特集論文

ServiceNowを活用したSOC運用基盤の強化

小坂哲也*
Tetsuya Kosaka
黛　潤一*
Junichi Mayuzumi

Advanced Security Operation Center Platform Based on ServiceNow

要　旨

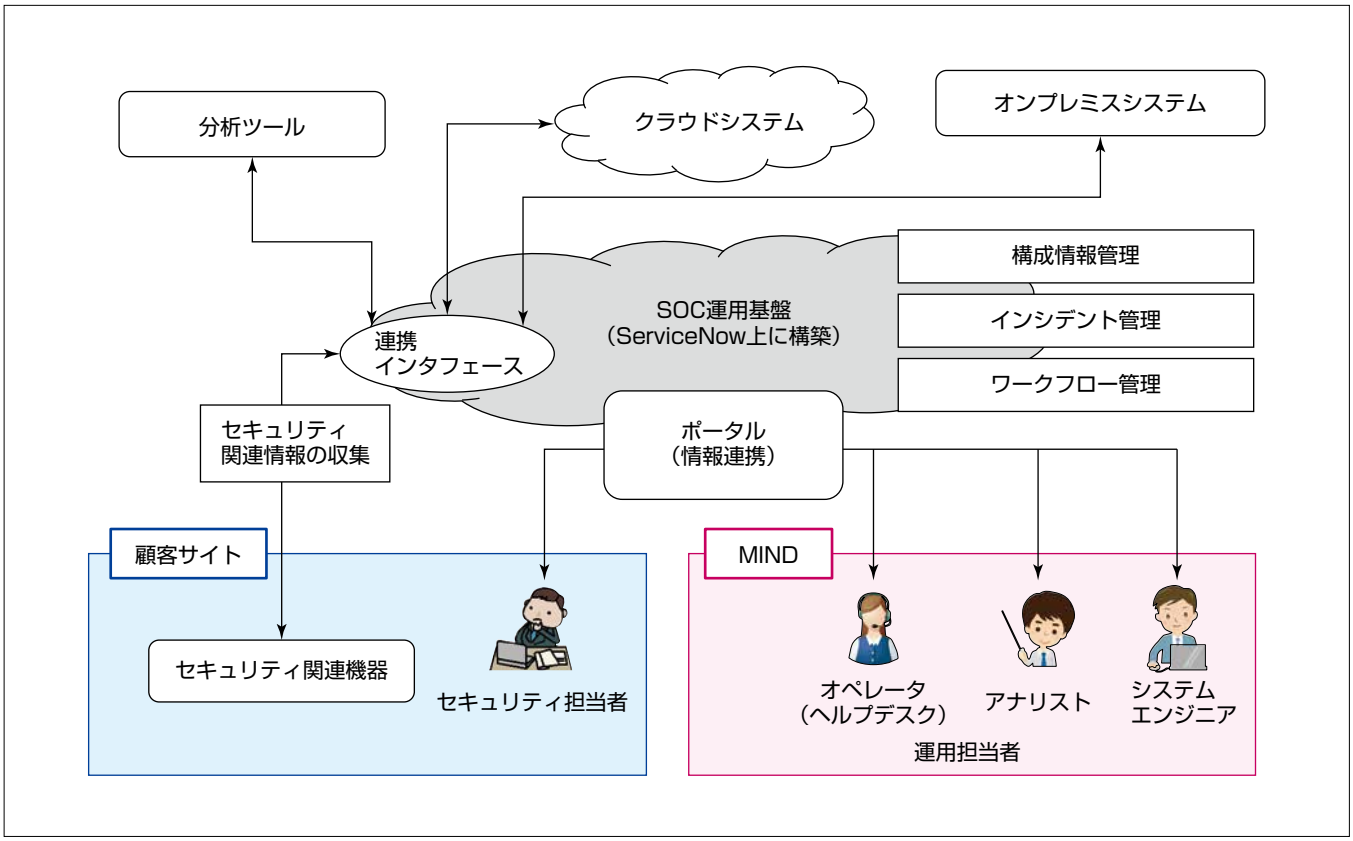
近年，標的型攻撃による機密情報の窃取，サービス妨害攻撃によるサービスの停止など，情報セキュリティ上の新たな脅威による被害が増大している(1)。これらの脅威に対応するため，セキュリティベンダーから最先端の様々なセキュリティ対策技術や製品が発表されている。

