\Orchestrating a brighter world NEC

情報セキュリティ報告書 2018

Information Security Report 2018

NECが考える情報セキュリティ

NECは、「情報セキュリティ」を事業継続のための重要な経営基盤として位置づけ、
社会から継続的に信頼される企業を目指しています。

さかい かずひろ
堺 和宏
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）

NECは「Orchestrating a brighter world」というブランドステートメントを掲げ、世界が抱える社会課題をICTの活用によって解決し、人が豊かに生きる「安全」「安心」「効率」「公平」な社会の実現を目指しています。

また、デジタルトランスフォーメーション*1によって新たなビジネスモデルやスキームが生み出され、世の中は大きな転換期を迎えています。NECは、デジタルトランスフォーメーションを単なるトレンドとしてではなく、産業構造を変えるほどの影響力を持った動きとして捉えています。新たな価値創造やビジネス変革を実現していくためには、これまで以上にICTの利活用が重要となります。

『「安全」「安心」「効率」「公平」な社会の実現』、『デジタルトランスフォーメーションの推進』において、「情報セキュリティ」は欠くことのできないものであり、NECは「情報セキュリティ」を事業継続のための重要な経営基盤として位置づけています。

巧妙化・高度化するサイバー攻撃への対策、お客様へ提供する製品・システム・サービスの高品質なセキュリティの確保、お取引先と連携した情報セキュリティ対策などを進めるとともに、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取り組みを行い、社会から継続的に信頼される企業になることを目指しています。NECの情報セキュリティは、以下の基本的な考え方に基づき、活動に取り組んでいます。

- 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
- 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。ぜひご一読くださいますようお願い申し上げます。

*1 Digital Transformation（DX）：リアルとサイバーをつなぎ合わせる情報技術で新たな価値を創造し、経済や生活をより良い方面に変えていくという概念

情報セキュリティ報告書 2018

NECが考える情報セキュリティ 02

デジタルトランスフォーメーション(DX)を支えるセキュリティ 04

サイバー攻撃対策 08

情報セキュリティ推進フレームワーク 10

情報セキュリティガバナンス 11

情報セキュリティマネジメント 12

情報セキュリティ基盤 14

情報セキュリティ人材 18

お取引先と連携した情報セキュリティ 20

セキュアな製品・システム・サービスの提供 22

NECのサイバーセキュリティ戦略 24

研究開発　最前線のサイバーセキュリティ技術 28

第三者評価・認証 30

NECグループの概要 31

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、2018年6月までの取り組みを対象に掲載しています。

本報告書に記載されている会社名、システム名、製品名などは、各社の商標または登録商標です。

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 CISOオフィス
〒108-8001 東京都港区芝五丁目7-1 NEC本社ビル
03-3454-1111(大代表)

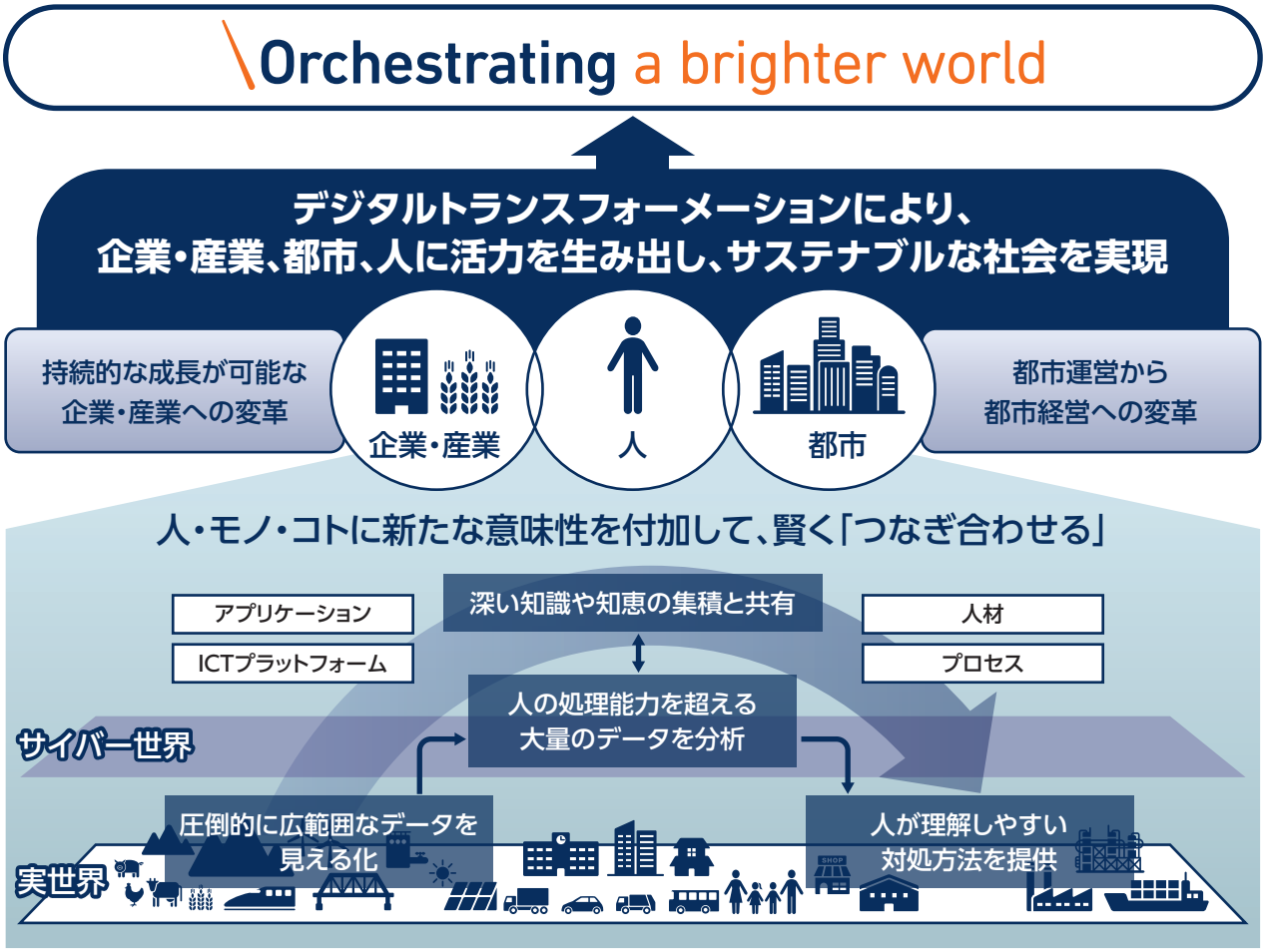
デジタルトランスフォーメーション(DX)を支えるセキュリティ

NECはデジタルトランスフォーメーションを、“実世界の出来事をデジタル化してサイバー世界に取り込み、人・モノ・コトをつなげて新しい価値を生み出し、生活やビジネスをより良く変えていくこと”と捉えています。

これには、さまざまな状況を「見える化」(デジタル化)し、集積された膨大なデータを高度に「分析」し、最適な「対処」を行うといった一連のプロセスが重要です。そのため、デジタルトランスフォーメーションをサポートする強固なセキュリティレベルを確保したプラットフォームが必要となります。このプラットフォームを実現するには、AI技術、IoT技術、ネットワーク技術、大量データを高速処理するコンピューティング技術、セキュリティ技術が不可欠です。

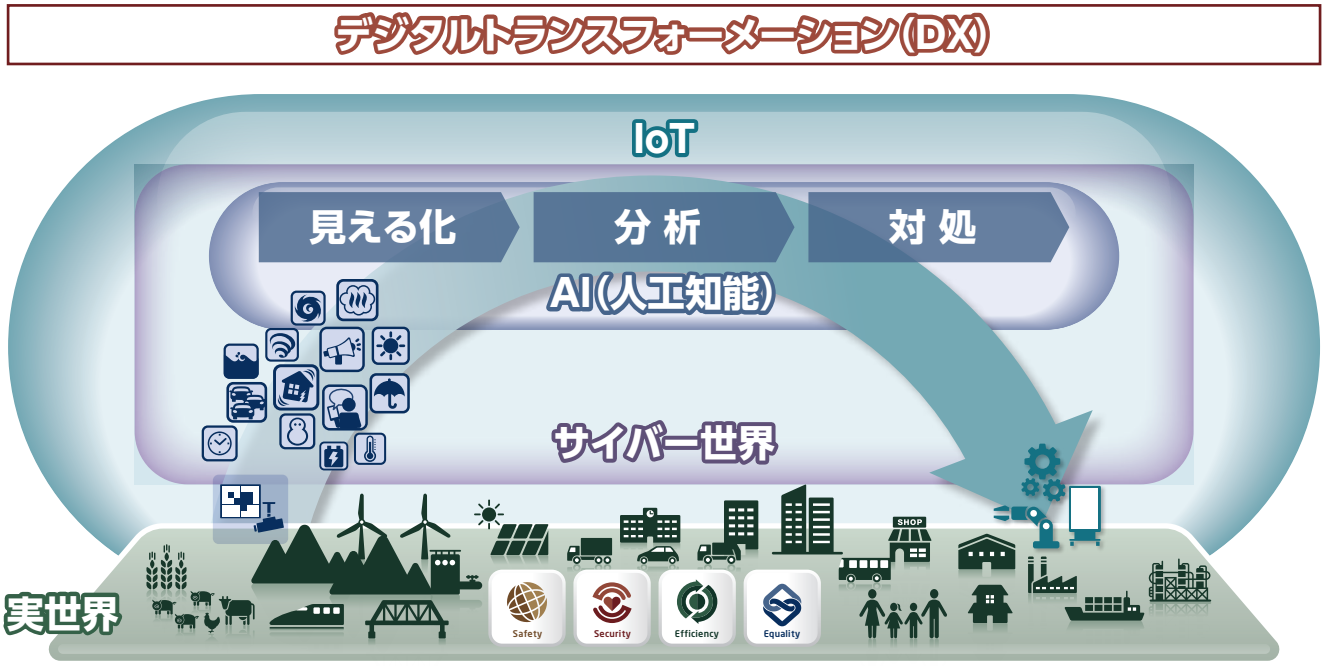
NECは、これらの技術を駆使し、デジタルトランスフォーメーションの実現に欠かせない「NEC DXソリューション」を拡充し、お客様への提案を加速しています。

また、NEC自らも、営業・マーケティング領域、設計・開発領域、生産領域、働き方の領域などでデジタルトランスフォーメーションを起こしています。このように、社内でデジタルトランスフォーメーションを実現するために、安全・安心に業務を行えるセキュアな基盤を構築・運用しています。



NECが考えるデジタルトランスフォーメーション

1 NEC the WISE IoT Platform



デジタルトランスフォーメーション(DX)とIoT

デジタルトランスフォーメーションの実現の場面として、AI・IoTを活用した、「働き方の変革」や「バリューチェーンの変革」「組織やエコシステムの変革」「運用モデルの変革」の実現が挙げられます。

IoTは、「実世界との接点」をつくる技術、ツールとなることができます。AIは、実世界から得られたデータを高速かつ高度な分析をすることができます。これにより「実世界の情報を見える化し、分析、それを実世界にまた戻す」という一連のサイクルをまわすことで、新たな価値の創造が実現できます。

働き方の変革では、これまでの経験やカンに基づく属人的なオペレーションから、リアルデータと分析に基づくオペレーションへと働き方を変え、安定した運用、形式知化と共有、時間・場所を問わないワーク環境などの新たな価値を創造します。

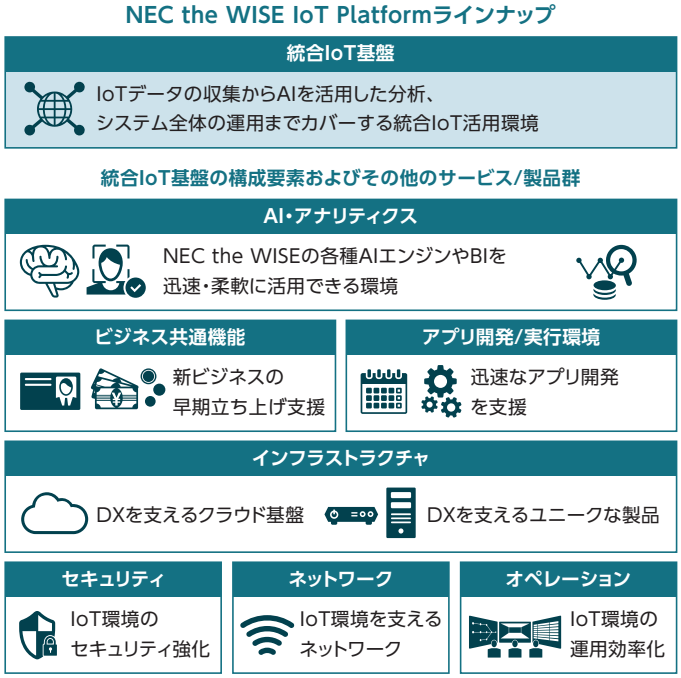
バリューチェーンの変革では、従来のバリューチェーン(例:製造⇒販売⇒消費者)の構造から、生産計画・商品開発の効率化、タイムリーにニーズにこたえる製品企画、今までにない購入体験・利用体験の提供など、消費者を中心としたものに変え、新たな価値を創出します。

