\Orchestrating a brighter world NEC

情報セキュリティ報告書 2024

Truly Open,Truly Trustedの実現

NECは、情報セキュリティの確保を経営上の重要事項と位置づけ、国のガイドラインや国際標準にも準拠し、社会から継続的に信頼される企業を目指します。

なかたに　のぼる
中谷　昇

日本電気株式会社
執行役 Corporate EVP
兼 CSO（チーフセキュリティオフィサー）
兼 NECセキュリティ株式会社 代表取締役社長

全世界がオープンに繋がり、AI利用が拡大する現在、サイバー攻撃の高度化やビジネス化、クラウド活用による情報漏えいリスクの増大、経済安全保障における情報管理の課題にどう対応するかが、国家・企業問わず重要な問題となっています。

このような状況を踏まえ、NECでは「ゼロトラストセキュリティプラットフォーム」の構築を推進しており、パスワードレス化などCISA*1のゼロトラスト成熟度モデルを踏まえた堅牢性と柔軟性を備えた対策をグループ全体で実施しています。

サイバーセキュリティ対策では、経済産業省の「サイバーセキュリティ経営ガイドラインVer3.0」や2024年2月に10年ぶりに改訂されたNIST（米国標準技術研究所）の「Cyber Security Framework（2.0版）」に基づき、深刻化するサイバー攻撃に対するインテリジェンス（事前防御）やレジリエンス（攻撃からの回復能力）を強化、実行する体制を構築しています。また、データドリブンサイバーセキュリティとしてダッシュボードによりサイバーセキュリティリスクを可視化。全従業員に示し、データを起点とした迅速な経営判断と現場の自律的なアクションに繋げ、Govern（統制）を実現しています。この取り組みを評価いただき、公益社団法人企業情報化協会の「2023年度IT優秀賞（マネジメント領域）」、および一般社団法人日本デジタルトランスフォーメーション推進協会の「日本DX大賞2024 特別賞」を受賞いたしました。

また、設計段階からセキュリティを考慮した「セキュリティ・バイ・デザイン」に基づき、高品質で安全なサービスを提供するために、サプライチェーンも含めた対策強化に取り組んでいます。DXを推進するセキュリティ人材を育成するために、国際的な情報セキュリティ資格であるCISSP*2の取得を推進するとともに、さらに教育機関と協力して将来の人材育成にも貢献しています。このような取り組みが評価され、日本IT団体連盟の「サイバーインデックス企業調査2023」で最高位の二つ星を獲得しました。

今後も、エンタープライズリスクマネジメントを実践するとともに、世界No.1*3と評される顔認証などを利用した「ウォークスルー入退管理」、「生成AIのセキュリティ活用」をはじめとする、社内で実装済みの最先端技術を提供することにより、社会から継続的に信頼される企業になることを目指します。

NECは、Purposeに「Orchestrating a brighter world」を掲げ、社会課題をICTの力で解決し、人が豊かに生きる「安全」「安心」「効率」「公平」な社会の実現に貢献してまいります。本報告書では、情報セキュリティに関する最新の取り組みをご紹介していますので、ご一読いただければ幸いです。

*1 CISA: Cybersecurity and Infrastructure Security Agency（米サイバーセキュリティ・インフラストラクチャセキュリティ庁）の略称。
*2 CISSP: Certified Information Systems Security Professional（セキュリティ プロフェッショナル認定資格制度）。
*3 米国国立標準技術研究所（NIST）による顔認証技術の精度評価で第1位を複数回獲得。

本報告書に関するお問い合わせ

日本電気株式会社
CISO統括オフィス
〒108-8001 東京都港区芝五丁目7-1 NEC本社ビル
03-3454-1111（大代表）

★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。

「情報セキュリティ報告書 2024」刊行にあたって

本報告書は、経済産業省が策定する「サイバーセキュリティ経営ガイドライン」Ver 3.0をベースに、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について、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、2024年6月までの取り組みを対象に掲載しています。

経済産業省「サイバーセキュリティ経営ガイドライン」Ver 3.0
重要10項目とのコンテンツ対比

- 指示1 サイバーセキュリティリスクの認識、組織全体での対応方針の策定
- 指示2 サイバーセキュリティリスク管理体制の構築
- 指示3 サイバーセキュリティ対策のための資源(予算、人材等)確保
- 指示4 サイバーセキュリティリスクの把握とリスク対応に関する計画の策定
- 指示5 サイバーセキュリティリスクに効果的に対応する仕組みの構築
- 指示6 PDCAサイクルによるサイバーセキュリティ対策の継続的改善
- 指示7 インシデント発生時の緊急対応体制の整備
- 指示8 インシデントによる被害に備えた事業継続・復旧体制の整備
- 指示9 ビジネスパートナーや委託先等を含めたサプライチェーン全体の状況把握及び対策
- 指示10 サイバーセキュリティに関する情報の収集、共有及び開示の促進

Contents

情報セキュリティ推進フレームワーク

指示1

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。

NECグループは、情報セキュリティの確保を経営上の重要事項と位置づけ、お客さまやお取引先からお預かりした情報資産およびNECグループの情報資産をサイバー攻撃などの脅威から守るとともに、セキュアな製品・システム・サービスをご提供します。増大するリスクに対してTruly Open, Truly Trustedな社会の実現を通じて、安全・安心・公平・効率という社会価値を創造し、誰もが人間性を十分に発揮できる持続可能な社会の実現を目指します。

NECグループでは、サイバー攻撃対策、お取引先と連携した情報セキュリティ、セキュアな製品・システム・サービスの提供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を3本柱に、NECグループに対する情報セキュリティガバナンスの徹底に取り組み、総合的かつ多層的な情報セキュリティの維持・向上をはかっています。

情報セキュリティ基本方針や全社規程の制定、共通的な情報セキュリティ基盤の整備を行い、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、モニタリングや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

指示2

事業活動から生じるリスクを的確にコントロールするために、
NECグループ全体で情報セキュリティレベルを効率的に高める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グループは、情報セキュリティの確保が経営上の最重要課題の一つであると認識し、これに対する投資を企業経営に必要不可欠な責務と位置づけています。グループ全体で「NECグループ経営ポリシー」を定め、各種ルールの共通化と制度・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確立しています。

情報セキュリティガバナンスに基づき、経営層は関係会社や海外現地法人を含めたグループ全体のモニタリング結果を踏まえて、年に1回のセキュリティ目標の見直し、および改善・是正の指示を実施します。

経営層・管理者層のサイクルとそれを監督する機能により、グループ全体の最適化を追求し、ステークホルダーに対し適切な情報を開示し、企業価値の持続的な向上をはかります。

2 | NECグループの情報セキュリティ推進体制

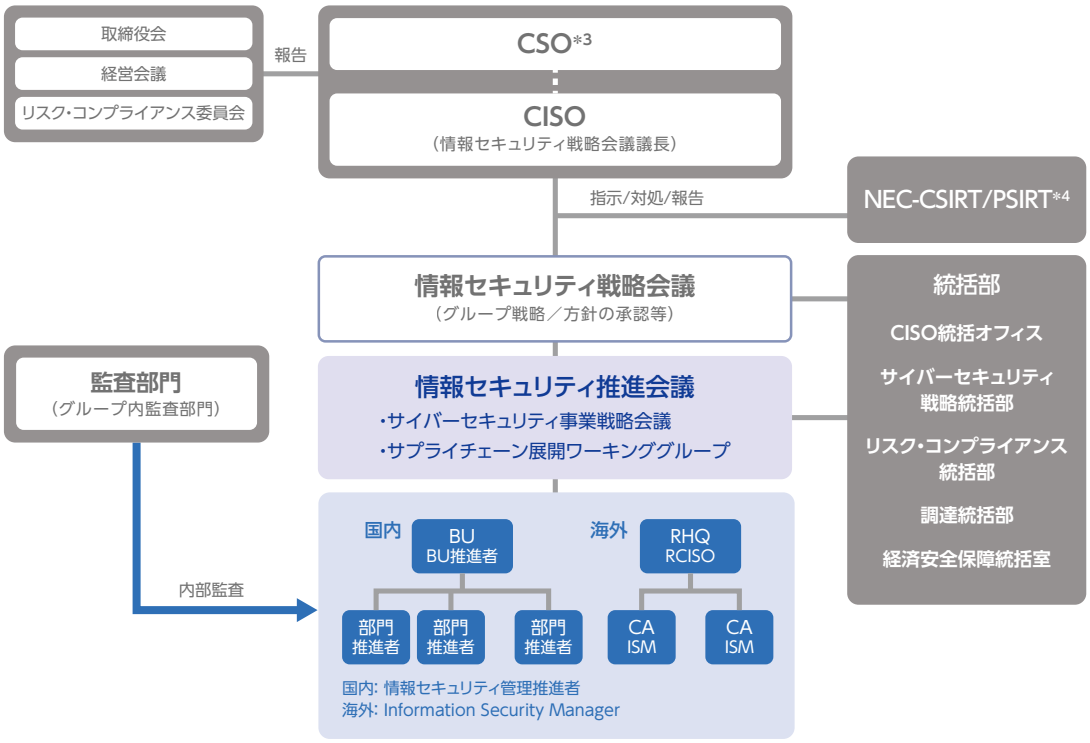
本体制は、情報セキュリティ戦略会議と下部組織、各関連組織で構成されます。情報セキュリティ戦略会議はCISOが議長を務め、情報セキュリティ施策の審議・評価・改善、事故の原因究明と再発防止策の方向付け、情報セキュリティビジネスへの成果活用などを審議します。また、ここで決定した施策の運営状況は、定期的に社長に説明し、了承を得ています。

CISOは、情報セキュリティ対策を推進するCISO統括オフィスと、サイバー攻撃を監視しインシデント発生時には迅速に収拾をはかるCSIRT*2を統括します。情報セキュリティ推進会議やワーキンググループは、セキュリティ実装の推進計画、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。

各部門長は情報セキュリティ管理責任者として主管するグループ会社も含め情報セキュリティの確保に責任を負い、ルールの周知徹底、施策の導入・運用、実施状況のモニタリング・見直し・改善などを継続的に実施します。

また、各海外拠点にRegional CISO*1を設置し、担当領域におけるセキュリティ管理とその結果に責任を持たせることで、ガバナンスを強化しています。

NECグループ情報セキュリティ推進体制



*1 CISO: Chief Information Security Officer　*2 CSIRT: Computer Security Incident Response Team　*3 CSO: Chief Security Officer　*4 PSIRT: Product Security Incident Response Team

情報セキュリティマネジメント

指示2 指示6

各種施策をNECグループ全体に定着させるため、情報セキュリティマネジメントや
セキュリティポリシーの体系を確立し、その維持・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、PDCAサイクルを継続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、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、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。

2 | 情報セキュリティに関するポリシー

NECでは、全グループの指針として「NECグループ経営ポリシー」を展開しています。まず、「NECグループ情報セキュリティ基本方針」*1を公開し、情報セキュリティ全般に関する規程、企業秘密管理に関する規程、ITセキュリティに関する規程などを体系化しています。

さらに、個人情報保護については、「NEC個人情報保護方針」*2を制定後、NECは2005年に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）」、「個人情報保護法」に準拠しています。また、2015年には「番号法」準拠のマイナンバー管理を追加しました。2022年に施行された改正個人情報保護法にあわせ、個人情報の保護規程やマニュアル類を見直しています。

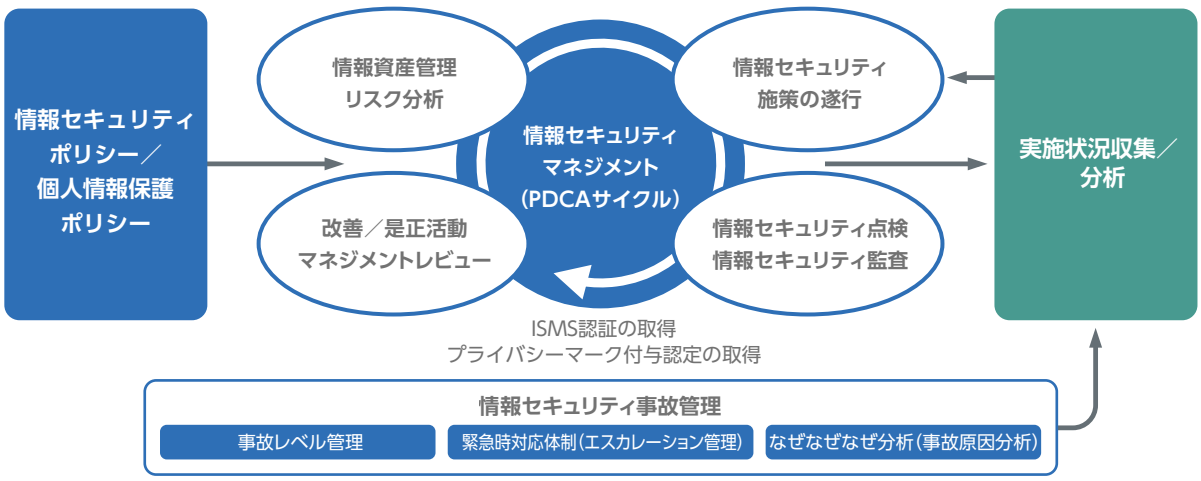
個人情報は、グループ共通の保護管理レベルで運用を推進し、NECグループで31社（2024年6月現在）がプライバシーマーク付与認定を取得しています。

3 | 情報セキュリティリスク管理

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の分析手法と、詳細リスクの分析手法とを使い分けてリスク評価と対策を実施しています。まずベースラインとなる基準で共通に実施すべきセキュリティを維持し、高度な管理が必要な場合は詳細リスク分析を行い、きめ細かな対策を実施します。

NECの情報セキュリティマネジメント



*1 NECグループ情報セキュリティ基本方針　https://jpn.nec.com/profile/governance/security.html
*2 NEC個人情報保護方針　https://jpn.nec.com/site/privacy/index.html

❷ 情報セキュリティ事故のリスク管理

情報セキュリティ事故の報告を義務付け、報告内容の分析結果をPDCAサイクルへ乗せてリスク管理を行います。事故情報はNECグループ全体で一元管理し、件数の変化、組織別や事故の類型別の傾向などを分析して、共通施策に反映しつつ効果測定を実施します。

❸ 事業継続に向けた取り組み

主要なシステムについて、サイバー攻撃に対する事業継続の観点による第三者評価を実施しています。また、事案発生時に適切に復旧するための演習を行っています。

4 | 重要情報管理

❶ Three Lines Model

NECグループではThree Lines Modelに関する情報管理の考え方に沿い、第1ラインであるリスクオーナー部門が情報を厳格に管理するとともに、第2ラインであるリスク管理部門は第1ラインのモニタリングや第1ラインのリスクマネジメントを支援します。さらに第3ラインである監査部門によって、管理状況を確認する仕組みを整えています。

❷ 重要情報の管理

NECグループでは、取り扱う企業秘密を秘密区分によって分類して管理しています。各組織では、当該組織で取り扱う情報を細分化し、どのような情報がどの秘密区分に該当するのかを明確にして、認識ミスや管理漏れのない情報管理を実現しています。また、重要な情報に対して、その重要度に応じた取り扱い・保管管理を定めており、情報漏えいなどの対策を徹底しています。

