\Orchestrating a brighter world

NEC

Information Security Report 2016

NECが考える情報セキュリティ

NECグループは、「情報セキュリティ」を重要な経営活動として位置づけ、
「社会ソリューション事業」を通じて新しい価値を創造していきます。

Information Security Report 2016

りゅうの　やすじろう
龍野 康次郎
日本電気株式会社
執行役員常務
兼CIO（チーフインフォメーションオフィサー）
兼CISO（チーフインフォメーションセキュリティオフィサー）

人類は今、世界の人口増加や都市化率の上昇、エネルギーや食糧への需要拡大など、地球規模での課題に直面しています。NECグループは、グローバルな社会課題を解決し、人が豊かに生きるために不可欠な「安全」「安心」「効率」「公平」という社会価値を創造したいと考えています。お客さまはもちろん、世界の国々や地域の人々とともに、文化や多様性を尊重し、明るく豊かな人々の暮らしや効率的で洗練された社会を支え、希望にあふれた未来につなげていきます。これこそが、NECグループの「社会ソリューション事業」であり、世界中のお客さま・パートナーに向けた事業ブランドメッセージである「Orchestrating a brighter world（世界の想いを、未来へつなげる）」に込めた想いです。

社会ソリューション事業が生み出す社会インフラが提供する価値は、今後、利用する情報が広がるにつれ一層高度化していきます。そうした中、「ビッグデータ」、「クラウド」、「SDN」、「サイバーセキュリティ」は、ますます重要なテーマとなってきています。中でも、サイバーセキュリティは、IoT（Internet of Things、モノのインターネット）を含め、あらゆるITシステムへの導入が必須であり、また2015年に、経済産業省およびIPA（独立行政法人情報処理推進機構）から、企業経営にとって必要なサイバーセキュリティ対策に関するガイドライン「サイバーセキュリティ経営ガイドライン」が発行されています。企業が事業を継続していくためには、サイバーセキュリティは特に重要性を増しています。NECグループは、業界トップクラスの技術を持つ企業との連携により2年前から競争力強化に取り組んでいます。また、グローバル成長戦略の柱の1つとして、「グローバルセーフティ事業」を掲げ、シンガポールに立ち上げたサイバーセキュリティの拠点を活用し、長年培ってきた技術を活かし現地主導型でグローバル展開を加速します。

NECグループは、これらの領域におけるコアアセットをフルに活用し、OneNECとして総合力を発揮し、新しい価値を創造していきます。そして、誰もが安心して情報通信技術の恩恵を享受し、豊かな社会を実現していくために、情報セキュリティを重要な経営活動として位置づけ、継続的に以下の活動に取り組んでまいります。

- 「OneNEC」として、NECグループが一体となって情報セキュリティの維持・向上を推進
- NECグループだけでなく、お取引先まで含めた施策を展開
- 適切な情報保護と適切な情報活用・共有を両立
- 情報セキュリティマネジメント、情報セキュリティ基盤、情報セキュリティ人材の各領域からの総合的アプローチにより、多層的に情報セキュリティを維持・向上
- お客さまに信頼されるセキュリティソリューションを社内で実証し、提供

本報告書は、NECグループの情報セキュリティへの取り組みをご紹介するものです。ステークホルダーのみなさまとのコミュニケーションをとおして、企業活動の改善をはかり、社会から信頼される情報セキュリティリーディングカンパニーを目指してまいります。ぜひご一読くださいますようお願い申し上げます。

情報セキュリティ報告書 2016

報告書の発刊にあたって

本報告書は、ステークホルダーのみなさまにNECグループの情報セキュリティに関する取り組みをご理解いただくことを目的に発刊いたしました。本報告書では、2016年6月までの取り組みを対象に掲載しています。

本報告書に関するお問い合わせ

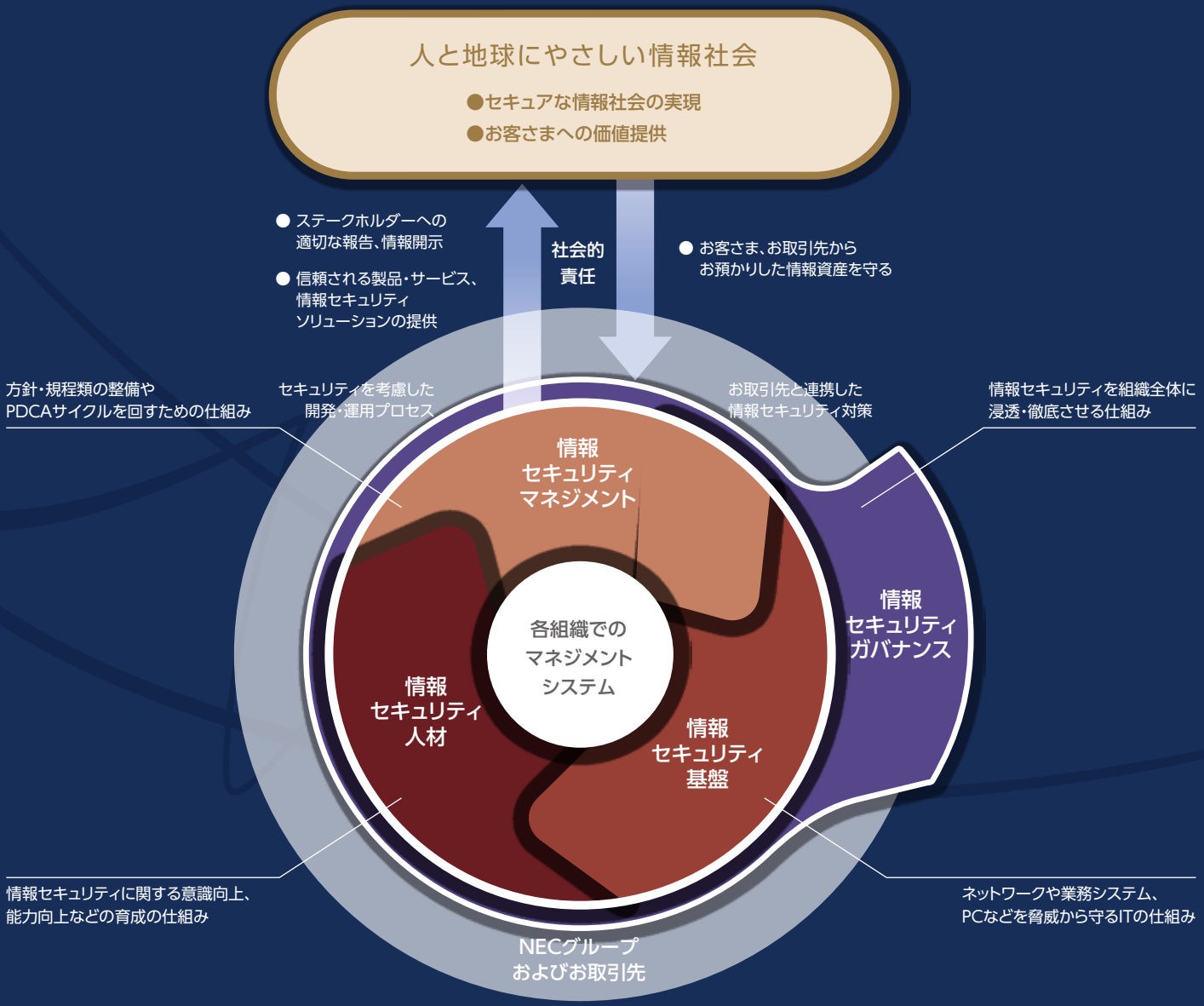
日本電気株式会社
経営システム本部 セキュリティ技術センター
〒108-8001 東京都港区芝五丁目7-1 NEC本社ビル
03-3798-6980

情報セキュリティ推進フレームワーク

NECグループは、グループ全体で情報セキュリティの維持・向上をはかり、
セキュアな情報社会の実現とお客さまへの価値を提供することで、
「人と地球にやさしい情報社会」の実現に貢献します。

情報セキュリティの脅威は、日々変化しており、ITで高度化された社会において、情報セキュリティは欠くことのできない重要な経営課題です。NECグループは、社会から信頼される企業として社会的責任を果たすため、「情報セキュリティ推進フレームワーク」を確立し、お客さま、お取引先からお預かりした情報資産を守り、信頼される製品・サービス・情報セキュリティソリューションの提供、ステークホルダーへの適切な報告・情報開示を通じて、セキュアな情報社会の実現とお客さまへの価値を提供します。

情報資産を守るための情報セキュリティの取り組みとしては、次の4つの要素（情報セキュリティガバナンス、情報セキュリティマネジメント、情報セキュリティ人材、情報セキュリティ基盤）を組み合わせることにより、総合的かつ多層的に情報セキュリティの維持・向上をはかっています。



これらは、全社的な取り組みとNECグループの各組織の取り組みに分けられます。

全社的な取り組みとしては、情報セキュリティ基本方針・全社規程の制定、共通的な情報セキュリティ基盤の整備、教育・意識啓発・人材育成の制度運営などの施策の立案・実施・見直し・改善を行うとともに、これらを組織全体に効果的・効率的に浸透・徹底させる仕組みとして情報セキュリティガバナンスがあります。また、グループ内だけでなくお取引先と連携したセキュリティ対策の展開や、信頼される製品・サービス・ソリューションを提供するための開発・運用プロセスの確立を推進しています。

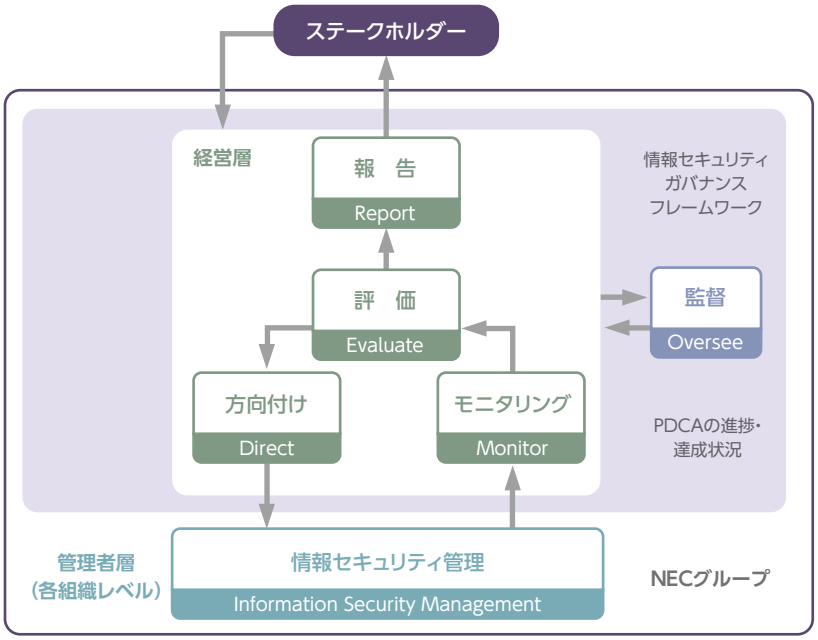
NECグループの各組織の取り組みとしては、全社の推進を受け、各組織の事業環境や内部組織体制を考慮した各組織でのマネジメントを行っています。

情報セキュリティガバナンス

事業活動と情報セキュリティを整合し、NECグループ全体で効率的、効果的に
情報セキュリティレベルを高め、事業活動から生じるリスクをコントロールするため、
情報セキュリティガバナンスを確立しています。

1 ‖ NECグループの情報セキュリティガバナンス

NECは、グループ全体が総合力を発揮するために「NECグループ経営ポリシー」を定め、事業遂行に関する各種ルールの共通化、制度・業務プロセス・インフラの統一を行いグローバルスタンダードな経営基盤の実現するベースを確立しています。「OneNEC」として全体のセキュリティレベルを向上させるためには、情報セキュリティのガバナンスが不可欠です。経営層は、セキュリティ目標を定め、グループ施策、体制構築、経営資源の割り当てなどの方針を決定します。そして、組織レベルでの施策の進捗・達成状況や情報セキュリティ事故の発生状況をモニタリングし、要求事項への適合性の評価、必要な指導や仕組みの改善により新たな方向付けを行います。こうした経営層と管理者層のサイクルとそれを監督する機能により、グループとしての全体最適を追求するとともに、ステークホルダーに対する適切な情報開示を行い、企業価値の持続的な向上をはかります。

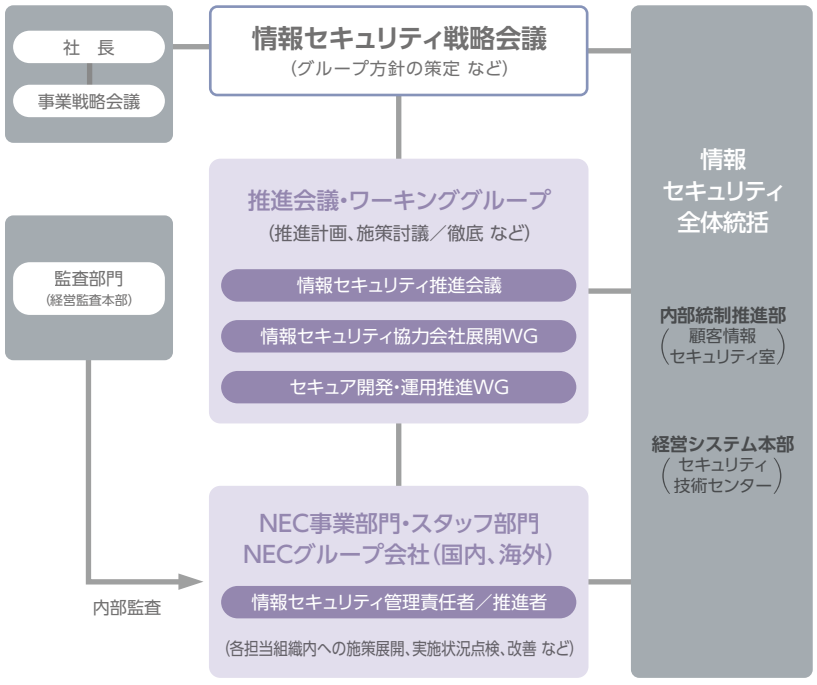


情報セキュリティガバナンス

2 ‖ NECグループの情報セキュリティ推進体制

NECグループの情報セキュリティ推進体制は、情報セキュリティ戦略会議とその下部組織、および各組織の推進体制で構成されます。「情報セキュリティ戦略会議」は、CISO(チーフインフォメーションセキュリティオフィサー)が議長を務め、サイバーセキュリティリスクを含む、情報セキュリティリスクに対応するため、「情報セキュリティ施策の審議・評価・改善」、「重大事故の原因究明と再発防止策の方向付け」、「情報セキュリティビジネスへの成果活用」などの審議を行います。下部組織である3つの推進会議やワーキンググループは、国内、海外、お取引先、セキュア開発・運用に関する「推進計画、実行施策に関する討議・調整、指示事項の徹底、施策進捗管理」などを行います。

各組織の情報セキュリティ管理責任者は、主管するグループ会社も含めて情報セキュリティに関する一義的な管理責任を負い、組織内へのルールの周知徹底、施策の導入・運用、実施状況の点検、見直し、改善などを継続的に実施し情報セキュリティの維持・向上をはかっています。



情報セキュリティ推進体制

NECグループが注力するセキュリティ分野

サイバー攻撃対策強化

サイバー攻撃が巧妙化・高度化する中、サイバーセキュリティリスク分析に基づく先進的な対策を
国内外で実施するとともに、CSIRT*1によるインシデント対応を行い、サイバーセキュリティ経営を実現しています。

*1 CSIRT: Computer Security Incident Response Team

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、復号化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標的型攻撃に類似した攻撃）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、以下のとおり4つに分類しています。

【サイバー脅威分析】
日々のサイバー攻撃の監視やマルウェア解析、情報共有により、NECグループへの攻撃状況や攻撃の特徴を把握します。また、脅威リスクレベルを判断し、状況に応じた対処を検討します。

【監視運用分析】
現状の監視運用のプロセスを適宜見直し、変化するサイバー脅威動向に追随する運用を検討するとともに、運用上の課題を整理します。

【ソリューション・IT分析】
対策製品・サービス、市場動向を調査し、日々進化する技術を把握します。またPoC*2評価、NECグループ内IT環境調査により、対象製品・サービスのグループ内IT環境への適合性などを分析します。

*2 PoC: Proof of Concept（新しい概念の実証試験）

【対策分析】
「サイバー脅威分析」、「監視運用分析」、「ソリューション・IT分析」の3つの分析に基づき、NECグループにとって、今後必要となる対策を検討し、その対策の対象範囲、効果やコストを整理します。

