

政府のサイバーセキュリティ戦略

谷脇 康彦 ●内閣サイバーセキュリティセンター 副センター長

深刻さを増すサイバー脅威に対し、政府は重要インフラの防護、人材育成と技術開発、国際連携強化対策を進めている。2014年11月成立の「サイバーセキュリティ基本法」を基盤にスタートした新体制は、2020年夏に向け重責を果たすことが求められている。

■サイバー脅威の現状

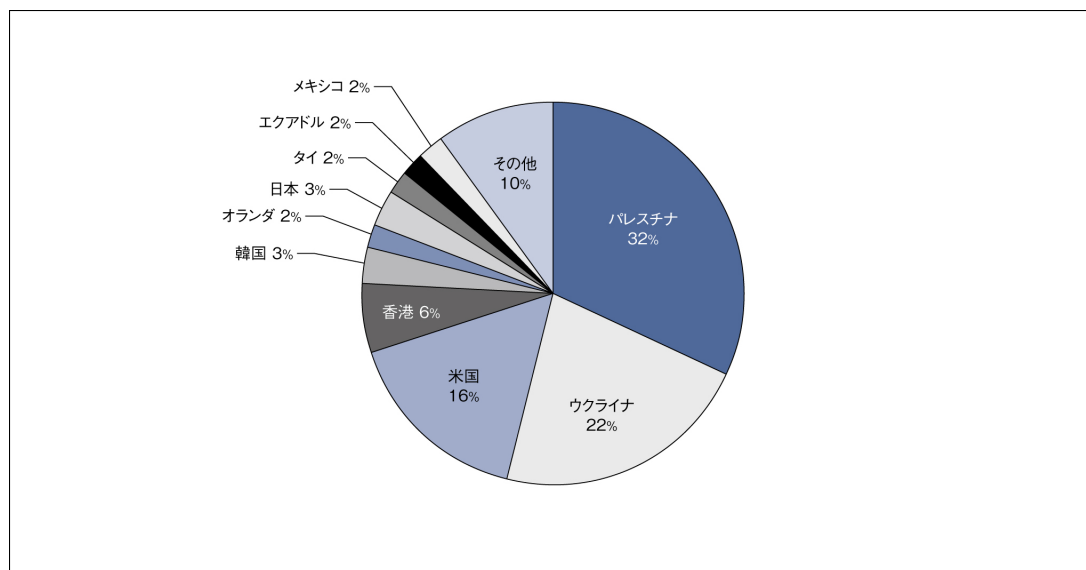
サイバー空間の脅威は深刻化の一途をたどっている。第一に、政府や独立行政法人の保有する機微性の高い情報を狙った巧妙な攻撃が急増している。内閣サイバーセキュリティセンター（NISC）では各府省の情報システムを24時間365日体制で監視しているが、2013年度の政府機関に対する攻撃（不正通信）は約508万件に上り、6秒に1回の割合で攻撃を受けている。2012年度の攻撃件数は約108万件であり、わずか1年で約5倍に急増している。

第二に、サイバー攻撃の対象範囲が拡大している。普及著しいスマートフォンは大量の個人情報を取り扱うが、これを標的とする不正サイトが約3千（2011年度末）から約5万7千（2013年度末）と、20倍の増加となっている。また、もはや電子部品やソフトウェアの塊である自動車に対するハッキングも技術的に可能との報告も米国で行われ、関係者に大きな衝撃を与えている。設置が進むスマートメーター（検針メーターに通信機能を備え

た次世代電力量計）も備えが必要な分野である。東京電力管内では2020年度末までに約2700万台のスマートメーターを設置する計画であり、他の電力各社もおおむね2023年度までに設置を完了する。これまで電力網は通信網と切り離されてきたが、これが一体化することから、サイバー攻撃による停電発生等に備える必要がある。

