サイバーセキュリティコミュニケーション制度設計のための国際比較分析

代表研究者　　氏名　趙章恩　　東京大学大学院情報学環　特任助教

1 研究の背景

第 4 次産業革命の特徴は、全てがネットワークでつながり大量のデータを集めて分析し、分析した結果を実生活で活かしまたデータを集めて分析を繰り返すことである。これはデータを安全に守りながら活用できる、サイバーセキュリティが保たれた社会であることを前提にした変化である。ヘルスケアやスマートシティを事例に考えると、サイバーセキュリティの問題はインターネット上の問題に留まらず、人の命にもつながっていることがわかる。

日本のサイバーセキュリティ基本法第二条では、「電子的方式､磁気的方式その他人の知覚によっては認識することができない方式により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損」する行為。「電子計算機に対する不正な活動による被害」を生じさせる行為から守ることをサイバーセキュリティと定義している。

しかし完全なサイバーセキュリティを保てる技術や政策は存在しないと想定すべき時代になった。ICT の利活用が高度になり技術が発展すればするほど、サイバーアタックの技術も発展している。日本は ICT の発展により世界有数のスマート社会になりつつある一方で、ランサムウェアといったサイバー犯罪被害や海外からのサイバーアタックも年々増加している。マカフィーは 2018 年のサイバーセキュリティは「AI の機械学習」攻防になると展望した[1]。コンピュータウィルスを予防するためアンチウィルスといったソフトウェアをインストールしなくても、端末の中にある AI が機械学習で予防的に対応できるようになる一方で、攻撃者もまた機械学習を使って人を騙す方法を研究したり、データのバックアップをしていない人を選んでランサムウェア攻撃をしたりといった抜け道を探す攻防になるということである。こうした状況から生活に欠かせなくなったインターネットを安全に利用できる環境を保つため、日本政府はサイバーセキュリティの強化を最優先課題にしている。サイバーセキュリティに関する法律や複数の戦略、ガイドラインの制定と改訂が行われる中、共通しているのは官民協力を重視しようという点である。企業だけ、政府だけ、自分の組織内で孤軍奮闘するのではなく、複数の組織が実効的な協力関係を維持、積極的にコミュニケーションを行い、サイバーセキュリティのレベルを上げていくべきだが、具体的にどうしたらいいのだろうか。官民協力を重視し、政府と企業の間で緊密なコミュニケーションをとる必要性は認識しているが、どのようにすればいいのだろうか。海外事例を比較し、政府と企業の間で行うサイバーセキュリティコミュニケーションの在り方について考察する。

2 サイバーセキュリティコミュニケーションに関する研究動向

経済産業省は2015年12月「サイバーセキュリティ経営ガイドライン」を策定した。ガイドラインは企業に対して「平時及び緊急時のいずれにおいても、サイバーセキュリティリスクや対策、対応に係る情報の開示など、関係者との適切なコミュニケーションが必要」であるとしている。政府と企業がサイバーセキュリティのためにそれぞれ対策をとるより、情報を共有して対策を講じる、被害状況を隠蔽せず開示して捜査に協力する、2次被害を防ぐ、といった方が効果的であり、いつでも官民が協力できる体制を維持する必要があるという意味だが、「適切なコミュニケーション」をするために、具体的に何をどうすればいいのかについては曖昧なままである。

サイバーセキュリティコミュニケーションに関して科学技術情報発信流通総合システムJ - STAGEジャーナル検索、NII学術情報ナビゲータで検索したところ、化学物質や食品の安全管理、災害関連リスクコミュニケーションに関する研究、サイバーセキュリティの技術や法制度に関する研究が中心だった。

情報セキュリティとリスクコミュニケーションに関する研究に範囲を広げると、伊東（2010）は企業の情報漏洩の多くは社内の人的ミスだったことを背景に企業のリスクマネジメントを推進していく上でリスク評価者（計画者）と対象組織が信頼関係にある連携（リスクコミュニケーション）が重要だとした。

---

[1] 2017 年 11 月 29 日付 McAfee Labs Previews Five Cybersecurity Trends for 2018
https://securingtomorrow.mcafee.com/mcafee-labs/2018-threats-predictions/　（2018 年 6 月 30 日アクセス）