5 | 情報セキュリティサーベイ・監査

❶ 情報セキュリティサーベイ

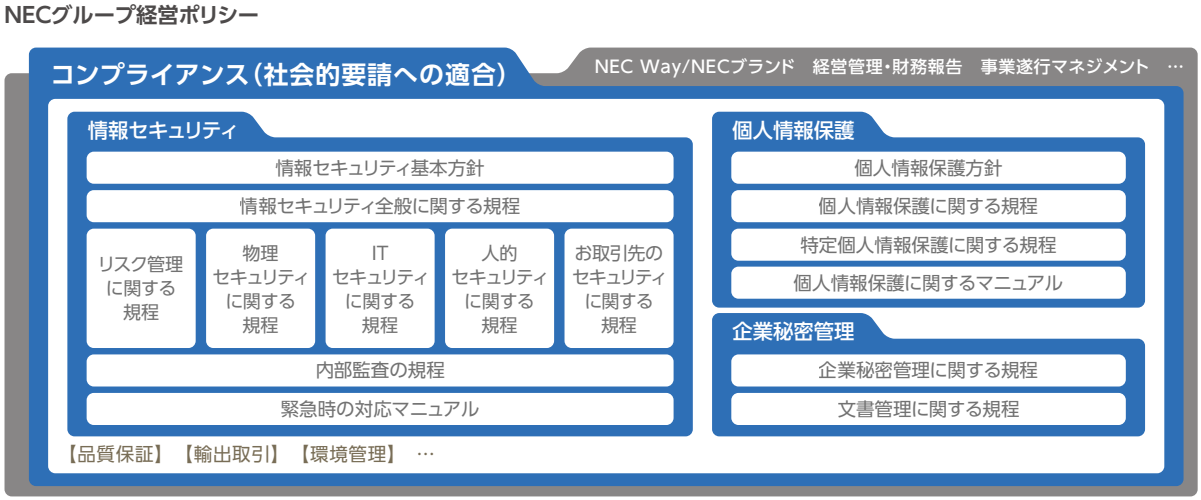
重要情報管理点検は、2020年7月に施行された「企業秘密管理規程」に基づき、最高機密事項、および極秘事項における各事業部の管理状況を確認し、それらに関して社員に「気づき」を与え、また対象施策の周知度、実施状況の「傾向分析」を把握し、NECグループの情報セキュリティの維持・向上につなげていました。

周知度の高まりと運用の定着により、今後は各事業部門での管理にシフトするため、2024年度からは、Three Lines Modelを適用し、セキュリティアウェアネスを意識した情報セキュリティサーベイに変更しています。

❷ 情報セキュリティ監査

監査部門が中心となり、重要情報の取り扱いなどの情報セキュリティマネジメントや個人情報保護に関する監査を年次で実施しています。ISO/IEC27001やJISQ15001に照らし、各組織の状況を監査しています。また並行して、各事業分野の動向を参考にしながら、各組織のISMS認証取得も推進しています。

(認証取得状況はP.30に掲載)



情報セキュリティ基盤

指示3 指示5

NECグループは、ゼロトラスト成熟度モデル（CISA*1）をベンチマークとして「DXを支えるゼロトラストの実現」を目指しています。同モデルはアイデンティティ、デバイス、ネットワーク、アプリケーション、データの5つの柱で構成されており、NECグループではそれぞれ以下のようなセキュリティ対策を実施しています。

1 | アイデンティティセキュリティ

クラウドサービスやテレワークの普及に伴い、サイバー攻撃の高度化が進む中、NECはゼロトラスト環境下で重要な認証の強化・高度化戦略として、「パスワードレス化」を推進しています。

NECでは、生体認証（顔認証、指紋認証など）やデバイス認証などの複数の認証方法を組みあわせる「多要素認証（MFA*2）」を導入することで、なりすましやサイバー攻撃のリスクを低減し、全社的なパスワードレス化を推進しています。昨年度では、ほぼ全ての利用者に対して多要素認証の導入が完了しています。

同時に、なりすましやサイバー攻撃の可能性がある場合に認証を追加で要求する「リスクベース認証」を取り入れることで認証の頻度を減らし、利用者の利便性向上とセキュリティ強化の両立を図り、「利用者に優しく、攻撃者に厳しい」セキュリティを実現しました。

また、NECでは、利用者の認証・認可情報をNECグループ全体で管理する認証基盤を有しており、ゼロトラスト基盤において重要な認証とデバイスの統合管理をグローバルで実現する「IAM基盤*3」を確立しています。

NECでは以下の4点を実現し、IAM基盤によってセキュリティとエンタープライズリソースの有効活用を可能にしています。

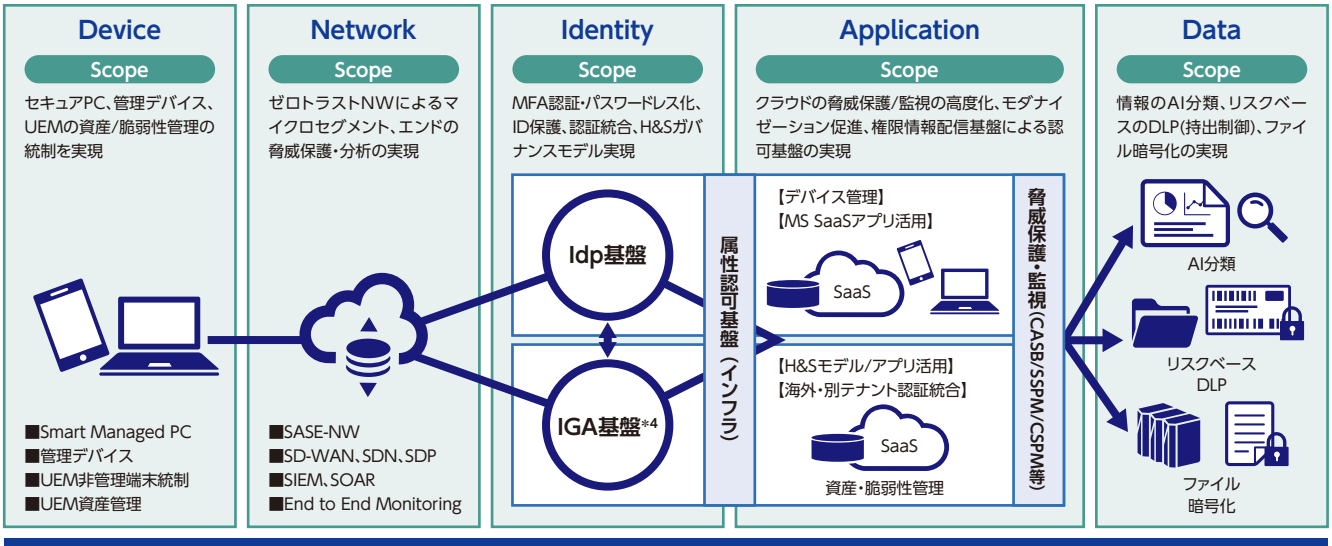
①「グローバルID活用」	アイデンティティ管理の実現（アカウント一意化、ライフサイクル適正化、中央統制）
②「認証・デバイス管理」	ユーザ認証（パスワードレス、多要素認証）、デバイス認証/管理端末化の統制環境の実現
③「グローバルアプリ管理」	共通システムやサービスのアクセス管理、シングルサインオン（SSO）の実現
④「セキュリティガバナンス」	グローバルでのセキュリティポリシーや設定情報の一元管理・統制の実現

2 | デバイスセキュリティ

エンドポイントの端末では、多様な働き方に対応したセキュアな標準端末のラインナップ（SmartPCシリーズ）を整備しています。

SmartPCシリーズは、クライアント側にデータを保持しないシンクライアント（SCPC：Smart Connect PC）、リアルとオンラインのハイブリット環境に最適なリッチクライアントベース端末（SMPC：Smart Managed PC）、ハイスペックなリソースに対応

ゼロトラスト基盤の概要とスコープ



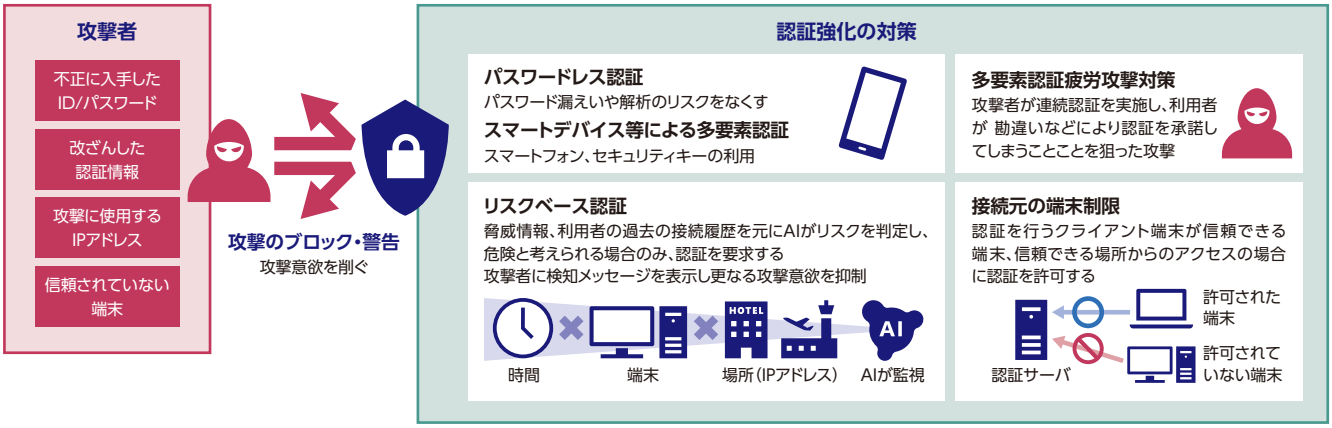
*1 CISA: Cybersecurity and Infrastructure Security Agency　*2 MFA: Multi-Factor Authentication　*3 IAM: Identity and Access Management
*4 IGA（Identity Governance and Administration）: ユーザ等のライフサイクル管理、アクセス権管理、プロビジョニング、資格情報管理等のアイデンティティガバナンスの仕組み

した端末(SEPC:Smart Engineer PC)でラインナップされています。SmartPCシリーズは顔認証、パスワードレス化、デバイス認証、端末管理化(Intune化)、および社内認証統合などに対応しています。

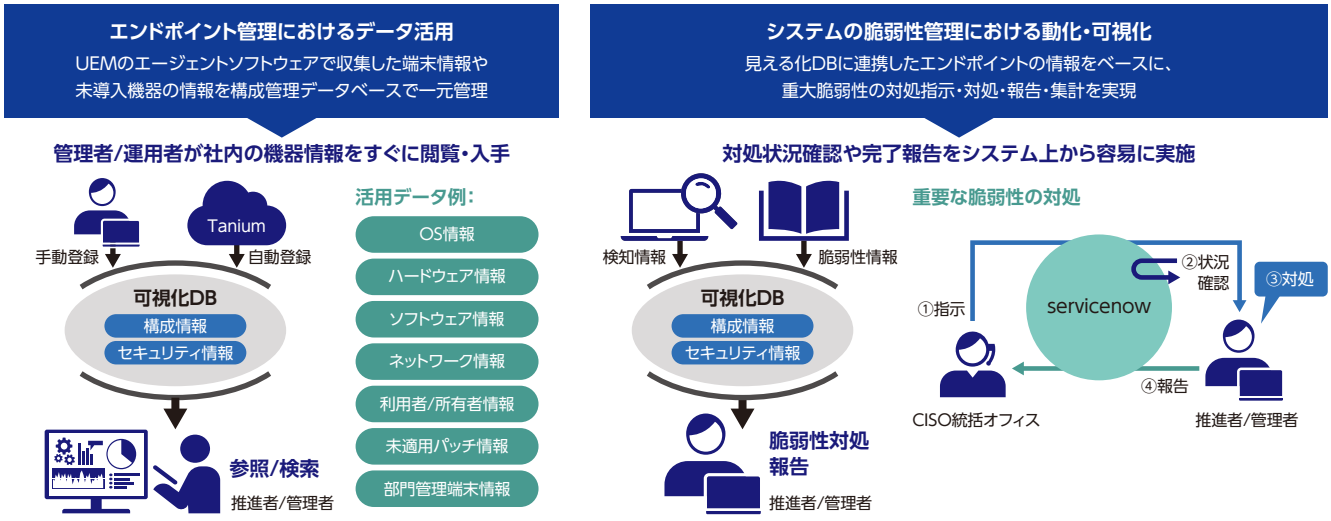
またNECでは、エンドポイントの脆弱性対策として統合エンドポイント管理基盤(UEM*5)を導入しています。UEMのエージェントソフトウェア導入を義務化することで、国内/海外を問わず、全てのIT資産に関する情報をクラウドで一元管理し、セキュリティリスクへの対応力向上や管理業務の効率化を図っています。

エンドポイント管理では、UEMを用いて各情報機器の環境を監視・可視化し、セキュリティ対策やIT資産管理の状況を把握しています。セキュリティ対策には、パッチの配布、ウイルス対策ソフトの最新化、EDRソフトの適正化を行い、禁止ソフトウェアの不正利用も監視しています。また、業務サーバや外部公開サーバなどに対する脆弱性スキャンを実行して問題を検出し、システム運用者に自動的に通知して改善を促しています。さらに、未対処の脆弱性も自動でフォローし、集計・可視化することで早期対応とコスト削減を図っています。ネットワークサイト管理では、UEMの監視により、エージェントソフトウェアの導入状況を検出し、未導入の場合には対処を促す仕組みを導入しています。また、セキュリティ対策が不十分な端末やマルウェアなどが検出された端末は、業務ネットワークから遮断する制御を行っています。社外への通信は、許可リスト型のWebアクセス制御(今後ID単位での制御を導入)などを実施しています。また、Googleが2024年2月に施行した「メール送信者のガイドライン」*6の要件である送信ドメイン認証(DMARC)にも対応済みです。

パスワードレス認証やリスクベース認証による認証高度化



UEMによるセキュアなエンドポイント管理



*5 UEM: Unified Endpoint Management
*6 メール送信者のガイドライン
https://support.google.com/a/answer/81126?hl=ja-jp#zippy=%2C%E6%97%A5%E3%81%82%E3%81%9F%E3%82%8A-%E4%BB%B6%E4%BB%A5%E4%B8%8A%E3%81%AE%E3%83%A1%E3%83%BC%E3%83%AB%E3%82%92%E9%80%81%E4%BF%A1%E3%81%99%E3%82%8B%E5%A0%B4%E5%90%88%E3%81%AE%E8%A6%81%E4%BB%B6

情報漏えいリスク対策では、「暗号化」、「デバイス制御」、「ログの記録」を多角的に実施して外部攻撃や内部不正を防止しています。「暗号化」ではハードウェアと情報の両レベルで防ぎ、ファイルごとにアクセス権や利用期限を設定するインフラを整備しています。これにより盗難、紛失、誤送信からくる情報漏えいを防止し、マルウェア感染時も情報を保護します。「デバイス制御」ではUSBメモリやSDカード、各種通信など外部からの情報漏えいリスクを防ぐため、業務上必要な場合のみにデバイス利用を限定しています。「ログの記録」では全PCの操作ログを記録し、事故発生時はログを分析することで影響範囲と状況の把握、再発防止策立案に用います。

3 | ネットワークセキュリティ

NECグループでは、接続元（エンドポイント）から接続先（システム・サービス）までEnd-to-Endで安全性と可用性を提供するために、ゼロトラスト志向のネットワーク基盤をグローバルに展開しています。

SD-WANは、グローバルの全297拠点に対してセグメンテーション・集中制御を実施することで、セキュリティ強化を実現します。また、ネットワーク変更のリードタイム短縮やネットワーク総帯域の倍増により、セキュリティを担保しつつ高い可用性といった価値も提供します。2024年度の上期末までに現在未展開の海外3地域（北米・LATAM・EU）にも展開完了予定です。

