

平成 23 年度情報セキュリティ産業の活性化方策に係る調査  
調査の概要

2012 年 3 月  
株式会社三菱総合研究所

## 1. 研究開発戦略に係る国際動向

研究開発戦略の国際動向に関する調査においては、2011年12月に公表された米国のサイバーセキュリティの研究開発戦略「Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity R&D Program」に関する取組みを調査した。

2009年に就任したオバマ大統領は、サイバーセキュリティを政権の優先課題と位置づけ、ブッシュ政権時代の連邦政府の情報通信インフラ防衛の取組みに対するトップダウンの見直しを指示し、その結果を2009年5月「Cyberspace Policy Review」として公表した。同文書ではサイバーセキュリティ政策を推進するためのアクションプランが示されているが、この中の1項目としてサイバーセキュリティの研究開発戦略の策定が指示されている。

米国の研究開発戦略策定に当たっては、まず「Cyberspace Policy Review」で示された game-changing な技術に焦点を置いた研究テーマの検討が行われた。戦略の策定作業は連邦政府の情報通信分野の研究開発を省庁横断的に取りまとめるネットワーク情報技術研究開発プログラム（NITRD）のサイバーセキュリティと情報保証分野（CSIA）を中心に行われた。NITRD CSIA では研究テーマの抽出に当たり、全米の産官学の各機関に対して game-changing な技術のアイデアを募集し、寄せられたレスポンスを基に2009年8月に OSTP と共催で「National Cyber Leap Year Summit」を開催し、研究テーマの初案について150名の参加者による議論を行っている。その後 NITRD CSIA に参加する連邦政府機関のプログラムマネージャを中心とした省庁横断作業部会を中心に研究テーマの具体化作業が行われ、2010年5月には戦略の骨子となる「Cybersecurity Game-Change Research & Development Recommendations」を公表している。ここでは研究テーマとして①Moving Target、②Tailored Trustworthy Spaces、③Cyber Economic Incentives が挙げられている。なお、2011年には新たな研究テーマとして Designed-in Security が加えられた。その後、作業部会を中心に戦略全体の取りまとめ作業を行い、2011年12月に White House の国家科学技術会議（NSTC）から全体が公開された。

戦略は戦略の推進力（Strategic Thrust）と題された以下の4つの内容で構成されている。

1.変化の誘発	4つの研究テーマ（①Designed in Security、②Moving Target、③Tailored Trustworthy Spaces、④Cyber Economic Incentives）を示している。テーマはいずれも脅威の根本原因を打破することを目的とした、これまでのセキュリティ対策とは根本的に異なるアプローチとなっている。
2.科学的な基盤の確立	サイバーセキュリティに科学的なアプローチで取り組むための基盤として、セキュリティサイエンス（Science of Security）の考えを示している。これは4つのテーマに横断的に関わる考え方として位置づけられている。
3.研究のインパクトの最大化	戦略に基づいて実施される研究の効果を最大化するため、他分野の研究テーマとの連携や官民の研究コミュニティの活動を推進するための取組みが示されている。
4.実用移行の加速	各種実用化プログラムの活用等、研究開発で得られた成果の実用化の推進方針を示している。

2012年2月にNITRDが公表した2013年度の大統領予算教書の補足資料によれば、NITRD CSIAに参加する各連邦政府機関のサイバーセキュリティに関する2013年度の研究プログラムは、上記の戦略の項目に沿った形で計画されている。なお、NITRD CSIA全体の予算規模も拡充され、2012年度予算5.9億ドル（推定）に対し、2013年度は約6.67億ドルが要求されている。

最後に米国のサイバーセキュリティの研究開発戦略への取組みから、日本の「情報セキュリティ研究開発戦略」の拡充及び将来の新たな戦略策定時の参考となる視点として以下の3点を抽出した。

- 研究開発戦略策定の策定プロセス  
産学官のステークホルダーに対して広く開かれた議論の場を提供し、時間をかけて研究テーマを検討する仕組み  
戦略の策定・拡充・推進過程に研究を実施する省庁の担当者が参加し、各省庁の方針を共有しながら検討を進める体制
- 研究テーマの見直し  
脅威やシステム環境の変化、最新の技術に対応した柔軟な研究テーマの見直し体制
- 他分野における研究開発戦略の活用  
情報セキュリティ以外の分野の研究開発においても、情報セキュリティに係るテーマについては本戦略が活用されるような推進策

