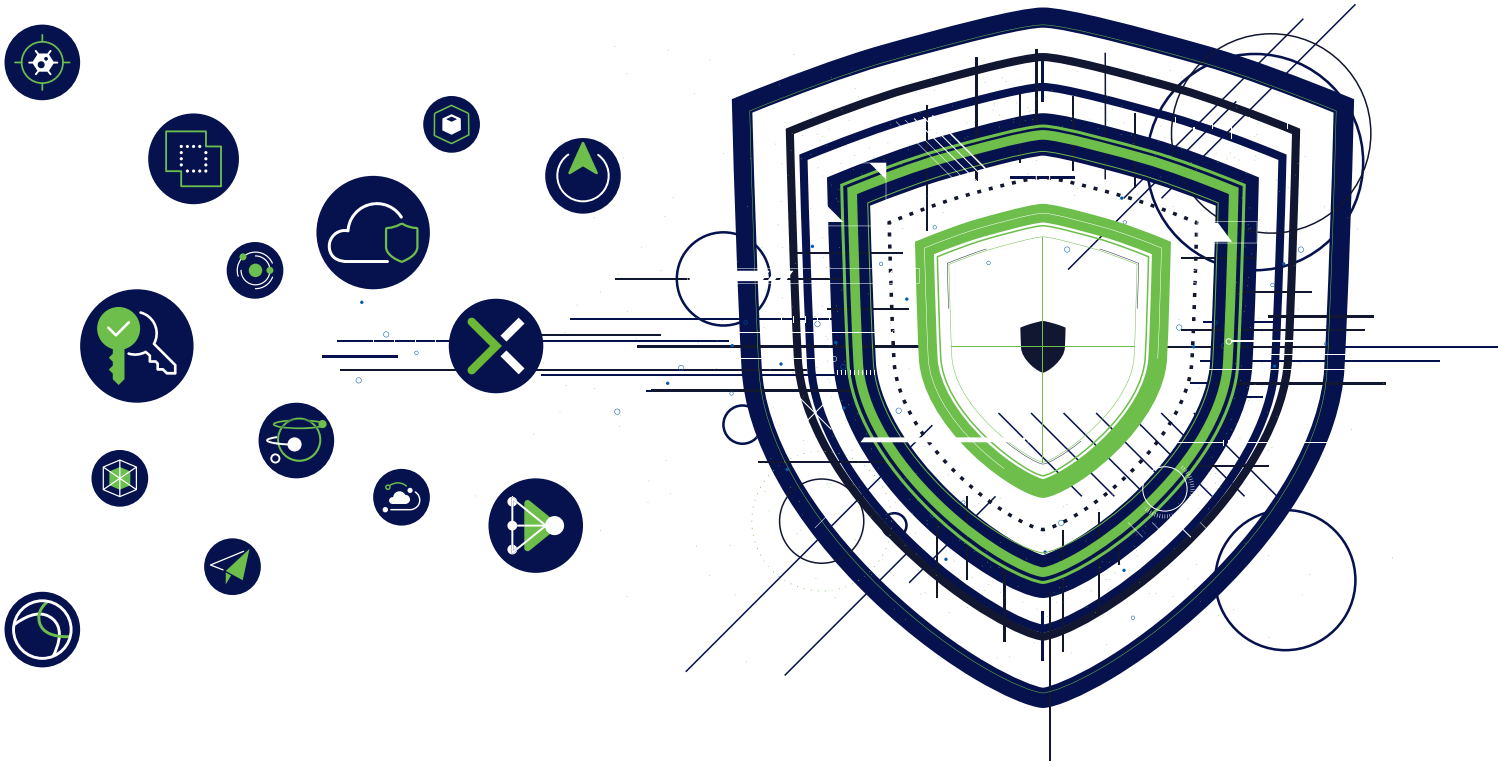
シスコ セキュリティ製品ガイド

場所を問わず、つないで、守る
シスコならではのセキュリティ



つないで、守る。つながるから、守られる。
シスコがネットワーク分野で積み重ねてきた実績は、サイバーセキュリティ分野で積み重ねてきた実績でもあります。
包括的なネットワーキングの知見を背景に、包括的なセキュリティを提供できるのは、シスコだけの強みです。
シスコが自信をもって提供するセキュリティ製品を、厳選して紹介します。

