資料４

NISC National Information Security Center

情報セキュリティ研究開発戦略の見直しについて

平成26年1月

内閣官房情報セキュリティセンター

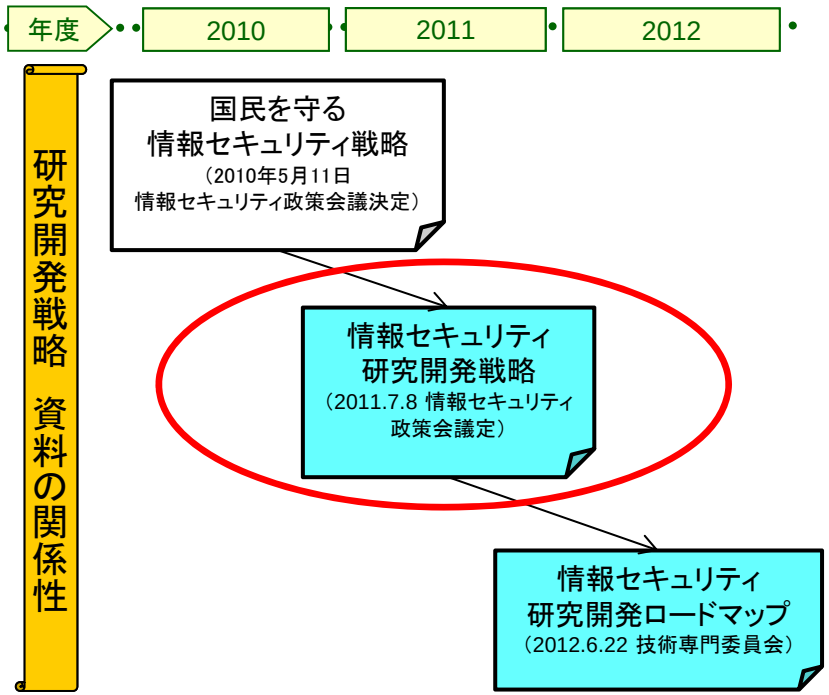
NISC National Information Security Center

1．情報セキュリティ研究開発戦略

1.1　情報セキュリティ研究開発戦略について

1.2　研究開発戦略の見直しの経緯

1．1　情報セキュリティ研究開発戦略について



①「情報セキュリティ研究開発戦略」とは

・情報セキュリティに係る研究開発を戦略的に推進するために2011年に策定したもの。（東日本大震災直後）
・情報セキュリティ研究開発での重要分野や予算必要性を示している。
・2011年～2015年の5か年スコープの計画である。
　また、～2020年までの研究開発の道筋を示している。
・参考URL:
　http://www.nisc.go.jp/active/kihon/pdf/kenkyu2011.pdf

②「研究開発戦略」のドキュメントの位置づけ

・第4期　科学技術基本計画に謳われている「能動的で信頼性の高い（ディペンダブルな）情報セキュリティに関する研究開発を推進」する際の具体的な中期的戦略文書として位置付ける。

