産業構造審議会情報セキュリティ部会報告書
情報セキュリティ総合戦略策定研究会報告書

情報セキュリティ総合戦略

世界最高水準の「高信頼性社会」実現による

経済･文化国家日本の競争力強化と総合的な安全保障向上

2003 年 10 月 10 日

経済産業省

戦略をまとめるにあたって

IT（情報技術）革命は、1990 年代から 2000 年前後のわずか 10 年程度で我々を取り巻く環境を大きく変えたパラダイム転換であった。その圧倒的な利便性によって、IT は今や我々の社会に欠かすことのできない基盤として浸透しており、我々の経済活動や社会生活は IT の円滑な稼動を前提として成立していると言っても過言ではない。こうした IT に対する依存度の高まりは、情報経済社会のさらなる高度化を加速する一方、金融、エネルギー、交通等の重要インフラが情報システムの事故やサイバーテロによって停止し、国の機能そのものが麻痺する危険性を顕在化している。したがって、そうしたリスクを極小化し情報セキュリティを確保する取り組みは、我々が IT 化のメリットを享受し、さらなる発展を遂げるための前提条件といえるだろう。

また、IT は、経済力、技術力、情報収集・解析力などの国際競争力や軍事力にも新たな変革をもたらした。すなわち、IT の活用は多面的な国家安全保障のバランスに直結するが、その基盤技術の多くを諸外国に依存している。こうした中で我が国は、情報経済化の進展の下で、国の主権をも脅かしかねないリスクを抱えてしまったことを直視しなければならない。

そうした状況を踏まえ、経済産業省では、我が国における情報セキュリティ政策の全体像を俯瞰する検討が必要と判断し、産業構造審議会の下に「情報セキュリティ部会」を設置、「情報セキュリティ総合戦略」の策定を行うこととした。同時に、「情報セキュリティ部会」に対し、専門的・実務的観点を付与した具体的な総合戦略案を提示する目的で、商務情報政策局長の諮問機関として「情報セキュリティ総合戦略策定研究会」が設置された。

「情報セキュリティ総合戦略策定研究会」は、2003 年 5 月から 10 月までの５ヶ月間に計 7 回開催され、情報セキュリティリスクの評価や具体的な施策を中心に綿密な検討を重ねてきた。また、その結果を受けて、「情報セキュリティ部会」は、同年 6 月から 10 月までの４ヶ月間に計３回開催され、戦略の視点や政策の全体像について活発な議論がなされた。本戦略は、こうした関係各位の献身的な努力によって完成に至ったところである。

本報告書は、戦略の考え方（第１章)、情報セキュリティ強化のための３つの戦略（第２章)、戦略実現のための具体的施策（第３章)、戦略の実現のための体制と進捗管理（第４章）で構成し、「情報セキュリティ総合戦略」を形作っている。本戦略をベースに、我が国の今後の情報セキュリティ政策が進められ、安全保障も含めた情報セキュリティ環境が確立されることを強く期待する。

2003 年 10 月

産業構造審議会　情報セキュリティ部会

部会長　　寺島 実郎

目　次

第１章
戦略の考え方

１．１．　IT の社会基盤化～社会の「神経系」を担う IT

情報技術（IT）は、1970 年代以降、軍事や科学技術計算の分野からビジネス分野へと適用領域を徐々に広げた。しかし、1990 年代後半以降、特に、インターネットを契機とする近年の爆発的な IT の普及は、単に、経済活動や日常生活への PC、インターネット、携帯電話などの急速な普及や電子商取引の拡大という次元でとらえるべき現象ではなくなりつつある。

第一に、今や、金融、物流、公共輸送、エネルギー供給、水、道路交通、医療など諸々の社会の根幹を支える制御・管理部分に、IT 関連機器やソフトウェアが目に見えない形で組み込まれ、各種社会システムの「神経系」として重要な機能を担い始めている。例えば、以下のような事例があげられる。

① 金融分野は、基幹業務の IT 化を先進的に進めてきており、日銀ネットワークや全銀ネットワークを介して金融機関同士の決済が一般化している。また、インターネットバンキングやインターネットトレーディングの普及、IT を運用に駆使した金融工学の急速な発達も注目される。

② 交通分野においても、IT の活用によって、旅客機や鉄道の安全かつ正確な運行を実現している。航空分野では、飛行計画情報や航空路監視レーダーの情報等を扱う管制情報処理システムが管制業務等の円滑な実施を下支えしている。また、鉄道分野では、車両と乗務員のスケジュールやダイヤの作成アルゴリズム、運行監視、特急列車の座席予約等が可能な電子乗車券システム等が実用化されてきた。

③ 電力分野では、電力の潮流を保つ給電指令や、事故が起こった場合の停電拡大防止のための制御指令などに、IT を活用している。また今後、電力供給の自由化範囲を現在よりも拡大し、電力取引所の機能を設ける方向になるなど、IT を活用した新たな基盤の構築が予想される。

今や、IT は、経済活動や市民生活に大きく影響をもたらすインフラの基幹の部分を支える基盤となっており、「インフラのインフラ」としての機能を果たしている。

第二に、個々の企業活動にとっても、IT は不可欠の「神経系」となりつつある。IT の利活用は、単なるインターネットによる接続や一企業内での LAN 構築というレベルを超え、顧客管理、在庫管理などの基幹的な情報の一元管理、さらには、電子タグや IC カードを通じた商品情報や顧客情報の共有、国境を越えた商品管理データベースの共有など企業の枠組みを超えた新たな次元に到達しつつある。いわば、重要な情報を伝達・共有する企業活動全体の「神経系」として急速に相互融合化を進め、社会全体にまたがる情報の相互共有、既存市場を越えた資源の全体最適化を進行させつつある。

このように、IT は、軍事・科学技術といった「電子計算機」としての用途を大きく離れ、企業経営における業務効率化、企業間における個々の取引の効率化の道具といった局面を経つつ、今や、経済、社会いずれにとっても必要不可欠な「神経系」として、その基盤を担いつつある。

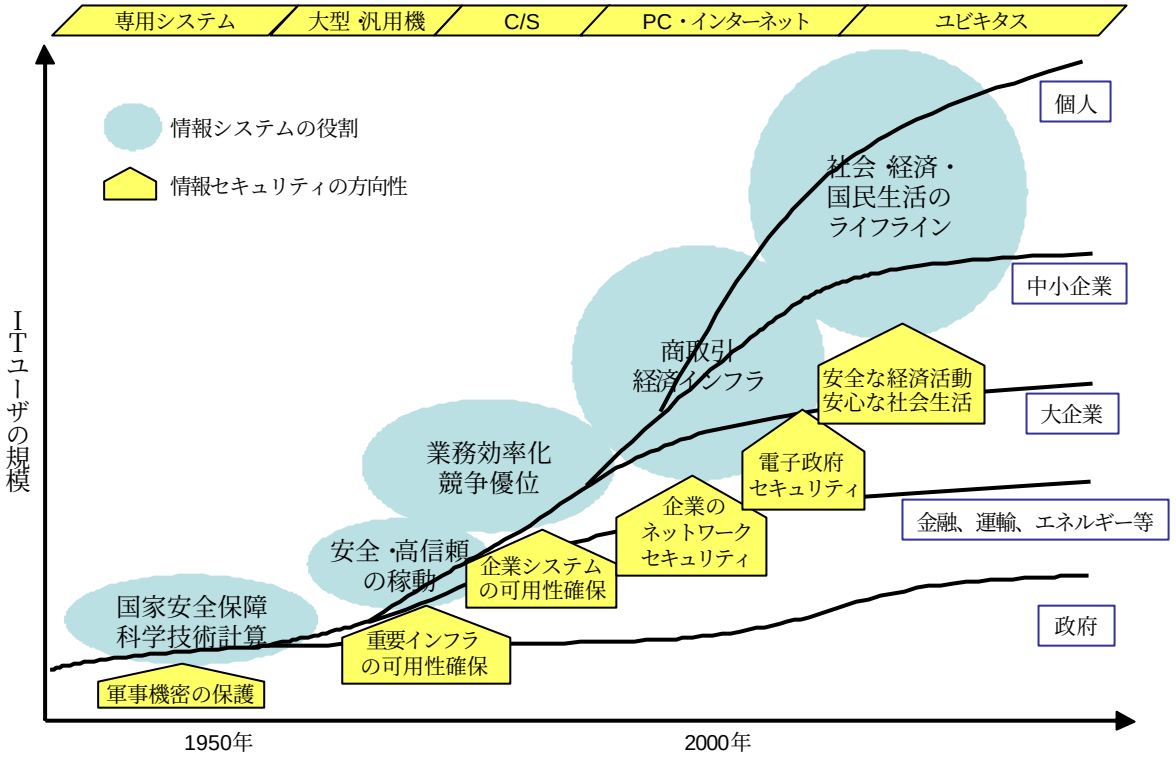

図 1- 1　IT の利活用の変遷

１．２．　社会全体が直面する新次元のリスク

実際に、こうしたITの社会基盤化は、情報セキュリティという側面から見れば、まったく新しい次元のリスクを社会全体にもたらしつつある。

歴史的視点でとらえれば、第一次（18世紀末　蒸気機関）、第二次（19世紀末､電気）に並ぶ第三次産業革命（ITをはじめとする先端技術）が生活の隅々まで急速に進行し始めた中で、これまで経験したことのなかった新しい形のリスクや犯罪、テロなどに対応していくことが求められつつあると見ることができる。

１．２．１．　リスクの拡大

第一に、個別のリスクがより全体的・国家的なレベルのリスクに転化しているという点が指摘できる。

従来、情報システムの不具合や内外からの悪意ある攻撃は、不具合を抱えたり攻撃を受けたシステムの所有者が自ら解決すべき問題であった。しかし、ITの社会基盤化に伴い、情報システムのダウン、機密漏洩、不正操作などの被害が、単に、それぞれの企業や個人の業務・生活に支障を来すだけではなく、経済活動全体の停滞や国民全体の生命・財産そのものに関わるリスクをもたらしかねない状況となっている。具体的には、次のような例があげられる。

①　情報システムのダウン

社会のIT依存度が高まっており、情報システムのダウンは業務の停止に直結するケースが多い。特に、経済活動や市民生活を支える重要インフラ[1]の機能停止は社会的影響が大きく、深刻な事態を招いている。

－　コンピュータウイルス、ワームに起因するもの

コンピュータウイルスやワーム[2]による被害は、今や社会的な問題となっている。2003年1月にはSlammerワーム[3]が、8月にはBlasterワーム[4]が出現し、わずかな期間で世界中に蔓延した。これらはソフトウェアの脆弱性[5]を突いて感

---

[1] 本戦略では、経済活動と国民生活のライフラインとして深く影響を及ぼす業種等を広く対象としており、内閣の情報セキュリティ対策推進会議（「重要インフラのサイバーテロ対策に係る特別行動計画」(2000年12月)）にて対象とされている重要インフラ７分野（情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス（地方公共団体を含む））以外にも、水道分野、医療分野、石油プラント分野等をその対象として捉えている。

[2] ネットワークを介して他のシステムへ自動的に感染することによって増殖するプログラム。

[3] 2003年1月に発生したワーム。Microsoft SQL Serverの脆弱性を標的とし、感染すると自分のコピーを大量に流し続け、ネットワークの帯域を消費する。

[4] 2003年8月に発生したワーム。Microsoft Windows OSの脆弱性を狙う。感染するとPCが再起動を繰り返す症状が発生。また、毎月16日以降または9月以降にはマイクロソフトのサイトにDoS攻撃をしかけるプログラムが組み込まれている。

[5] 何らかの理由により、性能を維持できなくなる原因となる、システムにおけるセキュリティ上の問題箇所。

染するもので、脆弱性が修正されていないとインターネットに接続しているだけで被害に遭う危険性があり、韓国では Slammer ワームが深刻なインターネット接続障害をもたらした。また、Blaster ワームの感染対象は個人も利用する OS を搭載したコンピュータであり、我が国でも個人ユーザを始め大きな被害が生じた。

－ サイバーテロ的なもの／不正アクセスによるもの

2002 年 10 月には、世界 13 箇所に設置されたルート DNS（Domain Name System）サーバに対する DDoS 攻撃（Distributed Denial of Service：分散型サービス妨害攻撃）が行われ、うち 2 箇所で一時的に機能が停止するなどの被害が発生、インターネットの構造上の脆弱性が露呈した。また、米カリフォルニア州の電力会社の送電網システムに外部者が不正侵入した事件（2001 年 6 月）や、豪クイーンズランド州で、市の水道施設の制御システムに侵入した犯人が汚水を河川や沿岸部に流した事件（2000 年 3 月）も発生している。さらに、インターネットバンキングに対する DDoS 攻撃の可能性を指摘する専門家の意見も出ている。

－ 人為的ミスに起因するもの

プログラムのバグ[6]や設定ミスのような人為的なミスが招いた情報システムの事故・事件が原因で、重要インフラ機能に影響を及ぼした事例は、金融機関の情報システム統合に伴うシステム障害（2002 年 4 月）や ATM の停止（2003 年 3 月）、日銀ネットのダウンによる金融機関間の決済停止（2003 年 7 月）、証券取引所の株価情報システムのダウン（2003 年 7 月）、FDP（飛行計画情報処理システム）のダウンによる航空ダイヤの混乱（2003 年 3 月）などが挙げられる。

② 機密情報の漏洩

－ 不正アクセスによるもの

米カード決済処理会社のシステムが不正侵入されクレジットカード番号約 800 万枚分が盗難に遭う（2003 年 2 月）など、システムへの不正アクセスによって企業の顧客のクレジットカード番号や顧客・社員等の名簿等が流出する事件は枚挙に暇がない。また、政府関係機関のシステムが不正アクセスされ、取引企業の機密情報が盗み出された事件（2001 年 12 月）のように、企業の競争力に直結する問題も発生している。

[6] プログラムがその作成者の想定と異なる挙動をとる現象、またはその原因となるプログラム上の誤り。

－　人為的なミスに起因するもの

防衛庁のシステム開発資料の一部が流出した事件（2002 年 8 月)、警察の捜査車両から捜査資料や PC の入った鞄が盗まれた事件（2003 年 1 月）など、セキュリティレベルが高いはずの機関でも問題が発生している点が注目される。また、自治体や医療機関等における個人情報の流出事故も起きている。

③ 不正操作

－　不正アクセスによるもの

不正アクセス・不正操作によって、単なる Web ページの改ざんだけでなく、実害の大きい事故・事件も生じている。

2003 年 3 月には、インターネットカフェに、入力操作を盗み取るキーロガーと呼ばれるソフトを仕掛け、入手したパスワード等を元に、1600 万円を不正に振り替える事件が発生した。

また、オークションサイトのユーザ 10 人の ID からパスワードを推察し、無断使用・販売した事件（2003 年 5 月）のように、インターネットユーザのパスワード等が盗まれて悪用される事件も増加している。

これらも、個々の企業やユーザの被害を超えて、経済取引システムそのものへの信用の問題へと発展する。

こうした事例を見ても分かるとおり、最近の情報セキュリティ関連の事故・事件は、問題を引き起こした当事者や被害に遭った当事者だけの問題にはとどまらず、周囲の取引相手、友人はもとより、さらには不特定多数への被害、経済取引システムそのものへの信用問題、社会インフラの機能麻痺など、社会経済システム全体に影響を及ぼす問題へと指数関数的に拡大していく性格を持つ。

また、通信コストの低価格化とネットワークの容量増大・常時接続化によるいわゆる「ブロードバンド化」が IT のユーザ数や取り扱うデータ量を急速に拡大させていることから、小さな一か所での脆弱性に起因する事故がシステム・ネットワーク全体に波及し大きな損害につながる可能性は飛躍的に高まっている。

１．２．２．　リスクの変質

第二に、IT のリスクは、急速な普及や技術革新に伴い、その特徴を変質させている。

①「IT のブラックボックス化」がもたらすリスク

ソフトウェアの再利用化、部品化、汎用パッケージ利用が進んだために、IT 製品や情報システムはメーカーやシステムインテグレータにとっても内部構造を理解できない一種のブラックボックスと化している。そのため、ソフトウェアの脆弱性が

開示されても、それが自社製品に及ぼす影響について正確に把握することが困難な状況にある。

また、多くのユーザにとって、IT の仕組みは既に理解しうる範囲を超えており、本来必要な、情報システムの脆弱性に対するユーザの積極的な対処を阻害する方向に作用している。

②IT 利用の多様化がもたらすリスク

企業や組織の LAN を守るため、インターネットとの接続点にファイアウォールやアンチウイルスツールを設置する形態が一般化している。しかし、ファイアウォールは、外部からの攻撃を防ぐことはできても、コンピュータウイルスに感染したモバイル PC を企業 LAN に接続して感染を広げるような、内部からの攻撃は防ぐことができない。さらに、企業 LAN への遠隔アクセスや無線 LAN といった IT の利用形態の多様化は利便性が向上する一方、新たなリスクを内在しており、技術的対策の導入がそれに追いつけない危険性がある。

③技術革新・ビジネスモデルの変化がもたらすリスク

Web ブラウザ「Mosaic」の登場後わずか 10 年で、Web を基盤としたアプリケーションはビジネスや生活を支える中核技術へと成長した。さらに今後は、Web サービス、P2P 技術[7]、電子タグ等によって組織間、業界内、異業種間をまたいだ顧客情報、商品情報など様々な情報の外部共有化が進展すると予測される。また、IPv6 や電子タグ、情報家電等の技術融合は、ユビキタス化された自律的な端末間通信時代の到来を予感させる。こうした IT の急速な技術革新は、ビジネスモデルの再構築を促す一方、例えば、顧客情報のプライバシーの確保、営業機密の漏洩防止など、新たなリスク要因をもたらすことも懸念される。

④責任所在の不明確化に伴うリスク

IT 市場は、ソフトウェアメーカー、PC メーカー、インターネットサービス事業者などがそれぞれの特性を発揮して市場を広げてきた。このため、それぞれのビジネスが独自に技術構成を高度化・複雑化させた結果、事故・事件発生時の原因特定や責任の明確化、影響分析を困難にするといった新たな問題を拡大させている。

１．２．３． 新次元のリスクへの対応と安全保障の観点から見た問題認識

こうしたリスクの拡大や変質に対応するためには、①個々の対策だけではなく、国全体として総合的にリスクを最小化する努力をする一方、②リスクの全てを未然に防ぐことはできない、すなわち「情報セキュリティに絶対はなく、事故は起こりうるもの」との前提

