サイバーセキュリティ経営報告書2026

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 代表取締役会長

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、法規制への対応力（Regulation）と企業価値の維持・向上（Reputation）、そして事業継続性を支えるレジリエンス（Resilience）の強化につながる、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を確立。日本のデジタルインフラを守り、経済安全保障と産業競争力の向上に貢献すべく、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し、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、日本IT団体連盟の「サイバーインデックス企業調査2025」で4年連続最高位の二つ星を獲得しました。

本報告書では、2026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 | サイバーセキュリティ・ガバナンス

指示1 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サイバーセキュリティ・ガバナンスを確立しています。

1 NECグループのサイバーセキュリティ・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ひとつであると認識し、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。

サイバーセキュリティ・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。

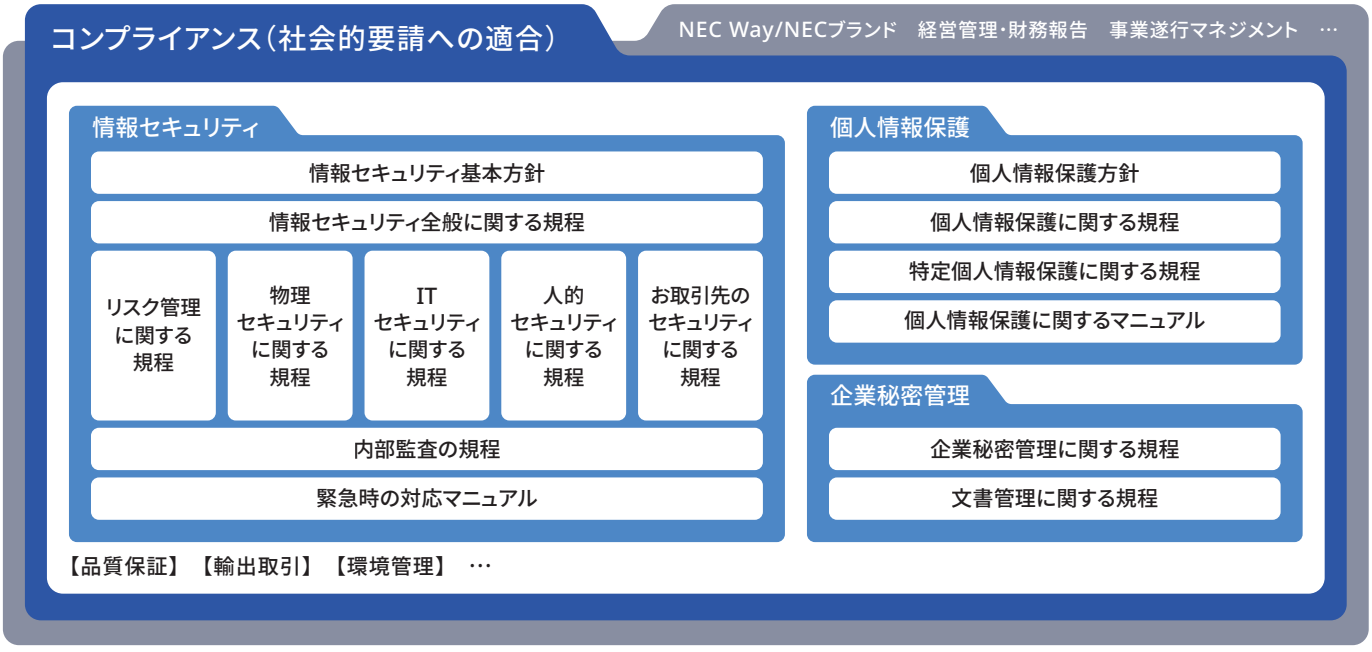
2 情報セキュリティに関するポリシー

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」、「番号法」に準拠しています。

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(2026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 AIに関するポリシー

NECグループは、AIや生体情報を含むデータの利活用を進めるにあたり、プライバシーへの配慮と人権尊重を最優先とする指針として「AIと人権に関するポリシー」を策定しています。本ポリシーは、各国・地域の法令遵守を前提に、社員一人ひとりが事業活動のあらゆる段階で人権を常に意識し、行動に結びつけるための経営上の基本方針です。運用面では、AIが社内外で適正な用途に用いられるよう徹底するとともに、技術開発と人材育成を推進し、ステークホルダーとの連携・協働を強化しています。外部有識者との対話も踏まえながら、信頼されるAI活用と社会課題の解決に取り組んでいます。

4 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。

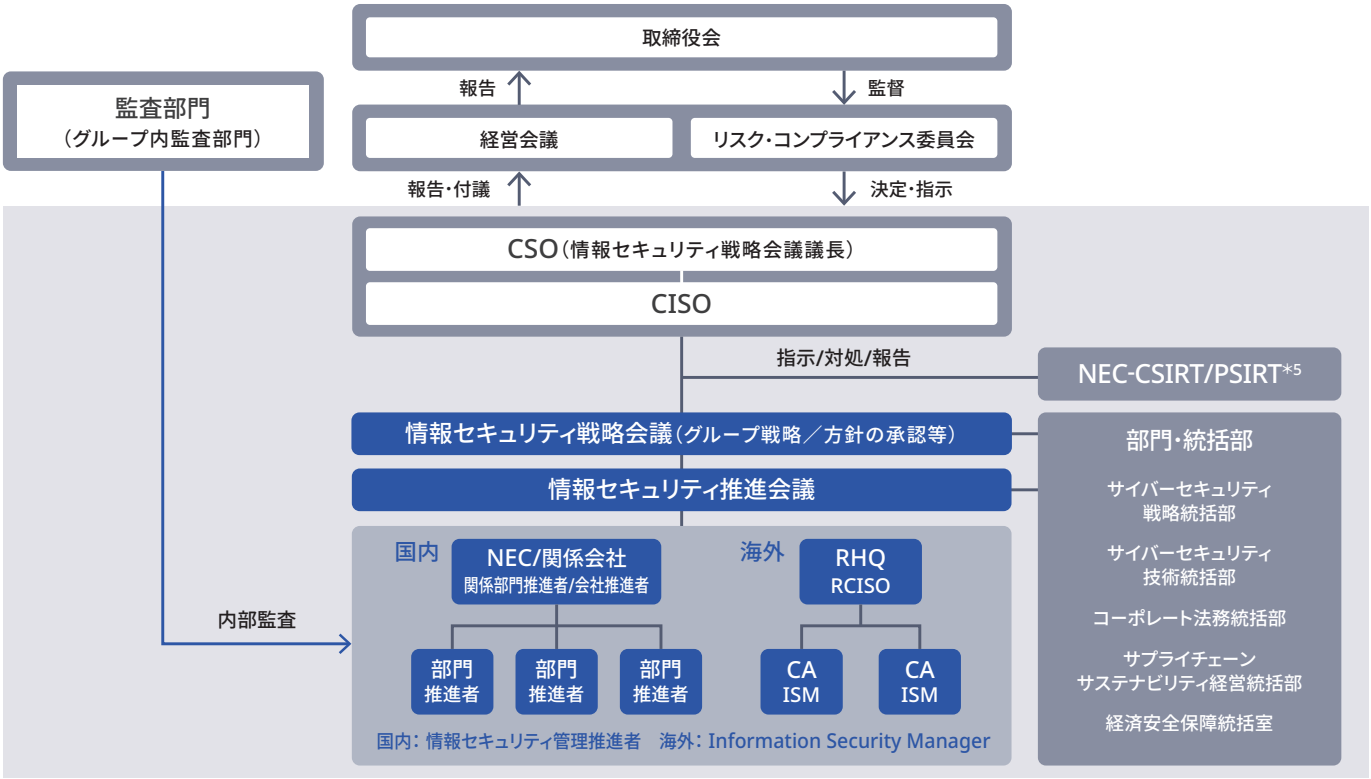
CISOは、情報セキュリティ対策を推進するサイバーセキュリティ技術統括部、サイバーセキュリティ戦略統括部と、サイバー攻撃を監視しインシデント発生時には迅速に収拾をはかるCSIRT*3を統括します。情報セキュリティ推進会議やワーキンググループは、情報セキュリティ推進計画の共有、情報セキュリティ施策の討議・調整、進捗報告、各組織の情報セキュリティ管理推進者への依頼、督促などを行います。

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

3 ｜ 情報セキュリティマネジメント

指示2 指示6

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、維持・向上するために、各種施策をNECグループ全体に実施しています。

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。なお、近年の関係法令に基づき、さらに高い機微性を有する情報については、取扱者を業務上必要な者に限定するとともに、専用の管理体制かつ保管環境にて厳格に運用予定です。

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実施する業務監査の一環として、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項目について年次で監査を実施しています。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）

4 ｜ 情報セキュリティ基盤

指示3 指示5

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、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。

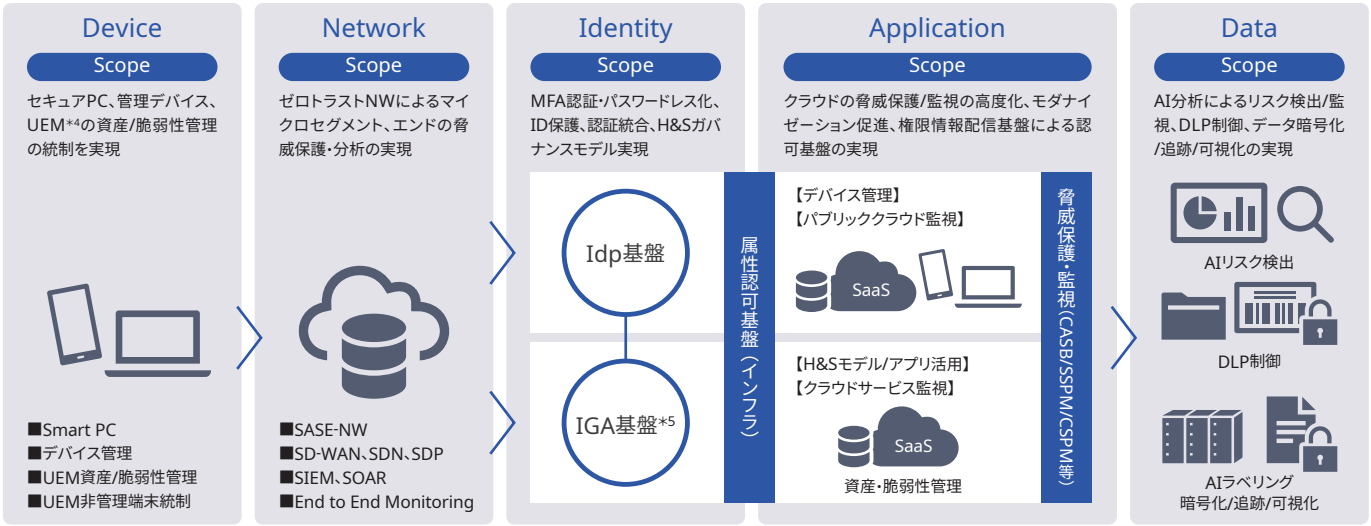
① グローバルID活用	アイデンティティ管理の実現（利用者アカウントの中央統制、ライフサイクル管理）
② 認証・デバイス管理	ユーザ認証（パスワードレス、多要素認証）、デバイス認証/管理端末化の統制環境の実現
③ グローバルアプリ管理	共通システムやサービスのアクセス管理、シングルサインオン（SSO）の実現
④ セキュリティガバナンス	グローバルでのセキュリティポリシーや設定情報の一元管理・統制の実現

