FERI INFORMATION

最近の「ハイエンド型サイバー攻撃」を考える

後編 日本版セキュリティストレージ構想とその実装技術

西本 一也 ㈱デジタルアセットマーケッツ・代表取締役

前編では、ハイエンド型サイバー攻撃の脅威や日本固有の脆弱性について解説した。後編では、そうした脅威への対応策として筆者らが有望と考えている手法を紹介する。

なお、本編は技術的な論点を含むため、最初に政策的なインプリケーションをまとめておく。現在のデータ保全の考え方では障害復旧だけでなく攻撃耐性も求められており、この考え方に即した「日本版セキュリティストレージ」が必要と考えている。そのための技術的な選択肢としてはデータ分散が有効である。ただし、導入や実運用には法規制が関係してくるため、関係者がハイエンド型サイバー攻撃におけるデータ破壊等のリスクへの正しい認識を持ち、極めて高度なセキュリティが保たれていることを条件としたうえでデータの国外バックアップなども認める議論が必要となる。本稿で紹介したような高度な技術は実装可能であり、その全体像を以下で紹介する。

データ保全はバックアップでは果たせない

一般的に「バックアップ」とは、データのコピーを別の場所に保存することで、障害や一部破損が発生した際に復旧を図るための仕組みである。しかし、バックアップはあくまで「障害への備え」であり、破壊や流出を伴うような意図的なサイバー攻撃に対しては限界がある。ハイエンド型サイバー攻撃のもとではバックアップも同時に破壊対象となる。

一方、「データ保全」は、どのような事象に対しても「確実に重要なデータを守り抜く」という概念であり、暗号化・分散化などの高度信頼技術がその中核にある。重要なのは、保全システムが破壊されないことを前提とした構造になっている点である。

日本では、処理効率を重視した集中型のバックアップ構造が主流となっており、「攻撃されることを前提としない」、もしくは「フロントで防御し、内部は処理性能を重視する」という設計思想に基づいたものが多い。内部に侵入された場合、バックアップでは防衛できない。バックアップも破壊されるのである。効率性の追求が耐攻撃性の軽視につながってきた側面がある。

欧米では、重要情報をデジタルアセットとして認識し、CISO を中心に保全体制を経営レベルで整備している。一方、日本では、ビッグデータや特許などの非財務資産が会計上の資産として反映されにくく、その価値が軽視されがちである。しかし実際には、こうした情報の

喪失が企業の存続を左右する場合も多い。特に研究機関の蓄積情報は盗難・転売により現金化される恐れもあり、最高強度のデータ保全が不可欠である。

世界標準となりつつあるセキュリティストレージ

海外では、こうした「データを守り抜く」という目的のために、サイバー攻撃への強靱な耐性を持つセキュリティストレージの導入が進んでいる。

日本では、「セキュリティは情報システム部門」、「ストレージはインフラ部門」といった縦割り構造が根強く、分野横断的な整合性が取れず、責任の所在も曖昧である。官民や中央・地方間でも担当が分断され、サイバーレジリエンスの概念が定着していない。さらに、海外製セキュリティ製品を導入しても、国内には中核機能を支えるデータの退避先（物理的シェルターや分散拠点）が乏しく、制度や商習慣など複合的な制約がセキュリティストレージ導入の障壁となっている。セキュリティストレージは、機密情報を扱う性質上、国家安全保障に直結し、多くの国で自国開発が原則とされている。国外技術への依存は安全保障上のリスクとされ、純国産が各国共通の前提となっている。

では、世界のセキュリティストレージは、どのような構造で設計されているのか。以下がその代表的な構成である。

① 流出させない仕組み（流出耐性）の確保

PQC（耐量子計算機暗号）を含む先進的な暗号技術を実装し、鍵管理を厳格に行うことで、情報の外部流出を防ぐ。ただし、鍵自体の窃盗や漏洩のリスクは完全には排除できず、信頼性の高い鍵管理体制を構築・維持することが難易度の高い課題となっている。

② 破壊されない仕組み（破壊耐性）の確保

重要なシステムやデータを物理的な破壊やサイバー攻撃から守るために、ネットワークから完全に分離する「エアギャップ構造」を採用したり、安全な物理的・論理的なシェルターへ退避させたり、複数の場所にコピーを分散（多重分散）させたりする対策を活用する。ただし、特に個人情報や機密性の高いデータに関しては、個人情報保護法や分野別の規制・ガイドラインによって、国外でのバックアップを含む国外へのデータ移転・保管に一定の制限や条件が課されているため、分散先が国内に限られやすい。

