技術と実績、エキスパートの総合力で
サイバー攻撃からICT環境を守る。

NEC Cyber Security Solutions

高度化、巧妙化するサイバー攻撃が
経営基盤を揺るがす可能性も。
その対策で、あなたの会社は生き残れますか？

サイバー攻撃の被害に遭うと、サービス停止による実被害、
風評による信用失墜、さらには事業の継続を左右する重要情報の流出など、
企業にとって計り知れない影響が生じます。
最悪の事態にならないために、組織の整備、人材の確保、投資…
総合的な経営判断も必要です。
やるべきことは見えていますか？

\Orchestrating a brighter world

NECのサイバーセキュリティ ソリューション

さまざまなものがインターネットにつながり、実空間とサイバー空間が融合していく
これからの社会において、サイバーセキュリティに取り組むことは、社会的な要求・要請です。
NECはサイバー空間に、安全・安心で快適な環境を提供することで
人と地球にやさしい情報社会の実現に貢献します。

Futureproof Security　安心の先へ。

企業価値を守る攻めの一手を!

サイバーセキュリティは社会全体の問題へ

サイバー攻撃は、時代とともに変化しています。Webサイトの改ざん、クレジットカード情報・個人情報の窃取や、インターネットバンキングでの不正送金が多発。最近では、IoTなどの新しい技術の普及で、ICTの利活用が拡大するなか、脆弱なIoT機器を踏み台にした大規模なDDoS攻撃(サービス停止攻撃)や重要インフラへの攻撃で大規模停電も発生しています。また、工場などの製造拠点やインフラが、新たなサイバー攻撃の標的となるリスクも高まり、ますますセキュリティ対策が重要になっています。

サイバー攻撃には、「情報・技術・人材」を融合したセキュリティ対策が必要

情　報

新たな攻撃手法への対応策
国際的な連携強化

攻撃手法・マルウェア対策
最新情報の共有・連携

＋

技　術

侵入を前提に対策する
多層防御

インシデント検知時の
緊急対応

＋

人　材

サイバーセキュリティ対策の
技術者育成

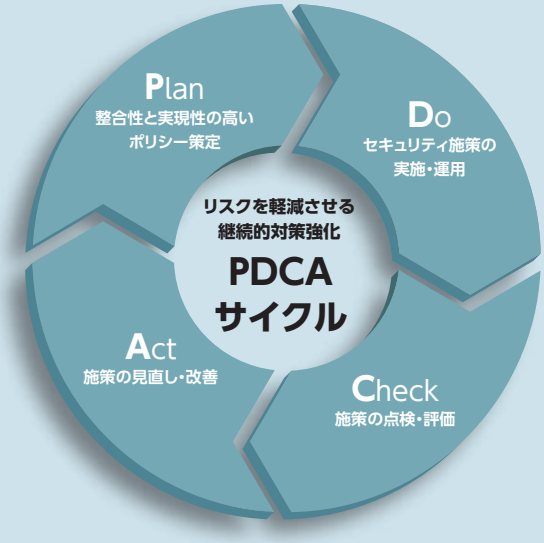
専門知識と技術を持つ
エキスパート連携

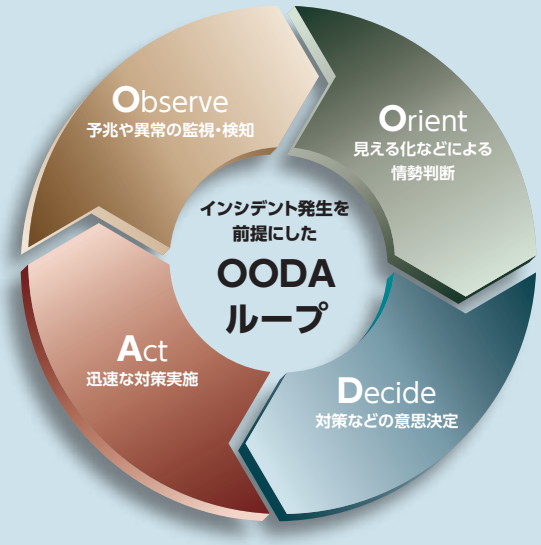
NEC Cyber Security Solutionsは、
「情報・技術・人材」の総合力を活かして
セキュアなサイバー空間を提供します。

NECは、インシデント発生を前提とした緊急対応まで、効果的で継続的なセキュリティ対策をサポートします。

サイバー攻撃からのリスクを減らす計画的な対策と、組織全体の継続的なセキュリティ強化を図ります。

サイバーセキュリティ対策は、導入すれば終わりという訳ではありません。高度化・巧妙化が進むサイバー攻撃に対抗するには、セキュリティ対策も計画的に強化し続けることが重要です。NECでは、さまざまなセキュリティ対策の効果的な連携による組織全体のセキュリティ強化とともに、ポリシー策定から対策、効果の点検、改善というPDCAサイクルにもとづき、脆弱性を解消するための継続的な対策を支援します。





インシデント発生時の適切な状況判断や迅速な対応もサポートします。

PDCAサイクルによるセキュリティリスク管理に加え、サイバー攻撃への備えとして特に重要になってくるのが、不正侵入やマルウェア感染などのインシデント発生を前提とした対策です。異常事態のすばやい検知、緊急時におけるタイムリーな意思決定や対応によって、被害の軽減が図れます。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（ウゥーダ）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支援します。

