「第１次情報セキュリティ基本計画(案)」への意見提出者一覧
（五十音順）

ＡＲＭＡ　International東京支部
International Information Systems Security Certification consortium((ISC)2)
有限責任中間法人　ＪＰＣＥＲＴ／ＣＣ
有限会社　インターネット応用技術研究所
インテック・ウェブ・アンド・ゲノム・インフォマティクス株式会社
株式会社　インテック・ネットコア
株式会社　ＮＴＴデータ
産業技術短期大学校
社団法人　情報サービス産業協会
独立行政法人　情報処理推進機構
特定非営利活動法人　情報セキュリティ研究所
セキュリティ・エデュケーション・アライアンス・ジャパン（ＳＥＡ／Ｊ事務局）
徳増晃秀（個人）
ドコモ・システムズ株式会社
日本ＩＢＭ株式会社
財団法人　日本情報処理開発協会
特定非営利活動法人　日本セキュリティ監査協会
日本放送協会
財団法人　ハイパーネットワーク社会研究所
株式会社　日立製作所
株式会社　ラック

※　五十音順にて記載しております。下記提出意見の意見番号との関連はありません。

提出意見一覧

(意見1)

該当箇所	1．第3章、第1節、(1) 2．第3章、第1節、(1)、イ、④
意見内容	1．　第3章、第1節、(3)、③にある「情報セキュリティ対策を行っている担当者のモチベーションの維持のための取組みを促進する」という部分は企業だけで無く、政府、地方自治体に対しても必要。第3章、第1節、(1)にも入れるべき。 2．　政府機関における人材育成と同等の内容にするべき(専門的職員を配置し、資格を保有させる。)
理　由	1．　内部統制、責任の重さ、資格維持等の個人負担を考慮して、何らかのインセンティブがあってしかるべき。苦しいだけでインセンティブが無いため人材が集まらないし、やりたいとも思わない。「**先ず隗より始めよ！**」です。新しい給料表を創り、人材を集めましょう。※企業だけとはいえ、この文章が入ったことは絶賛に値すると思います。ぜひ残してください。 2．　国家全体のセキュリティ強度は、最も低い所の強度となります。中央だけ強化しても意味がありません。人材を育てるには時間が掛かります。直接国民と接し、リスクも高い地方公共団体についても後回しせず、網を掛けるべきです。

(意見2)

該当箇所	P26(4)犯罪の取締りおよび権利･権益の保護･救済
意見内容	どんな素晴らしいシステムを構築しても、使用する人々の信頼･安心感がなければ、無駄な巨大投資になる。
理　由	1)　IT犯罪への対処は、ソフト面とともに、精神面(人の心)から対処 　ソフトプログラムでの防御策は、両者の凌ぎあいが続く。それはそれで必要と思います。しかしそれだけでなく、やっても無駄だと思わせることが、大切と思います。「IT犯罪は他の犯罪以上に、重犯罪である」とする法律の成文化。小･中学校の教育でも、IT犯罪は重犯罪であると教え込む。但し、犯罪者に「IT犯罪の対処マニュアル」作りに協力してもらう。又、事件があったとき犯罪者に協力してもらう。それらにより、恩赦で1階級づつ減免していく。(法律の刑は重いが、協力者へは恩赦制度で実質的には軽くしていく)これらにより、警察としても又、メーカーとしても「対処策のノウハウ」を得ていき蓄積が出来る。 2)　IT犯罪へは初動逮捕で確実に検挙を 　初動段階で押さえていかないと国民の不信感が増大する。かつ、犯罪者に「この程度でも捕まらない」が蔓延してしまう。連鎖犯罪になる。警察が、軽く見られてしまう。サイバー犯罪に取り締まり対する優秀なメンバーの選出、公安当局とも一体となって「サイバー犯罪者取締り特別チーム」の編成。普段からネットを常時監視しある程度の不審者の目安をつけておく。IT犯罪は初動で、確実に捕まるという神話にまで持っていく。やっても無駄だと思わせることが、ソフト面の防御以上に重要。

（意見3－1）

該当箇所	P3② 「、、安心･安全で、信頼できるIT社会の実現、、」
意見内容	情報セキュリティに絶対の対策はないため、「安心･安全で信頼できる」とはどれくらいのリスクを許容できるとすることなのかについて、国民的なコンセンサス作りなどが大事である
理　由	個々人の尺度が違うままでは、国民が満足し、信頼できるIT社会は実現できない。

（意見3－2）

該当箇所	P4④ 「このIT基盤を、真に依存可能で強固なものにすることが、情報セキュリティの役割である」
意見内容	情報セキュリティの対象である情報そのもの、世界を豊かにする知が表現された情報そのものを大事にするという国民の意思など、人的な基盤についての役割意識が欠けているのではないか。
理　由	インフラのみに注目している表現振りが基本計画全体に散見されるが、そもそも重要な対象である「情報」について着目するべき。

（意見3－3）

該当箇所	P5 「(2) 実現すべき基本目標」

意見内容	知を守る基盤としての捉え方が欠けている。
理　由	前項でも記載したように、守るべき対象物の属性への考慮がないため、インフラとしての基礎機能に終始してしまっている感がある。

（意見3－4）

該当箇所	P7　(1) 官民各主体の共通認識の形成：「何のために情報セキュリティ対策を行うのか」という点についての共通認識を形成する
意見内容	インフラについての共通認識に加えて、情報の価値の認識がなければ共通認識は難しい。インフラについての共通認識だけでは足りない。
理　由	インフラのみに注目している表現振りが基本計画全体に散見されるが、そもそも重要な対象である「情報」について着目するべき。（前述）

（意見3－5）

該当箇所	P7　(2) 先進技術の追求
意見内容	ヘテロなモノの集合体と人により、システムが形成されることに鑑み、セキュリティをアーキテクチャとして定義する視点が欠けている。ビルトイン型が、オープンなシステム構築に障害とならないような方向付けが不可欠である。

理　由	ネットワーク化社会において、異機種が接続され、誰もがアクセスする可能性があるため、まずはアーキテクチャとしてセキュリティを捉えることが重要。ビルトイン型の情報セキュリティシステムが排他的なものになり、他のシステムとの接続を困難にならないように注意するべき。

（意見3－6）

該当箇所	P9 「ITを安心して利用可能な環境」の構築
意見内容	「IT を安心して利用できる環境」は、国民の成熟したリスク認識の上に初めて構築可能と考える必要がある。そのための官民連携の施策を講じる必要性を加味するべき。
理　由	（上述）

（意見3－7）

該当箇所	P11 （3）企業・
意見内容	国際競争力の担い主である企業が、「競争力の源泉である知とその表現された情報」を大事にし、セキュリティ確保に取り組む姿勢が必要と考える。その部分の重要性の記述を充実すべき。

理　由	インフラのみに注目している表現振りが基本計画全体に散見されるが、そもそも重要な対象である「情報」について着目するべき。（前掲）

（意見3－8）

該当箇所	P11　(4) 個人
意見内容	安全と表現される場合の「リスクの認識、残留リスクの許容」という現実についての理解を求める努力についても言及すべきである。
理　由	（上述）

（意見3－9）

該当箇所	P13　(4) メディア・
意見内容	リスク認識についての国民的なコンセンサス作りに大きな役割が期待されるため、それについても言及するべき。

理　由	（上述）

（意見3－10）

該当箇所	P14　第3章　今後3年間に取り組む重点政策-「新しい官民連携モデル」の構築-
意見内容	「ITを安心して利用可能な環境を構築する」官民連携モデルが語られているが、一貫して守るべき対象の知を代表とする情報の価値について触れていない。そのため、具体的な情報の価値が官民を貫いて流通していく側面における統一的なセキュリティ確保の基準などについて官民連携のやり方の記載がかけている。施策がインフラ偏重になっているのではないか。
理　由	インフラのみに注目している表現振りが基本計画全体に散見されるが、そもそも重要な対象である「情報」について着目するべき。（前掲）

（意見3－11）

該当箇所	P15　ア　政府機関・
意見内容	政府機関については検査・評価とあいまいな表現になっているが、地方公共団体と同等に、情報セキュリティ監査について、明記するべき。

理　由	検査･評価とあいまいな表現になっているが、地方公共団体には明確に求めながら、政府機関に明記しないのはバランスを欠く。

(意見3－12)

該当箇所	P20 (4)個人
意見内容	リスク認識にかかわる教育が必要である
理　由	情報セキュリティに絶対はないため、万全の対策は施すとしても、情報セキュリティに関するリテラシーとして、個人には自己責任の原則とリスクの認識についての教育が必要。

(意見4)

該当箇所	P．7　第1章第2節(2)先進技術の追求 P．15　第3章第1節ア③(イ)セキュリティ強化に資する新規システム (機能)の導入の検討とその実現
意見内容	「セキュリティ強化を図るため、IPv6、国家公務員身分証ICカード、暗号、電子署名、生態認証等の新規システム(機能)の導入について総合的な検討等を行い、その実現を推進する。」に賛同する。また、特に日本のIPv6の優位性を維持できるように、政府機関の積極的な導入推進や国内普及のための施策を実施願いたい。

理　由	IPv4アドレスは2010年前後に枯渇するための対策と、IPv6を採用することにより、NATの存在を前提にしない以下の情報セキュリティの対策効果が期待できる。 (1)　エンドツーエンドレベルのセキュリティが確保できる。 (2)　従来のFWレベルの境界セキュリティの組み合わせによりより粒度の細かいセキュリティ対応が可能になる。 (3)　端末の一台一台の特定が可能になるため、アクセスログ管理がより精度高くでき、セキュリティの向上が図れる。

(意見5－1)

該当箇所	第3章 第1節 (1) ア ④⑤、および 第3章 第1節 (1) イ ④、 第3章 第1節 (3) ③、 第3章 第1節 (4) ①、 第3章 第2節 (2)、 人材育成について
意見内容	政府として関与すべき人材育成については、高度人材育成だけでなく、啓蒙教育を積極的に実施する必要がある。 上記該当箇所に人材育成の記述があるが、第2章 第2節 (1)の「政府が主体的に関与する部分」として考えた場合、高度人材育成以前の問題として、政府によりマインドセットとしての啓蒙教育を実施する必要があると考える。
理　由	人材育成を考えた場合、スキルセットとマインドセットに分けられ、情報セキュリティについても、スキルセットにあたる高度技術と、マインドセットに当たる啓蒙が考えられる。 マインドセットが十分でない状態で、スキルセットを育成しても効果は得られないとともに、提供価格が高額となる高度人材育成は民間企業で提供されるが、低価格となり利益が見込めないため、民間に期待しても啓蒙教育は提供されないこととなる。

(意見5－2)

