第２次情報セキュリティ基本計画（案）

「IT時代の力強い「個」と「社会」の確立に向けて」

情報セキュリティ政策会議

年　月　日

目次

はじめに ..... - 1 -

第１章　第１次情報セキュリティ基本計画の下での取組みと２００９年の状況 ..... - 4 -
第１節　第１次情報セキュリティ基本計画の下での取組み ..... - 4 -
（１）第１次情報セキュリティ基本計画の意義 ..... - 4 -
（２）我が国の国家目標と情報セキュリティの位置付け ..... - 4 -
（３）基本理念　-「情報セキュリティ先進国」の思想- ..... - 5 -
（４）実現すべき基本目標　-「ＩＴを安心して利用可能な環境」の構築- ..... - 5 -
（５）基本目標の実現における課題と解決の方向性　-「新しい官民連携モデル」の構築へ- ..... - 5 -
（６）情報セキュリティ問題に取り組む上での基本方針 ..... - 6 -
第２節　２００９年の状況 ..... - 6 -
（１）対策実施４領域 ..... - 6 -
①　政府機関・地方公共団体 ..... - 6 -
②　重要インフラ ..... - 9 -
③　企業 ..... - 10 -
④　個人 ..... - 14 -
⑤　情報を預ける側の主体 ..... - 15 -
（２）横断的な情報セキュリティ基盤 ..... - 16 -
①　情報セキュリティ技術戦略の推進 ..... - 16 -
②　情報セキュリティ人材の育成・確保 ..... - 18 -
③　国際連携・協調の推進 ..... - 21 -
④　犯罪の取締り及び権利利益の保護・救済 ..... - 22 -

第２章　第２次情報セキュリティ基本計画における基本的考え方と２０１２年の姿 ..... - 25 -
第１節　第１次情報セキュリティ基本計画からの移行 ..... - 25 -
（１）第１次情報セキュリティ基本計画の下での取組みの結果と第２次情報セキュリティ基本計画の位置付け ..... - 25 -
（２）第１次情報セキュリティ基本計画からの「継続」と「発展」 ..... - 25 -
①　具体的取組みの持続的な推進と新たな課題への政策的対応 ..... - 26 -
②　「事故前提社会」への対応力強化 ..... - 27 -
③　合理性に裏付けられたアプローチの実現 ..... - 27 -
（３）第２次情報セキュリティ基本計画における基本的考え方 ..... - 28 -
①　実現すべき基本目標 -「ＩＴを安心して利用できる環境」の構築- ..... - 28 -
②　取組みにあたっての基本理念　-「セキュリティ立国」の思想の成熟 - ..... - 28 -

（ア） 成熟した情報セキュリティ先進国へ ..... - 28 -
（イ） ＩＴ時代の力強い「個」と「社会」の確立に向けて ..... - 29 -
（ウ） 世界との協調・イニシアティブの発揮へ ..... - 30 -
③ 基本目標の実現に向けた取組み -対策実施側の取組みの促進と、情報提供側の意識向上へ- ..... - 30 -
（ア） 「新しい官民連携モデル」 ..... - 30 -
（イ） 対策実施側と情報提供側の双方からの検討（２つのアプローチ） .... - 31 -
④ 第２次情報セキュリティ基本計画の下で取組みを行う政策の領域 ..... - 32 -
（ア） 課題の把握から事前対策、事後対応まで視野に入れた取組み ..... - 32 -
（イ） 技術面での対応から制度面、人的側面の対応まで視野に入れた取組み - 32 -
（ウ） 国内における情報セキュリティ対策の推進から、情報セキュリティ確保のために国際的になされる活動も視野に入れた取組み ..... - 32 -
（エ） 国民の日常生活や経済活動といった個別主体に直接的に関係の深い領域から、安全保障や文化といった我が国全体に関わりが深い領域にまで対応した取組み ..... - 33 -
第２節 ２０１２年の姿 ..... - 33 -
（１）対策実施４領域 ..... - 33 -
① 政府機関・地方公共団体 ..... - 33 -
② 重要インフラ ..... - 35 -
③ 企業 ..... - 37 -
④ 個人 ..... - 38 -
⑤ 情報を預ける側の主体 ..... - 40 -
（２）横断的な情報セキュリティ基盤 ..... - 40 -
① 情報セキュリティ技術戦略の推進 ..... - 40 -
② 情報セキュリティ人材の育成・確保 ..... - 42 -
③ 国際連携・協調の推進 ..... - 43 -
④ 犯罪の取締り及び権利利益の保護・救済 ..... - 45 -

第３章 今後３年間に取り組む重点政策 ..... - 47 -
第１節 対策実施４領域における取組みの推進と政策目的の着実な実現 ..... - 47 -
（１）対策実施４領域 ..... - 47 -
① 政府機関・地方公共団体 ..... - 47 -
② 重要インフラ ..... - 54 -
③ 企業 ..... - 55 -
④ 個人 ..... - 57 -
（２）横断的な情報セキュリティ基盤の強化と発展 ..... - 58 -
① 情報セキュリティ技術戦略の推進 ..... - 58 -
② 情報セキュリティ人材の育成・確保 ..... - 60 -

③　国際連携・協調の推進 ..... - 61 -
④　犯罪の取締り及び権利利益の保護・救済 ..... - 65 -

第４章　政策の推進体制と持続的改善の構造について ..... - 67 -
第１節　政策の推進体制 ..... - 67 -
（１）内閣官房情報セキュリティセンター（ＮＩＳＣ）の強化と役割 ..... - 67 -
（２）各府省庁の強化と役割 ..... - 67 -
（３）状況の変化の適時適切な把握と新しい課題への対応 ..... - 68 -
第２節　他の関係機関等との関係 ..... - 68 -
第３節　持続的改善構造の構築 ..... - 68 -
（１）「年度計画」の策定とその評価等 ..... - 69 -
（２）年度途中での緊急事態対応に向けた取組みの実施 ..... - 69 -
（３）評価指標の改善 ..... - 69 -
（４）第２次情報セキュリティ基本計画の見直し ..... - 69 -

はじめに

我が国の情報セキュリティ問題への取組みは、２００５年４月に内閣官房に情報セキュリティセンター（以下「ＮＩＳＣ[1]」という。）が、同年５月に高度情報通信ネットワーク社会推進戦略本部（以下「ＩＴ戦略本部」という。）に情報セキュリティ政策会議が設置され、抜本的な強化が開始された。

具体的な強化策は、e-Japan 重点計画等の一部となっている「情報セキュリティ」の問題を個別重点的に捉えた上で、戦略的思考に基づいた体系的な計画を構築すること、すなわち、２００６年度から２００８年度までの３か年の中長期の戦略である第１次情報セキュリティ基本計画[2]（以下「第１次基本計画」という。）の策定という形で結実した。

これ以降、ＮＩＳＣが主導的な役割を担う形で、官民の各主体によって２年以上にわたって様々な取組みが進められ、対策は着実に進展してきた。

一方、昨今の社会情勢を見ると、証券取引システムや金融機関の現金自動預け払い機、自動改札システム等における障害の発生、不正アクセスによるカード情報の大量窃取、ファイル共有ソフト及びコンピュータ・ウイルスによる重要情報の漏えいなど、もはや社会基盤化したと言える情報技術（以下「ＩＴ」という。）を利用・活用する上でのリスクは依然として存在している。また、ボットネット等による脅威の深刻化や、ソーシャルエンジニアリングを駆使し、特定の組織・個人を狙う標的型攻撃（スピア型攻撃）のような攻撃手法など、新たなリスクも日々発生している。さらに、社会におけるＩＴの活用方法は、例えば、地上波デジタル放送の展開とともに、家電利用におけるネットワーク活用が国民生活にとって極めて重要になってきていることや、カーナビのネットワーク接続の進展が一般的になっていること、日常生活で必要な行政手続の電子化推進など、年々進化を遂げ、第１次基本計画策定時とは大きく変化している。こうした状況に連動して、情報セキュリティが対象とするべき事項も変化してきている。

このため、第１次基本計画に基づく各種の取組みの進展や社会環境の変化などを踏まえ、引き続き我が国全体として情報セキュリティ問題への取組みを力強く推進するために、２００９年度以降を念頭に置いた第２次情報セキュリティ基本計画（以下「第２次基本計画」という。）をここに策定する。情報セキュリティについては、中長期の視点から見た継続的な取組みが必要である一方、これを取り巻く環境変化が著しいことを踏まえ、第２次基本計画の計画期間については、第１次基本計画同様、3年間（２００９年度から２０１１年度まで）を対象とする。

---

1 National Information Security Center の略。

2 ２００６年2月2日　情報セキュリティ政策会議決定。

また、今後、第１次基本計画時の取組み同様、本基本計画に基づき、２００９年度から年度毎の推進計画を策定することとする。

第２次基本計画は、第１次基本計画の下での取組み状況、情報セキュリティ政策会議の下に設置された基本計画検討委員会の第１次提言、同提言を踏まえた政府での取組み、同じく情報セキュリティ政策会議の下に設置された重要インフラ専門委員会での検討などを踏まえて策定されている。

これによって、第２次基本計画の下での情報セキュリティ政策の取組みは、本基本計画を政策全体のいわば全体設計図とし、その下に政府機関分野、重要インフラ分野、そして政策全体の評価等に関する文書が、個別設計図として組み合わされる形でなされることとなる。個別設計図は、具体的には『政府機関の情報セキュリティ対策のための統一基準』（以下「政府機関統一基準」という。）、『重要インフラの情報セキュリティ対策に係る第２次行動計画』(以下「第２次行動計画」という。)、『「セキュア・ジャパン」の実現に向けた取組みの評価及び合理性を持った持続的改善の推進について』[3]及び『情報セキュリティの観点から見た我が国社会のあるべき姿及び政策の評価のあり方～「セキュア・ジャパン」の実現に向けた情報セキュリティ政策のＰＤＣＡ[4]サイクル確立へ～』[5]（以下これら二文書を「情報セキュリティ政策の評価等の枠組み文書」という。）の各文書となる。これらは、各々、関係府省庁等での検討や、重要インフラ専門委員会のような専門委員会による検討を踏まえて策定されたものであり、全体設計図が示す取組みの大きな方向性などを具体化するものである。

このような政策の全体構造の下、全体設計図である本基本計画では、第１章において、第１次基本計画の下での取組みを、基本理念や基本目標などを含めて簡単に振り返り、その結果、２００９年現在、どのような状況となっているのか述べる。第２章においては、第１章でまとめた状況を踏まえて、第２次基本計画の下で行う取組みに関する基本理念や基本目標などの要素について明確にした上で、第２次基本計画の取組み期間後である２０１２年に、どのような状況になると考えているのか述べる。そして、第３章においては、第２次基本計画の下で政府が今後３年間に取組みを行う重点政策について述べるとともに、最後に第４章においては、これらを実現し、継続させていくための政策の推進体制を示す。

なお、２００９年の状況、２０１２年の姿、重点政策のいずれにおいても、基

3　２００７年2月2日　情報セキュリティ政策会議決定。

4　Ｐｌａｎ（計画段階）・Ｄｏ（実施段階）・Ｃｈｅｃｋ（点検段階）・Ａｃｔ（改善処置段階）の略。

5　２００７年2月2日　情報セキュリティ政策会議了解。

本的には第１次基本計画の下での対策実施４領域、横断的基盤４領域の枠組みにのっとって分野ごとに記述を行う。ただし、昨今の状況を踏まえて、２００９年の状況及び２０１２年の姿においては、自身が有する情報を他の主体に預ける主体（情報提供主体）についても、別途柱立てを行った上で記述を行う。また、重点政策においては、情報提供主体に関する取組みは、対策を実施する主体の取組みの中で一緒に扱うこととする。

第２次基本計画における重要なメッセージの一つは、「事故前提社会」への対応力強化（第２章第１節を参照）である。これは、第１次基本計画の下での取組みが、事前対策に重点を置くような形で進められたことを受けて、万が一の事態における広い範囲での対応や復旧の準備にも注力することを意味する。もちろん、引き続き、あらゆる主体が情報セキュリティ上の問題の発生を防止するべく事前対策について最大限の努力を行う必要があることは言うまでもない。第２次基本計画を受けて、あらゆる主体は事前から事後まで、一貫した情報セキュリティ対策を進めることが期待される。

第１章 第１次情報セキュリティ基本計画の下での取組みと２００９年の状況

第１節　　第１次情報セキュリティ基本計画の下での取組み

（１） 第１次情報セキュリティ基本計画の意義

第１次基本計画は、言わば、我が国における情報セキュリティ政策の立上げと、全ての主体にとっての「気付きを与える」ための戦略であった。すなわち、第１次基本計画によって、情報セキュリティをＩＴ関連の政策の中でも個別重点的な政策分野として立ち上げ、以降、政府機関・地方公共団体、重要インフラ、企業、個人といった官民の各主体が、国民生活・社会経済活動において依存度が高まってきているＩＴの安全・安心な利用を可能とするべく、知見を集中し、取組みを進めてきた。

具体的には、官民の各主体は、高品質[6]、高信頼性[7]、安全・安心を実現するために、情報セキュリティ上の問題が生じない水準[8]の達成を目指し、毎年度の年度計画である「セキュア・ジャパン」に基づいて積極的に取組みを進めてきた。

以下、第１次基本計画における基本的な考え方を簡単に振り返り、その後、第２章においては、第１次基本計画と第２次基本計画における考え方の違いを明らかにしていく。

（２） 我が国の国家目標と情報セキュリティの位置付け

第１次基本計画では、「ＩＴの利用・活用と国家目標の実現」との関係で情報セキュリティの位置付けを明らかにしてきた。具体的には、１）ＩＴの利用・活用を通じた経済の持続的発展[9]、２）ＩＴの利用・活用を通じたより良い国民生活の

6　例えば、バグが発生しないとか、想定外の操作に対しても何らかの対応が可能なことが挙げられる。

7　例えば、攻撃などによって負荷がかかっても止まりにくい、壊れにくいという状態や、止まったり、壊れたりしても迅速に復旧できることが挙げられる。

8　政府機関に関しては「１）２００８年までに政府機関統一基準のレベルを世界最高水準のものとし、かつ２）２００９年初めには、すべての政府機関において、政府機関統一基準が求める水準の対策を実施していることを目指し」、重要インフラに関しては「２００９年度初めには、重要インフラにおけるＩＴ障害の発生を限りなくゼロにすることを目指し」、企業に関しては、「２００９年度初めには、企業における情報セキュリティ対策の実施状況を世界トップクラスの水準にすることを目指し」、個人に関しては「２００９年度初めには、「ＩＴ利用に不安を感じる」とする個人を限りなくゼロにすることを目指」すこととされている。

9　経済大国日本の持続的発展とＩＴの利用・活用との関係で、「・・・企業活動のグローバル化と分散化に対応して、強固な国際競争力と高い生産性を維持するためには、ＩＴの利用・活用 が不可欠であるということは言うまでもない。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、我が国の経済活動の持続的発展を遂げることが重要な国家目標である。」 とされている。

実現[10]、３）ＩＴの利用・活用によって発生する脅威からの安全保障[11]に関連し、情報セキュリティを「ＩＴ基盤を、真に依存可能で強固なものにする」ためのものとして位置付けている。

（３） 基本理念　-「情報セキュリティ先進国」の思想-

第１次基本計画では、「セキュリティ立国」の思想（『高品質、高信頼性、安全・安心』の代名詞としての「ジャパン・モデル」の確立と、その世界への展開を視野に入れること）に基づく取組みを推進することをうたってきた。そして、我が国の在り方を「情報セキュリティ先進国」となることとしてきた。

（４） 実現すべき基本目標　-「ＩＴを安心して利用可能な環境」の構築-

我が国の情報セキュリティ分野における最重要目標は、ＩＴ利用に際して、安全・安心を確保することである。第１次基本計画では、高度情報通信ネットワーク社会形成基本法（ＩＴ基本法）第２２条にうたわれている「高度情報通信ネットワークを安心して利用可能な環境（以下「ＩＴ安心利用環境」という。）」の構築を基本目標としてきた。第１次基本計画では、単に安全なだけではなく、「予防」、「（対策が施された環境の）認識・体感」、「事業継続性」という３条件を満足し、利用者が安心を実感しながらＩＴを利用・活用できる環境することを目指していた。

他方、実際に第１次基本計画の下での個別分野ごとの目標や、取り組まれた施策の多くは、事前対策を念頭に置いたものであった。

（５） 基本目標の実現における課題と解決の方向性　-「新しい官民連携モデル」の構築へ-

第１次基本計画では、ＩＴ安心利用環境を構築する際の課題[12]解決の方向性として、「ＩＴ社会を構成するあらゆる主体が、情報セキュリティ問題への取組みの重要性についての共通の認識の下、自らの責任を自覚しながら、それぞれの立場

10　より良い国民生活の実現とＩＴの利用・活用との関係で、「経済活動だけではなく、２１世紀の我が国が直面する社会問題の解決のためにも、ＩＴの利用・活用が不可欠となり始めている。・・・ＩＴを重要な手段として利用・活用し、我が国が直面する社会問題を解決し、安全・安心で、より良い国民生活を実現していくことが重要な国家目標である。」とされている。

11　我が国の安全保障におけるＩＴに起因する新たな脅威への対応との関係で、「・・・ＩＴの利用・活用の拡大によって新たな脅威が発生していることを認識し、これに十分対応していけるよう、関係機関がその体制を強化しつつ連携し、我が国の安全保障を確保していくことが重要な国家目標である。」とされている。

12　課題として、「１）顕在化した問題のみに対する対症療法的な対応が支配的であること、２）ＩＴ社会を構成する各主体が、組織の縦割り構造の中で独自の対応に終始していること」が挙げられている。

に応じた適切な役割分担の下で対策を実施」する「新しい官民連携モデル」の構築を掲げてきた。そして、我が国全体として国家的視野に立って情報セキュリティ問題へ取組んでいくこととされてきた。

（６） 情報セキュリティ問題に取り組む上での基本方針

第１次基本計画では、我が国全体として国家的視野に立った情報セキュリティ問題への取組みを行うに際して、資源の重点的・戦略的投入の強化に向けた基本方針を設定した。具体的には、「官民各主体の共通認識の形成」、「先進的技術の追求」、「公的対応能力の強化」、「連携・協調の推進」の４つを基本方針としてきた。

第２節　　２００９年の状況

現在、第１次基本計画に基づいて３か年の取組みを官民の様々な主体が進めてきたところである。以下では、第１次基本計画の下での取組みを受けて、２００９年時点で情報セキュリティに係る我が国の状況がどのようになっているのかを述べる。具体的には、対策実施４領域、横断的な情報セキュリティ基盤という第１次基本計画の枠組みに即して述べる。

また、異なる主体同士で情報のやり取りを行った上で、その情報を特定の主体が管理する際の情報セキュリティを考えると、情報を管理する側のみならず、例えば一般消費者のように情報を預ける側の主体に関する検討も重要である。情報を預ける側の主体については、第１次基本計画では対象としてこなかったものの、以下では、情報を預ける側の主体の２００９年の状況についても述べる。なお、これについては便宜的に、（１）「対策実施４領域」の⑤において記述する。

（１） 対策実施４領域

① 政府機関・地方公共団体

[政府機関]

政府機関については、第１次基本計画の下、「１）２００８年度までに政府機関統一基準のレベルを世界最高水準のものとし、かつ２）２００９年度初めには、すべての政府機関において、政府機関統一基準が求める水準の対策を実施していることを目指し」て、各政府機関のＰＤＣＡサイクル及び情報セキュリティ政策会議による評価・勧告を中心とした政府機関全体のＰＤＣＡサイクルという２階層のＰＤＣＡサイクルを構築し、情報セキュリティ対策を促進するため様々な取組みを推進してきた。（図１参照）

