特集 **時代の転換期とDX**

サイバー攻撃の進化と経営者に求められる対応
「セキュリティ・バイ・デザイン」でサイバー攻撃に立ち向かう

小田島　潤

CONTENTS

要　約

1　コロナ禍でサイバー攻撃とそれに伴うセキュリティ事件・事故が激増している。2020年度の被害件数は、19年度比で約2.3倍に増えたという報告もある。これは、明らかにテレワークの増加が影響している。コロナ禍でデジタル変革（DX）が加速したといわれているが、DXにおけるセキュリティの問題は経営を揺るがしかねない。

2　サイバー攻撃の歴史を振り返ると、2000年代半ばに登場した不正送金（バンキング）マルウエアなどにより金銭目的へと変化し、現在もランサムウエアによる被害が拡大し続けている。さらに10年以降には、米国とイスラエルによるイランの核燃料施設への攻撃疑惑など、重要インフラや国家機密にまで及ぶリスクが広く認識された。

3　最近ではソフトウエア製品の開発元などの取引先を経由して、最終的な攻撃目標への侵入を果たす「サプライチェーン攻撃」が非常に大きな脅威となっている。

4　これらの状況を踏まえると、リリース直前に脆弱性診断を行い、システムの穴を慌ててふさぐ「後付け」「外付け」のセキュリティ対策では、世界中の攻撃者に全く歯が立たないのは明らかである。システムの企画・設計段階から攻撃者の観点を踏まえてセキュリティ対策を「先回り」して「内蔵」する「セキュリティ・バイ・デザイン」が必要となる。

5　最後に、経営としてセキュリティ・バイ・デザインに取り組むために、セキュリティ・バイ・デザインの効用、セキュリティ専門人材の獲得と育成、セキュリティ組織の独立性、サイバー攻撃対策訓練の重要性、について述べる。

Ⅰ DX時代のセキュリティリスク

1 コロナ禍で激増するサイバー攻撃とセキュリティ被害

新型コロナウイルスの感染拡大により、緊急事態宣言が発出された2020年４月以降、サイバー攻撃による被害が数多く報道されている。最近では、21年10月に徳島の病院がランサムウエア攻撃[注1]を受け、約８万5000人分の患者情報が暗号化された。さらに、診療報酬計算や電子カルテ閲覧のための基幹システムが使用不能となり、一部の診療科を除き新規患者の受け入れを停止せざるを得ない事態に陥った。幸いなことに、本件が直接的な原因となって亡くなった方がいるという話は伝わってきていないが、20年９月にはドイツの大学病院がランサムウエア攻撃を受けて、当該病院に救急搬送された患者を受け入れることができず、別の病院への搬送中に亡くなったという痛ましい事件もあった。

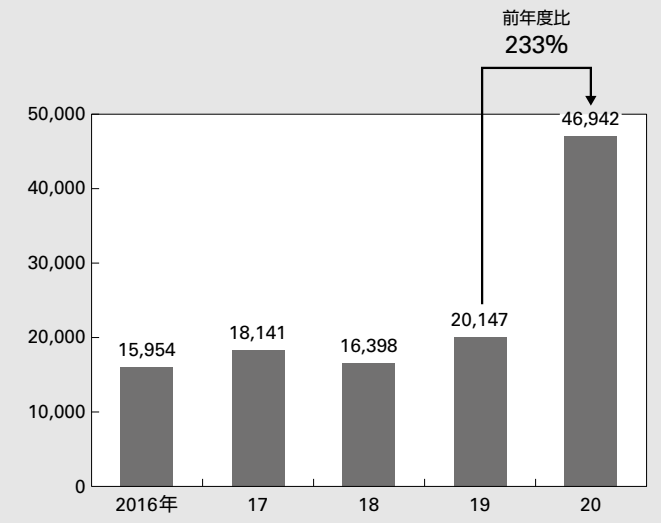
このコロナ禍で、サイバー攻撃による被害が増えていることは、数字でも裏付けることができる。図１は、JPCERT/CC[注2]によるセキュリティインシデントの年間報告件数推移であるが、20年度は19年度比で約2.3倍と激増している。

この背景には、コロナ禍の緊急事態宣言で多くの企業が急遽テレワークへの移行を強いられたことが一つの要因としてある。テレワークを行うために、社外のどこからでも社内のPCやサーバーへの遠隔ログオンを不用意に許可した結果、IDとパスワードを推測されて社内に侵入される事案や、社外から社内への通信を暗号化するVPN[注3]装置の脆弱性（セキュリティ上の弱点）を突かれて侵入される事案が急増している。最近報告されるランサムウエア被害の多くは、このパターンであると考えられる。ぜひ、自社のテレワーク環境のセキュリティについて再点検することを勧めたい。また、コロナ禍以前から主な攻撃手段だった、マルウエア添付や悪性Webサイトへのリンクを含むメールによる攻撃も、「コロナ給付金のお知らせ」や「ワクチン接種予約の方法」など、コロナ禍に便乗する形でより巧妙化している。

2 DXで特に注意すべきセキュリティ関連トピック

さて、今般のコロナ禍には、対面でのビジネスや出社による業務が難しくなり、電子商取引（EC）による物販・宅配や契約・経理事務のペーパレス化など、デジタル変革（DX）を加速した側面もある。DXとはデジタル技術でビジネスや経営を変革することであるため、DX関連システムにおけるセキュリティ問題は経営責任や法的責任に直結す

図1 セキュリティインシデントの年間報告件数推移



出所）一般社団法人JPCERTコーディネーションセンター「JPCERT/CCインシデント報告対応レポート 2021年１月１日～2021年３月31日」（2021年４月15日）より作成 https://www.jpcert.or.jp/pr/2021/IR_Report20210415.pdf

る。キャッシュレス決済システムの認証が甘く、攻撃を受けて金銭的被害に遭った事案では、当該事業会社の社長が退任を余儀なくされ、英国の大手航空会社では、チケット予約サイトの脆弱性により大量の個人情報が流出したため、欧州GDPR（一般データ保護規則）違反により巨額の制裁金を科せられるに至った。

その反面で、DXを実現するためには、多種多様な技術を駆使し、他社のシステムとも連携する必要がある。それは、技術的な複雑性が増すと同時に、セキュリティリスクも高まるということである。特に、プライバシー・IoT・FinTechの三つが、セキュリティ面で特に注意すべき領域である。

(1) プライバシー

まず、DXにおいて、顧客情報や行動履歴を収集・分析して、顧客の嗜好に合わせた商品をタイムリーに開発・提供するデジタルマーケティングは大きな武器の一つである。その一方で、前述のGDPRだけでなく、日本の個人情報保護法改正や米国のCCPA（カリフォルニア州消費者プライバシー法）など、プライバシー関連法による規制の強化は世界的な潮流である。加えて、最近では個人情報の取り扱いにかかわる消費者の関心も非常に高まっている。就職情報サイトから学生の内定辞退率のデータが顧客企業に提供されていた事案や、SNS[注4]の個人情報が中国で閲覧可能だった事案が大きく報道されたのは記憶に新しい。

プライバシーの問題はセキュリティと混同されることが多いが、注意すべき相違点もある。それは、行動履歴を含む個人情報はあくまで消費者や従業員個人の所有物であり、企業は預託を受けているに過ぎないということである。前述の事案は、その意識が希薄だったといわざるを得ない。法律の遵守はもちろん重要だが、情報を預ける個人の感情にも配慮する必要がある。その一方で、個人情報の漏洩はプライバシーにおける最大の問題であり続ける。個人情報に関しても、企業が所有する機密情報と同様に、然るべきセキュリティ対策により保護する必要がある。

(2) IoT

IoTは、リアルなモノをインターネットにつなげ、大量のデータを収集・分析し、モノを最適に制御することを目指す。アナログな物理空間とデジタルな仮想空間をつなぐDXの本命技術である。しかし、IoT機器においても、多数の脆弱性が報告されている。

