資料５

# 技術戦略専門委員会報告書（第１次案）

平成 20 年７月

情報セキュリティ政策会議

技術戦略専門委員会

# 目　次

# 1.はじめに

## 1.1.背景と目的

情報セキュリティ政策会議（議長：内閣官房長官）の下に技術戦略専門委員会が設置され、我が国における情報セキュリティに係る研究開発及び技術開発並びにそれらの成果利用の戦略に係る事項について調査検討を行っている。中でも、社会基盤としてのITにおける情報セキュリティ問題、すなわち①急速に拡大するIT利活用に、情報セキュリティ技術の開発が対応できていない。②既存の情報セキュリティ技術の限界を補完する組織・人間系の管理手法とのバランスを欠いているという状況に対する有効な解決策の一つである「グランドチャレンジ型」の研究開発・技術開発の必要性について、当委員会より提言を行い、その具体化に向けたテーマ選定のプロセス及びプロジェクト実施方法等の検討を求めているところである。

当委員会では、このたびグランドチャレンジ検討ワーキンググループを設置し、これらの検討を行うことした。

グランドチャレンジ検討ワーキンググループは、今後我が国として研究開発・技術開発に取り組むべき大規模かつ長期的な研究テーマ、長期的な研究開発の実施方法及び研究開発の推進体制等についての検討を行うものである。

本報告書は、当ワーキンググループの検討内容をまとめることで、今後我が国として取り組むべきものの方向性を探求し、限られた投資の中での効率的・効果的な研究開発・技術開発の実現に資することを目的とするものである。

## 1.2．グランドチャレンジとは

**（科学技術基本計画における情報セキュリティ研究開発の位置づけ）**

我が国における科学技術研究開発に関する基本的な基本計画である、平成18年3月28日に閣議決定された、第3期科学技術基本計画（平成18年度からの5カ年間の計画）には、その三つの理念のうち、理念3として「健康と安全を守る－安心・安全で質の高い生活のできる国の実現」が基本理念として謳われると共に、「情報セキュリティに対する脅威の増大」が理念の背景として示されているなど、情報セキュリティに関する研究開発の重要性は科学技術基本計画においても指摘されているところである。

**（第1次情報セキュリティ基本計画における情報セキュリティ研究開発の位置づけ）**

IT基本法等を踏まえて策定された第1次情報セキュリティ基本計画においては、我が国の国家目標として以下の3つが示されている。

・ 国家目標I－経済大国日本の持続的発展とITの利用・活用－
・ 国家目標II－より良い国民生活の実現とITの利用・活用－

・ 国家目標 III－我が国の安全保障における IT に起因する新たな脅威への対応－
この国家目標の中での情報セキュリティの位置づけは、「経済大国としての我が国を今後も持続的に発展させ、同時に IT を利用・活用したより良い国民生活を実現し、新たな観点からの国家の安全保障を確保しようとする我が国の国家目標の中で、この IT 基盤を、真に依存可能で強固なものにすることが、情報セキュリティの役割である」（第 1 次情報セキュリティ基本計画）とされると共に、「セキュリティ立国」の思想に基づく「情報セキュリティ先進国」の実現（「セキュア・ジャパン」を実現すること）が示されたところである。

これらの国家目標の下で、第 1 次情報セキュリティ基本計画では、まず実現すべき基本目標として、『IT 基本法が求める「IT を安心して利用可能な環境」の構築』が掲げられており、この基本目標を達成するための研究開発に対する方針として、「先進的技術の追求」が示されており、継続的な研究開発への取り組みの重要性が謳われている。先進的技術の追求とは、「急速に拡大するＩＴの利用・活用に対応し、次から次へと発生する新しい情報セキュリティの脅威に、対症療法的ではなく対応するためには、常に最先端の研究開発・技術開発の要素を取り入れた情報セキュリティ対策を推進していくこと」である。

なお、先進的技術の追求に際しては、以下の点が重要とされており、これは今回検討の対象となるグランドチャレンジの研究テーマに対しても重要な観点である。

1） 単一の技術や単一の基盤に依存することのリスクを認知し、その改善に取り組むこと
2） 既存の基盤に対する技術的な解決方法に加え、ビルトイン型の情報セキュリティ機能を持ったそもそもの基盤自体を新たに構築すること

従って、これらの計画等で示された目標や理念等の実現のためには、国としても情報セキュリティに関する研究開発を推進することが必要と考えられる。

**（当委員会が指摘した課題とグランドチャレンジ型研究開発）**

当委員会では、検討の結果を技術戦略専門委員会報告書（2005 年）として取りまとめたが、その中で、社会基盤としての IT における情報セキュリティ問題、すなわち①急速に拡大する IT 利活用に、情報セキュリティ技術の開発が対応できていない。②既存の情報セキュリティ技術の限界を補完する組織・人間系の管理手法とのバランスを欠いている。に対する有効な解決策の一つである「グランドチャレンジ型」の研究開発・技術開発の提言を行ったものである。

【「グランドチャレンジ型」研究開発・技術開発とは】

最近の科学技術研究の問題として、研究領域の細分化、先鋭化が進み、研究実施の目標設定が短期的なものが中心的になったり、他の研究領域との連関性を意識しない研究実施が行われたり、さらに最悪の場合には研究者が研究実施の目的を見失ったりすることが発生している。このような問題を解決するひとつの方策として、10 年程度の長期間にわたる持続的な研究開発を念頭に置き、特定の大目標を設定し、各種要素技術全体の統合開発を行う、「グランドチャレンジ型」の研究開発を設定することが注目されている。

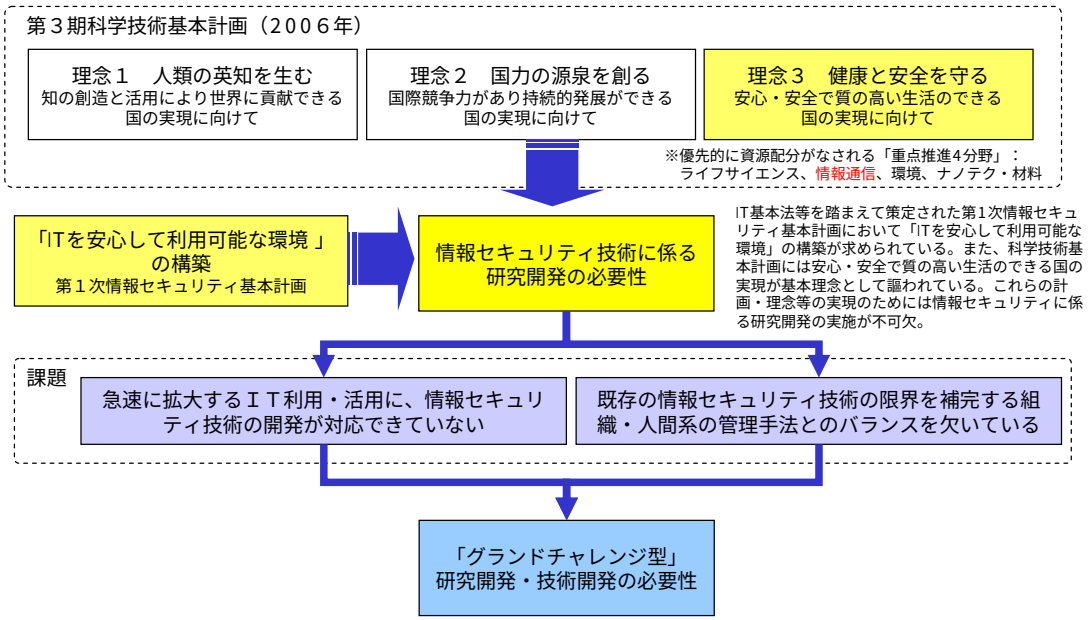
グランドチャレンジ型の研究開発を設定するプロセスでは、まず大目標として何を設定するかが大きな課題となる。この検討プロセスでは、分かりやすく象徴的なターゲットを選定する段階で、長期的な研究を行う意味と、先鋭化した個別研究領域の連関性の再認識、さらには、研究と社会の関係を明確化されることが期待できる。また、目標設定の検討プロセスを継続的に実施することにより、情報セキュリティ技術領域の問題点や新たな研究の方向性等が、より明確になることも期待できる。

さらに、実際にグランドチャレンジ型の研究開発を実施することで、目標が実現されるだけでなく、目標実現の過程で生み出される数多くの副産物が社会展開される効能を期待することができる。さらに、極度に細分化された研究領域を融合し、新たな意味づけを行うことも期待される。

また現在、IT は、我が国の国民生活・経済活動のあらゆる場面において深く利用されるようになったが、IT 社会を支える情報セキュリティ技術そのものは、必ずしも国民生活・経済活動にとって身近な技術とはなっていない。そこでこうしたグランドチャレンジ型の研究開発を推進することにより、国民の関心を高め、ひいては情報セキュリティ技術への投資に対して、幅広い支持を得られることが期待できる。

（出典：技術戦略専門委員会報告書（2005 年））

また、情報セキュリティ対策においては、対症療法的な対応だけでなく、長期的な視野に立ったビルトイン型の研究開発等が重要である。したがって、情報セキュリティ技術の研究開発・技術開発においても、短期的な問題解決はもとより、長期的な視野で抜本的な技術革新等の実現を目指す「グランドチャレンジ型」の研究開発・技術開発が必要と指摘した。




**図表 1　情報セキュリティ分野におけるグランドチャレンジ型研究開発とは**

## 1.3. 調査方法

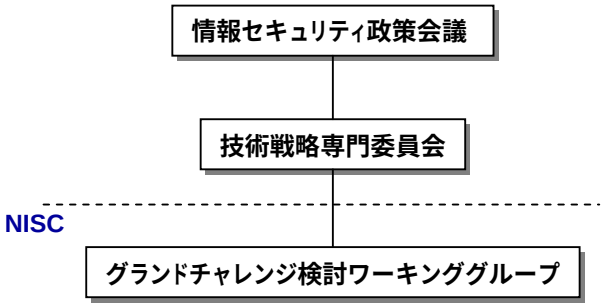
本調査研究は、グランドチャレンジ検討ワーキンググループにおける検討を支援し、そこでの検討結果をとりまとめると共に、ワーキンググループの結論を踏まえ、今後我が国として取り組むべきものの方向性について整理を行うものである。

情報セキュリティに関する大規模で長期的な研究開発（グランドチャレンジ型研究開発）のテーマを検討するにふさわしい専門家からなるワーキンググループを編成し、本調査の結節毎に、3 回の会合を開催して意見を聴取した。

### 1.3.1. グランドチャレンジ検討ワーキンググループ

このため、有識者及び内閣官房情報セキュリティセンターの職員からなるグランドチャレンジ検討ワーキンググループを設置し検討を行った。

グランドチャレンジ検討ワーキンググループは技術戦略専門委員会とも密接に連携しつつ検討を行った。




**図表 2 グランドチャレンジ検討ワーキンググループの位置づけ**

### 1.3.2.検討の経緯

第 1 回～第 3 回のワーキンググループを開催した（図表 3）。

**図表 3　検討の経緯**

| WG | 議題 |
|---|---|
| 第 1 回 | ・我が国政府における研究開発の動向<br>・WG における議論の方向性について |
| 第 2 回 | ・グランドチャレンジに関する検討 |
| 第 3 回 | ・中間報告書について<br>・グランドチャレンジテーマについて |

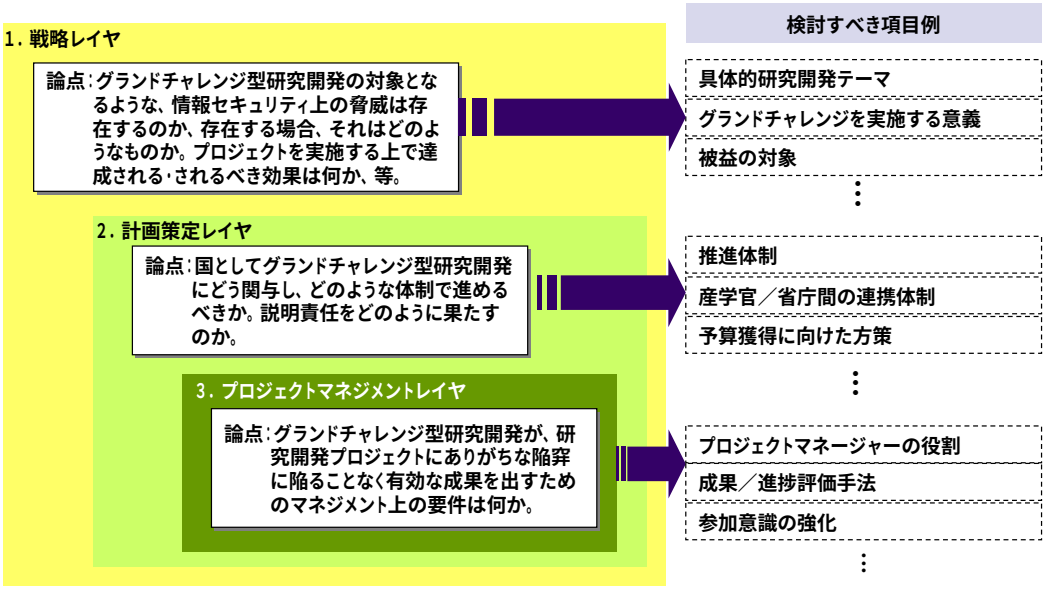
検討に際しては、3 つの論点を設定し、それぞれ検討を行った（図表 4）。

論点 1 としては、戦略レイヤとして、グランドチャレンジ型研究開発の対象となるような、情報セキュリティ上の脅威は存在するのか、存在する場合、それはどのようなものか。プロジェクトを実施する上で達成される・されるべき効果は何か、等の観点から検討を行った。具体的には、グランドチャレンジを実施する意義、具体的な研究開発テーマ、グランドチャレンジを実施することによる被益の対象、などについて検討を行った。

