



## *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 6<sup>th</sup>, 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

よろしくお願ひします



- 「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 <b>Virtual Appliance</b>	InterScan Messaging Security Suite plus	InterScan Web Security <b>Virtual Appliance</b>	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	<b>2024/6/30</b>	<b>2025/3/31</b>	<b>2024/6/30</b>	<b>2025/3/31</b>
推奨移行先	<b>Trend Micro Email Security Standard (EmS-std)</b>		<b>Trend Vision One Zero Trust Secure Access- Internet Access (ZTSA-IA)</b>	
形式	SaaS (Cloud)			

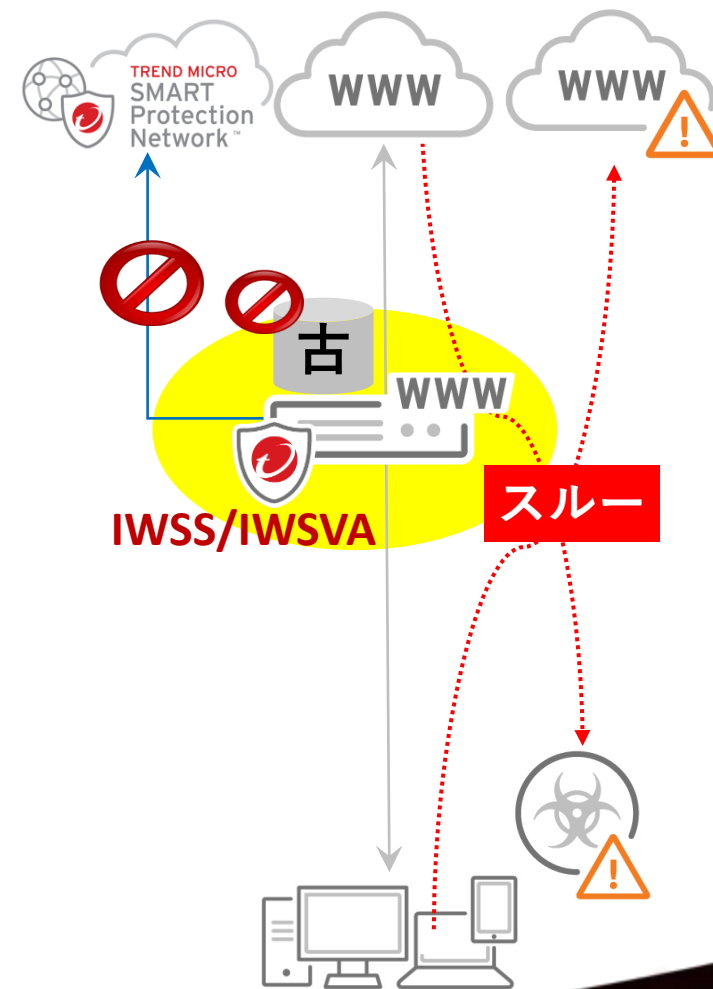
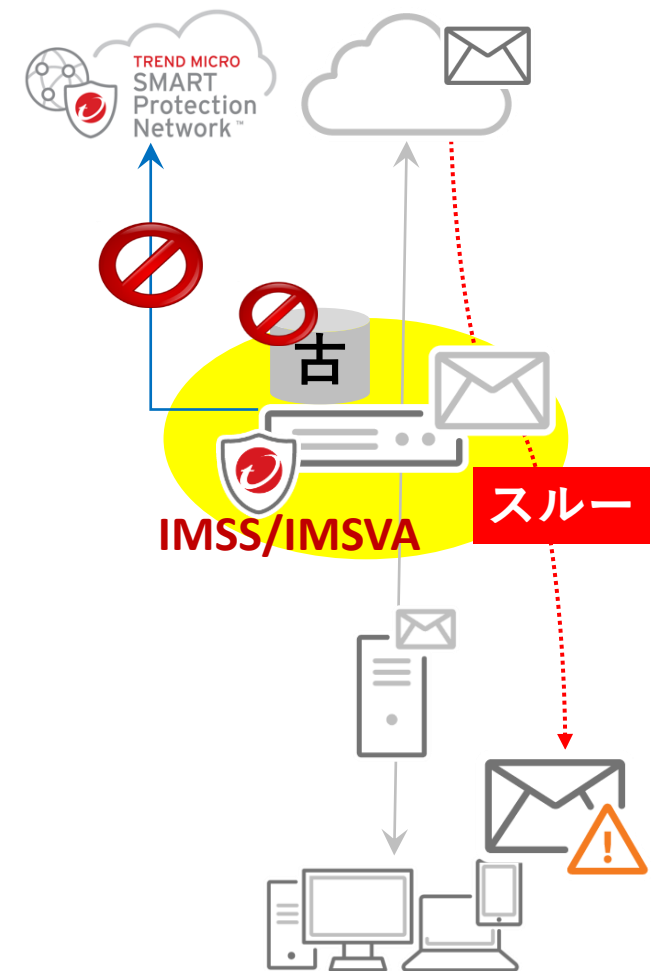
# サポート切れのInterScanを使い続けると？

