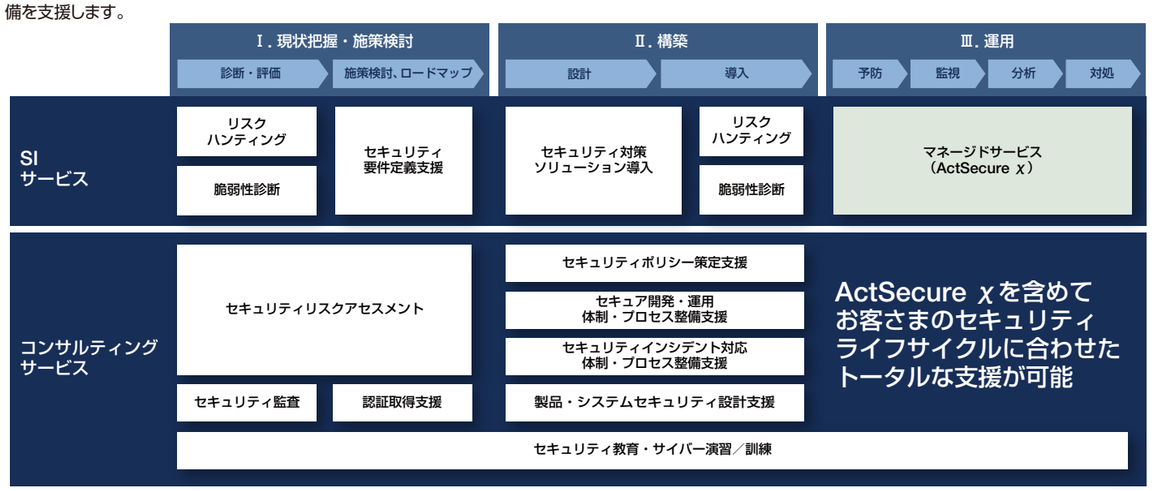
サービスメニュー　SIとコンサルティングを通じ、安全・安心な事業運営の環境を整備

セキュリティ プロフェッショナルサービスでは、多角的なリスク分析、セキュリティのポリシーや各種ルール・ガイドラインの策定、セキュリティ監査や脆弱性診断、各種認証取得支援、CSIRT体制構築支援など、経営観点で必要となる対策のコンサルティングとSecurity By Designの考え方にもとづくセキュアシステム構築のSIサービスを提供します。さらに、運用フェーズにおける予防・監視・分析・対処を支援するマネージドサービス（ActSecure χ）を含めて、お客さまのセキュリティライフサイクルに合わせたトータルな支援が可能です。

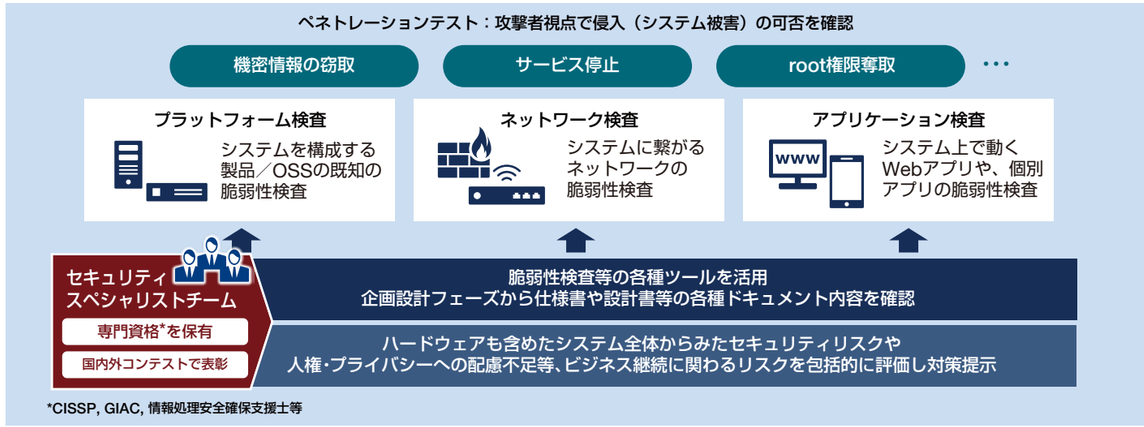
高度なセキュリティ人材の確保が経営課題となっている今、NECのセキュリティスペシャリストチームは、お客さまが事業運営に集中できる、安全・安心な環境整備を支援します。



PSIRT: Products Security Incident Response Team, 製造業における製品に関するセキュリティインシデント発生時の対応組織

リスクハンティング　ビジネスへの影響を考慮しながら包括的にリスクを評価、対策案を提示

リスクハンティングサービスは、ビジネス面を考慮しながら、セキュリティスペシャリストチームが脆弱性診断やペネトレーションテスト（侵入テスト）などで、ハードウェア、ソフトウェア、ネットワークなどシステム全体のリスク評価を行います。また、人権・プライバシーへの配慮、市場トレンドから将来的に考慮すべき懸念事項など、情報資産をビジネスに利活用する上で想定されるリスクについても、ビジネスプラン、仕様書やシステム設計図などを参照して評価し ます。これらのリスクに対してビジネスへの影響を考慮した対策を提示することで、ビジネスの企画やシステム設計段階からリスク低減を支援します。



*CISSP, GIAC, 情報処理安全確保支援士等

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）
https://jpn.nec.com/cybersecurity/