● インシデント発生時の対応例

CSIRT業務の全体像

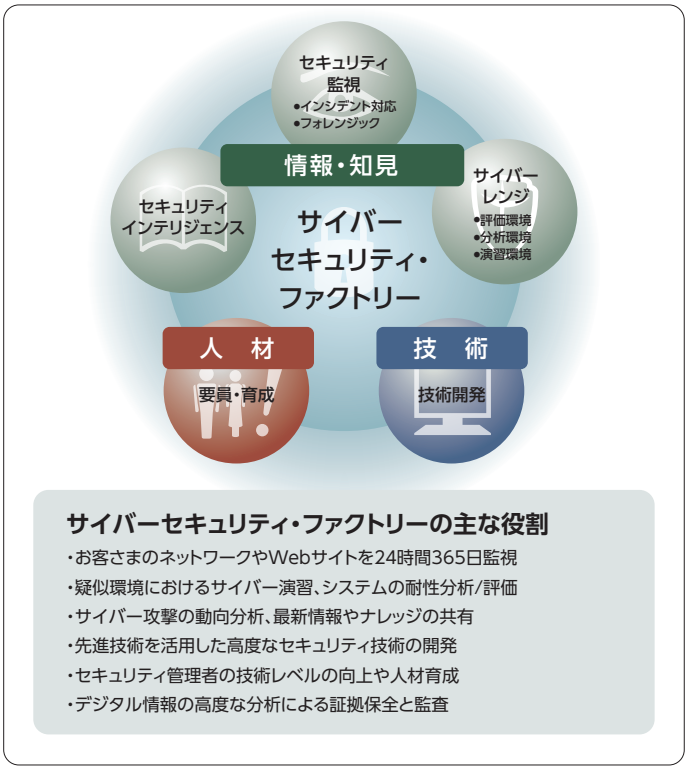
CSIRT：Computer Security Incident Response Team

インシデント対応のための組織的な取り組みを、NECはいち早く実践しています。

企業の間では、重要な情報資産を脅かすインシデント（事故）の発生を前提とした対応体制である「CSIRT（インシデントレスポンスチーム）」へ注目が高まっています。2000年に、「CSIRT」を立ち上げて活動を開始したNECでは、グローバルな外部機関連携やナレッジ共有、技術や経験の蓄積、検知や警戒、さらに被害の軽減など、「CSIRT」の組織的な取り組みを早くから実践。高度化・巧妙化するサイバー攻撃に対抗するため、検知したマルウェアを解析するなど、先進的な取り組みを推進しています。

NEC社内外のセキュリティインテリジェンスを集約。サイバーセキュリティ対策をワンストップで行う「サイバーセキュリティ・ファクトリー」を運用しています。

実際にインシデントが発生した際、対応には情報・技術・人材のすべての要素が必要です。そのためNECでは、サイバーセキュリティ対策の中核拠点として、「サイバーセキュリティ・ファクトリー」を2014年に本格稼働しました。
NECグループや外部の提携パートナー企業が連携したこの専門組織には、サイバーセキュリティに精通した専門家が集結しています。高度な技術、最新の攻撃手法やマルウェアの動向、その対策ノウハウを蓄積・共有しながら、セキュリティシステムの導入から構築、24時間365日の運用監視、インシデント発生時の緊急対応など、ワンストップでサポート。日本だけでなく、シンガポールや欧州、北米にも拠点を開設し、グローバルな監視体制を強化。また、専門家の監視業務を高度化・効率化するために、AIを活用した「脅威分析システム」を開発し、2017年に本格導入しました。



サイバーセキュリティ・ファクトリーの主な役割

- お客さまのネットワークやWebサイトを24時間365日監視
- 疑似環境におけるサイバー演習、システムの耐性分析/評価
- サイバー攻撃の動向分析、最新情報やナレッジの共有
- 先進技術を活用した高度なセキュリティ技術の開発
- セキュリティ管理者の技術レベルの向上や人材育成
- デジタル情報の高度な分析による証拠保全と監査

NECグループ

● 株式会社サイバーディフェンス研究所

CyberDefense

世界トップクラスの技術力を持つエンジニアによるペネトレーションテスト（人の手による脆弱性診断）、フォレンジック（不正行為の証拠分析）などの分野を中心に、高品質なセキュリティ技術サービスを提供します。

● 株式会社インフォセック

Infosec

官公庁や企業の情報セキュリティ管理やコンサルティング、システム設計、24時間365日のセキュリティ監視サービスにいたるまで、サイバーセキュリティに関わるサービスを広く提供します。

