Orchestrating a brighter world

NEC

情報セキュリティ報告書2023

Truly Open,Truly Trustedの実現

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

こだま ひろし
小玉 浩
日本電気株式会社
執行役Corporate EVP
兼 CIO（チーフインフォメーションオフィサー）
兼 CISO（チーフインフォメーションセキュリティオフィサー）

全世界がオープンに繋がる現在、AIによるサイバー攻撃の進化、クラウド活用の拡大による情報漏えいリスクの増大、経済安全保障における情報管理の課題にどう対応するかが、国家・企業問わず重要な問題となっています。

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

サイバーセキュリティ対策では、経済産業省の「サイバーセキュリティ経営ガイドラインVer3.0」やNIST（米国標準技術研究所）の「Cyber Security Framework（1.1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）を強化しています。さらに、データドリブン変革としてダッシュボードでサイバーセキュリティリスクを全従業員に示すことで、迅速な経営判断と現場の自律的なアクションに繋げています。

また、設計段階からセキュリティを考慮した「セキュリティ・バイ・デザイン3.0」に基づき、高品質で安全なサービスを提供するために、サプライチェーンも含めた対策強化に取り組んでいます。DXを推進するセキュリティ人材を育成するために、国際的な情報セキュリティ資格であるCISSP*2の取得を推進するとともに、教育機関と協力して将来の人材育成にも貢献しています。このような取り組みが評価され、日本IT団体連盟の「サイバーインデックス企業調査2022」で最高位の二つ星を獲得しました。

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

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

*1 CISA: Cybersecurity and Infrastructure Security Agency（米サイバーセキュリティ・インフラストラクチャセキュリティ庁）の略称。
*2 CISSP: Certified Information Systems Security Professional（セキュリティ プロフェッショナル認定資格制度）。
*3 米国国立標準技術研究所（NIST）による顔認証技術の精度評価で5回の第1位を獲得。

本報告書に関するお問い合わせ
日本電気株式会社
コーポレートIT・デジタル部門 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）

「情報セキュリティ報告書 2023」刊行にあたって

本報告書は、経済産業省が策定する「サイバーセキュリティ経営ガイドライン」Ver 3.0をベースに、ステークホルダーのみなさまにNECグループの情報セキュリティに関する取り組みについて、ご理解いただくことを目的に発刊いたしました。本報告書では、2023年6月までの取り組みを対象に掲載しています。

Contents

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

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

情報セキュリティ推進フレームワーク

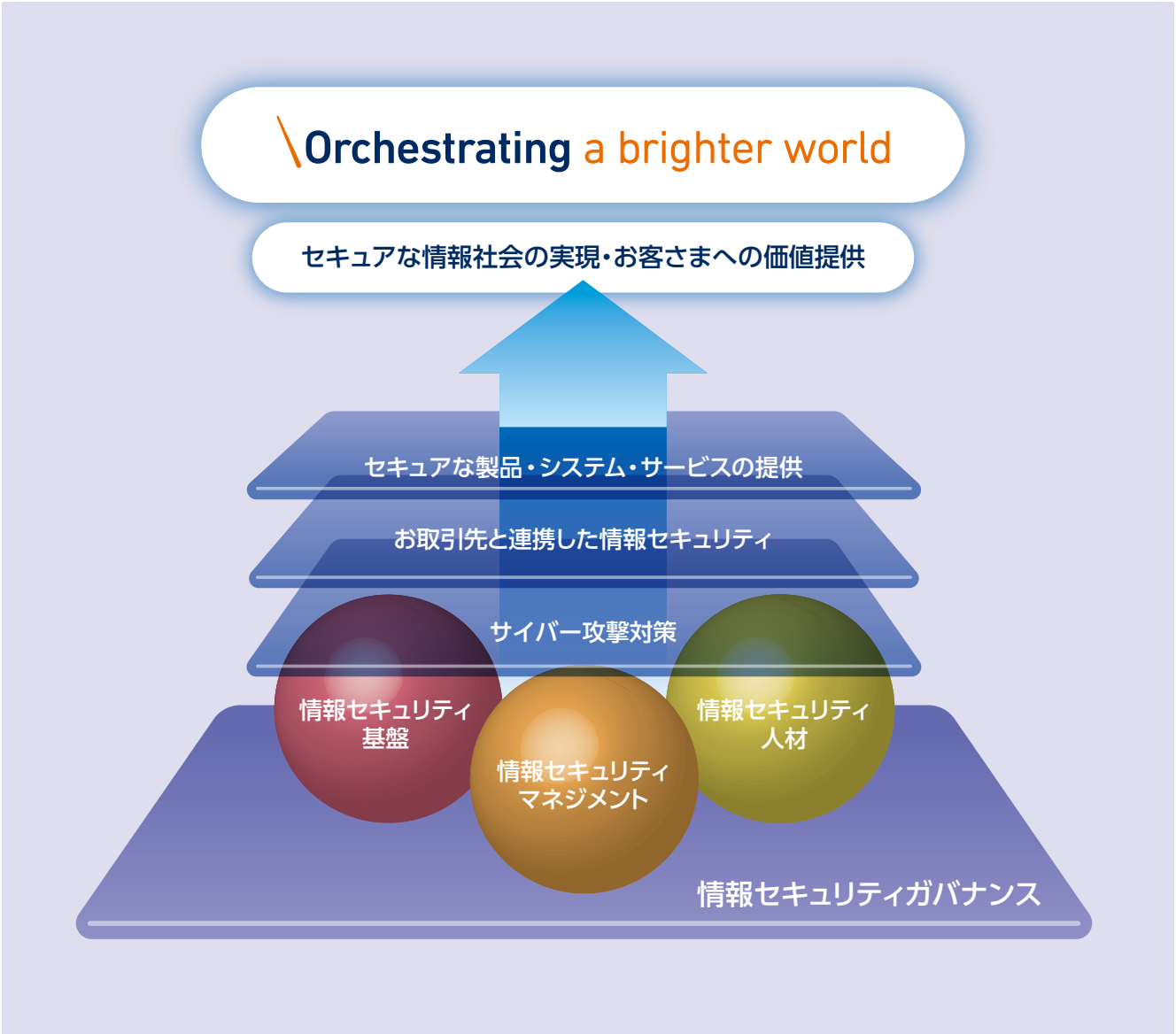
指示1

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

NECグループは、情報セキュリティの確保を経営上の重要事項と位置づけ、お客さまやお取引先さま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・サービスをご提供することで、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グループ内へ情報セキュリティガバナンスの徹底化に取り組み、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うとともに、経営層によるセキュリティ目標の設定、グループ施策、体制構築、経営資産の割り当ての方針を決定し、モニタリングや改善是正などを行っています。



情報セキュリティガバナンス

指示2

事業活動から生じるリスクを的確にコントロールするために、
NECグループ全体で情報セキュリティレベルを効率的に高める情報セキュリティガバナンスを確立しています。

1 NECグループの情報セキュリティガバナンス

NECグループは、情報セキュリティの確保が経営上の最重要課題の一つであると認識し、これに対する投資を企業経営に必要不可欠な責務と位置づけています。グループ全体で「NECグループ経営ポリシー」を定め、各種ルールの共通化と制度・業務プロセス・インフラの統一を行い、グローバルスタンダードな経営基盤を確立しています。また、各海外拠点にRegional CISO*1を設置し、担当領域におけるセキュリティ管理とその結果に責任を持たせることで、ガバナンスを強化しています。

情報セキュリティガバナンスに基づき、経営層はリスクの把握とこれに基づく情報セキュリティ目標の設定、必要な経営資源の割り当てを行うとともに、その取り組み状況に対するモニタリングを行い、改善・是正を継続的に実施します。

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

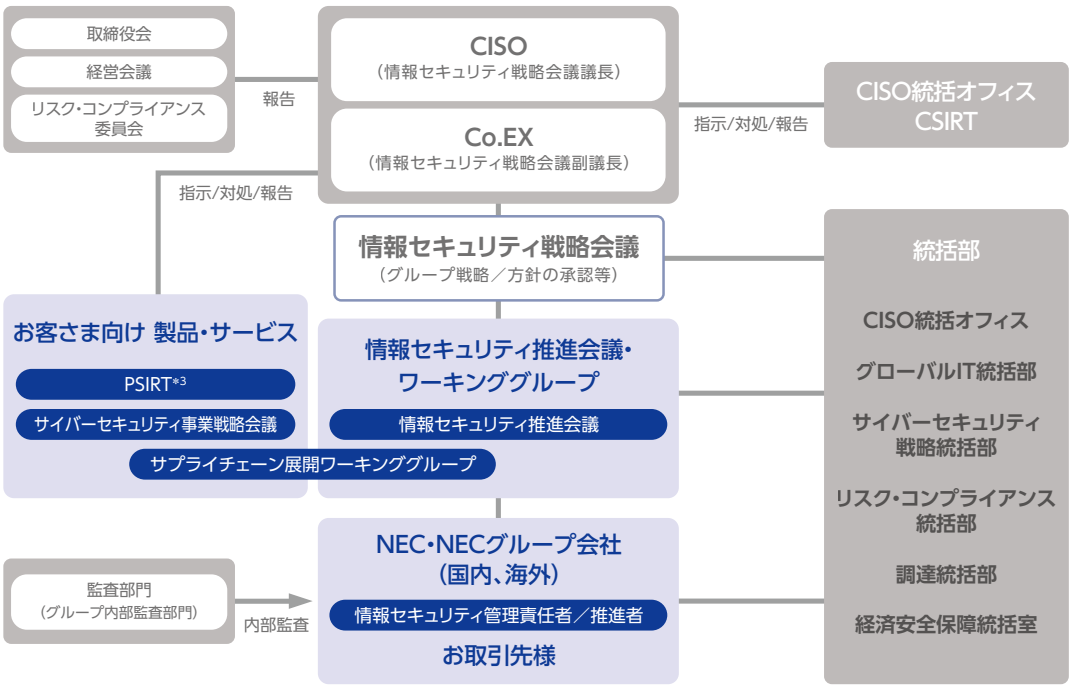
2 NECグループの情報セキュリティ推進体制

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

CISOを補佐するコーポレート・エグゼティブ（Co.EX）は、情報セキュリティ対策を推進するCISO統括オフィスと、サイバー攻撃を監視しインシデント発生時には迅速に収拾をはかるCSIRT*2を統括します。情報セキュリティ推進会議やワーキンググループは、セキュリティ実装の推進計画、実行施策討議・調整、指示事項徹底、施策進捗管理などを行います。

各組織の情報セキュリティ管理責任者は、主管するグループ会社も含め情報セキュリティの確保に責任を負い、組織内へルールの周知徹底、施策の導入・運用、実施状況の点検・見直し・改善などを継続的に実施します。

NECグループ情報セキュリティ推進体制



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

情報セキュリティマネジメント

指示2 指示6

各種施策をNECグループ全体に定着させるため、情報セキュリティマネジメントや
セキュリティポリシーの体系を確立し、その維持・向上の徹底をはかっています。

1 情報セキュリティマネジメントの体系

NECは、情報セキュリティや個人情報保護のポリシーに基づき、PDCAサイクルを継続し情報セキュリティの維持・向上に努めています。情報セキュリティ点検・監査の結果や情報セキュリティ事故の状況などに基づき、実施状況の把握・改善、ポリシーの見直しをしています。また、ISMS認証やプライバシーマーク付与認定の取得・維持も推進しています。

2 情報セキュリティに関するポリシー

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

さらに、個人情報保護については、「NEC個人情報保護方針」*2を制定後、NECは2005年にプライバシーマーク付与認定を取得し、日本工業規格「個人情報保護マネジメントシステム要求事項（JISQ15001）」、「個人情報保護法」に準拠しています。また、2015年には「番号法」準拠のマイナンバー管理を追加しました。2022年に施行された改正個人情報保護法にあわせ、個人情報の保護規程やマニュアル類を見直しています。

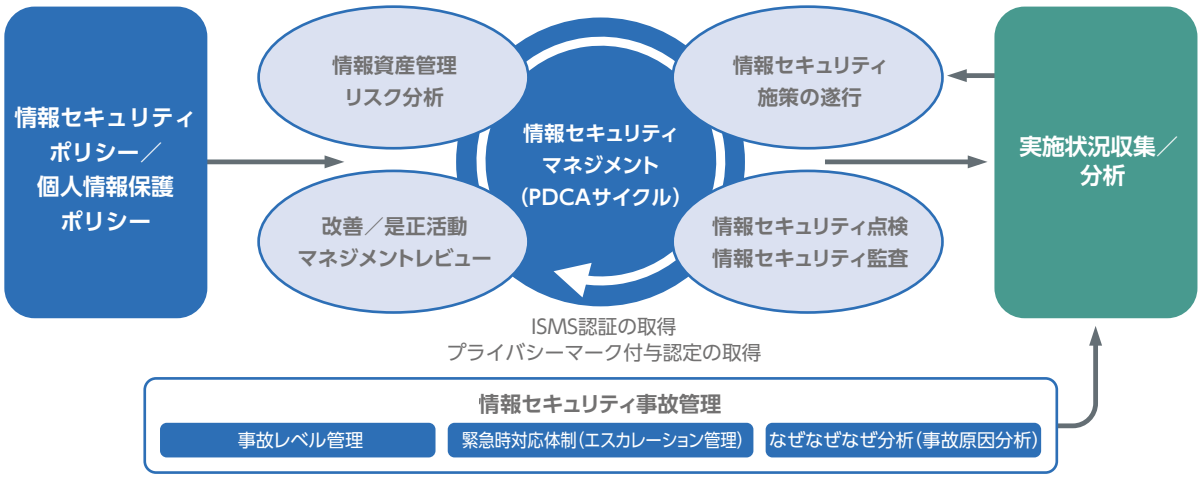
個人情報は、グループ共通の保護管理レベルで運用を推進し、NECグループで31社（2023年6月現在）がプライバシーマーク付与認定を取得しています。

