NISC National Information Security Center

資料2

情報セキュリティ研究開発戦略（素案）の検討

2011年　4月　11日

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

背景

「国民を守る情報セキュリティ戦略」
情報セキュリティ政策会議　第23回会合
（平成22年5月11日）決定

（4）技術戦略の推進等
①情報セキュリティ関連の研究開発の戦略的推進等
米国等の動向も踏まえ、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、新たな情報セキュリティ研究開発戦略を策定する。

「情報セキュリティ2010」
情報セキュリティ政策会議　第24回会合
（平成22年7月22日）決定

ア）新たな情報セキュリティ研究開発戦略の策定（内閣官房）
米国のサイバーセキュリティ強化法案等の動向を踏まえ、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、2011 年6 月を目処に新たな情報セキュリティ研究開発戦略を策定する。

（略）

情報セキュリティ研究開発戦略（仮称）の位置付け

■ 第4期科学技術基本計画の基となる「諮問第11号『科学技術に関する基本政策について』に対する答申」（平成22年12月24日総合科学技術会議決定）

2．重要課題達成のための施策の推進
（4）国家存立の基盤の保持
　ⅰ）国家安全保障・基幹技術の強化
（抜粋）
　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技術の研究開発を推進する。

具体化

情報セキュリティ研究開発戦略（仮称）

情報セキュリティ政策会議

〇策定プロセス
情報セキュリティ政策会議 技術戦略専門委員会での検討を踏まえ、各省協議を経て情報セキュリティ政策会議本体で本年6月をめどに決定する。
〇位置付け
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。

情報セキュリティ研究開発戦略（仮称）策定における基本的考え方

1. 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し、世界を先導するとともに、情報セキュリティ分野における従来の受動的対応から能動的対応に「ゲーム・チェンジ」するための革新的な取り組みを促進する。

2. 情報セキュリティについての課題を抜本的に解決するために、本戦略の推進にあたり、情報通信技術のパラダイムシフトを実現する次世代インターネットなどの革新的研究開発との連携を図る

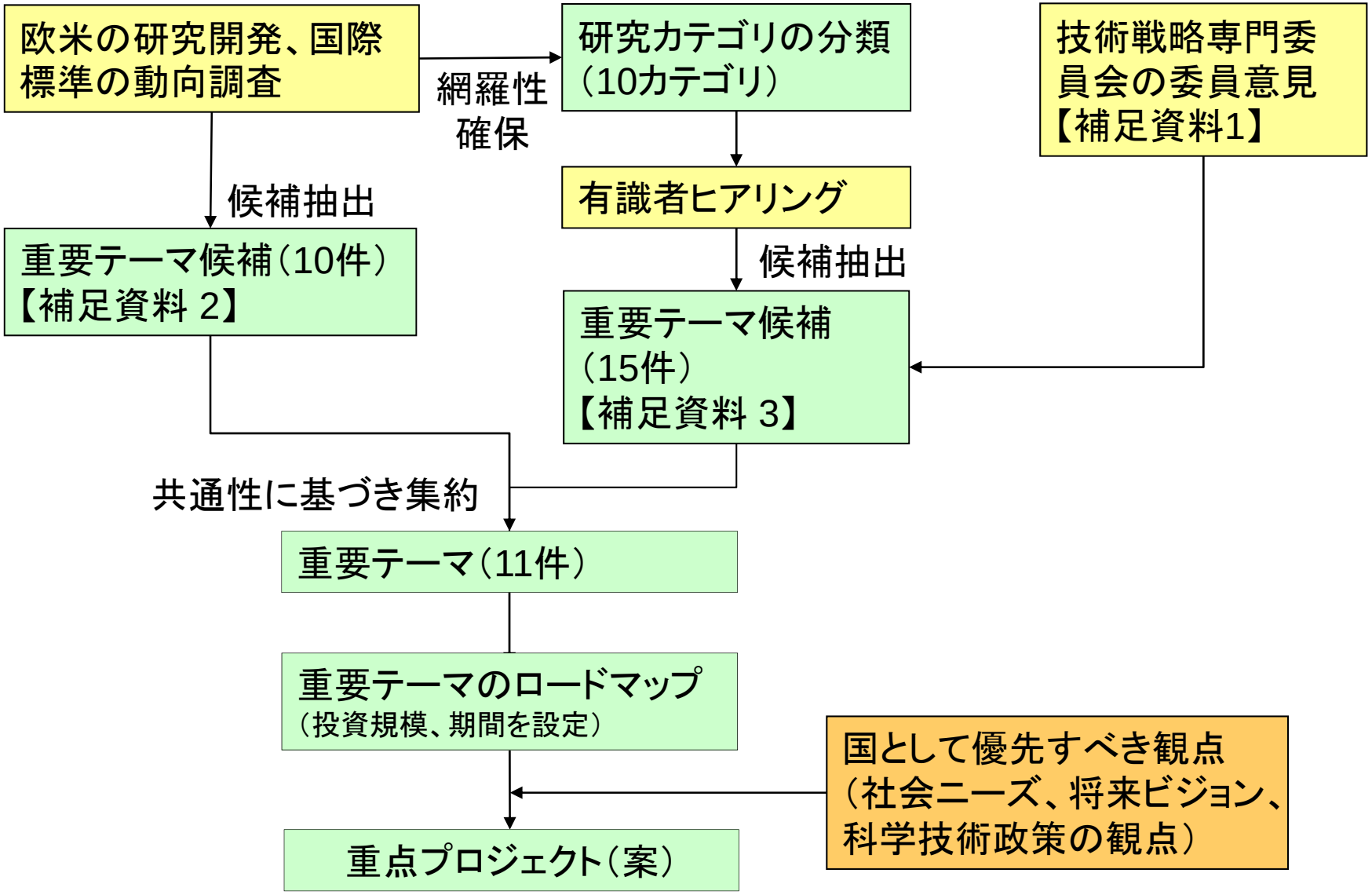
3. グリーン、ライフなどの社会的イノベーションを支える研究開発との連携を図り、社会的に高度な情報セキュリティ基盤の構築を促進する。

