CRDS-FY2006-SP-12

ATTAATC A AAGA C CTAACT CTCAGACC
AAT A TCTATAAGA CTCTAACT
CTC G CC AATTAATA
TTAATC A AAGA C CTAACT CTCAGACC
AAT A TCTATAAGA CTCTAAC
TGA C CTAACT CTCAGACC

戦略イニシアティブ

情報セキュリティの統合的研究推進

― 技術・法律・運用管理の一体化 ―

0101 000111 0101 00001
001101 0001 0000110
0101 11
0101 000111 0101 00001
001101 0001 0000110
0101 11
00110 11111100 00010101 011

独立行政法人科学技術振興機構 研究開発戦略センター
Center for Research and Development Strategy Japan Science and Technology Agency

Executive Summary

本戦略イニシアティブは情報セキュリティの研究開発推進方法として技術・法律・運用管理を一体化した新しい試みを提案するものである。具体的には、情報通信技術者、情報システム運用管理者、法律専門家からなる研究開発検討プロジェクトを編成して、技術・法律・運用管理の統合面から情報セキュリティ問題を検討した上で、抽出された課題の研究開発を推進することを提案する。

情報システムは社会の重要インフラとして社会・組織と密接な係わりがあり国民生活・社会経済活動においてなくてはならないものとなっている。このような状況の中で、行政機関や企業からの重要情報や個人情報の漏洩等の情報セキュリティ問題が社会的な問題になってきている。これらの問題は、社会・組織の仕組みと不可分であり社会の仕組み、規制、運用などのあり方も含めて統合的に検討することが必要である。

しかしながら、現在までは技術・法律・運用管理のそれぞれの面から独立に研究開発・検討がなされており、有機的連携が取れているとは言い難い。そこで本戦略イニシアティブでは技術・法律・運用管理を一体化した研究開発推進を提案する。提案内容をより具体的に示すために、情報セキュリティが関連するサービス事業を例に示す。

（1）サービス事業を推進しようとするサービスプロバイダーがプロジェクトを推進する責任者として、そのサービス事業を所掌する府省の協力も得て、対象とするサービスについて産学官一体となったプロジェクト体制を組む。そのプロジェクトの中で、情報通信技術者、情報システム運用管理者（国レベル、民間レベル）、法律専門家が、既に実施されているサービスの実証試験で発生した社会制度面での問題、プライバシー問題などの問題点等を基に、技術・法律・運用管理の統合面から情報セキュリティ問題を一体となって検討し課題を抽出する。抽出された課題を技術・法律・運用管理のそれぞれの面から研究開発・検討を推進する。

（2）プライバシー問題に対する不安を払拭できるように、産学官共同でプロトタイプシステムを構築しテストベッド（例えば特区）で具体的に規制の強化・緩和などを実施してみながら、研究開発成果を検証する。

（3）いろいろなサービスが社会で実用化されると、社会の価値観、人の意識も変化することも予想されるため、社会の価値観変化なども取り入れた検討を継続的に行うことが重要である。従って、研究・設計・構築→提供・使用→評価→再設計を繰り返しながら継続的に研究開発を推進する。

また、情報セキュリティ研究開発に関しては、重要性が認識されているにもかかわらず研究者の数は少ないのが現状である。本戦略イニシアティブを推進することにより、統合的情報セキュリティを検討できる技術者を育成することも提案する。

本戦略イニシアティブを推進することにより、以下の効果が得られる。

（1）サービス利用者が利便性を損なうことなく、情報セキュリティも保護される、より高いセキュリティを保証するサービスが実用化できるようになり、サービス利用者が安心してサービスを享受できるようになる。

（2）サービス事業者に対してのみ過大な社会的責任の負担を負わせることなく、サービスプロバイダーの責任範囲、運用機構の仕組み、不正防止のための規制なども検討され、それらが明確化されることが期待できるので、サービスプロバイダーが新しいサービス事業をしやすくなる。その結果、多くのサービス事業が世の中に広く普及するため、経済効果も大きく、産業界も活性化する。

（3）ネットワーク社会の安全･安心な情報システムの実現に必要な情報、コンピュータサイエンス、通信、電子、ソフトウェアなどの基盤的な学問・技術の発展を牽引する原動力となる。

CONTENTS

1. 情報セキュリティの統合的研究推進とは

統合的情報セキュリティの研究推進とは情報セキュリティに関する研究開発を行う際、技術・法律・運用管理を一体化して推進することである。具体的には、情報通信技術者、情報システム運用管理者、法律専門家からなる研究開発検討プロジェクトを編成して、技術・法律・運用管理の統合面から情報セキュリティ問題を検討した上で、抽出された課題の研究開発を推進することを提案する。

情報システムは社会の重要インフラとして社会・組織と密接な係わりがあり、国民生活・社会経済活動においてなくてはならないものとなっている。このような状況の中で、行政機関や企業からの重要情報や個人情報の漏洩等の情報セキュリティ問題が社会的な問題になってきている。これらの問題は全ての情報システムに共通の問題であり、社会・組織の仕組みと不可分で社会の仕組み、規制、運用などのあり方も含めて統合的に検討することが必要である。

特に情報セキュリティの研究開発に関しては、ファイル交換ソフト「Winny」の悪用による情報漏洩や著作権法違反、犯罪組織によるフィッシングを用いた詐欺事件などの対策は法律、運用方法なども含めて技術・法律・運用管理を一体として研究開発を行うべきものである。しかしながら現状では技術・法律・運用管理のそれぞれの面から課題を抽出し、その課題のみが研究開発され（【コラム１】参照）、社会の仕組み、規制、運用などのあり方も含めた統合的な研究開発は十分ではない。そこで技術・法律・運用管理を一体化して情報セキュリティを研究開発する推進方法を提案する。

情報セキュリティが重要となる具体的な例（サービス事業）で示すと、まずサービス事業を推進しようとするサービスプロバイダーがプロジェクトを推進する責任者として、そのサービス事業を所掌する府省の協力も得て、プロジェクト体制を組む。そのプロジェクトには、情報通信技術者、国レベルおよび産業界での情報システム運用管理者、法律専門家が参画する。検討に際しては、既に実施されているサービスの実証試験で発生した社会制度面での問題、プライバシー問題などを基に、技術・法律・運用管理の統合面から情報セキュリティ問題を検討し、研究開発課題を抽出する。その課題を技術・法律・運用管理面から研究開発し、その成果をインテグレーションしテストベッド等で評価検証する。いろいろなサービスが社会で実用化されると、社会の価値観、人の意識も変化することも予想されるため、社会の価値観変化なども取り入れた検討を継続的に行うことを提案する。

また、情報セキュリティ研究開発に関しては、重要性が認識されているにもかかわらず研究者の数は少ないのが現状である。本戦略イニシアティブを推進することにより、統合的情報セキュリティを検討できる技術者を育成することも提案する。

