03

セキュリティ

攻撃者より一歩先へ ～サイバー攻撃の最新動向と能動的防御戦略～

サイバー攻撃が巧妙化し、脆弱性侵害やサプライチェーン攻撃、AI悪用などの脅威が激化している。これまでの場当たり的な「漏水対策」から防御概念のアップデートが必要。受け身の防御ではなく、信頼できるビジネスを目指した強固なシステム基盤を整備した能動的な次世代防御対策が求められる。

続発する深刻なインシデント

これまでのサイバーセキュリティ対策は、インシデントや脆弱性に対し、ピンポイントな「漏水対策」が中心だった。しかし、この場当たり的な防御は、もはや現在の「圧倒的攻撃優位」の前では機能しない。守るべき資産の増大、非常に深刻なゼロディ攻撃[1)]を前に、従来の対策では防御網の一点突破を許し、企業価値そのものが致命的な打撃を受けている。防御の発想を根本から変え、網羅的・複層的に防御する強靭な対策を検討しなければ、現在の深刻なインシデントを防ぐことができない。

●多発する脆弱性侵害とゼロディの深刻化

資金力のある攻撃者や国家背景の攻撃者がSSL-VPNなどのネットワーク機器の脆弱性探索を高度化し、深刻なゼロディ攻撃が多発している。

●サプライチェーン攻撃の増加

海外子会社を起点に国内本社を狙う「Island Hopping[2)]」事例が日本国内でも確認されている。また、委託先・再委託先への侵害が重大インシデントにつながる事案が相次ぎ、膨大な数に上る委託先に対する評価・モニタリングが重要課題・業務負担となっている。

●個人を狙った金融関連・デジタル犯罪

生成AIによる攻撃、闇バイト、偽造身分証の活用が活発化。証券業界では、フィッシングで認証情報を盗み、口座を乗っ取る大規模なアカウントハッキングが発生し、相場操縦を目的とした新たな脅威となった。これを受け、金融庁や日証協は多要素認証の義務化等を柱とする監督指針・ガイドラインの改定案を公表した。金融機関は、厳格化した監督指針への対応負担も増加している。

●AIの悪用による脅威の増大

いま、サイバー攻撃の「AIティッピングポイント[3)]」に立っているという認識が必要である。生成AIが作成したフィッシングメールは、その巧妙さゆえに開封率が非常に高く、攻撃側のコストを大幅に低下させている。更に深刻なのは、AIが言語の壁をなくし、攻撃スピードを人間の数百～数万倍に高めた点である。AI悪用による脅威増大は、もはや未来の脅威ではなく、直近の脅威となった。

次世代サイバー防御のあり方

政府は能動的な防御（攻撃を未然に防ぎ、迅速に回復）を打ち出したが、金融機関もこれに呼応した防御方法の根本的な見直しが急務となっている。しかし、政府が提唱する能動的防御対策（通信情報取得、攻撃サーバ無効化等）を金融機関が個社自身で実施するのは事実上困難であり、金融機関として現実的な次世代防御対策を整備する必要がある。

