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　　趙　章恩　　東京大学　大学院情報学環　特任助教

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て分析、分析した結果を実生活で活かし、もう一度そのデータを集めて分析して社会をより豊かにしようとするデータ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。

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サイバーセキュリティの強化を最優先した政策が必要である。

2　先行研究と研究目的

サイバーセキュリティの強化を最優先課題にしている日本をはじめ世界各国で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が頻繁に行われる中、共通しているのは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も「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」とした。

「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、協力体制に関する研究としては、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。

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として、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。佐々木（2017）は、今までのセキュリティ評価のアプローチ法は脅威・資産・脆弱性を別々に分けて考えたが、これからは資産・脆弱性・脅威を包括的に考慮することをリスクととらえ、リスクを重視したアプローチが重要であること、多くの関与者（経営者・顧 客・従業員など）が存在する 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）が普及してから多くの関与者間の合意が得られるコミュニケーション手段が必要なリスク評価と対策を導く方法を考えなくてはならないことを指摘した。

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。

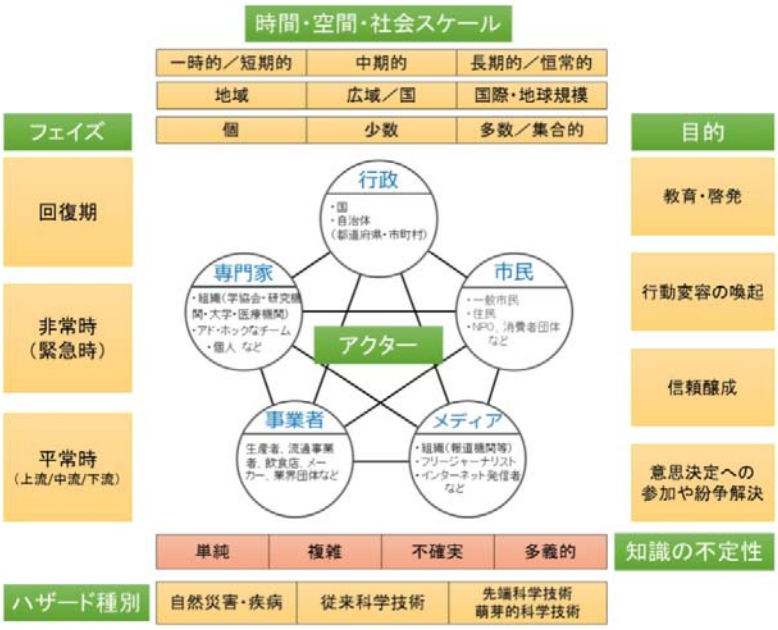
文部科学省（2014）の議論をサイバーセキュリティにあてはめて考えてみると、「ステークホルダー間で対話・共考・協働が積極的になされること」、「各ステークホルダーが多様な情報及び見方を共有しようとする活動」はサイバーセキュリティの分野でも重視されている。一般社団法人 JPCERT コーディネーションセンター（2015）が提案したサイバーセキュリティ対策の一つとしてリスクコミュニケーション（報告・情報公開）では、「インシデント対応は、ともするとインシデントが発生したことの隠蔽も含む、内向きの処理に終始しがちである。しかし、適法性だけでなく適正性にも配慮すれば、利害関係者に対しリスクの存在やインシデントの影響、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）は 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、図 1 のリスクコミュニケーションの類型枠組みを公開した。

図１　リスクコミュニケーションの類型枠組



文科省（2014）pp. 4

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。

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)PP. 11 を元に著者が内容追加

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。

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、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った。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。

3　海外のサイバーセキュリティコミュニケーションに関する事例調査

3-1 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。

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いけない。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、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。

