資料３

NISC National Information Security Center

情報セキュリティ研究開発戦略（改定版）（骨子案）

平成26年4月

内閣官房情報セキュリティセンター

1. これまでの情報セキュリティ研究開発戦略の進捗状況について

- 2011年7月に策定した、現在の「情報セキュリティ研究開発戦略」では2011年度から15年度までの5年度間に重点的に取り組むべき情報セキュリティ研究開発分野を特定と、研究開発予算の充実を掲げている。
- しかし、政府の情報セキュリティ研究開発費は2007年度から2014年度までを比較すると、補正予算等により大幅に研究開発予算が増加している年度もあるものの、当初予算は減少傾向となっている（図1）。一方、米国の情報セキュリティ研究予算は2007年度2014年で大幅に増加している（図2）。
- 他方、情報セキュリティに係る予算は増加傾向。平成26年度予算では、大規模サイバー攻撃事態に対処するための機能の強化、サイバー情報収集装置の整備　等より実践的な施策のための予算となっている。情報セキィリティの被害が深刻になる中、より実践的な対策を推進するための予算となっている。

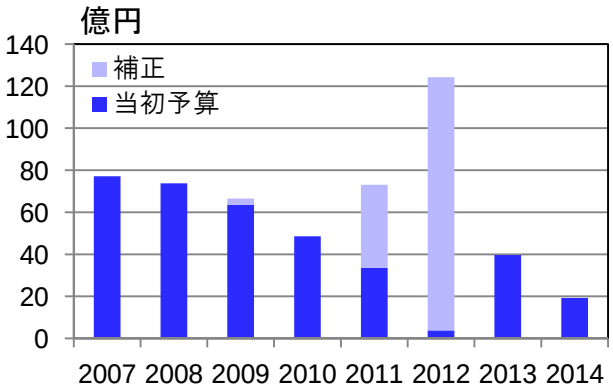


図 1：日本政府の情報セキュリティ研究開発予算の推移

（2010年度以前は、情報セキュリティ研究開発戦略（2011年7月策定版）の値を使用。2011年度以降は、内閣官房情報セキュリティセンターに登録された情報セキュリティ予算から、研究開発に該当するものを事務局で計上。各年度の計上値に独立行政法人の運営費交付金の内数等は含まず。）

