Keidanren
Policy & Action

サイバーセキュリティ対策の強化に向けた提言

2015 年 2 月 17 日

一般社団法人 日本経済団体連合会

現在、世界中において、サイバー攻撃[1]による被害が深刻化している。そこで、わが国では、サイバーセキュリティ基本法の制定などサイバーセキュリティ対策の強化が進められている。

経団連が1月1日に発表した「『豊かで活力ある日本』の再生」においては、ICTがグローバルな社会インフラとして定着する中で、サイバーセキュリティの確保に向けた対策の必要性を指摘した。

特に、国の重要インフラ等に対するサイバー攻撃は、国民生活に重大な障害が生じるおそれがあり、経済活動にも支障が生じ、国全体の産業競争力の喪失にもつながる大きな問題である。

そこで、経団連は、重要インフラ等を守るサイバーセキュリティ対策の強化に向けた具体的な取組みに関する提言を以下の通り取りまとめた。

1. 国内外の情勢

(1)国際情勢

ICT社会の進展により、サイバー攻撃は全世界に重大な影響を及ぼす可能性が高い脅威となった。2007年にはエストニア、2009年、2011年、2013年には韓国に対する大規模なサイバー攻撃が発生し、政府や企業の活動が停止した。2012年のロンドンオリンピックでは、イギリスに対して膨大な数のサイバー攻撃が行われた[2]。

国家安全保障においてサイバー攻撃は重大な脅威であり、米国のオバマ政権は、陸、海、空、宇宙に次ぐ第5の戦場として、サイバー空間を位置付けている。

昨年12月に米国において、ソニー・ピクチャーズ エンタテインメントに対するサイバー攻撃が起き、オバマ政権は北朝鮮が攻撃元であると断定し、北朝鮮への対抗措置をとることを表明した。

また、本年1月には、米中央軍のツイッターやYouTubeのアカウントに対するハッキングも起きた。

オバマ政権は、こうした事態を踏まえ、1月に政府と民間企業の情報共有の強化等を行うことを発表した。

---

[1] サイバー攻撃とは、情報通信ネットワークや情報システムを利用して行われる不正侵入、データの窃取・破壊、不正プログラムの実行、DDoS攻撃（Distributed Denial of Service Attack：分散型サービス不能攻撃）などを指し、企業の情報を盗み出す犯罪から、国家的なレベルでのテロや戦争を目的とした攻撃まで含む総称である。

[2] 2週間の開催期間中にロンドンオリンピックの公式サイトに対して2億1,200万回のサイバー攻撃、1秒間に1万1,000件のDDoS攻撃が行われた。

(2)国内情勢

2011 年に防衛関連企業へのサイバー攻撃が発生し、その後も政府機関や重要インフラ等に対するサイバー攻撃の件数が増加傾向にある。サイバー攻撃の対象は政府機関、重要インフラ、企業、個人と広範囲に及んでおり、また世界中からの多様な主体による攻撃が起きている。

2013 年 12 月に政府が策定した国家安全保障戦略および防衛計画の大綱において、サイバー攻撃が安全保障上の大きな脅威として位置付けられた。

昨年 11 月にサイバーセキュリティ基本法が成立し、同法に基づいて 1 月 9 日に政府はサイバーセキュリティ戦略本部（本部長：内閣官房長官）と、内閣官房に事務局となる内閣サイバーセキュリティセンター（NISC：National center of Incident readiness and Strategy for Cybersecurity)を設置[3]した。

2020 年の東京オリンピック・パラリンピックでは、わが国の政府機関や企業等に対して、高度な技術によるサイバー攻撃が集中することが懸念されており、サイバーセキュリティ対策の強化が急務となっている。

2. サイバー攻撃の脅威

サイバー攻撃により、わが国と海外との通信の途絶や、電力・ガスの供給または交通網や金融システムなどの停止が起きれば、国民生活や経済活動が麻痺して、国家としての機能も維持できなくなる。

政府の情報セキュリティ政策会議が決定した「重要インフラの情報セキュリティ対策に係る第 3 次行動計画」（2014 年 5 月 19 日）で示された重要インフラ（情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流、化学、クレジット、石油の合計 13 分野）は、国民生活や経済活動の根幹である。各々の重要インフラは相互に依存しており、サイバー攻撃による影響は社会全体に及ぶ可能性がある。

(1)サイバー攻撃の特徴

サイバー攻撃は、ボットネット[4]等を利用して行われる。攻撃者の特定や事後的な追跡が困難であり、攻撃が組織的なものか、個人によるものかなどは分からない。

また、例えば、攻撃者が、目的を達成するために防御システムを観察し、成功する可能性が十分に高い攻撃手段を準備することが可能であるなど、攻撃者が常に優位な立場にある。

