7 Mainstream 領域：サイバーセキュリティ

「3本の矢」戦略でお客様ビジネスの成長・発展に貢献しセキュリティ事業を拡大

NTT データ先端技術株式会社（以下、NTT データ先端技術）は長年にわたりセキュリティに関するコンサルティング／診断／監視・運用などのサービスや、システム構築／ソリューション導入などのセキュリティ SI ビジネスを提供している。本稿では、巧妙化・激化するサイバー攻撃に阻害されることなくお客様が安心してビジネスを加速できるように支援する「3 本の矢」戦略について紹介する。

セキュリティレベルの低いところを狙う攻撃への対応が重要に

ファイルを暗号化して利用できない状態にし、元の状態に戻したければ身代金を支払うよう要求するランサムウェアが急増している。日本でも大企業や医療機関などが大きな被害を受けている。2022 年には、大手製造業が工場停止の被害に遭ったと報道された。取引先子会社がリモート接続機器の脆弱性をつかれて不正アクセスされ、そこから取引先がランサムウェアに感染したためである。コロナ禍によるリモートワークの増加により、リモート接続機器も増加している。セキュリティ対策を十分に実施する間もなく、必要に迫られてリモート接続機器を配備するケースも多い。攻撃者はこうしたセキュリティ対策が不十分なリモート接続機器を狙ってくる。リモート接続機器は攻撃者の格好の的になっている。

セキュリティ対策がしっかりしている大企業であってもサプライチェーンの中にセキュリティレベルの低い箇所があれば攻撃されてしまう（図 1）。小規模な業務委託先も含め、サプライチェーン全体で脆弱性を管理することが重要だ。

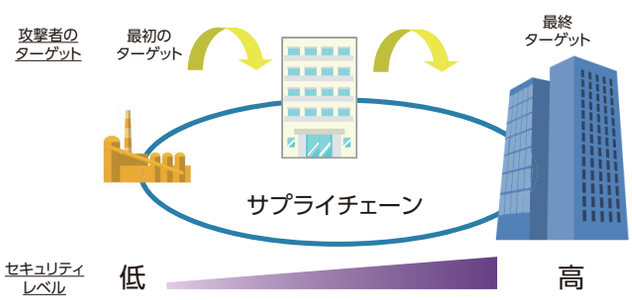

図 1　攻撃者はセキュリティレベルの低いところから攻撃

ソフトウェア開発・運用においてもサプライチェーン全体のセキュリティ強化が課題に

2020 年、米国の IT 管理ソフトウェア会社が提供した更新プログラムに攻撃者が操作可能なバックドアが仕組まれ、膨大な数の組織に影響が及んだ。このインシデントを受け、ソフトウェアサプライチェーン全体のセキュリティ強化を求める米国大統領令 14028 が 2021 年に発令され、米国政府による調達においてはソフトウェア部品表（SBOM：Software Bill of Materials）の作成が求められるようになった。日本でも企業や経済産業省が SBOM の導入・活用に向けた検討を開始している。

NTT データ先端技術株式会社
サイバーセキュリティ事業本部
セキュリティイノベーション事業部長
執行役員　星 敬一氏

「3 本の矢」戦略

こうした課題への対応が求められる中、NTT データ先端技術はお客様が安心してビジネスを加速していくためのセキュリティ支援策として、「3 本の矢」戦略（図 2）に注力している。以下、それぞれについて紹介する。

図 2 「3 本の矢」戦略

ゼロトラストセキュリティ

社内を信頼して外部との境界点で攻撃を防御する考え方は、リモートワークへの柔軟な対応、社内に侵入された攻撃に対する対応という面で十分とは言えない。そのため全ての通信を信頼せず、都度その正当性を確認してから通信を成立させるゼロトラストセキュリティの概念が普及しつつある。

「DX 推進やリモートワークの定着により、ゼロトラストは今後も重要なテーマであると考えられます。NTT データグループは既にゼロトラストネットワークを導入済であり、グローバル各社への導入経験、運用ノウハウが蓄積されています。カギとなる認証技術は自社で開発しており、日本の企業文化に合わせたカスタマイズにも柔軟に対応できます。セキュアかつ柔軟なリモートアクセス／クラウドアクセスやふるまい検知／ログ分析・監視などの実績のあるアセット、蓄積された運用ノウハウ、自社ソリューションの強みを活かして、お客様の DX 推進を支援していきます」（星氏）。

クラウドセキュリティ

クラウドセキュリティはゼロトラストセキュリティの一部だが、特に強化すべき分野であるため独立した 1 本の矢としている。クラウドシフト／リフトを支援するコンサルティング／構築サービス、クラウドセキュリティ診断、クラウド上のセキュリティ監視・運用を行う SOC サービスなどにより、お客様が安心してクラウドを活用できるようにする。

「クラウドを利用する際にデータの非公開設定やデータへのアクセス権限を誤ってしまう事例が多く、問題となっています。そのために CSPM ／ SSPM（Cloud/SaaS Security Posture Management）と呼ばれるクラウドセキュリティ設定管理ソリューションの強化に取り組んでいます」（星氏）。

サプライチェーンセキュリティ／ DevSecOps

3 本目の矢は大きく 2 つに分かれる。1 つはグループ会社・業務委託先・取引先まで含めたビジネスサプライチェーンのセキュリティマネジメント。脆弱性をスコアリングするソリューションにより関連する企業の評価リストを作成し、親会社や委託元が子会社や契約相手のセキュリティリスクを確認するといった対策である。

もう 1 つはソフトウェア開発における設計から製造・試験・運用まで、ソフトウェア開発ライフサイクル全体に関するセキュリティマネジメントだ。開発担当と運用担当が緊密に連携し迅速にソフトウェアを開発する DevOps に対し、その各工程でセキュリティ対策もしっかりと行う DevSecOps を実践するための各種支援サービスを想定している。

将来的には「統合マネージドセキュリティサービス（XDR）」の提供を目指す

2023 年 6 月、NTT データは、インシデントの未然防止から発生時の被害を最小限に抑える高度セキュリティ技術者によるアウトソーシングサービスを 2023 年 7 月から提供開始すると報道した。セキュリティ運用のアウトソーシングサービスもその 1 つだ。NTT データ先端技術もその一翼を担っている。

「このようなサービスは MDR（Managed Detection and Response）と呼ばれています。あらゆるものを対象とする XDR（Extended Detection and Response）の実現・提供を目指しています」（星氏）。

NTT データの案件を通じて培ったノウハウでお客様ビジネスの成長・発展に貢献

NTT データ先端技術には高度なセキュリティレベルが求められる NTT データのお客様にセキュリティソリューションを提供してきたノウハウの蓄積がある。その強みを活かし新規顧客の開拓にも力を入れるなど、セキュリティビジネスの拡大に力を入れている。

「お客様のビジネスの成長・発展に貢献することが目標です。セキュリティ対策の不備がビジネスを阻害することのないよう、3 本の矢で貢献していきたいと考えています」（星氏）。