eBook

# プロアクティブな CISOのための手引き

エクスポージャの見落としをなくし、
確信を持ってサイバーリスクを管理する

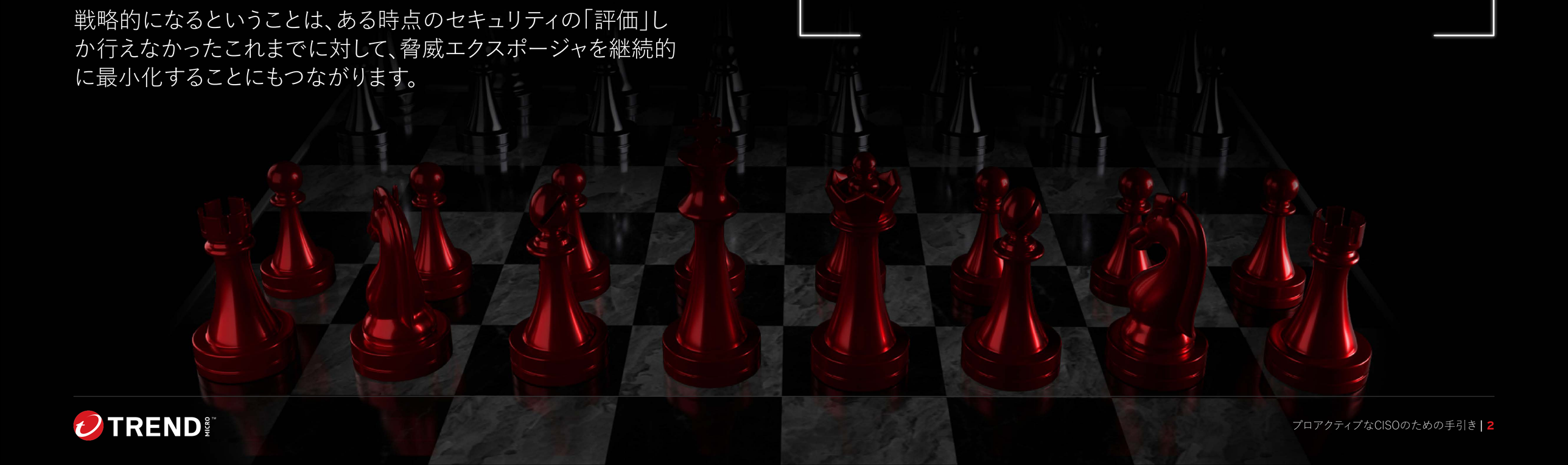
# 戦略的なCISOが意味するものは?

サイバー脅威をビジネスリスクの観点から考え、緊急対応に追われるのではなく、サイバーリスクをプロアクティブに管理する手順を整えることを意味します。

戦略的になるということは、ある時点のセキュリティの「評価」しか行えなかったこれまでに対して、脅威エクスポージャを継続的に最小化することにもつながります。

**戦略的かつ積極的なセキュリティアプローチの基盤を設定する本文書では、以下の項目をご紹介します:**

- 管理について多くの組織が誤解している点
- サイバーリスク管理の3つの重要な柱
- プロアクティブなセキュリティへのロードマップ
- 重要な成功要因



# リスクは決して眠らない

他のビジネスリスクとは異なり、サイバーリスクは動的、継続的で、組織全体に波及します。明確な境界はなく、終わりもありません。攻撃対象領域も、最新の脅威や技術と共に変化し続けます。

侵害が増加し続けることで、結果に対する経営者の責任は高まり、サイバーリスクの軽減は単なる技術的な課題ではなく、組織戦略上避けては通れない課題です。

高度なサイバーセキュリティ技術の効果にも期待できますが、特定領域に特化したツールの乱立は、リスクの削減につながるどころか、管理の複雑性につながります。一方で攻撃者は、最も障壁の低い攻撃経路を継続的に探し、確実に見つけ出しています。

