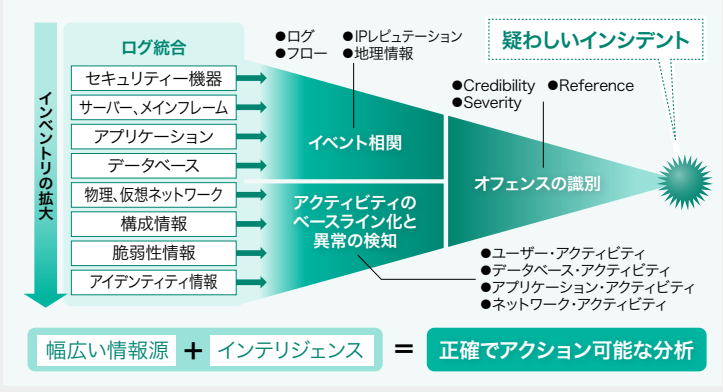
お客様事例


# セキュリティーに関する膨大なログをIBM Security QRadar SIEMで統合管理し、急増するサイバー攻撃に迅速対応

大手企業や公的機関からの情報漏えい事件が相次ぎ、悪質化するサイバー攻撃に危機感を募らせた三井生命保険株式会社（以下、三井生命）は、技術と組織の両面からセキュリティー対策の強化を図ってきました。しかし、そうした中でも検知する脅威情報は急速な勢いで増加しており、もはや人手に頼ったセキュリティー監視は限界に達していました。そこで導入したのが、IT環境全体を可視化し、危険予測を自動化するセキュリティー・インテリジェンス・プラットフォームであるIBM Security QRadar SIEMです。IBM Security QRadar SIEMは、リアルタイムで大量のログを相関分析し、システム上で発生している異常を検知、予期される脅威をいち早く発見します。さらに、ビジネス上のリスクが大きいと想定されるインシデントを特定し、警告してくれます。セキュリティー担当組織のメンバーは、IBM Security QRadarのアラートにしたがい、優先順位を付けて迅速且つより確実な対応処理を行うことができるようになりました。

## ［導入製品］ IBM Security QRadar SIEM




### 課題

- 既存のセキュリティーに対する脅威や情報が急増しており、全てを人手に任せる監視は困難
- セキュリティー脅威はますます高度化・巧妙化しており、より高い精度での脅威の発見が急務

### ソリューション

- 多岐にわたるセキュリティー対策機器やネットワーク機器、サーバーから収集したイベント・ログを統合的に管理し、相関分析を行う

### 効果

- 日本語化されたGUIを搭載、導入に関するマニュアルも充実しており、短期間でのシステム構築および実業務への展開が可能
- セキュリティー・イベント検知時の調査および作業の効率化
- 膨大なログ情報を分析し、本当に対処すべきインシデントを特定

## [ お客様課題 ]

### イベント・ログを統合管理する SIEMのアプローチに注目

標的型攻撃に代表されるサイバー攻撃による被害は後を絶たず、大手企業や公的機関からも大規模に個人情報が漏えいするなど深刻な社会問題となっています。

こうした状況に三井生命は危機感を募らせており、同社 システム企画部 CSIRT担当室長の恒本 均氏は、「サイバー・セキュリティーを統括するCSIRT（Computer Security Incident Response Team）、セキュリティー・リスクを監視するSOC（Security Operation Center）を2015年に立ち上げ、CISO（Chief Information Security Officer）を中心に社内体制を強化してきました。もちろんファイアウォールやIPS（Intrusion Prevention System）、マルウェア検知など、サイバー攻撃を水際で防御する仕組みについても継続的な改善・強化を図っています。しかし、他社での被害事例を見ても、サイバー攻撃から自社を完全に防御することはもはや不可能です。侵入・侵害といったサイバー攻撃をいかに迅速に検知できるか、が非常に重要であるといえますが、その一方で、システムやネットワークから発生する膨大な量のログやアラートを、人手により監視・分析を行い続けることは限界に近付いていました」と話します。

そうした中で三井生命が着目したのが、多岐にわたるセキュリティー製品やネットワーク機器、各サーバーから収集したイベント・ログを統合管理するSIEM（Security Information and Event Management）の活用です。

「監督官庁である金融庁の指針でも、特に検知に関して『通信ログ・イベントログ等の取得と分析、不適切な通信の検知・遮断通信記録（ログ）等の取得・分析を含むサイバー攻撃に対する監視等』が求められており、SIEMの導入は必須であると考えました」と恒本氏は話します。

