情報セキュリティポリシーに関する
ガイドライン

平成１２年　7月１８日策　　定

平成１４年１１月２８日一部改定

情報セキュリティ対策推進会議決定

目　次

Ⅰ. ガイドラインの目的

本ガイドラインは、「ハッカー対策等の基盤整備に係る行動計画」（平成 12 年 1 月 21 日情報セキュリティ関係省庁局長等会議決定）に基づき、平成１２年７月に情報セキュリティ対策推進会議[1]において策定された。その内容は、情報セキュリティを担保するために必要となる各省庁の情報セキュリティポリシーに関する基本的な考え方、策定、運用及び見直し方法について記したものであり、各省庁の情報セキュリティポリシー策定のための参考に資することを目的とするものである。

Ⅱ. 基本的な考え方

１．意義

(1) 情報セキュリティポリシーの必要性

行政活動において、これまで情報システムを利用した業務は、中央集中型のホストコンピュータに一部の人間がアクセスし、情報処理業務を行うことが一般的であり、また、外部との情報交換、報道発表等は紙面や口頭で行うことが一般的であった。しかし、現在職場におけるパソコンが急激に普及し、個人がパソコンを利用して情報処理業務を行い、また個々の端末から全世界的なネットワークと接続できる環境となってきている。これにより、行政活動、行政サービスの効率化が図られること、また、一般国民の間にもパソコンが普及していることから、行政の情報システムへの内外からのアクセスが極めて容易になった。さらに、今後の電子政府の実現により、このアクセスの容易性はますます高まることとなる。

かつて多くのパソコンを使用していなかった頃には、情報システム及び当該システムに記録された情報へのアクセス制御を行うことで、基本的に情報セキュリティ対策を一元的に行うことが可能であった。しかしながら、汎用の基本ソフトウエア及び分散管理の普及、並びに IT の進展及び電子政府に向けた取組みにより、情報を取り巻く環境が大きく変化していき、また、国民からの情報システムへのアクセスが増加すること等による脆弱性が増加していく結果、これまでの文書管理体制及び情報システムの物理的・技術的な安全対策だけでは、高度にネットワーク化した情報システムに対し、十分な情報セキュリティが確保できない状況になってきている。こうした、ネットワーク化、さらには携帯端末の普及等は、情報システム全体としては不安定なものとなる負の側面があるが、これを適切に管理することによって、情報セキュリティを確保することができれば、むしろ、負となるよりも大きな利便性を提供するものであることを認識するべきである。また、互いの信頼を前提とする民間や外国との情報交

[1] 関係行政機関相互の緊密な連携の下、官民における情報セキュリティ対策の推進を図るため、高度情報通信社会推進本部に設置された全省庁を構成員とする会議。議長は内閣官房副長官。

換を円滑に行うためにも、政府における情報セキュリティが十分に確保されていなければならない。

特に、近年の個人情報に対する国民の意識の高まりや、平成 13 年 9 月 11 日に米国において発生した同時多発テロなど社会的脅威の高まりなどの状況からも、情報セキュリティに関する重要性が増している。

これらの情報セキュリティの確保のためには、これらの情報システムの利用者の情報セキュリティに対する意識向上はもちろんのこと、これらの情報に関して利用者個人の裁量で、その扱いが判断されることのないよう、組織として意思統一され、明文化された文書である情報セキュリティポリシーを策定することが必要である。

(2) 情報セキュリティ対策の特性

IT の発展速度は極めて速いため、ある時に講じた最高の情報セキュリティ対策が、将来にわたっても最高のものとして永続することはない。その時々のハードウエア、ソフトウエアの導入は導入時には適切な情報セキュリティ対策であり得るが、継続性は保証されていない。情報セキュリティ対策は、本ガイドラインを基に情報セキュリティポリシーを策定することによって完結する一過性の取組みではなく、情報セキュリティポリシーの策定及びそれに続く日々の継続的な取組みによって確保される性質のものであることを十分に認識するべきである。

また、情報セキュリティポリシーの中には、継続的な情報収集及びセキュリティ確保の体制を構築しておくこと、また「いかに破られないか」のみならず「破られたときどうするか」についての対策も適切に規定し、当該規定に基づいた対策を十分に構築しておくことが重要である。

さらには、情報セキュリティポリシー及び情報セキュリティポリシーに関連する実施手順等の規定類を定期的に見直すことによって、各省庁の所有する情報資産に対して、新たな脅威が発生していないか、環境の変化はないかを確認し、継続的に対策を講じていくことが必要である。特に、情報セキュリティの分野では、技術の進歩やハッカーの手口[2]の巧妙化に鑑み、早いサイクルで見直しを行っていくことが重要である。

[2] 「ハッカー」は、さまざまな意味で用いられるが、本ガイドラインにおいては、「コンピュータに不正なアクセスを行う者」を指す。

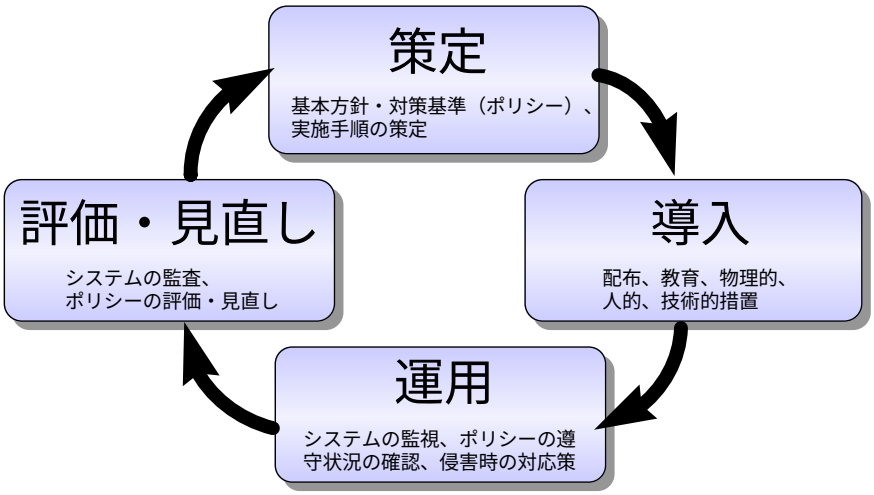

図１：情報セキュリティポリシーの実施サイクル

２．政府の情報セキュリティの基本的な考え方

現在、インターネットの急速な普及、電子商取引の実用化の動き等に見られる社会経済の情報化の進展に伴い、申請・届出等手続に係る国民負担軽減に対する要請が顕在化するとともに、行政と国民との間のコミュニケーションの活性化への期待が高まるなど、行政の情報化を取り巻く環境も急速に変化している。「高度情報通信社会推進に向けた基本方針」（平成10年11月9日高度情報通信社会推進本部決定）においては、このような環境変化に的確に対応していくため、セキュリティの確保等に留意しつつ、「紙」による情報の管理から情報通信ネットワークを駆使した電子的な情報の管理へ移行し、21世紀初頭に高度に情報化された行政、すなわち「電子政府」の実現を目指すこととしている。

一方、ネットワークに接続されている政府の情報システムは、常に、盗聴、侵入、破壊、改ざん等の脅威にさらされていることを認識し、政府としては、国民に対して、ネットワークを通じて正確な情報及び安定的な行政サービスを提供することを確保するとともに、個人のプライバシーに関する情報等の情報公開法で不開示とされる情報の機密の保持を確保しなければならない。

このような認識の下、次のような基本的な考え方に従い、政府全体としてセキュリティの水準を向上させていく必要がある。

(1) 各省庁[3]は、このガイドラインを踏まえ、情報セキュリティポリシーを策定し、これに基づく総合的・体系的な対策の推進を図る。その際、各省庁は、電子政府の基盤としてふさわしいセキュリティ水準を達成することを目標として、計画的に必要な措置を順次講ずる。

なお、このガイドラインが対象とする情報セキュリティを実現するためには、その前提として、文書等の情報の管理も適切に行われる必要がある。各省庁は、この

[3] 内閣官房、内閣法制局、内閣府、公正取引委員会を含む。

ような面での対策も必要に応じ考慮し、全体として高いセキュリティ水準を実現する。

(2) また、各省庁は、このガイドラインを踏まえ、その地方支分部局、所管の特殊法人等の情報セキュリティ水準の向上に努める。

(3) 内閣官房は、不正アクセスやコンピュータウイルス等が生じた場合における政府の緊急対処及び情報セキュリティ関連の人材育成や研究開発等の各省庁共通の課題について、政府内での協力・連携等の体制を確立・強化し、政府全体としてセキュリティ水準の向上を図る。

(4) 各省庁は、不正アクセス行為の禁止等に関する法律に定めるアクセス管理者による防御措置を実施すること等により、他の情報システムに対する攻撃に政府の情報システムが悪用されることを防止する。

(5) 我が国の情報通信基盤におけるセキュリティ水準の向上のため、民間との相互の情報交換を緊密にする等、官民の協力・連携を図る。

(6) 各省庁は、情報セキュリティポリシーを定期的に評価し、必要があれば更新することとし、少なくとも策定後1年を目途に更新の必要性の有無を検討する。

また、内閣官房は、このガイドラインについて、各省庁における情報セキュリティポリシーの実施状況、将来の技術、脅威の状況等を踏まえ、継続的に評価・見直しを行う。

３．定義

本ガイドラインで使用する用語の定義は、次のとおりである。

◯情報セキュリティ

情報資産の機密性、完全性及び可用性を維持すること。[4]