提携パートナー企業

- 株式会社ラック
- 株式会社FFRI
- トレンドマイクロ株式会社
- S&J株式会社
- エヌ・アール・アイ・セキュアテクノロジーズ株式会社

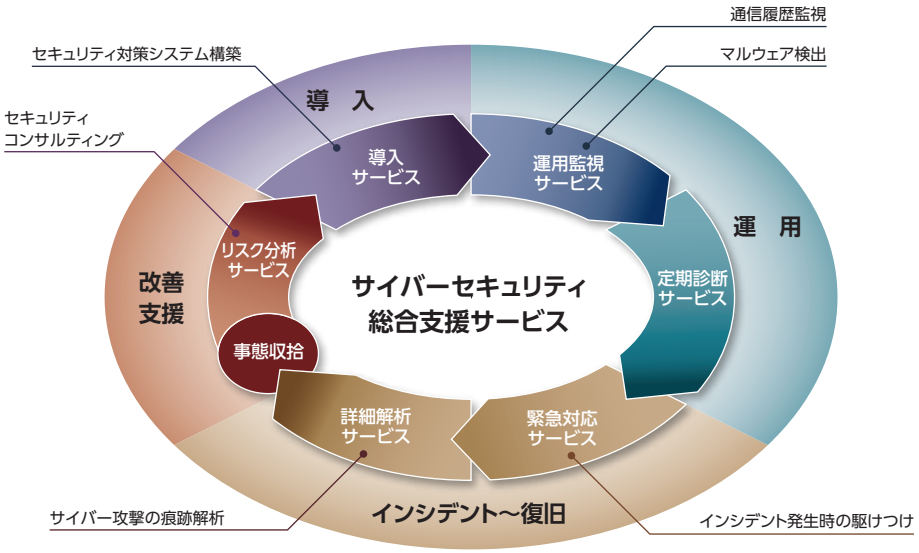
（順不同）

ワンストップな総合支援サービスで、強固なセキュリティライフサイクルを推進します。

NECのSOC（セキュリティオペレーションセンター）では、世界トップクラスのサイバーセキュリティスペシャリストによる先進の「セキュリティ運用監視ソリューション」や「フォレンジック（不正行為の証拠分析）」を提供しています。また、インシデントが発生した際には、多くの実績と経験を持つ専門家が緊急対応（駆けつけサービス）を行う「インシデント対応ソリューション」を提供します。
また、お客さまのSOC（プライベートSOC）とNECのSOCを、連携させることもできます。この連携により、「お客さまのナレッジの蓄積」と「高度専門ナレッジの活用」が両立でき、より高度な監視と、お客さまの要員の強化を実現します。

● NECが提供するサイバーセキュリティ総合支援サービス

NECサイバーセキュリティ・ファクトリーを主軸とするワンストップな総合支援



NECは、セキュアなサイバー空間の提供のため、社会と連携して「情報・技術・人材」を強化しています。

サイバー犯罪対策の専門組織と連携して最新情報を共有し、国際レベルでのセキュリティ強化に取り組んでいます。

NECは、インターポールと提携。サイバー犯罪に対する国際的なセキュリティ強化を支援しています。

サイバー犯罪に対する国際レベルでのセキュリティ強化を目指し、NECは、2012年、インターポール（国際刑事警察機構）とサイバーセキュリティ対策でパートナーシップ協定を締結しました。また2015年には、インターポールがシンガポールに開設し、本稼働を開始した「The INTERPOL Global Complex for Innovation（IGCI）」に、デジタル犯罪捜査のための中核システムや製品、技術支援要員を提供しました。IGCIは、デジタルセキュリティの領域での研究・開発、サイバー犯罪や犯罪者の調査・分析など、各国当局に重要な支援を行っています。

オペレーションセンター（Cyber Fusion Centre）

AISに加入し、サイバーインテリジェンスを強化しています。

NECは、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「Automated Indicator Sharing（AIS）」に日本の企業で初めて加入しました。AISは、DHS傘下の国家サイバーセキュリティ通信総合センター（NCCIC）が提供する情報システムを介して、米国連邦政府と米国内外の民間企業・団体などとの間で、サイバー攻撃の脅威情報（IPアドレス、ドメイン名、フィッシングメールの送信者アドレスなど）の迅速な共有を可能とします。これにより、最新のサイバー攻撃による脅威を迅速に把握し、特定の脅威による被害拡大の防止を実現します。

日本サイバー犯罪対策センター（JC3*）へ参画。産学官の連携に取り組んでいます。

NECは、サイバー空間の脅威に対処するための非営利団体「一般財団法人日本サイバー犯罪対策センター（略称：JC3：Japan Cybercrime Control Center）」に正会員として参画しています。

JC3は、産業界、学術研究機関、法執行機関が持つ対処経験などの蓄積・共有、警察による捜査権限のより効果的な行使など、脅威への先制的・包括的な対応を実現する産学官の新たな連携の枠組みです。

JC3は、国内および海外の関係機関との情報共有と協力関係を構築し、脅威の大本を特定して被害を軽減、無効化することを目指しています。

＊JC3創設にあたってはNEC シニアオフィサーの清水隆明が代表理事に就任しています。

IoT時代を見据え、セキュリティを考慮した開発・運用を推進しています。

NECは、ICTの総合ベンダーとして、さまざまなハードウェアやソフトウェア製品を開発してきました。さらにその実績やノウハウを活かしたシステム構築やネットワーク構築、運用サポートで、幅広い業種に向け多彩な業務ソリューションを提供しています。お客さまの業務形態を理解し、長年ICT環境の構築をしてきたNECだからこそセキュリティリスクを軽減できます。開発・運用の各フェーズにおいては社会インフラを含むシステム・製品・サービスを対象とし、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開発・運用実施基準を制定。セキュリティ国際標準、政府機関が定める基準、業界ガイドラインなどの要件を考慮し、日々発生する新たなサイバー攻撃への対策を随時反映しながら、セキュリティ品質を確保しています。

これからのIoT時代には、これまでも推進してきた、設計時からセキュリティ対策を組み込む「セキュリティ・バイ・デザイン」の考えのもと、安全・安心なICT環境を提供していきます。

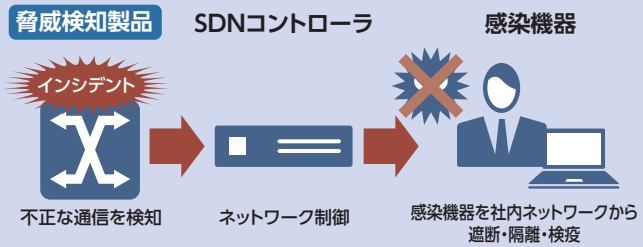
品川区の標的型攻撃対策の実証実験を実施し、社会インフラの強化に取り組んでいます。

NECでは、早くから着目してきたSDN（Software-Defined Networking）を積極的に活用。マルウェア感染やWebサイト改ざんなどの異常を検知すると、SDNのネットワーク制御機能により、問題のあるクライアントPCやサーバの通信を遮断したり、検疫ネットワークへ隔離したりする初動対応を自動で施します。

