サイバーセキュリティ対策の社内事例

吉田 篤正

要 旨

巧妙化・高度化するサイバー攻撃から企業を守るために、NECグループは20年以上にわたり蓄積したノウハウや、国際的なセキュリティ専門機関や警察などの外部機関との情報共有を通して、プロアクティブなサイバーセキュリティ対策をNECグループの国内外に展開しています。また、AI（人工知能）やSDN（Software Defined Networking）の技術を活用し、サイバー攻撃の被害を局所化するシステムの実用化を推進しています。本稿では、NECグループ内でグローバルに展開しているサイバーセキュリティ対策と、以前から実施している、お客様情報や秘密情報を守るための、情報セキュリティ基盤について紹介します[1)]。

KeyWords　サイバーセキュリティ／AI／SDN／ASI／GCAPS／NCSP／CSIRT／マルウェア／クラウド認証連携／多要素認証／InfoCage／OMCA

1. サイバーセキュリティ対策の強化

昨今、サイバー攻撃が巧妙化・高度化するなか、NECグループは、注力するセキュリティ分野の1つとして、サイバーセキュリティ対策の強化を最重要施策として位置付け、CISO（Chief Information Security Officer）を筆頭に、さまざまな活動をNECグループの国内外に展開しています。以下に、主な活動を紹介します。

1.1 サイバーセキュリティリスク分析

NECグループでは、標的型攻撃、ランサムウェア（ファイルが暗号化され、復号と引き換えに身代金を要求）、ばらまき型メール攻撃（不特定多数を狙った攻撃）など、日々発生するサイバー攻撃の脅威に対してリスク分析を行い、分析結果に基づきサイバー攻撃対策を実施しています。リスク分析は、「サイバー脅威分析」（NECグループへの攻撃状況や攻撃の特徴を把握し、リスクに応じた対処検討）、「監視運用分析」（変化するサイバー脅威動向に追随するよう運用プロセスを適宜見直し）、「ソリューション・IT分析」（対策製品・サービスのNECグループ内IT環境への適合性分析）、及び「対策分析」（NECグループにとって今後必要となる対策の検討）の4つに分類しています。

1.2 グローバルサイバー攻撃対策

NECグループでは毎年、サイバーセキュリティリスク分析に基づいて対策の計画を立案し、CISOの承認のもと、対策を実施しています。

とりわけ、社会ソリューション事業を国内外に展開するNECグループにおいて、グローバルで統一的にサイバーセキュリティリスクに対応することは、事業継続の必須条件ととらえています。

グローバルサイバー攻撃対策では、（1）未知の攻撃検知、（2）ログの統合管理・監視、（3）GCAPS（Global Cyber Attack Protection System）導入、（4）CSIRT（Computer Security Incident Response Team）体制の確立の大きく4点に注力し施策を展開しています（**図1**）。

（1）未知の攻撃検知

入口・出口対策として、未知のマルウェア検知システムを導入し、Web通信とメール受信を監視し、検知した未知のマルウェア情報などを基に、不正通信をフィルタリングするとともに、感染が疑われるPC及びサーバへの処置を実施します。