組織やエコシステムの変革では、IT／マーケティング／開発／サポートなどの各種部門が連携し、組織間連携による全体最適や、消費者／パートナー／市民を中心とした組織・エコシステムへと変化させ、個別最適でなく、新たな価値を創造します。

運用モデルの変革では、オペレーションの効率性向上など、デジタルに接続された製品・サービスを活用して運用を効率化し、イノベーションをも創生します。

デジタルトランスフォーメーションを実現させるために、最先端AI技術とIoTを利用する基盤として、NECでは「NEC the WISE IoT Platform」を提供しています。高効率なデータ収集基盤と、実証から本番まで、素早いシステム構築・移行が可能なビルディングブロック構造を持ち、セキュアで堅牢性の高いシステム構築が可能です。

また、さまざまな業種において培われてきた業務ノウハウ・価値を備えたビジネス共通機能、企業の事業活動などを支える共通アプリケーション、インフラストラクチャ、開発／実行環境、クラウド利用環境から、ネットワーク、セキュリティ、オペレーションまで、トータルにサポートされています。



NEC the WISE IoT Platform

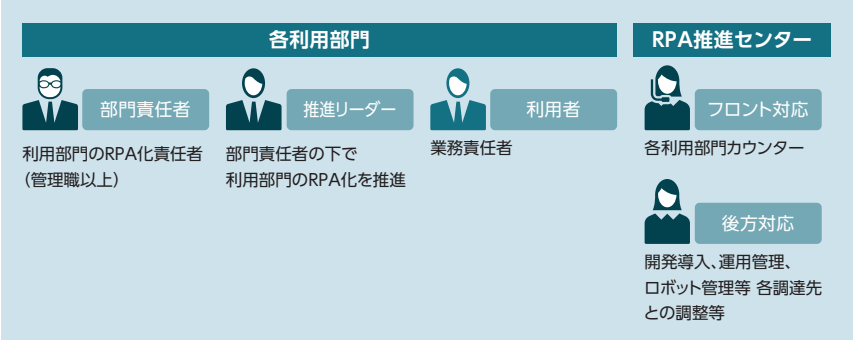
2 RPA*1による業務自動化

RPA技術は、業務システムへのデータ入力のような、従来は人が行っていた定型作業を自動化することから、生産性向上に大きく貢献できると期待されています。RPAは、デジタルトランスフォーメーションとしての営業・マーケティング領域、設計・開発領域、生産領域、働き方改革領域などへの積極的な利用が見込まれています。NECでは、管理されていないRPAの不正利用やRPAシステム更新時の不具合等のリスクに対応するため、RPAのセキュリティ対策を実施しています。

*1 RPA:Robotic Process Automation

❶ RPA推進センター運営体制

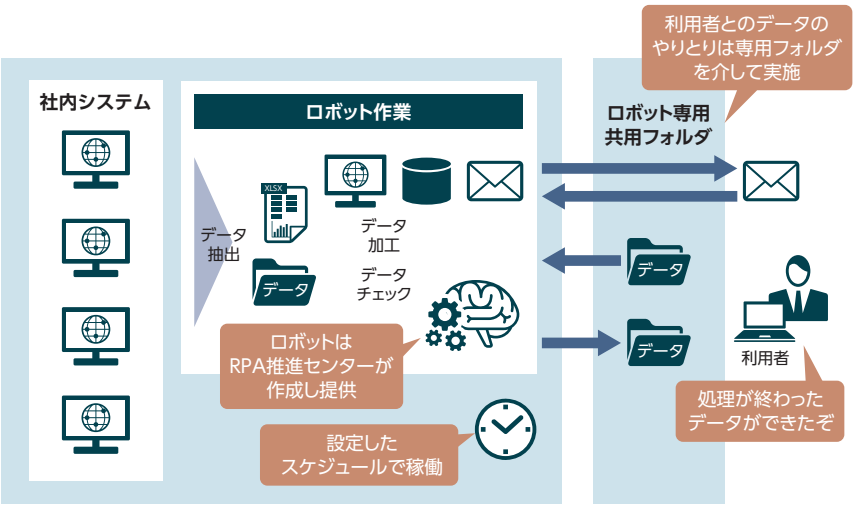
NECでは、社内で利用されるロボットを適切に管理し、RPAによる生産性の向上をサポートするために、RPA推進センター運営体制を敷いています。本体制は、RPAを一元管理するRPA推進センターと、RPA利用部門に設置される部門責任者、推進リーダー、および実際にRPAを利用する利用者で構成されています。この体制により、社内で利用するロボットを一元管理し、セキュリティ対策を実施しています。



体 制

❷ RPAインフラ環境

RPAを導入する際は、人とロボットの違いに起因するリスクに十分な対策を取ることが必要です。社内で利用するロボットをセキュリティ対策が施されたRPAインフラ環境上で稼働させ、監視を行うことで管理しています。本環境を用いることで、利用者は安全・安心にRPAを利用し、生産性を向上させていくことができます。



RPA利用イメージ

❸ ガイドラインの整備

人がPC上で行える定型作業はすべてロボットを利用することが可能ですが、用途やロボットの構造によってはセキュリティ事故が発生するリスクが増大します。NECでは、RPA推進センターがRPA利用に対するリスク評価を行い、対策をガイドラインとして整備しています。

3 クラウドサービス(SaaS: Software as a Service)セキュリティ

クラウドサービス(SaaS)は迅速に導入可能であることから、ビジネススピードの向上などによりデジタルトランスフォーメーションの実現には欠かせません。

NECでは、NECの持つ技術や基盤とクラウドサービス、もしくはクラウドサービス同士をつなぎ合わせることで、今までにない価値を提供しています。社内においても、クラウドサービスを安全・安心な環境で積極的に利用していくための施策を実施しています。

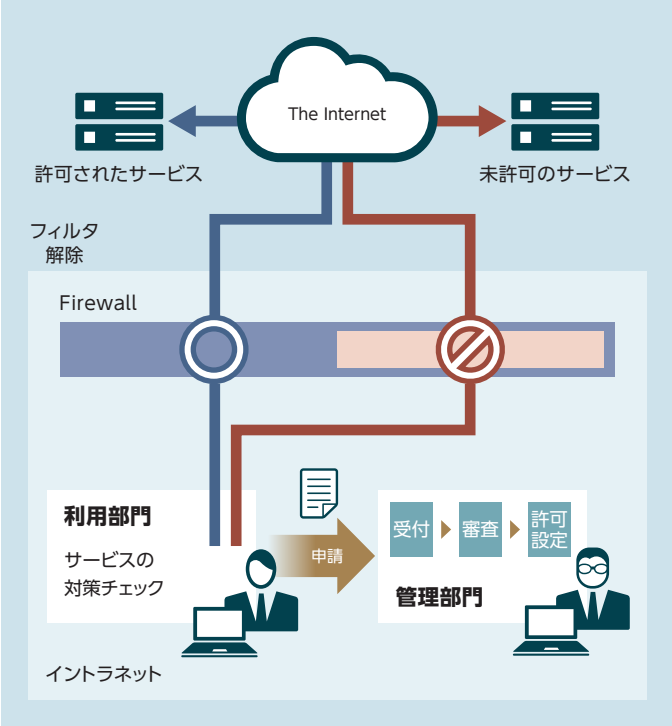
❶ クラウドサービス利用推進体制

NECでは社内でのクラウドサービス利用を適切に管理するために、クラウド活用センターを設置しています。クラウド活用センターでは、NECグループ全体で利用するクラウドサービスの提供や、セキュリティの確認を実施しています。

また、情報セキュリティ推進体制に従って、クラウドサービスのセキュリティに関する情報共有を行っています。

❷ クラウドサービス利用時のセキュリティポリシー

NECでは、社内でのクラウドサービスを利用する際の遵守しなければならないセキュリティポリシーを規定しています。利用者はクラウドサービスを利用する場合、事前にセキュリティを確認した上で、クラウド活用センターに申請を行い、承認を受けるプロセスになっています。

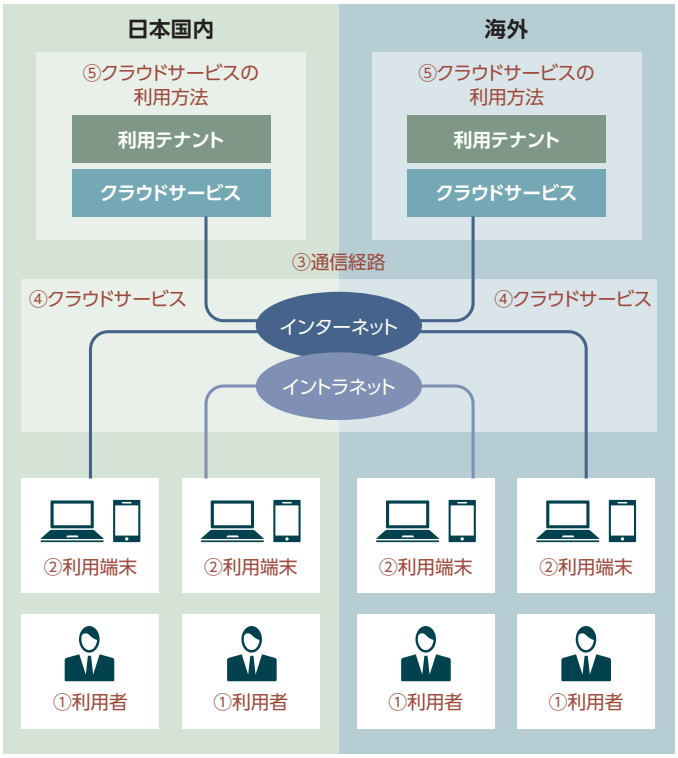


クラウドサービス利用時のセキュリティポリシー

❸ クラウドサービス利用時のセキュリティ対策

従来は、セキュリティ対策の施されたイントラネット内にシステムを構築することでセキュリティレベルを確保していました。しかし、インターネット上にあるクラウドサービスを利用する場合、これまでのセキュリティ対策だけでは十分ではありません。

NECではクラウドサービスを利用する際の環境を、利用者、利用端末、通信経路、クラウドサービス、クラウドサービスの利用方法の5つに分け、これら環境にてセキュリティ対策を実施することで、セキュリティレベルを確保しています。



クラウドサービス利用時のセキュリティ対策

❹ クラウドサービスの分類

NECでは、安全・安心かつ効率的にクラウドサービスを利用するため、NECグループ全体で利用するクラウドサービス、利用を要望する組織が申請を行った上で利用するクラウドサービス、利用を禁止しているクラウドサービスに分けて管理しています。

サイバー攻撃対策

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一律に実施するとともに、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では、標的型攻撃、ランサムウェア、BEC*2、ばらまき型メール攻撃*3など、日々発生するサイバー攻撃の脅威に対して4つに分類したリスク分析を行い、分析結果に基づくサイバー攻撃対策を実施しています。

*2: BEC: Business E-mail Compromise　ビジネスメール詐欺
*3: ばらまき型メール攻撃: 不特定多数を狙った攻撃

【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、脅威インテリジェンスの活用により、NEC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、運用上の課題を把握します。

【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*4評価、社内IT環境調査により、対象製品・サービスの社内IT環境への適合性などを分析します。

*4 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、効果やコストを分析します。

2 グローバルサイバー攻撃対策

NEC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*5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をすることは、事業継続の必須条件と捉えています。