毎日
頻度の目安
四半期

	分析項目	活動	関連検討/報告会議
サイバー脅威分析	・攻撃状況（頻度、範囲） ・攻撃手法とその特徴 ・マルウェアの特徴/挙動 ・攻撃元や通信先 ・リスクレベル ・対処方法	・攻撃監視、対処 ・サイバー事案対応 ・マルウェア解析 ・インテリジェンスサービス活用 ・脅威/脆弱性情報収集 ・各機関との情報共有	・サイバー攻撃対策検討会議 ・CSIRT技術検討会議 ・SOC間情報共有
監視運用分析	・社内運用内容 ・運用レベル目標 ・運用ルール、プロセス ・現状の運用の課題、問題点	・セキュリティ管理センター（SOC）やCSIRTによるサイバーセキュリティ運用	・サイバー攻撃対策検討会議 ・SOC間情報共有
ソリューション・IT分析	・対策施策製品/サービス内容 ・競合他社比較 ・市場動向 ・社内環境への適合性	・国内外カンファレンス参加/調査 ・PoC評価 ・外部機関との情報共有 ・各ベンダーとのミーティング	・サイバー攻撃対策検討会議 ・SOC間情報共有 ・情報セキュリティ戦略会議
対策分析	・対策内容 ・対策期待効果 ・対策後の残存リスク ・コスト ・対象範囲（資産や部門など）	・対策検討 ・情報セキュリティ戦略会議での計画審議/承認/実績評価	・情報セキュリティ戦略会議

分析結果から計画を立案するとともに、施策へのフィードバックも実施

サイバーセキュリティリスク分析

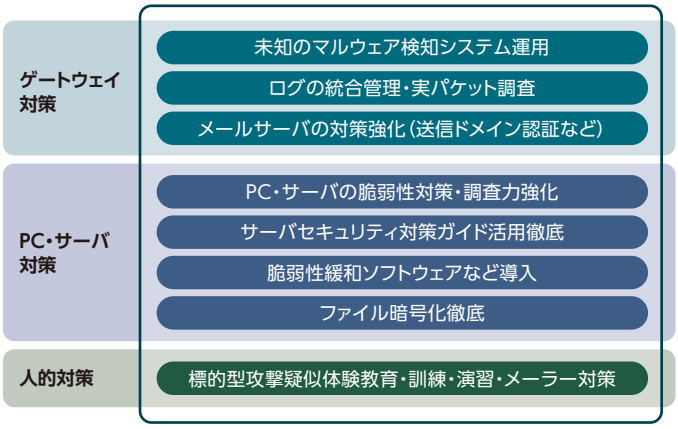
2 ‖ サイバー攻撃対策

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く対策の計画を立案し、CISO（チーフインフォメーションセキュリティオフィサー）承認の下、対策を実施しています。特に、標的型攻撃対策としては、未知のマルウェアによる攻撃検知を重点対策と位置づけ、「ゲートウェイ対策」、「PC・サーバ対策」、「人的対策」を多層的に実施しています。

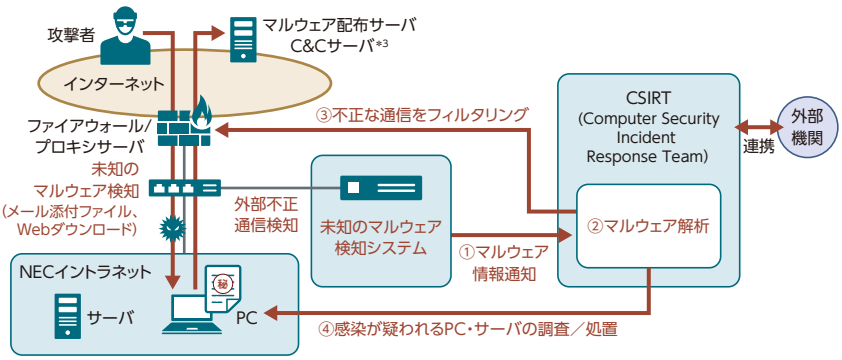
❶ ゲートウェイ対策

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通信とメール送受信を監視し、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。

また、NECグループ10万人規模の、通信や操作のログデータの統合的な管理・分析、パケットの調査を行い、攻撃者の痕跡を分析・調査しています。

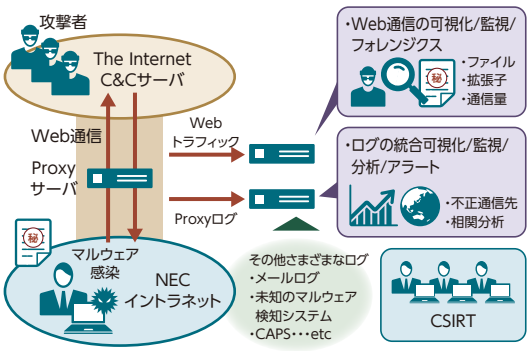


NECグループにおける標的型攻撃対策



*3 C&Cサーバ: Command & Controlサーバ

未知のマルウェア・不正通信の検知



ログの統合分析とパケットの調査

❷ PC・サーバ対策

PC・サーバの脆弱性対策強化およびインシデントレスポンスの効率化を目的として、2016年度よりグループ全社に対してGCAPS*4(外販ソリューション名:NCSP*5)を展開しています。

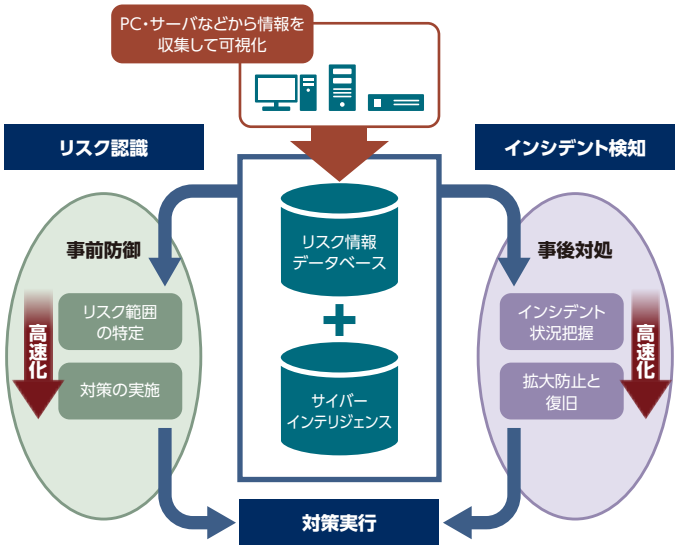
GCAPSでは、リスク認識に基づき対処を行う「事前防御」とインシデント検知発生時の「事後対処」の2つの側面からPC・サーバ対策の強化をはかっています。

*4 GCAPS: Global Cyber Attack Protection System
*5 NCSP: NEC Cyber Security Platform

❸ 人的対策

NECグループでは、全社員に対して、「標的型攻撃疑似体験教育」を実施し、高度な攻撃への対応力強化をはかっています。さらに、全社の各端末にOMCA*6を導入し、不審なメールへの気づきを与える対策を行っています。その他、特定部門への訓練や、経営者と関係部門を巻き込んだ総合演習も実施しています。

*6 OMCA: Outlook Mail Check Addin

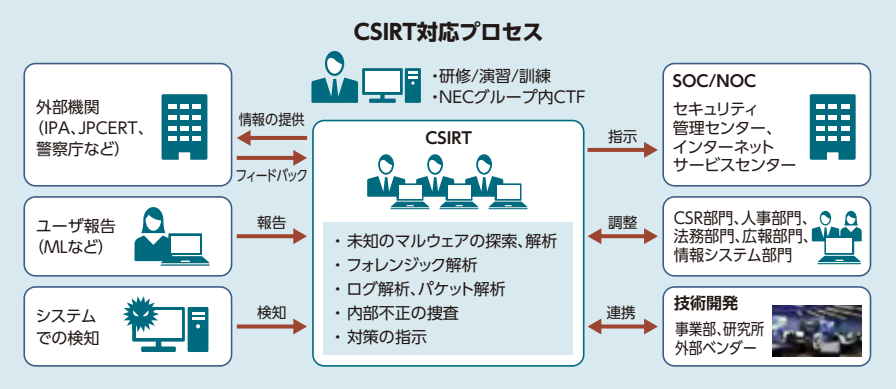


GCAPSのコンセプト

3 ‖ CSIRT活動

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て、攻撃やマルウェアの特徴などを分析しており、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、CSIRTの技術力向上のため、演習や訓練、NECグループ内のセキュリティコンテストCTF*7なども実施しています。

*7 CTF: Capture the Flag



CSIRTの全体像

4 ‖ グローバルサイバー攻撃対策

海外現地法人においても、国内と同様の考え方にて対策を実施しています。サイバー攻撃の検知状況や不正通信先などのサイバーインテリジェンスをグローバルに共有し、海外現地法人も対応できる体制を整備しています。

NECグループが注力するセキュリティ分野

海外現地法人の情報セキュリティ

NECグループでは、海外現地法人においても日本国内と同様の情報セキュリティレベルを目指し、
現地法人における情報セキュリティ対策（ポリシー・ルール、マネジメント、インフラ）を実施しています。

1 ‖ グローバルNECイントラネット

NECグループでは、グローバルNECイントラネットとして各地域イントラネットを介して海外の150拠点以上を接続しています。各地域のイントラネットはその地域の統括会社により管理され、地域間の相互接続などの運用をNECがグローバルで一元管理しています。

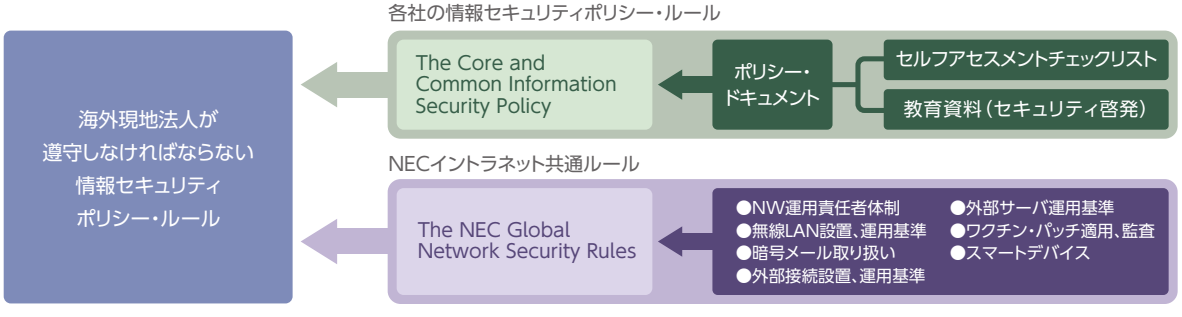
グローバルNECイントラネット

2 ‖ 情報セキュリティポリシー・ルール

NECグループでは、海外現地法人が遵守しなければならない共通の情報セキュリティポリシー・ルールを各社で定めています。

各社の情報セキュリティポリシー・ルールについては、NECが用意した雛形（The Core and Common Information Security Policy）を基に、所在国・地域の法規制に準拠し、自社の組織構造に合わせた役割をマッピングして作成されており、NECグループではグループ均質のセキュリティ対策を推進しています。この雛形はISO/IEC27001をベースにしており、グローバルでも受け入れやすいドキュメント体系としています。各社で加筆・変更した内容は、NECが確認し承認しています。例えば、ソフトウェア開発を受託している現地法人では、雛形に追記することで、情報セキュリティポリシーを強化しています。

また、グローバルNECイントラネット共通ルール（The NEC Global Network Security Rules）を展開しており、イントラネットを利用している現地法人はこれを共通ルールとして遵守しています。本ルールには管理体制、外部インターネットとの接続、オフィス内ネットワークなどに関するルールが含まれ、サイバー攻撃など新しい脅威への対策の導入など、適宜改定されます。



グローバル情報セキュリティポリシー・ルール

3 ‖ 情報セキュリティマネジメント

NECグループでは海外現地法人の従業員向けに情報セキュリティ教育のコンテンツを作成し、Webベース教育を毎年実施しています。教育コンテンツは7か国語で作成されており、母国語で教育が受講できるよう配慮され、各現地法人従業員などの情報セキュリティ意識向上につながっています。

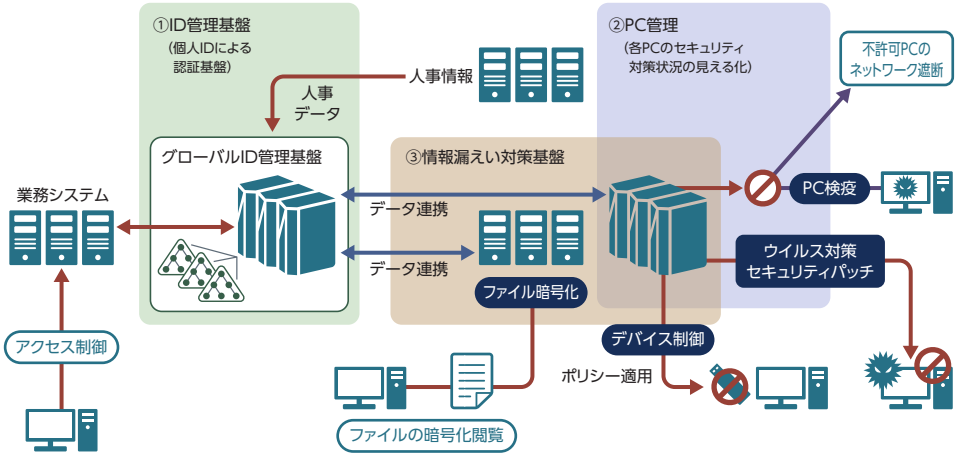
また、各社の情報セキュリティ対策状況を把握するため、上記Webベース教育と合わせて、情報セキュリティ点検を毎年実施しています。NECは点検結果を基に各社へ対策を指示するとともに、定期的に対策状況をフォローしています。

さらに各社のネットワークセキュリティ対策状況を把握するため、グローバルNECイントラネット共通ルールを基にしたネットワークセキュリティ監査を地域ごとに毎年実施しており、監査結果を基に定期的に対策状況をフォローしています。

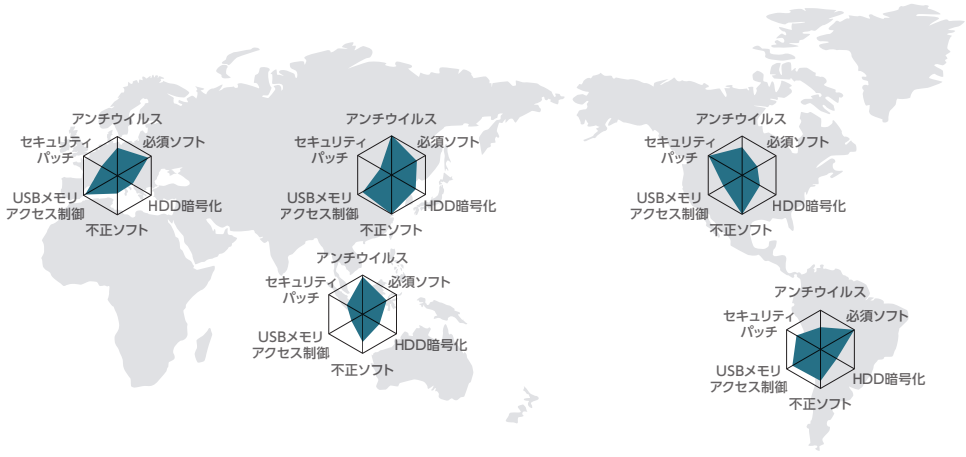
4 ‖ 情報セキュリティ基盤

情報漏えい対策基盤として、NECグループ内でやり取りするファイルを暗号化し、権限のある者しかファイルを閲覧することができない「ファイル閲覧制限管理」を導入しています。海外現地法人においても、日本国内と同様に全従業員に対して一意となるユーザIDを配付し、グローバルID管理基盤を使って一元管理しています。このユーザIDを使ってオフィス文書を暗号化し、第三者への情報漏えいを防止しています。

また、海外現地法人のすべてのPCについてセキュリティ対策状況の見える化および、ウイルス対策、セキュリティパッチ適用、ディスク暗号化の仕組みを導入しています。さらに、USBメモリなどの外部記憶媒体へのアクセス制限（デバイス制御）、不許可PCのネットワーク検疫を順次導入しています。



グローバル情報セキュリティ基盤



PCセキュリティ対策状況の見える化（サンプル）

5 ‖ グローバルでの個人情報保護の動き

「EUデータ保護規則」をはじめとして、各国にて個人情報保護に関する法令の動きが活発になっています。特に、EUデータ保護指令の改定の背景としては、急速なICT技術の進歩やグローバル化と、それによるリスクの拡大、および現行のデータ保護スキームの手続きの煩雑さ、などが挙げられます。これらの動きは、データ移転制限によるグローバルな事業活動や、クラウドなどの革新的なサービスの提供へ影響を与えると考えられるため、その動向の確認が必要となってきています。

NECグループ内では、情報セキュリティ基盤を支える認証情報などを個人情報と位置づけているため、関係部門や有識者と連携して、法令遵守の観点から、個人情報保護に関する国際動向を随時確認し、適宜対応をはかっています。