たとえば、米国で発売されたインターネットにつながる「ぬいぐるみ」には、利用者（子供）の個人情報が漏洩する脆弱性があった。実害はないように思われるが、場合によっては子供を巻き込む犯罪に悪用されかねない。この玩具メーカーに対するブランドイメージは確実に棄損されたであろう。

また、中国製のインターネット接続可能なあるWebカメラは、攻撃者に乗っ取られてDDoS攻撃[注5]の踏み台となった。このWebカメラの製造元は、DDoS攻撃の被害に遭った企業から製造物責任を問われ損害賠償請求の訴訟を起こされる恐れがある。

しかし、IoTのセキュリティにおける最大の問題は、自動運転車や「つながる車」などがハッキングを受け、遠隔から不正に操縦されるリスクである。2015年には、クライスラ

ーの「ジープ・チェロキー」に外部からハンドルやエンジンを不正に操作される脆弱性が見つかった。その結果、クライスラーは約140万台のリコールを余儀なくされた。幸運にも、この脆弱性を悪用した事故は発生しなかったが、一つ間違えれば人の命が失われる。IoTのセキュリティには、モノによって人命に直結するリスクがあることを、あらためて肝に銘じる必要がある。

その一方で、IoTにおいては無数の機器が遍在するため、ファイアウォールなどによるネットワークレベルでのセキュリティ対策が難しい。また、処理能力の制約から、ウイルス対策ソフトなどをIoT機器に搭載するのが難しい場合も多い。したがって、IoTにおいては後述する「セキュリティ・バイ・デザイン」が非常に重要となる。特に自動車は、サイバーセキュリティ対策が初めて義務化され、22年7月以降に発売される一部の新車は、セキュリティ・バイ・デザインの考え方に沿って設計・開発・製造することが求められるようになった。

(3) FinTech

最後にFinTechであるが、消費税増税後の消費冷え込み対策や東京五輪で来訪する外国人への対応を踏まえた政府の後押しもあり、QRコードなどによるキャッシュレス決済が急速に普及した。しかし、不幸にして、2020年まで3年連続でキャッシュレス決済サービスの脆弱性を突いた攻撃による金銭被害が発生し、大きく報じられた。

あるコンビニエンスストアのQRコード決済サービスでは、他人のIDとパスワードさえ知っていれば、専用アプリをインストールし、その人になりすまして買い物ができた。また、ある携帯電話会社のQRコード決済サービスでは、サービス開始当初はその会社の携帯電話の契約者に利用が限定されていたが、サービス利用者拡大を目指して、メールアドレスさえ提示すれば利用者登録が可能となり、身元確認が甘くなった。さらに、銀行の口座番号と暗証番号さえ知っていれば、他人の口座からお金を引き落として電子マネーとしてチャージすることができたため、不正利用による被害が発生した。

これらの事案に共通するのは、システム単体の実装面では一定のレベルでセキュリティ対策を実施していたと推測されるが、利用者認証や他社システム連携に関して、セキュリティ面での検討が果たして十分だったのかという点である。つまり、システム開発に入る前の、サービス企画・設計段階における検討である。

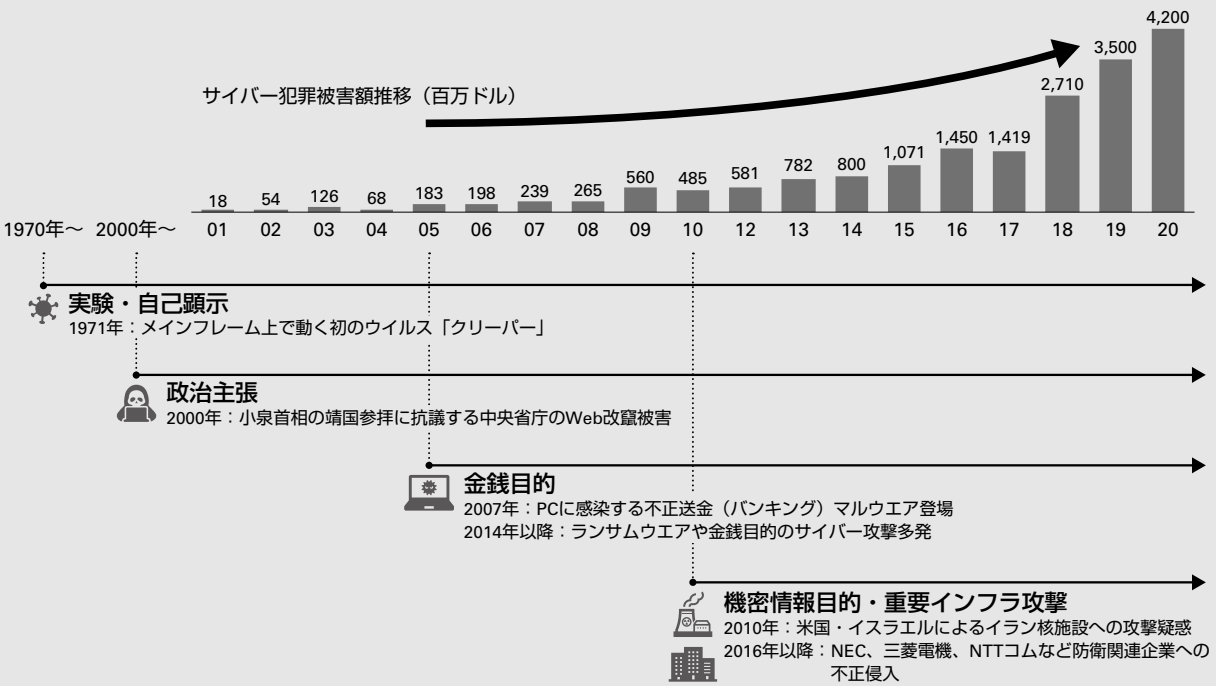
ほかにもFinTechの分野では、金融機関の決済機能をAPI[注6]で公開し、他業種を含めた他社の利用を促す動きが今後加速すると思われるが、ここでの脆弱性も金銭被害に直結するため、十分な検討が必要となる。また、ブロックチェーン（分散型台帳）上で取引条件をプログラム化し、仲介機能を持つ金融機関が存在せずとも自律分散的な金融取引を実現する、分散型金融（DeFi[注7]）も同様である。

Ⅱ サイバー攻撃の進化を振り返る

1 サイバー攻撃の歴史と進化

ここで、過去からのサイバー攻撃の歴史と進化を振り返ってみたい。1970年代のメイン

図2　サイバー攻撃の歴史と進化



出所）FBI Internet Crime Reportより作成
https://www.fbi.gov/investigate/cyber

フレーム時代から既に実験的なウイルスは存在していた。80年代に入って、研究者の間でインターネットが利用されるようになり、95年にはマイクロソフトが「Windows95」を発売し、本格的なインターネット時代が到来する。しかし、2000年の小泉首相（当時）の靖国神社参拝に抗議したハッカーによる中央官庁のWebサイト改竄事件の頃までは、サイバー攻撃は主に自己顕示や政治主張目的で愉快犯的に行われており、そこまで深刻な実害はなかったといえる。

しかし、00年代半ばに、PCに感染してインターネットバンキングを不正に操作し金銭を盗む「不正送金（バンキング）マルウエア」が登場してから、様相は一変した。サイバー攻撃が金銭目的に変わったのである。図2はFBIが公表したサイバー犯罪被害額の推移であるが、05年以降、増加の一途をたどっている。特に、18年以降の増加が顕著であるが、これは明らかにランサムウエア攻撃の被害拡大によるものである。10年には、米国とイスラエルがイランの核開発を遅らせるために行ったとされるサイバー攻撃（Stuxnet）が報告されており、16年以降にはNECや三菱電機など、防衛関連企業への不正アクセスと防衛機密の漏洩が疑われる事案も複数報告されている。つまり、サイバー攻撃が、金銭目的に加えて、重要インフラや国家機密を目的として行われているのである。