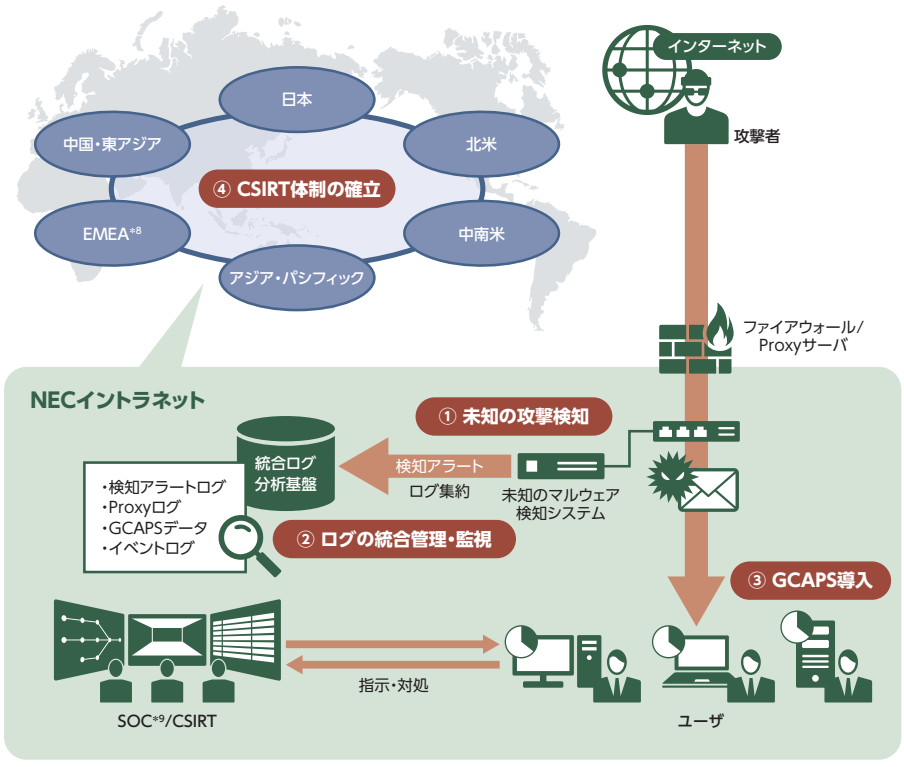
グローバルサイバー攻撃対策では、①「未知の攻撃検知」、②「ログの統合管理・監視」、③「GCAPS*6導入」、④「CSIRT体制の確立」の大きく4点に注力し施策を展開しています。

*5 CISO: Chief Information Security Officer
*6 GCAPS: Global Cyber Attack Protection System

❶ 未知の攻撃検知

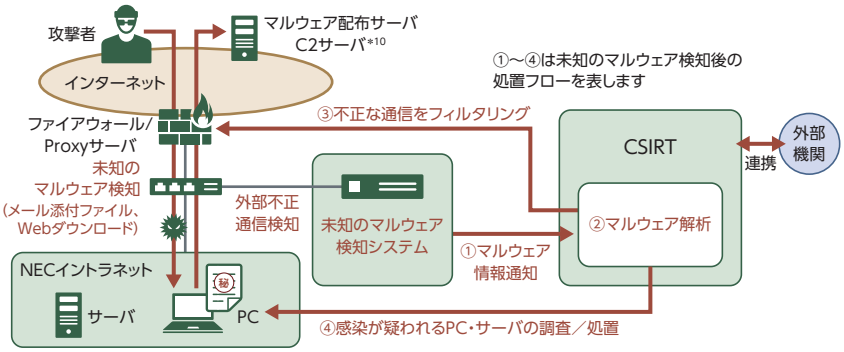
入口・出口対策として、未知のマルウェア検知システムを導入し、Web通信とメール受信を監視し、検知した未知のマルウェア情報などを基に、不正通信をフィルタリングするとともに、感染が疑われるPC及びサーバへの処置を実施します。また、SDN*7との連携により、感染端末からの不正通信の自動遮断を24時間365日体制で実施しており、二次感染の拡大防止、セキュリティリスクの極小化を実現しています。

*7 SDN: Software-Defined Networking



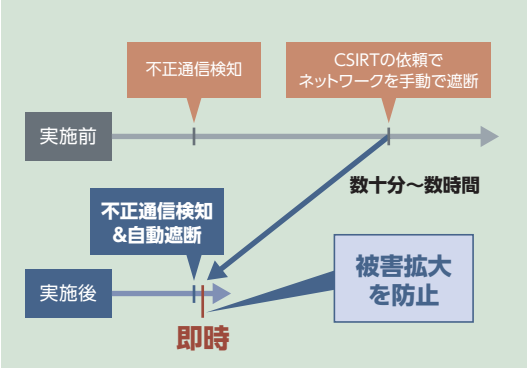
*8 EMEA: Europe, the Middle East and Africa　ヨーロッパ、中東、アフリカ　*9 SOC: Security Operation Center

グローバルサイバー攻撃対策の全体像



*10 C2サーバ: Command & Controlサーバ　マルウェアに感染した端末を不正に制御するサーバ

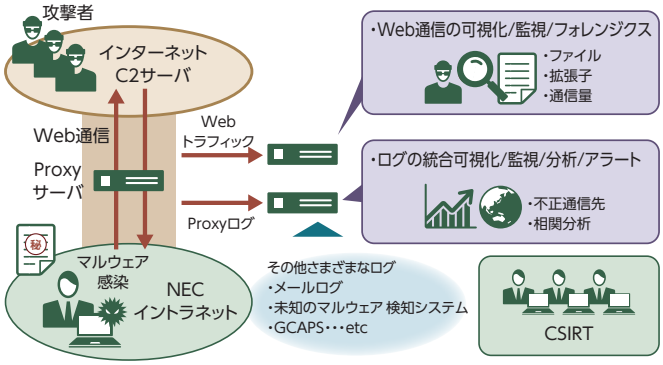
未知のマルウェア・不正通信の検知



未知のマルウェア検知システム×SDN連携による効果

❷ ログの統合管理・監視

NECグループ18万台のPC・サーバの通信や操作ログデータを統合的に集約管理し、解析調査の効率化、高度化をはかっています。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。



ログの統合分析とパケットの調査

❸ GCAPS導入

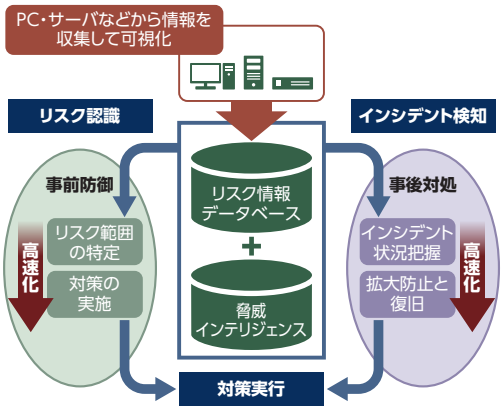
PC・サーバの脆弱性対策及びインシデントレスポンスの効率化を目的として、NECグループ全社に対してGCAPS（外販ソリューション名：NCSP*11）を展開しています。

脆弱性を利用する攻撃を防ぐため、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実施しています。

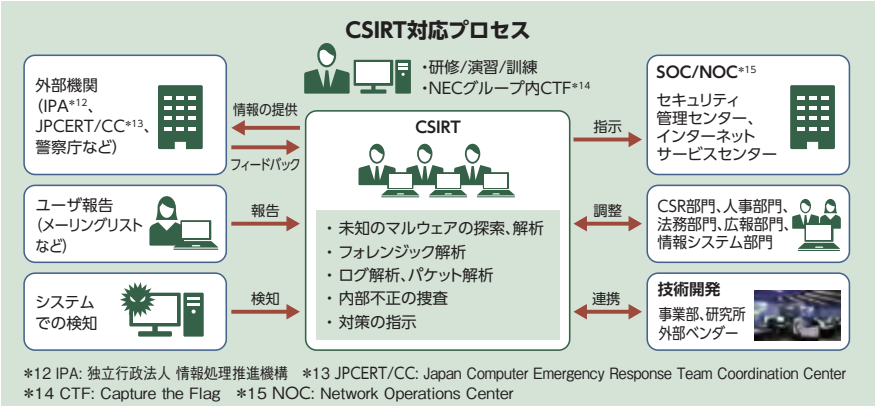
*11 NCSP: NEC Cyber Security Platform

❹ CSIRT体制の確立

NEC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脅威インテリジェンス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。



GCAPSのコンセプト



*12 IPA: 独立行政法人 情報処理推進機構　*13 JPCERT/CC: Japan Computer Emergency Response Team Coordination Center
*14 CTF: Capture the Flag　*15 NOC: Network Operations Center

CSIRTの全体像

3 サイバー攻撃対策におけるAIの活用

NECでは、「AI（人工知能）」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環境での価値実証を行いながら、NECの注力領域の成長と先進的な社内レファレンス構築をはかっています。

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*16を NEC Asia Pacific（シンガポール）の実IT環境に導入し、CSIRTによる監視業務を実施しています。実運用の中で得られた要求事項や改善点を製品開発部門へフィードバックすることでASIの品質向上に協力しています。

*16 ASI：Automated Security Intelligence　自己学習型システム異常検知技術

情報セキュリティ推進フレームワーク

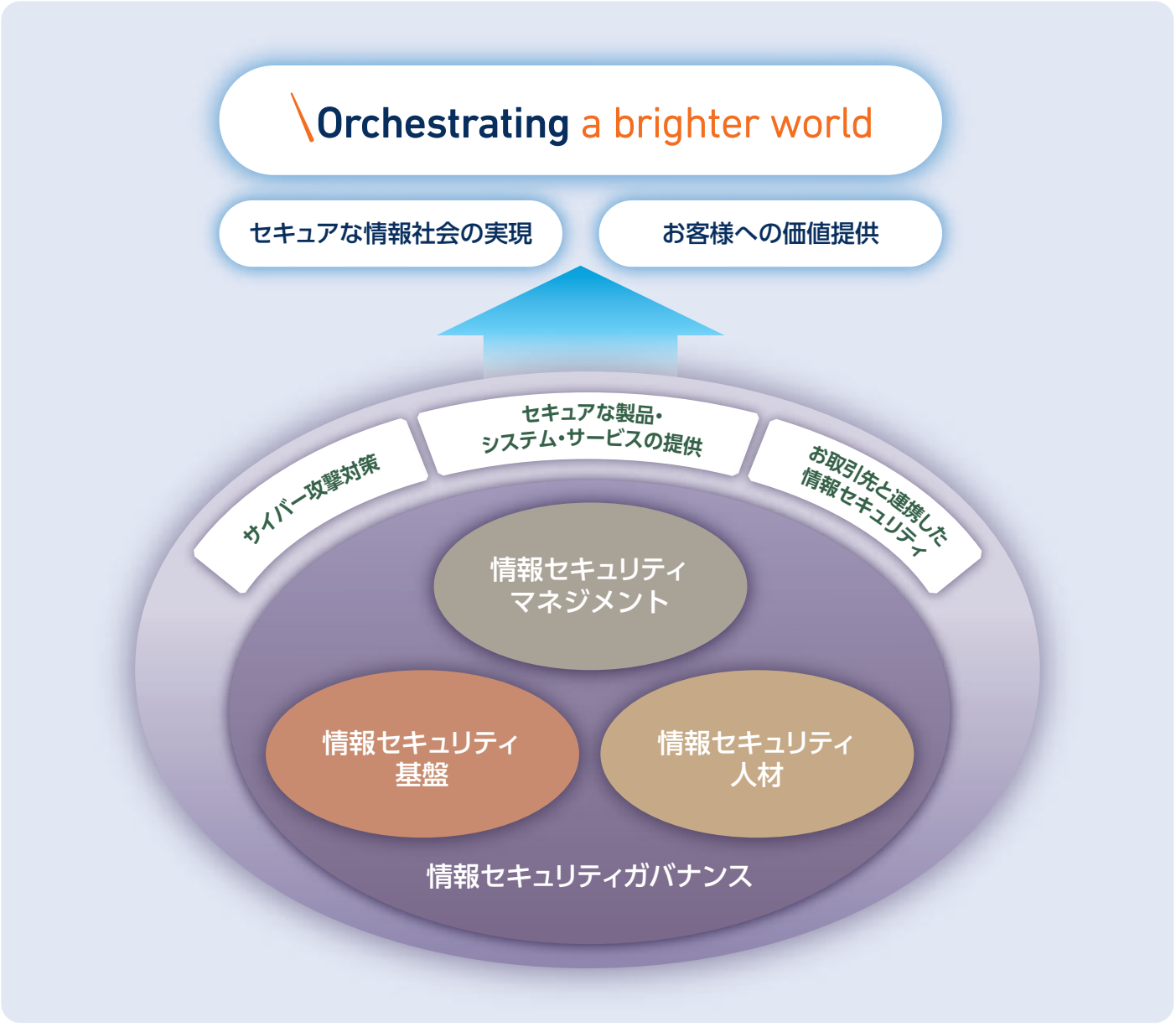
NECグループは、グループ全体で情報セキュリティの維持・向上をはかり、
セキュアな情報社会の実現とお客さまへの価値を提供することで、
「人と地球にやさしい情報社会」の実現に貢献します。

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、セキュアな情報社会を実現し、お客さまへ価値を提供します。

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、サイバー攻撃対策、セキュアな製品・システム・サービスの提供、お取引先と連携した情報セキュリティを推進するとともに、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3つを柱に、NECグループ内へ統制をはかり、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。

