独立行政法人Ａ機構の
情報セキュリティ対策のための技術基準
(政府機関統一技術基準 K305-101 版ベース)
解説書

本書において、空色マーカ部分は、必ず書き換えが必要な箇所、黄色マーカ部分は、書き換えについて検討をするとよいと思われる箇所をマークしたものです。これらが書き換えを要するすべてではありませんが、参考にしてください。

独立行政法人Ａ機構

NISD-K305-101C に基づく独立行政法人等基準（参考例）

目次

第 2.1 部　総則

2.1.1.1 本技術基準の位置付け

(1)　本技術基準の位置付け

独立行政法人Ａ機構の情報セキュリティ対策のための管理基準（以下「管理基準」という。）に準じる。

(2)　本技術基準の改訂

管理基準に準じる。

(3)　法令等の遵守

管理基準に準じる。

2.1.1.2 本技術基準の使い方

(1)　全体構成

管理基準に準じる。

(2)　対策項目の記載事項

管理基準に準じる。

(3)　対策レベルの設定

管理基準に準じる。

2.1.1.3 情報の格付の区分及び取扱制限の種類

(1)　格付及び取扱制限

管理基準に準じる。

(2)　格付の区分

管理基準に準じる。

(3)　取扱制限の種類

管理基準に準じる。

2.1.1.4 評価の方法

管理基準に準じる。

2.1.1.5 用語定義

管理基準に準じる。

以下は、本技術基準で初出の用語。

【あ】

● 「受渡業者」とは、職務従事者との物品の受渡しを目的とした者をいう。物品の受渡しとしては、宅配便の集配、事務用品の納入等が考えられる。

【か】

● 「公開されたセキュリティホール」とは、誰もが知り得る状態に置かれているセキュリティホールのことであり、ソフトウェアやハードウェアの製造・提供元等から公表されたセキュリティホール、又は JPCERT コーディネーションセンター等のセキュリティ関連機関から公表されたセキュリティホールが該当する。

【は】

● 「複数要素（複合）主体認証（multiple factors authentication）方式」とは、複数の方法の組合せにより主体認証を行う方法である。

【ま】

● 「モバイル PC」とは、端末の形態に関係なく、業務で利用する目的により必要に応じて移動する端末をいう。特定の設置場所だけで利用するノート型 PC は、モバイル PC に含まれない。

第 2.2 部　情報セキュリティ要件の明確化に基づく対策

2.2.1　情報セキュリティについての機能

2.2.1.1 主体認証機能

趣旨（必要性）

情報システムの利用においては、その利用主体の識別と主体認証を可能とする機能がない場合、本来アクセス権のない者が、故意又は過失により、情報の参照、改ざん又は消去を行うおそれがある。また、各主体及び情報システムにアクセスする者が各主体の識別と主体認証に関する情報の適切な取扱いに努めなければ、同様のおそれを招くことになる。

これらのことを勘案し、本項では、主体認証機能の導入に関する対策基準を定める。

また、独立行政法人A機構が有する各情報システムの利用者は、職務従事者に限られるものではない。例えば、外部の人々向けのサービスを提供する情報システムの利用者は、職務従事者以外の者である場合がある。識別コードと主体認証情報については、このような利用者の別にかかわらず保護すべきであるが、職務従事者以外の者は管理基準及び本技術基準の適用範囲ではないため、それらの者に対しては、これを保護するよう注意喚起することが望ましい。

なお、管理基準 1.4.1.1 において識別コードと主体認証情報の管理等に関する対策基準を、1.5.2.4 において主体認証・アクセス制御・権限管理・証跡管理・保証等の必要性判断等に関する対策基準を定めている。

遵守事項

(1)　主体認証機能の導入

【基本遵守事項】

(a)　情報システムセキュリティ責任者は、主体認証を行う必要があると認めた情報システムにおいて、識別及び主体認証を行う機能を設けること。

解説：識別のための機能を設けることが技術的にできない情報システム（識別コード自体が存在せず、主体認証情報（パスワード）の設定のみ可能であるような装置等）は、例外措置として判断されることになる。その場合には、識別されないことによる影響について勘案し、必要に応じて代替あるいは追加の措置を講ずる必要がある。

主体認証の方式として、知識、所有、生体情報の３つの方法が代表的である。「知識」による主体認証とは、パスワード等、本人のみが知り得る情報を提示することにより、検証する方法である。「所有」による主体認証とは、IC カード等、本人のみが所有する機器等を主体認証処理に介在させることにより、検証する方法である。「生体情報」による主体認証とは、指紋や虹彩等、本人の生体的な特徴により、検証する方法である。

生体情報による主体認証を用いる場合には、その導入を決定する前に、

この方式特有の誤認率と誤否率の課題があることを考慮して情報システムを設計する必要がある。この方式では、正当な本人に対して、本人の非によらない理由で、主体認証が正しくできなくなる場合があることを想定し、そのような場合の職務の遂行への影響について検討してから導入を決定すること。

機微な情報へのアクセスであれば、本人であっても主体認証が解決できるまでアクセス不可能でよいとするか、あるいは、別の方式と組み合わせる等について考慮するとよい。

なお、具体的な主体認証機能の設計に当たっては、当該情報システムに対して決定したセキュリティ要件（1.5.1.1(1)(b)を参照）を満たす必要がある。

(b) 情報システムセキュリティ管理者は、主体認証を行う必要があると認めた情報システムにおいて、主体認証情報を秘密にする必要がある場合には、当該主体認証情報が明らかにならないように管理すること。

（ア）主体認証情報を保存する場合には、その内容の暗号化を行うこと。

（イ）主体認証情報を通信する場合には、その内容の暗号化を行うこと。

（ウ）保存又は通信を行う際に暗号化を行うことができない場合には、利用者に自らの主体認証情報を設定、変更及び提供（入力）させる際に、暗号化が行われない旨を通知すること。

解説：主体認証情報の保存や通信を行う際に暗号化できない場合には、利用者は他の情報システムで用いていない主体認証情報を設定すべきである。その旨を利用者が判断できるように通知しなければならない。

保存又は通信を行う際に主体認証情報を暗号化できない情報システムでは、主体認証情報が漏えいする危険性がある。もしも、そのような問題が生じた場合に、そこで使われていた主体認証情報と同じものが他の情報システムでも使われた場合には、暗号化できる情報システムにおいても、不正に使われてしまうという二次被害を招きかねない。その危険性を低減するため、暗号化されない情報システムでの主体認証情報については、他の情報システムで用いていないものを利用者が設定する等の回避策をとる必要がある。そのため、利用者が暗号化されない旨を知る機会を得られるようにしておかなければならない。

したがって、暗号化できない情報システムにおいて、主体認証情報を入力させる際には、例えば、「この情報システムでは入力される情報が暗号化されません。他の情報システムで使用している主体認証情報（パスワード）を入力しないようにしてください。」等の警告を表示するようにすることが必要である。

(c) 情報システムセキュリティ責任者は、主体認証を行う必要があると認めた情報システムにおいて、利用者に主体認証情報の定期的な変更を求める場合には、利用者に対して定期的な変更を促す機能のほか、以下のいずれかの機能を設けること。

（ア）利用者が定期的に変更しているか否かを確認する機能

（イ）利用者が定期的に変更しなければ、情報システムの利用を継続させない機能

解説：定期的な変更を遵守事項とする場合には、それが実施されているか否かを確認できる機能を用意しておく必要がある。

その機能によって確認作業を自動化することが技術的に困難な場合は、例外措置の手続を実施した上で、管理者が定期的にパスワードの変更を促すメールを利用者に送信し、利用者がこれに従ってパスワードを変更した旨を返信することで確認するといった代替措置の適用も考えられる。

なお、生体情報による主体認証方式のように、利用者本人であっても変更できない情報を用いる場合には、定期的に変更する必要はない。

(d) 情報システムセキュリティ責任者は、主体認証を行う必要があると認めた情報システムにおいて、主体認証情報又は主体認証情報格納装置を他者に使用され、又は使用される危険性を認識した場合に、直ちに当該主体認証情報若しくは主体認証情報格納装置による主体認証を停止する機能又はこれに対応する識別コードによる情報システムの利用を停止する機能を設けること。

解説：主体認証情報自体の露呈、主体認証情報に関連する情報の露呈又はそれらが露呈した可能性について報告を受けた場合には、主体認証の停止、識別コードによる情報システムの利用停止のほか、主体認証情報の変更や別の主体認証方式の併用等の対策を講ずること。

(e) 情報システムセキュリティ責任者は、主体認証を行う必要があると認めた情報システムにおいて、知識による主体認証方式を用いる場合には、以下の機能を設けること。

（ア）利用者が、自らの主体認証情報を設定する機能

解説：知識による主体認証方式の場合には、本人による設定を可能にすることによって、以下の利点が期待できる。

・他者に設定された主体認証情報に比べ、本人が設定した主体認証情報の方が容易に記憶できる。

・本人以外の者が主体認証情報を設定する場合には、その設定者によるなりすましが懸念されるが、本人自身が設定することにより、そのおそれが少なくなる。

なお、例えば、運用上の理由等で他者による再設定を認めた場合には、同様に本人になりすますことは可能であるため、主体認証情報（パスワード）変更の通知機能によって、本人に設定が変更されたことについて通知することが望ましい。

（イ）利用者が設定した主体認証情報を他者が容易に知ることができないように保持する機能

解説：情報システムセキュリティ責任者であっても、他者の主体認証情報を知ることができないようにする必要がある。情報システムセキュリティ責任者に悪意がなくとも、悪意のある第三者によってその管理者権限が奪取されてしまった場合には、全ての利用者の主体認証情報を知られてし

まうおそれがあるため、不可逆の暗号化を用いる等により、情報システムセキュリティ責任者自らも、他者の主体認証情報を知ることができないような措置を講ずる必要がある。

(f)　情報システムセキュリティ責任者は、主体認証を行う必要があると認めた情報システムにおいて、知識、所有、生体情報以外の主体認証方式を用いる場合には、その要件を定めるに際して、以下の事項のうちその特性に応じて適用可能な要件を全て満たす主体認証方式を導入すること。

（ア）正当な主体以外の主体認証を受諾しないこと。（誤認の防止）

（イ）正当な主体が本人の責任ではない理由で主体認証を拒否されないこと。（誤否の防止）

（ウ）正当な主体が容易に他者に主体認証情報の付与（発行、更新及び変更を含む。以下この項において同じ。）及び貸与ができないこと。（代理の防止）

（エ）主体認証情報が容易に複製できないこと。（複製の防止）

（オ）情報システムセキュリティ管理者の判断により、ログオンを個々に無効化できる手段があること。（無効化の確保）

（カ）必要時に中断することなく主体認証が可能であること。（可用性の確保）

（キ）新たな主体を追加するために、外部からの情報や装置の供給を必要とする場合には、それらの供給が情報システムの耐用期間の間、十分受けられること。（継続性の確保）

（ク）主体に付与した主体認証情報を使用することが不可能になった際に、正当な主体に対して主体認証情報を安全に再発行できること。（再発行の確保）

解説：代表的な方式である、知識、所有、生体情報による主体認証方式以外の方法を用いる場合の検討事項を列挙している。セキュリティ上の求められる強度や利便性等も考慮の上、方式を決定することを求める事項である。なお、これらの要件は、必ずしも全て充足することを求めるものではない。例えば、主体認証情報（パスワード）等による「知識」方式の場合には、要件(ウ)や(エ)を技術的に充足する必要はない。また、上記の（ア）～（ク）以外に気づいた事項があれば、適宜追加することが望ましい。

【強化遵守事項】

(g)　特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システムセキュリティ責任者は、主体認証を行う必要があると認めた情報システムにおいて、複数要素（複合）主体認証方式で主体認証を行う機能を設けること。

解説：複数要素（複合）による主体認証方式を用いることにより、より強固な主体認証が可能となる。

これは、単一要素（単一）主体認証方式（「単一要素（単一）主体認証（single factor authentication / single authentication）方式」とは、知識、所有、生体情報等のうち、単一の方法により主体認証を行う方式である。）の場合には、何らかの理由によって主体認証情報が露呈してしまった際には、不正にログオンされる可能性が非常に高くなってしまうが、複数要素（複

合）主体認証方式の場合には、仮に一方の主体認証情報が露呈してしまっても、残りの主体認証情報が露呈しない限り、不正にログオンされる可能性は依然低いと考えられるからである。

(h) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システムセキュリティ責任者は、主体認証を行う必要があると認めた情報システムにおいて、ログオンした利用者に対して、前回のログオンに関する情報を通知する機能を設けること。

解説：識別コードによる前回のログオンに関する情報（日時や装置名等）を通知することで、本人の識別コードが他者によって不正に使われた場合に、本人が気付く機会を得られるようにすることを求める事項である。

(i) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システムセキュリティ責任者は、主体認証を行う必要があると認めた情報システムにおいて、不正にログオンしようとする行為を検知し、又は防止する機能を設けること。

解説：通知によって本人が知る機会を得ること及び組織が状況を管理できること等が考えられる。例えば、識別コードによるログインにおいて、指定回数以上の主体認証情報の誤入力が検知された場合に、その旨を本人に通知する、あるいは、当該識別コードによる情報システムへの以後のログインを無効にする（アカウントをロックする）機能の付加が挙げられる。

(j) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システムセキュリティ責任者は、主体認証を行う必要があると認めた情報システムにおいて、利用者が情報システムにログインする前に、当該情報システムの利用に関する通知メッセージを表示する機能を設けること。

解説：通知メッセージの例としては、以下のようなものがある。

・利用者が独立行政法人Ａ機構の情報システムへアクセスしようとしていること

・情報システムの使用が監視、記録される場合があり、監査対象となること

・情報システムの不正使用は禁止されており、刑法の罰則対象となること

(k) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システムセキュリティ責任者は、主体認証を行う必要があると認めた情報システムにおいて、利用者に主体認証情報の定期的な変更を求める場合には、以前に設定した主体認証情報と同じものを再設定することを防止する機能を設けること。

解説：一度使用した主体認証情報（パスワード等）の再利用を禁止することを求める事項である。なお、生体情報による主体認証方式のように、利用者本人であっても変更できない情報を用いる場合には、定期的に変更する必要はない。

(l) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システムセキュリティ責任者は、主体認証を行う必要があると認めた情報システムにおいて、

管理者権限を持つ識別コードを共用する場合には、当該識別コードでログインする前に個別の識別コードによりログオンすることが必要となる機能を設けること。

解説：管理者権限を有した識別コードを管理者グループで共用した場合には、そのログオン記録だけでは、共用している管理者のうち、実際に作業をした管理者を個人単位で特定することが困難となる。そのため、管理者個人を特定することを目的として、非管理者権限の識別コードを本人に付与した上、その識別コードで最初にログオンした後に限り、管理者権限を有する共用識別コードに切り替えて管理者作業を実施することを可能とする必要がある。

なお、当該情報システムのオペレーティングシステムが Unix 系の場合には、一般利用者でログオンした後に su コマンドで root に切り替えるという手順により、これを達成できる。また、その場合には、root によるログオンを禁止する設定により、その手順を強制することができる。

2.2.1.2 アクセス制御機能

趣旨（必要性）

主体認証によって、許可された主体だけが情報システムを利用できることになるが、情報システムを複数の主体が利用し、そこに重要度の異なる複数種類の情報がある場合には、どの主体がどの情報にアクセスすることが可能なのかを情報ごとにアクセス制御する必要がある。

これらのことを勘案し、本項では、アクセス制御に関する対策基準として、アクセス制御機能の導入、適正なアクセス制御についての遵守事項を定める。

なお、管理基準 1.4.1.1 において識別コードと主体認証情報の管理等に関する対策基準を、1.5.2.4 において主体認証・アクセス制御・権限管理・証跡管理・保証等の必要性判断等に関する対策基準を定めている。

遵守事項

(1) アクセス制御機能の導入

【基本遵守事項】

(a) 情報システムセキュリティ責任者は、アクセス制御を行う必要があると認めた情報システムにおいて、アクセス制御を行う機能を設けること。

解説：情報システムの利用者やそのグループの属性に応じてオブジェクト（制御対象）へのアクセス権を任意に設定できる方式（任意アクセス制御）を利用すること。なお、「任意アクセス制御（DAC : Discretionary Access Control）」とは、主体が客体に設定したアクセス制御について、その設定がそれ以後継承されるかが任意である方式であり、この方式では、その客体にアクセス許可されている主体が別の客体を作成し複製等する際に、元のアクセス制御を新しい客体のアクセス制御として継承するかは

当該主体の任意であり、変更が可能である。

【強化遵守事項】

(b) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システムセキュリティ責任者は、アクセス制御を行う必要があると認めた情報システムにおいて、利用者及び所属するグループの属性以外に基づくアクセス制御の機能を追加すること。

解説：情報システムの利用者や所属するグループの属性に応じてオブジェクト（制御対象）へのアクセス権を任意に設定できる方式のほか、情報システムの利用者やそのグループの属性以外に基づくアクセス制御を追加すること。

情報システムの利用者やそのグループの属性に基づくアクセス制御としては、例えば以下の方式が挙げられる。

・アクセス・コントロール・リスト（ＡＣＬ）制御

情報システムの利用者やそのグループの属性以外に基づくアクセス制御としては、例えば以下の方式が挙げられる。

・利用時間による制御
・利用時間帯による制御
・同時利用者数による制限
・同一ＩＤによる複数アクセスの禁止
・IP アドレスによる端末制限

(c) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システムセキュリティ責任者は、アクセス制御を行う必要があると認めた情報システムにおいて、強制アクセス制御機能を設けること。

解説：強制アクセス制御機能(MAC)の組み込みを導入すること。

強制アクセス制御機能を備えたものとして、トラステッドＯＳやセキュアＯＳ等で実装したものもある。

(2) 適正なアクセス制御

【基本遵守事項】

(a) 情報システムセキュリティ責任者は、職務従事者自らがアクセス制御を行うことができない情報システムについて、当該情報システムに保存されることとなる情報の格付及び取扱制限に従って、アクセス制御を行うこと。