品川区には、共同で行った実証実験を経て、SDNを活用した新たなセキュリティ機能を構築、2016年から稼働しています。

SDNの活用によるサイバー攻撃自動防御ソリューションなどにより、社会インフラのセキュリティ対策の強化を目指します。

● サイバー攻撃自動制御ソリューション



NECは、高いスキルを持つ実践的なセキュリティプロフェッショナルを育成しています。

サイバー攻撃が日々巧妙化する中、製品・システム・サービスのセキュリティ対応力を高め、さまざまな領域においてお客さまに貢献するため、セキュリティ人材の育成に力を入れています。
NECグループとして必要なセキュリティ人材を定義し、人材タイプごとの育成を実施。お客さまに必要なセキュリティ人材定義とも連動し、さらなるブラッシュアップを継続しています。さらに、サイバーディフェンス研究所などのNECグループおよび、パートナー企業と連携して、人材タイプの定義ごとに研修を用意し、お客さまに提供していきます。

独自の認定制度を設け、公的資格取得を推奨しています。

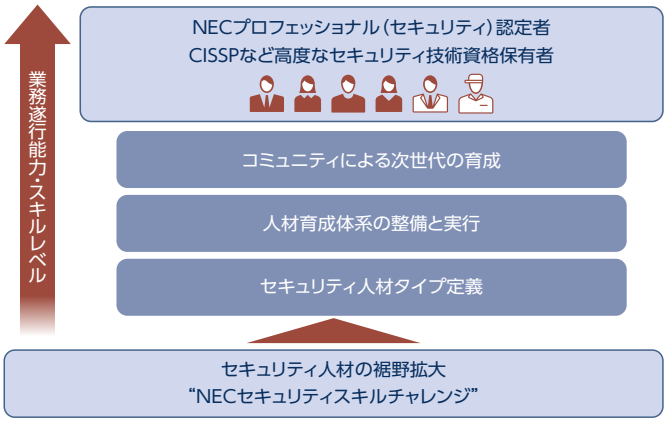
NECプロフェッショナル認定制度を設け、高度なセキュリティ専門性を有する人材を認定しています。また、セキュリティ公的資格の取得を強く推奨しており、国際資格であるCISSP*や「情報処理安全確保支援士」の取得者を拡充。セキュリティに関する高度なスキル、業務経験、資格を有している者が核となり、お客さまに適したソリューションの提供に貢献します。

*CISSP Certified Information Systems Security Professional

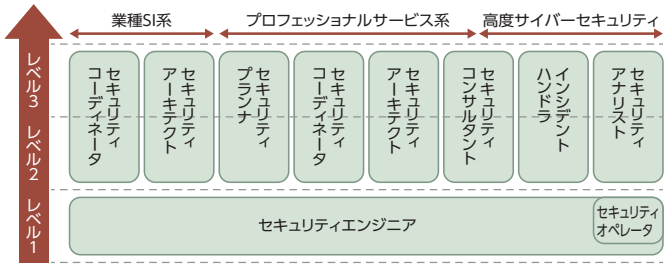
コミュニティによる次世代の育成と全社的CTFを実施しています。

NECグループでは既に300人以上からなる、セキュリティのコミュニティが形成されており、インテリジェンスの共有や技術の検討などの勉強会を定期開催するなどし、次世代のプロフェッショナルを育成しています。NECグループの全社員を対象に、社内CTF（Capture the Flag）である「NECセキュリティスキルチャレンジ」を開催しており、2016年度は約1000名が競技に参加し、セキュリティ人材の裾野拡大につなげています。

● プロフェッショナル人材育成



● セキュリティ人材タイプ



セキュリティ人材の基礎基盤を強化するために、政府や自治体、学術機関と共同で人材育成や演習を行っています。

シンガポール政府とサイバーセキュリティ専門家の育成に共同で取り組んでいます。

NECはシンガポール政府・経済開発庁と戦略的出向・研修（STRAT）プログラムの研修生受け入れ契約を締結しました。本活動を通じてシンガポールおよび周辺国のサイバーセキュリティ対応力向上に貢献できるよう、実践的なスキルを有する人材の育成や共同研究を行っています。

総務省のプロジェクト「サイバー攻撃に対する実践的な防御演習」に協力しています。

2013年から総務省が進めている「サイバー攻撃解析・防御モデル実戦演習の実証実験」プロジェクトに協力。官公庁や重要インフラ事業のシステム管理者に向けて、大規模な疑似ICT環境で標的型攻撃を防御する「実践的サイバー防御演習（CYDER）」を行っています。
2016年からは全国11地域の地方公共団体を対象にしたCYDERにも協力し、情報システム管理者のインシデントハンドリング能力の向上を支援しています。

北陸先端科学技術大学院大学に寄附講座を開設。将来の技術者の育成にも尽力しています。

北陸先端科学技術大学院大学と連携し、2015年からサイバーセキュリティに関する最先端の研究活動と人材育成を目的とした寄附講座「サイバーレンジ構成学」を開設しています。サイバーレンジ（サイバー空間の演習場）の構築技術を研究開発し、これを用いた教育プログラムを設計・開発。開発した教育プログラムは、他の大学や高等専門学校などの教育機関に提供しています。