[7] 通常の Client/Server モデルと異なり、コンピュータ同士がネットワークを介して同等の立場で通信するモデル（Peer to Peer）。Napster や Gnutella のようなファイル交換、動画チャットが可能なインスタントメッセー

で、生じた被害を最小化・局限化し、かつ、回復力の高い仕組み、すなわち「しなやかな事故前提社会システム」を構築するといった観点から、対策を検討することが求められる。

なお、今のところ、我が国においては、経済活動全体を停滞させたり、国民の生命・財産を危機に陥れるほどの重大な情報システム事故・事件は発生していない。これは、一つには、政府や重要インフラの基幹を支えるシステムについて、インターネットとの接続やそもそもの IT 化を慎重に行っていることが事故・事件の未発生をもたらしていると言える。

しかしながら、1.2.1.で示したように、我が国に限らず海外の事例も含めると、金融や電力といった経済活動や国民生活の根幹を支える重要インフラにおける事故・事件も発生しつつある。また、IT の社会基盤化がもたらした新次元のリスクが有する特性として、愉快犯から組織犯罪、さらにテロリストやサイバー兵士のレベルまで、政府や重要インフラに対し同様の手法で攻撃をしかけうることが挙げられる一方で、国際競争力・利便性を確保するためには、基幹を支えるシステムについても IT 化は避けて通ることができない。したがって、我が国の政府や重要インフラは、今や、常にサイバーテロの可能性を意識し、安全保障の観点から、最悪のシナリオを前提に最善の対策を選択することが要求される。

すなわち、情報セキュリティの問題は、単に「安全な経済活動」を阻害するといった次元の問題にはとどまらず、我が国の安全保障確保との観点から、国家的なレベルで検討すべき問題となっている。

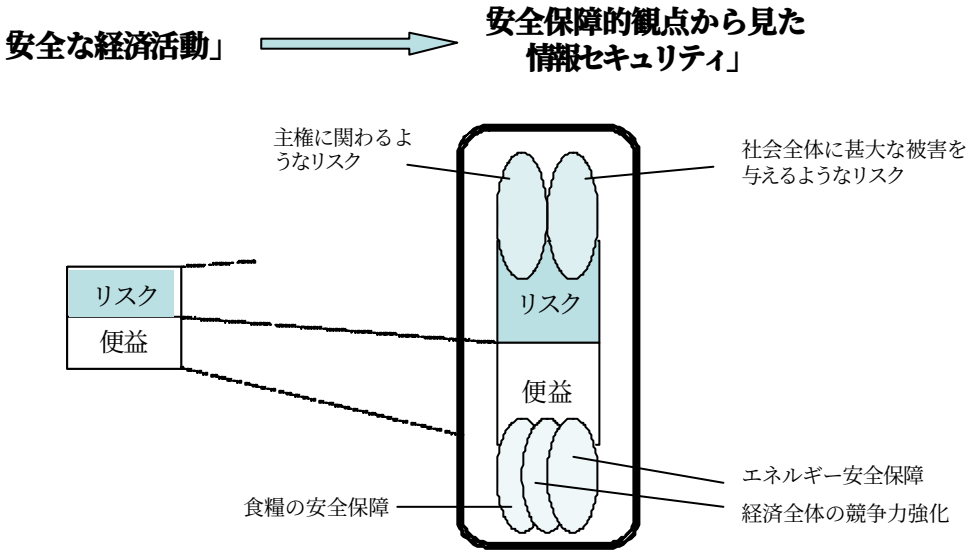

図 1- 2　安全保障的観点から見た情報セキュリティの位置付け

ジ、計算処理を分散して行うグリッドコンピューティング等の基盤技術となる。

１．３．　総合的な情報キュリティ対策の必要性

１．３．１．これまでの情報セキュリティ対策の課題

このように、情報セキュリティを巡るリスクの拡大・変質が急速に進展しているにもかかわらず、これまでの我が国の情報セキュリティ対策を見ると、個々のシステムの信頼性・安全性の確保や安全な経済活動の確保を目標とした受動的かつ対症療法的対応なものに限定されている。これまでの対策の課題は、次の４点に集約される。

①　国・自治体及び重要インフラ部門の対策が遅れている

国や自治体の情報セキュリティに対する取り組みは、先進的な企業に比べると遅れている。特に、自治体においては、電子自治体実現に向けた急激な変化に際し、セキュリティの確保が急務となっている。

また、経済活動や国民生活を支えている重要インフラについては、特に基幹システムの周辺の情報システムを中心に、実際に重要インフラ機能に影響を及ぼす事故が発生しており、今後、そうした情報システム事故によって、国民の生命・財産が脅かされる事態が発生するリスクが懸念される。

②　システムの自衛や個別取引の安全確保の段階にとどまっている

企業においては、各社内での個々のシステムに対する自衛的な対策や、個別の経済活動の安全性確保に重点を置いた対策が主であり、経営トップを含め、リスクの拡大や変質など IT の社会基盤化に伴う情報セキュリティ対策の重要性に対する認識はまだ甘い。特に、組織や産業を超えた情報共有や事故対応体制構築など、国家的なレベルからみた事故対応策については、未だ意識が希薄である。

③　対症療法的な対策しかとられていない

企業においては、情報セキュリティに係る事故が頻発しているにもかかわらず、我が身に置き換えて想定することができず、実際に被害が発生しない限り対策が進展し難い。また、対策の方向性、実施規模、実施方法などについて経営トップだけでなく現場エンジニアにとっても迷いがある。特に中小企業では、ファイアウォールやアンチウイルスなどの定番製品を導入した段階で停滞している感がある。

また、個人においても、基本的なウイルス対策さえも講じないままインターネットを利用している、リスクを回避するための自衛策を知らないままインターネットを通じた商品売買などに参加するなど、セキュリティリスクに対する認識が甘い。

このように、企業においても、個人においても、問題が起きてから対応する対症療法的対応が主であり、抜本的な対策まで踏み込めていないものが多い。

④ 政府の施策遂行において、縦割り構造での独自対応となっている

政府の情報セキュリティ政策の遂行においては、「縦割り分掌構造」の中でそれぞれの業種や所管インフラに向けた対策がバラバラに各省から打ち出されることが多かった。また、内閣官房の情報セキュリティ担当部局も、他の先進各国の情報セキュリティ政策の統括部局に比べて著しく小さな組織にとどまっている。情報セキュリティを巡るリスクの拡大・変質が進展する中で、全体の安全保障に関わる問題としての対応は不十分との意見が多い。

1．3．2.「高信頼性社会」構築による競争力強化と総合的な安全保障の向上

いわゆる 9.11 テロに直面した米国は、サイバーテロ対策を重要な国家戦略として掲げ、政府が「サイバー空間安全保障のための国家戦略」（2003 年 2 月）を発表し、実行に移しつつある。また、民間企業においても、単に IT システム上のバックアップを作るだけでなくデータ管理部門の責任者や運用要員なども含め丸ごとバックアップ会社を作る例などに見られるように、新たなリスクをにらんだ情報セキュリティ対策を経営上の当然の前提として織り込む事例が数多く見られるようになっている。

一方、我が国では、情報セキュリティ問題が「現実の脅威」であるとの認識は官民ともに薄い。したがって、政府も民間企業も情報セキュリティ対策を単なるコスト要因として扱い、もっぱら受身の姿勢で必要最小限の対応に終始してきた。しかしながら、情報経済化の急速な進展が生み出す新たなリスクや国際社会におけるテロのリスクなどを考えると、官民双方が協力しながら整合的かつ速やかに情報セキュリティへの対応を強化していかなければならない。

このためには、単に、「守り」の視点から受動的に情報セキュリティ問題に対応するだけではなく、ソフト・パワー（軍事力などのハード・パワーでなく、経済力や文化的な魅力によって国際関係上望ましい結果を導き出していくこと）に依拠する経済・文化国家日本としての重要な国家戦略の中に情報セキュリティ問題を組み込んでいくことが必要である。

我が国の一つの「強み」は、「品質・技術」に対する供給側・需要側双方のこだわり、良好な治安、官民間・企業間・地域コミュニティでの日本的な協調関係などである。情報経済化が進む中で、こうした我が国固有の「強み」と高度な情報セキュリティ対策は相互補強的に「高信頼性社会」と名付けられるような社会システムを形作ることができる（図 1-3 参照）。

より具体的に述べるとすれば、我が国が自らのポテンシャルを最大限に伸張することで目指す「高信頼性社会」とは、

1) 良好な治安と高度なセキュリティ技術に裏付けられたリアル・サイバー両面での安全社会
2) 政府、企業、個人の機密情報やプライバシー情報について、十分な可用性と管理可

能性が保証される社会

3) そのような安全社会を前提とする世界に例のない新たなビジネスモデルの群生、高齢者・女性活用型労働市場の活性化
4) 種々の協調関係を前提に成り立つ事故に強いサービス基盤の提供、そうしたサービス基盤から資源供給を受ける企業群の耐リスク能力に着目した市場評価
5) 高品質のハード・ソフトを内蔵した信頼性の高い製品群によるハイエンド市場の獲得、さらに信頼性の高い製品群に立脚した高度なサービスの提供
6) 高度な技術基盤と要求水準の高い市場に着目した海外からの直接投資の流入

などが「相互補強的」に生じる社会である。

以下に述べるように、こうした「高信頼性社会」は我が国経済・企業が「差別化戦略」を通じて競争力強化を図るための基盤となる、と同時に、21 世紀における我が国の総合安全保障強化にも貢献するものである。とりわけ、情報経済化が急速に進む中では、高度な「情報セキュリティ基盤」が「高信頼性社会」の一つの中核をなす度合いが増加していくと考えられる。

① 経済的な競争力強化

「神経系」としての IT の急速な社会経済への浸透は、物質的豊かさを問う「工業経済」から知恵とノウハウの活用の巧みさを問う「情報経済」へと向かう社会変革を全世界的に引き起こしつつある。その中で、今後、我が国社会が情報を社会共通の資産として生かせるのか、それとも、単に各個人や企業の持ち物として終わらせてしまうのかは、社会に張り巡らされた IT という「神経系」が利便性とともにもたらす新たなリスクや脆弱性を、如何に社会全体としてコントロールできるかにかかっている。

情報セキュリティ対策によって、情報の可用性と管理可能性が十分に保証された IT 基盤があれば、我が国企業は安心して重要情報を戦略的に他社・他部門や顧客と共有し、いち早く市場の動きに即した資源配分の変化を達成するなど企業競争力強化の基礎を作ることができる。また、様々な企業が安心して使える IT 基盤があれば、リスクプレミアム[8]の構造的低下を通じた海外からの投資誘引にもつながり、また、企業と従業員が社外においても安心して情報をやりとりできる環境があれば、急速に進展する高齢化と人口減少における経済活動の活性化及び雇用の増大にも貢献する。

② 総合的な安全保障の向上

これまで、エネルギーの安定供給の確保、食糧安全保障の確保、交通など、国家的な信頼性・安全性基盤を支える重要インフラや政府のシステムは、安全性・信頼性確保の

[8] リスクを引き受ける者（投資家、金融機関など）から、リスクの大きさに応じて要求される「リターンの上乗せ」、「割増金利」あるいは「保険料」のこと。例えば、リスクが高い企業は、リスクプレミアムが高いため、高

問題から、IT が十分に活用されないことが多かった。しかし、情報セキュリティ対策の向上により、十分な安全性・信頼性が担保されるようになれば、より効率的かつ多様な社会インフラが実現する。例えば、災害時の社会インフラの復旧における多様な代替手段の確保、より安価かつ柔軟なエネルギーの配送管理、一つのシステム障害に対して回復力の高い交通管理システムの構築など、我が国の総合的な安全保障をより高い水準で実現することにつながる。

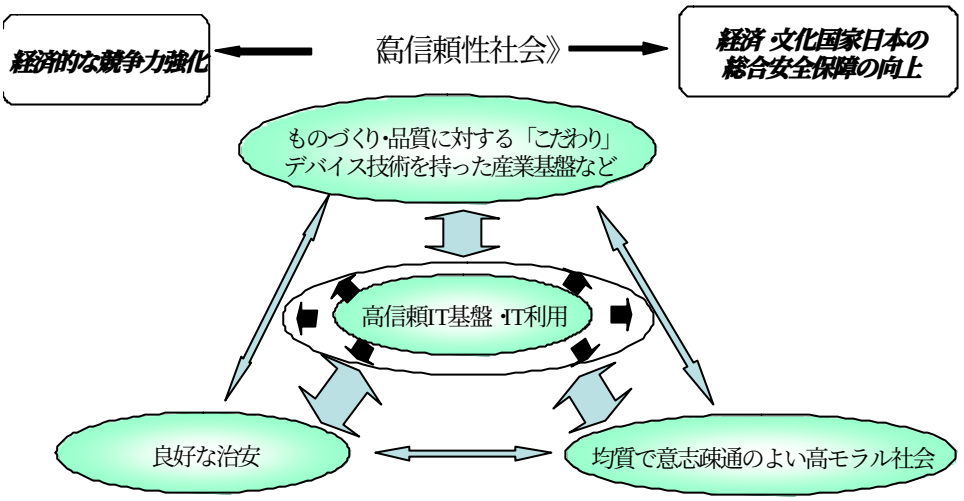

図 1- 3　「高信頼性社会」の構成要素

いリターンがなければ投資家は投資しにくい。

第２章
情報セキュリティ強化のための３つの戦略

２．１．　情報セキュリティ強化のための３つの戦略

第１章で示したとおり、IT は、一層、社会基盤としての役割を強め、社会生活にとっても、経済活動にとっても、不可欠な「神経系」となりつつある。この結果、IT がもたらすリスクも、個別のものから全体的な国家的なレベルのリスクへと拡大し、個々の当事者による受け身の対応を待っていては、リスクの構造的な拡大は止まらなくなった。しかし、現在の対策は、対症療法的な個別的なものにとどまっており、こうした急激な変化に対する国家的な視点からの対策は十分にとられていない。

経済的な国際競争力の強化や、「安全・安心」面での我が国本来の強みを活かすといった観点からも、「IT は危ないから使わない」といった受け身の対応は許されない。物質的豊かさを追求する「工業経済」から、知恵とノウハウの活用の巧みさが問われる「情報経済」へと向かう社会変革が全世界的に引き起こされつつある中で、IT を社会インフラとして他国以上に一層有効に使いこなし、かつ、「世界最高水準の『高信頼性』」を同時に獲得していくことは、もはや不可欠の課題と言える。

このため、本戦略では、経済・文化国家日本の強みを活かした「世界最高水準の『高信頼性社会』の構築」を「基本目標」として位置付け、その要となる「情報セキュリティ対策」について、従来の個別対症療法的対応からの脱却を図るとともに、国全体としての資源の重点的・戦略的投入強化に向けた３つの戦略を掲げることとする。

戦略１：しなやかな「事故前提社会システム」の構築（高回復力・被害局限化の確保）

第一に、事前に事故を予防することや、起きた事故に対症療法的に対応することばかりではなく、「情報セキュリティに絶対はなく、事故は起こりうるもの」との前提で、事故・事件からの迅速な回復力の確保を図った「しなやかな社会システム」を構築する。すなわち、全体として事故の回避（予防）、被害の最小化・局限化及び回復力の確保が達成されるよう、官民が連携して総合的な視点から対応を強化する。

その際には、市場機能、企業間競争を主体とし、さらに、官民連携のための仕組み作りや市場機能の補完のための標準的モデルの提示などの役割に公的セクタが積極的に踏み込むことが必要である。なお、その際の公的セクタの取り組みが特定の技術やビジネスモデルを強要しない中立的なものとなるよう留意することが必要である。

戦略２：「高信頼性」を強みとするための公的対応の強化

第二に、「安全・安心」面における日本本来の「強み」を活かしながら、「高信頼性」を我が国の比較優位にまで高めていくために、国家的視点に立脚した公的対応を強化する。公的対応としては、「戦略１」を構成するような狭義の「情報セキュリティ対策」にとどまらず、結果として「高信頼性社会」の実現に結果として不可欠となる、ソフトウェア開発技術における信頼性の高い技術基盤や、プライバシーの侵害、

サイバー犯罪などに対応するための法的基盤など、市場全体の底上げを図るような技術基盤・制度基盤両面にわたる対応を総合的に強化していくことが必要である。そして、公的対応を強化するにあたっては、個々の取り組みにおける国際的な調和に十分に配慮しながら、国際的な協調を積極的に図っていくことが必要である。

戦略３：内閣機能強化による統一的推進

「情報セキュリティ対策」を強化していくにあたっては、ただ闇雲に政府関与を強化するのではなく、「完全な政府施策領域」と「官民連携・協力領域」の区別を意識しながら、限られた専門的な人材資源や予算資源を適切に配分・管理していく必要がある。また、個々の対応においても、個別の主体がバラバラに対応をとるのではなく、官民や官官、民民それぞれの関係性の中で効果的な対応がとられるよう資源のポートフォリオ管理やそれぞれの連携・協調管理を行うことができる一元的な体制が必要である。

２．２．節以降で、それぞれの戦略について、さらに詳細にふれることとする。

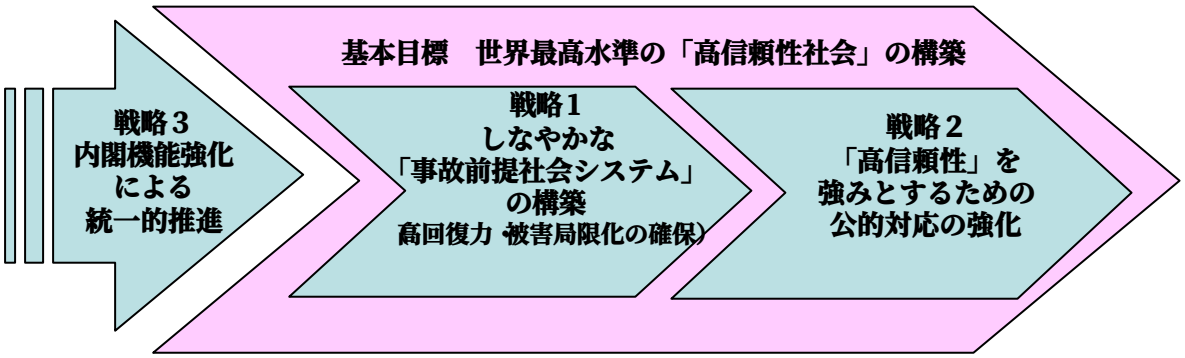

図 2- 1　情報セキュリティ強化のための３つの戦略

２．２．戦略１：しなやかな「事故前提社会システム」の構築（高回復力・被害局限化の確保）

情報セキュリティを巡るリスクの拡大と変質を考えると、まず、個々の対策に委ねるだけではなく、国全体として総合的にリスクを事前予防的に最小化する努力をすることが必要である。