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（Smart PCシリーズ）を整備しています。

Smart PC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。Smart PC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）、セキュリティ設定の自動適用、および社内認証統合などに対応しています。NECでは、統合エンドポイント管理基盤（UEM）を導入し、国内外に26万台あるIT資産をクラウド上で

ゼロトラスト基盤の概要とスコープ

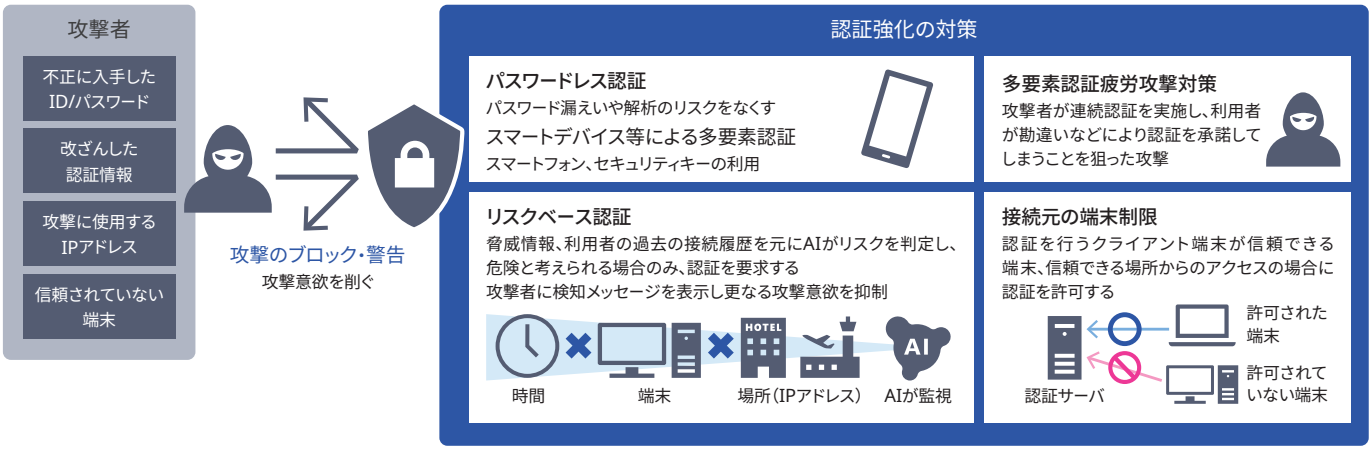


*1 CISA: Cybersecurity and Infrastructure Security Agency　*2 MFA: Multi-Factor Authentication　*3 IAM: Identity and Access Management
*4 UEM:Unified Endpoint Management Platformの略称。接続場所を問わず、様々な機器を一元管理し、セキュリティレベルの向上を実現する基盤
*5 IGA（Identity Governance and Administration）：ユーザ等のライフサイクル管理、アクセス権管理、プロビジョニング、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

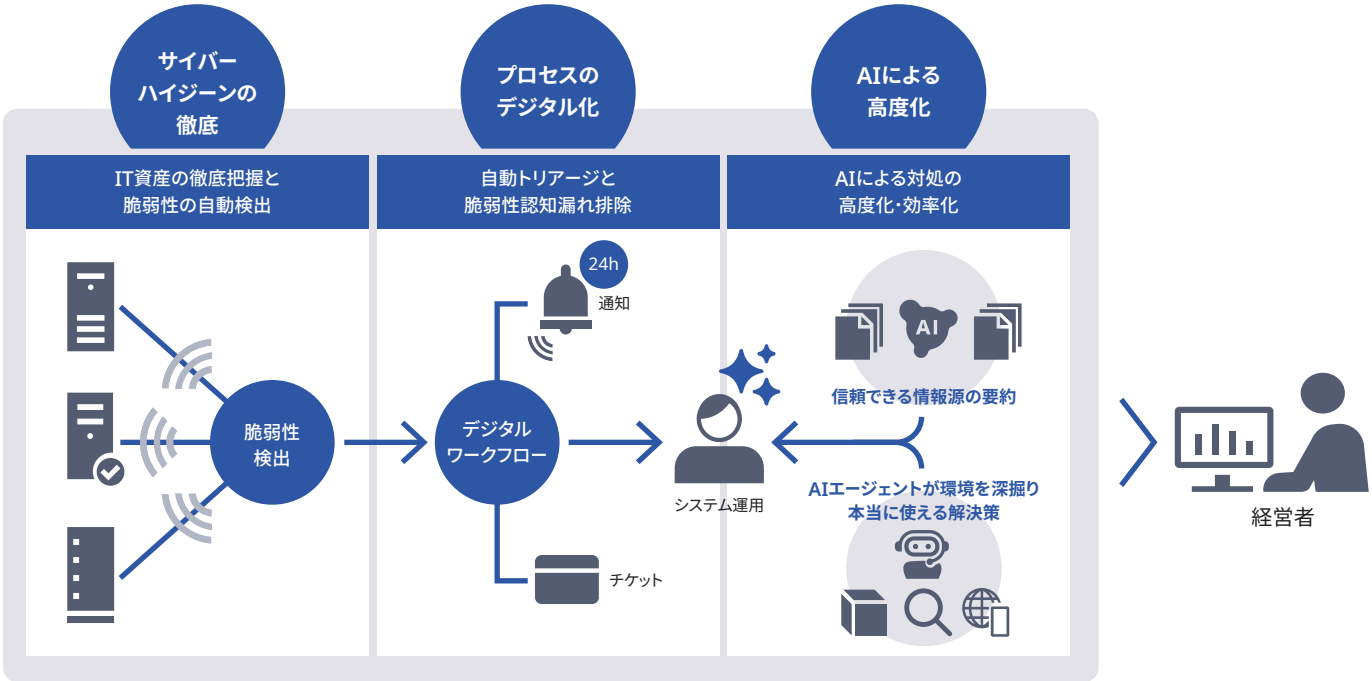
一元管理しています。この仕組みにより、脆弱性の検出や可視化を通じて、セキュリティリスクへの迅速な対応と管理業務の効率化を実現しています。また、サイバー攻撃から企業システムを保護する上で、サーバの脆弱性管理は必要不可欠であり、継続的な取り組みが必要です。社内1万台以上のサーバをセキュアに維持するため、脆弱性の早期検出・通知や可視化を実現するデータドリブンセキュリティを確立しました。近年は、AIを活用して脆弱性を悪用する攻撃が巧妙化しています。こうした状況を踏まえ、脆弱性の検出から通知・対処に至る一連の運用をさらに高度化するため、独自のAI技術を活用した仕組みを構築しました。AIが環境や脆弱性の特性を踏まえた最適な対処情報を生成することで、運用者の判断・対応負荷を軽減し、安全で正確かつ迅速な脆弱性対応を支援しています。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



AIを活用した自律型脆弱性管理の全体像



*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

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・監視がされています。特にグローバル展開においては、段階的にベースラインの引き上げを行うことで、国内と同等のセキュリティレベルを実現しました。リモート環境はクラウドベースのRemote Gatewayへの移行により、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（国内導入は完了・海外展開を推進中）。

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。

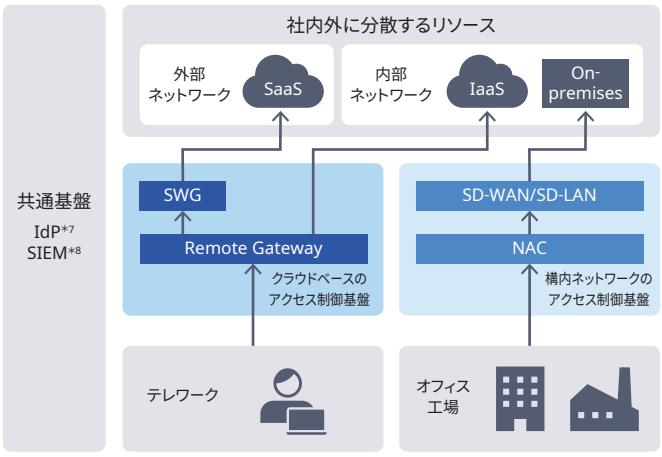
❷ グローバルSD-WAN展開

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。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拠点へ展開を実施しています。

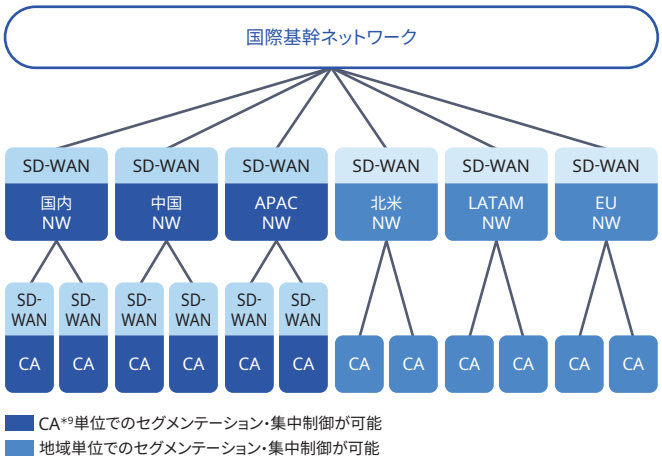
性能や可用性の革新：総帯域を4倍以上に拡張、ネットワーク変更のリードタイムを数分の一に短縮しました。可用性の面では専用線では費用負担の大きかった回線の冗長化を小規模な拠点でも実現しました。

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。

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



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可能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*10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 クラウドネイティブ環境の包括的なセキュリティ対策