2　サイバー攻撃進化の背景

それでは、何故このような事態に至ってい

るのであろうか。背景には、①サイバー空間内での国家対立激化、②地下のサイバー犯罪経済圏の隆盛、③一般社会におけるIT利用拡大に伴う攻撃表面の増大という、負の連鎖がある。

まず、サイバー空間内の国家対立に関しては、米国・中国・ロシア・北朝鮮といった国々がそれぞれ陸海空軍に次ぐ「サイバー軍」を組織し、システムに潜在する未知の脆弱性と、それを悪用するサイバー兵器の研究・開発を進めている。さらに、たとえば、経済制裁に苦しむ北朝鮮が他国の暗号資産取引所に侵入して外貨を獲得し、核開発に流用している疑惑[注8]や、ロシアがSNS上での言論操作や候補者のメール盗聴により米国大統領選に介入した疑惑[注9]も報道されている。また、米司法省は、企業や政府、大学などを標的とした世界的なサイバー攻撃に関与したとして、中国政府の支援を受けたとされる中国人ハッカー数人を訴追した[注10]。対立関係にある国家間のサイバー攻撃が激しさを増す一方で、開発されたサイバー兵器が何らかの理由で民間の地下社会に流出する場合がある。

2017年には、米国のNSA（国家安全保障局）が開発したとされるWindowsの未知の脆弱性を突く攻撃ツール（EternalBlue）が流出した。これを悪用して行われた世界的なランサムウエア攻撃が、同年の「WannaCry」（ワナクライ：泣きたくなる）である。NHKのニュースでも報道されたため、覚えている人も多いだろう。サイバー空間内の国家間対立で産み落とされたサイバー兵器だけでなく、各種システムに存在する脆弱性を突いた攻撃ツールや流出した個人情報などが地下社会で取引され、ランサムウエア攻撃に代表されるサイバー犯罪に悪用されている。それにより、身代金などの不正な金銭的利得が得られ、さらにサイバー犯罪への新規参入者が増えるという、地下のサイバー犯罪経済圏の拡大へとつながっている。

DXのかけ声の下、われわれの暮らす一般社会においては、クラウドやモバイルといったITの活用が広がっている。これは、われわれの生活を便利にする側面がある一方で、攻撃者から見た攻撃表面、すなわちつけ入る隙が拡大するともいえる。サイバー空間内での国家間対立によって、機密情報が盗まれるリスクや発電所などの重要インフラが機能不全に陥るリスク、地下のサイバー犯罪経済圏からの攻撃で金銭が奪われるリスクが一層高まっているのである。

それではここで、最近の動向も踏まえて、①から③の状況を個別に見ていく。

（1） サイバー空間内での国家対立激化

2020年12月に、米国のIT監視ソフトウエア開発大手ソーラーウィンズに端を発する、大規模なハッキング被害が発覚した。同社は何者かに侵入されて、彼らの開発するIT監視ソフトウエアにマルウエアが仕込まれた。その結果、彼らのIT監視ソフトウエアを利用する、米国政府機関やマイクロソフトまでもが、不正侵入の被害に遭ったという事件である。

このように、取引先を経由して、最終的な攻撃目標への侵入を果たすことを「サプライチェーン攻撃」と呼び、最近では非常に大きな脅威として認識されている。取引先に対しては、防御が手薄になりがちであるため、それを突いた非常に巧妙な攻撃であるといえ

る。さらに、ソフトウエアやハードウエアの開発元に侵入した上で、その製品に仕込んだマルウエアやバックドア（侵入のための裏口）を悪用した攻撃を防ぐのは非常に難しい。この問題については第Ⅲ章で後述する。

ソーラーウィンズの事件に関しては、米国当局がロシア政府の関与を断定し、21年４月の米バイデン大統領と露プーチン大統領の電話会談の際に、バイデン大統領が正式に抗議し、経済制裁を発動するに至っている[注11]。

（2） 地下のサイバー犯罪経済圏の隆盛

「ダークウエブ」という世界をご存知だろうか。実体としてはインターネット上に存在しているが、専用のソフトウエアがないと一般人にはアクセスできない闇の世界である。日本でも麻薬取引や殺人依頼のような犯罪情報がやり取りされており、「闇サイト」と呼ばれることがある。

サイバー犯罪の文脈では、盗まれた個人情報やクレジットカード番号、システムの脆弱性などの情報が盛んに売買されている。ビットコインなどの仮想通貨（暗号資産）の登場により、身元を明かさずにこれらの犯罪情報やランサムウエア攻撃の身代金を取引できるようになったことが、現在の状況に一層拍車をかけている。

さらに最近、大きな問題となっているのは、RaaS（Ransomware as a Service）すなわち「サービスとしてのランサムウエア」の存在である。これは、ランサムウエア攻撃を行う仲間（アフィリエイト）を募り、その攻撃によって得られた身代金の分け前を与えるという、とんでもないビジネスモデルである。このようなものが登場したために、ランサムウエアを開発する技術力のない犯罪者でもランサムウエア攻撃に加担し、巨額の身代金の一部を得られるようになってしまった。同様に、事前に侵入しておいた大量の脆弱なIoT機器を手先として悪用する、「サービスとしてのDDoS攻撃」も存在する。

これらの攻撃で狙われる企業に共通するのは、事業継続にITが重要な役割を果たしている企業や、身代金の支払能力のありそうな企業である。特に、冒頭で紹介した医療機関のランサムウエア攻撃被害は人命に直結するため、由々しき事態である。欧米や日本など、国籍に関係なく多くの組織が被害に遭っているが、たとえばロシア語を使うPCでは起動しないランサムウエアが存在するなど、背後にいるサイバー犯罪者の出自に関して、一定の推測が可能な場合もある。

（3） 一般社会におけるIT利用拡大に伴う攻撃表面の増大

ダークウエブに存在するRaaSが大きな被害をもたらしたのが、2021年５月に発生した米国東海岸のパイプライン停止である。これは、米国のコロニアル・パイプラインが、ロシア系の犯罪集団（RaaS）とされる「DarkSide」によってランサムウエア攻撃を受け、パイプラインの停止に至った[注12]という事件である。コロニアル・パイプラインは、背に腹は代えられず、身代金440万ドルを支払い、２日後にはパイプラインの操業を再開するに至った。

これ以外にも、21年には米国の食肉加工業者JBSがランサムウエア攻撃を受けて工場の操業を停止したり[注13]、米国フロリダ州の浄水場が不正アクセスを受けて人間の致死量を

超える水酸化ナトリウムを混入されたり[注14]といった事件が多発した。

従来、これらの工場や大規模プラントにおいては工場設備の制御系ネットワークに専用の機器が使われており、OA環境の情報系ネットワークとは物理的にも論理的にも隔離されているため、サイバー攻撃の被害に遭うリスクは低いといわれてきた。しかし、次のような背景もあり、最近では全く当てはまらなくなってきている。

第一には、コロナ禍もあって、工場などを安定的に操業継続するために遠隔からの運用監視や保守が増えてきている点が挙げられる。昔であれば、電話のダイアルアップ回線や専用線で遠隔保守が行われていたが、最近はインターネット経由でアクセスするのが一般的である。だが、インターネット経由であれば、遠隔保守の入り口までは誰でも来ることができる。そこで、IDとパスワードだけの弱い認証や前述したVPN機器の脆弱性を突かれて入り口を突破され、結果的に制御系ネットワークへの不正侵入を許す事案が発生している。

第二には、最近のDXの流れの中で、工場内の制御系ネットワークから生産設備の稼働状況などのデータを収集し、情報系ネットワークで分析することで、工場内の機器の故障検知や生産・稼働の最適化に活用する事例が増えている点である。データを収集・分析するためには、制御系ネットワークと情報系ネットワークを接続する必要があるが、その間のセキュリティ対策が不十分であると、たとえば情報系のOA環境でマルウエア感染が発生した場合、制御系の生産設備にまで影響が及ぶ危険性が生ずる。