これがサイバーリスクの管理を困難にしており、これまでのリアクティブなセキュリティ運用から、戦略的で、リスクベースのアプローチに変化するための確実な道筋がCISOには求められています。

**サイバーリスクは組織全体のデジタル資産への可視化を必要とします：**

- エンドポイント
- インターネットに接続する資産
- アプリケーション
- アカウント
- クラウド資産

**60%**

以上の組織は、未知、管理外、または管理が不十分で、インターネットに公開されている資産が侵害に関与したと回答 [1]

**75%**

が直面しているリスクの特定に1日以上かかると回答 [2]

# サイバーリスクにまつわる誤解

今日のほとんどのCISOは「リスクに対応する」方法論で、脆弱性を評価しています。把握したリスクを管理するという体系的なアプローチは、机上では良策に見えますが、実際には意図したほどリスク軽減の効果が得られないことが多くみられます。

ここでは、**リスク対応における一般的な6つの落とし穴**をご紹介します。理論的な解決策とコンプライアンス対応のための活動をしているため、これらは効果的なアプローチとは言えません。本当に必要なのは、**プロアクティブなリスク管理**です。

## 01

### なにもしない

リスクを把握しても、まだ実際の害を及ぼしていないため、未対応のまま放置する。

## 02

### 「チェックリスト」対策

文書の追加、ポリシー作成、またはトレーニング実施を、測定可能なセキュリティの改善に結びつけていない。

## 03

### 「振り返りのない」対策

セキュリティ対策を実装しても、それらが機能しているかの確認、脆弱性が減少したかを追跡していない。

## 04

### フォロー不足

予防措置によりリスク軽減が完了したと仮定し、検証や継続的なペネトレーションテスト、レッドチーム演習、リアルタイム監視が行われていない。

## 05

### 責任が不明確

セキュリティおよびITチームの範疇を超えたサイバーセキュリティの責任範囲が特定されていない。

## 06

### リスクを他人任せ

脆弱性に直接対処せずに、リスクをベンダー、パートナー、または保険会社に責任転嫁することで「対処」している。

# サイバーリスク管理の進化

組織の攻撃対象領域の拡大と複雑化により、CISOはプレッシャーにさらされています。CISOは脅威から守るだけでなく、積極的にリスクを管理することも期待されています。このプレッシャーは、AIの継続的な進化によって、より助長されると考えられます。

## エクスポージャ管理

脅威のエクスポージャが増加したことに対応して、サイバーセキュリティの専門家は攻撃対象領域管理に注力し始めています。

## リスクに対する認知が向上

専門家は、管理が必要なのは攻撃対象領域だけでなく、その上で発生するリスクにもあると認識しました。米国国立標準技術研究所(NIST)などの組織では、サイバーリスク管理のフレームワークが展開されています。

## IT以外への影響

サイバーリスクがIT環境に限定されないことも明らかになっています。サイバーリスクは生産性、収益、企業の評判に影響を与えます。このため、サイバーリスクのスコアリングや定量化といった新しいツールが必要となりました。

## 継続的なプロセス

専門家は、リスクの監視と評価が常時、継続的な活動である必要があることを把握しました。Gartner社ではContinuous Threat Exposure Management(CTEM)の概念を展開しています。

今日のサイバーリスク管理はまだ新しい分野です。AIリスクが課題を増大させる一方で、AIツールはサイバーリスク管理をこれまで以上にプロアクティブにできると考えられています。

# サイバーリスク管理の3つのプロアクティブな柱

結局のところ、サイバーリスク管理は、可視化、優先順位付け、軽減の三つの組み合わせにかかっています。
これらのそれぞれが重要なサイバーセキュリティのニーズに対応しており、それぞれにおいて同時に考慮すべき事項があります。

