シスコ医療機関向けセキュリティ ガイド

医療情報システムを保護する次世代セキュリティガイド

医療機関を標的にした巧妙なサイバー攻撃が非常に増えています。
働き方改革やオンライン診療を推進するためにも、
医療情報システムを取り巻く変化にしっかり対応できるセキュリティ対策を選びましょう。

厚生労働省のガイドラインとセキュリティ対策 P02
今日の課題：高度化するサイバー攻撃と多様化するネットワーク利用 P04
医療機関へのサイバー攻撃例：ランサムウェア攻撃の解説と対策 P06
「ゼロトラスト」を前提としたセキュリティ対策が必要 P08
Cisco Talos：シスコなら最新かつ未知のサイバー攻撃にも対応可能 P09
Cisco Secure Healthcare とプロフェッショナルサービス P10
シスコのセキュリティ製品紹介 P11
- リモートアクセス VPN P12
- 端末セキュリティ P13
- 多要素認証 P14
- インターネットアクセスセキュリティ P16
- ネットワークのふるまい検知 / 分析 P19
- メールセキュリティ P21
- 認証強化とセグメンテーション P22
- データ保護 P23

2022 年 7 月版

厚生労働省のガイドラインとセキュリティ対策

厚生労働省のガイドラインと関連するセキュリティ対策の概要

厚生労働省が公開している『**医療情報システムの安全管理に関するガイドライン**』（以降、ガイドライン）は、医療業界を取り巻く環境の変化に合わせて適宜改定されていますが、令和 3 年 1 月に改定された 5.1 版および令和 4 年 3 月に改定された 5.2 版では、サイバー攻撃の多様化や巧妙化が進み、医療機関の診療業務などに大きな影響をもたらすような被害が見られることが改定理由の 1 つとなっています。

たとえば「喫緊の課題」として取り上げられているランサムウェア対策に関しては、6.10 章でバックアップのあり方などの対策が記述されているほか、適切なリスク分析によって被害の発生可能性を軽減するとともに万が一の被害後の対応を迅速化するために、6.2 章では医療情報システムに関する全体構成図（ネットワーク構成図やシステム構成図など）およびシステム責任者一覧（設置事業者など含む）の整備を推奨するなど、より具体的な対策が記述されています。

一方、医療機関が利用する医療情報システムでも外部サービスとの連携が進んでいますが、アプリケーション間の安全性を確保する観点から、6.5 章で外部アプリケーションとの連携における利用者の認証・認可に関して記述されているなど、医療機関のネットワークが外部とつながることを想定したセキュリティ対策の重要性にも記述されています。

また、従来から利用が認められているシステムやサービスの利用形態に関しても、これらの利用が安全に管理されている状況下で可能であることが従来の記述に追記されています。具体的には 6.9 章で、PC やタブレット、スマートフォンなどで医療情報システムにログインする場合は二要素認証を使用することが望ましいこと、個人所有の端末を業務に使用する（BYOD；Bring Your Own Device）場合は管理者が適切に制御するなど十分な安全性の確保が必要であることなどが記述されています。

ガイドラインでは、その他にもさまざまなセキュリティ対策が記述されていますが、6.5 章の「**技術的安全対策**」で解説されている項目に従って、ガイドラインのポイントと該当するセキュリティ対策カテゴリについて、次の表にまとめます。

6.5 章「技術的安全対策」の解説項目とガイドラインのポイントおよび該当セキュリティ対策カテゴリ

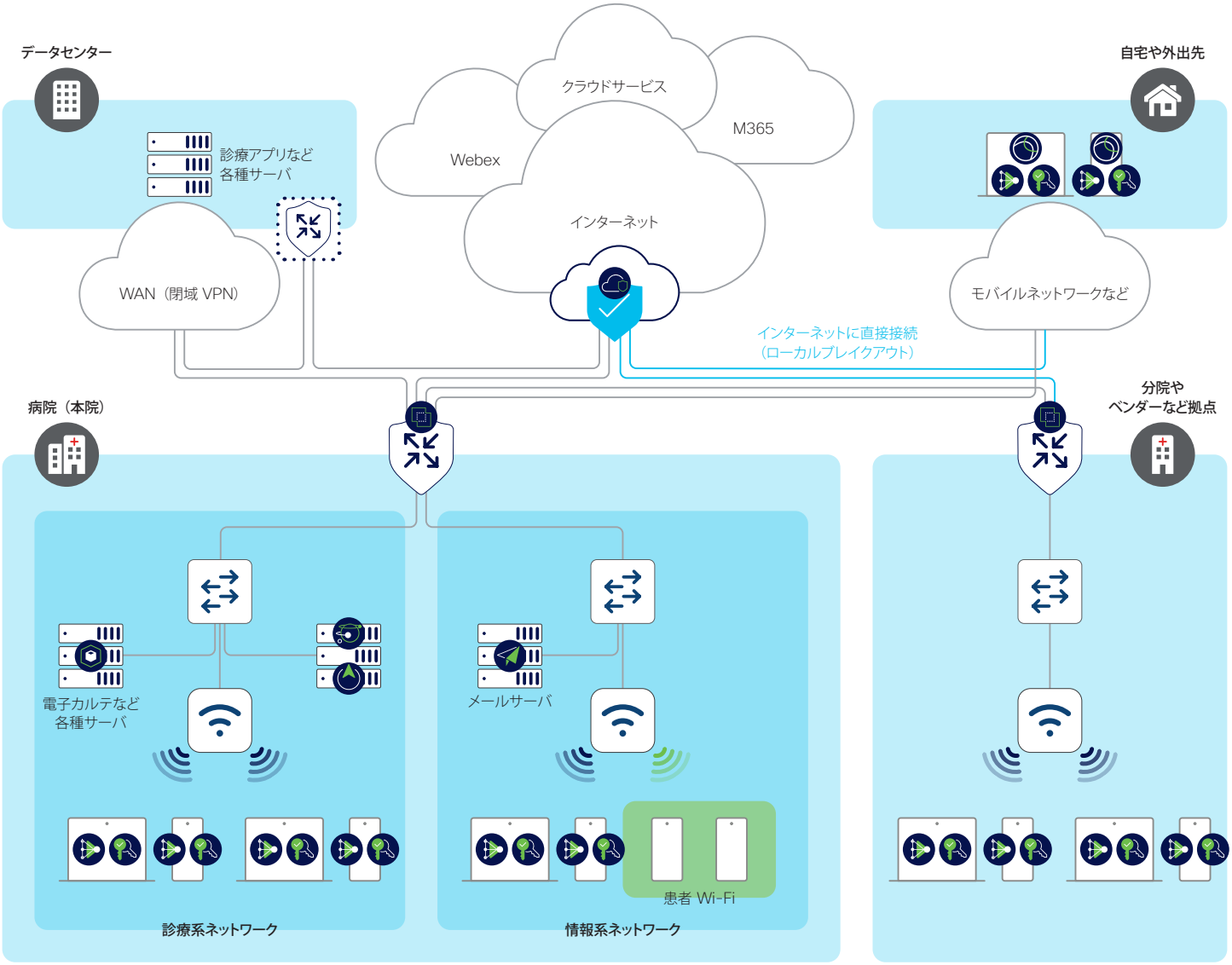
項目	ガイドラインのポイント	該当セキュリティ対策カテゴリ
利用者の識別・認証	• 医療情報システムには利用者を識別・認証する機能が必要 • 識別・認証の対象は、医療情報システムにアクセスするすべての職員および関係者 • 利用者が本人であることを識別・認証する手段は、ID・パスワード、IC カード、電子証明書、生体認証など • 認証の強度としては二要素認証を推奨（令和 9 年時点で稼動予定のシステムには原則として二要素認証の採用を推奨）	• MFA（Multi-Factor Authentication；多要素認証） • IDaaS（IDentity as a Service） • NAC（Network Access Control；ネットワークアクセス制御）
情報の区分管理とアクセス権限の管理	• 情報の種別、重要性、および利用形態に応じた区分管理に加えて、情報区分ごと、および組織における利用者や利用グループ（業務単位など）ごとに利用権限の規定が必要 • 付与する利用権限の必要最小限化が必要 • クラウドサービスを利用する場合は、その特性に注意した十分な考慮と対策が必要	• NAC（Network Access Control；ネットワークアクセス制御）
外部のアプリケーションとの連携における認証・認可	• REST API によるシステム連携がサイバー攻撃の起点となる可能性を踏まえたセキュリティ対策が必要	• API の適切な利用
アクセスの記録（アクセスログ）	• 個人情報を含む資源に関しては、すべてのアクセスの記録およびアクセスログの収集が必要 • ログの保護が必要、削除、改ざん、追加から防止	• ログ管理（監視） • SOC（Security Operation Center）
不正ソフトウェア対策	• コンピュータウイルス、マルウェア、ワームなど、さまざまな形態や呼称を持つ不正なソフトウェアが医療情報システムに侵入する可能性の考慮が必要 • 医療情報システムの脆弱性の最小化が必要 • ランサムウェアを含めた不正なソフトウェア対策全般における、多様かつ多層な対策の検討を推奨	• アンチウイルス /EPP（Endpoint Protection Platform） • EDR（Endpoint Detection and Response） • SASE（Secure Access Service Edge）/ SIG（Secure Internet Gateway） • IDS（Intrusion Detection System；侵入検知システム）/ IPS（Intrusion Prevention System；侵入防御システム）
ネットワーク上からの不正アクセス	• ファイアウォールに加えて、侵入検知システム（IDS）や侵入防御システム（IPS）の導入を推奨 • 不正なソフトウェアが侵入した場合を想定したモニタリングなど、ネットワーク内部の対策を推奨	• ファイアウォール / NGFW（Next-Generation Firewall；次世代ファイアウォール）/ UTM（Unified Threat Management；統合脅威管理） • IDS（Intrusion Detection System；侵入検知システム）/ IPS（Intrusion Prevention System；侵入防御システム） • NDR（Network Detection and Response）
医療等分野における IoT 機器の利用	• これまで想定していなかったセキュリティリスクが顕在化する可能性の考慮が必要 • 『**IoT セキュリティガイドライン ver 1.0**』を参照するように推奨 • IoT 機器を含む医療情報システムの接続状況や異常発生を把握するために可視化が必要	• NDR（Network Detection and Response） • IoMT（Internet of Medical Things）可視化

シスコの次世代セキュアネットワーク

厚生労働省のガイドラインに準拠するのはもちろん、今後予想される院内から院外へと広がる診療機会に備えて、ユーザがどこからでも安全に診療システムにアクセスできることを担保するためには、さまざまな利用形態や利用経路を想定したセキュリティ対策が必要です。

シスコの**次世代セキュアネットワーク**なら、ユーザがどこにいてもサイバー攻撃から保護できるクラウドセキュリティや、ユーザが「本人である」という信頼性を確立できる多要素認証、さらに端末やネットワークのセキュリティ健全性や通信（ふるまい）を監視して異常を検知し、脅威を防御および封じ込める対策など、多様かつ多層な対策が可能です。たとえば最新のランサムウェアや Emotet などのようなマルウェアにも、しっかり対応できます。

シスコのセキュリティ製品による厚生労働省のガイドラインに準拠したシステム構成イメージ



厚生労働省ガイドライン 6.5 章の技術的安全対策

- 利用者の識別・認証
- 情報の区分管理とアクセス権限の管理
- 外部のアプリケーションとの連携における認証・認可
- アクセスの記録（アクセスログ）
- 不正ソフトウェア対策
- ネットワーク上からの不正アクセス
- 医療等分野における IoT 機器の利用

シスコのセキュリティ製品

- EPP/EDR：端末セキュリティ（P13）
- MFA：多要素認証（P14）
- SASE/SIG：インターネットアクセスセキュリティ（P16）
- NDR：ネットワークのふるまい検知 / 分析（P19）
- NAC：認証強化とセグメンテーション（P22）
- NGFW/UTM（本ガイドには非掲載）
- リモートアクセス VPN（P12）
- メールセキュリティ（P21）
- データ保護（P23）

今日の課題：高度化するサイバー攻撃と多様化するネットワーク利用

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。たとえば、IPA が『**情報セキュリティ 10 大脅威 2022［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「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が、これらがまさに、巧妙化を続ける攻撃の典型例です。

厄介なことに、これらの攻撃は、従来のファイアウォールや IDS（Intrusion Detection System；侵入検知システム）、IPS（Intrusion Prevention System；侵入防御システム）などの「境界セキュリティ」で防御しきれるものではありません。従来のセキュリティを巧みにすり抜けて、内部に侵入し、感染活動を広げてゆくのです。

そのため、従来のように境界セキュリティで侵入を防止する対策はもちろんのこと、PC やタブレット、スマートフォンなどの端末で感染を防止する対策も求められますが、いち早く侵入や感染を察知して対応することで侵入後および感染後の被害の拡大を抑止するための対策が、ますます重要になっています。

情報セキュリティ 10 大脅威 2022 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	標的型攻撃による機密情報の窃取	2 位
3 位	サプライチェーンの弱点を悪用した攻撃	4 位
4 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
5 位	内部不正による情報漏洩	6 位
6 位	脆弱性対策情報の公開に伴う悪用増加	10 位
7 位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	
8 位	ビジネスメール詐欺による金銭被害	5 位
9 位	予期せぬ IT 基盤の障害に伴う業務停止	7 位
10 位	不注意による情報漏洩などの被害	9 位

*1　出典：IPA『**情報セキュリティ 10 大脅威 2022 組織編**』.

医療機関への深刻なサイバーセキュリティ侵害

サイバーセキュリティは、医療機関のあらゆる部門にとって最重要の課題となっています。医療業界は最も標的とされている産業であり、2021 年のデータ侵害の平均総コストは 923 万ドルでした。[*1]

一方、この時期はパンデミックが、医療業界が乗り越えるべき多くのハードルを新しく作り出しましたが、同時に変革やイノベーションの触媒となって、医療業界の変化を加速させました。たとえば、次のような例を挙げられます。

- ハイブリッドワークやテレワークが一般的になった
- オンライン診療など、遠隔医療の採用が広がった
- IoT や遠隔患者モニタリングの導入が加速した
- 医療のデジタル化が進展した
- デジタルな患者体験への注目が高まった

このような変化のたびに、医療機関には新たなセキュリティ要件が求められます。たとえば、患者に医療を提供する方法を改善するデジタル技術によって、さまざまな診療データへアクセスできる環境へと進化しています。デジタルトランスフォーメーション（Digital Transformation；DX）やイノベーションの推進にあたっては、オープンな相互運用性に高い注目が集まっています。このようにデジタル化が進むことで、脅威がより複雑かつ多様になり、絶えず新たなセキュリティリスクが発生し続けることになるからです。

実際に医療機関にとって、サイバーセキュリティ侵害の頻度と深刻度がこれまでになく高まっています。医療業界に対するサイバー攻撃は、2020 年には 2 倍以上に増加しました（約 28% がランサムウェアによる攻撃でした）。[*2]

医療機関や患者にとってのサイバーセキュリティ侵害には、センシティブな個人情報の盗難、医療情報システムや医療機器のハッキング、それらの復旧と引き換えの身代金要求（ランサムウェア攻撃）などがあります。

さらに、サイバー攻撃が患者の入院期間の延長、処置の遅延、他施設への転院につながるなど、臨床に影響を及ぼす可能性すらあります。たとえば、2021 年にカリフォルニア州サン ディエゴの医療機関 Scripps Health を襲ったサイバー攻撃では、医療情報システムの一部が数週間にわたって停止したため、システムがオフラインでの業務を余儀なくされました。その結果、専門的な治療の延期、入院患者の転院や新患の受け入れ不可による近隣病院への過負荷など、地域の医療に大きな支障を来しました。

*1　出典：IBM Security『**データ侵害のコストに関する調査レポート 2021**』.
*2　出典：IBM Security『**X-Force 脅威 インテリジェンス・インデックス 2021**』.