NECグループが注力するセキュリティ分野

お取引先と連携した情報セキュリティ

NECグループでは、お客さま情報を守るために、お取引先と一体となって情報セキュリティ対策の浸透活動や点検および是正活動を推進し、お取引先における情報セキュリティのレベルアップをはかっています。

1 ‖ 取り組み体系

NECグループの事業活動は、お取引先と連携して遂行されます。お取引先の技術力と共に、NECグループが定めた情報セキュリティ水準に達していることが非常に重要であると考えています。NECグループではお取引先の情報セキュリティ対策状況により、セキュリティレベルを分類しています。そして業務に求められている情報セキュリティレベルに応じて、適切なレベルのお取引先を選定して委託する仕組みを取り入れています。これにより、お取引先の情報セキュリティレベルを一定以上に維持推進するとともに、お取引先で発生する情報セキュリティ事故リスクを低減しています。

レベル(リスク度)	委託先としての適否
A　(リスク小)	委託先として適切。
B　(リスク中)	委託先として適切。 ただし求められるセキュリティ要件に対する改善が前提。
Z　(リスク大)	委託先として不適。 特別な事情がある場合に限り、業務委託可。 ただし求められるセキュリティ要件に対する改善が前提。

情報セキュリティレベル

NECグループとしてお取引先に要求している情報セキュリティ対策は、大きく分類して ①契約管理、②再委託管理、③作業従事者の管理、④情報の管理、⑤技術対策の導入、⑥セキュア開発・運用、⑦点検の実施 の7項となります。

❶ 契約管理

NECグループから業務を委託するお取引先との間で、秘密保持義務などを含む、会社間の包括契約(基本契約)を締結しています。

❷ 再委託管理

お取引先は委託元から書面による事前承諾を得ない限り、他社に再委託してはならない旨、基本契約で定めています。

❸ 作業従事者の管理

NECグループからの委託業務に従事する作業者が守るべきセキュリティ対策を、「お客様対応作業における遵守事項」として定め、自社に対し遵守を誓約してもらうことで、対策実施の徹底を推進しています。

❹ 情報の管理

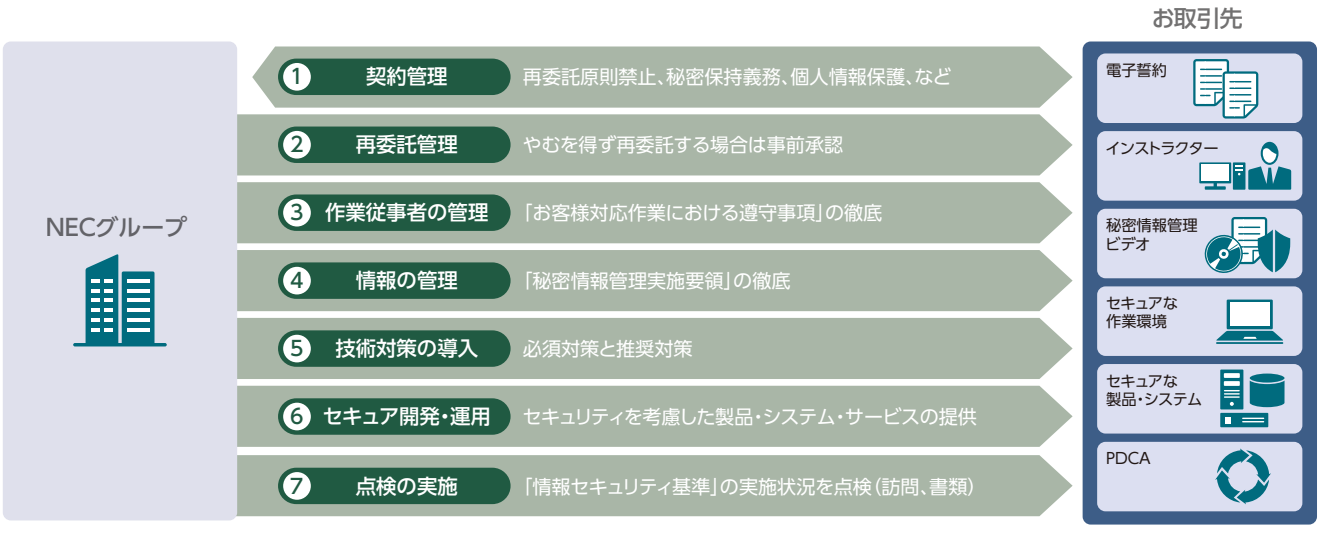
NECグループからの委託業務で取り扱う秘密情報の管理について、「秘密情報管理実施要領」(秘密表示、持ち出し管理、用済み後廃棄・返還など)を定め、購入要件として実施の徹底を推進しています。

❺ 技術対策の導入

マネジメント対策との両輪として技術対策を必須の対策(可搬型電子媒体の全体暗号化など)と推奨の対策(情報漏えい防止システムおよびセキュア情報共有基盤)に分けて導入を依頼しています。

❻ セキュア開発・運用

NECグループのお客さま向けの製品、サービスの開発・運用について、「お取引先様向けセキュア開発・運用実施要領」を定め、セキュリティを考慮



お取引先への情報セキュリティ対策

した開発・運用の実施を依頼しています。例えば、セキュアコーディング規約による開発や、製品・サービスのリリース前の脆弱性診断の実施などです。

❼ 点検の実施

NECグループのお取引先に対する情報セキュリティの要求水準を定義した基準書「お取引先様向け情報セキュリティ基準」に基づき、グループ全体の標準的な仕組み（体制、手順）の下、毎年1回（新規取引先は口座開設時）、お取引先の情報セキュリティ対策実施状況を点検し、適宜改善を指導しています。

2 ‖ お取引先への対策浸透活動

❶ 情報セキュリティ説明会

お取引先がNECグループの情報セキュリティ対策を理解し実施するために、サプライチェーン統括部門と情報セキュリティ部門とが連携し、全国のお取引先を対象に、年1回（対象約1,600社、うちISMS認証取得会社約700社）、情報セキュリティ説明会を全国各地（北海道から沖縄まで13拠点）で開催しています。

❷ 重点お取引先のレベルアップ活動

NECグループとの取引が特に多い重点お取引先（ソフトウェア関連の約100社）には密接な活動を行うことで、施策の実施徹底とレベルアップ促進をはかっています。

❸ 意識維持向上のためのビデオ配付

セキュリティ事故の分析結果を踏まえ、毎年、啓発ビデオを情報セキュリティ説明会で上映するとともに、お取引先に紹介し、社内教育に役立ててもらうことを推進しています。これまでのビデオの題材は、遵守事項、秘密情報管理、ウイルス感染、飲酒による紛失、メール誤送信、個人情報保護、事故発生時対応などです。

❹ 理解度テストシステムの運用

「お客様対応作業における遵守事項」の実施徹底のために、NECグループで用意した「理解度テスト」を定期的にお取引先に配付し、各社内の教育に活用してもらっています。さらに、自社のテスト結果をNECグループに登録すると、全お取引先における自社の位置づけを把握することができる仕組みを構築し、運用しています。

❺ 対策ガイドの配付

お取引先がNECグループの情報セキュリティ対策をより円滑に実施いただけるように、対策の実施ガイドを適宜提供しています。これまで、要求水準達成のための各種ガイド、ウイルス対策ガイド、開発環境セキュリティ対策ガイド、およびスマートデバイスセキュリティルール例などを発行しています。

❻ 委託先管理プロセスの標準化

お取引先における情報セキュリティ対策を推進するのみならず、委託元であるNECグループ側での委託先管理のプロセスを標準化し、サプライチェーンにおいて一貫した情報セキュリティ対策を進めています。

標準化された委託先管理プロセス

3 ‖ お取引先に対する点検および是正活動

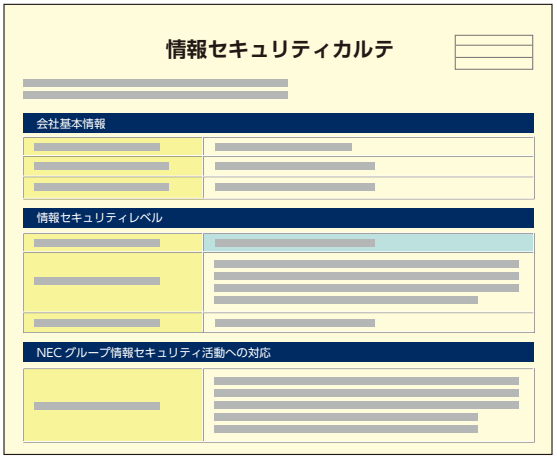
お取引先に対する点検は主に書類点検と訪問点検から構成されています。

書類点検は、NECグループと取引のある会社約1,600社を選定して毎年実施しています。新規のお取引先は口座開設時に実施しています。情報セキュリティ事故の状況などを勘案して毎年作成される点検項目について、お取引先は自社の対策状況を自ら点検し、点検結果をWebシステムに入力します。点検結果はNECグループで報告書にまとめ、Web経由で各社に個別にフィードバックしています。お取引先はNECグループお取引先全体における自社のセキュリティ水準を確認できるとともに、自社が直面している課題を把握でき、効率よく改善を進めることができます。

訪問点検はNECグループとの取引が多いお取引先を対象に、毎年100社前後を選定して実施しています。NECグループの点検担当者として認定された者（約300名）がお取引先を訪問して点検を行うため、お取引先自身による点検（書類点検）では検出できなかった課題事項に気づくことができます。

いずれの点検についても、改善が必要なお取引先は改善計画と改善状況をWebシステムに入力し、NECグループはその内容に基づきフォローアップを行い、お取引先のレベルアップをはかっています。

また点検結果とともに必要な各種情報セキュリティ対策の対応状況をカルテとしてまとめており、お取引先は自社の対応状況を総合的に把握できるようになっています。



情報セキュリティカルテ

NECグループが注力するセキュリティ分野

セキュアな製品・サービスの提供

安全・安心の観点から「ベタープロダクツ・ベターサービス」をお客さまに提供するため、
NECグループでは、製品・サービスにおける高品質なセキュリティを確保するためのさまざまな活動に取り組んでいます。

1 ‖ セキュリティを考慮した開発・運用の推進

❶ 全社推進体制

お客さまに提供する製品、サービスに関してセキュアな開発・運用を実施するため、NECグループはセキュア開発・運用推進体制を構築しています。本推進体制は、NECの各組織やグループ会社の代表者からなる「セキュア開発・運用推進WG（ワーキンググループ）」と、各事業部門に配置したセキュア開発・運用推進者（約400名）で構成されます。WGでは、製品、サービスの脆弱性や設定ミス・システム不具合に起因する情報セキュリティ事故の撲滅に向けたセキュア開発・運用施策案の討議や施策進捗状況の共有などを行います。

本WGで決定されたセキュア開発・運用施策は、「セキュア開発・運用推進連絡会議」を通じて各部門の推進者に展開され、推進者が部門内へ施策の周知徹底、実施状況の点検、改善などを継続的に実施しています。

❷ 全社標準のフレームワークの整備

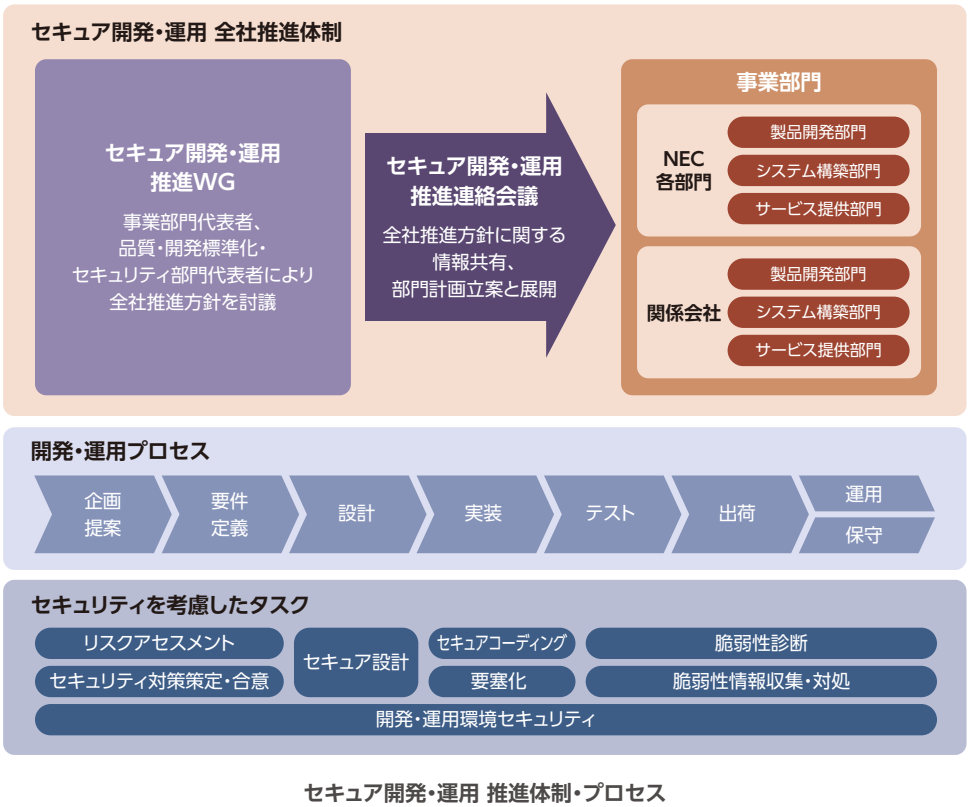
NECグループの全社標準である日本電気工業標準（NIS:NEC Corporation Industrial Standards）の1つとして、2014年に「セキュア開発・運用管理規程」を制定しました。本規程では、NECグループの各部門が実施すべきセキュア開発・運用に関する取り組み内容（部門内の推進体制構築、部門プロセス組み込み、セキュア開発・運用関連基準など）を定めています。

2015年には、巧妙化・高度化しているサイバー攻撃や内部不正によるセキュリティ事故の増加、制御機器・システムへの攻撃リスクの拡大を踏まえ、実施すべきセキュリティ対策の拡充（特権管理の強化など）を実施し、本規程を改定しました。

❸ セキュリティ品質の確保

製品、サービスのセキュリティ品質を確保するために、開発、運用の各フェーズにおけるセキュリティ確認項目を一覧した「セキュア開発・運用チェックリスト」を制定しています。本チェックリストでは、ISO/IEC15408などのセキュリティ国際標準、政府機関が定めるセキュリティ基準、業界ガイドラインなどの要件を考慮しており、さらに新たな脅威に対するセキュリティ対策を随時反映しています。具体的には、リスクアセスメント、セキュリティアーキテクチャ設計、セキュアコーディング、要塞化、脆弱性診断、セキュリティテスト、脆弱性情報収集対処、セキュリティ監視などのセキュリティ対策を定めています。本チェックリストは、NECグループの各組織の開発・運用標準に組み込まれており、各事業部門の開発・運用現場で活用されています。

さらに、各業務プロジェクトのセキュリティ対策状況を見える化し、対策が不十分な業務プロジェクトにセキュリティ対策を徹底させることを目的とした「セキュア開発・運用点検システム」を導入しています。本システムでは、約5,000のプロジェクトを管理しており、各業務プロジェクトで報告されたセキュリティ対策状況をセキュア開発・運用推進者が点検・監査し、問題プロジェクトへの改善などを行っています。



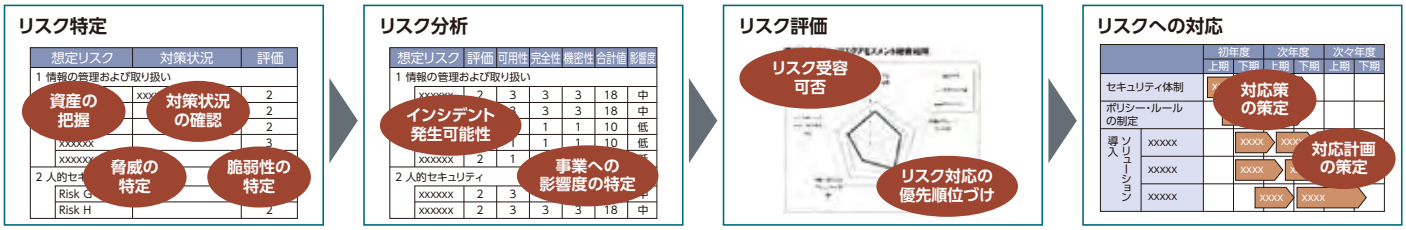
セキュア開発・運用 推進体制・プロセス

❹ リスクアセスメントを活用したセキュリティ強化

ICTは組織の活動効率化や収益性向上に必要不可欠なものとなっています。一方で、ICTに対するセキュリティ対策が不十分であることでインシデントが発生した場合、ビジネスに深刻な影響を与える可能性があります。経済産業省およびIPA*1が発行した「サイバーセキュリティ経営ガイドライン」においても、サイバーセキュリティは経営課題であると指摘されています。また、事業継続やサイバー攻撃への対策によって生まれる企業価値を確保するために、必要なセキュリティ投資についての経営判断が求められています。組織は、システムのリスクを適切に把握し、最適なセキュリティ対策を確実に講じておくことで、重大なインシデントの発生を防ぐことができます。そこで、NECグループでは、システムのリスクを早期に見える化し、可能な限り低減させるために、セキュリティに関するリスクアセスメントの実施に取り組んでいます。

