



Trend Vision One Zero Trust Secure Access

InterScan Web Securityからの 移行ガイド

トレンドマイクロ株式会社

2024/05/28

Rev3.0

更新情報

版数	更新日	内容
第1.0版	2023/11/10	第1.0版として公開
第1.1版	2024/02/14	資料名の修正 P.3：URL修正 P44：独自ユーザー管理の機能追加
第2.0版	2024/04/23	資料名の修正 全般：InterScan Web Security Suite（IWSS）への対応を追記
第3.0版	2024/05/23	資料名の修正 全般：オンプレミスゲートウェイに関する記載を追記

はじめに

本資料で用いられる略称

用語や略称	正式名称、または用語の意味
Vision One	Trend Vision One
ZTSA	Trend Vision One Zero - Trust Secure Access
ZTSA-IA	Trend Vision One Zero - Trust Secure Access – Internet Access
IWSVA	InterScan Web Security Virtual Appliance
IWSS	InterScan Web Security Suite
オンプレミスゲートウェイ	ZTSA-IA オンプレミスゲートウェイ

ご注意ください：製品使用許諾について

Trend Vision One Zero Trust Secure Access – Internet Access(ZTSA-IA)に移行いただきご利用いただく際には、

「トレンドマイクロ クラウドサービス 利用規約」

が、適用されます。

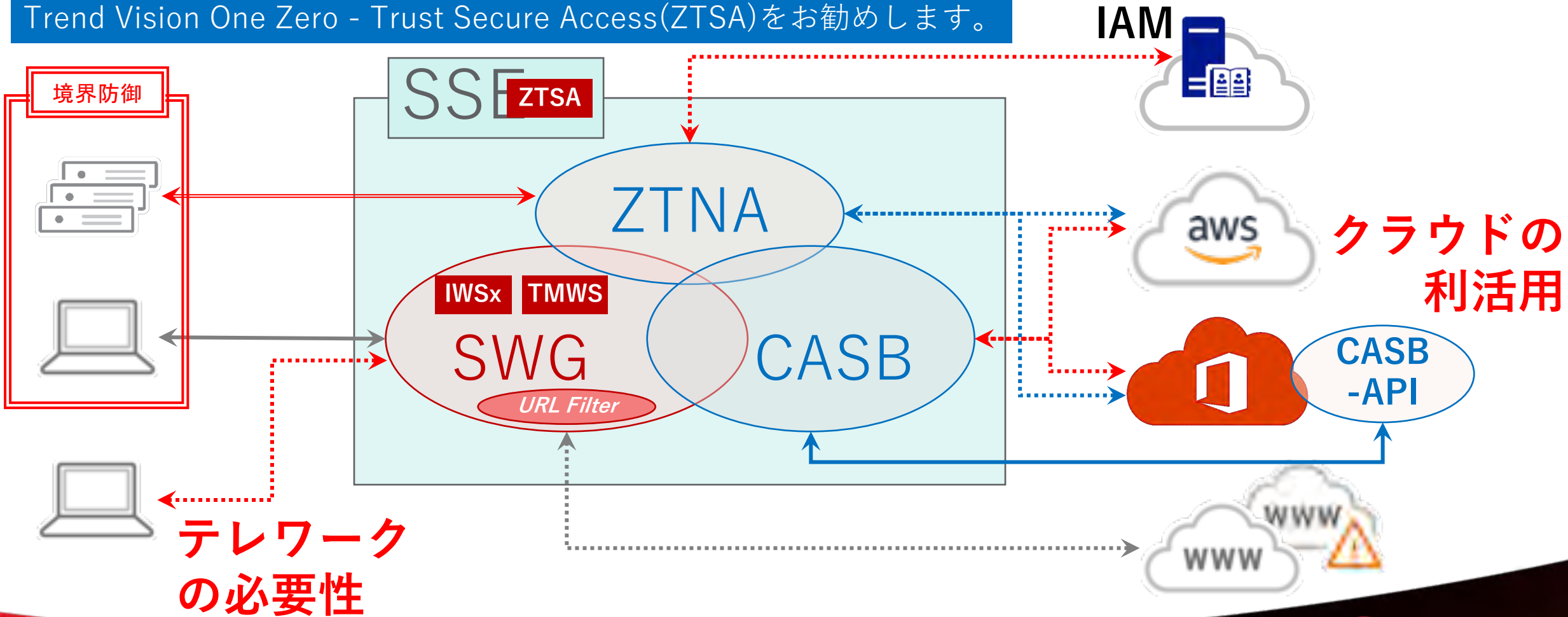
詳細につきましては、下記よりご確認ください：

https://www.trendmicro.com/ja_jp/about/legal/eula.html

InterScanからZTSAへ移行をお勧めする理由

お客様を取り巻くIT環境、脅威の状況の変化により、これまでのSWG(Secure Web Gateway)に加えて、ZTNA(Zero Trust Network Access)を含むSSE(Secure Service Edge)の必要性が高まっています。

Trend Vision One Zero - Trust Secure Access(ZTSA)をお勧めします。

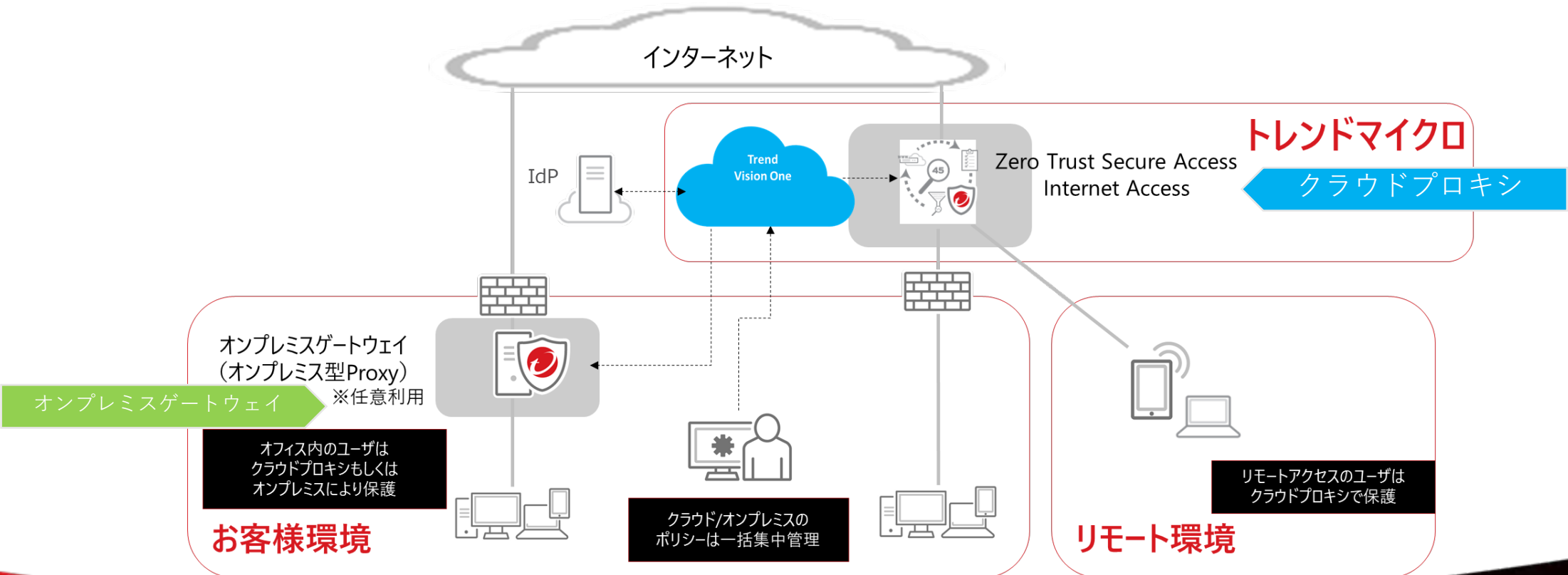


クラウドプロキシとオンプレミスゲートウェイ

Trend Vision One – Zero Trust Secure Accessのご利用構成のご紹介

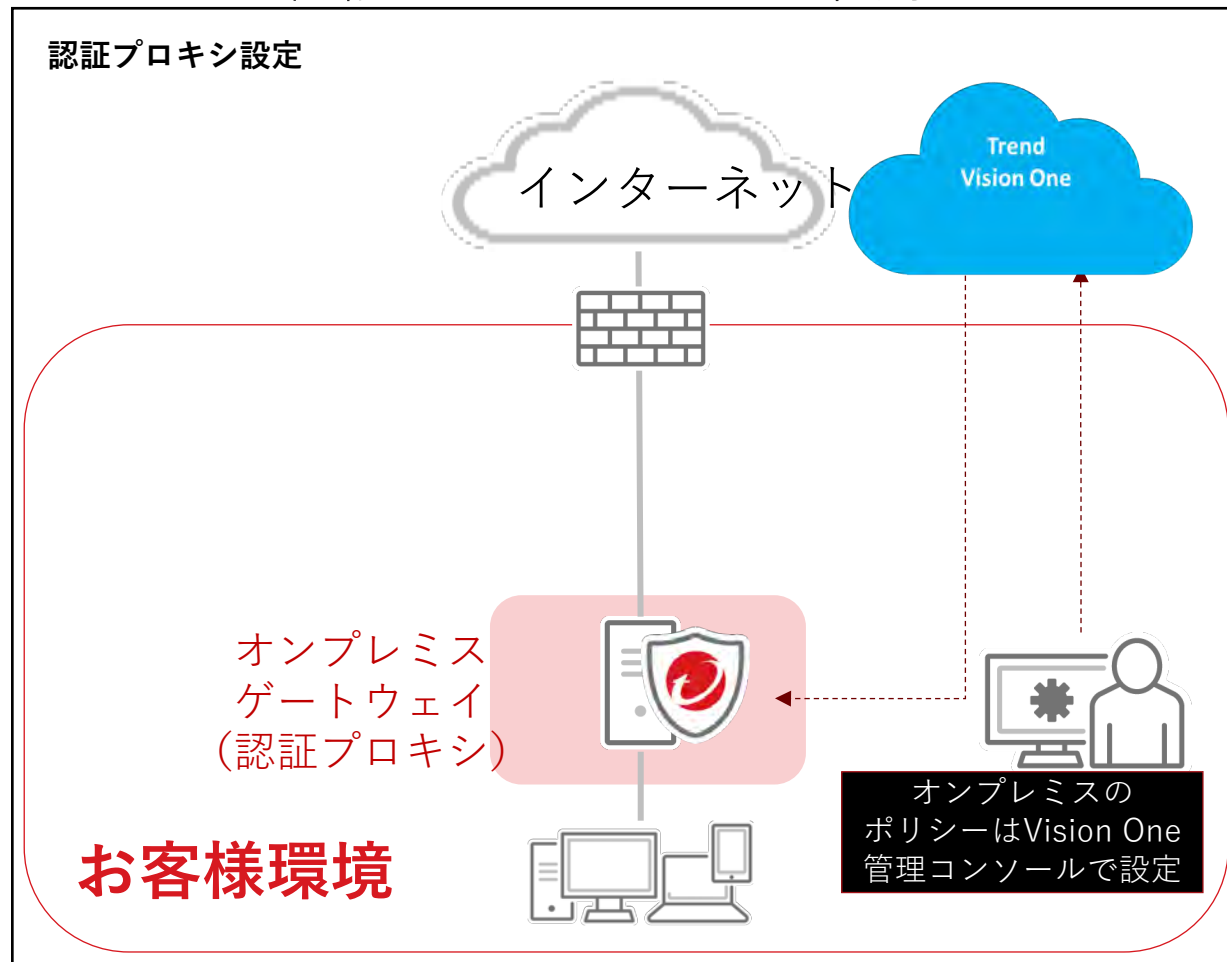
ZTSA-IA概要

ZTSA-IAではクラウドプロキシと仮想アプライアンスのオンプレミスゲートウェイをご利用いただけます。オンプレミスゲートウェイの構成、設定は本資料の右上のマークのページをご参照ください。



