海外における情報セキュリティの動向
―米国、欧州、韓国の現状―

株式会社 富士通総研 経済研究所
主席研究員 **榎並 利博**

1 はじめに

世界中の国の人々がお互いに行き来し、コンテナ技術によって大量の物流が効率化され、資本や情報が自由に流通することによって、人々の生活はますますグローバル化した世界と一体化してきている。ネットワークを介してWikipediaなどにグローバルな知恵が、apacheやLinuxなどのオープンソースにグローバルな技術が結集され、ネットワークを介してアメリカなどの先進国からよりコストの低い国へと事務作業のアウトソーシングが加速している。まさに世界はフラット化した状態になっており、トーマス・フリードマンの言葉を借りれば、2000年以降に始まったグローバリゼーション3.0は「個人がグローバルに力を合わせ、またグローバルに競争をする個人のグローバル化」の時代をもたらしているということになる。

このように現代のグローバル化した社会においては、人々の生活や経済がますます情報ネットワークに依存を強めたかたちで進化を遂げている。そして、社会基盤としての情報ネットワークの重要性が高まるにつれ、社会に対して悪意を持つ者にとってはネットワークが格好の攻撃対象となってくる。ネットワーク社会の黎明期、自分の技術力を誇るハッカーなどが情報化社会を脅かすものとしてその対策が急がれたが、現在では世界じゅうの人々の生活を支える情報ネットワークをグローバルなテロ活動組織からいかに防御するかという極めて重大な局面に差し掛かっているのである。

グローバルに活動する犯罪組織に対抗していくためには、国内の情報セキュリティ対策を実施するだけでなく、防衛省や他国と連携した国の安全保障という観点、グローバルな安全保障という観点から情報セキュリティ対策を考えていかなくてはならないだろう。本稿では米国、欧州、韓国の現状を探りながら、海外の情報セキュリティに関する動向を紹介したい。

2 米国における情報セキュリティ政策

米国における情報セキュリティ政策は、1993年に発足したクリントン政権時代に遡る。当時、情報スーパーハイウェイ構想を推進していたクリントン政権は、情報スーパーハイウェイの実体がオープンなネットワークであるインターネットと重なっていく過程のなかで、ネットワークを重要インフラとして位置づけて保護する政策をはじめて打ち出した。その後、ブッシュ政権時代に発生した2001年9月11日の同時多発テロ事件が、情報セキュリティ政策上の大きな転換点となる。テロリストによるサイバー攻撃に備え、新設した国土安全保障省内に国家サイバーセキュリティ部門を設置し、サイバーセキュリティに関する政策の取りまとめを行うこととなったのである。

しかし、国土安全保障省はサイバーセキュリテ

ィに深く関与している国防総省との連携が弱く、技術的知見についても乏しく現実にサイバー攻撃への対処が進んでいないという批判を受け始めた。そこで、ブッシュ大統領は2008年に包括的国家サイバーセキュリティイニシアティブを発表し、情報セキュリティ体制を一新することとなった。国土安全保障省内に、国家サイバーセキュリティ部門とは別に国家サイバーセキュリティセンターを設置し、国防総省の国家安全保障局（NSA）、国家情報局（ODNI）、行政予算管理局（OMB）など連邦政府内の他のサイバーセキュリティ組織と連携し、連邦政府のサイバーセキュリティの全体を把握する組織としたのである。

このような状況のなかで誕生したのがオバマ政権である。オバマ政権は就任早々、これまでの情報セキュリティ政策を60日間かけてゼロベースで見直し、2009年5月29日に「サイバースペース政策レビュー」を発表した。この報告書では、今やサイバースペースが米国経済、社会インフラ、治安、国防の基盤となっており、経済繁栄を維持しながらセキュリティを確保していくことは、連邦政府の基本的な責任であると位置づけている。そして連邦政府が自ら強いリーダシップを発揮し、国民への啓蒙活動を行い、民間企業とのパートナーシップを推進し、州政府や地方政府および国際的な連携を進め、インセンティブによって市場メカニズムを利用した施策を実行していくとしている。そして、次のような短期的な活動計画を挙げている。