コラム１　今までの研究開発推進

今までの情報セキュリティの研究開発においては、技術と法律と運用管理を一体化した情報セキュリティの研究開発の推進が必要であるにもかかわらず、情報技術者は、法律を一種の拘束条件として考え、技術のみでセキュリティ問題を解決しようと研究開発を推進してきた。また法律の検討に関しては、その犯罪判例に基づいて法律内容の改正、法律体系の整備などを行うため、法律は後追いの状態であった。また、情報通信技術の進展は早く、新しく開発された技術が実用化されるまでの時間が短いのに対し、法律に関しては法律成立までに多くの時間を要するなど時間軸が大きく異なるという現実もある。さらに、両者で使用する専門用語の違いもあり、お互いに相手の用語を理解し議論できるようになるまでに多くの時間を要するという現実もあり、連携した検討が進んでこなかったと考えられる。

研究開発の一例として技術面から見ると、ウィルス発生、不正侵入などの情報セキュリティ問題が発生した場合、緊急に対応する必要があるため、その対策はそのウィルスや不正侵入毎に対症療法的でパッチ等による修正を行っている。その結果、アプリケーションソフトウェアに至る所で修正がなされたり、ウィルス対策ソフトウェアパッケージがヴァージョンアップされたりしてシステム全体が複雑化してきている。そのため、情報システムの運用管理者／ユーザなどもシステムを完全に理解している状況ではなくなってきているという問題も抱えている。

各府省もこれらの問題に対応しようと技術面に重点を置いたファンディングを行い、不正侵入防止、不正のトレース技術などの応用研究に継続的に取り組んでいる。また、オペレーティングシステム、プログラム記述言語、暗号化技術などの情報セキュリティ基盤技術開発にも取り組んでいる。（詳細は付録Ⅰ参照）。

2. 情報セキュリティを統合的に研究推進する意義

ユーザにとって便利なサービスを提供するためには、そのユーザに関連するいろいろな情報をセンシング・処理して利用する必要があるが、そのためには情報の帰属問題（センシングされた情報の内容は誰のものか？）、情報のアクセス・利用権問題（誰が情報にアクセスして利用・処理できるか？）、自己情報コントロール問題（自分の情報を誰がどのように制御及び操作できるか？）など、基本的な事項を明確にする必要がある。しかしながら現状では、このような基本的な事項すら明確化されないままに、技術面からのみの情報セキュリティの研究開発、実証試験が行われている状況である。

そのため、技術・法律・運用管理を一体化した情報セキュリティ研究開発を推進することは大きく以下の三つの意義がある。

(1) 高セキュリティかつ使い勝手のよいサービスの享受

技術のみで情報セキュリティを解決しようとすると、サービスシステムのソフトウェア構成が複雑なものになると同時に、使い勝手も悪くなると考えられる。しかしながら、上記で述べた基本的事項を明確にした上で、法律に係わる課題、運用管理に係わる課題等も含めてセキュリティ問題を解決することにより、ユーザが利便性を損なうことなくセキュリティも保護され、かつ使い勝手のよいサービスを享受できることが期待できる。

また、法規制やガイドラインをバウンダリーとして技術検討を行うのではなく、社会制度、規制、運用などのあり方も含めて検討するため、不正侵入や盗聴などの不正を抑制するための法律やガイドライン、不正発生時の刑罰、被害者を救済するための法律やガイドラインなどの検討も事前に行える。そのため、盗聴などの不正に対しても、ユーザの貴重な財産が失われたりするようなことが少なくなると期待できる。

(2) 産業界活性化への貢献

情報セキュリティ問題が発生し世の中で大きく取り上げられると、企業が過剰反応し企業活動が萎縮してしまうケースが見られた。本戦略イニシアティブの推進により、サービスを提供する事業者に対してのみ過大な社会的責任の負担を負わせることなく、サービスプロバイダーの責任範囲、運用機構の仕組み、不正防止のための規制なども事前に検討されるため、企業が新しいサービス事業をしやすくなる。

また、技術のみで情報セキュリティ問題を解決しようとすると解決すべき課題の数が多くなると同時に、その開発スペックも複雑で高いレベルのものとなる可能性がある。本戦略イニシアティブを推進することにより、研究開発課題の絞り込み、過剰なスペック開発の回避も期待でき、サービス事業化に必須の情報セキュリティ研究開発の期間短縮が期待できる。

その結果、多くのサービス事業が世の中に早く普及するため、経済効果も大きく、産業界も活性化する。

(3) 融合分野での新しい技術の進展

サービス事業が経済的に成立するかを評価する手法などの研究開発を推進するため、自然科学と社会科学とを融合した分野での新しい技術の進展に貢献できる。

また、情報通信技術者、情報システム運用管理者、法律専門家が一堂に会して検討を進めることにより、それぞれの専門家間の垣根が取り払われることが期待できる。その結果、法律・運用管理面の検討を行う際に、情報通信技術の従来技術の展開もしやすくなる。例えば、法律の検討を実施するために判例の蓄積等は現在行われているが、判例の蓄積に留まらず、事例分析や法律の解釈等に対しても情報処理技術の適用等が進み、判例の分析時のサポートが期待できる。

3. 情報セキュリティ研究の統合的推進方法

情報通信技術者、情報システム運用管理者、法律専門家からなる研究開発検討プロジェクトを編成して、技術と法律と運用管理を一体化した情報セキュリティの研究開発を以下のフローに従って推進する。ここではサービスシステムを例にとって示す。推進方法の概略は図１の通りである。

① 統合的に検討すべき課題の抽出

参画メンバーが一堂に会して、社会制度、規制、運用などのあり方も含めて統合的に検討すべき課題等を抽出する。

この際、今までに発生した社会的な問題があれば、その問題を詳細に分析した上で検討を行うことが望ましいが、新たなサービス事業が社会で実用化される前にセキュリティ問題の検討を開始するため、検討する際には実際の判例などが存在しない場合もある。その際には、技術評価を目的として既に進められている実証試験で発生した社会的な問題を基に、社会制度、規制、運用などのあり方も含めて統合的に検討すべき課題等を抽出する。

また、サービス利用者の視点に立って、発生が予想されるセキュリティ問題も検討し、課題等を抽出する。

② 抽出された課題の技術・法律・運用管理面からの研究開発及び検討

上記で抽出された課題を技術・法律・運用管理面からの研究開発課題に分解し、それぞれの面から連携を取りながら研究開発・検討を推進する。

③ 研究開発及び検討結果のインテグレーション

サービス事業を実用化するために、情報セキュリティ問題に対する不安を払拭できるように上記②項で研究開発及び検討された結果をインテグレーションしてプロトタイプシステムを構築する。そのプロトタイプシステム構築は産学官共同で行い、研究開発成果が企業の新製品開発にスムーズに反映できるようにする。

④ テストベッド構築による成果の評価

テストベッド（例えば特区）で具体的に規制の強化・緩和などを実施してみながら、研究開発成果を検証する。

⑤ SPIN モデルによる継続的な研究開発検討の推進

いろいろなサービスが社会で実用化されると、社会の価値観、人の意識も変化することも予想されるため、社会の価値観変化なども取り入れた検討を継続的に行うことが重要である。

従って、研究・設計・構築→提供・使用→評価→再設計を繰り返す SPIN モデル（【コラム３】参照）を取り入れて継続的研究開発を推進する。この際、プロジェクト参画メンバー自身がサービス利用者視点に立って検討することはもちろん、消費者団体等の一般市民からの意見をヒヤリングすることなども考慮する。

