サイバーセキュリティ
経営報告書2025

NEC \Orchestrating a brighter world

「.JP（日本のサイバー空間）」を守る

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（Chief Security Officer）
兼 サイバーセキュリティ部門長
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の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は「.JP（日本のサイバー空間）」を守るをスローガンに掲げ、独自のサイバー脅威インテリジェンスの提供や、国産AI技術を活用した安全性・機能性の両立、グローバル推進体制の確立により、日本の経済安全保障への貢献すべく、サイバーセキュリティ事業を強化しております。

本報告書は、上記をはじめとするNECグループの事業を支えるサイバーセキュリティの取り組みについて、ステークホルダーのみなさまにご理解いただくことを目的として例年発刊しており、2025年からは近年の情勢、動向においてサイバーセキュリティが経営に資することを明示すべく、「情報セキュリティ報告書」から「サイバーセキュリティ経営報告書」に改称いたしました。

今後も、Digital Security Transformationによるサイバーセキュリティ経営を実践するとともに、「クライアントゼロ*1」として社内で実装済みの最先端技術や実運用における知見、ノウハウを付加価値として提供することにより、NECのPurposeである「Orchestrating a brighter world」、人が豊かに生きる「安全」「安心」「公平」「効率」な社会の実現に貢献し、継続的に信頼される企業になることを目指します。

*1 NECが掲げる、「自社をゼロ番目の顧客（クライアント）」として社内実践による知見・ノウハウをお客様や社会に還元、付加価値として提供する取り組み

経済産業省「サイバーセキュリティ経営ガイドライン」Ver3.0重要 10項目

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2 サイバーセキュリティリスク管理体制の構築	指示7 インシデント発生時の緊急対応体制の整備
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

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）

ふちがみ　しんいち
淵上　真一　CISSP
（Certified Information Systems Security Professional）

日本電気株式会社
Corporate Executive CISO（Chief Information Security Officer）
兼 NECセキュリティ株式会社 取締役

NECではCISA*2のゼロトラスト成熟度モデルを踏まえ、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、エンタープライズリスクマネジメントの実践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。データドリブンでの迅速な経営判断と全従業員のアウェアネス、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。

お客様へのシステム、サービス提供においては、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（SBD）」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*3の取得を推進するとともに、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。

これらの取り組みを評価いただき、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「日本セキュリティ大賞2024」で大賞および人材育成部門 優秀賞を受賞、日本IT団体連盟の「サイバーインデックス企業調査2024」で最高位の二つ星を獲得しました。

本報告書では、2025年5月までの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。

*2 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
*3 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）

Contents

2 ｜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様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、お客様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。

3 | 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重要事項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。

また、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。

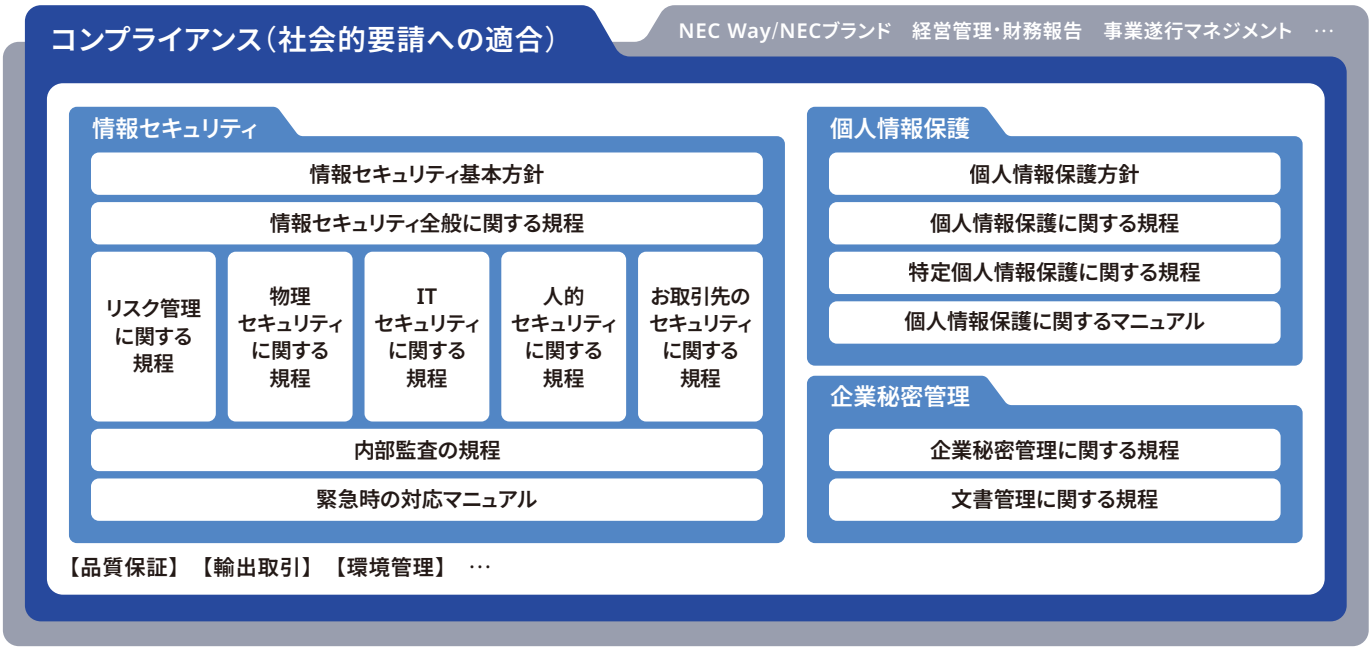
2 情報セキュリティに関するポリシー

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国内グループで28社(2025年3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。海外グループ会社については、共通の個人情報保護ガイドラインを展開した上で、各社にて適用を受ける各国・各地域の個人情報保護法等の法令・規則に準拠した個人情報保護ルールを導入しています。

NECグループ経営ポリシー



*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

3 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。

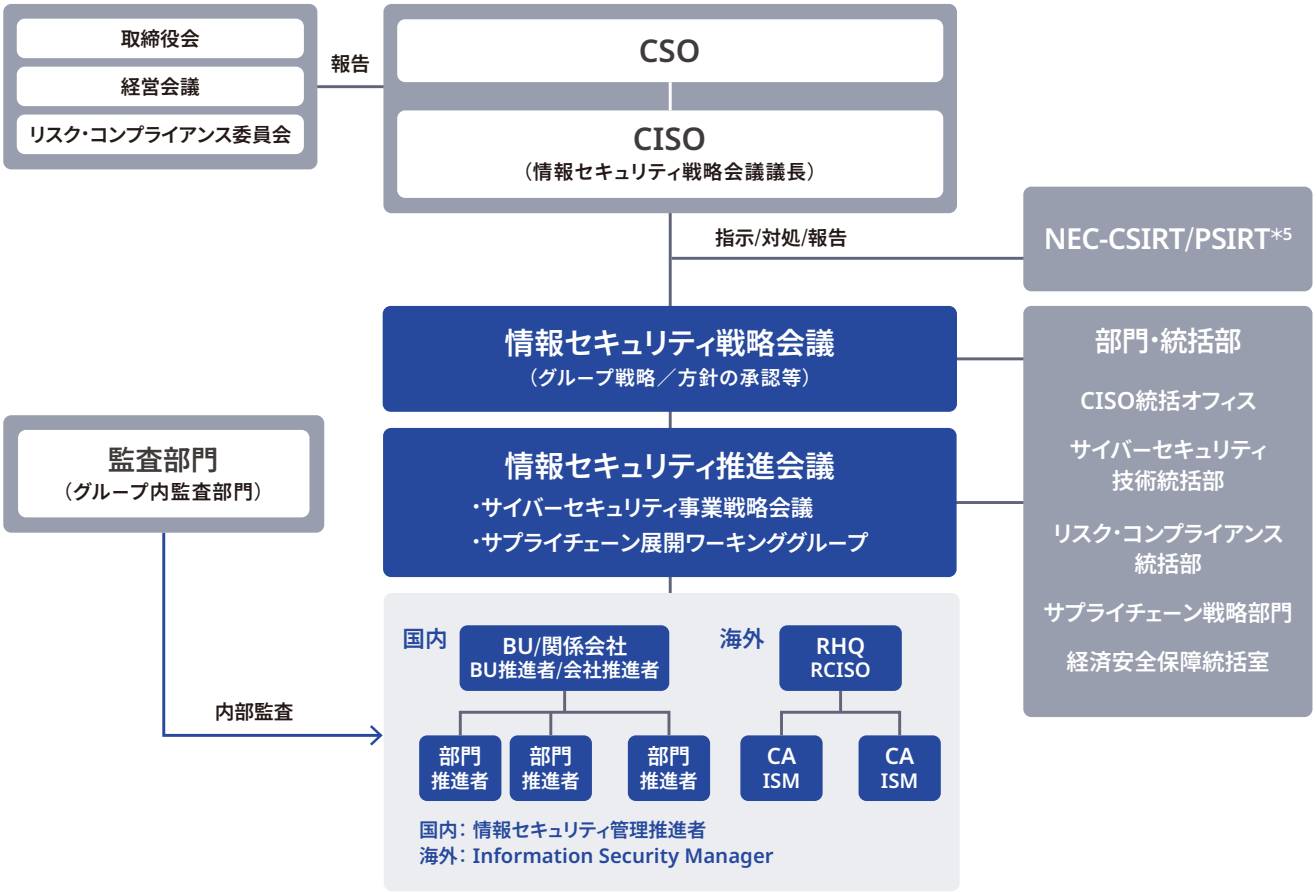
CISOは、情報セキュリティ対策を推進するCISO統括オフィスと、サイバー攻撃を監視しインシデント発生時には迅速に収拾をはかるCSIRT*3を統括します。情報セキュリティ推進会議やワーキンググループは、セキュリティ実装の推進計画、実行施策討議・調整、指示事項徹底、施策進捗管理などを行います。

NECは各部門長が、国内関係会社は社長または役員クラスが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。

以上の体制に加え、取締役がサイバーセキュリティに関与し、監督しています。

また、各海外拠点にISM*4を設置し、担当する拠点のセキュリティ管理とその結果に責任を持たせています。さらにRegional CISOが地域全体を統括することで、グローバル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



*3 CSIRT: Computer Security Incident Response Team　*4 ISM: Information Security Manager　*5 PSIRT: Product Security Incident Response Team

4 ｜ 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・向上を図っています。

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ポリシーに基づき、PDCAサイクルを継続することによる情報セキュリティの維持・向上、情報セキュリティ監査の結果やセキュリティ事故状況に基づいた改善とポリシー見直しを進めています。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。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。

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。

3 重要情報管理

❶ 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。

4 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

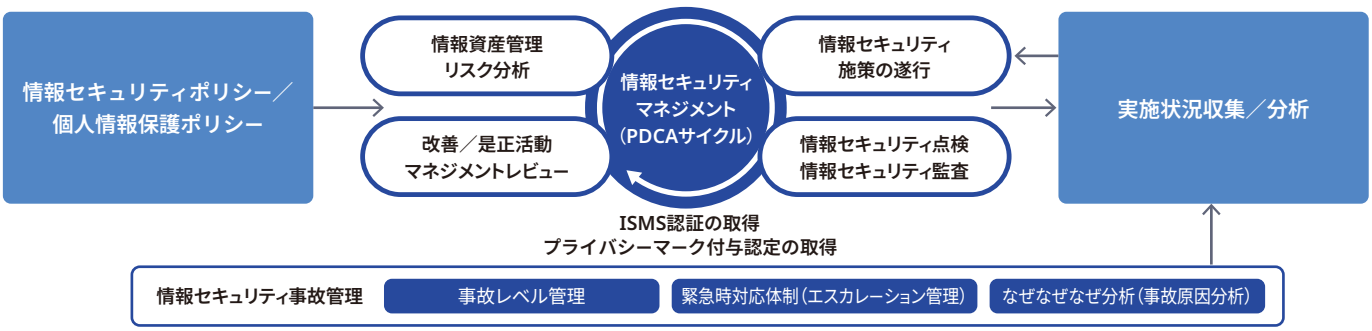
情報セキュリティサーベイは、従業員のセキュリティアウェアネスのレベルを継続的に評価・数値化し、改善を図ることで、高度なセキュリティ文化の醸成を目指す取り組みです。セキュリティアウェアネスとは、日々の業務に潜在するセキュリティリスクに自ら気づき、適切に判断し、対処するための心構えを指します。