◯情報資産

情報及び情報を管理する仕組み（情報システム並びにシステム開発、運用及び保守のための資料等）の総称。

◯情報システム

---

[4] 国際標準化機構（ISO）が定める標準に定義されるもの（ISO 7498-2:1989）。

機密性(confidentiality)　：情報にアクセスすることが認可された者だけがアクセスできることを確実にすること。

完全性(integrity)　：情報及び処理方法の正確さ及び完全である状態を安全防護すること。

可用性(availability)　：許可された利用者が、必要なときに情報にアクセスできることを確実にすること。

（参考）

また、本ガイドラインでは採用していないが、ISO/IEC JTC 1/SC 27においては、上記に加え、次の３点について定義している。

真正性(authenticity)　：利用者、プロセス、システム及び情報又は資源の身元が主張どおりであることを保証すること。

責任追跡性性(accountability)：主体の行為からその主体にだけ至る形跡をたどれることを保証すること。

信頼性(reliability)　：意図した動作と結果に整合性があること。

同一組織内において、ハードウエア、ソフトウエア、ネットワーク、記録媒体で構成されるものであって、これら全体で業務処理を行うもの。

◯情報セキュリティポリシー（以下「ポリシー」という。）

各省庁が所有する情報資産の情報セキュリティ対策について、各省庁が総合的・体系的かつ具体的にとりまとめたもの。どのような情報資産をどのような脅威から、どのようにして守るのかについての基本的な考え方並びに情報セキュリティを確保するための体制、組織及び運用を含めた規定。情報セキュリティ基本方針及び情報セキュリティ対策基準からなる。

◯情報セキュリティポリシーに関するガイドライン（以下「ガイドライン」という。）

政府全体の情報セキュリティについての基本方針及び各省庁におけるポリシー策定のために参考とする手引であるとともに、各省庁が最低限行うべき対策を示すもの。

◯情報セキュリティ基本方針（以下「基本方針」という。）

各省庁における、情報セキュリティ対策に対する根本的な考え方を表すもので、各省庁が、どのような情報資産を、どのような脅威から、なぜ保護しなければならないのかを明らかにし、各省庁の情報セキュリティに対する取組姿勢を示すもの。

◯情報セキュリティ対策基準（以下「対策基準」という。）

「基本方針」に定められた情報セキュリティを確保するために遵守すべき行為及び判断等の基準、つまり「基本方針」を実現するために何をやらなければいけないかを示すもの。

◯情報セキュリティ実施手順等（以下「実施手順」という。）

ポリシーには含まれないものの、対策基準に定められた内容を具体的な情報システム又は業務において、どのような手順に従って実行していくのかを示すもの。

４．対象範囲

すべての情報は、その重要度に応じて適切に分類された上で、その分類毎の適切な対策を講じていく必要がある。その中で情報システムに関係する部分については、従来の「紙」を基本とした文書の管理とは異なり、ハッカーによる攻撃など各省庁の情報資産に対する新たな脅威に対して、これまで以上に適切な管理を講じていく必要があるとの認識の下、各省庁において求められる文書管理を情報システムにおいても実現するために、ポリシーを策定するものである。

したがって、各省庁が策定するポリシーの対象範囲は、ハードウエア、ソフトウエア、記録媒体等の情報システム等（システム構成図等の文書を含む。）及びすべての情報のうち、情報システムに電磁的に記録される情報、並びにこれらの情報に接するすべての者とする。このため、以下本ガイドラインにおいて、「情報資産」の情報は、電磁的に記録されたものに限られる。

原則として、ポリシーは統一されたものを一つ定め、実施手順はそれぞれ部局ごとに定めることになるが、当該部局の業務形態上ポリシーを分ける必要がある場合は、この限りではない。

なお、情報システムの活用により、電磁的記録から印刷される文書の量が増大し、

容易に同一の文書を印刷することが可能となったことに鑑み、ポリシーの策定段階において、これまでの文書管理の方法に問題が発見された場合には、その在り方についても考慮されるべきである。

（例）

対象	例
情報システム等	コンピュータ、基本ソフトウエア、応用ソフトウエア、ネットワーク、通信機器、記録媒体、システム構成図等
情報システムに記録される情報	アクセス記録、文書及び図面等の電磁的記録
これらの情報に接するすべての者	常勤、非常勤及び臨時を含む職員、委託事業者等

５．ポリシーの公開

基本的に各省庁の判断によるところとなるが、情報公開法の趣旨を踏まえ公開か非公開かが判断されることとなる。一般的には、すべてを公開することは情報セキュリティ上の問題が起こり得ることから、公開する範囲については慎重に検討する必要がある。

ただし、各省庁の取組みとして、一定の対策を行っていることを公開することは、各省庁の情報セキュリティに対する姿勢を示す意味でも重要であることから、可能な範囲で公開することが望ましい。

６．ポリシーに関する留意点

(1) 組織としてどのような基本方針の下に情報セキュリティを確保していくのかを明確にすること。

情報システムがさらされている脅威（例えば、盗聴、侵入、改ざん、破壊、窃盗、漏洩、DoS 攻撃等）から保護する情報資産を明らかにするとともに、情報資産ごとに機密性、利用環境等を考慮したリスクの度合いによる分類を行う。これによって得られる情報資産と各々のリスクの度合いが、情報セキュリティ対策を考える基礎となる。

また、情報セキュリティ対策を講じるための体制を確立し、業務を担当する者、情報システムを管理する者及び情報システムを利用する者等、同じ情報システムにおいても複数の者が関わることを十分認識した上で、権限と責任の範囲を明確化することにより、組織として情報セキュリティ対策が適切に進められるようにする必要がある。

(2) ポリシーの継続的な運用及び見直しについて、次の事項に留意すること。

◯ポリシーは、適切に導入・運用されて初めて意味のあるものであり、適切に導入・運用されないポリシーは策定されていないのと同じであること。

◯ポリシーは、平成 15 年度にその基盤が構築される電子政府の実現のための情報セキュリティの十分な確保を当面の目標として策定していくものであるが、当初から極めて高度なポリシーを策定することは、現実的に運用が極めて困難となる

可能性があることから、実態に即したポリシーを計画的に策定・運用し、その実施状況を踏まえて見直し、平成 15 年度までに目標を達成すること。

Ⅲ. ポリシーのガイドライン

１．ポリシーの位置づけと基本構成

ポリシーの体系は図 2 に示す階層構造となっている。最上位には、政府全体としての情報セキュリティ対策における根本的な考え方である「政府の情報セキュリティの基本的な考え方」がある。これに従い、順に「（各省庁）基本方針」、「（各省庁）対策基準」及び「（各省庁）実施手順」がある。ガイドラインにおいて「情報セキュリティポリシー（ポリシー）」とは、定義にもあるとおり「（各省庁）基本方針」及び「（各省庁）対策基準」を示し、「実施手順」は含まれない。「実施手順」には、これまでの文書や情報システムに関する利用規程等既に定められているもの（その規定についても、内容によっては対策基準に該当する項目もある。）から、今回のポリシーの策定によって新たに必要となる手順（例えば、緊急時の体制や、監視体制の運用方法等）が含まれる。ポリシーを上位である基本方針から策定するに当たり、現存の規定類は、必要に応じて見直す必要がある。