論点 2 としては、計画策定レイヤとして、国としてグランドチャレンジ型研究開発にどう関与し、どのような体制で進めるべきか、説明責任をどのように果たすのかといった観点から検討を行った。具体的には、推進体制、産学官/省庁間の連携体制、予算獲得に向けた方策、などについて検討を行った。

論点 3 としては、プロジェクトマネジメントレイヤとして、グランドチャレンジ型研究開発が、研究開発プロジェクトにありがちな陥穽に陥ることなく有効な成果を出すためのマネジメント上の要件は何か、といった観点から検討を行った。具体的には、プロ

ジェクトマネージャの役割、成果／進捗評価手法、参加意識の強化などについて検討を行った。




**図表 4　検討の方法**

# 2.グランドチャレンジ型研究開発・技術開発

## 2.1.グランドチャレンジ型研究開発・技術開発に向けた戦略

グランドチャレンジ型研究開発・技術開発の実現に向けた戦略的視点として、グランドチャレンジ型研究開発の対象となるような、情報セキュリティ上の脅威は存在するのか、存在する場合、それはどのようなものか。プロジェクトを実施する上で達成される効果、あるいは達成されるべき効果は何か、等の観点から検討を行った。具体的には、グランドチャレンジを実施する意義、具体的な研究開発テーマ、グランドチャレンジを実施することによる被益の対象、などについて検討を行った。

### 2.1.1.グランドチャレンジ型研究開発の対象とする脅威

まず、グランドチャレンジ型研究開発の対象となるような、情報セキュリティ上の脅威は存在するのかについて、3 つの立場が存在する。

#### (1)大きな脅威にさらされているとする立場

情報セキュリティに関して大きな脅威にさらされているとする立場とは、様々な対策や制度等が講じられた現在においても、引き続き我が国は情報セキュリティに関する脅威にさらされているという立場である。具体的な脅威としては意図的な要因と非意図的な要因が存在する。

各種統計によれば、ウイルス感染の件数は全体として減少傾向にあるものの、一方でボット等による見えない感染が広がると共に、ウイルス感染による業務停止等の間接被害も引き続き大きい。またボット等に感染した PC が大きな原因となっているスパムによる経済的損失も非常に大きくなってきている。ここでの経済的損失には、スパムを削除するための人件費（生産性の低下）や、スパムメールを処理するために余計にかかる情報システムインフラ（ネットワーク、メールサーバー等）の整備コストなどが含まれる。政府機関等に対する標的方攻撃による国家機密漏洩のリスクや、企業の営業秘密の漏洩による経済安全保障上の脅威などがある。また、これらの脅威に対抗するためのセキュリティ対策コスト（管理コストや生産性の低下も含む）の増大も無視できないレベルにある（以上、意図的要因）。さらには近年、ソフトウエアのバグ、ハードウエア故障、操作ミス等によるシステムの停止が社会に大きな影響を与えている（非意図的要因）。

以上の脅威をまとめると以下のようになる。

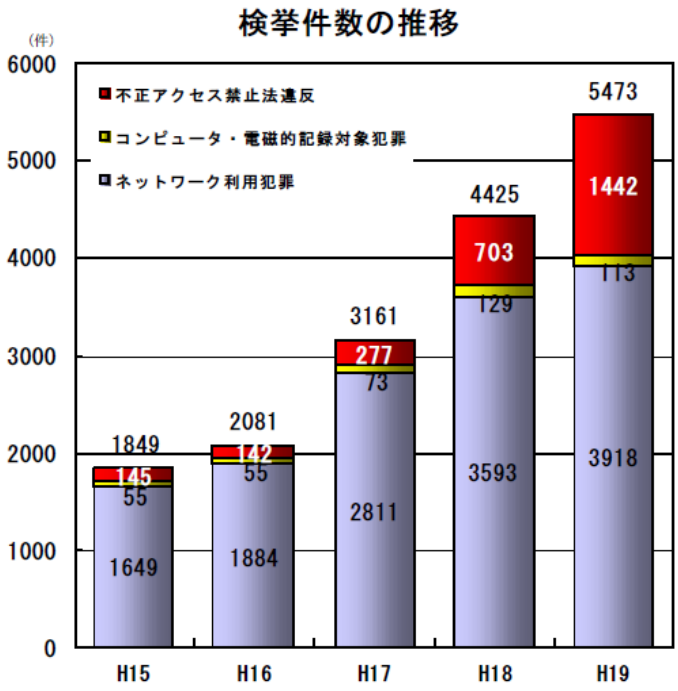
[意図的要因]

- ウイルス感染による直接被害と間接被害が大

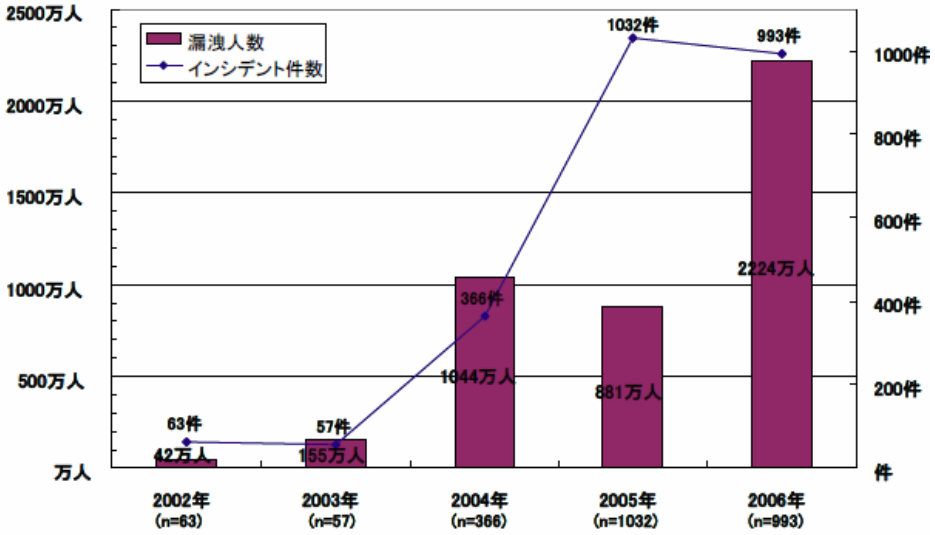
- スパムによる経済的損失（スパム削除コスト、インフラコスト）大
- 標的型攻撃による国家機密等の漏洩
- セキュリティ対策コスト（管理コスト、生産性低下も含む）の増大

[非意図的要因]

- ソフトウエアのバグ、ハードウエア故障、操作ミス等による影響の増加




**図表 5　サイバー犯罪の検挙件数（出典　警察庁）**




**図表 6　個人情報漏洩人数とインシデント件数（出典 JNSA）**

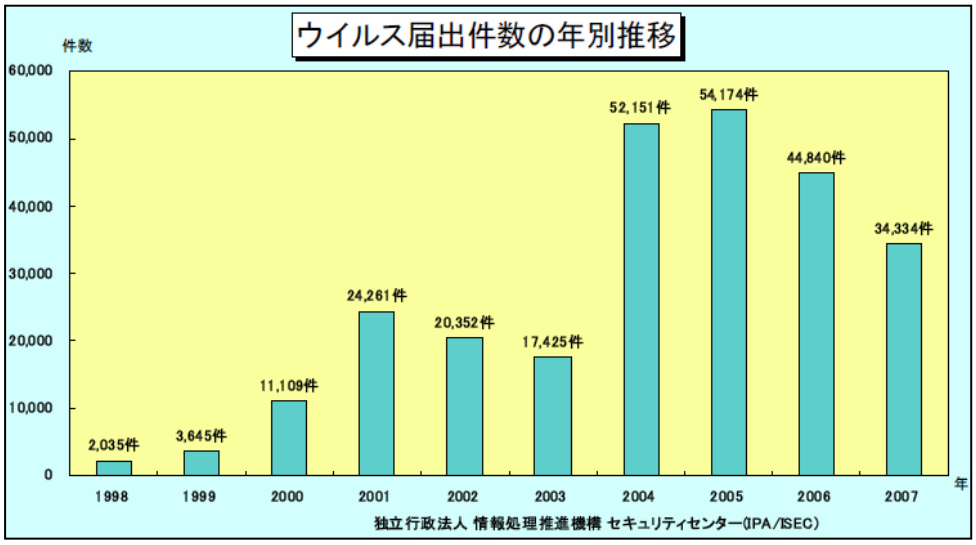
### (2)脅威はそれほど大きくないとする立場

情報セキュリティに関してはそれほど大きな脅威にさらされていないとする立場とは、様々な対策や制度等が講じられたことにより、被害の件数も減ってきており、また実質的な被害も少なくなってきているとする立場である。

例えば、各種統計によればウイルス感染数は 2005 年頃をピークに、ソフトウエア脆弱性対策、ウイルス対策等の進展により減少傾向にある。また、ボット等の感染数が増加したとしても、ボットは感染した PC 自体にはそれほど大きな被害をもたらさない可能性がある。また最近のスパム被害については、フィルタリング技術等により実際の被害は最小に押さえられている可能性もある。

以上の脅威をまとめると以下のようになる。

- ウイルス感染は減少傾向にあり、また感染しても実質的被害は少ない可能性
- フィルタリングによりスパム被害は抑止できている可能性




**図表 7　ウイルス届出件数の年別推移（出典　独立行政法人情報処理推進機構）**

### (3)脅威を評価するに十分な情報がないとする立場

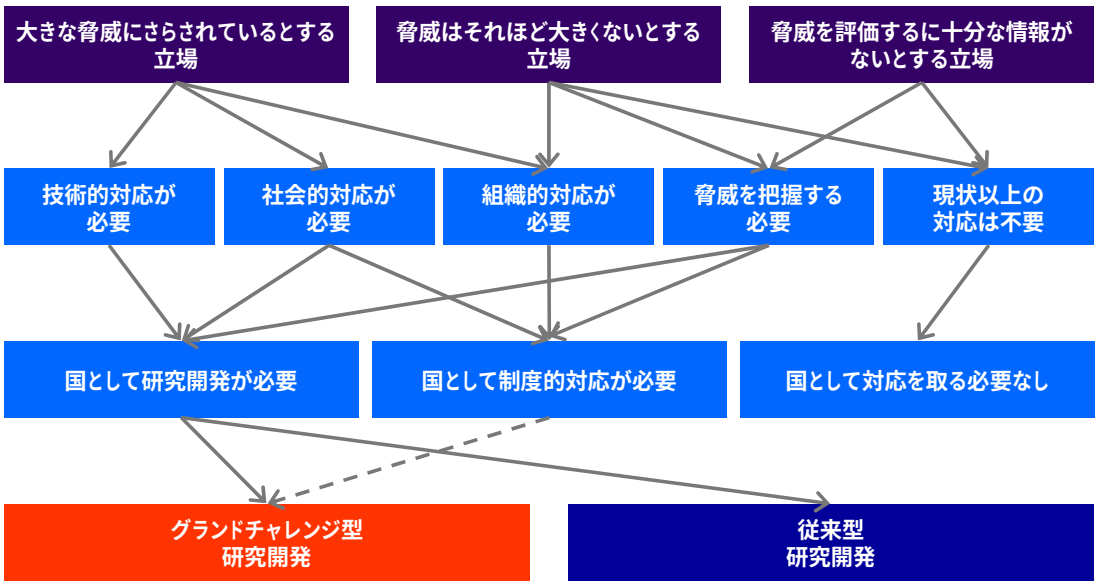
情報セキュリティに関して、そもそも脅威を評価するのに十分な情報が無いとする立場とは、脅威を評価するのに必要な統計情報や観測情報が十分に収集分析されていないため、脅威の評価が出来ないというものである。

- 標的型攻撃については実態が不明確
- 経済的被害の実態については十分な情報がないのではないか
- 経済合理的な対策水準が不明確（すでに過大な投資を行っている可能性）

### 2.1.2.グランドチャレンジ型研究開発の意義・目的

グランドチャレンジ型研究開発の対象とする脅威を、(1)大きな脅威にさらされているとする立場、(2)脅威はそれほど大きくないとする立場、(3)脅威を評価するに十分な情報がないとする立場、として整理した場合、それぞれについて、1)技術的対応が必要な場合、2)社会的対応が必要な場合、3)組織的対応が必要な場合、4)脅威を把握する必要がある場合、5)現状以上の対応は不要な場合に対応方針を分けることが出来る。

さらに、それぞれの対応方針が定まったところで、国としての対応方針として、国として研究開発が必要な場合と、国として制度的対応が必要な場合と、国として対応をとる必要がない場合に分けることが出来る。その上で、国として研究開発が必要な場合について、グランドチャレンジ型研究開発を行うのか、従来型研究開発により行うのかが問われることになる。