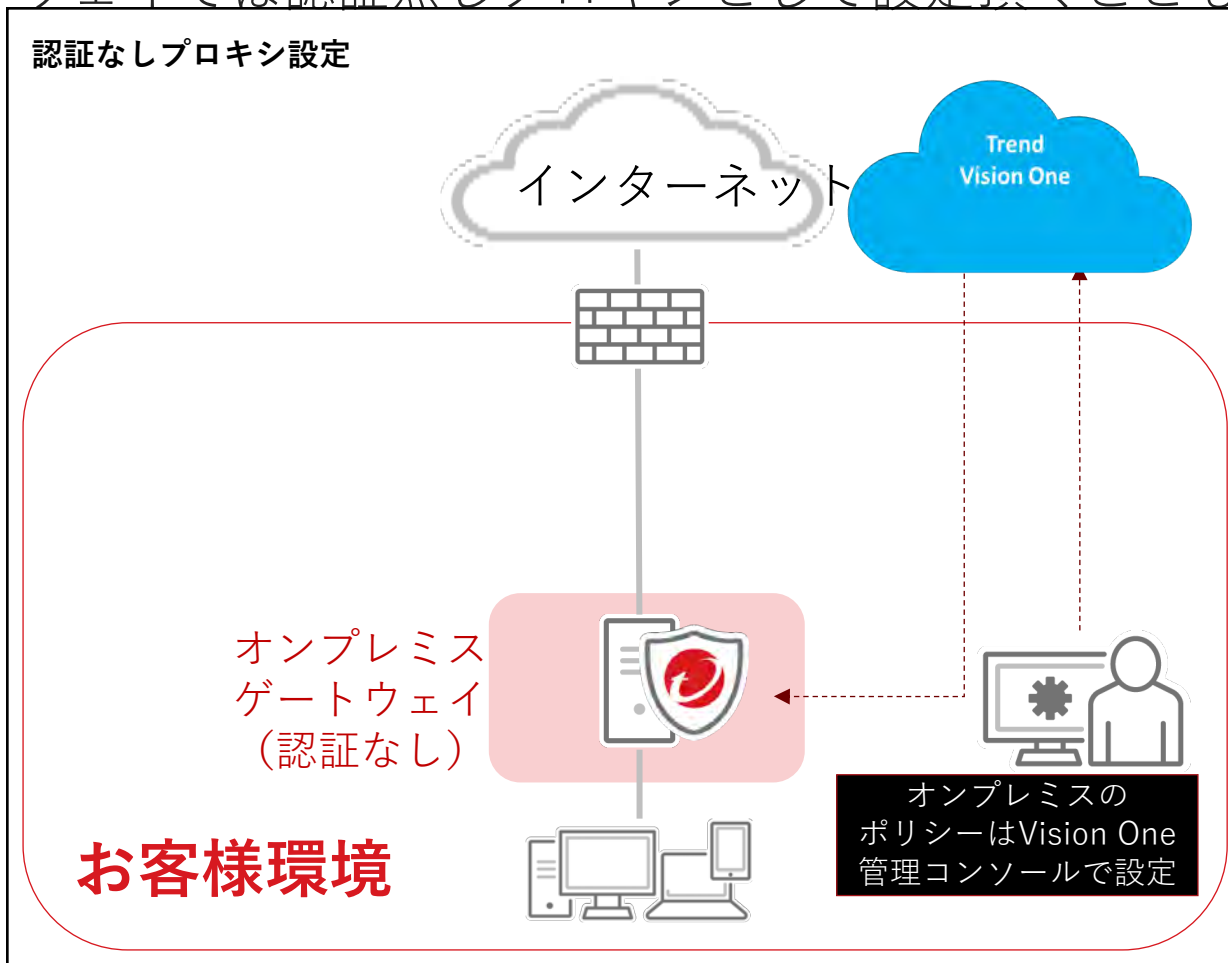
オンプレミスゲートウェイ：認証プロキシ

オンプレミスゲートウェイでは認証プロキシとしてご利用いただけます。



オンプレミスゲートウェイ：認証無しプロキシ機能

オンプレミスゲートウェイでは認証無しプロキシとして設定頂くことも可能です。



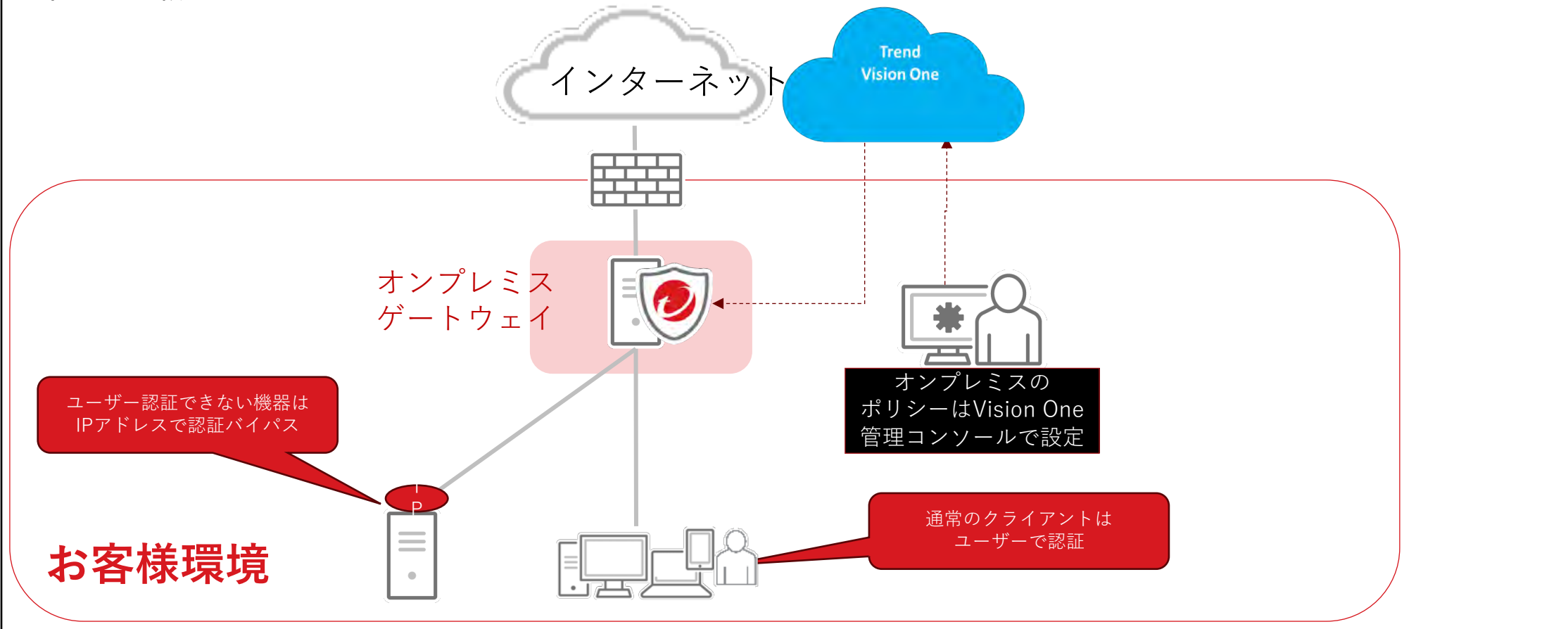
注意：

認証無しでご利用頂く場合は、オンプレミスゲートウェイのvCPU数に応じたライセンス数が必要となります。

オンプレミスゲートウェイ：認証バイパス設定

ユーザー認証が利用できない特定の機器向けに認証バイパスを行う設定も可能です。

上位プロキシ設定

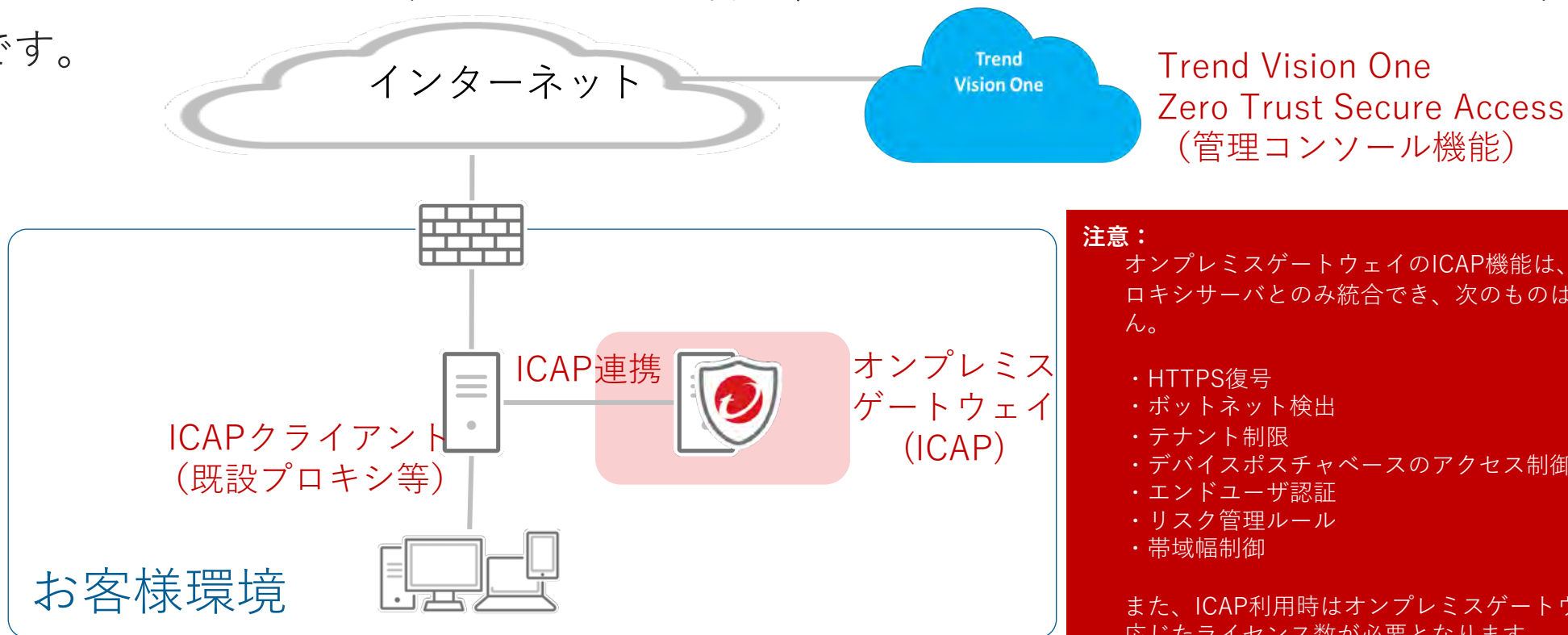


注意：

認証バイパスは1プライベートIPアドレスあたり1ユーザーとして計算されます。

オンプレミスゲートウェイ：ICAP設定

ネットワーク上にすでにICAPクライアントがあり、スキャンのためにWebトラフィックをオンプレミスゲートウェイに転送させたい場合は、オンプレミスゲートウェイでICAPが利用可能です。



移行概要

移行概要

- IWSVA/IWSSをご利用中の環境向けにZTSA - Internet Accessへの移行ツールの提供しております。
- 本ガイドでは移行に関して、事前に検討頂く事項や移行の手順などを記載しております。

InterScan
Web Security
(IWSVA/IWSS)



移行
ツール

Trend Vision One
Zero Trust Secure Access
- Internet Access
(ZTSA-IA)



注：

IWSVA/IWSSをTRSL(Trend Micro Reliable Security License)でご利用いただいているお客様向けの機能となります。それ以外のライセンスでご購入されているお客様につきましては、恐れ入りますがご利用いただくことはできません。

2024年4月よりIWSSからの移行も対象となりました。

IWSVA/IWSSからZTSAへの移行ステップ

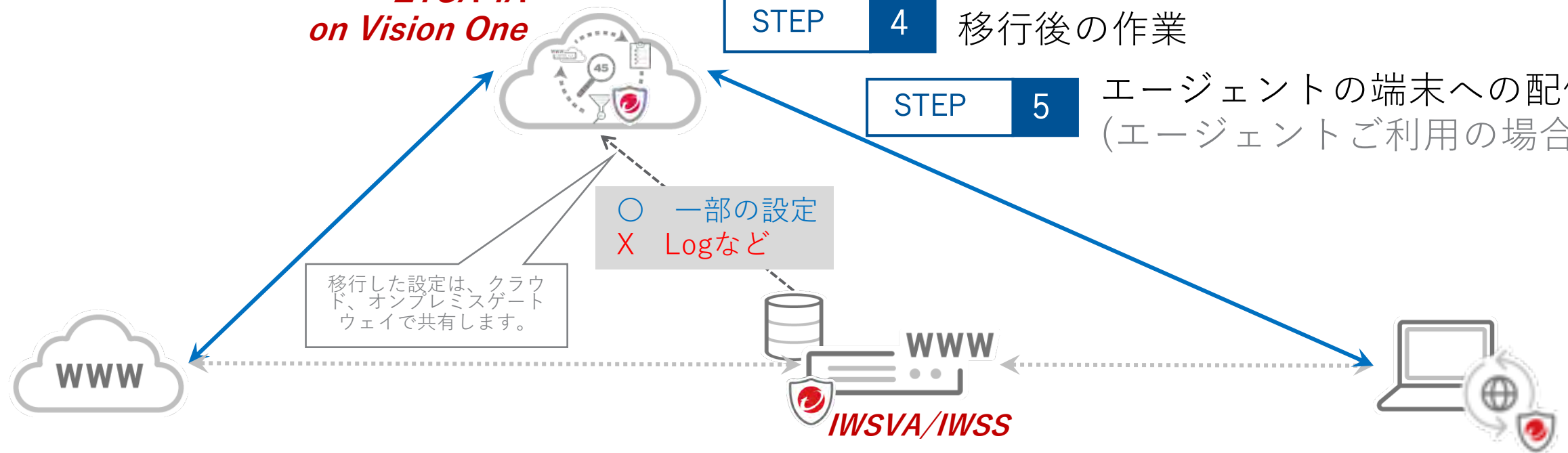
STEP 1 前提条件、移行情報の確認

STEP 2 ZTSAを開始し、IWSVA/IWSSのアクティベーションコードをZTSAに投入

**ZTSA-IA
on Vision One**

STEP 4 移行後の作業

STEP 5 エージェントの端末への配信
(エージェントご利用の場合)



STEP 3 IWSVA/IWSSバックアップファイルの取得
移行ツールを開始・アップロード

目次：移行作業 ～移行の全体ステップ～

STEP 1

前提条件、移行情報の確認

前提条件、移行可能な情報・対象外となる情報の確認

STEP 2

移行前作業の実施

ZTSA-IAの移行前準備の実施

STEP 3

移行の準備と実施

IWSVA/IWSSでのバックアップ取得、移行ツールの実行

STEP 4

移行後作業の実施

設定情報の確認、移行対象外項目の設定

STEP 5

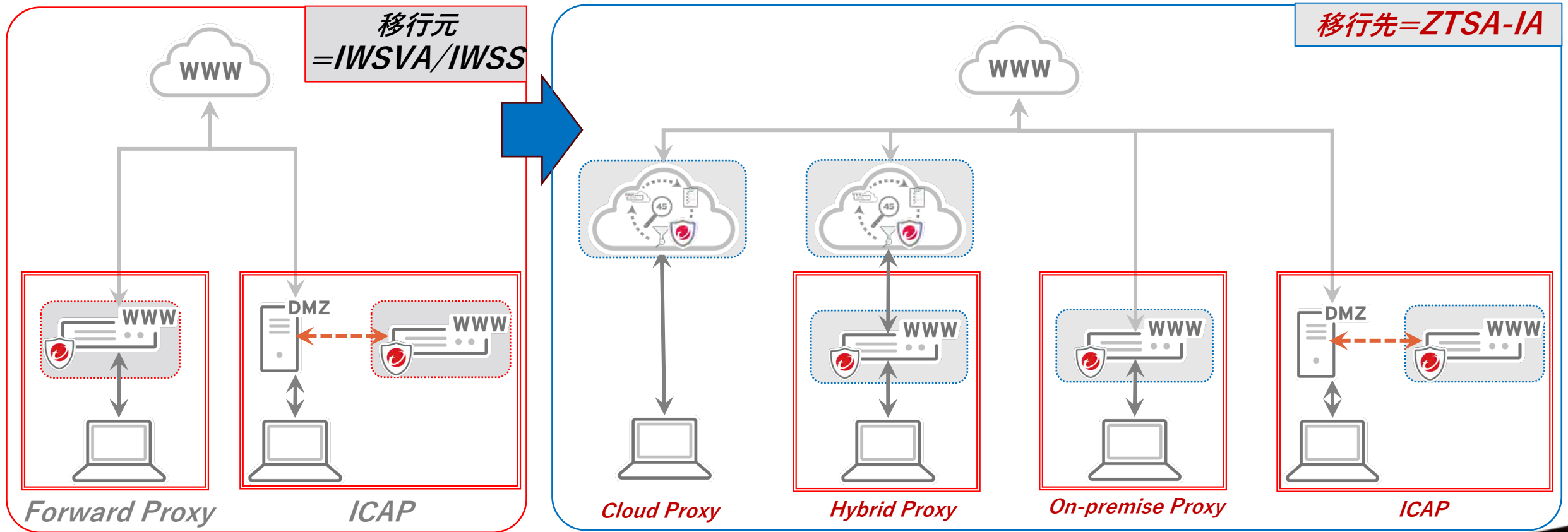
動作確認

クライアントへのエージェント配布、Pac設定・証明書配布などを実施頂き、ZTSA-IA経由でのWebアクセスの動作確認を実施

STEP1: 前提条件、移行情報の確認

<はじめに> IWSVA/IWSSからの移行のご注意点

- 移行元製品 : 「IWSVA 6.5 Service Pack 2 及び Pack 3」 「IWSS 6.5 ※Patch4のみ動作確認済み」
- 移行先トポロジ : 「フォワード・プロキシ」 及び 「ICAP」 のみ



STEP1: 前提条件、移行情報の確認（対象Ver）

IWSSから移行ツールを用いて設定情報を移行するには、以下の**対象製品バージョン**である必要があります。

- IWSVA 6.5 Service Pack 2
- IWSVA 6.5 Service Pack 3
- IWSS 6.5

※製品バージョンはIWSVA/IWSS管理コンソールの
「管理」 > 「システムアップデート」からご確認いただけます。

The screenshot displays the 'システムアップデート' (System Update) page in the Trend Micro management console. The page title is 'TREND MICRO InterScan® Web Security Virtual Appliance'. The left sidebar contains navigation options such as 'システムステータス', 'ダッシュボード', 'アプリケーション制御', 'HTTP', 'FTP', 'ログ', 'レポート', 'アップデート', '通知', '管理', '監査ログ', '配置ウィザード', '一般設定', 'ネットワーク設定', '管理コンソール', '設定のバックアップ/復元', 'システムアップデート', 'システムのメンテナンス', 'システムイベントログ', '製品ライセンス', and 'サポート情報'. The main content area shows 'インストールするパッチの選択' (Select patches to install) with a file selection button. Below this is a table titled '現在のIWSVA情報' (Current IWSVA Information) with the following data:

ホスト名	OSのバージョン	アプリケーションのバージョン	前回のアップデート
localhost.localdomain	3.10.0-1127.el7.x86_64	6.5-SP3_Build_Linux_3279	2021/10/20 10:02:48

The 'アプリケーションのバージョン' column is highlighted with a red box. Below the table, there are tabs for 'アプリケーションのパッチ' (Application Patches) and 'OSのパッチ' (OS Patches), and a section for 'パッチのメンバー' (Patch Members) with an 'インストール' (Install) button.

