\Orchestrating a brighter world NEC

情報セキュリティ報告書2022

NECが考える情報セキュリティ

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
執行役員常務
兼CIO（チーフインフォメーションオフィサー）
兼CISO（チーフインフォメーションセキュリティオフィサー）

全世界がオープンに繋がる今日、ランサムウェアをはじめとするサイバー攻撃の高度化・ビジネス化、高まる個人情報保護や経済安全保障等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では従来の境界型防御モデルから、すべてのアクセスを信頼せずに防御する「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に準拠し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、経済産業省が策定するサイバーセキュリティ経営ガイドラインVer 2.0やNIST（米国標準技術研究所）のCyber Security Framework（1.1版）に準拠し、深刻化するサイバー攻撃に対するインテリジェンス（攻撃者の動向等に基づく事前防御）やレジリエンス（攻撃からの回復能力）の強化をはかっています。また、セキュリティ・バイ・デザイン3.0の考え方に基づき、取り扱われるデータにフォーカスしてその安全性を確保するなど、高品質なセキュリティを確保したトータルパッケージの提供とサプライチェーン全体での対策強化を促進しています。このような施策が認められ、2021年には一般社団法人 日本IT団体連盟よりセキュリティ対策で特に優良で模範となる企業に授与される「星」を獲得しました。

今後も、包括的なアプローチによる情報セキュリティへの取り組みを強化するとともに、顔データを暗号化したまま認証可能な「秘匿生体認証」や顔認証による「ウォークスルー入退管理」など、社内で実装済みの最先端技術を提供することにより、お客さまや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、ブランドステートメントに「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。

本報告書に関するお問い合わせ
日本電気株式会社
コーポレートトランスフォーメーション部門 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 2022」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 2.0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、2022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 2.0 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対応するための仕組みの構築
- 指示6 サイバーセキュリティ対策におけるPDCAサイクルの実施
- 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対策及び状況把握
- 指示10 情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供

情報セキュリティ推進フレームワーク

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

NECグループは、情報セキュリティの確保を経営上の重要事項と位置づけ、お客さまやお取引先からお預かりした情報資産およびNECグループの情報資産をサイバー攻撃などの脅威から守るとともに、セキュアな製品・システム・サービスをご提供することで、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

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、その取組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。

*1 CISO: Chief Information Security Officer

2 NECグループの情報セキュリティ推進体制

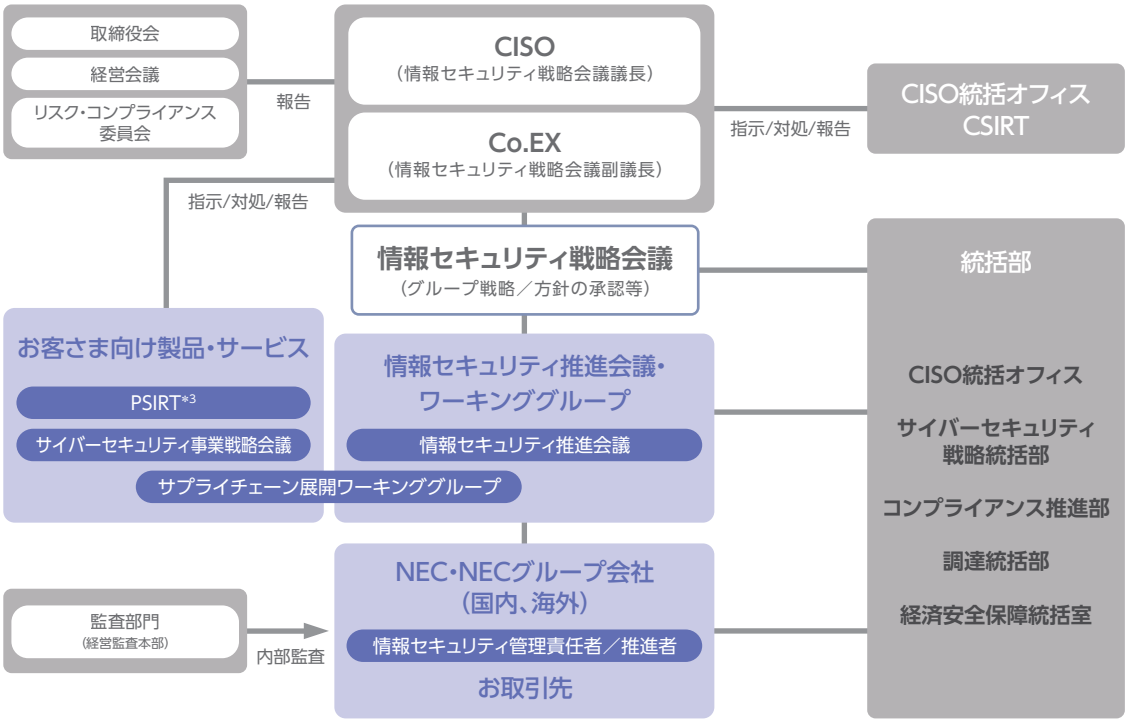
本体制は、情報セキュリティ戦略会議と下部組織、各関連組織で構成されます。情報セキュリティ戦略会議はCISOが議長を務め、情報セキュリティ施策の審議・評価・改善、事故の原因究明と再発防止策の方向付け、情報セキュリティビジネスへの成果活用などを審議します。また、ここで決定した施策の運営状況は、定期的に社長に説明し、了承を得ています。

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。

*2 CSIRT: Computer Security Incident Response Team

NECグループ情報セキュリティ推進体制



*3 PSIRT: Product Security Incident Response Team

情報セキュリティマネジメント

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、情報セキュリティの基本規程、情報管理に関する規程、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（2022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。

*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 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

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。

4 重要情報管理

❶ Three Lines Model

NECグループではThree Lines Model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ます。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。

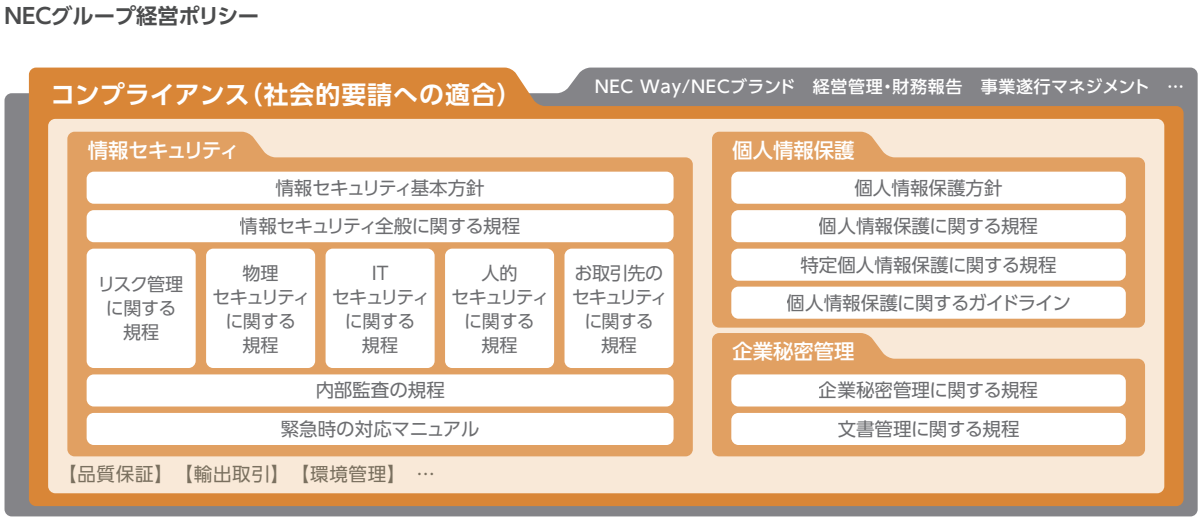
実施が不十分な項目は、各組織でその理由を把握して改善します。また、各組織の改善では対応できない課題である場合は、次年度のNECグループの情報セキュリティ推進計画で継続的に課題解決に取り組みます。

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プライバシーマークの監査を年次で実施します。ISO/IEC27001やJISQ15001に照らし、各組織の状況を定期的に監査します。

6 ISMS認証取得の取り組み

ISMS認証取得を目指す組織に対して、同規格の取得に必要な「標準コンテンツ」を核に「NetSociety for ISMS」サービスを提供し、認証取得を推進します。



情報セキュリティ基盤

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 CISA：Cybersecurity and Infrastructure Security Agency

1 アイデンティティセキュリティ

認証は、情報セキュリティ管理のかなめであり、人を確実に識別・認証することで、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を実現できます。

情報資産の適切な管理には、利用者の識別・認証、および利用者に応じた権限の付与が重要です。NECは、識別・認証・認可に用いる情報を一元管理する認証基盤を構築しています。これは社員だけでなく、必要に応じてお取引先なども含めた形で実現しています。

認証・認可に用いる情報は、ユーザIDやパスワードに加え、組織情報、役職情報などのアクセス制御情報があり、業務システムなどへのアクセスを個人単位で制御します。また、NECグループ各社が管理する認証・認可に用いる情報が、どのシステムでどのような目的に利用されるのかを一元管理しています。重要情報を扱うシステムでは、ユーザIDとパスワード（知識認証）に加え、電子証明書による個人認証（所有物認証）や顔認証（生体認証）を活用した、多要素認証の導入も推進しています。

クラウドサービスの認証では、社内の認証基盤と連携して社内外のサービスとのシームレスな認証を整備しています。これによりクラウドサービスの利用ニーズに対し、安全・安心に利用できる仕組みを実現しています。