**図表 8　グランドチャレンジの意義・目的**

以上により、グランドチャレンジ型研究開発を行う意義について整理すると以下のように整理することができる。

グランドチャレンジ型研究開発を行うのは主に、1）顕在化した脅威に対して技術的、社会的な対応が必要な場合であって、国として研究開発を行う場合もしくは、2）脅威を評価するに十分な情報がない場合に、脅威を把握するため国として研究開発を行う場合、でかつ従来型研究開発に適さないテーマの場合である。

### 2.1.3.グランドチャレンジ型研究開発の目標

次に、グランドチャレンジ型研究開発の目標の例について検討を行う。

グランドチャレンジ型研究開発は、10 年程度の長期間にわたる持続的な研究開発であると想定すると、その目標としては 10 年後まで有効な目標を設定する必要がある。また、グランドチャレンジ型研究開発とは、要素技術の開発ではなく、特定の大目標を設定し、各種要素技術全体を統合開発することを考慮すると、様々な要素技術を統合しなければ達成困難な目標を設定することが望ましい。

これらのことを考慮すると、例えばグランドチャレンジ型研究開発の目標の例としては以下のようなものが想定される。

**(1)実質被害ゼロ**

10 年後に、ユーザの被害を実質的に 0 にするための研究開発を実施する。ここで「実質的 0」とは、事故を 0 にするという意味ではなく、事故が発生してもユーザに被害が及ばないような、重層的な技術的対策や、制度的対策との組み合わせにより達成する。

**(2)情報セキュリティに係る社会的メカニズムの確立**

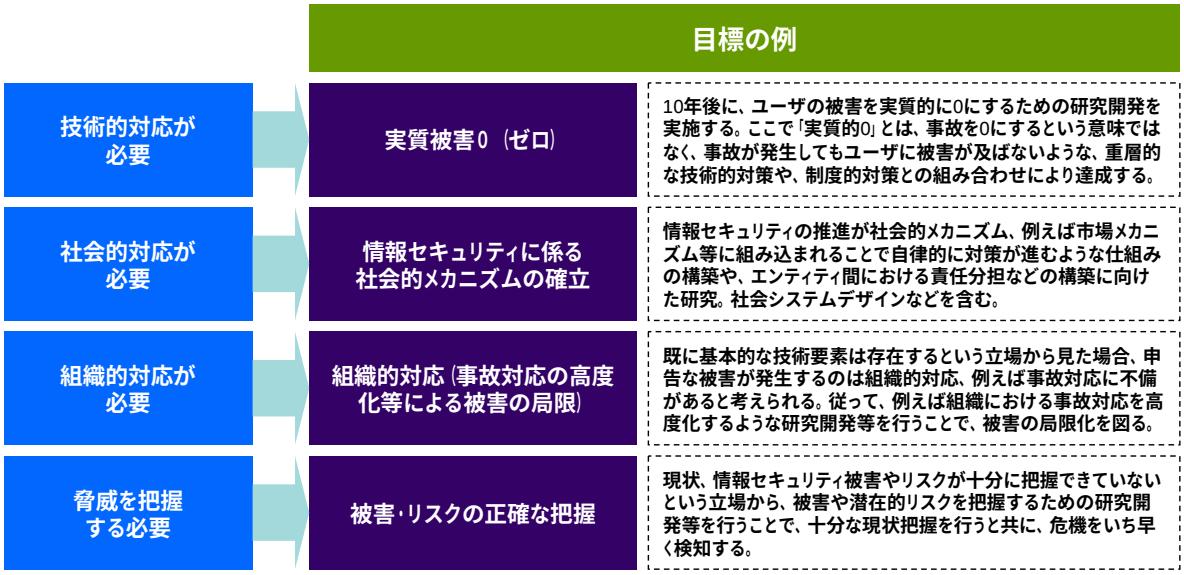
情報セキュリティの推進が社会的メカニズム、例えば市場メカニズム等に組み込まれることで自律的に対策が進むような仕組みの構築や、エンティティ間における責任分担などの構築に向けた研究。社会システムデザインなどを含む。

**(3)組織的対応（事故対応の高度化等による被害の局限）**

既に基本的な技術要素は存在するという立場から見た場合、深刻な被害が発生するのは組織的対応、例えば事故対応に不備があると考えられる。従って、例えば組織における事故対応を高度化するような研究開発等を行うことで、被害の局限化を図る。

**(4)被害・リスクの正確な把握**

現状、情報セキュリティ被害やリスクが十分に把握できていないという立場から、被害や潜在的リスクを把握するための研究開発等を行うことで、十分な現状把握を行うと共に、危機をいち早く検知する。

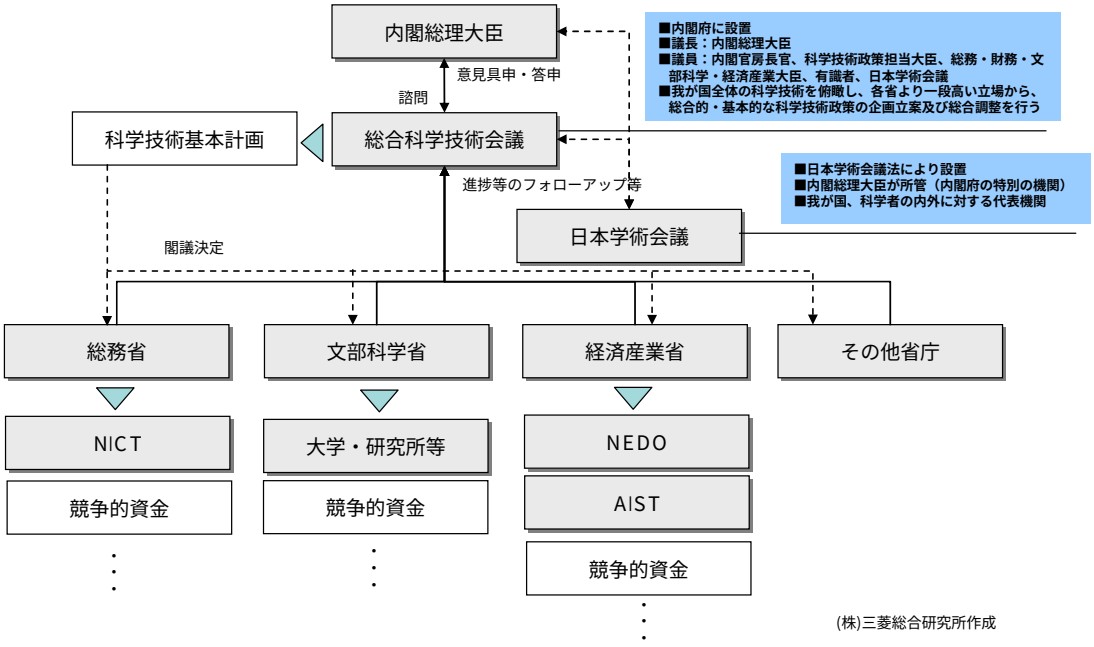



**図表 9　グランドチャレンジの目標の例**

## 2.2.研究開発の推進体制

グランドチャレンジ型研究開発・技術開発の実現に向けた計画策定の視点より、グランドチャレンジ型研究開発を推進するに際して、適切と考えられる最適な資金配分を促進するための枠組み構築方法等について検討を行った。

資金配分について検討する前に、現状の資金配分スキームについて概観する（図表10）。




**図表 10　情報セキュリティに関する研究開発予算施行体制**

我が国においては、内閣総理大臣を議長とし、有識者等からなる総合科学技術会議が設置されており、我が国全体の科学技術を俯瞰し、各省より一段高い立場から、総合的・基本的な科学技術政策の企画立案及び総合調整を行うこととされている。また総合科学技術会議は科学技術基本計画を策定するなど、我が国の科学技術関連政策に大きな影響を持っている。

一方で、総務省、文部科学省、経済産業省等は科学技術基本計画等に基づき、各省独自の研究開発プロジェクトを運営している。我が国において特徴的なのは、科学技術基本計画はあくまでも基本的な方針を示すにとどまり、個別具体的な研究開発プログラムに関して、各省の独立性が高いことである。

従って、内閣官房が主導してグランドチャレンジ型研究開発を進めようとした場合、以下の三種類の方法が主に考えられる。

1. 内閣官房自体の研究開発プロジェクトとして実施する方法
2. 総合科学技術会議の持つ総合推進調整を行うための経費を活用する方法
3. 科学技術基本計画等の改訂等を通じて各省庁のプロジェクトとして実施する方法

このうち、1 については設置法上の関係等より、内閣官房が直接研究開発を行うことは困難であり、また、3 については各省庁の独立性の高さより実際には困難が伴う。従って 2 の総合調整を行うための経費（科学技術振興調整費）を利用することが当面は妥当である。なお、科学技術振興調整費とは「総合科学技術会議の方針に沿って科学技術の振興に必要な重要事項の総合推進調整を行うための経費であり、以下の施策であって、各府省の施策の先鞭となるもの、各府省毎の施策では対応できていない境界的なもの、複数機関の協力により相乗効果が期待されるもの、機動的に取り組むべきもの等で、政府誘導効果が高いものに活用されるものである。（文部科学省 HP より）」とされている。

## 2.3.長期的な研究開発の実施方法

グランドチャレンジ型研究開発・技術開発の実現に向けたプロジェクトマネジメントの視点より、グランドチャレンジ型研究開発が、研究開発プロジェクトにありがちな陥穽に陥ることなく有効な成果を出すためのマネジメント上の要件は何か、といった観点から検討を行った。具体的には、以下の項目に関して検討を行った。

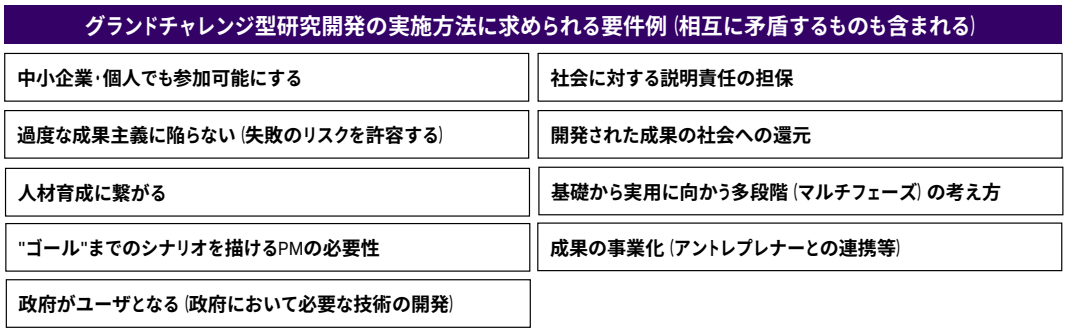
- プログラムマネージャー制等の検討
- プロジェクト評価手法及び体制の確立
- 開発予算（競争的資金等の活用を含む）の確保手法
- 長期間にわたるプロジェクト実施が可能な新たな制度の検討
- 多岐にわたる各種要素技術の統合管理手法

グランドチャレンジ型研究開発の実施方法については、大きく分けて以下の 4 種類が

ある。

- ゴール FIX チャレンジ型
- 大規模プロジェクト型
- 細分配型
- 個別課題別公募型

以下、それぞれについて、プロジェクト管理・評価と PM 等の役割、グランドチャレンジ型研究開発実施上の課題について検討を行う。




**図表 11　グランドチャレンジ型研究開発の実施方法に求められる要件例**

### (1)ゴール FIX チャレンジ型

特定の目標を設定し、期限内にその目標を達成したものに、何らかのクライテリアにより順位を設定し、優勝者もしくは上位入賞者に賞金等を支出する。類似の例としては米国 DARPA グランドチャレンジなどがある。

プロジェクト管理・評価と PM 等の役割であるが、委員会形式などにより、特定の目標（ゴール）を設定する。PM は個々の研究開発プロセスを管理する必要は無いが、シナリオライティング能力や、イベント企画などの能力が必要となる。

課題としては、国の予算制度の中で、賞金を支出することは一般的に困難である。制度設計によっては、一般競争入札（総合評価落札）の一種とみなされうる可能性がある。

### (2)大規模プロジェクト型

特定の目標・テーマを設定し、目標の実現に向けて、コンソーシアムないし技術研究組合などに対して、委託研究費もしくは補助金などを支給する。類似の例としては、経済産業省の半導体 MIRAI プロジェクトなどがある。

プロジェクト管理・評価と PM 等の役割であるが、単独ないし少数のプロジェクトマネージャによりプロジェクト全体の進捗管理等を行う。プロジェクトの評価は特定の目標・テーマが達成されたか否かにより行う。

課題としては、多数のバックグラウンドを持つ要員を束ねる必要があるため、マネジ

メントがうまく行かない場合、”烏合の衆”となりかねない危険がある。また、特定の団体に対する随意契約は困難である。

### (3)細分配型

ある分野を設定し、そこで必要になる要素技術の研究開発等に、広く資金を分配する。一件当たりの助成金額は少なくなる。類似の制度としては、文部科学省の科学研究費補助金などがある。

プロジェクト管理・評価と PM 等の役割であるが、多数の応募者の中から研究実施者を選定するための事務局機能が重要となる。件数が多いことから、プロジェクトの進捗管理は詳細に行わず、得られた成果（論文、特許）により評価を行う。