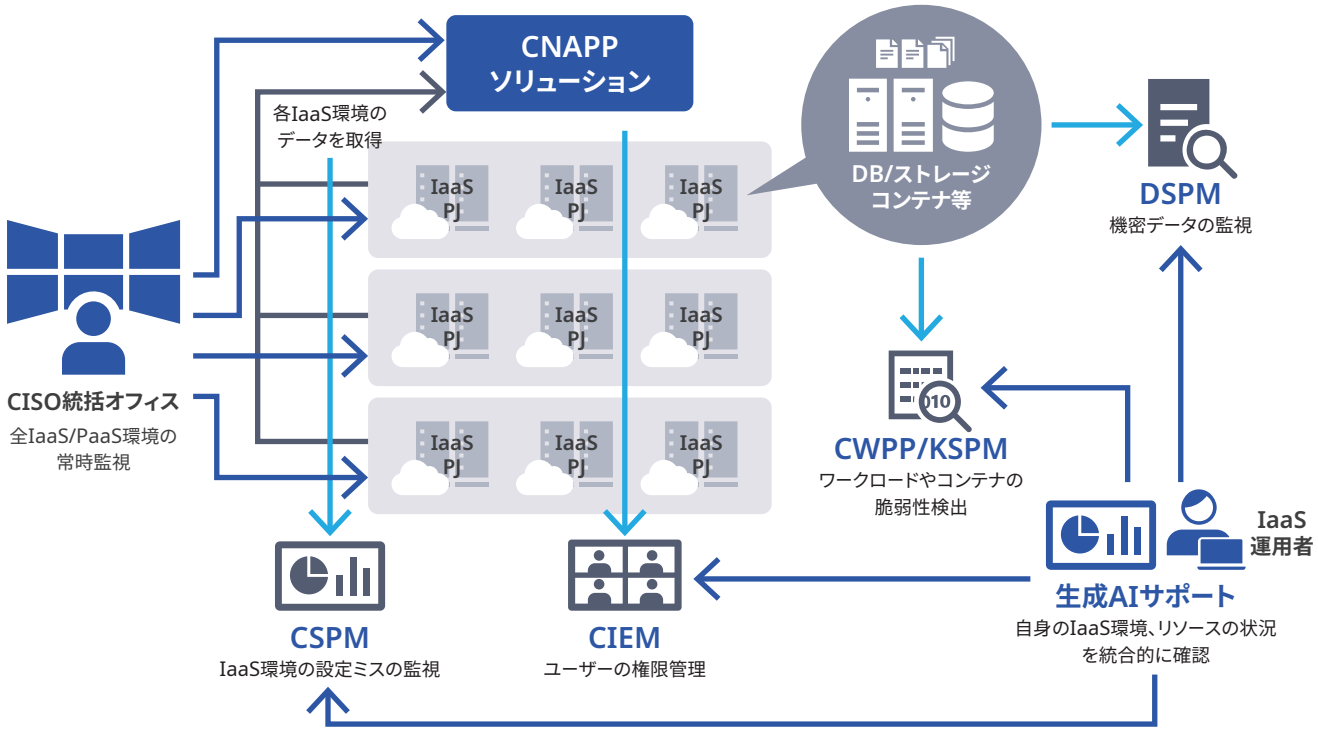
AWSやAzure、GCPなどパブリッククラウドの利用が拡大し、コンテナやサーバーレス等のクラウドネイティブ技術の活用が進んでいます。これにより、従来の設定ミスに起因するリスクだけでなく、保護すべき領域が拡大し、リスクが複雑化しています。NECグループでは、これらの多様なリスクへ統合的に対応するため、CNAPP*11を活用しています。CNAPPを活用することで、従来型のCSPMの機能を発展させ、クラウド環境全体を包括的に保護することが出来ます。

*7 IdP: Identity Provider　*8 SIEM: Security Information and Event Management　*9 CA（Corporate Affiliate）: 関連会社
*10 CASB: Cloud Access Security Broker　*11 CNAPP: Cloud-Native Application Protection Platform

❸ SaaSの設定ミスに起因するインシデントの防止

Microsoft365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セキュリティリスクが伴います。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。

クラウドネイティブ環境に対するCNAPPによる包括的なセキュリティ対策



5 データセキュリティ

❶ 情報の分類と保護（ファイルラベリング/暗号化）

NECグループでは、ゼロトラストセキュリティの考え方に基づき、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「InfoCage FileShell」を活用し、重要情報の区分に応じたファイルラベリング/暗号化を実施しています。ラベルに応じてアクセス制御や暗号化を適用することで、Officeファイルを含む各種ファイルの適切な取り扱いを徹底し、マルウェア感染などによる外部への情報流出を防止しています。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、重要度の高いファイルを取り扱う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。

❸ DLP（Data Loss Prevention）

企業の機密情報を保護し、全社的な情報漏洩対策を強化するため、新たにDLP施策を導入しました。働き方の多様化が進む中、既存の「情報漏えいリスク行動検知」施策は、退職者・退職予定者など一部の高リスク者に限定したものであり、監視範囲外で発生しうる潜在的リスクへの対応が課題でした。これに対し、今回導入したDLPは、全従業員のPC端末を対象とし、機密情報がUSBメモリやWeb経由等で不正に持ち出されるのをリアルタイムで監視・ブロックします。これにより、悪意ある行為だけでなく、操作ミスによる意図しない情報漏えいも防ぐことが可能となります。これら二つの施策は、それぞれ「特定人物の行動を深掘りする役割」と「全社を網羅的に保護する役割」を担います。両者を組み合わせることで、多層的なアプローチが可能となり、セキュリティの穴を埋め、社内全体のリスクを低減させることができます。

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

6 AIセキュリティ(Security for AI)

NECグループでは、自社利用およびSI・サービス事業において、AIを安全・安心に利用するための基盤を確立することを目的とした「AIセキュリティ(Security for AI)」推進プロジェクトを進めています。具体的には、AIを利用するための方針・ルール・体制といったガバナンス、遵守状況の把握といったマネジメント、そして管理およびリスク軽減のための基盤を確立しています。

❶ AIを取り巻くセキュリティの背景とビジネスリスク

AI技術の広がりと業務への適用が進む中、AIを取り巻くセキュリティ環境は複雑化しています。これに伴い、法的責任の追及、社会的信用の低下等のセキュリティに起因するAI関連のビジネスリスクが顕在化しており、これらのリスクを低減することは喫緊の課題です。これらのリスクに対応するため、NECグループではガバナンス、マネジメント、基盤という3つの軸でAIを守る体制を構築しています。

❷ AIアセットに対する脅威とセキュリティアプローチ

AIアセットの利用拡大に伴い、様々な脅威が顕在化・高度化しています。AIアセットは、LLM、学習データ、RAG、AIエージェント、A2A、MCPといった「デジタル空間」のものから、既存システム、センサー、機械・装置といった「現実空間」のものまで多岐にわたります。

これらのAIアセットに対する脅威(リスク)には、プロンプトインジェクションや情報漏えい、ユーザーリテラシーの不足等の現時点のリスクとAIエージェントの暴走や過剰な自律性、シャドーAI等の今後のリスクがあります。

これらの脅威に対し、ガバナンス、マネジメント、基盤の観点から体系的な対策を講じます。

- **ガバナンス:方針・ルール、ガイドラインの策定、リテラシー向上、体制整備**
- **マネジメント:遵守状況の把握(点検)と可視化**
- **基盤(技術):AIアセット検出(シャドーAI)、AI脆弱性診断、AIガードレール**

❸ NECにおけるSecurity for AIの実装方針

AIをセキュアに利用・提供するための制度・体制・仕組みを実装し、NECグループにおけるAIの安心・安全な利用とお客様へのAI提供を実現しています。

- **ガバナンス**

AIをセキュアに開発・提供および利用するための基本方針とルールを定め、AIガバナンスとして管理体制を確立しています。

- **マネジメント**

AIセキュリティに対する管理プロセスを確立します。ガイドライン・フレームワーク(NIST AI RMF[*14]、AI事業者ガイドライン、EU AI Actなど)を基に遵守事項を定め、社内向け・お客様向けAIシステム/サービス、LLM、AIエージェントなどのAIアセットのセキュリティ状況を把握し、改善サイクルを確立しています。利用者向け・開発者向け・提供者向けガイドラインを整備し、AIの安心・安全な利用・提供に活用しています。

- **セキュリティ基盤**

AIアセットに対するセキュリティの状況を把握し、AIアセットの保護やチェックをするための技術的な仕組みを実装しています。これには、AIアセット検出、AI脆弱性診断・監査、AIガードレール、シャドーAI検出などが含まれます。

これらの取り組みにより、お客様への説明責任を果たし、従業員のAIのスキル・リテラシー向上を図ります。

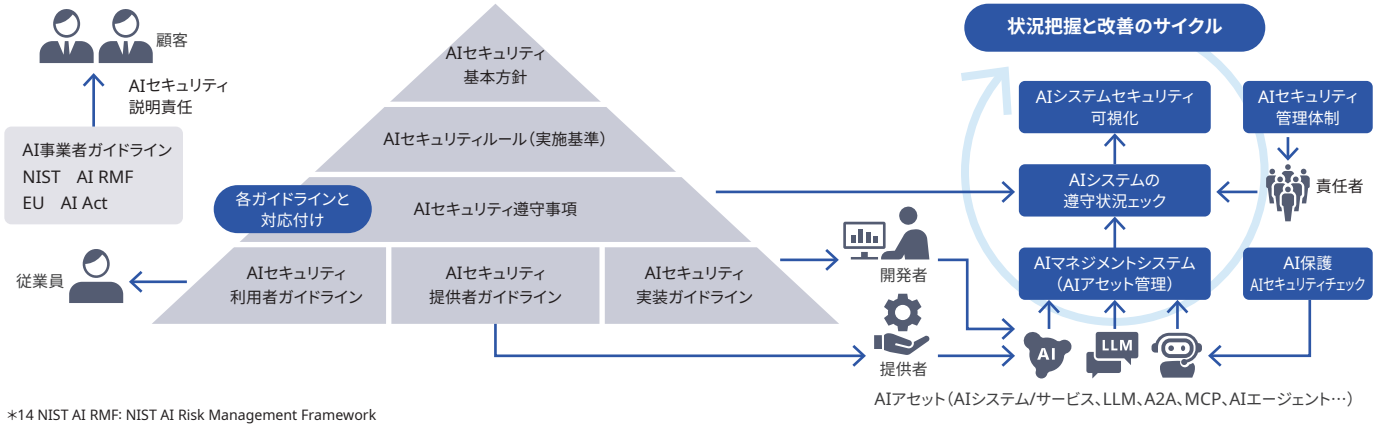
❹ 外部ガイドラインとの連携

ガバナンス領域では、社内利用におけるAIポリシー(AI利用、AIセキュリティ&倫理)やAIシステム/サービスの社内提供におけるポリシーを策定しています。利用者向け、開発・提供者向けのガイドラインを策定・浸透させ、AI利用者向けおよび開発・提供者向けの社内教育を開発・実施します。マネジメント領域では、NIST AI RMFやAI事業者ガイドラインの遵守項目を精査し、NECとしての遵守項目を作成しています。既存のセキュリティ体制との整合調整や、AIの登録・点検システムの要件定義、実装検討、導入を進めています。

セキュリティ基盤領域では、AIシステム保護サービスおよびAIシステム検証サービスの評価・選定、導入、継続的効果測定を実施しています。

これらの活動は、NIST AI RMF、総務省・経済産業省が策定するAI事業者ガイドライン、EU AI Act等の主要な外部ガイドライン・法規制を考慮して進めています。特に、NIST AI RMFを主なフレームワークとし、AI事業者ガイドラインの遵守項目を取り込みつつ、EU AI Actとも対応付ける方針です。また、広島AIプロセスで示されている、高度なAIシステムを開発する組織向けの国際行動規範にも留意し、AIライフサイクル全体にわたるリスク管理、透明性の確保、強固なセキュリティ管理、コンテンツ認証、責任ある情報共有などを重視して取り組んでいます。

Security for AIの全体像



*14 NIST AI RMF: NIST AI Risk Management Framework

5 ｜ 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、情報を集める、教育を受けるといった「知る」、ルールを守る、リスクを見つけるといった「気づく」、リスクを指摘する、対策に取り組むといった「アクション」といった要素や、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（2025年度修了率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、セキュリティ提案・実装、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98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。2025年度は10名以上が受講し、累計124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2025年度は延べ1,500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。2025年度は1,300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10,000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

