\Orchestrating a brighter world NEC

情報セキュリティ報告書 2020

Information Security Report 2020

NECが考える情報セキュリティ

NECは、「情報セキュリティ」を事業継続の重要な経営基盤として位置づけ、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）

近年、DX*1によって新たなビジネスモデルやスキームが生み出され、社会は大きな転換期を迎えています。「働き方改革」の浸透による新たなワークスタイルの実現は、企業の成長やイノベーション創出につながる一方で、多くの解決すべきセキュリティ課題を生じています。特に新型コロナウイルス感染症（COVID-19）の影響により社会のあり方が変化する中、New Normalを見据えた取り組みが必要です。

NECは、このような社会的状況を踏まえ、情報セキュリティを事業継続のための重要な経営基盤として位置づけ、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*2のCyber Security Framework（1.1版）に準拠しながら、高度化するサイバー攻撃への対策、製品・システム・サービスの高品質なセキュリティの確保、サプライチェーン全体での情報セキュリティ対策などを推進しています。

対策にあたっては、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など各領域からの総合的アプローチによる取り組みを行い、社会から継続的に信頼される企業になることを目指しています。

- NECグループが一体となった情報セキュリティ管理体制、リスクに備えた仕組みの構築、PDCAサイクルの実施
- サプライチェーン全体を含めたセキュリティ管理・施策を展開、状況把握体制の確立
- 情報保護と情報活用・共有の安全かつ適切な両立
- 独自のAIや自動化技術を備えたセキュリティソリューションを、社内で実証して提供
- インシデント発生時の対応、復旧体制整備によるアカウンタビリティとサイバーレジリエンシーの確保、レピュテーションリスクの低減

NECは、ブランドステートメントに「Orchestrating a brighter world」を掲げ、さまざまな社会課題をICTの力で解決し、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てまいります。本報告書では、それらICT事業に関わる情報セキュリティへの取り組みをご紹介していますので、ぜひご一読いただければ幸いです。

*1 DX: Digital Transformation の略称で、実世界の出来事をデジタル化してサイバー世界に取り込み、人・モノ・コトをつなげて新しい価値を生み出し、生活やビジネスをより良く変えていくこと。
*2 NIST: National Institute of Standards and Technology　米国標準技術研究所

本報告書に関するお問い合わせ

日本電気株式会社
経営システム本部 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）

「情報セキュリティ報告書 2020」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、2020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

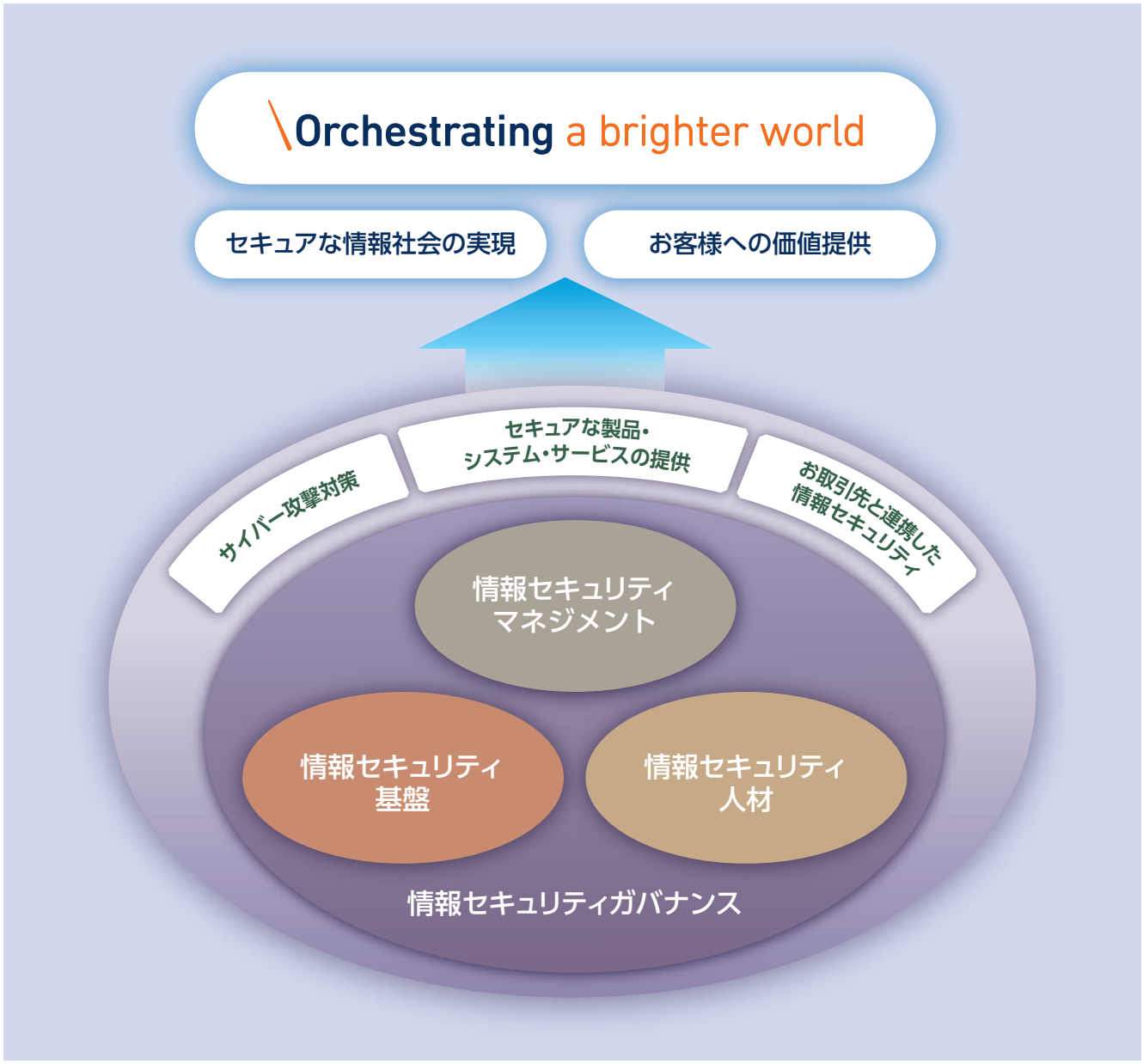
情報セキュリティ推進フレームワーク

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は、社会から信頼される企業としてその責任を果たすため、「情報セキュリティ推進フレームワーク」を確立し、お客さまやお取引先からお預かりした情報資産を守り、セキュアな情報社会の実現を通じて、お客さまや社会へ価値を提供します。

NECでは、サイバー攻撃対策、セキュアな製品・システム・サービスの提供、お取引先と連携した情報セキュリティ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は、グループ全体で「NECグループ経営ポリシー」を定め、各種ルールの共通化と制度・業務プロセス・インフラの統一を行い、グローバルスタンダードな経営基盤を確立しています。

情報セキュリティガバナンスに基づき、経営層はセキュリティ目標を定めグループ施策、体制構築、経営資源の割り当て方針を決定します。そして、組織レベルでの施策の進捗・達成状況や情報セキュリティ事故の状況をモニタリングし、要求事項への適合性の評価、必要な指導や仕組みの改善により新たな方向付けを行います。

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

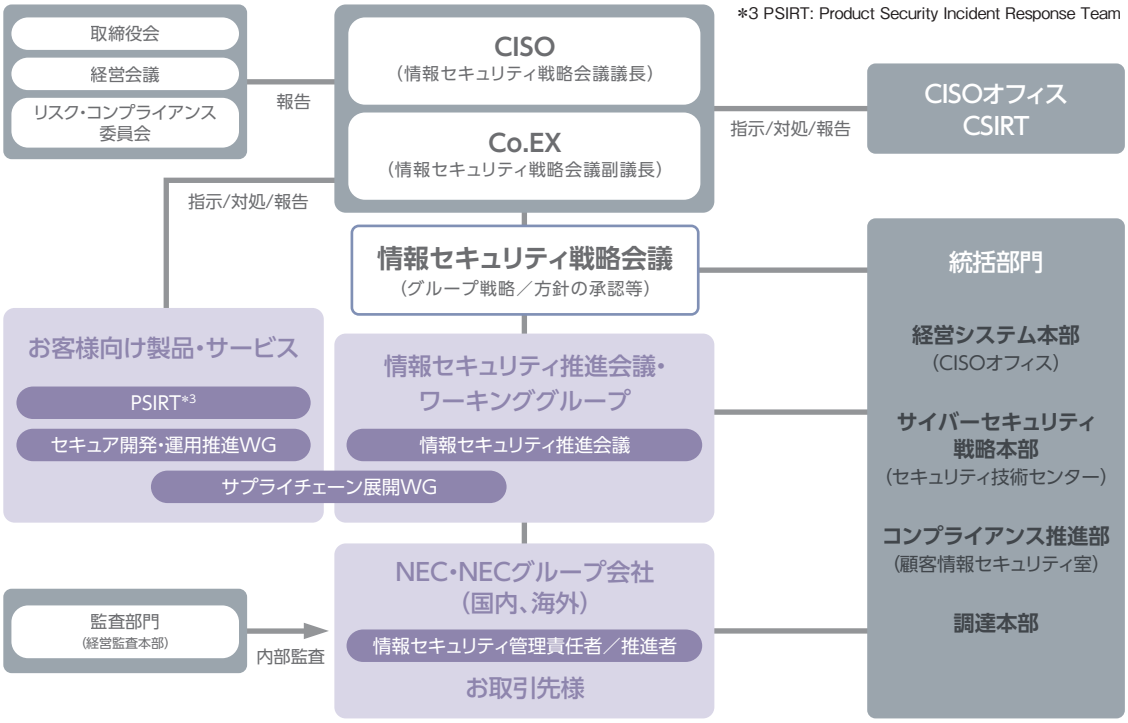
本体制は、情報セキュリティ戦略会議と下部組織、各関連組織で構成されます。情報セキュリティ戦略会議はCISO*1が議長を務め、情報セキュリティ施策の審議・評価・改善、事故の原因究明と再発防止策の方向付け、情報セキュリティビジネスへの成果活用などを審議します。また、ここで決定した施策の運営状況は、定期的に社長に説明し、了承を得ています。

CISOを補佐するコーポレート・エグゼティブ(Co.EX)は、サイバーセキュリティ対策を推進するCISOオフィスと、サイバー攻撃を監視しインシデント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、セキュア開発・運用の推進計画、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。

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

NECグループ情報セキュリティ推進体制



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、「情報セキュリティ基本方針」を公開し、情報セキュリティ基本規程、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、「NEC個人情報保護方針」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。2017年に施行された改正個人情報保護法とJISQ15001改定についても、個人情報保護規程やマニュアル改定、GDPR*1準拠のNECガイドラインの改定を実施しています。

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29社（2020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 GDPR: General Data Protection Regulation　EU一般データ保護規則

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「情報セキュリティ対策基準」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「情報セキュリティリスク評価基準」による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

NECの情報セキュリティマネジメント

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。重大事故は、専門アドバイザーの参加により、対応費用や影響度を数値化するインパクト分析も行います。結果は経営層に報告し、全社へ横展開します。

4 情報セキュリティ点検

❶ 情報セキュリティ点検の内容

情報セキュリティ事故を分析し、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ます。対策実施の有無や実施不可の状況を回答形式にし、個人へ気づきや是正を促します。具体的には秘密情報や個人情報の安全管理、外部委託先管理、標的型攻撃メール対策、セキュア開発・運用などを点検します。

