DX時代のトータルサイバーセキュリティ

吉府 研治　鈴木 章工　岡崎 巧　西野 真一郎　小川 賢一　薄羽 利光

要 旨

企業や組織はデジタルトランスフォーメーション（DX）の取り組みを推進する一方で、サイバー攻撃の影響をますます受けやすくなり、サイバーセキュリティはこれまで以上に大きな経営課題となっています。この状況に対応するために、NECは、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・デザインに基づき、DXに求められるセキュリティを実現するためのさまざまなサービスやDXオファリングを提供。企業や組織のDXを支え、安全・安心な社会の実現に貢献します。

KeyWords
セキュリティ・バイ・デザイン／ゼロトラスト／サイバーハイジーン／セキュリティコンサルティング／プロフェッショナルサービス／マネージドセキュリティサービス／セキュリティ人材育成

1. はじめに

企業や組織でのデジタルトランスフォーメーション（以下、DX）の取り組みの進展に伴い、サイバーセキュリティの重要性が高まっています。

本稿では、背景となるサイバーセキュリティの動向、NECのサイバーセキュリティ事業の特徴及びDXを支えるセキュリティサービス及びDXオファリングを紹介します。

2. サイバーセキュリティの動向

近年、企業や組織がDXを進めるにつれ、さまざまなシステムがつながり、企業や組織の外でのPC利用などが活発化しています。この状況を攻撃者から見ると、インターネットに直接接続している端末など攻撃可能な対象が増え、一度システムに侵入したら更に奥深くに入りやすくなったといえます。また、従来の金銭目的の攻撃者に加え、経済安全保障上の利益を目的とした高度なスキルを持つ攻撃者も増えています。

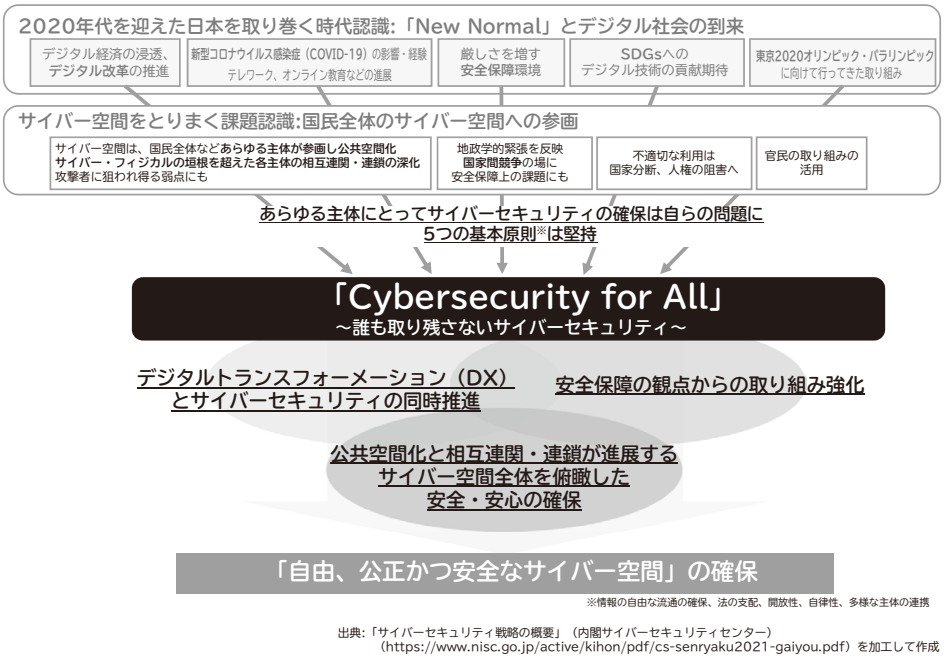
今や企業や組織は事業に影響を与えるようなサイバー攻撃に日々さらされており、サイバーセキュリティはこれまで以上に大きな経営課題となっています。

