

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 2021年8月現在の情報となります

DAIWABO INFORMATION SYSTEM CO., LTD. CONFIDENTIAL



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



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)

Dis 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。



DAIWABO INFORMATION SYSTEM CO., LTD. CONFIDENTIAL



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.C1WS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 [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

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



Tr



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/

nd Micro Cloud One™			<u>English</u> 日本語 ヘルプ マ		
end Micro Cloud One					
				c.	
	ログオン				
	アカウントとユーザ名 メールアドレス				
	メールアドレス: *				
	パスワード:*				
	アカウントを記憶				
	エクオン				
	サインアップ				
	Trend Micro Cloud Oneの 30日間の無償体験版 をお ださい。				\+ + <u>`</u> +
		1	こちらの"サイン 登録フォームを	アッフ [~] をクリックし ·開いてください。	いこにさ、
© 2020 Trend Micro Inc.		1 min			



Dis 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。

 \sim

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。

Cloud Oneにサインアップ

メールアドレス: *

名前: *



国: *

国を選択..

パスワード:*

パスワードの確認入力:*



<u>使用条件</u>、 <u>プライバシーポリシー (Global Privay Notice)</u>、およ

び<u>データ収集について</u>同意します。

サインアップ

すでにCloud Oneユーザとして登録していますか? ログオン

> すべての項目をご記入し、 使用許諾を確認し、 サインアップします。



つ「 シアカウントの作成

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
メールアドレス	ログイン時に使用します。
名前	任意の名前を入力します。
国	Japanを選択します。
パスワード/パスワードの確認入力	ログイン時のパスワードを入力します。







13

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。

Trend Micro Cloud One ™

curity Services Platform for Cloud Builders

Hello, _____

Thank you for signing up for Trend Micro Cloud One! To continue, please verify your email address using the link below. This link will expire in 24 hours.

Verify Emai

If the button isn't working, paste the following URL into your browser:

https://cloudone.trendmicro.com/?email=





2.C1WSコンソールへのログインと 利用開始の準備

①C1WS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



①C1WSコンソールにログインする



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





2. ダッシュボード画面の「Workload Securityアカ ウントの詳細」をクリックします。



1



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

〒1-12 [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

<u>アクティベーションコード:0x-00xΔ-Δ0x0ロ-xxロΔ0-Δロx★x-Δ0ロxx-Δロ★x0</u> 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 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。

アカウントの詳細

2.ダッシュボード画面の 「ライセンスのアップデート」を クリックします。

アカウント	
種類:	Cloud Oneによるライセンス許可
ステータス:	● 有効
作成日:	July 14, 2021 00:58
現在の保護対象数	0台

ライセンスのアップデート

アカウント ―― 種類:	Licensed through Cloud One	
新しいライセンス	情報	
◎ アクティベーシ	コンコード	

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。)



1



3.DSAインストール



Windows 手法 ① C1WSで作成したインストールスクリプトを実行







20

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。)

פֿעור 🕐	ログオ: 〇 サポート情報 - Q ヘルブセンターの検索	ر مراج مراج مراج مراج مراج مراج مراج مرا	/S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。
サポー	トリ香幸居			
インスト Agentの	ールスクリプト りダウンロード + ウィジェ:	水 の追加/削除…		
使用許	諾契約書			
コメント	およびフィードバック			
バージ	ョン情報			
インフ	(トールスクリプト			
Deep	Security Agentiz, RightScale, Chef, P	uppet、SSHなどのツールを使用して配信	できます。このインス	ストールスクリプトジェネレータを
使用	て、必要なスクリプトを生成できます。			
Window	wsとLinux以外のブラットフォームについては、~	インストールガイドを参照してください。		
ブラッ	~フォーム: Windows版	iAgentのインストール	2. "プラッ	ットフォーム"から、インストール対象のOSを選択します。
	心ス」創る:#"Agentを自	動的に有効化"のチェッ?	クボックスを	こ オンにします
	セキュリティポリシー:	ねし		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。
	コンピュータグループ:	コンピュータ	-	····································
	Relayグループ:	プライマリテナントのRelayグループ	•	で問題ありません。
	Deep Security Managerへの接続に使用す るプロキシ:	プロキシを選択	-] 5	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、
	Relayへの接続に使用するプロキシ:	プロキシを選択	- I -	フロキシをフルタワンメニューより選択します。
	備考 Agentからのリモート有効化では、 ヘルプのコマンドラインの手順ペー	ー ホスト名、説明、一意のID、およびその他の -ジを参照してください。	ブロバティも設定できま	フロキシの追加方法は次のページを確認してくたさい。 す。詳細に入れば、オンライン
✓	Deep Security ManagerのTLS証明書を確認	詳細を表示 6 インフト		S証明書お上びDSAのデジタル要名を検証する提合け、チェックをつけます
~	Agentのインストーラのデジタル署名を確認	細を表示		
	requires -version 4.0			□ 7 赤枠に表示されたスクリプトをコピーします。
© 2020	Trend N This script detects platform and architecture	ript It then downloads and installs the relevant Deep Security Ape	nt package	
	r(-NDT (SecurityPrincipal) Administrator")) {	[SecurityPrincipal.WindowsIdentity]:GetCurrent())JsInRole([Sec	urity Principal Mindows Buildin Role	
	Write-Warning "You are not running as an A exit 1	dministrator. Please try again with admin privileges."		