❷ 情報セキュリティ点検の方式

情報セキュリティ推進者が、組織全体をチェックする「組織点検」と、個人が対策の実施状況を回答する「個人点検」があります。個人点検は、従業員と管理者を対象に実行面と管理面を点検し、両者のギャップを分析することで精度の向上をはかります。

❸ 点検結果の活用による改善

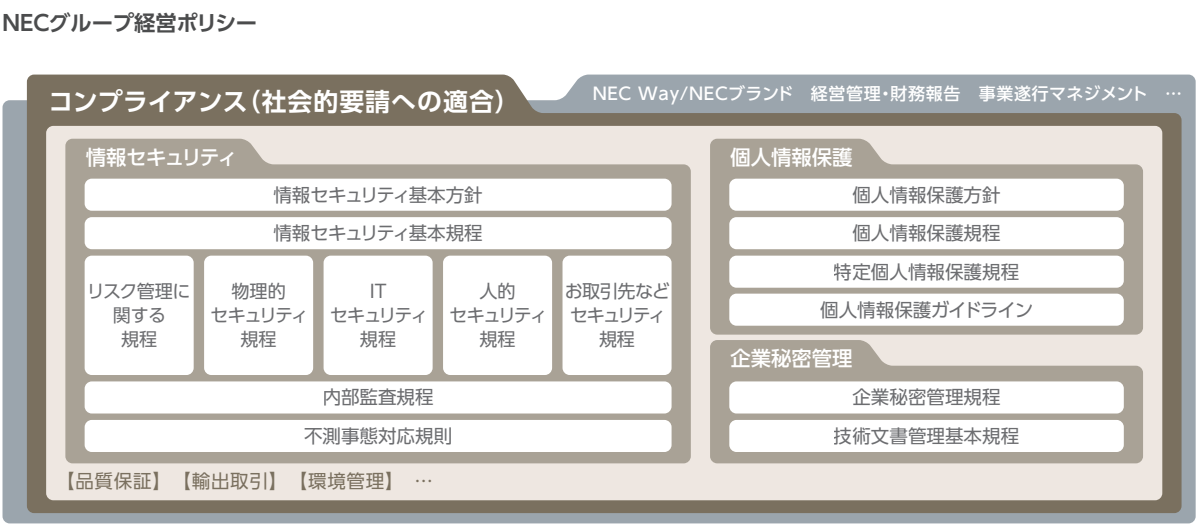
実施が不十分な項目は、その理由を把握して改善し、全社の傾向分析を経て残課題を解決します。さらに強化が必要な場合は、次年度の情報セキュリティ推進計画で継続的に取り組みます。

5 情報セキュリティ監査

経営監査本部が中心となり、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実施します。ISO/IEC27001やJISQ15001に照らし、各組織の状況を定期監査します。

6 ISMS認証取得の取り組み

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



情報セキュリティ基盤

お客さまのかけがえのない個人情報や機密情報を守るために、NECではゼロトラストの考え方に基づき、事業やプロジェクトを安全・安心かつ効率的に推進できる情報セキュリティ基盤を構築・運用しています。

1 情報セキュリティ基盤の特長と構成

情報セキュリティ基盤は、「利用者を管理・統制するICT基盤」、「PC、ネットワークを守るICT基盤」、「情報を守るICT基盤」の3つの柱からなり、これらが相互に連携し補完し合いながら、NECの情報セキュリティポリシーを実現しています。

2 利用者を管理・統制するICT基盤（認証基盤）

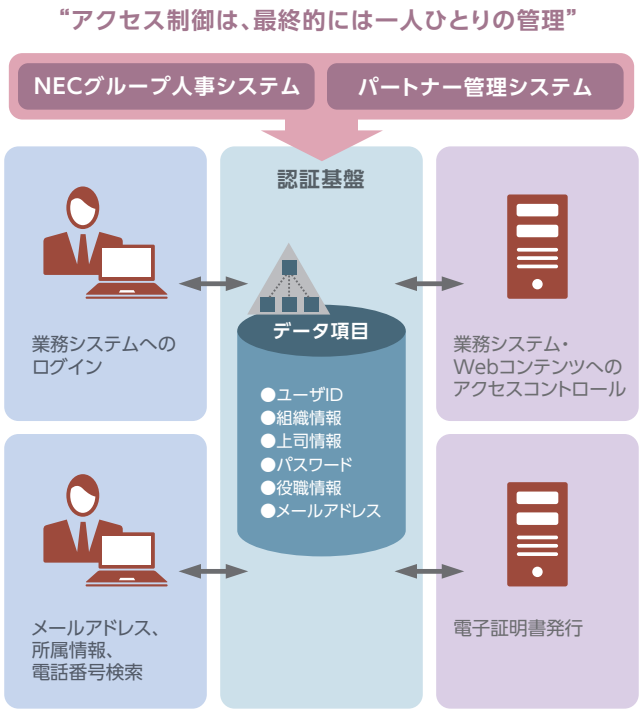
情報セキュリティにおける管理の基本は、個人を認証する仕組みです。人を特定し認証することで、情報資産への適切なアクセスコントロールや電子証明書を利用したなりすまし防止などを実現できます。

情報資産の適切な管理には、利用者の特定・認証と利用者に応じた権限の付与が重要です。NECは、社員だけでなく必要に応じてお取引先なども含め、認証と認可（権限付与）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。

認証と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と認可に用いる情報が、どのシステムでどのような目的で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のアクセス制御は、ユーザIDとパスワード（記憶認証）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）の導入も推進しています。

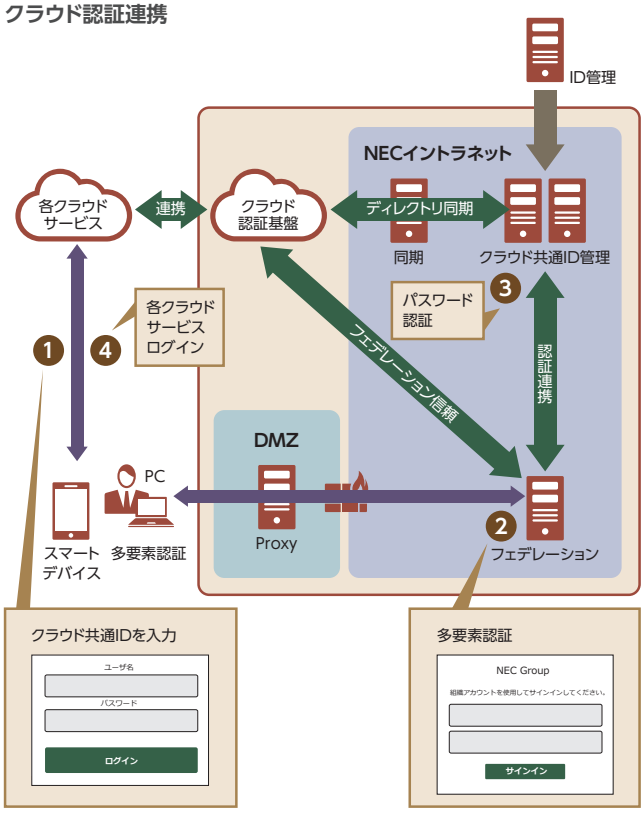
クラウドサービスの認証では、社内の認証基盤と連携して社内外サービスとのシームレスな認証を実現しています。外部との情報共有やクラウドサービスの利用ニーズに対し、安全・安心に利用できる仕組みを整備しています。

NECグループ認証基盤



●**情報は必要な人のみ開示**
●**アクセス制御**（個人単位に認証し社内システムの利用やWebコンテンツの参照を許可）
●**シングルサインオン**

クラウド認証連携



3 PC・ネットワークを守るICT基盤

NECイントラネットに接続される情報機器のセキュリティを維持し、ウイルスやワームからPC・ネットワークを守るICT基盤をグローバルに整備しています。近年、リスクが高まっている標的型攻撃に対しては多層的な対策が不可欠であり、情報機器に対してセキュリティ更新プログラムやウイルス対策ソフトを確実に適用することが重要です。

❶ ウイルスやワームからPCを守る

●ユーザ利用環境支援

イントラネットでは、PC・ネットワークの状態を把握するソフトウェアの導入を義務化しており、ネットワークやPCの状態を見える化することで、セキュリティリスクを可視化し、すべてのPCに必要なセキュリティ対策ソフトがインストールされているかどうかを即座に確認可能です。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、使用を禁止する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ユーザごとに監視しています。

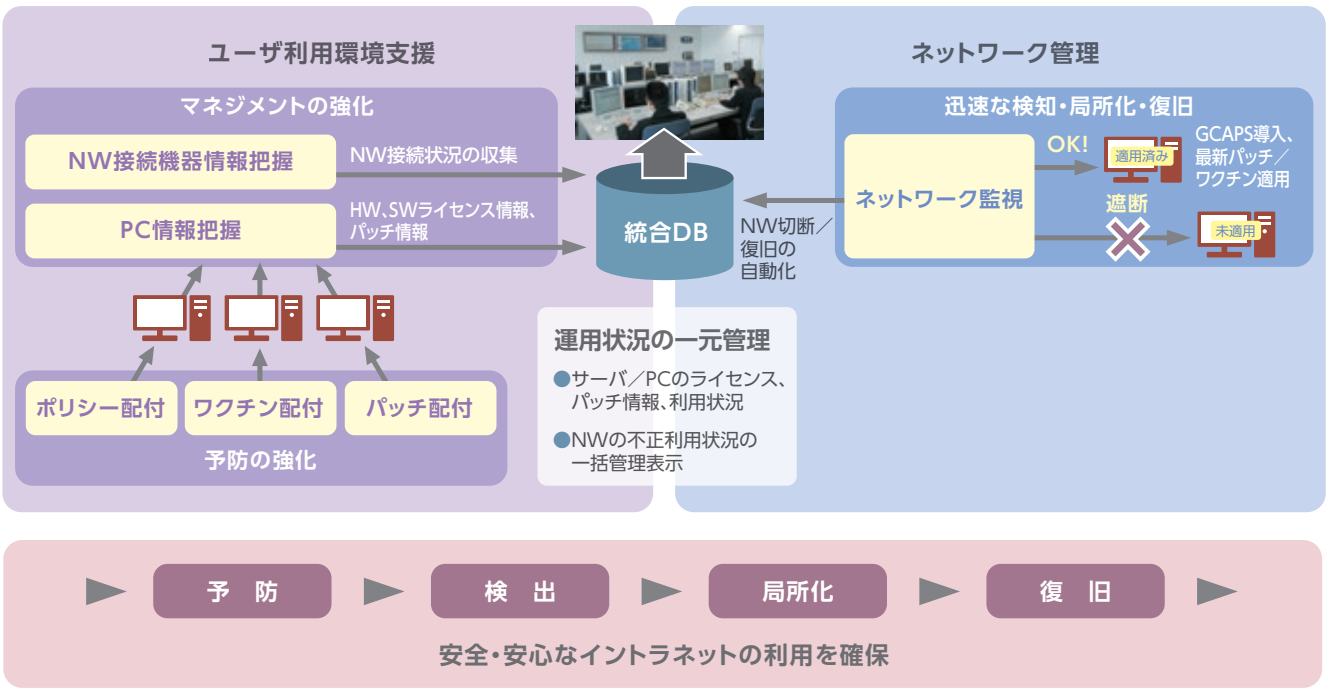
●ネットワーク管理

PCの状態を見える化すると同時に、セキュリティ対策が不十分なPCがイントラネットに接続されたり、イントラネット上でワームが検知された場合は、該当するPCやLAN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、アクセス禁止カテゴリによる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。