解説：共有ファイルサーバのアクセス制御のように、情報システムを職務従事者が利用する際に、自らがアクセス制御を行うことができない場合、情報システムの導入時及び運用時にアクセス制御を行うことを求めた事項である。例えば、要機密情報であれば、不適当な者から参照されないよう、読み取り制限の属性を付与し、完全性２情報であれば、不適当な者から変更されないよう、上書き禁止の属性を付与することがこれに当たる。

また、職務従事者自らがアクセス制御を行うことが出来る場合、

1.3.1.3(1)(b)の規程に基づき対策を行うこと。

2.2.1.3 権限管理機能

趣旨（必要性）

主体認証情報の機密性と完全性、及びアクセス制御情報の完全性を守ることは重要である。これらの機密性や完全性が損なわれると、主体認証やアクセス制御の機能に問題がなくとも、正当ではない主体からの情報へのアクセスを許してしまうことになる。

これらのことを勘案し、本項では、権限管理に関する対策基準として、権限管理機能の導入、識別コードと主体認証情報の付与管理についての遵守事項を定める。

なお、管理基準 1.4.1.1 において識別コードと主体認証情報の管理等に関する対策基準を、1.5.2.4 において主体認証・アクセス制御・権限管理・証跡管理・保証等の必要性判断等に関する対策基準を定めている。

遵守事項

(1) 権限管理機能の導入

【基本遵守事項】

(a) 情報システムセキュリティ責任者は、権限管理を行う必要があると認めた情報システムにおいて、権限管理を行う機能を設けること。

解説：権限管理を行う機能を設ける必要性があると認められた場合に、当該機能を情報システムに設けることを求める事項である。

【強化遵守事項】

(b) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システムセキュリティ責任者は、権限管理を行う必要があると認めた情報システムにおいて、最少特権機能を設けること。

解説：管理者権限を持つ識別コードを付与された者が、管理作業をする時に限定してその識別コードを利用することを可能とする最少特権機能を、情報システムに設けることを求める事項である。

(c) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システムセキュリティ責任者は、権限管理を行う必要があると認めた情報システムにおいて、主体認証情報の再発行を自動で行う機能を設けること。

解説：情報システムの利用を開始している主体が、主体認証情報の再発行を要求した場合には、当該情報システムにおいて、その主体により重要な情報が既に作成されている可能性があることから、再発行する主体認証情報を他の者が知り得ないように、新規に主体認証情報を発行する場合に比べて、一層安全な機能を設けることを求める事項である。

なお、再発行を自動化して他の者による操作を必要とすることなく主体認証情報を再発行することは、管理者による不正な操作が発生する機会を減らし、安全性を強化することができる。

(d) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システ

ムセキュリティ責任者は、権限管理を行う必要があると認めた情報システムにおいて、デュアルロック機能を設けること。

解説：不正操作及び誤操作を防止するために、情報システムにデュアルロック機能を設けることを求める事項である。デュアルロック機能とは、行為に対して、少なくとも 2 名の者が操作しなければその行為を完遂できない方式のことである。

(2) 識別コードと主体認証情報の付与管理

【基本遵守事項】

(a) 権限管理を行う者は、情報システムを利用する許可を得た主体に対してのみ、識別コード及び主体認証情報を発行すること。

解説：情報システムにおける識別コード及び主体認証情報は、情報システムを利用する許可を得た主体に対してのみ、本人確認の上で初期発行することが重要である。また、識別コード及び主体認証情報の安全な初期配布方法について求める事項である。

(b) 権限管理を行う者は、識別コードを発行する際に、それが共用識別コードか、共用ではない識別コードかの区別を利用者に通知すること。

解説：識別コードを利用者に発行する際に共用識別コードか共用ではない識別コードかの別について通知することにより、それらの区別を利用者が独自に判断するようなことを防ぐための事項である。ただし、共用識別コードを利用できるのは、情報システムセキュリティ責任者がその利用を認めた情報システムに限られることに注意すること。

(c) 権限管理を行う者は、管理者権限を持つ識別コードを、業務又は業務上の責務に即した場合に限定して付与（発行、更新及び変更を含む。以下この項において同じ。）すること。

解説：管理者権限を持つ識別コードの取扱いは、情報システムのセキュリティ対策上、非常に重要な事項である。そのため、管理者権限を持つ識別コードは、業務又は業務上の責務に即して最小限の者へ付与すること。必要以上の者に過大な管理者権限を付与しないこと。

(d) 権限管理を行う者は、職務従事者が情報システムを利用する必要がなくなった場合には、当該職務従事者の識別コードを無効にすること。また、人事異動等により、識別コードを追加し、又は削除する時に、不要な識別コードの有無を点検すること。

解説：識別コードの付与を最小限に維持するため、退職等により不必要となった識別コードについては、これを無効にすることを求める事項である。また、本人からの届出による場合のほか、人事異動等の時期を考慮の上、定期的及び必要に応じて不要な識別コードが存在しないことを確認することにより、無効の設定漏れを最小限にとどめることが期待できる。

(e) 権限管理を行う者は、職務従事者が情報システムを利用する必要がなくなった場合には、当該職務従事者に交付した主体認証情報格納装置を返還させること。

解説：識別コードの付与を最小限に維持し、かつ主体認証情報の不当な使用を

防止するために、退職等により不要になった主体認証情報格納装置の回収を求める事項である。

(f) 権限管理を行う者は、業務上の責務と必要性を勘案し、必要最小限の範囲に限って許可を与えるようにアクセス制御の設定をすること。また、人事異動等により、識別コードを追加し、又は削除する時に、不適切なアクセス制御設定の有無を点検すること。

解説：業務又は業務上の責務に即して、必要となる者に限り、当該者の業務遂行に必要となるアクセス権のみを付与することを求める事項である。

【強化遵守事項】

(g) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、権限管理を行う者は、単一の情報システムにおいては、１人の職務従事者に対して単一の識別コードのみを付与すること。

解説：１人の職務従事者に対して単一の識別コードのみを付与することを求める事項である。例えば、デュアルロック機能を備えた情報システムにおいては、１人の職務従事者に複数の識別コードでの主体認証を許してしまうと、デュアルロック機能による強化が万全とならなくなる。

(h) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、権限管理を行う者は、識別コードをどの主体に付与したかについて記録すること。当該記録を消去する場合には、情報セキュリティ責任者からの事前の許可を得ること。

解説：識別コードの付与に係る記録は将来の障害・事故等の原因調査に備えて、不用意に消去しないことを求める事項である。その情報システムへの将来の調査が不要になったものについては、消去することになるが、その場合には、許可を得た上で消去しなければならない。情報システムの関係者だけの判断で、識別コードをどの主体に付与したかを知るための記録を消去してはならない。

(i) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、権限管理を行う者は、ある主体に付与した識別コードをその後別の主体に対して付与しないこと。

解説：ある主体に付与した識別コードを再利用して別の主体に付与することを禁ずる事項である。このため、職位等に対応する識別コードが存在し、それを担当者が引き継いで使用する場合等、やむを得ずある主体に付与した識別コードをその後別の主体に対して付与する場合には、例外措置を申請する必要がある。そして、当該申請を許可するときは、その主体認証情報を新たに設定し、以前に使用していた主体による使用を禁ずるとともに、任意の時点で識別コードの利用主体を特定できるように、履歴を管理することが求められる。

なお、当該例外措置は、どの識別コードを誰が使用しているかを管理する ID マネジメントに係る重要事項であるため、情報セキュリティ責任者が許可・不許可を判断することが望ましい。

2.2.1.4 証跡管理機能

趣旨（必要性）

情報システムの利用においては、当該情報システムの制御及び管理の実効性を高め、また情報セキュリティに関する問題が発生した場合にこれに適切に対処するために、当該情報システムの動作及びその他必要な事象を記録し、事後にこれを調査する証跡管理を行う必要がある。また、証跡管理により、外部又は内部の者による不正利用又は過失行為を事前に抑止し、また事後に追跡することが可能となる。

これらのことを勘案し、本項では、証跡管理に関する対策基準として、証跡管理機能の導入、証跡の取得と保存についての遵守事項を定める。

なお、管理基準 1.4.1.1 において識別コードと主体認証情報の管理等に関する対策基準を、1.5.2.4 において主体認証・アクセス制御・権限管理・証跡管理・保証等の必要性判断等に関する対策基準を定めている。

遵守事項

(1)　証跡管理機能の導入

【基本遵守事項】

(a)　情報システムセキュリティ責任者は、証跡を取得する必要があると情報セキュリティ責任者が認めた情報システムには、証跡管理のために証跡を取得する機能を設けること。

解説：証跡を取得する機能を設ける必要があると認められた場合に、当該機能を情報システムに設けることを求める事項である。

(b)　情報システムセキュリティ責任者は、証跡を取得する必要があると情報セキュリティ責任者が認めた情報システムにおいては、証跡が取得できなくなった場合及び取得できなくなるおそれがある場合の対処方法を定め、必要に応じ、これらの場合に対処するための機能を情報システムに設けること。

解説：証跡の取得ができなくなった場合及び取得できなくなるおそれがある場合に対処する機能を情報システムに設けることを求める事項である。

設けるべき機能としては、用意したファイル容量を使い切った場合に証跡の取得を中止する機能、古い証跡に上書きをして取得を継続する機能、ファイル容量を使い切る前に操作する者に通知して対処をさせる機能等が考えられる。

なお、「必要に応じ」とは、定めた対処方法を実現するために必要な場合に限られる。

(c)　情報システムセキュリティ責任者は、証跡を取得する必要があると情報セキュリティ責任者が認めた情報システムにおいては、取得した証跡に対して不当な消去、改ざん及びアクセスがなされないように、取得した証跡についてアクセス制御を行うこと。

解説：不正アクセス、不正操作若しくは職務外利用又は誤操作を行った者にとって、その証跡は自己に不利益をもたらすものであることも考慮し、証

跡が不当に消去、改ざんされることのないように、適切な格付を与えてこれを管理することを求める事項である。証跡の格付は、多くの場合に、機密性２情報又は機密性３情報で、要保全情報となるものと考えられる。証跡は、訴訟において証拠として利用されることがある。その適切な取扱いを組織として定め、かつこれを遵守していることが、証跡に証拠力が認められる前提となることにも留意する必要がある。
また、証跡には情報システムを利用する者の行為が記録されるため、業務上の必要なくこれにアクセスすべきではない。
これらの理由で、証跡は、情報システムセキュリティ管理者を含む利用者が不当に消去、改ざん又はアクセスすることのないように、証跡を保存したファイルに適切なアクセス制御を適用する必要がある。
また、証跡として利用記録や監視記録を含めた場合には、対象となる利用者のプライバシーを侵害しないことにも配慮する必要があるため、アクセスできる者を制限することが重要になる。

【強化遵守事項】

(d)　特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システムセキュリティ責任者は、証跡を取得する必要があると情報セキュリティ責任者が認めた情報システムにおいては、証跡の点検、分析及び報告を支援するための自動化機能を情報システムに設けること。

解説：取得した証跡を効率的かつ確実に点検及び分析し、その結果を報告するために、その作業を自動化する機能を設けることを求める事項である。
証跡は、その量が膨大になるため、証跡の内容をソフトウェア等により集計し、時系列表示し、報告書を生成する等により、効率的かつ確実な点検、分析及び報告が可能となる。規模の大きい情報システムにおいては、複数のサーバ装置で取得した証跡をあわせた点検、分析及び報告の作業を支援する自動化も、必要に応じて導入する。

(e)　特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システムセキュリティ責任者は、取得した証跡の内容により、情報セキュリティの侵害の可能性を示す事象を検知した場合に、監視する者等にその旨を即時に通知する機能を情報システムに設けること。

解説：情報セキュリティの侵害の可能性を示す事象が発生した場合に、迅速な対処を可能とするために、監視する者等に即時に通知する機能を設けることを求める事項である。
独立行政法人Ａ機構外からの不正侵入の可能性、独立行政法人Ａ機構における持込み PC の情報システムへの接続等、通知すべき事象を定め、これを通知する機能を情報システムに組み込む。必要に応じ、情報システムの利用者に即時に注意を促す仕組みを設けることも考えられる。

(2)　証跡の取得と保存

【基本遵守事項】

(a) 情報システムセキュリティ管理者は、証跡を取得する必要があると情報セキュリティ責任者が認めた情報システムにおいては、情報システムに設けられた機能を利用して、証跡を取得すること。

解説：情報システムの運用中に、利用者の行動等の事象を証跡として取得することを求める事項である。

情報システムセキュリティ管理者は、証跡を取得するために、必要な操作を行う必要がある。

(b) 情報システムセキュリティ管理者は、証跡を取得する必要があると情報セキュリティ責任者が認めた情報システムにおいては、取得した証跡の保存期間が満了する日まで当該証跡を保存し、保存期間を延長する必要性がない場合は、速やかにこれを消去すること。保存期間は、外部にアクセスする情報システムにおいては３か月以上とし、特に重要な情報を取り扱う情報システムにおいては１年以上として定めること。

解説：取得した証跡を適正に保存し、又は消去することを求める事項である。

情報システムセキュリティ管理者は、証跡の保存期間が満了するまで当該証跡を保存する必要がある。

必要な期間にわたり証跡を保存するために、当該期間に取得する証跡を全て保有できるファイル容量としたり、証跡を適宜外部電磁的記録媒体に退避したりする方法がある。

なお、法令の規定により保存期間が定められている場合には、これにも従うこと。

(c) 情報システムセキュリティ管理者は、証跡を取得する必要があると情報セキュリティ責任者が認めた情報システムにおいては、証跡が取得できない場合又は取得できなくなるおそれがある場合は、定められた対処方法に基づいて対処すること。

解説：証跡の取得ができない場合又は取得できなくなるおそれがある場合の対処を定める事項である。

これらの場合には、情報システムセキュリティ管理者は、対処方法に定められた操作を行うことが求められる。対処方法に定められた操作としては、用意したファイル容量の残りが少ないことを通知された場合に、ファイルの切替えと証跡の退避を指示する操作等が想定される。

2.2.1.5 保証のための機能

趣旨（必要性）

管理基準及び本技術基準では、基本的なセキュリティ機能として、主体認証機能、アクセス制御機能、権限管理機能、証跡管理機能の各項で具体的に遵守事項を規定している。しかし、情報が適切な状態であることを保証するためには、これらの機能によるセキュリティ対策より上位の機能やそれ以外の機能等による対策全般についても導入の必要性を検討することが重要である。こうした対策は、限られた情報システムに導入されることにな

ると考えるが、基本的な対策ではないからといって最初から除外するのではなく、必要性の有無を確認し選択的に導入するという対応が適切である。

これらのことを勘案し、本項では、保証のための機能に関する対策基準を定める。

なお、管理基準 1.4.1.1 において識別コードと主体認証情報の管理等に関する対策基準を、1.5.2.4 において主体認証・アクセス制御・権限管理・証跡管理・保証等の必要性判断等に関する対策基準を定めている。

遵守事項

(1) 保証のための機能の導入

【基本遵守事項】

(a) 情報システムセキュリティ責任者は、保証のための対策を行う必要があると認めた情報システムにおいて、保証のための機能を設けること。

解説：保証のための対策を行う必要性があると認めた場合に、保証のための機能を情報システムに設けることを求める事項である。

保証のための機能とは、2.2.1.1～2.2.1.4 で示した遵守事項に限らない情報及び情報システムの安全性をより確実にするための機能のことをいう。これには大きく分けて以下の２つのものがある。

（ア）2.2.1.1～2.2.1.4 の機能とは異なる観点での保護を高めるための機能：

2.2.1.1～2.2.1.4 の機能は、主として情報及び情報システムの機密性、完全性及び可用性を保護することを目的とした機能である。これに加えて、情報及び情報システムの真正性（Authenticity）、否認防止（Non-Repudiation）のための機能等を設けることの必要性を、対象とする情報及び情報システムに対して検討し、必要な措置を講ずることによって、安全性をより確実にすることができる。

真正性の保護及び否認防止のための機能としては、例えば、電子署名及びタイムスタンプが挙げられる。

（イ）2.2.1.1～2.2.1.4 の機能及び上の（ア）の機能の動作が適正であることを確認するための機能：

2.2.1.1～2.2.1.4 の機能及び上の（ア）の機能は情報及び情報システムを保護するための機能といえる。それに対して（イ）は、それらの機能を監視して、異常やその兆候を検知し、検知された問題を解決する対処をすることによって、それらの機能の回復に備えるための機能である。これらの機能を設けることの必要性を、対象とする情報及び情報システムに対して検討し、必要な措置を講ずることによって、安全性をより確実にすることができる。

（イ）の機能としては、例えば、侵入検知システムやネットワーク監視等が挙げられる。

また、保証のための機能は、主体認証機能等のように個別のものではなく、複数の機能であったり、それら複数のものを組み合わせた機能であ

ったりする場合もある。情報セキュリティをより高めるために必要となる機能を設けることで本遵守事項を達成することができる。

2.2.1.6 暗号と電子署名（鍵管理を含む）

趣旨（必要性）

情報システムの利用においては、当該情報システムで取り扱う情報の漏えいや改ざん等を防ぐために、情報の暗号化及び電子署名が有効とされている。この際、あらかじめ定めた暗号アルゴリズム及び方法に基づき、暗号及び電子署名を適切な状況で利用する必要がある。

これらのことを勘案し、本項では、暗号化及び電子署名に関する対策基準として、暗号化機能及び電子署名機能の導入、暗号化及び電子署名に係る管理についての遵守事項を定める。

なお、管理基準 1.4.1.1 において識別コードと主体認証情報の管理等に関する対策基準を、1.5.2.4 において主体認証・アクセス制御・権限管理・証跡管理・保証等の必要性判断等に関する対策基準を定めている。

遵守事項

(1) 暗号化機能及び電子署名機能の導入

【基本遵守事項】

(a) 情報システムセキュリティ責任者は、要機密情報（書面を除く。以下この項において同じ。）を取り扱う情報システムについて、暗号化を行う機能を付加する必要性の有無を検討すること。

解説：暗号化を行う機能を情報システムに付加する前提として、情報システムセキュリティ責任者は、各情報システムについて、取り扱う情報の機密性の程度から暗号化を行う機能を付加する必要性の有無を検討しなければならない。

