サイバーセキュリティ対策の強化に向けた緊急提言

平成２７年７月３０日
自　由　民　主　党
政　務　調　査　会

はじめに

昨今のサイバー空間を取り巻くセキュリティ上の脅威は、先に発生した日本年金機構による情報漏洩事案に象徴されるように、ますます増大しており、わが国の社会経済活動や国民生活は、今まさに深刻なサイバー攻撃の脅威にさらされている。

陸・海・空・宇宙空間に次ぐ「第５の戦場」とも称される「サイバー空間」において、標的型攻撃はより複雑、巧妙になり、従来の境界防御のみで対応することには限界がある。標的型攻撃における攻撃者の一連の行動を細分化した、いわゆる「サイバーキルチェーン」の考え方に基づき、ネットワーク内部も含めた多層的な防御態勢の構築が不可欠である。

一方で、サイバー空間を「守る側」の体制については、官民ともに人材・投資の両面において圧倒的に不足し、危機的な状況に立たされている。

サイバーセキュリティに関しては、わが国と同様に、その脅威に直面している諸外国においても、急速に対策が進められている。例えば、フランスでは、サイバーセキュリティの司令塔機能を果たしている国家情報システムセキュリティ庁（ANSSI）における職員数は、現在 500 人規模となっている。また、米国では、2014 年度のサイバーセキュリティ予算額が130億ドルを超えており、さらに本年２月に官民の情報共有を強化するための大統領令が制定されたところである。また ASEAN 諸国においても、タイでは、サイバーセキュリティ強化のための新法成立に向けた取組が進められるなど、サイバーセキュリティが早急に取り組むべき最重要課題であるとの認識の下、世界的に様々な取組が行われている。

わが国においても、この状況下において、今後のマイナンバーの導入や、来たる 2020 年東京オリンピック・パラリンピック競技大会を見据え、サイバーセキュリティ対策の強化はまさしく焦眉の急であり、官民を挙げた抜本的な取組の強化が必要である。

党情報通信戦略調査会は、このような認識と危機意識のもと、サイバーセキュリティ政策の推進のあり方について、平成 27 年 7 月に数回にわたり、外部有識者等も交え、精力的に議論を重ね、以下の通り、提言を取りまとめた。

この提言が、政府のサイバーセキュリティ政策の推進やそのための予算編成に適切に反映され、今後官民連携のもとに着実に実行されることを強く要望する。

１　セキュリティ人材の登用・育成強化

わが国では、サイバーセキュリティ人材が圧倒的に不足しており、内閣サイバーセキュリティセンター（NISC）を中心として、以下のような取組を積極的に推進することで、2020 年までに、質的なレベルアップも含めて、少なくとも５万人のサイバーセキュリティ人材の育成に取り組むべきである。

（1）政府・民間におけるセキュリティ人材の登用

巧妙化、複雑化するサイバー攻撃に対応するためには、セキュリティ人材を積極的に採用し、組織内に専門家を確保することが不可欠となってくる。

そのためには、セキュリティを専門とすることがキャリアパス、処遇面において魅力的なものとしていくとともに、トップマネジメントにおけるセキュリティ人材の重要性に対する認識の醸成や、人材育成にかかる費用負担を軽減するための積極的支援が必要となる。

特に、政府及び地方公共団体においては、セキュリティ人材が絶対的に不足しており、人材の積極的な登用を強力に推進することが求められ、民間から専門的人材を登用する際にも、任期の長期化や待遇の改善を行うべきである。

例えば、専門家を短期的に採用するだけでなく、組織のセキュリティに関するマネジメントを担うポストを新設し、それに向けて、セキュリティ人材が中長期的なキャリアパスを描ける取組を、政府や地方公共団体においても行うことが必要である。

