

TREND VISION ONE™

Email and Collaboration Security



アタックサーフェス（攻撃対象領域）の拡大と巧妙化するフィッシングメールは、組織にとって緊急の課題となっています。QRコードフィッシング、クレデンシャルフィッシング、AIによるメールの脅威、ビジネスメール詐欺（BEC）攻撃などの高度な脅威により、メールやコラボレーションの環境はますます攻撃を受けやすくなっています。さらに、従来のメールセキュリティ保護では、多くの場合、既知の脅威への対応に限定されています。

今こそ、リアクティブなセキュリティからプロアクティブなセキュリティに移行する時です。AIを活用した関連インテリジェンスを基盤とする Trend Vision One™ Email and Collaboration Security でレジリエンスとイノベーションを促進し、進化する脅威を予測、追跡して、対処しましょう。

ユーザと機密データに対するプロアクティブなセキュリティ

ユーザを保護するには、まずリスクを特定する必要があります。IT 管理者や SOC 管理者は、担当部門に余分な労力をかけずに潜在的な被害を拡大前に軽減できるようにする、プロアクティブなアプローチを必要としています。Email and Collaboration Security は、AI を活用したエンタープライズサイバーセキュリティプラットフォームである Trend Vision One™ を通じて一元的な可視化と管理や、機能の連携を行うことで、セキュリティ担当部門をサポートします。

ゼロデイ脅威、BEC、サプライチェーン攻撃、高度なフィッシング手法や詐欺など、見逃される可能性のあるさまざまな異常を発見できます。プロアクティブな人的リスク管理を通じて、軽減処置に優先順位を付け、巧妙なフィッシング攻撃を回避しながら、人とデータを保護できます。

安全なコミュニケーション、円滑なコラボレーション

AI-Powered エンタープライズサイバーセキュリティ

AI ベースの関連インテリジェンスを活用して、巧妙なフィッシング、BEC、ランサムウェア、詐欺を予測、追跡し、対処できます。Microsoft 365 や Google Workspace™ などのアプリケーションに対して包括的かつ最新の保護が得られ、進化する脅威への防御と迅速な回復が可能になります。

ユーザリスクの可視化、優先順位付け、軽減

完全に統合されたプラットフォームを活用して、メールゲートウェイやコラボレーションアプリケーション全体にわたってリスクの高いユーザや設定ミスを特定できます。

Trend Vision One™ Cyber Risk Exposure Management (CREM) ソリューションにより、ID に関するリスクを確実に管理し、フィッシング攻撃に対するセキュリティ意識を高めることができます。

AIでレジリエンスを構築

Trend Vision One Email and Collaboration Security ソリューションは、AI を利用したトレンドマイクロのサイバーセキュリティアドバイザーである **Trend Companion™** と完全に統合され、メールとコラボレーションの環境に堅牢な保護を提供します。

主な効能

- メールの意図を検証し、ユーザの挙動を可視化
- 疑わしい兆候を相互に関連付け、人的リスクを管理
- 情報に基づいたプロアクティブな意思決定を支援
- セキュリティ意識とリスクレジリエンスを向上

円滑な運用

一元的な可視化と管理を簡単に実現できます。メール、ID、エンドポイント、ネットワーク、クラウドの全体にわたるクロスレイヤ検知と、Trend Vision One XDRによる対応の自動化より、調査を加速させます。運用につながる気づき（インサイト）と分析を活用してメールに関する脅威を軽減し、包括的な保護と効果的な運用のためにワークフローを簡素化できます。

AIを活用したメールセキュリティ

既知および未知の高度な攻撃手法に先手を打って対処しましょう。

メールの異常を特定

ライティングスタイル分析や異常検知などのAI技術を用いて機密データや財務関連のIT資産を保護し、メールの侵害や支払い情報やプロセスの乗っ取りを防止します。

悪意のある挙動を追跡

AIを利用して不審な用語や送信者の挙動を検知することで受信トレイを安全に保ち、高度なアルゴリズムを駆使してスパム、ソーシャルエンジニアリング攻撃、不正なダウンロードをブロックします。

