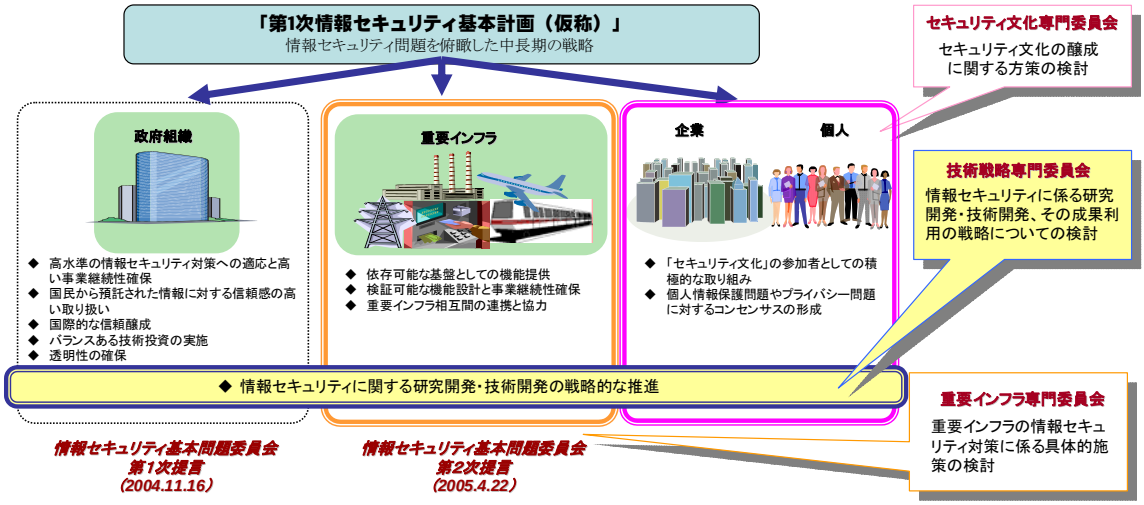
技術戦略専門委員会の概要

力強いIT社会の発展を下支えする情報セキュリティ研究開発・技術開発の戦略的推進

1　技術戦略専門委員会報告書の位置づけ

- ○ 「第1次情報セキュリティ基本計画（仮称）」に関する当面の審議の充実に資するため、情報セキュリティに係る研究開発・技術開発、その成果利用の戦略について検討し、「技術戦略専門委員会報告書」としてとりまとめ。
- ○ 情報セキュリティの確保においては、継続的な技術開発と、その社会展開を円滑に行い、成果を全ての主体が享受できる環境作りが必要であり、喫緊の課題を解決するための技術開発と、中長期的な視点に立った研究開発投資の戦略設定が強く求められているとの認識に基づいて議論。



「第１次情報セキュリティ基本計画（仮称）」に向けた検討の全体像

2　情報セキュリティ技術戦略を考える上での基本的な考え方

- ○ コンピュータとネットワークの普及と利用形態の変遷に応じて、求められる情報セキュリティ技術も大きく変化。
- ○ 情報セキュリティ技術の開発モデルを整理した上で、我が国における情報セキュリティ上の問題点と、その問題解決に利用される技術の役割を概観。
- ○ 情報セキュリティ技術は何のために求められるのか、そして将来的にどのような目標に向かって研究開発・技術開発が行われるべきか、情報セキュリティ技術戦略の基本的な考え方を提示。