リモート接続環境についてもゼロトラスト志向でグローバルに刷新を行っています。Secure Web GatewayとRemote Gatewayとを連携させたクラウドベースのアクセス制御基盤により、分散するリソースへの効率的なアクセスを実現するばかりでなく、エンドポイントセキュリティや次世代の認証基盤と連携することでさらなる価値を生み出します。2024年度の上期末までに海外全5地域にも展開完了予定です。

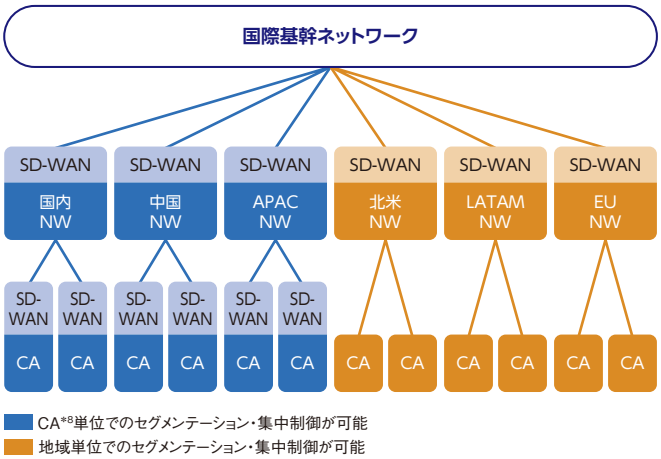
4 | アプリケーションセキュリティ

NECグループでは、DXを推進していく際に多くのクラウドサービスを導入しています。DXの浸透によりユーザの利便性が向上する一方、重要なデータもクラウド上に保管されることになり、社外からのアクセスも容易になることから十分なセキュリティ対策が必要です。クラウドサービス利用上のリスクを考慮し、その利便性を支える以下のようなセキュリティ対策を導入しています。

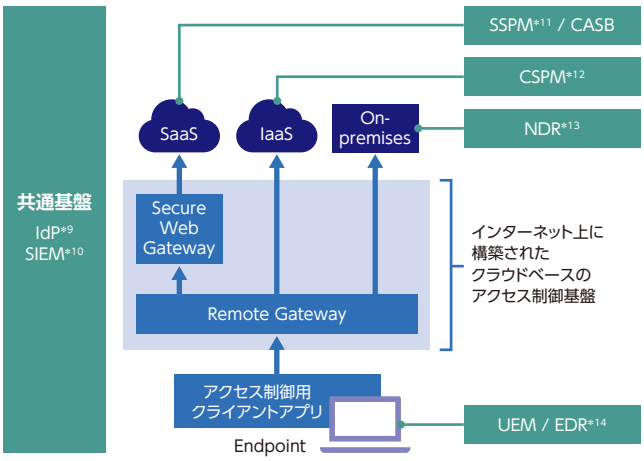
❶ SaaS利用状況の把握

クラウドサービス上のログや保管されているファイルを、CASB*7で監視・分析することで、重要なデータを取り扱うクラウドサービスに対する内部不正やサイバー攻撃への対策を実施しています。また、社内で使用されているクラウドサービスの利用状況を可視化し、未承認のリスクが高いクラウドサービスを監視しています。

SD-WANのグローバル展開



ゼロトラスト志向のリモート接続環境



*7 CASB: Cloud Access Security Broker　*8 CA（Corporate Affiliate）: 関連会社　*9 IdP: Identify Provider　*10 SIEM: Security Information and Event Management
*11 SSPM: SaaS Security Posture Management　*12 CSPM: Cloud Security Posture Management　*13 NDR: Network Detection and Response
*14 EDR: Endpoint Detection and Response

❷ パブリッククラウドの設定ミスに起因するインシデント防止

AWSやAzure、GCPなどパブリッククラウドの利用が増加しています。これらのサービスは利用が容易な反面、設定ミスなどにより外部への情報漏えいを発生させるリスクが伴います。NECグループでは、CSPMを活用して、グループ内で利用されるパブリッククラウドの設定をセキュリティスタンダードに沿って確認し、リスクの有無を常に確認しています。

❸ SaaSの設定ミスに起因するインシデントの防止

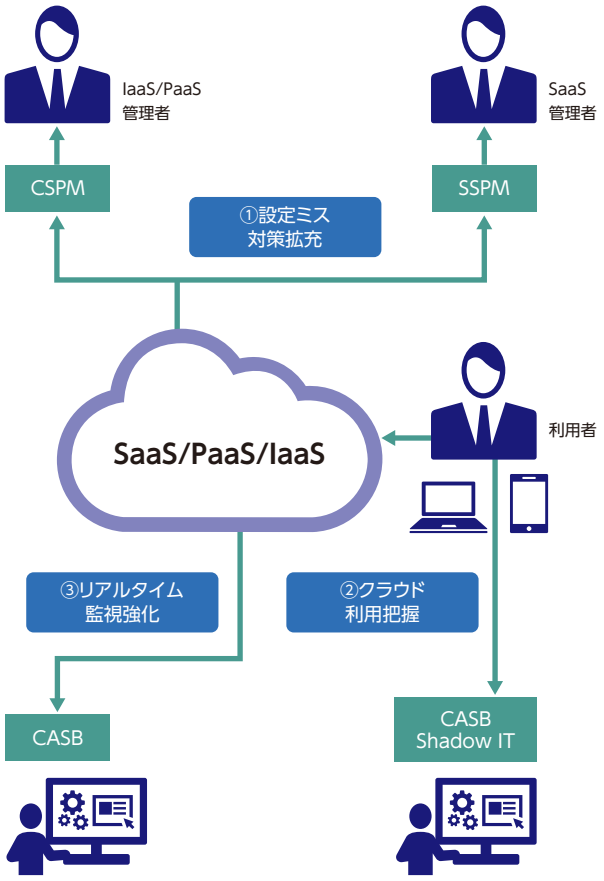
Microsoft 365やBox、Salesforceなどのクラウドサービスは利用時の設定項目が多く、運用する際には設定ミスによる情報漏えいリスクが伴います。NECグループでは、SSPMを利用することで、社内で利用するクラウドサービスの設定ミスを可視化・是正する対応をグローバルに実施しています。

5 | データセキュリティ

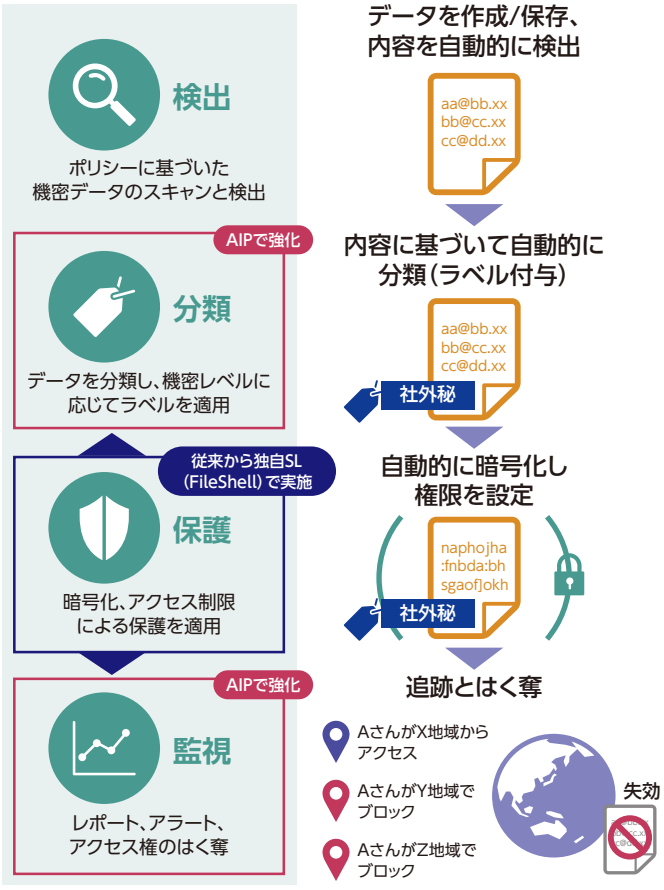
NECグループでは、ゼロトラストセキュリティ観点から、クラウド対応のAIP*15統合ラベルとNEC独自ソリューションの「InfoCage FileShell」を用いて、Officeファイル以外も含む各種ファイルの自動分類、暗号化、追跡、アクセス権管理を行い、マルウェア感染などによる外部への情報流出を防いでいます。

また、重要情報の安全管理を徹底するために、セキュアストレージを導入し、アクセス制御、暗号化、証跡管理、侵入調査、ISMS管理に対応させ、業務負荷を減らしつつセキュアな重要情報管理を行っています。さらに、重要度の高い社内システムについては、リスク分析、事業インパクト分析を基に脆弱性対策、ログ管理、ネットワーク保護、認証、アクセス制御、特権管理等を含む強固なセキュリティ対策を展開しています。

クラウドサービス利用上のセキュリティ対策



ファイル暗号によるデータセキュリティ



*15 AIP: Azure Information Protection

情報セキュリティ人材

指示3

NECでは、全社員を対象とした「情報セキュリティアウェアネスの向上」、「施策を推進する人材の育成」、お客様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つの観点で人材を育成しています。

1 | 情報セキュリティ人材の育成

NECでは、全社員を対象とした情報セキュリティの「アウェアネスの向上」、「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つの観点で人材を育成しています。

2 | 情報セキュリティアウェアネスの向上

情報セキュリティアウェアネスの向上をはかるには、情報セキュリティリスクを感じ取るリスク感覚や情報を適切に取り扱うための知識、情報セキュリティのリスクカルチャーが重要であり、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を実施し、情報セキュリティや個人情報保護の知識習得、アウェアネスの向上をはかっています（2023年度修了率 93%。海外7か国語対応）。情報管理、社外でのセキュリティ対策、委託先管理などセキュリティ脅威のトレンドなどを考慮し、教育内容を毎年更新しています。

❷ 情報セキュリティの遵守事項への誓約

お客様情報や個人情報（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、NECグループ全社員から誓約を取得しています。

❸ 情報セキュリティアウェアネスの向上施策

情報セキュリティリスクへの危機感を高め、社員自らが考え、判断し行動できるようにするため、セキュリティ動画などを活用したセキュリティアウェアネス向上施策を実施しています。また、テーマ・トークと呼ばれる職場での懇談会などを四半期ごとに実施して、個人個人のリスクに対する分析力・判断力の向上をはかるとともに、組織の情報セキュリティリスクカルチャーを醸成しています。アンケート結果から、情報セキュリティアウェアネスや情報セキュリティリスク感覚の向上がみられるなど、着実な効果をあげています。

3 | 情報セキュリティ施策を推進する人材の育成

情報セキュリティ推進体制のもと社内で各種施策を展開し、必要なスキルを備えた人材を育成しています。重要情報管理や個人情報保護、セキュア開発・運用、インシデント対応などに適切に対応できるようCISSP*2や情報処理安全確保支援士、個人情報保護士などの資格取得者を配置し、対応力を強化しています。

*1 WBT: Web Based Training　*2 CISSP（Certified Information Systems Security Professional）: 国際情報セキュリティ・プロフェッショナル認定

4 | Security By Design(SBD)を実践できる人材の育成と、人材の裾野を広げる活動

NECグループが提供する製品・システム・サービスに適切なセキュリティ実装を行い、お客さまのビジネスリスク低減に貢献するため、セキュリティ人材の育成に注力しています。

❶ NCSA(NEC Cyber Security Analyst)トレーニング

トップセキュリティ人材の強化を目的とし、セキュリティ技術の知識を持つ人材を対象に、CSIRT*3業務やリスクハンティングなど高度なセキュリティサービスに必要な実践的テクニカルスキルを、半年間の集中プログラムで習得します。2019年度まで実施したNCAT(NEC CISO補佐官トレーニング)とあわせ延べ75名が受講し、プロフェッショナルサービスの提供に携わっております。

❷ SBDスペシャリスト研修

各事業部門で、セキュリティ責任者を補佐し、SBDを実践する専門人材の育成を2019年度より行っております。また2021年度からは、営業職向けコースを新設し、インシデント事例や対策のためのオファリングなど、適切なセキュリティ提案に必要なスキル習得も進めています。2022年度は20名以上が受講し、累計82名が受講しております。本スペシャリストを中心に、システム開発に関わる全プロセスを俯瞰し、抜け漏れなく適切なセキュリティを実装することで、安全・安心なシステムをお客さまにお届けします。

❸ NECサイバーセキュリティ訓練場

セキュリティに関する適切なコミュニケーションのための知識、リスクアセスメントをはじめとしたスキルを、お客さまのシステムにかかわる全社員が学ぶことができる研修として提供しています。また実践的なセキュリティ対策訓練の場として、ECサイトを模した専用の仮想環境を用い、システム構築フェーズでの堅牢化技術を習得できます。リモートで受講可能な演習環境により、営業やSE職を中心に2023年度は延べ1,600名以上が修了しました。

❹ 全社的CTFの実施

セキュリティ人材の裾野拡大、セキュリティスキル向上に加え、セキュリティアウェアネス向上を目的とした社内CTF*4「NECセキュリティスキルチャレンジ」を開催しています。2023年度は850名以上が自主的に参加し、2015年の開始以来の参加者は延べ8,000名以上となりました。

❺ 営業・SEセキュリティ基礎教育

営業・SEとして必要な、SBDを核とするセキュリティの基礎知識をe-learning形式で展開し、2023年度は36,000名が受講しました。さらに、お客様に提供したシステムで発生したインシデント事例を参考としたビデオを視聴し気付きを得るテーマ・トークを実施しました。これにより、NECグループ全体のセキュリティ実装力の底上げをはかっています。

❻ 高度なセキュリティ技術資格保有者

お客さまへの最適なソリューションを提供するための情報セキュリティに関する高度なスキルの証明として、営業やSEなど、お客さま対応を行う社員にセキュリティ公的資格の取得を推奨しています。社内セミナーや勉強会などにより、国際資格であるCISSPや情報処理安全確保支援士(RISS)の取得者を拡充しています。特にCISSPについては、高度な技術的スキルを持つだけでなく、ビジネス観点でリスクを評価できる人材を育成するため、認定機関であるISC2と戦略的提携を締結して取得を促進しております。NECグループのCISSP保有者は450名となりました。

*3 CSIRT: Computer Security Incident Response Team　*4 CTF: Capture the Flag

サイバー攻撃対策

指示4 指示5 指示7 指示8 指示10

サイバー攻撃が高度化・巧妙化する中、先進的な対策をグローバルで実施するとともに、
CSIRT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。

