InterScan to Gateway-SaaS

【最終版】
オンプレミスから SaaSへの移行のススメ

Nov 6th, 2023　　Rev 3.0

トレンドマイクロ株式会社

Agenda

1. ゲートウェイオンプレミスInterScanのサポート終了(EOL)について

2. 何故、SaaSセキュリティに移行するのか？そのメリットとは？

3. SaaSへの移行をご支援する仕組みについて

Ver	Date	Note
1.0	Feb 18th, 2022	第1版
2.0	Apr 1st, 2023	一斉値上げに伴う、掲載希望小売価格の変更
3.0	Nov 6th, 2023	移行先変更(ZTSA-IA/EmS-std)、特別価格、Vision One連携メリット

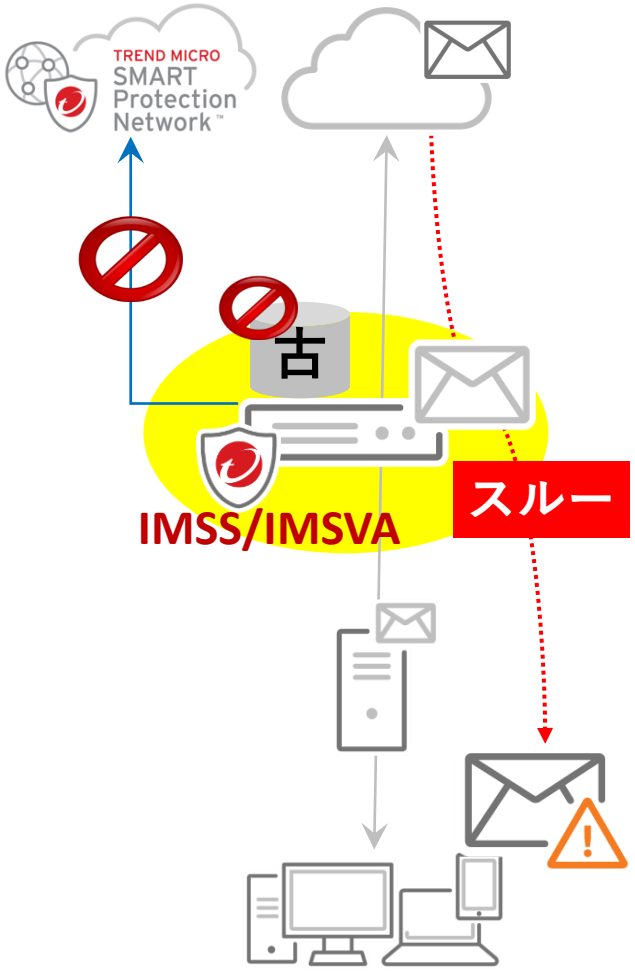
InterScanのサポート終了(EOL)と最新の移行先について

サポート終了日程と対象ライセンス/製品

- 「仮想アプライアンス版」と「ソフトウェア版」ではサポート終了日が異なります。
- サポート終了日までに推奨移行先のSaaS製品などへの移行の完了をお願いします。

ライセンス名	InterScan VirusWall (IVW)			
ライセンス名	InterScan Messaging Security (IMS)		InterScan Web Security (IWS)	
製品名	InterScan Messaging Security Virtual Appliance	InterScan Messaging Security Suite plus	InterScan Web Security Virtual Appliance	InterScan Web Security Suite plus
略称	IMSVA	IMSS	IWSVA	IWSS
形式	仮想アプライアンス	ソフトウェア	仮想アプライアンス	ソフトウェア
Latest Ver.※	9.1 Re-Pack	9.1	6.5 SP3	6.5
サポート終了日	**2024/6/30**	**2025/3/31**	**2024/6/30**	**2025/3/31**
推奨移行先	**Trend Micro Email Security Standard (EmS-std)**		**Trend Vision One Zero Trust Secure Access- Internet Access (ZTSA-IA)**	
形式	SaaS (Cloud)			

サポート切れのInterScanを使い続けると？



【InterScanサポート終了後】

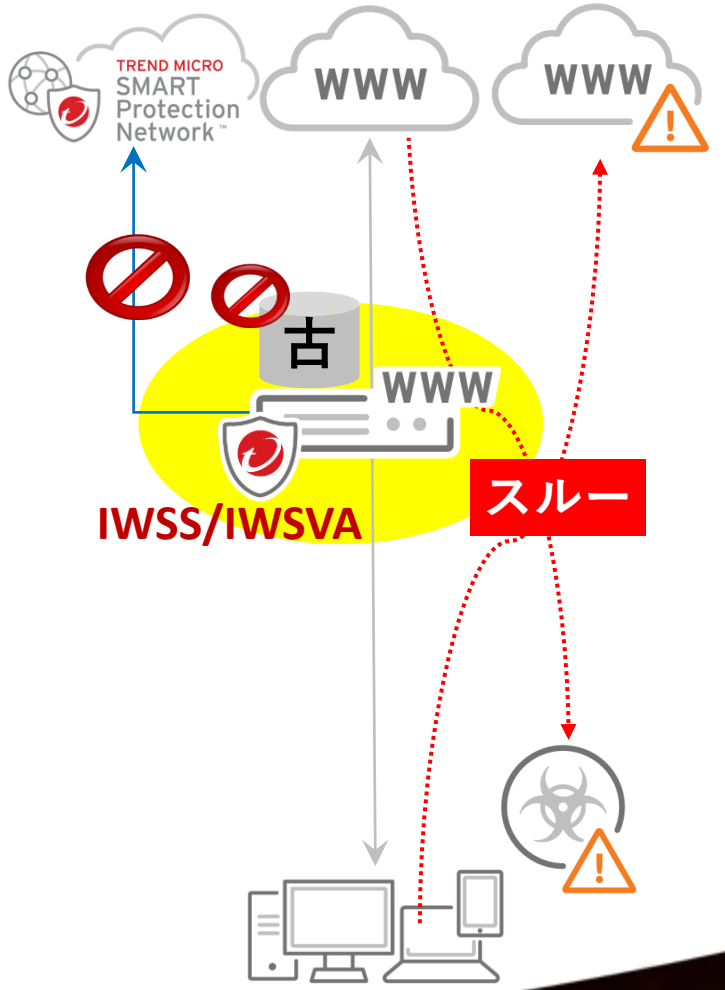
① Mail/Web共に通信や配送の遮断はない。

② 但し、アンチウイルス・アンチスパムなどの**パターンはダウンロードできないため、最新の検知が不可**

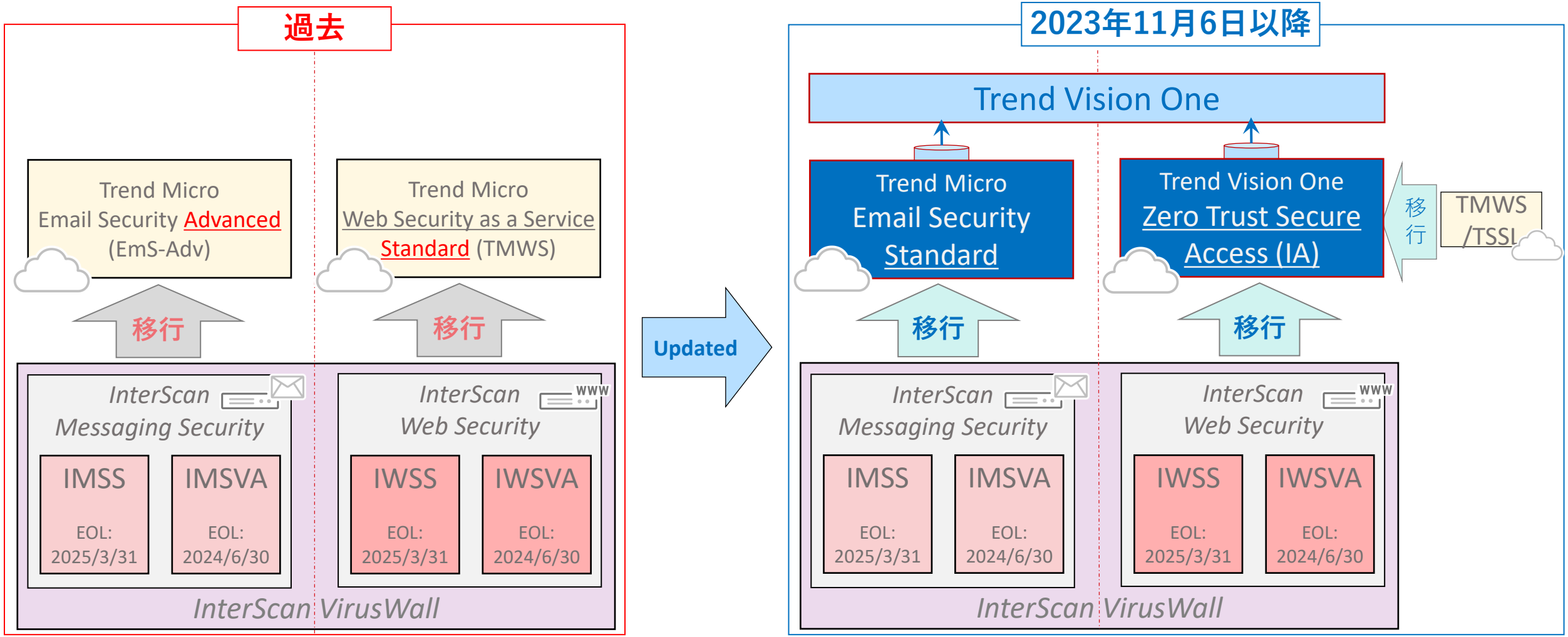
③ また、WRS/ERS/FRSなど**弊社クラウド(SPN)への接続も今後随時停止され、同技術による検査が不可となる場合もございます。**