2025 年 5 月版

Cisco Secure Access

SSE（セキュリティサービスエッジ）

あらゆるインターネットアクセスとアプリケーションアクセスを保護できる、フレキシブルかつシンプルなソリューション

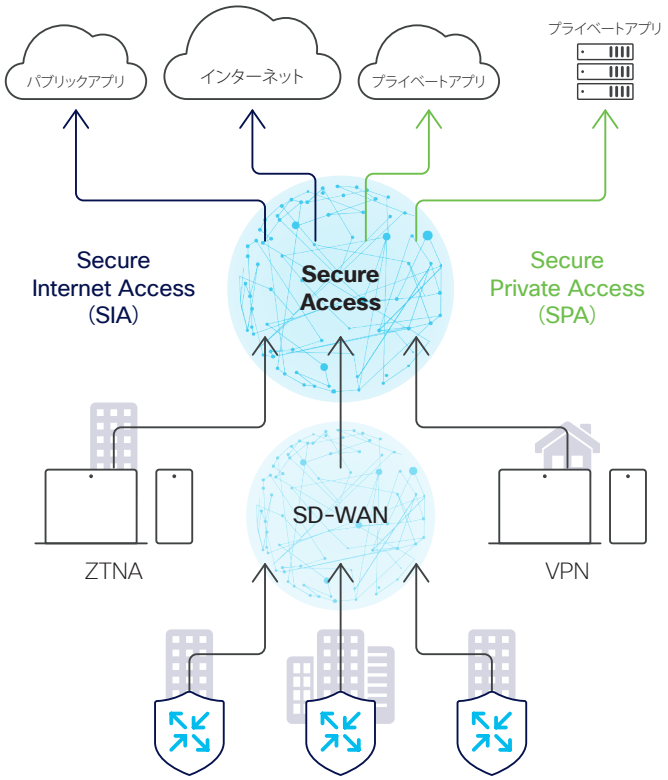
テレワークやハイブリッドワークの普及などによって、企業のネットワークおよびセキュリティに求められる要件は激変しました。モダンな働き方を指向する社員には、デバイスや場所を問わず、インターネット、そして社内外のアプリケーションへの安全なアクセスを提供する必要があります。

このようなネットワークおよびセキュリティ要件に応えるフレームワークが SASE（Secure Access Service Edge）であり、**Cisco Secure Access** は、SASE で SSE（Security Service Edge；セキュリティサービスエッジ）として定義されたセキュリティサービス部分を提供するソリューションです。

SASE を提唱した Gartner 社は、ユーザーエクスペリエンスを損なわずに提供すべき SASE のコア機能として次の機能を挙げていますが [*1]、Cisco Secure Access はセキュリティ機能をまとめて提供することができます。

- **セキュア Web ゲートウェイ（SWG）** ✓
- **クラウドアクセスセキュリティ制御（CASB）** ✓
- **クラウド提供型ファイアウォール（CDFW、FWaaS）** ✓
- **機密データとマルウェアの検知** ✓
- **リモートブラウザ分離** ✓
- **ゼロトラスト ネットワーク アクセス（ZTNA）** ✓
- SD-WAN

*1　出典：Gartner. *2022 Strategic Roadmap for SASE Convergence*.



Cisco Secure Access 製品ポートフォリオ

Cisco Secure Access は、サブスクリプションモデルのクラウドサービスです。保護対象となる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。必要なセキュリティのレベルや範囲に応じて、次の 4 つの製品パッケージから選択することができます [*1]。

Secure Internet Access（SIA）Essentials

- DNS レイヤのセキュリティ
- SSL 対応インテリジェントおよびフル プロキシ
- ドメインおよび URL ベースの Web フィルタリング
- クラウドアプリの検出とブロック（アプリ別にユーザー操作を制御可能）
- レイヤ 3 & 4 ファイアウォール
- 危険なファイルをブロック
- 2 アプリまでのクラウドマルウェア保護
- 500 サンプル / 日までのクラウドサンドボックス（Secure Malware Analytics）
- リモートブラウザ分離（潜在的に危険なカテゴリの Web サイトのみ）
- 脅威インテリジェンス（Talos & Umbrella Investigate）
- デジタルエクスペリエンス モニタリング（ThousandEyes ベース）
- SD-WAN 統合
- ISE 統合