STEP1: 前提条件、移行情報の確認 (配置モード)

- ZTSA-IAで利用可能な機能は、フォワードプロキシとICAP (要オンプレミスゲートウェイ) になります。
- IWSVA/IWSSで他の機能をご利用頂いている場合、プロキシの配置モードの設計から見直して頂く必要がございます。
- また、ZTSA-IAで対応しているプロトコルはHTTP/HTTPSのみとなります。

IWSVA/IWSSの配置モード	ZTSA-IAでの利用可否
プロキシ転送モード	○
ICAPモード	○
透過ブリッジモード	×
リバースプロキシモード	×
通常の透過モード	×
Web Cache Coordination Protocol (WCCP) モード	×

STEP1: 前提条件、移行情報の確認(手順・移行可否)

IWSVA/IWSS移行手順および移行可能な設定・移行できない設定については、下記にて詳細を公開しております。

項目	詳細	URL
IWSVA/IWSSからの移行	移行手順詳細	https://success.trendmicro.com/dcx/s/solution/000295252?language=ja
	設定移行詳細	https://success.trendmicro.com/dcx/s/solution/000295251?language=ja

STEP1: 前提条件、移行情報の確認（注意事項1）

IWSVA/IWSSの各設定項目については、移行にあたって事前に注意が必要な項目がございます。

IWSVA/IWSSの機能	ZTSA-IAでの注意事項
<ul style="list-style-type: none"> ・ [アプリケーション制御] > [ポリシー] 	<p>IWSVA/IWSSのアプリケーション制御ポリシーで選択したアプリケーションカテゴリのうち、“詳細な検索処理”条件のカテゴリのみが移行対象となります。</p> <p>”詳細な検索処理”条件ではないカテゴリ条件をご利用の場合は、カスタムクラウドアプリカテゴリを作成してご利用ください。</p>
<ul style="list-style-type: none"> ・ [アプリケーション制御] > [ポリシー] ・ [HTTP] > [高度な脅威保護] > [ポリシー] ・ [HTTP] > [URLフィルタ] 	<p>IWSVA/IWSSのポリシー条件としてクライアントIPアドレス条件を使用していた場合、プライベートIPアドレスの条件のみが移行されます。</p> <p>ただし、クラウドゲートウェイをご利用される場合は、クライアントのIPアドレスを識別するためにSecure Access Moduleをご利用頂くか、クラウドゲートウェイの到達前の機器でX-Forwarded-Forヘッダを付加して頂く必要がございます。</p>
<ul style="list-style-type: none"> ・ [アプリケーション制御] > [ポリシー] ・ [HTTP] > [高度な脅威保護] > [ポリシー] ・ [HTTP] > [URLフィルタ] 	<p>IWSVA/IWSSのポリシー条件としてLDAPユーザ/グループ条件を使用している場合、事前にZTSA側で参照先LDAPサーバのユーザ/グループ情報の同期が必要です。</p> <p>ZTSAでは、IWSVAでサポートするLDAPサービスのうち、“Active Directory”と“OpenLDAP”をサポートいたします。</p>
<ul style="list-style-type: none"> ・ [アプリケーション制御] > [ポリシー] ・ [HTTP] > [高度な脅威保護] > [ポリシー] ・ [HTTP] > [URLフィルタ] 	<p>IWSVA/IWSSの左記3つのポリシーは、すべてZTSAのインターネットアクセス制御ルールへ移行されます。ただし、ZTSAのインターネットアクセス制御ルールの上限数は100となります。</p> <p>上限数を超えるルールを移行しようとする場合、移行処理が行われず失敗となります。</p>
<ul style="list-style-type: none"> ・ [HTTP] > [HTTPS復号化] > [設定] 	<p>ZTSA「インターネットアクセス制御」で使用するHTTPSインスペクション用CA証明書を、クライアント端末にインストールいただく必要があります。</p>

STEP1: 前提条件、移行情報の確認（注意事項2）

IWSVA/IWSSの各設定項目については、移行にあたって事前に注意が必要な項目がございます。

IWSVA/IWSSの機能	ZTSA-IAでの注意事項
・ [FTP]	ZTSAでは、現在FTP検索機能を提供していません。
・ [ログ]	IWSVA/IWSSでのSyslog転送設定は、ZTSAへ移行されません。 クラウドゲートウェイをご利用の場合は、APIでのログ取得が可能です。 オンプレミスゲートウェイをご利用の場合は、オンプレミスゲートウェイから直接Syslog転送を行うことが可能です。
・ [管理] > [配置ウィザード]	ZTSA-IAで利用可能な機能以外の配置モードをご利用中の場合は構成の見直しが必要になります。
・ [管理] > [一般設定] > [ユーザの識別]	LDAPサービス連携設定は移行されません。 ZTSAで利用可能な認証基盤は”Active Directory + ADFS”、”OpenLDAP”、”Azure AD”、”Okta”となります。
・ [管理] > [一般設定] > [PACファイル]	PACファイルは移行されません。 ZTSAの管理コンソールからPACファイルを設定して頂く必要がございます。

STEP1: 前提条件、移行情報の確認(ZTSA要件)

ZTSAをご利用頂くために必要な前提条件は以下になります。

要件	オンラインヘルプ
システム要件	https://docs.trendmicro.com/ja-jp/documentation/article/trend-vision-one-ztsasysrequirements
通信要件	https://docs.trendmicro.com/ja-jp/documentation/article/trend-vision-one-ports-and-urls-used-002

STEP1: 前提条件、移行情報の確認(オンプレミスゲートウェイ要件)

要件	オンラインヘルプ
システム要件	https://docs.trendmicro.com/ja-jp/documentation/article/trend-vision-one-service-gateway-2-sy
サイジング情報	https://docs.trendmicro.com/ja-jp/documentation/article/trend-vision-one-onpremgateway-system
通信要件	https://docs.trendmicro.com/ja-jp/documentation/article/trend-vision-one-ports-and-urls-used-

STEP1: 前提条件、移行情報の確認 (PAC利用)

- Zero Trust Secure Accessをご利用頂くクライアント端末に以下の違いがございます。
「①エージェントを導入頂く場合」と「②エージェント無しでご利用頂く場合」
- エージェント無しの場合は制約がございますので、エージェントのご利用を推奨します。
ただし、オンプレミスゲートウェイで認証プロキシ以外をご利用頂く場合は②エージェント無しでご利用ください。

	①エージェント有り	②エージェント無し
Internet Access	<ul style="list-style-type: none"> • エージェントで認証して利用 ※PACファイル設定、証明書インストールはエージェントインストールに包括 • デバイス構成プロファイルが利用可能 	<ul style="list-style-type: none"> • PACファイルをブラウザに設定して利用 • HTTPSインスペクションを使う場合は証明書のインストール必要 • 認証はブラウザに表示されるポータルで実施 • クラウドゲートウェイを設定しない場合、全ての通信がHTTPSインスペクションの対象となる
Private Access (補足)	<ul style="list-style-type: none"> • エージェントで認証して利用 • 対応プロトコルはTCP/UDP • デバイス構成プロファイルが利用可能 	<ul style="list-style-type: none"> • ブラウザからユーザーポータル経由で利用 • 対応プロトコルはHTTP/HTTPS/RDP(web-based)/SSH(web-based)に限定される

STEP2: 移行前作業

STEP2: 移行前作業 (ZTSAアクセス)

2-1. Vision Oneコンソールへアクセスし、「**今すぐセットアップ**」をクリックします。

Vision One コンソールURL
<https://signin.v1.trendmicro.com>

Trend Vision One™

Trend Vision One 統合サイバーセキュリティ

プロアクティブなサイバーリスク管理

リスクを積極的かつ正確に管理および診断します。既知の資産、未知の資産、内部ネットワーク・インターネット接続されている資産など、継続的なアタックサーフェス (攻撃対象領域) の検出や資産リスク診断、自動化されたリスク軽減により、死角の排除、リスクへの露出の削減を実現します。

業界をリードする保護、検出、および対応

セキュリティ対策オペレーションを簡素化します。業界をリードするXDRソリューションとエンドポイントの保護、検出、および対応を統合します。Trend Vision Oneは、エンドポイント、ID、メール、ネットワーク、およびクラウドワークロードにネイティブなセンサを提供し、サードパーティとの広範な統合をサポートします。

統合された自動化

攻撃者の動きを遅くします。リスク軽減、脅威への対応、ゼロトラストアクセス制御を1つのコンソールから一元管理および自動化して、ステルス攻撃を防御および阻止します。

サインイン

メールアドレス/アカウント名

保存する

続行

サインインに関するヘルプが必要な場合

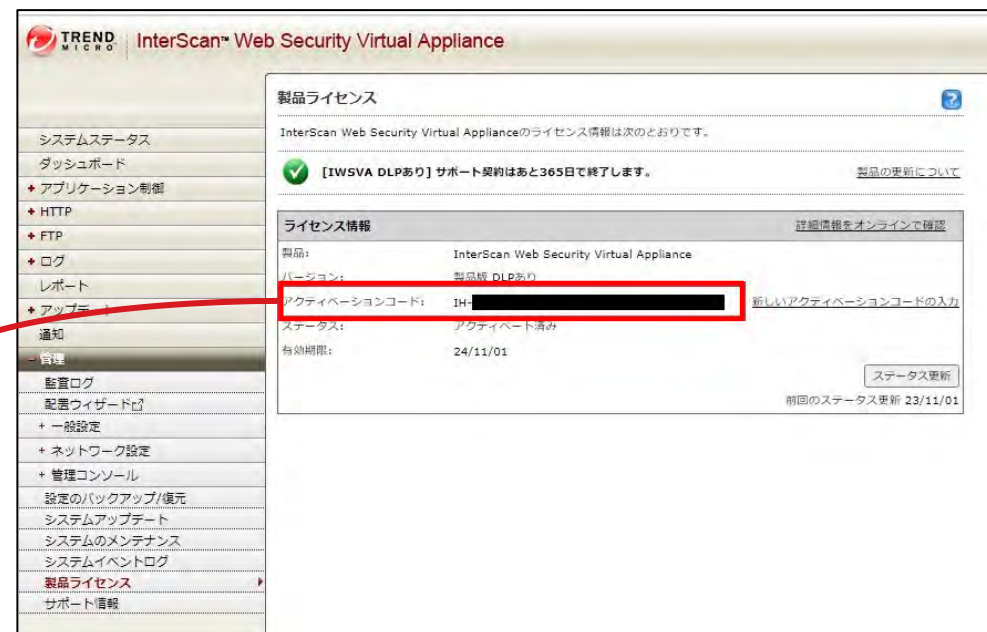
Trend Vision Oneをまだご利用でない、既存のトレンドマイクロ製品のお客さまですか? **今すぐセットアップ**

STEP2: 移行前作業 (IWSVA/IWSS ACのZTSAへの紐付け)

2-2. 現在使用中のIWSVA/IWSSのアクティベーションコードを入力します。



※アクティベーションコードはIWSVA管理コンソールの「管理」>「製品ライセンス」からご確認いただけます。



STEP2: 移行前作業 (許諾→サインイン→DC選択)

2-3. 使用許諾をご確認頂き、問題なければ☑️を入れ続行をクリックします。

登録済みビジネスのプライマリユーザアカウントにサインインする

プライマリユーザアカウントを使用して購入したすべてのトレンドマイクロソリューションを統合的に表示 ①

該当する使用許諾契約書 (グローバル|日本)、プライバシーポリシー (Global Privacy Notice) (グローバル|日本) およびデータ収集について (Data Collection Notice)を読み、内容に同意します。

続行

2-4. Customer Licensing Portalのアカウントをお持ちの場合は、そのCLPアカウントでサインインをしてください。

* アカウントをお持ちでない場合は、下部の「ビジネスをトレンドマイクロに登録」からアカウントを作成してください。

登録済みビジネスのプライマリユーザアカウントにサインインする

プライマリユーザアカウントを使用して購入したすべてのトレンドマイクロソリューションを統合的に表示①します。

メールアドレス/ユーザアカウント

続行

パスワードをリセット

ビジネスをトレンドマイクロに登録

2-5. Data Center Regionの選択で「Japan」を選択し、「Provision Console」をクリックします。

Data Center Region

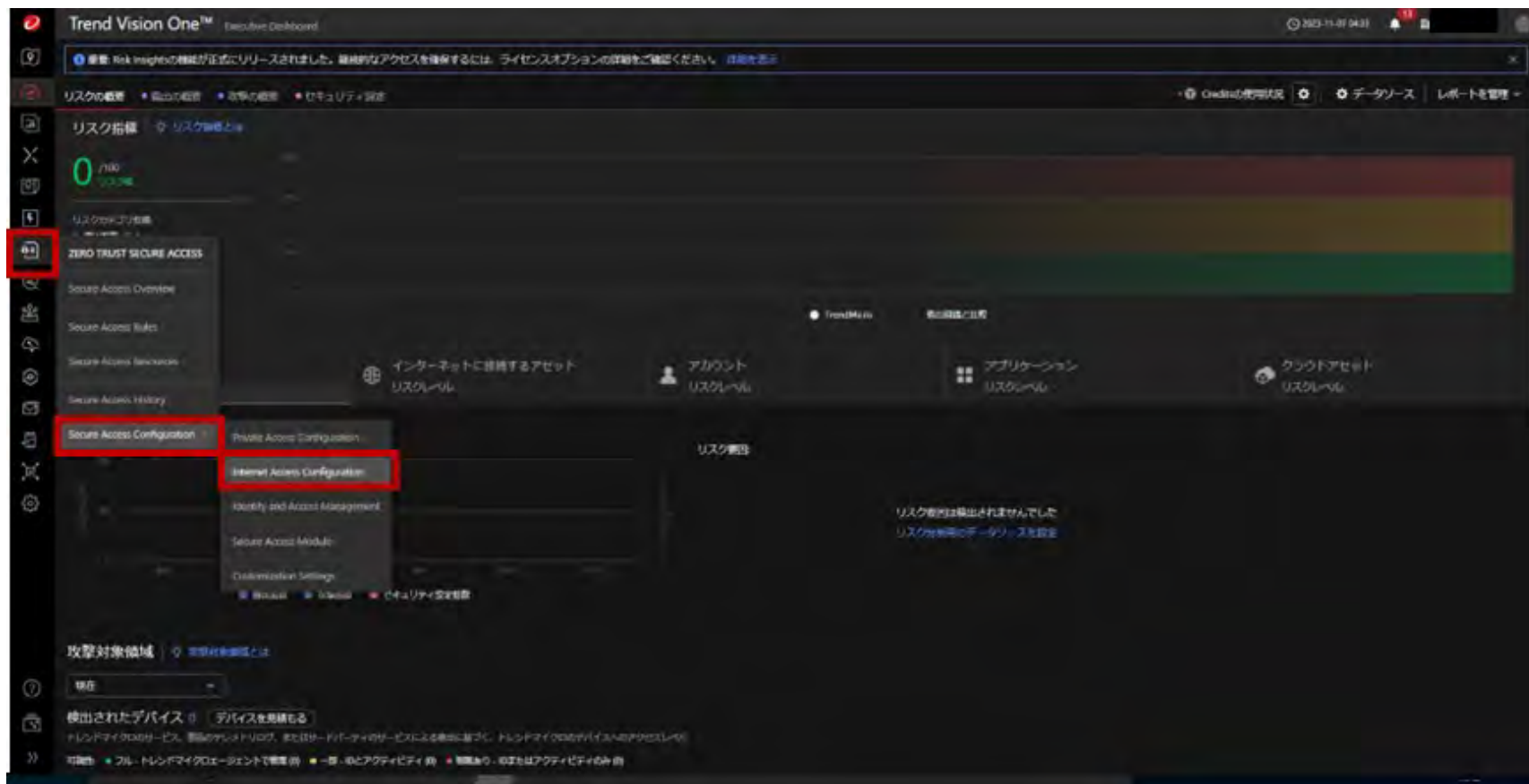
Select the geographic region where you want to provision your Trend Vision One console.