NECグループ内への統制は、情報セキュリティガバナンスとして、効果的・効率的に浸透・徹底させるため機能しています。

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を行うとともに、経営層によるセキュリティ目標の設定、グループ施策、体制構築、経営資産の割り当ての方針を決定し、モニタリング、改善是正などを行っています。

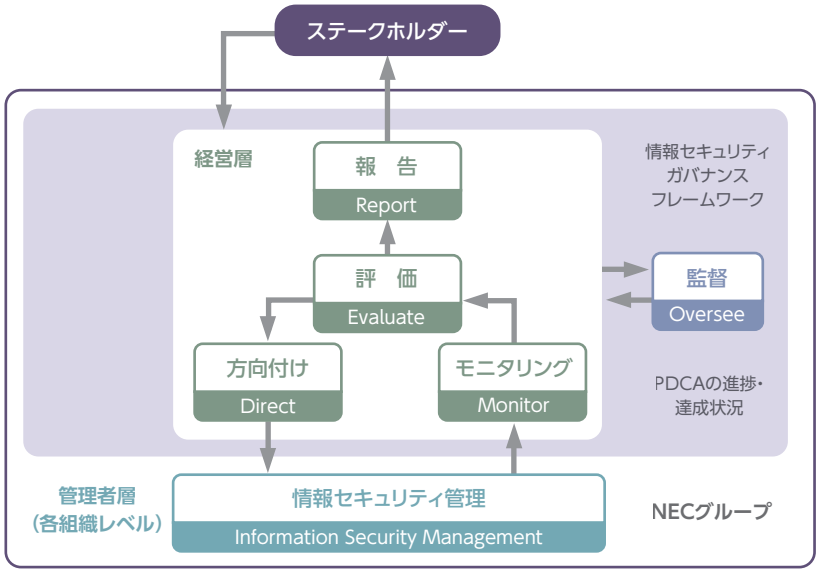


情報セキュリティガバナンス

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を実現するベースを確立しています。NECグループ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。



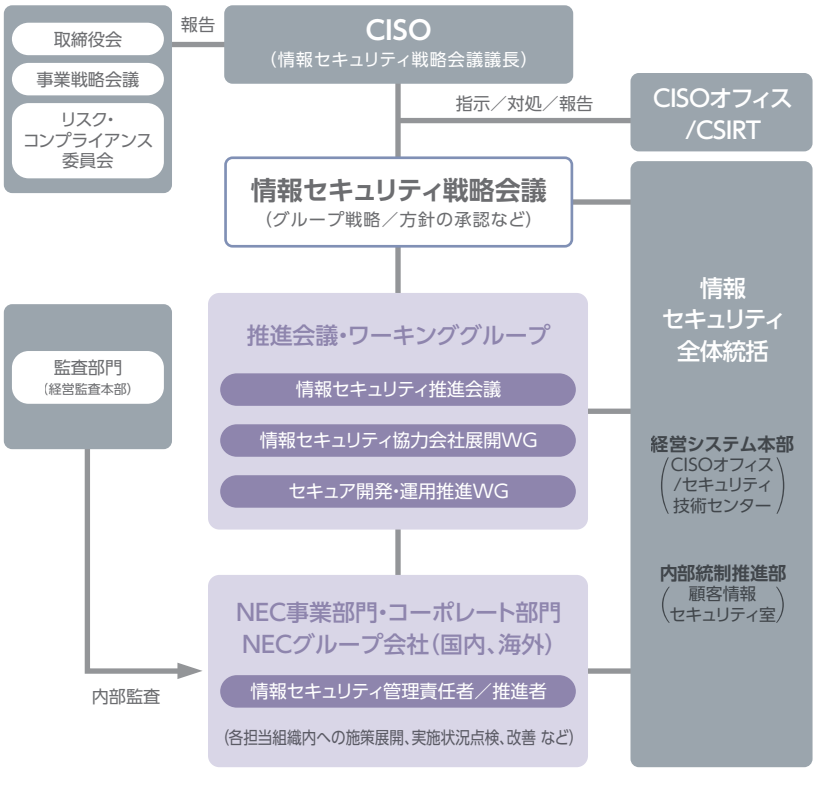
情報セキュリティガバナンス

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*1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。また、CISOから直接指示を受け、サイバーセキュリティ対策推進などを行うCISOオフィスと、サイバー攻撃を監視し、インシデント発生時に迅速に攻撃の解析、原因分析を行い、事態の収束を行うCSIRT*2をCISO配下に設置しています。推進会議やWG(ワーキンググループ)は、国内・海外、お取引先およびセキュア開発・運用の推進計画、実行施策討議・調整、指示事項徹底、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。

*1 CISO: Chief Information Security Officer
*2 CSIRT: Computer Security Incident Response Team



情報セキュリティ推進体制

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付与認定の取得・維持も推進しています。

NECの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

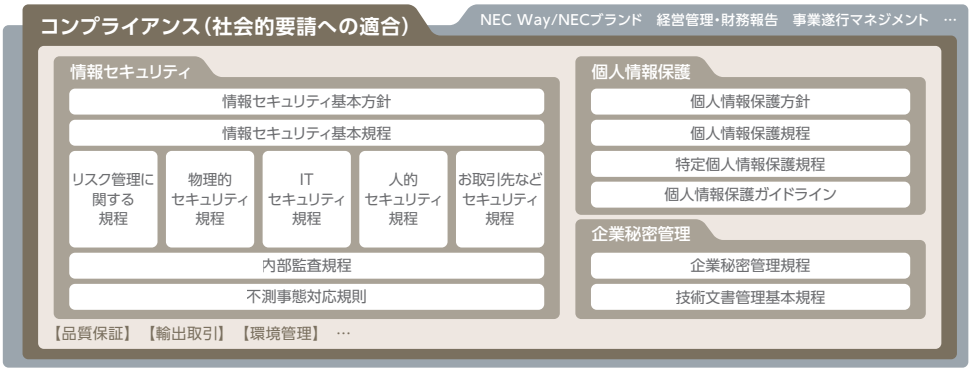
NECでは、国内・海外のグループ会社の共通ポリシーとして「NECグループ経営ポリシー」が展開されており、そこには情報セキュリティや個人情報保護のポリシーが含まれています。情報セキュリティや個人情報保護は、これまでも事業遂行上の重要事項として管理の強化に取り組んできました。

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付与認定を取得し、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。さらに2017年に施行された改正個人情報保護法への対応もマニュアルの改訂などで順次実施しました。2017年のJISQ15001改訂にともない、個人情報保護規程やマニュアルの改訂、GDPR*1に準拠したNECのガイドラインの改訂を順次実施しています。

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、NECグループで28社（2018年6月末現在）がプライバシーマーク付与認定を取得しています。

*1 GDPR: General Data Protection Regulation　EU一般データ保護規則



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、その報告内容を分析した結果を、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、効果測定を行い、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を行うことで、効果を上げています。

4 情報セキュリティ点検

NEC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、情報セキュリティ点検を毎年行っています。

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点検の重点項目に設定しています。また、対策実施の有無や、実施できていない状況を回答する形式にし、個人へ気づきを与え、是正を促す仕組みにしています。

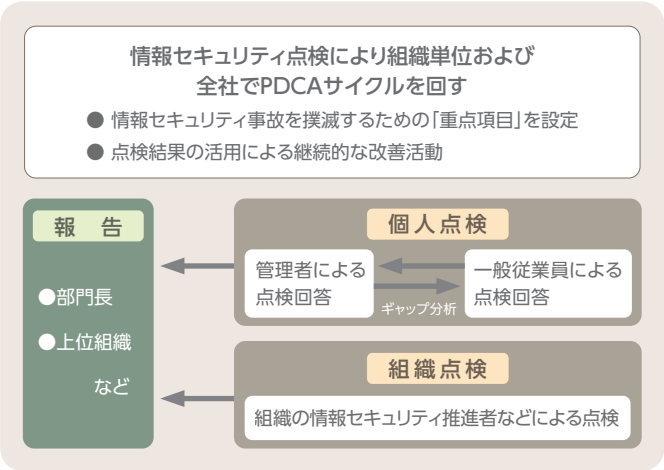
具体的には、社外への持ち出し管理、秘密情報や個人情報の安全管理、外部委託先（お取引先）管理、メール誤送信防止、標的型攻撃メール対策、セキュア開発・運用などの項目について点検しています。

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、個人へ気づきを与え、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、各組織で理由を把握し改善を行うとともに、全社として傾向分析を行い、残課題を解決します。さらなる強化が必要な場合は、次年度の情報セキュリティ推進計画へ反映することで、継続的な改善に取り組んでいます。



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。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では、経営監査本部による徹底した内部監査を、定期的に受ける制度が確立しています。

6 ISMS認証取得の取り組み

NEC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、多くの組織に利用されてきた実績があります。

情報セキュリティ基盤

NEC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つの基盤からなり、これらが相互に連携し、補完しあいながら、NEC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）

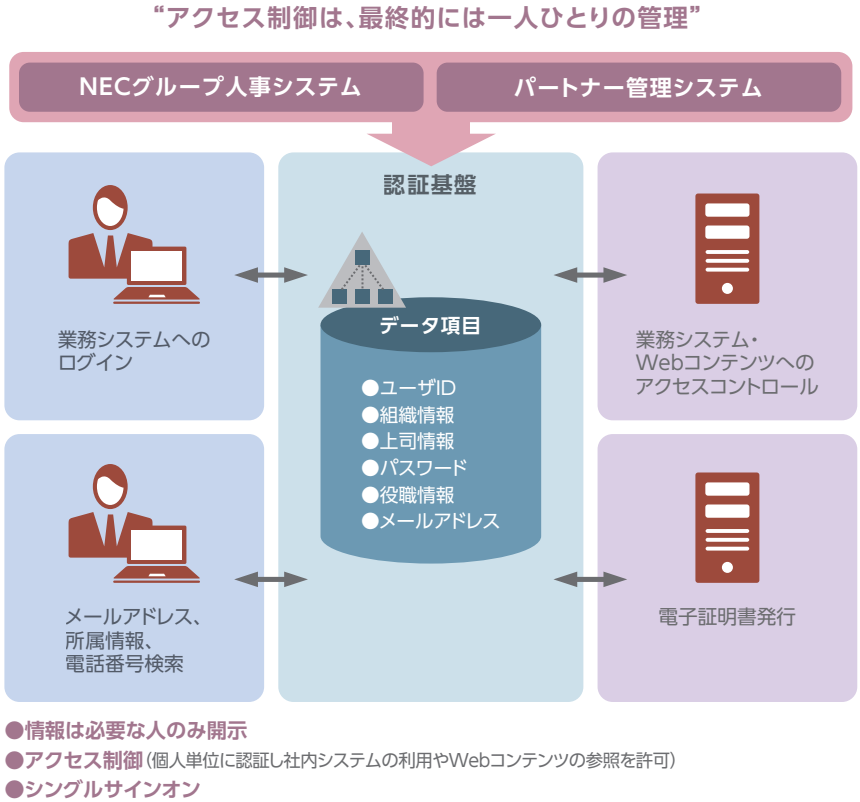
情報セキュリティにおける管理の基本は、個人を認証する仕組みを整えることです。人を特定し認証する仕組みにより、情報資産への適切なアクセスコントロールや電子証明書を利用したなりすまし防止などを実現できます。

情報資産を適切に管理するためには、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。

一方、重要情報を扱うシステムのアクセス制御には、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）の導入も予定しています。

クラウドサービスの認証については、社内の認証基盤との連携を実現することで、社内外サービスのシームレスな認証を可能としています。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に対し、安全・安心、そして快適に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

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基盤をグローバルに整備しています。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、情報機器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】