セキュリティ対策が効かず、通信・配送の間にInterScanが入っている意味が全くありません

サポート終了後は、いかなる障害その他が発生しても、弊社では一切ご対応出来ません



InterScanから推奨移行先のご案内 （Trend Vision Oneでの統合管理へ向けて）



SaaSセキュリティに
移行するメリットとは？

GatewayセキュリティをSaaS化するお客様のメリット

	メールセキュリティSaaS: EmS-std	WebセキュリティSaaS: ZTSA-IA
共通	①より高いセキュリティ検知力 ②運用管理に伴なう手間と費用の削減 ③簡単な利用開始と初期費用の削減	
個別	④社内ネットワーク帯域の有効活用	⑤ ZTNA(Zero Trust Network Access)による動的アクセス制御（認可）の利用
セキュリティプラットフォーム Trend Vision Oneとの連携（XDR/ASRMの活用）		

弊社メールセキュリティ　機能一覧

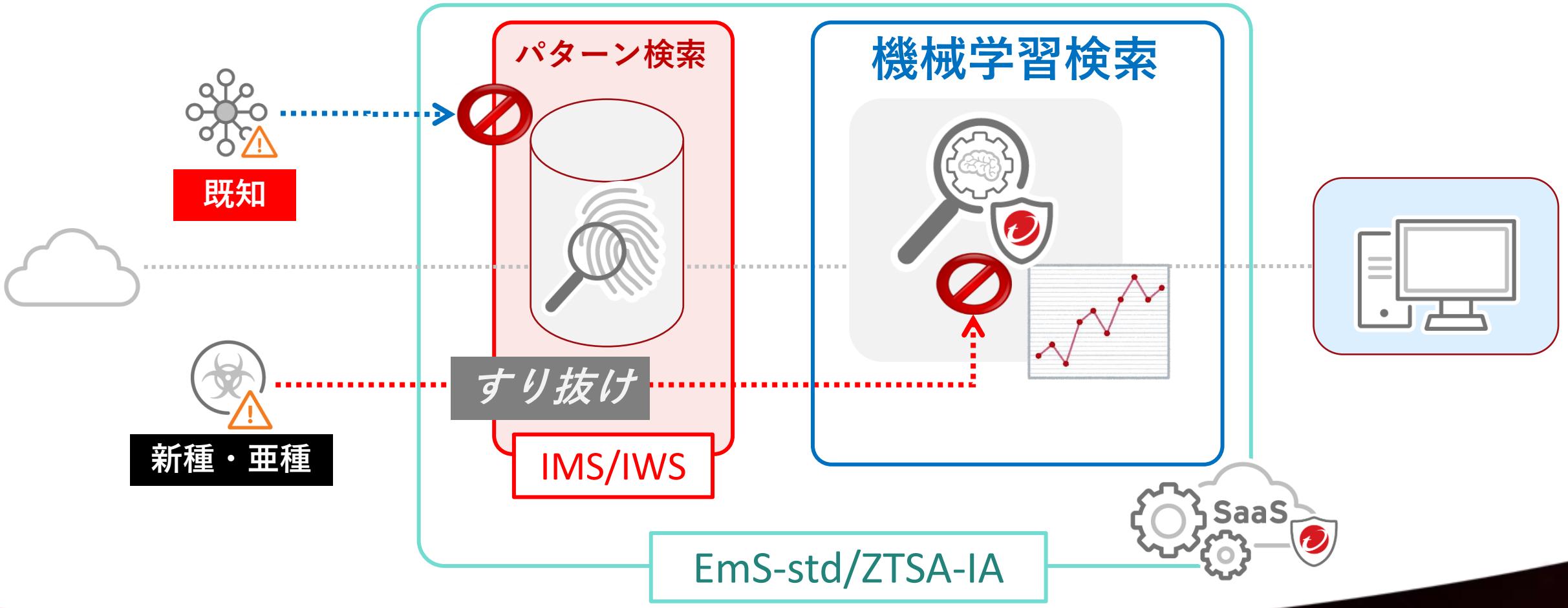
分類	機能	IMS	EmS-std	EmS-adv
送信者の真正性	送信者認証：SPF, DKIM, DMARC	○	○	○
	メール付帯情報(メールヘッダーなど）のなりすましメール検査	○	○	○
	EUQログイン情報としてAzure AD/OpenLDAPによる正当な受信者の判断	×	○	○
迷惑メール(SPAM)対策	IPレピュテーションによる不正な送信者対策	○	○	○
	ヒューリスティックを含む迷惑メールフィルタ対策	○	○	○
	マーケティングなどグレーメール分類	○	○	○
マルウェア対策	パターン検索による既知の脅威対策	○	○	○
	機械学習型検索による未知の脅威対策	×	○	○
	サンドボックスによる未知の脅威への動的解析	×	×	○
不正URL対策	Webレピュテーションによるフィッシングなど不正なURL対策	○	○	○
	Time-of-Click プロテクション	○	○	○
	添付ファイル内のURLの検索	×(SS)	○	○
	クラウドサンドボックスによるURLの検査	×	×	○
コンテンツフィルタ	実ファイルタイプによるポリシーの適用	○	○	○
	拡張子によるポリシーの適用	○	○	○
コンプライアンス	日本語テンプレート含む情報漏えい対策	○	○	○
運用	ファイルパスワード解析機能	×	×	○
	不達メール管理：メールサーバ障害時の最大10日分のメール業務継続	×	×	○
	監査ログ	○	○	○
	ログ検索のためのスライディングウィンドウ	-	30日間	60日間
	メッセージサイズ上限	10MB	50MB	150MB
Trend Vision One 連携（XDR/ASRM）		×	○	○

弊社Webセキュリティ　機能一覧

分類	機能	IWS	ZTSA-IA		TMWS-std
セキュリティ対策機能	マルウェア・ボットネット対策	○	○		○
	Webレピュテーション	○	○		○
	AI機械学習検索	×	○		○
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	○	○		○
	クラウドテナント制御	×	○		△(6件まで)
	情報漏えい対策	○	○		×
ゼロトラスト・ネットワークアクセス	デバイスポスチャによる認可	×	○		×
	リスク制御	×	○		×
	プライベートアクセス機能	×	○		×
オンプレミスゲートウェイ	オンプレゲートウェイ環境	VMware ESXi / Hyper-V	VMware ESXi / Hyper-V / AWS / Azure		VMware ESXi
	トポロジ	Forward/Revers Proxy/ICAP/Bridge/WCCP	Forward Proxy/ICAP		Forward Proxy
認証	オンプレディレクトリ	AD / ADFS / Open LDAP / 独自	AD / OpneLDAP		AD / ADFS
	クラウドディレクトリ	×	AzureAD / OKTA		AzureAD / OKTA /Google
運用	監査ログ	○	○		○
	ログ保管期間	---	180日		180日
	PACファイル管理	○	○		○
	クライアントエージェント	---	Windows/mac/iOS, iPadOS/Android		Windows/mac/iOS, iPadOS/Android
Trend Vision One 連携（XDR/ASRM）		×	○		×