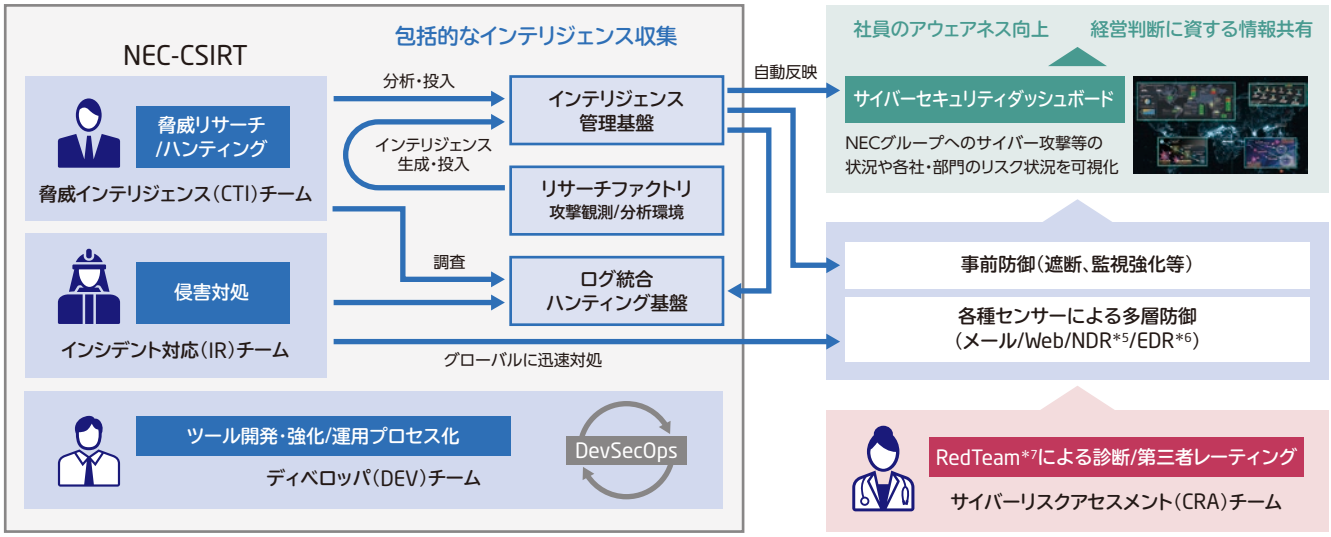
1 | グローバルサイバー攻撃対策

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統一的に行うとともに、CSIRTによりインシデントに対応し、サイバーレジリエンスを確保しています。また、第三者によるNIST CSF*1 1.1及びNIST CSF 2.0のGOVERN領域を中心とした新設項目の評価を行い、対策を強化しています。

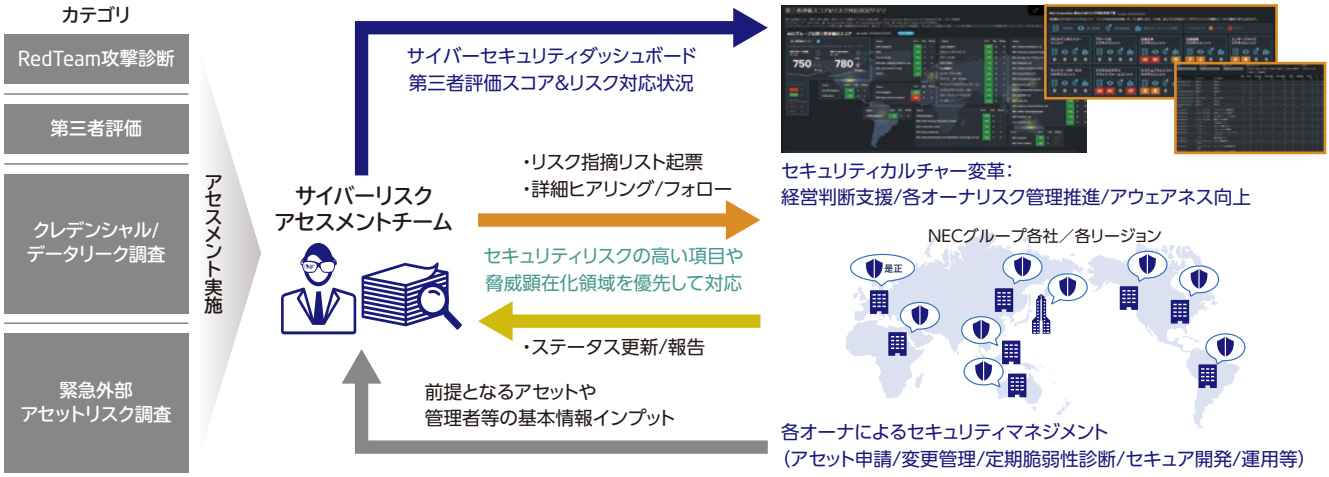
具体的には、サイバーセキュリティリスクに対して、グローバルに統一されたアプローチを取ることが、事業継続のためには重要であるという考えのもと、AIも活用して日々のサイバー攻撃の監視や状況の把握、分析を行うとともに、それに伴い監視運用プロセスの見直しを行っています。また、対策製品、サービス、市場動向を把握し、PoC*2評価や社内IT環境調査により、対象製品・サービスの社内IT環境への適合性を検討します。これらの結果から、今後必要となる対策を検討し、その対策の対象範囲、効果やコストを算出します。そして、上記の活動に基づいた推進計画を毎年立案し、CISO*3の承認のもと対策を実施します。

NECグループでは、包括的なサイバー防衛の考え方（CDC*4等）に基づいた対策を実施しており、次に述べる①～⑤が注力項目です。

サイバーセキュリティ対策の全体像



サイバーリスクアセスメント



*1 NIST CSF（Cyber Security Framework）：米国国立標準研究所（NIST）が発行している重要インフラのサイバーセキュリティを改善するためのフレームワーク
*2 PoC: Proof of Concept 新しい概念の実証実験　*3 CISO: Chief Information Security Officer　*4 CDC: Cyber Defence Centre
*5 NDR: Network Detection and Response　*6 EDR: Endpoint Detection and Response
*7 Red Team: 企業や組織に対し、実際の脅威に即した疑似的な攻撃を行い、組織としての攻撃への耐性とリスクの評価、および改善・追加対策案の提示を行うチーム

❶ Red Teamによるサイバーリスクアセスメント

NECグループのサイバーレジリエンス、アカウンタビリティ向上、アタックサーフェスマネジメントを目的とし、Red Teamによるサイバーリスクアセスメントを定期的に行っています。

監査法人及びセキュリティ専門企業と協力し、第三者による攻撃者視点での外部/内部の侵入調査、重要情報管理の調査、公開サーバの脆弱性などのアセットリスク調査、クレデンシャル情報やデータ漏えいなどの調査、Bitsight等の第三者評価を通じてグローバルにアセスメントを行い、既存のセキュリティ対策/運用における抜け漏れを洗い出し、サーバの管理者や海外現地法人などの責任者と連携して改善策を実施します。

❷ 脅威インテリジェンス生成・活用

脅威インテリジェンス専門チーム(CTI*8チーム)が、NECに対する脅威とその予兆を把握し、高度な事前防御を実施するとともに、NECグループの全社に展開したEDR、CSIRTで独自に開発したNDR、ログ統合分析基盤により、未知の脅威へのハンティングを実施しています。

また、アクティブな独自CTI生成強化を目的とした調査環境(Research Factory)を構築し、詳細な脅威分析を行っています。

❸ CSIRT体制強化

CISO配下にCSIRTを設置し、サイバー攻撃を監視して攻撃やマルウェアの特徴を分析し、関係機関とも情報を共有しています。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。

CSIRTは脅威インテリジェンスを活用するCTIチーム、インシデント発生時に対応するIRチーム、セキュリティ機器からのアラートを24/365で監視するSOCチーム、ツール・プラットフォーム・運用プロセスの各強化を行うDeveloperの4チームで構成されます。海外現地法人には、サイバー攻撃を常時監視する体制をシンガポールに構築し、日本のCSIRTと連携しながら検知状況や不正通信先などの脅威をグローバルに共有します。

インシデント発生時には関係部門と連携し、リスクを考慮しながらCISOの承認のもと復旧まで対応しています。

❹ 組織的なセキュリティレジリエンス強化

ランサムウェア等の世界的な脅威に備え、社員に対して攻撃メール訓練を行うとともに、インシデントが発生した場合、迅速に対応できるよう、マニュアルを整備しています。また、有事に備え、経営層や関係部門、専門家による総合的な演習を半年に一回以上実施しており、さらに社長による模擬記者会見も行っています。

❺ AIを活用した高度なサイバーセキュリティ対策

サイバーリスクアセスメントにおける診断業務、脅威インテリジェンスの生成・活用、NDRの検知、インシデント調査、攻撃メール訓練など、幅広い分野において生成AIを含めたAI活用により、自動化・効率化、高度化を進めています。

2 | サイバーセキュリティダッシュボードによるセキュリティ―カルチャー変革

NECグループへのサイバー攻撃の状況や、CTIチームが収集した脅威インテリジェンス情報、サイバーリスクアセスメントで判明した、各社・各部門のセキュリティリスク状況を可視化した、サイバーセキュリティダッシュボードをリリースし、全社員に公開しています。社員一人ひとりがリアルな状況を知り、リスクを実感することで、セキュリティアウェアネスの向上につなげることができます。また、経営幹部の会議や全海外現地法人が参加する会議の中でダッシュボードを使い、各組織のリスク対応状況を見ながら、リスクが高く脅威が顕在化している組織をその場で特定し、改善の指示を出すなど、スピーディな経営判断、各組織のアクションに役立てています。この活動の先進性が社外でも認められ、IT協会の2023年度(第41回)IT賞において「IT優秀賞(マネジメント領域)」を受賞しました。また、一般社団法人日本デジタルトランスフォーメーション推進協会の「日本DX大賞2024 特別賞」を受賞しました。

サイバーセキュリティダッシュボード

IT優秀賞受賞の様子

*8 CTI: Cyber Threat Intelligence

お取引先と連携した情報セキュリティ

指示9

NECではお客様の大切な情報を守るために、お取引先と一体となった情報セキュリティ対策の浸透や是正を推進し、サプライチェーン全体のセキュリティレベルの向上をはかっています。

1 | 取り組み体系

NECはお取引先と連携する際、その技術力とともに「情報セキュリティ水準」が、NEC の定める水準に達していることが重要だと考えています。お取引先の情報セキュリティ対策状況により、情報セキュリティレベルを分類し、適切なレベルのお取引先へ委託する仕組みを取り入れています。これにより、お取引先で発生する事故のリスクを低減しています。

お取引先に求める対策は、大きく分類すると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セキュリティ実装、⑦点検の実施 の7項目です。

❶ 契約管理

NECとお取引先との間で、秘密保持義務などを含む会社間の包括契約（基本契約）やお客様対応作業案件における覚書を締結しています。

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、第三者に再委託してはならない旨、基本契約で定めています。また、再委託先確認書兼体制確認書の提出を義務化しており、プロジェクト毎の体制を明確化しています。

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対策を、「お客様対応作業における遵守事項」として定め、作業従事者が自社に対し誓約してもらうことで対策実施を徹底しています。

❹ 情報の管理

業務で取り扱う秘密情報の管理について秘密指定の指針を定め、秘密表示、持ち出し管理、廃棄・返還の管理を定め、実施を徹底しています。

❺ 技術対策の導入

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など）に区分し、導入を依頼しています。

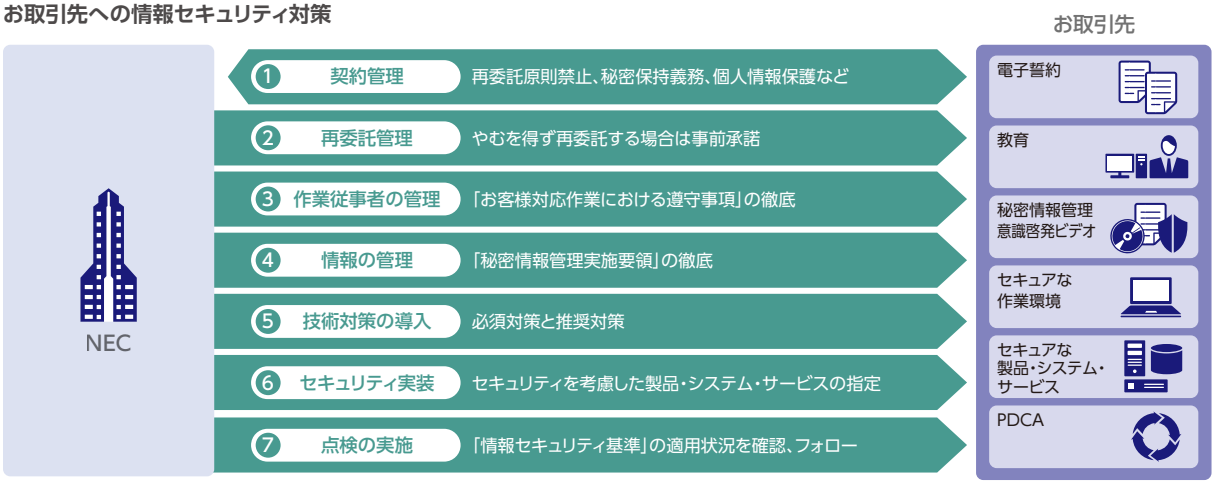
❻ セキュリティ実装

お客様向けの製品・システム・サービスの開発・運用について実施要領を定め、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。

❼ 点検の実施

NECの要求水準を定義した基準書「お取引様向け情報セキュリティ基準」に基づき、お取引先の対策実施状況を点検し、適宜改善を指導しています。また、昨今のサイバーセキュリティの情勢を踏まえ「お取引様向け情報セキュリティ基準」をインシデント発生の備えたものへ改訂を行い、更にお取引先と連携した活動を強化しています。

お取引先への情報セキュリティ対策



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

NECの情報セキュリティ対策を理解し実施していただくため、NECでは全国のお取引先（約1,800社、うちISMS認証取得会社約900社）を対象に、毎年情報セキュリティ説明会を開催しています。また、海外のお取引先向けの説明会やサイバーセキュリティ対策についての勉強会も随時開催しています。

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（ソフトウェア開発委託関連の約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を促進しています。また弊社CISOによるサイバーセキュリティに関する講演を実施し、情報セキュリティの意識啓発に努めています。

❸ 対策ガイドの配付

お取引先が情報セキュリティ対策をより円滑に実施できるよう、対策の実施ガイドを提供しています。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などを発行しています。

❹ 委託先管理プロセスの標準化

お取引先で情報セキュリティ対策を推進するだけでなく、委託元であるNEC側の委託先管理プロセスも標準化し、サプライチェーンで一貫した情報セキュリティ対策を進めています。

3 | お取引先に対する点検および是正活動

お取引先に対し、書類点検と訪問点検を実施しています。毎年、インシデントの状況などを勘案して点検項目を見直し、点検結果をお取引先に報告書でフィードバックします。改善が必要な課題に対するフォローアップを行い、お取引先のレベルアップをはかります。

❶ 書類点検・訪問点検

NECと取引のある会社、約1,800社を選んで書類点検を実施しています。お取引先は自社の対策状況を自ら点検し、点検結果はWebシステムによってリアルタイムでフィードバックを行っています。また、取引が多いお取引先には直接訪問、あるいはリモートを活用した訪問点検を実施しています。毎年訪問社数を増やしており（2023年度は約300社）NECの点検担当者（約100名）によって推進しています。

❷ 情報セキュリティカルテ

点検結果とともに、各種情報セキュリティ対策の対応状況をカルテにまとめ、システムで公開しています。お取引先は、常に自社の最新状態を確認することができます。

標準化された委託先管理プロセス

お取引先への点検・是正活動

4 | サイバーセキュリティ対策強化

サイバーセキュリティ対策を強化するため、これまでの情報セキュリティ基準を、インシデント発生を前提とし、「準備・検知・分析・抑制・回復・ユーザ対応」を含めたインシデント対応能力の確立を要求しているNIST SP800-171をベースとした内容に改訂しました（2022年4月）。毎年SSP（システムセキュリティ計画書）を実施し、情報セキュリティ基準への進捗状況を確認させていただき、お取引先が対策に苦労している項目については、サイバーセキュリティ対策の勉強会を開催しています。

