資料2

NISC National Information Security Center

情報セキュリティ研究開発戦略の取組みについて

2012年　3月　30日

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

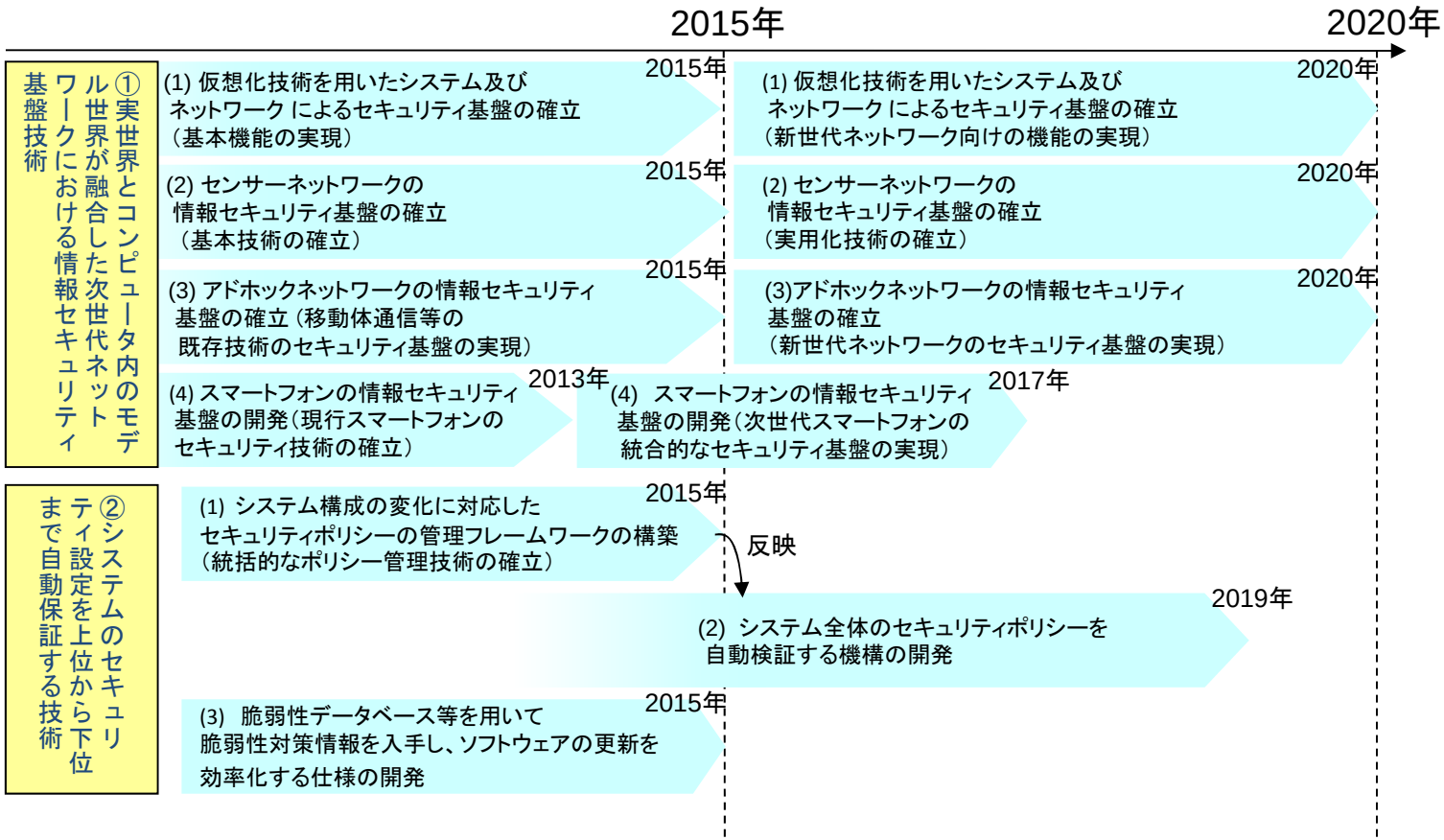
情報セキュリティ研究開発戦略の重要分野

重要分野		投資型	重要分野		投資型
ニュー・ディパ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	イノベーション型	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	長期基盤型
	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	長期基盤型		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	緊急対応型
	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	長期基盤型		⑨ITリスクに関する理論から実務までの体系化	イノベーション型
	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	緊急対応型	研究促進基盤の確立	⑩情報セキュリティ研究の基盤体系化	長期基盤型
ゼロディ・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	イノベーション型		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	イノベーション型
	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	緊急対応型		⑫情報理論的安全性を備えた暗号技術	長期基盤型