第三に、攻撃がグローバル化している。一例を挙げれば、2013年3月に韓国で大規模なサイバー攻撃が発生し、金融機関のATM等が機能停止し、大きな混乱が生じた。この攻撃に使用された不正プログラムは、わが国でも同時期に発見されている。国境のないサイバー空間において、多様な主体が攻撃を行っていることは、次のデータ（資料6-2-2）からも読み取ることができる。標的型メール攻撃（標的とされた機関にメールを送付して不正プログラムに感染させて情報を窃取するもの）に使用された不正プログラム等の接続先をみると、実にその97%は、海外のサーバーという状況である。

資料6-2-2 標的型メール攻撃に使用された不正プログラム等の接続先



出典：平成25年中のサイバー攻撃の情勢及び対策の推進状況について（警察庁、2014年2月）

■政府機関等の防御能力の強化

深刻化するサイバー脅威に対し、2013年6月、政府は「サイバーセキュリティ戦略」を策定し¹、①政府機関等の防御能力の強化、②人材育成や技術開発等の基礎体力の強化、③国際連携の強化を三本柱として推進することを決定した。この中で①の政府機関等の防御能力の強化については2つの観点からセキュリティ強化に努めている。

●政府機関への標的型攻撃への対応

第一に、政府機関に対する標的型攻撃への対応である。2014年5月、政府は各府省のセキュリティポリシーの基礎（ベースライン）となる「政府機関統一基準群」の改定を行った。ポイントとなるのは、政府機関が保有する防衛、外交、技術等の機微性の高い情報を窃取する攻撃、とりわけ標的型メール攻撃への対策強化である。標的型メール攻撃はセキュリティソフトを潜り抜け、受信者の心の隙を巧妙に突いて添付ファイル（不正プログラム）やメールに記載したリンクを踏ませて端末

を感染させる。情報システムの内部に侵入した攻撃者は静かにシステム内の探索を行い、管理者権限を奪取して機微な情報を探索・窃取し、外部に送信する。

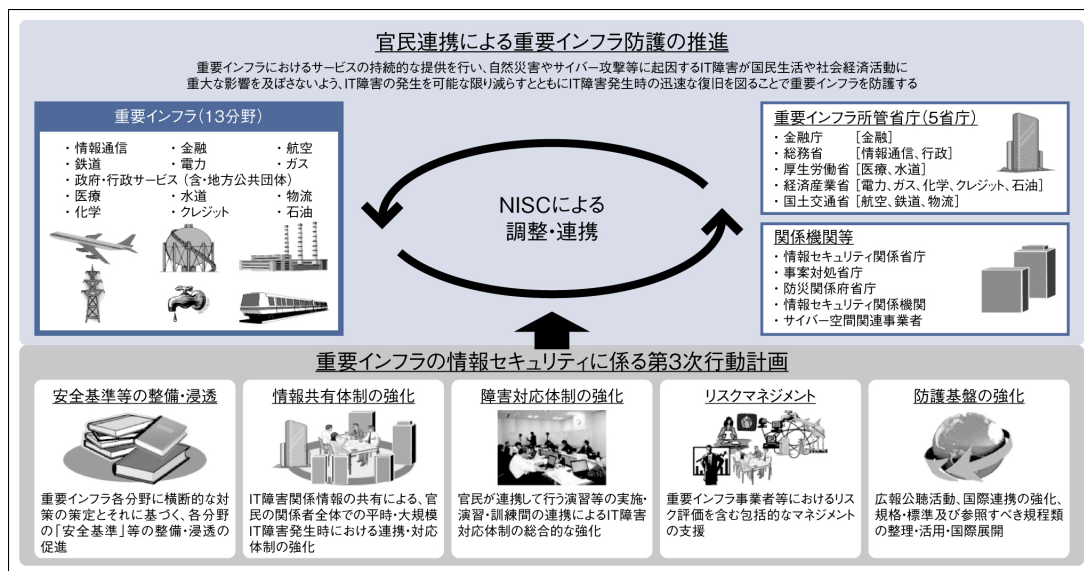
こうした標的型メール攻撃の成功率は10～15%であり、何度かメールのやり取りをして攻撃対象（受信者）を信用させてから不正プログラムを送り込む「やり取り」型の場合には約20%の確率で成功する。このため、従来の入口・出口対策に加え、内部探索しづらいシステム設計やトラップ（罠）による攻撃者の感知など、攻撃者に侵入されたことを可能な限り迅速に把握し、被害を最小化する多重防御の仕組みを導入することとしている。ただし、効率的に多重防御の仕組みを構築する観点から、重要な情報が保存されているサーバーを特定（リスク評価）し、評価結果に基づいて多重防御を行うべき情報システムを特定するなど、メリハリのある対策を進めている。

