

読売テレビ放送株式会社 様

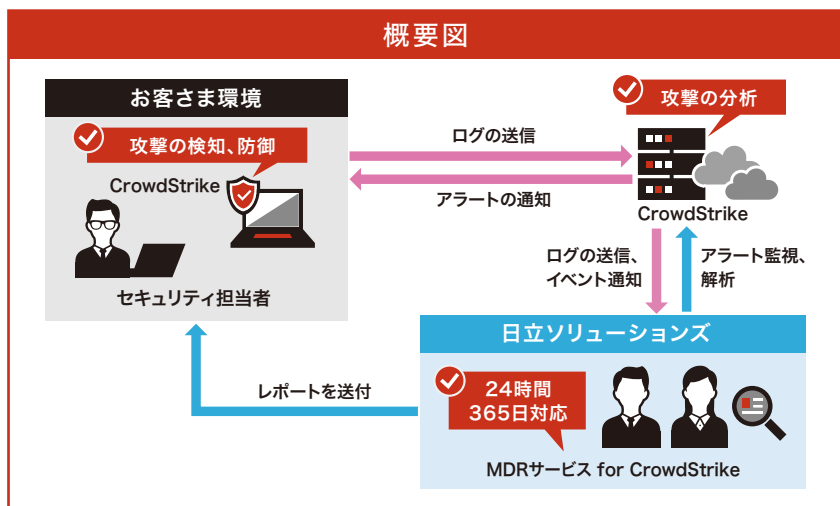
CrowdStrike・MDRサービス for CrowdStrike

EDRの導入で盤石なエンドポイントセキュリティへ大きく前進
24時間365日監視を専門家に任せて担当者の業務負荷を軽減



昼夜を問わず稼働しているテレビ業界にとって、放送停止という事態は絶対に回避しなければなりません。読売テレビ放送株式会社は、年々高度化・巧妙化していくサイバー攻撃の脅威に備え、ユーザーに最も近いレイヤーでの防御策を強化するべくEDR(Endpoint Detection and Response)の導入を決断。24時間365日の継続的な監視体制を確立するため、「CrowdStrike」と「MDR(Managed Detection and Response)サービス」をセットで導入しました。導入後は監視業務やアラート対応における担当者の負荷が大きく軽減され、さらなるセキュリティの強化に向けて、次の一手の検討も始まっています。

課題	効果
サイバー攻撃の手口が高度化・巧妙化しており、シグネチャベースの防御策ではリスクを回避しきれない	ユーザーの異常な行動パターンの検知によって既知・未知両方の脅威を早期に発見
過剰投資は避けつつも、セキュリティの強化はしたい	脅威の検知から防御、侵入後の分析・対処までを1製品でカバーすることで、安全性の確保と適切な投資を両立
24時間365日監視のための社内リソースが足りず、アラート対応のナレッジも乏しく正確な判断が難しい	セキュリティの専門家による高度な監視体制により、運用業務から解放され担当者の負荷が大幅に軽減



所在地 大阪府大阪市中央区城見1丁目3番50号

設立 1958年2月13日

従業員数 607名(2025年3月31日現在)

事業内容 放送法による基幹放送事業、放送番組の企画、制作および販売 ほか

URL <https://www.ytv.co.jp/>



DX推進局
情報システムグループ
土井 大志 氏



DX推進局
情報システムグループ
梅田 涼氏



DX推進局
情報システムグループ
谷 尚大氏

※所属は導入当時の
ものです

背景 シグネチャベースの防御策だけでは不十分に

日本テレビ系列の準キー局である読売テレビ放送株式会社は、1958年に大阪で開局して以来、報道番組から情報番組、バラエティ、ドラマ、スポーツ、アニメに至るまで、幅広いジャンルで人気番組を生み出し続けてきました。

社会の信頼に応える放送を実現するうえで、情報システム部門に求められることについて梅田氏はこう語ります。

「テレビ業界においては、放送停止という事態が最も大きな懸念事項です。具体的には、視聴者情報や放送素材などの機密情報の漏洩、スマートデバイスの脆弱性を突いた攻撃やランサムウェア感染による業務停止、テレワーク環境における感染被害などを主なリスクとして認識しています。また、今後放送設備のIP化*を進めるにあたっては、サイバー攻撃の標的化も懸念されます。24時間365日放送を届ける放送局にとって、セキュリティインシデントの発生による放送停止は絶対に避けなければならない事態であると考えています」

これまで同社は、CIS(Center for Internet Security) ControlsやNIST(National Institute of Standards and Technology)サイバーセキュリティフレームワークを指標としながら最新のセキュリティモデルの実装を進めてきたなかで、ユーザーに最も近いレイヤーでの防御策としてEDRの導入が必須であると考えていました。「もちろん何もして来なかったわけではなく、エンドポイントのセキュリティ対策としてEPP(Endpoint Protection Platform)製品を導入していました。ただ、年々高度化・巧妙化するサイバー攻撃に備えるためには、シグネチャベースの防御策だけでは不十分だと感じるようになっていたのです」と梅田氏。EDR導入は、従来の境界型の対策に代わり、ゼロトラストセキュリティの実現という大きなゴールに向かうための取り組みの一つでもありました。

*従来のSDI(Serial Digital Interface)ケーブルで映像や音声を送っていた仕組みを、IP(Internet Protocol)を使ったネットワーク伝送に置き換えること