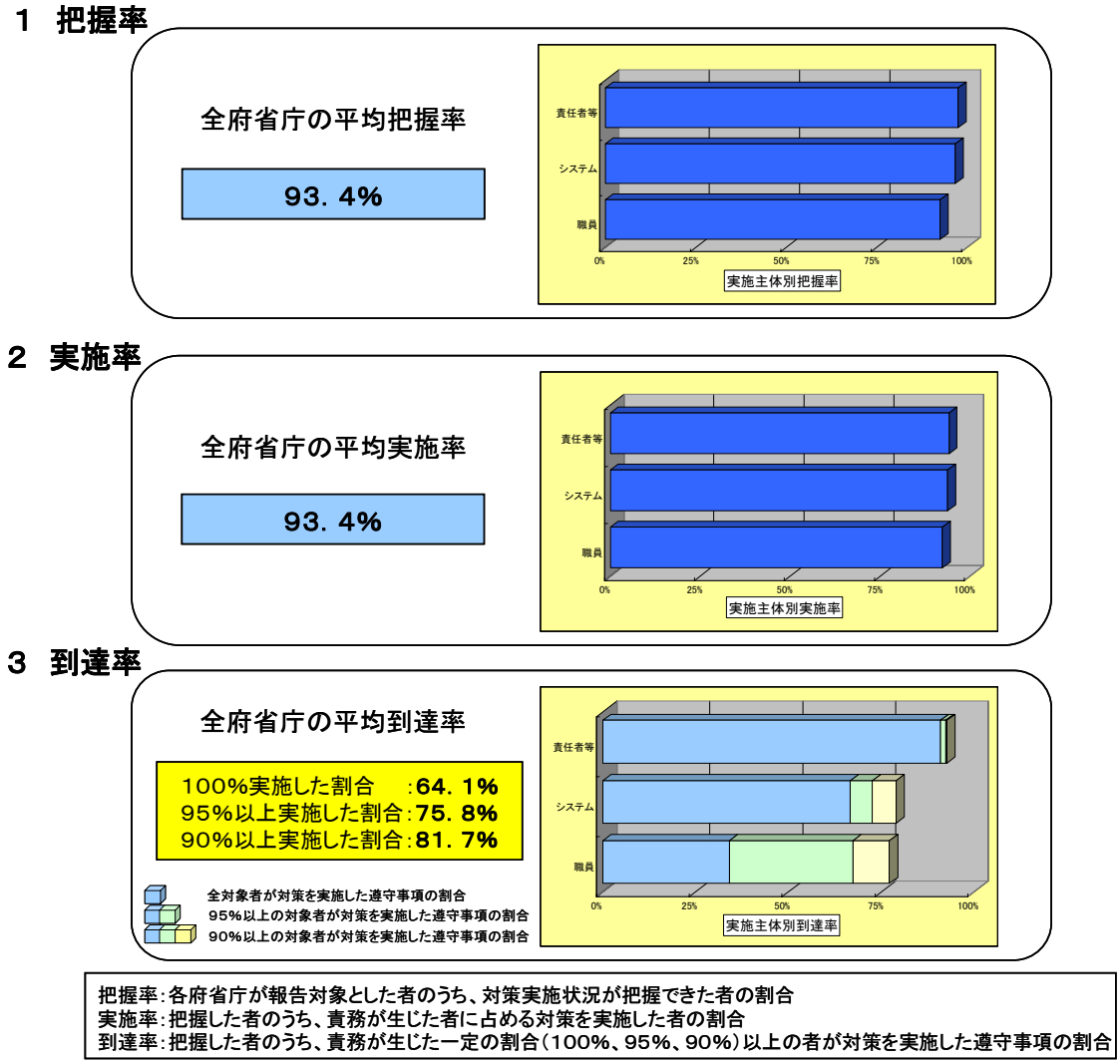


図１　政府機関の対策実施状況報告（２００７年度）の評価結果
（出典：「政府機関の対策実施状況報告（２００７年度）の概要」
２００８年４月２２日　情報セキュリティ政策会議報告より）

この結果、各政府機関における基本的なＰＤＣＡサイクルの構築は進んだものの、そこには以下のような課題も見受けられる。

第一に、これらのサイクルがまだ能動的なものとなり切れていない状況が、政府機関に見受けられるという点である。情報セキュリティ対策は、各政府機関の責任において講じていくことが原則である。それゆえＰＤＣＡサイクルも各政府機関の内発的な努力により能動的に推進されるべきものであるが、対策の実施やその結果の点検に際して、評価を受けるから実施するという受動的な意識が存在する機関があるともと考えられる。そのような機関においては、情報セキュリティ対策が対症療法的な対応に流れ、本質的な対策に至らない可能性がある。

第二の点は、上記とも関連するが、情報セキュリティ対策の推進に際して、自らが抱えるリスクを適切に把握し、それらを踏まえて自ら考えて実行するという意識がまだ十分に浸透していない状況が見受けられる。そのため、新しい脅威や想定していない事態が発生した場合に行政の継続性を確保できない危険性や、万全の措置を求めて情報セキュリティ対策上の要求が際限なく膨らんでいくおそれがある。

また、第三の点として、情報システムの構築に際して、利便性、コスト等とのバランスの中で適切な水準の情報セキュリティを確保するための取組みに苦慮している状況も見受けられる。

これらの課題の多くは、それぞれの政府機関のミッションとそれを支える情報セキュリティ、あるいはもっと広く情報システムとの関係性について、政府機関のトップマネジメントレベルではまだ十分理解されていないことに起因すると考えられる。また、情報システムを業務プロセスそのものを大きく変革するものとの認識も十分になされていないことが影響していると考えられる。

[地方公共団体]

地方公共団体については、第１次基本計画の下、「１）２００６年９月を目途に地方公共団体における情報セキュリティ確保に係るガイドラインの見直しを行うとともに、情報セキュリティ監査や研修等の対策を推進すること、また、２）２００６年度末までに地方公共団体間の情報共有体制が整備されることを目指し」て、様々な取組みを推進してきた。

結果、都道府県においては、監査の実施も含め、総じて対策が進展してきた状況にある。他方、市町村における監査の実施は、３割程度に留まるなど、様々な制約によって対策が遅れているものも存在する（図２参照）。今後も情報セキュリティに係る様々なリスクが生じ、それに対して対策を進めていく必要があると考えられるが、対策が十分に行えない小規模な市町村では、リスクが現実のものとなる可能性が高まり得る状況にある。

また、事務分野が多岐にわたる地方公共団体においては、国家行政組織と地方公共団体の担当組織の間で個別の関係を有する分野があり、情報セキュリティ対策への取組みも各々によって違いがある場合がある。結果、一つの地方公共団体を見た場合に、事務分野ごとの情報資産の活用度に基づいて許容される差異を超えて、情報セキュリティ対策の水準に違いが生じ得る状況にある。

さらに、地域における情報セキュリティの取組みを進める観点からは、地方公共団体がそれ自体の情報セキュリティ対策の取組みを行うこともさることながら、地域における情報セキュリティの基盤を強化するべく、地方公共団体が活動しやすい環境が整備されることも重要である。

現在、地方公共団体等が情報セキュリティに係る広報啓発活動や市民向けセミナー等を精力的に行っている例もみられるが、各々の地域における取組みの担い手が十分に育っていない地域もある。このため、地域における情報セキュリティ対策が実効性を伴わない可能性がある。

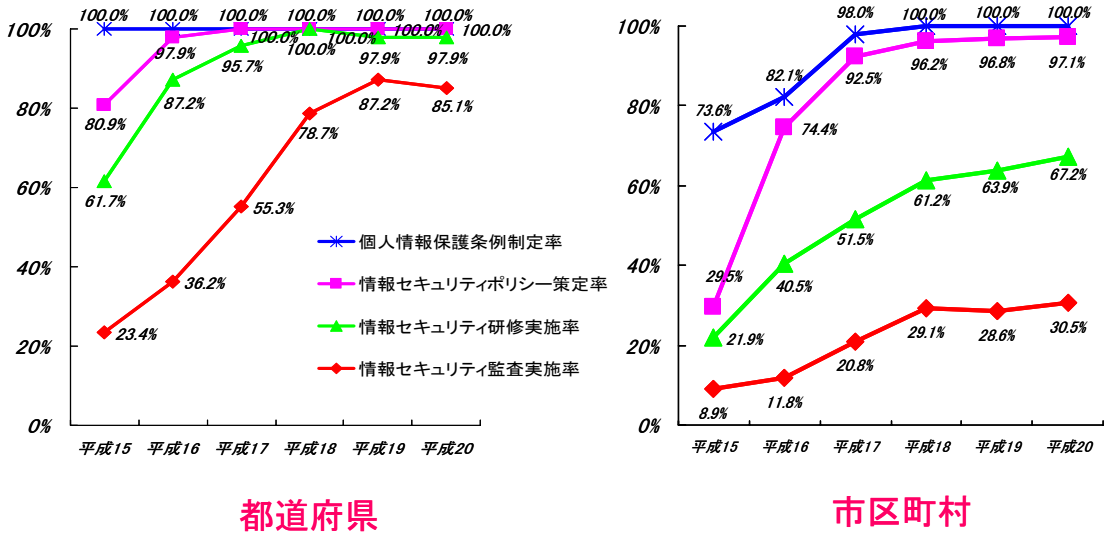


図　2　地方公共団体　情報セキュリティ対策の現状

（出典：総務省　「地方自治情報管理概要～電子自治体の推進状況～（平成 20 年 10 月）」）

②　重要インフラ

第１次基本計画の取組みを進める間にも、ＩＴの利用はさらに広範にわたるものとなっており、重要インフラ事業者等[13]の業務効率化や、サービスの利便性向上などの面で様々な工夫や進歩が続いている。また、サービス利用者においても、ネットワーク環境の充実やＩＴリテラシーの高まりによって、ＩＴを利用したサービスに触れる機会が増えている。今後も国民生活や社会経済活動は引き続きＩＴの利用を拡大しながら発展を続けると予想されるが、これは同時に社会がＩＴへの依存度を高める傾向にあることを意味する。

13　「重要インフラ事業者等」とは、「重要インフラの情報セキュリティ対策に係る第２次行動計画」中「Ｉ２定義と対象範囲」に示す定義による。以下同じ。

第１次基本計画の下、政府は重要インフラにおけるＩＴ障害の発生を限りなくゼロにすることを目指し、重要インフラ事業者等と共に取組みを進めてきた。重要インフラ分野では第１次基本計画に加えて、「重要インフラの情報セキュリティ対策に係る行動計画」（以下、「第１次行動計画」という。）が策定されており、①重要インフラにおける情報セキュリティ確保に係る「安全基準等」の整備（表１参照）、②情報共有体制の強化、③相互依存性解析の実施、④分野横断的な演習の実施、を施策の４本柱として推進してきた。

これによって、従来から各重要インフラ事業者等が取り組んできた対策に加えて、政府が施策面でこれを支援し、また分野横断的な観点から官民の取組みを連携させることを可能とする枠組みが構築された。しかし、ＩＴ依存の一層の深化に伴い、第１次行動計画や安全基準等の対象とならないサービスが開始・拡大している。また、安全基準等の適用対象とならないシステムも含めて、我が国の国民生活や社会経済活動に多大なる影響を及ぼすおそれが生じる障害が発生している。このため、こうした環境の変化に対して情報セキュリティ対策を機敏に対応させていく必要がある。

表１　安全基準等一覧（２００８年２月時点）

分野		安全基準等の名称
情報通信	電気通信	電気通信事業法、電気通信事業法施行規則、事業用電気通信設備規則等（関連する告示を含む） 情報通信ネットワーク安全・信頼性基準 電気通信分野における情報セキュリティ確保に係る安全基準（第1版）
	放送	放送における情報インフラの情報セキュリティ確保に関わる「安全基準等」策定ガイドライン
金融		金融機関等におけるセキュリティポリシー策定のための手引き 金融機関等コンピュータシステムの安全対策基準・解説書 金融機関等におけるコンティンジェンシープラン策定のための手引書
航空	航空運送	航空運送事業者における情報セキュリティ確保に係る安全ガイドライン
	航空管制	航空管制システムにおける情報セキュリティ確保に係る安全ガイドライン
鉄道		鉄道分野における情報セキュリティ確保に係る安全ガイドライン
電力		電力制御システム等における技術的水準・運用基準に関するガイドライン
ガス		製造・供給に係る制御系システムの情報セキュリティ対策ガイドライン
政府・行政		地方公共団体における情報セキュリティポリシーに関するガイドライン
医療		医療情報システムの安全管理に関するガイドライン第2版
水道		水道分野における情報セキュリティガイドライン
物流		物流分野における情報セキュリティ確保に係る安全ガイドライン

③　企業

第１次情報セキュリティ基本計画の下、「政府は２００９年度初めには、企業における情報セキュリティ対策の実施状況を世界トップクラスの水準にすることを

目指」し、取組みを進めてきた。例えば、情報セキュリティマネジメントシステム（ＩＳＭＳ）適合性評価の取得組織数は年々増加しており、国際比較においても最も多くなっている（図３、表２参照）。特に、企業にとって情報セキュリティの向上は、個人情報保護等の法的要請や、Ｐ to Ｐファイル交換ソフトウェア[14]に起因する情報流出等の顧客に対する責任や社会的責任といった観点から重要性を増しており、秘密情報や個人情報の持ち出し規定などのルールやセキュリティポリシーを定める企業が増えてきた（図４参照）。一方、企業の競争力・価値の源泉となる情報資産の利用・活用とその保護といった観点から、経営の一環として戦略的に情報セキュリティを推進するという取組みは未だ十分には認識されていない。また、大企業と中小企業の間で取組みに係る格差が拡大しつつある（図５参照）。このように、様々な課題も浮かび上がってきている。

課題は、第一に、企業における情報セキュリティ対策が真に有効なものとなるよう実効性を強化し、対策を更に促進することが必要という点が挙げられる。第１次基本計画の下では、「社会的責任にも配慮したコーポレートガバナンスと、それを支えるメカニズムである内部統制の仕組みを、情報セキュリティの観点から企業内に構築・運用することを推進」してきた。法的要求及び社会における企業の負うべき責任についての議論の中で、企業における内部統制システム構築については普及が進みつつある。しかし、内部統制システム構築は初期の段階であり、現在においては情報セキュリティ面での実装・実践について十分とは必ずしも言えない。このため、企業における情報セキュリティ対策の取組みが、企業価値の向上といった企業活動の基本的目的に対してプラスの影響を与えるという、実質的な効果を十分に発揮できない可能性がある。

第二には、情報セキュリティ対策によって、情報資産管理上の問題発生を未然に防ぐことは不可欠であるが、同時に、問題発生時に速やかに対応・復旧するための取組みの強化が必要という点が挙げられる。事前の対策をいくら進めたとしても、万が一の際への対応ができていないことで、情報セキュリティ上の問題が現実のものとなった際に、事業活動の停止や復旧の遅れが生じ、顧客の信頼を失う可能性がある。

第三には、認識不足及びリソース不足などを理由として情報セキュリティ対策を十分に実施することができない中小企業が少なくないことから、そのような中小企業を念頭に置いた取組みが必要という点が挙げられる。大企業を中心とした下請け構造及び大規模サプライチェーンにおいて、中小企業と協力しながら事業

14　インターネットを介して不特定多数の端末とファイル交換を行うためのソフトウェア。P to P（Peer to Peer）は、データの送受信にサーバの仲介を前提としない通信形態。

活動を進めることは我が国産業の競争力強化に欠くことができない。しかし、モノの流れ、ヒトの流れは情報の流れでもあり、情報資産の管理が不十分な企業が一つでも存在すれば、そこを介して価値の高い情報が流出し、関連企業全体の競争力低下につながる可能性がある。

そして、第四には、我が国の企業が進めるグローバルな事業展開、すなわち海外アウトソーシング、国際企業間取引（サプライチェーン）及び対外直接投資等の展開を円滑化するべく、日本国外のビジネス拠点において情報セキュリティ上の問題が生じないようにするための取組みが必要となってきている点が挙げられる。こうした取組みが十分に進まない場合、グローバル経済の下で我が国の産業が事業活動を進めていくことが難しくなる可能性がある。また、仮に海外拠点を活用するとしても、例えばアウトソーシング時に情報を過度に分散する必要が生じ、情報資産管理上のリスク及びコストが高まり、グローバルな事業展開のメリットを十分に享受できない可能性がある。

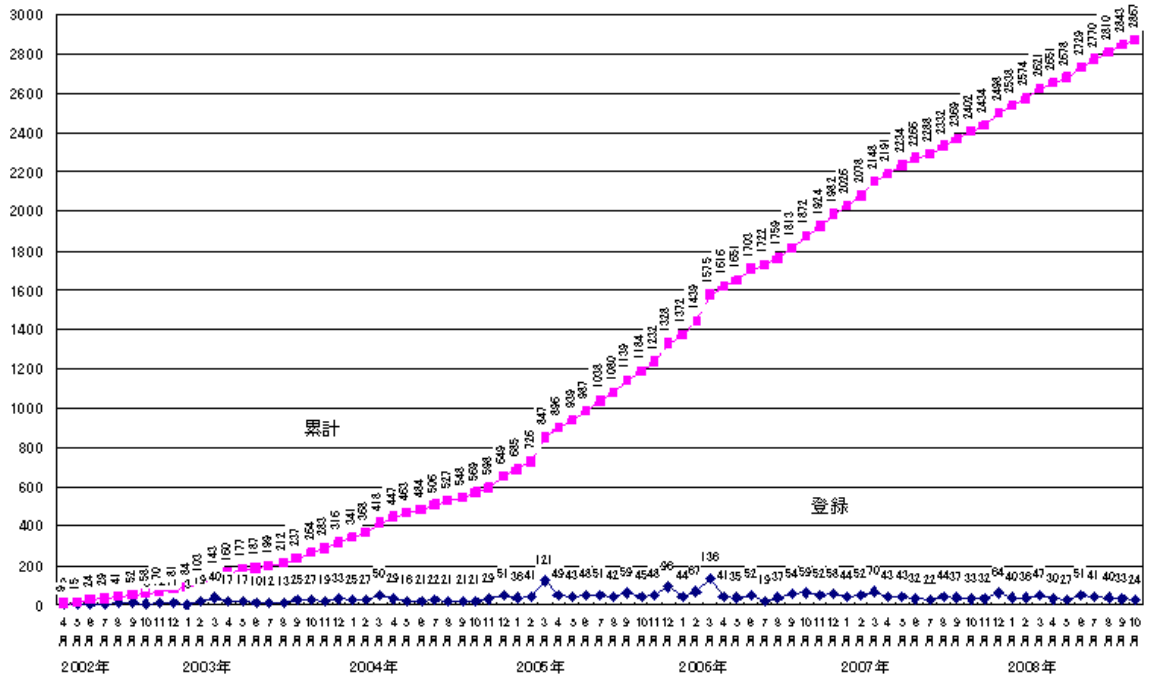


図 3　ＩＳＭＳ認証取得組織数推移
（出典：ＪＩＰＤＥＣ　ＨＰ、平成２０年１１月１１日現在の登録組織数）

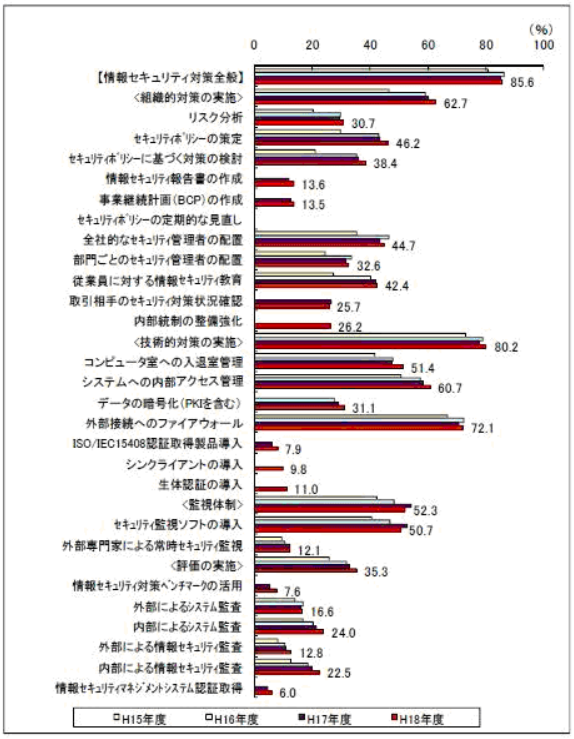
表 2　ＩＳＭＳ取得組織数の国際比較

国名	組織数	割合
日本	2863	57%
インド	433	9%
英国	368	7%
台湾	202	4%
中国	174	3%
ドイツ	108	2%
米国	82	2%
ハンガリー	74	1%
韓国	71	1%
チェコ	66	1%
総計	4987	

※　上位10カ国抜粋

（出典：International Register of ＩＳＭＳ Certificates のＨＰより作成

（平成２０年１１月現在））



（注）

1.情報セキュリティ対策の実施状況について「既に実施している」と回答した企業の割合の推移。

2.情報セキュリティ対策全般の実施率は、いずれかのセキュリティ対策の実施状況について回答した企業数に対する、いずれかのセキュリティ対策について「既に実施している」と回答した企業数により計算。

3.各カテゴリーの実施率は、それぞれのカテゴリーに属するいずれかのセキュリティ対策の実施状況について回答した企業数に対する、同カテゴリーに属するいずれかのセキュリティ対策について「既に実施している」と回答した企業数の割合により計算。