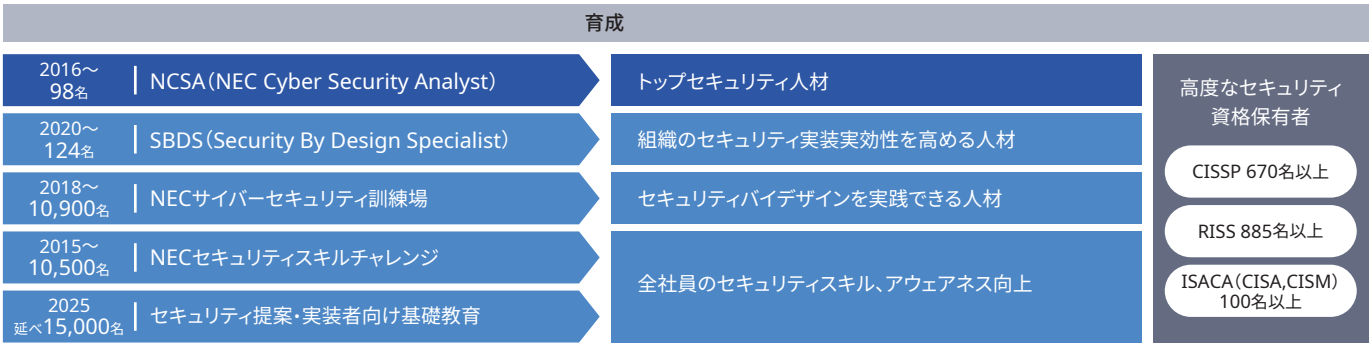
お客様向けの提案・実装プロセスに関わる全社員を対象に、2023年10月に施行されたサイバーセキュリティ管理規程に基づき、自身の役割に応じて実施すべき内容の理解度をサーベイにて測定しました。サーベイ実施後、個々のサーベイ結果（理解度）に応じた教育を展開し、2025年度の学習者は延べ15,000名となりました。

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670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ています。また、本提携により、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、専門人材を育成しています。これまでに、NECグループのISACA認定資格保有者は延べ100名以上となり、監査（チェック）とマネジメント（管理）の両面で対応できる人材層の拡充が進んでいます。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

セキュリティ・バイ・デザインの実践、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）

6 | 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NISTCSF*1 1.1及びNISTCSF2.0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*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。

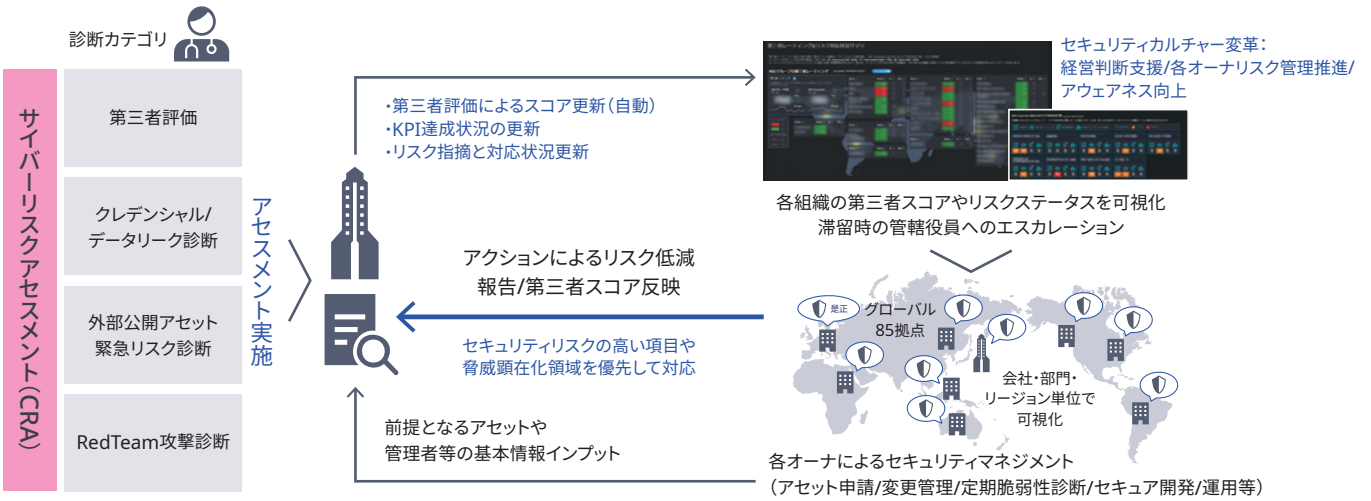
これらの取り組みが社外からも認められ、一般社団法人日本IT団体連盟が実施する「サイバーインデックス企業調査2025」において、取り組み姿勢および情報開示が特に優れていると評価され、最高位である「2つ星」を4年連続で受賞、その他複数の賞もいただいております。

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、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。

サイバーリスクアセスメント



*1 NISTCSF（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 Defense Centre
*4 RedTeam: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

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。

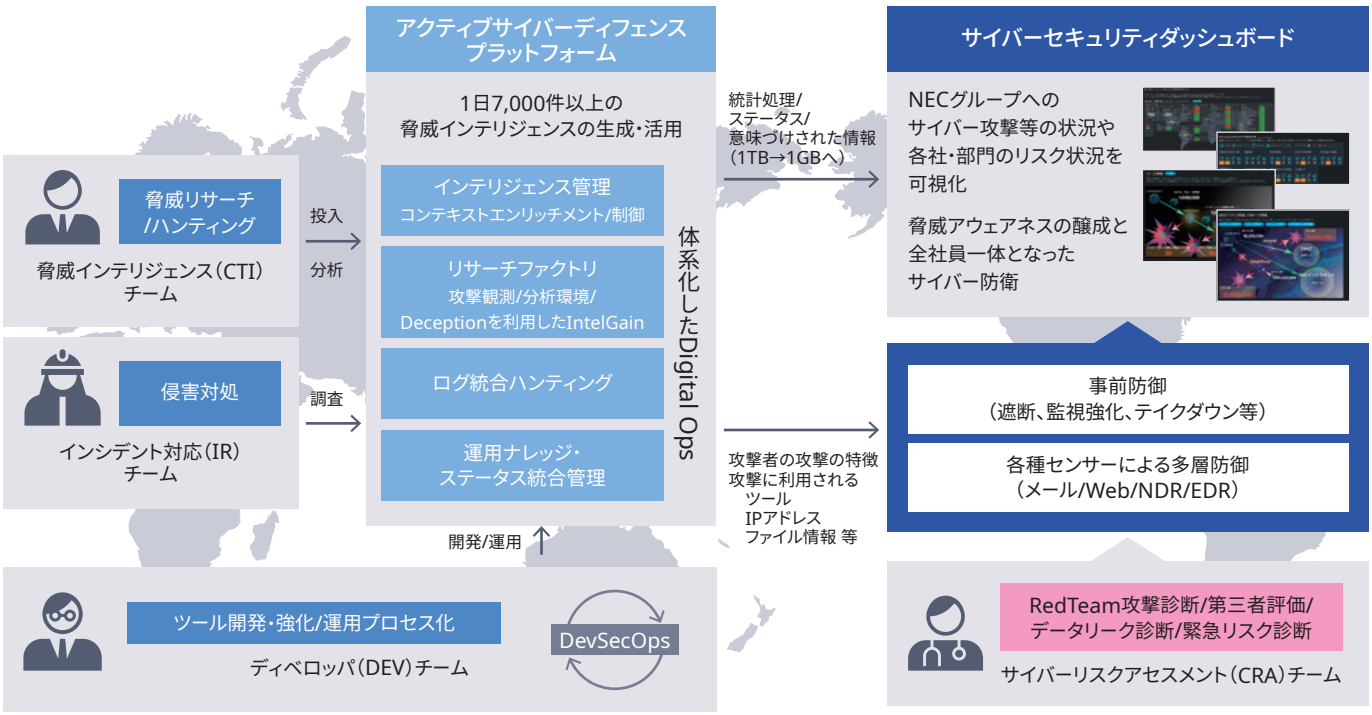
また、昨年度開催された大阪・関西万博のような大規模イベントでは、関連する企業がサイバー攻撃の標的となるリスクが高まるため、NECでは、NISCとのサイバー攻撃対応演習、特別エスカレーションルールの取り決め、期間中のセキュリティ体制構築、CSIRT/SOCによる重点監視と脅威インテリジェンス強化などの、サイバー攻撃への対策を講じました。

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ThreeLinesModel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



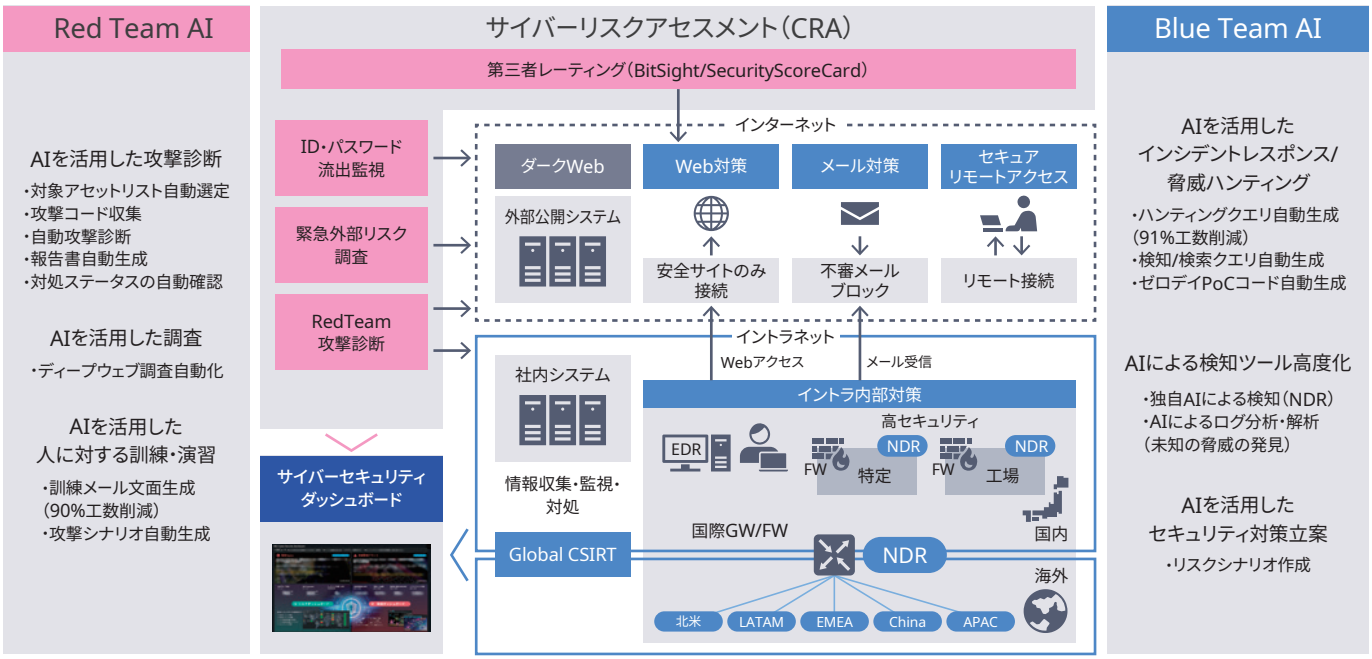
*5 CTI: Cyber Threat Intelligence
*6 EDR: Endpoint Detection and Response
*7 NDR: Network Detection and Response

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RedTeamAI/BlueTeamAI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AgenticAI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 ― 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、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。

また、画像・動画・音楽・音声・テキストなどAIをフル活用した、セキュリティエグゼクティブダッシュボードのサイネージにより、経営層が一目見て社内外のセキュリティ情勢を把握できるようにしています。

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ValueCreatorとしての役割を一層強化して参ります。

エグゼクティブダッシュボード

サイバーセキュリティダッシュボード

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 重要情報管理・保護、セキュリティレジリエンス

NECグループでは、安全性と利便性の両立を目指した重要情報の管理、データセキュリティによる情報漏洩対策、およびインシデント対応訓練やデータバックアップによるセキュリティレジリエンスの向上に取り組んでいます。昨今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、持続可能なデータドリブン経営のためのセキュリティ事例としてご活用いただいています。（p.6「重要情報管理」、p.10「データセキュリティ」、p.14「グローバルサイバー攻撃対策」参照）