（2）ログの統合管理・監視

NECグループ約18万台のPC・サーバの通信やセキュ

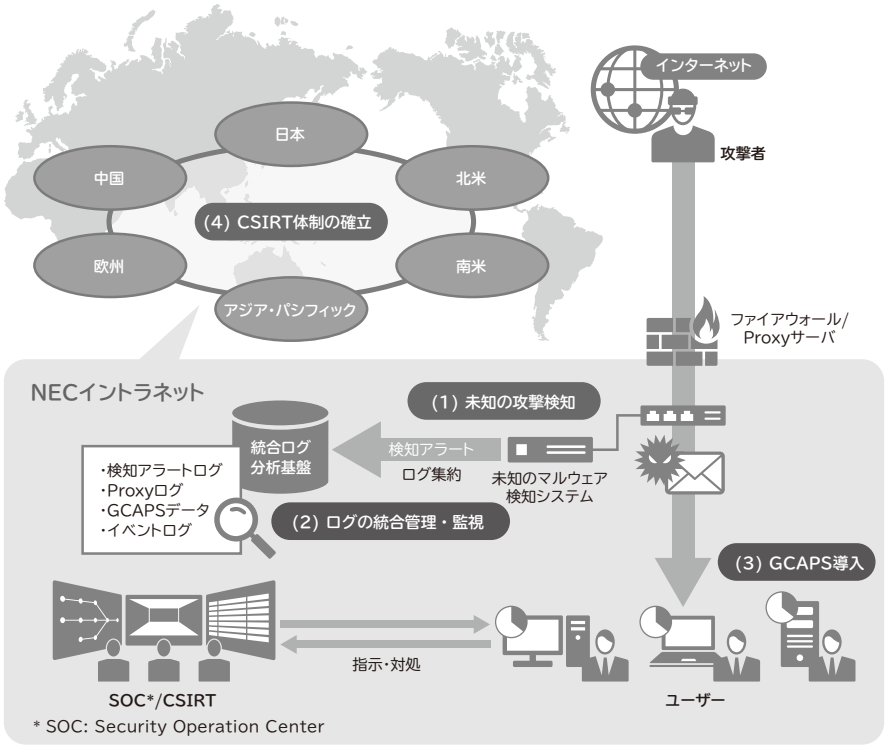


図1　グローバルサイバー攻撃対策の全体像

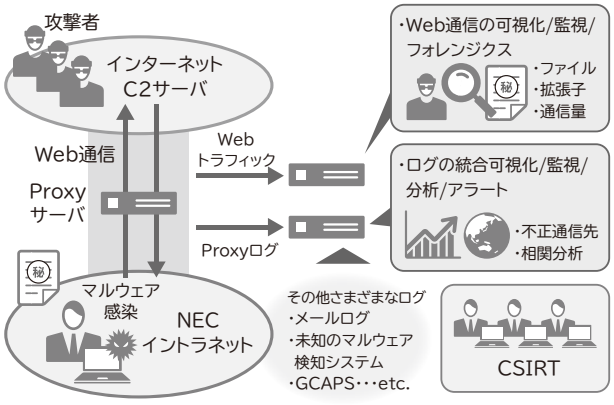


図2　ログの統合分析とパケットの調査

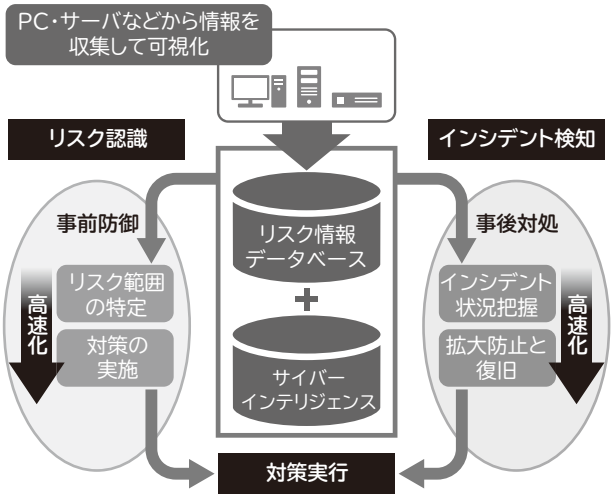


図3　GCAPSコンセプト

リティ機器のログを統合的に集約管理し、解析調査の効率化、高度化を図っています。また、複数のログを相関的に分析することで、潜在的なリスクの発見と、情報漏えいリスクの低減につなげています（**図2**）。

（3）GCAPS導入

PC・サーバの脆弱性対策及びインシデントレスポンスの効率化を目的として、NECグループ全社に対してGCAPS（外販ソリューション名：NCSP＜NEC Cyber Security Platform＞）を展開しています。GCAPSでは、リスク認識に基づき対処を行う「事前防御」とインシデント検知発生時の「事後対処」の2つの側面からPC・サーバ対策の強化をグローバルに