## 01 可視化

見えないものは保護できません。管理外の資産を見つけて対処する必要があります。

### 必要とされるのは...

#### 継続的なインサイト

これまで、セキュリティ担当部門はある環境の、ある時点のチェックに頼らざるを得ませんでした。これは、今日の脅威の状況に対応するには不十分です。攻撃者はたった1つの弱点を見つけるだけで攻撃を開始できるため、プロアクティブなリスク管理には、すべてのデジタル資産とビジネス運営における脆弱性、脅威、リスクの継続的かつリアルタイムの把握が必要です。

#### 継続的なコンプライアンス監視

プロアクティブなサイバーリスク管理は、リスクの継続的な発見、関係性の把握をサポートします。加えて、継続的な監視は、すべてのコンプライアンス要件に対して適用する必要があります。

#### ツールの統合

多くの組織は、ツールの乱立、シャドーIT、管理外の資産を抱えており、この全てがリスクの効果的な管理を妨げています。ツールを完全に統合できない場合でも、少なくとも収集したデータは単一のビューに統合されるべきです。

# 02 優先順位付け

すべてを優先してしまっては、何も優先事項ではありません。最初に対処すべきリスクの情報を把握することが重要です。

## 必要とされるのは...

### 継続的リスク評価

継続的な監視で大量の脆弱性を発見することはできますが、それらすべてが同じレベルのリスクをもたらすわけではありません。サイバーリスク管理を運用に結びつけることは、最新の脅威インテリジェンス、脆弱性検索、リアルタイムの資産管理の情報に基づいて、リスクを継続的に再評価し、再度優先順位付けすることを意味します。AIを活用したツールは、リスクデータとそのビジネスへの重要性へ関連付けをサポートします。

### Cyber Risk Quantification (CRQ)

CRQは、優先順位付けにとどまらず、特定のサイバーリスクに関連する侵害、攻撃、または損失のビジネスへの影響の可能性を算出します。これにより組織全体の戦略にプロアクティブな意思決定を統一させ、サイバーセキュリティをビジネスの中核に革新させるサポートを提供します。

# 03 軽減策

攻撃者のスピードに、軽減策が遅れてはなりません。発生したインシデントに対処するだけでなく、リスク対策のためのプロアクティブな戦略が不可欠で、これこそが侵害の発生を防ぐことができます。

## 必要とされるのは...

### 迅速かつ積極的な軽減

優先度高の脆弱性は可能な限り迅速に対処する必要があります。ゼロトラストアーキテクチャの導入、パッチの自動化、リアルタイムでの脅威への積極的な対応も積極的なリスク軽減にもつながります。

### 検証とフィードバック

セキュリティ担当部門は、サイバーリスク軽減の対策が効果的であるとただ信じるだけでは済まされません。取るべきすべてのステップは検証される必要があり、成果が出ていない場合には、戦略を即座に見直す必要があります。

### 自動化

効果的な優先順位付けにより、最速で行動を取る必要があるかを判断します。自動化されたプレイブックとツールが、このプロセスを劇的に加速します。自律的なAIを含む最新技術を活用したプロアクティブなサイバーセキュリティソリューションや機能が、セキュリティ担当部門によるリスクの優先順位付けと対処、リソースと人員の負担軽減をサポートします。

# サイバーリスク成熟のための道筋

プロアクティブなサイバーリスク管理の3つの柱を理解することは、重要な出発点です。どのようにこの柱を運用に結びつけし、組織にプロアクティブなサイバーセキュリティを組み込むかが、多くのCISOにとっての次の課題です。これは現在の段階を把握することから始まる、段階的な道筋です。

## 01
## リアクティブ型

ほとんどの組織は、この段階からプロセスが始まります。

脅威とエクスポージャの積極的な監視へのシフト

## 02
## 戦術型

戦術的な行動とは、組織のサイバーリスクへのエクスポージャを管理することです。

### リアクティブ型を示す指標:

- 大量のインシデンとアラートで、セキュリティ担当部門が疲れ切っている
- 資産、脅威、リスクの可視化が不十分
- 脆弱性の修正、侵害への対応に注力
- アラートに効果的に対処するための関連性の把握が不十分
- ツールとサイロが多すぎる
- CVEスコアに基づくパッチ適用
- 不完全なインベントリ、スプレッドシートベースの管理