●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など、セキュリティ対策の実施状況に関するデータを管理システムへ集約し、情報セキュリティの管理責任者や推進者が各事業部門の対応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、各種施策の迅速で円滑な推進を徹底化しています。

ウイルス、ワームからPC、ネットワークを守る



4 情報を守るICT基盤

情報漏えいの防止には、情報流出につながる経路を特定し、リスク分析の上で適切な対策が必要です。NECでは自社情報以外にも、お客さまとお取引先の大切な情報を管理しているため、ICT機器の特徴やリスクを考慮し、情報流出につながる経路に対して網羅的かつ多層的な対策を行っています。

❶ NECグループ 情報漏えい防止システム

NECの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、外部攻撃や内部不正による情報漏えいのリスク対策を行っています。

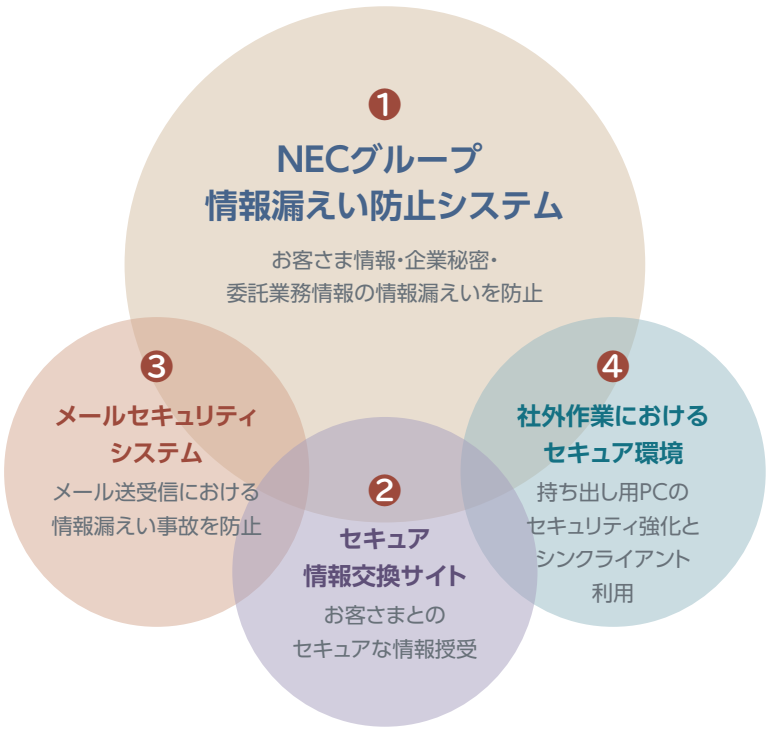
「暗号化」は、PCハードディスクとファイルの暗号化を行い、盗難・紛失による情報漏えいを防止します。ファイル暗号化は、アクセス権や利用期限を設け、デフォルトのセキュリティレベルとしてNECグループ全体で設定しています。したがって、マルウェア感染で外部に情報が送られたり、メールで情報を誤送信したりしても、暗号化されているため漏えいしません。

「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、情報の書き出しを禁止する利用制限をしています。また、業務でデバイスが必要な場合は、組織や利用者ごとにデバイスおよび利用制限を定義し、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ます。万が一、情報漏えい事故が発生した場合、ログを分析することで事故による影響範囲の特定や状況把握などの分析、再発防止策の策定などに威力を発揮します。

また、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事業上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。具体的には脆弱性情報収集・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、委託先管理などを実施しています。

情報を守るIT基盤の全体像



❷ セキュア情報交換サイト

お客さまやお取引先と重要な情報をやり取りするため、安全・安心な「セキュア情報交換サイト」を構築・運用しています。同サイトでは、ワンタイムURLとパスワードを設定し、アクセスが制限されたエリアで情報をやり取りできます。ワンタイムURLには有効期間があり、期限が過ぎるとURLは無効になります。また、利用終了とともに同サイト上から情報が削除されます。

セキュア情報交換サイトにより、USBメモリなどの外部記憶媒体による情報の交換機会が減り、盗難・紛失による情報漏えい事故のリスクが軽減します。

❸ メールセキュリティシステム

「OMCA*1」は、メール送受信における情報漏えい事故を防止します。
標的型攻撃の疑いがある不審メールに対して注意を喚起する機能や、メールの送信前に宛先と添付ファイルを確認する画面をポップアップする機能、メールを送信する際、設定時間分送信を遅延させる機能などを備えており、メールからの情報漏えいを防止しています。

＊ OMCA：Outlook Mail Check AddIn

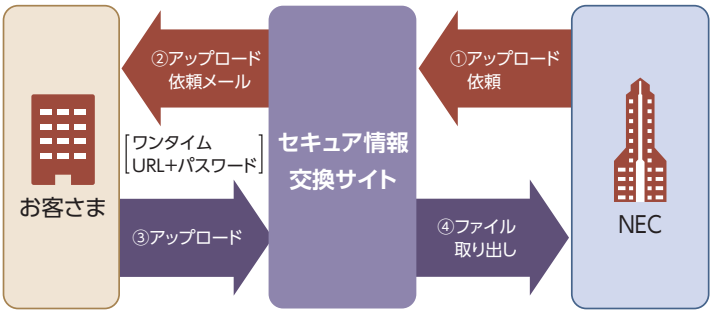
❹ 社外作業におけるセキュア環境

NECでは、情報セキュリティ事故を防ぐために、社外での安全なデジタルワークプレイス環境(詳細はP20の「デジタルワークプレイス環境の創造」を参照)を構築しています。

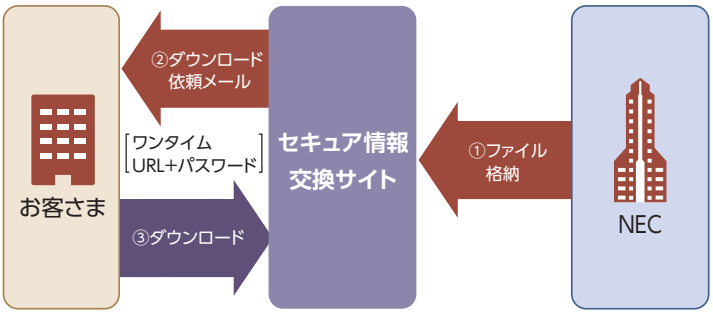
PCの社外持ち出しでは、目的や利用環境などにより「シンクライアント」や、PC内の情報保護を強化した「Trusted PC」などを利用します。Trusted PCは、「HDD全体の強固な暗号化」や「OS起動前のプリブート認証」、「遠隔からのデータ消去とPCのロック」、「未知の脆弱性に対する攻撃の緩和」、「オートランウイルス対策」などの機能を備えており、高度化するサイバー攻撃に対応できるよう設計されています。

セキュア情報交換サイト

アップロード(送信)イメージ図



ダウンロード(受信)イメージ図



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のと同時に、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「知識、意識の向上」、「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 情報セキュリティの知識、意識の向上

情報セキュリティの維持・向上をはかるには、情報を適切に取り扱うための知識や情報セキュリティに対する高い意識が重要であり、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教育を実施し、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、内部不正防止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、「お客さま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、職場懇談会などを通じて、リスクに対する分析力・判断力の向上をはかっています。

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。300名超（2019年度）のエンジニアが利用し、お客さまのシステムを担うセキュリティ技術を強化しています。

❷ 全社的CTFの実施

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。2019年度は約1,000名が自主的に参加し、セキュリティ人材の裾野拡大を促進しています。

*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WBT形式で提供します。NECグループ全体のセキュリティスキルの底上げをはかります。

❹ SBDスペシャリスト

各事業部門でSBDを実践する専門人材の育成を、2019年度から新たに開始しました。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）

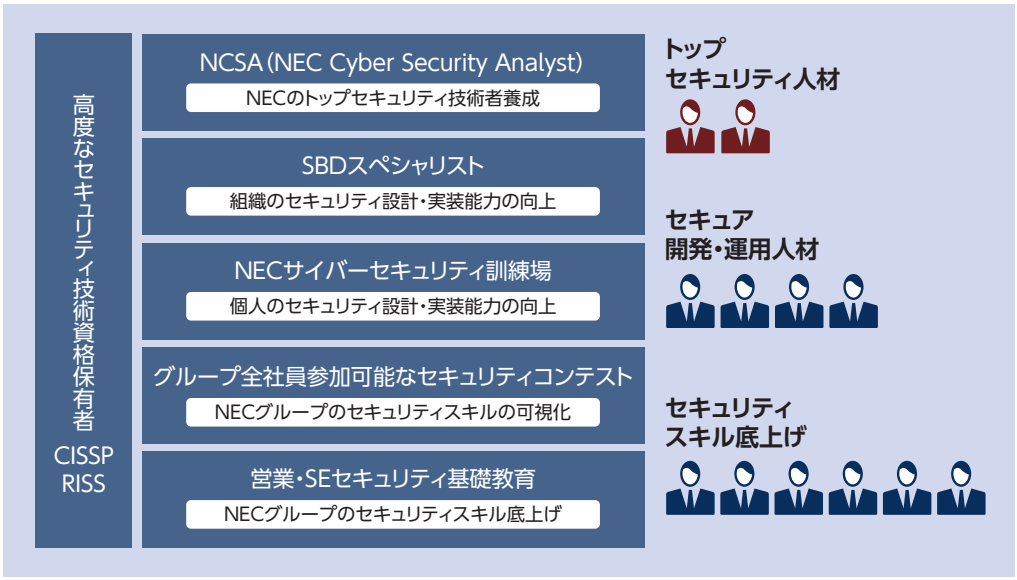
従来のNEC CISO補佐官トレーニングに対し、より実践的な内容に強化したNCSA（NEC Cyber Security Analyst）プログラムを2020年度から開始しました。トップセキュリティ人材の強化を目的とし、セキュリティ技術の知識を持つ人材を対象に、CSIRT*5業務やリスクハンティングなど高度なセキュリティサービスに必要なテクニカルスキルを、半年間の集中プログラムで習得します。

*5 CSIRT：Computer Security Incident Response Team

❻ 高度なセキュリティ技術資格保有者

セキュリティ公的資格の取得を強く推奨しており、国際資格であるCISSPやRISSの取得者を拡充しています。そして、情報セキュリティに関する高度なスキルや資格を有するスタッフが核となり、お客さまへの最適なソリューションを提供します。

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・巧妙化するなか、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 サイバー攻撃対策

サイバーセキュリティリスク分析による先進的な対策を国内外で一律に行うとともに、CSIRT*1によりインシデントに対応し、サイバーレジリエンシーを確保しています。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: National Institute of Standards and Technology Cyber Security Framework
NIST（米国標準技術研究所）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 サイバーセキュリティリスク分析

標的型攻撃、ランサムウェア、BEC*3、ばらまき型メール攻撃*4など、サイバー攻撃の脅威に対して4つのリスク分析を行い、その結果に基づきサイバー攻撃対策を実施しています。

*3 BEC: Business E-mail Compromise　ビジネスメール詐欺

*4 ばらまき型メール攻撃: 不特定多数を狙った攻撃

❶ サイバー脅威分析

日々のサイバー攻撃の監視やマルウェア解析、脅威インテリジェンスの活用で、攻撃状況や攻撃の特徴を把握します。また、脅威リスクレベルを判断し、状況に応じた対処を検討します。

