トピックス

デジタル化時代のセキュリティ基盤
―再考を要するサイバーセキュリティ対策の在り方―

デジタル化が進むにつれ、サイバー攻撃の手口がますます巧妙化するなど、情報システムに対する脅威は増し続けている。特にデジタルビジネスを進めようとする企業にとって、対策の不備は致命傷になりかねない。本稿では、デジタル化時代に対応したサイバーセキュリティ対策の在り方を再考するために必要な、いくつかの論点を提示する。

NRIセキュアテクノロジーズ コンサルティング事業本部
サイバーコンサルティング部 上級セキュリティコンサルタント
石井 晋也（いしい しんや）
専門はサイバーセキュリティのアーキテクチャー構想立案・計画策定支援

増大し続けるサイバー攻撃の脅威

セキュリティに関する事件・事故のニュースは後を絶たず、大規模な個人情報漏えいももはや珍しい話ではなくなった。企業にとって、そのような事件・事故はビジネスに直接の損害を与えるため、セキュリティ対策は経営課題としての重要度を増し続けている。

一方で、マルウェアなどに感染させることを狙った標的型攻撃や、多数の機器から大量の接続要求を送出してサービスを妨害するDDoS攻撃、継続的な接続要求でサービスを妨害するAPDoS攻撃など、いわゆるサイバー攻撃の手法は巧妙化の度合いをますます高めている。また、新しい手口が次々に開発されるだけでなく、攻撃は国境を越え、攻撃ツールは闇市場で簡単に手に入り、ボットネット（乗っ取られたコンピュータのネットワーク）は攻撃者の特定を困難にする。自社で対策をしていても、他社のサービスでID・パスワードが盗まれれば、それを使った攻撃にさらされてしまう。

防御者として受け身の立場にある企業は、常に攻撃者に先を越される上に、サイバーセキュリティ対策の難易度はますます上がり、想定外のコスト負担を強いられたりする。しかし、対策が追い付かなければ、デジタル化による社会生活の高度化の取り組みは頓挫しかねない。

例えば、IoT（Internet of Things。さまざまなセンサーや機器がインターネットに接続された状態またはその仕組み）や自動運転などを考えたとき、機器の乗っ取りや、攻撃者による機械学習の悪用などへの対策の不備が生命に関わる事故に発展する危険性があることは容易に想像できる。攻撃への耐性が不十分な機器を使ったことで事故が起きれば、その企業が市場から退場を迫られたり、業界を挙げたデジタル化の取り組みが否定されたりしかねないのである。

とはいえ、サイバーセキュリティ対策のコストは増大するばかりである。企業としての経済合理性を超えるコストを要求されれば、不本意ながら何らかの妥協点を見いださなければならなくなる。例えば、対策のコストが許容範囲を超える一部のリスクをあえて受け

入れること、対策を十分に取れないサービスをあきらめることなどである。

デジタル化時代のセキュリティ

筆者は、サイバーセキュリティ対策のレベルはまだまだ向上させる余地があり、それには従来とは異なるアプローチが必要だと考えている。ただし、サイバーセキュリティ対策を実装するに際しては、標準的に用いられているガイドラインに沿って行うのが定石であることは変わらない。

そのようなガイドラインとしてよく利用されているものの1つに、米国国立標準技術研究所（NIST）による「重要インフラのサイバーセキュリティを強化するフレームワーク（CSF）」がある。そこでは、セキュリティ対策として求められる機能を、特定・防御・検知・対応・復旧といった一連の流れに則して定義し、それぞれの機能を支えるための組織的管理プロセス・技術的対策を挙げている。

こうした基本的な対策に加えて、デジタル化時代に即したセキュリティ対策を検討するに当たっては、以下の3つのポイントも考慮しなければならない。

①“信頼のよりどころ”の変化

これまでのセキュリティ対策の原則は、インターネット、社内ネットワーク、その中間のネットワークといったようにネットワークをゾーニングし、境界ごとにファイアウオールや境界防御型GW（ゲートウェイ）を設置し、外部・内部の双方向での不正通信を監視・防御するものであった。これは、信頼した相手とそうではない相手をネットワークの境界で分離するという考え方である。

しかし昨今では、マルチクラウドやモバイル・IoT活用、API連携が進んだことで、内と外、サイバー空間と実体空間の境界は曖昧となり、「信頼された相手を境界内に囲う」という“信頼のよりどころ”が通用しなくなってきた。そのため、いつ、どのような場所からアクセスがあっても、相互に認証・認可してセキュアな通信を確立し、継続的にアクセスリスクを制御する「ゼロトラストアーキテクチャー」という設計思想が注目されている。

米国のGoogle社の取り組みはそうした代表例の1つである。同社は、VPNのような特権ネットワークを排除し、社内システムの90％以上をインターネットからアクセス可能にしているという。これは、ユーザーと機器に対するアプリケーションレベルのアクセスコントロールと、高度かつリアルタイムでの不正アクセス解析があって初めて成り立つ極端な例ではあるが、グローバル企業が目指すべき方向性の1つといえるだろう。

②3種類の対策の再設計

上記のような環境の変化に合わせて、境界防御型、統合監視型、ID&アクセス制御型という3種類の対策の役割をあらためて見直すとともに、それらを相互に連携させることも求められている。

境界防御型セキュリティとは、ファイアウオール、IDS（侵入検知システム）やIPS（侵入防止システム）、DDoS対策、WAF（Webアプリケーションファイアウオール）、APIファイアウオール、アンチウイルスゲートウェイのように、侵入や情報資産の持ち出し