該当箇所	第3章 第2節 (2) ③ 資格制度の創設について
意見内容	第2章 第2節 (1)の「競争的活動・自主的取組みを促進する部分」として考えた場合、政府として新たに資格制度を創設するのではなく、市場に現存する資格の有効性を検討し、ロードマップとして示していく必要があると考える。 既に、NPO 日本ネットワークセキュリティ協会では、同様の取り組みを始めており、推奨教育や資格を検討し、ロードマップを示していこうとしている。 JNSA 該当 URL： http://www.jnsa.org/active/2005/active2005_4_2.html

理　由	政府として市場に現存する幾多の資格を検討し、あるいは新資格制度を創設することは、民業を圧迫するだけでなく、既に資格を取得あるいは学習した者個々人の負担増加にもなりかねない。 また、既取得者に対する同資格の示されたロードマップを開示することにより、キャリアチェンジによる情報セキュリティ技術者人材不足解消にも貢献できると考える。

（意見6）

該当箇所	「基本計画」（案）13ページの9～10行目
意見内容	「（前略）メディアによって取り上げられるような環境の整備が必要」という記述を「メディアによって取り上げられるよう、迅速な公表に努める」などの表現に変更されるよう求めます。
理　由	「基本計画」（案）の表現は曖昧かつ多義的であり、メディアの編集の自由を制約するかのような誤解を与えかねないため、より明確かつ具体的な表現に変更すべきである。

（意見7－1）

該当箇所	シート1　はじめに
意見内容	重要インフラにおける情報システムの障害、大量の個人情報漏洩等並び構造計算書の偽装事件などが社会問題化し、…・ 赤太字部追加
理　由	IT利用に関連した脅威の増大だけではなく、逆にITを利用することで、紙書類のハンドリング課題で課題となっている事案も積極的に解決していくことが望まれる。 構造計算書を例にとれば、印刷物としての受け渡しの弱点を突かれており、電子ファイルとして改ざん防止対応を入れておけば、防御できることも多かったと報道されている。

(意見7－2)

該当箇所	シート6　⑶現在の課題と解決の方向性　例
意見内容	(例4;IT活用が不十分な例　追加　) 建築確認検査において、紙書類がベースであるため、偽造の摘出が困難であった。また、保存期限も5年とその重要性比して短かった。
理　由	ITの利用が不十分で重大な課題が残っている例も掲載することが望ましい。

(意見7－3)

該当箇所	シート11　⑶企業
意見内容	IT社会を構成する一員としての立場からも情報セキュリティ対策、企業活動の記録管理に取組む責任を認識した上で 赤太字部追加
理　由	姉歯氏による構造計算書偽装問題、、三菱自動車のクレーム隠し、ＪＲ西日本　福知山線事故要因体質改善などの大きな社会問題が発生しており、国民の安全･安心を守っていくには企業活動の適切な記録管理が不可欠である。

(意見7－4)

該当箇所	シート22　⑵情報セキュリティ人材の育成･確保

意見内容	情報セキュリティに関する高度な研究開発･技術開発を支える人材、記録管理を適切に行う人材の育成･確保が不可欠である。 赤太字部追加
理　由	情報セキュリティはあくまでもツールであり、情報を活かしてこそ活きてきます。官民の活動を電子的に適切記録、管理していくことは国民に対し、 広く安心、安全を提供することなります。特に、2005 年にレコードマネジメントに関して、ＩＳＯ１５４８９がJIS化されましたので、これをベースにＩＳＯ9000 をはじめ各種企業活動に適用していくことで、実効があがっていくものと考えます。 このような記録管理を実行していく人材が現在少なく育成、確保は不可欠と考えます。

(意見7－5)

該当箇所	シート 22　(2) 情報セキュリティ人材の育成･確保 ②情報セキュリティに関する資格制度の体系化
意見内容	最高セキュリティ責任者（ＣＩＳＯ）、記録管理責任者、各組織の運用担当者 赤太字部追加
理　由	2005 年にレコードマネジメントに関して、ＩＳＯ１５４８９がJIS化されております。このＩＳＯはＩＳＯ9000 をはじめ各種ＩＳＯのベースとして参照されようとしています。 IT技術を含めたレコードマネジメント（記録管理）についても資格制度化を行いモチベーションのアップが必要と考えます。

(意見8)

該当箇所	第3章　今後3 年間に取り組む重点施策 -「新しい官民連携モデル」の構築 第2節　横断的な情報セキュリティ基盤の作成 （2） 情報セキュリティ人材の育成･確保
意見内容	項目番号③として以下の内容の追記をお願いしたい。 ③世界に通用する情報セキュリティ技術･知識を習得した実務家･専門家の育成 セキュリティ脅威のボーダーレス化や解決に当っての世界レベルでの連携を円滑に行うためには、世界に共通して適用されている技術や知識の習得とこれを裏付ける国際的資格の取得を促進することが必須である。

理　由	1．人材育成の重要性について各所で述べられていますが、セキュリティ脅威のボーダーレス化、問題解決の国際協調の必要性から考えた時に、人材育成の要点として「国際的に通用する人材像」という観点が必須となり、その推進策についても触れる必要があります。 2．昨今のセキュリティ脅威は、脅威の発信元、使用される技術などが1 国家に限定されるものではありません。また脅威の広がりもまさに国境を越えて瞬時に発生する状況にあります。こういった現状に対して、「国際的に通用する人材」を育成し、国際協調の枠組みの中で種々の問題解決に当らなければいけないことは自明です。 3．同節（2）の②でも述べられているように教育の理解度を測る意味からも国際的に認められたNPO など第三者による客観的な個人に対する認証を取得することが非常に重要なポイントであると考えます。その意味からも「国際的に通用する人材」の育成にあたっては、国際的に認められている資格取得を前提にした教育体系を作っていき、その延長線として、個人が「国際的に通用する人材」であるかどうかの達成基準を明確にするために国際的資格を取得することを一つの要件とする必要があると考えます。 4．特にこの施策の政府機関での執行においては、情報セキュリティ対策業務に携わる専門的職員が、前述の人材として育成されていく必要性が高い中で、専門的職員の当該職務への在籍期間を従来より延長し、より専門性を高めるような施策も検討していただけることを期待します。 5．また政府機関や公共性の高い業種に携わる企業においては、諸外国で既に行われているように国際的な資格に準拠した政府推奨資格の設定、及び当該推奨資格の最低保有者数の指定やガイドライン化などを行っていく事で、国内外にも国際的に通用するセキュリティ立国を目指すという姿勢をアピールできるのではないかと考えます。この点についても是非とも検討していただける事を期待します。

（意見9）

（1）非営利組織の活用について

本基本計画では、第 2 章において、新しい官民連携モデルの構築における主体は、

・政府・地方公共団体

・教育機関・研究機関

・情報関連事業者・情報関連非営利組織

・メディア

が挙げられている。

　このうち、「情報関連非営利組織が、全国的に、または地域ごとに設立され、活動を行っていることは、適切なITの利用・活用推進、トラブル発生時における利用者の対応能力の向上、民間における連携対応体制の強化の観点からきわめて望ましいことであり、今後も、こうした非営利組織の積極的な活動が行われることが期待される。」とのことで、非営利組織の活動に高い評価と期待をされていることに対し

ては敬意を表する。しかしながら、第 3 章における具体的な取り組みの中には、非営利組織に対する政府の政策や非営利組織のとるべき活動方針が全く示されていないのは理解に苦しむところである。

そもそも非営利組織の活動の視点は、あくまで市民の目であるべきであるが、その活動は自主的運営による組織維持の観点から、ある程度の営利活動を行わざるを得ない。また、情報セキュリティ対策の支援という目的を遂行するためには、組織自体の信頼性確保が必要であり、その構成メンバーも大学等の教育者や公的資格などを有する有識者が中心となる。他方、非営利組織は市民を含む行政や企業などに対しても、企業のように自社製品に偏った、しかも営利に結びつく活動が中心となる組織や、行政のように自ら市民の中に積極的に飛び込んで活動することが難しい組織と異なった、市民中心の活動ができるという大きなメリットがある。

たとえば、我々の活動の1つに「自治体職員の個人情報保護に対する研修」があるが、この自治体の保有する個人情報は、企業等の保有する個人情報と異なり、情報の主体である個人の同意を得ることなく法的根拠の下に集められた情報である。これらの情報に対するセキュリティをどのレベルに置き、どれだけのコストをかけてセキュリティを確保するのか、その決定には民意が反映されていなくてはならない。我々は非営利組織としてその民意を代表する1つの組織として情報セキュリティに関する啓蒙活動を行い、地方自治体における個人情報保護の体制強化を訴えてきた。しかし、保護を強化するだけでは情報セキュリティの確保に必要なコストが増大するばかりであり、最終的には市民の税負担という形で跳ね返ってくることになる。我々非営利組織は、市民の視点で「知恵」と「汗」による活動を通じて、市民自らの個人情報を、自らの参加によってより低い税負担で保護していきたいと考えている。

しかしながら、非営利組織がこれらの活動を効果的に実行するのは極めて難しいのが実情である。すなわち、多くの場合、組織を維持し活動するための財政的な基盤が脆弱であり、しかもボランティアが中心ということで責任の所在が不明確になるほか、セキュリティ対策に必要な最新情報が十分に収集できないなど、何より非営利組織が活動できる基盤整備を推進する必要がある。

我々は、財政的には、主に地方自治体へのコンサルタントや研修、企画、サービスなどを実施して適切な対価を得ることにより組織の維持運営コストを賄っている。また、これらの活動を全国的に連携して展開することで、相互の組織の保有資産の有効活用を図り、支援者の活動領域を広げるべく情報セキュリティ関連の非営利組織が集う場を毎年2回開催しているところである。しかし、各地の状況は、リーダやメンバーの不在、活動内容の不安定、自治体の理解不足などのため、セミナーやコンサルタントを行う程度で、なかなか実質的なセキュリティ対策支援活動が実施できないのが実情である。

したがって、政府の期待を担い市民に本当に役立つ非営利組織本来の活動を推進するためには、行政の押し付けでなく、また企業による営利的な視点でなく、行政・企業と協調しながら最終的には市民に最大のメリットを与えられる活動の場が必要である。そのためには、行政からの補助や企業からの協賛に頼ることなく、自らの活動による妥当な収益を確保できる業務遂行能力を養う必要がある。そのための具体的な対応として、行政からは事務所などの活動拠点の安価な提供、企業からは取り扱っている機器やソフトの安価な提供、各種ベンダーからは脆弱性などの情報の提供を受けられるような制度作りが不可欠である。さらに自治体は、自らセカンドオピニオンとしての客観的なセキュリティ対策の評価を求めることや、市民のために有効なセキュリティ教育、サービスの委託などを推進すべきである。