3 情報セキュリティリスク管理

❶ 情報セキュリティのリスク評価

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

NECの情報セキュリティマネジメント



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

❷ 情報セキュリティ事故のリスク管理

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

❸ 事業継続に向けた取り組み

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

4 重要情報管理

❶ Three Lines Model

NECグループではThree Lines Modelに関する情報管理の考え方に沿い、第1ラインである情報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管理支援を行います。さらに第3ラインである監査部門によって、管理状況を確認する仕組みを整えています。

❷ 重要情報の徹底管理

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

5 情報セキュリティ点検・監査

❶ 情報セキュリティ点検

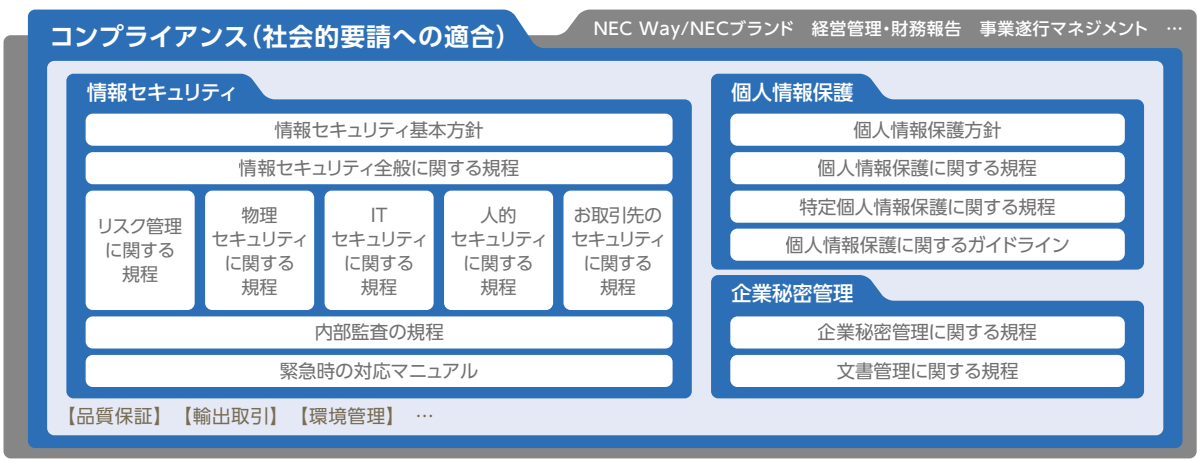
情報セキュリティ事故の分析結果や昨今のサイバー攻撃状況などを考慮して、情報漏えいをなくすための項目を点検の重点項目に設定し、年次で点検を実施しています（2022年度回答率97%）。点検によって各組織の対策実施状況を把握するとともに、重点対策の実施状況を回答することで、個人へ気づきや是正を促します。

実施が不十分な項目は、各組織でその理由を把握して改善します。また、各組織の改善では対応できない課題である場合は、次年度のNECグループの情報セキュリティ推進計画で継続的に課題解決に取り組みます。

❷ 情報セキュリティ監査

監査部門が中心となり、重要情報の取り扱いなどの情報セキュリティマネジメントや個人情報保護に関する監査を年次で実施しています。ISO/IEC27001やJISQ15001に照らし、各組織の状況を監査します。なお、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グループ経営ポリシー



情報セキュリティ基盤

指示3 指示5

NECグループは、ゼロトラスト成熟度モデル（CISA*1）をベンチマークとして「DXを支えるゼロトラストの実現」を目指しています。同モデルはアイデンティティ、デバイス、ネットワーク、アプリケーション、データの5つの柱に沿って実装度合いを表しており、それぞれNECグループでは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

情報セキュリティにおいて、利用者を確実に識別し、認証することは、非常に重要な要素です。これは、情報資産に対する適切なアクセスコントロールやなりすまし防止などのセキュリティ対策を実現する際の根幹となる技術です。識別・認証・認可に用いる情報としては、ユーザIDに加え、組織情報、役職情報などの属性情報があり、個人単位で業務システムなどへのアクセス制御を行っています。

NECでは、利用者の識別・認証、およびアクセス権の付与などの認可に用いる情報をNECグループ全体で管理する認証基盤を構築しており、社員だけでなく、業務内容によっては、お取引先なども含めた形で実現しています。また、これらの情報は、どのシステムでどのような目的で利用されているのかについて一元管理しています。

重要情報を扱うシステムでは、パスワードなどの「知識認証」に加え、電子証明書による「所有物認証」、顔認証などの「生体認証」といった多要素の認証を導入しています。クラウドサービスにおいては、社内の認証基盤と連携したシームレスに認証できる環境を整備しており、業務上のニーズを迅速に満たすとともに、安全・安心に利用できる仕組みを実現しています。

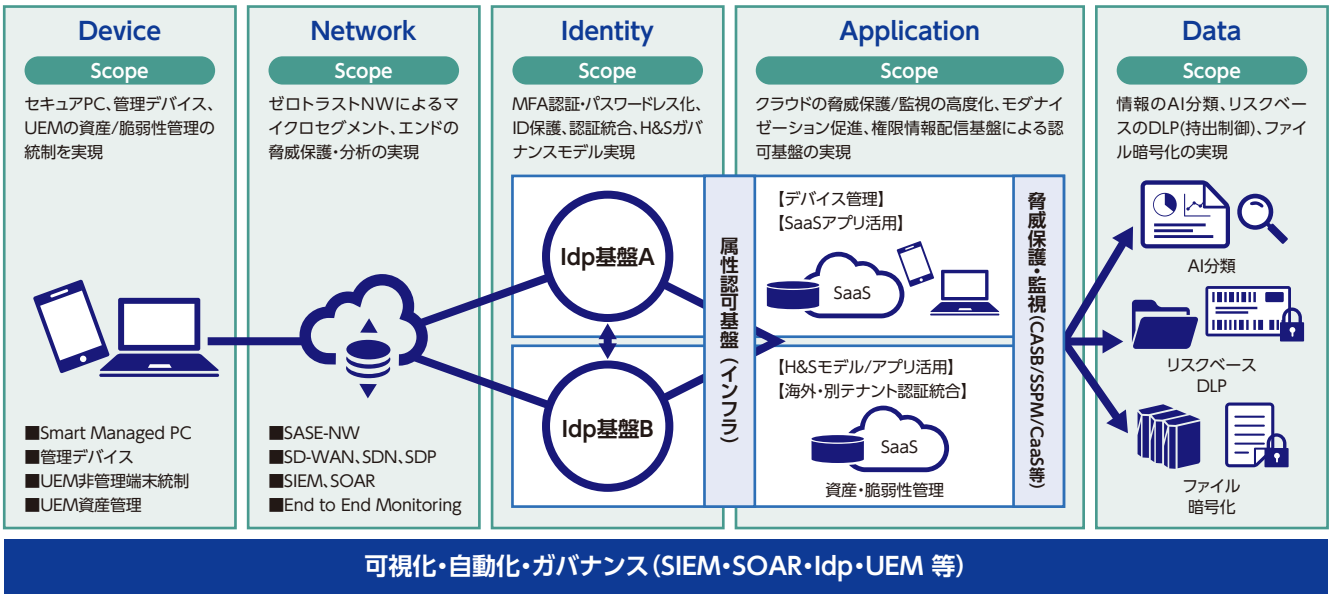
NECでは、認証の強化・高度化として、多要素認証（MFA）の展開拡大、およびセキュリティと利便性を両立させる「パスワードレス認証」を展開しています。

2 デバイスセキュリティ

エンドポイントの端末は、多様な働き方にあわせたラインナップを整備しています。クライアント側にデータを一切保持しないシンクライアントに加え、昨今のリアルとオンラインのハイブリット環境において、使い勝手と安全・安心を両立するリッチクライアントベースのPC（Smart Managed PC：SMPC）も展開しています。SMPCは、顔認証によるセキュアなログイン、占有リソースによる快適な動作環境、アプリケーションやデバイスのセットアップ簡素化などを実現し、業務の利便性や生産性アップだけでなく、従業員のエンゲージメント向上にも寄与しています。

また、セキュアなデバイス環境を実現するために、統合エンドポイント管理基盤（UEM*2）を導入しています。NECグループ全体のレジリエンス強化や、セキュリティ管理業務のコスト削減、社内DXの推進、リスクへの対処力の強化など、NECグループ全

ゼロトラスト基盤の概要とスコープ



*1 CISA: Cybersecurity and Infrastructure Security Agency　*2 UEM: Unified Endpoint Management

体のエンドポイントにおけるセキュリティ向上を目指しています。

情報漏えいリスクへの対応においては、「暗号化」「デバイス制御」「ログの記録」など多面的な対策により、外部からの攻撃や内部不正による情報漏えいなどを未然に防止しています。

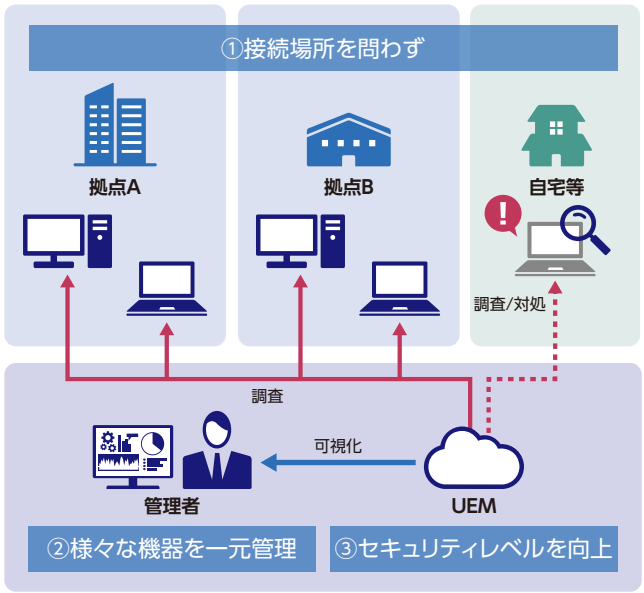
「暗号化」は、ハードウェアレベル、情報レベルの暗号化により、盗難・紛失、メール誤送信などの情報漏えいを防止します。情報レベルの暗号化では、ファイル単位にアクセス権や利用期限を設けたセキュリティ設定ができるようなインフラを整備しています。万が一、マルウェア感染で外部に情報が送られるようなことがあっても、暗号化対策により、情報が保護されます。

「デバイス制御」は、USBメモリやSDカード、CD、DVDなど外部記憶媒体や、スマートフォン、Bluetooth、赤外線などの通信に対して利用制限しており、情報書き出しや情報漏えいにつながる外部デバイスとの通信は原則行えません。業務上、これらデバイスの利用が必要な場合は、組織や利用者ごとにデバイスおよび機能制限を定義し、必要最小限の利用にとどめています。

「ログの記録」は、社内PCの操作ログをすべて記録しています。万が一、情報漏えい事故が発生した場合、ログの分析・解析により、事故の影響範囲の特定、状況把握、再発防止策を立案します。

その他、重点的に管理すべき社内システムを定義し、重要度の高いシステムにおいては、リスク分析や事業インパクト分析を実施の上、脆弱性情報の収集・対処、ログ管理、ネットワーク保護、認証、アクセス制御、特権管理、セキュア運用・保守手順、運用・保守作業チェック、セキュリティ設定、入退室管理、委託先管理など、強度の高いセキュリティ対策を実施しています。

UEMによるセキュアなエンドポイント管理



インフラのセキュリティでは、情報機器、ネットワークを様々なセキュリティの脅威から守る、ICT基盤をグローバルに整備しています。

❶ ユーザ利用環境支援

PCのセキュリティ環境を監視する、管理ソフトウェアの導入を義務化しています。これにより、すべてのPCに必要なセキュリティ対策が実施されているかを可視化しセキュリティリスクを即座に把握します。さらに、セキュリティパッチの配布やウイルス対策ソフトの定義ファイル更新を自動化し、確実に適用する仕組みも導入しています。また、利用禁止のソフトウェアを定義しており、ソフトウェアの適正利用状況についても利用者ごとに監視しています。

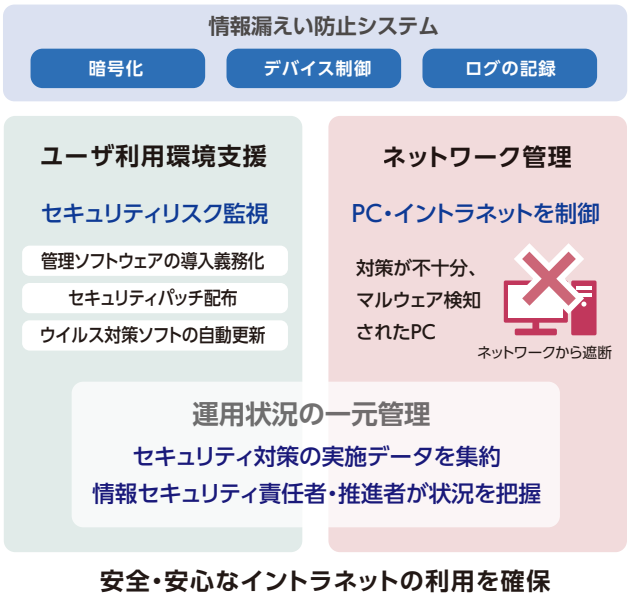
❷ ネットワーク管理

PC状態の見える化に加え、セキュリティ対策が不十分なPCをイントラネット接続から遮断し、マルウェアが検知された場合は、該当するPC・ネットワークをイントラネットから遮断する等の制御を行っています。また、社外への通信は、許可リスト型のWebアクセスフィルタリング、フリーメール対策、送信ドメイン認証などによる制御を実施しています。

