The bridge to possible

株式会社ＪＲ東日本情報システム

クラウド移行や働き方改革にも柔軟に対応 シスコと共に運用するセキュリティ監視「ハイブリッドSOC」

システムのクラウド化が進む中、限られた人員で約300のシステムのセキュリティ監視をどう行うか。この課題を解決するためにＪＲ東日本情報システム（JEIS）はセキュリティアーキテクチャを構築し、「Cisco Advanced Cloud Threat Analytics Service」を活用して「ハイブリッドSOC」を運用しています。リモートワークやクラウドサービスの利用など、新たな領域へも柔軟に対応しています。

株式会社 ＪＲ東日本情報システム

本社所在地
東京都新宿区大久保三丁目８番２号
新宿ガーデンタワー 7F

設立
1989 年 11 月 24 日

社員数
1,690 名（2023 年 4 月 1 日現在）

The bridge to possible

JR 東日本グループの一員である JEIS。「駅から街まで。日常に、さらなる革新を。」を掲げ、鉄道システムで培った高い技術力、先端 ICT を使って新しい価値を生み出すための研究開発力を背景に、同グループの事業を支える ICT システムの企画、開発、運用を担っています。

課題

- データセンターや社内といった内部のリソースを中心にしたセキュリティ対策からの脱却
- 運用中のシステムへの影響を最小限にした SOC サービス（Managed Security Service）の採用
- マルチベンダーで構成されたシステムに対する効率的かつ効果的なインシデント解析
- リモートワークやクラウドサービスの利用など、新たな領域への対応
- エンドポイントセキュリティへの対応

ソリューション

- シスコのマネージドセキュリティサービスの1つであるCACTAS（Cisco Advanced Cloud Threat Analytics Service）を通じて、システムの監視と脅威検知、通報業務をサポート
- シスコと EA（Enterprise Agreement）契約を締結。戦略的なパートナーシップを結ぶ

結果

- 24 時間、365 日のインシデント監視体制を確立
- マルチベンダーで構成されたシステムも監視可能
- エンドポイントの監視も可能
- 重大なインシデントを確実に知得し、誤検知、過検知も少ない効率的で的確な SOC 運用を実現

今後

- JR 東日本グループ会社に対して、エンドポイントのマネージドセキュリティサービスを展開し、JR 東日本グループにおける統一的なセキュリティ対策を実現

膨大なログから セキュリティインシデントを 確実にキャッチする シスコのCACTASを 中心としたSOC体制を 構築・運用しています

関口 義弘 氏

株式会社 J R東日本情報システム
ICT 基盤本部
セキュリティ対策室
次長

The bridge to possible

課題

**限られた人員で多種多様なシステムの
セキュリティインシデントをいかに効率的に対処するか**

JR 東日本グループの事業は、「運輸事業」、「流通・サービス事業」、「不動産・ホテル事業」など、多岐にわたります。JEIS は「Suica・駅サービスソリューション」「鉄道事業ソリューション」「生活・企業経理サービスソリューション」「システム基盤」という 4 つのドメインを主軸に、それらの事業を支える幅広いシステムを展開しており、約 300 の多種多様なシステムを運用しています。

また、システムの種類や数だけでなく、同社が担っている役割も多岐にわたります。システムの開発や運用に加えて、セキュリティの強化や運用も同社の重要な役割。仮にサイバー攻撃によって重大なインシデントを発生してしまうと、社会全体が混乱するリスクがある――。JR 東日本グループの ICT をリードする技術集団として、お客さまの信頼に応え、すべての人の心豊かな生活の実現に貢献するという企業理念のもと、強い使命感を持ち、JR 東日本やグループ会社と一体になって、様々なセキュリティインシデント対応にあたっています。

「システム開発時に必要なセキュリティ機能を盛り込むのはもちろんのこと、グループ各社の ICT の利用状況をチェックして JR 東日本グループのセキュリティルールが遵守されているかを確認したり、必要に応じてシステム設計や運用に関するアドバイスを行ったり、セキュリティに関する様々な関連業務を担っています」と関口 義弘氏は話します。

システムログなどを分析して、サイバー攻撃を検知したり、対策を検討したりする SOC（Security Operation Center）の運用も同社が行っているセキュリティ業務の 1 つです。しかし、前述したとおり同社が管理しているシステムは多種多様であり、全てのシステムログを収集、分析して監視を行い、サイバー攻撃の兆候を発見することは容易ではありません。

「休みなく稼働するシステムもあるため SOC は 24 時間 365 日対応が基本ですが、既存の人員や体制では、とても対応ができません。さらにほとんどのシステムやデバイスが社内にあった頃とは違い、最近は一部がクラウドや自宅などの社外へも拡大しています。そうすると、それらのシステムやデバイスをどのように監視するのかという課題も出てきます」と米津 宏太郎氏は言います。

