Empowered by Innovation NEC

情報セキュリティ報告書
2014

Orchestrating a brighter world

世界の想いを、未来へつなげる。

NECが考える情報セキュリティ

NECグループは、「情報セキュリティ」を重要な経営活動として位置づけ、
「社会ソリューション事業」を通じて新しい価値を創造していきます。

新野 隆
日本電気株式会社
代表取締役　執行役員副社長

現在、世界中の人々は、世界の人口増加や都市化率の上昇、エネルギーや食糧への需要拡大など、地球規模での課題に直面しています。NECは、グローバルな社会課題を解決し、人が豊かに生きるために不可欠な「安全」「安心」「効率」「公平」という社会価値を創造したいと考えています。お客さまはもちろん、世界の国々や地域の人々とともに、文化や多様性を尊重し、明るく豊かな人々の暮らしや効率的で洗練された社会を支え、希望にあふれた未来につなげていきます。これこそが、NECの「社会ソリューション事業」であり、世界中のお客さま・パートナーに向けた事業ブランドメッセージである「Orchestrating a brighter world　世界の想いを、未来へつなげる」に込めた想いです。

社会ソリューション事業が生み出す社会インフラが提供する価値は、今後、利用する情報が広がるにつれ一層高度化していきます。そうした中、「ビッグデータ」、「クラウド」、「SDN」、「サイバーセキュリティ」は、ますます重要なテーマとなってきています。中でも、サイバーセキュリティは、今後あらゆるITシステムに必須となるものです。NECは、業界トップクラスの技術を持つ企業との連携により競争力強化に取り組んでいます。また、グローバル成長戦略の柱の一つとして、「セーフティ事業」を掲げ、長年培ってきた技術を活かし現地主導型でグローバル展開を加速します。

NECは、これらの領域におけるコアアセットをフルに活用し、OneNECとして総合力を発揮し、新しい価値を創造していきます。そして、誰もが安心して情報通信技術の恩恵を享受し、豊かな社会を実現していくためには、情報セキュリティを重要な経営活動として位置付け、継続的に以下の活動に取り組んでまいります。

- 「OneNEC」として、NECグループが一体となって情報セキュリティの維持・向上を推進
- NECグループだけでなく、お取引先まで含めた施策を展開
- 適切な情報保護と適切な情報活用・共有を両立
- 情報セキュリティマネジメントの構築、情報セキュリティ基盤の整備、情報セキュリティ人材の育成の各領域からの総合的アプローチにより、多層的に情報セキュリティを維持・向上
- お客さまに信頼されるセキュリティソリューションを提供

本報告書は、NECグループの情報セキュリティへの取り組みをご紹介するものです。ステークホルダーのみなさまとのコミュニケーションを通して、企業活動の改善をはかり、社会から信頼される情報セキュリティリーディングカンパニーを目指してまいります。ぜひご一読くださいますようお願い申し上げます。

情報セキュリティ報告書 2014

NECが考える情報セキュリティ 02
情報セキュリティ推進フレームワーク 04
情報セキュリティガバナンス 06
情報セキュリティマネジメント 07
情報セキュリティ基盤 10
情報セキュリティ人材 14
海外現地法人の情報セキュリティ 16
お取引先と連携した情報セキュリティ 18
セキュアな製品・サービスの提供 20
情報セキュリティの取り組み事例 22
第三者評価・認証 34
NECグループの概要 35

報告書の発刊にあたって

本報告書は、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を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、2014年8月までの取り組みを対象に掲載しています。

本報告書に掲載されている社名やシステム名、製品名などは、各社の商標および登録商標です。

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 セキュリティ技術センター
〒108-8001 東京都港区芝五丁目7-1 NEC本社ビル
03-3798-6980

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。

情報セキュリティの脅威は、日々変化しており、ITで高度化された社会において、情報セキュリティは欠くことのできない重要な経営課題です。NECグループは、社会から信頼される企業として社会的責任を果たすため、「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、お取引先からお預かりした情報資産を守り、信頼される製品・サービス、情報セキュリティソリューションの提供、ステークホルダーへの適切な報告・情報開示を通じて、セキュアな情報社会の実現とお客さまへの価値を提供します。

情報資産を守るための情報セキュリティの取り組みとしては、次の4つの要素を組み合わせることにより、総合的かつ多層的に情報セキュリティの維持・向上をはかっています。

情報セキュリティを組織全体に
浸透・徹底させる仕組み

**情報セキュリティ
ガバナンス**

方針・規程類の整備や
PDCAサイクルを回すための仕組み

**情報セキュリティ
マネジメント**

ネットワークや業務システム、
PCなどを脅威から守るITの仕組み

情報セキュリティ基盤

情報セキュリティに関する意識向上、
能力向上などの育成の仕組み

情報セキュリティ人材

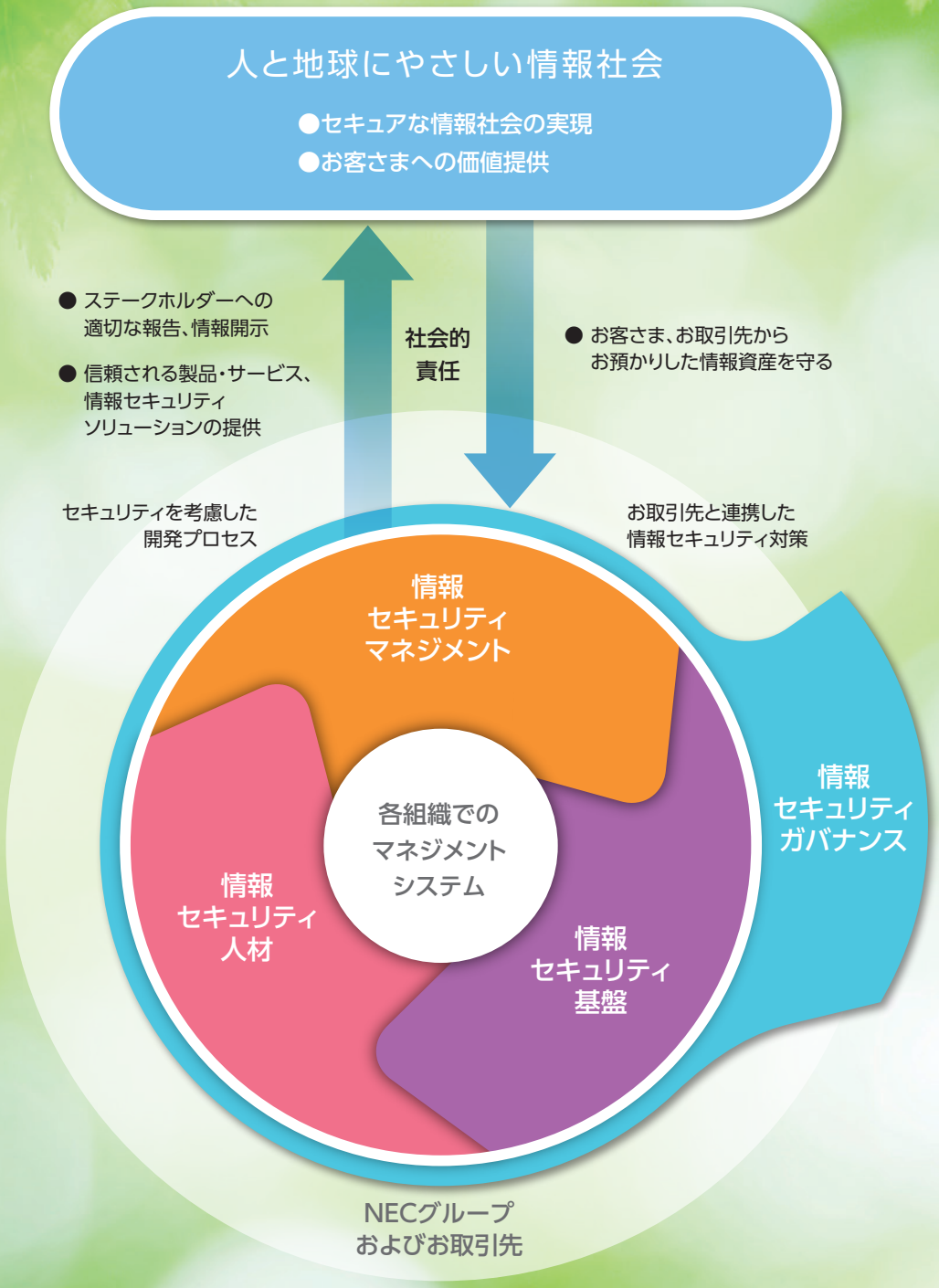
これらは、全社的な取り組みとNECグループの各組織の取り組みに分けられます。

全社的な取り組みとしては、情報セキュリティ基本方針・全社規程の制定、共通的な情報セキュリティ基盤の整備、教育・意識啓発・人材育成の制度運営などの施策の立案・実施・見直し・改善を行うとともに、これらを組織全体に効果的・効率的に浸透・徹底させる仕組みとして情報セキュリティガバナンスがあります。また、グループ内だけでなくお取引先と連携したセキュリティ対策の展開、信頼される製品・サービス・ソリューションを提供するための開発プロセスの確立を推進しています。

各組織の取り組みとしては、全社の推進を受け、各組織の事業環境や内部組織体制を考慮した各組織でのマネジメントを行っています。

NEC Security Vision

社会から信頼される情報セキュリティリーディングカンパニーを目指して



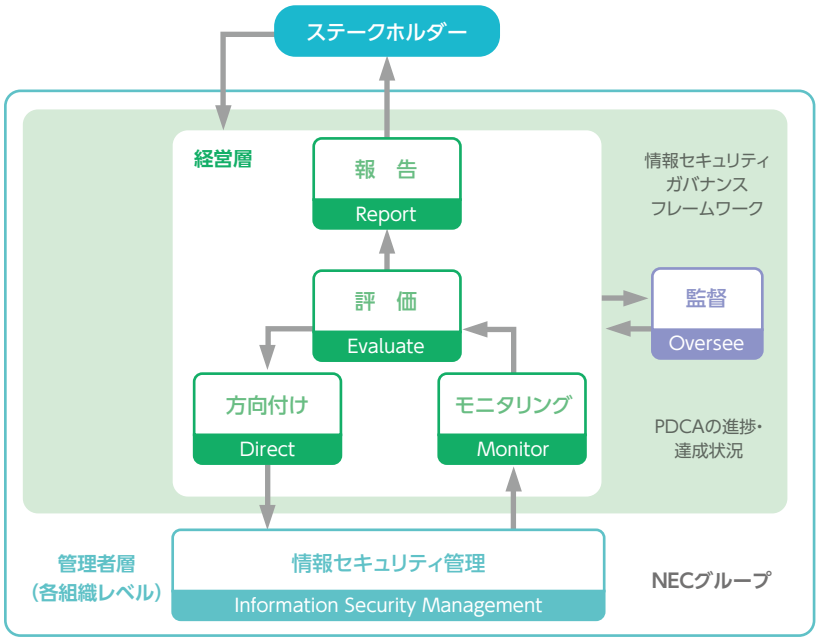
情報セキュリティガバナンス

事業活動と情報セキュリティを整合し、NECグループ全体で効率的、効果的に情報セキュリティレベルを高め、事業活動から生じるリスクをコントロールするため、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、グループ全体が総合力を発揮するために「NECグループ経営ポリシー」を定め、事業遂行に関する各種ルールの共通化、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の実現するベースを確立しています。「OneNEC」として全体のセキュリティレベルを向上させるためには、情報セキュリティのガバナンスが不可欠です。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などの方針を決定します。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発生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。こうした経営層と管理者層のサイクルとそれを監督する機能により、グループとしての全体最適を追求するとともに、ステークホルダーに対する適切な情報開示を行い、企業価値の持続的な向上をはかります。

情報セキュリティガバナンス

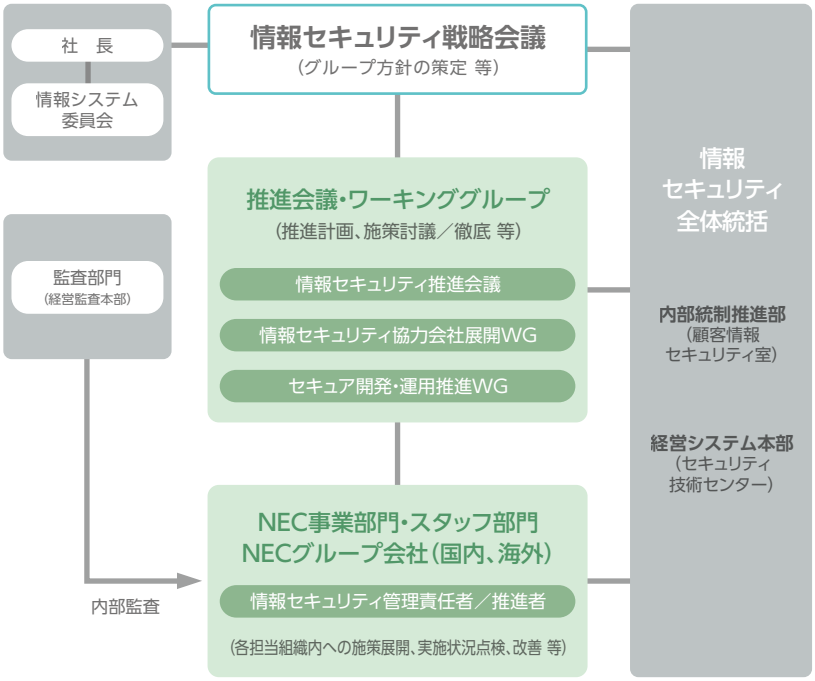


2 NECグループの情報セキュリティ推進体制

NECグループの情報セキュリティ推進体制は、情報セキュリティ戦略会議とその下部組織、および各組織の推進体制で構成されます。「情報セキュリティ戦略会議」は、情報セキュリティリスクに対応するため、「情報セキュリティ施策の審議・評価・改善」、「重大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」などの審議を行います。下部組織である3つの推進会議やワーキンググループは、国内、海外、お取引先、セキュア開発・運用に関する「推進計画、実行施策に関する討議・調整、指示事項の徹底、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て情報セキュリティに関する一義的な管理責任を負い、組織内へのルールの周知徹底、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。

情報セキュリティ推進体制



情報セキュリティマネジメント

情報セキュリティの各種施策をグループ全体に展開し確実に定着化させるため、
情報セキュリティマネジメントの体系を確立し、PDCAサイクルにより
情報セキュリティの維持・向上をはかっています。

1 情報セキュリティマネジメントの体系

NECグループでは、情報セキュリティや個人情報保護のポリシーに基づき、継続的にPDCAサイクルを回し情報セキュリティの維持・向上をはかっています。情報セキュリティ点検／監査の結果や情報セキュリティ事故の状況などを鑑み、情報セキュリティ対策の実施状況の把握・改善、ポリシーの見直しをしています。また、第三者認証で要求される管理水準を考慮し、ISMS認証やプライバシーマークの取得・維持も推進しています。

▌NECグループ情報セキュリティマネジメント

2 情報セキュリティに関するポリシー

NECグループは、国内・海外のグループ会社の共通ポリシーとして「NECグループ経営ポリシー」が展開されており、情報セキュリティや個人情報保護のポリシーが含まれています。情報セキュリティや個人情報保護は、これまでも事業遂行上の重要事項として管理の強化に取り組んできました。

情報セキュリティは「情報セキュリティ基本方針」を公開し、基本方針を実現するための規則や基準として、情報セキュリティ基本規程、情報管理に関する規程(企業秘密管理規程、個人情報保護規程、技術文書管理規程)、ITセキュリティに関する規程などを整備し体系化しています。

個人情報保護は、「NEC個人情報保護方針」を制定後、2005年にNECがプライバシーマークを取得し、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)」および「個人情報保護法」に準拠したマネジメントシステムを確立しています。個人情報は、グループ共通の保護管理レベルで運用するよう推進しており、28社(2014年8月末現在)がプライバシーマークを取得しています。

▌NECグループ経営ポリシー

3 情報セキュリティリスク管理

情報セキュリティマネジメントが有効に機能するためには、情報セキュリティのリスクを適切に評価し、管理する必要があります。

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を分析する手法と詳細リスクを分析する手法を使い分けてリスク評価と対策の実施を行っています。基本的には、共通に実施すべき水準として定められた「情報セキュリティ対策基準（ベースライン）」により、セキュリティを維持しています。高度な管理を必要とする場合は、「詳細リスク評価基準」に基づいた分析を行い、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

一方、情報セキュリティ事故の報告を義務付け、その内容を分析することで、PDCAサイクルを回す際のインプットとし、情報セキュリティのリスクを管理しています。事故情報はグループで標準化したルールで一元的に管理されており、件数の変化、組織別（NEC、グループ会社、お取引先）の傾向、事故の類型別の傾向などを分析し、共通施策に反映するとともに、効果測定やKPIとしてリスク管理しています。

また、情報セキュリティ事故の真の原因を追究するために、「なぜなぜなぜ分析」を実施しています。分析手法を確立し、当該部門が自身で分析を行える体制を整備しています。重大な事故は、専門のアドバイザーが参加・分析するとともに、対応費用や影響度を数値化することで、インパクト分析も行っています。結果は経営層に報告し、全社への横展開、全社施策への反映などにより、効果を上げています。

4 情報セキュリティ関連の新たなルール

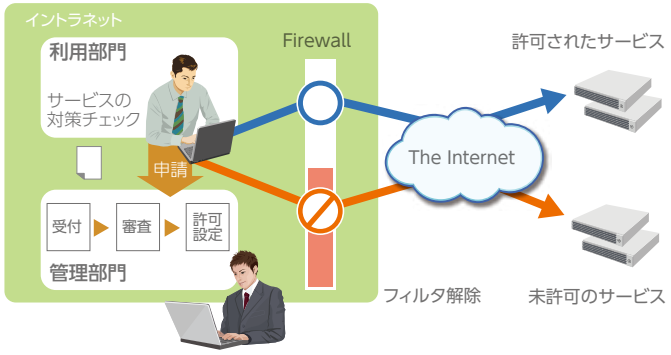
スマートフォンやタブレット、クラウドなどの最新の情報通信技術（ICT）活用に向けたルールづくりや運用の確立を進めています。