❸ 適用状況の一元管理

修正プログラムの適用やウイルス対策ソフトの導入有無など、セキュリティ対策の実施状況に関するデータを集約し、情報セキュリティ責任者や管理者が状況をタイムリーに把握できる仕組みを整えています。これにより、各種施策を迅速・円滑に徹底しています。

外部の攻撃や内部不正からデバイス、ネットワークを守る



安全・安心なイントラネットの利用を確保

3 ネットワークセキュリティ

NECグループでは、システムサービスとユーザのデバイスへ堅牢性と柔軟性を提供するため、ゼロトラスト志向のプラットフォームをグローバルに拡大・展開しています。

SD-WANは、イントラネットワーク内のセグメンテーションとグローバルでの集中制御による「未然防御」・「緊急遮断」・「ログ取得範囲の拡大」を実施することで、セキュリティ強化（被害の局所化・IR迅速化）を実現します。また、ネットワーク変更のリードタイム短縮やインターネットローカルブレイクアウトによるネットワークの最適化、ネットワーク総帯域の倍増を実現するなどセキュリティとユーザの利便性を両立します。

リモート接続環境についてもゼロトラスト指向でグローバルに刷新を行います。クラウド型のRASとProxyとを連携させたアクセス基盤によりSaaS、IaaS、オンプレミスと分散するリソースへの効率的なアクセスを実現するばかりでなく、エンドポイントセキュリティや次世代の認証基盤と連携したゼロトラスト志向でのセキュリティ強化を実現させます。

また、NECはメール成りすまし対策としてDMARCの導入を行っています。

4 アプリケーションセキュリティ

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

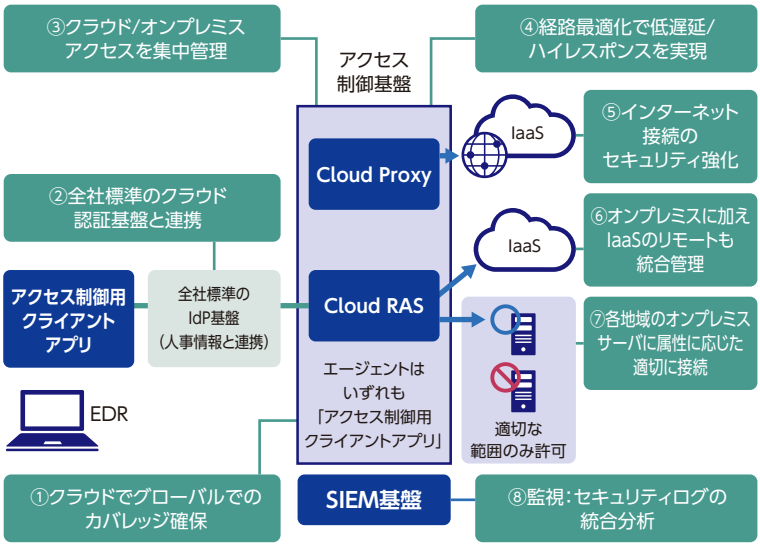
❶ SaaS利用状況の把握

クラウドサービス上のログや保管されているファイルを、CASB*3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。

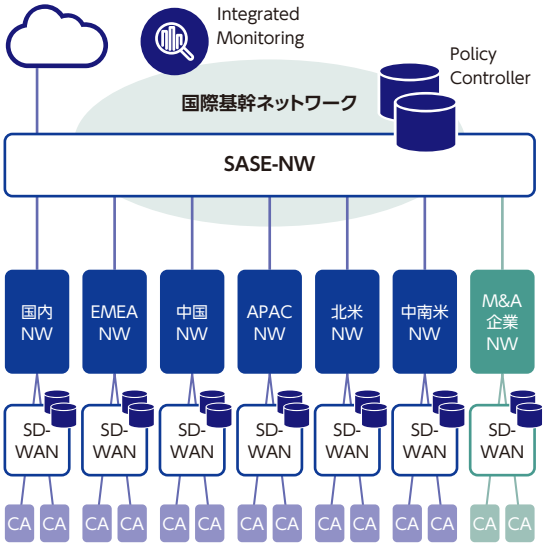
❷ パブリッククラウドの設定ミスに起因するインシデント防止

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ともないます。NECグループでは、CSPM*4を活用して、グループ内で利用され

ゼロトラスト志向のグローバルネットワークセキュリティ



SD-WANのグローバル展開



*3 CASB: Cloud Access Security Broker　*4 CSPM: Cloud Security Posture Management

るパブリッククラウドの設定をセキュリティスタンダードに沿って確認し、リスクの有無を常に確認しています。

❸ SaaSの設定ミスに起因するインシデントの防止

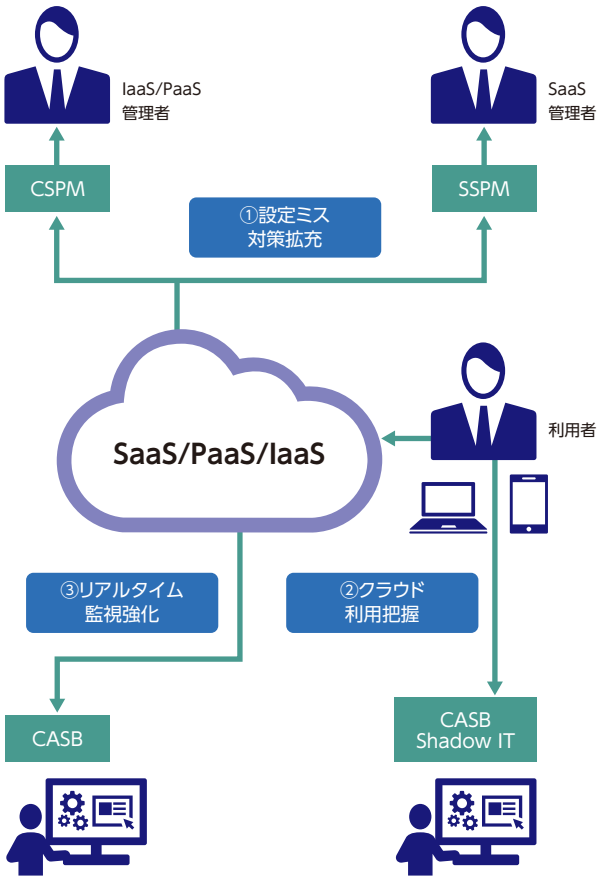
Microsoft365やBOX、Salesforceなどのクラウドサービスは利用時の設定項目が多く、運用する際には設定ミスによる情報漏えいリスクがともないます。NECグループでは、SSPM*5を利用することで、社内で利用するクラウドサービスの設定ミスを可視化・是正する対応をグローバルに実施しています。

5 データセキュリティ

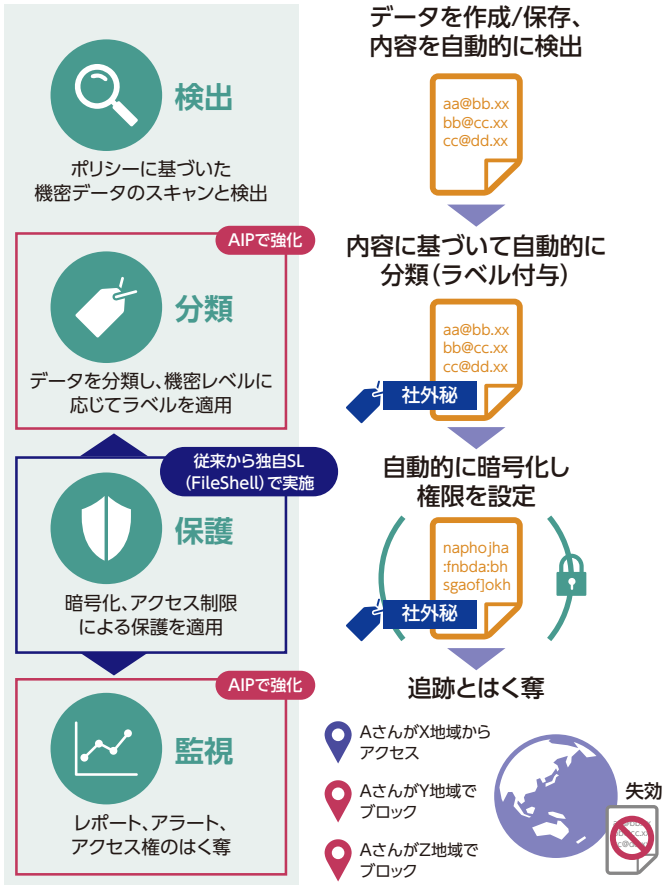
NECグループでは、ゼロトラスト時代のセキュリティを見据え、NEC独自のソリューション「InfoCage FileShell」によるデータ保護を行っています。クラウド環境に対応したAIP*6統合ラベルにより、ファイル単位の自動分類・暗号化や追跡、アクセス権管理などを実施しています。これにより、ゼロトラスト環境における的確なデータ管理を実現しています。

また、情報の管理を徹底するため、重要情報に該当する情報を安全に管理するインフラとして、セキュアストレージを導入しています。重要情報の管理要件であるアクセス制御や暗号化、証跡管理、侵入調査、ISMS管理に対応し、これらの要件に対する業務現場の負荷を低減し、セキュアな情報管理を実現しています。

クラウドサービス利用上のセキュリティ対策



InfoCage FileShell+AIP



*5 SSPM: SaaS Security Posture Management　*6 AIP: Azure Information Protection

情報セキュリティ人材

指示3

社員一人ひとりのセキュリティ意識を高めると同時に、セキュリティスキルの向上や
セキュリティプロ育成の施策を推進し、情報セキュリティに関する豊富な人材を確保しています。

1 情報セキュリティ人材の育成と人材の裾野を広げる活動

NECでは、全社員を対象とした情報セキュリティの「情報セキュリティアウェアネスの向上」、「情報セキュリティ施策を推進する人材の育成」、「セキュリティ・バイ・デザイン(SBD)を実践できる人材の育成」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、情報セキュリティの知識やスキルの向上をはかっています(2022年度修了率97%。海外7カ国語対応)。新しい脅威への対応や情報の取り扱い、テレワークにおけるセキュリティ対策などセキュリティのトレンドを考慮し、教育内容を毎年更新しています。

❷ 情報セキュリティの遵守事項への誓約

お客さま情報や個人情報(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、「お客様対応作業およ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 情報セキュリティの意識啓発活動

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、独自に制作したセキュリティ啓発動画などを活用した意識啓発活動を実施しています。また、テーマ・トークと呼ばれる職場での懇談会などを年間複数回実施して、個人個人のリスクに対する分析力・判断力の向上をはかるとともに、組織の情報セキュリティリスクカルチャーを醸成しています。アンケート結果から、テーマ・トーク実施前後では40ポイントの情報セキュリティ意識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、施策展開の推進者として必要なスキルを備えた専門スタッフを育成しています。推進者には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高い専門性が求められ、CISSP*2や情報処理安全確保支援士(RISS)、個人情報保護士など資格取得者による責任者を配置して、ビジネスユニット(BU)や事業部門ごとに情報セキュリティ推進者を育成し対応力を強化しています。

全社員対象の教育

*1 WBT: Web Based Training　*2 CISSP: 情報セキュリティ・プロフェッショナル認定資格

4 セキュリティ・バイ・デザイン(SBD)を実践できる人材の育成

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

❶ NECサイバーセキュリティ訓練場

お客さまとセキュリティに関する会話をするために必要な知識、適切なリスクアセスメントの手法を、お客さまのシステムにかかわる全社員が学ぶことができる研修として提供しています。また実践的なセキュリティ対策訓練の場として、ECサイトを模した専用の仮想環境を用い、システム構築フェーズでの堅牢化技術を習得できます。リモートで受講可能な演習環境により、営業やSE職を中心に2022年度は延べ1,900名以上が受講し、2019年3月以降延べ6,000名が受講となりました。

❷ 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。2022年度は800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7,200名以上となりました。

❸ 営業・SEセキュリティ基礎教育

営業・SEとして必要な、SBDを核とするセキュリティの基礎知識をe-learning形式で展開し、2022年度は延べ35,000人以上が受講しました。これにより、NECグループ全体のセキュリティ実装力の底上げをはかっています。

❹ SBDスペシャリスト研修

各事業部門で、セキュリティ責任者を補佐し、SBDを実践する専門人材の育成を2019年度より行っています。また2021年度からは、営業職向けコースを新設し、インシデント事例や対策のためのオファリングなど、適切なセキュリティ提案に必要なスキル習得も進めています。本研修は、2022年度までに累計55名以上が受講しました。本スペシャリストを中心に、システム開発に関わる全プロセスを俯瞰し、抜け漏れなく適切なセキュリティを実装することで、安全・安心なシステムをお客さまにお届けします。

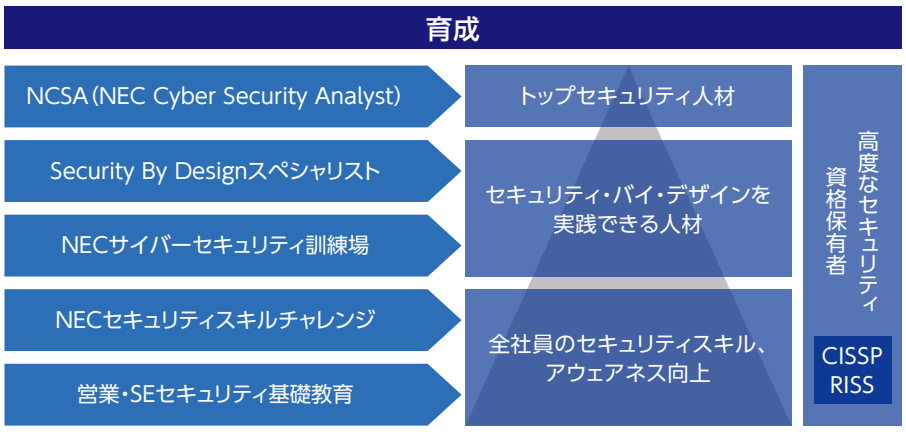
❺ NCSA(NEC Cyber Security Analyst)トレーニング