【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

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。

本作業は保護対象サーバ上 での作業となります。



- 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
- 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。

💋 Trend Micro Clo	ud One™ Workload Security ▼					ログオフ ヘルプ 🔻
ダッシュボード 処理 🎵		1.コンピュータタ	ブに移動	• • 🌲 ニュース • 🕐 ヘルブ (🛇 サポート情報 👻	🔍 ヘルブゼンターの検索
🛃 スマートフォルダ	コンピュータ サブグループを含む マ グループ	別 🔻				Q、このページを検索 ▼
📑 コンピュータ						
	+ 追加 ▼ □□ 削除 □ 詳細	□ イベント マ □ エクスボ・	-ト ▼ 囲,列			
	名前	ブラットフォーム	ポリシー	ステータス	ポリシーの送信の	成功 説明
	➤ コンピュータ(2)					
	冒 Redhat	Red Hat Enterprise 6 (64 bit)	Linux Server	● 管理対象 (オンライン)	1分前	
	Windows	Microsoft Windows Server 2012 R2 …	Windows Server 2012	🕚 管理対象 (オンライン)	1分前	
				\mathbf{A}		
			2	2. DSAをインストール "管理対象"と表示され	した保護対 れていればC	I象サーバが、 DK

これで、インストール作業は完了です。



DIS





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

			i e li e le legend ledergred	di nasala kana sa ja 😿	🌲 ニュース 🗸 ② ヘルブ 🛇 サポート情報 🖌
ダッシュボード 処理	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			
✿ システム設定 闘 予約タスク	ローカルソフトウェア グル	- ガ化ない マ			٩
	Q インボート。	コバティ 📑 エクスポート 👻	■ インストールスグリプトの生成.		
◇ 🝓 ユーザ管理	名前 🔺	ブラットフォーム	バージョー・・ リリースの種類	インボート済み	
46 ユーザ	Agent-AIX-12.0.0-1026.powerpc.zip	AIX powerpc	12.0.0.1026 LTS	May 4, 2020 16:49	
よ っ 役割	Agent-ADX-12.0.0-1090.powerpc.zip	AIX powerpc	12.0.0.1090 LTS	May 28, 2020 22:13	
□ 連絡先	Agent-ADC-12.0.0-1186.powerpc.zip	AIX powerpc	12.0.0.1186 LTS	July 9, 2020 23:42	
Δρι±	Agent-ADX-12.0.0-767.powerpc.zip	AIX powerpc	12.0.0.767 LTS	January 7, 2020 1…	
	Agent-ADX-12.0.0-817.powerpc.zip	AIX powerpc	12.0.0.817 LTS	January 17, 2020 …	
• • • • • • • • • • • • • • • • • • • •	Agent-ADX-12.0.0-911.powerpc.zip	AIX powerpc	12.0.0911 LTS	February 28, 2020***	
() SAML	Agent-ADC-12.0.0-967.powerpc.zip	ADX powerpc	12.0.0.967 LTS	April 1, 2020 21:48	
 ・ ・ ・	Agent-amzn1-10.0.0-2094.x88_64.zip	Amazon Linux (64 bit)	10.0.2094 LTS	March 14, 2017 14***	
> 🔒 セキュリティ	Agent-amzn1-10.0.0-2240.x88_64.zip	Amazon Linux (64 bit)	10.0.2240 LTS	May 3, 2017 2053	
✓ ◎ ソフトウェア	Agent-amzn1-10.0.0-2358.x86_64.zip	Amazon Linux (64 bit)	10.0.2358 LTS	July 13, 2017 19:26	
📕 Agentバージョン	8.64.zip 8.64.zip	Amazon Linux (64 bit)	10.0.0.2413 LTS	August 10, 2017 2	
= ローカル	Agent-amzn1-10.0.0-2470.x88_64.zip	Amazon Linux (64 bit)	10.0.0.2470 LTS	September 11, 20***	
	Agent-amzn1-10.0.0-2548.x88_64.zip	Amazon Linux (64 bit)	10.0.02548 LTS	October 16, 2017 …	
•	Agent-amzn1-10.0.0-2551 x88_64.zip	Amazon Linux (64 bit)	10.0.02551 LTS	October 21, 2017 ···	

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

	Agent-Windows-12.0.0-967.386.zip	Microsoft <mark>Windows</mark> (32 bit)	12.0.0.967	LTS	April 1, 2020 22:05
	Agent-Windows-12.0.0-967.x86_64.zip	Microsoft <mark>Windows</mark> (64 bit)	12.0.0.967	LTS	April 1. 2020 22:02
	Agent-Windows-12.5.0-1033.i386 zip	Microsoft <mark>Windows</mark> (32 bit)	12.5.0.1033	FR	すべて選択 (250)
	Agent-Windows-12.5.0-1033.x86_64.zip	Microsoft <mark>Windows</mark> (64 bit)	12.5.0.1033	FR	・ 🖹 バッケージのエクスポート
	Agent-Windows-12.5.0-713.386.zip	Microsoft <mark>Windows</mark> (32 bit)	12.5.0.713	FR	🖹 インストーラのエクスボート
25	Agent-Windows-12.5.0-713.x86_64.zip	Microsoft <mark>Windows</mark> (64 bit)	12.5.0.713	FR	■ ブロバティ
	Agent-Windows-12.5.0-834.086.zip	Microsoft <mark>Windows</mark> (32 bit)	12.5.0.834	FR)







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。





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。

インストールスクリプト	
Deep Security Agentは、Righ 要なスクリプトを生成できます	ale、Chef、Puppet、SSHなどのツールを使用して配信できます。このインストールスクリプトジェネレータを使用して、タ
WindowsとLinux以外のブラット	ームについては、インストールガイドを参照してください。
ブラットフォーム:	Windows版Agentのインストール 🔹

2. tenantID: <テナントID>※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
token: <テナントパスワード>上記2つをコピーする注意: 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: " " token: #& \$Env:ProgramFiles "¥Trend Micro¥Deep Security ¥dsa_control" -a dsm://agents.deepsecurity.trendmicro.com.443/ " tenantID: " " token: " token: Stop-Transcript echo "\$(Get-Date -format T) - DSA Deployment Finished" </powershell> 27 © 2020 Trend Micro Inc.





28

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.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

藏管理者: コマン	ドプロンプト		
c:¥Program F ドライブ C ボリューム	「iles¥Trend) のボリューム シリアル番号	licro¥Deep Security Agent>dir *cmd ラベルがありません。 は F42A-0C8D です	
c:¥Program	Files¥Trend	Micro¥Deep Security Agent のディレクトリ	
2014/06/18 2013/11/12 2013/11/12	12:17 13:40 13:39 3個のフ 0個のデ	221 dsa_control.cmd 92 dsa_query.cmd 92 sendCommand.cmd ァイル 405 バイト ィレクトリ 30,576,906,240 バイトの空き領域	

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 【注意!】このアドレスは例ですので Response: dd proxy-address:[dsm_proxy] with value:[192.168.2.103:8080/] dsa_control -x "dsm_proxy://<プロキシ AgentがC1WSとの通信に使用するプロキ 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 サーバのURL>/" シサーバのアドレスを設定します。 *注意: Basic認証のみ利用できます dsa control -x "" プロキシサーバのアドレスをクリアします。 Digest認証とNTLM認証はサポートしていません dsa_control -y "relay_proxy://<プロキシ 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。 サーバのURL>/" 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。 dsa control -u "root:Passw0rd!"