三菱電機インフォメーションネットワーク㈱(MIND)では，顧客に最適なセキュリティ環境の構築，24時間365日の運用監視，セキュリティ診断など，ネットワークセキュリティの導入検討，設計，構築から運用まで一貫したサービスを提供している。新たな脅威に対抗する技術をサービスに組み込むためには，既存の運用システムとの整合性や顧客に対する適切な情報提供が課題になる。

MINDでは，これらの課題を解決するSOC(Security Operation Center)運用基盤を開発した。SOC運用基盤は，開発プラットフォームとしてクラウド／オンプレミス上のシステムとの連携インタフェースや，ITSM(IT Service Management)ベースの管理・運用機能を持つServiceNow(注1)を採用し，セキュリティ運用サービスに必要な次の機能を提供する。

(1)　ポータル／メールによる顧客・運用担当者間の情報連携
(2)　セキュリティ関連機器からの情報収集と管理
(3)　分析ツールとの連携
(4)　クラウド／オンプレミス上の関連システムとの連携
(5)　運用業務の自動化を支援するワークフロー管理

（注１）　ServiceNowは，ServiceNow,Inc.の登録商標である。



SOC運用基盤を活用したセキュリティ運用サービスの構成

SOC運用基盤は，セキュリティ運用サービスに必要な構成情報，インデント，ワークフローを一元管理するとともに，セキュリティ関連機器が脅威を検知した際の，外部システムとの連携と顧客のセキュリティ担当者やMINDの運用担当者の対応業務を効率的に実行するためのフレームワークを提供する。

1. ま え が き

政府の働き方改革でのICT(Information and Communication Technology)の活用推進[2]や，工場，社会インフラなどでのIoT(Internet of Things)市場の成長(2019～2023年の年平均成長率32.8%)[3]など，情報システムの利活用は急速に拡大している。これに伴い，情報セキュリティ上の脅威が社会に及ぼす影響も拡大しており，セキュリティ運用サービスへの要求が高まっている。

これらの脅威に対応するため，セキュリティベンダーからは最先端の技術を駆使した製品が日々発表されているが，セキュリティ運用サービスに新たなセキュリティ製品を組み込むためには，既存の運用システムが持っている管理データとの整合性の維持や，オペレータ，アナリストなどの運用担当者側の業務フロー(情報連携)の最適化，及び，顧客に対する適切な情報提供などが課題になる。

MINDでは，これらの課題に対応するため，他システムとの連携インタフェースや，ITSMベースの管理・運用機能を持つServiceNowを開発プラットフォームにしてSOC運用基盤を開発した。

本稿ではSOC運用基盤を活用したセキュリティ運用サービスの事例と，セキュリティ運用の標準化への取組み，及び今後のセキュリティビジネスへの展開について述べる。

2. SOC運用基盤を活用した運用サービスの事例

2.1 ファイアウォール構築・運用支援サービスへの適用

MINDでは，顧客のセキュリティ要件に合わせた最適なファイアウォール(FW)の設置・構築，及び24時間365日の運用監視を提供するFW構築・運用支援サービスを提供している。

FW構築・運用支援サービスでは，通信のフィルタリングなどの基本サービスに加え，セキュリティ上の脅威を検知／防御するIDS/IPS(Intrusion Detection System/Intrusion Prevention System)の監視・運用サービスを提供しているが，従来のIDS/IPS監視・運用サービスでは，FWが検知した脅威を顧客にメール通知する運用にとどまっていた。SOC運用基盤をこのサービスに適用することによって，顧客のセキュリティ担当者(以下“顧客”という。)の脅威情報へのアクセスや，顧客とMINDの運用担当者(以下“運用担当者”という。)間の情報連携が容易になる。

2.2 提供サービスの概要

FW構築・運用支援サービスでのIDS/IPS監視・運用システムの構成を**図1**に示す。顧客サイトに設置されたFW上のIDS/IPSがセキュリティ上の脅威を検知した場合，FWは脅威情報を検知メールとしてSOC運用基盤に送付する。SOC運用基盤は送付された検知メールを解析し，インシデントとして保存する。