モバイル端末やアプリケーションの普及による境界セキュリティの限界

日本国内では、医療業務で使用する端末環境が大きく変化しています。

たとえば、PHS のサービス終了を受けてスマートフォンで内線サービスを構築する動きがあるほか、看護端末など持ち運びができるモバイル端末で、院内外から電子カルテシステムにアクセスできるアプリケーションも採用され始めています。

そのため、従来のファイアウォールや IDS、IPS による境界セキュリティだけでは不十分になりつつあります。境界セキュリティは、院内外ネットワークの境界で、院外からの脅威を防御して院内の安全や信頼性を確保するというセキュリティ手法ですが、モバイル端末の利用でセキュリティの懸念が高まっています。たとえば、院外のモバイル端末利用者が VPN（Virtual Private Network）接続を忘れた場合、病院で用意した境界セキュリティを経由せず、インターネットやクラウドサービスに直接接続する状況が考えられます。したがって、院外での無防備な状況でも端末や通信、データを保護できるセキュリティ対策が必要です。

さらに、院外でコンピュータウイルスに感染したモバイル端末が院内に持ち込まれて、院内ネットワークに感染を広げてしまうような事態も考えられます。このような事態に対応できるセキュリティ対策としても、境界セキュリティだけでは不十分です。

医療情報システムへのアクセス手段の多様化を踏まえて、厚生労働省のガイドラインでは改訂ごとに新しい内容が追記されています。令和 3 年 1 月に改定された 5.1 版では、医療機関などを標的とするサイバー攻撃の多様化と巧妙化、医療現場におけるスマートフォンや各種クラウドサービス利用などの普及、各種ネットワークサービスの動向への対応などに重点を置いた内容が追記されました。令和 4 年 3 月に改定された 5.2 版でも、医療機関などを標的とするサイバー攻撃のさらなる多様化と巧妙化や、モバイル端末の活用にあたってのセキュリティ対策など、さまざまな内容が追記されています。

TIP セキュリティ事故例

- フィッシングメール経由で感染、情報漏洩
- システムの脆弱性を利用した攻撃
  リモートアクセス VPN、VDI、保守用サーバ、院内 Wi-Fi など
- 物理的なアクセス、USB から感染
- 感染の拡大（ラテラルムーブメント）

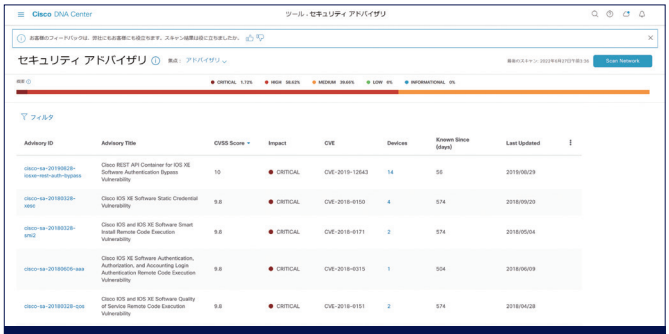
TIP ネットワーク機器の脆弱性や健全性をまとめて把握できる Cisco DNA Center

ランサムウェアなどのサイバー攻撃では、サポート期限が切れた OS やセキュリティパッチが適用されていないアプリケーションなど、脆弱性を抱えた「端末」が狙われると考えられがちですが、ルータやスイッチ、VPN 機器などの「ネットワーク機器」も例外ではありません。ネットワーク管理者は、端末だけでなくネットワーク機器にも脆弱性がないかどうか、常に確認する必要があります。

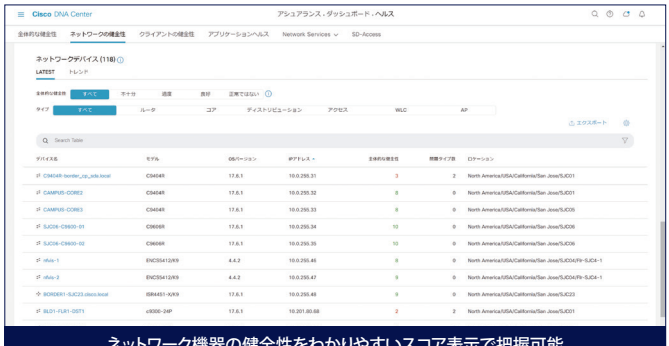
現在のネットワークは、**Software Defined Networking（SDN；ソフトウェア定義型ネットワーク）**というアプローチによって構築することができます。「SDN コントローラ」によって多数のネットワーク機器を一元管理することができるため、複雑な構成でネットワークを運用する医療機関では特に有効です。

シスコの SDN コントローラ（ネットワークコントローラ）**Cisco DNA Center** なら、ルータやスイッチ、Wi-Fi アクセスポイントなど、シスコのネットワーク機器の脆弱性をまとめて把握することができます。また、ネットワーク機器が問題なく稼動しているかどうか（健全性）も、わかりやすいスコアでまとめて把握することができます。

医療情報システムへのアクセス手段が院内だけでなく院外へと拡大し、システム管理者やネットワーク管理者の負担がますます増加することが予想されますが、管理負担を可能な限り低減することも、各種ソリューションの導入を検討するにあたって優先度が高い項目になっています。



ネットワークのスキャンで脆弱性情報に該当する機器を自動的に表示



ネットワーク機器の健全性をわかりやすいスコア表示で把握可能

ソフトウェアの更新が必要なネットワーク機器を一覧表示可能

医療機関へのサイバー攻撃例：ランサムウェア攻撃の解説と対策

ランサムウェア攻撃とは

ランサムウェア（Ransomware）とは、端末に侵入して保存されているデータを暗号化、または端末自体をロックして利用を制限したうえで、データや端末の復旧と引き換えに身代金（Ransom）を要求するマルウェアです。さらに最近のランサムウェアを利用した攻撃では、メール添付などで闇雲にランサムウェアを送信して感染させるのではなく、標的とした組織の内部に侵入してあらかじめ機密情報を窃取したうえで端末をランサムウェアに感染させるという、標的型攻撃と同様の手法が用いられることが多くなっています。たとえば、

1. 標的とした組織の端末の 1 つに侵入、それを足がかりに重要なシステムにも侵入する（たとえば Active Directory のドメインコントローラなど）
2. 組織の端末全体からデータ（機密情報）を窃取する
3. 組織の端末に保存されているデータを暗号化、または端末やシステムをロックする
4. データや端末、システムの復旧と引き換えに身代金を要求する
5. 復旧に対する身代金を拒否された場合、窃取した機密情報を暴露すると脅迫する（再度、身代金を要求する）

このように、データなどの復旧と引き換えの 1 度目の身代金要求と機密情報暴露の脅迫による 2 度目の身代金要求があることから、最近のランサムウェアによる攻撃は「二重脅迫型」と表現されることもあります。

医療機関が提供する救急医療は多くの場合、電子カルテやネットワーク化された医療機器などに依存しているため、医療機関が支払いに応じる可能性は高くなります。また、攻撃者は窃取した機密情報を闇市場で販売することもできます。闇市場におけるクレジットカード情報の価値は 12 ドルですが、カルテにはその 10 倍もの価値があります[*1]。これらの理由から、医療機関が絶好の標的となるわけです。

最近の POLITICO のレポート[*2]には、「医療機関は、情報技術予算の少なくとも 10% をセキュリティに費やすべきである」とありますが、業界全体の平均は 3% 程度に過ぎません[*3]。これは、ランサムウェア攻撃によって引き起こされる事態を考慮すると、非常に憂慮すべき数字です。

ランサムウェア攻撃によって、患者の個人情報を含む機密情報の漏洩や改ざん、医療情報システムの停止などの被害が発生します。電子カルテや PACS が停止すれば、復旧するまで診療を継続できなくなるだけではなく、復旧できない場合にはたとえば読影レポートの再作成が必要になるなど、二重三重の手間も発生します。

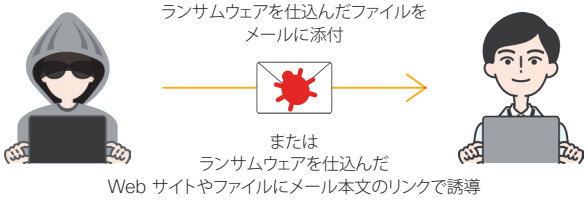
*1　出典：Experian Data Breach Resolution. ***2016 Data Breach Industry Forecast***.　*2　出典：POLITICO. ***Billions to install, now billions to protect***.
*3　出典：Healthcare IT News. ***Cybersecurity special report: Ransomware will get worse, hackers targeting whales, medical devices and IoT trigger new vulnerabilities***.

ランサムウェアの主な感染経路

ランサムウェアは、さまざまな方法で端末に侵入します。主な感染経路を紹介します。

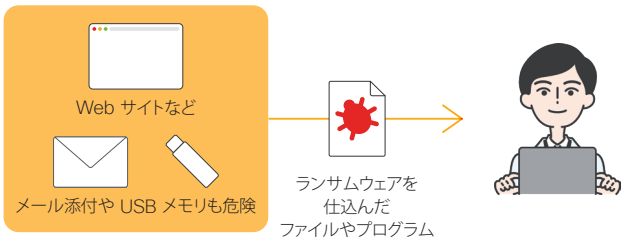
● メール経由

メールの添付ファイルにランサムウェアが仕込まれていることがあるほか、フィッシングメールと同様の手口で、メール本文に記載されたリンクをクリックするとランサムウェアが仕込まれた Web サイトの閲覧やファイルのダウンロードに誘導されることがあります。



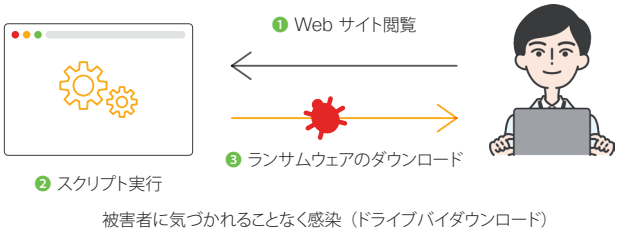
● ファイルやプログラムのダウンロード経由

Microsoft Word や PDF などのファイル、アプリケーションのインストーラやプラグインなどプログラムにランサムウェアが仕込まれていることがあります。



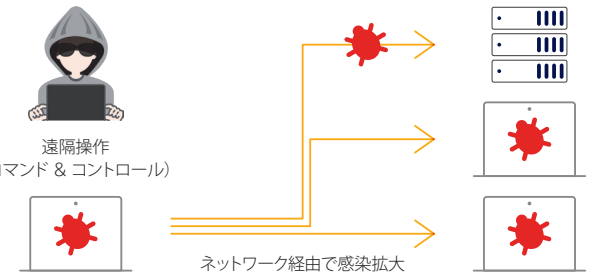
● Web サイト経由

Web サイトにランサムウェアが仕込まれていることがあります。一見して問題のない（たとえば大手企業の）Web サイトであっても攻撃者によって改ざんされていることがあるほか、「マルバタイジング」と呼ばれるバナー広告を利用した手口もあります。攻撃者は、古い OS やアプリケーション（ブラウザなど）の脆弱性を利用するスクリプトを埋め込み、Web サイトや広告を閲覧するだけでランサムウェアがダウンロードされるように仕向けます。



● ネットワーク経由

攻撃者は、できるだけ多くの端末を感染させるために、1 つの端末の侵入に成功するとネットワーク経由で他の端末に感染を広げます（ラテラルムーブメント）。最近ではテレワークの普及を背景に、脆弱性を抱えた VPN 機器への侵入を足がかりにして Active Directory のドメインコントローラに侵入し、ドメインに参加している端末をまとめて感染させる事例もあります。



ランサムウェア攻撃の対策

ランサムウェア攻撃の防御や被害からの復旧は複雑なテーマであり、「万能」な対策はありません。しかしながら、次のような対策 *1 を組み合わせて実践することによって、侵入など被害の兆候がある場合の対応を強化して、万が一、被害が発生してしまった場合でも被害の拡大を防ぐことができます。

セキュリティパッチを適用する

ほとんどの組織はランサムウェア攻撃を完全には防御できませんが、防御の「穴」を減らすことはできます。つまり、セキュリティ業界で長年にわたって提唱されてきたように、効果的な端末管理やネットワーク機器管理によってセキュリティパッチを確実に適用することが重要です。セキュリティパッチの適用に漏れがあったなど、管理不足によって侵入を許した事例は枚挙に暇がありません。

端末やシステム、ネットワークを監視する

ネットワーク内で自身のコピーを作成して感染を広げるワーム型のランサムウェアは、大量のコピーを作成しようとするために多くの場合、その兆候を見極めるために十分な活動を示します。ほとんどの場合、ワームはネットワークをスキャンして新たなコピー先となる端末を探索するため、単一の端末で短時間に多数のスキャンが実行されていること、あるいは多数の端末に接続が施行されていることなどが、感染拡大の兆候とみなせます。端末やシステム、ネットワークを監視して早期かつ適切に対応することで、感染の拡大を防ぐことができます。

最小限の機能だけ持たせる

端末やシステムには、所定の役割を果たすために必要最小限の機能だけ導入しましょう。たとえば Microsoft 社は、Windows のファイル共有で利用する古いプロトコル SMB 1.0（SMBv1/CIFS）を、必要でない限りは無効化するように推奨しています *1。SMB 1.0 が必要な場合でも、ファイル共有のアクセス権を必要最小限に設定しておきましょう。利用範囲を最小限にしておけば、このプロトコルを悪用した攻撃や被害の拡大を防ぐことができるかもしれないからです。

ネットワークのセグメンテーション

ネットワークのセグメンテーション、すなわち大きなネットワークを小さなネットワーク（セグメント）に分割して相互の通信を制限（制御）することが、攻撃の防御や被害の拡大防止に役立ちます。運用管理が複雑になりがちですが、セグメント化されていないフラットなネットワークでは、運用管理がシンプルな一方で感染拡大も容易になってしまいます。ネットワーク セグメンテーションは、システムを停止することができないなど、セキュリティパッチを適用することが不可能な環境でも効果的です。

*1　参考：Cisco Japan Blog「**ランサムウェア入門**」.