リスクコミュニケーションとは、リスク分析の全過程において、リスク評価者、リスク管理者、消費者、事業者、研究者、行政担当者などの関係者の間で情報や意見をお互いに交換しようというものである[2]。リスクコミュニケーションと海外の事例を参考にサイバーセキュリティコミュニケーションを定義してみると、大きく4つに分けることができた。企業のサイバーセキュリティ担当者が社内の人に向けて行う「内部コミュニケーション」、サイバーセキュリティを担当する企業と企業、企業と政府機関の間で行う「情報共有コミュニケーション」、サイバーアタックにより侵害事故が発生した企業が顧客に対して行う被害状況開示や今後の対策などについて説明・謝罪といった「対外コミュニケーション」、海外からのアタックや国境のないサイバー犯罪に対応するための「国際協力コミュニケーション」がある。

表1　サイバーセキュリティコミュニケーションの種類

種類	内容
内部コミュニケーション	企業のサイバーセキュリティ担当者が社内の人に向けて行う
情報共有コミュニケーション	サイバーセキュリティを担当する企業と企業、企業と政府機関の間で行う
対外コミュニケーション	サイバーアタックにより侵害事故が発生した企業が顧客に対して行う（被害状況や今後の対策などについて説明、謝罪など）
国際コミュニケーション	海外からのアタックや国境のないサイバー犯罪に対応するために行う

(著者作成)

一般社団法人JPCERTコーディネーションセンター（2015）が提案したサイバーセキュリティ対策の一つとしてリスクコミュニケーション（報告・情報公開）がある。「インシデント対応は、ともするとインシデントが発生したことの隠蔽も含む、内向きの処理に終始しがちである。しかし、適法性だけでなく適正性にも配慮すれば、利害関係者に対しリスクの存在やインシデントの影響、原因分析や再発防止策を積極的に説明することは極めて重要である。したがって、インシデント対応に関する報告や情報開示など、リスクコミュニケーションを適切に行う機能を強化することが望ましい」という説明からこれは対外サイバーセキュリティコミュニケーションにあたるといえる。本稿では主に情報共有コミュニケーションの事例と在り方について研究を行った。

3 サイバーセキュリティコミュニケーションの国際動向

3-1 日本の事例

日本政府は 2001 年国家 ICT 政策として e-Japan 戦略を発表、IT の利活用に焦点を当てていたが、インターネットの急速な利用拡大により不正アクセスやコンピュータウィルスの増加といった情報セキュリティの危機感が高まったことから 2005 年内閣官房の情報セキュリティ対策推進室の役割を強化した「情報セキュリティセンター（NISC)」を設置、国家政策としてサイバーセキュリティ問題を重視するようになった。

2006 年には情報セキュリティに関する政府の中長期的な方向性をまとめた「第 1 次情報セキュリティ基本計画（セキュア・ジャパン)」を公表、「官民における情報セキュリティ対策の体制の構築」のため自治体の情報セキュリティの確保に係るガイドラインの見直しを行った。2007 年には「官民における情報セキュリティ対策の底上げ」を目標にした施策を実施した。2009 年には「第 2 次情報セキュリティ基本計画」を、2010 年には「国民を守る情報セキュリティ戦略」を公表、2011 年には官民協力体制を強化するため、独立行政法人情報処理推進機構と経済産業省、内閣サイバーセキュリティセンター、企業が連携してサイバー情報共有イニシアティブ（J-CSIP : Initiative for Cyber Security Information sharing Partnership of Japan）を発足した。2013 年には情報セキュリティ政策の評価等の実施方針をまとめ、政策の見直しを行った。

2014 年にはサイバーセキュリティに関する施策を総合的かつ効果的に推進するため「サイバーセキュリティ基本法」を公布した。同法の第一条には、「高度情報通信ネットワークの整備及び情報通信技術の活用の進展に伴って世界的規模で生じているサイバーセキュリティに対する脅威の深刻化その他の内外の諸情勢の変化に伴い、情報の自由な流通を確保しつつ、サイバーセキュリティの確保を図ることが喫緊の課題となっている」、「サイバーセキュリティに関する施策を総合的かつ効果的に推進し、もって経済社会の活力の向上及び持続的発展並びに国民が安全で安心して暮らせる社会の実現を図るとともに、国際社会の平和及び安全の確保並びに我が国の安全保障に寄与することを目的とする」として、サイバーセキュリティがなぜ重要なのかを明記してある。また、サイバーセキュリティを保つのは国の責務、地方公共団体の責務、重要社会基盤事業者の責務、サイバー関連事業者その他の事業者、教育研究機関の責務であり、国民の努力も必要である