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*4業務やリスクハンティングなど高度なセキュリティサービスに必要な実践的テクニカルスキルを、半年間の集中プログラムで習得します。2019年度まで実施したNCAT(NEC CISO補佐官トレーニング)とあわせ延べ65名以上が受講し、プロフェッショナルサービスの提供に携わっています。

❻ 高度なセキュリティ技術資格保有者

お客さまへの最適なソリューションを提供するための情報セキュリティに関する高度なスキルの証明として、営業やSEなど、お客さま対応を行う社員にセキュリティ公的資格の取得を推奨しています。社内セミナーや勉強会などにより、国際資格であるCISSPや情報処理安全確保支援士(RISS)の取得者を拡充しています。特にCISSPについては、高度な技術的スキルを持つだけでなく、ビジネス観点でリスクを評価できる人材を育成するため、認定機関である(ISC)2と戦略的提携を締結して取得を促進しています。NECグループのCISSP保有者は、2021年度から約100名増となり、累計300名を超えました。

セキュリティ・バイ・デザイン(SBD)を実践できる人材育成



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

サイバー攻撃対策

指示4 指示5 指示7 指示8 指示10

サイバー攻撃が高度化・巧妙化する中、先進的な対策をグローバルで実施するとともに、
CSIRTによるインシデント対応を行い、サイバーセキュリティ経営を実現しています。

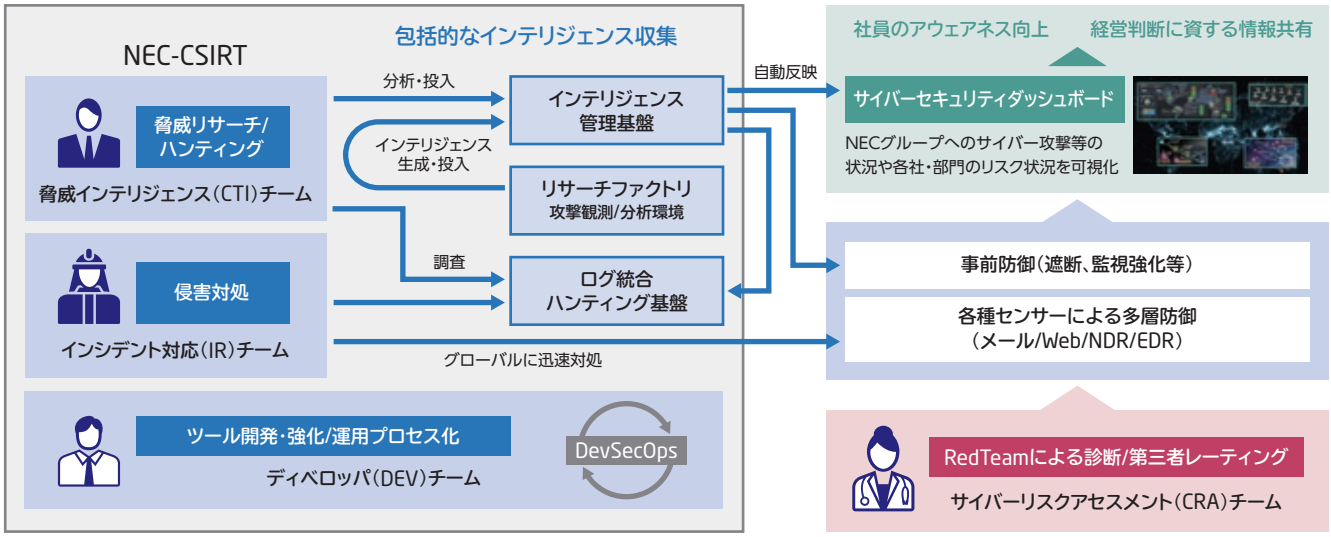
1 グローバルサイバー攻撃対策

サイバーセキュリティリスク分析に基づく先進的な対策を国内外で統一的に行うとともに、CSIRT*1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、NIST CSF*2に基づく第三者による評価を行い、対策を強化しています。

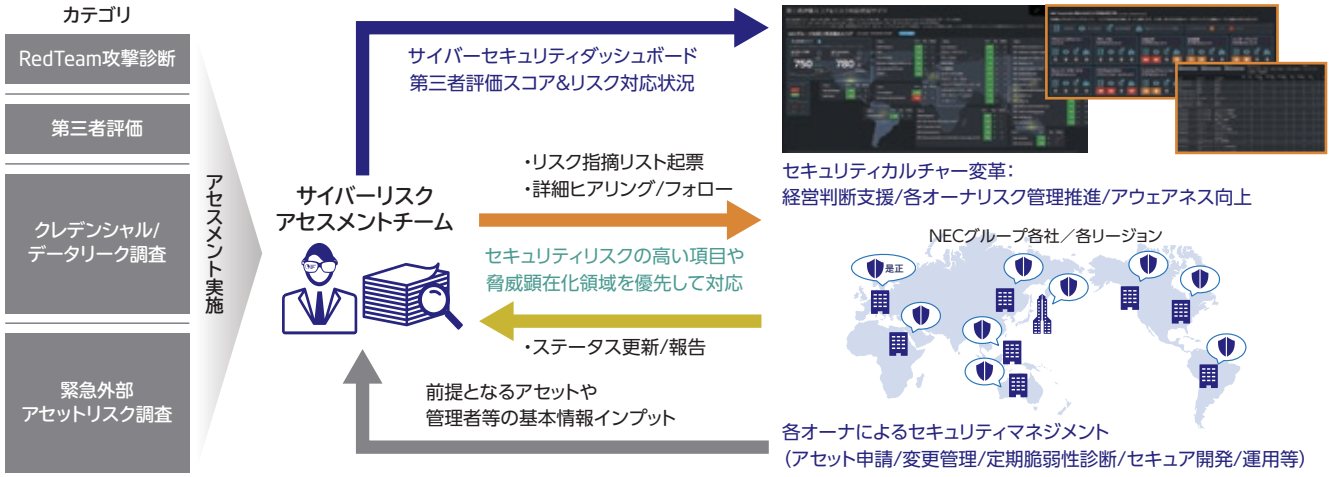
具体的には、サイバーセキュリティリスクに対して、グローバルに統一されたアプローチを取ることが、事業継続のためには重要であるという考えのもと、AI等を活用し、日々のサイバー攻撃の監視や状況の把握、分析を行うとともに、それに伴い監視運用プロセスの見直しを行っています。また、対策製品、サービス、市場動向を把握し、PoC*3評価や社内IT環境調査により、対象製品・サービスの社内IT環境への適合性を検討します。これらの結果から、今後必要となる対策を検討し、その対策の対象範囲、効果やコストを算出します。そして、上記の活動に基づいた推進計画を毎年立案し、CISO*4の承認のもと対策を実施します。

NECグループでは、多層防御の考え方に基づき、巧妙化するサイバー攻撃への対策を実施しており、特に①Red Team*5によるサイバーリスクアセスメント、②脅威インテリジェンス生成・活用、③CSIRT体制強化、④組織的なセキュリティレジリエンス強化に注力しています。

サイバーセキュリティ対策の全体像



サイバーリスクアセスメント



*1 CSIRT: Computer Security Incident Response Team
*2 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
*3 PoC: Proof of Concept 新しい概念の実証実験　*4 CISO: Chief Information Security Officer
*5 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
*6 NDR: Network Detection and Response　*7 EDR: Endpoint Detection and Response

❶ Red Teamによるサイバーリスクアセスメント

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

監査法人およ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洩などの調査、BitSight等の第三者評価を通じてグローバルにアセスメントを行い、既存のセキュリティ対策／運用における抜け漏れを洗い出し、サーバの管理者や海外現地法人などの責任者と連携して改善策を実施します。

❷ 脅威インテリジェンス生成・活用

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

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

❸ CSIRT体制強化

CISO配下にCSIRTを設置し、サイバー攻撃を監視して攻撃やマルウェアの特徴を分析し、関係機関とも情報を共有しています。インシデント発生時には保全や攻撃の解析を実施し、原因究明や事態の収束を行います。

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

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

❹ 組織的なセキュリティレジリエンス強化

ランサムウェア等の世界的な脅威に備え、社員に対しては標的型攻撃メール訓練を行うとともに、インシデントが発生した場合、迅速に対応できるよう、マニュアルを整備しています。また、有事に備えた関係部門や専門家による演習を、半年に1回以上実施しています。

2 サイバーセキュリティダッシュボードによるセキュリティ―カルチャー変革

NECグループへのサイバー攻撃の状況や、CTIチームが収集した脅威インテリジェンス情報、サイバーリスクアセスメントで判明した、各社・各部門のセキュリティリスク状況を可視化した、サイバーセキュリティダッシュボードをリリースし、全社員に公開しています。社員一人ひとりがリアルな状況を知り、リスクを実感することで、セキュリティアウェアネスの向上につなげることができます。また、経営幹部の会議や全海外現地法人が参加する会議の中でダッシュボードを使い、各組織のリスク対応状況を見ながら、リスクが高く脅威が顕在化している組織をその場で特定し、改善の指示を出すなど、スピーディな経営判断、各セキュリティ責任者への管理推進に役立てています。

サイバーセキュリティダッシュボード

*8 CTI: Cyber Threat Intelligence

お取引先と連携した情報セキュリティ

指示9

NECではお客さま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。そして、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）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、「お客さま対応作業における遵守事項」として定め、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）の導入を依頼しています。

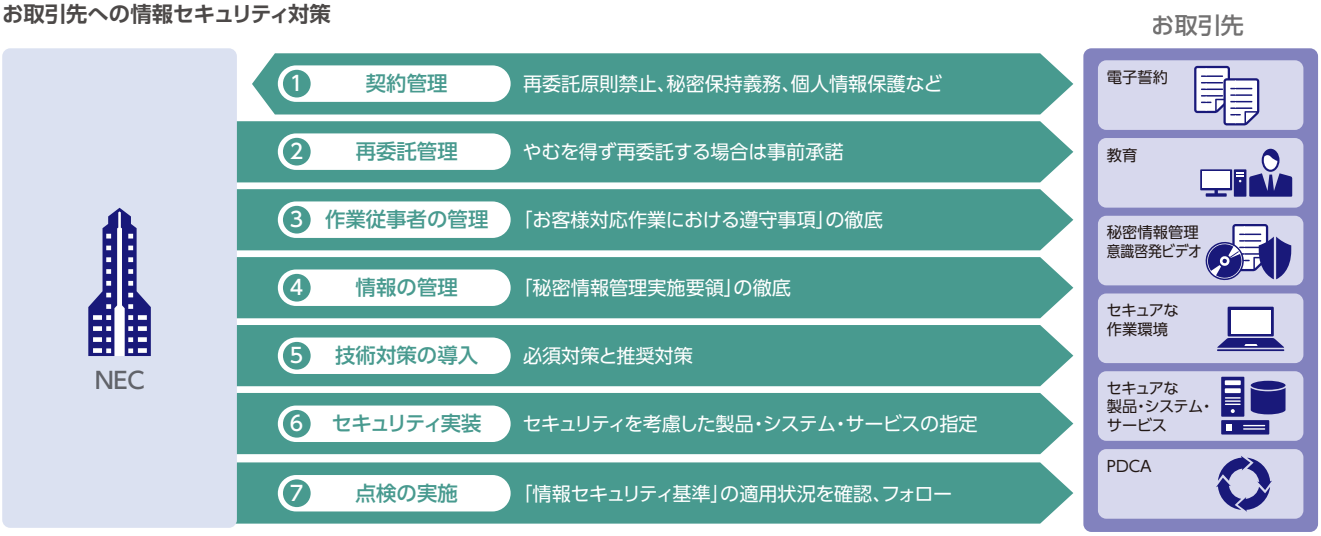
❻ セキュリティ実装

お客さま向けの製品・システム・サービスの開発・運用について実施要領を定め、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の備えたものへ改訂を行い、さらにお取引先様と連携した活動を強化しています。

お取引先への情報セキュリティ対策



2 お取引先への対策浸透活動

❶ 情報セキュリティ説明会

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

❷ 重点お取引先のレベルアップ活動

NECとの取引が特に多い、重点お取引先（ソフトウェア関連の約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。

❸ 対策ガイドの配付

お取引先が情報セキュリティ対策をより円滑に実施できるよう、対策の実施ガイドを提供しています。これまで要求水準達成のための各種ガイド、ウイルス対策ガイド、開発環境セキュリティ対策ガイドなどを発行しています。

❹ 委託先管理プロセスの標準化

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

3 お取引先に対する点検および是正活動

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

❶ 書類点検／訪問点検

NECと取引のある会社、約1,800社を選んで書類点検を実施しています。お取引先は自社の対策状況を自ら点検し、点検結果はWebシステムによってリアルタイムでフィードバックを行っています。また、取引が多いお取引先には直接訪問、あるいはリモートを活用した訪問点検を実施しています。毎年訪問社数を増やしており（2022年度は約200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、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をベースとした情報セキュリティ基準に2022年4月に改訂しました。また、第三者評価サービス（BitSight）を活用して、重点お取引先様のセキュリティ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、海外現地法人向けに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、委託先情報セキュリティ管理の意識啓発に努めています。引き続きグローバルサプライチェーン全体のセキュリティレベルの向上を図るべく今後も継続して開催していきます。

セキュアな製品・システム・サービスの提供

指示2 指示4

お客さまへ「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

お客さまに提供する製品・システム・サービスをセキュアに開発・運用するために、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。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」に定めており、その内容を強化することでサイバーセキュリティリスクの高まりに対応しています。