図 4　各情報セキュリティ対策について実施している企業の割合の推移

（出典：経済産業省「平成１９年情報処理実態調査結果」）

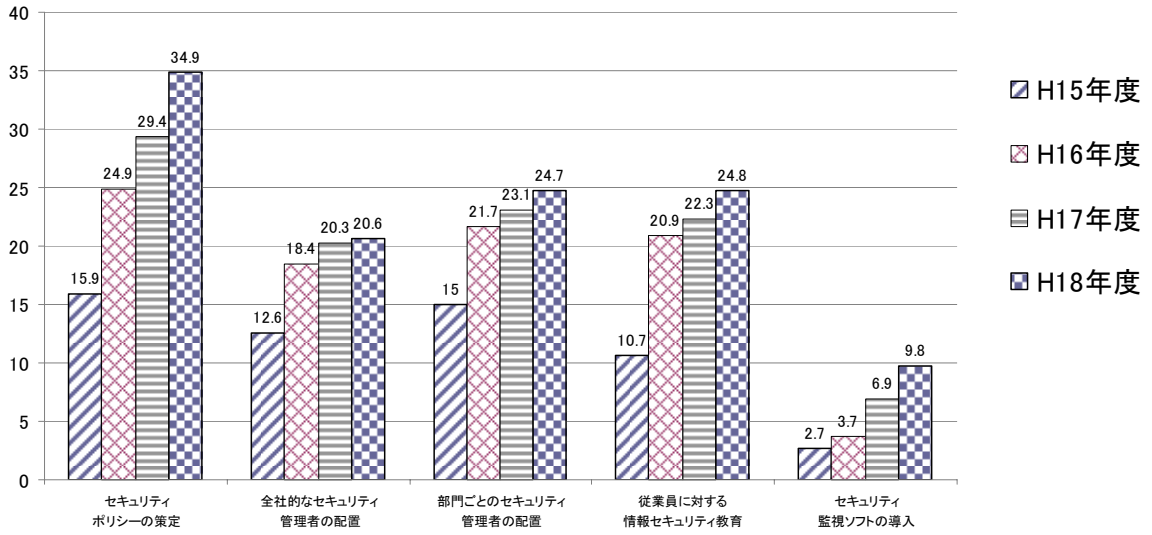


図 5　大企業と中小企業の格差
[対策実施率の差異]=[大企業における対策実施率]－[中小企業における対策実施率]
（経済産業省　「平成１９年情報処理実態調査」より作成）

④ 個人

個人分野では、第１次基本計画の下、「政府は、２００９年度初めには、「ＩＴ利用に不安を感じる」とする個人を限りなくゼロにすることを目指」し、取組みを進めてきた。しかし、例えば、インターネット利用に不安があるとする個人は４割を越えている（図６参照)。

個人が情報セキュリティに関連して直面するリスクに対しては、第１次基本計画の下では､広報啓発･情報発信などの手法によって取組みを進めてきたものの、リソースの限度も考慮すると、あらゆる個人に対して情報セキュリティ対策の重要性を浸透させることは容易ではない。取組みの手法に関する改善を加えない限りは、十分に効果が表れない可能性がある。

また、情報セキュリティ対策の重要性を理解しているにもかかわらず、対策を実施しない個人も少なからず存在していると考えられる。このため、広報啓発・情報発信のような手法の取組みでは、十分な効果が現れない可能性がある。

さらに、個人においては、情報セキュリティ対策の重要性について理解し、自身の対策を実施することで問題を発生させないというだけでは、取組みは不十分である。そもそもインターネットのサービス利用などを通じて自身に関する情報を預ける場合に、預けた主体が起こす問題によって、自身が大きな被害を受け得

ることを認識し、可能な対処を行うことが重要であるが、こうした点について未だ十分に理解が浸透していない可能性がある。

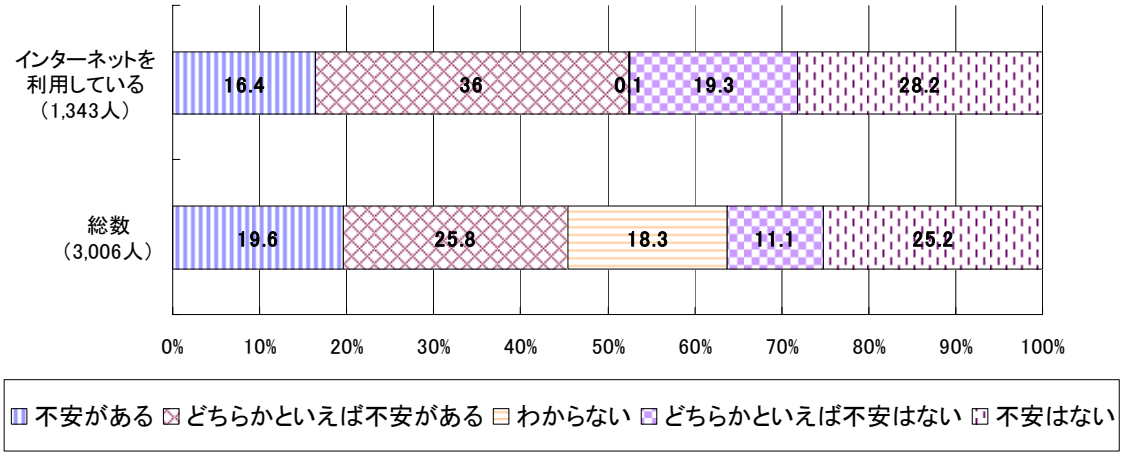


図 6　インターネット利用に対する不安感
（出典：内閣府　インターネット上の安全確保に関する世論調査（平成１９年調査））

⑤　情報を預ける側の主体

インターネット通信販売の充実や電子政府サービスの進展、ウェブやメールを通じた契約の増加など、日常生活でのＩＴの利用・活用が拡大するにつれて、個人や企業など様々な主体が、ＩＴを通じて自身の有する情報を相手側に預けるケースが増加している。そして、預けた情報が、更に第三者によって利用される場合も増えており、預けた情報がどこまで広がっているのか把握することは容易ではない。こうした状況下では、預けた電子情報がひとたび流出したり窃取されると、回収することはほぼ不可能となる。したがって、情報を預ける側の主体としても、このような事態が生じ得ることを十分に理解し、適切な行動をとることができないと、当初期待していた安全性と実際の安全性の間で大きな違いが生じる可能性がある。

とりわけ、最近では、インターネットを介した新しいサービス利用形態として、コンピュータを利用する際に、自身の有する情報を自身で管理するのではなく、自身が直接的に関与しないサーバなどで管理するような方式（例えば、クラウド・コンピューティング[15]と呼ばれるものなど）も見られるようになってきている。このため、情報を預ける側の主体の意識や実際に情報を預けるに際しての行動の

15　インターネット上に存在する計算機資源を使って、利用者がハードウェアやソフトウェアを保持・管理することなく、情報サービスやアプリケーションサービスを利用可能とする技術。

問題が更に大きくなっていると考えられる。

（２） 横断的な情報セキュリティ基盤

① 情報セキュリティ技術戦略の推進

第１次基本計画の下では、「先進的技術の追求」を基本方針の一つとして、「１）急速に拡大するＩＴの利用・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」を解決するため、①研究開発・技術開発の効率的な実施体制の構築、②情報セキュリティ技術開発の重点化と環境整備、③「グランドチャレンジ型」研究開発・技術開発の推進の３点が重点政策として掲げられ、取組みを進めてきた。

計画期間の３年間を経て、情報セキュリティ技術開発の重点化と環境整備に向けた事例も見られるようになった。具体的には、ボットを使ったサイバー攻撃等の課題を解決するための技術開発などの課題解決型の技術開発が数多く実施され、経路ハイジャックの検知・回復・予防に関する研究開発や仮想機械（バーチャルマシン）技術を用いた安全な環境の開発など、情報セキュリティ技術の高度化に向けた取組みの進展が見られた。

一方、組織・人間系の管理手法の高度化については、取組みが十分でなく、今後の実施が課題となる施策が存在する。また、２００７年度に構築した「研究開発・技術開発の効率的な実施体制」、「グランドチャレンジ型」研究開発・技術開発は一層の推進が必要である。

また、ＩＴの利用・活用の拡大などによる、第１次基本計画の期間の情報セキュリティを取り巻く社会情勢の変化に伴い、研究開発・技術開発の面で、新たに取り組むべき課題が浮かび上がってきた。

課題の第一は、情報家電、携帯電話・モバイル端末、ＲＦＩＤ[16]タグなど、情報機器やデバイスの急速な普及と高機能化、およびネットワーク上のサービス[17]の多様化などに伴って、国民のＩＴへの依存度が高まり、意図的・偶発的なものも含め、情報セキュリティに係る課題として扱うべき範囲が大幅に拡大する可能性が高いことである。

---

16 電波による非接触通信とＩＣチップを利用した認証技術

17 具体的なネットワーク上のサービスとしては、メールや検索サービス、ファイル保管、グループウェア、地図サービスなどが挙げられる。

第二は、高齢化など社会の世代構成の変化に対応して、使い方が簡単で、利用者のミスや誤認が情報セキュリティ上のリスクにつながらないようにするという発想[18]が、サービスや製品の設計・開発に際して、より重要となることである。（図７参照）

第三は、不正な経済的利得の獲得を目的として利用されるマルウェア[19]は年々増加しており、新たな脆弱性の発見や攻撃手法の開発のスピードも加速していることから、従来のセキュリティ対策では対応し切れなくなってきたことである。攻撃側と防御側の非対称[20]な状況に対抗するために、動的に変化していく脅威や潜在的な脅威に対応できる技術の開発と、それらの研究開発・技術開発を支援する実施体制が重要となっている。

18　いわばユニバーサル・デザインのコンセプトへの情報セキュリティの視点の導入である。

19　コンピュータウイルス、ワーム、スパイウェアなどの計算機及び利用者に害を与える悪意あるソフトウェアのこと。

20　攻撃者は攻撃手法の選択の自由度が高く、同時に複数のシステムに対して影響を及ぼせるなど、防御する側よりも有利な場合が多い。

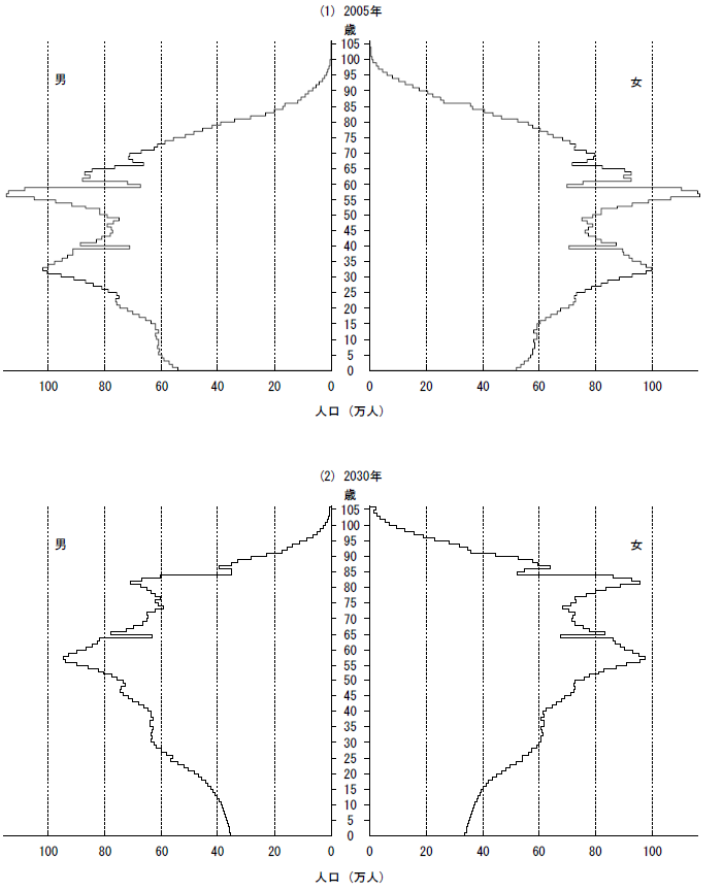


図 7 人口ピラミッドの変化：出生中位（死亡中位）推計
（出典：国立社会保障・人口問題研究所　「日本の将来推計人口（平成１８年１２月推計）」）

②　情報セキュリティ人材の育成・確保

情報セキュリティ人材の育成・確保については、第１次基本計画の下、「１）多面的・総合的能力を有する実務家・専門家の育成」を行うともに、「２）情報セキュリティに関する資格制度の体系化」について、人材育成・資格制度体系化専門委員会における検討をはじめとする様々な取組みを推進してきた。結果、現在、大学・大学院における情報セキュリティ人材の育成が推進されるとともに、実務家に対するキャリア・スキルのフレームワークの整備や、研修事業が行われている。

人材の育成においては、施策を開始してから成果が現れるまでに必要となる期間が長いため、第１次基本計画の下での成果は未だ明確にはなっていない。しかし、情報セキュリティに係る人材育成・確保に関する施策のニーズや問題点は、依然、多く存在する。例えば、政府機関においては情報セキュリティに携わる人員の不足や、短期のローテーションによって政府機関内部における知見が蓄積されない等の問題が指摘されている。そして、こうした指摘の有効性についての検

証も未だなされていない。また、情報セキュリティ業務に携わる人材の側からは、情報セキュリティ業務に携わっていく上での明確なキャリアパスが見えないと言った指摘も存在する。こうした状況が続くと、情報セキュリティ部門に優秀な人材が集まらなくなり、情報セキュリティを支える人材が不足する可能性もある。

また、資格制度の体系化については「人材育成・資格制度体系化専門委員会」によって検討がなされ、２００７年１月の報告の時点で資格制度の体系化まではなされている（図８参照）。しかし、情報セキュリティ業務に携わる人材から、資格の取得によって得られる知識が、業務において一定程度有効であると認められるものの、資格制度が実際に業務を行うための要件として明確になっている訳ではなく、資格を取得するインセンティブが明確ではないといった指摘もなされている。このため、情報セキュリティに携わる人材が保有するスキルを業務の上で明確に位置付けることができず、情報セキュリティ業務に対して、適切な人材を配置することが難しくなる可能性もある。

求められる能力		情報セキュリティに係る人材								
大分類	小分類	情報セキュリティに関する製品・サービス・ソリューション等を提供する企業等における人材				政府機関、企業等の組織において情報セキュリティ対策に係る人材				
		技術系の製品等を提供する企業等における人材		管理系の製品等を提供する企業等における人材		幹部、経営者	一般職員社員	情報セキュリティ対策を担当する者		
		セキュリティ専門	一般	セキュリティコンサルティング	セキュリティ監査			CISO又はCISOを補佐する者	技術系分野	管理系分野
セキュリティリテラシー						α	α	α	α	α
所属する組織のセキュリティポリシー						α	α	α	α	α
管理系分野	マネジメント技術	C	C	A	A	γ	－	α	β	α
	リスク分析技術	C	C	A	A	γ	－	α	β	α
	情報セキュリティポリシーの策定	C	C	A	A	γ	－	α	β	α
	情報セキュリティ監査	C	C	B	A	γ	－	α	β	α
	関連知識	C	C	A	A	γ	－	α	β	α
	法令・規格	C	C	A	A	α	－	α	β	α
	事業継続経営（BCP/BCM）	C	C	A	A	α	－	α	β	α
	リスクコミュニケーション	C	C	A	C	α	－	α	β	β
	費用対効果	C	C	A	B	α	－	α	β	β
	人員計画	C	C	A	B	α	－	α	β	β
	教育・訓練	C	C	A	B	γ	－	α	β	α
	物理セキュリティ	C	C	A	B	γ	－	α	β	α
	調達管理					γ	－	α	β	α
	プロジェクトマネジメント	A	B	B	C	－	－	α	α	β
	セキュリティ運用	A	B	B	B	－	－	β	α	β
技術系分野	セキュリティアーキテクチャ	A	B	B	B	－	－	β	α	γ
情報セキュリティ基本技術	ネットワークインフラセキュリティ	A	B	B	C	－	－	β	α	γ
	セキュアプログラミング技法	A	B	C	C	－	－	β	α	γ
	セキュリティプロトコル	A	B	B	B	－	－	β	α	γ
	認証	A	B	B	C	－	－	β	α	γ
	アクセス制御	A	B	B	C	－	－	β	α	γ
	PKI	A	B	B	C	－	－	β	α	γ
	暗号	A	B	B	C	－	－	β	α	γ
	電子署名	A	B	B	C	－	－	β	α	γ
	不正コピー防止・電子透かし	A	B	B	C	－	－	β	α	γ
ウイルス・侵入等対策技術	ファイアーウォール	A	B	B	C	－	－	β	α	γ
	侵入検知	A	B	B	C	－	－	β	α	γ
	ウイルス	A	B	B	C	－	－	β	α	γ
	不正アクセス手法	A	B	B	C	－	－	β	α	γ
アプリケーションセキュリティ	全般	A	B	B	C	－	－	β	α	γ
	Web	A	B	B	C	－	－	β	α	γ
	電子メール	A	B	B	C	－	－	β	α	γ
	DNS(Domain Name System)	A	B	B	C	－	－	β	α	γ
OSセキュリティ	Unix、Linux	A	B	B	C	－	－	β	α	γ
	Windows	A	B	B	C	－	－	β	α	γ
	TrustedOS	A	B	B	C	－	－	β	α	γ
レベル判定型の教育プログラム		－	SV(IPA) CompTIA	CISM CISSP	CISA SAAJ	－	－	SU(IPA) CISM CISSP	－	SU(IPA) CISM CISSP
訓練・実習型の教育プログラム		iisec 中央大・COE CMU	iisec 中央大・拠点/副 工学院大 CMU	iisec CMU	－	－	－	iisec・CISO CMU	中央大・拠点/副 工学院大	－
		－	YRP ソフトピア・Tec ひょうご	－	－			－	YRP ソフトピア・Tec ひょうご	YRP ソフトピア・Mgt ひょうご
		SANS・Tec	CSPM・Tec NISM SANS・Ess	SANS・Mgt	JASA			SANS・TOP	CSBM CSPM・Tec SANS・Ess	CSPM・Mgt

(1) 情報セキュリティに関する製品・サービス・ソリューション等を提供する企業等における人材に求められる能力の凡例

- **A** 情報セキュリティ対策に直結する製品等の製造・開発・提供に直接携わる者として、関連する先端的な技術・製品や高度な管理手法について熟知し、これらを製品等の中で活用・実装し、提供できる能力
- **B** 情報セキュリティ対策に関係する、
  - ・技術系の製品等の製造・開発・提供に携わる中で、情報セキュリティの要求事項を理解し、製品等の中で実装・提供できる能力
  - ・管理系の製品等の提供に携わる中で、技術系の製品等や専門外の管理系の手法や製品等についても相当程度理解し、顧客に助言等できる能力
- **C** 情報セキュリティに関する製品等を製造・開発・提供する上で知識として身に付けておくべき能力

(2) 政府機関、企業等の組織において情報セキュリティ対策に係る人材に求められる能力の凡例

- **α** 提供される製品等に関する知識・技能を含め情報セキュリティ対策の目的やその手法について深く理解し、組織における直接の担当者としてこれを主導的に活用し、実践できる能力
- **β** 提供される製品等に関する知識・技能を含め情報セキュリティ対策の目的やその手法について一定程度理解し、組織において外部人材等の専門能力を有する者と連携しつつ、これを活用し、実践できる能力
- **γ** 組織における情報セキュリティ対策に係る知識として身に付けておくべき能力
- **－** 特に業務上必須とはされない能力

図 8　情報セキュリティに係る人材に求められる能力と各種教育プログラムの体系図

（出典：情報セキュリティ政策会議　「人材育成・資格制度体系化専門委員会報告書」（平成１９年１月２３日））

③ 国際連携・協調の推進

第１次基本計画の下、政府は、「諸外国の情報セキュリティ関係機関との間でＰＯＣ[21]を確立し、定期的な情報共有が行われていること、（中略）及び連携を通じた我が国のベストプラクティスが各国に採用されていること[22] 」を目指し、取組みを進めた結果、内閣官房の組織としての認知度は高まってきたものの、今後は、より具体的な施策に基づいた国際連携・協調の推進を図っていく必要がある。一方で、情報セキュリティを取り巻く国際的な環境は、計画期間の３年間の間に大きく変化しており、国際連携・協調の推進方策の検討に当たってはこれらの環境変化も考慮に入れていく必要がある。

第一に、情報セキュリティ分野における国際連携に関しては、国家安全保障、重要情報インフラ[23]防護、グローバルな経済活動の継続性確保、サイバー犯罪防止等の様々な観点から、検討・対応を行うことが必要となってきている。このため、個々の国際機関の担当分野に関係が深い機関ごとの連携という、従来の縦割り的な国際連携に加えて、横断的な対応が求められるようになってきている。

第二に、不正アクセス、フィッシング、スパム、標的型攻撃、ウェブサイトからのマルウェアの感染等の脅威は、国境を越えて生じており、効果的な国際連携を通じた対策なしには、今後も増加の一途を辿っていくおそれがある。（表３参照）

第三に、諸外国の政府機関に対する、情報窃取を目的とした特定国からの攻撃の可能性に関する報告や、外国の一部政府機関に対するサービス不能攻撃に見られるように、現実社会における対立等が、サイバー空間にも影響を及ぼす可能性が高まっている。

第四に、政府機関及び重要インフラが、情報システムへの依存度を高め、また、これらの主体がサービスを提供する際や重要な情報発信を行う際などにインターネットを活用することが不可欠となっている。一方で、脅威は国境を越えて発生する可能性があることから、情報セキュリティの観点から見た事業継続性の確保にあたって、官民連携を促進するべく政府が最低限果たすべき役割の重要性が国