(b) 情報システムセキュリティ責任者は、暗号化を行う必要があると認めた情報システムには、暗号化を行う機能を設けること。

解説：情報の機密性の程度から暗号化を行う機能を付加する必要性が認められる場合に、当該機能を情報システムに設けることを求める事項である。

(c) 情報システムセキュリティ責任者は、要保全情報を取り扱う情報システムについて、電子署名の付与及び検証を行う機能を付加する必要性の有無を検討すること。

解説：電子署名の付与及び検証を行う機能を情報システムに付加する前提として、情報システムセキュリティ責任者は、各情報システムについて、取り扱う情報の完全性及び情報提供者の真正性確認の程度から電子署名の付与及び検証を行う機能を付加する必要性の有無を検討しなければならない。

(d) 情報システムセキュリティ責任者は、電子署名の付与又は検証を行う必要がある

と認めた情報システムには、電子署名の付与又は検証を行う機能を設けること。

解説：情報の完全性及び情報提供者の真正性確認の程度から電子署名の付与又は検証を行う機能を付加する必要性が認められる場合に、当該機能を情報システムに設けることを求める事項である。

【強化遵守事項】

(e) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システムセキュリティ責任者は、暗号化又は電子署名の付与又は検証を行う必要があると認めた情報システムにおいて、暗号モジュールを、交換ができるようにコンポーネント化して構成すること。

解説：選択したアルゴリズムが危殆化した場合を想定し、暗号モジュールを交換可能なコンポーネントとして構成するため、設計段階からの考慮を求める事項である。そのためには、暗号モジュールのアプリケーションインターフェイスを統一しておく等の配慮が必要である。

(f) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システムセキュリティ責任者は、暗号化又は電子署名の付与又は検証を行う必要があると認めた情報システムにおいて、複数のアルゴリズムを選択可能とすること。

解説：選択したアルゴリズムが危殆化した場合を想定し、設定画面等によって、当該アルゴリズムを危殆化していない他のアルゴリズムへ直ちに変更できる機能等を、情報システムに設けることを求める事項である。

(g) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システムセキュリティ責任者は、暗号化又は電子署名の付与又は検証を行う必要があると認めた情報システムにおいて、選択したアルゴリズムがソフトウェア及びハードウェアへ適切に実装され、暗号化された情報の復号又は電子署名の付与に用いる鍵及び主体認証情報等が安全に保護された製品を使用するため、暗号モジュール試験及び認証制度に基づく認証を取得している製品を選択すること。

解説：アルゴリズムの実装状況及び鍵等の保護状況を確認するに当たり、ISO/IEC 19790 に基づく暗号モジュール試験及び認証制度による認証を取得している製品を選択することを求める事項である。

アルゴリズム自体が安全であっても、それをソフトウェアやハードウェアへ実装する際、生成する疑似乱数に偏りが生ずる等の理由で疑似乱数が推測可能であったり、鍵によって処理時間に統計的な偏りが生ずる等の理由で鍵情報の一部が露呈したりすると、情報システムの安全性が損なわれるおそれがある。

なお、「適切に実装されている」とは、アルゴリズム自体の安全性だけではなく、疑似乱数の推測、鍵情報の一部露呈等の脅威に対応して実装していることをいい、その確認には、独立行政法人　情報処理推進機構(IPA)により運用されている暗号モジュール試験及び認証制度（JCMVP：Japan Cryptographic Module Validation Program）等が利用可能である。

(h) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システ

ムセキュリティ責任者は、暗号化又は電子署名の付与を行う必要があると認めた情報システムにおいて、暗号化された情報の復号又は電子署名の付与に用いる鍵を、第三者による物理的な攻撃から保護するために、耐タンパー性を有する暗号モジュールへ格納すること。

解説：暗号化された情報の復号又は電子署名の付与に用いる鍵について、技術的な対策等に加え、物理的対策を講ずることを求める事項である。鍵を格納する電磁的記録媒体が盗難され、鍵が開封される等しても、鍵情報が外部へ漏えいしない仕組みが必要である。

この場合、耐タンパー性を有するとは、例えば、JIS X 19790:2007 7.5 物理的セキュリティ（ISO/IEC 19790:2006）の規定に照らし合わせると、他のセキュリティ対策との組み合わせによりレベル２以上を選択することが可能であるが、他の組み合わせがない場合、レベル３以上が相当する。

(2) 暗号化及び電子署名に係る管理

【基本遵守事項】

(a) 情報システムセキュリティ責任者は、電子署名の付与を行う必要があると認めた情報システムにおいて、電子署名の正当性を検証するための情報又は手段を署名検証者へ提供すること。

解説：電子署名の付与を実効的に機能させるために、付与された電子署名を受け取った者が、その電子署名の正当性を容易に検証できるようにすることを求める事項である。

通常、付与された電子署名を検証するためには、署名時に使用した署名鍵に対応する検証鍵が必要であるが、この検証鍵自体の真正性を保証するためには、独立行政法人Ａ機構の窓口での直接提供、信頼できる機関による電子証明書の発行、検証鍵に付随する固有の情報（フィンガープリント等）の公開等の方法がある。

なお、電子署名の正当性を検証するための情報又は手段については、当該電子署名が付与された情報が真正なものであることを証明する必要がある間、提供することとなる。例えば、電子署名の有効期限内にアルゴリズムの危殆化が発生し、又は有効期限を超えるため、別の電子署名を付与する場合にあっては、これら全ての電子署名の正当性を検証するための情報又は手段を提供する必要がある。

【強化遵守事項】

(b) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システムセキュリティ責任者は、暗号化又は電子署名の付与又は検証を行う必要があると認めた場合、当該情報システムにおいて選択されたアルゴリズムの危殆化に関する情報を適宜入手すること。

解説：様々な機関から提供されているアルゴリズムの危殆化に関する情報を適宜入手しておくことを求める事項である。

例えば、CRYPTREC を始めとする暗号技術の有識者による発表に関心を払うことが必要である。

2.2.2　情報セキュリティについての脅威

2.2.2.1 セキュリティホール対策

趣旨（必要性）

セキュリティホールは、情報システムを構成する電子計算機及び通信回線装置上で利用しているソフトウェアに存在する可能性があり、そのセキュリティホールを攻撃者に悪用されることにより、サーバ装置への不正侵入、サービス不能攻撃、不正プログラム感染の原因になる等、情報システム全体のセキュリティを維持する上で大きな脅威となる。特に、サーバ装置へ不正侵入された場合、踏み台、情報漏えい等の更なるリスクにつながり、独立行政法人Ａ機構の社会的な信用が失われるおそれがある。これらのリスクを回避するため、セキュリティホールへの対処は迅速かつ適切に行わなければならない。

これらのことを勘案し、本項では、セキュリティホールに関する対策基準として、情報システムの構築時及び運用時についての遵守事項を定める。

遵守事項

(1)　情報システムの構築時

【基本遵守事項】

(a)　情報システムセキュリティ責任者は、電子計算機及び通信回線装置（公開されたセキュリティホールの情報がない電子計算機及び通信回線装置を除く。以下この項において同じ。）の設置又は運用開始時に、当該機器上で利用するソフトウェアに関連する公開されたセキュリティホールの対策を実施すること。

解説：電子計算機及び通信回線装置の設置又は運用開始時に、その時点において、当該機器上で利用しているソフトウェアのセキュリティホール対策が完了していることを求める事項である。

【強化遵守事項】

(b)　特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システムセキュリティ責任者は、公開されたセキュリティホールの情報がない段階においても電子計算機及び通信回線装置上で採り得る対策を実施すること。

解説：公開されたセキュリティホールへの対策だけでなく、明らかになっていないセキュリティホールについても対策を求める事項である。

対策としては、特定のメモリ上の実行権限の削除又はバッファオーバーフローの検知によるアプリケーションの実行停止等の対策を実施すること等が挙げられる。

(2)　情報システムの運用時

【基本遵守事項】

(a)　情報システムセキュリティ管理者は、管理対象となる電子計算機及び通信回線装置上で利用しているソフトウェアに関して、公開されたセキュリティホールに関連する情報を適宜入手すること。

解説：セキュリティホールに関連する情報の収集を求める事項である。セキュリティホールに関連する情報とは、セキュリティホールの原因、影響範囲、対策方法、セキュリティホールを悪用するツールの公開の有無等が挙げられる。

自動アップデート機能を持つソフトウェアの場合には、当該機能を利用して、定期的にセキュリティホールに関連する情報が報告されているかを確認する方法で差し支えないが、当該機能がない場合は、適時調査を行う必要がある。

(b) 情報システムセキュリティ責任者は、管理対象となる電子計算機及び通信回線装置上で利用しているソフトウェアに関して、セキュリティホールに関連する情報を入手した場合には、当該セキュリティホールが情報システムにもたらすリスクを分析した上で、以下の事項について判断し、セキュリティホール対策計画を策定すること。

（ア）対策の必要性
（イ）対策方法
（ウ）対策方法が存在しない場合の一時的な回避方法
（エ）対策方法又は回避方法が情報システムに与える影響
（オ）対策の実施予定
（カ）対策試験の必要性
（キ）対策試験の方法
（ク）対策試験の実施予定

解説：セキュリティホールが情報システムにもたらすリスクを分析し、対策計画の策定を求める事項である。

「対策試験」とは、セキュリティホール対策の実施による情報システムへの影響の有無について、他の情報システムを用いて試験することをいう。

(c) 情報システムセキュリティ管理者は、セキュリティホール対策計画に基づきセキュリティホール対策を講ずること。

解説：セキュリティホール対策計画に基づいて対策が実施されることを求める事項である。

(d) 情報システムセキュリティ管理者は、セキュリティホール対策の実施について、実施日、実施内容及び実施者を含む事項を記録すること。

解説：セキュリティホール対策の実施記録の様式は問わないが、実施日、実施内容及び実施者は必ず記録しなければならない必須事項である。これらの事項のほかに必要事項があれば、適宜追加する。

(e) 情報システムセキュリティ管理者は、信頼できる方法でパッチ又はバージョンアップソフトウェア等のセキュリティホールを解決するために利用されるファイル（以下「対策用ファイル」という。）を入手すること。また、当該対策用ファイルの完全性検証方法が用意されている場合は、検証を行うこと。

解説：入手した対策用ファイルに悪意あるコードが含まれている可能性を考慮

し、対策用ファイルを信頼できる方法で入手することを求める事項である。
信頼できる方法としては、ソフトウェアの開発元等が公開するウェブサイトからのダウンロード又は郵送された外部電磁的記録媒体を利用して入手する方法が挙げられる。また、改ざん等について検証することができる手段があれば、これを実行する必要がある。

(f) 情報システムセキュリティ管理者は、定期的にセキュリティホール対策及びソフトウェア構成の状況を確認、分析し、不適切な状態にある電子計算機及び通信回線装置が確認された場合の対処を行うこと。

解説：電子計算機及び通信回線装置上のセキュリティホール対策及びソフトウェア構成の状況を確認し、対策を担保するための事項である。
「セキュリティホール対策及びソフトウェア構成」とは、導入されているソフトウェアの種類及びこれらのセキュリティホール対策状況のことである。調査の間隔については、短いほど効果が高いため、可能な範囲で短くすることが望ましい。「不適切な状態」とは、パッチが適用されていない等、セキュリティホール対策が講じられていない状態のことである。

(g) 情報システムセキュリティ責任者は、入手したセキュリティホールに関連する情報及び対策方法に関して、必要に応じ、他の情報システムセキュリティ責任者と共有すること。

解説： 公開されたセキュリティホールに関連する情報の入手及びセキュリティホール対策を効果的に実施するために、情報システムセキュリティ責任者間の連携を求める事項である。

2.2.2.2 不正プログラム対策

趣旨（必要性）

不正プログラムは、これに感染した情報システム及びデータを破壊することから完全性、可用性に対する脅威となるだけでなく、主体認証情報等の要機密情報を漏えいさせることから機密性に対する脅威ともなる。

さらに、不正プログラムに感染した情報システムは、他の情報システムの再感染を引き起こす危険性のほか、迷惑メールの送信やサービス不能攻撃等の踏み台として利用される危険性等他者に対するセキュリティ脅威の原因となり得る。

これらのことを勘案し、本項では、不正プログラムに関する対策基準として、情報システムの構築時及び運用時についての遵守事項を定める。

遵守事項

(1) 情報システムの構築時

【基本遵守事項】

(a) 情報システムセキュリティ責任者は、電子計算機（当該電子計算機で動作可能なアンチウイルスソフトウェア等が存在しない場合を除く。以下この項において同じ。）にアンチウイルスソフトウェア等を導入すること。

解説：動作可能なアンチウイルスソフトウェア等が存在する電子計算機について、アンチウイルスソフトウェア等を導入することを求める事項である。
なお、多くのメインフレームシステム並びにオペレーティングシステム及びアプリケーションを搭載していない電子計算機については、動作可能なアンチウイルスソフトウェアが存在しないため、本遵守事項は適用されない。ただし、アンチウイルスソフトウェア等が新たにサポートを開始する場合には、速やかな導入が求められることから、情報システムセキュリティ責任者は、該当する電子計算機の把握を行っておくとともに、アンチウイルスソフトウェア等に関するサポート情報に常に注意を払っておくことが望ましい。
なお、アンチウイルスソフトウェア等には、他社製品・技術だけでなく、同一社の製品でもアンチウイルスソフトウェアの他、パーソナルファイアウォールやスパイウェア対策ソフト等も含む。

(b) 情報システムセキュリティ責任者は、想定される不正プログラムの感染経路の全てにおいてアンチウイルスソフトウェア等により不正プログラム対策を実施すること。

解説：電子計算機以外の想定される感染経路に対しても、不正プログラム対策の実施を求める事項である。
不正プログラムの感染経路には、電子メール、ウェブ等のネットワーク経由のほか、不正プログラムに感染した外部電磁的記録媒体経由も考えられ、複数の感染経路を想定した対策が必要である。

【強化遵守事項】

(c) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システムセキュリティ責任者は、想定される不正プログラムの感染経路において、複数の種類のアンチウイルスソフトウェア等を組み合わせ、導入すること。

解説：複数の種類のアンチウイルスソフトウェア等を導入することにより効果的な不正プログラム対策の実施を求める事項である。
アンチウイルスソフトウェア等は、製品ごとに不正プログラム定義ファイルの提供時期及び種類が異なる。また、これらは現存する全ての不正プログラムを検知及び除去できるとは限らず、アンチウイルスソフトウェア等の不具合により不正プログラムの検知又は除去に失敗する危険性もある。このことから、不正プログラムによる被害が発生する可能性を低減させるため、感染経路において異なる製品や技術を組み合わせ、どれか１つの不具合で、その環境の全てが不正プログラムの被害を受けることのないようにする必要がある。例えば、メールサーバに導入するアンチウイルスソフトウェアと端末に導入するアンチウイルスソフトウェアを異なるパターンファイルを用いた製品にすること等が考えられる。

(d)　特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システムセキュリティ責任者は、想定される不正プログラムの感染経路において、拡散することを防止するための対策を実施すること。

解説：ネットワーク及び外部電磁的記録媒体を経由した感染拡大を防止することを求める事項である。ネットワークを経由した感染拡大の防止策としては、例えば、不正プログラム定義ファイル又はパッチ適用等が最新化されていない端末をネットワークに接続させない情報システムや、通信に不正プログラムが含まれていることを検知すると、その通信を検知したネットワークからの通信を遮断する情報システムの導入等が挙げられる。また、外部電磁的記録媒体を経由した感染拡大の防止策としては、例えば、自動再生機能の無効化、外部電磁的記録媒体の電子計算機接続時の手動検索、及びアンチウイルスソフトウェアのリアルタイム検索機能の有効化等が挙げられる。

(2)　情報システムの運用時

【基本遵守事項】

(a)　情報システムセキュリティ管理者は、不正プログラムに関する情報の収集に努め、当該情報について対処の要否を決定し、特段の対処が必要な場合には、職務従事者にその対処の実施に関する指示を行うこと。

解説：不正プログラムに対し特段の対処が必要な場合に実施することを求める事項である。

「特段の対処が必要な場合」とは、新たな不正プログラムの存在が明らかになった後でも利用中のアンチウイルスソフトウェア等に用いる定義ファイルが配布されない等、日常から行われている不正プログラム対策では対処が困難と判断される場合が挙げられる。

(b)　情報システムセキュリティ責任者は、不正プログラム対策の状況を適宜把握し、その見直しを行うこと。

解説：1.5.2.7(1)(a)の規定による統括情報セキュリティ責任者が整備する規程に基づいた対策の状況及び本項の対策の状況を適宜把握し、問題点が発見された場合は改善することを求める事項である。

2.2.2.3 サービス不能攻撃対策

趣旨（必要性）

インターネットを経由して外部に提供しているサービスを実現する電子計算機、並びにそのアクセスに利用される通信回線及び通信回線装置は、利用者が自由にアクセス可能である利便性を確保するために、サービス不能攻撃により、通常の利用者がサービスを利用できなくなるといった可用性に対するリスクがある。

このため、インターネットに接続しているサーバ装置、並びにそのアクセスに利用され

る通信回線及び通信回線装置については、高い可用性を維持するための対策が必要となる。この対策については、ソフトウェアのセキュリティホールを悪用する攻撃に対するものと、大量のアクセスによる攻撃に対するものに大別され、両者とも実施する必要がある。

これらのことを勘案し、本項では、サービス不能攻撃に関する対策基準として、情報システムの構築時及び運用時についての遵守事項を定める。

遵守事項

(1) 情報システムの構築時

【基本遵守事項】

(a) 情報システムセキュリティ責任者は、要安定情報を取り扱う情報システム（インターネットからアクセスを受ける電子計算機、通信回線装置又は通信回線を有する情報システムに限る。以下この項において同じ。）については、サービス提供に必要な電子計算機及び通信回線装置が装備している機能をサービス不能攻撃対策に活用すること。

解説：電子計算機や通信回線装置が設けている機能を有効にすることを求める事項である。

対策としては、例えば、3-way handshake 時のタイムアウトの短縮、各種 Flood 攻撃への防御機能、アプリケーションゲートウェイ機能、パケットフィルタリング機能を利用すること等が挙げられる。