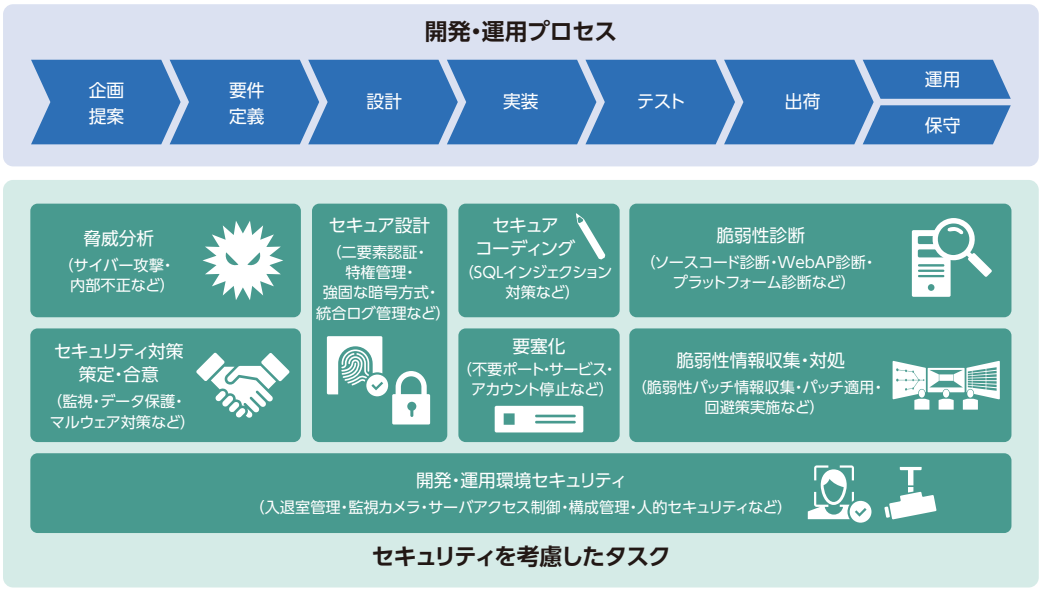
また、近年、ビジネスパートナーや委託先といったお取引先がサイバー攻撃を受け、お取引先に提供した重要情報の流出や製品等の生産・供給の遅延が発生する事件も増加しています。NECはこのような攻撃によるリスクに対応するため、お取引先も含めたセキュリティ対策の見直しと強化を図り、お客さまへの製品・システム・サービスの供給を継続できるようにしています。2022年度は前年度の「お取引先様向け情報セキュリティ基準」の改訂に基づき、お取引先のセキュリティ管理体制や対策状況を確認することによりさらなる対策の強化を推進しました。

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「セキュリティ・バイ・デザイン（SBD）」の思想に基づき、企画・提案フェーズから実装フェーズ、運用・保守フェーズまでを含めたセキュリティ実装を行っています。システム開発の早い段階でセキュリティを確保することは、コストの削減や納期遵守、保守性に優れたシステム開発などさまざまなメリットに直結します。特に、お客さま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、提案・実装時に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

セキュリティ実装プロセス



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。

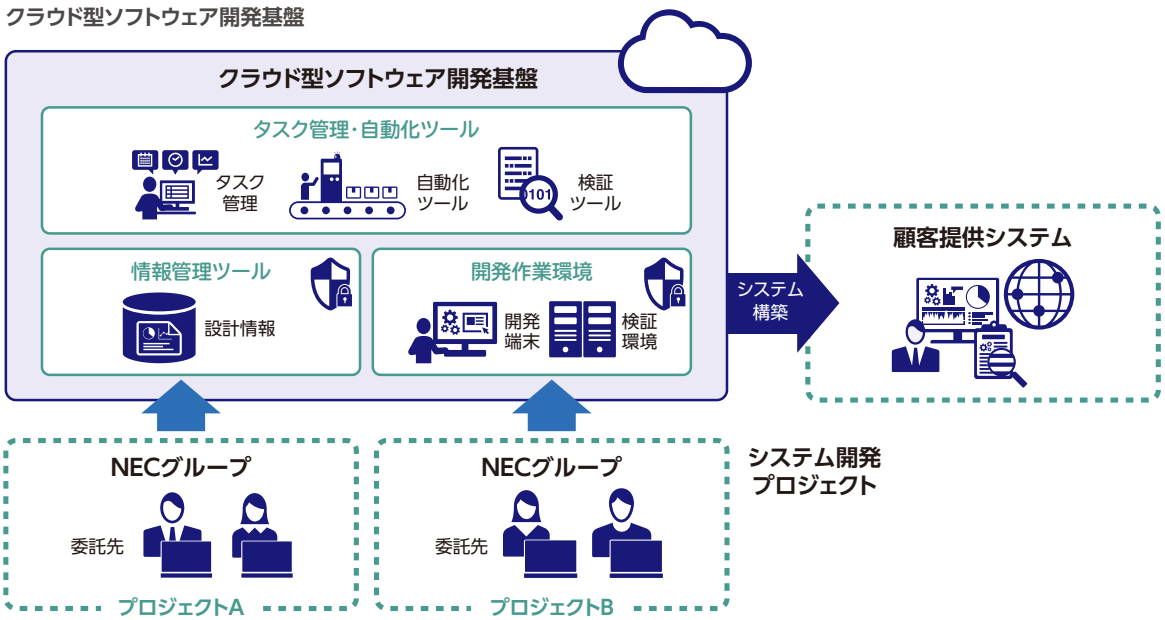
製品・システム・サービスの開発では、各フェーズでセキュリティタスクが実施されていることを確認するために、チェックリストを作成し活用しています。本チェックリストに基づき、セキュリティタスクの実施状況を可視化するために開発された「セキュリティ実装点検システム」により業務プロジェクトが管理され、セキュリティ対策状況の効率的な点検・監査が実施されています。

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」と「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。サイバーインテリジェンス共有基盤では、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、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。サイバーセキュリティインテリジェンスを各事業部門にタイムリーに展開していくことで、最新の脅威に備えたセキュリティ対策を徹底し、各製品・システム・サービスの運用・保守段階においても、インシデント影響の少ない安全なビジネス環境の構築を実現しています。また、NECではPSIRT機能を保有し、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、脆弱性へ対策しています。

❸ セキュリティ実装のためのソフトウェア開発基盤

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

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



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

NECのサイバーセキュリティ戦略

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

1 基本方針

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

昨今のDX*1の促進により、テレワークの活用が増加するなど人々の働き方が大きく変化する状況の中で、フィジカル空間（現実空間）とサイバー空間が高度に融合し、あらゆるモノ同士がつながるようになってきています。このような世界では、あらゆる場所にセキュリティリスクが存在する可能性があり、かつ新たに発生するセキュリティリスクへ対応が求められます。事業環境の激しい変化に対応しながら安全に事業を遂行するためには、これまで以上にサイバーセキュリティは重要な課題となっています。

NECは、国内の交通管制をはじめ防災・消防システム、生産管理から水管理、ATM、物流システム、さらには海底から宇宙まで、社会にとって必要不可欠な基盤を支え続けてきた多くの技術を蓄積・活用することで、フィジカルとサイバーを融合したトータルセキュリティを世界に向けて展開しています。また新たなサイバーリスクに対応するため、「攻撃からまもる」に加え「正しくつくる」「正常をつづける」ことを重視し、セキュリティを後付けするのではなく、設計段階から構築、運用に至るすべてのフェーズでのセキュリティ実装を、実施体制も含めて推進しています。

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

社会基盤を支えるNECの事業領域

*1 DX: Digital Transformation

2 社会への貢献

❶ 関係組織との連携

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

従来より日本サイバー犯罪対策センター(JC3*2)に参画し、国内の学術研究機関、産業界、法執行機関の官民産学連携を推進、サイバー犯罪への対応を進めています。またICT-ISACへの参画やCyber Threat Alliance(CTA)への加盟など、サイバー攻撃の脅威情報の活用を推進しています。

さらに2021年にはサイバーリスク対応のための組織フレームワークに関する国際標準化に取り組み、その結果はITU-T勧告として発行されました。これらの活動で得た成果を社会に還元させることで、安全・安心で快適な環境づくりに貢献しています。

❷ 国の活動への貢献

特別顧問である遠藤信博が、サイバーセキュリティ戦略本部(内閣)の委員、産業サイバーセキュリティセンター(IPA*3)のセンター長やサプライチェーン・サイバーセキュリティ・コンソーシアム(SC3)の会長を務めており、また執行役 Corporate SEVP 兼 Co-COO(チーフオペレーティングオフィサー)である堺和宏が一般財団法人 日本サイバー犯罪対策センター(JC3)の代表理事を務めています。このように、NECは国家的なセキュリティプロジェクトへ積極的に貢献しています。また、経団連やSC3、JDTF*4などの業界団体を通じて省庁へ提言することでも、官民一体となった安全・安心な社会づくりに貢献しています。

関係組織との連携

組織加盟

日本サイバー犯罪対策センター(JC3)参画 (2014年11月)
産学官(警察)それぞれがもつサイバー空間の脅威への対処経験を集約・分析・共有。脅威の大本を特定・軽減・無効化することを目指す。執行役 Corporate SEVP 兼Co-COO(チーフオペレーティングオフィサー)の堺 和宏が代表理事を務める。

ICT-ISACへ参画 (2017年3月)
通信事業者、放送事業者、ソフトウェアベンダー、情報提供サービス事業者、情報関連機器製造事業者など多様な事業者がサイバー攻撃などに関して情報共有し、業界の枠を超えて連携・協調し、脅威に対処するために発足したICT-ISACへ参画。NECは前身となるTelecom-ISACから参画。

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

セキュリティ企業間での情報共有CTA加盟 (2018年10月)
セキュリティ企業間でサイバー攻撃の脅威情報を共有する米国の非営利団体「Cyber Treat Alliance (CTA)」へ加盟。加盟から現在まで、CTAへの脅威情報提供を継続。

組織間連携

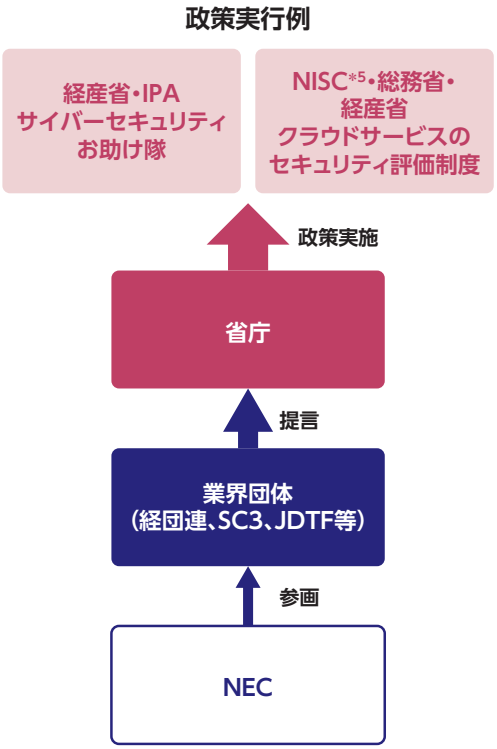
インターポールとサイバーセキュリティ対策で提携 (2012年10月)(2017年3月)(2022年10月)
国際レベルでのセキュリティ強化を目指して、複雑で高度化するサイバー犯罪などを調査・分析する、グローバルなサイバーセキュリティ対策で提携。2017年からは国際刑事警察機構主催のサイバー犯罪捜査演習「Digital Security Challenge」において、演習シナリオ作成や解析対象データの開発等を支援し、本演習開催に貢献。2022年10月の第5回演習開催にも協力。

情報通信インフラにおけるサプライチェーンセキュリティリスクへの対策技術を開発 (2021年10月)(2022年11月)
情報通信インフラシステムのセキュリティに関する透明性確保によりサプライチェーンセキュリティリスクの抜本的低減を図るため、日本電信電話株式会社と「セキュリティトランスペアレンシー確保技術」を開発。2022年11月からフィールド実証開始。

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

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

業界団体を通じた政策提言



*2 JC3: Japan Cybercrime Control Center *3 IPA(Information-technology Promotion Agency, Japan):独立行政法人情報処理推進機構
*4 JDTF(Japan Digital Trust Forum):一般社団法人デジタルトラスト協議会 *5 NISC(National center of Incident readiness and Strategy for Cybersecurity):内閣サイバーセキュリティセンター

3 世界トップレベルの人材と技術

❶ 高度なサービス提供のための体制

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

❷ 社内人材育成

NECグループは、セキュリティ人材育成に向けた取り組みにも力を入れており（詳細はP12の「情報セキュリティ人材」を参照）、セキュリティ技術を競うコンテストの世界大会で上位入賞を果たした社員も在籍しています。