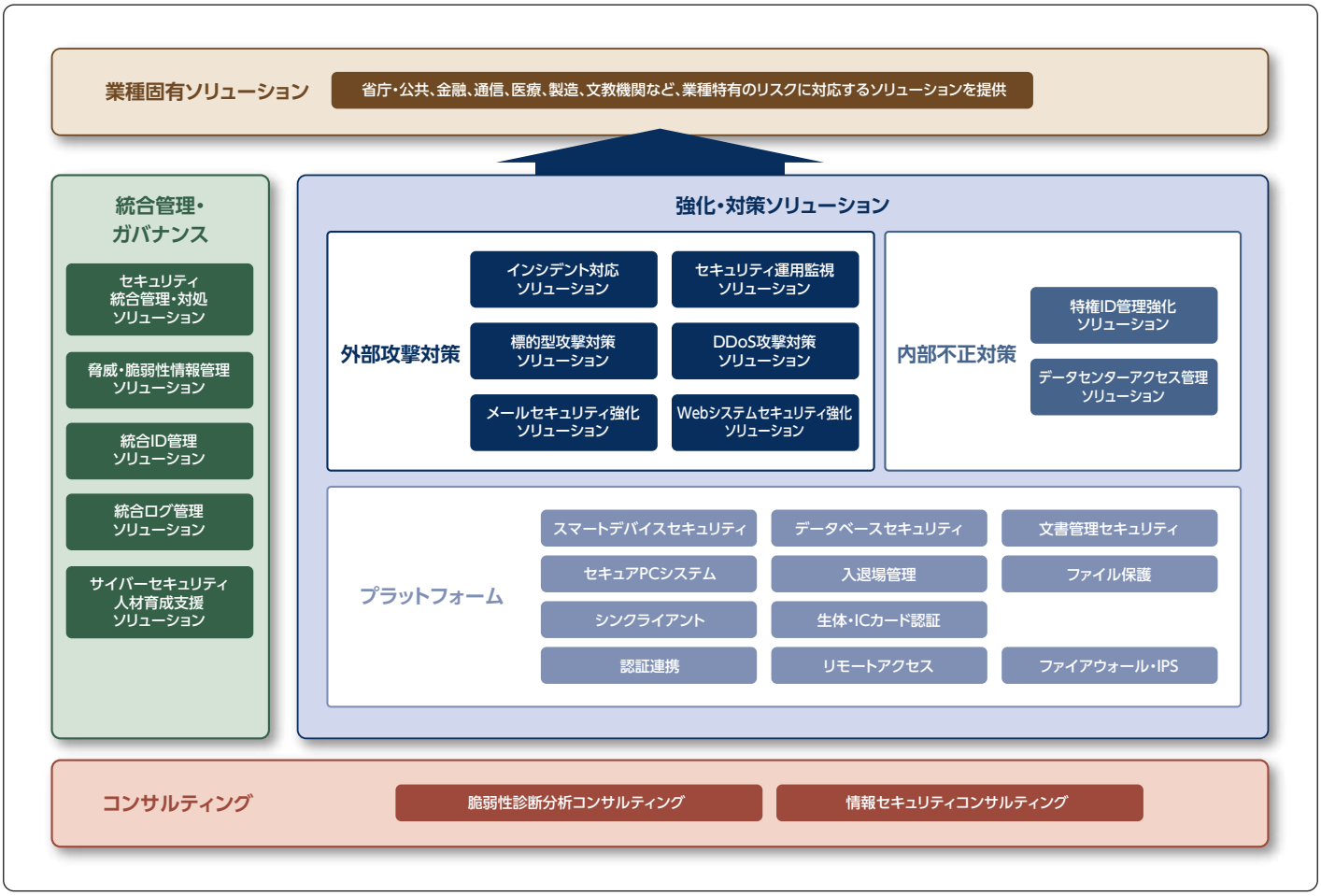
ASEAN諸国のセキュリティ人材育成に貢献しています。

NECは、ASEAN地域における6か国（カンボジア、インドネシア、ラオス、ミャンマー、フィリピン、ベトナム）のサイバーセキュリティ主管官庁などの職員を対象とした研修を実施しています。本研修は、ASEAN諸国の標的型攻撃に対するインシデントレスポンス能力の向上を目的としており、最新の脅威情報・セキュリティ対策などの講義や、「実践的サイバー防御演習（CYDER）」と同様の演習などを行うことで、サイバー攻撃に的確に対応できるセキュリティ人材の養成を目指すものです。さらに、タイやマレーシアの政府関連機関の職員を対象としたCYDERを実施し、各国の人材育成に貢献しています。

NECは、サイバーセキュリティのコンサルティング、対策、運用、インシデント対応まで、トータルにソリューションを提供します。

日々高度化・巧妙化するサイバー攻撃に対し、システムの強化や新たな技術開発に取り組み、その実績や知見を標準的なソリューションにして提供しています。組織とシステムを俯瞰したセキュリティ対策強化を実現します。

脆弱性診断によるリスクの見える化や改善提案、お客さまに適したセキュリティポリシー策定をサポートする「コンサルティング」をはじめ、策定したセキュリティポリシーを実現する基盤となる「プラットフォーム」、標的型攻撃やWebシステムへのDDoS攻撃など、サイバー攻撃の対策システムとその運用監視やインシデント対応まで幅広くサポートする「外部攻撃対策」、内部の人為的な不正や偶然・ミスによる情報漏えいを防ぐ「内部不正対策」、全社的な統制とセキュリティレベルの維持・向上を図る「統合管理・ガバナンス」の5つの領域から、組織とシステム全体を俯瞰したトータルソリューションを提供します。さらにNECでは、これらのソリューションに加え、さまざまな業種に特有なリスクを軽減する「業種固有ソリューション」においてもコンサルティングから運用まで、豊富な提供実績と構築ノウハウをもとに、お客さまへ確かな安心をお届けします。



「コンサルティング」：多角的な診断によって解決策を提案します。

多角的な分析で、業務改善・組織づくりまで支援します。

お客さまのICT環境全体をさまざまな角度から分析し、セキュリティ対策の実施状況を確認、業務改善や運用を含めたソリューションの提案を行います。
また、NECグループにおける長年の「CSIRT」の運用実績と経験を活かし、インシデント発生を前提とした緊急対応や統制のとれた組織づくりを支援します。

サイバーセキュリティ経営観点のコンサルティングサービス

NECは、サイバーセキュリティ経営の観点から企業の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。NEC自身の実践経験を活かし、サプライチェーンのビジネスパートナーを含めたセキュリティ対策や、IoT時代を見据えたセキュアなものづくりを支援します。また、NEC自身の「サイバーセキュリティ経営ガイドライン」への対応実績を基に、ICT環境のみならず制御系システムを開発・運用する企業も対象にリスクを見える化し、その対策を提案する「リスクアセスメントサービス」を提供します。