❶ 外部サービス基準の制定

クラウドサービスの急速な普及にともない、インターネットを経由して高機能なサービスを迅速かつ容易に利用できるようになる一方、企業秘密などを外部のシステム上で処理することで、少なからず情報漏えいのリスクが存在します。NECグループでは、クラウドなどの外部サービスを業務利用する場合の基準を設けています。

具体的には、外部サービスの業者が安全なサービスを提供しているかに関し、データセンター、システム技術、運用などのセキュリティ対策をチェックシートにより事前評価し、申請・審査の上、利用できるようにしています。利用の多いサービスなどは、あらかじめ評価の上、許可サービスを定める反面、リスクが高いサービスは、利用を禁止するものもあります。

▌外部サービスの利用手続き



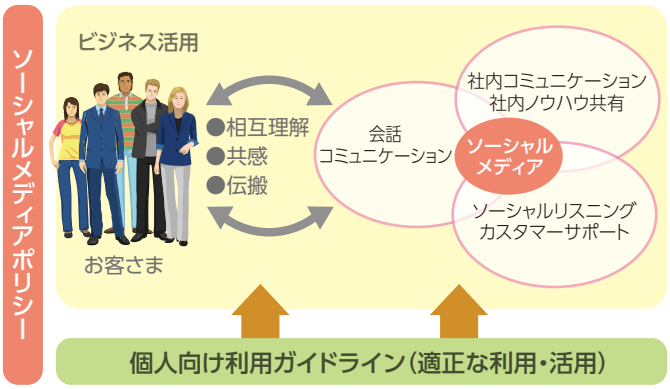
❷ スマートデバイスの利用ルール

スマートフォン、タブレットなどの携帯情報端末を活用する場面が増える中、これらを安全に利用するためのルールを制定しています。PC並の機能を持つ反面、セキュリティ技術が十分に確立されていないケースもあるため、会社で推奨する端末に限定するとともに、パッチやバージョンアップ、ウイルス対策、信頼できるアプリケーションの利用、自動ロック設定などを定めています。また、格納する情報の最小化、万が一の盗難・紛失時の速やかな連絡なども義務づけています。

❸ ソーシャルメディアへの対応

NECグループでは、ソーシャルメディアポリシーを公開し、ビジネス活用と個人利用の観点からガイドラインを制定・運用しています。ソーシャルメディアの普及に伴い、これらを活用したお客さまとの双方向のコミュニケーションを進める一方、企業秘密やプライバシー情報などの情報漏えい、ネット上での非難・批判、私的な利用といったリスクも高まっています。このような中、ポリシーの基本的な方針は維持しつつ、主に個人向け利用のガイドラインを見直しました。個人の情報発信や対応が会社に与える影響に対する自覚と責任の理解を進めるとともに、企業秘密などの漏えい、第三者の正当な権利侵害、誤解を与える内容やグループ社員としてふさわしくない情報発信などに留意する内容とし、安全な活用を進めています。

▌ソーシャルメディアの活用とガイドラインの見直し



5 情報セキュリティ点検

NECグループでは、情報セキュリティ対策の実施状況を確認し、実施が不十分な対策の改善計画を立案・実行する活動として、国内・海外のグループ会社を対象に、情報セキュリティ点検を毎年継続して実施しています。

❶ 情報セキュリティ点検の内容

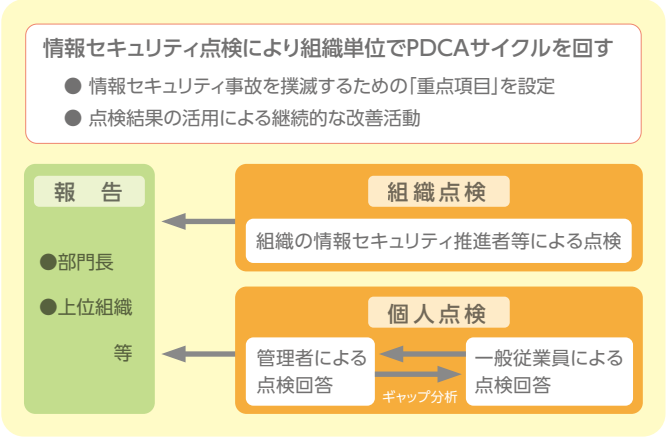
情報セキュリティ事故を分析の上、主として情報漏えい事故を撲滅するための項目を重点項目に設定しています。また、点検は、実施状況のチェックだけでなく、実施できていない場合の理由を回答する形式にし、是正対応に役立てる形にしています。

具体的には、外部記憶媒体の安全対策、社外作業の安全対策、個人情報の管理、外部委託作業時の秘密情報管理、メール誤送信防止などの項目の確実な徹底をはかりました。

❷ 情報セキュリティ点検の方式

情報セキュリティ点検の方式は、各組織の情報セキュリティ管理責任者が組織全体の状況をチェックする「組織点検」と、個人個人が対策の実施状況を回答する「個人点検」があります。従来、組織点検を中心に実施していましたが、現場の実態をきめ細かく把握し、より有効性の高い改善をはかるため、個人点検の実施対象を拡大しています。また、個人点検では、一般従業員と管理者を対象に実行面と管理面の点検を実施しており、両者のギャップを分析することで、管理側の問題を発見できるようにするなどの精度の向上をはかっています。

▌情報セキュリティ点検（組織点検／個人点検）



❸ 点検結果の活用による改善

点検の結果、実施が不十分な項目については、各組織において理由の把握および改善計画の立案を行い、組織的に問題解決に取り組みました。また、残課題の解決やさらなる強化が必要な内容は、次年度の情報セキュリティ推進計画へ反映することで、継続的な改善の取り組みを行っています。

6 情報セキュリティ監査

NECの経営監査本部が中心となって、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ています。監査の基準としては、ISO/IEC27001やJISQ15001に照らし、各組織の情報セキュリティマネジメントの状況を監査しています。NECグループでは、定期的に、経営監査本部による徹底した内部監査を受ける制度を確立しています。

7 ISMS認証取得の取り組み

NECグループでは、事業上ISMSの認証取得が必要な組織を対象に、ISMSの規格として必要な部分を確実に満たせるように設計された「標準コンテンツ」を核に、コンサルテーション、監査体制構築、教育、効率的な審査対応（差分審査など）のサービスを提供しています。なお、この仕組みは、NECグループやお取引先において、多数の組織が利用してきた実績とノウハウがあり、ソリューション（「NetSociety for ISMS」サービス）として提供しています。

情報セキュリティ基盤

NECグループでは、お客さま情報や秘密情報を守るために、
利用者を管理・統制して、PCやネットワーク、業務システムを安心・安全かつ
効率的に利用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IT基盤」、「PC、ネットワークを守るIT基盤」、「情報を守るIT基盤」の3つの基盤が相互に連携し、補完しあいながら、NECグループの情報セキュリティポリシーを実現しています。

「利用者を管理・統制するIT基盤」は、なりすましによるシステムの悪用の防止や利用者に必要以上の権限を与えないなどのセキュリティ対策を行うための基盤です。「PC、ネットワークを守るIT基盤」は、ウイルスやワームからPCやネットワークを守る、イントラネットを不正アクセスから守る、不適切なソフトウェアのインストールをさせない、ウイルスなどの蔓延による業務停滞を防ぐなどを実現する基盤です。そして、「情報を守るIT基盤」は、情報漏えいを防ぎ、安全に情報を利活用するために、情報機器や情報の暗号化により、万が一、第三者の手に情報が渡っても悪用を防止する、標的型攻撃対策、誤送信防止、社外作業での安全な作業、外部との安全な情報交換などを実現する基盤です。

2 利用者を管理・統制するIT基盤

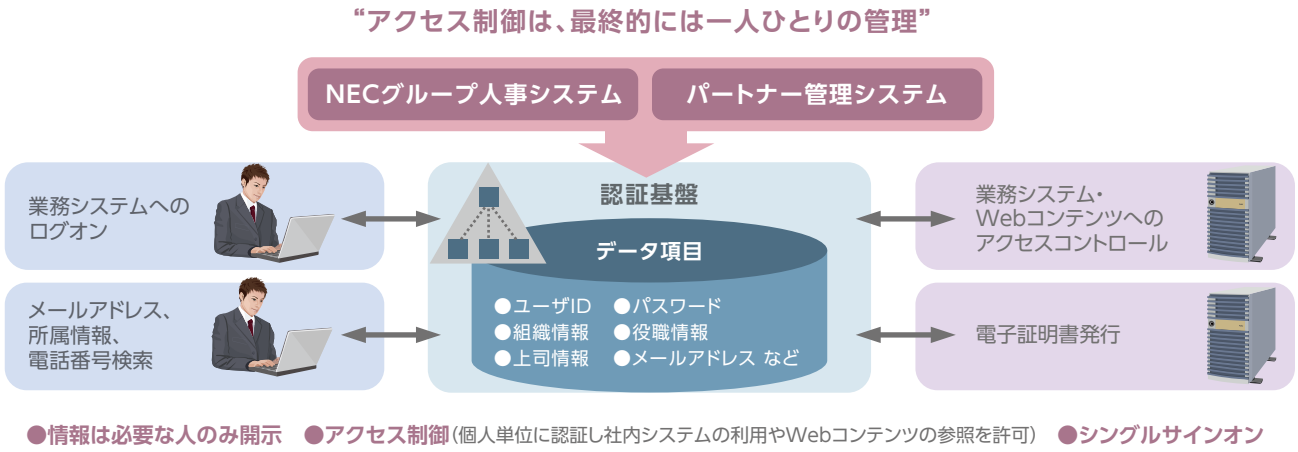
情報セキュリティにおける管理の基本は、個人認証の仕組みです。人を特定する仕組みにより、情報資産への適切なアクセスコントロールや電子証明書を利用したなりすまし防止などを実現できます。

❶ 認証基盤による適切なアクセス制御

情報資産にアクセスするためには、利用者の特定とその利用者に応じた権限の付与が重要です。そこでNECグループでは、社員だけでなく業務上の必要性に応じてお取引先なども対象として、情報を一元管理した認証基盤を構築しています。

認証情報は、ユーザID、パスワードに加え、組織情報、役職情報など個人単位でのアクセス制御を実施しています。また、NECグループ各社の認証情報がどのシステムでどの目的で利用されているのか、一元管理を実現しています。また認証情報を利用したICカード認証によるプリンタ（紙）出力も実施しています。

NECグループ認証基盤



❷ 電子メール証明書による暗号化、電子署名

NECグループ認証基盤と第三者認証機関のシステムを連携することにより、NECグループ社員に所属会社と本人を保証する電子メール証明書を発行しています。お客さま情報など重要な情報をメールで送信する際は、この電子メール証明書を利用してS/MIMEにより、なりすまし防止や暗号化を実現することで、安全なメールのやり取りを実施しています。また、内部統制やJ-SOX法対応の確証に利用するメールには、この電子メール証明書で電子署名を行い、メール差出人の身元を確実に証明しています。

③ PC、ネットワークを守るIT基盤

PC、ネットワークを守るIT基盤では、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、ネットワークを守ります。また、昨今、リスクが高まっている標的型攻撃への多層的な対策が必要となってきており、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大切です。

❶ ウイルス、ワームからPCを守る

【ユーザ利用環境支援】

NECグループでは、NECイントラネットに接続する際は、PCおよび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、ネットワークやPCの状態の見える化を実施することで、すべてのPCに必要なセキュリティ対策ソフトが確実にインストールされるようにしています。また、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の更新を自動化し、確実に適用する仕組みとしています。また、使用禁止ソフトを定義しており、ユーザのソフトウェアの適正利用についても監視しています。

【ネットワーク管理】

PCの状態を見える化するとともに、イントラネット上に侵入検知の仕組みを設けており、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りした場合、該当するPCやLANをイントラネットから遮断するよう制御しています。また、社外への通信（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の実施、フリーメール対策、SPF認証の実施）の管理も実施しています。

【運用状況の一元管理】

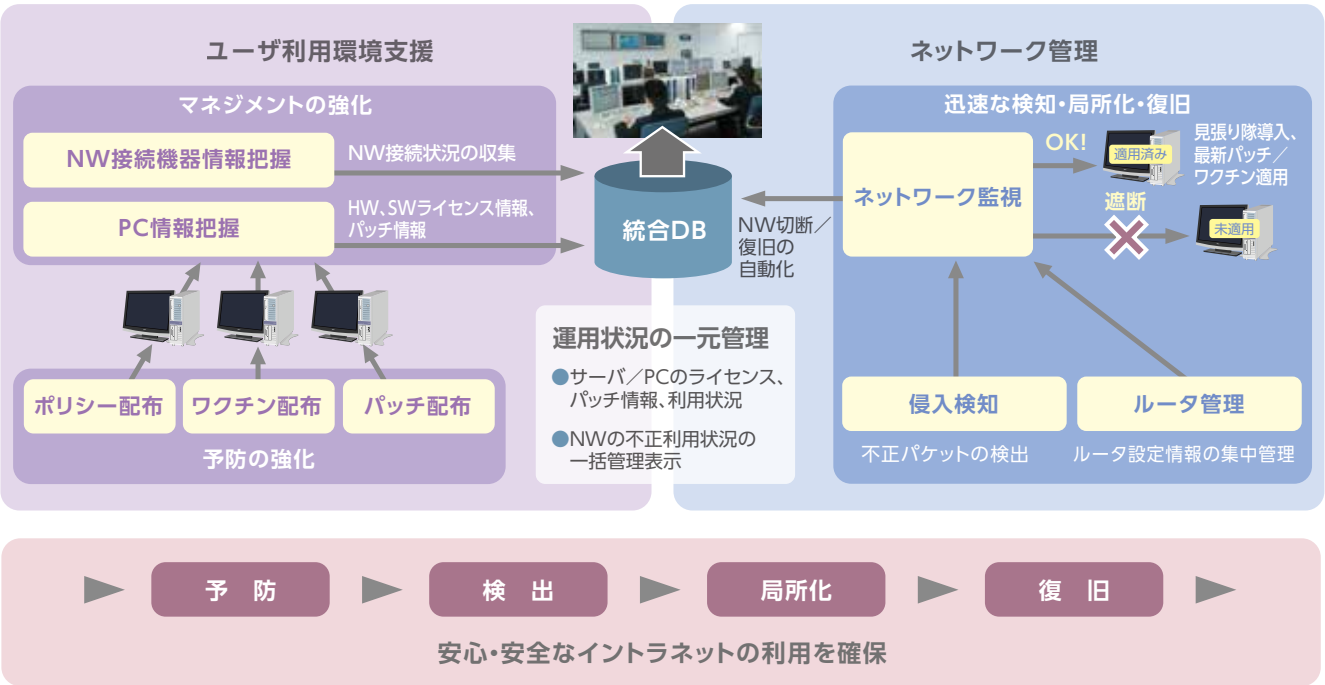
修正プログラムの適用やウイルス対策ソフトなど、セキュリティ対策の実施状況に関するデータは管理システムに集められ、情報セキュリティの管理責任者や推進者が自部門の対応状況をタイムリーに把握できる仕組みになっています。これにより、各種施策の円滑な推進と徹底を容易にしています。

❷ 脆弱性検査ツールによるチェック

脆弱性検査ツールを使用し、NECイントラネットに接続された情報機器の脆弱性をネットワーク経由でチェックしています。

発見された脆弱性は、システムにより一元管理されており、各部門の管理者は自部門の状況を閲覧して、発見された脆弱性を指示された修正方法に従い是正します。これらの是正状況についてもシステムにより一元管理され、NECグループ全体の対応状況をフォローできるようになっています。

▌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IT基盤

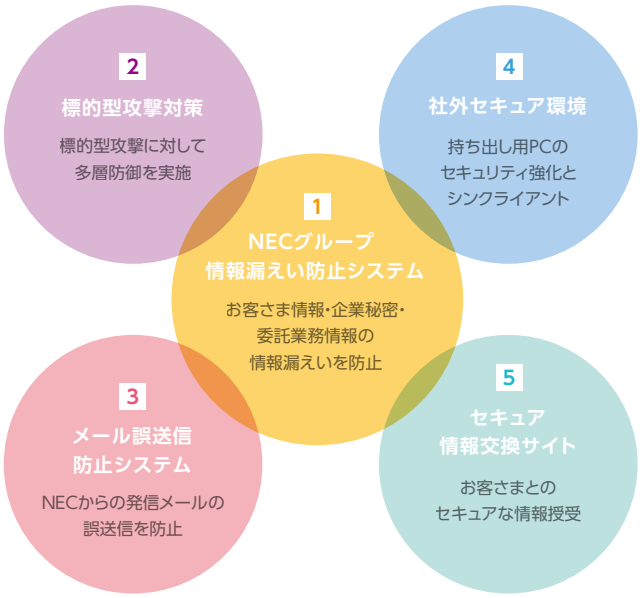
情報漏えいを防止するには、情報流出につながる経路を特定し、リスク分析を行った上で適切な対策を講じる必要があります。NECグループでは、グループの情報以外にも、お客さまからお預かりした情報やお取引先に開示する情報などを管理していますので、ネットワーク、PC・電子媒体などのITの特徴やリスクを考慮し、各経路に対して網羅的かつ多層的な対策を行っています。

❶ NECグループ 情報漏えい防止システム

NECグループでは、自社製品であるInfoCageシリーズを活用した情報漏えい防止システムを構築しています。本システムにより、ハードディスクおよびファイルの暗号化、USBメモリなどの外部記憶媒体の利用制御、PC操作の記録・監視を実現し、盗難・紛失が発生した場合でも重要な情報の漏えいを防ぎ、被害を最小限に抑えています。また、PCの操作記録の分析により、情報漏えい事故の影響範囲を特定し、状況を的確に把握するなど、情報漏えい事故の抑止、および事故分析や再発防止策の策定などに大きな効果を発揮しています。また、重要な業務に携わる従業員などのPCの操作ログの管理や、会社が許可していない外部媒体への書き出し制御などを実施しています。