4. 本戦略の推進にあたり、情報セキュリティについての課題を抜本的に解決する観点から、科学技術分野の新たな研究テーマについて積極的な貢献を行う。

5. 本戦略の推進にあたり、国際連携を強化する。

6. 本戦略の推進にあたり、研究開発の評価を適切に行うとともに、必要な予算の確保や研究開発の各段階におけるインセンティブ付与に努める。

具体化に向けた検討の流れ



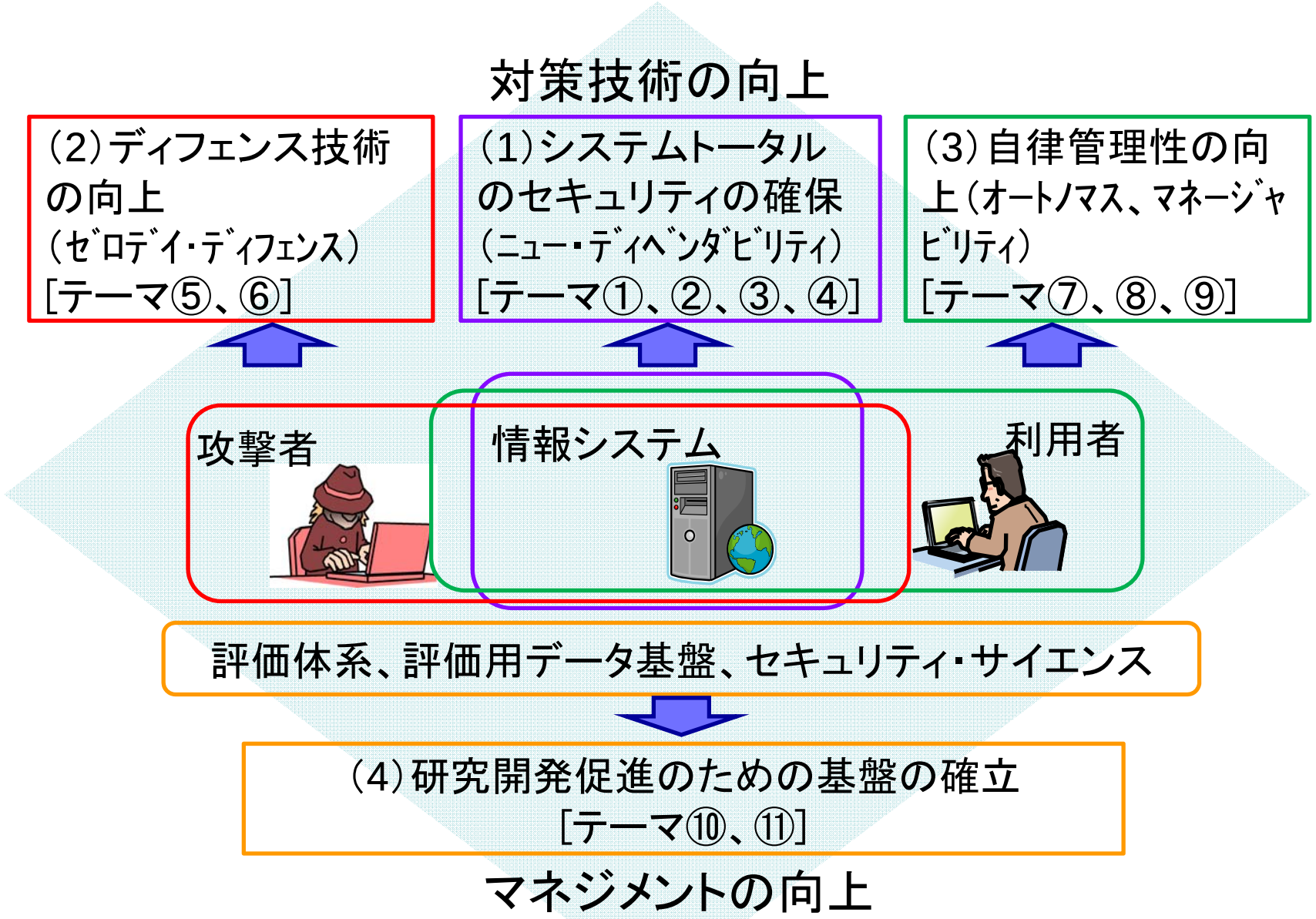
研究カテゴリー別における重要テーマ(1/2)