このような状況に対し、日本政府は2021年9月に策定したサイバーセキュリティ戦略[1)]のなかで、自由、公正かつ安全なサイバー空間を確保するために、「デジタル改革を踏まえたデジタルトランスフォーメーションとサイバーセキュリティの同時推進」を含む3つの方向性を示しています（**図1**）。更に、業務、製品・サービスなどのシステムの企画・設計段階からサイバーセキュリティを確保する「セキュリティ・バイ・デザイン」（以下、SBD）の考え方、デジタル化とサイバーセキュリティ確保の取り組みを同時に推進すること、すなわち「DX with Cybersecurity」に言及しています。

つまり、これからの企業や組織は、サイバー攻撃が激化・高度化するなか、DX with Cybersecurityを実現し事業を継続することが求められています。そのためには、セキュリティ対策を後付けするのではなく、システムの企画段階から体系的に検討・導入・運用し、今後発生しうる事件・事故へ備えることが必要です。

3. NECのサイバーセキュリティ事業の特徴

NECはお客様のビジネスを止めないことが何よりも重要であるとの考えから、SBDを「正しくつくる」「正常を



出典:「サイバーセキュリティ戦略の概要」（内閣サイバーセキュリティセンター）
（https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2021-gaiyou.pdf）を加工して作成

図1　日本政府のサイバーセキュリティ戦略の課題認識と方向性

つづける」「攻撃からまもる」と整理し（**図2**）、製品を販売するだけでなく、システムの企画・設計から開発、運用・監視までのライフサイクル全般にわたる各種サービスを提供しています。

また、従来のオフィス環境ではPCなどの端末も業務アプリケーションも社内にあったのに対し、DXやテレワークの環境下では社外に持ち出した端末から社内システムにアクセスしたり、社内の端末から社外のクラウドを利用したりすることが前提となります。もはや、社内にあるから安全という従来の常識は通用せず、端末からアプリケーションへのすべての通信をセキュリティ上問題ないか確認する（ゼロトラスト）必要があります。また、端末やシステムに存在する脆弱性を常に排除する活動（サイバーハイジーン）も合わせて求められます。

NECはこれらの考えをベースに、お客様のセキュリティ上の課題を解決する一連の製品・サービス（**図3**）についてノウハウや技術などを集約し、DXオファリングメニューとして提供しています。第4章以降では、システムの企画・構築・運用の各段階におけるサービスと、ベースとなる人材育成について順を追って紹介します。

図2　求められるサイバーセキュリティ対策

4. セキュリティコンサルティングサービス

DX with Cybersecurityを実現するためには、高度化・巧妙化するサイバー攻撃への対応だけでなく、プライバシー保護や、それらのベースとなる政府機関などによるセキュリティレギュレーション/ガイドラインへの準拠方針をDXの企画・構想策定段階から検討する必要があります。

NECでは、DXに取り組むお客様の情報システム部門（IT）や製品開発部門（IoT）、生産部門（OT）に対して各種セキュリティコンサルティングサービスを提供しています。これらには、(1) NECで長年整備・運用してきた自社システムへのセキュリティ対策から得たノウハウの活

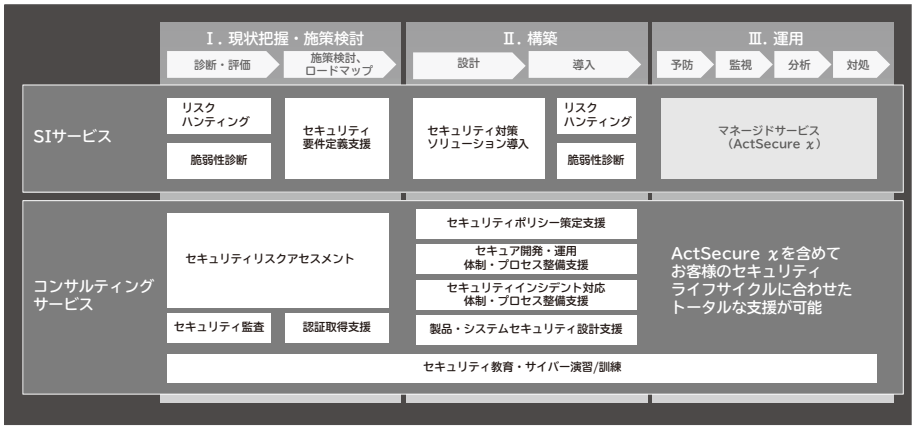


図3　NECのセキュリティサービス

用、(2) CISSP (Certified Information Systems Security Professional) や情報処理安全確保支援士などのセキュリティ資格保有者やセキュリティの国際標準化委員会メンバーによる豊富なコンサルティング実績、(3) 各種セキュリティレギュレーション/ガイドラインへの準拠、という特徴があります。