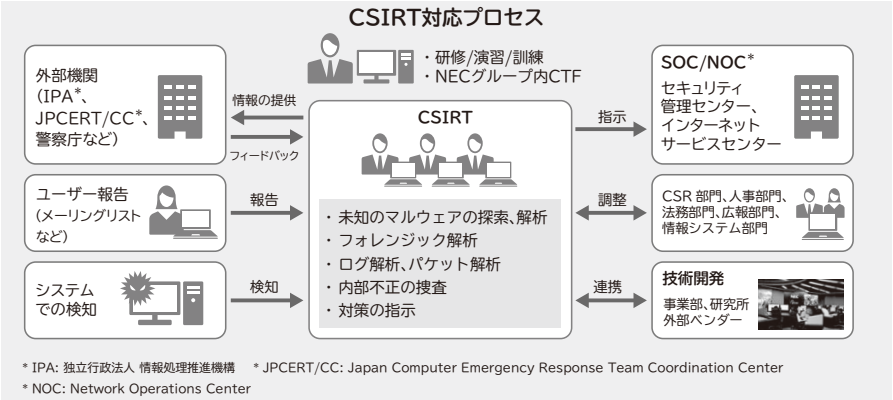


図4　CSIRTの全体像

実施します（**図3**）。

（4）CSIRT体制の確立

NECグループでは、CISO配下にCSIRTを設置しています。CSIRTではサイバー攻撃を監視し、攻撃やマルウェアの特徴を分析しており、各関係機関との情報共有も行っています。インシデント発生時には保全や攻撃の解析を実施し、原因究明や事態の収束を行います。また、サイバー攻撃の検知状況や不正通信先などの情報に基づいた、「サイバーインテリジェンス」と呼ばれる知見をグローバルに共有して、各海外現地法人のCSIRTが連携する体制を整備しています（図1、**図4**）。

人材面では、CSIRTの技術力向上のため、研修や演習、NECグループ内のセキュリティコンテストCTF（Capture The Flag）などを実施しています。また、組織全体での対応力強化のため、経営者参加型の総合演習も実施しています。

1.3 NEC先端技術領域の価値実証

NECグループでは、SDNやAIを組み合わせたサイバーセキュリティの先端技術領域において、実際のIT環境での価値検証・実証を行いながら、NECの注力領域の成長と先進的な社内リファレンス構築を図っています。

（1）SDN×サイバー攻撃対策連携

ランサムウェアや標的型攻撃などのマルウェア感染後の更なる迅速な被害局所化を実現するため、SDNを活用したサイバー攻撃自動防御システムの価値検証を行ったうえで、それをNECグループ内に導入しております。

（2）ASI（Automated Security Intelligence）

AIを活用したNECの自己学習型システム異常検知技術である「ASI」の価値検証を、NECの研究所と連携して進めています。具体的にはシンガポールのNEC Asia PacificのIT環境にASIを導入し、エンドポイントでの未知の攻撃検知と攻撃追跡性能を評価し、評価結果をASIの事業化検討にフィードバックしています。

2. 情報セキュリティ基盤

NECグループでは以前から、お客様情報や秘密情報を守るために、利用者を管理・統制して、PCやネットワーク、業務システムを安全・安心かつ効率的に利用できる情報セキュリティ基盤を構築・運用しています。

情報セキュリティ基盤は「利用者を管理・統制するIT基盤」「PC、ネットワークを守るIT基盤」「情報を守るIT基盤」の3つの基盤が相互に連携し補完し合いながら、NECグループの情報セキュリティポリシーを実現しています。以下に、これら3つの基盤を紹介します。

2.1 利用者を管理・統制するIT基盤（認証基盤）

情報セキュリティにおける管理の基本は、個人認証の仕組みです。人を特定し認証する仕組みにより、情報資産への適切なアクセスコントロールやデジタル証明書を利用した、なりすまし防止などを実現できます。現在、NECグループでは、利用者を管理・統制する認証基盤の強化を進めています。主な強化施策として、「クラウドサービスとの認