**社内のデバイスのみならず、
クラウドや自宅など
社外にある
システムやデバイスの
監視にも対応**

ソリューション

**セキュリティ監視に精通したベンダーと連携した
ハイブリッド SOC を目指す**

膨大なシステムとデバイス数、限られた人員と体制という課題を解決し、最適な SOC 運用を実現するために、同社は SOC 運用を協業して担うことが可能なベンダーを模索しました。

「セキュリティ監視・運用の全てを委託するのではなく、お互いの強みを活かした『ハイブリッド SOC』を目指しました。具体的には、インターネット境界における監視と分析、インシデントの予兆を検知した際の通報をベンダーに依頼。通報を受けた後の対処は私たちやグループ会社で行うという役割分担です。例えばログを一見する限りは危険な事象に見えても、現場にインタビューすると、背景や要因が明らかになり、無害な事象だと判断できる場合もあります。危険な事象と判断する場合も同様のプロセスを踏むことで確実な対応が可能です。このようなインシデントかどうかのジャッジは、ベンダー任せにせず、実際に現場でのシステムの使い方や業務ノウハウを有する私たちが行った方が効率的と考えられるからです」と関口氏は説明します。

**既存システムの運用に対する影響が最小限
シスコのログ収集・分析の仕組みは魅力的**

このようなハイブリッド SOC の運用方針に基づき、同社は複数のベンダーの提案を比較し、最終的にシスコの提案

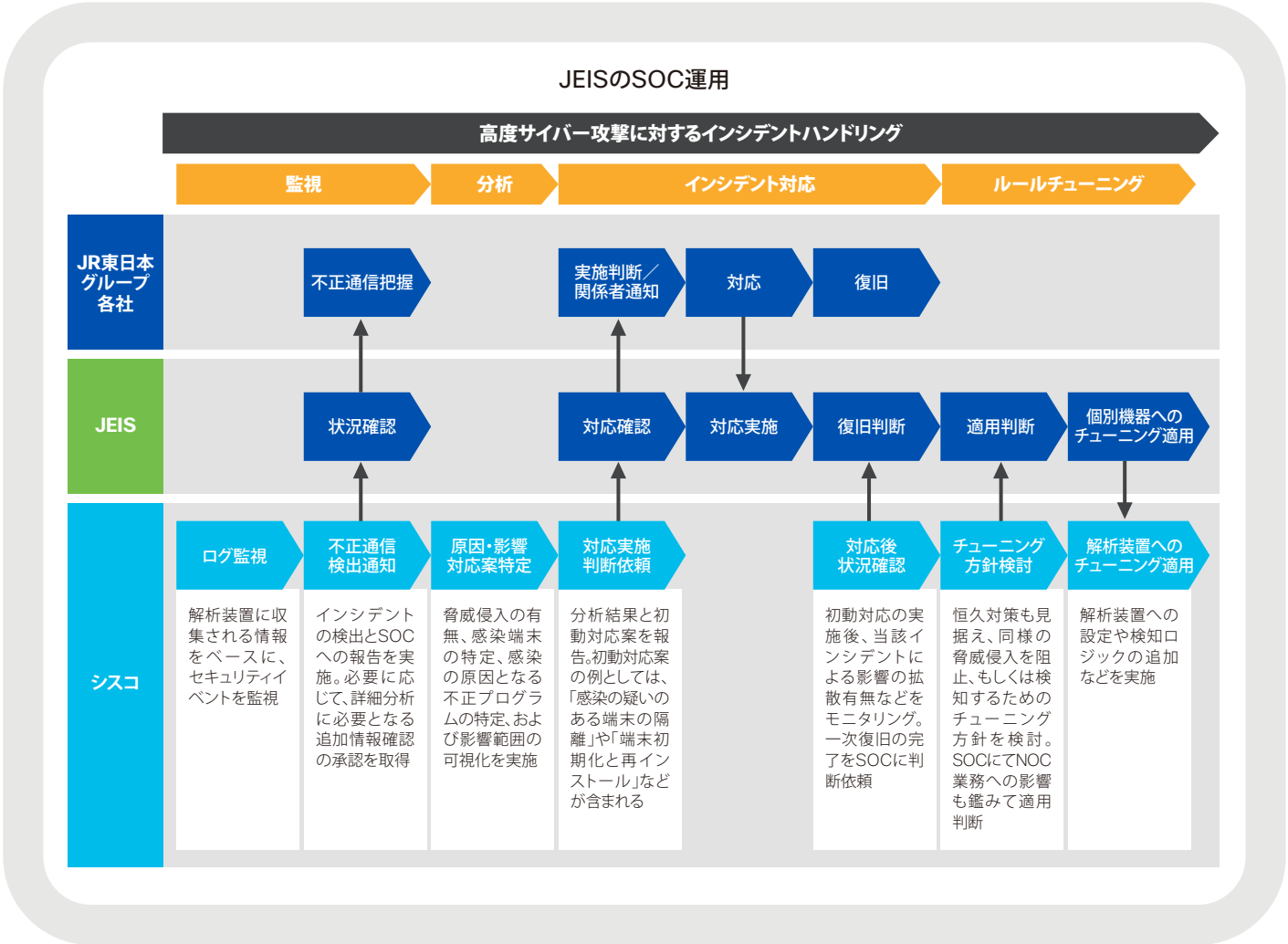
を採用しました。

「まず評価したのが対応力の高さです。多種多様なシステムは、様々なベンダーの製品やサービスで構成されています。あるベンダーからは『特定の機器の監視やログ分析にしか対応できない』と言われたのですが、シスコは『どんな機器やサービスにも対応する』と約束してくれました」と米津氏は言います。

