O-043

韓国におけるサイバーセキュリティ政策の変化と社会環境への影響に関する考察

A Study on cyber security policy changes and the impact of social environment in Korea

趙　章恩†
Changeun Cho

1. 研究の背景

2003 年 1 月 25 日、通信キャリアを対象にしたハッキング攻撃により全国のインターネットがつながらなくなる事件を経験してから、韓国政府は国家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し、国家サイバー安全管理規定を制定、国家サイバー安全センターとインターネット侵害事故対応センターを設立した。

それからスマートフォンの普及、ネットワークの高速化、既存の産業と ICT の融合によるスマートホーム・スマート教育・スマートヘルスケアなど新しいサービスの登場といった社会環境の変化の中でサイバーセキュリティ政策も変化し続けてきた。

サイバーセキュリティ政策は大きく個人情報保護の側面と国家安全の側面に分けられ、さらに国家、企業、個人それぞれのサイバーセキュリティ脅威に合わせた政策がある。常に社会環境の変化に応じて更新・変化している。

特に近年、韓国政府のサイバーセキュリティ政策更新周期は短くなり、多様な政策を打ち出しているにも関わらず韓国内のサイバーセキュリティ侵害事故は後を絶たない。

韓国政府の最新の政策としては、2015 年に発表した「K-ICT セキュリティ発展戦略」と 2016 年に発表した「エネルギー・製造・交通・医療・家電分野の K-ICT 融合セキュリティ発展戦略」、「サイバーセキュリティ人材養成総合計画」 などがある。一連の政策は社会環境を守るためのサイバーセキュリティ政策から、サイバーセキュリティ産業そのものを育て、韓国を代表する産業として海外輸出を促進する政策に変化したという特徴もある。

本稿では韓国におけるサイバーセキュリティ政策の変化を分析し、社会環境へ与えた影響と、社会環境の変化がサイバーセキュリティ政策に与えた相互作用に関して分析する。

2. サイバー犯罪の現状

韓国は既に数多いサイバー犯罪、大規模な個人情報ハッキング事件、DDos 攻撃事件などを経験してきた。

韓国大統領令第 267 号「国家サイバー安全管理規定」第 2 条によると、サイバーアタックとは「ハッキング、コンピューターウィルス、論理爆弾（悪意あるプログラムの一種で、特定の時間が経つとコンピュータの破壊活動を実行するプログラム）、メール爆弾、サービス妨害など電子的手段によって国家情報通信網に不法侵入・撹乱・麻痺・破壊したり情報を窃取、棄損したりする攻撃行為」を意味する。

韓国知識情報保安産業協会の調べによると、2006 年～2015 年の間、韓国内で発生した自然災害による被害額は 1 兆 7000 億ウォンなのに対し、サイバーアタックによる経済的被害額は 3 兆 6000 億ウォンと、2 倍以上多かった[1]。

韓国産業研究院の調査では、電気自動車やスマート家電などが日常的に使われる IoT 時代のサイバーアタックによる被害額は、最悪の場合 2020 年には 17 兆 7000 億ウォン、2030 年には 26 兆 7000 億ウォンに上る可能性もあり、国家信用度の下落、個人情報やデータ流出による 2 次、3 次被害を考慮すると被害はさらに増える可能性が高いことがわかった[2]。

表 1　韓国で発生した主なサイバー犯罪事例

年度	対象	内容
2003 年	KT（通信キャリア）	DNS サーバー攻撃により 9 時間全国のインターネット接続が中断
2006 年	オンラインゲーム　「リネージュ」	120 万人の個人情報を盗用して会員登録
2008 年	オークション	1080 万人の個人情報がハッキングで流出
2009 年	政府サイト・ポータルサイト・銀行	DDoS 攻撃で WEB サイトアクセス不能
2011 年	農協	ハッキングでシステム障害発生、ATM・窓口業務の正常化に 18 日所要
2011 年	ポータルサイト「NATE」	3500 万人の個人情報がハッキングで流出

† 東京大学大学院情報学環　セキュア情報化社会研究寄附講座
The University of Tokyo Interfaculty Initiative in Information Studies.