フィッシングの意図を検知

AIを活用した分析に基づいて脅威を検知し、メールにスコアを割り当て、コンテンツをキャプチャして分析することにより（QRコード攻撃の検知など）、フィッシングURLを高い精度で識別します。

詐欺サイトをスキャン

コンピュータビジョンとAIを活用した可視化を活用して高リスク要素を検知し、優先順位を付けることにより、従業員が偽のWebサイトにアクセスしたときにリアルタイムでアラートを生成します。



ゲートウェイ、API、インライン保護を統合した一元的な可視化と管理

業界をリードする機能を活用して、企業のメールおよびコラボレーション環境を保護できます。

Trend Vision Oneを通じて以下の機能にアクセスできます。

Cloud Email Gateway Protection (CEGP)	Cloud Email and Collaboration Protection (CECP)	Cyber Risk Exposure Management (CREM)	XDR for Email
メール関連の高度な脅威を検知して、お客さまに到達する前に阻止し、送受信時の機密データの暗号化によってメールの送受信を保護します。また、障害発生時もメールの継続性を確保し、データの漏洩を防止します。	BEC、ATO、高度なフィッシング攻撃に対する脅威対策とデータ保護を強化し、Microsoft 365、Google Workspace、Box™、Dropbox™などのコラボレーションサービス全体でクラウドファイル共有のコンプライアンスを強化します。	可視化と人的リスクに関する情報の取得により、IDに関するリスクの検証を継続的に行えます。内部ユーザや経営層など標的となる可能性の高い従業員、高リスクのイベントが発生したユーザについて、リスクに優先度をつけて軽減し、修復処置を実行します。	高度な分析結果を製品に組み込まれた機能で活用し、メールおよびコラボレーション環境を安全に保ちます。他のセキュリティレイヤから得られたデータでメールの挙動を保管します。すべては統合型の一つのプラットフォーム内で実行できます。

簡単かつ柔軟にメールセキュリティを簡素化

数ステップで、セキュリティイベントの把握を開始できます。Microsoft 365、オンプレミスのMicrosoft Exchange、Google Workspaceのメール環境であっても、メールとコラボレーションの環境全体にわたってデータプライバシーとセキュリティの要件を満たしつつ、メールのセキュリティを確保できます。

高度な分析と得られた深い気づき（インサイト）によってプロアクティブに保護を強化することで、セキュリティ担当部門がメール関連の脅威に迅速に対処し、リスクの高いユーザを管理できるようになります。絶えず進化する脅威に対抗し、迅速に対策を改善するために、俊敏性（アジリティ）、柔軟性に富み、先進の技術を採用している Trend Vision One プラットフォームをご活用ください。