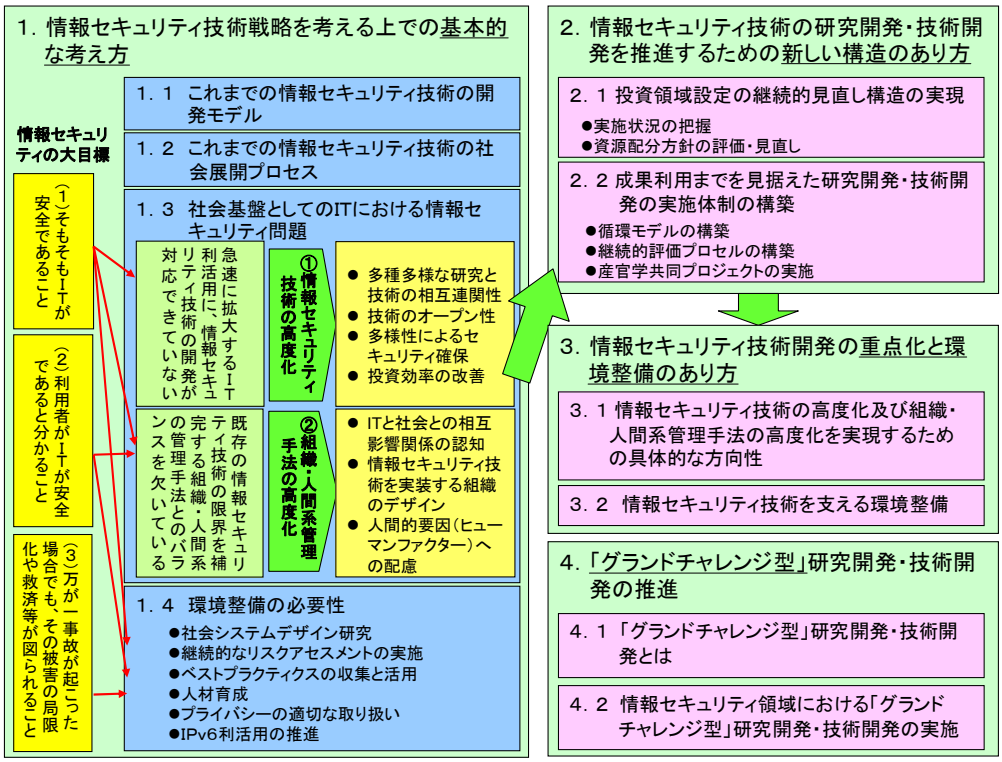


図1　報告書の全体像

(1)我が国における情報セキュリティ上の問題点と問題解決に利用される技術の役割とその方向性

(ア)我が国における情報セキュリティ上の問題点の全体俯瞰

○ IT基本法にいう「高度情報通信ネットワークを安心して利用可能」[1]な環境とすることが求められている。ここでいう、「安心して利用可能」な環境とは、大きく、以下の3つの条件が満足される環境として構築されるべきもの。

1) そもそも「高度情報通信ネットワーク(IT)が安全である」こと。

2) 利用者が、「高度情報通信ネットワーク(IT)が安全である」と分かる(認識・体感できる)こと。

3) 万が一事故が起こった場合でも、その被害の局限化や救済等が図られるとともに業務の継続性が保たれること。

○ これまでは顕在化した問題のみに対処する対症療法的な対応が先行してきたため、利用者の視点からみれば、この3条件を満足した環境として実現できているとは言い

1 高度情報通信ネットワーク社会形成基本法第22条(高度情報通信ネットワークの安全性の確保等)には以下のように記されている。「高度情報通信ネットワーク社会の形成に関する施策の策定に当たっては、高度情報通信ネットワークの安全性及び信頼性の確保、個人情報の保護その他国民が高度情報通信ネットワークを安心して利用することができるようにするために必要な措置が講じられなければならない。」

難い。

（イ）情報セキュリティ技術の役割と今後の方向性

○ 情報セキュリティ技術の問題点

- 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。
- 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。

○ 情報セキュリティ技術の高度化

急速に拡大するIT利活用に対応すべく、以下の点に留意しつつ、情報セキュリティ技術高度化の取組みを実施することが必要。

①多種多様な研究と技術の相互連関性

情報セキュリティ技術を成立させている様々な基礎技術、関連技術についても、その高度化が必要。

②技術のオープン性

技術の特性によりオープン性を確保できないものを除き、知的財産権等に関する問題を整理しつつ、技術のオープン性を様々なレベルで確保し、ブラックボックス性を排除する努力が必要。

③多様性によるセキュリティ確保

同一の機能を提供するも、その実装や設計思想が異なるものを複数用意することで安全性を高めるという解決方法、いわゆる多様性によるセキュリティ確保という手法が存在することにも留意する必要。

④投資効率の改善

研究開発・技術開発の投資領域の特定、実施段階での効率的な活動展開、さらに、実用化・普及プロセスにおける効率化などの、研究開発・技術開発のプロセスそのものの投資効率の改善にも持続的に取り組むことが必須。