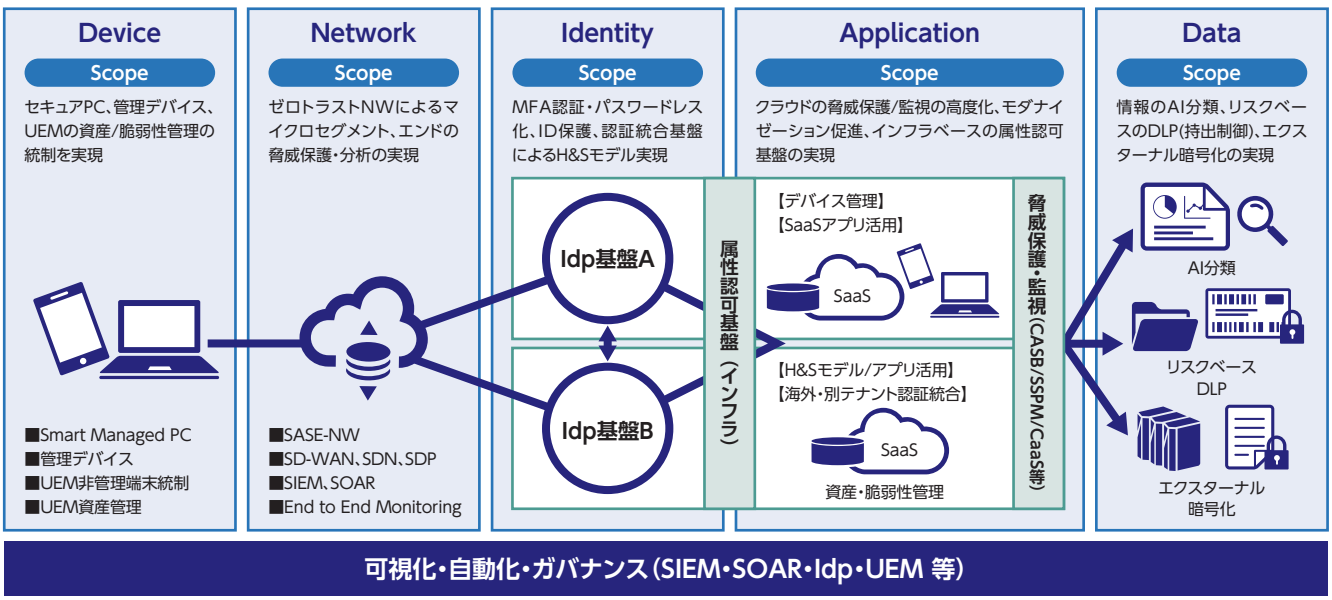
2 デバイスセキュリティ

エンドポイントの端末には、多様な働き方に対応したセキュアで使い勝手のよいリッチクライアントベースPC（Smart Managed PC）を採用しています。安全・安心と利活用の両立をめざした設計で、シンプルかつセキュアな顔認証によるログインをはじめ、占有リソースによりオフライン選択できる快適な動作環境、アプリケーションやデバイスの拡充設定の簡素化などを実現しています。これにより、業務の利便性や生産性をアップすると同時に、従業員のエンゲージメント向上に繋がります。

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。

情報漏えい防止システムでは、「暗号化」「デバイス制御」「ログの記録」を実施し、外部からの攻撃や内部不正による情報漏えいリスクへの対策を実施しています。

ゼロトラスト基盤の概要とスコープ



リスクへの対策を実施しています。

「暗号化」は、記憶装置とファイルを暗号化し、盗難・紛失による情報漏えいを防止します。ファイル暗号化は、アクセス権や利用期限を設けた一定のセキュリティレベルをNECグループ全体でデフォルト設定しています。もしマルウェア感染で外部に情報が送られたり、メールで情報を誤送信したりしても、暗号化対策により情報は漏えいしません。

「デバイス制御」では、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、赤外線など通信デバイスに対して、情報書き出しの禁止制限をしています。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」では、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、事故による影響範囲の特定や状況把握、再発防止策の策定をします。内部からの情報漏えい防止のために、事故が発生した際の影響度合いを考慮し、重点的に管理すべき社内システムを定義しています。重要度の高いシステムには脆弱性情報の収集・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。

また、イントラネットに接続する情報機器のセキュリティを維持し、ウイルスやマルウェアからPC・ネットワークを守る、次のようなICT基盤をグローバルに整備しています。

*2 UEM：Unified Endpoint Management

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明らかにすることで、セキュリティリスクを即座に可視化します。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。

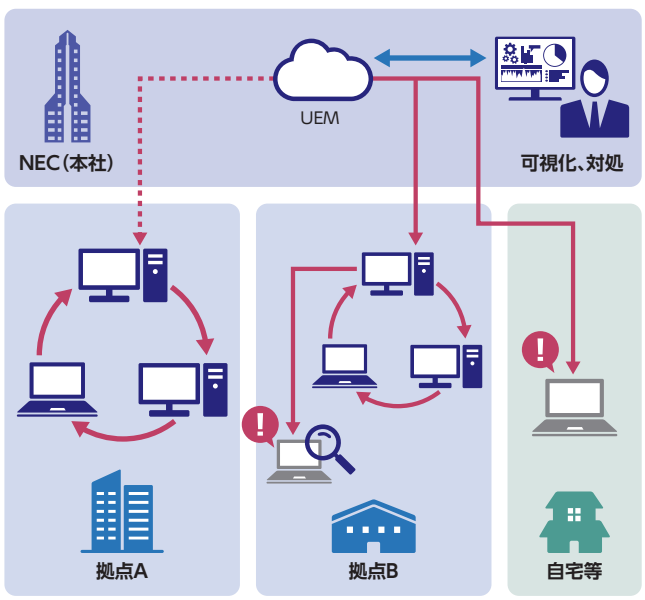
❷ ネットワーク管理

PCの状態の見える化に加え、セキュリティ対策が不十分なPCをイントラネットに接続したり、イントラネット上で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。

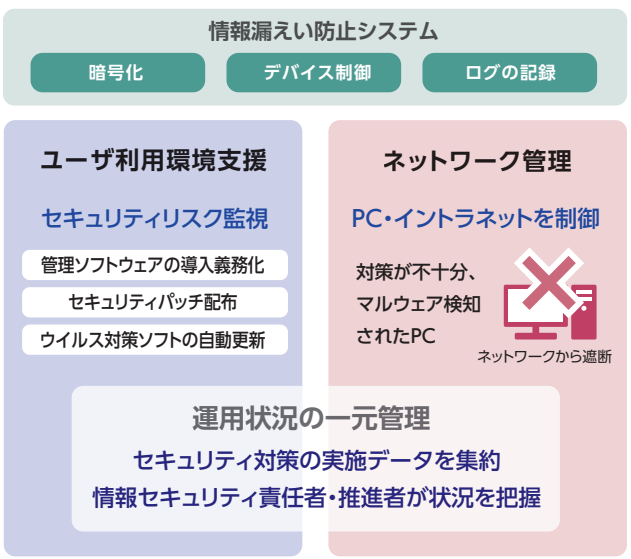
❸ 適用状況の一元管理

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、各部門の情報セキュリティ責任者や推進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。

UEMによるセキュアなエンドポイント管理



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柔軟性および堅牢性を提供するため、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り、「未然防御」・「緊急遮断」・「ログ取得範囲の拡大」を実施し、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で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。

また、リモート環境をゼロトラスト指向でグローバルに刷新します。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。

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

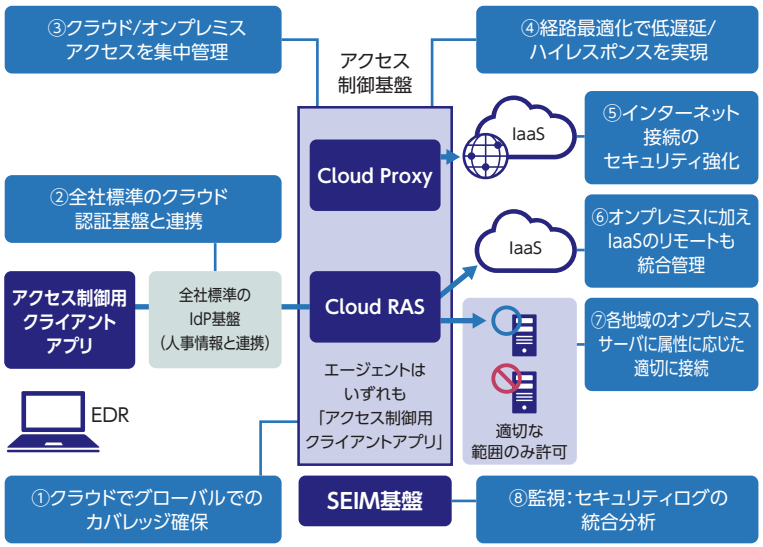
クラウドサービス上のログを、CASB*3で監視・分析することで、重要なデータを取り扱うクラウドサービスに対する内部不正やサイバー攻撃への対策を実施しています。また、社内で使用されているクラウドサービスの利用状況を可視化し、未承認のリスクが高いクラウドサービスを監視しています。

*3 CASB：Cloud Access Security Broker

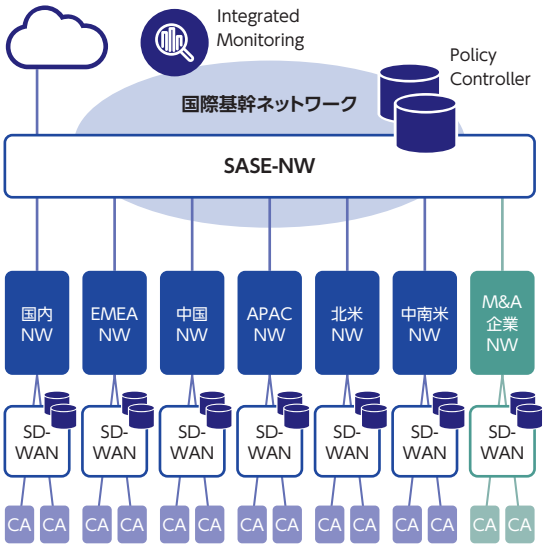
❷ パブリッククラウドの設定ミスに起因するインシデント防止

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リモートアクセス基盤のグローバル刷新



SD-WANのグローバル展開



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。

*4 CSPM：Cloud Security Posture Management

❸ SaaSの設定ミスに起因するインシデントの防止

Microsoft 365やBox、Salesforceなどのクラウドサービスは利用時の設定項目が多く、運用する際には設定ミスによる情報漏えいリスクがともないます。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・是正する運用を実施しています。

