資料３－２

NISC National Information Security Center

情報セキュリティ研究開発戦略の取組状況について

2011年　12月　1日

内閣官房情報セキュリティセンター（NISC）
http://www.nisc.go.jp/

情報セキュリティ研究開発戦略の取組状況

- 「情報セキュリティ研究開発戦略(平成23年7月8日情報セキュリティ政策会議)」にある重点分野に関して、各省が予算化して取り組んでいるものをNISCで調査。

- それぞれの重点分野について、取り組まれている施策が、完全に対応できているわけではない。
- 5ヶ年計画である情報セキュリティ研究開発戦略を推進するためには、ロードマップの詳細化とともに、具体的施策への展開が必要である。

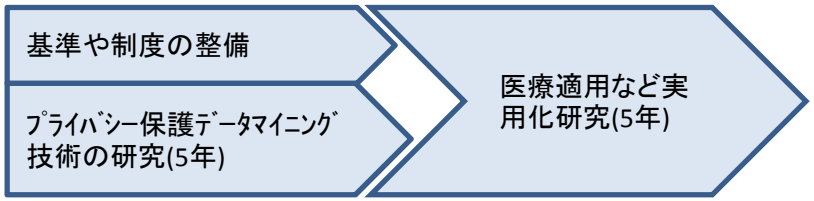
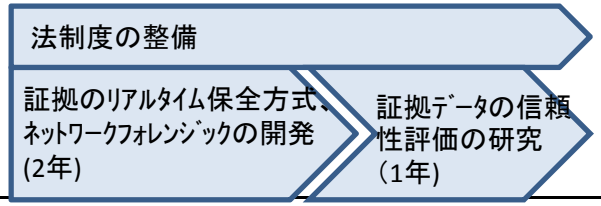
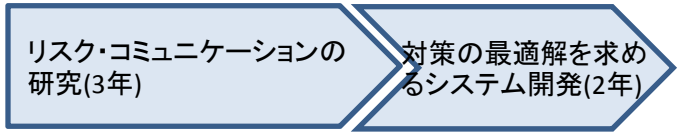
情報通信システム全体のニュー・ディペンダビリティの確保

No.	重要テーマ	概要・ロードマップ（イメージ）	取組施策の例
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	コンテキストアウェアネス（センサーを用いて実世界の状況をコンピュータ内に能動的に収集、処理する）を実現するうえで、利便性と安全性のバランスを考慮した情報セキュリティ基盤の確立が必要。 利便性と安全性のバランスを考慮した情報セキュリティ基盤技術の開発（5年）	「IT活用による生活安全技術を目指し、暗号などのセキュリティ基盤技術やネットでの認証技術の研究等を行う。（産総研）」 「実用化を目指した組込みシステム用ディペンダブル・オペレーティングシステム（JST）」
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	米国のセキュリティ・オートメーションの研究動向も踏まえ、ポリシーに基づいてレイヤ間の整合性を自動検証する形式手法の基礎研究も必要。 コンフィグレーション及びポリシーの記述方法の研究(5年) → 自動検証する形式手法等の研究(5年)	「適材適所にセキュリティ技術を自動選択し、セキュアなネットワークを最適に構成するためのセキュリティアーキテクチャの研究開発（NICT）」 「情報基盤における安全性や信頼性の確立を目指し、形式手法を利用した基幹ソフトウェアのセキュリティ評価技術等の研究開発を行う。（産総研）」
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・アーキテクチャの構築技術	自己治癒型のネットワークの研究開発の前提として、ネットワークの仮想化・多様化に係わる基礎研究も必要。 ネットワークの仮想化・多様化技術の研究(5年) → 基盤技術を用いた自己治癒型ネットワークの研究(5年)	「新世代ネットワークのセキュリティアーキテクチャの実現（NICT）」
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技術	生体情報を用いたIDマネージメントを国際的に行うためには、国際標準化のプロセスに沿った取り組みも必要。 統合技術の開発、ISOの提案取纏め(1年) → ISO標準化プロセス、実証実験(2年)	「ITによる生活安全技術：安全な社会生活の実現をIT技術で支援するため、消費者情報保護のための情報セキュリティ技術の開発を行う。（産総研）」

攻撃者の行動分析に基づくゼロデイ・ディフェンス

No.	重要テーマ	概要・ロードマップ（イメージ）	取組施策の例
⑤	攻撃者の行動分析等による予防基盤技術	(a)攻撃者のプロファイリングは、セキュリティ研究の全般に有益な情報となるため、研究成果を活用する基盤構築が必要。 攻撃者のﾌﾟﾛﾌｧｲﾘﾝｸﾞ等に基づくモデル構築(3年) → 活用基盤の設計・構築(2年) (b) WebやSNS等を利用した新たな脅威の観測・分析・対策技術や、先行的防御の実現を目指した予防基盤技術の確立が必要。 (c) IPv4アドレスの枯渇によりIPv6の普及が見込まれ、IPv6環境の実践的なセキュリティ検証と防御技術の確立が必要。	「国際連携によるサイバー攻撃予知・即応技術の研究開発（総務省）」 「実践的サイバーセキュリティ技術の確立（NICT）」
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	(a)海外を含めた広域観測には、マルウェアの挙動分析の研究及び海外のステークフォルダとの調整が必要。 広域観測に向けた海外の関係者との調整(3年) → 広域観測基盤の構築(2年) (b)能動的なディフェンスを実現するためには、その前段としてサイバー攻撃を能動的に観測するメカニズムの確立と観測網構築が必要。	「国際連携によるサイバー攻撃予知・即応技術の研究開発（総務省）」 「広域の攻撃観測とマルウェアの解析、さらにそれらを統合するサイバーセキュリティ技術の研究開発（NICT）」 「実践的サイバーセキュリティ技術の確立（NICT）」：Web等の観測・分析技術