❷ AIとセキュリティ

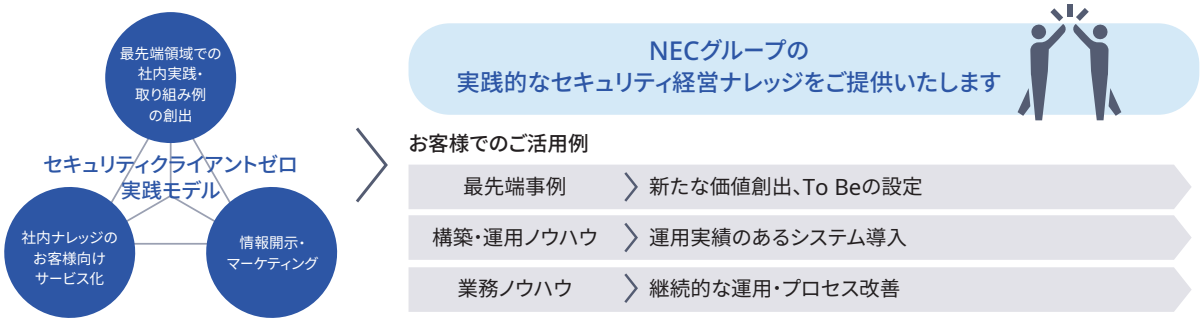
NECグループでは、AIの安全な利活用を目指す「Security for AI」（p.11）と、セキュリティ対策にAIを活用する「AI for Security」の両者を推進しています。社内セキュリティ施策においては、「AI for Security」を実践し、セキュリティ対策の効率化・自動化、品質の向上に取り組むとともに、セキュリティクライアントゼロ事例としてのノウハウを蓄積しています。

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、AIプラットフォームを含む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

7 | 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。

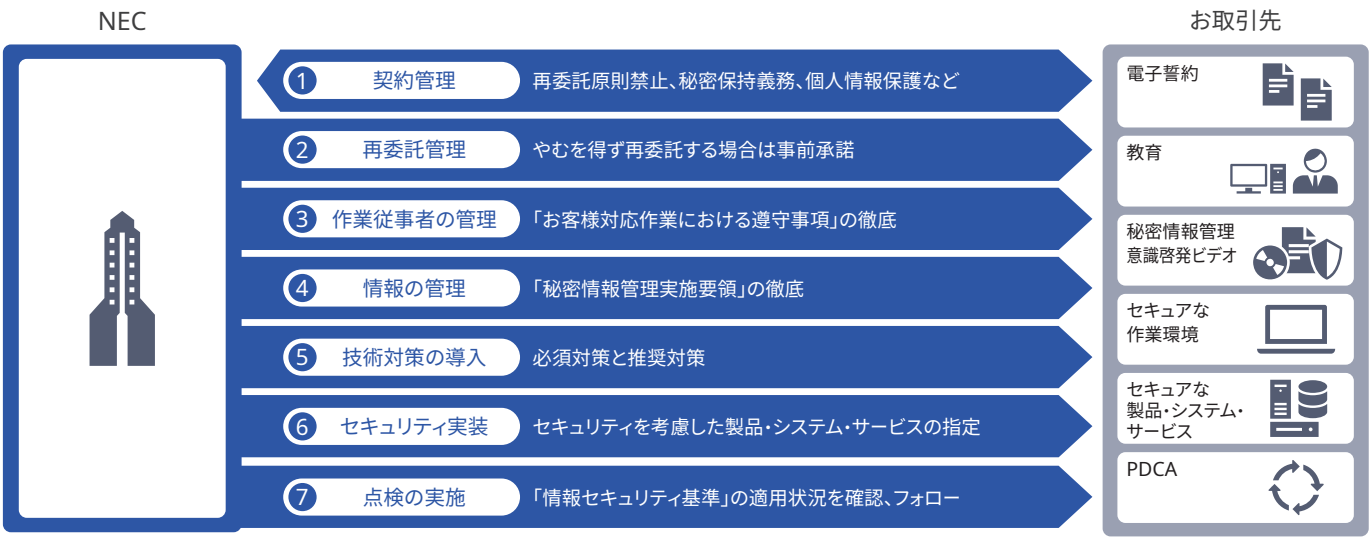
❻ セキュリティ実装

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「お取引先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「お取引先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

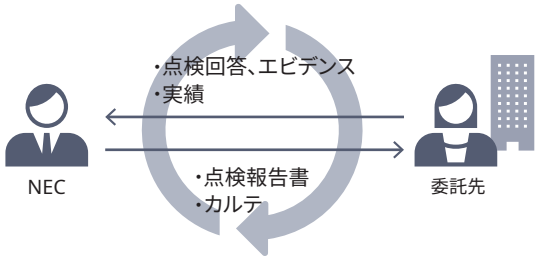
NECと取引のある会社、約1,800社を対象に書類点検を実施しています。お取引先は自社の対策状況を自ら点検し、点検結果はWebシステムによってリアルタイムでフィードバックを行っています。また、取引が多いお取引先には直接訪問、あるいはリモートを活用した訪問点検を実施しています。2025年度は対象220社に対し、NEC点検担当者約70名によって推進しています。

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2025年度にかけて中国、インド、ベトナムで開催しました。またオフショア開発を実施しているお取引先様へもNIST SP800-171をベースとした基準での書類点検、訪問点検を開始しました。

海外についても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。

8 | 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750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います。

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います。2025年度はサイバーセキュリティ管理規程の改訂を行いました。この改訂では、万が一セキュリティインシデントが発生してしまった際のビジネスリスクを低減することを目的に、提案・開発段階でシステムインテグレーターとしての責任履行およびお客様との責任範囲明確化を実施する内容を追加しました。また、NECの国内グループ会社のうち100%子会社においては、サイバーセキュリティ管理規程の展開が完了しており、ビジネスリスク低減に関する改訂内容についても反映できるよう活動を開始しています。

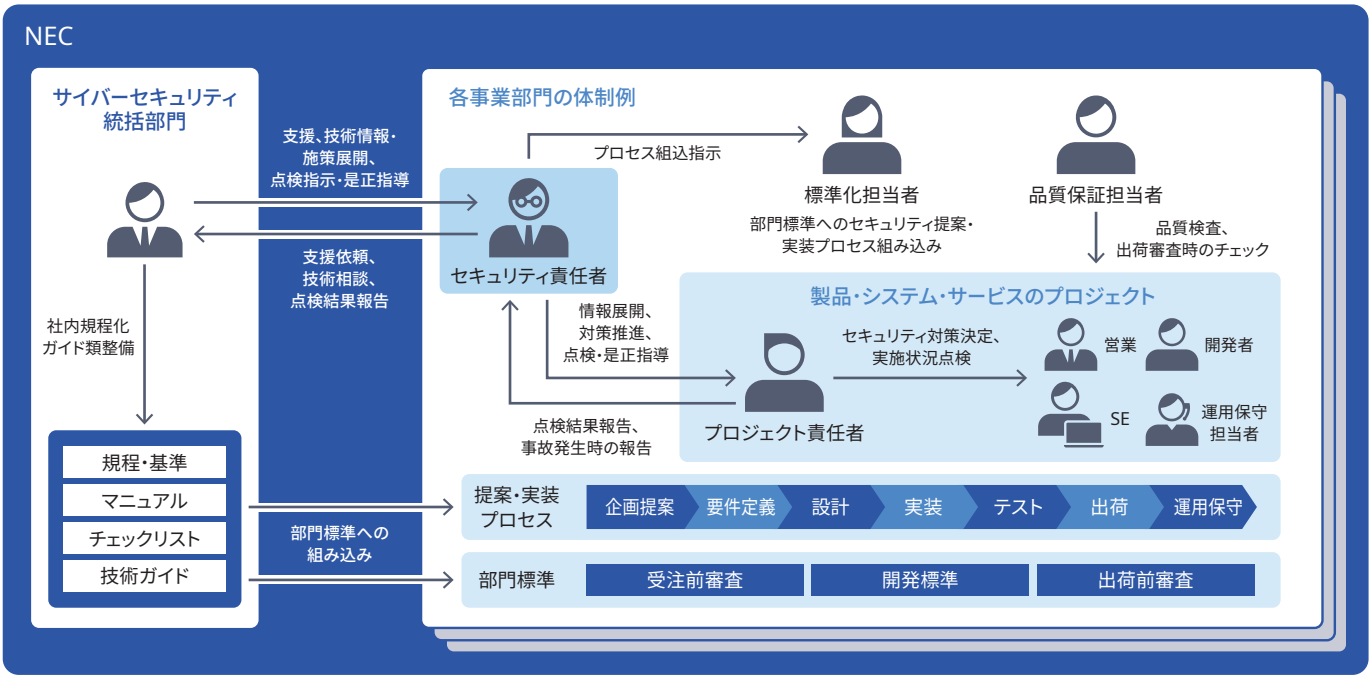
❷ セキュリティ実装の主要な取り組み

NECでは、セキュリティを確保する「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。今後は、フロンティアAIの活用により、出荷前の段階における脆弱性の検出および対応の高度化を図り、お客様に対してより一層安心・安全な製品・システム・サービスの提供を実現してまいります。

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

セキュリティ実装プロセス



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、脆弱性リスク指標、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おり、事業リスクを判断する情報として活用されています。

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。脆弱性公開ポリシーの公開、社外からの受付窓口の設置、貢献ページの運用、CNA*1機関として活動するなど、グループ会社を含めた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。加えて、ものづくりをしているNECグループ会社を含めた情報連係を図るために、NECグループPSIRTコミュニティを設立し、PSIRT活動がNECグループ全体で機能するように取り組んでいます。これらの取り組みの結果、2025年度において、当社の業績や見通しに重大な影響を与えるデータ侵害や情報漏えいはありませんでした。