*5 SSPM：SaaS Security Posture Management

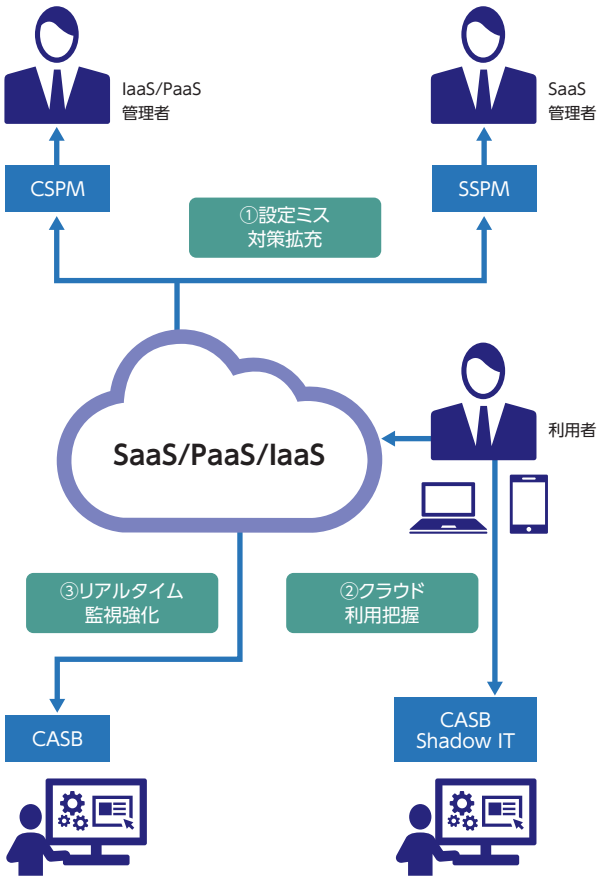
5 データセキュリティ

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推進しています。さらに、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・暗号化やトラッキング、アクセス権管理などを実施しています。これにより、トラッキングによる利用状況のトレースが可能となり、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。

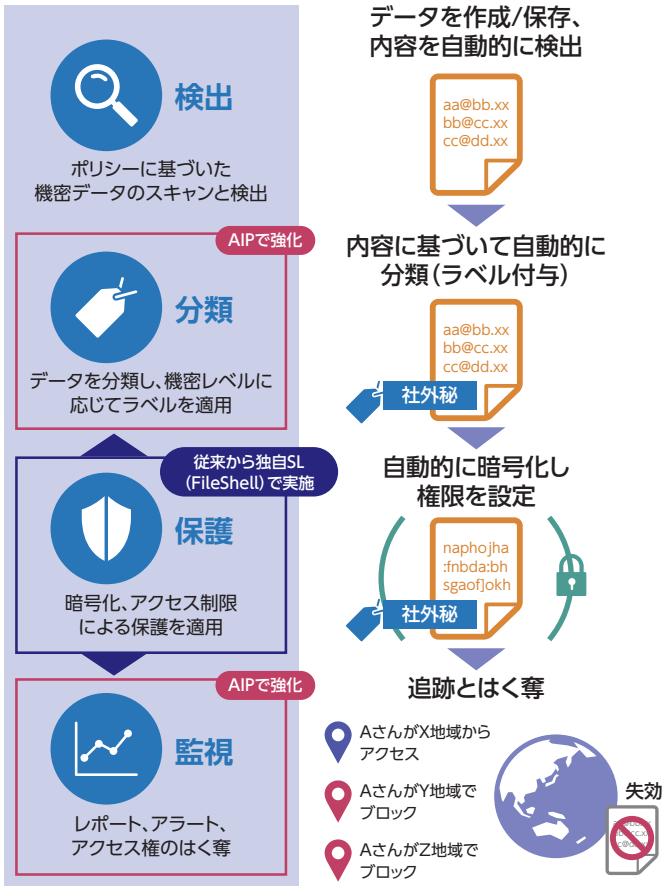
また、重要情報の管理を徹底するため、極秘事項に該当する情報を安全に管理するインフラとして、セキュアストレージを導入しています。極秘事項の管理要件であるアクセス制御や暗号化、証跡管理、侵入調査、ISMS管理に対応し、これらの要件に対する業務現場の負荷を低減して、セキュアな情報管理を実現しています。

*6 AIP：Azure Information Protection

クラウドサービス利用上のセキュリティ対策



InfoCage FileShell+AIP



情報セキュリティ人材

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

NECでは、全社員を対象とした情報セキュリティの「アウェアネスの向上」、「施策を推進する人材の育成」、お客さまに価値を提供できる「プロフェッショナルな人材の育成」の3つの観点で人材を育成しています。

2 情報セキュリティアウェアネスの向上

情報セキュリティアウェアネスの向上をはかるには、情報セキュリティリスクを感じ取るリスク感覚や情報を適切に取り扱うための知識、情報セキュリティのリスクカルチャーが重要であり、そのための教育や啓発を行っています。

❶ 情報セキュリティ、個人情報保護教育

NECグループの全社員を対象に、情報セキュリティと個人情報保護（マイナンバー対応を含む）に関するWBT*1を実施し、情報セキュリティの知識やスキルの向上をはかっています。新しい脅威への対応や意識啓発、情報の取り扱い、テレワークのセキュリティ対策などセキュリティ脅威のトレンドなどを考慮し、教育内容を毎年更新しています。

*1 WBT：Web Based Training

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、映像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通じて、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RISS*3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。

*2 CISSP：情報セキュリティ・プロフェッショナル認定資格
*3 RISS：情報処理安全確保支援士

全社員対象の教育

4 プロフェッショナルな人材の育成

製品・システム・サービスのセキュリティ対応力を高め、お客さまの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

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します。リモートで受講可能な演習環境により、新型コロナウィルス感染症(COVID-19)の影響下でも、2019年3月以降延べ4,000名が受講し、お客さまのシステム開発・運用を担うセキュリティの知識と技術を強化しています。

❷ 全社的CTFの実施

セキュリティ人材の裾野拡大を目的とし、NECグループ全社員を対象に、社内CTF*4「NECセキュリティスキルチャレンジ」を開催しています。2015年の開始以来、延べ6,000名以上が自主的に参加し、セキュリティスキルの向上に役立てています。

*4 CTF: Capture the Flag

❸ 営業・SEセキュリティ基礎教育

営業・SEとして必要な、セキュリティ・バイ・デザイン(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、2021年度は延べ30,000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スキル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年度より行っており、これまでに延べ40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さまにお届けします。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。

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

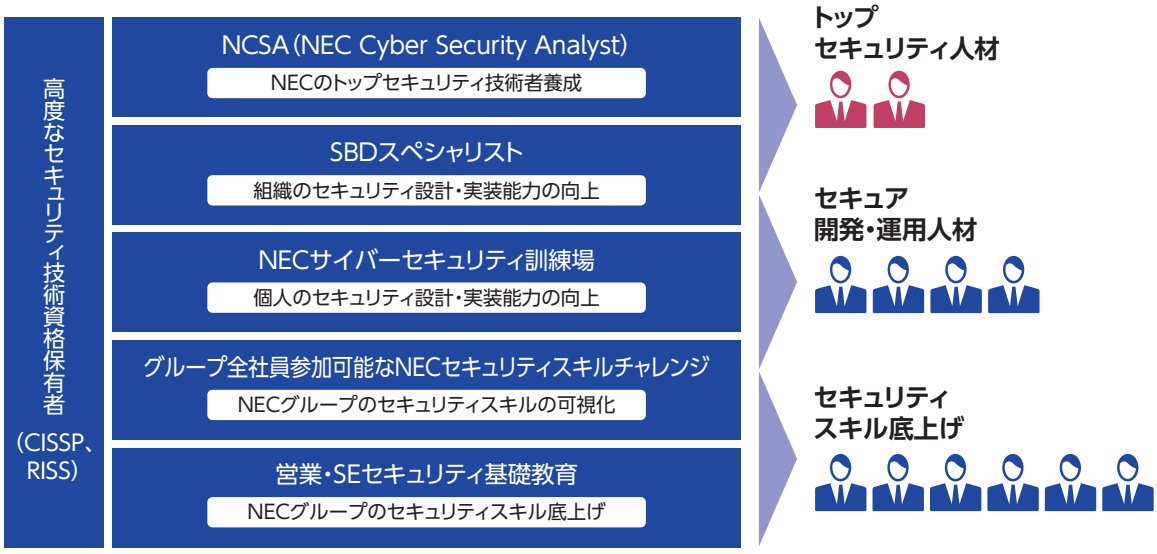
トップセキュリティ人材の強化を目的とし、セキュリティ技術の知識を持つ人材を対象に、CSIRT*5業務やリスクハンティングなど高度なセキュリティサービスに必要な実践的テクニカルスキルを、半年間の集中プログラムで習得します。2019年度まで実施したNCAT(NEC CISO補佐官トレーニング)とあわせ延べ60名が受講し、プロフェッショナルサービスの提供に携わっています。

*5 CSIRT: Computer Security Incident Response Team

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、セキュリティ公的資格の取得を強く推奨しています。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の取得者を拡充しています。NECグループのCISSP保有者は、200名を超えます。

プロフェッショナルな人材の育成



サイバー攻撃対策

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。

*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

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、日々のサイバー攻撃の監視や状況の把握、分析を行い、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、⑤重要情報管理に注力しています。