この取り組みにより、各従業員がセキュリティを意識し、リスクを考慮した行動をとる習慣を身につけることができ、組織全体のセキュリティ文化の向上に寄与します。

❷ 情報セキュリティ監査

監査部門が中心となり、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に照らし各組織を監査し、各事業分野の動向を参考に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）

NECの情報セキュリティマネジメント



5 ｜ 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）に基づき、「ゼロトラスト基盤」を実現しています。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

昨今のデジタルシフトに伴う環境が変化する中、高度化・複雑化するサイバー攻撃などのセキュリティリスクに対応するため、ゼロトラスト基盤において根幹となる重要な戦略として認証強化・高度化に取り組んでいます。

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）」により、全社的な認証強化・高度化を進め、ほぼ全ての利用者に対するパスワードレス化を実現し、なりすましやサイバー攻撃のリスクを低減しています。

あわせて、なりすましやサイバー攻撃の可能性がある場合のみ追加の認証を要求する「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ではゼロトラストの環境において重要な利用者の認証・認可情報をNECグループ全体で管理する基盤として「IAM基盤*3」を有しており、グローバルに認証とデバイスの統合管理を実現しています。

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。

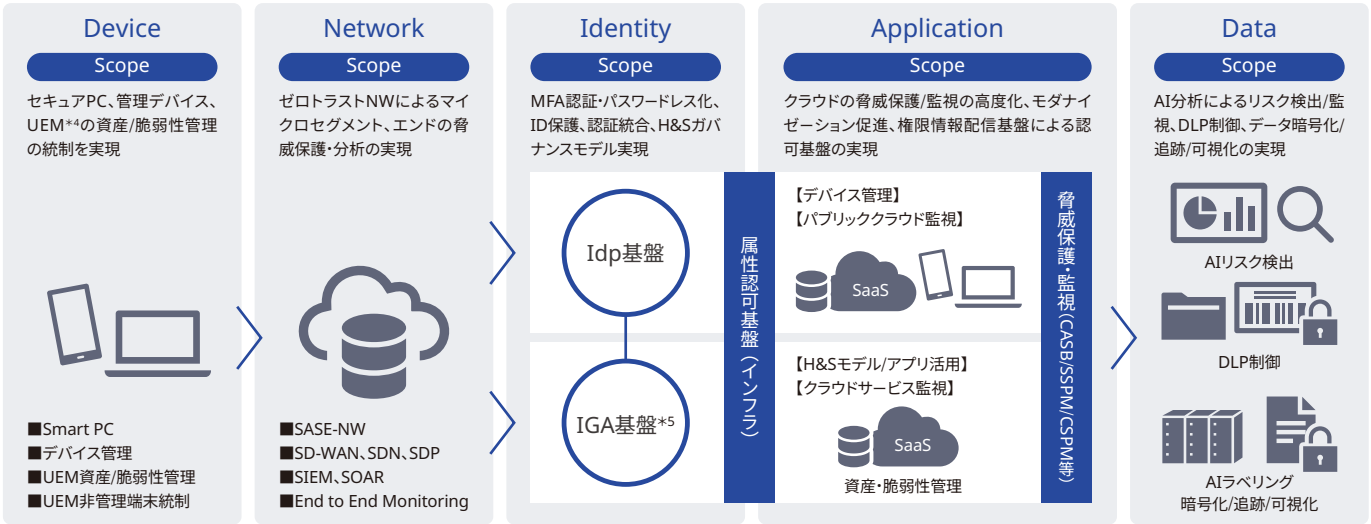
① グローバルID活用	アイデンティティ管理の実現（利用者アカウントの中央統制、ライフサイクル管理）
② 認証・デバイス管理	ユーザ認証（パスワードレス、多要素認証）、デバイス認証/管理端末化の統制環境の実現
③ グローバルアプリ管理	共通システムやサービスのアクセス管理、シングルサインオン（SSO）の実現
④ セキュリティガバナンス	グローバルでのセキュリティポリシーや設定情報の一元管理・統制の実現

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ド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

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 UEM: Unified Endpoint Management Platformの略称。接続場所を問わず、様々な機器を一元管理し、セキュリティレベルの向上を実現する基盤
*5 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

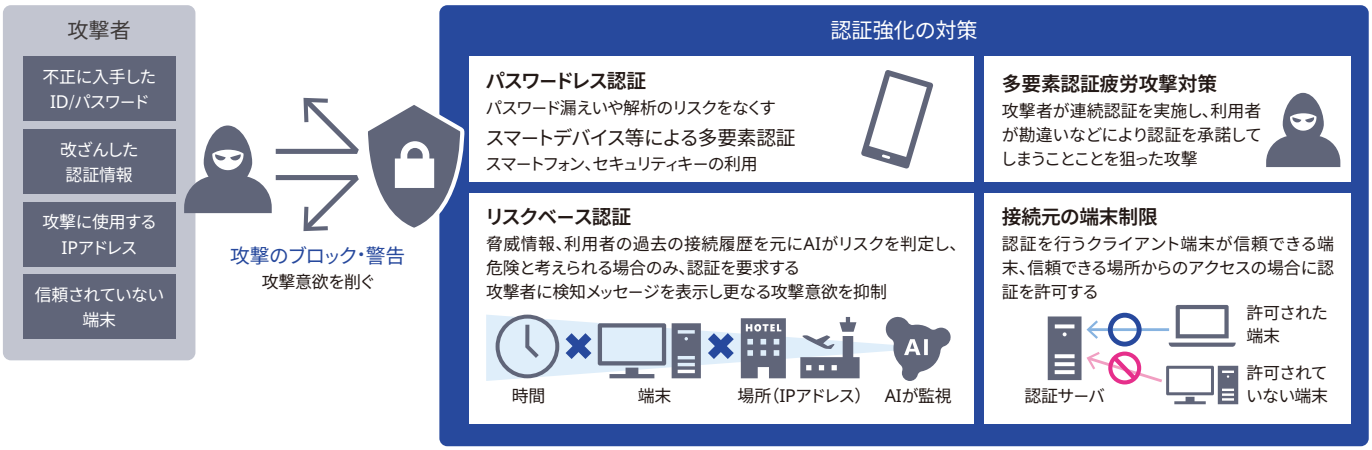
に対応しています。

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）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/海外にある26万台の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。

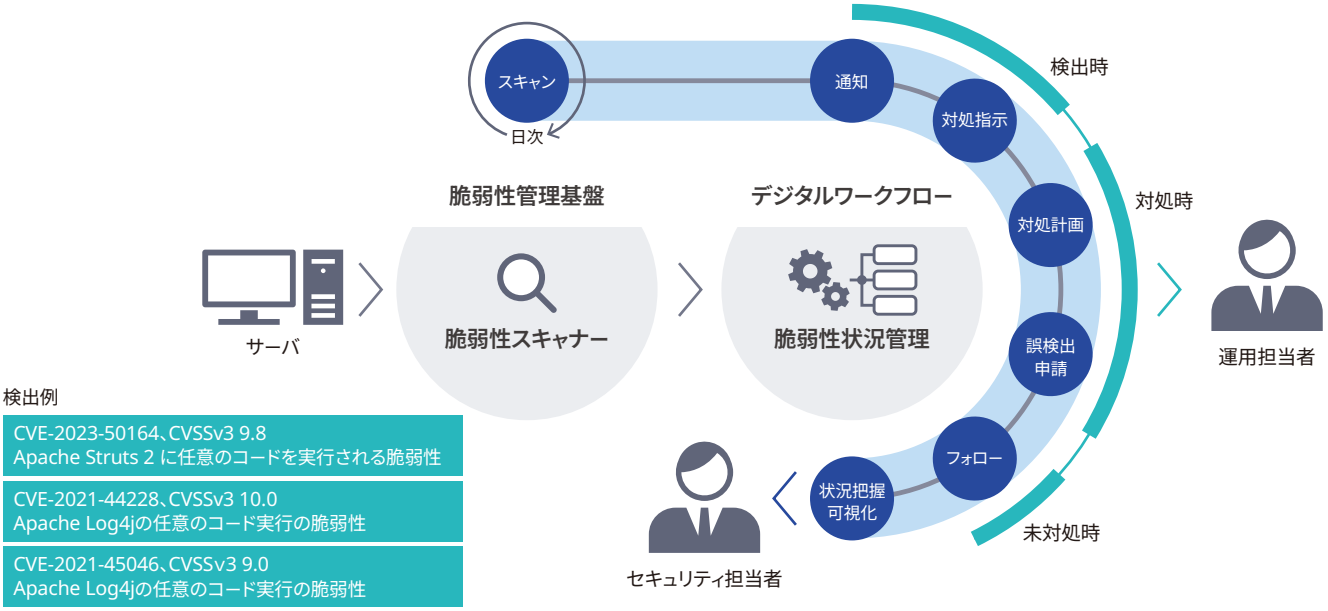
サーバOSの脆弱性管理はサイバー攻撃からの企業システム保護に不可欠であり、継続的な取り組みが重要となります。社内サーバ1万台以上をセキュアに維持するため、2024年度は脆弱性の早期検出・通知、継続的な把握、脆弱性状況の可視化を可能とするデータドリブンセキュリティを実現しました。可視化では、サイバーセキュリティダッシュボードと連携し、脆弱性の対処状況・傾向を可視化することで、経営判断やITシステムのセキュリティアウェアネス向上をサポートしています。セキュリティ対策が不十分な端末やマルウェアなどが検出された端末は、業務ネットワークから遮断する制御を行っています。社外への通信は、許可リスト型のWeb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。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。

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。

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によるデータドリブンセキュリティの実現



検出例

- CVE-2023-50164、CVSSv3 9.8
  Apache Struts 2 に任意のコードを実行される脆弱性
- CVE-2021-44228、CVSSv3 10.0
  Apache Log4jの任意のコード実行の脆弱性
- CVE-2021-45046、CVSSv3 9.0
  Apache Log4jの任意のコード実行の脆弱性

*6 メール送信者のガイドライン
https://support.google.com/mail/answer/81126

3 ネットワークセキュリティ

NECのグローバルネットワークはインターネット・内部ネットワークの区別なくゼロトラスト志向のインフラを展開し、ビジネス環境の安全性確保と可用性確保を支えています。

❶ ゼロトラスト志向のネットワーク

真のゼロトラストアプローチ実現のためエンドポイント・サービスをつなぐネットワークにおいて適切なアクセス制御・接続の認証・認可の環境を実現しています。

・インターネット防御：グローバル約30ヶ国のあらゆるインターネット宛ての通信はSecure Web Gatewayにより集中防御・監視をされており、リモート環境は国内中心にクラウドベースのRemote Gatewayにより自社の通信境界をインターネットに触れさせずに安全に運用しています。

・オフィスや工場の防御：自社の拠点内外の通信のゼロトラストアプローチ実現のために構内ではNetwork Access ControlとSDNベースの仮想ネットワークを組み合わせた制御を進めています（NAC導入は2024年度より、SDN導入は2016年度より）。これによりオフィス業務と特殊業務（生産や開発系）通信の分離を実現しています。

❷ グローバルSD-WAN展開

オンライン会議をはじめとするSaaSやセキュリティ制御のためのトラフィック増と集中制御を実現しています。2024年度までにグローバル6地域間の通信制御、地域間トラフィックの多い国内・APAC・中国本土の地域内・国内の制御のために全289拠点へ展開を完了しました。

・性能や可用性の革新：総帯域を4倍以上に拡張、ネットワーク変更のリードタイムを数分の一に短縮しました。可用性の面では専用線では費用負担の大きかった回線の冗長化を小規模な拠点でも実現しました。