また、重点お取引先に攻撃リスク低減・セキュリティレベル向上を目的に、第三者評価結果を開示し、リスクの改善活動を実施しています。これによりお取引先のリスク低減を支援しています。

5 | グローバルでのサプライチェーンマネジメント強化

グローバルでのサプライチェーンマネジメント強化を図るため、海外現地法人向けの情報セキュリティ説明会を開催し海外現地法人の従業員に対する、情報セキュリティの意識啓発に努めています。2022年度は中国で開催し、2023年度はインドとベトナムで開催しました。引き続きグローバルサプライチェーン全体のセキュリティレベルの向上を図るべく今後も継続して開催していきます。

セキュアな製品・システム・サービスの提供

指示2 指示4

お客様へ「ベタープロダクツ・ベターサービス」を提供するために、NECは製品・システム・サービスの高品質な安全・安心を実現するさまざまなセキュリティ確保の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 全社推進体制とルール

お客様に提供する製品・システム・サービスをセキュアに開発・運用するために、NECではセキュリティ実装推進体制を構築しています。本推進体制は、全社のサイバーセキュリティ統括部門と各事業部門に配置したセキュリティ責任者で構成されています。セキュリティ責任者は、製品・システム・サービスの脆弱性や設定ミス、システムの不具合に起因する情報セキュリティ事故の撲滅に向け、全社のサイバーセキュリティ統括部門と各事業部門との橋渡し役として、各種セキュリティ施策の浸透や現場におけるセキュリティ対策の支援を担っています。2023年度は全事業部門へ約400名のセキュリティ責任者を配置し、隔週の会議体とコミュニティを利用し、サイバーセキュリティ統括部門と各事業部門間の連携を強化しました。

セキュリティ責任者の役割や各部門でのセキュリティ実装のプロセスは「サイバーセキュリティ管理規程」に定めています。サイバーセキュリティ管理規程はNECグループ経営ポリシーのルールのひとつとしても定めており、NECグループ会社においても、NECと同様のセキュリティ実装推進体制の構築とサイバーセキュリティ管理規程の制定を推進しています。

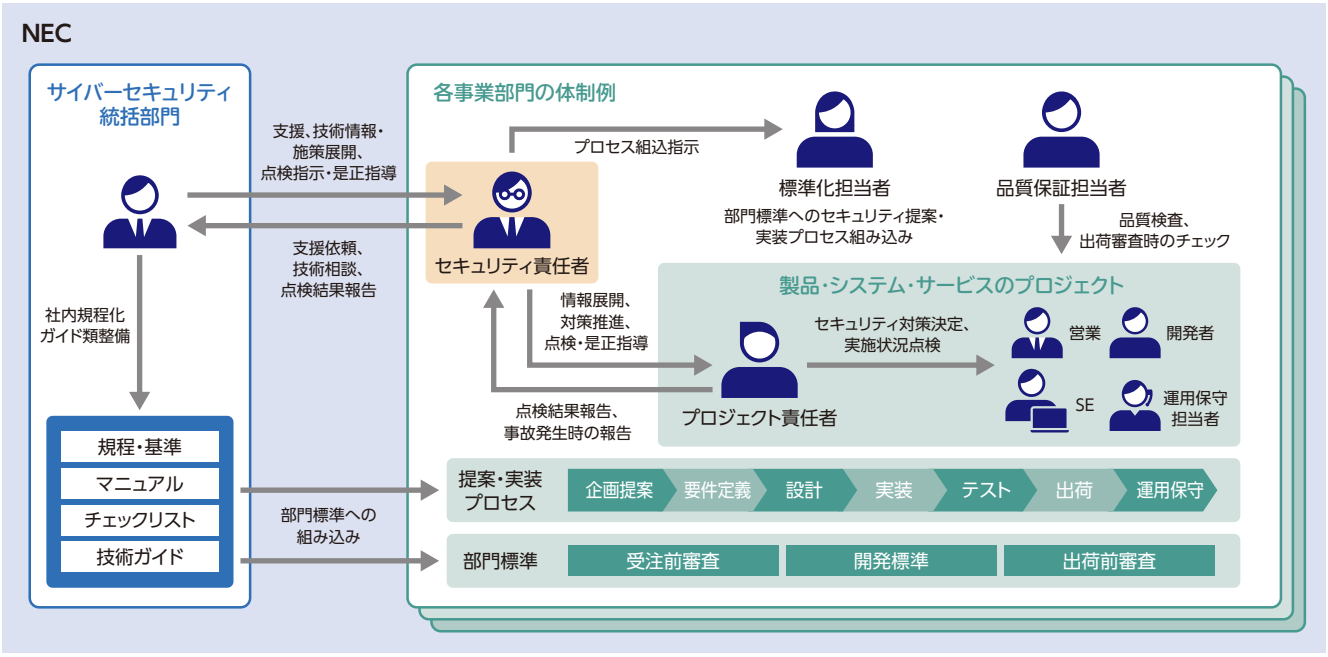
❷ セキュリティ実装の主要な取り組み

NECでは、セキュリティを確保する「セキュリティ・バイ・デザイン（SBD）」の思想に基づき、企画・提案フェーズから実装フェーズ、運用・保守フェーズまでを含めたセキュリティ実装を行っています。システム開発の早い段階でセキュリティを確保することは、コストの削減や納期遵守、保守性に優れたシステム開発などさまざまなメリットに直結します。特に、お客様のシステム環境に対しては、最適なセキュリティを早期から検討・実現するために、要件定義段階におけるリスクアセスメントの実施に注力しています。

また、セキュリティ実装において考慮すべきセキュリティ要件のベースラインとして、「サイバーセキュリティ実施基準」を定義しています。本基準では、ISO/IEC15408やISO/IEC27001などのセキュリティ国際標準はもちろん、政府機関が定めるセキュリティ基準や業界ガイドラインなどの要件を考慮し、厳密なセキュリティ要件を定めています。さらに、最新技術に対してのセキュリティ対策も実装できるようガイドラインを随時発行・展開し、開発・運用するシステム・製品・サービスに安心して導入できるようにしています。

製品・システム・サービスの開発では、各フェーズでセキュリティ

セキュリティ実装プロセス



タスクが実施されていることを確認するために、チェックリストを作成し活用しています。本チェックリストに基づき、セキュリティタスクの実施状況を一元管理し可視化するために開発された「セキュリティ実装点検システム」により業務プロジェクトが管理され、セキュリティ対策状況の効率的な点検・監視が実施されています。また、サイバーセキュリティ統括部門では、集約された情報を活用することでより実効性のある施策の展開およびセキュリティ実装におけるガバナンス強化を実現します。

製品・システム・サービスの運用・保守フェーズでは、脆弱性情報を一括収集・配信する「脆弱性管理システム」、「サイバーインテリジェンス共有基盤」を活用し、セキュリティ確保に取り組んでいます。「脆弱性管理システム」はアジャイル開発を活用して刷新し、柔軟な機能拡充と効率的な脆弱性管理を実現しています。また、収集した脆弱性情報は各事業部門に展開するだけでなく、製品・システム・サービスをご利用いただいているお客様にまで提供し、脆弱性に関するリスクを把握いただけるよう取り組んでいます。サイバーインテリジェンス共有基盤は、サイバーセキュリティの脅威情報(サイバー攻撃の手口、インシデント事案、脆弱性、セキュリティ対策のためのインジケータ情報など)を各事業部門へ迅速に共有する機能を備えています。

また、NECではPSIRT(Product Security Incident Response Team)を設置し、NECグループの製品に関する脆弱性情報の収集・対処を実施しています。社外からの受付窓口を設置、脆弱性公開ポリシーを公開、CNA*1機関として活動するなど、自社製品の未公開脆弱性情報やお客様システムの脆弱性情報を適切にハンドリングすることで、脆弱性に対処しています。

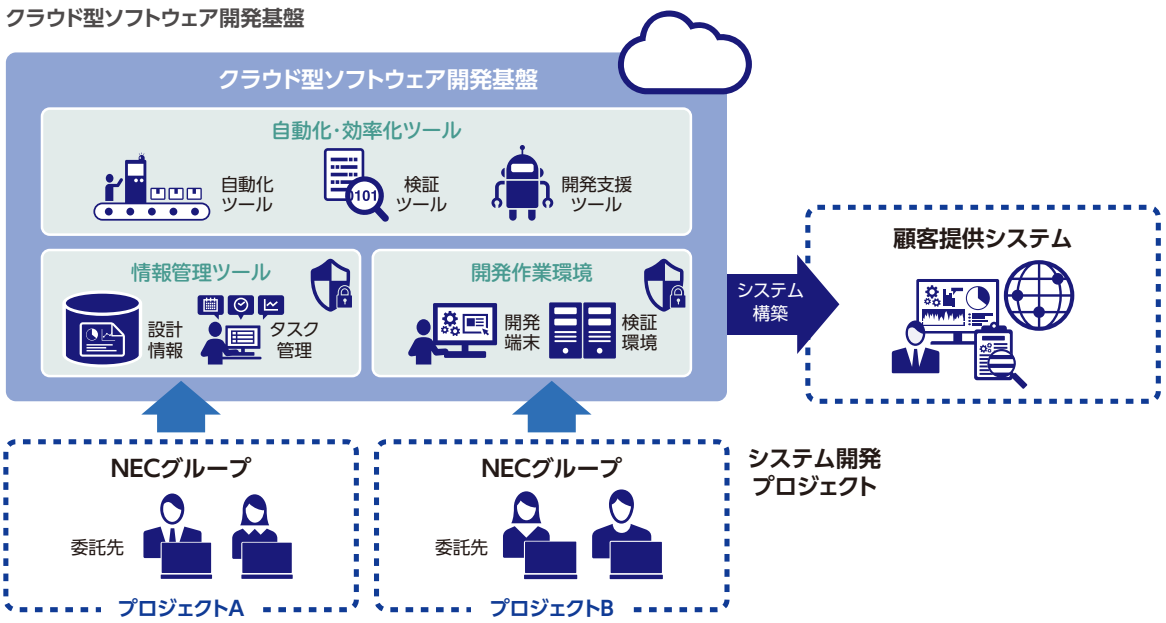
❸ セキュリティ実装のためのソフトウェア開発基盤

NECはシステム開発を行う社内標準環境として、クラウド型のソフトウェア開発基盤を整備しています。開発基盤はソースコード・仕様書などの設計情報やタスクを管理する情報管理ツール、ビルドやテストの自動化やAIを用いた開発支援などを行う自動化・効率化ツール、実装やテストを行う開発作業環境などを備えた統合開発環境です。セキュリティ脆弱性検査の検証ツールなどセキュリティ実装を効率化、自動化するツールも備えており、システム開発の生産性・品質・セキュリティを向上させます。

また、クラウド型の開発基盤として各業務プロジェクトおよび委託先含めたサプライチェーンの開発環境を集約することで、開発環境自身のセキュリティ管理を一元化しています。これにより、各業務プロジェクトで利用する開発環境のセキュリティ対策をサイバーセキュリティ実施基準に従うよう統制し、開発中に使用するお客様のシステムの設計情報を安全に管理できるようにしています。

❹ ハードウェア生産拠点(工場)のセキュリティ強化

NECの工場では、第三者によるリスクアセスメントを実施し、サイバー攻撃対応BCP訓練などのリスクに応じた対策を行っています。



*1 CNA(CVE Numbering Authority):脆弱性に対してCVE*2番号を割り当てる組織
*2 CVE(Common Vulnerabilities and Exposures):一般公表されている脆弱性情報のデータベース、一意に識別するためにCVE番号が割り当て登録される

NECのサイバーセキュリティ戦略

グローバルで社会問題化しているサイバー攻撃に対し、NECは総力をあげて
安全・安心で快適な社会基盤を提供することで、人と地球にやさしい情報社会の実現に向けて貢献しています。

1 | 基本方針

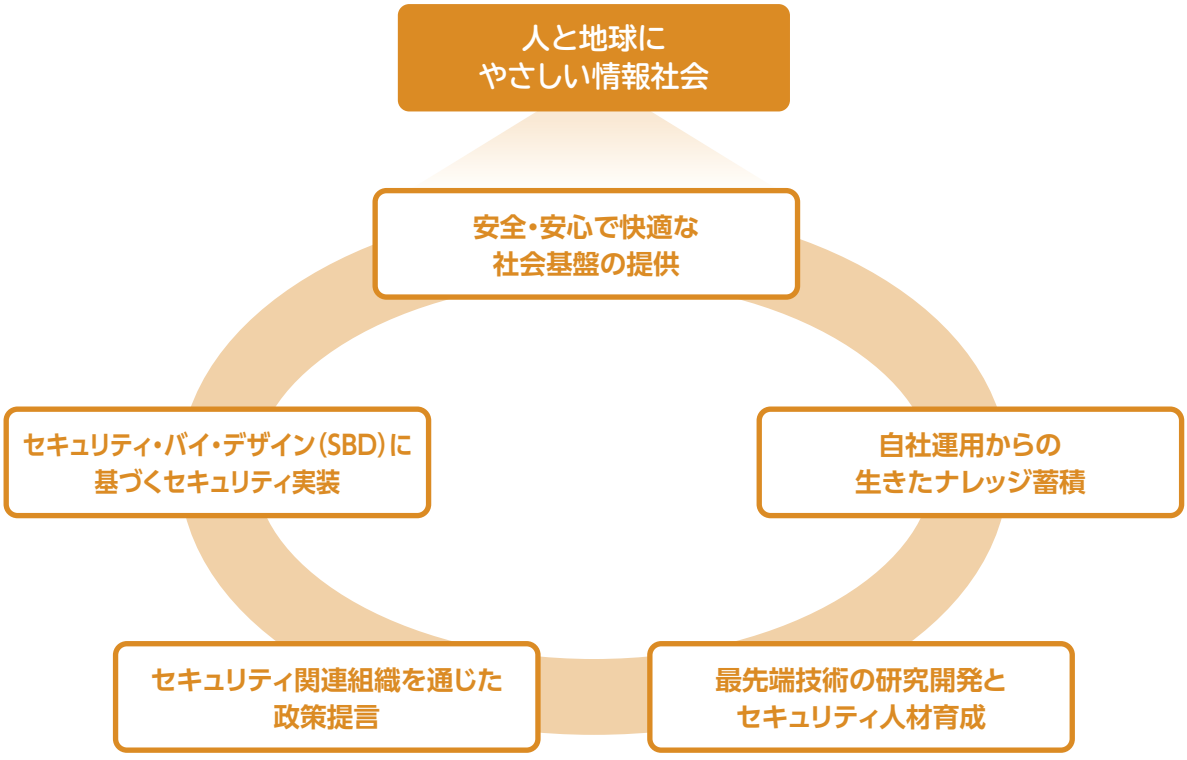
NECは、1977年10月に「変化する社会ニーズへの通信企業の対応」と題する基調講演の中で、「コンピュータと通信の融合」という構想を実現すべくC&C*1という構想を提唱しました。その宣言に沿って世界中のコンピュータをつなぎ、人とモノ、モノとモノをつなぐことで、多種多様な社会ニーズに応え社会の発展に貢献してきました。

昨今のDX*2の促進により、テレワークの活用が増加するなど人々の働き方が大きく変化する状況の中で、フィジカル空間（現実空間）とサイバー空間が高度に融合し、あらゆるモノ同士がつながるようになってきています。このような世界では、あらゆる場所にセキュリティリスクが存在する可能性があり、新たに発生するセキュリティリスクへ対応が求められます。事業環境の激しい変化に対応しながら安全に事業を遂行するためには、これまで以上にサイバーセキュリティは重要な課題となっています。