*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

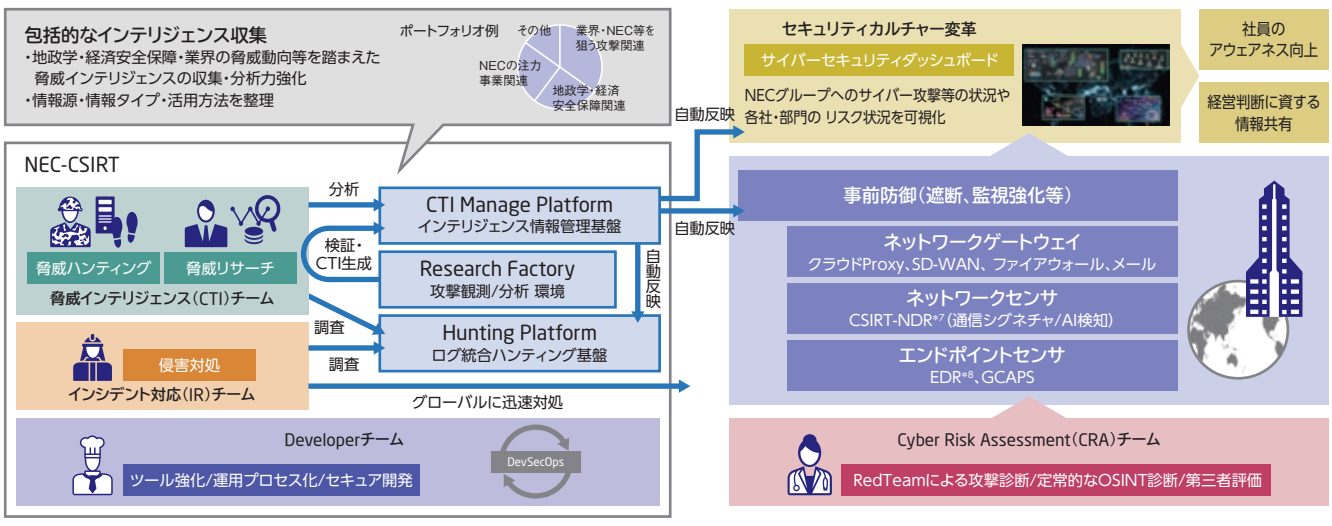
❶ Red Teamによるサイバーリスクアセスメント

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を目指し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。重要情報管理の調査、公開サーバの脆弱性やデータ漏えいなどのリスク調査、攻撃者視点での外部／内部の侵入調査の3つをパッケージ化し、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、改善策を実施します。なお、監査法人およびセキュリティ専門企業による第三者の攻撃診断についても実施しています。

❷ 脅威インテリジェンス生成・活用

脅威インテリジェンス専門チーム(CTI*6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とログ統合分析基盤に

サイバーセキュリティ対策の全体像



*7 NDR: Network Detection and Response *8 EDR: Endpoint Detection and Response

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。

*6 CTI: Cyber Threat Intelligence

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、ランサムウェアの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強化しました。また、有事に備え、関係部門や専門家による演習を半年に一回以上実施しています。さらに、第三者による重要システムのレジエンス評価を実施し、高水準な事業継続性の実現をはかっています。

❺ 重要情報管理

会社として守るべき重要な情報を厳格に保護するため、Three Lines Modelの考え方に基づいてリスクオーナーを明確にし、管理しています。また、情報漏えいなどが発生した際に経営や事業に甚大な影響を与える情報については、セキュリティレベルの高いストレージに格納し、厳重に管理しています。

2 TOKYO2020におけるNECグループのサイバーディフェンス

2018年からサイバー脅威インテリジェンスの専門体制を構築し、脅威予兆を含むインテリジェンスを収集・活用した事前防御を実施してきました。大会開催前には、RedTeamによるサイバーリスクアセスメント(CRA)をグローバル全社に行い、セキュリティリスクの特定および低減をはかる対策を展開するとともに、有事に備えたCSIRTの対応訓練を行いました。

大会開催期間中は特別監視体制を敷き、CSIRTによる監視強化、重要情報管理の徹底、社内システムのインシデント状況の迅速な一元的把握により、世界的イベントを無事に乗り越えることができました。

これらのノウハウは、NECにおけるディフェンスレガシーとして継続するとともに、全社員のアウェアネス向上をはかるため、サイバーセキュリティダッシュボードとして公開し、NEC社内のセキュリティカルチャー変革に役立てています。

サイバーセキュリティダッシュボード

お取引先と連携した情報セキュリティ

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セキュア開発・運用、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。

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、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実施要領を定め、秘密表示、持ち出し管理、用済み後廃棄・返還などの実施を徹底しています。

❺ 技術対策の導入

技術対策として必須の対策（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。

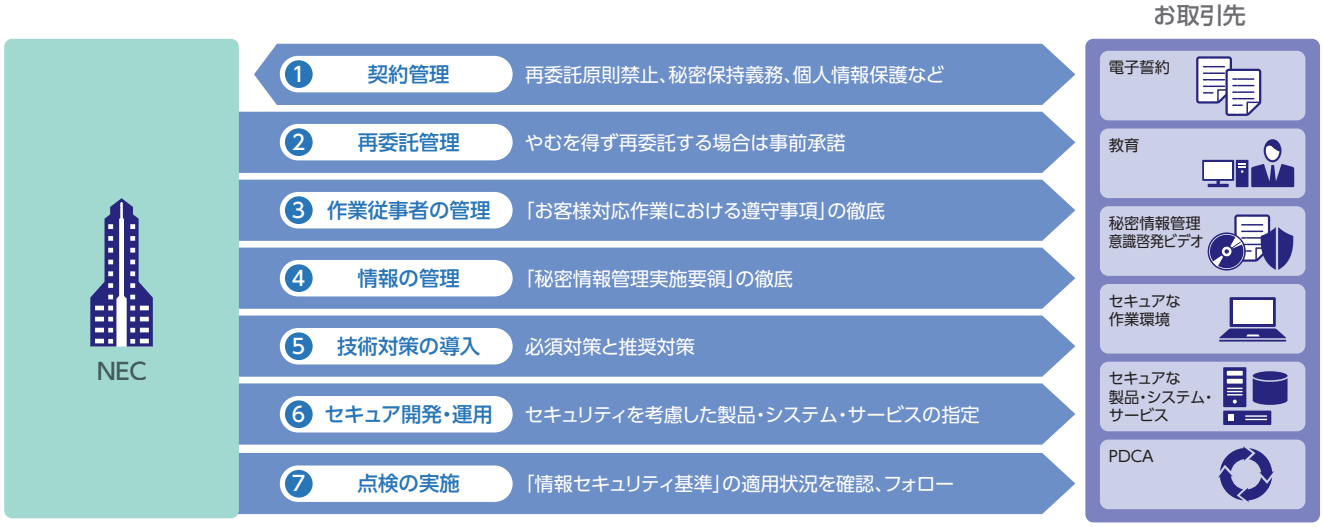
❻ セキュア開発・運用

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。

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するため、NECでは全国のお取引先（約1,800社、うちISMS認証取得会社約850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。

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

NECと取引のある会社、約1,800社を選んで実施します。お取引先は自社の対策状況を自ら点検し、点検結果をWebシステムに入力でき、登録内容は常に更新できます。

❷ 訪問点検

取引が多いお取引先を対象に、毎年200社前後を選んで実施します。NECの点検担当者（約100名）が、お取引先を直接訪問、あるいはリモートにて点検を行います。

❸ 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

セキュアな製品・システム・サービスの提供

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

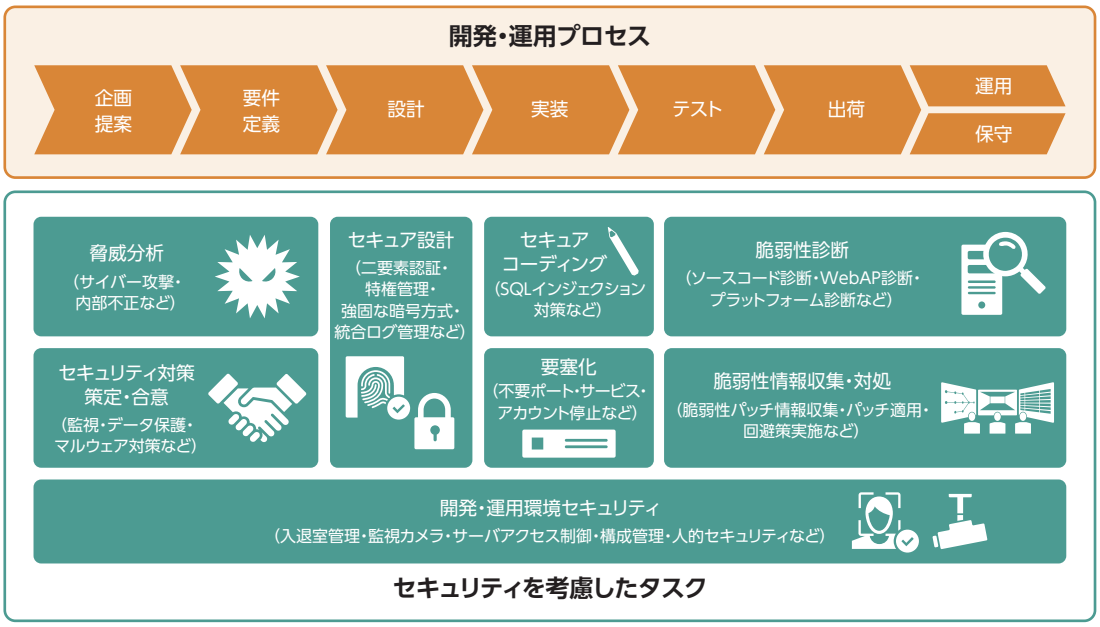
お客さまに提供する製品・システム・サービスをセキュアに開発・運用するために、NECではセキュリティ実装推進体制を構築しています。本推進体制は、全社のサイバーセキュリティ統括部門と各事業部門に配置したセキュリティ責任者で構成されています。セキュリティ責任者は、製品・システム・サービスの脆弱性や設定ミス、システムの不具合に起因する情報セキュリティ事故の撲滅に向け、全社のサイバーセキュリティ統括部門と各事業部門との橋渡し役として、各種セキュリティ施策の浸透や現場におけるセキュリティ対策の支援を担っています。セキュリティ責任者の役割や各部門でのセキュリティ実装のプロセスは「サイバーセキュリティ管理規程」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、2021年度はNIST（米国立標準技術研究所）のセキュリティガイドラインを参考にお取引先向けのセキュリティ基準の改訂を行いました。近年、ビジネスパートナーや委託先がサイバー攻撃を受け、自社から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はこのようなサプライチェーン攻撃に対応するため、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年度は上述の基準改訂に基づいて、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ています。

