セキュリティオペレーションセンター運用の社内実践とセキュリティダッシュボード

In-house Practice of Security Operation Center: Operation and Security Dashboard

● 貞松孝美　● 米山義彦　● 矢島　介

あらまし

昨今，サイバー犯罪が国内外で急増し，その手口も一層複雑・巧妙化している。サイバー攻撃の対象は個人から企業へ移り，企業の機密情報を狙った不正アクセスなどのサイバースパイ活動が顕著になっている。このような状況の中，現状に即したサイバー攻撃を防御するセキュリティ対策の改善に加えて，早期のリスク検知および迅速なインシデント対応能力の向上がグローバルレベルで求められている。富士通グループでは，不正アクセスなどの兆候をいち早く検知し，セキュリティオペレーションセンター（SOC）で即座にインシデント対応を行っている。しかし，既存の運用モデルでは，インシデント対応業務のグローバルレベルでの標準化に加え対応の高速化が課題となっている。

本稿では，この課題を解決するために，現状の業務プロセスを分析し，運用を統一した上で自動化ツールを導入することでインシデント対応時間の短縮をグローバルレベルで実現し，社内ネットワークに存在し得るリスクを早期に排除する取組みについて述べる。更に，SOCのパフォーマンスを評価する指標として定めたKPI（Key Performance Indicator）によって運用状態を可視化するセキュリティダッシュボードを紹介する。

Abstract

Recently, cyber crimes have been rapidly increasing in Japan and overseas and their methods are becoming more complicated and sophisticated. Targets of cyber attacks are shifting from individuals to corporations, and cyber spy activities targeting confidential information of corporations have become conspicuous. The total amount of damage caused by attacks, such as unauthorized access to corporations, is increasing year by year, and the amount is said to have exceeded USD 375 billion worldwide. Under the circumstances, there is a global need to improve capabilities to promptly identify risks and quickly respond to incidents, in addition to improving security measures that can respond to the actual conditions for defending against cyber attacks. The Fujitsu Group has been implementing in-house activities to quickly detect signs of cyber attacks and other cyber threats for immediate incident response at the security operations center (SOC). With the existing operation model, however, there still remains demand for global-level standardization of incident response operations for faster responses. This paper describes an approach to meeting this challenge. It involves analyzing the actual business processes and standardizing their operations before introducing an automation tool, with which incident response time can be reduced and potential risks in the corporate network can be eliminated at an early stage. In addition, it presents a security dashboard that visualizes the operation status of the SOC by using the key performance indicators (KPIs).

ま え が き

企業の機密情報などを不正に窃取する標的型攻撃が増加している中，サイバー攻撃の手法も日々変化し，巧妙化してきている。[(1)] 企業への不正アクセスなどの攻撃がもたらす被害総額は年々増加し，2013年には全世界で3750億ドルを上回ったとされている。[(2)] 情報漏えい事故は日本企業のみならず，グローバルレベルで大規模に発生しており，標的型攻撃などのあらゆる脅威から機密情報を防御し，迅速に対応する仕組みの導入が求められている。

富士通グループでは，標的型攻撃などのセキュリティ脅威に対して，セキュリティアラートを国内の統合ログ管理システムに集約している。これにより，セキュリティアラートの発生をセキュリティオペレーションセンター（SOC）でいち早く検知し，アラートへのレスポンス，およびリスクに対する是正処置を24時間365日迅速に対応している。

SOC運用を効率化するためには，情報収集から被害状況の調査，是正対応に至る各ステップを自動化する必要がある。グローバルで統一したSOC運用を定義・設計し，対応方法を標準化することで，よりスピーディーなSOC対応スキームの導入を実現した。

本稿では，SOC業務を効率化するために自動化ツールを導入し，運用のスピードアップを達成した社内実践のアプローチと，SOC運用の状態を可視化するダッシュボードの導入について述べる。

インシデント対応のアプローチ

従来，富士通グループの社内ネットワークに接続している国内・海外のグループ会社に対して，SOCサービスを日本で集中して提供していた。そのサービス課題を以下に示す。

(1) 集中管理されたSOCから，各地域で検知したセキュリティアラート対応をコントロールする中で，時差や言語の壁によるコミュニケーション不足，および現場要員のスキル確保が課題であった。

(2) SOCサービスを効率的に運用し，各地域に統制を効かせた管理を実現するためには，プロセスの標準化を行い，現場型の統制（地域ごとにセキュリティ要員を配置）に変更する必要があった。