DXオファリングとして、セキュリティリスクアセスメント、セキュリティポリシー策定支援、セキュア開発・運用体制・プロセス整備支援、セキュリティインシデント対応体制・プロセス構築、製品・システムセキュリティ設計支援の各種コンサルティングサービスを提供しています。次に、セキュリティアセスメントとセキュア開発プロセス整備の導入事例を紹介します。

ある金融業のお客様はDXに伴うクラウド環境へのシフトの際に、サイバー攻撃のリスクを懸念し、自社ITシステムのセキュリティ対策強化を課題としていました。そこで、DXシステムのセキュリティアセスメント（脅威分析）を実施したところ、なりすましや不正侵入などの脅威に対して数十件の脆弱性が見つかり、脅威への対策が不十分であることが判明しました。そこで、NECからゼロトラストを踏まえた各種セキュリティ強化策を提案し、脅威への対策を行いました。あわせてSBDを踏まえた自社ITシステムのセキュア開発プロセスの構築を支援しました。その結果、お客様が新規に開発するITシステムは、開発の上流段階からセキュリティが考慮されるようになり、テスト工程や運用段階で検出される脆弱性の件数が低減され、後戻り工数を削減できました。

本事例以外にも製造業向けのIoT製品のセキュア開発支援、重要インフラ向けOTポリシー策定支援などでお客様のセキュリティ強化に貢献しました。

5. プロフェッショナルサービス

プロフェッショナルサービスは、お客様の企画・設計段階から、構築、運用までを支援する、セキュリティのプロフェッショナルによるトータルサポートサービスです。

前述したゼロトラストやサイバーハイジーンを実現するには、製品・サービスを個別に導入するのではなく、各製品・サービスを適切に設定し、連携して動作させることで通信の確認や脆弱性の排除を漏れなく継続的に行う必要があります。

そのためにはセキュリティの設計・構築・運用に関する高度な専門知識が必要で、その知見が不足していると設定ミスなどからセキュリティ上のリスクが生じることもあります。

プロフェッショナルサービスはこの支援を行うサービスで、次の特徴があります。

- SBDの考え方に基づいた設計、構築、運用を支援
- 数多くの製品の導入、構築から運用までを実践してきた経験豊富な技術者による対応

これら豊富な知見を活用して、セキュリティ対策の迅速な導入を実現するオファリングメニューを提供しています。例えば、「クラウドセキュリティ（Zscaler Internet Access）導入支援プロフェッショナルサービス」は、セキュアなインターネットアクセス環境を構築する製品の

Zscaler Internet Accessに関して、要件ヒアリング、パラメータ設計、構築、試験、お客様管理者向け操作説明までの一連の作業を支援するサービスです。また、Microsoftのクラウドサービスについてもオファリングメニューとして提供しています。

今後はプロフェッショナルサービスとして運用支援サービスを加え、トータルサポートを提供していくとともにオファリングメニューの継続的な改善や、 MicrosoftやAWSなどのクラウドシフトにおけるセキュリティ対策メニューの拡充を図っていきます。

6. マネージドセキュリティサービス

テレワークの普及やクラウドシフトにより、以前から監視しているファイアウォールなどに加え、従業員が社外に持ち出す端末（エンドポイント）やクラウドへのアクセスも重要な監視対象になっています。その結果、セキュリティ運用・監視業務はますます高度化し、負荷も増大しています。NECは、これら課題に対応するマネージドセキュリティサービスを提供しています。

ActSecure χマネージドセキュリティサービス（**図4**）は、クラウドからエンドポイントまでのセキュリティログ監視によりお客様の安全なクラウド活用を支援します。