Secure Internet Access（SIA）Advantage

SIA Essentials に加えて

- レイヤ 7 ファイアウォールと侵入防御システム
- データ漏洩防止
- サードパーティの生成 AI 利用保護
- 無制限のクラウドマルウェア保護
- 無制限のクラウドサンドボックス（Secure Malware Analytics）
- リモートブラウザ分離

Secure Private Access（SPA）Essentials

- クライアントベース ZTNA
- クライアントレス ZTNA（HTTP/HTTPS）
- モバイルデバイス ZTNA
- VPN アクセス（VPNaaS）
- レイヤ 3 & 4 ファイアウォール
- 500 サンプル / 日までのクラウドサンドボックス（Secure Malware Analytics）
- 脅威インテリジェンス（Talos & Umbrella Investigate）
- デジタルエクスペリエンス モニタリング（ThousandEyes ベース）
- SD-WAN 統合
- ISE 統合

Secure Private Access（SPA）Advantage

SPA Essentials に加えて

- クライアントレス ZTNA（SSH/RDP）
- 侵入防御システム
- データ漏洩防止
- 無制限のクラウドサンドボックス（Secure Malware Analytics）

*1　SIA Essentials と SPA Advantage または SIA Advantage と SIA Essentials の組み合わせには非対応。

Cisco Umbrella

インターネットアクセスセキュリティ

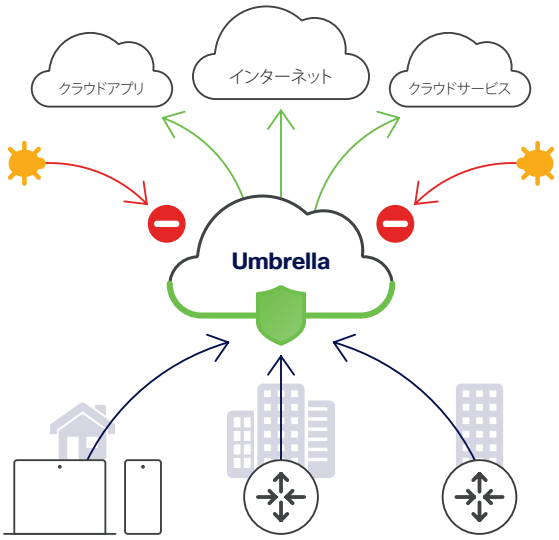
あらゆるインターネットアクセスを保護できる、最も効果的でシンプルなソリューション

インターネットにアクセスするデバイスや場所の多様化に伴って、ユーザーが脅威に遭遇するリスクは増大し、対策もまた複雑化しています。既存のセキュリティを確実に強化できるだけでなく、簡単に導入および運用管理できるソリューションが必要とされるようになりました。

Cisco Umbrella は、インターネット上の脅威をブロックするための最前線として機能する、最も効果的でシンプルなソリューションです。

インターネット利用に欠かせない DNS レイヤのセキュリティをベースにしているため、インターネットに接続するあらゆるデバイスに適用可能。本社、支社、自宅などの場所、移動中、VPN のオン / オフを問わず、インターネットにアクセスするあらゆるユーザーを保護できます。

Umbrella による DNS レイヤのセキュリティは、ルータや PC などの設定を少々変更するだけで、すぐに利用を開始することができます。専用の管理サーバーなどを所有する必要がなく、サブスクリプションモデルのクラウドサービスとして提供されるため、シンプルかつ短期間で導入可能です。さらに、次のような幅広いセキュリティを追加することもできます。



主な機能：DNS レイヤのセキュリティをベースに、幅広いセキュリティを提供

Cisco Umbrella は DNS レイヤのセキュリティをベースに、**セキュア Web ゲートウェイ**（Secure Web Gateway；SWG）、**クラウドアプリセキュリティ制御**（Cloud Access Security Broker；CASB）、**クラウド提供型ファイアウォール**（Cloud-Delivered FireWall；CDFW）など、幅広いセキュリティを提供します。インターネットアクセスを保護およびきめ細やかに制御するだけでなく、組織として未許可のクラウドアプリやサービスの利用を把握して制限する、クラウドベースのファイアウォールや IPS でも保護する、情報漏洩を検出および防止するなど、高度なセキュリティや多層防御を Umbrella だけで実現することができます。