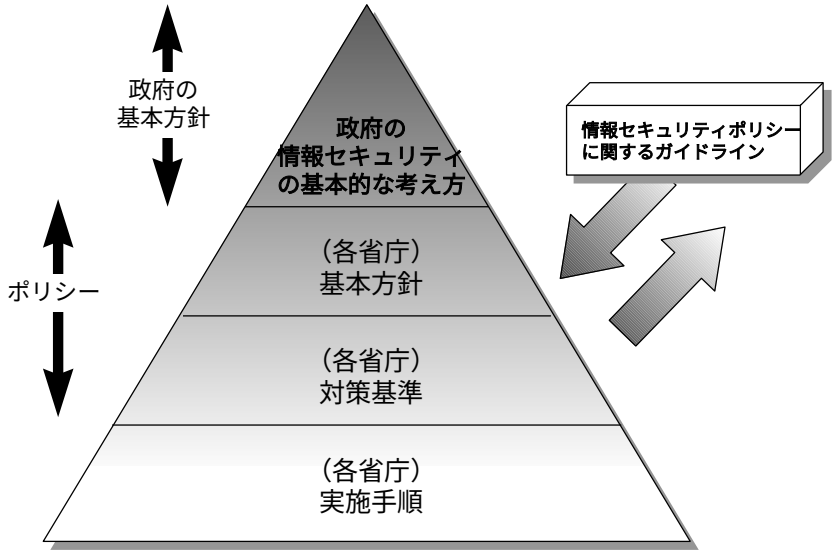

図２：ポリシーの位置づけ

２．策定手続

ここでは、ポリシー策定の手引きとして、ポリシーを策定する手続及びポリシーに定めるべき事項について示す。

(1) 策定手続の概要

ポリシーは、図 3 に示すとおり、策定のための①組織・体制を確立し、その組織・

体制の下で②基本方針の策定、③リスク分析及び④対策基準の策定を行い、⑤各省庁内において正式に定めるものとする。

また、各省庁においては、それぞれのポリシーに従い、対策基準に定められた事項を実施する手順を定めた⑥実施手順を策定することとなる。

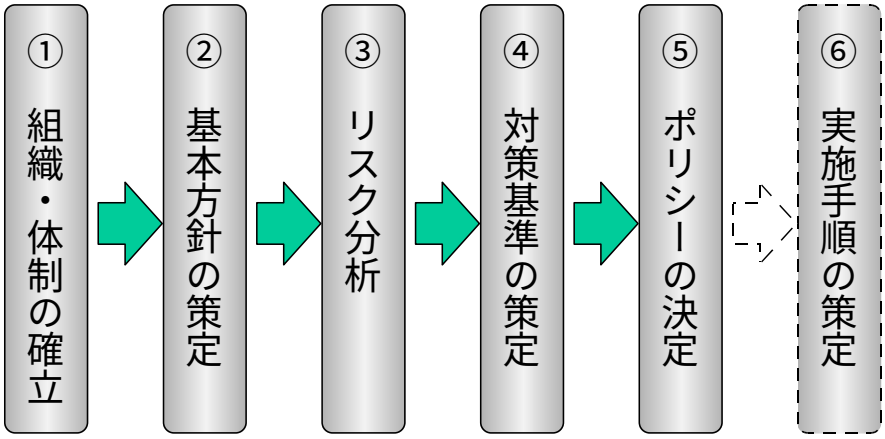

図３：ポリシー策定手続の概要

(2) 策定のための組織・体制

ポリシー策定には、組織の幹部の関与を明確にするとともに、その責任の所在を明確にするため、関係部局の長、情報システムの管理者及び情報セキュリティに関する専門的知識を有する者などで構成する組織（本ガイドラインでは、以下「情報セキュリティ委員会」とする。）を設ける必要がある。このため、ポリシーには、情報セキュリティ委員会の目的、権限、名称、業務、構成員等を定める。ポリシーでは組織内の様々な情報に係る問題を取り扱うことから、すべての部局等の関係者がこれにかかわることが考えられるが、中心的な構成員としては、次のような関係者を含むことが考えられる。

・情報システム関係（LAN 管理担当課等）
・技術関係（内外の技術的知識を有する専門家等）
・監査関係（政策評価、内部監査等を行う課又は官房総務課等）
・文書関係課
・人事関係課
・会計関係課
・広報関係課
・庁舎管理担当課

また、ポリシーの策定について、各部署の情報セキュリティ担当者となり得る者を体制に組み込むほか、必要に応じて職員からの意見を聴取し、疑問点に対し的確に説明できるようにする等、策定段階からポリシーが職員に理解されるような環境を醸成することが重要である。

なお、情報セキュリティ委員会による承認を受けて、ポリシー策定作業の一部を下

部の組織（策定作業班）に行わせることができる。やむを得ない場合、この策定作業班に外部の者を含めることができる。策定作業班に業務を行わせる場合、正式な辞令の発令等を伴う幹部からの承認を受けた組織を編成し、省庁内全職員には、幹部の命令に基づく任務であることを認識させることが重要である。

（例）

・情報セキュリティ委員会
次の組織の代表者からなる委員会を設置する。
・委員長　官房長
・情報システム課
・官房総務課
・官房文書課
・秘書課
・会計課
・広報課
委員会の庶務は、情報システム課が行う。
また、すべての局及び部の関係者として、各局総務課、Ａシステムの担当課（Ａ課）は、ポリシーの決定手続に加わることとする。
策定作業班の職員は、ポリシーを策定していく上で、省庁内の様々な部局等と調整を行うとともに、理解を求めていかなければならない。

(3) 基本方針の策定

各省庁の情報システムに求められる情報セキュリティの確保のため、それぞれの省庁が対策を講じることとする基本方針を定める。

この基本方針には、情報セキュリティ対策の目的、対象範囲など、各省庁の情報セキュリティに対する基本的な考え方を示す。

また、ポリシーを理解するために必要な用語について、その定義を定める。

なお、基本方針は、情報セキュリティに関する基本的な方向性を決定づけるものであることから、頻繁に更新される性質のものではないことに留意する必要がある。

(4) リスク分析

①概要

リスク分析とは、保護すべき情報資産を明らかにし、それらに対するリスクを評価することである。様々なリスク分析方法が考えられるが、ここでは具体的な方法の一つを示すこととする。

具体的な手順は次のとおりである。

(a) 各省庁の保有する情報資産を調査し、重要性の分類を行い、この結果に基づき、要求されるセキュリティの水準を定める。

(b) 各省庁の情報資産を取り巻く脅威を調査し、その発生頻度及び発生した際の被害の大きさからリスクの大きさを求める。

なお、一般的に両者の積をリスクの大きさとしている。

(c) リスクの大きさがセキュリティ要求水準を下回るよう対策基準を策定し、適切なリスク管理を行う。

なお、情報資産に変更があったとき、又は情報資産に対するリスクに変化が生じたときには、関係する情報資産についてリスク分析を再度行い、その結果ポリシーの見直しが必要となった場合にはその見直しを行う。また、定期的なポリシーの評価・見直しの際にも、リスク分析から再検討することが必要である。また、リスク分析の際に発見された情報資産の脆弱性で、早急に対応する必要のあるものについては、速やかに措置を講ずることが重要である。

リスク分析を行った結果の資料は、ポリシー策定の基礎資料として保管する必要があるが、当該資料には情報資産の脆弱性の分析が記されているため、厳重な管理が必要である。

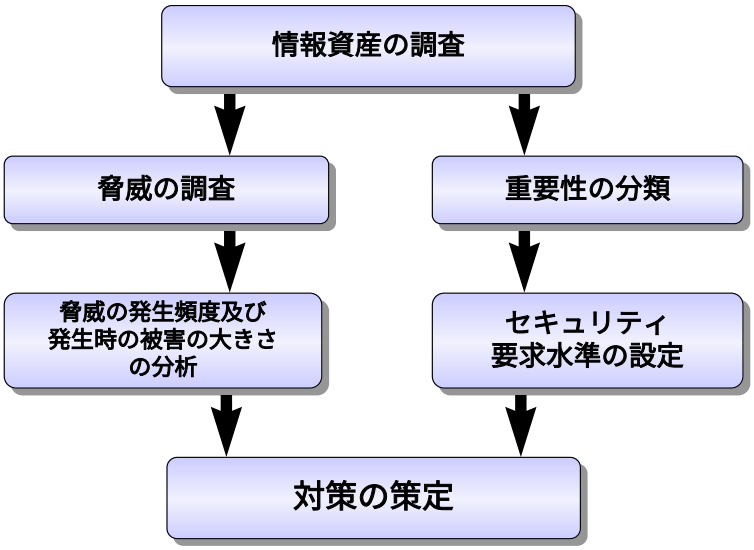

図４：リスク分析のフロー

②情報資産の調査

保護すべき情報資産を明らかにするにあたって、情報がどこにあり、誰が管理し、どのような状況で扱われているかについて調査する。

具体的な調査項目としては、次のものがある。このほか、リスク分析の結果等を検討した資料を作成する。

（例）

情報資産調査票	
情報資産	
用途	
管理者	
利用者（アクセス権限）	
保存（設置）場所	
保存（設置）期間	
重要性	Ⅰ・Ⅱ・Ⅲ・Ⅳ 機密性［Ⅰ・Ⅱ・Ⅲ・Ⅳ］

	完全性［Ⅰ・Ⅱ・Ⅲ・Ⅳ］ 可用性［Ⅰ・Ⅱ・Ⅲ・Ⅳ］

③重要性による分類

調査した情報資産に対し、機密性、完全性、可用性の 3 つの側面から重要性を検討し、情報資産を分類する。

この分類は、情報資産をどのように扱い、保護するかを決めるための判断基準となり、これに基づき要求されるセキュリティ水準が定められる。

（重要性の 3 つの側面）

(a) 機密性・・情報資産の機密に基づく重要性

(b) 完全性・・情報資産の完全性・正確性に関する重要性

(c) 可用性・・情報資産の利用可能性・継続性に関する重要性

（例）

重要性の分類
Ⅰ：セキュリティ侵害が、国民の生命、財産、プライバシー等へ重大な影響を及ぼす。
Ⅱ：セキュリティ侵害が、行政事務の執行等に重大な影響を及ぼす。
Ⅲ：セキュリティ侵害が、行政事務の執行等に軽微な影響を及ぼす。
Ⅳ：影響をほとんど及ぼさない。

（例）

重要性に基づくセキュリティ要求水準の設定（重要性の 3 つの側面を勘案して定める。）

重要性Ⅰ → セキュリティ要求水準１
重要性Ⅱ → セキュリティ要求水準２
重要性Ⅲ → セキュリティ要求水準３
重要性Ⅳ → セキュリティ要求水準４

④リスク評価

調査したすべての情報資産についてリスク評価を実施する。

(a) 取り巻く物理的、技術的、人的環境における脅威について調べる。

（脅威の例）
物理的脅威・侵入、破壊、故障、停電、災害等
技術的脅威・不正アクセス、盗聴、コンピュータウイルス、改ざん・消去、DoS 攻撃、なりすまし等
人的脅威　・誤操作、持ち出し、不正行為、パスワードの不適切管理等

