新たな社会に適応するサイバー経営の在り方

デジタルエコノミーの浸透に伴い、サイバー空間はフィジカルな社会との融合が進展している。これは社会の利便性を高める一方で、セキュリティリスクの増加をもたらしている。安全・安心なデジタル化の社会の実現には、サイバーセキュリティの確保が必須となる。業務スタイルの変化、IoTやAIなどの進化、サイバー攻撃の動向などを踏まえ、CISO（最高情報セキュリティ責任者）が中心となり、組織として最適化された『サイバーセキュリティ経営』を策定し、自律的なセキュリティ対策の実践が求められる。

背景と現在の状況

サイバー空間を取り巻く状況は、ますます複雑化している。世界経済フォーラムが発表するグローバルリスク報告書では、標的型攻撃や産業制御システムをターゲットとするサイバー攻撃が重要課題となり、日本国内でも大規模なセキュリティインシデントが継続的に発生している。今後、いくつかの国際的なイベントの催しが予定されているが、過去の他国の開催状況を鑑みると、イベント開催期間中においても関連団体、民間企業での被害発生が予想される。また、IoTの爆発的な増加やAI活用が進み、さまざまなモノが自動化・ロボット化し、ネットワークに接続される「Society 5.0」の実現が産学官を問わず推進されている。社会課題を解決する今までにない新しい価値を生み出す一方で、保護対象の管理が困難になりこれらのシステムへのハッキングも増加傾向にある。こうした状況を踏まえ、日本政府は2020年およびその後の持続的な発展のため、サイバーセキュリティエコシステムの推進を掲げている。

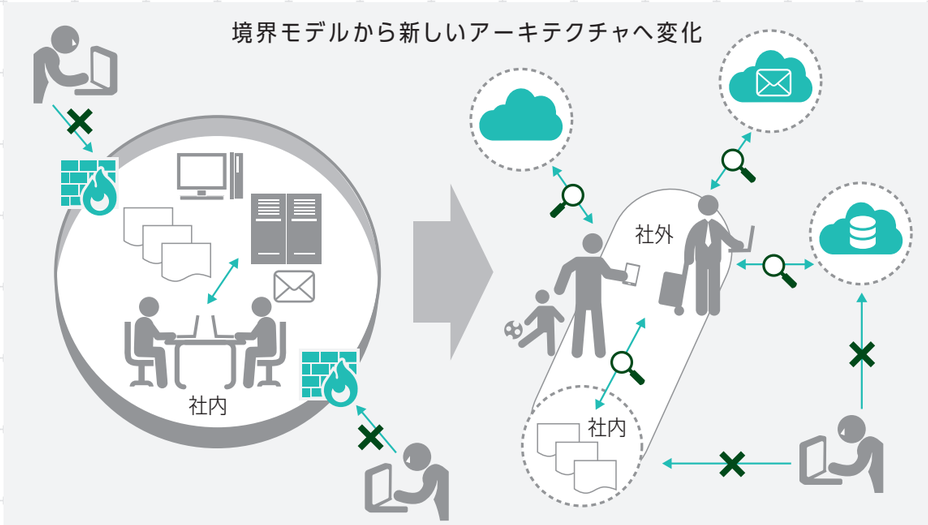
3〜5年後の姿

サイバー攻撃の高度化、テクノロジーや環境の変化によって、これまでパッチワーク的に行われてきたセキュリティ対策では、セキュリティインシデントの発生を未然に防ぐことは困難である。自社を取り巻く脅威やリスクをベースとする中長期的観点でのサイバーセキュリティ戦略とそれに基づいた『サイバーセキュリティ経営』の策定が、企業経営のスタンダードとなる。

セキュリティアーキテクチャの再定義

クラウドを基盤としたAI、IoT、VRなどのテクノロジーの活用が促進され、既存構造を覆すイノベーションが牽引される。これにより、サイバー空間と実空間のさらなる一体化が進展し、セキュリティアーキテクチャのあるべき姿も大きく変化する。

セキュリティ対策をネットワーク境界の内・外という概念ではなく、いかなるアクセスもその信頼度を0（ゼロ）とするゼロトラストの発想の下、ボーダレスなセキュリティ対策が必要となる。働く環境の多様化（働き方改革）や、クラウド活用によるシステム構成の複雑化により、既存の防御機構が有効にならないケースが散見される。そのため、ユーザーやデバイスの情報や、その振る舞いなどに基づく認証および認可の制御やエンドポイントを重視したアーキテクチャが用いられる。さらに、脅威インテリジェンスやAIを活用したセキュリティソリューションとの連動により、未知の脅威への対応が強化される。



ネットワーク境界の内・外という概念ではなく、ボーダレスなセキュリティが求められる。

©2019 Nihon Unisys, Ltd. All rights reserved.