Cisco Umbrella 製品ポートフォリオ

Cisco Umbrella は、サブスクリプションモデルのクラウドサービスです。保護対象となる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。必要なセキュリティのレベルや範囲に応じて、次の 4 つの製品パッケージから選択することができます。

DNS セキュリティ Essentials

- DNS レイヤのセキュリティ
- ドメインベースの Web フィルタリング
- クラウドアプリの検出とブロック

DNS セキュリティ Advantage

DNS セキュリティ Essentials に加えて

- SSL 対応インテリジェントプロキシ
- 危険なファイルをブロック（危険性が高いドメインのみ）
- 脅威インテリジェンス（Talos & Umbrella Investigate）

SIG Essentials

DNS セキュリティ Advantage に加えて

- SSL 対応フルプロキシ
- URL ベースの Web フィルタリング
- レイヤ 3 & 4 ファイアウォール
- 危険なファイルをブロック
- クラウドアプリの検出とブロック（アプリ別にユーザー操作を制御可能）
- リモートブラウザ分離（オプション）
- ユーザー組織専用の送信元 IP アドレス（オプション）

SIG Advantage

SIG Essentials に加えて

- レイヤ 7 ファイアウォールと侵入防御システム *1
- 無制限のクラウドサンドボックス（Secure Malware Analytics）
- データ漏洩防止 *1

*1　Umbrella SIG アドオンライセンスで SIG Essentials に追加可能。

Cisco Duo

多要素認証

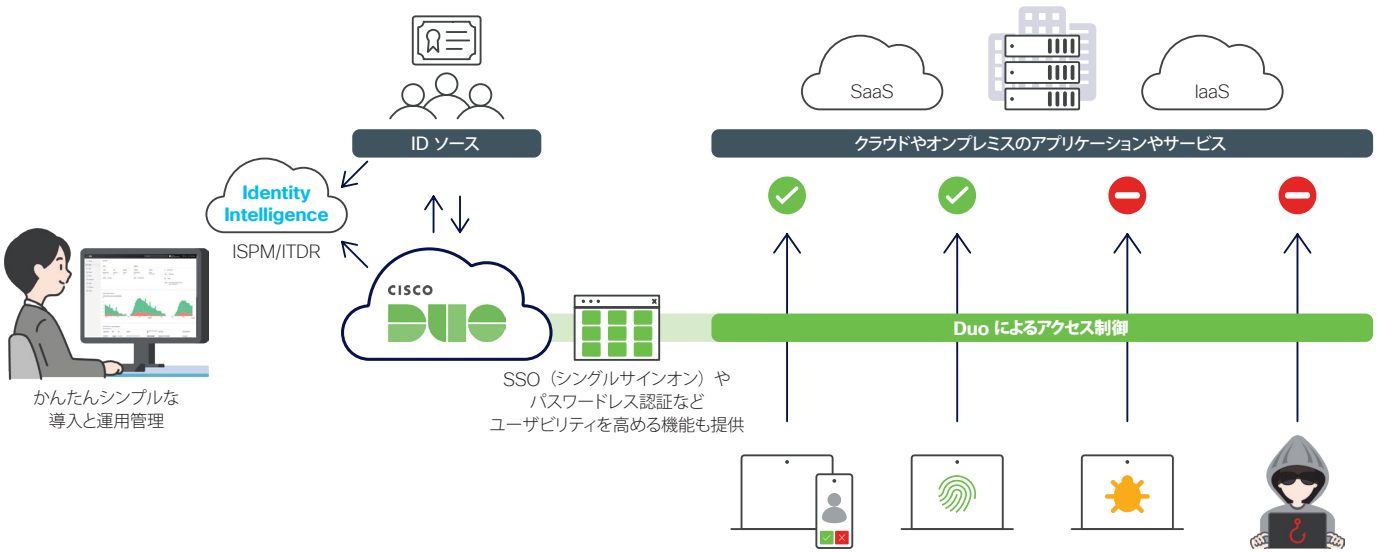
多要素認証をベースにした、鉄壁のアクセスセキュリティとアイデンティティセキュリティ

ID とパスワードだけに頼った認証方式では非常に危険であることがわかっています。たとえば、2024 年に都道府県警察が検挙した不正アクセスのうち、ID とパスワードの窃取によるものが検挙数の 90% 以上を占めていました[*1]。そのため、ID とパスワードによる 1 つ目の認証方式に所有者認証や生体認証のような 2 つ目以降の認証方式を追加する多要素認証、さらに万が一の窃取などに対応できる ID 管理が、ますます重要視されています。

*1 出典：警察庁・総務省・経済産業省
「令和 6 年 1 月 1 日（月）から同年 12 月 31 日（火）までの不正アクセス行為の発生状況」.