加えて、NISCや各省におけるセキュリティ人材の採用枠を、定員純増の形で創設すべきである。

さらに、各府省における幹部から一般職員に至るまで全ての職員のサイバーセキュリティ能力の質的向上を図ることも必要である。政務を含む幹部が、インシデント発生時等に的確な判断を迅速に行うための意識醸成や、一般職員に対するサイバーセキュリティに関する教育を常に行うべきである。

また、政府機関等で重大なインシデントが発生した際には緊急的な対応が必要となるため、官民の所属に捉われずに、対処できる優秀な人材を機動的に招集できる仕組みを導入すべきである。

【具体的な取組】

○ 政府・地方公共団体における民間の専門的人材登用の際の任期の長期化や待遇の改善
○ 政府・地方公共団体における組織のセキュリティマネジメントを担うポストの新設
○ 政府・地方公共団体におけるセキュリティ人材の中長期的キャリアパスの形成
○ NISCや各省におけるセキュリティ人材の採用枠の創設（定員の純増）
○ 政務を含む府省の全ての職員に対するサイバーセキュリティ能力向上のための教育の実施
○ インシデント発生時に対処できる人材を機動的に招集できる仕組みの構築

（2）実践的な訓練・演習を通じた人材育成

セキュリティ人材の育成にあたっては、特に、サイバー攻撃を受けることを前提とした実践的な演習を通じて、多重防御の設計をどう構築すべきか、及び攻撃を受けた際にどのように対処すべきかを経験することが必須である。

政府機関、重要インフラのみならず、地方公共団体、中小企業、教育機関等の幅広いニーズに対応して、実践的な演習の機会を確保することが不可欠となり、そのための演習予算を抜本的に拡充すべきである。

例えば、サイバーセキュリティに関する資格制度の検討を行う際にも、実践的な訓練・演習を通じたスキルの取得を要件とすることが求められる。

また、限られた期間にサイバー攻撃が集中することが予想される 2020 年東京オリンピック・パラリンピック競技大会に向けても、実際の大会を想定した大規模な演習※を繰り返し実施し、攻撃への対処能力を高めることが欠かせないため、相応の予算措置が必須である。

（※ロンドン大会では少なくとも5回にわたり演習を実施。）

さらに、サイバー攻撃への対処はボーダーレスな課題であり、国際的に連携して、合同のサイバーセキュリティ訓練・演習等に取り組むことも重要である。

【具体的な取組】

○ 政府、重要インフラのみならず、地方公共団体、中小企業、教育機関等の幅広いニーズに対応できる実践的な演習予算の抜本的拡充
○ 資格制度における、実践的な訓練・演習を通じたスキルの取得の要件化
○ 2020 年東京オリンピック・パラリンピック競技大会に向けた大規模演習を繰り返し実施するための予算措置
○ 国際的に連携した合同のサイバーセキュリティ訓練・演習の実施

２ セキュリティ予算の抜本的拡充

現在、わが国のセキュリティ研究開発予算額は、対 GDP 比率において、米国のわずか 12 分の1にすぎない。このようにわが国では、サイバーセキュリティに関する研究開発予算をはじめとして、サイバーセキュリティ分野に配分すべきリソースが圧倒的に不足している。そのため次のような取組については、重点的・戦略的に政府予算を配分することが重要となる。

（1）政府予算の抜本的拡充

新たなサイバー攻撃に対応するためには、従来のシーリングの枠組みにとらわれず、政府システムにおける多重防御の取組の加速化をはじめ、セキュリティ対策を強化し、NISCによる監視・監査体制の拡充、上記の人材育成のための演習基盤構築、サイバー脅威に関する情報の共有・分析等を行うISAC（情報　共有・分析センター）における官民の情報共有を円滑に行うための基盤の構築など、抜本的な取組強化のための予算確保が必須となる。

なお米国においては、地方自治も含め 19 分野にわたり ISAC が設置されている一方で、わが国の現状は、通信・金融のわずか2分野にとどまっており、これ以外の分野でも幅広く情報共有が行われるよう、ISAC の展開を進めるべきである。