第三には、これまで制御系ネットワークにおいてはPLC[注15]などの専用機器が使われていたが、最近ではPCなどの汎用IT機器が使われることも多いという点である。さらに、制御系では可用性が最重要視されるため、機器の停止が必要なバージョンアップやパッチ（修正プログラム）適用といった作業が忌避され、脆弱性が放置される場合もある。既に販売と保守が終了しているWindows2000マシンがいまだに現役で稼働しているという話も聞いたことがある。このような環境に、万が一マルウエアが入り込んだらと考えるだけで恐ろしい。

人命にもかかわる大規模プラントだけでなく、一般の企業ITにおいても、クラウドやモバイルなどの利用拡大により、攻撃表面が増大している。特に、AWSやAzureといったパブリッククラウド上にシステムを構築することが一般的になっている昨今では、物理的なファイアウォールなどのセキュリティ機器を構築・設置する必要はなく、管理者画面でのクリック一つでアクセス制御などのセキュリティ設定が可能となっている。しかし、このように非常に便利になった反面、担当者のセキュリティ知識不足や単純な操作ミス・勘違いなどにより、アクセス制御設定が甘くなり、個人情報の露呈や不正アクセスといった被害が多発している。テレワークが常態化し、自宅に持ち帰った社用PCやスマートフォンで業務を行っていたところ、それらの端末が知らぬ間にマルウエアに感染し、出社して社内ネットワークに接続した途端に感染が拡大し、機密情報の漏洩などの被害に遭った事案も報告されている。

Ⅲ サプライチェーンセキュリティの動向

さらに、最近では前述したソーラーウィンズ事件のようなサプライチェーン攻撃の脅威が非常に高まっている。サプライチェーン攻撃には、①IT統制の及ぶ国内外子会社を経由した攻撃、②IT統制の及ばない外部委託先や関連会社を経由した攻撃、③ソフトウエア製品の開発元を経由した攻撃、の三種類に大別される。それぞれ、リスクの内容と対策が異なってくる。

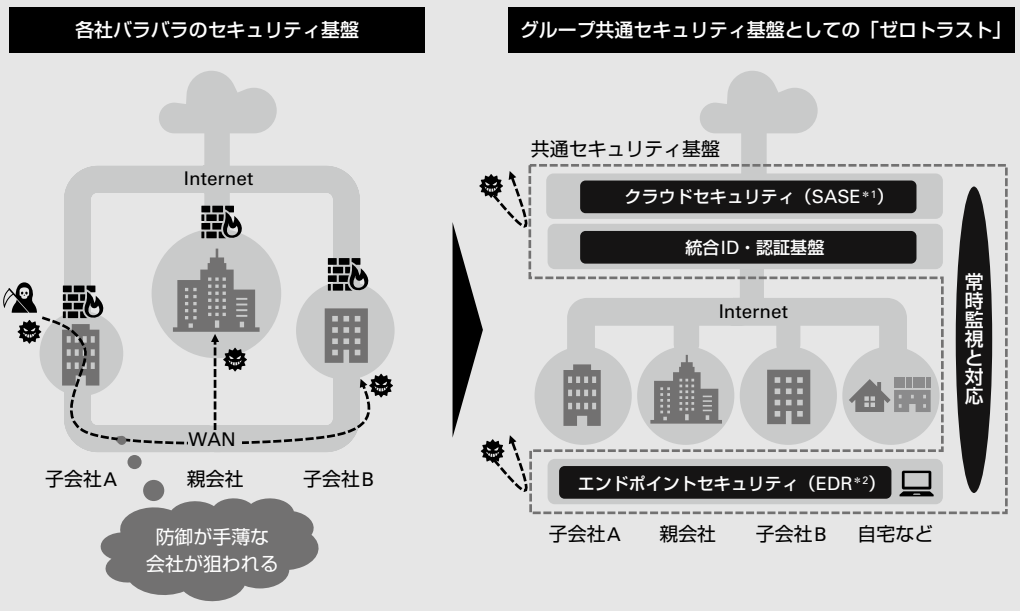
1 IT統制の及ぶ国内外子会社を経由した攻撃

子会社や海外拠点と親会社が直接社内ネットワークで接続されている場合、親会社の保有する個人情報や機密情報に不正アクセスされる可能性があるため、子会社や海外拠点経由での攻撃は非常にリスクが高い。防衛関連企業が、アジアの海外拠点から侵入を許し、防衛機密にアクセスされた可能性が発覚した事案も報じられている。

この場合、親会社がグループ共通のセキュリティ基盤を用意し、子会社や海外拠点も一定のコストを負担してこの基盤に相乗りすることにより、親会社と同等のセキュリティレベルまで引き上げることが対策の一案である。従来の「境界型」モデルでそれを実現しようとすると、社内（企業グループ内）と社外（インターネット）を区別し、その境界部分でセキュリティを守る考え方であるため、親会社のデータセンターにファイアウォールなどの境界型セキュリティ機器を設置し、子会社や海外拠点からのインターネット通信はすべて親会社のデータセンターを経由することになる。

しかし、特に海外拠点の場合、日本の親会社との通信遅延が問題となり、Web会議などの大容量通信が多くなった最近では使いも

図3　企業グループ共通セキュリティ基盤のイメージ



*1 SASE：Secure Access Service Edgeの略。包括的なWAN機能と種々のネットワークセキュリティ機能を組み合わせて提供
*2 EDR：Endpoint Detection and Responseの略。端末における侵入の検知と対応・復旧を迅速化するセキュリティ製品群

のにならない上に、社内ネットワークの通信コストなども馬鹿にならない。したがって、この際、企業グループ全体として「ゼロトラスト」モデルに移行し、端末での攻撃検知・防御機能と、認証やセキュリティ機能を提供するクラウドサービスを、各社共通で導入することを提案したい。インターネット接続を各社個別に行うことで、ネットワーク速度などの利便性は落とさずに、各社のセキュリティレベルを引き上げることができる。図3に、ゼロトラストモデルによる企業グループ共通セキュリティ基盤のイメージを示す。

2 IT統制の及ばない外部委託先や関連会社を経由した攻撃

外部委託先や関連会社が、EDI[注16]や業務委託のために直接ネットワーク接続されている場合、委託元の個人情報や機密情報が不正アクセスを受ける可能性がある。直接ネットワーク接続されていない場合でも、個人情報や設計書などの機密情報を渡している場合、委託先や関連会社からそれらの情報が漏洩するリスクがある。

このケースでも、共通のセキュリティ基盤を用意し、相乗りしてもらうことが可能であれば、それが望ましい。しかし、コスト負担の問題などもあって難しい場合、まずは委託先や関連会社のセキュリティ対策状況を把握することが第一歩となる。監査のために往訪したり、質問票への回答を求めたりすることになるが、監査には一定の基準が必要である。もちろん、自社のセキュリティポリシーやルール・ガイドラインに沿った監査でもよいが、被監査企業の負担を軽減し、項目の抜け漏れをなくすために、各種業界標準を参照することを勧める。業界に関係なく参照できる基準として、日本には経済産業省のサイバーセキュリティ経営ガイドライン[注17]があるが、最近注目すべき基準として、米国の国立標準技術研究所（NIST）が定めたNIST SP800-171がある。これは、米国の国防総省が調達先の民間企業に対して求める基準であり、日本の防衛省でも同等のセキュリティ基準が策定される予定である[注18]。

委託先や関連企業の監査は、監査側・被監査側双方の負担が大きい。また、Excelなどによる質問票の配布・回答・収集・分析も、手間がかかる上に回答の客観性などの面で課題が多い。そこで最近では、各種基準に準拠した質問への回答・分析作業を効率化し、外形的かつ客観的な評価も追加できるWebサービスが登場している[注19]。セキュリティの対策状況を把握して初めて、対策強化の依頼や契約・調達先の変更が可能となる。