❸ 国内セキュリティ人材育成

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

なお、企業で実際に活用されている教材や演習環境を用いた人材育成は、高専機構において初めての取り組みとなります。

❹ お客さまへの教育プログラム提供

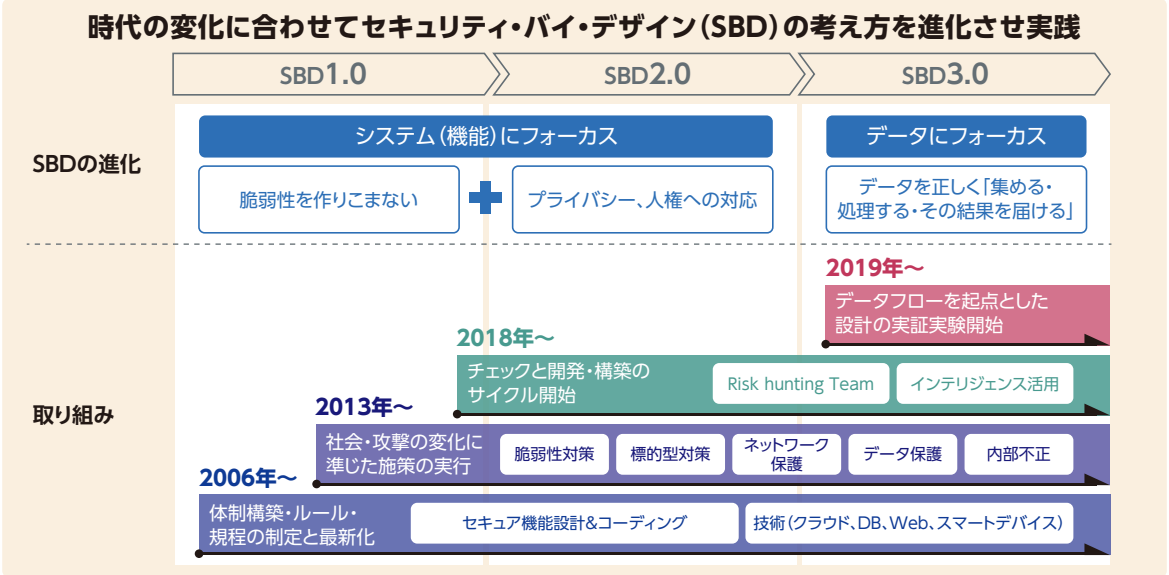
NECは、NECアカデミー for DXとして、経済産業省と独立行政法人情報処理推進機構(IPA)が2022年12月公開の「デジタルスキル標準」に対応したDX推進人材育成プログラムを提供しています。

本プログラムでは、サイバーセキュリティリスクの影響を抑制

NEC執行役員常務兼CIO兼CISO（当時）小玉浩の講演

NEC社員による出前授業

SBD3.0によるセキュリティ実装の考え方



して顧客価値の高いビジネスの安定的な提供を担う推進人材の育成を目的としたプログラムや、具体的なサイバーセキュリティリスク対策を担う専門人材の育成を目的としたプログラムを提供しています。

4 セキュリティ実装の徹底

NECは、お客さまへ安全・安心な製品・システム・サービスを提供するために、セキュリティ実装を推進する体制を構築しています。また、サプライチェーンに対するサイバー攻撃によるリスクへ対応するため、NECでは前年度に改訂したお取引先向けのセキュリティ基準に基づくお取引先のセキュリティ管理体制や対策状況を確認し、お客様への製品・システム・サービスの供給を継続できるようにしています（詳細はP18の「セキュアな製品・システム・サービスの提供」を参照）。

また、DXの加速によりデータ、システムなどが複雑に絡み合う環境のセキュリティを確保するために、NECはデータを中心としたセキュリティ実装の考え方としてセキュリティ・バイ・デザイン（SBD）3.0を掲げ、いち早く最新の脅威に対応できるセキュリティの実現を目指しています。

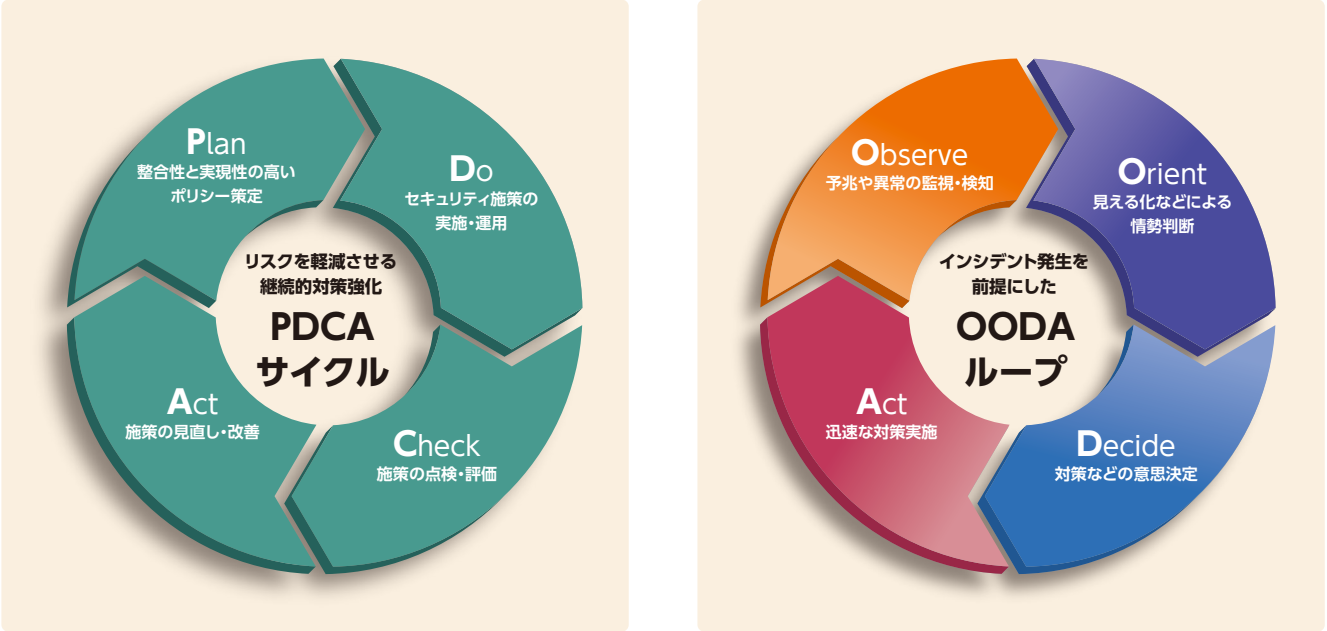
■ DX時代におけるサイバーセキュリティ（NEC）
https://jpn.nec.com/cybersecurity/nec_cybersecuritywhitepaper202004.pdf

5 自社運用ノウハウをもとにセキュリティ強化をサポート

サイバーセキュリティ対策は、製品やサービスを導入すれば終わりではありません。高度化・巧妙化が進むサイバー攻撃に対抗するには、サイバーセキュリティ対策を適切に運用し、正しい状態を維持しつづけることが重要です。このためには、サイバーセキュリティのポリシー策定から対策、効果の点検、改善というPDCAサイクルを実現し、脆弱性を解消する継続的な対応が欠かせません。また、不正侵入やマルウェア感染など、インシデントが発生した場合に備えることも重要です。

NECでは、グローバルに展開するNECグループの社員約11万人が利用するシステムでの運用実績に基づき、運用時に活用できるサイバーセキュリティ対策も提供します。また、監視・検知・情勢判断・意思決定・対策実施の流れによる、「OODA（ウゥーダ）ループ」という概念を取り入れており、適切でスピーディなインシデント対応をサポートします。

PDCAサイクルによる継続的なセキュリティ対策および「OODAループ」によるスピーディなインシデント対応



DXによる新たなセキュリティリスクへの対応

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

1 DXによるリスクの変化

❶ セキュリティリスクの変化

地政学的な状況の変化とともに民間企業も国家的なサイバー攻撃の標的になっており、先端技術情報等を保有する企業はセキュリティリスクが増大しています。また、DXが急速に進む一方で経済目的のサイバー攻撃が激化し、あらゆるシステムやデータが標的となり企業の事業継続が脅かされています。DXによりシステム間連携が進み、被害は1つの組織にとどまらないことも最近のセキュリティリスクの傾向として挙げられます。このような状況の中、経済安全保障リスクに対応するために可決した「経済安全保障推進法」には、サイバー攻撃への対応についても言及されています。また、NISCが発行する「重要インフラのサイバーセキュリティに係る行動計画」では、基幹インフラを支える重要設備の安全性確保の義務化や、サイバーセキュリティ体制が適切でないことにより会社に損害が発生した場合の経営層の損害賠償責任にも言及されています。

❷ クラウド環境におけるセキュリティリスク

守るべき情報がオンプレミスからクラウド上へ移行したことや、社外からのリモート接続が増加したことなどの理由により、従来のネットワーク境界中心の対策は限界を迎えつつあります。また、データが随所に分散し、場合によってはクラウド上のデータが正しく運用されない恐れもあります。したがって、技術的な安全性だけでなく利用者の安心を考慮したデータガバナンスと、データ重要度・機密性を考慮したクラウドサービスを選定することが重要です。

2 アーキテクチャーとともに変化するセキュリティ

❶ DXを支えるトラストなサイバー空間のあり方

「脅威は外側から来るもので守るべき情報資産は境界内部にある」という従来のペリメタモデルは、クローズドな世界においては安全であるという考え方でした。しかし、DXの世界では脅威はあらゆる場所にあり、すべてのITの衛生管理を徹底する必要があるため、セキュリティは、“ゼロトラスト”と、“サイバーハイジーン（公衆衛生）”の考え方が重要になります。

❷ 全体最適化への対応

セキュリティ対策が部分最適化されてしまっていることや、そのことに気づいていないことも問題として挙げられます。例えば、個々のセキュリティ対策の結果を見ただけでは、何が起きて

セキュリティリスクの変化

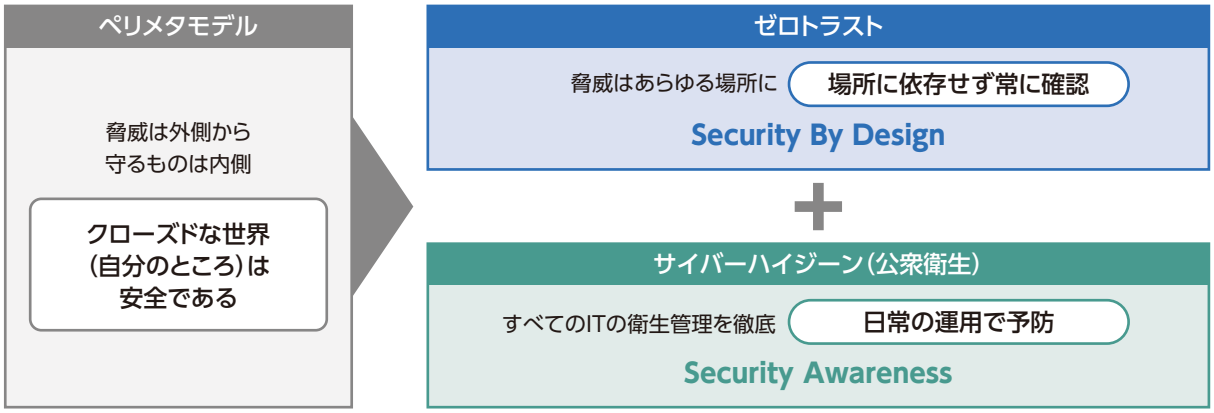
いるかが分かりづらく、顕在化させるべきリスクが潜在化してしまいがちです。新たに対策を追加した部分だけを見れば最適かもしれませんが、企業全体で見ると対策に漏れやダブりが生じ、それが、さまざまな経営・投資判断・ガバナンス上の問題につながっている可能性があります。NECでは、部分最適を改めて全体最適化を図っていくことが、現在のセキュリティにおける重要なテーマと考えています。

3 安全にDXを進めるためにご支援できること

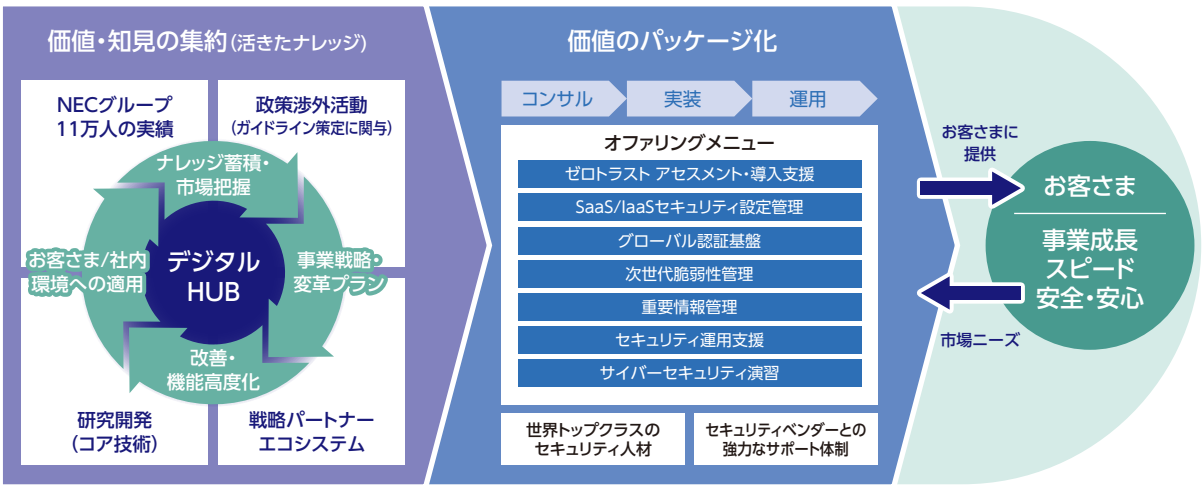
❶ 社内で培ったノウハウのソリューション化

NECには研究開発と戦略パートナー連携により、NECグループ11万人のセキュリティ対策実績に裏付けられた価値と知見が“生きたナレッジ”として集約・蓄積されております。そしてNECは「ゼロトラスト アセスメント・導入支援」「重要情報管理」「セキュリティ運用支援」など、テーマや直面している課題ごとにコンサルティングから実装、運用までをトータルにサポートする「オファリングメニュー」を提供しています。これらは、すべてNEC自身が取り組んできたセキュリティ強化施策、そしてお客さま支援の経験から価値を抽出し、パッケージ化したものです。現場で磨かれ、確立された方法論やノウハウを活かして、極めて実践的なサポートを実現しています。