一方で、全ての事故を事前に予防しようとする考え方は、その実現性において効率的ではない。事前予防的な事故の回避に加えて、「情報セキュリティに絶対はなく、事故は起こりうるもの」との前提で、被害の最小化・局限化、回復力の確立を図る仕組みを、あらかじめ構築しておくことが必要である。すなわち、事故の回避（予防）、被害の最小化・局限化、回復力の確立が最適に組み合わされた対策を講じることができる基盤を構築する。

政府関与の方向、すなわち、政策的対応についていえば、政府が 100%結果を保証することを前提に完全な事前予防策をとろうとすれば、技術的な内容まで特定した技術基準等の規制を課す、特定の製品以外の市場参入を認めないなどの対応となる。しかし、この場合、仮に事故を予防することができたとしても、他方で、急速な技術やビジネスモデルの進歩・革新の中で、IT がもたらす利便性は相対的に損なわれ、「高信頼性社会」を目指す「攻め」の政策の前提条件たる、情報経済の時代に勝ち抜く国際競争力の獲得という点で、後れをとることになる。

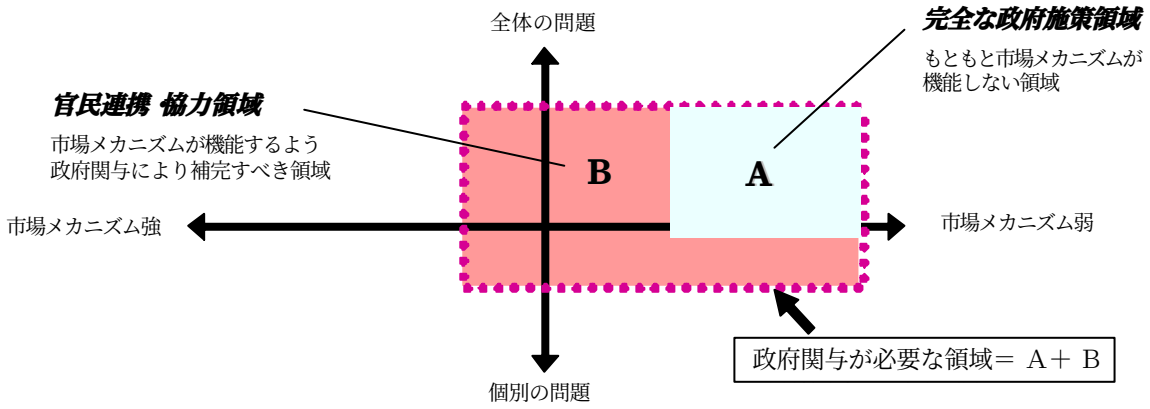

図 2- 2　情報セキュリティ分野における政府関与のあり方

そのためには、従来の官民役割分担のあり方を再度見直し、情報セキュリティの分野における政府関与の「リバランス」を、新たな考え方の下に明確化することが必要である。

政府の役割は、本来上図でいうＡ領域、すなわち、個別の主体では全く解決がつかず、市場メカニズムも全く及ばない「完全な政府施策領域」を中心に検討されるべきである。

しかし、それだけでは、国・自治体や重要インフラ部門以外に、拡大・変質するリスクに悩まされるケースを解決することができない。「しなやかな『事故前提社会システム』の構築」（高回復力・被害局限化の確保）を大胆に目指し、国家レベルでの総合的な安全保障問題に対応していくためには、「完全な政府施策領域」（A領域）自体を拡大するというアプローチではなく、市場メカニズムを活用しながらも積極的に政府がその機能を補うという官民が連携協力して取り組む中間領域的な考え方が必要である。そして、国・自治体及び重要インフラ部門等「完全な政府施策領域」への投資とともに、「官民連携・協力領域」（B領域）に対して積極的に投資をしていくこと（すなわちB領域の拡大）で、情報セキュリティ戦略の国家規模的強化を図っていかねばならない。

ただし、「官民連携・協力領域」を拡大する際には、事故の完全予防という考え方を改め、トータルで事故の発生と被害の極小化を図るという観点から、市場中立性、技術中立性に十分配慮した、市場競争を最大限に生かした対策をとることが必要である。

具体的には、より費用対効果の高い対策の実施に向けた予防対策の見直しと強化と、ある程度の確率で事故が発生しうることを受け入れた上で、技術選択の自由度やビジネスモデル選択の自由度を事業者から奪わないような形での技術中立性、市場中立性が保証された事故対応策の抜本的強化が必要である。そのことが、事前に事故を予防することや、起きた事故に対症療法的に対応することばかりでなく、被害を最小化、局限化し、回復力の高い、「しなやかな社会的仕組み」を構築することにつながっていく。

解決を図らなければならない現在の課題には、事故原因を作った者と当面の解決手段を持つ者との乖離、及び、それぞれへの市場による対策への動機付けの欠如といった特徴がある。これを踏まえ、国・自治体、企業・個人が個別に対応しただけでは明らかにされないリスクの開示及び意識の向上に向けた社会的な仕組み作り（セキュリティ意識の向上）や、日常的な脆弱性対策における政府、ソフトウェアベンダ及びシステムユーザの間の連携（セキュリティ脆弱性の低減）を図る。さらに、いざ事故が発生した場合の官民連携した対策手段の共有体制の国家レベルでの確立に取り組む。

また、併せて、事故発生の許容度が低い国・自治体及び重要インフラ部門における対策をこれらとは明確に差別化し、国、自治体、関係政府機関の間でも緊密な協力を得ながら、それぞれがこれらに対する抜本的な対応強化を図ることが必要である。

これらについて対策を例示すると以下のとおりである（詳細は、第３章を参照）。

【事前予防策】

①　国・自治体、重要インフラにおける事前予防策の強化

－　情報管理体制の見直しとそれに伴った技術開発及びシステム構築
－　システム調達時における IT 製品や暗号などに係る安全性基準等の利用
－　情報セキュリティ監査の実施や ISMS 認証取得の促進
－（重要インフラの）情報セキュリティ監査の実施

―サイバーテロを想定した情報セキュリティ技術の開発

② 企業・個人における新たな事前予防策

― 脆弱性に対処するためのルールと体制の整備
― コンピュータウイルス等の警戒情報を提供する機能の整備
― 情報セキュリティに関わる多面的な実務家・専門家の育成手法の検討
― プロフェッショナル向け資格認定制度のあり方の検討
― セキュリティインシデント[9]対応機関におけるセキュリティ技術者研修の実施
― 情報セキュリティ分野の研究・教育人材の育成
― 政府による積極的な普及啓発活動の実施
― 義務教育段階からのセキュリティリテラシー教育の実践
― 経営者・従業員を対象としたセキュリティ研修の強化
― 個人ユーザが負担感なく安全な IT 製品・サービスを利用できる環境整備

③ 技術とセキュリティマネジメントの両輪からなる既存の事前予防策の強化

― IT セキュリティ評価・認証制度の普及促進
― 暗号の安全性評価の強化
― 安全性向上に向けた技術・製品・サービスの開発
― 暗号・認証技術を用いた安全な情報流通体制の確立
― 情報セキュリティ監査の実施や ISMS 認証取得の促進
― 情報セキュリティ格付けのあり方の検討
― 情報セキュリティ関連の国内基準・標準の全体的な整合性の検討

【事故対応策】

④ 国・自治体・重要インフラにおける事故対応策

― 国・自治体における情報共有・活用体制の見直し
― サービス継続・復旧計画の策定ガイドラインの整備
― 情報システム事故に関する省庁間の情報共有と調査委員会の設置
― サイバーテロ演習・訓練の実施
― 重要インフラにおける情報共有・活用体制の設置

⑤ 企業・個人における事故対応策

― IT 事業者間における情報共有・活用・協力体制の設置
― サービス継続・復旧計画の策定ガイドラインの整備
― リスクに対する定量的評価手法の開発
― 保険機能をはじめとする被害軽減手段のあり方の検討
― 情報セキュリティ関連の法制度上の問題点に係る検討

[9] コンピュータセキュリティに関係する人為的事象。例えば、リソースの不正使用、サービス妨害行為、データの破壊、意図しない情報の開示や、さらにそれらに至るための行為などがある。

２．３．戦略２：「高信頼性」を強みとするための公的対応の強化

物質的豊かさを追求する「工業経済」から、知恵とノウハウの活用の巧みさが問われる「情報経済」へと向かう社会変革が全世界的に引き起こされつつある中で、IT の便益を他国以上に追求するとともに、他国以上の高い安全性、信頼性を達成することは、我が国の国際競争力向上の上で不可避の課題である。

具体的には、①情報経済の便益を最大限活用した競争力の高い企業群に向けた環境整備を優先するとともに、②海外からの投資を呼び込むに足るだけの信頼性の高い IT 基盤の整備、③少子高齢化の環境の中で一人あたりの生産性を上げるために安心して IT を使える環境整備、④セキュリティ意識の高い国民による最先端技術を通じた高い便益の提供を目指さねばならない。

また、①IT の活用による食糧・エネルギーなどの安全保障の向上、②脆弱性低減によるサイバーテロに強い社会の構築、③安全基盤の輸出を通じた国際貢献など、経済・文化国家日本の総合的な安全保障の向上をソフト面から強化できるだけの環境整備を行わねばならない。

したがって、「しなやかな『事故前提社会システム』の構築」（高回復力・被害局限化の確保）（戦略１）の要となる「情報セキュリティ対策」ばかりでなく、国家的な視点から個々の主体を超える共通的かつ基盤的な公的対応の強化に積極的に取り組み、情報セキュリティに関わる市場競争自体の水準の底上げを目指さねばならない。

そして、公的対応の強化においては、「安全な経済活動」と「安全保障」の両面に効果があるような投資へ重点的な配分を行うとの視点が重要である。

具体的には、国家規模での情報収集・解析機能の強化、サイバー犯罪やプライバシーの侵害を的確に防止するような法的基盤の整備を行う。また、すべての IT の導入に不可欠となる信頼性の高いソフトウェア開発技法の導入など、IT の開発や利用に携わる個々の主体では取り組めないような公的な課題について、政府自らが積極的に取り組む。そして、公的対応を強化するにあたっては、個々の取り組みにおける国際的な調和に十分に配慮しながら、国際的な協調を積極的に推進する。

これに関する対策を例示すると、以下のとおりである（詳細は第３章を参照）。

【政府による更に踏み込んだ各種対策の強化】

① 「しなやかな『事故前提社会システム』の構築（高回復力・被害局限化の確保）」
＝戦略１　の充実強化

【国の基盤となる領域のリスクへの対応】

② 情報収集・解析機能の整備

③ 一極集中・依存リスクを回避した IT 基盤の形成
④ RMA への取り組み強化
⑤ 犯罪対策の推進
⑥ プライバシー情報保護のあり方に関する検討
⑦ 情報セキュリティに関する国際協調の推進

【基礎技術基盤の確立】
⑧ ソフトウェア製造技術の高度化
⑨ セキュアプログラミング手法の確立と実用化
⑩ デバイス等基盤技術に関する産業基盤の強化

２．４．戦略３：内閣機能強化による統一的推進

「情報セキュリティ対策」を強化していくにあたっては、ただ闇雲に政府関与を強化するのではなく、「完全な政府施策領域」と「官民連携・協力領域」の区別を意識しながら、限られた専門的な人材資源や予算資源を適切に配分・管理していく必要がある。また、個々の対応においても、個別の主体がバラバラに対応をとるのではなく、官民や官官、民民それぞれの関係性の中で効果的な対応がとられるよう資源のポートフォリオ管理やそれぞれの連携・協調管理を行うことができる一元的な体制が必要である。

この理由は以下の３点にまとめられる。

第一に、事前の対策ばかりに対応が集中しても、事後対応ばかりに対応が集中しても、全体として最適化は得られない。双方のバランスが重要である。

第二に、政府・重要インフラへのセキュリティ関連投資の強化はもとより、官民連携した領域に重点的な投資を必要とするからこそ、各省庁がバラバラに資源投入すると、全体として金銭的のみならず人材的にも有限な政策資源の無駄遣いになる恐れがある。

第三に、特定商取引の安全や犯罪捜査など特定政策目的に偏った問題意識に縛られることなく、市場メカニズムの活用による経済活力の維持と安全性・信頼性の確保という全体的な視点から、我が国全体のバランスのとれた法制度、基盤整備を図っていく必要がある。

このため、具体的には、個々の政策機関における情報セキュリティ対策体制の強化を図ると同時に、内閣官房の体制を大幅に拡大し、内閣官房による重複業務の調整等一元的な推進体制を構築することが必要である。内閣官房には、我が国全体としての情報セキュリティ対策を実施する上での国家的な拠点として機能することが期待される。

具体的な対策を例示すると、次のとおりである。

【内閣官房情報セキュリティ対策推進室の機能の大幅拡大】

①政府・自治体・重要インフラなどの事故情報を総合的に収集する体制の構築
②国･自治体の機密保持等に必要な技術開発等の企画・立案
③各省庁に対するセキュリティ監査や侵入テスト等の検査の実施
④情報セキュリティに関する国としての対外窓口
⑤情報セキュリティ政策に関する各推進体制間の総合的な調整
⑥情報セキュリティ政策の実施に向けた進捗管理（プロセスマネジメント）

【統一的な推進体制の構築】

⑦各省の役割の明確化、内閣官房による各省庁における重複業務の調整
⑧政府横断的な「情報セキュリティ政策委員会」における情報共有、統一的実行

２．５．e-Japan 戦略との関係

本戦略は、「e-Japan 重点計画 - 2003」の一部を詳細化したものと位置付けられる。具体的には、重点政策の一つである「高度情報通信ネットワークの安全性と信頼性の確保」について、安全保障的観点を補足し、同計画で提示されている官民の役割分担の原則「民を主役に官が支援する」や、民間が意欲を持って IT 革命を推進していくための政府の役割である

①大きな方向性の提示
②市場競争を重視した規制改革・競争政策
③民間の活動に対する動機付け
④最小限の投資、格差是正、安全性確保
⑤政府自らの活動の効率化・高度化と資源の効率的配分

の５項目に則って、具体的な施策に展開したものである。

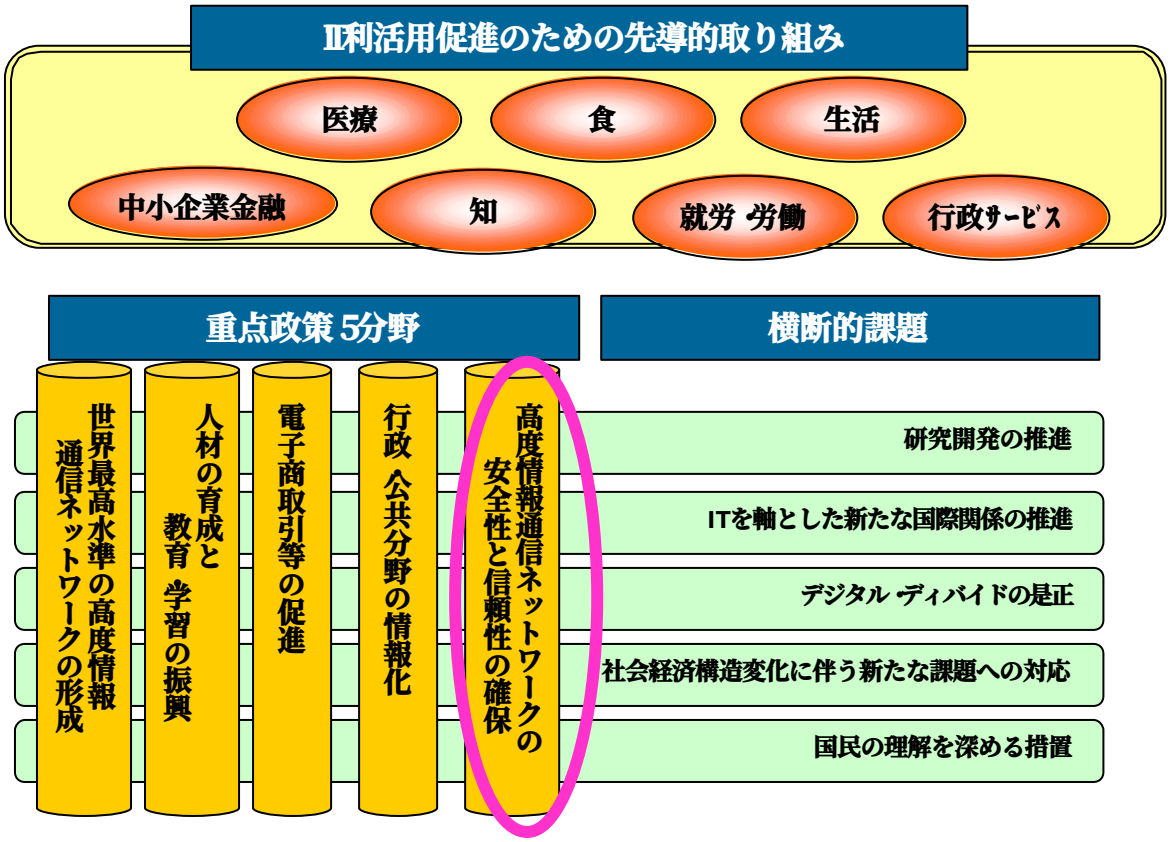

図 2- 3　e-Japan 重点計画 –2003 の構成と本戦略との関係（本戦略は囲み部分に対応）

第３章
戦略実現のための具体的施策

３．１．戦略実現のための具体的施策の構成

本章では、「戦略１：しなやかな『事故前提社会システム』の構築（高回復力・被害局限化の確保）」と「戦略２：『高信頼性』を強みとするための公的対応の強化」を実現するための具体策を総合的に提示する。

①従来の重点施策との関係

これまでの情報セキュリティ関連施策は、個々のシステムの信頼性・安全性の確保や安全な経済活動の確保を目標とした、技術開発とセキュリティマネジメント推進を主とする「企業・個人のセキュリティ向上」における「事前予防策」が中心であった。他の分野・領域についても着手はしているが、民間の専門家によれば、「形はあるが実質は伴っていない」との声が多く聞かれた。