・セキュリティの革新：従来の基盤では難しかった地域を超えた緊急時の通信一斉遮断や拠点単位の通信監視を実現しました。特に緊急遮断では単に基盤を導入するだけでなく、想定される被害（特定サーバへの攻撃、ランサムウェアのラテラルムーブメント）に対し複数の対応シナリオを用意しSOC/NOC連携の机上訓練も実施しています。またインターネットアクセスが可能なSD-WANルータの管理者権限の防御として（なりすまし・内部不正対策の高度化として）、予定外作業実施へのアラート機能や本人・上司へのログイン通知をはじめとする高度な管理機能を国内に展開しました。

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

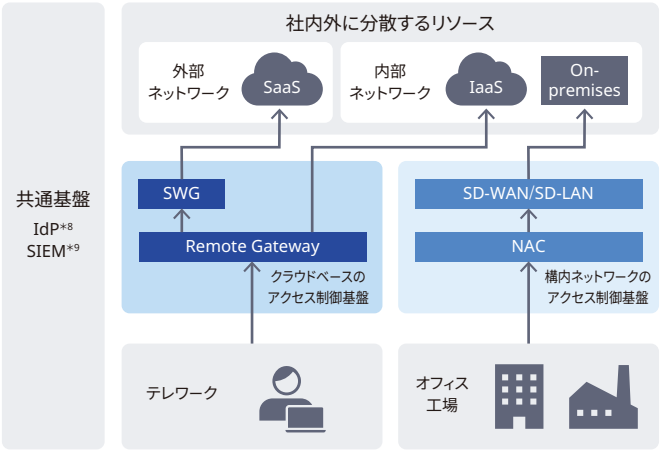
クラウドサービス上のログや保管されているファイルを、CASB[*7]で監視・分析することで、重要なデータを取り扱うクラウドサービスに対する内部不正やサイバー攻撃への対策を実施しています。また、社内で使用されているクラウドサービスの利用状況を可視化し、未承認のリスクが高いクラウドサービスを監視しています。

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

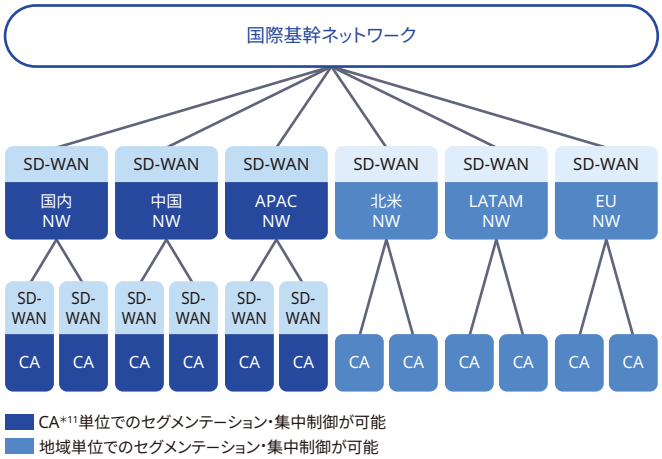
AWSやAzure、GCPなどパブリッククラウドの利用が増加しています。これらのサービスは利用が容易な反面、設定ミスなどにより外部への情報漏えいを発生させるリスクが伴います。

NECグループでは、CSPM[*10]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。

ゼロトラストネットワーク全体像



SD-WANのグローバル展開



*7 CASB: Cloud Access Security Broker　*8 IdP: Identify Provider　*9 SIEM: Security Information and Event Management　*10 CSPM: Cloud Security Posture Management　*11 CA（Corporate Affiliate）: 関連会社

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[*12]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

❶ ファイルラベル/暗号化

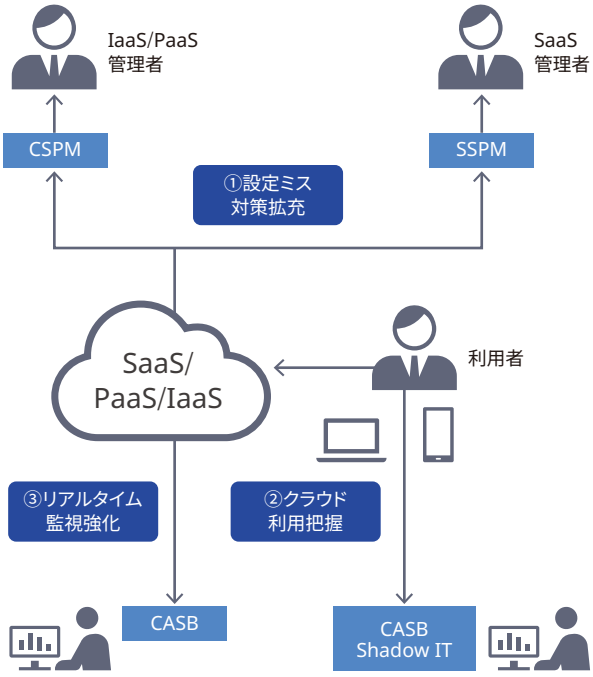
NECグループでは、ゼロトラストセキュリティ観点から、クラウド対応のAIP[*13]統合ラベルとNEC独自ソリューションの「InfoCage FileShell」を用いて、Officeファイル以外も含む各種ファイルの自動分類、暗号化、追跡、アクセス権管理を行い、マルウェア感染などによる外部への情報流出を防いでいます。

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。

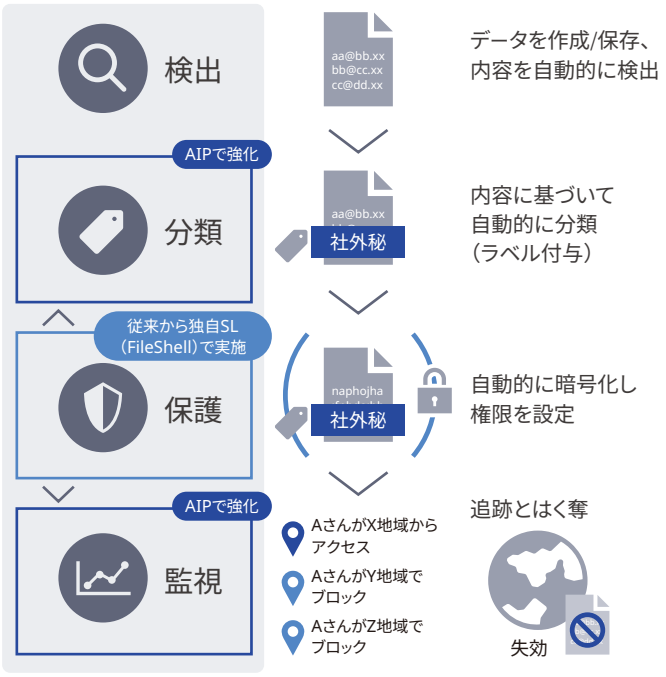
❷ 情報漏えいリスク行動検知

昨今、過失・不注意、故意に関わらず、情報の持ち出しによる情報漏えい事故が社会問題となっています。中には、意図的な不正（内部不正）による情報の持ち出しもあり、転職者が会社の秘密情報を転職先の会社に提供する等の情報漏えいの事案が後を絶たない状況です。また、IPA(独立行政法人 情報処理推進機構)の「情報セキュリティ10大脅威」においても「内部不正による情報漏えい等の被害」は、上位にランクインしています。背景として、雇用の流動化が進んでいること、テレワークの普及により心理的に不正を引き起こしやすい環境に変化していること、DXの浸透により情報流出経路が多様化していること、等が要因と考えられます。このような状況から、NECグループでは内部不正を含む情報漏えいのリスクがある行動を検知・可視化し、対象者への注意や警告を行う仕組みを導入することで、リスクにつながる行動の牽制・抑止、予防を行っています。

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



情報漏えいリスク行動検知

*12 SSPM: SaaS Security Posture Management　*13 AIP: Azure Information Protection

6 ｜ 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。

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（2024年度修了率（2024年度実績）98%。海外7か国語対応）。セキュリティ脅威のトレンドなどを考慮し、教育内容は毎年更新しています。また、新入社員や中途採用社員の受け入れ時にも、学生と社会人との違い、前の会社とNECとの違いといった点にフォーカスし、教育を実施しています。

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。

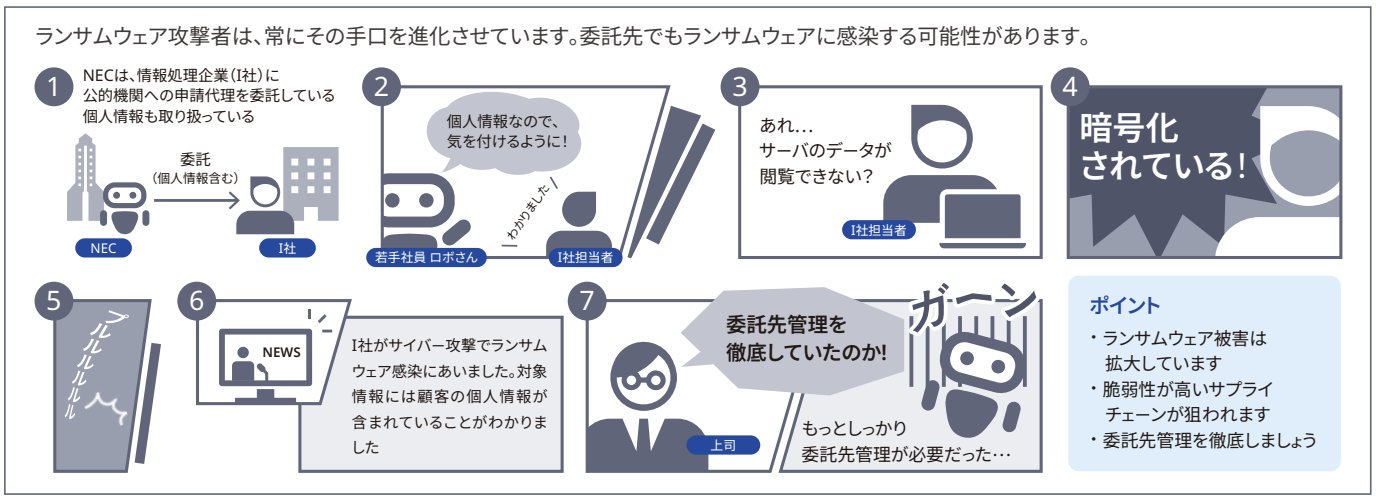
❸ 情報セキュリティアウェアネスの向上施策

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、セキュリティアウェアネス向上施策を実施しています。例えば、マイクロテーマ・トークと呼ばれるセキュリティ動画を活用した職場での懇談会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。セキュリティ動画は、セキュリティ脅威のトレンドや社内外で起きたインシデント、ヒヤリハット事例を反映し、毎年作成しています。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。

情報セキュリティ教育資料サンプル



*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、お客様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。累計84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

各事業部門が、組織としてSBDを実践する専門人材の育成を2019年度より行っています。セキュリティ責任者を補佐する人材を育成する「補佐育成コース」と、セキュリティ提案を実務リードする営業職を育成する「営業職向けコース」を用意し、適切なセキュリティ提案・実装に必要なスキル習得を進めています。2024年度は20名以上が受講し、累計107名が受講しています。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様にお届けします。

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、お客様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2024年度は延べ1,700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*3「NECセキュリティスキルチャレンジ」を開催しています。2024年度は1,000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9,000名以上となりました。