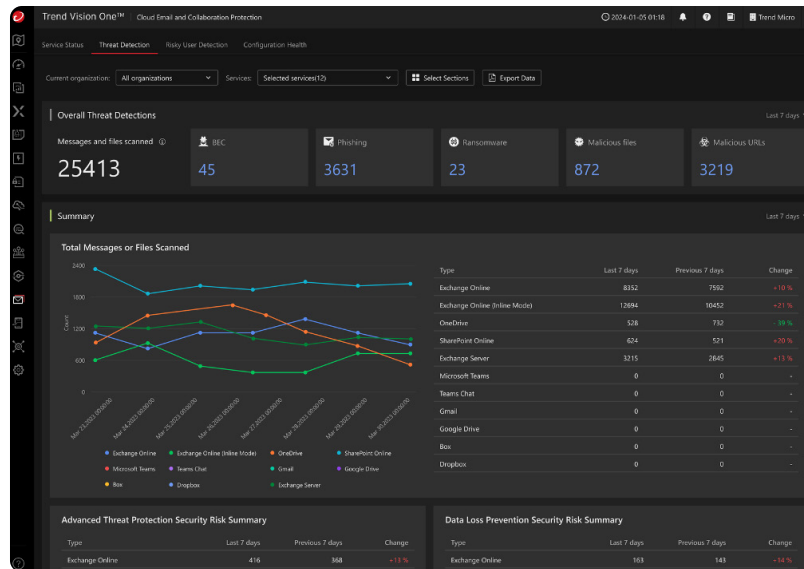


図1: Trend Vision Oneによるクラウドでのメールとコラボレーションの保護

ソリューションアーキテクチャ

クラウドの効率性を活かしながら、従業員のセキュリティを維持し、分析ご担当者の作業環境を一元化して、メールおよびコラボレーション環境の保護を最適化できます。

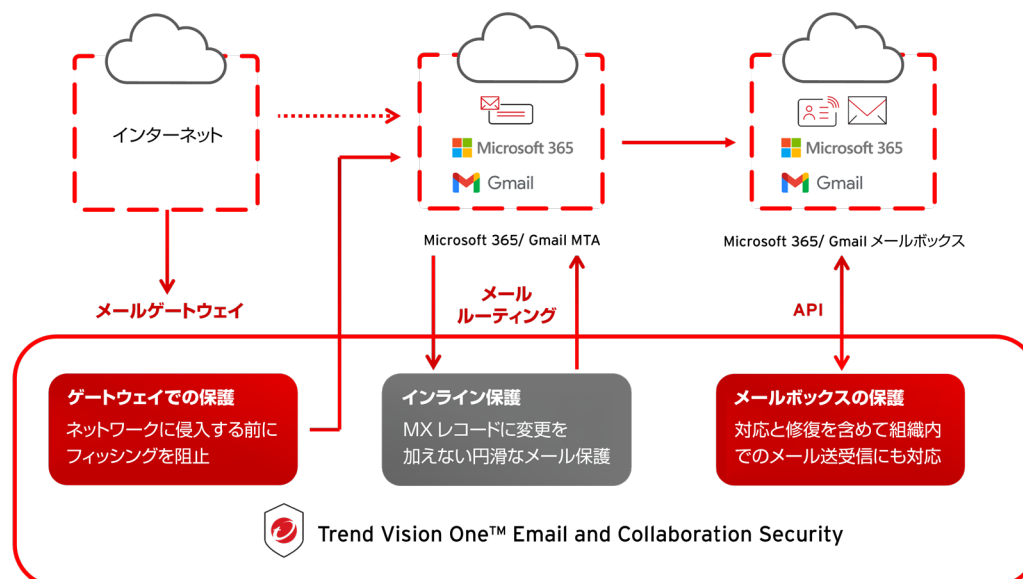


図2: Email and Collaboration Securityのアーキテクチャの概要

AIを活用した相関インテリジェンス検知モデル

相関インテリジェンスを適用して、メールとコラボレーションに関するさまざまな脅威の兆候を関連付けることができます。

ニュースレターや関係者との頻繁なやり取りなど、従業員が毎日受け取る大量のメールは、IT管理者が不要なメールを効果的に管理するうえで課題となります。ユーザの個々のやり取り、挙動、振る舞いなどを識別することが困難であるため、これはセキュリティ担当部門の日常の業務にも影響を及ぼします。

AIに基づく相関インテリジェンスを活用すれば、継続的な脅威監視、メール検証、高度な攻撃に対するプロアクティブな防御を実現できます。分析ご担当者、IT管理者、従業員のそれぞれに適切な行動を案内することで、安全な業務遂行を支援できます。