このように、非営利組織への補助や協賛だけでなく、行政や企業でできない分野、非営利組織のほうが効率のよい分野を定めて、その活動を活性化することによって組織が維持できるような支援を積極的に行われることを期待したい。

本章には、続けて「こうした非営利組織には、情報セキュリティに関する啓蒙活動、警戒・脅威情報や脆弱性情報等の提供、そしてわが国に求められる実践的人材の育成にも寄与することが期待される。」と書かれているが、現在のように何らの効果的支援もなく、ただ期待しているだけでは、それに的確に答

えることは多くの場合困難であると思われる。従って、本当に市民のセキュリティ対策に有効な活動を行うために、現場の組織として活躍できる「場」を構築するにあたっての適切な支援を望みたい。そうすることで、非営利組織は、国民のセキュリティ対策支援に大きな力を発揮するとともに、自治体にとってもセキュリティ対策コストの適切化、実質的な市民サービスの推進に非常に有効な手段となるはずである。

このような活動が全国的に連携して有効に実施されると、本計画第 1 章の基本理念に示された「防災や災害対策などの国民生活の視点に立った、安全・安心で、信頼できるIT社会の実現が求められている。」という課題に答えられるとともに、そのような活動を行政や企業が支援することにより「広く、多面的な課題を解決する必要のある情報セキュリティ問題への取り組みは、個々の主体が各々で行うだけでなく、わが国全体として一体となって行う必要がある。」という呼びかけに、市民の立場から具体的に応えることが可能となる。

もともと、わが国の社会的セキュリティ、つまり社会の安全性は世界に誇るものであったが、過度の個人主義とインターネットによる最悪の非セキュリティ社会との結合により、これまでの社会の安全性が却って情報社会の不安となっている。したがって、わが国では市民レベルのセキュリティ対策を充実させることにより、世界に示すべきセキュリティ立国の国づくりが可能となると思われるが、現在では一般市民をサポートする組織が存在しないのが現状である。これを実現するためには、営利目的でなく全国的に地に足のついた市民が主体となったサポート部隊が存在する必要がある。それでこそ、「わが国は、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」を確立する潜在的可能性、すなわち「セキュリティ立国」の思想に基づく国づくりが有効であると考えられる。」のである。

従って、本計画に示された「情報セキュリティにおける「新しい官民連携モデル」を構築し、わ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り組んでいくことが必要である。「新しい官民連携モデル」の下で、わが国全体としての資源の重点的・戦略的投入の強化が図られ、国際的に見ても、わが国が常に世界をリードする「情報セキュリティ先進国」になることを求め続けることが重要である。」との認識を実行に移すには、官民というのが行政と企業だけの連携でなく、市民活動そのものを1つの主体的活動として組み込む必要がある。官民つまり行政と企業が市民に向かってセキュリティ対策を押し付け、それで企業が営利を貪るような図式でなく、市民が自主的にセキュリティ対策に取り組むことで、自らの安全を図るような仕掛けを構築することこそ「ジャパンモデル」にふさわしいと考えるものである。

非営利組織は、そのような各地域における市民中心のセキュリティ活動を推進するのに最もふさわしい位置にいると思われるので、ぜひとも、各地の非営利組織が自主的に活動できるような具体的な政策の提示や制度の構築を推進していただきたい。

(3) 人材育成について

これまでコンピュータ関連のシンポジウムを多数開催しているが、我々は参加者らとの情報交換を通じて、セキュリティに関する人材の必要性を痛感し、そのための具体的な活動を計画しているところである。

本計画の第 3 章では、「政府機関の情報システム管理部門において、情報セキュリティ対策業務に携わる専門職員については、全員が情報セキュリティに関する資格を保有することを目指す」とあるが、これは既存の資格取得を推進するのか新たな資格制度を新設するつもりなのかが不明である。また、個人情報そのものを取り扱っている地方自治体に、そのような資格取得者を確保することが詠われていないことにも疑問を持つ。

我々は、企業の経営トップにおけるセキュリティへの理解を得るための活動も、自治体の職員や一般市民のセキュリティに関するリテラシー向上も共に緊急の課題であるが、実際にその活動を効果的に実施するのに、どのような方策でどのような体制で実現するのかが重要であると考えている。このような場

面でこそ、各地における有用な非営利組織の設立とその活動の支援体制を整備すべきである。

また、既存の情報セキュリティに関する資格も重要であるが、実際の事故が発生したとき、その事態に適切に対応する人材の決定的な不足に対して非常な危機感を持っている。特に、そのような情報セキュリティに対する危機管理を行うとともに、事故発生の折にはすばやい原状復帰とともに、その工程でフォレンジックに配慮するなどの適切な対応が不可欠である。

日本でも、セキュリティに関する専門の大学院設立や大学のコースの新設など、順次その教育体制が整備されつつあるが、先に総務省から発表された「情報セキュリティ人材が約 12 万人不足している」との報告を待つまでもなく、必要な人材の育成には全く追いついていない状況である。さらに、情報セキュリティに関するインシデントに正しく対応できる危機管理担当者などは、ほとんど存在していないに等しいのが現状である。

我々は、このような状況に鑑み、全国の自治体や市民の情報セキュリティ対策を支援する非営利組織の設立とその連携を推進するとともに、非営利組織の中核となって活動できる人材の育成を行う必要が急務であると考えている。また、情報セキュリティの事故発生時にすばやく対応できる専門の技術を身につけた要員を地方自治体に配置すべきであり、その支援にかけつける非営利組織の活動も有効であると考えている。

このような観点から、我々は、特に「情報セキュリティの危機管理要員」の養成を行うべく、専門の教育機関の設立に向けた企画・検討を行っている。本計画では、「情報セキュリティ関連の高等教育機関（大学院等を中心）において、他分野の学生や社会人を受け入れる等、多面的・総合的能力を有する人材の育成・確保やリカレント教育への主体的な取り組みを促進する。」と述べられているが、従来の大学のような理論中心の学習でなく、経営的な視点からの実践的な危機管理教育とともに、実際に導入しているハードウェア、ソフトウェアをベースに、事故発生時に実質的な事後対応ができる技術者の養成を行うことが重要である。特に、めまぐるしく変化する情報セキュリティ対策とともに、そのような変化に応じた最善の事故対応の具体的な技術の習得は、従来の既存の大学などではカリキュラム編成上困難な場面が多く、非営利組織の持つ自治体や企業との協調による柔軟性を活かすことによって、より実践に役立つ危機管理要員の養成が可能であると考えている。

本計画に示されるような「個人が高度な情報セキュリティ機能を享受しながら負担感なく利用できる製品やサービス（情報セキュリティ・ユニバーサルデザイン）」を提供するためには、行政や企業だけでは実現が難しく、そのような場面にこそ、信頼に足る非営利組織の効果的な活動の場があるものと思われる。情報セキュリティに対する基本計画を策定したり、情報セキュリティ関連製品を開発するのは中央であるとしても、全国の自治体や市民は、その地域においてセキュリティ対策を実施するわけであるし、一旦事故が発生すれば直ちにその対処にあたらなければならないのであるから、そこで効果的な支援ができる非営利組織の存在は非常に有効であると考える。しかし、放置しておけば、前述のようにそのような非営利組織が効果的な活動を行うのは非常に難しいのが現状である。したがって、本計画において、今後 3 年間に取り組む重点政策として、ぜひとも全国の非営利組織の整備と具体的な支援策を組み込まれるように切に望むものである。

（意見１０）

該当箇所	第3章　今後 3 年間に取り組む重点施策－「新しい官民連携モデル」の構築 第2節　横断的な情報セキュリティ基盤の作成 （2）　情報セキュリティ人材の育成・確保

意見内容	項目番号③として以下の内容の追記をお願いしたい。 ③世界に通用する情報セキュリティ技術･知識を習得した実務家･専門家の育成 セキュリティ脅威のボーダーレス化や解決に当っての世界レベルでの連携を円滑に行うためには、世界に共通して適用されている技術や知識の習得とこれを裏付ける国際的資格の取得を促進することが必須である。
理　由	1．人材育成の重要性について各所で述べられていますが、セキュリティ脅威のボーダーレス化、問題解決の国際協調の必要性から考えた時に、人材育成の要点として「国際的に通用する人材像」という観点が必須となり、その推進策についても触れる必要があります。 2．昨今のセキュリティ脅威は、脅威の発信元、使用される技術などが 1 国家に限定されるものではありません。また脅威の広がりもまさに国境を越えて瞬時に発生する状況にあります。こういった現状に対して、「国際的に通用する人材」を育成し、国際協調の枠組みの中で種々の問題解決に当らなければいけないことは自明です。 3．同節(2)の②でも述べられているように教育の理解度を測る意味からも国際的に認められた NPO など第三者による客観的な個人に対する認証を取得することが非常に重要なポイントであると考えます。その意味からも「国際的に通用する人材」の育成にあたっては、国際的に認められている資格取得を前提にした教育体系を作っていき、その延長線として、個人が「国際的に通用する人材」であるかどうかの達成基準を明確にするために国際的資格を取得することを一つの要件とする必要があると考えます。 4．特にこの施策の政府機関での執行においては、情報セキュリティ対策業務に携わる専門的職員が、前述の人材として育成されていく必要性が高い中で、専門的職員の当該職務への在籍期間を従来より延長し、より専門性を高めるような施策も検討していただけることを期待します。 5．また政府機関や公共性の高い業種に携わる企業においては、諸外国で既に行われているように国際的な資格に準拠した政府推奨資格の設定、及び当該推奨資格の最低保有者数の指定やガイドライン化などを行っていく事で、国内外にも国際的に通用するセキュリティ立国を目指すという姿勢をアピールできるのではないかと考えます。この点についても是非とも検討していただける事を期待します。

(意見11－1)

該当箇所	P9　第2章第1節　対策実施主体の役割と連携 P12　第2章第2節(3)　情報関連事業者･情報関連非営利組織 P19　第3章第1節(3)①　企業の情報セキュリティ対策が市場評価に繋がる環境の整備 P19　第3章第1節(3)②　質の高い情報セキュリティ関連製品およびサービスの提供促進

意見内容	対策実施主体が製品･サービスの安全･安心に対する適切な評価を行い、対価を認めるという文化を醸成する必要があることを明記すべきである。
理　由	情報関連業者がより安全･安心な製品･サービスを適切な時期と価格で提供できるよう努力する必要があることは間違いないが、同時に製品･サービスの利用者側が、提供側の努力に対して価値を認めるという関係が構築されない限り、結局はコスト重視の製品･サービスの提供、選択へ流れてしまい、万一問題が発生した場合の結果責任だけが製品･サービスの提供者に問われるということが懸念される。発注者側も安易に低価格の製品･サービスに飛びつかず、安全･安心の観点からそれらのセキュリティレベル、価格などを見極めて発注すべきである。 長期的に見れば安全･安心なサービスの提供が国際的競争力の向上に繋がると言う論には賛同するが、短･中期的には市場原理だけで安全･安心の向上を期待することは難しく、対策実施主体における評価を認める文化の醸成が必要である。