DXを支えるセキュリティベース



安全にDXを推進するためのオファリングを提供



*オファリングメニューにはオファリング化予定のものを含む

❷ DX/クラウドシフトに求められるセキュリティソリューション

DX/クラウドシフトによるセキュリティ課題と今後対策すべきポイントは、次の4点と考えています。

課題	対策すべきポイント	ソリューション例
ID管理: ゼロトラスト	・利用するクラウドサービスのID管理の実態を把握して、ユーザ、アプリケーション、デバイスなどを識別 ・シームレスかつセキュアなサービス実現のため、オンプレミスとクラウドサービスのIDの統合管理を実施	・SSO ・多要素認証 ・コンテキストベース認証
情報管理: 重要情報管理・データガバナンス	・機密レベルに応じた情報のラベリングと、暗号化対策等の多層防御による重要情報を保護 ・重要情報管理ルールの策定および体制構築	・AIP統合ラベル ・InfoCage FileShell
設定管理: サイバーハイジーン	・クラウド設定監査ツールを活用し、クラウドの設定不備などを継続的に可視化し自動で是正	・CSPM*2 ・SSPM*3
運用管理: Security Operation By Design	・設計段階からセキュリティ監視まで意識するために、セキュリティ運用のライフサイクルを見据えたSOBD*1を実施	・プロフェッショナルサービス

❸ プロフェッショナルサービス

NECは、上流工程からお客様の計画策定や技術面でのアドバイザリーを実施しています。また、新たな脅威や課題をお客様と共有し、その対策や改善の継続的なご提案を通じて高品質なセキュリティ運用監視を実現しています。

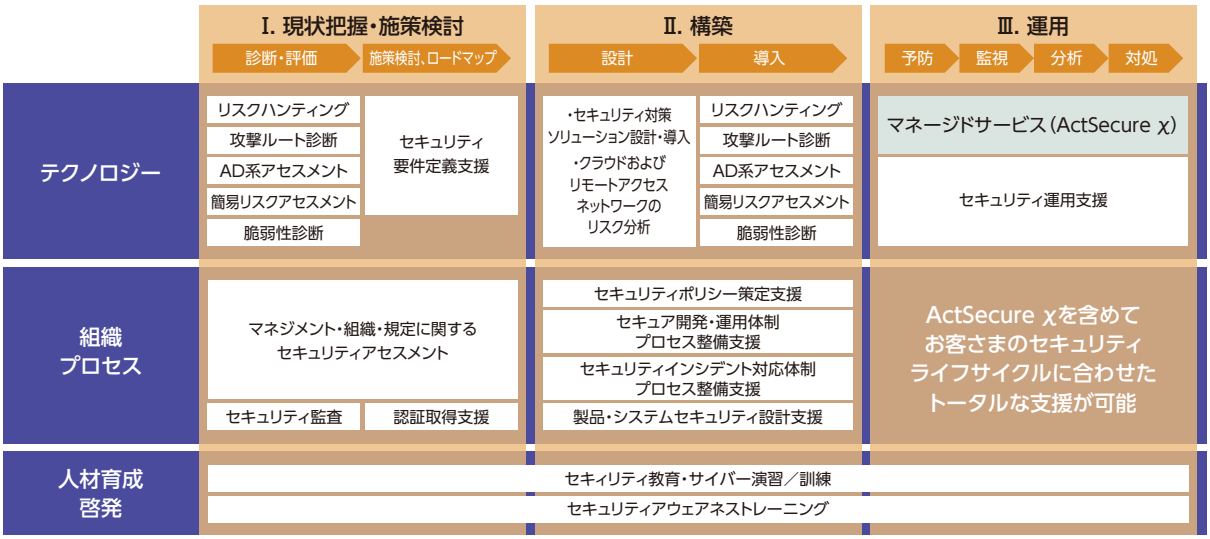
4 全体最適に向けてNECがご支援できること

今般、NECはデータドリブンサイバーセキュリティ事業を立ち上げました。本事業では、運用監視データを活用した「運用監視・対処」と「経営判断・プロセス改革」という2つのサイクルでセキュリティ業務のDXを実現します。

運用監視・対処は、お客さま環境からセキュリティ運用監視データや脆弱性・脅威情報をデータレイクに収集し統合管理、ダッシュボードによる可視化と高度な知見とデータを駆使して監視・検知・対処という日々のインシデント対応をサポートします。インシデントが発生した際にはアラートを上げ、原因や影響範囲を究明し対処案を提示します。

加えて、経営判断・プロセス改革は、運用監視・対処を通じて得たさまざまなデータを分析し、攻撃の状況やお客さまが抱え

プロフェッショナルサービス



*1 SOBD(Security Operation By Design):システム設計の上流段階で運用監視を見据えたセキュリティ実装を行うこと
*2 CSPM: Cloud Security Posture Management　*3 SSPM: SaaS Security Posture Management

るセキュリティ業務の課題を把握します。それを踏まえて、最適なアーキテクチャーや運用プロセスなど、セキュリティ対策の全体最適につながる提案を行っていきます。

データドリブンサイバーセキュリティ事業は、短期サイクルで繰り返す日々の運用監視し、そして、中長期サイクルで取り組む継続的なセキュリティの改善、2つの取り組みを連携させながらお客さまとの伴走型でサポートしていくものです。このようなサポートによって、経営的な観点では、セキュリティガバナンスの強化、適切な投資判断や説明責任遂行のサポートといった価値を提供します。さらに、運用監視・インシデント対応の観点では、迅速な検知、特定、復旧による被害の最小化などを実現します。そして、セキュリティ対策の観点では、お客さまの既存の対策や、受けている攻撃に適した対策の全体最適化を可能にします。

❶ セキュリティダッシュボード

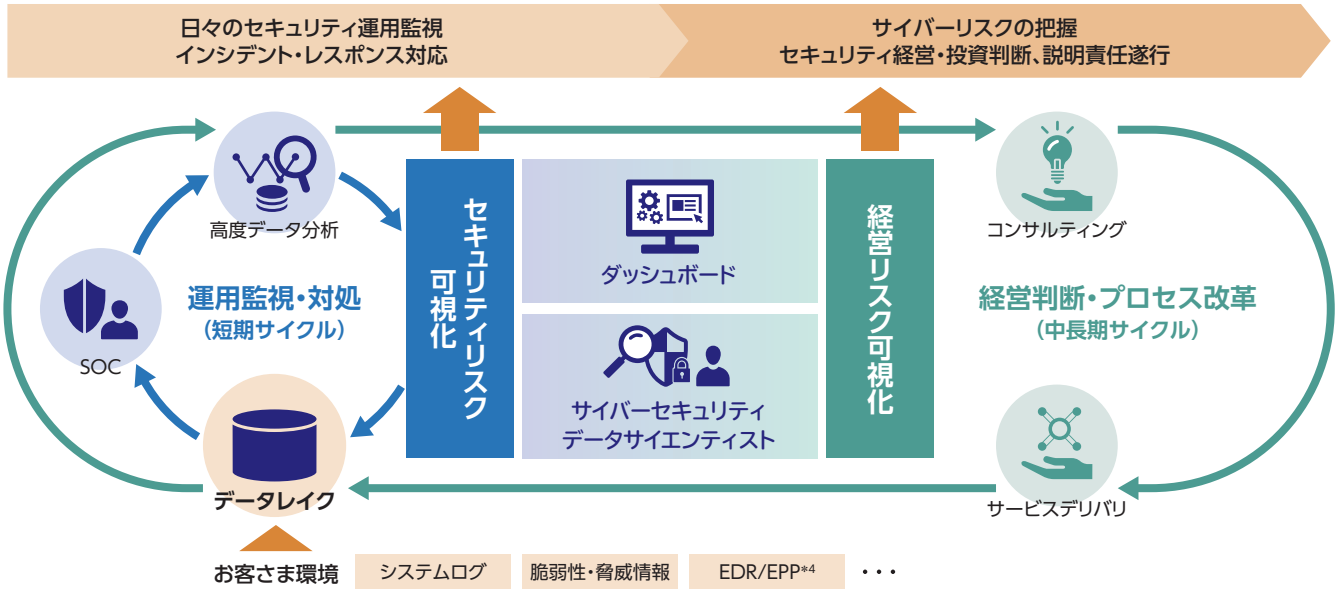
可視化・監視のカギを握るダッシュボードは、運用監視・対処と経営判断・プロセス改革という2つの目的に合わせて最適なものをご提案します。前者は、各セキュリティ対策状況の確認やインシデント状況の把握、ログ解析、調査など、情報セキュリティモニタリングを行うために最適化しています。後者は、パッチや対策の未適用数／割合、サイバー攻撃の疑い件数など経営リスクを可視化しやすいように設計しています。この2つのダッシュボードを通じて、お客さまは自社のセキュリティ対策状況やリスクの現状を把握したり、お客様導入済みの既存SLの部分最適を是正したりすることにつながります。

❷ セキュリティ監視分析

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

DXの浸透やテレワークの普及でクラウドシフトは進みましたが、一方でセキュリティリスクは増大しています。経済的な損失への備えだけでなく、経済安全保障にまつわる要請への対応も求められる中、急速に変化するICT環境に対応し、いかに効果的なセキュリティ対策を講じるかが重要です。NECは、新たに立ち上げたデータドリブンサイバーセキュリティ事業で、それを実践し、お客さまの大切な資産やビジネスの保護に貢献します。DXにおけるセキュリティソリューションおよびデータドリブンサイバーセキュリティについて詳しく知りたいお客様は、お気軽にNECまでお問合せください。

データドリブンサイバーセキュリティによる全体最適化プロセス



*4 EDR/EPP: Endpoint Detective and Response, Endpoint Protection

最前線でのサイバーセキュリティ技術の研究開発・事例

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

1 研究テーマのコンセプト

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

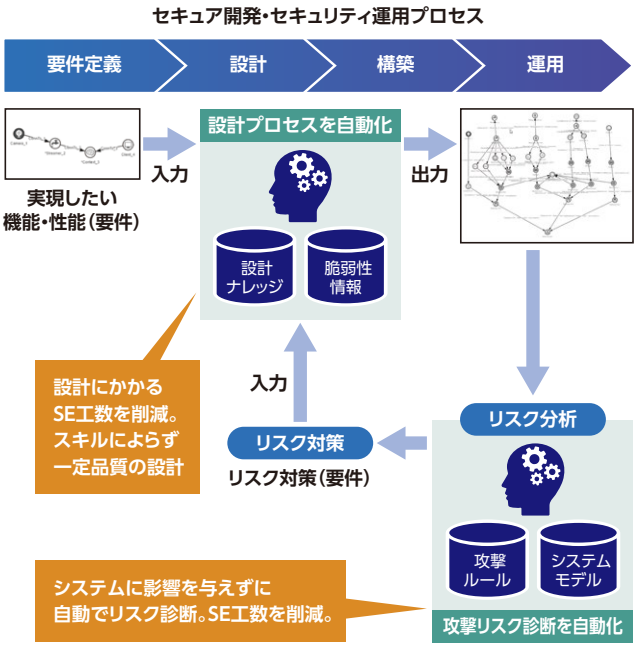
本章では、システムセキュリティ研究の例として、セキュアなICTシステムの設計を自動化する「セキュアシステム自動設計」を、データセキュリティ研究の例として、生体特徴量を暗号化したまま顔認証を行う「秘匿生体認証」および、組織間でデータを互いに開示することなくAIモデルを構築する「高秘匿連合学習」を取り上げ、以下に紹介します。

2 セキュア開発・セキュリティ運用の自動化

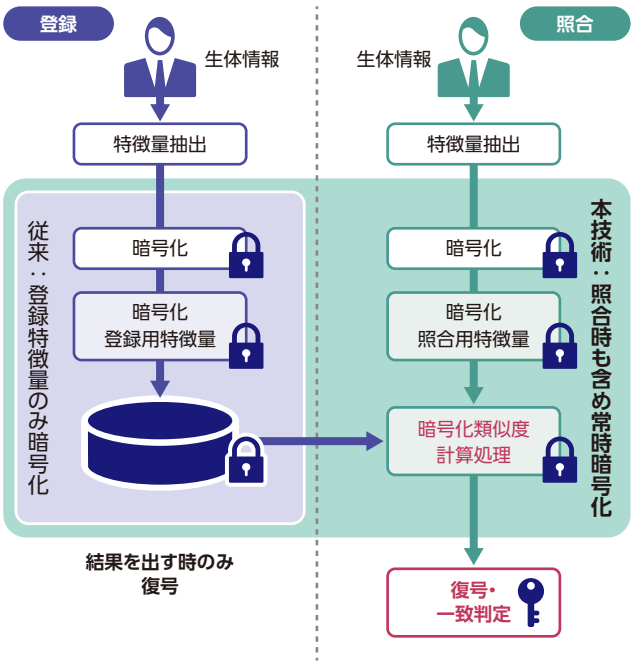
企業システムや社会システムのDX化推進に伴いICTシステムは複雑化しており、サイバー攻撃のリスクも高まっています。サイバー攻撃リスクが増え続ける中、ICTシステムのセキュリティを強化するためには、システムの企画・設計段階からセキュリティを考慮すること(セキュリティ・バイ・デザイン)が求められます。しかし、これまでのように人手による設計・開発では、複雑なICTシステムのセキュリティ確保が困難になってきており、対応工数が莫大になっています。NECでは、複雑なICTシステムの設計を自動化する技術を開発しています。セキュリティを含んだICTシステムに求められる機能や性能(要件)をもとに、AIがICTシ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

しかし、セキュアなICTシステムを構築したとしても、新たな脆弱性が発見されるなど、時間の経過により、サイバー攻撃のリスクが高まってきます。そのため、システム運用においても、セキュリティリスクを定期的に診断し、対処していく必要があります。通常、人手で実際にシステムを調査することでリスクを判定しますが、人手による時間・工数がかかること、実システムの調査により