[2]厚生労働省　http://www.mhlw.go.jp/topics/bukyoku/iyaku/syoku-anzen/riskcom/01.html

と強調した。ところが、こうした法整備や政策的対応にも関わらず、2015 年日本年金機構の情報漏洩が社会問題になり、これをきっかけに 2020 年代初頭までを見据えつつ、サイバーセキュリティ政策の基本的な方向性を示す新たな国家戦略「サイバーセキ ュリティ戦略」が制定された。サイバーセキュリティ専門家育成の一環として、国家資格である「情報処理安全確保支援士」制度も始まった。

2015 年 12 月には経済産業省及び独立行政法人情報処理推進機構が「サイバーセキュリティ経営ガイドライン」を発表した。ガイドラインは、サイバーセキュリティは経営問題であり、知財など企業価値を守るため IT 及びセキュリティに対する投資を経営判断としてすべきであるとして、経営者が認識する必要のある 3 原則及び情報セキュリティ対策を実施する上でのトップとなる最高情報セキュリティ責任者（CISO）に指示すべき重要 10 項目について説明している。3 原則は、①経営者がリーダーシップをとって、経営に対して受容できるリスクのレベルを勘案し、サイバーセキュリティに投資する、②情報漏えいリスクの軽減のために、自社のみならず、系列企業及びビジネスパートナーのセキュリティ対策も策定する、③サイバーセキュリティ対策について関係者に説明し、コミュニケーションをとり、信頼を構築する、である。企業のサイバーセキュリティを重視し、サイバーセキュリティを保つために関係者が協力すること、コミュニケーションをとることが重要だという記述が登場する。政府省庁のサイバーセキュリティ体制から自治体のサイバーセキュリティ体制、企業のサイバーセキュリティ体制へ政策が拡大し、そして官民協力体制へと範囲が広がっている。

2016 年には「改訂サイバーセキュリティ基本法」公布、2017 年には「重要インフラの情報セキュリティ対 策に係る第 4 次行動計画」を発表し、各関係主体（重要インフラ事業者等、政府機関、情報セキュリティ関係機関等）の在り方として、多様な関係主体間でのコミュニケーションが充実していることを項目の一つに挙げ、コミュニケーションをうまく行うことで関係主体の連携、相互自主的な協力、統制の取れた対応ができると見た。さらに「リスクコミュニケーション」という言葉も登場する。リスクマネジメント及び対処態勢の整備のためにはリスクに関して情報を共有し協議するためにもコミュニケーション方案を確立しないといけないという見方だ。

官民情報共有のためのコミュニケーションに関しては、企業のサイバー攻撃による被害拡大防止のため、2011 年 10 月、独立行政法人情報処理推進機構と経済産業省、内閣サイバーセキュリティセンターが連携して企業とのサイバー情報共有イニシアティブ(J-CSIP : Initiative for Cyber Security Information sharing Partnership of Japan)を発足させた。重工、重電等、重要インフラで利用される機器の製造業者を中心に、情報共有と早期対応の場を作るためである。2017 年時点で「重要インフラ製造業者」「電力業界」「ガス業界」「化学業界」「石油業界」、「クレジット業界」、「自動車業界」、「資源開発業界」の 8 つの Special Interest Group から 154 の組織が参加している。独立行政法人情報処理推進機構と各参加組織（あるいは参加組織を束ねる業界団体）間で締結した秘密保持契約（NDA）のもと、参加組織およびそのグループ企業において検知されたサイバー攻撃等の情報を独立行政法人情報処理推進機構に集約。情報提供元に関する情報や機微情報の匿名化を行い、独立行政法人情報処理推進機構による分析情報を付加した上で、情報提供元の承認を得て共有可能な情報とし、参加組織間での情報共有を行っている。J-CSIP は、公的機関である独立行政法人情報処理推進機構を情報の集約点として参加組織間で情報共有を行い、高度なサイバー攻撃対策に繋げていく取り組みである。官民の情報共有は J-CSIP だが、民民(企業間同業種間)のサイバーアタック情報共有も積極的に行われている。金融 ISAC(Information Sharing and Analysis Center)、ICT-ISAC、電力 ISAC などがある。同業種間の情報共有を信頼できる第 3 機関の仲裁で横につなげた情報共有が J-CSIP といえる。