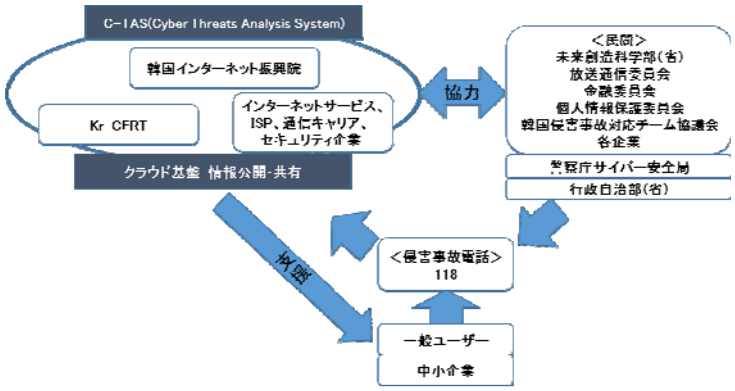
2014 年 1 月には「情報保護準備度評価制度」を導入、企業が評価制度で高いレベルを獲得すれば政府の入札でもっと高い点数がもらえるようにし、企業が自発的にサイバーセキュリティ対策を行うことを狙った。強化制度の項目はサイバーセキュリティ投資割合、担当組織有無、担当者人数、個人情報保護法律違反回数など 30 項目で点数に応じて 5 段階評価している。政府のサポートにも関わらず、企業がサイバーセキュリティ対策を疎かにして大量に個人情報を流出させ国民に被害を与えた場合は厳しく処罰することにした。2017 年からはハッキングで顧客の個人情報を流出させた企業は、政府合同調査団の調査結果、サーバー管理者のパスワードを 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。

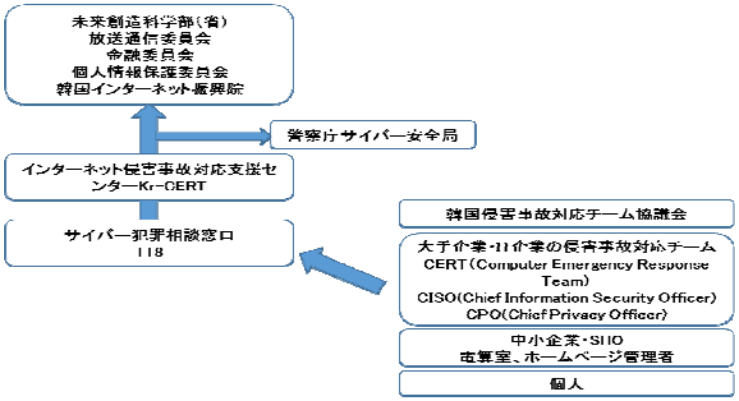
C-TAS に参加しているのは政府機関、サイバーセキュリティ会社、ポータルサイト、インターネットショッピング、オンラインゲームなど約 100 社で、無料で参加できる。C-TAS の参加は任意である。政府が企業から一方的に情報をもらうだけ、または企業が一方的に情報をもらうだけでは C-TAS は成り立たない。コミュニケーションを促進するためには C-TAS の正確性・信頼性が重要であり、信頼性を保つために政府機関である韓国インターネット振興院がコーディネーター役として間に入っている。

図 2　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）pp. 10

図 3　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）pp. 10

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に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 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。

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。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。

2018 年以降の変化としては、データ利活用を重視するデジタル・ガバメントへ移行しながら、データ収集・活用とセキュリティのバランスをどうするか、といったことも政策に反映されるようになった。韓国行政安全部の「電子政府 50 年史」によると、韓国では 2007 年電子政府のさらなる発展とデータ活用の効率を向上するため行政データベース標準化、行政用語標準化を行い、「電子政府具現のための行政業務等の電子化促進に関する法律」を「電子政府法」に改訂、急変する情報化推進環境に対応するため行政データの共同活用対象を行政機関から公共機関と学校に拡大し、行政情報のサイバーセキュリティを強化するための条項を追加した。

この改訂に伴い、電子政府の安全性の強化とデータ保護のため「電子政府サービスセキュリティ委員会」を発足、電子政府サイトのセキュリティ脆弱点分析を行った。また、全省庁が協力して電子政府のサイバーセキュリティ対策を樹立し、サイバーアタック対応業務を行うことにした。中央政府と 16 の自治体が参加する電子政府サイバー侵害事故対応協議会（G-CERT）も組織、個人データを大量に保存している自治体の情報セキュリティも強化した。2007 年から毎年、個人情報保護システム・データ保護システム・データ管理体制・電子政府担当者のサイバーテロ訓練結果などを重点評価し、サイバーセキュリティ水準を一層強化するよう

にした。

2010 年には再度電子政府法を改訂して行政データの共同活用対象を拡大すると同時に、情報保護対策を強化するため行政データを利用する全ての公共機関で「電子政府情報保護責任官」を指定するようにした。行政データ管理者の役割と責任を明確にし、行政データ流出及び未許可保存・誤用・乱用など禁止行為の処罰をより厳しくした。また電子文書の効力を認め、全ての添付書類は電子的に処理するようにした。

