韓国政府のICT戦略変化考察　-サイバーセキュリティを中心に

A Study of changes in the Korean government ICT strategy - focusing on cyber security

趙　章恩[1]
Changeun CHO

[1] 東京大学情報学環 セキュア情報化社会研究寄附講座
The University of Tokyo Interfaculty Initiative in Information Studies Graduate School

Abstract　National ICT strategy of the Korean government starts from the government computerization in 1975, it has been development ICT industry starting with the 1999 Cyber Korea 21. Strategy changed with the development of technology. The most important social and economic challenges are included in ICT strategy. Recent ICT strategy is made focus on cyber security. Among the national ICT strategy, increased the importance of cyber security.
キーワード　韓国、ICT戦略、サイバーセキュリティ、政策

１．研究の背景

韓国では ICT の発展によりインターネットを介した情報流通が増え、インターネット上での経済活動も盛んになっている。インターネットを介して家電や家の中の物を遠隔操作できるスマートホーム、デジタル教材とクラウドシステムを使うスマート教育、スマートフォンやスマートウォッチなどで健康状態をモニタリングするスマートヘルスケアなども浸透し、インターネットがないと生活が不便なほどネット依存度も高くなっている。ICT の最先端サービスが登場すればするほど、DDos 攻撃、ランサムウェア、個人情報ハッキングなど ICT を利活用した脅威も巧妙になっている。このような背景から、誰もが安心してインターネットを使えるよう、サイバーセキュリティの重要性も高まっている。

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試算となった。サイバーアタックにより被害が発生した場合は、国家信用度の下落、個人情報やデータ流出による2次3次被害が出る可能性が高く、間接的な被害規模は計り知れない。すべてのモノと人がつながるIoTの時代には、一つのデバイスがハッキングされるとすぐそのデバイスとつながっている他のデバイスやサービスもハッキングの被害にあることが想定される。サイバーアタックはインターネット上の脅威に留まらず、オフラインの実生活に影響を与えるだろう[2]。

韓国政府は 90 年代後半から「IT 強国」を目指した政策を進めてきた。韓国政府はほぼ毎年、政府が韓国社会の課題を ICT を利活用してどう解決するか、ICT 産業のどの部分を育成するのか、ICT 発展のためにどの規制を緩和するのか、といった国家 ICT 政策を発表している。ここ数年、韓国の国家 ICT 政策はセキュリティを強調する項目が増えている。韓国政府は、韓国が IT 強国であり続けるためには、ICT 発展と同時にサイバーセキュリティ戦略が重要になるしかないとみている。

２．サイバーアタックの現状

韓国の大統領令第 267 号「国家サイバー安全管理規定」第 2 条では、サイバーアタックを「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いう」と定めている。

韓国は既に数多いサイバーアタックを経験してきた。

2003 年、通信キャリア KT の DNS サーバーが攻撃を受け、全国で 9 時間インターネットに接続できなくなった事件が発生し、韓国政府は初めてサイバーセキュリティ対策を強化し、サイバーアタック対応センターを設立した。

2009 年には政府機関のサイトが DDos 攻撃に合い、サイトにアクセスできなくなった事件が発生し、国家サイバーテロ対策を強化した。

2014 年には韓国水力原子力（公共機関）のパソコ

[1] 2015 年 2 月 15 日付
『電子新聞』http://www.etnews.com/20150213000168（2016 年 6 月 23 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

ンがハッキングされ、原子力施設の設計図などの資料が盗まれオンライン掲示板に公開された事件が発生したことで、社会に不安が広がり、韓国政府は政府機関・公共機関・企業のサイバーセキュリティに対する責任を強化する対策をとった。

2016 年 3 月には国家情報院が、北朝鮮のハッキング部隊が韓国政治家のスマートフォンをハッキングしようとして未遂に終わったと公表し、スマートフォンやモバイルデバイスのサイバーアタック対策が問題になっている。

表 1　韓国で発生した主なサイバーアタック事例

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
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
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、原子力関連資料を盗んでオンライン掲示板に公開した
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）

近年のサイバーアタックは、円滑なサービスができないよう妨害したり、パソコンのデータや個人情報を盗んだり、金銭的被害を与えることが目的となっている。データを人質にして匿名で現金化できる電子貨幣「ビットコイン」を要求するランサムウェアは 2015 年 1～3 月 56 種から 2016 年 1～3 月 963 種に 17 倍も増えた[3]。

サイバーアタックは韓国内に限らず、北朝鮮や海外から韓国に対して攻撃が行われるケースも年々増加傾向にある。ユーザーがインターネットを安心して利用できる環境を保つためには、企業だけの対策では難しく、政府の政策が重要になってきた。