---

21 Point of Contact の略。

22 「情報セキュリティの観点から見た我が国社会のあるべき姿及び政策の評価のあり方（２００７年２月２日情報セキュリティ政策会議了解）」

23 ＯＥＣＤ情報コンピューター・通信政策委員会、情報セキュリティ・プライバシー部会における勧告文書“Recommendation of the Council on the Protection of Critical Information Infrastructure”において、重要情報インフラは①重要インフラを支える情報部分②政府の電子業務の極めて重要な部分を支える情報インフラ③国家経済に極めて重要な情報インフラの全てまたはいずれかを含むものとして説明されている。その他、Ｇ８、ＩＴＵ、Meridian で定義を付けずに使用されている。

際的に認識されてきている。

第五に、企業活動のグローバル化、ボーダーレス化の影響を受け、世界規模の最適調達、最適生産を目指した産業活動の細分化・専門化が進んでいる。このような企業活動に合わせて、企業が保有する重要な情報も国境を越えてやり取りが行われるようになっているため、情報システムを通じた情報の完全性、機密性、可用性が確保されない場合、あるいは現地企業の一定程度の情報セキュリティ水準が確保できない場合には、我が国企業のグローバルな事業活動の展開を阻害する可能性がある。

同様に、情報システムの設計、資材調達、生産、供給に係る一連の過程（サプライチェーン）がグローバル化・複雑化していることを受け、サプライチェーンを経て提供される製品・サービスの品質の検証が困難な状況にあることが明らかになってきている。一部では、マルウェアが組み込まれた製品が市場に流通する等、品質を確保するための手段が明確化されない限り、政府等による情報システムの調達に際して、安全保障上の懸念が生じるおそれがある。

表 3　不正アクセス行為の認知件数の推移

区分＼年次	平成15年	平成16年	平成17年	平成18年	平成19年
認知件数（件）	212	356	592	946	1,818
海外からのアクセス	35	37	53	37	79
国内からのアクセス	158	303	487	855	1,684
アクセス元不明	19	16	52	54	55

（出典：国家公安委員会、総務省、経済産業省　「不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況」（平成２０年２月２９日））

④　犯罪の取締り及び権利利益の保護・救済

第 1 次基本計画の下、各種の研修等の実施によるサイバー犯罪[24]取締りのための技能水準の向上、捜査・解析用資機材の整備・増強、デジタルフォレンジック[25]に係る知見の集約・体系化、サイバーテロ[26]対策に係る官民連携の促進等の基盤整備が進められた。

24　インターネット等の高度情報通信ネットワークを利用した犯罪やコンピュータ又は電磁的記録を対象とした犯罪等の情報技術を利用した犯罪。

25　不正アクセスや機密情報漏えい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（Digital Forensics）。

26　重要インフラの基幹システムに対する電子的攻撃又は重要インフラの基幹システムにおける重大な障害で電子的攻撃による可能性が高いもの。

また、サイバー犯罪は容易に国境を越えて行われることから、Ｇ８等の国際的な協議の場で捜査機関相互の協力や各国国内の体制整備に関する議論、国際刑事警察機構（ＩＣＰＯ‐Interpol）における捜査手法に関する情報の交換等への積極的な参加、アジア大洋州地域サイバー犯罪捜査技術会議の開催等を通じた国際的な連携強化が推進された。

さらに、サイバー犯罪条約を締結するため「犯罪の国際化及び組織化並びに情報処理の高度化に対処するための刑法等の一部を改正する法律案」が第 163 回国会に提出された（現在も継続審議中）。

このほか、サイバー空間上における権利利益の保護・救済に関する調査研究、サイバー空間の安全性・信頼性を向上させるための基礎技術の開発等についても一定の進捗を見た。

この結果、犯罪の取締り及び権利利益の保護・救済のための基盤整備はある程度進捗したものの、そこには以下のような課題も見受けられる。

サイバー犯罪は年々増加し、犯罪の手口についても高度化・多様化しており、捜査がより困難なものとなっている可能性がある（図９参照）。

また、２００７年内閣府調査「インターネット上における安全確保に関する世論調査」によれば、インターネット利用者の半数以上（５２．３％）がインターネットの利用に関して不安を感じている状況（インターネットを利用しない者を含めた全体では４５．４％）にあり、今後も強力に対策を実施し続けなければ、国民の不安感が十分に軽減されない可能性がある（図６参照）。

さらに、海外においては、外国の政府機関のコンピュータ・ネットワークへの侵入やサービス不能攻撃などが報告されており、我が国においてもサイバーテロの脅威が現実のものとなっている。

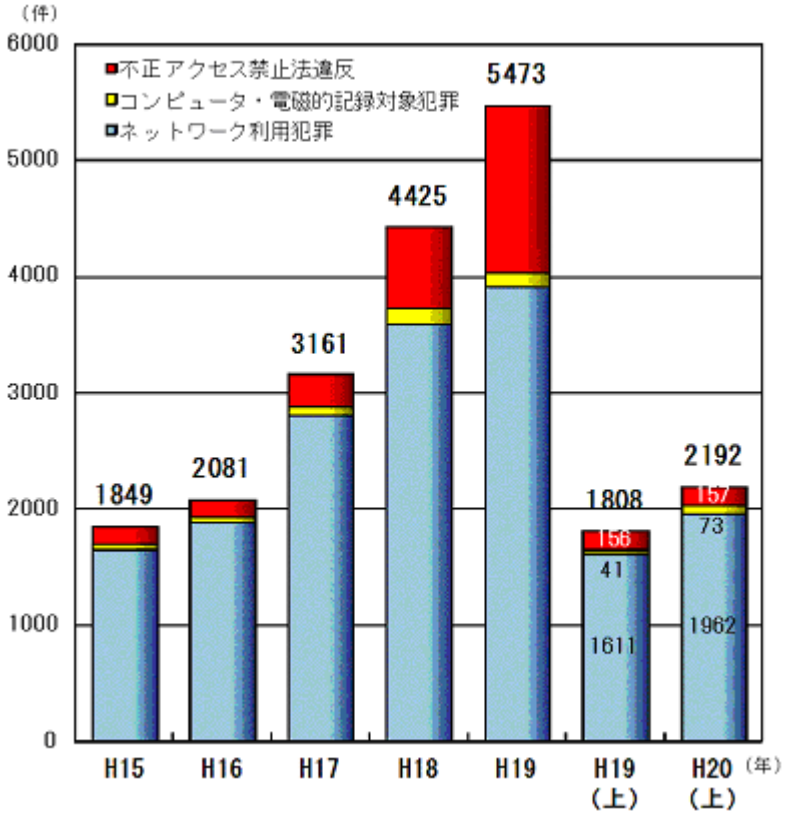


図 9　検挙件数の推移

（出典：警察庁　「平成２０年上半期のサイバー犯罪の検挙状況等について」
（平成２０年８月２１日））

第２章 第２次情報セキュリティ基本計画における基本的考え方と２０１２年の姿

第１節　　第１次情報セキュリティ基本計画からの移行

（１） 第１次情報セキュリティ基本計画の下での取組みの結果と第２次情報セキュリティ基本計画の位置付け

これまでの状況を踏まえると、第１次基本計画に基づく取組みは、おおむね当初の計画どおり実現できたと言える。しかし、現実の社会情勢を見ると、取組みの進展に反して、情報セキュリティ上のリスクは減少しているとは必ずしも言えない。リスクは、少なくとも、企業間（Ｂ to Ｂ[27]）、消費者向け（Ｂ to Ｃ[28]）電子商取引の拡大や様々な分野での情報システムによる基幹業務の遂行など、ＩＴの社会基盤化の更なる進展によって、より大規模なサイバー攻撃やＩＴ障害の発生の可能性へと、また、特定の組織や個人を狙う標的型攻撃や、検知や感染の認識が困難なボットに代表される、サイバー攻撃の巧妙化などによって、より目に見えにくいものへと、変質し始めている。

このため、第１次基本計画からの移行にあたっては、第１次基本計画の下での取組みを、現実を踏まえつつ必要な改善を図ることで、より良いものとする余地がある。

第２次基本計画は、このことを念頭に置いた、我が国全体を俯瞰した中長期的な戦略である。

（２） 第１次情報セキュリティ基本計画からの「継続」と「発展」

第２次基本計画は、第１次基本計画の「継続」の観点から、第１次基本計画の精神を基本的に継承する。第１次基本計画の下では、情報セキュリティ上の問題が生じない水準を実現するべく、例えば、組織において、あらかじめ基本方針を定め、対策推進体制を構築し、情報の取扱いや技術対策についてのルールを定めて適切に運用するといった、事前対策に特に焦点を当てた取組みを推進したところであるが、こうした取組みについては、第２次基本計画の下でも引き続き実現されることが望ましい。そして、その実現に向けて、各主体は引き続き最大限の尽力を行うべきである。とりわけ、マルウェアや不正アクセスによる被害や個人情報の漏えいの発生など、現時点の情報セキュリティ水準では十分であるとは言えず、対策を更に推進して水準を向上することが不可欠であることを関係者は十

27　Business to Bussiness の略。

28　Business to Consumer の略。

分に認識することが必要である。

他方、第１次基本計画からの「発展」が必要な側面もある。例えば、第１次基本計画の下で追求された水準は、時として絶対的な無謬性[29]の追求と言っても過言ではない水準であった。情報セキュリティに係るリスクの状況に鑑みると、このような水準の事前対策を実現することは、現実には容易でない[30]。実現可能性や、結果を追求するためのコストとのバランス、情報セキュリティの確保と引換え（トレードオフ）になり得る利便性とのバランスの観点を考慮する必要があるからである。また、このような絶対的な無謬性を追求するとしても、日々、情報セキュリティに係るリスクが変化する中で、リスクが現実化する可能性を無視するべきではない。このため、事前対策を中心とする従来の取組みを引き続き着実に推進することが不可欠であるのは言うまでもないが、現実に即した対策を実施できる政策体系を構築し、リスクが現実となった際に、様々な主体がより実際的な対応をとれるように取り組むという視点も必要である。

第２次基本計画は、第１次基本計画を以下の３つの観点に基づいて継続・発展させる。

①　具体的取組みの持続的な推進と新たな課題への政策的対応

第一に、第２次基本計画の下でも、第１次基本計画の下での取組み同様、各々の主体が努力を継続する必要があることは言うまでもない。

他方、第１次基本計画の下での取組みは、情報セキュリティ分野の立上げ期ということもあり、具体的取組みの下地となる基盤（枠組み）作りが少なくなかった[31]。第２次基本計画では、関係者は、第１次計画の下で構築された基盤（枠組み）を活用し、具体的取組みを実際に機能させていくべきである[32]。

29　第２次基本計画において、「無謬性」とは、一切誤りはなく完璧であることを意味する。情報セキュリティ分野において、重要な要素としてしばしば挙げられる integrity（完全性：情報や情報の処理方法が、正確で完全であるようにすること）を意味するわけではない。

30　「情報セキュリティ上の問題が生じない水準の事前対策」の実現が、「現実には容易ではない」としている趣旨は、「どれほど対策を実施したとしても、失敗や問題が生じることはあり得る（完璧であるという結果の実現は難しい）ということを認める、すなわち容認せざるを得ないリスクは存在し、これを acceptable risk として捉える」という意味であり、「必要な対策を行う体制や対策の内容などの改善を含め、対策を徹底的に行うことは容易ではない（ゆえに、適切な水準の対策であっても対策の徹底を行わなくても良い。）という意味ではない。「適切な水準の対策については徹底するべき」ということについては、ここに改めて強調する。

31　例えば、サイバー攻撃等に対する政府横断的対応体制の構築や、重要インフラのセプターカウンシル創設に向けた検討、人材育成分野における官民連携の協議会創設に向けた取組み、国際会議における新たな会議創設の提案などが挙げられる。

32　なお、政府機関統一基準に基づく対策など、依然取組みを強化することが必要な水準であるとは考えられるものの、短期間で一定の状況改善を実現できたものも存在している。これらについては、的確な対策を持続的に実施しつつ、ＩＴを巡る技術革新や社会制度の変化等を踏まえ、柔軟に対策の修正・向上を図っていくことが必

また、誤操作の可能性の高まりのような高齢化社会におけるＩＴの利用・活用への不安への対応や、人の国際的な移動の増加や事業活動の国際展開の増加のようなグローバル化の下でのＩＴ利用の安全・安心の確保など、従来は十分な対応を行ってきたとは必ずしも言えない新たな課題への政策的な対応を、果敢に行うことも必要である。

②　「事故前提社会」への対応力強化

第二に、第２次基本計画の下では、事故が生じ得ることを前提とした形での対応力を強めること、すなわち「事故前提社会」への対応力強化を実現する。このため、関係者は、事前対策の取組みにもかかわらず情報セキュリティ上の問題が生じた場合を考え、事態の認知・分析、情報連絡、迅速な対応・復旧などの事後対応にも十分な目配りを行う。すなわち、あらゆる関係主体は、情報漏えい、情報システムのサービス機能低下・停止などの情報セキュリティ上の問題の発生を防止するべく事前対策に最大限の努力を行いつつ、それでも万が一の事態が有り得ることを認識し、これに向けた準備を怠らない。そして、万が一の事態においては、その影響範囲、影響の度合い、緊急度、原因などの事実関係を明らかにしつつ、迅速な対応・復旧を広く進めることで、事業継続性を確保する。

「事故前提社会」への対応力強化に向けては、事故の可能性を完全に排除する情報セキュリティ対策の実現は容易ではないという点に関する理解（気付き）を社会全体で増進する必要がある。また、万が一問題が顕在化しても、気付きを持って自ら考える主体が、過敏な反応を起こさず、事実を冷静に受け止めて適切な対応を迅速に行うための取組みが不可欠である。

なお、ここで「事故前提社会」とは、事故が有り得るから諦めて予防のための対策を行なわないということや、被害に遭うのは仕方がないことであると諦めるということを意味するものでは決してない。

③　合理性に裏付けられたアプローチの実現

第三に、「事故前提社会」において、最適な水準（常に変化し続けるリスク[33]に関し、各々の主体及び社会全体にとって客観的に許容可能な範囲内に管理できる

要である。

33　「事故前提社会」では、脅威によってリスクが現実のものとなり得る事態を想定し、リスクを予見・予防するとともに、生じる損害や障害を極力小さくするべく、対処の手立てなどを検討するというリスク・マネジメント手法が重要となる。

情報セキュリティ水準）の対策を効果的・効率的に実施すること[34]、すなわち合理性に裏付けられたアプローチを実現する。情報セキュリティの取組みによる安全・安心の実現においては、コストと効果のバランスを実現すること、及び情報セキュリティの取組みを進めても利便性は失われず、むしろ情報セキュリティの取組みによって利便性が更に確固たるものとなることが有用であることから、このアプローチは肝要である。

これに際しては、アプローチの合理性を保つため、併せて対策の内容や水準に関する説明責任などを確実に果たすべきである。具体的には、リスクの把握と変化するリスクへの柔軟な対応を行う機能の強化や、最適な対策水準の設定、説明責任の明確化といった取組みの実現が不可欠である。

（３） 第２次情報セキュリティ基本計画における基本的考え方

① 実現すべき基本目標 -「ＩＴを安心して利用できる環境」の構築-

ＩＴの利用・活用が進む中で、その安全・安心を確保することによって、社会全体の発展を促すことは、情報セキュリティ政策の根本的な目的の一つである。このため、第２次基本計画においても、第１次基本計画で基本目標とされた、ＩＴ安心利用環境の構築を引き続き基本目標として中心に据え、構築のために解決が必要な政策課題への対応を図る。

第２次基本計画の下で、様々な主体が進める取組みは、最終的にはＩＴ安心利用環境の構築につながるものである。

② 取組みにあたっての基本理念 -「セキュリティ立国」の思想の成熟-

（ア） 成熟した情報セキュリティ先進国へ

基本目標の実現に向けては、基本的な理念、すなわち情報セキュリティの観点から見て、望ましい我が国の在り方を念頭に置きながら取組みを進めるべきである。第１次基本計画では、前述のように、「セキュリティ立国」の思想に基づく取組みを推進し、我が国が「情報セキュリティ先進国」となることを謳ってきた。

しかし、「「事故前提社会」への対応力強化」及び「合理性に裏付けられたアプローチの実現」の観点も踏まえながら、情報セキュリティ政策を発展させていく

---

34 より具体的には、情報資産の重要性とリスクの的確な評価（アセスメント）に応じた対策を確実に実施することを意味する。

ことを考えると、「セキュリティ立国」の思想には、１）冷静で迅速な対応、及び、２）最適な水準の対策の効果的・効率的な実施と説明責任の明確化という新たな要素が加わることが必要である。また、高品質や高信頼性といった概念は、第１次基本計画の下では、事実上、抽象的に完璧を求めることを意味してきたと言えるが、第２次基本計画ではより現実に即して、情報セキュリティ上の問題を生じさせないために、主体ごとに求められる最適な情報セキュリティ水準を達成できるような高い水準の品質や信頼性、と考えるべきである。

情報セキュリティに関して、第２次基本計画の下で目指すべき我が国の在り方は、情報セキュリティ上の問題を生じさせないための最適な水準の取組みと結果の実現ではあれ、絶対的な無謬性の追求ではない。むしろ、『冷静で迅速な対応、最適な水準の対策の効果的・効率的な実施と説明責任の明確化、主体ごとに求められる最適な情報セキュリティ水準を達成できる高品質や高信頼性、利用者にとっての安全・安心の確保』という、「セキュリティ立国」の思想の成熟による、より現実に即して実効的な情報セキュリティ対策が冷静に実現される「成熟した情報セキュリティ先進国」である。なお、いわゆる情報弱者[35]や高齢者[36]など、情報セキュリティに関連する取組みを自ら行いたくとも十分にできない可能性がある主体については、最適な情報セキュリティ水準を達成できるように支えていくことも重要である。

（イ） ＩＴ時代の力強い「個」と「社会」の確立に向けて

成熟した情報セキュリティ先進国の実現を念頭に置きながら情報セキュリティ対策を進めるには、様々な側面からの対応が必要である。この対応は、ＩＴに係る技術や制度の側面の具体的な対策が基本となる。

しかし、これらに加えて、情報セキュリティ対策を実施しながらＩＴを利用・活用するにあたっての、国民や、個々の主体の集まりによって成り立つ社会全体の意識改革も不可欠である。つまり、我が国国民や社会が、セキュリティに関する絶対的な無謬性の追求からは脱却し、

１）（対策に係る最大限の努力は必要であるが）事故の可能性を完全に排除する事前対策を目指したとしても、結果がそうはならない場合を考えておく必要があると理解すること、

35 本基本計画においては、様々な理由により、情報技術や通信技術の利用に困難を抱える人のことを言う。

36 情報弱者に該当することも少なくないと考えられるが、高齢者が誤操作によって情報セキュリティ上の問題を生じるような場合を念頭に置き、ここでは別途記載する。

２）万が一、実際に情報セキュリティ上の問題が発生したとしても、当事者は適切に対処して問題を解決し、周囲は問題の本質及び被害の規模を理解しながら、事態の深刻度合いを捉えられること、

が必要である。

このためには、情報セキュリティ対策の実施主体が、真摯に、かつ透明性を持って対策を進めることが大前提であるが、その前提の下で、国民や社会全体が、絶対的に完璧ではないという意味で受容すべき一定のリスクを受容し、このような現実を主体的に支えられるようになることが必要である。つまり、自ら理性的かつ主体的に考えるＩＴ時代の力強い「個」と「社会」の確立が不可欠である。

（ウ） 世界との協調・イニシアティブの発揮へ

成熟した情報セキュリティ立国の思想を念頭に置いて取組みを進めることによって、我が国の情報セキュリティ政策は、ＩＴ安心利用環境の構築に向けた、より現実に即したものとなる。我が国の情報セキュリティの取組みは、国際社会との関係でもより受入れられやすくなり、真にＩＴ先進国として発信や貢献を行える状態へ到達したと言えるようになる。

我が国は成熟したセキュリティ立国の思想の下、自国の取組みに自信を持って世界と協調し、その中で相応しいイニシアティブをとっていく。
また、同時に、世界における最高水準の取組みや、最先端の技術や最新のリスクの動向などについても、情報収集を怠らないようにするなどの十分な目配りを行い、我が国の取組みが世界の水準に遅れをとらないような留意も必要である。

③ 基本目標の実現に向けた取組み -対策実施側の取組みの促進と、情報提供側の意識向上へ-

（ア） 「新しい官民連携モデル」

第１次基本計画の下での３カ年が過ぎた現段階においても、構築から維持・発展を行い、ＩＴ社会を構成するあらゆる主体の気付きを伴った参加と適切な役割分担を追求することが不可欠である。第２次基本計画においては、第１次基本計画で掲げられた「新しい官民連携モデル」の維持・発展によって政策を更に進化させる。