膨大なログをリアルタイムに分析し、未知の脅威に対する検知精度を向上していく上で、今後はディープ・ラーニングやAIの能力が不可欠になると考えています。

三井生命保険株式会社
システム企画部
CSIRT担当室長
**恒本 均氏**

## [ ソリューション ]

### 他社製品を圧倒する 豊富なテンプレートを標準搭載

SIEMにターゲットを絞りソリューション選定を進める中で、三井生命が出会ったのがIBM Security QRadar SIEMです。

「2016年7月に開催されたIBM QRadar アップデート・セミナーに参加したのがきっかけです。その場で示された製品ロードマップによると、IBMはセキュリティー製品ポートフォリオのコアにIBM Security QRadar プラットフォームを据えようとしており、将来性があると感じました。既存ユーザーの参加者からも話を聞いてみたところ総じて評価は高く、弊社にとっても最適なソリューションになると判断しました」と恒本氏は話します。

さらに三井生命グループのIT戦略の中核としての役割を担っているSIパートナー、エムエルアイ・システムズ株式会社（以下、エムエルアイ・システムズ） 技術・運用本部 テクニカルグループ 主任システムズ・デザイナーの我妻 祐樹氏が、「セキュリティー対策は社内の知見を磨くことが大切という考え方から、私たちはSIEMについても自らシステム構築・運用にあたることを基本としています。その点、IBM Security QRadar SIEMは世界的なセキュリティー研究開発機関であるIBM X-Forceの知見に裏付けられた数百種類の分析ルールおよび1,000種類を超える検索パターンなど、他社製品を圧倒する豊富なテンプレートを標準で備えています。このソリューションを通じて最新のセキュリティー対策を進められることは大きな魅力でした」と続けます。

また、「短期間で実業務への展開が可能なことも選定の決め手となりました」と話すのは、エムエルアイ・システムズ 技術・運用本部 テクニカルグループ 主任システムズ・スペシャリストの平井 芳直氏です。

「先に恒本さんが指摘されたように、もはや人手による監視と分析作業は限界に近付いており、新年度からSIEMの運用を開始したいという強い要望がありました。IBM Security QRadar SIEMは日本語化されたGUIを搭載するほか、マニュアルも充実しており、スムーズに構築作業に入ることができます」

実際、IBM Security QRadar SIEMの導入が正式に決定したのは2017年1月中旬のことで、4月の運用開始までに、システム構築には実質2カ月の猶予しか残されていませんでした。そこで三井生命とエムエルアイ・システムズは、まず情報漏えい対策で最優先の課題となる出口対策に全力を集中。ファイアウォールやIPS、プロキシ・サーバー、標的型攻撃対策システムなどのセキュリティー製品から発生するログの収集および相関分析ルールの定義を進めていきました。

その結果、三井生命は当初の計画をさらに短縮し、2017年3月末よりIBM Security QRadar SIEMの運用を開始することができました。

「導入の初期段階で基本機能と概念をしっかり理解しておけば、IBM Security QRadar SIEMは多様なセキュリティー製品から発生する新たなログを収集すると同時に運用に移行することも可能です。非常に即効的であり、どんな企業にもなじみやすい環境を提供していると思います」と我妻氏は評価します。