3 ソフトウエア製品の開発元を経由した攻撃

ソーラーウィンズ事件がまさにこのパターンである。まず、ソフトウエアやハードウエア製品の開発元が侵入され、開発製品にマルウエアやバックドアが仕込まれる。すると、当該製品を導入した企業や組織がさらに侵害を受け、機密情報の漏洩やランサムウエア攻撃の被害へとつながる。

ソーラーウィンズ事件やコロニアル・パイプライン事件を受け、米国政府はサプライチェーン攻撃のリスクを危険視し、2021年5月にはバイデン大統領がセキュリティ強化に関する大統領令14028号に署名した。その中でも、特に「ソフトウエア・サプライチェー

ン・セキュリティの強化」が掲げられており、米国政府が調達するソフトウエアには、後述する「ソフトウエア部品表（SBOM）」の開示を含むセキュリティ・バイ・デザインの実践と開発環境のセキュリティ強化が求められることになる。米国政府調達の購買力は非常に大きいため、今後グローバル規模のソフトウエア製品ベンダーがセキュリティ・バイ・デザインを実践し、開発製品のセキュリティレベルが底上げされることが期待される。さらに、日米関係と経済安全保障を重視する、日本の岸田政権の今後の動向が注目される。日本でも同様の調達基準が採用される可能性もある。

Ⅳ セキュリティ・バイ・デザインとは何か

1 サイバー攻撃の進化と最近の状況に応じたセキュリティ戦略

第Ⅱ章で示した三つの負の連鎖が存在する最近の状況は、完全に攻撃者優位の世界であることを、まずは認識すべきである。この状況において、従来のようにシステムのリリース直前に脆弱性診断を受けて、指摘された欠陥をリリース期日までに慌てて修正したり、セキュリティ製品を突貫工事で導入してリリースに間に合わせたりするような、「後追い」「外付け」のセキュリティ対策では、世界中に存在する攻撃者に全く歯が立たないことは容易に想像できるだろう。すなわち、セキュリティ対策を「先回り」して「内蔵（ビルトイン）」するセキュリティ・バイ・デザインが必要となる。

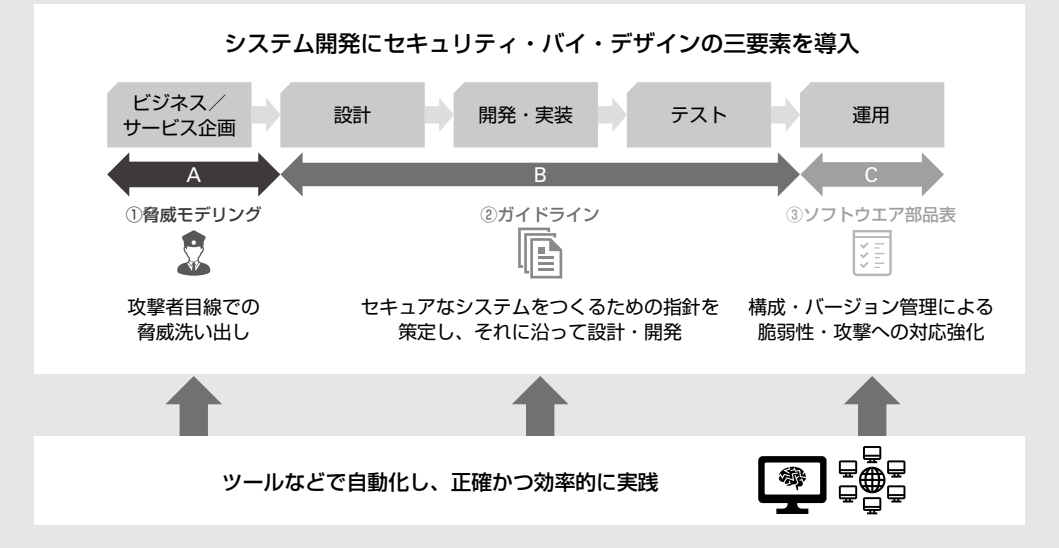
セキュリティ・バイ・デザインとは、一般的にはシステム開発の早い段階、すなわちDXのビジネスやサービスの企画・設計段階から攻撃者の目線でセキュリティ対策を検討し、システムの仕様としてつくり込む「システムのデザイン（設計）によるセキュリティ」を意味するが、セキュリティを組み込む開発プロセスをツールなどにより自動化する「プロセスのデザインによるセキュリティ」も重要である。

2 セキュリティ・バイ・デザインの進め方

セキュリティ・バイ・デザインの要諦は、①脅威モデリング、②ガイドライン、③ソフトウエア部品表（SBOM[注20]）の三つに集約される。①脅威モデリングとは、DXのビジネスやサービスの企画段階において、攻撃者の目線で脅威を洗い出し、セキュリティ対策を検討することである。②ガイドラインとは、セキュアなシステムを設計・開発するための考え方や方針を手引書として策定し、それを自社の技術者や開発者に周知・徹底することである。③ソフトウエア部品表とは、IoTを含めた最近のシステムには、数多くのオープンソースソフトウエア（OSS）や商用ソフトウエアが部品として組み込まれるため、システムの構築段階でそれらを一覧にしておき、本番リリース後も組み込まれたソフトウエア部品のバージョン情報や設定情報を維持管理しつつ、これを参照して新しい脆弱性や攻撃に対応するためのものである。

これらのプロセスを人力だけに頼っていては、DXに求められるスピードや品質を満たせないため、ツールなどを活用して極力自動

図4　セキュリティ・バイ・デザインの進め方



化し、正確かつ効率的に実践する必要がある。この一連の流れを、図4に示す。

(1) 脅威モデリング

脅威モデリングにはいくつかの手法があるが、本稿では一番有名なマイクロソフトの開発した「STRIDE」を紹介する。STRIDEとは、表1に示すように、攻撃者の脅威（手口）を六つの英単語で表し、その頭文字を取ったものである。

STRIDEによる脅威モデリングを具体例も踏まえて説明する。たとえば、キャッシュレス決済のサービスを企画したとする。キャッシュレス決済においては、店頭でQRコードなどを提示するスマートフォンアプリと、それと通信するキャッシュレス決済事業者のWebサーバーが必要となる。通常、キャッシュレス決済を利用する前には、自らの銀行口座から引き落とした現金と引き換えに、相当額の電子マネーをチャージする必要がある。したがって、電子マネーのチャージを例に取ると、図5の上部に示すようなデータフローとなる。まずは、あらゆるユースケースで想定され得るデータフロー図を描くことが、脅威モデリングの第一歩となる。

次に、各データフローにおいて、前述したSTRIDEの六つの脅威に照らして、具体的にどのような脅威があり得るかを検討する。たとえば、前述したキャッシュレス決済の事案はいずれも認証の部分、すなわち「S：なりすまし」の脅威が顕在化して金銭被害につながった。特に、コンビニエンスストアの事案の際に、各種報道で「二段階認証」「二要素認証」という専門用語が連呼され、IDとパスワードだけに依存しない認証方式の重要性が認識されるようになった。そこで、自社の開発範囲である、スマートフォンアプリとWebサーバーの間には二要素認証を実装したが、他社である銀行の決済システムの認証部分までは考慮が及ばず、金銭被害を受けるに至ったのが、携帯電話会社の事案である。図5の中央に示したように、銀行の決済シス