（イ） 対策実施側と情報提供側の双方からの検討（２つのアプローチ）

第１次基本計画の下での「新しい官民連携モデル」は、ＩＴ社会を構成するあらゆる主体の参加を念頭に置き、

１）対策実施主体、すなわち対策を実際に適用し、実施する主体（①政府機関・地方公共団体、②重要インフラ、③企業、④個人）、

２）問題の理解・解決を促進する主体、すなわち対策実施主体が実際に対策を適用し、実施するにあたり、その対策の手法や環境整備を側面的に支援し、問題の理解・解決を促進する主体（①政策を立案・実施する主体としての政府・地方公共団体、②初等中等教育機関、高等教育機関及び研究開発・技術開発実施機関、③情報システムの構築や通信サービスの提供等ＩＴ基盤を構築・提供している事業者（以下「情報関連事業者」という。）や非営利組織（以下「情報関連非営利組織」という。）、④メディア）

を設定している。第２次基本計画の下でも、この枠組みは維持することとする。

しかし、「事故前提社会」への対応力強化とともに、合理性に裏付けられたアプローチを実現するべく、ＩＴ時代の強い「個」と「社会」を確立する観点からは、対策の実施に関わる側だけを念頭に置くのでは必ずしも十分ではない。情報セキュリティ対策によって守るべき情報資産は、対策を実施する主体自身のものだけではなく、他の主体から預かったものである場合もある。情報の受渡しの過程に関わる全ての主体が、事故の可能性を完全に排除することを目指したとしても、結果がそうはならない場合を考えておくべきであるということに関して、理解を深めることが必要である。

したがって、第２次基本計画では、情報を預ける側も政策の対象とし、

３）対策実施主体[37]を含めた対策推進側[38]以外に、個人情報のような自己の情報等を預ける情報提供主体[39]（、及び、その逆側の立場で情報を預かる情報管理主体[40]）

---

37 第１次基本計画では、対策を実施に適用し、実施する主体（対策実施主体）として、政府機関・地方公共団体、重要インフラ、企業、個人の４主体が挙げられている。

38 ここでは、対策実施主体以外に、第１次基本計画における「問題の理解・解決を促進する主体（以下「対策支援主体」という。）を含む。

39 潜在的にそうなり得る者も実際に情報を預けている者も双方を含む。つまり、全ての主体が情報提供主体となり得る。

40 実質的には、対策実施主体と同じ範囲を指す。

を設定する。つまり、第２次基本計画では、

１）対策を直接実施する主体や、対策を支援する主体を念頭に置いた第１次基本計画の下での従来のアプローチ

を補完・強化する形で、

２）情報を預ける主体を念頭に置いた新たなアプローチ

を採用し、２つのアプローチから取組みを進める。

④ 第２次情報セキュリティ基本計画の下で取組みを行う政策の領域

以上を踏まえて、ＩＴ安心利用環境の構築に向けて今後取組みを進める政策の領域は、以下のようにいくつかの側面から整理できる。このことからもわかるように、第２次基本計画の扱う政策領域は、相当程度多面的なものとなる。

（ア） 課題の把握から事前対策、事後対応まで視野に入れた取組み

情報セキュリティ政策を、より現実に即して実効的な政策とする観点から、課題の把握から事前の対策、さらには問題が発生した際の事後対応までを一貫して行う領域とする。そして、情報セキュリティ政策を、一連の対応能力が高い政策へ発展させる。

（イ） 技術面での対応から制度面、人的側面の対応まで視野に入れた取組み

情報セキュリティ対策の推進には、対策に係る技術的な側面に加えて、制度面や対策を実施する人的な側面からの総合的な対応が必要である。これらのバランスの良い組み合わせが必要であり、第２次基本計画の下においても、技術開発に関する取組みから人材育成のような取組みまで、総合的に取組みを行う。また、規範を含めた制度面に係る検討も進める。

（ウ） 国内における情報セキュリティ対策の推進から、情報セキュリティ確保のために国際的になされる活動も視野に入れた取組み

ＩＴの利用・活用が国境を越えて当たり前のこととなっていることに鑑みると、情報セキュリティ政策は、国内だけを対象として推進するのでは不十分である。

国内での対策はそれとして進めるが、同時に国際的な取組みと相互に有機的に結びついた政策へと発展させる。

（エ） 国民の日常生活や経済活動といった個別主体に直接的に関係の深い領域から、安全保障や文化といった我が国全体に関わりが深い領域にまで対応した取組み

第２次基本計画の下で取組みを行う情報セキュリティ政策の領域は、個人のＩＴ活用時における注意を喚起することや、企業の経済活動において預かった情報をどう管理するかといった、個別主体の日々の活動に直接的に関係の深いものが挙げられる。加えて、我が国の安全保障上重要な、情報セキュリティに係る脅威情報の国際的な把握や、情報セキュリティが重要であるという文化の醸成など、我が国全体に関わりの深い領域も挙げられる。

第２節　　２０１２年の姿

以下においては、第２次基本計画に基づく取組みを３年間進めることで、我が国の姿が計画期間終了後の２０１２年においてどのような姿となっているか述べる。ここにおいても、２００９年の状況と同様、対策実施４領域及び横断的な基盤４分野の枠組みにのっとって述べる。なお、情報を預ける側の主体については便宜的に「対策実施４領域」の⑤という形で記述する

（１） 対策実施４領域

① 政府機関・地方公共団体

[政府機関]

今後、行政分野へのＩＴの活用により、国民の利便性の向上と行政運営の簡素化、効率化、高度化等を推進していく中で、安全で安心な電子政府に対する国民からの関心はより高まり、情報セキュリティに対する要求は一層高度なものとなっていく。このため、政府機関は、**国内外の様々な組織にとって模範となるような情報セキュリティ対策を実施し、国民からの信頼に応えることができる安全かつ安心で効率的な行政運営、行政サービスの提供を行うことが可能な情報セキュリティ水準を確保していくこと**を目指して最大限の努力を行う。

このような将来像を目指すためのマイルストーンとして、第２次情報セキュリティ基本計画の下で、政府機関においては２０１２年時点で以下のような「姿」

を実現することを目標として、関係者は今後の取組みを進めていく。

第一は、**『政府機関における情報セキュリティガバナンス[41]の確立に向けた組織・体制の強化』**である。２０１２年には、全ての政府機関において能動的に情報セキュリティ対策に取り組む体制を確立するとともに、政府全体を通じて情報システムに情報セキュリティ対策が適切に組み込まれる仕組みを構築することにより、政府機関における情報セキュリティガバナンスの確立に向けた合理的な取組みが進展している。こうした体制の下で、政府機関において、情報セキュリティ人材の育成・確保等に向けた対策が計画的に推進され、適切な情報セキュリティ対策を適時に行うための取組みが、予算面の対応も含め進んでいる。また、技術面の知見を蓄積・活用する仕組みの構築も推進されている。

第二には、**『政府機関における事後対応力の強化』**である。２０１２年においては、各政府機関が保有する情報システムの災害・障害時の対応方針が、当該情報システムが支えている行政の優先度や重要性等に基づいて決定され、必要なシステムについては事業継続計画が策定されているなど、事後対応にも十分配慮した対策が進展している。また、万が一、事故等が発生した場合に備え、緊急時の対応及び復旧を念頭においた関係機関の連携体制の強化が図られている。

[地方公共団体]

第２次基本計画の下で、政府は**各々の地方公共団体において、また幅広い行政分野全体において、望ましい情報セキュリティ対策が実施されること**を目指して最大限の努力を行う。

結果、情報セキュリティに関連して、地方公共団体が直面する社会の状況は、２０１２年には以下のようになっていると考えられる。多くの地方公共団体においては、人口減少や厳しい財政状況の下、セキュリティも含めた情報システムに対する投資を現行水準で維持することは､容易ではなくなりつつある｡このため、地域間での取組みの連携など、一定のコストで必要な機能やセキュリティを効率的に確保する手法が積極的に模索されている。地方公共団体の行政分野は相当幅広いものであることから、望ましい情報セキュリティの確保が様々な分野において強く求められていることに加えて、地方分権の進展によって、地方公共団体が自ら､情報セキュリティへの取組みをより一層積極的に行うことが望まれている。

２０１２年のこのような社会において、地方公共団体の情報セキュリティの取

41　本基本計画において、政府機関に関して目指す情報セキュリティガバナンスとは、政府機関における内部統制の一環として、情報セキュリティ対策が効果的に推進されるような内部統制を確立することを意味する。

組みが以下のような「姿」となっていることを目指し、関係者は今後の取組みを進めていく。

第一に、『**地方公共団体の規模によらず、また幅広い行政事務全般にわたっての情報セキュリティ対策の進展**』である。２０１２年には、国、地方を問わず、官、民、ＮＰＯ等が小規模な市町村も含めた地方公共団体の取組みを応援するべく協力体制を構築しつつある。こうした体制の下、地方公共団体では規模に応じた対策が進展し、様々な制約によって対策が遅れている小規模な自治体を含め、おおむね全ての地方公共団体で望ましい対策が実施されている状況にある。また、特に、小規模な地方公共団体の対策促進のためには、効率的な取組み手法が確立されることが望ましいところ、成果が実証されている取組みを効率的に実施する手法が確立しつつある。さらに、複数地方公共団体間での対策の連携など、限られたリソースの下で効率的な取組みを進める手法が積極的に模索されている。

また、２０１２年には、国家行政組織と地方公共団体の担当組織の間での個別の関係も踏まえながら、地方公共団体独自では手が届きにくい分野においても、情報セキュリティに係る取組みが進展している。

第二に、『**情報セキュリティの観点から地域で行われる活動の活発化**』である。２０１２年には、地方公共団体が、情報セキュリティの観点から地域で行われる活動を促進できる環境が構築されている。結果、地域において、情報セキュリティ対策推進の中核を担うことができるような知識を有する人材が育つ土壌ができてきている。

② 重要インフラ

政府は重要インフラの領域については、第２次行動計画を別途策定し、重要インフラ事業者等がとることが望ましい自主的な対策と、内閣官房を中心とした政府及び関係機関等において実施することが望ましい施策からなる体系的な枠組みを整理している。政府は、第２次行動計画に示された官民連携の枠組みによって、重要インフラにおけるＩＴ障害[42]の発生を限りなくゼロにすることを目指し、**重要インフラにおけるＩＴ障害が国民生活や社会経済活動に重大な影響を及ぼさない**よう重要インフラを防護するとともに、重要インフラ事業者等のサービスの維持及びＩＴ障害発生時の迅速な復旧等の確保を図る。

重要インフラ分野の情報セキュリティ対策は、第２次行動計画にまとめられているとおり、重要インフラ事業者等の自主的な取組みを含むものであり、２０１

42 第２次行動計画においては、「ＩＴ障害」を「重要インフラサービスにおいて発生する障害（サービスレベルを維持できない状態等）のうち、ＩＴの機能不全が引き起こすもの」と定義している。

２年における姿を設定して重要インフラ事業者等に義務的な取組みを求めることは適当でない。そのため、実現が期待される将来像を示す事によって、重要インフラ事業者等をはじめとした関係主体の取組みの方向性を示すこととする。

なお、第２次行動計画に基づく情報セキュリティ対策に取り組む関係主体は「ＩＴ障害が国民生活や社会経済活動に重大な影響を及ぼさないようにすること」を目標として取組みを進めることとしており、政府はこの目標の下、以下の将来像の実現に向けて最大限の努力を行う。

第一に、『**政府機関や重要インフラ事業者等の主体的な取組み及び連携の確立**』である。情報セキュリティ対策に取り組む各関係主体は、各々守るべき重要インフラサービスと維持すべきサービスレベルを踏まえて、自らがなすべき必要な対策を理解している。各関係主体は自らの置かれている状況を正しく認識しており、自らの活動目標を主体的に定めている。各関係主体は各々必要な取組みを進めており、これについて定期的に自己検証を行っている。また、他の関係主体の活動状況を把握し、互いに自主的な協力をすることができる。

関係主体はＩＴ障害発生時の対応において、ＩＴ障害の規模に応じて、誰がどのような情報を集積しているか、誰とどのような情報を共有すべきか、また自らは何をなすべきかを理解している。自らの自主的な対応に加えて、必要に応じて他の関係主体と連携を図り統制の取れた対応を取ることができる。

第二に、『**ＩＴ障害に関する情報共有の価値の普遍化**』である。重要インフラ事業者等においては、いわゆる「情報セキュリティガバナンス」という考え方が十分に浸透し、情報セキュリティ対策は単に情報システムの保守運用の観点からだけではなく、企業経営の観点からも検討が必要であることを理解しており、システムの保守と企業経営のそれぞれの責任者が適切に関与する体制を有するようになっている。また、情報セキュリティ対策の対外的な説明に努めている。また、社会基盤の情報セキュリティ対策の強化のためには可能な限り情報共有するという姿勢が積極的に評価される価値観が醸成されている。

この体制において、重要インフラ事業者等は自らの事業におけるＩＴ障害の発生は隠すべきものではなく、事業者等内の対策に取り組む関係者間で共有すべきものであるという認識を有している。対策に取り組む関係者はＩＴ障害の発生状況等の情報を把握できており、必要に応じて当該情報を分野毎のセプターやセプターカウンシル等の第1次行動計画の下で構築された情報共有の枠組みを通じて外部の関係主体と共有し、公式又は非公式の連携を行うようになっている。

第三に、『**環境変化への機敏な対応体制の常備化**』である。政府の諸施策、関係主体間のリスクコミュニケーション、国際連携・協調等を通じて、重要インフラ

の情報セキュリティ対策に資する国内外の多様な情報が内閣官房に寄せられるようになっている。内閣官房はこれを踏まえて関係主体との連携を図り、より効果的な対策を進めるための総合調整機能を発揮している。

特に、特異重大な脅威やＩＴ障害に係るリスクについての認識が得られ、これへの対処が重要インフラ事業者等だけでは困難な場合は、内閣官房、重要インフラ専門委員会、セプターカウンシルの連携によって、解決策の検討とその実現に向けた調整が速やかに実施されるようになっている。

③ 企業

第２次基本計画の下で、政府は**企業における情報セキュリティ対策の実施状況を世界トップクラスの水準にすること**を目指して引き続き最大限の努力を行う。

結果、情報セキュリティに関連して、企業が直面する社会は、２０１２年には以下のようになっていると考えられる。

いわゆる「団塊の世代」の退職などを受けて労働力人口は減少しており、事業活動の更なるＩＴ化によって効率的で労働生産性が高いビジネス運営モデルへの転換が始まっている。このため、経営管理のＩＴへの依存度が更に高まり、情報セキュリティが経営に占める重要性も高まってきている状況にある。また、海外の拠点も十分に活用しながら効率的なビジネス運営を行う必要が更に高まり、且つグローバル化に伴う世界規模での最適生産のために企業活動の細分化、専門化がさらに進展し、海外へのアウトソーシング、直接投資が拡大している。このため、特に関係の深い東アジア地域はもとより、例えばインド、中東地域においても情報セキュリティ対策を徹底し、日系企業にとって安全・安心なビジネス拠点として確保していく必要性が認識され始めている。加えて、我が国経済はグローバルなサプライチェーンマネジメント網の中へ入り、国内企業における情報セキュリティ対策は当然に不可欠のものとなってきている。とりわけ、モノ作りをはじめとして強い国際競争力を有する中小企業における対策推進が喫緊の課題となっている。

２０１２年のこのような社会において、企業の情報セキュリティの取組みが以下のような「姿」となっていることを目指し、関係者は今後の取組みを進めていく。

第一に、**『情報セキュリティガバナンス[43]の経営の一環としての認識の定着と、**

43　本基本計画において、企業に関して目指す情報セキュリティガバナンスとは、　企業経営の一環として、情報セキュリティ対策を適切に実施することを意味する。

それに応えられるツールの存在』である。２０１２年には、企業における情報セキュリティ対策の重要性を経営層も含めて十分に認識するとともに、対策推進のために必要な体制も構築されており、情報セキュリティは財務統制などと並ぶ経営上の重要な要素となっている。情報資産の活用度によって、企業ごとに情報セキュリティガバナンスの重要性が変化することから、情報資産の活用度の高い企業においては、経営層も含めて情報セキュリティ対策の重要性を理解しており、外部監査などを通じて社内のセキュリティ対策について十分に状況を把握している。また、対策にあたっては、コストや利便性とのバランスなども極めて重要であることから、こうした諸要素に配慮がなされた製品やサービスが利用可能となるとともに、対策を促進するための様々な活動が政府や情報関連事業者などの対策支援主体によって積極的になされている。

第二に、『**「事故前提社会」への対応力強化に向けた緊急対応体制・事業継続性確保等の進展**』である。２０１２年には、企業における情報セキュリティ対策自体の事前の対策が進むとともに、規模が大きい企業や、事業活動における情報セキュリティの重要性が大きい企業を中心に、事後対応の準備も進みつつある。

第三に、『**大企業から中小企業にわたった、各企業における適切な対策の進展**』である。２０１２年には、情報セキュリティ対策の進展が十分ではなかった中小企業向けの対策ツールの提供が進むなど、企業の事業規模を問わず、適切かつ必要な対策が行われつつある。

第四に、『**国を問わず、日系企業の進出先における情報セキュリティ対策の進展**』である。２０１２年には、海外のビジネス拠点において、顧客情報の漏えいをはじめ、様々な情報セキュリティ上の問題が生じないことが重要であることについて、政府、日系企業が十分に意識し、対策が始まっている。また、我が国政府と海外ビジネス拠点の政府間でもこうした取組みの重要性を共有し、官民も連携を行いながら、企業が安全・安心にＩＴを活用できる環境整備のための取組みを進めている。

④ 個人

第２次基本計画の下で、政府は**「ＩＴ利用に不安を感じる」とする個人を限りなくゼロにすること**を目指して引き続き最大限の努力を行う[44]。

---

44 当該目標は、ＩＴ基本法第２２条のＩＴ安心利用環境を個人の領域において具体化する趣旨である。個人がＩＴを利用するに際して、リスクに対して鈍感になり、結果、ＩＴ利用に不安を感じなくなることを目指すという趣旨ではない。

結果、情報セキュリティに関連して、個人が直面する社会は、２０１２年には以下のようになっていると考えられる。

教育機関や企業におけるＩＴの利用・活用の急速な広がりもあり、青少年から高齢者までの広範な世代がコンピュータに関する知識を有している。これを受けて、個人の日常生活におけるコンピュータの利用は特別なことではなくなっており、大部分の世帯が、ブロードバンド・インターネットサービスを活用している。そして、これに対応するように、情報家電、ゲーム機をはじめとする様々な機器がネットワークに接続できるようになり、人々の生活に密着した多種多様なサービスが広範に提供されている。また、より一層のインターネットを基盤としたサービスの拡大が進むとともに、２０１１年の地上デジタル放送への完全移行や、ネットワーク機能が強化された新たな移動体通信サービスの広がりにより、様々な双方向サービスが普及し始めている。携帯電話等の人々の生活の中にあるネットワーク利用端末も、より高性能化している。

２０１２年のこのような社会において、個人が以下のような「姿」となっていることを目指し、関係者は今後の取組みを進めていく。

第一に、『**セキュリティ意識の向上を伴う個人のＩＴ利用の拡大**』である。個人は、ネットワークサービスをパソコンや携帯電話、テレビ、ゲーム機等から積極的に利用するようになり、生活がよりＩＴに依存するようになっている。同時に、多くの個人は、パソコンだけではなく、組込み型システムを内蔵する携帯電話や家電製品等に関する情報セキュリティ上のトラブルについても認知するようになり、高信頼性を保証する製品が高い人気を持つようになっている。そして、仮にトラブルが発現しても、ベンダー等から提供される情報に基づいて適切に対応できる個人が多数となっている。

第二に、『**サービス提供側と利用側である個人の互いにバランスのとれたセキュリティ意識の向上**』である。サービス利用時に、個人情報やプライバシー情報を提供しなければならない状況が増加し、サービスを運営する企業・組織においては、こうした個人に係る情報の保護についての関心が高まっている。そして、サービスにおける個人情報利用方針、情報保護レベル等のリスクを明示することも始まっている。他方、個人の側では、リスクに関する情報の非対称性、すなわちサービス利用者とサービス提供者の間でのリスクに関する情報量の格差の存在にもかかわらず、情報を提供する利点とリスクを理解した上で、情報提供の可否を判断できる者が増えてきている。

第三に、『**リスクを理解しても対策を行わない個人等に関する対応の開始**』であ

る。サービス利用におけるリスクを理解した上でも、対策を行わない個人は、一定数存在し続ける。また、情報弱者も一定数存在し続けると考えられる。これに対応するために、サービス提供者、製品提供者は、互いに協力して利用者任せの情報セキュリティ管理を廃し、より責任を持った形でサービスや製品を提供することが取組みの第一歩であると認識し始めている。