---

[3] 現在、事務局の人員は約 80 名程度である。

[4] ウイルスなどに感染したコンピューターのネットワーク。

(2)サイバー攻撃への対処

サイバー攻撃の技術は日々進歩しており、全ての攻撃を未然に防ぐことは技術や対策費用等の面から現実的ではない。サイバー攻撃を受けた場合、被害を極小化するダメージコントロールが重要であり、攻撃を的確に把握し、迅速に対応することが必要である。また、企業の業種などに適したサイバーセキュリティ対策の方針の策定が求められる。

(3)攻撃対象の拡大

外部のインターネットにつながる情報システムに加えて、組織内に閉じた形で利用されることが多い制御システムも攻撃対象となる。

サイバー攻撃の目的が従来の情報の窃取や改ざんから、重要インフラ等の機能停止など社会全体へ影響を与えることにまで拡大している。重要インフラ等を支える制御システムはインターネットから切り離されているが、サイバーセキュリティ対策が重要になっている。

スマートフォンなどインターネットに接続してサービスを提供する機器の普及に伴い、サイバー攻撃の潜在的な対象は拡大している。今後、スマートカーの普及やIoT[5]の進展によって、攻撃対象の一層の拡大が想定される。

3. 重要インフラ等に対するサイバーセキュリティ対策

重要インフラ等を対象にした大規模なサイバー攻撃に対しては、直接の攻撃対象となる企業だけでなく、政府機関や他の重要インフラ事業者等との連携が必要となる。まず、政府は重要インフラ等をサイバー攻撃から守ることを明確にし、抑止力を向上させる必要がある。

また、サイバー攻撃に備えて官民の連携強化を図るとともに、実際に大規模なサイバー攻撃が起きた場合には、被害を受けた企業だけで対処することは難しいため、政府が中心となり対策を実施すべきである。

(1)具体的施策

①情報共有の強化

サイバー攻撃に関する官民の情報共有については、重要インフラ事業者等が連携するセプターカウンシル[6]を積極的に活用することが重要であり、内閣官房はその運営及び活動に対する支援や、活動の強化等に必要な環境の整備を図

---

[5] Internet of Things：あらゆる「モノ」をインターネットに接続し、相互に通信や情報交換を行う仕組み。

[6] セプターカウンシル（CEPTOAR（Capability for Engineering of Protection, Technical Operation, Analysis and Response）- Council）：重要インフラの各分野の代表で構成される情報共有・分析のための協議会。

ることになっている。この他にも多くの会議体[7]があり、これらが連携できる情報共有体制の更なる強化が必要である。セプターカウンシルについては、引き続き内閣官房を中心とした支援により実効性を確保する必要がある。

サイバー攻撃の被害、対応、予防等に関する情報や知見について、官民の具体的な共有方法を検討する必要がある。その際、関係者間の秘密保持について配慮する必要がある。

②演習の実施等

サイバー攻撃の深刻度に応じて、官民の連携のあり方を具体的に検討する必要がある。例えば、攻撃範囲、連続的かつ長期的、同時多発的、機能不全に陥るかなどの要素が考えられ、大規模なサイバー攻撃の判断基準と対応指針を整備することが求められる。そのためには官民合同のサイバーセキュリティ訓練や演習を重ねる必要がある。

③技術開発とシステム運用

サイバー攻撃に対する防御能力の強化を目的に、以下の技術を開発する必要がある。

・サイバー攻撃を事前に探知し、無効化して被害を予防する技術
・一連の攻撃を的確かつ迅速に探知、あるいは攻撃者の事後的な追跡を可能とする技術
・攻撃に利用される不正な接続先や攻撃情報などを関係機関や企業に自動的かつ速やかに伝達できる情報共有技術
・制御システムへの攻撃に対するシステムの機能を維持する技術
・攻撃パターンの分析を含めた先端的な防御技術
・情報を匿名化して共有する技術

こうした重要な技術開発について、来年 3 月に政府が策定する予定の第 5 期科学技術基本計画（2016 年度～2020 年度）に盛り込むべきである。

優れた防御システムを構築し、これを継続的に運用することが重要であり、訓練や攻撃の分析等を通じてシステムの能力向上を図る。こうした技術開発やシステム運用について、民間企業の取組みに対するインセンティブを検討する必要がある。

④人材育成の強化

高度化が進むサイバー攻撃に対応するためには、最上位の技術レベルを有す

[7] サイバー情報共有イニシアティブ（担当省庁：経済産業省）、サイバーインテリジェンス情報共有ネットワーク（同：警察庁）、サイバーディフェンス連携協議会（同：防衛省）、テレコム・アイザック推進会議（同：総務省）等。