(意見11－2)

該当箇所	P13　第2章第2節(4)メディア
意見内容	メディアが情報セキュリティ、IT、関連法規等に関する正しい理解をした上で報道する必要があることを明記すべきである。
理　由	昨今、様々なIT障害、個人情報漏洩についてメディアで取り上げられる機会が増えたが、必ずしも正しい理解をされずに報道されているケースが見受けられる。IT社会やITベンダに対する不安や不信を必要以上にあおることによって国民の理解が偏ったものになる可能性を否定できないことから、IT製品、情報システムの特性や利用環境等を正しく理解した上での報道を心がけるよう記述に加えるべきである。

(意見11－3)

該当箇所	P15　第3章第1節(1)ア③ 中期的なセキュリティ対策の強化･検討
意見内容	今後3年間の重要な取り組み項目として、暗号アルゴリズムの2010年問題(注)への取り組みを追記すべきである。 (注) http://www.imes.boj.or.jp/japanese/jdps/2005/05-J-22.pdf

理　由	セキュリティ政策の中でも暗号政策は極めて重要なものであると考える。特に現在様々なシステムで利用されている暗号アルゴリズムが2010年以降危殆化する可能性があることは、情報関連業者にとっても対策実施主体にとっても今から対策を検討しておく必要がある重大な課題である。

（意見11－4）

該当箇所	P16　第3章第1節（1）イ②情報セキュリティ監査実施の推進
意見内容	各地方公共団体の監査結果をしかるべき機関に登録し、対策レベルの比較、評価、目標設定などができるようにすることを追記すべきである。
理　由	総務省が地方公共団体向けの情報セキュリティ管理基準を公表し、監査の推進を行っているが普及には至っていない。 推進スピードをいっそう高めるためには、横並びの評価や目標設定などが住民にも目に見える形で環境整備を図ることが必要である。登録機関としては、例えば本基本計画に示されている「自治体情報共有・分析センター」（仮称）が考えられる。

（意見11－5）

該当箇所	P17　第3章第1節（2）重要インフラ
意見内容	「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」とあるが、目標に掲げる表現としては不適切であると考える。

理　由	IT障害という定義は本基本計画ではなされていないが、『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」策定にあたっての指針（案）』によれば、操作ミスや天災なども含まれていると判断できる。 これらに起因するIT障害の発生を限りなくゼロにすることは難しく、経済産業省から出されてる情報セキュリティ総合戦略でも「事故前提社会」が謳われており、本基本計画でも「事業継続計画」の重要性が述べられている。 重要なことは「重要インフラにIT障害が発生しても、国民生活に大きな影響を与えるようなサービス中断の発生を限りなくゼロにすること」であると考える。

（意見11－6）

該当箇所	P19　第3章第1節（3）① 企業の情報セキュリティ対策が市場評価に繋がる環境の整備
意見内容	政府調達の競争入札で情報セキュリティ対策レベルの評価を入札条件にする旨の記載があるが、評価する側、される側の準備状況を十分踏まえた上での実施とすべきである。
理　由	今後3年間の重点政策ということではあるが、セキュリティ人材の慢性的な不足から、その準備には相応の時間を要する。例えば、情報関連事業者の中でもＣＣ：Common Criteria（ＩＳＯ１５４０８）に精通し、ＳＴ：Security Target やＰＰ：Protection Profile を定義できる人数はごく少数である。まずはビジネス環境の整備、人材育成が急務であると考える。また、第三者評価は重要なことであると考えるが、昨今建築業界においても問題となっているように、評価が形式的なものになり重大な見過ごしが生じないよう、評価機関や審査員の育成、評価についても十分時間をかけて準備すべきである。

（意見12）

該当箇所	第4章　　今後３年間に取り組む重点施策－「新しい官民連携モデル」の構築 第3節　　横断的な情報セキュリティ基盤の作成 （2）　　情報セキュリティ人材の育成・確保 および、 （3）　　国際連携・協調の推進
意見内容	情報セキュリティ人材の育成・確保に関して、以下の内容を追加することを検討頂きたいと存じます。 ● 国際的に通用する情報セキュリティ技術および知識を有する人材の育成と確保の重要性および必要性 ● 資格制度の体系化における国際連携・強調の重要性および必要性

理　由	情報セキュリティ人材の不足が叫ばれて久しい昨今ではございますが、当基本計画を皮切りに、人材の育成に拍車が掛かることは重要且つ必然的な流れかと存じます。 該当箇所に記載されておりますとおり、人材の育成は急務であると認識しておりますが、当該問題の解決に当たっては日本国内のみならず、世界的な国際協調も重要なポイントであることから、世界的にも通用するような育成プログラムおよび資格制度を導入する必要性があるかと存じます。 また、わが国の人材育成プログラムが国際的にも認知されることによって、世界的な基準からも安心･安全な国家ということをアピールすることができ、ひいては各国間における影響力･波及効果があるかと存じます。 なお、当然ではございますが、これらの考え方に対する基盤として、昨今の情報セキュリティ犯罪、各国間における問題解決手法やその対策などのボーダレス化の問題が根底にあることは言うまでもございません。 さらに、世界的に認知されるプログラムの導入とすることによって、人材のスキル基準が明確となり、国際交流をも円滑にすることができると考えております。 これらの現状や課題、それに対する効果などをかんがみ、国際的に通用する人材育成･確保に関する検討は必須であることから、当該基本計画においても、検討して頂ければ幸いでございます。

(意見13－1)

該当箇所	第2章第1節(3)企業、(4)個人、第2節(2)教育機関･研究機関 第3章第1節(1)政府機関･地方公共団体　イ地方公共団体、(3)企業
意見内容	「情報モラル」の普及啓発、および教育の強化推進 本計画の第2章第2節で指摘されているように、個人が老若男女を問わず情報セキュリティに関するリテラシーを向上させていくことが必要であり、そのためには初等教育で、また世代横断的にも、情報セキュリティ教育を推進していくことが重要と考えられる。 さらに、本計画の第2章第1節(3)で指摘されているように、企業は、IT 社会を構成する一員としての立場から、情報セキュリティ対策に取り組む責任があるが、その際には、情報セキュリティ人材の確保･育成とならんで、社員全体の意識啓発が重要なテーマだと考えられる。 そこで、個人、教育機関、児童生徒、また企業における情報セキュリティ教育の強化推進にあたって、人的な側面、とくに意識面に重点を置いた「情報モラル」普及啓発事業の本格的な導入･推進を提案したい。 具体的な事業項目を以下に挙げる。 ・ 小学校、中学校の教員、及び児童･生徒の保護者に対する情報セキュリティ及び情報モラル研修についての支援 ・ 初等中等教育の授業カリキュラムに情報セキュリティ及び情報モラルの授業導入

	・　地域住民に向けた情報モラルの広報啓発や情報発信事業 ・　企業を対象とする情報モラルの広報啓発や情報発信事業 ・　情報モラルに関する人材育成の支援事業
理　由	昨今頻発している情報セキュリティ事故については、技術的な問題だけではなく、人的ミス（単純な操作ミス、判断ミス）や倫理観・道徳観の欠如などに起因している面が数多く見受けられる。本基本計画が目指す情報セキュリティ先進国となるためには、こうした問題にも対応できうる情報モラル教育が重要と考えられる。ここであえて「モラル」を主張するのは、技術、法律、制度、内部統治などの形式的外部的要件の整備だけでなく、意識、倫理など人間の内面的な部分に働きかける教育や取り組みが必要かつ有効と考えるからである。 情報社会において、新しい官民連携モデルを構築していくにあたっても、人と人のインターフェースをより柔軟にするためにも、根底には情報モラルが必要であると考えられる。IT 社会が進行発展するにつれて、小学校や中学校における児童生徒のネット利用の現状は、事件が起きるまで見えにくいものとなっている。特に最近は携帯電話の普及率が急速に高まっており、学校はもとより家庭でも把握できない状況となっている。2004 年におきた長崎の女児殺傷事件をはじめ、子どもたちの間で起きている掲示板への誹謗中傷の書き込みなどの問題に対しては、その場かぎりでない、継続的・体系的な情報モラル教育が必要である。 こうした背景から、情報を取り扱う際に必要な考え方や態度＝「情報モラル」を、小さいうちから身につけることは必須である。また、こうした情報モラル・情報セキュリティについての知識と意識は、成人にも学習する場がきわめて少ない。時代の変化によって変わりうる情報モラルや情報セキュリティについての教育が必須と考えられる。 また、企業がITを活用して情報を扱う際にも、顧客や取引先、従業員など、やり取りする相手の権利や安全を損なうことのないように配慮することが必須である。安全や人権、社会的公正への配慮が、情報社会で企業に求められる情報モラルであり、情報セキュリティ教育の推進と同時に企業の個々人、さらには、企業が組織として確立すべきものであると考えられる。 当研究所では、従来より教育現場における情報モラルの調査研究と普及啓発活動に取り組んできたが、その延長で、2003 年度からは中小企業庁の委託により全国的に企業を対象とした「情報モラル」セミナーの開催、パンフレット作成、ビデオ製作など、情報モラルの普及啓発事業に取り組んできた。（別紙資料 1 および資料 2 参照） こうした当研究所のこれまでの経験と、それを踏まえた研究と考察によって、この情報モラルの啓発は、教育現場のみならず、企業や家庭、地域も含めて、一般個人が自分では知らないうちに加害者になってしまうという現在の課題に対して、十分効

	果的な対策になりうると確信するものである。 さらに、情報社会において企業が問われる社会的責任の一つとしても、情報モラルの確立への取り組みは必要であり、こうした内容についての普及啓発は、社会から信頼を得る企業の育成のためにも重要と考え、あえて提案するものである。