⑤ 情報を預ける側の主体

第２次基本計画の下、社会全体で、合理性に裏付けられたアプローチを追求する中で、政府は、**対策情報を預ける側の主体も含めて社会全体が情報セキュリティに係る自身の問題を主体的に考えられるようになること**を目指して最大限の努力を行う。結果、情報を預ける側の主体に関して、我が国は２０１２年には以下のようになっていると考えられる。

第一に、**『情報を預ける側の主体全体としての意識の向上』**である。啓発活動やモデル契約書の提供などを通じて、当該情報を電子情報として預けることの必要性と万が一の場合のリスクの許容性について、個々の主体が無意識にある程度の注意を払うようになっている。

第二に、**『対策知識が十分でなくとも情報を預ける際に安全が確保される技術的発展の実現』**である。技術の発展により、意識的な対策をとらなくても預けた情報が保護されるようになっている。［参照：「（２）①情報セキュリティ技術戦略の推進」の２０１２年の姿］

（２） 横断的な情報セキュリティ基盤

① 情報セキュリティ技術戦略の推進

社会全体のＩＴへの依存度が高まり、情報セキュリティの対象範囲と重要性が大幅に増すなか、政府は、第２次基本計画の下で、**我が国の情報セキュリティ関連技術の研究開発が、世界で最も効果的・効率的に進められる体制となること**を目指して最大限の努力を行う。結果、情報セキュリティに関連して、研究開発・技術開発の面で、社会は２０１２年には以下のようになっていると考えられる。

２０１２年にはＮＧＮ[45]（次世代ネットワーク）やＩＰｖ６[46]の普及が進み、固定通信と移動通信の融合が進むとともに、認証、課金処理、権利管理、顧客管理

45 Next Generation Network の略。

46 Internet Protocol version 6 の略。

などの機能コンポーネントが連携した安全なポータルが実現して、キャリア以外のサードパーティのサービスの提供が増加している。また、地上波も含めた全てのテレビ放送がデジタルに移行し、通信と放送の融合のメリットを活かしたデータ放送や双方向サービスが広く利用されている。その結果、ＳａａＳ[47]やＡＳＰ[48]をはじめとするネットワーク上のサービスは、企業向け・個人向けともにますます多様化し、サービス間の連携による高付加価値化も進んでいる。

このような背景の中、企業では業務の効率化と再構築のために、積極的に電子会議や勤務管理、旅費精算などのネットワーク上のサービスを活用している。生活者も場所や端末の種別などを意識することなく、多種多様なサービスを享受している。オフィスや家庭においては、パソコンや情報家電、ゲーム機などに加えて、照明機器やエアコンといった白物家電も、ホームサーバを経由してネットワークに接続されるようになっている。

こうして、利用者の利便性が向上する反面、不正アクセスなどセキュリティの脅威も増大し、計算機や情報のみならず国民の生活全体を如何に守るかが、大きな関心事となっている。また、ネットワーク経由で提供されるサービスが普及し、相互連携するようになることは、業務情報やプライバシー情報、あるいは認証情報などがどこに保管され、どのように流れているかを把握することや、障害発生時の原因の切り分けが困難になることを意味する。このような環境の中で、信頼性の高い製品やサービスをリーズナブルなコストで提供することの重要さが、ますます増している。

さらに、生活の中にＩＴが溶け込むことで、日常的にＩＴを利用する若年層や高齢層が増加し、個人が情報セキュリティ上のリスクにさらされる可能性が高まっている。そのため、機能や自由度の制約と引き換えに、事前に十分検証された情報セキュリティ対策が施されて、安全・安心に使えるタイプの機器が、一つの商品のジャンルとして確立されている。

２０１２年のこのような社会において、技術戦略の情報セキュリティの取組みが以下のような「姿」となっていることを目指し、関係者は今後の取組みを進めていく。

具体的には、第一には、**『利用者による情報セキュリティ対策が不要な端末や情報家電の提供』**である。これまでも、ウイルス対策ソフトや脆弱性修正プログラムなどの手法によるセキュリティ対策や、利用者に情報セキュリティの重要性を認知させる取組みなどが行われてきた。２０１２年には、啓発活動による利用者

---

47 Software as a Service の略。

48 Application Service Provider の略。

の意識の向上への取組みは引き続き継続しつつ、利用者に負担を与えずにセキュリティを確保するとともに、高齢者らの、認識力の衰えなどによるミスや誤認があっても情報セキュリティ上のリスクを防ぐという観点から、例えば出荷段階から情報セキュリティの設定が適切になされ、アクセシビリティに関する規格標準等に配慮した安全で安心な機器やソフトウェア等が提供されている。

第二に、**『設計段階からセキュリティを作り込む開発手法の普及と定着』**である。２０１２年には、情報セキュリティは、信頼性や性能のようなソフトウェアやシステムの品質と同じく、設計段階から考慮すべき要素であると広く認識されている。効率的に安全なソフトウェアを開発する手法の確立と、その手法を用いた開発を重ねることによるノウハウと人材の蓄積により、情報セキュリティ対策をすべき対象範囲の拡大への対応や、妥当なコストで脆弱性や重大な欠陥の事前の回避が可能となっている。また、そのことが、例えば、携帯電話やＩＣカードなどの組込み系のような、日本企業が先進的な機器やサービスを提供している分野の製品の重要な付加価値要因となり、国際競争力の源泉となっている。

第三に、**『リスクの形式的な表記法や、リスクの評価方式の共通化』**である。この共通化により、ソフトウェアや情報システムのセキュリティに関するリスク情報の迅速な共有が促進されている。また、共通化は、新たな脅威の危険性の客観的な評価や、効率的に安全なソフトウェアを開発する手法の確立や、情報セキュリティ対策の合理性の判断などに大きく寄与している。

② 情報セキュリティ人材の育成・確保

第２次基本計画の下で、社会全体のＩＴ依存度の高まりを受けて**情報セキュリティ人材の重要性が社会で十分に認識され、その業務が魅力的なものとして、優秀な人材が官民を問わず情報セキュリティ分野にすすんで集まること**を目指して、政府をはじめ、各主体が種々の取組みを展開する。結果、情報セキュリティに関連して、人材育成・確保の面で、社会は２０１２年には以下のようになっていると考えられる。

第一に、**『政府機関におけるセキュリティ人材のニーズの高まりと対応の開始』**である。政府機関においては、情報セキュリティ上の脅威の増加を背景に、情報セキュリティを支える人材に対するニーズや、人材の重要性に関する認識がよりいっそう高まっている。そうした意識の高まりを受けて、政府機関において必要となる情報セキュリティに携わる人材を育成・確保するためのロードマップが描かれるとともに、そのロードマップに従った情報セキュリティ人材の育成・確保が積極的に推進されている。

第二に、『**民間企業におけるセキュリティ人材のニーズの高まりと対応の開始**』である。民間企業においても、業務効率化のためＩＴへの依存度が更に高まり、もはや企業経営の重要な一部となっている情報セキュリティ対策において、ＩＴの進歩にも対応することのできる情報セキュリティ専門家へのニーズが高まっている。このニーズに対して、政府は企業が情報セキュリティ人材に係る環境整備・基盤整備をおこなうことで、企業における情報セキュリティ人材の育成・確保を推進している。

第三に、『**情報セキュリティに関する能力向上に係る環境整備の進展**』である。民間を含めた情報セキュリティ部門においては人材を募る際の要件として、資格の保有を要件や考慮要素とする例も一部で見られ始めている。このように、情報セキュリティ業務に携わる人材が能力を高めることに係る環境整備が行われ始めている。さらに、情報セキュリティ業務に携わる人材の側から見ると、資格保有等によるキャリアアップの道筋が見えやすくなることで、能力を高めることに対するインセンティブが生じている。他方、情報セキュリティに携わる人材を雇用する官民の組織においては、かけがえのない人材として、情報セキュリティに携わる人材を育成する意識が芽生えつつある。

③　国際連携・協調の推進

第２次基本計画の下で、グローバルなＩＴ安心利用環境を実現するための取組みが国際的に進められているなか、政府は、**我が国の官民連携を中心とした取組みが世界最先端・最高のベストプラクティスとして世界に貢献すること**を目指して最大限の努力を行う。

このような状況下において、情報セキュリティに関連して我が国が直面する世界の状況は、２０１２年には以下のようになっていると考えられる。ＩＴは世界中で人々の生活にますます浸透し、利用者は国境を気にすることなく様々なコミュニケーションを行っている。結果、ＩＴは、あらゆる主体にとって従来よりも劇的に低いコストで、国境と関係なく革新（イノベーション）をもたらす道具であるとの認識が飛躍的に広まっている。一方で、ＩＴは、悪意ある者が低いコストでグローバルな活動を行うことも可能としている。また、ＩＴを活用した大規模な情報蓄積、業務管理の実現によって、無知や事故がもたらす影響も大規模なものとなり、国境を越えた影響も大きくなっている。

重要インフラの領域においては、規制緩和による事業者間の競争圧力、消費者からの利便性向上の要請を受け、情報システムを利用した事業管理のみならず、

消費者との取引においても、ＩＴの利用・活用は更に拡大している。国境を越えるサービスを提供する重要インフラ事業者は、国境を越えた主体間の依存性、接続性の他、複数国の情報セキュリティ政策を考慮に入れる必要性も高まっている。このような状況に対応するため、我が国は、早期から対応を行ってきた他国政府と協力し、事業継続性確保のための最新のベストプラクティスを、国内環境に合致する形で還元するべく努力を行っている。また、第２次行動計画を中心とした我が国の官民連携体制について、その優れた点を世界に発信していく取組みを行うなど、国内外の取組みの有機的な連携を進めている。

企業の領域においては、グローバル化に伴う企業活動の細分化、専門化が更に進展し、海外へのアウトソーシング、直接投資が拡大している。製品・サービスは、少なからぬ部分がＩＴを活用したグローバルなサプライチェーンを経て製造、提供されている。経済活動は国家の領域を超えて行われており、世界における情報セキュリティ対策の推進という観点から、グローバル企業の果たす役割は拡大している。

なお、近年のコーポレートガバナンスの要請や会計監査に関する統制の強化に見られるように、企業の経済活動に一定の規制・統制が要求される場合、情報セキュリティの領域においても相応の規制・統制が求められる可能性は否定できない。しかし、政府は、企業の事業活動のグローバル化を支援・促進することを重要な課題として捉え、情報セキュリティに関する国境を越えた政府間の連携、官民の連携を通じて、情報セキュリティに関する規制・統制が過度なものとならないよう適切に調整を行うことにより、企業が安全・安心にＩＴを活用できる環境整備を実施する努力を継続している。

個人の領域においては、世界各国で、ＩＴを利用・活用する人口が若年層を中心に増加している。世界の個人ユーザーは、ＩＴを活用して無限大の知識にアクセスすることが可能となり、個人が国家の領域を超えて、自由に社会的、文化的、政治的活動を行うことが容易になっている。一方で、ＩＴの利用・活用が急拡大する国においては、ＩＴの抱えるリスクについて無防備なユーザーが急増することとなり、これに対応するためにＩＴの利用・活用に対する規制の声が急速に高まることも考えられる。このような状況下で、我が国は、自由と統制のバランス、官民のバランスの取れた情報セキュリティ政策をグローバルに展開する努力を継続している。

このように、ＩＴの普及は、世界的に個々の主体の自由な発想・活動を更に促進し、新たな創造や革新を可能としていく。一方で、ＩＴは、その利便性を維持するために、政府が最低限果たすべき役割の重要性を高めていく性質を有する。

２０１２年には世界がこのような状況となることを認識しながら、情報セキュリティの国際連携・協調面の取組みが、以下のような「姿」となっていることを目指し、関係者は今後の取組みを進めていく。

第一に、『**グローバル化へ対応し、世界と連動した政策の実施**』である。政府は、情報セキュリティに係る国内の政策が、企業をはじめとする個々の主体のグローバルな活動にも影響を与えることを理解している。そして、各国政府、国際機関の動向を十分に注視し、必要な要素を我が国の政策に反映する取組みを行っている。同時に、我が国のベストプラクティスと言える政策が、関係の深い国・地域、ひいてはグローバルに採用され、我が国の主体が国内で進める情報セキュリティの取組みを以て、グローバルに必要とされる取組みを進めていると言える環境作りをしている。このように、我が国では、国内外の取組みが有機的に連動している。

第二に、『**アジアにおける情報セキュリティ分野の取組みへのイニシアティブの発揮**』である。第１次基本計画同様、内閣官房情報セキュリティセンター（ＮＩＳＣ）はＰＯＣとしての機能を強化し、情報セキュリティ政策・オペレーションに関する国際的な情報連携の要としての活動を行っている。特に、欧米の機関との関係において、情報セキュリティに関するアジアの玄関としての地位を確立するとともに、アジアにおける情報セキュリティ先進国として位置付けられている。

第三に、『**情報セキュリティ文化の醸成へ向けたグローバルレベルでの貢献**』である。情報セキュリティの推進には、情報セキュリティの政策担当者や情報セキュリティが事業の信頼に直結する企業のみならず、より広い政策分野の担当者やＩＴ利用者全体の意識向上が不可欠である。このため、我が国政府は、国際機関や他国政府と協力しながら、グローバルレベルでの情報セキュリティ意識の向上のための取組みを行っている。

④　犯罪の取締り及び権利利益の保護・救済

第２次基本計画の下で、政府は、犯罪の取締り及び権利利益の保護・救済が進むことにより**サイバー空間が安全にかつ安心して利用できるものとすること**を目指して引き続き最大限の努力を行う。

このような努力を進めるなか、我が国が直面する社会の状況は、２０１２年には以下のようになっていると考えられる。

ＩＴは、国民生活の利便性を向上させ、社会経済基盤として機能している。こ

のため、サイバー犯罪や権利利益の侵害がひとたび発生すると、国民に直接かつ深刻な影響が及びかねない状況となっている。このような状況の中、サイバー犯罪もその手口を一層高度化・多様化させており、サイバー空間の安全性・信頼性を維持するためには、犯罪の取締りを的確に推進していくことが不可欠な状況となっている。

このため、サイバー犯罪の取締りが強力に進められている。

また、国民の間では、サイバー犯罪の未然防止や被害拡大防止、情報流出対策等の重要性に対する意識が従来以上に高まっており、個人、社会の両面から積極的に犯罪抑止や情報セキュリティへの取組みが行われている。

さらに、各種情報セキュリティ技術の開発・普及が進み、サイバー空間の安全性・信頼性を向上させるための選択肢も増加している。

２０１２年のこのような社会において、サイバー犯罪の取締りや権利利益の保護・救済に関する取組みが以下のような「姿」となっていることを目指し、関係者は今後の取組みを進めていく。

第一に、『**犯罪の取締りの一層の強化**』である。サイバー空間の安全・安心が確保されるためには、サイバー犯罪を迅速かつ的確に検挙するとともに、犯罪抑止のための対策を進めていくことが大前提となる。このため、政府は、犯罪の取締りのための施策を強力に推進している。あわせて、増大するサイバーテロの脅威に備えるための基盤整備についても推進している。

第二に、『**対策に向けた意識の高揚と知識の充実**』である。犯罪や権利利益の侵害に強いＩＴ社会を構築するためには、国民一人ひとりが被害に遭わないための知識を身に付け、それを実践することが大切である。このため、政府は、効果的な広報啓発の推進に努めている。

第三に、『**権利利益の保護・救済のための基盤の整備**』である。国民が安全にかつ安心してサイバー空間を利用するためには、サイバー空間上で権利利益が保護されていることが不可欠である。政府は、基本的人権に十分配慮しつつ、サイバー空間の権利利益の保護･救済のための基盤の整備に向けて引き続き努めている。

第３章 今後３年間に取り組む重点政策[49]

第１節　　対策実施４領域における取組みの推進と政策目的の着実な実現

（１） 対策実施４領域

① 政府機関・地方公共団体

[政府機関]

政府機関においては、第１次基本計画期間中に決定した政府機関統一基準とそれに基づく評価・勧告という枠組みを維持しつつ、以下の対策に重点的に取り組んでいくこととする。

（ア） 全ての政府機関において能動的に情報セキュリティ対策に取り組む体制の確立

１）ＰＤＣＡサイクルの各プロセスにおけるマネジメントの強化

各政府機関においては、情報セキュリティガバナンスの確立を図るため、最高情報セキュリティ責任者の下で、当該機関の情報セキュリティ対策について責任を持って統括することが可能な体制を、情報システム統括部門（ＰＭＯ）又はそれと同等の権能を有する部門に整備する。また、最高情報セキュリティ責任者を補佐する専門的知見を有する最高情報セキュリティアドバイザーを設置するとともにそのスタッフとなる人材を必要に応じて確保し、上記の体制の下でこれらの専門家の指示やアドバイスが組織全体に迅速かつ確実に反映できる仕組みを構築する。

各政府機関においては、行政に対する国民の信頼の確保に向けて情報セキュリティ対策に係る説明責任を明らかにする観点から、それぞれの情報システムの現状を把握した上で、情報セキュリティに対する考え方、情報セキュリティ対策に係る目標や計画及びその実績と評価など、それぞれの政府機関においてＰＤＣＡサイクルが有効に機能しているかどうかを数値指標などの客観的指標を積極的に活用して記述した「情報セキュリティに係る年次報告書」（情報セキュリティ報告書）を作成する。その際、情報セキュリティ報告書の客観性を確保する観点から、

49　情報提供主体を対象とする取組みについては、便宜的に、第１次基本計画以来の既存の政策構造（対策実施４領域、横断４分野）の中で、関係の深い部分に盛り込む形とする。

最高情報セキュリティアドバイザーがその作成に参画するほか、外部監査制度の活用についても、導入可能な政府機関においては積極的に推進することとする。また、作成した情報セキュリティ報告書は、最高情報セキュリティ責任者が、情報セキュリティ政策会議の下に設置されている「情報セキュリティ対策推進会議」等の場において報告し、公表する。

各政府機関における情報セキュリティ対策のバランスを確保するとともに、一層の充実・向上を推進する観点から、政府機関の情報セキュリティ報告書作成のためのガイドラインを策定するとともに、各政府機関が作成した情報セキュリティ報告書の定量的評価等を行い、その結果を情報セキュリティ政策会議に報告する。また、各政府機関の最高情報セキュリティアドバイザーが集まる会議体を設置し、情報セキュリティ報告書の比較・評価等を行うとともに、それらを通じて得られた知見の共有やフィードバックを積極的に図ることとする。

技術や環境の変化を踏まえ、政府機関における情報セキュリティ対策を常に最新かつ適切なものとするため、政府機関統一基準については、引き続き毎年その見直しを行う。

政府機関において特別に秘匿すべき情報（特別管理秘密）を取り扱うシステムに係る情報セキュリティ対策については、政府機関統一基準に基づくＰＤＣＡサイクルを基本としつつ、「カウンターインテリジェンス機能の強化に関する基本方針」[50]に基づく特別管理秘密に係る基準を踏まえた対策を、各政府機関自らの責任において着実に講じていくこととし、その実施状況を重層的にチェックする仕組みをカウンターインテリジェンスセンターを中心とする内閣官房及び関係政府機関が協力して構築する。

２）政府機関における人材の育成・確保及び職員の意識啓発

政府機関における情報セキュリティ関連業務を調査・検証し、これらの業務に携わる人材に必要とされるスキルをまとめる。

各政府機関においては、まとめられたスキルを踏まえ、情報セキュリティ対策に関わる内部人材の教育や確保・登用等に係る具体的な計画を、「行政機関におけるＩＴ人材の育成・確保指針」[51]に基づき作成した「ＩＴ人材育成・確保実行計画」に明記し、それを推進する。

50　２００７年8月9日　カウンターインテリジェンス推進会議決定。

51　２００７年4月１３日　各府省情報化統括責任者（ＣＩＯ）連絡会議決定。

また、各政府機関においては、セキュリティ対策に係る民間専門家の活用を促進するため、最高情報セキュリティアドバイザーやそのサポートスタッフの活用などの戦略的なアウトソーシングを進めるほか、任期付き採用制度などの積極的な活用を図る。

各政府機関においては、官民人事交流制度の活用による人材育成の促進のほか、階層別研修に情報セキュリティに関する内容を盛り込むなど、幹部職員も含めた全職員の情報セキュリティに関する意識の向上方策を、人事担当部門と情報システム部門の密接な協力の下に推進する。

3）情報セキュリティ対策を適時に行うための予算面での取組み

情報セキュリティ対策は適時の対処が必要であるため、各政府機関においては、あらかじめ可能な限りの想定を行うとともに、保守契約等においても適時適切な対応が可能となるような契約を交わすなどの取組みが必要となるが、その際には「成果重視事業[52]」制度の活用も検討するなどの工夫を行うほか、会計部門と情報システム部門が密接に協力し、予算の効率的活用に配慮して対策を進める。

4）運用・管理を委託している情報システムの情報セキュリティ対策の強化

各政府機関においては、政府機関外の組織に運用・管理を委託している情報システムについて、政府機関統一基準等を踏まえた適切な契約により、委託元の政府機関の情報セキュリティポリシーの遵守を確保するとともに、適切な運用が行われているかを確認するための取組みを進める。