①より高いSaaSセキュリティの検知力

- InterScanではすり抜けてしまう「新種・亜種の不正プログラム」も、SaaS製品に搭載されたAI機械学習により検知範囲が広がり、リスクを軽減します。



②運用管理に伴なう手間と費用の削減

バージョンアップやパッチなどの変更管理

随時サイジングの手間と故障への対応

冗長化要

オンプレミス

- データ
- アプリケーション
- OS
- 仮想化
- サーバ
- ストレージ
- ネットワーク

お客様メンテ管理対象

SaaS

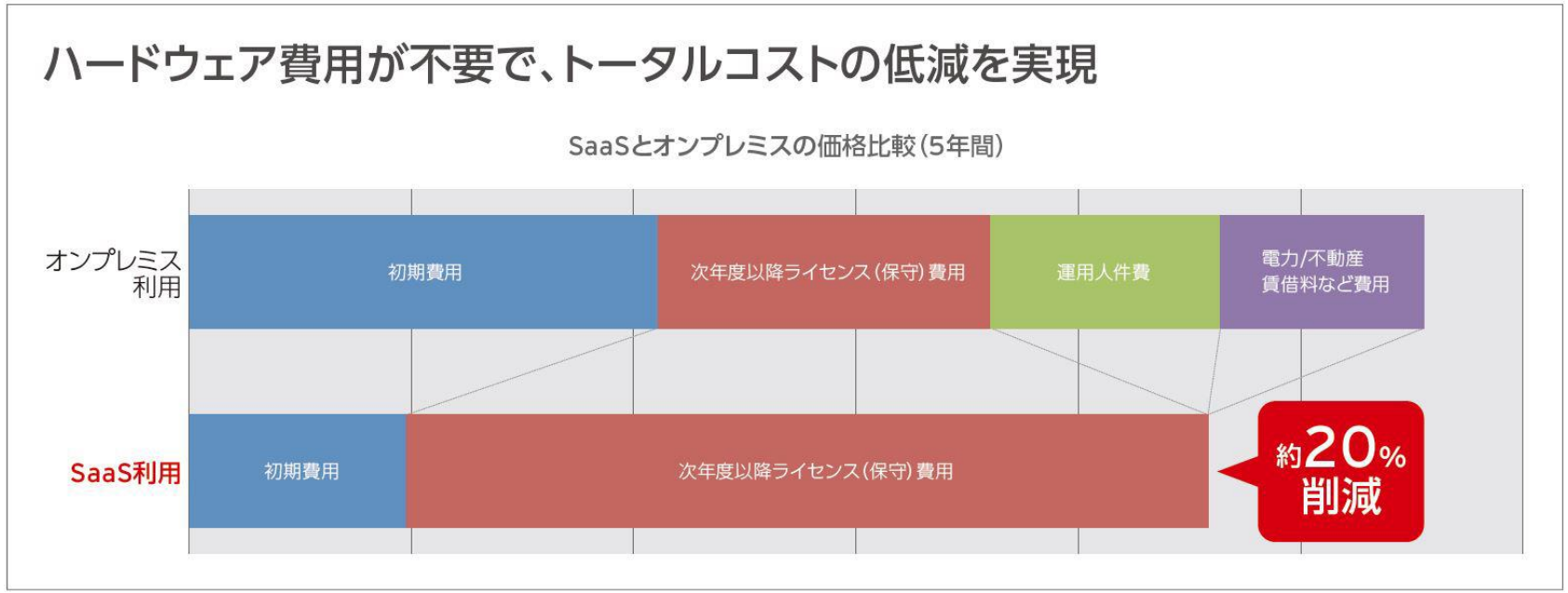
- データ
- アプリケーション
- OS
- 仮想化
- サーバ
- ストレージ
- ネットワーク

メンテ不要
トレンドマイクロの対応範囲

冗長化済

③クラウド活用によるコストの最適化

- SaaSはライセンス費用が上がる？！⇒いえいえ、**コストの比較はTCO**で。
- SaaSの利用により「サーバー・ストレージのHW費用」「パッチなど変更管理の人件費」「電力・不動産など諸費用」が不要です。
- バージョン毎のサポート終了がSaaSは無いため、「バージョンアップに関わる費用」が不要で、「継続してご利用」頂けます。