この課題に向けて、NECは多岐にわたる取り組みで対応しています。国内外のセキュリティ関連組織と連携した活動を進め、国内関連組織や業界団体等を通じて内閣官房・省庁へ政策提言を実施しています。また研究開発や社内外の人材育成を通じて、高度なセキュリティサービスの提供だけではなくセキュリティ人材の輩出にも貢献しています。更に新たなサイバーリスクに対応するため、「セキュリティ・バイ・デザイン（SBD）」に基づき設計段階から構築、運用に至るシステムライフサイクルにおけるすべてのフェーズでのセキュリティ実装を、実施体制の構築も含めて推進しています。加えて、自らを最初のユーザとする「クライアントゼロ」をサイバーセキュリティにおいても実践する等、グループ11万人のセキュリティ対策から生きたナレッジの蓄積を進めています。

これらの実績とノウハウを基盤に、NECはサイバーセキュリティで安全・安心な情報社会の実現に貢献していきます。

安全・安心に貢献するNECのサイバーセキュリティ推進の取り組み



*1 C&C: Computer&Communication　*2 DX: Digital Transformation

2 | 社会への貢献

❶ 関連組織との連携

増加するサイバーリスクへの対応を強化するために、NECでは国内外の関連組織と連携しています。

一般財団法人日本サイバー犯罪対策センター(JC3*3)に発足時から参画し、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ています。またICT-ISAC*4への参画やCyber Threat Alliance(CTA)への加盟など、サイバー攻撃の脅威情報の活用を推進しています。さらに2021年にはサイバーリスク対応のための組織フレームワークに関する国際標準化に取り組み、その結果はITU-T*5勧告として発行されました。こ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。

❷ 国の活動への貢献

特別顧問である遠藤信博が、内閣のサイバーセキュリティ戦略本部委員、経団連サイバーセキュリティ委員会の委員長やサプライチェーン・サイバーセキュリティ・コンソーシアム(SC3)の会長を務めており、また執行役 Corporate SEVP 兼 Co-COO*6である堺和宏がJC3の代表理事を務めています。このように、NECは国家的なセキュリティプロジェクトへ積極的に貢献しています。また、経団連やSC3、JDTF*7などの業界団体を通じて省庁へ提言することでも、官民一体となった安全・安心な社会づくりに貢献しています。

関連組織との連携

組織加盟

日本サイバー犯罪対策センター(JC3)へ参画 (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・分析・共有し、脅威の大本を特定・軽減・無効化することを目指す。執行役 Corporate SEVP 兼 Co-COO (チーフオペレーティングオフィサー)の堺 和宏が代表理事を務める。

ICT-ISACへ参画 (2017年3月)
通信事業者、放送事業者、ソフトウェアベンダー、情報提供サービス事業者、情報関連機器製造事業者など多様な事業者がサイバー攻撃などに関して情報共有し、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。NECは前身となるTelecom-ISACから参画している。

産業サイバーセキュリティ人材育成検討会へ参画 (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させた。2017年からは一般社団法人サイバーセキュリティリスク情報センター(CRIC)内組織へ移行し、情報共有についての取組みを、さらに強化している。

セキュリティ企業間での情報共有団体(CTA)へ加盟 (2018年10月)
セキュリティ企業間でサイバー攻撃の脅威情報を共有する米国の非営利団体Cyber Threat Alliance(CTA)へ加盟した。脅威情報の共有や利活用を通じ、自社のセキュリティ対策強化をすると共に、セキュリティ関連のサービス及び製品の開発に活用している。

セキュリティ・トランスペアレンシー・コンソーシアムを設立 (2023年10月)
製品・システム・サービス等におけるセキュリティの透明性を高め活用可能にすることによって、サプライチェーンセキュリティリスク対応等の社会課題の解決を目指し、日本電信電話株式会社とともにコンソーシアムを設立した。NECは幹事事業者として、ソフトウェア構成に関する可視化データの作成及び提供を促進するとともに、活用シーンのさらなる拡大を目指す。

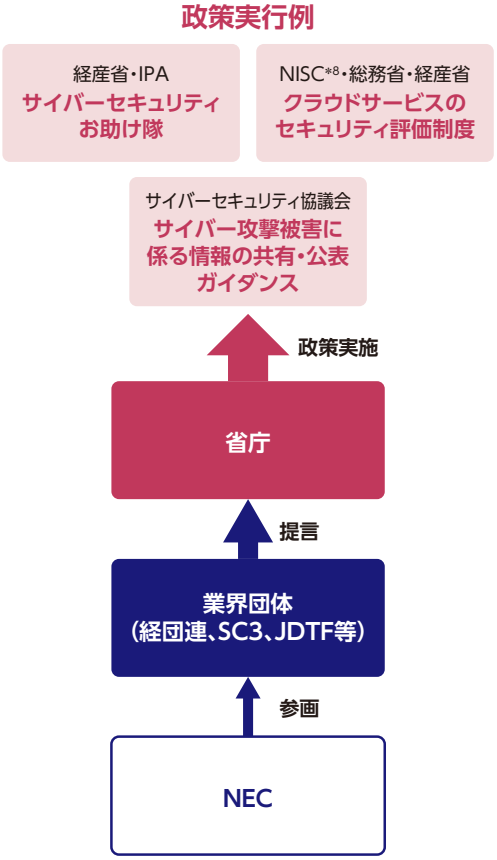
組織間連携

情報通信インフラにおけるサプライチェーンセキュリティリスクへの対策技術を開発 (2021年10月)
情報通信インフラシステムのセキュリティに関する透明性確保によりサプライチェーンセキュリティリスクの抜本的低減を図るため、日本電信電話株式会社と「セキュリティトランスペアレンシー確保技術」を開発した。

サイバーリスク対応のための組織フレームワークに関するITU-T勧告が発行 (2021年11月)
日本電信電話株式会社 、NTTセキュリティ株式会社、NTTテクノクロス株式会社とともに、サイバーリスクへの対応を戦略的かつ組織的に実現するサイバーディフェンスセンターの概念と、その構築・マネジメント・評価プロセスについて国際標準化に向けて取組み、ITU-TからITU-T 勧告X.1060として発行された。

国立高専機構とNEC、サイバーセキュリティ分野における包括連携協定を締結 (2022年7月)
全国の51の国立高等専門学校に対して、NECが有する最新のセキュリティの技術や知見を掛け合わせた産学共同の教育支援を行うことで、企業でこれまで以上に活躍できる実践力を持った人材の育成・輩出に貢献する。

業界団体を通じた政策提言



*3 JC3: Japan Cybercrime Control Center *4 ICT-ISAC: ICT Information Sharing and Analysis Center
*5 ITU-T(International Telecommunication Union Telecommunication Standardization Sector): 国際電気通信連合電気通信標準化部門 *6 チーフオペレーティングオフィサー
*7 JDTF(Japan Digital Trust Forum): 一般社団法人デジタルトラスト協議会 *8 NISC(National center of Incident readiness and Strategy for Cybersecurity): 内閣サイバーセキュリティセンター

3 | 世界トップレベルの人材と技術

❶ 高度なサービス提供のための体制

NECのグループ会社には、高度なサービスの提供を実現するNECセキュリティ株式会社や株式会社サイバーディフェンス研究所があります。特に、セキュリティ監視を行うセキュリティオペレーションセンターについては、日本に限らず、北米やシンガポールなどの海外拠点にも設置しています。海外に拠点があることで、日本の情報だけでなく、海外のサイバー攻撃の情報を活用し、24時間対応の監視を実現することでお客様に安全・安心を提供していきます。

❷ 社内人材育成

NEC及びNECのグループ会社は、セキュリティ人材育成に向けた取り組みにも力を入れており（詳細はP.12の「情報セキュリティ人材」を参照）、セキュリティ技術を競うコンテストの世界大会で上位入賞を果たした社員も在籍しています。

❸ 国内セキュリティ人材育成

2022年7月に独立行政法人国立高等専門学校機構（以下、高専機構）と、サイバーセキュリティ分野における人材育成強化を目的に包括連携協定を締結しました。この協定により、高専機構の60年に渡る社会ニーズに応じた社会実装教育による高度技術者育成と、NECが有する最新のセキュリティの技術や知見を掛け合わせた産学共同の教育支援を目指します。教職員とNECの専門技術者との情報交換などによる最新動向の共有、トップセキュリティエンジニアによる出前授業、学生が活用できるサイバーセキュリティ演習環境の提供、体系的なセキュリティ知識習得のための教材作成などを共に行うことで、企業で活躍できる実践力を持ったエンジニアの育成・輩出に貢献しています。

2023年9月には高専女子学生向けのイベント「K-SEC CAMP FOR GIRLS in KISARAZU」を高専機構と共催し、NECの女性セキュリティエンジニア3名とのキャリアワークショップや社内のCTF問題を活用したテクニカルワークショップを行いました。

❹ お客様への教育プログラム提供

NECは、NECアカデミー for DXとして、経済産業省と独立行政法人情報処理推進機構(IPA)が2022年12月に公開した「デジタルスキル標準」に基づき、DX推進人材育成プログラムを提供しています。

本プログラムでは、リスク検討や体制構築等ビジネスにおけるセキュリティマネジメントを担う推進人材を育成するプログラムや、サイバーセキュリティリスク対策を担う専門人材を育成するプログラムを提供しています。

高専機構とNECが主催したテクニカルワークショップ

4 | セキュリティ実装の徹底

NECは、お客様へ安全・安心な製品・システム・サービスを提供するために、セキュリティ実装を推進する体制を構築しています。昨今のサイバー攻撃の増加や巧妙化などを鑑み、2022年9月に策定したサイバーセキュリティ管理規程を2023年10月から全社規程として施行しています。さらに業務プロジェクトのセキュリティ対策状況や脆弱性情報を一元管理して活用することで、セキュリティ施策展開およびセキュリティガバナンス強化を実現しています。(詳細はP.18の「セキュアな製品・システム・サービスの提供」を参照)

また、DXの加速によりデータ、システムなどが複雑に絡み合う環境のセキュリティを確保するために、NECは「セキュリティ・バイ・デザイン(SBD)」に基づき、いち早く最新の脅威に対応できるセキュリティの実現を目指しています。

5 | 自社運用ノウハウをもとにセキュリティ強化をサポート

サイバーセキュリティ対策は、製品やサービスを導入すれば終わりではありません。サイバーリスクマネジメントが重要課題となっている昨今、高度化・巧妙化が進むサイバー攻撃に対抗するには、サイバーセキュリティ対策を適切に運用して正しい状態を維持し続ける、データドリブンなサイバーセキュリティ経営とアクションを実行する文化の醸成が不可欠です。

NECでは、NECグループに対するサイバー攻撃状況や各社・部門毎のリスク状況を可視化するサイバーセキュリティダッシュボード(P.26参照)を活用し、グローバルに展開するグループ11万人のセキュリティ対策からの生きたナレッジを蓄積しています。これにより経営陣の迅速な意思決定や全社員の危機意識の醸成、俯瞰的な分析による自律的なアクションなどのセキュリティ強化を促進しています。

DXによる新たなセキュリティリスクへの対応

DXが浸透する中、安全性確保への社会的要請が強まっています。DX時代におけるセキュリティリスクへの対応、およびお客様が安全にDXを進めるために、NECグループの支援体制についてご紹介します。

1 | DXによるリスクの変化

❶ セキュリティリスクの変化

DXが急速に進む一方で経済目的のサイバー攻撃が激化し、あらゆるシステムやデータが標的となり企業の事業継続が脅かされています。DXによりシステム間連携が進み、被害は1つの組織にとどまらないことも最近のセキュリティリスクの傾向として挙げられます。このような状況の中、国際機関や国、各業界においても、国や人の安全を脅かすセキュリティの脅威に対応して安全を確保するため、経済安全保障推進法*1をはじめとして各分野で法規制・ガイドラインの整備が進みつつあります。その中で企業は自社だけではなく、委託先などを含めたサプライチェーン全体でのセキュリティ対策への対応が求められるようになってきています。

❷ クラウド環境におけるセキュリティリスク

守るべき情報がオンプレミスからクラウド上へ移行したことや、社外からのリモート接続が増加したことなどの理由により、従来のネットワーク境界中心の対策は限界を迎えつつあります。企業でクラウドサービスの利用が普及する一方で、利用者側の設定ミスや誤操作などを原因とする情報漏えいや不正アクセスも多く発生し、クラウドサービスへのセキュリティ対策が急務となっています。

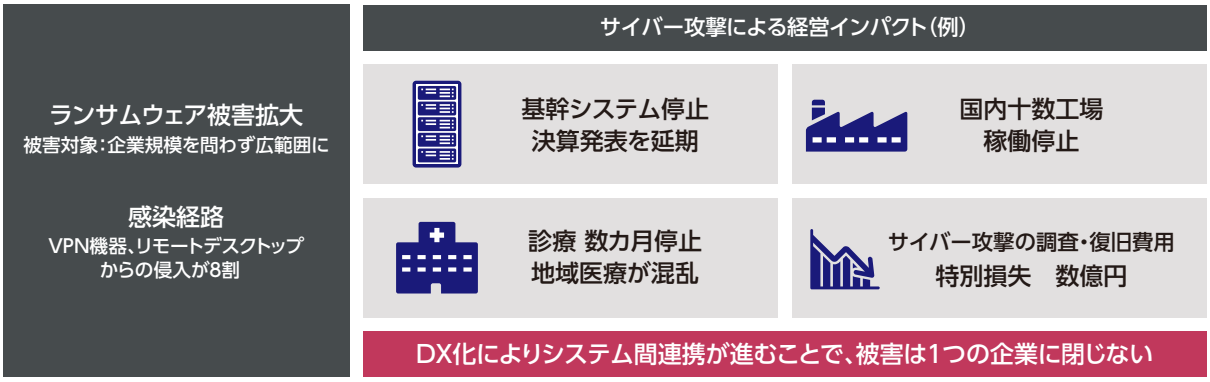
❸ 外部公開IT資産からの侵入リスクの増加

DXが進展する中、クラウドやテレワークの利用拡大に加え、企業が所有するIT資産が増加、点在するとともにテレワークなどリモート化も進んでいることから、サイバー攻撃の起点となるAttack Surface（攻撃対象領域）が増加しています。また、従来のランサムウェアはメールやWebサイトが主な感染経路でしたが、最近では外部に公開されたサーバやネットワーク機器の脆弱性などが悪用された感染が急激に増加しており被害が深刻になっています。そのような背景から、インターネットからアクセス可能なIT資産の情報を調査し、それらに存在する脆弱性を発見して管理するASM*2が注目を集め、経済産業省からもASM導入ガイダンス*3が公開されています。

2 | アーキテクチャーとともに変化するセキュリティ対策

DXによりテレワークの導入やクラウドサービス利用が進むことで、守るべき情報資産を社内に置いてネットワークの境界で防御する従来の考え方では、安全性の担保が困難になっています。DXを安全に推進するためには、情報資産と脅威が社内外に存在することを前提に、アクセスするものはすべて信頼せずに都度、認証・認可を行うゼロトラストモデルを採用し、脆弱性を常に排除するサイバーハイジーン（衛生管理）の徹底が急務となっています。また、認証・認可された利用者であっても故意・過失、また

セキュリティリスクの変化



*1 経済安全保障推進法（内閣府）：https://www.cao.go.jp/keizai_anzen_hosho/index.html
*2 ASM: Attack Surface Management　*3 ASM導入ガイダンス（経済産業省）：https://www.meti.go.jp/press/2023/05/20230529001/20230529001.html