(b) 各情報資産が直面するそれぞれの脅威に対するリスクの大きさについて、(a)脅威の発生頻度及び(b)発生時の被害の大きさから評価する。

なお、発生頻度及び被害の大きさを直接検討することに代えて、簡易的に発生頻度を情報資産の脆弱性に、被害の大きさを情報資産の重要性とする方法もある。

各情報資産について、全ての脅威に対してリスクの大きさを調査する必要がある。

（例）

（段階的な評価水準設定）
(a) 脅威の発生頻度
A：かなりの頻度で発生する。　（脆弱性がかなり大きい。）
B：時々発生する。　（脆弱性が大きい。）
C：偶発的に発生する。　（脆弱性が小さい。）
D：ほとんど発生しない。　（脆弱性がほとんどない。）
(b) 発生時の被害の大きさ
　重要性のランク付けと近似させる方法（つまり、重要性が大きい場合、被害の大きさも大きくなるとの考え方）がある。厳密に求めるには、重要性の3つの側面を勘案して定めることが必要である。
　＜被害の大きさ例＞
　ａ：　重要性Ⅰと同じ
　ｂ：　重要性Ⅱと同じ
　ｃ：　重要性Ⅲと同じ
　ｄ：　重要性Ⅳと同じ

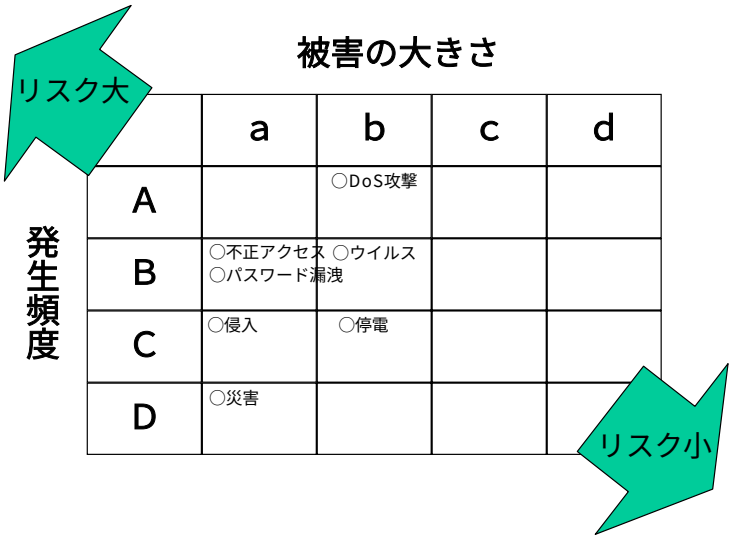

図５：リスク分析（例）

⑤リスクに対する対策

　リスク評価により定められた、情報資産の脅威ごとのリスクの大きさと、要求されるセキュリティ水準とを比較することにより、情報セキュリティ対策の方針が定められる。

　対策基準の検討において、算定されたリスクの大きさを基準として、発生頻度及び被害の大きさを低減させ、セキュリティ要求水準を満足させる対策基準を定める。また、脅威の発生頻度又は被害の大きさを低減させる対策には、脅威を防止するものだけでなく、実際に被害が発生した場合に、如何に情報を守るか、如何に改ざんされないか、如何に継続して使用できるようにするか（あるいは障害が起きても如何に早急に復旧できるか）、といった観点を考慮に入れながら、対策を講じることが重要である。

具体的には、情報資産の重要性を勘案して定められたセキュリティ要求水準を達成する対策を講じることとなるが、セキュリティ要求水準が高いほど、発生頻度及び被害の大きさ（リスクの大きさ）は小さくならなければならない。

例えば、リスクの大きさをセキュリティ要求水準まで低減させる方法は、次の 3 つに分類できる。

(a) 「アクセス権限の付与を必要最低限の者に限る」等被害の大きさを小さくすることによってリスクの大きさを低減させる方法。

(b) 「コンソールからのみログインを許可する」等発生頻度を小さくすることによってリスクの大きさを低減させる方法。

(c) 「情報システムの改ざんなどを検知する」等被害の大きさと発生頻度のいずれも小さくすることによってリスクの大きさを低減させる方法。

具体的に定める対策は、情報資産及びその脅威の内容に応じて、利用者の利便性を考慮した効果的かつ効率的なものとする必要がある。

（例）対策基準の検討（不正アクセス）

リスク評価の結果（発生頻度Ｂ、被害の大きさａ）

↓

「不正アクセス」のリスクを低減させるための**対策基準の検討**

○アクセス権限の付与を必要最低限の者に限ること。
○コンソールからのみログインを許可すること。
○修正プログラム（パッチ）を導入すること。
○アクセス記録を監視・記録すること。
○情報システムの改ざんなどを検知すること。
○緊急時対応により情報資産を保護すること。等

↓

リスクの低減（発生頻度Ｃ、被害の大きさｃ）

(5) 対策基準の策定

リスク分析の結果によって得られた各情報資産に対する個々の対策について、体系化した上で対策基準を定める。

①構成

対策基準の構成は、次のとおりとする。

(i) 組織・体制
(ii) 情報の分類と管理
  (a) 情報の管理責任
  (b) 情報の分類と管理方法
(iii) 物理的セキュリティ
(iv) 人的セキュリティ
  (a) 役割・責任及び免責事項
  (b) 教育・訓練
  (c) 事故、欠陥に対する報告

(d) アクセスのための認証情報等の管理
(e) 非常勤及び臨時職員等の雇用及び契約

(v) 技術的セキュリティ
(a) コンピュータ及びネットワークの管理
(b) アクセス制御
(c) システム開発、導入、保守等
(d) コンピュータウイルス対策
(e) セキュリティ情報の収集

(vi) 運用
(a) 情報システムの監視及びポリシーの遵守状況の確認（運用管理）
(b) 運用管理における留意点
(c) 侵害時の対応策
(d) 外部委託による運用契約

(vii) 法令遵守

(viii) 情報セキュリティに関する違反に対する対応

(ix) 評価・見直し

②組織・体制

情報セキュリティの確保のための組織・体制については、幹部が率先して情報セキュリティの確保を推進することが重要であることから、情報セキュリティについて最高責任者（最高情報セキュリティ責任者(CISO[5])）を定め、その責任及び権限を明確にする必要がある。具体的には、この最高責任者を長とする情報セキュリティ委員会（策定時の委員会と同じ）に対して、日々のポリシーの遵守状況の確認体制の確立、導入の際の改善点（現実との齟齬）の調査及び見直し、並びに教育・啓発活動を行う役割を担わせることになる。

ポリシーには、最高情報セキュリティ責任者及び情報セキュリティ委員会の目的、任務、権限等を定めるとともに、構成員及び事務局、監査班等の設置を定める。また、委員会の任務が確実に遂行されるために必要な事務局及び監査班の体制及び権限について定める。特に、ポリシーの遵守状況の確認体制については、監査班の任務を定め、実施状況に関する監査、予算、組織等の措置状況について確認をし、委員会へ報告する体制を整備する。

[5] Chief Information Security Officer

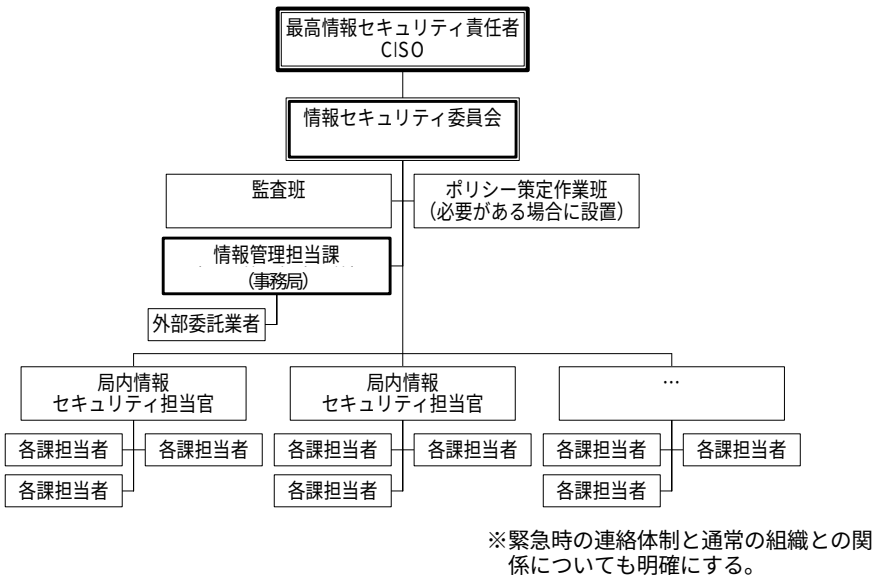

図６：組織図例

③情報の分類と管理

リスク分析によって行われた情報の管理方法に関する分類ごとに情報の管理の方法を定める。

(i) 情報の管理責任

それぞれの情報について、誰が管理責任を負うのかについて定める。情報を管理する者及び利用する者の 2 つの責任が考えられるが、それぞれ、具体的な責任と役割を定める必要がある。

また、情報管理責任者を各課において定めることとし、当該課において作成された文書の管理の責任を負うこととする。また、作成中の文書、電子メール等の管理責任が定められていない情報については、個人において適切に管理しなければならないことを定める。

（例）

情報は当該情報を作成した課部局等が情報管理責任者として管理責任を有する。 Ａ局として作成された情報　→Ａ局総務課 Ａ局Ｘ課として作成された情報　→　Ａ局Ｘ課 省として作成された情報　→　大臣官房総務課（又は、管理責任者として指定された課）

(ii) 情報の分類と管理方法

省庁が保有する情報について、リスク分析における情報資産の分類結果を踏まえ、その分類と管理方法を定める。

具体的には、情報の分類、情報の分類に関する表示のほか、情報の管理方法としてのアクセス権限の設定、暗号化、媒体の管理、情報の変更又は廃棄の管理、分類の有効期限等について定める。