Region: Japan

Provision Console

STEP2:移行前作業 (ZTSA-IAを構成1)

2-6. Vision Oneコンソールが表示されたら、**「Zero Trust Secure Access」** > **「Secure Access Configuration」** > **「Internet Access Configuration」** を開きます。



STEP2:移行前作業 (ZTSA-IAを構成2)

2-7. Internet Access Service (SWG) を設定が表示されたら、「今すぐ開始」をクリックします。

Trend Vision One™ Internet Access Configuration

Trend Micro Internet Access Service (SWG) を設定

インターネットアクセスゲートウェイを実施することで、組織全体でのユーザのクラウドアプリの使用状況とWebアクティビティを監視および制御してリスクを軽減します。これにより、移動中、自宅、または企業ネットワークのいずれの場所でも、あらゆるユーザまたはグループがいつでも安全にインターネットにアクセスできるようになります。

今すぐ開始

プライベートアクセスを保護

Trend Micro Private Access Serviceをインストールして、自営ネットワークリソースと許可されたユーザ/デバイスとの間に接続された接続を確立します。これにより、オンラインサービスのデータセンターやクラウド（SaaS）環境など、適切なネットワークを介して内部アプリケーションやシステムに安全なアクセスが保証されます。

手順1. (オプション) ゲートウェイとネットワークの場所を管理します。

企業ネットワーク上にあるIPアドレスのグループを定義して、Webアクティビティを許可し、インターネットアクセス制限ルールを適用します。企業ネットワークまたはプライベートクラウドネットワークの場所を指定して、クラウドベースのインターネットアクセスゲートウェイまたは独自のオンプレミスゲートウェイ経由で安全にインターネットリソースにアクセスできるようにします。

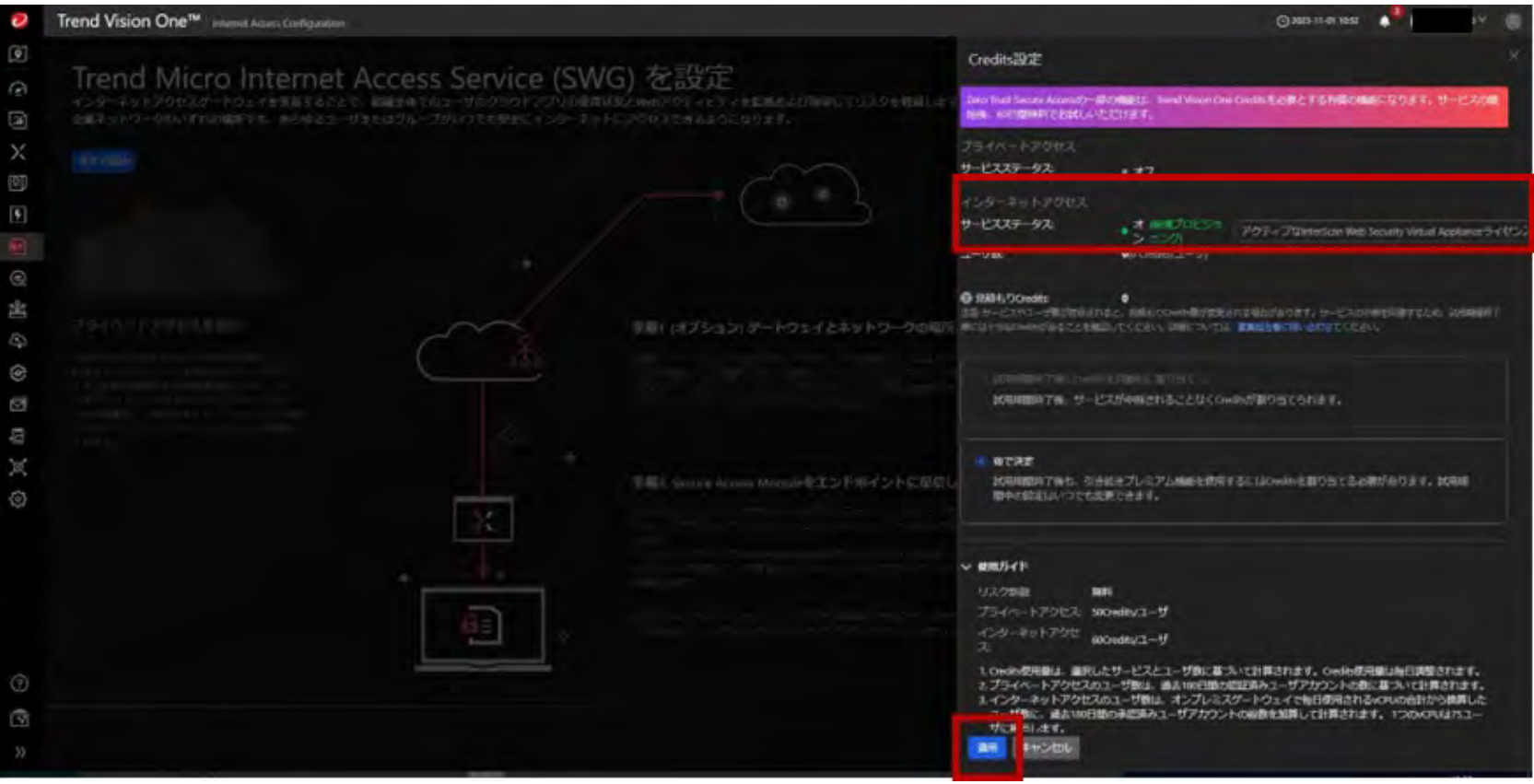
手順2. Secure Access Moduleをエンドポイントに配信します。

エージェントインストールコマンドをコピーして、パブリックエンドポイントに適用します。インターネットアクセスゲートウェイは、エージェントがインストールされた管理対象エンドポイントにのみ有効になります。エージェントを介してSecure Access Moduleをエンドポイントに配信します。これにより、Trend Vision Oneのモジュールを通じて、管理下のエンドポイントからクラウドアプリケーションやWebサイトへのアクセスを保護できます。

重要: 一部の Trend Vision Oneのインストールで、デバイスが自動的に検出され、自動でクライアントソフトウェアのインストールが開始され、インストールが完了するまでインストールが完了しない場合があります。インストールが完了したら、インストールが完了するまでインストールが完了しない場合があります。

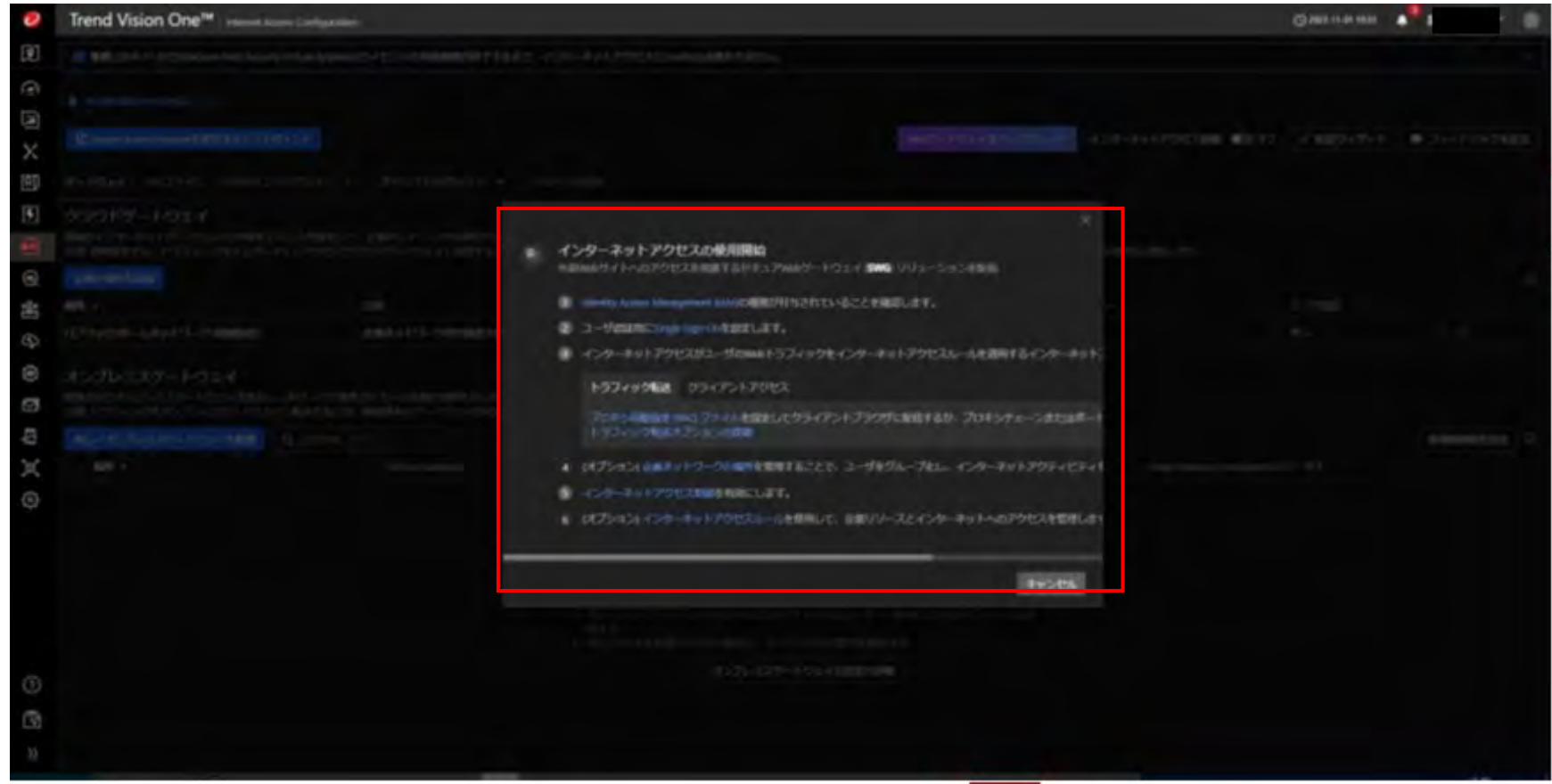
STEP2:移行前作業 (ZTSA-IAを構成3)

2-8. インターネットアクセスが「オン (新規プロビジョニング)」になり、「アクティブなInterScan Web Security ライセンス」と表示されていることを確認し、「適用」をクリックします。



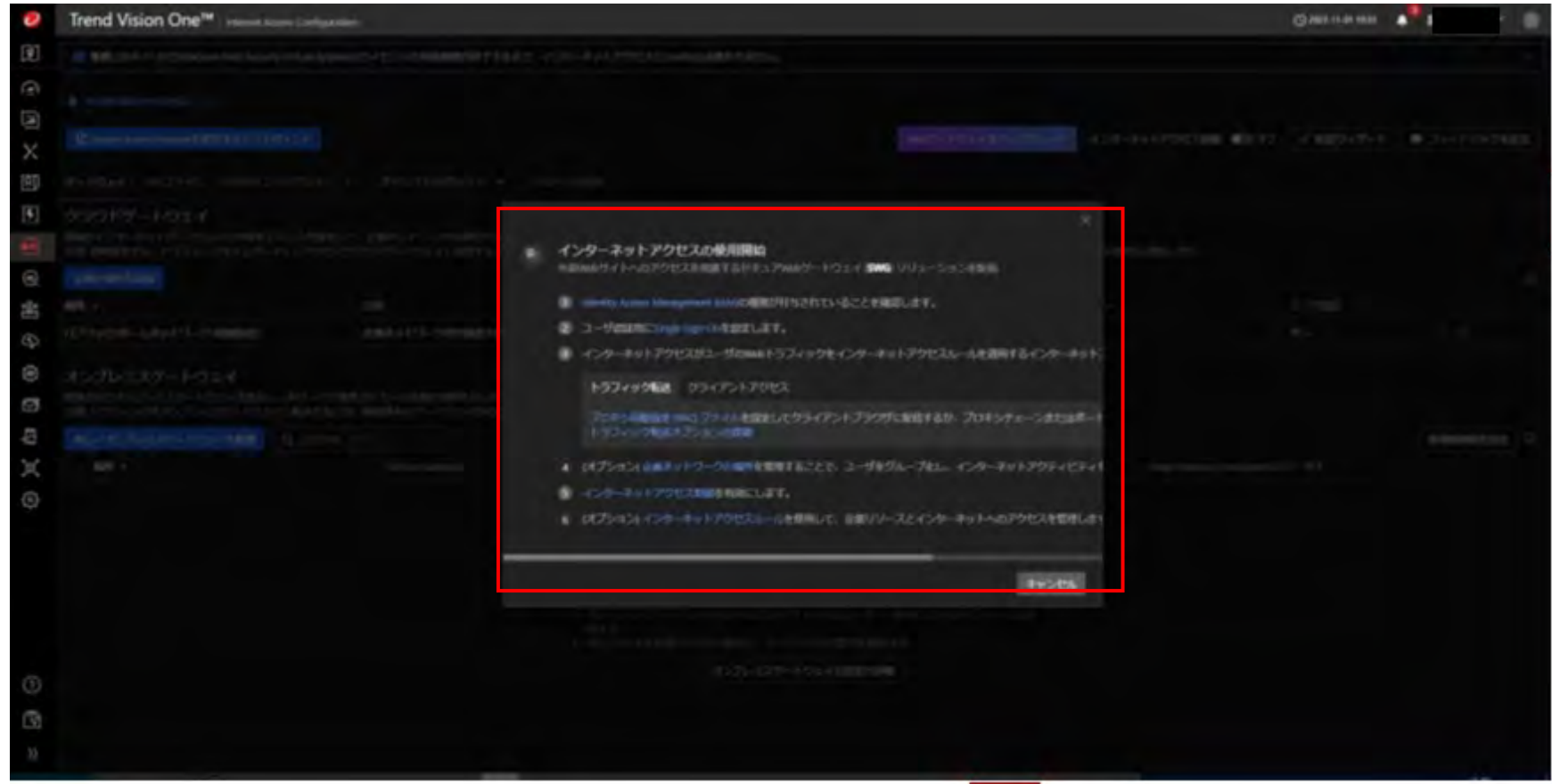
STEP2:移行前作業 (ZTSA-IAを構成4)