リスクアセスメントとは、情報システムの運用により生じる業務、資産などに対するリスクを特定、評価し、リスク対策の優先順位をつけるプロセスです。例えば、リスクアセスメントをお客さまシステムの企画、提案段階で行うことで、費用対効果が高いセキュリティ対策を選定でき、コストと安全性のバランスを保つことができます。また、オンプレミス、クラウドサービス、仮想化などの環境の違いによって発生するリスクや、内部犯行や標的型攻撃などの新たな脅威がもたらすリスクも考えられます。これらを特定し、影響度の評価を行うことで、さまざまな要因で異なるリスクへも対応しています。

*1 IPA: 独立行政法人情報処理推進機構



リスクアセスメントの概要

2 ‖ 日々発生する脆弱性への迅速な対応

❶ 脆弱性情報共有の体制

NECグループでは、日々発見される新たな脆弱性情報に漏れなく迅速に対処するため、独自の脆弱性情報管理システムを運用し、約600名の推進体制を通じてグループ全体で脆弱性情報を共有しています。また、脆弱性対策の実施を品質確保の全社ルールに盛り込むことで、このシステムの利用徹底をはかっています。

自社製品についてはIPAやJPCERT/CC*2と連携して脆弱性情報や対策パッチなどを迅速にNECグループ内公開する管理体制を構築しています。この体制では、出荷後の製品に脆弱性が発見された場合、製品開発部門へ速やかに通知され、対策パッチが公開されるまで、NECグループ内で状況をフォローアップします。

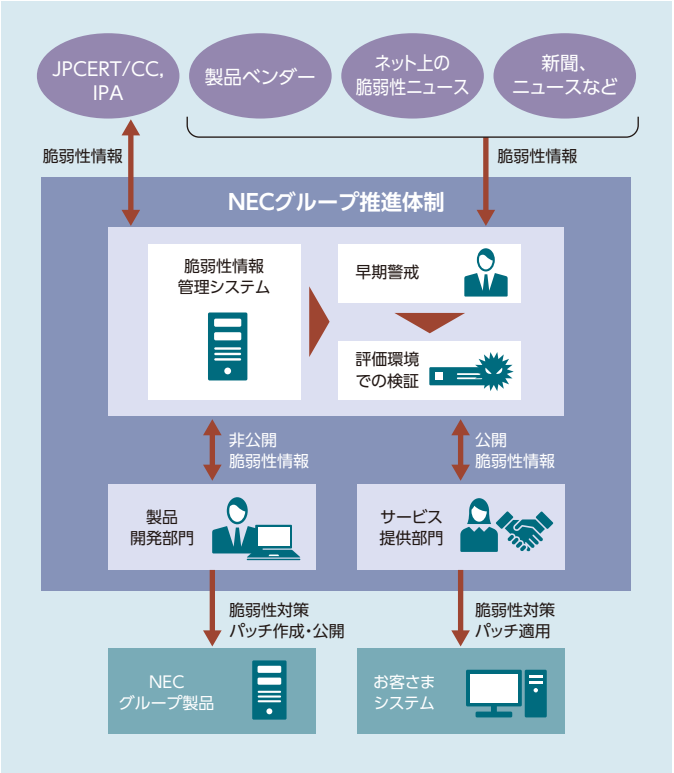
開発部門やサービス提供部門は、脆弱性情報管理システムから脆弱性の原因や対策方法などの詳細情報を入手し、自社製品やお客さまシステムの脆弱性に対策を行う運用となっています。さらに対策状況をプロジェクトごとに管理し、対策が未実施の場合は警告することで漏れのない確実な脆弱性対策を実現しています。

*2 JPCERT/CC: Japan Computer Emergency Response Team Coordination Center

❷ 脆弱性情報の収集と検証に関する取り組み

サイバー攻撃に対しては、いち早く脆弱性情報をキャッチし、対策の準備をすることが重要です。NECグループでは、お客さまのシステムで利用されている製品・技術の脆弱性情報を日々収集・監視しています。特に影響範囲が広く危険度の高い脆弱性情報を素早く共有するための仕組みとして、早期警戒体制を構築しています。

脆弱性を悪用した攻撃ツールがインターネット上に公開されると攻撃を受ける危険性が高くなります。これらの脆弱性については、各業務プロジェクトで確実に対処ができる体制を構築しています。具体的には公開されている修正パッチや回避策の情報共有だけではなく、NECグループ内部の評価環境に対して疑似的に攻撃を行い、修正パッチや回避策適用前後の動作や影響を検証します。その検証結果をNECグループ内で情報共有することで、各業務プロジェクトで脆弱性対策を確実に実施しています。



脆弱性対応推進体制

維持・向上を目指すセキュリティ分野

情報セキュリティマネジメント

情報セキュリティの各種施策をグループ全体に展開し確実に定着化させるため、
情報セキュリティマネジメントの体系を確立し、PDCAサイクルにより情報セキュリティの維持・向上をはかっています。

1 ‖ 情報セキュリティマネジメントの体系

NECグループは、情報セキュリティや個人情報保護のポリシーに基づき、継続的にPDCAサイクルを回し情報セキュリティの維持・向上をはかっています。情報セキュリティ点検／監査の結果や情報セキュリティ事故の状況などに基づき、情報セキュリティ対策の実施状況の把握・改善、ポリシーの見直しをしています。また、第三者認証で要求される管理水準を考慮し、ISMS認証やプライバシーマークの取得・維持も推進しています。

NEC グループ情報セキュリティマネジメント

2 ‖ 情報セキュリティに関するポリシー

NECグループでは、国内・海外のグループ会社の共通ポリシーとして「NECグループ経営ポリシー」が展開されており、情報セキュリティや個人情報保護のポリシーが含まれています。情報セキュリティや個人情報保護は、これまでも事業遂行上の重要事項として管理の強化に取り組んできました。

情報セキュリティについては、「情報セキュリティ基本方針」を公開し、基本方針を実現するための規則や基準として、情報セキュリティ基本規程、情報管理に関する規程（企業秘密管理規程、個人情報保護規程、特定個人情報保護規程、技術文書管理規程）、ITセキュリティに関する規程などを整備し体系化しています。

個人情報保護については、「NEC個人情報保護方針」を制定後、2005年にNECがプライバシーマークを取得し、日本工業規格「個人情報保護マネジメントシステム要求事項（JISQ15001）」および「個人情報保護法」に準拠したマネジメントシステムを確立しています。また、2015年には、「番号法」に準拠したマイナンバーの管理を同マネジメントシステムに追加しました。

個人情報は、グループ共通の保護管理レベルで運用するよう推進しており、28社（2016年6月末現在）がプライバシーマークを取得しています。

NEC グループ経営ポリシー

3 ‖ 情報セキュリティリスク管理

情報セキュリティマネジメントが有効に機能するためには、情報セキュリティのリスクを適切に評価し、管理する必要があります。

❶ 情報セキュリティのリスク評価

NECグループでは、ベースライン基準との差異を分析する手法と詳細リスクを分析する手法を使い分けてリスク評価と対策の実施を行っています。基本的には、共通に実施すべき水準として定められた「情報セキュリティ対策基準（ベースライン）」により、セキュリティを維持しています。高度な管理を必要とする場合は、「情報セキュリティリスク評価基準」に基づいた詳細リスク分析を行い、きめ細かな対策を実施します。

❷ 情報セキュリティ事故のリスク管理

一方、情報セキュリティ事故の報告を義務付け、その内容を分析することで、PDCAサイクルを回す際のインプットとし、情報セキュリティのリスクを管理しています。事故情報はグループで標準化したルールで一元的に管理されており、件数の変化、組織別（NEC、グループ会社、お取引先）の傾向、事故の類型別の傾向などを分析し、共通施策に反映するとともに、効果測定やKPIとしてリスク管理しています。

また、情報セキュリティ事故の真の原因を追究するために、「なぜなぜなぜ分析」を実施しています。分析手法を確立し、当該部門が自身で分析を行える体制を整備しています。重大な事故は、専門のアドバイザーが参加・分析するとともに、対応費用や影響度を数値化することで、インパクト分析も行っています。結果は経営層に報告し、全社への横展開、全社施策への反映などにより、効果を上げています。

4 ‖ 情報セキュリティ点検

NECグループでは、情報セキュリティ対策の実施状況を確認し、実施が不十分な対策の改善計画を立案、実行する活動として、国内・海外のグループ会社を対象に、情報セキュリティ点検を毎年継続して実施しています。

❶ 情報セキュリティ点検の内容

情報セキュリティ事故を分析の上、主として情報漏えい事故を撲滅するための項目を重点項目に設定しています。また、点検は、実施状況のチェックだけでなく、実施できていない場合の理由を回答する形式にし、是正対応に役立てる形にしています。

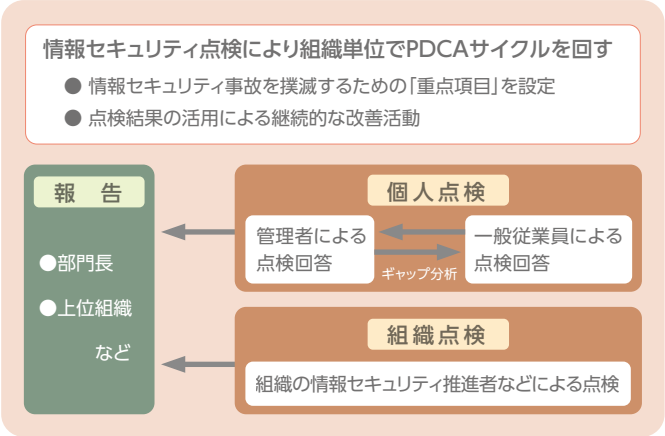
具体的には、外部記憶媒体の安全管理、社外への持ち出し管理、秘密情報や個人情報の安全管理、外部委託先（お取引先）管理、メール誤送信防止、標的型攻撃メール対策、セキュア開発・運用などの項目の確実な徹底をはかっています。

❷ 情報セキュリティ点検の方式

情報セキュリティ点検の方式は、各組織の情報セキュリティ推進者などが組織全体の状況をチェックする「組織点検」と、個人個人が対策の実施状況を回答する「個人点検」があります。従来、組織点検を中心に実施していましたが、現場の実態をきめ細かく把握し、より有効性の高い改善をはかるため、現在では一部の海外現地法人を除き、個人点検を実施しています。また、個人点検では、一般従業員と管理者を対象に実行面と管理面の点検を実施しており、両者のギャップを分析することで、管理側の問題を発見できるようにするなどの精度の向上をはかっています。

❸ 点検結果の活用による改善

点検の結果、実施が不十分な項目については、各組織において理由の把握および改善計画の立案を行い、組織的に問題解決に取り組んでいます。また、残課題の解決やさらなる強化が必要な内容は、次年度の情報セキュリティ推進計画へ反映することで、継続的な改善の取り組みを行っています。



情報セキュリティ点検（個人点検／組織点検）

5 ‖ 情報セキュリティ監査

NECの経営監査本部が中心となって、情報セキュリティマネジメントやプライバシーマークの監査を実施しています。監査の基準としては、ISO/IEC27001やJISQ15001に照らし、各組織の情報セキュリティマネジメントの状況を監査しています。NECグループでは、定期的に、経営監査本部による徹底した内部監査を受ける制度を確立しています。

6 ‖ ISMS認証取得の取り組み

NECグループは、ISMSの認証取得が必要な組織を対象に、ISMSの規格として必要な部分を確実に満たせるように設計された「標準コンテンツ」を核に、コンサルテーション、監査体制構築、教育、効率的な審査対応（差分審査など）のサービスを「NetSociety for ISMS」サービスとして提供しています。なお、このサービスは、NECグループやお取引先において、多数の組織が利用してきた実績があります。

維持・向上を目指すセキュリティ分野

情報セキュリティ基盤

NECグループでは、お客さま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。

1 ‖ 情報セキュリティ基盤の特長と構成

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、補完しあいながら、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。

2 ‖ 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電子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。

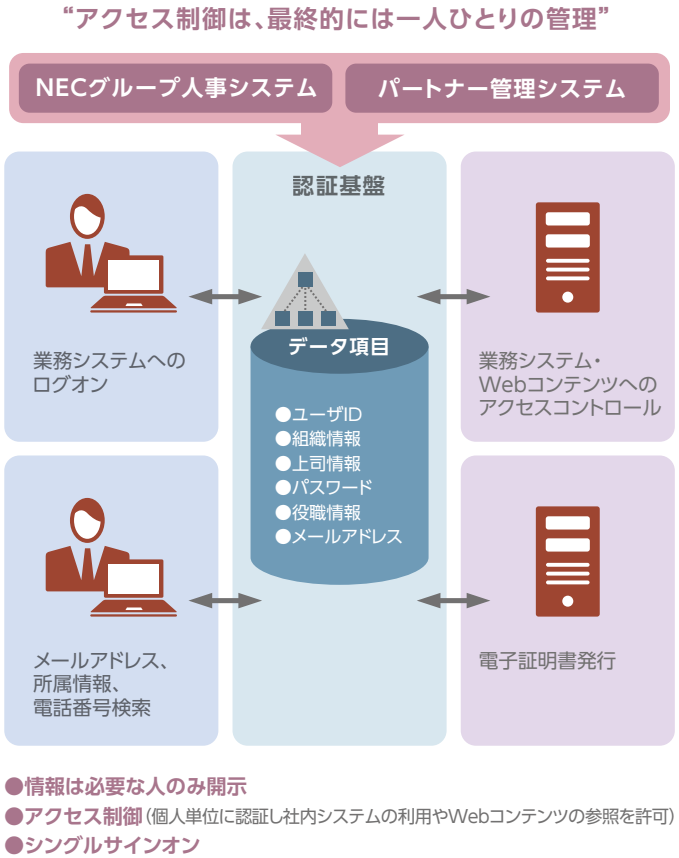
❶ NECグループ認証基盤

情報資産にアクセスするためには、利用者の特定、認証とその利用者に応じた権限の付与が重要です。そこでNECグループでは、社員だけでなく業務上の必要性に応じてお取引先なども対象として、認証、権限付与(認可)に用いる情報を一元管理した認証基盤を構築しています。

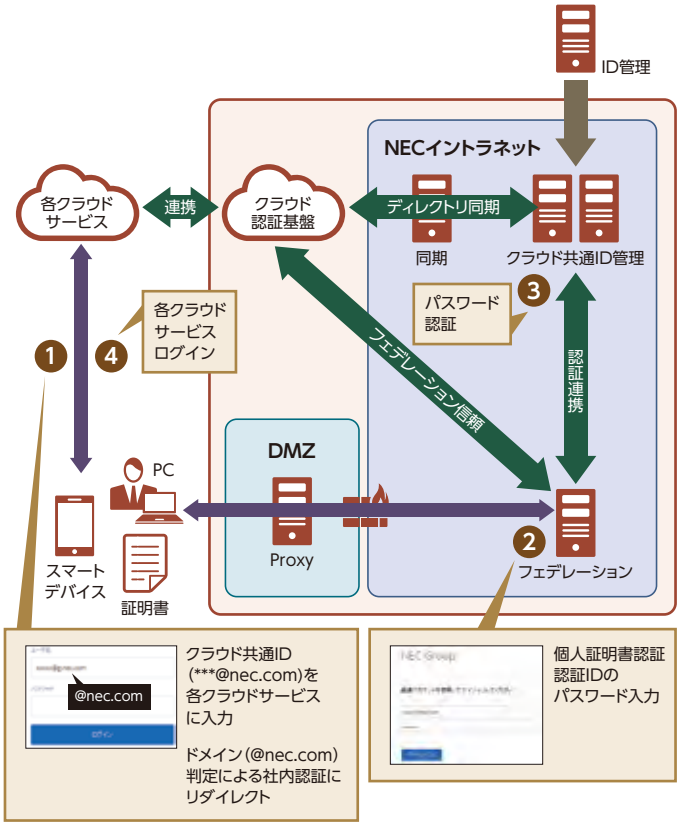
認証、認可に用いる情報は、ユーザID、パスワードに加え、組織情報、役職情報などのアクセス制御情報があります。これらを利用し、業務システムなどへのアクセスを個人単位で制御しています。また、NECグループ各社が管理している認証、認可に用いる情報がどこのシステムでどのような目的で利用されているのかを一元的に管理しています。さらにICカード認証によってプリンタへの(紙)出力も制御しています。