プロキシの認証に、「root」とバスワード「Password!」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)。

Dis

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)

C:\Program Files\Trend Micro\Deep Security Agent>dsa_control -a dsm://agents.deepsecurity.trendmicro.com
:443/ "tenantID: " "token: "
Activation will be re-attempted 30 time(s) in case of failure
dsa_control
HTTP Status: 200 - OK
Response:
Attempting to connect to https://agents.deepsecurity.trendmicro.com:443/
SSL handshake completed successfully - initiating command session.
Connected with ECDHE-RSA-AES256-GCM-SHA384 to peer at agents.deepsecurity.trendmicro.com
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 'GetDockerVersion' 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.
C:\Program Files\Trend Micro\Deep Security Agent>_



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。

🤣 Trend Micro Clo	ud One™ Workload Security →			ログオフ ヘルプ 🔻
ダッシュボード 処理	P7-+ 1×2+21#-+ -222-9	- 1. コンピュータタブに移動	🖡 • 🌲 ニュース • 🕐 ヘルブ 🔇 サボ	ート情報 ✔ 🔍 ヘルブセンターの検索
🔽 スマートフォルダ	コンピュータ サブグループを含む 💌 グルー	ブ別・		Q このページを検索 ▼
📑 コンピュータ				
	昔 追加 → 面前除 □ 詳細 ◆ 処理 →	首イベント ▼ ■ エクスポート ▼ 囲 列		
	名前 🔺	ブラットフォーム ボリシー	ステータス ポリシ・	ーの送信の成功 説明
	> コンピュータ(2)			
	📑 Redhat	Red Hat Enterprise 6 (64 bit) Linux Server	管理対象(オンライン) 1 分前	
	Windows	Microsoft Windows Server 2012 R2 ··· Windows Server 2012	管理対象(オンライン) 1分前	
			\bigtriangleup	_

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 C1WSで作成したインストールスクリプトをShellで実行







32

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。)

⑦ へルゴ サポ・	ログ 1 ② サポート協報 - Q ヘルジセンターの相 -ト協報	1177 ~LJ → 1. C	WS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。
インス Agent 使用 コメン バー:		ジェナの道加/副株		
インス	トールスクリプト			
Deep S 使用し ⁻	Security Agentlä、RightScale、Chef、P て、必要なスクリプトを生成できます。	uppet、SSHなどのツールを使用して酢	できます。このインストールスクリプトジェネレータを	
ブラット:	Sectinuxはないのシンターンオームについては、 フォーム: Linux版Agentの	ロンストール・マンストール・マン	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。	
		動的に有効化"のチェッ	りボックフをオンにします	
_		なし		
	コンピュータグループ:	⊐ンピュ <i>−</i> タ	 4. パリシー、シルーン、Relay、それそれに圧乱のとおり送が ▶ この設定はあとから再設定できます。すでに設定済みの 	でしょう。 設定が無い場合には初期設定のまま
	Relayグループ:	- プライマリテナントのRelayグループ	- で問題ありません。	
	Deep Security Managerへの接続に使用す るプロキシ:	プロキシを選択	▼ 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、
	Relayへの接続に使用するプロキシ:	プロキシを選択	ノロキシをノルタワ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。	
	備考 Agentからのリモート有効化では、 ヘルプのコマンドラインの手順ペー	ホスト名、説明、一意のID、およびその他 - ジを参昭してください。	ゴロバティも設定できます。詳細については、オンライン	
	Deep Security ManagerのTLS証明書を確認 Agentのインストーラのデジタル署名を確認	詳細を表示 詳細を表示 詳細を表示	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。
© 202	20 Trend N Northernet - 1/2 Northernet - 1/2	ity trendmicro.com /43/* verdmicro.com /47	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

[root@Linux02 ~]# ./install.sh 〇美仁

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 ~]# Is -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。

#!/bin/bash

ACTIVATIONURL='dsm://agents.deepsecurity.trendmicro.com'443/' MANAGERURL='https://app.deepsecurity.trendmicro.com'443' CURLOPTIONS='--silent ---tlsv12' 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。

🤣 Trend Micro Clou	ud One™ Work	kload Security 👻							ログオフ へル	プ 🔻
			tmc1test 👻 ry	oma_kobayashi@trendmicro.co	🌲 🗕 qi.	ニュース • ⑦ ヘルブ	◎ サポート情報		センターの検索	
ダッシュボード 処理 🎵	ブラート イベントとし	パート コンピュータ	*(コー 1:=コンピュータ	タブに移動						
🔁 スマートフォルダ	コンピュータ	サブグループを含む 🔻	グルーブ別 🔻					Q 20~-	ジを検索	•
🖥 コンピュータ										
	+ 追加 - (■ 詳細…	処理 ▼	ポート マ 囲 列						
	名前 ▲		ブラットフォーム	ポリシー		ステータス	ボリシーの送信	の成功	説明	
	✓ コンピュータ(2)									
	Redhat		Red Hat Enterprise 6 (64 bit)	Linux Server	•	管理対象(オンライン)	1分前			
	Windows		Microsoft Windows Server 2012 R2	··· Windows Server 2012		管理対象(オンライン)	1分前			
					2	DSAをインスト		P 灌 寸兔	サーバガ	

"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 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