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 ハードウェア製品のセキュリティ強化

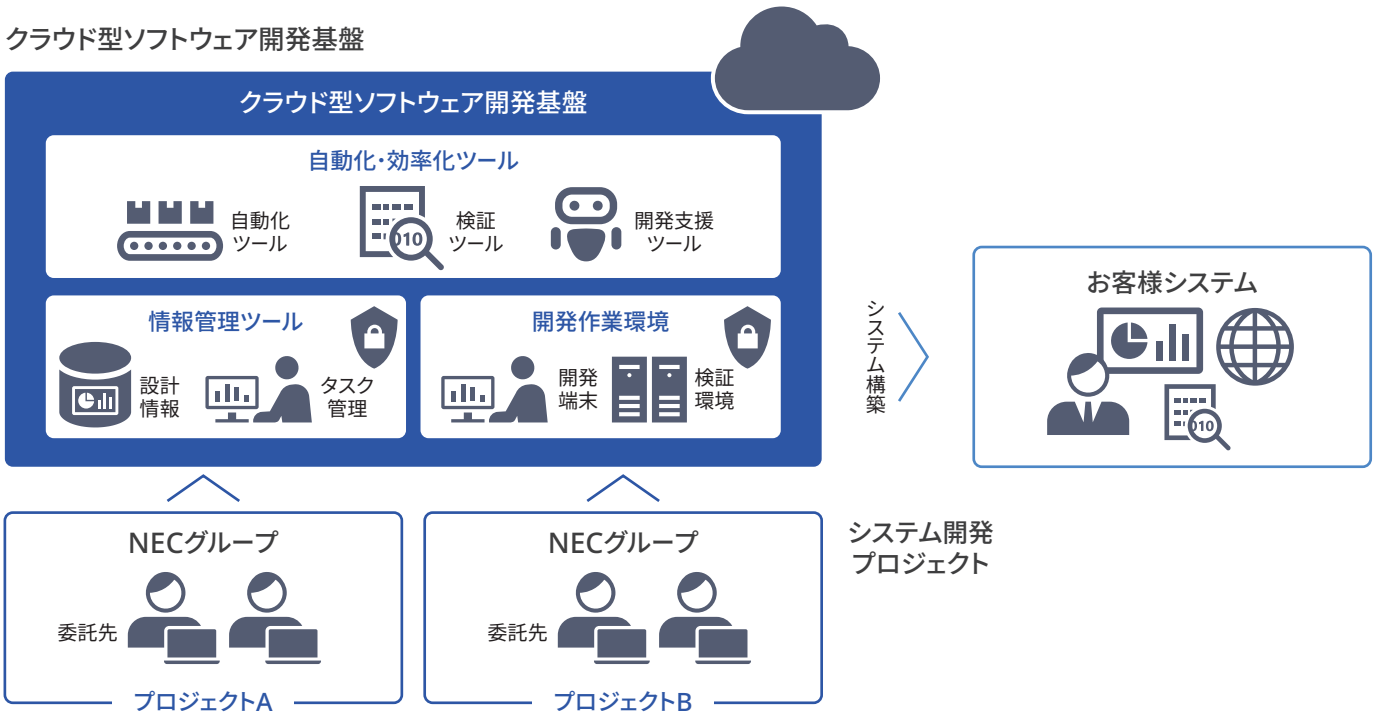
ハードウェア製品については、企画・設計・実装・評価・保守に至る開発ライフサイクル全体でセキュリティを考慮した設計・実装を行っています。製品そのものに加え、開発環境におけるセキュリティ基準を定め、セキュアな製品開発基盤の強化にも取り組んでいます。

また、日本国内のIoT製品向け認証制度である「JC-STAR（セキュリティ要件適合評価及びラベリング制度）」の取得を開始しています。

❺ 生産（工場）拠点のセキュリティ強化

生産（工場）拠点では、経済産業省の工場セキュリティガイドラインをベースとした第三者によるリスクアセスメントの結果から定量的な目標を設定してセキュリティ対策を推進しています。また工場のサイバー攻撃に備え定期的なサイバーBCP訓練を継続するとともに、リスクの可視化を進めデータドリブンなサイバーセキュリティの実現に取り組んでいます。

クラウド型ソフトウェア開発基盤



*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

9 | 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。

2025年は日本のサイバーセキュリティ政策にとって大きな転換点となる年でした。1月から開催された第217回通常国会で「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）が可決成立し、能動的サイバー防御（Active Cyber Defense;ACD）の実施に向けた体制の整備・強化が始まりました。サイバー対処能力強化法及び同整備法は順次施行され、7月には内閣サイバーセキュリティセンター（NISC）が発展的に改組され各種取り組みの司令塔たる国家サイバー統括室（National Cybersecurity Office: NCO）が、翌2026年4月には通信情報利用の適正確保のためサイバー通信情報監理委員会が新設されました。10月からはアクセス無害化についても措置が可能になり、また官民連携の強化として特別社会基盤事業者が使用する特定重要電子計算機の届出やインシデント発生時の報告義務化が予定されています。そして2025年12月には4年ぶりにサイバーセキュリティ戦略が更新され、社会全体のサイバーセキュリティおよびレジリエンスの向上により、深刻化するサイバー脅威を防御・抑止するという方向性が示されました。

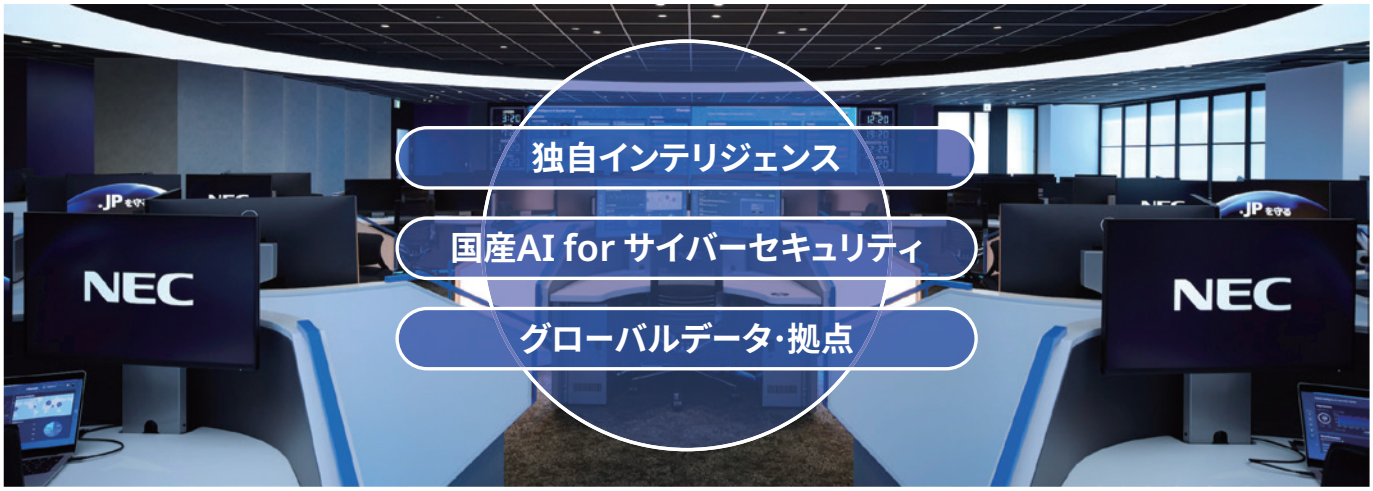
しかしランサムウェア攻撃をはじめとする企業へのサイバー攻撃は量・質ともに著しい勢いで深刻化し続けています。2025年も海外からと思われるサイバー攻撃により企業が数カ月の事業停止に追い込まれる事案が複数発生しました。サイバー攻撃の影響は、直接攻撃を受けた企業だけでなくサプライチェーンにまでおよび、一企業へのサイバー攻撃が取引先企業の事業やブランドを棄損することにもなりました。サイバー攻撃は産業化しており、その損害額は2025年には10.5兆ドルに、2031年には12.2兆ドルに上るとも推計[*1]されています。これは米国や中国のGDPに次ぐ額であり、日本の名目 GDP4.3兆ドル[*2]の2倍を超える額に上ります。独立行政法人情報処理推進機構（IPA）発行の「情報セキュリティ10大脅威2026［組織編］」[*3]（10大脅威）でも、昨年に引き続き「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」「地政学的リスクに起因するサイバー攻撃（情報戦を含む）」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続けています。また「AIの利用をめぐるサイバーリスク」が初めて選出されて、AIを利用したシステムの様々な脆弱性を狙った外部からの攻撃リスクや AI悪用による攻撃の容易化を招く可能性が指摘されています。

このような政府のサイバーセキュリティ体制整備・強化の動向やサイバー空間を取り巻く状況の悪化に対応し、NECも「.JP（日本のサイバー空間）を守る」というミッションを掲げ、サイバーセキュリティ事業の強化に取り組んでいます。2025年5月にはKDDI株式会社とサイバーセキュリティ事業における協業の検討を開始する基本合意書を締結[*4]し、10月にはサイバーセキュリティ分野の更なる強化に向けて、両社のシナジーを活用した事業展開を検討する合弁会社「United Cyber Force株式会社」を設立[*5]しました。

また2025年11月には次世代サイバーセキュリティサービス「CyIOC

「.JPを守る」次世代サイバーセキュリティサービス「CyIOC」

CyIOC



*1 Cybersecurity Ventures、Cybercrime To Cost The World $12.2 Trillion Annually By 2031、https://cybersecurityventures.com/official-cybercrime-report-2025/
*2 International Monetary Fund、GDP, current prices、https://www.imf.org/external/datamapper/NGDPD@WEO/OEMDC/ADVEC/WEOWOR
*3 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2026、https://www.ipa.go.jp/security/10threats/10threats2026.html
*4 KDDIとNEC、国内最大規模のサイバーセキュリティ事業を目指し、協業に向けた基本合意書を締結、https://jpn.nec.com/press/202505/20250508_02.html

（サイオック）」の提供を開始しました。米国立標準技術研究所（NIST*6）が策定した機密性の高い重要情報（CUI）を扱う際のセキュリティ基準「NIST SP800-171」をベンチマークとして*7、日本に新設および米国既存施設をアップグレードしたCyber Intelligence & Operation Centerを司令塔とし、NEC独自の脅威インテリジェンスを活用して、サイバー攻撃の予兆把握からプロアクティブな防御、インシデント対応まで包括的な支援をご提供しています。

2026年も政府はサイバーセキュリティ体制の強化をさらに進めています。近年相次いだ医療機関へのサイバー攻撃事案を踏まえ、「医療分野」を特定社会基盤事業（基幹インフラ事業）へ追加することが検討されています。重要社会基盤事業者（重要インフラ事業者）についても、各分野における個々のサイバーセキュリティ対策のさらなる強化し、分野や事業者を横断して講ずるべきサイバーセキュリティ対策を確保するための「重要インフラ統一基準」の策定が予定されています。また「サプライチェーン強化に向けたセキュリティ対策評価制度（SCS（Supply Chain Security）評価制度）」が2026年度中に開始され、サプライチェーンに属するすべての企業がその立ち位置に応じて必要なセキュリティ対策を容易かつ適切に決定できるようになると期待されています。さらに2月から開催された第221回国会（特別会）で提出された国家情報会議設置法案では、安全保障の確保などへの対処を調査審議する国家情報会議の設置と内閣情報調査室を国家情報局へ発展的に改組することが決定しています。

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なインフラを支え、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。

「.JP（日本のサイバー空間）を守る」ためのインテリジェンスは、日本国内で得られるものだけでは充分とは言えません。海外とつながり海外のインテリジェンスを直接入手することが必要です。またサイバーセキュリティ戦略でも言及されているように、サイバーセキュリティに関する技術の多くを海外に依存しているなかサイバー対応に必要な人材・技術を我が国で持続的に産み出していく環境形成が急務であり、国産のサイバーセキュリティ技術や国産のAIを活用することが重要です。そしてなにより24時間365日絶え間なく「.JP（日本のサイバー空間）を守る」体制が不可欠です。

そのため、海外のインテリジェンスを直接入手し、海外を含めた日本企業の拠点を守るため、CyIOCサービスを拡張し、2027年4月からは欧州拠点を開設してFollow-The-Sunモデルによる運用の完成を目指しています。またガバメントAIでの試用にも選定された、NEC独自開発のAI「cotomi」でCyIOCを強化してまいります。

独自に収集するインテリジェンスと「cotomi」、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。

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会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。また経済産業省産業サイバーセキュリティ研究会ワーキンググループ3（産業振興・人材育成）の「サイバーセキュリティ・サービス事業者の信頼性強化に向けた検討会」や、日本成長戦略会議の戦略分野分科会（デジタル・サイバーセキュリティワーキンググループ、情報通信成長戦略官民協議会）に有識者として参画しています。