また、各省の業務等の ICT 化により節約できた予算を、サイバーセキュリティ対策に重点的に振り向ける等、抜本的な予算の組み替えを行うべきである。

その際には、政府全体としてのセキュリティレベルの底上げを図るために、各府省における取組の進捗状況等を可視化し、先進的なセキュリティ対策を行っている府省の取組を基準として、対策が遅れている府省や地方公共団体にも対策を促す等の仕組みが求められる。

加えて、予期できない大規模なインシデント等に迅速に対応できるよう、インシデント対応に要する予算・設備を NISC 主導で弾力的に運用できる仕組みの導入が必要である。

【具体的な取組】

○ 従来のシーリングにとらわれないセキュリティ枠を創設し、各省のセキュリティ予算を特別枠として確保
○ ISAC における官民情報共有の基盤構築
○ 幅広い分野での ISAC の設置
○ 各省の業務等の ICT 化により節約できた予算のサイバーセキュリティ対策への重点的振替
○ 先進的なセキュリティ対策を行っている府省の取組を基準とし、対策が遅れている府省や地方公共団体にも対策を促す等の仕組み
○ インシデント対応に要する予算・設備を NISC 主導で弾力的に運用できる仕組みの導入

（2）国産セキュリティ技術の振興

巧妙化・多様化が進むサイバー攻撃に対して、先行した対策を講じられるようにする技術開発は、喫緊の課題である。

国産の技術による世界一安全なサイバー空間の実現を目指し、従来の境界防御に加えてネットワークの内側でもリアルタイムに観測・分析を行うなど、標的型攻撃に対する先導的な研究開発及び成果の普及・展開の取組を推進する必要がある。例えば、研究開発により得られた成果を政府が率先して採用していくべきである。

【具体的な取組】

○ 先行した対策を講じられるようにする技術開発
○ 標的型攻撃に対する先導的な研究開発及び成果の普及・展開
○ 政府による率先した成果の採用

（3）セキュリティ産業の裾野の拡大

来たるべき IoT 社会においては、脆弱性を有する多くの端末・システムが普及する恐れがあるため、セキュリティの確保が一層重要な課題となる。「セキュリティ・バイ・デザイン」の考え方に基づき、センサ等の分野で強みを持つわが国発の IoT セキュリティ技術・システムを起点として、産業競争力の強化につなげることが重要である。具体的には、実装しやすい軽量な暗号の開発や、ガイドラインの策定などについて、政府が積極的に推進していく必要がある。

【具体的な取組】

○ リソースが限られた IoT 機器に実装しやすい軽量な暗号の開発
○ IoT 機器の運用に関するセキュリティ面でのガイドラインの策定

３ マイナンバー導入を踏まえた地方公共団体における対応強化

来たるマイナンバー導入に際するセキュリティ確保は、国民生活に重大な影響を与える政府における重要な課題である。

特に、マイナンバーシステムがつながる地方公共団体まで含めて、LG-WAN（総合行政ネットワーク）を始めとする地方公共団体のネットワークに対するサイバー攻撃の監視体制の構築や、セキュリティ人材の登用・育成など、トータルな対応が必要となる。

また、地方公共団体のセキュリティ対応能力の向上のため、セキュリティインシデントへの対応を行う CSIRT（コンピューターセキュリティインシデント対応チーム）や、インシデント発生時に技術的な支援を行う地域版 CYMAT（情報セキュリティ緊急支援チーム）の設置についても、検討を進めていく必要がある。

加えて、小規模な地方公共団体にも十分なセキュリティ対策を講じることができるよう、クラウドサービスの活用を推進し、重要な情報やシステムを集中的かつ効率的に守る仕組みの構築が不可欠である。なお、このような取組を進める際には、政府は地方6団体等、各地方公共団体の意見を十分に聴き、理解を求めた上で、国・地方が一体的となって推進していくことが重要である。