・サイバーセキュリティ政策・活動を調整するサイバーセキュリティ政策担当官を指名し、省庁間でのサイバーセキュリティ関連の戦略・政策を調整して、国家安全保障会議（NSC）を強力な組織とする。
・情報通信インフラの安全を確保するための国家戦略を見直す。
・サイバーセキュリティを大統領のマネジメント優先事項として位置付け、評価指標を確立する。
・NSCのサイバーセキュリティ部局にプライバシー・市民の自由担当官を任命する。
・サイバーセキュリティに関連する政策立案過程で、省庁間における法的な検討を行って首尾一貫した政策ガイダンスを策定するため、省庁横断的な仕組みを構築する。
・サイバーセキュリティを推進するための啓蒙活動や教育キャンペーンを実施する。
・国際的なサイバーセキュリティ政策のフレームワークのなかの米国政府の位置付けを強化し、国際的なパートナーシップを強化してすべての課題に対応できる取り組みを行っていく。
・サイバーセキュリティ事件に対応するための計画を準備し、官民パートナーシップ強化のための対話を開始する。
・他の大統領府と連携して、サイバーセキュリティ対策に資する研究開発のフレームワークを策定し、研究者に事象データへのアクセスを提供する。
・サイバーセキュリティに基いたIDマネジメントのビジョンと戦略を策定する。

この発表後の2009年7月、米国と韓国の政府機関のウェブサイトが大規模なハッカー攻撃を受けた。韓国政府は、北朝鮮通信庁のIPアドレスが使われているため、北朝鮮政府が関与した組織的なテロ活動であると断定しており、米国連邦政府はあらためて組織的なサイバー攻撃を認識することとなった。また年末にはGoogleをはじめ20社以上の大企業がサイバー攻撃の対象として狙われるという組織的な事件も起こっている。

サイバー犯罪からサイバー戦争へという事態の変化に対し、国防総省は2010年5年21日、サイバー司令部（Cyber Command）の設置を発表した。

サイバー領域は陸、海、空、宇宙と同等の重要性を持ち、軍事ネットワークを守ることは国防にとって極めて重要だという認識のもと、この新しい司令部にサイバー関連の機能を集約して一つの組織に統合している。本格稼動は10月からで、フォートミード陸軍基地に設置されるサイバー司令部では約1000人が活動する予定となっている。産業界との連携や情報共有を進め、イギリス、オーストラリア、カナダとも国際的な連携を強め、国土安全保障省のサイバーセキュリティ組織ともうまく省庁間連携できるとしている。このように米国ではサイバー犯罪から情報を保護するという姿勢から、サイバー戦争へ対応するという姿勢へと軸足を移しつつある。

3 欧州における情報セキュリティ政策

欧州委員会は2010年3月、現在の経済危機から脱し今後10年間の経済成長を支えるための戦略として“Europe 2020”を発表した。この戦略においては、スマートな（賢い）成長（知識とイノベーションに基づく経済の発展）、持続可能な成長（省資源、環境配慮型、競争力のある経済）、包摂的成長（社会的絆を生み出す高雇用率の経済）の3つを柱としている。そして、この戦略において主要な役割を果たす7つのフラッグシップ・イニシアティブの一つである“A Digital Agenda for Europe”が5月に発表された。これは情報技術（ICT）を活用してEurope 2020を実現していくための行動計画であり、情報セキュリティに対する欧州の姿勢を伺うことができる。

このアジェンダのなかの情報セキュリティ関係の記述において、まずICTが技術的な信頼性に欠けるため、まだヨーロッパでは受け入れられていないことを指摘している。実際にスパムメールが増殖し、ウィルスやマルウェアがはびこるだけでなく、エストニア[注1]、リトアニア[注2]、グルジア[注3]がサイバー攻撃を受けるなどICTを活用したテロ活動が頻発したことがその要因である。しかし、欧州としては、今後の経済発展のためにはICTによって欧州市場を一つの市場へと統合していくことが不可欠であると認識しており、そのためにEUと加盟国は情報セキュリティ対策に協力して取組むという姿勢を打ち出している。その鍵となるアクション項目が下記の2点である。

・欧州ネットワーク情報セキュリティ庁（ENISA）の強化案など、現在よりも一層強化したネットワーク情報セキュリティポリシーを作ること、およびサイバー攻撃への迅速な対応のためにCERT（Computer Emergency Response Team：危機対応チーム）のネットワークを設立すること。
・2010年までにサイバー攻撃と戦うための法案を提出し、2013年までに欧州および国際間でのサイバースペースにおける裁判権の関連規則を準備する。

欧州ネットワーク情報セキュリティ庁（ENISA）とは、EUの情報セキュリティを支援するための組織であり、加盟国から独立した機関である。サイバーセキュリティ事件そのものに対応するための組織ではなく、セキュリティに関する情報提供や政策アドバイスなどを使命としていたが、今回のアジェンダで従来よりも強化されることとなった。さらに、その他のアクションとして下記が挙げられている。