❷ 監視運用分析

監視運用のプロセスを適宜見直し、変化するサイバー脅威動向に追随する運用を検討するとともに、運用上の課題を把握します。

❸ ソリューション・IT分析

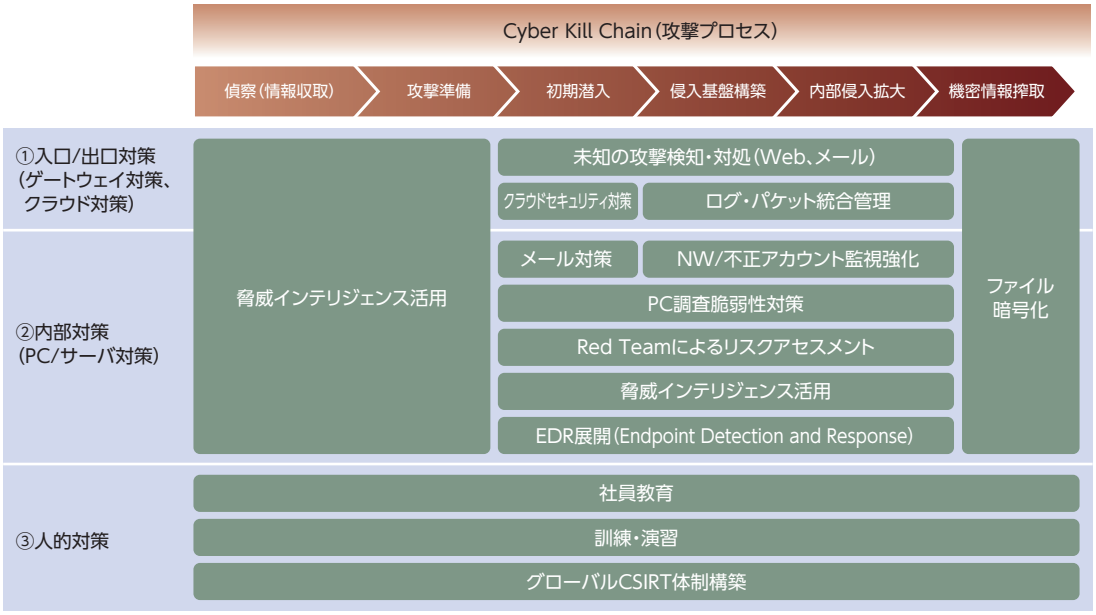
対策製品・サービス、市場動向を調査し、日々進化する技術を把握します。またPoC*5評価、社内IT環境調査により、対象製品・サービスの社内IT環境への適合性などを分析します。

*5 PoC: Proof Of Concept　新しい概念の実証試験

❹ 対策分析

サイバー脅威分析、監視運用分析、ソリューション・IT分析の3つの分析により、今後必要となる対策を検討し、その対策の対象範囲、効果やコストを分析します。

グローバルサイバー攻撃対策の全体像



3 グローバルサイバー攻撃対策

NECは毎年、サイバーセキュリティリスク分析に基づく推進計画を立案し、CISO*6の承認のもと対策を実施します。特に社会ソリューション事業において、グローバルで包括的なサイバーセキュリティリスクへの対応は事業継続の必須条件です。

グローバルサイバー攻撃対策では、多層防御の考え方により巧妙化するサイバー攻撃への対策を強化しています。中でも、①未知の攻撃検知・対処、②Red Team*7によるリスクアセスメント、③脅威インテリジェンス活用、④CSIRT体制強化の4点に注力しています。

*6 CISO: Chief Information Security Officer
*7 Red Team: 企業や組織に対し、実際の脅威に即した疑似的な攻撃を行い、組織としての攻撃への耐性とリスクの評価、および改善・追加対策案の提示を行うチーム

❶ 未知の攻撃検知・対処

入口・出口対策として、未知のマルウェア検知システムによりWeb通信とメール受信を監視し、検知した未知のマルウェア情報などをもとに不正通信をフィルタリングするとともに、感染が疑われるPCおよびサーバへの処置を実施します。グループ全体のPC・サーバにはEDR*8を展開し、端末内の詳細な振る舞いの収集・分析を通じて、未知の攻撃を早期に検知し、リモートフォレンジックなどにより、CSIRTによるインシデントレスポンスを支援します。また、PC・サーバの脆弱性対策として、GCAPS*9（外販ソリューション名：NCSP*10）を展開しています。

*8 EDR: Endpoint Detection and Response
*9 GCAPS: Global Cyber Attack Protection System
*10 NCSP: NEC Cyber Security Platform

❷ Red Teamによるリスクアセスメント

NECグループのサイバーレジリエンシー、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漏えいなどのリスク調査、攻撃者視点でのイントラネット侵入調査の3つをパッケージ化し、サイバーリスクアセスメントを行い、既存のセキュリティ対策の抜け・漏れを洗い出し、改善策を実施します。

❸ 脅威インテリジェンス活用

NECに対する脅威とその予兆を把握し、対策をすり抜けるような高度な脅威に対してリスクの回避、被害の極小化、収束時間短縮化をはかるため、脅威インテリジェンスを活用します。社内外から提供される脅威インテリジェンスを活用し、高度に運用できる専門体制を整備しています。

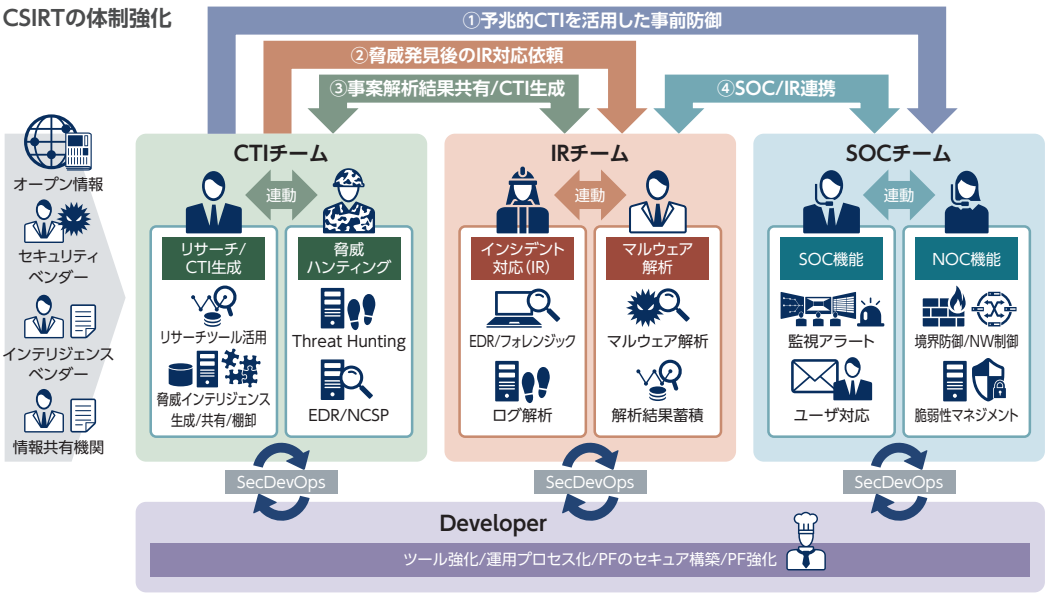
❹ CSIRT体制強化

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*11チーム、インシデント発生時に対応するIR*12チーム、セキュリティ機器からのアラートを監視するSOC*13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。国内のアラート監視については、株式会社インフォセックで監視を行っています。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。

また、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。

*11 CTI: Cyber Threat Intelligence
*12 IR: Incident Response
*13 SOC: Security Operation Center



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。

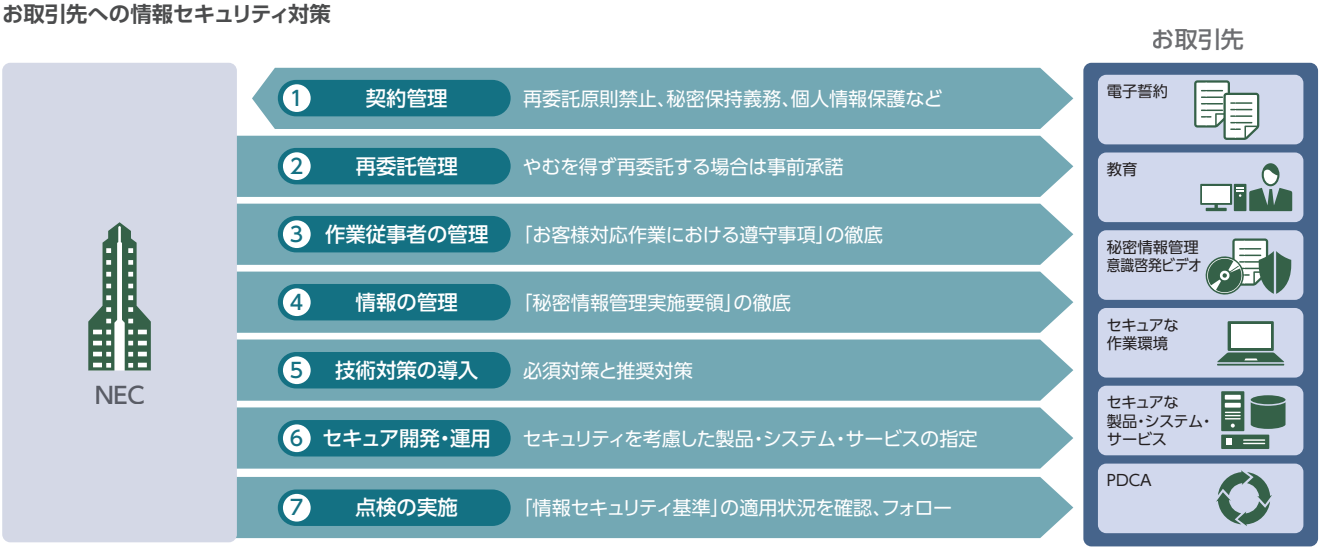
❻ セキュア開発・運用

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。たとえば、セキュアコーディング規約による開発やリリース前の脆弱性診断の実施などです。

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1,400社、うちISMS認証取得会社約700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 意識維持向上のためのビデオ利用

啓発ビデオをお取引先に紹介し、社内教育での活用を推進しています。既存の教材は、遵守事項、秘密情報管理、サイバー攻撃、ウイルス感染、飲酒による紛失、メール誤送信、個人情報保護、事故発生時対応などです。

❹ 理解度テストシステムの運用

「お客さま対応作業における遵守事項」の実施徹底に、NECで用意した「理解度テスト」をお取引先に配布し、社内教育と自社の位置付け把握に活用してもらっています。

❺ 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。

❻ 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1,400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50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して点検を行います。

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

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ではセキュア開発・運用推進体制を構築しています。本推進体制は、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・システム不具合に起因する情報セキュリティ事故の撲滅に向けた、セキュア開発・運用施策案の討議や施策進捗状況の共有などを行います。セキュア開発・運用施策は、各部門のセキュリティ責任者によって部門内へ周知徹底され、実施状況の点検や改善などが継続的に行われています。

