官民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

A Study on Public-Private Cybersecurity Communication

趙　章恩 *
Changeun Cho

1. 研究背景

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やすくなることである。集めたデータを分析し、分析した結果を実生活で活かし、社会をより豊かにするためのデータ分析が繰り返しやすくなることも特徴といえる。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。

2014 年 11 月成立した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がサイバーセキュリティであると定義している。

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するため、完全無欠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。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 が機械学習をして攻撃を予防・対応できるようになる一方で、攻撃者もまた AI の機械学習で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

* 東京大学大学院情報学環

キーワード：サイバーセキュリティ、サイバーアタック、情報セキュリティ、コミュニケーション、官民協力

抜け道を探す攻防になるということである。

このような状況から、日本政府は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、サイバーセキュリティの強化を情報化政策の最優先課題にしている。

2. 先行研究と研究目的

近年、日本をはじめ、世界各国でサイバーセキュリティの強化を最優先課題にし、現状に照らし合わせサイバーセキュリティに関する法律や政策、ガイドラインの制定と改訂を頻繁に行う動きがある。中でも共通しているのは、官民協力や民間協力、国際協力など関係者の協力体制をよりよくしようという点である。

日本のサイバーセキュリティ基本法第三条では「サイバーセキュリティに関する施策の推進は、インターネットその他の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による情報の自由な流通の確保が、これを通じた表現の自由の享有、イノベーションの創出、経済社会の活力の向上等にとって重要であることに鑑み、サイバーセキュリティに対する脅威に対して、国、地方公共団体、重要社会基盤事業者（国民生活及び経済活動の基盤であって、その機能が停止し、又は低下した場合に国民生活又は経済活動に多大な影響を及ぼすおそれが生ずるものに関する事業を行う者をいう。以下同じ。）等の多様な主体の連携により、積極的に対応することを旨として、行われなければならない」、「サイバーセキュリティに関する施策の推進は、サイバーセキュリティに対する脅威への対応が国際社会にとって共通の課題であり、かつ、我が国の経済社会が国際的な密接な相互依存関係の中で営まれていることに鑑み、サイバーセキュリティに関する国際的な秩序の形成及び発展のために先導的な役割を担うことを旨として、国際的協調の下に行われなければならない」としている。

「多様な主体の連携」、「国際的協調」といったことが強調されているように、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、複数の組織が実効性のある協力関係を維持、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という必要性は認識しているが、具体的にどうしたらいいのだろうか。

情報化社会においてサイバーアタックの発生やサイバーセキュリティが保たれない状況に陥るのは社会の機能が止まることにもつながるため、自然災害と変わらない脅威となり得る。自然災害、化学物質や食品の安全管理に関する国家・社会・企業のリスクの評価、リスクの管理、協力体制に関しては、リスクコミュニケーションをテーマにした研究が多数ある。

厚生労働省（2018）によると、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。

文部科学省(2014)はリスクコミュニケーショ

ンを「リスクのより適切なマネジメントのために、社会の各層が対話・共考・協働を通じて、多様な情報及び見方の共有を図る活動」と定義し、「社会の関与者（ステークホルダー）はそれぞれがリスクのより適切なマネジメントのために果たしうる役割があり、ステークホルダー間で対話・共考・協働が積極的になされることが望ましい。各ステークホルダーが多様な情報及び見方を共有しようとする活動全体がリスクコミュニケーションと言える」とした。また文科省（2014）は日本のリスクコミュニケーションの課題を「リスクに関する問題解決を目指す取組のほとんどが個人のレベルで行われている。発信側の話題設定の範囲と受け手側の知りたい問題の範囲にズレがあることが少なくないなど、リスクコミュニケーションの基本的な視座を理解した取組が行われておらず、十分に機能していない」とし、そのため「リスクコミュニケーションの基礎的素養の涵養」、「問題解決に向けたリスクコミュニケー ションの場の創出」などを「今後のリスクコミュニケーションの推進方策」として策定した。