Cisco Duo は、業界をリードするゼロトラストアクセス（Zero Trust Access；ZTA）およびアイデンティティ（ID）セキュリティ ソリューションです。

多要素認証やデバイス可視化による健全性確認をベースにしたアクセス管理、多層防御、さらに機械学習によるリスクベース認証、AI 駆動型の ISPM（Identity Security Posture Management；ID セキュリティポスチャ管理）や ITDR（Identity Threat Detection and Response；ID 脅威検知 / 対応）など、最先端のテクノロジーによるアクセスおよび ID セキュリティを実現します。



主な機能

ユーザー認証
- 多要素認証（MFA）
- プッシュ通知フィッシング対策
- パスワードレス認証
- デスクトップ認証
- セキュアでシームレスな ログインエクスペリエンス
- ID ポスチャ / 脅威検知

デバイストラスト
- デバイス可視化
- 信頼済みエンドポイント（Trusted Endpoints）
- デバイスヘルス

認証 / アクセスポリシー
- リスクベース認証
- アクセスポリシー

シングルサインオンとリモートアクセス
- シングルサインオン（Duo SSO）
- リモートアクセス（Duo Network Gateway）

Cisco Duo 製品ポートフォリオ

Cisco Duo は、サブスクリプションモデルのクラウドサービスです。保護対象となる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。アクセス管理に必要な機能に応じて、次の 3 つの製品エディションから選択することができます。

Essentials
- 多要素認証（MFA）
- プッシュ通知フィッシング対策
- パスワードレス認証
- 信頼済みエンドポイント
- 基本的なデバイス可視化
- アクセスポリシー
- シングルサインオン（SSO）

Advantage
Essentials に加えて
- セキュアでシームレスなログインエクスペリエンス
- ID ポスチャ / 脅威検知
- 高度なデバイス可視化
- デバイスヘルス
- リスクベース認証
- 適応型アクセスポリシー

Premier
Advantage に加えて
- より高度なデバイスヘルス
- VPN レス リモートアクセス

Cisco Secure Firewall

ファイアウォール

ハイブリッドワークやマルチクラウド環境に最適な次世代ファイアウォール

Cisco Secure Firewall は、複雑化し、変化を続けるネットワークと脅威に対応できる、AI/ML 駆動型のファイアウォールです。

業界をリードする Snort 3 侵入防御システム（Intrusion Prevention System；IPS）や高度なマルウェア防御、TLS 1.3 で暗号化されたレイヤ 7 トラフィックを復号せずに可視化および制御できる Encrypted Visibility Engine（EVE）など、シスコ独自のセキュリティ機能だけでなく、世界最大の脅威インテリジェンスの 1 つである Cisco Talos による最新かつ最先端のデータベース、および最先端の AI と ML（機械学習）による脅威検知やポリシー最適化を活用して、ネットワークを保護できます。

物理、仮想、およびクラウドネイティブな各種ファイアウォールで構成される充実したポートフォリオによって、SD-WAN を含むモダンなユースケースに対応可能。それらをクラウドまたはオンプレミスで一元管理できるだけでなく、シスコの各種セキュリティ ソリューションを統合する XDR プラットフォーム Cisco XDR など、さまざまなシスコ セキュリティ製品と連携させて効率的に運用できます。