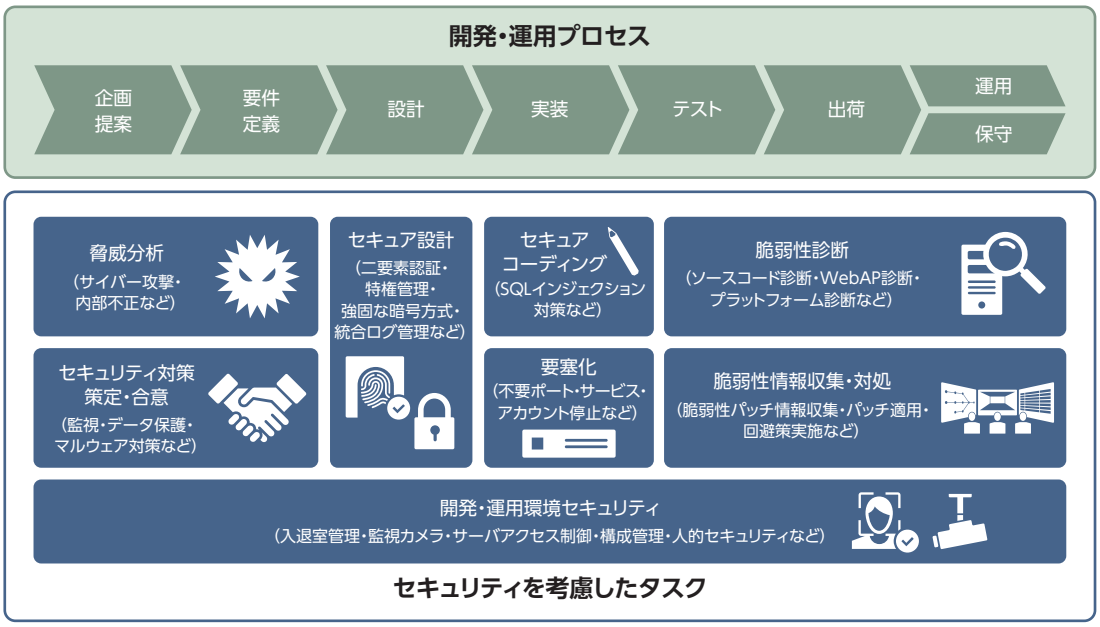
❷ NECのセキュア開発

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ア開発・運用を実施しています。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。

NECでは、開発・運用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、「セキュア開発・運用実施基準」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。

従来は、情報資産の機密性に応じてセキュリティ要件を定めていましたが、ランサムウェアやサービス妨害（DoS[*1]）などサイバー攻撃手法や攻撃対象の多様化に伴い、機密性以外にも完全性や可用性を考慮する必要が生じてきました。そこで基準を見直し、新たにNIST SP800-53などの要件を追加し

セキュア開発・運用プロセス



て、より現状に即したセキュア開発・運用実施基準へと改訂しました。

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「セキュア開発・運用点検システム」により、約7,000もの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。

また、攻撃者視点でのシステム分析に基づく、チェックリストやツールによる定型的な検査では、見つけるのが難しいリスクを発見するスキルに長けた、リスクハンティングチームを立ち上げました。チェックリストを用いた従来の網羅的な検査に加え、特にリスクが高い領域に対してはリスクハンティングチームの検査を行うことによって、さらに堅牢なシステム開発・運用体制を実現しています。

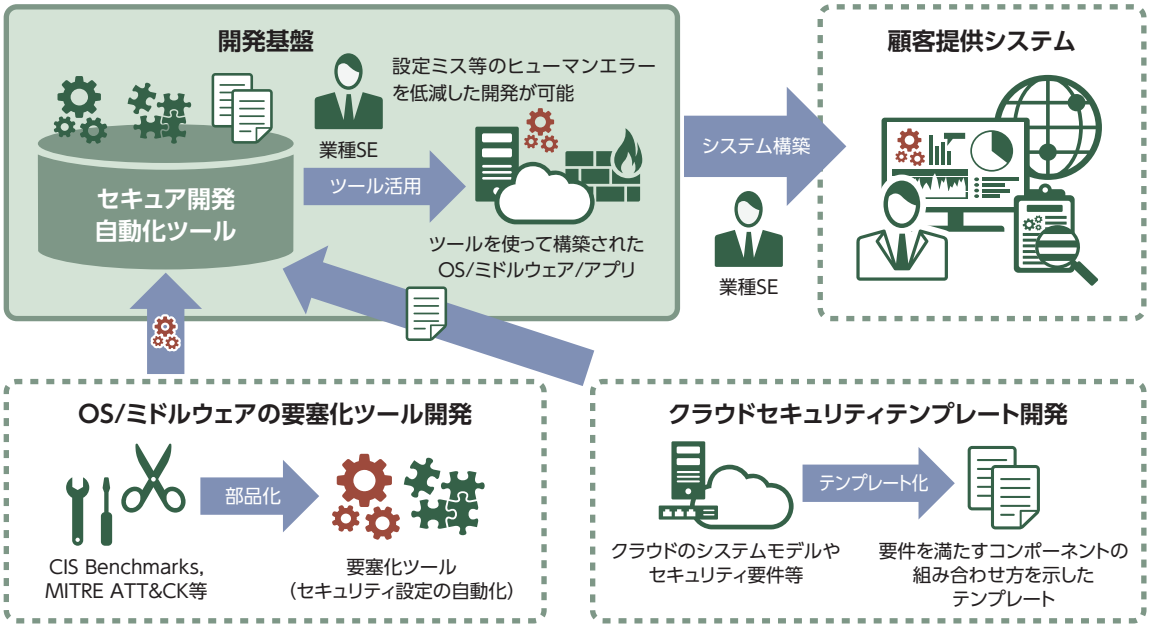
❸ セキュア開発自動化ツールの整備

既述した通り、NECではセキュア開発・運用実施基準に準拠したシステム開発を行っています。しかし、セキュリティを開発プロセスに組み込む際に、各担当者の独自なセキュリティ設定による“抜け漏れ”や、ヒューマンエラーによる設定ミスが生じてしまうという課題が残ります。

このような課題を解決するために、NECではセキュア開発の自動化ツールを整備しています。たとえば、サーバにセキュアな設定を自動的に施す「OS/ミドルウェアの要塞化ツール」が挙げられます。また、近年急増しているクラウドの構築においても、環境全体へ均質的なセキュリティを実現する技術を導入しています。具体的には、IaC*2と呼ばれるクラウド環境をコードで記述する技術を使い、セキュアなクラウド環境そのもののテンプレートを配布して活用する取り組みを進めています。

*1 DoS: Denial of Service attack
*2 IaC: Infrastructure as Code

セキュア開発自動化ツールの整備



デジタルワークプレイス環境の創造

どのような状況下でもデジタルワークプレイスの活用を通じて、NECはユーザの利便性と
安全・安心な情報セキュリティを確保しながら、ビジネスを止めずに事業の継続を推進します。

1 働き方改革とデジタルワークプレイス

NECは、過去30年以上にわたり、社員一人ひとりが能力を最大限に発揮できる、働きやすいデジタルワークプレイス環境づくりを進めてきました。1987年に早くもサテライトオフィスを開設して、1993年には研究職に限りテレワークを導入し、2018年にはテレワーク対象者をNECグループ全体に拡大しています。このような豊富な実績をベースに、NECは早くからICTインフラの整備をはじめ、社内制度の見直しと業務・プロセスの最適化、そして社員の意識改革の3つの側面から働き方改革に取り組んできました。

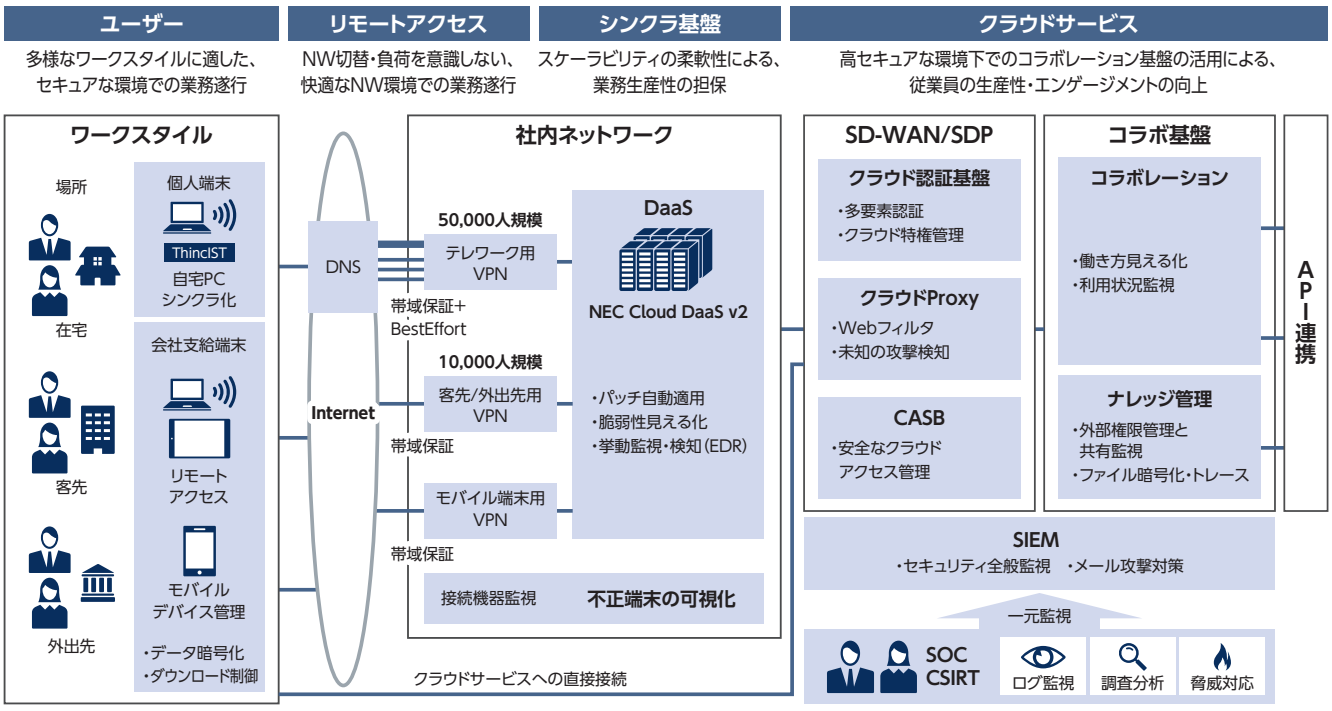
ICTインフラの整備では、業務システムをクラウドベースのプラットフォームへと刷新し、社内外の関係者とのコラボレーションを促進するコミュニケーション基盤の強化と、社員全員に業務端末を配布し、いつでもどこでも誰とでも仕事が行えるデジタルワークプレイス(テレワークなど)環境を実現しています。これらの取り組みは社会にも認められ、2019年度には第20回テレワーク推進賞および会長賞を受賞しました。

2 デジタルワークプレイスの展開

NECのデジタルワークプレイスは、社内全体の情報共有基盤からビジネス・コラボレーション基盤への進化を目指しています。PC・タブレット・スマートフォンなど、モバイル端末の利便性を向上してスマートワークを加速させ、お客さまやお取引先とNECグループとで協働体制が容易に築けるプラットフォームを構築します。

デジタルワークプレイスは、アカウント用のドメインを統合し、誰もがいつでも場所を問わず、複数台の端末を利用できることを想定しています。そこでは、端末の種類を問わず安全・安心に利用でき、ファイルをセキュアに受け渡しできる環境を整備し、機密情報は強力な暗号化で漏えいを防ぐなど、「情報資産の保護」が不可欠なテーマです。これらの基盤整備により、働く時間や場所にとらわれず、NECグループ内だけでなくお客さまやお取引先とのスムーズなコミュニケーションを実現し、共創力の強化を目指しています。