❷ セキュリティ実装の主要な取り組み

NECでは、セキュリティを確保する「セキュリティ・バイ・デザイン（SBD）」の思想に基づき、企画・設計フェーズから構築フェーズ、運用管理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。

セキュリティ実装プロセス



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。

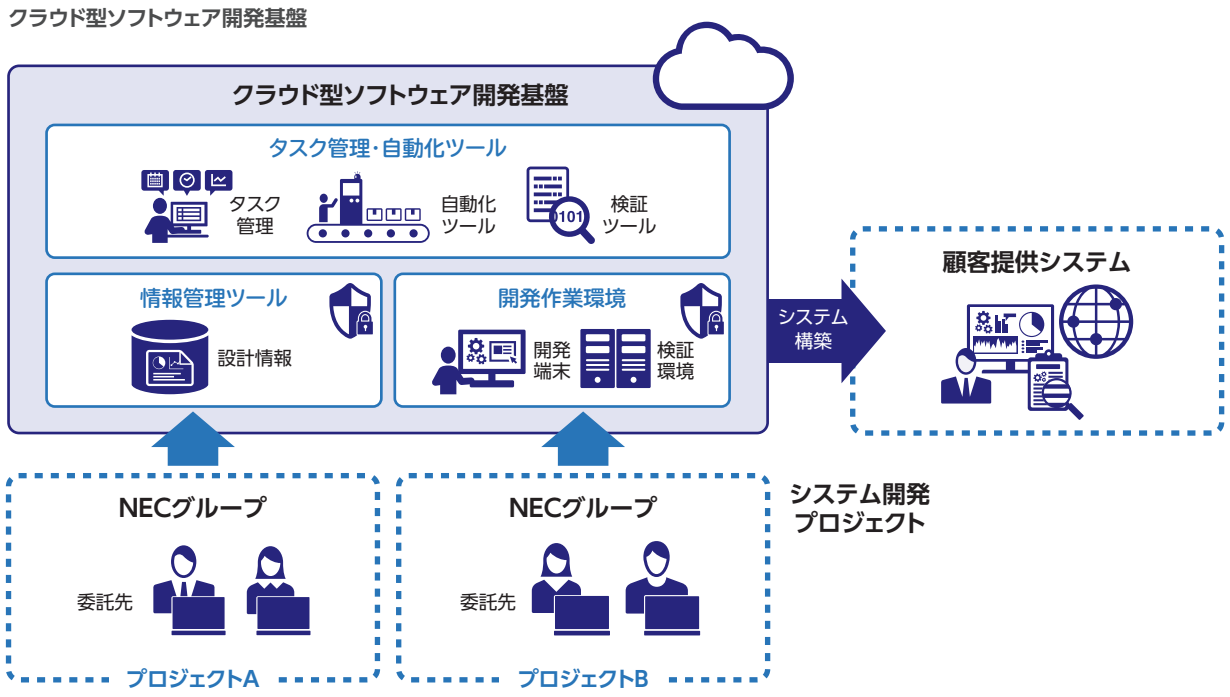
製品・システム・サービスの開発では、各フェーズでセキュリティタスクが実施されていることを確認するために、チェックリストを作成し活用しています。本チェックリストに基づき、セキュリティタスクの実施状況を可視化するために開発された「セキュリティ実装点検システム」により業務プロジェクトが管理され、セキュリティ対策状況の効率的な点検・監査が実施されています。

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ため、サイバーセキュリティ上のさまざまな脅威情報を自動的に収集するツール、収集した情報を分析する作業環境、そしてそれらの収集・分析した情報を展開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。

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事で、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。



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繋ぎ、人とモノ、モノとモノを繋ぐことで、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、あらゆるモノ同士が繋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、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。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。

*1 DX：Digital Transformation

社会基盤を支えるNECの事業領域

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では国内外の関係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することで、サイバー犯罪への対応を進めています。また、一般社団法人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。

*2 JC3: Japan Cybercrime Control Center

❷ 国の活動への貢献

NECの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、執行役員副社長 兼 CDO(チーフデジタルオフィサー)兼ICT事業トランスフォーメーション統括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。

*3 IPA: 独立行政法人情報処理推進機構　*4 JDTF: 一般社団法人デジタルトラスト協議会

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。脅威の大本を断ち、被害の防止を目指す。NEC執行役員副社長兼CDO(チーフデジタルオフィサー)兼ICT事業トランスフォーメーション統括 堺 和宏が代表理事を務める。

ICT-ISACに参画 (2017年3月)
多様な事業者がサイバー攻撃等の情報収集・分析および対応について情報共有し、業界の枠を越えて連携・協調し、脅威に対処するために発足したICT-ISACに参画。
(NECは前身となる一般財団法人日本データ通信協会テレコム・アイザック推進会議から参画)

産業横断サイバーセキュリティ検討会 参画 (2016年1月)(2017年4月)
日本電信電話株式会社、株式会社日立製作所とともに、サイバーセキュリティ人材育成に向けた検討会を発足。2017年からは「一般社団法人サイバーリスク情報センター(CRIC)」内組織に移行し、情報共有についての取組みを、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 Threat Alliance(CTA)」に加盟。加盟から現在まで、CTAへの脅威情報提供を継続。

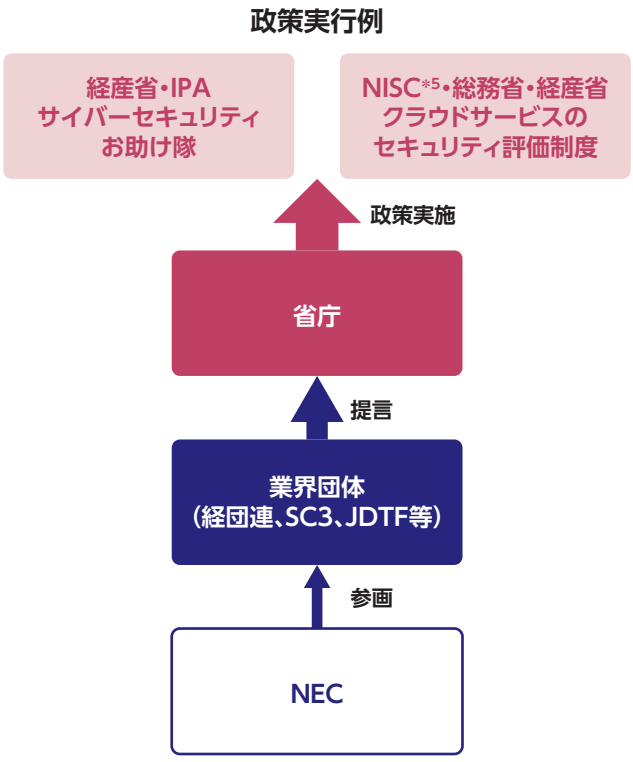
組織間連携

インターポールが加盟国警察向けに実施するオンライン形式のサイバー犯罪捜査演習を支援 (2020年10月)
国際刑事警察機構主催のサイバー犯罪捜査演習「Digital Security Challenge(デジタルセキュリティチャレンジ)」において、演習シナリオの作成や解析対象となるデータの開発などを支援し、本演習の開催に貢献。

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)
日本電信電話株式会社とともに、5G・IOWN等の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を確保することによってサプライチェーンセキュリティリスクの抜本的な低減をはかるため、「セキュリティトランスペアレンシー確保技術」を開発。

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について共同で国際標準化に向けた取り組みを行い、国際電気通信連合(ITU)の電気通信標準化部門よりITU-T 勧告X.1060を発行。

業界団体を通じた政策提言



*5 NISC: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株式会社インフォセックがあります。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さまに安全・安心を提供しています。

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。

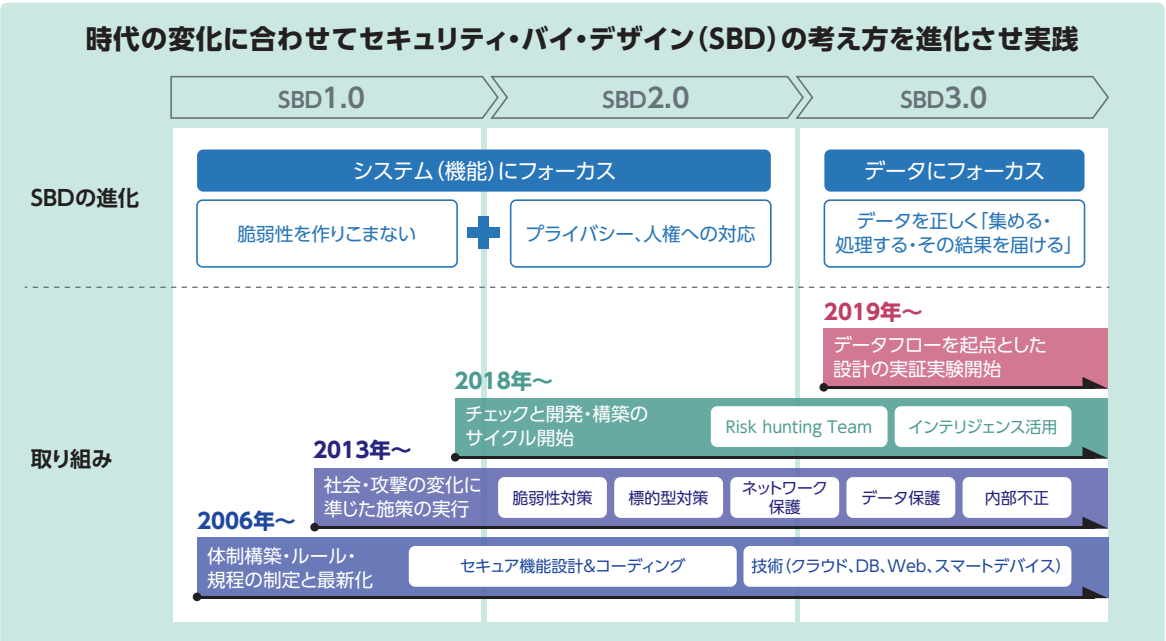
❸ 国内セキュリティ人材育成

北陸先端科学技術大学院大学との共同研究を通して、サイバーセキュリティに関する最先端の研究活動と日本のセキュリティ人材基盤の強化に貢献しています。

❹ お客さまへの教育プログラム提供

NECは、DX推進に必要なデジタル人材育成を支援するNECアカデミー for DXにおいて、サイバー攻撃に有効な堅牢化の実践スキルおよびインシデント対応スキルの獲得を目的としたプログラムやセキュリティ人材の可視化と育成を目的としたプログラムを提供しています。

