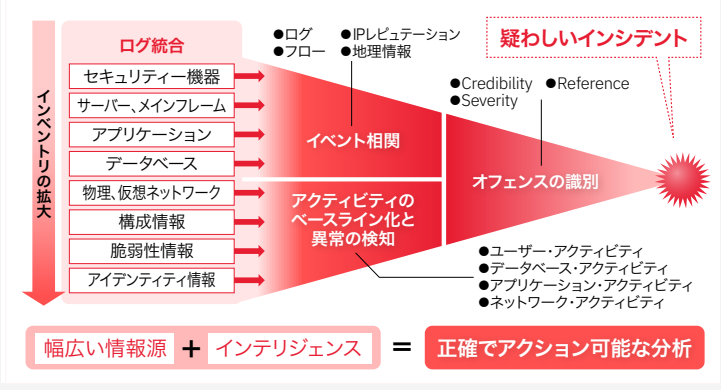
お客様事例

IBM QRadar SIEMでサイバー攻撃を見える化し、単独のセキュリティー対策製品では防御しきれない情報漏えいのリスクを最小化

日本航空株式会社（以下、JAL）は、サイバー・セキュリティー対策を経営の重要課題と位置付けており、大量の個人情報を扱う企業としての責務を果たすとともに、お客様により良いエクスペリエンス（体験価値）を提供していくための施策として、その強化を目指しています。そうした中で2015年9月にIBM QRadar SIEMを導入。以後3年以上の年月をかけて、SOC（Security Operation Center）の活動を支えるサイバー・セキュリティー基盤のコアとして運用を熟成させてきました。サイバー攻撃を「見える化」することで情報漏えいのリスクに素早く対応。さらに今後に向けて対処の「自動化」と「全体最適化」を視野に入れたグランドデザインを描いています。

［導入製品・サービス］ IBM QRadar SIEM



課題

- 事前対策の観点から、情報漏えいリスクを把握して業務横断的に脅威を監視・分析する仕組みが必要
- 事後対策の観点から、脅威を発見した際に感染が疑われる端末以外への影響分析を正確に行えることが重要
- 情報漏えいが疑われる際に、その可能性のある情報をすばやく特定するセキュリティー監視の体制が必要

ソリューション

- 導入済みのセキュリティー製品を一元管理し、正確な脅威の把握と迅速な対策を実現
- ネットワーク・フローの不審な振る舞いを見ることで、シグネチャー型に依存することなく脅威を識別
- グローバルなセキュリティー研究開発機関であるIBM X-Forceによる最新のサイバー攻撃に関する知見を提供

効果

- 3年以上にわたり自社システムから情報が漏えいするセキュリティー・インシデントは発生していない
- 蓄積されたログの解析に基づいて常に確証をもった対処が可能となった

[お客様課題]

事前対策と事後対策の
両面からセキュリティーを強化

JALグループは、「挑戦、そして成長へ」をテーマとする2017～2020年の中期経営計画を策定。航空事故ゼロおよび重大インシデント・ゼロを目指す「安全」、世界トップレベルのお客さま満足を実現する「顧客満足」、営業利益率10%以上、2020年度までにROIC（投資利益率）9%以上を目指す「財務」の3つの目標の実現を目指すJAL Visonを推進しています。

そこで欠かすことができないのがサイバー・セキュリティー対策です。JAL IT企画本部 IT運営企画部 セキュリティ戦略グループ グループ長の福島 雅哉氏は、「私たちは2014年に顧客情報システムへの不正アクセスを受け、個人情報を漏えいさせてしまうという苦いインシデントを経験しているだけに、サイバー・セキュリティー対策は経営面からも重要課題となっています。お客さまの大切な情報をお預かりする企業としての責務を果たし、さらにお客さまにより良いエクスペリエンス（体験価値）を提供していくための施策として、常にサイバー・セキュリティー対策の強化を目指しています」と話します。

具体的にはJALは、セキュリティー脅威の「特定」「防御」を中心とした事前対策と、侵入したマルウェアの「検知」「対応」「復旧」といった事後対策の両面から取り組みを強化しており、福島氏はそれぞれ次のような課題解決のポイントを示します。

まず事前対策の観点からは、単独のセキュリティー製品の機能だけでは防御しきれない情報漏えいリスクを把握することが必要です。イベント・ログの一元管理と相関分析を行い、横断的に脅威を監視・分析する仕組みが求められます。

