

静岡 SBS グループ

(株式会社 静岡新聞社 / 静岡放送 株式会社)



多種多様な職種とデバイス、働き方の変化に対応する 新たな統合セキュリティ対策を実現



製品 & サービス

- Cisco Umbrella
- Cisco AMP for Endpoint
- Cisco Threat Response
- Cisco ISE (Identity Services Engine)

課題

- 複合メディア企業として社内
に多種多様な職務とデバイスが存在
- ランサムウェアなど未知の脅威に
EPP製品での対策に限界
- シンプルな導入と運用が可能な、
統合的なセキュリティ対策を検討

ソリューション

- 多種多様な職務と利用デバイスの
共通したセキュリティ対策として
Cisco Umbrella を導入
- 物理端末のエンドポイントセキュリティに
Cisco AMP for Endpoint を採用
- CTR (Cisco Threat Response) で連携、
統合管理を実現

結果～今後

- 3ヵ月間で約 1,000 件もの脅威への
アクセスを未然にブロック
- インシデント対応の一本化で
レポートもしやすい
- Cisco AMP for Endpoint が持つ
オフライン機能 TETRA の実装も予定
- クラウドサービス、アプリケーションを守る
CASB 機能に期待
- Cisco ISE を発展させ、
SD-Access 環境への移行を検討

静岡新聞社と静岡放送が軸となり幅広いメディア活動を営む静岡 SBS グループは、グローバルスタンダードの知見とテクノロジーを積極的に取り入れ活用し、進化する地域メディア企業を目指しています。今回、新たなセキュリティ対策として Cisco Umbrella と Cisco AMP for Endpoint を導入。多種多様な職種とデバイス、働き方の変化に対応し、安全性と生産性を両立する ICT 利活用環境を実現しました。

インシデントが起きてからではなく、未然に防いでいることが可視化されるシスコ セキュリティ ソリューションの満足度は高いものがあります。

— 株式会社 静岡新聞社 静岡放送 株式会社 システム統括局 システムセンター副部長 松田 武之 氏

課題

静岡 SBS グループは静岡新聞社と静岡放送、2つの会社を軸として形成。静岡県内で新聞、テレビ、ラジオ、Web メディア、イベントなどの幅広いローカルメディア活動を営んでいます。県内外には総局 2カ所、支社 3カ所、支局 25カ所があり、新聞は約 62 万部と県紙（地方新聞）で国内トップの発行部数を誇ります。また、ハワイにある唯一の日本語新聞社や住宅展示場など、さまざまな業種のグループ企業も保有しています。複合的なメディア企業のため社内には新聞編集、ニュースやイベントの取材、Web ニュース配信、ローカル番組の制作、番組編成、広告や CM、新聞の営業、イベント事業などに加えて Web ページ管理、書籍販売など、さまざまな部門や職種が存在し、働く環境も多岐にわたります。さらに同社は 2018 年 4 月から、デザイン思考と企業変革に向けたマインドセットを取得する目的で米国シリコンバレーでの研修を開始し、時代の変化に即応して新たな価値を提供する地域メディアを目指しています。

グループの ICT 管理を行うシステム統括局 システムセンター副部長の松田武之氏は、近年の働き方の変化とそれに伴うセキュリティへの課題を、次のように話します。

「複合メディア企業である当社は一般企業と異なり、24 時間 365 日、どこかからの部署が仕事をしている環境です。その中で当社は働きがい改革と呼ぶ、新たな取り組みを実施しています。オフィス環境もミーティングやコラボレーションスペースを整備し、これまでのように決まった場所、席、端末で仕事をするのではなく、場所や端末も問わず、多様なスタイルで仕事を行うようになってきています。」



株式会社 静岡新聞社 静岡放送 株式会社
システム統括局 システムセンター
副部長
松田 武之 様



株式会社 静岡新聞社 静岡放送 株式会社
システム統括局 システムセンター
穂積 隼人 様

ICT 環境では社内インフラとしてのネットワークシステムを構築しており、仮想基盤を使用した仮想デスクトップを活用してきましたが、Windows 7 のサポート終了が近いことや事業継続的な観点もあり、新たなノート型端末として Google の Chrome OS を搭載した Chromebook の導入が決まりました。そのほかにも社内インフラ以外の独自システムが部署によって導入されており、それらを含めるとさまざまな OS で動く 1,000 台以上の端末が利用されています。また、当時は WannaCry やランサムウェアが蔓延した時期でもあり、これらに共通のセキュリティ対策を必要としていました。そのような多様な環境の中でのセキュリティを数名の担当者で守らなければなりませんので、複雑で手間のかかるものでは運用が回りません。これまでのセキュリティ対策は何かが起こった後に気がついて、そこから対応を取っていくもので、どうしても遅れがちになります。しかし打開する良い解決策がなく、悩んでいました。」

