「第１次情報セキュリティ基本計画(案)」への提出意見に対する考え方

番号	該当箇所	ご意見の概要	ご意見に対する考え方
1	第３章第１節（１）「政府機関・地方公共団体」(P.14)	第３章第１節（３）③「企業における情報セキュリティ人材の確保・育成」(P.19)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。	ご指摘の点は重要と認識しており、今後の政策運営に適切に反映してまいります。
	第３章第１節（１）イ④「職員の研修等の支援」(P.17)	政府機関における人材育成と同等の内容にすべき。（専門的職員を配置し、資格を保有させる。）	ご指摘の内容については、今後の政策の推進に当たっての参考の一つとさせていただきます。
2	第３章第２節（４）「犯罪の取締りおよび権利・権益の保護・救済」(P.23)	ＩＴ犯罪を行っても無駄だと思わせるよう、１）「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を行い、２）ＩＴ犯罪へは初動逮捕で確実に検挙すべき。	ご指摘の内容については、今後の政策の推進に当たっての参考の一つとさせていただきます。
３－１	第１章第１節（１）②中、「、、安心・安全で、信頼できるIT社会の実現、、」(P.3)	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。	ご指摘を踏まえて、以下のような修正を加えます。 第１章第２節（１）「官民各主体の共通認識の形成」(P.7)を以下のように修正。 ＜修正後＞ （前略）この自律的な取組みを促進するためには、それぞれが「何のために、どの程度のリスクに対応して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ことが必要である。 また、第３章第２節の前文(P.21)を以下のように修正。 ＜修正後＞ 各主体がそれぞれ「何のために、どの程度のリスクに対応して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の形成を促進し、（後略）
３－２	第１章第１節（１）④中、「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」(P.4)	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。	本計画は、ＩＴ戦略本部の中に設置された情報セキュリティ政策会議として、インフラとしてのＩＴの安全性・信頼性を確保するということを大きな軸として策定しているものです。ご指摘のように、情報セキュリティの対象は「情報」そのものであるという視点は重要であり、「情報」そのものを対象とするとの視点は、第１章第１節（１）①「国家目標Ⅰ（略）」(P.3)に「物質的な豊かさを追求する『工業経済』は、知恵とノウハウの活用の巧みさが問われる『情報経済』へと、その軸足を移しつつある。」と記述し、重要性の認識を提示しているところです。
３－３	第１章第１節（２）「実現すべき基本目標」(P.5)	知を守る基盤としての捉え方が欠けている。	３－２に対する回答に同じです。
３－４	第１章第２節（１）中、「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(P.7)	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。	３－２に対する回答に同じです。
３－５	第１章第２節（２）「先進技術の追求」(P,7)	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。	ご指摘の内容については、今後の政策の推進に当たっての参考の一つとさせていただきます。
３－６	第２章「ＩＴを安心して利用可能な環境」の構築(P.9)	「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。	３－１に対する回答に示した修正を加えます。また、官民連携の施策を講じる必要性へのご指摘については、今後の政策の推進に当たっての参考の一つとさせていただきます。
３－７	第２章第１節（３）「企業」(P.11)	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。	３－２に対する回答に同じです。
３－８	第２章第１節（４）「個人」(P.11)	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。	３－１に対する回答に同じです。
３－９	第２章第２節（４）「メディア」(P.13)	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べき。	３－１に対する回答に同じです。

３－１０	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-」(P.14)	「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。	３－２に対する回答に同じです。
３－１１	第３章第１節（１）ア「政府機関」(P.15)	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、明記すべき。	ご指摘の点については、各政府機関が情報セキュリティ監査を実施することについて、政府機関統一基準（平成１７年１２月１３日情報セキュリティ政策会議決定）に明記されているところです。
３－１２	第３章第１節（４）「個人」(P.20)	リスク認識にかかわる教育が必要である。	３－１に対する回答に同じです。
４	第１章第２節（２）「先進的技術の追求」(P.7) 第３章第１節（１）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」(P.15)	「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すべき。	ご指摘の点は重要と認識しており、政府機関によるIPv6の導入については、その実現への道筋を明確にするため、第３章第１節（１）ア③（イ）の第２段落を次のとおり修正いたします。 「特に、今後、すべての政府機関の情報システムがIPv6を早期に利用できるようにするため、原則として2008年度までに、各府省の情報システムの新たな開発（導入）又は更改に合わせて、情報通信機器やソフトウェアのIPv6対応化を図る。」