❺ セキュリティ提案・実装者向け基礎教育

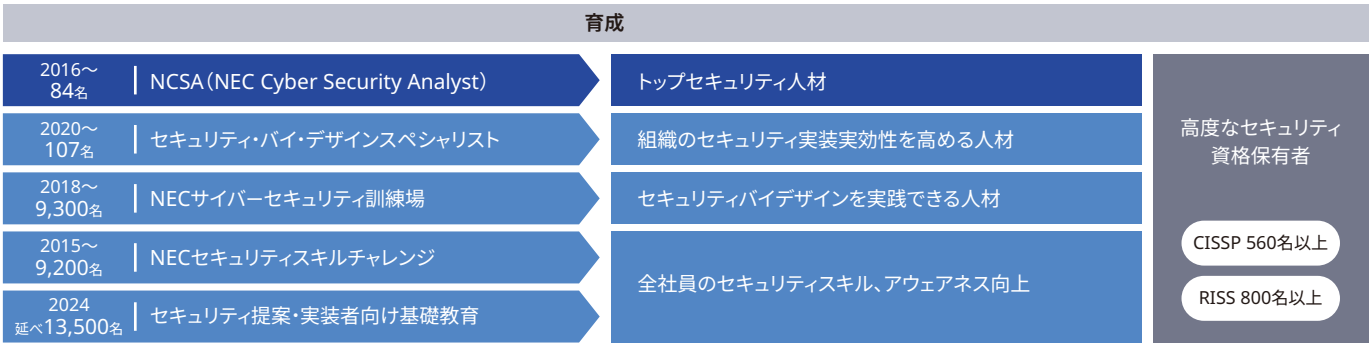
お客様向けの提案・実装プロセスに関わる全社員を対象に、2023年10月に施行されたサイバーセキュリティ管理規程に基づき、自身の役割に応じて実施すべき内容の理解度をサーベイにて測定しました。サーベイ実施後、個々のサーベイ結果（理解度）に応じた教育を展開し、2024年度の学習者は延べ13,500名となりました。

❻ 高度なセキュリティ技術資格保有者

お客様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、お客様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。2024年度から、セキュリティ人材の高度化や裾野の拡大として、国際資格であるCCSP、CISA、CEH、CCT*4を新たに追加しました。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560名となりました。また2024年度には、リスク管理やITガバナンスに精通し、より広い範囲での情報セキュリティマネジメントを実践できる人材の育成強化のため、認定機関であるISACAと戦略的提携を締結しました。この提携により、リスク管理やITガバナンスに精通し、より広い範囲での情報セキュリティマネジメントを実践できる人材の育成強化を目指します。この提携により、NECグループ社員向けにCISAとCISM*5の認定トレーニングを実施し、専門人材を育成します。またNECグループのセキュリティスペシャリストから公式トレーナーを輩出し、現場で培ったシステム実装における豊富な知見に裏付けされた実践力を加えたトレーニングを、お客様へも提供していく予定です。

サイバーセキュリティタレントマネジメント全体像

SBDの実践、適切なセキュリティ実装により、事業価値を創出・向上できる人材の育成、マネジメント



*3 CTF: Capture the Flag
*4 CCSP（Certified Cloud Security Professional）：クラウドセキュリティプロフェッショナル認定、CISA（Certified Information Systems Auditor）：公認情報システム監査人
CEH（Certified Ethical Hacker）：認定ホワイトハッカー、CCT（Certified Cybersecurity Technician）：認定サイバーセキュリティ技術者
*5 CISM（Certified Information Security Manager）：公認情報セキュリティマネージャー

7 | 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・複雑化する中、先進的な対策をグローバルで実施するとともに、経営者のリーダーシップに基づく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基、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の承認の下対策を実施します。

NECグループでは、包括的なサイバー防衛の考え方（CDC*3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。

これらの取り組みが社外からも認められ、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セキュリティ大賞2024において「大賞（セキュリティ対策・運用部門）」を受賞、その他複数の賞もいただいております。

受賞の様子

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*4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、

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 CDC: Cyber Defence Centre
*4 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

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。表出したリスクの対応状況はダッシュボードでガラス張りにし、対処が滞った場合はトップへの自動エスカレーションを行うことで、自律的なアクションを促進するマネジメントサイクルを確立しています。

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[*5]チーム)が、体系化したDigital Opsの基、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[*6]、CSIRTで独自に開発したNDR[*7]、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リサーチファクトリやおとり環境(Deception)を構築し、詳細な脅威分析を行っています。独自に生成されたCTIを事前防御と脅威ハンティングに活用することで、能動的なサイバー防御(Active Cyber Defense)を実現します。

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の承認の下復旧まで対応しています。

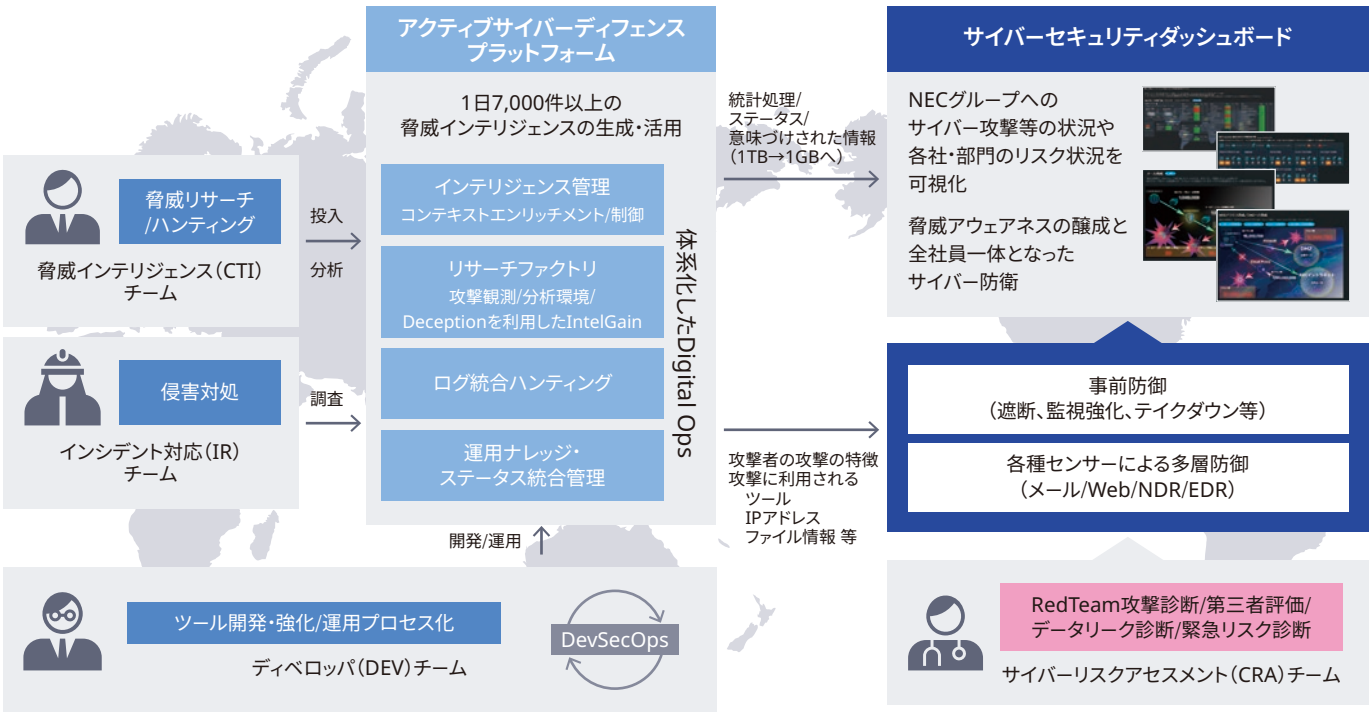
また、大阪・関西万博のような大規模イベントでは、関連する企業がサイバー攻撃の標的となるリスクが高まることが予想されます。NECでは、NISCとのサイバー攻撃対応演習、特別エスカレーションルールの取り決め、期間中のセキュリティ体制構築、CSIRT/SOCによる重点監視と脅威インテリジェンス強化により、サイバー攻撃への対策を講じています。

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を重大な経営リスクと捉え、組織として攻撃に対する耐性を高めるため、社員に対して攻撃メール訓練を行うとともに、セキュリティインシデント対応マニュアルを整備しています。インシデントが発生した場合、迅速に対応できるよう、マニュアルにはThree Lines Modelを踏まえた責任・役割分担、渉外対応、法務対応等の実施事項を明記しています

また、経済産業省が策定したサイバーセキュリティ経営ガイドラインVer3.0を踏まえて経営層が主体的に関与できるよう、経営層や関係部門、専門家を交えたインシデント対応訓練を年に1回以上実施しています。

サイバーセキュリティ対策の全体像



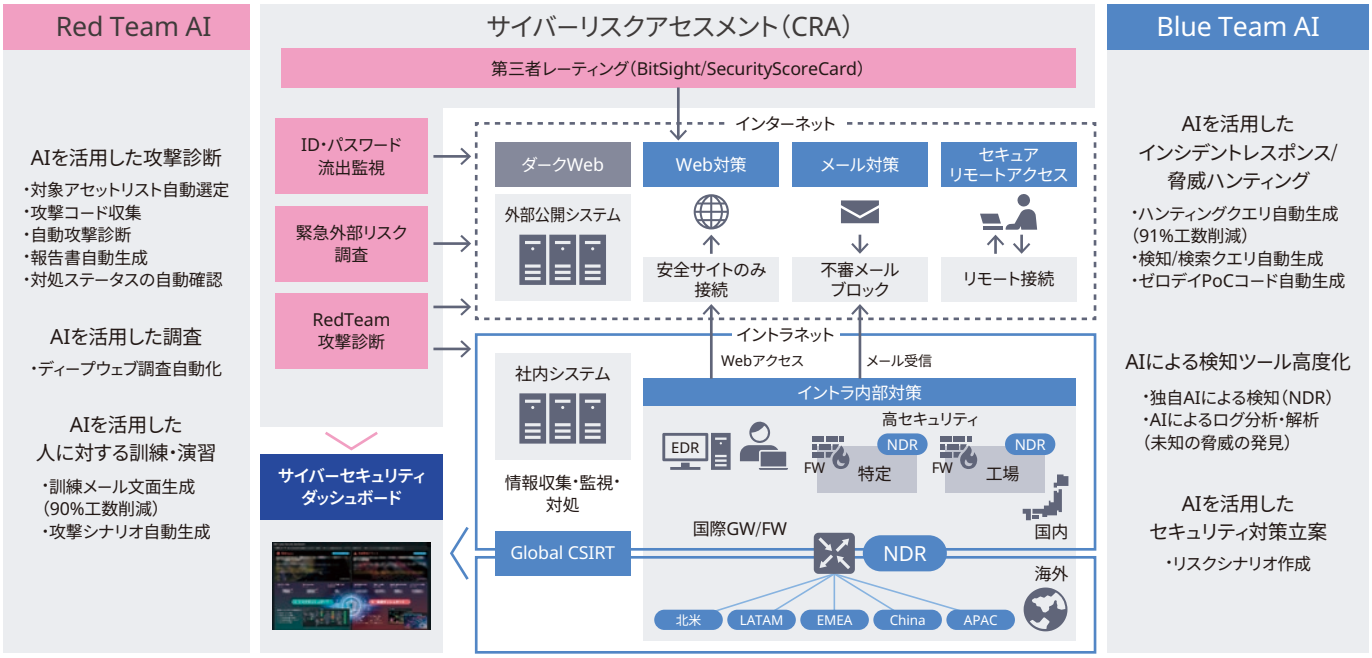
*5 CTI: Cyber Threat Intelligence　*6 EDR: Endpoint Detection and Response　*7 NDR: Network Detection and Response

❺ AIを活用した高度なサイバーセキュリティ対策

AIによる攻撃の活発化を受け、防御側もRed Team AI/Blue Team AIによる次世代のサイバー攻撃対策を実現しています。

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のアノマリ検知、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を含めた多様なAIを活用しています。社内の研究所と共同で攻撃診断 Agentic AIを開発しており、自動化・効率化・高度化を進めています。

サイバー防衛における生成AI活用



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ーカルチャー変革

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、セキュリティ施策のパフォーマンス等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、改善のためのアクション促進と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。

ダッシュボードは現在もアジャイルに開発を続けており、言語・音声・

サイバーセキュリティダッシュボード

∗8 レーティングが600点以下の組織は、750点以上の組織と比較して6.4倍の確率でランサムウェアの被害を受ける
https://www.bitsight.com/blog/ransomware-prevention
∗9 NECサーベイより算出

画像・音楽の生成AIを用いて国内外のセキュリティニュース、およびそれらにインスパイアされた楽曲を動的かつ自動で配信する機能を追加しました。セキュリティニュースを一般社員にも親しみやすい形にすることで全員参加のセキュリティを実現しています。

今後デジタル社会における説明責任がより重要になっていく中で、NECは安全・安心で持続的な社会の実現に向けValue Creatorとしての役割を一層強化して参ります。

