資料3

NISC National Information Security Center

情報セキュリティ研究開発戦略（案）の概要

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/

情報セキュリティ研究開発戦略（案）の構成

「研究開発戦略」策定の目的と今までの経緯

1．はじめに

「科学技術基本計画（総合科学技術会議が策定）」における「情報セキュリティ」の具体化

2．これまでの取組み

グランドチャレンジ型研究開発の検討 → 技術戦略専門委員会 報告書2006 → 技術戦略専門委員会 報告書2008 → **本戦略**

情報セキュリティ研究開発戦略

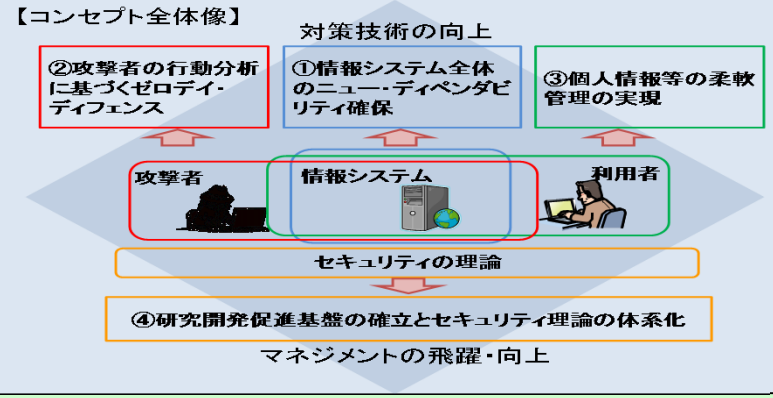
3．情報セキュリティに係る環境変化

情報技術の変革、脅威の増大、研究予算の削減

大震災の発生

4．情報セキュリティ研究開発戦略のコンセプト

攻撃者の経済的負担を増大させる革新的な取組（「ゲーム・チェンジ」）に重点をおいた研究開発を促進



5．情報セキュリティの研究開発における重要分野

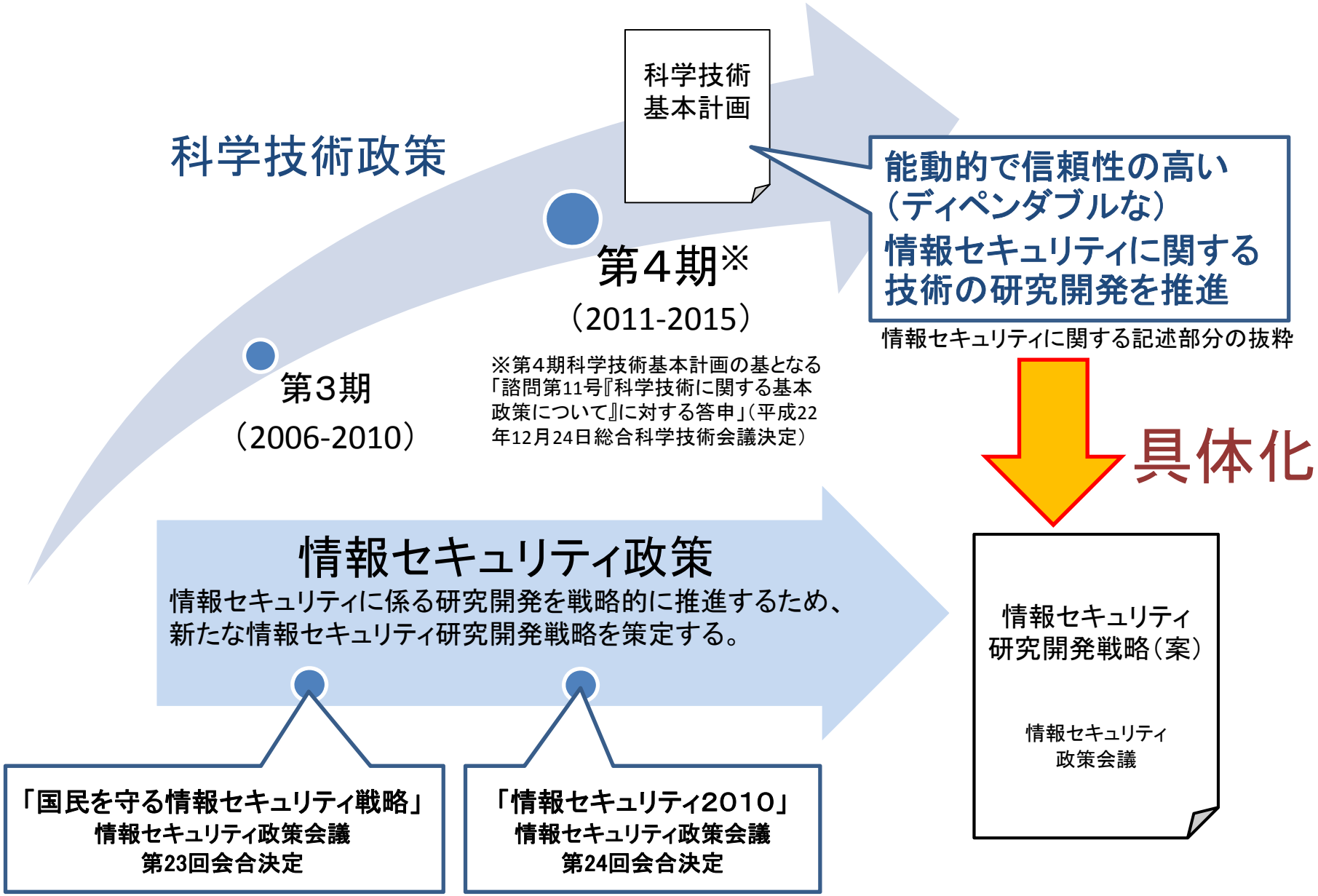
4つのコンセプトに紐づく、12の重要分野を選定

投資の型を設定し、研究開発ロードマップを作成