		・マー・マー appane link que di Manenie ban en (g) マ 🌲 ニュース マ ⑦ ヘルブ ③ サポート情報 マ 🔍 ヘルブセン
ダッシュボード	処理 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
システム設定 アメカカスカ	ローカルソフトウェア グループ化しない マ	Q 2014-928
V THINKS	マーク・ボート、 □ 前外、 ■ ブロバティ ■ エクスボー	ト ▼ ■ インストールスクリプトの生成. 田 列.
✓ 🍕 ユーザ管理	名前 - ブラットフォーム	バージョ… リリースの種類 インボート済み
🏭 ユーザ	Agent-ADX-12.0.0-1026.powerpc.zip ADX powerpc	12.0.0.1026 LTS May 4, 2020 16:49
る 』 役割	Agent-ADX-12.0.0-1090.powerpc.zip ADX powerpc	12.0.0.1090 LTS May 28, 2020 22:13
E目 連絡先	Agent-ADX-12.0.0-1188.powerpc.zip ADX powerpc	12.0.0.1186 LTS July 9, 2020 23:42
==	Agent-AIX-12.0.0-767.powerpc.zip AIX powerpc	12.00.767 LTS January 7, 2020 1
	Agent-AIX-12.0.0-817.powerpc.zip AIX powerpc	12.0.0.817 LTS January 17, 2020 ····
V 🖸 7472	A 214 24 (S Agent-ADX-12:0.0-911.powerpc.zip ADX powerpc	12.0.0.911 LTS February 28, 2020
(B) SAN	Agent-AIX-12.0.0-967.powerpc.zip AIX powerpc	12.0.0967 LTS April 1, 2020 21:48
✓ ⑦ アップデート	S Agent-amzn1-10.00-2094.x86_64.zip Amazon Linux (64 bit)	10.002094 LTS March 14, 2017 14…
> 🔒 セキュリ	Agent-amzn1-10.00-2240.x86_64.zip Amazon Linux (64 bit)	10.002240 LTS May 3, 2017 2053
Vフトウェ	7 🖲 Agent-amzn1-10.00-2358.x86_64.zip Amazon Linux (64 bit)	10.002358 LTS July 13, 2017 19:26
Age	t/ 「ージョ」 🖲 Agent-amzn1-10.00-2413.x86_64.zip Amazon Linux (64 bit)	10.002413 LTS August 10, 2017 2***
= D-	カル 🖲 Agent-amzn1-10.0.0-2470.x86_64.zip Amazon Linux (64 bit)	10.0.2470 LTS September 11, 20***
Selav⊘ĵ	Agent-amzn1-10.0.0-2548.x86_64.zip Amazon Linux (64 bit)	10.0.2548 LTS October 16, 2017
♦	- (8) Agent-amzn1-10.0.0-2551.x86_64.zip Amazon Linux (64 bit)	10.0.02551 LTS October 21, 2017

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





つう 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 DIS

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。

インストールスクリプト		
Deep Security Agentは、RightScale、(要なスクリブトを生成できます。	Shef、Puppet、SSHなどのツールを使用し	して配信できます。このインストールスクリブトジェネレータを使用して、必
WindowsとLinux以外のブラットフォーム	こついては、インストールガイドを参照して	てください。
ブラットフォーム:	Linux版Agentのインストール	¥

2. tenantID: $\langle \overline{\tau} \rangle$ 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。







39

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>/"

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。	Provy認証でユーザバプロードがある提合け _I	1を使って登録してください
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。	*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 "<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。	dsa_control -u "root:PasswOrd!"	プロキシの認証に、「root」とパスワード「PasswOrd!」を使用します(基本認証のみ。Diges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>"





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。

🤣 Trend Micro Clo	ud One™ Workload Security ▼					ログオフ ヘルプ 🔻
ダッシュボード 処理 🗌	די אינ צעב אראיניאין אינאראין אינא	tmc1test - ryom	a_kobayashi@trendmicro.co.jp アブに移動	• ▲ ニュース • ⑦ ヘルブ	② サポート情報 → Q ヘルブセ	ンターの検索
📐 スマートフォルダ	コンピュータ サブグループを含む マ グルー	ブ別 👻			Q 20~-9	を検索 ▼
📑 コンピュータ	+ 追加 → 前削除 ■詳細 + 処理 -	首 イベント マ ■ エクスボ	-ト ▼ 囲列			
	名前 ▲	プラットフォーム	ポリシー	ステータス	ボリシーの送信の成功	説明
	▼ コンビュータ(2)					
	📕 Redhat	Red Hat Enterprise 6 (64 bit)	Linux Server	● 管理対象 (オンライン)	1 分前	
	Windows	Microsoft Windows Server 2012 R2 …	Windows Server 2012	管理対象 (オンライン)	1分前	
_		_	_	2. DSAをインスト "管理対象"と表	〜ールした保護対象サ 示されていればOK	ナーバが、