このため、「戦略１」及び「戦略２」を実現するためには、

1) **対策の遅れが指摘される国・自治体及び重要インフラの事前対策強化（3.2.1.）**
2) **企業・個人の個別対応では対処しきれない全体のリスクへの対応強化（3.2.2.）**
3) **技術とセキュリティマネジメントの両輪からなる既存の事前予防対策の対応強化（3.2.3.）**
4) **事前予防策だけではなく、事故前提の対応策の抜本的強化（3.3.）**
5) **「高信頼性社会」の構築のための、国家的視野からの全体を支える基盤の強化（3.4.）**

を総合的に行う必要がある。したがって、以下（図 3-1）に示す枠組みに従って、具体的な施策を提示する。具体的施策の項目を一覧すると図 3-2 となる。

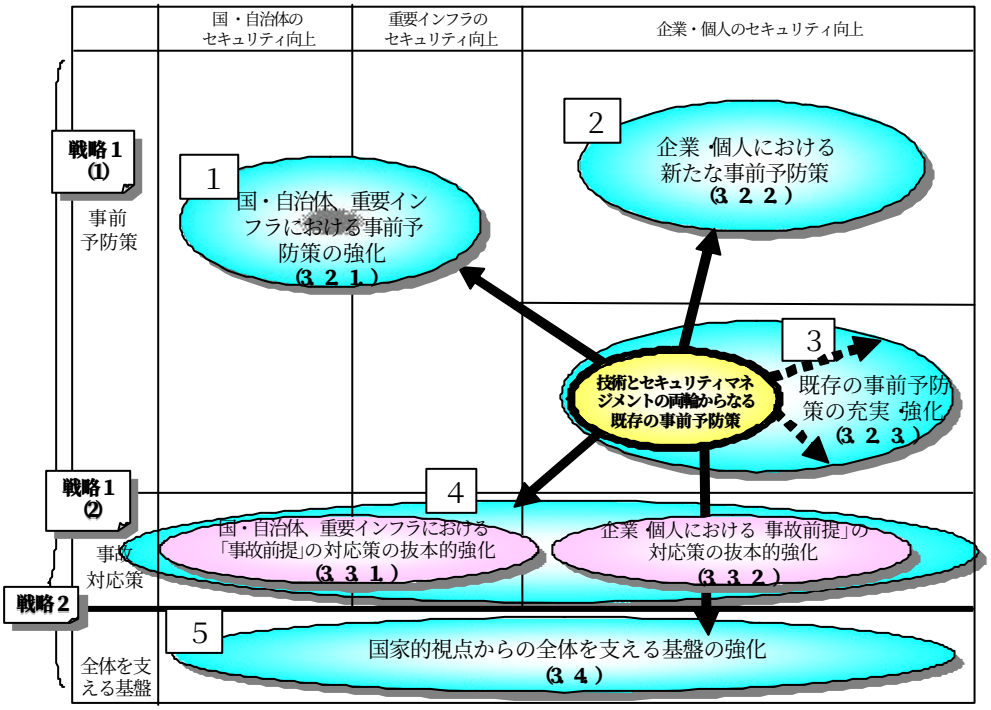

図 3- 1　これまでの施策との関係及び施策の柱立ての構成

②アクションプランの提示

加えて、単なる施策内容の方向性の提示にとどまらず、具体的な実現目標と実施時期を含んだアクションプランを明示する。具体的には、施策ごとに、我が国全体として、統一的な体制の下で情報セキュリティ対策への重点投資が十分かつ適切に行われたことを前提とし、施策の実現時期の目標を「３年以内に実現する項目」（緊急に措置すべき項目）と「3 年以内に着手し実行に移す項目」（中長期的視点も含めて着実に措置すべき項目）とに分けて提示する。

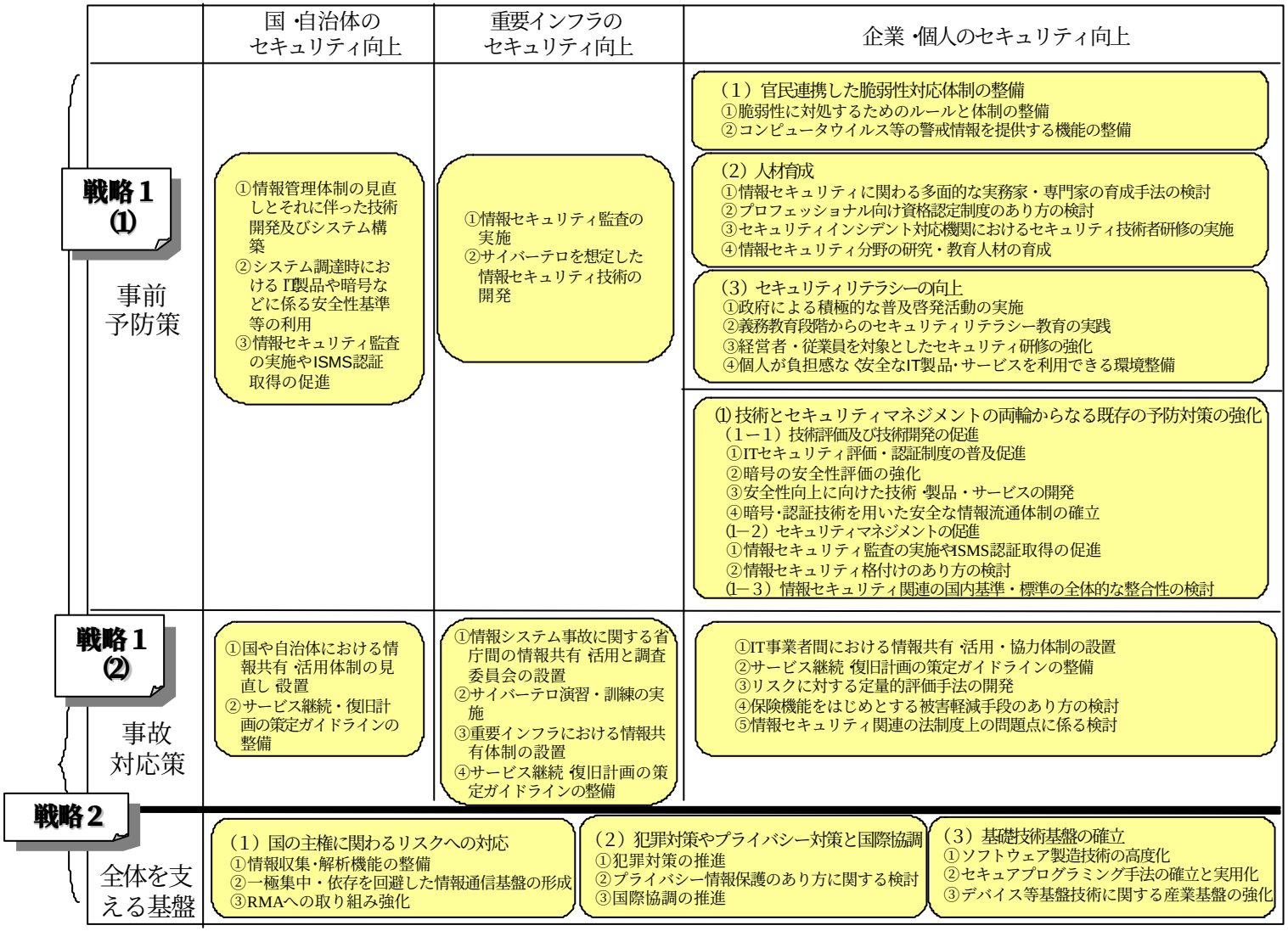

図 3- 2　具体的施策の構成

３．２.「戦略１：しなやかな『事故前提社会システム』の構築(高回復力・被害局限化の確保)」を実現するための具体的施策（１）～事前予防策の強化

しなやかな「事故前提社会システム」の実現のためには、まず各般の主体が国家的視野に立って、事故の事前予防策を講じることが必要である。我が国においては、これまでも事故の事前予防策を促進するための施策を講じてきたが、①対策の遅れが指摘される国・自治体及び重要インフラの事前予防策を強化するとともに、②企業・個人の各々の対策に委ねるのではなく全体の底上げを図るための新たな基盤整備を行い、③技術とセキュリティマネジメントを両輪とした対策を中心に講じてきた既存の施策の充実・強化を図っていくことが必要である。

３．２．１．国・自治体・重要インフラにおける事前予防策

国・自治体及び重要インフラ部門は、経済活動や国民生活に与える影響の甚大さにもかかわらず、その情報セキュリティ対策の遅れが指摘されている。今後は、世界最高水準のセキュリティを確保するための積極的な取り組みが必要である。

なお、ここでいう重要インフラ部門とは、経済活動と国民生活のライフラインとして深く影響を及ぼす業種等を広くその対象とすべきであり、内閣の情報セキュリティ対策推進会議（「重要インフラのサイバーテロ対策に係る特別行動計画」(2000 年 12 月)）にて対象とされている重要インフラ７分野（情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス（地方公共団体を含む））以外にも、例えば、水道分野、医療分野、石油分野等は、その対象として捉えるべきである。

（１）国・自治体における事前予防策

国・自治体は、情報セキュリティの事前予防対策として、①まず自らが保有する情報の重要度に応じた適切な管理体制を見直した上で「セキュリティポリシー」を構築し、②それに伴ったシステム構築や必要な技術開発を行い、③システム調達の際には安全性の基準を積極的に利用・構築し、④情報セキュリティ監査[10]などを利用して、情報セキュリティマネジメント[11]の体制構築も含めて適切に運用されているかどうかを確認する一連のプロセスを不断に取り入れていかねばならない。その際、個人情報を含め地域と密着したサービスを行う自治体と、公的基盤作りを中心とする国との役割の違いを意識しつつ、緊急情報や技術開発成果等の共有化が可能な領域は一体として体制を整備するなどの対応が求められる。

---

[10]情報セキュリティに係わるリスクのマネジメントが効果的に実施されるように、リスクアセスメントに基づく適切なコントロールの整備・運用状況を、情報セキュリティ監査人が独立かつ専門的な立場から検証又は評価し、保証を与えあるいは助言を行なうこと。2003 年 4 月より、経済産業省告示に基づく「情報セキュリティ監査制度」の運用が開始されている。（http://www.meti.go.jp/policy/netsecurity/audit.htm）

[11] セキュリティポリシーに基づき、組織の持つ情報資産の機密性、完全性、可用性を適切に維持・管理する作業を指す。

①情報管理体制の見直しとそれに伴った技術開発及びシステム構築

3 年以内に実現する項目	・情報資産分類と適切な管理体制（セキュリティポリシー）の見直し
3 年以内に着手し実行に移す項目	・機密情報保持等に必要な技術開発

国・自治体は、自らが保有する情報の重要度に応じた情報資産分類と適切な管理体制を見直した上で、「セキュリティポリシー」を整備することが必要である。そして、それに伴ったシステム構築を目指すとともに、国・自治体の機密情報保持等に必要な技術開発（セキュア OS 等）についても、必要に応じ積極的に行い、自らに適用していくことが必要である。なお、技術開発や技術の適用に際しては、国が自治体に対して技術供与や情報提供等の支援を行うこととする。

②システム調達時における IT 製品や暗号などに係る安全性基準等の利用

3 年以内に実現する項目	・カスタムアプリケーションの設計ガイドラインの策定・公表
3 年以内に着手し実行に移す項目	・安全性基準の認証等取得製品・システムの導入 ・再委託構造におけるセキュリティ確保

国・自治体は、システムの調達において、ISO/IEC15408[12]等の国際標準に基づく認証を取得した製品・システムや CRYPTREC[13]により策定された電子政府推奨暗号リスト[14]に掲載された暗号の積極導入を図る。加えて、カスタムアプリケーション（例えば、近年採用が進んでいる Web アプリケーション）の構築において脆弱性を排除するための設計ガイドライン（もしくはチェックリスト）の整備を行い、それに則ったシステム調達を促進する。

また、システム開発における再委託構造におけるセキュリティ確保に留意することが必要である。

[12] 情報処理関連製品および情報処理システムのセキュリティレベルを評価する目的で 1999 年に制定された国際規格。

[13] Cryptography Research and Evaluation Committees：電子政府の安全性及び信頼性を確保するため、暗号技術の安全性を客観的に評価することを目的として、総務省及び経済産業省により推進されている暗号技術評価プロジェクト。（http://www.ipa.go.jp/security/enc/CRYPTREC/）

[14] 2003 年 2 月 20 日に総務省及び経済産業省により策定された電子政府における調達において推奨される暗号のリスト。2003 年 2 月 28 日の行政情報システム関係課長連絡会議において、各府省は同リストに掲載された暗号の利用を推進する旨が合意されている。

③情報セキュリティ監査の実施や ISMS 認証取得の促進

3 年以内に実現する項目	・情報セキュリティ監査の実施、結果の公開 ・先進省庁や外郭団体における ISMS 認証取得
3 年以内に着手し実行に移す項目	―

国・自治体は、情報セキュリティ監査を実施する。また、監査を行った場合は、適切な形で、その結果を公開することを促進する。さらに、先進省庁や外郭団体においては、ISMS 認証（情報セキュリティマネジメントシステム適合性評価制度）[15]の取得も視野に入れて取り組む。

（2）重要インフラにおける事前予防策

「重要インフラのサイバーテロ対策に係る特別行動計画」[16]の該当業種（情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス（地方公共団体を含む））では、同計画のフォローアップ[17]において、サイバーテロを想定したセキュリティポリシー策定や監査等はほぼ完了との整理である。しかしながら、新たな次元のリスクが発現している現在、社会的影響という観点から見ると、今後、重要インフラ部門はそのサービスの維持を最優先課題として、サイバーテロ対策も含め、設定ミスやバグ、内部犯行等も含めたシステムリスクの予防や事後対応にも注力し、一層のセキュリティ確保の対策を講じる必要がある。

①情報セキュリティ監査の実施

3 年以内に実現する項目	・情報セキュリティ監査の実施
3 年以内に着手し実行に移す項目	―

重要インフラでは、情報システムのダウンによる事故のリスクを避けるため、あえて基幹業務の IT 化を進めていないケースも見られる。しかし、実際には基幹システムの周辺領域に導入した情報システムの脆弱性が原因となって、結果的に業務が停滞する事故・事件も生じている。そこで、業務プロセスの遂行に影響する情報システムが増加していることを踏まえ、重要インフラ部門は、基幹システムの周辺システムとの関係も含めて、情報セキュリティ監査を定期的に実施する必要がある。

---

[15] 2002 年 4 月より、日本情報処理開発協会から提供されている制度。個別の問題毎の技術対策の他に、組織のマネジメントとして、自らのリスク評価により必要なセキュリティレベルを決め、プランを持ち、資源配分して、システムを運用する。（http://www.isms.jipdec.jp/）

[16] 情報セキュリティ対策推進会議「重要インフラのサイバーテロ対策に係る特別行動計画」（2000 年 12 月）

[17] 情報セキュリティ対策推進会議「重要インフラのサイバーテロ対策に係る特別行動計画のフォローアップについて」（2002 年 3 月）、「重要インフラのサイバーテロ対策に係る特別行動計画に基づく取組みの推進について」（2002 年 11 月）　（http://www.kantei.go.jp/jp/it/security/index.html）

②サイバーテロを想定した情報セキュリティ技術の開発

3 年以内に実現する項目	―
3 年以内に着手し実行に移す項目	・サイバーテロを想定した技術開発

安全保障的観点も踏まえ、重要インフラに対するサイバーテロの脅威に対抗すべく、それに耐えうる最先端・最高水準の情報セキュリティ技術の開発に取り組む。例えば、未知の不正侵入手法やコンピュータウイルス、サービス不能攻撃からの効果的な防御、広域的な攻撃の予測、ソフトウェアの耐タンパー性、IP トレースバック、セキュア OS 等の技術開発が挙げられる。

３．２．２．企業・個人における新たな事前予防策

企業・個人は、原則として自己責任の下で費用対効果に見合ったセキュリティ対策を講じる主体であり、本来市場メカニズムの下で、適切な対策がもたらされるべきものである。しかしながら、第１章、第２章で示したように、情報セキュリティを巡るリスクが変質・拡大し、個々の企業や個人に生じた事故が、それぞれの企業や個人の業務・生活に支障を来すだけではなく、経済活動全体の停滞や国民全体の生命･財産そのものに関わるリスクをもたらしかねない状況となっているなど、その対策のあり方を見直さなければならない。

従来は、政府の施策としても、企業や個人が、情報セキュリティの技術の導入や情報セキュリティのマネジメントの構築を容易にするための施策を中心にして行ってきており、国際標準も取り入れながら、成熟度も上がってきている。今後は、①個々の企業・個人の対応ではまかないきれないリスク対応への国全体としての基盤整備に加え、②企業等を支える情報セキュリティ人材の国家的視野での育成や、③セキュリティリテラシーの向上のための方策を講じる必要がある。

その際、施策の実施手法としては、あくまで、市場メカニズムを活用しながらも積極的に政府がその機能を補うという官民が連携協力して取り組む（2.2 参照）という技術中立的、市場中立的な対策を促進する必要がある。また、企業は業務の維持が、個人はプライバシー情報の保護や犯罪に巻き込まれないことが重要であり、それぞれ必要な対策や求められる役割が異なる点に留意する必要がある。

（１）官民連携した脆弱性対応体制の整備

①脆弱性に対処するためのルールと体制の整備

3 年以内に実現する項目	・脆弱性に対処するためのルールと体制の整備
3 年以内に着手し実行に移す項目	―

我が国では、情報システムの脆弱性やコンピュータウイルス、ワーム等の詳細を把握し対策を講じるための情報を収集し分析する体制が弱く、米 CERT/CC[18]やウイルスワクチンソフトベンダ[19]などの情報を基に危険性を判断しているのが現状である。そのため、国内を中心に使用されるソフトの脆弱性への対応や急速に広がるコンピュータウイルス感染の被害を食い止める緊急対応を行うことが難しい。

そこで、政府と IT 事業者[20]が中心となって、情報システムの脆弱性情報を集積す

[18] Computer Emergency Response Team / Coordination Center ：セキュリティインシデントや脆弱性に関する情報の収集・発信を行う組織。1988 年のワーム事件をきっかけとして、カーネギーメロン大学の SEI（Software Engineering Institute）内に設置された。（http://www.cert.org）

