資料７

基本計画検討委員会 各府省庁提出意見

目　　次

平成20年２月21日

内閣官房情報セキュリティセンター

内閣官房内閣情報調査室

「「第２次情報セキュリティ基本計画」（仮称）に係る検討の視点（例）」に関する意見

○　「政府機関・地方公共団体における情報セキュリティ対策について（２）」（９ページ）の「９．安全保障・外交等の機密情報を扱う場合をどうするか。ＣＩ（カウンターインテリジェンス）との関係。」について

意見：ＣＩ推進会議においても検討が行われるということを認識していただき、基本計画検討委員会で議論される場合には、一方的な決定がなされることのないよう、事前にＣＩセンター設置準備チーム（平成２０年４月以降はＣＩセンターとなる。）と綿密な協議を行っていただきたい。

警　察　庁

「第２次情報セキュリティ基本計画」（仮称）の検討に関する警察庁意見書

１　「「第２次情報セキュリティ基本計画」（仮称）（以下「次期計画」という。）に係る検討の視点（例）」に関する意見

（１）検討の視点として追加すべき事項、重点を置くべき事項、その他構成・分類に関する意見

ア　第１次情報セキュリティ基本計画（以下「第１次計画」という。）を踏まえた次期計画の策定

第１次計画では、対策実施領域ごとに目標を掲げ、当該目標の達成に向けて様々な施策を推進してきたが、第１次計画で掲げられた施策自体の評価は行われていないため、これらの取組みがそれぞれの分野でどの程度情報セキュリティの向上に寄与してきたのかということが不明である。

そのような状況を踏まえると、次期計画の策定の前に、第１次計画で掲げた施策について、情報セキュリティの向上にどの程度寄与したのかということ等について、妥当性を検証した上で次期計画の検討を行うべきであり、また、検証結果を踏まえ、第１次計画の内容に問題点があるようであれば、当該問題点を見直しつつ、次期計画の策定作業を行うべきである。

イ　事案対処の観点を含めた重要インフラにおける情報セキュリティ対策の推進、連携強化（10 頁「重要インフラにおける情報セキュリティ対策について」について）

サイバー攻撃による IT 障害の未然防止及び現実に発生した際の迅速かつ的確な業務の復旧、被害拡大防止等に資するためには、重要インフラ事業者等とサイバーテロ対策を含めた危機管理に関するノウハウを蓄積している事案対処省庁との連携を一層強化し、事案対処の観点を十分に取り入れた対策を推進していく必要があることから、「事案対処の観点を含めた重要インフラにおける情報セキュリティ対策の推進、連携強化」という視点を追加すべきである。

（２）個々の視点に対する意見

ア　情報セキュリティ対策に係る組織等に関する意見（９頁「政府機関・地方公共団体における情報セキュリティ対策について」の８番について）

各機関における情報セキュリティ対策に係る組織や情報セキュリティ対策担当者の位置付けは、保有システムの内容によって大きく異なるほか、当該機関における職員の採用・運用のあり方や組織構成にかかわっている。

このため、情報セキュリティ対策に係る組織や情報セキュリティ対策担当者のキャリアパスについては、政府機関等に対して一律に示すべきではないと考える。

イ　情報セキュリティ意識の向上のための取組みの充実等の必要性について（18頁「個人に対する情報セキュリティ対策について」の１番及び２番について）

情報セキュリティ意識の向上には、持続的な取組みにより各個人への浸透を図ることが必要であり、昨年より始まった情報セキュリティの日に関連する各種活動や日頃からのホームページによる広報啓発等、政府、民間等の各主体における様々な取組みの普及・定着とともに、内容の充実を図ることが必要であると考える。

ウ　サイバー犯罪の取締りの推進の必要性（25頁「情報セキュリティ分野における犯罪の取締り、権利利益の保護・救済について」の１番について）

サイバー犯罪の増加・巧妙化に対して、サイバー犯罪の取締り、被害防止のための広報啓発活動、実体法及び手続法の実効性を確保するための官民連携等を推進することが必要であると考える。

