情報セキュリティ技術に関する取り組みについて

２００４年１２月６日
内閣官房情報セキュリティセンター

「IT を安心して利用可能な環境」を実現するためには、情報セキュリティ技術の高度化と、その技術を理解した上での利用・活用が不可欠である。しかし、現状は、１）急速に拡大するＩＴ利用・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くという問題が存在している。

したがって、政府は、民間部門における取り組みとの役割分担を明確にしつつ、今後３年間に、情報セキュリティに関する技術戦略として、主に以下の政策に重点的に取り組んでいくこととする。

１．研究開発・技術開発の効率的な実施体制の構築

限られた投資の中で効率的・効果的に研究開発・技術開発を実施するために、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と継続的な見直しを行う。また、投資効率の改善のため、成果利用までを見据えた研究開発・技術開発を実施するための体制を構築し、その成果を政府が活用することを前提とした新たな研究開発・技術開発に取り組むこととする。

＜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。

(3) 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。

(4) 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。

(5) 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。

２．情報セキュリティ技術開発の重点化と環境整備

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ため、基盤としてのＩＴを強化することに直結する中長期的な目標に対する研究開発・技術開発を促進する。一方、短期的な目標設定がなされている研究開発・技術開発については、その投資効率を把握し、バランスの良い投資を行う。なお、高い投資効率が見込まれるものの民間の取組みが期待できない萌芽的研究開発に対しては政府が主体的に取り組むこととする。

＜具体的な方向性＞

(1) ＩＴ強化直結型研究への重点化

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

(2) 萌芽的研究への投資強化

①デジタルフォレンジック 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

(3) 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。

(4) 情報セキュリティ技術を支える環境整備

① 社会システムデザインに関する研究促進

②継続的なリスクアセスメントの実施
③ベストプラクティスの収集と活用
④人材育成
⑤プライバシーの適切な取扱い
⑥ＩＰｖ６の利活用推進

３．「グランドチャレンジ型」研究開発・技術開発の推進

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、中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、短期的な問題解決のための技術開発だけでなく、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・技術開発に取り組むこととする。

＜具体的なテーマの例＞

(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 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。

別紙

情報セキュリティ技術に関する取り組み