[19] コンピュータウイルスやワームを検出・駆除するソフトウェア（ワクチンソフト）を提供する事業者。

[20] IT の製品や部品、関連サービスを提供する事業者。情報システムやソフトウェアのメーカー、システムインテグレータ、コンサルティグファーム、情報サービス事業者等が該当する。

るためのルールを構築し、それを分析する体制を整備する。具体的には、

1) 不正アクセスやコンピュータウイルス感染等の被害通報の受付
2) ネットワークのトラフィック観測に基づく異常予測
3) 脆弱性の通知と公開に関する一連の手続きルールの明確化（IT 事業者や研究者等が発見した製品・システムの脆弱性の通報の受け付け、製造元もしくはサービス提供者の対処、一定期間後の公開等）
4) 脆弱性及びウイルス、ワーム等の危険性を検証・解析する体制
5) 脆弱性及びウイルス、ワーム等の危険性を警告・公表する体制

が必要である。

特に、電子政府の拡大に対応し、通報されたシステムの脆弱性やコンピュータウイルス、ワームの危険性について迅速に検証・解析する体制を、政府として整備することが重要である。中でも、オープンソース[21]のツールや製造元が倒産した製品のように責任を負うべき事業者が明確でない場合の対応、ネットワーク全体に障害をもたらすような緊急性が高く社会的影響の大きい問題への対応等について、本体制の持つ役割は重要である。

②コンピュータウイルス等の警戒情報を提供する機能の整備

3 年以内に実現する項目	・警戒情報を提供する機能の整備
3 年以内に着手し実行に移す項目	―

上記①で整備した脆弱性に対処するルールと体制の整備をもとに、コンピュータウイルスやワームの発生についての予測機能を整備し、天気予報的に注意を促す機能の整備を検討する。その際、JPCERT/CC[22]、Telecom-ISAC Japan[23]、情報処理振興事業協会セキュリティセンター（IPA/ISEC）、NIRT[24]、自治体・重要インフラや IT 事業者間の情報共有体制（3.3.1(1)①及び(2)②、3.3.2①参照）が相互に連携して、国全体の情報共有を効率的に実現する体制を整える。特に、IT ベンダの SOC（Security Operation Center）や、IPA-ISEC 、Telecom-ISAC Japan 等が有するリアルタイムのトラフィック監視情報を有効に活用する。

[21] ソフトウェアのソースコードを無償で開示し、世界中のプログラマがそれを自由に改良して再配布することを認めるソフトウェアの開発方式。

[22] JPCERT コーディネーションセンター：セキュリティインシデント（コンピュータセキュリティに関係する人為的事象で、意図的および偶発的なもの（その疑いがある場合を含む））報告への対応や、国内外のコンピュータセキュリティインシデント情報のコーディネーション等を行う団体。（http://www.jpcert.or.jp/）

[23] 通信サービスの提供を妨げる各種インシデントを収集・分析し、その分析結果を会員間で共有する ISP 向けの会員制組織。（https://www.telecom-isac.jp/）

[24] National Incident Response Team：国民生活に重大な影響を与えるおそれのある情報セキュリティに係る事案について各省庁等における情報セキュリティ対策の立案に必要な調査・助言等を行うため、内閣官房情報セキュリティ対策推進室に設置された緊急対応支援チーム。（http://www.bits.go.jp/shoukai/nirt/）

（2）人材の育成

情報セキュリティ人材の育成を行うための取り組みは遅れている。人材育成には時間を要すること、また多様な人材像（コンサルタント、システムエンジニア、アナリスト、オペレータ等）が求められることから、多岐に渡る経年的な対策が必要である。

また、いわゆるセキュリティ技術者の育成に努めることが重要なのは当然であるが、それに加え、企業の情報セキュリティ最高責任者（CISO）[25]や IT 分野に強い法律家など、多面的な実務家・専門家の人材も不足していることから、そうした人材育成にも焦点を当てることも必要である。

なお、ここで提示する具体策の効果は、企業・個人の事前予防策だけでなく、政府・自治体、重要インフラにも、また事故対応対策にも及ぶものである。

①情報セキュリティに関わる多面的な実務家・専門家の育成手法の検討

3 年以内に実現する項目	・大学院・大学等の他分野相互受け入れ交換枠の設置
3 年以内に着手し実行に移す項目	・多面的能力を有する人材育成

現在、我が国に必要なセキュリティ人材として特に欠けているのは、情報セキュリティの意味を理解し判断できる情報セキュリティ最高責任者（CISO）や法律家、また法的知識や経営的視野を有する技術者である。こうした多面的能力を有する人材は限られており、その育成は社会的に極めて有用である。例えば、経営・財務分野や法務分野の人材が情報技術（セキュリティ）の専門教育機関で学ぶことで、情報セキュリティ技術に明るい経営者や法律家の候補を育成できる。逆に、情報セキュリティの人材が財務や法務の専門教育機関で学ぶことによって、情報セキュリティ上の社外事故・事件にも法的素養を持って対処できる人材を育成できる。

そこで、大学院・大学等の情報セキュリティ、経営・財務・法務等の専攻・学科において他分野の学生・社会人を相互に受け入れる交換枠を設けるなど、多面的能力を有する人材を育成する制度のあり方について検討する。また、電子政府の普及にかんがみ、政府や自治体における実務家を養成すべく、社会人を再教育・訓練するリカレント教育の取り組みも必要である。

②プロフェッショナル向け資格認定制度のあり方の検討

3 年以内に実現する項目	・プロフェッショナル向け資格認定制度の創設
3 年以内に着手し実行に移す項目	―

開発工程ではセキュリティ分野に知見のあるコンサルタントやシステムエンジニア、

[25] 組織の情報セキュリティについての権限と責任を担い、経営の観点から率先して情報セキュリティを組織的に推進する、情報セキュリティに関する最高責任者（Chief Information Security Officer）。

また運用工程で監査を行うアナリストが求められる。

そこで、そうした人材の能力評価の指標として、IT ベンダを選別する検討材料にも適用できる、セキュリティ技術に優れたプロフェッショナル向けの資格認定制度（例えば情報セキュリティアドミニストレータ[26]の上位資格に相当するもの）のあり方について検討する。その際、欧米の資格制度との整合性についても検討に含めることが望まれる。

③セキュリティインシデント対応機関におけるセキュリティ技術者研修の実施

3 年以内に実現する項目	・セキュリティインシデント対応機関における技術者研修の実施
3 年以内に着手し実行に移す項目	―

運用工程では、セキュリティ上の事故・事件対応に強いオペレータが求められる。

そこで、JPCERT/CC 等のセキュリティインシデントの最前線機関が、企業、自治体等のセキュリティ担当者や大学の学生を受け入れ、OJT 型の実践的研修を提供する事業を支援する。受講者は、本研修を通じてシステム運用における事故発生時の応急処置や被害拡大防止等の対応を習得することができる。

④情報セキュリティ分野の研究・教育人材の育成

3 年以内に実現する項目	・大学・大学院における情報セキュリティ分野の研究環境の強化・拡充
3 年以内に着手し実行に移す項目	・情報セキュリティ分野の研究人材の育成

情報セキュリティ技術の高度化のためには、システムエンジニアやオペレータ等のレベルアップとともに、研究人材の充実が不可欠である。しかし、現在の大学・大学院における情報セキュリティ分野の教育人材や研究環境の不足は否めず、情報セキュリティ技術の高度化ニーズに応えられる研究人材を育成する環境が不十分である。

そこで、大学や大学院の研究・教育環境を強化・拡充し、情報セキュリティ分野の研究者・教育者の育成を進める。

その際、情報セキュリティ技術は、応用数学や OR[27]、シミュレーション手法開発といった基盤的分野から、DDoS 攻撃対策や不正アクセスの手法解析等の実践的分野までを含めた幅広い総合的研究領域であることから、多様な領域の研究人材を育成できるよう、バランスのとれた配分を図る必要がある。特に、基盤的分野は研究開発資金の配分が比較的手薄になる傾向もあって、人材も集まりにくく弱体化が懸念されて

[26] 情報処理技術者の公的資格の一つ。情報セキュリティに関する基本的な知識を持ち、情報システムのセキュリティポリシーの策定、実施、分析、見直しを行う能力が要求される。
（http://www.jitec.jp/1_11seido/h13/ss.html）

[27] Operation Research：問題を数量モデル化し分析する手法。企業等の競争戦略分析に利用されている。

いる点に配慮し、競争的資金等の配分のバランスについて評価し、技術力の効果的な強化方法を検討する。

また、大学や大学院の研究成果について、産業界と連携し、実用化の円滑な促進を図る。

（3）セキュリティリテラシーの向上

社会全体のセキュリティレベルを向上し、リスクを低減するには、ユーザの啓発が不可欠である。2003 年 8 月に発生した Blaster ワーム騒動の例からも明らかなように、個人ユーザのセキュリティ対策の遅れがネット社会全体を揺るがすリスクとなりうる。

したがって、個人ユーザは、ネット社会の参加者としてのリスクと責任を自覚し、多くのソフトウェアには問題点があって、自ら修正用ソフトを適用するなどしなければならないこと、自分や家族のプライバシー情報を守ること、犯罪に巻き込まれないよう注意すること、さらに自らのシステムが他者の事故・事件の原因とならないよう努めることが重要である。

しかし、実際には、リスクに対する意識は低く、犯罪等の事故・事件に巻き込まれるケースも少なくない。また、リスクを理解していても、ツールの設定が難解で、対応できないケースが考えられる。

そこで、IT のユーザ層のセキュリティリテラシーを向上させることで、レベルを底上げし、情報セキュリティを巡る国全体としてのリスクの低減を図る。

①政府による積極的な普及啓発活動の実施

3 年以内に実現する項目	―
3 年以内に着手し実行に移す項目	・政府による普及啓発活動の実施

政府は、個人を中心とした IT のユーザ層に対し、基本ソフト（OS）等の修正用ソフトの重要性やプライバシー情報の保護、ネット犯罪や踏み台[28]化のリスクと対策などの、情報セキュリティに関わる基本的なリテラシーを啓発する活動を積極的に行うことが必要である。その際、「情報セキュリティの日」の創設や、優良な普及啓発コンテンツ提供の促進など、児童、中・高校生、主婦層、高齢者層のような、IT の利用環境は整いつつあるがセキュリティリテラシーを確立しにくい層に訴求するための有効な方策について検討する。

[28] 不正アクセス等により他者のコンピュータを乗っ取り、さらなる不正アクセスや迷惑メール配信の中継等に悪用すること。

②義務教育段階からのセキュリティリテラシー教育の実践

3 年以内に実現する項目	―
3 年以内に着手し実行に移す項目	・義務教育段階からのセキュリティリテラシー教育の開始

義務教育の段階からセキュリティリテラシーに関する内容を学習カリキュラムに組み込み[29]、子供がネット社会の一員となるための基礎的素養としてセキュリティ意識（セキュリティ文化）を身につけられる環境を整備するよう、検討を進める。その際、IT リテラシーの内容の一部として盛り込む他に、「知らない人についていかない」「道路に急に飛び出さない」といった一般的な安全教育や安全保障教育の一部として盛り込むことが必要である。

また、セキュリティリテラシーを教育する者も不足しており、地域社会と連携する形で人材を確保することも検討する。

③経営者・従業員を対象としたセキュリティ研修の強化

3 年以内に実現する項目	・各企業における経営者、従業員に対するセキュリティ研修の実施―
3 年以内に着手し実行に移す項目	―

企業の経営者層については、情報セキュリティ対策の重要性や適正な投資規模についての理解を促すよう、役員向け研修に組み込むことが求められる。

また、内部犯行防止については技術的な対策にも限界があることから、従業員に対して倫理教育を含む情報セキュリティの意識啓発に有効な研修の実施に取り組むことが求められる。さらに、こうした研修について、何らかの受講の動機付けを適用することが望ましい。

④個人ユーザが負担感なく安全な IT 製品･サービスを利用できる環境整備

3 年以内に実現する項目	・IT 事業者による「IT 製品・サービスに関するフェイルセーフガイドライン」の策定
3 年以内に着手し実行に移す項目	・IT 事業者による「安全サービス」の市場化 ・政府による個人安全製品提供のための技術開発

個人ユーザのリテラシー向上策を図ると同時に、個人ユーザが負担感なく、IT 製品・サービスを安全に利用できるような環境整備を行う。ここにおいては、IT 事業者の役割が重要となる。具体的には、

1) IT 製品やサービスにつき、インストール、設定・調整等を工夫する共通のフェイルセーフガイドライン（例えば、無線 LAN ルータの暗号化機能設定の半

[29] 中学校学習指導要領 技術・家庭科の解説書や、高等学校学習指導要領 情報科（情報 C）の解説書において、セキュリティに関連する記述が含まれている。

自動化、PC のプリインストールソフトやプラグインソフトのリスト化）を、IT 事業者を中心として策定したり、

2) **個人ユーザのパソコンの設定を遠隔で診断したり、ワーム感染の危険がある場合などにアクセス制限を実施したりするサービス（安全サービス）が、IT 事業者によって提供されたりする**

環境が整備されることが必要である。

また、政府は、IPv6 の導入や情報家電の普及が進む中で、個人にとって安全な IT 製品を提供するための技術開発を積極的に支援していくことが必要である（3.2.3.(1)③参照）。

３．２．３．技術とセキュリティマネジメントの両輪からなる既存の事前予防策の強化

自己責任の原則の下で行われるべき企業・個人のセキュリティ対策を促進する施策については、従来から、情報セキュリティ技術の導入やセキュリティマネジメントの構築を容易にするための施策を中心に実行してきた。これについては、国際標準をも取り入れながら制度構築等を行い、その成熟度は上がってきていると言えるが、今後、当該施策の一層の普及促進を図るとともに、ユーザの視点から見て、より実効性の高い制度等に昇華させていくことが必要となる。

（1）技術評価及び技術開発の促進

企業及び個人に情報セキュリティ技術の導入を促進するための施策としては、①ユーザがその技術を導入する際の尺度として、その技術を国際標準等に基づき客観的に評価・認証する仕組みを提供する取り組み（技術評価）と、②現時点では市場性が薄いものの、将来的にその技術が市場性を持つと見込まれる場合に、その市場化を加速するために政策的にセキュリティ技術・サービスを開発する取り組みとの両面から行う必要がある。

①IT セキュリティ評価・認証制度の普及促進

3 年以内に実現する項目	―
3 年以内に着手し実行に移す項目	・IT セキュリティ評価認証制度の体制強化

IT 製品・システムについては、我が国では国際標準 ISO/IEC15408 に基づく IT セキュリティ評価・認証制度が運用され、今秋には、国際的な相互承認アレンジメント（CCRA：Common Criteria Recognition Arrangement）[30]への加盟もなされる予定である。しかし、現時点においては、未だ本制度が十分に利用されている状況にはない。そのため、本制度の普及促進を目的として、以下の施策を実施する。

- 電子政府等において調達される IT 製品及び情報システムについて本制度における認証取得の促進
- 評価・認証業務を実施できる専門家の育成をはじめとする評価・認証体制の強化
- ベンダやユーザに対する研修、コンサルティングを行う専門家の育成をはじめとするベンダやユーザによる本制度の利用を促進するための環境整備

②暗号の安全性評価の強化

3 年以内に実現する項目	・暗号アルゴリズムの実装に関する基準の策定
3 年以内に着手し実行に移す項目	・暗号プロトコルの安全性評価手法の確立

[30] 1998 年に、米英仏独加の５カ国が統一した IT 製品の安全性評価基準（CC：Common Criteria）に基づいた認証結果を国際的に相互承認するために創設された枠組み。

軍事・外交上の秘匿行為に利用されるだけではなく、電子商取引、携帯電話等に利用されている暗号技術については、暗号技術検討会を中心とする CRYPTREC において、暗号アルゴリズムの安全性評価を行い、電子政府推奨暗号リストを策定したところである。

しかし、暗号技術については、暗号アルゴリズムそのもののみならず、その実装方法に問題があることも多いため、IC カードをはじめとする暗号製品の安全性を評価することも必要である。さらには、安全性・信頼性の高い通信に不可欠な暗号プロトコル[31]に関しては、その安全性を評価するための基準が世界的に見ても存在しないという課題があり、これらの分野についても一定の安全性評価が実施できるよう取り組むことが必要である。そのため、今後は以下の施策を実施する。

・電子政府等における電子政府推奨暗号の利用促進
・電子政府推奨暗号の安全性に関する継続的な評価
・暗号製品に関するセキュリティ要件等、暗号アルゴリズムの実装に関する調査研究
・暗号プロトコルの安全性評価手法等に関する調査研究

③安全性向上に向けた技術・製品・サービスの開発

3 年以内に実現する項目	―
3 年以内に着手し実行に移す項目	・安全性向上に向けた技術開発のロードマップ作成と一部実用化

企業や個人のそれぞれの市場において、投資対効果の高い情報セキュリティの技術・製品・サービスが求められている。

例えば、LAN 内の機器の安全性をリアルタイムに集中管理する技術や、脆弱性の自動検出、情報セキュリティ製品・サービスの IPv6 対応、生体認証技術等のテーマについて、技術開発や製品化、サービス化を促進することが重要である。特に、そうした取り組みに注力しているセキュリティベンチャー企業については、技術の社会的意義を踏まえ、国が積極的に支援することが必要である。

④暗号・認証技術を用いた安全な情報流通体制の確立

3 年以内に実現する項目	・金融・医療等の分野で暗号・認証技術の適用をルール化
3 年以内に着手し実行に移す項目	・セキュリティと匿名性を両立させる暗号応用技術の技術開発

企業情報の流通という観点から見ると、顧客情報や新製品情報等の機密情報をはじめ、IR、電子調達、電子商取引、EDI/CALS など、組織内・組織間・業界内・業界

[31] 暗号アルゴリズムを組み合わせてデータ守秘等を実現する通信プロトコル。

間といった範囲で情報流通が活発化することは確実である。その一方、様々な企業・自治体で個人情報漏洩のトラブルが頻発している。

したがって、そうした情報の利活用を促進する上で、安全な情報流通体制の確立は不可欠であり、情報セキュリティ技術の適用が極めて重要になる。特に、政策情報や個人情報を扱う国･自治体、企業の経営状況や個人の資産・負債、病歴等を扱う金融業界や医療業界のような、機密性の確保が極めて重要な分野では暗号・認証技術の適用をルール化するなどの取り組みが有効である。さらに、個人情報保護法制を踏まえ、セキュリティと匿名性を両立させる暗号応用技術の研究開発を促進する。