セキュア開発・セキュリティ運用プロセスの自動化



秘匿生体認証を用いた生体特徴量の保護



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

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

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

システム停止などの悪影響が発生するなどの課題があります。NECは、サイバー攻撃リスク診断技術によりICTシステムに生じるサイバー攻撃リスクを自動で診断することができます。自動設計で得られたシステム情報を利用して、コンピュータシミュレーションによる網羅的な攻撃パターン調査を行うことで、運用中のシステムに影響を及ぼすことがなく、自動でセキュリティリスクを判定できます。さらに、診断結果をもとにセキュアなシステム構成を自動で導出することで、システムのセキュリティを維持することができます。*2*3

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

3 秘匿生体認証

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

秘匿生体認証では、特徴量を暗号化したまま顔認証の照合処理を実現するため、(1)マルチパーティ計算や(2)準同型暗号による秘密計算技術を活用しています。大規模な利用シーンにおいては、マルチパーティ計算を用いた方式が適しており、登録ユーザ数100万人程度で1秒以内の顔認証の照合処理を行うことが可能です。また、中～小規模の利用シーンでは1台のサーバで提供可能な準同型暗号を用いた方式が適しており、登録ユーザ数1万人程度で1秒以内の顔認証の照合時間を実現しています。*6

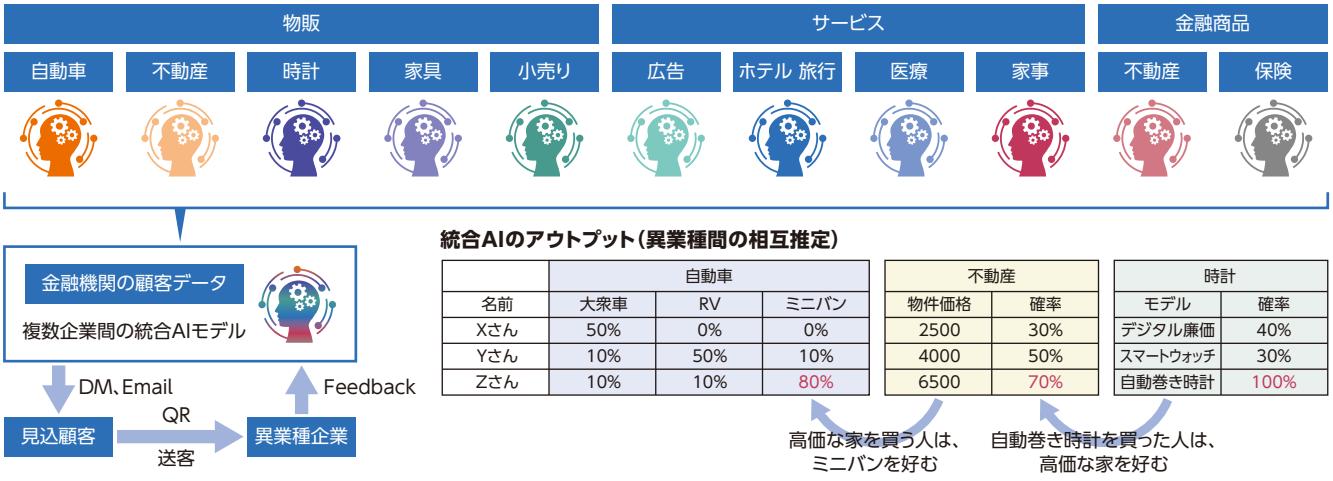
本技術の活用により、顔認証をはじめとした生体認証の安心・安全な利用に貢献します。

4 ハイブリッド高秘匿連合学習

様々な企業がデータを収集し、集めたデータを用いて構築したAIを営業活動に活用しています。例えば、見込み顧客推定などがAIで行うことができますが、このようなAIを業種をまたぐように拡張すること、例えば自動車業界の購買データを使って不動産の購入価格帯を予測するようなAIを構築することは困難です。もちろん両業種のデータを一か所に集めることができれば問題なく構築できます。しかし、異なる業種が保有するデータを集積することは、企業秘密の他社提供といった機密上の問題だけではなく、個人情報保護に関わる法的な問題にも関係し、容易には実施できません。ハイブリッド高秘匿連合学習は、直接的にはデータを集めず、業種をまたぐような属性推定を実現します。本技術の活用により、多様な業種のAIを統合し、相互に属性推定が行えるような統合AI基盤の提供を目指しています。*7

ハイブリッド高秘匿連合学習による異業種連携

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



	自動車		
名前	大衆車	RV	ミニバン
Xさん	50%	0%	0%
Yさん	10%	50%	10%
Zさん	10%	10%	80%

不動産	
物件価格	確率
2500	30%
4000	50%
6500	70%

時計	
モデル	確率
デジタル廉価	40%
スマートウォッチ	30%
自動巻き時計	100%

*4 顔認証の利活用 ～人権に配慮したNECの取り組み～ *5 今岡仁, 櫻井和之, 塚田正人, 宮川伸也, 大網亮磨, 一色寿幸, "生体認証が切り拓く未来", NEC技報 Vol.74 No.2 (2022).
*6 Hiroto Tamiya, Toshiyuki Isshiki, Kengo Mori, Satoshi Obana, Tetsushi Ohki, "Improved Post-quantum-secure Face Template Protection System Based on Packed Homomorphic Encryption", BIOSIG2021 (2021).
*7 "高秘匿連合学習 プライバシー・機密情報保護とAI活用を両立", NEC 研究開発特集記事, https://jpn.nec.com/rd/special/202103/index.html

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 World 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3年連続(2020、2021、2022)で獲得。2022年は100点満点を獲得。

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

国内業界団体による格付け
日本IT団体連盟 サイバーインデックス

「特に優れた取り組み姿勢および情報開示を継続的に確認できた」とする星二つを獲得(最高位)。
(日経500種平均構成銘柄の企業の中から11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。

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ネットワーク・センサ株式会社
- NECフィールディング株式会社
- NECフィールディングシステムテクノロジー株式会社
- NECプラットフォームズ株式会社
- 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
- 日本電気航空宇宙システム株式会社
- 日本電気通信システム株式会社
- フォワード・インテグレーション・システム・サービス株式会社
- ランゲージワン株式会社
- 株式会社ベストコムソリューションズ
- NECキャピタルソリューション株式会社

2 プライバシーマーク付与認定の取得状況

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

プライバシーマーク付与認定を受けたグループ会社

- 日本電気株式会社
- アビームコンサルティング株式会社
- アビームシステムズ株式会社
- NEC VALWAY株式会社
- NECソリューションイノベータ株式会社
- NECネクサソリューションズ株式会社
- NECネッツエスアイ株式会社
- NECネッツエスアイ・サービス株式会社
- NECネットイノベーション株式会社
- NECファシリティーズ株式会社
- NECフィールディング株式会社
- NECフィールディングシステムテクノロジー株式会社
- NECプラットフォームズ株式会社
- NECマグナスコミュニケーションズ株式会社
- NECマネジメントパートナー株式会社
- 株式会社NECライベックス
- 株式会社KIS
- 株式会社サンネット
- 株式会社ニチワ
- 株式会社ブリースコーポレーション
- 株式会社ベストコムソリューションズ
- 株式会社ワイイーシーソリューションズ
- キューアンドエー株式会社
- KISドットアイ株式会社
- K&Nシステムインテグレーションズ株式会社
- NEC静岡ビジネス株式会社
- 日本電気通信システム株式会社
- ディー・キュービック株式会社
- フォワード・インテグレーション・システム・サービス株式会社
- ランゲージワン株式会社
- NECキャピタルソリューション株式会社

3 ITセキュリティ評価認証の取得状況

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

ISO/IEC15408認証取得製品・システム

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

NECグループの概要

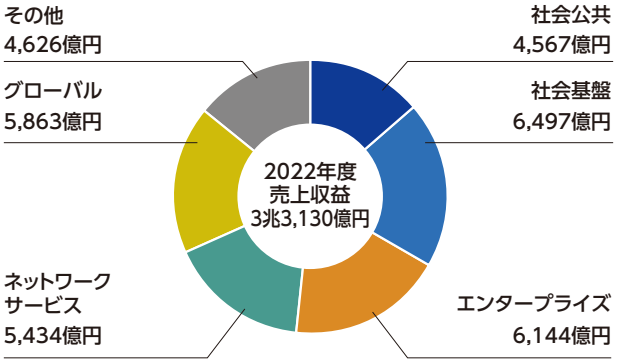
会社概要

商　　号	日本電気株式会社　NEC Corporation
本　　社	東京都港区芝五丁目7番1号
創　　立	1899年(明治32年)7月17日
資 本 金	4,278億円※
連結従業員数	118,527名※
連結子会社数	284社※

※2023年3月31日現在

事業紹介

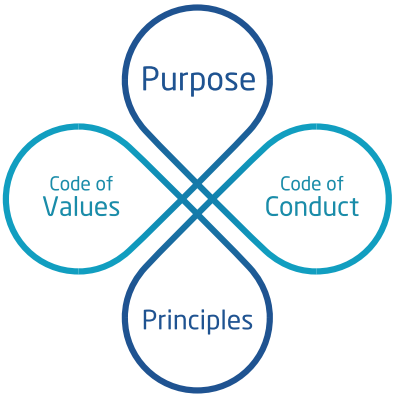
セグメント別売上収益



※2022年3月31日現在

NEC Way[経営理念]

NEC Way



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

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

私たちはNEC Wayの実践を通して社会価値を創造していきます。

Purpose
存在意義

\Orchestrating a brighter world

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

Code of Values
行動基準

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

Principles
行動原則

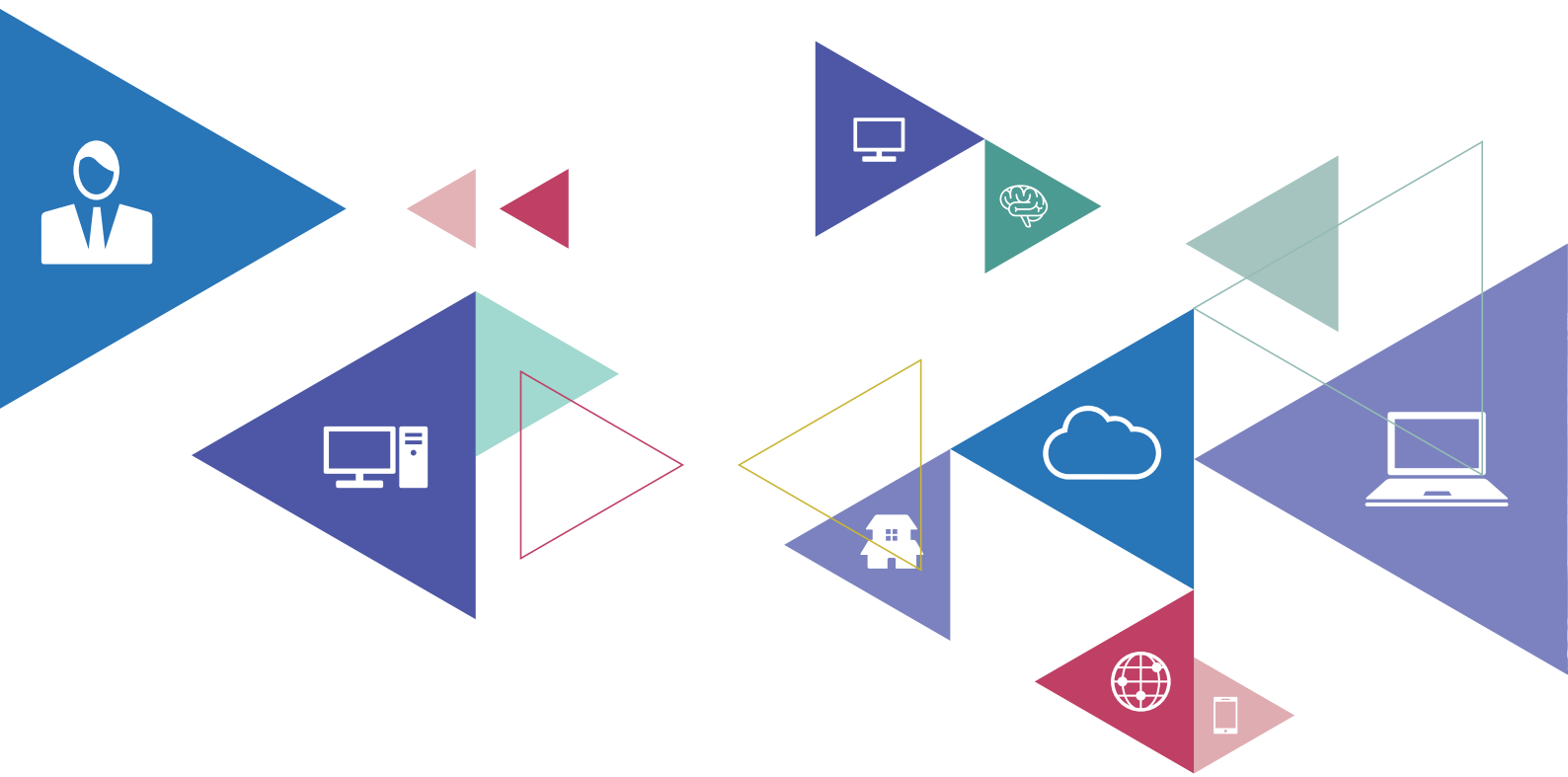
創業の精神「ベタープロダクツ・ベターサービス」
常にゆるぎないインテグリティと人権の尊重
あくなきイノベーションの追求

Code of Conduct
行動規範

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

コンプライアンスに関する疑問・懸念の相談、報告

情報セキュリティ報告書2023



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

2023年７月発行

Cat.No. U04-23070131J