❷ 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。



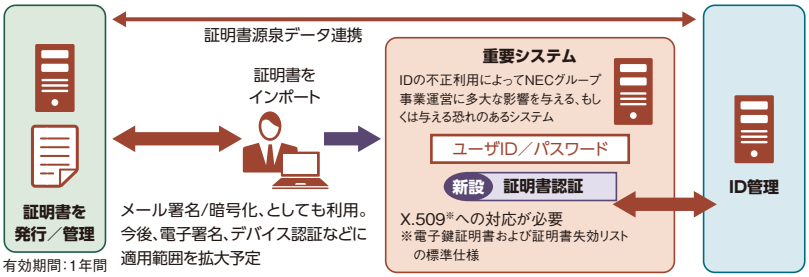
NEC グループ認証基盤



クラウド認証連携

❸ 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ログインには、ユーザID、パスワード（記憶認証）だけでなく、電子証明書を利用した認証（所有物認証）を導入しています。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。



多要素認証

3 ‖ 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多層的な対策が必要となってきており、セキュリティ更新プログラムやウイルス対策ソフトを確実に適用することが重要です。

❶ ウイルス、ワームからPCを守る

【ユーザ利用環境支援】

NECイントラネットでは、PCおよ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、すべてのPCに、必要なセキュリティ対策ソフトが確実にインストールされるようにしています。また、セキュリティパッチの配付やウイルス対策ソフトの定義ファイルの更新を自動化し、確実に適用する仕組みも導入しています。さらに使用を禁止するソフトウェアを定義しており、ユーザのソフトウェアの適正利用状況についても監視しています。

【ネットワーク管理】

PCの状態を見える化するとともに、NECイントラネット上に侵入検知の仕組みを設けており、セキュリティ対策が不十分なPCがイントラネットに接続されたり、イントラネット上でワームが検知されたりした場合、該当するPCやLANをイントラネットから遮断するよう制御しています。また、NECグループ外への通信は、アクセス禁止カテゴリによるWebアクセスフィルタリング、フリーメール対策、SPF認証（送信ドメイン認証）などを実施しています。

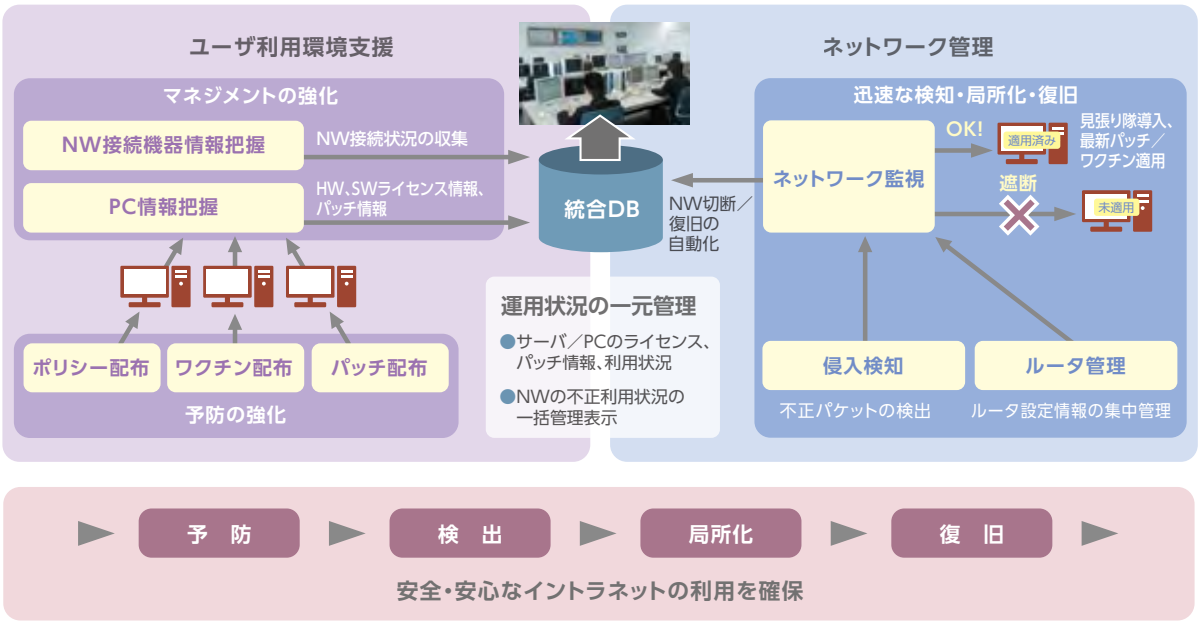
【適用状況の一元管理】

修正プログラムの適用やウイルス対策ソフトなど、セキュリティ対策の実施状況に関するデータは管理システムに集められ、情報セキュリティの管理責任者や推進者が自部門の対応状況をタイムリーに把握できる仕組みになっています。これにより、各種施策の円滑な推進と徹底を容易にしています。

❷ 脆弱性検査ツールによるチェック

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ています。

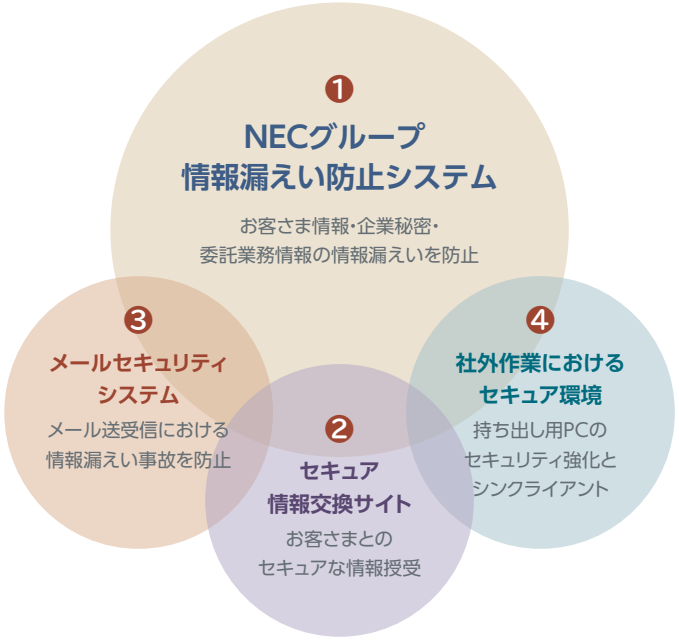
発見された脆弱性は、システムにより一元管理されており、各部門の管理者は自部門の状況を閲覧して、発見された脆弱性を指示された修正方法に基づき是正します。これらの是正状況についてもシステムで一元管理しており、NECグループ全体の対応状況をフォローできるようにしています。



ウイルス、ワームから PC、ネットワークを守る

4 ‖ 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上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、お客さま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・電子媒体などのITの特徴やリスクを考慮し、情報流出につながる経路に対して網羅的かつ多層的な対策を行っています。



情報を守るIT基盤の全体像

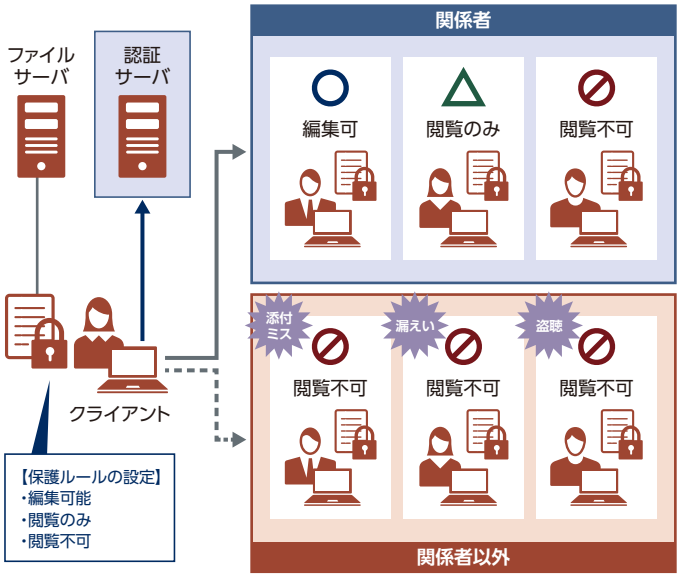
❶ NECグループ 情報漏えい防止システム

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」、「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。

「暗号化」は、PCハードディスクおよびファイルの暗号化を行い、盗難・紛失による情報漏えいを防止しています。特に、InfoCage FileShellを導入し、PC上にあるすべてのファイル（動作上問題があるシステム関連のファイルなどを除く）を暗号化しています。

ファイル暗号では、アクセス権、利用期限などを設定でき、最低限のセキュリティレベルとして、NECグループ標準（NECグループ外の人は閲覧不可）を設定しています。そのため個人情報流出事案にみられるように、マルウェアに感染して外部に情報が送られたり、メールなどで情報を誤って送信したとしても、情報が漏えいしないようにしています。

昨今は、大手通信教育機関における大規模な情報漏えい事件にもみられるように、内部不正による情報漏えいにも対応することが求められています。



InfoCage FileShellによるファイル暗号と利用制限

情報漏えい防止システムでは、「デバイス利用制御」を行っています。例えば、USBメモリ、SDカード、CD、DVDなどの外部記憶媒体や、スマートフォン、Bluetooth、赤外線などの通信デバイスに対して、情報の書き出しをすべて禁止するなどの利用制限を設定し、NECグループのポリシーとして配付し、制御しています。

なお、業務上、デバイスを使用せざるを得ない場合に対応するために、組織ごとに利用制限をカスタマイズできる仕組みを用意しています。組織や利用者ごとに利用可能なデバイスや利用制限を定義して、組織として必要最小限の利用だけを行うようコントロールしています。

また、「デバイス制限」に加えて、「ログの記録・監視」による管理も行っています。従業員などのPCの操作ログをすべて記録しており、会社が許可していない外部媒体への書き出しや大量な情報の入手などの不正を検知し、是正指導を行っています。

情報漏えい防止システム概要

万一情報漏えいの事故などが発生した際は、このログを分析することにより、事故の影響範囲の特定や状況把握などの事故分析や、再発防止策の策定などにも大きな効果を発揮しています。

NECグループでは、さまざまな種別・ソースのログを収集・蓄積・分析する「ログ監視システム」（データの収集・集約、蓄積、分析、可視化など）を導入するなど、異常行動を検知し、内部不正や外部脅威の兆候をいち早く発見できるよう、インフラの高度化を進めています。

また、内部不正による情報漏えいなどを防止するために、事故が発生した場合の事業上の影響度合いを考慮して、重点的に管理すべきNECグループ内のシステムを定め、対策しています。具体的には、①脆弱性情報収集・対処、②ログ管理、③ネットワーク保護、④認証、⑤アクセス制御、⑥特権管理、⑦セキュア運用・保守手順、⑧運用・保守作業チェック、⑨セキュリティ設定、⑩入退室管理、⑪委託先管理などを実施しています。

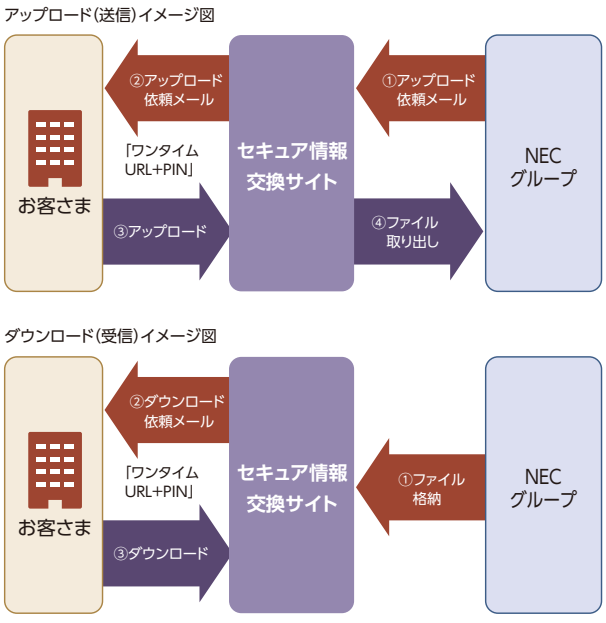
❷ セキュア情報交換サイト

NECグループでは、お客さま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ます。このエリアにアクセスするためにはワンタイムURLとパスワードが必要です。

ワンタイムURLには有効期間があり、期限が過ぎるとこのURLは無効になります。また、1回のみの使用に限定されるため、情報が取得されるとセキュア情報交換サイト上からこの情報が削除されます。

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。



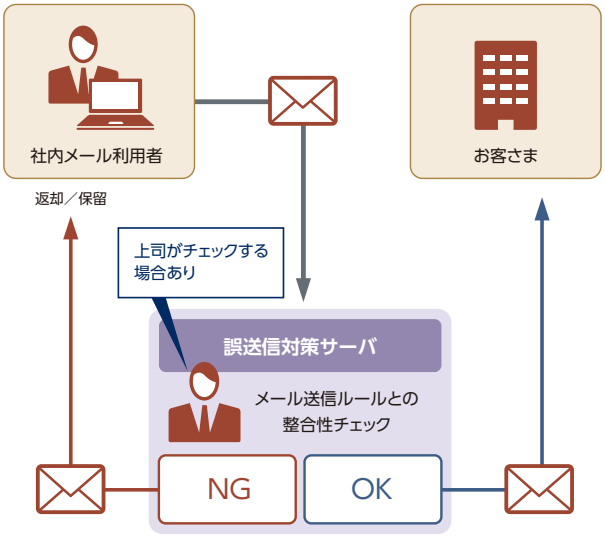
セキュア情報交換サイト

❸ メールセキュリティシステム

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を防いでいます。メールアドレスなどのチェックを上司などの第三者が行える機能も備えており、故意にメールを転送して情報を漏えいさせることも防止しています。

ほか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を持つOMCA*1をNECグループ内に展開し、メールセキュリティの向上をはかっています。

*1 OMCA：Outlook Mail Check Addln



メール誤送信防止システム

❹ 社外作業におけるセキュア環境

NECグループでは、情報セキュリティ事故を低減させるため、社外でのセキュアな業務環境を構築しており、多数のグループ社員が活用しています。

PCを社外に持ち出して利用する場合、社内での利用と比較すると脅威が増大します。

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」、「OS起動前のプリブート認証機能」、「遠隔からのデータ消去、PCのロック機能」、「未知の脆弱性に対する攻撃を緩和する機能」や「オートランウイルス対策機能」などを搭載しており、昨今の高度化するサイバー攻撃に備えています。

維持・向上を目指すセキュリティ分野

情報セキュリティ人材

NECグループは、一人ひとりの情報セキュリティの意識の向上をはかるとともに、
セキュリティ推進のスキル向上やセキュリティプロフェッショナルを育成する各種施策を行い、
情報セキュリティの人材を確保しています。

1 ‖ 情報セキュリティ人材の育成

NECグループでは、情報セキュリティ人材を確保するために、全社員を対象とした「情報セキュリティの知識、意識の向上」、「情報セキュリティの施策を推進する人材の育成」、お客さまに価値を提供できる「プロフェッショナルな人材の育成」の3つの観点で施策を推進しています。

2 ‖ 情報セキュリティの知識、意識の向上

情報セキュリティの維持、向上をはかるためには、情報を適切に取り扱うための知識や情報セキュリティに対する高い意識が重要であり、そのための教育や啓発を行っています。

❶ 情報セキュリティ、個人情報保護教育

NECグループの全社員を対象に、情報セキュリティと個人情報保護（マイナンバー対応を含む）に関するWBT（Web Based Training）教育を実施し、情報セキュリティの知識やスキルの向上をはかっています。教育内容は、セキュリティ脅威のトレンドなどを考慮し、毎年見直しを行っております。具体的には、新しい脅威への対応や意識啓発、情報の取り扱い、内部不正防止、委託先管理、およびセキュア開発・運用などの施策内容の確認と理解を目指しています。

❷ 情報セキュリティの遵守事項への誓約

NECグループでは、お客さま情報、個人情報（マイナンバーを含む）、企業秘密を扱う際に、最低限遵守すべき事項として「お客様対応作業及び企業秘密取り扱いの遵守事項」を定めています。遵守事項の内容を理解し、確実に実行してもらうため、NECグループ全社員から誓約を取得しています。誓約は、「電子誓約システム」を運用することで効率的な管理と徹底をはかっています。

❸ 情報セキュリティの意識啓発活動

情報セキュリティリスクに対する危機感を高め、自ら考え判断して行動できるようになるために、紛失事故や開発・運用時の事故など、主に人の行動に起因するヒヤリハットを題材にしたビデオを活用して意識啓発活動を実施しています。各組織に適した方法（①職場懇談会、②なぜなぜなぜ分析、③ビデオ視聴会など、対話による気づき、分析力・判断力の向上につながる手法）で効果的に実施しています。

3 ‖ 情報セキュリティの施策を推進する人材の育成

NECグループでは、情報セキュリティ推進体制を構築し、各種施策を展開しています。推進者は施策展開に重要な役割を担うため、施策展開に必要なスキルを持った推進者を養成しています。