次に事後対策の観点からは、脅威を発見した際に、感染が疑われる端末以外への影響分析を正確に行えることが重要です。また、情報漏えいが疑われる際に、その可能性のある情報をすばやく特定するセキュリティー監視の体制を確立しておかなければなりません。さらに万一インシデントが発生した場合に備えて、セキュリティー・スペシャリストによる緊急対応の支援体制も用意しておくべきとしています。

[ソリューション]

SIEMはきわめて専門性の高いセキュリティー製品
だからユーザー視点の使い勝手の良さを重視した

上記のような施策を推進する中でJALが着目したのが、SIEM（Security Information and Event Management）の活用です。そして2015年9月にIBM QRadar SIEMの導入を決定。チューニング作業を経て、2016年3月より定常運用を開始しました。

IBM QRadar SIEM導入以前は、JALは新たな脅威が出現するたびに、それに対抗する新たなソリューションを導入してきました。この結果、例えばウイルス対策では既知ウイルスに対抗する製品、未知ウイルスに対抗する製品、エンドポイントの資産管理など、さまざまなセキュリティー製品がばらばらに導入されて乱立。それらの製品を管理する組織の足並みも揃わない、いわゆる部分最適の状態にありました。

「結局、対症療法的なサイバー・セキュリティー対策を繰り返すことは抜本的な課題解決にはなりえず、むしろ混乱を招く恐れさえあります。この弊害を乗り越えるのがSIEMのアプローチなのです」と福島氏は強調します。

世界で数多くの採用実績を有するIBM QRadar SIEMは、JAL社内にすでに導入されている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。潜在しているリスクや発生しているインシデントの横断的な相関分析を行うことで、正確な脅威の把握と迅速な対策をサポートします。さらに、セキュリティー機器からのインシデント情報だけでなく、ネットワーク・フローからも不審な振る舞いを検知します。これによりシグネチャー型に依存することなく、サイバー攻撃や情報漏えいの

「IBM QRadar SIEMは、セキュリティー対策基盤のコアとなっています。JAL社内のSOCの活動はIBM QRadar SIEMなくしては成り立ちません。

日本航空株式会社
IT企画本部　IT運営企画部
セキュリティ戦略グループ
グループ長
福島 雅哉氏

リスクを識別することを大きな特長としています。

もっとも、JALがIBM QRadar SIEMに注目したのは、こうした機能面だけではありません。「本来SIEMはきわめて専門性の高いセキュリティー製品であり、これを使いこなすためには相当に高度なスキルとマンパワーが要求されます。そうした中で私たちが重視したのが、ユーザー視点で見たときの使い勝手の良さです。この点においてIBM QRadar SIEMは他社のSIEM製品を大きくリードしており、選定の決め手となりました」と福島氏は振り返ります。

また、IBMのグローバルなセキュリティー研究開発機関であるIBM X-Forceによる最新のサイバー攻撃に関する知見、脅威インテリジェンス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の提供、万一のインシデントが起こった際に“後ろ盾”として控えているIBMのセキュリティー運用経験者の存在なども、他社にない大きな付加価値として捉えられました。要するにこれらの有形無形のノウハウや安心感もすべて包括した形で提供されるのが、IBM QRadar SIEMのソリューションなのです。

「その意味でIBM QRadar SIEMは、セキュリティー対策基盤のコアとなっています。現在、JAL社内にSOC（Security Operation Center）を立ち上げ、24時間365日のセキュリティー監視・運用体制を敷いていますが、その活動はIBM QRadar SIEMなくしては成り立ちません」と福島氏。さらにJAL IT企画本部 IT運営企画部 セキュリティ戦略グループの西本友香氏は、「IBM QRadar SIEMとSOCの連携のもと、JALグループとしてのセキュリティー対策のグランドデザインが策定されています」と話します。