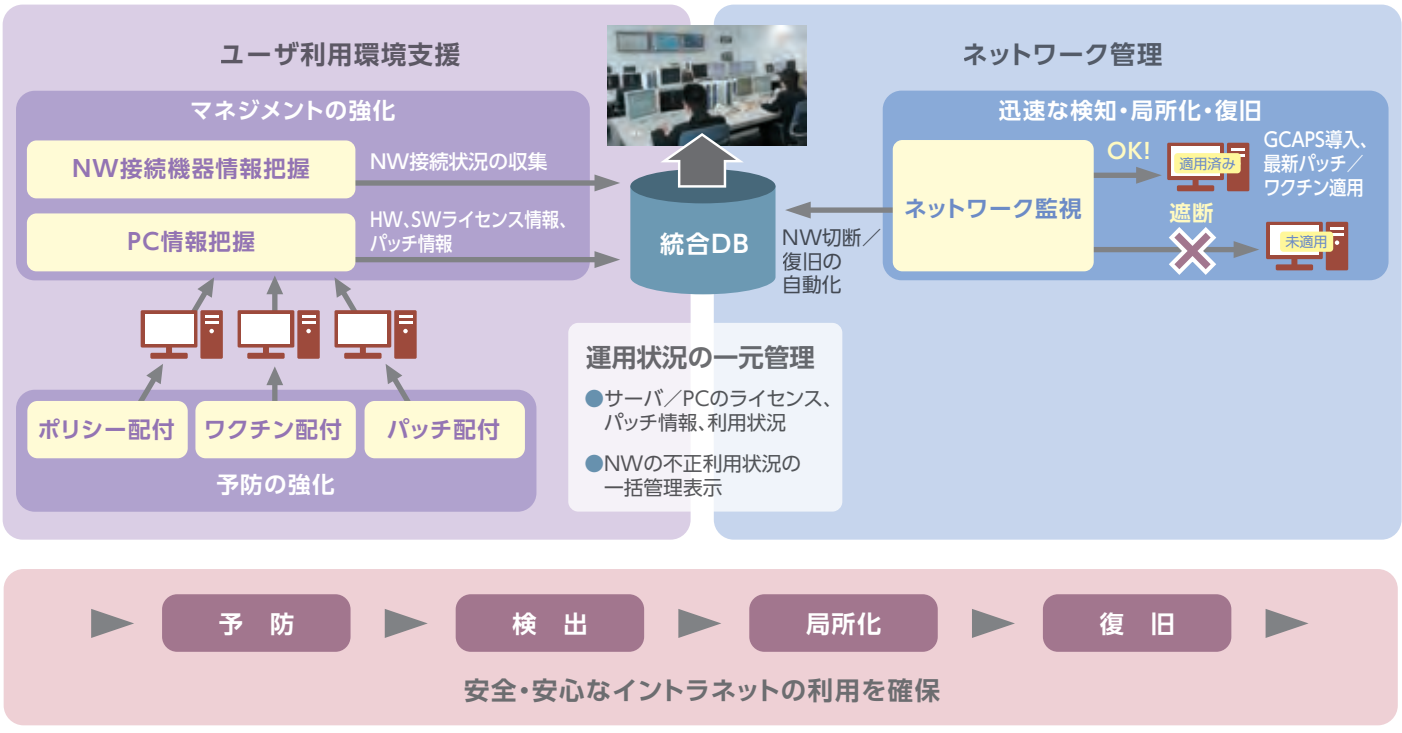
NECイントラネットでは、PCおよびネットワークの状態を把握するソフトウェアの導入を義務化しており、ネットワークやPCの状態を見える化することで、セキュリティリスクを可視化し、すべてのPCに、必要なセキュリティ対策ソフトが確実にインストールされているか、即座に確認できるようにしています。また、セキュリティパッチの配付やウイルス対策ソフトの定義ファイルの更新を自動化し、確実に適用する仕組みも導入しています。さらに使用を禁止するソフトウェアを定義しており、ユーザのソフトウェアの適正利用状況についても監視しています。

【ネットワーク管理】

PCの状態を見える化するとともに、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、社外への通信は、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）などによる制御を実施しています。

【適用状況の一元管理】

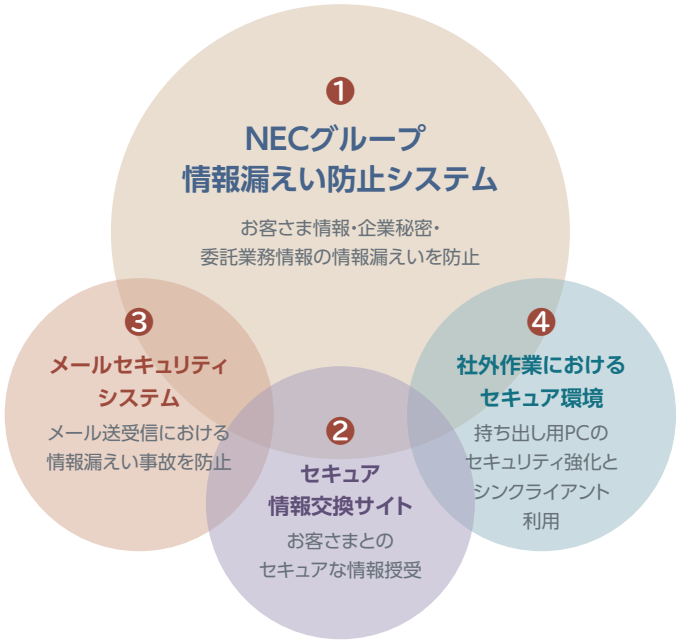
修正プログラムの適用やウイルス対策ソフトなど、セキュリティ対策の実施状況に関するデータは管理システムに集められ、情報セキュリティの管理責任者や推進者が自部門の対応状況をタイムリーに把握できる仕組みになっています。これにより、各種施策の円滑な推進と徹底を容易にしています。



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では、NEC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・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

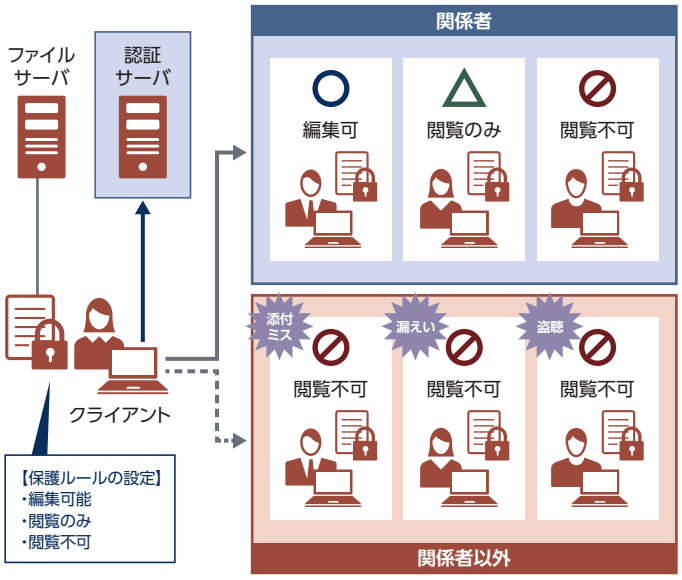
❶ NECグループ 情報漏えい防止システム

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、デフォルト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りしても、情報が防御されているため、漏えいしません。

昨今は、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。

情報漏えい防止システム概要

また、「デバイス制御」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記憶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。

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。

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社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。

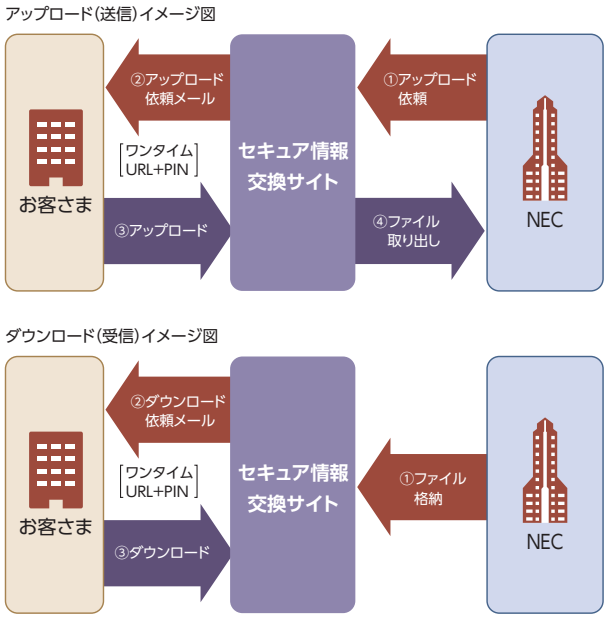
❷ セキュア情報交換サイト

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。



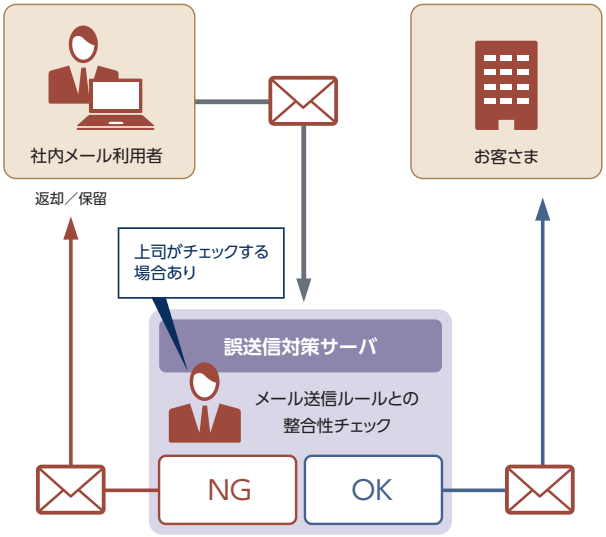
セキュア情報交換サイト

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。操作の利便性のために、メールアドレスや添付ファイルを、Web画面でわかり易く確認できる機能を用意しています。メールアドレスなどのチェックを本人ではなく、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ポップアップする機能を持つOMCA*1を社内に展開し、メール送受信時の安全性の向上をはかっています。

*1 OMCA: Outlook Mail Check Addin



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。

情報セキュリティ人材

NEC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*1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て、毎年見直しを行っています。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。

*1 WBT: Web Based Training

❷ 情報セキュリティの遵守事項への誓約

NEC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、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、サイバー攻撃や紛失事故など、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。職場懇談会を行うことで、対話によって気づきを得るとともに、分析力・判断力の向上をはかっています。

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

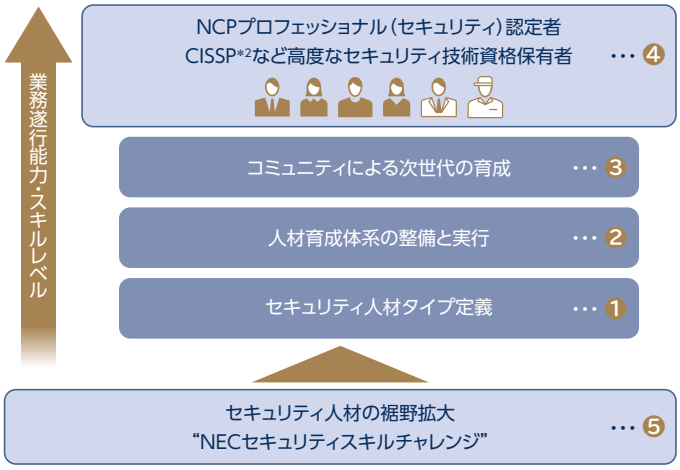
各組織の新任推進者が、情報セキュリティ対策を推進する上で必要な知識（管理体制、役割、セキュリティ施策、推進内容など）を、いつでも学習できる仕組みを整えています。また、各組織で異なるリスクをマネジメントするスキルを向上させるため、事故を題材にした映像を使った演習型の研修なども開催し、実践力を養うとともに、リスク管理や「自律考動」（リスクを自ら考え、判断して行動すること）を推進しています。

❷ 監査人育成

NEC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。標準化された手法で監査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を拡大するために、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できるセキュリティ人材の育成に力を入れています。

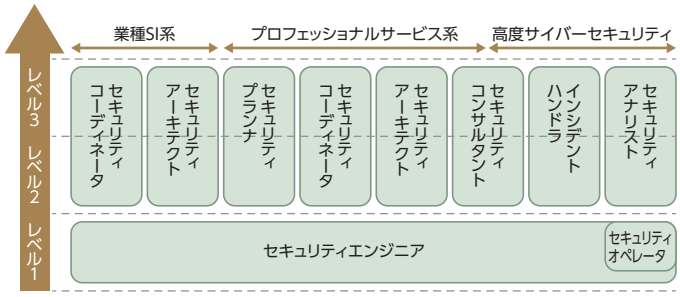


*2 CISSP: Certified Information Systems Security Professional

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

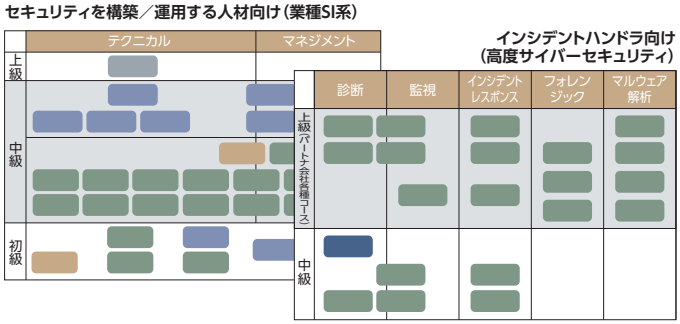
NECとして必要なセキュリティ人材を定義し、人材タイプごとの育成をはかっています。お客さまに必要なセキュリティ人材定義とも連動し、さらなるブラッシュアップを継続しています。