るトップ人材やホワイトハッカーの育成が必要である。また、セキュリティシステムを運用する人材の増員と技能の強化も重要である。産学官が連携して、こうしたセキュリティ人材のキャリアパスを整備すべきである。その際、各企業や各省庁において、国際的な人材交流も含め、人材の円滑な雇用に向けた仕組みも検討する必要がある。

わが国のセキュリティ人材は質と量の両面で不足しており[8]、産学官が連携し、人材の充足に取り組むことが重要である。このため、持続的かつ長期にわたる取組みが必要であり、優れた若者や女性などの活躍を推進する必要がある。

⑤国際連携の推進

サイバー攻撃は世界中で発生しており、日本国内だけの情報では十分な対応ができない。海外の政府機関や企業と情報を共有し、国際的な連携を推進すべきである。例えば、欧米などの諸外国との情報共有の推進、サイバー防衛協力や合同演習を実施する必要がある。

サイバー空間の安全性を確保するため、国連におけるサイバー攻撃に関する国際規範の策定に政府が積極的に参加する必要がある。攻撃者の追跡や特定をして、適切な対処を可能とする国際的な仕組みの検討によるサイバー攻撃に対する抑止力の向上が求められる。

また、サイバーセキュリティに関する国際会議をわが国で開催することにより、専門家の交流促進や知見の共有を図り、わが国のサイバーセキュリティを向上させるべきである。

⑥重要インフラ分野の見直し

現在の重要インフラ 13 分野については、分野の追加等の見直しを適宜行うべきである。情報システムの障害が国民生活や経済活動に多大な影響を及ぼすおそれのある分野として、スマートシティやスマートタウン、ITS[9]等の新たなネットワーク系サービス等が挙げられる。

⑦インターネットの安全性の向上

インターネットの安全性が向上すれば、サイバー攻撃の抑制に資する。このため個人も含めた利用者が、インターネットの利用に関する知見を深める必要がある。例えば危険な電子メールやウェブサイトの判別方法、ウイルスに感染した場合の対処方法、適切な防御手段の導入や更新等の必要性を官民が挙げて

---

[8] 情報処理推進機構は、わが国のセキュリティ人材は 26 万 5,000 人いるが、16 万人が能力不足、8 万人が量的に不足で、合計 24 万人（16 万人＋8 万人）が不足していると試算している。

[9] Intelligent Transport Systems：高度道路交通システム。

周知すべきである。

(2)政府の体制整備

重要インフラ等に対するサイバー攻撃が起きたときに、重要インフラ事業者からの被害等について政府として対応する部門の一元化を行う必要がある。

企業に対して関係する省庁がそれぞれに報告を求めるのではなく、政府として情報を集約する機能を内閣官房に一元化するとともに、各省庁の実行力を強化し、連携して迅速な対応ができる体制を構築すべきである。

サイバーセキュリティ戦略本部はサイバーセキュリティ基本法に基づく強力な権限を与えられており、政府機関や重要インフラ等を対象とするサイバー攻撃に対して関係省庁をまとめ、リーダーシップを発揮する必要がある。サイバーセキュリティ戦略本部は、国家安全保障会議や IT 総合戦略本部と緊密に連携し、関係省庁に対して勧告権の適切な行使を含む積極的な関与が求められる。

4. 産業界の取組み

サイバーセキュリティの確保は、重要インフラ関係企業だけでなく、全ての企業にとって、企業の信用の維持や、事業の継続に関わる重要な課題[10]である。また、守るべき対象が情報システムから制御システム、スマートフォン等の新しいデバイス、さらには IoT へと拡大する状況に企業は対応する。

産業界は、サイバーセキュリティを技術上の問題だけではなく、経営上の重要課題として位置付け、経営層の意識改革を図る。経営層の強力なリーダーシップのもと、CISO（Chief Information Security Officer：最高情報セキュリティ責任者）の設置など組織の改革や人材の育成などに努め、業種間の分野横断的な情報の交流や意見交換なども進める。その際、各企業が緊急事態に対応する CSIRT[11]を設置し、同業種の企業の CSIRT と連携を強化する。

人材育成については、企業と大学・大学院等が連携し、高度セキュリティ人材を育成するセキュリティ講座を全国に展開するため、企業が支援（寄付金、講師派遣、実践的なノウハウの提供、演習環境や場の提供など）する仕組みが 2015 年度に始まる[12]。

こうした産業界の取組みは国家のサイバーセキュリティの向上に資する。

以　上

---

[10] 営業秘密などの知的財産や個人情報保護などにも関わる。

[11] Computer Security Incident Response Team：コンピューターのセキュリティに関する事案が発生した際に対応するチーム。

[12] NTT と早稲田大学、NEC と北陸先端科学技術大学院大学が連携した寄附講座が 2015 年 4 月に開講する。