また、次章の研究開発課題概要で述べる「共通認識として明確化すべき項目例」の全ての項目に関して、情報通信技術者、情報システム運用管理者、法律専門家が合意に至らないような場合も発生すると予想される。その際は三者間で共通認識として得られた項目をベースに研究開発

を推進し、SPIN モデルによる開発推進方法で開発を廻すことも考える。

なお、研究開発検討プロジェクトへは以下のようなメンバーが参画することが必要である。

① 推進責任者

具体的サービス（例えば物流サービス）を事業化しようとするサービスプロバイダーがプロジェクトを推進する責任者として、そのサービス事業を所掌する府省の協力も得て、対象とするサービスシステムについて産学官一体となったプロジェクト体制を組む。

② 研究開発統括者

技術・法律・運用管理面の研究開発・検討の統括者を決め、その統括者が強い指導力及び権限を持って研究開発するようにする。研究統括者は情報通信技術者が担うことが望ましい。

③ 研究開発・検討メンバー

情報セキュリティ技術研究開発を行っている産学官の技術者、セキュリティ認証などを実施している機関の専門家、実際のサービス事業を推進するサービスプロバイダーの運用管理責任者、サービス内容に関して詳細を熟知している情報システム製作企業の技術者、情報通信やセキュリティの訴訟に詳しく、実務として担当している法学者・弁護士、必要であれば自治体の担当者などの実務を理解しているメンバーの参画を求める。

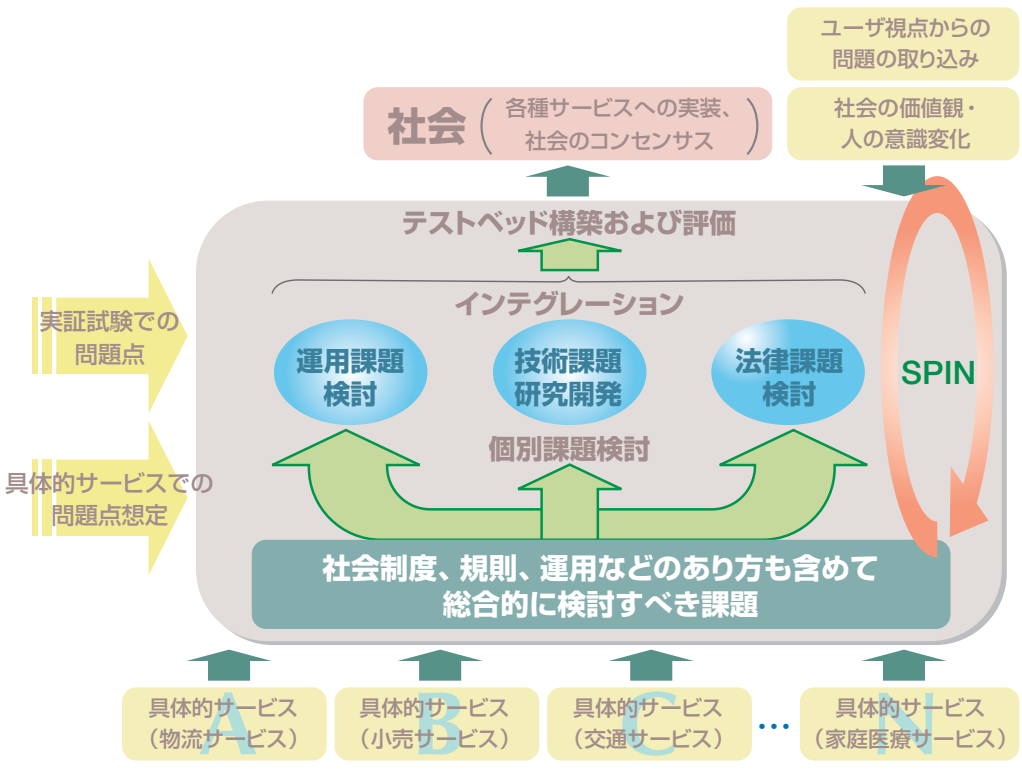


図２　具体的な研究開発の推進方法

コラム 2　関連する行政への期待

本戦略イニシアティブを推進することにより、情報通信技術者、情報システム運用管理者、法律専門家が一体となった研究開発が推進できるようになるが、さらに本戦略イニシアティブを強力に推進するためには、関連する府省が以下のことを支援することが重要である。

(1) 技術・法律・運用管理を一体化した情報セキュリティ研究開発推進の必要性発信

情報セキュリティ問題が国家的課題であることは既に認識されているが、技術・法律・運用管理を一体化した情報セキュリティ研究開発推進の必要性も国民、研究開発技術者、行政担当者に認識してもらうよう積極的に情報発信を行う。

(2) 研究開発・検討の推進支援

必要となったサービス事業毎の研究開発・検討推進プロジェクトの発足を支援すると同時に、情報通信技術者、情報システム運用管理者、法律専門家の一体となった研究開発・検討推進を支援する。

(3) 専門家参画要請の支援

サービス内容に関して詳細を熟知している企業の技術者、技術・運用管理面の研究開発を推進している産学官の技術者、情報通信・情報セキュリティの訴訟に詳しく実務として担当している法学者・弁護士など専門家の参画要請も支援する。

(4) 運用管理面で必要と認められた事項の推進

認証機構の仕組み、情報セキュリティ確保のためのソフトウェアの評価基準等、研究開発・検討の中で必要と認められた事項の推進を行う。

コラム 3　SPIN モデルによる継続的な研究開発

種々の情報システム開発の研究成果としては、そのシステムのプロトタイプシステムを構築し、その後実社会で使用し、評価することが求められている。評価結果を反映し新しい設計やそれに伴う新しい要素技術の開発が必要となる可能性もあり、その場合は 2 回目の開発ループを実施する必要がある。これは SPIN(SPiral-up model for Innovator Nippon)モデル[1] の考え方である。

情報セキュリティの研究開発においても同様の推進方法を行う必要がある。その図を図 2 に示す。まず、サービスシステムにおける情報セキュリティの研究開発及びソフトウェア設計・構築を行い、それをサービスシステムに実装し、利便性とプライバシー問題のバランスなどのメトリクスで評価を行った上で、再設計・再構築を行う必要がある。情報セキュリティの研究開発及びソフトウェア構築の内容としては、暗号・認証技術、機器・ネットワークセキュリティ技術、プライバシー、コンテンツ保護技術、運用管理のための技術などが挙げられる。サービスシステム例としては、交通・物流サービス、スーパー・小売りサービス、家庭医療サービスなどが挙げられる。評価の観点としては、技術面からの評価、運用・ビジネス面からの評価、法規制面からの評価などが挙げられる。

図 2　SPIN（SPiral-up model for Innovator Nippon）による研究開発推進

4. 情報セキュリティ研究の統合的推進時の研究課題

技術と法律と運用管理を一体化した情報セキュリティの研究開発は多くの情報システムで必要になるが、本提案においては具体的な研究開発課題を示すために、今後増大するだろう様々なサービスシステムでのプライバシー問題を例に研究開発課題概要の提案を行う。

