深刻化するサイバー攻撃対策を「確実な実践」に導くセキュリティアセスメント

栗林 利充　田中 洋　駒込 大祐　楠田 徹

要 旨

セキュリティ対策の強化は、企業・団体における深刻な経営課題となっています。一方で、攻撃の巧妙化、ITの活用シーンの広がり、対策の複雑化などから、「今どれだけのセキュリティ対策を行うべきか」の判断は非常に難しくなっています。本稿で紹介するセキュリティアセスメントは、ポリシーと対策レベル、通信実態、運用体制の3つの観点から、現状の可視化を行い、その結果をもとに、セキュリティ対策の投資計画の策定まで行います。企業・団体において、「いつどれだけの経営資源（ヒト・モノ・カネ）をセキュリティ対策に費やすべきか」の経営判断ができる材料を提供します。

KeyWords　セキュリティコンサル／セキュリティ診断／サイバー攻撃対策／内部犯行対策／セキュリティ強化計画策定

1. はじめに

サイバー攻撃や内部犯行などによる情報漏えい事件は拡大の一途をたどっており、多くのお客様企業・団体にとって、事業継続にかかわる深刻な経営課題となっています。攻撃手法は巧妙化・悪質化が進み、それに比例して、対策も多様化・複雑化しています。また、クラウド利用、スマートデバイス、社内SNSなどITの活用シーンの広がりは、皮肉にも対策すべきポイントの増大につながっています。

結果、多くのお客様企業・団体において「自社は今どれだけのセキュリティ対策を行うべきか」を判断することが、非常に難しくなっています。

本稿では、これらの悩みに応え、サイバー攻撃・内部犯行などの脅威から情報資産を守る最適解を導くためのツールである、セキュリティアセスメントについて紹介します。

2. セキュリティアセスメントの概要

セキュリティアセスメントは、お客様企業・団体におけるセキュリティ対策状況を可視化（診断）し、その結果をもとに、今後の対策の整備・実行計画を策定するコンサルティングサービスです。アセスメントの視点を図1に示します。ポリシーと対策レベル、通信実態、運用体制の3つの観点から、現状の可視化を行い、その結果をもとに、セキュリティ対策の投資計画の策定まで行います。企業・団体において、「いつどれだけの経営資源（ヒト・モノ・カネ）をセキュリティ対策に費やすべきか」の経営判断ができる材料を提供します。

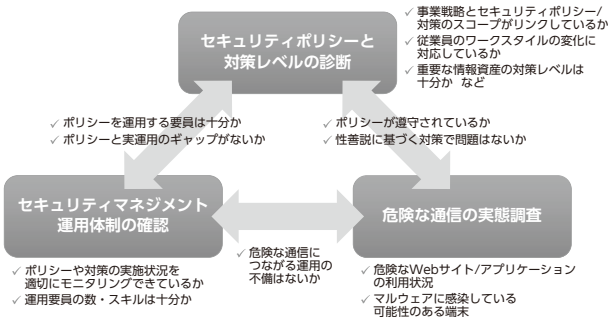


図1　セキュリティアセスメントの視点

3. セキュリティアセスメントのポイント

セキュリティアセスメントの開発において留意したのは、「短期間で、脅威の実態を正しく認識してもらい、確実な整備・運用を実現できるようにする」ことでした。前述の3つ

の視点ごとに、本アセスメントのポイントを、一般的な簡易アセスメントとの違いも含めて示します。

3.1 ポリシー・対策レベルのアセスメント

セキュリティポリシー評価とヒアリングを通じ、セキュリティ対策の不足がないかを確認します。一般的な簡易アセスメントの多くは、ベースラインアプローチという手法に基づき、対策の実践状況を、企業内全体を対象に、「広く浅く」診断します。その場合、対策の対象範囲が絞りきれず、対策の意思決定がしにくくなりがちです。

本アセスメントでは、ベースラインアプローチに、部分的な詳細リスク分析を加えた手法をとります。両アプローチの違いと、本アセスメントによるアプローチイメージを表1、図2に示します。企業内全体のIT（図2-②）を対象としたアセスメントに加え、重要な情報資産にかかわるIT環境（図2-①）をターゲットに深堀したアセスメントを実施することで、セキュリティ対策投資の重点ターゲットを設定できるようにします。