(b) 情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、サービス不能攻撃を受けた場合に影響が最小となるように情報システムを構築すること。

解説：要安定情報を取り扱う情報システムがサービス不能攻撃を受けた場合の影響を分析し、情報システムを構築することを求める事項である。影響としては、通信回線の帯域圧迫によるアクセス障害や、サーバの処理能力低下等が考えられる。このため、例えば、サービス不能攻撃を受けたことを検出した場合には、即座に情報システムを外部ネットワークより遮断する、通信回線の通信量に制限をかける等といった手段を有する情報システムを構築する必要がある。

(c) 情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、サービス不能攻撃を受ける電子計算機、通信回線装置又は通信回線から監視対象を特定し、監視方法及び監視記録の保存期間を定めること。

解説：サービス不能攻撃に関する監視対象の特定と監視方法及び監視記録の保存期間を定めることを求める事項である。

インターネットからアクセスされるサーバ装置、そのアクセスに利用される通信回線装置及び通信回線の中から、特に高い可用性が求められるサーバ装置、通信回線装置及び通信回線を優先的に監視する必要がある。

「監視方法」については、サービス不能攻撃を受けることに関する監視には、稼動中か否かの状態把握、負荷の定量的な把握がある。監視方法は多種多様であるため、適切な方法を選択する必要がある。

「監視記録の保存期間」については、監視対象の状態の変動を把握するという目的に照らして、保存期間を定める必要がある。

(d) 情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、電子計算機や通信回線装置における対策だけでは大量のアクセスによるサービス不能攻撃を回避できないことを勘案し、インターネットに接続している通信回線を提供している事業者とサービス不能攻撃発生時の対処手順や連絡体制を整備すること。

解説：情報システムセキュリティ責任者が、電子計算機や通信回線装置に係るサービス不能攻撃の対策を実施しても、独立行政法人Ａ機構外へ接続する通信回線及び通信回線装置への過負荷の影響を完全に排除することは不可能である。このため、独立行政法人Ａ機構外へ接続する通信回線を提供している事業者へも対策の協力を依頼できる体制を整備することを求める事項である。

【強化遵守事項】

(e) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、電子計算機、通信回線装置又は通信回線に対するサービス不能攻撃の影響を排除し、又は低減する対策装置を導入すること。

解説：通信回線については、通信量の制限や通信の遮断が有効であり、サービス不能攻撃の影響を排除し、又は低減するために必要な装置の導入を求める事項である。例えば、巧みに偽装したパケットや正規の送信元アドレスを使用した巧妙な DDoS 攻撃を抑制するには、電子計算機及び通信回線装置が持つ既存のセキュリティ対策機能に加え、サービス不能攻撃の影響を排除し、又は低減することのできる専用の対策装置の導入が挙げられる。

(f) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、サービス不能攻撃を受けた場合に攻撃への対処を効果的に実施できる手段を確保しておくこと。

解説：大量のアクセスによるサービス不能攻撃を受け、サーバ装置、通信回線装置又は通信回線が過負荷状態に陥り利用できない場合における対処を効果的に実施するための事項である。

例えば、対処としては、サービス提供に利用している通信回線等がサービス不能攻撃により過負荷状態に陥っていても、サービス不能攻撃を受けているサーバ装置、通信回線装置及びそれらを保護するために設置されている対策装置を操作できる手段を確保することが挙げられる。より具体的には、管理者が当該装置等を操作するための電子計算機及び通信回線等を、サービス提供に利用している電子計算機及び通信回線等とは別に用意すること等が挙げられる。

(g) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システ

ムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、サービス提供に必要な電子計算機、通信回線装置又は通信回線を冗長構成にすること。

解説：サービス不能攻撃が発生した場合、サービスを提供する電子計算機、通信回線装置及び通信回線を代替電子計算機、代替通信回線装置又は代替通信回線に切り替えることにより、サービスが中断しないように、情報システムを構成することを求める事項である。
サービス不能攻撃の検知及び代替計算機等への切替えは短時間にできるようにすることが必要である。

(2) 情報システムの運用時

【基本遵守事項】

(a) 情報システムセキュリティ管理者は、要安定情報を取り扱う情報システムについては、監視方法が定められている場合は、監視方法に従って電子計算機、通信回線装置及び通信回線を監視し、その記録を保存すること。

解説：電子計算機、通信回線装置及び通信回線の通常時の状態を記録し把握することを求める事項である。
電子計算機、通信回線装置及び通信回線を監視している場合、監視対象の状態は一定ではなく変動することが一般的である。時間変動、曜日変動、週変動、月変動、季節変動を検討した上で記録を一定期間保存する。

2.2.2.4 踏み台対策

趣旨（必要性）

インターネット等の独立行政法人A機構外の通信回線に接続された情報システムは、第三者によって不正アクセスや迷惑メール配信の中継地点として、意図しない用途に使われてしまうこと、いわゆる、踏み台とされてしまうおそれがある。踏み台とされた情報システムは、独立行政法人A機構外に迷惑をかけるだけにとどまらず、例えば、当該情報システムが提供していたサービスを利用者が利用できないという可用性に対する水準の低下や、独立行政法人A機構内の他の情報システムに対するセキュリティ脅威の原因ともなり得る。これらを防ぐためには、独立行政法人A機構が意図しない目的で独立行政法人A機構の情報システムが使われないようにすることが必要である。

これらのことを勘案し、踏み台防止に関する対策基準として、情報システムの構築時及び運用時についての遵守事項を定める。

遵守事項

(1) 情報システムの構築時

【基本遵守事項】

(a) 情報システムセキュリティ責任者は、情報システム（インターネット等の独立行政法人A機構外の通信回線に接続される電子計算機、通信回線装置又は通信回線を

有する情報システムに限る。以下この項において同じ。）が踏み台として使われることを防止するための措置を講ずること。

解説：電子計算機等に対し、踏み台になることを避けるための対処の実施を求める事項である。

対策としては、アンチウイルスソフトウェア等の導入、セキュリティホールの対処、不要なサービスの削除、フィルタリング機能の有効化、不審なプログラムの実行禁止、アンチウイルスソフトウェア等で検出されないボットの通信の監視等が挙げられる。

(b) 情報システムセキュリティ責任者は、情報システムを踏み台として使われた場合の影響が最小となるように情報システムを構築すること。

解説：管理する情報システムを踏み台として使われた場合の影響を分析し、情報システムを構築することを求める事項である。影響としては、通信回線の帯域圧迫によるアクセス障害や、サーバの処理能力低下等が考えられる。このため、踏み台として使われたことを検出した場合には、即座に情報システムを外部ネットワークより遮断する、問題が発生している電子計算機のみ切り離す、等といった手段を有する情報システムを構築する必要がある。

【強化遵守事項】

(c) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システムセキュリティ責任者は、情報システムが踏み台になっているか否かを監視するための監視方法及び監視記録の保存期間を定めること。

解説：踏み台に関する監視方法及び監視記録の保存期間を定めることを求める事項である。

「監視方法」については、意図しない稼動負荷やインターネットへの通信の有無の把握、電子計算機に意図しない処理を行わせる命令の有無の監視等がある。監視方法は多種多様であるため、適切な方法を選択する必要がある。

「監視記録の保存期間」については、監視対象の状態の変動を把握するという目的に照らして、保存期間を定める必要がある。

(2) 情報システムの運用時

【強化遵守事項】

(a) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システムセキュリティ管理者は、定められた監視方法に従って情報システムを監視し、その記録を保存すること。

解説：情報システムの通常稼働時の状態を記録し把握することを求める事項である。

情報システムを監視している場合、監視対象の状態は一定ではなく変動することが一般的である。時間変動、曜日変動、週変動、月変動、季節変動を検討した上で記録を一定期間保存する。

第 2.3 部　情報システムの構成要素についての対策

2.3.1　施設と環境

2.3.1.1 電子計算機及び通信回線装置を設置する安全区域

趣旨（必要性）

電子計算機及び通信回線装置の設置環境について、悪意を持った者が電子計算機及び通信回線装置に物理的に接触できる状況においては、なりすまし、物理的な装置の破壊のほか、情報の漏えい又は改ざんが行われるおそれがある。また、設置環境に関する脅威としては、自然災害の発生により情報システムが損傷する等のおそれもある。

これらのことを勘案し、本項では、安全区域に関する対策基準として、安全区域への立入り及び退出、訪問者及び受渡業者、電子計算機及び通信回線装置のセキュリティ確保、安全区域内のセキュリティ管理並びに災害及び障害についての遵守事項を定める。

遵守事項

(1)　立入り及び退出の管理

【基本遵守事項】

(a)　情報システムセキュリティ責任者は、安全区域に不審者を立ち入らせない措置を講ずること。

解説：安全区域への不審者の立入りを防止し、安全区域のセキュリティを確保するための事項である。
措置としては、身分を確認できる物の提示の義務化、安全区域の所在の表示の制限等が挙げられる。
なお、本項の全ての遵守事項のうち、施設等の施設全体で対策が実施されている遵守事項については、当該対策を更に居室等ごとに実施することまでは求めておらず、施設における対策により代替可能である。

(b)　情報システムセキュリティ責任者は、要保護情報を取り扱う情報システムについては、安全区域を物理的に隔離し、立入り及び退出を管理するための措置を講ずること。

解説：要保護情報を取り扱う情報システムを構成する電子計算機及び通信回線装置が設置された安全区域を、物理的隔離及び立入り及び退出の管理によりセキュリティを確保するための事項である。
措置としては、壁、施錠可能な扉、パーティション等で囲むことで安全区域を隔離し、安全区域が無人になる際には扉を施錠する、当該鍵の貸し出しを管理するといった措置が挙げられる。安全区域の扉を開放したまま無人の状態にしてはならない。

【強化遵守事項】

(c)　特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システ

ムセキュリティ責任者は、安全区域へ立ち入る者が立入りを許可された者であるかの確認を行うための措置を講ずること。

解説：安全区域へ立ち入る者が立入りを許可された者であるかの確認を実施することで、許可されていない者の立入りを排除するための事項である。
なお、立入りを許可された者であるかの確認のために主体認証を行う機能を設けた場合は、立ち入る者の主体認証情報の管理に関する規定の整備、当該主体認証情報の読取防止のための措置を講ずること等が望ましい。

(d) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システムセキュリティ責任者は、安全区域から退出する者が立入りを許可された者であるかの確認を行うための措置を講ずること。

解説：立ち入った者の退出を把握するための事項である。

(e) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システムセキュリティ責任者は、立入りを許可された者が、立入りを許可されていない者を安全区域へ立ち入らせ、及び安全区域から退出させない措置を講ずること。

解説：安全区域の立入り及び退出時に立入りを許可された者であるかどうかの確認を確実に実施するための事項である。
対策としては、１人ずつでないと立入り及び退出が不可能な設備の利用、警備員の配置による目視確認等が挙げられる。

(f) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システムセキュリティ責任者は、安全区域へ継続的に立ち入る者を許可する手続を整備すること。また、その者の氏名、所属、立入許可日、立入期間及び許可事由を含む事項を記載するための文書を整備すること。

解説：文書を整備することで、安全区域へ継続的に立ち入る者を把握するための事項である。

(g) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システムセキュリティ責任者は、安全区域へ立入りを許可された者に変更がある場合には、当該変更の内容を前事項の文書へ反映させること。また、当該変更の記録を保存すること。

解説：変更の内容を前事項の文書へ反映することで安全区域へ継続的に立ち入る者を把握するための事項である。
また、変更内容についての記録を保存し、後で参照できるようにしておく必要がある。

(h) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システムセキュリティ責任者は、安全区域への全ての者の立入り及び当該区域からの退出を記録し及び監視するための措置を講ずること。

解説：安全区域への立入り及び当該区域からの退出の記録、監視を行い、安全区域のセキュリティが侵害された場合に追跡することができるようにするための事項である。
「記録し及び監視する」とは、警備員又は監視カメラ等による記録及び

監視のほか、安全区域への立入り及び当該区域からの退出を管理する装置における立入り及び退出の記録を取得し、当該立入り及び退出の記録を定期的に確認することが挙げられる。

(2) 訪問者及び受渡業者の管理

【強化遵守事項】

(a) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システムセキュリティ責任者は、安全区域への訪問者がある場合には、訪問者の氏名、所属及び訪問目的並びに訪問相手の氏名及び所属を確認するための措置を講ずること。

解説：訪問者の身元を確認するための事項である。

確認方法としては、例えば、訪問者に必要事項を記入させ、名刺又は社員証等と記入された内容とを照合する方法が挙げられる。

(b) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システムセキュリティ責任者は、安全区域への訪問者がある場合には、訪問者の氏名、所属及び訪問目的、訪問相手の氏名及び所属、訪問日並びに立入り及び退出の時刻を記録するための措置を講ずること。

解説：訪問記録の作成を求める事項である。

(c) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システムセキュリティ責任者は、安全区域への訪問者がある場合には、訪問相手の職務従事者が訪問者の安全区域への立入りについて審査するための手続を整備すること。

解説：訪問者の安全区域への立入りについて、訪問相手の職務従事者が審査するための手続を整備することを求める事項である。

手続としては、「警備員等が訪問相手の職務従事者に連絡し、訪問者の立入りについて審査する」、「訪問相手の職務従事者が、安全区域との境界線まで迎えに行き審査する」等の方法が挙げられる。

(d) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システムセキュリティ責任者は、訪問者の立ち入る区域を制限するための措置を講ずること。

解説：訪問者が許可されていない区域へ立ち入らないようにすることを求める事項である。措置の例としては、扉を施錠し許可された者のみが開閉可能にすることや警備員による訪問者の確認等の方法が挙げられる。

(e) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システムセキュリティ責任者は、安全区域内において訪問相手の職務従事者が訪問者に付き添うための措置を講ずること。

解説：訪問者が許可されていない区域へ立ち入らないように職務従事者が監視することを求める事項である。

(f) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システムセキュリティ責任者は、訪問者と継続的に立入りを許可された者とを外見上判断できる措置を講ずること。

解説：継続的に立入りを許可された者と訪問者を区別するための事項である。

これにより、許可されていない区域への訪問者の立入りが検知できる。対策としては、訪問者用の入館カードを作成し掲示を求める、訪問者の入館カード用ストラップの色を変える等が挙げられる。貸与した物は、訪問者の退出時に回収する必要がある。

(g) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システムセキュリティ責任者は、受渡業者と物品の受渡しを行う場合には、以下に挙げるいずれかの措置を講ずること。

(ア) 安全区域外で受渡しを行うこと。

(イ) 業者が安全区域へ立ち入る場合は、当該業者が安全区域内の電子計算機、通信回線装置、記録媒体に触れることができない場所に限定し、職務従事者が立ち会うこと。

解説：安全区域内の職務従事者と物品の受渡しを行う業者の立入りを制限するための事項である。「記録媒体」には電磁的記録媒体及び情報システムから出力された書面等の非電磁的な媒体が含まれる。

(3) 電子計算機及び通信回線装置のセキュリティ確保

【基本遵守事項】

(a) 情報システムセキュリティ責任者は、要保護情報を取り扱う情報システムについては、設置及び利用場所が確定している電子計算機の盗難及び当該場所からの不正な持ち出しを防止するための措置を講ずること。

解説：設置場所が固定された電子計算機に関して、盗難及び不正な持ち出しを防止するための事項である。

「設置及び利用場所が確定している」とは、サーバ装置及び据置き型 PC のように、設置及び利用する場所が固定され、他の場所で利用することがないという意味である。

対策としては、端末であればセキュリティワイヤーによる固定、サーバ装置であればサーバラックへの設置及び当該サーバラックの施錠、施設からの退出時における持ち物検査等が挙げられる。

なお、重要システムを設置している場合やサーバ室に設置している複数のサーバラックの運用主体が異なる場合、サーバラックの鍵を適切に管理すること等が考えられる。

【強化遵守事項】

(b) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システムセキュリティ責任者は、要保護情報を取り扱う情報システムについては、電子計算機及び通信回線装置を他の情報システムから物理的に隔離し、安全区域を共用しないこと。

解説：他の情報システムと共用の安全区域に設置していることにより安全性が確保できない場合に、安全区域を共用せずに物理的に隔離することを求める事項である。

(c) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システ

ムセキュリティ責任者は、要保護情報を取り扱う情報システムについては、設置及び利用場所が確定している通信回線装置の盗難及び当該場所からの不正な持ち出しを防止するための措置を講ずること。

解説：設置場所が固定された通信回線装置に関して、盗難及び不正な持ち出しを防止するための事項である。
対策としては、基幹の通信回線装置（ファイアウォール、ルータ、レイヤ３スイッチ、レイヤ２スイッチ等）であればサーバラックへの設置及び当該サーバラックの施錠、終端の通信回線装置（レイヤ２スイッチ等）であれば床下への埋設等が挙げられる。

(d) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システムセキュリティ責任者は、要機密情報を取り扱う情報システムについては、電子計算機及び通信回線装置の表示用デバイスを盗み見から保護するための措置を講ずること。

解説：電子計算機に接続されたディスプレイ、通信回線装置のメッセージ表示用ディスプレイ等を許可のない第三者に見られないように対策を実施することを求める事項である。
対策としては、偏光フィルタの利用等が挙げられる。

(e) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システムセキュリティ責任者は、要保護情報を取り扱う情報システムについては、情報システムで利用する電源ケーブル及び通信ケーブルを含む配線を、損傷及び盗聴を含む脅威から保護するための措置を講ずること。

解説：電源ケーブルの損傷及び通信ケーブルからの通信の盗聴等の脅威から、情報システムを保護するための事項である。
対策としては、ケーブルの床下への埋設、ケーブルのナンバリング等が挙げられる。

(f) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システムセキュリティ責任者は、要機密情報を取り扱う情報システムについては、電磁波による情報漏えい対策の措置を講ずること。

