Cisco Secure Network Analytics で実現するランサムウェア早期対策ソリューション

ランサムウェアによるビジネスへの影響は深刻

- 業務や設備が停止
- 事業継続の危機
- 高額な身代金
- 多額の復旧コスト
- 風評被害の発生
- 社会的信用の失墜

早期把握で被害の拡大を防ぐことが何よりも重要

昨今、日本国内ではランサムウェアによる被害が増加しています。IPA が発表している「情報セキュリティ 10 大脅威 2023」でもトップとなっており※、その攻撃対象はあらゆる業種に及びます。

工場の生産ライン管理など製造系のネットワークや、電子カルテや個人情報を扱う医療機関なども例外ではありません。デジタル化の進展、クラウドやインターネットの利用が進むにつれて、こうしたクローズドとされてきたネットワーク環境も変化しており、近年のランサムウェア被害は製造業や医療分野でも多く見られます。

こうした状況に対応すべく、セキュリティ対策も変化しています。攻撃者の侵入を防ぐ、従来からの境界型防御だけでなく、重大なインシデントの予兆を早期に把握し、被害が拡大する前に対処できる仕組み= NDR（Network Detection and Response）の重要性が大きく高まっています。

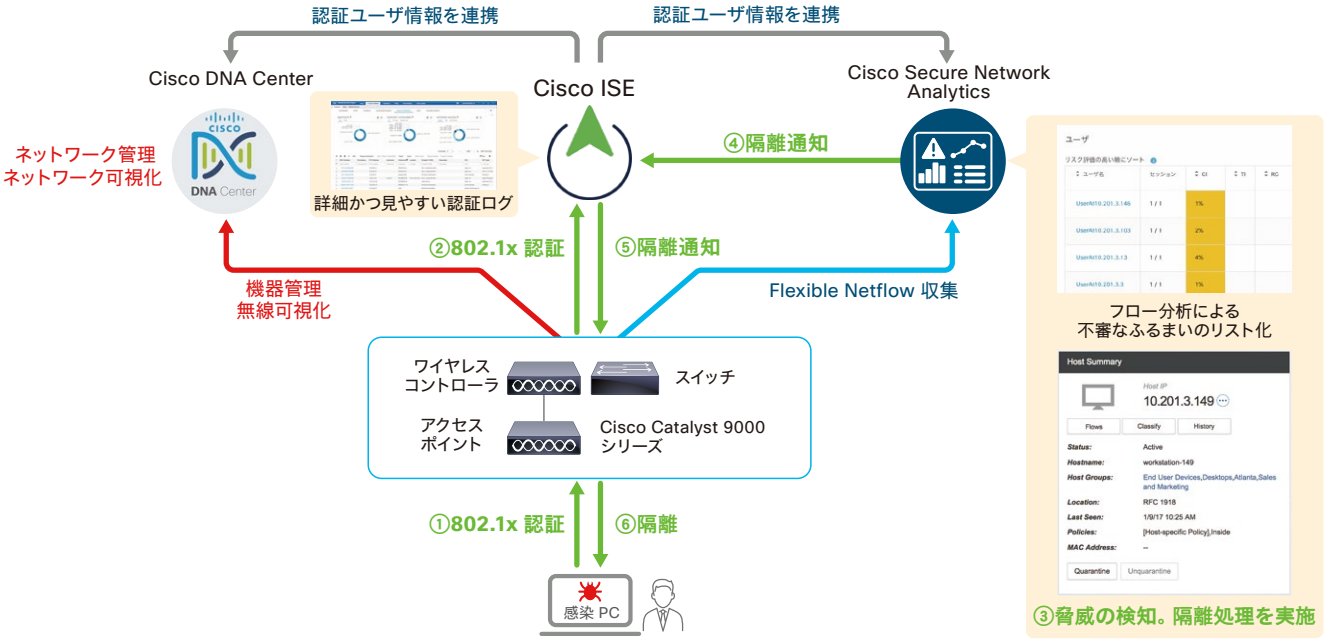
シスコは、攻撃者の偵察行為をはじめとする怪しいふるまいをネットワーク全体で網羅的に監視し、脅威の兆候を早期に発見、可視化する「セキュリティ脅威分析とネットワークトラフィックの可視化」で、ランサムウェアによるビジネスへの影響の最小化に貢献しています。

※ https://www.ipa.go.jp/security/vuln/10threats2023.html

Cisco Secure Network Analytics を活かした ランサムウェア早期対策ソリューション

Cisco Secure Network Analytics（SNA）※は、Cisco Catalyst シリーズをはじめとする
Flexible NetFlow 対応機器からフロー情報を収集、分析してネットワーク全体の通信状況を可視化。
不審なふるまいをいち早く検知し、ランサムウェアなど重大なインシデントの兆候をタイムリーに把握できます。
さらに、リアルタイム認証基盤の Cisco Identity Services Engine（ISE）や
ネットワーク統合管理ソフトウェアの Cisco DNA Center と連携することで
疑わしい端末の自動隔離や日々のネットワークのヘルスチェックまで、セキュリティ対策の水準を引き上げます。