サービスシステムにおいては、人・物の位置情報、映像情報、環境情報（製造・生産や輸送時の温度、圧力など）などの情報を誰もが利用できて新たなサービスを提供できる仕組みができれば、サービスプロバイダーがいろいろなサービスを提供すると考えられる（付録Ⅲ章参照）。

その結果、ユーザは利便性の高いサービスを享受できるようになる反面、プライバシー問題に対する不安も大きくなる。それらのサービスにおけるプライバシー問題を解決する情報セキュリティの研究開発を効率的かつ効果的に推進するためには、まず情報通信技術者、情報システム運用管理者、法律専門家が共通認識として明確化しておくべき項目がある。プロジェクト参画メンバーの共通認識として明確化すべき項目例として以下のような項目が挙げられる。

- センシングされた情報は誰のものか？
- どんな情報まで公開するか？誰までなら公開して良いのか？
- どのような時（事件、事故）は公開しないといけないか？
- どのような情報を誰がどのように扱えるか？
- その際の責任の所在、責任範囲は？
- 自己情報コントロールのあり方は？
- 不正予防、規制遵守、被害者救済のための法律のあり方？
- センサ情報の傍受（盗聴）に関する問題？

上記項目を明確化した上で社会制度、規制、運用などのあり方も含めて統合的に検討し、課題を抽出すると、以下のような課題例が挙げられる。

（1）技術面での研究開発課題例

■ 自己情報コントロール技術

情報のコントロールをサービスプロバイダーの運用管理者が行うか、サービス利用者が行うかによって、システムアーキテクチャ構成も異なり、開発スペック即ち研究課題の困難さも変わってくる。

また、個人の持つ情報（例えば、車等の所有物でのセンサ情報）が環境問題、リサイクル問題などで情報の公開が義務づけられる場合も考えられる。そのため、それらのことも予め考慮したシステムアーキテクチャ構成にしておく必要がある。

そのシステムアーキテクチャを実現するために、いろいろな情報群を効率よく処理するための情報粒度の大きさ及びデータ構造化方式、個人認証を含めたデータへのアクセス方式、自己情報コントロール方式、匿名化方式などを研究開発する必要がある。

■ 異業種・異分野のサービスが連携可能なロバストな個人認証技術

いろいろなネットワークを形成して各種サービスが実現されることが予想される。

そのために、異種ネットワーク間での認証の仕組み、統一的な認証機構の運用方法等を決定し、異種ネットワークの分散認証技術、PKI (Public Key Infrastructure)が使えないネットワークでの認証技術などを研究開発する必要がある。

その際、サービス事業が廃止されたり統合されたりすることも考えられるため、そのようなことも想定した研究開発を行う必要がある。

■ 低価格盗聴防止技術

将来は特に、電子タグを初めとする無線を利用したサービスが増大すると考えられる。サービス利用者にとっては、利便性が増大する反面、情報が盗聴されプライバシーが侵されるという不安が大きくなるため、盗聴防止技術が重要となる。

盗聴防止技術としてはセンサ側での暗号化、リーダ側での盗聴防止処理方策が考えられるが、現状の暗号化技術ではまだコストが高くなるので、低価格チップとして搭載可能な暗号化技術などの研究開発が必要である。

あるいは、リーダ側に擬似IDを発信して正当な権限のないリーダ側からは読み取られない方式、リーダ側で認証情報を毎回変化させ暗号化する方式などリーダ側での研究開発が必要である。

■ 社会・経済的評価

プライバシー問題に関しても現在の個人情報保護法に見られるように、企業が過剰反応し企業活動が萎縮してしまう可能性がある。このような過剰反応を回避するためには、情報が漏洩した場合の企業としての事業マイナス分、過剰反応をしたことによる事業マイナス分などを的確に評価して示す研究開発が必要である。

また、情報セキュリティ問題に対するサービスプロバイダーとしての投資効果を評価するROI(Return on Investment)技術の研究開発も必要である。

(2)運用管理面での検討課題例

■ 運用管理・認証の仕組み

情報セキュリティ技術が実社会で効果的、効率的に運用されるようにするためには、組織としての認証、個人としての認証等の運用管理方法、信頼のおける認証機関（例えば、公開鍵基盤PKIの認証機関/認証局CA（Certificate Authority）のようなもの）の設置なども検討する必要がある。

■ ガイドライン検討

法律の制定、施行までには長い時間を要するため、実際の法律施行まで待ってサービス事業の実用化をしようとすると事業化が遅れる。そこで、法律の施行に先立って、運用管理のガイドラインによって対応することによりサービス事業の早期実現を目指す必要がある。そのためには、法律に先行した以下のような運用管理のガイドラインを検討する必要がある。

- サービスプロバイダーに対しサービス事業の認可を与えるようにするためのガイドライン（認可を取得すれば事業化でき、企業の社会的責任も明確にするもの）
- サービス事業普及を促進させるためのガイドライン
- 不正を抑制するための罰則等のガイドライン
- 問い合わせや苦情に関する責任体制のガイドライン

■ データ構造等の標準化

企業がサービス事業に新規参入できるようにしたり、サービス事業へ

キラーアプリケーションを提供できるようにして市場拡大を目指すためには、センシングされた情報のデータ構造の標準化などを含め、プラットフォームとしてどのようなアーキテクチャ構成にすべきか検討しておく必要がある。海外との連携が必要なサービス事業については、国際標準化の活動は特に重要である。

(3)法律面での検討課題例

■ 実証試験結果、想定事象に基づく各種規定の検討

具体的なサービス事業を例題として、その実証試験等で発生したプライバシー問題を基に検討を進めると同時に、発生が予想されるプライバシー問題をサービス利用者の視点に立って検討する必要がある。運用管理面で述べたガイドライン検討内容の法規制面からの検討の他に、以下のような項目を法律面から検討を行う必要がある。

- 罰則と責任分担の明確化
- センサ情報の帰属・アクセス・利用権
- 自己情報コントロールの権利
- センサ情報の傍受（盗聴）

■ 条例のあり方、時限法の導入などの検討

個人情報保護法の「情報」という定義に関しては地方（条例）に任せきりであり、その条例に従って企業が運用管理しているのが現状である。しかしながらプライバシー情報に関しては国として統一し、条例のあり方等も検討することが必要である。

また、グローバルなビジネス展開を支えることのできる枠組み（例えば時限法の導入など）の検討も必要になる。

5. 科学技術上の効果

本戦略イニシアティブではアルゴリズム、モデル化など技術面の研究開発のみに留まらず、認証の仕組み作り検討、ガイドライン作成及び法規制検討、プロトタイプ製作による実証試験評価まで実施するため、以下のような多くの効果が得られる。

（1）自然科学と社会科学とを融合することにより、新たな情報科学技術の進展に貢献する。例えば経済学との融合による ROI 研究等が進展する。

（2）今後予想される電子マネーや電子投票などの社会基盤、医療、ライフサイエンス分野でのプライバシー問題に展開することが期待できると同時に、その分野の研究開発が加速される。

（3）情報セキュリティ問題解決には多くの工学が必要になるため、情報セキュリティ基盤技術、コンピュータ科学、情報通信工学、システム工学などの研究が促進され、情報通信関連産業の技術開発が促進される。