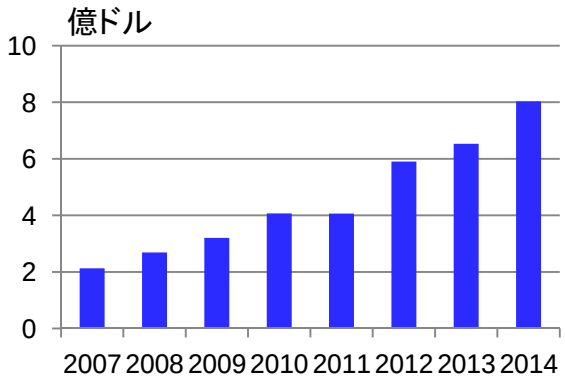


図 2：米国政府（NITRD CSIA）の情報セキュリティ研究開発予算の推移

（2013, 2014年は予算要求額）

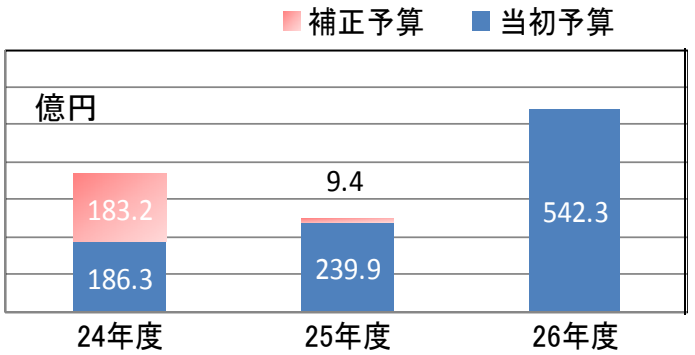
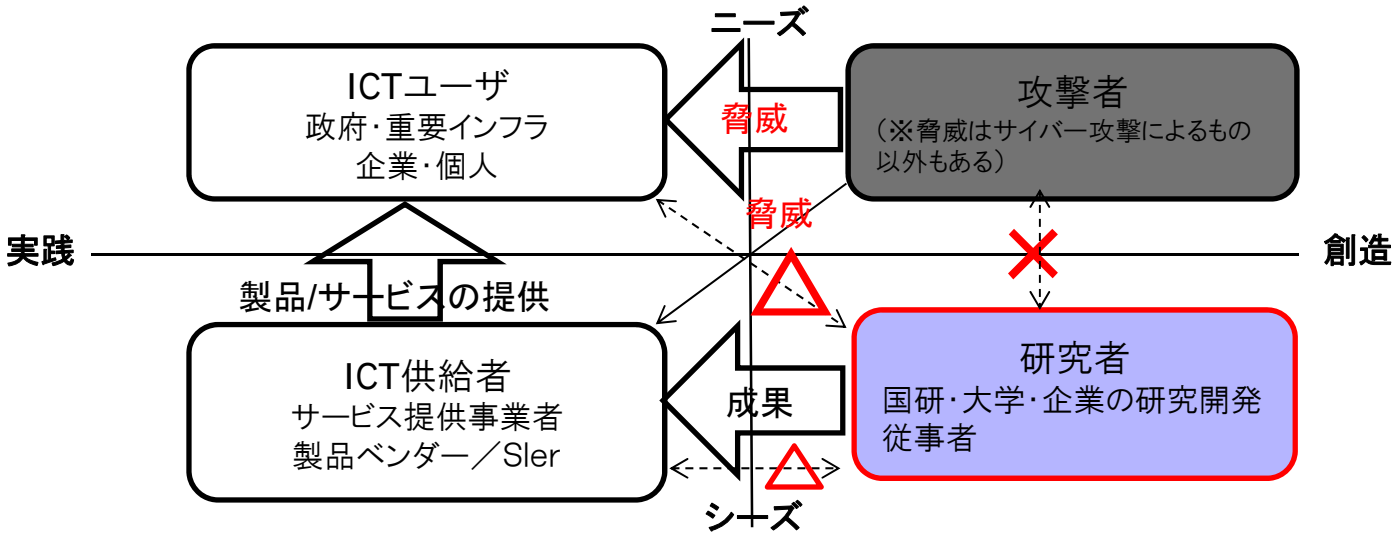


図 3：日本政府の情報セキュリティに係る予算の推移

2. 研究開発の見直しにあたっての課題

- 研究・技術開発に当たっては、現実にどのような脅威があり、具体的なニーズが何であるかということを適時適切に把握して取り組むための環境等の整備が必要。
- 研究・技術開発に必要な情報等が十分に循環しない状況であること、さらに、攻撃者の情報を研究開発者において把握することが難しいことなどの、研究開発をより実践的なものとしていくための課題を解決する必要がある。
- システムのOSなど重要な製品が海外製品となり、国内技術の空洞化が進展すると、根本的な対策を措置できないことから、重要な製品等については、我が国として必要な技術力を獲得・保持するとともに、サイバーセキュリティがグローバルな問題であることを踏まえると、グローバルに通用するもの、産業競争力につながることが必要。



3. 今後の情報セキュリティ研究開発推進方針①

従来よりも実践的で有効に成果が用いられるような研究開発の推進方針の検討にあたっては、現在の情報セキュリティ関連の研究開発者の輪やリソースに限りがある状況や、情報セキュリティの課題は単に技術に限った問題ではないこと、グローバル化していること等を踏まえることが必要。

（1）サイバー攻撃の検知・防御能力の向上

- 情報セキュリティの研究分野としては、情報保証(Information Assurance)やコンピュータ・ネットワーク防御（Computer Network Defense）、情報セキュリティマネジメント、暗号等の基礎分野など様々な専門領域があるが、研究開発等を進めるには、情報共有や問題意識の共有など、できる限り一体となって取り組むことが求められる。
- また、サイバーセキュリティを含む情報セキュリティ上の脅威は、組織の運営・事業継続に重大な影響を及ぼすものであることから、情報や情報システムなどに係る研究と組織の経営等に係る研究は、連携して行われることが求められる。
- さらに、サイバー空間と実空間が融合していることから、サイバーセキュリティの問題を考えるにあたっては、単に情報システム等の脅威を考えたり、技術的な研究のみならず、国際政治、安全保障、危機管理、経済、心理などさまざまな領域の研究とも連携して行われることが求められる。
- このため、以下のような施策を推進していく。
  ① 現実の脅威や新たな攻撃への対処や、攻撃者の把握などのため政府全体としての情報の一元化と、研究者等に対する情報共有の枠組みの構築の推進。
  ② 情報セキュリティ技術と社会科学、経営学など他分野との融合。コミュニティ作り等を促進。