を防ぐことを目的としたセキュリティ対策群である。昨今では、Webアプリケーションサーバーにエージェントソフトウェアをインストールする方式のWAF製品や、認証済み端末からの通信要求のみ動的に通過を許可するSDP（Software Defined Perimeter）、攻撃者が侵入できるエリアを隔離しコンテンツを無害化する技術が注目を集めている。これらの新技術の評価と併せて、従来の対策の有効性もあらためて確認・評価する必要がある。

統合監視型セキュリティには、ネットワークに接続された端末機器（エンドポイント）でのマルウェア感染の検知と隔離・駆除、振る舞い可視化を行うEDR（Endpoint Detection and Response）、ユーザーと利用システムの挙動を統合的に分析するUEBA（User Entity Behavior Analytics）、各種のログデータを統合的に収集・分析して脅威を検知するSIEM（Security Information and Event Management）などがある。これらは、攻撃者の侵入の兆候、侵入後の活動や攻撃の予兆を捉えることで動きを封じ込めるためのセキュリティ対策群である。

サイバー攻撃は常に攻撃者が防御者に先行するものであり、また最近では攻撃の巧妙化により、ネットワークの境界で侵入を防ぐことが難しくなっている。そのため、侵入後の攻撃の予兆や挙動を可能な限り早期に捉える対策の意義は極めて大きい。統合監視型セキュリティは、今後、多面的な分析手法や人工知能（AI）技術の活用により、デジタル化時代においても中核的な分野になると考えられる。

ID&アクセス制御型セキュリティとは、アクセス元のIDと、そのIDの同一性を保証する認証（ログイン後の継続的保証を含む）、さらにそのIDに許可されたアクセス権限の検証を行うことで識別・認可を行うセキュリティ対策群である。アクセス元やアクセス先は、物でもサービスでもよい。具体的な対策としては、ユーザー認証・認可、クライアント認証・認可、サーバー認証・認可、メッセージ認証・署名、認証付き暗号など（前提となるハッシュ関数、暗号化方式を含む）がある。

現状では、ID&アクセス制御型セキュリティが不十分なことが少なくない。例えば、マルウェアをサーバーに侵入させて顧客データベースに不正なアクセスを行う攻撃があったとき、高度なマルウェア監視をする以前に、データベースへのアクセス権限管理や、メッセージ認証対策や通信元システムのクライアント認証を実施していれば、高い確率でリスクを避けられた可能性がある。このように、IDとアクセス制御を少しだけでも向上させることの有効性は計り知れない。

ID&アクセス制御型セキュリティを、境界防御型、統合監視型と連携させることで、それらの防御能力は最大限に発揮されるようになり、段階的にオペレーションの自動化を図ることが可能になる。例えば、ID管理（IDコード体系・付与ルールなど）の設計が各システム全体で統一されていると、誰が、何から、どこに、どのような権限範囲で、どこを経由して、何をしているかを確実に把握することができ、全体としてセキュリティレベルが向上する。そのためには、各システムに個別に埋め込まれているID機能を分離して統合するか、一部のID機能だけを分離して連

携させることが必要だが、これらは後から実装できるものではなく、システムの設計段階からの十分な検討が必要である。そのため、システム更改の機会などに合わせて現実的な対策を適宜検討していくことが求められるだろう。それらの過程で、認証や署名、暗号化・復号の中核となる秘密鍵のセキュアな管理方式を設計することも忘れてはならない。

③組織機能の見直し

本来、セキュリティ対策は、システム設計・開発のプロセスに初めから組み込まれているのが理想である。設計・開発の段階から、運用まで見据えて脆弱性を取り除くことが、結果的に総合的なセキュリティ能力を高めることにつながるからである。一方で、設計・開発チームは魅力的なソフトウェアをできるだけ早く安く開発することを求められているために、セキュリティを組み込む作業は往々にして後回しになる。

しかし、増大し続ける脅威がこのような現状を許さなくなっており、組織機能を見直そうという動きも見られる。例えば、設計・開発チームに、脆弱性の特定やハッカーへの攻撃などを行うセキュリティチームのメンバーを参加させたり、プロジェクト全体に共通するセキュリティチームを編成したりすることなどである。このような対策はまだ試行錯誤の段階であり、今後もデジタル化時代に最適な組織とその機能については、さらなる活発な議論が続いていくであろう。

セキュリティ対策を投資と捉える

2017年11月に、筆者は、企業のデジタル化を支援する米国のソフトウェア会社、CA Technologies社がラスベガスで開催した「CA World '17」に参加した。

あるパネルディスカッションで、「セキュリティとイノベーションのバランスをどう考えるべきか」という質問があり、それに対する金融機関の担当者の答えは次のようなものだった。「"セキュリティファースト"である。イノベーションを果たしたとしても、情報漏えいを引き起こすことは許されない」

逆に言えば、"セキュリティファースト"とは、最新のセキュリティ技術と対策の限界を知ることで、ITをビジネスにどこまで活用していいのかを判断することである。適切なセキュリティ対策を前提にして、ビジネスとしてやっていい範囲を決めるというのは、極めて当たり前のことであろう。

セキュリティは、企業のデジタル化やビジネスIT（事業に直接的に貢献するためのIT）を支えるための"総力戦"であり、技術者に要求されるレベルも高い。デジタルビジネスとセキュリティの要求を相互に橋渡しできる人材の重要性は、今後、一層高まるであろう。こうした人材の問題も含めて、デジタル化に対応したセキュリティ対策の巧拙が、企業のデジタルビジネスの成功を左右する大きな要素になることは間違いないだろう。

最後に、デジタル化時代におけるリスク回避は社会全体の課題でもあるという点を付け加えておきたい。ビジネスの内容に応じた登録・免許制、罰則規定、税制面でのバックアップや、官民の一層の情報共有・連携なども、本質的なセキュリティのために大切であると筆者は考えている。 ■