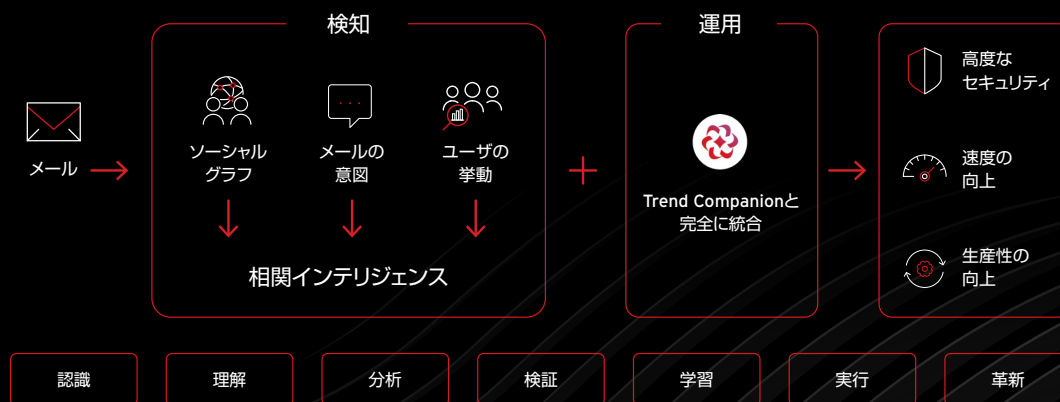


図3：AIを活用した相関インテリジェンス検知モデルの概要

人間の知性を変革

ユーザ同士の関係や、通信フロー、メールのやり取りを継続的に監視し、巧妙に仕組まれた脅威を発見できます。

- AIを活用した相関インテリジェンスでメールのセキュリティを強化し、検知の精度と速度を向上
- Trend Companion™との統合によりメールの意図を検証し、ユーザの挙動を分析して、不審な兆候の相関を把握
- AI生成バナーを適用して不審なメールの兆候を明示することで、ユーザの迅速な認識を促進し、報告を支援
- SOC担当部門と管理者が管理コンソールから直接、フィッシングシミュレーションや意識向上トレーニングを開始可能
- 分析ご担当者、管理者、従業員が情報に基づいた意思決定を行い、悪意のあるコンテンツやフィッシングURLに迅速に対処できるようにすることで、セキュリティ意識とレジリエンスを向上

脅威調査の結果

[トレンドマイクロ2025サイバースクリプト](#)

- メールは依然としてサイバー犯罪者がよく利用する攻撃経路
- 2024年にTrend Vision One Email and Collaboration Securityソリューションがブロックした高リスクのメール関連脅威は5,700万件
- ユーザ側で蔓延するリスク、特に情報漏洩防止（DLP）違反

Trend Vision Oneでメールとコラボレーションのセキュリティを強化

Cyber Risk Exposure Management

影響の優先順位付け、エクスポージャ（攻撃されるリスク）の低減、サイバーレジリエンスの構築を通して、サイバーリスクを予測、評価、軽減します。

XDR for Email

自社製センサと他社製の情報源を円滑に連携させ、メール、ID、エンドポイント、ネットワーク、クラウドのすべてを対象に脅威を検知して、それらを互いに関連付けます。

Threat Intelligence (脅威インテリジェンス)

Trend Zero Day Initiative™ (ZDI) の強力な脆弱性インテリジェンスを活用してサイバー脅威に先手を打って備え、複雑なアラートやリスクに対処します。

