セキュリティLCMサービス

八巻 剛　柴田 旭　大越 義彦　児玉 純

要 旨

日々変化するサイバーセキュリティの脅威に対し、お客様はシステムを導入するだけでなく、サイバー攻撃を未然に防ぐための日々の運用やセキュリティインシデントの対応を求められ、多くの企業は自社では十分対応できていない状況です。これらに対し、NECでは、お客様のサイバーセキュリティ対策の持続的な向上を目的に、コンサルティングから、構築・運用まで一貫して提供する「セキュリティLCMサービス」を開始しています。本稿では、「セキュリティLCMサービス」の特徴と導入後の効果などを紹介します。

KeyWords　セキュリティLCM／インシデントレスポンス／CSIRT／SIEM／サイバー攻撃／コンサルティング／アセスメント／フォレンジック

1. はじめに

近年、サイバーセキュリティに対するニーズは高まり続けています。2015年に日本年金機構から個人情報が漏えいして以降、サイバー攻撃や不正アクセスに対する関心は高まりましたが、その対策は進まず、さまざまな企業や組織がサイバー攻撃を受け、多くの被害が報告されました。2015年12月には経済産業省が、独立行政法人情報処理推進機構（IPA）とともに「サイバーセキュリティ経営ガイドライン」を策定し、サイバーセキュリティは経営課題と明確に位置付け、経営者にサイバーセキュリティ対策を推進するよう要請しました。これらを受けて、企業はサイバーセキュリティ対策を進めていますが、対策が不十分であったり、対策が効果的に機能しなかったりと多くの課題が見えてきています。急速に高まるサイバー攻撃という脅威に対して、企業が抱える課題を明らかにして、その課題に対するNECの取り組みを紹介します。

2. 企業が抱える課題

さまざまなお客様に対してサイバーセキュリティ対策を支援していくなかで、多くのお客様が共通の課題を抱えていることが見えてきました。その課題は、要約すると下記2点になります。

(1) セキュリティに対する専門的な知識がない

セキュリティ対策は、セキュリティ事故が起きないようにする事前対策と、セキュリティ事故が起きた後どう対処するかの事後対策と、大きく2つに分類されます。事前対策は、出入口対策やエンドポイント対策といったシステム観点の対策から従業員教育など非常に多岐にわたります。それらを網羅的かつ効果的に施策として実施していくためには、幅広い知識が必要になります。事後対策は、PCや紙の紛失といった対応が比較的確立されているものから、標的型のサイバー攻撃といった対応が多くの企業で確立されていないものまであり、特に後者に対応するためには、非常に高度な専門知識が必要になります。

(2) セキュリティに対応できる人材が少ない（いない）

組織の中にセキュリティに対応できる人材が少なく、その限られた人に業務が集中し、セキュリティ対策が進まない事態に多くの企業が陥っています。人材を増やそうにも、育成するには多くの時間とコストがかかるため実現できていないのが実態です。

これらの課題に対して、自社でできることと、外部の専

門家に委託することをうまく線引きし、対応していくことが最も現実的かつ効果的です。

3.「セキュリティLCM」の企画・開発

顧客が抱える課題に対しての解決の一助として、NECが1990年代後半より培ってきたセキュリティ技術・対策の知見を外販サービス向けに体系化した「セキュリティLCM」を2016年より提供しています。

LCMとはライフサイクルマネジメントを意味しており、「セキュリティLCM」はセキュリティ環境の現状把握・施策検討から運用までの一貫した支援だけでなく、時間の経過とともに変化する脅威に合わせて、再度現状把握・施策検討から見直しをするセキュリティのライフサイクルマネジメントを意味します。NECは、このセキュリティライフサイクルマネジメントを適切に循環させるためのサービスを提供しています。特に、コンサルティングやシステム構築・運用はNECの持つ総合力を生かせる領域です。

NECは、1990年代よりセキュリティシステムの開発・構築、マルウェアの解析といった領域に注力しており、2000年以降はCSIRT（Computer Security Incident Response Team）体制の構築・運用、「Nimda」や「Code Red」の解析・インシデント対応を経て、多くの知見を蓄積しています。それらの開発や知見を通して、高度なセキュリティ技術者を数多く育成及び保持する環境を有しております。

近年では、民間企業においても、情報窃取を目的とする高度な標的型攻撃やランサムウェアなどの金銭窃取を目的とするサイバー犯罪攻撃の激化が、顕著になっています。このような喫緊の課題に対して、出入口対策やエンドポイント対策といったツールのみで解決できない問題に対処すべく、顧客の要員育成や戦略の立案、アセスメント実施、インシデントレスポンス支援といった多角的なサポートが求められています。