このような環境では、インシデント対応に時間がかり、また費用も嵩みます。攻撃者は発見されずに潜伏する機会に恵まれており、コンプライアンス対応も、実際のリスクではなく、チェックリストに基づいて進められています。

### 戦術的な取り組みによるメリットもありますが、次の理由により制限されています:

- 手動プロセス
- 一貫性のない優先度づけ、本来のリスクではなく、CVSSのスコアが高い脆弱性を追求
- すでに有効でないパッチ
- セキュリティとITの分散

改善されたインサイトによるメリットもありながら戦術型から脱却できないという点は、セキュリティ対策部門が課題に先んじるのではなく、あくまで後追いしているということを意味しています。これでは脅威に圧倒され、見落とすリスクを増加させてしまいます。

続けてお読みください →

リスクベースの
エクスポージャ管理
への移行

# 03
## リスク主導型

リスク主導の組織におけるサイバーセキュリティはリスクの把握に支えられ、リスクを軽減することを目的としています。

戦略的、継続的な
リスク管理への移行

# 04
## プロアクティブ型

この段階では、可視化、優先度づけ、軽減のための戦略が連携するようになります。これがリスクエクスポージャ及びビジネスへの影響の可能性を最小化するための、検知/把握、評価、戦略的な対応のサイクルです。

### これには以下が含まれます：

- リスクベースのセキュリティフレームワーク
- 設定や相互接続、脆弱性に基づく、サイバーリスクスコアの自動化、アセットごとのリスクレベル決定
- ビジネスとの関連性における、シナリオベースのサイバーリスクの理解のために、リスクを自動的に定量化
- 意思決定を導くリスクベースの優先順位付け
- 自動修復とコンプライアンス管理

ソリューションとツールの自動化により、攻撃対象領域の状態のリアルタイムビューを維持。加えて、脅威インテリジェンスにより、既知、未知およびゼロデイ脅威への対応をサポート

事実に基づいた脅威の報告ではなく、AIおよび自動化された、事前に脅威を予測、対処する、プロアクティブなサイバーリスク管理

リスクがビジネスに与える影響に関するインサイトと、継続的な監視および測定によってプロアクティブなセキュリティを確保している組織は、サイバーセキュリティのビジネスへの影響を定量化し、その価値を実践することができます。サイバーセキュリティは、継続的なデジタル変革を支える存在となり、イノベーションを保護・支援しながら、顧客の信頼を維持します。

### その他のメリット：

- ビジネス、イノベーションの目標に沿ったサイバーセキュリティ
- 迅速で自動化された保護と、情報に基づいた意思決定
- サイバーリスクと保護対策に関する適切な報告、会話により、サイバーセキュリティを経営層のリスク管理に連携できる

**92%** **リスク主導型のアプローチにより、トレンドマイクロのお客様におけるランサムウェアの可能性を92%低減し、リスクスコアを業界平均以下に引き下げた。[3]**

# CISOに支持されたベストプラクティス

主要な要件を満たし、各プロセスを乗り越えてもなお、サイバーリスク管理を成功に導くためにはいくつかの要素があります。

## リスクのみに焦点を置く対策を避ける

サイバーリスクの管理には、集中力、実践、統制が必要です。リスクに関する習熟度が低い組織では、実施しているセキュリティ対策や活動では測定可能な方法でリスクを削減できない」、「上層部に伝達されるにつれて、リスクの報告の意味が薄れていっている」と感じられている状況が散見されます。