SBD3.0によるセキュリティ実装の考え方



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徹底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リスクの1つとしてサイバー攻撃が取り上げられることから、NECではNIST（米国立標準技術研究所）のセキュリティガイドラインを参考に、お取引先向けのセキュリティ基準を改訂するなど国際標準に沿った対策を行い、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（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）。

さらに、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、いち早く時代の流れに対応できるセキュリティの実現を目指しています。

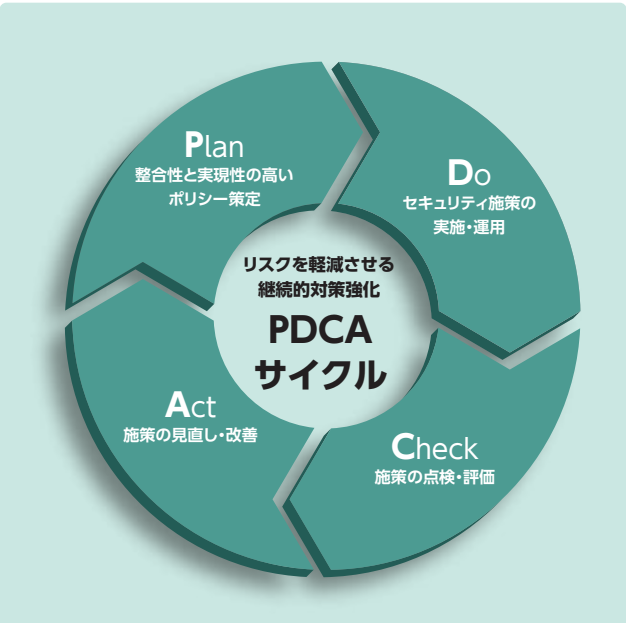
■ DX時代におけるサイバーセキュリティ（NEC）
https://jpn.nec.com/cybersecurity/nec_cybersecuritywhitepaper202004.pdf

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



「OODAループ」によるスピーディなインシデント対応

DX/クラウドシフトによる新たなセキュリティリスクへの対応

DXの要であるクラウドシフトが浸透する中、安全性確保への社会的要請が強まっています。
DX時代におけるクラウドのセキュリティリスクへの対応、およびお客さまが安全にDX/クラウドシフトを進めるために、NECグループの支援体制についてご紹介します。

1 DX/クラウドシフトによるリスクの変化

❶ セキュリティリスクの変化

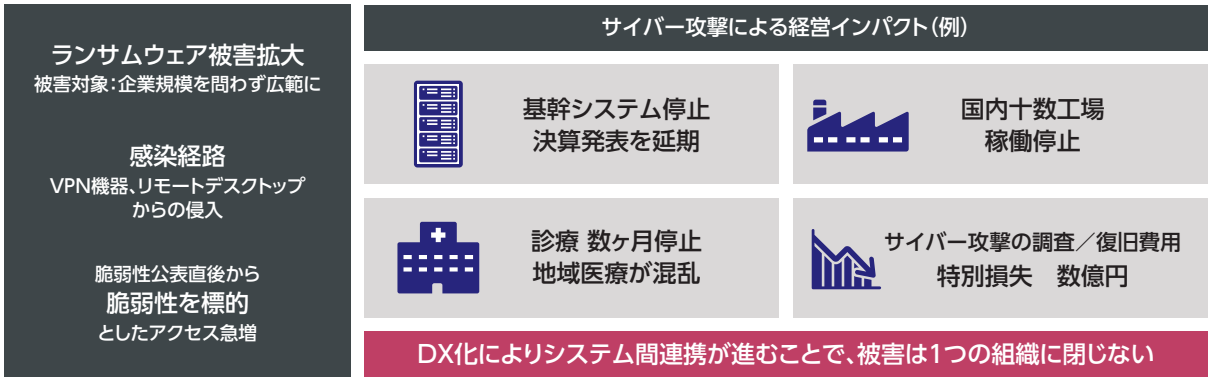
地政学的な状況の変化とともに民間企業も国家的なサイバー攻撃の標的になっており、先端技術情報等を保有する企業はセキュリティリスクが増大しています。また、DXが急速に進む一方で経済目的のサイバー攻撃が激化し、あらゆるシステムやデータが標的となり企業の事業継続が脅かされています。DXによりシステム間の連携が進み、被害が1つの組織にとどまらないことも最近のセキュリティリスクの傾向として挙げられます。

❷ クラウド環境におけるセキュリティリスク

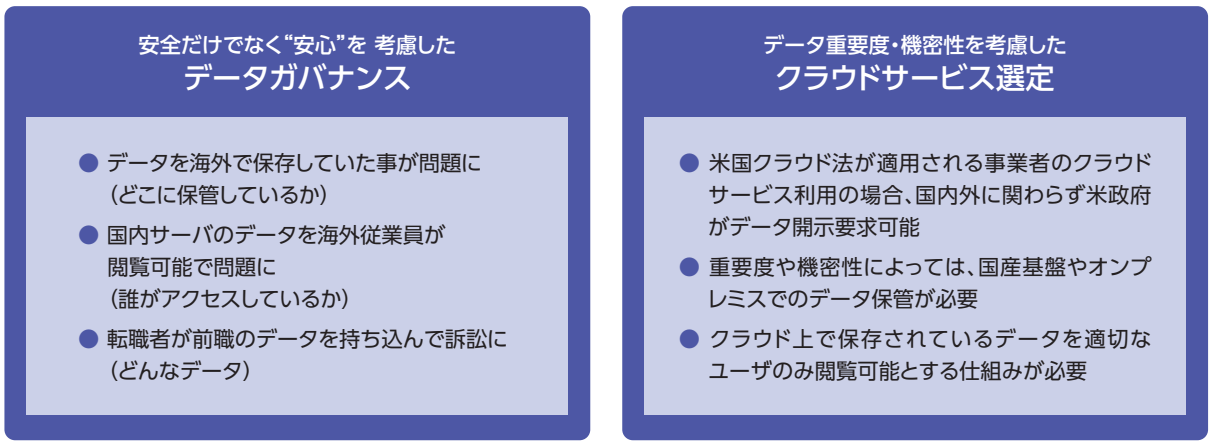
守るべき情報がオンプレミスからクラウド上へ移行し、社外からのリモート接続の増加により、従来のネットワーク境界が中心の対策は限界を迎えつつあります。データが随所に分散し、場合によってはクラウド上のデータが正しく運用されない恐れもあります。したがって、技術的な安全性だけでなく利用者の安心を考慮したデータガバナンスと、データ重要度・機密性を考慮したクラウドサービスを選ぶことが重要です。

また、クラウド環境では意図しない設定に起因するインシデントも発生しています。脆弱性情報を事前に認識していたにもかかわらず、クラウドの運用面の不備によりサイバー攻撃を防げず、大量の個人情報漏えいから企業価値の毀損・訴訟と経営問題へ発展する可能性もあるため、今まで以上に設計段階からの運用計画が重要になります。

セキュリティリスクの変化



クラウド環境におけるセキュリティ課題

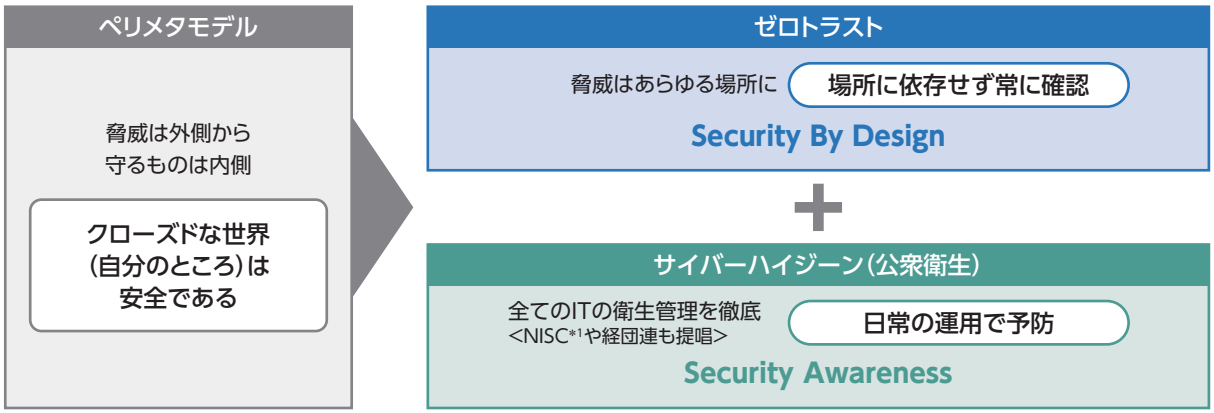


2 アーキテクチャーとともに変化するセキュリティ

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な考え方でした。しかし、DXの世界では脅威はあらゆる場所に存在し、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)”の考え方がベースとなります。