▌情報漏えい防止システム概要

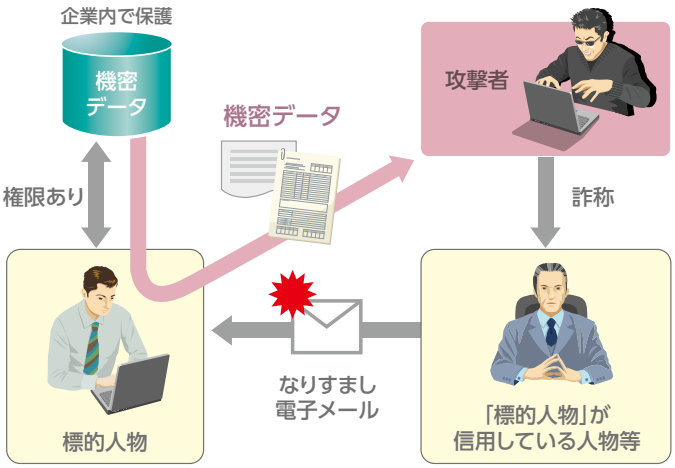
▌情報を守るIT基盤の全体像



❷ 標的型攻撃対策

標的型攻撃と呼ばれる「特定の人物に対して、送信者などを詐称したメールなどで未知のマルウェア（ウイルス）を送り、巧妙な手口で感染させることにより機密情報などを窃取するサイバー攻撃」が多発しており、組織や会社において大きな問題となっています。

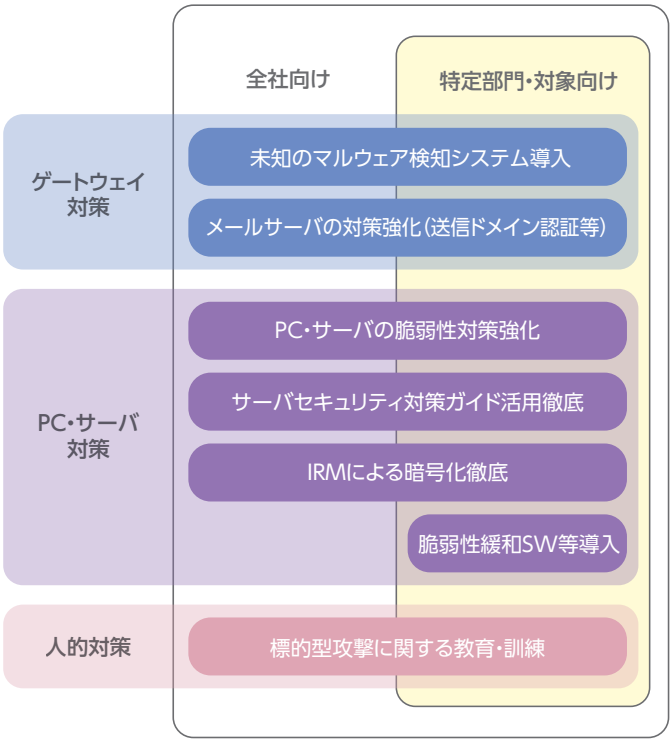
▌標的型攻撃



NECグループにおける「標的型攻撃対策強化方針」は「未知のマルウェア検知（見える化）を重点対策と位置づけるともに、多層防御の考え方を取り入れ、全社向けと特定部門・対象向けに強化が必要な対策を実施する」というものです。

具体的には、ゲートウェイ対策、PC・サーバ対策、人的対策について、全社向け・特定部門に対策の強化をはかっています。

▌標的型攻撃対策としての多層防御の考え方

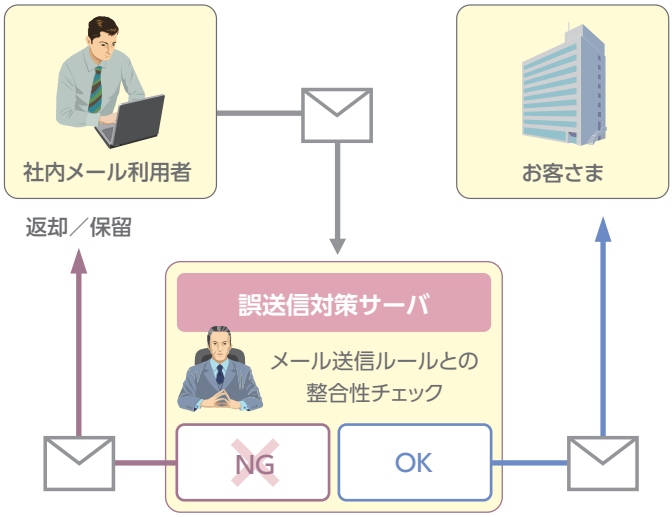


❸ メール誤送信防止システム

メールアドレスの入力間違いやファイルの添付間違いなど、些細なミスから情報漏えい事故は発生します。

NECグループでは、「メール誤送信防止システム」を導入し、NECグループ社内から社外に送信するメールは、発信前に必ず宛先や添付ファイルの内容を確認する仕組みになっています。また、上司などの第三者が宛先や内容を確認してからでないと社外へメールを送れないようにする制御も可能です。これにより、ミスの発生をさらに低減できるとともに、故意の転送などによる情報漏えいを防止しています。

▌メール誤送信防止システム



❹ 社外セキュア環境

NECグループでは、情報セキュリティ事故を低減させるため、社外でのセキュアな業務環境を構築しており、多数のグループ社員が活用しています。

【持ち出し用PCのセキュリティ強化】

PCを社外に持ち出して利用する場合、社内での利用を比較すると脅威が増大します。

そこで、盗難・紛失時におけるPC内の情報保護を強化するため、「HDD全体の強固な暗号化」、「OS起動前のプリブート認証」、「遠隔からのデータ消去/PCのロック」の機能を搭載したセキュアな持ち出し用PC(Trusted PC)をNECグループにて導入しています。このPCには「未知の脆弱性に対する攻撃を緩和する機能」や「オートランウイルス対策機能」なども搭載しており、昨今のサイバー攻撃の活発化に備えています。

【シンクライアント】

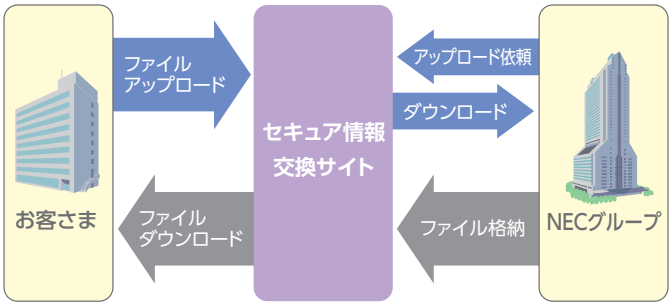
シンクライアントシステムは、運用管理の効率化と環境への配慮から仮想PC方式を採用しています。仮想PCへのセキュリティパッチ適用はシステム運用者が一斉に実施するため、標的型攻撃などで新たな脆弱性を利用した攻撃が行われた場合にも、短期間で適用を完了させることが可能です。利用者は、日々のセキュリティ対策の煩わしさから解消され、業務に専念することができます。

シンクライアント端末については、Windowsの便利さを維持しつつ、未知の脆弱性対策など高度なセキュリティ対策を実現した端末を利用しています。また、CDやUSBメモリで起動可能にしたタイプも開発しており、個人が所有するPCを会社に接続可能なセキュアなシンクライアント端末化することが可能です。これは地震などの災害対策やパンデミック(大規模感染)が発生した際に、社会インフラ関係業務の維持に重要な役割を果たす仕組みです。

❺ セキュア情報交換サイト

NECグループでは、お客さまやお取引先と重要な情報を安全・確実にやり取りするため、「セキュア情報交換サイト」を運用しています。ワンタイムURL(一回使用すると二度と使えなくなる接続先)とパスワードにより、ファイルをセキュアに受け渡しします。これにより、USBメモリなどの外部記憶媒体を持ち運ぶ必要がなくなり、外部記憶媒体の盗難・紛失による情報漏えい事故のリスクを軽減しています。

▌セキュア情報交換サイト



情報セキュリティ人材

NECグループは、ひとり一人の情報セキュリティの意識の向上をはかるとともに、セキュリティ推進のスキル向上やセキュリティプロフェッショナルを育成する各種施策を行い、情報セキュリティの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グループでは、情報セキュリティ人材を確保するために、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」、「情報セキュリティの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つの観点で施策を推進しています。

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・向上をはかるためには、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に関するWBT（Web Based Training）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。教育内容は、毎年見直しを行っており、情報の取り扱いに関する知識や意識啓発だけでなく、情報セキュリティ事故のケーススタディを通じて、リスク対応力を磨くものやよくある場面での留意点を伝えるなど、実践的な内容となっています。

❷ 標的型攻撃メール疑似体験教育

標的型攻撃メールによる企業内への不正侵入や情報搾取などのリスクが高まってきており、こうした攻撃に対するひとり一人の知識や認識が重要となってきています。NECグループでは、標的型攻撃メールの見分け方や受信した際の適切な対処方法を学べる疑似体験型の教育を実施しました。実際の業務に即したシナリオに基づいて、メール画面を操作しながら標的型攻撃メールを見分ける問題を出題し、具体的なイメージによる危機感をもってもらうとともに、判断力を養うことが可能な内容となっています。

❸ 情報セキュリティの遵守事項への誓約

NECグループでは、お客さま情報、個人情報、企業秘密を扱う際に、最低限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」を定めています。遵守事項の内容を確実に理解し実行してもらうため、NECグループ社員から誓約を取得しています。誓約は、「電子誓約システム」を運用することで効率的な管理と徹底をはかっています。

▌標的型攻撃メールの教育画面

❹ 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に対する危機感を高め、自ら考え判断して、行動できるようになるために、紛失事故と誤送信/誤配付など、主に人の行動に起因するヒヤリハットを題材にしたビデオを活用して意識啓発活動を実施しています。展開にあたっては、①職場懇談会、②なぜなぜなぜ分析、③ビデオ視聴会など、対話による気づき、分析力・判断力の向上につながる手法を提示し、各組織に適した方法で効果的に実施しています。

3 施策を推進する人材の育成

NECグループでは、情報セキュリティ推進体制を構築し、各種の施策を展開しています。各組織の推進者は、展開にあたって重要な役割を担っており、必要なスキルの養成を行っています。

❶ 情報セキュリティ推進者の育成

各組織の推進者が情報セキュリティ対策を推進する上で必要な知識（管理体制、役割、セキュリティ施策・推進内容など）を修得する教育として、新任向けの「NECグループ情報セキュリティ推進活動」を開催しています。また、各組織で異なるリスクをマネジメントするスキルを向上させるため、事故を題材にした映像を使った演習型の「情報セキュリティリスク管理スキルアップ研修」を開催し、実践力を養うとともに、リスク管理力や「自律考動」を促進しています。

❷ セキュア開発・運用の人材育成

NECグループがお客さまに提供する製品・サービスのセキュリティ品質を向上させるため、セキュア開発・運用推進者や製品・サービスの開発者／品質保証担当者を対象に、セキュア設計、サーバ要塞化、セキュアコーディングなどの「セキュア開発教育」を実施し、ノウハウの習得や定着化を通じて、セキュア開発・運用に関する人材育成の強化を進めています。

❸ 監査人育成

NECグループでは、お取引先の情報セキュリティの維持・向上のために、お取引先に対する情報セキュリティの監査（訪問点検）を施策として展開しています。手法の標準化と監査人（訪問点検）の育成のスキームを確立し、これを実施するリーダや担当者となる人材を育成しています。

4 プロフェッショナルな人材の育成

信頼される製品・サービス、情報セキュリティソリューションの提供を通じて、お客さまに価値を提供するために、情報セキュリティのプロフェッショナルを育成しています。

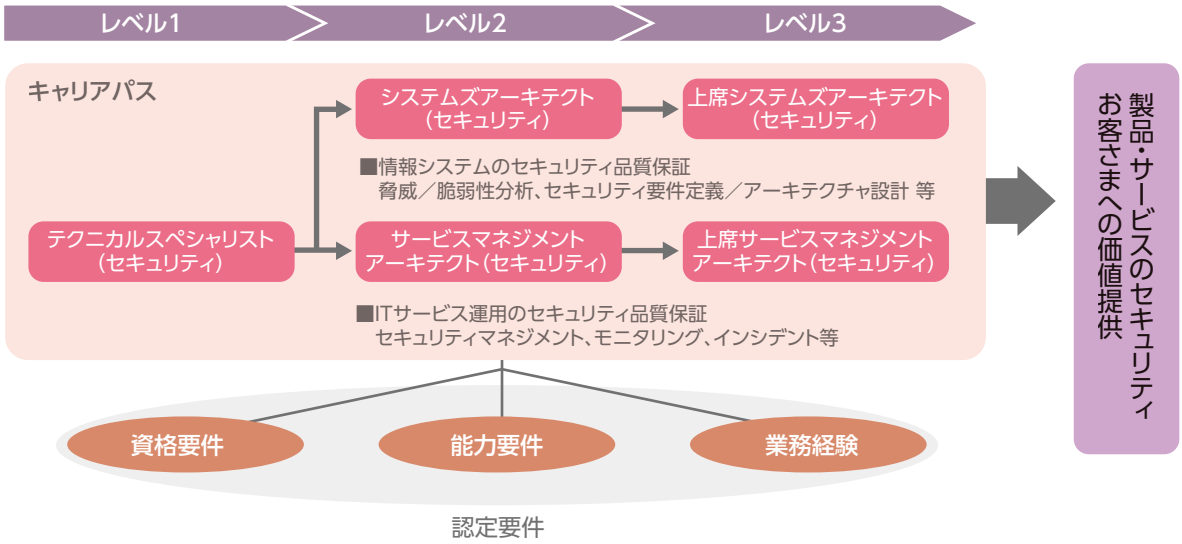
❶ セキュリティ人材の拡充

高度な専門性を有する人材を育成する制度として、プロフェッショナル認定制度を運営してきました。最近の高度化するセキュリティ脅威への対策、クラウドやスマートデバイスなどのIT利活用環境の変化、政府や業界のセキュリティ人材育成強化の動きを受け、NECグループでは、プロフェッショナル認定制度に高度なセキュリティ人材タイプを追加しました。

従来のテクニカルスペシャリスト（セキュリティ）の上位に、上流でのセキュリティ設計を重視し、情報システムのセキュリティ品質を保証する「システムズアーキテクト（セキュリティ）」とサイバーセキュリティ対応などを含むITサービス運用のセキュリティ品質を保証する「サービスマネジメントアーキテクト（セキュリティ）」を定義し、計画的な育成・強化をはかります。

情報セキュリティに関する高度なスキル、業務経験、資格を有している者が核となって、製品・サービスのセキュリティ確保やお客さまへの最適なソリューションの提供に貢献します。

情報セキュリティのプロフェッショナル人材のキャリアパス



❷ 実践特化型サイバー演習

セキュリティ対応力を向上させるトレーニングとして、CTF（Capture The Flag）と呼ばれる実践型のサイバー演習を導入しました。CTFとは、旗とり合戦のことで、例えば、「ハッキング痕跡をサーバのログから探し、その手段を解明せよ!」「アプリケーションサーバを解析し、違法行為のエビデンスを発見せよ!」などの訓練課題が与えられ、持てる技能を最大限に発揮し、いかに早く答えにたどり着くことができるかを競う演習です。巧妙に隠された解答を自ら発見し、実感することで真の理解と技術習得が可能で高い効果をあげています。

座学
（1時間）

CTF演習
（5時間）

解説
（1時間）

海外現地法人の情報セキュリティ

NECグループでは、海外現地法人においても日本国内と同様の情報セキュリティレベルを目指し、現地法人における情報セキュリティ対策（ポリシー・ルール、マネジメント、インフラ）を実施しています。

1 グローバルNECイントラネット

NECグループではグローバルNECイントラネットとして各地域イントラネットを利用して海外の150拠点以上へ接続しています。各地域のイントラネットはその地域の統括会社により管理され、地域間の相互接続などのグローバルな運用をNECが一括管理しています。

グローバルNECイントラネット

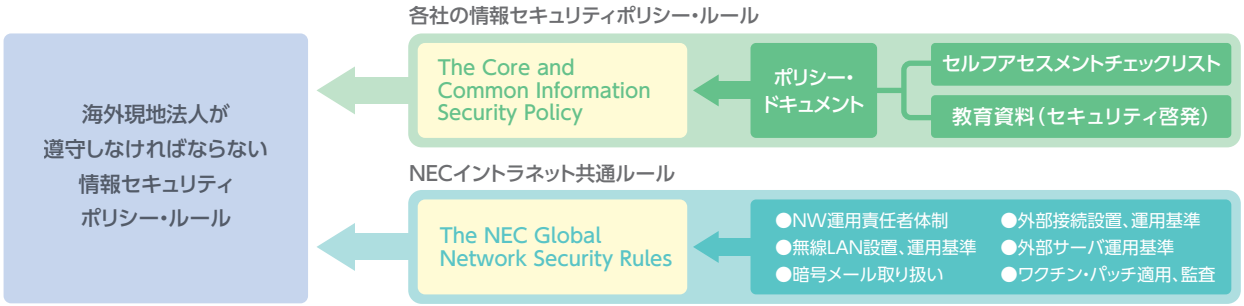
2 情報セキュリティポリシー・ルール

NECグループでは海外現地法人が遵守しなければならない共通の情報セキュリティポリシー・ルールをNECにて定義しています。

各社の情報セキュリティポリシー・ルールについては、NECが用意した雛形（The Core and Common Information Security Policy）を利用し、NECグループ均質のセキュリティ対策を推進しています。この雛形はISO/IEC27001ベースになっており、グローバルで定着化が容易なドキュメント体系となっています。各社は、所在国・地域の法規制に準拠し、自社の組織構造に合わせた役割をマッピングして、雛形と同じ内容、形式にて情報セキュリティポリシー・ルールを作成します。各社での加筆・変更内容はNECにて内容を確認し承認しています。例えば、ソフトウェア開発を受託している現地法人では、雛形に追記することで、情報セキュリティポリシーを強化しています。