早期から各種戦略と法を制定した流れからすると日本は十分サイバーセキュリティ対策を取っているともいえるが、問題は複数の省庁が関わっているため、サイバーアタックや犯罪が発生した際にどこに情報を提供すればいいのか混乱が生じる可能性がある点である。電子署名・認証に関することは総務省、情報セキュリティ政策は経済産業省、サイバー犯罪対策は警察庁、全般的な政策は高度情報通信ネットワーク社会推進戦略本部（IT 総合戦略本部）、その他に官房長官が本部長のサイバーセキュリティ戦略本部、国家安全保障会議、内閣サイバーセキュリティセンターなどである。その他にも、個人情報保護委員会、独立行政法人情報処理推進機構（IPA）、国立研究開発法人情報通信研究機構（NICT）、国立研究開発法人産業技術総合研究所（AIST）、一般財団法人日本情報経済社会推進協会（JIPDEC）、日本銀行金融研究所情報技術研究センター（CITECS）、金融情報システムセンター（FISC）、日本ネットワークセキュリティ協会（JNSA）、JPCERT コーディネーションセンターなどの政府傘下団体があり、それぞれ相談窓口が設けている。また省庁や組織ごとに情報提供のフォーマットも違うため、企業にとっては負担になるしかない。

3-2 韓国の事例

韓国では、サイバーセキュリティは全ての企業がビジネスをする上で、もっとも気にすべきことの一つと

して重要性が高まっている。不正アクセス、ランサムウェア（企業のデータを勝手に暗号化して金品を要求する事件）被害や、IoT デバイスのハッキングなどにより企業の売上が急減するといったサイバー犯罪を数多く経験した。サイバーアタックで企業から漏えいした個人情報が振り込め詐欺用の口座開設に使えわれたことあり、盗まれた個人情報やデータを使った 2 次犯罪、3 次犯罪も問題になった。

韓国政府は 1970 年代から国家電算網普及拡張政策を実施、1994 年に情報通信政策を担当する省庁を設立、1996 年韓国情報保護センターを設立して官民協力体制を作り、情報保護と暗号化に関する研究・政策樹立を始めた。1998 年には情報保護システム評価認証制度を実施、インターネットサービス会社は政府が決めたガイドラインを守ってサイバーセキュリティ対策を講じるようにした。1999 年からは毎年官民共同でサイバーテロ模擬訓練を行っている。比較的早い時期から官民協力を意識した情報セキュリティ政策、サイバーセキュリティ政策をとっていたが、サイバーアタックを避けられなかった。2003 年 1 月には「インターネット大乱」と呼ばれる事件が発生した。韓国最大手通信キャリア「KT」の DNS サーバーがハッカーの攻撃を受け、全国で 9 時間インターネットに接続できなくなる事件が発生した。電子政府、電子メール、IP 電話、インターネットバンキング、企業のイントラネットなどインターネットにつながらないと利用できる全てのシステムが中断したことで、社会的に大混乱が生じ、経済的にも大きな打撃を受けた。この事件から韓国政府は国家の危機管理の一環としてサイバーセキュリティの重要性を認識するようになり、「サイバーアタック対応センター」を設立した。さらに、韓国政府は「Cyberkorea21」、「e-Korea」、「Broadband IT Korea」といったインターネットをより広く普及させ利活用を促進する戦略から、インターネットをより安全に使えるようにする政策へと方向を変えた。それまでは企業のサイバーセキュリティ対策は企業の経営判断に任せていたが、インターネットが使えなくなることはオンライン上の問題ではなく、実生活に多大な影響を与える脅威であるとの認識が広まり、サイバーセキュリティ認証制度を導入し、認証を受けた企業は政府の入札で優遇したり、企業のホームページ上に認証の有無を告知させたり、企業に対しても厳しくサイバーセキュリティ対策をとるようにした。

2010 年には、政府傘下機関である韓国インターネット振興院内にサイバーアタックワンストップ電話相談窓口「118」を開設した。電話窓口は 24 時間 365 日運営している。どこに連絡したらいいのかわからず被害拡大した問題を解決するためである。なりすまし電子メールの添付ファイルを開けてしまった、悪性コードを仕組まれたかもしれない、DDos 攻撃が発生した、ハッキングでデータを盗まれた、といった時にまずどこに連絡したらいいのかわからず対策が遅れ、被害がどんどん大きくなってしまうことを防ぐために、まずは 118 に電話するよう呼びかけている。個人も企業も 118 に電話するか、ホームページから相談できるよう窓口に一つにした。118 で集めたデータを韓国インターネット振興院が収集してサイバーアタック情報・犯罪などに分類し、それぞれ担当する組織、警察や政府機関に情報を提供し対策を求める。他の企業とも脅威情報を共有し、被害の連鎖を食い止める。これにより政府省庁も現場の実態を把握でき、官と民の間のサイバーセキュリティ政策的対応に関する温度差をなくせた。