この①②を相互に補完し、統合的に運用することで、はじめてセキュリティストレージとしての性能が成立する。実装上は、①にゼロトラストアーキテクチャの考え方を適用し、②には独立環境へのデータ退避（シェルター型保全）を行うことが一般的だ。エアギャップ構造だけではマルウエア攻撃への対応にはなっても内部工作や EMP 攻撃（前編参照）へのソリューションとはならない。

繰り返しになるが、日本には②のシェルター構造が存在せず、海外で標準となっているセキュリティ技術の中核機能を規制等により実装できないという矛盾を抱えている。裏を返せ

ば、退避先の整備こそが、世界標準のセキュリティストレージ実現への鍵であり、「セキュリティインフラの主権化」に向けた核心である。

フィンテックから進化したデータ保全技術

「可用性を高める」のではなく「退避先を分散させる」という発想の切り替えが求められており、フィンテックから進化したデータ保全技術がその手がかりとなる。

性能とセキュリティという相反する課題を解決するためのアプローチとして、「分割分散」による「条件付き無意味化」という新しい手法が考えられる。分散型台帳技術の発達は、台帳の分散という攻撃耐性上の長所を備えている一方で、アプリケーション層には情報セキュリティ面で不十分なものが多く、資産管理などにリスク管理上の課題を抱えている。実際、暗号資産の流出事故は散発的に発生し続けている。そもそもパブリック型の台帳情報は誰からも可読であり、また、秘密鍵の管理は個人や暗号資産交換所に依存している。

暗号資産などの分散型台帳技術では、こうした可読性についてアカウントと所有者情報を分離することでプライバシーを保っている。これに対し、多くの中央集権型の台帳システムでは外部からクローズドにすることで「見えない・意図しないアクセスをさせない」ことを達成している。後者のような伝統的なシステムをハイエンド型サイバー攻撃への対応のため他国・他地域に分散配置する場合、接続点の増加や統一的なアクセス管理の困難さにより、かえって情報セキュリティの問題が高まる。

分割分散と条件付き無意味化により、こうした課題を克服することが可能となる。具体的には、伝統的台帳や分散型台帳のいずれであっても、情報を解釈不可能なように加工することで、他国に台帳を保有したとしても情報セキュリティが確保されるというアプローチをとる。この分割分散された情報を安全に管理するために、特別なブロックチェーン構造と高度な暗号処理が必要となるが、そうした技術実装はすでに可能であることを確認している（当該新技術をテーブルチェーン構造と呼称している、後述参照）。

分散型台帳技術の領域で生まれたこの新しいアプローチは、サイバーセキュリティ分野にも適用可能な汎用性を持つ。同技術を応用することにより、前編で紹介した日本が抱えるセキュリティ上の脆弱性に対応する「日本版セキュリティストレージ」としての展開が可能となる。

条件付き無意味化とゼロトラスト

個人情報保護法において、個人情報を非識別化する手法として匿名化や仮名化が挙げられているが、プライバシー強化技術（PETs：Privacy Enhancing Technologies）には、データの非識別化・加工技術以外にも様々な手法がある。暗号化計算技術やアクセス制御技術であり、前者の暗号化計算技術には、暗号化されたまま加算や乗算などの演算を行える準同型暗

号（Homomorphic Encryption）、複数の当事者がそれぞれのデータを秘匿したまま、共同で演算結果を得られる安全な秘密計算（Secure Multi-Party Computation）、自分がある情報を「知っている／正しい」と証明しながら、その内容自体は明かさないゼロ知識証明、情報を複数の断片に分割し、個別には意味を持たないが復元すれば元データが得られるという秘密分散などがある。後者のアクセス制御技術には、伝統的な認証・認可技術に加えて Verifiable Credentials などのプライバシー重視のデジタル証明技術や、Trusted Execution Environment（TEE）技術などがある。

ただし、PETs であっても権限者が単一であった場合、脆弱さが残存する。システムを操作・設定・管理する権限者が一人、または一組織しかいない場合、その権限者が悪意を持つ、あるいは誤った運用を行うと、セキュリティやプライバシーが確保できなくなる。以下で紹介する「条件付き無意味化」は、暗号化計算技術に属する新たな手法の一つであるが、多重化と組み合わせることで PETs が抱え込みやすい単一権限者の問題を回避している。