そんな中で松田氏は、展示会で Cisco Umbrella の存在を知る。「世界最大規模のデータ解析を行っている脅威インテリジェンス組織 Cisco Talos の仕組みやリアルタイム性、デバイスに入る前に脅威を遮断する、という考え方がとても魅力的でした。社に戻り、すぐに検討がはじまりました。」(松田氏)

多種多様な職務と利用デバイスに 共通して安全性を高めるセキュリティ対策として、 Cisco Umbrella に着目しました。

ソリューション

社内で利用される多種多様なデバイス

430



Chromebook

共通端末 直接 G-Suite 利用
ブラウザ経由で仮想デスクトップ
持ち出し可

300



シンククライアント

共通端末 仮想デスクトップ用
(一部 Chromebook へ移行予定)

500



仮想デスクトップ

VMware Horizon
(統合:400 / 記者:100)

400



物理端末

仮想デスクトップで
利用できないアプリ用

600



スマートフォン

iPhone & Android

※上記以外にも、新聞制作用 200 台、記者端末 200 台 (Mac 含む) / 印刷局 30 台 / 広告系 130 台 (Mac 含む) / 放送系 80 台 / SBS 学苑 40 台など、利用デバイスが多数存在

Chromebook の本格導入に合わせ Cisco Umbrella を導入

同社はシスコ パートナーを通じて Cisco Umbrella の詳細情報の提供を受けデモを行い、検証を開始。そして 2018 年後半、新たな社内インフラシステム用端末として Chromebook の本格導入が始まるのに合わせ、Cisco Umbrella が導入されました。システム統括局 システムセンターの穂積隼人氏は、Cisco Umbrella の印象と採用の理由を、次のように話します。

「社内 AD の上位 DNS を Cisco Umbrella のアドレスに変更するだけで利用開始できる、導入の簡単さに驚きました。懸念していた Chrome OS への適用も問題ないことがわかり、すぐに採用が決定しました。ユーザー側での面倒な設定が必要なく、意識せずに安全性が高められる点がわれわれの働き方に合致しています。Chromebook は社外に持ち出して利用される機会も多いため、Chrome OS の拡張機能を G Suite で一括管理する形で Cisco Umbrella を利用し、アカウントごとのログまで特定できています。」

物理端末のエンドポイントセキュリティに Cisco AMP for Endpoint を採用

さらに穂積氏は、これをきっかけにエンドポイントセキュリティについてもこれまでの局所的な対策からトータルな対策として何が必要なのか、という検討が加わった、と話します。

「マルウェア対策として従来型の EPP (Endpoint Protection Platform) 製品を利用していたのですが、WannaCry やランサムウェアなどを含めた脅威のすべてをブロックすることはもはや現実的ではありませんでした。ちょうど社内インフラシステムの更新時期ということもあり、侵入される前提で EDR (Endpoint Detection and Response : エンドポイントでの検出と対応) 製品を導入しよう、となりました。半年ほどの期間をかけシスコを含めた 6 社の製品を比較検討し、その結果、2019 年初旬、物理端末の入れ替えに合わせて Cisco AMP for Endpoint の採用も決定しました。AMP なら Umbrella と CTR (Cisco Threat Response) で連携でき、統合管理できるという点が、採用の決め手でした。」

導入ソリューション

DNS レイヤでユーザを最前線で保護するクラウドセキュリティ Cisco Umbrella

Cisco Umbrella は、DNS の名前解決を利用してインターネット上の脅威からユーザを最前線で防御する、「セキュア インターネットゲートウェイ: Secure Internet Gateway (SIG)」です。本社、拠点、外出先などの場所、VPN の ON/OFF を問わず、あらゆるユーザとデバイスを保護できる、最も簡単かつ迅速に導入可能なクラウド型セキュア DNS です。

業界初の DNS の技術によりインターネット上の脅威を未然に防御

- すべてのプロトコルとポートが保護対象悪意あるサイトをアクセス前にブロック
- 目的に応じた柔軟にカスタマイズ可能なアクセスポリシーを設定
- マルウェア (ランサムウェア) 対策にも有効