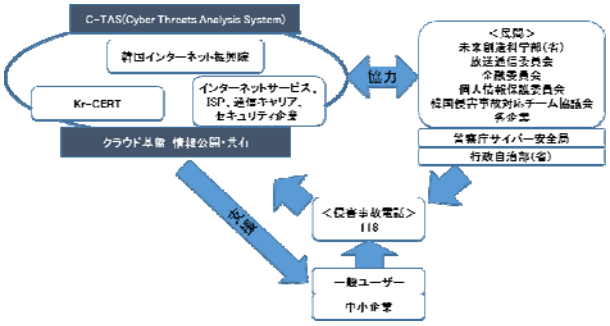
2014 年 1 月には情報保護準備度評価制度を導入し、企業が評価制度で高いレベルを獲得すれば政府の入札でもっと高い点数がもらえるようにし、企業が自発的にサイバーセキュリティ対策を行うことを狙った。強化制度の項目はサイバーセキュリティ投資割合、担当組織有無、担当者人数、個人情報保護法律違反回数など 30 項目で点数に応じて 5 段階評価している。政府のサポートにも関わらず、企業がサイバーセキュリティ対策を疎かにして大量に個人情報を流出させ国民に被害を与えた場合は厳しく処罰することにした。2017 年からはハッキングで顧客の個人情報を流出させた企業は、政府合同調査団の調査結果、サーバー管理者のパスワードを 1234、0000 など簡単な数字に設定して 10 年以上変更していなかった、セキュリティプログラムのアップデートを 1 年以上していなかったなど、明らかにサイバーセキュリティ対策を疎かにしていたことが原因と分かった場合、企業はハッキングの被害者ではなく加害者とみて売上の 3%に当たる課徴金を賦課するなど、企業に対する処罰を厳しくした。

2014 年 8 月には、韓国インターネット振興院が中心になり企業が政府に情報を提供する仕組みとして「C-TAS（Cyber Threats Analysis and Sharing System）[3]」を始めた。リアルタイムで悪性コード、ランサムウェア被害、データ盗難といったサイバーアタックやシステム侵害事故を企業が政府に提供し、政府は企業から収集したサイバーアタック情報を匿名で収集して分析し、重要な部分を他の企業と共有するクラウ

[3] 韓国インターネット振興院　https://www.krcert.or.kr/data/noticeView.do?bulletin_writing_sequence=25824 2018 年 6 月 30 日アクセス

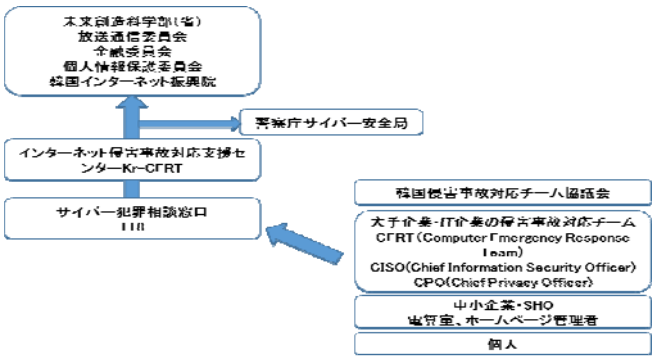
ドサービスである。これはサイバーアタックの防止と迅速な対応のため、政府と企業のサイバーセキュリティコミュニケーションを円滑にするための試みであった。C-TAS は企業が所定のフォーマットでデータを保存すると、クラウドコンピューティングでデータを統合保存、政府の専門家がプロファイリングと総合分析を行い、危険を探知する。分析結果は再度企業がサイバーアタックを予防できるよう企業に提供する。企業ごとに同じサイバーアタックや被害でも違う用語や表現を使うことがありデータがまとまらない可能性があったため、用語の標準化も行った。企業間ではサイバーアタック情報を企業秘密として明かさず、複数の企業が連鎖被害にあうこともよくあったが、C-TAS を使うことで企業名を明かすことなく情報をシェアできるので、現在どのようなサイバーアタックが起きているのか、または起ころうとしているのか企業から得た情報を政府が分析して再度企業に情報を提供、企業は政府の支援を得てすぐ対策をとれるようになった。企業のサイバーセキュリティ情報格差をなくすことで、中小企業も素早くサイバーアタックに対応できるようにする狙いもあった。C-TAS に参加しているのは政府機関、サイバーセキュリティ会社、ポータルサイト、インターネットショッピング、オンラインゲームなど約 100 社で、無料で参加できる。C-TAS の参加は任意もある。政府が企業から一方的に情報をもらうだけ、または企業が一方的に情報をもらうだけでは C-TAS は成り立たない。相互コミュニケーションで常に信頼できる情報が往復するようにコミュニケーションを促進しないといけない。