取り組み 検知力の高さにコストを加味してEDRを選定

EDR製品の選定にあたっては、検知力、使い勝手、コストをポイントに競合製品を含む3つの製品を比較検討したという同社。同一の検体でPoC(Proof of Concept)を実施したところ、検知力の高さで高評価を獲得したのが、日立ソリューションズが提案した「CrowdStrike」でした。「『CrowdStrike』は世界的にこの分野におけるフロントランナーであると認識していましたし、実際、アナリスト企業が発表するレポートで高い評価を得ていることも知っていましたので、大きな期待がありました。当社の規模に対して過剰投資にならないよう、コストとのバランスを考慮しながら検討を進めた結果、『CrowdStrike』がベストな選択であるとの結論に至りました」と梅田氏。

当時の日本国内での実績だけを考えれば、「CrowdStrike」の選択に不安がなかったわけではありませんが、日立ソリューションズからの提案と信頼関係が同社の決断を後押ししました。日立ソリューションズが持つ、既存資産やネットワーク構成の分析力、想定される課題を考慮した提案、導入後の運用を見据えた設計などの技術やノウハウも同社にとって大きな評価ポイントとなりました。また、複数製品を候補に挙げるのではなく、「CrowdStrike」にしばって提案した日立ソリューションズについて、

「パートナーとして当社のシステムに携わっていただいております。ハードウェアからソフトウェアまで当社の既存環境を熟知されていることが最大のアドバンテージであったことは間違いありません。要望にもとづいて対応するというより、当社環境の状況や注意すべきポイントを把握したうえで提案いただけている安心感がありました」と谷氏。

土井氏も「過去にさまざまな製品選定で一緒に取り組んだ実績から、我々がこだわるポイントを理解されています。ある程度スクリーニングしたうえで提案されていることも想像できたので、『CrowdStrike』を提案いただいた時点ですぐに検討を開始しました」と語ります。

効果 「CrowdStrike」と「MDR」でセキュリティ強化と負荷軽減を両立

同社は「CrowdStrike」の導入によって既知・未知の脅威に対して検知から防御、侵入後の対処・攻撃の分析までを対策すると同時に、日立ソリューションズがインシデントの監視からインシデント発生時の対応支援までをワンストップで提供する「MDRサービス」をセットで契約。「EDRは最後の砦。そこに、『CrowdStrike』が入っているというのは大きな安心感があります」と語る梅田氏。続けて、「その一方で、サイバー攻撃の高度化・巧妙化に伴い、攻撃者がシステムに侵入してからほかのシステムへの横展開を始めるまでの時間が短縮し続けており、数分で被害が拡大するケースもあります。万が一インシデントが発生した場合の対応として24時間365日の継続的な監視と、インシデント発生時の被害の拡大防止、迅速な復旧までを社内のリソースだけで対応するのは基本的に不可能であり、『MDRサービス』を利用するという選択は必須要件だと考えていました」と説明します。「実際、我々の目が行き届かない休日も、監視が継続している状態を維持できるようになりました。アラートが発生した際には専門家の方々が分析を行い、我々が理解しやすい形でレポートにしてくれるので、その内容にもとづいてしかるべき担当者にスムーズにエスカレーションできます。従来はアラートの内容を自分たちで調べて、確信がないところで判断せざるを得ない場面もありましたが、導入後は担当者の負荷が大きく軽減されたうえに、セキュリティインシデントを抑えることができています。これが一番の成果です」と(土井氏)

「CrowdStrike」と日立ソリューションズの専門家による監視体制が揃ったことで、放送を止めないための強固なセキュリティの環境が整いつつあります。

展望 EDRとSIEMを組み合わせて対策を強化

同社は、EDRである「CrowdStrike」の導入に続き、多様なセキュリティ機器からログデータを収集・管理するSIEM(Security Information and Event Management)も導入。「今後はEDRとSIEMの組み合わせにより、さらに強固なセキュリティ対策を実現していく考えで、日立ソリューションズには引き続き支援をお願いしたい」と谷氏。

信頼性の高い製品を味方に付けた安心感と、EDR運用を専門家に任せることから来る安心感とで、これまで抱えてきた不安感が大きく払拭された同社。より戦略的なタスクに集中できる環境を得て、セキュリティインシデントを起因とする放送停止リスクの回避に向けた次の一手についても検討が始まっています。

※本事例の内容は公開時点(2026年4月3日)の情報です。*CrowdStrikeは、CrowdStrike, Inc.の米国およびその他の国における商標または登録商標です。※本文中の会社名、商品名は各社の商標、または登録商標です。※本文中および図中では、TMマーク、®マークは表記していません。*製品の仕様は、改良のため、予告なく変更する場合があります。*本製品を輸出される場合には、外国為替及び外国貿易法ならびに米国の輸出管理関連法規などの規制をご確認のうえ、必要な手続きをお取りください。なお、ご不明な場合は、当社担当営業にお問い合わせください。*本文中の情報は、事例作成時点のものです。

株式会社日立ソリューションズ

www.hitachi-solutions.co.jp



本事例のwebページはこちら

www.hitachi-solutions.co.jp/crowdstrike/case01/



本カタログ掲載商品・サービスの詳細情報

CrowdStrike
www.hitachi-solutions.co.jp/crowdstrike/



MDRサービス for CrowdStrike
www.hitachi-solutions.co.jp/security/sp/
solution/task/mdr_crowdstrike.html