※旧 Stealthwatch Enterprise



1 フロー情報を活用して脅威の兆候を早期に把握 Cisco SNA

- ネットワークスイッチやワイヤレスコントローラなどのネットワーク機器からフロー情報を収集、分析
- 通常と異なる不審なトラフィック（ふるまい）からセキュリティ脅威の兆候を検出

2 疑わしい PC（ユーザ）を自動隔離 Cisco SNA+Cisco ISE

- Cisco ISE の豊富なユーザ認証情報を Cisco SNA と連携。不審な通信主体が「誰」の「何」かすぐにわかる
- 疑わしい挙動を示す PC（ユーザ）をネットワークから隔離して、セキュリティ脅威を迅速に封じ込め

3 ネットワーク全体の可視化と安全性の担保 Cisco DNA Center

- LAN 全体をダッシュボードで可視化し統合管理。包括的な運用業務の自動化やアシュアランス機能を提供
- ネットワーク機器の脆弱性情報も一元的に可視化し、自動化されたアップデート作業でセキュリティ強化を実現

トータルなシスコ ソリューションならではのメリット

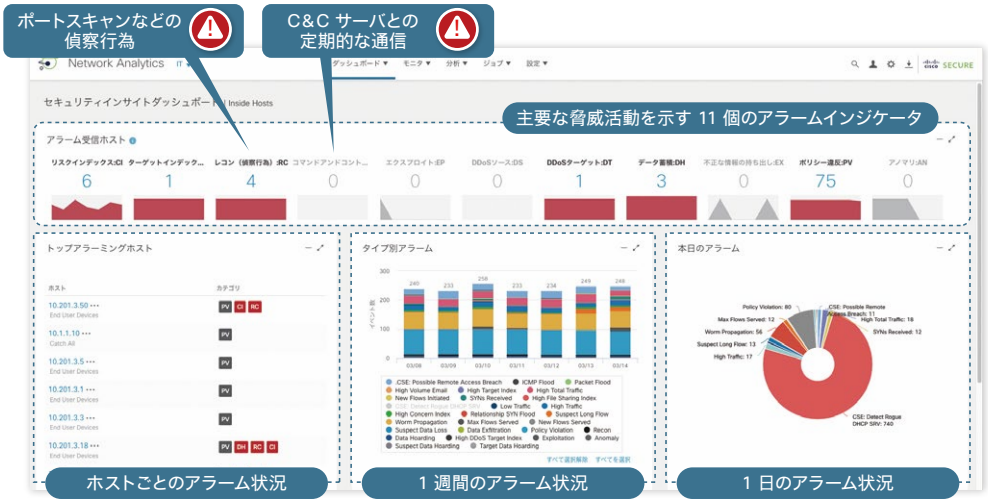
Flexible NetFlow に対応したシスコのスイッチ、ワイヤレス、ルータ（Cisco Catalyst シリーズ）で構成したネットワークでは、ネットワーク全体をセキュリティセンサー化して常に監視することで、セキュリティ強度を大きく高められます。「暗号化トラフィック分析（Encrypted Traffic Analytics、ETA）」機能で、暗号化されたトラフィックの可視化および分析も可能です。
さらに、シスコのリアルタイム認証基盤 Cisco Identity Services Engine（ISE）と連携した迅速な隔離や、Cisco SNA と Cisco DNA Center を組み合わせた包括的な可視化も、より確実なセキュリティ対策のポイントとなります。

インシデント早期検知

ネットワークふるまい検知 / 分析ソリューション

Cisco Secure Network Analytics

「脅威が見える」「見えるから防御できる」を実現



ネットワーク機器から、送信元、宛先 IP アドレス、プロトコルなどを含むフロー情報を収集し、機械学習を用いた高度な分析エンジンで通常と異なる不審なふるまいを検出します。マルウェア、分散型 DDoS 攻撃、Advanced Persistent Threat（APT）、内部脅威などを特定できます。
シスコの誇るグローバルな脅威インテリジェンス（Talos）の知見と情報も活用することで、常に最新かつ高度なセキュリティ脅威に対応します。

- ダッシュボード画面（上図）で、主要な脅威の活動状況の把握や、優先順位付けしたセキュリティインシデントの調査が可能
- ネットワーク上のトラフィックを可視化し、脅威発見だけでなく障害の迅速な原因特定や、ネットワーク拡張計画のためのキャパシティプランニングを支援