・2012年までに欧州サイバー犯罪プラットフォームを設立する。
・2011年までに欧州サイバー犯罪センター構築の実現可能性を検討する。

・諸外国と協力してグローバルなリスクマネジメントを強化し、サイバー犯罪や攻撃に対して国際協調による行動を起こす。
・2010年から、EUによるサイバーセキュリティ準備訓練を支援する。
・EU個人データ保護規制のフレームワークをわかりやすく法的に強固なものにする一環として、セキュリティ侵害に関する届出条項の拡大を検討する。
・個人のプライバシーおよび個人情報の保護に関する新しいテレコム・フレームワークを実装するため、2010年までにガイダンスを提供する。
・違法コンテンツ・ホットラインを設け、子どもたちへネットワークの安全性についての啓蒙キャンペーンを実施し、欧州全体での協力体制の強化とベストプラクティスの共有を行う。
・特に未成年者の利用に関して、利害関係者間の対話、およびSNSや携帯電話などのサービスプロバイダーの自主規制を推進する。

そして加盟各国は次のような行動を実行することになっている。
・2012年までに、各国のレベルでCERTのネットワークを機能させる。
・委員会と共同で大規模攻撃シミュレーションを実行し、2010年時点における脆弱な戦略を対象にテストを行う。
・有害あるいは攻撃性のあるコンテンツを通報するホットラインを設置し、子どもたちへの啓蒙キャンペーンや学校におけるセキュリティ教育を実施し、2013年までに子どもを守るためのプロバイダー自主規制を推進する。
・各国の警報プラットフォームを欧州警察サイバー犯罪プラットフォームに適合させる作業を2010年に開始し、2012年までに完了させる。

欧州各国でもそれぞれ情報セキュリティ対策を実行している。イギリスやフランスではそれぞれ専門部署や機関を設けて情報セキュリティ対策の強化を図っており、2007年に大規模なサイバー攻撃を受けたエストニアでは、その後NATO7カ国の支援を受けて調査や研修を行い、防衛省が中心となって対策を取りまとめている。

各国ではそれぞれの事情により情報セキュリティへの取り組み姿勢が異なるが、これまで見たように欧州全体としてはICTによる市場統合を行って経済発展につなげるという大きなビジョンを持っており、そのビジョンを実現するために各国が連携して情報セキュリティ対策に取組んで行く方針である。

4 韓国の情報セキュリティ

韓国では隣国との緊張関係から、情報セキュリティは国家の安全保障に関わるものとして、諜報機関を中心に業務が統括されている。李政権以前では、韓国における情報セキュリティに関わる組織として、全体を調整する国家安全保障会議（NSC）を中心に、公共部門を統括する国家情報院（NIS）、民間部門を統括する情報通信部（MIC）、国防を担う国防部（NMD）が構成されていた。そして具体的な実行組織として、国家情報院の下の国家サイバー安全センター（NCSC）、情報通信部の下の国家情報保護振興院（KISA）およびインターネット侵害事故対応支援センターなどが組織化されていた。

しかし、2008年の李明博政権の誕生により、情報セキュリティに関わる組織構造が大きく変わった。民間部門を統括していた情報通信部が廃止され、その機能は公共政府安全部（MOPAS）、韓国知識経済部（MKE）、放送通信委員会（KCC）に

分散されている。政府機関におけるセキュリティは国家情報院が主導的な立場をとり、その配下にある国家サイバー安全センターが実行組織となっている。そこでは国全体の情報セキュリティ政策の調整、セキュリティ対策の促進、脅威に関する情報の収集と対処などを行っている。その後、2009年7月には韓国政府のウェブサイトが北朝鮮による大規模なサイバー攻撃を受け、2010年5月には哨戒艦沈没事故を契機として緊張が高まったことなどで、北朝鮮によるサイバーテロを想定した警戒および対策を国レベルで強化している状況にある。

一つの事例として、地域情報開発院（KLID）の情報セキュリティ対策状況（2010年5月時点）について報告する。この組織は、日本の財団法人地方自治情報センターに該当する組織であり、全国自治体情報化の推進・支援を行っている。このセンターは総勢109名で運営されており、情報セキュリティに関する事業としては、技術支援センター運営、サイバー侵害対応支援センター運営、行政電子署名認証（GPKI）維持管理の3つを実施している。特徴としては、システム障害などに対応するための技術支援センターとサイバー攻撃などに対応するためのサイバー侵害対応支援センターとが明確に分かれていることである。

技術支援センターでは、自治体の各業務システムサーバの監視を行っており、システムの異常などを検知し、各自治体の運用管理を支援している。**写真**はそのセンターに設置されている大画面モニターであるが、ここで全国自治体のサーバやネットワークの状況がすべて把握されている。モニターに対面して10名程度の職員が着座しており、それぞれ各自のパソコンで異常状況の調査などを行っている。機能としては、自治体統合管制、統合状況画面監視、電子政府統合ネットワーク管制、主要行政情報管理システム管制、自治体業務別予測/分析、KIOSK統合管制、業務別使用率分析報告、内外部網業務サーバ統合管制、業務サーバの保安ログ確認、自治体WAS統合状況確認、実時間機能リソース確認、WAS機能管制、ネットワークトラフィック確認などである。