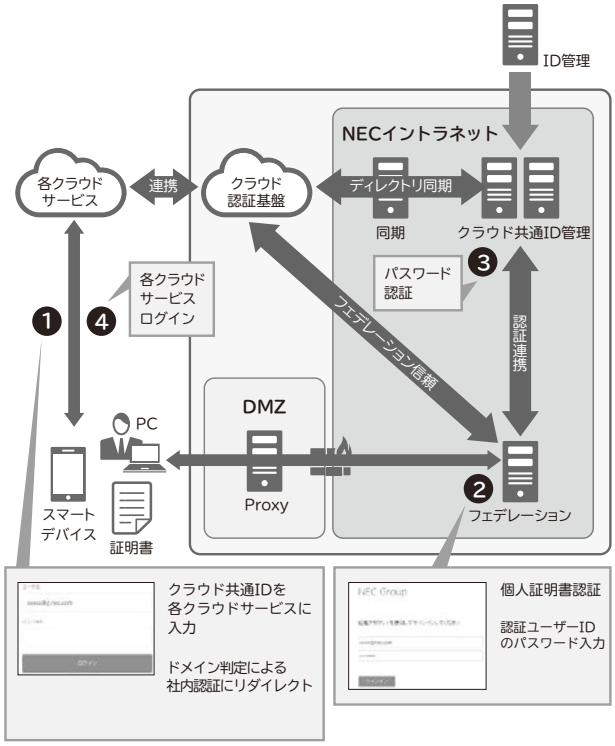


図5　クラウド認証連携

証連携」及び「多要素認証」について紹介します。

(1)クラウドサービスとの認証連携

ビジネス環境の多様化が進むにつれ、外部との情報共有や、クラウドサービスを利用するニーズが増えてきています。そこで、NECグループは、グループ内の認証基盤とクラウドサービスとの認証連携を実現し、安全・安心にクラウドサービスを利用できる仕組みを基盤として導入しています(**図5**)。

(2)多要素認証

内部不正対策、サイバー攻撃(標的型攻撃)対策を強化するため、重要情報を扱うシステムのアクセス制御には、ユーザーID、パスワード(記憶認証)だけでなく、デジタル証明書を利用した個人認証(所有物認証)の導入を推進しています。また、今後は顔認証(生体認証)も組み合わせることを実現していきます。

2.2 PC、ネットワークを守るIT基盤

NECイントラネットに接続される情報機器のセキュリティを維持し、ウイルスやワームからPC、ネットワークを守るIT基盤を整備しています。昨今、リスクがますます高まっている標的型攻撃に対して、セキュリティ更新プログラムやウイルス対策ソフトの確実な適用が重要です。

NECイントラネットでは、PC及びネットワークの状態を把握するソフトウェアの導入を義務化しており、ネットワークやPCの状態を見える化することで、ユーザーのソフトウェアの適正利用状況を監視しています。

セキュリティ対策が不十分なPCやマルウェアに感染したLANはイントラネットから自動遮断し、また、NECグループ外への通信は、Webアクセスフィルタリング、フリーメール対策、送信ドメイン認証などを実施しています。

また、脆弱性検査ツールを使用し、NECイントラネットに接続された情報機器の脆弱性をネットワーク経由でチェックし、発見された脆弱性はシステムにより一元管理しています。発見された脆弱性は各部門で是正し、是正状況についてもシステムで一元管理しており、NECグループ全体の対応状況をフォローできるようにしています。

2.3 情報を守るIT基盤

情報漏えいを防止するには、情報流出につながる経路を特定し、リスク分析を行ったうえで適切な対策を講じる必要があります。NECグループでは、グループの情報以外にも、お客様からお預かりした情報やお取引先に開示する情報などを管理しています。そのため、ネットワーク、PC、外部記憶媒体などのITの特徴やリスクを考慮し、情報流出につながる経路(マルウェア感染、メール、外部記

