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

吉府 研治　伊東 真理　山田 知秀

要 旨

IoT時代を迎え、サイバー攻撃が企業経営にとってますます大きなリスクの1つになり、経営者が主体的にサプライチェーンも含めたサイバー攻撃対策にかかわっていくことが必要不可欠となってきています。経済産業省発行のサイバーセキュリティ経営ガイドラインをベースにアセスメントしたお客様のセキュリティ対策状況を踏まえ、お客様の経営やものづくりのセキュリティ対策（ITシステム、製品開発、制御システム）を支援するコンサルティングサービスを紹介します。

KeyWords
セキュリティコンサルティング／サイバーセキュリティ／セキュア開発・運用／CSIRT／PSIRT／セキュリティ教育／リスクアセスメント

1. はじめに

近年、サイバー攻撃による被害は年々増加しており、情報セキュリティ事件・事故は組織のビジネスを停止させる可能性を含むことから、経営に直結する問題となっています。この状況を鑑み、経済産業省及びIPA（情報処理推進機構）は「サイバーセキュリティ経営ガイドライン」[1) 2)]を発行しました。NECではこのガイドラインを踏まえた、サイバーセキュリティコンサルティングサービスを提供しており、本稿ではその概要を紹介します。

2.「サイバーセキュリティ経営ガイドライン」

2014年11月、サイバーセキュリティ基本法が成立し、各関係者（国、地方公共団体、重要インフラ事業者、サイバー関連事業者、教育研究機関など）の責務が規定され、政府はサイバーセキュリティに関する基本的な計画（サイバーセキュリティ戦略）を定めることになりました。この計画では、対象者別の基準・ガイドラインの活用促進も記載しており、民間企業の経営者向けに経済産業省及びIPAが「サイバーセキュリティ経営ガイドライン」を策定しました（2015年12月初版）。このガイドラインでは、経営者が認識すべきサイバーセキュリティに関する3原則、トップダウンで取り組むべき重要10項目を明記しています（**図1**）。

3. サイバーセキュリティ課題とNECでの取り組み

NECは、「サイバーセキュリティ経営ガイドライン」への対応に関するアンケートを、約200社の企業を対象に行いました。各社の回答からは、年商、業種を問わず、経営者によるリーダーシップ表明/体制構築に課題を持つ企業が多数あると言えます。また、系列企業やサプライチェーンを含めたセキュリティ対策、事故発生時の対応体制、人材育成などが項目別の課題の上位を占めています（**図2**）。

NECグループでは、CISO（最高情報セキュリティ責任者）のもと、関係部門が連携して「社内」「協力会社」「お客様向けSI・サービス及び社製品」の情報セキュリティを推進し、「サイバーセキュリティ経営ガイドライン」の重要10項目に対応しています。上述の課題に対しては、外部委託時のセキュリティ確保やセキュア開発・運用指示、事故に対応するNEC-CSIRT体制整備、認定制度や育成制度を通じた高度なセキュリティ人材の育成を行っています。サイバーセキュリティコンサルティングサービスには、このようなNECグループにおけるサイバーセキュリティ活動で