主な機能

Snort 3 侵入防御システム
最も巧妙な攻撃にも対抗できる
業界をリードする侵入防御システム

高度なマルウェア防御
マルウェアからネットワークを保護
万が一の感染時も遡って検知および追跡可能

暗号化されたトラフィックを復号せずに可視化
TLS 1.3 暗号化トラフィックを可視化
レイヤ 7 ルールを適用可能

世界最大の脅威インテリジェンス
Snort ルールセットなど
常に最新のデータベースで更新

AI/ML 駆動型
脅威の検知、ポリシーの最適化や管理など
随所で最先端の AI/ML を活用

物理および仮想ファイアウォール
ハードウェアアプライアンスだけでなく
クラウドネイティブなソフトウェアでも提供

セキュリティと SD-WAN を一元管理
オンプレミスまたはクラウドで
複数のファイアウォールを一元管理可能

XDR
Cisco XDR に統合可能
より迅速に脅威を検知、調査、対応可能

Cisco Secure Firewall 製品ポートフォリオ（物理ファイアウォール）

Secure Firewall 1200 シリーズ

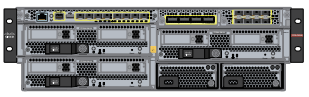
- 3 モデル（デスクトップ）
  3 モデル（1 RU）
- デスクトップ、1 RU
- FW + AVC スループット：
  最大 6.0 ～ 24.0 Gbps
- FW + AVC + IPS スループット：
  最大 6.0 ～ 18.0 Gbps
- TLS スループット：
  最大 1.0 ～ 4.1 Gbps
- IPsec VPN スループット：
  最大 5.0 ～ 22.0 Gbps
- IPsec VPN ピア：
  最大 200 ～ 1,500

Secure Firewall 3100 シリーズ

- 5 モデル（1 RU）
- FW + AVC スループット：
  最大 10.0 ～ 45.0 Gbps
- FW + AVC + IPS スループット：
  最大 10.0 ～ 45.0 Gbps
- TLS スループット：
  最大 3.2 ～ 11.5 Gbps
- IPsec VPN スループット：
  最大 5.5 ～ 39.4 Gbps
- IPsec VPN ピア：
  最大 2,000 ～ 20,000

Secure Firewall 4200 シリーズ

- 3 モデル（1 RU）
- FW + AVC スループット：
  最大 71.0 ～ 149.0 Gbps
- FW + AVC + IPS スループット：
  最大 71.0 ～ 147.0 Gbps
- TLS スループット：
  最大 20.0 ～ 45.0 Gbps
- IPsec VPN スループット：
  最大 51.0 ～ 148.0 Gbps
- IPsec VPN ピア：
  最大 20,000 ～ 30,000



Secure Firewall 4200 シリーズ

- 1 モデル（3 RU）
- FW + AVC スループット：
  最大 190.0 Gbps
- FW + AVC + IPS スループット：
  最大 190.0 Gbps
- TLS スループット：
  最大 28.0 Gbps
- IPsec VPN スループット：
  最大 110.0 Gbps
- IPsec VPN ピア：
  最大 60,000

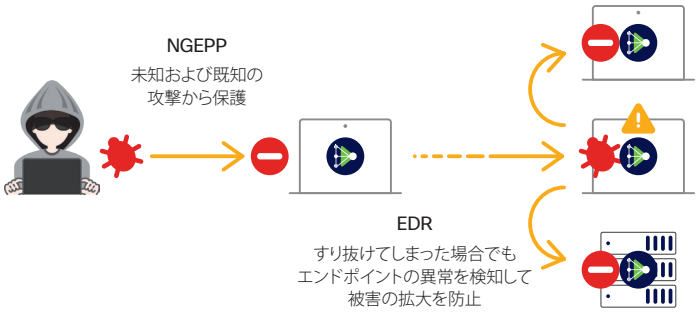
Cisco Secure Endpoint

エンドポイントセキュリティ

エンドポイントの保護から侵害の検知、調査、対応まで実現する、統合型エンドポイントセキュリティ

今日のサイバー攻撃では、いわゆるアンチウイルスソフトウェアを代表とするEPP（Endpoint Protection Platform）を簡単にすり抜けてしまうほど巧妙な攻撃も珍しくありません。

巧妙化を続けるランサムウェア攻撃や Emotet のように進化を続けるマルウェアに対抗するためには、たとえ未知の攻撃であっても防御できる対策、あるいは侵入や被害を迅速に検知して拡大を防げる対策が必要です。前者が NGEPP（Next Generation Endpoint Protection Platform）、後者が EDR（Endpoint Detection and Response）と呼ばれるセキュリティ対策です。



