S-H26-356

# サイバー脅威化における情報保全体制に関する調査研究

(一財)ディフェンス リサーチ センター 研究委員 横山 恭

## 1. 背景と目的

最近の世界的なサイバー攻撃の傾向として、政府機関や企業に対する機密情報の窃取を目的とした攻撃が増加している。例えば、2014年5月19日、米司法省は、商業利益のために、米国の企業及び労働者団体に対して、サイバー・エスピオナージ（諜報活動）を行った5人の中国軍のハッカーを起訴した。これまで、サイバー攻撃をめぐっては中国や北朝鮮の政府機関による関与が指摘されていたが、この事例により、国家機関による諜報目的のサイバー攻撃（以下、サイバー諜報活動という。）の実態が明らかとなった。

また、上記のようなネットワークを通じたサイバー攻撃の他にもインサイダーによる情報漏えい事案も増加している。インサイダー脅威そのものは目新しいものではないが、最近の事例は、膨大なデータが瞬時のうちに盗み出され、そのデータがインターネットのウェブサイトに公開されてしまうデジタル時代におけるインサイダー脅威を浮き彫りにしている。

サイバー空間に記録・保管された「秘匿すべき情報」の漏えい、改ざん又は破壊等を防止するのが「サイバー脅威下の情報保全」である。多種多様なサイバー諜報活動に対応するには、伝統的な情報保全活動である「秘密保全」と「防諜（スパイ対策）」、さらに非伝統的な情報保全活動である「サイバーセキュリティ対策」が必要となる。この3つの要素が上手くかみ合うことで、重要な情報を保護し、漏えいを防止し、さらに、犯罪者を逮捕・起訴することができる。

本稿調査研究の目的は、サイバー脅威が増大する中、それに適切に対応するための施策を提言することにある。したがって、サイバー諜報活動の方法、サイバー諜報活動の実例と対策を調査するとともに、情報保全体制の現状を調査し、最後に、政府が策定・実施すべき政策と政府機関や民間企業が措置すべき事項について提言として取り纏めた。本調査研究が、今後の我が国のサイバー脅威下における情報保全体制の在り方の検討の資となれば幸甚である。

## 2. サイバー諜報活動の方法

サイバー諜報活動の武器となるマルウェアについて調査した結果、毎日2万件の新しいマルウェアが世界で登録されている。これまでに2億以上のマルウェアが登録されている。初期のマルウェアは人目を引く迷惑な攻撃を目的としていが、今日ではその目的は、情報の窃取等の違法行為が中心になっている。中にはスタックスネットのような国家が関与したと思われる高度で洗練されたマルウェアが出現している。

また、サイバー諜報活動に使用される攻撃手法には、ハッキング攻撃（セキュリティ・ホール攻撃、標的型メール攻撃、ドライブバイダウンロード攻撃、水飲み場攻撃）、インサイダー攻撃、サプライチェーン攻撃、及び盗聴がある。従来は、ソフトウェアの脆弱性を突いたセキュリティ・ホール攻撃が広く使用されている。最近は、特に人間の脆弱性を突いた標的型メール攻撃や水飲み場攻撃が広く使用されている。

## 3. サイバー諜報活動の実例と対策

ハッキング攻撃（セキュリティ・ホール攻撃〈バッファ・オーバーフロー、SQLインジェクション、及びクロス・サイト・スクリプティング〉、標的型メール攻撃、ドライブバイダウンロード攻撃、水飲み場攻撃）、インサイダー攻撃、サプライチェーン攻撃、盗聴について、それぞれの概要、攻撃要領、事例及び対策を調査した。

ハッキング対策の要諦は、①強固なパスワードを使用する、②最新のパッチを適用する、③ウイルス対策ソフトを導入する、③怪しいメールは開かない、④怪しいサイトにアクセスしない、などの個人でできる基本的なセキュリティ対策を確実に履行することである。これだけのことを履行すれば相当のハッキング攻撃が防御できる

また、インサイダー攻撃、サプライチェーン攻撃、盗聴については、それぞれ特有の対策が必要である。ただし、サプライチェーン攻撃対策については、対策への取組みが最も進んだ米国においても未だ確定したものはない。

## 4. 情報保全体制の現状

我が国の情報保全体制の強化の経緯と情報保全活動の根拠となる法律として、「秘密保全」と「防諜（スパイ対策）」に関しては、特定秘密保護法の成立により刑罰が強化され、秘密適格性確認制度が法制化された。これにより秘密取扱者適格性確認制度の法制化と機密漏えいの罰則強化が実現し、我が国の伝統的な情報保全体制は以前に比べて格段に強化された。しかし、スパイを取り締まるための法律が未整備であることや行政的通信傍受が認められていないなど未だ米国や英国の水準に到達していない。国際基準から見れば未だ不十分である。

他方、「サイバーセキュリティ対策」に関しては、「国家安全保障戦略」においてサイバー脅威は安全保障上の脅威であるとの認識が示された。また、2015（平成27）年1月に、政府機関のサイバーセキュリティ政策の司令塔となる「サイバーセキュリティ戦略本部」と「内閣官房情報セキュリティセンター（NISC）」が設置された。このように脅威認識面や法制面、組織面において強化されたと言える。しかし、我が国のセキュリティ対策は、情報セキュリティに対する経営層の理解・認識が足りないことや要な情報セキュリティ人材が不足していることなど未だ不十分である。

## 5. 提言

4 項の現状の問題点や課題を踏まえて、政策上の提言と政府機関及び民間企業が早急に措置すべき事項について取り纏めた。

●政策上の提言

①スパイ防止法を制定する。

②サイバー空間の犯罪捜査のための「通信傍受に関する法律」の改正し、犯罪捜査のための通信傍受要件を緩和する。

③包括的な「秘密取扱者適格性確認制度」のための法整備を行う。

④英国の MI5 のような防諜機関を創設する。

⑤英国の MI6 のような対外情報機関を創設する。

⑥インテリジェンス機関に対する監視システムを整備する。

⑦インテリジェンス常任委員会の国会設置と委員（国会議員）の守秘義務を新設する。

⑧運用規則等内部統制システムを整備する。

⑨情報要員の長期間勤務とそれに見合う処遇を行う。

⑩基本的人権やマスコミの知る権利等への配慮を行う。

●政府機関及び民間企業が早急に措置すべき事項

①各組織は、情報セキュリティのリスクマネージメントを、組織全体のリスクマネージメントに統合する。

②各組織は、取りあえず、軽減戦略トップ 4 を実装する。

## 6. 謝辞

本調査研究は、（一財）新技術振興渡辺記念会より、平成 26 年度上期の科学技術調査研究助成を受けて、平成 26 年 4 月より平成 27 年 3 月までの間、（一財）ディフェンス リサーチ センターが実施したものである。関係各位に深甚なる謝意を表する。（了）