IBM QRadar SIEMとSOCの連携のもと、JALグループとしてのセキュリティー対策のグランドデザインが策定されています。

日本航空株式会社
IT企画本部　IT運営企画部
セキュリティ戦略グループ
西本 友香氏

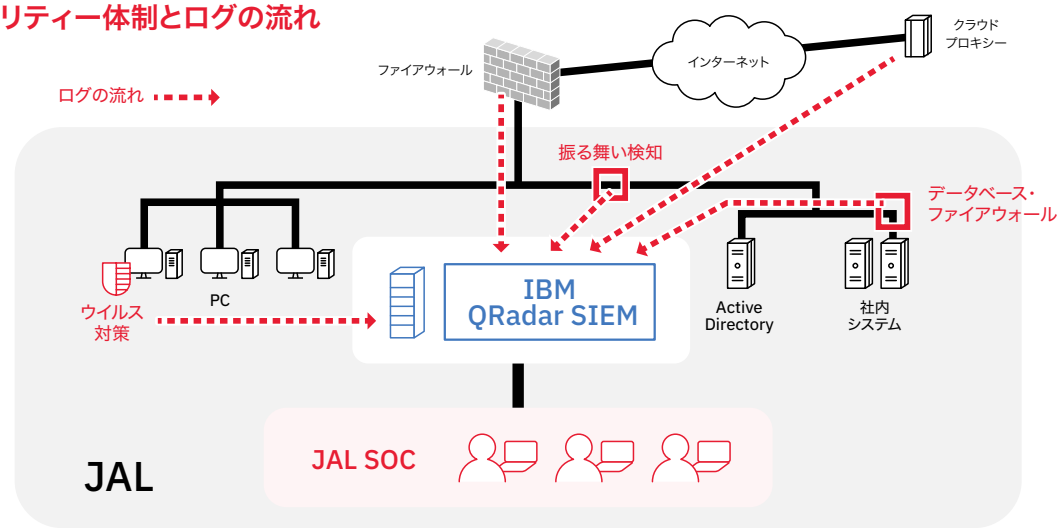
【効果/将来の展望】

「姿の見えない敵」の足跡を捕らえ「見える化」を徹底する

導入から3年以上が経過した現在、IBM QRadar SIEMはJALグループのセキュリティー監視・運用体制にすっかり定着し、さまざまなITシステムの安全性を支えています。「2014年以降、軽微な情報漏えいも一切起こしていません」と福島氏は話します。

サイバー攻撃者という「姿の見えない敵」の痕跡をしっかり捕捉し、「見える化」を徹底したことがこの効果をもたらしました。「例えばあるフィッシングサイトが問題となった際にも、社内からそのサイトにアクセスしていないかどうか、IBM QRadar SIEMに蓄積されたログ

セキュリティー体制とログの流れ



左から福島氏、西本氏

を分析することで、『問題なし』という結論を得ることができました。常に確証を持って対処できることが非常に大きいのです」と福島氏は説明します。

そしてJALは今後、この「見える化」をさらに進めた「自動化」と「全体最適化」に乗り出していく計画です。「サイバー攻撃や脆弱性のリスクを見える化できるならば、対処も自動化できるはず。その上で複数のセキュリティー製品をオーケストレーションすることで自動化の対象範囲を広げ、全体最適化された運用へとつなげていきます。ここまで達成してこそIBM QRadar SIEMの真価を発揮し、従来型のセキュリティー対策では不可能だった事前対策を強化できると考えています」と福島氏は構想を示します。

また、その手段としてAIの活用も検討しており、「IBM QRadar Advisor with WatsonやIBM Resilientも有力候補として期待しています」と西本氏は話します。

ただ、ますますターゲットを拡大し、手口を巧妙化させていく昨今のサイバー攻撃の動向を考慮すると、個々の企業によるサイバー・セキュリティー対策には早晩限界が訪れるとも予想されています。だからこそ「社会共通の課題として、皆で一致団結してサイバー攻撃の撲滅に取り組むべき」と福島氏は説きます。

企業と企業が協力しあって、情報資産を集団防御（Collective Defense）によって守る時代へと変えていく必要があり、JALはIBMと共にその一翼を担っていくという強い意欲を打ち出しています。

JAPAN AIRLINES

日本航空株式会社

〒140-8637　東京都品川区東品川2-4-11
https://www.jal.com/ja/

『世界のJAL』に向け、「SKYTRAX 5スター」の獲得、国際線中長距離LCC会社「ZIPAIR Tokyo」の設立、成田＝シアトル線、羽田＝マニラ線の開設、外国航空会社との新規提携や拡充などを推進。また、『一歩先を行く価値』を作るオープンイノベーションの拠点「JAL Innovation Lab」の開設や、スタートアップ企業に投資するコーポレートベンチャーキャピタル「Japan Airlines イノベーションファンド」設立など、『常に成長し続ける』ための取り組みを着実に進めています。