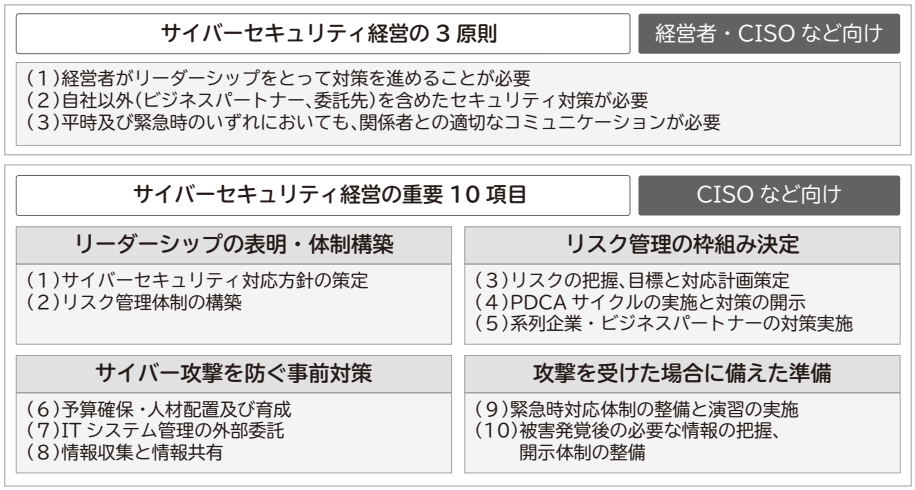


図1　「サイバーセキュリティ経営ガイドライン」の概要

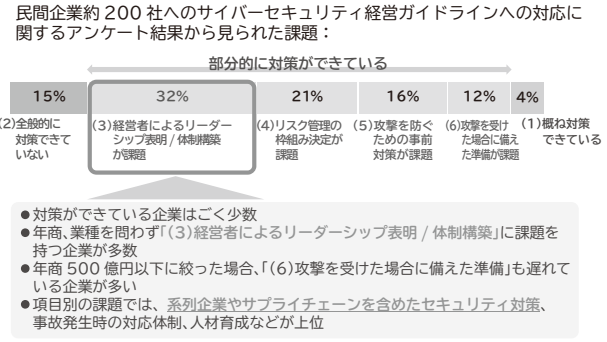


図2　企業へのアンケート結果から見た課題

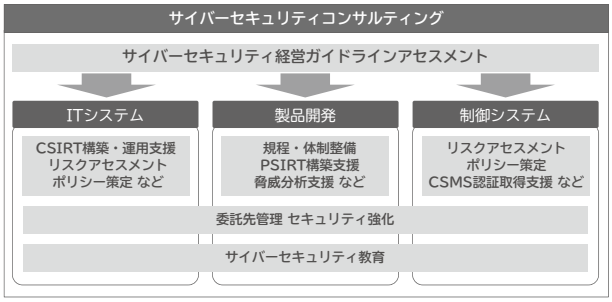


図3　サイバーセキュリティコンサルティングサービス

得られた知見を取り入れています。

4. サイバーセキュリティコンサルティングサービス

サイバーセキュリティが経営問題として位置付けられるなか、NECではサイバーセキュリティ経営の観点から企業のセキュリティ対策を支援するコンサルティングサービスを提供しています（**図3**）。

このサービスは、情報システム部門を中心としたITシステム領域だけでなく、企業が提供する製品にかかわる製品開発領域、そして制御システムや工場を対象とした制御システム領域の3つの領域をカバーするセキュリティコンサルティングを提供しています。また、組織全体におけるセキュリティ課題を見える化するために、「サイバーセキュリティ経営ガイドラインアセスメントサービス」を提供しています。

アセスメントサービスでは、「サイバーセキュリティ経営ガイドライン」の重要10項目に基づいてリスクを分析・評価し、リスクの影響度に応じた対策を提案します。リスク分析・評価には、NEC自身の「サイバーセキュリティ経営ガイドライン」への対応実績を基にした独自のチェックリストを活用します。これにより見つかった課題への対策として、技術的なソリューションや、領域別の支援サービスがあります。以降では代表的な領域別支援サービスについて記述します。

4.1 ITシステム向けサービス

(1) CSIRT構築・運用支援サービス

NECは2002年に社内CSIRTを立ち上げ、十数年にわたる運用実績があります。また、多くのお客様にITシステムや運用サービスを提供してきました。これらの技術力やノウハウを元に、お客様が中心となって