TIP 境界セキュリティをすり抜ける攻撃から医療機器を保護

最新のランサムウェアなど、従来のファイアウォールや IDS、IPS による境界セキュリティをすり抜ける攻撃への対策として、すでに多くの企業が導入しているソリューションが、いわゆるアンチウイルスソフトウェアのように攻撃をブロックして保護する「**EPP（Endpoint Protection Platform）**」です。さらに近年は EPP に加えて、攻撃を可視化して検知および対応を支援する「**EDR（Endpoint Detection and Response）**」を導入する企業も増えてきました。たとえばシスコでは、EPP と EDR を兼ね備えた製品として **Cisco Secure Endpoint** を提供しています（詳細は 13 ページ）。

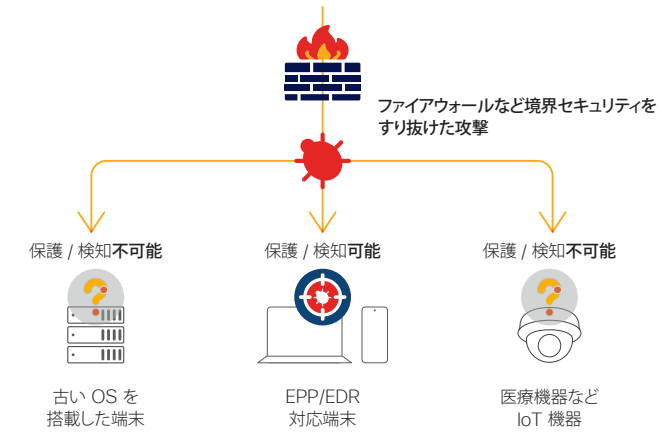
EPP や EDR は、PC やスマートフォンなど端末を個別に保護する観点では有効ですが、各端末に「エージェント」と呼ばれるプログラムを実装することが不可欠であるため、エージェントをインストールすることができない端末は保護できません。たとえば、Windows XP や Windows 7 のようにサポートが終了した古い OS や、セキュリティカメラやセンサー、一部の医療機器のような IoT 機器には、ほとんどの EPP や EDR ではエージェントをインストールできません。

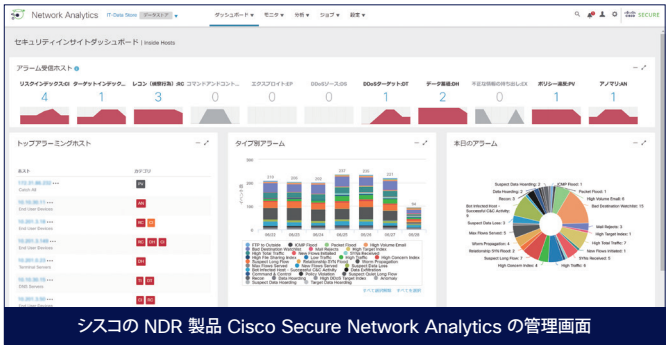
一方で、古い OS や IoT 機器を標的とした攻撃はリスクが高く、たとえばアメリカでは FBI が Windows 7 のサポート終了を受けて民間企業に注意を喚起したほか、日本でも総務省が IoT 機器の脆弱性を悪用した攻撃が増加していると注意を喚起しています。

したがって、EPP や EDR に加えて、これらのソリューションのセキュリティ上の盲点を補完するソリューションが必要となりますが、それが **NDR（Network Detection and Response）**です。

NDR を導入すれば、ネットワークで発生する異常なふるまいを検知して分析することができるため、たとえば IoT 機器のハッキングなど、EDR では検知できない異常にもいち早く気づいて対応することができるようになります。

シスコでは、NDR 製品として **Cisco Secure Network Analytics** を提供しています（詳細は 19 ページ）。





シスコの NDR 製品 Cisco Secure Network Analytics の管理画面

「ゼロトラスト」を前提としたセキュリティ対策が必要

ゼロトラストセキュリティ

従来のファイアウォールや IDS、IPS による境界セキュリティだけでは不十分になりつつある中で、「**ゼロトラスト**」（zero trust）という概念枠組みでセキュリティを実装するアプローチが注目を集めています。

境界セキュリティを含む従来のアプローチでは、たとえば「職員（の端末）によるアクセスだから安全」「院内ネットワークからのアクセスだから安全」のように、個々のユーザや端末、ネットワークが常に信頼できることを前提にアクセスを制御してきました。

ところがゼロトラストに基づくアプローチでは、文字どおり「信頼がない」ことを前提にセキュリティを実装します。つまり、ユーザ、端末、アプリケーション、そしてネットワークのすべてが信頼できないことを前提とした、いわゆる性悪説に基づくアプローチとも言えます。たとえば、ゼロトラストに基づくアプリケーションやネットワークへのアクセス制御では、

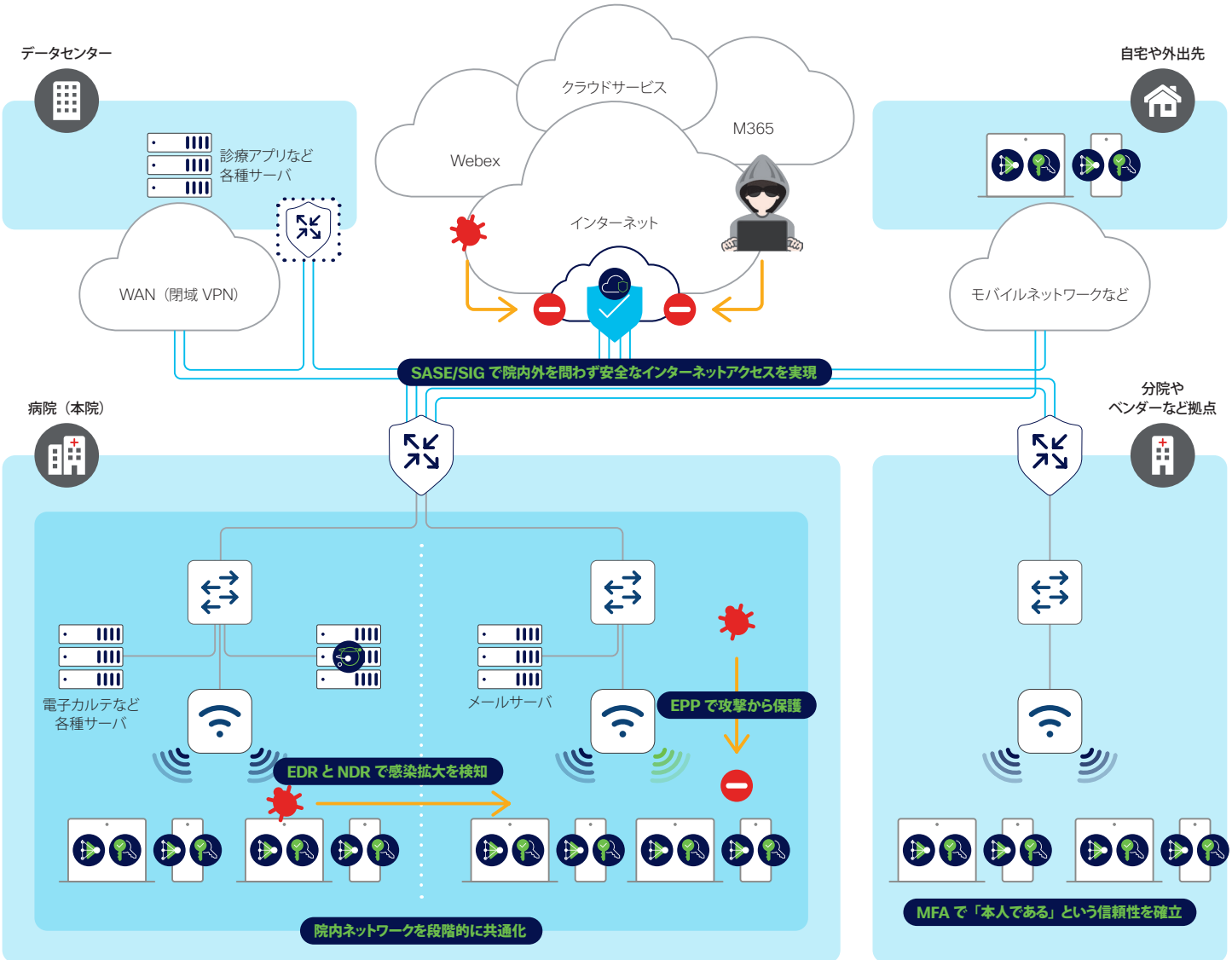
1. ユーザや端末が信頼できるかどうか検証する（信頼性を確立）
2. 必要最小限のリソースにアクセスできる必要最小限の権限を許可する（信頼性に応じて許可）
3. ユーザや端末が信頼できるかどうかアクセス要求の都度くり返し検証する（継続的に信頼性を検証）

このように、ゼロトラストに基づいてセキュリティを実装すれば、攻撃者がアクセスできる対象を狭めることができます。

シスコの次世代セキュアネットワークも、ゼロトラストのアプローチを採用しています。MFA（）によってユーザが「本人である」という信頼性を確立し、SASE/SIG（）によって院内外を問わずインターネットアクセスを制御するとともにサイバー攻撃から保護します。シスコの MFA は EPP/EDR（）と連携できるため、併せて導入すれば、端末の信頼性はより確実なものとなります。なお、この 3 つの製品はサブスクリプションモデルのクラウドサービスであるため、迅速かつ簡単に導入できるだけでなく、運用管理もシンプルです。

さらに、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、医療機器など IoT 機器の感染も含めてネットワークで発生する異常なふるまいを検知および分析できる NDR（）の導入も推奨します。

これらの製品を導入することで、情報系ネットワークや診療系ネットワークなど病院ネットワークの共通化に向けて段階的に移行することができるようになり、インターネット（クラウドサービス）の積極的な利用やテレワークの促進など、業務効率を高めることもできるようになります。



*1 「ゼロトラスト」（zero trust）は、2010 年に Forrest Research 社が発案した概念枠組みです。あくまで概念枠組みであり、最近になって注目されている「ゼロトラスト ネットワークアクセス」とは別物です。
ゼロトラスト ネットワークアクセス（Zero Trust Network Access；ZTNA）は、ベンダー各社によって定義や特長は異なりますが、製品やソリューションのカテゴリと言えます。
VPN の代替手段として推奨されることもあり、主として（社内）アプリケーションのアクセス制御にゼロトラストのアプローチを適用しています。
シスコでは、ZTNA 製品として Cisco Secure Access by Duo を提供しています（詳細は 14 ページ）。

Cisco Talos：シスコなら最新かつ未知のサイバー攻撃にも対応可能

Cisco Talos とは

セキュリティ製品を選定するにあたっては、それらが利用するデータベースの規模や、データを分析して実効性のある知見を蓄積するインテリジェンスの有無が重要な判断基準となります。これらが、サイバー攻撃など脅威の検知率、あるいは誤検知率のような指標を左右するからです。

Cisco Talos は、最先端のセキュリティ調査能力を持つ、世界最大の研究機関の 1 つです。Talos の強みは、脅威の全体像を捉えて進行中の事態を把握し、データに基づいて適切な知見を得られることです。データサイエンティストやエンジニアなど、シスコが誇る最強の専門家たちが日々、新旧のマルウェアサンプルなど膨大な脅威情報を分析し、未知の脅威に対しても迅速に、かつ正確な知見を積み重ねています。

シスコの各セキュリティ製品が使用するデータベースには Talos による知見がリアルタイムで反映されるため、常に最新かつ最先端のデータベースによって医療情報システムを保護できます。

6,250 億
1 日に分析する Web 要求数

200 以上
1 年に発見する脆弱性数

140 万以上
1 日に分析する新マルウェアサンプル数

300 億
1 日に分析する端末イベント数

84 万
保護するネットワーク数

6,700 万
保護するメールボックス数

8,700 万
保護する端末数

脅威を可視化する能力で他を圧倒

Cisco Talos には、世界中のどのセキュリティベンダーよりも脅威を可視化する能力があります。これを裏付けるのは、広範なセキュリティ製品ポートフォリオとパートナーシップです。

シスコは、ファイアウォール、IPS、Web セキュリティ、メールセキュリティ、端末セキュリティ、その他にも本ガイドで紹介する製品群など、包括的なセキュリティ製品ポートフォリオを提供しているだけでなく、さらにそれぞれのカテゴリで市場をリードしています。これらの世界中で導入されている製品群から得られる膨大なテレメトリデータが可視化、すなわち巨大なデータベースの構築を支えています。

また、自社製品から得られる情報だけでなく、185 を超える業界団体とのパートナーシップによって、情報収集活動の裾野を広げています。

さらに、お客様が日常的に利用しているさまざまなソフトウェアについても、それらの脆弱性を積極的に発見し、ソフトウェアベンダーの対応を支援しています。ソフトウェアベンダーがパッチを開発している期間であっても、シスコのセキュリティ製品のお客様であれば、該当する脆弱性を利用した攻撃から保護されます。

大規模な専門家体制で広範囲にわたって迅速に対応

Cisco Talos では、400 人を超える研究者、アナリスト、エンジニア、開発者、およびその他のオペレータが、24 時間体制で脅威情報を分析して、攻撃者の追跡やマルウェアの検出と対策など、実効性のある知見を蓄えています。

また、脅威のトレンドなど分析した情報の発信や、注意喚起にも注力しています。最近では、ウクライナ侵攻に関わるセキュリティリスクについて精力的に監視と分析を続けて、さまざまな情報を提供しているところです。このような公益的な活動を世界でも先頭に立って進める中で、自治体や政府機関とも連携しています。

未知のサイバー攻撃にも迅速に対応可能

未知のマルウェアによる猛攻撃から医療情報システムを保護するためには、高度な検出テクノロジー、大量の情報収集、リバースエンジニアリングなどの分析、そしてスピードが重要です。迅速に検出できれば、攻撃や被害を把握するまでの時間を短縮できます。

たとえば、「検出にかかる時間」（Time To Detect；TTD）という指標があります。これは、異常な通信などセキュリティ侵害の発生から実際の攻撃や被害を検出するまでにかかる時間のことです。Cisco Talos を後ろ盾とする端末セキュリティ Cisco Secure Endpoint を例にすると、Secure Endpoint のお客様では TTD の中央値が 3.5 時間ですが、業界平均では日単位です。

このようにシスコのセキュリティ製品では Talos によって、未知のサイバー攻撃に対する迅速な対応を実現しています。

Cisco Secure Healthcare とプロフェッショナルサービス

Cisco Secure Healthcare：セキュアな医療環境のためのアーキテクチャ

シスコは医療機関に、包括的かつエンドツーエンドのセキュリティポートフォリオを提供します。このポートフォリオに含まれる製品群は、Cisco Talos を後ろ盾として効果的に連携し、医療機関向けのアーキテクチャである **Cisco Secure Healthcare** を実現します。