Cisco Secure Endpoint は、NGEPP と EDR を兼ね備えたエンドポイントセキュリティです。リリース以来、セキュリティのアナリストやテスト機関から、数々の高評価を得てきました[*1]。既知のマルウェアのデータパターン（シグネチャ）を検知する複数の防御エンジンや、未知のマルウェアも検出する機械学習ベースの分析エンジンなど、既知および未知の攻撃を防御可能。万が一、マルウェアの侵入を許してしまった場合でも、侵入経路や被害の影響度、影響範囲を把握して隔離するなど、迅速かつ適切に対応できます。

Secure Endpoint は、サーバーからデスクトップ PC、ノート PC やスマートフォンまで、幅広いエンドポイントにインストールできる Secure Endpoint コネクタと、脅威の監視と分析など、一元管理のプラットフォームとなる Secure Endpoint コンソールで構成されます。専用の管理サーバーを所有する必要がなく、サブスクリプションモデルのクラウドサービスとして提供されるため、シンプルかつ短期間で導入できるほか、導入後も機器の保守や老朽化に伴う更新費用がかかりません。

*1　出典：Cisco.com. *Secure Endpoint Third-Party Validation*.

主な機能：サイバー攻撃からの保護、攻撃の検知と調査、被害の拡大防止や再発防止などの対応まで、一貫してサポート

保護

- ファイルレピュテーションで既知の脅威をブロック
- シグネチャベースの防御エンジンで既知の脅威をブロック
- ポリモーフィック型マルウェアをブロック
- 機械学習ベースの分析エンジンで既知および未知のマルウェアをブロック
- エクスプロイトを防止
- ファイルやプロセスの疑わしいふるまいを検出、動作を防止
- スクリプトベースの攻撃をブロック
- USB デバイスを制御
- コネクタベースのファイアウォール機能

検知

- Talos によるクラウドベースの IoC（侵害の痕跡）で侵害を検知
- ユーザー定義の IoC（侵害の痕跡）で侵害を検知
- 少数しか存在しない実行ファイルを自動分析、被害が拡大する前に侵害を検知
- Vulnerability Management による脆弱性推論でリスクスコアを算出
- Orbital による事前に定義された 100 以上のクエリでエンドポイント内部をリアルタイムで調査

調査

- ダッシュボードで侵害の調査と対応を合理化
- イベント検出時のフォレンジック スナップショットでファイルおよびデバイスを追跡、攻撃の痕跡や侵害の影響範囲を特定
- コマンドライン可視化で攻撃の痕跡を特定
- ビルトインサンドボックスで動的なファイル分析
- Secure Malware Analytics によるクラウドサンドボックスで高度かつ動的なファイル分析
- エンドポイントを隔離
- リモートスクリプトでエンドポイントを自動隔離

対応

Cisco Secure Endpoint 製品ポートフォリオ

Cisco Secure Endpoint は、サブスクリプションモデルのクラウドサービスです。保護対象となるエンドポイント（デバイス）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。必要な NGEPP および EDR 機能に応じて、次の 3 つのライセンス階層から選択することができます。

Essentials

- 次世代アンチマルウェア
- 継続的なモニタリング：ファイルやプロセスの疑わしいふるまいを検知
- 動的なファイル分析
- エンドポイント隔離
- アプリケーション制御
- USB デバイス制御

Advantage

Essentials に加えて

- Orbital によるエンドポイント内部のリアルタイム調査
- Secure Malware Analytics クラウドによるサンドボクシング
- リスクベースの脆弱性対策
- ホストファイアウォール：コネクタベースのファイアウォール機能