研究カテゴリ	重要テーマ	達成目標	内容	重要テーマ候補との対応関係
暗号基盤技術	情報理論的安全性を備えた暗号技術	長期利用に耐えうる暗号(暗号危殆化の解決)と組込みシステム等への暗号利用の拡大	計算理論的な暗号技術は、暗号危殆化の問題が付きまとう。情報理論的な暗号に基づく鍵管理により、長期に耐えられる暗号を実現する。また、情報理論的な暗号は、線形演算をベースとすることで計算量が抑えられるため、計算資源の小さい組込みシステムなど幅広い分野への応用が可能となる。	・情報理論的安全性を備えた暗号技術
バイオメトリック技術	ID管理とバイオメトリクスを統合するシステム・アーキテクチャの設計・構築	ID認証基盤の共通化による安全性と利便性の向上	バイオメトリクスの要素技術は性能面では成熟が進んでいるが、システム全体のグランド・デザインが遅れている。ID管理、バイオメトリクス、アプリケーション等の要素技術をSOA, SAML等により統合したオープンなシステム・アーキテクチャを構築する。	・ID管理に関するｼｽﾃﾑｱｰｷﾃｸﾁｬの全体像(ﾌﾚｰﾑﾜｰｸ)の構築
セキュアネットワーク構築技術	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	自己治癒型システムにより、一定の被害の発生を事前に防止するネットワークの実現。	ネットワークに多様性と冗長性を持たせることにより、ネットワークに障害が発生しても自動的にリカバリーするための仕組みを実装することにより、一定の被害を防止する。IPv4, v6の共存環境で多様性を持たせたダイバーシティネットワークや仮想化ネットワーク等の研究を進める必要がある。	・障害に対する自動ﾘｶﾊﾞﾘｰ可能なﾈｯﾄﾜｰｸｱｰｷﾃｸﾁｬの構築技術 ・次世代ｲﾝﾀｰﾈｯﾄｲﾝﾌﾗのｾｷｭﾘﾃｨ確保【欧米】
ネットワーク観測防御技術	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	ユビキタスネットワーク環境における自律的な安全性の確保。	ゲーム機やスマートフォンなどの情報機器のIPv6接続により、ネットワークの大規模化が進んでいる。従来の専門家のオペレーションによる攻撃検知・対処から、異常検知手法による自動化と、検知から防御への連携技術を実現する必要がある。	・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 ・ﾙｰﾀ等へのDDoS検知機能の組込み
プライバシ保護技術	プライバシ情報の利活用を促進する自己情報コントロール技術	プライバシ情報の積極利用と安全確保のバランスを所有者が管理できる環境の実現。	医療情報、位置情報、ライフログなどプライバシ情報の安全な積極活用のニーズが高まっている。機密レベルは個々人により多様であり、データの機密性と有効活用のレベルを自己コントロールする技術を実現する。また、機密性を確保したままでデータを有効に分析するための秘密計算やデータ匿名化技術を開発する。	・自己情報ｺﾝﾄﾛｰﾙ権を管理する技術 ・ｱﾄﾞﾎｯｸﾈｯﾄﾜｰｸのｾｷｭﾘﾃｨ設定の管理技術 ・ｾﾝｻｰﾈｯﾄﾜｰｸにおけるﾌﾟﾗｲﾊﾞｼｰ保護 ・ｻｰﾋﾞｽ・ﾌﾟﾗｲﾊﾞｼｰ保護【欧米】