## 【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

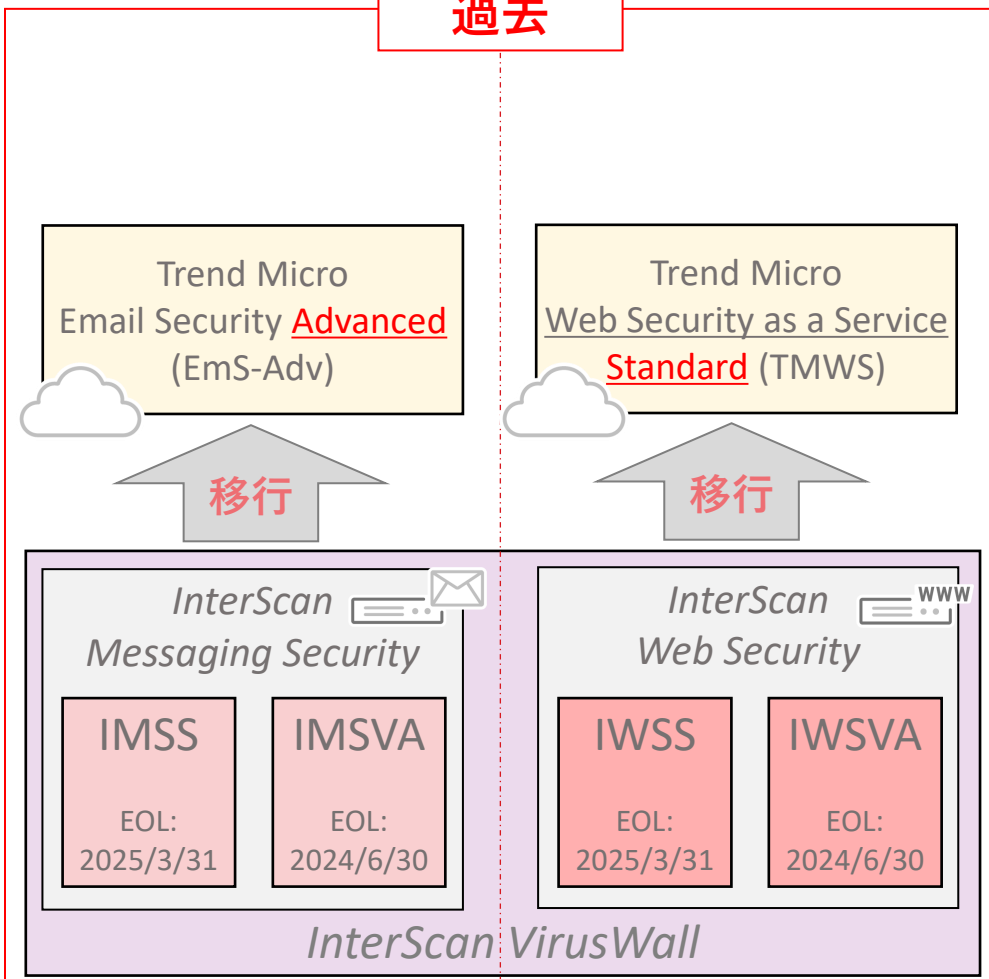
サポート終了後は、いかなる障害その他が発生しても、弊社では一切ご対応出来ません





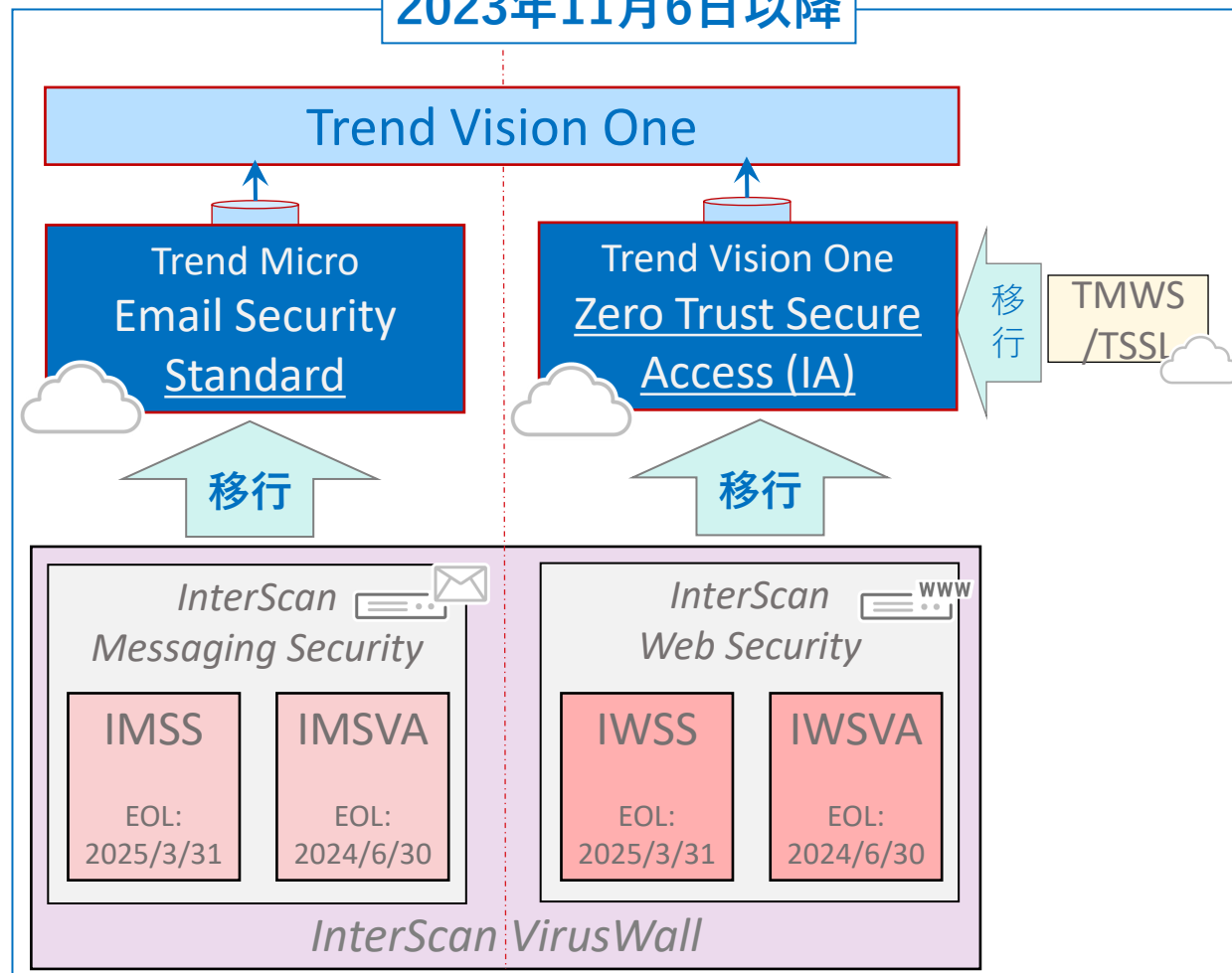
# InterScanから推奨移行先のご案内 (Trend Vision Oneでの統合管理へ向けて)

過去



Updated

2023年11月6日以降



# 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	<p>① より高いセキュリティ検知力</p> <p>② 運用管理に伴なう手間と費用の削減</p> <p>③ 簡単な利用開始と初期費用の削減</p>	
個別	<p>④ 社内ネットワーク帯域の有効活用</p>	<p>⑤ ZTNA (Zero Trust Network Access) による動的アクセス制御 (認可) の利用</p>
<p>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)</p>		



# 弊社メールセキュリティ 機能一覧

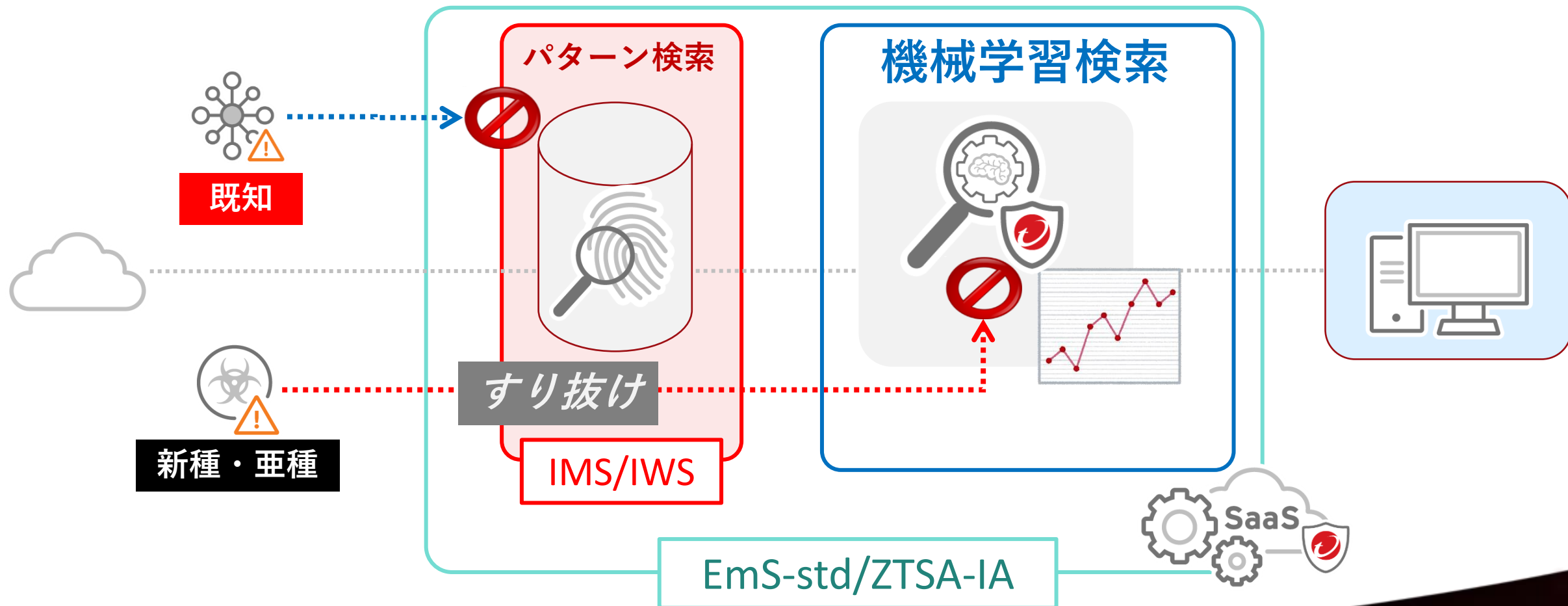
分類	機能	IMS	EmS-std	EmS-adv
送信者の真正性	送信者認証：SPF, DKIM, DMARC	○	○	○
	メール付帯情報(メールヘッダーなど) のなりすましメール検査	○	○	○
	EUQログイン情報としてAzure AD/OpenLDAPによる正当な受信者の判断	×	○	○
迷惑メール (SPAM)対策	IPレピュテーションによる不正な送信者対策	○	○	○
	ヒューリスティックを含む迷惑メールフィルタ対策	○	○	○
	マーケティングなどグレーメール分類	○	○	○
マルウェア対策	パターン検索による既知の脅威対策	○	○	○
	機械学習型検索による未知の脅威対策	×	○	○
	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
<b>Trend Vision One 連携 (XDR/ASRM)</b>		×	○	○