○ 組織・人間系の管理手法の高度化

開発された情報セキュリティ技術が実環境で効果的、効率的に運用されるため、以下の点に留意しつつ、組織・人間系の管理手法の高度化が必要。

①IT と社会との相互影響関係の認知

情報セキュリティが社会におけるさまざまな主体やその活動とどのような影響関係にあるかを把握することが必要。相互影響関係や予測される脅威、脆弱性情報など

情報セキュリティ上重要な事項をいかに社会に向けて伝達・告知するかというリスク・コミュニケーションについての研究が必要。

②情報セキュリティ技術を実装する組織のデザイン

組織論的及び経営情報論的な視点からの研究が必要。

③人間的要因（ヒューマンファクター）への配慮

情報システムやネットワークシステムを運用する人間の生理的・心理的要因の把握やマン・マシン・インタフェースの考慮によって、ミスやエラーを防御することが必要。これらを研究の対象としている人間工学や認知科学の研究を推進。

（ウ）情報セキュリティ技術を支える環境整備の必要性

○ IT基本法に述べる「高度情報通信ネットワークを安心して利用可能」な環境で求められる前述3条件のうち、3)「万が一事故が起こった場合でも、その被害の局限化や救済等が図られるとともに業務の継続性が保たれること」という点を満足するためには、情報セキュリティ技術の高度化及び組織・人間系の管理手法の高度化だけでは実現することは難しく、こうした情報セキュリティ技術を支える環境整備が同時になされることが必要。具体的には、以下の通り。

①社会システムデザイン研究の実施

既存の社会制度を、情報セキュリティ確保の観点から高度情報通信ネットワーク社会に適合させていくことが必要。技術開発と並行して、新たな技術の普及による高度情報通信ネットワーク社会の変化を捉え、必要となる社会制度の整備や、技術の普及戦略を開発する、いわゆる社会システムデザインに対する研究を実施することが必要。この研究からは、長期的な視点に立った政策提言や、具体的な法整備の必要性の特定と方向性提示、さらには技術の普及において必要となる補完的な技術開発を特定するといった成果が期待される。

②継続的なリスクアセスメントの実施

高度情報通信ネットワーク社会における情報セキュリティ確保では、そもそも社会を「何から」守るのかという明確な認識が不可欠。様々な観点から社会を捉え、リスクアセスメントを継続的に実施することが必要。我が国のリスクアセスメント能力を強化することは、現在解決すべき問題を特定するだけではなく、新たな研究開発・技術開発の必要性を明らかにし、運用環境整備の方向性の明確化に資する。さらには、前項で述べた社会システムデザインにおける要求条件の明確化も果たすことができる。

③ ベストプラクティスの収集と活用

様々なノウハウを収集し、その中で有効性の高いもの、いわゆるベストプラクティスを発見し、社会知として活用していく取組みを強化。

④人材育成

技術立国の我が国が、今後も持続的に発展していくためには、研究者、技術者が安定的に育成され供給されることが必要。近年、高校生や大学生の「理系離れ」の問題が指摘されており、さらに「IT離れ」も具体的な現象として現れてきている。IT技術を持続的に発展させるためには、長期的には「理系離れ」、「IT離れ」問題を解決する取組みが必須。さらに、各組織においてITを運用するオペレータにおいても、情報セキュリティ技術についての理解と活用方法を体得することが必要。

⑤プライバシーの適切な取扱い

認証強化と合理的な匿名性機能提供をバランス良く行うことにより、真にプライバシー保全に貢献することができ、ひいては健全な高度情報通信ネットワーク社会の発展に寄与することが可能。このような視点からの、認証機能強化、匿名性保証基盤確立についても取組みが不可欠。

⑥IPv6利活用の推進

近年開発されているネットワーク技術、さらには今後開発が進められる次世代ネットワーク技術はIPv6が基盤となり、研究開発・技術開発成果の積極的活用の観点からもIPv6の利活用を推進することが重要。

3 情報セキュリティ技術の研究開発・技術開発を推進するための新しい構造のあり方

○ 投資領域設定の継続的見直し構造の実現

具体的な研究開発・技術開発のどの領域について推進するかを判断する場合、現在の研究開発領域の意味、技術構成要素の特性、研究期間の考え方が、投資主体と研究開発・技術開発の実施主体によって大きく変化することを踏まえた投資を推進。

＜具体的な方策＞

①実施状況の把握

総合科学技術会議の協力を得て、情報セキュリティ政策会議は、産官学を通じた我が国における情報セキュリティに関連する研究開発・技術開発の実施状況の把握を実施する。

②資源配分方針の評価・見直し

総合科学技術会議に対して、情報セキュリティ政策会議は、情報セキュリティ領域に対する資源配分方針について継続的に評価・見直しの提言を行う枠組みを構築する。

○ 成果利用までを見据えた研究開発・技術開発の実施体制の構築

情報セキュリティ技術の高度化のために必要な投資効率の改善を実現するためには、成果利用までを見据えた研究開発・技術開発の実施体制を構築することが必要。そのためには、以下の3点からなる新たな体制を構築することが適当。