3.2 通信実態のアセスメント

次世代ファイアウォールをミラーポートに接続し、不正通信の有無を確認します。社内ネットワークに対する不審な振る舞いをする通信がないか、許可されていないフリーメールや社外ファイル共有サービスの利用など、セキュリティポリシーに違反する行為が発生していないか、などを確認します。これらの脅威は、実被害が表面化するまで認識されないケースが多く、ヒアリングベースのアセスメントでは正しい回答を得にくいものです。本アセスメントでは、次世代ファイアウォールから検出したログをもとに、脅威発生状況の事実をお客様に認識してもらえるようにします。

3.3 組織・体制のアセスメント

セキュリティ対策整備後に、それら対策を実際に運用できるかどうかを、セキュリティ対策における現状の役割分担や人的リソースの十分性などから評価します。対策の運用についてIT部門（IT子会社を含む）内の対応組織が決まらない、あるいは、スキルある特定要員がすべての管理・運用を担わざるを得ず運用が回らない、などのケースがこれまでも見受けられました。抽出した施策を円滑に運用できる体制づくりについて、NECとのコラボレーションも視野に入れた検討を行います。

4. セキュリティアセスメントの進め方

セキュリティアセスメントの進め方を図3に示します。

標準的な期間は2カ月と設定しています。週次ペースのワークセッション7回、ワークセッション1回当たりの時間は約2時間～2時間半を想定しています。

最初の工程である、「基本情報把握」にて、現在のIT環境の確認や、重要な情報資産と関連するIT環境について確認します。

その後の「脆弱性調査」では、アセスメントシートをもとにしたヒアリングによりポリシー・対策状況の確認を行います。アセスメントシートの構成を表2に示します。8分野42個のメイン項目と、256個のサブ項目で構成されます。

表1　リスク分析の代表的手法

リスク分析手法	手法概要
ベースラインアプローチ（簡易リスク分析）	一般に公開されている基準やガイドラインを用いて簡易にリスク分析を行う手法。 情報資産、脅威、脆弱性の洗い出しなどは行わない。
詳細リスク分析	情報資産、脅威、脆弱性の洗い出しと評価を行い、そこからリスクの大きさを評価する。 ベースラインアプローチに比べ時間と手間が掛かる。

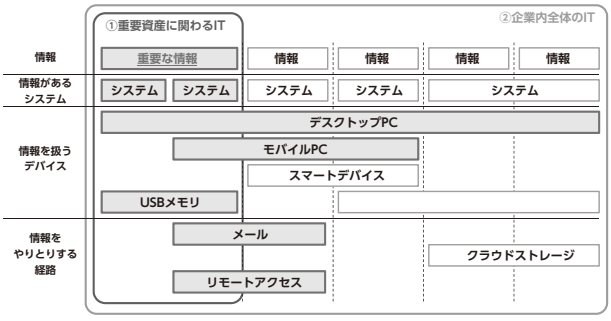


図2　本アセスメントのアプローチイメージ

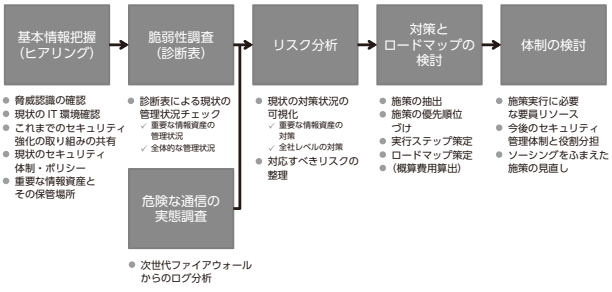


図3　セキュリティアセスメントの進め方

並行して、「危険な通信の実態調査」として、次世代ファイアウォールによる通信実態のアセスメントを行います。

これらの結果をもとに、「リスク分析」を行います。分析では、項目別結果分析や、情報処理推進機構（IPA）のベンチマークデータやこれまでのアセスメント対象企業などのデータをもとにした他社比較なども行いながら、対策が不足している領域を明確化します。