NECが実現するデジタルワークプレイス



3 デジタルワークプレイスの活用

2020年春、COVID-19*1は、わずか数ヶ月でパンデミックといわれる世界的な流行となりました。国内においても、感染拡大を防ぐためにあらゆる場面で「3密」の解消や「行動変容」が広く求められています。このような状況の中で、NECではビジネスを止めず事業を継続するために、デジタルワークプレイスが最大限に活用されています。

デジタルワークプレイスの基本コンセプトは、社員のワークスタイルや利用シーンに合わせ、自分がいる場所や仕事の内容に合った端末モデルを選択できる点にあります。そこでは、万全な情報セキュリティを確保しながら、さまざまな仕事をこなす3種類の端末、「シンクライアント」「Trusted PC」「モバイル基盤」が活躍しています。

*1 COVID-19: 新型コロナウィルス感染症

❶ シンクライアント

NECは2006年より、情報漏えい対策とTCO削減を目的としてグループ全体で導入しています。仮想デスクトップ（VPC）は、2020年4月現在で約60,000台が稼働し、端末内にデータを残さず盗難・紛失時にも情報漏えいを防ぐSS10・ソフトウェアシンクライアントの導入、社内の自席PCをVPCで利用するなど、業務の場所を選ばずセキュアな業務環境を実現しています。

❷ Trusted PC（FAT型持ち出し専用PC）

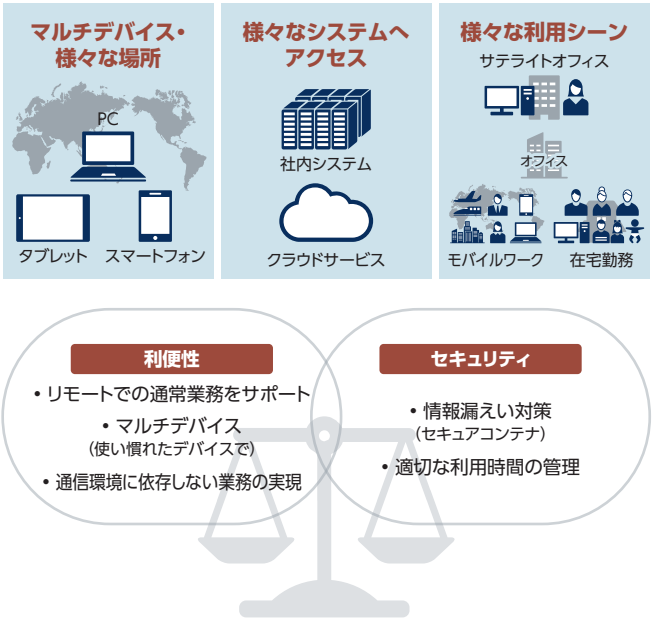
ネットワークにつながりにくい環境でも、業務ができる利便性と安全性を両立したTrusted PCを支給しています。2012年から導入し、2020年4月現在で約20,000台が稼働中です。盗難・紛失時でもデータ読み出し不可能な対策をはじめ、サイバー攻撃対策、情報漏えい対策など徹底したセキュリティ機能の搭載で、利用開始から重大なインシデントの発生はゼロです。

❸ モバイル基盤の刷新

NECでは、多様化する利用端末やシステム、業務場所のニーズへ柔軟に対応できるよう、利便性と情報セキュリティを両立したモバイルワークプレイスを構築しています。特に働き方や行動の変容が求められる状況で、十分な情報セキュリティを確保した上でのモバイル基盤の刷新は、事業の継続や持続可能なビジネス環境を創出する大きなテーマとなります。

端末利用の基本コンセプト

モバイル基盤のコンセプト



4 デジタルワークプレイスの製品・システム・サービス

NECは、働き方改革やワークライフバランスの向上をめざして、デジタルワークプレイスを進めてきましたが、COVID-19の感染禍にともないビジネスや事業を継続する観点から、その対応への重要性が増大しています。NECでは、「テレワーク環境をすぐにも構築・追加したい」、「企業戦略としてデジタルワークプレイスに適したICT基盤に整備したい」、「テレワーク環境のセキュリティを万全にしたい」、「テレワークの社員管理を確立したい」、「コールセンター業務をチャットボット化したい」、「在宅のまま社員研修を実施したい」など、お客さまの多種多様な課題やニーズに対応できる製品・システム・サービスを提供しています。

デジタルワークプレイスの環境整備で重要なポイントは、「情報資産を守る」ことです。テレワーク利用者が増えるにつれ、増大するセキュリティリスクをいかに抑えるかが重要なテーマとなります。本報告書では、テレワークのセキュリティ対策に絞った製品・システム・サービスの一部をご紹介します。

テレワーク導入 セキュリティアセスメントツール(無償)

セキュリティリスクを見える化し、効率的・効果的な対策を推進

情報漏えいやサイバー攻撃による被害は、経営を揺るがしかねない大きな課題です。テレワーク環境の整備に加え、社会に対して説明できるセキュリティ対策が不可欠です。本ツールは、セキュリティ対策の現状を総務省「テレワークセキュリティガイドライン」(第4版)をもとに5つの観点から網羅的にチェックでき、20の質問に回答するだけでテレワークを想定したセキュリティ対策が十分か、強化すべきポイントは何かを知ることができます。

お客さまに質問用紙をお渡しし、ご回答後にNEC側でセキュリティリスクを見える化して、集計結果をお戻しする無償サービスです。

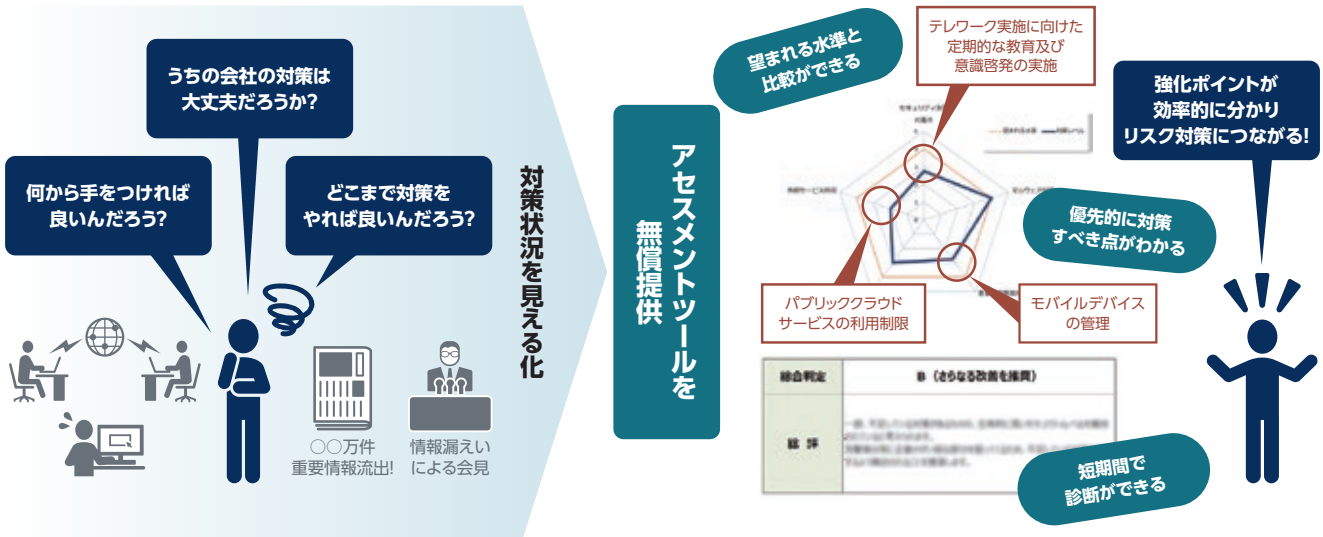
テレワーク導入 セキュリティリスクアセスメント

導入アセスメントを通じて、セキュリティ対策の優先度を明確化

セキュリティコンサルタントによる、テレワーク導入に関するアセスメントサービスを提供します。企業組織や社内システム、機器類などをサイバーセキュリティ経営ガイドライン、テレワークセキュリティガイドライン(総務省)、NIST SP800-171などに基づいてアセスメントを実施し、対策立案を支援するサービスです。セキュリティリスクを見える化してコストと影響を分析し、優先度を判断することができます。

- 対象に合った基準・ガイドラインをベースに作成したNECグループ独自コンテンツを使用。
- ヒアリング・アセスメントシートを組み合わせ、アセスメントを効率的に実現。
- アセスメント結果をレポートし、問題点の説明や影響、根本原因を踏まえた対策方針を提案。
- 発見された問題点には優先順位を決め、適切な対策を施すことでセキュリティリスクを低減。
- アセスメントを定期的に実施することで、セキュリティレベルの維持と向上を推進。

リスクを可視化しセキュリティ対策を推進



テレワーク導入セキュリティコンサルティング

多角的な分析で、経営観点による業務改善・組織づくりまでを提案

NECはサイバーセキュリティ経営の観点から、テレワーク導入に対するセキュリティ対策を支援するコンサルティングサービスを提供しています。自社内での実践経験を活かし、サプライチェーンのお取引先を含めたテレワーク導入に向けて、組織のセキュリティポリシーの見直しや、セキュリティ管理体制の整備を支援するサービスです。

セキュリティ対策支援サービス

テレワーク導入に向けたセキュリティ対策をトータルに支援

さまざまな業務でのテレワーク導入に向けた、セキュリティアセスメントツール（無償）やセキュリティリスクアセスメント、セキュリティコンサルティングなどで見える化されたリスクに対し、対策の立案から具体的なSIまでセキュリティ強化を実施するサービスです。

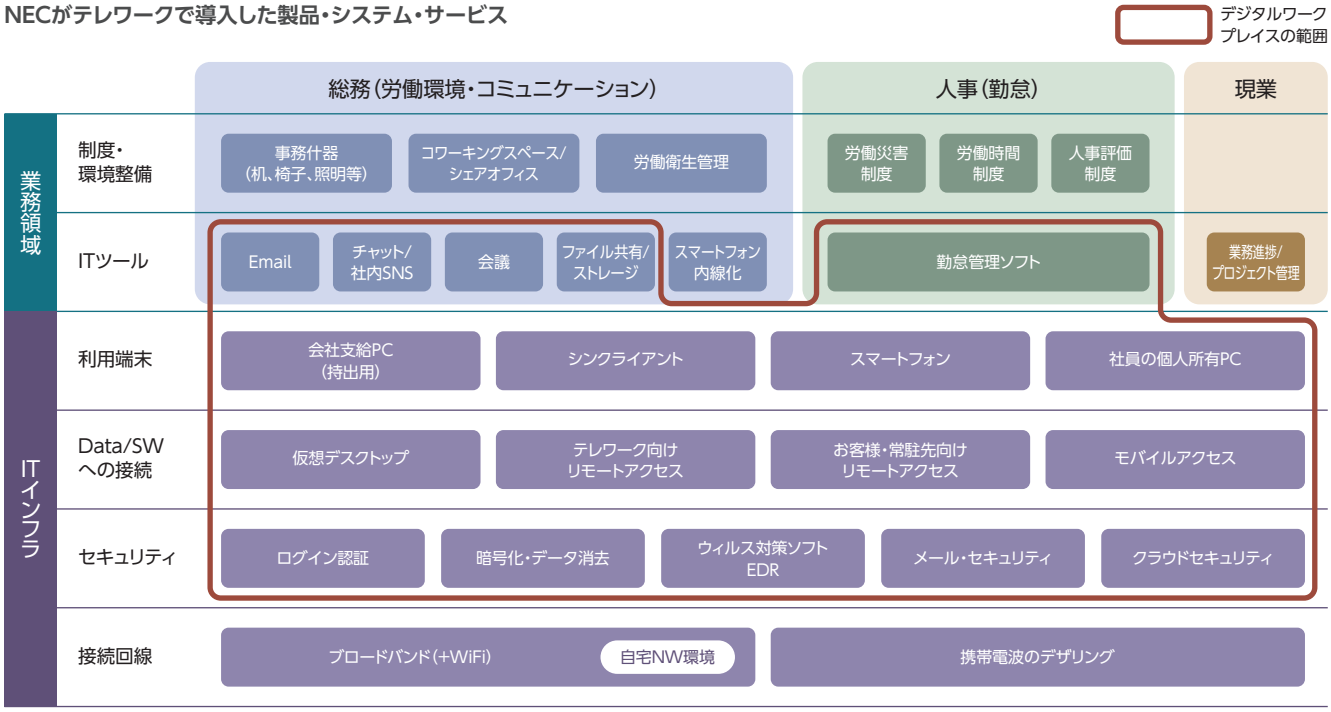
お客さまが投資された既存のセキュリティ対策を活かしつつ、テレワーク環境の整備とともにサイバー攻撃や情報漏えいにも対応できる、セキュリティ対策の導入をトータルに支援します。