❶ 情報セキュリティ推進者の育成

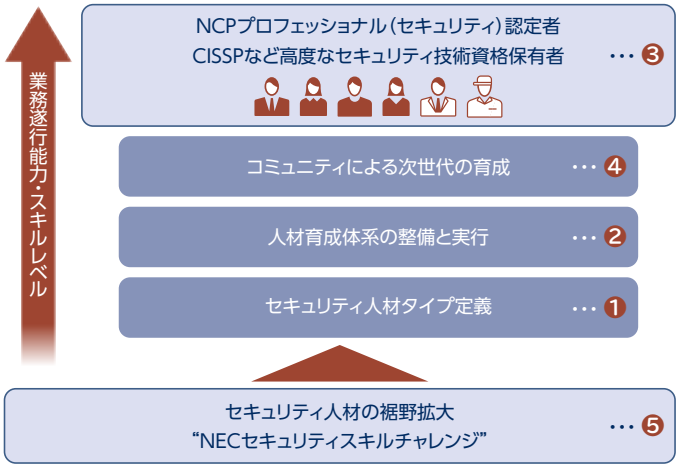
各組織の推進者が情報セキュリティ対策を推進する上で必要な知識（管理体制、役割、セキュリティ施策、推進内容など）を修得する研修を開催しています。また、各組織で異なるリスクをマネジメントするスキルを向上させるため、事故を題材にした映像を使った演習型の研修なども開催し、実践力を養うとともに、リスク管理や「自律考動」を促進しています。

❷ 監査人育成

NECグループでは、お取引先の情報セキュリティの維持・向上のために、お取引先に対する情報セキュリティの監査（訪問点検）を行っています。標準化された監査手法で点検を行えるような育成スキームを確立し、監査のできる人材を育成しています。

4 ‖ プロフェッショナルな人材の育成

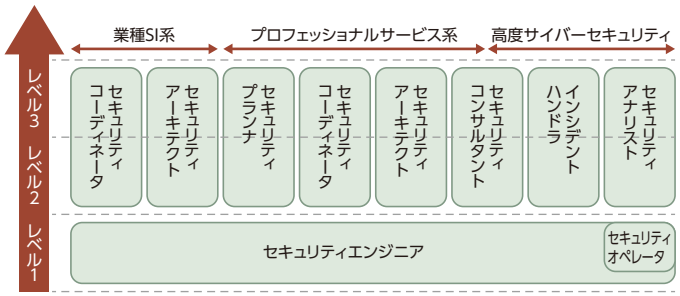
サイバーセキュリティ事業の拡大や製品・システム・サービスのセキュリティ対応力を高め、さまざまな領域においてお客さまに貢献するため、セキュリティ人材の育成に力を入れています。



プロフェッショナル人材育成

❶ セキュリティ人材タイプの定義

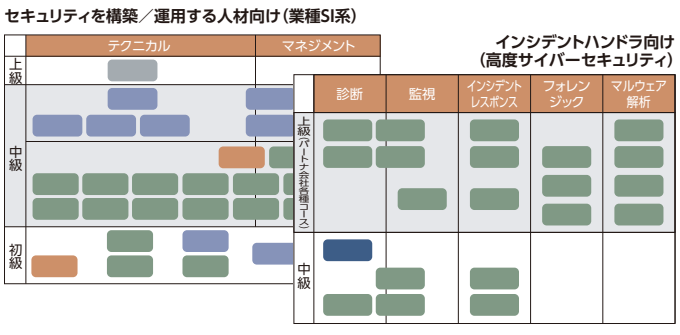
NECグループとして必要なセキュリティ人材を定義し、人材タイプごとの育成をはかっています。お客さまに必要なセキュリティ人材定義とも連動し、さらなるブラッシュアップを継続しています。



セキュリティ人材タイプ

❷ 人材育成体系の整備と実行

サイバーディフェンス研究所などのNECグループおよび、パートナー企業と連携し、人材タイプの定義ごとに研修を最適化しています。整備した研修はお客さまも順次受講できるように整備しております。



研修コース

❸ トップ人材を維持する認定制度と高い処遇

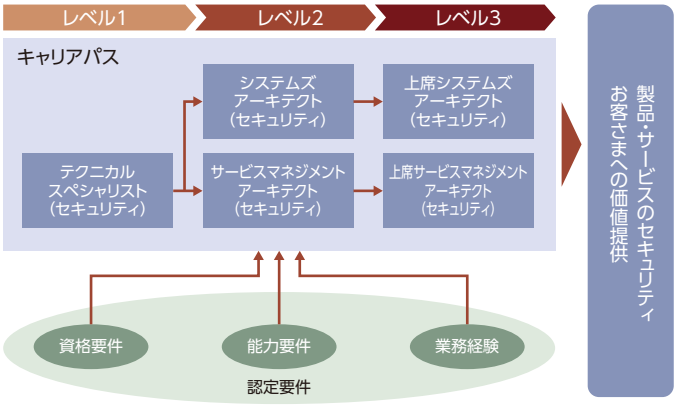
プロフェッショナル認定制度（NCP認定制度）を設け、高度なセキュリティ専門性を有する人材を認定し、市場価値とリンクした高い処遇を与えています。

NCP上席プロフェッショナル報酬体系

また、セキュリティ公的資格の取得を強く推奨しており、国際資格であるCISSP*1や情報処理技術者試験（情報セキュリティスペシャリスト）、今後新設される「情報処理安全確保支援士」の取得者を拡充しています。

情報セキュリティに関する高度なスキル、業務経験、資格を有している者が核となり、お客さまへの最適なソリューションの提供に貢献します。

*1 CISSP Certified Information Systems Security Professional



- システムズアーキテクト（セキュリティ）：情報システムのセキュリティ品質を保証
  ・脅威／脆弱性分析、セキュリティ要件定義／アーキテクチャ設計など
- サービスマネジメントアーキテクト（セキュリティ）：ITサービス運用のセキュリティ品質を保証
  ・セキュリティマネジメント、モニタリング、インシデント対応など

プロフェッショナル認定制度（セキュリティ）

❹ コミュニティによる次世代の育成

お客さまからの期待に応えながら、NECグループのサイバーセキュリティ事業を拡大するためには、次世代のプロフェッショナル人材を組織的・継続的に育成していくことが必要です。NECグループでは既に300人以上のプロフェッショナル人材によるコミュニティが形成されており、インテリジェンスの共有や技術の検討などの勉強会を定期開催するなど、次世代のプロ育成をフォローしています。

❺ 全社的CTFの実施

NECグループの全社員を対象に、社内CTF（Capture the Flag）である「NECセキュリティスキルチャレンジ」を開催しています。2015年度は約600名が競技に参加し、2週間かけて100問の問題に取り組みました。参加者にはセキュリティ業務の非従事者が半数程度おり、セキュリティ人材の裾野拡大につながっています。

お客さまに提供するサイバーセキュリティ

NECのサイバーセキュリティ戦略

サイバー攻撃は国内だけにとどまらずグローバルで社会問題化しています。
NECはグループの総力をあげてサイバー空間に、安全・安心で快適な環境を提供することで
人と地球にやさしい情報社会の実現に貢献します。

1 ‖ 基本方針

NECグループは、1977年10月に「変化する社会ニーズへの通信企業の対応」と題する基調講演の中で、「コンピュータと通信の融合」という構想を実現すべくC&C（Computer&Communication）を宣言しました。その宣言に沿って世界中のコンピュータをつなぎ、人とモノ、モノとモノをつなぐことで、多くの社会ニーズに応え社会の発展に貢献してまいりました。

NECグループは国内の交通管制をはじめ、消防・防災システム、生産管理から水管理、ATM、物流システム、さらには海底・宇宙まで、社会にとって必要不可欠な基盤を支えてきた多くの技術を蓄積・活用することで、フィジカルとサイバーを融合したトータルセキュリティを世界に展開しています。

これから、IoT*1（モノのインターネット）の登場によって、自動車やスマートメーターといったモノがサイバー空間につながり、私たちの生活はますます便利で快適になる一方で、サイバー攻撃の脅威はグローバルで社会問題化し、サイバー空間からの攻撃が現実世界に影響を及ぼすサイバーフィジカルアタックの問題が深刻化しつつあります。

サイバーセキュリティの在り方も従来の防御・検知だけでなくビッグデータ、SDN*2、クラウドを活用した、予知予測、防御の自動化といった新しいセキュリティ技術の研究開発が進んでいます。

その中には、インテリジェンス（学習情報）を活用した判断を支援する仕組みや、AI技術（人工知能）を活用し異常検知からシステム切り離しの判断と対処を自動化し被害を局所化するシステムの実用化を推進しています。

また、フィジカルにおいてもセンサ機器の信号情報を解析し、「故障予測の実現」、「監視カメラ画像情報から人の行動を解析し迷子を捜すソリューション」、「盗難にあった自動車や物の追跡」などさまざまな分野でサイバー空間を活用した実証実験を進めています。

NECグループは、これからも世界中でフィジカルとサイバーの融合を進め、セキュアなサイバー空間を作り上げ、明るく希望に満ちた暮らしと社会を実現し、より良い未来につなげていきます。

*1 IoT: Internet of Things
*2 SDN: Software-Defined Networking

社会基盤を支えるNECの事業領域

2 ‖ サイバーセキュリティへの投資

❶ 人材と技術

NECのサイバーセキュリティ事業を支えるエンジンは人材・技術・情報です。NECは国内だけにとどまらず、グローバルで継続的に投資をしています。2013年サイバーディフェンス研究所、2014年株式会社インフォセックをグループに迎え、シンガポール政府・経済開発庁と戦略的出向・研修(STRAT)プログラムの研修生受け入れ契約を締結、また、実践的サイバー防御演習(CYDER*3)、外部機関のセキュリティコンテストCTF*4に参画、北陸先端科学技術大学院大学校に寄付講座を開設し人材の育成を積極的に行うことで、日本のセキュリティ人材基盤の強化に貢献しています。

*3 CYDER: Cyber Defense Exercise with Recurrence
*4 CTF: Capture the Flag

人材基盤強化

	サイバーディフェンス研究所　グループ会社化 先進の技術・知見を持つトップ人材を強化	(2013年3月)
Infosec	**株式会社インフォセック　グループ会社化** セキュリティ監視に強いノウハウ、監視業務を強化	(2014年2月)
	**シンガポール政府との共同人材開発** 国際的に不足するサイバーセキュリティ専門家の育成	(2014年9月)
	**実践的サイバー防御演習　CYDER** 総務省「サイバー攻撃解析・防御モデル実践演習の実証実験」プロジェクトを2013年度から受託。NECが演習プログラムを作成・運用	(2014年10月)
JAIST	**北陸先端科学技術大学院大学　寄付講座開講** 講座名:サイバーレンジ構成学:サイバーセキュリティ領域の人材育成	(2014年11月)

2015年に経済産業省およびIPA*5から大企業および中小企業を対象にした、「サイバーセキュリティ経営ガイドライン」が公開され、多くのお客さまでサイバーセキュリティ対策が進められています。

しかし、その一方でサイバーセキュリティ人材の不足が大きな課題となっており、NECは多くのお客さま、お取引先、関係機関と連携し、人材の育成に力を入れています。

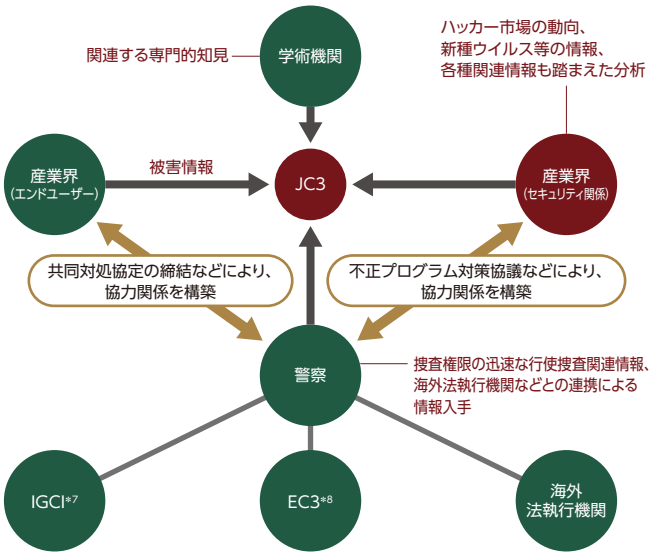
NECグループが提供する教育プログラムには、標的型攻撃メール訓練をはじめさまざまなプログラムがあります。その中でもサイバー攻撃演習プログラムは、情報システム部のセキュリティ担当として、インシデントの発見、報告、問題箇所の特定、隔離、分析、解析、被害状況の確認など、インシデントハンドリングの一連の流れを実際に体験しながら学習します。体験することで、お客さまの技術力の向上や、お客さま事業を支えるICT基盤のサイバーセキュリティ対策の充足度を確認する気付きの場となることを期待しています。

このプログラムは、CSIRT*6の方々にご利用いただく機会が増えており、国内のお客さまだけでなくグローバルで広く活用されています。

*5 IPA:独立行政法人情報処理推進機構
*6 CSIRT: Computer Security Incident Response Team

❷ 情報基盤の強化

増加するサイバー犯罪に対する情報基盤を強化するために、国内外の関連組織と連携しています。制御システムセキュリティセンターへの参画をはじめ、2015年には日本サイバー犯罪対策センター(JC3)に参画し、国内の学術研究機関、産業界、法執行機関の官民産学連携を推進、サイバー犯罪への対応を進め、それらの活動で得た成果を社会に還元させることで安全・安心で快適な環境づくりに貢献しています。



*7 IGCI: The INTERPOL Global Complex for Innovation　*8 EC3: European Cybercrime Centre

日本サイバー犯罪対策センターを中心とした枠組み

2012年、NECはインターポール(国際刑事警察機構)とグローバルなサイバーセキュリティ対策で提携しました。この提携は、インターポールの国際的なネットワークとNECの最先端サイバーセキュリティソリューションにより、複雑で高度化するサイバー犯罪などを調査・分析し、国際レベルでのサイバーセキュリティ強化を目指すものです。また2015年には、インターポールがシンガポールに開設した「The INTERPOL Global Complex for Innovation」の中に設置された「インターポール・デジタル犯罪捜査支援センター」に中核システムも提供しています。

オペレーションセンター(Cyber Fusion Centre)

3 ‖ グローバルへの展開

❶ 世界のサイバーセキュリティ動向

サイバー攻撃の脅威は国内だけにとどまらずグローバルで社会問題になっており、サイバーセキュリティへの関心は年々高まりを見せています。NECは、サイバー攻撃やサイバー空間を利用したサイバー犯罪に関し、法令、政策、組織論から最新の技術動向に至る多くの国際会議・カンファレンス、フォーラムに参加し、グローバルレベルで最新の取り組みについて協議を行っています。2016年もこの流れは変わらず、グローバルトレンドのキーワードとしてIoTセキュリティをはじめ、インターネットガバナンス、情報共有フレームワーク、開発途上国への技術支援といった多くのテーマについて議論の活発化が予想されます。

日本でも、2014年のサイバーセキュリティ基本法をはじめ、2015年にはマイナンバー制度（社会保障・税など）が施行され、サイバーセキュリティの重要性は増しており、テロ、サイバー攻撃への対策が急務とされております。

❷ グローバルセーフティ

NECは、これまで国内の重要な社会基盤を支え、安全・安心で快適な環境を提供してきました。今後も、これまで培ってきた人材、高い技術力を活かし、世界最高精度を誇る指紋認証、顔認証、国民ID管理システム、決済ネットワークといった、フィジカルとサイバーの両面でトータルセキュリティを提供してまいります。既に、アメリカをはじめとし、南アフリカ、ブラジル、アジア諸国を中心に展開し、APAC（Asia Pacific）では、セキュリティコンサル、MSS*8提供ベンダーとして、NECのプレゼンスは年々高まっています。NECグループは、世界中のお客さまの期待に応えるべく、2016年1月にシンガポールにサイバーセキュリティの拠点を立ち上げ、セキュリティソリューションのグローバル展開は、今後もますます加速していきます。

*8 MSS: Managed Security Service

シンガポールにグローバルセーフティ事業部を設置、グローバル事業遂行体制を確立

- シンガポール、アルゼンチン他、リージョナルコンピテンスセンターおよび各国のセーフティチームメンバー総勢500名で事業を遂行
- シンガポールに5拠点目となる研究所を設立、セーフティ事業における研究開発に注力
- 日本、シンガポール、豪州、ブラジルにSOCを配置、グローバルカバレッジを順次拡大

世界に展開するグローバルセーフティ

4 ‖ セキュリティオペレーションセンターのグローバル化

NECグループは、サイバー攻撃の脅威から国内のさまざまな重要インフラや多くのお客さまのICT基盤を守るべく、グループの総力をあげてセキュリティオペレーションセンターの展開を推進してきました。

国内の複数あるセキュリティオペレーションセンターの中でも、サイバー攻撃の脅威に対応するための中核拠点として2014年に日本にサイバーセキュリティ・ファクトリーを開設しました。2016年1月に新設したシンガポールのサイバーセキュリティ・ファクトリーは、日本のサイバーセキュリティ・ファクトリーと協働し、サイバー攻撃の脅威情報を共有、お客さまに24時間の安全・安心を提供してまいります。