（意見13－2）

該当箇所	第3章第1節　対策実施4領域における情報セキュリティ対策の強化 (1) 政府機関・地方公共団体、(2) 重要インフラ、(3) 企業、(4) 個人
意見内容	「地域情報セキュリティセンター（仮称）」の創設 本基本計画の根本テーマとして提唱されているように、新しい官民連携モデルの構築は、これからの情報セキュリティ対策でもっとも必要なことと考えられる。また対策実施4領域における強化も非常に重要と考えられる。 しかし、これまで情報化を推進してきたなかで、地域における情報格差（デジタルデバイド）問題は常に顕在化し、いまだに解消されていない問題である。情報セキュリティにおいても、同様に地域における格差が存在し、今後より拡大するおそれがあると考えられる。 そこで、標題のように、地域における情報セキュリティ施策推進の中心機関として、「地域情報セキュリティセンター」を官民連携のもとに創設・運用することが、情報セキュリティ分野における地域格差の増大を食い止め、地域社会においてもっとも安全で安心なIT利用環境の形成に資する施策と考えられ、提案するものである。 このセンターの主な機能は、情報セキュリティ推進に関する意識啓発、PDCAサイクルの構築・推進、横断的な情報交換・調整、技術指導、人材育成などである。また、当研究所が別途提案する「IT安心安全ネットワーク構想」の推進母体ないし支持母体となることも期待される。 このセンターは、基本計画に提唱されている「自治体情報共有・分析センター」と連携することで、広範囲に自律的な機能と役割を果たすことが可能になると考えられる。 実際には、県、市町村、重要インフラサービス機関、企業、ISP、メディア、NPO、大学、研究機関などが連携している協議会などがすでに存在していれば、それを利用、発展させることも考えられる。 日本の各地域には、上記のような連携組織があるところも多いと思われる。また、たとえば奈良県においては、「NPO法人なら情報セキュリティ総合研究所」が存在し、「情報セキュリティサミット」を毎年開催、県や地域の財団などとも連携して取り組みを進めている。兵庫県においては、県主導で、米国カーネギーメロン大学の情報セキュリティ専門大学院を開設している。

	また、当研究所は、中小企業庁より委託を受け「情報モラル」セミナーを全国各地で開催してきたが、その経験からも、地域において連携の中心となりえる機関、団体は必ず存在しているといえる。 よって、自治体情報共有・分析センターを中心にしつつ、これらの取り組みの延長上に、国の施策として「地域情報セキュリティセンター」位置づけ、その創設と全国的な組織化・連携の推進を図ることが望ましいし、かつ実現可能と考え、提案するものである。
理　由	・基本計画においては、「自治体情報共有・分析センター」が提唱されているが、一読した限りにおいては、あくまで行政内部のセキュリティ対策の推進・連携機関であり、民間企業や非営利部門も含めた地域全体に発生する各種のセキュリティ問題全般への対応・施策推進の中心機関という位置づけではないと思われる。 個人情報保護法施行の際にもみられたが、国の各省庁からは、それぞれ分野別、個別に指導・指示がなされる例が多く、国レベルであれば効率的である「縦割り」も、こと地方・地域においては、いずれにしても限られた人員での対応が迫られ、必ずしも有効ではないという問題がある。この問題の克服は、確固たる情報セキュリティ基盤を形成するためにはきわめて重要と考えられる。 しかしながら、現在の基本計画においては、地域において、具体的に、分野・組織を横断した連携・セキュリティ基盤の施策は、必ずしも明確には打ち出されていないと考えられる。 中央・大都市であれば可能な、企業、個人における自発的取り組み、自己責任による取り組みも、人的、経済的資源において劣っている地域では必ずしも十分に実現できるとはいえない現状がある。こうした点について、基本計画では十分な施策が打ち出されておらず、このままでは、地方公共団体がそれぞれ独自ないしバラバラに取り組みを進める可能性も強い。しかし、地方においても隣接する自治体、地域同士がネットワークでは直接接続され、セキュリティ環境の面からも、一定以上の水準で整備されていることが望ましい。 現在、大分においては、以下のような連携組織がある。こうした機関を発展させることで、情報セキュリティ対策のための人的ネットワーク、技術的ネットワークを確立して、セキュリティ事故に対する予防や実際に起きた際に被害が広がらないような仕組みや対応などが検討できる。 ・　大分県情報教育研究会 ・　大分県ISP協議会 ・　防災情報ネットワーク研究会 ・　豊の国IX研究会 当研究所は、これらの仕組みのいくつかにおいては事務局などの機能を果たしており、実際にこうした連携組織を利用して、個人が負担感なく情報関連製品・サービスを利用できる環境整備を行った事例もある。（別紙資料３参照） ただし、地域情報セキュリティセンターが県単位に一箇所必要かどうかは、各地域の実態に即して慎重に検討する必要がある。連携と協働の実現には、現実的には多くの労力と調整能力が必要であり、また情報セキュリティに関する人材が地域にそ

	れほど多くいるとは思われないため、ブロック（たとえば九州地域ブロックとか）ごとぐらいが適当ではないかとも考えられる。

（意見１３－３）

該当箇所	第１章第１節（１）　⑤「情報セキュリティ先進国」の実現 同（３）現在の課題と解決の方向性－「新しい官民連携モデル」の構築へ－　②「情報セキュリティ先進国の実現 同（４）連携・協調の推進 第３章第２節（３）国際連携・協調の推進
意見内容	国際連携・協調の推進に際しても、我が国として「新しい官民の連携モデル」を基軸に進めるべきであると考える。とくに「政策研究」における連携・協調を深めることに注力する必要があると考えられる。 　その場合、アジア太平洋の近隣諸国との協調活動を重視すべきであり、ODA 活動の一環として、途上国政府の情報セキュリティ担当者に対する育成支援活動の実施も必要である。 　国際連携・協調推進のために、我が国が主導して「情報セキュリティ研究国際ネットワーク（仮）」を設置し、主要な研究機関による相互交流を推進することを提案したい。同ネットワークの具体的な活動としては、以下が考えられる。 ・　各国政府の政策担当者、法律、国際政治、経済、情報技術などの専門研究者、企業の戦略・実務担当者による国際会議の開催 ・　情報セキュリティ関連政策データベースの創設、運用 ・　途上国政府担当者を対象とした政策形成支援プログラムの実施

理　由	情報セキュリティに関しては、国連主催の世界情報通信サミット(WSIS)において議論された「インターネットガバナンス」の主要テーマの一つであり、グローバルな観点から各国が連携して取り組みを推進することの必要性が確認されている。WSIS では、インターネットガバナンスに関して継続的に協議する「フォーラム」の設置が合意され、現在その準備活動が始まろうとしているが、このフォーラムは政府、企業、市民社会が対等に参加する、いわゆる「マルチステークホルダー」で構成され、活動が進められることで合意された。本基本計画が提唱する「新しい官民の連携モデル」は、グローバルに合意された、この「マルチステークホルダー」アプローチと軌を一にするものとする必要がある。 ここで、学術・政策研究者は、「市民社会」の重要な構成員であり、政策研究の推進は、「マルチステークホルダー」での取り組みを具体的に進めるものといえる。 しかしながら、情報セキュリティに関する学術研究の推進状況をみると、技術面での研究開発の取り組みは進んでいる一方、社会システム・社会学的な観点からの取り組みは、我が国においても、またグローバルにみても、技術の進歩状況と比較しておおきく立ち遅れている現状がある。 社会学的観点から情報セキュリティの政策研究に関する国際的連携・交流を推進し、各国の取り組み実態を明らかにし、相互理解を深化させ、国際的な人材の育成に資することは、政府における関連政策の立案・策定・実施過程を知的、社会的な意味で支援するもので、国際的なハーモナイゼーションを含めた、実際に有効な政策の形成・実現に寄与するところが大きい。また、企業関係者の参加は、民間部門、一般社会における現実の状況に即した施策の立案、実施に資するものと考えられる。 こうして、我が国が中心となって、アジア太平洋の近隣諸国（米国、韓国、シンガポール、オーストラリア、中国など）に対して、政策研究の推進・交流を提唱することで、政策研究分野における我が国のリーダーシップを発揮することが可能となり、本基本計画が再三にわたって提唱している「ジャパンモデル」を具体的に推進するための有力な手段となると考えられる。とくに我が国は、一方で欧米諸国との協調の実績、信頼があると同時に、他方では、ＡＰＮＧや APCERT など、セキュリティ分野を含めたインターネットの普及推進においてアジア諸国との協調・支援活動での実績を有し、異なる状況をもつ欧米とアジア諸国の橋渡し役を果たすことができる戦略的な位置にある。 また、途上国の政策担当者への支援活動は、セキュリティの水準はもっとも弱いレベルで規定されること、インターネットがグローバルに相互接続されるなか、サイバーテロやスパム、フィッシングなどの犯罪、障害の起源が必ずしも先進国に限定されるものではないなどの現状を踏まえ、こうした脅威に対応するための環境を国際的に整備する上で、有効かつ必要な方策であり、かつ「ジャパンモデル」の推進・普及にとって意義があると考えられるものである。