5）技術面の知見を蓄積・活用する仕組みの構築

情報セキュリティ対策の推進に当たって、我が国における情報セキュリティに係る技術的・専門的な知識や経験の利用を図るため、関連する独立行政法人や情報セキュリティ関係団体などの研究者・実務家の知見を集合的に活用するための仕組みの構築を推進する。

6）情報セキュリティに関連する法令との整合性確保

現在検討が進められている文書管理法制等も含め、情報セキュリティと関連が

52　限られた財政資金を効率的に活用する観点から、位置付けを明確にして定量的な目標をたて、事後評価を行う事業。予算執行では事業の性格に応じた弾力化を行うなど確実な事業の成果を目指すことになる。

深いと考えられる法制度等と政府機関統一基準との整合性の確保が図られるよう、必要な調整を進める。

（イ） 政府全体を通じて情報システムに情報セキュリティ対策が適切に組み込まれる仕組みの構築

政府機関における各種情報システムの構築を行うに際して、トータルコストの抑制や利便性・柔軟性の実現、情報セキュリティの確保といった様々な方向性をもった要件を止揚する観点から、情報システムの構築や運用段階のみならず、企画・設計段階からの情報セキュリティ対策の組込みについても意識するための方策（Security by Design）を、業務・システムの最適化の取組みと一体的に推進する仕組みの構築を図る。その際、政府全体として情報セキュリティ対策を含めた情報システムのＴＣＯ（Total Cost of Ownership：システムの導入、維持・管理などにかかる費用の総額）の低減を推進するための手法について検討を行う。

また、情報システムや物品の調達に際して、必要となる情報セキュリティ対策を設定するために参考となる各種情報を提示し、その活用を図る。

（ウ） 電子政府の利便性・セキュリティレベルの向上

行政サービスの利便性向上と行政運営の効率化・高度化を推進するとともにセキュリティレベルの向上を図る観点から、電子政府に係るシステムのセキュリティ機能の在り方について検討することとし、特に利用者とのインターフェースに係るものについては、利用者の利便性を向上し、かつ安全を確保できるものとなるよう、費用対効果を勘案した上で、実装方法を含めて検討を行う。

（エ） 政府機関における事業継続性確保・緊急対応能力の強化に係る検討

現在、中央防災会議の策定した「首都直下地震対策大綱」（２００５年９月）に基づき、各政府機関において首都直下型地震を対象とした業務継続計画の策定は行われているが、その他の災害や障害発生時においても行政の継続性を確保する観点から、各政府機関は保有する情報システムの災害・障害時対応の必要性・優先度について決定するとともに、必要なものについては業務継続計画を策定する。また、政府機関の保有する重要なシステムや情報のバックアップ体制について政府横断的な方向性を検討する。

緊急時における対応力（レスポンス・リカバリー）の強化を図る観点から、

２００８年度に本格運用を開始したＧＳＯＣ[53]を核として、各政府機関や国内外の関係機関との連携をより一層深め、緊急時における連絡体制や攻撃等の分析・解析及び対策立案機能を強化することにより、政府全体としてサイバー攻撃等に対する緊急対応能力を向上させるとともに、我が国の安全保障体制の強化を図る。

（オ） 独立行政法人等の情報セキュリティ対策の推進

独立行政法人等の情報セキュリティ対策を推進するため、独立行政法人等を所管する政府機関は、中期目標の中に情報セキュリティ対策に係る事項を明記し、独立行政法人等が組織として情報セキュリティ対策に取り組む体制を構築させる。各独立行政法人等は、その業務特性及び対策の実施状況に応じて、政府機関統一基準を含む政府機関における一連の対策を踏まえ、自らの情報セキュリティ対策に係るＰＤＣＡサイクルを構築する。また、独立行政法人等及び独立行政法人等を所管する政府機関は、緊急時を含め実効性のある連絡体制を整備する。

（カ） その他個別の情報セキュリティ対策の推進

１）政府機関の情報システムのＩＰｖ６対応化

ＩＰｖ４アドレス枯渇への先導的な対応を実施する観点から、政府機関においては、各情報システムの新たな開発（導入）又は更改に合わせてＩＰｖ６対応を計画的に進め、特に電子政府システムをはじめとする外部と直接通信を行う情報システムについては、原則として、２０１０年までにＩＰｖ６対応化を図ることとしているが、その際、ＩＰｖ４からＩＰｖ６への移行期におけるセキュリティ上の課題に適切に対応する。

２）政府機関への成りすましの防止

悪意の第三者が政府機関又は政府機関の職員に成りすまし、一般国民や民間企業等に害を及ぼすことが無いよう、正統な政府機関又は政府機関の職員であることを容易に確認可能とするため、電子メールやウェブサーバでドメイン名として政府機関のドメインであることが保証されるドメイン名を使用することや、政府機関から発信する電子メールへの電子署名の付与等電子証明書の活用に係る取組みを推進する。

---

53 Government Security Operation Coordination team の略。

３）政府機関における安全な暗号利用の推進

電子政府の安全性及び信頼性を確保するため、政府機関で使われている推奨暗号について、その安全性を継続的に監視・調査するとともに、技術動向及び国際的な取組みを踏まえ、現行の「電子政府推奨暗号リスト」の２０１３年度改訂に向けて、関係機関において所要の作業を進める。また、「政府機関の情報システムにおいて使用されている暗号アルゴリズムＳＨＡ－１及びＲＳＡ１０２４に係る移行指針」[54]の策定時の経験を適切に継承し、安全性が低下した暗号について速やかに安全な暗号への移行を進める。

［地方公共団体］

（ア） 小規模な地方公共団体も含めた合理的・自主的な情報セキュリティ対策の促進

小規模な地方公共団体も含め、全ての地方公共団体において、望ましい情報セキュリティ対策が実施されることを目指し、対策の促進を行う。具体的には、対策や監査の基となる情報資産のリスク分析の実施を促進するとともに、情報セキュリティポリシーの策定等の検討や監査の実施に向けたガイドラインの見直し、業務継続計画の策定に資するガイドライン[55]の普及などを行う。また、人材面では、取組みを担う職員等の能力向上に向けた共同勉強会や地域セミナーの開催などを進める。

（イ） 複数地方公共団体間での情報セキュリティ対策の連携に向けた取組みの応援

地方公共団体において情報セキュリティ対策に投資できるリソースの限度を考慮し、複数地方公共団体間で効率的に対策を実施するための連携に向けた取組みを応援する。このため、全国の地方公共団体に対するベスト・プラクティスの紹介やモデルケースができるような応援を行う。また、地方公共団体の長の理解促進のための勉強会や検討会を実施し、組織トップの意識を高めるとともに、例えば、相互監査等の取組みにおけるアドバイザー派遣などを検討する。

54　２００８年4月２２日　情報セキュリティ政策会議決定。

55　総務省「地方公共団体におけるＩＣＴ部門の業務継続計画（ＢＣＰ）策定に関するガイドライン」（平成２０年８月）

（ウ） 地方公共団体の取組みを応援する主体の強化

地方公共団体の対策を進めるには、取組みを応援する主体を強化することが有効である。このため、官・民・ＮＰＯによる共同勉強会を開催するなど情報セキュリティに役立つ知見を有するあらゆる主体の協力体制を構築するとともに、ＬＧＷＡＮ（総合行政ネットワーク）内のポータルサイトを活用した自治体向け支援体制の強化などを進める。

（エ） 地方公共団体が担う幅広い行政分野での対応促進

国家行政組織と地方公共団体の担当組織の間の個別の関係を踏まえた形で、地方公共団体が担う幅広い行政分野における情報セキュリティ対策を促進する。例えば、学校におけるＩＴ基盤の整備に際して、情報セキュリティの視点も十分に加味することや、関係省庁から、都道府県教育委員会に対し、情報セキュリティ対策上有効な方策を伝達することや、ベストプラクティスを紹介し、都道府県教育委員会の意識向上を促進するといったことが考えられる。

（オ） 地方公共団体間、地方公共団体と政府機関間でのベスト・プラクティスの相互活用の促進

約１８００の地方公共団体の情報セキュリティ対策を促進するには、地方公共団体間でベスト・プラクティスを相互活用することが効率的である。このため、ＬＧＷＡＮ(総合行政ネットワーク)内に設置しているポータルサイトを利用し、地方公共団体間での情報共有を促進する。また、ベスト・プラクティスを地方公共団体の長や現場担当者などの様々な階層において共有できるよう検討会や意見交換会等を開催する。

加えて、地方公共団体同様、公的組織である政府機関との間でのベスト・プラクティスの相互活用も有効と考えられることから、これに向けた方策の検討を実施する。

（カ） 地域の情報セキュリティ対策の担い手の育成支援

地域において情報セキュリティ対策を担えるような人材の育成に際しては、地方公共団体による促進活動が有効であることから、地方公共団体のこのような活動が行いやすくなるような環境整備に取り組む。具体的には、地方公共団体が情報セキュリティをテーマとした住民向け教養講座等を開催しやすいよう、講座で活用できるような参考資料等を作成、紹介する。また、Teaching teachers（教えることのできる人材の教育・育成）の発想に基づき、地方において人材育成が促

進されるような取組みを行う。

② 重要インフラ

重要インフラの情報セキュリティ対策に関する関係主体は、第２次行動計画に基づいて、各々重要インフラサービスの維持に努め、またＩＴ障害発生時の迅速な復旧等を確保することに努めることとする。また、情報セキュリティ対策の実施状況について指標を用いた検証を毎年実施するとともに、行動計画の評価を実施し、各々の取組みの継続的改善を図ることとする。これらについての具体的な取組みは第２次行動計画に詳述しているが、以下にその概要を示す。

（ア） 「安全基準等」の整備及び浸透

第１次行動計画で策定された指針について、事業継続の観点からの具体的内容の補充を含め、指針の位置づけや記載内容の具体性のレベルの見直しを行う。また、重要インフラ事業者等のＰＤＣＡサイクルとの整合性を踏まえた安全基準等の整備の推進などの底上げに資する取組みのみならず、３年毎に個別の先進的な対策を伸ばしその浸透を図る観点からの取組みも推進する。

（イ） 情報共有体制の強化

第１次行動計画で構築されたセプター、セプターカウンシルを含む関係主体間で共有する情報についての整理を行い、情報提供、情報連絡等に必要な環境整備等を推進するとともに、各セプター、セプターカウンシルの自主的な活動の充実強化を推進する。

（ウ） 共通脅威分析

第１次行動計画で実施してきた、ある重要インフラ分野にＩＴ障害が発生した場合に他のどの重要インフラ分野に影響が波及するか、という相互依存性解析を継続するとともに、重要インフラ分野共通に起こりうる脅威が何であるかを把握するための検討を行う。

（エ） 分野横断的演習

第１次行動計画において得られた分野横断的な演習手法に関する知見を踏まえ、各重要インフラ所管省庁、各重要インフラ事業者等、各重要インフラ分野のセプター等の協力を得て、ＩＴ障害の発生を想定した、重要インフラ分野横断的な演

習を実施する。

（オ） 環境変化への対応

社会環境や技術環境等の状況の変化に合わせて情報セキュリティ対策を機敏に対応させていくために、第２次行動計画策定時に想定しなかった環境の変化を察知する能力の向上に努める。また、こうした環境の変化に対して第２次行動計画の枠組みだけでは十分に対応できない場合は、内閣官房は必要な対応が可能となるような体制の検討を行う。

③ 企業

（ア） 情報セキュリティガバナンスの「経営の一環としての位置付け」の確立

情報セキュリティガバナンスを経営の一環として位置付けるため、そのための取組みを推進し、経営層に対する啓発活動の推進、合理的な情報セキュリティガバナンス確立プロセスモデルの開発などの取組みを行う。また、経営者における意識向上を図るための体制の強化を目指すとともに、情報セキュリティマネジメントシステム（ＩＳＭＳ）適合性評価や情報セキュリティ監査、ＩＴセキュリティ評価及び認証制度、暗号モジュール試験及び認証制度などの制度、情報セキュリティ報告書モデル、情報セキュリティ対策ベンチマークなどのツールの普及・開発・改善等を更に進め、具体的な取組みが浸透することを目指す。さらに、情報システム等の政府調達の競争参加者に対して、必要に応じて、これらの制度や第三者評価の結果等を活用した情報セキュリティ対策レベルの評価を入札条件等の一つとする。加えて、情報セキュリティガバナンスのための取組みが企業にとって過度の負担とならないよう、投資効率を測る手法を実際に活用可能にするための検討を促進する。また、情報セキュリティガバナンスが「経営の一環としての位置付け」を確保するには、関連法制との関係で整理が必要となる論点もある。このため、関連法制度の分析整理を行い、ガイダンスとして整備するような取組みも推進する。

（イ） 企業の情報セキュリティ向上に資する製品やサービスの提供促進と活動の推進

企業における情報セキュリティ対策が進展するよう、企業が理解しやすい形で必要な情報セキュリティ対策を選択できる環境を整備する。第１次基本計画に続き、企業の情報セキュリティ関連リスクに対する定量的評価手法の実用化を目指した研究を促進するとともに、ＩＴセキュリティ評価及び認証制度の活用を促進

する。
また、情報セキュリティ向上に資する製品やサービスの提供促進と活動の推進のためには、対策支援主体側の取組みの強化も必要である。対策を容易化するＳａａＳやＡＳＰなどの活用促進や、迷惑メール対策の強化、暗号技術や認証技術、ＮＧＮ／ＩＰｖ６移行環境のセキュリティ評価システム等の技術開発の促進等の取組みを進める。なお、取組みにあたっては、ＴＣＯにも目配りした製品やサービスの提供が促進されるような視点も重要である。

（ウ） 企業における情報セキュリティ人材の育成・確保

経営層の情報セキュリティ対策への理解増進とともに、企業の情報セキュリティ対策の推進を担う人材の育成・確保が必要不可欠であることから、人材育成に向けたセミナー開催等の広報啓発を推進する。また、対策においては、新たなＩＴの利用・活用など、環境の進化に柔軟に対応できる人材や企業のマネジメント全体を俯瞰した上で判断できるスキルを持った人材などの育成・確保も必要不可欠である。その際には、情報セキュリティ人材の目指すキャリアパスを考慮に入れることも重要である。こうしたことを踏まえ、官民の適切な役割分担のもと、客観的な人材評価メカニズムである各スキル標準の整合化を図った共通キャリア・スキルフレームワークとそれに準拠した情報処理技術者試験の活用、及び民間の人材育成に関するフレームワークや各種資格試験の活用を促進する。また、産学連携による高度情報セキュリティ人材を育成するためのカリキュラム整備や教員強化、インターンシップの充実等に取り組むための体制を整備する。
また、技術者向けの情報セキュリティに係るモデルキャリア開発計画の策定や専門家コミュニティへの支援を進めることで、広く企業の情報セキュリティを担うことのできる人材の育成・確保に取り組む。
さらに、今後の課題となるＮＧＮ／ＩＰｖ６への移行などの新しい環境への移行に対応できる実践的な情報セキュリティ人材や法令遵守、情報資産や事業継続等に関するリスクを特定しつつ、情報セキュリティ対策を実践できる人材の育成を推進する。

（エ） 「事故前提社会」への対応力強化に向けた事業継続性確保・緊急対応体制等の強化

コンピュータウイルスや脆弱性などの情報セキュリティ上の問題に対する的確かつ実効的な対応を行うため、平時からの情報共有のための連絡体制の構築、主体間の連携強化が図られるための取組みを進める。また、事業継続性確保を強化するために企業における事業継続計画策定の促進を図るとともに、そのための事業継続計画策定ガイドラインの普及、改善の取組みを推進する。さらに、情報セ

キュリティ上の問題が発生した場合に迅速かつ実効的に対応を行うために必要な緊急時対応体制の強化を推進する。

（オ） 中小企業の情報セキュリティ対策の推進

人員、予算、ＩＴインフラなど、主にリソース不足から対策が遅れがちである中小企業の情報セキュリティ対策が促進されるよう、様々な対策の中から適切な対策を容易に選択できるような環境を整備する。例えば、適切な情報セキュリティレベルを測るために活用される情報セキュリティベンチマークを引き続き改善し、自社の情報セキュリティレベルを客観的評価として提示するための統一的なチェックリストの開発、普及を図る。

また、中小企業のセキュリティ対策を促進するためには、簡便かつ安価なセキュリティ対策ツールを提供するなどの効果的な取組みが必要であるため、ＳａａＳやＡＳＰなどの活用の促進及びこれらサービス提供事業者における情報セキュリティ対策基準の提示・啓発などの取組みを行う。

さらに、中小企業の経営者、情報システム担当者等の情報セキュリティへの理解を深めるため、セミナーの開催など普及・啓発活動を推進し、情報セキュリティ対策の促進を図る。

（カ） 日系企業のグローバルな事業展開を支える情報セキュリティ政策の推進

我が国企業がグローバルな事業展開を行うにあたり、日本国外のビジネス拠点において情報セキュリティを確保するための取組みを推進する。例えば、アジアなど我が国企業の事業活動に関係の深い国や地域を念頭に、円滑なアウトソーシングを行える環境づくりや、セキュアなネットワーク環境の構築へ向けた国際連携・協力を推進する。

④ 個人

（ア） 情報セキュリティ教育の強化・推進

ＩＴの利用・活用には積極的であるものの、リスクの認識や情報セキュリティ対策の重要性の認識が必ずしも十分ではない児童・生徒や保護者への教育・啓発を推進する。こうした観点も踏まえつつ、学校や地域における情報モラル[56]等の教育を推進する。

---

56 情報モラルとは、「情報社会で適正な活動を行うための基になる考え方と態度」（高等学校学習指導要領解説　情報編）のこと。

また、消費者である個人が様々なサービス等の利用において生じ得るリスクを認識し、そのリスクを被害に変えないための環境を整備する。個人に対する啓発活動とともに、サービス提供事業者や対策支援主体によるリスク情報、対策情報の適切な提供、事故発生時の対応等の取組みを促進する。

（イ） 個人の底上げに向けたより効果的な普及・啓発活動の実現

個人の底上げに向け、周知・啓発活動を、関係府省庁が更に連携し、より効果的に実施できるような取組みを進めていく。また、ＩＴに関して必ずしも詳しくない個人を含めた一般利用者のセキュリティレベルを効果的に上げるために、質問への適切なアドバイスや訪問対応を行えるサポータの育成、地域団体ネットワークの実現を促進する。

（ウ） 対策が困難な個人も含めた情報セキュリティ水準向上に向けた取組み

対策の必要性を認識していても対策を実施しない個人など、対策が困難な個人を含めた情報セキュリティ水準の向上のためには、対策支援主体による取組みが必要不可欠である。このため、迷惑メール対策の強化や電気通信事業者が予防的措置として実施する情報セキュリティ対策の利用促進などの取組みを促進する。

（２） 横断的な情報セキュリティ基盤の強化と発展

① 情報セキュリティ技術戦略の推進

２０１２年における姿を実現するために、民間や大学における自主的な研究開発を促すとともに、産学官は適切な役割分担を行いつつ連携していくことが必要である。その中で、政府は、リスクの高い分野、公共性の高い分野、基礎的な分野、あるいは多様な分野に共通的な研究開発支援の環境整備など、非常に重要だが民間や大学等では実施困難なものに対して、重点的に取り組む。

（ア） 情報セキュリティ技術開発の重点化と多様性の維持

基盤としてのＩＴの強化、および国民が安心してＩＴを利用できるような環境の実現を目標とした、研究開発・技術開発を重点的に促進する。経済環境が厳しさを増す中で、ＩＴを利用して生産性向上を図ることと、その分野における将来にわたる主導的かつ優位な地位を確保するという視点を持って、研究開発・技術開発を推進することが、従来以上に求められる。具体的には、利用者に対策への過度の負担を強いない、事前に情報セキュリティ対策が埋め込まれた、安全・安

心な機器の実現や利用者環境の提供を、重点的に取り組むべき課題として取組みを推進する。

一方で、研究開発・技術開発の多様性を確保するため、市場として成立していないために企業が取り組まない分野や将来的なリスクに対抗するための先行的な開発、開発コストが巨大な分野、および基礎研究など、我が国として戦略的に維持すべき分野に対しては、政府が積極的に取り組むこととする。

（イ） 「グランドチャレンジ[57]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、喫緊の対応が必要でありながら対策が十分でない課題や、中長期的な視野で抜本的な技術革新等の実現が求められる課題が存在する。これらの対策が困難な課題に対応するため、「グランドチャレンジ型」の研究開発・技術開発を推進する。

喫緊の課題の解決に向けては、要素技術の統合化・実装化で迅速な対応を図る。また、既に開発済みであっても、制度や教育が追いついてないなどの理由から技術成果が利用されていない場合があり、組織・人間系の管理手法の高度化や利用者の啓発と並行して、統合的な対策を推進することが有効となる。