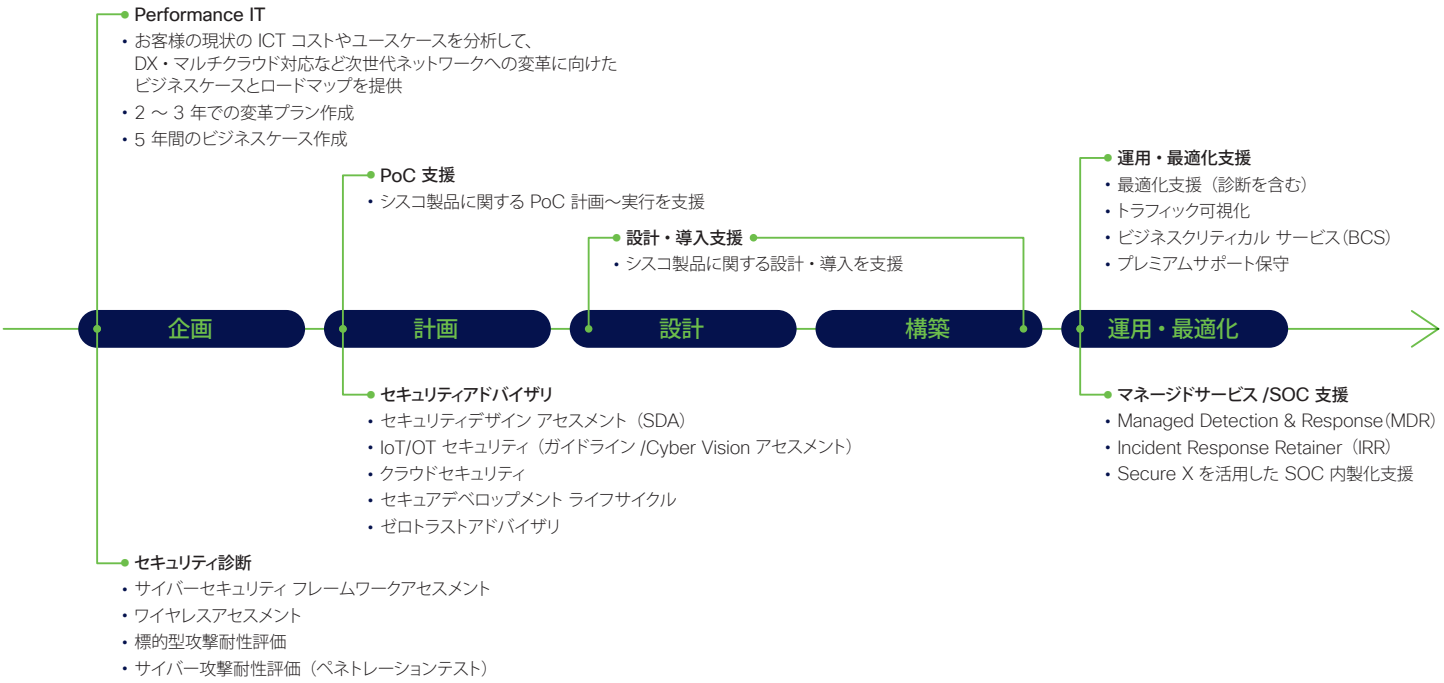
Cisco Secure Healthcare は、医療機関が規制を遵守できるようなセキュリティ アプローチで、病院、患者、端末を保護するように設計されたアーキテクチャです。相互に運用可能であることが検証されたセキュリティ製品群による統合基盤で、可視化やアクセス制御、柔軟なセグメンテーションを促進します。

Cisco Secure Healthcare によって、グループベースや端末ベースなど柔軟なアクセス制御が可能になり、ネットワークやアプリケーションを適切に保護できるようになります。また、ネットワークで発生する異常な挙動を検知して、プロアクティブなセキュリティ対策を実現するだけでなく、生命を救う医療機器も保護できるようになります。さらに、端末保護も強化できるだけでなく、インターネットからの脅威に対して場所を問わず機能する防御網も構築できるようになります。

これらのソリューションを組み合わせて、医療情報システム、および患者データや財務データ、知的財産など、デジタルデータを確実に保護しましょう。

Cisco Customer Experience：セキュリティ対策の導入から運用まで一貫して医療機関を支援

シスコのカスタマーエクスペリエンス サービス **Cisco Customer Experience（CX）**では、セキュリティ対策の導入から運用まで一貫して医療機関を支援する、各種プロフェッショナルサービスを提供しています。



プロフェッショナルサービス提供例			提供期間	主な成果物
企画	サイバーセキュリティ フレームワークアセスメント	• アメリカ国立標準技術研究所（NIST）が作成している、グローバルスタンダードであるサイバーセキュリティ フレームワーク（CSF）からテクノロジー領域を抽出し、技術的な対策実施状況を評価します。	ご契約から 8 週間程度	サイバーセキュリティ テクノロジー対策 評価結果報告書
	標的型攻撃耐性評価	• ホワイトハッカーが実践的な APT 攻撃を安全な方法で実施して、お客様システムの脆弱性やサイバー攻撃への耐性を評価します。 • 同時に、お客様システムのセキュリティ担当者（SOC や CSIRT など）がその攻撃をどのように検知して対応するのか、その手順や脅威への対応能力をリアルタイムに確認して、改善をアドバイスすることも可能です。	1 ～ 2 か月程度	テクニカルレポート
計画	ゼロトラストアドバイザリ	• お客様の既存システムに対して、ゼロトラストの達成度を評価します（NIST とシスコの両側面）。 • プランに応じて、ロードマップなどの作成を支援することも可能です。	2 か月程度	アセスメントレポート
	PoC 支援	• ご要望の PoC を実現するための役務をカスタマイズで提供します。	1 ～ 2 か月程度	
設計～構築	シスコ製品設計・導入支援	• ご要望のプロジェクトを成功させるための役務をカスタマイズで提供します • 通常の設計支援に加えて、ドキュメントレビュー、切り分け支援、作業立ち合いなどの迅速な支援も可能です。 • API 連携などが必要となるような開発系の支援も可能です。	1 ～ 12 か月	技術 QA コメント票 活動報告書
運用・最適化	トラフィック可視化	• NetFlow を利用したトラフィックの可視化によって、アクセスコントロールリストの作成やセグメンテーションを支援します。	3.5 ～ 6 か月程度	アセスメントレポート

シスコのセキュリティ製品紹介

リモートアクセス VPN	Cisco AnyConnect Secure Mobility Client	P12
端末セキュリティ	Cisco Secure Endpoint	P13
多要素認証	Cisco Secure Access by Duo	P14
インターネットアクセスセキュリティ	Cisco Umbrella	P16
ネットワークのふるまい検知 / 分析	Cisco Secure Network Analytics	P19
メールセキュリティ	Cisco Secure Email	P21
認証強化とセグメンテーション	Cisco Identity Services Engine	P22
データ保護	Cohesity on Cisco UCS	P23

リモートメンテナンス VPN を一元管理する流れ

多くの医療機関では、各診療システムを提供している各ベンダーが個別に VPN 機器を設置して、病院ネットワークへの VPN 接続によるリモートメンテナンスを実施しています。

ところが、近年のサイバー攻撃では、このリモートメンテナンス VPN が標的となっています。各ベンダーからの提案によって VPN 機器を調達する場合は買取契約が多く、ファームウェアの更新など導入後の適切な管理を怠ると、VPN 機器の脆弱性を悪用されてしまうからです。

そのため先進的な医療機関では、医療情報部など医療情報システムを管理する部署が VPN 機器を選定および調達するなど、各ベンダーではなく医療機関で VPN を一元管理する事例が増えています。ベンダー側にとっても VPN 機器を運用管理する負担がなくなるため、今後はさらに増えると考えられます。

一元管理型リモートメンテナンス VPN に最適なマルチセキュリティ対応 VPN クライアント

リモートメンテナンス VPN を医療機関で一元管理する場合に最適な VPN クライアントソフトウェアが、**Cisco AnyConnect Secure Mobility Client** です。Windows や macOS、iOS、Android、ChromeOS など、幅広い OS に対応しているため、ベンダー側で利用するほとんどの端末で利用できます。また、AnyConnect は IPsec IKEv2 による VPN 接続だけでなく SSL VPN にも対応しているため、ベンダーに証明書を配布すれば、より安全な VPN 接続を提供することもできます。医療機関が病院に設置する VPN 機器には、この SSL VPN 接続を提供できるシスコのルータや UTM を導入することを推奨します。

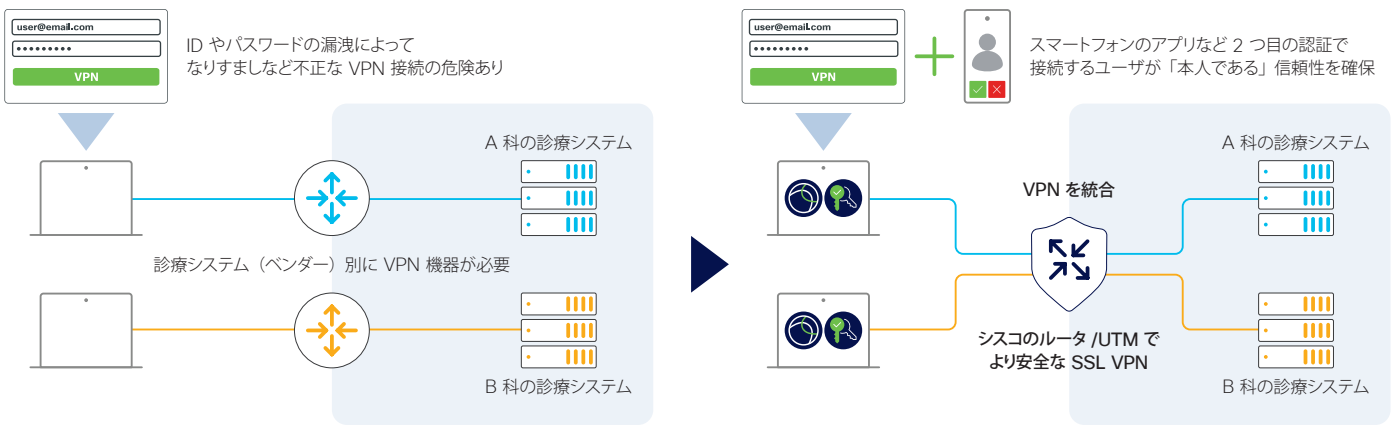
さらに AnyConnect はマルチセキュリティ対応 VPN クライアントでもあり、**Cisco Secure Endpoint** や **Cisco Secure Access by Duo**、**Cisco Umbrella** など、シスコの他のセキュリティ製品と連携および統合することができます。

たとえば最近では、リモートメンテナンス VPN 端末を利用するベンダー作業者の身元（本人であること）を確認するために多要素認証を導入する医療機関もありますが、AnyConnect と Duo を組み合わせれば、多要素認証による VPN をスムーズに導入することができます。多要素認証によって、ID とパスワードによる 1 つ目の認証方式に 2 つ目以降の認証方式を追加することで、ベンダー作業者の身元を確認できない場合には VPN 接続を許可しないなど、たとえベンダー作業者の ID やパスワードが漏洩した場合でも病院ネットワークへの不正な VPN 接続を防ぐことができます。

AnyConnect はもちろん、ベンダー作業者のリモートメンテナンスに限らず、医療従事者や職員のテレワークなどにも有効です。また、Duo に限らずシスコの他のセキュリティ製品との連携でも、さまざまなメリットをもたらします。シスコの医療機関向けポートフォリオのユースケースの 1 つである「ヘルスケアのためのサイバーセキュリティ」では、ビジネスニーズの 1 つとして安全なリモートアクセスに着目していますが、AnyConnect はこのポートフォリオの一部として、たとえばリスク管理の強化、ダウンタイムリスクの低減、サイバー攻撃に対する迅速な対応などに貢献します。

TIP VPN 接続前に端末の健全性をチェック

Cisco Secure Access by Duo には端末の健全性をチェックする機能もあります。たとえば、VPN に接続する端末の OS やブラウザが古いと脆弱性が存在することが疑われ、マルウェアなどに感染している可能性さえ疑われますが、このようなリスクを避けるため、特定のバージョンに満たない OS やブラウザの場合は警告を表示、あるいは接続を拒否することができます。



一元管理型リモートメンテナンス VPN に移行して、AnyConnect による SSL VPN と Duo による多要素認証を導入

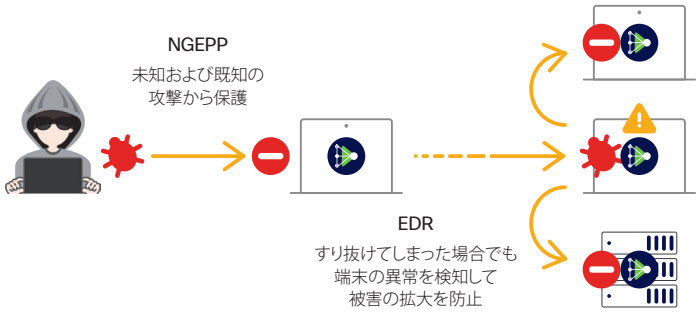
Cisco Secure Endpoint

端末セキュリティ

NGEPP + EDR：端末を攻撃から保護、さらに脅威の検知、調査、対応も実現する、統合型端末セキュリティ

医療機関を標的としたサイバー攻撃では、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 を兼ね備えた端末セキュリティです。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端末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 クラウドで構成されます。専用の管理サーバ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。

おすすめポイント

- マルウェアからの保護、検知、調査、対応まで、感染対策を一貫サポート
- 第三者機関にも認められた精度、信頼性、および安定性 *1
- クラウドサービスだから、専用の管理サーバの所有と保守が不要

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

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

- ファイルレスマルウェアから保護
- ふるまい分析で悪意のある動作から保護
- アンチウイルスで保護
- 機械学習で検知および保護
- 各種プラットフォームと連携、攻撃対象を削減

検知

- ファイルやプロセスのアクティビティを継続的に監視
- 端末内部の詳細な情報をリアルタイムで検索
- サンドボクシングで高度な解析
- IoC（侵害の痕跡）による ふるまい検知とフォレンジック調査
- 脆弱なソフトウェアを特定、攻撃パスを遮断
- イベント検出時のフォレンジック スナップショット取得
- SecureX 脅威ハンティングで高度な脅威検知、MITRE ATT&CK フレームワークとマッピング
- SecureX プラットフォームによる XDR

調査

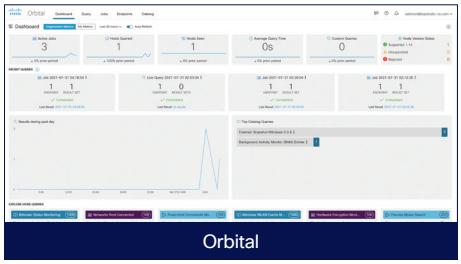
- ファイルやネットワークトラフィックの許可 / ブロックリスト
- アプリケーションの許可 / ブロックリスト
- 端末を隔離
- SecureX リボンで迅速な調査
- SecureX 経由で各種セキュリティ製品と統合、脅威対応を迅速化および自動化