③「情報セキュリティ研究開発ロードマップ」とは

・研究開発戦略での12の重要分野をさらに細分化し、33分野の研究開発を示したもの。
・実施項目・実施スケジュールなどを示している。

1．2　研究開発戦略の見直しの経緯

情報セキュリティを取り巻く環境の変化

(1)情報セキュリティリスクの深刻化

甚大化するリスク　情報窃取のための標的型攻撃、重要インフラ機能障害を引き起こす攻撃等、**サイバー攻撃が複雑・巧妙化**。

拡散するリスク　あらゆるものがインターネットに接続されることにより、**制御システム等もサイバー攻撃の対象に**。

グローバルリスク　世界各国の情報通信技術利用拡大に伴い、国境のないサイバー空間では、**リスクもボーダレスに拡大**。

「サイバーセキュリティ戦略」の策定

（研究開発の記述より抜粋・要約）

サイバー空間を取り巻くリスクの急激な変化に適切に対応できる創意工夫に満ちた情報セキュリティ技術

⇒　**我が国のサイバー防御能力**の向上、経済成長につながる**新産業創出**、**国際競争力**の向上

① サイバー攻撃の検知・防御能力の向上

② 制御システム、ICチップなど社会システム等を保護するためのセキュリティ技術の確立

③ ビッグデータ（パーソナルデータ等）利活用等の新サービスのための技術開発

環境の変化・サイバーセキュリティ戦略を踏まえ、より実践的な内容となるよう

「情報セキュリティ研究開発戦略」の見直しが必要

NISC National Information Security Center

２．情報セキュリティ研究開発戦略の課題と施策

２.１　最新の脅威に対応した研究開発の推進（大課題）

２.２　サイバー攻撃の検知･防御能力の向上

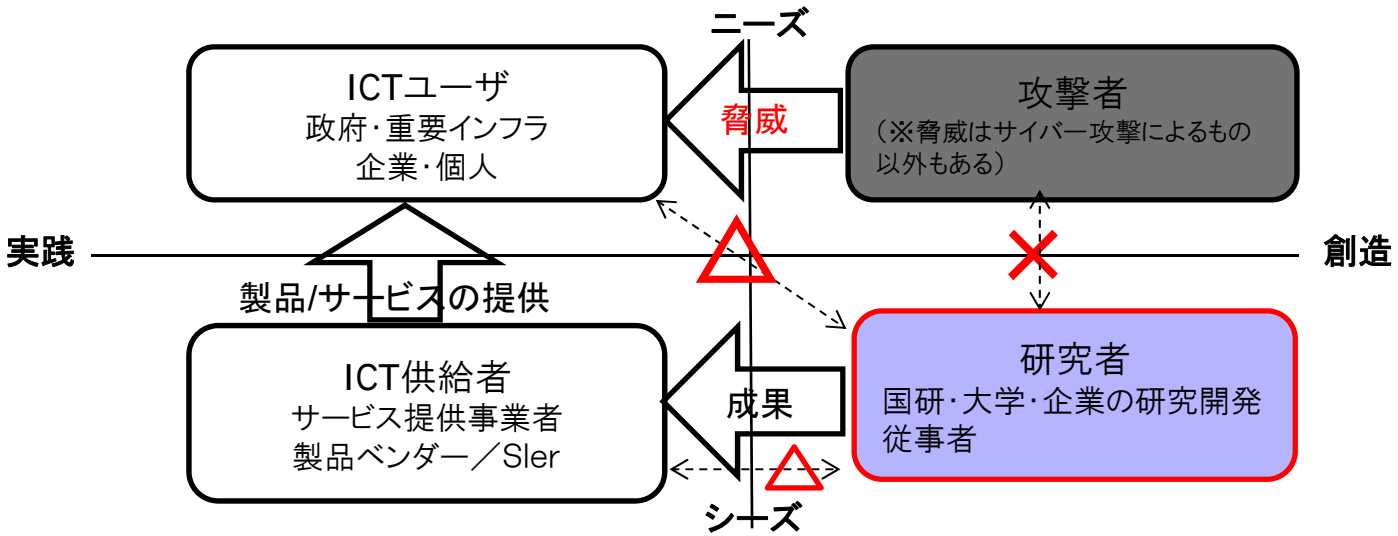
２.３　我が国の社会システム等を防護するための
セキュリティ技術の強化

２.４　産業活性化につながる新サービス等における
サイバーセキュリティの研究開発

２.５　重要分野の見直し

2．1　最新の脅威に対応した研究開発の推進（大課題）

【大課題】
セキュリティは実用性が重要。
サイバー攻撃が高度化・複雑化している中で、研究者による自由な研究などに加え、
最新の脅威や今後の動向を見据えたうえで、
より実践的・実用的な研究開発を推進することが重要ではないか。
そのためには関係者間で問題意識や情報流通につきより緊密な連携が求められるのではないか。（仮説）



2．2　課題と施策（1）　サイバー攻撃の検知・防御能力の向上

【小課題（1）】
①現実の脅威や新たな攻撃などに対処する能力を高めるための研究開発の進め方はどうあるべきか。
②成果が実用化される研究開発を進めるにはどうすべきか。