IDS/IPS監視・運用システムによって提供中の主なサービスを次に述べる。

2.2.1 脅威検知時の顧客へのメール連絡サービス

SOC運用基盤は，FWが検知した脅威情報を顧客に通知メールで連絡する。通知メールには，検知したFWのホスト名や検知時間，検知した脅威の種別(ThreatID)と，SOC運用基盤上のインシデント管理に格納されている詳細情報にアクセスするためのURL(Uniform Resource Locator)が記載されている。顧客はURLをクリックすることによって，検知した脅威の詳細をポータル上で確認する。

また，フラッド攻撃のような同じ攻撃を連続して検知した場合，SOC運用基盤は，最初の攻撃を検知したタイミングで顧客に対し，通知メールで初報を行う。その後，同じ攻撃が継続した場合，検知ごとに通知メールを送らずに，一定時間後に同一攻撃の検知数を1通の通知メールに集約して送付する(**図2**)。これによってフラッド攻撃時に顧客へ大量の通知メールが送付されることを抑制する。

2.2.2 セキュリティアラーム調査サービス

顧客は検知された脅威に対して調査が必要と判断した場合，ポータル上から調査を依頼する。SOC運用基盤は，

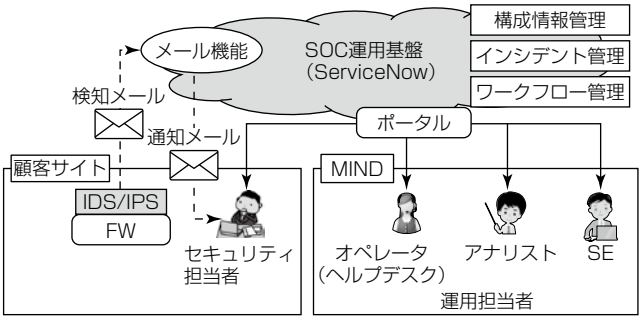


図1．IDS/IPS監視・運用システムの構成

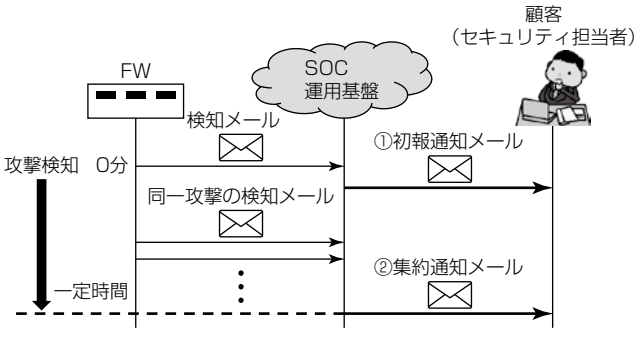


図2．フラッド攻撃検知時の通知メールの集約

調査依頼に基づき自動的に調査内容を含む依頼タスクを生成するとともに，依頼の概要を担当のアナリストに通知メールによって連絡する。アナリストは通知メールに記載されているURLをクリックすることによって，ポータル上で依頼タスクを開き，依頼内容の確認・対応を行う。

調査依頼の状態(処理中，ユーザー問合せ中，クローズ等)や顧客とアナリスト間のやり取り，調査結果などは依頼タスク上で管理される。

また，脅威の調査は，年度ごとのサービス契約によってMINDから顧客に対して発行される“調査依頼チケット”を消費する。SOC運用基盤は，顧客の調査依頼チケットの残数を管理し，依頼時にチケットが不足する場合，ポータル上でチケットの追加を可能にする。

2.2.3　問合せサービス(ヘルプデスク)

顧客はFW構築・運用支援サービスに関する問合せをポータル上から行う。

SOC運用基盤は依頼タスクを生成するとともに，問い合わせ種別ごとに適切なオペレータに通知メールを送付する。オペレータは通知メールに記載されるURLをクリックすることによって，ポータル上で依頼タスクを開き，問合せ対応を行う。また，質問への回答が困難な場合，オペレータはポータル上からSEに対し，依頼タスクのエスカレーションを実施する。