セキュリティクライアントゼロ推進

NECが掲げる「クライアントゼロ」とサイバーセキュリティ領域における取り組み

サイバーセキュリティ領域における「クライアントゼロ」の取り組み

NECは、自社をゼロ番目のクライアント（顧客）＝「クライアントゼロ」と位置づけ、社内実践で得た「活きた」経験をリファレンスとし、お客様や社会に知見、ノウハウをご提供しております。

サイバーセキュリティ領域では、2014年より継続的に本書を発行し、NECグループにおけるセキュリティの取り組みをご紹介してまいりました。

「クライアントゼロ」の取り組みとしては、企画フェーズからBluStellar Scenario*1と連動し、NEC社内をリファレンスとした課題整理・ポリシー設計、NEC社内運用ノウハウを持つメンバによるソリューション導入・運用、研究所と連携した先端技術など、様々な知見、ノウハウを幅広くお客様にご活用いただいています。

今後も、安全・安心なお客様の事業推進や社会活動に貢献できるよう、「クライアントゼロ」として新たなセキュリティリスクへの対応や最先端技術の実践し、知見、ノウハウを拡充していきます。

セキュリティクライアントゼロ事例

セキュリティクライアントゼロの取り組みでは、以下のようなNECグループの実践的なセキュリティ経営のナレッジを、お客様、社会へ継続的にご提供します。

❶ サイバーセキュリティダッシュボード

NECのデータドリブン経営をリードするこの取り組みは、昨今のグローバル、サイバー・フィジカル横断でのセキュリティリスクの増大を背景に、多くのお客様からご紹介のお引き合いをいただき、サイロ化したセキュリティ施策の可視化、統合と、持続可能なセキュリティリスクへの対応事例としてご活用いただいています。（p.16「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ーカルチャー変革」、p.24「NECがご支援できること」参照）

❷ AIとセキュリティ

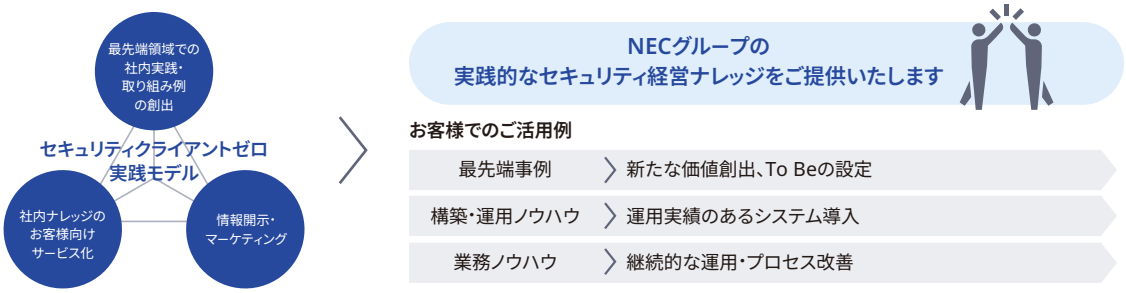
NECグループでは、AIの安全な利活用を目指す「Security for AI」と、セキュリティ対策にAIを活用する「AI for Security」の両者を推進しています。社内セキュリティ施策においては、「AI for Security」を実践し、セキュリティ対策の効率化・自動化、品質の向上に取り組むと共に、セキュリティクライアントゼロ事例としてのノウハウを蓄積しています。

これら最先端事例については、お客様への事例紹介の他、外部アナリストとの意見交換やニーズ調査等を実施、サイバーセキュリティ事業へフィードバックすることで、いち早くお客様や社会へ還元する体制を構築しています。この推進体制のもと、NECセキュリティの高度なセキュリティ知見や研究所の開発技術を融合、お客様へのご提供を進めており、新たな価値創造やTo Be（あるべき姿）としてご検討いただいています。（p.27-29「『.JP（日本のサイバー空間）』を守るための技術・研究・事業開発」参照）

❸ 実践的なセキュリティ運用事例

NECグループでは12万人の従業員が活動しており、その基盤となる社内の安全・安心の確保はNECの経営課題に直結します。このため、サイバー攻撃対策はもちろんのこと、グローバルセキュリティガバナンス・監査体制や、重要情報管理・保護、ゼロトラストセキュリティ基盤などの安定した運用、継続的な改善をおこなっており、これらの事例をより実践的なノウハウとしてご活用いただいています。

セキュリティクライアントゼロの取り組み



*1 お客様を未来へ導く価値創造モデルであるNECのブランド「BluStellar（ブルーステラ）」が提供するDX実現構想および成功シナリオ。セキュリティは「事業成長を支え続けるセキュリティ経営改革」のテーマで提供

8 ｜ 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。

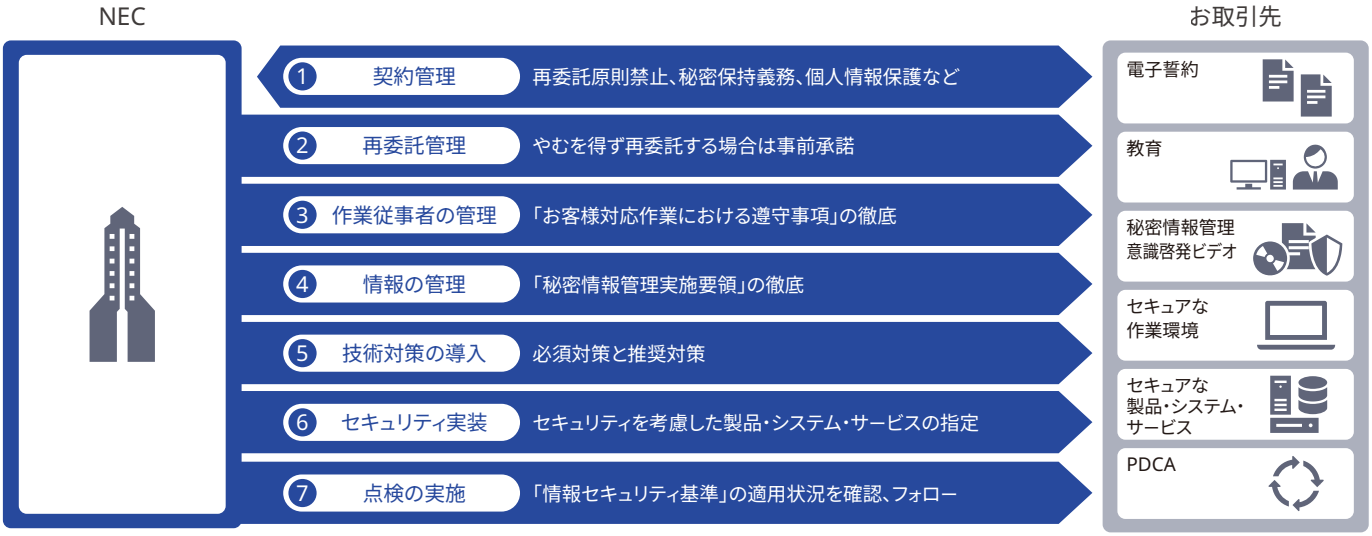
❻ セキュリティ実装

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に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。その中で情報セキュリティや個人情報保護についての最新動向や対応に関する注意事項などを共有するとともに、サイバーセキュリティに関する教育も実施し、情報セキュリティ事故が起こらないよう啓発活動を行っています。また、海外のお取引先向けの説明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情報セキュリティ基準ガイド、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

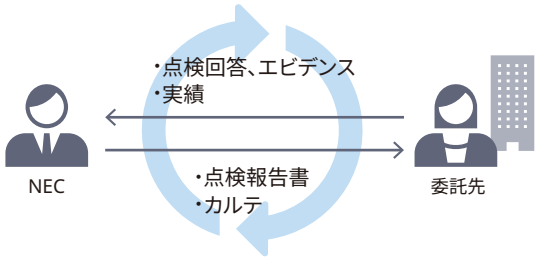
NECと取引のある会社、約1,800社を対象に書類点検を実施しています。お取引先は自社の対策状況を自ら点検し、点検結果はWebシステムによってリアルタイムでフィードバックを行っています。また、取引が多いお取引先には直接訪問、あるいはリモートを活用した訪問点検を実施しています。毎年訪問社数を増やしており（2024年度は約350社）NECの点検担当者（約100名）によって推進しています。

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年度から2024年度にかけて中国、インド、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。

9 | 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。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行っております。

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ます。2024年度は海外グループ会社への「サイバーセキュリティ管理規程」適用のモデルケースとして、一部の海外グループ会社において、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行いました。

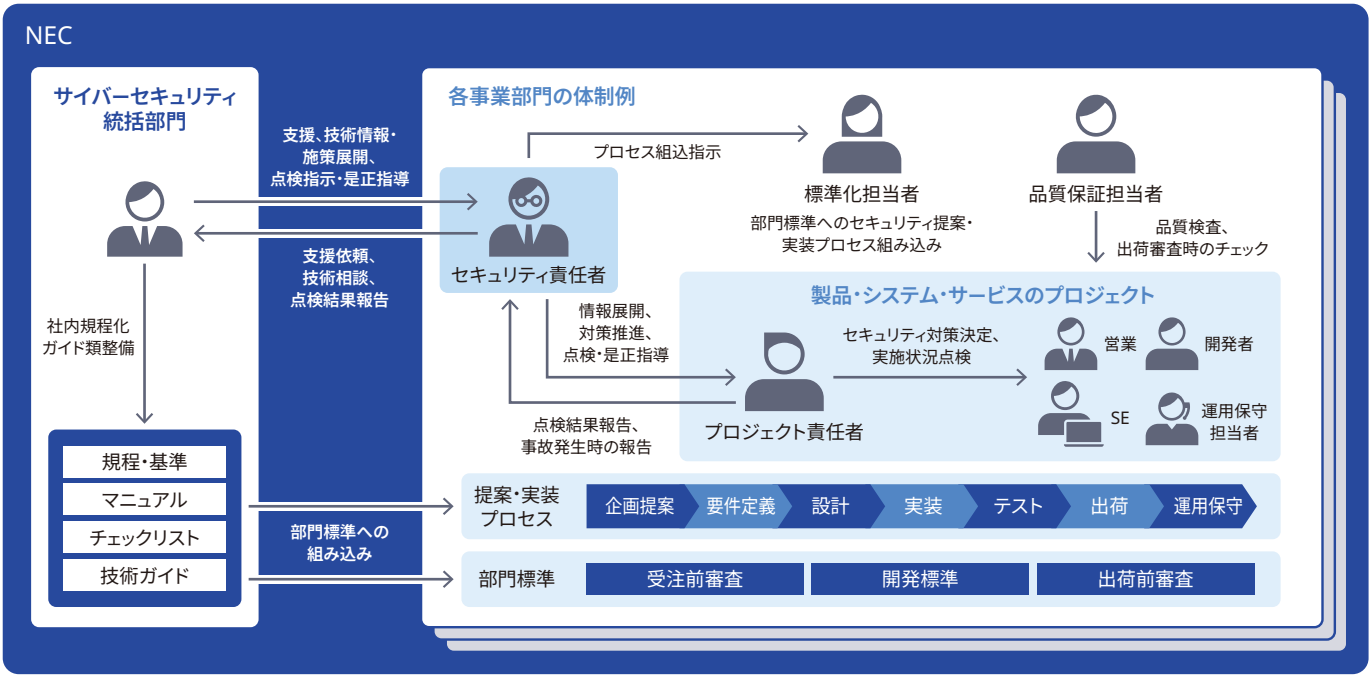
❷ セキュリティ実装の主要な取り組み

NECでは、セキュリティを確保する「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、セキュリティ実装の実施状況を一元管理

セキュリティ実装プロセス



し可視化するために開発された「サイバーセキュリティチェックリスト管理システム」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。

