クラウド管理型メールゲートウェイセキュリティ・サービス

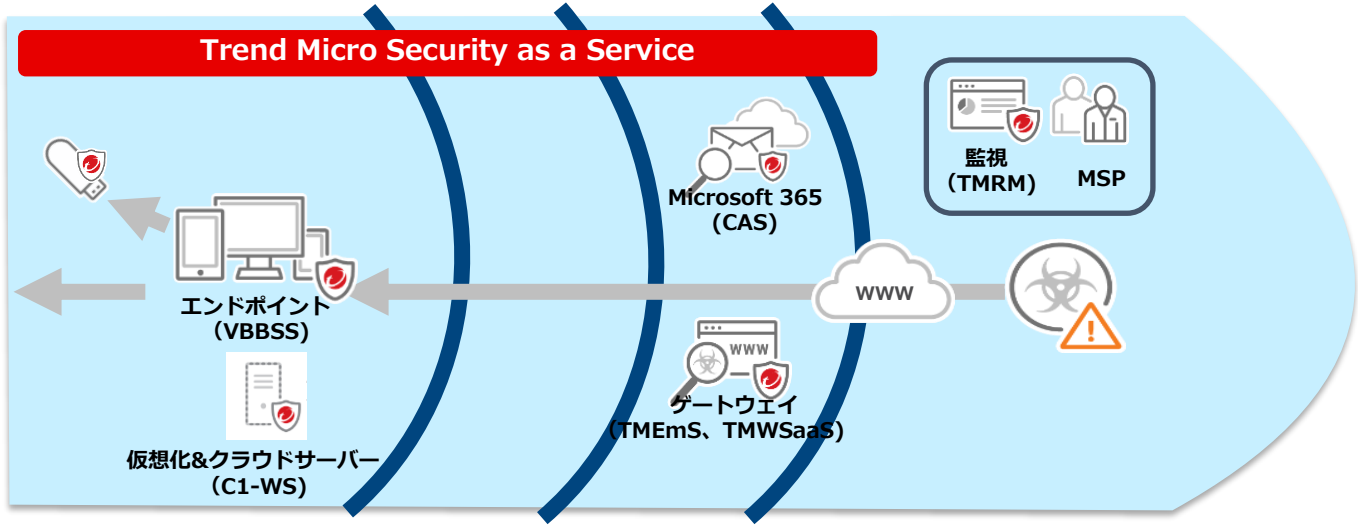
Trend Micro Email Security Advanced

SB C&S株式会社

Trend Micro Security as a Service とは

クラウド管理型セキュリティサービス

- 充実したクラウド型の多重防御セキュリティサービス
- 初期費用の低減、簡単な導入、運用負担の軽減を実現します



安い初期費用で中小企業でも大企業レベルのセキュリティを実現！

Trend Micro Security as a Service のラインアップ

エンドポイント

ウイルスバスタービジネスセキュリティサービス (VBBSS)

パソコン、モバイル、タブレットをランサムウエア、
ウイルス・スパイウエアから防御

サーバーセキュリティ

**Trend Micro Cloud One
– Workload Security　(C1WS)**

脆弱性、ランサムウエア、ウイルスから
サーバーを多層防御

M365/Gsite/Box/Dropbox

**Trend Micro Cloud App Security
(CAS)**

AI技術やサンドボックス分析により
ビジネスメール詐欺(BEC)やランサムウエアの
高度な脅威からOffice 365を保護

Webセキュリティ

**Trend Micro Web Security as a
Service – Standard (TMWSaaS)**

クラウド型サービスでインターネットの脅威を
ブロックしてウェブアクセスを制御

E-mailセキュリティ

**Trend Micro Email Security Advanced
(TMEmS)**

クラウド型サービスで効率的に
スパムメールを防御

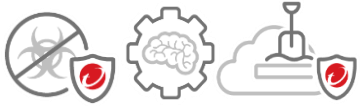
クラウド管理型セキュリティサービスのメリット

- トレンドマイクロ社が構築するクラウド上で管理運用するサービス
- お客さま環境に管理サーバーを用意する必要なし

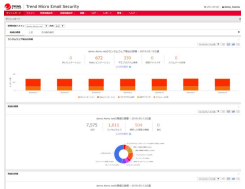
即応性	クラウド上で自動的にバージョン管理されるため新たな脅威にも迅速に対応
柔軟性	1ライセンスから購入可能。導入後のライセンス増減も柔軟に対応
コスト削減	管理サーバー不要のため初期投資や維持費用などコスト削減を実現
誰でも簡単	専門知識がなくても誰でも簡単にサービス導入・運用可能
どこでも簡単	ウェブサイトで簡単管理。サービス利用に必要なものはインターネット環境のみ

Trend Micro Email Security Advanced とは

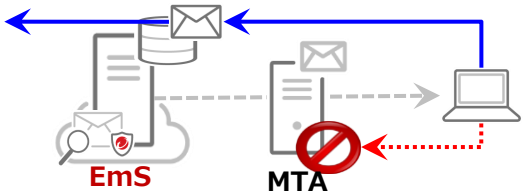
クラウド管理型のメールセキュリティサービスとなり、
TMEmSを経由してメール受信を行うことで、標的型攻撃やマルウエアなどのメールの脅威を検知・防御します。
トレンドマイクロ社が提供するウェブサイトの管理画面でセキュリティ状況を把握することができます。
クラウド型のため常に最新バージョンに自動更新され最新の脅威にも対応します。