NECグループのセキュリティオペレーションセンターから提供されるセキュリティサービスには、24時間365日のセキュリティ運用監視サービスをはじめ、高度なセキュリティインテリジェンス、インシデントレスポンス支援など、さまざまなサイバーセキュリティリスクに対応した対策サービスを提供しています。その他にもネットワーク監視やヘルプデスクなどお客様ICT基盤の安定・継続的な運用をOneNECで支援できる設備・体制を整えております。

お客さまに提供するサイバーセキュリティ

NECサイバーセキュリティソリューション

最新のサイバー攻撃動向や情報漏えい事案対応などの知見に基づき、
お客さまがこれまで投資されてきた既存のセキュリティ対策を活かしながら、
セキュリティ対策の強化をトータルにご支援します。

1 ‖ 自社運用のノウハウを基にしたソリューションを提供

❶ 数えるマネジメント

NECグループのセキュリティ対策の第一歩は、人、ID、PC、サーバ、ログにいたるまで数値で見える化し、どこにどのような問題点があるのかを把握するとともに、数値を読み解くことで誰もが理解できる形で対策優先度を示すことに努めてまいりました。見える化によって、「実はパッチが未適用だった」、「PCにウイルス対策ソフトがインストールされていない」、といった今まで人に依存していたセキュリティ運用の課題を、NECグループの数えるマネジメントでお客さまの悩みを解決します。

❷ NECグループで実証したソリューション

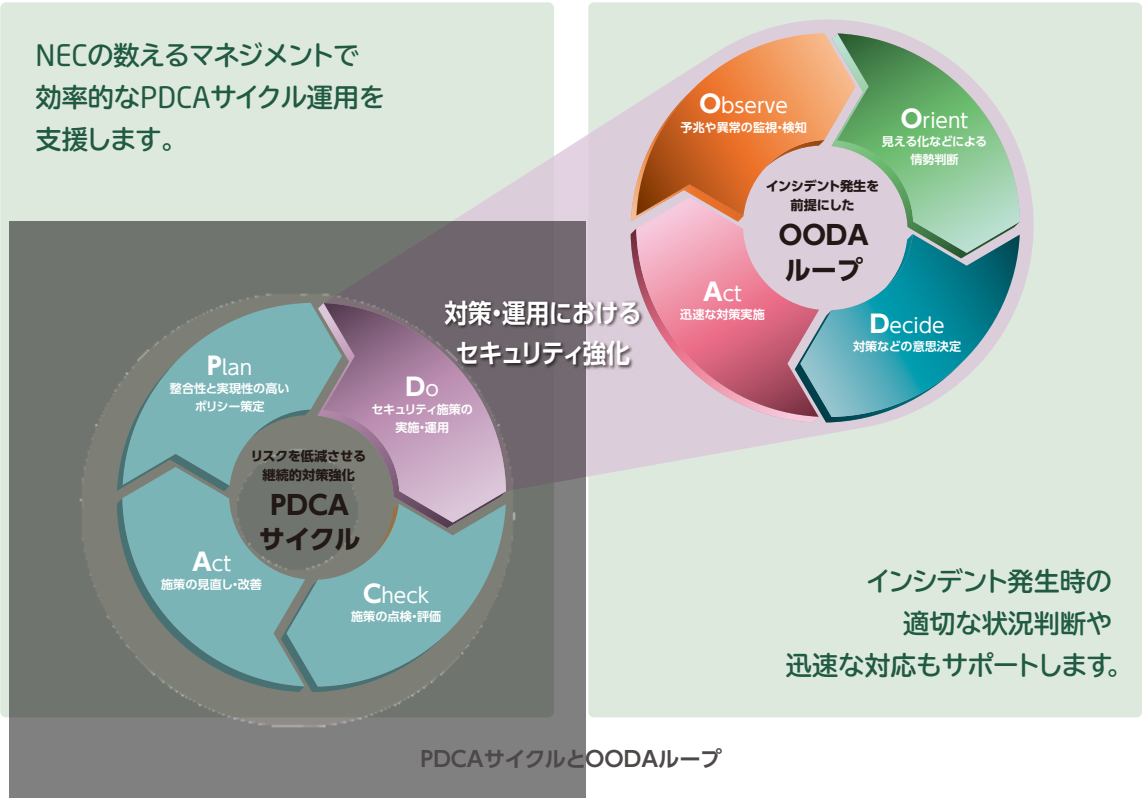
NECグループが提供するサイバーセキュリティソリューションは、NECグループで実証し、利便性と安全性の効果を検証したものを提供しています。さらに自社運用で得たノウハウや知見をお客さまにフィードバックすることで、保守運用においても可用性および品質面の向上に寄与します。

2 ‖ PDCAとOODA（ウゥーダ）

セキュリティ対策は、セキュリティ製品を導入して終わりではありません。適切な運用・監視を行い、情報セキュリティマネジメントサイクルであるPlan（計画）- Do（実施）- Check（点検）- Act（改善）を回し続けることで、セキュリティ品質の劣化を防ぐ必要があります。

また、昨今の高度化したサイバー攻撃は、PDCAサイクルを回すスピードよりも早く、そして多くの攻撃が行われます。このためOODA（ウゥーダ）という概念を取り入れてDo（実施）の中で、監視（Observe）、情勢判断（Orient）、意思決定（Decide）、行動（Act）を高速に回すことで、インシデント発生および予兆の迅速な検知、正確な情勢判断による初動対応の迅速化を可能とし、被害の局所化を支援します。

NECグループのサイバーセキュリティソリューションは、お客さまの事業環境に合わせて必要なセキュリティ機能をご提供することで、お客さまと共に安全・安心で快適な社会づくりに貢献します。



PDCAサイクルとOODAループ

3 ‖ NEC-CSIRTをモデルにしたCSIRT構築支援

NECグループは、2000年7月に社内でインシデントレスポンス業務を中心とするチームを発足させてサイバーセキュリティ対策を進めてきましたが、インシデントの増加や最新攻撃動向の調査、攻撃手法の分析など業務を拡大させ、2005年にNECグループあるいはお客さまで発生したインシデント解析・対応支援を開始しました。現在では、経営戦略の重要テーマとしてCSIRTの“C”は、Computerだけでなく Corporateの“C”として、フィジカルとサイバーの両面で事業継続の脅威となる事象に対応する役割を担っています。

一般的なCSIRTの機能は、インシデント対応をはじめ、フォレンジック、復旧作業、外部機関との連携などさまざまですが、お客さまの事業規模・業種・業態・組織に合わせて整備する必要があり、無理にすべての機能を準備しようとしても人員やスキル不足、設備の過剰投資になり兼ねません。NECグループのアセスメント・コンサルティングサービスを活用いただくことで、お客さまの事業規模や業種に合わせて必要なCSIRTの立ち上げから業務内容の支援まで、幅広いニーズにお応えします。また、お客さまCSIRTの構築後も円滑なCSIRT運営をお手伝いさせていただきます。

4 ‖ インシデントレスポンス支援システム

❶ NCSP（NEC Cyber Security Platform）

NCSPは、NECグループが自社開発した脆弱性に対する対策立案・実行、インシデントレスポンスを支援するセキュリティ統合管理・対処ソリューションで、NECグループが提供するサイバーインテリジェンスを活用し、社内システムの最新のセキュリティリスク（脆弱性）をリアルタイムに見える化、さらに、セキュリティリスクへの対策提示と対策実行を支援し、サイバー攻撃を受ける前にプロアクティブなセキュリティ対策を実現します。

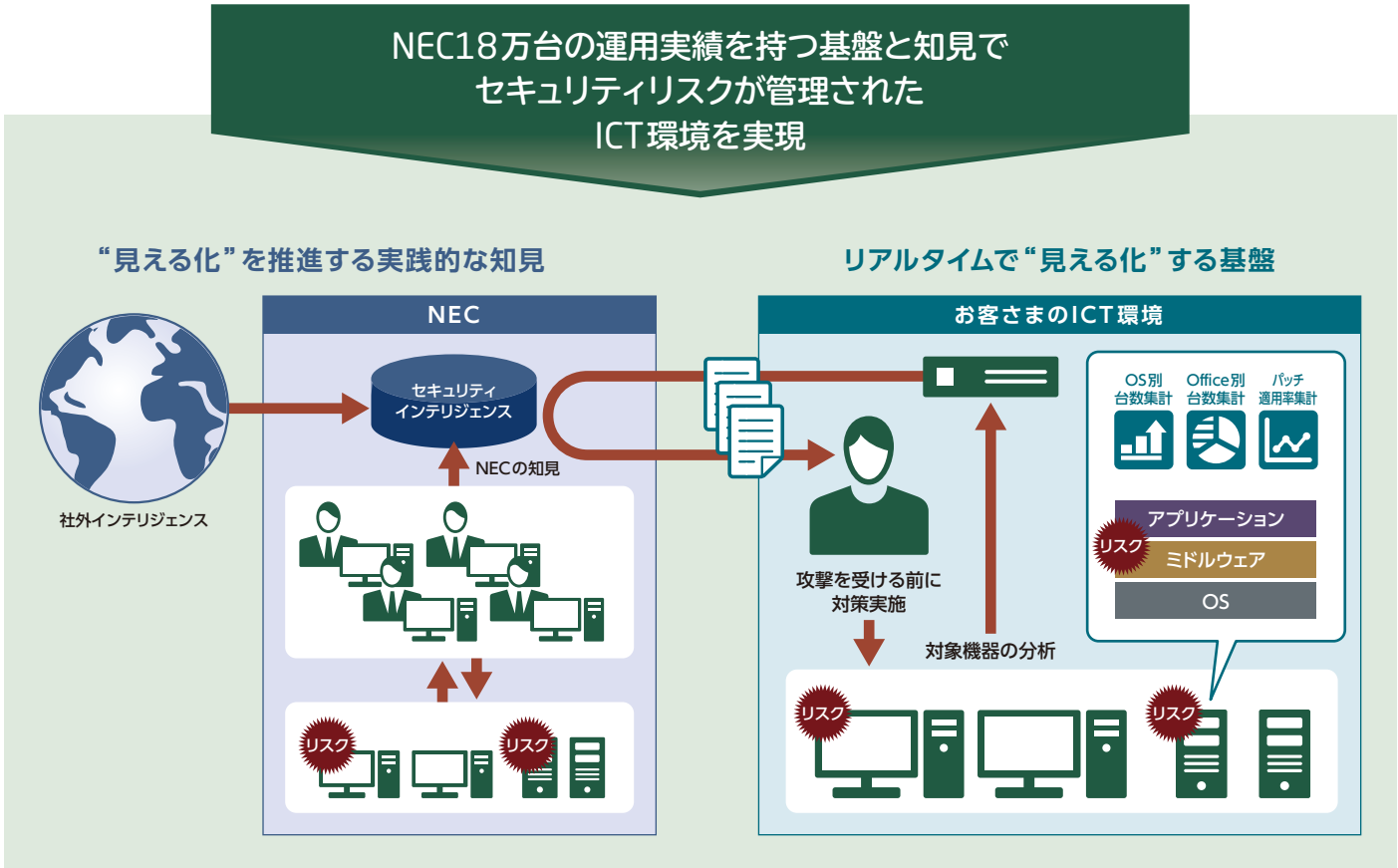
NECグループのCSIRTはグローバルを含めて18万台のPC、サーバの運用過程で発生するインシデントレスポンスをNCSPで効率化します。

❷ 脆弱性対策立案・実行支援機能

脆弱性管理を効率よく実現するために「日本語／英語による脆弱性情報配信」、「複数の対策方法を立案」、「適用の実施と確認」を一元的に管理し、脆弱性情報を受けてから迅速に状況を把握することができます。

❸ インシデントレスポンス支援

異常検知時の端末切り離しの初動対処を、ネットワーク切断することなく、リモートから実施することができ、隔離した環境でリモートからの調査解析を支援することで、インシデントレスポンス業務の効率化を実現しています。

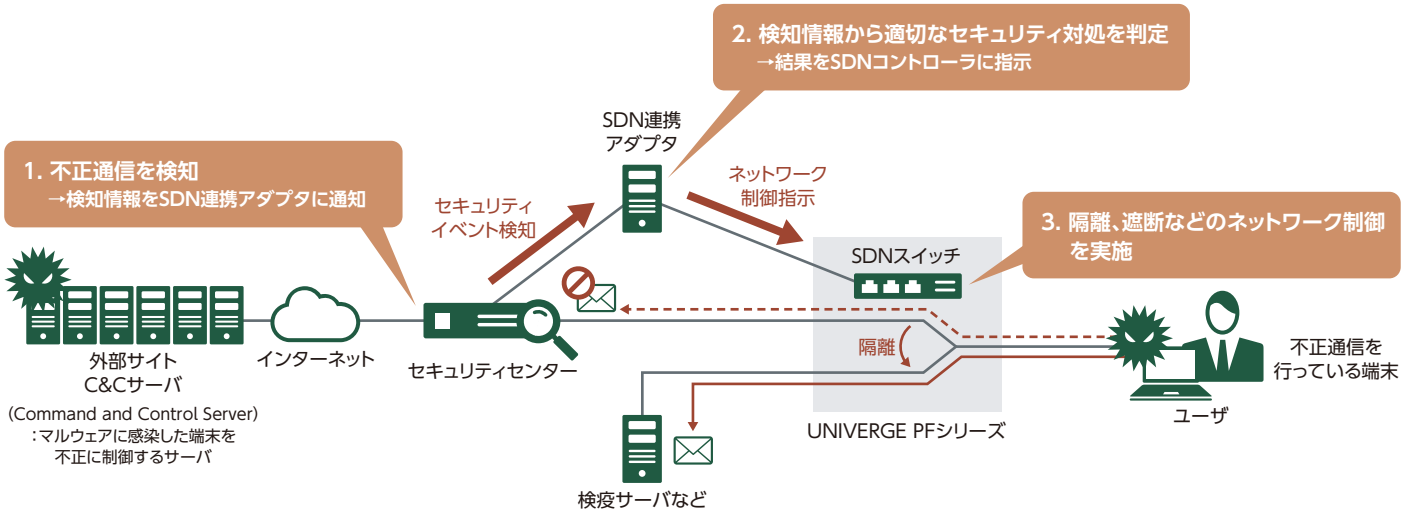


NEC Cyber Security Platformの概要

5 ‖ プロがいなくても初動を迅速に実現するサイバー攻撃自動防御ソリューション

NECグループの注力事業の1つであるSDNを活用した、サイバーセキュリティのプロがいなくても初動を自動で迅速に実現するサイバー攻撃自動防御ソリューションを開発し提供しています。

このソリューションでは、SDN環境に設置されている各種セキュリティセンサが異常を検知すると、SDN連携アダプタに異常情報を通知します。SDN連携アダプタは通知された異常情報に基づき、SDNコントローラに異常端末を社内ネットワークから切り離す指示を自動で実施することで、被害の局所化を迅速に実現します。



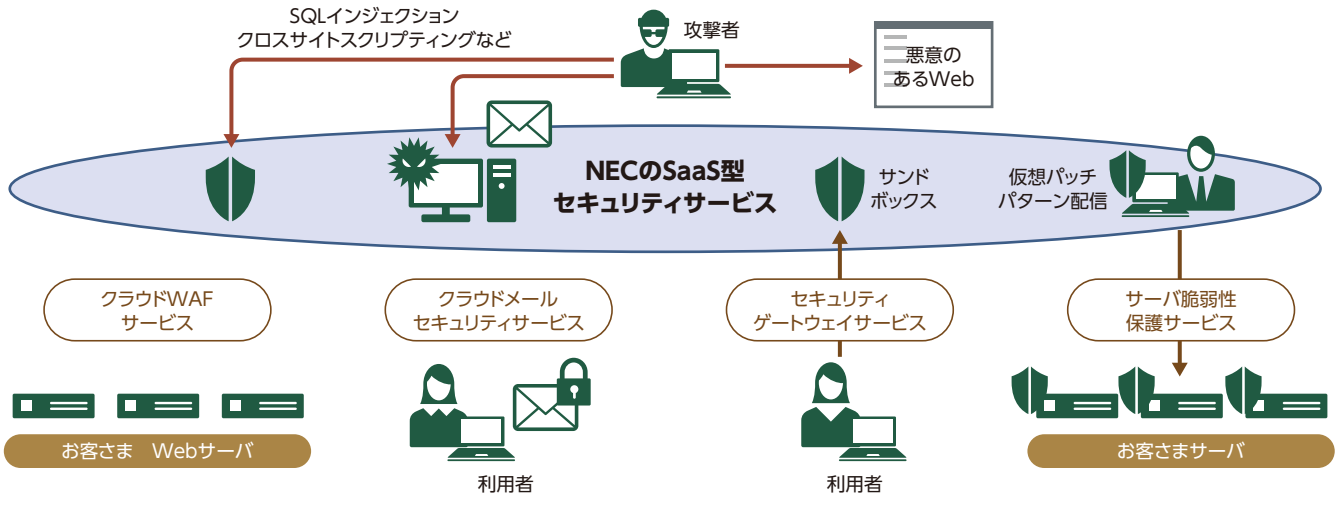
SDNと連携したサイバー攻撃自動防御ソリューション

6 ‖ クラウドから提供されるサイバーセキュリティサービス

NECグループのサイバーセキュリティサービスは、これまで培ってきた高い技術力と、NEC Cloud IaaSという、高いコストパフォーマンスと高性能・高信頼、そして、CSA*1やFISC*2（金融機関などコンピュータシステムの安全対策基準）に準拠した、厳格なアクセス管理を施しているクラウドサービスにより提供されています。