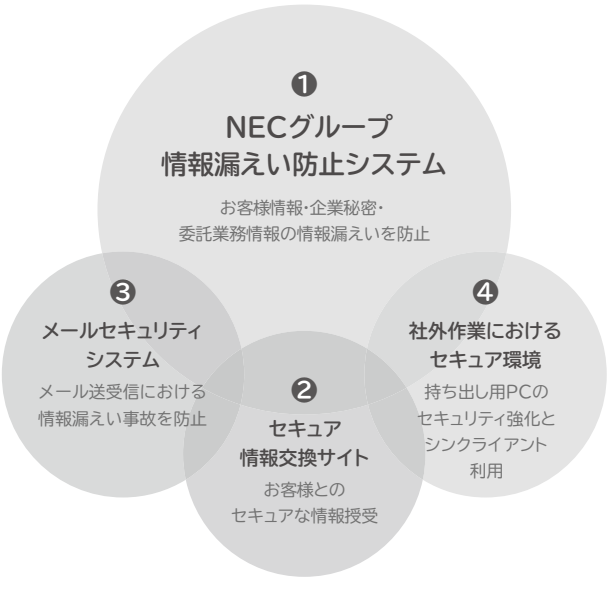


図6　情報を守るIT基盤の全体像

憶媒体、持ち出し）に対して網羅的かつ多層的な対策を行っています（**図6**）。

（1）NECグループ情報漏えい防止システム

NECグループでは、自社製品であるInfoCageシリーズを活用した情報漏えい防止システムを構築し、「暗号化（InfoCage FileShellを導入）」「デバイス制御」「ログの記録・監視」を実施することにより、外部攻撃や内部不正による情報漏えいリスクへの対策を行っています（**図7**）。

（2）安全な情報交換の仕組み

NECグループでは、お客様やお取引先と重要な情報を安全・確実にやり取りするため、「セキュア情報交換サイト」を運用しています。セキュア情報交換サイトでは、アクセスが制限されたエリアで情報をやり取りし、このエリアへのアクセスにはワンタイムURLとパスワードが必要です。このサイトを利用すれば、USBメモリなどの外部記憶媒体を使って情報を交換する機会が減り、盗難・紛失による情報漏えい事故のリスクが軽減されます。

また、NECグループでは「メール誤送信防止システム」を導入し、メールアドレスの入力誤りやファイルの添付誤りによる情報漏えい事故や、故意にメールを転送して情報を漏えいさせることを防止しています。

他にも標的型攻撃メールの疑いがある不審なメールに対して注意喚起する機能や、メール送信前に、宛先と添付ファイルを確認する画面をPC上でポップアップする機能を持つOMCA（Outlook Mail Check AddIn）をNECグループ内に展開し、メール送受信時の安全性の向上を図っています。

（3）社外作業におけるセキュア環境

NECグループでは、PCの持ち出しの目的や利用環境などにより、「シンクライアント端末」や盗難・紛失時におけるPC内の情報保護を強化した持ち出し用の「Trusted PC」などを利用しています。「Trusted PC」は、「HDD全体の強固な暗号化機能」や「遠隔からのデータ消去、PCのロック機能」などを搭載しています。

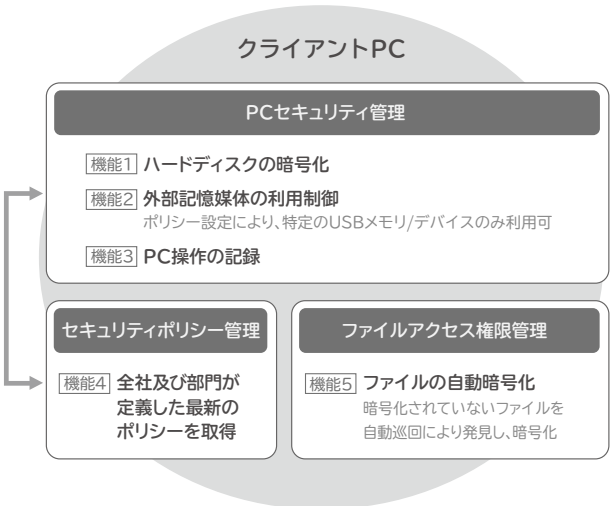


図7　情報漏えい防止システム概要

参考文献

1）NEC：情報セキュリティ報告書2017
http://jpn.nec.com/csr/ja/security/index.html

執筆者プロフィール

吉田 篤正

経営システム本部
エキスパート

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

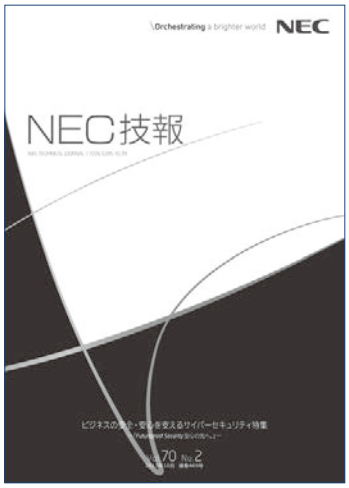
◇ 特集論文

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