エ　サイバー犯罪の取締りの強化を可能とする制度がネットワーク利用環境に与える影響について（25 頁「情報セキュリティ分野における犯罪の取締り、権利利益の保護・救済について」の２番について）

新しい制度について議論する場合、その影響については当然に考慮されるものであり、情報セキュリティ対策の影響についての視点は重要である。しかし、情報セキュリティの確保を目的とする当会議において、影響について結論を得るまでの体制は確保されておらず、議論に際しての態度としては「影響にも配慮しつつ」セキュリティの確保について議論することが適当であり、あえて項目をたてて影響について結論を得るようなことは適当ではないと考える。

オ　デジタルフォレンジックの確立等の必要性について（20頁「情報セキュリティ分野における技術開発の取組みについて」の１番、24 頁「情報セキュリティ分野における国際連携・協調の推進に向けた取組みについて」の５番、25頁「情報セキュリティ分野における犯罪の取締り、権利利益の保護・救済について」の１番について）

○　サイバー犯罪の増加・巧妙化に対応するためには、デジタルフォレンジックの確立に向けた取組み及びデジタルフォレンジックに係る体制の強化による効果的かつ効率的な捜査等の推進が必要であると考える。

○　デジタルフォレンジックに必要な技術情報の共有のため、官民の技術協力等の推進が必要であると考える。

○　国境を越えたサイバー攻撃への対応等については、サイバー犯罪条約締結に向けた刑事基本法制の整備、これに対応したデジタルフォレンジックの確立に向けた取組み及びデジタルフォレンジックに係る体制の強化、国内外関係機関との連携の強化等が必要であると考える。

○　不正プログラムやファイル共有ソフトによる犯罪や不正行為に対応するための情報収集・分析等の強化が必要であると考える。

○　重要インフラへのサイバーテロ等に対する事案対処能力の強化を図る必要があると考える。

2　現在進めている、政府機関を対象とした情報セキュリティ政策に対する意見及び今後の政策への要望について

ア　各府省庁の実状に合わせた情報セキュリティ対策の展開

これまで、情報セキュリティ対策のために実施すべき施策については、政府機関で一律に政府機関統一基準、評価、自己点検等、様々なものが示されてきたが、各府省庁の持つネットワーク等の実状により、その効果は異なるため、各府省庁の実状に合わせて各府省庁の裁量で行うべき対策も含めて検証し、見直す必要がある。

そのため、情報セキュリティ政策会議で示されている政府機関の情報セキュリティ対策のための施策について、その進捗、効果及び人的・物的なコストを十分に検証し、各府省庁の実状に合わせた情報セキュリティ対策を展開できるようにするべきである。

イ　情報セキュリティ対策を実施するための基盤の確保

各府省庁において情報セキュリティ対策を実施するためには、相応の予算や事務量が必要になるところ、昨今の厳しい財政状況の下、各府省庁の情報セキュリティ対策部門の予算や人員はほとんど増加していない。

このため、今後、政府機関については、情報セキュリティ対策を実施するために必要な基盤である予算、人員、体制等を充実・確保するための具体的な施策を実施していかなければ、次期計画において提案された情報セキュリティ対策がいかに効果的であっても、実施することができなくなってしまうおそれがある。

よって、各府省庁の情報セキュリティ対策を実施するための基盤（予算、人員、体制等）を充実・確保するための具体的な方策を検討し、実施していくべきである。

政府機関を対象とした情報セキュリティ政策に関する意見

総　務　省

1　「政府機関の情報セキュリティ対策のための統一基準」について

「統一基準」は、各府省庁で遵守されるべき最低限の基準を統一的に定めたものとして、政府全体の情報セキュリティ対策の底上げに一定の成果を上げてきたものと考えられる。

しかしながら、情報の取扱いから、セキュリティ要件、情報システムの構成要素、調達・開発等、非常に多岐にわたる行政事務を網羅した一律の基準となっていることから、それに基づいた省庁対策基準についても、遵守事項が大部に及ぶとともに、内容においても情報システムの運用等に携わる一部の職員が理解すれば十分と見られる遵守事項も多く、大多数の一般職員にとって難解であり、馴染みにくいものとなっている。