行政安全部の 2018 年 1 月 21 日付報道資料によると、『電子政府 2020 基本計画』に基づくサイバーセキュリティ政策として 2018 年現在もっとも力を入れているのは、民間企業と協業できる新しい電子政府エコシステム造成のために必要な民間データベースとの連携に備え、情報漏えいやシステム破壊といった危険を認識し能動的に自己防衛する人工知能活用サイバーセキュリティシステム構築である。電子政府システム統合センターには約 2 万 6000 台の電算装備がある。膨大なログデータを分析して能動的にデータとシステムを守るため人工知能を活用する。新しい攻撃を予測、脆弱点を識別するといった進化し続ける攻撃手法に機敏に対応するためには人がモニタリングするのではなく、システムアクセスログの中で非正常行為を人工知能が自らみつけて攻撃を遮断する、既知の攻撃から守るだけでなく、新しい侵害類型を見破る力があるサイバーセキュリティ対策が必要である。予防・管制・対応・分析を人工知能で自動化して人は難易度の高い意思決定だけ支援する方式に変えていく。

韓国の場合、行政業務の電子化、各種手続きのオンライン化、公共データの開放、行政データの共同活用対象拡大を進めてきたが、官民を超えたデータ流通、民間サービスまで含めたワンストップ・サービスを提供するというところまでは至らず、日本の『デジタル・ガバメント実行計画』にある 3 段階目に留まっている。行政と民間の壁を超えたデータ連携とサイバーセキュリティ対策が今後の課題といえる。

官民データ連携のためには情報の保護と活用のバランスが重要になるだろう。韓国の場合、60 年代から行政電算化を始め、2002 年 G4C 電子政府を開始、後からサイバーセキュリティ対策を強化した。2007 年より全省庁と自治体が参加する電子政府サイバーセキュリティ政策樹立、サイバーアタック対応組織、電子政府サイバーセキュリティ政策評価を行ってきた。2016 年からは日本の『デジタル・ガバメント実行計画』に近い『知能型電子政府』を目指す計画を発表し、膨大なデータを分析して能動的にデータとシステムを守る AI 活用サイバーセキュリティ導入、経験豊かな民間のサイバーセキュリティ専門家を公務員として採用、専門家が外部から参加するのではなく内部者として知能型電子政府を積極的に守れるようにした。韓国は ICT 進化に沿って随時電子政府法を改訂しながらサイバーセキュリティ対策をアップグレードしてきた。

内閣サイバーセキュリティセンターのサイバーセキュリティ戦略本部が 2018 年 6 月 7 日公表した『官民データ活用推進基本計画の案に対するサイバーセキュリティ戦略本部の意見』によると、「官民データ利活用社会の実現は重要であるが、今後官民のデータ利活用が進展すれば、データの真正性・完全性の重要性が増し、それを毀損するような IoT、サプライチェーン、オープンイノベーションの脆弱な部分を狙う動きや意図しない動きが発生し、政府機関や重要インフラ事業者だけでなくそれ以外の事業者及び個人に対しても深刻な影響が生ずる可能性が高まり、国民生活への脅威が更に深刻化することが予想される」という。このような問題に備え、「官民データが安全に利活用できるよう、官民の各主体が各々の役割を認識し、連携してサイバーセキュリティ対策を強化することが官民データ流通の基盤強化にもつながる」と提案している。さらにサイバーセキュリティ戦略本部は「関係するそれぞれのシステムについて、その企画・設計段階からセキュリティの確保を盛り込む（セキュリティ・バイ・デザイン）とともに、インシデント等が発生した場合に備えた対応体制が適切に整備されているかに配意することが必要である」とも提案している。このセキュリティ・バイ・デザインは日本の『デジタル・ガバメント』、韓国の『知能型電子政府』の根幹になるデジタル改革の基盤整備、官民データ連携において非常に重要な要素になるとみられる。

韓国政府は 2019 年 1 月、「民間部門情報保護総合計画 2019」を発表した。5G 商用化によって、IoT がさらに日常に浸透する中、IP カメラのハッキング、スマート家電やスマートファクトリーのロボットを乗っ取るランサムウェア事件など、ネットワークの高度化に合わせたサイバーアタックも進化した。韓国が目指す 5G ベースデジタル経済発展計画を支えるため、ビッグデータと人工知能を使ったサイバーセキュリティ体制を整え、予測能力向上と早期遮断を目指す。そのために官民協力を強化するため、IoT の脆弱点点検システムを構築し、積極的に協力する企業にはインセンティブとしてインフラ保護関連研究開発資金を支援する。サイバーセキュリティに国境はないことを考慮し、海外の政府や企業とも官民協力を強化することにした。

