シスコの XDR（Extended Detection and Response）ソリューション

Cisco XDR

巧妙化を続けるサイバー攻撃、サイロ化するセキュリティ対策、膨大なアラート——
ネットワーク運用チーム（NetOps）やセキュリティ運用チーム（SecOps）に要求されるミッションは近年ますます過酷なものとなり、
組織が抱えるリスクもまた増大しています。

シスコが満を持して投入する XDR（Extended Detection and Response）は、この困難な状況を一変させるソリューションです。
サイバーセキュリティ業界をリードする広範な製品ポートフォリオを有するという、シスコならではの優位性を背景に、
ネットワーク運用チームやセキュリティ運用チームの次のようなニーズを満たすように設計された、統合プラットフォームを提供します。

- 攻撃を早期に検知
- 調査時間を短縮
- 対応時間を短縮・自動化
- ビジネスへの影響が大きい順に対処
- 影響を受けるアセットを正確に特定

ネットワーク運用チームやセキュリティ運用チームの課題

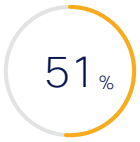
巧妙化を続けるサイバー攻撃

マルウェアの高度化、攻撃者が検出を回避する技術の向上、Internet of Things（IoT）やクラウドサービスの拡大に伴って発生する脆弱性の悪用など、サイバー攻撃が巧妙化を続けています。

情報セキュリティ 10 大脅威 2023 脅威ランキング（「組織」向け脅威） *1

順位	「組織」向け脅威	昨年順位
1 位	ランサムウェアによる被害	1 位
2 位	サプライチェーンの弱点を悪用した攻撃	4 位
3 位	標的型攻撃による機密情報の窃取	2 位
4 位	内部不正による情報漏洩	6 位
5 位	テレワークなどのニューノーマルな働き方を狙った攻撃	3 位
6 位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	
7 位	ビジネスメール詐欺による金銭被害	5 位
8 位	脆弱性対策情報の公開に伴う悪用増加	10 位
9 位	不注意による情報漏洩などの被害	9 位
10 位	犯罪のビジネス化（アンダーグラウンドサービス）	

たとえば、IPA が『**情報セキュリティ 10 大脅威 2023［組織編］**』で選出したランキングでは、「ランサムウェアによる被害」とともに「サプライチェーンの弱点を悪用した攻撃」や「標的型攻撃による機密情報の窃取」「修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）」「脆弱性対策情報の公開に伴う悪用増加」がランクインしています *1。これらがまさに、巧妙化を続ける攻撃の典型例です。一方、Enterprise Strategy Group（ESG）による調査では、セキュリティ担当者の 51% が「現在使用しているツールでは高度な脅威を検出および調査することが難しい」と回答しています *2。



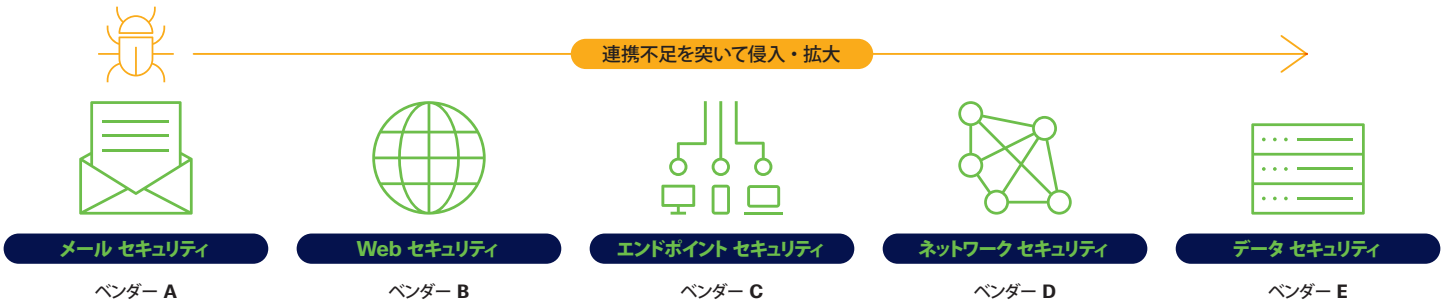
のセキュリティ担当者が
現在使用しているツールでは高度な脅威を検出
および調査することが難しいと感じている *2

*1　出典：IPA『**情報セキュリティ 10 大脅威 2023［組織編］**』。
*2　出典：Enterprise Strategy Group. *SOC Modernization and the Role of XDR*.