したがって、政府統一基準について、対象者に応じたより効果的なセキュリティ対策を講ずるため、行政事務従事者が遵守すべき事項と情報システム関係者等が遵守すべき事項を区分し、特に行政事務従事者向けの基準について、実施すべき事項をより明確化し、平易な記述とするよう努めるべきである。

また、情報システム関係者等向けの基準についても、現在、全てのシステムについて一律に基本遵守事項・強化遵守事項が示されているが、情報システムのセキュリティ対策について真に実効性を持たせるためにも、情報システムの構成や取り扱う情報の重要度等に応じた規定の整理について検討するべきである。

2　情報セキュリティ対策に必要な予算・人員等の確保について

各府省庁における情報セキュリティ対策については、一層の強化が求められているにも関わらず、昨今の厳しい財政状況の下、予算面・人員面での制約はますます厳しくなっている。したがって、各システムの情報セキュリティ対策については、情報システムの構成や取り扱う情報の重要度等に応じ、優先順位をつけて施策を進めていくべきである。また、情報セキュリティ対策の実施状況報告や重点検査等については、各省の担当者が年間を通じ平均的に業務がこなせるよう計画上考慮して実施していただきたい。

また、政府全体として確実に実施しなければならない施策については、それらが確実に実施可能となるような予算・人員等が各省において確保されるよう、内閣官房を中心に政府全体として計画的に取り組むべきである。また、緊急に全府省庁で対策が必要となった場合等における必要な予算等の確保方策についても検討すべきである。

法　務　省

「第２次情報セキュリティ基本計画」（仮称）の検討に係る意見等について

第１　意見募集項目２(1)について

１　「政府機関の情報セキュリティ対策のための統一基準」について

(1)　政府機関の情報セキュリティ対策の指針である「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「統一基準」という。）は，情報流出防止や情報システムの障害回避等の観点から，個々の行政事務従事者が実施すべき対策のほか，情報システムセキュリティ要件の明確化に基づく対策，情報システムの構成要素についての対策等，多くの事項が盛り込まれている。そのため，これに準拠する省庁対策基準も多岐に渡る内容を含んだ大部のものとならざるを得ず，多くの行政事務従事者にとって馴染みにくく，読みづらいものとなっている。

現在の統一基準，ひいてはこれに準拠する省庁対策基準に規定されているあらゆる事項を全ての行政事務従事者が理解する必要があるとは考えがたいことから，「全ての行政事務従事者が理解し，遵守すべき事項」と「情報システムの構築・運用等の特定業務に従事する者など，一部の行政事務従事者が理解し，遵守すれば足りる事項」を区分し，それぞれ別の規定として整理することが望ましいと考える。

(2)　また，統一基準では，相当多数の項目が「基本遵守事項」とされ，その実施が必須とされているが，その中には「強化遵守事項」と位置づけ，必要に応じて実施することが適切ではないかと思われる事項も含まれており，その内容を精査することが望ましいと考える。

(3)　さらに，情報システムの構成等によっては，現行の統一基準が一律に要求している情報セキュリティ対策の実施が過剰なセキュリティ対策の実施につながるおそれもあると考えられることから，真に必須と考えられる事項のみを統一基準として定め，それ以外の事項は，情報システムの構成や取り扱う情報の重要度等に応じた情報セキュリティ対策のレベルごとに，必要とする事項を整理した上で統一基準の下位規定として整備すべきであると考える。

２　情報セキュリティ対策の重点検査等について

省内における情報セキュリティ維持・向上を図る上で，行政事務従事者を対象とした情報セキュリティに関するリテラシ向上のための教育のより一層の充実，各種情報システムにおけるセキュリティ水準確保等のための対策の拡充が望まれる。その実現には，情報セキュリティ対策関連業務のうち，重点的に実施すべきものについては十分な人材を投入し，その他の業務についてはできる限りの効率化を図るなどして，限られた人材・資源を有効に活用することが必要であり，このような取組は，政府機関における行政効率化の要請にも合致すると思われる。