３．ICT政策の変化とサイバーセキュリティ

(1)初期段階の ICT 政策：ICT 産業の育成

韓国政府の ICT 政策は、1975 年「行政電算化委員会」を構成したのがその始まりである。本格的に ICT 産業を育成する戦略として登場したのが、1999 年の「サイバーコリア 21」である。

70～80 年代の ICT 戦略は、国家電算ネットワークの普及と利用に焦点が当てていた。90 年代からはブロードバンドの基盤構築と普及に焦点を当てた。2000 年代からは社会全体の情報化、インターネットで情報を広め共有する知識社会、電子政府を目指した。

1998 年に国家情報院が政府機関全体のサイバーアタック対応窓口になり、軍は国軍機務司令部がサイバーアタックやサイバーテロの情報収集をする窓口になった。

2000 年あたりから企業でもそれぞれ CERT(Computer Emergency Response Team)を運営するようになった。2003 年には韓国インターネット振興院の中に「インターネット侵害事故対応支援センター（krCERT/CC)）」を設置し、企業と一般利用者のサイバーセキュリティ窓口になった。

韓国侵害事故対応チーム協議会（CONCERT）によると、大手企業の場合はほとんど CERT があるが、中小企業の場合は CERT を運営するのが難しいため、韓国インターネット振興院をはじめ政府機関のサイバーアタック感知・情報提供に依存している。

2002 年にはブロードバンド加入世帯が全世帯の 7 割を超える 1000 万を突破、韓国政府は 2002 年「e-Korea Vision 2006」、2003 年「Broadband IT Korea Vision 2007」を発表した。

韓国政府の ICT 戦略にサイバーセキュリティ対策の事が登場したのは、「2003 インターネット大乱」と呼ばれる事件がきっかけになった。2003 年 KT の DNS サーバーが攻撃を受け、全国で 9 時間インターネットに接続できなくなった事件のことである。

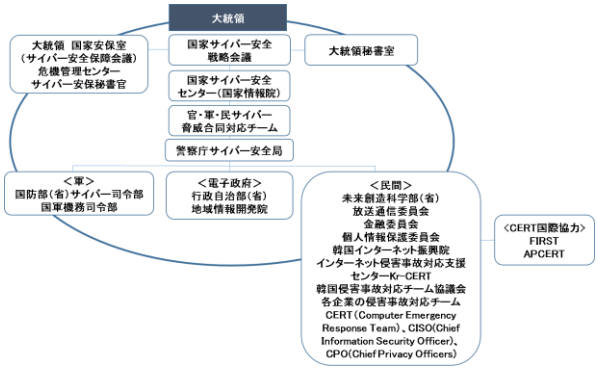
その後 2006 年にはモバイル、有無線融合とセキュリティに焦点を当てた「u - Korea 基本計画」が発表された。

2009 年には民間のサイバーセキュリティを担当する機関を統合して韓国インターネット振興院が窓口になり、2010 年には韓国インターネット振興院が運営するサイバーセキュリティ相談電話『118』が登場した。韓国インターネット振興院の傘下には、情報保護産業支援センター、バイオ認識情報試験センター、不法スパム対応センター、フィッシング対応センター、電子政府 SW·IoT セキュリティセンター、地域情報保護支援センターがある。

その後、政府のサイバーセキュリティ対策組織として、「個人情報犯罪政府合同捜査団」、警察庁の「サイバー安全局」、国家情報院の「国家サイバー安全センター」、韓国インターネット振興院の「インターネット侵害対応センター」、韓国地域情報開発院の「サイバー侵害対応支援センター」なども設置された。

[3] 2016 年 5 月 3 日付『保安ニュース』
http://www.boannews.com/media/view.asp?idx=50500（2016 年 6 月 23 日アクセス）

図 1　韓国のサイバーセキュリティ対策組織図



（韓国インターネット振興院『2015 国家情報保護白書』pp.11 を参考に筆者作成）

（2）2015 年以降の ICT 政策：ICT 産業発展のためサイバーセキュリティ重視

韓国政府は、2015 年 5 月国家 ICT 戦略である『K-ICT 戦略』を発表し、その中でサイバーセキュリティの重要性を強調した。同年 11 月には『K-ICT セキュリティイノベーション拡散戦略』を発表し、ICT 産業を守るためのサイバーセキュリティではなく、サイバーセキュリティ産業そのものを育成することにした。2019 年までサイバーセキュリティ研究開発に 2500 億ウォンを投資し、サイバーセキュリティ関連スタートアップを支援、サイバーセキュリティ分野の海外輸出を増やすための支援も始めることにした。韓国のサイバーアタック経験を生かしたノウハウと技術、海外企業の技術を提携し、世界市場で役立つサイバーセキュリティ製品やサービスを生むための支援も始めた。アフリカ、中南米、中東、東南アジアを戦略拠点にし、デジタルフォーレンシク、サイバーアタック侵害対応モデルを輸出する。途上国のサイバーセキュリティを助ける「サイバーセキュリティ協力ネットワーク」を組織し、韓国がかつて電子政府やデジタル病院の構築を助けたようにサイバーセキュリティでも技術援助を行う。