また、グローバルNECイントラネット共通ルール（The NEC Global Network Security Rules）を整備しており、イントラネットを利用している現地法人はこれを共通ルールとして遵守しています。本ルールには管理体制、外部インターネットとの接続、オフィス内ネットワークなどに関するルールが含まれます。

グローバル情報セキュリティポリシー・ルール



3 情報セキュリティマネジメント

NECでは海外現地法人の従業員向けに情報セキュリティ教育のコンテンツを作成し、Webベース教育を毎年実施しています。その際、教育コンテンツを7か国語作成し、どのユーザも母国語で教育が受講できるよう配慮し、各現地法人従業員などの情報セキュリティ意識向上を目指しています。

また、各社での情報セキュリティ対策状況を把握するため、上記Webベース教育と合わせて、毎年情報セキュリティ点検を実施しています。点検結果をNECにて確認し、各社へ対策などのフォローを随時実施しています。

さらに、各社でのネットワークセキュリティ対策状況を確認するため、NECより地域毎にグローバルNECイントラネット共通ルールをベースとしたネットワークセキュリティ監査を毎年実施し、対策などのフォローを実施しています。

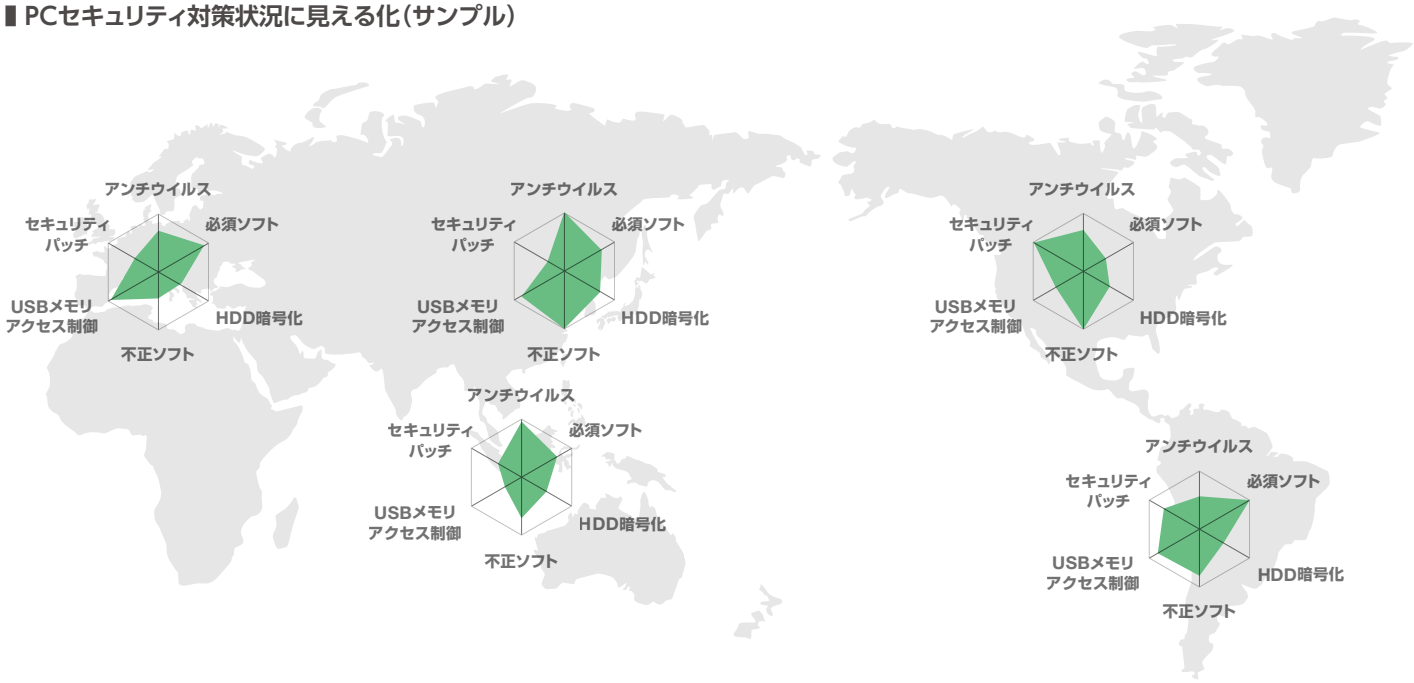
4 情報セキュリティ基盤

NECグループでは、海外現地法人においても全従業員に対して一意となるIDを配布し、グローバルID管理基盤にて一元管理しています。このIDを利用して、日本国内同様、オフィス文書の暗号化をグローバルで実現しています。

PC管理としては、海外現地法人の全てのPCのセキュリティ対策状況の見える化および、ウイルス対策、セキュリティパッチ適用の仕組みを順次導入しています。この仕組みにより、各社でのPCのセキュリティ状況を確認することが可能となります。この状況に基づき、さらにUSBメモリなどのアクセス制限（デバイス制御）、不許可PCのネットワーク検疫などの各種セキュリティ施策を展開しています。

※情報漏えい対策基盤としては、日本国内同様にグループ内でやり取りするファイルを暗号化し、認証された権限のある者しかファイルを閲覧することができない「ファイル閲覧制限管理」を導入しています。この仕組みにより、第三者への情報漏えいを防止しています。

▌PCセキュリティ対策状況に見える化（サンプル）



5 グローバルでの個人情報保護の動き

「EUデータ保護規則案」をはじめとして、各国にて個人情報保護に関する法令の動きが活発になっています。特に、EUデータ保護指令の改定の背景としては、急速なICT技術の進歩とグローバル化と、それによるリスクの拡大、および現行のデータ保護スキームの手続きの煩雑さ、などが挙げられます。この規則強化の動きについては、データ移転制限によるグローバルな事業活動や、クラウドなどの革新的サービス提供に影響があると考えられるため、その動向の確認が必要となってきています。

NECグループ内においても、情報セキュリティ基盤を支える認証情報も、個人情報として位置づけられるため、関係部門や有識者とも連携を密にして、情報システムだけでなく、法令遵守の観点から、個人情報保護に関する国際動向を随時確認しています。

また、NECは一般社団法人電子情報技術産業協会(JEITA)の委員会に参加しており、「EUデータ保護規則案」に対するJEITA意見書（日本産業界としての意見・要望）の作成に参加するなど、積極的に活動しています。

6 M&Aにおける情報セキュリティ対策

M&Aを実施する場合、買収先企業とNECグループの情報セキュリティポリシーや対策において、特に海外においては、文化や価値観の違いなど、大きなギャップが存在するケースがあります。この場合、NECグループでは前述したNECグループ共通の情報セキュリティポリシー・ルールに合わせるため、フィット&ギャップを新会社の情報セキュリティ管理責任者と実施し、早期にNECグループ会社として、情報セキュリティ対策を実施するようプロセスを確立しています。

実際に、NetCracker社やNEC Energy Solutions社のM&Aの際、このプロセスにて情報セキュリティポリシー、ルールに合わせ、NECグループ会社の一員として情報セキュリティ対策を実施しています。

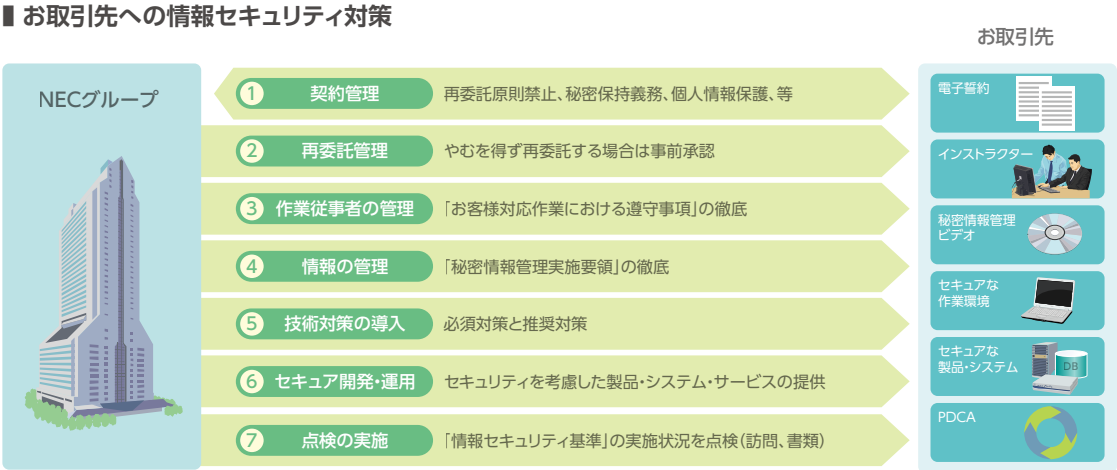
お取引先と連携した情報セキュリティ

NECグループでは、お客さま情報を守るために、お取引先と一体となって情報セキュリティ対策の浸透活動や点検および是正活動を推進し、お取引先における情報セキュリティのレベルアップをはかっています。

1 取り組み体系

NECグループの事業活動は、お取引先と連携して遂行されます。お取引先の技術力だけでなく、情報セキュリティも一定水準以上であることが非常に重要であると考えています。NECグループとしてお取引先に要求している情報セキュリティ対策は、大きく分類して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項となります。

▌お取引先への情報セキュリティ対策



❶ 契約管理

NECグループから業務を委託するお取引先との間で、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

お取引先から他社への再委託は基本契約で禁止しており、再委託の際は、委託元から書面による事前承諾を得ることとしています。

❸ 作業従事者の管理

NECグループからの委託業務に従事する作業者が守るべきセキュリティ対策を、「お客様対応作業における遵守事項」として定め、自社に対し遵守を誓約いただくことで、対策実施の徹底を推進しています。

❹ 情報の管理

NECグループからの委託業務で取り扱う秘密情報の管理について、「秘密情報管理実施要領」（秘密表示、持ち出し管理、用済み後廃棄・返還等）を定め、購入要件として実施の徹底を推進しています。

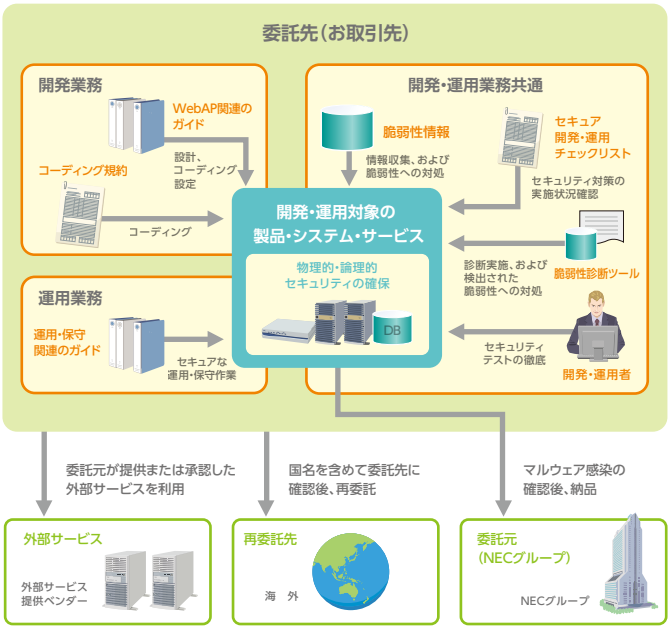
❺ 技術対策の導入

マネジメント対策との両輪として技術対策を必須の対策（可搬型電子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およびセキュア情報共有基盤）に分けて導入を依頼しています。

❻ セキュア開発・運用

2013年度から、NECグループの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、「お取引先様向けセキュア開発・運用実施要領」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。例えば、セキュアコーディング規約による開発や、製品・サービスのリリース前の脆弱性診断の実施などです。

▌セキュリティを考慮した開発・運用



❼ 点検の実施

NECグループのお取引先に対する情報セキュリティ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」（2014年度改訂）に基づき、グループ全体の標準的な仕組み（体制、手順）のもと、毎年1回（新規取引先は口座開設時）、お取引先の情報セキュリティ対策実施状況を点検し、適宜改善指導を行っています。

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

お取引先がNECグループの情報セキュリティ対策を理解し実施するために、資材部門と情報セキュリティ部門とが連携し、全国のお取引先を対象に、年1回（対象約2,000社、内ISMS認証取得会社約700社）、情報セキュリティ説明会を全国各地（北海道から九州まで12拠点）で開催しています。

❷ 重点お取引先のレベルアップ活動

NECグループとの取引が特に多い重点お取引先（約100社）を対象とした、レベルアップ説明会を年1回開催し、点検の結果や施策への対応状況などを記載した「情報セキュリティカルテ」を各社に配付し、施策の実施徹底とレベルアップ促進をはかっています。

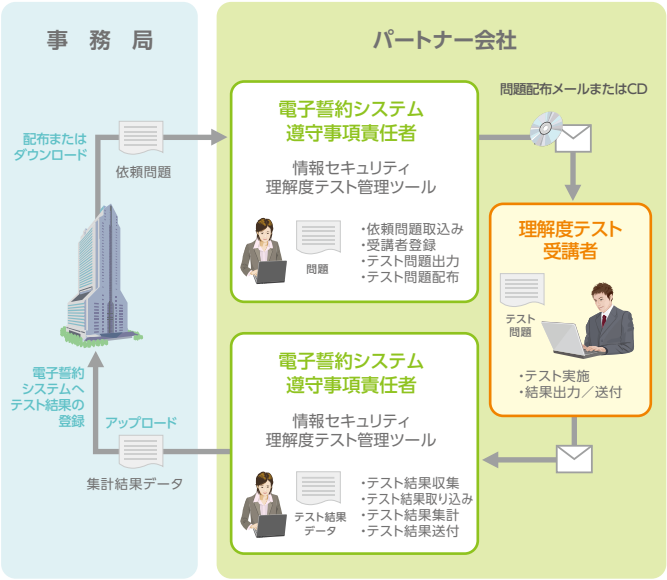
❸ 意識維持向上のためのビデオ配付

セキュリティ事故の分析結果を踏まえ、毎年、啓発ビデオを情報セキュリティ説明会で上映するとともに、お取引先に提供し、社内教育に役立ててもらうことを推進しています。これまでのビデオの題材は、遵守事項、秘密情報管理、Winny情報漏えい、ウイルス感染、飲酒による紛失、メール誤送信、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

「お客様対応作業における遵守事項」の実施徹底強化のために用意した「理解度テスト」を定期的にお取引先に配付し、各社内の教育に活用いただいています。さらに、自社のテスト結果を登録いただくと、全お取引先における位置付けをフィードバックする仕組みを構築し、運用しています。

▌理解度テストシステムイメージ



❺ 対策ガイドの配付

お取引先がNECグループの情報セキュリティ対策をより円滑に実施いただけるように、対策の実施ガイドを適宜提供しています。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、Webシステム向けセキュア開発・運用ガイド、およびスマートデバイスセキュリティルール例などを発行しました。

3 お取引先に対する点検および是正活動

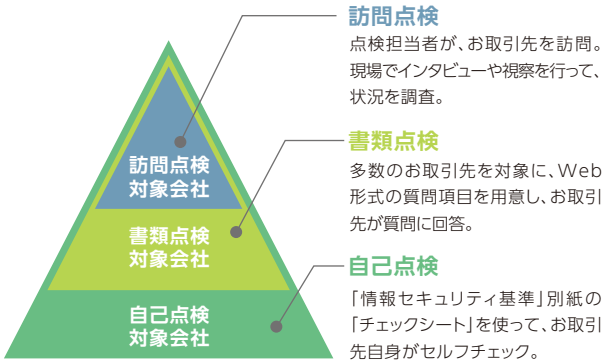
お取引先に対する点検は主に書類点検と訪問点検から構成されています。

書類点検は、NECグループと取引のある会社約2000社に対して毎年実施しています。新規のお取引先は口座開設時に実施いただきます。情報セキュリティ事故の状況などを加味して毎年作成される点検項目について、お取引先は自社の対策状況を自ら点検し、点検結果をWebシステムに入力します。点検結果はNECグループで報告書にまとめ、Web経由で各社に個別にフィードバックしています。お取引先はNECグループお取引先全体における自社のセキュリティ水準を確認できるとともに、自社が直面している課題を把握でき、効率よく改善を進めることができます。

訪問点検はNECグループとの取引が多いお取引先を対象に、毎年100社前後を選定して順次実施しています。NECグループの点検担当者として認定された者（約300名）がお取引先を訪問して点検を行うため、お取引先自身による点検（書類点検）では気づかなかった課題を発見することができます。

いずれの点検についても、改善が必要なお取引先は改善計画と改善状況をWebシステムに入力し、NECグループはその内容に基づきフォローアップを行い、お取引先のレベルアップをはかっています。

▌点検対象会社の構成



▌書類点検報告書

セキュアな製品・サービスの提供

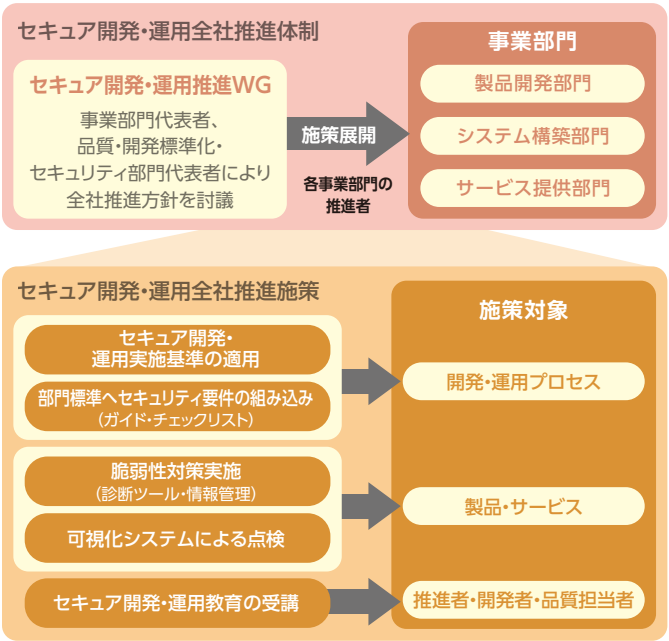
セキュリティの観点から「ベタープロダクツ・ベターサービス」をお客さまに提供するため、NECグループでは、製品・サービスにおける高品質なセキュリティを確保するためのさまざまな活動に取り組んでいます。