また、脅威インテリジェンスとの連携、ログ収集、分析、通報を統合的に対応可能なことも評価しました。

「SOC サービスを提供している他社からは『ログを収集し、送信する仕組みの構築を JEIS 側で行ってほしい』と言われました。それはある面では当然の要求であると思うのですが、設計変更を伴い運用面でも大きな負担になってしまいます。それに対して、シスコはログ収集の工数がかからない監視方法を提案してくれたのです」（米津氏）

その後、クラウド利用や在宅勤務の拡大などで、共通のインターネットゲートウェイを通過しない通信が増え、その対応が課題となりましたが、それに対してもシスコは速やかに解決策を提示。「リモートワーク可能な PC などを含む約 6 万台を超えるデバイスは、当社がマネージドサービスとしてグループ会社に提供している『JR 東日本エンドポイントセキュリティサービス（JRE-ESS）』で保護しています。そこから収集できるエンドポイントのログを解析することで課題を解決しています。また、パブリッククラウドに移行したシステムについても、ログを CACTAS と連携して SOC による監視を行っています。このように、時代の変化や様々なシステム構成に柔軟に対応できるシスコの姿勢には大きな信頼を寄せています」と関口氏は話します。



The bridge to possible

結果～今後

CACTAS の分析精度の高さに驚き

このような方法でシスコは、JR 東日本グループの多種多様なシステムのセキュリティを 24 時間 365 日体制で監視。シスコが誇る脅威インテリジェンス&リサーチ グループ Cisco Talos の情報などを参考にしながら Cisco SOC チームが分析を行い、不正な通信など脅威の足跡を検知し、重大な兆候があった場合は JEIS に通知しています。

「実際に運用を開始してから 3 年が経過しましたが、良い意味で予想を超えてくれたのが CACTAS の分析精度の高さです。危険度を 4 つのレベルに分類し、最も緊急性が高い事象と、2 番目に危険な事象に限り通知してもらうようにしているのですが、この判断が本当に的確であると感じます。軽微な兆候に必要以上に振り回されたり、重大な兆候を見逃してしまったりという事象はこれまでにほとんどありません」と関口氏は強調します。

シスコの CACTAS 運用チームとは定期的なミーティングを通して、検知した事象の振り返りや最新のセキュリティ動向などを共有して、どのようなシステムが攻撃対象になりやすいかなどを把握し、対策の強化に役立てています。

また、同社はシスコのサポートの幅広さや柔軟な対応も高く評価しています。

「サイバー攻撃の最新動向をアナリストがレポートにまとめたり、インターネット上に拡散している JR 東日本グループに関する情報を収集して、なんらかの危険を感じたら注意を促したり、SOC 監視の枠を超えて、私たちのセキュリティ業務をサポートしてもらっています。諸外国の要人が来日するなどのイベント開催期間など、一定期間、特定のシステムの監視レベルを強化するなど、監視のチューニングなどにも柔軟に対応してくれます」と米津氏は述べます。

シスコと共にさらなるセキュリティ強化に取り組む

同社は、クラウドシフトが進む新しいシステム環境の安全性を高めるためにもシスコ製品を積極的に活用したいと考えており、シスコとの間で EA（Enterprise Agreement）契約を提携し、戦略的なパートナーシップを結んでいます。今後は、このパートナーシップを有効活用し、さらなるセキュリティの強化を図っていきます。

「現在、エンドポイントセキュリティサービスである JRE-ESS の機能強化をシスコと共に行っています。マルチベンダーに対応できるシスコ社の SOC サービスに今後も期待しています」と関口氏は最後に述べました。

株式会社ＪＲ東日本情報システム
ICT 基盤本部
セキュリティ対策室
次長
関口 義弘 氏

株式会社ＪＲ東日本情報システム
ICT 基盤本部
セキュリティ対策室
上級エキスパート
米津 宏太郎 氏

The bridge to possible

JR東日本グループのICTをリードする技術集団として、様々なソリューションを提供。社会インフラを支えている。

URL https://www.jeis.co.jp/

製品 & サービス

- CACTAS (Cisco Advanced Cloud Threat Analytics Service)
- Enterprise Agreement

2376-2306-000-BL