研究カテゴリー別における重要テーマ(2/2)

研究カテゴリ	重要テーマ	達成目標	内容	重要テーマ候補との対応関係
セキュア・システム構築技術	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	システム・トータルの信頼性を確保するための基盤の確立。	レイヤー化、コンポーネント化が進む中で、システムの上位から下位までトータルに整合性を保証する仕組みが求められている。セキュリティ・ポリシやコンフィグレーションに基づきシステム間の整合性を形式手法等のアプローチにより自動検査する技術を開発する。	・上位レイヤのコンフィグレーションを下位まで自動的に保証する技術 ・アイソレーションとアクセスコントロールを保証する技術 ・セキュア・ソフトウェアエンジニアリング【欧米】 ・高信頼・証明可能なセキュアシステムとアーキテクチャ【欧米】
コンテンツセキュリティ技術	フォレンジックス等を支援するためのデータ管理・追跡技術	デジタル情報が一般化した経済社会におけるガバナンス確保の基盤確立。	社会経済活動における「情報」の役割増大を踏まえ、デジタル情報に対応したフォレンジックス、トレースバックなどの技術開発を行う。	・フォレンジック、トレースバック及びアトリビューション技術【欧米】
マネジメント技術（デシジョンサポート技術）	攻撃者の行動分析による脅威予測技術	攻撃者の行動予測に基づくセキュリティ対策の最適化。	内部攻撃者、ネットワーク攻撃者の行動観測によるプロファイリング、インセンティブやゲーム理論に基づく行動モデルの分析により、攻撃者の予測モデルから脅威を洗い出し、対策の最適化を行う技術を開発する。	・敵対行動の予測【欧米】 ・内部の脅威検知・緩和【欧米】
マネジメント技術（セキュリティメトリクス手法）	サイバー・セキュリティ技術を評価する体系の確立	サイバーセキュリティ研究の最適化、有望研究の促進。	サイバーセキュリティをサイエンスとして評価できるような体系にしなければ、セキュリティ分野の発展は期待できない。セキュリティの他の分野全般に対して、研究の選別や適切な普及方法を明らかにするための評価手法の開発や体系化を行う。	・サイバーセキュリティサイエンスの確立 ・メトリクスとリスクベース意思決定【欧米】 ・重要インフラ、ネットワーク、情報と制御システムマネジメント【欧米】
マネジメント技術（評価用データの整備）	サイバーセキュリティ実証研究のためのデータ基盤の構築	サイバーセキュリティ研究の促進の基盤。	理論研究は進展しても、問題となるのは実証研究のためのデータが必要になること。そのために、データを継続的に観測する仕組みが必要になる。例えば、情報処理実態調査におけるセキュリティ評価やマネジメントに関する調査項目の修正や追加をより適切なものとするために、学術研究成果の知見を活用することが考えられる。	・サイバーセキュリティ研究のためのデータ基盤の確立 ・脅威観測データの形式の統一化と共有方式の開発
マネジメント技術（効果的な改善手法）	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	システム設計におけるセキュリティ対策の費用対効果を改善する仕組みの確立。	標準化された評価認証により、システムの部品であるセキュリティ製品を適切に普及させることができる。製品認証は、システム設計の費用対効果を改善する上でも有用である。また、認証制度とそのための基盤を世界に先駆けて具体化することで、我が国の産業競争力の向上につながる。例えば、バイオメトリクスなどがその候補である。	・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制度 ・バイオメトリクスの適合性評価フレームワークの確立