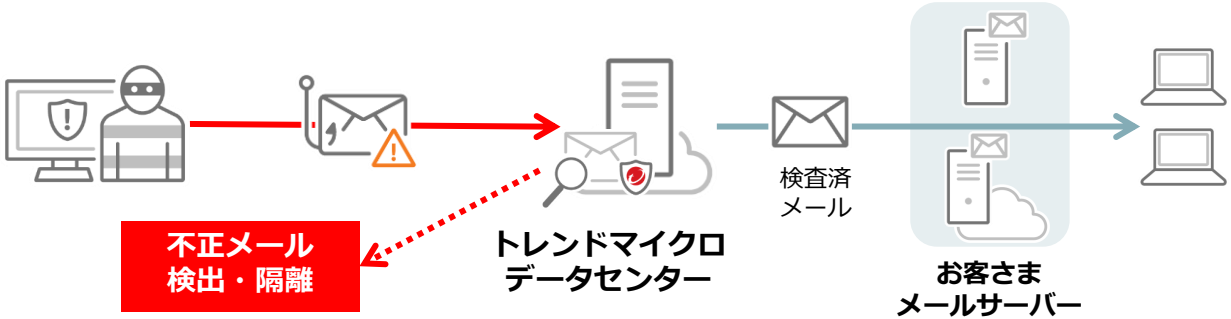
機械学習・サンドボックス等の高度な検索を用いた不正なファイルやURLを検出



ダッシュボードで状況把握
ログ(CEF)のSIEM直接転送



「不達メール管理」による継続維持



TMEmSの機能紹介

送信元の真正性の確認

DMARC/DKIM/SPF　ERS　SNAP

スパム・フィッシング対策

不正URL防御
WRS
Time-of-Clickプロテクション
URLサンドボックス

迷惑メールの排除
TMASE
グレーメール

マルウェア対策

パターン検索
既知の脅威防御
VSAPI/ATSE

機械学習
未知の脅威防御
Xgen-ML

サンドボックス
未知の脅威防御
DD-cloud

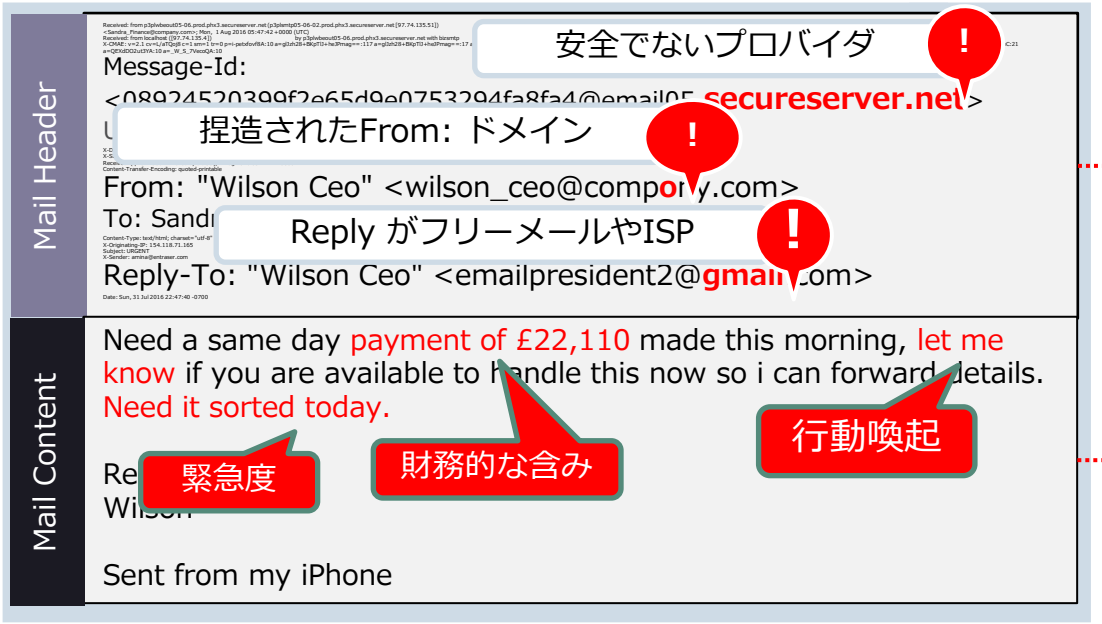
コンテンツフィルター