中長期的な研究開発の推進のためには、将来の社会像を予測し、そこで必要となる情報セキュリティ技術を検討することで、研究開発・技術開発テーマの開拓を行なう。具体的には、設計段階から製品にセキュリティを作り込むための手法の確立や、開発ノウハウの蓄積は短期的に実現できるものではなく、また多くの知見を集約する必要があるため、中長期的なビジョンと実施体制、および支援環境をもって当たることが望ましい。

（ウ） 研究開発・技術開発の効率的な実施体制の構築と基盤の整備

国が支援するプロジェクトにおいては、その投資効果を最大化するために、研究開発・技術開発の計画策定時にプロジェクトの途中で得られた成果を活用する手順（プロセス）を組み込むとともに、プロジェクトの内容および実施状況の公開を促進する。また、情報セキュリティを取りまく環境の移り変わりが激しい中で、社会情勢変化や技術革新の影響を評価し、必要性が高い場合には計画変更が可能な、柔軟なプロジェクト管理の仕組みを導入し、新たな脅威への迅速な対応を可能とする。

さらに、直接的な研究開発・技術開発の取組みに加え、情報セキュリティ分野の特殊性に鑑み、研究開発支援の環境整備を官民の連携によって積極的に推進する。具体的には、リスクの表記法や評価方式の共通化、情報セキュリティに関す

57 持続的な研究開発を念頭に置き、特定の大目標を設定し、各種要素技術全体の統合開発を行うもの。

るデータベースの整備と共有、及び隔離ワークベンチ[58]の構築などによって、研究開発の支援と加速を図る。

② 情報セキュリティ人材の育成・確保

（ア） 政府機関における人材の育成・確保及び職員の意識啓発（再掲）

政府機関における情報セキュリティ関連業務を調査・検証し、これらの業務に携わる人材に必要とされるスキルをまとめる。

各政府機関においては、まとめられたスキルを踏まえ、情報セキュリティ対策に関わる内部人材の教育や確保・登用等に係る具体的な計画を、「行政機関におけるＩＴ人材の育成・確保指針」に基づき作成した「ＩＴ人材育成・確保実行計画」に明記し、それを推進する。

また、各政府機関においては、セキュリティ対策に係る民間専門家の活用を促進するため、最高情報セキュリティアドバイザーやそのサポートスタッフの活用などの戦略的なアウトソーシングを進めるほか、任期付き採用制度などの積極的な活用を図る。

各政府機関においては、官民人事交流制度の活用による人材育成の促進のほか、階層別研修に情報セキュリティに関する内容を盛り込むなど、幹部職員も含めた全職員の情報セキュリティに関する意識の向上方策を、人事担当部門と情報システム部門の密接な協力の下に推進する。

（イ） 企業における情報セキュリティ人材の育成・確保（再掲）

経営層の情報セキュリティ対策への理解増進とともに、企業の情報セキュリティ対策の推進を担う人材の育成・確保が必要不可欠であることから、人材育成に向けたセミナー開催等の広報啓発を推進する。また、対策においては、新たなＩＴの利用・活用など、環境の進化に柔軟に対応できる人材や企業のマネジメント全体を俯瞰した上で判断できるスキルを持った人材などの育成・確保も必要不可欠である。その際には、情報セキュリティ人材の目指すキャリアパスを考慮に入れることも重要である。こうしたことを踏まえ、官民の適切な役割分担のもと、客観的な人材評価メカニズムである各スキル標準の整合化を図った共通キャリア・スキルフレームワークとそれに準拠した情報処理技術者試験の活用、及び民

58 マルウェアなどを実際に動作させて研究を行うための、ネット環境を模した実験設備。現実のインターネットからは隔離されており、マルウェアは物理的に封じ込められている。

間の人材育成に関するフレームワークや各種資格試験の活用を促進する。また、産学連携による高度情報セキュリティ人材を育成するためのカリキュラム整備や教員強化、インターンシップの充実等に取り組むための体制を整備する。

また、技術者向けの情報セキュリティに係るモデルキャリア開発計画の策定や専門家コミュニティへの支援を進めることで、広く企業の情報セキュリティを担うことのできる人材の育成・確保に取り組む。

さらに、今後の課題となるＮＧＮ／ＩＰｖ６への移行などの新しい環境への移行に対応できる実践的な情報セキュリティ人材や法令遵守、情報資産や事業継続等に関するリスクを特定しつつ、情報セキュリティ対策を実践できる人材の育成を推進する。

（ウ） 情報セキュリティ人材が保有するスキルの見える化の推進

情報セキュリティ分野に人材を集め、高い能力を有する人材に支えられた情報セキュリティを構築するためには、長期的な視点から、情報セキュリティ人材が自らの能力を高めることが業務に結びつくようにし、人材の側からキャリアパスを描くことができるようにすることが有効である。

このため、実際の業務において求められるスキルを明確にするとともに、人材が保有するスキルが外部からわかりやすくするための政策を実施する。例としては、情報セキュリティ資格制度・教育制度と業務において求められるスキルや情報セキュリティ人材の目指すキャリアパスの関係を見えやすくするための取組みや、共通キャリア・スキルフレームワーク：ＩＴＳＳ[59]や民間の人材育成における各種有効なフレームワークの活用により、保有するスキルを外部に明示できる仕組みを構築する取組みが挙げられる。

③ 国際連携・協調の推進

第２次情報セキュリティ基本計画の下での取組みを通じた２０１２年における姿を実現するため、政策、オペレーション、標準の領域において、地域の特性等を考慮し、以下の６つの観点から政策を推進する。

（ア） 情報セキュリティ政策に関するＰＯＣ機能の強化と情報共有の促進

第１次基本計画に引き続き、ＮＩＳＣは様々な国際機関やフォーラムにおいて、情報セキュリティ政策を横断的に取り扱うＰＯＣとしての役割を明確化する努力

59 ＩＴスキル標準（Information Technology Skill Standards）の略。

を継続し、その機能を強化することを目指す。

具体的には、三つの観点からの取組みを行う。第一に、国家安全保障、重要情報インフラ防護、グローバルな経済活動の継続性確保、サイバー犯罪防止等の様々な観点から議論が行われる情報セキュリティ関連の国際会合等の機会に、最新の動向の把握・収集をより強力に進める。そのためには、信頼（Trust）の醸成及び顔の見える貢献が必要であることから、これらの国際会合等を機会横断的に把握・収集する機能を強化する。第二に、高い信頼関係を通じて把握・収集した動向については、国内の必要な関係機関・関係者に適切に共有されることで、初めて意味あるものとなる。このことを十分に踏まえ、ＮＩＳＣはＰＯＣとして、国内の政府関係機関に対して、適切なルールに基づいた共有を進め、政府関係機関の政策立案・実施への意味ある貢献を目指す。第三に、グローバルにＩＴを安全・安心に利用できる環境を構築する観点から、我が国の動向について、必要かつ適切なものについては、ＰＯＣを通じて公式に発信することで、世界に貢献することを目指す。

（イ） 世界の脅威動向を把握するための官民連携の確立と、効率的・効果的な国際連携活動の推進

サイバー空間の安全・安心の確保に向けて、政府にとどまらず、国家レベルのＣＥＲＴ[60]、ＩＳＰ[61]や様々な企業内のＣＳＩＲＴ[62]、研究機関等の主体も、従来から緊密な国際連携を進めてきている。このような状況を踏まえ、政府は、特に強みを発揮できる分野に注力する。また、世界の脅威動向の把握やインシデントへの対応をはじめとする情報セキュリティ関連の国際的な活動に関して、我が国全体として、効率的・効果的に進めるための官民連携体制を構築する。これによって、既に活動を行っている国内の関係機関と、国際連携活動における補完・共助の関係を築くことを目指す。

具体的には三つの観点から取組みを行う。第一に、日本政府が持つ官民連携体制について海外に積極的に発信し、国際連携に関する官民の役割分担を明確化する。第二に、官民連携を通じて、我が国から発信が可能な情報を明確化するための国内の連携強化を行う。第三に、諸外国の政府内外機関との信頼関係を向上し、情報共有を加速するため、国際的な情報共有に係る考え方を整理する。

なお、上述の政府が特に強みを発揮できる分野としては、従来から諸外国政府

60 Computer Emergency Response Team の略。

61 Internet Service Provider の略。

62 Computer Security Incident Response Team の略。

機関等との間で進めてきた最新の政策動向に関する意見交換に加え、例えば、政府機関、重要インフラに関係の深い脅威や脆弱性等のリスク情報の共有、政府機関、重要インフラ分野におけるインシデント対応の国際的な連携体制構築が考えられる。その際には、関係機関等による既存の国際的な活動を活用しつつ進めることとする。

（ウ） アジアにおける知恵の結集と情報セキュリティ水準の向上（One-Asiaの実現）

不正アクセス、フィッシング、スパム、標的型攻撃、ウェブサイトからのマルウェアの感染等の脅威は、国境を越えて生じると同時に、地理的、文化的、政治的に関係の深い地域においてある程度共通の特徴が存在する。したがって、既に欧州地域内や、米国を中心とする地域において象徴的に見られるように、地域内における連携が行われるようになってきている。このような状況を踏まえ、我が国は、アジアにおける脅威に対応し、情報セキュリティ対策の強化のための連携を推進するべく、以下の取組みを実現することを目指す。

取組みは、三つの観点から行う。第一に、人のつながりの必要性を認識し、アジアにおける脅威動向の把握・分析を我が国とともに行う専門家・研究者を積極的に養成する。第二に、現在、国際機関や国際フォーラム等で議論されているアジアにおける共同の脅威動向の把握機能創設のための取組みに対し、我が国にとっても大きなメリットのある形で支援を行う。第三に、我が国は第１次基本計画期間中に構築した米国、欧州との連携を更に強化し、ベストプラクティスの共有や共同の取組みを通じて得られた教訓、情報をアジア地域に積極的に還元していく。

なお、取組みの推進に際しては、効率性を重視し、既存の枠組みを最大限活用するとともに、関係機関と連携することとする。

（エ） 経済活動のグローバル化に対応した情報セキュリティの確保

政府は、日系企業のグローバルな経済活動の安全・安心を確保するためのビジネス環境構築に向けた取組みを行う。すなわち、海外のビジネス拠点において重要な情報資産が確実に守られ、高い事業継続性が確保されることを目指す。

具体的には、第一に、日系企業の事業活動に係る海外拠点において、高い水準の情報セキュリティ対策が実現されるような体制の構築を目指す。第二に、可用性の確保された、信頼性の高いネットワーク環境の構築を目指す。第三に、ＩＴ

製品・サービスについて、グローバル化を阻害しない形で、製造過程のサプライチェーン全体を通じて一貫したセキュリティ、信頼性を確保するための取組みの国内外における推進を目指す。このような取組みは、情報セキュリティの面でも品質の高い我が国の製品・サービスの国際競争力の向上に資することとなる。

政府は、特に関係の深い地域との間で直接議論を行う場を活用するとともに、後発の国･地域に対して積極的に支援を行う国際機関への積極的な関与等を通じ、取組みを進める。

（オ） 標準化を含んだ我が国の戦略的貢献の実現

情報セキュリティ対策に係る統一的な基準作りや標準化は、従来から様々な国際機関で行われている。近年、標準化の取組みは、従来のような技術的な領域のみならず、政策的な領域についても行われている。議論は多岐にわたり、情報セキュリティの分野に限定しても、幅広い活動の中から政府が全ての活動に関与することは非常に困難な状況となっている。一方で、我が国からは、標準化には数多くの企業を含めた関係機関が継続的な参加・貢献を通じて個別に行っている。

国際機関を通じた国際貢献には、海外の関係者との継続的な関係の構築が不可欠であるため、政府は、標準化の取組みに参画し関係を構築している国内の関係機関、企業等と連携しながら、国際機関におけるガイドラインの策定や標準化の動向を把握し、我が国が戦略的に貢献できる体制を整備することを目指す。

（カ） 情報セキュリティ文化の醸成

情報セキュリティ文化の醸成は、第１次基本計画においても、目的の一つとして掲げられている。近年、情報システム、インターネットの分野と関係の深い国際機関における議論を通じ、意識も国際的に高まってきている状況である。

真の情報セキュリティ文化の醸成のためには、企業における経営者の意識向上が必要であることと同様、世界の政府ハイレベルの認識の共有を通じた取組みが必要であることを認識し、政府は、諸外国の政府機関と協力しながら、Ｇ８、ＡＰＥＣ等のハイレベルの場を活用した取組みを目指す。

このような共通認識の醸成を通じ、インシデント発生時のオペレーションによる連携のみならず、ハイレベルからのメッセージを発出することができる環境の構築を目指す。

表４に、国際連携・協調の推進に向けた取組みの各種施策の俯瞰図を示す。

表 4　国際連携・協調の推進に向けた取組みの各種施策

分野	リージョナル	グローバル
政策	（ウ）アジアにおける知恵の結集と情報セキュリティ水準の向上 （エ）経済活動のグローバル化に対応した情報セキュリティの確保	（エ）経済活動のグローバル化に対応した情報セキュリティの確保 （カ）情報セキュリティ文化の醸成
オペレーション	（ウ）アジアにおける知恵の結集と情報セキュリティ水準の向上（One-Asia の実現）	（イ）世界の脅威動向を把握するための官民連携の確立と、効率的・効果的な国際連携活動の推進
標準化	（オ）標準化を含んだ我が国の戦略的貢献の実現	

（注）　（ア）の施策については、全ての政策実施の前提となるため、ここに掲載されていない。

④　犯罪の取締り及び権利利益の保護・救済

（ア）　犯罪取締りのための基盤整備の推進

法執行機関における取締り体制の強化、技能の向上、国際協調の推進等の基盤強化を一層推進する。

さらに、原因特定や犯行過程解明に不可欠な情報提供がなされ、被疑者の検挙や被害の拡大防止につなげられるよう、法執行機関と被害者等との間の良好な協力関係の構築を一層推進するなど、犯罪に強いＩＴ社会構築のための官民連携に向けた取組みを推進する。

また、サイバーテロに対しても、その特性を考慮した上記の取組みにより備えを強化する。

（イ）　犯罪抑止のための広報啓発の推進

国民がサイバー犯罪の被害者とならないよう、犯罪の被害状況や手口、具体的な対策の方法等に関する広報啓発を一層推進する。

（ウ）　権利利益の保護・救済のための基盤整備の推進

国民の基本的人権に十分配慮しつつ、サイバー空間の権利利益の保護・救済の

ための基盤の更なる整備に努める。具体的には、情報を預ける側の権利利益を情報を預かる側が保護・救済する取組みに係る情報開示の促進、サイバー空間の安全性・信頼性を向上させる技術の開発・普及などに取り組む。

第４章 政策の推進体制と持続的改善の構造について

第１節　　政策の推進体制

「成熟した情報セキュリティ先進国」を目指しながら、「ＩＴを安心して利用できる環境」の構築を行うためには、あらゆる主体での意識共有とともに参加が不可欠である。政府は、第２章で示すようにＩＴ時代の力強い「個」と「社会」の確立を図りつつ、第３章で示した重点政策を中心に、官民における統一的、横断的な情報セキュリティ対策を推進すべく、全体としての適正な資源配分を行っていく必要がある。

（１） 内閣官房情報セキュリティセンター（ＮＩＳＣ）の強化と役割

ＮＩＳＣは、第１次基本計画の下での取組みと同様、国際的にも国内的にも、最高の英知を結集していくための体制として、政府全体の推進体制を有効に機能させるための中核として強化することを引き続き目指す。また、横断的な情報セキュリティ問題に関する国際ＰＯＣとしての役割を十分に果たせるよう引き続き強化を図る。

さらに、ＮＩＳＣは、情報セキュリティに関わる多くの知見が民間に蓄積されていることから、民間の人材を積極的に活用することに努めるとともに、柔軟に、政府内の人材を最大限活用し、その能力の維持・強化を図る。また、同時に、政府職員の人材育成の中核拠点として機能することも引き続き目指す。

本基本計画の内容からも明らかなように、情報セキュリティ政策の政策領域は多岐にわたる。このため、ＮＩＳＣは関連領域を担当する様々な機関との結節点となるとともに、課題ごとに解決に向けた関係機関の連携体制の最適化を柔軟に進め、情報セキュリティに関連する課題に対する我が国全体としての解決能力の最大化を実現するために、率先して活動に取り組む。

（２） 各府省庁の強化と役割

各府省庁は、引き続き、情報セキュリティ政策会議、ＮＩＳＣを中核とした、情報セキュリティ政策を推進する枠組みの下、自府省庁の情報セキュリティ政策及び関連領域に係る体制の充実・強化を図る。体制の充実・強化にあたっては、必要に応じて民間の人材の積極的な活用を含め、有効な方策を柔軟にかつ最大限活用する。そして、推進体制が縦割りにならないよう十分に留意しながら、官民における統一的・横断的な情報セキュリティ対策の推進が行われるよう、各種政

策の実施に引き続き努める。

（３） 状況の変化の適時適切な把握と新しい課題への対応

情報セキュリティ分野は、脅威や技術など、様々な側面において変化が早い。このため、刻々と変化する状況を適時適切に把握するとともに、新たに生起する課題に対して迅速かつ的確な対応を行うことが重要となる。また、新たにトレンドとなる政策手法についても適切な検討を進めることが不可欠である。さらに、情報提供主体を対象とした新たな取組みを進めることも必要である。

このため、ＮＩＳＣをはじめとする様々な関係機関・関係者が連携し、また情報セキュリティ政策会議の下に適宜設置される専門委員会も活用し、法律、技術、啓発など政策に係る幅広い視点全般から、検討を動的にかつ柔軟に進める体制を強化する。

第２節　　他の関係機関等との関係

第２次基本計画は、我が国の情報セキュリティ問題を俯瞰した中長期の戦略を定めるものであるが、情報セキュリティ政策は、国民生活・社会経済活動に広く関係するものであり、その実施に当たっては、第１次基本計画同様、様々な関係機関との連携を行っていく必要がある。

様々な関係機関の中でも、ＩＴ戦略本部との関係においては、情報セキュリティ政策がＩＴ政策の主要な部分の一つとして位置付けられるものであり、かつ、第２次基本計画が「ＩＴ新改革戦略」の情報セキュリティ関連部分を実質的に担うものであることに留意する必要がある。また、総務省行政管理局とは行政情報システムに関連する取組みを中心に連携を更に強化することが不可欠である。

中央防災会議との関係においては、情報セキュリティ政策のうち重要インフラ関連部分について必要な連携を行うことが必要である。また、総合科学技術会議との関係においては、情報セキュリティ政策のうち研究開発・技術開発関連部分と全体の科学技術政策とが整合して推進されることを確保する必要がある。さらに、国民生活審議会との関係においては、個人情報保護等の観点から、情報を提供する側の主体に係る取組みを進めるにあたって十分な連携を確保する必要がある。

情報セキュリティ政策会議及びＮＩＳＣは、これらの会議の十分な協力を得つつ、情報セキュリティ政策を推進することとする。

第３節　　持続的改善構造の構築

情報セキュリティを巡る問題は、新たなリスク要因が次々と発生し、その変化

が早いことから、政策の効果を常に評価し、改善を行うことが必要である。このため、政府は、第１次基本計画の下での取組みに続き、以下のような持続的改善のための構造を活用する。

（１） 「年度計画」の策定とその評価等

政府は、第２次基本計画の実現を図るため、毎年度、より具体的な施策の実施プログラムを「年度計画（セキュア・ジャパン２０ＸＸ）」として策定するとともに、その実施状況を社会情勢の変化とともに評価し、結果を公表する。また、補完調査を必要に応じて実施し、この結果も併せて、「２０ＸＸ年度の情報セキュリティ政策の評価等」として公表する。この取組みに当たっては、詳細を情報セキュリティ政策の評価等の枠組み文書によって定められた枠組みにのっとることとする。

なお、政府以外の関係機関における対応が不可欠である等、施策を円滑に進捗させる観点から、中長期的な計画を定めることが必要なものについては、単年度にこだわらず、複数年度のマイルストーン設定も行う。

（２） 年度途中での緊急事態対応に向けた取組みの実施

政府は、「年度計画」の実施途中であっても、新たなリスク要因や想定し得なかった事故、災害や攻撃の発生等の緊急事態に対応するための取組みを実施する。

（３） 評価指標の改善

各対策実施領域等における、情報セキュリティに関する評価の指標は、情報セキュリティ政策の枠組み文書によって設定されているところ、政府は、同枠組み文書に定めた方法により、今後も引き続き評価指標の改善を図る[63]。

（４） 第２次情報セキュリティ基本計画の見直し

政府は、第２次基本計画について、３年後に見直しを行うとともに、環境変化が生じた場合には、期間中であっても見直しを行うこととする。

---

63 なお、重要インフラの領域については第２次行動計画において先行的に評価指標の改善を行っているため、同枠組み文書における評価指標の改善に際しては、第２次行動計画における評価指標を基本として検討することとする。