*1 Japan Cybercrime Control Center

*5 KDDIとNEC、サイバーセキュリティ分野の強化に向け合弁会社を設立、https://jpn.nec.com/press/202511/20251120_01.html
*6 National Institute of Standards and Technology
*7 非公開の別施設である「CyIOC for Government」では、米国連邦政府機関の情報システムについてのセキュリティ基準である「NIST SP800-53」をベンチマークしています。

10 | 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。

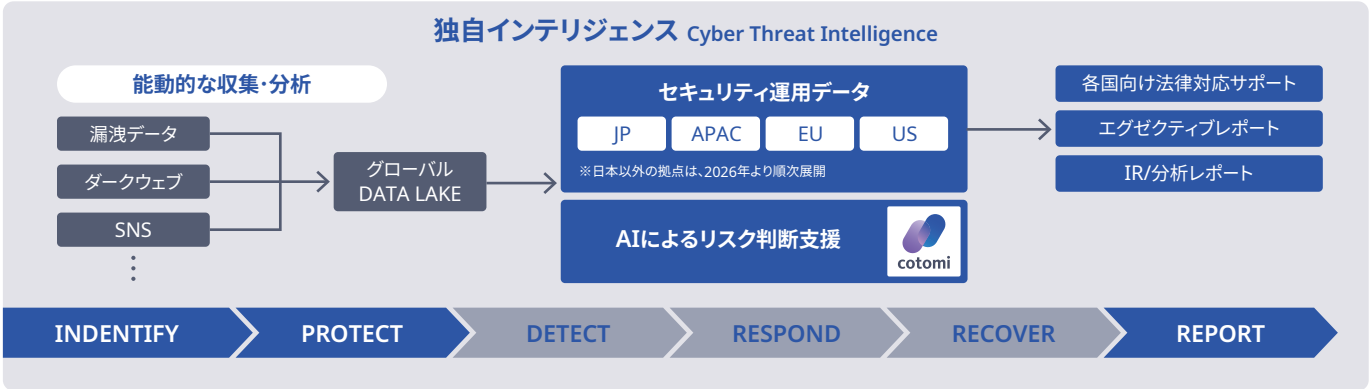
多くの企業がセキュリティ対策に取り組む一方で、セキュリティインシデントの発生や被害は増加し続けています。ランサムウェア被害の報告数も2020年下期から約5倍となるなど、企業規模を問わず被害が拡大し、事業継続が脅かされています。この背景には、急速な業務DXやクラウド利用拡大により、企業が守るべきIT資産・データが社内外に分散し、攻撃対象領域が広がっていることがあります。2025年に大手飲料メーカーや物流企業で報じられた事案のように、攻撃者は公開IT資産の脆弱性や設定不備を足掛かりに侵入し、被害を拡大させる手口が顕在化しています。さらに、激化するサイバー攻撃に対し、「国民生活や経済活動の基盤」と「国家及び国民の安全」を守るため、能動的サイバー防御の実施体制を整備する国家の動きも見られます。重要インフラを担う特定社会基盤事業者を中心に、より高度なセキュリティ対策への取り組みが求められています。

こうしたことを実現するには、自組織のセキュリティ体制構築とシステム全体で「今、何が起きているか」「どこまで対策できているのか」を可視化・把握し続けることが重要です。また、対策導入が部分最適に留まると、兆候把握や優先順位付けが難しくなり、リスクが潜在化しやすくなります。そのため、脅威インテリジェンスを活用した継続的監視と迅速な対処が不可欠です。こうした課題に対してNECでは、独自インテリジェンスとAIを活用した次世代サイバーセキュリティサービス「CyIOC」を中心に、高度なセキュリティ業務DXの実現を支援しております。

NECの次世代サイバーセキュリティサービス「CyIOC」

「.JP（日本のサイバー空間）を守る」というミッションのもと、国内およびグローバルに事業を展開する企業をこれらの脅威から防御するため、NEC独自のインテリジェンスとAI技術を融合した次世代サイバーセキュリティサービスです。

CyIOC



インテリジェンスからレポーティングまで：

専任チームがダークウェブや地政学リスクに基づく脅威情報を収集し、プロアクティブ防御とAIによるレポーティングを提供します。

高度化するサイバー攻撃への対処：

CyIOCによるプロアクティブな防御では、収集した独自インテリジェンスに基づくグローバル規模での防御センサーへ事前にルールをインプットし、攻撃者のTTPs（Tactics, Techniques, Procedures）に基づいた高度な監視で、機器単体では気づきにくい高度な攻撃を検知いたします。

AI活用による価値向上：

AIによる自動分析でアラートの約90%を自動判定し、残り約10%は熟練アナリストが精査します。これにより、全体の約0.02%にあたる「真に重大なアラート」のみをお客様へ通知し、意思決定の質と効率を飛躍的に向上させます。

米国基準のベンチマークで実施：

組織や企業におけるサイバーセキュリティへの対応の開始や改善に向けて、NIST（米国国立標準技術研究所）が提示した「NIST SP800-53」をベンチマークとして新設された「Cyber Intelligence & Operation Center」がCyIOCの司令塔となります。世界的な標準に準拠したセキュリティ基準が高い監視センターを構築し、法規制に応じたデータ保護を実施いたします。

グローバルで展開（27年度から）：

グローバル拠点に高度人材を配置し、24時間365日体制で監視を実行します（Follow the sun）。途切れない監視と対応を基にインテリジェンスとAIを駆使し、各地法制度 / 言語 / 文化 / 時差といったグローバル特有課題を踏まえてグローバル全体で日本品質のセキュリティ対策を提供します。さらに、各拠点で検知した不審なアクセス情報を還元することで、さらなる脅威インテリジェンスの強化につなげます。

関係機関への報告支援（27年度から）：

国家や国民の安全をサイバー攻撃から守るための体制整備を目的としたサイバー対処能力強化法[*1]では「特定重要電子計算機のサイバーセキュリティが害されたこと又はその原因となり得る一定の事象を認知したときは、その旨及び一定の事項を事業所管大臣及び内閣総理大臣に報告しなければならない」と義務付けられています。こうした関係機関への報告も、CyIOCで収集した情報や分析結果を元に支援いたします。

*1 出典：https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo_torikumi/pdf/setsumei.pdf

クライアントゼロによる価値創出

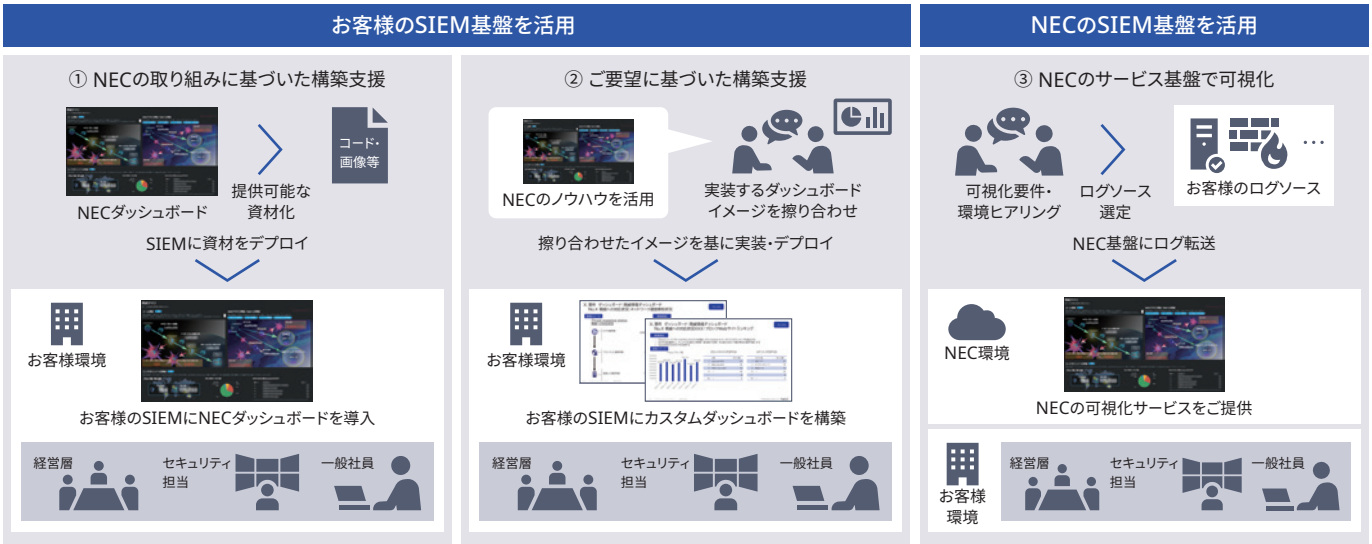
NECは、お客様への新たな価値創造モデルとして「BluStellar」を発足しました。実績に裏打ちされた業種横断の先進知見とNECのテクノロジーにより、社会課題と経営課題を解決し、お客様を未来へ導くモデルです。また、コンサルや製品・サービスを組み合わせた価値創造シナリオ「BluStellar Scenario」により、お客様の課題を解決します。

本項では、Scenarioによる価値提供の一要素であるクライアントゼロの取り組みについて、代表例をいくつか紹介します。前項のCyIOCやクライアントゼロによるNECの付加価値を加えた提案も含め、NECはセキュリティリスクの可視化・課題整理から運用・監視まで、セキュリティ課題の解決を一気通貫で支援可能です。

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、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、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

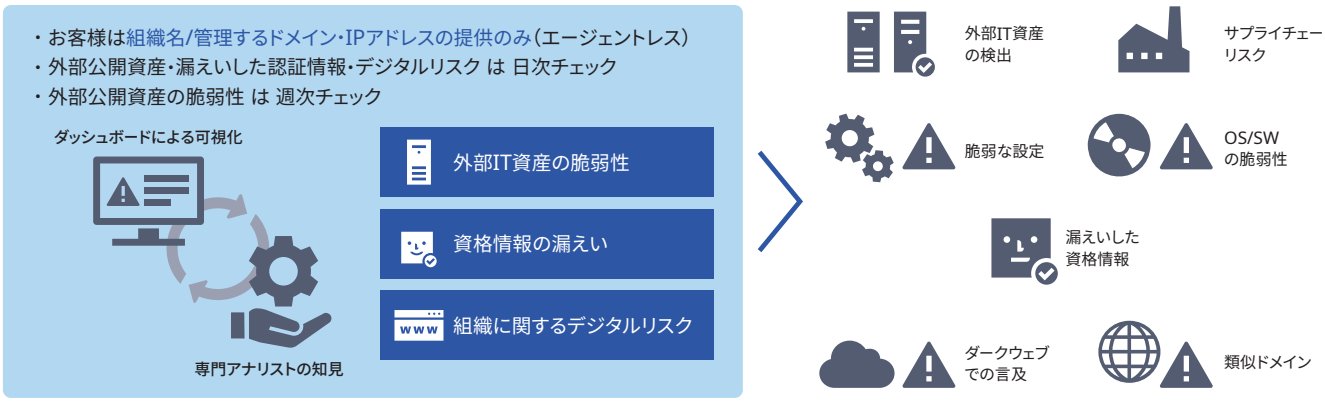


2 外部IT資産リスク可視化サービス

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。

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

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）

4 重要情報保護ソリューション

クラウド化や経済安保法制の進展により、重要情報の定義・管理・保護の仕組みが不可欠となっています。NECは、リスクアセスメント/基本構想策定から、Microsoft Purview（秘密度ラベル・DLP・IRM）の設計・導入、InfoCage FileShellによるファイル暗号化、AI自動ラベリングによる利便性向上まで一気通貫で提供します。ガバナンスとIT対策を連動させ、管理状況の可視化と漏えいリスク低減を実現し、経営層への報告体制構築も支援します。