●重要インフラ事業者のセキュリティ対策

第二に、重要インフラ事業者のセキュリティ対策の強化である。重要インフラ事業者はIT依存度が高く、情報システムがサイバー攻撃によって機能不全の状態に陥ると社会経済活動に深刻な影響を及ぼす。このため、2014年5月、政府は「重要インフラの情報セキュリティ対策に係る第3次行動計画」を決定した²。本行動計画では重要インフ

ラの分野を通信、電力、鉄道、航空など従来の10分野に加え、クレジットカード、石油、化学の3分野を新たに重要インフラとして指定し、政府機関や重要インフラ事業者を含む関係者相互のインシデント情報の共有、分野横断的演習の実施、共通脅威分析の実施等の施策を引き続き講じていくこととしている（資料6-2-3参照）。

資料6-2-3 重要インフラを守る「第3次行動計画」の全体像



出典：重要インフラの情報セキュリティ対策に係る第3次行動計画（内閣官房情報セキュリティセンター、2014年6月）

今回の行動計画では、重要インフラ事業者の経営層に情報セキュリティの重要性を訴求する内容が盛り込まれた他、中小の重要インフラ事業者が優先的に取り組むべき対策を明らかにすることとされた。行動計画の方針に沿って、重要インフラ事業者が安全基準等を策定する場合の指針等の改定作業が現在進められており、年度内を目途に完了する運びとなっている。

■セキュリティ確保のための基礎体力の強化

次に、戦略の2つめの柱である「基礎体力の強化」について、人材育成と技術開発の2つの観点から述べることにする。

わが国におけるセキュリティ人材は約26.5万人いるが、そのうち約16万人は一定の水準に達していないといわれている。また絶対数も約8万人不足している。しかし、セキュリティ分野に限定することなくわが国のIT人材を俯瞰してみると、約106万人存在している。こうした人材のリカレン

ト教育などによりセキュリティ分野の知識を持ってもらうことで、人材不足のかんりの部分を補うことができる。

しかし、人材育成には、需要面と供給面の双方で十分な環境整備ができていない。需要面においては、企業の経営層の意識改革が求められる。具体的には、サイバー攻撃を深刻な経営リスクとしてとらえ、社内の人材・体制の整備を図るよう行

動することが必要である。例えば、企業における個人情報漏えいインシデントを原因別にみると、不正アクセスによるものは全体のわずか5.0%に過ぎない。しかし、インシデントの規模から上位10件をみると、そのうち7件は不正アクセスを原因とするものであり、ひとたび不正アクセスによる情報漏えいが発生すると、深刻な損害を企業が蒙ることとなる（資料6-2-4）。

資料6-2-4 インシデント・トップ10

No.	漏えい人数	業種	原因
1	400 万人	情報通信業	不正アクセス
2	169 万 2496 人	情報通信業	不正アクセス
3	47 万人	卸売業、小売業	不正アクセス
4	42 万 6000 人	公務（他に分類されるものを除く）	紛失・置忘れ
5	24 万 3266 人	情報通信業	不正アクセス
6	17 万 5297 人	情報通信業	設定ミス
7	15 万 0165 人	卸売業、小売業	不正アクセス
8	12 万 0616 人	金融業、保険業	管理ミス
9	10 万 9112 人	情報通信業	不正アクセス
10	9 万 7438 人	情報通信業	不正アクセス