は、外的要因により内部情報が持ち出され、外部へ流出してしまうのを防ぐことが必要となります。さらにテクノロジーによる対策以外にもセキュリティ意識やリテラシーを向上させる教育を継続的に実施し、人を対象としたサイバー攻撃への対応力を強化するなどの人的対策も重要です。

対策すべき箇所が分散し、データやシステムが複雑に連携するDXの環境下では、全体的なセキュリティリスクの把握や網羅的なセキュリティ対策を行うことが難しくなり、顕在化させるべきリスクが潜在化してしまいがちです。NECでは、まずは組織全体のセキュリティリスクを可視化し、戦略策定から設計、運用・監視まで一貫したプロセスで対応し、部分最適を改めて全体最適化を図っていくことが、現在のセキュリティにおける重要なテーマと考えています。

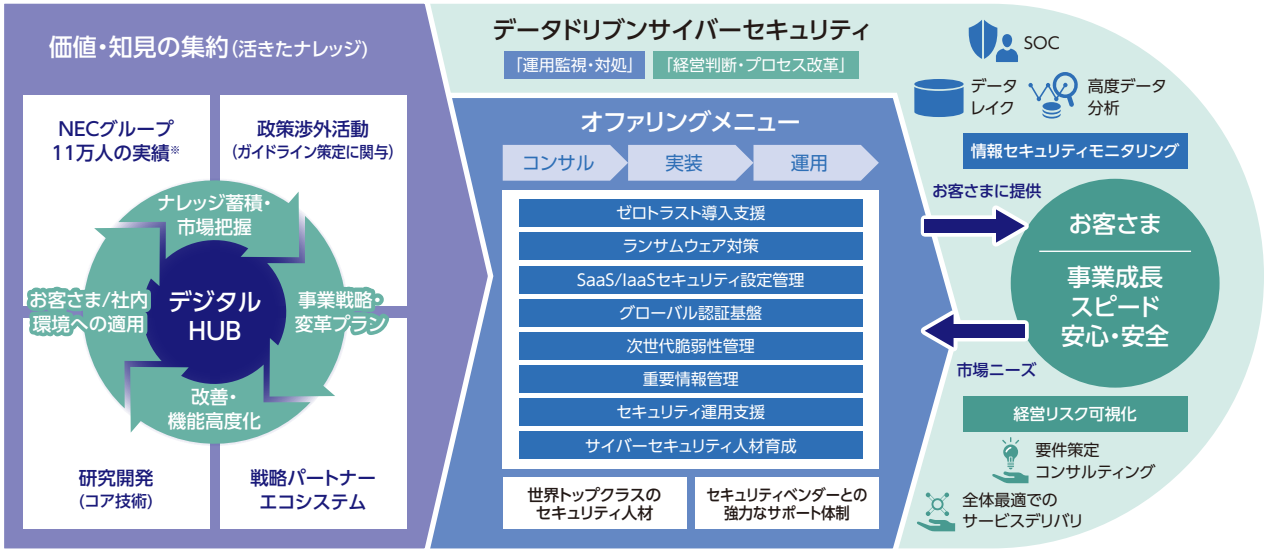
3 | 安全にDXを進めるためにご支援できること

NECでは、研究開発と戦略パートナー連携により、最先端のテクノロジーを最初に自社に実装する「クライアントゼロ」という取り組みを推進しています。また、NEC自身が取り組んできたセキュリティ対策と多くのお客様支援実績により裏付けられた価値と知見を「活きたナレッジ」として収穫・蓄積しています。さらにこれらをパッケージ化した「オファリングメニュー」として提供し、お客様のテーマや直面している課題に合わせてコンサルティングから実装、運用までをトータルにサポートしています。

DX/クラウドシフトに求められるセキュリティソリューション例

課題	対策すべきポイント	ソリューション例
統合ID・アクセス管理	・分散しているシステムやアプリケーション・SaaSのログイン情報やアクセス権限を一元管理 ・強固な認証方式（シングルサインオン、多要素認証）を採用	・SECUREMASTER、Okta
重要情報管理	・機密性や重要度によってデータを分類 ・重要と分類された情報への操作を制御	・重要情報保護ソリューション導入サービス
サイバーハイジーン	・社内で使用しているIT資産、脆弱性の洗い出し ・IT資産の脆弱性をリアルタイムに把握し、排除	・UEM（Unified Endpoint Management）
クラウド設定管理	・クラウドの設定不備などを継続的に可視化し、自動で修正	CSPM※4、SSPM※5
セキュリティリスクの可視化と是正	・組織内のセキュリティリスクを網羅的に可視化・分析 ・継続的、効率的なセキュリティリスクマネジメントの実施	・データドリブンサイバーセキュリティサービス
従業員のセキュリティ意識・リテラシーの向上	・従業員のセキュリティレベルを可視化 ・継続的・効果的な教育やトレーニングの実施	・NECセキュリティアウェアネストレーニング

安全にDXを推進するためのオファリングを提供



※2024年6月時点

*4 CSPM（Cloud Security Posture Management）：クラウド基盤のセキュリティ設定管理　*5 SSPM（SaaS Security Posture Management）：SaaSのセキュリティ設定管理

さらに2023年には、政府機関および重要インフラ企業等へのセキュリティサービスの提供と運用の豊富な実績のある旧株式会社インフォセックスを母体として高い専門性と実践経験を持つセキュリティ人材を結集し、NECセキュリティ株式会社を発足しました。2024年からは、NEC内のサイバーセキュリティ事業を同社に統合し、高度かつ包括的なサイバーセキュリティのソリューションやサービスを提供しています。

旧株式会社インフォセックスのこれまで培ってきた知見に加え、NECグループ11万人の情報セキュリティ基盤への運用の実績、NECグループの高度なサービス提供を支えるセキュリティ高度専門人材を融合させることで、お客様のセキュリティ戦略の策定から対策導入・運用・監視・対処まで、End to Endで効率的かつ効果的なセキュリティリスクマネジメントの実現を支援していきます。

4 | 全体最適に向けてNECがご支援できること

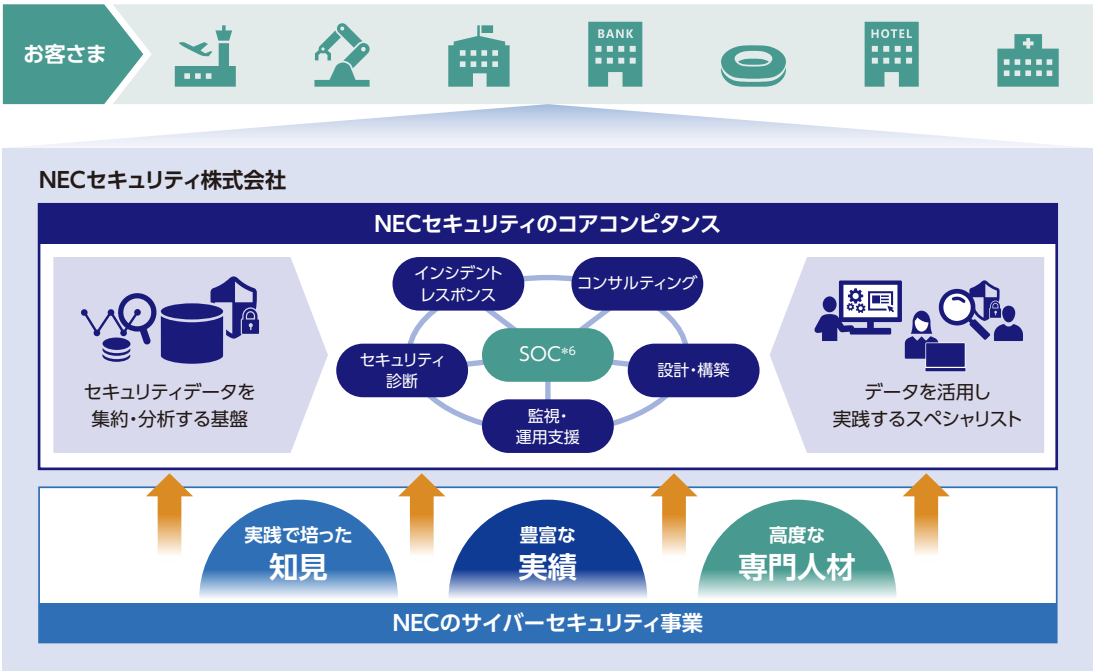
セキュリティリスクの潜在化を解消するためには、システム全体で「今、何が起きているか」、「どこまで対策できているのか」を把握し続けることが重要です。NECではこれを実現するために独自のサイバーセキュリティダッシュボードを作り、システム管理者含む従業員および経営層のそれぞれの観点から必要なデータを可視化し、データを起点としたデータドリブンでのセキュリティリスクマネジメントとサイバーセキュリティ経営の実践を実現しています。

NECでは、これまで社内で蓄積してきたサイバーセキュリティダッシュボードの構築や運用で得たナレッジをもとにデータドリブンセキュリティサービスをお客様に提供し、お客様のセキュリティ業務DXの実現を支援しています。

サイバーセキュリティダッシュボード：

可視化・監視のカギを握るサイバーセキュリティダッシュボードは、運用監視・対処と経営判断・プロセス改革という2つの目的に合わせて最適なものをご提案します。前者は、各セキュリティ対策状況の確認やインシデント状況の把握、ログ解析、調査など、情報セキュリティモニタリングを行うために最適化しています。後者は、パッチや対策の未適用数・割合、サイバー攻撃の疑い件数など経営リスクを可視化しやすいように設計しています。この2つのサイバーセキュリティダッシュボードを通じて、お客さまは自社の全体的なセキュリティ対策状況やリスクの現状を把握したり、お客様導入済みの既存ソリューションの部分最適を是正したりすることにつながります。

NECセキュリティ株式会社が提供するサービス



*6 SOC: Security Operation Center

セキュリティ監視分析：

セキュリティ監視分析において豊富な経験を持つサイバーセキュリティデータサイエンティストと呼ばれる専門人材が、膨大な運用監視データから現在起こっていることを分析し、お客さまのセキュリティ業務の課題を洗い出します。この分析結果をもとに、セキュリティ実装において豊富な知見を持つテクニカルコンサルタントとも連携し、お客さまに最適なアーキテクチャー、運用プロセスの提案を行っていきます。

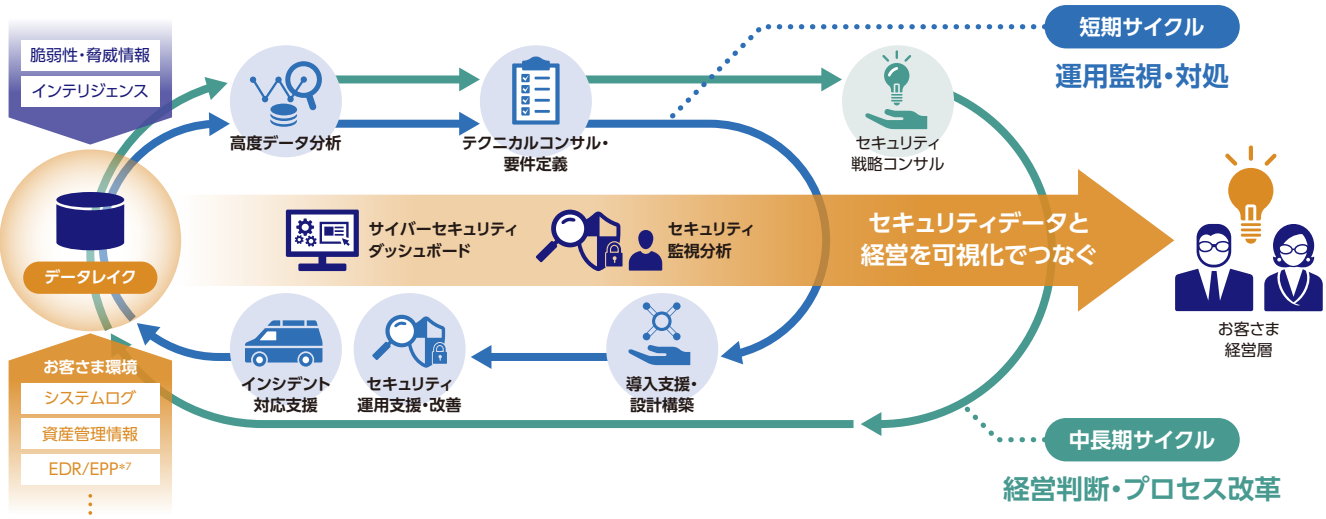
外部IT資産リスク可視化サービス：

ランサムウェアを始めとする昨今のサイバー攻撃に頻繁に悪用され、対策上の要注意ポイントとなっている外部公開IT資産に関する脆弱性と、漏えいした認証情報にフォーカスしてリスクを分析・可視化します。

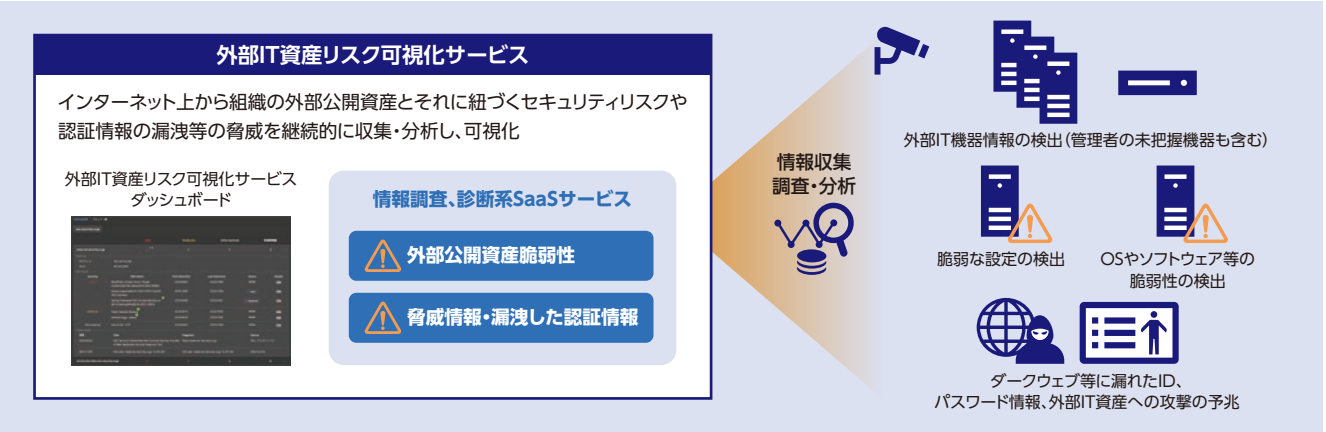
本サービスでは、ペネトレーションテストやインシデントレスポンスの豊富な経験を持つ専門人材が、これまでの経験をもとにサイバー攻撃への対策として注視すべきデータを可視化できるように設計しており、お客さまが早期に対応すべきリスクを可視化することでサイバー攻撃被害の防止や抑制につながります。

最後に、DXが急激に進む一方でセキュリティリスクに晒されるようになりセキュリティ対策が急務となっています。NEC ではNECで蓄積した知見や経験を活かし、お客様のセキュリティ対策を支援しています。NECがご提供している各種ソリューションや支援メニューについて詳しく知りたいお客様は、NECまでお気軽にお問合せください。

データドリブンサイバーセキュリティによる全体最適化プロセス



外部IT資産リスク可視化サービス



*7 EDR/EPP: Endpoint Detection and Response, Endpoint Protection

最前線でのサイバーセキュリティ技術の研究開発・事例

NECはセキュリティ・バイ・デザイン(SBD)の設計思想のもと、システムセキュリティとデータセキュリティの両面による研究開発を通じて、サイバー攻撃の脅威から社会基盤や組織を守ります。