リスクコミュニケーションと情報セキュリティを組み合わせた研究として、伊東・廣松（2010）がある。伊東・廣松（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重要なのはリスク評価者（計画者）と対象組織が信頼関係を保つための連携（リスクコミュニケーション）だとした。リスクコミュニケーションとサイバーセキュリティを組み合わせた研究としては佐々木（2017）がある。佐々木（2017）は、今までのセキュリティ評価は脅威・資産・脆弱性を分けて考えたが、これからは資産・脆弱性・脅威を包括的にリスクととらえ、リスクは不確実性を伴うということを意識してセキュリティ評価を行い、関与者の合意が得られる最適案を導き出せるコミュニケーション・協議が行えるアプローチを考えないといけないとした。さらに、従来とは違う点として、IoT（Internet of Things、IP アドレスを持つデバイス類・各種センサーなど）普及により多くの関与者（経営者・顧 客・従業員など）が存在するため関与者間の合意が得られる新たなコミュニケーション手段が必要であり、複数のサイバーセキュリティリスク（ウィルス、個人情報侵害など）が同時に存在するため一つの対策だけではサイバーセキュリティを保つ目的の達成が困難であることから残存リスク等を最小化するための関与者間コミュニケーションも必要で、関与者を満足させられる新たな対応が必要であると提案した。

先行研究と文部科学省（2014）の議論をサイバーセキュリティにあてはめて考えてみると、「ステークホルダー間で対話・共考・協働が積極的になされること」、「各ステークホルダーが多様な情報及び見方を共有しようとする活動」はサイバーセキュリティの分野でも重視されている。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）があり、「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

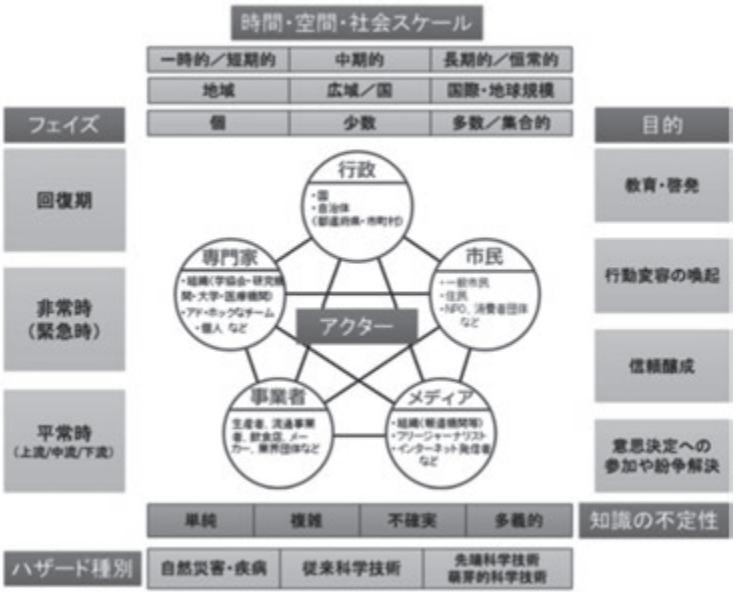

図 1.　リスクコミュニケーションの類型枠組
文科省（2014）p.4

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」という説明がある。先行研究は主に課題としてコミュニケーション不足を取り上げ、活発なコミュニケーションを目標に掲げるところに留まっている。コミュニケーションの過程に関する研究は少ないといえる。

経済産業省（2015）（2017）の「サイバーセキュリティ経営ガイドライン」は、日本で初めて具

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
組織内部のための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
情報共有のための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
外部向け事後対策 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

文科省（2014）、趙（2016）p.11 を元に著者が内容追加

体的に企業がすべきサイバーセキュリティ対策をまとめたガイドラインである。ガイドラインでは、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。

本稿ではサイバーセキュリティに特化したリスクコミュニケーションをサイバーセキュリティコミュニケーションとし、その方法と特徴について考察するため、以下のようにサイバーセキュリティコミュニケーションの分類を試みた。文部科学省（2014）が International Risk Governance Council のリスクコミュニケーション類型と日本の実例に照らし合わせ公開した、図1のリスクコミュニケーションの類型枠組みを参考にした。

図1のリスクコミュニケーション類型にあるコミュニケーションの主体であるアクターをみると、行政、市民、メディア、事業者、専門家がコミュニケーションの目的、フェイズ、スケール、ハザード種類など幅広く情報を共有するコミュニケーションの形になっている。この中でアクターと目的をサイバーセキュリティ分野に置き換えてみると、サイバーセキュリティの分野で行われているコミュニケーションモデルは大きく4つ考えられる。

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「組織内部のための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「情報共有のための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・事業者が外部に向け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「外部向け事後対策のための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情報共有に向けた「国際協力のためのコミュニケーション」である。