3-2 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。さらに 2015 年から、官民の間で迅速で効果的なサイバーセキュリティ対策を立てるため、サイバーセキュリティ情報共有促進行政命令「EXECUTIVE ORDER - Promoting Private Sector Cybersecurity Information Sharing」も推進した。

3-3 欧州の事例

EU は 2017 年、「Resilience, Deterrence and Defence : Building strong cybersecurity for the EU」という共同声明を発表した。サイバーセキュリティに対するレジリアンス強化、サイバーアタック予測能力強化、サイバーセキュリティに関する国際協力強化を目指し、欧州全体でワンストップ窓口を作り、ここで最新のサイバーアタック情報を取りまとめ、実効性のある対応方案を提示、サイバーアタックによる被害者を助けることにした。欧州企業はもちろん、欧州でビジネスをする全ての企業が一定のサイバーセキュリティを守るよう認証フレームワーク（EU Cyber Security Certification Framework）を開発し、ソフトウェアやインターネットサービス、ICT 製品はデザインの段階からサイバーセキュリティを考慮する「security by design」の考えを守るよう呼びかけた。認証フレームワークは 2023 年まで 3 つの段階を決め、企業が自社のサイバーセキュリティはどの段階なのか表示し、ユーザーがそれを見て選択できるようにする。

EU はサイバーアタックが欧州のデジタル単一市場と経済、社会全体を滅ぼす可能性があるとして、2016 年よりサイバーセキュリティ研究資金として 4.5 億ユーロを投資、その 3 倍の額を民間企業が投資するよう呼びかけている。主にエネルギー、医療、交通、金融産業のためのセキュリティサービスと製品開発を助けるための投資を行うという。

欧州のサイバーセキュリティ戦略と官民協力体制構築は 2000 年代から始まっている。欧州委員会（EC）は 2004 年 EU 加盟国のネットワークと情報セキュリティをサポートするため「欧州ネットワーク情報セキュリティ庁（European Network and Information Security Agency、ENISA)」設立し国家間情報共有拡大を図った。2010 年には「欧州 2020 戦略（Europe 2020)」を発表した。欧州のスマートかつ持続可能で包容的な成長のために、デジタル単一市場の構築という目標のもと、サイバー犯罪にも効果的に対応するため Europe 2020 の中に「欧州デジタルアジェンダ（Digital Agenda for Europe)」を定め、さらに 7 つのアジェンダを提示した。7 つのうちの一つが「情報セキュリティの強化と信頼の構築」である。欧州全体にとって重要な項目としてサイバー安全保障とデジタルプライバシーが選ばれた。欧州のデジタル単一市場構想にとって何よりも重要なのは信頼と安全であることがうかがえる。サイバー犯罪に効果的に対応するため、2012 年には EU 侵害事故対応チーム（Computer Emergency Response Team、CERT）を創設、2013 年にはヨーロッパサイバー犯罪センター（European Cybercrime Center、EC3）を開所した。

2013 年には欧州連合（EU）も「EU サイバーセキュリティ戦略（Cybersecurity Strategy of the European Union：An Open、Safe and Secure Cyberspace)」を発表し、サイバーセキュリティと信頼構築に関する戦略を取り決めた。加盟国・EU 当局・民間企業が参加する情報共有体制を構築し、サイバー脅威の予防と迅速な対応を目指した。そのために果たすべき役割と責任、サイバーセキュリティを守るために取るべき体制など

を具体的で拘束力を持つよう取り決めていった。

EC が 2015 年に発表した欧州セキュリティアジェンダ（European Agenda on Security）は、欧州全体でサイバー犯罪に対処しようとする内容が盛り込まれた。2016 年に発表した NIS 指針(The Directive on Security of Network and Information Systems)は、加盟国の NIS 担当機関や情報セキュリティ・インシデント・チーム（CSIRT）などを通じたサイバーセキュリティ能力の向上、加盟国間の戦略的協力と情報共有体制整備、経済や社会に重要なサービス（エネルギー、交通、水、金融、医療など）提供者と、検索エンジン、クラウドコンピューティング、電子商取引などのデジタルサービスプロバイダーに適切なセキュリティ対策を講じさせ、サービスに重大な影響を与えるサイバーアタック兆候の報告、この 3 つを義務付けた。