# 弊社Webセキュリティ 機能一覧

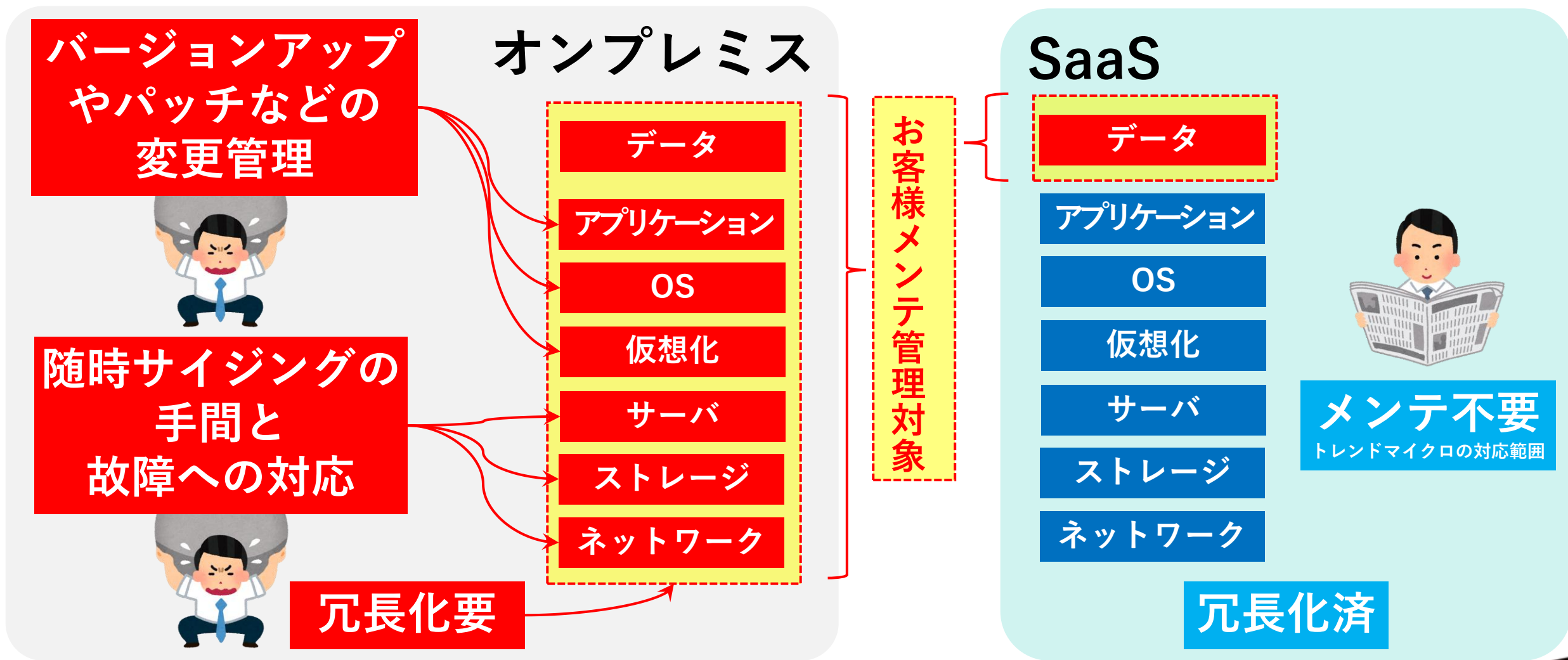
分類	機能	IWS	ZTSA-IA	TMWS-std
セキュリティ 対策機能	マルウェア・ボットネット対策	○	○	○
	Webレピュテーション	○	○	○
	AI機械学習検索	×	○	○
コンプライアンス 対策機能	URLフィルタリング機能	○	○	○
	アプリケーション制御	○	○	○
	クラウドテナント制御	×	○	△(6件まで)
	情報漏えい対策	○	○	×
ゼロトラスト・ ネットワークアクセス	デバイスポスチャによる認可	×	○	×
	リスク制御	×	○	×
	プライベートアクセス機能	×	○	×
オンプレミス ゲートウェイ	オンプレゲートウェイ環境	VMware ESXi / Hyper-V	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。

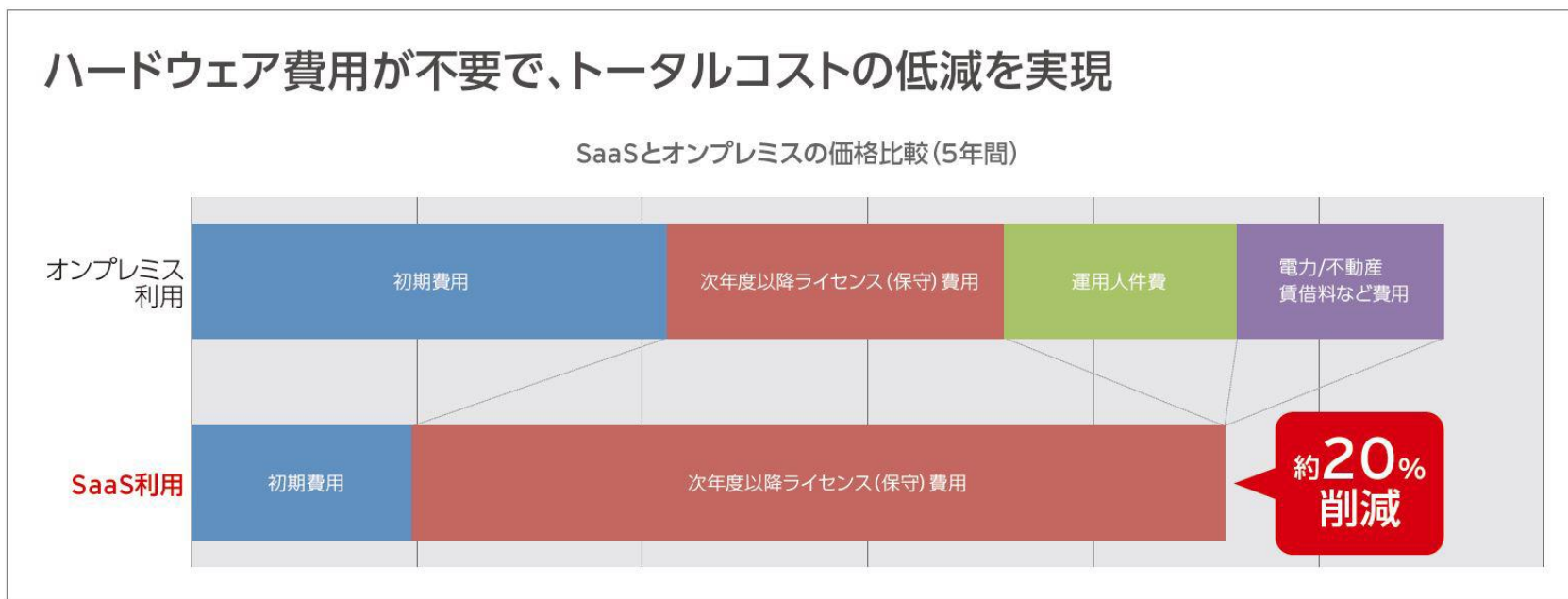


## ②運用管理に伴なう手間と費用の削減



### 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的費用」「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](https://www.trendmicro.com/ja_jp/business/campaigns/on-premises-gateway-products-migration-guide/saas-price-compare.html)