課題としては、適切な分野の設定を行わないと、単なるばら撒きとの批判を免れなくなる。また、”グランドチャレンジ”としてのまとまり間を出すことは困難なことが挙げられる。

### (4)個別課題別公募型

ある分野を設定し、特定の課題、例えば要素技術開発、国際標準化、中小企業育成、人材育成、コミュニティ形成などに対して、公募等により実施者を募集し、委託研究費もしくは補助金等の形式で資金を提供。多くの制度がここに該当する。

プロジェクト管理・評価と PM 等の役割及び課題については、大規模プロジェクト型と細分配型の中間の性質を持つ。

| | | 概要 | プロジェクト管理・評価とPM等の役割 | 課題 |
|---|---|---|---|---|
| ビジョナリィ・ゴール型 | ゴールFIXチャレンジ型 | 特定の目標を設定し、期限内にその目標を達成したものに、何らかのクライテリアにより順位を設定し、優勝者もしくは上位入賞者に賞金等を支出する。類似の例としては米国DARPAグランドチャレンジなどがある。 | 委員会形式などにより、特定の目標（ゴール）を設定。PMは個々の研究開発プロセスを管理する必要は無いが、シナリオライティング能力や、イベント企画などの能力が必要となる。 | 国の予算制度の中で、賞金を支出することは一般的に困難である。制度設計によっては、一般競争入札（総合評価落札）の一種とみなされうる可能性がある。 |
| | 大規模プロジェクト型 | 特定の目標・テーマを設定し、目標の実現に向けて、コンソーシアムないし技術研究組合などに対して、委託研究費もしくは補助金などを支給する。類似の例としては、経済産業省の半導体MIRAIプロジェクトなどがある。 | 単独ないし少数のプロジェクトマネージャによりプロジェクト全体の進捗管理等を行う。プロジェクトの評価は特定の目標・テーマが達成されたか否かにより行う。 | 多数のバックグラウンドを持つ要員を束ねる必要があるため、マネジメントがうまく行かない場合、”烏合の衆”となりかねない危険がある。また、特定の団体に対する随意契約は困難である。 |
| テクニカル・コンポーネント型 | 細分配型 | ある分野を設定し、そこで必要になる要素技術の研究開発等に、広く資金を分配する。一件当たりの助成金額は少なくなる。類似の制度としては、文部科学省の科学研究費補助金などがある。 | 多数の応募者の中から研究実施者を選定するための事務局機能が重要となる。件数が多いことから、プロジェクトの進捗管理は詳細に行わず、得られた成果（論文、特許）により評価を行う。 | 適切な分野の設定を行わないと、単なるばら撒きとの批判を免れなくなる。また、”グランドチャレンジ”としてのまとまり間を出すことは困難。 |
| | 個別課題別公募型 | ある分野を設定し、特定の課題、例えば要素技術開発、国際標準化、中小企業育成、人材育成、コミュニティ形成などに対して、公募等により実施者を募集し、委託研究費もしくは補助金等の形式で資金を提供。多くの制度がここに該当する。 | プロジェクト管理等としては、大規模プロジェクト型と細分配型の中間の性質を持つ。 | 課題としては、大規模プロジェクト型と細分配型の両方の性質を持つ。 |

**図表 12　グランドチャレンジ型研究開発の実施方法**

## 2.4.具体的研究開発テーマ

以上の検討を踏まえ、具体的な研究開発テーマについて検討を行う。なお、具体的研究開発テーマの詳細は付録に示した。

2.1.3 の通り目標を定めた場合、グランドチャレンジ型研究開発テーマは以下のようなものが考えられる（図表 13）。

| | |
|---|---|
| 実質被害0（ゼロ） | ・エンドユーザでも複雑な設定等を行うことなく、安全にITを利用可能なユーザブルセキュリティ技術や、自身が安全な環境にいるか否かを直感的に把握可能なユーザーインターフェース技術等<br>・現在大きな社会的・経済的な損出となっている迷惑メールについて、実質的にその被害を0にするような総合的な技術の開発。（スパム0（ゼロ））<br>・絶対安全なソフトウェアの構築技術の開発。Trustworthyシステム技術、セキュアプログラミング技術。スキルの高く無い開発者でも安全なアプリケーションを開発できるような、プログラム自動構成技術や、アプリの安全性を簡単に検証できる技術等。 |
| 情報セキュリティに係る社会的メカニズムの確立 | ・不確定性（リスク）を許容する社会のあり方に向けた研究。<br>・未成年や高齢者などの情報弱者向けに、いわゆるThe Internetから隔離されることで安全なネット環境を実現する技術もしくは社会的な仕組み。（あっInternet）<br>・情報セキュリティに関する研究・社会実験を促進するために、情報セキュリティに関わる社会的制約を受けない情報セキュリティ特区や、大規模なアウトブレーク等を模擬することのできるセキュリティテストベッドの整備。<br>・企業・個人等を含む社会全体が蒙っている被害等を適宜把握するための手法に関する研究。もしくはこのような情報を集約・分析・提供する体制の整備。 |
| 組織的対応（事故対応の高度化等による被害の局限） | ・企業内におけるインシデントハンドリングを支援する技術の開発。<br>・情報セキュリティ投資の投資対効果に係る研究開発。 |
| 被害・リスクの正確な把握 | ・インターネットが曝されている脅威・危険度をリアルタイムで把握する技術の開発。<br>・企業・個人等を含む社会全体が蒙っている被害等を適宜把握するための手法に関する研究。もしくはこのような情報を集約分析する体制の整備。（再掲）<br>・様々な組織が収集している観測データを共有し、あるいは統合・分析・提供するための技術の開発。 |

**図表 13　グランドチャレンジ型研究開発のテーマ例（目的別整理）**

一方で、グランドチャレンジ型研究開発テーマについて、目標別の整理ではなく、研究開発の射程（長期（10 年）・短期（5 年））、粒度（複合・要素）の 2 軸、計 4 象限で整理することも出来る。ここで、射程及び粒度については以下のように定義する。

射程－短期：

- 既に顕在化しており、喫緊の対応が求められる課題

射程－長期：

- 現在は顕在化していないが、今後想定される脅威への対応を想定した課題（要素技術としては既に存在しているものも含む）
- 概ね１０年後に解決されることが期待される課題

粒度－複合（大規模）：

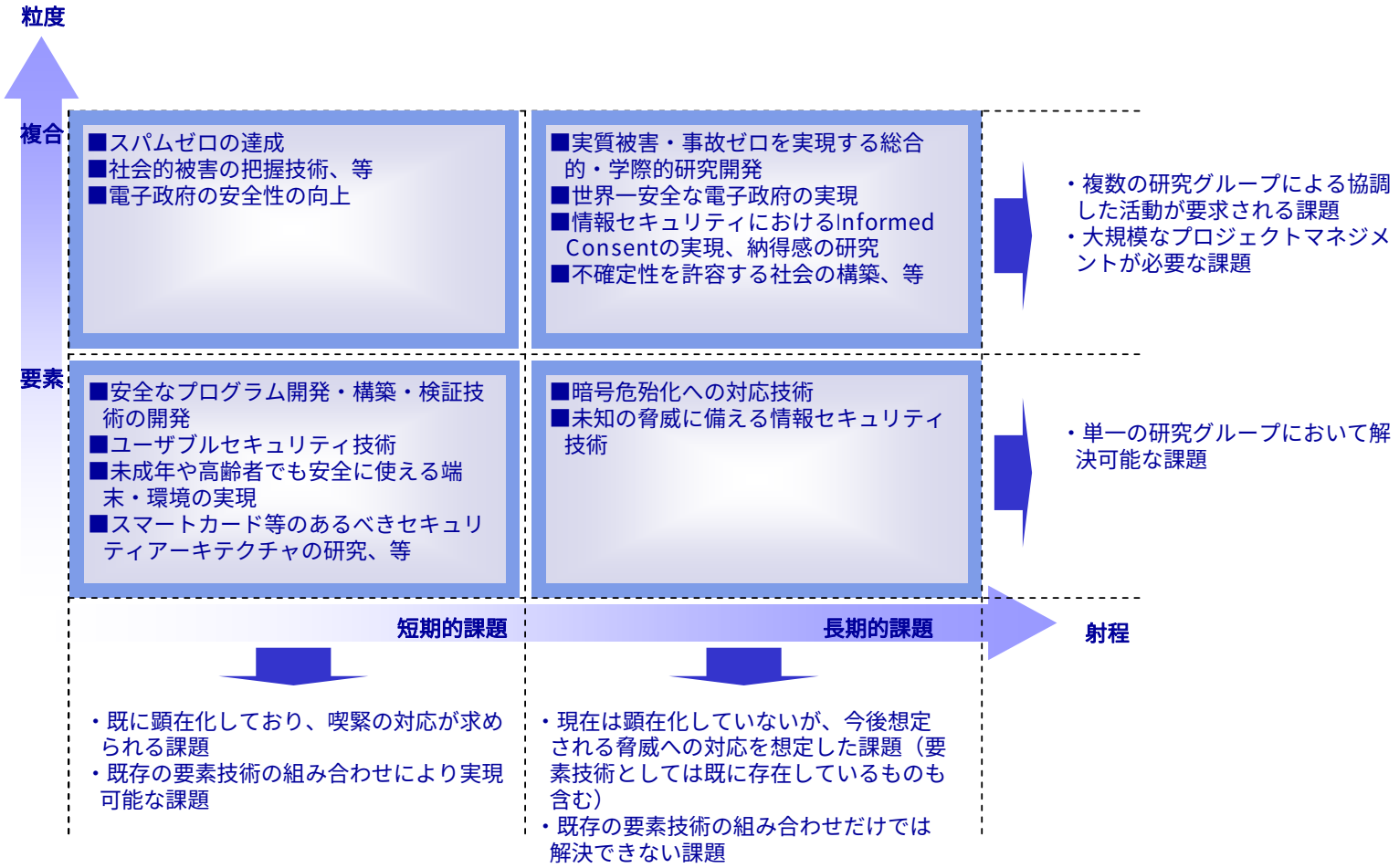
- 既存の要素技術の組み合わせだけでは解決できない課題
- 複数の研究グループによる協調した活動が要求される課題

・ 大規模なプロジェクトマネジメントが必要な課題

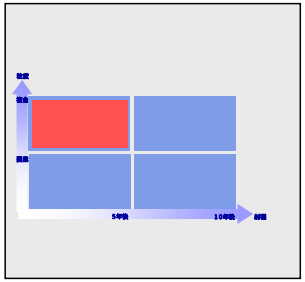
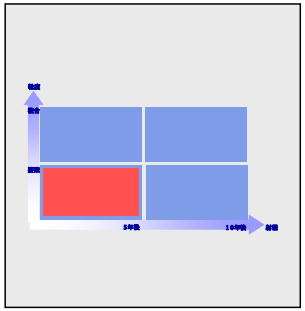
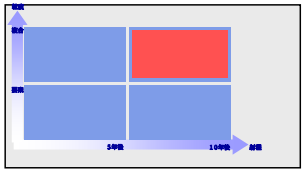
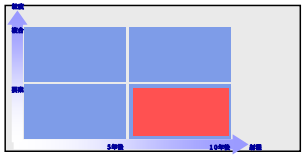
粒度－要素（小規模）：

・ 既存の要素技術の組み合わせにより実現可能な課題
・ 単一の研究グループにおいて解決可能な課題

以上のように定義した場合、グランドチャレンジ型研究開発は以下のように整理できる（図表 14・図表 15）。




**図表 14　グランドチャレンジ型研究開発のテーマ例（属性別整理）**

| | | | |
|---|---|---|---|
| 短期 | 大規模 |  | ・電子政府の積極展開に必要なセキュリティ戦略を詳細に立案実行し、世界一安全な電子政府を実現するための研究開発。<br>・情報システム等の安全性についてユーザが事前に納得して利用できるような、Informed Consentを情報セキュリティにおいて実現するための研究開発。<br>・現在大きな社会的・経済的な損出となっている迷惑メールについて、その発生を抑止すると共に、発生した迷惑メールについてもユーザの負担なしに排除できるような技術・制度の研究開発。（スパム・ゼロ）<br>・企業・個人等を含む社会全体が蒙っている被害等を適宜把握するための手法に関する研究。もしくはこのような情報を集約・分析・提供する体制の整備。 |
| | 小規模 |  | ・エンドユーザでも複雑な設定等を行うことなく、安全にITを利用可能なユーザブルセキュリティ技術や、自身が安全な環境にいるか否かを直感的に把握可能なユーザーインターフェース技術等<br>・安全なソフトウェアの構築技術の開発。Trustworthyシステム技術、セキュアプログラミング技術。スキルの高く無い開発者でも安全なアプリケーションを開発できるような、プログラム自動構成技術や、アプリの安全性を簡単に検証できる技術等。<br>・未成年や高齢者などの情報弱者向けに、安心して使える端末や、Internetから一部隔離することで安全なネット環境を実現する技術もしくは社会的な仕組み。<br>・情報家電、電子私書箱、スマートカード等の情報セキュリティのあるべき姿を示し実現していく研究開発。 |
| 長期 | 大規模 |  | ・情報セキュリティ事故を限りなくゼロにする、あるいは事故が発生しても実質被害につながらないような仕組みを実現するための研究。<br>・不確定性（リスク）を許容する社会のあり方に向けた研究。 |
| | 小規模 |  | ・暗号の危殆化への対応、きめ細かく課題の解決法やスケジューリング、危機管理方策を立案実行する仕組みの研究。<br>・未知の脅威に対する検出・防御技術の研究開発。 |