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・サービスに関してセキュアな開発・運用を実施できるようにするため、NECグループ全社としてセキュア開発・運用推進体制を構築しています。本推進体制は、ビジネスユニットやグループ会社の代表者からなる「セキュア開発・運用推進WG（ワーキンググループ）」と、各事業部門に配置したセキュア開発・運用推進者（約400名）で構成されます。WGでは、製品・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。本WGで決定されたセキュア開発・運用施策は、「セキュア開発・運用推進連絡会議」を通じて各部門の推進者に展開され、推進者が部門内へ施策の周知徹底、実施状況の点検、改善などを継続的に実施しています。

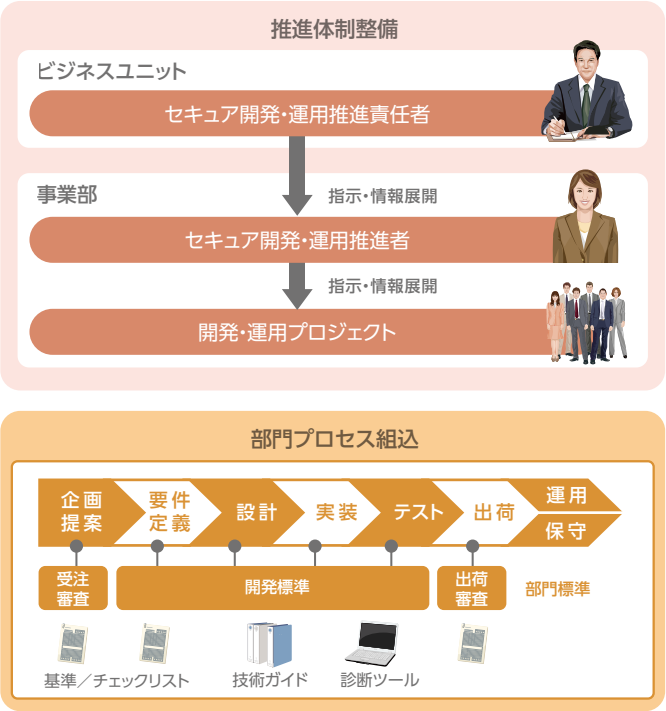
セキュア開発・運用推進体制・施策

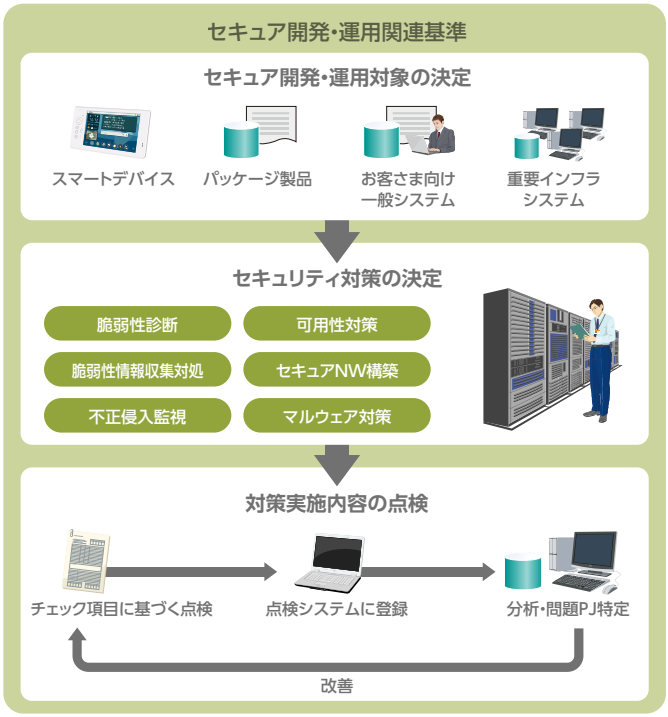


❷ 全社標準の整備

NECグループの全社標準である日本電気工業標準（NIS:NEC Corporation Industrial Standards）の一つとして「セキュア開発・運用管理規程」を制定しています。本規程では、NECグループの各部門が実施すべきセキュア開発・運用に関する取組内容（部門内の推進体制構築、部門プロセス組込、セキュア開発・運用関連基準など）について規定しています。

セキュア開発・運用管理規程





セキュア開発・運用関連基準としては、お客さま向けサービスに対するサイバー攻撃による情報漏えいや改ざんの防止を主な目的とした「セキュア開発・運用実施基準」を制定しており、脆弱性診断（ソースコード・Webアプリケーション・プラットフォーム診断）、脆弱性情報収集・対象などのセキュリティ対策を義務化しています。また、昨今増加している重要インフラを狙ったサイバー攻撃により重要インフラを停止させないことを目的とした「重要インフラ向け基準」も制定し、可用性対策、クローズド環境のセキュアネットワーク構築、マルウェア対策などのセキュリティ対策を義務化しています。各事業部門は、これらの基準に該当する製品・サービスに対して基準を適用し、基準で定めた各セキュリティ対策を実施することで、重要インフラを含む社会ソリューションの領域においてセキュアな製品・サービスを提供しています。

❸ セキュリティ品質確保

製品・サービスのセキュリティ品質を確保するために、開発・運用の各フェーズにおけるセキュリティ確認項目を定義した「セキュア開発・運用チェックリスト」を制定しています。本チェックリストは、ISO/IEC15408などのセキュリティ国際標準、政府機関が定めるセキュリティ基準、業界ガイドラインなどの要件を考慮して制定しており、さらに日々発生する新たなサイバー攻撃に対するセキュリティ対策を随時反映しています。

本チェックリストでは、要件定義フェーズ：脅威分析、設計フェーズ：セキュリティアーキテクチャ設計、製造フェーズ：セキュアコーディング・要塞化、テストフェーズ：脆弱性診断・セキュリティテスト、運用保守フェーズ：脆弱性情報収集対処・セキュリティ監視などのセキュリティ対策を定めています。本チェックリストは、ビジネスユニット・グループ会社の開発・運用標準に組み込んでおり、各事業部門の開発・運用現場で活用されています。

また、各プロジェクトのセキュリティ対策状況を見える化し、対策が不十分なプロジェクトにセキュリティ対策を徹底させることを目的とした「セキュア開発・運用点検システム」を導入しています。本システムでは、約2,000のプロジェクトを管理しており、各プロジェクトで報告されたセキュリティ対策状況を推進者が点検・監査し、問題プロジェクトへの改善などを実現しています。

❹ ソフトウェアファクトリによる集中管理と脆弱性診断

NECグループは、グループ内の各種ソフトウェア開発プロジェクトに対して、安全かつ効率的な開発をサポートするクラウド開発環境「ソフトウェアファクトリ」を運用しています。このソフトウェアファクトリではソースコードが集中管理されており、専門家チームが検査ツールを用いて脆弱性診断を実施することで、脆弱性に対して迅速かつ適切に対処しています。

2 日々発生する脆弱性への迅速な対応

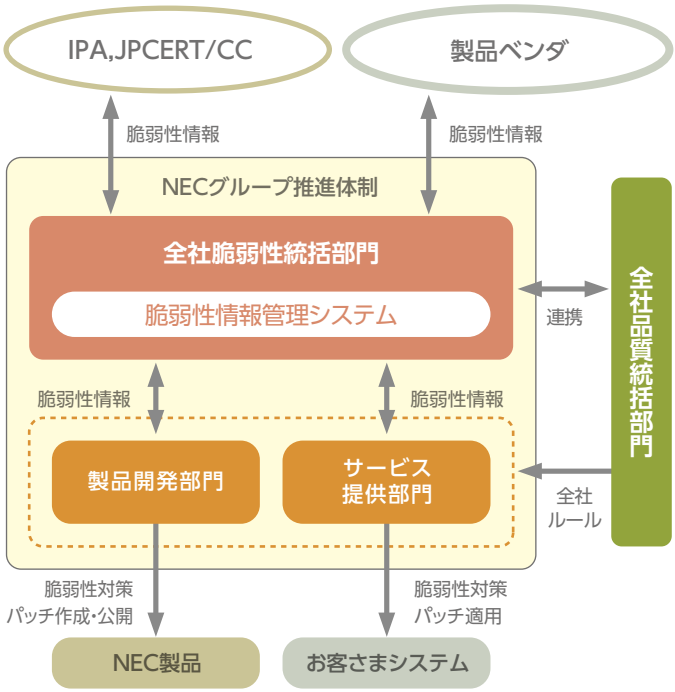
セキュリティを考慮して開発することで、セキュリティ上の欠陥である脆弱性の多くを取り除くことが可能です。しかし、使用するOSやソフトウェア製品などにも日々新たな脆弱性が発見されていますので、漏れなく迅速に対処する必要があります。

そのため、NECグループでは独自の脆弱性情報管理システムを運用し、約600名の推進体制を通じてグループ全体で脆弱性情報を共有しています。また、脆弱性対策の実施を品質確保の全社ルールに盛り込むことで、システム利用の徹底をはかっています。

自社製品については、IPAやJPCERT/CCと連携して脆弱性情報や対策パッチなどを迅速に公開する管理体制を構築しています。この体制では、出荷後の製品に脆弱性が発見された場合、脆弱性の内容が一般に公開される前に製品開発部門へ速やかに通知されるようになっています。

また、お客さまシステムや自社製品において、脆弱性対策を漏れなく迅速に実施するための体制を構築しています。この体制では、脆弱性の原因や対策方法などの詳細情報が脆弱性情報管理システムを通じて開発部門やサービス提供部門へ速やかに通知されるようになっています。さらに、対策状況をプロジェクトごとに管理し、対策が未実施の場合は警告を行うことで漏れのない確実な脆弱性対策を実現しています。

脆弱性対応推進体制



情報セキュリティの取り組み事例 ❶

NECのサイバーセキュリティ戦略

サイバー攻撃のリスクが深刻化し、攻撃対象も拡大しています。
NECは、社会ソリューション事業に注力する中、サイバー空間において、
安心・安全で快適な環境を提供し、人々が豊かに生活できる社会を実現します。

NECのサイバーセキュリティ

❶ サイバーセキュリティにおける全体戦略

昨今、標的型メール攻撃に代表されるサイバー空間を取り巻くリスクが深刻化しています。ICT（情報通信技術）の利用拡大とともに、マルウェアを利用した攻撃やシステムの脆弱性を狙った攻撃が広がっています。攻撃対象も従来の情報システムだけでなく、制御システムなどの社会インフラまで拡大しており、各国政府や企業は、グローバルなリスクとしてサイバー攻撃を認識してきています。

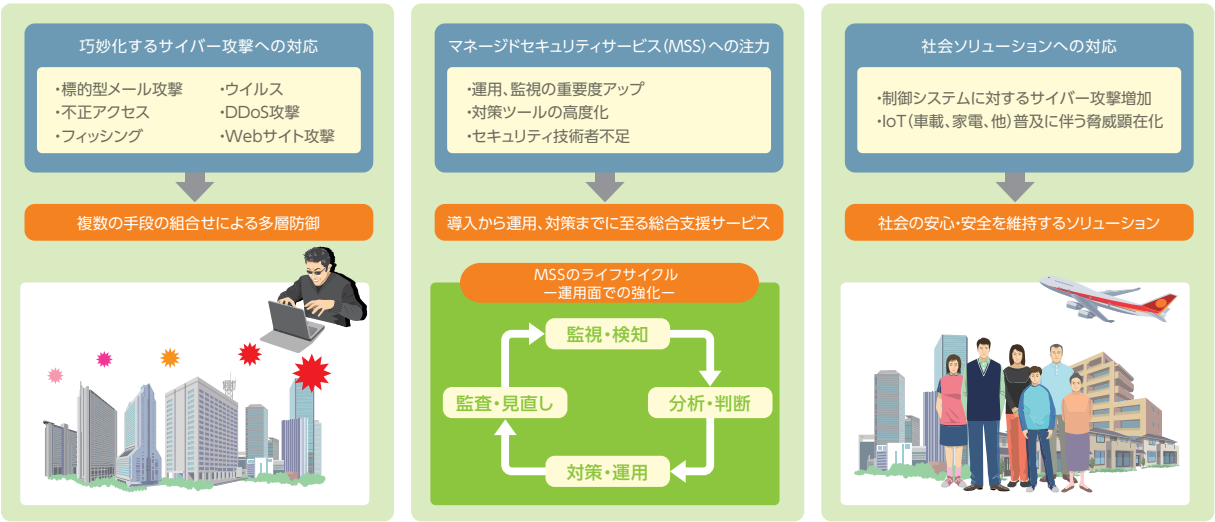
サイバー攻撃への対応は、ユーザの管理能力をこえた対応が必要であり、危険性を認識しているものの、対策率はまだ低く、安心・安全な環境を得るためのサービス提供が期待されています。

NECでは、革新的な新産業・新サービスの創出および全産業の成長の促進する社会、健康で安心して快適に生活できる、世界一安全で災害に強い社会、公共サービスがワンストップで誰でもどこでもいつでも受けられる社会といった、「世界最高水準のIT利活用社会」の実現を支えるために、サイバーセキュリティ事業を進めていきます。

❷ サイバーセキュリティ事業戦略

NECは、ITシステム、ネットワークなど、お客さま環境全体の提案ができる総合ベンダーであり、社内で培われた事例やノウハウを有し、自社開発のセキュリティ製品や差異化が可能な独自技術を持っていることが大きな強みです。2014年4月に、「サイバーセキュリティ戦略本部」を設置し、これらの強みを活かしたトータルなサービスを提供し、お客さま企業を守るためのサービス提供や社会インフラを守る事業を展開します。

▌サイバーセキュリティの事業戦略



【お客さま企業を守るソリューション】

攻撃の高度化、多様なツール、多層防御の必要性などにより、お客さまだけでは、対処が困難な状況が生まれています。そうしたサイバー攻撃の危険に直面しているお客さまに対し、NECでは、「マネージドセキュリティサービス（Managed Security Service）」のソリューションを提供していきます。

マネージドセキュリティサービスは、既存の統合ID管理、セキュアPC管理、ネットワークセキュリティ管理、サーバ/メールのセキュリティ管理、統合ログ管理といったソリューションに加え、「サイバー攻撃対策：統合監視・運用ソリューション」、「スマートデバイスソリューション」、「クラウドセキュリティソリューション」、「SDNネットワーク認証とアクセス制御ソリューション」など、新たなサービスを標準ソリューションとします。そして、単に製品導入ではなく、以下のようなマネジメントの仕組みづくりを行います。

①複数の機器が出力する情報の統合的分析
②攻撃の状況の把握
③顕在化した攻撃に対する迅速な対処の実行
④実施した対策の改善

【社会インフラを守るソリューション】

国民生活や利便性を支える社会インフラのセキュリティ課題の解決に向け、①法令施行やサイバー攻撃の脅威の高まりに応じたシステムへのサイバーセキュリティの組み込み、②PoC（Proof-of-Concept：概念実証）を通じたソリューションの共同開発と製品・サービスのセキュリティOEM供給、の2つのアプローチでソリューションの創出をはかります。あらゆるものがICTで制御されるようになり、サイバー攻撃の脅威が広がっています。例えば、「社会保障・税番号」における個人情報の分散管理、公的個人認証の活用、アクセス制御、通信暗号化など、「発送電分離」におけるオープンネットワーク、ポリシーの異なる機関間の連携、アクセス認証など、「制御システム」におけるStuxnetのようなマルウェアへの対策、あらゆるものがインターネットにつながる「Internet of Things」におけるハッキング対策、マルウェア対策などです。

❸ サイバーセキュリティ戦略を支える体制

サイバーセキュリティ戦略本部は、全社戦略を策定し、共通機能を遂行と関連する事業部門の支援により、全体の事業拡大をはかります。実際には、人材とコアプログラムへの投資を通じて、今後の核となるサービス事業の立ち上げ、および、セキュリティ事業拡大のための標準ソリューションの整備やコンサルティングや営業・SEの支援を通じて市場開拓を行います。

また、関連する事業部と連携して新規ソリューションの開発や新たな事業領域でパートナーとなるお客さまと共に、ソリューションを創出します。

❹ サイバーセキュリティ強化にむけて

NECは、今後成長が期待されるサイバーセキュリティ事業の強化に向けて、グループ企業の強化、研究・開発、人材育成、組織間連携、業界活動への参画などの取組みを進めます。

【NECグループの強化】

日々攻撃の脅威が増し標的も多様化しているサイバー攻撃に対し、政府や社会インフラを提供する事業者でのセキュリティ対策が必要とされています。NECでは、サイバーセキュリティのプロフェッショナルな人材による高度な技術力を備え、他社にはないトータルなソリューションを実現し、高品質な技術サービスを提供するために、「サイバーディフェンス研究所」、「インフォセック」をグループ会社として迎えいれました。これにより、