実ファイルによる検査　拡張子による検査
サイズによる検査　キーワードによる検査
圧縮ファイル検査
インテリトラップ

Trend Micro Email Security Advanced

TMEmSの機能紹介

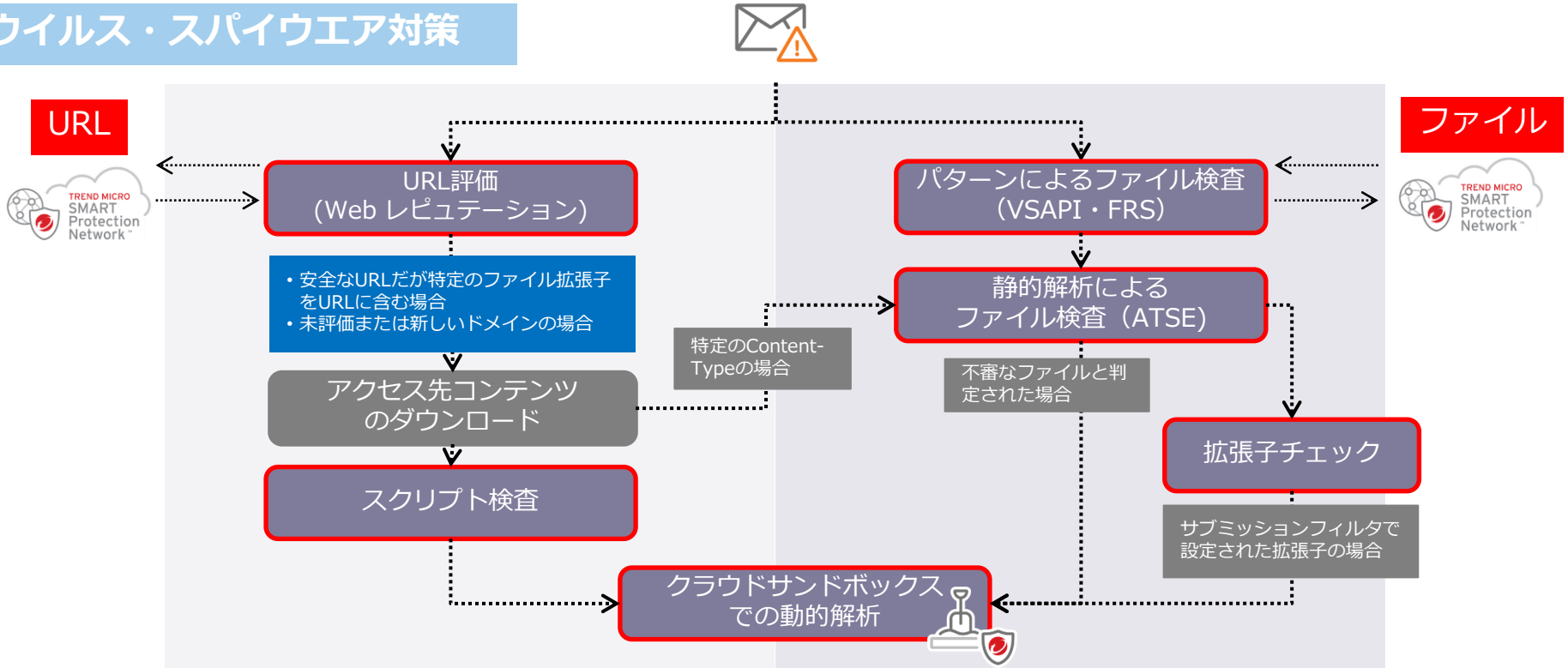
なりすましメール対策



AIを併用してメールの挙動や意図を分析し、なりすましメールを検出

TMEmSの機能紹介

ウイルス・スパイウエア対策



クラウドサンドボックスやATSEで既存・未知の脅威を検知し駆除します

TMEmSの機能紹介

マルウエア対策

○ シングルベンダー＆マルチテクノロジ

パターン検索

機械学習検索

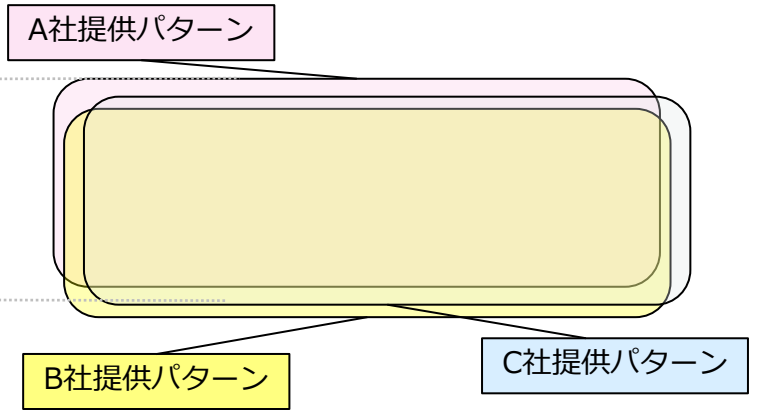
脆弱性・静的コード検索

サンドボックス動的解析

カバー領域の差異が