Trend Companion

生成AIによって生産性とセキュリティを向上させ、膨大なデータと高品質の分析を活用して実用的な気づき（インサイト）を獲得します。

Identity Security

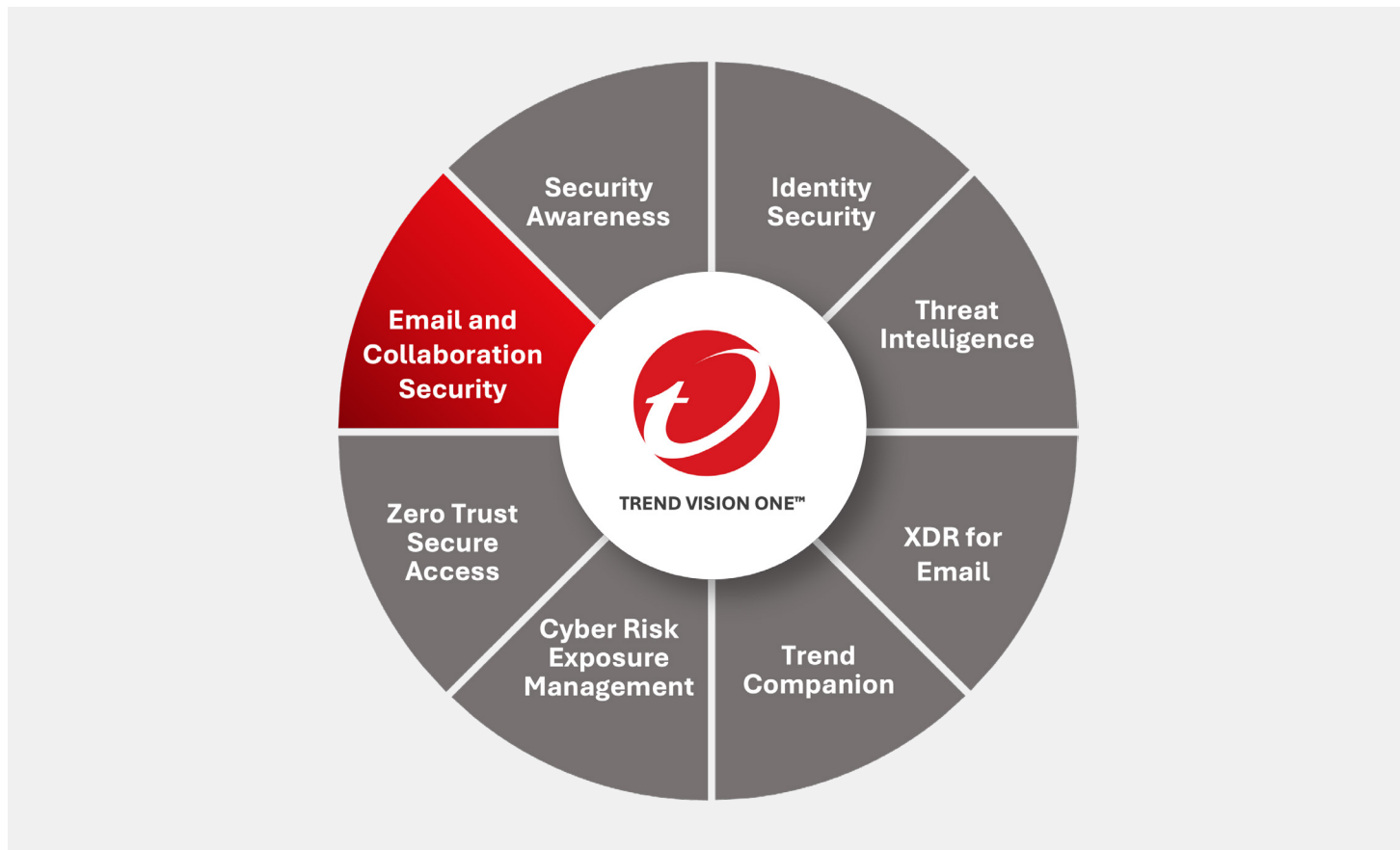
IDに関連した異常な挙動やアクセスパターンを監視して、ランサムウェア、フィッシング、サプライチェーン攻撃をブロックします。

Security Awareness

AIを利用した攻撃経路分析により、攻撃を受けやすい従業員を予測し、脅威のシミュレーションとトレーニングモジュールを提供します。

Zero Trust Secure Access

AIの活用が進む今日、一元的な可視化を通じてリスクに優先順位を付け、デジタル資産全体にわたってIDとデバイスを継続的に評価および検証します。





プロアクティブセキュリティ、始動。

Trend Vision One™ は、サイバーリスクの管理（Cyber Risk Exposure Management）、セキュリティ運用（Security Operations）、多層防御を一元化し、脅威の予測と防止をサポートする唯一のAI-Powered エンタープライズ サイバーセキュリティプラットフォームです。