重要分野のコンセプト



(1)システムトータルのセキュリティ確保への移行（ニュー・ディペンダビリティの確保）

クラウド化、仮想化、端末のユビキタス化、リアルタイムセンシング機能の強化、ユーザ情報を活用したコンテクストアウェア化を支えるニュー・ディペンダブルな情報システム構築技術の確立が求められている。要素技術が成熟する中、レイヤーやコンポーネントから構成されるシステムのトータルなセキュリティを確保する仕組みやフレームワークが必要。

No.	重要テーマ	技術ロードマップ	関連施策	必要額
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	コンテキストアウェアネス（センサーを用いてリアル空間の状況をコンピュータ内に能動的に収集・処理を行う）を実現するため、セキュアでディペンダブルな情報システム構築技術の研究が必要。		20億円×5年＝100億円
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	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）	5億円×10年＝50億円
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	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が必要。 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)		5億円×10年＝50億円
④	ID管理とバイオメトリクスを統合するシステム・アーキテクチャの設計・構築	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が必要。 国内調整・ISOの提案取纏め(1年) → ISO標準化プロセス、実証実験(2年)		10億円×3年＝30億円

(2)ディフェンス技術の向上（ゼロデイ・ディフェンス）

様々な脅威や未知の攻撃から情報システムに関わる被害を未然に防止でき、被害が発生した場合にもその被害を局限化する技術が必要。攻撃の後追い対策による不利な状況を根本解決するための技術が求められている。

No.	重点分野	技術ロードマップ	関連施策	必要額
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。		5億円 ×5年＝ 25億円
⑥	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 (a)サイバー攻撃観測網の構築	(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。	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）	15億円 ×5年＝ 75億円

(3)自律管理性の向上(オートノマス、マネージャビリティ)

ステークホルダーの多様化への柔軟な対応が求められる。すなわち、ユーザのみならず、ベンダーのスキルレベルの多様化が問題となっており、プライバシ情報の積極活用と保護のバランスなど多様性に対応したセキュリティの管理技術が求められる。

No.	重点分野	技術ロードマップ	関連施策	必要額
⑦	プライバシ情報の利活用を促進する自己情報コントロール技術	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。 基準や制度の整備 ﾌﾟﾗｲﾊﾞｼｰ保護ﾃﾞｰﾀﾏｲﾆﾝｸﾞ技術の研究(5年) 医療適用など実用化研究(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) 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)	5億円×10年＝50億円
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	技術的な要件が法制度と関連するため、技術的な研究開発は法制度の整備と並行して進めることが必要。 海外の状況を踏まえた法制度の整備 証拠のﾘｱﾙﾀｲﾑ保全方式、ﾈｯﾄﾜｰｸﾌｫﾚﾝｼﾞｯｸの開発(2年) 証拠ﾃﾞｰﾀの信頼性評価の研究1年)		10億円×3年＝30億円
⑨	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	適切なコストで実現できるシステムの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)	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) 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)	10億円×3年＝30億円

(4)研究開発促進のための基盤の確立

実証研究のためのデータの共通化・整備、研究の効率化のための評価体系の確立、他のセキュリティ分野の前提技術の開発が有効である。

No.	重点分野	技術ロードマップ	関連施策	必要額
⑩	サイバー・セキュリティ技術を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	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の研究開発（NICT）	10億円×5年＝50億円
⑪	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。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) 組込システムへの導入 (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) 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）	5億円×10年＝50億円