これで、インストール作業は完了です。













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。

	コンピュータ	✔ サブグループを含む ▼ グループ別	•					Q このページを検索
コンピュータ				_				
	+ 追加 ▼	■ 削除 🗉 詳細 🕈 処理 👻	□ イベント マ □ エクス)	∜─ト ▼ 問列				
	名前 ▲	7	ラットフォーム	ポリシー		ステータス	ボリシーの送信	の成功 説明
	▼ コンピュータ(2)							
	Redhat	Re	ed Hat Enterprise 6 (64 bit)	Linux Server		音2:家該当コン	ピュータ	画面を開きます
	Windows	м	crosoft Windows Server 2012 R2 *	··· Windows Server 2012		管理対象(オンライン)	2 時間 前	
	_							
	Law 2007							
	■ 概要	An, all dan a set i ge de SM						
	 	通信方向		4. []	ンピュ	ータ]タブを開	き、[通	
	 祇要 不正プログラム対策 Webレビュテーション 	通信方向 00.1.5.1.1.1.1.1.1.0.2.mで注意すの	SNG2 (A	4. [그	ンピュ [.] 5向1で	ータ]タブを開 "Agent/App	lき、[通 lianceか	
	 概要 不正プログラム対策 Webしビュテーション アクティビティ監視 	通信方向 つー 0-10-10-10-10-10-10-10-10-10-10-10-10-10		4. [コ 信方	ンピュ 5向]で 100/100	ータ]タブを開 "Agent/App 選択します	lき、[通 lianceか	
	 祇要 不正ブログラム対策 Webレビュテーション アクティビティ監視 アブリケーションコントロー 	通信方向 う う い い い い い い い の 3000000 ハートビート	(99-20-(AA	4. [コ 信が ら開	ンピュ [.] 5向]で 1 1 開始"を	ータ]タブを開 "Agent/App 選択します。	lき、[通 lianceか	
	 	通信方向	(明定 (A)APP)に同時4.6) (総要 (10 分) (総事 (3)	● 4. [コ 信だ ら開	ンピュ 5向]で 16/10	ータ]タブを開 "Agent/App 選択します。	lき、[通 lianceか	
	 祝要 不正ブログラム対策 アレディビディ監視 アブリケーションコントロー 変更監視 セキュリティログ監視 	通信方向 ハートビート ハードビート ハッガを超えるハードビートが失われた場合にアラーを発令 ハートビート間隔 、、、の数を超えるハービーが失われた場合にアラーを発令、 ハートビート間でコンピュージのローカルジステム時間が次の時間を	46-27 (A /A - ク - A)に定用(AA) 截手(10 分) 截手(5) 超す(5) 26	4. [コ 信だ ら開 5. [f	ンピュ [.] 5向]で 1 1 開始"を 1 8 合]を	ータ]タブを開 "Agent/App 選択します。	き、[通 lianceか い。	
	 秋要 スポブログラム対策 マレングングラインディ監視 アクティビティ監視 アブリケーションフルロー 変更整視 セキュリティログ監視 ファイアウォール 	通信方向 ハートビート ハービート増展 大の数を超えるハードビーが快われた場合にフラートを発売。 ハービー増度にシビュージのローカルジステム時間が次の時間を えて変更がた場合にフラートを発売。	#All (10 分) 截承 (10 分) 截承 (10 分) 截承 (10 例)	4. [コ 信だ ら開 5. [f	ンピュ・ 5向]で 閉始"を 呆存]を	ータ]タブを開 "Agent/App 選択します。 :押してくださ!	lき、[通 lianceか い。	
	 祝要 スポブログラム対策 アルブログラム対策 アクティビティ監視 アブリケーションコントロー 変更監視 セキュリティログ監視 ファィアウォール (a) 5cm 	通信方向 ハートビート ハーレビーや問題 次の数を超えるハートビーが外失われた場合にフラートを発売 ハービー相同にコンビュータのローカルシステム時間が次の時間を えて変更された場合にフラートを発売 スで変更された場合にフラートを発売 、 ポリシーの変更をすぐに送信	#Aller (A A - E PRAL)	く 4. [コ 信だ ら開 5. [f	ンピュ・ 5向]で 閉始"を 呆存]を	ータ]タブを開 "Agent/App 選択します。 :押してくださ!	lき、[通 lianceか い。	
	 祝要 スポブログラム対策 WebUビュテーション アクライビティ監視 アブリケーションフルロー 変更監視 セキュリティログ監視 ファイアウォール /a3 trian インタフェース 	進信方向 ハートビート ハービート ハービート ホンの数を超えるハードビートが快われた場合にアラートを発令、 ハービート間層 大の数を超えるハードビートが快われた場合にアラートを発令、 ハービート間でコンピュータのローカルジステム時間が次の時間を えて変更がた場合にアラートを発令、 ボリシーの変更をすぐに送信 ポ ッ シーの変更をすぐに送信 ポ	#AF (10 分) 截手 (10 小)	4. [コ 信だ ら開 5. [f	ンピュ・ 5向]で 開始"を 呆存]を	ータ]タブを開 "Agent/App 選択します。 :押してくださ!	lき、[通 lianceか い。	
	 試表 不正力グラム対策 Webレビュテーション アグライビライ監視 アブリケーションコントロー 変更監視 セキュリティログ監視 ブライアウォール (a) ream インダフェース ア 	通信方向 ハートビート ハービート ハービート ロービー・問題 次の数を超えるハードビーが少失われた場合にフラートを発売。 ハービー・問題 次の数を超えるハービー・が快われた場合にフラートを発売。 ハービー・問定コンビュータのローブルシステム時間が次の時間を えて変更わた場合にフラートを発売。 ポリシーの変更をすぐに送信 ポレッーの変更をすぐに送信 ポレッーの変更をすぐに送信 ポレッーの変更をすぐに送信 パレーブルシューティング	#A型 (A (A - F A) 二甲NA) 截承 (10 分) 截承 (10 分) 截承 (5) 截承 (前月羽) 截承 (13, -)	く 信だ。 ら開 、 、 5. [f	ンピュ 5向]で 開始"を 呆存]を	ータ]タブを開 "Agent/App 選択します。 :押してくださ!	lき、[通 lianceか い。	
	 試表 不正プログラム対策 アレブレイシュシーション アクティビティ監視 アプリアーションコントロー 変更監視 セキュリティログ監視 ファイアウォール バス 15歳 インダフェース 認定 アプティト 	 通信方向 ハートビート ハートビート ハートビート問題 次の数を超えるハートビートが失われた場合にアラートを発売 ハービート間にコンピュータのローブルシステム時間が次の時間を えて変更がた場合にアラートを発売 ポリシーの変更をすぐに送信 ポリシーの変更をすぐに送信 ドップルシューティング ログレベル: 	Water (A (A A)(2000AA) Water (A (A A)(2000AA) Water (10 分) Water (10 分) Water (10 分) Water (10 小) Water (10 小) Water (10 小)	・ 4. [コ 信だ ら開 5. [f	ンピュ・ 5向]で' 閉始''を 呆存]を	ータ]タブを開 "Agent/App 選択します。 :押してくださ!	lき、[通 lianceか い。	
	 試要 不正プログラム対策 アレブクラム対策 アクティビティ監視 アプリーションコントロー 変更監視 セキュリティログ監視 ファイアウォール (A3 5 5 6 a 6 アンダブテート アンダブテート オーパーラッド 	 通信方向 ヘートビート ハートビート ハービー・時隔 次の数を超えるハードビートが失われた場合にアラートを発売 ハービー・時間に、 次の数を超えるハードビートが失われた場合にアラートを発売 ハービー・時間に、火ビー・カジローカルシステム時間が次の時間を えて変更れた場合にアラートを発売 ボリシーの変更をすぐに送信 ポレッーの変更をすぐに送信 ドブルシューティング ログレベル・ 	Work (A (A . F A) (2 M MA) Work (A (A . F A) (2 M MA) Work (A (A A) (2 M MA) Work (A (A A) Work (A (A A)	・ 4. [コ 信だ ら開 ・ ・ ・ ・ ・	ンピュ・ 5向]で 開始"を 見た 呆存]を	ータ]タブを開 "Agent/App 選択します。 :押してください	lき、[通 lianceか い。	
	 試表 不正プログラム対策 アンボンイン・4 アグライビア・4 アグライビア・4 アグライビア・4 マグライビア・4 マグライブの当ール (A) 3 FEAR アンダブアート 202 アブデート オーバーライド 		Water (A (A . F ALCENTIAL) Water (10 分) 超歩 (5) 超歩 (5) 超歩 (5) 超歩 (10 小) 砂索 (10 小) 砂索 (10 小)	・ 4. [コ 信だ ら閉 ・ 5. [f	ンピュ [.] 5向]で 開始"を 駅存]を	ータ]タブを開 "Agent/App 選択します。 :押してくださ!	lき、[通 lianceか 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。