（意見13－4）

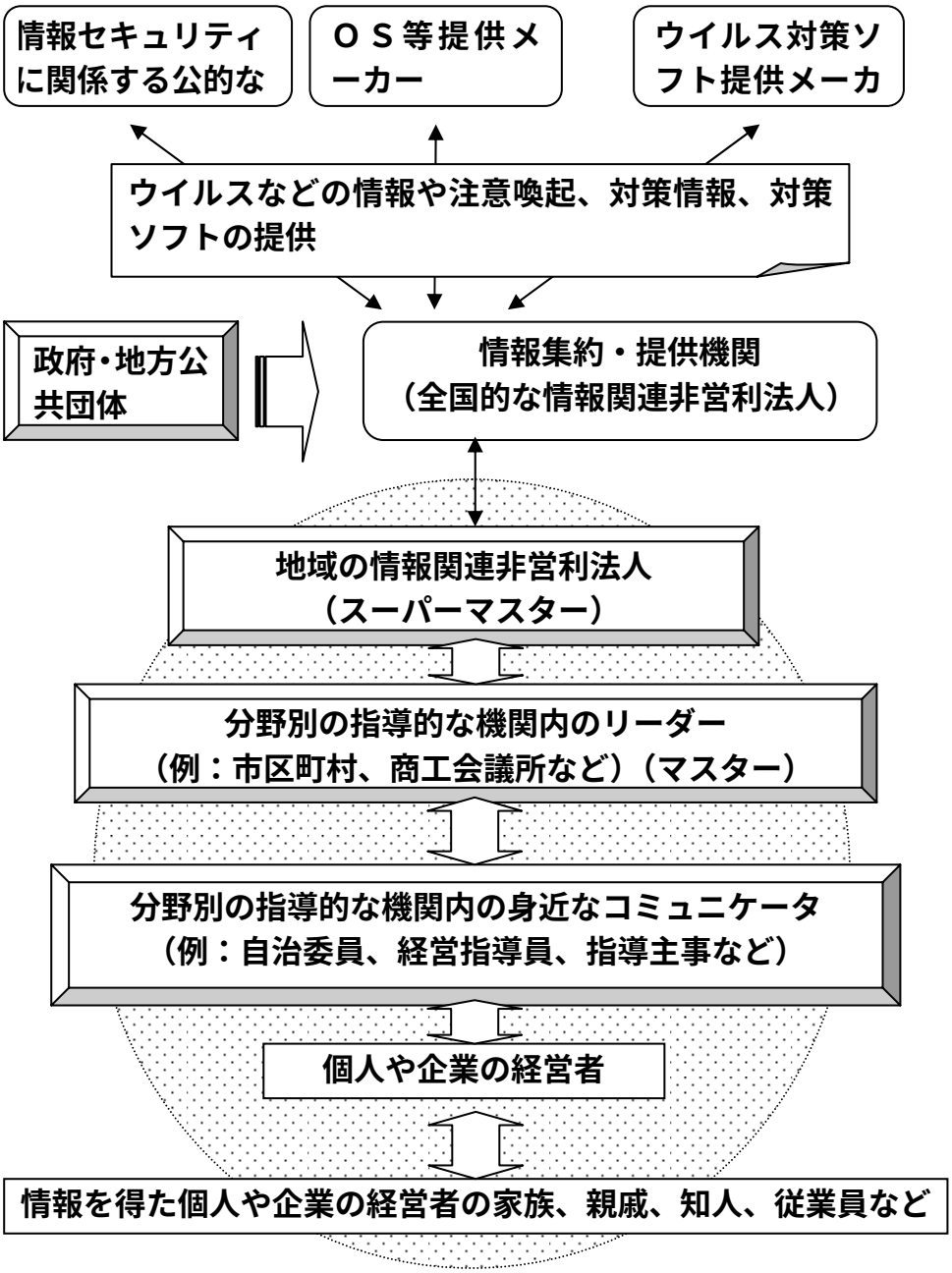
該当箇所	第3章第1節(1)政府機関･地方公共団体、(3)企業、(4)個人
意見内容	「ITを安心して利用できる環境」を全国的に構築する上で、地方、地域で、企業とりわけ中小企業や個人に対する施策を進める際には、専門家に限らず、一般利用者、普通の個人にわかりやすいセキュリティ情報の提供、意識啓発が必要である。 そのためには、情報関連の非営利組織(NPO)の活用が効果的である。 具体的には、全国的な情報関連NPOをセキュリティ関連情報の集約･提供機関と位置づけ、これと地域毎に存在する情報関連 NPO とが相互に連携を図り、情報提供･啓発活動を推進するというものである。ただし、その実現にあたっては、政府機関･地方公共団体の財政的な支援や連携が不可欠である。 地域の情報関連 NPO は、地方公共団体や商工会議所、農協のような地域における分野別の指導的な機関と連携して、住民に密着した形でセキュリティ情報を伝えることができるコミュニケーター役を務めることで、IT を安心して利用、活用できる環境の形成が可能となる。 このように「IT安心･安全ネットワーク」の構築をいわば「ヒューマンネットワーク」として推進することで、地域におけるすべての個人や企業に対して情報セキュリティに関する情報を確実に伝達･浸透させることが可能になる。

理　由	本基本計画は、全体的には国・中央・大都市・先進企業の観点を中心に策定され、地方・地域の実態が十分反映されていない印象が強い。 地方においては、行政、企業ともに情報セキュリティに関する問題意識が大都市、中央に比べて立ち遅れており、取り組みを推進するための人的・経済的資源の面でもハンディがあることは否定できない。 これは、個人においても同様であり、「個人の自己責任」を強調するだけでは、地方の都市や農村、過疎地域などの生活者にまでセキュリティ意識を浸透させていくことは困難である。 当研究所では、ITが国民生活・社会経済活動において不可欠なものになる、という考えから、情報セキュリティも含めて、地域における IT 普及推進の実践活動に携わってきたが、その経験に即して、上記提案を行うものである。 当研究所では、地域における IT 普及支援活動の一例として、大分県より委託を受け、県民からの IT 全般に関する質問・相談を電話で受け付ける、「IT サポートセンター」を実施・運用してきた。 また、ITを活用する機会が少ない高齢者、障害者、育児中の主婦などを対象にして 2003 年から、マイクロソフト社が支援するＵＰプログラムにいち早く取り組んできた。http://www.microsoft.com/japan/mscorp/citizenship/ca/up/ さらに、高齢者による自発的な IT 利用教育に取り組んできたＮＰＯ「シニアネット大分」に対しても、場所的、人的支援を行ってきた。 http://www.oct-net.ne.jp/~sno-oita/ これらの活動を通じて、高齢者や障害者などがITを活用することにより、よりよい生活の実現の可能性があることがわかった。その反面、情報セキュリティに関しては、「関心がない」、「関連の電子メールやお知らせは読んでも意味がわからない」、「フィッシングなどネット詐欺が多いので直接知っている人からの情報しか信じない」、という状況が一般的で、全般に意識がきわめて低いこともわかった。 （なお、これについては、大分市の協力を得て、同市が実施しているIT初心者講座でアンケートを実施中である。2006 年 3 月集計予定。 別紙資料４参照） 当研究所が提案する「IT安心・安全ネットワーク」は、急速に増えているIT初心者や、電子商取引の普及によりITを導入せざるをえない中小企業、とりわけ零細企業者を対象にして、ヒューマンネットワークをベースにして、情報セキュリティに関する情報を伝達する仕組みである。

	以下に提案の具体的な内容を簡単に説明する。 このネットワークは、情報の伝達者と被伝達者が、お互いに顔が見えるヒューマンネットワークを基礎とするところに特徴がある。 参考にしたのは、民生委員の制度であるが、「スーパーマスター」、「マスター」、「コミュニケーター」と 3 層にわたる人員を配置し、人材の育成、情報の円滑な伝達を可能とする仕組みである。 ・情報集約・提供機関（全国に 1 カ所） 全国的に活動が可能な情報関連 NPO が情報の集約・提供を担当する。情報セキュリティ関係の情報をもちろん、著作権などの情報モラルに関する情報も集約し、初心者にもわかるコンテンツにしてホームページに掲載したり、地域の情報関連 NPO へのタイムリーな情報発信、情報セキュリティの人材育成研修の実施、質疑対応なども行う。 ・地域の情報関連 NPO（都道府県に 1 団体程度） ■スーパーマスター：情報集約・提供機関から情報を得て、都道府県内の各分野の団体に情報を伝える。また、各分野のリーダー育成研修を行うほか、質疑対応を行う。 ・各分野の指導的機関（市町村、商工関係指導団体など） ■マスター：各分野の指導的機関内のリーダーであり、スーパーマスターから情報を得て、コミュニケーターに情報を伝える。また、コミュニケーターからの質疑対応を行う。 ■コミュニケーター（例：町内会の自治委員、経営指導員など） マスターから情報を得て、担当する個人や企業の経営者などに情報を伝える。また、個人などからの質疑対応を行う。コミュニケーターは、情報セキュリティに関する特別な知識を持つ必要はなく、マスターからの情報を印刷して、確実に伝える役割を持つ。 なお、以上の仕組みは、2006 年 4 月から大分県ほか全国数カ所で実証実験として稼働する予定であるが、本基本計画においても、こうした仕組みを採用し、全国的な普及を推進することが望ましいと考えて提案するものである。

地域 IT 安心安全ネットワーク構想

（イメージ図）



（意見14－1）

該当箇所	第1章　第1節　（1）　⑤　4ページ
意見内容	セキュリティ立国となることに加えて、海外諸国への情報提供や指導等も踏まえたリーダー的な役割を担うことも必要である。
理　　由	国境のないIT世界で情報セキュリティを確立するためには、関連諸国に対しても、セキュリティの底上げを指導したりする必要があるため

（意見14－2）

該当箇所	第3章　15ページ
意見内容	政府機関の中長期的なセキュリティ対策強化で（イ）セキュリティ強化のシステム導入が述べられていますが、システムと同時にそれを利用する人間についての管理のあり方についても検討していただきたい
理　　由	内部でも悪意を持つ、もしくはシステムを適切に利用する意識の薄い人間がいることを想定し、システムログイン後のトレーサビリティやモラル向上のための統一規範の確立などをあわせて検討することで、バランスの取れたシステム導入となることが期待できるため

（意見14－3）

該当箇所	第3章　第1節　(1)政府機関･地方公共団体　ア政府機関　①政府機関統一基準とそれに基づく評価･勧告によるPDCAサイクルの構築 15ページ
意見内容	「外部委託先の情報セキュリティ対策の水準の確保」については、ISMS　適合性評価制度に基づく認証の取得など、情報セキュリティの実現に係る企業の自主的な取り組みが尊重されるような運用として頂きたい。
理　　由	情報セキュリティ対策に係るコストが、いたずらに増加することを避けるため。

（意見14－4）

該当箇所	第3章　16ページ

意見内容	第3章－今後3年間に取組む重点政策－「新しい官民連携モデル」の構築における主体の領域を①政府機関、地方公共団体、②重要インフラ、③企業、④個人の4領域に分けて具体的な対策のあり方が述べられているが、ア.政府機関に比べて、イ.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役割が明確ではなく、注釈が必要である。
理　由	政府機関統一基準については、情報セキュリティ政策会議が決定し、それに基づき評価・勧告されるということで、その役割が明確になっているが、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については、どういう役割があるのか不明であるため。

（意見14－5）

該当箇所	第3章　17ページ
意見内容	各地方公共団体が講じる情報セキュリティ対策について、その実効性の評価・見直しによって継続的な対策レベルを向上させるため、情報セキュリティ監査だけでなく、政府機関と同様な仕組みとして、情報セキュリティマネジメントを構築し、PDCA サイクルに基づく個々のプロセスが確実に実施される仕組みが必要である。
理　由	政府機関と同様に、地方公共団体としての情報セキュリティ対策レベルを向上させるための仕組みを確立するため。

（意見14－6）

該当箇所	第3章　17ページ
意見内容	イ.地方公共団体の職員の研修等の支援によるセキュリティ強化だけでなく、政府機関と同様に情報セキュリティ対策業務に携わる専門的職員については、全員が情報セキュリティに関する資格を保有することを目指す必要がある。
理　由	地方公共団体のセキュリティ強化を図るためには、研修等の支援だけでなく、政府機関と同様、地方公共団体の専門的職員にも何らかの情報セキュリティに関する資格を保有させ、我が国の中央・地方政府機関が情報セキュリティ対策を一体的に進める必要があるため。

（意見14－7）

該当箇所	第3章　17ページ

意見内容	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」の策定については、重要インフラ事業分野ごとの自主性に任せるのではなく、政府主体の第三者評価制度等により検査・評価を行うことも視野に入れる。
理　由	重要インフラの情報セキュリティ対策に係る行動計画の実効性を確保するとともに、「安全基準等」の改善に結びつけるため。

（意見14－8）

該当箇所	第3章　19ページ
意見内容	企業における質の高い情報セキュリティ関連製品及びサービスの提供促進については、第三者評価の活用を推進することが期待できる。このため、質の高い情報セキュリティ関連製品だけでなく、サービスの提供も含め、第三者評価の結果等を活用する企業に対してインセンティブが与えられる環境を整備する必要がある。
理　由	質の高いサービスを提供する企業についても、何らかのインセンティブを与えることが、全体としての情報セキュリティの向上につながるため。

