FERI INFORMATION

最近の「ハイエンド型サイバー攻撃」を考える

前編　情報流出に破壊リスクが加わる時代へ

西本　一也 ㈱デジタルアセットマーケッツ・代表取締役

国家によるサイバー攻撃の脅威

情報のデジタル化が進展する現代社会において、サイバー空間は陸・海・空・宇宙に続く「第 5 の戦場」として国際的な注目を集めている。この文脈での「サイバー攻撃」は、従来のランサムウェアやフィッシングといった犯罪的手口とは異なり、国家による戦略的かつ破壊的な行為が中心となる。政府機能や重要インフラへの攻撃、大学や研究機関からの先端技術の窃取など、地政学的リスクや有事に端を発する広域的かつ無差別な「ハイエンド型サイバー攻撃」が現実の脅威として顕在化している。

こうした脅威の高まりを受け、経済産業省所管の独立行政法人 情報処理推進機構（IPA）は、2025 年版「情報セキュリティ 10 大脅威」[1] において、「地政学的リスクに起因するサイバー攻撃」を新たに第 7 位に位置づけており、対応の必要性が認知されるようになってきた。

情報流出対策がもたらす破壊耐性の低下

近年のサイバー攻撃の多くは、個人情報の流出や、バックアップの無効化によるシステム復旧の妨害を通じて、情報を人質とした身代金要求を目的とするものであった。

日本においても一定の被害は確認されているものの、海外と比較すれば深刻な被害は相対的に少ないと評価されている。その背景には、以下のような要因が考えられる。

① 日本では大企業を中心に一定水準のセキュリティ対策が講じられていたこと。

② 依然としてメインフレーム（大型汎用機）による処理が多く、システムへの侵入を困難とする構造が残存していること。

③ 「身代金要求には応じない」という企業方針が広く徹底されており、攻撃者にとって費用対効果が低いため、他国を標的とする方が有利であったこと。

過去の事例では、攻撃者がシステム内に侵入したとしても、完全なシステム破壊に至ることは稀であった。そのため、日本国内では、海外に比して致命的被害の件数は少なく、サイバー攻撃に対する危機意識が相対的に低い状態が長期間にわたり続いていたと考えられる。

ただし、例外も存在する。たとえば、暗号資産交換業界においては、サイバー攻撃への警戒が非常に高い。これは、オープン型のシステムであることや、扱うデジタルアセットが一度盗まれれば保有アカウントが追跡できたとしてもアカウント保有者が誰なのかを突き止めることが困難であり、テロ資金等への使用に直結する危険性があるためである。

近年になり状況は急激に変化している。とりわけ、ロシアによるウクライナ侵攻以降、サイバ

ー攻撃の様相が大きく転換した。具体的には、情報の流出を目的とした従来型の攻撃に加え、システムを無条件で破壊する「ワイパーマルウェア」が確認されるようになり、攻撃の目的が「流出」から「破壊」へと拡大してきたことが挙げられる。日本国内における企業への攻撃でも、従来は一時的なバックアップ無効化にとどまっていたものが、近年ではバックアップそのものを破壊する事例が報告されている。

さらに注目すべきは、サイバー犯罪のビジネスモデルの変化である。従来の「身代金要求」型から、「攻撃代行」や「機密情報の転売」といった新たな収益手段への移行が進んでおり、もはや金銭を目的とするサイバー犯罪組織と、国家の支援を受けたサイバーアクターの区別が困難になりつつある。

このように、サイバー攻撃の脅威は、流出から破壊へ、また身代金要求から地政学的目的の実現へと変貌を遂げており、日本においても従来の「情報流出対策」だけでは不十分となってきている。今後は、破壊的攻撃への耐性、すなわち「サイバーレジリエンス」の強化が、あらゆる組織にとって不可欠な課題となるであろう。