（2）セキュリティマネジメントの促進

企業における情報セキュリティマネジメントの構築を促進する。セキュリティマネジメントの構築は、内部犯行防止にも有効であることに加え、「事故対応策」（3.3 参照）にもつながる[32]ものである。

①情報セキュリティ監査の実施や ISMS 認証取得の促進

3 年以内に実現する項目	・株式公開企業や個人情報取扱事業者における情報セキュリティ監査の実施、ISMS 認証の取得 ・企業情報開示の項目で監査の実施と結果を任意記載化
3 年以内に着手し実行に移す項目	・中小企業における情報セキュリティ監査の実施、ISMS 認証の取得

企業における情報セキュリティ監査の利用促進を図る。具体的には、情報セキュリティ監査制度の普及促進を図るとともに、情報セキュリティ監査の実施状況を IR（Investor Relations）情報として、投資家や格付け機関に積極的に開示するような環境整備を促進する。証券取引法等の企業情報開示の項目において、情報セキュリティ監査の実施とその結果を任意記載化することも検討する。さらに、こうした取り組みと連動して、情報セキュリティ監査の実施が損害保険の支払負担軽減につながる仕組みのあり方についても検討する（3.3.2.④参照）。

また、ISMS 認証制度についても、国際相互承認の推進や、審査体制の強化など、その利用の促進を図る。

②情報セキュリティ格付けのあり方の検討

3 年以内に実現する項目	―
3 年以内に着手し実行に移す項目	・情報セキュリティ格付けの仕組み立ち上げ

[32] ISO/IEC17799:2000（Information technology－Code of practice for information security management）（JIS X 5080:2002（情報技術－情報セキュリティマネジメントの実践のための規範））、ISMS 認証基準（Ver2.0）においては、「事業継続管理」に係る管理策を定めている。

企業の情報セキュリティに対する取組状況を総合的かつ客観的に評価し、その格付けを行う仕組みを整備することが考えられる。そこで、まず情報セキュリティ格付けのあり方について検討する。その際、格付けの位置付けを、政府等の調達時の制約とすべきか、企業の IR の一環とすべきか、企業間取引の参加資格とすべきか、有効な活用方策についても検討する。

（3）情報セキュリティ関連の国内基準・標準の全体的な整合性の検討

3 年以内に実現する項目	・情報セキュリティ関連の国内基準、標準の全体構成、相関整理の実施（整合性確保の下固め）
3 年以内に着手し実行に移す項目	・情報セキュリティ関連の国内基準、標準を全体的に審議、推進できる上位機関の制定、および整合性審議

IT セキュリティ評価・認証制度、ISMS 適合性評価制度、情報セキュリティ監査制度、電子政府推奨暗号リスト等、我が国では、情報セキュリティ関連の基準・標準を、海外との整合性を重視する形で整備してきた。その一方、国際標準で要求される水準は高く、コストや時間を要することから、特に海外市場をターゲットとしない IT 製品・サービスにとっては活用が難しいという見方もある。

そこで、国際標準に配慮しつつ、かつ、ユーザにとって最適な形で提供できる、我が国の情報セキュリティ関連の基準・標準の全体としての構成や整合性について検討する。例えば、IT セキュリティ評価・認証制度への橋渡しとなるような、より簡易に利用できる制度構築の必要性や、技術基準とマネジメント基準の総合的評価のあり方等について検討する。

３．３．「戦略１：しなやかな『事故前提社会システム』の構築（高回復力・被害局限化の確保）」を実現するための具体的施策（２）～事故対応策の抜本的強化

情報セキュリティの事故を予防する取り組みをいかに講じても、何らかの事故は発生することは必然である。したがって、3.2.で示した事前予防策だけではなく、起きた事故に対して被害の最小化・局限化し、回復力の高い、国全体としての基盤を整備することが「しなやかな『事故前提社会システム』の構築（高回復力・被害局限化の確保）」のための、重要な要素となる。これまでの施策は、事前予防策を促進する施策に重点が置かれており、事故対応策のための取り組みは極めて遅れている。したがって、「戦略１」の実現のため、事故対応策の抜本的強化を図っていくことが必要である。

３．３．１．国・自治体・重要インフラにおける事故対応策

国・自治体及び重要インフラ部門で事故が生じれば、経済活動や国民生活に与える影響は甚大である。したがって、その被害を最小化し、事故から早急に復旧することをあらかじめシステムとして盛り込んでおくことを強く推進することが必要である。

（１）国・自治体における事故対応策

①国や自治体における情報共有・活用体制の見直し

3 年以内に実現する項目	・国(NIRT)、自治体の情報共有・活用体制の充実強化
3 年以内に着手し実行に移す項目	―

現在、中央省庁の情報セキュリティに関する事故緊急対応体制として内閣官房に NIRT が設置されている。しかし、その規模・機能とも限られており、内閣官房の機能・体制の強化（4.1.参照）とともに、その機能強化を図る。

また、自治体は数が多く、規模の格差も大きいため、個々の自治体では、自律的な情報セキュリティ対策の実施が困難なケースもある。そこで、個々の自治体が適切なセキュリティ対策を実施できるよう、緊急性の高い脆弱性情報やインシデント情報等を自治体間で共有し、活用する体制を充実・強化する。

②サービス継続・復旧計画の策定ガイドラインの整備

3 年以内に実現する項目	・国・自治体・重要インフラ向け「サービス継続・復旧計画策定ガイドライン」策定
3 年以内に着手し実行に移す項目	―

情報セキュリティの事故が起こった場合、事故が起こっても行政サービスを継続す

ること、また、その事故から早急に復旧することが必要である。そのためには、そうしたサービスの継続や事故からの復旧の対策をあらかじめ計画化することが必要であり、各主体の計画策定の指標となるよう、国・自治体、さらには重要インフラ部門をも対象とした「サービス継続・復旧計画の策定ガイドライン」を策定・公表する。そして、本ガイドライン等にしたがって、国・自治体の各主体が、「サービス継続・復旧計画」を策定する。

また、国・自治体は、事故発生時どのように対処すべきかを検証するため、実践的な訓練を実施する。

（2）重要インフラにおける事故対応策

①情報システム事故に関する省庁間の情報共有と調査委員会の設置

3 年以内に実現する項目	・「重要インフラ情報セキュリティ委員会」の設置 ・「情報システム事故調査委員会」の設置
3 年以内に着手し実行に移す項目	―

経済活動を含めた事故発生時の影響の大きさを考慮すれば、重要インフラにおける情報システム事故について、航空や鉄道の事故の場合と同様に、事故の原因や再発防止策を徹底することが重要である。

そこで、各所管省庁における重要インフラ情報セキュリティ担当官を任命し、内閣官房を中心とした「重要インフラ情報セキュリティ委員会」を組織する。これによって、省庁を超えて問題意識を共有し、必要な情報を共有化できる体制を整える。さらに、重要インフラのシステム事故の原因を分析し再発防止策を検討するため、官民の専門家で構成される「情報システム事故調査委員会」の設置を検討する。

②サイバーテロ演習・訓練の実施

3 年以内に実現する項目	・全重要インフラ部門におけるサイバーテロ演習・訓練の実施
3 年以内に着手し実行に移す項目	―

高度なサイバーテロシナリオを想定した実践的な演習や、システム事故を想定した訓練を、政府と一体となって実施する。例えば、米国では、1996 年以降、重要インフラを対象としたサイバーテロ演習を繰り返し、被害の発生可能性や対策の改善点等について検討を重ねてきた。こうした取り組みは、通常運用時には見えにくい問題点やトラブルの要因を明らかにするとともに、関係者がその危険性を現実的に理解する機会としても有効である。

③重要インフラにおける情報共有・活用体制の設置

3 年以内に実現する項目	・全重要インフラ部門における情報共有・活用体制の設置
3 年以内に着手し実行に移す項目	―

IC カード型の定期やプリペイドカードについて、複数の鉄道会社が共通化したり、クレジットカード機能を組み込むなど、業界における共通基盤を整備する動きが活発化している。こうした共通の情報システム基盤に事故・事件が発生すると、その社会的影響は極めて大きい。そこで、今後様々な形で構築される業界共通基盤の保護の目的を中心とした重要インフラごとの情報共有・活用体制を整備する。この情報共有・活用体制において、いわゆる脆弱性情報やインシデント情報等、さらに物理的要因も含めた業界特有のリスク分析などを扱うことが必要となる。

④サービス継続・復旧計画の策定ガイドラインの整備（再掲）

3 年以内に実現する項目	・国・自治体・重要インフラ向け「サービス継続・復旧計画策定ガイドライン」策定
3 年以内に着手し実行に移す項目	―

国・自治体・重要インフラ部門を対象とした「サービス継続・復旧計画の策定ガイドライン」を策定・公表する。そして、本ガイドラインにしたがって、重要インフラ部門の各主体が、「サービス継続・復旧計画」を策定する。

なお、実際のサービス継続・復旧作業には費用の確保が不可欠であり、「サービス継続・復旧計画」においては、保険の活用等による対応を明確化することが望まれる。

3．3．2．企業・個人における事故対応策

企業経営が、従来の資産重視型からキャッシュフロー重視型に変化していくと、キャッシュフローを安定的に維持することが企業価値の源泉となる。したがって、事故の防止は重要であるが、情報セキュリティリスクを完全になくすことができない以上、情報システムのダウンや情報漏洩などの事故を根絶することは非常に難しく、安定したキャッシュフローの維持に問題が生じる可能性がある。そこで、企業においても、事故を予防するだけでなく、事故の発生を前提として、被害拡大防止やダメージの低減に努め、スムーズな復旧を果たすための事故対応の基盤整備が求められる。

①IT 事業者間における情報共有・活用・協力体制の設置

3 年以内に実現する項目	・IT 事業者間における情報共有・活用・協力体制の設置
3 年以内に着手し実行に移す項目	―

情報システムの脆弱性を出荷・納品の時点で完全に排除しておくことは困難であるため、IT 事業者は修正用ソフトウェア等の開発体制を確保するとともに、新たな脆弱性が報告された場合には、速やかに対策を講じ、それを企業や個人等のユーザに正しく伝え、修正用ソフトウェアの適用を促す姿勢が求められる。しかし、コスト的な制約や情報・ノウハウの不足のため、個々の IT 事業者は場当たり的な対策に終始せざるを得ない状況にある。例えば、ソフトウェアの部品化・再利用化に伴い、メーカーやシステムインテグレータにとってもシステムがブラックボックスと化しており、その脆弱性の影響範囲を正確に把握できずにいる。

また、情報システムの運用を請け負う IT 事業者は、システムダウン等の原因となる脆弱性について情報収集を効率的に行うとともに、被害を最小化し、サービスを継続するための計画や訓練を進めることが重要である。

そこで、IT 事業者が協同して情報システムの事故・事件の予防と事後対応の推進を図るための情報共有・協力体制を設置する。この体制では、次の機能を確立することを目指す。

- IT 事業者が運用する SOC 間の連携
- IT 事業者間のトラブルシューティング情報の共有化
- IT 事業者間での脆弱性情報の共有化
- 自社の製品やシステムに採用した組み込みソフトウェアの情報の開示
- 個人ユーザに対する修正用ソフトウェアやセキュリティ情報の効果的な提供
- コンピュータウイルスやワームの発生に関する予測

さらに、本体制と JPCERT/CC、Telecom-ISAC Japan、情報処理振興事業協会セキュリティセンター（IPA-ISEC）、NIRT、自治体・重要インフラの情報共有体制（3.3.1(1)①及び(2)②参照）が相互に連携して、国全体の情報共有を効率的に実現する体制を整える。特に、IT ベンダの SOC や、IPA-ISEC 、Telecom-ISAC Japan 等が有するリアルタイムのトラフィック監視情報をベースに、迅速な被害拡大防止の実現を図る。

②サービス継続・復旧計画の策定ガイドラインの整備

3 年以内に実現する項目	・国・自治体・重要インフラ向け「サービス継続・復旧計画策定ガイドライン」策定
3 年以内に着手し実行に移す項目	―

国・自治体・重要インフラを対象とした「サービス継続・復旧計画の策定ガイドライン」の策定・公表により、企業における、同計画の策定を促進する。

なお、実際のサービス継続・復旧作業には費用の確保が不可欠であり、企業のサービス継続・復旧計画においては、保険の活用等による対応を明確化することが望まれる。

③リスクに対する定量的評価手法の開発

3 年以内に実現する項目	・リスクに対する定量的評価手法を開発・公開、政府自身や外郭団体に適用 ・公的機関において情報セキュリティに関する事故データを収集する体制の整備
3 年以内に着手し実行に移す項目	―

企業における情報セキュリティ投資について理解が得られない理由の一つとして、リスクに対する明確な指標がなく、投資が進まないことが挙げられる。

そこで、政府が、情報セキュリティを巡るリスクに対する定量的評価手法を開発・公開し、それを政府自身や外郭団体に適用する取り組みを行う。

また、情報セキュリティの事故データについて、現在でも様々な機関で調査が行われているが、その方法は非統一的であり、公的機関において、リスクの定量的評価に繋がるようなデータ収集を継続的に行う体制を整備する。

④保険機能をはじめとする被害軽減手段のあり方の検討

3 年以内に実現する項目	・保険等による被害軽減モデル案の提示
3 年以内に着手し実行に移す項目	―

事故の予防は極めて重要であるが、その一方、絶対的な安全はない。そうした観点に立って、事故が発生した場合の被害を軽減する手段として、損害保険の適用、技術的冗長性の確保、契約事項の強化等を利用したモデル案の提示を行う。

損害保険については、リスクの定量的評価手法の充実や、サービス継続・復旧計画への位置付けの明確化などにより、情報セキュリティの分野において、より有効に機能する方策について検討する。

また、技術的冗長性については、例えばソフトウェアのバグを考慮すれば、回線やハードウェアの二重化だけでなく、ソフトウェアについても本番版とは異なるものをバックアップ版として用意しておくことが望ましいが、実際にはコスト的な制約があるので、現実的な最適解を模索する必要がある。

さらに、契約の面では、瑕疵担保責任や免責事項、SLA（サービス品質保証制度）[33]等のあり方が重要な検討課題である。

[33] Service Level Agreement：企業と顧客との契約で、提供されるサービスの基準を主に数値により明確に定義、測定し保証するもの。主に、サービスの可用性、故障回復時間、障害通知などが対象とされる。

⑤情報セキュリティ関連の法制度上の問題点に係る検討

3 年以内に実現する項目	―
3 年以内に着手し実行に移す項目	・情報セキュリティ関連の法制度上の問題点に係る検討

情報セキュリティに関する法制度として、電子署名法、不正アクセス禁止法、個人情報保護法制などが成立している。ただし、現行の法制度や規制等ではカバーしきれない点や、改善すべき点も指摘されている。

そこで、情報セキュリティの観点から見た法制度上の問題点（新たな脅威、法制度上の整合、環境変化により炙り出されてきた未解決の問題等）や改善策、望ましいあり方について検討する。例えば、不正アクセスとコンピュータウイルスの法制度上の区分、スパイウェアの取り扱い、ソフトウェアの製造者責任のあり方、十分な情報セキュリティ対策を実施していたことをもって取締役の責任や行政処分の軽重をつける米国のガイドラインの効果検証などが検討対象として考えられる。

３．４．「戦略２：『高信頼性』を強みとするための公的対応の強化」を実現するための具体的施策～戦略１の実現及び国家的視点からの全体を支える基盤の強化

世界最高水準の「高信頼性社会」の実現に向けて高い目標を立て、それらを官民が協調しながら実現していくためには、「戦略１」で挙げた各般の施策（3.2.及び 3.3.で掲げた施策）を着実に実現するとともに、①国の主権に関わるリスクへの対応や、②犯罪対策やプライバシー対策、国際協調、そして、③我が国の「強み」を活かした基礎技術の基盤を確立していくことなど、国家的視点から、全体を支えるような基盤を強化する施策を実施していくことが必要である。

３．４．１．国の主権に関わるリスクへの対応

①情報収集･解析機能の整備

3 年以内に実現する項目	―
3 年以内に着手し実行に移す項目	・情報収集・解析機能の整備

政府が複雑化する社会に対する包括的理解をどのように確立するべきかという問題は、国家運営の根幹に関わる極めて重要なものである。そうした観点に立って見直すと、我が国においては、情報収集および解析の機能が十分でない点が指摘される。政府として迅速かつ統合的に対処すべき問題についての情報収集・解析を行うシンクタンク的な機能の整備を検討する。

②一極集中・依存リスクを回避した IT 基盤の形成

3 年以内に実現する項目	―
3 年以内に着手し実行に移す項目	・一極集中・依存リスクを回避した IT 基盤の形成

2003 年 8 月に発生した Blaster ワームの問題によって、社会全体が一つの OS に依存していることのリスクが明らかになった。こうした知見を踏まえ、地理的集中、機能的集中など、一極集中・依存リスクが生じる恐れのある基盤（OS、GPS 等）について、企業や国民が選択肢を持てるように、国として何らかの代替案を確保することを検討する。

③RMA への取り組み強化

3 年以内に実現する項目	―
3 年以内に着手し実行に移す項目	・RMA への取り組み強化

IT を軍事兵器に適用した RMA[34]の分野が急速な変貌期を迎えていることを踏まえ、一層注力していくことが求められる。特に、アドホックネットワークやユビキタス関連の技術については、非軍事分野への適用も容易であり、そうした変動する技術分野の最先端にキャッチアップすることは、産業政策的にも重要である。

３．４．２．犯罪対策やプライバシー対策と国際協調

①犯罪対策の推進

3 年以内に実現する項目	―
3 年以内に着手し実行に移す項目	・犯罪対策の推進 ・犯罪対策のための技術開発

我が国では、警察庁がサイバーフォース（機動的技術部隊）等を設置し、ハイテク犯罪やサイバーテロ対策にも積極的に取り組んでいる。企業のサイトが不正アクセスの踏み台にされたり、DDoS 攻撃に悪用されるリスクを考慮すれば、産業界にも状況に応じて可能な限り犯罪捜査に協力する姿勢が求められる。

また、政府は、不正アクセスや情報漏洩等の痕跡を把握するための証拠保全（フォレンジックス）ツールや不正アクセス等の発信元を追跡する IP トレースバック等の技術開発・利用促進に取り組むことが必要である。