6．東日本大震災を踏まえた重点分野

耐災害性の高い情報通信システム構築技術、リスク・マネジメント等を重点化する分野として選定

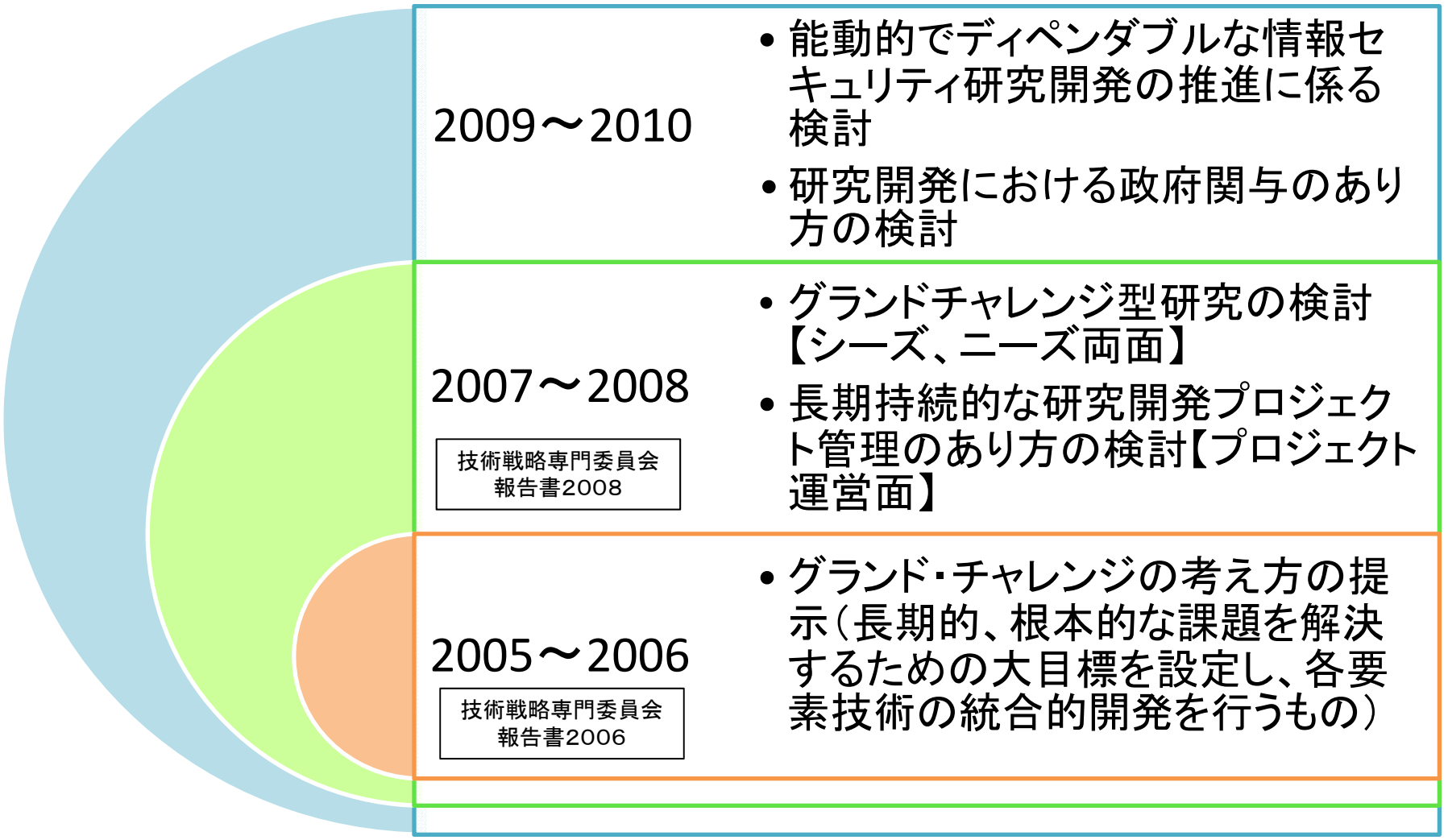
「研究開発戦略」策定の目的



3

これまでの取組み

「グランドチャレンジ型研究開発」の考え方を包含するとともに、益々複雑化する脅威に対応するための研究開発を推進



情報セキュリティ研究開発戦略の基本的な考え方

①サイバー攻撃の非対称性を解消する（サイバー攻撃を無効化させ、攻撃者の経済的負担を増大させる）能動的研究に変える革新的取組みの推進

②情報セキュリティの観点から耐災害性に強い情報通信システムの構築や「リスク・マネジメント」、「リスク・コミュニケーション」に係る研究の推進

③社会的イノベーションを支える研究開発と連携し、高度な情報セキュリティ基盤の構築に寄与する研究開発の促進

④次世代インターネットなどの革新的研究開発との連携

⑤我が国の情報セキュリティ産業のグローバル展開へ貢献

⑥研究開発における国際連携の推進

⑦官民の役割分担を明確化し、官民連携を推進。また、必要な予算の確保、研究開発の各段階における動機付けに努力

情報セキュリティ研究開発戦略のコンセプト（全体像）