対策例

- リモートアクセス
- クラウドセキュリティ対策
- 認証強化
- 情報漏えい対策
- エンドポイントセキュリティ対策

最後に、COVID-19による感染禍は数年つづくといわれており、従業員がいつでもどこでも業務が行えるデジタルワークプレイス環境の整備が急務となっています。下の図は、NECがテレワークを実践する上で、グループ内に導入した製品・システム・サービスです。太線枠内がデジタルワークプレイスの範囲ですが、お客さまやお取引先のご参考になれば幸いです。

NECがテレワークで導入した製品・システム・サービス



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、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るため、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

増加するサイバー犯罪に対する情報基盤を強化するために、NECでは国内外の関連組織と連携しています。

制御システムセキュリティセンターへの参画をはじめ、2014年には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、そ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

取締役会長である遠藤信博が、サイバーセキュリティ戦略本部（内閣）の委員や産業サイバーセキュリティセンター（IPA*3）のセンター長を兼務しているのをはじめ、NECは国が主宰する多くの研究会で委員に就任するなど、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。このような活動を通じて、NECは官民一体となった安心・安全な社会づくりを目指しています。

*3 IPA: 独立行政法人情報処理推進機構

関係組織との連携

情報基盤強化

制御システムセキュリティセンター（CSSC）参画 （2013年11月）
経産省官民連携プロジェクトで、重要インフラ機器・制御システムのセキュリティを確保。

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。脅威の大本を絶ち、被害の防止を目指す。
NEC 執行役員常務 堺 和宏が代表理事を務める。

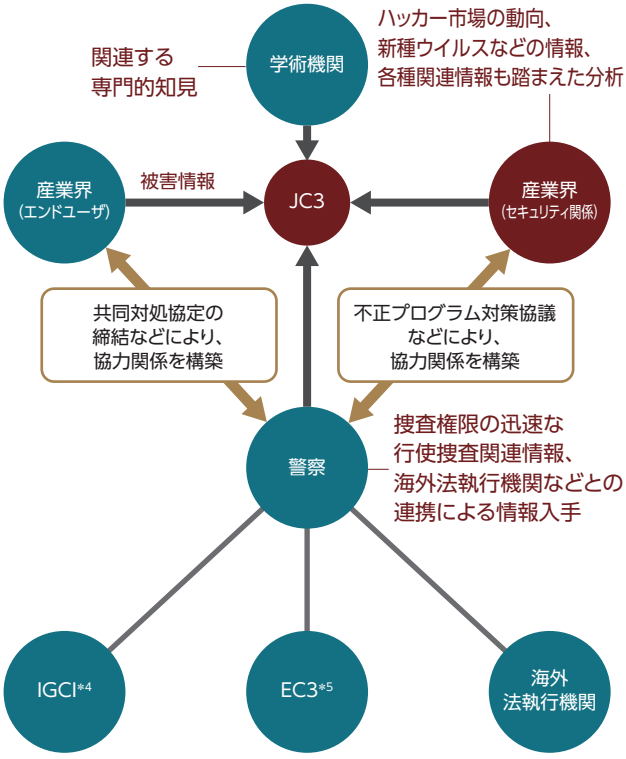
米国国土安全保障省（DHS）の官民情報共有 AIS※参加 （2017年3月）
米国国土安全保障省（DHS）が推進する、官民でサイバー攻撃の脅威情報を迅速に共有する枠組み「AIS」に日本企業として初めて加入。
※Automated Indicator Sharing

ICT-ISAC発足に参画 （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、業界の枠を超えて連携・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Telecom-ISACから参画）

産業横断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。

日本サイバー犯罪対策センター（JC3）を中心とした枠組み



*4 IGCI: The INTERPOL Global Complex for Innovation
*5 EC3: European Cybercrime Centre

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強化

NECは国内だけにとどまらず、グローバルで継続的なセキュリティ投資を実行しています。2013年に株式会社サイバーディフェンス研究所、2014年に株式会社インフォセック、2016年にはNEC Solucoes de Seguranca Cibernetica Brasil S.Aをグループ会社化し、高度なサービスの提供を実現するために体制強化を促進しています。

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。

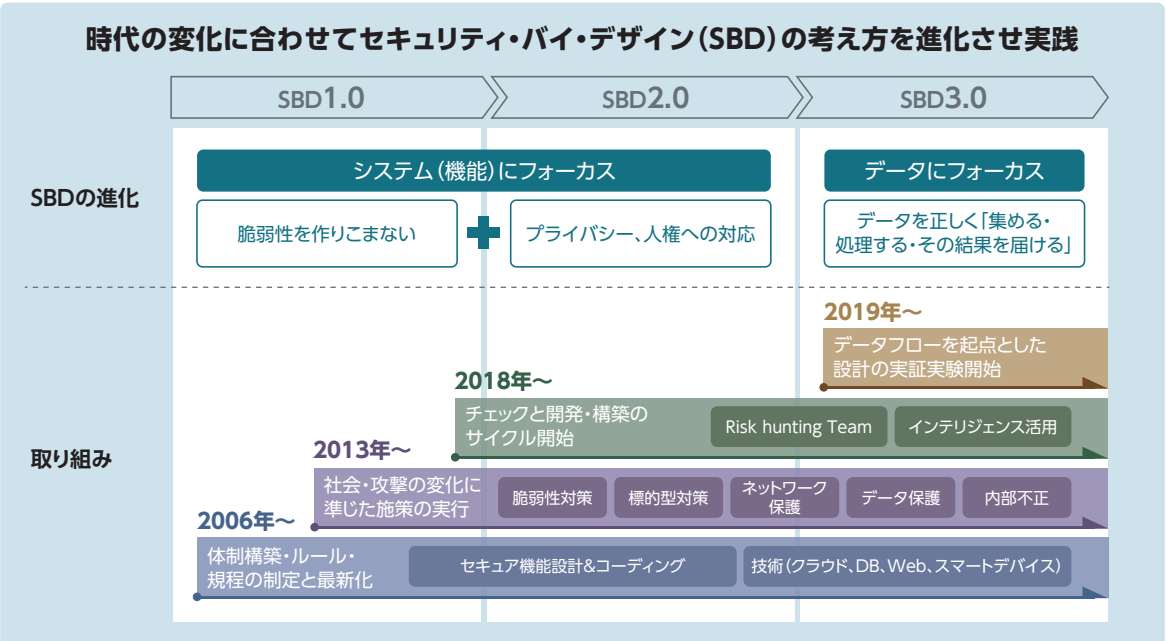
❸ 国内セキュリティ人材育成への投資

北陸先端科学技術大学院大学校に寄付講座を開設し、人材の育成を積極的に行うことで、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が提供する教育プログラムには、標的型攻撃メール訓練をはじめ、さまざまなプログラムが存在しています。中でも、サイバー攻撃演習プログラムは、インシデントハンドリングの一連の流れを実際に体験しながら学習することができます。実体験を通じて、お客さまの技術力の向上や、お客さまの事業を支えるICT基盤のサイバーセキュリティ対策における充足度を確認する、“気づき”の場となることを期待しています。

SBD3.0によるセキュア開発・運用の考え方



4 セキュア開発・運用の徹底

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、セキュア開発・運用を徹底する体制を構築しています。また、開発した製品・システム・サービスに対して、世界トップレベルの技術力を備えたエンジニア（リスクハンティングチーム）が脆弱性の有無を確認して、十分なセキュリティ対策が実施されているかを検証する体制も構築しています（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ア開発・運用の考え方としてSBD3.0*6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。

*6 SBD3.0: Security By Design（セキュリティ・バイ・デザイン） 3.0

■ 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

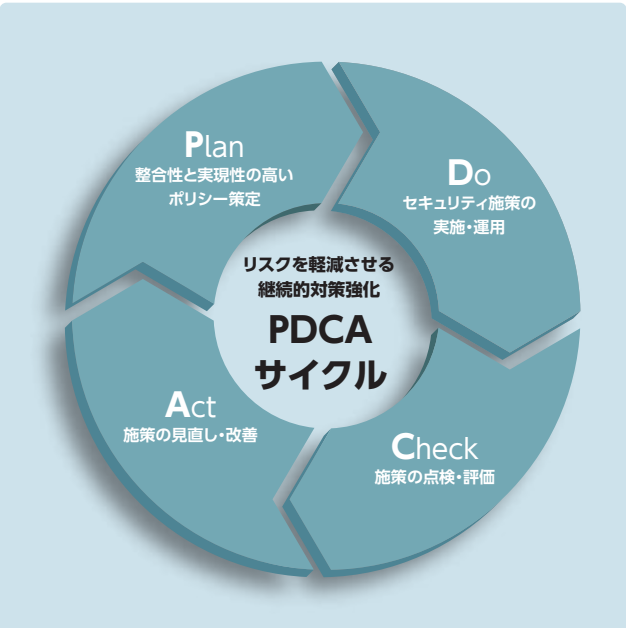
5 自社運用ノウハウをもとにセキュリティ強化をサポート

サイバーセキュリティ対策は、導入すれば終わりというわけにはいきません。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。

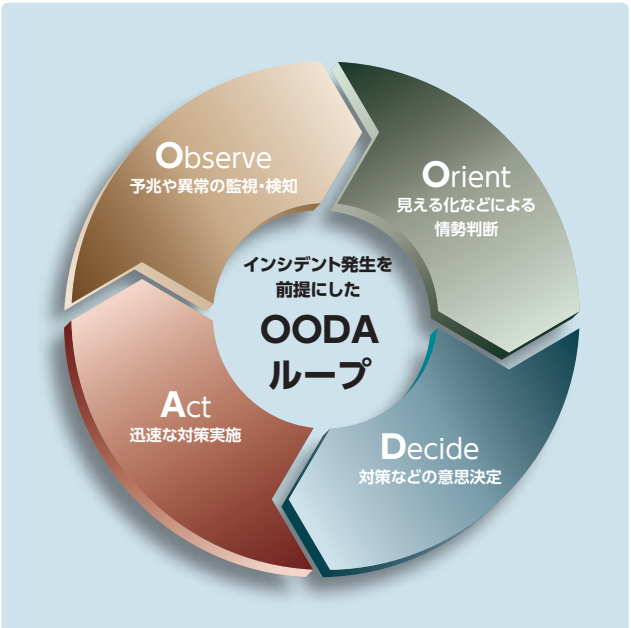
サイバーセキュリティのポリシー策定から対策、効果の点検、改善というPDCAサイクルを実現し、脆弱性を解消する継続的な対策が欠かせません。NECでは、グローバルに展開するNECグループの社員約11万人が利用するシステムでの運用実績に基づき、利用者目線でのサイバーセキュリティ対策を提供します。