2-9. 「インターネットアクセスの使用開始」が表示されたら、表示されている手順に沿って設定を行います。



STEP2:移行前作業 (ZTSA-IAを構成4)

2-9. 「インターネットアクセスの使用開始」が表示されたら、表示されている手順に沿って設定を行います。



Step2補足

オンプレミスゲートウェイ導入手順

※オンプレミスゲートウェイを導入されない場合は、Step3へお進みください。

Step2補足：導入手順

- Service Gatewayの導入手順
- ZTSAオンプレミスゲートウェイサービスの導入
- オンプレミスゲートウェイ設定
 - ①認証プロキシ設定
 - ②認証無しプロキシ設定
 - ③認証バイパス設定
 - ④ICAP設定

Step2補足：Service Gatewayの導入手順

オンプレミスゲートウェイの利用にはService Gatewayの導入が必要となります。

Service Gatewayの導入は、ご利用の仮想基盤毎に手順が異なりますので、該当の手順をご参照ください。

仮想基盤	導入手順（オンラインヘルプ）
VMware ESXi	https://docs.trendmicro.com/ja-jp/documentation/article/trend-vision-one-deploying-a-service-_001
Microsoft Hyper-V	https://docs.trendmicro.com/ja-jp/documentation/article/trend-vision-one-deploying-a-service-_002
Microsoft Azure	https://docs.trendmicro.com/ja-jp/documentation/article/trend-vision-one-deploying-a-sg-azure
AWS	https://docs.trendmicro.com/ja-jp/documentation/article/trend-vision-one-deploying-a-sg-aws-a

Step2補足：Service Gatewayの導入手順

Service Gatewayの管理コンソールには「新しいオンプレミスゲートウェイを配置」から「Service Gateway Inventoryに移動」をクリックすることで移動することができます。（左ペインのメニューから直接進むこともできます。）

Trend Vision One™ | Internet Access Configuration

利用者情報の外部送信について

Secure Access Moduleを使用するエンドポイント

ゲートウェイ PACファイル HTTPS-インスペクション 許可リスト/拒否リスト グローバル設定

クラウドゲートウェイ

組織のインターネットゲートウェイの外部IPアドレスを指定して、企業ネットワークの場所から送信されるインターネットトラフィックを特定および検察
注意: 初期設定では、トラフィックをインターネットアクセスクラウドゲートウェイに送信するように設定されているすべてのエンドポイントは、企業の

企業の場所を追加

場所 ↑	説明	IPアドレス	IPの確認
パブリックホームネットワーク (初期設定)	企業ネットワーク内で設定されていないその...	-	-

オンプレミスゲートウェイ

配置されたオンプレミスゲートウェイを表示し、各サーバで管理されている企業の場所を示します。
注意: トラフィックをオンプレミスゲートウェイに転送するには、接続済みのゲートウェイのFQDNまたはIPアドレスをPACファイルに追加します。PACフ

新しいオンプレミスゲートウェイを配置

位置情報、IPアドレス

場所 ↑	Service Gateway	IPアドレス	vCPU	サービスステータス
------	-----------------	--------	------	-----------

オンプレミスゲートウェイが接続されている

オンプレミスゲートウェイに接続するには:

- Service Gateway仮想アプライアンスをダウンロードしてインストールする
- Zero Trust Secure Access On-Premises Gatewayサービスを有効化する

接続されたオンプレミスゲートウェイを使用してトラフィックを転送するには:

- オンプレミスゲートウェイのFQDNまたはIPアドレスを正しいポート番号とど
- PACファイルを対象デバイスに配信し、トラフィックの管理を開始する

オンプレミスゲートウェイの設定の詳細



オンプレミスのZero Trust Secure Accessゲートウェイを設定

Service Gateway仮想アプライアンスを配置し、Zero Trust Internet Accessオンプレミスゲートウェイサービスを有効化

- Service Gateway Inventoryに移動して、Service Gateway仮想アプライアンスを配置します。
- 「Zero Trust Secure Accessオンプレミスゲートウェイサービス」を有効にします。

Service Gateway Inventoryに移動

詳細については、オンラインヘルプセンターを参照してください。

接続済みのオンプレミスゲートウェイにトラフィックを転送する

- オンプレミスゲートウェイのFQDNまたはIPアドレスをPACファイルに追加します。
- 保護対象のエンドユーザデバイスにPACファイルを配信します。

詳細については、オンラインヘルプセンターを参照してください。

Step2補足：Service Gatewayの導入手順

仮想アプライアンスのイメージはService Gatewayの管理画面からダウンロードできます。

Trend Vision One™ Service Gateway Management

+ Virtual Applianceをダウンロード Trend Hosted Service Gatewayに登録

Service Gateway 接続ステータス バージョン サービス アクティブな接続 CPU使用率 メモリの使用率

Service Name	Version	Status
On-premises directory connection	1.0	Enabled
Smart Protection Services	2.0	Enabled
Suspicious Object List Synchronization	1.0	Enabled

Service Gatewayの専用サービスとサードパーティ製品を橋渡し

Service Gatewayは、組織のネットワーク内におよびサードパーティアプリケーションへのGateway Managementを介して、接続されます。

Service Gatewayアプライアンスにサービスを

- 接続管理の手間とネットワークトラブ
- オンプレミスのサードパーティアプリ

情報を取得



Service Gateway仮想アプライアンス

1 ネットワーク環境を設定

配信する前に、トレンドマイクロのサービスに接続するためのFQDNが設定されていることを確認します。
ファイアウォール要件を表示

2 仮想アプライアンスを配置

ディスクイメージの種類:

- VMware ESXi (OVA)
- Microsoft Hyper-V (VHDX)

仮想アプライアンスの仕様:

- 標準イメージ
12コアCPU、16GBメモリ、500GBストレージ
- 最小イメージ
8コアCPU、12GBメモリ、200GBストレージ

ディスクイメージのダウンロード

2.82GB(ファイルの詳細 | ダウンロードURLをコピー)

配信手順を表示 サードパーティのライセンス情報を表示
アプライアンスの仕様の詳細

登録トークン:

配信プロセス中にトークンを適用します。

Service Gatewayの導入手順

仮想アプライアンスを起動するとログイン要求が表示されます。

オンラインヘルプで指定されているアカウントと初期パスワードでログインします。

ログインが成功するとパスワード変更要求が表示されますので任意のパスワードに変更します。

```
Trend Micro Vision One - Service Gateway

To access the Command Line Interface (CLI), log on with your administrator account credentials:
Hint: Num Lock on

localhost login: admin
Password: ██████████
You must change your password to continue.
New password: ██████████
Retype new password: ██████████
Changing password for user admin.
New password: Retype new password: passwd: all authentication tokens updated successfully.
```


Service Gatewayの導入手順

パスワード変更が完了するとコマンド一覧が表示されます。

「enable」と入力すると管理コマンドが有効になります。

```
New password:
Retype new password:
Changing password for user admin.
New password: Retype new password: passwd: all authentication tokens updated successfully.
*****
* Trend Micro Vision One - Service Gateway *
*
* WARNING: Authorized Access Only *
*
* Version: 3.0.6.10187 *
* Status: Unregistered *
* Trend Micro Vision One console: - *
*****
Welcome admin - Wed May 22 00:54:13 UTC 2024

Available commands:
enable Enable administrative commands
exit Exit the CLI
help Display the CLI syntax
history Display the session's command history
log Process debugging data
show Display Service Gateway settings

> enable

Administrative commands:
configure Configure Service Gateway settings
connect Test connection to Trend Micro Vision One
exit Exit administrative commands
help Display the CLI syntax
history Display the session's command history
ping Ping a specific address
reboot Restart the Service Gateway after a specified delay or immediately
register Register the Service Gateway to Trend Micro Vision One
shutdown Shut down the Service Gateway after a specified delay or immediately

#
```

Service Gatewayの導入手順

以下のコマンドを入力してネットワーク設定を行います。

コマンド「`configure△network△primary△ipv4.static△インターフェイス△IPアドレス/サブネットマスク△ゲートウェイIPアドレス△DNSサーバIPアドレス△DNSサーバIPアドレス（2つ目）`」

※△はスペースを表現しております。

```
configure  Configure Service Gateway settings
connect   Test connection to Trend Micro Vision One
exit      Exit administrative commands
help      Display an overview of the CLI syntax
history   Display the current session's command line history
logout    Logout of the current CLI session
ping      Ping a specific address
reboot    Restart the Service Gateway after a specified delay or immediately
register   Register the Service Gateway to Trend Micro Vision One
shutdown  Shut down the Service Gateway after a specified delay or immediately

#
#
#
# configure network primary ipv4.static eth0 172.17.1.241/24 172.17.1.1 10.34.47.251
Please wait... This might take a few minutes. Do not shut down the Service Gateway.
[ 1023.622940] IPv6: ADDRCONF(NETDEV_CHANGE): cali9e28683eb0c: link becomes ready
[ 1024.397174] IPv6: ADDRCONF(NETDEV_CHANGE): calicc824706dba: link becomes ready
[ 1026.448893] IPv6: ADDRCONF(NETDEV_CHANGE): cali1e164d48a7f: link becomes ready
[ 1026.683863] IPv6: ADDRCONF(NETDEV_CHANGE): calieb00c25f546: link becomes ready
IPv4 address configured successfully.
#
#
#
```

Step2補足：Service Gatewayの導入手順

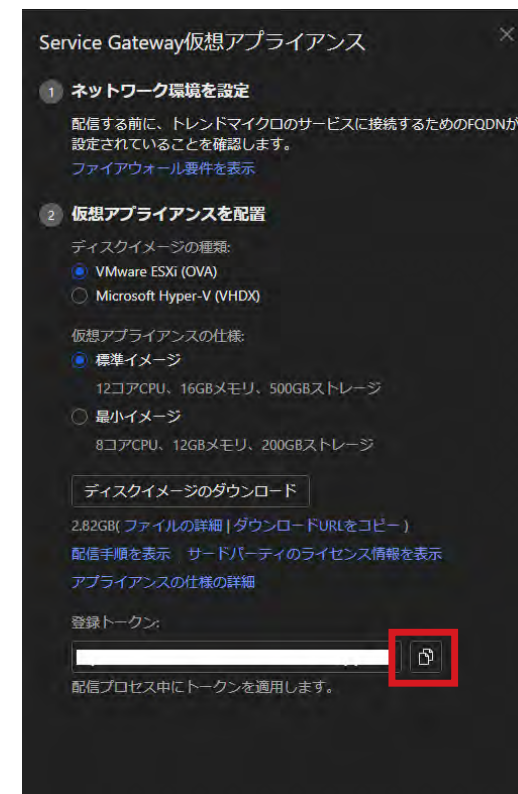
管理コンソールの仮想アプライアンスダウンロード画面から登録トークンをコピーします。

Service GatewayにSSHクライアントで接続し管理コマンドを有効化した後に以下コマンドを入力しService GatewayをVision Oneに登録します。

コマンド「register△トークン」

※△はスペースを表現しております。

```
# register  
  
Please wait... This might take a few minutes. Do not shut down the Service Gateway.  
Service Gateway registered to Trend Micro Vision One successfully.  
Successfully connect to sgi-iot.xdr.trendmicro.co.jp  
Successfully connect to upload.xdr.trendmicro.co.jp  
Successfully connect to api.xdr.trendmicro.co.jp  
#
```



Step2補足：Service Gatewayの導入手順

Vision Oneへの登録が完了すると一覧に表示されます。

ホスト名の変更はService Gateway設定から変更できます。

The screenshot displays the Trend Vision One Service Gateway Management interface. A table lists Service Gateways with columns for connection status, version, and services. The entry 'v1sg.6547de34(172.17.1.241)' is highlighted. A configuration modal for this gateway is open, showing settings for automatic updates and preferred update times. A red box highlights the gateway ID in the table, and another red box highlights the edit icon in the modal. A red arrow points from the edit icon in the modal to the gear icon in the table header.

Service Gateway	接続ステータス	バージョン	サービス
v1sg.6547de34(172.17.1.241)	正常	3.0.6	0

Service Gateway設定

v1sg.6547de34

Service Gatewayのアップデート

- 自動アップデート
 - 最新バージョンへのアップデート
 - X日以上前の最新バージョンにアップデートします。

優先アップデート時間:

月曜日 08:00 UTC+9

Service Gatewayは、優先アップデート時間にアップデートが失敗した場合、次にService Gatewayが再起動されます。

Step2補足： ZTSAオンプレミスゲートウェイサービスの導入手順

ZTSAオンプレミスゲートウェイサービスは、Service Gatewayの「サービスを管理」から導入します。



Step2補足：ZTSAオンプレミスゲートウェイサービスの導入手順

ZTSAオンプレミスゲートウェイサービスの導入が完了すると、Internet Access Configurationのオンプレミスゲートウェイに表示されます。

The screenshot shows the Trend Vision One Internet Access Configuration interface. The left sidebar contains navigation options like Platform Directory, Attack Surface Risk Management, Dashboards and Reports, XDR Threat Investigation, Threat Intelligence, Workflow and Automation, Zero Trust Secure Access, Secure Access Overview, Secure Access Rules, Secure Access Resources, Secure Access History, Secure Access Configuration, Private Access Configuration, Identity and Access Management, Secure Access Module, and Customization Settings. The main content area is titled 'Internet Access Configuration' and includes a notification about external user information, a 'Secure Access Moduleを使用するエンドポイント' button, and a toggle for 'インターネットアクセス制御' (Internet Access Control) which is turned on. Below this, there are tabs for 'ゲートウェイ', 'PACファイル', 'HTTPS-インスペクション', '許可リスト/拒否リスト', and 'グローバル設定'. The 'ゲートウェイ' tab is active, showing 'クラウドゲートウェイ' (Cloud Gateway) and 'オンプレミスゲートウェイ' (On-Premise Gateway) sections. The 'オンプレミスゲートウェイ' section contains a table with the following data:

場所	Service Gateway	IPアドレス	vCPU	サービスステータス	認証を適用	Deep Discovery Analyzerのステータス
> sg-va-demo	sg-va-demo	172.17.1.241	6	正常	オン	無効

Step2補足：①認証プロキシ設定

オンプレミスゲートウェイの導入直後は、認証プロキシとしてご利用いただけます。

The screenshot shows the Trend Vision One Internet Access Configuration interface. The left sidebar contains navigation options like Platform Directory, Attack Surface Risk Management, Dashboards and Reports, XDR Threat Investigation, Threat Intelligence, Workflow and Automation, Zero Trust Secure Access, Secure Access Overview, Secure Access Rules, Secure Access Resources, Secure Access History, Secure Access Configuration, Private Access Configuration, Internet Access Configuration, Identity and Access Management, Secure Access Module, and Customization Settings.

The main content area is titled 'Trend Vision One™ Internet Access Configuration' and shows the 'Secure Access Module' settings. The 'Internet Access Configuration' section is active, displaying 'Cloud Gateway' and 'On-premise Gateway' options. The 'On-premise Gateway' section includes a table of gateways and a 'Apply authentication' button highlighted with a red box.