攻撃者の経済的負担を増大させる革新的な取組み（「ゲーム・チェンジ」）に重点をおいた研究開発を促進

対策技術の向上

②攻撃者の行動分析に基づくゼロデイ・ディフェンス

①情報システム全体のニュー・ディペンダビリティ確保

③個人情報等の柔軟管理の実現

攻撃者

情報システム

利用者

セキュリティの理論

④研究開発促進基盤の確立とセキュリティ理論の体系化

マネジメントの飛躍・向上

４つの重要コンセプト

①情報システム全体のニュー・ディペンダビリティ※の確保

次世代の社会システムは、リアルとバーチャルが一層密接に結く。このとき、実世界とコンピュータを繋ぐセンサーや制御機器を構成要素には高い信頼性が求められるため、ニュー・ディペンダブルなシステム構築技術が必要となる。

②攻撃者の行動分析に基づくゼロデイ・ディフェンス

サイバー攻撃対応は後追いとなっており、根本解決を目指した研究開発を推進する。このため、ネットワークを広域に観測し、攻撃の公算や影響を予測し、未知の攻撃への対策の最適化を行う技術が求められている。

③個人情報等の柔軟管理の実現

個人情報等に対する個人の意識や社会のとらえ方は、災害発生時と復興時では変化する。一度インターネットに流出した情報回収の困難性を鑑み、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。