（ア）循環モデルの構築

技術利用の現場からのニーズの掘り起こしと研究開発現場へのフィードバック、研究領域の調整という循環モデルを構築することが必要。その際に、政府は、情報セキュリティ技術への政府自身のニーズが大きいという特性に鑑み、その成果を政府自身が積極利用するよう検討していくこと、客観的に評価された技術を活用するという視点を盛り込むことが必要。

（イ）継続的評価プロセスの構築

成果利用の可能性を評価する枠組みも必要。その際、成果の国際展開を視野に入れた評価、特に標準化、リファレンスモデル化などの取組みによる国際性を持った成果利用を積極的に推進することが不可欠。

（ウ）産官学の共同プロジェクトの実施

情報セキュリティ技術の研究開発・技術開発、そしてその成果の活用を行う、産官学の関係者が適切な役割分担の下で、共同してプロジェクトを行うことにより、成果の社会展開の加速化を実現することが必要。

＜具体的な方策＞

①循環モデルの構築

情報セキュリティ研究開発・技術開発における成果を、調達を通し、最大限、直接政府が活用するためのガイドラインを策定。また、政府において活用することを前提とし、情報セキュリティ政策会議と内閣官房が主導した、新たな研究開発・技術開発を推進。

②継続的評価プロセスの導入

総合科学技術会議の協力を得て、情報セキュリティ政策会議が、情報セキュリティ技術に関する研究開発・技術開発全般について、1)事前評価、2)中間評価、3)事後評価の各段階における投資効果の評価を実施。

③産官学の共同プロジェクトの実施

総合科学技術会議の協力を得て、情報セキュリティ政策会議が、産官学共同による研究プロジェクトを主導。

4 情報セキュリティ技術開発の重点化と環境整備のあり方

○ 情報セキュリティ技術の高度化及び組織・人間系の管理手法の高度化を実現するための具体的な方向性

情報セキュリティ技術の高度化及び組織・人間系の管理手法の高度化の具体的な方策を実現するためには、以下の投資強化が必要。

（ア）IT強化直結型研究への重点化

公的研究資金の重点的な投入によって、多くの成果創出が期待される領域を例示すると以下のとおり。

①脆弱性を無くす高信頼ソフトウェア開発環境構築のための研究開発
②次世代ネットワーク基盤に関する研究
③先進的な大規模分散処理環境におけるセキュリティ技術の確立
④安全なシステムアーキテクチャに係る研究
⑤電子認証技術の強化
⑥IT に起因するリスクアセスメントに係る研究
⑦高信頼性組織デザインについての研究
⑧重要な情報を守るための情報管理技術の確立
⑨情報セキュリティ評価技術の研究

(イ) 萌芽的研究への投資強化

民間の取組みが乏しい萌芽的研究として考えられる例は以下のとおり。

①デジタルフォレンジック[2]に係る研究
②情報の長期間保存技術に関する研究
③高信頼情報処理アーキテクチャに関する研究

(ウ) 基礎研究領域に対する投資の充実・強化

情報セキュリティに関連する技術の基盤となる基礎研究領域、特に応用数学、離散数学、コンピュータ言語、情報理論、符号理論、シミュレーション技術及びソフトウェア・ハードウェアの安全性検証などに対して積極的な投資を行い、技術基盤の拡充を図る。また、事前に特定の仮説を用意しない探索的研究を促進することにより、広い視野での知見の醸成や新たな仮説の発見に努めるとともに、情報セキュリティ技術の次期研究シーズの育成を図ることも重要。

○ 情報セキュリティ技術を支える環境整備

情報セキュリティ技術を支える環境整備として、以下の取組みが必要。

(ア) 社会システムデザインに関する研究促進

社会システムデザインに関する研究が必要となる領域が何であるかを継続的に検討し、特定された領域について、長期的な視点にたった政策提言、具体的な法整備の必要性の特定と方向性提示、技術普及で必要となる補完的な技術開発の特定。

(イ) 継続的なリスクアセスメントの実施

内閣官房で着手している重要インフラの相互依存性解析を広範に実施することや、官民連携しての現在のインターネットで観測される情報セキュリティ攻撃事象の収集と解析に着手。