【参考】研究開発戦略の比較

	日本 （重点分野の共通コンセプト案）	米国(NITRDなど)	欧州(FP7、ENISAなど)
大方針	• システムトータルのセキュリティ確保への移行（ニュー・ディペンダビリティの確保） • ディフェンス技術の向上（ゼロデイ・ディフェンス） • 自律管理性の向上（オートノマス、マネージャビリティ） • 研究開発促進のための基盤の確立	•Moving Target（攻撃対象が変化することで、攻撃の困難さやコストを増加させる。） •Tailored Trustworthy Spaces（ユーザの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）	•セキュアで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 •ヘテロジニアスなネットワークとシステムにおける信頼性の向上 (Trustworthy ICT)
予算	科学技術基本計画に基づく各省庁の政策実現	各省庁の予算の積算と省庁横断プログラムによる調整	EUの大枠テーマに基づき、個別の研究を助成
研究戦略の考え方	• 技術的な裏付けに基づく重点分野と社会ニーズ、将来ビジョンの両面の整合性に基づき抽出	• 上位戦略との整合性 • 政府内でのニーズ • 技術の重要性、求められる技術レベルと現状レベルのギャップ	• 上位戦略との整合性 • 市場における競争力、優位性を得ることの重要性。 • ツール開発、標準化に積極的 • 他プログラムとの重複回避
民間の研究開発との切り分け	民間では取組みにくい分野、早急な解決が期待される分野に、国が関与することで産業の強化を図る。	民間が可能な研究開発は民間に任せる。政府が主体となるべき研究分野に重点をおき、成果は政府機関内で活用するとともに、民間にも積極的に移行する。	欧州企業の育成・振興を目的とした研究開発。官民連携プロジェクトが多い。

【参考】情報セキュリティ研究開発予算の算出

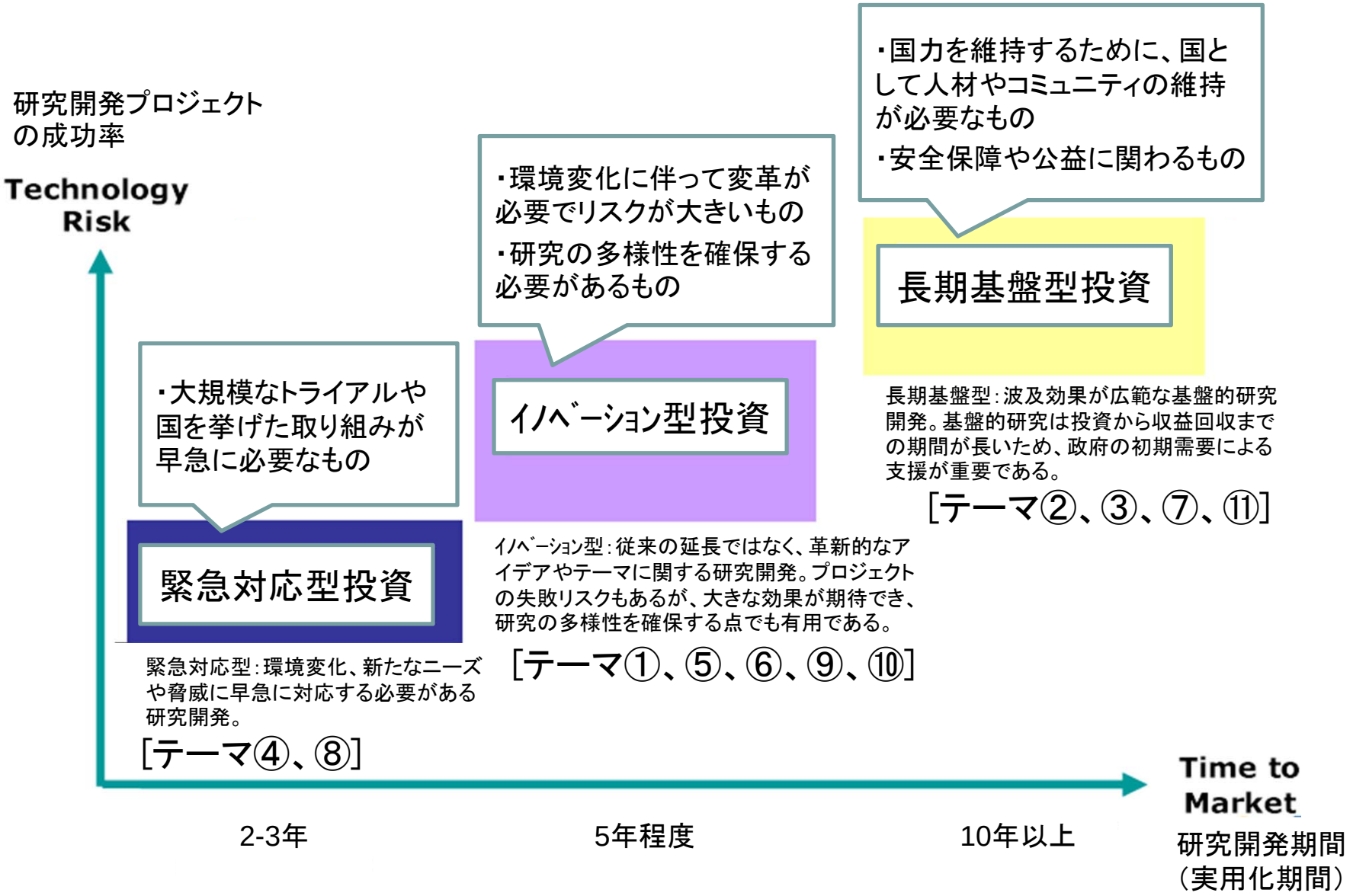
情報セキュリティ分野における重要テーマの研究に必要な費用は、年間100億円となる。また、重要テーマ以外の研究に20億円/年が必要であるため、合計120億円/年が必要である。

