重要性分類Ⅲ

社会保険診療報酬支払基金
情報セキュリティポリシー

令和７年６月１８日改定
支払基金最高情報セキュリティ責任者

目次

第 1 部 総則

1.1 本ポリシーの位置付け

1.1.1 基本方針

社会保険診療報酬支払基金（以下、「支払基金」という。）における情報セキュリティの基本は、支払基金で取り扱う情報の重要度に応じた「機密性」・「完全性」・「可用性」を確保することであり、支払基金が自らの責任において情報セキュリティ対策を講じていくことが原則である。

支払基金の業務は、個人の診療内容など個人情報を中心とする重要かつ膨大な情報を取り扱うものであり、医療保険制度の円滑な運営を支える機関として情報資産の適切な情報セキュリティ対策を実施することは、その社会的責務である。

この社会的責務を果たしていくため、支払基金は、支払基金の管理する情報資産に係る安全対策に必要な情報セキュリティを確保、維持し、医療保険制度の安定的かつ効率的な運営の実施並びに情報資産の適切な保護のための本情報セキュリティポリシーを策定し、支払基金が管理する情報資産をあらゆる脅威から守るために必要な情報セキュリティの確保とその継続的な強化・拡充に最大限取り組むものとする。

1.1.2 改定

情報セキュリティの水準を適切に維持していくためには、情報技術の進展や内外の環境の変化等の状況の変化を的確にとらえ、それに応じて情報セキュリティ対策の見直しを図ることが重要である。

本ポリシーの見直しは定期的に行い、必要に応じ規定内容の追加・修正等の改定を行うことによって、その適用性を将来にわたり維持するものとし、本ポリシーが改定された場合には、その内容を情報システムの実施手順書等に適切に反映させるものとする。

なお、本ポリシーは、支払基金における情報セキュリティ対策が国の行政機関等と同等の水準にあることを示す一つの基準とするために、サイバーセキュリティ基本法第 25 条第 1 項第 2 号に定める国の行政機関、独立行政法人及び指定法人におけるサイバーセキュリティに関する対策の基準である、「政府機関等のサイバーセキュリティ対策の運用等に関する指針」、「政府機関等のサイバーセキュリティ対策のための統一規範」、「政府機関等のサイバーセキュリティ対策のための統一基準」（以下「統一基準」という。）及び「政府機関等の対策基準策定のためのガイドライン」に準拠している。よって、これらが改定された場合には、その内容と本ポリシーとの乖離を明らかにし、適切に反映させるものとする。

1.1.3　本ポリシー及び情報システムの実施手順書等の遵守

本ポリシー及び情報セキュリティに関係する文書等及び情報システムの実施手順書等は、支払基金における情報セキュリティ確保のための対策であり、支払基金において情報及び情報システムを取り扱う者は、その実施に責任を負うとともに、これらを尊重し、遵守しなければならない。

1.1.4　法令等の遵守

情報及び情報システムの取扱いに関しては、法令及び基準等（以下「関連法令等」という。）においても規定されているため、情報セキュリティ対策を実施する際には、本ポリシーのほか関連法令等を遵守しなければならない。なお、これらの関連法令等は情報セキュリティ対策にかかわらず当然に遵守すべきものであるため、本ポリシーでは、あえて関連法令等の遵守について明記していない。また、情報セキュリティ対策に係る内容について定めた既存の政府決定等及び情報セキュリティを巡る状況に応じて策定される政府決定等についても同様に遵守するものとする。

1.2　使い方

1.2.1　本ポリシー及び情報システムの実施手順書等との関係

本ポリシーは、支払基金において、情報セキュリティの確保のために実施すべき対策及びその水準を更に高めるための対策の方針と基準を定めたものである。情報システムの実施手順書等については、本ポリシーで定めた以上の情報セキュリティ確保を目標として作成する必要がある。