一方、サイバー侵害対応支援センターは2009年6月に設立された新しい組織である。これは数年前のサイバー攻撃を契機として、2005年から2008年の間に自治体と協議を行って設立した組織である。246（16の広域自治体と230の基礎自治体）の自治体すべてを対象としてサイバー侵害を監視している。国家サイバー安全センター、政府統合電算センター、韓国インターネット振興院（NIDA）とも連携し、サイバー侵害対応システムで24時間365日監視しており、昼間は15人体制、夜間は2名体制で対応している。トラフィック異常時に自治体の担当者へ連絡し、ハッキング行為なのかテロなのかを判断し、自治体担当者が対応できない場合はセンターが対応を支援している。技術支援センターとすぐ隣り合わせの場所にあり、大画面モニターや職員の配置などはほとんど同じであったが、このセンターは写真撮影が許可されなかった。

具体的な機能としては、企画支援、分析・対応、

写真　技術支援センターにおける各自治体の業務サーバ監視状況

状況管制の3つがある。企画支援としてはサイバー侵害対応戦略及び政策立案、サイバー侵害対応支援センター運営･管理、サイバー侵害対応専門教育企画及び運営、16市道との協議窓口、政府統合電算センター及び関係機関との連携、サイバーテロに備える訓練、分析・対応としてはサイバー侵害対応戦略及び政策立案・運営、弱点診断及び対応、サイバーテロの原因分析、サイバー攻撃の対応方法確立及び普及、各種規約の作成及び普及、サイバー侵害対応の模擬訓練実施、テロ事故の事例収集、状況管制としてはサイバーテロ事故の状況統制、脆弱点の発見管理及び対応方法確立・普及、サイバー攻撃事故対応のシステム運営、サイバー攻撃・侵害事故の類型分析、サイバー攻撃・侵害事故の統計管理及び報告を実施している。

5 おわりに

米国や韓国では、民間取引の安全確保のための情報セキュリティから、安全保障のための情報セキュリティへと軸足が移っている。米国ではサイバー司令部を創設し、韓国では自治体へのサイバー攻撃についても監視体制を広げ、情報セキュリティ対策を強化している。欧州ではICTを欧州全体の経済成長のための重要な手段として位置づけ、安全な取引が可能な統合デジタル市場というビジョンを実現するために、各国およびEU加盟国が協調してサイバー攻撃へ対抗しようとしている。このように各国の事情はさまざまであるが、ますます重要性が高まるネットワークの保護を安全保障の範疇で捉える傾向にあると指摘できる。

2010年5月11日、日本では情報セキュリティ政策会議が新たに「国民を守る情報セキュリティ戦略」を発表した。サイバー攻撃の発生を念頭に置いた政策を強化しているものの、テロという意識はあまり強くないようである。しかも、防衛省との具体的な連携に関する記述はなく、国際連携においても犯罪やサイバー攻撃については触れているが、テロや戦争といった安全保障に関する意識については諸外国との隔たりを感じる。本稿が今後の日本の情報セキュリティ政策を考えるうえでの一助となれば幸いである。

【注】

1.2007年4月に政府機関がDDoS※攻撃を受ける。個人や犯罪組織の能力をはるかに超えた規模の攻撃であり、テロというより戦争と呼ぶほうがふさわしいとの指摘もある。
※Distributed Denial of Service：大量のデータを送りつけてサーバの機能を麻痺させる。

2.2008年6月に300近いWebサイトが攻撃を受ける。

3.2008年8月に政府機関がDDoS攻撃を受ける。

【参考文献】

・株式会社三菱総合研究所、「各国の情報セキュリティ政策における情報連携モデルに関する調査」（平成20 年度内閣官房情報セキュリティセンター委託調査）、平成21 年3 月
・株式会社NTTデータ経営研究所、「ヨーロッパの情報セキュリティ政策における協力・連携体制に関する調査」（平成21 年度内閣官房情報セキュリティセンター委託調査）、平成22 年3 月
・The United States Government,“ Cyberspace Policy Review”, 2009.5.29
・European Commission,“Europe 2020”, 2010.3.3
・European Commission,“A Digital Agenda for Europe”, 2010.5.19
・韓国地域情報開発院、「大韓民国地域情報化の脈」、2010年5月説明資料

※本記事への問い合わせ：enami.toshihiro@jp.fujitsu.com