サイロ化するセキュリティ対策

ほとんどの組織は、マルチベンダーによる複数のソリューションでセキュリティインフラを構築しています *1。ところが多くの場合、異なるベンダーによるソリューション間ではデータやテレメトリを共有できず、さらに互いに連携しない複数の管理コンソールで運用せざるをえないなど、セキュリティ対策のサイロ化をもたらしています。

セキュリティ対策のサイロ化は、組織にとって深刻な状況そのものです。互いに孤立したセキュリティ対策の「隙間」あるいは「盲点」は攻撃者の格好のターゲットとなり、攻撃の検知を遅らせます。また、脅威の全体像を把握することが困難であることから、脅威の影響が及ぶ範囲の調査や対応を遅らせ、場合によっては不完全な対応にもつながります。



*1　ESG による調査では、54% の組織が 26 以上のセキュリティツールを使用（出典：Enterprise Strategy Group. *ESG Complete Survey Results: SOC Modernization and the Role of XDR*）。

膨大なアラート

ネットワーク運用チームやセキュリティ運用チームにとって「アラート疲れ」という言葉は単なる比喩ではありません。攻撃を早期に検知するためにも、真に重大な脅威から優先して対処するためにも、アラートの処理は非常にストレスフルな作業であり、そのストレスは増しています。ESG による調査では、セキュリティ運用が 2 年前に比べて困難になった理由として、セキュリティ担当者の 37% が「アラートの量や複雑さが増している」と回答しています *1。

しかし、アラートのすべてが重要というわけではありません。Verizon が FBI Internet Criminal Complaint Center（IC3）に報告された損失を集計したところ、ビジネスメール詐欺（BEC）の 42%、コンピュータデータ漏洩（CDB）の 76%、ランサムウェア攻撃の 90% が金銭的損失をもたらさなかったことがわかりました *2。一方で、Cyentia Institute が Advisen のサイバー損失データに基づいて算出したところ、サイバー損失が発生した場合の 10% は 2,000 万ドルを超えたこともわかりました *3。

このようなインシデントの実態から、限られたリソースで優先して対処すべきアラートをいかに判別するかが重要であることがわかります。

のセキュリティ担当者が
アラートの量や複雑さが増していると感じている *1

… が実質的に無害 *2 な一方で

損失が発生した場合の 10% は **2,000** 万ドル超の被害

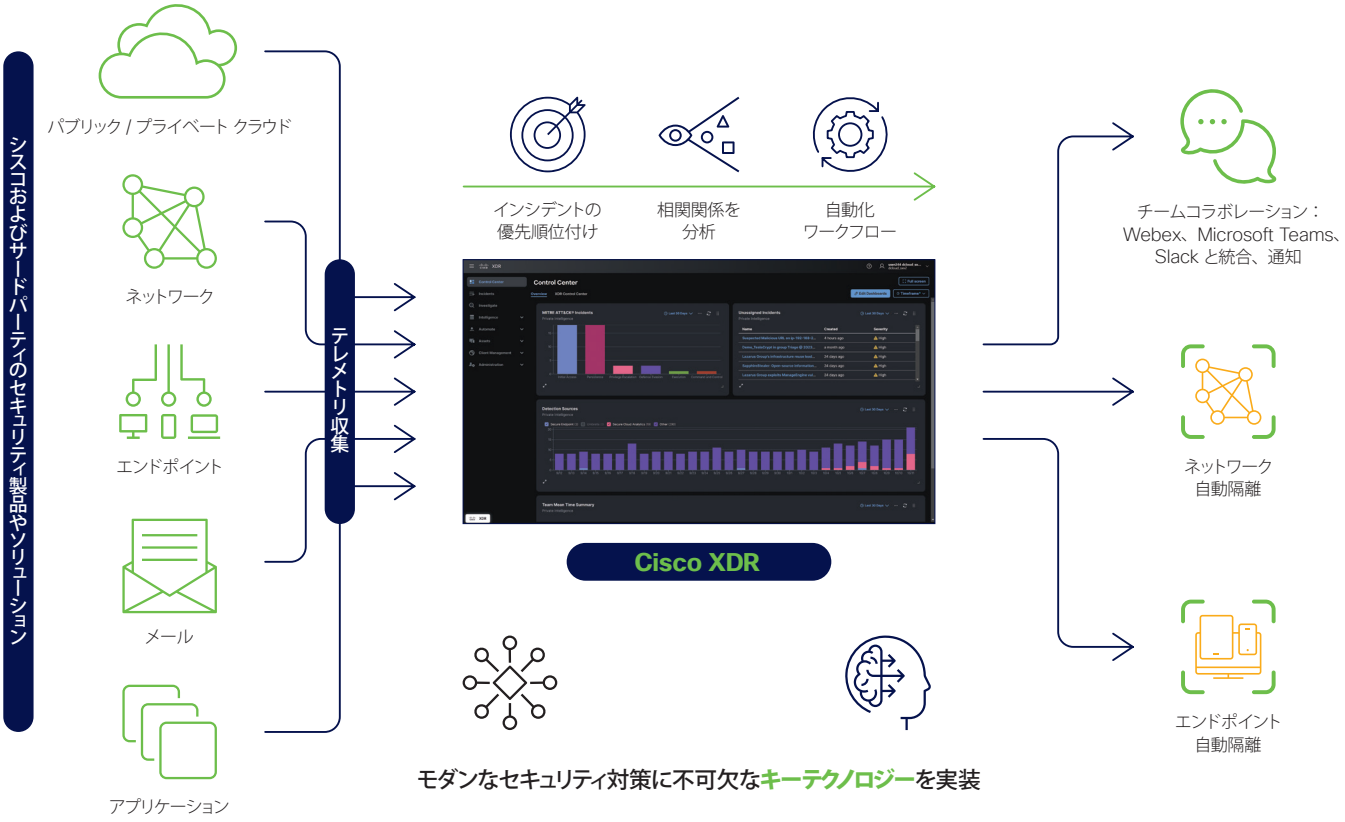
*1　出典：Enterprise Strategy Group. *SOC Modernization and the Role of XDR*.　*2　出典：Verizon. *2021 Data Breach Investigations Report*.
*3　出典：Cyentia Institute. *The Information Risk Insights Study (IRIS) 20/20*.