（意見14－9）

該当箇所	第4章　23ページ
意見内容	(4)①サイバー犯罪 については、「国際間の政治的情勢等を考慮した、サイバー攻撃情報を発信する体制を強化する。」を追加する。
理　由	政治的情勢に起因する海外からのサイバー攻撃（例えば、外交により不利益を感じた諸国がわが国に対して行う攻撃等）が増加している事実に鑑み、それらを未然に防ぐ、またはそれらの攻撃に事前に備えるため、相互に警告を発する必要がある

（意見14－10）

該当箇所	第4章　24ページ
意見内容	適正な資源配分を行うという観点から、力量のある民間人に復旧作業を速やかに行うための特権（安全確認ができている災害現場に入れる）等を付与し、その力量を十分に活用できるような枠組みを作る。

理　由	災害等に際しては、ある程度災害が沈静化しても、優秀な人材を有している民間組織などは立ち入ることができず、結果として復旧作業に遅延が生じることがある。したがって、事業継続を維持するためにある程度の「特権」を民間人にも付与することが重要と思われる。（医者の権限等をイメージしている）

（意見15）

該当箇所	第2章「新しい官民連携モデル」の構築における各主体の役割と連携
意見内容	コンピュータ脆弱性やサイバーテロに関する官民連携だけでなく、P2P 等による情報漏洩対策も官民連携のテーマとしてとりあげるべき
理　由	WINNY に代表される P2P ネットワーク上での情報流出事故は今後も続くと思われ、ウイルス感染による流出データは1TB 以上になっている（独自調査結果）。流出当事者は流出の事実を知らず、所属する企業や自治体も機密情報が世界中に半永久的に流出し続けていることに気づいていない。一企業で WINNY のダウンロード解析を行っている場合、他社情報を見つけても、通知するルールがなく、逆に不正利用している疑いをかけられる懸念もある。また、日本企業の機密情報が海外企業、国際テロ等に悪用される懸念もある。公平な第三者組織が WINNY 等 P2P ネットワークデータをダウンロード分析し、流出元へ通知する仕組みが必要と思われる。また、該当データをキャッシュしている PC から削除する仕組みの開発も望まれる。コンピュータ脆弱性だけでなく情報漏洩事故に対する官民連携モデルの確立が望まれる。

（意見16－1）

該当箇所	P15　①政府機関統一基準とそれに基づく評価・勧告による PDCA サイクルの構築
意見内容	以下の文章を追加すべきと考えます。（下線部は追加事項） 政府機関の情報セキュリティ対策の水準を世界最高のものとするため、政府機関統一基準について、技術や環境の変化を踏まえ、毎年その見直しを行うものとする。また、各政府機関の情報セキュリティ対策の実施状況を、政府機関統一基準に基づき、必要な範囲で検査・評価しその達成状況を公開するとともに、勧告を通じた各政府機関の対策の改善と政府機関統一基準等の改善に結びつけることで、政府全体としての PDCA サイクル（Plan・Do・Check・Actサイクル）を確立する。

理由	政府機関の情報セキュリティ対策は、地方公共団体、重要インフラ事業者、一般企業等の他の組織の規範となるべきものですが、達成状況を公表することで、どの政府機関を規範とすべきかがわかります。なお、米国においても政府機関の達成状況は問題なく公表されていますので、我が国においても公表は可能と考えます。

（意見16－2）

該当箇所	P16　①情報セキュリティ確保に係るガイドラインの見直し等
意見内容	以下の文章を追加すべきと考えます。（下線部は追加事項） 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等を行うとともに、各地方公共団体における当該ガイドライン等を踏まえた対策の実施を推進する。 特に、当該ガイドラインには、政府機関統一基準に準じた情報セキュリティ対策を盛り込んだ上で、これに基づき必要な範囲で検査・評価・勧告を行い、地方公共団体の情報セキュリティ確保に結びつける。
理　由	地方公共団体は、政府機関以上に国民に密着した行政サービスを行っており、情報セキュリティの確保は最重要事項であると考えます。現在、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が行われているようですが、当該ガイドラインにおいては、対策項目の達成水準を具体的に示し、評価・検証可能なようにすべきであると考えます。その際、政府機関統一基準との整合性は我が国の行政サービス全体の向上の観点から非常に重要であると考えますので、当該ガイドラインについては、政府統一機関基準に照らしながら具体的に示すべきであると考えます。

（意見16－3）

該当箇所	P17　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
意見内容	以下の文章を追加すべきと考えます。（下線部は追加事項） 「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』策定にあたっての指針」を踏まえ、それぞれの重要インフラ事業分野ごとに、必要な又は望ましい情報セキュリティ対策の水準について。「安全基準等」に明示することを目標とする。 特に、当該「安全基準等」には、政府機関統一基準に準じた情報セキュリティ対策を盛り込んだ上で、これに基づき必要な範囲で検査・評価・勧告を行い、重要インフラの情報セキュリティ確保に結びつける。 さらに、指針については1年ごと及び必要に応じて適時見直すこととし、「安全基準等」については、情報セキュリティを取り巻く環境の変化に応じ、随時見直しを行う。

理由	重要インフラは、直接、国民の生活に結びつくライフラインであり情報セキュリティの確保は最重要事項であると考えます。現在、重要インフラにおける「安全基準等」の策定が進められているようですが、それぞれの事業分野ごとの安全基準等において、指針に示された対策項目の達成水準を具体的に示し、評価・検証可能なようにすべきであると考えます。その際、政府機関統一基準との整合性は重要であると考えますので、「安全基準等」については、政府機関統一基準に照らしながら具体的に示すべきであると考えます。

（意見17）

該当箇所	P．16　イ　地方公共団体　②情報セキュリティ監査実施の推進
意見内容	地方公共団体の情報セキュリティ監査実施をスピードアップするため、実施した監査結果の所定項目についてしかるべき機関に登録することを義務付ける。これにより、地方公共団体相互に監査の有無、対策レベルの比較及び自己評価を可能にする。この登録機関として、「自治体情報共有・分析センター」（仮称）なども候補とする。
理　由	総務省では地方公共団体向けに情報セキュリティ管理基準を公表し、監査実施の推進を行っているが、これをスピードアップする手段として、監査結果の概要（所定の項目）についてしかるべき機関に登録することを義務付ける。このような情報共有化により、各々の地方公共団体相互に、監査の有無や講じた情報セキュリティ対策の実効性の比較・分析・見直し・自己評価等が可能になる。結果として、各地方公共団体で継続的な情報セキュリティ対策レベルの向上がいっそう促進されると考える。

（意見18－1）

該当箇所	第3章　　第１節　（1） 「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、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」
意見内容	統一基準を充足しているとみなすセキュリティ評価の仕方についても、課題として挙げるべきではないか。

理　由	例えば企業に対しては、第3章　第1節　(3)②　に「IT セキュリティ評価及び認証制度、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、情報セキュリティ監査といった第三者評価の活用を推進」、「また、こうした第三者評価の審査等の効率化を図る」と記載されている。政府機関 (上記「該当箇所」) においても、統一基準を充足しているとみなす評価の考え方、仕方について明確にすることが必要と考える。 また、リスクレベルが高い情報システムについては、より厳しい目で評価することも必要と考えられるので、このための評価の方法についても検討する必要がある、と考えます。

(意見18－2)

該当箇所	第3章　第 2 節 (1) ③「グランドチャレンジ型」研究開発・技術開発の推進 及び、第 3 章　第 2 節 (3) ②「情報セキュリティ領域での我が国発の国際貢献」
意見内容	セキュリティ評価基準及びその充足の評価方法についても、中長期的かつ国際的な視野で、より効率的かつ実効的な物を開発していくターゲットとすべきであると思われるが如何か。
理　由	既存のセキュリティ評価では必ずしも満たされていない効率的かつ実効的な評価方式 (セキュリティ評価基準自体のあり方を含む) を、中長期的かつ国際的な視野で検討していくことも必要である、と考える。

(意見19－1)

該当箇所	1 ページ「はじめに」の第 2 段落
意見内容	「これまでの無差別な攻撃から、特定の動機を持って、特定のサイトを狙った攻撃が顕在化してきている。行為者も組織化している。」といった内容の追加。
理　由	昨今のインシデントの状況を分析した結果、上記内容が傾向として見えてきている。背景を説明する際には、より近時の傾向を正確に伝えることが重要と思われるため。

（意見19－2）

該当箇所	7 ページ「(1) 官民各主体の共通認識」
意見内容	「共通認識」とは誰と誰の間の「共通認識」か不明確。
理　由	「共通認識」とは「官」と「民」の間での「相互理解」という意味か、または「官」は「官」、「民」は「民」の中、それぞれの内部での「共通認識」かが分かりづらいため。

（意見19－3）

該当箇所	7 ページ「(2) 先進的技術の追求」
意見内容	先進的技術だけでなく、「既存の仕様の再検討」も必要と思われる。
理　由	既存技術にも見直しの必要な点があるため。

（意見19－4）

該当箇所	10 ページ下から 3 行目
意見内容	「組織内 CSIRT (Computer Security Incident Response Team)構築の必要性」を加えて欲しい。
理　由	記載されている重要インフラに関する内容は、端的に表現すれば、「CSIRT の構築」と言い換えることが可能。「キーワード」として使用すると印象が強まると思われるため。

（意見19－5）

該当箇所	11 ページ「(4) 個人」

意見内容	「一般個人にとっては IT の仕組みは理解しがたい」というよりは、「便利で高度なシステムほど、ユーザから見るとブラックボックス化する傾向が著しい。ユーザは中身がどのような仕組で動いているかは意識しない。」というべきではないかと思われる。
理　由	「IT の仕組みは理解しがたい」だけでは具体性がなく実情を理解しづらいため。

（意見19－6）

該当箇所	12 ページ「(2) 教育機関・研究機関」
意見内容	「既存基盤技術の国際的な改訂に積極的に取り組む。」を加えるべき。
理　由	既に国際的に使われているインターネット基盤技術も、未だ未熟な段階であり、仕様レベルにおける脆弱性も発見されている状況にある。研究機関には、先進技術の追求の他、基盤技術の見直し、改定、運用の成熟化について国際的にも働きかけを行うことが、国際貢献につながることと考える。

（意見19－7）

該当箇所	12 ページ「(3) 情報関連事業者・情報関連非営利組織」
意見内容	情報関連非営利組織に期待されるポイントとして、「国際的な関連機関間の連携や活動に基づく、日本からの国際的な貢献」という点を追記してほしい。
理　由	例えば、情報関連非営利組織間の国際連携について、既に、アジア太平洋地域 CSIRT 連携体制（APCERT）等の実績があるため。