1 “電子新聞”,2015 年 2 月 15 日付, http://www.etnews.com/20150213000168（2016 年 6 月 24 日アクセス）

2 韓国産業研究院、『IoT 時代の安全ネットワーク、融合保安産業』、2014 年 4 月 15 日、pp.8

2014 年	韓国水力原子力	ハッカーが悪性コードを仕込んだメールを送信してハッキング、原子力施設の設計図などの資料をオンライン掲示板に公開
2014 年	クレジットカード会社「KB カード」、「ロッテカード」、「NH 農協カード」	3 社重複込みで住民登録番号や口座情報含む 1 億 580 万件の個人情報流出、セキュリティ関連会社社員が持ち出して広告会社などに販売
2015 年	大統領官邸、外交部（省）職員	ハッカーが悪性コードを仕込んだメールを送信、PC ハッキング
2016 年	政治家	北朝鮮ハッキング部隊のスマートフォンハッキング未遂

（韓国メディアの報道から抜粋、筆者作成）

韓国で発生したサイバー犯罪は、北朝鮮や海外から攻撃しているケースも年々増加傾向にあり、官軍民が協力して常にサイバーセキュリティ情報を共有するシステムを構築した。

3. サイバーセキュリティ政策の変化

韓国のサイバーセキュリティ政策は 2003 年の通信キャリアを対象にしたハッキング攻撃のきっかけに本格的な議論が始まり、2009 年「国家サイバー危機総合対策」が制定された。サイバー犯罪に関しては、2001 年「情報通信網利用促進等に関する法律」を「情報通信網利用促進及び情報保護等に関する法律」に改訂、個人情報侵害やハッキングなどを処罰できるようにした。その後、「個人情報保護法」、「電子署名法」、「クラウドコンピューティング発展及び利用者保護に関する法律」、「情報通信振興及び融合活性化等に関する特別法」などを制定して、ICT の利用促進と並んでセキュリティも強化する政策を行った。

韓国政府のサイバーセキュリティ政策は事後対策で、事件が起きてから対策を打ち出し、それを上回る事件が起きてまた政策を修正する、という繰り返しだった。2015 年 9 月の国政監査では、議員らが「ハッキング被害は増え続けているのにこれといった対策がない。ハッキング防止こそ国民の生活に関わる最も重要な課題」だとして、ハッキング防止のための国家予算を増やすことを要求した。韓国政府は、ICT と他産業の融合によるイノベーションで新しいビジネスができるようにしないと経済に悪影響を与える、そのためには安心・安全社会を維持し、セキュリティが保たれたネットワーク環境を作る必要があるとして、サイバー犯罪を予防できる政策作りを急いだ[1]。さらに、サイバーセキュリティ政策は ICT 産業を守るための政策ではなく、サイバーセキュリティ産業そのものを育成する政策へと変わるべきという声も登場した。

3.1 知識情報保護から融合セキュリティへ

スマートフォンが普及し、IoT、モバイル金融など ICT と他産業の融合サービスが増えている中、一つのデバイスがハッキングされるとドミノ倒しのように被害が拡大してしまう。

韓国では 2008 年知識経済部（部は省に当たる）の提案で、物理的セキュリティと知識情報セキュリティを一つにした「融合セキュリティ」の概念を取り入れてサイバーセキュリティ対策を考えるようになった。建物の出入り、防犯カメラといった物理的セキュリティが ICT と融合し、個人情報保護や知識情報の保護が ICT と融合、さらに ICT＋他産業の融合で新しいサービスが生まれる過程で発生するセキュリティ問題、これらを総合的に考えてサイバーセキュリティ政策を打ち出そうとした。電気、水道、ガス、交通、医療情報、行政情報など国の重要なインフラと情報がほぼ全てネットワークでつながるようになった今、ハッキングによる被害は個人情報が盗まれたというレベルに留まらず、国の安保までも危険にさらすことになるため、融合セキュリティを守る政策は何よりも重要である。

3.2 2015 年 4 月 K-ICT セキュリティ発展戦略

2015 年 4 月未来創造科学部が発表した「K-ICT セキュリティ発展戦略」は、今までの韓国政府のサイバーセキュリティ政策を覆す内容であった。インターネットの普及や ICT 産業の振興が優先で、サイバーセキュリティは外側を守るためのものという認識だったのが、「K-ICT セキュリティ発展戦略」はサイバーセキュリティそのものが主人公で、これからは韓国を代表する産業としてサイバーセキュリティを育てるという内容だった。