そのようなニーズに対して、NECの擁する高度な技術者集団と蓄積したナレッジをベースにした「セキュリティLCM」で包括的なサポートを実現します。

4.「セキュリティLCM」の全体像と特徴

「セキュリティLCM」の全体像は以下のとおりで、「Ⅰ.現状把握・施策検討」「Ⅱ.構築」「Ⅲ.運用」といったフェーズごとに、支援サービスを提供しています（**図1**）。

「Ⅰ.現状把握・施策検討」フェーズ向けには、今のセキュリティ対策で十分か多角的に診断・評価するサービスや、診断・評価結果とあるべき姿のギャップを埋めるための セキュリティ強化計画を策定するサービスなどがあります。

「Ⅱ.構築」フェーズ向けには、セキュリティシステムを構築する支援や、その構築したセキュリティシステムを効率的に運用するための運用設計支援サービスなどがあります。

「Ⅲ.運用」フェーズ向けには、日々のCSIRT運用の支援として、インシデントを検知するサービスやインシデント

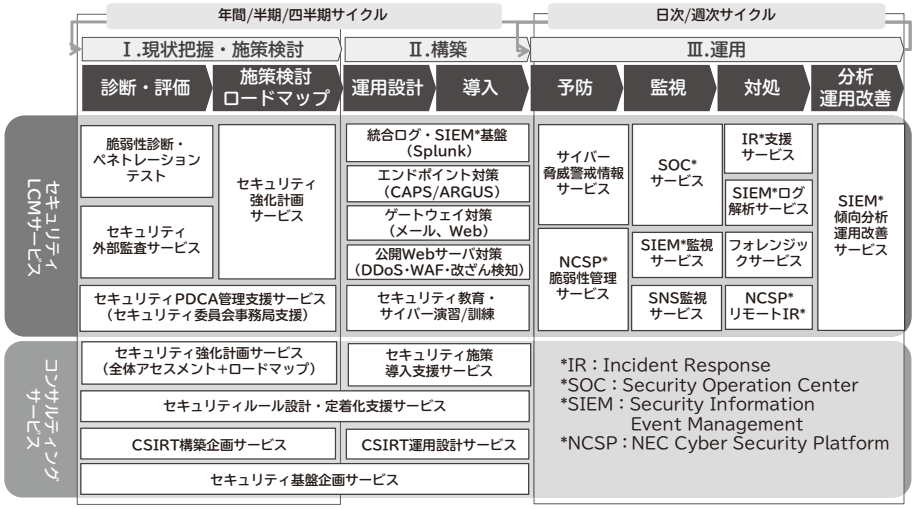


図1 「セキュリティLCM」の全体像

発生時に専門家によるアドバイスや調査といった支援が受けられるサービスなどがあります。

また「セキュリティLCM」の特徴は、以下の2点になります。

(1)NECの知見を生かしたサービス提供

NECは防衛事業をしていることもあり、日々多くのサイバー攻撃を受けるため、さまざまな多層の対策がされています。また、10万人を超えるNECグループ全体のセキュリティを維持するために、システム化・自動化を推進し、効率的な運用を長年にわたり実施してきました。本サービスには、これらのNECの知見が随時取り込まれています。

例えば、全PCのセキュリティパッチの適用状況を即座に可視化できたり、膨大なログからサイバー攻撃の兆候や攻撃を受けたPCを特定できたりする仕組みが構築されています。これらをテンプレート化し、随時サービスに取り込んでいます。

(2)お客様のニーズに合わせた柔軟な支援

抱えている課題や対応すべき脅威の優先度は、お客様ごとに異なりますので、お客様の状況やニーズに応じて、必要なサービスだけを組み合わせて提供することもできますし、セキュリティライフサイクルを全体的かつ持続的に支援することもできます。

例えば、インシデント発生時の初動や解析に課題を感じているお客様には、“IR支援サービス”にて専門家によるアドバイスや調査を即座に提供できますし、セキュリティ全体を一から見直したいお客様には、「Ⅰ.現状把握・施策検討」「Ⅱ.構築」「Ⅲ.運用」のすべてのフェーズを一貫かつ持続的に支援することができます。

5. “IR支援サービス”の内容と特徴

「セキュリティLCM」のなかで、特に多くのお客様が課題としているセキュリティインシデントの緊急対応を専門家が支援するサービスである“IR支援サービス”について紹介します。

セキュリティインシデント対応は、迅速な初動対応と専門的知識に基づく適切な対処が求められます。「セキュリティLCMサービス」では、インシデント発生時に情報提供ポータルを介して相談を受け付け、リモートでセキュリティエンジニアによる初動対応のアドバイスなどの対応を行います。インシデントハンドリングやマルウェア解析などの経験のあるセキュリティエンジニアをあらかじめプールしておき、シェアード型で提供することで、緊急のセキュリティインシデントに対して、迅速かつリーズナブルに支援することができます。