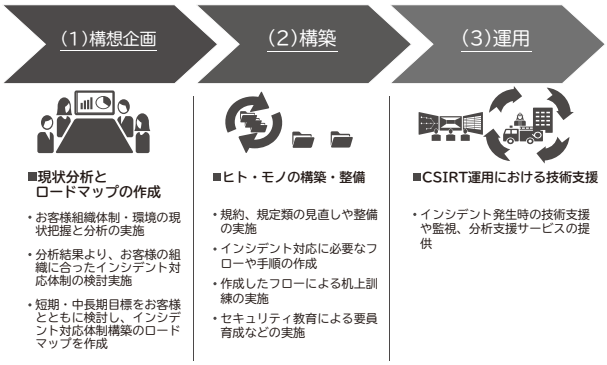


図4　CSIRT構築・運用支援サービス

運用する組織内CSIRTの構築・運用を支援するサービスを提供しています（**図4**）。

4.2 製品開発向けサービス

(1)セキュア開発規程・体制整備支援サービス

セキュア開発・運用の効率的な推進には、基本方針や部門横断の規程づくり、これらの方針や規程を含む各種施策を検討・展開・改善する体制の構築が重要です。体制構築には、関連部門（社内IT部門、品質推進・管理部門、調達部門）との関係の整理、施策を討議し決定するワーキンググループや、事業部門における推進者の設置が欠かせません。本サービスでは、NECにおける推進ノウハウをベースに、お客様のセキュア開発・運用の規程・ガイドラインの策定、体制構築を支援します（**図5**）。

(2)PSIRT・脆弱性管理プロセス構築支援サービス

製品・システムの脆弱性に起因する事故の未然防止、発生する影響の最小化には、公開済み/未公開の脆弱性情報の収集・対処に加え、第三者や関係者により発見された自社製品の脆弱性に適切・迅速に対処する必要があります。本サービスではNECのPSIRT（Product Security Incident Response Team：自社製品・システムの脆弱性対応窓口）の構築・運用ノウハウを元に、PSIRT構築、自社製品・システムの脆弱性の管理プロセス構築を支援します（**図6**）。

(3)製品・システム脅威分析支援サービス

機器やシステムのIoT化が進むなか、セキュリティの脅威が増大しています。ネットワーク接続機能を備える機器が導入される環境全体に対するシナリオベースの脅威分析を行い、対策を検討・決定するケースが増えており、NECでは脅威分析の実施支援・教育サービスを提供しています（**図7**）。

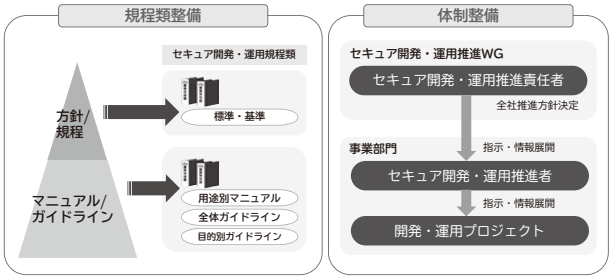


図5　セキュア開発規程・体制整備支援サービス

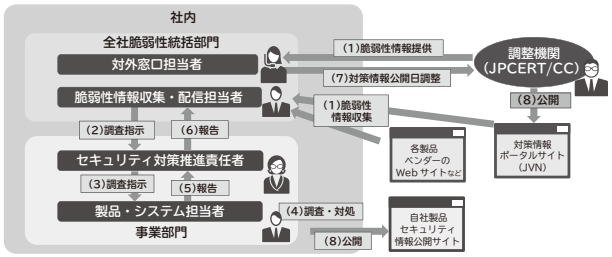


図6　PSIRT・脆弱性管理プロセス構築支援サービス

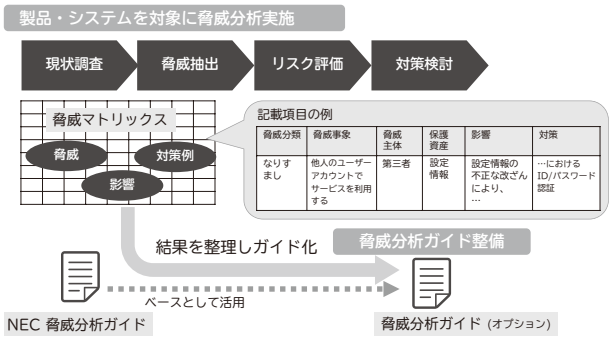


図7　製品・システム脅威分析支援サービス

4.3 制御システム向けサービス

(1)制御システムセキュリティアセスメントサービス

制御システムセキュリティの国際基準であるIEC62443、NIST Cyber Security Frameworkなどをベースに、組織、システムの両面からセキュリティリスクを洗い出し、検出リスクと対策ロードマップを提示します。