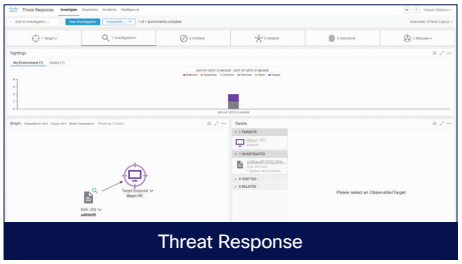
対応

XDR：シスコの各種セキュリティプラットフォームとの統合によって、より高度で迅速な検知、調査、対応機能を提供

Cisco Secure Endpoint は、シスコの各種セキュリティ製品による情報を統合管理する **Cisco SecureX** プラットフォーム、端末内部の情報を収集および追跡するための各種クエリをサポートする **Cisco Orbital**、攻撃など脅威がネットワークを伝播する経路も含めて可視化する **Cisco Threat Response** と連携することで、より高度で迅速な検知、調査、および対応を実現する XDR（Extended Detection & Response）機能も標準で提供します。

SecureX


Orbital

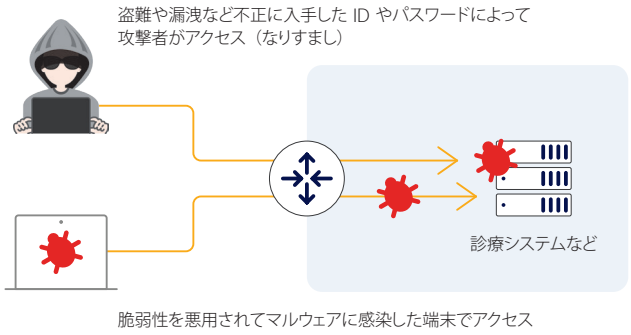

Threat Response

Cisco Secure Access by Duo

多要素認証

リモートアクセス VPN に潜む脅威：なりすましや感染した端末によるアクセス

診療システムを提供するベンダーによる院外からのシステムメンテナンス、医療従事者による院外からの電子カルテ閲覧、さらにパンデミックで急速に普及したテレワークなど、リモートアクセス VPN で病院ネットワークに接続する機会が増えています。



医療機関に限らず、また、VPN 接続に限らず多くの場合、ID とパスワードによる認証方式が一般的ですが、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、2021 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]。

また、リモートアクセス VPN ではベンダーの端末、医療従事者や職員が個人で所有する端末など、医療情報部などの管理外の端末が病院ネットワークに接続することになります。しかし、管理外の端末が安全であるという保証はありません。たとえば、古い OS を搭載した端末やセキュリティパッチを適用していない端末では、脆弱性を悪用されて、利用者が知らない間にマルウェアなどに感染していることもあります。

*1　警察庁・総務省・経済産業省「**令和 3 年 1 月 1 日から同年 12 月 31 日までの不正アクセス行為の発生状況**」.

診療アプリケーションを保護する多要素認証を提供

Cisco Secure Access by Duo は、VPN やアプリケーションにアクセスしようとするユーザおよび端末に対して、ユーザの多要素認証（Multi-Factor Authentication；MFA）や端末の健全性チェックを適用できるクラウドセキュリティサービスです。

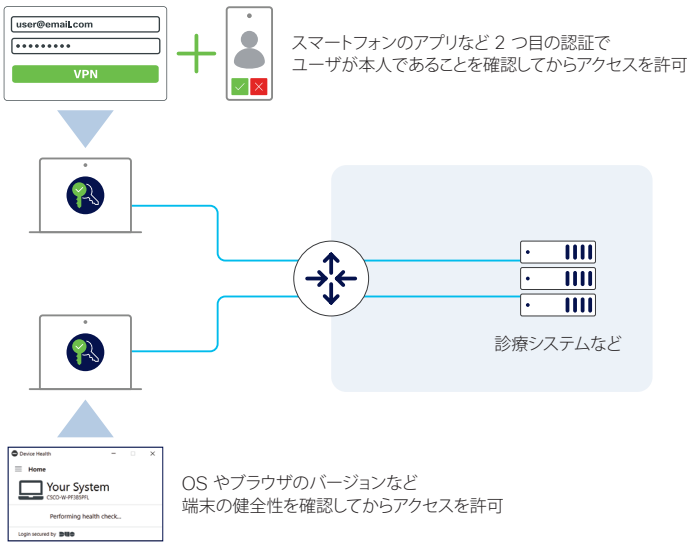
多要素認証（**ユーザトラスト**）によって、ID とパスワードによる 1 つ目の認証方式に加えて、たとえばユーザが所持する端末などによる所有者認証、顔や指紋などユーザ本人の生物学的特徴による生体認証のように、さまざまな要素を 2 つ目以降の認証方式とすることで、VPN やアプリケーションにアクセスしようとしているユーザが「本人である」という信頼性を確立することができます。

Duo は、最近注目されているパスワードレス認証にも対応しています。たとえば PC のカメラによる顔認識など、所有要素と生体要素の組み合わせによる認証でユーザが本人である信頼性を確立します。パスワードレス認証を採用することで、パスワードの漏洩対応など管理負担を軽減するとともに、ユーザに優しい手間いらずの認証方式で信頼性を強化できます。

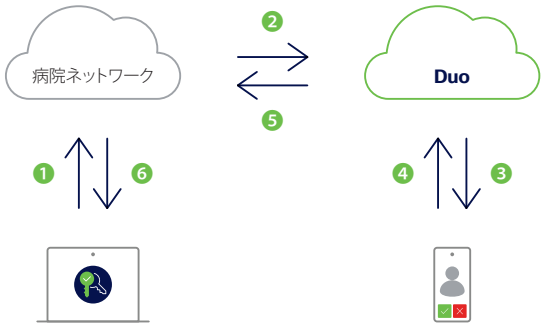
また、Duo には端末の健全性をチェックする機能（**デバイストラスト**）もあります。たとえば、端末の OS やブラウザが古いと脆弱性が存在することが疑われ、マルウェアなどに感染している可能性さえ疑われますが、このようなリスクを避けるため、特定のバージョンに満たない OS やブラウザの場合は警告を表示、あるいは接続を拒否することができます。この他にも、アンチウイルスソフトウェアの有無、現在接続中のネットワークなど、さまざまな条件で健全性をチェックすることができます。

シスコの医療機関向けポートフォリオのユースケースの 1 つである「ヘルスケアのためのセキュアでアジャイルなネットワーク」では、病院や診療所、医療従事者や職員の自宅から院内外のアプリケーションへと常に信頼性が高い接続を実現する諸機能を提供しますが、その中で Duo は、院内アプリケーションへの接続では **Cisco AnyConnect Secure Mobility Client** と、クラウドサービスなど院外アプリケーションへの接続では **Cisco Umbrella** と連携して、安全で信頼性が高い接続を確立する機能を担います。

ユーザと端末の信頼性を確保してからアクセスを許可



多要素認証の流れ



1. VPN に接続したい PC で 1 つ目の認証
2. Duo に 2 つ目の認証要求を送信
3. スマートフォンのアプリに 2 つ目の認証を要求（プッシュ通知）
4. スマートフォンのアプリで 2 つ目の認証（プッシュ通知にワンタップで応答）
5. ルータなど VPN 機器に 2 つ目の認証成功を送信
6. VPN への接続を許可

多要素認証だけでなく、さまざまな機能を提供

Cisco Secure Access by Duo には 3 つのエディション（ライセンス）があり、**Duo MFA** では多要素認証を、**Duo Access** では多要素認証とデバイストラストを提供します。さらに **Duo Beyond** では、多要素認証とデバイストラストに加えて、たとえば院内外に分散した Active Directory と連携できるディレクトリ同期、証明書レスでの管理端末に限定したアクセスなど、医療情報部などのセキュリティを強化しつつ、管理負担を軽減する諸機能を提供します。

おすすめポイント

- 2 つ目の認証はアプリのプッシュ通知にワンタップ応答で OK、パスワードレス認証もサポートなど、ユーザビリティを確保しつつ認証強化が可能
- 医療機関に分散する複数の Active Directory と連携可能
- 院内アプリケーションへの VPN レスでのリモートアクセスもサポート

機能（抜粋）		Duo MFA	Duo Access	Duo Beyond
ユーザトラスト（多要素認証）	スマートフォンアプリのプッシュ通知で認証（Duo Mobile アプリ）	✓	✓	✓
	SMS、電話着信、ハードウェアトークンによるパスコード認証、U2F と WebAuthN による生体認証など	✓	✓	✓
	ユーザによる自己登録と自己管理	✓	✓	✓
デバイストラスト（端末の可視化）	アプリケーションにアクセスする端末を一元管理できるダッシュボード	✓	✓	✓
	端末の健全性をチェック（Duo Device Health アプリ）		✓	✓
	アンチウイルスやアンチマルウェアなどサードパーティ製ソフトウェアが有効かどうか識別			✓
適応型認証 / ポリシー	アプリケーション全体またはアプリケーション別にアクセスを制御	✓	✓	✓
	ユーザグループ別にアクセスを制御	✓	✓	✓
	端末が接続中のネットワークに基づいてアクセスを制御	✓	✓	✓
	ユーザの場所に基づいてアクセスを制御		✓	✓
	端末の健全性に基づいてアクセスを制御、健全性が低い場合は修正するようにユーザに通知		✓	✓
	異常なアクセスや危険なアクセスを検知（Duo Trust Monitor 機能）		✓	✓
	モバイルデバイス管理（MDM）への登録状況に基づいてアクセスを制御			✓
シングルサインオン（SSO）とリモートアクセス	クラウドベースの SSO を提供（Duo Central ポータル）*1	✓	✓	✓
	オンプレミスで運用しているアプリケーション / サーバにリモートアクセス（Duo Network Gateway サーバ）			✓
	クラウドで運用しているアプリケーション / サーバにリモートアクセス（Duo Network Gateway サーバ）			✓

*1　オンプレミスベースの SSO は Duo Access Gateway で提供。

導入事例：国立がん研究センター中央病院 *1

厚生労働省所管の国立研究開発法人国立がん研究センターは、新型コロナウイルス（COVID-19）の感染拡大を受けた政府によるテレワーク推進の流れもあり、Cisco Secure Access by Duo を導入。多要素認証と端末の健全性チェックによって、安心、安全なテレワークの拡大に向けた先行導入を実施しました。

情報統括センター 副センター長の田中勝弥氏は、今回のテレワーク拡大の取り組みについて、次のように経緯を話します。

「2020 年 3 月、COVID-19 感染拡大に伴う政府のテレワーク推進の流れを受けて、センターでも対応を検討しました。患者さまと対面する必要のある医療スタッフは難しいものの、スタッフ部門の事務処理など、テレワークが可能な業務もあります。それ以前から働き方改革の観点でテレワークのしくみ自体はあったので、それを拡大するかたちで実行しようと考えました」

国立がん研究センターではテレワーク希望者に対して以前から、Cisco AnyConnect Secure Mobility Client による VPN 経由でセンター内の自身の PC にアクセスする、リモートデスクトップを提供していました。しかし、従前にテレワークを実施していたスタッフは 10 名に満たず、テレワークを拡大させるうえでは貸し出し PC の不足が課題となりました。新たに PC を調達、展開する時間もない緊急事態下で、センターは自宅 PC の使用を解禁せざるをえない状況になったのです。

そこで、この少し前にシスコの担当者からタイムリーに案内を受けていた Duo の導入を検討、直ちに検証を開始しました。その狙いを、田中氏は次のように説明します。

「センターからの貸与ではない自前の PC を利用してもらうにあたり、懸念したのは、スタッフの本人確認と端末の脆弱性でした。テレワークでは個人情報を扱う業務は担当させませんが、管理部門としては万が一の情報漏洩も考えて、できる限り対策しておく責任があります。Duo は、同時期に内閣サイバーセキュリティセンターが推奨していた多要素認証に加えて、OS のバージョンやアンチウイルスソフトウェアの有無など端末の健全性もチェックして、脆弱性を抱えた端末にはアクセスさせない機能があり、当方の求めるところと合致しました。まさに、テレワークのためのソリューションだという印象です」

こうして国立がん研究センターは、職務内容や IT リテラシーなどを勘案して、情報統括センターおよび中央病院医療情報部のスタッフの約 20 名を対象に、テレワークの拡大に向けた先行導入を開始しました。従来の AnyConnect による VPN（リモートデスクトップ）に Duo によるスタッフの多要素認証と端末の健全性チェックを追加し、端末の保護と感染疑い端末のアクセス制御のため、Cisco Secure Endpoint も連携させています。

日々のテレワークで実際にこのしくみを経験している医療情報部の岡田幸枝氏と渡辺清美氏は、その使い心地について「最初に端末の紐付け設定が終わってしまえば、日々の接続は意識しないくらい簡単で、業務上の面倒さは特にありません」と話します。

また、田中氏は立ち上がりまでのスピード感についても高く評価しています。「今回、トライアルライセンスの貸与からわずか 1 か月足らずで、スタッフに展開することができました。このスピードは、機器を導入して構築する必要がないクラウドサービスならではですし、スモールスタートで実環境を検証してから本格的に導入するかどうか見極められる点もメリットです。その間、シスコと連携して高い技術力で対応してくれた構築パートナーにも感謝しています。今後もシスコには ユーザが使いやすく、組織としても導入と管理がしやすいサービス、ソリューションの提供に期待しています」

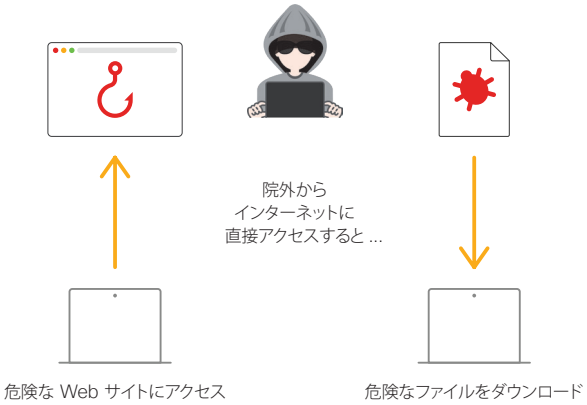
*1　Cisco.com から抜粋（www.cisco.com/c/ja_jp/about/case-studies-customer-success-stories/2198-ncc.html）。