【考えられる施策例（1）】
①研究開発に資するべく、現実の脅威に関するサイバー攻撃情報の流通や新たな攻撃の調査分析などを国内外の関係者が連携しつつ行うことはどうか。
例1）政府が保有するサイバー攻撃情報を、有効性を維持ししつつ開示可能な形に整え、研究者等へ提供
例2）国際連携・国内関係機関間の連携などにより、仮想空間での新たな攻撃方法の調査分析検知方法の研究
例3）不正プログラム分析や脆弱性研究の着実な実施の観点からセキュリティ確保目的のフェアユースなリバースエンジニアリングの適法性の明確化

②ICTユーザの経営層などがサイバーセキュリティに関する脅威を認識するための施策を推進することが実用的な研究開発投資につながるのではないか。
例1）サイバーセキュリティを巡る国際情勢、政策、法律、事業戦略などの分析研究の促進
例2）経営層が事業戦略にITを位置づけて、その基盤としてのセキュリティ対策の意義（事業戦略への影響の認識）を理解させるための施策を促進
例3）事業戦略等とサイバーセキュリティの関係などに関する問題意識・情報も関係者間で共有することを促進（IT・セキュリティ関連の研究部門と経営学の研究部門との連携など）

２．３　課題と施策（２）　我が国の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

【小課題（２）】
①社会インフラ等のセキュリティ向上のための研究開発はどうあるべきか
②情報セキュリティ技術は、安全保障、機微な情報の保護等の観点からも重要な技術であるところ、どのようにコア技術を保持していくか。

【考えられる施策例（２）】
①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制度の充実を進めていくことはどうか。
例１）ICチップのセキュリティ技術開発の促進
例２）ハードウェアセキュリティ（制御システム等）の評価技術の研究開発促進

②我が国の安全保障、危機管理、産業競争力強化、国際競争力等の観点も含めて、国内で保有するべき高度なサイバーセキュリティ技術（システム、ネットワーク等）の研究開発を促進すべきではないか。
例１）高度なサイバーセキュリティ技術を確保するためのICT基盤技術開発の一層の関係者間連携促進
例２）国として保持すべき暗号等の基礎研究能力の維持・強化

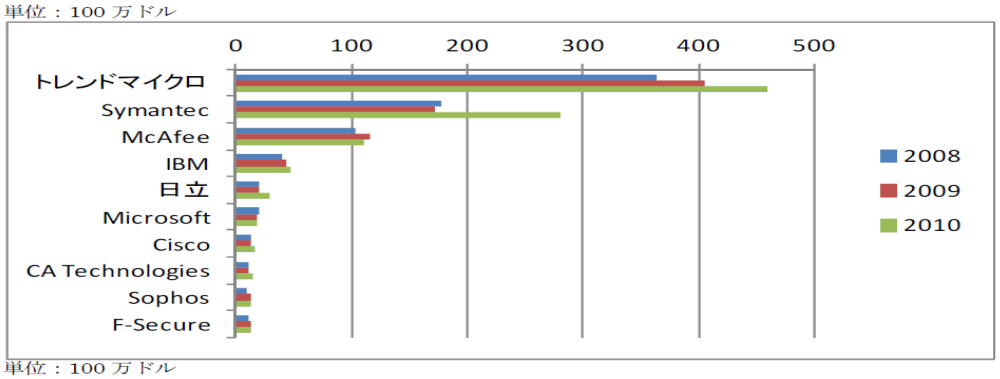


図１　日本における情報セキュリティ（ツール）のベンダーシェア
（経済産業省「平成23 年度企業・個人の情報セキュリティ対策促進事業」調査報告書（2012年3月））

２．４　課題と施策（３）　産業活性化につながる新サービス等におけるサイバーセキュリティ研究開発

【小課題（3）】
産業活性化につながる研究開発とするには、将来のICT産業の発展の方向を見据えて
サイバーセキュリティ技術の研究開発を促進すべきではないか。

【考えられる施策例（3）】
今後発展が期待される新たなビジネスにおいてサイバーセキュリティの程度を特に高めてセキュリティ品質を売りとするような取組を推進するのはどうか。
例１）オープンイノベーション（業態を超えた横連携）による研究開発の促進－発展が想定されるICT分野で上流工程からセキュリティ設計を組み込むため、関係機関等が自組織を超えた連携を積極的に促進
例２）認証技術に依拠する社会システムの戦略的推進
例３）研究開発成果の活用によるベンチャー支援（研究開発成果に基づく製品の調達など）