（4）ネットワーク社会での情報セキュリティを確保するためには、組織、制度、行政サービス等に関する研究開発も必要になり、法律学、経済学などの発展も期待できる。

6. 社会・経済的効果

本戦略イニシアティブの推進により、以下のような多くの効果が得られる。

（1）組織的な運用・管理、早い段階からの法規制面でのサポートが可能となるため、サービス利用者が利便性を損なうことなく、プライバシーも保護されるサービスを利用できるようになる。また、盗聴・改竄などによってサービス利用者の貴重な財産が失われたり、サービス利用者に重い負担を負わせたりすることを避けることが期待でき、ユーザが安心してサービスを享受できるようになる。

（2）情報セキュリティ機能が強化されるため、各種サービス事業に対する不正・攻撃等で経済、産業、社会の機能がストップするような致命的事態も回避することが期待でき、世界を魅了するネットワーク社会を実現できるようになる。その結果、第三期科学技術基本計画の中で「世界一安全・安心な国」を掲げている我が国の存在感をアピールすることができる。

（3）企業の事業化認可取得条件、認証機構設置、サービス事業普及促進、不正侵入や盗聴等の不正抑制などのガイドライン策定あるいは法律制定も検討するため、企業のみに過大な社会的責任を負わせることなく、サービスプロバイダーの事業責任範囲を明確にすることが可能になり、企業がサービス事業をしやすくなる。また、既に実証試験等で技術評価が行われている多くのサービス（例えば物流サービス、小売りサービス、家庭医療サービスなど）が早期に事業化・普及すると考えられる。

さらに戦略イニシアティブ「IRT（IT と RT の融合）」[2] の中でも提案をしているセキュリティ監視サービス、遠隔サービス、構造物・自然災害の診断システム、最適広域環境測定システム、統合交通・輸送システムなど新たなサービス創出も期待される。

その結果、多くのサービス事業が世の中に広く普及するため、経済効果も大きくなると同時に、産業界も活性化し、世界で勝ち抜く産業競争力の強化が実現できる。

7. 時間軸に関する考察

以下のことを考えると、本研究開発はできるだけ早期にスタートし、技術面、運用管理面の研究開発は、実用化を目指してテストベッドによる検証を含め5年程度で行う必要がある。また、ガイドライン・法制度の提案も5年以内に実施する必要がある。研究開発終了後は技術面の成果をスムーズに企業へ移行でき、企業がサービス事業を推進できるようにする必要がある。

(1)電子タグ、監視カメラなどの情報が増大しつつあり、社会的側面を含む情報セキュリティ問題の体系的な研究開発、およびその研究開発への投資の必要性は叫ばれているが、その研究開発は少ない。

(2)電子タグを利用した各種サービスの実証試験では技術評価のみ実施されているが、プライバシー問題等を含めた社会制度面での評価は未実施の状態であり、社会制度面の課題を開発しないと早期事業化できない。

(3)総合科学技術会議の情報通信分野推進戦略、内閣官房情報セキュリティセンターの第1次基本計画なども2006年からスタートし5年間で実施すべき課題等を抽出しているが、それらの課題の時間軸と整合性が取れた研究開発課題でもあり、早急に研究開発を実施する必要がある。

なお、セキュリティを確保したサービスが社会に実装された場合、社会変化、人の意識変化も踏まえた、さらなるセキュリティ向上が望まれるので、研究開発は継続的に実施する必要がある。

8. 検討の経緯

本プロポーザル作成に当たっての経緯、およびその過程における結論は以下の通りである。

（1）白浜俯瞰ワークショップ開催[3]
（平成16年1月29～31日）
① 情報セキュリティ研究開発の重要性が指摘された。

（2）産学官の技術者による検討会開催（平成17年5月20日、6月28日）
① 「技術と法律と管理」の総合的観点から研究領域を検討する必要があるとの結論を得た。
② 法律専門家も含めて検討を実施することとした。
③ 日本が強い組込みシステムにおけるセキュアなOS開発も必要であるとの結果を得た。（戦略プログラム「組込みシステム用ディペンダブルOS」[4]として作成済み）

（3）技術者、法律専門家での検討会開催（平成17年9月16日、11月16日、12月25日）
① 「技術と法と管理」総合面からの情報セキュリティ検討の必要性を確認した。
② 技術面からと法律運用面から研究領域が存在するかワーキンググループを発足し、研究開発課題を検討することとした。

（4）情報セキュリティ基盤研究に関するG－TeC（米国）実施
（平成18年1月9～13日）
① 技術・法律・運用管理を一体化した情報セキュリティ研究開発に関する課題の必要性は認識されているが、研究開発はまだ開始された段階である。
② どちらかと言えばROIなど経済効果を評価する技術の研究開発の方に重点が置かれている。

（5）技術面の検討ワーキンググループ（WG）、法律運用面の検討WGを発足し、WG検討会を開催
（法律運用WG：平成18年4月27日、5月22日、6月19日、8月7日、技術WG：平成18年6月19、26日）
① プライバシー問題に絞って検討を実施した。
② 本プロポーザルで提案する研究開発課題を抽出した。
③ 推進方法についても討議した。

付　録

Ⅰ　我が国の情報セキュリティ取り組み現状

Ⅱ　海外の情報セキュリティ取り組み状況

Ⅲ　サービス事業におけるプライバシー問題例

付録

Ⅰ．我が国の情報セキュリティ取り組み現状

インターネットでの不正アクセス、情報漏洩などの犯罪に対する今までの対策は対症療法的でパッチ等による修正が多く、情報システム全体が複雑化してきているという問題点はあるものの、以下のような技術・運用管理面からその都度対応してきた。法律面の対応としては、不正等の判例に基づいて法律内容を訂正したり、法律体系の整備を行ったりするため、法律は後追いの状態であると言われている。

① 技術面での技術開発：認証技術、侵入検知・防御システム、ウィルス対策など
② 運用管理面での技術開発：入退室管理、情報収集、対策普及・指示など
③ 法律面での検討：刑罰などの法制度の見直し・整備など

このような状況下で、各省庁も情報セキュリティ技術の強化を図るために、付表１に示すように文部科学省、総務省、経済産業省が積極的に研究開発領域を指定した上でファンディングを行い、継続的な研究開発に取り組んでいる。大学、産業界、独法研究機関はそれらのファンディングを活用して、「セキュリティ情報の分析と共有システムの開発」、「コンピュータウィルスや不正アクセスなどのサイバー攻撃への対処」、「企業・個人の情報セキュリティ対策事業」などの研究開発を実施している。

また、大学、産業界、独法研究機関も付図１に示すように、今後研究開発すべき課題として基盤的な研究開発、技術・法律・運用管理を一体化した研究開発課題を挙げている。

付図１は情報セキュリティ技術を基盤研究技術、暗号・認証技術、機器・ネットワークセキュリティ技術、運用管理と関係する技術および法律と関係する技術のカテゴリーに分けて整理したものである。それぞれの技術カテゴリーにおいて、現在関連府省が開発・検討を推進している課題、今後開発・検討が期待される課題に分けて整理している。基盤研究技術の中のセキュアなOS、セキュアプログラミングに関しては文部科学省のＨ18年戦略目標「高セキュリティ・高信頼性・高性能を実現する組込みシステム用次世代基盤技術の創出」の中で、科学技術振興機構のCREST「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」として研究開発が推進されるようになった。

