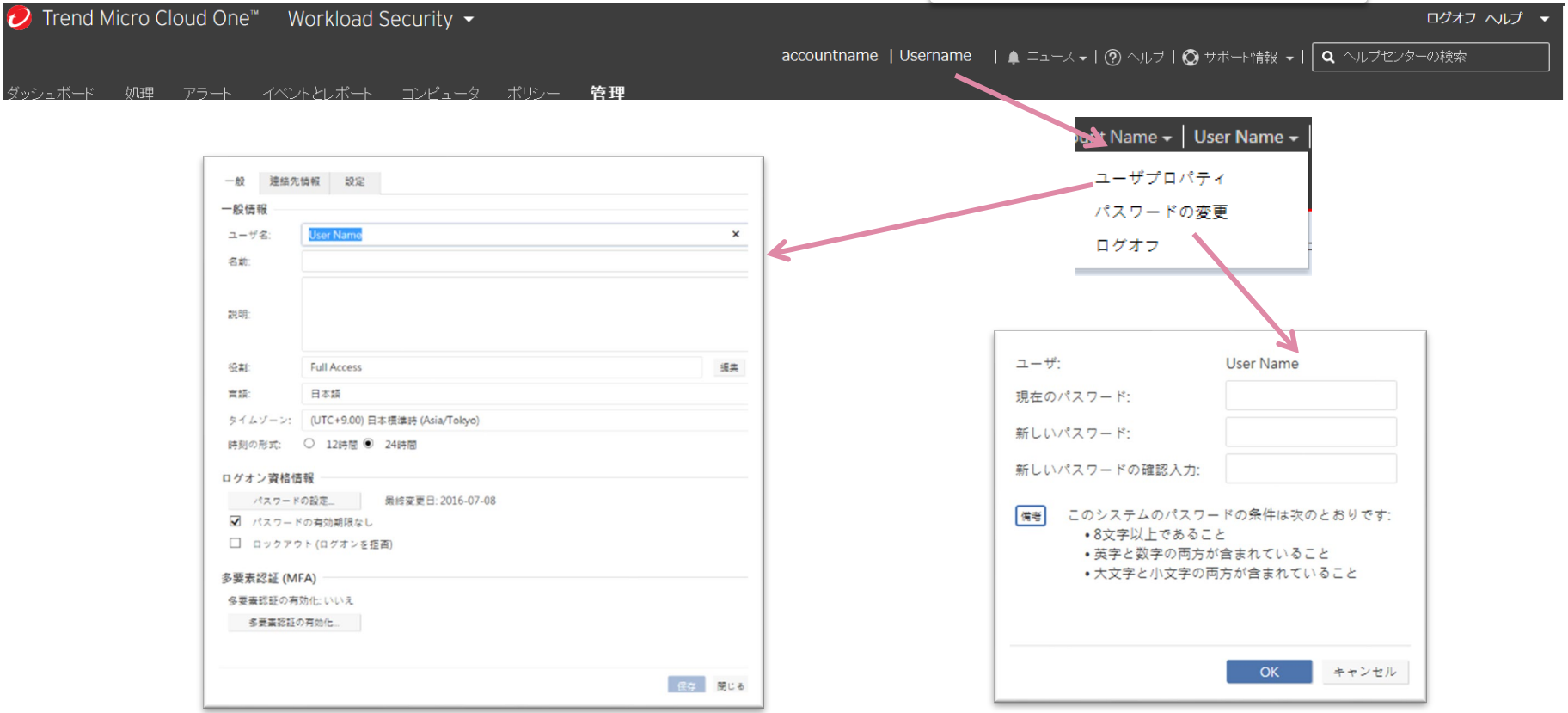
(詳細設定はC1WSC1WSコンソールのヘルプにあるマニュアルをご参照ください。)

