日本のテクノロジー及び メディア業界における サイバー攻撃対象領域について

世界第3位の経済大国である日本は、それゆえ、サイバー犯罪の標的になりがちであるとも言えます。自動車、金融サービス、製造業など、さまざまな産業のグローバルな中心地として機能する日本に対する攻撃は、日本国内の企業や組織にとどまらず、国外にも広がっています。

世界的にも複雑で堅牢な市場を擁する日本のテクノロジー・メディア業界は、サイバー攻撃における標的にもなっています。Rapid7の最新のレポートでは、日本を取り巻くサイバー攻撃の全体像を概観しています。本ドキュメントでは、特にテクノロジー、メディア、通信の各業界を中心にRapid7の研究者が分析した結果、明らかになった主な傾向と調査結果をご紹介します。

情報技術業界

技術関連企業は、一般に、顧客個人を特定できる情報を狙う攻撃者の標的となりがちですが、企業自体がターゲットになることはめったにありません。情報技術ベンダーは、価値の高い顧客情報を大量に所有していることが多いためか、Rapid7の調査では、ランサムウェアグループによって狙われるケースが多いことがわかっています。

ランサムウェアによる侵害は、幅広い影響を及ぼします。引き続き影響が発生し続けている2022年に発生した侵害でも同様の影響が見られました。例えば、あるITベンダーを標的とした侵害では、結果としてその顧客の少なくとも10社が影響を受けました。被害企業の中には、他のランサムウェア攻撃に悪用可能な情報を大量に保有していたオンライン保険会社もありました。

東京に本社を置くFortue500企業の一社が、シンガポールの子会社が踏み台となった侵害を受けた結果、政府組織を含む他の62の組織の侵害につながった例に見られるように、海外子会社は日本企業にとって深刻な脆弱性であり続けています。この件では、自衛隊も影響を受けた可能性が示唆されています。

ゲーム業界

日本のゲーム市場は好調で本社を日本に置くゲーム企業も多いため、この業界も攻撃者の興味を惹く傾向にあります。2022年7月には、ランサムウェアグループのBlackCat（元DarkSideと推測される）が、エルデンリングやパックマンなどのゲームを生んだゲーム会社を侵害しています。これも、海外に拠点を置くパートナーや子会社に起因する侵害と考えられています。

ここでは、日本のテクノロジー・メディア業界に対する攻撃の影響のごく一部をご紹介しました。同業種をはじめ、他のいくつかのセクターに関する詳細な分析については、レポートをご覧ください。