５－１	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 (P.16,P.17,P.19,P.20,P.21)	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。	本基本計画においては、高度人材育成と普及啓蒙的活動の両面が必要であるとの立場に立っています。
５－２	第３章第２節（２）③ 資格制度の創設について(P.22)	第２章 第２節（１）「政府・地方公共団体 （略）」(P.11)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。	ご指摘の該当箇所（第３章第２節（２）②「情報セキュリティに関する資格制度の体系化」(P.22)）については、そもそも「資格制度の創設」ではなく「資格制度の体系化」について記載しているものです。
６	第１章第２節（４）「メディア」（P.13）	「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」表現に変更すべき。	「迅速な公表に努める」ことは「メディアによって取り上げられるような環境の整備」の一部に含まれるものと考えており、今後も引き続き情報の迅速な公表に努力してまいります。
７－１	「はじめに」(P.1)	社会問題化している事例として、「構造計算書の偽造事件」を追加すべき。	ご指摘の部分については、本計画が中長期（３年間）の計画であることを踏まえて、特定のものではなく、一般的な事例等を挙げているものであり、ご指摘の具体的事例をここで提示することは適切でないと考えます。
７－２	第１章第１節（２）「実現すべき基本目標－「ＩＴを安心して利用可能な環境」の構築へ－」(P.6)	ＩＴ活用が不十分な例として、「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。」を追加すべき。	「ITの活用が不十分」ということについては「IT新改革戦略」のスコープであって、情報セキュリティの基本計画のスコープではないと考えます。
７－３	第２章第１節（３）「企業」(P.11)	ＩＴ社会を構成する一員としての立場から、「企業活動の記録管理」に取り組む責任を追加すべき。	記録管理の必要性は、情報セキュリティ対策に取り組む責任の中に包含される事項であり、ご指摘の内容については、今後の政策の推進にあたっての参考の一つとさせていただきます。
７－４	第３章第２節（２）「情報セキュリティ人材の育成・確保」（P.22）	記録管理を適切に行う人材の育成・確保を追加すべき。	７－３に対する回答に同じです。
７－５	第３章第２節（２）②「情報セキュリティに関する資格制度の体系化」 (P.22)	情報セキュリティに関する資格制度として、「記録管理責任者」を追加すべき。	７－３に対する回答に同じです。
８	第３章第２節（２）「情報セキュリティ人材の育成・確保」（P.22）	情報セキュリティ人材の育成・確保策として、項目番号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」を追加すべき。	ご指摘を踏まえて、本文第３章第２節（２）「情報セキュリティ人材の育成・確保」(P.22)の第２段落の留意が必要な事項に「国際的に通用する人材の育成が必要なこと」を追加いたします。

９	第２章第２節（３）「情報関連事業者・情報関連非営利組織」(P.12) ほか	非営利組織が自主的に活動できるよう人材育成等の具体的な政策提示を推進していただきたい。また、全国の非営利組織の整備とともに具体的な支援策を重点政策として組み込むべき。	問題の理解・解決を促進するそれぞれの主体の役割と連携についての個別の具体策については、今後、年度計画等において具体化していきたいと考えており、ご指摘の内容については、今後の政策の推進に当たっての参考の一つとさせていただきます。
１０	第３章第２節（２）「情報セキュリティ人材の育成・確保」(P.22)	情報セキュリティ人材の育成・確保策として、項目番号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」を追加すべき。	８に対する回答に同じです。
１１－１	第２章第１節「対策実施主体の役割と連携」(P.9) 第２章第２節（３）「情報関連事業者・情報関連非営利組織」(P.12) 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」(P.19) 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」(P.19)	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。	ご指摘の内容については、第２章第２節（３）「情報関連事業者・情報関連非営利組織」（P.12）、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」（P.19）、及び、第３章第１節（３）②「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（P.19）に含めて記述しているところであり、今後の政策運営に適切に反映してまいります。
１１－２	第２章第２節（４）「メディア」(P.13)	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。	ご指摘の内容については、今後の政策の推進に当たっての参考の一つとさせていただきます。
１１－３	第３章第１節（１）ア③「中長期的なセキュリティ対策の強化・検討」(P.15)	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年問題への取り組みを追記すべき。	ご指摘を踏まえ、暗号利用について、以下を追記いたします。 ※追記する文章 第3章第1節 (1) ③ (エ)「政府機関における安全な暗号利用の促進」(P.16) 電子政府の安全性及び信頼性を確保するため、電子政府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、暗号の適切な利用方策について検討を進める。