出典:「情報セキュリティ研究開発戦略」(2011年7月8日情報セキュリティ政策会議)

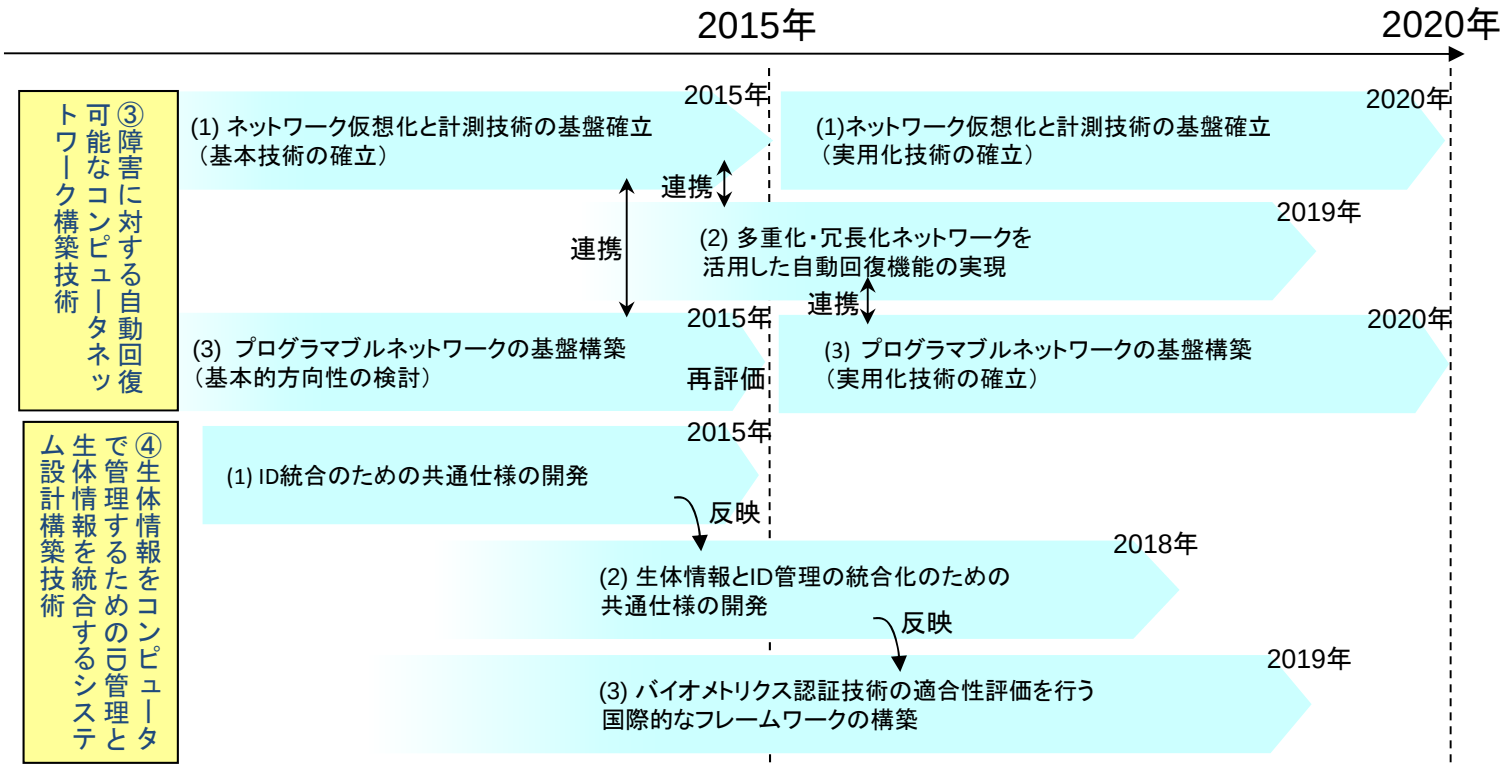
技術ロードマップ詳細化イメージ（１）

コンセプト①：情報システム全体のニュー・ディパンダビリティの確保（1／2）



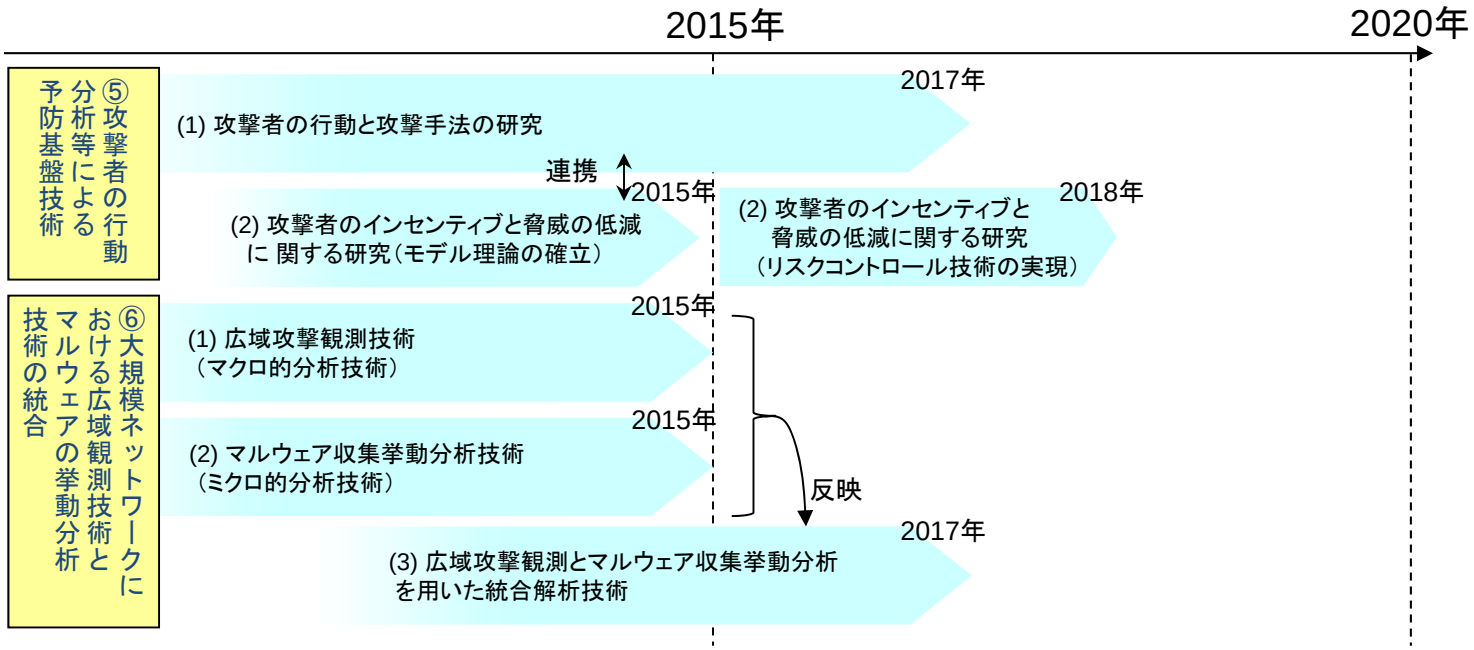
技術ロードマップ詳細化イメージ（２）

コンセプト①：情報システム全体のニュー・ディパンダビリティの確保（2／2）



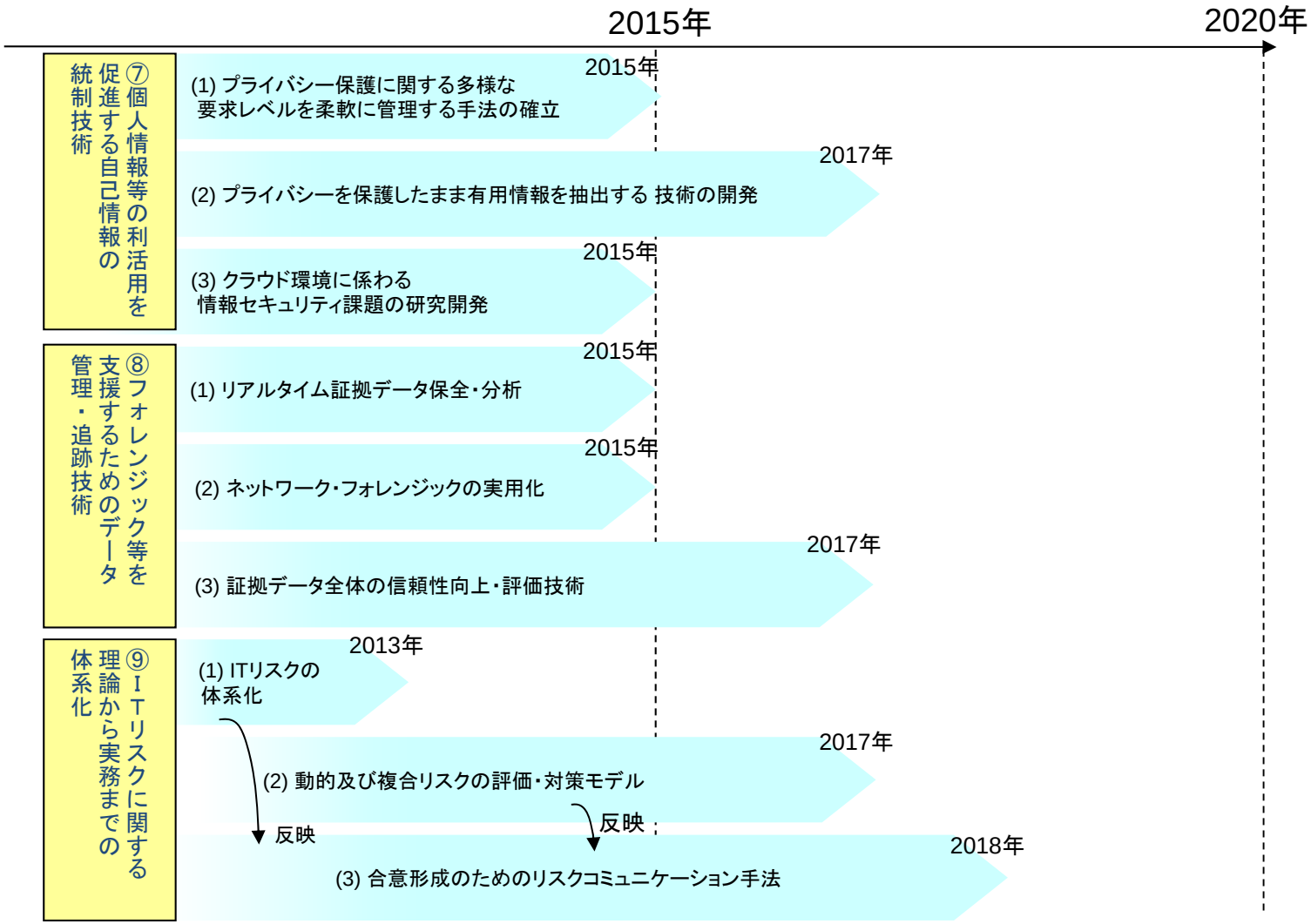
技術ロードマップ詳細化イメージ（３）

コンセプト②：攻撃者の行動分析に基づくゼロディ・ディフェンス（先読みの防御）



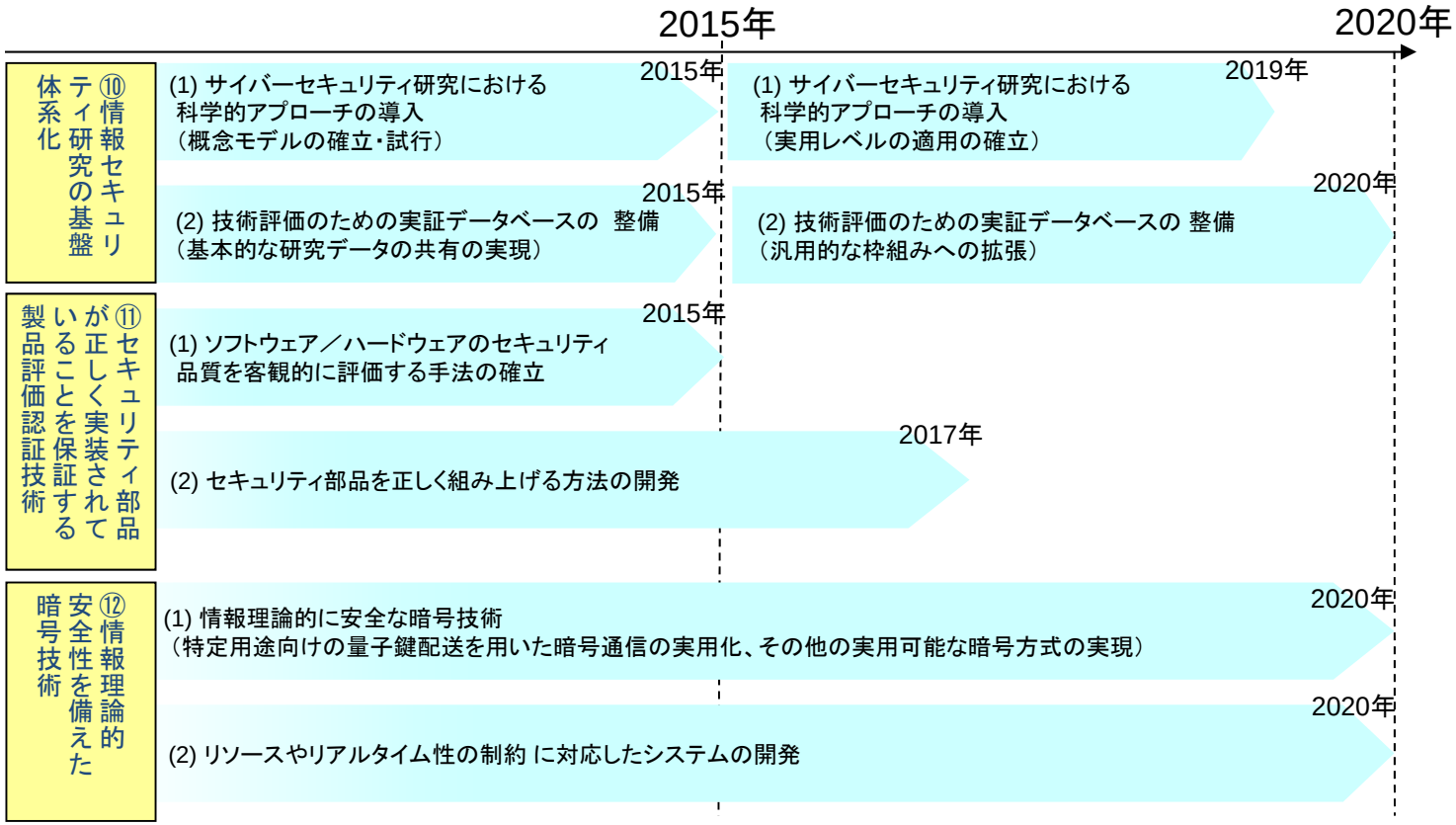
技術ロードマップ詳細化イメージ（４）

コンセプト③：個人情報等の柔軟管理の実現



技術ロードマップ詳細化イメージ（５）

コンセプト④：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



情報セキュリティ研究開発戦略に関する各省取組一覧

分類	重要テーマ名	推進テーマ	各省・独法の取組	備考
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	(1)仮想化ネットワークによるセキュリティ基盤の確立	「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）」	
		(2)センサーネットワークの情報セキュリティ基盤の確立	「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）」 「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）」	