「統合管理・ガバナンス」:ICT環境を経営的な視点から組織的に管理します。

ガバナンスが求められる領域は、クラウド上のシステムやスマートデバイスまで広がっています。

クラウド、スマートデバイスの普及といったICTの発達により、企業におけるセキュリティ管理の範囲は広がっています。ネットワークの社内外の境界が曖昧となったことで、境界をまたいだアクセスコントロールなど、レベルの高い統制が求められています。このような複雑な状況において、これまで以上にクライアントPCやサーバの脆弱性把握と迅速な対応が重要です。

NECの「数えるマネジメント」は、リスクの見える化に有効です。

人、ID、クライアントPC、サーバ、ログにいたるまで、数値で見える化を行うことで、どこにどんな脆弱性があるのかを把握できます。また、その数値を読み解くことで、企業が直面するリスクの程度や必要な対策の優先度を迅速に判断することが容易になります。

NECは脆弱性、標的型攻撃、内部情報漏えいなどの増え続ける脅威に対し、これまで自社グループやさまざまなパートナーとの連携から得たノウハウを「プロアクティブ(先読み対策)サイバーセキュリティソリューション」として提供します。

ウイルス、マルウェアからPCを守るために 「数えるマネジメント」

セキュリティ対策レベルにバラツキがあると、そこがサイバー攻撃に対する弱点となります。NECでは、従来からセキュリティ環境を見える化する「数えるマネジメント」を実践。社内ネットワークに接続される機器を正確に把握し、すべてのクライアントPCにセキュリティ対策ソフトウェアを確実にインストールさせています。

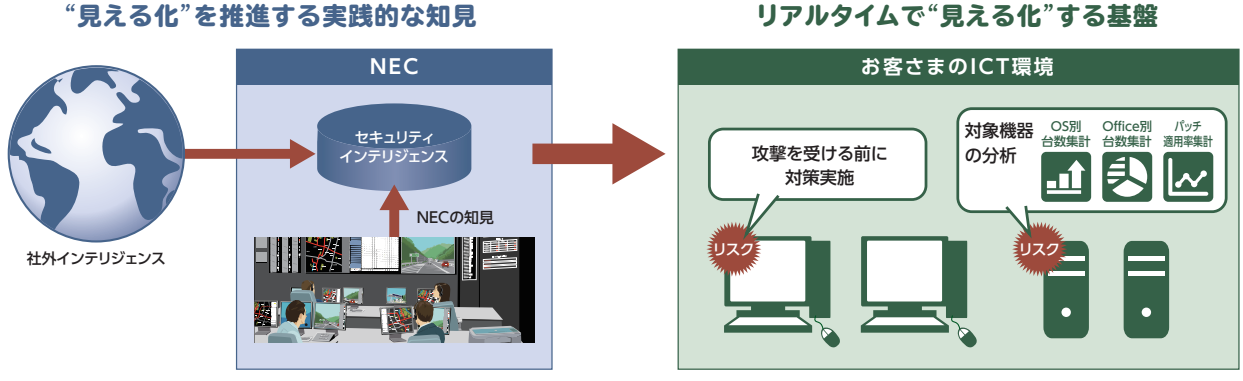
また、パッチの未適用などセキュリティ対策が不十分なクライアントPCが社内ネットワークに接続されたり、クライアントPCにマルウェアが検知されたりした場合に、該当するクライアントPCを社内ネットワークから隔離・遮断する検疫ネットワークを開発するなど、着実な取り組みが、安心へとつながっています。

自社で積み重ねてきた「数えるマネジメント」のノウハウをもとに「先を読み、対策する(プロアクティブ)」新しいサイバーセキュリティ対策を提供します。

突如としてソフトウェアに脆弱性が公表され、昨日まで大丈夫だと思っていたICT環境に、緊急の対応が求められるケースはますます増加しています。最新の脅威・脆弱性情報を常に入手し、いかにICT環境に潜むリスクをコントロールするかが、対策の大きなポイントとなっています。

NECでは自ら実践している「数えるマネジメント」の実績を積み重ね、日々報告される脆弱性や、不正アプリケーションなどに対し、NECグループ内にある18万台のクライアントPCとサーバの中から対策が必要な機器を1時間で見える化し、早急に対処できる基盤を導入しています。また、世界中から集めた最新の脅威・脆弱性情報を、NECのサイバーセキュリティ専門家が知見で分析し「セキュリティインテリジェンス」に蓄積しています。この「セキュリティインテリジェンス」と、リアルタイムで見える化し対処する基盤をもとに、サイバー攻撃を受ける前に先読みし、効率的に対策を実施できる「プロアクティブサイバーセキュリティソリューション」として「NEC Cyber Security Platform」を提供します。

NEC18万台の運用実績を持つ基盤と知見で
リスクが管理されたICT環境を実現



「プラットフォーム」：利便性を維持できるセキュリティ基盤を利用することが大切です。

情報資産保護のため、適切に機能する基盤を提供します。

事業を支えるICT環境には、情報資産を守るための文書管理システム、フィジカルセキュリティ、持ち込みPCの検疫システムなど、バランスのとれたセキュリティ基盤が必要不可欠です。