この図の中で、特に技術・法律・運用管理を一体として研究推進すべきと考えられる課題についても明示した。標準化活動など既に進められているものもあるが、これらは新たに開発された技術の標準化などがあり、常に検討すべき課題である。

Ⅱ．海外の情報セキュリティ取り組み状況

主要な国の情報セキュリティの全般的な研究開発に関し、国レベルでの対応を付表2に、研究開発課題例を付表3に示す。欧米とも積極的かつ継続的に研究開発を推進しているが、特に米国が進んでいる。表からも判るように、技術・法律・運用管理を一体化した情報セキュリティ研究に関する課題は、米国I3P (Institute for Information Infrastructure Protection)で進められている「法律・政策・経済に関わる問題」、NSFでの「ネットワークシステムの安全性・セキュリティ・プライバシー」、英国のBristol大学で進められている「法律及び公的ポリシー問題」、ドイツのDarmstadt大学で進められている「情報関連法及びサイバー関連法」程度である。

技術・法律・運用管理を一体化した情報セキュリティ研究には、プライバシー問題以外にサイバーフォレンジクス、著作権問題、リスク評価、コスト評価、ROIなども考えられるが、米国でもどちらかと言えばROIなど経済効果を評価する技術の研究開発の方に重点が置かれているようである。例えば、CMUでは Information Systems Management (ISM) 研究所のSTIM（Security Through Interaction Modeling）センターで、ビジネスプロセスの信頼性とリスクを評価する研究、Perdue大学のCERIASでは、リスク評価、セキュリティの経済的側面などについて研究が開始されている[5)]。

また、PITAC(President's Information Technology Advisory Committee)[6)]の中でも以下のような10項目の研究開発推進を提言している。その中で情報セキュリティ対策を破る非技術的事項への対策を挙げ、プライバシー保護、リスク解析、コスト評価など心理学的、社会学的、制度的、法律的および経済学的な非技術的な対策も含めて人間の行動に基づく研究が必要であると提言している。

① 認証技術

② セキュリティプロトコル
③ ソフトウェア工学とソフトウェア品質保証
④ トータルシステムセキュリティ
⑤ モニタリングと検出
⑥ 異常軽減と回復方法
⑦ Cyber Forensics: 犯罪者捕獲と犯罪行為の阻止
⑧ 新技術のためのモデルとテストベッド
⑨ 評価指標、ベンチマーク、最良事例
⑩ 情報セキュリティ対策を破る非技術的事項への対策

Ⅲ．サービス事業におけるプライバシー問題例

ネットワーク社会のイメージを付図 2 に示す。ネットワーク社会では、電子タグが多くの製品に取り付けられるようになると考えられる。また超小型無線装置が種々のセンサに内蔵され、センサ同士が無線で自律的に情報をやり取りし状況認識を行うようになると考えられる。そのため、ユーザはリアルタイムで便利なサービスを利用できるようになる反面、プライバシー問題に対する不安も大きくなると考えられる。（但し、これらのサービスは全てがプライバシー問題に関係する訳ではない。）ネットワーク社会で考えられる主なサービス例において、その効果、及びプライバシー問題例を以下に示す。

① 小売りサービス

消費者にとっては、農産物や商品の生産者などの各種情報を参照することが可能になり、安全な食品か？商品が本物か偽物か？などの判定も可能になる。例えば農産物であれば、生産者、生産日、生産地、使用した肥料、物流時の温度状態などの情報を得ることができ安全な食品を購入できる。また、いろいろな商品を購入しても一括して精算できレジ等で混雑することがない。さらには自分の嗜好に合ったマーケティング情報の提供を受けることができるようになる。

小売業者にとっては、精算の効率化、POS(Point Of Sales System)レジとの連動による在庫管理・発注管理の効率化、盗難防止対策、偽造品判定、今後のマーケティング情報としての活用による売上増への貢献などのメリットがある。

しかしながら、消費者にとっては、購入した商品がどのようなものか無線等により盗聴される可能性がある。例えば、農産物の種類の他にも、下着の種類・色、本の種類なども盗聴されて悪用される可能性がある。また、小売業に蓄えられた情報をトレースすることにより、購買履歴も管理されそれらの情報が盗聴されて悪用される可能性がある。

② 交通サービス

車の所有者やドライバーにとっては、道路・駐車場の混雑状況がリアルタイムで把握でき、スムーズな移動が可能になる。また、車が故障した場合も車のいろいろな情報をサービス業者へ送信することができるため、故障発生時にもサービス提供業者に素早い対応をしてもらえる。さらには、車が盗難に合っても道路側に設置されたリーダの情報等から車の所在を突き止めることができる。

サービス提供業者にとっては、道路・駐車場の混雑情報提供、交通違反を起こしそうな時の警告、車の盗難・故障発生時の早急な対応、車部品の環境保全・リサイクル情報としての管理等が行えるようになる。

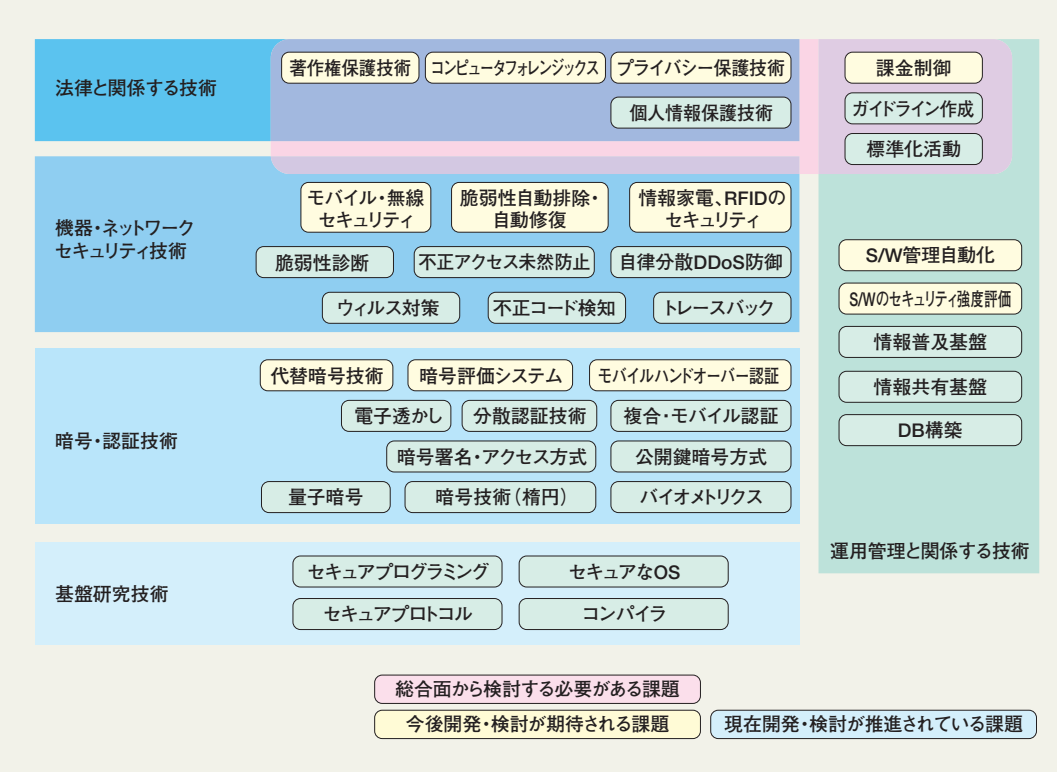
しかしながら、車の所有者にとっては移動経路、搭乗者、目的地などが個人の行動履歴として蓄積されるため、それらの情報が盗聴・読み取られ第三者によって悪用される可能性がある。