分析結果をもとに「対策とロードマップの検討」を行います。対策については、NEC側で準備するTOBEモデルをもとに、現状のIT環境をふまえたディスカッションを行いつつ、検討を行います。サイバー攻撃のTOBEモデルを図4に示します。

技術的対策だけでなく、ユーザー教育などのマネジメント対策も含めて抽出します。

これらの対策の実行ロードマップを策定します。ここでは、リスク分析で設定した対策の優先度、施策の技術的な関連性、IT中期計画などをふまえ、今後3年を目安としたロードマップを策定します。対策ごとの概算費用についても、SEメンバーと連携して、前提条件とともに算出・設定します。

表2　アセスメントシートの構成

分野	内容
Ⅰ. マネジメント体制	セキュリティ方針、体制、外部委託先との契約
Ⅱ. 人的・物理的対策	オフィス対策、サーバルーム対策
Ⅲ. 情報管理	PC・スマートデバイス・USBメモリなどの外部記憶媒体の管理、メール・インターネット利用ルール
Ⅳ. アクセス管理	ユーザーのID・パスワード管理、システム管理者のアクセス管理
Ⅴ. 不正侵入対策	ウイルス対策、脆弱性対策
Ⅵ. システム・ネットワーク構成・運用管理	サーバ・システム・ネットワークの変更・運用ルール、障害対応、バックアップ、ネットワークセグメンテーション
Ⅶ. システム・ネットワーク監視	サーバ・システム・ネットワークの監視、ログ管理
Ⅷ. インシデントレスポンス	セキュリティ事件・事故発生時の対応プロセス・体制

最後に、これら施策を行ううえでの、「体制の検討」を行い、アセスメントの標準工程は完了です。

5. セキュリティアセスメント実践事例

5.1 住宅製造業A社

A社では、内部犯行による情報漏えい事故が社会問題化するなか、これまでの性善説に則ったセキュリティ対策からの転換の必要性を、会社レベルで認識する必要があると判断。そして、セキュリティ投資計画の上申を行うために、本アセスメントを活用しました。

約2カ月の実施期間を経て上申は無事完了し、認証基盤環境強化などを含む先行施策の実行に取り組んでいます。

5.2 鉄道業B社

B社ではグループ経営強化に向け、グループ会社のリスク耐性強化が必要と判断。グループ会社のセキュリティ遵守意識の醸成と、セキュリティにかかわるIT環境の見える化に向けて本アセスメントを活用しました。実施期間は約半年にわたり、本社IT部門とグループ会社経営層とのセキュリティ強化計画の整合、及びIT子会社によるセキュリティのシェアドサービス化に向けた具体検討が進んでいます。

5.3 化学素材系製造業C社

C社では、グループレベルでのセキュリティ強化をIT戦略として掲げるも、IT子会社のセキュリティ要員不足が深刻化していました。そこで、社外とのコラボレーションを含めた体制検討を行うために、本アセスメントを活用しました。約

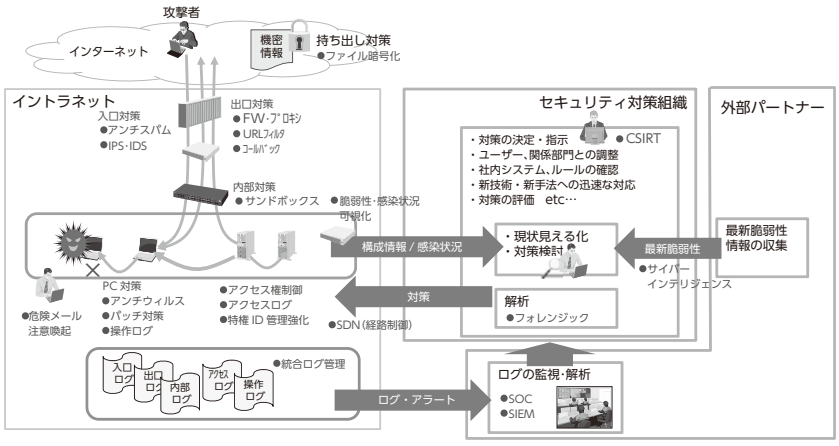


図4　サイバー攻撃対策のTOBEモデル

1カ月の実施期間で、本社IT部門とIT子会社との役割分担見直し及び、NECとのコラボレーションを含むIT子会社のセキュリティ管理体制を検討しました。

6. むすび

以上、セキュリティアセスメントの概要・ポイント・事例について紹介しました。セキュリティは、NECの社会ソリューションを形成する重点戦略テーマであり、本アセスメントは商談拡大に向けたドアオープナーツールです。今後もお客様課題の変化に追随し、技法のブラッシュアップを行っていきます。