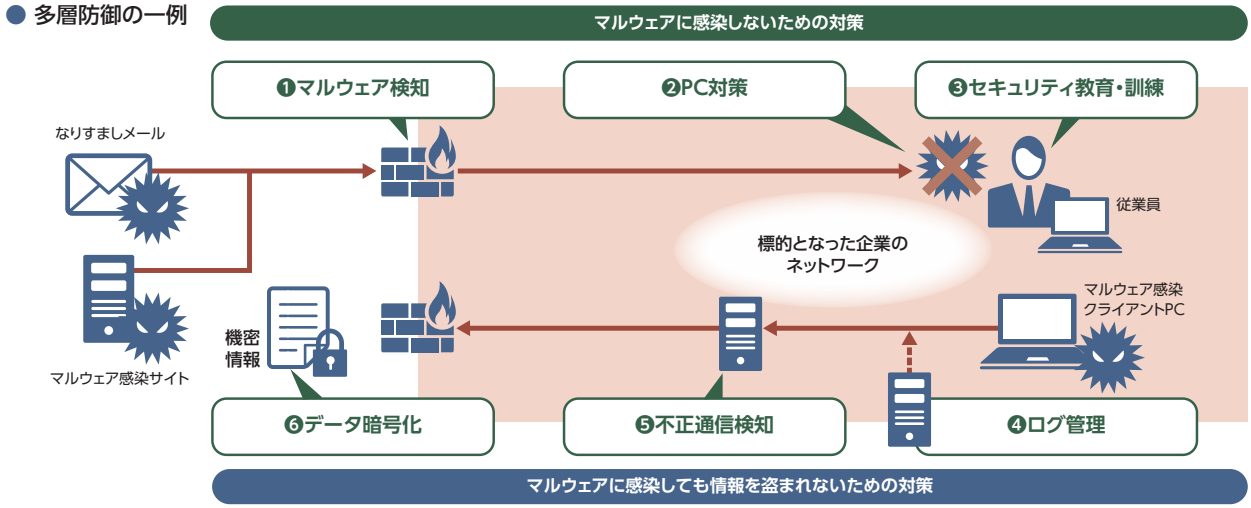
NECグループにおける運用ノウハウをもとに、利用者の利便性維持という視点を大切にしつつ、外部攻撃、内部不正に対応しながら、企業の機密情報や顧客情報を守るためのセキュリティ基盤を提供します。

「外部攻撃対策」：侵入を前提とし、複数の対策を組み合わせて被害を軽減することが重要です。

対策技術と人的な対策を多層的に組み合わせることで、標的型攻撃から情報資産を守ります。

標的型攻撃では、従来のウイルス対策ソフトウェアでは検知・駆除できない未知のマルウェアがよく用いられています。企業内のクライアントPCが未知のマルウェアに感染した場合、ただちに感染したクライアントPCを特定し、対処を行うことが必要です。こうした未知のマルウェアによる情報の窃取を防ぐため技術的な対策として有効なのが、「多層防御」です。NECでは、マルウェアの活動を迅速に検知する仕組みづくりなどの技術的な対策と、ユーザ教育や監視サービスなどの人的サービスを組み合わせ、「多層防御」を提供します。

● 多層防御の一例



企業の顔である公開Webシステムを守ります。

次々に見つかる脆弱性を突いてWebサイトが改ざんされ、アクセスしたユーザを不正なサイトへ誘導したり、クライアントPCをマルウェアに感染させたりするケースが多発しています。NECでは、Webシステム/アプリケーションの状態を見える化し、新たな脆弱性に対して優先度をつけた対策を提案します。

金銭目的のランサムウェアの被害を防ぎます。

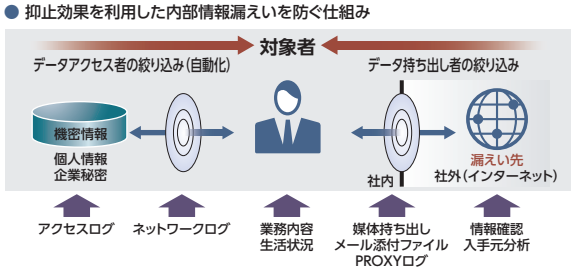
ランサムウェアは、データを暗号化したり、クライアントPCやサーバ自体を使用不能にしたりし、それらを使用可能な状態に戻すことと引き換えに「身代金」を要求するマルウェアです。感染リスクを軽減するためには、多層防御の考え方のもと、脆弱性対策が有効です。また、万が一、感染しても復元できる環境を整えることも重要です。

「内部不正対策」：最新ICT活用による業務効率向上と引き換えに現れるリスクへの対応が必要です。

セキュリティポリシーの策定、教育、リスク分析を含めた、トータルな対策の継続的なアップデートが必要不可欠です。

メール、CD-R、USBメモリ、クラウドストレージ、スマートフォン、これらは業務を効率的に行う上では欠かせないものになっています。その一方で、こういったICTの発達とともに、内部の人為的な不正やミスによる、情報漏えいの経路も増えていきます。新しいデバイスやサービスを利用する上でのリスクを分析し、セキュリティポリシーの更新や社員教育などの対策を強化し続けることが必要です。また、アクセス制限、シンクライアント化、外部記憶媒体・デバイスの制御、データの暗号化などの対策と併せて、操作監視やログ解析装置の導入は抑止効果の点からも効果的です。