セキュリティ人材タイプ

❷ 人材育成体系の整備と実行

株式会社サイバーディフェンス研究所などのNECグループおよび、お取引先と連携し、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います。



研修コース

❸ 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。

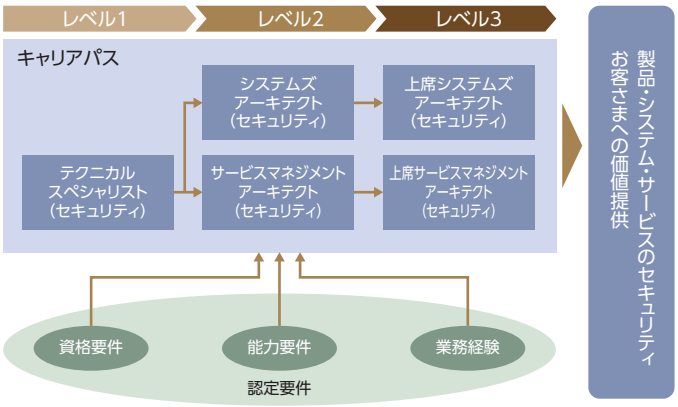
❹ トップ人材を維持する認定制度と高い処遇

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や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。



- 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)

❺ 全社的CTFの実施

NECグループの全社員を対象に、社内CTF*3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。2017年度は参加者が約1,200名に達しており、セキュリティ人材の裾野拡大につながっています。

*3 CTF: Capture the Flag

お取引先と連携した情報セキュリティ

NEC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ともに、NEC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。

情報セキュリティレベル

NEC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項です。

❶ 契約管理

NEC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から委託された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

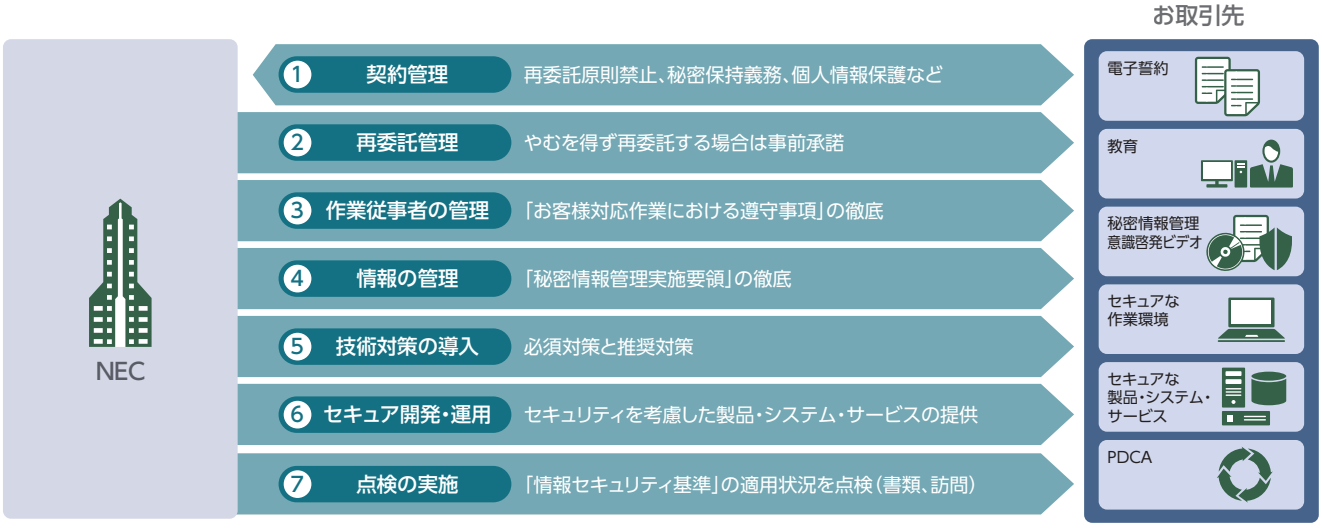
NECから委託された業務で取り扱う秘密情報の管理について、「お取引先様向け秘密情報管理実施要領」(秘密表示、持ち出し管理、用済み後廃棄・返還など)を定め、調達要件として実施の徹底を推進しています。

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(可搬型電子機器や外部記憶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のお客さま向けの製品・システム・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



お取引先への情報セキュリティ対策

開発や、製品・システム・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、NECの標準的な仕組み（体制、手順）のもと、毎年（新規お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が連携し、全国のお取引先を対象に、毎年（対象約1,500社、うちISMS認証取得会社約800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10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利用

セキュリティ事故の分析結果を踏まえ、毎年、情報セキュリティ説明会で啓発ビデオを上映するとともに、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、サイバー攻撃、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に登録すると、全お取引先における自社の位置付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の情報セキュリティ対策をより円滑に実施できるように、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

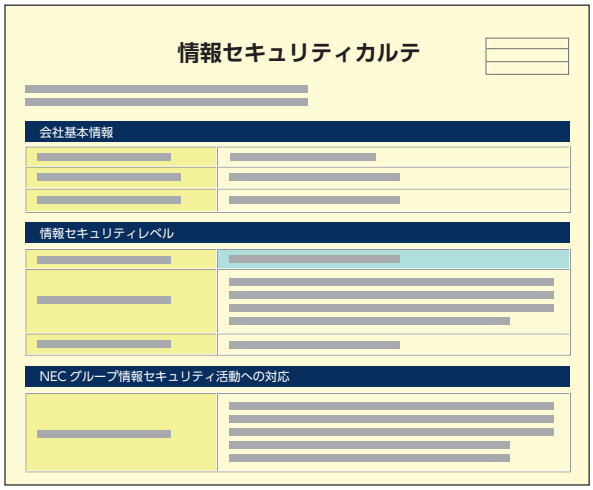
お取引先に対する点検は主に書類点検と訪問点検から構成されており、定期点検に加え、適宜、臨時点検を実施しています。

書類点検は、NECと取引のある会社約1,500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見直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。点検結果は報告書の形で各社にフィードバックされます。お取引先はNECの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。加えてお取引先は登録内容を都度更新でき、NECは常に最新の状態を確認することができます。

訪問点検はNEC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の点検担当者として認定された者（約100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、NECは改善が必要なお取引先に対して、改善状況を確認して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

セキュアな製品・システム・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では、製品・システム・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・システム・サービスをセキュアに開発・運用するため、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500名）で構成されています。WGでは、製品・システム・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」などを通じて各部門の推進者に展開され、推進者によって部門内へ施策の周知徹底、実施状況の点検、改善などが継続的に実施されています。

❷ 全社標準やそれに基づくガイドライン等の整備

NECの全社標準である日本電気工業標準において、「セキュア開発・運用管理規程」が定められています。本規程では、NECでのセキュア開発・運用推進体制、部門内で実施するタスク、関連する各種基準など基本的な事項を定めています。

また、セキュリティを担保するためのタスクや基準の実践的な事項は各種ガイドライン・テンプレートとして策定しています。最近は、IoTのセキュリティリスクが増していることを受け、IoTシステムに対するリスクアセスメントの実施方法やモデルケース毎に求められる具体的なセキュリティ対策（認証機能や暗号化など）などの標準化を進めています。

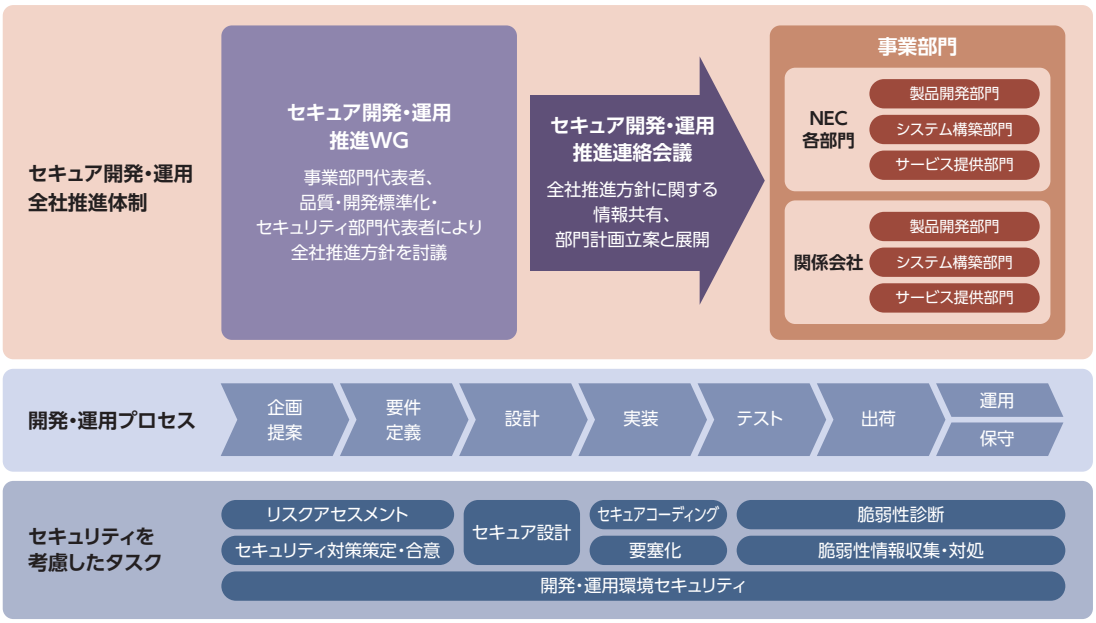
❸ セキュリティ品質の確保

製品・システム・サービスのセキュリティ品質を確保するために、開発・運用プロセスにおいてセキュリティタスク（リスクアセスメント、セキュア設計、要塞化、脆弱性診断など）が実施されていることを確認するためのチェックリストを活用しています。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が考慮されていることに加え、新たな脅威に対するセキュリティ対策についても随時反映されています。

また、本チェックリストに基づいたセキュリティ対策状況を見える化するために「セキュア開発・運用点検システム」を活用しています。本システムによって、約7,000の業務プロジェクトが管理されており、管理者はセキュリティ対策状況を効率的に点検・監査することが可能になっています。

❹ リスクアセスメントの活用

近年、セキュリティリスクの把握と対策の必要性について、経営層がリーダーシップを持って取り組む必要性が指摘されています。2017年11月



セキュア開発・運用 プロセス

に改訂された「サイバーセキュリティ経営ガイドラインVer2.0」において、セキュリティ対策は事業継続性の確保やサイバー攻撃に対する防衛力の向上にとどまらず、ITの利活用による収益力の向上においても重要な要素であるとした上で、セキュリティへの投資は必要不可欠かつ経営者の責務であると指摘しています。必要なセキュリティ対策へ適切に投資するためには、対象のリスクを正しく判断することが重要であると考え、NECではリスクアセスメントの実施に力を入れています。リスクアセスメントとは、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。一般的に、お客様システムの企画・提案段階など開発プロセスの早い段階でリスクアセスメントを行うほど、コストと安全性のバランスを保った費用対効果の高いセキュリティ対策を選定することができます。このため、NECでは開発プロセスの初期からリスクアセスメントを実施し、お客様に提供する製品・システム・サービスにおけるセキュリティを確保しています。

NECでは、社内でリスクアセスメントを行うだけでなく、お客様向けにもリスクアセスメントサービスを提供しています。また、最近では制御システムへのサイバー攻撃の脅威が増していることから、ISO/IEC27001やIEC62443といったセキュリティ規格に対応した、制御システム向けリスクアセスメントサービスについても力を入れて取り組んでいます。

リスクアセスメントの流れ

2 脆弱性への迅速な対応

❶ 脆弱性情報の共有体制

サイバー攻撃から製品・システム・サービスを守るためには、いち早く脆弱性情報をキャッチし、必要な対策を行うことが重要です。日々発見される大量の脆弱性について漏れなく迅速に対応するため、NECは脆弱性のハンドリングを行うPSIRT*1を組織しています。PSIRTは脆弱性情報の収集や分析、IPA*2、JPCERT/CC*3などの外部機関とのPOC*4対応を行っており、PSIRTを中心として収集した脆弱性情報をNECグループ内に展開する体制を構築しています。特に影響範囲が広く、かつ深刻な脆弱性に関しては、その情報をいち早くキャッチし、NECグループ内に広く周知徹底するために早期警戒体制を敷いています。

NECは、情報セキュリティ早期警戒パートナーシップ*5に参画しています。NECが提供する製品に関する脆弱性が発見されると、IPAやJPCERT/CCと連携して一般公開される前に情報を入手し、製品部門が修正パッチの開発など必要な対策を行い、脆弱性情報の公開と同時に修正パッチ等の対策プログラムをお客様に提供できる運用体制を敷いています。