１１－４	第３章第１節（１）イ②情報セキュリティ監査実施の推進」(P.16)	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。	ご指摘の内容については、今後の政策の推進に当たっての参考の一つとさせていただきます。
１１－５	第３章第１節（２）重要インフラ(P.17)	「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。	IT障害の定義は、第２章第１節（２）「重要インフラ」脚注１２に示ししたとおりです。すなわち、ご指摘のように「操作ミスや天災」の発生をゼロにするのではなく、それらの要因によって発生する「サービスの停止や機能の低下等」の障害を限りなくゼロにすべきである、という趣旨は本基本計画に既に述べられており、その観点から、本基本計画ではあくまでも「IT障害の発生を限りなくゼロとすることを目指す」ことを目標としているものです。
１１－６	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」(P.19)	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について、評価する側、される側の準備状況を十分踏まえた上で実施すべき。	ご指摘の内容については、今後の政策の推進に当たっての参考の一つとさせていただきます。
１２	第３章第２節（２）「情報セキュリティ人材の育成・確保」(P.22)及び 第３章第２節（３）「国際連携・協調の推進」(P.22)	「国際的に通用する情報セキュリティ技術及び知識を有する人材の育成と確保の重要性並びに必要性」及び「資格制度の体系化における国際連携・強調の重要性及び必要性」の旨の内容を追加願いたい。	８に対する回答に同じです。
１３－１	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 (P.11,P.12,P.14,P.19)	「情報モラル」の普及啓発及び「情報モラル」に関する教育の強化推進について言及するべき。	ご指摘の点は重要と認識しており、今後の政策運営に適切に反映してまいります。
１３－２	第３章第１節（１）「政府機関・地方公共団体」、（２）「重要インフラ」、（３）「企業」、（４）「個人」 (P.9,P.10,P.11)	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、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、人材育成を行う「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・運用することを提言すべき。	ご指摘の内容については、今後の政策の推進に当たっての参考の一つとさせていただきます。

１３－３	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 (P.4,P.6,P.8,P.22)	・ 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 を追加すべき。	ご指摘の内容については、今後の政策の推進に当たっての参考の一つとさせていただきます。
１３－４	第３章第１節（１）「政府機関・地方公共団体」、（３）「企業」、（４）「個人」 (P.14～P.20)	政府機関・地方公共団体の財政的な支援や相互の連携の下、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体制を構築することを提言すべき。	ご指摘の内容については、本基本計画の実現についての具体像を検討するに当たっての参考の一つとさせていただきます。
１４－１	第１章第１節（１）⑤「「セキュリティ立国」の思想に基づく「情報セキュリティ先進国の実現」」 (P.4)	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。	ご指摘の内容については、今後の政策の推進に当たっての参考の一つとさせていただきます。
１４－２	第３章第１部（１）ア③（イ）「セキュリティ強化に資する新規システム（機能）の導入検討とその実現」(P.15)	政府機関の中長期的なセキュリティ対策強化でシステム導入が述べられているが、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すべき。	ご指摘の点は重要と認識しており、今後の政策運営に適切に反映してまいります。
１４－３	第３章第１節（１）ア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」 (P.15)	「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、企業の自主的な取り組みを尊重した運用をされたい。	ご指摘の内容については、今後の政策の推進に当たっての参考の一つとさせていただきます。
１４－４	第３章第１節（１）イ「地方公共団体」(P16,P.17)	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。	地方公共団体については、重要インフラの一つとして、「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』策定のための指針」を踏まえたガイドラインを作成することにしていま
１４－５	第３章第１節（１）イ「地方公共団体」(P16,P.17)	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。	ご指摘の点は重要と認識しており、今後の政策運営に適切に反映してまいります。
１４－６	第３章第１節（１）イ「地方公共団体」(P16,P.17)	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。	ご指摘の内容については、今後の政策の推進に当たっての参考の一つとさせていただきます。
１４－７	第３章第１節（２）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」 (P.17)	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。	ご指摘の内容については、今後の政策の推進に当たっての参考の一つとさせていただきます。