DXを支えるセキュリティベース



*1 NISC: 内閣サイバーセキュリティセンター

❷ 対策が必要なポイント

DX/クラウドシフトによるセキュリティの課題と対策が必要なポイントは、次の4点になります。

課題	対策すべきポイント
・境界防御の限界、ゼロトラストの考え方ですべてのアクセスを検査 ・SaaS利用の加速と、マルチクラウド化によるID管理の最適化	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、ユーザ、アプリケーション、デバイスなどの識別と、多要素認証導入によりセキュリティを強化 ・シングルサインオンによるシームレスかつセキュアなサービスを実現するため、オンプレミスとクラウドサービスのID統合管理を実施
・クラウドシフトで分散しているデータの格納場所や、アクセス元に対するガバナンス ・クラウドサービス上のデータ保護に関する、ユーザの管理負荷軽減	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と体制構築を行うことでガバナンスを実現
・クラウドサービスの頻繁な機能アップデートに追随した設定管理 ・サービス仕様の理解不足による設定ミスの抑止	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、設定不備などを継続的に可視化して自動是正
・システム環境の変化への対応(境界防御型からゼロトラスト型) ・エンドポイント、クラウドワークロード、SaaS等多岐にわたる監視運用対象機器の設計最適化	運用管理:Security Operation By Design (SOBD*2) ・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すえたSOBDを実施

*2 SOBD: 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。

3 安全にDX/クラウドシフト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や知見が、“生きたナレッジ”として集約・蓄積されており、そのノウハウを付加価値としてお客さまに提供しています。

❷ 統合ID・アクセス制御

オンプレミスと各種クラウドサービスのID管理をはじめ、シングルサインオン（SSO）、多要素認証、コンテキストベース認証、アクセス制御を実現するクラウドベースのIDaaS*3のソリューションを提供します。これにより、ゼロトラスト環境におけるID統合とアクセス制御を実現します。

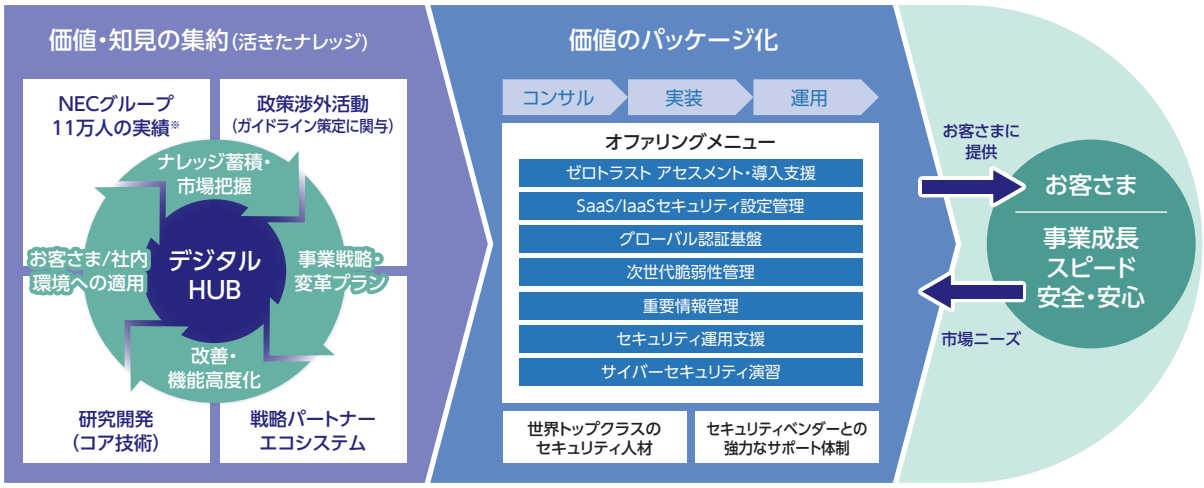
*3 IDaaS：ID as a Service

❸ 情報ラベリング・暗号化

情報（ファイル）単位での暗号化・アクセス管理が可能なAIP*4統合ラベルを用い、AIPとInfoCage FileShellでファイルの自動分類とデータ暗号化を行います。データの重要性に応じたデータ分類と適切な保護の自動化を実現し、利便性と操作性が向上します。

*4 AIP：Microsoft Azure Information Protection

安全にDXを推進するためのオファリングを提供



※オファリング化予定も含む

AIP統合ラベルによる情報ラベリング・暗号化

実施内容

- 企業秘密管理規程を踏まえたファイルのラベリング
- 情報区分に応じた自動暗号化とアクセス管理（Officeファイル以外も含む）

実現価値

- クラウドや、リモートPCからデータが流出しても情報漏えいを防げる
- 情報区分応じた印刷禁止、添付禁止、保管場所の制御

AIP　クラウドベースのデータ保護ソリューション　AIP

- コンテンツにラベルを適用してドキュメントや電子メールの検出、分類、および保護

検出　分類　保護　監視

＋

AIPの運用性を強化する　InfoCage Fileshell

- OfficeやPDF以外も拡張子を変えずに暗号化、利便性維持
- ローカルやファイルサーバ格納時の自動保護

❹ IaaS/SaaSセキュリティ設定管理 プロフェッショナルサービス

クラウド利用が進むにつれ、SaaSやIaaSの機能は高度化・複雑化しています。お客さま自身が、クラウドの利用実態を把握し続けることが困難となり、セキュリティ設定不備によるインシデントが多発しているのが現状です。NECでは、IaaS/SaaSのセキュリティアセスメントを行うことでリスクを可視化し、設定の改善、運用までをサポートするCSPM*5/SSPM*6を活用したプロフェッショナルサービスを提供しています。

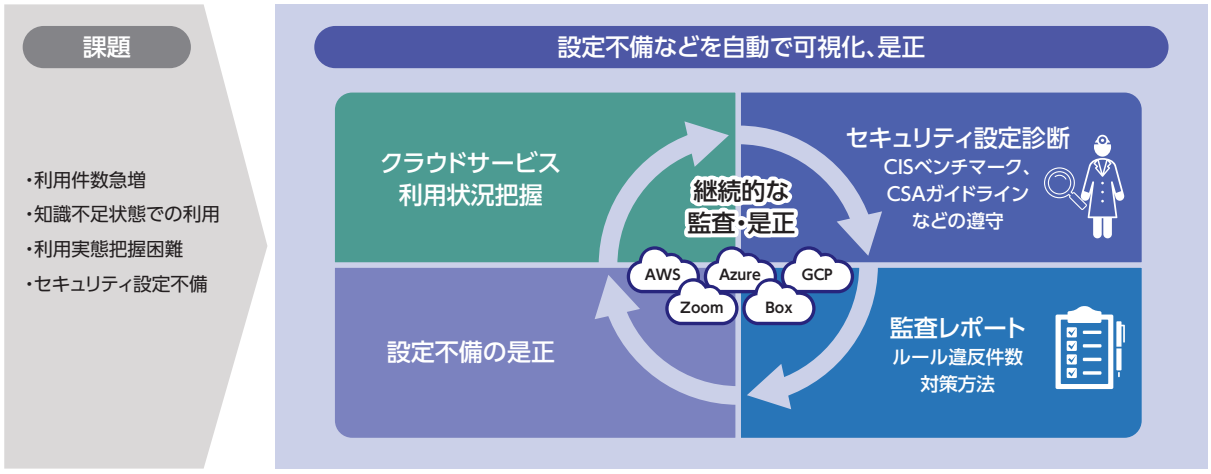
*5 CSPM: Cloud Security Posture Management
*6 SSPM: SaaS Security Posture Management

❺ プロフェッショナルサービスのデリバリ事例

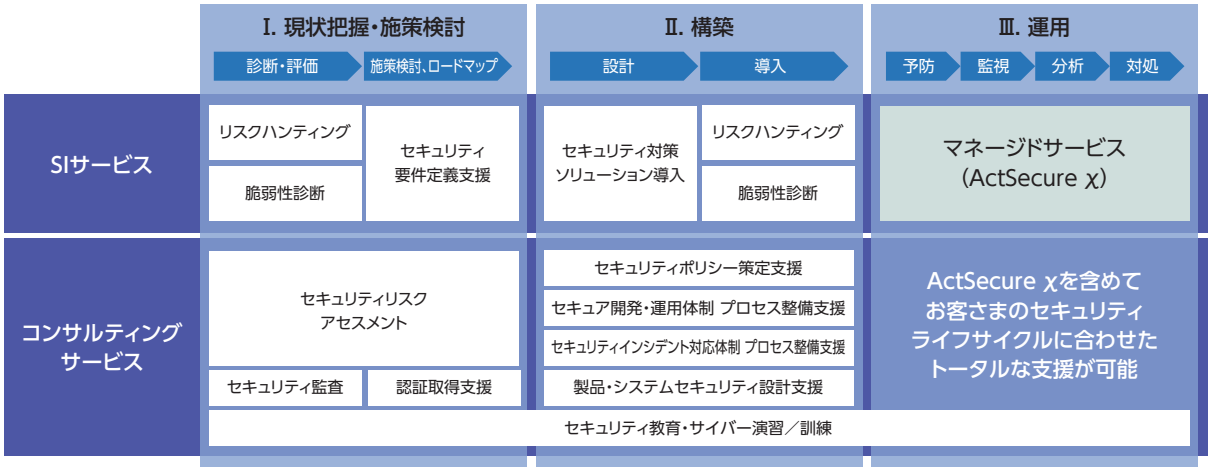
NECは、上流工程からお客さまの計画策定や技術面でのアドバイザリーを実施しています。また、新たな脅威や課題をお客さまと共有し、その対策や改善の継続的なご提案を通じて、高品質なセキュリティ運用監視を実現しています。

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、セキュリティリスクは逆に増大しています。脆弱性問題や誤設定によるインシデントが多発し、改めて組織のガバナンスが問われています。インシデント発生時にも、説明責任を果たせる状態を維持し迅速に事業を継続するためには、ID管理・情報管理・設定管理・運用管理の4点が重要です。DX/クラウドシフトにおけるセキュリティソリューションについての詳細は、お気軽にNECまでお問い合わせください。