出典：2013年情報セキュリティインシデントに関する調査報告書～個人情報漏えい編～（NPO日本ネットワークセキュリティ協会、2014年12月）

供給面においても、環境改善が必要である。具体的には、セキュリティ業務従事者のスキルを客観的に評価する仕組みの整備、過去の具体的なインシデントを基にサイバー演習を行う実践的な演習環境の整備などが求められる。

こうした問題意識をふまえ、2014年5月、政府は「新・情報セキュリティ人材育成プログラム」³を策定したところであり、その具体化に向けた取り組みが各府省において進められている。

基礎体力の向上に向けたもう一つの取り組みが、技術開発力の強化である。2014年7月、政府は「情報セキュリティ研究開発戦略（改訂版）」⁴を策定し、サイバー攻撃の検知・防御能力の向上に向けた技術開発等に注力する方針を明らかにした。同時に、産業活性化につながる新事業創出への貢献が期待できるセキュリティ技術の開発を進めるた

め、今後、IoT（Internet of Things）のセキュリティに関連した技術開発等について検討を深めていくこととしている。

■国際連携の強化

戦略の三本目の柱は国際連携の強化である。サイバー空間には国境がないことから、セキュリティ確保に向けた信頼醸成や体制強化（キャパシティ・ビルディング）には各国の連携が極めて重要である。こうした問題意識の下、2013年10月、政府は「サイバーセキュリティ国際連携取組方針」⁵を決定し、サイバーセキュリティに関する国際連携強化に向けたわが国の方針を内外に明らかにした。

これまでも政府は米国、英国、ASEAN等の国々と国際連携のための政策協議を進めてきたが、2014年にはさらにイスラエル、フランス、EU、エスト

ニアとの間でサイバー協議を開始したところである。また、ロシアおよび豪州との間でも新たに協議を開始することとなっている。

さらに、2014年10月には重要インフラ防御担当の政府機関30か国の専門家が集まるMERIDIAN会合をわが国に招致し、ホスト国として積極的にコンセンサス作りに努めた他、国連やOECDにおける議論に積極的に参画している。

政府としては、こうした二国間や多国間の協議の場を通じ、サイバーセキュリティ分野の国際連携を引き続き強化していくこととしている。

■サイバーセキュリティ確保体制の強化

2014年11月、国会において「サイバーセキュリティ基本法」が成立した。IT関連の基本法としては2001年1月に施行された「IT基本法」がある。しかし、IT基本法はあくまで民間主導を原則に、ITインフラの整備やIT利活用を推進していくことをその目的としている。サイバーセキュリティ基本法はサイバーセキュリティ分野における国（政府）の主導的な役割を規定した上で、地方自治体、重要インフラ事業者、セキュリティ関連事業者、一般のユーザー企業や国民との連携の下でサイバーセキュリティの確保を目指すことを基本的立場としている。このため、IT基本法とは別に新たな法律として制定したものである。

これまで政府のサイバーセキュリティの推進体制は、関係閣僚や民間有識者で構成する情報セキュリティ政策会議とその事務局である内閣官房情報セキュリティセンターが担ってきた。しかし、いずれの組織も法的基盤がなく、各府省の任意の協力の下で戦略の策定や各府省の情報システムの監視等を行ってきた。しかし、基本法の制定により、こうした組織の法的基盤が明確化された。

●「基本法」に基づく新体制のスタート

具体的には、まず情報セキュリティ政策会議は内閣官房長官を本部長とするサイバーセキュリティ戦略本部に改組された。本部はサイバーセキュリティ戦略を策定し、閣議決定する。戦略の策定に際してはIT総合戦略本部や国家安全保障会議(NSC)の意見をあらかじめ聞く。