---

2 (Digital Forensics) 不正アクセスや機密情報漏洩などコンピュータに関する犯罪や法的紛争が生じた際に、原因究明や捜査に必要な機器やデータ、電子的記録を収集・分析し、その法的な証拠性を明らかにする手段や技術の総称。

（ウ）ベストプラクティスの収集と活用

内閣官房がベストプラクティスの収集に努め、別に定める政府統一的基準に含まれるガイドラインに、個々のベストプラクティスの活用方法を含めることで、各府省庁でのベストプラクティスの活用を促進。

（エ）人材育成

①情報セキュリティ技術の研究開発・技術開発に従事する人材育成の強化。

②広くITの研究開発・技術開発に携わる人達を対象に情報セキュリティについて理解し、既存成果を具体的に活用する能力を持たせる。

③ITを運用するオペレータが、情報セキュリティの理解と活用法の体得。

①、②については、大学、大学院などの高度IT人材育成機関による教育カリキュラムの開発と実施、③については官民が実施しているIT人材資格制度において情報セキュリティ活用能力を求めるよう制度を変更することを、内閣官房が関係省庁や関係諸団体に対して働きかける。

（オ）プライバシーの適切な取扱い

プライバシー保護の強化に向けて、①認証機能の評価、②合理的な匿名性保証基盤の確立に向けた取組みが不可欠。このため、これらの研究状況を把握するとともに、必要となる技術的要素を特定。

（カ）IPv6の利活用推進

政府は、各府省庁のネットワーク基盤である霞が関WAN、各府省庁内ネットワーク及び電子政府システムをIPv6に対応させる。同時に、民間におけるIPv6利活用をより一層推進し、我が国の世界最高のブロードバンド基盤を、技術レベルの面からも最先端とする取組みを強力に推し進める。

５ 「グランドチャレンジ型」研究開発・技術開発の推進

○ 「グランドチャレンジ型」研究開発・技術開発とは

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的開発を行う、「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。

○ 情報セキュリティ領域における「グランドチャレンジ型」研究開発・技術開発の実施

「グランドチャレンジ型」領域としては、現時点において、例えば次のようなテーマが考えられる。

①コンピュータウィ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。

②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。

③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。

④認証等の基礎となるトラストポイント[3]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。

⑤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。

3 (Trust point)電子商取引などでユーザはCA（Certificate Authority）（電子的な身分証明書を発行する機関）が発行する証明書をアプリケーションで利用する。その際、ユーザはルートCA、もしくはいずれかのCAを信頼し、そのCAが発行する証明書は正しいという前提に立って証明書を検証する。ユーザが信頼するCAはそのユーザにとっての「トラストポイント」と呼ばれる。

委員名簿

【委員長】

佐々木　良一	東京電機大学教授

【委員】

河田　惠昭	京都大学防災研究所所長
志方　俊之	帝京大学教授
篠田　陽一	北陸先端科学技術大学院大学教授
須藤　修	東京大学大学院教授
田尾　陽一	セコム株式会社顧問
中西　晶	明治大学助教授
西尾　章治郎	大阪大学大学院教授（文部科学省科学官）
宮川　晋	ＮＴＴコミュニケーションズ株式会社先端ＩＰアーキテクチャセンタ・経営企画部（兼務）担当部長
米澤　明憲	東京大学大学院教授

（五十音順、敬称略）

（参考）技術戦略専門委員会報告書までの検討の経緯

【情報セキュリティ政策会議】

２００５年　７月１４日　第１回会合

セキュリティ分解専門委員会及び技術戦略専門委員会の設置について

２００５年　９月１５日　第２回会合

「第１次情報セキュリティ基本計画（仮称）」の骨子と方向性について

【情報セキュリティ政策会議技術戦略専門委員会】

２００５年　８月２２日　第１回会合

（１）セキュリティ文化専門委員会及び技術戦略専門委員会の設置について
（２）会議の公開等について
（３）情報セキュリティ政策会議の概要について
（４）我が国における情報セキュリティに係る技術戦略の推進についての問題意識について
（５）政府による情報セキュリティ関連研究開発・技術開発の現状について
（６）技術戦略に関する問題点の抽出と論点の整理についての検討

２００５年　９月２１日　第２回会合

情報セキュリティ技術戦略の骨子と方向性についての検討

２００５年１０月１２日　第３回会合

技術戦略専門委員会報告書骨子（案）についての検討

２００５年１１月　４日　第４回会合

技術戦略専門委員会報告書（案）についての検討