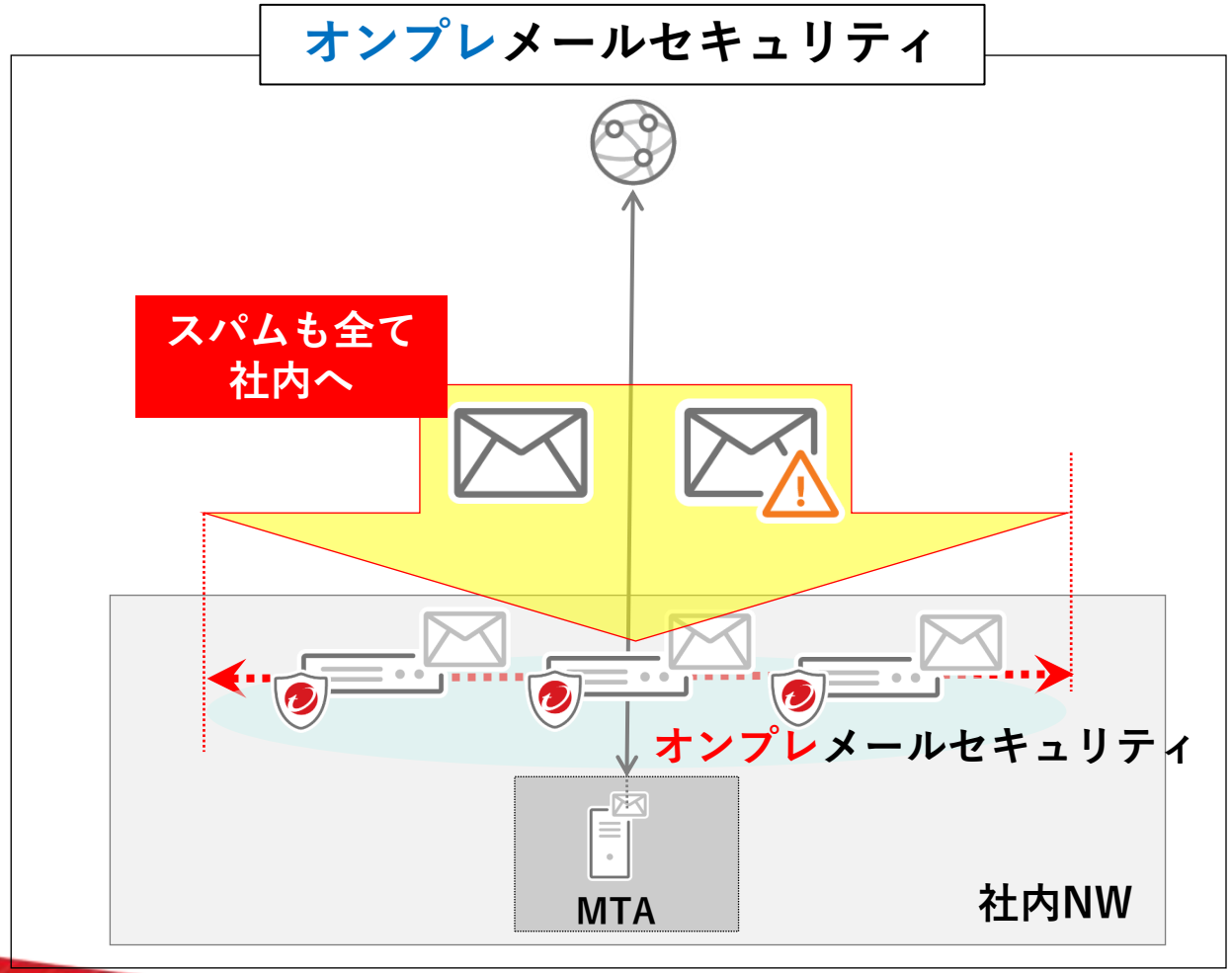


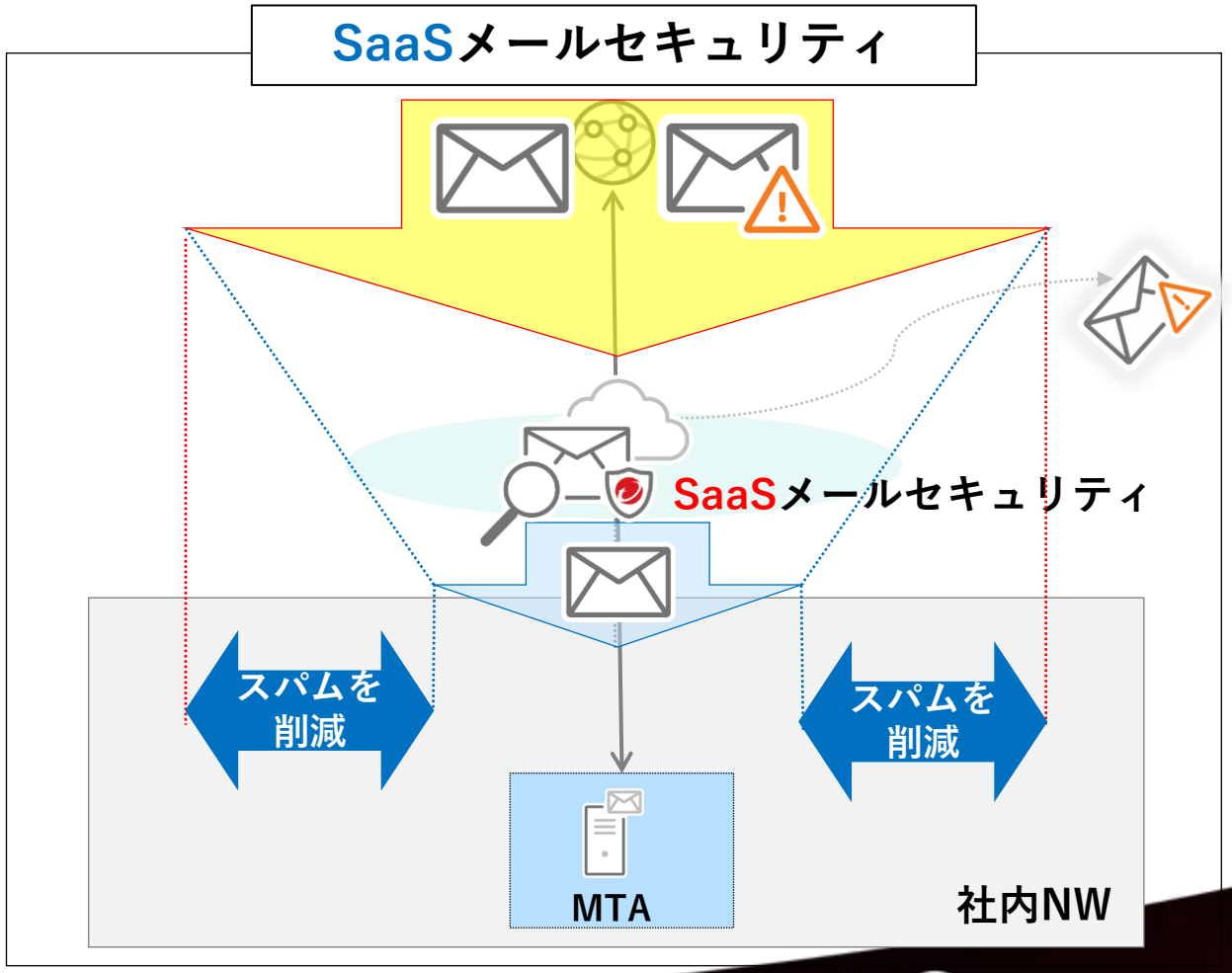
https://www.trendmicro.com/ja_jp/business/campaigns/on-premises-gateway-products-migration-guide/saas-price-compare.html