Cisco Umbrella

インターネットアクセスセキュリティ

多様化するインターネットアクセスと増大するリスク

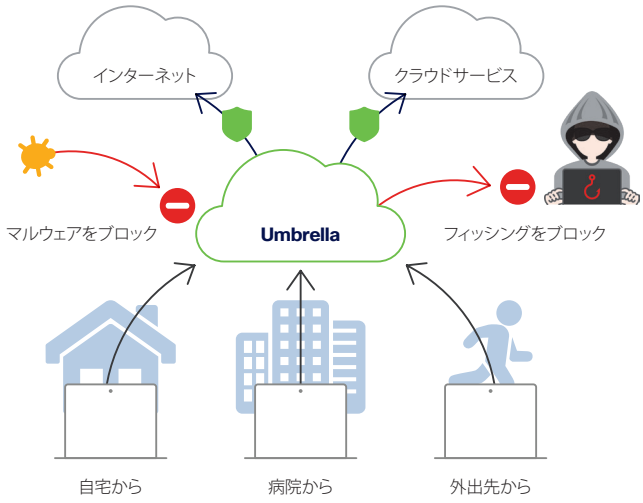
多くの医療機関では、医療従事者や職員によるインターネットの業務利用を、ファイアウォールなど境界セキュリティで保護された病院ネットワークに接続する特定の端末に限定してきました。ところが近年では、スマートフォンなどモバイル端末の利用拡大、さらにテレワークの導入など、院外で端末を利用する機会が増えています。院外から VPN で病院ネットワークに接続してインターネットにアクセスすれば境界セキュリティで保護されますが、VPN をオンにし忘れて直接インターネットに接続してしまう可能性があります。また、個人所有の端末を業務に使用する（BYOD）場合、プライベートのインターネットアクセスでは VPN をオンにしないでしょう。このように無防備な状態でのインターネットアクセスには、周知のことながらさまざまなリスクがあります。



簡単かつ迅速に導入できるクラウドセキュリティで、あらゆるインターネットアクセスを保護

インターネットアクセスの多様化に伴って増大するリスクに対する、最もシンプルな対策が **Cisco Umbrella** です。Umbrella は、インターネットアクセスに欠かせない DNS（Domain Name System）のしくみを利用したセキュリティ対策です（**DNS レイヤセキュリティ**）。そのため、本院、分院、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端末を保護できます。フィッシングサイトなど危険な Web サイトへの接続をブロックしたり、マルウェアなど危険なファイルのダウンロードをブロックしたりすることができるだけでなく、インターネットアクセスのモニタリングや Web サイトのフィルタリングなど、積極的な監視とアクセス制御も可能です。

Umbrella の DNS レイヤセキュリティは、ルータや端末などインターネットにアクセスする機器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。



おすすめポイント

- インターネットアクセスの入り口（DNS レイヤ）で危険な通信をブロック
- インターネットにアクセスする端末の場所を問わず保護可能
- きわめて簡単な設定で、シンプルかつ短期間で導入可能

導入事例：武蔵野赤十字病院

武蔵野赤十字病院の医師控え室では、医師が個人で所有する PC の持ち込みを許可し、職員サービスの一環としてインターネットにアクセスできる環境も提供しています。病院側のセキュリティ対策としてはファイアウォールや IDS を導入していましたが、セキュリティ対策が不十分な持ち込み PC による利用もあるなど、対策には限界がありました。そこで、よりシンプルで安全なインターネットアクセスのあり方を模索していたところ、出会ったのが Cisco Umbrella です。

医療情報管理課の岡田謙二郎氏は、次のように話します。

「専用のハードウェアが不要の Umbrella を導入することで、簡単に、しかも初期費用をかけずに、精度が高いセキュリティ環境を実現できました。医師の持ち込み PC にソフトウェアをインストールしたりデータを更新したりする必要がないため、管理者側の負担がほとんどないことが採用の決め手になりました」

Cisco Umbrella は、これまでのセキュリティ対策とは異なり、インターネットアクセスの入り口（DNS レイヤ）で通信を監視します。そのため、潜在的な脅威の可視化も可能になりました。武蔵野赤十字病院では、管理者がブラウザベースの管理画面でマルウェアなど潜在的な脅威の検出状況を監視しています。今後は、院外からのインターネットアクセスも保護できる、Cisco Umbrella ローミングクライアントの採用も検討しています。

*1　Cisco.com から抜粋（www.cisco.com/c/m/ja_jp/solutions/cisco-start/case-studies/1619-musashino-jcr.html）。

ランサムウェア攻撃の防御で Cisco Umbrella が果たす役割

ランサムウェア攻撃の初期段階では多くの場合、攻撃者が侵入した 1 つの端末から他の端末へと感染が広がる一連の挙動（ラテラルムーブメント）が発生します。このとき攻撃者は他の端末を見つけて感染を広げるために、攻撃対象のネットワーク外、つまりインターネットから、侵入した端末と通信します。

したがって、この通信をブロックすることができれば、データの暗号化や端末のロックなど、身代金の要求につながる被害を回避、あるいは最小化できる可能性があります。Cisco Umbrella の DNS レイヤセキュリティには、このような通信（コマンド & コントロール コールバック）をブロックする機能があります。

なお、EDR である **Cisco Secure Endpoint** や NDR である **Cisco Secure Network Analytics** も併せて導入すれば、それぞれ端末とネットワークの不審な挙動を迅速に検知することができるようになります。Umbrella も含めた多層防御で被害の拡大を予防しましょう。

ランサムウェア攻撃を防御するために検討すべきこと	Cisco Umbrella で実現する対策
ネットワークや端末の通信を監視して、 攻撃者が将来の攻撃に備えて準備している怪しい活動を把握する。	ネットワークや端末の通信をすべて可視化して、疑わしい通信を自動的に検出する。
医療機器などの IoT 機器、古い OS を搭載した端末やサーバ、管理外の患者の端末など、 アンチウイルスソフトウェアなどがインストールされていない機器も保護する。	Umbrella を経由してインターネットにアクセスする、すべての機器を保護する。
危険な Web サイトや IP アドレスへのアクセスをブロックする。	インターネットの入り口（DNS レイヤ）で危険であるかどうか確認し（遅延なし）、接続が確立する前にブロックする。IP アドレスへのアクセスは、セキュア Web ゲートウェイでブロックする。

DNS レイヤのセキュリティ対策をベースに、幅広いセキュリティ対策をクラウドサービスで提供

Cisco Umbrella は DNS レイヤのセキュリティ対策をベースに、**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対策を提供します。たとえば、医療従事者や職員による勝手なクラウドアプリ利用（ファイルなどデータのアップロード）を検出してブロックする、Umbrella でファイアウォールや IPS の機能も提供するなど、高度なセキュリティ対策や多層防御が Umbrella だけで可能です。

DNS レイヤ セキュリティ / セキュア Web ゲートウェイ / クラウドアプリ セキュリティ制御 / クラウド提供型 ファイアウォール / リモート ブラウザ分離 / データ漏洩防止 / XDR と 脅威インテリジェンス

セキュリティサービス			DNS セキュリティ		SIG	
			Essentials	Advantage	Essentials	Advantage
DNS レイヤセキュリティ	マルウェアやフィッシング、ボットネットなどの危険性が高いドメインをブロック		✓	✓	✓	✓
	SecureX、Splunk や Anomali などとの統合、エンフォースメント API によるカスタムリストに基づいてドメインをブロック		✓	✓	✓	✓
セキュア Web ゲートウェイ（SWG）	Web トラフィックのプロキシと検査［SSL（HTTPS）トラフィック対応］			危険なドメインのみ	✓	✓
	Web フィルタリング（カテゴリベース）	ドメインベース	✓	✓	✓	✓
		URL ベース			✓	✓
	カスタマイズ可能なブロック / 許可リスト	ドメインベース	✓	✓	✓	✓
		URL ベース			✓	✓
	アンチウイルスおよびレピュテーション（AMP）によって危険なファイルをブロック			危険なドメインのみ	✓	✓
	Secure Malware Analytics で疑わしいファイルを分析（サンドボックス）				1 日あたり 500 サンプル	無制限
	無害なファイルが危険なファイルに変化しても特定できる、遡及可能なセキュリティ				✓	✓
クラウドアプリセキュリティ制御（CASB）	クラウドアプリの検出とブロック	ドメインベース	✓	✓	✓	✓
		URL ベース			✓	✓
	クラウドアプリ別にきめ細やかに制御（アップロードやファイル添付、投稿の禁止など）				✓	✓
	契約クラウドのファイルストレージをスキャン、マルウェアを除去				2 アプリ	4 アプリ *1
クラウド提供型ファイアウォール（CDFW）	IP/ ポート / プロトコルを可視化および制御				✓	✓
	アプリケーションの可視化と制御、および IPS				オプション	✓
	IPsec トンネル終端対応				✓	✓
データ漏洩防止（DLP）	Web およびクラウドアプリのトラフィックをインラインで検査、機密データを保護				オプション	✓
リモートブラウザ分離（RBI）	危険な Web サイト、Web アプリ、または任意の宛先へ安全にアクセス				オプション	オプション
XDR（拡張型検知 / 対応）と脅威インテリジェンス	SecureX との統合（API）によって、シスコのセキュリティ製品全体で脅威の調査と修復を高速化および効率化	レポーティング API およびエンフォースメント API	✓	✓	✓	✓
		すべての API		✓	✓	✓
	ドメイン、IP、ASN ベースで、シスコによる詳細な分析データにアクセスして迅速に調査			✓	✓	✓

*1　継続的に追加。

Cisco Umbrella SIG Advantage パッケージの機能紹介

Cisco Umbrella の幅広いセキュリティ対策をすべて利用できるパッケージ（ライセンス）が、**Cisco Umbrella SIG Advantage** です。Cisco Umbrella SIG Essentials で提供する機能に加えて、次の機能を提供します [*1]。

- デフォルトで提供：レイヤ 7 アプリケーションおよび IPS 対応クラウド提供型ファイアウォール
- デフォルトで提供：データ漏洩防止（Data Loss Prevention；DLP）
- オプションで提供：リモートブラウザ分離（Remote Browser Isolation；RBI）

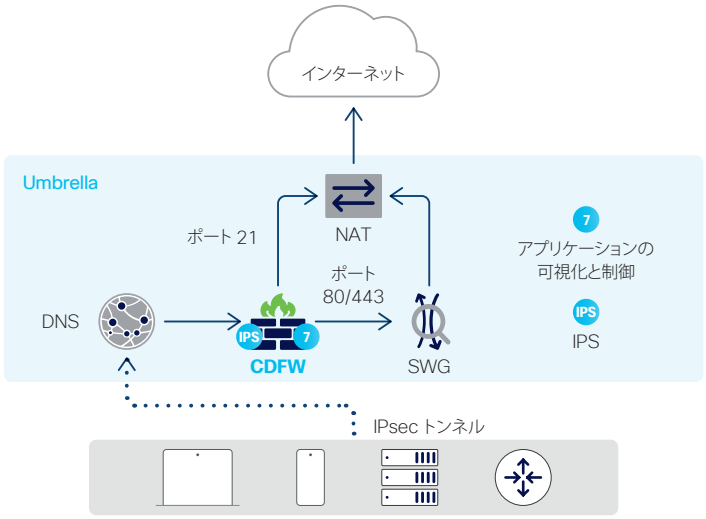
*1　Umbrella SIG Essentials を導入済みの場合は個別に追加可能。

レイヤ 7 アプリケーションおよび IPS 対応クラウド提供型ファイアウォール

インターネット送信に使用するポートとプロトコルを可視化および制御するレイヤ 3 およびレイヤ 4 ファイアウォールに加えて、Umbrella SIG Advantage ではアプリケーションを可視化および制御するレイヤ 7 ファイアウォール、さらに IPS（侵入防御システム）もサポートします。

- クラウドベースではない約 2,800 のアプリケーションを可視化（継続的に追加）
- Cisco Snort 3 対応 IPS、40,000 以上の膨大なシグネチャを使用（Cisco Talos から継続的に追加）
- 不必要なトラフィックや望ましくないトラフィックを、ポート、プロトコル、さらにアプリケーションおよび IPS ベースのポリシーで制御（許可 / ブロック）

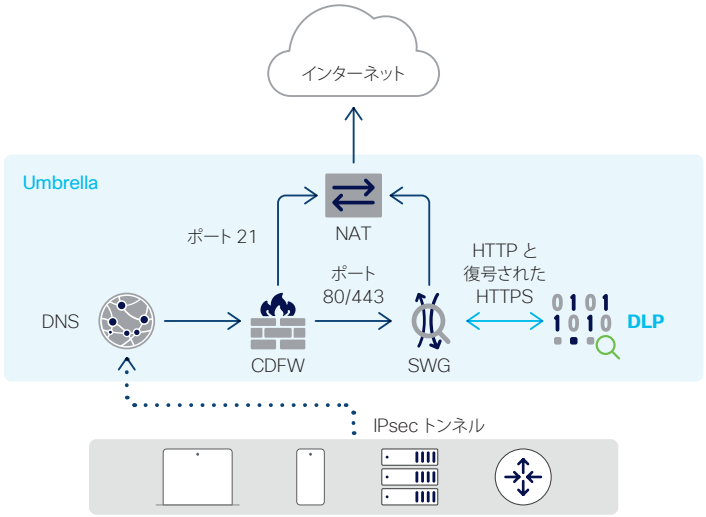
クラウド提供型ファイアウォールを使用するためには、**Cisco Secure Firewall** や **Cisco Meraki MX**、**Cisco ISR** など、IPsec 対応デバイスとのトンネル設定が必要になります。



データ漏洩防止

インターネットに向かうトラフィックを監視、事前に定義した機密データの有無をリアルタイムで分析し、機密データが流出する前にブロックします。セキュア Web ゲートウェイ上で動作するため、暗号化されたトラフィックにも対応します。

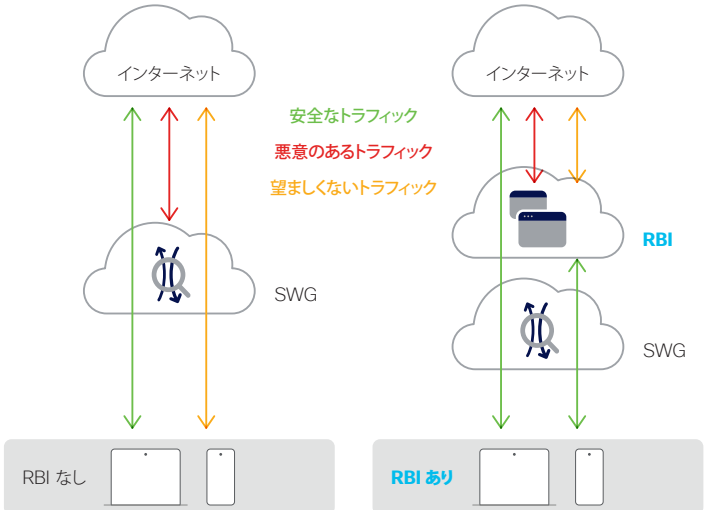
- PII、PCI、PHI を含む 80 以上の機密データ辞書を内蔵
- 任意のフレーズ（プロジェクトコードなど）を含むユーザ定義の辞書を作成可能
- 特定のアイデンティティや宛先に適用するなど、カスタマイズ可能なポリシー
- しきい値や近接度の設定によって、誤認識を軽減
- 機密データの使用に関する詳細なレポートで、不正使用を特定