図 1　韓国の政府と企業間のサイバーセキュリティコミュニケーション



（韓国インターネット振興院の説明を元に筆者作成）

図 2　韓国のサイバーセキュリティワンストップ窓口「118」の仕組み



（韓国インターネット振興院の説明を元に筆者作成）

2017 年 3 月からは C-TAS の高度化のため、ビッグデータ分析・機械学習を C-TAS に導入、サイバー攻撃の類型や脅威情報を視覚化するダッシュボードを開発している。より多くの情報共有のためには C-TAS 参加企業を増やすべきだが、参加は任意なのでどうすれば参加企業をより増やせるのかが課題である。

官民の情報共有は C-TAS に一本化しているが、民と民の間の情報共有は日本と同じく ISAC があり、サイバーアタック情報を共有・分析している。韓国には情報通信 ISAC、教育 ISAC、エネルギーISAC、行政 ISAC、金融 ISAC があり日本や米国、英国など海外の ISAC と連携している。

韓国の場合、企業は ISAC にも参加するが、サイバーアタックの被害をすぐ公開しない企業も多く狭い範囲の同業種の間だけで個別コミュニケーションによって情報を共有することが多い。例えばポータルサイト

業界、オンラインゲーム業界、オンラインショッピング業界という具合で情報を共有した。そのため、同業種間は情報共有が盛んでも異業種間の情報共有がなく連鎖被害が大きかった。ハッカーがオンラインゲームサイトを攻撃してユーザーの ID とパスワードを盗み、ID とパスワードを使いまわしするユーザーが多いことからすぐオンラインショッピングサイトで同じ ID とパスワードを使って不正アクセス、オンラインショッピングサイトに保存されてある個人情報から住所やクレジットカード番号などを盗み詐欺に悪用するといったことが起きていた。オンラインゲームとオンラインショッピングの横のつながりがなかったため、ハッキング状況を共有できなかった。こうした問題を解決するためにも C-TAS が必要といえる。

2015 年には全省庁が参加する「K-ICT 戦略」、「K-ICT セキュリティイノベーション拡散戦略」、「K-ICT セキュリティ 2020」、「情報保護産業の振興に関する法律」が発表され政策に変化が見られた。これまでは情報化、ICT 利活用が先でサイバーセキュリティはおまけのような位置だったとすると、2015 年からはサイバーセキュリティ産業を韓国代表産業に育成する、情報システムに限らずインフラ設備全般においてサイバーアタック後の迅速な回復能力や未知の脆弱性を攻撃されても跳ね返せる力を持つ政策や組織を作る、外部からの攻撃に耐えて組織を持続させ安全な環境を保つ、そのために民間企業と協力する、人材養成に投資する、といった内容の政策に変わった。

2016 年 2 月には全省庁と通信事業者が参加する「サイバー侵害対応官民共同協議会」を発足、ランサムウェアと IoT に特化したサイバーセキュリティ官民コミュニケーション強化を図った。官民が共同でチームを作り、攻撃されやすい、または攻撃の踏み台として悪用されそうな IoT デバイス機種をモニタリングして、政府機関がデバイスの利用者へ連絡、アタックされないよう対策を教える制度である。共同協議会での合意により、悪性コードを仕組んだサイトは発見から 30 分以内に一般ユーザーがアクセスできないよう遮断できるようになった。民間企業だけでは解決できないユーザーの個人情報を政府機関が把握して連絡をとるなど官民連携でサイバー攻撃を未然に防ごうとしている。

2016 年 6 月には海外のサイバーセキュリティ会社が参加する「グローバルサイバー脅威インテリジェンスネットワーク」を開設した。サイバーアタックは国境を越えて行われている。2018 年ピョンチャン冬季オリンピックを狙ったサイバーテロが起こる可能性もあるため、韓国政府は海外企業との国際サイバーセキュリティコミュニケーションにも力を入れようとしている。ランサムウェア対策に特化した政府合同調査団も発足し、人質にされたデータを取り戻すための暗号解読技術研究も支援することにした。

韓国国会（2017）は、官民サイバーセキュリティ情報共有を活発するための課題として、企業にばかり情報共有を望むのではなく、官が共有する情報も重要だとした。官の情報をすぐ機密扱いにせず、詳細に分類して活かそうということである。また状況共有する官の範囲も拡大し、参加する組織を増やして分析できる情報を増やすことも必要であるとした。さらに、政府省庁を役割で管轄を決め縦割りにせず、サイバーセキュリティという価値中心に横につなげることで参加する組織を増やせる、どの組織も負担なくコミュニケーションに参加して情報を共有する仕組みが必要という政策提言だった。