④メール個別：社内ネットワーク帯域の有効活用

✓ SaaSではメール流量全体の半分(*)と言われる**スパムを前段のクラウドで排除し、社内ネットワーク帯域の無駄な流量を軽減**

https://www.soumu.go.jp/main_content/000693529.pdf





総務省：電気通信事業者１０社の全受信メール数と迷惑メール数の割合（2021年8月時点）

⑤Web個別：ゼロトラスト（動的アクセス制御）の実装

←弱　NIST SP 800-207準拠＝セキュリティ強度　→強

IAMとのSSO連携による
ユーザを認証

Azure AD
okta
ADFS

Trend Micro vision one

アカウント
パスワード
MFA

正しいユーザ？

認証されたユーザの**アクセスを認可**

接続する
時間帯？

どこから
アクセス？

アクセス先
のアプリ？

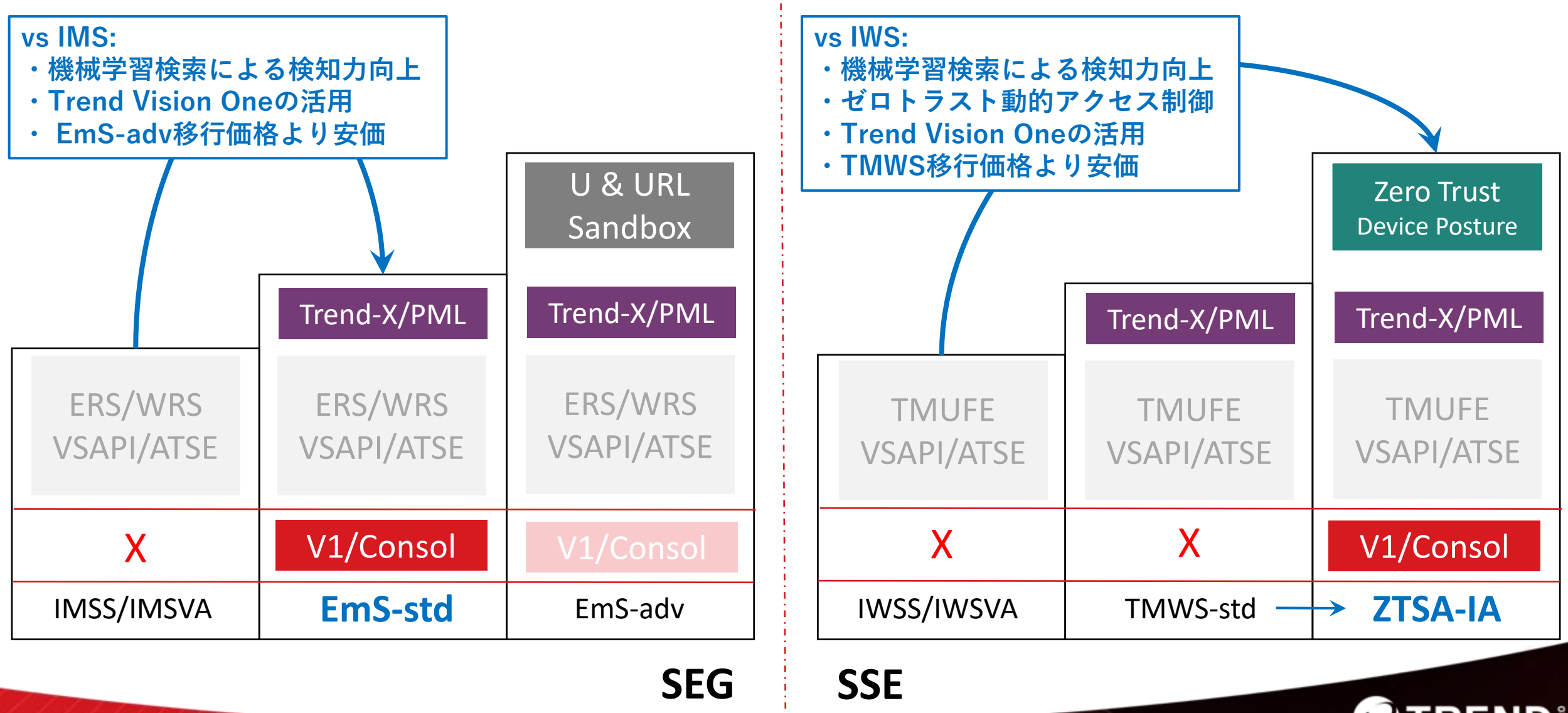
条件を満たす
デバイス

XDRと他評価を元にリスクスコアで判断

接続許可

アカウント
ロック

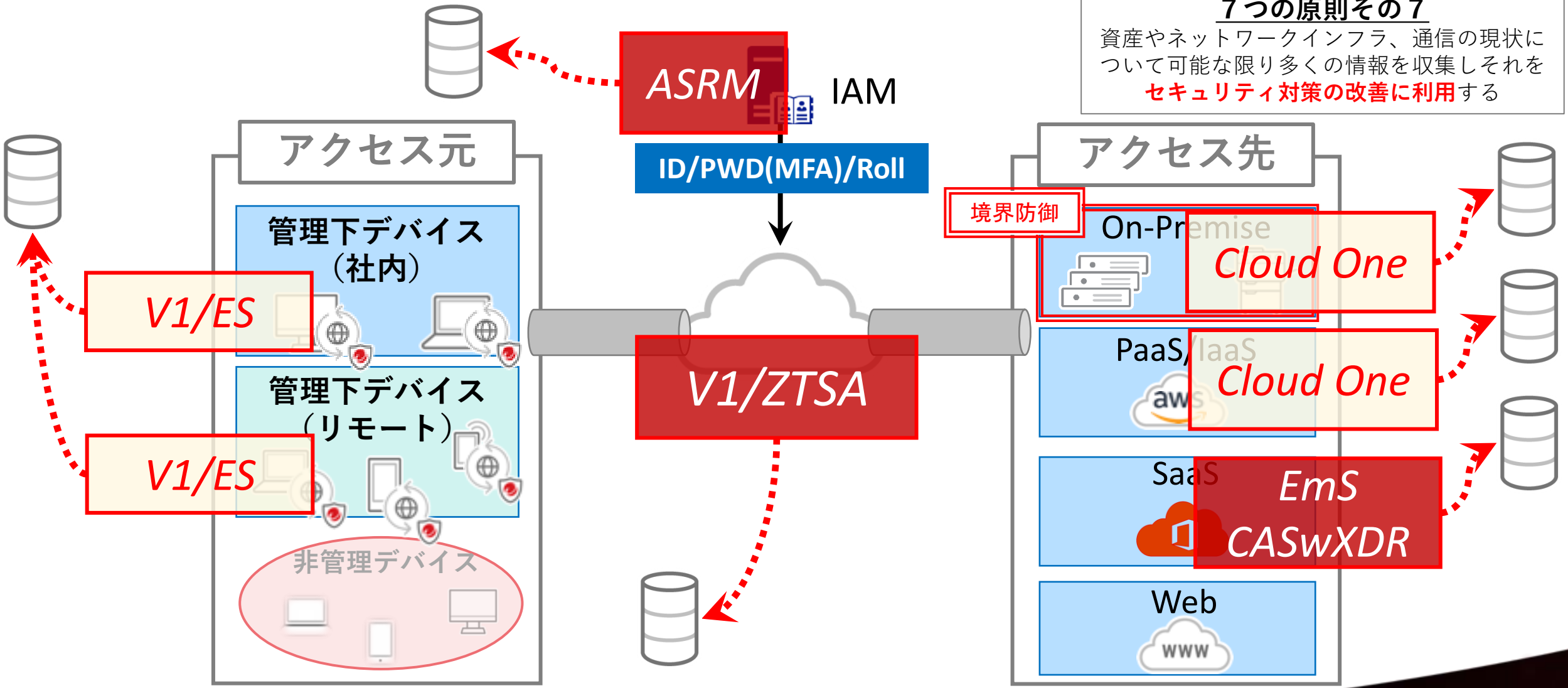
InterScan vs SaaS 移行の機能差異とメリット



Trend vision One 連携のメリット

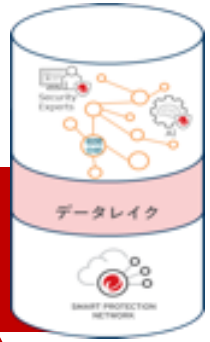
テレメトリのTrend Vision Oneへの連携

7つの原則その7
資産やネットワークインフラ、通信の現状について可能な限り多くの情報を収集しそれを**セキュリティ対策の改善に利用**する

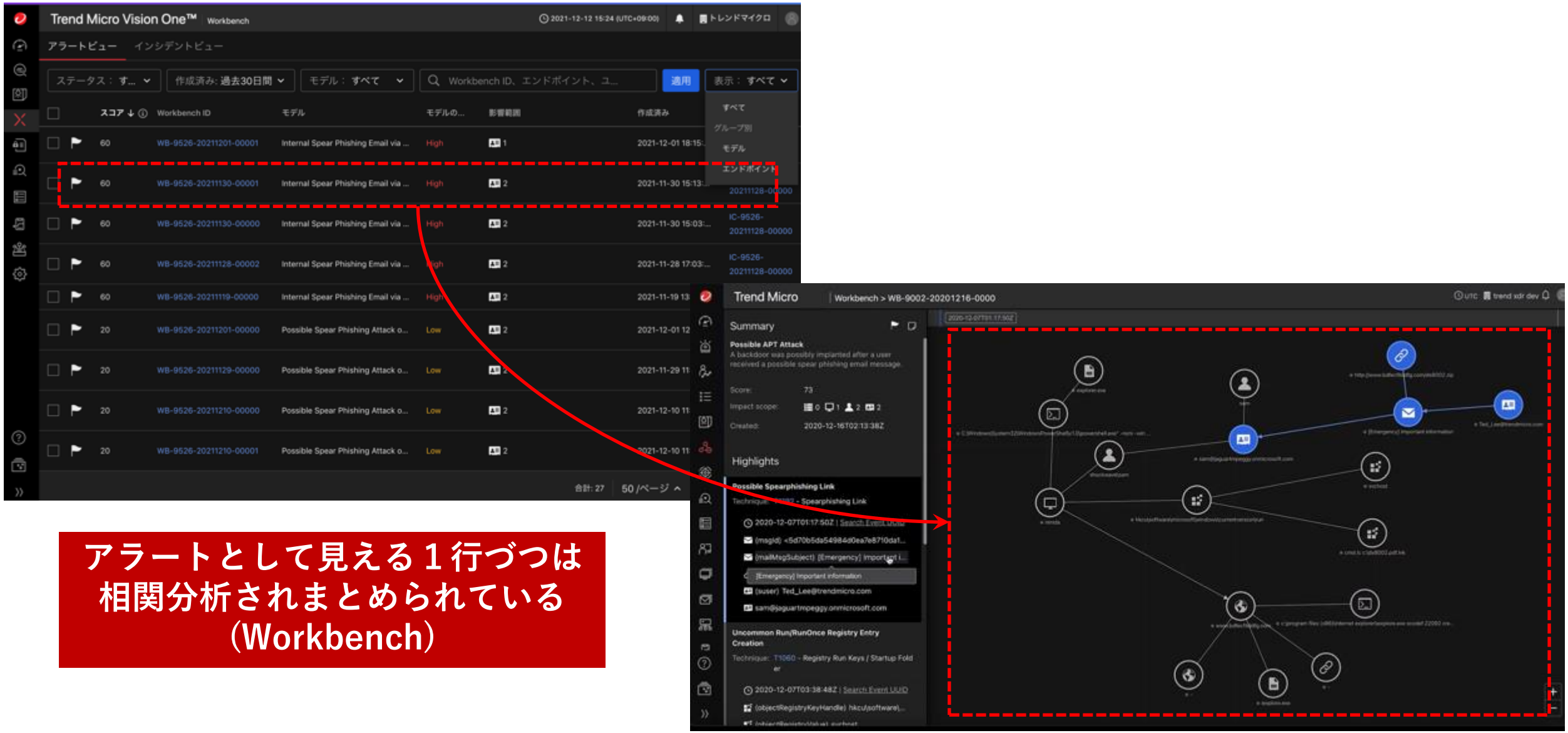


SIEM (Security Information and Event Management)