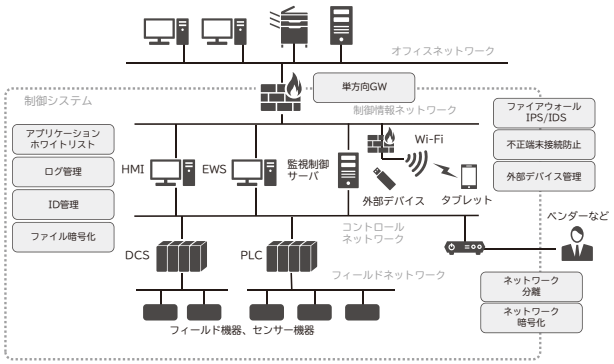


図8　制御システムのイメージとセキュリティ対策の例

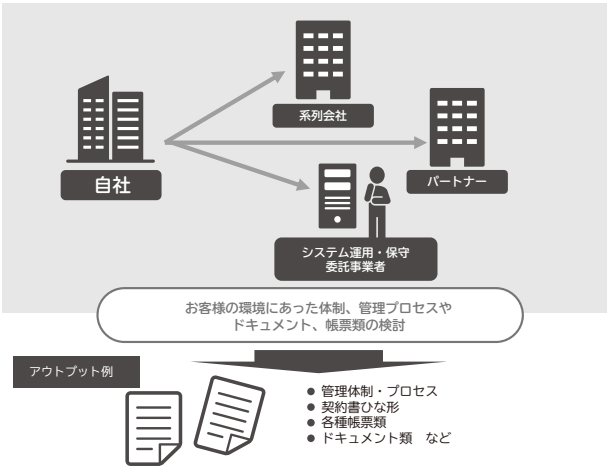


図9　委託先管理セキュリティ強化支援サービス

(2)制御システムセキュリティコンサルティングサービス

制御システムの構築から運用に至る各フェーズや協力会社の管理、インシデントの検知や発生時の対応まで、制御システムの特殊性や可用性に配慮したセキュリティ対策を提供します（**図8**）。

4.4 領域横断のサービス

(1)委託先管理セキュリティ強化支援サービス

NECのプロセス元にした委託先管理のモデルプロセスと照らし合わせてお客様の現状を分析し、課題改善のためのプロセス立案やマニュアルなどの整備により、お客様の委託先管理のセキュリティ面での強化を支援します（**図9**）。

(2)サイバーセキュリティ教育サービス

情報セキュリティの基礎知識から、不正攻撃から情報システムを守るための専門的な技術ノウハウまで、さまざまな知識やスキルを、座学やマシン実習を通して学習できる教育メニューを提供しています。組織全体のセキュリティ底上げから、インシデント対応シミュレーションやマルウェア感染体験トレーニングといった専門的なご要望まで幅広く対応します。

5. まとめ

NECでは、長年にわたる社内情報セキュリティ対策やCSIRTの運用、そしてNECグループの製品・システム・サービスのセキュリティを確保するセキュア開発・運用の取り組みをノウハウ化し、お客様のセキュリティ対策を支援するさまざまなコンサルティングサービスを提供しています。

今後も、更なる先進的なセキュリティ対策を実践しながら、お客様のサイバーセキュリティ経営における課題解決を支援するサービスを提供していきます。

参考文献

1) 経済産業省：サイバーセキュリティ経営ガイドライン
http://www.meti.go.jp/policy/netsecurity/mng_guide.html
2) IPA：サイバーセキュリティ経営ガイドライン解説書
https://www.ipa.go.jp/security/economics/csmgl-kaisetsusho.html

執筆者プロフィール

吉府 研治
サイバーセキュリティ戦略本部
シニアエキスパート

伊東 真理
サイバーセキュリティ戦略本部
エキスパート

山田 知秀
サイバーセキュリティ戦略本部
セキュリティ技術センター
主任

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

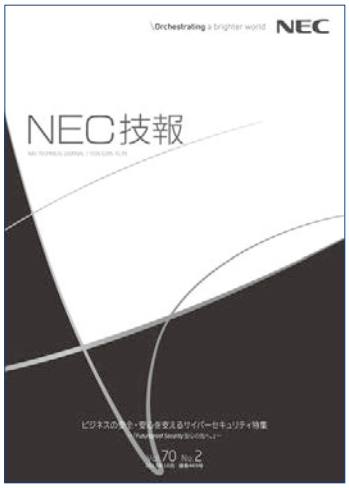
◇ 特集論文

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