**図表 15　グランドチャレンジ型研究開発のテーマ例（属性別整理（２））**

# 3.公的研究資金の投入方策等に関する検討・考察

情報セキュリティ技術に関する研究開発・技術開発に対して行われる、我が国の公的研究資金の投入方策等に関して検討・考察を行った。

- 長期的目標に対する研究開発・技術開発の促進のため、公的研究資金を重点的に投入する方策についての検討
- 短期的目標設定のなされている研究開発･技術開発の投資バランスの改善検討(過少投資、過大投資が発生しない投資ポートフォリオのあり方についての検討)
- 萌芽的研究開発への投資強化への検討

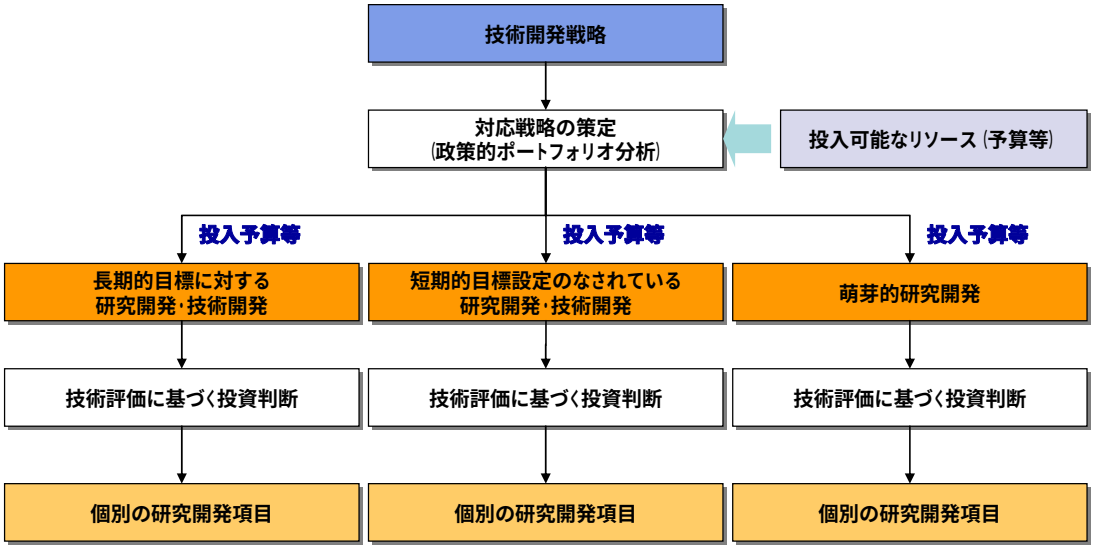
## 3.1.公的研究資金の投入方策等に関する検討

### 3.1.1.投資ポートフォリオのあり方

投資ポートフォリオのあり方については、図表 16に示すようなフレームが考えられる。

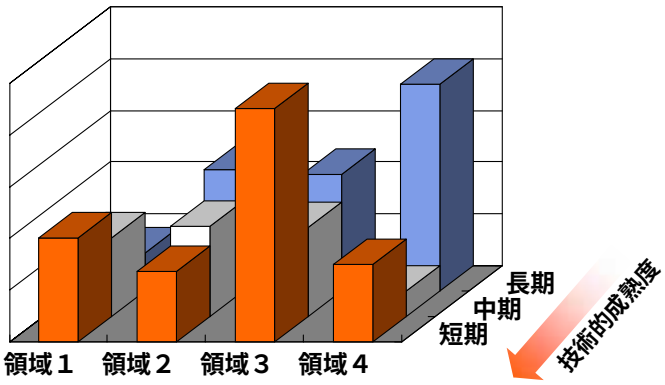
第一段階として、情報セキュリティ研究開発に関する技術開発戦略を策定し、国として投入可能なリソース（予算等）を入力として、分野毎、例えば、長期・短期・萌芽的研究分野のいずれにどの程度の割合でリソースを分配することが適当かを判断する。

第二段階として、それぞれの分野（例：萌芽的研究開発）の中で、具体的にどの案件（テーマ）に対して資金を投入するかを、技術評価に基づいて投資判断を行う。これにより個別の研究開発項目をどのように選定するかについてのポートフォリオを作成することができる。




**図表 16　投資ポートフォリオに関する考え方**

第一段階の対応戦略の策定に際しては、各領域毎のポートフォリオに、その成熟度を評価軸として加え、長期的な観点から最適な投資領域の設定を行うことも考えられる（図表 17）。



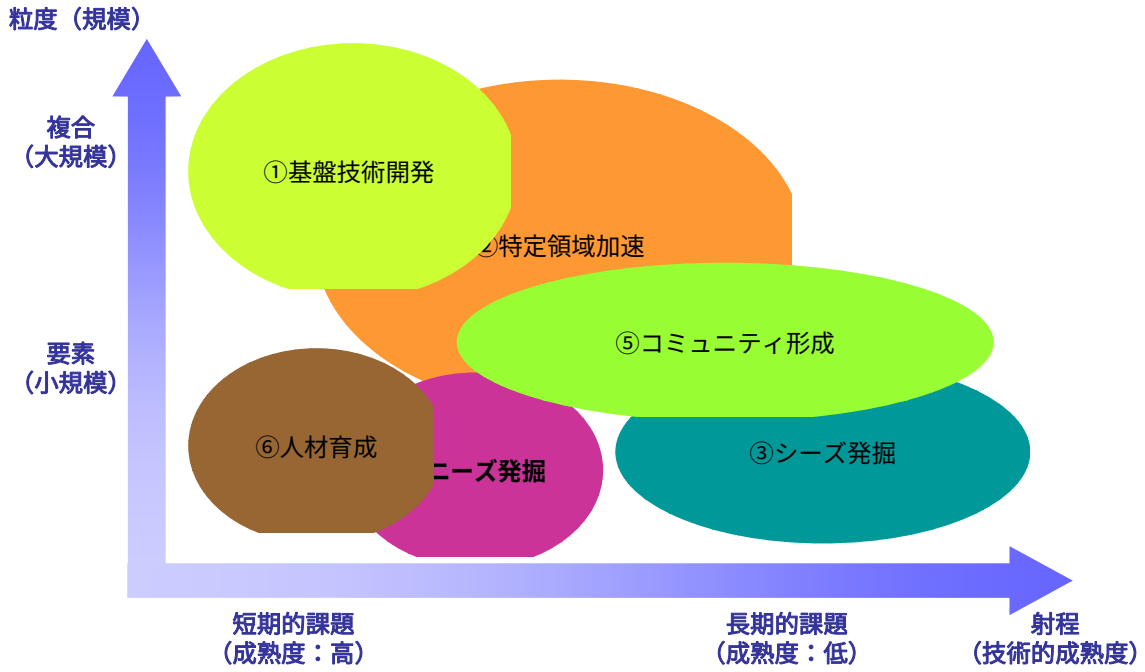

**図表 17　技術的成熟度を加味した新しいポートフォリオのあり方**

また、図表 16では、分野として長期・短期・萌芽的研究という分類を取ったが、それ以外にも目的別の分類を行うことも考えられる。具体的な目的の例としては、以下のようなものが考えられる。

① 基盤技術開発：波及効果の大きい基盤技術について、その技術を確立することを目的としたもの。
② 特定領域加速：特定の研究領域について政策的意図から研究を加速するものであり、比較的狭い研究領域の深堀を目的としたものと、実用化に近い分野に大規模な投資を行うことで、当該分野の産業化等を目的としたもの等がある。いわゆる狭義のグランドチャレンジはここに分類される。
③ シーズ発掘：新しい技術的シーズを発掘することを目的としたもの。
④ ニーズ発掘：新しい社会的ニーズ等の発掘を目的としたもの。新規性よりも実用性などが重視される。
⑤ コミュニティ形成：複数の研究主体が連携して研究を行うことにより新しいコミュニティの形成を期待するもの。具体的には産官学の連携や、国際連携、あるいは分野を跨いだ学際的な連携などがある。
⑥ 人材育成：研究者の育成を目的としたもの。具体的には若手研究者や国際研究者の育成など。

この場合は、分野毎に技術的成熟度がほぼ対応しており、例えば、①基盤技術開発は成熟度の高いもの（短期）であり、③シーズ発掘は成熟度の低いものと捉えることができる。なお、③シーズ発掘は、諸外国では長期的研究開発分野として捉えられることが多いが、我が国においては研究が失敗するリスクが高いことから、短期的研究開発分野

として扱われる場合があることに留意する必要がある。これらの関係を図示したものが**図表 18である。**




**図表 18　技術開発分野（目的）と技術的成熟度**

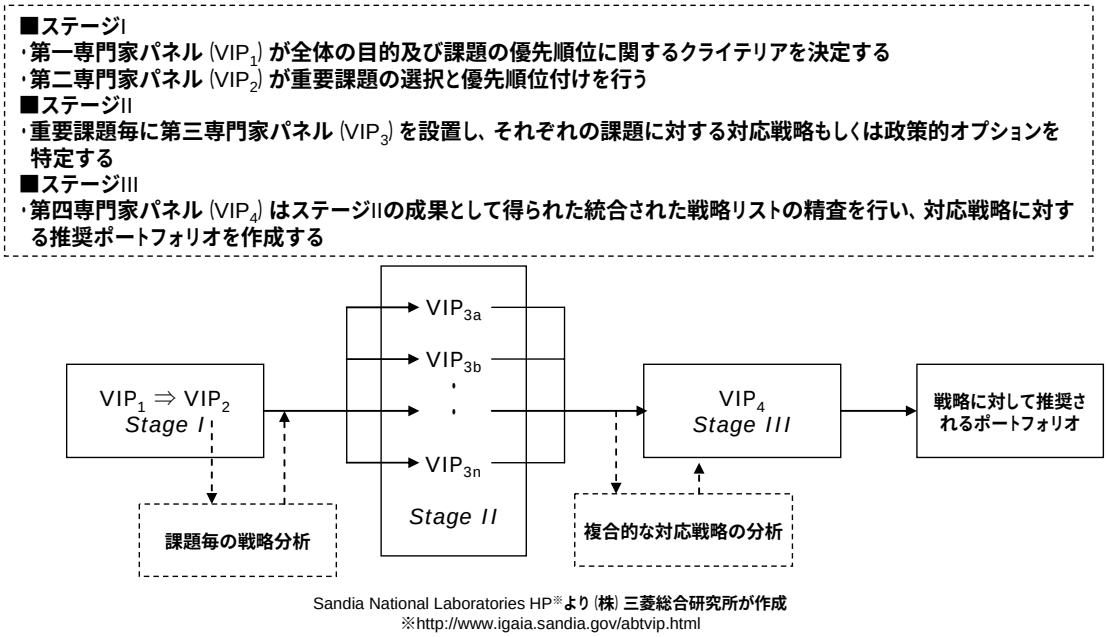
参考までに、米国政府における研究開発投資ポートフォリオ分析手法の例を図表 19 に示す。この手法は、米国エネルギー省（DOE）傘下のサンディア国立研究所（SNL）によって開発された Vital Issue Process (VIP)である。VIP は、一対比較法により限られた予算内においてプログラム間の重要度を順位付けする等を目的とした定性的分析手法と位置づけられる。

VIP には目的に応じて、いくつかの形態が存在するが、政策的ポートフォリオの決定には４つのステージからなる手法を用いる（図表 19)。

VIP の特徴は、特定の評価手法に依存せずに、専門家による議論と意見集約を重視した手法である。また、専門家パネルを設置することで、公平性・中立性も担保できることが期待されている。この評価プロセスの中に、一般的な評価手法である BCG Matrix や、NPV などの手法を評価指標として組み込むことも可能である。一方で、複数の専門家パネルを開催する必要があるなど、評価コストは大きくなりがちであり、また多くの専門家が介在することにより、結果としてリスクの高い案件が排除される可能性が高まる点には注意する必要がある。

我が国において適用することを想定した場合、専門家による合意形成を重視する本手

法は比較的受け入れられやすいものと考えれれるが、一方で、専門家の絶対数が米国に比較して少ない事は適用上の障害となりうる。



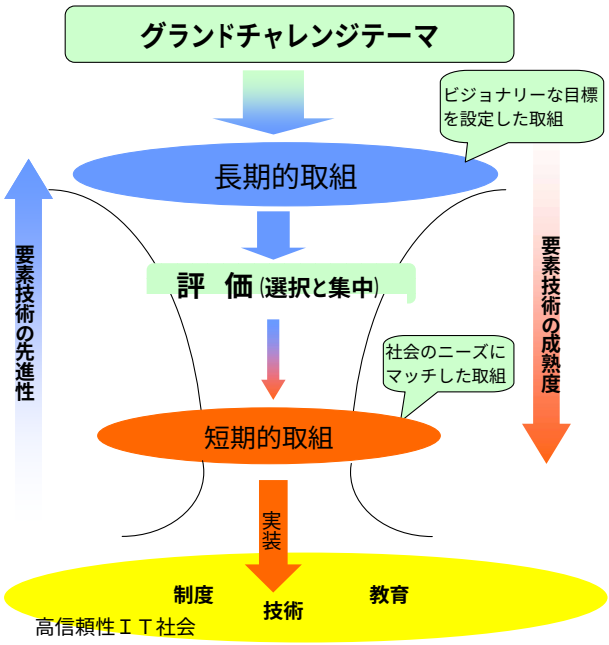

**図表 19　米国政府における研究開発投資ポートフォリオ分析手法の例**

### 3.1.2.公的資金の重点的投入方策

情報セキュリティ技術に関する研究開発・技術開発に対して行われる、我が国の公的研究資金の投入方策等に関して、特に長期・短期・萌芽的研究開発についてどのように考えるかについて検討を行った。