Cisco XDR の概要と特長

シンプルかつ効果的な運用を実現するセキュリティ統合プラットフォーム

Cisco XDR は、ネットワーク運用チームやセキュリティ運用チームの仕事を一変させるクラウドベースのソリューションです。運用を劇的にシンプル化すると同時に、最も高度な攻撃の早期検知、インシデントがビジネスに及ぼす影響をスコアで判別できるアラート、見落としのない短時間の調査、影響範囲の正確な特定、対応時間の短縮と自動化など、比類なく効果的な運用を実現します。

クロスドメインテレメトリと AI および ML（機械学習）を組み合わせたアプローチによって、盲点のないセキュリティインフラ構築をサポート。さらにビルトインの自動化ワークフロー、ステップバイステップのガイド付きで対応方法を推奨するプレイブックなど、運用チームの負担を軽減する機能を導入してすぐに活用できます。



モダンなセキュリティ対策に不可欠な<u>キーテクノロジー</u>を実装

クロスドメインテレメトリ

シスコのセキュリティ製品ポートフォリオだけでなく、戦略的パートナーの各種製品やソリューションもサポート。これら複数のソースから自動的にテレメトリを収集、統合、関連付けて、単一の管理コンソールで可視化します。

AI & ML（機械学習）

テレメトリの相関分析による高度な脅威の検出、誤検知の軽減、セキュリティリスクとビジネスリスクに基づくインシデントの優先順位付けなど、AI や ML（機械学習）を随所で活用しています。

Cisco XDR 対応シスコ製品（抜粋 *1）

カテゴリ	製品
エンドポイント セキュリティ（EDR）	Cisco Secure Endpoint
メール セキュリティ	Cisco Secure Email
アプリケーション / アイデンティティ	Cisco Duo
	Cisco Identity Services Engine（ISE）
	Cisco Orbital
	Cisco Secure Web Appliance
	Cisco Umbrella

カテゴリ	製品
次世代ファイアウォール（NGFW）	Cisco Secure Firewall
ネットワーク可視化 / 分析（NDR）	Cisco Secure Cloud Analytics
	Cisco Secure Network Analytics

*1　詳細は「Cisco XDR Integrations」（www.cisco.com/c/en/us/products/security/xdr/integrations.html）を参照。

Cisco XDR 戦略的パートナー製品 / ソリューション（対応予定を含む抜粋 *1）

カテゴリ	製品 / ソリューション
エンドポイント セキュリティ（EDR）	CrowdStrike Falcon Insight
	Cybereason Endpoint Detection and Response
	Microsoft Defender for Endpoint
	Palo Alto Networks Cortex
	SentinelOne Singularity
	Trend Vision One
メール セキュリティ	Microsoft Defender for Office 365
	Proofpoint Email Protection
アプリケーション / アイデンティティ	Microsoft Entra ID（旧 Azure Active Directory）

カテゴリ	製品 / ソリューション
次世代ファイアウォール（NGFW）	Check Point Security Gateway & Management
	Fortinet Fortigate
	Palo Alto Networks Next-Generation Firewall
ネットワーク可視化 / 分析（NDR）	Darktrace Respond & Detect
	ExtraHop Reveal(x) 360
セキュリティ情報イベント管理（SIEM）	Microsoft Sentinel
	Splunk
パブリッククラウド	Amazon Web Services（AWS）
	Google Cloud Platform（GCP）
	Microsoft Azure