1.2.2　適用対象

本ポリシーが適用される対象範囲を以下のように定める。

⑴　本ポリシーにおいて適応対象とする者は、全ての役職員等関係者とする。

⑵　本ポリシーにおいて適用範囲とする「情報」は、以下の情報とする。

(ｱ)　役職員等関係者が職務上使用することを目的として支払基金が調達し、又は開発した情報処理若しくは通信の用に供するシステム又は外部電磁的記録媒体に記録された情報（当該情報システムから出力された書面に記載された情報及び書面から情報システムに入力された情報を含む。）

(ｲ)　その他の情報システム又は外部電磁的記録媒体に記録された情報（当該情報システムから出力された書面に記載された情報及び書面から情報システムに入力された情報を含む。）であって、役職員等関係者が職務上取り扱う情報

(ｳ)　(ｱ)及び(ｲ)のほか、支払基金が調達し、又は開発した情報システムの設計又は運用管理に関する情報

(ｴ)　紙媒体（診療報酬請求書、診療報酬明細書、各種帳票、業務用文書等を言う。

以下同じ。）に記録されたデータ

1.2.3 全体構成

本ポリシーは、部、節及び款の 3 つの階層によって構成されている。

部の構成として、「情報セキュリティ対策の基本的枠組み」、「情報の取扱い」、「外部委託」、「情報システムのライフサイクル」、「情報システムの構成要素」、「情報システムのセキュリティ要件」、「情報システムの利用」にそれぞれ分類している。

さらにそれぞれの部において、内容に応じて節として対策項目に分け、その下に款として、遵守事項は、統一基準において求められている必ず実施すべき対策事項であり、基本対策事項は、遵守事項に対応した個別具体的な対策実施要件、対策の実施例や考え方を解説したもの（基本対策事項は規定していない場合もある）を定めている。具体的には以下のとおりである。

⑴ 「情報セキュリティ対策の基本的枠組み」では、基金全体として情報セキュリティ対策を実施する際の実施体制や点検・評価手順、違反や例外措置等、組織としての運用に関係する各役職員等関係者の権限と責務を明確にするために整備すべき事項を定めている。

⑵ 「情報の取扱い」では、情報の作成、利用・保存、提供・公表、運搬・送信、及び消去等といった情報のライフサイクルに着目し、各段階において各役職員等関係者が情報を保護するために業務の中で常に実施すべき事項、情報を取り扱う区域の管理と情報処理において制限すべき事項等を定めている。

⑶ 「外部委託」では、支払基金外の者に情報システムの開発等を委託する際に遵守する事項、約款による外部サービスの利用に際して遵守する事項、ソーシャルメディアサービスによる情報発信に際して遵守する事項、クラウドサービスの利用に係る外部委託に際して遵守する事項を定めている。

⑷ 「情報システムのライフサイクル」では、遵守事項が適切に実施されるように、情報システムの計画、構築、運用、移行、廃棄及び見直しといった情報システムのライフサイクルの各段階において実施すべき事項と、情報システムに係る情報セキュリティを確保するために整備すべき事項を定めている。