場所	説明	IPアドレス	IPの確認	タイムゾーン	ユーザ認証
パブリック/ホームネットワーク (初期設定)	企業ネットワーク内で設定されていないその...	-	-	UTC	オン

場所	Service Gateway	IPアドレス	vCPU	サービスステータス	認証を適用	Deep Discovery Analyzerのステータス
> sg-va-demo	sg-va-demo	172.17.1.241	6	正常	オン	無効

Step2補足： ②認証無しプロキシ設定

認証無しプロキシはエージェントレスの端末からのアクセスでご利用いただけます。

オンプレミスゲートウェイの設定画面から「Secure Access Moduleをインストールせずに接続するエンドポイント」のチェックを外します。

The screenshot displays the configuration interface for an on-premise gateway. A dialog box titled '企業イントラネットの場所の設定' (Enterprise Intranet Location Settings) is open, showing the following details:

- 名前: sg-va-demo
- 説明: (例) https://のようなPACファイルを使用する二重認証の企業イントラネット
- タイムゾーン: アジア/東京
- タブ: 詳細設定 (selected), ログ転送, ICAPの統合, Deep Discovery Analyzer
- ユーザー認証: 次に対してユーザー認証を要求する
- Secure Access Moduleをインストールせずに接続するエンドポイント (highlighted with a red box)
- 注: Secure Access Moduleをインストールしていないエンドポイントでユーザー認証を完了する必要がない場合、インターネットアクセスは、vCPUの合計使用率に基づいてユーザー数の計算を制限します。新しいCredits計算は24時間後に有効になります。
- 上位プロキシルール:
 - データトラフィックの上位プロキシを有効化

A red arrow points from the highlighted checkbox to the '認証を適用' (Apply Authentication) button in the background interface.

Step2補足： ②認証無しプロキシ設定

認証を適用が「クライアントアクセスのみ」になっていれば設定完了となります。

オンプレミスゲートウェイ

配置されたオンプレミスゲートウェイを表示し、各サーバで管理されている企業の場所を示します。
注意: トラフィックをオンプレミスゲートウェイに転送するには、接続済みのゲートウェイのFQDNまたはIPアドレスをPACファイルに追加します。PACファイルの設定

新しいオンプレミスゲートウェイを配置 帯域幅制御を設定

場所 ↑	Service Gateway	IPアドレス	vCPU	サービスステータス	認証を適用	Deep Discovery Analyzerのステータス
> sg-va-demo	sg-va-demo	172.17.1.241	6	● 正常	クライアントアクセスのみ	無効

Step2補足：③認証バイパス設定

認証バイパスの対象とするIPアドレスグループを作成します。

Secure Access Resourcesの「IPアドレスグループ」から作成します。

The screenshot displays the Trend Vision One interface for configuring Secure Access Resources. The left sidebar shows the navigation menu with 'Secure Access Resources' highlighted. The main content area shows the 'IPアドレスグループ' (IP Address Group) configuration page. A red box highlights the '+ 追加' (Add) button, and a red arrow points to the '名前' (Name) field in the configuration dialog. The dialog is titled 'IPアドレスグループ設定' (IP Address Group Configuration) and contains the following fields:

- 種類 (Type): プライベートIPアドレスグループ (Private IP Address Group), パブリックIPアドレスグループ (Public IP Address Group)
- 名前 (Name): Server_group
- 説明 (Description): Server group
- IPアドレス (IP Address): 172.17.1.0/24

Buttons for '保存' (Save) and 'キャンセル' (Cancel) are visible at the bottom of the dialog.

Step2補足： ③認証バイパス設定

オンプレミスゲートウェイの設定から作成したIPアドレスグループを選択します。

選択されたIPアドレスグループのIPアドレスからアクセスが発生した場合、認証をせずに通信が行われます。

The screenshot displays the 'Enterprise Intranet Location Settings' dialog box. The 'Name' field is set to 'sg-va-demo'. The 'Time Zone' is set to 'Asia/Tokyo'. Under 'User Authentication', the checkbox 'Secure Access Moduleをインストールせずに接続するエンドポイント' is checked. Below this, a note states: 'ユーザー認証のバイパスを許可するプライベートIPアドレスグループを選択します。注意: 認証をバイパスするプライベートIPアドレスは、インターネットアクセスユーザー数にユーザーとして含まれません。' The 'Available Groups' section shows 'Server_group' selected. The 'Selected Groups' section also shows 'Server_group'. A red arrow points from the 'Server_group' in the 'Selected Groups' section to the '認証を適用' button in the background interface.

Step2補足：④ICAP設定

オンプレミスゲートウェイの設定の「ICAPの統合」から「ICAPを有効化」を有効化することでICAPが利用可能となります。

企業イントラネットの場所の設定

インターネットアクセスオンプレミスゲートウェイで保護する企業イントラネットの場所を定義します。

名前:
sg-va-demo

説明:
例: hr.pacのようなPACファイルを使用するニューヨークの人事管理エンドポイント

タイムゾーン:
アジア/東京

詳細設定 ログ転送 **ICAPの統合** Deep Discovery Analyzer

オンプレミスゲートウェイは、Internet Content Adaptation Protocol (ICAP) クライアントとの統合をサポートしており、脅威対策またはDLPを実行します。

ICAPを有効化

REQMOD: icap://172.17.1.241:1344/REQ-Service
RESPMOD: icap://172.17.1.241:1344/interscan

ICAP over SSLを有効化

ICAPサーバ (オンプレミスゲートウェイ) からのICAP応答ヘッダ:

X-Virus-ID
 X-Infection-Found

ICAPクライアントからのICAP要求ヘッダ:

X-Authenticated-User

注意: ICAPが有効な場合、インターネットアクセスは、合計CPU使用量に基づいてユーザ数の計算を開始します。新しいCredits計算は24時間以内に有効になります。

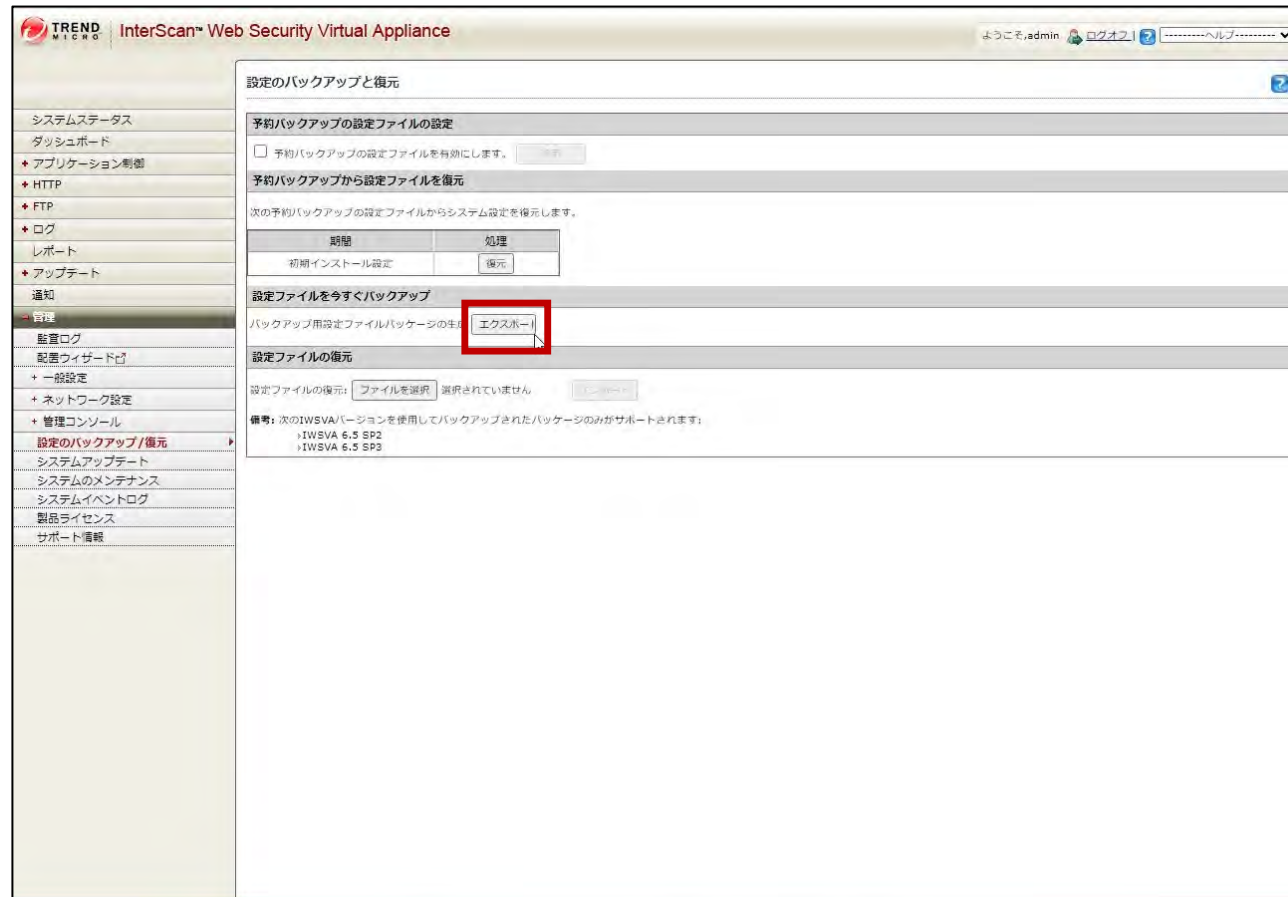
保存 キャンセル

STEP3: 移行作業

STEP3: 移行作業 (IWSVA/IWSS設定吸い上げ)

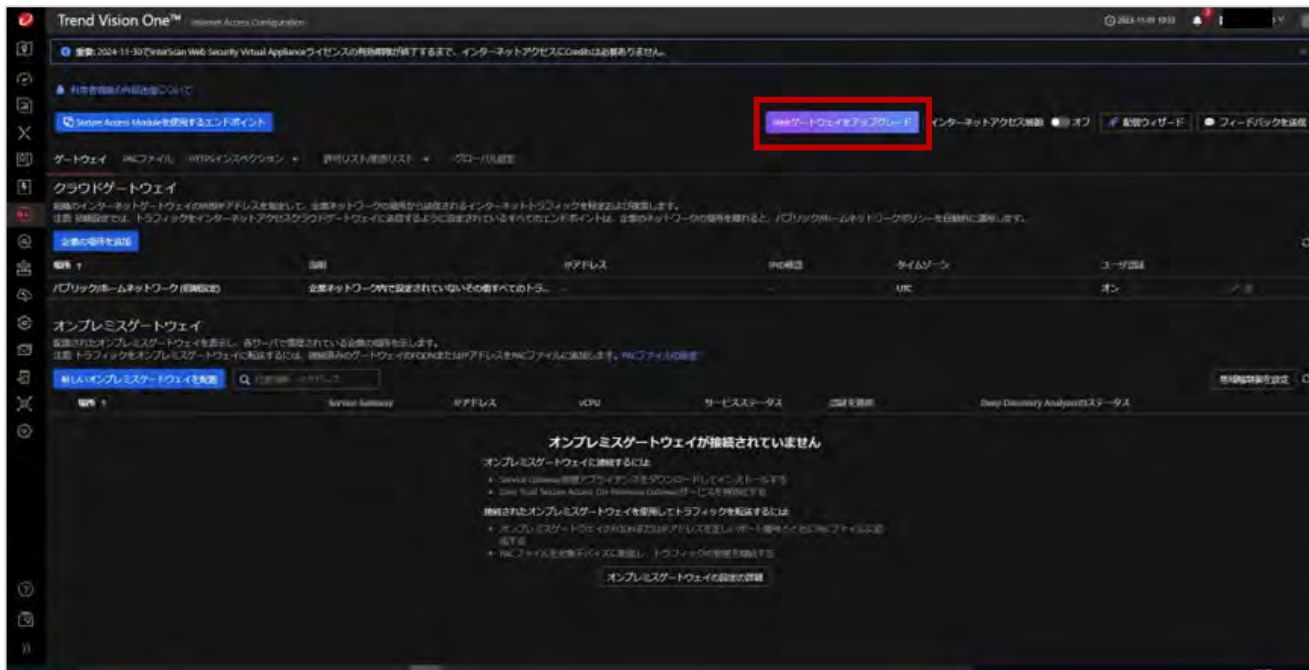
3-1. 移行元のIWSVA/IWSSでバックアップを取得します。

IWSVA/IWSSの管理コンソールの「**管理**」 > 「**設定のバックアップ/復元**」 > 「**エクスポート**」をクリックして取得します。(tarファイルが出力されます。)

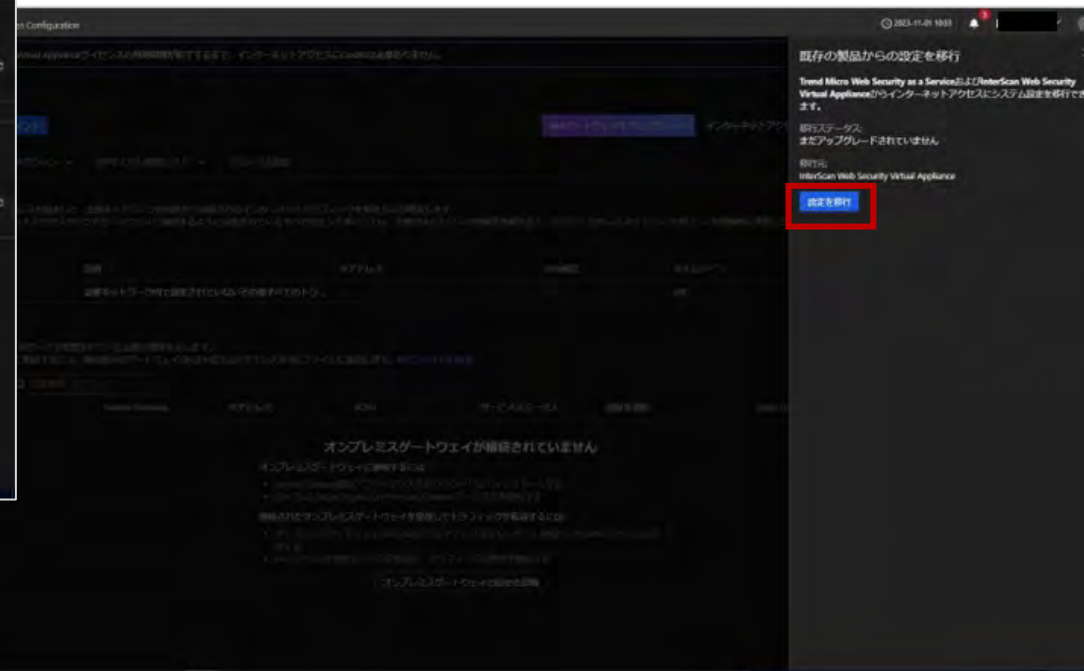


STEP3: 移行作業 (設定移行 1)

3-2.Vision Oneコンソールの「Internet Access Configuration」に戻り「webゲートウェイをアップグレード」をクリックします。