● 抑止効果を利用した内部情報漏えいを防ぐ仕組み

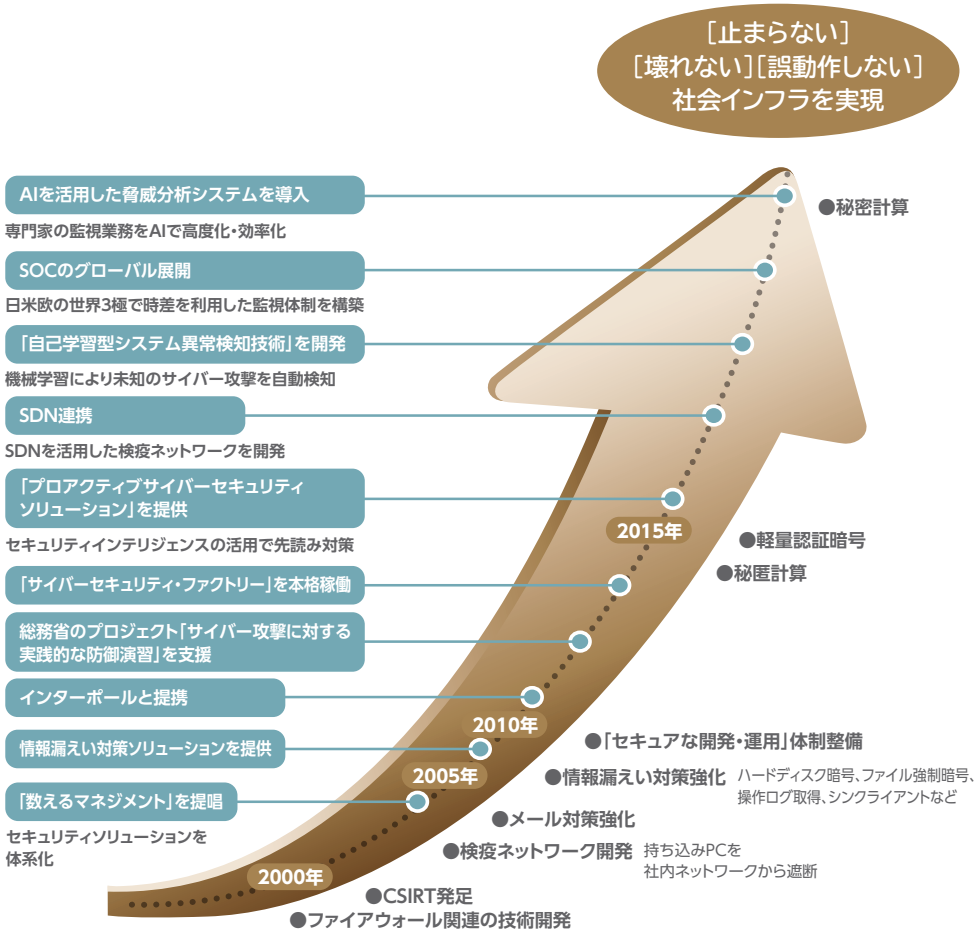


Futureproof Security 安心の先へ。——
NECの新たな取り組みに、ご期待ください。

多くのお客さまのシステムを構築してきた経験・実績と、「情報・技術・人材」を掛け合わせた先進のサイバーセキュリティ対応力で社会インフラの安心を支えます。

NECグループにある18万台のクライアントPCとサーバを結んだネットワークシステム。この大規模なICT環境を安全に維持するために、NECでは自ら開発したセキュリティ技術やソリューションを融合・活用しています。そこで実証した技術とノウハウをもとに、企業や社会インフラを守るソリューションを開発・提供しています。

NECはこれまでも、不正に持ち込んだクライアントPCを検知して隔離する「検疫ネットワークシステム」を国内で初めて製品化したほか、セキュリティの脅威や脆弱性を定量化して見える化する「数えるマネジメント」をいち早く提唱して実践。現在はSDNやAIを活用した最先端の技術開発を行い、サイバーセキュリティソリューションの革新や新たな価値創造を実現するリーディングカンパニーとして、お客さまに安心と安全を提供します。



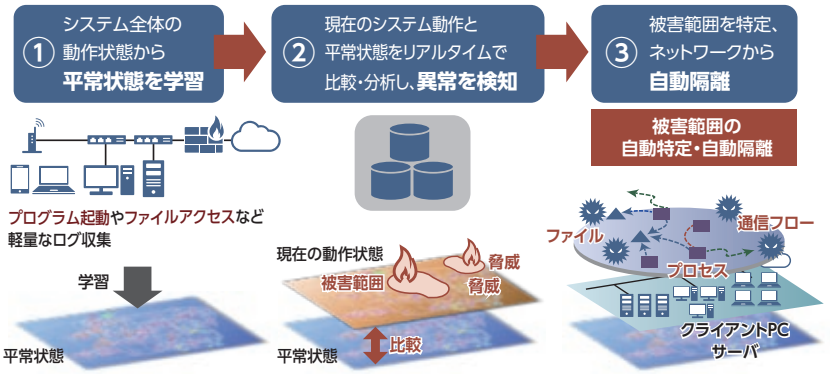
AIを活用し未知のサイバー攻撃を自動で検知・隔離する技術を研究開発しています。

NECでは、今後に向けた新たな取り組みも進めています。AIを活用し、未知のサイバー攻撃を自動検知する「自己学習型システム異常検知技術」を開発しました。これにより、従来の人手による作業に比べ、1/10以下の時間で被害範囲の特定ができるようになります。

クライアントPCやサーバなどシステム全体の複雑な動作状態（プログラムの起動、ファイルへのアクセス、通信など）から平常状態を学習し、平常状態と現在のシステムの動きをリアルタイムに比較・分析することで、平常状態から外れた場合に検知します。

また、システム管理ツールやSDNなどを活用することで、該当箇所のみをネットワークから自動で隔離することもできます。

● 自己学習型システム異常検知技術



◎未知のサイバー攻撃もリアルタイムに自動検知
◎従来の人手による分析の1/10以下の時間で被害範囲を特定

Futureproof Security
安心の先へ。

お問い合わせは、下記へ

NEC サイバーセキュリティ戦略本部
〒108-8001 東京都港区芝五丁目7-1 (NEC本社ビル)
URL：http://jpn.nec.com/cybersecurity/
E-mail: info@cybersecurity.jp.nec.com

日本電気株式会社　〒108-8001　東京都港区芝五丁目7-1 (NEC本社ビル)

2017年10月現在

Cat.No. D03-17100285J