		(3)アドホックネットワークの情報セキュリティ基盤の確立		
		(4)スマートフォンの情報セキュリティ基盤の開発		
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	(1)システム構成の変化に対応したセキュリティポリシーの管理フレームワークの構築	「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）」	
		(2)システム全体のセキュリティポリシーを自動検証する機構の開発	「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)脆弱性データベース等を用いて脆弱性対策情報を入手し、ソフトウェアの更新を効率化する仕様の開発	「CYBEXを活用した国際的セキュリティ知識ベースの構築（NICT）」	
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	(1)ネットワーク仮想化と計測技術の基盤確立	「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）」	
		(2)多重化・冗長化ネットワークを活用した自動回復機能の実現		
		(3)プログラマブルネットワークの基盤構築		
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	(1)ID統合のための共通仕様の開発		
		(2)生体情報とID管理の統合化のための共通仕様の開発		
		(3)バイオメトリクス認証技術の適合性評価を行う国際的なフレームワークの構築		

分類	重要テーマ名	推進テーマ	各省・独法の取組	備考
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	(1)攻撃者の行動と攻撃手法の研究	「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）」	
		(2)攻撃者のインセンティブと脅威の低減に関する研究	「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）」	
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	(1)広域攻撃観測技術（マクロ的分析技術）	「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）」	
		(2)マルウェア収集挙動分析技術（ミクロ的分析技術）	「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）」 「新世代情報セキュリティ研究開発事業（経産省：H24終了予定）」 「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）」 「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）」	
		(3)広域攻撃観測とマルウェア収集挙動分析を用いた統合解析技術	「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）」	

分類	重要テーマ名	推進テーマ	各省・独法の取組	備考