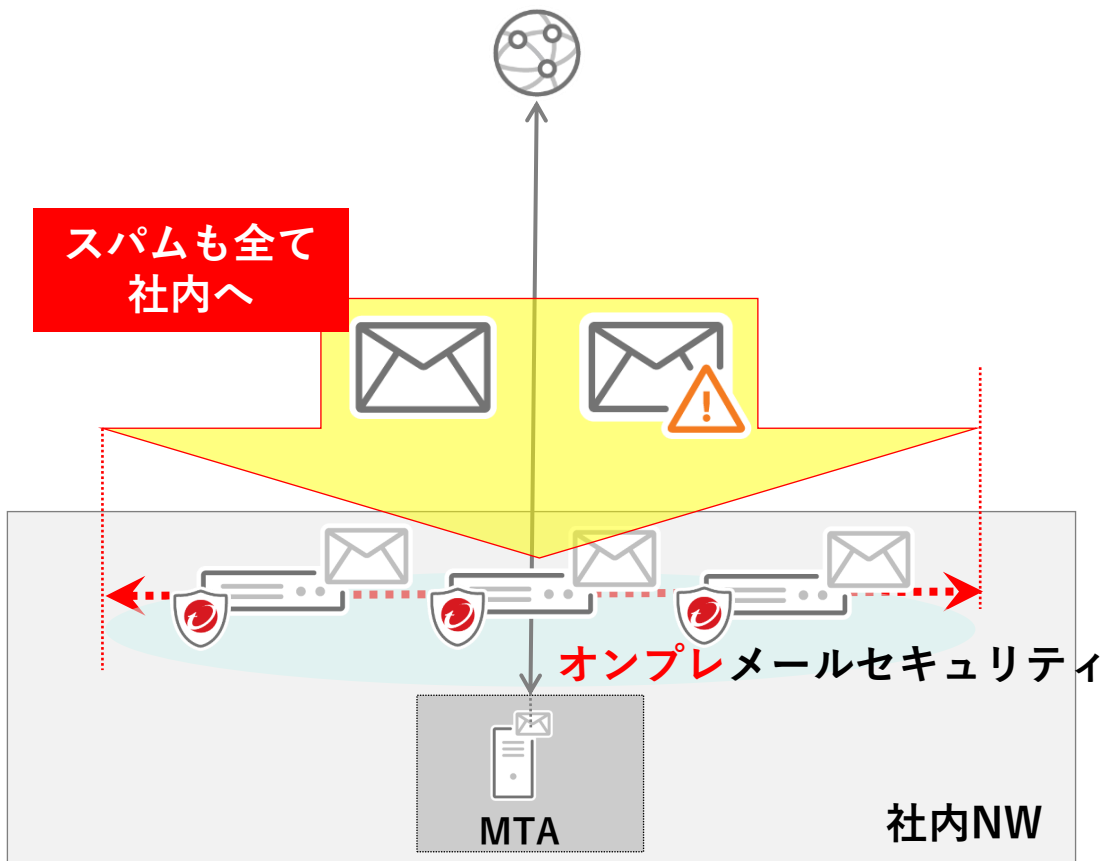


# ④メール個別：社内ネットワーク帯域の有効活用

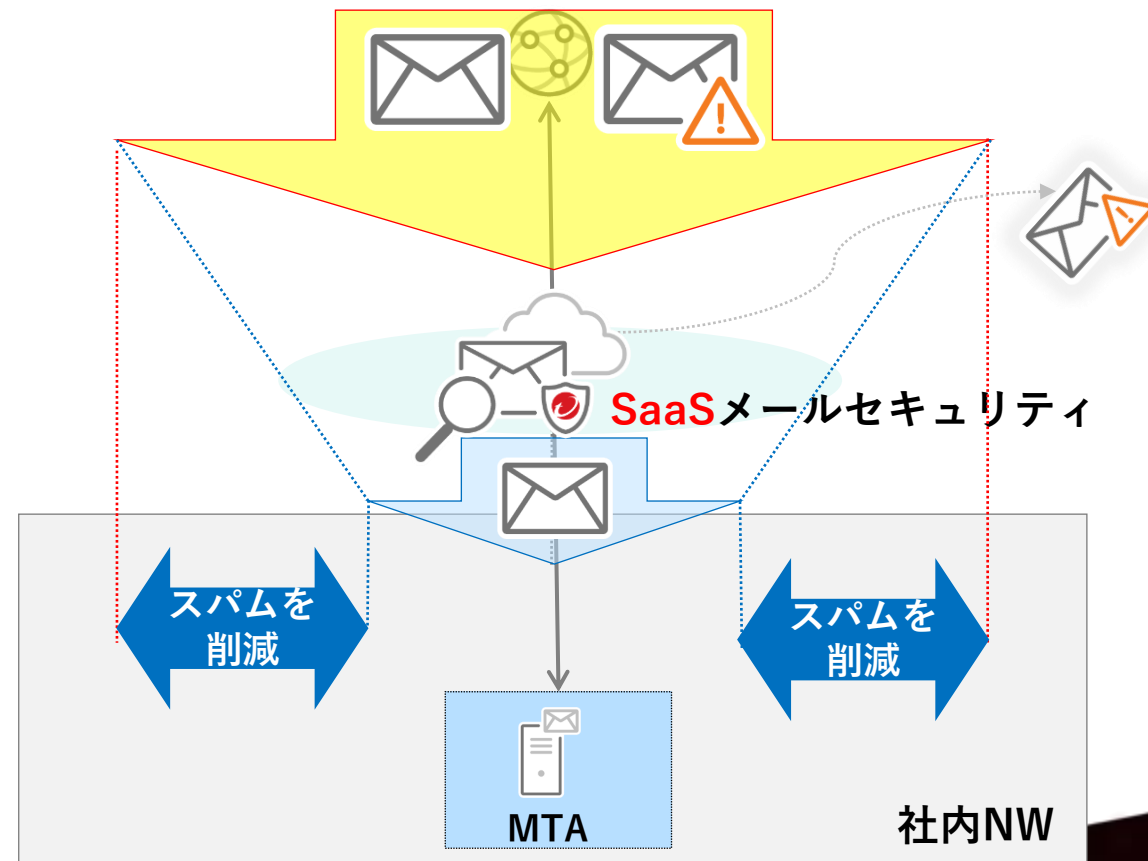
- ✓ SaaSではメール流量全体の半分(\*)と言われる スパムを前段のクラウドで排除し、社内ネットワーク帯域の無駄な流量を軽減

[https://www.soumu.go.jp/main\\_content/000693529.pdf](https://www.soumu.go.jp/main_content/000693529.pdf)

## オンプレメールセキュリティ



## SaaSメールセキュリティ



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）

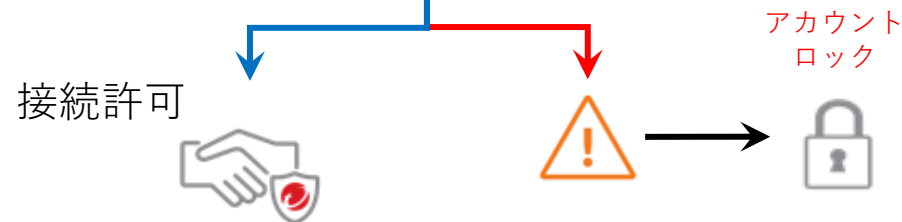
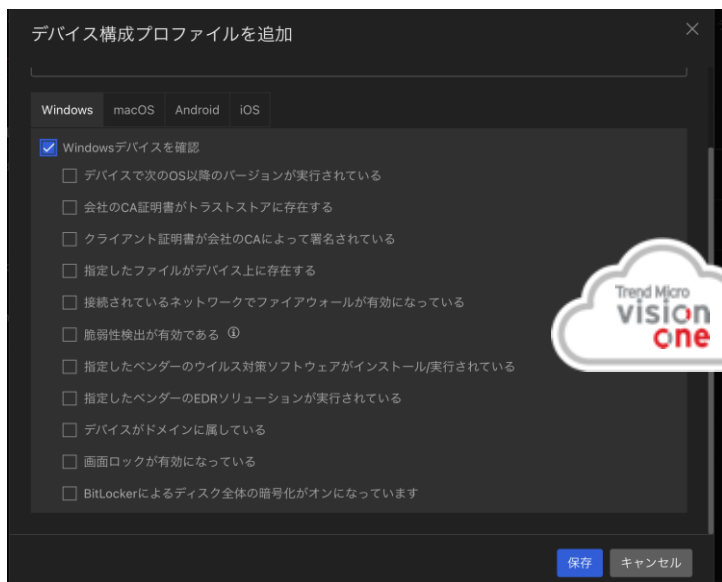
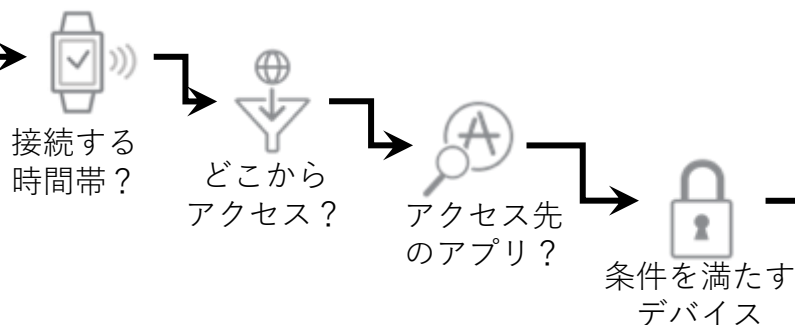
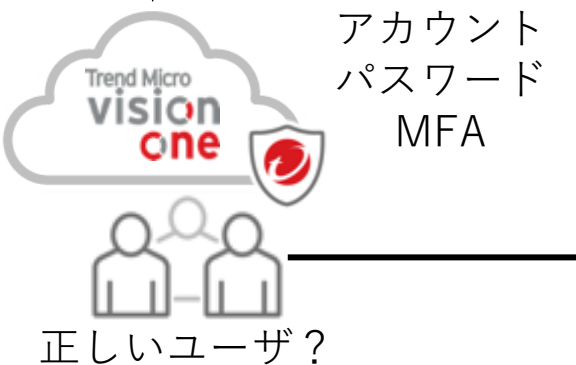
# ⑤ Web個別：ゼロトラスト（動的アクセス制御）の実装