最適な結果に結びつかないと考えられるサイバーセキュリティ活動やプロセスを特定し、測定可能な、データに基づいた意思決定を可能な限り達成することが必要です。

※ 訳者注
関係者全体でリスクを数値などのデータとして共有、データに基づく対策の実施が可能なリスク管理が必要。

## 経営層の賛同を得る

サイバーセキュリティを重視する経営層の方針が、サイバーセキュリティ管理の実装、長期的な効果に大きな影響を与えることが多くみられます。経営層の賛同はプロアクティブなセキュリティソリューションへの投資に対する承認のみを指すのではなく、リスク管理を組織におけるサイバーセキュリティの文化、考え方の一部として、組織内に浸透させることを意味しています。

これを実践するためには、成果主導の指標（ODM：Outcome-drive Metrics）や保護レベルに関する同意（Protection-level Agreement）など、サイバーリスクエクスポージャ管理のための具体的なビジネスケースの設定がCISOには求められます。またサイバーセキュリティの課題に関する密なコミュニケーション、責任説明も必要とされます。

## 「コンプライアンス対応済み」は「安全である」とは異なる

サイバーセキュリティのポリシーや、データ保護に関する法律や法規制への準拠は、非常に重要です。しかしコンプライアンス要件を満たすことが、組織のセキュリティ状態そのものを強化するものではありません。
お客様組織が直面する実際のリスクを理解することが非常に重要で、統制に基づき、優先度づけを行いながら対処することも非常に重要となります。

## シミュレーションを活用する

現在の攻撃対象領域およびネットワーク環境の監視に加えて、モデルやシミュレーションによって潜在的な脆弱性を明らかにし、セキュリティインシデントの影響を乗り越え、起こりうる結果を適切に把握することが可能になります。このような取り組みには、仮想的なレッドチーム演習、ペネトレーションテスト、攻撃シミュレーション、モンテカルロシミュレーションなどを例に挙げることができます。特に後者はITを活用したランダムなシナリオのテストを可能にします。

AI、機械学習、確率指標（Probability Indicator）、デジタルツインがこの観点で利用可能な技術として存在しており、リスクに関する会話の立脚点を提供するとともに、経営層を会話に参加させる仕組みを提供する支援として活用できます。

# サイバーリスク管理の明確なビジョン

サイバーリスクは今日の組織にとって重要な戦略的懸念事項です。つまり、CISOはサイバーリスクについて、ITの観点にとどまらず、それがビジネスにどのように影響するのか、戦略的に伝達することが期待されています。リスクを継続的、プロアクティブ、そして計測可能な方法で管理する必要があるということです。

上記の命題を達成するためには、攻撃対象領域全体の可視化、リスクの迅速かつ効果的な優先度づけ、エクスポージャを最小化し、最も問題の大きいリスクを削減することが求められます。

このような対策を一足飛びに実現することは困難です。サイバーリスク成熟化のプロセスは長期に渡り、また継続が必要です。お客様の現状のリスク状態の把握から開始し、プロアクティブなセキュリティ戦略の段階的な実装に着手していただくことで、攻撃者の先を見越した対策が可能になります。

## Trend Vision One™

**サイバーリスクエクスポージャ管理、セキュリティ運用のための機能、多層防御を一元的に提供する、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り、これまで以上の可視化、正確な優先度づけ、自動的なリスク軽減を提供し、脅威の予見、防止をサポートします。**

**Trend Vision Oneの詳細、**
**お客様のサイバーリスクエクスポージャ管理に**
**どのようにお役立ていただけるか、**
**ぜひ体験版でご確認ください**

出典:
[1] ESG Research Brief: Continuous Cyber Assets Analysis is Key to Effective Risk Mitigation and Threat Management, January 2025
[2] Analysis Perspective: Worldwide SIEM, Exposure Management, and AI-Related Technologies, IDC, September 2024, Doc # US52584624
[3] Trend™ Research blog: Anubis: A Closer Look at an Emerging Ransomware with Built-in Wiper, June 2025

Copyright ©2025 Trend Micro Inc. All rights reserved.
[EBK00_Risk_Never_Sleeps_250730US] TrendMicro.com