欧州は地域的特徴から、加盟国の官官サイバーセキュリティコミュニケーションが盛んに行われていた。ユーロポール（European Police Office）と欧州ネットワーク情報セキュリティ庁（ENISA)、侵害事故対応チーム（CERT-EU）は欧州全域のサイバーセキュリティ強化とよりよい解決策を提示することを目標に随時情報共有するだけでなく、捜査・分析・追跡・訓練・人材育成・戦略樹立などあらゆる面で協力している。

4　官民サイバーセキュリティコミュニケーションの在り方

事例から韓国・米国・欧州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、利害関係者全員の参加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するために必要な点、情報共有が長年続いている事例の共通点として（1）標準化、(2）ワンストップ窓口・利便性、(3）相互信頼、(4）インセンティブ、この 4 つをあげられる。

4-1 標準化

官民のサイバーセキュリティ情報共有のためにはまずどのような情報を共有するのか、情報の範囲や用語の標準化を考えないといけない。韓国の C-TAS は主に情報通信業の企業が参加しているが、業種に関係なく参加する企業を増やそうとしている。そのため、C-TAS は企業ごとに違っていたサイバーアタックに関する用語や表現を取りまとめるためフォーマットを作り、全ての用語を標準化した。用語の標準化によって、API を使い自動的に情報を収集できるようになった。標準化は情報共有の必要性や目的意識のすり合わせという面からも最初に取り掛かるべき点であるといえるだろう。

4-2 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、情報共有と協力の拠点を一カ所に絞り、わかりやすくすることが有効だった。企業に負担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。

韓国 C-TAS の特徴はオープン 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。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。

また韓国の「118」電話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。

4-3 相互信頼

韓国と米国の事例をみると、情報共有によって企業の機密情報が洩れるのではないか、何が損をするのではないか、という認識があると情報共有は進まない。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。

4-4 インセンティブ

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。欧州では EC や EU の認証フレームワークや指針を守らないと罰則が厳しく欧州でビジネスをすることが難しくなるなど拘束性が高い協力体制を整えようとする傾向が強かった。

日本でも 2 次被害 3 次被害の可能性を念頭に置き、サイバーセキュリティは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。

5　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。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。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。本稿では成功事例の共通点を主に考察したが、失敗した政策と成功した政策の違いを、データを用いて定量的に分析する研究にもチャレンジしたい。

【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/.../csirt_for_management_layer_20151126.pdf 2018 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

韓国インターネット振興院（2018）「C-TAS 紹介ページ」https://www.krcert.or.kr/data/noticeView.do?bulletin_writing_sequence=25824 2019 年 6 月 13 日アクセス

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 2019 年 6 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 2019 年 6 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
韓国行政安全部(2016)「電子政府 2020 基本計画」
韓国行政安全部(2017)「電子政府 50 年史」
韓国行政安全部(2018)「2018 電子政府 655 億ウォン投資で知能型政府本格始動」2018.1.21 付報道資料
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 www.mhlw.go.jp/topics/bukyoku/iyaku/syoku-anzen/riskcom/01.html 2019 年 6 月 13 日アクセス
佐々木良一(2016)「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
趙章恩(2018)「韓国のデジタルガバメントとサイバーセキュリティ政策変化に関する考察」『第 17 回情報科学技術フォーラム講演論文集』講演番号 N-017 2018 年 9 月 20 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 6 月 13 日アクセス
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
McAfee Labs (2017) 「 Previews Five Cybersecurity Trends for 2018 」 https://securingtomorrow.mcafee.com/mcafee-labs/2018-threats-predictions/ (2019 年 6 月 13 日アクセス)
The Department of Homeland Security, Information Sharing
https://www.dhs.gov/topic/cybersecurity-information-sharing (2019 年 6 月 13 日アクセス)

〈発 表 資 料〉

題 名	掲載誌・学会名等	発表年月
韓国の第 4 次産業革命とサイバーセキュリティ	一般社団法人 CiP 協議会 You Go Ex	2018 年 8 月
韓国のデジタルガバメントとサイバーセキュリティ政策変化に関する考察	第 17 回情報科学技術フォーラム講演論文集	2018 年 9 月
インターネット上の海賊版サイト対策に	情報文化学会全国大会講演予	2018 年 10 月

関する日韓比較	稿集	
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 11 月
サイバーセキュリティエコシステムに関する考察	社会情報学会中国・四国支部研究会	2018 年 12 月
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	東京大学大学院情報学環紀要	2020 年 3 月（査読中）