本稿では先行研究から一歩踏み込み、サイバーセキュリティにおけるリスクコミュニケーションをどのようにすればいいのかを考察するため、主に日本（内閣サイバーセキュリティセンター[2]）・韓国（インターネット振興院 Korea Internet & Security Agency[3]）・米国（United States Department of Homeland Security[4]）の政府機関ホームページにあるサイバーセキュリティ政策資料を元にサイバーセキュリティ政策の変化を調べ、重要視されているサイバーセキュリティ政策としてのコミュニケーション、「多様な主体の連携」の中でも主に政府と企業の間で行うサイバーセキュリティにおける実効性のあるコミュニケーション方法に焦点を当てている。官民の間で情報共有を活発にするために取り組んだ事例を比較し、円滑なコミュニケーションを行うための政策変化と各国の特徴について研究を行い、日本、韓国、米国の官民のサイバーセキュリティ分野での情

報共有・共同対策事例と政策の変化の流れを考察した。

本稿は第8回横幹連合コンファレンスで発表した趙（2017）の論文を加筆・修正したものである。

3. サイバーセキュリティ政策とサイバーセキュリティコミュニケーションに関する動向

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。

経済産業省（2015）（2017）の「サイバーセキュリティ経営ガイドライン」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。2017 年にはガイドラインの改定を行い、経営者が CISO 等に指示すべき 10 の重要事項を見直し、「関係者とのコミュニケーション：情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供」を追加した。

2016 年には「改訂サイバーセキュリティ基本法」を公布、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した。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をどうするか明確な方法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がある。さらに、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われたこともあり、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ない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。

韓国の場合は、サイバーセキュリティ政策が侵害事故のスピードに追い付かず、常に事後対策としてサイバーセキュリティ政策を改定する中で官民のサイバーセキュリティコミュニケーションの必要性を痛感し、体制を整えていったのが特徴である。

ソンヘリョン（2015）は、韓国で2009年7月7日発生したサイバーアタックの事例をリスクコミュニケーションの失敗事例として取り上げた。大統領官邸や国会、政府省庁のウェブサイト、インターネットバンキング、インターネットポータルサイトなどに72時間近くアクセスできなくなり社会が混乱に陥った。通常ウェブサイトにアクセスできなくする攻撃は金銭目的が多いが、2009年のサイバーアタックは社会の混乱を狙ったサイバーテロであった。韓国はサイバーセキュリティ関連法律やガイドラインはあったが、官民の協力体制がなくどのようにコミュニケーションすればいいのかわからなかったため政府省庁と企業がそれぞれ情報を集め解決策を模索するしかなかった。その結果、間違った情報が拡散し社会の不安が増したことや事後対策が遅れたことを指摘した。政府省庁間の協力体制もなく、省庁ごとに違う対策を発表したことも事後対策が遅れる原因となった。また国民に対するサイバーセキュリティキャンペーンや教育、政府関係者のサイバーアタック模擬訓練は行っていたが、2003年1月の「インターネット大乱」から6年が経過しサイバー

セキュリティが実生活の脅威になるという認識が薄れていたこともあり、効果がなかったと分析した。

ソンヘリョン（2015）はさらに、「リスクは完全に取り除けるものではなく常に管理するしかない。リスク管理は信頼に基盤しないと効果がない。信頼を得るためには幅広い利害関係者の参加が必要であり、参加によってリスクをより効果的に統制できる。信頼がないと専門家が安全と言ってもその他大勢は安心せず社会に混乱が生じる。信頼関係は相手が何を考えているのか、同じ価値観を共有しているのか、これからどのようなことをするのかを把握しないと築けない。そのためにコミュニケーションが必要になる。コミュニケーションの過程を管理することがリスク管理の核心である」とし、2009年当時の韓国は政府と企業をはじめ、関係者の間で信頼を築けるコミュニケーションがなかったため、リスクを効果的に統制できなかったと分析した。

2009年の失敗をもとに、韓国はサイバーセキュリティにおけるリスクコミュニケーション、特に官民協力のためのサイバーセキュリティコミュニケーションに力を入れるようになった。

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電話相談窓口サイバーワンストップセンター（サイバー民願センターともいう）「118（局番なし）」を開設した。電話とホームページの窓口は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が拡大するといっ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