④研究開発促進基盤の確立とセキュリティ理論の体系化

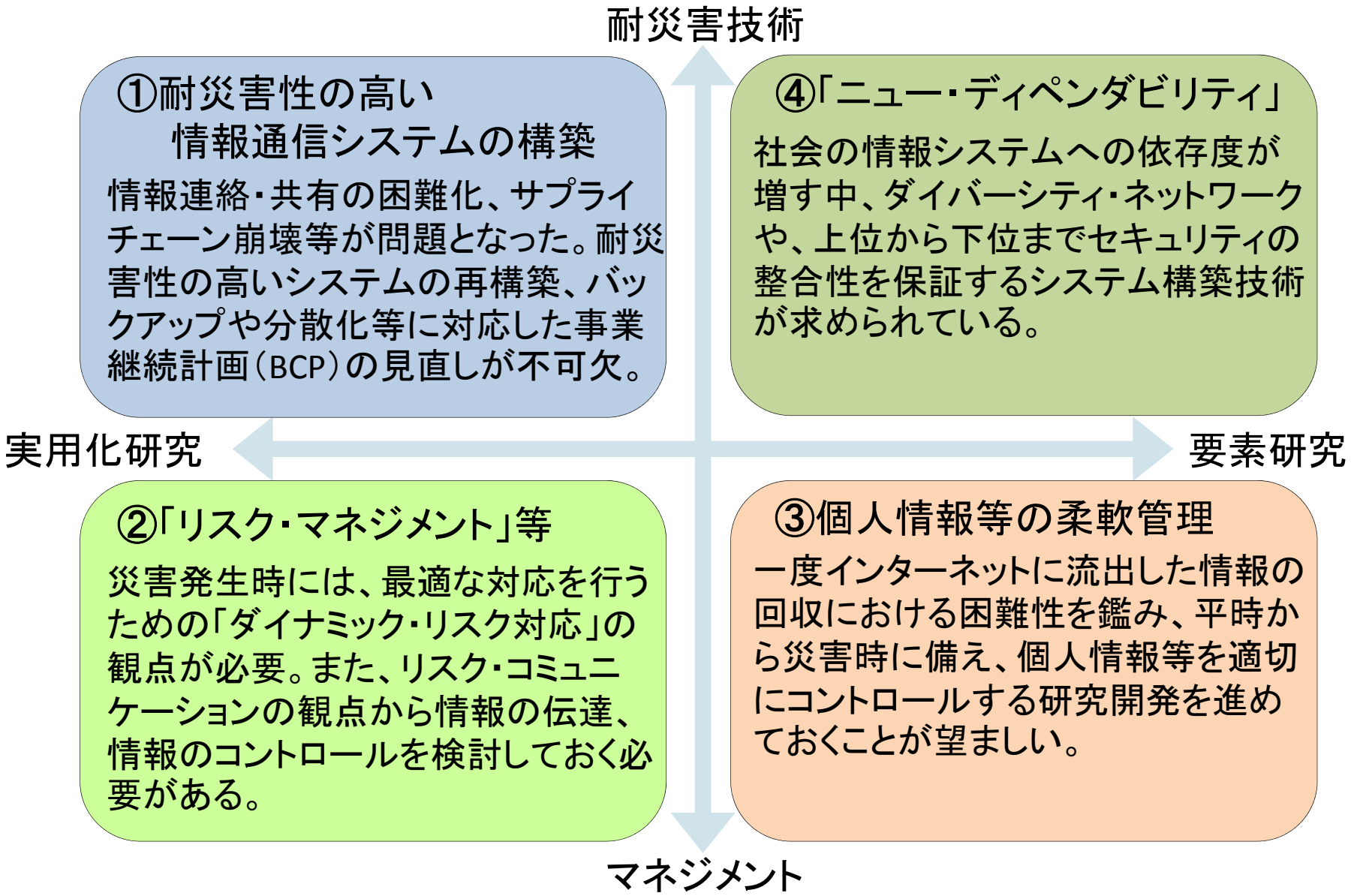
現在の情報セキュリティ技術は、リスクに対応するノウハウ集になっており、技術が理論的に体系化されていない。セキュリティ技術を理論的に評価できるようにすることで、より優れた研究や適切な普及方法を明らかにすることができる。

※情報セキュリティは、従来、人間の不正行為に基づく事象を主な対象としていたが、情報通信技術への社会の依存度の増大に伴い、自然現象や経年劣化、ヒューマンエラー等も含めた事象への総合的対応が必要になり、従来のディペンダブルの概念を拡張するとともに、サイバー攻撃を無効化するなど「能動的」な情報セキュリティの要素を追加したものを「ニュー・ディペンダビリティ」という。

重要分野の研究開発ロードマップ

重要分野		投資型
ニュー・ディペンダビリティの確保	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
	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
	障害に対して自動回復可能なネットワーク構築技術	長期基盤型
	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	緊急対応型
ゼロデイ・ディフェンス	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
	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
柔軟管理の実現	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
	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
	IT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
研究促進基盤の確立	情報セキュリティ研究の理論の体系化	長期基盤型
	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
	情報理論的安全性を備えた暗号技術	長期基盤型

震災からの復旧・復興、新たな成長に寄与する研究開発



（参考）米国・欧州の研究開発戦略との比較

	日本 （本研究開発戦略）	米国 （NITRD-CSIAの戦略）	欧州 （FP7，ENISAの戦略）
主要なコンセプト	・ニュー・ディペンダビリティの確保 ・ゼロディ・ディフェンス ・個人情報等の管理の柔軟性の向上 ・研究開発を促進するための基盤整備	・Moving Target （攻撃対象を変化させ、攻撃の困難さとコストを増加） ・Tailored Trustworthy Spaces （コンテキストに応じた適切なセキュリティの実現） ・Cyber Economic Incentives （適切な投資判断に必要な科学的指標の提供）	・信頼できるインフラの構築 ・重要インフラ防護技術の向上 ・Trustworthy ICT （異種なネットワークとシステムにおける信頼性の向上）
2010年度予算 （GDP比）	48.5億円 （0.0009%）	3.69億ドル（332億円） （0.0025%）	0.8億ユーロ※（89.6億円） ※Trustworthy ICTの予算

2.8倍

1ドル＝90円換算、1ユーロ＝112円換算

日本の情報セキュリティ研究予算は米国の15%（GDP比を考慮しても1/3程度）