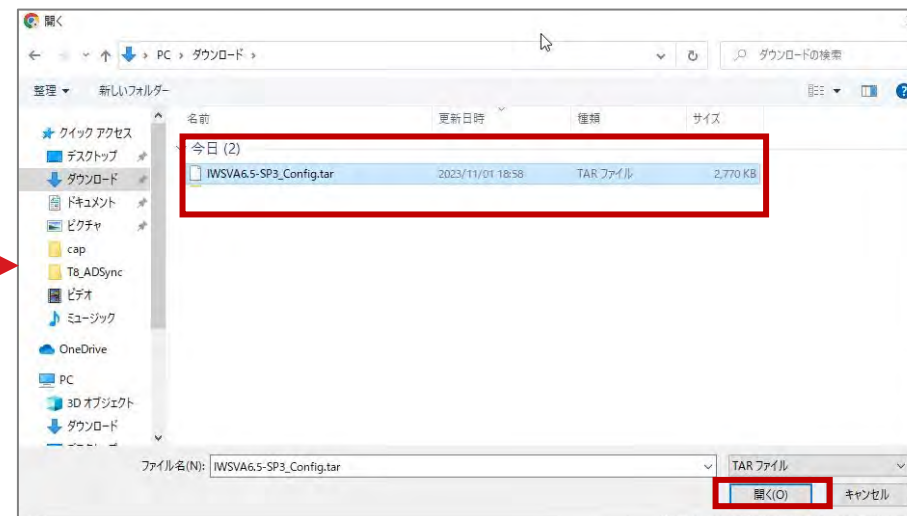
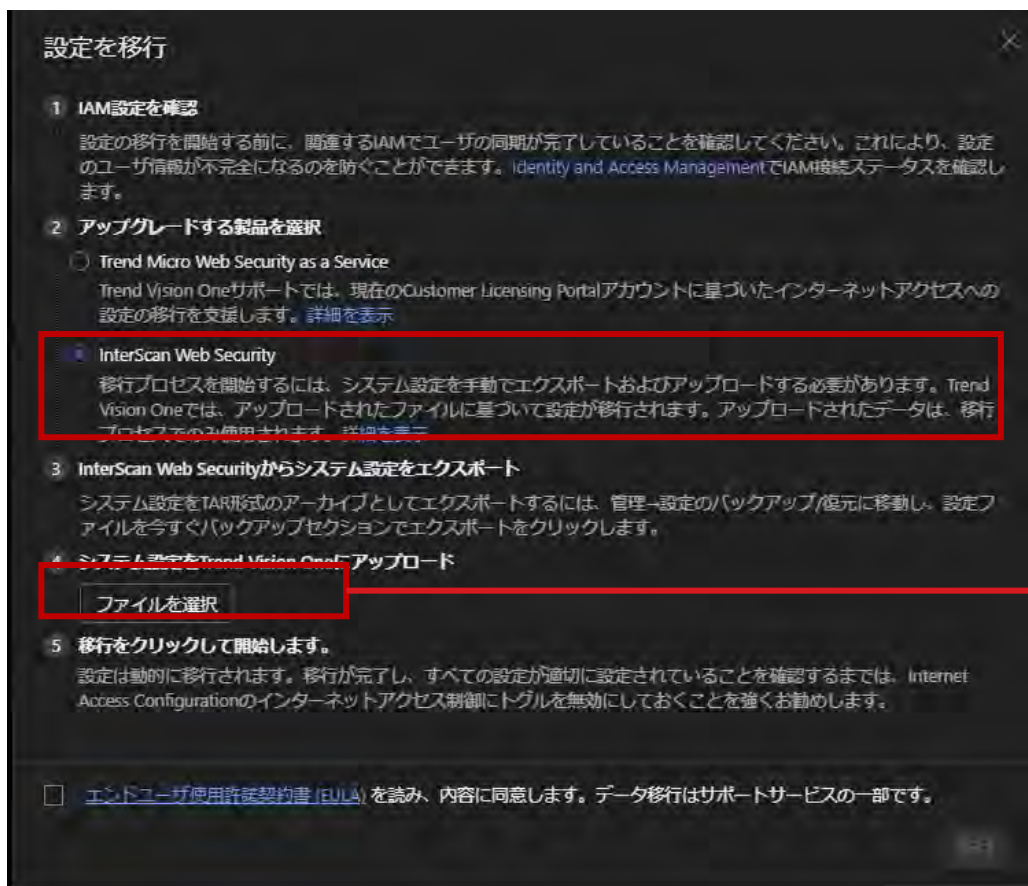


3-3.「既存の製品からの設定を移行」が表示されたら「設定を移行」をクリックします。



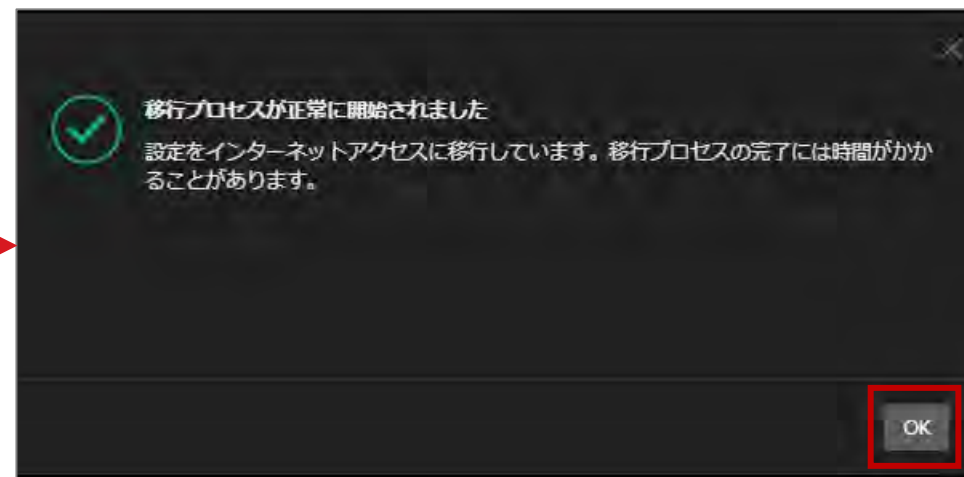
STEP3: 移行作業 (設定移行 2)

- 3-4. 「**InterScan Web Security**」を選択し、「**ファイルを選択**」をクリックします。
手順3-1で出力されたtarファイルを選択します。



STEP3: 移行作業 (移行ツール稼働)

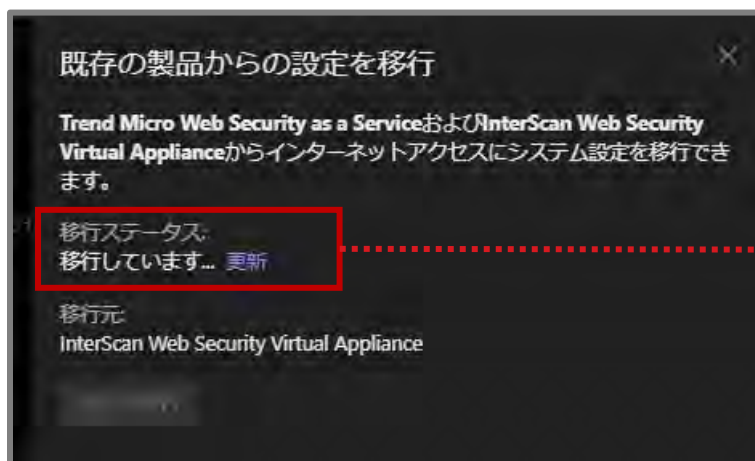
3-5. 指定したtarファイルが表示されていることを確認し、EULA同意にチェックを入れて「**移行**」をクリックします。
「移行プロセスが正常に開始されました」と表示されたら「**OK**」をクリックします。



STEP3: 移行作業 (移行完了)

3-6. 移行ステータスが「移行しています...」と表示され移行が開始されます。「更新」をクリックするとステータスが更新されます。

「移行済み」と表示されると移行が完了となります。「移行ログをダウンロード」をクリックすると移行ログがダウンロードできます。確認後、右上の「×」をクリックして、移行ツール画面を閉じます。



移行完了



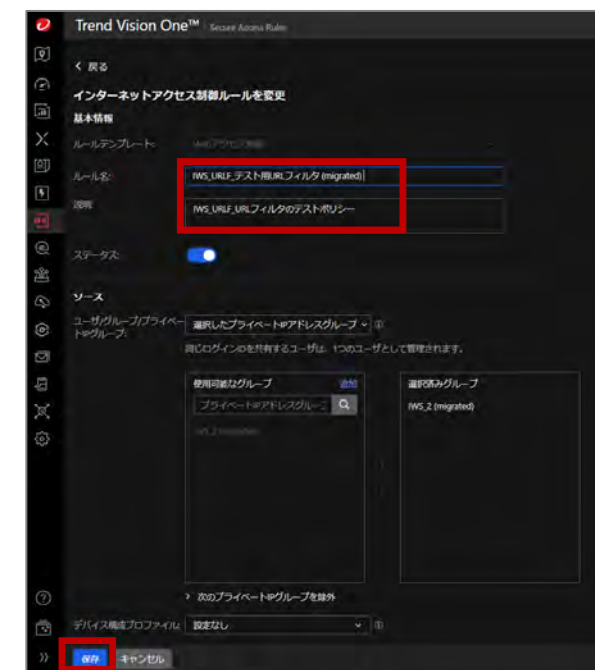
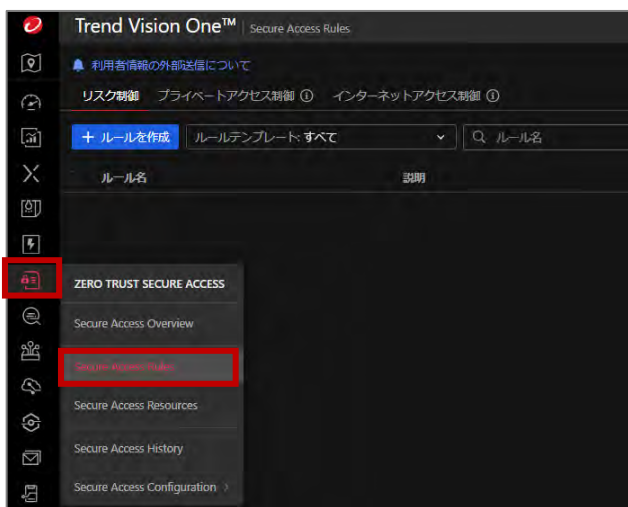
STEP4: 移行後作業

STEP4: 移行後作業 (移行確認1)

4-1. 移行された情報の確認を行います。
メニューから「**Zero Trust Secure Access**」>「**Secure Access Rules**」を選択します。

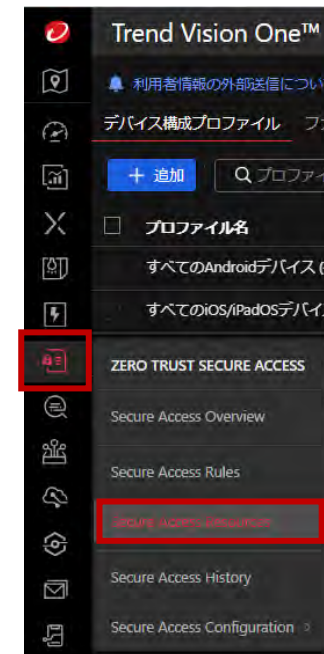
4-2. 「**インターネットアクセス制御**」を開き、
ルールを確認します。
* 移行されたルール名は、**先頭に「IWS_」**
末尾に「(migrated)」が付きます。

4-3. ルール名をクリックすると、
編集画面が表示されます。
ルール名や説明等を編集し下部の
「**保存**」をクリックし保存します。



STEP4: 移行後作業 (移行確認2)

4-4. メニューから「Zero Trust Secure Access」 > 「Secure Access Resources」を選択します。



4-5. 「Secure Access Resources」に各オブジェクトが移行されていることを確認します。
下図はIPアドレスグループに移行されたオブジェクトの例になります。

名前	種類	説明	IPアドレス	適用されたルールの数	最終更新日
<input type="checkbox"/> IWS_2 (migrated)	プライベートIP...	IWS_2	172.17.1.191-172.17.1.195	1	2023-11-01 11:28:55

STEP4補足:オンプレミスゲートウェイを指定したポリシー設定

オンプレミスゲートウェイを指定したポリシー設定を行うことが可能です。

インターネットアクセス制御ルールを作成する際に以下の指定を行います。

- ソースの場所で「選択した場所」を選択
- 企業ネットワークの場所で作成したオンプレミスゲートウェイを選択

Trend Vision One™ Secure Access Rules

< 戻る

インターネットアクセス制御ルールを作成

基本情報

ルールテンプレート: Webアクセス制御

ルール名: ルール名

説明: 説明

ステータス:

ソース

ユーザー/グループ/プライベートIPグループ: すべてのユーザー/グループ

同じログインIDを共有するユーザーは、1つのユーザーとして管理されます。

> 次のユーザー/グループを除外

デバイス構成プロファイル: 設定なし

場所: 選択した場所

企業ネットワークの場所

ゲートウェイ別の使用可能な場所

企業ネットワークの場所

オンプレミスゲートウェイ

sg-va-demo

ゲートウェイ別の選択した場所

オンプレミスゲートウェイ

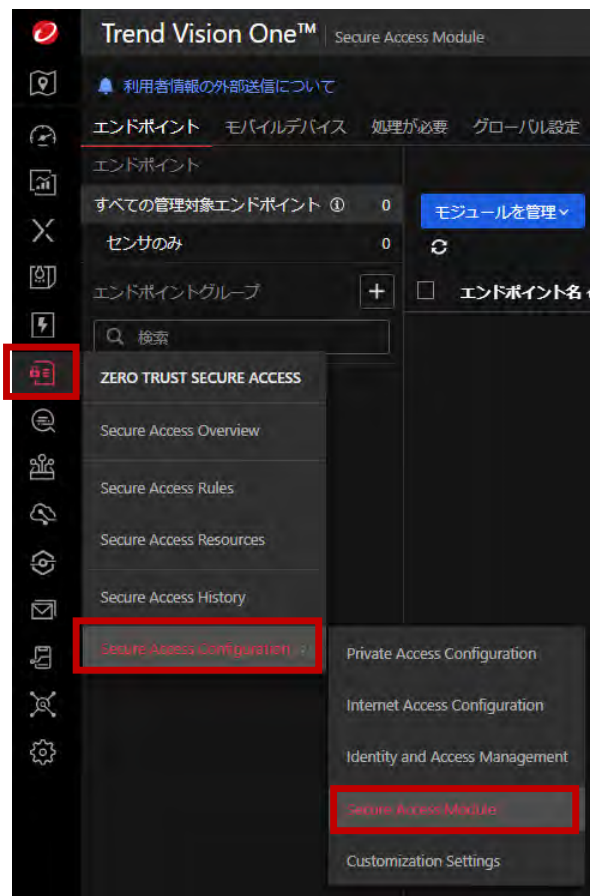
sg-va-demo

STEP5:動作確認

STEP5: 動作確認

5-1. エージェントの導入を行います。

メニューから「*Zero Trust Secure Access*」 > 「*Secure Access Configuration*」 > 「*Secure Access Rules*」を選択します。



STEP5: 動作確認(Agent準備)

- 5-2. 「エージェントインストーラをダウンロード」をクリックし、対象OSを選択後「インストーラをダウンロード」をクリックします。「EndpointBasecamp.exe」がダウンロードされます。

The screenshot displays the Trend Vision One console interface. A red box highlights the 'エージェントインストーラをダウンロード' (Download Agent Installer) button in the top right area of the console. A red arrow points from this button to a modal dialog box titled 'エージェントインストーラをダウンロード'. The dialog box contains the following text:

エージェントインストーラをダウンロード

Trend Vision Oneの機能を有効にする前に、できるだけ多くのエンドポイントにエージェントをインストールして、リスクのあるエンドポイント特定してください。

Endpoint Sensorの検出と対応設定によっては、センサのみのエージェントについて、エージェントインストーラの配信でCreditsが消費される場合があります。設定を確認または変更するには、Endpoint Inventory > 設定 > 一般センサ設定に移動します。

Windows (32ビット、64ビット)

Secure Access Moduleの配信では次のバージョンがサポートされます。

- Windows 8 / 8.1 / 10 / 11
- Windows Server 2016、2019、および2022

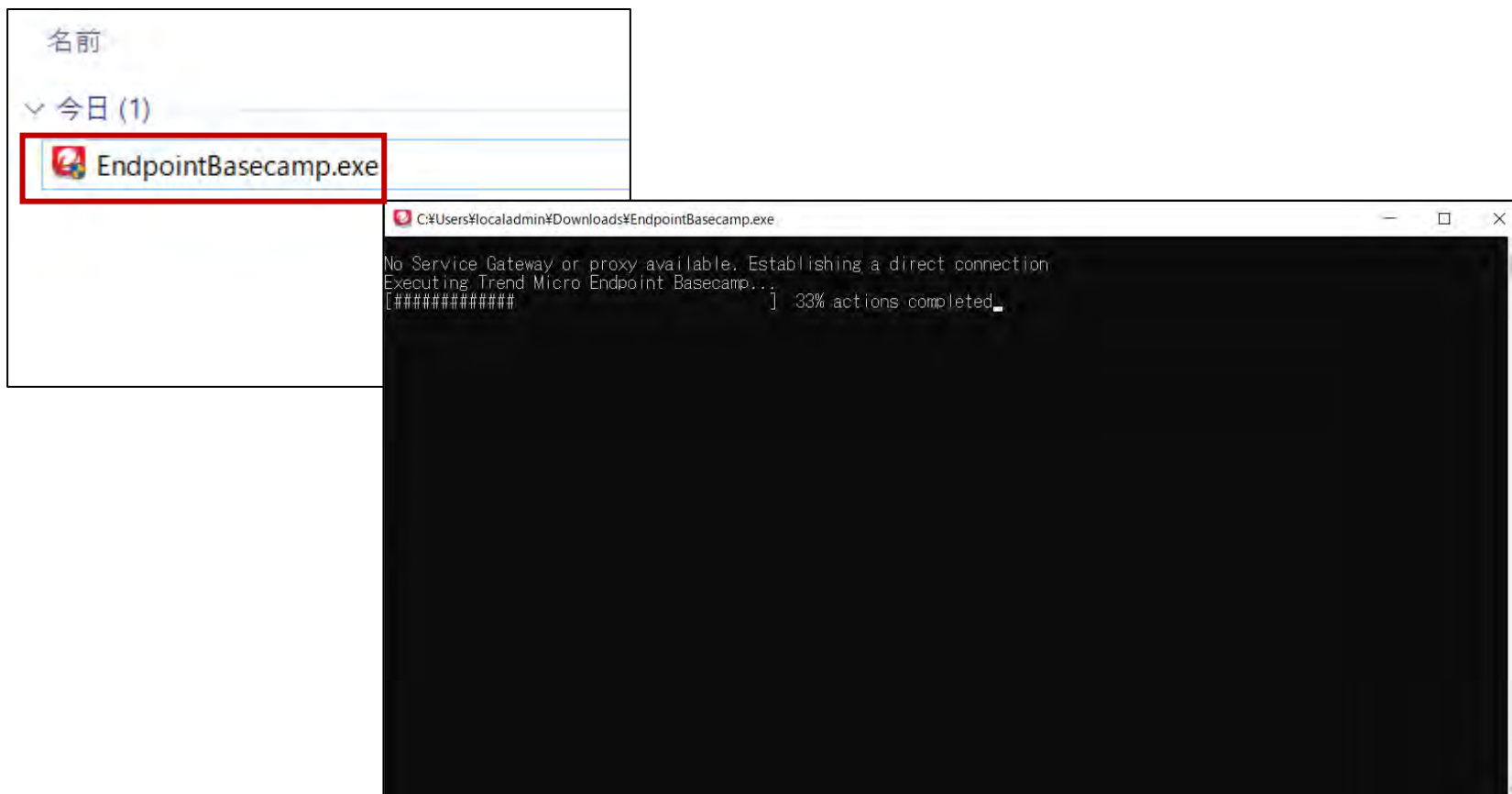
インストーラをダウンロード

ダウンロードリンクの取得

エンドポイントから既存のエージェントを削除するには、Endpoint Inventory > エージェントインストーラに移動して、アンインストールツールをダウンロードします。

STEP5: 動作確認 (Agentインストール)

5-3. 導入するエンドポイントで「EndpointBasecamp.exe」を実行してインストールします。



STEP5: 動作確認(配信)

- 5-4. 一覧にエンドポイントが表示されたら、チェックを入れ、「**モジュールを配信**」を選択します。配信画面が表示されますので「**配信**」をクリックして配信します。配信が完了するとモジュール配信ステータスが「**配信済み**」になります。

The screenshot illustrates the workflow for distributing modules to endpoints in the Trend Micro Vision One console. It shows the initial selection of endpoints, the navigation to the distribution menu, the configuration of the distribution dialog, and the final status change from '未配信' (Not Distributed) to '配信済み' (Distributed).

エンドポイント名	OS	モジュール配信ステータス
DESKTOP-F3EK6I8	Windows 10	未配信

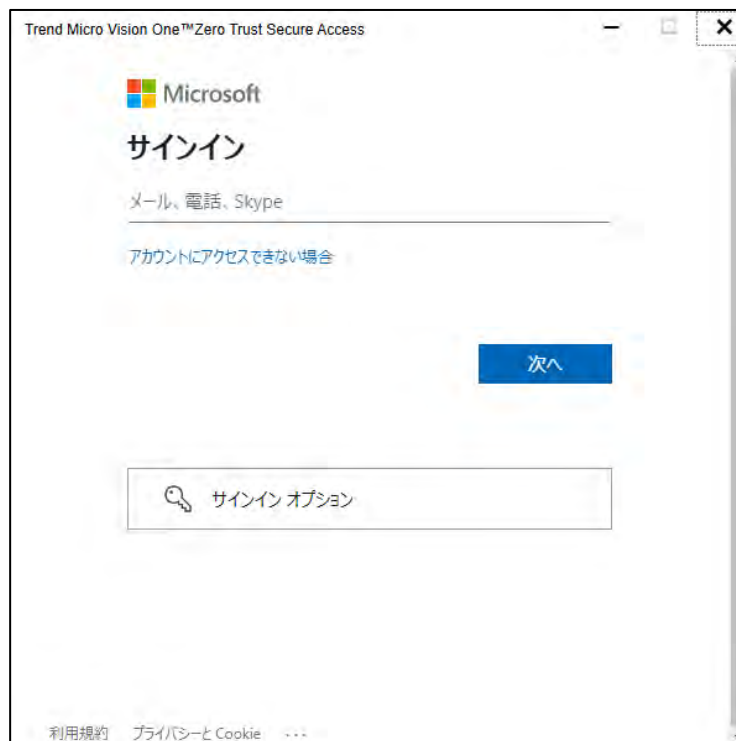
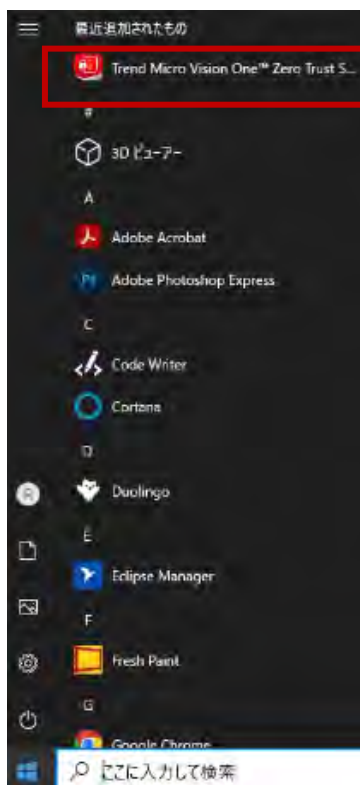
エンドポイント名	OS	モジュール配信ステータス
DESKTOP-F3EK6I8	Windows 10	モジュールを配信中

エンドポイント名	OS	モジュール配信ステータス
DESKTOP-F3EK6I8	Windows 10	配信済み

STEP5: 動作確認(認証)

5-5. エージェントを起動して認証します。

「インターネットアクセス」が「接続済み」になれば利用可能な状態になります。
移行したフィルタリング設定等が適用されることをご確認ください。



※Microsoft Entra ID(旧Azure AD)と連携した場合の画面例になります。

STEP5: 動作確認(補足)

補足.エージェントの導入ができない端末の場合、証明書のインストールとPACファイルの設定を実施します。
証明書は「Internet Access Configuration」の「HTTPSインスペクション」から取得します。
PACファイルは「PACファイル」から確認します。

Trend Vision One™ Internet Access Configuration

重要: 2024-11-30でInterScan Web Security Virtual Applianceライセンスの有効期限が終了するまで、インターネットアクセスにCreditsは必要ありません。

Secure Access Moduleを使用するエンドポイント Webゲートウェイをアップグレード インターネットアクセス制御: オン 配信ウィザード フィードバックを送信

ゲートウェイ PACファイル **HTTPSインスペクション** 許可リスト/拒否リスト グローバル設定

HTTPSインスペクションルール

優先度	ルール名	場所	URL	最終更新日	ステータス
1	初期設定のHTTPSイ...	すべての場所	任意のURL	-	オン

ゲートウェイ **PACファイル** HTTPSインスペクション 許可リスト/拒否リスト グローバル設定

+ 追加 Pacファイル名, FQDN, IPアドレス

PACファイル名 ↑	説明	参照ゲートウェイ ①	PACファイルの場所	適用済みプラットフォーム ①
proxy.pac	初期設定のPAC...	proxy.ztsa-iag-int.trendmicro.co...	https://pac.jp.ztsa-iag.trend..	Windows, macOS, iOS/iPadOS, Android

初期設定の証明書を管理

証明書の管理 バイパスモード

カスタムゲートウェイ証明書を使用するには、証明書の生成に使用する必要な証明書署名要求 (CSR) をダウンロードします。詳細については、オンラインヘルプを参照してください。

CSRをダウンロード ↓

カスタム証明書を適用しないユーザには、HTTPSインスペクションルールに添付された初期設定のルートCA証明書がインターネットアクセスから提供されます。

クラウドゲートウェイ証明書

カスタム証明書をアップロード

発行先: Trend Micro Web Security Cloud Root CA
発行元: Trend Micro Web Security Cloud Root CA
有効期間: 2020年8月17日 (月) 午前 06:59:21 から 2040年9月1日 (土) 午前 06:59:21
SHA-1サムプリント: 50xC1:23:63:F1:8F:C8:42:E3:DD:50:8E:17:5B:4F:0D:57:AC:8F:6F

組み込み証明書にリセット

組み込み証明書のダウンロード (Internet Access Service提供)

保存

オンプレミスゲートウェイ証明書

カスタム証明書をアップロード

発行先: Trend Micro Web Security Onpremise Root CA
発行元: Trend Micro Web Security Onpremise Root CA
有効期間: 2023年11月1日 (水) 午前 10:33:01 から 2053年11月1日 (土) 午前 10:33:01
SHA-1サムプリント: 92:2E:E0:8B:24:B6:D6:7A:56:CA:A6:50:19:C8:D7:5E:47:4E:44:1E

組み込み証明書にリセット

組み込み証明書のダウンロード (Internet Access Service提供)

保存

参考情報: 製品別機能簡易比較 他

製品別 機能比較表 1/3

	IWSVA/IWSS	TMWS		ZTSA
	ver.6.5	Standard	Advanced	Internet Access
セキュリティ対策機能				
フォワードプロキシ	○	○	○	○
マルウェア・ポットネット対策	○	○	○	○
Webレピュテーション	○	○	○	○
AI機械学習検索	×	○	○	○
仮想アナライザ・サンドボックス	×	×	○	プレビュー ※Sandbox analysisが必要
リスク制御	×	×	×	○ ※ASRMと連携
コンプライアンス対策機能				
URLフィルタリング機能	○	○	○	○
アプリケーション制御	○	○	○	○
クラウドサービスフィルタ	×	△ (6件まで)	○	○ ※新機能名：テナント制御
情報漏えい対策	○	×	△ ※テンプレートカスタマイズ不可	◎ ※テンプレートカスタマイズ可能
デバイスポスチャ	×	×	×	○
プロトコル				
対応プロトコル	HTTP/HTTPS/FTP	HTTP/HTTPS	HTTP/HTTPS	HTTP/HTTPS
HTTPSインスペクション	○	○	○	○

製品別 機能比較表 2/3

	IWSVA/IWSS	TMWS		ZTSA
	ver.6.5	Standard	Advanced	Internet Access
オンプレミスゲートウェイ				
ハイブリッド構成	×	○	○	○
オンプレミスゲートウェイ 導入環境	VMware ESXi, Hyper-V ※IWSVAのみ	VMware ESXi	VMware ESXi	VMware ESXi, Hyper-V, Amazon AWS, Microsoft Azure
ICAPモード	○	○	○	○
認証				
オンプレミスAD	○	○	○	×
オンプレミスAD + ADFS	○	○	○	○
Entra ID(旧AzureAD)	×	○	○	○
Okta	×	○	○	○
Google	×	○	○	△ ※Private Preview
OpenLDAP	○	×	×	○
独自ユーザー管理	×	○	○	○

製品別 機能比較表 3/3

	IWSVA/IWSS	TMWS		ZTSA
	ver.6.5	Standard	Advanced	Internet Access
運用				
RBAC	○	○	○	○
監査ログ	○	○	○	○
ログ保管	-	180日	180日	180日
Syslog転送	○	○	○	○ ※クラウドはAPIによるJSON形式の提供 オンプレミスゲートウェイはSyslog転送
PACファイル管理	○	○	○	○
クライアントエージェント				
Windows	-	○	○	○
Mac	-	○	○	○
iOS/iPadOS	-	△ ※Mobile VPNのみ	△ ※Mobile VPNのみ	○ ※Mobile Security + Intuneが必要
Android	-	○	○	○ ※Mobile Security + Intuneが必要
拡張性				
Vision One連携	×	△	△	○
プライベートアクセス機能	△ ※リバースプロキシモードで一部対応	×	×	○ ※ZTSA-Private Accessで対応

参考情報

ZTSAのご利用にあたり参考となる情報を下記URLで公開しております。

項目	URL
[Trend Vision One : Zero Trust Secure Access] 問題発生時の調査に必要な情報一覧	https://success.trendmicro.com/dcx/s/solution/000290943?language=ja
[Trend Vision One] 製品ライセンス 購入後の アクティベーションの手順	https://success.trendmicro.com/dcx/s/solution/000289592?language=ja

項目	URL
[Trend Vision One : Zero Trust Secure Access] 公式製品Webページ（無料体験版リンク含む）	https://www.trendmicro.com/ja_jp/business/products/network/zero-trust-secure-access.html
[Trend Vision One : Zero Trust Secure Access] オンラインヘルプ	https://docs.trendmicro.com/ja-jp/documentation/article/trend-vision-one-zero-trust-secure-ac