また、既に分類された情報が複製された場合又は伝送された場合には、当該複製等もその分類に従い管理する。

（例）

A　原則

当省内の情報は、情報公開法の趣旨を踏まえ公開、非公開について定めることとする。

（以下、個人のプライバシーに関する情報や、情報セキュリティ上問題が生じる可能性のある情報等、情報公開法の趣旨を踏まえ公開することが不適当と判断される情報について必要に応じて定める。）

B　情報の分類に関する表示

印刷したもの、ディスプレイ等への表示、記録媒体へ格納する際の媒体（FDへのラベル等）、ファイル名等について第三者が重要性の識別を容易に認識できないよう留意しつつ、分類がわかるように必要な表示を行わなければならない。

C　情報の管理（分類ごとに定める。）

(a) アクセス権限の設定と暗号化

情報の分類ごとに、アクセス権限を設定する。秘密とされた情報は必ず暗号化を行い、暗号鍵と別に厳格に管理しなければならない。

(b) 媒体の管理

秘密情報を記録した記録媒体（FD、MO、CD-R、DAT、MT、DVD-RAM 等）は、施錠可能な場所に保管する。

(c) 情報の変更又は廃棄の管理

情報の変更又は廃棄に当たっては、情報管理責任者の承認を得て行うこと。また、作業の日付、作業担当者及び処理内容の履歴を保持すること。秘密情報を削除するときは、記録媒体の初期化など情報を復元できないような処理を実施すること。

④物理的セキュリティ

情報システムの設置場所について、不正な立入り、損傷及び妨害から保護するための適切な設備の設置、出入管理及び執務室にあるパソコン等の盗難対策等物理的な対策について具体的な項目を定める。

なお、モバイル機器を利用した情報漏洩を防ぐ等、今後のモバイル機器の普及等を考慮した対策について検討する必要がある。

また、無線 LAN について、物理的セキュリティにおいて設置の可否の基準を定めるとともに、設置を許可する場合の暗号、認証について技術的セキュリティの項目で基準を定める。

（例）

コンピュータ等の機器及びネットワーク機器について、リスク分析に基づいたⅠ、Ⅱ、Ⅲ、Ⅳの分類に応じて、適切な物理的対策を講じなければならない。

Ⅰ　二重鍵及び IC 認証カードの採用、監視カメラの設置、防磁壁の設置、入退出管理の徹底、消火設備の設置、配線の防護。

Ⅱ　機器への鎖の設置、配線の防護。

Ⅲ　…

これらの機器は、当該機器の管理責任課において、適切に管理をしなければならない。

⑤人的セキュリティ

情報セキュリティの向上は、利便性の向上とは必ずしも相容れないものであり、利用者の理解が得にくい場合もあることから、十分な教育及び啓発が講じられるように必要な対策を人的セキュリティとして定める必要がある。

(i) 役割・責任、免責事項

基本方針で定めた対象範囲のうち、各対象者の情報セキュリティに関する役割・責任（誰が責任をとるのか、管理職・職員の役割）及び外部業者との関係（プログラム開発担当者との関係も含む。）について定める。

免責事項については、例えば、自らの責任となる情報セキュリティ障害について、積極的にその障害について申告した場合は免責されることを定める等、ポリシーを円滑に運用するために必要な事項を定める。

(a) 最高情報セキュリティ責任者

すべての情報セキュリティに関する権限及び責任を持つこと、また、運用に関し、重大な事項に関する決定権限を持つ等の役割を定める。

(b) 情報セキュリティ担当官（管理職等）

各課部局において情報セキュリティ担当官を設置すること、各組織における指示系統、意見の集約及び責任等果たさなければならない職務の規定等を定める。例えば、各課の職員は、ポリシーに関する違反や問題が起こった際には、情報セキュリティ担当官に連絡し、助言又は指示を仰ぐこと、又はどのような場合に情報セキュリティ担当官が最高情報セキュリティ責任者に報告すべきか等を定める。

(c) システム管理体制

情報セキュリティ対策において重要な役割を担うシステム管理体制について、その体制、責任、権限を定める。

（ア） システム管理者

情報システムの整備・運用・管理を実施するシステム管理者の設置を定め、自身の管理する情報システムに関し、ポリシーの遵守等の情報セキュリティに係る責務を明確にする。また、システム管理者が管理する情報システムに関し、実施手順を定めるなどポリシー遵守に必要な措置を講ずるほか、ポリシーの範囲内で部局等によらず必要な権限を行使できる旨を定める。

なお、本権限行使に関する調整、監督は、情報セキュリティ委員会が行う。

（イ）システム管理要員

情報セキュリティ対策を適切に実施するために十分な管理要員の配置について定める。システム管理要員は、システム管理者の命に従い、システム管理作業を行う。

(d) 職員等

・情報セキュリティ対策の遵守義務

職員がポリシー及び実施手順（個別マニュアルとしてもよい）に記載されている内容を遵守して、情報セキュリティ対策を有効に機能させる義務があること、不明な点に関する助言の推奨等を定める。

・外部委託に関する管理

各省庁が省庁外の業者（受託事業者から下請けとして受託した業者を含む。）等に情報システムの開発及び運用管理を委託する場合には、対象範囲にしたがってポリシー、実施手順の遵守義務が当該業者に発生することを認識し、これを遵守させる必要があること、そのための教育の実施を行うこと、ポリシーが遵守されなかった場合の規定（損害賠償等）を契約書に明記すること等を定める。

また、受託業者は、情報セキュリティ上重要な情報を取り扱う可能性があることから、受託業者及び情報セキュリティ上重要な情報を取り扱う者の技術的能力、信頼性等について考慮する必要がある。

なお、外部委託に関する契約については、⑥(iii)「システムの開発、導入、保守等」、⑦(iv)「外部委託による運用契約」の項についても合わせて考慮する。

・非常勤及び臨時職員

非常勤及び臨時職員についても、職員に準じた責任及び役割があることを定める。

・その他

情報セキュリティに係わる職員等が、異動、退職等により、業務を離れる場合には、当該職員等が知り得た情報が情報セキュリティ上問題となるおそれがあることに留意する必要がある。

(ii) 教育・訓練

ポリシーの実施の一部は、情報システムに組み込まれた技術的措置によって自動的に実現することが可能であるが、多くの部分は組織の責任者及び利用者の判断や行動に依存している。したがって、情報セキュリティに対する意識を醸成し、また保つために、幹部を始めとしたすべての職員が情報セキュリティの重要性を認識し、ポリシーを理解し、実践するための教育・訓練を計画的に実施する必要がある。

これは、不正アクセスから防御することはもとより、コンピュータウイルスの混入、内部者による情報の漏洩、外部への攻撃などを防ぐ観点からも重要である。

具体的には、研修、説明会の実施及びその他の啓発活動を実施することを定める。新入職員への初任者研修にも取り入れる等、積極的な教育が必要である。

(iii) 事故、欠陥に対する報告

職員は、情報セキュリティに関する事故やシステム上の欠陥を発見した場合には、独自にその事故又は欠陥の解決を図らずに速やかに情報セキュリティ担当官に報告をし、その指示を仰ぐことが必要である。その事故又は欠陥による被害を拡大しないためにも、この報告義務及びその方法を定める。

また、電子申請・届出等の実施に伴い、国民が政府の情報システムを利用し、重要な情報のやり取りを行う機会が増えることから、国民からの事故・欠陥に対する報告・連絡も適切に受理し、対応を行うために必要な基準を定める。

(iv) アクセスのための認証情報等の管理

情報システムへアクセスするための認証情報（ID・パスワード、バイオメトリックス認証に係る情報等）及びこれを記録した媒体（IC カード等）（以下「認証情報等」という。）は、人的セキュリティに起因して侵害されやすい情報である、管理者からの認証情報等の発行からユーザでの管理に至るまで、人的な原因で漏えいするリスクを最小限とするための基準を定める。具体的には、ユーザにおける認証情報等の管理に関する基準を定める。特に、ID・パスワードについては漏えいしやすい情報であるため、ユーザにおける管理方法を明示するとともに、アクセス制御機能において文字数等によるパスワードの制限を行うなど、これを補完するための技術的セキュリティとの有効な連携が必要である。

（例）

①パスワードの管理

利用者は、パスワードについて次の事項を遵守しなければならない。

・パスワードを秘密にしておくこと。
・パスワードのメモは作らないこと。ただし、メモが安全に保管される場合はその限りではない。
・情報システム又はパスワードに対する危険のおそれがある場合は、パスワードを変更すること。
・適切な長さを持つパスワードを選択すること。その文字列については、想定しにくいものにしなければならない（詳細は実施手順で定める。）。
・パスワードは定期的に、若しくはアクセス回数に基づいて変更し、古いパスワードの再利用をしてはならない。管理者用パスワードはさらにこのサイクルを頻繁にすること。
・利用者のパスワードは他人に使用させないこと。
・モバイル機器にパスワードを記憶させてはならない。

②IC カードの管理

利用者は認証用の IC カードについて次の事項を遵守しなければならない。

・認証用の IC カードは厳重に管理すること。
・認証用の IC カードを紛失した場合には直ちにシステム管理者へ届け出ること。
・その他認証用の IC カードの利用についてシステム管理者が定める事項を遵守すること。