長期的目標と短期的目標について、グランドチャレンジ研究開発の観点からは、成熟度という視点で整理することが適当である（図表 20）。なお、萌芽的研究開発については長期的目標の一部に組み込まれると考えられる。

- 長期的取組
  構成技術の成熟度は未だ低いものの、グランドチャレンジテーマに向けて先進的な技術開発・研究開発の取組を行う
- 短期的取組
  高信頼性 IT 社会の実現のため、充分な「成熟度」を持つ構成要素を有機的に統合する取組を行う




**図表 20　長期的取組と短期的な取組について**

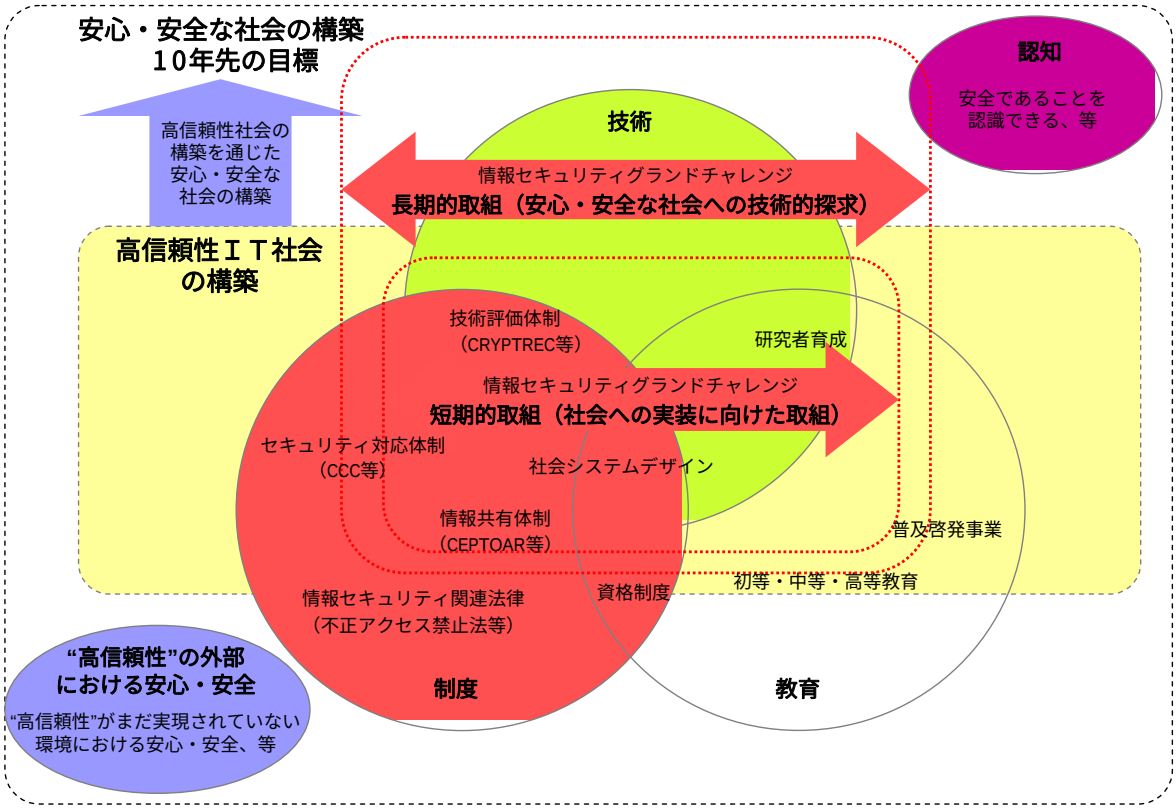
### 3.2.グランドチャレンジ型研究開発・技術開発の実現に向けて

以上の検討を踏まえ、特に、平成 21 年度からの実施を念頭に考察を行った。

グランドチャレンジ型研究開発・技術開発は、長期的には第 3 期科学技術基本計画や第一次情報セキュリティ基本計画に示されているように「安心・安全な社会の構築」を長期的目標とすべきであると考えられる。

しかしながら、「安心・安全な社会の構築」は一足飛びに実現する目標ではないため、短期的目標として「高信頼性 IT 社会の構築」を掲げ、高信頼性 IT 社会を実現することを通じて安心・安全な社会の構築につなげるという二段階の戦略をとることが考えられる。

グランドチャレンジの対象としては、技術を中心としつつ、情報セキュリティの特色を鑑み、制度・教育との連携等についても視野に入れた方が望ましい。長期的には、単なる技術開発ではなく、安全であることをエンドユーザが容易に認識できることを如何に確保するか（認知の問題）や、高信頼性がまだ実現されていない環境における安心・安全を如何に確保するか（"高信頼性"の外部における安心・安全）なども視野に入れた研究開発が望まれる（図表 21）。




**図表 21　グランドチャレンジ型研究開発の位置づけ**

ここでは、長期、短期の研究開発の実施・検討方法としては、具体的に以下のように想定する。

長期・・・次期総合科学技術基本計画を目途に「安心・安全な社会の構築」を実現するためのテーマ。20 年度も引き続きグランドチャレンジ検討 WG にて審議を継続。

短期・・・平成２１年度の科学技術振興調整費等を目標に、「安心・安全な社会の構築」の基盤要素たる高信頼性社会を実現するの為のテーマ。現状において、暗号、デバイス、システム、etc 広範囲の分野に散らばる情報セキュリティ関係技術開発・研究開発事項を束ねる為のテーマ。

また、具体的に想定される短期的な研究開発テーマ案を図表 22に示す。

### 情報セキュリティリスクの評価・分析技術

（1） 背景と目的：
- 情報セキュリティ対策の基本はリスク分析であるにもかかわらず、リスク分析が正しく行われていることは少ない。
- 複合的なコンポーネントから構成される情報システムのリスク分析技術は確立されていない。
- また、定量的リスク分析に必要なデータの蓄積がない。

（2）期待される効果：
- 人間系も含めた情報システムの信頼性向上。

（3）概要：
- 小規模なシステム（組込システム等）から大規模システム情報システム（重要インフラの業務システム等）に対応できる、リスク分析技術。
- 情報システムを運用する人間系を含めたリスク分析技術。
- システム間、あるいは外部環境とシステムの相互依存性を加味したリスク分析技術。
- リスク分析に必要な基礎的データの収集と蓄積。
- 脆弱性の存在がシステムに与えるリスク量の算出技術。

### 情報セキュリティ実装工学

（1） 背景と目的：
- 情報セキュリティ関係の個々の要素については、これまで様々な研究が行われてきているところ。
- しかしながら、それら技術をシステムとして実装したり、社会に普及していく際に検討すべきことについては、十分に研究がなされていない。

（2）期待される効果：
- ソフトウエア脆弱性や暗号危殆化時における社会的コストの最小化。

（3）概要：
- 情報システムのライフサイクルを通じたセキュリティ確保・技術の体系的研究。
- 暗号危殆化時において、社会的影響を最小化するようなシステム構成技術。また、ユーザーへのデプロイ手法の研究。
- 稼動を停止できないシステム（原子力発電所の制御システム）等における脆弱性発生時の対処技術。

### 新たな情報システムアーキテクチャに対応した新しいセキュリティモデルの提示

（1） 背景と目的：
- 従来の情報システム構築技術は、信頼できるドメイン内に閉じたシステムを対象に研究されてきた。
- 今後普及が見込まれる、P2P、SaaS、グリッドなどの新しいシステムアーキテクチャに対応したセキュアなシステム構築技術について十分な研究がなされていない。

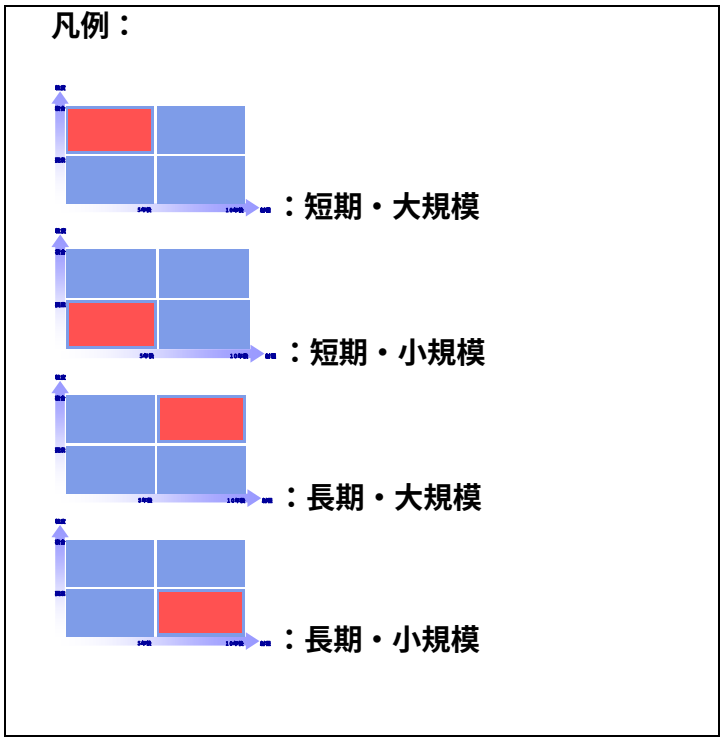
（2）期待される効果：
- 安全なインターネットサービスの提供。

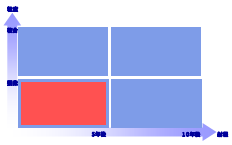
（3）概要：
- 新しいシステムアーキテクチャに対応した脆弱性のモデル化、体系化の研究。
- 分散化、匿名化された情報の保護技術。
- 問題が発生したときの責任分界のあり方に関する研究。
- 事業継続性・可用性の確保技術。

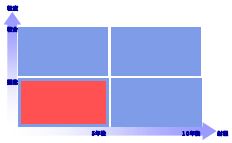
**図表 22　高信頼性社会の構築に向け、情報セキュリティ技術において早急に対応が必要な技術開発・研究開発テーマ**

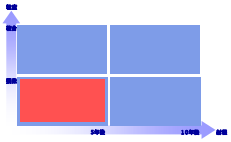
# 付録：グランドチャレンジ研究テーマ案

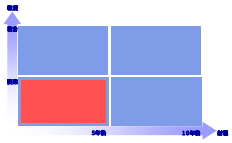
ここでは、グランドチャレンジ検討ワーキンググループや技術戦略専門委員会において提案された、グランドチャレンジ研究テーマの案について列挙する（順不同）。ここに示された研究テーマ案は、必ずしもワーキンググループ・委員会の総意として合意されたものではなく、また粒度等もまちまちであるなど、整理されたものではないが、今後の参考のために示すものである。

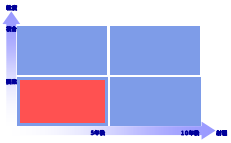


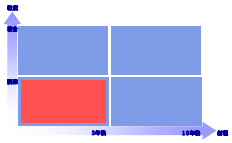
| | |
|---|---|
| 項番 | 1 |
| テーマ名 | ユーザブルセキュリティ技術 |
| 概要 | エンドユーザでも複雑な設定等を行うことなく、安全に IT を利用可能なユーザブルセキュリティ技術や、自身が安全な環境にいるか否かを直感的に把握可能なユーザインターフェース技術等の開発。 |
| 分類 |  |
| 背景と目的 | ・例えば一般のユーザが Web サイトにアクセスした際に、自分が安全なサイトを閲覧しているか否かを容易に判断する方法がない。<br>・SSL 等で認証された安全なサイトにアクセスしている場合でも、その確認方法は一般ユーザにとっては複雑である。またブラウザの種類やバージョンによっても異なるなど、ユーザにとっては混乱の原因となる。 |
| 具体的研究項目 | ・ユーザインターフェース技術<br>・ユーザに対する提示項目、提示方法等の標準化<br>・安全な Web サイトか危険な Web サイトを判別する方法（ホワイトリスト方式、ブラックリスト方式等） |
| 期待される効果 | ・エンドユーザの安全性向上 |
| 備考 | グランドチャレンジ検討 WG<br>－実質被害０　（ゼロ） |