プロセス標準化，現場型の統制を徹底することにより，インシデント対応速度は改善したが，インシデント対応プロセスで行う情報収集，是正依頼，リスク緊急度の把握，同一事象の統合などの手順が煩雑であり，インシデント対応スピードの更なる向上や作業工数の削減についても改善の余地があった。

(3) 現場型の統制に切り替えることにより，現場での運用を可視化し，インシデント対応品質を確保する必要が出てきた。

これらの課題を解決するために，自動化ツールを導入し，作業要員の作業アシストやインシデント対応のスピードアップ，工数の削減をグローバルレベルで実現した。更に，インシデント対応状況を可視化するため，作業のパフォーマンスを評価するKPI（Key Performance Indicator）を定めることでダッシュボード化も実現した。これらを実現するために，以下のステップでアプローチした。

(1) 現状分析

国内および海外のSOC運用の現状を分析し，標準化することで自動化が可能となるプロセスを明確化する。

(2) 運用設計

明確化された作業プロセスにおいて，それぞれのインプット・アウトプットとなるデータを特定し，それぞれのプロセスをワークフローでつなぎ合わせることで，一連の自動化対象フローを作成する。これにより，インシデント対応する上で必要な重要情報をインプット情報に対して自動的に付加し，即座に対応可能となる一連のアクションが作成できる。

(3) 運用への適用

策定した各フローをオートメーション機能（FUJITSU Software Systemwalker Security Control）[(3)] に関連付け，アラート情報を基にインシデントチケット(注)を自動的に作成する。

(注) セキュリティ監視機器が発するアラート情報を基に必要な情報を付加し，SOCオペレーターが対応可能な状態にしたものであり，SOCオペレーターが対応する単位となる。

(4) KPIの設定

インシデント対応作業のKPIを作業フェーズごとに定め，チケット管理システムと連動させることでダッシュボードとして可視化する。

本自動化ツールおよびダッシュボードで用いた手法とその効果について，次章以降で詳細に述べる。

現 状 分 析

● インシデント対応数

SOC運用においては，一日に6億件強のセキュリティアラートを分析しており，1か月あたり100件強のインシデント対応を実施している。ここで言うインシデントとは，マルウェア感染や不正な外部通信，情報漏えいにつながる内部通信など，情報管理やシステム運用に関して脅威となる事案のことを指す。

特に，社内におけるマルウェア感染の脅威は増加し続けており，近年発生した情報漏えいやセキュリティ侵害のインシデントの原因として，マルウェアへの感染は高い割合を占める傾向にある。そのため，SOCでのインシデント対応はマルウェアへの感染の監視強化へとシフトしている。

● 作業内容

SOC業務におけるインシデントへの初動対応作業を分類すると，以下の4項目に分けられる。

(1) リスクレベルの判定
(2) 対応優先度の判定
(3) マルウェアなどが感染した端末の管理者特定
(4) 端末管理者への対応依頼

具体的には，初めにセキュリティアラートの確認として，ネットワークゲートウェイに設置されたセンサー機器のログを参照し，マルウェアなどの脅威兆候をチェックする。

(1) インシデント検知時刻
(2) 機器ホスト名
(3) 発生イベント名
(4) 機器IPアドレス
(5) 接続先IPアドレス
(6) アクセス先URL

これらの情報を基に，アラート対応マニュアル，アラート判定マニュアルを参照し，脅威の度合いを認識するためのリスクレベルと対応優先度を判定する。更に，インシデントが発生している端末の管理者を調査するために，ネットワークデータベース検索システムを用いて，メールアドレス，電話番号，所属，氏名などの情報を取得する。その後，管理者連絡用のメールテンプレートを用いて，OS情報，セキュリティ定義の更新日などをヒアリングし，ウイルススキャン，OSの再インストールなどの対応を依頼する流れとなる。

インシデントの放置時間とセキュリティリスクの深刻度は比例しており，インシデントを長時間放置することで不正な外部通信による情報漏えいの継続や，被害拡大の危険性がある。そのため，初動対応をいかに正確に早く行うかが重要になる。

作業の効率を判断するために，インシデント1件あたりにかかる初動対応作業の平均時間を計測した結果，作業全体で約30分であった。初動対応全体の流れを俯瞰すると，対応手順などの各種判定，Webシステムでの検索，テンプレート選択など，そのほとんどが人手で行われていることが分かった。主に時間を要しているのがマニュアルの参照で，これは個々のSOCオペレーターがセンサー機器から得たインシデント情報を基に必要な情報を検索し，慎重に読解した上で，順次作業を行っているためである。