すり抜けの差異に

＊　異なるテクノロジを多層化することで、カバーする領域を大幅に増やし、また各機能が多段化し、検索時間を短縮できる

X　マルチベンダー＆シングルテクノロジ



＊　多様化する攻撃の今日では、従来のパターン検索によるマルチベンダー化では重なる領域が多いだけで、カバー領域全体が大して増えない。

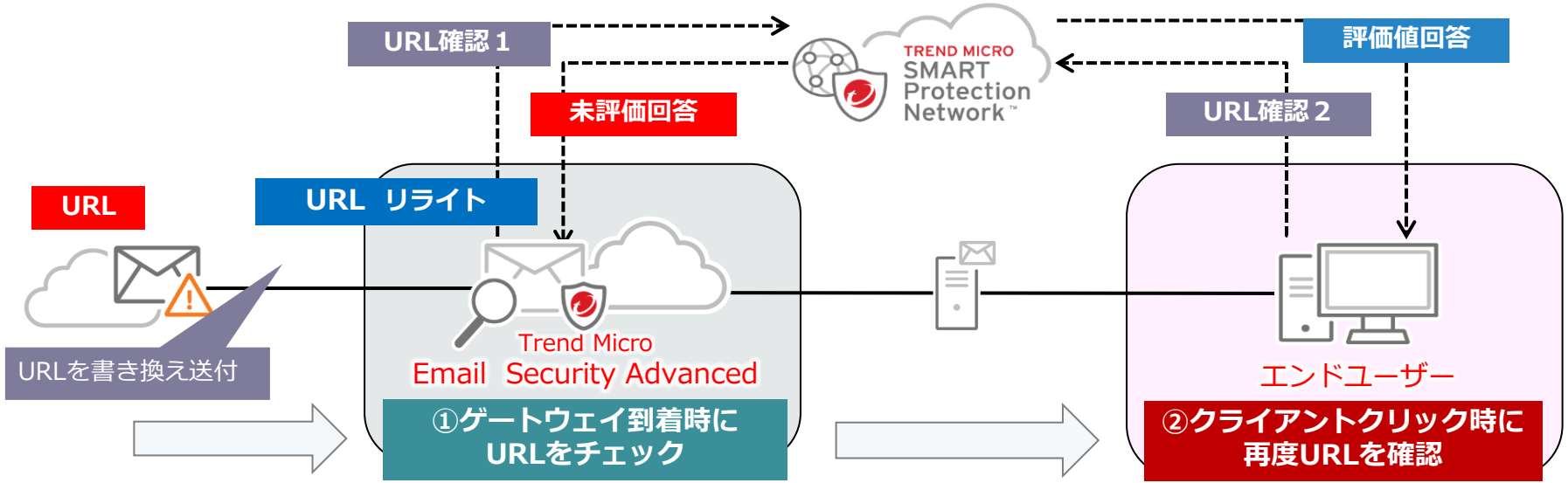
カバー領域を大幅に増やし最新の脅威にも対応

TMEmSの機能紹介

不正URL対策 総合

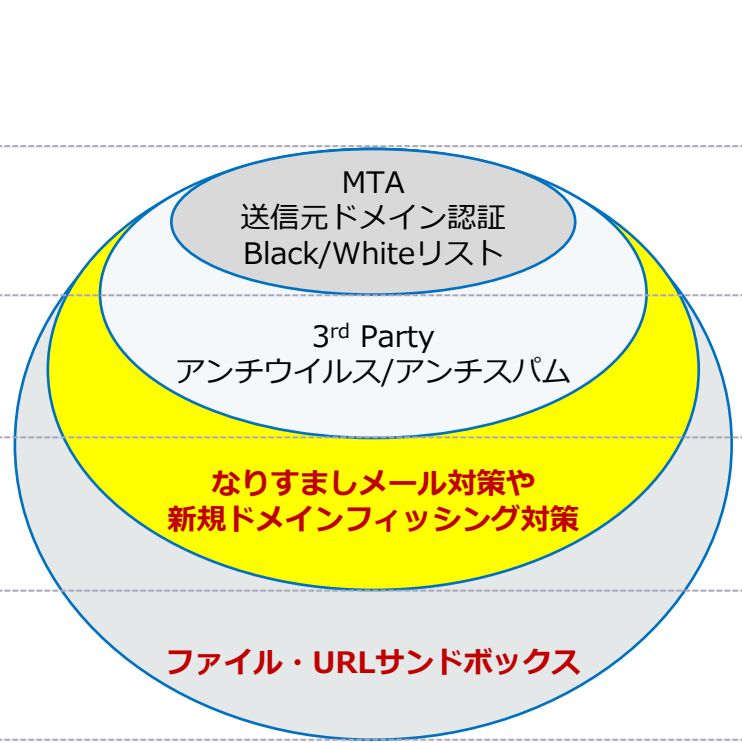
ロ Time-of-Click プロテクション

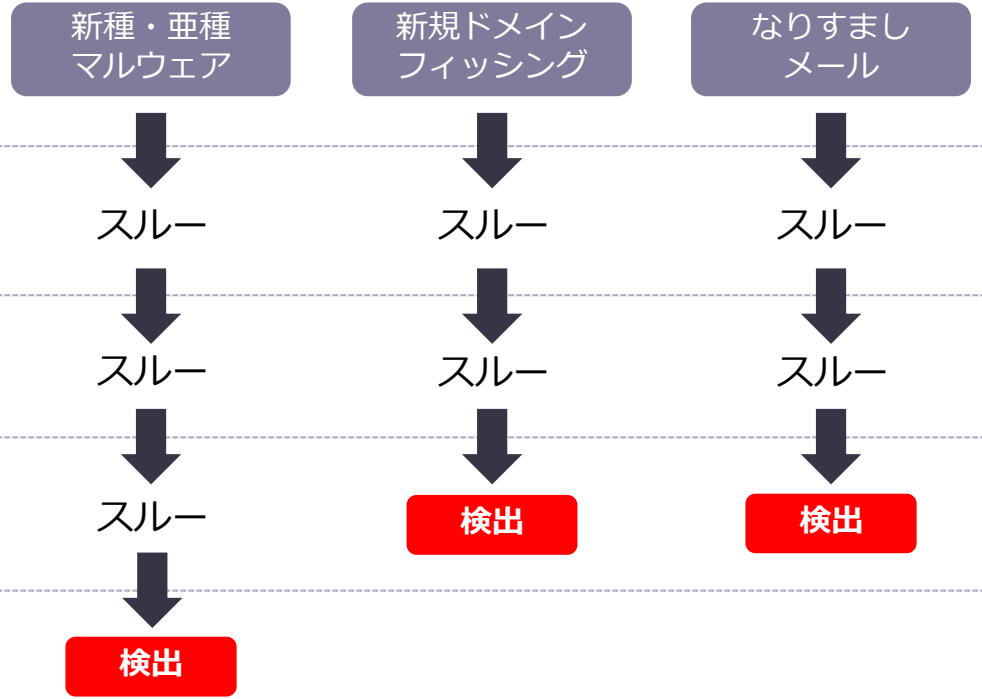
メール本文に記載されているURLを置き換えて分析し不正なURLをブロックします