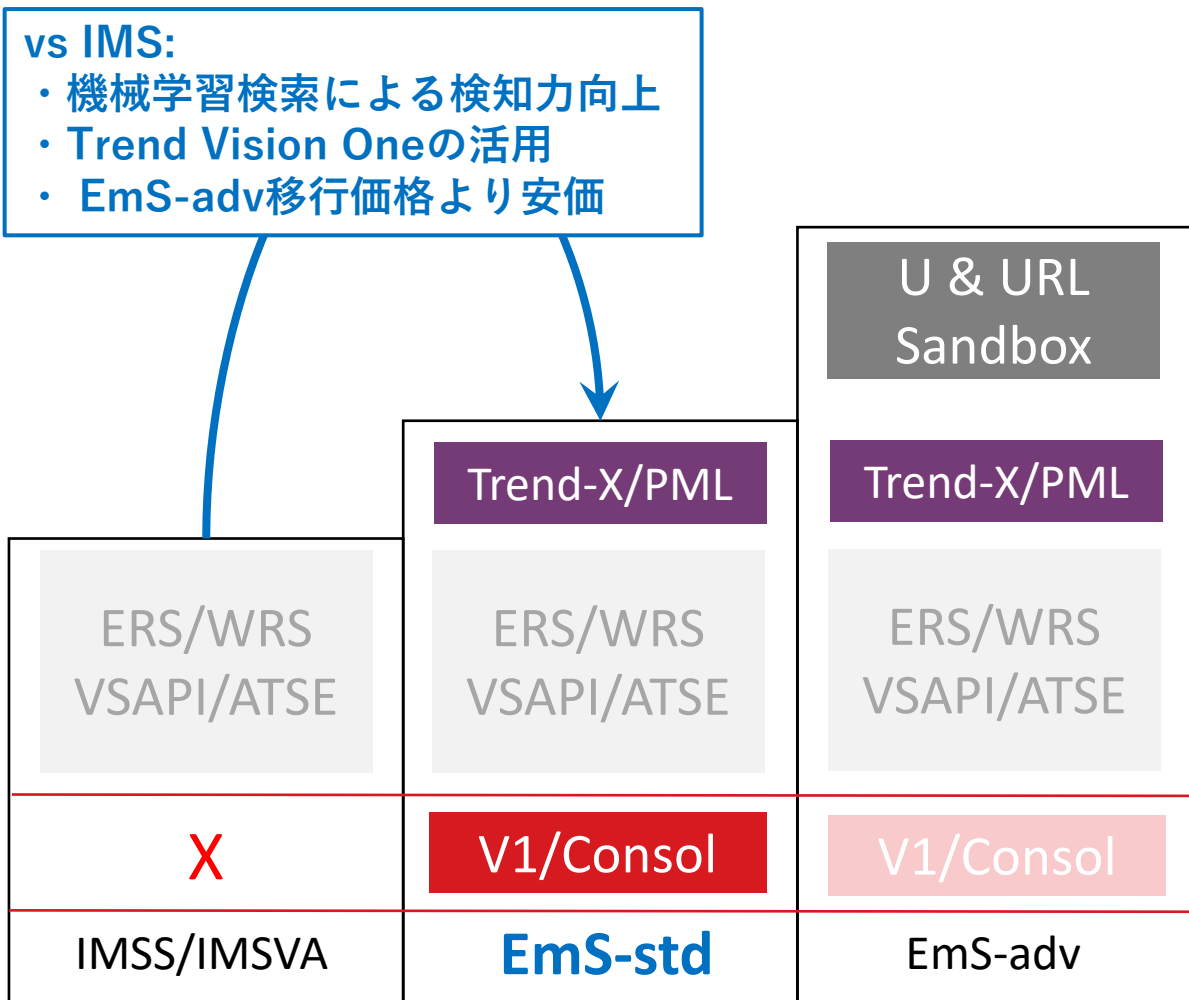
IAMとのSSO連携による  
ユーザを認証

認証されたユーザのアクセスを認可

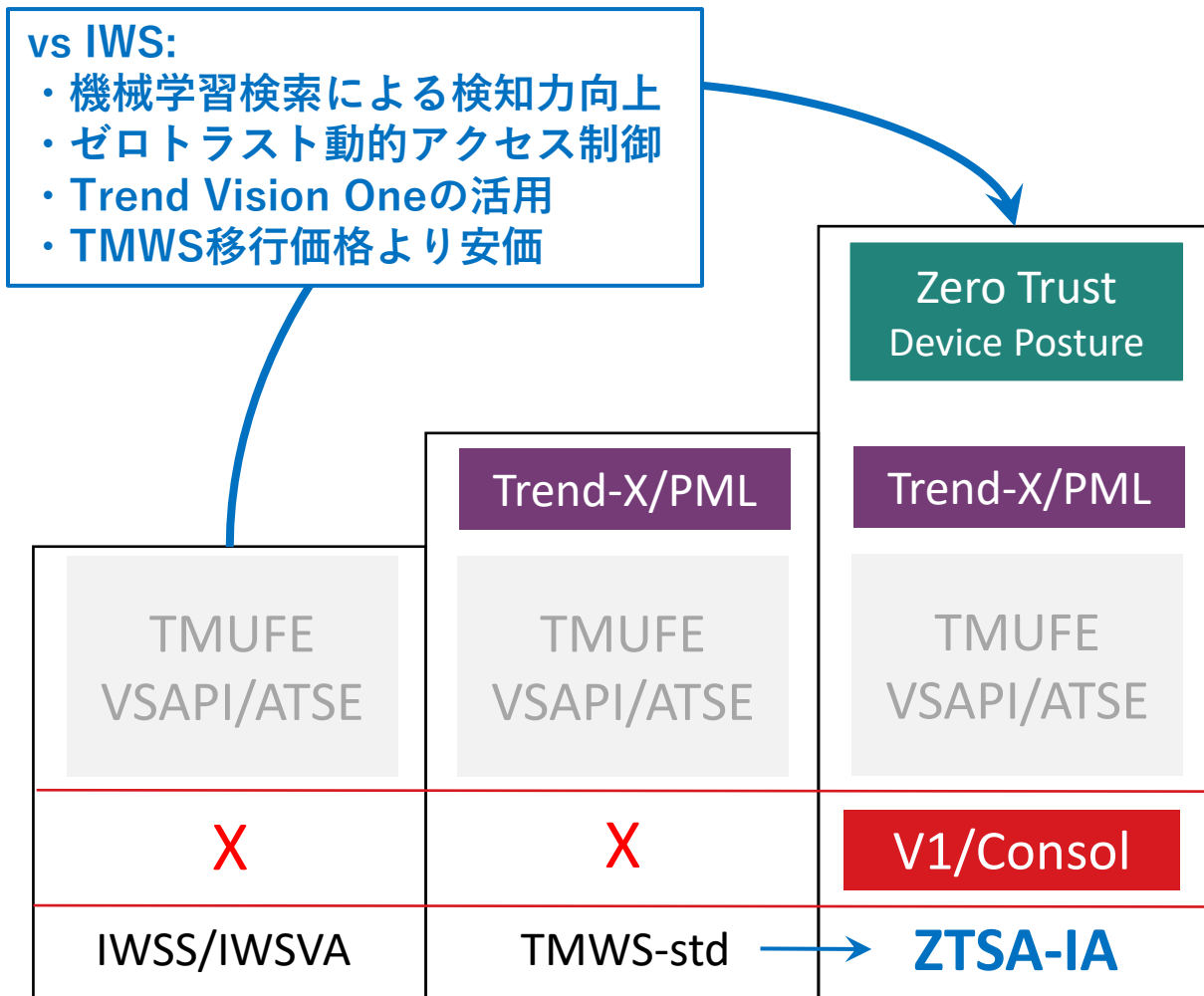
XDRと他評価を元にリスクスコアで判断



# InterScan vs SaaS 移行の機能差異とメリット



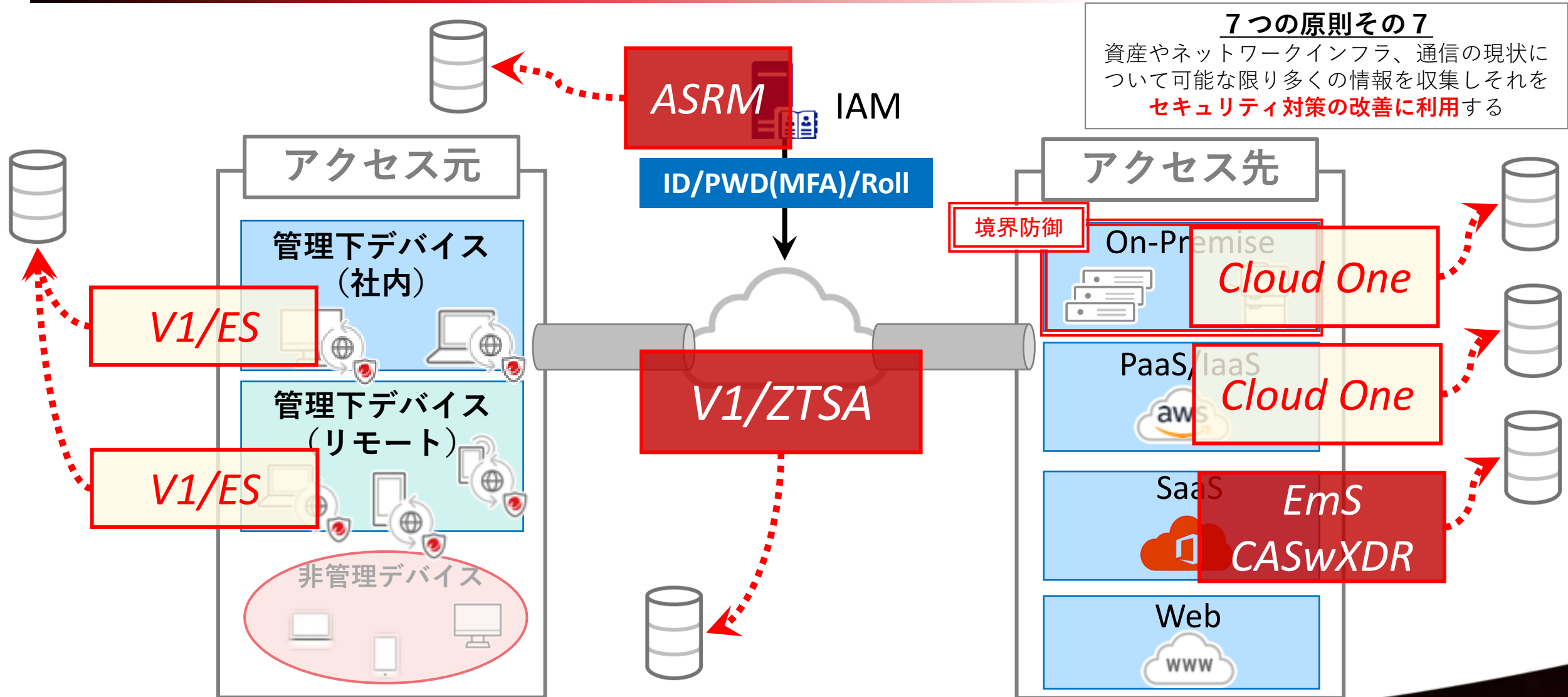
**SEG**



**SSE**

# Trend vision One 連携のメリット

# テレメトリのTrend Vision Oneへの連携



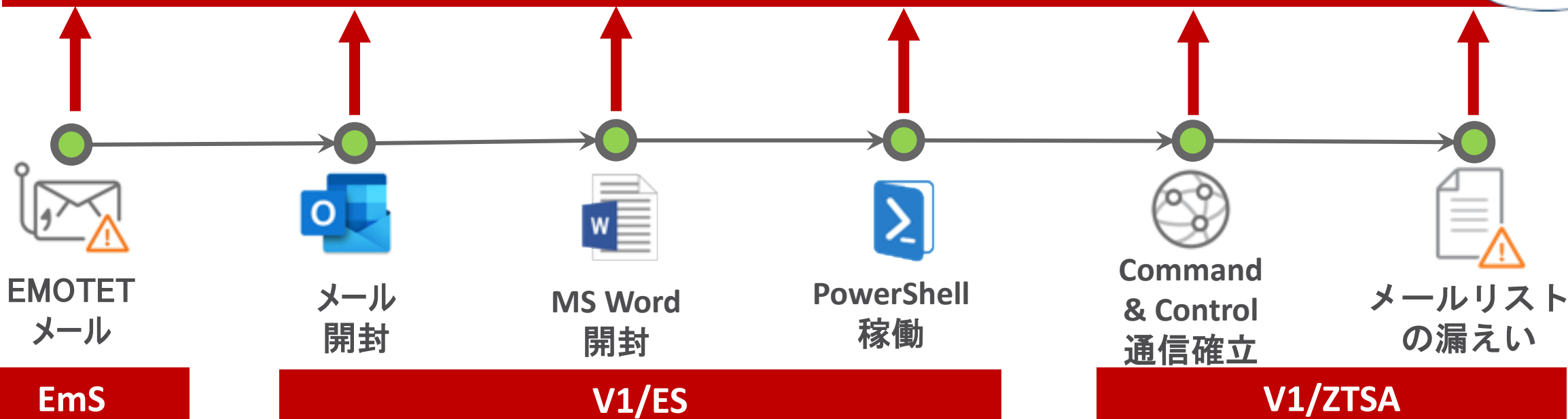


# SIEM (Security Information and Event Management)

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）



Trend Micro Vision One™ Workbench

アラートビュー インシデントビュー

ステータス: す... 作成済み: 過去30日間 モデル: すべて

Workbench ID, エンドポイント, ユ...

適用 表示: すべて

スコア	Workbench ID	モデル	モデルの...	影響範囲	作成済み
60	WB-9526-20211201-00001	Internal Spear Phishing Email via ...	High	1	2021-12-01 18:15...
60	WB-9526-20211130-00001	Internal Spear Phishing Email via ...	High	2	2021-11-30 15:13...
60	WB-9526-20211130-00000	Internal Spear Phishing Email via ...	High	2	2021-11-30 15:03...
60	WB-9526-20211128-00002	Internal Spear Phishing Email via ...	High	2	2021-11-28 17:03...
60	WB-9526-20211119-00000	Internal Spear Phishing Email via ...	High	2	2021-11-19 13:...
20	WB-9526-20211201-00000	Possible Spear Phishing Attack o...	Low	2	2021-12-01 12:...
20	WB-9526-20211129-00000	Possible Spear Phishing Attack o...	Low	2	2021-11-29 11:...
20	WB-9526-20211210-00000	Possible Spear Phishing Attack o...	Low	2	2021-12-10 11:...
20	WB-9526-20211210-00001	Possible Spear Phishing Attack o...	Low	2	2021-12-10 11:...

すべて  
グループ別  
モデル  
エンドポイント

Trend Micro | Workbench > WB-9002-20201216-0000

Summary

**Possible APT Attack**  
A backdoor was possibly implanted after a user received a possible spear phishing email message.