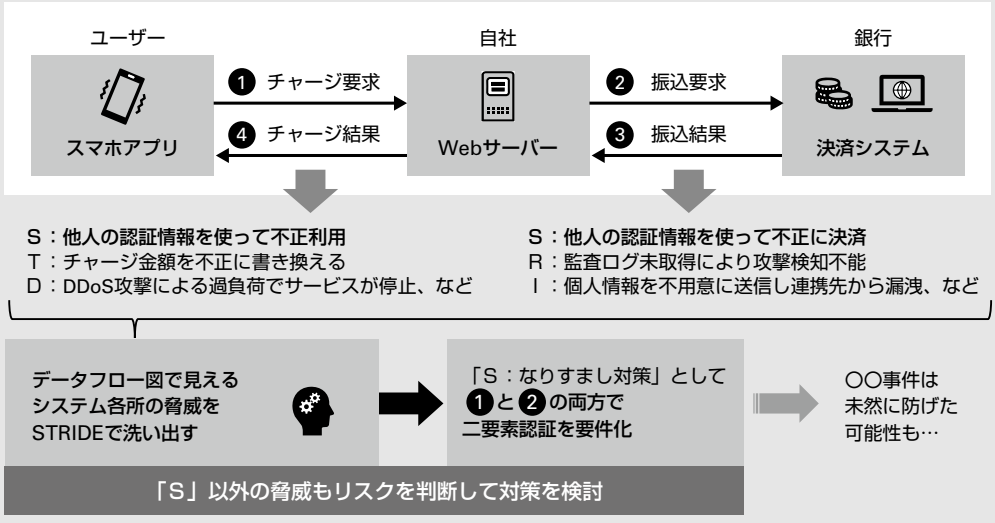
表1 「STRIDE」で表される六つの脅威

脅威	日本語	説明
Spoofing	なりすまし	正規ユーザーの認証情報（ID／パスワードなど）を不正に取得して、本人になりすます
Tampering	改竄	データベースに格納されたデータや、ネットワーク上を流れるデータを不正に書き換える
Repudiation	否認	利用者が実行した操作を、後から「やった覚えはない」と否定する
Information Disclosure	情報漏洩	本来アクセスが許可されない人に情報が閲覧可能となる
Denial of Service	サービス不能	サーバーの処理能力を超える大量のデータを送信し、ほかの正規のユーザーが利用できなくなるなど
Elevation of privilege	特権昇格	管理者に与えられる特権が不正に取得され、本来許可されない操作が実行される

テムとの間にも、「S：なりすまし」のリスクが存在することが脅威モデリングの結果判明するため、この区間も二要素認証を要件とするのが正解だったといえる。現に当該事案では、金銭被害の発覚後に二要素認証を採用する銀行との接続のみを許可し、口座番号と暗証番号だけで引き落としが可能な銀行との接続は解除された。

図5の中央に示すように、「S：なりすまし」以外の脅威ももちろん存在する。それらに関しても、脅威が顕在化する確率と発生し得る被害の大きさを勘案の上で、どのようなセキュリティ対策を実装すべきかを検討する。この際、事業部門とIT部門が共同で検討することが望ましい。万が一、脅威が顕在化した場合のビジネス上の影響と、それを回避するためのセキュリティ対策のコストを比較衡量した上で、不測の事態の際にも説明責任を果たし得る判断をすることが重要となる。脅威モデリングの最大の効用は、ビジネ

図5 脅威モデリングの例



スやサービスの企画段階で事業部門とIT部門がセキュリティのリスクや対策を議論するための材料を与えてくれることである。

脅威モデリングにおいては、データフローの作図やSTRIDEの脅威と対策の洗い出しを支援する無償のツール（英語）が存在する[注21]。このツールのアウトプットを、事業部門にも分かりやすい言葉に翻訳し、検討に活用してもらいたい。

(2) ガイドライン

2000年代後半に、金融商品取引法（J-SOX法）が成立し、上場企業においてITの調達・構築・運用にかかわる内部統制が整備されたが、その際にセキュリティ関連のガイドラインを策定した企業も多いであろう。したがって、セキュリティガイドラインのベースを既に持っている企業も多いと思われるが、その内容が最新のITやデジタル技術に即したものになっているか、自社の技術者や開発者（委託先を含む）が正しく理解して実装できる適切な詳細度の記述になっているかは、注意する必要がある。

たとえば前述したように、最近ではAWSやAzureといったパブリッククラウドを活用してシステムを構築するケースが増えているが、パブリッククラウドにおいてセキュリティ上注意すべき設定項目などを具体的にガイドラインで規定し、そのとおりに技術者が設定したかを確認する必要がある。Webアプリケーション開発やスマートフォンアプリ開発でも、それぞれセキュリティ上注意すべき点は多い。

その一方で、あまりにガイドラインの記述が詳細になり過ぎると、使用製品や開発言語のバリエーションが増えれば増えるほど膨大な数と量のガイドラインが必要となる。さらに、製品のバージョンアップに追随してガイドラインも更新する必要があるなど、維持管理の手間もかかる。したがって、技術者や開発者の解釈が揺るがない程度の適切な詳細度を保ちつつ、使用製品や開発言語に依存し過ぎない記述レベルとすることが重要となる。各企業でそのようなガイドラインを一から作成するのは現実的ではなく、各種業界団体や標準化団体から出ているガイドラインを参考にしつつ、適宜策定・更新していくのが望ましい。

また、繰り返しになるが、ガイドラインを策定して満足するだけでなく、自社の技術者や開発者への周知・徹底と、ガイドラインどおりにシステムが設計・実装されたかの確認が非常に重要となる。この確認にも、ソースコード診断や脆弱性診断などの各種ツールを活用できる。

(3) ソフトウエア部品表（SBOM）

10年以上前は、OSSで危険度の高い脆弱性が公表されてから、実際にその脆弱性を悪用した攻撃が来るまで、2～3日程度のタイムラグがあった。その間に、本番システムの大量のサーバー群に一台ずつログインして、当該OSSの利用有無や脆弱性に該当するバージョンかどうかなどを調査し、パッチ適用や設定変更での回避などの緊急対策を行っても何とか間に合っていた。

しかし最近では、危険度の高い脆弱性が公表されてから、2～3時間以内に攻撃が観測される場合もある。日本時間の休日や深夜帯に脆弱性が公表されることも多く、いちいち

実機で調査している余裕はない。特に、IoT機器の場合、出荷してしまうと手元に実機がないので調査のしようがない。したがって、IoT機器を含むシステムの開発・構築時に、システムに組み込まれたソフトウエアのバージョン情報や設定情報などをソフトウエア部品表として作成しておき、リリース（出荷）後も更新していく必要がある。新たな脆弱性や攻撃が報告されたタイミングでソフトウエア部品表を参照することで、自社システムへの影響を迅速に判断することができる。

システムの規模が大きくなるほど、組み込まれるソフトウエアの数は膨大となる。管理すべき項目は、バージョン番号や各種設定情報など多岐にわたるため、これをExcelなどのワークシートを使って手作業で正確に維持管理するのはほぼ不可能である。ソフトウエア部品表に関しても、その生成や検索・更新、公表されている脆弱性の該当状況の把握のために、ソフトウエア構成解析ツールが活用できる。

(4) ツールを活用した自動化とシステム開発プロセスへの組み込み

ここまで述べてきたように、①脅威モデリング、②ガイドライン（に沿った設計・開発）、③ソフトウエア部品表（の作成と維持管理）にかかわる、ほぼすべてのプロセスを支援または自動化し、正確かつ効率的に実践するツールが存在する。図6に、個別のプロセスに対応したツール群を示す。

これらを、開発・テスト環境や本番環境に組み込むことにより、現場の技術者や開発者にそれほど負荷をかけず、開発のスピードを必要以上に落とすことなく、セキュリティを着実に組み込むことが可能となる。

3 ゼロトラストとの関連性

従来のセキュリティ・モデルは、社内を「信頼できるもの」、社外（インターネット）を「信頼できないもの」として区別し、その境界にセキュリティ対策を実装する境界型モデルであった。それに対し、クラウドやモバイルの技術が進化する中、コロナ禍でテレワ