(v) 非常勤及び臨時職員等の雇用及び契約

非常勤及び臨時職員にも、情報セキュリティの確保の観点から、ポリシーの遵守について明確に理解させる必要がある。特に、パソコンを使用する作業を行わせる場合、当該パソコンのアクセス管理や当該職員が有する情報システムへの権限などを明確にし、これらの職員による不正アクセス等を防ぐことが必要である。

したがって、非常勤及び臨時職員等の雇用について、ポリシーの周知徹底を行い、同意書に署名させる等、当該職員に対して行わなければならないことを定める。

⑥技術的セキュリティ

(i) コンピュータ及びネットワークの管理

情報システムの運用管理手順やネットワーク管理、記録媒体の保護、他の組織とデータ交換を行う際の留意点や規定について定める。

リスク分析の結果に従い、機器の取扱い、管理の方法を定める。

（例）

情報資産の分類に従って、情報を以下のとおり管理する。

I

・すべてのアクセス記録を取得し、一定期間保存すること。また、定期的にそれらを分析、監視すること。

・情報システムの更新については、内容、必要性、計画を文書にて管理責任者に提出し、承認を受けた上で行う。代替機による動作確認、検証の後に本体への更新を行わなければならない。更新の際には、現状の保存を行い、復帰が即座に可能な状態にしておき、原則として執務時間外に行わなければならない。

・緊急時に直ちに対処できるようにするため、特に重要なシステムとして情報セキュリティ委員会が定めるシステムには、非常用の予備システムを準備すること。

・非常用の予備システムの動作検証を少なくとも四半期ごとに行うこと。

・定期的に管理者の教育を行うこと。

・定期的に情報システムのバックアップ用の複製を取ること。

II

・情報システムに重大な影響を与える可能性のあるものとして、情報セキュリティ委員会が定める操作については、すべてのアクセス記録を取得し、一定期間保存すること。

・情報システムの更新については、内容、必要性及び計画を文書にて管理責任者に提出し、管理責任者が情報システムに重大な影響を与えると判断した場合は、最重要の手順、又は現状復帰の準備を整えつつ原則として執務時間外に行う。影響が少ない場合は、管理責任者の指示により作業を行うこと。

・定期的に情報システムのバックアップ用の複製を取ること。

III

・ネットワークに接続する情報システムについては、手順書に従い必要な項目を申請した上で、管理責任者の承認を得た上で接続を行うこと。

各情報システムの設定については、個別に実施手順書に定める。

IV

・取扱は自由。ただし、無断でネットワークに接続してはならない。

また、利用者に対する情報システム使用の規定について定める。

（例）

情報システムを使用する際の規定

○業務目的以外の使用の原則禁止

職員による情報システム、ネットワーク資源の使用は、原則業務目的に沿っ

たものが許可される。業務目的以外での業務システムへのアクセス、メールアドレスの使用及びインターネットへのアクセスを行わないこと。

◯業務上のデータの持ち出しの禁止

職員は、分類上Ⅰに該当する業務上データを省庁外に持ち出してはならない。また、分類上Ⅰに該当する情報資産の設置場所に、個人の所有するデータが記録された媒体を持ち込んではならない。職員の所属する組織の長（課であれば課長、室であれば室長）の許可がある場合には、この限りでない。

例えば、携帯端末又は記録媒体に格納された情報の省庁外への持ち出し又は当該情報資産が設置されている執務室内への持ち込み、及びネットワークを介してのデータ転送（メールによる個人アドレスへのデータの送信、又はその逆等）等を行う際は、許可を必要とする。

◯無許可ソフトウエアの導入の禁止

職員は、各自に供用されたパソコンに対して、情報システム管理課で認められていないソフトウエアの導入を行わないこと。特にネットワーク上の情報を盗聴するような監視ソフトウエアや、ネットワークの状態を探索するセキュリティ関連のソフトウエア及びハッキングソフトウエアの使用は厳禁する。

業務を円滑に遂行するために必要なソフトウエアについては、個別に情報セキュリティ担当官の許可を得て利用することができる。

◯機器構成の変更の禁止

職員は、各自に供用されたパソコンに対して、機器の増設／改造を行わないこと。特にモデム等の機器を増設して他の環境（インターネット等）へのネットワーク接続を行うことや、省庁外からのアクセスを可能とする仕組みを構築することは禁止する。

(ii) アクセス制御

情報へのアクセスは、業務要件に従って許可される必要があることを定め、利用者の権限と責任について言及する。システム管理者側において措置すべきパスワードの管理方法やシステム管理者の権限を定める。重要なシステムは、特殊の個人認証方法を採用する等システムに応じたアクセス制御についても定める。また、外部から利用者の接続を許可する場合（いわゆるモバイル端末による接続等）の基準、情報及び情報システムへのアクセス要件等を定める。

なお、地方支分部局等からの専用線等による接続がある場合、当該接続についても、適切なセキュリティが確保されている必要性があることから、状況に応じて、これらの接続に係るアクセス制御等の対策を行うことが重要である。

（例）

◯利用者登録（ユーザ登録）

情報システムに対するアクセスを許可するための正式な利用者登録及び登録抹消手順を定めることとする。

◯ログイン／ログアウト時の留意点

（実施手順に具体的な設定方法を定める。）

◯メール自動転送の制限

◯サーバへのアクセス権限の付与

(iii) システム開発、導入、保守等

新たに情報システムの開発又は導入若しくは更新をしようとする場合は、ポリ

シーに従ってリスク分析を行い、適切な情報セキュリティ対策を施すために必要な事項について定める。また、システム開発等を受託する者に対する必要な事項を定める。

これらの新たな機器、ソフトウエア、媒体及びサービスの導入の際には、事前に不具合の確認等のセキュリティに関する確認を行うことが重要である。また、これらの仕様書等についても取扱いには注意する必要がある。

廃棄、修理又は返却する機器については、その機器に存在する情報が、外部に漏洩することを防ぐため、例えばハードディスクを廃棄する際には、内容を読み出せないような措置を施してから廃棄する等の取扱いについて定める。

（例）

・守秘義務 ・再委託管理 ・情報システム仕様書等の管理 ・各種政府調達に係る指針[6]の要件（ISO15408 等） ・作業区域、作業管理 ・作業中の情報セキュリティにかかわる事故への対応 ・作業報告書の提出 ・機器の搬入出時の手続き ・導入時の脆弱性試験 ・ソースコードの提出 ・その他の情報システムに応じたポリシーを遵守するための要件

また、保守のための規定として、監視体制及び情報システムの修正に関する規定についても定める。この際、⑦(iv)「外部委託による運用契約」の項についても考慮する。

（例）

情報システムの 24 時間監視体制、システムの修正プログラム（パッチ）の導入決定に係る方針、時期等

(iv) コンピュータウイルス対策

コンピュータウイルスに感染することを防止するために必要な対策を定める。コンピュータウイルスに対応するためのシステム整備、職員の守るべき規定等を定める。コンピュータウイルスが発見されたときの対応については、侵害時の対応として定める。

（例）

---

[6] 政府調達に係る主な指針

ハードウエア、ソフトウエア及び役務サービスを調達する場合に遵守するべき以下の方針の中で、情報セキュリティ確保の観点からの情報機器の基準、外注時の留意事項等について定められている。

・「各省庁の調達におけるセキュリティ水準の高い製品等の利用方針」（平成１３年3月２９日、行政情報化推進各省庁連絡会議了承）

・「国の行政機関における情報システム関係業務の外注の推進について」（平成１２年3月３１日、行政情報システム）各省庁連絡会議了承）

①許可されていないソフトウエアの導入の禁止（法令遵守とも関連）
②外部ネットワークからファイル及びソフトウエアを取り入れる際には、サーバ側、端末側においてウイルス対策ソフトを実行
③サーバ側、端末側のワクチンソフトについては、ワクチンプログラムを常に最新のものにバージョンアップするとともに、ウイルス情報の更新を頻繁に行うことが必要
④重要なソフトウエア、情報システム及び情報について、その内容を定期的に確認

(v) セキュリティ情報の収集

セキュリティホールは、日々発見される性質のものであることから、積極的に情報収集を行う必要がある。このため、情報収集の体制、分析の手順、情報収集先等を定める。深刻なセキュリティホールが発見された場合、直ちに対応できるよう留意する必要がある。

⑦運用

(i) 情報システムの監視及びポリシーの遵守状況の確認（以下「運用管理」という。）

ポリシーの実効性を確保するため、また、不正アクセス及び不正アクセスによって他の情報システムに対する攻撃に悪用されることを防ぐためには、情報システムの利用者等が、ポリシーを遵守しているかどうかについて、また、インターネットを介した不正アクセスを含めた情報システムの稼働状況について、ネットワーク監視等により常に確認を行うことが必要である。したがって、ポリシーの各対象者による自己確認及び情報管理担当課による自動監視装置等の活用等によるネットワーク監視等を適切に実行することを定める。これらは、ポリシー遵守の確保のみならず、ポリシーそのものの問題点やポリシーが実態に整合的であるかどうかを評価するためにも重要である。

運用管理を適切に実施するためには、一部の担当者に大きな負担とならないような体制を構築することが重要である。また、システムが稼働している間は、常時監視しなければならず、障害が起きた際にも、速やかに対応できる体制である必要がある。このため、リスクに応じた侵入検知装置等の設置、監視体制の整備等の必要な措置を定める。また、アクセス記録の取得・分析についても、明確に行うことを定める。アクセス記録は、時刻等の記録内容の正確性を確保するために消去や改ざんを防止するなど、適切に保管するための措置を講ずる。