簡単・迅速な導入

- クラウドベースのソリューションのため、追加のハードウェアなどは不要

働き方改革に最適

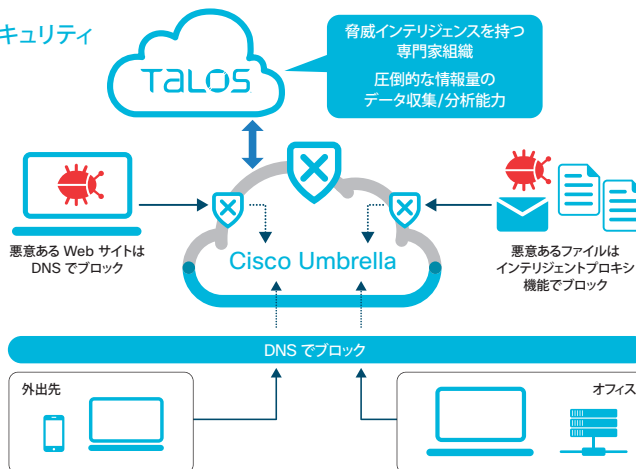
- 社内、社外、VPN 接続の ON/OFF を問わず、あらゆる場所、ユーザ、デバイスを保護

業界最高水準の検知率、最新の脅威に対応

- 世界最大級の解析力と情報提供体制を誇るシスコのセキュリティ インテリジェンス & リサーチグループ「Cisco Talos」と連携し、常に最新のセキュリティを提供

インターネットの利用状況を可視化

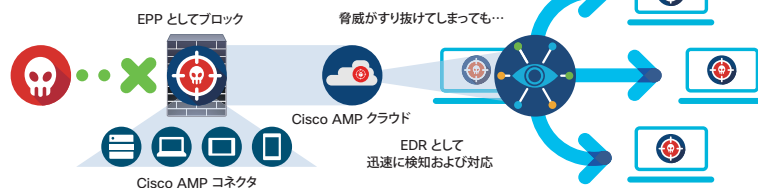
- 脅威に関するさまざまな情報をグラフィカルに可視化
- 意図せず利用しているクラウドアプリケーションなどの「シャドー IT」も見える化



Cisco Umbrella は、DNS の設定を変更するだけで簡単に導入でき、LAN を利用するすべての社内ユーザ、リモートユーザを保護できるクラウドセキュリティ サービスです。世界最大級の解析力と情報提供体制を誇るシスコのセキュリティ インテリジェンス & リサーチグループ (Cisco Talos) と連携し、常に最新のセキュリティを提供。お客様側でソフトウェアやデータを更新する手間がかかりません。

EPP と EDR を兼ね備えた Cisco AMP for Endpoints

Cisco AMP for Endpoints は、EPP と EDR を兼ね備えた次世代エンドポイントセキュリティです。従来は複数の製品やソリューションが必要とされた攻撃サイクル「攻撃前 (Before)」「攻撃中 (During)」「攻撃後 (After)」に、次のような対策を包括的かつ一元的な手段で提供するソリューションです。



脅威の侵入を阻止

15 の検知および防御エンジンとクラウドベースの脅威インテリジェンス (Cisco Talos) で脅威をリアルタイムでブロックします。

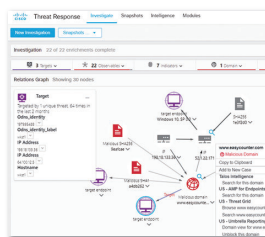
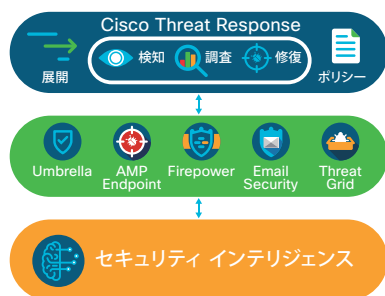
未知の脅威も検知

あらゆるファイルアクティビティを継続的に監視および記録して、隠れた脅威も迅速に検知します。

迅速な対応

検知された脅威の完全な履歴から、迅速かつ過渡的に被害を特定して、ファイルを隔離できます。

オプションのサンドボックス Cisco Threat Grid で、一般的なサンドボックスを大きく上回る高度な静的/動的解析と脅威インテリジェンスをシームレスに統合可能です。



各製品を自動的に統合、検出から修復までを行う CTR (Cisco Threat Response)

CTR は、特定のシスコ セキュリティ製品を自動的に統合し、検出、調査、修復という運用機能を高速化する統合型セキュリティ アーキテクチャです。

製品と統合済

シスコのセキュリティ製品と統合済みで提供されるため、効率的なセキュリティ統合管理が実現します。

時間と労力を削減

サイバー調査を大幅にスピードアップし、修正措置を即座に行うことができます。

追加コスト不要

統合型シスコセキュリティ製品ライセンスがあれば、追加コスト不要です。

Cisco Threat Response は、シスコの各種セキュリティ製品を統合でき、さまざまな脅威情報を集約できます。これによって複数製品にまたがる調査を 1 つのコンソールから実施できます。また発見した脅威は直接隔離するなどの対策が取れます。