より少なく、より明確なアラートを攻撃の流れと共に



相関分析（一連の1つの攻撃）



アラートとして見える１行づつは相関分析されまとめられている（Workbench）

相関分析から「リスク指標の表示」へ

EmS/CAS

V1/ES

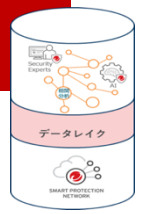
C1

ZTSA

IdP
IAM

テレメトリ

高度な相関分析



Attach Surface Risk Management（ASRM）

予防対応へ

SaaSへの移行を支援する特別プログラム

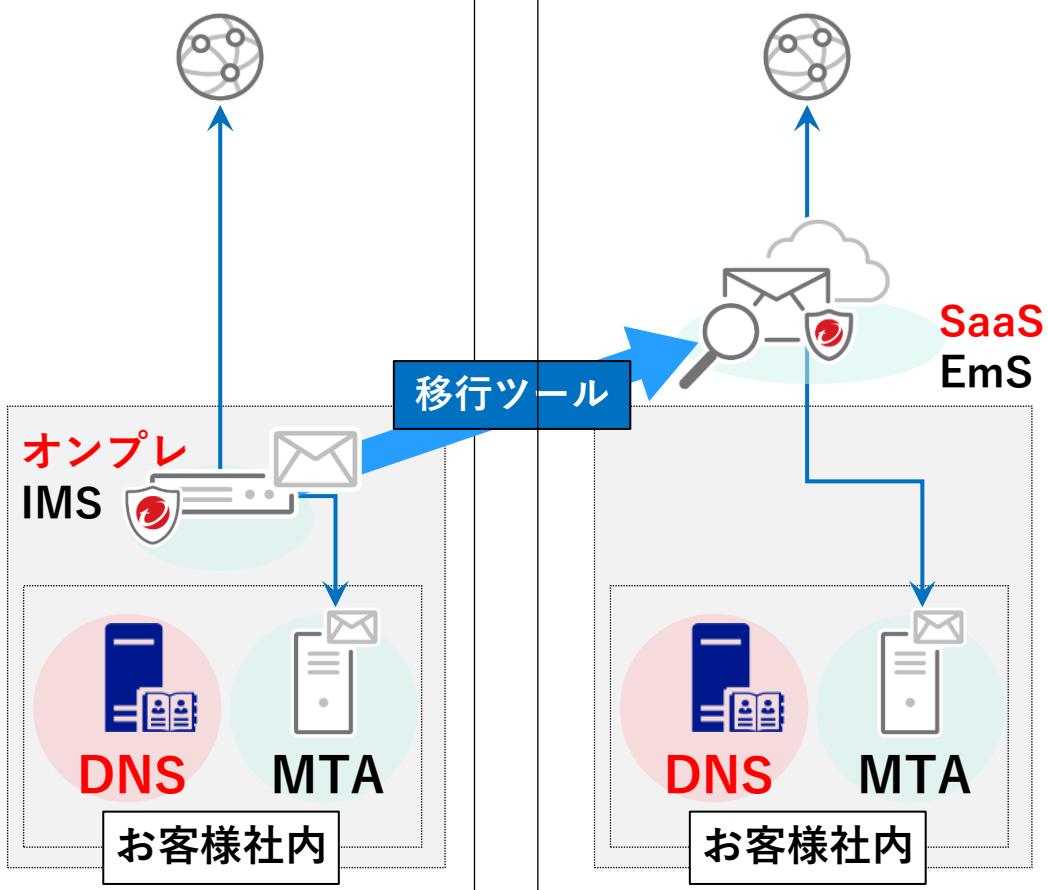
メール：IMS→EmS 移行ツールのご案内

✓ 詳細な「**EmS　InterScan MSS/IMSVA移行ガイド**」をご用意しております。

【対象製品・バージョン】
・InterScan Messaging Security Suite 9.1 Linux版
→ 9.1.0.1361以降のビルド

・InterScan Messaging Security Virtual Appliance 9.1
→ 9.1.0.2011以降のビルド

*移行ツールを用いて、TMEmSへ設定情報を移行するには、上記製品・バージョンに対して、特定のHotfixを適用する必要があります。
こちらのHotfixに関しては、Download Centerに公開しておりませんので、
弊社サポート窓口までお問い合わせをお願いいたします。



＊本移行ツールでは、**IMSS/IMSVAの全ての設定を移行することはできません。**

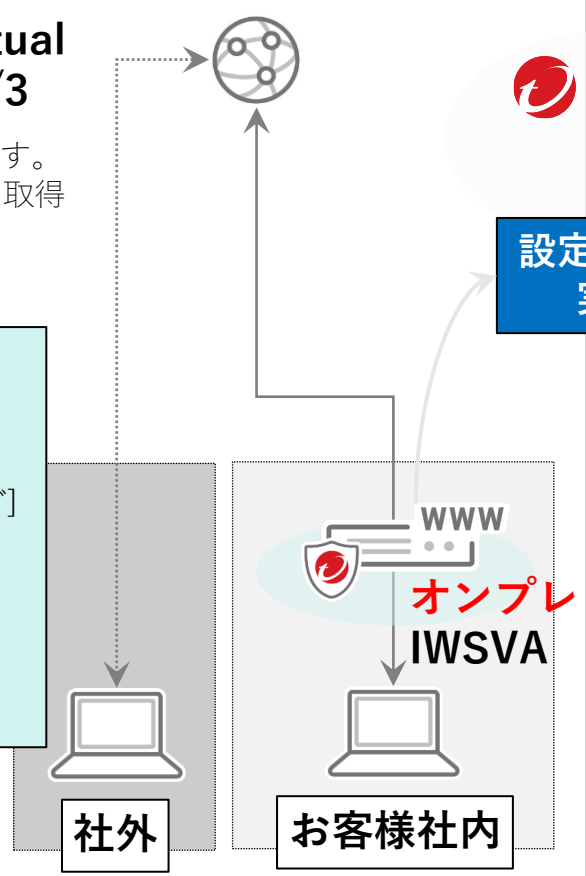
Web：IWSVA→ZTSA-IA 移行支援のご案内

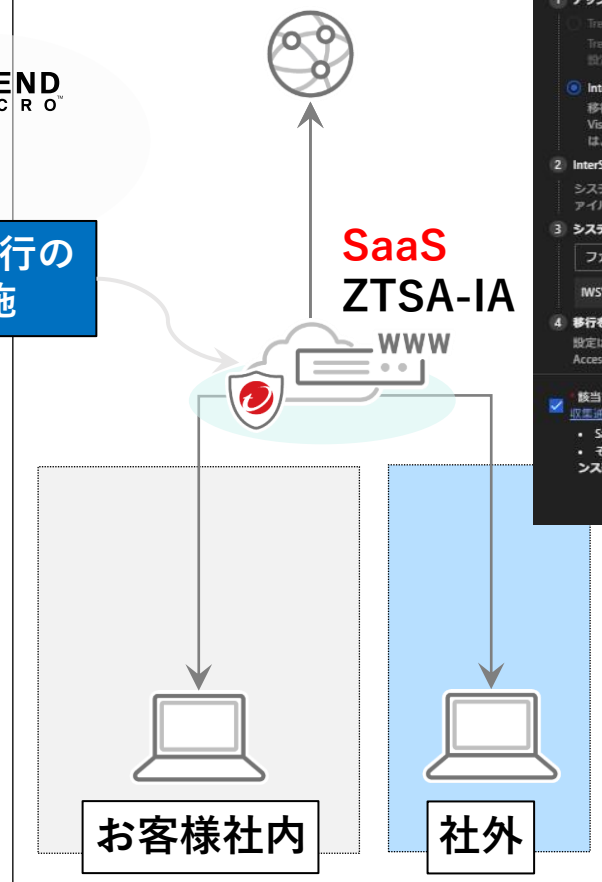
【対象製品・バージョン】
・InterScan Web Security Virtual Appliance 6.5 Service Pack 2/3

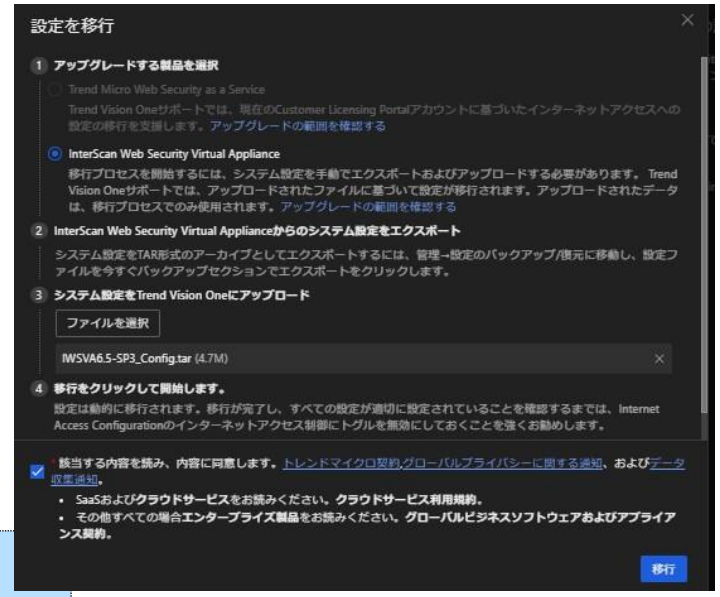
移行ツールの実行は以下の手順で実施します。
1) IWSVAの設定バックアップファイルの取得
2) 移行ツールの実行