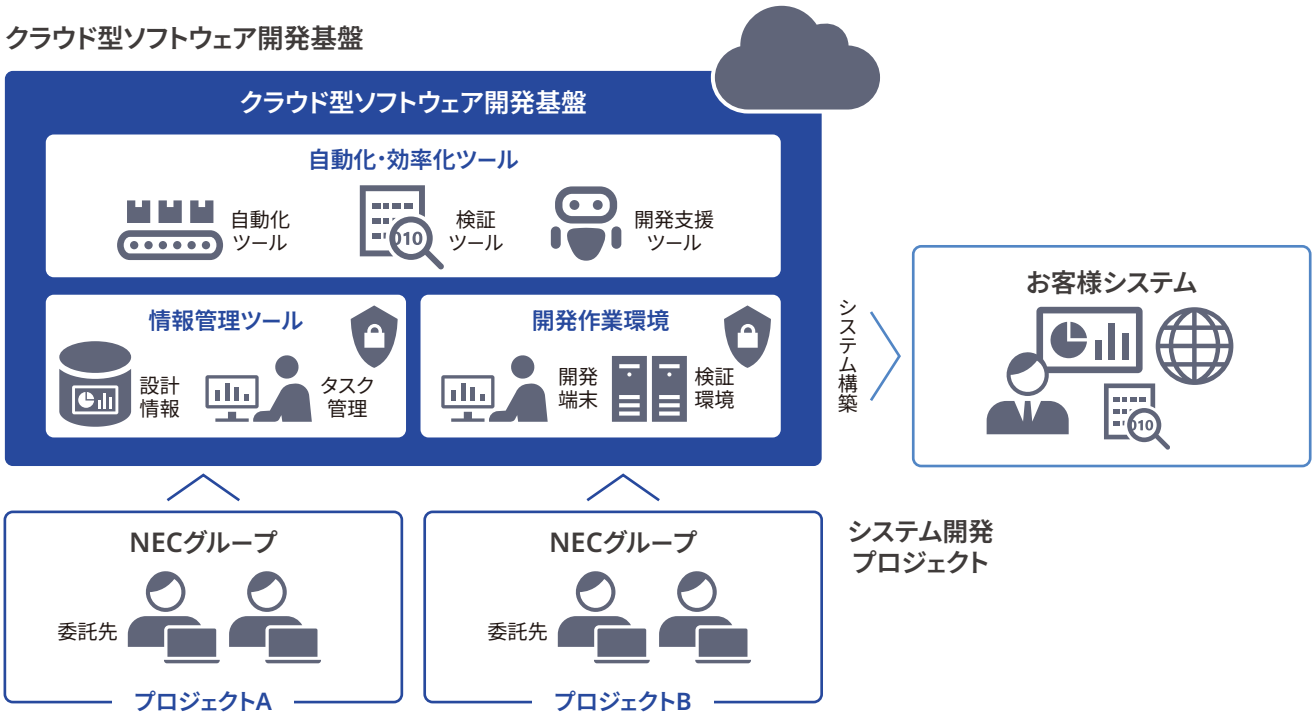
❸ セキュリティ実装のためのソフトウェア開発基盤

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本基盤に集約し、開発環境からの情報漏洩や生成AI利用時の著作権問題など開発環境起因のリスクへの対策の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 ハードウェア開発・生産拠点のセキュリティ強化

NECのハードウェア開発拠点および生産(工場)拠点では、技術情報の管理やセキュリティ対策が適切であるか正しく把握するため、第三者によるリスクアセスメントを定期的に受診しています。また国内の生産拠点では、毎年、サイバー攻撃対応に対応したBCP訓練を実施し、万が一のセキュリティインシデントに備えたリスク軽減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

10 | NECのサイバーセキュリティ戦略

激化するサイバー攻撃やサイバーセキュリティ強化に向けた制度の変化に対応し、NECはインテリジェンスとAIを活用して「.JP（日本のサイバー空間）」を守るために貢献しています。

1 日本のサイバー空間を取り巻く状況

昨今フィジカル（現実）空間での刑法犯認知数は減少を続け2021年には戦後最少を記録[*1]する一方、サイバー空間における攻撃や犯罪は、量・質ともに著しい勢いで深刻化しています。特にサイバー攻撃によって、企業が金銭を要求・窃取される事例や、事業停止に追い込まれる事例が発生しており、サイバー攻撃は企業の事業継続を中断しうるリスクとなりつつあります。独立行政法人情報処理推進機構発行の「情報セキュリティ10大脅威2025[組織編]」[*2]でも、「ランサム攻撃による被害」や「サプライチェーンや委託先を狙った攻撃」が挙げられており、日本のサイバー空間の安全性が脅かされています。

急激な業務のDXやクラウドの利用拡大により、企業が守るべきシステムやデータが社内外に分散し続けてシステムが複雑になることで、企業全体としてのセキュリティリスクが潜在化しインシデントの発生や被害の拡大につながりやすくなります。またサイバー空間における攻撃や犯罪はフィジカル空間での犯罪や攻撃と異なり目に見えにくく、「今、何が起きているか」「どこまで対策できているのか」を把握することが難しいという特徴があります。

このようにサイバー空間の安全性が脅かされ事業継続に影響が及びつつある状況に対抗し、DXを安全・安心かつ持続的に進めるためには、サイバーセキュリティのリスクを経営観点で可視化する必要があります。NECは実データを起点（データドリブン）としてリスクを分析・可視化する「データドリブンサイバーセキュリティ（DDCS）サービス」を提供し、お客様のセキュリティリスクマネジメントに活用いただいてきました。

しかし、サイバー空間を取り巻く状況は悪化の一途をたどっています。「情報セキュリティ10大脅威2025[組織編]」では「地政学的リスクに起因するサイバー攻撃」が初めて選出され、政治的に対立する周辺国に対して社会的な混乱を引き起こすことを目的としたサイバー攻撃を行う国家の存在や、そのような国家からの攻撃に備えて組織として常にサイバー攻撃への対策を強化していく必要性が明記されました。

このような社会情勢の変化を踏まえ、政府はサイバー安全保障分野において官民の対応能力を強化する動きを加速させています。2022年5月に成立した「経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律」（経済安全保障推進法）では、電気・ガス・水道などの基幹的なインフラサービスの安定的な提供が日本国外からのサイバー攻撃などにより妨害されないよう、サービス提供において使用される重要な設備について事前審査が実施されることになりました。また2024年5月に成立した「重要経済安保情報の保護及び活用に関する法律」（重要経済

「.JP（日本のサイバー空間）」を守る

*1 警察庁、令和6年警察白書、p.48、第2部第2章第1節1刑法犯（1）刑法犯の認知・検挙状況、https://www.npa.go.jp/hakusyo/r06/pdf/pdfindex.html
*2 独立行政法人情報処理推進機構、情報セキュリティ10大脅威 2025 組織編、https://www.ipa.go.jp/security/10threats/eid2eo0000005231-att/kaisetsu_2025_soshiki.pdf

安保情報保護活用法）では、サイバー脅威・対策等に関する情報（インテリジェンス）など安全保障上特に秘匿性が高い情報の取り扱いにあたって適正審査を実施する「セキュリティ・クリアランス制度」が創設され、2025年5月に施行されました。

さらに2024年6月から約半年にわたって開催された「サイバー安全保障分野での対応能力の向上に向けた有識者会議」での提言を受け、2025年1月から開催された第217回通常国会で可決成立した「重要電子計算機に対する不正な行為による被害の防止に関する法律」（サイバー対処能力強化法）および「重要電子計算機に対する不正な行為による被害の防止に関する法律の施行に伴う関係法律の整備等に関する法律」（サイバー対処能力強化法整備法）では、能動的なサイバー防御の実施体制を整備するため「官民連携の強化」「通信情報の利用」「アクセス・無害化措置」の実現と、内閣サイバーセキュリティセンター（NISC）を発展的に改組して能動的サイバー防御（ACD*3）を含む各種取組の司令塔たる内閣官房新組織の設置などの体制整備を目指しています。「アクセス・無害化措置」ではサイバー攻撃による重大な危害を防止するため、警察および自衛隊による措置が可能となります。また司令塔組織の前身となるNISCについても、新たに警察庁や防衛省からの出向者が幹部に就任するなどの体制強化が実施されました。

このような政府のサイバーセキュリティ体制強化の動向に対応し、政府や企業を含めた「.JP（日本のサイバー空間）」を守るため、NECも新たなサービスと技術の開発を進めています。今後新たな手法で激化していくサイバー攻撃に対応するためには、大量のインテリジェンスをいち早く収集・分析して対抗策を講じる必要があります。またこのようなインテリジェンスは秘匿性が高い情報であり、今後サイバーセキュリティ領域での「官民連携」が進めば政府機関との共有も想定され、相応の取り扱いが求められます。

NECはこれまで海底ケーブルや宇宙・防衛事業、ミッションクリティカルシステムなど日本の重要インフラを支え、日本の安全・安心を長年支えてきた実績を基盤に、日本の技術で「.JP（日本のサイバー空間）」を守ることを目指します。独自のインテリジェンスと生成AI「cotomi」を活用し、AIとサイバーセキュリティ技術を組み合わせてグローバルにサイバーセキュリティ事業を展開し、海外に進出した日本企業を含めた「.JP（日本のサイバー空間）」を守るため、安心・安全な情報社会の実現に貢献してまいります。

セキュリティ関連組織との連携

「.JP（日本のサイバー空間）」を守るためには、技術やインテリジェンスだけでなく、これらを活用し対策を講じていくための制度や法令も不可欠です。NECはサイバーセキュリティ対策のサービスを提供するだけでなく、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を通じて内閣官房・省庁へ政策提言を実施しています。

特別顧問である遠藤信博は、「サイバー安全保障分野での対応能力の向上に向けた有識者会議」の構成員として、サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させるための新たな取組の実現に必要となる法制度の整備等について提言を取りまとめました。

また、2024年5月から執行役 Corporate EVP 兼 CSO 兼 サイバーセキュリティ部門長 兼 NECセキュリティ株式会社 代表取締役社長を務める中谷昇は、警察庁情報技術犯罪対策課課長補佐やインターポール（国際刑事警察機構）事務総局のIT局長兼CISO、民間企業で最高情報セキュリティ責任者を務めるなど、サイバーセキュリティについて官民双方で豊富な業務経験を有しており、一般財団法人日本サイバー犯罪対策センター（JC3*1）の代表理事を務めています。

*1 Japan Cybercrime Control Center

*3 Active Cyber Defense

11 | NECがご支援できること

DXを安全・安心かつ持続的に進め、サイバーセキュリティのリスクに経営観点で対応するために、NECグループが提供する支援体制をご紹介します。

多くの企業がセキュリティ対策に取り組んでいる一方、セキュリティインシデントの発生や被害は増加し続けています。ランサムウェア被害の報告数も2020年下期から約5倍になるなど、企業規模を問わず被害が拡大し事業継続が脅かされています。

この背景には、急激な業務のDX、クラウドの利用拡大により、企業が守るべきシステムやデータが社内外に分散し続けていることが挙げられます。守るべき対象が分散しているために対策の導入が部分最適になりやすく、加えて、システムが複雑になることで導入時に運用までのプロセスを考慮することが難しくなります。こうした導入～運用プロセスの分断と、対策の部分最適が繰り返されることで、企業全体としてのセキュリティリスクが潜在化し、インシデントの発生や被害の拡大につながりやすい状態となるのです。

