ウクライナ情勢と連動して発生したサイバー攻撃から得るべき教訓

2022 年 7 月
名和 利男

1. ウクライナ情勢と連動して発生したサイバー活動の捉え方

- ウクライナ情勢と連動して発生したサイバー活動の観測および分析を通じて、今後の「サイバー戦」および「認知戦（影響作戦）」の状況認識と教訓を獲得することが期待できる。
  - 具体的なサイバー活動は、別紙の「表 1」および「表 2」のとおり。

2. 状況認識(Situation Awareness)と得るべき教訓(Lessons Learned)

状況認識：軍事行動が行われる一定期間（数ヶ月から数年）前から、段階的かつ急激に活性化した「**潜在的なサイバー攻撃（偵察活動）**」

- 教訓：従来のサイバーセキュリティ対策では検知困難であるため、既存の「想定脅威」を引き上げて、それに適応したセキュリティコントロールを実装および維持する。（専門家の支援が必要）

状況認識：ハイブリッド攻撃等により相手国の世論を操作して判断や行動を変容させる「**認知戦**」

- 教訓：DDoS 攻撃と SNS 拡散を連携させた「世界に対する過大な攻撃効果の強調」、データ破壊（ワイパー）攻撃とウェブサイト改ざんを連携させた「相手国民に対する臨在感、被支配感・迫害感の強要」などにより過度な恐怖や不安感を抱く運用関係者へのフォローアップを行う。

状況認識：軍事行動と連動した情報通信システムの「**能力破壊攻撃**」

- 教訓：軍事行動の発生前後において、緊急かつ重要な情報の周知・伝達・処理等に係るコンピュータやネットワーク（衛星通信を含む）の機能やサービスを破壊するサイバー攻撃の発生を想定したコミュニケーション計画の立案、整備、および実効性の確保努力を行う。

状況認識：重要施設の安定運用に影響を与えるインフラ事業者の「**IT システムへのサイバー攻撃**」

- 教訓：インターネットプロバイダー、電力関連企業、主要メーカー等の施設内ネットワーク（IT システム）に対する多様なサイバー攻撃（アカウント乗っ取り、データ破壊攻撃等）の発生を踏まえ、有事において日本の急所となる発電所、変電所、交通施設、通信施設、浄水施設、ガスプラント等の事業者におけるサイバーリスクを見積もった上で、相応したレジリエンスの計画と実効性の確保に向けた検証・訓練の積み重ね努力による成熟度を向上させる。

3. 日本における取り組みの課題

- サイバー攻撃の発生事実や恐れの大部分が認知されていない状況が十分に理解されていない。
  - 現場に実装されているセキュリティコントロールの前提となる「想定する脅威」が「実際の脅威」と乖離し、意思決定者に対して必要な「洞察」や「文脈」が提供されていない。
- 官民における現体制は、「実際の脅威」に適合したセキュリティコントロールの実現を困難にしている。

組織間の調整・合意形成の難易度の高さと実務担当者のインセンティブ不足 ＞ 得られた教訓における「とるべき(事前)行動」の必要性と重要性に係る認識とモチベーション

図 1: 日本の現体制における課題の例

別紙

表 1「特定国家の支援を受けたサイバー攻撃グループ」が仕掛けたと推定されるサイバー活動

2021 年 4 月～	ロシアが世界各国にサイバー偵察を活性化
2021 年 10 月～	ロシアがウクライナにサイバー偵察を強化
2022 年 1 月 13 日	ウクライナのデータ破壊マルウェア攻撃
2022 年 1 月 13 日	ウクライナ政府サイトの同時多発的な改ざん
2022 年 1 月 14 日～	ロシアのサイバー犯罪グループに不自然な現象
2022 年 2 月 15 日	ウクライナの軍や銀行等に DDoS 攻撃
2022 年 2 月 23 日	ウクライナに再度のデータ破壊マルウェア攻撃
2022 年 2 月 23 日	ウクライナ兵士に脅迫的なテキストメッセージ
2022 年 2 月 23 日	ウクライナの軍や銀行等に再度の DDoS 攻撃
2022 年 2 月 24 日	欧州の通信衛星システムにサイバー攻撃
2022 年 2 月 25 日	ウクライナ軍へのスピアフィッシング攻撃
2022 年 2 月 25 日	ウクライナの水力発電所にサイバー攻撃の兆候
2022 年 3 月 28 日	ウクライナの通信会社にサイバー攻撃
2022 年 3 月 31 日	ドイツの風力タービンメーカーがサイバー攻撃
2022 年 4 月 8 日	ウクライナの高圧変電所にサイバー攻撃
2022 年 4 月 8 日	フィンランドの政府機関に対する DDoS 攻撃
2022 年 4 月 22 日	ウクライナの全国郵便局に DDoS 攻撃

表 2「国際ハッカー集団アノニマス」が仕掛けたと推定されているサイバー活動

2022 年 2 月 25 日	ロシア国防総省のデータベースをハッキング
2022 年 2 月 27 日	ロシアの国家テレビチャネルをハイジャック
2022 年 3 月 2 日	ロシアの宇宙科学研究所のサイト改ざんと情報流出
2022 年 3 月 2 日	ロシア国内の防犯カメラを侵害
2022 年 3 月 10 日	ロシアのクラウドデータベースへの侵害
2022 年 3 月 11 日	ロシアに 700 万のテキストメッセージ送信キャンペーン
2022 年 3 月 15 日	ロシアの主要組織への DDoS 攻撃