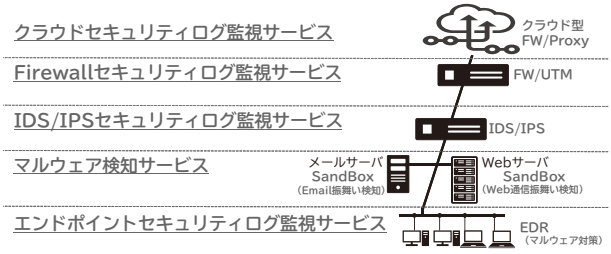


図4　ActSecure χマネージドセキュリティサービス

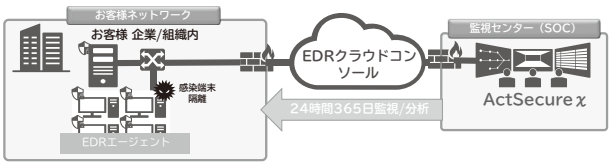


図5　エンドポイントセキュリティログ監視サービス

DXオファリングとして提供しているクラウドセキュリティログ監視サービスでは、クラウド上のファイアウォール/プロキシサービスから出力されるアラートを監視し、検知したアラートの重要度を判定し、お客様へ通知する一方、重要アラートに関しては通信遮断などの対処を行います。エンドポイントセキュリティログ監視サービス（提供予定）では、端末にインストールされたセキュリティ製品から上がるアラートの重要度を判定し、端末隔離、当該プロセスの停止などの初動対応を迅速に行います（**図5**）。

ActSecure χマネージドセキュリティサービスでは、NEC社内監視でも活用している独自インテリジェンスや、AIとセキュリティ専門アナリストの組み合わせにより、高精度でありながら迅速・効率的なセキュリティ監視を24時間365日提供し、お客様のセキュリティ向上を支援します。

7. セキュリティ人材育成

企業や組織が安全にDXを進めるためには、SBDの考え方に合わせてシステムのセキュリティ設計・実装を推進し実践できる人材の育成が必要です。しかし、セキュリティ演習の多くは、インシデント発生時の事後対応に重点を置いています。そこで、NECグループではセキュリティ設計・実装を組み込むための実践的な演習を開発し、人材育成プログラムに取り込んでいます（**図6**）。

業界に先駆けて2019年よりシステムエンジニア向けに常設の「NECサイバーセキュリティ訓練場」の演習環境（延べ2,800名以上が参加）を用意しています。演習では、自らがセキュア構築を行い堅牢化したシステムが実際に攻撃を受けるという体験を通してセキュア構築の重要性を学びます。そして、丁寧な振り返りにより実践的なセキュリティ設計・実装能力とインシデント対応スキルを習得します。

また、2015年より延べ5,000名以上が参加している「NECセキュリティスキルチャレンジ」という社内コンテストによりスキルを可視化し、公的機関や業界団体などで体系化された人材像*と紐付けることで潜在的なセキュリティ人材発掘や育成を行っています。

NECは、グループのエンジニアが活用するこれらの実践的育成プログラムを、「NECサイバーセキュリティ訓練場演習」「NECサイバーセキュリティ競技場演習（CTF:

* セキュリティ知識分野（SecBoK）人材スキルマップ（特定非営利活動法人日本ネットワークセキュリティ協会）、iコンピテンシ ディクショナリ（独立行政法人情報処理推進機構）など

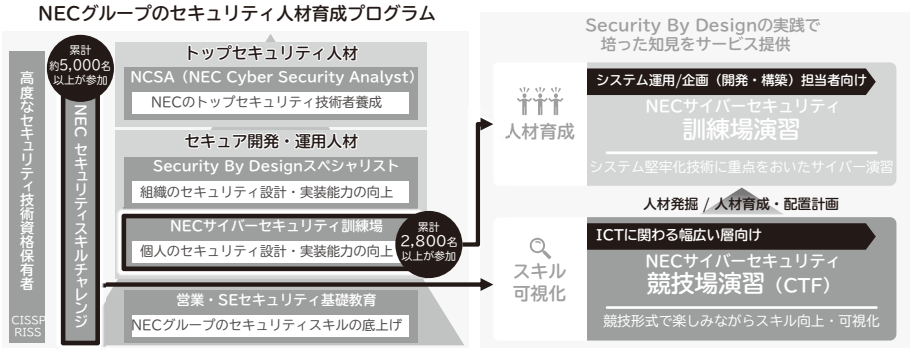


図6　NECグループのセキュリティ人材育成プログラム

Capture The Flag)」としてオファリング化し、お客様に提供しています。これらのサービスを活用することにより、お客様はセキュア構築とインシデント防止のための実践的なスキルの向上、組織内の潜在的なスキルを保有する人材の発掘・育成が見込めます。