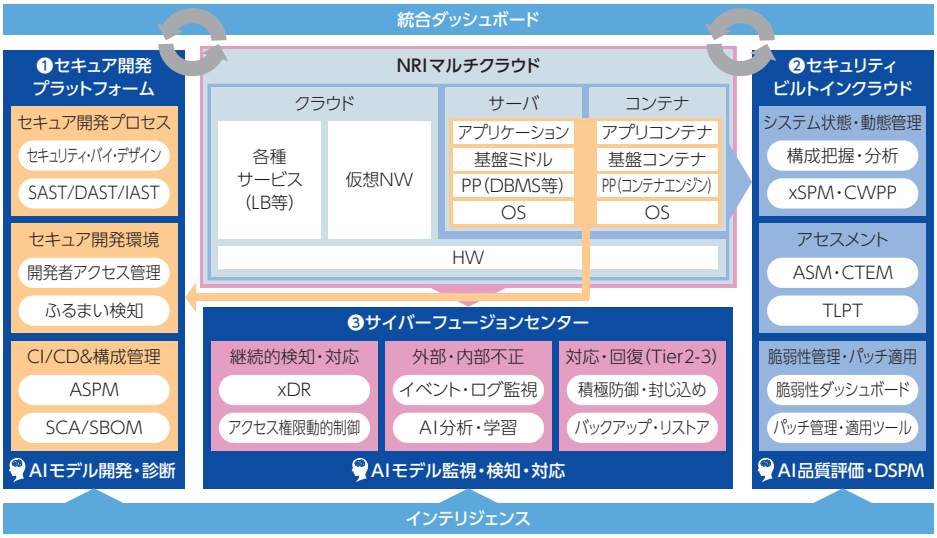
この防御の発想の核となるのは、受動的な「サイバーセキュリティ＝システムの安全」という概念を超えた「サイバーセキュリティ＝ビジネス全体の信頼（トラスト）」を目指すものでなければならない。NRIでは、このIT基盤へのアップデートを「デジタルトラスト基盤」と定義し、データ・システム・組織・ビジネスそのものへの信頼性を包括する対策を提唱している。

デジタルトラスト基盤を確立するには、セキュリティ業務プロセス全体を俯瞰したIT基盤とビジネスの連動強化が不可欠である。これは、ビジネス企画・システム構想段階からセキュリティ対策を組み込むことを意味する。

NOTE

1) システムの脆弱性が発見された当日（またはメーカーなどが対策を公開する前）に行われる、高深刻度の攻撃。
2) サプライチェーン攻撃の一種であり、海外子会社を起点として、国内本社を狙う攻撃。
3) AI悪用により脅威が急速に増大する転換点となっている状況。
4) Software Bill of Materials。ソフトウェアを構成するコンポーネント（部品）のリスト。Software Composition Analysis。ソフトウェア構成分析ツール。
5) Security Operations Center。サイバー攻撃の監視・分析・対応を行う専門組織。
6) Chief Information Security Officer。最高情報セキュリティ責任者。

図表　デジタルトラストを支える3つのIT基盤



（出所）野村総合研究所

デジタルトラストを支える3つの強靭化基盤

デジタルトラスト基盤は、戦略的な未然防止対策から迅速な回復サービスまでをトータルで提供する次の3つのIT基盤で構成される（図表）。

①セキュア開発プラットフォーム（SSDPF）

「セキュリティ・バイ・デザイン」思想を組み込み、ソフトウェア及びAI開発環境・工程に必須のセキュリティ対策を標準機能として実装。SBOM・SCA[4]等の統合により、コード品質とソフトウェア透明性を確保し、開発生産性と統制強化を両立する。

②セキュリティビルトインクラウド（SBC）

IT基盤とセキュリティ運用が一体化されたクラウド環境の構築。システム構成管理、脆弱性管理、パッチ適用などのセキュリティ機能をクラウド基盤と一体で提供し、常にIT基盤をセキュアな状態を維持する「IT基盤へのセキュリティ機能統合」を推進する。

③サイバーフュージョンセンター（CFC）

従来のSOC[5]のレベルをはるかに超えるインテリジェンス駆動型の脅威予測・防御・対応基盤。独自の脅威インテリジェンス分析やAI解析を用い、マルチAIエージェントが、経営判断支援からセキュリティ全般にわたる高度な意思決定と対処を支援する。

こうした3つの統合的なアプローチにより、組織全体のセキュリティにおける可視性・検証力の向上、およびセキュリティ投資判断の合理化を実現し、漏水対策の繰り返しではなく、継続的で効率的な対策を実現することができる。

金融機関の経営者、CISO[6]、サイバー担当者は、見えない敵との戦いに打ち勝つために、サイバー攻撃からシステムを守ることだけを考えるのではなく、「ビジネスを守るために何を準備すべきか」を考える時期に来ている。

Writer's Profile

森田 太士 Daiji Morita
セキュリティソリューション事業開発部
担当部長
専門はリスクマネジメント
focus@nri.co.jp