図6　セキュリティ・バイ・デザインを支援・自動化するツール群

ークを余儀なくされ、前述したセキュリティ事件・事故の多発や、上記の境界に通信が集中することによる利便性の低下が大きな問題となっている。そこで今、脚光を浴びているのがゼロトラストモデルである。メールやWeb会議など、社外クラウドの業務利用や社外である自宅からの業務が増えている現状に照らすと、もはや社内と社外の区別に意味はなく、境界だけではセキュリティを守れない。したがって、社内・社外の別を問わず、通信相手を「決して信頼せず（＝ゼロトラスト）、常に検証せよ」とする考え方である。

一見、簡単なように思えるが、これを正しく実装・展開するのは非常に難しい。何故なら、従来の境界型モデルであれば、境界の内側に多数存在する社内のサーバーや端末で、セキュリティ対策をそこまで意識しなくてもよかったが、ゼロトラストモデルではその境界が消滅するため、社内外を問わず企業の管理下にあるサーバー（クラウド上を含む）や端末自身で、セキュリティ対策を実装する必要が出てきたためである。

本来であれば、社内であってもサーバーや端末の間でどのようなデータが流れ、どのような脅威が存在するかを洗い出した上で、セキュリティ対策を検討する脅威モデリングが必要となるはずである。少なくとも、新たにDXのビジネスやサービスを企画・設計し、サーバーや端末上で稼働するアプリケーションを開発する「ビジネスIT」においてゼロトラストを正しく実装するには、セキュリティ・バイ・デザインが必要なのである。一方で、財務会計などの定型的なバックオフィス業務やメールなどのOA業務をつかさどる「コーポレートIT」においては、主要なデータの流れには一定のパターンがあり、脅威と対策も明確であるため、市場にある製品やサービスを導入・活用することでゼロトラストの理想に近付けることができる。

ただし、セキュリティ・バイ・デザインやゼロトラストを取り入れても、リリース後の統合的な運用監視や新たな脆弱性と攻撃への迅速な対応が、相変わらず重要であることは強調しておきたい。

V 経営として取り組むセキュリティ・バイ・デザイン

セキュリティ・バイ・デザインを実践する、欧米の事業会社や公的機関10社以上のCISO[注22]にインタビューを行ったところ、前述したような具体的な実践例だけでなく、経営レベルでもいくつか有益な示唆が得られたため、ここで紹介して本稿の締めくくりとしたい。

1 セキュリティ・バイ・デザインの効用

DXのビジネスやサービスの企画段階で定めたセキュリティ仕様に不備がある場合、リリース直前の脆弱性診断では検出できない可能性がある。たとえば、前述のキャッシュレス決済サービスの事案において、IDとパスワードのみで任意のスマートフォンに専用アプリをインストールして利用できることが「仕様」だった場合、リリース直前の脆弱性診断では問題点として指摘されなかったとしても不思議ではない。本来、脆弱性診断とはシステムの実装面での不備を検出するのが目的であり、仕様そのものは前提と見なされる

ためである。脆弱性診断では検出されない可能性のある、企画段階でのセキュリティ仕様の不備や設計段階での考慮漏れなどを防ぐために、脅威モデリングやガイドラインおよびそれらの実践を支援するツールが必要なのである。

また、自動車や電化製品などにおいても、図4の上部に示したような企画から設計、開発という流れに沿って製造される。この場合、上流工程（左側）で混入した不具合を下流工程（右側）で検出して改修しようとすると、手戻りが発生し、必要以上の工数（コスト）がかかる。したがって、上流工程で品質を高める取り組みを行うことにより最終的な製品の品質や安全性を高めると同時に、工程全体でのコストを抑える「シフトレフト」という考え方があるが、セキュリティ・バイ・デザインも全く同じ発想である。セキュリティに加えて、品質やプライバシーなどの向上にも上流工程から積極的に取り組むことで、結果的にかかるコストを抑え、広義の品質として顧客や投資家に訴求できる。

2 セキュリティ専門人材の獲得と育成

セキュリティ・バイ・デザインに取り組むに当たって、システム開発部門やIT部門にセキュリティの専門家を中途採用して丸ごと任せてしまえばよいと考える人もいるだろう。しかし、ほとんどのCISOが口をそろえて、欧米でもセキュリティ専門家は希少であり、中途での採用は非常に難しいというのである。その理由としては、そもそも市場からの需要に対して絶対数が不足している点、年俸が高騰しており事業会社として提示できる待遇では採用が難しい点、また彼らは純粋にセキュリティ課題やサイバー攻撃への対応を「知的な楽しみ」と捉え、魅力的な題材を提供し続けるのが難しい事業会社では定着してくれない点を挙げていた。

それを踏まえ、まずは自社IT部門の技術者や開発者が、自分の担当分野（ネットワークやWebアプリケーション開発など）におけるガイドラインを正しく理解し、実践するためのセキュリティ教育に注力するとのことであった。そして、担当分野の変更や拡大に伴って、より広範なセキュリティ知識を身につけた人材や、セキュリティに興味を持って技術習得の意欲が高まった人材を、専門性を要するセキュリティ部門に配置転換する。セキュリティ部門には最初からセキュリティの専門家はいないため、適宜、外部の専門家を活用するとのことであった。

3 CISOおよびセキュリティ組織はCIOとIT組織から独立性を保つ

DXの流れが加速する中で、CIO[注23]やIT部門（CDO[注24]とデジタル部門と読み替えてもよい）には、最新のITやデジタル技術をシステムとして実装し、いち早く市場に投入することが求められる。その一方で、CISOやセキュリティ部門には、セキュリティ侵害を防ぎ、それに投入するコストを最適化することが求められており、両者の目的には相反がある。したがって、CISO以下のセキュリティ部門は、CIO以下のIT部門とは分離し独立性を保つべきというのが、大半のCISOの主張であった。

これは、IT部門の人員にセキュリティ関連の知識や業務が不要ということではない。

前述したように、セキュリティ・バイ・デザインにおいては、IT部門の人員がガイドラインの内容を正しく理解して実践することが求められる。また、システムの根幹をなすサーバーやネットワーク機器などの脆弱性対応（パッチ適用など）も、IT部門が担当した方が安全かつ効率的である。一方で、セキュリティ部門が担当するのは最新のITやデジタル技術に対応した新しいガイドラインの策定・更新や、新しい脆弱性が発見された際のソフトウエア部品表を参照しながらの対応判断と指揮命令などである。

確かに、CISOの地位が高く、専門性のあるセキュリティ人材を一定数確保している欧米の事業会社では、CIO以下のIT部門とCISO以下のセキュリティ部門を明確に分離独立させて、牽制を図りつつ、相互協力しながら、DXの推進と日々のシステム運用を両立できるのであろう。しかし、ITやセキュリティに深い知見を持つ役員級の人材を二人以上抱える日本の事業会社が少ないのも事実である。外部招聘などにより専任のCISOを任命しても、セキュリティ部門に一定の専門性を有する人員を配置できない場合、本来の分離独立の趣旨とは乖離してしまう懸念がある。たとえば、セキュリティ確保を「錦の御旗」「人質」として、セキュリティ部門がDX推進の抵抗勢力となってしまう場合もある。