1 | 研究テーマのコンセプト

NECグループでは、誰もが安心してデジタル技術を活用できる社会を実現するためにセキュリティ・バイ・デザイン(SBD)の考えのもと、システムセキュリティおよびデータセキュリティの両面から最先端の研究開発を行っています。

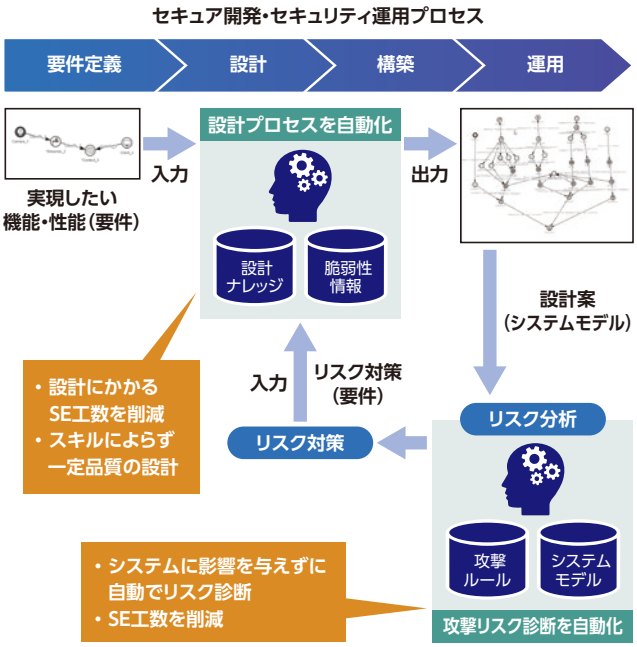
本稿では、システムセキュリティ研究の例として、セキュアなICTシステムの設計を自動化する「セキュアシステム自動設計」を紹介します。また、データセキュリティ研究の例として、生体特徴量を暗号化したまま顔認証を行う「秘匿生体認証」および、組織間でデータを互いに開示することなくAIモデルを構築する「ハイブリッド高秘匿連合学習」を紹介します。

2 | セキュア開発・セキュリティ運用の自動化

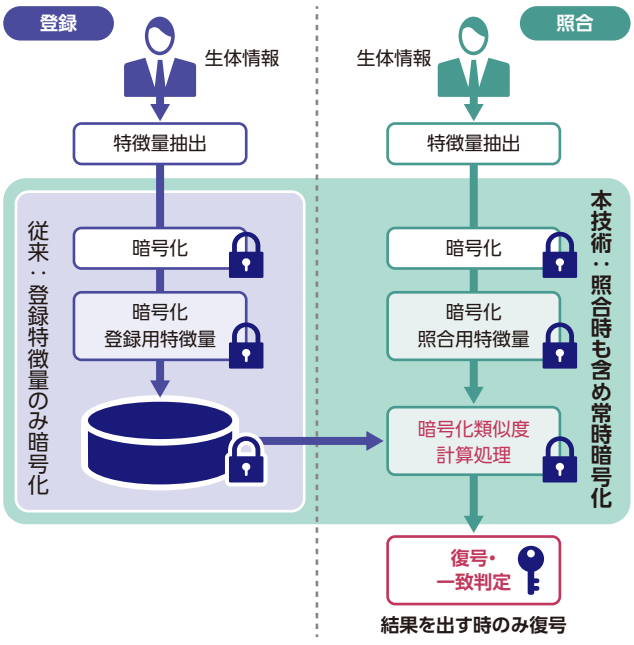
企業システムや社会システムのDX化推進に伴いICTシステムは複雑化しており、サイバー攻撃のリスクも高まっています。サイバー攻撃リスクが増え続ける中、ICTシステムのセキュリティを強化するためには(セキュリティ・バイ・デザイン)が求められます。しかし、これまでのように人手による設計・開発では複雑なICTシステムのセキュリティ確保が困難であり、対応工数が莫大になっています。NECでは、複雑なICTシステムの設計を自動化する技術を開発しています。セキュリティを含んだICTシステムに求められる機能や性能(要件)をもとに、AIがICTシステムを構成する部品を自動で組み合わせて評価することで、要件に合ったセキュアなシステム構成を導出します[*1]。

しかし、セキュアなICTシステムを構築したとしても、新たな脆弱性が発見されるなど、時間の経過により、サイバー攻撃のリスクが高まってきます。そのため、システム運用においても、セキュリティリスクを定期的に診断し、対処していく必要があります。通常、人手で実際にシステムを調査することでリスクを判定しますが、人手による時間・工数がかかること、実システムの調査によりシステム停止などの課題があります。NECは、サイバー攻撃リスク診断技術によりICTシステムに生じるサイバー攻撃リスクを自動で診断することができます。自動設計で得られたシステム情報

セキュア開発・セキュリティ運用プロセスの自動化



秘匿生体認証の流れ



*1 S. E. Ooi, R. Beuran, T. Kuroda, T. Kuwahara, R. Hotchi, N. Fujita, Y. Tan, "Intent-Driven Secure System Design: Methodology and Implementation", Elsevier Computers & Security, vol. 124, January 2023, 102955. https://www.sciencedirect.com/science/article/pii/S0167404822003479

*2 一般財団法人 テレコム先端技術研究支援センター2022年度SCAT表彰 会長賞「サイバー攻撃リスク自動診断技術の研究開発と実用化」柳生智彦、植田啓文、井ノ口真樹、木下峻一、水島 諒 https://jpn.nec.com/rd/awards/2022/2022-06.html https://www.scat.or.jp/cms/wp-content/uploads/2022/12/award-press2022.pdf

*3 公益財団法人 電気科学技術奨励会 第69回電気科学技術奨励賞「サイバー攻撃リスクを洗い出す自動診断技術の開発と実用化」井ノ口真樹、木下峻一、柳生智彦 https://jpn.nec.com/rd/awards/2021/2021-06.html http://shoureikai.or.jp/img/awards/past/award_69.pdf

を利用して、コンピュータシミュレーションによる網羅的な攻撃パターン調査を行うことで、運用中のシステムに影響を及ぼすことがなく、自動でセキュリティリスクを判定できます。さらに、診断結果をもとにセキュアなシステム構成を自動で導出することで、システムのセキュリティを維持することができます[*2*3]。

NECでは、これまで多くの工数を要したシステムのセキュア開発、セキュリティ運用を自動化し、システムの設計・開発、運用を支援します。

3 | 秘匿生体認証

本人確認の手段として導入が進む顔認証では、登録された生体情報が万が一漏えいした場合、なりすましなどに悪用されるリスクにつながります。このようなリスクに対応するため、顔認証などの生体認証において、生体情報から取得した生体特徴量を登録時のみならず照合時も含めて全て暗号化したまま行う「秘匿生体認証」の研究開発に取り組んでいます[*4*5]。

秘匿生体認証では、特徴量を暗号化したまま顔認証の照合処理を実現するため、「マルチパーティ計算」や「準同型暗号」による秘密計算技術を活用しています。大規模な利用シーンにおいては、マルチパーティ計算を用いた方式が適しており、登録ユーザ数100万人程度で1秒以内の顔認証の照合処理を行うことが可能です。また、中～小規模の利用シーンでは1台のサーバで提供可能な準同型暗号を用いた方式が適しており、登録ユーザ数1万人程度で1秒以内の顔認証の照合時間を実現しています[*6]。さらに、本技術をデジタル署名に応用し、生体特徴量からデジタル署名を生成してデータに付与する技術を開発しています[*7]。生体特徴量から生成されたデジタル署名を検証することで、本人によってデータの真正性が保証されていることを確認できるようになります。

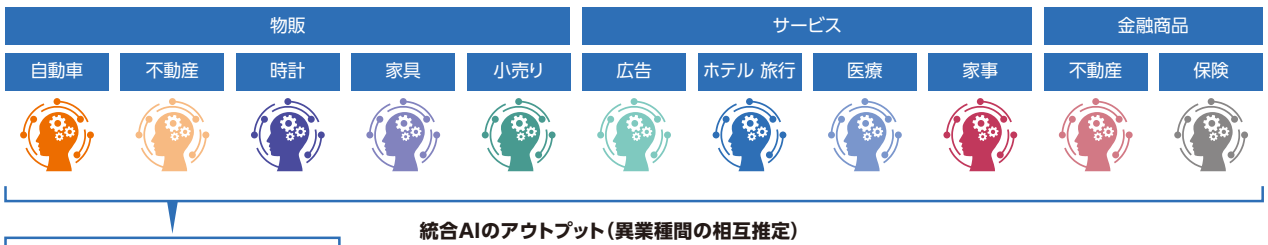
これらの技術の活用により、顔認証をはじめとした生体認証の安心・安全な利用に貢献します。

4 | ハイブリッド高秘匿連合学習

様々な企業がデータを収集し、集めたデータを用いて構築したAIを営業活動に活用しています。例えば、見込み顧客推定などがAIで行うことができますが、このようなAIを拡張して業種をまたぐようにすること、例えば自動車業界の購買データを使って不動産の購入価格帯を予測するようなAIを構築することは困難です。もちろん両業種のデータを一か所に集めることができれば問題なく構築できます。しかし、異なる業種が保有するデータを集積することは、企業秘密の他社提供といった機密上の問題だけではなく、個人情報保護に関わる法的な問題にも関係し、容易には実施できません。ハイブリッド高秘匿連合学習は、直接的にはデータを集めず、業種をまたぐような属性推定を実現します。本技術の活用により、多様な業種のAIを統合し、相互に属性推定が行えるような統合AI基盤の提供を目指しています[*8*9]。

ハイブリッド高秘匿連合学習による異業種連携

異業種（自動車、不動産、時計など）のローカルAIを、複数企業間で統合し、相互の推定を可能とする統合AI基盤を実現



統合AIのアウトプット（異業種間の相互推定）

	自動車			不動産		時計	
名前	大衆車	RV	ミニバン	物件価格	確率	モデル	確率
Xさん	50%	0%	0%	2500	30%	デジタル廉価	40%
Yさん	10%	50%	10%	4000	50%	スマートウォッチ	30%
Zさん	10%	10%	80%	6500	70%	自動巻き時計	100%

高価な家を買う人は、ミニバンを好む

自動巻き時計を買った人は、高価な家を好む

*4 顔認証の利活用 ～人権に配慮したNECの取り組み～　*5 今岡仁, 櫻井和之, 塚田正人, 宮川伸也, 大網亮磨, 一色寿幸, "生体認証が切り拓く未来", NEC技報 Vol.74 No.2 (2022).
*6 Hiroto Tamiya, Toshiyuki Isshiki, Kengo Mori, Satoshi Obana, Tetsushi Ohki, "Improved Post-quantum-secure Face Template Protection System Based on Packed Homomorphic Encryption", BIOSIG2021(2021).
*7 Haruna Higo, Toshiyuki Isshiki, Saki Otsuki, Kenji Yasunaga, "Fuzzy Signature with Biometric-Independent Verification", BIOSIG2023(2023)
*8 "高秘匿連合学習　プライバシー・機密情報保護とAI活用を両立", NEC 研究開発特集記事, https://jpn.nec.com/rd/special/202103/index.html
*9 Junki Mori, Ryo Furukawa, Isamu Teranishi, Jun Sakuma: "Heterogeneous Domain Adaptation with Positive and Unlabeled Data". IEEE Big Data 2023:

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。

グローバルなESG投資指数 DJSI APAC Index

情報セキュリティ/サイバーセキュリティ/システムの利用可用性の項目においてITサービスセクター内で最上位クラスの評価を4年連続(2020～2023)で獲得。2022、2023年は100点満点を獲得。

Member of
Dow Jones
Sustainability Indices
Powered by the S&P Global CSA

国内業界団体による格付け
日本IT団体連盟 サイバーインデックス

「特に優れた取り組み姿勢および情報開示を継続的に確認できた」とする星二つを獲得(最高位)。
(日経500種平均構成銘柄の企業の中から14社が選出)

IT連
日本IT団体連盟

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。
一般社団法人情報マネジメントシステム認定センターのISMS認証取得組織検索に公表されている会社のみ掲載(2024年6月14日時点)

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スペース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セキュリティ株式会社
- 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
- NEC静岡ビジネス株式会社
- 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ネッツエスアイ・サービス株式会社
- 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ビジネスインテリジェンス株式会社
- 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
- 株式会社ベストコムソリューションズ
- 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
- KISドットアイ株式会社
- K&Nシステムインテグレーションズ株式会社
- NEC静岡ビジネス株式会社
- 日本電気通信システム株式会社
- 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

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
  (セキュア情報交換システム)
- NEC ファイアウォール SG
  (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

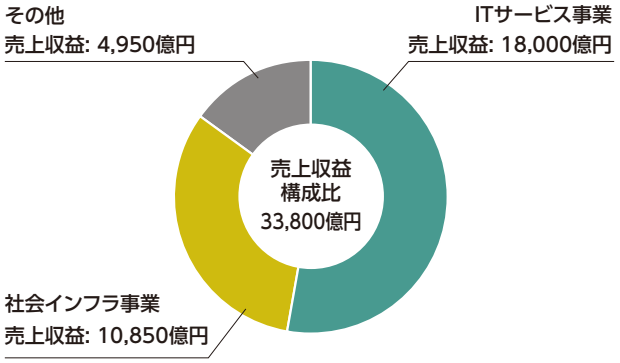
会社概要

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	4,278億円※
連結従業員数	105,246名※
連結子会社数	254社※

※2024年3月31日現在

事業紹介

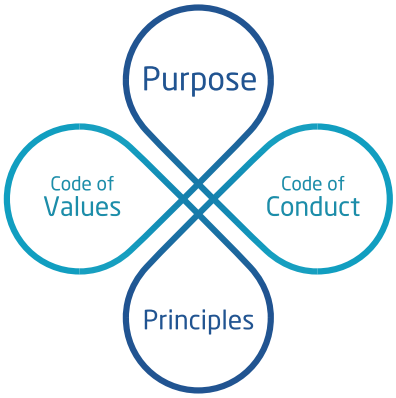
セグメント別売上収益



※2024年3月31日現在

NEC Way[経営理念]

NEC Way



「NEC Way」は、
NECグループが共通で持つ価値観であり行動の原点です。

企業としてふるまう姿を示した
「Purpose(存在意義)」「Principles(行動原則)」と、
一人ひとりの価値観・ふるまいを示した
「Code of Values(行動基準)」「Code of Conduct(行動規範)」
で構成されています。

私たちはNEC Wayの実践を通して社会価値を創造していきます。

Purpose
存在意義

\Orchestrating a brighter world

NECは、安全・安心・公平・効率という
社会価値を創造し、
誰もが人間性を十分に発揮できる
持続可能な社会の実現を目指します。

Code of Values
行動基準

視線は外向き、未来を見通すように
思考はシンプル、戦略を示せるように
心は情熱的、自らやり遂げるように
行動はスピード、チャンスを逃さぬように
組織はオープン、全員が成長できるように

Principles
行動原則

創業の精神「ベタープロダクツ・ベターサービス」
常にゆるぎないインテグリティと人権の尊重
あくなきイノベーションの追求

Code of Conduct
行動規範

1. 基本姿勢
2. 人権尊重
3. 環境保全
4. 誠実な事業活動
5. 会社財産・情報の管理

コンプライアンスに関する疑問・懸念の相談、報告

情報セキュリティ報告書2024

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)
https://jpn.nec.com

VEGETABLE OIL INK

2024年７月発行
© NEC Corporation 2024
Cat.No. U01-24060210J