# 可視性を向上させて広範なセキュリティを実現

リアクティブなセキュリティプロトコルはもはや過去のものです。セキュリティ運用を制御し、ビジネスをプロアクティブに保護しましょう。

## セキュリティリーダーが直面している課題

### 攻撃による被害額が増大

445 万ドル ランサムウェア攻撃による（身代金を除く）平均被害額[1]

効果的な脅威の検出と対応は、ビジネスを通常どおり運営し、成長に注力し続けるために不可欠です。

### 誰もが攻撃対象

83% データ漏洩を複数回経験している組織の割合[1]

攻撃の量、頻度、巧妙さが増すにつれて、SOC チームの負担も増大しています。

### アラート疲れが深刻化

37% アラートの量と複雑さが増大したことで、セキュリティ環境がより困難になっていると回答した IT 担当者とセキュリティ担当者の割合[2]

さまざまな検出信号や複雑な調査がアラート疲れの一因となり、アナリストの離職率を高めています。

現在のセキュリティツールでは、BlackTech、Volt Typhoon、Wizard Spyder などの高度な攻撃者を検出し、調査することは困難です。

## SOC エクスペリエンスが向上すれば、ビジネスはより安全になります。

セキュリティリーダーとそのチームは、より優れた有効性、エクスペリエンス、ROI を求めています。

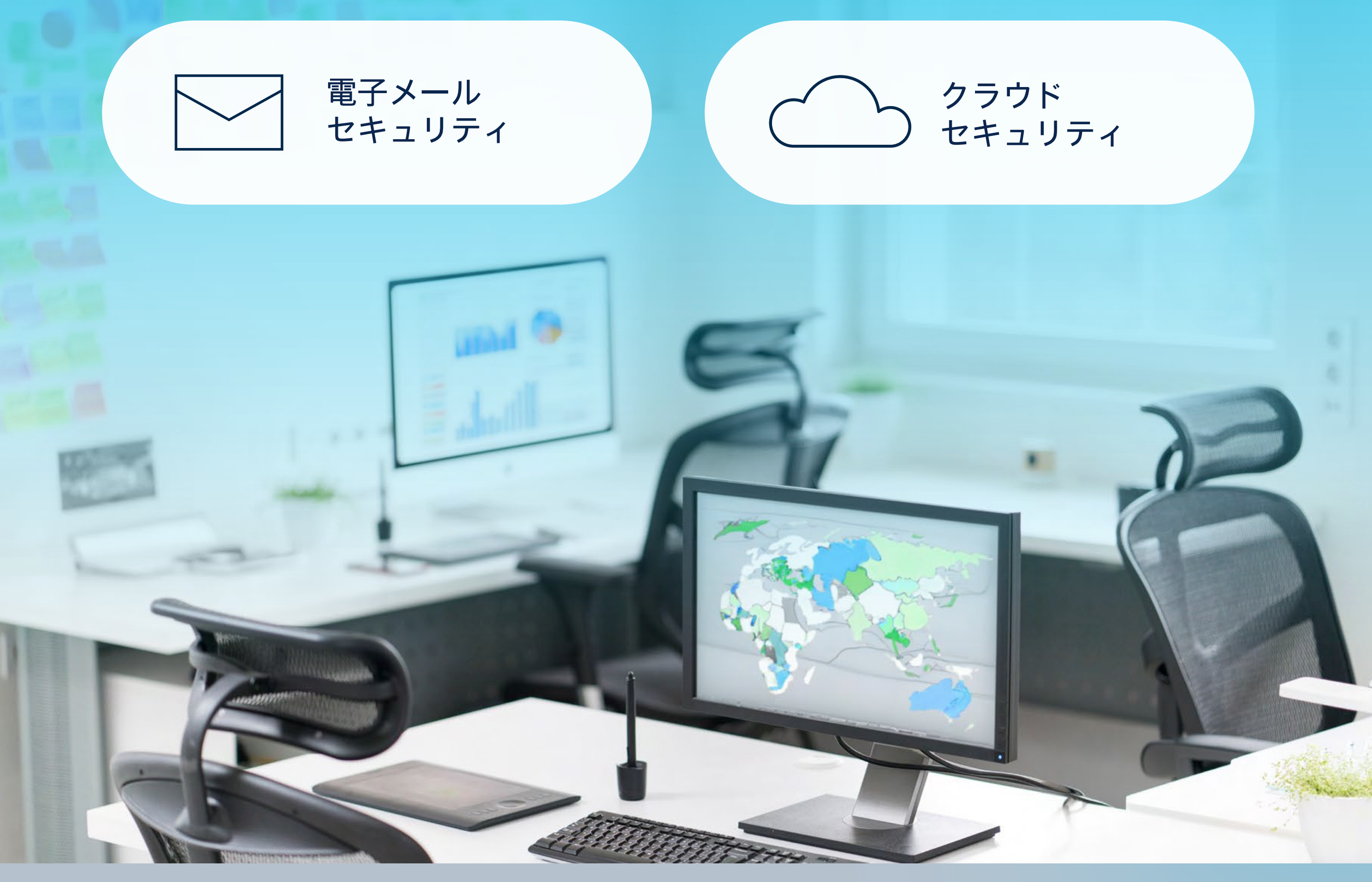
**より優れた有効性：**関連付けられたテレメトリを使用し、人間の直感と AI の組み合わせることで、ランサムウェアのような高度な脅威を検出および対応します。

**より優れたエクスペリエンス：**統合されたビューと自動化の向上により、より多くの情報を把握し、より迅速に対応し、アナリストの極度の疲労を軽減します。

**より優れた ROI：**SOC の生産性を最適化するために構築された自動応答とガイド付き調査により、既存のセキュリティリソースをさらに活用できます。

Cisco Breach Protection Suite を使用すると、セキュリティチームはエンドポイント、電子メール、ネットワーク、クラウド環境全体にわたって、ランサムウェア、フィッシング、マルウェア、組織内に潜む脅威などの脅威を阻止できます。

- Extended Detection and Response（XDR）
- エンドポイントセキュリティ
- ネットワークにおける検出と対応（NDR）
- 電子メールセキュリティ
- クラウドセキュリティ



## Breach Protection は、次のような方法で実現します。

- 脅威をより迅速に検出 → 脅威にさらされるリスクを最小限に抑制
- 潜在的な影響によるインシデントの優先順位付け → ビジネスリスクの最小化
- 迅速な調査の実施 → 攻撃を完全に把握
- 応答時間の短縮 → 損害を引き起こす前に攻撃を阻止

## 可視性を向上させて広範なセキュリティを実現

シスコは、何十億もの認証要求、フィッシング攻撃、不正な Web ページを確認し、エンドポイントから接続するすべてのプロセスを追跡しています。これにより、セキュリティチームは状況を把握し、ランサムウェアなどの脅威をその場で阻止できます。

Cisco Security Cloud によって提供されるエンドツーエンドのプラットフォームビューにより、高度な攻撃をより効果的に阻止するための可視性と機能が得られます。

Breach Protection は以下によって強化されています。

500 人の脅威研究者

TALOS

AI を活用したアルゴリズム

5,500 億件

毎日観測されるセキュリティイベント

人間の直感と AI や自動化を組み合わせることで、誰よりも効果的に脅威を阻止します。

## 期待をはるかに超えた脅威の検出と対応

Breach Protection の詳細はこちら