コア技術

情報通信システム全体のセキュリティ向上
・サイバー攻撃の検知／防御
・認証／アクセス制御（追加）
・スマートフォン／クラウドのセキュリティ
・次世代ネットワークセキュリティ

個人情報等の柔軟管理
・プライバシーの保護／
　パーソナルデータ利活用技術
・フォレンジック支援（データ管理・追跡）

ハード・ソフトウェアセキュリティ
・制御システムセキュリティ（追加）
・セキュリティデバイス（追加）
・ソフトウェアの安全性確保

基礎・理論
・セキュリティ理論体系化／調査研究
・標準化／評価／制度／環境整備
・暗号技術

適用　フィードバック

セキュリティ品質を上流工程からどう組み込むか。

発展が期待される応用分野（※例）

医療・健康
・在宅医療や介護医療などで、情報流通の変革によりセキュリテニーズが増加

次世代インフラ
・次世代インフラの安全・安心を確保するためのセキュリティ技術

ビックデータ
・ビッグデータ（パーソナルデータ等）利活用等の新サービスのためのセキュリティ対策技術（匿名化・暗号化）

・・・

2．5　課題と施策（4）　重要分野の見直し①（現在のリスト）

現在の研究開発の
重要分野の選定背景

東日本大震災を踏まえた
情報通信システムの
信頼性、セキュリティ
の向上　等

サイバー攻撃・マルウェア
セロデイ攻撃への対応

個人情報等の利活用
・暗号技術　等

（現在の研究開発戦略の重要分野）
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		進捗状況
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	総務省や経済産業省配下で研究を進めている
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	ネットワークで類似した研究をしているが、目立った研究は見当たらず
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	ネットワークや耐災害性部門の領域で研究が進められている
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	産総研等にて生体情報に関する研究開発を実施している
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	総務省配下で研究を進めている
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	総務省配下で研究を進めている
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	現状は大学等での研究推進を想定
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	現状は民間等での研究推進を想定
⑨	ITリスクに関する理論から実務までの体系化	現状は大学等での研究推進を想定
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	国研でテストベッドなどを整備 現状は大学等での研究推進を想定
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	経済産業省配下で、制御システム等の認証評価の取組を推進
⑫	情報理論的安全性を備えた暗号技術	総務省や経済産業省配下で研究を進めている

環境の変化、2.2~2.4の議論などに連動して
重要分野の見直しが必要

2．5　課題と施策（4）　重要分野の見直し②（変更の方針案）

＜見直しの考え方＞
①リスク（最近の脅威）に応じた研究開発への見直し
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からのセキュリティ品質の確保

【甚大化するリスク】
社会インフラを支える
制御システムを狙った
サイバー攻撃の発生

【拡散するリスク】
スマートフォン等の普及、
あらゆるものの
インターネット接続の進行と
セキュリティリスクの顕在化

【グローバルリスク】
海外等からの不正アクセス

発展が期待される分野での
セキュリティ研究開発

「日本再興戦略」等
から抜粋

**セキュリティ研究開発の
重点分野（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	アクセス制御／認証 （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）
基礎・理論	
⑩	セキュリティ理論体系化
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
	：

NISC National Information Security Center

３．ご議論頂きたいポイント

3.　ご議論頂きたいポイント

セキュリティの研究開発における課題と施策について、ご意見やご提案を頂きたい。

（1）課題や施策案についての賛否や過不足について、ご意見・ご提案頂きたい。
　例）　課題の認識について妥当か。重要な課題が漏れていないか。
　　施策案、施策例について、効果的なものとなっているか。実現は現実的か。

（2）施策について、よい具体策があればご意見・ご提案頂きたい。

（3）研究開発の重要分野の見直し方針案についての賛否や過不足など

（4）その他

NISC National Information Security Center

４．ご参考資料

4. ご参考資料 重要分野の見直し(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	アクセス制御/認証 (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)
基礎・理論	
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
⑤	農業のIT化に伴う情報セキュリティ技術
	:

＜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。