IWSVAから移行可能な項目

1.[アプリケーション制御] > [ポリシー]
2.[HTTP] > [HTTPS復号化] > [ポリシー]
3.[HTTP] > [HTTPS復号化] > [トンネリング]
4.[HTTP] > [高度な脅威保護] > [ポリシー]
5.[HTTP] > [URLフィルタ] > [ポリシー]
6.[HTTP] > [URLアクセス設定]
7.[HTTP] > [設定] > [除外リスト]
8.[HTTP] > [設定] > [カスタムカテゴリ]
9.[HTTP] > [設定] > [デジタル証明書]





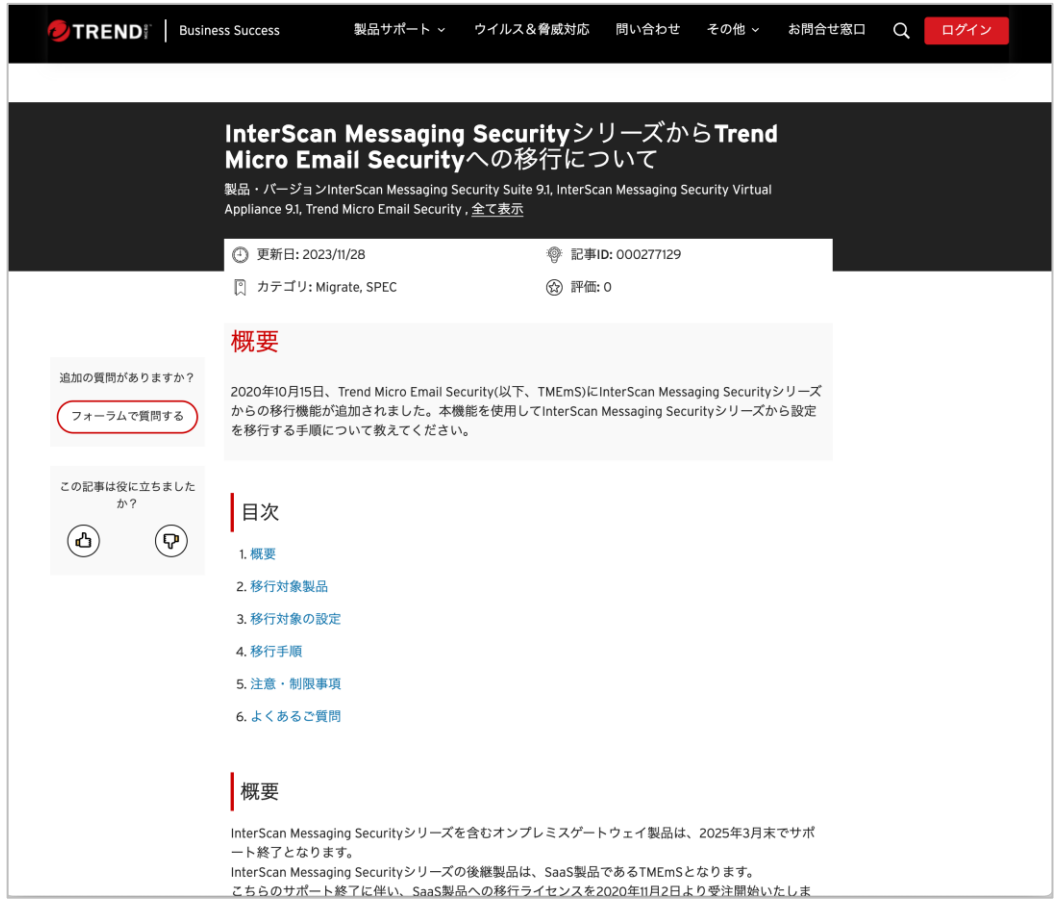


＊本移行ツールでは、**IWSVAの全ての設定を移行することはできません。**

移行手順についてのご案内

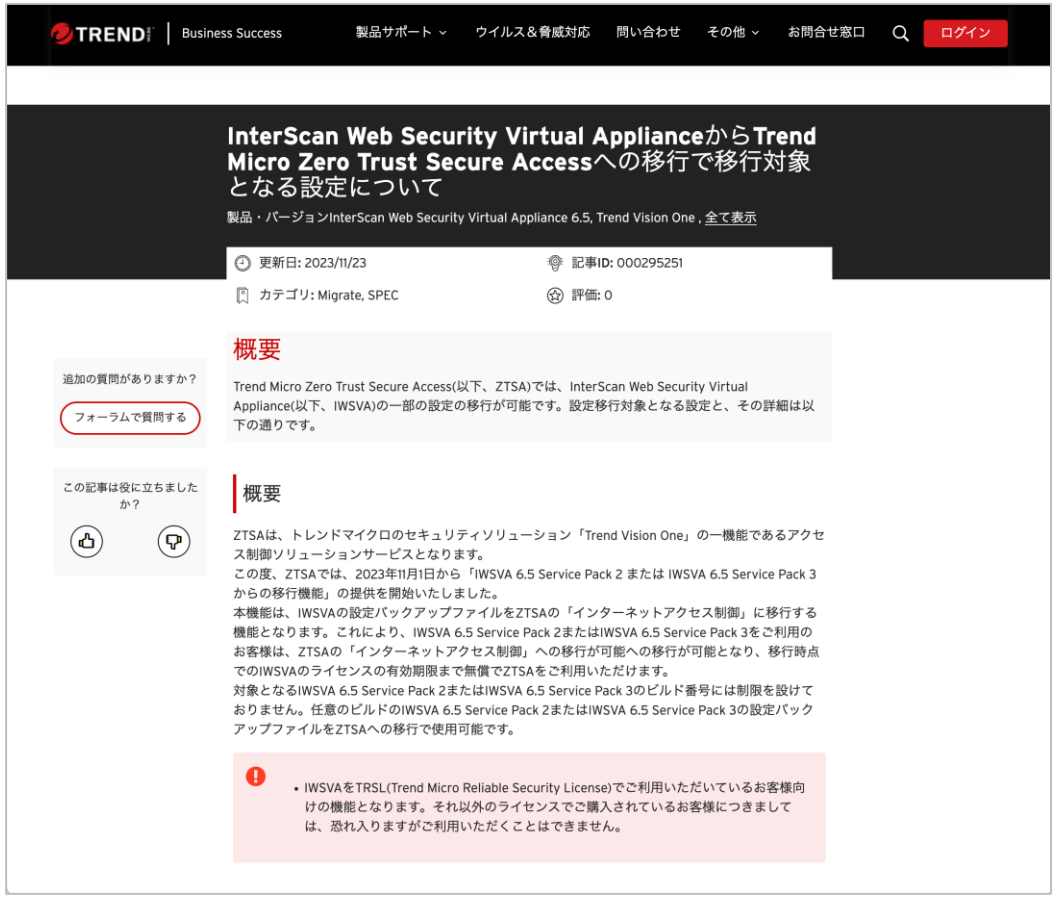
【IMSVA or IMSS からEmS】

https://success.trendmicro.com/dcx/s/solution/000277129?language=ja



【IWSVAからZTSA-IA】

https://success.trendmicro.com/dcx/s/solution/000295251?language=ja



EmS-std新規 及び ZTSA-IA新規優待（価格）

- 永年InterScanをお使いのお客様に感謝を込めて、SaaSの移行に際して特別な価格をご用意しました

TSSL(TRSL)			EmS-Std	IMS 更新	EmS-adv
			新規	更新	新規優待
A	5	24	¥3,180	¥2,520	¥3,460
B	25	49	¥2,880	¥2,460	¥3,390
C	50	99	¥2,780	¥2,420	¥3,350
D	100	249	¥2,580	¥2,190	¥3,120
E	250	499	¥2,280	¥1,750	¥2,670
F	500	999	¥1,580	¥1,200	¥2,100
G	1,000	1,999	¥980	¥773	¥1,660
H	2,000	4,999	¥630	¥449	¥1,330
I	5,000	9,999	¥540	¥389	¥1,260
J	10,000	19,999	¥480	¥373	¥1,250
K	20,000	49,999	¥420	¥335	¥1,210
L	50,000		¥380	¥314	¥1,190