3-3 米国の事例

米国の場合、2006 年国家機関であるアメリカ合衆国国土安全保障省の下に「サイバーセキュリティ＆コミュニケーション（Office of Cybersecurity and Communications）」部署を設置し、サイバーセキュリティコーディネーターをおいて省庁間情報共有・官民情報共有を指揮するようにしている。3000 人以上の個人と専門家の意見を反映した、サイバーアタック発生後の標準対策案といえる「サイバーセキュリティフレームワーク」も作成した。フレームワークは、政府政策と企業のルールがぶつかり逆にサイバーセキュリティ対策をうまくできないという民間企業の不満から始まったもので、現実とかけ離れたガイドラインや政策をなくすため、官民のコミュニケーションを頻繁に行う事から始め、効率よいコミュニケーション方法についてもまとめたフレームワークである。サイバーセキュリティ＆コミュニケーション部署の中には「全国サイバーセキュリティおよびコミュニケーション統合センター（National Cybersecurity and Communications Integration Center）」があり、24 時間 365 日のサイバー監視、インシデント対応、管理センターとして、インシデント情報を統合するポイントとして機能している。

米国では官民が共有するサイバーアタックの情報に顧客情報が含まれるのか、プライバシー侵害ではないか、どのような情報を共有するのかについては敏感であった。その結果、2015 年 12 月には官民のインシデント情報共有の実効性を高め、情報共有の範囲、情報共有によるプライバシー侵害免責などを取り決めた法律「Cybersecurity Information Sharing Act of 2015」を制定、情報共有及び分析組織「Information Sharing

and Analysis Organizations (ISAOs)」も設立した。

伊東（2010）はリスクマネジメントを推進していく上でリスク評価者と対象組織との間のリスクコミュニケーションには両者が考える主要な価値が同じであるという信頼性が重要であると評価したが、韓国の官民のサイバーセキュリティコミュニケーションにおいても、民の参加率は信頼性に比例するとみられる。官民がより効率的なサイバーセキュリティ対策を取るという主要な価値を共有し、政府機関に情報提供しても個人情報を侵害したと訴えられることがない、自社の経営や評判に支障をきたすことがないという信頼性が重要な影響を与えたとみられる。

4 まとめ

4-1 各国の特徴から見たサイバーセキュリティコミュニケーションの在り方

事例から官民のサイバーセキュリティ情報共有をより実効性のあるものにするためには、円滑で相互利益になるコミュニケーションが必要であることがわかった。

① ワンストップ窓口

企業が時間や手間をかけず情報共有できるようにする仕組み､共有情報フォーマットで集まったデータを有効に活用できるようにする。

日本の J-CSIP と韓国 C-TAS の特徴は企業が提供した情報は匿名で処理し、政府が収集した情報を分析して企業のためになる情報を返すという点、政府機関が企業から一方的に情報を吸い上げるのではなく収集した情報を政府省庁と共有・分析して再度企業のためになる情報を提供することで相互コミュニケーションが活発に起こるようにする点である。違いは以下の点である。J-CSIP は「重要インフラ製造業者」「電力業界」「ガス業界」「化学業界」「石油業界」、「クレジット業界」、「自動車業界」、「資源開発業界」の 8 つの Special Interest Group に分けて情報を管理しているのに対し､C-TAS はグループ分けせず主に情報通信業界の参加が多い。C-TAS は企業ごとにサイバーアタックに関する用語や表現が違うためフォーマットを作り用語も標準化した、その後オープン API を使ってデータの自動収集・分類で極力企業の手間をかけず情報を収集できるようにしている。

また韓国の 118 のように全国どこからでも誰でもサイバーセキュリティに関して 24 時間 365 日相談･通報できるコミュニケーション窓口の一本化は日本でも有効とみられる。日本の場合、総務省、警察庁、情報処理推進機構など窓口が複数ある。業務の縦割りで迅速な対応ができない可能性があるからだ。韓国は窓口一本化によりサイバーアタックの実態や攻撃者に関する情報を集めやすくなり俯瞰的視点が持てた。

② 協力のガバナンス変化

政府機関が企業の情報を吸い上げる情報共有ではなく、政府機関は調整者として情報を共有、収集した情報を分析して企業のリスクマネジメントに役立つよう情報を共有する水平的なコミュニケーションが必要である。