3. 今後の情報セキュリティ研究開発推進方針②

（2）社会システム等を防護するためのセキュリティ技術の強化

- あらゆる分野で情報通信技術が利用される中で、社会システム等を構成する要素に関するセキュリティ対策や研究開発が必要。
- 社会インフラを構成するシステムは多種多様で、対象が広範囲であることから、現場の具体的なニーズを十分把握した上で、国として特に重要な分野を特定し、重点的に進めていくことが必要。
- 制御システムやICチップなど、社会インフラ等を構成する要素に関するセキュリティ技術開発の促進や評価・認定制度の国際的な相互承認制度の確立も図る。
- ID連携や認証技術を活用した社会システムの戦略的推進や、社会システム設計、国際標準化を踏まえた情報セキュリティ対策、研究開発を実施。

（3）産業活性化につながる新サービス等におけるセキュリティ研究開発

- 今後発展が期待される新たなICT分野（健康・医療、社会インフラ等）にて上流工程からセキュリティ品質を組み込み、競争力等の観点も含めて、国内で保有するべき高度なセキュリティ技術の研究開発を促進。
  上流工程からセキュリティ品質を組み込むことで、効率的な対策が可能。
- それらの製品が使われることにより、メンテナンス等の新たなサービス分野の需要も発生するため、日本ブランド品質のひとつとしてセキュリティを位置づけ、日本発のグローバルICT製品・サービスの実現を目指す

3. 今後の情報セキュリティ研究開発推進方針③

（4）情報セキュリティのコア技術の保持

- 変化の激しい情勢に対応し、日々高度化・巧妙化するサイバー攻撃等にプロアクティブに対応していくためには、攻撃や防御のための技術の原理、システム等の仕組みなどを自ら考え、開発していくことが必要。
- 例えば、暗号は、独立国家として、国の機密情報の保護をはじめ、商用においても認証など様々な分野で基盤として用いられており、危殆化する前により強固な暗号へ移行することが不可欠なものであり、引き続き、暗号技術の動向を監視し、評価し、必要な開発能力を維持することが必要。

（5）国際連携による研究開発の強化等

- サイバー攻撃等に的確に対応できる高度な対策技術の開発に向け、各国が「強み」を有する技術を有機的に組み合わせ、発展させることが有効であり、国際連携による研究開発を積極的に推進。
- サイバー空間のセキュリティを確保するためのシステムなどは広く国際的に取引されるようになってきているが、その相互運用性や求められるセキュリティ水準を確保するための技術的な標準の重要性が増している。このため、様々な国際標準化の取組が行われている中で、サイバーセキュリティ技術に関する国際標準の策定・普及や相互承認枠組作りを進めていくことが重要。
- なお、国際連携のパートナーを選定するにあたっては、我が国やサイバー空間を脅かすおそれがない者であることが必要である。

4. 研究開発の進め方

（1）社会還元を促進するための取り組み

- 情報セキュリティを巡る脅威やニーズといった研究・技術開発に必要な情報等が十分に循環しない状況を改善し、攻撃情報やニーズの集約化を行うことにより、社会的なニーズに対応した研究開発の促進を行っていく。
- その際、海外での取組も参考に研究開発成果を社会還元する取組を実施。

  例）欧州・英・韓等では、実学であるサイバーセキュリティ研究開発についても、
  研究成果の社会還元を促進するため技術移転部門を活用している。
  我が国の研究機関においても契約面や広報面の充実をはかりつつ、
  リエゾンオフィスを通じ、ニーズシーズのマッチングや、研究成果の社会還元を促進すべきである。

（2）より効果的な研究開発の実施

- 情報セキュリティは国境を越えるボーダレスな問題であることから、その技術力はグローバルに通用するものである必要がある。
- 情報セキュリティを巡るグローバルな競争を勝ち抜くために、研究開発投資の充実やより効果的な研究開発の実施、基礎力となるコア技術の保持などを実施。
- 情報セキュリティの研究開発と情報通信技術等、他の研究とが連携して推進できるよう、我が国におけるプロジェクトの予算、体制、進捗状況を把握しつつ、総合科学技術会議や関係省庁との連携を実施。

5. 重要分野の見直し方針①

(1)産官学の役割の考え方

①産(民間)→ビジネスレベル(製品開発やサービスのレベル)につながる分野での研究開発
②官(政府、国研)→国家や国民にとってリスクの高い課題等、国として重要な課題についての研究開発
(民間でできるものは民間に任せる)
③学(大学)→研究開発人材育成。学問として重要な課題についての研究開発

(2)政府等の研究機関における情報セキュリティ研究開発の重要分野の考え方(見直し方針)