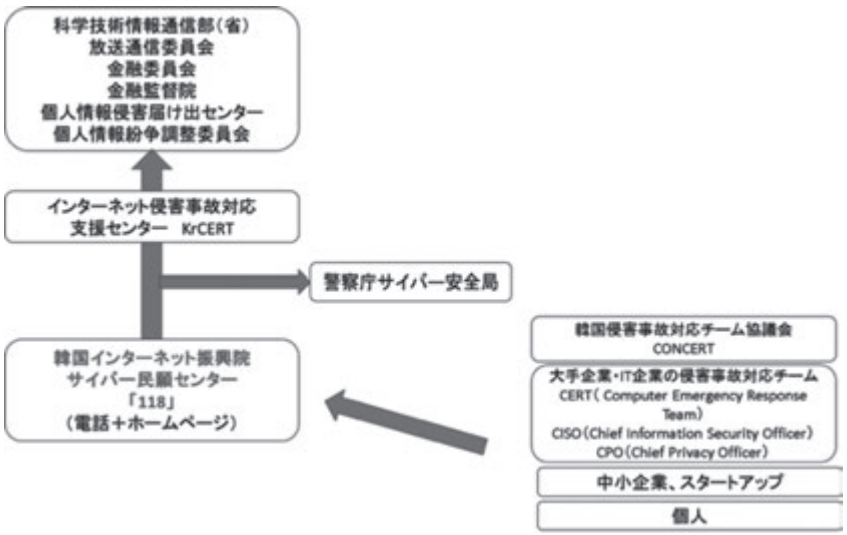

図2.　韓国のサイバーセキュリティワンストップ窓口「118」の仕組み
趙（2016）p.10を元に著者が更新

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した。

2014 年 1 月には「情報保護準備度評価制度」を導入、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）」[5] 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 は侵害事故情報の収集（情報収集とプロファイリング）、侵害事故総合分析（危険探知と相関分析）、情報共有のプロセスで行われる。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の参加は任意である。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。コミュニケーションを促進するためにはC-TASの正確性・信頼性が重要であり、信頼性を保つために政府機関である韓国インターネット振興院がコーディネーター役として間に入っている。

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。近年、データが付加価値創出の中核となっていることから「情報＝資産」の認識が強くなっており、情報共有を忌避する企業が出ていることもあり、企業のサイバーセキュリティに関する情報とその他の情報を分けて考えてもらう必要もありそうだ。

韓国の場合、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

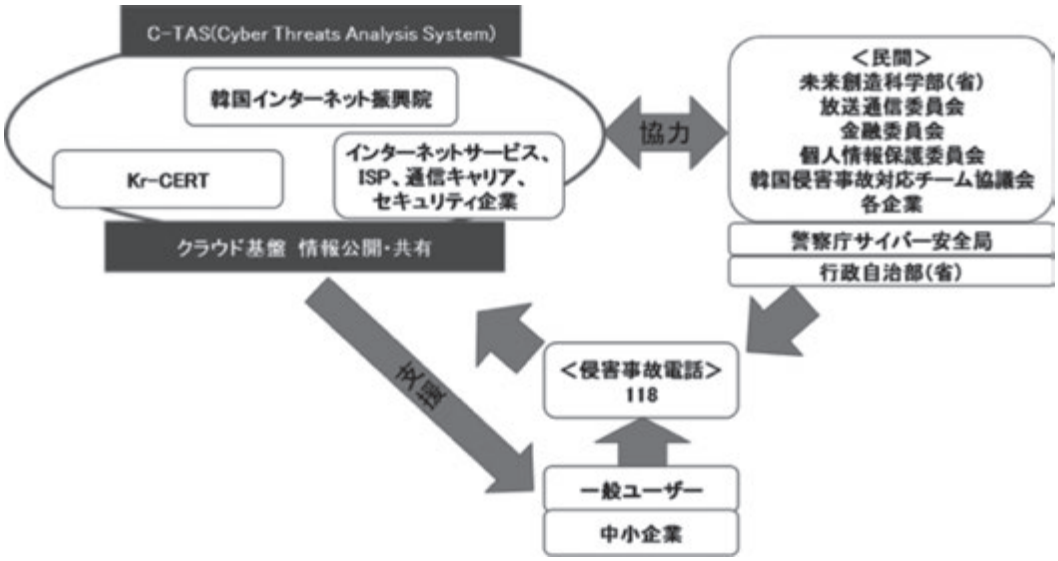

図3.　韓国の政府と企業間のサイバーセキュリティコミュニケーションモデル
趙（2016）p.10

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。実際 2014 年 C-TAS が稼働してからは、2003 年や 2009 年より規模が大きいサイバーアタックが発生しても予防から事後対策までの対応をより迅速にでき、まとまった対策をたてられたため社会が混乱に陥る様子は見られなかった。