問合せの状態(処理中，ユーザー問合せ中，クローズ等)やエスカレーション履歴，回答などは全て依頼タスク上で管理される。

2.2.4　各種履歴の閲覧サービス

顧客は，過去6か月に検知した脅威，セキュリティ調査依頼や問合せの履歴をポータル上で検索・参照する。

3. セキュリティ運用の標準化への取組み

3.1　標準化によるメリット

MINDでは，SOC運用基盤を活用した運用の標準化に取り組んでいる。運用を標準化するメリットを次に述べる。

3.1.1　顧客の利便性向上

MINDは，設計から構築，運用まで一貫したセキュリティサービスを提供しており，顧客からの問合せ対応や情報提供などの運用はサービスごとに異なる形態で行われている。

これらのサービスの運用をSOC運用基盤で標準化することによって，顧客はMINDが提供するすべてのサービスをSOC運用基盤上の共通インタフェースを介して利用できる(**図3**)。必要な情報へのアクセス方法や問合せ・依頼方法及び，情報の管理方式を標準化することによって，顧客の利便性を高める。

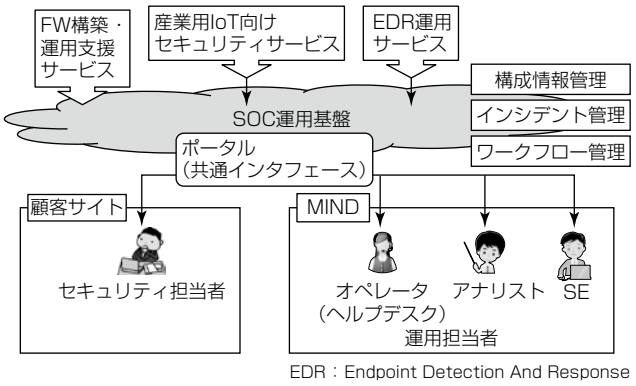


図3．セキュリティ運用の標準化

3.1.2　運用の効率化

3.1.1項で述べたサービスごとに運用形態が異なる点は，MINDの運用上の課題となっている。例えば，顧客からの問合せを受け付けるオペレータは，サービスごと／受付内容ごとに異なる作業マニュアルを参照しながら受付業務を行っており，オペレータの作業負荷の低減が課題になっている。

既存サービスで使用している構成情報やインシデント情報，ワークフローなどをServiceNowが提供するITSMベースの管理・運用環境に統合することによって，オペレータはすべてのサービスの受付作業を標準化された作業手順で行うことができる。また，SOC運用基盤のワークフロー管理機能の活用によって，受付後の対応業務の自動化・効率化が可能になる。

3.2　ポータルと通知メールのデザインガイドライン

セキュリティ運用の標準化への取組みの中から，顧客が利用するポータルと，SOC運用基盤から顧客や運用担当者に向けて送付される通知メールのデザインガイドラインについて述べる。

3.2.1　顧客向けポータルのデザインガイドライン

MINDの運用サービスが顧客に対して統一感のある情報提供を行うために，顧客向けポータルのデザインガイドラインを規定している。一例として共通トップページのデザインガイドラインについて述べる。

MINDの運用サービスは，ログイン後表示される共通トップページ“MINDサービスポータルへようこそ”を起点とする(**図4**)。

共通トップページには，(a)MINDのロゴ，(b)ログインアイコン，(c)MINDサービスポータルからのお知らせ，(d)顧客が契約中のサービスからのお知らせ，(e)顧客が契

約中の個別サービスへのリンク一覧，(f)MINDのオフィシャルサービス紹介サイトへのリンクを配置する。顧客は(e)のリンクをクリックすることによって，利用サービス(FW構築・運用支援サービス等)のトップページに遷移する。

3.2.2 通知メールのデザインガイドライン

SOC運用基盤が顧客や運用担当者に送付する通知メールの可読性を高めるために，通知メールのデザインガイドラインを規定した。

FWがセキュリティ上の脅威を検知した際に顧客に送付する通知メール(**図5**)を例に“顧客向け通知メール”のデザインガイドラインを示す。

メール件名の形式(a)は，“【MIND＋サービス名】＋通知種別”とし，メール本文の先頭にこのメールが送信専用メールである注意書き(b)を配置する。宛名の下には，“下記機器にて，アラームを検知いたしました”などの通知内容(c)と，検知した脅威の種類や発生時刻など，顧客や運用担当者がポータルにアクセスしなくても認識する必要がある情報を概要(d)に記載する。最後に，この依頼タスクの管理番号(e)と，ポータル上に依頼タスクを表示するためのリンク(f)を配置する。