③ 家庭内医療サービス

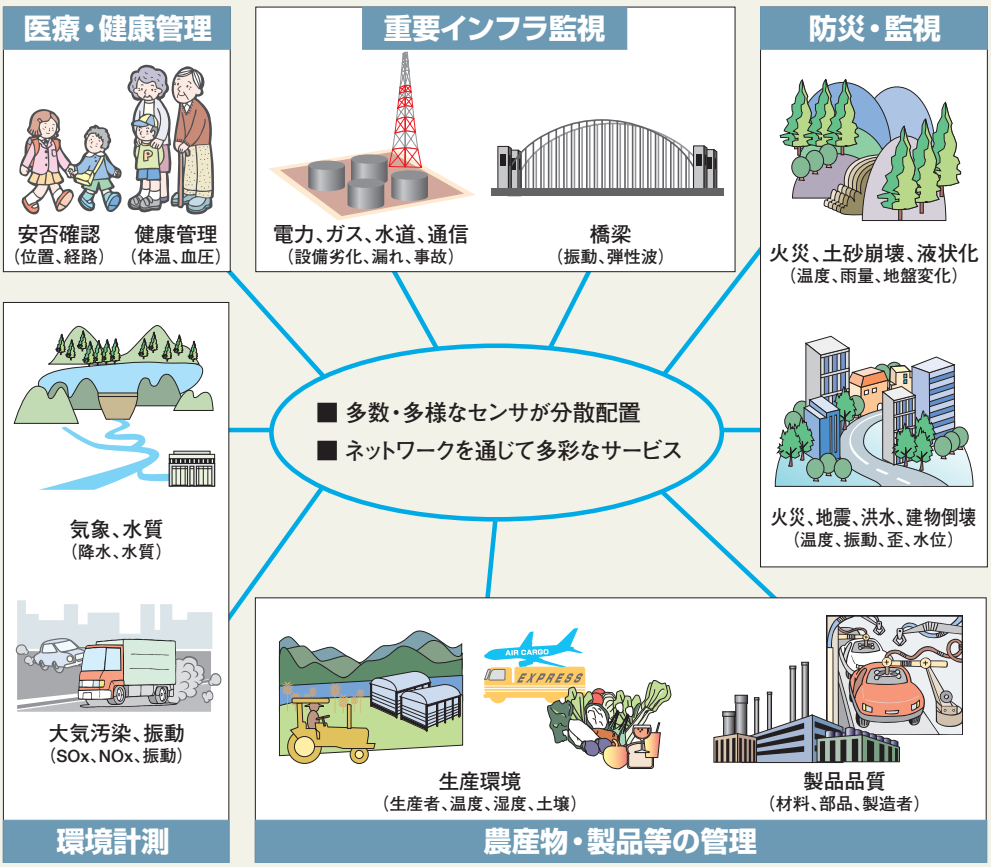
サービス利用者にとっては、日常生活において血圧、体温、尿検査などを自分でセンシングし、その情報を病院へ送ることにより遠隔から日常生活健康診断および生活指導などを行ってもらえる。また、家庭において倒れたりした際に、家庭内でセンシングされた情報、病院で蓄積されている病歴・アレルギー性等の情報を用いて救急車での緊急対応の参考データとなる。

サービス提供者にとっては、緊急処置により人命救助に貢献することができる。

しかしながら、サービス利用者にとっては、個人の健康状態・病歴などが読み取られ、改竄・悪用される可能性がある。



付図1　情報セキュリティ技術俯瞰（運用管理および法律と関係する技術）



付図2　今後予想されるユビキタスネット社会のイメージ

付表1　各省庁の情報セキュリティ研究に対する投資（平成16年度）

単位:億円
経済産業省は17年度計画

省庁	課　　題	投資額	投資額（合計）	備考（出展）
文部科学省	重要課題解決型研究等の推進「セキュリティ情報の分析と共有システムの開発」	6.4	6.4	（科学技術振興調整費）
総　務　省	(1) コンピュータウイルスや不正アクセスなどのサイバー攻撃への対処 ①ネットワークセキュリティ基盤技術の研究 ②コンピュータウイルスなどに関する研究基盤の構築	24.7 （13年度～） 1.8 （15年度～）	26.5	情報通信分野における情報セキュリティ対策について（総務省情報通信政策局情報セキュリティ対策室2004年7月）
総　務　省	(2) 電子商取引や新規ビジネスの創出に資するネットワークの安全性・信頼性の確保 ①高度ネットワーク認証基盤技術に関する研究開発 ②タイムスタンプ・プラットフォーム技術の研究開発	10.4 （16年度～） 1.7 （15年度～）	12.1	
経済産業省	(1) 企業・個人の情報セキュリティ対策事業 (2) 先進社会基盤構築ソフトウェア開発事業	16.5 6.1	22.6	平成17年度情報政策の概要（経済産業省商務情報政策局情報政策ユニット）

付表2　各国の研究開発概要

国　名	研　究　開　発　概　要　国
米　国	ファンディング機能（約1億2,200万ドル/2004年）としての役割を果たし、SF,DARPA,NIH,NASA,NIST、諸大学などの構成機関を通じて研究開発を推進。必要技術のR＆Dを推進するNITRD、国防を目的としたサイバーセキュリティ関連のR＆Dを推進するDARPA（2003年度予算：約3,000万ドル）、サイバーセキュリティR＆D法に基づき公募型のR＆Dを推進するNISTおよびNSFなど国主導によるR＆Dが中心
英　国	国防省管轄下の研究機関であるDERAから分割民営化されたQinetiQ、Royal Holloway University、University of Cambridge等の大学の研究機関などによる国などからの委託・助成によるR＆Dが中心 Research Councilを通じて、これらのR＆Dの投資の可否を判断する仕組みを運用
独	情報セキュリティ分野のR＆Dは連邦政府のITセキュリティ施策の中枢的な機関であるBSI（4,522万ユーロ/2002年）において僅かに実施されているが、大半は連邦政府などからの委託・助成を受けたFrauhofer（約10億ユーロ/2002年）、Max Planck Society（約12億4千万ユーロ）等の民間が中心。
仏	国防総事務局の傘下で情報セキュリティ分野の技術調査・研究を担うDCSSI（約800万ユーロ/2003年）のほか、青少年・国民教育・研究省の傘下でファンディング機能を果たし、INRIA（約1億1,400万ユーロ/2002年）、CNRS（約25億3,300万ユーロ/2002年）との共同研究として、ITセキュリティに関する研究プログラムを推進するMRNTや、財政・産業省の傘下で中小企業を主な対象として公募型のR＆Dを推進するDIGITIPなど国主導によるR＆Dが中心。
韓　国	情報通信部管轄下のKISA（約462億ウォン/2003年）、ETRI（約3,783億ウォン）により国主導によるR＆Dが推進されている。KISAが実用化に近い領域を担当し、ETRIが基礎的な研究及び技術開発を担当するという役割分担。