解説：ディスプレイケーブル等から生ずる電磁波による情報漏えいのリスクについて対策を講ずるための事項である。
具体的には、電磁波軽減フィルタの利用等が挙げられる。

(4) 安全区域内のセキュリティ管理

【基本遵守事項】

(a) 職務従事者は、安全区域内において、身分証明書を他の職務従事者から常時視認することが可能な状態にすること。

解説：安全区域への立入りを許可されていることを外見上判断できるようにするための事項である。

【強化遵守事項】

(b) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、職務従事者

は、情報システムセキュリティ責任者の許可を得た上で、要保護情報を取り扱う情報システムに関連する物品の安全区域への持込み及び安全区域からの持ち出しを行うこと。

解説：情報システムに関連する物品の持込み及び持ち出しによって生ずるリスクに対処するための事項である。

「情報システムに関連する物品」とは、安全区域に存在する情報システムで利用するための物品が挙げられ、これにはハードウェア、ソフトウェア、電磁的記録媒体及び情報システムから出力された書面等が含まれる。

(c) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システムセキュリティ責任者は、要保護情報を取り扱う情報システムに関連する物品の安全区域への持込み及び安全区域からの持ち出しに係る記録を保存すること。

解説：情報システムに関連する物品の持込み及び持ち出しを記録し、追跡性を確保するための事項である。記録を取得する項目としては、持込み及び持ち出しを行う者の名前及び所属、日時、物品又は事由等が挙げられる。

(d) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システムセキュリティ責任者は、要機密情報を取り扱う情報システムについては、情報システムに関連しない電子計算機、通信回線装置、電磁的記録媒体及び記録装置（音声、映像及び画像を記録するものを含む。）の安全区域への持込みについて制限すること。

解説：情報漏えいの原因となる可能性のある電子計算機、通信回線装置、電磁的記録媒体及び記録装置（音声、映像及び画像を記録するものを含む。）の持込みを制限するための事項である。

(e) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システムセキュリティ責任者は、安全区域内での作業を監視するための措置を講ずること。

解説：安全区域での作業を監視するための事項である。

第三者による立会いや、監視カメラの導入等が挙げられる。

(5) 災害及び障害への対策

【強化遵守事項】

(a) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、自然災害及び人為的災害から電子計算機及び通信回線装置を保護するための物理的な対策を講ずること。

解説：地震、火災、水害、停電、爆発及び騒じょう等の災害から電子計算機及び通信回線装置を保護するための事項である。

対策としては、サーバラックの利用のほか、ハロゲン化物消火設備、無停電電源装置等の設備、空調設備、耐震又は免震設備、非常口及び非常灯等の設置又は確保が挙げられる。

(b) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システ

ムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、安全区域内において災害又は障害が発生している場合には、作業する者の安全性を確保した上で必要な場合に電子計算機及び通信回線装置の電源を遮断できる措置を講ずること。

解説：作業する者が災害等により安全区域内に設置された電子計算機及び通信回線装置に近づくことができない場合に、作業する者の安全性を確保した上で電子計算機及び通信回線装置の電源を遮断できるようにするための事項である。

2.3.2　電子計算機

2.3.2.1 電子計算機共通対策

趣旨（必要性）

電子計算機の利用については、不正プログラム感染や不正侵入を受ける等の外部的要因により、保存されている情報の漏えい、改ざん又は当該電子計算機の機能停止等の被害に遭うおそれがある。また、職務従事者の不適切な利用等の内部的要因による情報セキュリティの侵害も起こり得る。このように電子計算機の利用は、当該電子計算機及び当該電子計算機が取り扱う情報の情報セキュリティが損なわれるおそれを有している。

これらのことを勘案し、本項では、電子計算機に関する対策基準として、電子計算機に関する設置時、運用時及び運用終了時についての遵守事項を定める。

遵守事項

(1)　電子計算機の設置時

【基本遵守事項】

(a)　情報システムセキュリティ責任者は、要安定情報を取り扱う電子計算機については、当該電子計算機に求められるシステム性能を将来の見通しを含め検討し、確保すること。

解説：通常の運用において十分な性能を確保することを求める事項である。
例えば、電子計算機の負荷に関して事前に見積もり、試験等を実施し、必要となる処理能力及び容量を想定し、それを備える必要がある。また、将来にわたっても十分な性能を確保できるように、拡張性や余裕を持たせておく必要がある。

(b)　情報システムセキュリティ責任者は、要保護情報を取り扱う情報システムについては、電子計算機を安全区域に設置すること。ただし、モバイル PC について情報セキュリティ責任者の承認を得た場合は、この限りでない。

解説：電子計算機が設置される物理的環境における脅威への対策を求める事項である。
人為的な脅威としては建物内への侵入、部外者による操作、失火による火災又は停電等があり、環境的脅威としては地震、落雷又は風水害等がある。そのため、物理的な隔離、入退者の主体認証装置、消火設備、耐震設備又は無停電電源装置等を利用する必要がある。

(c)　情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、サービス提供に必要な電子計算機を冗長構成にする必要性を検討し、必要と判断した場合には、その電子計算機を冗長構成にすること。

解説：障害・事故等が発生した場合、サービスを提供する電子計算機を代替電子計算機に切り替えること等により、サービスが中断しないように、情報システムを構成することを求める事項である。可用性を高めるためには、電子計算機本体だけでなく、ハードディスク等のコンポーネント単

位で冗長構成にすることも考えられる。
なお、災害等を想定して冗長構成にする場合には、代替の電子計算機を遠隔地に設置することが望ましい。

(d) 情報システムセキュリティ責任者は、職務従事者の離席時に、電子計算機を不正操作から保護するための措置を講ずること。

解説：職務従事者の離席時に、電子計算機を第三者による不正操作から保護するための事項である。
対策としては、例えば、スクリーンのロック等が挙げられる。スクリーンのロックについては、設定を義務付けるだけでなく、一定時間操作がないと自動的にロックする仕組み又は電子計算機のログインに利用する主体認証情報格納装置を事務室への立入りの許可の確認にも利用する方法等が考えられる。また、スクリーンのロックを設定できない電子計算機については、施錠管理可能な棚又はラック等に収納したり、キーボード、マウス及び USB ポート等を使用できないようにロックしたりする方法等が考えられる。

(2) 電子計算機の運用時

【基本遵守事項】

(a) 職務従事者は、職務の遂行以外の目的で電子計算機を利用しないこと。

解説：電子計算機を業務目的以外に利用することを禁止する事項である。例えば、悪意のあるウェブサイトを閲覧することによって、不正プログラムに感染させられてしまうことから回避するため、業務目的外でのウェブサイトの閲覧を禁止すること等が求められる。

(b) 職務従事者は、離席時に電子計算機を不正操作から保護するための措置を講ずること。

解説：職務従事者が、離席時に電子計算機を第三者による不正操作から保護するために、スクリーンのロック、ログオフ又は施錠管理等の実施を求める事項である。

【強化遵守事項】

(c) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システムセキュリティ責任者は、所管する範囲の電子計算機で利用されている全てのソフトウェアの状態を定期的に調査し、不適切な状態にある電子計算機を検出した場合には、当該不適切な状態の改善を図ること。

解説：電子計算機で利用されているソフトウェアの状態を定期的に調査し、不適切な状態にある場合にその改善を図ることを求める事項である。「定期的」とは、1 か月から 6 か月ごとに実施することを想定しており、短い期間で実施するとセキュリティ確保に効果的である。
また、「不適切な状態」とは、利用を許可されていないソフトウェアがインストールされている、ソフトウェアが動作するための適切な設定がなされていない、最新のセキュリティパッチが適用されていない等の状態

のことをいう。

(3) 電子計算機の運用終了時

【基本遵守事項】

(a) 情報システムセキュリティ責任者は、電子計算機の運用を終了する場合に、電子計算機の電磁的記録媒体の全ての情報を抹消すること。

解説：電子計算機の運用を終了する場合に、当該電子計算機に内蔵される電磁的記録媒体から、全ての情報を抹消することを求める事項である。

「ファイル削除」の操作ではファイル管理のリンクが切断されるだけであり、ファイルの情報自体は抹消されずに電磁的記録媒体に残留した状態となっているおそれがある。また、ファイルの情報自体へ別の情報を上書きした場合であっても残留磁気により復元される可能性があることが指摘されている。したがって、当該電磁的記録媒体に保存されている全ての情報を適切な方法で抹消する必要がある。

2.3.2.2 端末

趣旨（必要性）

端末については、当該端末を利用する者が専門的知識を有していない場合が多いことから、当該利用者の過失による不正プログラム感染等のリスクが高い。また、可搬性の高い端末については、紛失又は盗難のリスクも高くなる。

このように端末の利用は、その特性により、電子計算機に共通的なリスク以外にも情報セキュリティが損なわれるおそれを有している。

これらのことを勘案し、本項では、端末に関する対策基準として、端末の設置時及び運用時についての遵守事項を定める。

遵守事項

(1) 端末の設置時

【基本遵守事項】

(a) 情報システムセキュリティ責任者は、端末で利用可能なソフトウェアを定めること。ただし、利用可能なソフトウェアを列挙することが困難な場合には、利用不可能なソフトウェアを列挙し、又は両者を併用することができる。

解説：多様なソフトウェアを利用することによりセキュリティホール等の脅威が増大し、その対処が困難となる可能性があるため、端末で利用するソフトウェアを制限することを求める事項である。

(b) 情報システムセキュリティ責任者は、要保護情報を取り扱うモバイル PC については、独立行政法人Ａ機構外で使われる際にも、独立行政法人Ａ機構内で利用される端末と同等の保護手段が有効に機能するように構成すること。

解説：独立行政法人Ａ機構外で利用されるモバイル PC は、独立行政法人Ａ機構内で利用される端末と異なる条件下に置かれるため、独立行政法人Ａ

機構外で端末が利用される際の保護手段として、端末で動作するパーソナルファイアウォール等の具備を求める事項である。
例えば、モバイル PC が通常接続される通信回線で実施されているアクセス制御及び監視等は、他の通信回線では同等に実施されているとは限らないため、モバイル PC において実施する必要がある。

(c) 職務従事者は、モバイル PC を利用する必要がある場合には、情報システムセキュリティ責任者の承認を得ること。

解説：モバイル PC には様々なセキュリティ上のリスクが考えられるため、不必要にリスクを増大させないために、業務上必要なモバイル PC の利用にとどめるための事項である。

(d) 情報システムセキュリティ責任者は、要機密情報を取り扱うモバイル PC については、電磁的記録媒体に保存される情報の暗号化を行う機能を設けること。

解説：モバイル PC が物理的に外部の者の手に渡った場合には、モバイル PC から取り外された内蔵電磁的記録媒体、及びモバイル PC で利用していた外部電磁的記録媒体を他の電子計算機を利用して解読する等の攻撃によって要機密情報が読み取られる危険性がある。このような情報漏えいの対策として、端末に暗号化機能を装備することを求める事項である。

(e) 情報システムセキュリティ責任者は、要保護情報を取り扱うモバイル PC については、盗難防止及び盗難後の被害を軽減するための措置を定めること。

解説：モバイル PC は容易に搬出することが可能なため盗難又は紛失に遭う可能性が高いことから、情報システムセキュリティ責任者にその対策を定めることを求める事項である。
対策としては、独立行政法人A機構内においては、モバイル PC を安全区域内に設置している場合においても固定物又は搬出が困難な物体と容易に切断できないセキュリティワイヤーでつなぐことや、帰宅時に施錠できるキャビネットに保存すること、独立行政法人A機構外においては、常に身近に置き目を離さないこと等が挙げられる。盗難後の被害を軽減するための具体的な措置としては、例えば、遠隔データ消去機能等が挙げられる。

【強化遵守事項】

(f) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システムセキュリティ責任者は、職務従事者が情報を保存できない端末を用いて情報システムを構築すること。

解説：端末から情報が漏えいすることを防ぐために、シンクライアント等の端末を利用することを求める事項である。

(2) 端末の運用時

【基本遵守事項】

(a) 職務従事者は、端末で利用可能と定められたソフトウェアを除いて、ソフトウェアを利用しないこと。

解説：多様なソフトウェアを実行することによりセキュリティホール等の脅威が増大することから、定められたソフトウェア以外の利用を禁止する事項である。

(b) 職務従事者は、要保護情報を取り扱うモバイル PC を利用する場合には、盗難防止措置を行うこと。

解説：モバイル PC を利用する職務従事者に対して、モバイル PC の盗難防止措置について、情報システムセキュリティ責任者が定めた手順に従い、措置を実施することを求める事項である。

(c) 職務従事者は、要機密情報を取り扱うモバイル PC については、モバイル PC を独立行政法人A機構外に持ち出す場合に、当該モバイル PC で利用する電磁的記録媒体に保存されている要機密情報の暗号化を行う必要性の有無を検討し、必要があると認めたときは、情報を暗号化すること。

解説： モバイル PC で利用する電磁的記録媒体の紛失又は盗難により保存されている情報が漏えいすることを防ぐため、必要に応じて、ハードディスク、USB メモリ等に記録されている情報に対してファイル又は電磁的記録媒体全体を暗号化することを求める事項である。暗号化する方法としては、ハードディスク全体やファイルを暗号化するソフトウェアの導入や OS に標準装備されている暗号化機能の使用が挙げられる。

(d) 職務従事者は、情報システムセキュリティ責任者が接続許可を与えた通信回線以外に端末を接続しないこと。

解説：適切な管理がなされていない通信回線に端末を接続することにより、通信傍受等の脅威にさらされることを回避するための事項である。
独立行政法人某C機構内通信回線でも許可を得た通信回線以外に接続してはならない。モバイル PC を独立行政法人A機構外に持ち出した際に接続する通信回線についても接続許可を得る必要がある。

【強化遵守事項】

(e) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システムセキュリティ管理者は、情報システムにおいて基準となる時刻に、端末の時刻を同期すること。

解説：情報システム内で同期されている基準となる時刻に、端末の時刻を同期させることを求める事項である。
情報セキュリティが侵害された際に、時刻が同期していないとログの解析等が困難になる。標準時との同期が望ましいが、情報システム内で同期が取られていれば差し支えない。

2.3.2.3 サーバ装置

趣旨（必要性）

サーバ装置については、当該サーバ装置の電磁的記録媒体等に大量の情報を保存してい

る場合が多いことから、当該情報の漏えい又は改ざんによる影響も端末と比較して大きなものとなる。

また、サーバ装置は、通信回線等を介してその機能が利用される場合が多く、不正プログラム感染や不正侵入等を受けるリスクが高い。独立行政法人Ａ機構が有するサーバ装置が不正アクセスや迷惑メール送信の中継地点に利用されるようなことになれば、外部の人々からの信頼を大きく損なうことにもなる。さらに、サーバ装置は、同時に多くの者が利用できるため、その機能が停止した場合に与える影響が大きい。

このようにサーバ装置の利用は、その特性により、電子計算機に共通的なリスク以外にも情報セキュリティが損なわれるおそれを有している。

これらのことを勘案し、本項では、サーバ装置に関する対策基準として、サーバ装置の設置時及び運用時についての遵守事項を定める。

遵守事項

(1)　サーバ装置の設置時

【基本遵守事項】

(a)　情報システムセキュリティ責任者は、通信回線を経由してサーバ装置の保守作業を行う場合は、通信を秘匿する必要性の有無を検討し、必要があると認めたときは、送受信される情報を秘匿するための機能を設けること。この場合、独立行政法人Ａ機構外通信回線を経由する保守作業については、通信を秘匿する必要があると判断すること。

解説：通信回線を経由してサーバ装置の保守作業を行う際のセキュリティ強化を求める事項である。

情報システムセキュリティ責任者から保守作業を許可されている者がサーバ装置へログオンして作業する場合を想定し、例えばインターネットを介してサーバ装置の保守作業を行う場合等、通信の秘匿する必要がある場合には、設置時に暗号化するための機能を設け、運用時に実際の情報の暗号化を実施できるようにしておくこと等が考えられる。

(b)　情報システムセキュリティ責任者は、サービスの提供及びサーバ装置の運用管理に利用するソフトウェアを定めること。

解説：サーバ装置において、サービスの提供及びサーバ装置の運用管理に必要となるソフトウェアを定めるための事項である。必要なソフトウェアを定める方法としては、サーバ装置の仕様書において定める、独立の文書として定める等が挙げられる。

(c)　情報システムセキュリティ責任者は、利用が定められたソフトウェアに該当しないサーバアプリケーションが稼動している場合には、当該サーバアプリケーションを停止すること。また、利用が定められたソフトウェアに該当するサーバアプリケーションであっても、利用しない機能を無効化して稼動すること。

解説：不要なサーバアプリケーションの停止及び不要な機能の無効化により、サーバ装置から潜在的な脅威を排除するための事項である。なお、ソフトウェアの設定は初期状態が安全であるとは限らないことについても留

意して確認すること。

【強化遵守事項】

(d) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システムセキュリティ責任者は、利用が定められたソフトウェアに該当しないソフトウェアをサーバ装置から削除すること。

解説：利用が定められたソフトウェアに該当しないものが導入されている場合、利用を禁止していても不正侵入した攻撃者等に悪用される可能性があるため、当該ソフトウェアをサーバ装置から削除することを求める事項である。

(e) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システムセキュリティ管理者は、要安定情報を取り扱うサーバ装置の内、サービス提供に必要なサーバ装置については、負荷を複数のサーバ装置に分散又はサーバ装置を冗長構成とすること。

解説：障害や過度のアクセス等によりサービスが提供できない事態となることを防ぐため、複数のサーバ装置による負荷分散、負荷分散装置の設置、DNS による負荷分散又は冗長構成等の実施を求める事項である。

(2) サーバ装置の運用時

【基本遵守事項】

(a) 情報システムセキュリティ責任者は、定期的にサーバ装置の構成の変更を確認すること。また、当該変更によって生ずるサーバ装置のセキュリティへの影響を特定し、対処すること。

解説：サーバ装置のソフトウェア及びハードウェア等の構成が不正に変更されていないか定期的に確認し、また、変更によるセキュリティレベルの低下等が発生していないか検討し、変更状況に応じて対処することを求める事項である。

(b) 情報システムセキュリティ管理者は、要安定情報を取り扱うサーバ装置については、サーバ装置の運用状態を復元するために必要な措置を講ずること。

解説：サーバ装置の運用状態を復元するための必要な措置を講ずることによりサーバ装置に保存されている情報及びその情報を用いたサービスの可用性の担保を目的とした事項である。