個人情報については、日本では 2022 年に改正個人情報保護法が施行され、欧州の GDPR（EU 一般データ保護規則：General Data Protection Regulation）の要素を取り入れ、個人の権利拡充と企業の責務強化が図られた。これは情報の「流出」に対して徹底した対応を求める考え方となっている。個人情報の保護を徹底するがゆえに、暗号化や秘密分散・秘密計算などで個人情報を処理したとしても、法的には個人情報であることに変わりはない。これが制約となって、国外へのデータ退避を選択せざるを得ないような有事シナリオに対しても対応が困難になっているのが現状である。

つまり、現状は情報の「流出防止」が対策の中心であり、その結果、国外への分散保管が困難になって国内で集中管理されているため、そこを狙った破壊攻撃に対いて脆弱な状況になっているといえる。また、他の機密・秘密情報も最重要情報として個人情報と同様の対応が必要とされている。サイバー攻撃の目的が金銭から破壊へと変遷する状況下、「流出」と「破壊」への対応はトレードオフの関係にあるため、その関係を改善し、かつバランスのとり方を最適化することがデータ保全の喫緊の課題となっている。

情報流出耐性と破壊耐性の両立

世界的にサイバー攻撃の高度化および増加が進行するなか、各国では最新のサイバーセキュリティ対策に対する注目が高まり、その強化が急務とされている。日本においても官民の取り組みが進められているが[2、3]、導入されている対策ツールの大半は欧米諸国で開発されたものであり、国内で独自に開発されたものは限定的である。また、日本のサイバーセキュリティ対策の主軸は、「フロント防衛」（境界型防御）と「インシデント対応」に置かれており、これらは主としてシステム障害への対処という側面に重きを置いたものであると考えられる。

たとえば、世界最強のセキュリティ水準といわれる米国防総省ペンタゴンやマイクロソフトであっても、実際にシステムに侵入された事例が過去にあった。彼らが優秀たる所以は、その事実を客観的に評価し、サイバー攻撃を未然に 100％確実に防御することは困難であると定義づけ、

侵入されることを前提として、攻撃による被害から回復する能力を事前に備える「サイバーレジリエンス」という概念を構築したことにある。具体的な対処方法としては、単純な防衛対応のみではなく、「ゼロトラストアーキテクチャ」の徹底や「セキュリティストレージ」の導入などの点が日本よりも進んでいる。

特に注目すべきは、以下のようなハイエンド型サイバー攻撃に対する具体的な防御策である。ハイエンド型サイバー攻撃では、国家レベルまたはそれに準ずる高度な技術力と資源を持つ攻撃主体が、特定の重要対象に対して長期間にわたり、巧妙かつ執拗に仕掛けるサイバー攻撃が行われる。政府機関、防衛産業、インフラ企業などが代表的なターゲットになり、標的のネットワークに長期間潜伏し、監視・情報窃取・破壊活動を行うこともある。代表例を３つ挙げる。

① 内部者工作： 最も成功率が高く、検知が難しい攻撃手法。ただし、局所的な攻撃となる。

② ワイパー型マルウェア： ハッキング AI によってゼロデイ脆弱性を解析し、標的にワイパーウェアを感染させる新型攻撃。最近、実際に攻撃用 AI のコードが発見された。

③ EMP 攻撃（Electromagnetic Pulse Attack：電磁パルス攻撃）[4、5、6]： 成層圏での核爆発により、人体には害を及ぼさずに、電磁波によって広範囲に電子機器等を破壊する攻撃。広範囲にわたって同時に被害を及ぼす。日本国内のデータセンターには EMP 攻撃への対策がほとんどなく、他国に比較して特に脆弱とされている。

この①～③のいずれの攻撃にも対応することこそが、いわゆる「想定外の攻撃への対処力」であり、欧米諸国においては政府のみならず、民間企業の一部においても高い危機感をもって備えが進められている。ここで言う「想定外」とは、従来のシステム障害のように発生確率を前提とした対応を行うことが不可能なものであり、あらかじめ対策マニュアルを策定することが極めて困難な種類の攻撃である。