*1　詳細は「Cisco XDR Integrations」（www.cisco.com/c/en/us/products/security/xdr/integrations.html）を参照。

Cisco XDR 製品型番

Cisco XDR は、組織の大小を問わず簡単に導入および拡張できる、SaaS モデルで提供されます。
組織のユーザー数に応じたライセンスを 1 ～ 5 年のサブスクリプションとして契約します。

Cisco XDR サブスクリプション

製品型番	製品説明
XDR-SEC-SUB	XDR サブスクリプション

Cisco XDR ライセンス *1

製品型番	製品説明	サブスクリプション期間	ライセンス単位	最低数量
XDR-ESS*2	XDR Essentials ライセンス	1 ～ 5 年	ユーザー	100 ～
XDR-ADV*2	XDR Advantage ライセンス	1 ～ 5 年	ユーザー	100 ～
XDR-PRE*2	XDR Premier ライセンス	1 ～ 5 年	ユーザー	100 ～

*1　CCW では XDR-SEC-SUB が必要。詳細は発注ガイドを参照。
*2　デフォルトでは US データセンターを利用。APJC データセンターを利用する場合は -AP 製品型番、EMEA データセンターを利用する場合は -EU 製品型番を選択。

Cisco XDR アドオンライセンス *1

製品型番	製品説明	サブスクリプション期間	ライセンス単位	最低数量
XDR-ING-1GB*2	1 ユーザーあたり毎月 1 GB の追加データ収集ライセンス *3	1 ～ 5 年	ユーザー	100 ～
XDR-DATARET-180*2	1 ユーザーあたり 180 日間のデータ保持ライセンス *4	1 ～ 5 年	ユーザー×データ収集量	200 ～
XDR-DATARET-365*2	1 ユーザーあたり 365 日間のデータ保持ライセンス *4	1 ～ 5 年	ユーザー×データ収集量	200 ～

*1　CCW では XDR-SEC-SUB が必要。詳細は発注ガイドを参照。
*2　デフォルトでは US データセンターを利用。APJC データセンターを利用する場合は -AP 製品型番、EMEA データセンターを利用する場合は -EU 製品型番を選択。
*3　デフォルトは 2 GB。　*4　デフォルトは 90 日間。

Cisco XDR 製品パッケージ機能比較

機能	Essentials	Advantage	Premier
オンプレミス / クラウドの不正なエンティティを検出できる、NDR（Network Detection and Response）機能	✓	✓	✓
膨大なイベントとテレメトリを収集できる、ビルトインのセキュリティ アナリティクス & コリレーション エンジン	✓	✓	✓
ビルトインの Cisco Talos を含む複数の脅威インテリジェンスを組み合わせてコンテキストを取得、脅威を評価	✓	✓	✓
包括的ながらシンプルなユーザーエクスペリエンスで利用できる、高度な脅威ハンティング	✓	✓	✓
インシデントに迅速に対応できる、ビルトインの対応プレイブック	✓	✓	✓
インシデントに対する完了済み作業の確認、重要な情報に関するメモの投稿など、チームコラボレーション機能	✓	✓	✓
インシデントに対する優先度スコアの割り当て（優先順位付け）と関連情報の自動追加	✓	✓	✓
デバイスインベントリおよびポスチャデータを収集	✓	✓	✓
ユーザーインベントリおよびポスチャデータの収集	✓	✓	✓
ノーコード / ローコードで構築できる、自動化ワークフロー	✓	✓	✓
実績豊富なプリセットとして利用できるワークフローのライブラリ	✓	✓	✓
サードパーティのセキュリティツールを統合		✓	✓
Cisco Software Support Services（SWSS）Enhanced	✓	✓	✓
シスコのマネージドサービス［Cisco Managed Detection and Response（MDR）］			✓
Cisco Talos インシデント対応チーム（CTIR）			✓
シスコ テクニカル セキュリティアセスメント（CTSA）			✓

Cisco XDR
www.cisco.com/site/jp/ja/products/security/xdr/index.html

シスコ お問い合わせ窓口

自社導入をご検討されているお客様へのお問い合わせ窓口です。
製品に関して ｜ サービスに関して ｜ 各種キャンペーンに関して ｜ お見積依頼 ｜ 一般的なご質問

お問い合わせ先

お電話での問い合わせ
平日 9:00 - 17:00
0120-092-255

お問い合わせウェブフォーム
cisco.com/jp/go/vdc_callback

シスコシステムズ合同会社
〒 107-6227 東京都港区赤坂 9-7-1 ミッドタウン・タワー
cisco.com/jp

2398-2310-01A-TO