

# 継続的エクスポージャー管理 XM Cyber

CTEMに基づき、リスクの優先順位付けと  
迅速な修正を支援するプラットフォーム

攻撃者視点でのシミュレーションを通じて、企業の重要資産に至る攻撃経路を可視化し、リスクの優先順位付けと修正を支援するプラットフォームです。オンプレミスやクラウド環境を含むハイブリッド環境全体を対象とし、脆弱性や設定ミス、アイデンティティの問題を検出することで、効率的なセキュリティ態勢の改善を実現します。

## ソリューションの特長

### 特長 1 包括的にエクスポージャーを検出

脆弱性、設定ミス、クレデンシャル、クラウド、ADなどの高リスクな権限付与を継続的かつ網羅的に検出

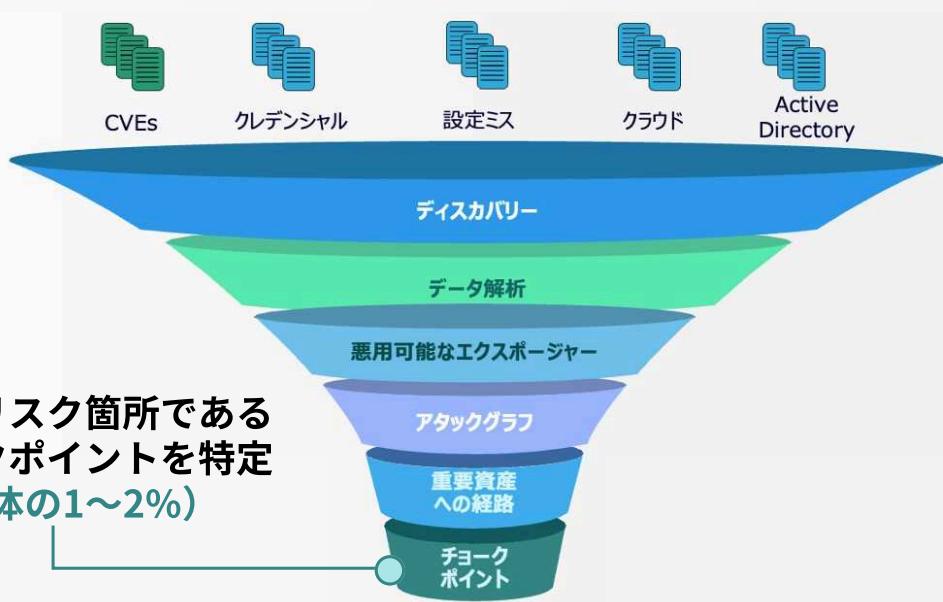
### 特長 2 影響度に応じて優先順位付け

重要資産に対して影響度の最も高いポイントを特定・優先順位付けし対処することでリスク低減の効果を最大化

### 特長 3 リスク監査や経営報告への活用

監査や経営に対し、重要資産への影響度などビジネスリスクを報告することで、  
予防に向けたアクションやKPI報告に活用

## ソリューションイメージ



サイバーリスクを継続的に可視化し  
優先順位付することで脅威を未然に防ぐ

## 利用イメージ

### 4. 再評価しセキュリティレベルをスコアリング

継続的に組織全体のセキュリティ状況を解析  
数値で見える化し、最新の状況を確認



### 1. 複合的なリスクを検出

組織内のエクスポートヤーを洗い出し  
リスクがどこに潜むかを特定



### 3. 修正方法を具体的にご案内

優先順位に応じた修正箇所に対し、  
修正方法をマニュアルレベルでご案内



### 2. アタックパスにより優先順位づけ

効率的にラテラル・ムーブメントを遮断できる  
踏み台地点や、重要資産への経路を特定



## ソリューションメニュー

### XM CEM (継続的エクスポートヤー管理)

#### XM アタックグラフ解析™

#### XM アタックパスマネジメント

XM ECM  
脅威インテリジェンス  
(リーククレデンシャル)

XM EASM  
外部アタックサーフェス  
マネジメント

XM VRM  
脆弱性管理

XM SCM  
コンプライアンス  
チェック SSPM

XM CDR  
脅威検出と対応

## POC概要

目的	本番環境でのXM Cyberの検証 各種手続きや操作性の確認、および攻撃経路の可視化
POC環境 ご利用期間	1ヵ月半～2ヵ月
対象	(1) ユーザ端末：ワークステーション&サーバ (2) パブリッククラウド
提供モデル	クラウドサービス

留意事項  XM Cyber社とのNDA締結が必要となります。

提供期間終了後、評価環境は初期化されます。



IIJ Global

### お問い合わせ

株式会社IIJグローバルソリューションズ  
E-Mail : info@iijglobal.co.jp  
URL : www.iijglobal.co.jp

- ・本内容は、予告なく変更することがあります。（2025年3月作成）
- ・記載されている企策名あるいは製品名は、一般に各社の商標または登録商標です。