最新の情報でURLを評価できるため、未知の攻撃や時間差攻撃を防御

TMEmSの機能紹介

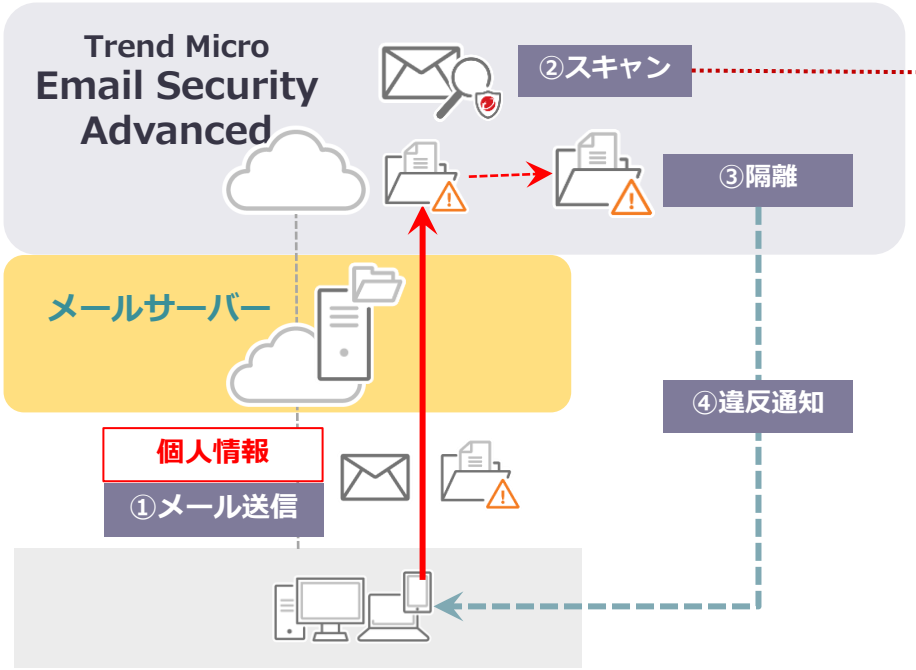


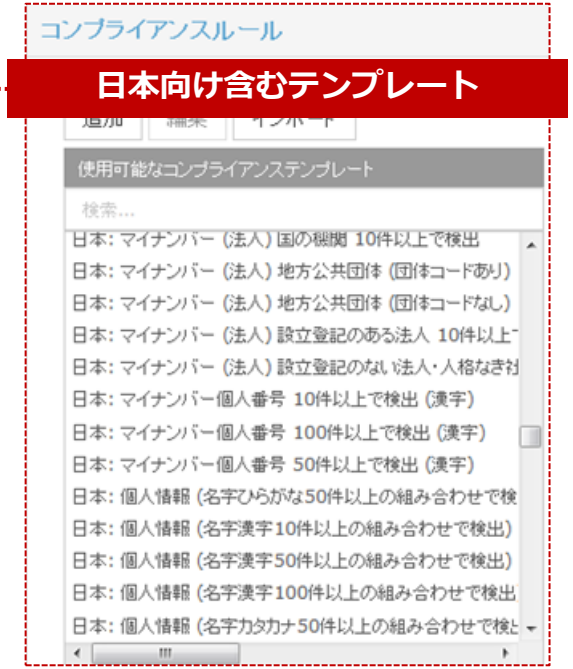


不足するセキュリティをTMEmSで補完

TMEmSの機能紹介

情報漏えい対策

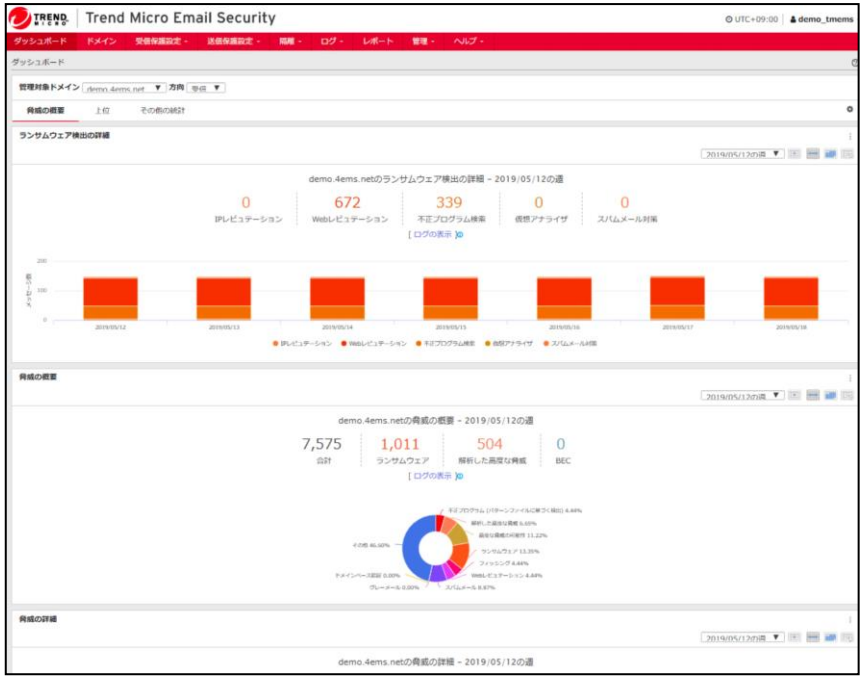




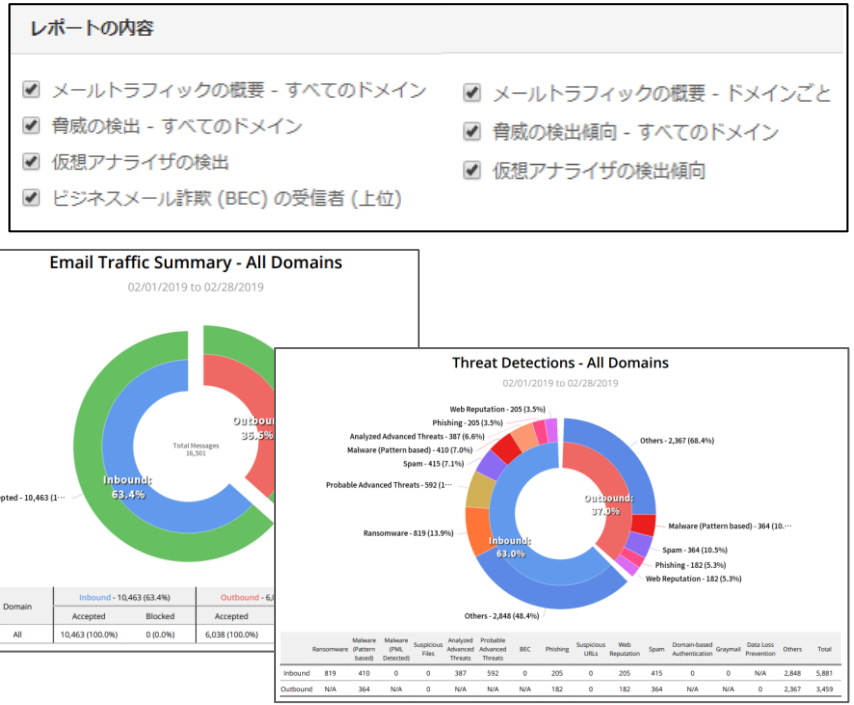
送信メールをスキャン個人情報漏えいのリスクがあるメールを隔離・通知

TMEmSの管理運用

■直感的で検知などを把握しやすいダッシュボード

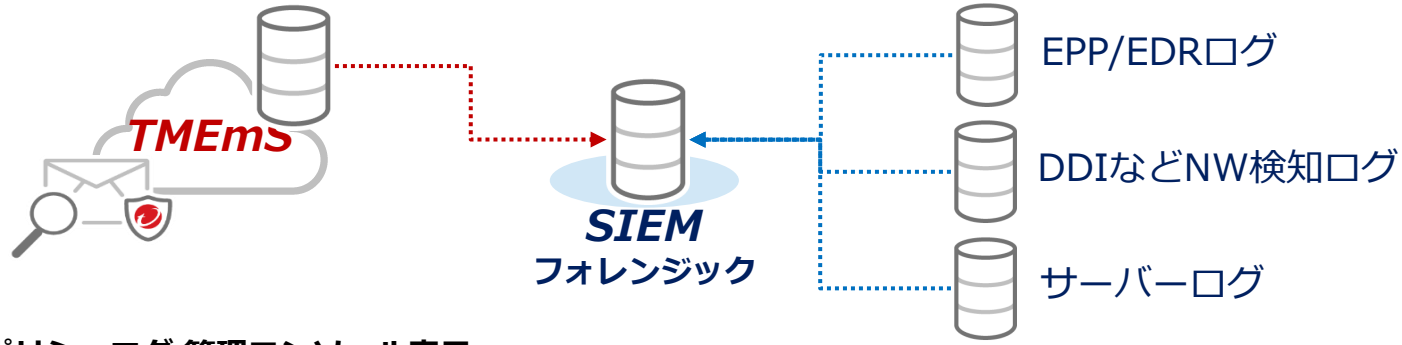


■予約・カスタマイズが可能なレポート