主な内容は以下の通りである。

企業の年間予算から一定水準以上をサイバーセキュリティに投資する。サイバーセキュリティクラスターを造成して、企業と研究機関とテストベッドを連携してシナジー効果を出す。韓国のサイバーセキュリティ企業の海外進出を政府が助ける。ホワイトハッカーを養成して大学進学や徴兵でも特技を活かせるようにする。最精鋭サイバーセキュリティ専門家、特に国防と金融分野のセキュリティ専門家を 2019 年まで 7000 人養成する。サイバーセキュリティ技術開発に投資する企業は税制優遇する。企業の情報保護最高責任者（CISO）ホットラインを構築する。

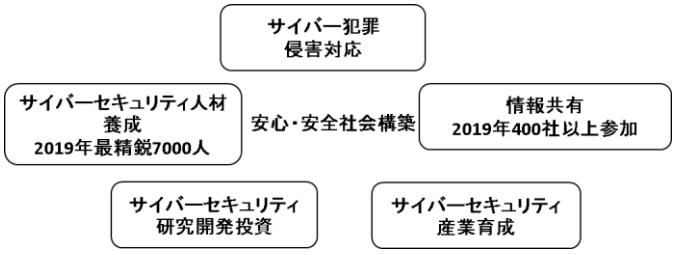

図 1　「K-ICT セキュリティ発展戦略」の基本構想

[3] “INEWS24”,2015 年 9 月 21 日付, http://news.inews24.com/php/news_view.php?g_menu=020200&g_serial=920306（2016 年 6 月 26 日アクセス）

このような政策の結果として、先進国とのサイバーセキュリティ技術格差を、2015 年 1.6 年から 2019 年 0.3 年に短縮、世界最高レベルのサイバーセキュリティ強国を目指す。

3.3 2015 年 11 月　K-ICT セキュリティイノベーション拡散方案

続けて韓国政府が発表した「K-ICT セキュリティイノベーション拡散方案」は、モバイル・クラウドコンピューティング・IoT の 3 大分野のサイバーセキュリティスタートアップを育成するという内容である。「K-ICT セキュリティイノベーション拡散方案」は、スタートアップ、人材、技術イノベーションの 3 大要素を加速することを目指すアクションプランとなっている。

グローバル市場で通用する技術を確保するため国際共同研究を推進し、省庁間で横のつながりを拡大しながら効率よく共同研究と情報共有するため「サイバーセキュリティ研究開発調整協議会」を発足、官民の情報共有体制も強化した。捜査のためだけでなく、常にサイバーアタックや悪性コードなどの情報を共有し、事前に事故を防止できるようにする。

サイバーセキュリティを ICT 産業育成のおまけとして考えるのではなく、サイバーセキュリティの技術力向上による他の ICT 産業も成長できるという考え方に切り替わった。

3.4 2016 年 5 月　K-ICT 融合セキュリティ発展戦略

「K-ICT 融合セキュリティ発展戦略」はエネルギー・製造・交通・医療・家電分野の ICT 融合サービスセキュリティ実証実験に関する支援策である。

IoT、人工知能など ICT 技術の発展により、製造業、交通、医療など伝統産業と ICT の融合が急速に拡大していることから、技術や社会の変化に応じたサイバーセキュリティ脅威も広がっている。融合製品やサービスが普及される速度に融合セキュリティ対策の速度が追い付いていないと言う問題もある。

想定される問題は、スマートカーをハッキングして事故を起こす、ヘルスケアデバイスをハッキングして人命に被害が出る、電力施設をハッキングして社会を不安にさせるといったことをあげられる。

こうした融合分野のサイバーセキュリティに備えるため、韓国政府は 2016 年 6 月から 12 月までスマートホーム・家電、金融、産業制御、医療の 4 つの分野で実証実験を行うことにした。

スマートホーム・家電は、セキュリティチップを利用し、デバイスのセキュリティ強化を狙った実証実験を行う。金融は、生体認証（指紋・虹彩など）を利用して金融情報にアクセスできる権限を制限する技術の実証実験を行う。産業制御は、浄水施設のデータを自治体業務ネットワークに送る安全な通信装置の実証実験を行う。医療は、モバイルへするケア・ヘルスケア用デバイスのそれぞれのセキュリティを統合管理できる技術について実証実験を行う。