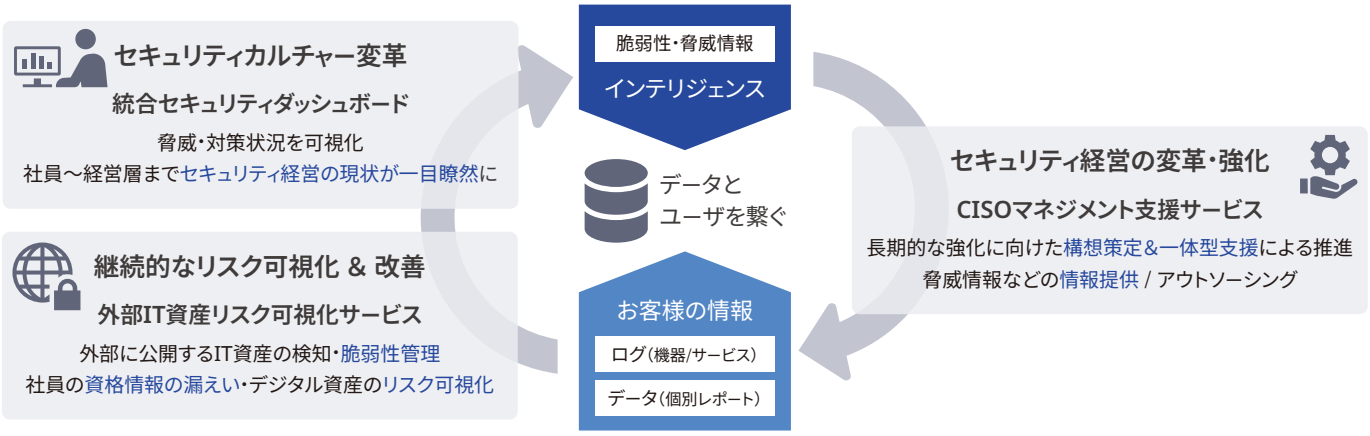
また昨今、経済安全保障の観点から、企業のセキュリティ対策における安全確保義務や、経営責任の明確化といった動きがあります。セキュリティリスクが潜在化した状態では企業全体として適切なセキュリティ対策が取られているとは言いがたく、経営・投資判断・ガバナンス上の課題に直結することとなります。

セキュリティリスクの潜在化を解消してサイバーセキュリティのリスクを経営観点で可視化するには、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。

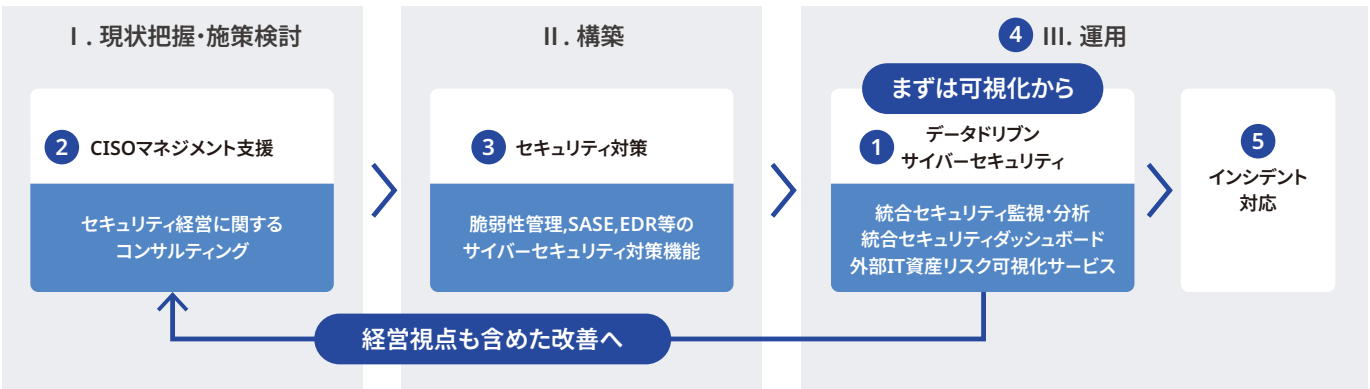
NECでは、これまで社内で蓄積してきたサイバーセキュリティダッシュボードの構築や運用で得たナレッジを基に「データドリブンサイバーセキュリティサービス（DDCS）」をお客様に提供し、お客様のセキュリティ業務DXの実現を支援しています。

データドリブンサイバーセキュリティサービス全体像

データドリブンサイバーセキュリティサービス（DataDriven Cyber Security service）
俯瞰的・効率的なセキュリティ経営を実現するため、データを起点（データドリブン）とするセキュリティ経営変革を実現するための手段を用意。



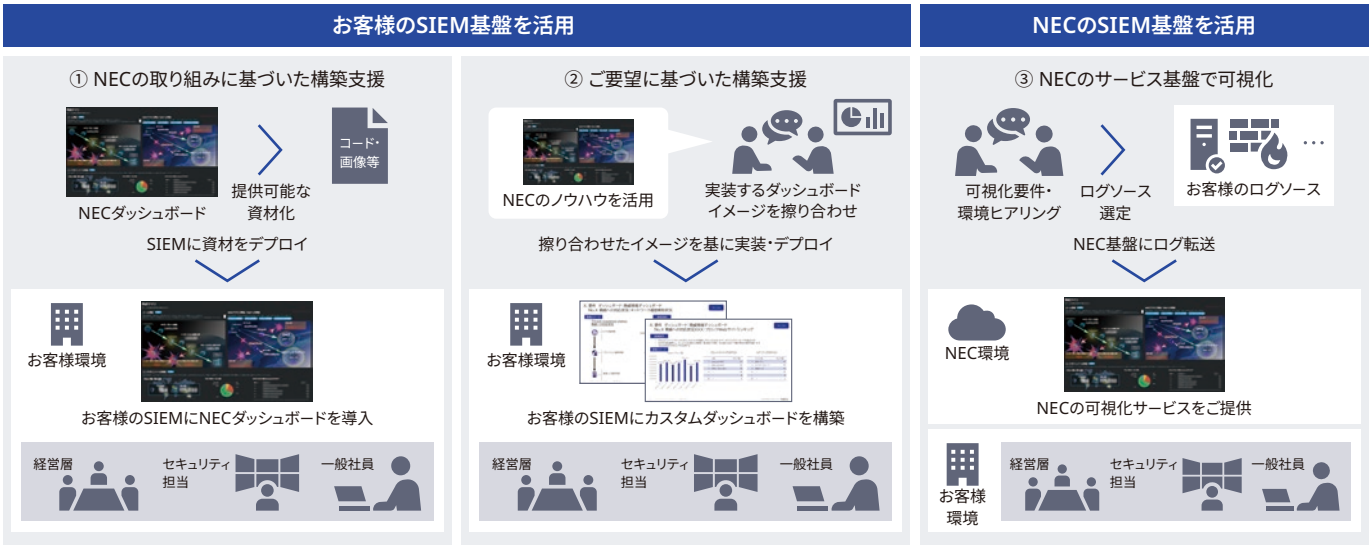
データドリブンサイバーセキュリティサービスの位置づけと流れ



1 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、お客様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。

サイバーセキュリティダッシュボード ご提供メニュー



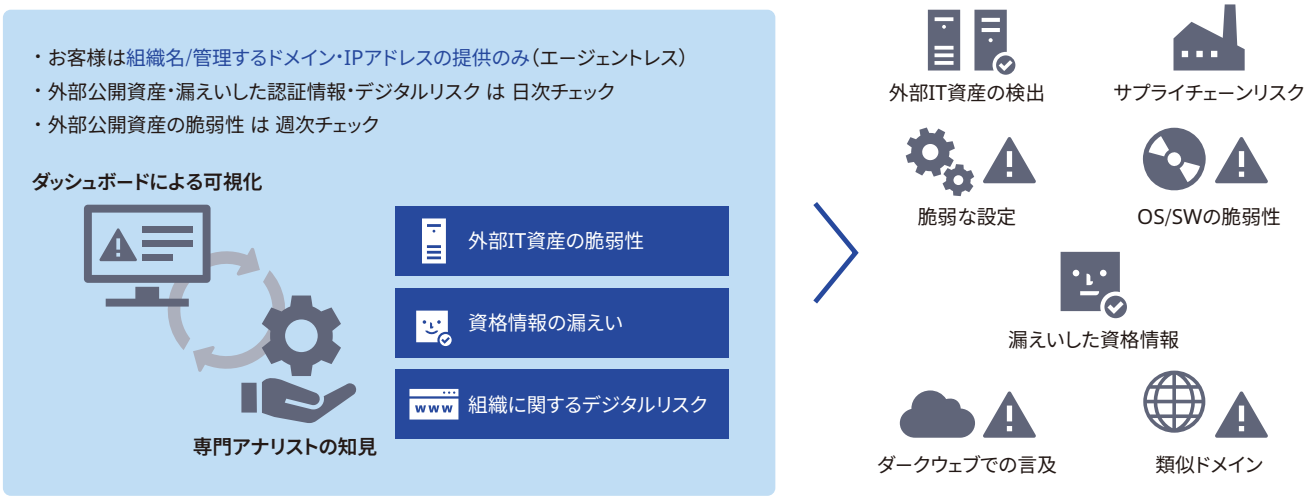
2 外部IT資産リスク可視化サービス

外部に公開されている企業のIT資産（VPN機器やクラウドサービスなど）を調査し、設定不備や脆弱性情報などのリスク情報をダッシュボード経由でリアルタイムに可視化します。発見されたリスクは、NECグループのセキュリティ専門家がリスクや影響の大きさを精査、及び推奨対処の提言まで行うため、セキュリティ人材が不足している組織でも実効性があるリスク対処の仕組みを迅速に実現できます。

また、調査範囲を取引先まで広げた「サプライチェーンリスク管理」、外部漏えいした認証情報を調査する「クレデンシャルリーク調査」、ドメインの不正利用や偽サイトを発見しテイクダウンを行う「ブランド棄損抑止」といった機能も備えており、サイバー空間におけるプロアクティブな防御を包括的に支援します。

外部IT資産リスク可視化サービス

企業を取り巻く脅威・リスクに対して確かな情報源と専門アナリストの高度な知見を活かし
サイバー空間におけるプロアクティブな防御を包括的に支援。



3 CISOマネジメント支援サービス

NECグループのセキュリティ専門家が、CISOの補佐役として、NECのグローバル含めたセキュリティ経営の実践で培った知見を活かし、セキュリティリスクマネジメントにおける短期および中長期サイクルでの全体最適化を伴走型で支援します。

具体的には、お客様保有資産に対する脅威情報やお客様の業界内でのインシデント動向について、NECが持つサイバー脅威分析の知見や技術を活用し、経営判断に資する高精度なサイバー脅威インテリジェンスを提供します。さらに、脅威に対するセキュリティ対応状況の分析、組織の成熟度評価を行い、お客様が目指すセキュリティレベルの達成に向けた戦略策定・計画立案を支援し、構築・運用フェーズにおいてもPMOとしてプロジェクトを推進します。

CISOマネジメント支援サービス

経営層/セキュリティ責任者の視点でセキュリティ経営の高度化に貢献するため、
お客様が抱える一般的な課題に対して長期的な支援メニューをご用意。

構想策定 & 一体型支援	**構想策定** 経営層/実働メンバの抱える課題を見極めて あるべき姿の構想策定を実施 長期的な強化・目標達成に向けて 実効性のあるロードマップの策定を支援	**一体型支援** お客様のセキュリティ担当チームの一員となり 構想策定で定めた優先度の高い課題に対して、解決へ向けた施策を検討 お客様の組織体系・文化への理解を深めつつ、 実情を考慮した 内側から施策推進 / スキルトランスファーによる支援を実施
セキュリティ・トレンド 継続的な情報提供	**セキュリティ関連情報の提供** ・直近のインシデント事例 ・インシデント事例に基づく傾向と対策 ・サイバー攻撃による被害事例の一覧 ・脅威アクター / 攻撃キャンペーンの動向　など	**セキュリティ・トレンドの把握** セキュリティ戦略に携わる経営層（CISO/CIO）が 国内外のトレンド・インシデントを俯瞰的に把握 自社のセキュリティ経営状況・潜在的なリスクを思案し 全社的なセキュリティ強化を通じた被害抑制を目指す
マネージドサービス（アウトソーシング）	**定常業務のマネージング** ・監視 / 障害対応（SoC/MDR） ・運用業務の代行 ・インシデントレスポンス支援 ・脆弱性情報の提供	**本業に集中できる環境へ** セキュリティ経営・運用に対する人的リソースが不足する一方 長期的なセキュリティ強化を目指すお客様に対して 自社で対応する業務を切り分けた上で アウトソーシングを活用⇒本業により集中できる環境を支援

ご支援の一例（サンプル）

NECグループでは、専門的なテクニカルスキルだけでなくビジネス観点でのリスク評価ができる専門人材の育成に注力し、国際資格CISSPの取得を進めており、450名の資格保有者（2024年6月時点）が在籍しています。