運 用 設 計

SOCオペレーターによる初動対応時間の分析結果から，対応速度の効率を高める必要があることが分かった。このため，システムによる作業の自動化を目指し，以下に示す作業プロセスの標準化をはじめとした運用体制の設計を行った。

● プロセスの明確化

作業プロセスの標準化として，SOCの実際の作業に基づいて，最小限かつ必須と考えられる作業を抽出した。作業の前後関係を把握するため，各作業を実施するのに必要な入力情報，および各作業が完了した際に得られる出力情報も同時に洗い出すことで，インシデント対応に必要なプロセスを明確化した。そのプロセスは次のとおりである。

(1) 対応手順の判定

発生イベント名（アラート名）に基づき，必要な対応手順を判定

（2）リスクレベルの判定
　あらかじめ設定した定義に基づき，リスクレベルを判定
（3）対応優先度
　リスクレベルと外部通信の回数から対応の優先度を判定
（4）メールテンプレートの選択
　端末管理者への連絡用メールテンプレートを選択
（5）High Value Target（HVT）の判定
　サーバや幹部社員所有の機器など，攻撃対象として影響度合いの大きい機器（HVT）か判定
（6）繰返し事象の判定
　外部通信の回数を監視し，作業チケットに情報を反映。情報の漏えい，感染拡大の兆候を対応者に通知

HVTの判定と繰返し事象の判定は，従来の対応作業に加えて新たに追加した項目である。これらの項目は，昨今のマルウェア脅威の判定結果を加味し，作業の自動化において正確な判断と対応を行うために必要であると分かったため採用された。

● 導入システムの選定

対応プロセスの自動化，およびインシデントの管理を目的としたことから，これらの管理機能を保有しているミドルウェアSystemwalker Security Controlを選定した。選定理由として，作業プロセスを標準化する流れにおいて，作業をワークフローとして構築することで，将来プロセスを変更しても柔軟に対応できることがメリットとして挙げられる。インシデントのチケット管理システムについても，グローバル全体でインシデント情報を一元化することで，全体状況の把握や対応者の割当ての最適化が図れると判断した。ミドルウェアの導入に当たっては，開発元にSOC運用のノウハウを提供することで，対応プロセスの自動化，およびインシデント管理に必要な機能の早急な実現が可能となった。

● システムを中心とした体制への変更

作業プロセスをワークフロー化するに当たり，インシデント対応者とSOCオペレーターの作業役割を再定義した。

各役割の詳細を以下に示す。

（1）ローカルオペレーター
　インシデント発生元を特定し，迅速なリスク対応を行う各拠点選任のオペレーター
（2）インシデントマネージャー
　インシデント対応の支援，および全体マネジメントを行う管理者
（3）システムオペレーター
　セキュリティ監視基盤を運用し，迅速に障害復旧対応を行うシステム運用管理者

上記のように，各インシデント対応者の役割を明確に分離することで，導入したシステムが提供するワークフローの自動化，およびチケット管理システムに最適な運用体制を整備した。

● インシデントチケットの自動生成

グローバルに配備されたセキュリティ監視機器で検知されたセキュリティアラートは，国内に構築している統合ログ管理システムで一元的に集約される。

統合ログ管理システムで脅威の相関分析が行われ，インシデント対応が必要とされるセキュリティアラートが抽出される。抽出されたセキュリティアラートに対し，前述の「プロセスの明確化」で述べた一連の作業プロセスがSystemwalker Security Controlのワークフローにより自動的に判断され，セキュリティアラートに対して情報が付加される。

情報が付加されたセキュリティアラートは，Systemwalker Security Controlのチケット管理システムに送信され，インシデントチケットとして登録される。登録されたインシデントチケットには，マルウェアに感染した端末のIPアドレス情報や，端末の管理者情報などが付加されており，IPアドレス情報から対象の拠点を任されているローカルオペレーターにチケットが送信される仕組みとなっている（**図-1**）。

● 各SOCオペレーターの作業の流れ

ローカルオペレーターはインシデントチケットを受信後，チケット管理システムにログインし，チケットに記載された感染情報を確認する。その後，対応を開始した旨をチケット管理システムに登録し，チケットに添付された連絡用メールテンプレートを用いて端末の管理者に確認・対応を依頼する。