機能と仕様

機能	Cloud Email and Collaboration Protection (CECP)	Cloud Email Gateway Protection (CEGP)
	APIおよびインライン	MX
マルウェアスキャン、スパム対策、Web レピュテーション、高度な脅威対策（ATP）	✓	✓
情報漏洩防止（DLP）	✓	✓
エンドユーザ隔離	✓	✓
IPレピュテーション	✓	✓
ドメイン認証		✓
メールの継続性		✓

機能と仕様（続き）

機能	Cloud Email and Collaboration Protection (CECP)	Cloud Email Gateway Protection (CEGP)
	APIおよびインライン	MX
メールの暗号化		✓
送信者ポリシーフレームワーク (SPF)		✓
DKIM (Domainkeys Identified Mail)		✓
DMARC (Domain-based Message Authentication, Reporting, and Conformance) 監視		✓
BIMI (Brand Indicators for Message Identification)		✓
クラウドサンドボックス	✓	✓
BEC対策	✓	✓
ライティングスタイル分析	✓	✓
QRコード検知	✓	✓
パスワード推測	✓	✓
不審オブジェクト	✓	✓
レトロスキャン	✓	
Microsoft Information Protection (MIP) との連携	✓	
コラボレーションアプリの保護	✓	
Microsoft 365、Google Workspace、Box、Dropbox連携	✓	
手動スキャン	✓	
API修復	✓	
エンドユーザフィードバック管理	✓	
ターゲット攻撃ユーザの可視化	✓	
アカウント乗っ取りの可視化	✓	
アカウントブロック	✓	

機能と仕様（続き）

	XDR for Email
フィルタと検索	✓
メールとクロスレイヤの高度な検出のためのワークベンチ	✓
メールのための対応	✓
メールアカウントのための対応	✓
確認された攻撃手法：MITRE ATT&CK™マトリックスマッピング	✓
イベントデータの保持	✓
脅威インテリジェンスによるメールテレメトリのスweep	✓

	Cyber Risk Exposure Management
全体像を把握いただくためのエグゼクティブダッシュボード	✓
リスクユーザ評価（リスクスコアとリスクイベント）	✓
セキュリティ設定状況確認のためのダッシュボード	✓
脅威検知、セキュリティ状況確認のためのダッシュボード	✓
セキュリティ意識向上トレーニング	✓

トレンドマイクロについて

サイバーセキュリティの世界的なリーダーであるトレンドマイクロは、デジタルインフォメーションを安全に交換できる世界の実現に向けて取り組んでいます。Trend Vision One エンタープライズサイバーセキュリティプラットフォームは、数十年におよぶセキュリティ分野の知見、国際的な脅威研究、そして終わりのないイノベーションに基づき、AIを活用して50万以上の組織と、2億5,000万人以上の個人ユーザを、クラウド、ネットワーク、デバイス、エンドポイントなどのさまざまな環境で保護しています。

[TrendMicro.com](https://www.trendmicro.com)

Copyright ©2025 Trend Micro Incorporated. All rights reserved. Trend Micro、Trend Micro t ボールロゴ、Trend Vision One、Trend Companion、および Trend Zero Day Initiative は、Trend Micro Incorporated の商標または登録商標です。その他の会社名および製品名は、各社の商標または登録商標です。本書に含まれる内容は予告なしに変更される場合があります。[SB01_Email_Collaboration_Solution_Brief_250925US]

当社が収集する個人情報とその目的の詳細については、トレンドマイクロのWebサイトでプライバシーポリシーをご覧ください。[trendmicro.com/privacy](https://www.trendmicro.com/privacy)

30日間の無料体験版を
お試しください

[TrendMicro.com/trial](https://www.trendmicro.com/trial)