活用例として、新宿区様にて実運用を踏まえてカスタマイズしたNECサイバーセキュリティ訓練場演習を行った結果、担当職員のスキルアップにとどまらず、情報共有などの運用上の課題にも気づきを得ていただいています。

8. むすび

本稿では、DXの進展に伴いサイバーセキュリティの重要性が高まっていること、企業はSBDの考え方に基づき企画から運用まで一気通貫のセキュリティ対策を導入しなければならないこと、そしてそのニーズに応えるNECの各種セキュリティサービス及びDXオファリングを説明しました。NECは、今後も企業や組織のDXをセキュリティで支え、安全・安心な社会の実現に貢献します。

参考文献

1) 内閣サイバーセキュリティセンター：サイバーセキュリティ戦略の概要，2021.9
https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2021-gaiyou.pdf

執筆者プロフィール

吉府 研治
DX戦略コンサルティング事業部
シニアエキスパート

鈴木 章工
サイバーセキュリティ事業部
シニアエキスパート

岡崎 巧
サイバーセキュリティ事業部
エキスパート

西野 真一郎
サイバーセキュリティ戦略本部
マネージャー

小川 賢一
サイバーセキュリティ事業部
主任

薄羽 利光
サイバーセキュリティ戦略本部
主任

関連URL

セキュリティ プロフェッショナルサービス
https://jpn.nec.com/cybersecurity/professionalservice/index.html

ActSecure χ マネージドセキュリティサービス
https://jpn.nec.com/actsecure/actsx_mss.html

セキュリティ教育・サイバー演習／訓練
https://jpn.nec.com/cybersecurity/professionalservice/education/index.html

NEC 技報のご案内

NEC技報の論文をご覧いただきありがとうございます。
ご興味がありましたら、関連する他の論文もご一読ください。

NEC技報WEBサイトはこちら

NEC技報（日本語）　NEC Technical Journal（英語）

Vol.74 No.2　社会のデジタルトランスフォーメーションを加速するDXオファリング特集

社会のデジタルトランスフォーメーションを加速するDXオファリング特集によせて
NECがDXオファリングで目指す社会のデジタルトランスフォーメーション
社会のデジタルトランスフォーメーションを加速するDXオファリング

◇ 特集論文

お客様の事業変革やイノベーションを促進するDXオファリング
企業のDX戦略と実現ロードマップを描くDX戦略コンサルティングサービス
「NECのデザイン思考」で新事業創造と事業改革を加速 Future Creation Design DXオファリング Suite

お客様との接点を改革するDX オファリング
イベント活性化― 安全・安心と施設を核とした地域活性化
NECの生体認証技術が実現する安全・安心な空港運営
都市・不動産DXの現在地 ～データプラットフォームを活用した新たな価値創出のあり方～
DX効果の最大化のためのユーザーサポート ～厚労省プロジェクトを通じての考察～

お客様の業務改革を推進するDXオファリング
新たな働き方やビジネスを生み出す場所 ～NEC デジタルワークプレイス～
フィールドサービスマネジメント領域でのDXの取り組み
産業のDXを加速し豊かな社会を実現するローカル5G
SCM（Supply Chain Management）高度化支援
データドリブン経営を実現する、DXオファリングとその導入事例

デジタル人材の育成やデジタル組織運営を支援するDX オファリング
デジタル時代のDX人材育成
DX時代の組織人材変革を支援するDXオファリング

DXを支えるIT インフラ
DX時代のトータルサイバーセキュリティ
DXにおけるITサービスマネジメントの取り組み
DXオファリングを支える「NEC Digital Platform」

DXオファリングを支える先端技術及びメソドロジー
DXオファリングを支える国産・自社開発のIaaS「NEC Cloud IaaS」
生体認証が切り拓く未来
加速度的な成長を実現するコンポーザブル経営とデジタル変革

◇ NEC Information

2021年度C&C賞表彰式典開催

Vol.74 No.2
（2022年3月）

特集TOP