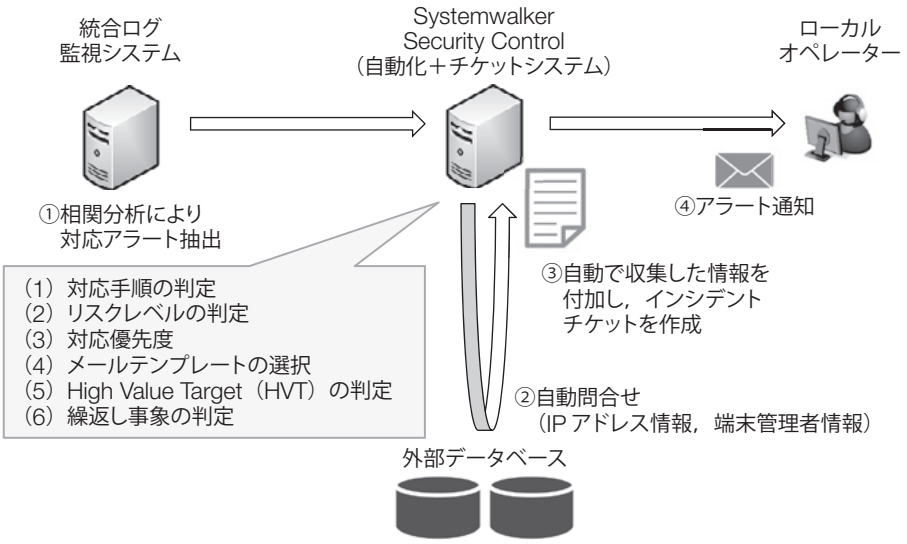

図-1　インシデントチケットの自動生成

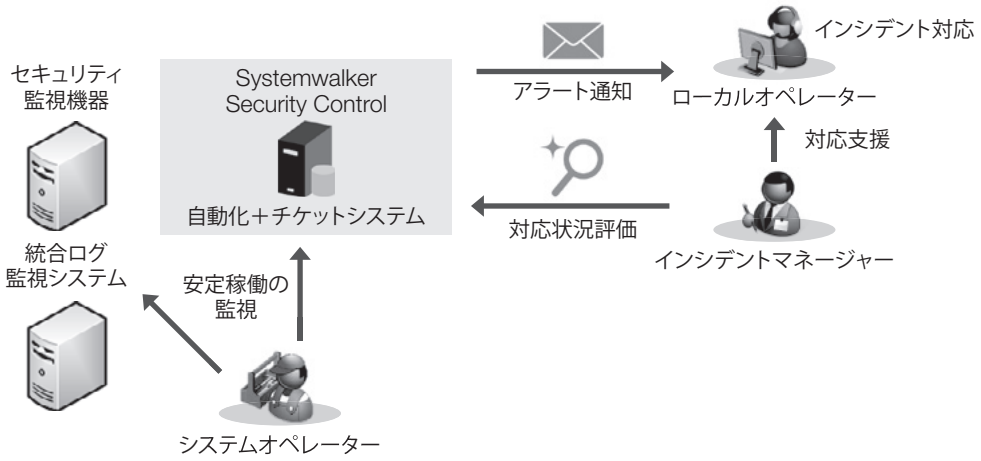

図-2　SOCオペレーターの関係

インシデントマネージャーは自身の担当エリアのチケットを参照し，ローカルオペレーターのインシデント対応状況を管理する。ローカルオペレーターが対応方法に困り，遅延している場合には対応支援を実施する。対応が完了したらチケット管理システムにログインし，対応に問題ないことを確認の上，チケットをクローズする。

システムオペレーターは，グローバルに配備したセキュリティ監視機器，統合ログ管理システム，およびチケット管理システムの安定稼働を監視し，SOCの安定運用を確保する（**図-2**）。

自動化機能の拡張

前章で述べたローカルオペレーター，インシデントマネージャーに加え，セキュリティイベントの相関関係を分析し，攻撃シナリオやロジックを特定した後に解析作業を行う分析官（セキュリティアナリスト）の業務についても自動化対象とした。セキュリティアナリストの主な役割は，以下の三つである。

（1）セキュリティログの分析・調査
（2）セキュリティ脅威や脆弱性などの情報収集
（3）セキュリティ監視機器の設定変更指示や経営層に向けた新規施策の提案

この中で「セキュリティログの分析・調査」業務の自動化を実現した。攻撃シナリオを特定するためには，各種セキュリティ監視機器により検知されるセキュリティアラートを調査・分析する必要がある。相関分析で攻撃シナリオを特定できた場合，これを検知するルールを策定し，セキュリティアラートの調査対象を拡大することで，セキュリティリスクが社内ネットワーク内に存在するか確認している。