②プライバシー情報保護のあり方に関する検討

3 年以内に実現する項目	・プライバシーマーク制度の見直し
3 年以内に着手し実行に移す項目	・プライバシー情報保護の適切なモデルの提示

現代においては、個人の行動に係る情報が様々な局面で流通している。これらの情報を収集・解析することによって得られる情報、いわゆるプライバシー情報について、その解析・交換・流通をどこまで許容し、いかにプライバシー情報を保護するか、適切なモデルの可能性について検討する。

なお、個人情報保護法制の成立とともに、プライバシー情報保護についての社会意識は高まっている。IT 業界では、個人情報保護法制の成立以前から、個人情報を取り扱う事業者が遵守すべき規準を明示したプライバシーマーク制度[35]が整備・推進されてきた。今後、個人情報保護法制に適合した形でプライバシーマーク制度を見直すとともに、普及・啓発活動に取り組む。

---

[34] Revolution in Military Affairs：技術の高度化が軍事戦略や作戦行動におよぼす変革。急速に高度化する IT を活用して、リアルタイムに把握した情報に基づき、敵の最も緊要な部分に対し攻撃を加え、敵の組織的活動を低下させ、作戦を有利に運ぶ。

[35] 個人情報の取り扱い上、適切な保護措置を講じる体制を整えた民間事業者に対し「プライバシーマーク」の使用を認める制度（(財）日本情報処理開発協会実施）。1998 年より運用開始。（http://privacymark.jp/）

③情報セキュリティに関する国際協調の推進

3年以内に実現する項目	―
3 年以内に着手し実行に移す項目	・情報セキュリティに係る国際協調の推進

我が国政府は、情報セキュリティ推進施策の実施に当たり、国際協調に積極的に取り組んできた。具体的には、OECD（経済協力開発機構）の情報セキュリティガイドライン[36]策定、APEC（アジア太平洋経済協力）における情報・通信インフラのセキュリティについての声明、CCRA（IT セキュリティ評価・認証制度に係る国際相互承認）への加盟（NITE）、アジア PKI フォーラム[37]、APCERT（アジア太平洋コンピュータ緊急対応チーム）の設立[38]、GBDe（Global Business Dialogue on Electronic Commerce）[39]や G8 リヨン・グループ（国際組織犯罪上級専門家会合）[40]における検討、欧州評議会サイバー犯罪条約への署名[41]などが挙げられる。犯罪対策やプライバシー情報保護も含め、今後も引き続き、情報セキュリティ分野において官民連携を維持しつつ積極的に国際協調に取り組む。

３．４．３．基礎技術基盤の確立

①ソフトウェア製造技術の高度化

3年以内に実現する項目	・産学連携拠点の整備
3 年以内に着手し実行に移す項目	―

ソフトウェアはあらゆる産業の基盤となっており、産業全体の競争力強化、構造改革の実現に極めて大きな役割を果たす。その一方で、ソフトウェアの不具合を原因とする事故・事件が最近多発し、ソフトウェアの品質・信頼性の向上が喫緊の課題となっている。また、より大規模のソフトウェアをより短期間で開発する要求が増大し、生産性の向上も求められているところである。そのため、産学連携の下でソフトウェア工学（高品質のソフトウェアを効率的に開発する生産技術体系）の実践を強化する拠点（ソフトウェアエンジニアリングセンター：SEC）を創設し、我が国ソフトウェ

[36] 1992 年に OECD で採択された情報セキュリティガイドライン（Guideline for the Security of Information Systems）が、2002 年 8 月に改訂された。“Culture of Security”の提唱、情報通信ネットワーク社会を前提とした点、個人を含む全ての参加者の責任、情報セキュリティマネジメントの概念の導入等が特徴。（http://www.oecd.org/sti/security-privacy）

[37] アジア地域の国々に対する統括的な PKI を実現するためのフォーラム。（http://www.asia-pkiforum.org/）

[38] アジア太平洋地域に存在する CSIRT（コンピュータインシデント緊急対応チーム）の協力関係をサポート・促進する目的で、2003 年 2 月、APSIRC2003（台湾）にて発足。（http://www.apcert.org/）

[39] 電子商取引に関する世界共通ルールの構築を目的として、世界のネット関連企業で構成される国際ビジネス会議。（http://www.gdbe.org/）

[40] G8 各国の組織犯罪対策の上級専門家によって構成される政府間会合。2002 年 5 月には、国際組織犯罪と闘うための 40 の勧告」を見直し、テロ対策を補足した「国際犯罪に関する G8 勧告」を策定。

[41] インターネットを利用した国際犯罪に各国が共同して対処するため、欧州が提唱した条約。日米欧など 30 カ国が 2001 年 11 月に署名。

アの競争力を強化する。具体的には、国自身による先進的ソフトウェア開発・実践的人材育成を通じたベストプラクティスの創出、データ・事例の収集・分析によるソフトウェアの「価値」評価基準の策定を通じた競争環境整備及び品質等向上に向けた動機付け、組込みソフトウェアの開発工程改善手法の開発を通じた我が国からの「強み」発信を推進していく。

②セキュアプログラミング手法の確立と実用化

3 年以内に実現する項目	・産学連携拠点の整備
3 年以内に着手し実行に移す項目	―

現状では、技術的視点から「いかなるソフトウェアもバグ（脆弱性につながるバグを含む）を完全になくすことはできない」と認識されているが、これを可能な限り少なくすることが、高信頼社会を構築するための抜本的な解決策となる。したがって、脆弱性を最少化するセキュアプログラミング手法を確立することが重要である。

なお、現在 SEC (Software Engineering Center) の設置が別途検討されていることから、その研究テーマとして採択することが有効である。加えて、国や自治体のシステム開発時に、上記の成果として得られたセキュアプログラミング手法の適用を発注要件とすることを検討する。

③デバイス等基盤技術に関する産業基盤の強化

3 年以内に実現する項目	―
3 年以内に着手し実行に移す項目	・デバイス等基盤技術に関する産業基盤の強化

デバイス技術や暗号技術、そして今後の情報家電市場の拡大などを見込んだセキュリティと匿名性を利用させる暗号応用技術、著作権保護の技術など、情報セキュリティを基軸に構築され、我が国の「強み」を活かすことのできる基盤技術は、いわば IT における技術的な管制高地に相当する。こうした基盤技術に立脚したに立脚した産業基盤の強化を進め、我が国の競争力維持・向上に戦略的に取り組む。

第４章
戦略の実現のための体制と進捗管理

４．１．「戦略３：内閣機能強化による統一的推進」

「情報セキュリティ対策」を強化していくにあたっては、ただ闇雲に政府関与を強化するのではなく、「完全な政府施策領域」と「官民連携・協力領域」の区別を意識しながら、限られた専門的な人材資源や予算資源を適切に配分・管理していく必要がある。また、個々の対応においても、個別の主体がバラバラに対応をとるのではなく、官民や官官、民民それぞれの関係性の中で効果的な対応がとられるよう資源のポートフォリオ管理やそれぞれの連携・協調管理を行うことができる一元的な体制が必要である。

ここでは、その具体策を提示する。これはすなわち、本戦略の実現のための体制を示すものである。

①内閣機能の強化

本来、社会全体にとって最適な情報セキュリティの全体像やそれを実現するための戦略を検討すべき内閣官房の情報セキュリティ対策推進室や NIRT は、諸外国に比べ規模が小さく、十分に機能しきれていない面がある。

そこで、内閣の体制や人員を強化し、以下の機能を担う組織として変革を進める。

- 政府・自治体・重要インフラなどの事故情報を総合的に収集する体制の構築 (3.3.1.(1)①、3.3.1.(2)③、3.3.2.①参照)
- 国・自治体の機密情報保持等に必要な技術開発等の企画・立案（3.2.1.(1)①参照）
- 各省庁に対するセキュリティ監査や侵入テスト等の検査の実施（3.2.1.(1)③参照）
- 情報セキュリティに関する国としての対外窓口
- 情報セキュリティ政策に関する各推進体制間の総合的な調整
- 情報セキュリティ政策の実施に向けた進捗管理（プロセスマネジメント）

②統一的な推進体制の整備

情報セキュリティに関する研究開発、技術・製品・システム評価、標準化・ガイドライン策定、普及啓発・教育、緊急時対応といった、国と民間企業との協調体制が重要な施策については、役割分担と連携方法を明確化し、我が国において統一的な施策展開の実現を図る。

そうした目標に向け、内閣官房の主催で各省庁の情報セキュリティ関連政策担当官や公的な研究所を含めた「情報セキュリティ政策委員会」を発足、情報の共有と意識のすり合わせを行い、整合のとれた施策展開の一助とする。

４．２．望ましい実現時期

ここでは、第３章に示した戦略実現のための具体的施策において提示した施策の実現目標を一覧する。

「戦略１：しなやかな『事故前提社会システム』の構築(高回復力・被害局限化の確保)」を実現するための具体的施策（１）～事前予防策の強化

（１）国・自治体、重要インフラにおける事前予防策

（１－１）国・自治体における事前予防策

①情報管理体制の見直しとそれに伴った技術開発及びシステム構築

3 年以内に実現する項目	・情報資産分類と適切な管理体制（セキュリティポリシー）の見直し
3 年以内に着手し実行に移す項目	・機密情報保持等に必要な技術開発

②システム調達時における IT 製品や暗号などに係る安全性基準等の利用

3 年以内に実現する項目	・アプリケーションレイヤーの設計ガイドラインの策定・公表
3 年以内に着手し実行に移す項目	・安全性基準の認証等取得製品・システムの導入 ・再委託構造におけるセキュリティ確保

③情報セキュリティ監査の実施や ISMS 認証取得の促進

3 年以内に実現する項目	・情報セキュリティ監査の実施、結果の公開 ・先進省庁や外郭団体における ISMS 認証取得
3 年以内に着手し実行に移す項目	－

（１－２）重要インフラにおける事前予防策

①情報セキュリティ監査の実施

3 年以内に実現する項目	・情報セキュリティ監査の実施
3 年以内に着手し実行に移す項目	－

②サイバーテロを想定した情報セキュリティ技術の開発

3 年以内に実現する項目	－
3 年以内に着手し実行に移す項目	・サイバーテロを想定した技術開発

（２）企業・個人における新たな事前予防策

（２－１）官民連携した脆弱性対応体制の整備

①脆弱性に対処するためのルールと体制の整備

3 年以内に実現する項目	・脆弱性に対処するためのルールと体制の整備
3 年以内に着手し実行に移す項目	－

②コンピュータウイルス等の警戒情報を提供する機能の整備

3年以内に実現する項目	・警戒情報を提供する機能の整備
3 年以内に着手し実行に移す項目	―

（２－２）人材の育成

①情報セキュリティに関わる多面的な実務家・専門家の育成手法の検討

3年以内に実現する項目	・大学院・大学等の他分野相互受け入れ交換枠の設置
3 年以内に着手し実行に移す項目	・多面的能力を有する人材育成

②プロフェッショナル向け資格認定制度のあり方の検討

3年以内に実現する項目	・プロフェッショナル向け資格認定制度の創設
3 年以内に着手し実行に移す項目	―

③セキュリティインシデント対応機関におけるセキュリティ技術者研修の実施

3年以内に実現する項目	・セキュリティインシデント対応機関における技術者研修の実施
3 年以内に着手し実行に移す項目	―

④情報セキュリティ分野の研究・教育人材の育成

3年以内に実現する項目	・大学・大学院における情報セキュリティ分野の研究環境の強化・拡充
3 年以内に着手し実行に移す項目	・情報セキュリティ分野の研究人材の育成

（２－３）セキュリティリテラシーの向上

①政府による積極的な普及啓発活動の実施

3年以内に実現する項目	―
3 年以内に着手し実行に移す項目	・政府による普及啓発活動の実施

②義務教育段階からのセキュリティリテラシー教育の実践

3年以内に実現する項目	―
3 年以内に着手し実行に移す項目	・義務教育段階からのセキュリティリテラシー教育の開始

③経営者・従業員を対象としたセキュリティ研修の強化

3 年以内に実現する項目	・各企業における経営者、従業員に対するセキュリティ研修の実施
3 年以内に着手し実行に移す項目	―

④個人ユーザが負担感なく安全な IT 製品･サービスを利用できる環境整備

3 年以内に実現する項目	・IT 事業者による「IT 製品・サービスに関するフェイルセーフガイドライン」の策定
3 年以内に着手し実行に移す項目	・IT 事業者による「安全サービス」の市場化 ・政府による個人安全製品提供のための技術開発

（3）技術とセキュリティマネジメントの両輪からなる既存の事前予防策の強化

（3－1）技術評価及び技術開発の促進

①IT セキュリティ評価・認証制度の普及促進

3 年以内に実現する項目	―
3 年以内に着手し実行に移す項目	・IT セキュリティ評価認証制度の体制強化

②暗号の安全性評価の強化

3 年以内に実現する項目	・暗号アルゴリズムの実装に関する基準の策定 ･電子政府推奨暗号の安全性に関する継続的評価
3 年以内に着手し実行に移す項目	・暗号プロトコルの安全性評価手法の確立

③安全性向上に向けた技術・製品・サービスの開発

3 年以内に実現する項目	―
3 年以内に着手し実行に移す項目	・安全性向上に向けた技術開発のロードマップ作成と一部実用化

④暗号･認証技術を用いた安全な情報流通体制の確立

3 年以内に実現する項目	・金融・医療等の分野で暗号・認証技術の適用をルール化
3 年以内に着手し実行に移す項目	・セキュリティと匿名性を両立させる暗号応用技術の技術開発

（3－2）セキュリティマネジメントの促進

①情報セキュリティ監査の実施や ISMS 認証取得の促進

3 年以内に実現する項目	・株式公開企業や個人情報取扱事業者における情報セキュリティ監査の実施、ISMS 認証の取得 ・企業情報開示の項目で監査の実施と結果を任意記載化
3 年以内に着手し実行に移す項目	・中小企業における情報セキュリティ監査の実施、ISMS 認証の取得

②情報セキュリティ格付けのあり方の検討

3 年以内に実現する項目	―
3 年以内に着手し実行に移す項目	・情報セキュリティ格付けの仕組み立ち上げ

（3）情報セキュリティ関連の基準・標準の全体的な整合性の検討

3 年以内に実現する項目	・情報セキュリティ関連の国内基準、標準の全体構成、相関整理の実施（整合性確保の下固め）
3 年以内に着手し実行に移す項目	・情報セキュリティ関連の国内基準、標準を全体的に審議、推進できる上位機関の制定、および整合性審議

「戦略１：しなやかな『事故前提社会システム』の構築（高回復力・被害局限化の確保）」を実現するための具体的施策（２）～事故対応策の抜本的強化

（１）国・自治体・重要インフラにおける事故対応策

（１－１）国・自治体における事故対応策

①国や自治体における情報共有・活用体制の見直し

3 年以内に実現する項目	・国(NIRT)、自治体の情報共有体制の充実強化
3 年以内に着手し実行に移す項目	―

②サービス継続・復旧計画の策定ガイドラインの整備

3 年以内に実現する項目	・国・自治体・重要インフラ向け「サービス継続・復旧計画策定ガイドライン」策定
3 年以内に着手し実行に移す項目	―

（１－２）重要インフラにおける事故対応策

①情報システム事故に関する省庁間の情報共有と調査委員会の設置

3 年以内に実現する項目	・「重要インフラ情報セキュリティ委員会」の設置 ・「情報システム事故調査委員会」の設置
3 年以内に着手し実行に移す項目	―

②サイバーテロ演習・訓練の実施

3 年以内に実現する項目	・全重要インフラ部門におけるサイバーテロ演習・訓練の実施
3 年以内に着手し実行に移す項目	―

③重要インフラにおける情報・活用共有体制の設置

3 年以内に実現する項目	・全重要インフラ部門における情報共有体制の設置
3 年以内に着手し実行に移す項目	―

④サービス継続・復旧計画の策定ガイドラインの整備（再掲）

3 年以内に実現する項目	・国・自治体・重要インフラ向け「サービス継続・復旧計画策定ガイドライン」策定
3 年以内に着手し実行に移す項目	―

（2）企業・個人における事故対応策

①IT 事業者間における情報共有・活用・協力体制の設置

3 年以内に実現する項目	・IT 事業者間における情報共有・協力・活用体制の設置
3 年以内に着手し実行に移す項目	―

②サービス継続・復旧計画の策定ガイドラインの整備

3 年以内に実現する項目	・国・自治体・重要インフラ向け「サービス継続・復旧計画策定ガイドライン」策定
3 年以内に着手し実行に移す項目	―

③リスクに対する定量的評価手法の開発

3 年以内に実現する項目	・リスクに対する定量的評価手法を開発・公開、政府自身や外郭団体に適用 ・公的機関において情報セキュリティに関する事故データを収集する体制の整備
3 年以内に着手し実行に移す項目	―

④保険機能をはじめとする被害軽減手段のあり方の検討

3 年以内に実現する項目	・保険等による被害軽減モデル案の提示
3 年以内に着手し実行に移す項目	―

⑤情報セキュリティ関連の法制度上の問題点に係る検討

3 年以内に実現する項目	―
3 年以内に着手し実行に移す項目	・情報セキュリティ関連の法制度上の問題点に係る検討

「戦略２：『高信頼性』を強みにするための公的対応の強化」を実現するための具体的施策
～戦略１の実現及び国家的視点からの全体を支える基盤の強化

（１）国の主権に関わるリスクへの対応

①情報収集･解析機能の整備

3 年以内に実現する項目	―
3 年以内に着手し実行に移す項目	・情報収集・解析機能の整備

②一極集中・依存リスクを回避した IT 基盤の形成

3 年以内に実現する項目	―
3 年以内に着手し実行に移す項目	・一極集中・依存リスクを回避した IT 基盤の形成

③RMA への取り組み強化

3 年以内に実現する項目	―
3 年以内に着手し実行に移す項目	・RMA への取り組み強化

（２）犯罪対策やプライバシー対策と国際協調

①犯罪対策の推進

3 年以内に実現する項目	―
3 年以内に着手し実行に移す項目	・犯罪対策の推進 ・犯罪対策のための技術開発

②プライバシー情報保護のあり方に関する検討

3 年以内に実現する項目	・プライバシーマーク制度の見直し
3 年以内に着手し実行に移す項目	・プライバシー情報保護の適切なモデルの提示

③情報セキュリティに関する国際協調の推進

3 年以内に実現する項目	―
3 年以内に着手し実行に移す項目	・情報セキュリティに係る国際協調の推進

（３）基礎技術基盤の確立

①ソフトウェア製造技術の高度化

3 年以内に実現する項目	・産学連携拠点の整備
3 年以内に着手し実行に移す項目	―

②セキュアプログラミング手法の確立と実用化

3 年以内に実現する項目	・産学連携拠点の整備
3 年以内に着手し実行に移す項目	―

③デバイス等基盤技術に関する産業基盤の強化

3 年以内に実現する項目	―
3 年以内に着手し実行に移す項目	・デバイス等基盤技術に関する産業基盤の強化

４．３．戦略の評価体制

今後、戦略の実施状況について評価し、内容を改訂する機能が必要である。

個々の情報セキュリティ対策だけでなく、情報セキュリティ政策においても、想定外の事態に対しどれだけ迅速に対処し、新しい方策を講じていくことができるかが重要であり、そうした観点から問題点を抽出・改善する意味でも、評価の構造が求められる。そこで、専門家からなる非常勤の「情報セキュリティ政策顧問会議」を設置し、戦略の実施状況の評価と改善案の検討を行う。