③ インセンティブ

サイバーセキュリティを疎かにし情報漏洩やシステム障害が発生した場合、漏洩した情報を別の犯罪に悪用する、一カ所にサイバーアタックで穴が開くとつながっている他のシステムに影響を及ぼして連鎖被害が発生、予想を超える広範囲で被害が発生するといった 2 次 3 次被害をもたらすため、経営ガイドラインといったマニュアルを実行したらインセンティブがある、実行しなかった場合の罰則があるといったことも必要である。米国の場合は、政府との情報共有に関しては顧客の個人情報を侵害したとみなさない、情報共有のためのモニタリングや政府と情報共有したことで企業に訴訟を起こすことはできない（訴追免責）といったインセンティブを適用した。韓国は官民協力体制構築、教育実施にも関わらずサイバーセキュリティ対策を疎かにし、初歩的なミス（ソフトウェアのアップデートをしなかった、セキュリティソフトを使用しなかった、管理者パスワードを 1234 のように簡単な数字にしたなど）人的ミスによる被害が発生した企業の処罰を厳格にした。

4-2 今後の課題

本稿では官民の情報共有のためのサイバーセキュリティコミュニケーションに焦点を当てたが、サイバーセキュリティは政府機関、公共機関、企業、一般ユーザーなどインターネットを使うすべての関係者の協力

が必要である。また、サイバーアタックに国境はないことから、官民協力は国内だけでなく国際協力体制を築くのも重要である。企業のサイバーセキュリティ担当者が社内の人に向けて行う内部コミュニケーション、サイバーアタックにより侵害事故が発生した企業が顧客に対して行う（被害状況や今後の対策などについて説明、謝罪など）対外コミュニケーション、海外からのアタックや国境のないサイバー犯罪に対応するために行う国際コミュニケーションに関しても研究を広げていきたい。

【参考文献】

伊東俊之（2010）,情報セキュリティにおけるリスクコミュニケーション,2010 年秋季経営情報学会全国研究発表大会要旨集

一般社団法人 JPCERT コーディネーションセンター（2015）,経営リスクと情報セキュリティ～CSIRT：緊急対応体制が必要な理由～, 2015 年 11 月 26 日

韓国行政研究院（2015）,A Study on Cyber Security Policy and Governance in the ICT Convergence Environment: Focused on“Authentication”,2015.12

韓国未来創造科学部（2015）,K-ICT 戦略,2015 年 5 月

韓国警察庁サイバー安全局（2015）,サイバー脅威情報活用方案研究,2015 年 10 月

趙章恩(2016)， 政府と企業間のサイバーセキュリティコミュニケーションに関する考察―韓国を事例に中心に, 2016 年経営情報学会秋季全国研究発表大会, 講演番号 A1-3

韓国情報通信戦略委員会（2016）, K-ICT 戦略 2016, 2016 年 5 月

韓国国会（2017）,第 4 次産業革命時代のサイバーセキュリティ』国会討論会,2017 年 9 月 25 日

経済産業省製造産業局ホームページ リスクコミュニケーション
http://www.meti.go.jp/policy/chemical_management/law/risk-com/r_index2.html 2018 年 6 月 30 日アクセス

厚生労働省ホームページ リスクコミュニケーションとは
www.mhlw.go.jp/topics/bukyoku/iyaku/syoku-anzen/riskcom/01.html 2018 年 6 月 30 日アクセス

Homeland Security, Information Sharing
https://www.dhs.gov/topic/cybersecurity-information-sharing, 2018 年 6 月 30 日アクセス

韓国インターネット振興院 https://www.kisa.or.kr/main.jsp, 2018 年 6 月 30 日アクセス

独立行政法人 情報処理推進機構 https://www.ipa.go.jp/index.html, 2018 年 6 月 30 日アクセス

内閣サイバーセキュリティセンター https://www.nisc.go.jp/, 2018 年 6 月 30 日アクセス

〈発 表 資 料〉

題　　名	掲載誌・学会名等	発表年月
韓国における官民サイバーセキュリティ協力体制に関する考察	日本情報経営学会第 74 回全国大会	2017 年 6 月
韓国における中小企業のサイバーセキュリティマネージメントと官民連携事例研究	2017 年経営情報学会秋季全国研究発表大会	2017 年 9 月
サイバーセキュリティコミニケション事例研究-韓国に おける官民協力体制の変化を中心に	情報経営学会第 75 回全国大会	2017 年 11 月
サイバーセキュリティコミュニケーションに関する日韓比較研究	第 8 回横幹連合コンファレンス	2017 年 12 月
日韓のサイバーアタック動向と政策的対応に関する考察	社会情報システム学シンポジウム	2018 年 2 月