また、戦略本部は各府省のセキュリティ対策に関する施策を評価し、第三者的に監査を行うほか、政府機関において重大なインシデントが発生した場合には原因究明調査を行う。さらに、各府省の防御体制の強化など、戦略の推進に必要と認められる場合に、各府省からの資料提出を義務付けるとともに、必要に応じて勧告を行うこととされた。

基本法の成立を受け、政府は「我が国のサイバーセキュリティ推進体制の機能強化に関する取組方針」⁶を決定するとともに、内閣官房組織令等の改正を行い、NISCの名称を内閣サイバーセキュリティセンターと改称し、同センターの業務を組織令等に具体的に規定した（2015年1月、基本法の全面施行とともに組織令等も施行）。また、新体制においては、現行約80名のNISCについても大幅な人員の拡充を図るとともに、最大5年任用することができる任期付職員を民間部門から順次採用するなど体制を強化することとしている。

なお、2020年夏にはオリンピック・パラリンピック東京大会が開催される。2012年夏のロンドン大会では2週間のオリンピック開催中に公式サイトに対する攻撃が2億回を越えた。こうした経験を参考とし、今回の体制強化も踏まえつつ、官民一体となって東京大会に向けたサイバーセキュリティ対策を強力に推し進めることが求められる。（本文中、意見にわたる部分は筆者の個人的見解である）

1. サイバーセキュリティ戦略 [PDF] (内閣官房情報セキュリティセンター、2013年6月)
<http://www.nisc.go.jp/active/kihon/pdf/cyber-security-senryaku-set.pdf>
2. 重要インフラの情報セキュリティ対策に係る第3次行動計画 [PDF] (内閣官房情報セキュリティセンター、2014年5月)
http://www.nisc.go.jp/active/infra/pdf/infra_rt3.pdf
3. 新・情報セキュリティ人材育成プログラム [PDF] (内閣官房情報セキュリティセンター、2014年5月)
<http://www.nisc.go.jp/active/kihon/pdf/jinzai2014.pdf>
4. 情報セキュリティ研究開発戦略(改訂版) [PDF] (内閣官房情報セキュリティセンター、2014年7月)
<http://www.nisc.go.jp/active/kihon/pdf/kenkyu2014.pdf>
5. サイバーセキュリティ国際連携取組方針 [PDF] (内閣官房情報セキュリティセンター、2013年10月)
http://www.nisc.go.jp/active/kihon/pdf/InternationalStrategyonCybersecurityCooperation_j.pdf
6. 我が国のサイバーセキュリティ推進体制の機能強化に関する取組方針 [PDF] (内閣官房情報セキュリティセンター、2014年11月)
<http://www.nisc.go.jp/conference/seisaku/dai41/pdf/houshin20141125.pdf>

1

2

3

4

5

6



1996, 1997, 1998, 1999, 2000, ...

[インターネット白書ARCHIVES] ご利用上の注意

このファイルは、株式会社インプレスR&Dが1996年～2015年までに発行したインターネットの年鑑『インターネット白書』の誌面をPDF化し、「インターネット白書 ARCHIVES」として以下のウェブサイトで公開しているものです。

<http://IWParchives.jp/>

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容(技術解説、データ、URL、名称など)は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者(執筆者、写真・図の作成者、編集部など)が保持しています。
- 著作者から許諾が得られなかった著作物は掲載されていない場合があります。
- このファイルの内容を改変したり、商用目的として再利用したりすることはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用される際は、出典として媒体名および年号、該当ページ番号、発行元(株式会社インプレスR&D)などの情報をご明記ください。
- オリジナルの発行時点では、株式会社インプレスR&D(初期は株式会社インプレス)と著作権者は内容が正確なものであるように最大限に努めました。すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

お問い合わせ先

株式会社インプレス R&D

✉ iwp-info@impress.co.jp