ダッシュボード 処理 アき	→ ^{イベントとレポート} < 1.[*]C1WSコジリールの[コンピュータ]をクリックします。	
スマートフォルダ	コンピュータ サブグループを含む マ グループ別 マ	Q このページを検索
	+ 追加 → 前 削除 国 詳細 + 処理 → 首 イベント → 탄 エクスポート → 田 列	
	名前 ▲ ブラットフォーム ポリシー ステータス	ポリシーの送信の成功 説明
	コンピュータ (2)	
	📲 Redhat Red Hat Enterprise 6 (64 bit) Linux Server 🌒 管理対象(大人二) 2	2.2 仮想パッチを使いたいコンピュ
	冒 Windows Microsoft Windows Server 2012 R2 … Windows Server 2012 ● 管理対象(オンライン)	₂:画面を開きます。
-		
概要	一般 詳細 侵入防御イベント	
▶ 不正プログラム対策	侵入防御	
9 Webレビュテーション	設定: オン ▼ 4. 侵入防御の設定を「オン」にします。	
▶ アクティビティ監視	ステータス: 🌒 オン,防御,58 ルール	
アプリケーションコントロ		
変更監視	 ● 防御 → 5.1 受入防御の割作を1防御」にしま9。 ○ 検出 	
・ セキュリティログ監視		「検出」でドライラ
🦻 ファイアウォール	コンテナのネットワークトラフィックの検索:	た上で「防御」に
) 侵入防御 🦛 3.	侵入防御メニューを開きます。	
© 2020 Trend N	icro Inc.	



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。

- 概要	一般 詳細 侵入防御イベント		
♥ 不正プログラム対策	コンテナのネットワークトラフィックの検索:	(Jt) •	
🐻 Webレビュテーション	現在割り当てられている侵入防御ルール		
アクティビティ監視			
🗵 アプリケーションコントロ-			
◎ 変更監視	割り当て/割り当て解除 🖹 プロバティ 📑 エクスボート	r © アブリケーションの種類 田. 列	
・ セキュリティログ監視		アプリケーションの種類	
■ ファイアウォール	- <mark>侵入防御メニューを開さま9。</mark>	Web Client SSL	
⊖ 侵入防御	😝 1005307 – Identified Fraudulent Digital Certificate	Web Client SSL	
■ 1/47=-7 (😝 1001933 – Identified Suspicious Usage Of Shellcode For Client	Web Client Common	
	l000834 - SMTP Decoding	Mail Server Common	
	😌 1004790 - Identified Diginotar Certificate	Web Client SSL	
♥ / ッ// - r	4	•	
X、オーバーライド	推奨設定		
	現在のステータス: 58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: 2020-07-10 15:12		
	▼ 不肺/次の推発設定には45のません	「「「「「」」「「」」「「」」」」の「「」」」」	(可能や損金)」を「けいした乳ウレキオ
	侵入防御の推奨設定を自動的に適用(可能な場合): (はい	、 2. 「 1 包入防御の推突設定で自動的に適用((「明記な場合)」を「はい」に設定します。
	推奨設定の検索 推奨設定の検索のキャン	セル 推奨設定をクリア	
		🛛 🙀 🚺 🚺 3. 保存して終了しま	す。
		i della	
1			
© 2020 Tren	d Micro Inc.		



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。









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。

י_−¢	 コンピュータ サブグルーブを含む + 追加 ▼ 面 削除 目 詳細 	グループ別 ▼ ◆ 処理 ▼ 「 ゴイベント ▼ ■ エクスポート ▼ 田 列」	
	名前 ▲	ブラットフォーム ポリシー ステータス ポリシーの送信の成功 説明	
	コンピュータ(ク)		
	E Dadhat		
	Windows	Microsoft Windows Server 2012 R2 … Windows Server 2012 ● 管理画面を開きます。	
	 提契数定 現在のステータス: 377 前回の推奨設定の検索: 201 ▲ 未解決の推奨設定: 5個 侵入防御の推奨設定を自動的に適用(可能な) 	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た 11-25 17:03 動 のレールの割り当て 品: 4. [現在割り当てられている侵入防御ルール] 自動的に洗い出されたルールが適用されて	か確認します。 で い
	 推奨設定 現在のステータス: 377(前回の推奨設定の検索: 201) ▲ 未務決の推奨設定: 5個 (尺入防御の推奨設定さ自動句に通用(可能な 推奨設定の検索 	の役入防御ルールが割当てられています 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た 4. [現在割り当てられている侵入防御ルール] 自動的に洗い出されたルールが適用されて ることを確認します。	か確認します。 で い
	#契政定 現在のステータス: 377 前回の推奨設定の検索: 201 承報決の推奨設定: 5個 使入防御の推奨設定注き自動的工造用(可能な 推奨設定の検索	の役入防御ルールが割当てられています。 3. 11-25 17:03 第のレールの割り当て 自動 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	か確認します。 で い
上で、	#実設定 377/1 現在のステータス: 377/1 前回の推躍設定の検索: 201 ▲ 未解決の推奨設定を自動的に適用(可能な 1 復入防御の推奨設定を自動的に適用(可能な 推奨設定の検索 ● #資設定の検索 ● 「ため面の「ない」 ● 大都決の推奨設定を自動的に適用(可能な ● ●	の使入防御ルールが割り当てられています 11-25 17:03 動加レールの割り当て 為合: [現在割り当てられている侵入防御ルール] 自動的に洗い出されたルールが適用されて ることを確認します。 ***********************************	か確認します。 で い