ダッシュボードでセキュリティ状況を把握し、必要なレポートを出力可

TMEmSの管理運用



TMEmS ポリシーログ 管理コンソール表示

2018/12/13 12:54:47	@	.com	@	.ml	不正プログラム	隔離	1:20181213: 125447 ABCDEF
2018/12/13 12:51:38	@	com	.@	.ml	不正プログラム	隔離	1:20181213: 125138 ABCDEF
2018/12/13 12:08:43	@	.com	.@	.ml	コンテンツ	隔離	1:20181213: 120842 ABCDEF

TMEmS ポリシーログ Syslog表示

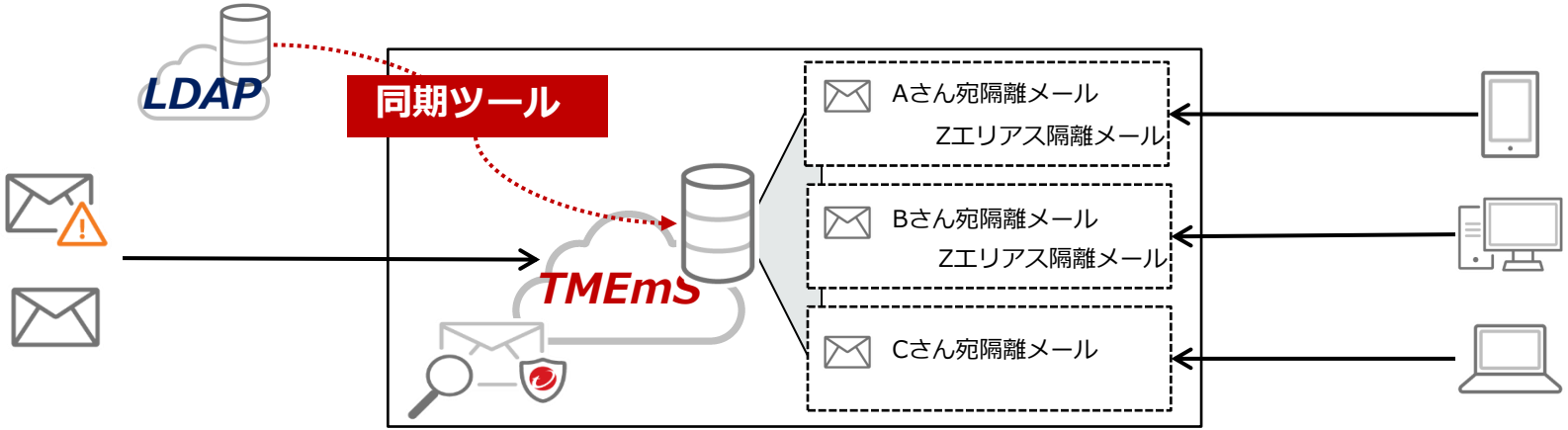
Dec 13 03:51:58 uiout.tmes.trendmicro.com 2018-12-13T03:51:58Z forwarder.tmes.trendmicro.com tmes[1]: timestamp="2018-12-13 03:51:38" event_type=virus domain_name=xxx.ml sender=xxx@xxx.com recipient=xxx@xxx.ml direction=incoming message_id=<0000000000004fde65057cdf3b7c@xxx.com> subject="1:20181213: 125138 ABCDEF" message_size=2478 policy_name="xxx: xxx.ml: Virus" policy_action=Quarantine

直接送付が可能なフォーマットされたログ

TMEmSの管理運用

システム管理者の負荷低減：エンドユーザーによる隔離メール管理(EUQ)