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。また、2025年11月より次世代サイバーセキュリティサービス「CyIOC（サイオック）」を立ち上げ、お客様のサイバー攻撃対策をより強力に支援いたします。

11 ｜「JP（日本のサイバー空間）」を守るためのグローバルな研究・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

セキュリティ・バイ・デザインを支援するAI Agentによって「正しくつくる」、「正常をつづける」、「攻撃からまもる」の実現を目指しています。NECでは、これらの実現にあたって日本の研究開発部門を中心にドイツの欧州研究所、イスラエルの研究センターとともに技術開発および事業化を進めています。これら国内外の研究所の最新の研究開発成果についてご紹介します。

AI × セキュリティ 技術開発コンセプト

2 国内研究所　セキュリティ経営Agent

国内研究所では、セキュリティ経営Agentの1つとして経営インパクトを推定する技術の研究開発を進めています。「正常をつづける」ためのセキュリティ対策を実施する際に、予算や人員が限られる中、どこから対策を実施すべきかを判断することが重要です。対策が必要なシステムと事業の関係性を把握し、システム停止による企業活動への影響や個人情報の漏洩による損失といった事業影響の大きさを推定することで、対策の優先度づけを可能にします。

しかし、事業被害の大きさや損失額を推定するには、自社で運用しているシステムや事業に熟知し、過去に起きた類似の被害事例などから被害額の平均を見積もるなど、知識やスキルが求められます。NECの国内研究所ではこれらの分析を代替するAI Agentの研究開発に取り組んでいます。開発中の経営インパクト推定技術では、JCICモデル*3を用いてAI Agentが事業被害額を自動的に算出します。また、過去のサイバーセキュリティインシデントの事例から対象企業に関連する事例を選別し、提示するAI Agentを開発中です。このAI Agentを用いることで、過去の類似事例をインシデントが発生した際の参考情報とすることができます。これらの技術を活用することで、セキュリティ担当者は事業への影響を上位層へ説明するのが容易になり、経営者はセキュリティ対策の必要性を理解し、適切な投資判断ができるようになります。NECは、これらのAI Agentの開発を通してセキュリティ経営の効率化を支援します。

経営インパクトを推定する技術

*1 CSIRT: シーサート（Computer Security Incident Response Team）　*2 PSIRT: ピーサート（Product Security Incident Response Team）
*3 一般社団法 日本サイバーセキュリティ・イノベーション委員会（JCIC）「サイバーリスク数値化モデル」 https://www.j-cic.com/pdf/report/QuantifyingCyberRiskSurvey-20180919(JP).pdf

3 欧州研究所　セキュリティ運用Agent

欧州研究所では、セキュリティ運用Agentとして、脅威情報の分析を支援するAI Agentの研究開発に取り組んでいます。「攻撃からまもる」ためには、事前にどのような手口でシステムが攻撃されるかを知ることが重要です。近年、攻撃者によるAIの悪用が広がることで、サイバー攻撃が巧妙化、迅速化しています。これに対抗するには、防御側もAIを活用してサイバー攻撃に関する情報を収集、分析し、前もって防御を固めることが重要です。

しかしながら、脅威情報の分析は非常に難しく、膨大なセキュリティに関する情報を読み解き、攻撃に関する断片的な情報を組み立てていく必要があるため、熟練のノウハウや知識が要求されます。NECの欧州研究所は、サイバー脅威に関する情報を自動で関連付ける技術*4を研究開発しています。本技術は、NEC内で活用されているだけでなく、2025年度に製品化され、お客様にもお使いいただくことができます。

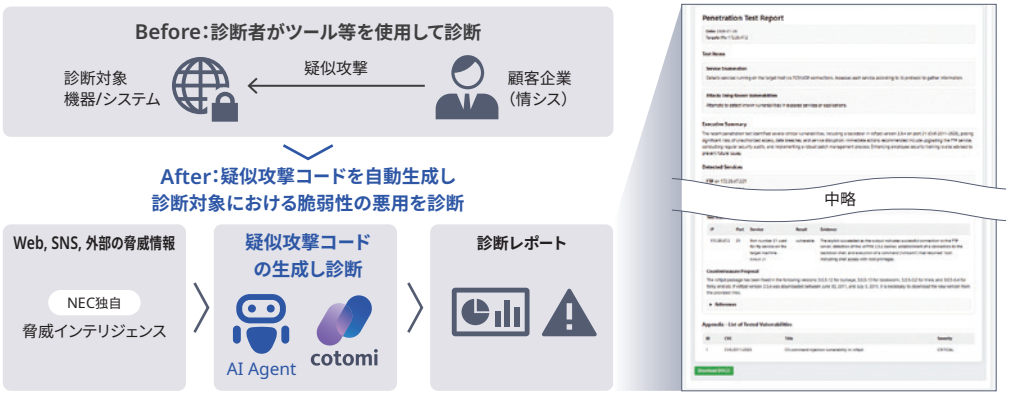
脅威情報を分析する技術

4 イスラエル研究センター　セキュリティ運用Agent

イスラエル研究センターでは、セキュリティ運用Agentのもう1つの技術として、ペネトレーションテストを支援するAI Agentの研究開発に取り組んでいます。機器やシステムを「攻撃からまもる」ために、診断対象に疑似的に攻撃を加えることで脆弱性の有無や悪用の可否を確認することの重要性が高まっています。具体的には、ペネトレーションテストにおける診断者は、診断対象の脆弱性の有無を調査し、脆弱性を見つけた際には、その脆弱性が悪用可能であるか確認するために疑似攻撃コードを作成して検証します。検証の結果、悪用可能とわかった場合は、攻撃方法とともに診断結果を報告します。

一方で、疑似攻撃コードの作成には、脆弱性の知識だけでなく、診断対象のシステムで利用されているソフトウェアやハードウェアに関する深い知識が必要です。そのため、熟練者が時間をかけて診断する必要があり、網羅的な診断は人材不足や費用面から非常に困難となっています。NECは、イスラエル研究センターのAI技術を活用し、この課題に取り組んでいます。このAI Agentは、公開されている疑似攻撃コードや脆弱性の検証コードを基に、指定した脆弱性を悪用する、実行可能な疑似攻撃コードを生成します。AI Agentの支援を得ることで、熟練者でなくても容易に脆弱性の悪用可能性を検証できるようになるため、網羅的な診断もできるようになります。

攻撃診断を支援する技術



*4 NEC技報 2023年「サイバー脅威インテリジェンス生成自動化」 https://jpn.nec.com/techrep/journal/g23/n02/230207.html

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・質ともに十分ではありません。そのため、NECでは国内の学生やお客様に向けた実践的なセキュリティ教育支援を推進しています。

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）と締結した包括連携協定に基づき、産学共同での高度技術者育成を加速させています。この取り組みの一環として、サイバーセキュリティ分野で高度なスキルを備え、そのスキルを活かして社会で活躍できる人材を輩出することを目的に、より実践的なセキュリティスキルの習得と、キャリア意識の向上に向け、様々なプログラムを実施しました。2025年10月から2026年1月にかけて、鹿児島工業高等専門学校の全5学科の3年生200名以上を対象に、必修講義「リベラルアーツII」で「セキュリティリスクアセスメント」の実践的講義を昨年度に続き実施しました。さらに、より高度なスキルを持つ人材の育成に向けて、2026年3月には、セキュリティコンテスト上位入賞の高専生19名を対象とした「K-SEC トップオブトップス講習会」を実施しました。同講習会では、NECのトップエンジニアが講師を務め、攻撃者視点を学ぶCTFの作問・解答演習を行いました。加えて、2025年12月には木更津工業高等専門学校の「高専キャリアラボ」にて、第一線で活躍するエンジニアがキャリア形成に関する講演を行うなど、学生がセキュリティを自分ごととして捉え、将来の選択肢を広げられるよう、多角的な支援を継続しています。

また、技術系の女子学生だけでなく、当分野で活躍する女性が少ないことを踏まえ、2025年9月に高専女子学生向けイベント「2025 K-SEC CAMP FOR GIRLS」をNECオフィスで開催し、全国から集まった27名の女子学生に、女性エンジニアとのキャリアワークショップやCTF（サイバーセキュリティ競技）演習を提供しました。

その結果、参加者はリスクアセスメント手法の理解や攻撃者視点の獲得など、実践的なセキュリティスキルを習得しました。加えて、将来のキャリア像の明確化や選択肢の拡大といった成果も得られました。

活動指標
- ・2025年度年間実施回数：（目標）4件／（実績）4件
- ・具体的な内容
  - 鹿児島高専：「セキュリティリスクアセスメント」の実践的講義（全4回）
  - 2025 K-SEC CAMP FOR GIRLS：高専女子学生向けCTF演習およびキャリアワークショップ
  - K-SEC トップオブトップス講習会2024：トップレベル高専生向けCTF作問・演習
  - 木更津高専「第16回 高専キャリアラボ」：キャリアの育て方に関する講演

参加者数
- ・当社従業員の参加数：延べ26名（第一線で活躍するセキュリティ専門エンジニアなどが講師やメンターとして参加）
- ・これらのプログラムに参加し、実践的なセキュリティスキルに関する講義・演習に参加した学生数：（目標）延べ250名／（実績）延べ250名以上

木更津工業高等専門学校での「高専キャリアラボ」講演

12 | 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（2026年6月15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
- NECセキュリティ株式会社

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）

13 | NECグループの概要

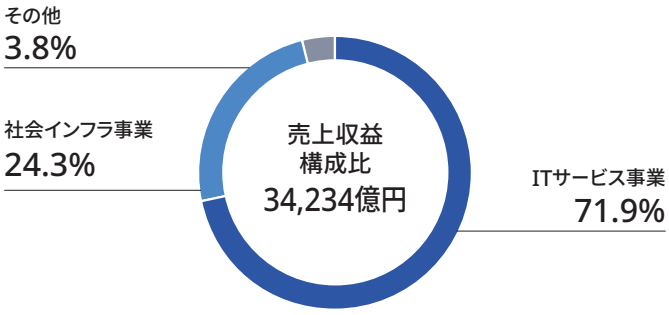
会社概要

商　　号	日本電気株式会社　NEC Corporation ［法人番号 7010401022916］
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	101,800名※
連結子会社数	252社※

※2026年3月31日現在

事業紹介

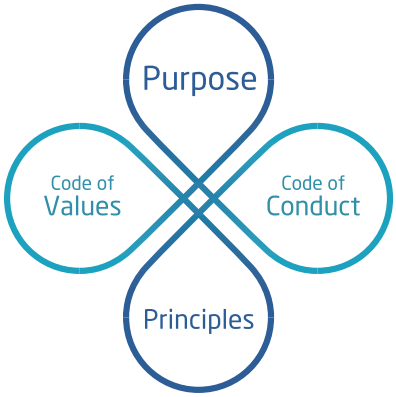
セグメント別売上収益



※2025年4月1日付で実施した組織体制の変更に伴い、
報告セグメントの内容を過去実績も含め変更しています。

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

2026年7月発行

Cat.No. U01-26060362J