AN INVESTIGATION OF THE OWNER OF



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

~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。

DAIWABO INFORMATION SYSTEM CO., LTD. CONFIDENTIAL

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。

	コンピュータ サ	ブグループを含む 👻 グルー	-ブ別 👻				へ この	ページを検索
コンピュータ								
	+ 追加 - 面削附	1 目詳細 4 処理		エクスボート 👻 🖽 列				
	名前 ▲		ブラットフォーム	ポリシー		ステータス	ポリシーの送信の成功	説明
	▼ コンピュータ(2)							
	Redhat		Red Hat Enterprise 6 (64 bit)) Linux Server	٠	管理対象 (オンライン)	2 時間 前	
	- Windows		Microsoft Windows Server 20	012 R2 ··· Windows Server 201:	4 • 2	「不正プロク	ラバ対策を使いけ	FU
						コンピュー	タ画面を開きます	J
概要	一般 Shart Protection	詳細 いはファイル 不正:	プログラム対策イベント					
 概要 不正プログラム対策 	一般 Suart Protection 不正プログラム対策	詳細 いはファイル 不正	プログラム対策イベント					
 概要 不正プログラム対策 Webレビュアーンヨン 	一般 Si art Protection 不正プログラム対策 設定: オン	詳細 いはファイル 不正:		ふ「不正プログ	ラム対策1			
 概要 不正プログラム対策 Webレビュアーンヨン アクティー 監視 	 一般 Shart Protection 不正ブログラム対策 設定: オン ステータス: ● オン,リアルター 		^{カクラム対策イベット} 4.[一般]タブか D設定を[オン]に	ら、[不正プログ: :します。	ラム対策]			
 概要 不正プログラム対策 Webレビュテーンヨン アクティー 監視 アブリン コントロー 	 一般 S art Protection 不正プログラム対策 設定 オン ステータス・● オン,リアルター リアルタイム検索 		^{カクラム対策イベント} 4.[一般]タブか D設定を[オン]に	ら、[不正プログ: :します。	ラム対策]			
概要 小正プログラム対策 Webレビュテーンヨン アクテノへ監視 アブリンションコントロー 変更監	 一般 Si art Protection 不正プログラム対策 認定 オン ステータス: ● オン,リアルター リアルタイム検索 □ 継承 		^{カクラム対策イベント} 4.[一般]タブか D設定を[オン]に	^ら、[不正プログ: :します。	ラム対策]			
概要 不正プログラム対策 Webしとュテーンヨン アクテノへ監視 アブリンションコントロー 変更監 セキュリティログ監視	 一般 Si art Protection 不正プログラム対策 認定: オン ステーダス: オン,リアルター リアルタイム検索 二 継承 不正プログラム検索設定 	詳細 いロゴファイル 不正 (ム Default Real-Time Scan Conf	プログラム対策イベント 4. [一般]タブが D設定を[オン]に iguration	ら、[不正プログ: します。 ■#	ラム対策]			
 概要 不正プログラム対策 Webしビュテーンヨン アクラン (監視) アブリン ションコントロー 変更監 セキュリティログ監視 アプログラム対象 	 一般 Si art Protection 不正ブログラム対策 設定: オン ステーダス: オン,リアルター リアルタイム検索 二 総承 不正フログラム検索設定 (6) (7) (7)	詳細 Add ファイル 不正 人 し と ロット ファイル 不正 2 2 2 2 2 2 2 2 2 2 2 2 2	プログラム対策イベント 4. [一般]タブか D設定を[オン]に figuration 、 、	ら、[不正プログ: します。 ^{編集} ^{編集}	ラム対策]			
概要 不正プログラム対策 アクライン アクライン 全国 アブリン ションコントロー 変更監 セキュリティログ監視 モプ、ログ、ラム対象 日の、日本の ● 侵入防御	 一般 Si art Protection 不正ブログラム対策 設定: オン ステータス: ● オン,リアルター リアルタイム検索 二 継承 不正プログラム検索設定 (5) を開きます。 手動検索 	詳細 いはファイル 不正 した し し Every Day All Day	ブログラム対策イベント 4. [一般]タブか D設定を[オン]に figuration	ら、[不正プログ: します。 ^{編集} ^{編集}	ラム対策]			
概要 不正プログラム対策 アレクラム対策 アクティーション アクティーを読視 アブリン コントロー 変更監 セキュリティログ監視 ビプログラム対撃 人防御 インタフェース	 一般 Si art Protection 不正プログラム対策 設定: オン ステータス: ● オン,リアルター リアルタイム検索 一 継承 不正プログラム検索設定: (長) を開きます。 手動検索 一 継承 	詳細 いはファイル 不正 した 日本 日本 日本 日本 日本 日本 日本 日本 日本 日本	ブログラム対策イベント 4. [一般]タブか D設定を[オン]に Figuration ・ ・	ら、[不正プログ: :します。 ^{選集} ^{選集}	ラム対策]			
 概要 不正プログラム対策 アプログラム対策 アグリションコントロー 変更話 セキュリティログ監視 ビキュリティログ監視 レク、コンコントロー (人) (人) (人) (人) (人) (人) (人) (人) (人) (人)	 一般 Si art Protection 不正プログラム対策 設定 オン ステータス: ● オン,リアルター リアルタイム検索 ● 継承 不正プログラム検索設定 (基家 手動検索 ● 継承 不正プログラム検索設定 	詳細 ・11ファイル 不正 くム 2 Default Real-Time Scan Conf Every Day All Day Default Manual Scan Configur	プログラム対策イベント 4. [一般]タブか D設定を[オン]に figuration ・ ・	26、[不正プログ: します。 ^{画来} ^{画来}	ラム対策]			
 概要 不正プログラム対策 アモプログラム対策 アクラン 監視 アブリン コンコントロー 変更監 セキュリティログ監視 ビクログラム対号 侵入防御 インタフェース 設定 アップデート 	 一般 S art Protection 不正プログラム対策 設定 オン ステータス: オン,リアルタイム検索 一 総承 不正プログラム検索設定 (5) (5) (7) (7)<!--</td--><td>詳細 ロジフィイル 不正 (ム 2 (ム 2) Default Real-Time Scan Configur Default Manual Scan Configur</td><td>プログラム対策イベント 4. [一般]タブか D設定を[オン]に figuration ・ ・</td><td>26、[不正プログ: します。 ^{選集} ^{選集}</td><td>ラム対策]</td><td></td><td></td><td></td>	詳細 ロジフィイル 不正 (ム 2 (ム 2) Default Real-Time Scan Configur Default Manual Scan Configur	プログラム対策イベント 4. [一般]タブか D設定を[オン]に figuration ・ ・	26、[不正プログ: します。 ^{選集} ^{選集}	ラム対策]			