リモートブラウザ分離

ブラウジング中のプログラムの実行など、ブラウザ機能を端末から切り離されたクラウドの仮想環境で提供することで、リスキーなユーザを保護、あるいはリスキーな Web サイト閲覧を無害化します。次の 3 つのパッケージから選択可能、既存のブラウザ設定を変更せずに迅速に導入できます。

- Isolate Risky
  未分類、または潜在的に危険なセキュリティカテゴリの Web サイト閲覧を分離
- Isolate Web Apps
  Box や Slack、Gmail など特定のアプリ、または SNS やファイルストレージなど特定のカテゴリでアプリを分離
- Isolate Any
  任意の宛先（ドメイン、URL、IP アドレス）、任意のコンテンツカテゴリ、任意のアプリを制限なく分離



Cisco Secure Network Analytics

ネットワークのふるまい検知 / 分析

ネットワークの不審なふるまいを検知、分析して、被害の拡大を防止できる「エージェントレス」セキュリティ対策

攻撃者による侵入を許してしまっても、適切な対策を実施することで被害の拡大を防止できることがあります。たとえば、攻撃者が病院ネットワークに侵入後、電子カルテのサーバに保存されたデータを狙う場合には、次の例のような一連の挙動が発生しますが、

- 特定の端末、たとえば職員の端末に侵入する
- 職員の端末を起点に、病院ネットワークを偵察（スキャン）する
- 電子カルテサーバに侵入可能な端末を特定、侵入する
- 電子カルテサーバに侵入する
- 電子カルテサーバに保存されたデータを外部に送信する

このような不審な挙動によって、ネットワークには通常とは異なる通信などの「ふるまい」が見られます。とりわけ、単一の端末で短時間に多数のスキャンが実行されていること、あるいは多数の端末に接続が施行されていることなどは、被害拡大の十分な兆候とみなせる不審なふるまいです。このように、ネットワークのふるまいを監視して異常を検出、さらに分析して異常の原因を突き止めることができれば、被害の拡大を防止することができます。

Cisco Secure Network Analytics（SNA）は、病院ネットワークを医療機器も含めて包括的に可視化して、不審なふるまいを検知および分析することができる、NDR（Network Detection and Response）と呼ばれるセキュリティ対策を実現します。

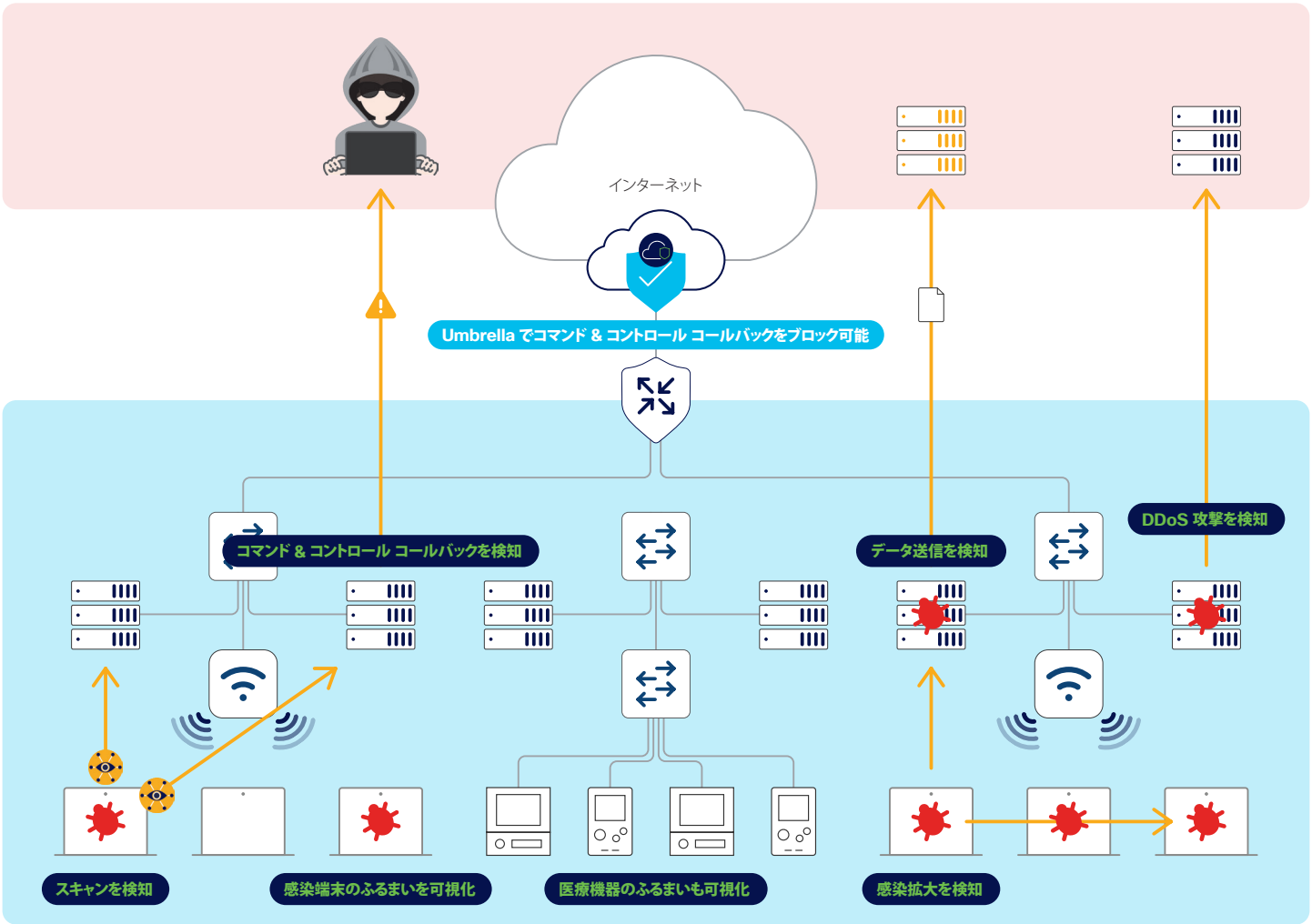
各端末に専用ソフトウェアをインストールする必要がないため（エージェントレス）、たとえば電子カルテ端末などのパフォーマンスに影響を与えません。仮にトラブルで SNA が停止しても、電子カルテシステムは引き続き利用可能です。

病院ネットワークを構成するネットワーク機器、または病院ネットワークに設置した専用のセンサーからテレメトリデータを収集し、同じく病院ネットワークに設置した専用のサーバで可視化および分析します。また、不審な挙動を収集するために病院のネットワーク機器単位でミラーポートを設定する必要がないため、病院ネットワークの限定したエリアを対象にする、全体を対象にするなど、手間いらずかつフレキシブルにふるまい検知セキュリティ対策を展開できます 。

おすすめポイント

- エージェントレス：端末や医療機器へのソフトウェアのインストールが不要
- ネットワークやシステムに影響を与えずに導入可能
- AI を活用したふるまい分析でネットワークの脅威を検知

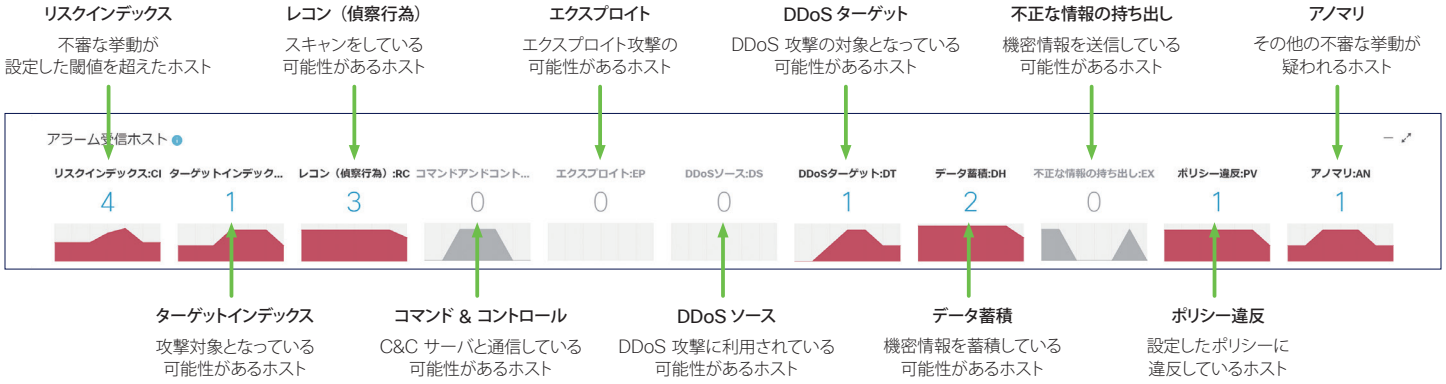
SNA で検知できる不審な挙動（例）



わかりやすい管理画面で不審なふるまいを一目で把握可能

Cisco Secure Network Analytics の管理画面では、不審な挙動をした端末などホストの数を、疑われる脅威カテゴリ別に一目で把握できます。

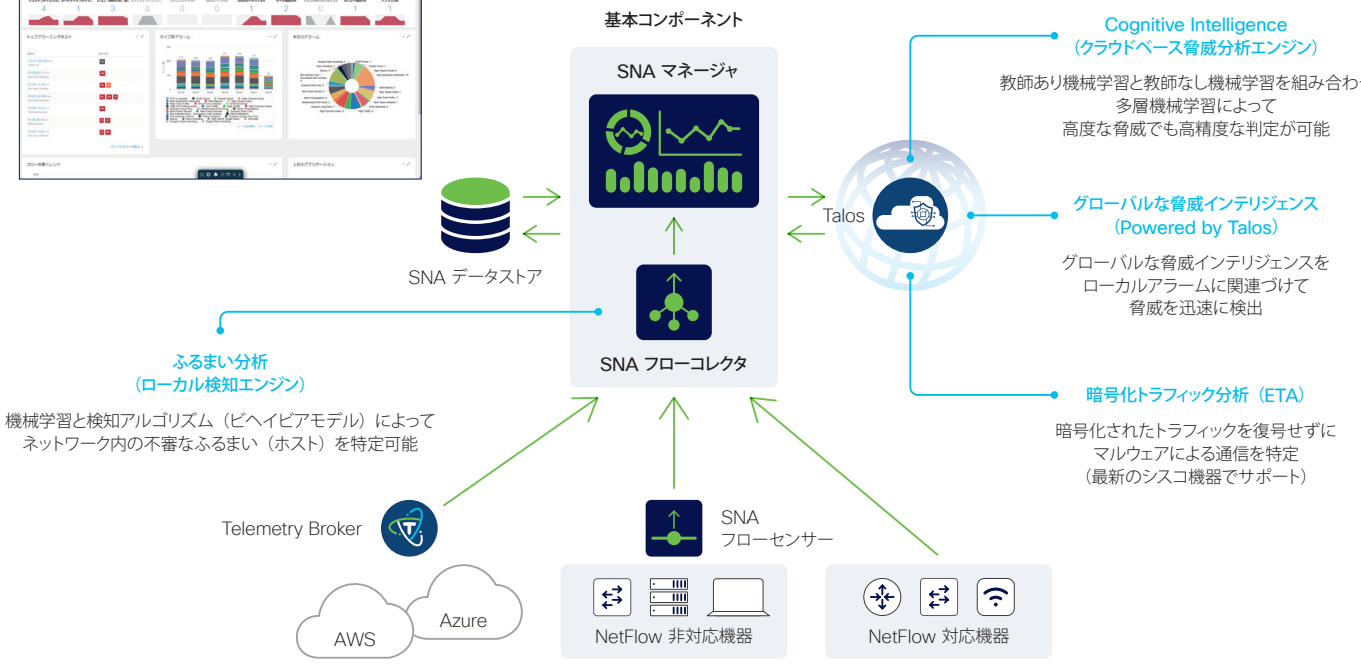
さらに、セキュリティポリシーを集中管理する **Cisco Identity Services Engine（ISE）**と連携することで、ユーザ情報など、より豊富なテレメトリ情報を活用できるだけでなく、検知した脅威を迅速に封じ込めることができるようになります。これらは、Cisco ISE の管理画面を操作することなく可能です。



ネットワークを包括的に可視化、業界最先端の機械学習とビヘイビアモデルで、ランサムウェア攻撃による脅威も分析可能

Cisco Secure Network Analytics は、病院ネットワークを構成するネットワーク機器、または病院ネットワークに設置した専用のセンサーからテレメトリデータを収集、可視化して、業界最先端の機械学習と検知アルゴリズム（ビヘイビアモデル）、および Cisco Talos による脅威インテリジェンスで分析することで、サイバー攻撃などの脅威を検知します。

病院ネットワークを **Cisco Catalyst 9000 シリーズ スイッチ**などの最新のシスコ機器で構成している場合は、**暗号化トラフィック分析（Encrypted Traffic Analytics；ETA）**によって暗号化されたトラフィックも可視化および分析できます。



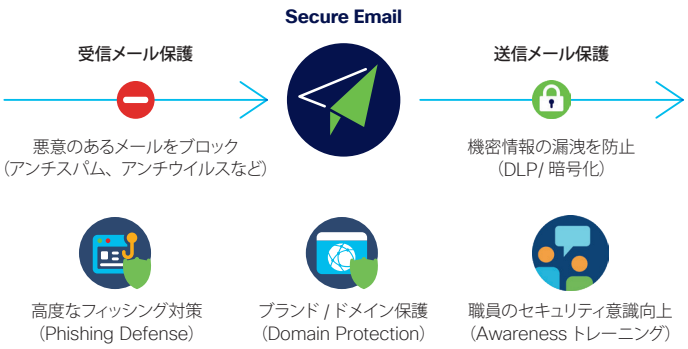
Cisco Secure Email

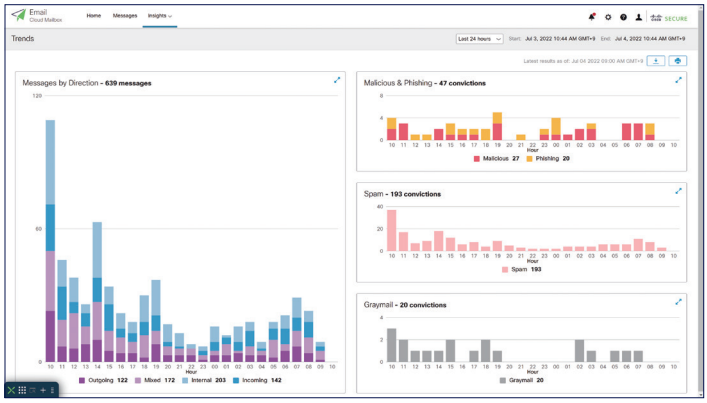
メールセキュリティ

あらゆる規模の医療機関で柔軟に導入できる、マルチレイヤの電子メールセキュリティ

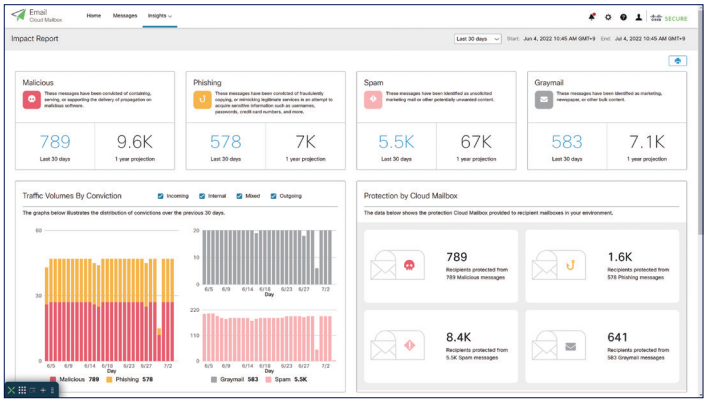
電子メールは最も重要なビジネスコミュニケーション ツールであると同時に、脅威の侵入および情報の流出の主要な経路でもあります。**Cisco Secure Email** はマルチレイヤのメールセキュリティによって、スパムやフィッシング、メール詐欺、マルウェア、情報漏洩、さらに組織ブランド（ドメイン）の悪用など、さまざまな攻撃から電子メールを保護します。