K-ICT セキュリティイノベーション拡散戦略により、軍のサイバー司令部と警察サイバー安全局サイバー捜査隊の役割を強化、人材育成に力を入れている。年間 74～80 人のホワイトハッカーを採用、徴兵の代わりに服務できるようにした。ハッキング大会で入賞したり、関連学科に在学していたり、サイバーセキュリティ関連の部活履歴があれば、徴兵でサイバーセキュリティに関連した勤務に就くようにして、専門性を活かせるようにもした。サイバーセキュリティ分野の雇用を 2014 年 36000 人から 2019 年 55000 人に増やそうとしている。

また、北朝鮮からのハッキング脅威が増加していることから、官民軍合同対策を立てるための情報共有も強化することにした。

（3）2016 年以降の ICT 政策：オリンピック、人工知能とサイバーセキュリティ

2016 年 5 月に発表した『K-ICT 戦略 2016』でも、2018 年ピョンチャン冬季オリンピックに向けサイバーセキュリティを重視し、人工知能をサイバーセキュリティに活用することを決めた。

2015 年から K-ICT 集中育成産業として支援している IoT、クラウドコンピューティング、ビッグデータ、5G、UHD（4K・8K）、デジタルコンテンツ、スマートデバイスに人工知能を追加した。

サイバーセキュリティに人工知能を導入することにした。2019 年まで人工知能基盤サイバーテロ対応技術を開発する。ピョンチャン冬季オリンピックでは、人工知能を活用したセキュリティとして、映像認識で事故が起こりそうな時を予測して防止する、無断侵入を事前に感知して防止するなど、防止や予防に力を入れる。ピョンチャン冬季オリンピックで韓国のサイバーセキュリティ技術を披露し、輸出のきっかけにするのが狙いである。

人材育成に力を入れるため、最精鋭サイバーセキュリティ専門人材を育成する「サイバーセキュリティ人材養成総合計画」を盛り込んだ。今後 5 年間、サイバーセキュリティ専門家の中でも最精鋭 7000 人を養成することを目標に、小中高校時代からサイバーセキュリティの教育をさせるという内容である。2017 年まで小中高校別「サイバーセキュリティ」科目の教材を開発し、小学生からコーディングと一緒にサイバーアタックの防衛について教える。コーディングとはプログラミング言語でプログラムを作成することを意味し、韓国では 2018 年から小中高校でコーディングを義務教育として教えることが決まった。サイバーセキュリティ科目を教える教員も養成し、サイバーセキュリティ関連の職業体験イベントも随時行う。ジュニアハッキング大会を頻繁に開催し、小学生から素質のあるホワイトハッカーを見つけ、教育を行う。サイバーセキュリティ英才教育を行う。

大学ではサイバーセキュリティに特化した学科を増やす。現在 4 校ある「サイバーセキュリティ特性化大学」を 2020 年には 12 校にする。雇用契約型大学院といって、特定企業に就職する条件で企業から修士課程 2 年間の学費と生活費を支援してもらう制度があるが、これをサイバーセキュリティ分野にも適用する。その他大学でもサイバーセキュリティ講座を増やす。

ホワイトハッカーは軍の徴兵もサイバーセキュリティ特技兵として活躍できるようにする。女性のサイバーセキュリティ専門家が出産・育児で経歴が断絶するのを防ぐため、本人が希望すれば再教育を行い、再就職できるようサポートする。サイバーセキュリティ産業そのものの育成にも力をいれ、民間企業のセキュリティ分野投資拡大を誘導する。

IoT のように複数の製品や産業分野が融合する分野は特にサイバーセキュリティが重要になるので、「融合産業セキュリティ強化のためのガイドライン」も早期制定する。

日本でも東京オリンピックを控えサイバーテロによる社会の混乱を生じさせないため、サイバーセキュリティの重要性が台頭している。韓国はオリンピックだけでなく北朝鮮という脅威を感じる存在がある。