さらに、財政難やセキュリティ人材の不足が深刻化している地方公共団体における対応には限界があり、政府が積極的に支援できるよう、予算措置による情報システム監視や人材育成に係る支援策を講じるべきである。

【具体的な取組】

- ○ LG-WAN に対するサイバー攻撃の集中監視機能の設置のほか、地方公共団体の情報システムにおける監視機能の強化、セキュリティ人材の登用・育成
- ○ 地方公共団体における CSIRT や地域版 CYMAT の設置
- ○ 地方公共団体におけるクラウドサービスの活用を進めるとともに、地方と政府の役割体制を整理
- ○ 政府の予算措置による地方公共団体における情報システムの監視、セキュリティ人材育成等のセキュリティ対策への支援

４ 制度的検討等

セキュリティ人材の育成やセキュリティ産業の振興をさらに進めるためには、サイバー攻撃へのより効果的な対策への取組を萎縮させているような制度を見直す必要がある。

特にサイバー犯罪は、インターネットバンキングにおける相次ぐ不正送金の被害の拡大の例からも明らかなとおり、広範囲にわたって非常に深刻な被害を及ぼす犯罪であるだけなく、犯人の特定が困難なことも多いのが特徴である。こうした犯罪に対して厳格な対処を可能とするため、例えば、攻撃手法の調査を行うためのアクセス行為やマルウェアの分析・解析等を、正当な目的によるサイバー攻撃対策として特例的に可能とするなどの制度的枠組みを、不正アクセス禁止法、著作権法、通信の秘密等の側面から、体系的に検討することが必要である。

また、外部からの攻撃のみならず、内部犯行への対応も重要な課題である。雇用契約において、情報漏えいやそれに伴う損害への対応等に関する事項を明確に盛り込むことで、雇用側が内部犯行や情報漏えいに対し厳格な姿勢で臨むことを明確にする等、雇用慣行の見直しについても検討を早急に進める必要がある。

さらに、政府や地方公共団体の職員についても、既存の守秘義務規定の枠組みでの対応にとどまらず、情報漏えい等について厳格な処分の導入等の検討を進めるべきである。

【具体的な取組】

○ 攻撃手法の調査を行うためのアクセス行為やマルウェアの分析・解析等を、正当な目的によるサイバー攻撃対策として特例的に可能とするなどの制度的枠組みの体系的検討

○ 内部犯行への対応として、個人情報の漏えいやそれに伴う損害への対応等に関する事項を明確化する等の雇用慣行の見直し

○ 政府や地方公共団体における情報漏えい等について厳格な処分の導入

結びに

党情報通信戦略調査会は、サイバーセキュリティ対策とそのための人材育成について、いずれも将来におけるわが国のサイバー空間の安全を確保する上で必要不可欠であることから、特に NISC が中心となって各府省が連携して積極的な取組を進めていくことを強く期待する。

具体的には、例えば NISC が司令塔となり、各府省が将来も見据えたサイバーセキュリティに関する人材の育成を含む取組の計画を策定し、その計画に基づいて、中長期的な観点でリソースが重点的に配分されるような枠組みを構築することが必要である。このようなしっかりとしたグラウンドデザインに基づいたサイバーセキュリティ対策を進めることは、新しい産業の創出、経済社会全体の効率化、良質で低廉な行政サービスの安定的提供等につながり、安全なサイバー空間を適切に活用した経済成長及び健全な行政の実現を期待することができると確信している。

一方で、医療分野におけるレセプトのオンライン化によって、業務の効率化やコストの削減がどの程度進んだかが必ずしも明確になっていない現状もあるように、今後は各分野における具体的な目標やその達成状況、投資の進展状況等を明確にして取り組んでいく。

党情報通信戦略調査会は、以上に掲げた各取組について、官民が総力を挙げて推進し、来年度の予算編成の際には、これらの取組を進めていく上で不可欠となる予算上の措置が適切に行われることを強く政府に求める。