サーバ装置の運用状態を復元するための必要な措置の例として、以下のようなものがある。

・サーバ装置の運用に必要なソフトウェアの原本を別に用意しておく。

・前回内容からの変更部分の定期的なバックアップを実施する。

なお、取得した情報を記録した電磁的記録媒体は、施錠された保管庫に保存等して、業務上の必要がある場合にこれらの情報を利用する情報システムセキュリティ管理者に限ってアクセスできるようにする。また、災害等を想定してバックアップを取得する場合には、記録媒体を遠隔地に保存することが考えられる。「定期的」とは、1 日又は 1 週ごとに実施

することを想定しており、短い期間で実施するとセキュリティ確保に効果的である。

(c) 情報システムセキュリティ管理者は、サーバ装置の運用管理について、作業日、作業を行ったサーバ装置、作業内容及び作業者を含む事項を記録すること。

解説：運用管理作業の記録を文書として残すための事項である。

独立行政法人Ａ機構において、ある程度統一的な様式を作成する必要がある。

(d) 情報システムセキュリティ管理者は、情報システムにおいて基準となる時刻に、サーバ装置の時刻を同期すること。

解説：情報システム内で同期されている基準となる時刻にサーバ装置を同期させることを求める事項である。

情報セキュリティが侵害された際に、時刻が同期していないとログの解析等が困難になる。標準時との同期が望ましいが、情報システム内で同期が取られていれば差し支えない。

【強化遵守事項】

(e) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システムセキュリティ管理者は、サーバ装置のセキュリティ状態を監視すること。

解説：サーバ装置のセキュリティ状態を監視するための事項である。

「セキュリティ状態を監視」するとは、サーバ装置上での不正な行為及び無許可のアクセス等の意図しない事象の発生を監視することである。

監視の方法の例としては、アクセスログを定期的に確認することや、侵入検知システム、アンチウイルスソフトウェア又はファイル完全性チェックツール等の利用が挙げられる。

(f) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システムセキュリティ管理者は、要安定情報を取り扱うサーバ装置について、当該サーバ装置のシステム状態を監視し、当該サーバ装置に関する障害等の発生を検知すること。

解説：日常的なサーバ装置のシステム状態について監視を行うことで、障害等の発生を早期に検出し、またこの影響の拡大を未然に防止するための事項である。

「システム状態を監視」するとは、サーバ装置の CPU、メモリ、ディスク入出力等の性能及び故障等を監視することである。監視方法は、状況に応じて、ツールの利用、手動から、適切な方法を選択することが可能である。

2.3.3　アプリケーションソフトウェア

2.3.3.1 電子メール

趣旨（必要性）

電子メールの送受信とは情報のやり取りにほかならないため、不適切な利用により情報が漏えいする等の機密性に対するリスクがある。また、電子メールサーバに過負荷等が加えられることによって、機能が損なわれる等の可用性に対するリスクがある。この他、内容を偽ったメールによるいわゆるフィッシング詐欺等に電子メールを利用する職務従事者が巻き込まれるリスクもある。このようなリスクを回避するためには、適切な電子メールサーバの管理及び電子メールの利用が必要である。

これらのことを勘案し、本項では、電子メールサーバの管理及び電子メールの利用に関する対策基準として、電子メールの導入時及び運用時についての遵守事項を定める。

遵守事項

(1)　電子メールの導入時

【基本遵守事項】

(a)　情報システムセキュリティ責任者は、電子メールサーバが電子メールの不正な中継を行わないように設定すること。

解説：迷惑メールの送信等に使われることを回避するために、電子メールを不正に中継しないように電子メールサーバを設定することを求める事項である。

(b)　情報システムセキュリティ責任者は、電子メールクライアントから電子メールサーバへの電子メールの受信時及び送信時に職務従事者の主体認証を行う機能を備えること。

解説：電子メールの受信時に限らず、送信時においても不正な利用を排除するために SMTP 認証等の主体認証を行うことを定めた事項である。

(c)　情報システムセキュリティ責任者は、電子メールの送信元について、なりすましの防止策を講ずること。

解説：「なりすましの防止策」には、送信ドメイン認証(SPF)（具体的には、DNS サーバへの SPF レコードの記録）、及びメールマガジンへの電子署名の添付等が挙げられる。

なお、SPF レコードを登録する際、電子メールサーバを外部委託先において運用している場合には、外部委託先のグローバル IP アドレスを独立行政法人A機構のものとして SPF レコードに登録することは、同じ IP アドレスを民間業者も共用し、なりすましのおそれがある。このため、外部委託先には、同じサーバの他の利用者によるなりすまし防止策を講じたり、政府ドメイン名を使用する機関向けに民間業者と共用しない専用の IP アドレスを割り振られた場合を除き、認められない。

(2)　電子メールの運用時

【基本遵守事項】

(a)　職務従事者は、業務遂行に係る情報を含む電子メールを送受信する場合には、独立行政法人Ａ機構が運営し、又は外部委託した電子メールサーバにより提供される電子メールサービスを利用すること。ただし、独立行政法人Ａ機構支給以外の情報システムによる情報処理について許可を得ている者については、この限りでない。

解説：独立行政法人Ａ機構が運営し、又は外部委託した電子メールサーバにより提供される電子メールサービス以外の電子メールサービス（以下「独立行政法人Ａ機構以外の電子メールサービス」という。）を、業務遂行に係る情報を含む電子メールの送受信に利用することを禁ずる事項である。

なお、上記の「送受信」には電子メールの「転送」が含まれている。したがって、独立行政法人Ａ機構以外の電子メールサービスの電子メールアドレスに業務遂行に係る情報を含む電子メールを転送することは、許可を得ている場合を除き、認められない。特に、自動転送については、許可を受けている場合であっても、当該電子メールに含まれる情報の格付及び取扱制限にかかわらず行われるため、要機密情報の移送についての遵守事項に違反しないようにも留意する必要がある。

(b)　職務従事者は、受信した電子メールにより、スクリプトが電子計算機で実行されないように電子メールの内容を表示させること。

解説：例えば HTML メールの表示により、偽のウェブサイトに誘導するために表示が偽装されること、意図しないファイルが外部から取り込まれること等の不正なスクリプトが実行されることを防ぐことを定めた事項である。

「スクリプト」とは、ここでは JavaScript 等の電子計算機にて簡易的に実行することができるプログラムをいう。

「スクリプトが電子計算機で実行されないように表示させる」とは、表示をテキスト形式のみに設定して表示することや端末でスクリプトの実行を禁止された情報システムを用いて表示することが挙げられる。

そのため、情報システムの管理者により、職務従事者が使用する電子メールクライアントの設定が上述のとおり適切に行われ、かつ、職務従事者が電子メールクライアントの設定を勝手に変更しないよう制限することにより対策を実施することも考えられる。

なお、本遵守事項は、スクリプトが電子計算機で実行されないのであれば、電子メールの文字装飾や画像の表示を禁止するものではない。

また、本遵守事項は、端末等にインストールされる電子メールクライアントを対象としているため、ウェブブラウザにより読み書きする電子メール（いわゆるウェブメール）は対象外となる。

2.3.3.2 ウェブ

趣旨（必要性）

ウェブを利用するに当たっては、サーバにおいて、OS 等既成のソフトウェアや開発したウェブアプリケーション等の複数の要素で構成されていること、一方で、クライアントにおいてもサーバと同様に情報処理が行われていることから、様々な脅威が考えられる。

これらのリスクを回避するためには、システムのライフサイクル全般に対して適切な対策を組み合わせて実施することが必要である。

これらのことを勘案し、本項では、ウェブに関する対策基準として、ウェブサーバの導入、ウェブアプリケーションの開発、ウェブの運用についての遵守事項を定める。

なお、ウェブサーバの導入及び運用については、本項に加えて、2.3.2.3 にて定めたサーバ装置に係る対策基準を、また、サービス不能攻撃等のウェブにおける脅威への対策としては、2.2.2.3 にて定めた情報セキュリティについての脅威に係る対策基準を参照する必要がある。

遵守事項

(1)　ウェブサーバの導入時

【基本遵守事項】

(a)　情報システムセキュリティ責任者は、情報セキュリティが確保されるよう適切にウェブサーバのセキュリティ設定をすること。適切なセキュリティ設定として、以下に挙げる事項を含む措置を講ずること。

(ア) ウェブサーバの機能を適切に制限すること。

(イ) ウェブサーバに保存された情報へのアクセス制限を適切に設定すること。

(ウ) 識別コードを適切に管理すること。

(エ) 通信時の盗聴による情報漏えいのリスクを検討し、必要と判断した場合には、暗号化と電子証明書による認証の機能を設けること。

解説：ウェブサーバの導入時の設定に関して以下の項目を適切に行うことにより、セキュリティを確保することを求める事項である。

（ア）は、ウェブサーバで提供する機能の内、不要な機能を停止又は制限することを求めている。例えば、スクリプトやファイル実行の制限や保存場所の限定、インデックス表示の禁止、ホームページ作成ツールやコンテンツマネジメントシステム(CMS)等における不要な機能の制限等が挙げられる。

（イ）は、情報の漏えいやウェブページの改ざんを防ぐために、情報へのアクセス権限を適切に設定することを求めている。例えば、ウェブコンテンツファイルへのアクセス権限は、コンテンツの作成や更新に必要な者以外に更新権を与えない、公開を想定していないファイルをウェブ公開用ディレクトリに置かない等が挙げられる。

（ウ）は、OS やアプリケーションのインストール時に、標準で作成される識別コードやテスト用に作成した識別コード等の適切な管理を求めて

いる。これらの識別コードはブルートフォース(総当たり)攻撃の標的になるリスクがあるため、その必要性を確認して、不要なものは削除することが重要である。また、初期状態で用意されるサンプルのページ、プログラム等も削除するといった注意が必要である。

（エ）は、通信時の盗聴による第三者への情報漏えいの防止及びウェブサーバの詐称を利用者が検知できるようにするための事項である。第三者への漏えいを防止する必要のある情報には、例えば、サービスの利用者の個人情報等が挙げられる。ウェブサーバにおいてこれらを解決するための機能としては、例えば、SSL 及び TLS が挙げられる。この機能を設けることにより、通信内容の暗号化が可能になるとともに、ウェブサーバの利用者は、ウェブサーバの電子証明書を参照することでその正当性を確認することができる。

なお、独立行政法人A機構のウェブサーバに電子署名を付与する必要があると認めたときの SSL 及び TLS に用いる電子証明書は、政府認証基盤（GPKI）で発行したものを使用することが望ましい。

【強化遵守事項】

(b) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システムセキュリティ責任者は、要機密情報を取り扱う情報システムについては、ウェブサーバに保存する情報を特定し、当該サーバに要機密情報が含まれないことを確認すること。

解説：万が一、不正侵入等が発生した場合であっても、当該サーバから要機密情報が漏えいしないよう、被害範囲の限定を図るための事項である。

全ての利用者が利用することが想定されているデータを除き、特定の利用者のみが利用するデータ等を、ウェブサーバに保存しないことが必要である。

(2) ウェブアプリケーションの開発時

【基本遵守事項】

(a) 情報システムセキュリティ責任者は、情報セキュリティが適切に確保されるようにウェブアプリケーションの開発においてセキュリティ対策機能を組み込むこと。適切なセキュリティ機能として、以下に挙げる事項を含む措置を講じること。

(ア) 利用者による URL の確認を妨げないこと。
(イ) 主体認証と情報へのアクセス制御を適切に行うこと。
(ウ) ウェブアプリケーションが使用するファイルのパス名を限定すること。
(エ) 不正な入力データを排除すること。
(オ) 不正な出力データを排除すること。
(カ) 安全なセッション管理を行うこと。

解説：ウェブアプリケーションの開発を行う場合に、以下のセキュリティ機能を実装することにより、セキュリティを確保することを求める事項である。

なお、セキュリティ機能の実装方法の詳細については、独立行政法人情報処理推進機構(IPA)による「セキュアプログラミング講座」（http://www.ipa.go.jp/security/awareness/vendor/programming/index.html）の「Web アプリケーション編」または、「安全なウェブサイトの作り方」（http://www.ipa.go.jp/security/vuln/websecurity.html）を適宜参照することが望ましい。

（ア）は、利用者が URL（ウェブアドレス）を確認できない場合、攻撃者が用意した危険なサイト（フィッシングサイト等）に誘導される可能性があることから、それを避けることを求めるものである。この対策としては、例えば、アドレスバーを隠さない、右クリックを無効にしない等が挙げられる。

（イ）は、主体認証を行うウェブアプリケーションにおいて、パスワード等の漏えいによる利用者のなりすまし防止や主体認証後の利用者のファイルへのアクセスについて適切に制御することを求めるものである。ユーザ ID とパスワードによって主体認証を行う場合、例えば、パスワードの設定時にその文字列に適切な条件を課す、利用者本人がパスワードを変更できるようにする、入力されたパスワードは隠し文字にして表示しない等の対策が挙げられる。また、利用者が設定したパスワードはハッシュ関数を用いて復元できない形にすることも重要である。ファイルへのアクセス制御については、ウェブサイトでどの主体がどの情報にアクセスする必要があるのかについて検討し、それに基づきアクセス制御を設計・実装することが重要である。特に、主体認証後にのみ参照可能なファイルが主体認証前に参照できてしまうことがないよう、適切にアクセス制御を行うことが求められる。

（ウ）は、ウェブアプリケーションが使用するファイルのパス名を外部のパラメータから指定する仕様になっていると、公開を想定しないファイルが参照されるリスクがあり、これを防止することを求めるものである。この対策としては、外部のパラメータからパス名を指定する仕様を排除するのが安全だが、これができない場合は、例えば、ファイルにアクセスする前に入力されたパラメータの検査を行う、ファイルのディレクトリと識別子を固定の文字列にしてアクセスする等の方法が挙げられる。

（エ）、ウェブサーバを用いて提供するサービスにおいて、利用者から文字列等の入力を受ける場合には、不当な入力データを排除することによって、バッファオーバフロー攻撃や SQL インジェクション等の攻撃を防ぐことを求めるものである。対策としては、例えば、ウェブアプリケーションへの入力を正しく定義し、不正なデータが渡されないよう、入力されたパラメータの長さや内容を検査し、無害化する機能を設ける等が挙げられる。

（オ）は、ウェブアプリケーションが出力する画面や OS の関数、SQL

コマンド等の呼び出しといった出力情報に不正なデータの混入を排除することにより、クロスサイトスクリプティングや SQL インジェクション等の攻撃を防止することを求めるものである。対策としては、例えば、HTML に埋め込むデータを全て検査してエスケープ処理する、外部プログラムを呼び出す際のプログラム名、オプション、パラメータ等はできる限り固定の文字列にする等が挙げられる。また、ウェブアプリケーション又はデータベース等から発信されるエラーメッセージ、稼動している製品名及びそのバージョン、登録されているユーザ ID 等は、攻撃を試みる者に対し攻撃の糸口となり得る情報を与えてしまう危険性がある。これらのことを回避するため、不必要な情報は出力しない措置を講じることが求められる。

（カ）は、セッション管理の不備により利用者になりすましてアクセスされることを防止するため、適切なセション管理を求めるものである。対策としては、例えば、セション ID の有効期間を主体認証直後のレスポンスからログアウトまでに限定する、推測困難なセッション ID を設定する、セッション ID を URL パラメータに格納しない、Cookie に入れる情報はセッション ID 以外に必要最小限とする、SSL を使用する Cookie は secure 属性にする等が挙げられる。

【強化遵守事項】

(b) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システムセキュリティ責任者は、ウェブサーバを用いて提供するサービスが特定のウェブブラウザに依存しないように情報システムを構築すること。

解説：万一、特定の種類のウェブブラウザに脆弱性が発見され、利用する危険性が高くなった場合においても、他の種類のウェブブラウザも利用可能とすることで、提供するサービスを継続可能にすることを求める事項である。そのためには、例えば、2 種類以上のウェブブラウザ又は同一製品の異なるバージョンで動作するように、情報システムの構築時に配慮し、その動作確認をおこなうことが考えられる。なお、開発時に公開されているバージョンだけでなく、例えば、利用を想定しているブラウザの次期バージョンについて、正式リリース前に情報が公開されたり、プレビュー版での動作検証可能な状態にあれば、前もって利用可能かどうかを検証する等、その後に公開が想定されるバージョンにも対応できるよう、構築時に配慮することが望ましい。

(3) ウェブの運用時

【基本遵守事項】

(a) 職務従事者は､情報セキュリティの確保がなされるよう適切にウェブクライアントのセキュリティ設定をすること。

解説：職務従事者が意図しない悪意のあるソフトウェアが電子計算機において実行されること等により、情報が漏えいしてしまうことや他の電子計算

機を攻撃してしまうこと等を防止するため、ウェブクライアントのセキュリティ設定を適切に行うことを求める事項である。
具体的には、閲覧するウェブサイトの信頼性やウェブクライアントが動作する電子計算機にて扱う情報の機密性等に応じて、以下のようなセキュリティ設定項目について適切な値を選択すること。
・ActiveX コントロールの実行
・JavaScript の実行
・Java の実行
・Cookie の保存等
そのため、情報システムの管理者がウェブクライアントのセキュリティ設定を上述のとおり行い、かつ、職務従事者が当該設定を勝手に変更しないよう制限することにより対策を実施することも考えられる。

(b) 職務従事者は、ウェブクライアントが動作する電子計算機にソフトウェアをダウンロードする場合には、電子署名により当該ソフトウェアの配布元を確認すること。

解説：ソフトウェアをダウンロードする場合は、電子署名により配布元の正当性を確認することを求める事項である。

(c) 職務従事者は、閲覧しているウェブサイトに表示されるフォームに要機密情報を入力して送信する場合には、以下の事項を確認すること。

(ア) 送信内容が暗号化されること。

解説：主体認証情報等を入力して送信する場合には、情報漏えいを防止するため、ブラウザの鍵アイコンの表示を確認する等により、SSL や TLS 等の暗号通信が使用されていること等の手段を限定することを求める事項である。なお、「閲覧しているウェブサイトに表示されるフォームに要機密情報を入力して送信する場合」とは、例えばウェブメールを使用する際に主体認証情報等を入力すること等を指す。