結果～今後

導入後の効果と満足度について、松田氏は次のように語ります。

「導入後、すぐにセキュリティに関する問い合わせが減り、その効果を実感しました。管理者側としてもインシデントが起きた際の対応も一本化されますし、定期的に社内の情報セキュリティ委員会で報告する際のレポートも非常に楽になりました。Cisco Umbrella は 3 か月間で約 1,000 件、1 日平均 10 件近くの脅威へのアクセスを止めている計算になります。インシデントが起きてからの対応ではなく、未然に防いでいることが可視化されるので、満足度は高いですね。今年度は Cisco AMP for Endpoint が持つオフライン機能の TETRA の実装も予定しています。」

静新 SBS グループ



株式会社 静岡新聞社

設立 1941年12月1日
資本金 1億5,000万円
社員数 438名
社長 大石剛
本社 静岡市駿河区登呂3-1-1
支社支局 県内外に3支社、2総局、25支局
(静岡新聞社と静岡放送の事業を兼務)
業務内容 新聞発行、出版、Web など

静岡放送 株式会社

設立 1952年10月1日
資本金 1億8,000万円
社員数 238名(2014年4月現在)
社長 大石剛
本社 静岡市駿河区登呂3-1-1
支社支局 県内外に3支社、2総局、25支局
(静岡新聞社と静岡放送の事業を兼務)
業務内容 テレビ、ラジオ、データ放送、
Web など

■静岡新聞社は1941年、県下有力新聞6社が合併して誕生。1961年、新聞界の先陣を切ってカラー印刷を開始、1964年東京オリンピックのカラー写真が注目されて以来カラー印刷技術は業界トップクラスの評価を受け、2006年には「国際新聞カラー品質コンテスト」で世界3位、日本の新聞では初受賞を果たした。発行部数は約62万部と県紙としては常にトップを誇る。

■静岡放送は静岡県初の民間放送会社として1952年にラジオ放送、1958年にテレビ放送を開始。業界に先がけてラジオ、テレビの自動送出装置を導入、2000年にPC向けデータ放送を開始、2005年に県内の民放に先駆けデジタル放送を開始するなど、新しいメディアに対し常に研究を続けている。現在、テレビ中継局59局、ラジオ中継局12局を有し、静岡県下をくまなくカバーしている。

加えて穂積氏は、アプリケーションの安全性を高める役割への期待を語ります。

「アプリケーションの利用状況の把握はシャドウ IT の抑制にも効果を発揮します。いま、当社では G-Suite を利用していますが、今後、Office365 などほかのクラウドサービスの利用が拡大していくと想定されます。Cisco Umbrella の CASB 機能を活用してたとえば Office365 の OneDrive だけを禁止する、といった使い方も可能なことがわかってきており、ファイルインスペクションの機能と共に検討を進めています。」

最後に今後の展開とシスコへの期待について、松田氏は次のように語ります。

「すでに活用を開始している Cisco Umbrella と Cisco AMP for Endpoint、CTR だけでなく、認証基盤として Cisco ISE (Identity Services Engine) も導入済みです。これをさらに発展させて、SD-Access 環境への移行検討を具体的に進めています。われわれは少ない人数でグループ全体の ICT を管理していますので、セキュリティを維持しながら、時代の変化へ迅速に、しかも簡単に対応できるようにすることで運用工数の削減を目指したいです。24 時間 365 日何かしらの業務が動いていて、多種多様な職務とデバイスが存在する社員に対しても、より安全で生産性を高められる環境を提供したいと考えています。こうした課題を 1 つずつクリアしていくために、幅広い知見と技術力で長年に渡って当社の情報基盤の企画から検討、導入、運用を支援いただいているシスコ パートナーとの協働により、実現に向けたチャレンジを続けていきます。シスコにはこれからも、誰もがよりわかりやすく、使いやすいソリューションの提供に期待しています。」

その他の詳細情報

Cisco Umbrella の詳細は、

www.cisco.com/jp/go/umbrella を参照してください。

Cisco AMP for Endpoints の詳細は、

www.cisco.com/c/ja_jp/products/security/amp-for-endpoints/ を参照してください。

Cisco Threat Response の詳細は、

www.cisco.com/c/ja_jp/products/security を参照してください。

「働きがい」を高める静岡新聞本社オフィス

丹下健三氏設計の歴史ある本社ビル内は、コミュニケーションの活性化と生産性向上を目指し、いたるところに木のぬくもりのあるフリーのコラボレーションエリアが新設され、社員の働きがいを高めています。地域に貢献するメディアとして、市内を一望できる高層レストランや、地元小学生の社会科見学コースとしても知られています。



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10:00-12:00, 13:00-17:00

0120-092-255

お問い合わせウェブフォーム

cisco.com/jp/go/vdc_callback



©2020 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2020年2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

<http://www.cisco.com/jp>