クラウドで提供されるサイバーセキュリティサービスには、WAF（Web Application Firewall）、メールセキュリティ、セキュリティゲートウェイ、サーバ脆弱性保護の4つのサービスを提供しており、お客さまのインターネット接続回線を経由して、新たなセキュリティ設備を導入することなく、短期間で安全で安心なセキュリティ対策を利用することができます。

*1 CSA: The Cloud Security Alliance
*2 FISC: The Center for Financial Industry Information Systems



クラウド型のセキュリティサービス

お客さまに提供するサイバーセキュリティ

研究開発　最前線のサイバーセキュリティ技術

日々巧妙化・高度化するサイバー攻撃に対しNECは新しいサイバーセキュリティ技術を研究開発し、
新たなソリューションやサービス開発に還元することで、サイバー攻撃への対応力を強化しています。

1 ‖ 研究テーマのコンセプト

NECグループは、「Futureproof Security安心の先へ。」というスローガンの下、高度化する社会インフラに対してシステムセキュリティ、データセキュリティの両面から研究開発を行い、「止まらない」、「壊れない」、「誤作動しない」社会インフラを実現することで、お客さまに安全・安心で快適な環境を提供します。

システムセキュリティは、SDNを活用した検疫ネットワークや、ビッグデータ分析を活用した未知の攻撃に対する防御の実現など、巧妙化・高度化するサイバー攻撃に対して複数の技術要素を連携させることで防御力を高めます。

データセキュリティは、データベース暗号、リソースの少ないIoT機器に暗号機能を実装するための「軽量暗号」をはじめ、世界初となる暗号化したままデータ処理を実現する「秘匿計算技術」を開発しています。

研究テーマのコンセプト

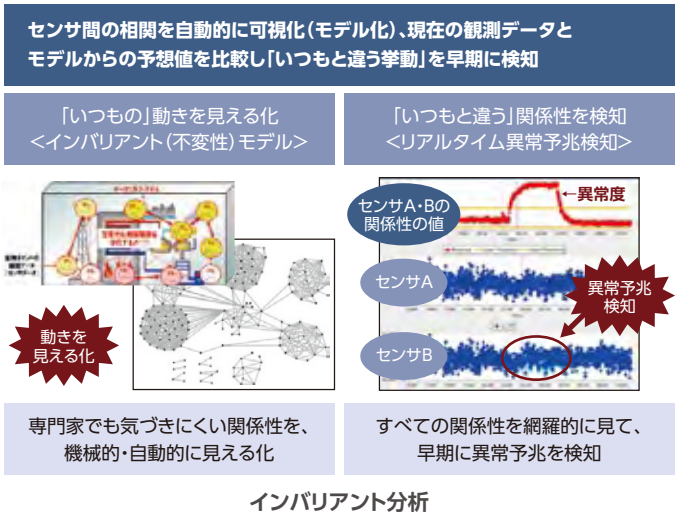
2 ‖ ビッグデータ分析

NECグループは、長年にわたり人工知能（AI）に関連した研究に取り組んでおり、その中でも特に先進技術による新たな法則の発見や、予兆を検知し予知を行う研究開発を推進しています。

❶ インバリアント分析

センサからの大量の時系列データを分析し、平常時に成り立つセンサ間の不変関係（インバリアント）を関係式として自動でモデル化します。このモデルとセンサデータから「いつもと違う」動きを早期に検出することで、システムに起こっている異常の予兆を検知します。

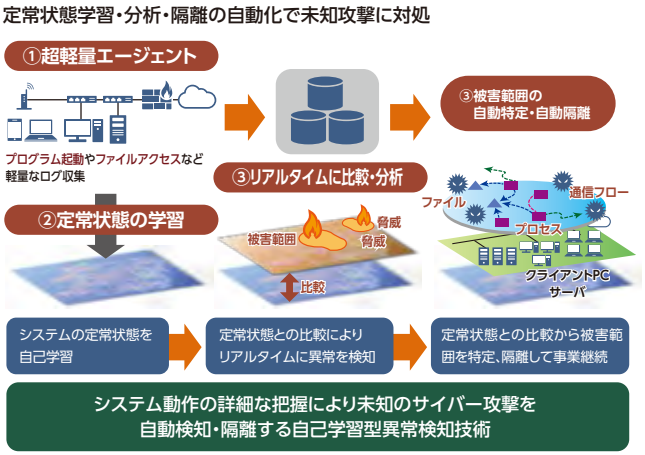
センサ間の相関を、機械学習により自動的に抽出し、専門家でも気づきにくい関係性を見つけることができます。また、人間が総合的に判断するプロセスと同じように、センサ間の関係性を網羅的に見ることでシステムの状態を判断します。



インバリアント分析

❷ 自己学習型システム異常検知技術

人工知能(AI)技術により、未知のサイバー攻撃を自動検知します。この技術は、端末やサーバなどのプログラムの起動やファイルアクセス、通信といったシステム全体の複雑な動作状態から定常状態を機械学習し、定常状態と現在のシステムの動きをリアルタイムに比較、分析することで、定常状態から外れた動作を検知、未知の攻撃への対応が可能となります。さらに、システム管理ツールやSDNなどと連携することで異常端末をネットワークから自動隔離します。従来の対処に比べて10分の1以下の時間で被害範囲の特定が可能で、システム全体を止めることなく被害範囲の拡大を最小限に抑えられる技術です。



自己学習型システム異常検知技術

❸ セキュアネットワーク

近い将来IoTをはじめ産業インターネットの普及が予測されています。しかし、人、モノがつながるサイバー空間は必ずしも安全ではなく、つながる人、モノの信頼性、それらが送信するデータの真正性は保証されていません。

NECグループは、これからのネットワークに求められる、これらの課題を解決し、あらゆる人が公平に利益を享受できるためのセキュアネットワークの研究開発を進めています。

❹ サイバーインテリジェンス

NECグループは、サイバー攻撃の兆候を素早く捉え、適切なタイミングで効果的な対策を自動で実施することを可能にする研究開発を進めています。

サイバー攻撃対策強化に向けた脅威情報の共有にも取り組み、標準化団体のOASIS*1で検討が進められているSTIX*2やTAXII*3といった、脅威情報を記述する仕様や組織間の情報共有手法などの研究開発に積極的に取り組んでいます。

*1 OASIS: 構造化情報標準促進協会
(Organization for the Advancement of Structured Information Standards)
*2 STIX: 脅威情報構造化記述形式(Structured Threat Information eXpression)
*3 TAXII: 検知指標情報自動交換手順(Trusted Automated eXchange of Indicator Information)

3 ‖ 暗号・秘匿計算技術

❶ 軽量暗号

IoTの登場でモノがネットワークに接続されるようになると、モノの機器認証や盗聴に対する通信データの保護が必要になります。しかし、多くのセンサ機器では、性能面やリソース、電力不足により標準的な暗号技術だと十分な実装ができません。NECグループは、リソースが少ない機器でも高い処理性能と世界トップクラスの軽量化を実現した軽量暗号TWINE(トゥワイン)を2012年に発表、2015年にデータ処理量を従来の半分(理論限界)に効率化した認証暗号方式OTR*4を発表、これらによってさまざまな環境下にあるセンサ機器を安全にサイバー空間へつなぐことを可能にします。また、NECグループが開発した認証暗号「AES-OTR」が、米国国立標準技術研究所の支援で行われている技術審査会にて、第一次選考を通過、次世代認証暗号への採択を目指し、認証暗号の設計・実装技術を強化します。

*4 OTR: Offset Two-Round

❷ 秘匿計算

NECグループは、データベースのデータを暗号化したまま処理できる世界初の秘匿計算技術を開発しました。

この技術により、暗号化されたデータベースの情報をそのまま活用することができ、アプリケーションの処理に応じて復号化する必要がなくなるため、データの漏えいや窃取のリスクを軽減することができます。

4 ‖ クラウド技術

❶ セキュアストレージアーカイブ

クラウドストレージサービスの普及に伴い重要なデータがクラウド上に保管されるようになり、さらなる活用を進めるためにデータを安全に保管・活用する技術の研究開発に取り組んでいます。

実現には、秘密分散技術でデータを暗号化して分散保存かつ冗長化し、定期的に高速検査することで、消失した場合でもデータを自動復旧します。

これにより機密性、完全性、可用性を担保し、お客さまが安全・安心で効率的に活用できる新たなクラウドサービスの価値を創造します。

第三者評価・認証

NECグループでは、情報セキュリティに関連する
第三者評価・認証に積極的に取り組んでいます。

1 ‖ ISMS認証の取得状況

情報セキュリティマネジメントシステム国際規格ISMS（ISO/IEC27001）認証を取得した組織を持つ会社は、以下のとおりです。

ISMS認証取得組織を持つグループ会社

- 日本電気株式会社
- アビームコンサルティング株式会社
- アビームシステムズ株式会社
- NECエンジニアリング株式会社
- NECスペーステクノロジー株式会社
- NECソリューションイノベータ株式会社
- NECネクサソリューションズ株式会社
- NECネッツエスアイ株式会社
- NECネットワークワーク・センサ株式会社
- NECネットワークプロダクツ株式会社
- NECビジネスプロセッシング株式会社
- NECフィールディングシステムテクノロジー株式会社
- NECプラットフォームズ株式会社
- 株式会社インフォセック
- 株式会社NEC情報システムズ
- 株式会社KIS
- 株式会社サイバーディフェンス研究所
- 株式会社サンネット
- 株式会社ワイイーシーソリューションズ
- キューアンドエー株式会社
- 静岡日電ビジネス株式会社
- 昭和オプトロニクス株式会社
- 日本電気航空宇宙システム株式会社
- フォワード・インテグレーション・システム・サービス株式会社

2 ‖ プライバシーマーク付与認定の取得状況

一般財団法人日本情報経済社会推進協会（JIPDEC）からのプライバシーマーク使用許諾状況は、以下のとおりです。

プライバシーマーク付与認定を受けたグループ会社

- 日本電気株式会社
- アビームコンサルティング株式会社
- VALWAY121ネット株式会社
- NECエンジニアリング株式会社
- NECソリューションイノベータ株式会社
- NECネクサソリューションズ株式会社
- NECネッツエスアイ株式会社
- NECネットイノベーション株式会社
- NECビジネスプロセッシング株式会社
- NECファシリティーズ株式会社
- NECフィールディング株式会社
- NECフィールディングシステムテクノロジー株式会社
- NECプラットフォームズ株式会社
- NECマグナスコミュニケーションズ株式会社
- NECマネジメントパートナー株式会社
- 株式会社NEC情報システムズ
- 株式会社NECライベックス
- 株式会社KIS
- 株式会社サンネット
- 株式会社ニチワ
- 株式会社ワイイーシーソリューションズ
- キューアンドエー株式会社
- キューアンドエーワークス株式会社
- 静岡日電ビジネス株式会社
- ディー・キュービック株式会社
- フォワード・インテグレーション・システム・サービス株式会社
- ランゲージワン株式会社
- リバンスネット株式会社

3 ‖ ITセキュリティ評価認証の取得状況

ITセキュリティ評価の国際標準であるISO/IEC15408の認証を取得した主な製品・システムは、以下のとおりです。
（認証製品アーカイブリストへの掲載を含みます）

ISO/IEC15408認証取得製品・システム

- DeviceProtector AE
（情報漏えい防止ソフトウェア）
- InfoCage PCセキュリティ
（情報漏えい防止ソフトウェア）
- NECグループ情報漏洩防止システム
（情報漏えい防止ソフトウェア）
- NECグループセキュア情報交換サイト
（セキュア情報交換サイト）
- NEC ファイアウォール SG コアユニット
（ファイアウォール）
- PROCENTER
（文書管理ソフトウェア）
- StarOffice X
（グループウェア）
- WebOTX Application Server
（アプリケーションサーバ）
- WebSAM SystemManager
（サーバ管理）

NECグループの概要

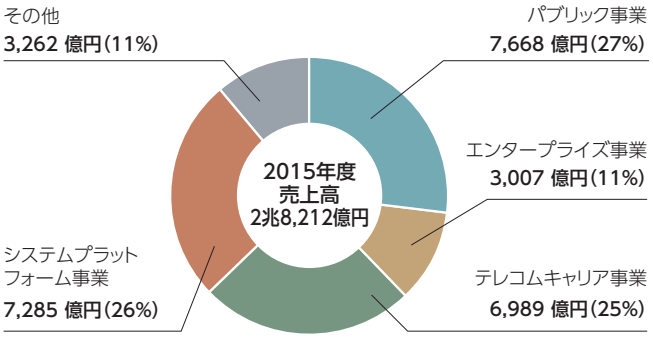
会社概要

商　　号	日本電気株式会社　NEC Corporation
本　　社	東京都港区芝五丁目7番1号
創　　立	1899年(明治32年)7月17日
資 本 金	3,972億円※
連結従業員数	98,726名※
連結子会社数	217社※

※2016年3月31日現在

事業紹介

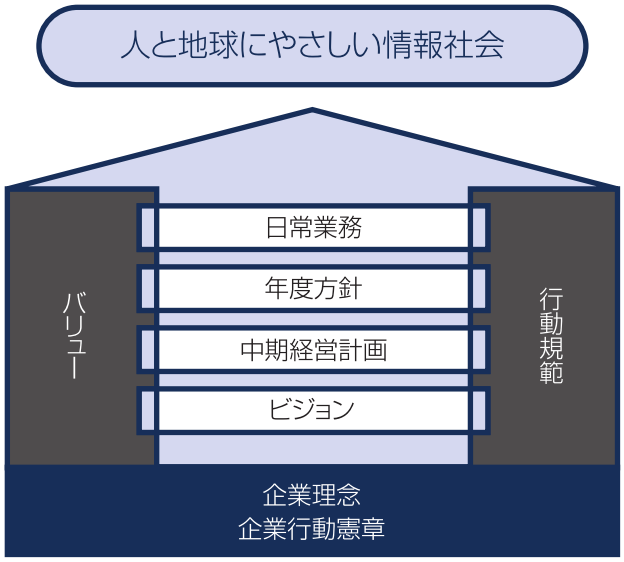
セグメント別売上高(構成比)



※2016年3月31日現在

NEC Way

「NEC Way」は、企業理念、ビジョン、バリュー、企業行動憲章、行動規範を含むNECグループの経営活動の仕組みを体系化したものです。私たちはNEC Wayの実践をとおしてお客さまやその先の社会に貢献し、人と地球にやさしい情報社会を実現していきます。



NECグループ 企業理念

NECはC&Cをとおして、
世界の人々が相互に理解を深め、
人間性を十分に発揮する
豊かな社会の実現に貢献します。

1990年制定

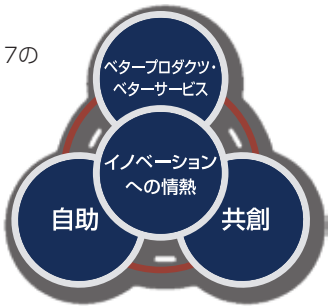
NECグループ ビジョン2017

企業理念に基づいて、NECグループが10年後に実現したい社会像・企業像をまとめました。「2017」には、C&C宣言40周年にあたる2017年に向けたビジョンという意味を込めました。

人と地球にやさしい情報社会をイノベーションで実現する
グローバルリーディングカンパニー

NECグループバリュー

企業理念とNECグループビジョン2017の実現に向けて、NECグループ社員の価値観と行動原理をまとめました。
私たちが、100年を超える歴史の中で受け継ぎ、将来にわたってお客さまや社会に役立ち続けるための源泉となるものです。



価値観	重要な行動原理
[行動の原動力] **イノベーションへの情熱**	●物事の本質を追究する ●従来の常識を創造的に破壊する ●世界中の知恵を新結合する
[個人一人ひとりとして] **自 助**	●スピードを持って動く ●最後までやり抜く ●枠を超えて挑戦する
[チームの一員として] **共 創**	●個性を尊重する ●オープンに聴き学ぶ ●枠を超えて協働する
[お客さまに対して] **ベタープロダクツ・ベターサービス**	●生活者視点で考える ●お客さまの喜びを創造する ●世界のベストを追求する

日本電気株式会社
〒108-8001 東京都港区芝五丁目７番１号
TEL:(03)3454-1111(大代表)
http://jpn.nec.com

VEGETABLE OIL INK

Waterless Printing Naturally

2016年７月発行