このような観点から,現状では五月雨式に要求されている情報セキュリティ対策の実施状況報告や重点検査等については,実施時期及び実施回数を十分に吟味し,体系化した上で,適切な時期に必要な回数のみ行われるよう調整するとともに,検査項目等を厳選し,基本的かつ重要な事項にポイントを絞った報告及び検査等とすることが望ましいと考える。

また,その結果の公表に当たっては,各府省庁に脆弱性があるという情報を積極的に公表することによる悪意のあるユーザからの攻撃対象となる危険性と政府機関の情報セキュリティ対策の現状の報告としての必要性等を比較考量し,慎重に実施すべきものと考える。

第２　意見募集項目４(1)について

政府機関の電子申請システム等の利用者である国民がインストールを必要とするＪＲＥ（Java Runtime Environment）に脆弱性が発見された事案のように,多数の国民に対し被害を及ぼすおそれがあり,かつ政府機関に共通する問題が発生した場合,政府機関が迅速にセキュリティ確保のために必要な統一的対策を講じることが可能となるよう,このような事態に備えて,あらかじめ政府機関共通の対応経費として一定額の予算を確保するなどの方策を中長期的な視点で検討していくことが必要であると思料する。

外　　務　　省

１．「『第２次情報セキュリティ基本計画』（仮称）に係る検討の視点（例）」に対する意見

（１）「政府機関・地方公共団体における情報セキュリティ対策について（２）」(P.9)

項目７．については、「政府機関の情報セキュリティ対策は、各府省庁の責任において実施しているが、限られた予算と不十分な人員の下、施策の優先順位付けが必要ではないか。」という視点で検討すべきと考える。

(理由)

「セキュア・ジャパン２００７」第１章第３節「２００６年度の評価」１．において、「「各政府機関でのＰＤＣＡサイクルの確立」、「政府全体でのＰＤＣＡサイクルの確立」という対策の大部分を占める施策がA’となっていることから体制や人員等の不足が大きな課題であることがうかがえる」とされており、人員面が十分でないことは既に明らかになっている。また、厳しい予算事情を考慮すれば、優先順位が不明確な施策に対して予算を満額確保できる保証はなく、経費捻出のために他の施策にしわ寄せが及ぶ懸念がある。したがって、施策の優先順位付けについての検討が必要と考える。

（２）「政府機関・地方公共団体における情報セキュリティ対策について（２）」(P.9)

項目９．「安全保障・外交等の機密情報を扱う場合をどうするか。ＣＩ（カウンターインテリジェンス）との関係」については、削除を検討して頂きたい。

(理由)

「政府機関・地方公共団体における情報セキュリティ対策」では、あくまでも政府・自治体に共通する横断的な「情報セキュリティの仕組み」に関する項目が議論されるべきと考える。

安全保障・外交等の機密等については重要な論点であるが、一部の省庁が保有する特殊な情報のセキュリティについては、当該省庁が各々の情報の性格（指定された機密性等）に応じてセキュリティ対策を施すべきであり、地方公共団体を含めた全体の中での検討には馴染まないものと認識している。

（３）「国際連携・協調の推進に向けた取り組みについて」(P.24)

項目１．について、国際機関での取組みとの整合性について議論すること自体は結構なことであると考える。

当省としては、既存の枠組みで対処可能なものは引き続き関係省庁と協議しつつ、また、新規の提案については内閣官房における更なる具体的検討を踏まえ、可能な協力につき協議に参画していきたいと考えている。

２．政府機関を対象とした情報セキュリティ政策に関する意見

（１）現在進めている、政府機関を対象とした情報セキュリティ政策に対する意見、及び今後の政策への展望について

現在の「第１次情報セキュリティ基本計画」の「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－」内「 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」の「（１）ア 政府機関」の「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」の第２パラグラフに「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、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。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。」と記述されているところ、（更に、「セキュア・ジャパン２００７」には、「第３章 第１節 ア ①【具体的施策】ウ）本格的な評価の推進及び結果の公表」に「また、評価の結果については、政府全体としての効果的な対策の推進を図るとともに、国民への説明責任を果たすためのものとして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。」と記述されているところ、）