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ったため、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た。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。また情報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・廣松（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、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 日本・韓国・米国の官民サイバーセキュリティコミュニケーションの特徴

事例から日本・韓国・米国のサイバーセキュリティ政策は官民のサイバーセキュリティ情報共有を重視する傾向にあることがわかった。また、官民の情報共有をより実効性のあるものにするため積極的に取り組んでいる部分として（1）ワンストップ窓口・利便性、（2）協力のガバナンス変化・信頼性、（3）インセンティブ・活発な参加を促進できる仕掛けをあげられる。

（1）ワンストップ窓口・利便性

官民のサイバーセキュリティ情報共有を活発にするには、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ためワンストップ窓口が有効だった。

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・信頼性

韓国と米国の事例をみると、官民のサイバーセキュリティ情報共有は、政府機関が企業の情報を吸い上げる一方的な情報共有ではなく、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

表２：日本・韓国・米国の官民サイバーセキュリティコミュニケーション特徴

	ワンストップ窓口・利便性	協力のガバナンス変化・信頼性	インセンティブ・活発な参加
日本	○	○	
韓国	○	○	○
米国	○	○	○

筆者作成

ションになったことで信頼性を保ち、情報共有が持続し活発になった。特定企業の利益追求のための情報共有ではなく、政府機関がコーディネーターになることで信頼性を維持する必要もあった。

（3）インセンティブ・活発な参加

企業が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、漏洩した情報が別の犯罪に悪用される、サイバーアタックで一カ所に穴が開くと連動している他のシステムにも影響を及ぼして連鎖被害が発生する、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。

韓国の場合、官民協力体制を構築し、教育を実施した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､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）や人的ミスを起こして被害が発生した場合、企業に対する処罰を厳格にした。政府機関が公表したサイバーセキュリティ経営ガイドラインを守ったにも関わらず被害が発生した場合は、政府が専門家を企業に派遣して被害が拡大しないよう手助けする。

米国の場合、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。

日本でも２次被害３次被害の可能性を念頭に置き、官民一体となって対策を取るためにも、経済産業省が公表した「サイバーセキュリティ経営ガイドライン」といった政府機関が提示したルールを守ったにもかかわらずサイバーアタックによって被害が発生した場合は救済策を提供するインセンティブを、守らなかった場合は罰則を強化するといったことも必要になるとみられる。

4.2 今後の課題

本稿では先行研究でサイバーセキュリティの課題と目標として取り上げられた活発な情報共有、コミュニケーションの過程に焦点を当てた。政府と企業の間の官民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注目し、３国がどうしてサイバーセキュリティコミュニケーションに力を入れているのかその背景や政策の変化を調べ、官民サイバーセキュリティコミュニケーションの取り組みと３国の特徴を考察した。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ため、サイバーセキュリティにおける関係者のコミュニケーション過程に関する研究は重要と考えられる。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き、より迅速な対応ができる国際協力に向けたサイバーセキュリティコミュニケーションの過程も分析する必要がある。サイバーセキュリティ政策や官民協力のモデルにおいて新しい動きが多い先進事例が多い欧州で2018年5月25日から適用開始された「EU一般データ保護規則（GDPR）」の影響による官民情報共有の変化なども追加調査し、国際比較として発展させていくこと、現状把握と特徴を見出した事例調査から定量的分析へ発展させ官民サイバーセキュリティコミュニケーションの実効性を示すことが今後の課題である。

謝辞

本研究は電気通信普及財団の研究調査助成を受けたものである。

註

[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10月13日アクセス）

[2] 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）

[3] 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）

[4] The Department of Homeland Security, Information Sharing
https://www.dhs.gov/topic/cybersecurity-information-sharing（2018年6月30日アクセス）

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

参考文献

伊東俊之，廣松毅（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』https://www.jstage.jst.go.jp/article/jasmin/2010f/0/2010f_0_20/_article/-char/ja/　2018年10月13日アクセス

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日公表
https://www.jpcert.or.jp/csirt_material/files/csirt_for_management_layer_20151126.pdf2018年10月13日アクセス

韓国インターネット振興院（2013）「国内主要インターネット事故経験から見た侵害事故現況」『Internet & Security Focus』2013年9月号

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

韓国未来創造科学部（2016）「K-ICT 戦略2016」2016年7月11日
https://www.msit.go.kr/web/msipContents/contentsView.do?cateId=mssw11211&artId=1302053　2018年10月13日アクセス