SEG

TSSL(TRSL)			ZTSA-IA		IWS	TMWSstd
			新規	新規優待	更新	新規優待
A	5	499	¥5,710	¥3,200	¥1,980	¥3,410
			¥5,710		¥1,950	¥3,390
			¥5,710		¥1,920	¥3,350
			¥5,710		¥1,760	¥3,200
			¥5,710		¥1,380	¥2,790
B	500	999	¥4,220	¥2,280	¥967	¥2,390
C	1,000	1,999	¥3,550	¥1,680	¥621	¥2,040
D	2,000	4,999	¥3,220	¥1,380	¥341	¥1,720
E	5,000	9,999	¥2,950	¥1,280	¥314	¥1,710
F	10,000	24,999	¥2,690	¥1,200	¥297	¥1,690
G	25,000		¥2,320	¥1,150	¥260	¥1,640
					¥243	¥1,620

SSE

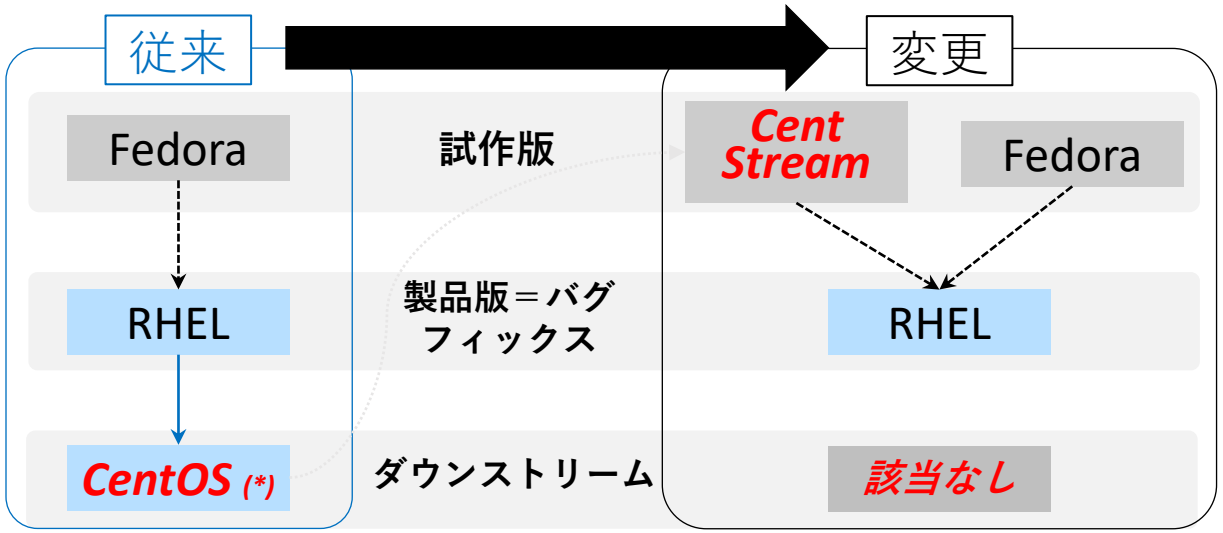

TREND
MICRO

Appendix

仮想アプライアンス版の終了は何故早まったのか？

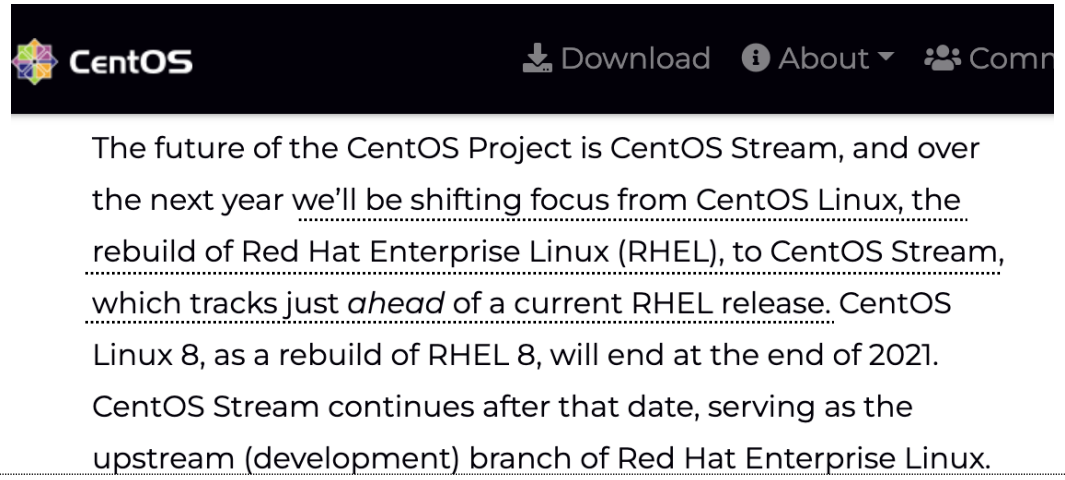
RH社によるCentOSの位置付け変更とサポート終了

- 従来のCentOSは、バグ修正された製品版のRedHat Enterprise Linux(RHEL)のダウンストリームだったが、Fedoraと同様に今後はRHELのアップストリーム版(Cent Stream)に変更
- バグが収束されていないアップストリーム版を製品に組み込んでお客様に提供はできない為、Red Hat社の定める従来のCent OS終了日24年6月末が＝InterScan仮想アプライアンスのご提供可能な最長サポート期間にせざろう得ません

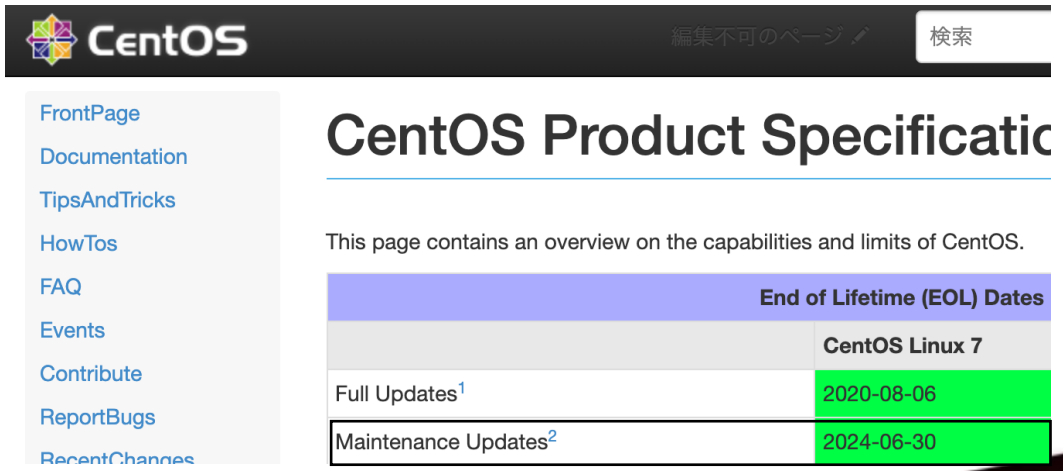


(*)弊社InterScan仮想アプライアンスに採用

https://blog.centos.org/2020/12/future-is-centos-stream/



https://wiki.centos.org/About/Product



Appendix

Remind: 仮想アプライアンスとソフトウェア

- 前ページの通り、仮想アプライアンスに包含されているCentOSのサポート終了により、当初よりも前倒しした「24年６月末（＝Red Hat社指定）」でのサポート終了となります

	仮想アプライアンス（EOL=24年6月）	ソフトウェア（EOL=25年３月）
メール	IMSVA Cent OS（Library） （トレンドマイクロ提供） Virtual machine Server（HW） （お客様ご自身手配）	IMSS （トレンドマイクロ提供） Redhat Linux Virtual machine（任意） Server（HW） （お客様ご自身手配）
Web	IWSVA Cent OS（Library） （トレンドマイクロ提供） Virtual machine Server（HW） （お客様ご自身手配）	IWSS （トレンドマイクロ提供） Redhat Linux Virtual machine（任意） Server（HW） （お客様ご自身手配）