①リスク(最近の脅威や今後の動向)に応じた研究開発の実施
②社会インフラ、ハードウェアセキュリティ(制御システム等)への対応
③発展が期待される分野での上流工程からのセキュリティ品質の確保
④情報セキュリティのコア技術(暗号化等)の保持

①情報セキュリティ上の脅威の例

情報セキュリティ上の脅威の例	
①	サイバー攻撃による情報の搾取や破壊、サービス妨害
②	IDパスワードの盗用やなりすまし
③	スマートフォンやパソコン等での悪意あるアプリの増大
④	ソフトウェア脆弱性を狙った攻撃
⑤	社会システムを構成する、制御システムを狙った攻撃
⑥	個人情報やプライバシー情報、機密情報の漏えい
⑦	情報通信システムでの情報の盗聴・傍受

5. 重要分野の見直し方針②

②社会インフラ、ハードウェアセキュリティ（制御システム等）への対応

社会インフラ、ハードウェアセキュリティ（制御システム等）への対応	
①	制御システムセキュリティ
②	セキュリティデバイス

③今後発展が期待される分野

今後発展が期待される分野	
①	医療健康分野（在宅医療の促進や、病院間でのカルテ情報交換）
②	次世代インフラ（防災・減災分野でのセンサー情報等）
③	ビッグデータの利活用
④	家電等のネットワーク接続
⑤	自動車のネットワーク接続（ITS分野）
⑥	東京オリンピック

④情報セキュリティのコア技術

情報セキュリティのコア技術	
①	サイバー攻撃の検知／防御技術
②	認証技術（バイオメトリクスを含む）
③	情報通信ネットワーク
④	暗号技術
⑤	制御システムのセキュリティ技術
⑥	標準化／評価技術

参考資料　重要分野の見直し案（変更の比較表）

（現在の研究開発戦略の重点分野）
情報セキュリティの研究開発における重要分野

情報通信システム全体のニュー・ディペンダビリティの確保	
①	実世界とコンピュータ内のモデル世界が融合した次世代ネットワークにおける情報セキュリティ基盤技術
②	システムのセキュリティ設定を上位から下位まで自動保証する技術
③	障害に対する自動回復可能なコンピュータネットワーク構築技術
④	生体情報をコンピュータで管理するためのID管理と生体情報を統合するシステム設計構築技術
攻撃者の行動分析に基づくゼロデイ・ディフェンス	
⑤	攻撃者の行動分析等による予防基盤技術
⑥	大規模ネットワークにおける広域観測技術とマルウェアの挙動分析技術の統合
個人情報等の柔軟管理の実現	
⑦	個人情報等の利活用を促進する自己情報の統制技術
⑧	フォレンジック等を支援するためのデータ管理・追跡技術
⑨	ITリスクに関する理論から実務までの体系化
研究開発の促進基盤の確立とセキュリティ理論の体系化	
⑩	情報セキュリティ研究の基盤体系化
⑪	セキュリティ部品が正しく実装されていることを保証する製品評価認証技術
⑫	情報理論的安全性を備えた暗号技術

セキュリティ研究開発の
重要分野（変更の方針案）

情報通信システム全体のセキュリティの向上	
①	サイバー攻撃の検知／防御
②	ID連携／認証／アクセス制御 （追加）
③	スマートフォン／クラウドのセキュリティ
④	次世代ネットワークセキュリティ
ハード・ソフトウェアセキュリティの向上	
⑤	制御システムセキュリティ （追加）
⑥	セキュリティデバイス （追加）
⑦	ソフトウェアの安全性確保 （範囲の拡大）
個人情報等の柔軟管理の実現	
⑧	プライバシー保護／パーソナルデータ利活用
⑨	フォレンジック支援技術（データ管理・追跡技術）
研究開発の促進基盤の確立とセキュリティ理論の体系化	
⑩	セキュリティ理論体系化／調査研究
⑪	標準化／評価／制度／基盤整備
⑫	暗号技術

＋

発展が期待される応用分野でのセキュリティ研究開発（※例）	
①	医療健康分野での情報流通変革に伴い必要となるセキュリティ技術の開発
②	次世代インフラで必要となるセキュリティ技術の開発
③	ビッグデータにおける情報の秘匿化、暗号化などのセキュリティ技術の開発
④	家電、自動車、東京オリンピックで必要となるセキュリティ技術の開発
	：

＜凡例＞

→ 変更前後で実質的な内容がほぼ同一なもの。

⇢ 分野のカバー範囲、まとめ方に変動があるもの。