C1WS: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	C1WSコンソールバージョンを確認できます

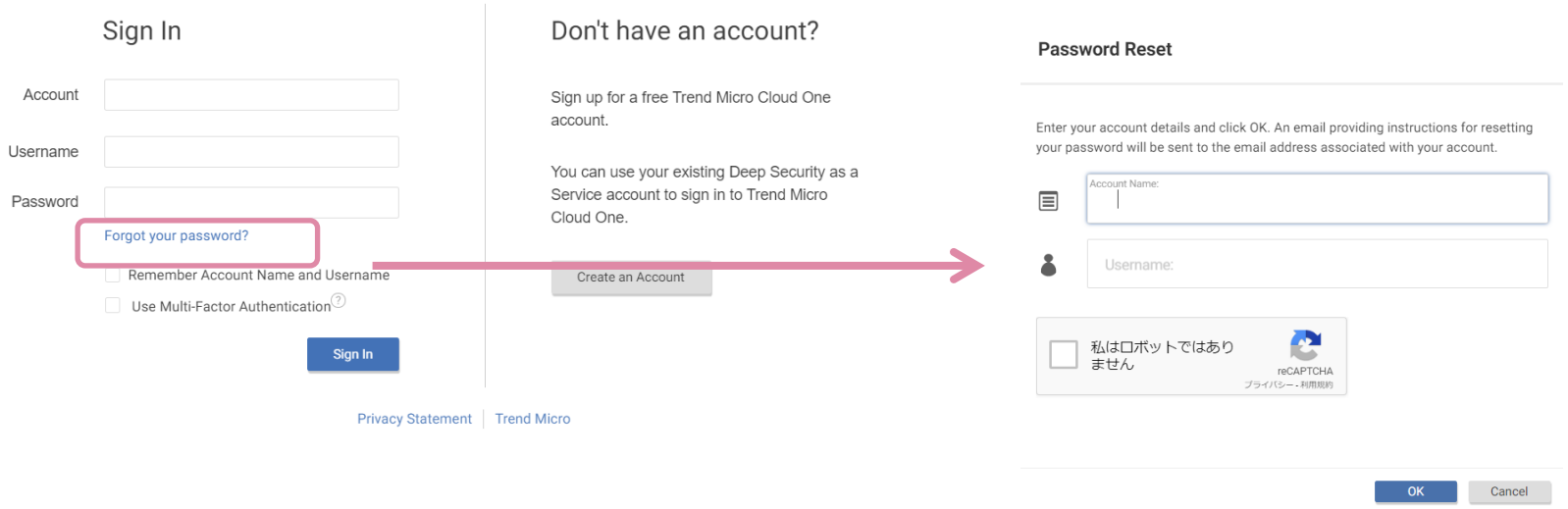
C1WS:ユーザプロパティ

ユーザ情報、パスワードの変更などの編集が行えます



C1WS：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



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。 Auto-Scaling機能で増えたインスタンス数の分、C1WSのライセンスを追加購入する必要がございますのでご注意ください。 ※販売店さまによって上記の限りではない場合もございます。詳しくは購入元の販売店さまにお問い合わせください。
DSAが攻撃を検知した時や、オフラインになった時等、C1WS管理マネージャから管理者に通知メールは届きますか？	届きます。 メールアドレスは[管理]＞[ユーザ管理]＞[ユーザ]よりユーザごとに登録が可能です。
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。 本資料のP45をご参加ください。
ルールのチューニングは可能ですか？	可能です。 [ポリシー]＞[ルール]＞[侵入防御ルール]より該当のルールをダブルクリックで詳細設定が可能です。
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。
C1WSコンソール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。 本資料のP45に記載のある予約タスクの設定から、[レポートの生成および送信]を選択することが出来ます。
C1WS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でも、DSAが動作を止めることはありません （参考FAQ:https://success.trendmicro.com/jp/solution/1310095）
C1WS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？	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。
C1WSコンソール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C1WSログオン後に、ユーザプロファイル＞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、C1WSに移行したい場合、設定を移行することは可能でしょうか?	設定の移行、ログの移行共にできません。 設定のExport/Import機能はありますが、C1WSの仕組み上お使いいただくことができません。
C1WS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C1WS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	C1WSコンソールから、[コンピュータ]で該当サーバをダブルクリックして詳細を開きます。[概要]> [処理] 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。
C1WSの製品FAQはどこにありますか？	C1WSが提供しているDSAは基本的にパッケージ版のDSと同機能を提供しています。C1WSの製品FAQはDSのFAQを参照してください。
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、デモサーバではないサーバにDSAをインストールしてOKか？	可能です。
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？	C1WSにはDSAバージョンコントロール機能があります。 https://cloudone.trendmicro.com/docs/jp/workload-security/agent-version-control/

FAQ　～製品仕様関連③～

質問	回答
C1WS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、C1WS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 IPアドレスの詳細はhttps://cloudone.trendmicro.com/docs/workload-security/communication-ports-urls-ip/を確認してください。 ※IPアドレスは不定期に追記されます。
C1WS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？	保存期間が4週間（32日）に変更となります。
C1WS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。 ①C1WS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、C1WS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）
C1WS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：C1WS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：①C1WS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②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
C1WS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せんか？	●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 ⇒ https://success.trendmicro.com/jp/solution/1097204 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みてください。

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？	購入元の販売店さまとの契約次第となります。
C1WSの取り扱いをしている販売店は？	C1WSをお取扱いいただいている販売店さまは、下記Webページをご参照ください。 http://www.trendmicro.co.jp/jp/business/solutions/saas/
標準価格はありますか？	ありません。C1WSに標準価格設定はなく、価格は販売店さまにて決定しております。
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。
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。ご注意ください。

サポートページ⇒　https://success.trendmicro.com/jp/product-support/cloud-one-workload-security