Microsoft 365 のセキュリティを補完する **Cisco Secure Email Cloud Mailbox** や、クラウド、オンプレミス、さらにハイブリッド構成や段階的な移行もサポートする柔軟な導入オプションによって、あらゆる規模の医療機関に最適なソリューションを提供します。





メールの利用状況や脅威のトレンドを視覚的に把握可能
（Cisco Secure Email Cloud Mailbox）



脅威の詳細を把握できるレポート
（Cisco Secure Email Cloud Mailbox）

医療機関で導入が進む iPhone を保護する Cisco Security Connector

医療機関で導入が進む iPhone でフィッシングメールなどのサイバー攻撃を避ける場合には、**Cisco Security Connector** という選択肢もあります。iOS 自体のセキュリティは非常に優れていますが、フィッシングなどによる情報漏洩に対しては無防備です。Cisco Security Connector なら、院内はもちろん、公共 Wi-Fi や携帯電話のモバイルネットワークを利用する院外でも、**Cisco Umbrella** によるインターネットアクセスセキュリティを適用して、iPhone から危険な Web サイトへのアクセスをブロックすることができます。Cisco Security Connector は、**Cisco Meraki システムマネージャ**などのモバイルデバイス管理（MDM）で簡単に展開することができます。

Cisco Umbrella によるインターネットアクセスセキュリティと
Cisco Secure Endpoint（Cisco Clarity）による端末セキュリティを提供

Cisco Umbrella によるインターネットアクセスセキュリティで
フィッシングなど危険な Web サイトへのアクセスをブロック

患者 Wi-Fi の提供、モバイル機器の業務利用など、多様化する利用形態に応じた適切なアクセス制御が必要

患者 Wi-Fi の提供、スマートフォンやタブレットなどモバイル機器の業務利用、さらに医療機器のネットワーク接続（IoMT；Internet of Medical Things）など、ここ数年で医療機関におけるネットワークの利用形態が劇的に変化しています。

病院ネットワークに接続するユーザや端末の種類が増えただけでなく、その組み合わせも増えています。たとえば 1 人の職員が、病院支給の端末と個人所有の端末の両方で病院ネットワークにアクセスする場合もあります。この場合、たとえば病院支給の端末なら電子カルテへのアクセスを許可しても、個人所有の端末ならアクセスをブロックするなど、適切なアクセス制御が必要です。

高度な可視化とセグメンテーションで脅威に対策できる、統合認証サーバ

Cisco Identity Services Engine（ISE）は、RADIUS および TACACS+ 認証サーバ機能を中心とした、さまざまなセキュリティ機能を提供する統合認証サーバです。ネットワークに接続するための認証時に、ユーザや端末の属性（**グループ**）、接続方法など、さまざまな条件によってアクセス可能なネットワーク領域を限定することで（**セグメンテーション**）、センシティブな個人情報を扱う病院ネットワークへのアクセスを適切かつシンプルに制御できます。

セキュアアクセス
802.1X 認証などによる
有線 / 無線アクセス
証明書の発行 / 配布サービス
リモートアクセスやゲストアクセス

セグメンテーション
わかりやすい GUI による
グループベースのアクセスポリシー
IP アドレスや VLAN に依存しない
ネットワークアクセス制御

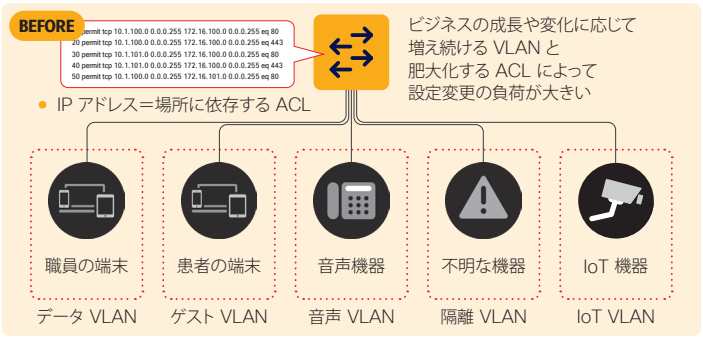
プロファイリング
接続する端末を
可視化および分析
セキュリティポスチャを自動更新
医療機関のリスクを低減

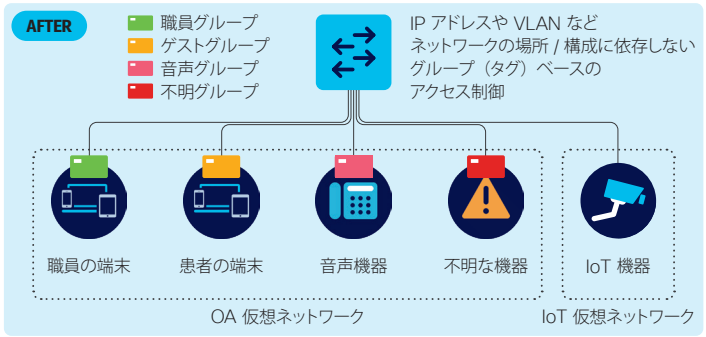
脅威の封じ込め
脆弱性や脅威スコアに基づく
端末自動隔離
サードパーティのエコシステムと
API で連携可能

検疫
端末のポスチャ評価
コンプライアンス準拠を確認
AnyConnect および
EMM/MDM と連携可能

ユーザや端末の「グループ」ベースでアクセス制御

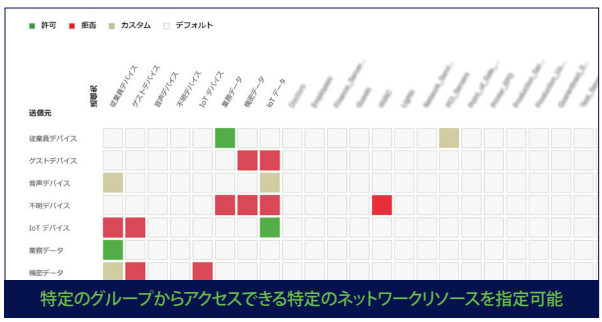
ネットワークの場所や構成に大きく依存するため設定変更の負荷が大きい IP アドレスや VLAN ベースのアクセス制御から、Cisco ISE のユーザや端末の認証に基づくグループベースのアクセス制御に移行すれば、設定変更の負荷を大幅に軽減することができます。

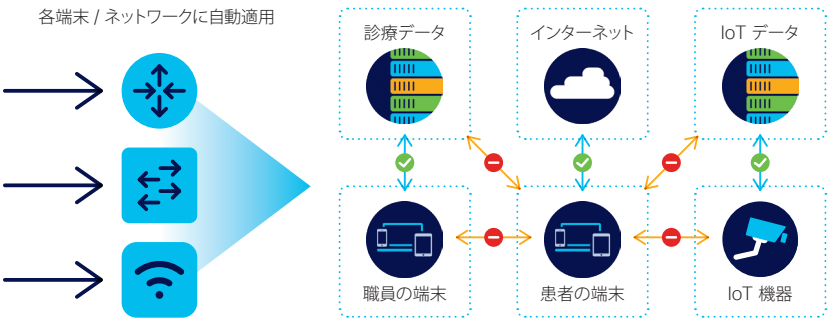




わかりやすい管理画面でアクセス許可 / 拒否を定義可能

シスコのネットワーク機器を一元管理する Cisco DNA Center と連携することで、わかりやすい「ポリシー対応表」で「許可」や「拒否」などのアクセスを定義することができます。人事異動や勤務環境の変更などでユーザの属性が変化するたびに、ACL や VLAN の設定を見直す必要がありません。





Cohesity on Cisco UCS

データ保護

バックアップデータをランサムウェア攻撃から保護できるデータ保護対策

ランサムウェア対策の 1 つとして、しばしばバックアップの重要性が取り上げられますが、巧妙な攻撃者はバックアップデータも標的とすることに注意が必要です。そのため、厚生労働省のガイドライン 5.2 版でも記述されているように、バックアップの適切なあり方を検討および実装しておくとともに、データの復元など万が一の被害に備えた復旧計画を策定しておくことが求められます。

シスコのサーバ製品 **Cisco Unified Computing System（UCS）**なら、業界をリードする Cohesity 社のデータ保護対策を、動作が検証された構成で簡単に導入できます（**Cohesity on Cisco UCS**）。

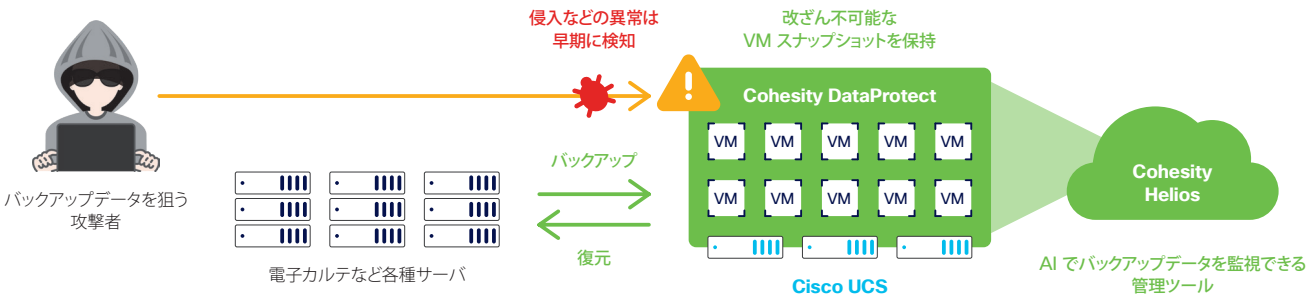
多くの医療機関は日々、大量の医療情報データをバックアップしていますが、Cohesity on Cisco UCS ならデータのバックアップにかかる時間だけでなく、データの復元にかかる時間も数分レベルに短縮できるため、万が一のランサムウェア被害後の迅速な復旧に貢献します。

世代数の制限がないバックアップや、磁気ディスクへの書き込み、データの暗号化（AES-256、FIPS 準拠）など、厚生労働省のガイドラインにもしっかり対応。さらに、データの改ざんや上書きを防止するイミュータブルバックアップ、バックアップデータの監視による異常の早期検知など、ワンランク上のランサムウェア対策を実現します。

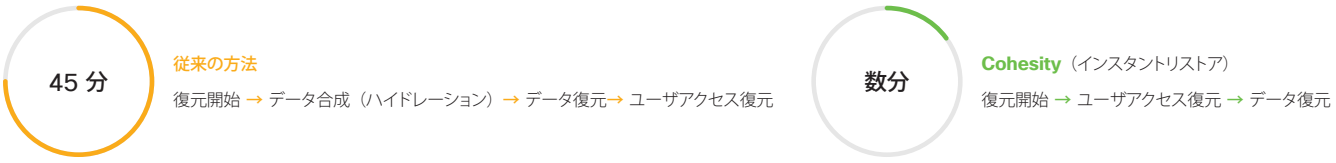
おすすめポイント

- Cisco UCS での動作が検証された構成（Cisco Validated Designs）で Cohesity 社のデータ保護対策を導入可能
- バックアップデータの改ざんや上書きを防止
- 高速なデータ復元でシステムの早期復旧に貢献

AI でバックアップデータを監視、侵入を早期に検知

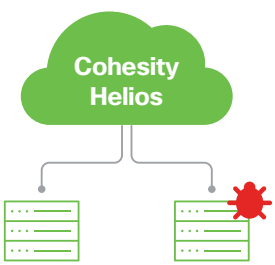


迅速なデータ復元（典型的な 50 MB VM をユーザが利用できるようになるまでの比較）

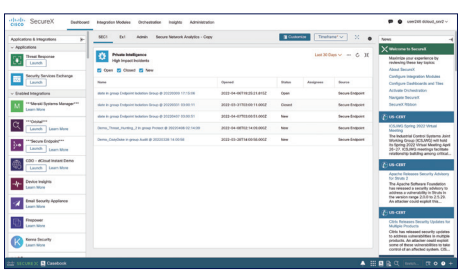


Cohesity + Cisco SecureX でランサムウェア対策をさらに強化

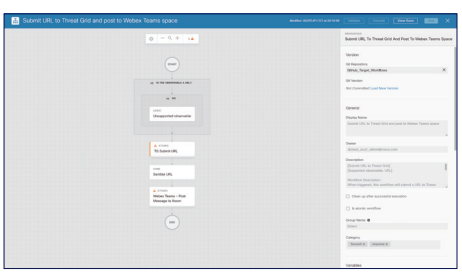
Cohesity ソフトウェアをインストールした Cisco UCS がバックアップサーバとして機能、Cohesity の管理ツール **Helios** で監視します。Cohesity Helios は AI（機械学習）を使用してバックアップデータを監視するため、たとえばランサムウェアの侵入など、異常の早期検知が可能です。異常を検知すると、Cisco SecureX にアラートを送信します。Cisco SecureX では、シスコや他社のセキュリティ製品から得られた情報を連携させて、異常の原因や、異常が脅威として特定された場合の影響範囲を調査できるだけでなく、脅威の封じ込めやデータの復元など、対応作業を自動化することもできます。



バックアップサーバ
Cohesity on Cisco UCS
（Cisco Intersight から簡単導入可能）



Cisco SecureX で異常の原因や
異常が脅威として特定された場合の影響範囲を調査可能
（シスコや他社のセキュリティ製品と連携可能）



Cisco SecureX オーケストレーションで
脅威の封じ込めやデータの復元など
対応作業を自動化可能

シスコ コンタクトセンター

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

©2022 Cisco Systems, Inc. All rights reserved.
Cisco、Cisco Systems、および Cisco Systems ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における商標登録または商標です。
本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。「パートナー」または「partner」という用語の使用は Cisco と他社との間の
パートナーシップ関係を意味するものではありません。(1502R) この資料の記載内容は 2022 年 7 月現在のものです。この資料に記載された仕様は予告なく変更する場合があります。

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

2336-2207-005-TO