

# 情報セキュリティ研究開発戦略の 具体的な推進方策について

2011年 6月 21日

内閣官房情報セキュリティセンター(NISC)

<http://www.nisc.go.jp/>

## ご意見を頂きたい観点

- 研究開発の推進能力が国際競争力の源泉。
- 各重要テーマについて、研究開発を推進するため、早急に具体的な推進方策を確立する必要がある。



- 各テーマにおける主要プレイヤー（研究者、研究機関）
- 各プレイヤーの強み（弱み）
- 効果的なフレームワーク（官民連携、国際連携など）
- その他の課題

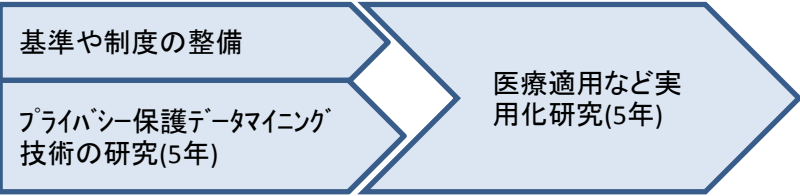
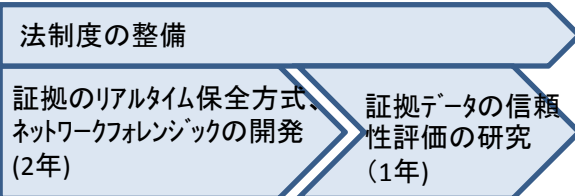

# 情報通信システム全体のニュー・ディペンダビリティの確保

No.	重要テーマ	概要・ロードマップ	関連施策等
①	リアルとバーチャル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	<p>コンテキストウェアネス(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。</p> <p>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)</p>	
②	システムのセキュリティ・コンフィグレーションを上位から下位まで自動保証する技術	<p>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。</p> <p>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)</p> <p>自動検証する形式手法等の研究(5年)</p>	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)
③	障害に対する自動リカバリー可能なネットワーク・アーキテクチャの構築技術	<p>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。</p> <p>ネットワークの仮想化・多様化技術の研究(5年)</p> <p>基盤技術を用いた自己治癒型ネットワークの研究(5年)</p>	
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	<p>生体情報を用いたIDマネ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。</p> <p>統合技術の開発、ISOの提案取纏め(1年)</p> <p>ISO標準化プロセス、実証実験(2年)</p>	

# 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	関連施策等
⑤	<p>攻撃者の行動分析等による予防基盤技術</p>	<p>(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。</p> <div data-bbox="752 491 1413 608" style="border: 1px solid black; padding: 5px; margin: 10px 0;"> </div> <p>(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。</p> <p>(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。</p>	
⑥	<p>大規模ネットワークにおけるマルウェア収集挙動分析と広域攻撃観測の統合技術</p> <p>○サイバー攻撃観測網の構築</p>	<p>(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ホルダとの調整が必要。</p> <div data-bbox="752 1098 1413 1214" style="border: 1px solid black; padding: 5px; margin: 10px 0;"> </div> <p>(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。</p>	<p>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)</p>

# 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	関連施策等
⑦	プライバシー情報の利活用を促進する自己情報コントロール技術	<p>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。</p> 	<p>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)            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)(METI)</p>
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	<p>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。</p> 	
⑨	ITリスクに関する理論から実務までの体系化	<p>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。</p> 	

# 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

No.	重要テーマ	概要・ロードマップ	関連施策等
⑩	サイバー・セキュリティ技術の評価する体系の確立、および実証研究のためのデータ基盤の構築	<p>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。</p>	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の研究開発(NICT)
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技術	<p>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。</p>	<p>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)</p> <p>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(METI)</p>
⑫	情報理論的安全性を備えた暗号技術	<p>(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。</p> <p>(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。</p>	現代暗号と量子ICTを組み合わせる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	関連施策等
①	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	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。	ITリスクに関する理論から実務までの体系化
③	個人情報等の柔軟管理	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。	個人情報等の柔軟管理の実現
④	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。	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