本来、「無意味化」とは一方向性で復元不可能な状態を指し、システムのテストなどで本番データをランダム合成により無意味な状態に加工する手法をいう。しかし、ある条件下でのみ復元可能な、いわば「条件付き無意味化」という技術に拡張すれば、ハイエンド型サイバー攻撃への対応と情報セキュリティを両立可能な新しい技術として応用可能領域が広がる。

秘密分散と無意味化は混同されることがあるので、両者の違いを明確にしておく。秘密分散は、ある機密情報を複数の断片に分割し、各断片単体では意味を持たないようにして、所定の数の断片が揃うと元の情報を復元できる技術を指す。暗号鍵の分散保管などが秘密分散の応用事例である。なお、断片化しても断片情報を管理する部分（復元用情報）が漏洩すると元の情報が復元されるため、秘密分散では分割された断片をエアギャップ構造で管理することが多い。

次に、無意味化とは、データやプログラムの構造・内容を意図的に読解不能・意味不明な形に変換し、元の意味や情報を直接的に把握できないようにする技術を指す。リバースエンジニアリングを防ぐためのプログラムの難読化などに応用されている。ただし、こちらも管理機能が単一権限で運用されていると元の情報に復元可能である。例えば欧州の GDPR 規制では秘密分散により個人情報が保護されているとはみなされないため、法的な観点も考慮したうえで適切な技術選択を行う必要がある。

具体的な実装方法

「条件付き無意味化」は、例えば、以下の 3 段階の処理のように秘密分散と無意味化を組み合わせることによって実現可能である。

① データを細かく分ける（モザイク化シェア分散）：元のデータをバラバラの破片（「シェア」と呼ぶ）に分ける。

② それぞれの破片をさらに分解する（定サイズ分解）：分けられた破片を、それぞれ同じくらいのサイズに分解する。

③ ダミーを加えて複製を多数作成し、広範囲に分散保存する：分解した情報に偽の情報（ダミーデータ）を加えて数を増やし、たくさんのコピーを作って、国内外の離れた場所にバラバラに保存する。

このプロセスの中では、計算量的安全性（解読や攻撃に要する計算量が現実的な時間や計算能力では実現不可能であるほど大きい状態）に依拠する暗号技術だけに頼らず、情報理論的に安全と評価できる物理分散構造を取り入れているのが特徴である。すなわち、計算量的安全性に依拠する暗号技術だけに頼ると、計算機性能の向上や新しいタイプのコンピュータ（量子計算機等）の出現等に対抗していくことが困難であるため、物理的な情報分散構造によって情報復元が情報量的に不可能となる方法（情報理論的安全性に依拠する手法の一つ）との組み合わせを考えたものである。

分散・分解された各情報は、それぞれ別個の鍵によって管理されており、その鍵もまた後述のように異なる方式で安全に管理される。各管理情報は強度の暗号化が施され、個別のアドレスにてブロックチェーン上に記録されるが、その構造は通常の台帳型ではなく、可変かつ多次元的なテーブル構造を採用している（前出のテーブルチェーン構造）。ゼロトラストの原則を鍵管理に適用し、「多重確認・合意ベース」の構造を採用する考え方は、現代の高度なセキュリティシステムにおける推奨アプローチであり、学術的にも活発に研究されている。データの復号には複数の独立した鍵群を揃える必要があり、さらにその組み合わせ方法も毎回変わるようにすることで、極めて高いセキュリティが実現できる。これが従来とは異なる新しい「合言葉合意技術」（PAKE: Password-Authenticated Key Exchange）である。

また、データは同じサイズで構造が似たモザイク状の断片が大量に混在する状態（「砂粒化」と呼称している）に変換されており、外部から意味を読み取ったり、原形を復元したりするのが非常に難しい構造となっている。例えばこの砂粒化データを復号するには、分散保存されている複数の場所（「砂場」と呼称している）から正しい粒子だけを選び出し、正確な順序で並べる必要があり、さらに決められた手順に従って復号処理を行う必要がある。各過程が暗号化されたデータを復号する多段階の鍵に相当し、このような多層構造により、データが流出しても復元はほぼ不可能である。こうした仕組みにより量子計算耐性を実現している。

なお、ここでいう鍵は、一般的な暗号鍵とは異なり、元データの一部や分散構造に埋め込まれた情報をもとに、その都度生成される動的かつ非固定型の鍵である。暗号資産では暗号鍵の盗難・流出や紛失が課題となっている。暗号鍵の紛失は暗号資産の紛失と同義であり、相続時に問題となるケースが少なくない。企業による管理すら困難であるものを資産保有者個人に委ねるのは金融インフラの設計として果たして適切であろうか。