情報セキュリティ分野の研究費用を国際比較すると、2007年度は米国191億円(2.13億ドル)、日本64.3億円であり、GDP比では日米同程度の予算規模であった。

ところが、2010年度には、米国は334億円(3.72億ドル)に増加し、日本は48.5億円へと減少しており、GDP比で比べると2.5倍の差となっている。

仮に、前記年間120億円が情報セキュリティの研究費用に充てられるとすれば、米国とGDP比で同水準が確保できることになり、日本のこれまでの技術水準を維持することができる。

研究開発の投資タイプ



国が研究開発に関与する理由及び投資タイプ

	重要テーマ	国が関与する理由	投資の型
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	社会インフラを支えている重要システムは、セキュアでディペンダブルな情報システムを実現するべきであり、評価の制度設計に伴うため官民が協力して取り組むべき。	ｲﾉﾍﾞｰｼｮﾝ型
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	米国ではセキュリティ・オートメーションの研究が活発になっており、政府共通設定基準の議論も進んでいる。このため、政府が基準を示すなどの関与が必要であるが、ポリシーに基づいてシステム間の整合性を自動評価する技術などは未成熟であり、形式手法などの基礎研究が必要。	長期基盤型
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	次世代インターネットを見据えた研究であり、基礎となるネットワークの仮想化・多様化技術も未成熟。また、高信頼技術は効果を新たな収益に結び付けにくいため、個々の企業では取り組み難い。	長期基盤型
④	ID管理とバイオメトリクスを統合するシステム・アーキテクチャの設計・構築	関心分野はSAML等による認証ｼｽﾃﾑ･ｱｰｷﾃｸﾁｬの標準化である。国際的にも多数のｽﾃｰｸﾎﾙﾀﾞｰとの調整・合意が必要であり、諸外国の後塵を拝すことがないように官民一体として取り組む必要がある。	緊急対応型
⑤	攻撃者の行動分析等による予防基盤技術	攻撃者に有利な状況が続いており、プロファイリングは脅威の根本解決に繋がる可能性を持っている。一方、収益モデルが確立しにくい分野であり、民間だけでは取り組みが難しい。	ｲﾉﾍﾞｰｼｮﾝ型
⑥	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	マルウェアの挙動分析に必要な広域観測には、海外の多くのステークホルダとの調整が必要。革新的なアイデアを生むためには脅威の全体像を把握することが必要であり、国内の研究基盤を整備する観点で政府の関与が望ましい。	ｲﾉﾍﾞｰｼｮﾝ型
⑦	プライバシ情報の利活用を促進する自己情報コントロール技術	プライバシ情報の機密レベルは、国民の意識の相場観や法制度にも係わるため企業では取組み難い。なお、基礎となる秘密計算やプライバシ保護データマイニング技術は未成熟であり、医療分野等の応用には長期の研究が必要。	長期基盤型
⑧	フォレンジックス等を支援するためのデータ管理・追跡技術	国家機密の情報漏えいや知的財産の国外流出を防ぐ観点で、ネットワークフォレンジックスや証拠データの信頼性評価の研究開発等には官民が協力して取り組むべき。	緊急対応型
⑨	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	評価技術は責任分解の基準にも係わり、多くの関係者の事前調整が必要になるため、制度設計に伴う評価認証技術の開発には政府が関与すべき。	ｲﾉﾍﾞｰｼｮﾝ型
⑩	サイバー・セキュリティ技術を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	セキュリティをサイエンスとして評価する体系を確立することは、研究の多様性を確保する上で有用。ただし、必要性は理解されるが、収益モデルが期待し難い分野であるため政府の支援が望ましい。	ｲﾉﾍﾞｰｼｮﾝ型
⑪	情報理論的安全性を備えた暗号技術	情報理論的暗号の基盤となる量子通信の研究は10～20年の長期基礎研究とされており企業単独での取組みは難しい。また、政府が使用する暗号を評価できる人材やコミュニティの維持が国として必要。	長期基盤型