## 2. 情報セキュリティ技術の科学的な評価フレームワークの調査及び評価フレームワークの構築

現在の情報セキュリティ技術は、情報システムに関わる環境において生じる攻撃などの脅威に対する対処療法的なノウハウの集合となっており、科学としての体系化や評価尺度が十分に整備されていない。「情報セキュリティ研究開発戦略」を推進するための評価フレームワークを策定するに当たり、情報セキュリティ技術を科学的に評価する手法の米国における動向を調査し、それらの結果も踏まえて「情報セキュリティ研究開発戦略」の評価フレームワークを策定した。

情報セキュリティ技術を科学的に評価する手法については、主に以下のような知見が得られた。

- セキュリティサイエンスの動向  
米国におけるサイバーセキュリティ研究では、科学的なアプローチを導入することにより効果的かつ合理的に研究開発を推進すべきとの問題意識が高まっている。これまでに繰り返しワークショップが開催され、現在議論の途上にあるが、サイバーセキュリティの共通言語の構築、メトリクスの確立、再現可能な実験基盤の確立などの課題が掲げられている。
- 情報セキュリティに関する評価法の動向

情報セキュリティ研究開発を科学的なアプローチで取組むために、リスクやセキュリティ対策の導入効果等に関する評価手法が重要となる。対象に応じたリスクや対策レベルの評価手法や投資効果の評価手法が提案されている。これらの手法は、対象や目的に応じてカスタマイズを行い適用することが必要となると考えられる。

以上のような動向調査も踏まえて、「情報セキュリティ研究開発戦略」の重要分野を具体化した要素課題と達成時期の検討を行った。要素課題と達成時期の全体像は、研究開発ロードマップとしてまとめられ、以下に示す通りである。研究開発ロードマップを含む評価フレームワークは、戦略を今後推進する際に活用されることが想定されるものである。