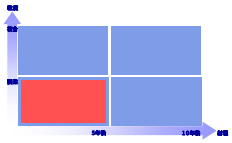
| | |
|---|---|
| 項番 | 2 |
| テーマ名 | 安全なソフトウエア構築技術 |
| 概要 | 絶対安全なソフトウエアの構築技術の開発。Trustworthy システム技術、セキュアプログラミング技術の開発。スキルの低い開発者でも安全なアプリケーションを開発できるような、プログラム自動構成技術や、アプリの安全性を簡単に検証できる技術等の開発。 |
| 分類 |  |
| 背景と目的 | ・ウイルスやボット等の多くはソフトウエア脆弱性が原因になっている。<br>・WEB が直面している脅威である SQL インジェクションや XSS なども WEB アプリケーションの脆弱性が大きな問題になってきている。<br>・特に WEB アプリケーションの開発者は、いわゆるプログラマとしての能力が高くない場合も多いため、脆弱性を作りこみやすい。また、その安全性を検証するコストが高くなってきている。 |
| 具体的研究項目 | ・セキュアプログラミング技術<br>・プログラム自動構成技術<br>・安全性検証技術 |
| 期待される効果 | ・エンドユーザの安全性向上<br>・ソフトウエア脆弱性の減少<br>・ソフトウエア生産性の向上 |
| 備考 | グランドチャレンジ検討 WG<br>－実質被害０　（ゼロ） |

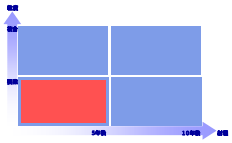
| | |
|---|---|
| 項番 | 3 |
| テーマ名 | 情報セキュリティに関する被害の把握技術の開発 |
| 概要 | 企業・個人等を含む社会全体が蒙っている被害等を適宜把握するための手法に関する研究。もしくはこのような情報を集約・分析・提供する体制の整備。 |
| 分類 |  |
| 背景と目的 | ・企業個人における情報セキュリティ対策の阻害要因として、どこまで対策を実施すべきかわからない、という意見がアンケート調査等で上位に位置づけられている。<br>・この理由として、情報セキュリティに対する投資がどの程度効果があるのか、という点について定量的な情報が無いことが大きな理由として考えられている。<br>・また、情報セキュリティ政策を策定する際においても、どのような政策を講ずれば、社会的便益を最大化できるかについて、信頼に足る定量的な情報が少ない状況にある。<br>・被害状況を定量的に把握する技術・体制を開発・整備することで、適正な情報セキュリティ対策の促進を目的とする。 |
| 具体的研究項目 | ・情報セキュリティリスク定量化<br>・情報セキュリティに関する統計調査手法<br>・情報集約・分析体制 |
| 期待される効果 | ・企業個人における適切な情報セキュリティ対策の進展<br>・国等における効果的な情報セキュリティ政策の立案 |
| 備考 | グランドチャレンジ検討 WG |

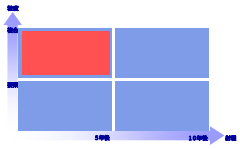
| | |
|---|---|
| 項番 | 4 |
| テーマ名 | 企業内インシデントハンドリング支援技術 |
| 概要 | 企業内において、情報セキュリティに係るインシデント・ハンドリング（事故対応）を支援する技術の開発。 |
| 分類 |  |
| 背景と目的 | ・企業における情報セキュリティ対策は進展を見ているが、事故対応体制の整備は端緒についたばかりである。<br>・企業において情報セキュリティインシデントが発生し、事故・被害の拡大防止などが失敗した事例を見ると、その理由が対応体制の不備に起因している場合が多い。<br>・企業における情報セキュリティインシデント対応等を支援する技術を開発することで、被害の抑制等につなげる。 |
| 具体的研究項目 | ・意思決定エキスパートシステム<br>・チケッティングシステム<br>・事業継続支援システム<br>・脅威度分析システム<br>・ソフトウェアリポジトリ |
| 期待される効果 | ・企業における情報セキュリティ対策の促進。<br>・社会的な被害の最小化。 |
| 備考 | グランドチャレンジ検討 WG<br>－組織的対応（事故対応の高度化等による被害の局限） |

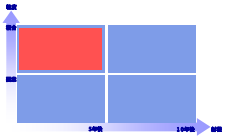
| | |
|---|---|
| 項番 | 5 |
| テーマ名 | 情報セキュリティ投資対効果 |
| 概要 | 情報セキュリティ投資の投資対効果に係る研究開発。 |
| 分類 |  |
| 背景と目的 | ・企業における情報セキュリティ対策の阻害要因として、どこまで対策を実施すべきかわからない、という意見がアンケート調査等で上位に位置づけられている。<br>・この理由として、情報セキュリティに対する投資がどの程度効果があるのか、という点について定量的な情報が無いことが大きな理由として考えられる。<br>・また、情報セキュリティ政策を策定する際においても、どのような政策を講ずれば、社会的便益を最大化できるかについて、信頼に足る定量的な情報が少ない状況にある。<br>・投資対効果を定量的に把握する技術を開発・整備することで、適正な情報セキュリティ対策の促進を目的とする。 |
| 具体的研究項目 | ・情報セキュリティ ROI, NPV, IRR 等の投資対効果評価手法<br>・投資対効果のモデル化<br>・情報セキュリティリスク定量化 |
| 期待される効果 | ・企業個人における適切な情報セキュリティ対策の進展<br>・国等における効果的な情報セキュリティ政策の立案 |
| 備考 | グランドチャレンジ検討 WG<br>－組織的対応（事故対応の高度化等による被害の局限） |

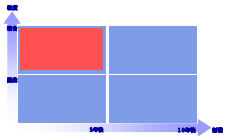
| | |
|---|---|
| 項番 | 6 |
| テーマ名 | 観測情報共有分析技術 |
| 概要 | 様々な組織が収集している観測データを共有し、あるいは統合・分析・提供するための技術の開発。 |
| 分類 |  |
| 背景と目的 | ・分散管理されているインターネットでは、どのような障害や攻撃が発生しているのか、リアルタイムに把握することが困難である。<br>・また、近年深刻化しているボットやターゲット型攻撃などは、単一の観測点ではその状況を把握することが困難になってきている。<br>・様々な団体で開発・実装されているネットワーク観測システムの観測データを共有し、統合的に分析する技術を開発する。 |
| 具体的研究項目 | ・ネットワーク広域観測技術<br>・ハニーポット技術<br>・情報共有フォーマット<br>・情報の匿名化技術<br>・国際標準化 |
| 期待される効果 | ・ネットワークの安全性向上 |
| 備考 | グランドチャレンジ検討 WG<br>－被害・リスクの正確な把握 |

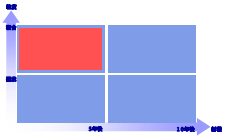
| | |
|---|---|
| 項番 | 7 |
| テーマ名 | 情報セキュリティリスクの評価・分析技術 |
| 概要 | 情報システム等の情報セキュリティに関する安全性の評価を行う技術の研究を行う。 |
| 分類 |  |
| 背景と目的 | ・情報セキュリティ対策の基本はリスク分析であるにもかかわらず、リスク分析が正しく行われる場青は少ない。<br>・コンポーネント単位のシステムの情報セキュリティ評価手法（ISO/IEC 15408）は既に存在している。<br>・複合的なコンポーネントから構成される情報システムのリスク分析技術は確立されていない。また、コンポーネントレベルでの評価もコスト的な負担が大きい。<br>・また、定量的リスク分析に必要なデータの蓄積がない。 |
| 具体的研究項目 | ・小規模なシステム（組込システム等）から大規模システム情報システム（重要インフラの業務システム等）に対応できる、新しいリスク分析技術。<br>・情報システムを運用する人間系を含めたリスク分析技術。<br>・システム間、あるいは外部環境とシステムの相互依存性を加味したリスク分析技術。<br>・リスク分析に必要な基礎的データの収集と蓄積。<br>・脆弱性の存在がシステムに与えるリスク量の算出技術。 |
| 期待される効果 | 人間系も含めた情報システムの信頼性向上。 |
| 備考 | 情報通信 PT |

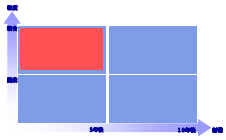
| | |
|---|---|
| 項番 | 8 |
| テーマ名 | 悪意を持ったプログラムへの対策技術 |
| 概要 | コンピュータウイルスなどの悪意を持ったプログラムによる脅威を根絶できるような情報処理環境の構築。 |
| 分類 |  |
| 背景と目的 | ・近年、ボットなどの悪意を持ったプログラムが大きな脅威となってきている。<br>・これらは、完成度の高いツール等を用いて自動的あるいは容易に作成が可能となっており、派生種を含めるとその種類は膨大であり、日々増加しつつある。<br>・このような悪意のあるプログラム（ボット等）については、従来のシグネチャ方式によるウイルス対策ソフトでは必ずしも十分な対処ができないことから新しい対策手法が求められている。 |
| 具体的研究項目 | ・ヒューリスティック型検知技術。<br>・仮想化技術、サンドボックス技術等の安全にプログラムを実行する環境を構成するための技術。<br>・悪意のあるプログラムの制御サーバを検出、無効化する技術。 |
| 期待される効果 | ・エンドユーザの安全性向上 |
| 備考 | 技術戦略専門委員会報告書 2005 |

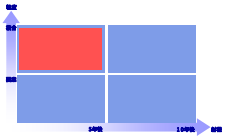
| | |
|---|---|
| 項番 | 9 |
| テーマ名 | スパム０（ゼロ） |
| 概要 | 現在大きな社会的･経済的な損出となっている迷惑メールについて、実質的にその被害を０にするような総合的な技術等の開発。 |
| 分類 |  |
| 背景と目的 | ・現在、ある統計によれば全電子メールの 8 割以上が迷惑メール（スパム）である。<br>・企業・個人が受け取った迷惑メールと、そうでないメールを判別し、迷惑メールを削除するのに要している作業の人件費や生産性の低下などによる社会的コストは膨大である。<br>・また迷惑メールが通信インフラに与える負荷も大きく、通信事業者は過大な設備投資を迫られている。 |
| 具体的研究項目 | ・発信者認証技術<br>・サービスプロバイダの認証技術<br>・ボット対策技術<br>・迷惑メールを判別する技術 |
| 期待される効果 | ・エンドユーザの安全性向上<br>・社会的コストの低減 |
| 備考 | グランドチャレンジ検討 WG<br>－実質被害０　（ゼロ） |

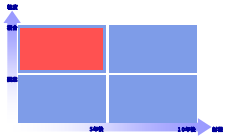
| | |
|---|---|
| 項番 | 10 |
| テーマ名 | あっ Internet（仮称） |
| 概要 | 未成年や高齢者などの情報弱者向けに、いわゆる The Internet から隔離されることで安全なネット環境（あっ Internet）を実現する技術もしくは社会的な仕組み。 |
| 分類 |  |
| 背景と目的 | ・高齢者や子供などの IT リテラシーが低いユーザが出会系サイトやフィッシング詐欺などの被害者になるケースが増えている。<br>・機能や出来ることに制限が存在したとしても、だれでも安全に使える擬似的なインターネット環境が必要になってきている。 |
| 具体的研究項目 | ・システム開発<br>・ユーザインターフェース研究<br>・フィルタリング技術 |
| 期待される効果 | ・エンドユーザの安全性向上 |
| 備考 | グランドチャレンジ検討 WG<br>－情報セキュリティに係る社会的メカニズムの確立 |

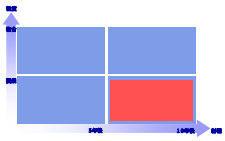
| | |
|---|---|
| 項番 | 11 |
| テーマ名 | インターネットの危険度リアルタイム把握技術 |
| 概要 | インターネットが曝されている脅威・危険度をリアルタイムで把握する技術の開発。 |
| 分類 |  |
| 背景と目的 | ・分散管理されているインターネットでは、どのような障害や攻撃が発生しているのか、リアルタイムに把握することが困難である。<br>・また、ウイルスやボットなどの悪意のあるプログラムの影響をリアルタイムに把握することは技術的にも困難。<br>・これらの脅威や危険度をリアルタイムで把握することができれば、ネットワーク管理者が対策を迅速に講ずることが可能となる可能性がある。 |
| 具体的研究項目 | ・ネットワーク広域観測技術<br>・ハニーポット技術<br>・マルウエア自動解析技術 |
| 期待される効果 | ・ネットワークの安全性向上 |
| 備考 | グランドチャレンジ検討 WG<br>－被害・リスクの正確な把握 |

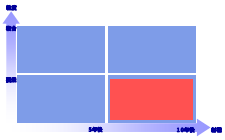
| | |
|---|---|
| 項番 | 12 |
| テーマ名 | 情報セキュリティの積極先行展開 |
| 概要 | アプリケーションが必要とするセキュリティを確保するための目標（基準、尺度、スケジュール）を決定し、アプリケーションの展開と歩調を合わせた形で、セキュリティも確保してゆく。<br>さらには、セキュリティがアプリケーション開発やその方向性を誘導するなど、セキュリティをシステムやサービス展開の柱にしていく。<br><br>例）情報家電、電子私書箱、スマートカード等の情報セキュリティのあるべき姿を考え確保する。 |
| 分類 |  |
| 背景と目的 | ・様々な情報システム等における情報セキュリティ対策は必ずしもその最初の設計段階から組み込まれたものではなく、様々な脅威が発生した結果を踏まえて、対症療法的に対策がとられた場合も多い。<br>・特定の情報システムやアプリケーションを想定し、そのシステムやアプリケーションが本来具備すべき情報セキュリティのあり方をゼロベースで検討し、それをシステムやアプリケーションに組み込んでいくことが重要。<br>・これにより、結果としてシステムやアプリケーションの普及が促進されると共に、セキュアであることをシステムやアプリケーションの売りとして展開していくととが可能と想定される。 |
| 具体的研究項目 | ・情報家電等の情報セキュリティ対策 |
| 期待される効果 | ・エンドユーザの安全性向上<br>・情報セキュリティ産業の振興 |
| 備考 | 技術戦略専門委員会 |