研究開発において国として優先すべき観点

分類	内容
社会のニーズや環境変化への対応	• 災害発生時、復興時、平常時で変化するプライバシ情報の取り扱いに対する社会的要求の解決 • 災害・障害に対する自動リカバリー可能なネットワークなど、ニューディペンダビリティを備えた情報システムの構築 • ITリスクのトレンドの変化（Dynamic Risk及びMultiple Risks）に対応するための技術の確立
情報セキュリティ以外の分野の研究開発戦略との連携（他分野との有機的連携を図ることにより革新的な研究開発を促進）	• 次世代インターネットなどの革新的研究開発との連携による情報セキュリティ課題の抜本的な解決（Game Changeの発想） • グリーン、ライフなどの社会的イノベーションを支える高度な情報セキュリティ基盤の構築（詳細は次頁）

科学技術基本計画との連携の観点

成長の柱としての2大イノベーションの推進

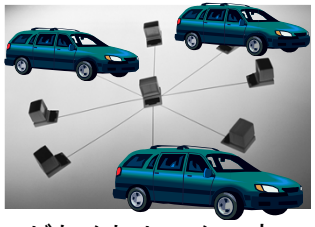
第4期科学技術基本計画の基となる「諮問第11号『科学技術に関する基本政策について』に対する答申」（平成22年12月24日総合科学技術会議決定）

グリーン・イノベーション

省エネ性能向上

ﾌﾟﾗｲﾊﾞｼｰを保護した計測ﾃﾞｰﾀ分析（秘密計算など）

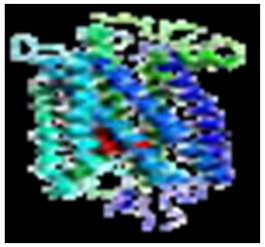
高度交通システム



ｱﾄﾞﾎｯｸﾈｯﾄﾜｰｸの安全性確保

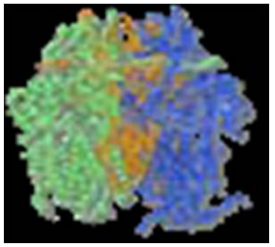
ライフ・イノベーション

ゲノム解析



膨大なｹﾞﾉﾑﾃﾞｰﾀの解析・ｹﾞﾉﾑ情報の復元

タンパク質挙動解析



ｱﾙﾂﾊｲﾏｰ病等の原因物質の振る舞いを解明

成長を支えるプラットフォーム（科学・技術・情報通信）

- ハイパフォーマンス・コンピュータ
- 高度情報セキュリティ基盤
- 超高速ネットワーク
- ・・・

グリーン、ライフなどの社会的イノベーションを支える高度な情報セキュリティ基盤の構築

「国として優先すべき観点」を踏まえた重点分野の選定

現時点において、優先すべき観点は以下と考える。
(1)災害復興
(2)Game Change
(3)科学技術政策との連携

これらの観点を用いると、当面、優先的に推進する研究開発は次のようになる。

重点プロジェクト名称	内容
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	社会インフラを支えている重要システムは、セキュアでディペンダブルな情報システムを実現するべきであり、これらを兼ね備えた情報システム構築技術などを開発する。
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	ニューディペンダビリティを備えた情報システムを構築するために、セキュリティ・ポリシやコンフィグレーションに基づきシステム間の整合性を形式手法等のアプローチにより自動検査する技術などを開発する。
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	ネットワークに障害が発生しても自動的にリカバリーするための仕組みの研究を行う。なお、自己治癒型のネットワークの研究の前提として、ネットワークの仮想化・多様化に係わる基礎研究が必要である。
⑦プライバシ情報の利活用を促進する自己情報コントロール技術	プライバシ情報の積極活用のニーズが高まっているが、機密レベルの考え方は多様である。データの機密性と有効活用のレベルを自己コントロールする技術の研究開発を行う。なお、機密性を確保したままでデータを有効に分析するための秘密計算やデータ匿名化等の基礎研究が必要である。