セキュリティー対策は社内の知見を磨くことが大切という考え方から、私たちはSIEMについても自らシステム構築・運用にあたることを基本としています。

エムエルアイ・システムズ株式会社
技術・運用本部 テクニカルグループ
主任システムズ・デザイナー
**我妻 祐樹氏**

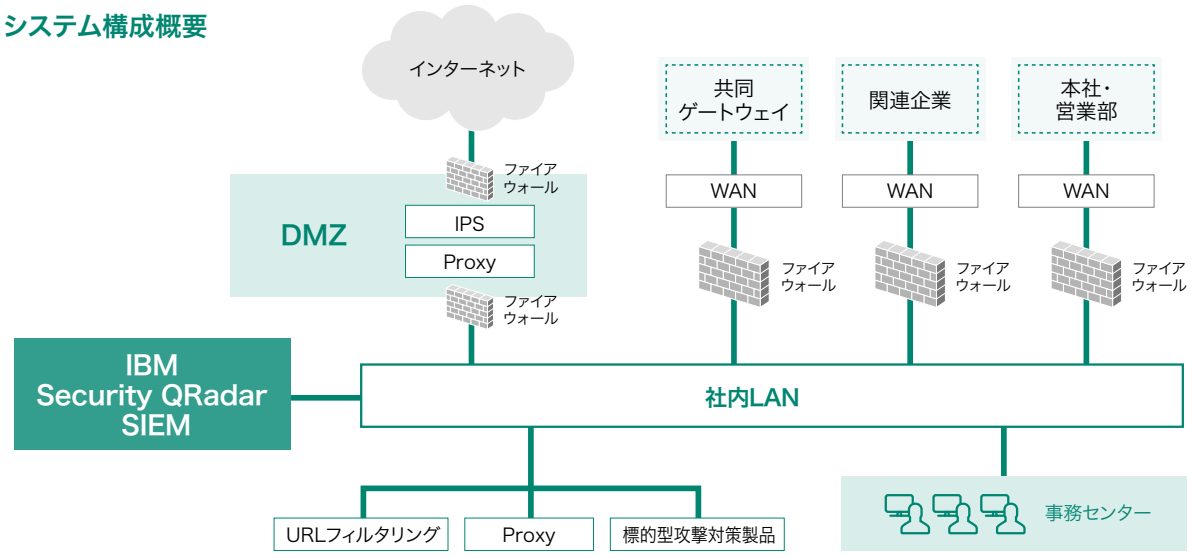
## [ 効果/将来の展望 ]

### IBM Watsonによる コグニティブ技術の導入や検知後の対応作業を自動化する プラットフォームとの連携も検討

ファイアウォールからIPS、プロキシ・サーバー、マルウェア検知まで、膨大なログが一元的にIBM Security QRadar SIEMに集められたことで、セキュリティーに関連するさまざまなKPIの監視や分析のスピードが大幅に向上しました。

「これまではSOCメンバーがある条件に沿ったログを分析したいと思ったら、システム管理者へリクエストを出しとりまとめて提供するという形をとっていました。このようなスタイル

**システム構成概要**



IBM Security QRadar SIEMは日本語化されたGUIを搭載するほか、マニュアルも充実しており、スムーズに構築作業に入ることができます。

エムエルアイ・システムズ株式会社
技術・運用本部 テクニカルグループ
主任システムズ・スペシャリスト
**平井 芳直氏**

ですと、複数のセキュリティー製品にまたがったログの収集や、複雑な検索条件（特定の時間帯に絞った検索、など）といったリクエストがあると、提供までに数時間を要することもありました。IBM Security QRadar SIEM の運用を開始した現在、SOC のメンバーは任意の検索パターンに基づいて必要なログに自ら直接アクセスすることが可能となり、脅威のより早い検知や、優先順位の高い対応を効率的に行えるようになりました」と我妻氏は話します。

この成果を踏まえ、三井生命はIBM Security QRadar SIEMによるセキュリティー監視の対象を出口対策から内部対策へと拡大しつつあります。

「IBMのアドバイスも受けながら、たとえば退職予定者や臨時雇用者による疑わしい行動をパターン化するなど新たな分析ルールの導入、定義に着手しており、2017年度内の運用開始を目指しています」と平井氏は話します。

さらに、IBM QRadar Advisor with Watsonによるコグニティブ技術の導入、不正の検知後の対応作業を自動化するプラットフォームとの連携なども検討中です。

「膨大なログをリアルタイムに分析をし、未知の脅威に対する検知精度を向上していく上で、今後はディープ・ラーニングやAIの能力が不可欠になると考えています。また、重大なリスクやセキュリティー・インシデントを検出した後、CSIRTや関連部門の責任者に迅速にアラートを出し適切な対応を求めるワークフローとの連動を自動化する仕組みにも大きな期待を寄せています」と恒本氏は話します。

ユーザー・コミュニティーにも積極的に参加し、他社との情報交換を行いながら三井生命はIBM Security QRadar SIEMのより効果的な「使いこなし」を進めていく考えです。

三井生命

**三井生命保険株式会社**

〒135-8222 東京都江東区青海1-1-20 ダイバーシティ東京オフィスタワー
http://www.mitsui-seimei.co.jp/

1927年、三井財閥傘下の生命保険会社として発足。初代社長団琢磨が創業時に掲げた「いつの時代も、お客さまのためにあれ」という経営哲学を、創業以来90年間の長きにわたり受け継ぐ。2016年4月には、日本生命相互会社と経営統合を行い、三井生命としての新たな歴史をスタート。両社ともに強みをもつ営業職員チャネルの強化のため、商品相互供給をすすめる。


〒103-8510 東京都中央区日本橋箱崎町19-21