本稿で紹介している手法では、鍵の管理をシステムの利用者に委ねず、鍵は存在している

がシステム的に確実に保全されたかたちで裏側に隠してしまうというアプローチをとる。具体的には、上述の分散された情報に基づく動的鍵の採用と、その分散された情報自体をさらに暗号化し、それらの復号鍵も分散情報のなかに隠していくという方式を採用している。

こうした工夫を施した無意味化は「条件付き無意味化」と呼ぶことができ、保全対象データを外資系クラウド経由で海外拠点へ広く分散保存することが可能となる。仮にクラウド事業者が所在地国家の強権的命令などにより全データを取得したとしても、その内容を解読することはできない。近年の国際政治動向からすると、こうしたリスクは民主主義国家においても看過しえないリスクとなっている。

理想的な運用手法を考えると、まず国内事業者が初期の分割・分散処理を行い、その後に海外へコピー・分散する形が望ましく、これが日本の脆弱なデジタル基盤への実践的な対応策になると考えられる。

将来展望

前節で述べたアプローチは、サイバーセキュリティ分野にも応用できる汎用性を持っており、「日本版セキュリティストレージ」として有望と考えている。また、この技術は、単なるセキュリティ手法にとどまらず、次世代情報処理の基盤となる可能性を秘めている。日本はクラウドコンピューティングにおいて外資に遅れを取っているため、今後は以下の対応を展望している。

その中核をなすのは、①エッジコンピューティングによるデータ構造管理と、②フォグコンピューティング（エッジコンピューティングとクラウドコンピューティングの間に位置する形態）による分散データ処理構造という二つの要素を融合したアーキテクチャであり、その機能面からセキュリティデータベースと呼称できる。フォグ型アーキテクチャにおけるセキュリティデータベースの構造は、現在のデータベースマネジメントシステム（DBMS）や暗号化データベースとは全く異なるものである。

これらを中核技術としたシステムは、バッチ処理（まとめて処理すること）を行うセキュリティストレージとして運用可能であるが、さらに進化させ、金融機関や決済システムのような金融ホールセールビジネスを支えるインフラの構築に活用していくことも可能である。現在の金融インフラの主流であるオンプレミス型の中央集中管理システムも、新しく登場した分散分権型のシステムのいずれも、単一（集中型）の権限管理や、鍵管理の難しさ、オフチェーン利用に伴う即時処理の困難さ、KYC など、各々が複数の課題を抱えている。

こうした課題へのソリューションとして、トラストレスな構造のもとでオンチェーン即時処理を実現する次世代金融インフラのかたちとして、データ保全の方式を大きく変革するようなシステム（例えば、データセンターやクラウドに依存しない、セキュリティ構造を内部にもつ複数のデバイス接続によるシステム）を構想していくことを目指している。これは、

GAFA をはじめとする海外 IT 大手が、DX 時代に向けて「DMP（データマネジメントプラットフォーム）」による Web3 的なインターネット拡張を模索する中、「オンプレミス構造を分散処理するホールセール型オンチェーン構造」という真逆の分散型アプローチを考えるものである。

この構造が真価を発揮するのは、6G 通信や IOWN（Innovative Optical and Wireless Network）といった次世代通信基盤との連携時である[1]。前述したようなデータセンター不要のセキュリティストレージが加われば、分散化された次世代情報インフラが簡易的かつ安価に実現できるようになる。具体的には、さまざまな場所に「ストレージ型 IoT デバイス」を設置するだけで、その一部が破壊されたり盗まれたりしても、全体としては問題が発生しない構造が実現可能となる。

サイバー攻撃から逃れる唯一の方法は、脆弱性をゼロにすることである。したがって、もしそこが攻撃されると全てがダメになってしまうような場所（単一障害点、SPOF: Single Point of Failure）をなくし、複数の仕組みやインフラの所在場所を組み合わせる「マルチ構造」で徹底的にリスクを分散させる必要がある。また、攻撃者側は効率化・自動化を進めているため、守る側も効率的に防御できる構造を持つ必要がある。そのためには、システムの入り口で防御するだけでなく、データ処理の仕組みの中に防御する機能を組み込むことが重要である。

防御コストを抑え、効率的な防御を実現する上述のような構造こそが、暗号化と分散化の真の可能性であり、Web3 にもつながる事業型次世代技術、すなわち、ビジネスとして展開できる未来に向けた技術の本質であると考えている。

（後編おわり）

[1] NTT IOWN についてはリンク先を参照。https://www.rd.ntt/iown/