このように，SOC運用基盤から送付される通知メールのフォーマットを統一し，可読性の向上を図っている。

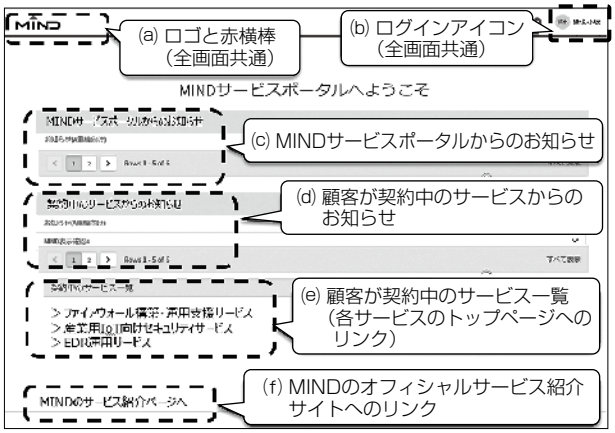


図4．MIND運用サービスの共通トップページ

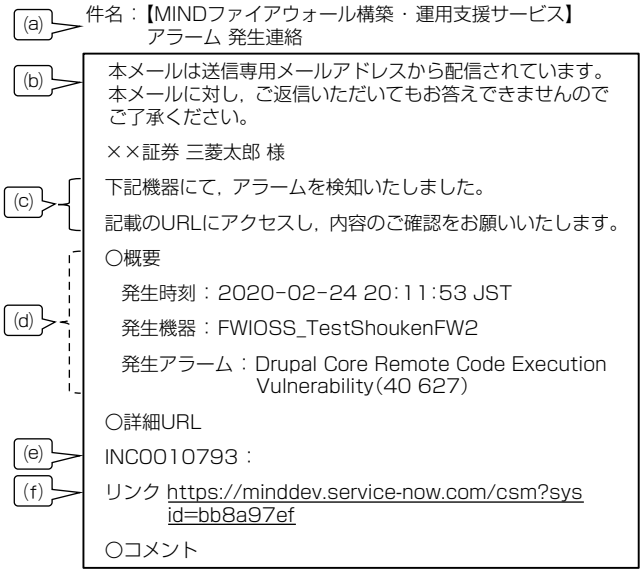


図5．顧客向け通知メールの例

4．SOC運用基盤を活用したビジネス展開

今後の展開として，EDR運用サービスや産業用IoT向けセキュリティサービスへの適用を検討している。EDR運用サービスでは，ユーザーが利用するパソコンやサーバの不審な挙動を監視し，攻撃検知時に端末の隔離などを行うことによって被害の拡大を抑制する。EDRとSOC運用基盤の連携によって，アナリストの迅速な対応・対策支援が可能になる。産業用IoT向けセキュリティサービスでは，MINDがこれまで蓄積した企業向けサービスの脅威ナレッジと異なるIoTに対する脅威ナレッジが必要であるため，IoTに関する脅威情報を提供するクラウドサービスとのAPI(Application Programming Interface)連携等，ServiceNowの連携インタフェース開発を進め，運用基盤の強化を図っていく。

また，AI(Artificial Intelligence)を活用した新たな監視技術やRPA(Robotic Process Automation)などの運用効率化技術を積極的にSOC運用基盤に取り込み，MINDのセキュリティサービスの高付加価値化を目指す。

5．む　す　び

情報システムの社会的な利活用が進むに伴い，サイバー攻撃による被害も拡大している。このような背景から，国内のセキュリティサービス／製品市場は，年平均成長率5.7%(2018～2023年)と旺盛(おうせい)な需要が見込まれる一方，セキュリティ人材不足や高度化する脅威への対処が課題になっている(4)。

MINDでは，ServiceNowを活用したSOC運用基盤の強化によって，新たな監視技術の柔軟な導入と運用効率の向上を図るとともに，顧客に対する適切な情報提供環境の整備を進めていく。

参考文献

(1) 情報処理推進機構：情報セキュリティ10大脅威2020
https://www.ipa.go.jp/files/000080871.pdf
(2) 高市早苗：平成29年版情報通信白書の公表にあたって，総務省(2017)
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h29/pdf/29daijin.pdf
(3) MM総研：IoT技術の国内利用動向調査(2019年11月実施)
https://www.m2ri.jp/news/detail.html?id=387
(4) 富士キメラ総研：2019ネットワークセキュリティビジネス調査総覧(市場編)(2019)