(イ) 当該ウェブサイトが送信先として想定している組織のものであること。

解説：主体認証情報等を入力して送信する場合には、ウェブサーバの電子証明書の内容から当該ウェブサイトが想定している組織のものであるかを確認することにより、当該情報の送信先を限定することを求める事項である。なお、ウェブサイトの閲覧時にウェブサーバの電子証明書が適切でない旨の警告ダイアログが表示された場合には、当該ウェブサイトがなりすましに利用されている可能性がないかを確認することが必要である。

【強化遵守事項】

(d) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システムセキュリティ責任者は、職務従事者が閲覧することが可能な独立行政法人Ａ機構外のウェブサイトを制限し、定期的にその見直しを行うこと。

解説：ウェブサイトからの不適切なソフトウェアのダウンロードや私的なウェブサイトの閲覧を制限するため、コンテンツフィルタ等により閲覧することが可能な範囲の制限を定める事項である。
情報システムセキュリティ責任者は、制限を実施する方法として、ウェ

ブクライアント、ウェブプロキシ及びその他の装置の設定等、状況に応じて、適切な方法を選択することが可能である。

2.3.3.3 ドメインネームシステム（DNS）

趣旨（必要性）

ドメインネームシステム（DNS : Domain Name System）は、クライアント等からの問い合わせを受けて、ドメイン名やホスト名と IP アドレスとの対応関係について回答を行うインターネットの基盤をなすサービスである。DNS の可用性が損なわれた場合は、ホスト名やドメイン名を使ったウェブや電子メール等の利用が不可能となる。また DNS が提供する情報の完全性が損なわれ、誤った情報を提供した場合は、クライアント等が悪意あるサーバに接続させられる等の被害にあう可能性がある。このようなリスクを回避するためには、DNS サーバの適切な管理が必要である。

これらのことを勘案し、本項では、DNS に関する対策基準として、DNS の導入時及び運用時についての遵守事項を定める。

遵守事項

(1) DNS の導入時

【基本遵守事項】

(a) 情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムの名前解決を提供する DNS のコンテンツサーバにおいて、名前解決を停止させないための措置を講ずること。

解説：要安定情報を取り扱う情報システムの名前解決を提供する DNS のコンテンツサーバにおいて、名前解決を停止させないために、求められる可用性の度合いに応じた措置を求める事項である。

DNS のコンテンツサーバは、冗長化しておくことが一般的である。その際には、ネットワーク障害等を考慮して各々の DNS のコンテンツサーバをそれぞれ異なるネットワークに配置しておく、災害等を考慮して物理的に離れた建物や遠隔地に設置しておく等、情報と情報システムに要求される可用性に応じて、最適な構成を検討する必要がある。ISP 等が提供するセカンダリ DNS の利用も、冗長化による措置の例である。あるいは、悪意ある者からのサービス不能攻撃に備え、ソフトウェアや通信回線装置で適切なアクセス制御を実施しておくことも重要である。

また、要求される可用性の度合いに応じて、保守作業による復旧等、冗長化以外の措置を探ることも考えられる。

(b) 情報システムセキュリティ責任者は、DNS のコンテンツサーバにおいて管理するドメインに関する情報を運用管理するための手続を定めること。

解説：DNS のコンテンツサーバにおいて管理するドメインに関する情報（ゾーン情報）を運用管理するための手続を定めることを求める事項である。

「管理するドメインに関する情報を運用管理するための手続」では、例えば、管理するドメインに関する情報の設定や更新、正確性の維持等の手順や管理するドメインの構成範囲を明確化しておくことが考えられる。

(c) 情報システムセキュリティ責任者は、DNS のキャッシュサーバにおいて、名前解決の要求への適切な応答をするための措置を講ずること。

解説：DNS のキャッシュサーバの第三者による不正利用やキャッシュ情報の汚染等を防ぐための措置を講ずることを求める事項である。キャッシュサーバにおいては、独立行政法人A機構外からの名前解決の要求には応じず、独立行政法人A機構内からの名前解決の要求のみに回答を行うように措置を講ずる必要がある。キャッシュサーバを動作させる場合は、サーバの設定やファイアウォール等でアクセス制御を行うことが重要である。

また、適正な名前解決の代行を維持するために、ルートヒントファイルの更新の有無を定期的に確認し、最新のものに維持する必要がある。「定期的」とは、3ヶ月に一度程度実施することを想定している。

(d) 情報システムセキュリティ責任者は、DNS のコンテンツサーバにおいて、独立行政法人A機構内のみで使用する名前の解決を提供する場合、当該情報が外部に漏えいしないための措置を講ずること。

解説：DNS のコンテンツサーバにおいて、独立行政法人A機構内のみで使用する名前の解決を提供する場合、独立行政法人A機構の職務従事者以外の者が内部のみで使用している名前情報を取得できないようにすることを求める事項である。例えば、内部向けの名前解決を提供するコンテンツサーバを外部向けのコンテンツサーバとは別々に設置し、サーバの設定やファイアウォール等でアクセス制御を行う等の方法が考えられる。

【強化遵守事項】

(e) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システムセキュリティ責任者は、重要な情報システムに対し名前解決を提供する DNS サーバにおいて、コンテンツサーバによるドメイン名の情報提供時には電子署名を付与し、キャッシュサーバによる名前解決時には電子署名を検証すること。

解説：電子署名によって DNS のコンテンツサーバのなりすましや同サーバからの提供情報の改ざんを DNS のキャッシュサーバで検出できるようにすることを求める事項である。その対策としては、DNSSEC の利用等が挙げられる。

DNSSEC は、公開鍵暗号技術を用いて改ざん等を防止するため、その導入には情報の提供側である DNS のコンテンツサーバと情報の問い合わせ側である DNS のキャッシュサーバの双方に対応が必要となる。

外部の人々等への信頼できるサービスの提供と、独立行政法人A機構内の情報セキュリティ向上の観点から、政府系ドメインを管理する DNS のコンテンツサーバ、及び独立行政法人A機構の DNS のキャッシュサーバに対する円滑な DNSSEC の導入が望ましい。

(2) DNS の運用時

【基本遵守事項】

(a) 情報システムセキュリティ管理者は、DNS のコンテンツサーバを複数台設置する場合は、管理するドメインに関する情報についてサーバ間で整合性を維持すること。

解説：複数台の DNS のコンテンツサーバが保有し管理するドメインに関する情報について、整合性を維持することを求める事項である。例えば、主系統のコンテンツサーバの管理するドメインに関する情報が変更された場合に、ゾーン転送等によって、情報システムの可用性に影響を及ぼさない適切なタイミングで副系統のコンテンツサーバの管理するドメインに関する情報も更新するといった方法が考えられる。

なお、主系統のコンテンツサーバから副系統のコンテンツサーバへ安全にゾーン転送を行う対策として、例えば、TSIG の利用等が考えられる。

(b) 情報システムセキュリティ管理者は、DNS のコンテンツサーバにおいて管理するドメインに関する情報を運用管理するための手続に基づいて、当該情報が正確であることを適宜確認すること。

解説：管理するドメインに関する情報が正確であるかどうかを確認することを求める事項である。管理するドメインに関する情報の設定ミスや不正な改ざん等が発生していないかを確認する必要がある。

2.3.4　通信回線

2.3.4.1 通信回線共通対策

趣旨（必要性）

通信回線の利用については、当該通信回線の不正利用、これに接続された電子計算機又は通信回線装置への不正アクセス、送受信される情報の盗聴、改ざん及び破壊等、当該通信回線を含む情報システム及び当該情報システムが取り扱う情報の情報セキュリティが損なわれるおそれを有している。

これらのことを勘案し、本項では、通信回線に関する対策基準として、通信回線の構築時、運用時及び運用終了時についての遵守事項を定める。

遵守事項

(1)　通信回線の構築時

【基本遵守事項】

(a)　情報システムセキュリティ責任者は、通信回線構築によるリスクを検討し、通信回線を構築すること。

解説：情報システムセキュリティ責任者は、通信回線構築によるリスクを考慮して、通信回線の構築及び運用開始を判断する必要がある。独立行政法人Ａ機構外通信回線と接続する場合のリスク軽減措置としては、例えば、ファイアウォールやウェブアプリケーションファイアウォール(WAF)等を利用する方法が考えられる。リスクを検討した結果、情報システムセキュリティ責任者は、情報システムのセキュリティが確保できないと判断した場合には、他の通信回線から独立させて閉鎖的な通信回線とするか、通信回線を構築しない等の判断を行うことが望ましい。なお、物理的に分割されたシステムに限らず、論理的に分割されたシステム間の通信も同様に考慮すること。(「論理的に分割されたシステム」とは、一つの情報システムのきょう体上に複数のシステムを共存させることを目的として、論理的に分割させた状態の情報システムをいう。例えば、仮想化ソフトウェアを利用することが考えられる。なお、仮想化ソフトウェアとは、１つのハードウェアで複数のオペレーティングシステムを同時に実行する機能を有するソフトウェアをいう。以下同様。)

(b)　情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、通信回線及び通信回線装置に求められる通信性能を発揮できる能力を、将来の見通しを含め検討し、確保すること。

解説：通常の運用において十分な通信回線の能力を確保し、情報の可用性を確保するための事項である。例えば、通信回線の負荷に関して事前に試験等を実施し、必要となる容量及び能力を想定する等の対策が考えられる。なお、将来にわたっても十分な容量及び能力を確保できるように、余裕を持たせておく必要がある。

(c) 情報システムセキュリティ責任者は、通信回線装置が動作するために必要なソフトウェアを定めること。ただし、ソフトウェアを変更することが困難な通信回線装置の場合は、この限りでない。

解説：通信回線装置としての機能や動作の明確化を行うとともに、セキュリティホール等の脅威への対処を確実なものとするために、通信回線装置が必要とするソフトウェアを定めておくことを求める事項である。

(d) 情報システムセキュリティ責任者は、通信回線に接続される電子計算機をグループ化し、それぞれ通信回線上で分離すること。

解説：電子計算機が接続されている通信回線の境界で効果的にアクセス制御するために、まず電子計算機をグループ化し通信回線上で分離することを求める事項である。独立行政法人Ａ機構外通信回線と接続する独立行政法人Ａ機構内通信回線の場合は、独立行政法人Ａ機構外通信回線上の電子計算機は、独立行政法人Ａ機構内通信回線に接続される電子計算機とは別のグループとし、分離する必要がある。

なお、「グループ化」とは、対象機器をその利用目的、求められるセキュリティレベル、管理部署等から分類することをいう。

(e) 情報システムセキュリティ責任者は、グループ化された電子計算機間での通信要件を検討し、当該通信要件に従って通信回線装置を利用し、アクセス制御及び経路制御を行うこと。

解説：グループ化された電子計算機間の通信の制御を行うことで、セキュリティを確保するための事項である。情報システムセキュリティ責任者は、グループ化された電子計算機間で情報システムの運用上必要となる通信を全て確認した上で、通信要件を検討する必要がある。必要最小限のアクセスのみを許可するように、当該通信要件に従ってアクセス制御を行う。

(f) 情報システムセキュリティ責任者は、要機密情報を取り扱う情報システムについては、通信を秘匿する必要性の有無を検討し、必要があると認めたときは、通信を秘匿するための機能を設けること。

解説：通信における要機密情報を保護するための事項である。情報システムセキュリティ責任者は、通信回線上を要機密情報が送受信される場合には、当該情報の秘匿の必要性を検討して、運用時の暗号化に備えて構築時にそのための機能を設けておく必要がある。

また、通信路の暗号化は、情報の機密性だけでなく完全性を保護する上でも有用である。

なお、通信路の暗号化のために、例えば、IPsec、SSL 及び TLS 等を使用することも考えられる。

(g) 情報システムセキュリティ責任者は、要保護情報を取り扱う情報システムについては、通信回線に利用する物理的な回線のセキュリティを検討し、適切な回線を選択すること。

解説：通信回線に利用する物理的な回線（例えば、有線 LAN における LAN ケ

ーブル、無線 LAN における伝搬路等の通信路）の種別によって、盗聴、改ざん等の脅威及びそれらに対する有効なセキュリティ措置が異なることから、適切な回線を選択することを求める事項である。
回線に応じたセキュリティ対策を実施する必要があるが、回線によってはセキュリティ対策を実施しても万全でない場合もあるので、回線の選択に当たっては十分に検討する必要がある。また、通信回線を仮想的に構築する場合には、物理的に同一の通信回線となる場合があることに注意する必要がある。

(h) 情報システムセキュリティ責任者は、遠隔地から通信回線装置に対して、保守又は診断のために利用するサービスによる接続についてセキュリティを確保すること。

解説： 遠隔地からの通信回線装置の保守や診断に利用するサービスのセキュリティを確保するための事項である。セキュリティ確保の方法として、識別コード及び主体認証情報（パスワード）による主体認証、接続する電子計算機の識別コードによるアクセス制御、通信の暗号化等の機密性の確保だけでなく、通信回線が利用できない状況での代替接続手段の確保等の可用性の確保も挙げられる。

(i) 情報システムセキュリティ責任者は、通信回線装置を安全区域に設置すること。

解説：通信回線装置及び通信ケーブルが設置される物理的環境における脅威への対策を求める事項である。

(j) 情報システムセキュリティ責任者は、電気通信事業者の専用線サービスを利用する場合には、セキュリティレベル及びサービスレベルを含む事項に関して契約時に取り決めておくこと。

解説：独立行政法人Ａ機構内通信回線同士を専用線で接続する場合に、当該専用線のサービスレベルを確保するための事項である。
情報システムセキュリティ責任者自身が契約を行わない場合には、セキュリティレベル及びサービスレベルを含む事項の取決めについて、契約する者に対して依頼すること。なお、セキュリティレベル及びサービスレベルが約款に記述されていれば、それで代替することが可能である。

(k) 情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、サービス提供に必要な通信回線又は通信回線装置を冗長構成にする必要性を検討し、必要と判断した場合には、その通信回線又は通信回線装置を冗長構成にすること。

解説：障害・事故等によりサービスを提供できない状態が発生した場合、サービスを提供する通信回線又は通信回線装置を代替通信回線又は代替通信回線装置に切り替えること等により、サービスが中断しないように、情報システムを構成することを求める事項である。

【強化遵守事項】

(l) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システムセキュリティ責任者は、通信を行う電子計算機の主体認証を行うこと。

解説：通信を行う電子計算機の主体認証を行うことで、通信相手の電子計算機

が正しい相手であることを確認するための事項である。

(2) 通信回線の運用時

【基本遵守事項】

(a) 情報システムセキュリティ管理者は、通信回線装置のソフトウェアを変更する場合には、情報システムセキュリティ責任者の許可を得ること。

解説：通信回線装置のソフトウェアは機能の改善等を目的に変更を行う必要が生ずる場合がある。この変更の必要性が生じた時に、情報システムセキュリティ管理者は、独断での変更は行わず、情報システムセキュリティ責任者の許可を得てから行う事を求める事項である。

(b) 情報システムセキュリティ管理者は、通信回線及び通信回線装置の運用管理について、作業日、作業を行った通信回線及び通信回線装置並びに作業内容及び作業者を含む事項を記録すること。

解説：運用管理作業の記録を文書として残すための事項である。
独立行政法人Ａ機構において、ある程度統一的な様式を作成することが望ましい。

(c) 情報システムセキュリティ責任者は、情報システムのセキュリティの確保が困難な事由が発生した場合には、他の情報システムと共有している通信回線から独立した閉鎖的な通信回線に構成を変更すること。

解説：他の情報システムと通信回線を共有している場合であって、情報システムのセキュリティの確保が困難な事由が発生した時に、他の情報システムを保護するための事項である。

(d) 職務従事者は、情報システムセキュリティ責任者の許可を受けていない電子計算機及び通信回線装置を通信回線に接続しないこと。

解説：通信回線に無断で電子計算機及び通信回線装置を接続された場合に生ずるリスクを防止するための事項である。

(e) 情報システムセキュリティ管理者は、情報システムにおいて基準となる時刻に、通信回線装置の時刻を同期すること。

解説：情報システム内で同期されている共通の時刻に設置した通信回線装置の時刻を同期させることを求める事項である。
有事の際に、時刻が同期していないとログの解析等が困難になる。標準時との同期が望ましいが、情報システム内で同期が取られていれば差し支えないものとする。

【強化遵守事項】

(f) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システムセキュリティ責任者は、所管する範囲の通信回線装置が動作するために必要な全てのソフトウェアの状態を定期的に調査し、不適切な状態にある通信回線装置を検出した場合には、当該不適切な状態の改善を図ること。ただし、ソフトウェアを変更することが困難な通信回線装置の場合は、この限りでない。

解説：通信回線装置における不正なソフトウェアの存在確認等を定期的に行い、対処がなされていない場合にその改善を図ることを求める事項である。

「定期的」とは、1 か月から 6 か月ごとに実施することを想定しており、短い期間で実施するとセキュリティ確保に効果的である。
なお、「不適切な状態」とは、許可されていないソフトウェアがインストールされている、定められたソフトウェアが動作するための適切な設定がなされていない等の状態のことをいう。

(g) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システムセキュリティ管理者は、通信回線装置を不正操作から保護するための措置を講ずること。

解説：情報システムセキュリティ管理者が通信回線装置を第三者による不正操作から保護するための事項である。対策としては、コンソールターミナル等での作業終了後の確実なログアウト、施錠可能なラック内への設置等が挙げられる。

(3) 通信回線の運用終了時

【基本遵守事項】

(a) 情報システムセキュリティ責任者は、通信回線装置の利用を終了する場合には、通信回線装置の電磁的記録媒体の全ての情報を抹消すること。

解説：運用を終了した通信回線装置が再利用され、又は廃棄された後、終了前に保存していた情報が漏えいすることを防ぐために、情報の抹消を求める事項である。
抹消の方法としては、通信回線装置の初期化、内蔵電磁的記録媒体の物理的な破壊等の方法がある。