（意見19－8）

該当箇所	15 ページ「①政府機関統一基準とそれに基づく評価....の構築」
意見内容	各政府機関内に「組織内 CSIRT の構築」をすることを入れるべきではないか。

理　由	各政府機関の情報セキュリティ対策の実施をするにあたり、実施体制の構築を明記しておくことが必要と考える。

（意見19－9）

該当箇所	17 ページ「③自治体情報共有…創設促進」
意見内容	「政府等から提供される情報の共有等…」だけではなく、 脆弱性情報ポータルサイトである「JP Vendor Status Notes(JVN)」 などの、情報関連非営利組織が発信する脅威情報も加えるべきではないか。
理　由	既に運用されている民間情報発信の仕組みを活かすことを通じた、民間との連携についても、具体的に示すべきと思料する。

（意見19－10）

該当箇所	17 ページ「④職員の研修等の支援」
意見内容	『地方公共団体のセキュリティ強化を図る』実施主体が不明確
理　由	支援を実施するのは政府機関なのか、もしくは、民間（情報関連事業者・情報関連非営利組織）であるのか、どの実施主体が担うのかによって研修のためのカリキュラム等は異なるため。

（意見19－11）

該当箇所	18 ページの「④分野横断的な演習の実施」
意見内容	演習の実施内容の記述はあるが、当該演習の実施主体を組織内に構築する必要性について述べられていない。
理　由	演習はテーマ設定の変更等を行い、さまざまなケースを想定した定常的な実施が望ましい。このような定常的な開催の実現のために、当該演習のための体制を組織内に整備することが必要になるものと思料する。

（意見19－12）

該当箇所	23 ページ上「①国際的な安全・安心… への貢献」

意見内容	既に民間の情報関連非営利組織が行なってきた成果についても言及すべき。
理　由	情報関連非営利組織においては、既にさまざまな国際連携の取組みを実施してきている（前述）。これら成果も考慮すべきである。

（意見19－13）

該当箇所	23ページ「②情報セキュリティ領域での我が国発の国際貢献」
意見内容	情報関連非営利組織等が『日常的に』発信するサイバー関連脅威情報や分析情報、また、インシデント対応ポリシーや運用手順など非技術的な情報を、国内のみでなく海外にも同時に発信することも、重要な日本発の国際貢献と思料する。
理　由	先進技術や国際標準に係わる活動のみが国際貢献ではないと思料する。サイバー関連脅威情報や分析情報、また、インシデント対応ポリシーや運用手順などの非技術的な情報の海外への発信による貢献も求められている。

（意見19－14）

該当箇所	24ページ「(1) 内閣官房… (NISC) の強化」
意見内容	当該機構は、それぞれ固有の特性を有する10分野の重要インフラに係る対策も実施していくので、特に、各重要インフラ所管省庁の若手を集めて、将来の人材育成につなげていくことが必要と思料する。 また、各重要インフラ所管省庁の人材育成状況については、政策会議で議論すべきではないか。
理　由	民間でも人材は不足しており、政府機関の人材育成は非常に重要である。なかでも分野が多岐にわたる重要インフラについては、各重要インフラ所管省庁が積極的にNISCでの研修を行うべきと考える。

（意見19－15）

該当箇所	25ページ

意見内容	(短期間で)拙速に評価を下すことなく、中長期的なビジョンでの評価を願う。
理　由	本基本計画は、成果が短期間では認識しづらい内容のものが多いと思われるため。

(意見20－1)

該当箇所	第1章　第1節　(2)実現すべき基本目標 ①「ITを安心して利用可能な環境」の構築　p5 「以下の　3　つの条件が満足されている環境を構築することが求められている。1)予防、2)認識・体感、3)事業継続」
意見内容	「予防」「認識・体感」「事業継続」の3条件は、官民をとわず、情報システム、情報資産の保有主体が満足すべきものである、という認識を基本計画で明確に示したことは重要である。ただ、「情報セキュリティに絶対はなく、事故は起こりうるもの」という前提に立てば、第　3　章の目標設定に伺えるように予防に偏重するのでなく、予防/認識・体感/事業継続の　3　要素をバランスよく実行すべきであることをより明確に示すべき。
理　由	経済産業省の「情報セキュリティ総合戦略」に謳われているように、「情報セキュリティに絶対はなく、事故は起こりうるもの」である。また、「情報システムに対する新しい脅威の手段、方法は日々発展しており、すべての脅威から情報システム、情報資産を完全に守ることは不可能に近い」という認識は、ほぼ常識化していると考えられる。 一方、第3章で設定される目標「IT障害の発生を限りなくゼロにすること(重要インフラ)」、「リスクに応じた適切な対策を実施していること(企業)」からは、予防措置への偏重が伺える。「十分な予防対策」を敷くことは重要であるが、予防に専念する余り、万が一の備えがおろそかになってはいけない。すなわち、IT　事故発生時の被害極小化、事業継続の確保にも十分な対策が必要である。また、予防対策を手厚くすることは多大なコストがかかる。IT　事故予防のために過大なコストがかかってしまい、企業や公共事業体などの本来の活動が損なわれることがないよう、政府によりセキュリティ対策の望ましい基準を明示するなどの支援が期待される。

(意見20－2)

該当箇所	第2章　第2節　(3)情報関連事業者・情報関連非営利組織　P12 「なお、その際には、安全・安心なサービスの提供が、最終的には、その情報関連事業者の国際競争力の向上にも繋がるというプラスの視点を持つことも重要である」
意見内容	以下、「ただし、市場競争を通じて、国際的な規模でどのようなレベルの情報セキ

	ュリティが確保されるべきかについては、官民レベルでの国際的な対話を通じて明確にされていくことが期待される。」と付け加えるべき
理　由	安全･安心なサービスや製品を提供することは、情報関連事業者にとっての重要な役割と認識する。ただし、達成すべきレベルについては、提供対象の性格、コスト、提供タイミング、国内外の市場情勢等との兼ね合いもある。国際的な競争力向上のためには、これら事項を総合的に加味したコンセンサスの醸成が必要と考える。 市場競争において、「高価で安全なサービス」が「安全性は劣っても、便利で比較的廉価なサービス」よりも優位であるとは限らなかった過去の実例（PKI や個人認証サービスの事例）も想起されたい。

（意見２０－３）

該当箇所	第３章　第１節　(1)政府機関･地方公共団体　ア 政府機関　①政府機関統一基準とそれに基く評価･勧告による PDCA サイクルの構築　P15 「政府全体としての PDCA サイクルを確立する･･（中略）･･また、外部委託先の情報セキュリティ対策の水準の確保の観点についても、十分に留意する必要がある。」
意見内容	「政府全体としての PDCA サイクルを確立するとともに、セキュリティ監査などの仕組みを通じて、PDCA サイクルが有効に機能することを目指す」 「外部委託先の情報セキュリティ対策の水準の確保の観点についても、ベストプラクティスの普及を中心に十分に留意する必要がある。」と訂正すべき。
理　由	PDCA サイクルを確立することは情報セキュリティ確保にとって非常に重要だが、確立したサイクルが有効に機能していることを客観的に保証することも不可欠。例えば米国の場合は、FISMA（合衆国情報セキュリティマネジメント法）の枠組みで PDCA を確立しつつ、政府機関がその有効性をスコアという形で客観化し、PDCA が有効に機能していることの評価に役立っている 外部委託先の情報セキュリティ対策については、産業界でも監査等の手法の検討が進んでいる状況を考慮し、官民対話を通じた「ベストプラクティス」ベースでの実現が望ましい

（意見２０－４）

該当箇所	第３章　第１節　(2)重要インフラ　P17 「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」
意見内容	「IT 障害発生によるサービスの停止時間を限りなくゼロにすることを目指し」に訂正すべき
理　由	「情報セキュリティに絶対はなく、事故は起こりうるもの」であり、万が一事故が発生しても、事業継続措置により被害を極小化することが目標として妥当と考えられる

	((2)実現すべき基本目標　P5 へのコメント参照)

(意見20－5)

該当箇所	第 3 章　第 2 節　(1)情報セキュリティ技術戦略の推進　①研究開発･技術開発の効率的な実施体制の構築　P21 「投資効率の改善のため、成果利用までを見据えた研究開発･技術開発を実施するための体制を構築し、その成果を政府が活用することを前提とした新たな研究開発･技術開発に取組むこととする」
意見内容	「民間における研究開発成果の市場適合性の向上･促進を目的とし、政府は、民間を対象とするテスト･ベッドの提供を推進する」を追記。
理　由	情報セキュリティ実装にあたり、具体的に利用される技術は、政府支援により研究･開発されたものばかりではなく、民間で研究･開発されるものも多い。ただし、「安全性重視が競争力強化に繋がる市場環境がまだ形成されていない」という現状に対しては、第 2 章　第 2 節　(1)での記述「市場原理が働きにくい部分などには政府が主体的に関与する(p12)」の通りの支援が望ましい部分である。その際、政府機関への採用前提の援助といった直接支援手段のみならず、民間がある程度自由に検証や実証実験を行えるテストベッドの提供といった間接的な支援が合わせて実施されることが必要と考える。 また、「基本計画」でも「政府は、民間部門における取組みとの役割分担を明確にしつつ」(P21)と述べているとおり、民間での研究開発が、わが国の情報セキュリティ向上に果たす役割も大きいと考えられる。

(意見21)

該当箇所	P.7　第 2 節 (2) 先進的技術の追求
意見内容	IPv6の推進について賛同いたします。2010年前後にIPv4アドレスが枯渇すること、日本のIPv6の優位性の維持とそのビジネス展開への必要性なども踏まえ、国としてIPv6導入のための施策を戦略的かつ集中的に打っていくことが大事と考えます。

理　由	IPv6を用いることにより以下のようなセキュリティの効果が期待できます。 ・NATの存在を前提としないため、エンドツーエンドレベルのセキュリティ　が可能になります。これと、従来のファイアウォールレベルの境界セキュリティとを組合わせることにより、より粒度の細かいセキュリティ対応ができます。 ・NATの存在を前提としないため、一台一台の端末の特定が可能になります。アクセスログ管理がよりきちんとできるためセキュリティが向上します。 ・IPv6ではグローバルにユニークなアドレスを利用することにより、クローズドネットの利便性が向上します。NTT東日本が総務省IPv6移行実証実験で実験しているようなMP/MH(Multi-Prefix/Multi-Home)インフラが広がってくると、防犯、医療、バンキングなど家庭へのさまざまなアプリケーションサービスが、セキュリティに不安のあるインターネットではなく、専用のクローズドネットでよりセキュアに提供されるようになります。