１４－８	第３章第１節（３）「企業」 (P.19)	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。	ご指摘の内容については、今後の政策の推進に当たっての参考の一つとさせていただきます。
１４－９	第３章第２節（４）①「サイバー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」(P.23)	「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。」を追加すべき。	ご指摘の点は重要と認識しており、今後の政策運営においても適切に対応してまいります。
１４－１０	第４章(P.24)	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べき。	ご指摘の内容については、今後の政策の推進に当たっての参考の一つとさせていただきます。
１５	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」(P.9)	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。	ご指摘の部分の記述は、脆弱性やサイバーテロに限定したものではなく、情報漏洩対策に係る官民連携も含める趣旨で記述しているものであり、今後の政策運営においても適切に対応してまいります。

１６－１	第３章第１節（１）ア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」(P.15)	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、一般企業等の規範となるべきものであり、どの政府機関を規範とすべきかの判断のため「達成状況を公開する」と追加すべき。	ご指摘を踏まえ、第3章第1節⑴ア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」(P.15)の第2段落の後に、以下を追記いたします。 ※追記する文章 なお、評価の結果については、情報セキュリティの維持･確保にも配慮しつつ公表することとする。
１６－２	第３章第１節（１）イ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」(P.16)	以下の文章を追加すべき。（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。	ご指摘の内容については、今後の政策の推進に当たっての参考の一つとさせていただきます。
１６－３	第３章第１節（２）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」(P.17)	以下の文章を追加すべき。（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。	今後、「安全基準等」については、「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」の決定後、各分野ごとに具体的な策定・見直しを進めていくことになっています。その際には、分野の特性等を十分に踏まえつつ、ご指摘の政府機関統一基準だけでなく、国際規格等、既存のベストプラクティスを参考にすることも有効な選択肢の一つであると考えられます。 いずれにせよ、ご指摘の内容については、今後の政策の推進に当たっての参考の一つとさせていただきます。
１７	第３章第１節（１）イ②「情報セキュリティ監査実施の推進」(P.16)	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し、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とを提言するべき。	ご指摘の内容については、今後の政策の推進に当たっての参考の一つとさせていただきます。
１８－１	第３章第１節（１）「政府機関・地方公共団体」(P.14)	政府機関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。	ご指摘の点については、「政府機関の情報セキュリティ対策の強化に関する基本方針」及び「政府機関の情報セキュリティ対策における統一基準の策定と運用等に関する指針」（ともに平成１７年９月１５日情報セキュリティ政策会議決定）で既に明確化しています。
１８－２	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」 (P21,P23)	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。	ご指摘の内容については、今後の政策の推進に当たっての参考の一つとさせていただきます。
１９－１	「はじめに」(P.1)	「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。」といった内容を追加すべき。	ご指摘の点は認識した上で、近年の事例等を列挙しているものです。
１９－２	第１章第２節（１）「官民各主体の共通認識」(p.7)	「共通認識」とは誰と誰の間の「共通認識」か不明確。	ご指摘の点は、政府機関、重要インフラ、企業、個人の領域のそれぞれの主体が、「何のために、どの程度のリスクに対応して情報セキュリティ対策を行うのか」という点についての、「全体としての」共通認識についての記載であり、官民間、民民間等、特定の関係者間の共通認識を意味するものではありません。
１９－３	第１章第２節（２）「先進的技術の追求」(P.7)	先進的技術だけでなく、「既存の仕様の再検討」も必要である。	ご指摘の点は、今後の政策の推進に当たっての参考の一つとさせていただきます。
１９－４	第２章第１節（２）「重要インフラ」(P.10)	「組織内 CSIRT (Computer Security Incident Response Team)構築の必要性」を加えるべき。	ご指摘の内容については、今後の政策の推進に当たっての参考の一つとさせていただきます。

１９－５	第２章第１節（４）「個人」(P.11)	「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。	ご指摘の点も踏まえた上で、「ＩＴの仕組みは理解しがたい」と記述しているものです。