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	(1)プライバシー保護に関する多様な要求レベルを柔軟に管理する手法の確立	「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）」	
		(2)プライバシーを保護したまま有用情報を抽出する技術の開発	「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）」 「新世代情報セキュリティ研究開発事業（経産省：H24終了予定）」	
		(3)クラウド環境におけるプライバシー保護技術の確立	「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）」 「新世代情報セキュリティ研究開発事業（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	(1)リアルタイム証拠データ保全・分析技術		
		(2)ネットワーク・フォレンジックの実用化		
		(3)証拠データ全体の信頼性向上・評価技術		
⑨	ITリスクに関する理論から実務までの体系化	(1)ITリスクの体系化		
		(2)動的および複合リスクの評価・対策モデル		
		(3)合意形成のためのリスクコミュニケーション手法		

分類	重要テーマ名	推進テーマ	各省・独法の取組	備考
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	(1)サイバーセキュリティ研究における科学的アプローチの導入		
		(2)技術評価のための実証データベース等の整備	「IT融合による新産業創出のための研究開発事業（サイバーセキュリティテストベッドの構築）(経産省)」 「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）」	
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	(1)ソフトウェア/ハードウェアのセキュリティ品質を客観的に評価する手法の確立	「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)」 「新世代情報セキュリティ研究開発事業（経産省：H24終了予定）」 「耐タンパディペンダブルVLSIシステムの開発・評価(JST)」 「情報基盤における安全性や信頼性の確立（産総研）」	
		(2)セキュリティ部品を正しく組み上げる方法の開発	「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）」	
⑫	情報理論的安全性を備えた暗号技術	(1)情報理論的に安全な暗号技術の研究	「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）」	
		(2)リソースやリアルタイム性の制約を考慮した方式の研究開発		

分類	重要テーマ名	推進テーマ	各省・独法の取組	備考
震災からの復旧・復興、新たな成長に寄与する研究開発				
⑬	耐災害性の高い情報通信システムの構築	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）の見直しに係る研究開発	②、③の研究に関連して推進	
⑭	リスク・マネジメント等	災害発生時における情報の伝達、情報のコントロールに係る研究	⑨の研究に関連して推進	
⑮	個人情報等の柔軟管理	個人情報等を適切にコントロールする研究開発	⑦の研究に関連して推進	
⑯	ニュー・ディペンダビリティ	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の研究開発	②、③の研究に関連して推進	