（イ）これまで端末・ウェブサーバ、電子メールサーバについての検査を実施し、その評価の結果を各府省毎に公表されてきたが、我が国の政府機関に情報セキュリティ上問題があるということを公表することによる負の側面にも十分な考慮が必要と考える。日本国行政府の、端末・ウェブサーバ、電子メールサーバといった特定のものについての情報セキュリティ対策状況として不十分な点があるということを一般に公表していく場合、世界各国・地域との関係上、我が国の国益を損じることとなる可能性すら排除できない。国民への説明責任の重要性は言を俟たないが、国益を損ずることの無きよう慎重な配慮が必要である。

（ロ）また、当該検査の評価結果を公表することに伴って、各府省庁においては当該検査へリソース（人的、予算的）を傾注せざるを得ず、その負担も大きい。当省（外務省）を含む各府省庁は、極めて限られた人的資源の中で、情報セキュリティ対策に当たっているところ、最小のコストで最大の効果を得るべく対策のためのリソースの最適配分を可能とすることを前提に、公表・不公表のあり方を考えて頂きたい。

（２）当省固有の留意点について

在外公館における情報セキュリティ対策については、国ごとに情報インフラの整備状況が異なり、我が国のように情報インフラが整備されている国ばかりではない点に配慮願いたい。言語や文化、現地業者等、環境は多種多様であり、国内での対策に重点をおいた基準を、在外公館にも一律に適用することは現実的ではない場合が多々ある。対策の趣旨を踏まえつつ個別に対処する方が、限られた予算と人員の下、適切な情報セキュリティ対策が行えると考える。

３．情報セキュリティ対策に係る予算の特殊事情について

情報セキュリティ対策に係る予算については、各府省とも種々の情報システムの中で、OS のアップデートやウィルス防止ソフトのパターンファイルの更新に加えて、システム機器ハードウェア・ソフトウェアの更新及びシステム内アプリケーション・ソフトの更新並びにこれらのソフトの上で稼働している開発済みシステムのアップグレード（稼働テストを含む）が必要となる。このための経費は減価償却が終わるタイミングを待たず、各 OS やアプリケーション・ソフトのサポート切れのタイミングがあるため、それぞれのシステムのヴァージョンに応じて対応することが求められる。この他、当省の特殊事情として、在外公館におけるシステムの更新作業が必要となる。本省から２００程存在する各在外公館にリモート接続で対応できる範囲であればともかく、この種の作業に当たっては、物理的サーバの更新やメモリ増強、OS のアップグレード等、物理的にシステムエンジニアが現地において作業せざるを得ない場面が多い。この結果、全在外公館に短期間でシステムエンジニアを派遣して作業を実施するとなると多額の経費がかかるため、予算上の制約から、現実問題として十分な対応が困難な状況にある。

ついては、政府として情報セキュリティ対策が重要という認識の下で、この手の情報セキュリティ対策を充分かつ適切・迅速に実施していくためには、予算手当に係る情報セキュリティ当局の支援を得て、十分な予算確保を行っていけるよう重点対策のひとつとして掲げていただきたい。

以上

経済産業省からの意見

１．「情報セキュリティ基本法」に関する記述について

情報セキュリティ対策は、ＩＴの利活用等と一体的に議論がなされる必要がある。新たな法律の必要性については、ＩＴ基本法で不足部分があるかということを十分に精査した上で検討すべきである。

（総論部分について）

２．ＩＴインフラへの依存が高まった結果、トラブル発生時に予想される影響度に応じて、事業継続性の視点が必要となるのではないか。

→（補足説明）

ＩＴインフラへの依存が高まっていることから、ＩＴインフラにトラブルが生じた際の脆弱性を抱えていることが考えられる。重要インフラの事業継続性は検討されているが、企業や個人などについても事業継続性の視点が必要となると考える。

３．情報共有が日常的に行われるようになった結果、他者の情報を預かる側の「預かり責任」を問う視点が必要となるのではないか。

→（補足説明）

自ら保有する情報についてはしっかりとした保全を講じる場合があっても、他者の情報に対する対処は講じられていないケースがある。他者の情報を預かる者の責任を問える仕組みの検討や意識等の向上を図ることが必要と考える。