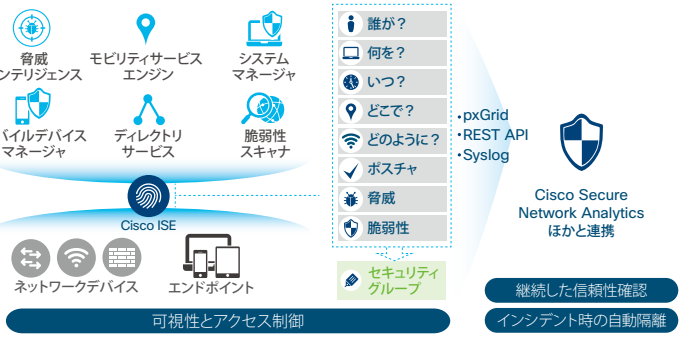
端末認証 アクセス制御（隔離）

次世代認証基盤

Cisco Identity Services Engine（ISE）

「誰」の「何」が接続されているかを詳細に把握。検出した脅威の封じ込めも実施

ネットワークアクセス制御とセキュリティポリシー管理を一元的に行います。ユーザとデバイスの情報を詳細に可視化し、それに基づいて認証を行うことで、有線、無線、VPN などの接続方法に関係なく、ネットワークへの安全で柔軟なアクセスを提供します。また、Secure Network Analytics や Cisco DNA Centerなどの連携ソリューションが発見した脅威の封じ込めを行うことで、ネットワークのレジリエンスを高めます。



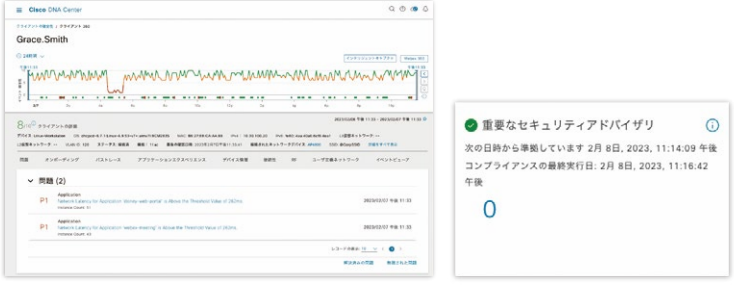
ネットワーク統合管理 脆弱性対応

ネットワーク統合管理ソフトウェア

Cisco DNA Center

ネットワークの可視化と運用自動化機能で脆弱性対応を効率化

ネットワーク管理と運用の自動化を一元的に行えるプラットフォームです。AI/機械学習を活用してネットワークの状態やトラフィックを高精度に分析し、わかりやすいダッシュボードを通じて問題の発見や解決を迅速に行うことができます。
セキュリティ向上に欠かせない接続端末の可視化や設定情報の管理、脆弱性情報の一覧化もでき、対処に必要な OS 更新も自動化できます。



導入事例

キオクシア株式会社

工場の生産活動を守るための新セキュリティネットワークが脅威を検知して早期に対処

ソリューション

Cisco Catalyst 2960-X
Cisco Secure Network Analytics
Cisco Firepower
Cisco Identity Services Engine
Cisco Security ELA

効果

- ネットワークそのものが脅威を検知、駆除する仕組みを実装。暗号化通信もそのまま可視化、分析
- 仮に脅威が生産エリアに侵入しても早期に発見し、迅速に対処でき、ネットワークの監視、不正通信の遮断、感染端末の隔離などを自動化を実現

日立 Astemo 株式会社

DX を前進させるための環境づくり

ソリューション

Cisco DNA Center
Cisco Identity Services Engine
Cisco Secure Network Analytics
CX カスタマーサクセス
CX プロフェッショナルサービス

効果

- より悪質化している現在のサイバー攻撃への備えを強化
- 簡単な操作でネットワークの構成変更や運用が行えるようになり、定期メンテナンスの工数を 3 分の 1 に削減

新電元工業株式会社

仮想化技術とゼロトラストによる次世代 ICT 環境

ソリューション

Cisco DNA Center
Cisco SD-Access
Cisco Identity Services Engine
Cisco Secure Network Analytics
ワイヤレス ソリューション

効果

- ふるまい検知と SDN、認証を連携させて、セキュリティの自動化にも取り組みたい
- 人中心のポリシー制御でゼロトラストセキュリティを実装し、手間のかかるアクセスコントロールリストによる管理を脱却

北陸コンピュータ・サービス株式会社

自社ネットワークを Cisco DNA により刷新し「ビジネスに貢献するネットワーク」を実現

ソリューション

Cisco DNA Center
Cisco Catalyst 9000 シリーズ（スイッチ/ワイヤレス）
Cisco Webex Meetings/Devices
Cisco Secure Network Analytics
Cisco Spaces

効果

- 予兆を検知したプロアクティブな運用の実現、OS やパッチのアップデートなど業務負荷の高い作業の自動化にも期待

関連情報 機能や効果をさらに知りたい方はこちらをご覧ください

Cisco Secure Network Analytics パンフレット（PDF）

Cisco DNA Center 活用ガイド

導入事例ページ

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

2360-2303-003-F