「ネットワークセキュリティ技術の研究開発の在り方に関する調査研究」調査報告書（通信総合研究所2004年3月30日）を基に作成

NSF：　全米科学財団
DARPA：国防高等研究プロジェクト庁
NIST：　国立標準技術研究所
NITRD：ネットワーキング／情報技術研究開発
DERA：　Defense Evaluation and Research Agency
QinetiQ：民間企業
BSI：　連邦情報技術安全局
DCSSI：情報システムセキュリティ中央局
INRIA：国立情報科学オートメーション研究所
CNRS：国立学術研究所
MRNT：新技術研究担当省
DIGITIP：産業・技術・情報・郵政局
KISA：　情報保護振興院
ETRI：　電子通信研究所

付表3　各国のセキュリティ研究機関が取り組んでいる研究開発テーマ

国　名	研　究　機　関	研　究　内　容
米　国	University of Washington	OS Support for Application Installation, Execution, and Management in an Untrustworthy World
	NYU, MIT, UCLA	Securing Untrusted Software with Interposition
	Princeton, Naval Postgraduate School, USC-ISI	Secure Core for Trustworthy Commodity Computing and Communications
	CMU	Real-time Mach
	IBM	Design and Implementation of a TCG-based Integrity Measurement Architecture SHype
	UCB	システムコールのアクセス制御
	CITI	Preventing Privilege Escalation
	Stanford University	Terra：A Virtual Machine-Based Platform for Trusted Computing 静的プログラム解析、モデルチェッカーを用いる脆弱性解析 データライフタイムに関する研究
	University of Iowa	擬似サイバーアタック生成システムとセキュリティツール検証環境
	University of Southern California	Cyber Defense Technology Experimental Research network プロジェクト
	I3P	法律・政策・経済に関わる問題
	NSF	ネットワークシステムの安全性・セキュリティ・プライバシー
英　国	QinetiQ	安全性及びセキュリティ管理、システムアシュアランス及び評価、システム検証
	Royal Holloway University	セキュリティ管理、携帯電話セキュリティ
	University of Cambridge	セキュリティプロトコル、形式検証、セキュリティシステムの信頼性、ハードウェアセキュリティ、アイソレーション研究（XEN）
	University of Bristol	計算的整数論、法律及び公的ポリシー問題
独	Fraunhofer Institute	携帯サービス向けセキュアサイト用サービスプラットフォーム
	Max Planck Society	クリティカルソフトウェア
	DKFI	電子トランザクションにおける信頼性
	Universität Darmstadt	セキュア OS、モバイルアプリケーション及び OS のセキュリティ、情報関連法及びサイバー関連法
	Universität Bochum	デジタル著作権管理における OS のセキュリティ
	Technische Universität München	セキュアシステム開発を支援するツール開発、組み込み型セキュリティ、携帯端末のセキュリティ
	Universität Karlsruhe	アイソレーション研究（L4）
仏	INRIA	セキュリティプロトコル、セキュリティソフトウェアの検証環境、セキュアなソフトウェアコンポーネント
	CNRS	情報セキュリティ管理ポリシー
	Ministry of Research	セキュリティポリシー検証システム、メモリのダイナミックチェック、セキュアオブジェクト指向プログラム、アドホックネットワークにおけるプロトコルのセキュリティ、ユーザ端末デバイスのセキュリティ
韓　国	韓国情報保護センター	情報セキュリティ管理体系、乱数評価
	韓国電子通信研究院	モバイル通信におけるセキュリティ、無線 LAN セキュリティ
	韓国情報戦略開発院	無線 LAN 連動セキュリティプラットフォーム技術
	韓国先端科学技術大学	ネットワーク脆弱性予測分析に関する研究

「情報セキュリティ研究のあり方に関する研究会」報告書（産業技術総合研究所 H16 年 4 月 30 日）を基に作成

DKFI ：Deutsches Forschungszentrum für Kuenstliche Intelligenz GmbH
INRIA：Institut National de Recherche en Informatique et en Automatique
CNRS：Centre National de la Recherche Scientifique

参考資料

1）科学技術未来戦略ワークショップ（電子情報通信系俯瞰 WS）報告書(CRDS-FY 2005-WR-16）

2）戦略イニシアティブ「IRT － IT と RT の融合－」（CRDS-FY 2004-IN-01）

3）科学技術未来戦略ワークショップ（電子情報通信系）報告書(CRDS-FY 2003-WR-02）

4）戦略プログラム「組込みシステム用ディペンダブル OS」（CRDS-FY 2005-SP-05）

5）G-TeC 報告書「情報セキュリティ基盤技術（米国）」CRDS-FY 2005-GR-07

6）REPORT TO THE PRESIDENT February 2005「Cyber Security : A Crisis of Prioritization」
(President's Information Technology Advisory Committee)

本戦略イニシアティブは以下の先生方のご協力を得てまとめたものである。

（五十音順）

石井　夏生利	情報セキュリティ大学院大学
江崎　浩	東京大学
大蒔　和仁	産業技術総合研究所
岡田　仁志	国立情報学研究所
岡村　久道	英知法律事務所
国領　二郎	慶應義塾大学
佐藤　慶浩	日本ヒューレット・パッカード株式会社
篠田　陽一	北陸先端技術大学院大学
新保　史生	筑波大学
鈴木　正朝	新潟大学
砂原　秀樹	奈良先端技術大学院大学
田中　英彦	情報セキュリティ大学院大学
早貸　淳子	JP-CERT コーディネーションセンター
林　紘一郎	情報セキュリティ大学院大学
松島　裕一	情報通信研究機構
山口　英	内閣官房情報セキュリティセンター
湯淺　墾道	九州国際大学
米澤　明憲	東京大学

戦略イニシアティブ

情報セキュリティの統合的研究推進

ー 技術・法律・運用管理の一体化 ー

独立行政法人 科学技術振興機構 研究開発戦略センター

制作担当　生駒グループ

〒102−0084　東京都千代田区二番町3番地
電話　03−5214−7481
ファクス　03−5214−7385
http://crds.jst.go.jp/
平成19年2月

ATTAATC A AAGA C CTAACT CTCAGACC

CT CTC G CC AATTAATA

T AA TAATC

TTGCAATTGGA CCCC

AATTCC AAAA GGCCTTAA CCTAC

ATAAGA CTCTAACT CTC G CC

AA TAATC

AAT A TCTATAAGA CTCTAACT CTAAT A TCTAT

CTC G CC AATTAATA

ATTAATC A AAGA C CTAACT CTCAGACC

AAT A TCTATAAGA CTCTAACT

CTC G CC AATTAATA

TTAATC A AAGA C CTAACT CTCAGACC

AAT A TCTATAAGA CTCTAACT

ATTAATC A AAGA C CT

GA C CTAACT CTCAGACC

0011 1110 000

00 11 001010 1

0011 1110 000

0100 11100 11100 101010000111

001100 110010

0001 0011 11110 000101