攻撃シナリオを手動で抽出した場合，即時性が重要なセキュリティアラートの発見が遅れ，セキュリティリスクがより長時間社内ネットワークに存在することになる。攻撃シナリオを自動化ツール上でルール（ワークフロー）として策定し，そのルールに適合するイベントを大量のログから自動的に検索して相関分析を行うことで，瞬時に複数リスクの特定が可能となる。

本自動化ツールにより自動的に検出されたセキュリティアラートについては，SOCオペレーターがインシデント対応を即座に行うことになる。

SOC稼働状況の可視化

インシデント対応の品質を確保するため，SOCのパフォーマンスを評価する指標としてKPIを定め，SOC稼働状況を可視化することとした。指標として以下の項目を設定した。

（1）初動時間

インシデント発生から初動対応までにかかった時間

（2）クローズ時間

インシデント発生から対応完了までの時間

（3）解決率

インシデントマネージャーへエスカレーションせずにローカルオペレーターで解決できた割合

（4）エラー率

人為的ミスが発生した割合

上記KPI値を自動で算出・表示する仕組みとして，セキュリティダッシュボードシステムを導入した。本システムは，チケット管理システムから各インシデントの対応状況を自動的に収集し，KPI値を算出した上でダッシュボード画面に表示する。また，各インシデントの対応ステータス，リスクレベルについても，ダッシュボードで可視化した。

本システムにより，SOCオペレーターの状況が可視化され，対応速度の低下や対応品質の低下，インシデント増大による対応遅延，リスクの高いインシデントの対応遅延などをリアルタイムで把握でき，状況に応じた適切な対処が可能となった（**図-3**）。

自動化に伴う効果

インシデント対応，ログ分析・調査などの各種SOC業務を標準化した上でプロセスを自動化することにより，SOC業務全般において以下に示す工数削減を実現した。

（1）ローカルオペレーターの工数削減

インシデントの初動対応時間を，従来の手順に比べ97％削減（30分→1分へ短縮）

（2）セキュリティアナリストの工数削減

自動化ツールの導入により，グローバルレベルでセキュリティアナリスト機能の集約が可能となり，コストを50％削減

また，工数削減以外に以下の定性的な観点からも効果を生み出した。

（1）標準化によるリスク判定精度の向上

インシデント対応プロセスを標準化したことにより，リスク判定プロセスについても自動化され，より精度の高いリスク評価が可能となった。これにより，緊急性を考慮した迅速なインシデント対応を実現した。

（2）リスクの可視化

従来は，発見した攻撃シナリオを基に手動でアラート検索・調査・特定まで行っていた。これを自動化することにより，より多くの時間を異なる攻撃シナリオの調査・分析に費やすことができる。

図-3　セキュリティダッシュボード画面

これにより，様々な種類の攻撃を検知するルールの策定にも注力することが可能となり，不正なネットワーク通信などの新たな脅威の発見にも寄与できる。

むすび

運用自動化ソフトウェアを用いた業務の自動化は近年のトレンドであり，様々なジャンルでの実例が取り上げられているが，運用をシステムに預けることに不安を持つ企業は多い。セキュリティ分野のSOC運用にこの手法を適用した例は少なく，大きな挑戦であった。部門間の連携を通じて，多くの実績に基づいたノウハウを収集したことが現在のSOCを実現できた理由であると考える。

マルウェアの脅威は常に進化・増大しており，それに合わせてセキュリティ対策も常に進化を求められている。システムと運用の柔軟な体制を土台として，増え続ける脅威に対抗できる施策を今後も追加し，富士通はセキュアなネットワーク環境の維持に挑戦し続けていく。

参考文献

(1) 総務省：平成25年版情報通信白書.
http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h25/pdf/index.html
(2) Center for Strategic and International Studies：Net Losses：Estimating the Global Cost of Cybercrime. June 2014.
http://www.mcafee.com/hk/resources/reports/rp-economic-impact-cybercrime2.pdf
(3) 富士通：FUJITSU Software Systemwalker Security Control.
http://systemwalker.fujitsu.com/jp/securitycontrol/

著者紹介

貞松孝美（さだまつ　たかよし）
セキュリティマネジメントサービス事業本部マネージドセキュリティ事業部 所属
現在，ビジネス化に向けたマネージドセキュリティサービスの企画・検証に従事。

米山義彦（よねやま　よしひこ）
総務・リスクマネジメント本部セキュリティマネジメント統括部 所属
現在，社内ネットワークのセキュリティマネジメントに従事。

矢島　介（やじま　かい）
総務・リスクマネジメント本部セキュリティマネジメント統括部 所属
現在，社内ネットワークのセキュリティマネジメントに従事。