Score: 73  
Impact scope: 0 1 2 2  
Created: 2020-12-16T02:13:38Z

Highlights

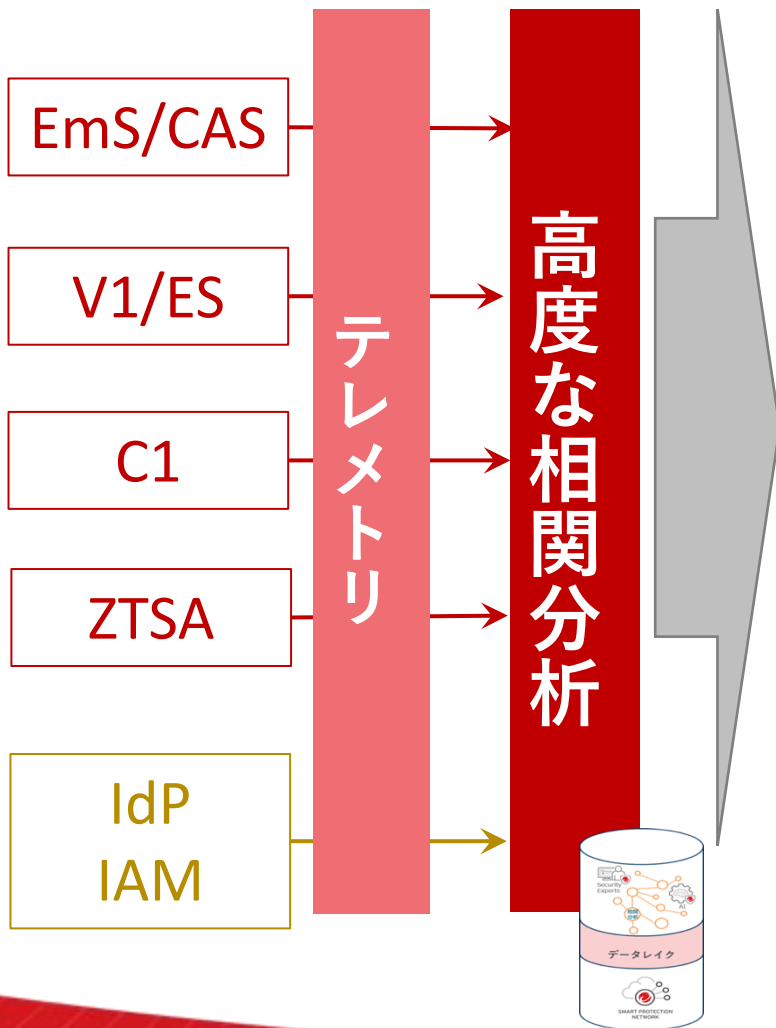
**Possible Spearphishing Link**  
Technique: T1566 - Spearphishing Link

2020-12-07T01:17:50Z | Search Event...  
[msgId] «5d70b5da54984d0ea7e8710daf...  
[mailMsgSubject] [Emergency] Important I...  
[Emergency] Important information  
[user] Ted\_Lee@trendmicro.com  
sam@jaguartmpeppy.onmicrosoft.com

Uncommon Run/RunOnce Registry Entry Creation  
Technique: T1060 - Registry Run Keys / Startup Folder  
2020-12-07T03:38:48Z | Search Event...  
[objectRegistryKeyHandle] hku\software...  
[! Indicators] [Indicator] [Indicator]