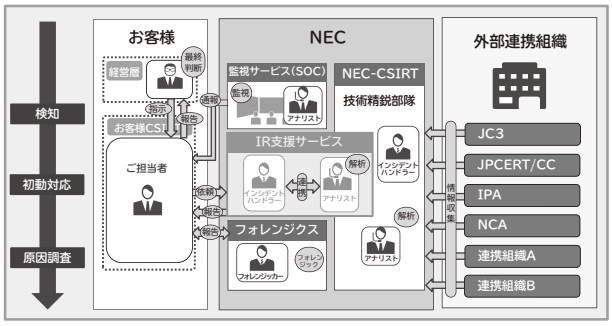


図2　IR支援サービス

例えば、マルウェア感染が疑われる事象が発生した場合、マルウェアの挙動を把握するためのマルウェア解析を単に実施するだけでなく、解析結果を元に他に感染が疑われる端末がないかといった被害の特定や、不正な通信が発生している場合には通信を止めるための手法など、インシデントへの対処方法まで踏み込んでアドバイスを行います。これらの対応はお客様企業自身で対応することが困難な場合も多く、複数の企業を受け持ちシェアード型で提供する本サービスだからこそ、経験に基づいた迅速な対応が可能となります。

6.「セキュリティLCM」の今後の展望

サイバーセキュリティは日々進歩しており、今この瞬間にも新たな技術が生まれると同時に、新たな脅威も増大しています。また、サイバーセキュリティは技術だけでなく、ガバナンスなどのマネジメントも求められます。このような広範囲かつ進歩の早い分野において、NECが今までに培ってきた技術・知見、更に現在も、研究・開発を行っている新技術を融合することで高い価値を創造していきます。

執筆者プロフィール

八巻 剛
プラットフォーム・エンジニアリング本部
シニアマネージャー

柴田 旭
プラットフォーム・エンジニアリング本部
主任

大越 義彦
プラットフォーム・エンジニアリング本部

児玉 純
プラットフォーム・エンジニアリング本部

NEC 技報のご案内

NEC 技報の論文をご覧いただきありがとうございます。
ご興味がありましたら、関連する他の論文もご一読ください。

NEC技報WEBサイトはこちら

NEC技報（日本語）　NEC Technical Journal（英語）

Vol.70 No.2　ビジネスの安全・安心を支えるサイバーセキュリティ特集
～Futureproof Security　安心の先へ。～

ビジネスの安全・安心を支えるサイバーセキュリティ特集によせて
増大するサイバー犯罪の根源的な解決へ～“産学官”のオールジャパンで立ち向かう第三者機関の姿とは？～
サイバーセキュリティを取り巻く社会動向とNECの取り組み

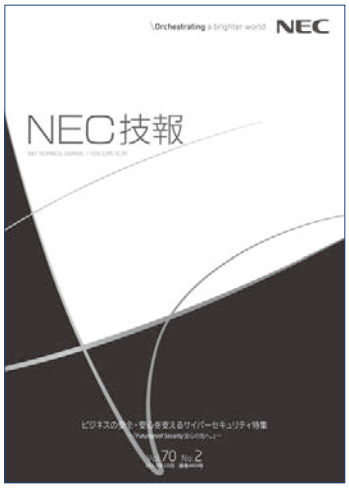
◇ 特集論文

社会の動向とNECの取り組み
重要インフラに対するサイバー攻撃の実態と分析
2017 サイバー攻撃最新動向 NEC Cyber Threat Intelligence活用モデル
サイバーセキュリティ対策の社内事例

サイバーセキュリティソリューション
複雑化 / 高度化するサイバー脅威に対抗するSOCとセキュリティ監視サービス
攻撃被害を極小化するためのインシデント対応支援ソリューション
サイバー演習によるインシデントハンドリング能力の強化
セキュリティ統合管理・対処ソリューション「NEC Cyber Security Platform」
クラウド型ファイル暗号化サービス －ActSecureクラウドセキュアファイルサービス－
セキュリティLCMサービス
EMMを活用したセキュアなモバイルワークソリューション
IoT 時代の経営を支援するサイバーセキュリティコンサルティング

サイバーセキュリティへのAI技術の活用
AI（人工知能）を活用した未知のサイバー攻撃対策
採るべき対策の「なぜ？」に答えるAIの可能性
オープンソースインテリジェンスを活用したサイバー脅威の検出と自動分析
犯罪捜査支援のためのサイバー・フィジカル統合分析技術

お客様に安全・安心を届けるための社内の取り組み
安全・安心な製品・サービスをご提供するための取り組み ～セキュア開発・運用～
サイバーセキュリティ人材のタレントマネジメント



Vol.70 No.2
（2017年10月）

特集TOP