2.3.4.2 独立行政法人A機構内通信回線の管理

趣旨（必要性）

独立行政法人Ａ機構内通信回線の利用については、当該通信回線の不正利用、これに接続された電子計算機又は通信回線装置への不正アクセス、送受信される情報の盗聴、改ざん及び破壊等、当該通信回線を含む情報システム及び当該情報システムが取り扱う情報の情報セキュリティが損なわれるおそれを有している。また、利用する回線により想定される脅威及びリスクが異なる。

これらのことを勘案し、本項では、独立行政法人Ａ機構内通信回線に関する対策基準として、独立行政法人Ａ機構内通信回線の構築時及び運用時、回線の対策についての遵守事項を定める。

遵守事項

(1) 独立行政法人Ａ機構内通信回線の構築時

【強化遵守事項】

(a) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システ

ムセキュリティ責任者は、通信回線装置に物理的に接続した電子計算機を、通信回線に論理的に接続する前に、当該電子計算機が通信回線に接続することを許可されたものであることを確認するための措置を講ずること。

解説：通信回線に接続する電子計算機の確認を行うことを求める事項である。当該措置を実施するための技術としては、電子計算機固有の情報による主体認証、IEEE 802.1x 等が挙げられる。

(2) 独立行政法人Ａ機構内通信回線の運用時

【強化遵守事項】

(a) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システムセキュリティ責任者は、通信要件の変更の際及び定期的に、アクセス制御の設定の見直しを行うこと。

解説：適正なアクセス制御の維持を求める事項である。通信要件については、組織、情報システム又はサービスの変更等により変化するため、当該変更等に応じてアクセス制御の設定も見直す必要がある。「定期的」とは、６か月から１２か月ごとに実施することを想定しており、短い期間で実施するとセキュリティ確保に効果的である。また、必ずしも当該変更等が適時連絡されるとは限らないので、情報システムセキュリティ責任者は定期的にアクセス制御の設定の見直しを行う。

(b) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システムセキュリティ管理者は、要安定情報を取り扱う情報システムについては、日常的に、通信回線の利用状況及び状態を確認、分析し、通信回線の性能低下及び異常を推測し、又は検知すること。

解説：確保している性能では適正な運用が困難な状態及び通信回線装置等の故障により通信不能な状態等により、情報の可用性を損なう事態を回避するため、通信回線の利用状況及び状態の確認を求める事項である。問題の発生を推測でき、又は検知できた場合には、事前に対策を行うことが求められる。

(c) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システムセキュリティ管理者は、独立行政法人Ａ機構内通信回線上を送受信される通信内容を監視すること。

解説：通信回線上を送受信される情報から不正アクセス行為を検知するための事項である。「通信内容を監視する」とは、侵入検知システム等を利用して、通信される情報から不正な行為及び無許可のアクセス等の意図しない事象の発生がないかを監視することが挙げられる。

(3) 回線の対策

【基本遵守事項】

(a) 情報システムセキュリティ責任者は、VPN 環境を構築する場合には、以下に挙げる事項を含む措置の必要性の有無を検討し、必要と認めたときは措置を講ずること。

（ア）利用開始及び利用停止時の申請手続の整備
（イ）通信内容の暗号化
（ウ）通信を行う電子計算機の識別又は利用者の主体認証
（エ）主体認証記録の取得及び管理
（オ）VPN 経由でアクセスすることが可能な通信回線の範囲の制限
（カ）VPN 接続方法の機密性の確保
（キ）VPN を利用する電子計算機の管理

解説：VPN を利用して論理的な独立行政法人Ａ機構内通信回線を構築する場合に、セキュリティを確保することを求める事項である。「VPN」には、インターネット VPN、IP-VPN、SSL-VPN 等が挙げられる。

(b) 情報システムセキュリティ責任者は、無線 LAN 環境を構築する場合には、以下に挙げる事項を含む措置の必要性の有無を検討し、必要と認めたときは措置を講ずること。この場合、要機密情報を取り扱う無線 LAN 環境については、通信内容の暗号化を行う必要性があると判断すること。

（ア）利用開始及び利用停止時の申請手続の整備
（イ）通信内容の暗号化
（ウ）通信を行う電子計算機の識別又は利用者の主体認証
（エ）主体認証記録の取得及び管理
（オ）無線 LAN 経由でアクセスすることが可能な通信回線の範囲の制限
（カ）無線 LAN に接続中に他の通信回線との接続の禁止
（キ）無線 LAN 接続方法の機密性の確保
（ク）無線 LAN に接続する電子計算機の管理

解説：無線 LAN を利用して論理的な独立行政法人Ａ機構内通信回線を構築する場合に、セキュリティを確保することを求める事項である。
なお、要機密情報を取り扱う無線 LAN 環境については、通信内容の暗号化を求めているが、WEP（Wired Equivalent Privacy）、TKIP（Temporal Key Integrity Protocol）等は、比較的容易に解読できたり、通信の妨害を発生させることができるという脆弱性が報告されており、また同様の問題が起こる可能性があるため、最新の情報に従い適切な方式や設定値を選択すること。この場合、暗号化については、暗号と電子署名の標準手順に従わなければならない。
参考：総務省「国民のための情報セキュリティサイト」の「情報管理担当者のための情報セキュリティ対策－実践編」（http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/j_business/admin00.htm）にある、「安全な無線 LAN の利用」のページの解説を適宜参照。

(c) 情報システムセキュリティ責任者は、公衆電話網を経由したリモートアクセス環境を構築する場合には、以下に挙げる事項を含む措置の必要性の有無を検討し、必要と認めたときは措置を講ずること。

(ア) 利用開始及び利用停止時の申請手続の整備
(イ) 通信を行う者又は発信者番号による識別及び主体認証
(ウ) 主体認証記録の取得及び管理
(エ) リモートアクセス経由でアクセスすることが可能な通信回線の範囲の制限
(オ) リモートアクセス中に他の通信回線との接続の禁止
(カ) リモートアクセス方法の機密性の確保
(キ) リモートアクセスする電子計算機の管理

解説：公衆電話網を経由してリモートアクセスを利用する場合に、セキュリティを確保することを求める事項である。

2.3.4.3 独立行政法人A機構外通信回線との接続

趣旨（必要性）

独立行政法人Ａ機構内通信回線と独立行政法人Ａ機構外通信回線との接続については、独立行政法人Ａ機構外通信回線に接続された電子計算機からの不正アクセス、サービス不能攻撃等のほか、独立行政法人Ａ機構外通信回線に送受信される情報の漏えい、改ざん又は破壊等、独立行政法人Ａ機構外通信回線を含む情報システム及び当該情報システムが取り扱う情報の情報セキュリティが損なわれるおそれを有している。

これらのことを勘案し、本項では、独立行政法人Ａ機構外通信回線と接続する場合の独立行政法人Ａ機構内通信回線に関する対策基準として、独立行政法人Ａ機構内通信回線と独立行政法人Ａ機構外通信回線との接続時及び運用時についての遵守事項を定める。

遵守事項

(1) 独立行政法人Ａ機構内通信回線と独立行政法人Ａ機構外通信回線との接続時

【基本遵守事項】

(a) 情報システムセキュリティ責任者は、情報セキュリティ責任者の許可を得た上で、独立行政法人Ａ機構内通信回線を独立行政法人Ａ機構外通信回線と接続すること。

解説：独立行政法人Ａ機構内通信回線を独立行政法人Ａ機構外通信回線と接続するとリスクの増大を招くので、情報セキュリティ責任者の判断を得ることを求める事項である。情報セキュリティ責任者は、様々なリスクを検討した上で許可の可否を判断する必要がある。

(b) 情報システムセキュリティ責任者は、独立行政法人Ａ機構内通信回線を独立行政法人Ａ機構外通信回線と接続することにより情報システムのセキュリティが確保できないと判断した場合には、他の情報システムと共有している独立行政法人Ａ機構内通信回線又は独立行政法人Ａ機構外通信回線から独立した通信回線として独立行政法人Ａ機構内通信回線を構築すること。

解説：独立行政法人Ａ機構内通信回線に接続している情報システムを、独立行政法人Ａ機構外からの脅威から保護するための事項である。セキュリティの確保が困難な情報システムについては、他の情報システムと共有している独立行政法人Ａ機構内通信回線から独立した通信回線として構成

するか、独立行政法人Ａ機構外通信回線から切断した通信回線として構築することになる。独立した通信回線の場合でも、遵守すべき対策基準は実施する必要がある。

(2) 独立行政法人Ａ機構外通信回線と接続している独立行政法人Ａ機構内通信回線の運用時

【基本遵守事項】

(a) 情報システムセキュリティ責任者は、情報システムのセキュリティの確保が困難な事由が発生した場合には、他の情報システムと共有している独立行政法人Ａ機構内通信回線又は独立行政法人Ａ機構外通信回線から独立した通信回線に構成を変更すること。

解説：他の情報システムと通信回線を共有している場合であって、情報システムのセキュリティの確保が困難な事由が発生した時に、他の情報システムを保護するための事項である。

(b) 情報システムセキュリティ責任者は、通信回線の変更の際及び定期的に、アクセス制御の設定の見直しを行うこと。

解説：適正なアクセス制御の維持を求める事項である。通信要件については、組織、情報システム又はサービスの変更等により変化するため、当該変更等に応じてアクセス制御の設定を見直す必要がある。「定期的」とは、３か月から６か月ごとに実施することを想定しており、短い期間で実施するとセキュリティ確保に効果的である。また、必ずしも当該変更等が適時連絡されるとは限らないので、情報システムセキュリティ責任者は定期的にアクセス制御の設定の見直しを行う。

(c) 情報システムセキュリティ管理者は、要安定情報を取り扱う情報システムについては、日常的に、通信回線の利用状況及び状態を確認、分析し、通信回線の性能低下及び異常を推測し、又は検知すること。

解説：確保している性能では適正な運用が困難な状態及び通信回線装置等の故障により通信不能な状態等により、情報の可用性を損なう事態を回避するため、通信回線の利用状況及び状態の確認を求める事項である。問題の発生を推測でき、又は検知できた場合には、事前に対策を行うことが求められる。

(d) 情報システムセキュリティ管理者は、独立行政法人Ａ機構内通信回線と独立行政法人Ａ機構外通信回線との間で送受信される通信内容を監視すること。

解説：独立行政法人Ａ機構外通信回線と送受信される情報から不正アクセス行為を検知するための事項である。「通信内容を監視する」とは、侵入検知システム等を利用して、通信される情報から不正アクセス等の行為がないかを監視することが挙げられる。

第 2.4 部　個別事項についての対策

2.4.1　その他

2.4.1.1 情報システムへの IPv6 技術の導入における対策

趣旨（必要性）

独立行政法人A機構ではインターネットの規格である IPv6 通信プロトコルに対応するための取組が進められているが、現在広く使用されている IPv4 通信プロトコルからの移行過程においては、新旧の規格が共存することから、十分に検討し、適切な措置を講じないと、情報システムのセキュリティを損なうおそれがある。また、昨今、電子計算機及び通信回線装置には IPv6 技術を利用する通信機能が標準で備わっているものが増えていることから、意図せず IPv6 技術を利用する通信機能が動作している可能性がある。このため、情報システムの IPv6 対応化計画の有無にかかわらず、IPv4 技術を利用する通信と IPv6 技術を利用する通信が共存する環境を前提として、対策を講ずる必要がある。

これらのことを勘案し、本項では、IPv4 技術を利用する通信と IPv6 技術を利用する通信が共存する情報システムのセキュリティ確保に関する対策基準を定める。

遵守事項

(1)　IPv6 移行機構がもたらす脆弱性対策

【基本遵守事項】

(a)　情報システムセキュリティ責任者は、情報システムに IPv6 技術を利用する通信（以下「IPv6 通信」という。）の機能を導入する場合には、IPv6 移行機構が他の情報システムに情報セキュリティ上の脅威を及ぼすことを防止するため、必要な措置を講ずること。

解説：IPv4 技術を利用する通信と IPv6 通信の両方を共存させることを可能とする IPv6 移行機構の選定と利用に当たり、必要な措置を求める事項である。

IPv6 通信プロトコルに対応している端末やサーバ装置には、多様な IPv6 移行機構（デュアルスタック機構、IPv6-IPv4 トンネル機構等）が実装されている。それらの IPv6 移行機構は、それぞれが想定する使用方法と要件に基づき設計されていることから、その選定と利用に当たっては、セキュリティホールの原因をつくらないよう十分な検討と措置が必要である。

例えば、デュアルスタック機構を運用する場合には、IPv4 のプライベートアドレスを利用したイントラネットの情報システムであっても外部ネットワークとの IPv6 通信が可能となるため、デュアルスタック機構を導入した電子計算機を経由した当該外部ネットワークからの攻撃について対策を講ずる必要がある。また、IPv6-IPv4 トンネル機構を運用する場

合、トンネルの終端が適切に管理されないと本来通信を想定しないネットワーク間の IPv6 通信が既設の IPv4 ネットワークを使って可能となるため、独立行政法人A機構内のネットワークが外部から攻撃される危険性がある。管理された電子計算機以外のトンネル通信を当該 IPv4 ネットワークに設置されたファイアウォールにて遮断する等、不適切な IPv6 通信を制御する対策が必要である。

(2) 意図しない IPv6 通信の抑止と監視

【基本遵守事項】

(a) 情報システムセキュリティ責任者は、IPv6 通信を想定していない通信回線に接続される全ての電子計算機及び通信回線装置に対して、IPv6 通信を抑止するための措置を講ずること。

解説：通信回線が IPv6 通信を想定していない場合には、当該通信回線に接続される端末等の IPv6 通信の機能を停止する措置を求める事項である。

IPv6 通信を想定していない通信回線においては、ファイアウォールや侵入検知システム等のセキュリティ機能に不正な IPv6 通信を制御する措置が講じられず、悪意ある者による IPv6 通信を使った攻撃に対して無防備となるおそれがある。さらに、IPv6 通信が可能な電子計算機においては、IPv4 ネットワークに接続している時でも IPv6 通信による当該電子計算機への接続を可能とする自動トンネリング機能を提供するものがある。この機能を利用すると、電子計算機と外部のネットワークとの間に利用者や管理者が気付かないうちに意図しない経路が自動生成され、これがセキュリティを損なうバックドアとなりかねないことから、自動トンネリング機能を動作させないよう電子計算機を設定する必要がある。また、ルータ等の通信回線装置についても IPv6 通信をしないよう設定し、意図しない IPv6 通信を制限することが求められる。

【強化遵守事項】

(b) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、情報システムセキュリティ責任者は、IPv6 通信を想定していない通信回線を監視し、IPv6 通信が検知された場合には通信している装置を特定し、IPv6 通信を遮断するための措置を講ずること。

解説：意図しない IPv6 通信が情報システムに与える脅威から情報システムを守るための事項である。

IPv6 技術にはアドレスの自動構成機構が提供されている。電子計算機から送出されるアドレスの自動構成を要求する通信パケットや、ルータから送出されるアドレスの自動構成を提供する通信パケットが独立行政法人A機構内通信回線を流れている場合には、管理者や利用者が気付かないうちに IPv6 技術のアドレス自動構成機構が利用されていることを示唆している。また、IPv6 通信を想定していない独立行政法人A機構内通信回線において、IPv6-IPv4 トンネル機構で使用する通信パケットが検

知された場合は、IPv6 技術を使った悪意のある通信がなされているおそれがある。独立行政法人Ａ機構内通信回線を管理する者は、このような通信の有無を監視して、IPv6 通信が検知された場合は、当該通信の遮断等の措置を講ずる必要がある。

A.1 解説書別添資料

A.1.1 組織・体制イメージ図

管理基準に準じる。

A.1.2 取扱制限の種類に係る付表例

管理基準に準じる。

A.1.3 情報セキュリティ対策に関するＢ省が所管する独立行政法人等群における決定等

管理基準に準じる。

A.1.4 用語解説

管理基準に準じる。

以下は、技術基準で初出の用語。

【あ】

● 「暗号モジュール」とは、暗号化及び電子署名の付与に使用するアルゴリズムを実装したハードウェア、ソフトウェア、ファームウェア及びそれらの組合せをいう。

【か】

● 「強制アクセス制御（MAC：Mandatory Access Control)」とは、主体が客体(情報、ファイル等)に設定したアクセス制御について、その設定の継承を情報システムが強制的に行う方式をいう。強制アクセス制御の機能を備えた情報システムでは、主体が客体を保護すべき対象とした場合には、アクセスを許可された者であっても、それを保護すべき対象ではないものとすることはできない。すなわち、主体が設定したアクセス制御の継承は、任意ではなく強制されることになる。

【た】

● 「耐タンパー性」とは、暗号処理や署名処理を行うソフトウェアやハードウェアに対する外部からの解読攻撃に対する耐性をいう。
● 「電子メールクライアント」とは、電子メールサーバにアクセスし、電子メールの送受信を行うアプリケーションをいう。

【な】

● 「名前解決」とは、ドメイン名やホスト名と IP アドレスを変換することをいう。

【ま】

● 「無線 LAN」とは、無線通信で情報を送受信する通信回線をいう。無線 LAN の規格としては、802.11a、802.11b、802.11g、802.11n 等が挙げられる。

【ら】

● 「ルートヒントファイル」とは、最初に名前解決を問い合わせる DNS コンテンツサーバ（以下「ルート DNS」という。）の情報をいう。ルートヒントファイルには、ルート DNS のサーバ名と IP アドレスの組が記載されており、ルート DNS の IP アドレスが変更された場合はルートヒントファイルも変更される。ルートヒントファイルは InterNIC（Internet Network Information Center）のサイトから入手可能である。

【A～Z】

● 「CRYPTREC（Cryptography Research and Evaluation Committees）」とは、電子政府推奨暗号の安全性を評価・監視し、暗号モジュール評価基準等の策定を検討するプロジェクトである。

● 「IPv6 移行機構」とは、物理的にひとつのネットワークにおいて、IPv4 技術を利用する通信と IPv6 を利用する通信の両方を共存させることを可能とする技術の総称である。例えば、電子計算機や通信回線装置が２つの通信プロトコルを併用するデュアルスタック機構や、相互接続性のない２つの IPv6 ネットワークを既設の IPv4 ネットワークを使って通信可能とする IPv6-IPv4 トンネル機構等がある。