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



## Attach Surface Risk Management (ASRM)



予防対応へ

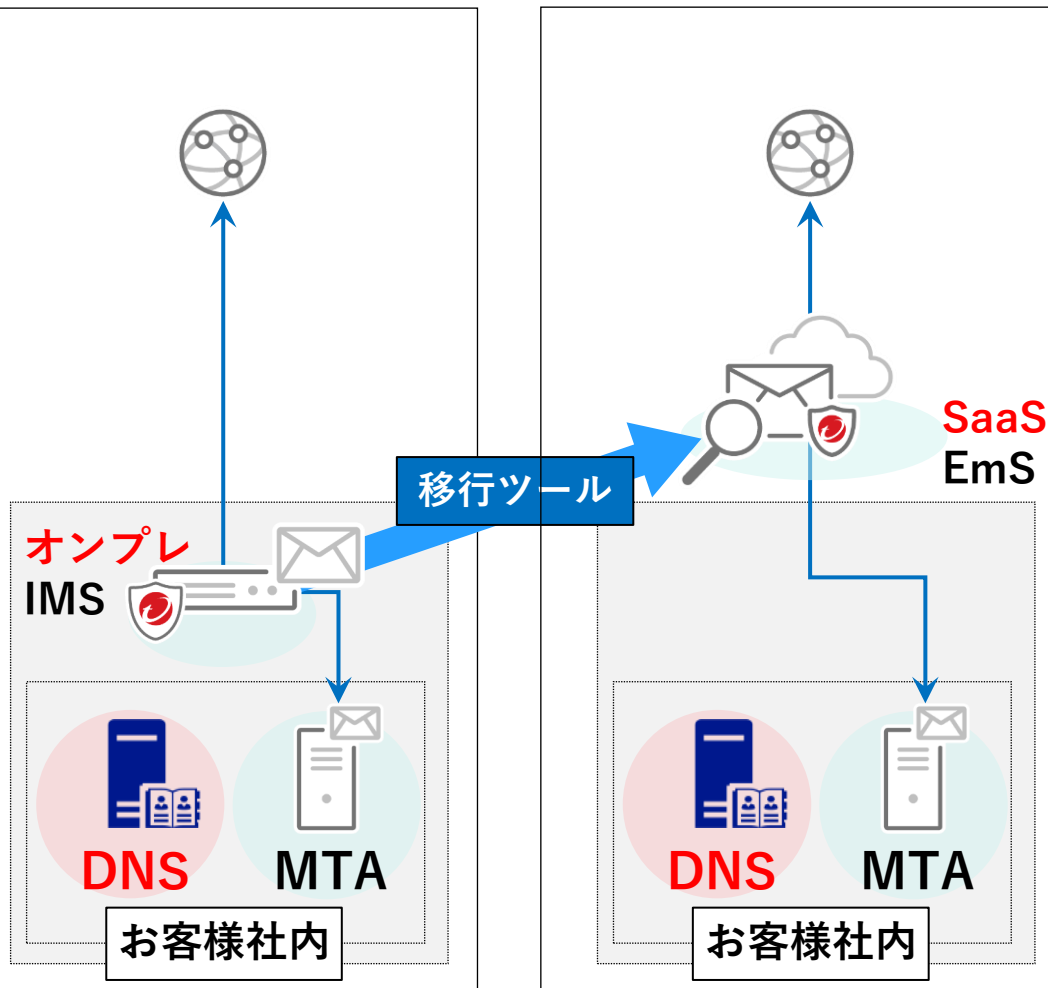
# SaaSへの移行を支援する 特別プログラム

# 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、IMS/IMSVAの全ての設定を移行することはできません。



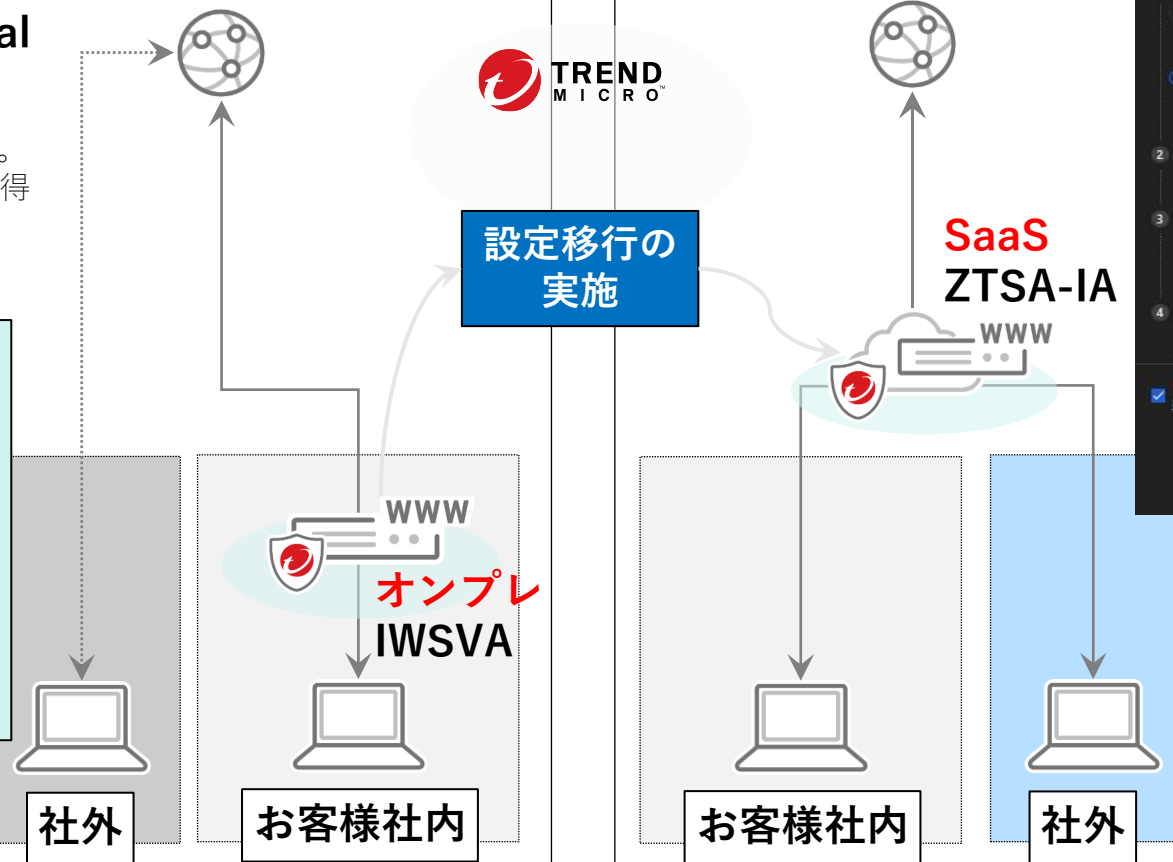
# Web : IWSVA → ZTSA-IA 移行支援のご案内

## 【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>

The screenshot shows the top navigation bar with the Trend Micro logo and 'Business Success' text. Below it are menu items: '製品サポート', 'ウイルス&脅威対応', '問い合わせ', 'その他', and 'お問合せ窓口'. A search icon and a 'ログイン' button are also present. The main heading is 'InterScan Messaging SecurityシリーズからTrend Micro Email Securityへの移行について'. Below the heading is a sub-heading: '製品・バージョンInterScan Messaging Security Suite 9.1, InterScan Messaging Security Virtual Appliance 9.1, Trend Micro Email Security , 全て表示'. Metadata includes '更新日: 2023/11/28', '記事ID: 000277129', 'カテゴリ: Migrate, SPEC', and '評価: 0'. There are two buttons: '追加の質問がありますか? フォーラムで質問する' and 'この記事は役に立ちましたか?'. A table of contents lists: 1. 概要, 2. 移行対象製品, 3. 移行対象の設定, 4. 移行手順, 5. 注意・制限事項, 6. よくあるご質問. A '概要' section is partially visible at the bottom.

## 【IWSVAからZTSA-IA】

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

The screenshot shows the top navigation bar with the Trend Micro logo and 'Business Success' text. Below it are menu items: '製品サポート', 'ウイルス&脅威対応', '問い合わせ', 'その他', and 'お問合せ窓口'. A search icon and a 'ログイン' button are also present. The main heading is 'InterScan Web Security Virtual ApplianceからTrend Micro Zero Trust Secure Accessへの移行で移行対象となる設定について'. Below the heading is a sub-heading: '製品・バージョンInterScan Web Security Virtual Appliance 6.5, Trend Vision One , 全て表示'. Metadata includes '更新日: 2023/11/23', '記事ID: 000295251', 'カテゴリ: Migrate, SPEC', and '評価: 0'. There are two buttons: '追加の質問がありますか? フォーラムで質問する' and 'この記事は役に立ちましたか?'. A '概要' section is visible, followed by a detailed text block explaining the migration process and a warning box with a red exclamation mark icon.

# 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

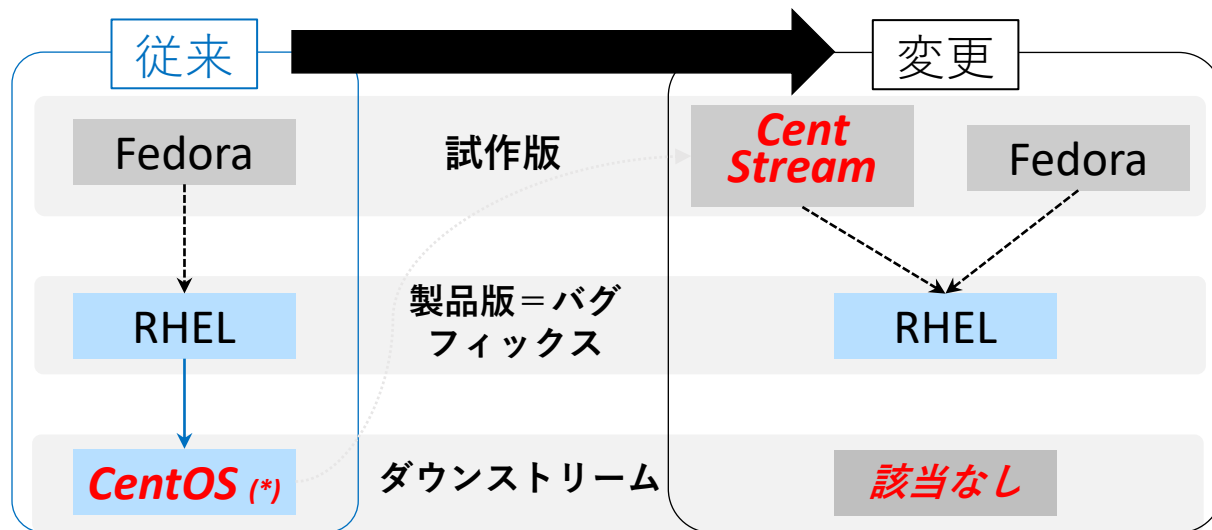
SSE



# 仮想アプライアンス版の終了は何故早まったのか？

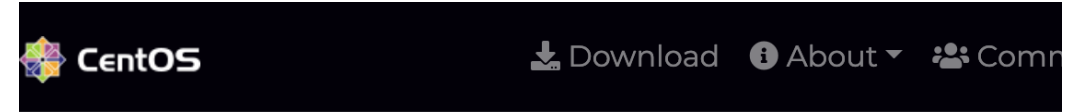
## RH社によるCentOSの位置付け変更とサポート終了

- 従来のCentOSは、バグ修正された製品版のRed Hat 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**にせざらう得ません



(\*)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/>



The future of the CentOS Project is CentOS Stream, and over the next year we'll be shifting focus from CentOS Linux, the rebuild of Red Hat Enterprise Linux (RHEL), to CentOS Stream, which tracks just ahead of a current RHEL release. CentOS Linux 8, as a rebuild of RHEL 8, will end at the end of 2021. CentOS Stream continues after that date, serving as the upstream (development) branch of Red Hat Enterprise Linux.

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

The screenshot shows the CentOS Product Specificatic page on the CentOS Wiki. It features a navigation menu on the left and a table of End of Lifetime (EOL) Dates on the right.

End of Lifetime (EOL) Dates	
CentOS Linux 7	
Full Updates <sup>1</sup>	2020-08-06
Maintenance Updates <sup>2</sup>	2024-06-30



# 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含まれている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	<div style="border: 1px solid black; padding: 5px; margin-bottom: 5px;"> <b>IMSVA</b>  <i>Cent OS (Library)</i> </div> <div style="border: 1px solid black; padding: 5px; margin-bottom: 5px;">Virtual machine</div> <div style="border: 1px solid black; padding: 5px;">Server (HW)</div>	<div style="border: 1px solid black; padding: 5px; margin-bottom: 5px;"> <b>IMSS</b> </div> <div style="border: 1px solid black; padding: 5px; margin-bottom: 5px;">Redhat Linux</div> <div style="border: 1px solid black; padding: 5px; margin-bottom: 5px;">Virtual machine (任意)</div> <div style="border: 1px solid black; padding: 5px;">Server (HW)</div>
Web	<div style="border: 1px solid black; padding: 5px; margin-bottom: 5px;"> <b>IWSVA</b>  <i>Cent OS (Library)</i> </div> <div style="border: 1px solid black; padding: 5px; margin-bottom: 5px;">Virtual machine</div> <div style="border: 1px solid black; padding: 5px;">Server (HW)</div>	<div style="border: 1px solid black; padding: 5px; margin-bottom: 5px;"> <b>IWSS</b> </div> <div style="border: 1px solid black; padding: 5px; margin-bottom: 5px;">Redhat Linux</div> <div style="border: 1px solid black; padding: 5px; margin-bottom: 5px;">Virtual machine (任意)</div> <div style="border: 1px solid black; padding: 5px;">Server (HW)</div>