特に①および③は、現時点において有効な対処手段が事実上存在しないとされる。①に関しては、セキュリティ・クリアランスの対応が進んでいるが運用基準の策定や実施はこれからであり、特に民間企業への広範な実効性ある適用は容易ではない。③に関しては、その破壊力が核抑止力に匹敵するレベルであるとされており、具体的な威力が一部で公にされている点も注目すべきである。なお、メインフレーム（大型汎用機）は②の攻撃には比較的強いが、①および③への耐性は十分とは言い難い。また、②の攻撃に関する詳細は公開されていないが、これは防御側が手の内を明かすことにより、攻撃側に対策を講じられることを防ぐ意図があると考えられる。

ハイエンド型サイバー攻撃に対しては、既存のサイバー防衛手法では対応が困難であるという認識を持ち、早急に独自の対処体制を構築する必要がある。有事シナリオの想定は容易ではないが、海外ではこうした攻撃が今現在進行している地域が複数あり、自国では発生しないと想定できる根拠は何もない。海外事例を他山の石として、すぐにできることから対処することが有事リスクの増大している現状への対応になる。

日本特有の脆弱性と純国産セキュリティストレージの必要性

日本は世界的にも稀な長期安定国家であり、「有事」を前提とした政策が他国に比べ少ない。例えば、核シェルター、EMP 対策、セキュリティストレージといった物理的・デジタル的な防衛インフラが未整備である。

国内のデータセンターは、建築基準法や FISC（金融情報システムセンター）のガイドラインに基づく高度な耐震・電力対策がなされており、バックアップは 3 - 2 - 1 ルールが適用されるなど対応が図られている。これらの対策により、災害時等に最小時間でのサービス復旧を実現できる構造になっている。しかし、こうした構成を含む BCP（Business Continuity Plan、事業継続計画）は、あくまでも災害対応であってサイバー攻撃を想定しておらず、サイバー攻撃や有事リスクへの対応には限界がある。

さらに、東京・大阪に 85%以上のデータセンターが集中している点、EMP 攻撃への無防備、ゼロトラストの不在、暗号化・分散化の未整備といった点は、海外からは明確なリスクとして指摘されている。外資系企業が提供するクラウドサービスのセキュリティを信頼している企業も多いが、実際には国内法規制に従った「国内運用」が大半であり、データの海外退避はほとんどなされていない。また、鍵の管理をクラウド提供者に委ねているケースも多く、これは「金庫と鍵を同じ相手に預けている」という状況と同じようなものだといえる。クラウドは安価で性能が良いため軽い業務には適しているが、重要性の高い情報等を扱う場合は、クラウドのセキュリティを十分に理解して慎重に活用すべきである。

国内では、災害対応の BCP として短時間復旧を重視した設計が主流である。このもとでは、暗号強度を高めると処理時間が長くなるというジレンマを抱えることになる。1 日 1TB 以上の重要データを取り扱う大企業では、暗号処理だけで数日を要する可能性もある。このようなジレンマを回避するためにも、「データ保全とバックアップは異なる概念である」という認識へのシフトが求められる。重要なのは、「どのような事態が起きても、重要情報を確実に守り抜く」ことができるサイバーレジリエンスに焦点を当てた情報管理体制である。後編では、その具体的な対応策を考える。

（前編おわり）

[1] 独立行政法人 情報処理推進機構（IPA）、情報セキュリティ 10 大脅威 2025、2025 年 1 月 30 日
https://www.ipa.go.jp/security/10threats/10threats2025.html

[2] 内閣府、内閣官房 Web サイト「サイバー安全保障に関する取組」
https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo_torikumi/index.html

[3] 内閣サイバーセキュリティセンター（NISC）Web サイト
https://www.nisc.go.jp

[4] 一政祐行（防衛研究所）、「米ソの大気圏内核実験と高高度電磁パルス（HEMP）研究」、一般財団法人 安全保障貿易情報センター、CISTEC journal、No.173、2018.1

[5] NTT 宇宙環境エネルギー研究所、「電磁パルスとは？HEMP など電磁パルスによる被害の仕組み・原理と対策」、Beyond Our Planet、2022 年 2 月 21 日

[6] 日経クロステック、電磁パルス（EMP）攻撃の正体とは？
https://xtech.nikkei.com/dm/atcl/column/15/092500129/092600001