Premier

Advantage に加えて

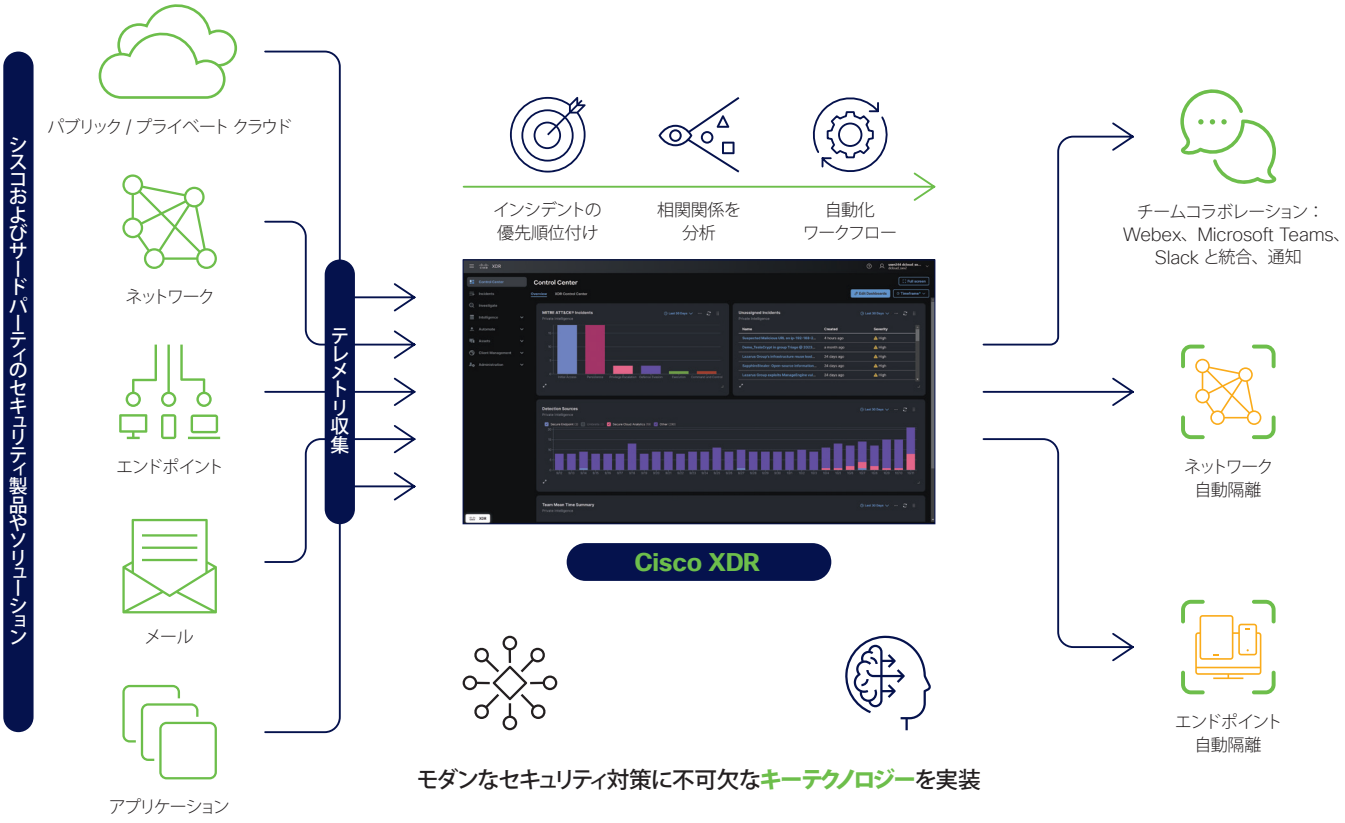
- Talos 脅威ハンティング：上級アナリストによる高度な調査

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、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 XDR ソリューションです。

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、セキュリティ運用を劇的にシンプル化するさまざまな機能によって、運用チームの負担を劇的に軽減します。

また、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。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、効果的かつ効率的な検知と対応を実現します。



モダンなセキュリティ対策に不可欠なキーテクノロジーを実装

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 *1。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。

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

Cisco XDR 製品ポートフォリオ

Cisco XDR は、サブスクリプションモデルのクラウドサービスです。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。必要な統合および連携機能に応じて、次の 3 つのライセンス階層から選択することができます。

Essentials

- セキュリティ アナリティクス & コリレーション
- 脅威インテリジェンス
- 脅威ハンティング
- インシデント対応アクション（プレイブック）
- インシデントに対する優先度スコアの割り当て
- インシデント管理
- ケースに対する優先度スコアの割り当て
- アセットに関するコンテキスト取得
- ユーザー定義の自動化ワークフロー
- シスコ定義の自動化ワークフロー
- Software Support Enhanced（SWSS）

Advantage

Essentials に加えて

- サードパーティのセキュリティツールと統合

Premier

Advantage に加えて

- Managed Detection and Response（MDR）（シスコのマネージドサービス）
- Talos インシデント対応チーム（CTIR）
- テクニカル セキュリティアセスメント（CTSA）

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

2505-1-TO