なお、詳細な内容（アクセス記録の保存期間、監視の人数体制等）は実施手順として定める。

(ii) 運用管理における留意点

利用者の電子メールを閲覧する等のシステムソフトウエア、セキュリティ管理ソフトウエアを使用する行為によって国民のプライバシーに対する侵害があってはならない。また、セキュリティ対策として行われる場合においては、職員のプライバシーの問題にも影響することを考慮する必要がある。このため、これらのソフトウエアの使用については、どのような条件が揃ったときに、どのような体制で当該ソフトウエアを使用できるのかについての規定を定める。

なお、これについて、利用者の理解を得ておくことが望ましい。

（例）

システム管理者は、情報セキュリティ上の問題が起こる可能性のあるものとして責任者（管理職）が認めた場合のみ、責任者又は責任者が予め指定した者が立ち会うことにより利用者個人の電子メールを閲覧することができる。

(iii) 侵害時の対応策

情報セキュリティが侵害された場合、又は侵害されるおそれがある場合等における具体的な措置について、緊急時対応計画として定めることが必要である。

緊急時対応計画には、情報資産への侵害が発生した場合等における連絡、証拠保全、被害拡大の防止、復旧等の必要な措置を迅速かつ円滑に実施し、再発防止の措置を講じるための一連の業務を定める。

特に、原因究明に基づく対策、原因者特定、法的措置等に備えるための十分な証拠の保全、迅速な被害回復が行えるよう、検証や訓練などにより十分確認して策定する。

また、自らが所有する情報資産における被害拡大防止のほか、外部への被害拡大のおそれがある場合には、その防止に努める。情報が漏洩することにより被害を被るおそれのある関係者に対し早急に連絡することが重要である。

なお、当該事案が不正アクセス禁止法違反等の犯罪の可能性がある場合には、警察・関係機関と緊密な連携に努める。

このほか、実施手順として明快な緊急時マニュアルを管理者及び利用者向けに作成する。

◯緊急時対応計画に盛り込むべき事項

(a) 連絡先

連絡先、連絡担当者、連絡手段を定める。

（例）情報集約担当者（連絡窓口）、情報資産管理部署・省庁内の連絡体制、内閣官房内閣安全保障・危機管理室情報セキュリティ対策推進室、警察等の関係機関、その他

(b) 事案の調査

侵害事案を把握するために必要な調査方法・項目を定める。

（例）症状の分類、原因の特定、被害・影響範囲の把握、記録

(c) 事案への対処

対処措置の判断基準、責任者、実施者、実施手順等を定める。

（例）連絡、ネットワークの切断、情報システムの停止、記録の取得（アクセス記録、対処行動記録等）、復旧、再発の監視

(d) 再発防止の措置

事案の検証を行い、再発防止のための措置を定める。

（例）情報セキュリティ委員会への報告、当該事案に係るリスク分析、再発防止計画の策定（ポリシー評価を含む。）

(iv) 外部委託による運用契約

外部委託による運用を実施する際には、ポリシーを遵守するための必要な要件

を契約等に定める必要がある。具体的には、次の例の要件のうち外部委託の内容に応じて必要なものを明確化する必要がある。

（例）
・守秘義務
・再委託管理
・システム管理記録・障害記録の提出・管理
・情報システム仕様書等の管理
・監視に係る措置
・緊急時の措置
・情報セキュリティに関する情報の収集
・ソフトウエアのバージョン管理
・その他の情報セキュリティを継続的に維持するための要件

⑧法令遵守

関連する法令への遵守等について定める。遵守すべき法律や行政指導として、どういうものが存在するかを列挙し、法令違反が起こらないようにすることが目的である。例えば、著作権法、不正アクセス禁止法、個人情報保護法等がある。

⑨情報セキュリティに関する違反に対する対応

ポリシーに違反した関係者及びその監督責任者に対しては、その重大性に応じて国家公務員法上等の懲戒の対象となり得ることをポリシーに定める。これは、ポリシー及び実施手順を軽視する傾向のある職員等に対する抑制策となるとともに、求められる情報セキュリティ水準の確保のためにも必要である。

なお、業務中に情報セキュリティに係る違反的な行動がみられた場合には、上司等の指示により直ちに端末の利用を停止させる等の迅速な対応ができるようにする必要がある。

⑩評価・見直し

ポリシーには、ポリシー及び情報セキュリティ対策の評価、情報システムの変更、新たな脅威等を踏まえ、定期的に対策基準の評価・見直しを行うことを定める。また、情報セキュリティ委員会の権限として、ポリシーの評価・見直しの実施を定める。

(i) 監査

情報システムの情報セキュリティについて、監査を行い、その結果をポリシーの評価・見直しに反映させる必要がある。

委員会の監査に関する責務を明確化し、それに必要な体制、権限を定める。

監査班等の監査を行う者は、組織内の情報セキュリティ対策の監査・報告について中立性を保証され、監査に必要な情報へのアクセス等の権限が明確に与えられる必要がある。また、監査作業に伴う情報漏えいのリスクを最小限とするため、監査班等が取り扱う監査に係る情報について、これらの保管・管理、守秘義務等の基準を定める。

監査を行う者は、十分な専門的知識を有するものでなければならない。また、適正な監査の実施の観点から、監査の対象となる情報システムに直接関係しない

者であることが望ましく、外部の活用も考慮に入れるべきである。

(ii) 点検

ポリシーに沿った情報セキュリティ対策の実施状況について、利用者に対するアンケートや自己点検を行うことを定める。これらの結果は、実態に即したポリシーへの更新を行う際に必要な情報として活用するものである。

(iii) ポリシーの更新

ポリシーの更新は、策定の場合と同様に、情報セキュリティ分野の専門家による評価も活用しつつ、関係部局の意見等を踏まえ、その妥当性を確認する手続を経ることが必要である。

ポリシーには、関係部局からのポリシーの更新案に対する意見を反映させるための手続を定め、情報セキュリティ委員会によるポリシーの決定を必要とすることを定める。

(6) ポリシーの決定

策定されたポリシー案については、情報セキュリティ分野の専門家による評価、関係部局の意見等を踏まえ、その妥当性を確認する手続を経ることが必要である。

ポリシーには、関係部局からのポリシー案に対する意見を反映させるための手続を定め、各省庁における正式なポリシーの決定を必要とすることを定める。

３．導入

(1) 導入作業の概要

ポリシーの運用開始までに、ポリシーを関係者に周知徹底し、確実に実施するための措置を行う。

(2) 実施手順の作成

実施手順はポリシーに記述された内容を具体的な情報システムや業務においてどのような手順に従って実行していくかについて定める。この実施手順は、ポリシーを遵守しなければならない者全員について、各々の扱う情報、実施する業務等に応じて情報セキュリティを確保するためにどのようにしなければならないかを示すいわゆるマニュアルに該当するものである。したがって、業務を実施する環境に応じて、必要のある場合には個別に定める必要がある。また、既存の規定等で対応できる事項については、適用される規定を定めることが必要である。

特に、担当する者が異動する場合においてもセキュリティ水準を維持するほか、各部署、地方局等で情報システムを相互接続する場合において一律なセキュリティ水準を確保するなど、実施手順は、ポリシーに基づく対策の手順をルール化することによる対策の継続性、一貫性の確保という点で非常に重要である。

なお、実施手順は、対策基準に基づき個別の目的のために作成し、評価・見直しなどの実施サイクルを柔軟に行うことが有効であるから、必ずしも情報セキュリティ委員会による承認を受けることなく、システム管理者等において策定、更新及び廃止す

ることができることとする。

(3) ポリシーへの準拠

情報セキュリティ委員会は、ポリシーの運用開始に先立ち、実態及び実施手順のポリシーへの準拠状況の検証を情報セキュリティ担当官に実施させる。準拠状況を収集・検討し、適切な助言、措置等を行った上で運用を開始する。

情報セキュリティ担当官は、自分の責任範囲におけるすべての情報資産について導入された、物理的セキュリティ対策、人的セキュリティ対策、技術的セキュリティ対策、緊急時対応計画及び実施手順が、ポリシーに準拠しているかどうかを検証する。

(4) 配布及び説明会

情報セキュリティ委員会は、ポリシーを関係者に周知するための、ポリシーの配布や説明会を行う。また、実施手順については、各課部局において行う。

外部委託業者等についても必要に応じて該当部分の配布等を行うとともに、ポリシーへの準拠を合意させることが望ましい。

なお、実施手順については、外部に漏洩しないよう、厳重に取り扱うことを関係者及び外部委託業者等に対して徹底する。

４．運用

ポリシーを確実に運用していくために組織・体制の確立、監視、侵害時の対応等の措置を適切に行う必要がある。

(1) 運用管理

情報セキュリティ委員会の下で、情報管理担当課及び各課部局の情報セキュリティ担当官は、ポリシーに従って、物理的セキュリティ対策、人的セキュリティ対策、技術的セキュリティ対策等が適切に遵守されているか確認する。