４．人に依存したシステム設計から、可能な限り人為ミスを排除した「フェイルセーフ」の考え方を重視すべきではないか。

→（補足説明）

「人的要因に対する対策と意識作り」に関して、人為ミスを排除できるような仕組みを構築することが重要であると考える。

（各論部分について）

５．大学・研究機関などのアカデミアも、情報セキュリティ対策の重要なターゲットではないか。

→（補足説明）

大学・研究機関などのアカデミアは非常に高度な技術情報等を有しており、他分野と同様に情報セキュリティ対策を講じない理由はない。各論において、大学・研究機関について触れておくべきではないかと考える。

６．大企業と中小下請企業の情報共有の際、中小企業側だけでなく大企業側にも「預かり責任者」としての適切な情報管理を求める視点が必要でないか。

→（補足説明）

大企業から中小企業に渡した情報の適切な管理の強化については大企業から要望が多いところであるが、一方で中小企業から大企業に渡した情報が他社に横流しされているというケースがある（例えば、大企業に提出した加工データが、競合他社で使用されているなど）。取引先の情報を預かっている際の意識の向上と適切な対処に企業規模を問わず必要であると考える。

７．安全保障・外交等の国家にとって重要な機密情報の流出対策を検討すべきではないか。

→（補足説明）

機密情報を「扱う場合」は記載されているが、政府機関・地方公共団体からの情報漏えいが大きな社会問題となっていることに鑑み、「流出対策」についても検討することが重要であると考える。

国　土　交　通　省

「「第２次情報セキュリティ基本計画」（仮称）の策定に向けた、情報セキュリティ政策に関する意見の募集について」意見提出

意見１：情報セキュリティに係る人材育成・教育の政府統一的な推進を求める。

（理由）

今まで主に各種の制度設計に取り組まれてきたと認識しているが、人的問題は機器等のハードや各種制度の設計・構築をもってしても防げない部分であり、かつまたシステムの設計・管理に携わる者のみに止まらず、利用する関係者すべてにリスクが内在するものであることから、関係者全て（国民・公務員）を対象とした情報セキュリティ教育が求められる。また、関係スタッフが必ずしも十分でない、個別省庁等の負担の軽減を図る観点からも、最低限必要な情報セキュリティに係る知識・マナー等を示し、その普及啓発を一元的かつ大規模に図ることが効果的と考える。

意見２：情報セキュリティに係る各種の実態把握（特に浸透状況）に際し時間的な猶予を頂けるよう改善を求める。

（理由）

情報セキュリティの浸透状況の把握に際し、組織が大きく階層的であるほど反映にタイムラグが生じるにも関わらず、現状の調査等においては改正後速やかに反映される単層構造の組織を対象にしたかのごとき調査が行われている。

現実の組織においては各種の手順を踏んで進展するため、浸透に必要な時間的猶予が与えられなければ、関係する担当者等に無用な対策疲れを及ぼすとともに、結果として情報セキュリティへの取り組み意欲の低下が懸念されるため。

意見３：情報セキュリティに係る評価・公表手法の改善を求める。

（個別名称公表に係る配慮）

（理由）

各組織単位の情報セキュリティ評価は、努力目標を明確に示すものの、反面、責任の追及や、結果の隠蔽・改ざんにも繋がりかねない危険性を包含している。特に階層的な組織においては、担当者に複数の階層から圧力がかかり、必ずしも正確な実態が保証されると言い切れない。

現場の担当者から正確な実態を把握するためにも、評価及びその結果の公表については、無用な圧力がかかること無く、正確な実態（特に改善すべき事項等）が明らかになるような工夫をする必要があると考える。

意見４：情報セキュリティに係る予算・契約制度の弾力化に向けた検討を求める。
（理由）
　現状においては予算枠に縛られると共に、競争契約が求められているが、非常時を考えた場合等、一刻を争うべきシステム・機器の復旧が本当に競争契約で対応が可能なのか、あるいは全ての非常時まで想定した管理契約が存在しうるのか、全省的に共通の課題として考え方を整理すべきでないか。
　重要なシステムに破損・障害が生じ緊急の復旧を考えた場合、競争契約の制約の下での対応は不可能ではないかとの危惧を感じるものである。