韓国行政研究院（2015），「A Study on Cyber Security Policy and Governance in the ICT Convergence Environment: Focused on “Authentication”」『基本研究課題2015』2015年12月

韓国未来創造科学部（2015）「K-ICT 戦略」2015年3月25日
https://www.msit.go.kr/web/msipContents/contentsView.do?cateId=mssw315&artId=1256544　2018年10月13日アクセス

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

経済産業業（2015）「サイバーセキュリティ経営ガイドライン Ver1」2015年12月28日公開

経済産業業（2017）「サイバーセキュリティ経営ガイドライン Ver2.0」2017 年 11 月 16 日公開
経済産業省製造産業局（2018）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 10 月 13 日アクセス
厚生労働省（2018）リスクコミュニケーションとは
https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/shokuhin/syokuchu/01_00001.html　2018 年 10 月 13 日アクセス
佐々木良一（2017）「IoT 時代の リスク評価・リスクコミュニケーション」『2016 年度第 4 回 IT リスク学研究会講演』 2017 年 2 月 20 日　http://www.jssm.net/wp/wp-content/uploads/2017/02/ 佐々木 IT リスク学用 IoT 時代のリスク評価法に関する考察 .pdf 2019 年 2 月 21 日アクセス
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予稿集』pp.9-12 講演番号 A1-3　2016 年 9 月 15 日
趙章恩（2017）「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』講演番号 A-2-4　2017 年 12 月 2 日
文部科学省科学技術・学術審議会 研究計画・評価分科会 安全・安心科学技術及び社会連携委員会（2014）「リスクコミュニケーションの推進方策」 2014 年 3 月 27 日公開
http://www.mext.go.jp/b_menu/shingi/gijyutu/gijyutu2/064/houkoku/__icsFiles/afieldfile/2014/04/25/1347292_1.pdf　2019 年 2 月 21 日アクセス
송해룡（2015）「한국 실패 사례에서 배우는 리스크 커뮤니케이션 전략　6 장 7·7 디도스 공격 사태」『커뮤니케이션이해총서』커뮤니케이션북스（ソンヘリョン（2015）「韓国の失敗事例から学ぶリスクコミュニケーション第 6 章 7.7DDos 攻撃」『コミュニケーション理解叢書』コミュニケーションブックス）

趙　章恩（ちょう・ちゃんうん）
［**生年月**］1974 年 6 月
［**出身大学または最終学歴**］韓国梨花女子大学卒業、東京大学大学院学際情報学府博士課程単位取得満期退学
［**専攻領域**］社会情報学、サイバーセキュリティ政策、放送通信政策
［**主たる著書・論文**］
『メディア・ローカリズム』（共著、中央経済社、2019）
「インターネット上の海賊版サイト対策に関する日韓比較」、『情報文化学会講演予稿集 26』、（2018 年）
「サイバーセキュリティ人材育成方案に関する日韓比較」、『情報経営学会第 77 回大会予稿集』、（2018 年）
［**所属**］東京大学大学院情報学環・特任助教
［**所属学会**］社会情報学会、情報経営学会、情報文化学会、情報通信学会

A Study on Public-Private Cybersecurity Communication

Changeun Cho*

It is an era supposed that there is no technology or policy that can completely defend cyber attacks. That actually cause damage to society such as the leakage of a lot of personal information, corporate confidentiality and stop supplying of infrastructure. The Cyber Security Center of the Ministry of Economy, Trade and Industry has announced strategies in December 2015, because of maintaining cyber security is a very important issue from the viewpoint of people's lives, social economic activities, and security and crisis management. The Ministry of Economy, Trade and Industry established “Cybersecurity Management Guidelines” and instructed companies to disclose information on cybersecurity risks and countermeasures and to proper communication with stakeholders. However, it is vague about what to do specifically to make "proper communication". It is effective that not only companies and government struggle within their own organizations, but multiple groups maintain adequate cooperative relationships, communicate positively, and raise the level of security. This paper compares policies and countermeasures of Japan, Korea and the United States, and considering the way of cyber security communication between public and private. International comparison shows that easy and mutually beneficial communication is necessary to make cyber security information share effectively between public and private. According to the case studies, the following three were necessary to facilitate cyber security communication between public and private: Simplification of government cyber security department, changing governance of cooperation, and offering incentives.

* Interfaculty Initiative in Information Studies Project Assistant Professor

Key Words：Cybersecurity,Cyberattack,Information security,communication,public-private partnership.