（4）2016 年以降の ICT 政策：サイバーセキュリティ産業育成

2016 年 6 月には『K-ICT 戦略 2016』の中にあるサイバーセキュリティ政策とは別に、サイバーセキュリティ産業そのものを育成することを目標にした『第 1 次情報保護産業振興計画（K-ICT セキュリティ 2020』を樹立した。同計画は、より巧妙なサイバーアタックが発生し、社会の混乱と国家安保に脅威となっていることから、サイバーセキュリティの競争力強化と、次世代成長産業としてのサイバーセキュリティ産業育成を目的としている。まずは政府機関・公共機関から韓国のサイバーセキュリティ関連製品やサービスを積極的に導入してサイバーセキュリティ市場規模を育てる、サイバーセキュリティ専門家の待遇を改善する、人材を育成する、その結果サイバーセキュリティ産業の競争力が改善する、韓国のサイバーセキュリティ関連製品やサービスを利用する企業が増える、というサイクルが生まれることを目指している。韓国に根付いているサイバーセキュリティ製品の値引き、最安値入札慣行をなくし、適正な価格で販売できるようにすることも目指す。

方法としては、サイバーセキュリティクラスターを造成してスタートアップを増やし、有望なアイデアや技術をビジネス化するために必要なことを政府が支援する。政府系研究機関が開発した技術はどんどん民間企業に移転する。ICT と既存産業の融合において、医療・エネルギー・交通・家電・製造分野は融合製品・サービスの企画段階からセキュリティを重視し、必ずサイバーセキュリティ技術を適用することにした。防犯カメラ、バイオ認証、スマートカード、ビッグデータ基盤映像分析といった物理的なセキュリティとサイバーセキュリティの融合分野にも政府が投資する。政府、公共機関、民間企業がサイバーアタック情報をより詳しく共有し、データ分析の結果を政府が民間企業に提供して製品開発に役立てるようにする。すべての産業においてサイバーセキュリティの重要性が増していることから、政府・公共機関・民間企業のサイバーアタック情報共有に関しては協力を強制できる法制度を制定する方向で進んでいる。

国境を超えたサイバーアタックを事前に探知して防衛できるよう、主な先進国のサイバーセキュリティ組織と行っている国際協力関係も強化する。

その結果として、2020 年までサイバーセキュリティスタートアップ 100 社、グローバル市場で活躍する韓国のサイバーセキュリティ会社 10 社を育成し、2015 年末時点で 1 兆 6000 ウォン規模の韓国サイバーセキュリティ輸出規模を 2020 年 4 兆 5000 億ウォンに拡大する。

同計画は 2015 年 12 月施行された『情報保護産業の振興に関する法律』によるものである。同法は、「安全な情報通信利用環境を造成し、国民経済の健全な発展」を目的としている。

(5)サイバーセキュリティ政策の変化

韓国の国家 ICT 政策は ICT そのものの普及発展戦略から始まり、だんだんと ICT のためにサイバーセキュリティを重視する戦略に切り替わっている。2015 年からは人工知能といった新しい技術をサイバーセキュリティと融合し、事故後の対策から予防する方向へ戦略を切り替えた。また、先進国とは韓国が経験したサイバーアタックの情報を共有して今後のサイバーセキュリティ技術発展に役立て、途上国には韓国のサイバーセキュリティノウハウを伝授することで国際協力も強化している。

2016 年からは ICT 政策そのものがサイバーセキュリティ産業の育成に焦点を当てた内容になりつつあり、韓国経済の発展のためにサイバーセキュリティ産業を育成して海外輸出を増やすといった政策を取り組んでいる。

４．今後の課題

韓国の事例からすると、政策と組織を強化しても、サイバーセキュリティは万全といえず常に脅威にさらされている。サイバーセキュリティ対策を講じても、すぐ抜け道を見つけ攻撃されるため、サイバーセキュリティ政策は常に最新の ICT 状況に合わせ、アップデートしていかないといけない。韓国の事例から日本で起こり得る問題を想定して回避できるよう、政策面、組織面での対策案方について研究を続け、日本のサイバーセキュリティ政策樹立に役立てるようにする。

参考文献

1) 情報通信戦略委員会（2016）：『K-ICT 戦略 2016』、2016 年 5 月
2) 未来創造科学部（2015）：『K-ICT セキュリティイノベーション拡散方案』、2015 年 11 月
3) 未来創造科学部（2015）：『K-ICT 戦略』、2015 年 5 月
4) 韓国インターネット振興院（2015）：『2015 国家情報保護白書』、2015 年 4 月
5) 韓国産業研究院（2014）:『IoT 時代の安全ネットワーク、融合保安産業』、2014 年 4 月、pp.8
6) 2016 年 5 月 3 日付『保安ニュース』http://www.boannews.com/media/view.asp?idx=50500（2016 年 6 月 23 日アクセス）
7) 2015 年 2 月 15 日付『電子新聞』http://www.etnews.com/20150213000168（2016 年 6 月 23 日アクセス）