１９－６	第２章第２節（２）「教育機関・研究機関」(P.12)	「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。	ご指摘の点は、今後の政策の推進に当たっての参考の一つとさせていただきます。
１９－７	第２章第２節（３）「情報関連事業者・情報関連非営利組織」(P.12)	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」という点を追記すべき。	ご指摘を踏まえて、第２章第２節（３）「情報関連事業者・情報関連非営利組織」(P.13)の項の最後に、以下を追記いたします。 ※追記する文章 　さらには、情報関連非営利組織の中には、国際的な連携・協調の役割を果たすものも生まれており、国際連携・協調の観点からの情報関連非営利組織の積極的な活動の展開が期待される。
１９－８	第３章第１節（１）ア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」(P.15)	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。	ご指摘の内容は第３章第１節（１）ア④「サイバー攻撃に対する政府機関における緊急対応能力の強化」(P.16)に含める趣旨で記述しているものです。
１９－９	第３章第１節（１）イ③「自治体情報共有...創設促進」(P.17)	「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。	ご指摘の点は、「政府等から提供される情報」に含める趣旨で記述しているものであり、今後の政策運営においても適切に対応してまいります。
１９－１０	第３章第１節（１）イ④「職員の研修等の支援」(P.17)	『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。	本章は、今後３年間の政府の取組みについて記述しており、ここでは、地方公共団体の取組みについて政府が支援するものです。
１９－１１	第３章第１節（２）④「分野横断的な演習の実施」(P.18)	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。	ご指摘の内容については、今後の政策の推進に当たっての参考の一つとさせていただきます。
１９－１２	第３章第２節（３）①「国際的な安全・安心... への貢献」(P.23)	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。	１９－７に対する回答に同じです。
１９－１３	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」(P.23)	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である。	非営利組織における取組みについては、１９－７に対する回答に示した修正を加えます。政府における取組みについては、第３章第２節（３）①「国際的な（略）」(P.23)にもその内容を含める趣旨で記述しているところであり、今後の政策運営においても適切に対応してまいります。
１９－１４	第４章第１節（１）「内閣官房... (NISC)の強化」(P.24)	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。 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。	ご指摘の点は、今後の政策の推進に当たっての参考の一つとさせていただきます。
１９－１５	第４章第３節(P.25)	(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。	ご指摘の点は、今後の政策の推進に当たっての参考の一つとさせていただきます。
２０－１	第１章第１節（２）①「「ITを安心して利用可能な環境」の構築」(P.5)	「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。	ご指摘の点は重要と認識しており、今後の政策運営に適切に反映してまいります。
２０－２	第２章第２節（３）「情報関連事業者・情報関連非営利組織」(P.12)	「・・・持つことも重要である」の後に、「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。	ご指摘の点は重要と認識しており、今後の政策運営に適切に反映してまいります。
２０－３	第３章第１節（１）ア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」(P.15)	「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。	１つ目のご指摘については、「政府機関の情報セキュリティ対策の強化に関する基本方針」及び「政府機関の情報セキュリティ対策における統一基準の策定と運用等に関する指針」（ともに平成１７年９月１５日情報セキュリティ政策会議決定）で既に明確化されており、２つ目のご指摘については、原案の趣旨に含まれる内容であるため、原案のとおりとさせていただきます。

	２０－４	第３章第１節（２）「重要インフラ」(P.17)	「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。	IT障害の定義は、第２章第１節(2)「重要インフラ」脚注１２に示したとおりであり、「サービスの停止」もこれに含まれるものです。ご指摘の点については、重要な視点として考慮されており、その観点から、本基本計画ではあくまでも「IT障害の発生を限りなくゼロとすることを目指す」ことを目標としているものです。
	２０－５	第３章第２節（１）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」	「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」を追記すべき。	ご指摘の点は、今後の政策の推進に当たっての参考の一つとさせていただきます。
	２１	第１章第２節（２）「先進的技術の追求」(P.7)	IPv6の推進について賛同。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重要である。	ご指摘の点は重要と認識しており、今後の政策運営に適切に反映してまいります。