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て準備をしておくことも重要です。NECでは、監視・検知・情勢判断・意思決定・対策実施という流れによる、「OODA（ウォーダ）ループ」という概念を取り入れ、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



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研究開発を行っています。

システムセキュリティでは、巧妙化・高度化するサイバー攻撃によるセキュリティリスクを可視化する「サイバー攻撃リスク自動診断技術」、アンチウィルスソフトが導入できないIoT機器に対するセキュリティ対策「軽量改ざん検知技術」など、最先端のセキュリティ技術を開発しています。

また、データセキュリティでは情報漏えい事故の根絶に向け、IoT機器に暗号機能を実装するための「軽量暗号」や、暗号化したままデータ処理を実現する「秘密計算技術」を開発しています。

2 サイバー攻撃リスク自動診断技術

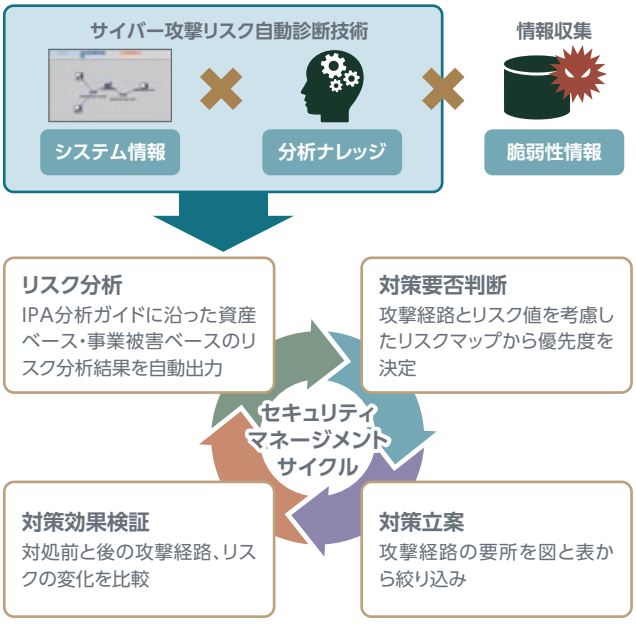
増え続けるサイバー攻撃への備えでは、常に最新の情報を収集し、新しい脅威や脆弱性に対してシステムの潜在的リスクを把握し、事前に対処することが重要です。しかし、リスク分析や対応要否判断、対策検討には多大な工数と、セキュリティの専門知識が必要となります。

サイバー攻撃リスク自動診断技術は、ルール化されたセキュリティエキスパートの分析ロジックにより、最新の脆弱性情報を用いてシステムの潜在リスクを自動的に洗い出します。資産ベース・事業被害ベースのリスク分析結果が、IPA*1による制御システムのセキュリティリスク分析ガイドのシート形式、およびトポロジー上の攻撃経路図として出力されます。

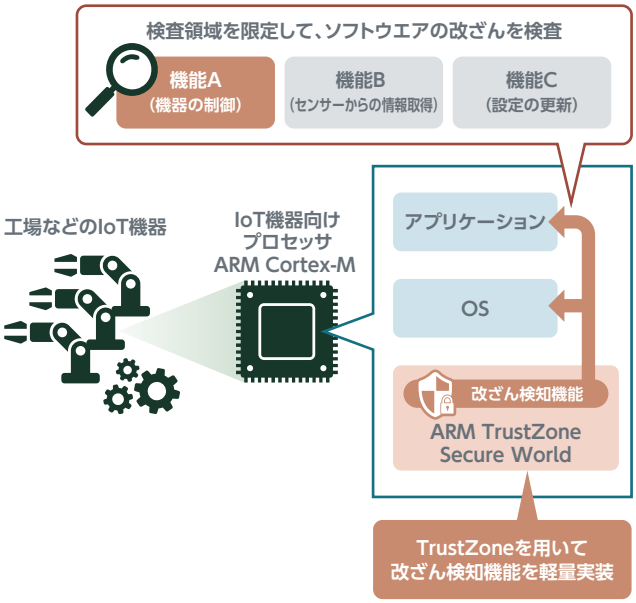
攻撃に使われる手法や脆弱性の種類に応じて、攻撃経路のリスク指標が自動算出され、優先的に対処すべき攻撃経路を判断することができます。また、攻撃経路の構造に基づいて効果的な対策箇所や対策種類を絞り込み、対策前と対策後の分析結果差分比較機能により、対策効果を簡単に事前評価できます。

*1 IPA: 独立行政法人情報処理推進機構

サイバー攻撃リスク自動診断技術の概要



軽量改ざん検知技術の仕組み



3 軽量改ざん検知技術

近年、社会インフラシステムなどの効率的な運用のために、IoTの活用が進んでいます。IoTに接続される機器（IoT機器）は、CPU性能やメモリ容量が十分ではなく、従来のセキュリティ対策を導入することができませんでした。

軽量改ざん検知技術は、このようなIoT機器へ導入することができ、稼働中のIoT機器のソフトウェアに対する改ざん検知を実現します。IoT機器向けプロセッサARM Cortex-MのTrustZone*2を用いて、改ざん検知機能を実装する軽量なアーキテクチャを採用することにより、メモリ容量に制約のあるIoT機器にも導入できます。

また、ソフトウェア構造をベースに、これから実行されるコードが格納されているメモリ領域を特定し、その領域に絞って改ざんの有無を検査することで、機器本来の動作への影響を最小限にとどめ、稼働中のIoT機器上でもスムーズな検査が可能となります。

*2 TrustZone: メモリ上に保護領域を構築する機能

4 データセキュリティ

❶ 軽量暗号

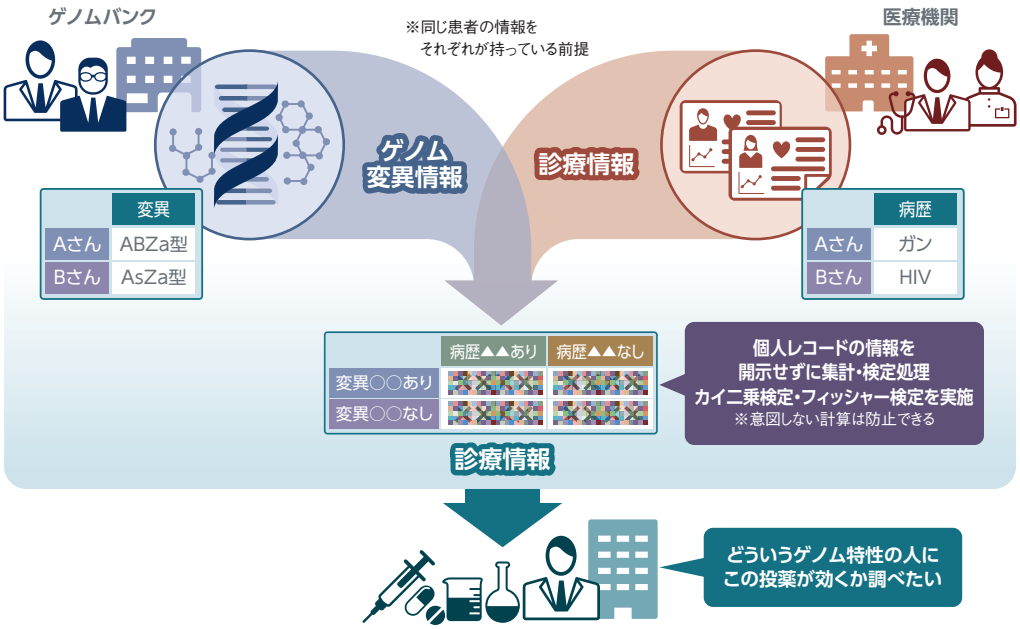
軽量暗号は、リソースが少ないIoT機器でも快適に動作する暗号です。NECは、世界トップクラスの軽量暗号技術を保有しており、米国における軽量暗号標準化に向けて提案中であり、現在選考が行われています。軽量暗号を活用し、さまざまなIoT機器を安全にサイバー空間へとつなぐことができます。

❷ 秘密計算

秘密計算は、データを暗号化したままで処理することができる技術です。マルウェアによる攻撃や、組織の内部犯行に対して情報漏えいを強力に防止し、さらに複数組織がそれぞれ保有する秘密情報を隠したままで利活用することができます。

従来の秘密計算は性能に課題がありましたが、複数サーバにデータを秘密分散したままの状態で処理する方式の改良により、NECは2016年に最高性能を達成しました。また、秘密計算を使った開発を容易にする技術を開発し、2019年にはゲノム研究者が開発した独自の解析アルゴリズムに、数日で秘密計算が適用できることを実証しました。

ゲノム研究における秘密計算の適用事例



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 VALWAY株式会社
- NECスペースステクノロジー株式会社
- NECソリューションイノベータ株式会社
- NECチャイナ・ソフトジャパン株式会社
- NECネクサソリューションズ株式会社
- NECネッツエスアイ株式会社
- NEC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
- 静岡日電ビジネス株式会社
- 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
- 株式会社プリースコーポレーション
- 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
- キューアンドエーワークス株式会社
- 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
- 静岡日電ビジネス株式会社
- 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

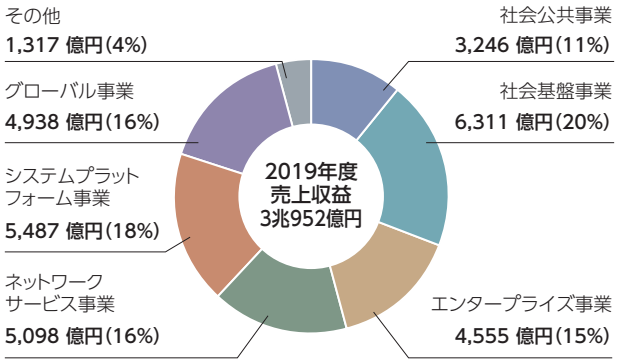
会社概要

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	3,972億円※
連結従業員数	112,638名※
連結子会社数	300社※

※2020年3月31日現在

事業紹介

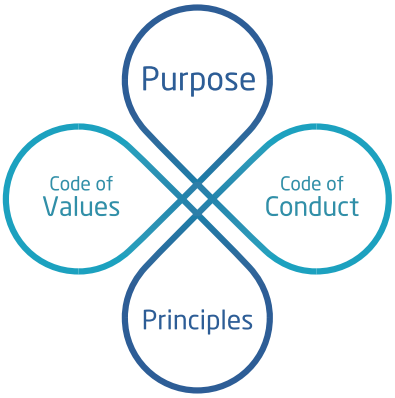
セグメント別売上収益(構成比)



※2020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

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

VEGETABLE OIL INK

2020年７月発行

Cat.No. K99-20070090J