*1 PSIRT: Product Security Incident Response Team
*2 IPA: 独立行政法人情報処理推進機構
*3 JPCERT/CC: 一般社団法人JPCERTコーディネーションセンター
*4 POC: Point of Contact
*5 ソフトウェア製品・Webアプリケーションの脆弱性情報の円滑な普及をはかるための官民連携体制

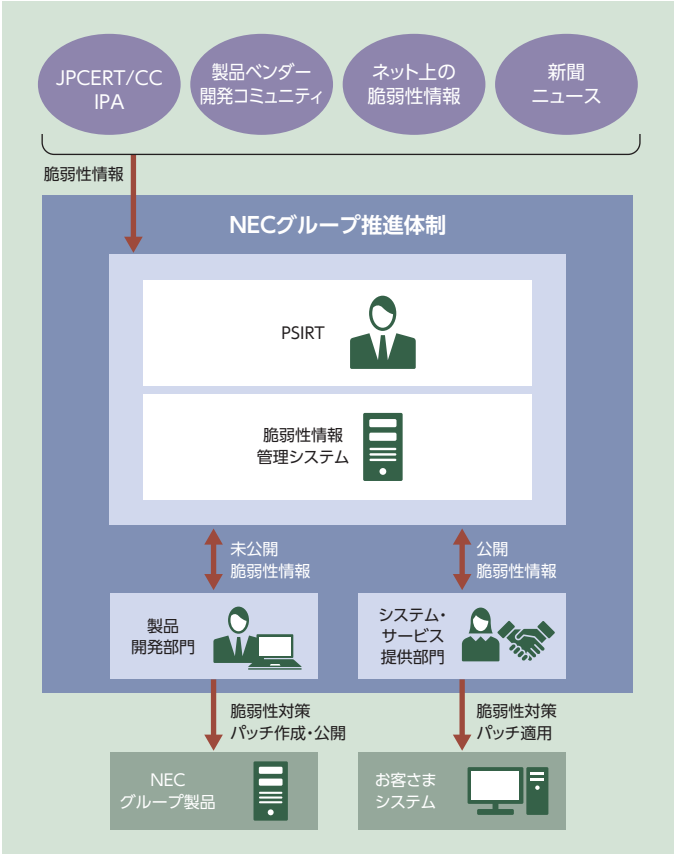
❷ 脆弱性情報の収集、展開

NECは、脆弱性に対して「製品開発事業者」と「SI・サービス事業者」のふたつの側面で対応しています。

製品開発事業者としては、NEC製品に関連する脆弱性情報を前述の情報セキュリティ早期警戒パートナーシップを通して入手して、対処しています。

SI・サービス事業者としては、お客さまシステムに対して漏れのない確実なセキュリティ対策を行うために、製品ベンダーや開発コミュニティ、ネットから脆弱性情報を日々入手し、各業務プロジェクトに対して、そこで利用しているソフトウェアの脆弱性情報をピックアップして展開しています。

入手した情報をNECグループ内に展開、管理するためのインフラとして、独自の脆弱性情報管理システムを運用しています。このシステムを活用し、脆弱性情報の確実な展開と管理を行っています。



脆弱性対応推進体制

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きました。

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、さらには海底から宇宙まで、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あり方も従来の防御・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があり、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　モノのインターネット
*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年株式会社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会社化し、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

株式会社サイバーディフェンス研究所　グループ会社化 (2013年3月)
先進の技術・知見を持つトップ人材を強化

株式会社インフォセック　グループ会社化 (2014年2月)
セキュリティ監視に強いノウハウ、監視業務を強化

実践的サイバー防御演習(CYDER)実施 (2013年9月)
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年度より受託。NECが演習プログラムを作成・運用

北陸先端科学技術大学院大学　寄付講座開講 (2014年11月) (2017年10月)
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
本講座を継続し、培った技術を官公庁・企業へ普及推進

Follow The Sunによる24時間監視体制 (2016年10月)(2017年3月)
「Infosec Austria」「Infosec America」を設立。日本を含めた世界3拠点の時差を利用することにより、24時間のセキュリティ監視体制(Follow The Sun)を確立

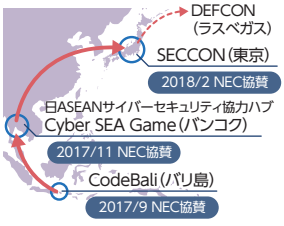
NEC セキュリティスキルチャレンジ開催 (2016年2月)
NECグループ内で、実践的なセキュリティ人材の発掘と育成のためのセキュリティ技術コンテストを2016年より継続的に開催

日本のサイバー捜査官の草分け 木村公也氏を採用 (2017年4月)
サイバー犯罪捜査の第一線で活躍してきた、木村氏を採用。
サイバーセキュリティ関連ソリューションの企画・開発、営業アドバイス、人材育成、講演など。JC3人材育成も担当

IPA 産業サイバーセキュリティセンター 参加 (2017年4月)
重要インフラ、社会基盤のサイバーセキュリティリスクに対応する人材・組織・システム・技術を生み出すことを目的とした同センターの人材育成プログラムに参加

英国のITサービス企業NPS社*5を買収 (2018年1月)
海外でのセーフティ事業拡大を加速　*5:Northgate Public Services Limited

グローバルでの人材育成
CodeBali※6、日・ASEANサイバーセキュリティ協力ハブ※7を通じ、各国でCYDERによる演習、およびセキュリティコンテストを実施。優勝チームはSECCON※8へ参加



※6:Id-SIRTII/CC(インドネシアのサイバーセキュリティ中核組織)主催の国際カンファレンス
※7:総務省が推進する日・ASEAN統合基金2.0(JAIF)のプロジェクト
※8:国内最大級のセキュリティコンテスト(日本ネットワークセキュリティ協会(JNSA)主催)

2015年に経済産業省およびIPA*9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*10の方に利用される機会が増えており、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。

*9 IPA:独立行政法人情報処理推進機構
*10 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。

情報基盤強化

制御システムセキュリティセンター(CSSC) 参画 (2013年11月)
経済産業省官民連携プロジェクトで、重要インフラ機器・制御システムのセキュリティを確保

日本サイバー犯罪対策センター(JC3) 参画 (2014年11月)
産学官(警察)それぞれがもつサイバー空間の脅威への対処経験を集約。
脅威の大本を絶ち、被害の防止を目指す。
NEC シニアオフィサー清水隆明が代表理事に就任

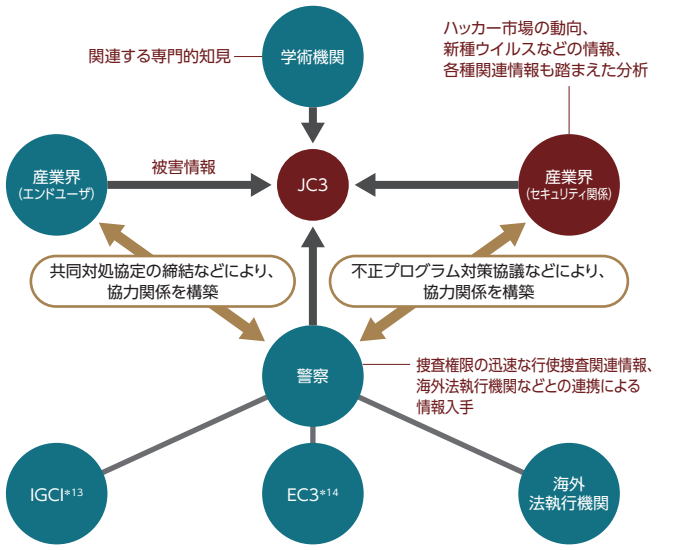
米国国土安全保障省(DHS)の官民情報共有 AIS*11参加 (2017年3月)
米国国土安全保障省(DHS)が推進する、官民でサイバー攻撃の脅威情報を迅速に共有する枠組み「AIS」に日本企業として初めて加入
*11:Automated Indicator Sharing

ICT-ISAC発足に参画 (2017年3月)
多様な事業者がサイバー攻撃等の情報収集・分析および対応について情報共有し、業界の枠を超えて連携・協調し、脅威に対処するために発足したICT-ISACに参画(NECは前身となるTelecom-ISACから参画)

産業横断サイバーセキュリティ人材育成検討会 参画 (2016年1月) (2017年4月)
日本電信電話株式会社、株式会社日立製作所とともに、サイバーセキュリティ人材育成に向けた検討会を発足。2017年からは「一般社団法人サイバーリスク情報センター(CRIC)」内組織に移行し、情報共有についても取り組みを開始

制御システムセキュリティセンターへの参画をはじめ、2014年には日本サイバー犯罪対策センター(JC3*12)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。

*12 JC3:Japan Cybercrime Control Center



*13 IGCI: The INTERPOL Global Complex for Innovation　*14 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

サイバー犯罪に対する国際レベルでのセキュリティ強化を目指し、NECは、2012年、インターポール（国際刑事警察機構）とサイバーセキュリティ対策でパートナーシップ協定を締結しました。また2015年には、インターポールがシンガポールに開設し、本稼働を開始した「The INTERPOL Global Complex for Innovation」（IGCI）に、デジタル犯罪捜査のための中核システムや製品、技術支援要員を提供しました。IGCIは、デジタルセキュリティの領域での研究・開発、サイバー犯罪や犯罪者の調査・分析など、各国当局に重要な支援を行っています。

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。この流れは衰えず、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います。

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いきます。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*15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。

*15 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、ブラジルに加え、欧州、北米にも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(SOC)のグローバル化

NEC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SOC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日本のサイバーセキュリティ・ファクトリーが2014年に稼働開始しました。その後、シンガポールのサイバーセキュリティ・ファクトリーを始めとして、欧州、北米にもSOCを開設しました。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、お客さまに安全・安心を提供してまいります。

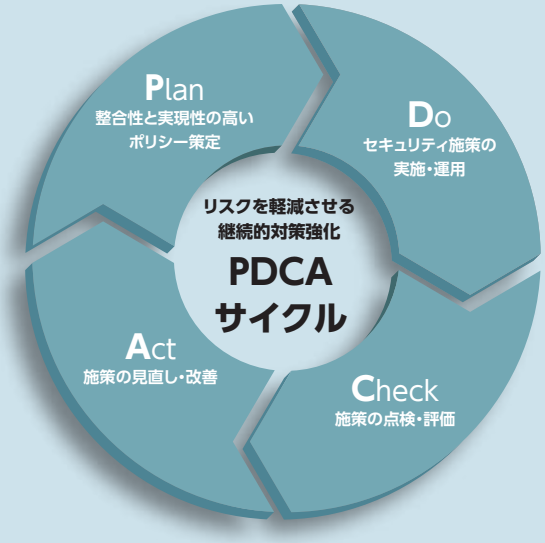
NECのSOCから提供されるセキュリティサービスでは、24時間365日のセキュリティ運用監視サービスをはじめ、高度なセキュリティインテリジェンス、インシデントレスポンス支援など、さまざまなサイバーセキュリティリスクに対応した対策サービスを提供しています。その他にもネットワーク監視やヘルプデスクなど、お客さまICT基盤の安定・継続的な運用をOneNECで支援できる設備・体制を整えています。

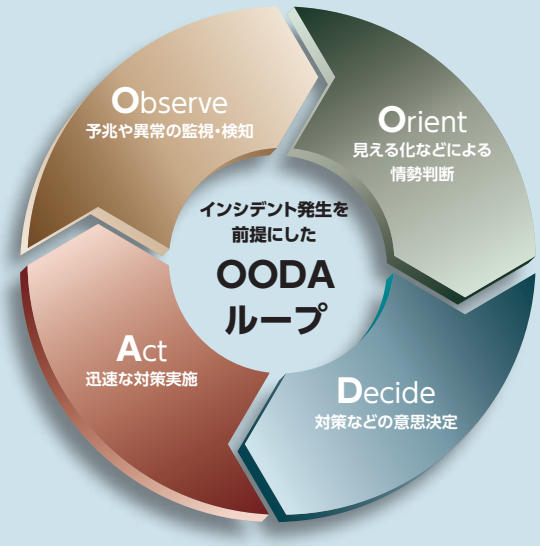
サイバーセキュリティ・ファクトリー

5 自社運用ノウハウを基にセキュリティ強化をサポート

サイバー攻撃からのリスクを減らす計画的な対策と、組織全体の継続的なセキュリティ強化を図ります。

サイバーセキュリティ対策は、導入すれば終わりというわけではありません。高度化・巧妙化が進むサイバー攻撃に対抗するには、セキュリティ対策も計画的に強化し続けることが重要です。NECでは、さまざまなセキュリティ対策の効果的な連携による組織全体のセキュリティ強化とともに、ポリシー策定から対策、効果の点検、改善というPDCAサイクルにもとづき、脆弱性を解消するための継続的な対策を支援します。