つぶ 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。

	アラート イベントとレポー	ト コンピュータ ポリ	< <u>1</u> ₽ C1WS	<u>コンソールの</u>	0[コンピュ-	-タ]をクリックし	ます。	
🛃 スマートフォルタ	コンピュータ +	ナブグループを含む 💌 グル	ーブ別 🔻				Q	このページを検索
冒 コンピュータ								
	+ 追加 - 🔟 削	除 🗉 詳細 🕈 処理		➡ エクスポート 👻	田, 列			
	名前 ▲		ブラットフォーム	ボリシー		ステータス	ボリシーの送信の成功	功 説明
	▼ コンピュータ(2)							
	Redhat		Red Hat Enterprise 6 (64 I	bit) Linux Sei	ver	● 管理対象 (オンライン)	2 時間 前	
	Windows		Microsoft Windows Server	2012 R2 ··· Windows	Server 2012) 2.8個別設定を	使いたいコン	ピュータ
						画面を開き	ます。	
■ 概要 →	一般 Smart Protection	n 詳細 検出ファイル	不正プログラム対策イベント					
😵 不正プログラム対策	不正プログラム対策						一般 検索除外	処理 オプション 割り当て対象
	設定: オン	•					一般情報 名前: Defau	ult Manual Scan Configuration
↑止ノリクフム刈束	┛ ステータス: ● オン,リア.	ルタイム					1 月1	
		承]のチェックを ダ	います.				10.00 m 55 M 5	7 0h tá ata
◎ 変重監想		N1000 T 0 0 GM						TRANKAS
	不正プログラム検索設定:	Default Real-Time Sca	n Configuration	▼ 編集	6 設定ī	両両が閉きますの 。	秋索対象ディレクトリ: 6	* すべてのディレクトリ
	スケジュール:	Every Day All D		▼ 編集	必要に広	「て冬蒲設定を行う		○ ティレクトリリスト: ディレクトリリストの選択
					の受に応じてください		検索するファイル: ()	1 すべてのつァイル
	手動検索	5. [Default F	Real-Time Sca	in			6	■ トレンドマイクロの推奨設定で検索されるファイルタイプ
	□ 継承	Configuration	1]を選択し、[編	r			c	ファイル拡張子リスト: ファイル拡張子リストの選択
- 1237 <u>1</u> -X			and a set of the set o	▼ 編集				
■ 「レメノエース (◆ 設定	不正プログラム検索設定:	[集]をクリックし	ノまり 。			個別設定を行わたい	い提合け 木べ	
 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	不正プログラム検索設定: 予約検索	集]をクリックし	ジます。			個別設定を行わない	い場合は、本ペ ふくて結構です	ОК ++>тели
 ■ 12371-X ● 設定 ● アップデート X: オーバーライド 	 不正ブログラム検索設定: 予約検索 ※承 	集」をクリックし	ッま 9 。			個別設定を行わないジの設定は実施した	い場合は、本ペ ふくて結構です	ок +«У±и



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。

ダッシュボード 処理 アラート イヘ	ミントとレポート コンピュータ ポリシー	管理	
✿ システム設定 予約タン	スク	(=1. C1WS	コンソールの[管理]をクリックします。
☑ 予約タスク < 2. [予約タ	7スク]を開きます。		
▶ イベントベースタスク	🔟 削除 🔲 ブロバティ 🕕 複製	▶ 今すぐタスクを実行	
✓ ● ユーザ管理 名前 ▲	3. [新規]をクリックします。	スケジュール	
👪 ユーザ	小アップデートタスク セキュリティアップデー…	毎日09:20 (UTC+9.00)	
▓ 役割			
https://spp.deepsecurity.trendmicro.com/ - 転換予約タスクウゼード - Internet Exp この予約タスタの増速と模型を入力してください。 確認: コンピュータの不正プログラムを検索 ※ 即用化 <p< th=""><th>・・・・・・ ・・・・・ ・・・・・ ・・・・・ ・・・・・・</th><th>仮想パッチと同様に設 しで、インストール 対策・仮想パッチ</th><th>^{産し、 完了して下さい。} いおよび不正プログラ 「の初期段階設定は終</th></p<>	・・・・・・ ・・・・・ ・・・・・ ・・・・・ ・・・・・・	仮想パッチと同様に設 しで、インストール 対策・仮想パッチ	^{産し、 完了して下さい。} いおよび不正プログラ 「の初期段階設定は終
	(詳紙	こ す。 GJが又れてる	ヽ ヽ し / こ ₀ コンソールのヘルプにあるマニュアルを
		照ください。)	





DAIWABO INFORMATION SYSTEM CO., LTD. CONFIDENTIAL



C1WS:ヘルプメニュー

) ヘルブ 🔇 サポート情報 👻
サポート情報
インストールスクリプト
Agentのダウンロード
使用許諾契約書
コメントおよびフィードバック
バージョン情報

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で	
コメントおよびフィードバック	も対応はできかねますのであらかじめご了承ください)	
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: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

	Sign In	Don't have an account?	Password Reset	
Account Username Password Forgot your password?		Sign up for a free Trend Micro Cloud One account. You can use your existing Deep Security as a Service account to sign in to Trend Micro Cloud One.	Enter your account details and click OK. An email providing instructions for resetting your password will be sent to the email address associated with your account.	
	Remember Account Name and Username Use Multi-Factor Authentication [®] Sign In Privacy Statement	Create an Account	私はロボットではあり この こ	





7.よくあるご質問と回答集(FAQ)

DAIWABO INFORMATION SYSTEM CO., LTD. CONFIDENTIAL

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: <u>https://success.trendmicro.com/jp/solution/1310095</u>)
C1WSのアカウントがロックされてしまった場合、バ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、ユーザブロファイル> 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。



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C1WSD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	C 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/





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「イベントとレボート」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レビュテーション)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