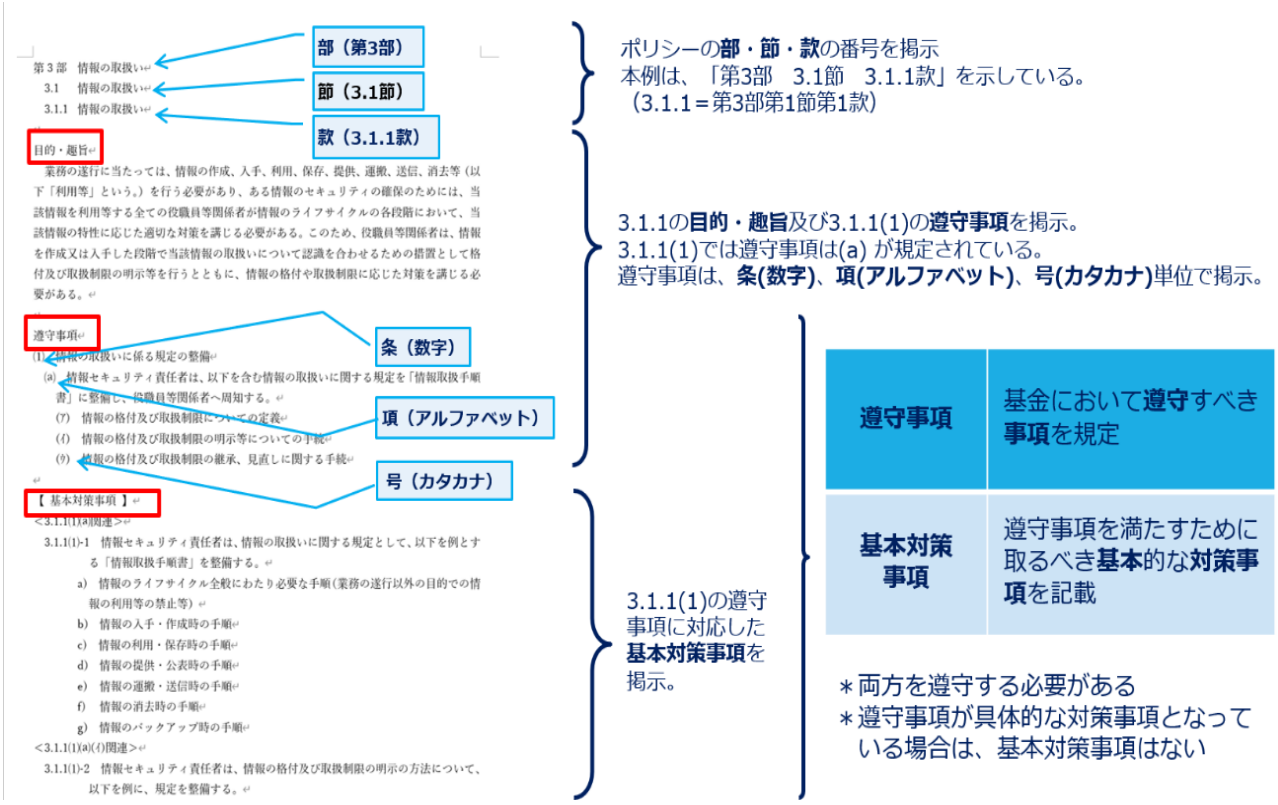
⑸ 「情報システムの構成要素」では、電子計算機及び通信回線等の個別の情報システムの特性及びライフサイクルの観点から、情報システムにおいて実施すべき事項を定めている。

⑹ 「情報システムのセキュリティ要件」では、情報システムにおいて、アクセス制御の観点等、導入すべきセキュリティ機能を示すとともに、不正プログラム及びサービス不能攻撃等の脅威を防ぐために、情報システムにおいて実施すべき事項を定めている。

⑺ 「情報システムの利用」では、情報セキュリティを確保するために必要な情報シ

ステムの利用に関する運用手順書の整備に関する事項、役職員等関係者が遵守するべき事項について定めている。

【参考】第 2 部以降の基本的な記述構成



1.2.4　対策項目の記載事項

本ポリシーは、支払基金として実施すべき情報セキュリティに関する対策基準について、対策項目ごとに遵守事項を示している。

支払基金においては、重要な情報資産及びこれらを取り扱う情報システムが多数あるのみならず、種類、規模、用途も多種多様なものとなっている。

本ポリシーの目的は、支払基金全体の情報セキュリティ水準を向上させることにあるため、本ポリシーで規定する各対策項目を全ての保護すべき情報とこれを取り扱う情報システムに適用することを前提としている。なお、本ポリシーは、統一基準に準拠し、「遵守事項」も含めた構成としているため、セキュリティ侵害が国民の皆様に影響を及ぼすような特に重要な情報を取り扱う情報システムについては、その事項の必要性について検討し、適切な対策を講じる必要がある。