ステルス化された攻撃手法への対抗

暗号化されたマルウェア、難読化を行うポリモーフィック型マルウェア、実行ファイルが存在しないファイルレスマルウェアなどステルス化された攻撃手法により、既存のエンドポイント対策ソフトで検知できない状況も生まれている。こうした高度な標的型攻撃や脆弱性を突いた不正アクセスで用いられる未知のマルウェアに対応すべく、新たな防御技術を用いたソリューションにより、エンドポイント対策の強化が図られている。

セキュリティと利便性が両立したパスワードレスの社会へ

現在、新しい主体認証モデルが普及し、我々はパスワードとIDの管理の悩みから解放されつつある。よりセキュアでかつ利便性が向上したパスワードレスの新たな認証モデルが、金融機関やその他のサービスで採用され始めている。これには指紋や虹彩などの生体情報の認証情報をサーバには送信せず、ユーザーが持つスマートフォンなどで検証され、その結果をサーバ側がトラスト（信頼）しパスワードレスを実現するFIDO※1や、利用者の利用用途や行動状況パターンなどを分析するリスクベース認証といった技術が用いられる。

サイバーレジリエンス（Resilience）のさらなる向上の必要性

医療システムや鉄道システムなどの日常生活に不可欠な重要インフラに関係するシステムがランサムウェアに感染し、操業を停止せざるを得ない状態に陥る事案がすでに発生している。

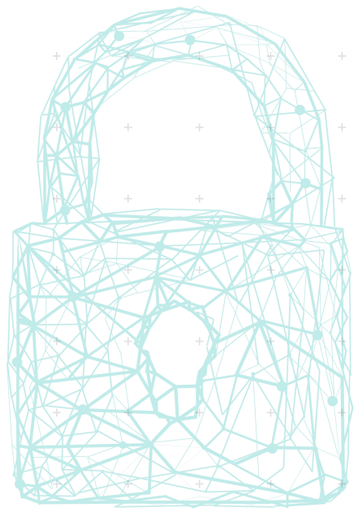
相次ぐセキュリティインシデントの経験から、100%の防御は不可能との認識の下、インシデント対応や復旧に軸足を移した企業が増加し、大多数の上場企業にCSIRT※2が設置されている。この一方で、実効性を持つCSIRTを維持できている組織は少ない状況である。実効性の担保と向上のためには、平常時の教育や訓練に加えて、脅威情報の収集による予見やインシデント対処の自動化による対処能力を保持し、セキュリティインシデントからの迅速な復旧と回復を図るレジリエンスのさらなる向上が求められている。

※1 FIDO：Fast IDentity Online
※2 CSIRT：Computer Security Incident Response Team

グローバルなサイバー攻撃の増加、諸外国の取り組み

ハードウェア製品や情報システムへの不正改造、悪意ある変更を加えるサプライチェーンリスク、SNS操作、フェイクニュースなどを使った情報操作に国家の組織的な関与が疑われる事案もこれまでに発生している。

その影響範囲は拡大し、社会的、経済的な被害も指数的に増加している。このような状況に対し、各国はサイバーセキュリティをめぐる戦略的な取り組みを強化している。米国は、連邦政府や重要インフラの強化に関する大統領令をはじめとして、オープンでセキュアなインターネットの推進をリード。また、欧州連合（EU）では、独自の枠組みを推進し、一般データ保護規則（GDPR）を強化し、全世界へ対応を訴求している。これらはグローバル展開する企業にとって、データの利活用における一定のリスクとなっていく。



©2019 Nihon Unisys, Ltd. All rights reserved.