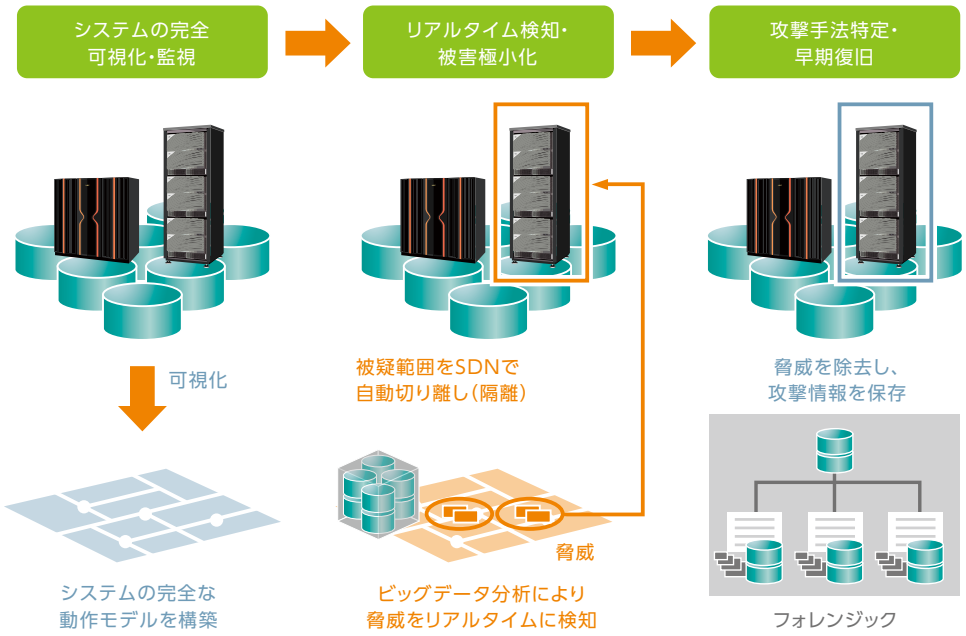
- ・セキュリティ対策の企画・立案
- ・セキュリティシステムの設計・構築、運用監視
- ・セキュリティ脆弱性診断
- ・サイバー教育・演習
- ・ハッキング、フォレンジック分野の技術サービス

などの機能を獲得し、海外企業と提携も含めた豊富な実績に基づく、質の高いサービスを提供します。

【セキュリティの研究・開発】

サイバー攻撃の巧妙化に対応するため、異常を迅速に検出し、疑わしいデバイス、ネットワークを隔離し、被害の最小化、局所化、さらには無害化するための技術を、ビッグデータ技術、SDN技術も活用し研究・開発しています。また、サイバー攻撃を受けても原理的に情報漏えいが発生しないICTシステムの実現に向けて、暗号化されているデータを復号せずに処理する、高度な暗号技術の研究・開発も行っています。

セキュリティの研究・開発



【業界活動への参画】

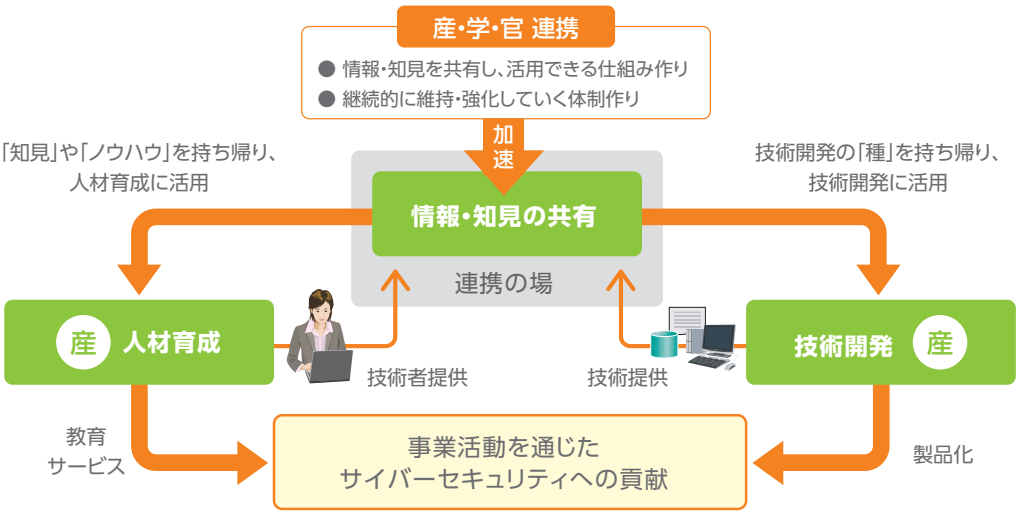
深刻なサイバー攻撃が増える中、さまざまな企業・団体が団結して、組織をこえて情報共有・連携していくことが重要です。

NECは、政府への政策提言、大学との連携、業界団体への参画などを通じて、サイバーセキュリティコミュニティを形成し、業界としての知見の拡大、対策の強化に取り組んでいます。

社会インフラを支える情報通信・公共団体・金融などの各業界におけるサイバー攻撃の分析、対策方針を検討する活動や、クラウド、制御システムといった新たな領域のセキュリティを維持確保するための研究開発、国際標準化活動、各システムのセキュリティ検証、普及啓発する活動に貢献しています。

NECはこれらの活動で得た情報・知見を、人材育成、技術開発に活用しています。

▌サイバーセキュリティコミュニティの形成と情報・知見の共有



【インターポールとの提携】

NECは、国際刑事警察機構（以下、インターポール）とグローバルなサイバーセキュリティ対策で提携（2012年12月）し、インターポールの国際的なネットワークとNECの最先端のサイバーセキュリティソリューションにより、複雑で高度化するサイバー犯罪などを調査・分析しインターポール加盟各国へ提供する最先端のサイバーセキュリティ対策の開発に取り組んでいます。

インターポールは、新たなサイバー犯罪に関する研究開発・トレーニング・捜査支援活動を行う施設（The INTERPOL Global Complex for Innovation）をシンガポールに設立。NECは、同施設内に設置される「インターポール・デジタル犯罪捜査支援センター（The INTERPOL Digital Crime Centre 以下、IDCC）」に、サイバーセキュリティに関する脅威情報を調査/分析し、新たな捜査手法を開発、トレーニングするためのシステムと要員を提供します。

両者は共同で、インターポール加盟各国へ提供する最先端のサイバーセキュリティ対策の開発に取り組みます。IDCCに構築する、捜査支援のためにサイバー犯罪の脅威情報を調査・分析し、情報発信・共有するオペレーションセンター「Cyber Fusion Centre（CFC）」、マルウェアなどを解析し、新たな捜査手法を開発する「Digital Forensic Lab（DFL）」、サイバートレーニングを行う「Training Room」をベースに、サイバーセキュリティ、デジタルセキュリティソリューションの展開が進むことで、周辺国のサイバー犯罪に対する協力活動が進み、グローバル警察事業、警察関連技術、セーフティ領域の技術融合による新たなイノベーションを繋げていきます。

写真右：INTERPOL Secretary General Ronald K. Noble氏
同左：NEC代表取締役 執行役員社長 遠藤信博

IDCCのオペレーションセンター（Cyber Fusion Centre）のイメージ

サイバーディフェンス研究所

『人間がもたらす脅威には人間しか対処できない。』サイバースペースの脅威の変化にグローバルな協調活動で対処します。専門性と高い倫理観を持つ人材を揃え、セキュリティ、ハッキング、フォレンジックなどさまざまな分野において突出したチームが高品質な技術サービスを提供し、安全・安心なサイバー社会の実現に貢献しています。

サイバーディフェンス研究所は、NECグループ内において独立性を保ちつつ、NECのサイバーセキュリティ事業を補完、強化しています。

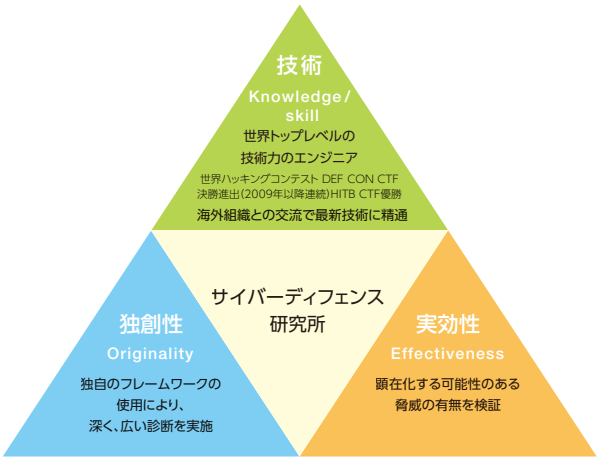
日本政府・官庁の政策への提言と社会への啓発にはじまり、官公庁・電力・交通・金融・通信などの社会インフラを提供する事業者へのセキュリティ対策を提供しています。また、パートナーを組む組織、団体、企業、ハッカーコミュニティなど、独自のグローバルな情報ネットワークとの協調活動により、最新の脅威情報、脆弱性情報、セキュリティ技術などを交換し、未来を先取りした活動を目指しています。

【セキュリティ診断】

世界トップクラスの技術力を持つエンジニアによる、高品質かつ独創性のあるセキュリティ診断で、制御システム、企業（組織）ネットワーク、Web アプリケーションの安全性を向上させます。

【コンサルティング、研究開発】

重大なインシデントが発生する前に、サイバー関連情勢の調査や想定する脅威に対する訓練シナリオの策定、サイバー演習の実施を通して、関係主体者に期待される機能・能力、そして相互コミュニケーション力を強化する活動を支援しています。各組織の適切なインシデントの予防に加え、インシデントが発生した際に被害を最小化および局限化し、迅速に回復する組織能力を確保することに貢献しています。



インフォセック

インフォセックは、2001年情報セキュリティ専門会社として設立し、官公庁や企業の情報セキュリティ管理やガバナンス確立のコンサルティングから、ICTシステム全般に関わるセキュリティ企画、サイバー攻撃対処システムの設計・構築・運用・保守、そして24時間365日のセキュリティ監視サービスにいたるまで、広く情報セキュリティおよびサイバーセキュリティに関わるサービスを提供しています。

また、インフォセックはNECのサイバーセキュリティファクトリー主要メンバーとして、監視サービスや情報分析など重要な役割を担い、また人材確保・育成の中核と位置付けられています。この活動から、国内にとどまらず海外でのサイバーセキュリティビジネスを開拓し、先端技術・製品の先行採用、海外人材の登用、運用管理ノウハウを蓄積し、付加価値を高めたサービスやインテリジェンスの提供を拡大していきます。

【セキュリティ運用監視サービス“InfoCIC”】

サイバーセキュリティ対策になると、ソフトやハード製品を導入すれば済むものではなく、むしろ導入後の運用管理、緊急時対応こそが成否の鍵を握っています。

Infosec Cyber Intelligence Center “InfoCIC”は、プロフェッショナルの目で、セキュリティ監視デバイスから生成されるログを収集・分析して、「24時間365日」常時サイバー攻撃を監視しています。また、”Cyber Intelligence”の名の通り、日々監視、分析した攻撃手法やマルウェア情報などの蓄積を行い、監視精度の向上、知見の獲得をはかっています。

情報セキュリティの取り組み事例 ②

サイバーセキュリティ・ファクトリー

巧妙化するサイバー攻撃からお客さまの情報資産を守るために、
サイバー攻撃対策の機能を集結させた中核拠点である
「サイバーセキュリティ・ファクトリー」により、高度で総合的なサービスを提供します。

NECのサイバーセキュリティ・ファクトリー

昨今、標的型攻撃などを中心としたサイバー攻撃による被害が拡大しており、公的機関の機微情報、企業の最新技術、個人情報などが組織的なプロ集団に狙われています。企業の社会的信用の失墜、事業停止など、企業活動の継続が困難になることもあり、対策の強化がますます必要となっています。

サイバーセキュリティ・ファクトリーは、サイバー攻撃対策の導入・運用を支援するために必要な仕組みを備えた中核拠点です。

NECグループ、および外部のセキュリティ専門会社との連携により「サイバー攻撃対策の専門家」を集結させ、サイバー攻撃の監視業務やインシデントの詳細解析などのサービスの提供を実際に行いながら、サイバー攻撃情報を収集・分析し、対応に必要な技術やノウハウを創出・蓄積しています。

サイバーセキュリティ・ファクトリーでは、日々進化する脅威に対応するため、技術開発、情報共有、人材育成の観点から、相乗効果を生み出す新しい形の活動として、次の5つの取組みを行っています。

❶ セキュリティ監視

最新のセキュリティオペレーションセンター（SOC）を擁し、お客さまのネットワークやウェブサイトを24時間365日体制で監視し、不正な通信やマルウェア（悪意のあるソフトウェア）感染といったインシデント対応やフォレンジックなど、セキュリティのプロフェッショナルが速やかに対応します。

❷ サイバーレンジ

サイバー攻撃を受けた際の一連の対処を模擬環境で実践するためのサイバー演習、自社および他社の製品の攻撃耐性や有用性の評価・分析を行います。また、マルウェアの解析などから得られた分析結果や知見を知識ベースに蓄積し、サイバー攻撃に対する最適な対処方法の設計やサービス、製品開発、システム設計・構築にフィードバックします。

❸ サイバーインテリジェンス

サイバー攻撃の証跡を収集し、最新の攻撃手法やマルウェアの動向を調査するとともに、連携パートナー企業、官民協議会、インターポールなどと協力し、情報の共有や知見の創出を行い、新たなサイバー攻撃手法の予測などの実現に寄与します。

❹ サイバーセキュリティ技術開発

サイバーレンジ、サイバーインテリジェンスでの知見に加え、ビッグデータの技術を活用した解析作業の自動化などの新しい技術を集結させ、サイバー攻撃対策のノウハウを活用可能な形に変えることで、より多くの高度な攻撃に対応可能な技術を開発します。

❺ 要員・ナレッジ

ファクトリーで実務経験を積み、蓄積した知見の共有を行うことにより、プロフェッショナルとして育成するとともに、サイバーレンジ、サイバーインテリジェンスの成果をサイバー演習に反映するなど、効果的な育成手法の開発に取り組み、セキュリティ人材の技術レベルの底上げや不足する技術者の育成に貢献します。

▌サイバーセキュリティ・ファクトリーの構成

▌セキュリティオペレーションセンター（SOC）

サイバーセキュリティ総合支援サービス

サイバーセキュリティ総合支援サービスは、サイバーセキュリティ・ファクトリーと連携し、コア技術やナレッジを活用するとともに、セキュリティのプロフェッショナルを擁したサービスです。「導入」、「運用」、「インシデント～回復」の3つのフェーズで構成され、サイバー攻撃対策システムの設計・構築からセキュリティシステムの運用監視、異常検知時の緊急対応などをワンストップで提供します。

❶ 導入フェーズ

導入フェーズは、脆弱性の診断やペネトレーションテストにより、お客さまのセキュリティ対策状況を診断・調査し、セキュリティコンサルティングを通じて、最適なソリューションを提案します。

❷ 運用フェーズ

運用フェーズは、運用監視サービスと定期診断サービスで構成されています。運用監視サービスは、ネットワークの入口・出口に加え、端末まで監視が可能であり、標的型メール攻撃などで内部に入り込んだウイルスなどの不正なプログラムも検知します。

定期診断サービスは、ソフトウェアのアップデートが適切に行われているか、お客さまのシステムの運用中のさまざまな変更により、脆弱性が作り込まれていないか、などを定期的にチェックします。

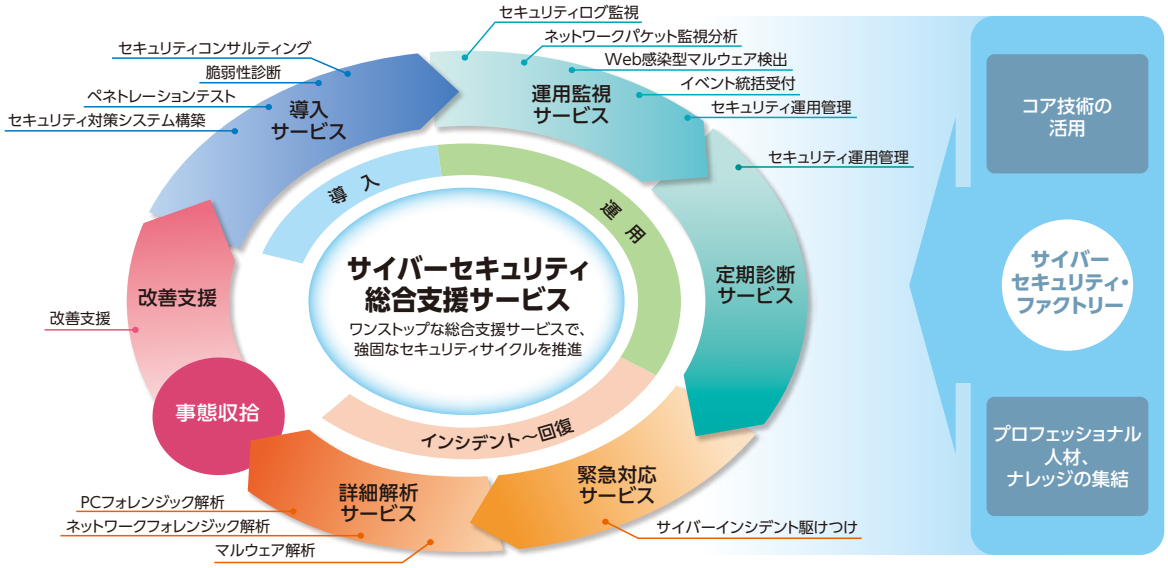
❸ インシデント～回復フェーズ

インシデント～回復フェーズは、緊急対応サービス詳細解析サービスで構成されています。緊急対応サービスは、お客さまのシステムでインシデントの可能性が高いと判断した場合に、専門要員が現地に駆けつけ、適切な初動対応・現場保全を実施する「サイバーインシデント駆けつけサービス」を提供します。対処にあたっては、サイバーセキュリティ・ファクトリーの分析官（アナリスト）と連絡をとりながら、証拠保全やシステムなどの停止・復旧などを行います。

詳細解析サービスは、PC、ネットワーク、マルウェアの解析を行い、感染源の特定や漏えいした情報の特定、被害の内容を解析します。

インシデントの原因となった問題に対しては、対応策を検討・提案し、改善を支援します。

総合支援サービスのメニュー



その他の活動

サイバーセキュリティ・ファクトリーでは、サイバーセキュリティへの理解促進や人材発掘に積極的に取り組んでおり、SECCON、Hardening、CODE BLUEなどの国内のサイバーセキュリティ・イベントの活性化に関与しています。また、サイバーセキュリティ・ファクトリの場を活かしたパートナー各社との連携を推進するとともに、CRIC（サイバーリスク情報センター）などの新しい情報共有活動に積極的に関わり、ファクトリーの知見を適用していきます。