執筆者プロフィール

栗林 利充
コンサルティング事業部
シニアエキスパート

田中 洋
株式会社インフォセック
セキュリティコンサルティングユニット
ユニットマネージャー

駒込 大祐
コンサルティング事業部
主任

楠田 徹
グローバルプロダクト・サービス本部
主任

関連URL

NEC コンサルティングサービス
http://www.nec.co.jp/service/consult

NEC 技報のご案内

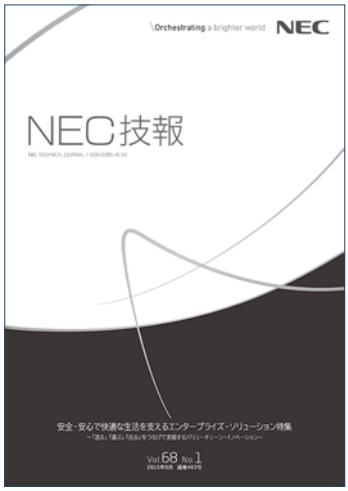
NEC技報の論文をご覧いただきありがとうございます。
ご興味がありましたら、関連する他の論文もご一読ください。

NEC技報WEBサイトはこちら

NEC技報(日本語)　　NEC Technical Journal(英語)

Vol.68 No.1　安全・安心で快適な生活を支えるエンタープライズ・ソリューション特集
～「造る」「運ぶ」「売る」をつなげて実現するバリューチェーン・イノベーション～

安全・安心で快適な生活を支えるエンタープライズ・ソリューション特集によせて
NECが考えるバリューチェーン・イノベーション
～バリューチェーン・イノベーションが実現する安全・安心で快適な生活～



Vol.68 No.1
(2015年9月)

特集TOP

◇ 特集論文

バリューチェーン・イノベーション「造る」
製造業を元気に！ NECものづくり共創プログラム
IoTを活用した次世代ものづくり ～NEC Industrial IoT～
インダストリー4.0と自動車業界におけるものづくり改革の最新動向

バリューチェーン・イノベーション「運ぶ」
アジア新興国における物流可視化クラウドサービス

バリューチェーン・イノベーション「売る」
小売業の方向性とICTの貢献 ～Consumer-Centric Retailingの追求～
サービスの高度化を支える電子決済
オムニチャネル時代のポイントとECソリューション「NeoSarf/DM」
「おもてなし」をグローバルに展開するNEC Smart Hospitality Solutions

豊かな生活/豊かな暮らし
公共交通ICカードソリューションの取り組みと今後の展望
スマートモビリティへの取り組み
EV充電事業の商用化を支えるEV充電インフラシステム
IoTを活用した端末・サービス基盤と業際ビジネス実現に向けた取り組み

エンタープライズ領域を支える先進のICT/SIへの取り組み
新たな価値を創出するビッグデータ活用
補修用部品の在庫最適化に貢献する需要予測ソリューション
異種混合学習技術を活用した日配品需要予測ソリューション
プラント故障予兆検知サービスのグローバル展開
食品メーカーの商品需要予測へのビッグデータ技術活用
事業貢献を実現するマルチクラウド活用法と移行技術
SDNを活用したグループ統合ネットワーク ～東洋製罐グループホールディングス株式会社様～
企業を狙う標的型攻撃の動向とサイバーセキュリティ対策ソリューション
深刻化するサイバー攻撃対策を「確実な実践」に導くセキュリティアセスメント
今後のIoT時代を見据えた制御システムのセキュリティ
画像識別・認識技術を活用したVCAソリューションへの取り組み
短納期・低コストを実現する現場SEから生まれたWeb開発フレームワーク
IoT時代に新たな社会価値創造を実現する組込みシステムソリューション
NECにおけるSAPプロジェクトの先進的な取り組み