また、2024年4月より、NECセキュリティに専門人材を結集し、サイバーセキュリティ事業拡大に向けた体制強化を行い、今後も最先端のサイバーセキュリティ技術を活用したソリューション開発・提供力を一層強化し、政府機関、重要インフラ、企業などのサイバー攻撃対策を支援するサイバーセキュリティ事業の拡大を加速します。

NECはDXに関して、ビジネスモデル、テクノロジー、組織・人材の3軸で、戦略構想コンサルティングから実装に導くオファリングなど、End to Endのサービスを提供しています。さらに、従来型のSIerから「Value Driver」への進化を目指し、その価値提供モデルを「BluStellar（ブルーステラ）」として体系整理しました。業種横断の先進的な知見と研ぎ澄まされた最先端テクノロジーによりビジネスモデルを変革し、社会課題とお客様の経営課題を解決に導きます。

12 ｜「JP（日本のサイバー空間）」を守るための技術・研究・事業開発

NECは、AI技術を活用して「正しくつくる」「正常をつづける」「攻撃からまもる」を効率化・高度化し、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グループで研究・開発している、SBDを支援するAI技術・Agent群から「正常をつづける」、「攻撃からまもる」を支援する「システムリスク診断Agent」を紹介します。また、「正しくつくる」を支援する「ガイドラインチェックAgent」、および組織のセキュリティガバナンス向上を通じて「正常をつづける」を支援する「情報セキュリティ内部監査Agent」を紹介します。

2 システムリスク診断Agent

ICTシステムの複雑化に伴い、多くの脆弱性や、新しい攻撃手法が報告されています。これらに備えるためには、積極的に新たな脅威・脆弱性や攻撃者の動向などのインテリジェンス情報を収集するだけでなく、システムへの影響を分析し、事前に問題点の解消や対策をおこなう必要があります。しかし、実施には時間や手間がかかる上、膨大なインテリジェンス情報の活用ノウハウが必要です。NECは、これまでに培ったサイバー攻撃リスク自動診断技術*1を応用したAIの研究開発に取り組んでいます。

開発中のシステムリスク診断Agentは、人の代わりにインテリジェンス情報を分析し、汎用の攻撃ナレッジに変換することで、日々報告される新しい脅威・脆弱性がシステムに与える影響の分析や、対策の立案を可能にするものです。

NECは、このようなAIを使ってシステムリスクの分析・診断業務を効率化、および高度化することで、SBDにおけるシステムの「正常をつづける」、「攻撃からまもる」活動を支援します。

AI × セキュリティ 技術開発コンセプト

システムリスク診断Agent

背景・課題

- 企業存続を脅かす新たな攻撃/脅威や脆弱性が増加。被害が拡大
- 適切な対策には自社の弱点を把握するセキュリティリスク診断の実施が必要
- 診断は非専門家には難しく、定期的に脅威・脆弱性を把握し診断することは困難

提供価値

- 脅威・脆弱性のチェックからシステムリスク診断と対策立案の実行、図・イメージを含むレポート生成まで自律的に実行
- 専門家が処理した場合と同等の品質を確保

Why NEC

NEC独自のサイバー攻撃リスク自動診断技術とAgentを組み合わせて、攻撃診断や対策立案に、NEC独自のナレッジデータベースを活用定期的な診断で状況に即した対策案を提示可能

*1 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

*2 CSIRT: シーサート（Computer Security Incident Response Team）

3 ガイドラインチェックAgent

システムの企画・設計段階からセキュリティを組み込むSBDを実践することで、セキュアなシステムを構築することができます。しかし、セキュア開発に関するガイドラインは多岐にわたる上、ガイドラインの汎用的な記述と実システムの企画、設計における具体的な記述とを突合してガイドラインへの適合を解釈する作業に膨大な時間や知識、ノウハウが要求されます。そのため、人手で実施する際にはどうしても確認漏れや判断ミスが発生してしまいます。NECは、長年のセキュア開発の経験や、独自に作成したセキュア開発ガイドラインの知見を基に、ガイドラインチェックを支援するAIの研究開発に取り組んでいます。このAIは、例えばガイドラインの汎用的な記述と、実システムの具体的な記述のギャップを埋めるコンテキスト(解釈方法など)を生成することで、ガイドラインのチェック項目に該当する設計文書の記載箇所の抽出や、チェック項目の適合性判定といった作業を、人に代わって実施します。

このようなAI技術でSBDにおけるガイドラインチェック業務を効率化、および抜け漏れを排すことで、システムを「正しくつくる」活動を支援します。

4 情報セキュリティ内部監査Agent

SBDの実践においては、システム観点だけでなく、組織のセキュリティガバナンスも重要です。SBDの実践度合や組織の対応状況を把握することで、セキュリティを向上することができます。NECは、NECグループ各社に対する情報セキュリティ内部監査を実施し、日々セキュリティの向上に努めています。しかし、監査の実施や報告書作成に多くの時間を要しており、また監査人によって監査の品質がばらつくことや、業種固有のガイドラインへの対応に難しさがあります。NECは、長年の監査ノウハウやセキュリティコンサルティング業務の知見を基に、情報セキュリティ監査を支援するAIの研究開発に取り組んでいます。AIと監査人とが協力することで、監査にかかる時間の短縮や、報告書の品質向上、ならびに均一化を実現します。さらに、NECがもつ業種固有の知見を使って、業種に即した提言案を作成することも可能です。

情報セキュリティ内部監査を効率化し、監査品質を向上するAIにより、組織のセキュリティガバナンス向上を通じて、お客様のシステムの「正常をつづける」活動を支援します。

ガイドラインチェックAgent

背景・課題

- システムの企画・設計段階から実装、運用までセキュリティを組み込むSBDの考え方が必要とされている
- セキュア開発のガイドラインが多岐にわたる上、ガイドラインの汎用的な記述と、実システムの具体的な記述を突合して解釈する作業が大変。漏れやミスが発生

提供価値

- 機械の目を使って確認漏れや解釈の違いを防止
- 高品質かつ属人性を排除した均一なガイドラインチェックにより、セキュアなITシステムの効率的な開発を実現

Why NEC

チェック対象となる設計書の背景やシステム状況、利用場面などの補足情報を独自機能で自動追加
業種に特化した設計書でも高精度なチェックを自律的に実施可能

情報セキュリティ内部監査Agent

※NECグループ会社17社向けの内部監査において、標準的な対応での独自算出

背景・課題

- 米国証券取引委員会（SEC）や標準技術研究所（NIST）から、セキュリティガバナンスを強化するよう要請

提供価値

- 監査報告書の作成時間を短縮、スキルの違いによるばらつきがあった監査品質を向上
- 内部監査のためのアンケート回答のチェックや監査報告書の作成を支援

Why NEC

NECの監査ノウハウやセキュリティコンサル業務の知見をナレッジ化しAgentが活用
（将来的には）業種特有の事情を考慮した是正対応などの必要な対策も提言

5 これからのサイバーセキュリティ事業

これからの「.JP（日本のサイバー空間）」を守るためには、これらAI技術の活用やインテリジェンスに加え、地政学リスクを踏まえた分析が不可欠です。しかしインテリジェンスを人手で収集・分析するのは莫大な労力と時間が必要になります。またインテリジェンスを収集・販売している事業者も国内外に多数存在しますが、安全保障の観点では海外への依存は望ましいことではありません。

NECは、独自の生成AI「cotomi」を活用してインテリジェンスをリアルタイムに収集し高度な分析を行うことで、信頼できる国産のインテリジェンスを蓄積し、これらに基づく安心・安全なサービスを政府や企業へ提供していくことを目指します。

またインテリジェンスを安全に取り扱うには、セキュリティ・クリアランス制度に準拠した設備や人材が不可欠です。NECはサイバーセキュリティ事業のコアとして、日本政府が求めるセキュリティ・クリアランスを満たすCyber Intelligence & Operation Centerを新設し、提供するサイバーセキュリティサービスの拡充をはかってまいります。

さらに、これらの技術を活用したサイバーセキュリティ事業をグローバルに展開し、24時間対応を実施することで、海外に進出した日本企業の事業継続に強力に貢献してまいります。

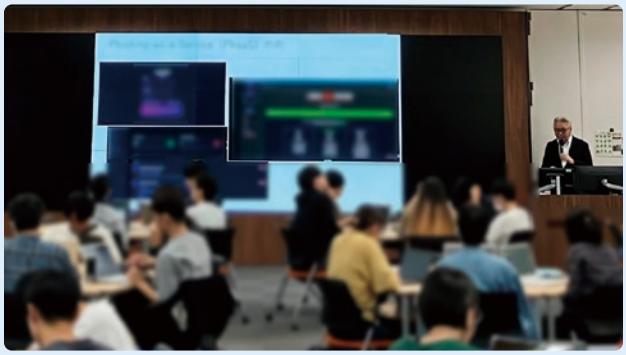
NEC独自のインテリジェンス

人材育成

これらのサービス提供や事業展開に向け、NECグループではサイバーセキュリティ専門人材を多数育成してきました。しかし「.JP（日本のサイバー空間）」を守るためには、NECグループの人材だけでは量も質も充分ではありません。そのため、NECでは国内の学生やお客様へのセキュリティ研修を実施しております。

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年にわた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行っています。2024年9月に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グループ女性エンジニア5名とのキャリアワークショップやWebアプリケーションの脆弱性診断のハンズオンデモ体験ができるテクニカルワークショップを行いました。加えて、2024年10月から2025年2月にかけて、鹿児島工業高等専門学校の情報工学科や都市環境デザイン工学科など全5学科の3年生200名以上を対象に、一般科目「リベラルアーツII」の必修講義の1つとして「セキュリティリスクアセスメント」の講義を実施いたしました。

また2024年10月から11月にかけて、長崎県立大学情報システム学部にて「セキュアシステム設計技法」講座を実施しました。本講座は拡大するサイバー攻撃への対策として、システム開発には不可欠なセキュア開発の手法について、座学だけでなく実際の開発現場で使われている手法の実践演習などを通じて理解を深めることを目的に、セキュア開発を推進しているNECのエンジニアが教育コンテンツを無償で提供し講師を務めました。



長崎県立大学 情報システム学部での「セキュアシステム設計技法」講座

13 | 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5年連続（2020~2024）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2つを獲得（最高位）。
（日経500種平均構成銘柄の企業の中から13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（2025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
- 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
- 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
- NECライフキャリア株式会社

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）

14 | NECグループの概要

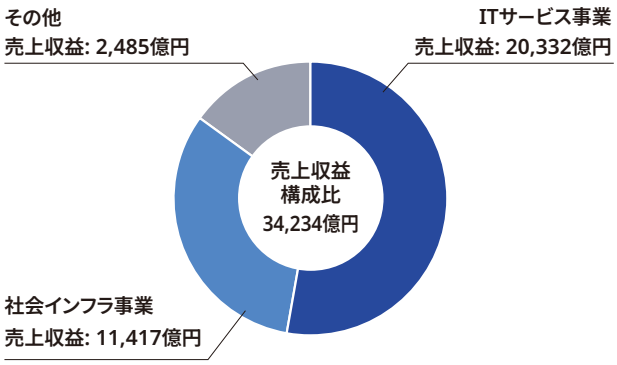
会社概要

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	104,194名※
連結子会社数	249社※

※2025年3月31日現在

事業紹介

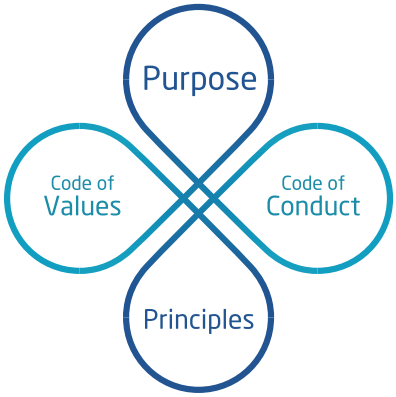
セグメント別売上収益



※2025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。

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 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

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

日本電気株式会社
〒108-8001 東京都港区芝5丁目7-1
TEL: (03) 3454-1111 (大代表)
https://jpn.nec.com

VEGETABLE OIL INK

2025年7月発行

Cat.No. U01-25070292J