*SECCON：日本最大規模のセキュリティコンテスト（ハッカー大会）。
日本ネットワークセキュリティ協会（JNSA）主催。
*Hardening：守る技術（堅牢化 = Hardening）を持つエンジニアを発掘、顕彰するための競技大会。
WAS Forum主催。
*CODE BLUE：日本発の情報セキュリティ国際会議。2014年2月に第一回会議開催。
*CRIC：サイバー空間におけるリスク事案および対処に関する情報共有や研究活動を行う民間団体。

社会ソリューション事業への注力

NECグループは、ICT活用によって社会インフラを高度化し、新たな価値を提供する「社会ソリューション事業」に注力しています。私たちは、世界的な社会課題を解決し、安全・安心・効率・公平といった『社会価値創造型』企業への変革を進めています。

NECが考える新しい社会インフラ

NECが考える新しい社会インフラとは、『人が生きる、豊かに生きる』ためのインフラです。

具体的には、防災・セキュリティ・電子行政・金融インフラなどの「パブリック」、情報ネットワークやそのサービスビジネスを含む「テレコムキャリア」、流通・物流インフラ・交通などの「エンタープライズ」といったお客さま基盤を軸とした3つの事業領域に、今後成長が期待される「スマートエネルギー」を加えた4つの事業領域を「社会ソリューション事業」として定義しました。クラウド基盤やブロードバンドネットワークなど、NECグループの強みであるICTのさらなる高度化をはかり、経営資源をこれらの領域に集中することで、安全・安心・効率的・公平な社会の実現に貢献していきます。

NECが注力する社会ソリューション事業

人が生きる、豊かに生きるための社会インフラを、ICTを通して提供する

ICTによる社会インフラの高度化について、NECグループは、交通管制や消防・防災システム、水管理のシステム、さらには海底地震計や電子カルテなど、既に豊富なソリューション実績を有しています。これらのシステムは、海底から宇宙までの各種センサや次世代ネットワーク技術、IT基盤技術の上で成り立っており、それぞれが社会に欠かせないインフラとして人々の生活を支えています。目には見えなくとも、私たちの日常生活になくてはならない、人が生きるためのインフラを、現在もNECのICTで支えているのです。

今後、ICTの活用において、特に重要になってくるのが情報の利活用、いわゆるビッグデータの領域です。

NECグループは、

①情報を収集する先進的な各種センサや
　ヒューマンインタフェースを含めたクラウド技術

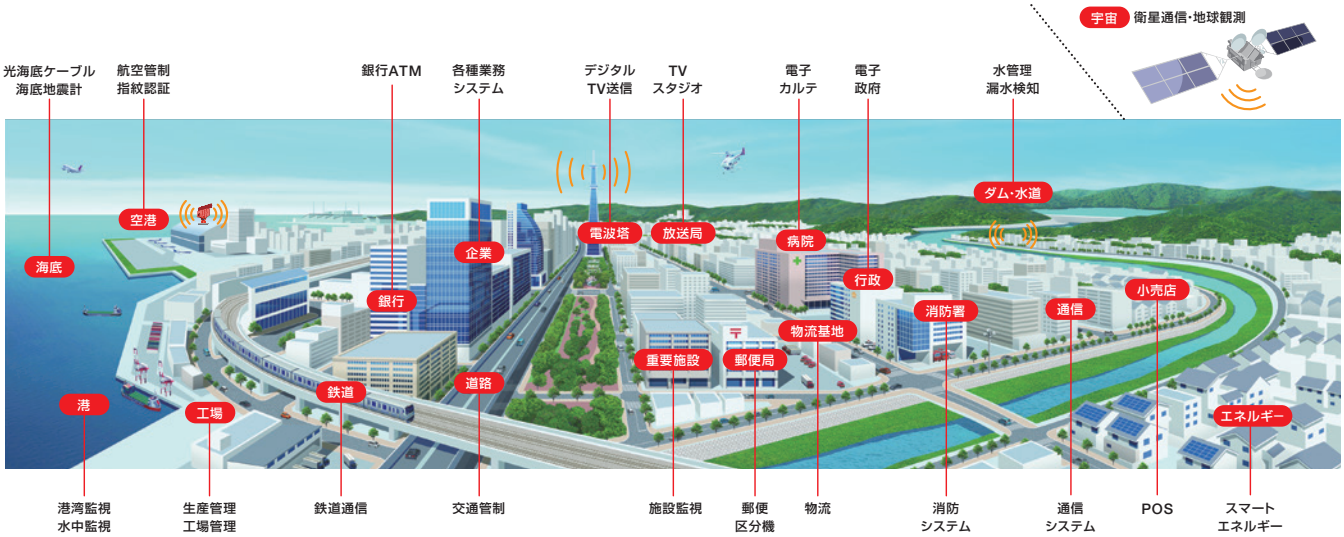
②収集した情報を分析する高性能・高信頼のIT基盤技術

③大量の情報流通を支える次世代のネットワーク基盤となるSDN
　(Software-Defined Networking)

④昨今大きな社会問題となりつつあるサイバーセキュリティ

などにおいて、独自性・競争優位性のあるICTアセットを数多く保有しています。これらのICTアセットをフルに活用することで、さまざまな社会課題の解決に向けた、新しい価値の創造に積極的に取り組んでいます。

こうした「社会ソリューション事業」への取り組みを具体化するものとして、2013年に「NEC Cloud IaaS」や「NEC Big Data Solutions」を発表しました。



クラウドセキュリティの取組み

NECは、最新のデータセンター技術やクラウド基盤サービス「NEC Cloud IaaS」により、ICTを活用した高度な社会インフラを 提供する社会ソリューション事業における注力領域であるクラウド事業を強化します。

NEC Cloud IaaSの特長

NEC Cloud IaaSは、高いコストパフォーマンスと高性能・高信頼なサービスメニューに加え、他社のクラウドやお客さまの既存システムも含めて統合運用管理できるクラウド基盤サービスです。

本サービスでは、ネットワーク構成や設定などをソフトウェアで柔軟、動的にコントロールするSDN(Software-Defined Networking)技術を活用しています。この技術により、ネットワークを仮想化し、お客さま毎に通信環境が論理的に分離された安全な環境を実現しています。また、お客さまが既存システムのプライベートアドレスを変更することなくクラウド環境に移行したり、運用ポータルからネットワーク構成の変更を自由に行うことも可能になります。

NEC Cloud IaaSは、安全性や信頼性を向上するために以下の取組みを行っています。

①利便性とセキュリティの両立
②各種スタンダードに準拠した厳格な運用
③セキュリティサービスの提供
④監査法人による有効性評価と情報の公開

❶ 利便性とセキュリティの両立

NEC Cloud IaaSが設置されている神奈川データセンターは、マシンルームへの入退管理の仕組みとして、ICカード認証に加え、顔認証とサークルゲートを採用し、なりすましや共連れを防止しています。NECの顔検出・顔照合エンジン「NeoFace®」は、米国国立標準技術研究所(NIST)の技術ベンチマークテストにおいて、世界一の精度を獲得しています。顔認証は他の生体認証と異なり、顔をカメラに向けるだけでよいため、マシンルーム利用者の利便性も向上します。

❷ 各種スタンダードに準拠した厳格な運用

NEC Cloud IaaSではCSA*1、FISC*2などが発行している各種クラウドセキュリティのスタンダードに準拠した厳格なアクセス管理を行い、信頼性を向上しています。

サービス運用におけるセキュリティ品質を担保するため、運用要員は作業時に都度、作業申請を行います。管理者が作業承認するとワンタイムIDが払い出され、運用要員はこのアカウントを使用して作業を行います。作業完了報告が完了するとワンタイムIDは失効します。全ての作業履歴は記録され、作業申請内容と作業履歴を突合するモニタリングを行い、アクセスや操作の正当性を保証する仕組みになっています。

また、ISMSの認証取得、FISC安全対策基準への準拠により、金融機関のお客さまにも安心してご利用いただくことができます。

❸ セキュリティサービスの提供

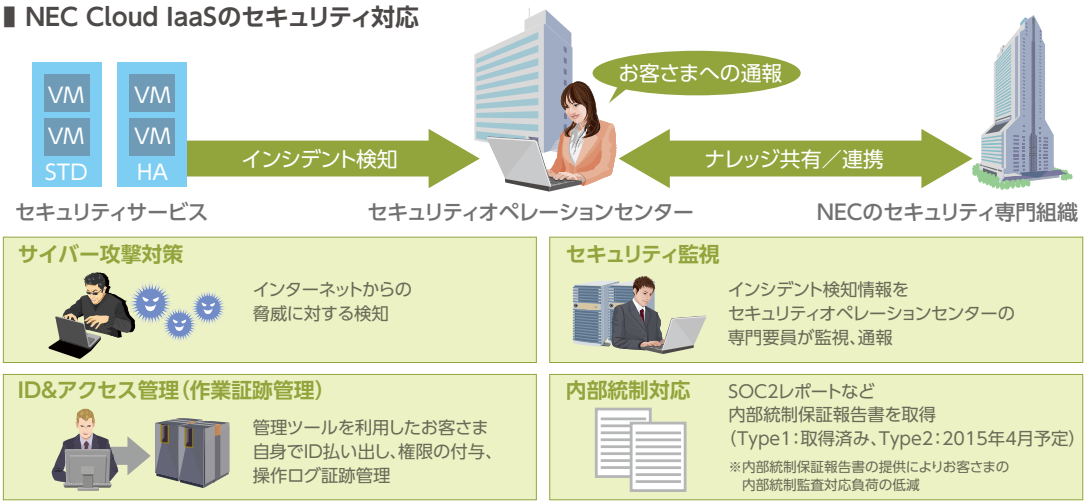
外部からの脅威に対しては、セキュリティオペレーションセンターが24時間365日体制で監視を行う不正侵入監視サービスを提供し、NEC社内のセキュリティ専門組織と連携して問題解決に当たります。また、ID・アクセス管理などのお客さまの運用の信頼性向上を支援するサービスを提供します。セキュリティ技術と内部統制対応により、お客さまシステムの安全性を向上します。

❹ 監査法人による有効性評価と情報の公開

セキュリティ、可用性、事業継続性、コンプライアンスに関するポリシーと手順を遵守していることについて、NEC Cloud IaaSは監査法人による検証を予定しています。監査法人による検証報告書(SOC1、SOC2*3 Type2 報告書)を2015年4月に取得予定です(一時点の評価であるSOC2 Type1報告書を神奈川データセンターで取得済み)。

*1 CSA:The Cloud Security Alliance　*2 FISC:The Center for Financial Industry Information Systems
*3 SOC1,SOC2:Service Organization Control1,2

NEC Cloud IaaSのセキュリティ対応



ビッグデータソリューションとセキュリティ技術

NECは最先端のメディア処理技術と独自の分析技術を開発し、
お客さまとの共創によるノウハウを活用して、
さまざまな社会課題の解決に取り組んでいます。

1 NECのビッグデータ活用ソリューション

NECは世界トップクラスのメディア処理技術と、高度なデータ分析技術により、実世界の多様な情報を意味解析し、新たな法則の発見や将来の予知・予測を実現しています。これらの技術は、以下のような領域でその有効性が確認されています。

❶ オペレーションの高度化・最適化

社会システムの大規模化・複雑化に伴い、安定稼働を維持するための業務負荷は増大の一途です。

NECは、センサデータの相関を可視化し、「いつもと違う挙動」を早期に発見するインバリアント分析技術により、収集したセンサデータの相関性やバランスを常時監視し、プラントやネットワークの故障予兆監視や構成機器の品質管理、インフラ構造物の異常検知を実用化しました。

❷ 製品/サービス価値の向上・改善

膨大なデータから将来予測し、適切な対応を行うには、経験豊富な専門家の確保が必要となります。

NECは多種多様なデータ群から複数の規則性を導出し、状況に応じた規則の選択により高精度に推定する異種混合技術を開発しました。この技術により、実績データと現在の関連情報の相関性に基づく将来予測を実現しました。

❸ 情報管理の強化、犯罪・不正の検知

治安や経営を左右するリスク情報を網羅的に把握するには、膨大な工数が必要となります。

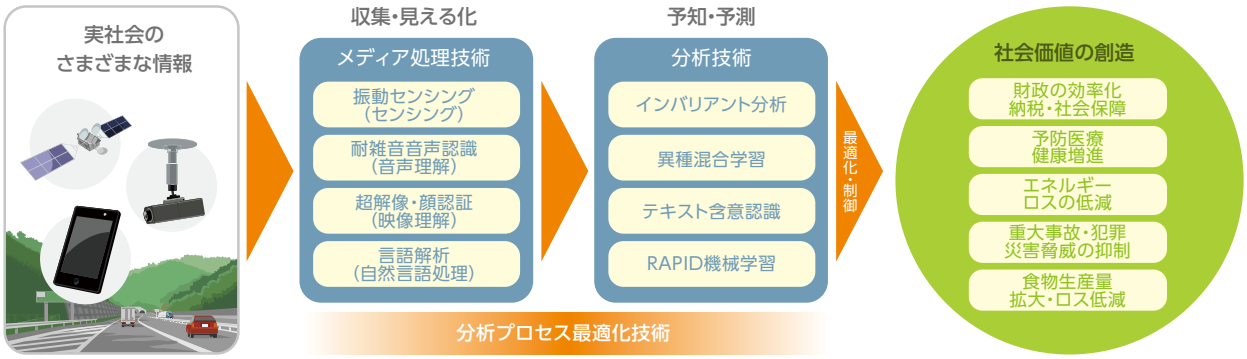
NECは「管理すべき情報が含まれているかどうか?」を文意から自動判定するテキスト含意技術を開発しました。この技術により、注視すべきコンテンツを自動抽出し、特定情報のみを厳密に管理することで、企業内の情報ガバナンス強化やサイト・SNSの動向分析などを効率的に行います。

❹ カスタマーマネジメント(傾向分析)

多種多様なデータから傾向を適切に把握するには、事前の仮説設定とルール作りが重要です。

NECは人の思考と類似したプロセスを自動化する機械学習技術により、行動分析やプロファイリングに関する仮説の有効性の検証を実現しました。

▌メディア処理技術と分析技術による価値の創造

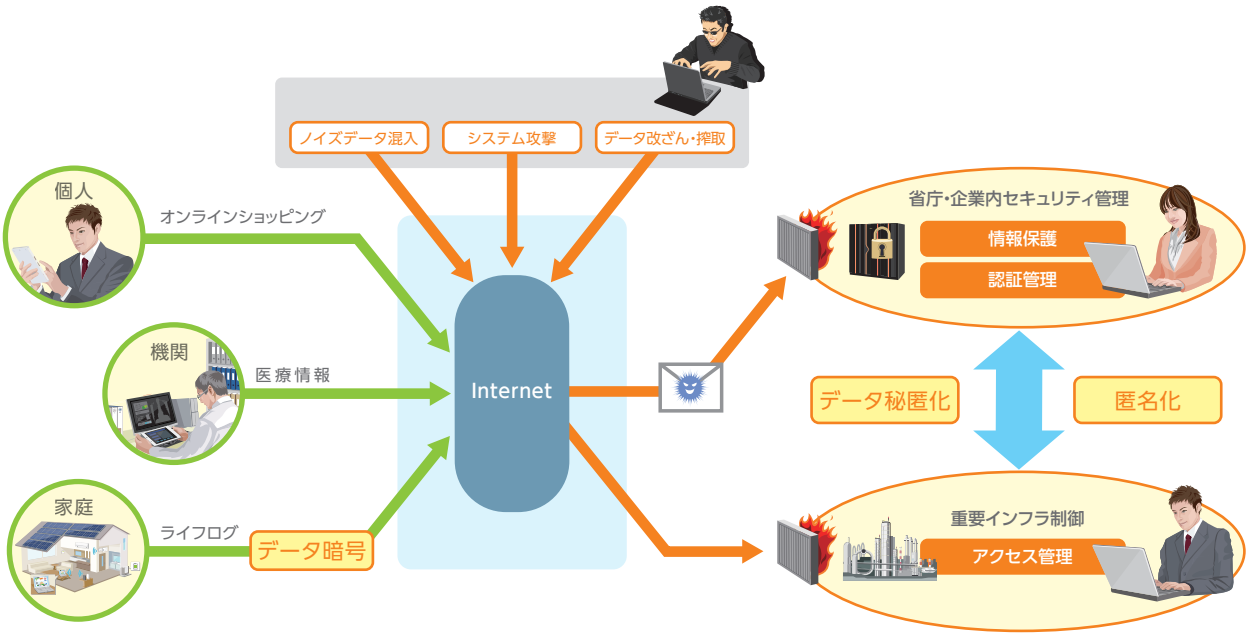


2 ビッグデータ環境でのセキュリティ課題と対応

NECが提供するデータ分析技術は、未知の攻撃に対する迅速な対処にも有効です。例えば、産業システムへの攻撃に対して、稼働状況をインバリアント分析し、未知の攻撃に対する予兆をいち早く検知することで被害の最小化を実現します。また、セキュリティインシデントが発生した際に、専門家の勘と経験に依存せずにログデータやイベント情報を自動的に分類・解析し、データや発生した事象の相関性に基づく仮説を効率的に抽出することが可能となります。さらに、インターネットやコミュニティサイトから、サイバー攻撃に関するインテリジェンス情報を定期的に収集・分析することで、サイバー犯罪や不正の予兆をいち早く確認し、適切な事前対処を実現します。

一方で、社会システムのビッグデータ活用が普及することにより、新たな脅威や問題が発生する可能性があります。NECはビッグデータ解析技術の実用化による価値創造と併せて、起こりうるセキュリティインシデントに向けての技術開発を進めています。例えば、システムに不正侵入することによるシステム稼働停止に加えて、①センサデータの改ざん・搾取、ノイズデータの混入による誤動作、あるいは②特定のパーソナルデータの搾取などへの対処が必要となります。