個人情報等の柔軟管理の実現

No.	重要テーマ	概要・ロードマップ（イメージ）	取組施策の例
⑦	個人情報等の利活用を促進する自己情報の統制技術	医療情報への適用を行うための実用化研究の前提として、秘密計算やプライバシー保護データマイニング技術等の基礎研究が必要。 	「災害に備えたクラウド移行促進セキュリティ技術の研究開発（旧：クラウド対応型セキュリティ技術の研究開発）（総務省）」 「適材適所にセキュリティ技術を自動選択し、セキュアなネットワークを最適に構成するためのセキュリティアーキテクチャの研究開発（NICT）」 「ITによる生活安全技術：消費者の情報や権利を保護するための情報セキュリティ対策技術（産総研）」 「新世代情報セキュリティ研究開発事業（アクセス制御、クラウド）（経産省：H24終了予定）」
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	ネットワーク・トレースバック技術やサイバー攻撃の証拠データの収集・信頼性評価技術が必要。なお、法制度の整備と並行して進めることが必要。 	「適材適所にセキュリティ技術を自動選択し、セキュアなネットワークを最適に構成するためのセキュリティアーキテクチャの研究開発（NICT）」
⑨	ITリスクに関する理論から実務までの体系化	リスクに対する社会の捉え方は、災害発生時と通常時では異なるため、許容されるリスクを調整するリスク・コミュニケーションの仕組みが必要。 	

研究開発の促進基盤の確立と情報セキュリティ理論の体系化

No.	重要テーマ	概要・ロードマップ（イメージ）	取組施策の例
⑩	情報セキュリティ研究の基盤体系化	セキュリティをサイエンスとして評価する方法の研究と理論研究の実証のためのデータ基盤の構築が必要。 データ収集制度の整備 ﾃﾞｰﾀ形式の統一、評価方法の体系化の研究(3年) ﾃﾞｰﾀ基盤の構築(2年)	「マルウェア検体や攻撃トラフィック等のセキュリティ情報を安全に研究利用するためのサイバーセキュリティ研究基盤（NONSTOP）の研究開発（NICT）」 「情報基盤における安全性や信頼性の確立（産総研）」
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品質評価認証技術	適切なコストで実現できるソフトウェアの品質評価技術が求められており、標準化のプロセスに沿った研究が必要。 国内調整・ISOの新作業項目の提案取纏め(1年) ISO標準化プロセス(2年)	「高度大規模半導体集積回路セキュリティ評価技術開発事業(経産省)」 「適材適所にセキュリティ技術を自動選択する技術の一環として、セキュリティ技術の組み合わせ方の正当性を評価する手法の研究開発及びプロセスのISOにおける標準化（NICT）」 「アーキテクチャ安全性評価技術の確立（NICT）」 「情報基盤における安全性や信頼性の確立（産総研）」
⑫	情報理論的安全性を備えた暗号技術	(a)情報理論的な暗号では、大きな秘密鍵を事前に共有する仕組みが重要。量子暗号の場合、その手段として量子通信が有望。 量子通信の特定環境における実現(10年) (b)量子計算機が実現されても安全性が低下しない、長期に渡って安全性を保証できる暗号技術が必要。 安全性評価手法(5年) 実装技術(5年) 数学的アルゴリズム開発(2年) 次世代PKI・電子署名試験環境構築(3年)	「現代暗号と量子ICTを組み合わせて新たな秘匿通信システムを実現する量子セキュリティ技術の研究開発（NICT）」

震災からの復旧・復興、新たな成長に寄与する研究開発

No.	重要テーマ	概要	関連分野
⑬	耐災害性の高い情報通信システムの構築	情報連絡・共有の困難化、サプライチェーン崩壊等が問題となった。耐災害性の高いシステムの再構築、バックアップや分散化等に対応した事業継続計画（BCP）の見直しが不可欠。	②、③の研究に関連
⑭	「リスク・マネジメント」等	災害発生時には、最適な対応を行うための「ダイナミック・リスク対応」の観点が必要。また、リスク・コミュニケーションの観点から情報の伝達、情報のコントロールを検討しておく必要がある。	⑨の研究に関連
⑮	個人情報等の柔軟管理の実現	一度インターネットに流出した情報の回収における困難性を鑑み、平時から災害時に備え、個人情報等を適切にコントロールする研究開発を進めておくことが望ましい。	⑦の研究に関連
⑯	「ニュー・ディペンダビリティ」	社会の情報システムへの依存度が増す中、ダイバーシティ・ネットワークや、上位から下位までセキュリティの整合性を保証するシステム構築技術が求められている。	②、③の研究に関連