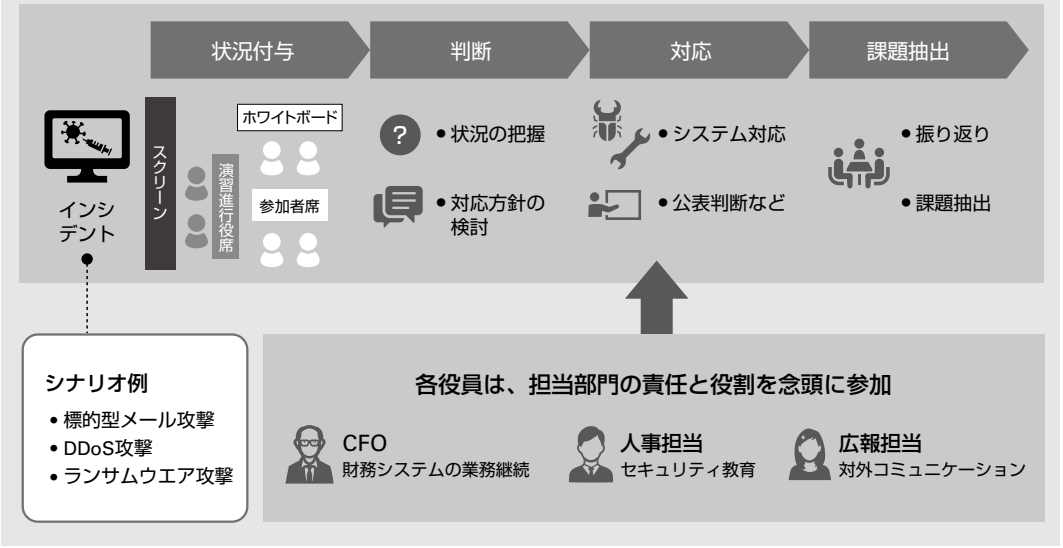
そこで、セキュリティ部門の分離独立を進めるには、前述したようにIT部門の技術者や開発者にセキュリティ教育を施し、一定のスキルが身についた人材をセキュリティ部門に配置転換するなどして、技術的な知見を有するセキュリティ人材を育成することが先決であろう。それまでは、CIOがCISOを兼務し、IT部門の中にセキュリティ機能を内包する形でもやむを得ないのかもしれないが、両者の目的や役割には相反するところがあることは認識しておきたい。セキュリティ予算がIT予算の一部となり、IT予算不足によって必要なセキュリティ施策が実行できないという事態だけは避けなければならない。

4　役員層を巻き込んだサイバー攻撃対策訓練で、不測時の事業継続をデザインする

最後に、セキュリティ・バイ・デザインの考え方は、これから開発する新規システムには適用しやすいが、そのような考えなしに開発された既存システムも多数存在するだろう。経済産業省のサイバーセキュリティ経営ガイドラインやコーポレートガバナンスコードは、経営層がサイバーセキュリティに積極的に関与し、その実効性を評価・公表することを求めている。まずは、自社の既存システムにおけるセキュリティ対策状況や改善計画について、取締役会や経営会議などで定期的に議論することが重要である。しかし、昨今のサイバー攻撃の脅威の高まりを踏まえ、ここであえてサイバー攻撃の被害に遭った場合を想定し、経営層も巻き込んだ「サイバー攻撃対策訓練」の実施を提案したい。

この訓練の実施に際しては、IT部門やセキュリティ部門だけでなく、事業部門やほかの本社部門とその担当役員も巻き込んだ訓練とすることが望ましい。たとえば、「標的型メール攻撃を受けて、社員が添付ファイルを開いてマルウエアに感染した」「ECサイトがDDoS攻撃を受けて、商品の注文が受けられなくなった」「ランサムウエア攻撃を受け

図7　サイバー攻撃対策訓練実施の流れ



て、財務会計システムが使用不能になった」などのシナリオが考えられる。サイバー攻撃対策訓練実施の流れを図7に示す。

ここで注意したいのは、事前にシナリオを練り込んで、関係各所が問題なく対応できるように準備万端を整え、「問題ありませんでした」と予定調和で終わる訓練に意味はないということである。もちろん、訓練とは知らずに過剰反応して実際の業務に支障を来すことは避けたいのと、役員を含む参加者の予定を調整するために事前の周知や情報共有は必要である。しかし、訓練本来の目的は、サイバー攻撃を受けた場合の準備不足を洗い出し、可能な範囲でセキュリティ対策の強化や、代替手段による事業継続の方策を探ることである。

たとえば、役職員向けに疑似的な攻撃メールを送信し、マルウエアを擬した添付ファイルを開いた社員を特定できる「標的型攻撃メール訓練」を行う企業も多いだろう。この訓練は、添付ファイルを開いた社員を罰することではなく、本人の気付きを促しつつ、人事（人材開発）担当部門にセキュリティ教育の浸透度や改善点を把握してもらうのが第一の目的である。

2021年には、実際にランサムウエア攻撃を受けて財務会計システムが使用不能となり、決算発表の延期を余儀なくされた企業もあった。バックアップを準備しておいても、緊急時に期待どおり復旧・稼働できるかは別の問題である。訓練を機に、実際にバックアップへの切り替えを実施して正しく業務継続できるかの確認や、バックアップが正しく動作しなかった場合の対応方法を検討しておくのは、非常に有意義である。

セキュリティ侵害に遭った場合の公表基準や、公表する際の記者会見などを担当する役員の選定、記者会見のリハーサルなど、事前の検討・準備が望ましい事項もある。サイバー攻撃に関しては、第一義的に攻撃者が悪いのであって、必要以上に被害者が責められる日本の風潮には疑問を禁じ得ない。だからこ

そ、本稿で紹介したセキュリティ・バイ・デザインを取り入れつつ、不測時にも対外的な説明責任を果たせるセキュリティ対策と態勢を整え、サイバー攻撃を受けても被害を最小限に食い止めていただけることを願ってやまない。

注

1 主にPCやサーバー上のデータを暗号化することで、システムを利用不能とし「復旧してほしければ身代金（ランサム）を払え」と脅迫するサイバー攻撃
2 JPCERTコーディネーションセンター（JPCERT/CC）は、インターネットを介して発生する侵入やサービス妨害といったセキュリティインシデントについて、日本国内に関する報告の受付、対応の支援、発生状況の把握、手口の分析、再発防止のための対策の検討や助言などを、技術的な立場から行う機関
3 Virtual Private Network（仮想専用線）の略。暗号化を行うことでインターネットなどのオープンなネットワーク上に盗聴されない安全な通信路をつくり出すこと
4 Social Networking Serviceの略。Webやチャットなどによるインターネット上のコミュニティサイト
5 Distributed Denial of Servicesの略。数万台規模の分散した機器から大量の通信を浴びせかけることで、通常のサービス提供を阻害する攻撃
6 Application Programing Interfaceの略。プログラムの機能を外部に公開するためのインタフェース
7 Decentralized Financeの略
8 https://www.nikkei.com/article/DGXZQOGN090C80Z00C21A2000000/
9 https://www.huffingtonpost.jp/kazuhiro-taira/russia-america_a_23482597/
10 https://jp.reuters.com/article/usa-cyber-china-charges-idJPKBN2EP1GB
11 https://www.jiia.or.jp/research-report/russia-fy2021-01.html
12 https://internet.watch.impress.co.jp/docs/column/dlis/1331673.html
13 https://www.itmedia.co.jp/news/articles/2106/10/news112.html
14 https://xtech.nikkei.com/atcl/nxt/column/18/00676/021700072/
15 Programmable Logic Controllerの略。主に製造業の装置などの制御に使用され、入力機器からの信号を取り込み、プログラムに従ってさまざまな処理を行い、出力機器を制御する装置
16 Electronic Data Interchangeの略。ネットワーク経由で標準的な書式に統一された発注書、納品書、請求書などのビジネス文書を電子的に交換すること
17 https://www.meti.go.jp/policy/netsecurity/mng_guide.html
18 https://xtech.nikkei.com/atcl/nxt/column/18/00001/06507/
19 https://www.nri-secure.co.jp/service/solution/secure-sketch
20 Software Bill of Materialsの略
21 https://docs.microsoft.com/ja-jp/azure/security/develop/threat-modeling-tool
22 Chief Information Security Officerの略。最高情報セキュリティ責任者
23 Chief Information Officerの略。最高情報責任者
24 Chief Digital Officerの略。最高デジタル責任者

著者

小田島 潤（おだしまじゅん）
野村総合研究所（NRI）執行役員、システムコンサルティング事業本部副本部長
専門は情報セキュリティおよびその周辺領域