新たな脅威に対するビッグデータ解析技術の活用



❶ データの改ざん・搾取への対処

ビッグデータ活用の特徴として、人の経験や知見だけに依存せずに、データそのものの推移や相関性にのみ注目し、予測する点があります。そのため、現在の厳密な認証基盤の整備に加えて、データそのものの秘匿化や信頼性を検証する手段が必要となります。

収集・分析したデータが機密情報の場合、管理されるデータはデータベース内で暗号化されていても、データ処理時にデータベース上でデータが復号されるため、データベースの管理者や管理者の権限を盗み取った者からデータの改ざん・搾取されるリスクがあります。

NECは世界に先駆けて、収集・分析したデータを暗号化したまま再利用できる秘匿計算技術を開発しました。これにより、データベースの管理者やデータベースの管理を委託された者によるデータの盗み見といったリスクがなくなります。また、標的型攻撃などで攻撃者がデータベース管理者権限を獲得したとしても、データそのものの搾取や改ざんをデータベース側で防止することが可能となります。

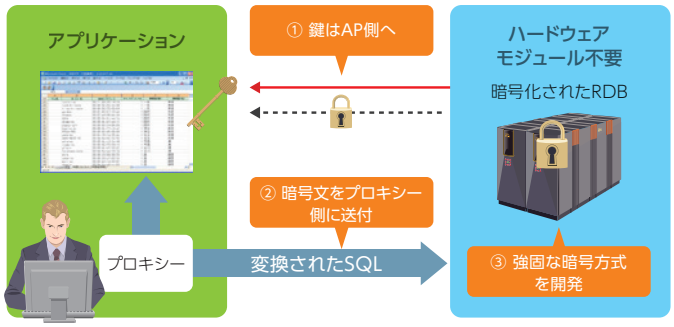
❷ 特定のパーソナルデータの搾取への対処

ビッグデータの適用例として、収集・分析した情報をさまざまな業務や用途に利活用するケースがあります。特に、収集する情報が個人のライフログといったプライバシーに関わる場合、関連する情報と紐付ける事で個人を特定化される可能性があり、安全管理の徹底が求められています。

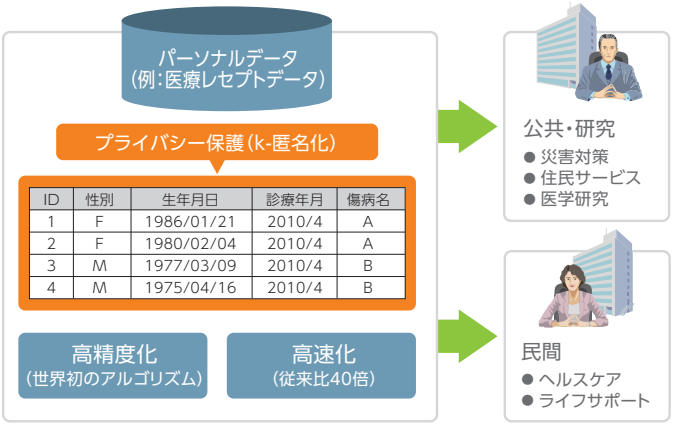
NECは個人の傾向や特徴を把握するために必要な情報を失わずに、個人が特定されるリスクを低減する匿名化技術を高速に処理する仕組みを開発しました。これにより、医療情報や健康情報、さまざまな行動履歴情報といったパーソナルデータの安全な有効活用が可能となります。

NECはビッグデータ関連技術の実用化を通じて、お客さまとの新たな価値創造に取り組むと共に、セキュアに情報の利活用を活性化する安心・安全な社会システムの実現に貢献します。

秘匿計算技術



匿名化技術（k-匿名化）



情報セキュリティの取り組み事例 4

グローバルセーフティ事業の取り組み

NECは、成長戦略の柱の一つとして、これまで培ってきた技術に、海外現地のSI力、顧客基盤を強化し、現地主導型の「セーフティ事業」のグローバル展開を加速しています。

NECのグローバルセーフティ事業

【Safer Citiesの背景・コンセプト】

「Safer Cities（セーファー シティーズ）」は、NECがグローバルに展開するセーフティ事業の新体系です。人々が安全・安心に、幸せで豊かな生活を送ることができる世界を実現するため、危機の未然予防や、対応力を強化する先端技術、ソリューションを提供します。

NECはSafer Citiesのグローバル展開を強化するため、シンガポールに、グローバルセーフティ事業部を設立しました（2013年）。日本国外に拠点をおくことにより、グローバルな市場情報・ニーズに基づいた戦略の立案、新技術・ソリューションの開発、これまでの海外におけるソリューションの経験と能力を十分に生かした重要市場への展開を実現しています。また、新たな研究拠点として、同じくシンガポールにNECラボラトリーズシンガポールを設立しました（同年）。シンガポールでは、政府機関や大学などによるさまざまな都市問題を解決するためのプロジェクトが多数活動しており、新たな技術やソリューションの研究、および実証を行っています。こうした技術やソリューションは、東南アジア諸国だけではなく、南米、アフリカといった新興国などへの展開を図っています。

【Safer Citiesの7つの事業領域】

都市人口の増加やテロ攻撃の脅威等、国家や都市レベルの安全を脅かし、重大な危険や傷害をもたらす可能性がある事象に対し、NECはさまざまな技術・製品・サービスなどを組み合わせて提供しています。「Safer Cities」では7つの事業領域でソリューションを用意しています。

❶「国民ID・出入国管理」

世界最高精度を誇る指紋照合・顔照合などのバイオメトリクス照合技術をコアに、国民IDシステム、選挙ID管理システム、出入国管理システムなどを実現するソリューション。

❷「犯罪対策」

世界一の精度を誇るバイオメトリクス照合技術を中心に、監視カメラ映像による人物検知や犯罪捜査支援などの治安維持を支援するソリューション。

❸「重要施設監視」

空港、港湾、発電所、ガス施設、プラント、スタジアムなど、被害が社会生活に大きなインパクトを与える重要施設において、脅威の発生を未然に防ぐ、映像監視や高機能センシングシステムを中心としたエリア監視、および警戒警備を実現するソリューション。

❹「防災・救急」

地震、津波、洪水、火事、台風など自然の脅威に対し、災害の発生を事前に把握し、災害発生時の被害を最小限に押さえ、平常の状態に復旧させるためのソリューション。

❺「行政サービス」

NECが長年培ってきた技術を活用し、感染症の予防や電子政府化など、公共の安全・安心につながる行政サービスを支えるソリューション。

❻「サイバーセキュリティ」

人々の生活に大きな影響を与える情報化社会において、サイバー空間の安全を実現するソリューション。

❼「省庁間連携」

自治体、省庁、関係機関など、さまざまな組織間の情報を共有するためのネットワークインフラや、ビッグデータから有用な情報を抽出・提示するデータ分析・可視化ソリューション。

▌Safer Citiesの7つの事業領域

セーフティ事業のソリューション事例

NECは、セーフティ関連のソリューションを世界40カ国で500システム以上導入しており、これらの豊富な実績をもとに、技術・製品・サービスの開発、パートナー連携、顧客への積極的な提案をグローバルに展開し、新たな価値創造と高度な社会インフラの構築に貢献していきます。

❶「国民ID・出入国管理」のソリューション

NECは、国民IDなどの国家レベルから公共機関、企業まで、安全・安心な社会生活を実現するための公共安全基盤のソリューションを提供してきました。

【バイオメトリクス認証】

顔照合技術は、他のバイオメトリクス技術にはない、離れたところから認証情報を取得できるメリットを持っており、新しい市場開拓が可能な基盤技術として研究開発から事業化までを強化しています。また、指から指紋だけではなく静脈などの情報を一度に取得することで、精度を高めたマルチモーダル指認証技術や大型の解析装置を何台も備えた研究室でなければできなかったDNA解析を持ち運び可能な装置で処理することを実現する、ポータブルDNA解析装置の開発などを進めています。

【入国管理ソリューション】

シンガポールとマレーシアの境界（コーズウェイ橋）では、20万人/日以上が出入りしており、NECは、シンガポールのICA（出入国管理局）と共同で旅行者の出入国を迅速に処理できるシステムであるEIACS（自動出入国管理システム）を納入しています。パスポート保持者の指紋データを格納した「バイオパス」という電子パスポートにより、セキュリティ・ゲートでパスポート番号や指紋が一致しなかった場合、自動的に通報されます。この指紋認証システムの他人誤認率は0.001パーセントで、世界で最も精度が高い指紋認証技術が採用されています。

国民ID・出入国管理

●主なソリューション
- 国民IDシステム　・選挙ID管理システム
- 出入国管理システム
- e-Passport/e-visaシステム

●導入実績
- 南アフリカ　国民IDシステム
- シンガポール　e-Passport/e-visaシステム
- マカオ　自動出入国管理システム

❷「重要施設監視・省庁間連携」のソリューション

NECは、各種センサーや解析技術などにより、社会インフラ基盤設備のセキュリティソリューションの実績を多く持っています。

【シンガポール 安全都市実証実験】

NECは、シンガポール内務省（MHA）、シンガポール経済開発庁（EDB）主導によるパブリックセーフティ分野の実証実験「Singapore Safe City Testbed」に参加し、安全かつ安心な社会を維持する新技術の研究開発・実証を行いました。本実証実験は、都市問題の解決に向けた政府機関横断の情報連携基盤「Inter-Agency Collaboration（IAC）」の実現を目的としたものです。NECは、複数の政府機関がそれぞれ保有するセンサーやネットワークを統合してデータを収集し、ビッグデータ分析、相関モデリング、リスク判定等をベースとした分析技術を用いて事件・事故の発生や予兆を検知し、関連する政府機関に安全かつ迅速に情報の発信を行うソリューションを開発・実証しました。具体的には、NEC製・他社製を問わず解析エンジンを接続し、リアルタイムの大規模監視を実現する「メディア解析プラットフォーム」、デジタル署名技術を応用し、監視カメラとその映像の正当性を検証して信頼性を高める「e-Evidenceテクノロジー」、公共の場において、非常事態発生時に警告の表示や避難経路の誘導を行う「共有デジタルサイネージ」といった新技術の開発で成果をあげています。

【アルゼンチン ティグレ市 街中監視システム】

NECは、アルゼンチン ティグレ市の街中監視システムに世界No.1の高速・高精度な顔認証技術を提供しています。主に鉄道や船のターミナル駅などに設置されたネットワークカメラの映像と膨大な写真データベースをリアルタイムに照合することで、検察・司法機関・公共福祉団体などにおいて、行方不明者の捜索などの監視を実現しています。

また、ひったくりなどの犯罪につながりやすい「バイクの2人乗り検知」や安全のための「ノーヘルメットでの運転検知」、不審な行動（車両）を見つける「行動検知」、不審車両の特定のための「ナンバープレート認証」などの独自技術を開発し、提供しました。また、過去の犯罪発生地域を表示する「犯罪発生マップ」などの先進機能も納入しています。これらの最新技術を街中監視システムに統合し、街中のさらなる安全対策に貢献しています。

重要施設監視・省庁間連携

●主なソリューション
- 高機能センシングシステム
- 映像監視ソリューション　・可視化ソリューション
- プラント監視システム　・ビッグデータ解析システム

●導入実績
- ブラジル スタジアム監視システム
- シンガポール Singapore Safe City Test Bed
- アルゼンチン 街中映像監視システム

第三者評価・認証

NECグループでは、情報セキュリティに関連する
第三者評価・認証の取得に積極的に取り組んでいます。

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
- NECエンジニアリング株式会社
- NECソリューションイノベータ株式会社
- NECソフト沖縄株式会社
- 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ネットワークプロダクツ株式会社
- NECビジネスプロセッシング株式会社
- NECフィールディング株式会社
- NECプラットフォームズ株式会社
- NECマネジメントパートナー株式会社
- NEC東芝スペースシステム株式会社
- NECトーキン株式会社
- NECキャピタルソリューション株式会社
- 日通NECロジスティクス株式会社
- 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
- 埼玉日本電気株式会社
- 長野日本電気株式会社
- 静岡日電ビジネス株式会社
- 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
- 株式会社KIS
- 株式会社N&J金融ソリューションズ
- 株式会社NEC情報システムズ
- 株式会社サイバーディフェンス研究所
- 株式会社インフォセック
- 株式会社サンネット
- 株式会社ネットコムセック
- 株式会社ワイイーシーソリューションズ
- 昭和オプトロニクス株式会社
- 日本アビオニクス株式会社
- 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

（順不同）

プライバシーマークの取得状況

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取得

- 日本電気株式会社
- NECエンジニアリング株式会社
- NECソフト沖縄株式会社
- NECソリューションイノベータ株式会社
- NECトーキン株式会社
- 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ネットイノベーション株式会社
- NECパーソナルコンピュータ株式会社
- NECビジネスプロセッシング株式会社
- NECフィールディング株式会社
- NECファシリティーズ株式会社
- NECプラットフォームズ株式会社
- NECマネジメントパートナー株式会社
- NECマグナスコミュニケーションズ株式会社
- 株式会社NECライベックス
- NECフィールディング システムテクノロジー株式会社
- 静岡日電ビジネス株式会社
- 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
- ネッツエスアイ東洋株式会社
- VALWAY121ネット株式会社
- 株式会社KIS
- 株式会社N&J金融ソリューションズ
- 株式会社NEC情報システムズ
- 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
- リバンスネット株式会社
- アビームコンサルティング株式会社

（順不同）

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。

ISO/IEC15408認証取得製品・システム

- StarOffice X（グループウェア）
- WebSAM SystemManager（サーバ管理）
- InfoCage PCセキュリティ（情報漏洩防止ソフトウェア）
- WebOTX Application Server（アプリケーションサーバ）
- 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グループ情報漏洩防止システム（情報漏洩防止ソフトウェア）
- NEC ファイアウォール SG コアユニット（ファイアウォール）
- PROCENTER（文書管理ソフトウェア）

NECグループの概要

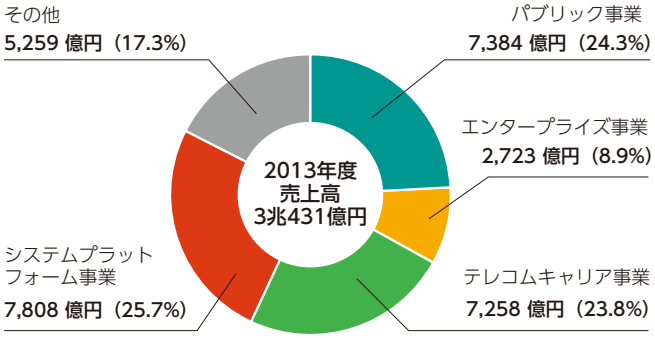
会社概要

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	3972億円※
連結従業員数	100,914名※
連結子会社数	258社※

※2014年3月31日現在

事業紹介

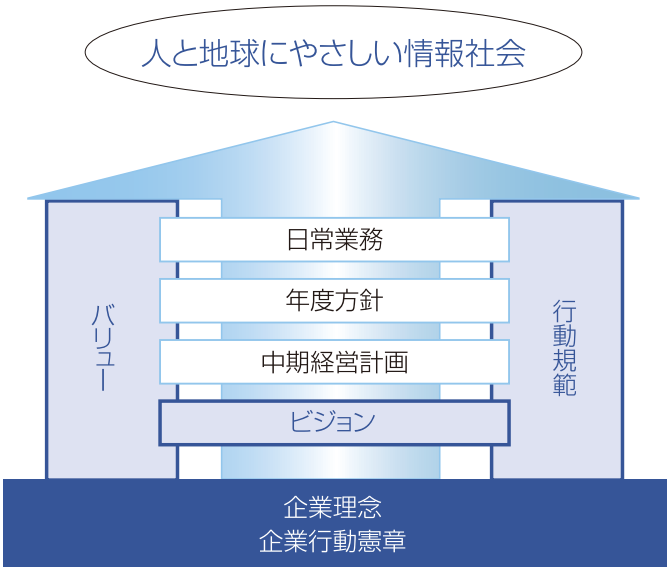
セグメント別売上高(構成比)



※2014年3月31日現在

NEC Way

「NEC Way」は、企業理念、ビジョン、バリュー、企業行動憲章、行動規範を含むNECグループの経営活動の仕組みを体系化したものです。私たちはNEC Wayの実践を通してお客さまやその先の社会に貢献し、人と地球にやさしい情報社会を実現していきます。



NECグループ 企業理念

NECはC&Cをとおして、
世界の人々が相互に理解を深め、
人間性を十分に発揮する
豊かな社会の実現に貢献します。

1990年制定

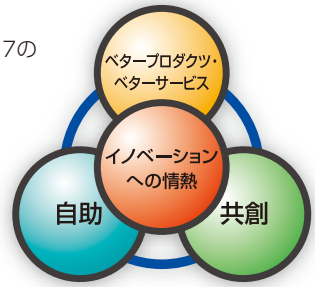
NECグループ ビジョン2017

企業理念に基づいて、NECグループが10年後に実現したい社会像・企業像をまとめました。「2017」には、C&C宣言40周年にあたる2017年に向けたビジョンという意味をこめました。

人と地球にやさしい情報社会をイノベーションで実現する
グローバルリーディングカンパニー

NECグループバリュー

企業理念とNECグループビジョン2017の実現に向けて、NECグループ社員の価値観と行動原理をまとめました。私たちが、100年を超える歴史の中で受け継ぎ、将来にわたってお客さまや社会に役立ち続けるための源泉となるものです。



価値観	重要な行動原理
[行動の原動力] **イノベーションへの情熱**	●物事の本質を追究する ●従来の常識を創造的に破壊する ●世界中の知恵を新結合する
[個人一人ひとりとして] **自 助**	●スピードを持って動く ●最後までやり抜く ●枠を超えて挑戦する
[チームの一員として] **共 創**	●個性を尊重する ●オープンに聴き学ぶ ●枠を超えて協働する
[お客さまに対して] **ベタープロダクツ・ベターサービス**	●生活者視点で考える ●お客さまの喜びを創造する ●世界のベストを追求する

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)
http://jpn.nec.com/

VEGETABLE OIL INK

Waterless Printing. Naturally.

2014年8月発行
©NEC Corporation 2014