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）

2021年2月現在

Cat.No. D03-21020315J

\Orchestrating a brighter world　NEC

トップクラスのセキュリティスペシャリストチームが
New Normal時代の新たなリスクからビジネスをまもる

セキュリティ プロフェッショナルサービス

トップクラスのセキュリティスペシャリストチームが New Normal時代の新たなリスクからビジネスをまもり お客さまの安全なDX推進をサポート

New Normal時代に向けて、働き方や産業構造の変化へ対応するために、企業のデジタルトランスフォーメーション(DX)が、急速に進んでいます。一方で、セキュリティ問題がビジネスリスク、ひいては一般社会からのレピュテーションリスクにまでつながることから、セキュリティ対策は事業継続のための経営課題となっています。

NECでは、セキュリティスペシャリストチームによるコンサルティングとシステム構築(SI)を軸に「セキュリティ プロフェッショナルサービス」を提供。お客さまが安全・安心にDXを進めるために必要なセキュリティ対策を用意し、ビジネス継続を支援します。

これからのセキュリティ対策の在り方

ゼロトラスト+サイバーハイジーンの考え方がDXセキュリティのベースに

DXによりテレワークの導入やクラウドサービス利用が進むことで、守るべき情報資産を社内に置いてネットワークの境界で防御する従来の考え方では、安全性の担保が困難になっています。DXを安全に推進するためには、情報資産と脅威が社内外に存在することを前提に、アクセスするものはすべて信頼せずに都度、認証・認可を行うゼロトラストモデルを採用し、脆弱性を常に排除するサイバーハイジーン(衛生管理)の徹底が急務となっています。

NECでは、システムやサービスの企画設計段階からゼロトラストの考え方で「正しくつくる」、そして、正常な状態を維持し続けるために、サイバーハイジーンの考え方で「手洗い・うがい」のように日頃から基本的な脆弱性対策を徹底することが、企業のレジリエンス(回復力)強化につながると考えています。「正常をつづけやすく」「攻撃からまもりやすく」つくることで、社会の変化により発生する新たなリスクから事業活動をまもることができます。

ゼロトラスト

脅威はあらゆる場所に

トラストの積上げ

＋

サイバーハイジーン

全てのITの衛生管理を徹底

日常の運用で予防

Security By Design

プロセス、ワークフローのアーキテクチャレベルから
ビジネスの影響度を考慮したセキュリティを組込み

- **正しくつくる**
  「正常をつづけやすく」「攻撃からまもりやすく」企画・設計し、つくる
- **正常をつづける**
  常に状態をチェックし、問題に対処しつづける
- **攻撃からまもる**
  異常を検知し、原因究明・復旧をする

必要な対策 ビジネスリスクの見える化、安全性を継続するための対策が必要

このようなサイバーセキュリティの変化に対応するためには、抑止・予防・検知・復旧の各段階において、ゼロトラストを実現するためのセキュリティ実装が必要です。また、サイバーハイジーンの徹底のためには、導入時から安全性を継続するための対策を実装しておくことが不可欠です。

さらに、データやシステムが複雑に連携することで新たな価値を生み出すDXの環境下では、ビジネス全体のフローとして見たときに問題がないか、人権/プライバシー保護やアクセシビリティへの配慮がされているかなど、ビジネス面でのリスクを考慮することも重要となります。

NECは、お客さまの業務を理解し数多くの安全・安心なICT環境を構築運用してきた実践経験と専門技術を活かした「セキュリティ プロフェッショナルサービス」を提供。ビジネスリスクの見える化からお客さまの事業に即した対策まで、安全なDX推進を支援します。

	導入時に必要な対策		安全性を継続するために必要な対策	
抑止	ガバナンス強化	• リスクアセスメント • ポリシー策定支援	ガバナンス強化	• 体制・仕組み構築支援 • 教育・講習／講演
予防	ガバナンス強化	• 脆弱性分析コンサルティング		
	リスクハンティング			
	統合ID管理	アクセス制御	脆弱性対策・パッチ管理	
	不正接続防止	検疫	データ保護	
	ネットワークセキュリティ対策	クラウドセキュリティ対策		
検知	ウイルス対策	不正侵入検知（IPS）	セキュリティ監視	
	EDR	WAF	メールセキュリティ	
	SIEM		DDoS対策	
復旧			初動対応	

マネージドサービス　プロフェッショナルサービス　赤文字：コンサルティング　青文字：SIサービス

NECの強み Security By Designの知見と先見性を持った「セキュリティスペシャリストチーム」

本サービスの提供で重要な役割を担うのが、Security By Designの知見と市場トレンドから将来的なビジネスリスクまでを見通す先見性を持った「セキュリティスペシャリストチーム」です。CISSPやGIAC、RISSなどの高度な専門資格を保有し、セキュリティ技術を競う国内外のコンテストで、上位入賞を果たしたトップクラスの専門人材で構成されています。

さらに、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」や日本サイバー犯罪対策センター(JC3)などに参画し、積極的に外部インテリジェンスを活用するとともに、これらの活動を通して安全・安心な社会の実現にも貢献しています。

高度な専門人材

- 高度な国際・国家資格保有
- コンテスト入賞
- 世界トップクラスの技術力

社内外のインテリジェンス

- 外部団体への参画、パートナー連携
- 長年のセキュア開発運用での知見

CISSP:Certified Information Systems Security Professional
GIAC:Global Information Assurance Certification
RISS:Registered Information Security Specialist（情報処理安全確保支援士）