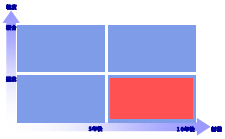
| | |
|---|---|
| 項番 | 13 |
| テーマ名 | 情報セキュリティ実装工学 |
| 概要 | 情報セキュリティの要素技術を実際のシステムあるいは社会制度の中に実装・普及するための方策について研究を行う。 |
| 分類 |  |
| 背景と目的 | ・情報セキュリティ関係の個々の要素についてはこれまで様々な研究が行われてきているところ。<br>・しかしながら、それら技術をシステムとして実装したり、社会に普及していく際に検討すべきことについては十分に研究がなされていない。 |
| 具体的研究項目 | ・情報システムのライフサイクルを通じたセキュリティ確保/技術の体系的研究。<br>・暗号危殆化時において社会的影響を最小化するようなシステム構成技術。また、ユーザーへの普及・配布手法の研究。<br>・稼動を停止できないシステム（原子力発電所の制御システム）等における脆弱性発生時の対処技術。 |
| 期待される効果 | ソフトウエア脆弱性や暗号危殆化時における社会的コストの最小化。 |
| 備考 | 情報通信 PT |

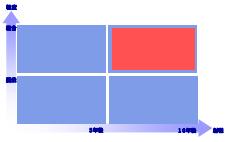
| | |
|---|---|
| 項番 | 14 |
| テーマ名 | 情報セキュリティサービスの品質コントロール技術 |
| 概要 | 情報サービス、ネットワークサービスにおいて、利用者側が情報セキュリティサービスの品質グレードを指定し、利用できる環境の構築。例えば、電気通信事業者やプロバイダーが指定するのではなく、利用者がグレードをコントロールし、かつユーザブルに利用可能な「迷惑電話・迷惑メール防止サービス」の提供など。 |
| 分類 |  |
| 背景と目的 | ・IT 化の進展に伴い、ユーザが求める情報セキュリティサービスに対する要求が多様化していきている。<br>・例えば、それほど可用性が要求されないが、低廉な料金が求められる場合や、高価でも構わないが高い情報セキュリティ水準が求められるような場合が、ユーザ毎やサービス毎に異なってきている。<br>・一律の情報セキュリティ対策を全てのサービス等に要求することはいたずらなコストの増大を招くなど、経済合理性の観点からも問題がある。 |
| 具体的研究項目 | ・マルチグレードの情報セキュリティサービス実現技術。<br>・サービスレベルの合意形成。 |
| 期待される効果 | ・社会的コストの低減。 |
| 備考 | 技術戦略専門委員会報告書 2005 |

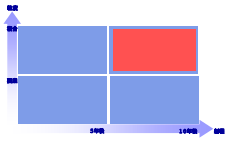
| | |
|---|---|
| 項番 | 15 |
| テーマ名 | グローバルトラストネットワーク |
| 概要 | 認証等の基礎となるトラストポイントの国際化とネットワーク化。例えば日本が先導してトラストポイントに求められる要件と検証を行い、各国が持つトラストポイントについて相互互換性を保証する「グローバルトラストネットワーク」を形成する取組み。 |
| 分類 |  |
| 背景と目的 | ・インターネット等で様々なサービスが提供されるようになってきたが、個人認証等については、各サービス毎にまちまちであり、利便性を大きく損なっている。またそれぞれのサービス毎に認証基盤を構築する必要があるのは、コスト的にも高いものになることなどから、認証技術の重要性が高まってきている。<br>・また認証技術として有望視されている PKI については、各国政府がそれぞれ整備を行っていること等から、一部の例外を除けば相互認証は困難である。<br>・我が国が先導することで、認証の基礎となるトラストポイントの相互互換性を確保することで、世界中のどこでも容易に認証が可能な環境を整備する必要がある。 |
| 具体的研究項目 | ・相互認証技術。<br>・PKI 関連技術。 |
| 期待される効果 | ・社会的コストの低減<br>・エンドユーザーの安全性向上 |
| 備考 | 技術戦略専門委員会報告書 2005 |

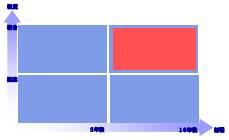
| | |
|---|---|
| 項番 | 16 |
| テーマ名 | 不確定性（リスク）を許容する社会のあり方に向けた研究。 |
| 概要 | 不確定性（リスク）を許容する社会のあり方に向けた研究。 |
| 分類 |  |
| 背景と目的 | ・近年、社会として不確定性（リスク）を許容しない風潮が強まってきている傾向にある。<br>・社会として不確実性を許容しないことによる、社会的コストの増大が懸念される。 |
| 具体的研究項目 | ・社会学的研究<br>・リスクマネジメント<br>・リスクコミュニケーション |
| 期待される効果 | ・社会としての全体最適化 |
| 備考 | グランドチャレンジ検討 WG<br>－情報セキュリティに係る社会的メカニズムの確立 |

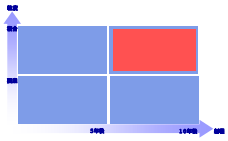
| | |
|---|---|
| 項番 | 17 |
| テーマ名 | 新しいセキュリティモデルに関する研究開発 |
| 概要 | 新たな情報システムアーキテクチャに対応した新しいセキュリティモデルに関する研究開発を行う。 |
| 分類 |  |
| 背景と目的 | ・従来の情報システム構築技術は、信頼できるドメイン内に閉じたシステムを対象に研究されてきた。<br>・今後普及が見込まれる、P2P、SaaS、グリッドなどの新しいシステムアーキテクチャに対応したセキュアなシステム構築技術について十分な研究がなされていない。 |
| 具体的研究項目 | ・新しいシステムアーキテクチャに対応した脆弱性のモデル化、体系化の研究。<br>・分散化、匿名化された情報の保護技術。<br>・問題が発生したときの責任分界のあり方に関する研究等における脆弱性発生時の対処技術。<br>・事業継続性・可用性の確保技術。 |
| 期待される効果 | ・安全なインターネットサービスの提供 |
| 備考 | 情報通信 PT |

| | |
|---|---|
| 項番 | 18 |
| テーマ名 | 情報セキュリティ・ユニバーサルデザイン |
| 概要 | 情報システムを運用する回避不可能な人為的ミス等から発生するトラブルやエラーを根絶する、「情報セキュリティ・ユニバーサルデザイン」の確立。 |
| 分類 |  |
| 背景と目的 | ・近年の情報セキュリティ事故の多くは、設定時、運用時、トラブル対応時における人為的なミスによるものが多い。<br>・これらは、同種ソフトウエア毎やバージョンが変わる毎に操作方法が異なったり、用語や操作が複雑なことが人為的ミスの大きな要因となっている。<br>・「情報セキュリティ・ユニバーサルデザイン」について研究を行うことで、これらの人為的ミスを減少させ、最終的には根絶することを目標とする必要がある。 |
| 具体的研究項目 | ・ユーザーインターフェース技術。<br>・共通のデザインガイドライン等。 |
| 期待される効果 | ・エンドユーザの安全性向上<br>・情報システム運用コスト（教育コストも含む）の低減 |
| 備考 | 技術戦略専門委員会報告書 2005 |

| | |
|---|---|
| 項番 | 19 |
| テーマ名 | 情報セキュリティテストベッド（特区） |
| 概要 | 情報セキュリティに関する研究・社会実験を促進するために、情報セキュリティに関わる社会的制約を受けない情報セキュリティ特区や、大規模なアウトブレーク等を模擬することのできるセキュリティテストベッドの整備。 |
| 分類 |  |
| 背景と目的 | ・情報セキュリティに関する大規模な社会実験は、そもそも社会通念上も、法制度上（不正アクセス禁止法等）も許されるものではない。<br>・一方で、大規模な DDOS 攻撃や、ウイルスの感染など、可能な限り実社会に近い形での実験を行わないと、その性状の把握や、効果的な対策の策定が困難な場合がある。<br>・企業や大学の研究者を対象とした大規模な実験環境を構築することで、一般のインターネットでは実験できない、新しい攻撃手法に関する防御技術や、製品・サービス等のストレステストを実施することができる。 |
| 具体的研究項目 | ・大規模ネットワークシミュレーション技術<br>・攻撃のエミュレーション<br>・ネットワーク観測技術<br>・ネットワークの隔離技術 |
| 期待される効果 | ・情報セキュリティ関連研究の進展<br>・研究者の育成<br>・産業化 |
| 備考 | グランドチャレンジ検討 WG<br>－情報セキュリティに係る社会的メカニズムの確立 |

| | |
|---|---|
| 項番 | 20 |
| テーマ名 | 未知なる脅威への対処技術 |
| 概要 | 将来発生するであろう未知なる脅威に対して、可能な限り自動的かつリアルタイムに対応できる技術を開発する。 |
| 分類 |  |
| 背景と目的 | ・今日具体化している脅威については、官民を問わず必要な者が必要な範囲で対応している。<br>・しかし、現在未だ現れていない脅威（特に相手に悪意のあるもの）を想定し対応策を準備することについては、国家的な対応（体制、技術、予算、etc）が必要になる可能性がある。<br>・また、将来の脅威への対応については、国等による相応のインセンティブが必要となる可能性もある。 |
| 具体的研究項目 | ・免疫型情報セキュリティー技術<br>・マルウエアの自動分析技術<br>・不正侵入検知技術 |
| 期待される効果 | ・ネットワークの安全性向上<br>・エンドユーザの安全性向上 |
| 備考 | 技術戦略専門委員会 |

| | |
|---|---|
| 項番 | 21 |
| テーマ名 | 重要課題を展開する際に必要となる情報セキュリティの確保 |
| 概要 | 国や国民にとって必要な課題を展開する際に、必要となるセキュリティを徹底的に確保する。<br>例）電子政府の積極展開に必要なセキュリティ戦略を詳細に立案実行し、世界一安全な電子政府を実現する。そして、世界の手本となる電子政府とする。<br>例）暗号の危殆化への対応、きめ細かく課題の解決法やスケジューリング、危機管理方策を立案実行する。 |
| 分類 |  |
| 背景と目的 | ・電子政府システムなど国民生活にも大いに関係する、大規模な情報システムが構築されているが、それらの情報セキュリティ対策についてはシステム毎に個別に考えられているのが現状である。<br>・電子政府システムの安全性を横断的に確保するためには、電子政府システムの企画段階から情報セキュリティを徹底的に考慮したシステムを開発する必要がある。<br>・また、暗号の危殆化など、社会に大きな影響を与える脅威に対して、国として講ずるべき施策（研究開発も含む）について、総合的な対策を打ち出す必要がある。 |
| 具体的研究項目 | ・電子政府の情報セキュリティ対策<br>・暗号危殆化対策技術 |
| 期待される効果 | ・エンドユーザの安全性向上<br>・電子政府の普及 |
| 備考 | 技術戦略専門委員会 |

| | |
|---|---|
| 項番 | 22 |
| テーマ名 | 高信頼性インターネット環境 |
| 概要 | 通信障害等を自律的に検知し、回復することのできる高信頼性のあるインターネット環境の構築。 |
| 分類 |  |
| 背景と目的 | ・社会全体がインターネットに依存する比率が高くなるにつれて、インターネットの信頼性に対する要求が高まってきている。<br>・インターネットは当初より頑健性を求めて開発されてきたものであるが、近年、ネットワークトポロジーが分散型からスター型に近づきつつあること等により、特定の障害によりネットワーク全体の信頼性を毀損する恐れがあることが指摘されてきている。<br>・そのため、インターネットにおいて通信障害等が発生した場合、自動的に障害箇所や原因を検知し、回復することができる環境の整備が必要である。 |
| 具体的研究項目 | ・ロバストなルーティング技術。<br>・障害検知技術。<br>・ネットワークの多重化技術。 |
| 期待される効果 | ・社会全体の信頼性の向上 |
| 備考 | 技術戦略専門委員会報告書 2005 |

【別紙】

**グランドチャレンジ検討ワーキンググループ**
**委員名簿**

（座長）
武田 圭史　カーネギーメロン大学日本校 教授

（構成員）
新井 悠　　株式会社ラックサイバースペース総合研究所 先端技術開発部長
大岩 寛　　産業技術総合研究所情報セキュリティ研究センター 研究員
門林 雄基　奈良先端科学技術大学院大学情報科学研究科 准教授
鎌田 敬介　JPCERT/Coordination Center 早期警戒グループマネージャー
小池 英樹　電気通信大学 大学院情報システム学研究科 教授
寺田 真敏　株式会社日立製作所 Hitachi Incident Response Team (HIRT)
野川 裕記　株式会社セキュアウェア 取締役
福本 佳成　楽天株式会社システムセキュリティ部 部長
星澤 裕二　株式会社セキュアブレイン 執行役員
吉岡 克成　横浜国立大学　学際プロジェクト研究センター 助教