さらに、ICT と交通・医療・エネルギーなど産業間の融合が拡散したことにより、ハッキングといったサイバーアタックの脅威が日常生活にまで拡大する恐れがあることから、これに対応する融合セキュリティ産業を育成し、「ICT 融合安心社会」を実現するため、「融合産業別セキュリティガイドライン」を公表し、製品やサービスの開発段階から適用するようにした。国民が安心して ICT とその他産業の融合で生まれた新しい製品やサービスを利用できるようにするためである。

融合セキュリティにおいては、それぞれの産業振興政策を担当する省庁間の協力が大事であるため、全省庁が参加する「政策協議会」を定期的に開き、「ICT 融合産業と融合セキュリティ産業間の協力のためのアライアンス」を構成することにした。

3.5 2016 年 6 月　第 1 次情報保護産業振興計画 K-ICT セキュリティ 2020

「K-ICT セキュリティ 2020」では、IoT やヘルスケア、スマートホーム、スマート工場など最新技術動向を素早く対応できるサイバーセキュリティ技術の開発支援と、韓国のサイバーセキュリティ産業の海外輸出を促進することにより焦点を当てている。

アフリカ、中南米、東南アジアなどを対象に ODA の一環としてサイバーセキュリティ、サイバー犯罪捜査を手助けする支援も行う。

「K-ICT セキュリティ 2020」は、2015 年 1 兆 6000 億ウォンだったサイバーセキュリティ産業の輸出を 2020 年 4 兆 5000 億ウォンに伸ばし、雇用も 2020 年まで 1 万 9000 人以上増やすことを目標としている。サイバーセキュリティ関連スタートアップも 2015 年 16 社から 2020 年には 100 社以上生まれるよう政府が起業を支援することも目指している。

公共機関のサイバーセキュリティ予算を持続的に拡大し、民間企業のサイバーセキュリティ投資も税制優遇などで後押しする。IT システム構築の際に維持補修費用の他にサイバーセキュリティの持続サービス対価を明確にし、サイバーセキュリティサービス市場を拡大する。

4. まとめ

韓国のサイバーセキュリティ政策は情報化推進がメインでサイバーセキュリティはその外側を守るものという考えから、サイバーセキュリティ産業分野そのものを育成する方向へ変化している。

その影響で学校ではサイバーセキュリティ人材育成に力を入れるようになった。2018 年からはソフトウェア開発を小中高校で義務的に行い、サイバーセキュリティに関する教育も行うことでホワイトハッカーを養成する。

スマートフォンやスマートホームなど融合デバイス市場では性能だけでなく、セキュリティプログラムを適用しているかどうかが重視されている。

サイバーセキュリティが重要視されるようになってから、ヘルスケアや電気自動車など新しいサービスに対する不安が減り、新規サービスの活性化が見込まれる。

今後も続けてサイバーセキュリティ政策の効果を測定し、実際に韓国社会・経済においてどのような変化があったのか、政策の効果はあったのかなどの研究を行い、日韓のサイバーセキュリティ政策樹立に役立てたい。

参考文献

[1] “電子新聞”,2015 年 2 月 15 日付, http://www.etnews.com/20150213000168（2016 年 6 月 24 日アクセス）
[2] “INEWS24”,2015 年 9 月 21 日付, http://news.inews24.com/php/news_view.php?g_menu=020200&g_serial=920306（2016 年 6 月 26 日アクセス）
[3] 韓国産業研究院, “IoT 時代の安全ネットワーク融合保安産業”、2014 年 4 月, pp.8
[4] 韓国インターネット振興院, “2015 国家情報保護白書” ,2015 年 4 月
[5] 未来創造科学部, “K-ICT セキュリティ発展戦略” ,2015 年 4 月
[6] 未来創造科学部, “K-ICT セキュリティイノベーション拡散方案” ,2015 年 11 月
[7] 未来創造科学部, “第 1 次情報保護産業振興計画 K-ICT セキュリティ 2020” ,2016 年 6 月