クラウド設定ミス防止への対策



プロフェッショナルサービス



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、以下にご紹介します。

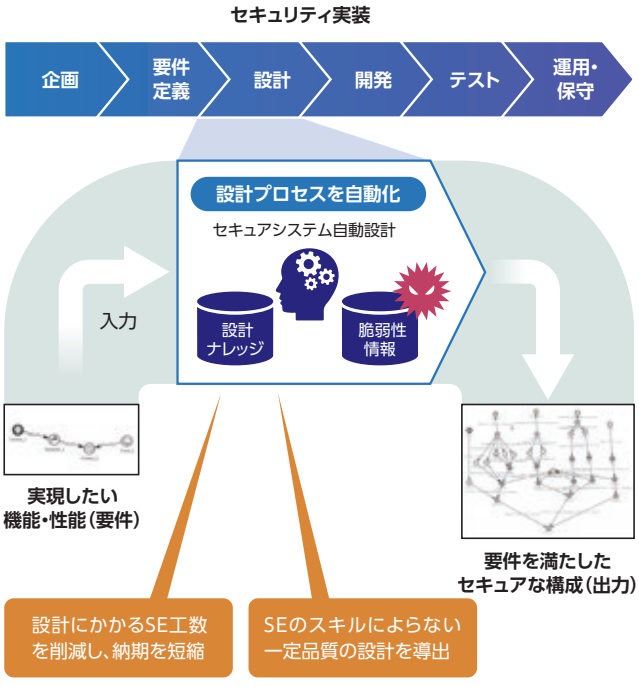
2 セキュアシステム自動設計

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。

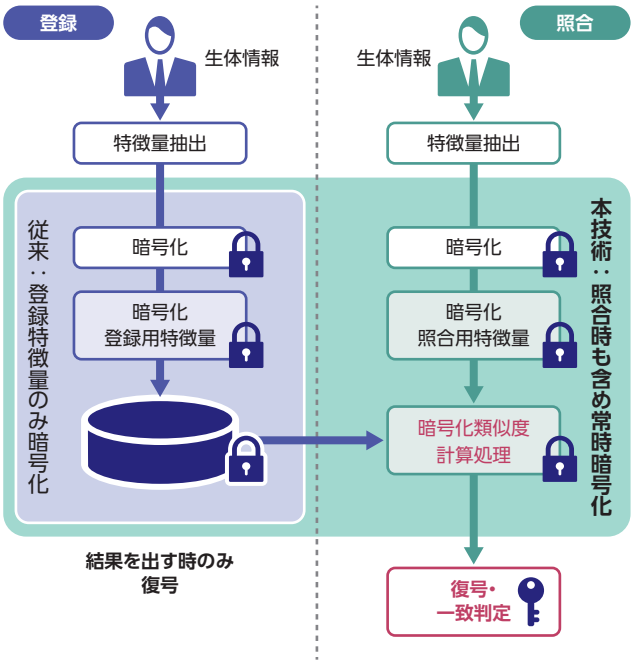
セキュアシステム自動設計技術は、セキュリティを考慮したICTシステムの設計を自動化します。ICTシステムに求められる機能や性能(要件)をもとに、AIがICTシステムを構成する部品を自動で組み合わせて評価することで、要件に合ったシステム構成を導出します。システムの脆弱性や攻撃経路成立のリスクを診断しながら、部品を組み合わせることで、システムの脆弱性をついた攻撃が成立しないようなシステム構成を導出できます。

本技術により、これまで多くの工数を要したセキュアシステムの設計を自動化し、システムの設計・開発、運用を支援します。

セキュアシステム自動設計による設計プロセスの自動化



秘匿生体認証を用いた生体特徴量の保護



3 秘匿生体認証

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

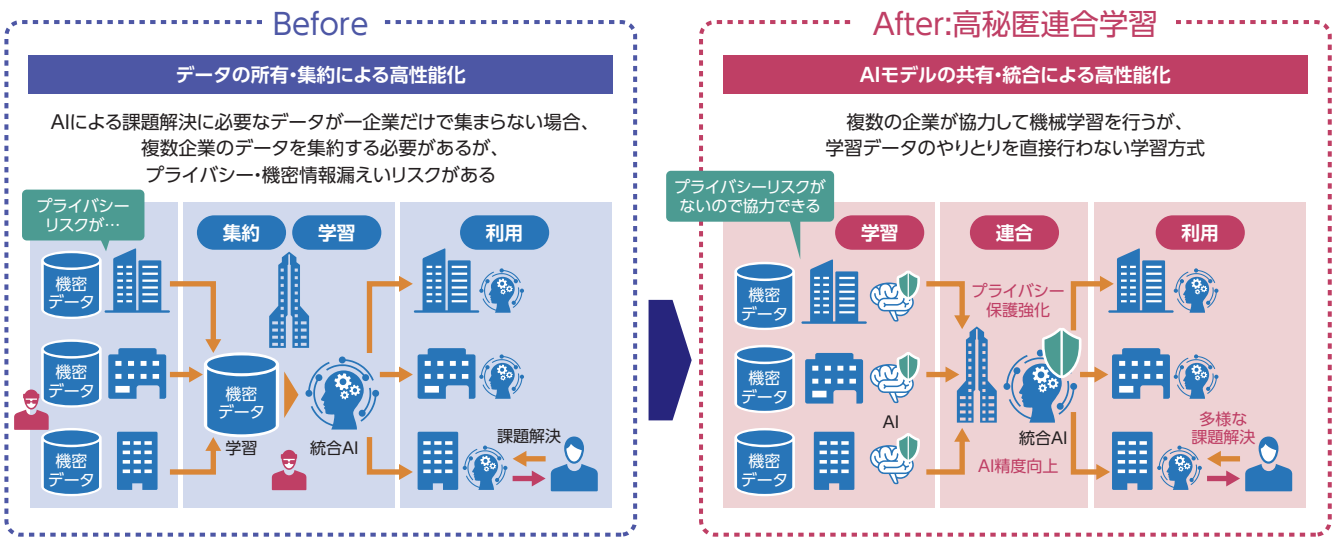
秘匿生体認証では、特徴量を暗号化したまま顔認証の照合処理を実現するため、マルチパーティ計算や準同型暗号による秘密計算技術を活用しています。大規模な利用シーンにおいては、マルチパーティ計算を用いた方式が適しており、登録ユーザ数100万人程度で1秒以内の顔認証の照合処理を行うことが可能です。また、中～小規模の利用シーンでは1台のサーバで提供可能な準同型暗号を用いた方式が適しており、登録ユーザ数1万人程度で1秒以内の顔認証の照合時間を実現しています。

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全・安心な利用に貢献します。

4 高秘匿連合学習

AIの精度向上には偏りのない大量のデータが必要ですが、このようなデータを自組織だけで確保できない場合に、対象データの企業秘密や個人情報を保護した上で、他組織のデータも活用して高精度なAIを構築する手法が連合学習です。連合学習では、自他組織のデータを一カ所に集めることなく、それぞれのデータを自組織で学習し、その結果を統合することで高精度なAIを構築します。これにより学習に用いたデータが外部に直接漏えいすることはありませんが、AIモデル経由で学習データを推測する攻撃が存在します。これに対して、高秘匿連合学習ではモデル統合者からの攻撃については秘密計算によって保護し、各組織からの攻撃については攻撃シミュレーションを活用して耐攻撃性の高い学習を実現することで保護可能にします。また、画像処理AIだけでなく、テーブルデータや系列データを扱えるAIについても連合学習を実現するとともに、組織間でデータに偏りがある場合での対策・改善を行うことで、高精度で多様な課題解決とセキュリティの両立を目指しています。

高秘匿連合学習による高精度AIモデルのセキュアな構築



第三者評価・認証

NECでは、情報セキュリティに関連する第三者評価・認証に積極的に取り組んでいます。

1 ISMS認証の取得状況

情報セキュリティマネジメントシステム国際規格ISMS（ISO/IEC27001）認証を取得した組織を持つ会社は、以下のとおりです。

ISMS認証取得組織を持つグループ会社

- 日本電気株式会社
- アビームコンサルティング株式会社
- アビームシステムズ株式会社
- NECスペーステクノロジー株式会社
- NECソリューションイノベータ株式会社
- NECチャイナ・ソフトジャパン株式会社
- NECネクサソリューションズ株式会社
- NECネッツエスアイ株式会社
- NECネットワーク・センサ株式会社
- NECフィールディング株式会社
- NECフィールディングシステムテクノロジー株式会社
- NECプラットフォームズ株式会社
- 株式会社インフォセック
- 株式会社KIS
- 株式会社サイバーディフェンス研究所
- 株式会社サンネット
- 株式会社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

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
- リバンスネット株式会社

3 ITセキュリティ評価認証の取得状況

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

ISO/IEC15408認証取得製品・システム

- DeviceProtector AE
（情報漏えい防止ソフトウェア）
- InfoCage PCセキュリティ
（情報漏えい防止ソフトウェア）
- NECグループ情報漏洩防止システム
（情報漏えい防止ソフトウェア）
- NECグループセキュア情報交換サイト
（セキュア情報交換サイト）
- NEC ファイアウォール SG
（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

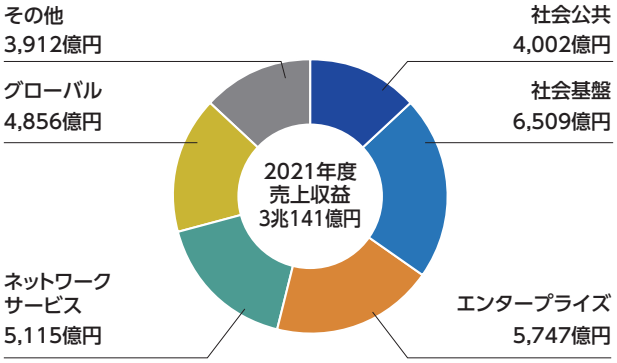
会社概要

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	117,418名※
連結子会社数	289社※

※2022年3月31日現在

事業紹介

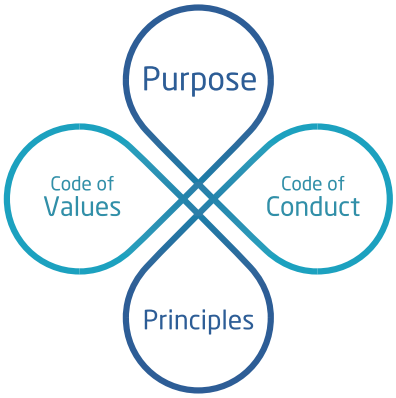
セグメント別売上収益



※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2022

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

2022年７月発行

Cat.No. U04-22070016J