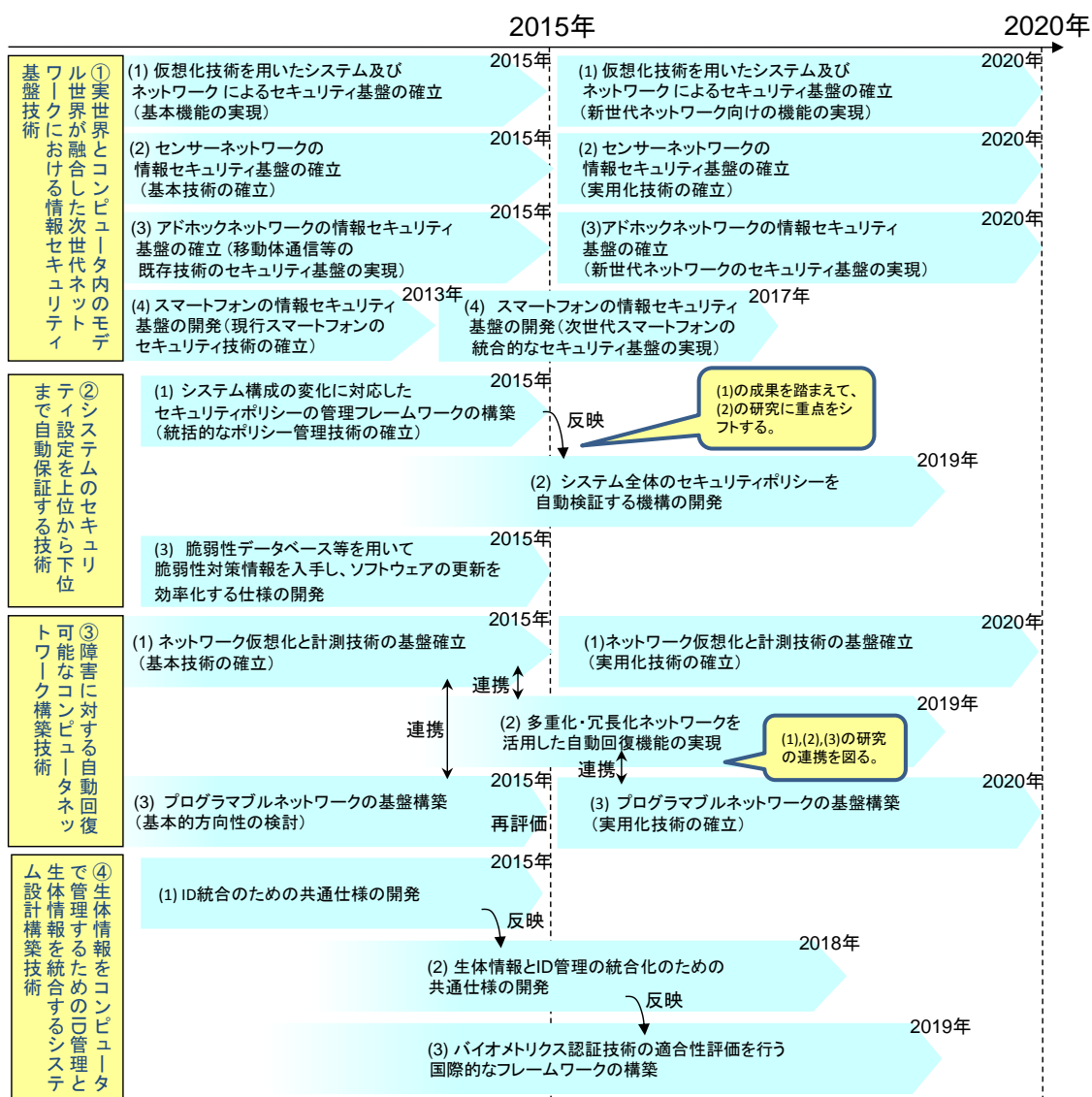


図1 研究開発ロードマップ (1/3)

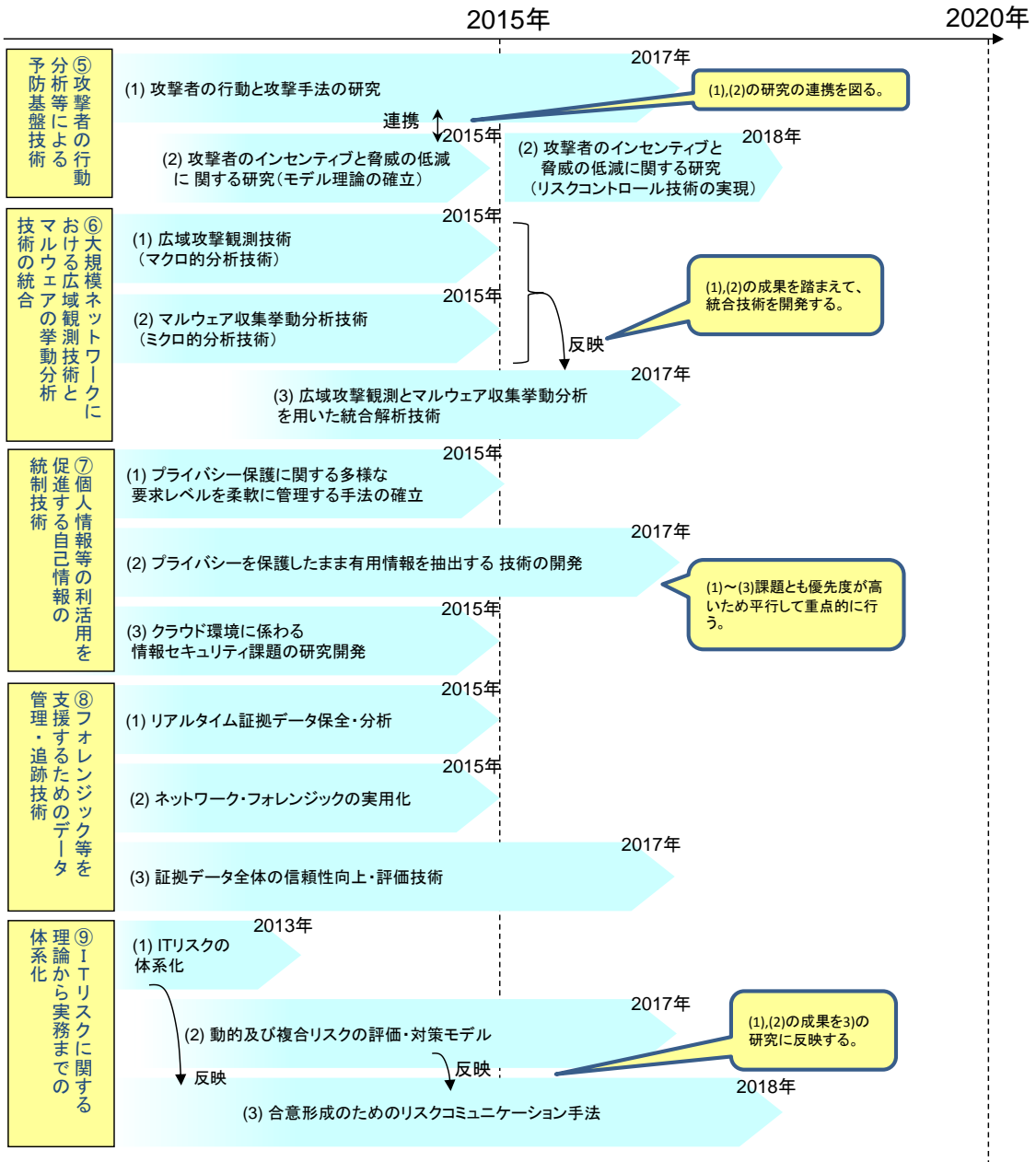


図 2 研究開発ロードマップ (2/3)