おわりに

第３章で提示した具体策を実現するにあたって、以下のような中長期的な重要課題についても併せて議論を深め、必要に応じ、今後の戦略の見直しに反映させていく必要がある。

①総合的な安全保障という視点から見た産業構造に係る分析

一極集中・依存が生じる恐れのあると指摘したケースとは逆に、国内企業が市場の生命線となる技術・製品をほぼ独占するようなケースもある。こうした存在は国際競争を前提とした産業政策上極めて重要であり、政策的に積極的な事業支援を必要とする場合もあると考えられる。しかし、今のところ、そのような視点では十分な調査研究がなされておらず、そうした重要な企業の実態が明らかにされていない。

②システム開発における多層的な下請け構造

我が国のシステム開発は、大手のシステムインテグレータが受注した場合も、実際にはその下請けや二次、三次、四次請けの企業が開発を行う、多層構造の体制で進められるケースが少なくない。さらに最近では、人件費が安い外国の企業に委託するケースも増えている。発注者が実際の開発工程に関与できない構造は、特に政府系のシステムの場合、結果的に主権リスクを内包する危険性がある。

③セキュリティ投資に係るコスト

本戦略を実行に移すためには、政府・自治体レベルはもちろんのこと、企業・個人レベルでも相応のセキュリティ投資が必要となる。米国では、2001 年 9 月 11 日の同時多発テロ以降、セキュリティの確保に要するコストの負担について、社会的に組み込まれたとの見方がある。日本ではそのようなコストの負担について、社会的にコンセンサスを得ることは容易ではないと思われる。検討においては、セキュリティ投資を積極的に行う組織等へのインセンティブや情報セキュリティに関する税制の導入についての提案もなされたが、今後、セキュリティ確保を図るための投資を促す施策や社会全体のコスト負担の最適解について検討を行う必要がある。また、社会全体のコスト負担に加え、セキュリティレベルと各主体が行うセキュリティ投資に係るコストの関係のベンチマークの策定についても併せて検討する必要がある。

④セキュリティとプライバシーの関係

セキュリティ確保のために公的な基盤を強化すると、結果として公的機関による個人の監視につながるとの懸念や、cookie や電子タグなど利便性が高まる新技術が普及すると、知らない間にプライバシーが損なわれうる場合があるとの懸念が指摘されることがある。暗号等のセキュリティ技術の高度化やセキュリティ対策の促進は、本来、各個人の情報の管理可能性を高めるものであり、結果としてプライバシー保護につながるものであるが、

今後、こうした、プライバシーとセキュリティ、そして新技術の相関関係について、深化した検討が必要である。

情報セキュリティ部会」委員名簿

【部会長】

寺島　実郎	財団法人日本総合研究所理事長／株式会社三井物産戦略研究所所長

【委員】

青木　千栄子	株式会社ディーワンダーランド代表取締役社長　兼　CEO
池上　徹彦	会津大学学長／独立行政法人産業技術総合研究所理事
今井　秀樹	東京大学教授
岡部　直明	株式会社日本経済新聞社取締役論説主幹
金杉　明信	日本電気株式会社代表取締役社長
坂村　健	東京大学教授
重村　勝弘	日立製作所ディフェンスシステム事業部顧問
島田　精一	日本ユニシス株式会社代表取締役社長
杉浦　康之	三菱商事株式会社国際戦略研究所所長
土居　範久	中央大学理工学部教授／慶應義塾大学名誉教授
中村　直司	株式会社 NTT データ代表取締役副社長
山口　英	奈良先端科学技術大学院大学情報科学研究科教授

【オブザーバ】

吉原　順二	内閣官房情報セキュリティ対策推進室副室長／内閣参事官
久保田　誠之	内閣府総合科学技術会議／参事官
宮城　直樹	警察庁生活安全局生活安全企画課セキュリティシステム対策室長／警視長
河村　延樹	防衛庁長官官房情報通信課長
牧　慎太郎	総務省自治行政局自治政策課情報政策企画官
武井　俊幸	総務省情報通信政策局情報流通振興課長

「情報セキュリティ総合戦略策定研究会」委員名簿

【委員長】

土居　範久	中央大学理工学部教授／慶應義塾大学名誉教授

【委員長代理】

山口　英	奈良先端技術大学院大学情報科学研究科教授

【委員】

岩村　奉武	社団法人日本経済団体連合会情報通信委員会情報化部会委員 （石川島播磨重工株式会社　理事・情報システム部長）
歌代　和正	株式会社インターネットイニシアティブ取締役技術本部 システム技術部部長
大木　栄二郎	NPO ネットワークリスクマネジメント協会幹事 （IBM ビジネスコンサルティングサービス株式会社チーフ・セキュリティ・オフィサー）
大野　浩之	内閣官房情報セキュリティ対策推進室 NIRT 総括・指導担当 （独立行政法人通信総合研究所 非常時通信グループリーダー）
岡村　久道	弁護士・近畿大学講師
勝山　光太郎	社団法人電子情報技術産業協会セキュリティ政策専門委員会委員長 （三菱電機情報技術総合研究所情報セキュリティ技術部部長）
楠　正憲	マイクロソフト　アジア リミテッド法務・政策企画統括本部政策企画本部 技術戦略部長
小山　覚	NTT コミュニケーションズ株式会社 IP インテグレーション事業部担当部長
佐々木　良一	東京電機大学工学部情報メディア学科教授
下村　正洋	NPO 日本ネットワークセキュリティ協会事務局長 （株式会社ディアイティ代表取締役社長）
田尾　陽一	セコムトラストネット株式会社代表取締役会長
高木　浩光	独立行政法人産業技術総合研究所グリッド研究センター セキュアプグラミングチーム長
手塚　悟	日本PKIフォーラム相互運用技術検討部会部会長 （株式会社日立製作所システム開発研究所第 7 部長）
中尾　康二	株式会社 KDDI 技術開発本部情報セキュリティ室長
長嶋　潔	東京海上火災保険株式会社情報産業部ｅリスクプロジェクトリーダー
西尾　秀一	情報サービス産業協会セキュリティ委員会委員 （NTT データ・セキュリティ株式会社技術本部コンサルティング部長）
廣川　聡美	横須賀市企画調整部情報政策担当部長
保科　剛	日本ユニシス株式会社アドバンストテクノロジ本部長
松浦　幹太	東京大学生産技術研究所・大学院情報学環助教授
松本　勉	横浜国立大学大学院環境情報研究院教授
丸山　満彦	公認会計士　監査法人トーマツ　エンタープライズリスクサービス部 シニアマネジャー
三輪　信雄	株式会社ラック代表取締役社長

【オブザーバ】

情報処理振興事業協会セキュリティセンター
製品評価技術基盤機構
日本情報処理開発協会
JPCERT コーディネーションセンター

活動記録

【情報セキュリティ部会】

2003 年 6 月 13 日	第１回会合	総合戦略策定の基本的視点について
2003 年 9 月 3 日	第２回会合	情報セキュリティ総合戦略骨子案について
2003 年 10 月 7 日	第３回会合	情報セキュリティ総合戦略（案）について

【情報セキュリティ総合戦略策定研究会】

2003 年 5 月 14 日	第１回会合	論点整理について
2003 年 5 月 29 日	第２回会合	検討に関する基本方針について 情報セキュリティに係るリスクイメージについて
2003 年 6 月 12 日	第３回会合	「総合戦略」策定の検討手順について 第１回情報セキュリティ部会の資料案について
2003 年 7 月 1 日	第４回会合	視点の整理について 情報セキュリティの課題の全体像について 重要インフラセキュリティについて
2003 年 8 月 8 日	第５回会合	「戦略」の視点について 重点課題と実現化施策について
2003 年 9 月 8 日	第６回会合	情報セキュリティ総合戦略骨子案について
2003 年 10 月 2 日	第７回会合	情報セキュリティ総合戦略（案）について

（参考）　本文中に用いた関連用語一覧（五十音、アルファベット順）

【あ行】

アジア PKI フォーラム
アジア地域の国々に対する統括的な PKI を実現するためのフォーラム。
（http://www.asia-pkiforum.org/）

暗号プロトコル
暗号アルゴリズムを組み合わせてデータ守秘等を実現する通信プロトコル。

インシデント
コンピュータセキュリティに関係する人為的事象。例えば、リソースの不正使用、サービス妨害行為、データの破壊、意図しない情報の開示や、さらにそれらに至るための行為 などがある。

ウイルスワクチンソフトベンダ
コンピュータウイルスやワームを検出・駆除するソフトウェア（ワクチンソフト）を提供する事業者。

オープンソース
ソフトウェアのソースコードを無償で開示し、世界中のプログラマがそれを自由に改良して再配布することを認めるソフトウェアの開発方式。

【さ行】

サイバー犯罪条約
インターネットを利用した国際犯罪に各国が共同して対処するため、欧州が提唱した条約。日米欧など 30 カ国が 2001 年 11 月に署名。

重要インフラ
本戦略では、経済活動と国民生活のライフラインとして深く影響を及ぼす業種等を広く対象としており、内閣の情報セキュリティ対策推進会議（「重要インフラのサイバーテロ対策に係る特別行動計画」(2000 年 12 月)）にて対象とされている重要インフラ７分野（情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス（地方公共団体を含む））以外にも、水道分野、医療分野、石油プラント分野等をその対象として捉えている。

重要インフラのサイバーテロ対策に係る特別行動計画
情報セキュリティ対策推進会議「重要インフラのサイバーテロ対策に係る特別行動計画」（2000 年 12 月）（http://www.kantei.go.jp/jp/it/security/index.html）

重要インフラのサイバーテロ対策に係る特別行動計画のフォローアップ
情報セキュリティ対策推進会議「重要インフラのサイバーテロ対策に係る特別行動計画のフォローアップについて」（2002 年 3 月）、「重要インフラのサイバーテロ対策に係る特別行動計画に基づく取組みの推進について」（2002 年 11 月）
（http://www.kantei.go.jp/jp/it/security/index.html）

情報セキュリティアドミニストレータ
情報処理技術者の公的資格の一つ。情報セキュリティに関する基本的な知識を持ち、情報システムのセキュリティポリシーの策定、実施、分析、見直しを行う能力が要求される。
（http://www.jitec.jp/1_11seido/h13/ss.html）

情報セキュリティ監査
　情報セキュリティに係わるリスクのマネジメントが効果的に実施されるように、リスクアセスメントに基づく適切なコントロールの整備・運用状況を、情報セキュリティ監査人が独立かつ専門的な立場から検証又は評価し、保証を与えあるいは助言を行なうこと。2003 年 4 月より、経済産業省告示に基づく「情報セキュリティ監査制度」の運用が開始されている。
　（http://www.meti.go.jp/policy/netsecurity/audit.htm）

情報セキュリティマネジメントシステム（ISMS）適合性評価制度
　2002 年 4 月より、日本情報処理開発協会から提供されている制度。個別の問題毎の技術対策の他に、組織のマネジメントとして、自らのリスク評価により必要なセキュリティレベルを決め、プランを持ち、資源配分して、システムを運用する。（http://www.isms.jipdec.jp/）

脆弱性
　何らかの理由により、性能を維持できなくなる原因となる、システムにおけるセキュリティ上の問題箇所。

セキュリティマネジメント
　セキュリティポリシーに基づき、組織の持つ情報資産の機密性、完全性、可用性を適切に維持・管理する作業を指す。

【た行】

電子政府推奨暗号リスト
　2003 年 2 月 20 日に総務省及び経済産業省により策定された電子政府における調達において推奨される暗号のリスト。2003 年 2 月 28 日の行政情報システム関係課長連絡会議において、各府省は同リストに掲載された暗号の利用を推進する旨が合意されている。

【は行】

バグ
プログラムがその作成者の想定と異なる挙動をとる現象、またはその原因となるプログラム上の誤り。

踏み台
　不正アクセス等により他者のコンピュータを乗っ取り、更なる不正アクセスや迷惑メール配信の中継等に悪用すること。

プライバシーマーク制度
　個人情報の取り扱い上、適切な保護措置を講じる体制を整えた民間事業者に対し「プライバシーマーク」の使用を認める制度（(財）日本情報処理開発協会実施)。1998 年より運用開始。（http://privacymark.jp/）

【ら行】

リスクプレミアム
　リスクを負担する者（投資家、金融機関など）から、リスクの大きさに応じて要求される「リターンの上乗せ」、「割増金利」あるいは「保険料」のこと。例えば、リスクが高い企業は、リスクプレミアムが高いため、高いリターンがなければ投資家は投資しにくい。

【わ行】

ワーム
　ネットワークを介して他のシステムへ自動的に感染することによって増殖するプログラム。

【アルファベット】

APCERT（Asia Pacific Computer Emergency Response Team）
アジア太平洋地域に存在する CSIRT（コンピュータインシデント緊急対応チーム）の協力関係をサポート・促進する目的で、2003 年 2 月、APSIRC2003（台湾）にて発足。
（http://www.apcert.org/）

Blaster ワーム
2003 年 8 月に発生したワーム。Microsoft Windows OS の脆弱性を狙う。感染すると PC が再起動を繰り返す症状が発生。また、毎月 16 日以降または 9 月以降にはマイクロソフトのサイトに DoS 攻撃をしかけるプログラムが組み込まれている。

CCRA（Common Criteria Recognition Arrangement）
1998 年に、米英仏独加の５カ国が統一した IT 製品の安全性評価基準（CC：Common Criteria）に基づいた認証結果を国際的に相互承認するために創設された枠組み。

CERT/CC（Computer Emergency Response Team / Coordination Center）
セキュリティインシデントや脆弱性に関する情報の収集・発信を行う組織。1988 年のワーム事件をきっかけとして、カーネギーメロン大学の SEI（Software Engineering Institute）内に設置された。（http://www.cert.org）

CISO（Chief Information Security Officer）
組織の情報セキュリティについての権限と責任を担い、経営の観点から率先して情報セキュリティを組織的に推進する、情報セキュリティに関する最高責任者。

CRYPTREC（Cryptography Research and Evaluation Committees）
電子政府の安全性及び信頼性を確保するため、暗号技術の安全性を客観的に評価することを目的として、総務省及び経済産業省により推進されている暗号技術評価プロジェクト。
（http://www.ipa.go.jp/security/enc/CRYPTREC/）

G8 リヨン・グループ（国際組織犯罪上級専門家会合）
G8 各国の組織犯罪対策の上級専門家によって構成される政府間会合。2002 年 5 月には、国際組織犯罪と闘うための 40 の勧告」を見直し、テロ対策を補足した「国際犯罪に関する G8 勧告」を策定。

GBDe（Global Business Dialogue on Electronic Commerce）
電子商取引に関する世界共通ルールの構築を目的として、世界のネット関連企業で構成される国際ビジネス会議。（http://www.gdbe.org/）

ISO/IEC15408
情報処理関連製品および情報処理システムのセキュリティレベルを評価する目的で 1999 年に制定された国際規格。

IT 事業者
IT の製品や部品、関連サービスを提供する事業者。情報システムやソフトウェアのメーカー、システムインテグレータ、コンサルティグファーム、情報サービス事業者等が該当する。

JPCERT/CC
JPCERT コーディネーションセンター：セキュリティインシデント（コンピュータセキュリティに関係する人為的事象で、意図的および偶発的なもの（その疑いがある場合を含む））報告への対応や、国内外のコンピュータセキュリティインシデント情報のコーディネーション等を行

う団体。（http://www.jpcert.or.jp/）

NIRT（National Incident Response Team）
国民生活に重大な影響を与えるおそれのある情報セキュリティに係る事案について各省庁等における情報セキュリティ対策の立案に必要な調査・助言等を行うため、内閣官房情報セキュリティ対策推進室に設置された緊急対応支援チーム。（http://www.bits.go.jp/shoukai/nirt/）

OECD 情報セキュリティガイドライン
1992 年に OECD で採択された情報セキュリティガイドライン（Guideline for the Security of Information Systems）が、2002 年 8 月に改訂された。“ Culture of Security ”の提唱、情報通信ネットワーク社会を前提とした点、個人を含む全ての参加者の責任、情報セキュリティマネジメントの概念の導入等が特徴。（http://www.oecd.org/sti/security-privacy）

P2P（Peer to Peer）
通常の Client/Server モデルと異なり、コンピュータ同士がネットワークを介して同等の立場で通信するモデル。Napster や Gnutella のようなファイル交換、動画チャットが可能なインスタントメッセージ、計算処理を分散して行うグリッドコンピューティング等の基盤技術となる。

RMA（Revolution in Military Affairs）
技術の高度化が軍事戦略や作戦行動におよぼす変革。急速に高度化する IT を活用して、リアルタイムに把握した情報に基づき、敵の最も緊要な部分に対し攻撃を加え、敵の組織的活動を低下させ、作戦を有利に運ぶ。

SLA（Service Level Agreement）
企業と顧客との契約で、提供されるサービスの基準を主に数値により明確に定義、測定し保証するもの。主に、サービスの可用性、故障回復時間、障害通知などが対象とされる。

Slammer ワーム
2003 年 1 月に発生したワーム。Microsoft SQL Server の脆弱性を標的とし、感染すると自分のコピーを大量に流し続け、ネットワークの帯域を消費する。

Telecom-ISAC Japan
通信サービスの提供を妨げる各種インシデントを収集・分析し、その分析結果を会員間で共有する ISP 向けの会員制組織。（https://www.telecom-isac.jp/）