インシデント発生時の適切な状況判断や迅速な対応もサポートします。

PDCAサイクルによるセキュリティリスク管理に加え、サイバー攻撃への備えとして特に重要になってくるのが、不正侵入やマルウェア感染などのインシデント発生を前提とした対策です。異常事態のすばやい検知、緊急時におけるタイムリーな意思決定や対応によって、被害の軽減がはかれます。NECでは、監視・検知、情勢判断、意思決定、対策実施という流れによる「OODA(ウォーダ)ループ」という概念を取り入れ、適切でスピーディなインシデント対応を支援します。

PDCAサイクルとOODAループ

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。

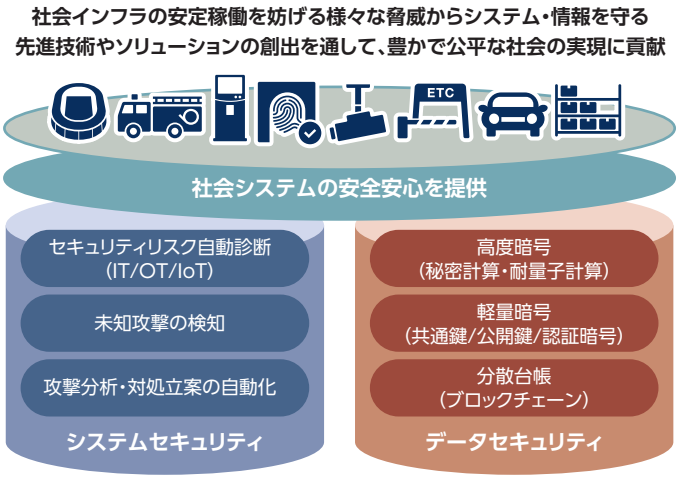
1 研究テーマのコンセプト

NECは、「Futureproof Security安心の先へ。」というスローガンのもと、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、巧妙化・高度化するサイバー攻撃に対して、AIを活用したセキュリティリスクの自動診断、未知のサイバー攻撃の検知、攻撃の手口やシステムに及ぼす影響の自動分析、効果的な対応策の自動立案など、最先端のセキュリティ技術を開発しています。

データセキュリティは、情報漏えい事故の根絶に向けて、暗号化したままデータ処理を実現する「秘密計算技術」やIoT*1機器に暗号機能を実装するための「軽量暗号」を開発しています

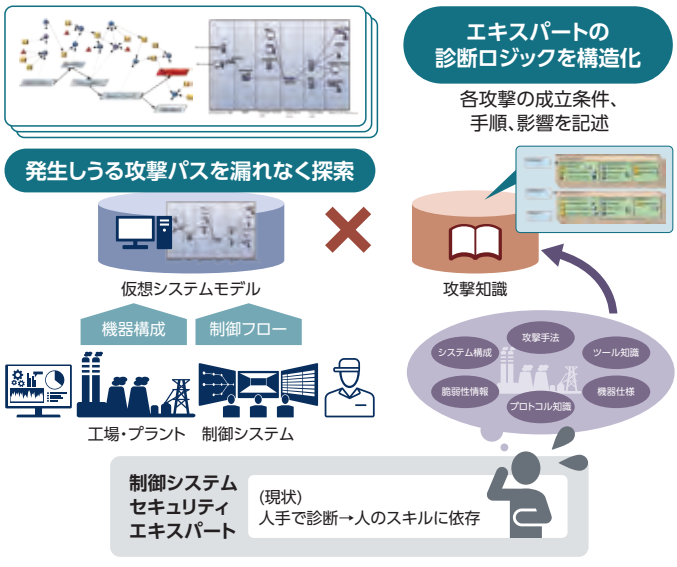
*1 IoT: Internet of Things　モノのインターネット



NECのセキュリティ研究

2 セキュリティリスク自動診断技術

工場やプラントなど、「止められない」システムに潜在するセキュリティリスクを網羅的に洗い出します。この技術は、複雑な制御システムを仮想空間上にモデル化し、守るべき対象へ攻撃が到達する可能性（攻撃パス）を探索し、攻撃によって引き起こされる物理的な被害を提示します。また、制御システムのセキュリティエキスパートと協力し、専門家が経験的に利用している個々の攻撃の知識を計算機が自動診断できるように構造化します。これにより、システムの運用に影響を与えることなく、最新の攻撃知識を用いていつでもセキュリティ診断を行うことができます。



セキュリティリスク自動診断技術

3 AIを活用したセキュリティ

❶ 分析官作業支援AI

標的に応じた攻撃手段の多様化や個別化、潜伏や痕跡消去などの巧妙化が進展している一方で、対抗手段の1つとしてマルウェアやその振る舞いの自動検知にAI技術が利用され始め、成果が現れてきています。機械学習を用いたAI技術は、従来のシグネチャやルールによる方法に比べて、亜種や未知のマルウェアを検知可能にし、攻撃の多様化への対抗手段として有望です。しかしながら、このような機械学習型AIは、人手で知識を与えなくてよい替わりに大量の学習用データが必要になり、ターゲットが限定された標的

型攻撃では学習に十分なデータが収集できない場合があるほか、学習した判断基準をセキュリティの分析官が確認したり、部分的に変更することも容易ではありません。

そこで、NECでは、セキュリティのインシデント対応のように、攻撃の状況を周囲のコンテキストとともに推論し、人と連携しながら問題を解決する新しい論理思考型のAI技術を研究しています。論理思考型AIには、結果を導き出した経緯を人間にも分かる形で提示できるほか、推論のための知識を部分的にも追加・修正することが容易という利点があります。この技術により、センサで検知した異常を起点に関連する事実としてのデータを可能な限り集め、サイバー攻撃に関する知識を用いてマルウェアや攻撃者自身がどのような操作を行っているのかを推定します。最終的に攻撃目的が達成された状態までの流れを導出し、そこに含まれる各操作や途中の状態を得られている事実と照合しながら、全体を検証していきます。これにより、概ね攻撃の流れが妥当と判断できたら、その流れを止めて攻撃への対策が完了するまでの手順も導出し、分析官に確認をとるといったプロセスの実現を目指しています。

NECは、機械学習型AIと論理思考型AIそれぞれの特徴を活かして分析官の分析作業を支援することで、高度なサイバー攻撃に効率的に対応することが、AIを活用したセキュリティの未来の姿と考えています。

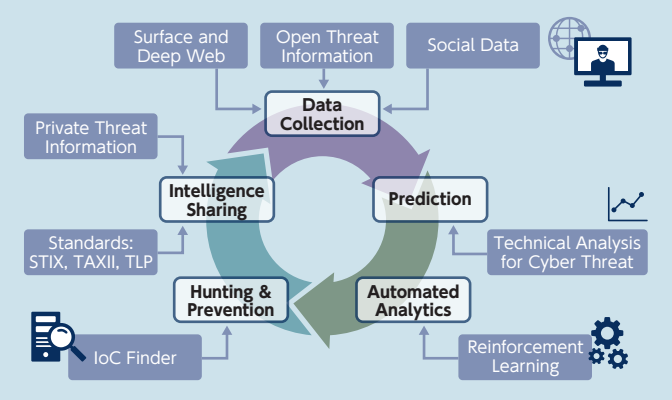
❷ オープンソースインテリジェンスを活用した脅威分析AI

国内外の重要施設や企業を狙ったサイバー攻撃の犯行予告がソーシャルメディア上で流布し、攻撃ツールやインフラがディープウェブ*2上で取引される現状から、サイバー脅威分析におけるオープンソースインテリジェンスの重要性が増しています。

こうした背景から、NECでは、金融工学分野で用いられるテクニカル分析手法によって脅威のトレンドがピークに達する兆候を掴む技術と、機械学習型AIの一種である深層強化学習によってサイバー攻撃の全体像を分析する技術を研究しています。これらの技術の連携によって、膨大なオープンソース情報からサイバー攻撃への迅速かつ的確な事前対策の自動化を実現します。

NECはサイバー攻撃予防技術の研究活動を推進し、安全・安心で持続可能な社会の実現に今後も貢献してまいります。

*2: 一般の検索エンジンでは検索できないWebサイト



セキュリティマネジメント

4 暗号・秘密計算技術

❶ 軽量暗号

NECは、リソースが少ないIoT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年に発表し、2015年には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*3を発表しました。これらの暗号を活用することで、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。

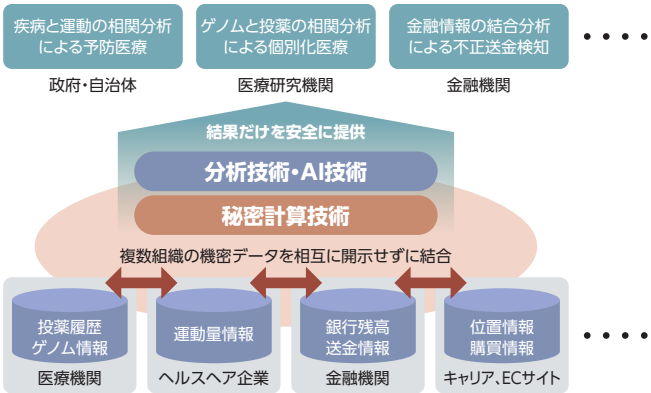
*3 OTR: Offset Two-Round

❷ 秘密計算

秘密計算はデータを暗号化したままで処理することを可能にすることでマルウェアや内部犯行に対しても強固な情報漏洩の防止を実現します。

秘密計算は性能が課題でしたが、複数サーバにデータを秘密分散したままの状態で処理するマルチパーティ計算により、NECは2016年に最高性能を達成する方式の開発に成功しました。認証システムにおける実証では秒間1万件以上の認証処理を実現し、大規模組織における用途においても実用可能であることを示しました。

マルチパーティ計算は、情報漏洩の防止に加え、複数組織がそれぞれ持つ秘密情報を、隠したまま共同で利用して、新たな知見を生み出すことも可能にします。今後、データ利活用基盤のコア技術として実用化すべく、マルチパーティ計算の研究開発を推進します。



秘密計算によるデータ活用

5 クラウド技術

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 VALWAY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チャイナ・ソフトジャパン株式会社
- 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・センサ株式会社
- 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
- 株式会社インフォセック
- 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
- 株式会社ブリースコーポレーション
- 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
- 日本電気通信システム株式会社
- 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
- ランゲージワン株式会社

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
- アビームシステムズ株式会社
- NEC VALWAY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
- 株式会社ブリースコーポレーション
- 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
- KISドットアイ株式会社
- 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）
- NEC ファイアウォール SG ソフトウェア
（ファイアウォール用ソフトウェア）
- 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

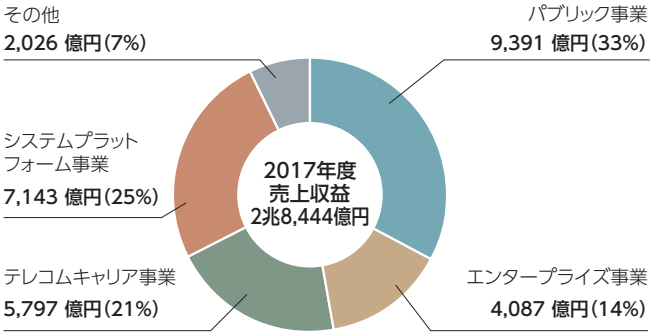
会社概要

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	111,200名※
連結子会社数	303社※

※2018年3月31日現在

事業紹介

セグメント別売上収益(構成比)



※2018年3月31日現在

NEC Way

NEC Wayとは

NECグループ一人ひとりが持つべき考え方、業務への取り組み姿勢を「NEC Way」として体系化しています。

企業理念の実践や具体化の土台となるのは、倫理観や、「企業行動憲章」および「行動規範」というNECグループで定めている行動指針です。

そして、NECが実現したい社会像・企業像である「NECグループビジョン」や「Orchestrating a brighter world」の実現に向け、従業員は、「NECグループバリュー」と総称する4つの価値観(イノベーションへの情熱、自助、共創、ベタープロダクツ・ベターサービス)と行動原理と行動規範に則って、日々の業務に取り組んでいます。また、2016年には、社会価値の創造に向け、求められる人財を、高い視座と広い視野を持ち、枠を超えて挑戦し、やり遂げる人であることと定義しました(「人財哲学」)。

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

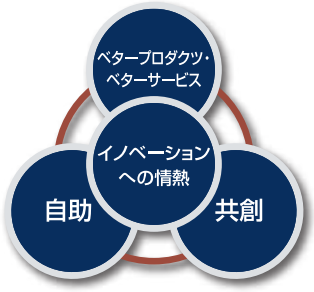
NECグループビジョン

企業理念に基づいて、NECグループが実現したい社会像・企業像をまとめました。

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

2018年７月発行
© NEC Corporation 2018
Cat.No. K99-18070011J