情報セキュリティ上重大な問題が生じる可能性のあるポリシー違反が発見された場合には、緊急時対応計画に従って処理する。

これらの結果は侵害事案の証拠となるほか、ポリシーの実効性を測る資料となるので、厳重に保管し、評価・見直しの際に活用する。

(2) 侵害時の対応

①訓練の実施等

緊急時対応計画の円滑な実施のため、定期的に訓練を実施する。訓練の結果を踏まえ、緊急時対応計画の評価・見直しを適切に実施する。

②連絡における留意事項

連絡手段は、情報セキュリティ上安全なものを用いる。（重要な内容については、メールを利用しないようにする等、盗聴等による脅威を増加させないようにする。）

情報セキュリティ上重要な任務を担う者は、２４ 時間連絡をとれる手段を複数用意することが望ましい。

③調査における留意事項

調査に時間をとられることによって、必要な連絡に遅れがあってはならない。

④対処における留意事項

対処を実施する際に、責任者の許可無く担当者が実施できる範囲、責任者の許可が必要な範囲を定める。また、責任者との連絡が不可能な場合の権限の委任、事後報告についても考慮する。

⑤再発防止計画

再発防止計画については、当該侵害に関するリスク分析の結果を踏まえ、ポリシー、各種措置、緊急時対応計画、実施手順の評価・見直しに係る検討結果を具体的に示す。

５．評価・見直し

ポリシー及び情報セキュリティ対策の評価、情報システムの変更、新たな脅威等を踏まえ、定期的に対策基準の評価・見直しを適切に行うことが重要である。ポリシーを常に実態に即したものとし、情報セキュリティ水準を高く保つためにも、この評価・見直しについては、情報セキュリティ委員会の下で行うことが必要である。

(1) 監査

各省庁は情報セキュリティ対策を実施するに当たり、客観的な視点からポリシーに基づいた対策が適切に行なわれていることを説明できることが重要であり、このため監査を適切に実施することが必要である。

これを踏まえ、委員会において適切な対策状況のレビューを実施する。具体的には、委員会は計画的なポリシーの遵守状況を監査するものとし、この作業を監査班に行わせる。

また、システム管理者は、監査に必要な記録等の適正な保管・管理を実施するとともに、情報システムの開発、導入、運用時において、情報システムの脆弱性調査等必要なシステム監査を活用するなどポリシーの遵守について確認する。

外部の機関を活用して監査を行う場合、当該機関に情報システムの弱点が知られることになるということを十分留意の上、信頼性について慎重な検討を行い、機関の選定を行うことが必要である。

(2) ポリシーの更新

特にポリシー導入後の最初に行われるポリシーの更新においては、ポリシーと実態との相違を十分考慮することが重要であることから、関係部局の意見聴取等を行い、実態把握を行うことが望ましい。また、ポリシーを更新する際には、実態に即したものとするために、新たにリスク分析から行わなければならない。また、日頃から新たな攻撃方法の情報収集に努め、ポリシーの更新に活用することも必要である。

新たなポリシーが完成した際には、再度配布及び適用が必要となり、これには、当初にポリシーを導入した時と同様多大な労力が必要となる。効果的な方法を検討し実施することが必要である。

(3) ガイドラインへの反映

ポリシーの評価・見直し結果については、このガイドラインへ反映させる必要がある。

Ⅳ. 付録

１．用語解説

CD-R (Compact Disk Recordable)	一度だけ書き込み可能な CD を利用した記録媒体
DAT(Digital Audio Tape)	磁気テープにデジタル方式で記録する記録媒体
DoS 攻撃(Denial of Service)	サービス不能攻撃。コンピュータやネットワークに不正に負荷をかけたり、セキュリティホールを突くなどして業務を妨害する攻撃
DVD-RAM (Digital Versatile Disk-Random Access Memory)	書き換え可能な DVD を利用した記録媒体
FD(Floppy Disk)	フレキシブル・ディスクを利用した記憶媒体
HDD(Hard Disk Drive)	固定ディスクを利用した記憶装置
IC カード	IC チップが埋め込まれているカード状の電磁的記録媒体
IT(Information Technology)	情報技術
LAN(Local Area Network)	限られた範囲（省庁内等）を結ぶネットワーク又はセグメント
MO(Magneto-Optical disk)	光磁気ディスクを利用した記録媒体
MT(Magnetic Tape)	磁気テープを利用した記憶装置
アクセス(access)	（情報資産を）利用すること
アクセス権限	（情報資産を）利用する権限
コンピュータウイルス (computer virus)	第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり、自己伝染機能、潜伏機能、発病機能のいずれか一つ以上を有するもの
サーバ(server)	サービスを提供するソフトウエア又はハードウエア
システムソフトウエア(system software)	情報システムの管理をするためのプログラム
セキュリティ管理ソフトウエア	情報セキュリティ管理をするためのプログラム
セキュリティホール (security hole)	情報セキュリティ上問題となるソフトウエアの欠陥
ソースコード(source code)	プログラミング言語で記述されたプログラムの原本
ソフトウエア(software)	プログラム、データ等の総称
ディスプレイ(display)	ブラウン管、液晶などを利用した出力装置
データ(data)	電磁的記録
ネットワーク(network)	通信のために用いられる装置及び回線
ネットワーク資源	ネットワークを構成する資源
ハードウエア(hardware)	コンピュータ機器の総称

バイオメトリックス認証	指紋や虹彩等個人に特有の生体的特徴により認証を行う方法
パスワード(password)	利用者を認証するための符号
ハッキングソフトウエア (hacking software)	情報資産に攻撃をするためのプログラム
バックアップ(backup)	プログラム、データ等と同一の内容を別の媒体に記録すること
ファイル(file)	記憶装置又は記録媒体上に記録されているプログラム、データ等
ホストコンピュータ (host computer)	ネットワーク上のコンピュータ又は中央集中型情報システムにおける中央処理コンピュータ
無線 LAN	LAN の一部又は全部の回線を無線化したもの
メールアドレス(mail address)	電子メールの宛先
モデム(modem) (MOdulater-DEModulater)	音声（アナログ）通信回線とコンピュータを結び、音声信号及びデジタルデータの相互変換を行う装置（変復調装置）
モバイル端末	携帯可能な情報システム
リスク(risk)	情報システムが侵害を受ける危険性
ログアウト(logout)	アクセスを終了すること
ログイン(login)	アクセスを開始すること
ワクチンソフト (vaccine software)	コンピュータウイルスの検査、予防又は修復のいずれかの機能を含むソフトウエア
修正プログラム（パッチ）	ソフトウエアの（情報セキュリティ上の）欠陥を修正するための追加的ソフトウエア
電磁的記録	電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られた記録であって情報処理の用に供するもの
不正アクセス	不正アクセス禁止法第 3 条第 2 項に規定する不正アクセス行為その他の不正な手段により利用者以外の者が行うアクセス又は利用者が行う権限外のアクセス
不正アクセス禁止法	不正アクセス行為の禁止等に関する法律（平成 11 年法律第 128 号）

２．参考資料

(1) 情報通信ネットワーク安全・信頼性基準（昭和６２年・郵政省告示）
http://www.soumu.go.jp/joho_tsusin/whatsnew/kokuji/network_0203.html
(2) コンピュータウイルス対策基準（平成7年・通商産業省告示）
http://www.meti.go.jp/policy/netsecurity/CvirusCMG.htm
(3) コンピュータ不正アクセス対策基準（平成8年・通商産業省告示）
http://www.meti.go.jp/policy/netsecurity/UAaccessCMG.htm
(4) システム監査基準（平成8年・通商産業省公表）
http://www.meti.go.jp/policy/netsecurity/systemauditG.htm
(5) 情報システム安全対策指針（平成9年・国家公安委員会告示）
http://www.npa.go.jp/hightech/antai_sisin/kokuji.htm
(6) 行政情報システムの安全対策指針（平成11年7月30日　行政情報システム各省庁連絡会議幹事会了承）
http://www.soumu.go.jp/gyoukan/kanri/990816c.htm
(7) 各省庁の調達におけるセキュリティ水準の高い製品等の利用方針（平成 13 年 3 月 29 日、行政情報化推進各省庁連絡会議了承）
http://www.soumu.go.jp/gyoukan/kanri/a_01_f.htm
(8)「国の行政機関における情報システム関係業務の外注の推進について（平成 12 年 3 月 31 日、行政情報システム各省庁連絡会議了承）
http://www.soumu.go.jp/gyoukan/kanri/a_01_f.htm
(9) BS7799 Information security management
(10) ISO/IEC 15408　（セキュリティ技術ー情報技術セキュリティの評価基準）
(11) ISO/IEC TR 13335 Information technology - Guidelines for the management of IT security -（ＧＭＩＴＳ）
(12)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書（（財）金融情報システムセンター）
http://www.fisc.or.jp/ippan_3.htm
(13) RFC2196サイトセキュリティハンドブック
http://www.ipa.go.jp/SECURITY/rfc/RFC.html
(14) CIRCULAR NO. A-130 Security of Federal Automated Information Resources
http://www.whitehouse.gov/OMB/circulars/a130/a130.html
(15) Special Publification 800-12 An Introduction to Computer Security: The NIST Handbook
http://csrc.nist.gov/publications/nistpubs/
(16) Special Publification 800-14 Generally Accepted Principles and Practices for Securing Information Technology Systems
http://csrc.nist.gov/publications/nistpubs/

(17) Special Publification 800-18 Guide for Developing Security Plans for Information Technology Systems
http://csrc.nist.gov/publications/nistpubs/
(18) Practices for Securing Critical Information Assets

３．ポリシーの例

ポリシーの例は、ガイドラインの一部をなすものであり、各省庁が原則として守らなければならない事項を定めるものである。ただし、リスク分析等に基づく各省庁の実情に合わせた独自の対策基準の策定を妨げるものではない。