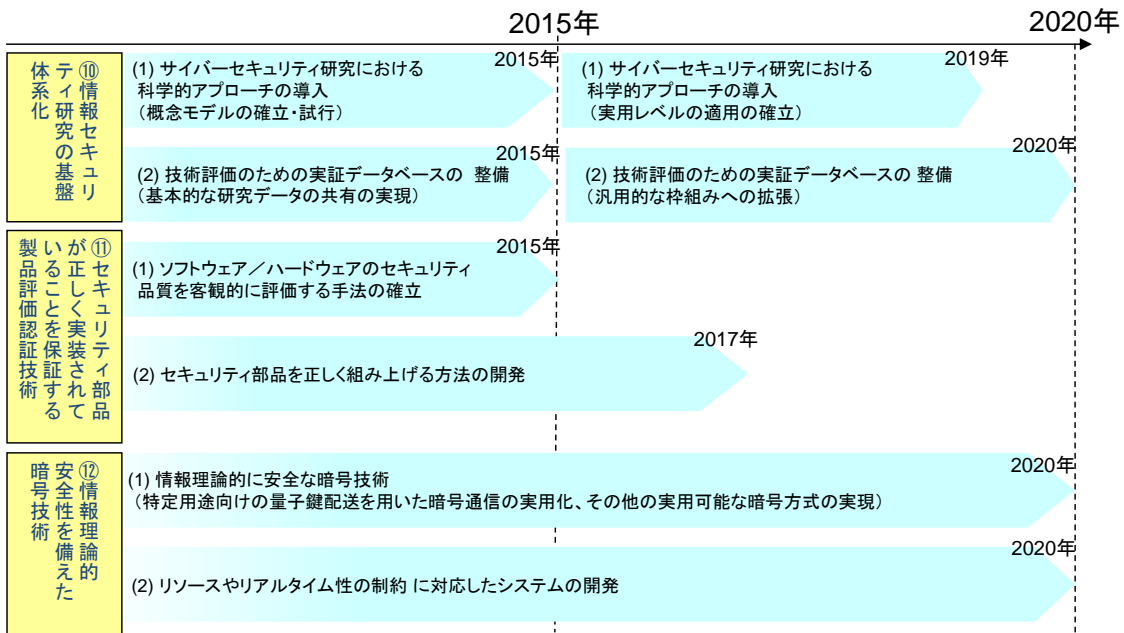


図3 研究開発ロードマップ (3/3)

### 3. 情報セキュリティ研究成果の実用化に係る方法論の調査及び提言

研究成果の実用化に係る動向調査では、米国土安全保障省のサイバーセキュリティ研究開発センターにおける取組みとして、研究ライフサイクル全体を俯瞰しバランスよく研究予算の配分を行う制度や、DODの技術達成度レベル評価に基づく防衛調達システムなどの参考となる取組みを示した。このような調査結果も踏まえ、研究成果の実用化について以下のような提言をまとめた。

- 社会ニーズを反映した研究競争環境の醸成  
 情報セキュリティ分野においては、常に変化する脅威に対応するための課題解決型の研究が求められる。そのためには、戦略に基づく研究の方向性を明確にしつつ、その戦略に沿って、研究競争環境を醸成するための予算配分を行うことが重要である。
- 産学官の知見及びノウハウの共有と活用の仕組み  
 情報セキュリティ分野は、他の ICT 技術と組み合わせることで意味をもつ研究が多いため、産学官の人材流動性を高めることによりオープン・イノベーションを促進するための施策を実施することが重要である。
- 研究ライフサイクル全体を考慮した予算配分の仕組み  
 基礎研究から実用化にいたる研究ライフサイクル全体を俯瞰し、バランスよく研究の投資配分を行うとともに、国家安全保障に係る技術を戦略的に保持するしていくことを考慮し、政府調達と関係づけて研究開発予算を検討することが重要である。