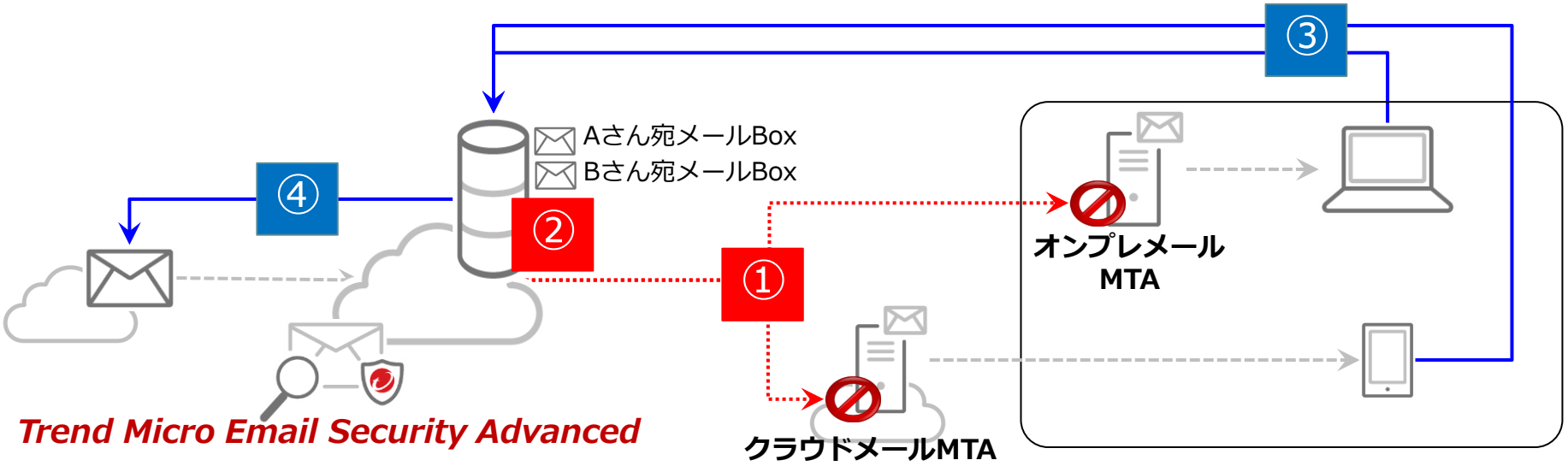
- 要・不要の判断について個別性の高い隔離したスパムメールを「エンドユーザーが個別に確認しハンドルする」ことで、正確で且つシステム管理者の負荷を大幅に軽減します。
- LDAPと連携することで、ユーザー別のメールボックスやメールエリアスを自動マージしたEUQを実現。エンドユーザーの閲覧の手間を低減します。



TCO削減に効く　運用効率の高いEUQ

TMEmSの管理運用

① 次の送付先MTAの障害を検知
② （リトライを続けながら）最大10日間の送受信メールを保存開始。
③ EUQに紐づくユーザーからTMEmSの保存ボックスに直接アクセスが可能
④ 障害中の送受信メールを、閲覧・ダウンロード・返信転送などが可能



不達メール継続管理

TMEmS機能一覧

分類	機能	TMEmS	IMS
送信者の真正性	送信者認証：SPF, DKIM, DMARC	有り	有り
	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	有り	有り
	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	有り	-
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	有り	有り
	ヒューリスティックを含む迷惑メールフィルタ対策	有り	有り
	マーケティングなどグレーメール分類	有り	有り
マルウェア対策	パターン検索による既知の脅威対策	有り	有り
	機械学習型検索による未知の脅威対策	有り	-
	サンドボックスによる未知の脅威への動的解析	有り	△(+DDAn)
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	有り	有り
	Time-of-Click プロテクション	有り	有り
	添付ファイル内のURLの検索	有り	有り(VA)
	クラウドサンドボックスによるURLの検査	有り	△(+DDAn)
コンテンツフィルター	実ファイルタイプによるポリシーの適用	有り	有り
	拡張子によるポリシーの適用	有り	有り
	容量・キーワードによるポリシーの適用	有り	有り
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	有り	有り
運用	不達メール管理：メールサーバー障害時の最大10日分のメール業務継続	有り	-
	フォーマットされたSyslogの外部転送	有り	-
	Connected Threat Defense：ファイル及びURLのSO受信	有り	△(+DDAn)
	レポートの拡張：カスタマイズ可な定期レポート	有り	-
	エンドユーザー隔離 – LDAP連携でのメールボックスやエイリアスの自動マージ	有り	-

ご購入方法

SB C&Sでは２パターンの販売モデルをご用意しています。
ビジネスに応じた販売モデルをご選択いただけます。

SP販売モデル	再販モデル
サービスプロバイダー契約を結びパートナーさまにライセンスの管理やユーザーサポートをお任せする販売モデルです。販売ツールの提供や技術支援など特別支援プログラムもご用意しております。	弊社にてサービスとユーザーサポートを提供する販売モデルです。初回購入時に書類をご提示いただく必要がございます。導入支援を行うSOC再販サービスもご用意しています。
①サービスプロバイダー契約書の締結 ②ユーザーサポートの提供 ③サービス利用許諾の作成 ④ウェブ管理画面(LMP)の操作 ⑤ライセンスや顧客情報の管理運用 ⑥毎月の利用レポート提出	①同意書の締結 ②申請書Webのご提出 ③サービス利用許諾のユーザー同意

SB C&S

SB C&S株式会社
〒105-0021 東京都港区東新橋丁目9番2号汐留住友ビル
ネットワーク&セキュリティ販売推進室