一方、直ちに実装が難しい事項については、本ポリシーの記載事項を保護する対象のセキュリティ要件ととらえ、対策の実施よりも対策を実施することを検討し、情報システムの更新時又は導入時点で、情報システムのセキュリティを向上させるため

に、本ポリシーの対策項目を実装し、より高い情報セキュリティを確保すべきである。

1.3　情報の格付の区分・取扱制限

1.3.1　情報の格付の区分

取り扱う情報について、機密性、完全性及び可用性の３つの観点から区別し、それぞれにつき格付の区分の定義を以下に示す。なお、支払基金以外の組織等へ情報を提供する場合は、支払基金の対策基準における格付区分について、適切に伝達する。

機密性についての格付の定義（機密性２情報（重要性分類Ⅱ）及び機密性３情報（重要性分類Ⅰ）を「要機密情報」という。機密性についての格付を定義する場合、次の重要性分類に従って分類する。）

・重要性分類

Ⅰ　業務上必要とする最小限の者のみが扱う情報

Ⅱ　公開することを予定していない情報

Ⅲ　外部に公開できる情報のうち業務上重要な情報

Ⅳ　上記以外の情報

格付の区分	分類の基準
機密性３情報（重要性分類Ⅰ）	業務で取り扱う情報のうち、業務上必要とする最小限の者のみが扱う情報
機密性２情報（重要性分類Ⅱ）	業務で取り扱う情報のうち、公開することを予定していない情報
機密性１情報（重要性分類Ⅲ）	外部に公開できる情報のうち、業務上重要な情報
機密性０情報（重要性分類Ⅳ）	公表済みの情報、公表しても差し支えない情報等、機密性１情報（重要性分類Ⅲ）、機密性２情報（重要性分類Ⅱ）又は機密性３情報（重要性分類Ⅰ）以外の情報

完全性についての格付の定義（完全性２情報を「要保全情報」という。）

格付の区分	分類の基準
完全性２情報	業務で取り扱う情報（書面を除く。）のうち、改ざん、誤びゅう又は破損により、業務の適切な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報
完全性１情報	完全性２情報以外の情報（書面を除く。）

可用性についての格付の定義（可用性２情報を「要安定情報」という。）

格付の区分	分類の基準
可用性２情報	業務で取り扱う情報（書面を除く。）のうち、その滅失、紛失又は当該情報が利用不可能であることにより、業務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報
可用性１情報	可用性２情報以外の情報（書面を除く。）

また、その情報が要機密情報、要保全情報及び要安定情報に一つでも該当する場合は「要保護情報」という。

1.3.2　情報の取扱制限

「取扱制限」とは、情報の取扱いに関する制限であって、複製禁止、持出禁止、配布禁止、暗号化必須、読後廃棄その他の情報の適正な取扱いを役職員等関係者に確実に行わせるための手段をいう。

役職員等関係者は、格付に応じた情報の取扱いを適切に行う必要があるが、その際に、格付に応じた具体的な取扱い方を示す方法として取扱制限を用い、情報の格付けのみでは、取扱制限ができない場合は、取扱制限を記載する。

取扱制限の種類の基本的な定義については、「情報取扱手順書」に示すが、これら以外の取扱制限の種類についても適宜定めることができるものとする。

1.4　用語定義

【あ】

- 「アクセス制御」とは、情報又は情報システムへのアクセスを許可する主体を制限することをいう。
- 「アプリケーション」とは、OS 上で動作し、サービスの提供、文書作成又は電子メールの送受信等の特定の目的のために動作するソフトウェアをいう。
- 「アプリケーション・コンテンツ」とは、支払基金が開発し提供するアプリケーションプログラム、ウェブコンテンツ等の総称をいう。
- 「アプリケーション・コンテンツの提供時に基金外の情報セキュリティ水準の低下を招く行為の防止に関する手順書」とは、支払基金がアプリケーション・コンテンツを提供するときに支払基金外の情報セキュリティ水準の低下を招く行為を防止するための運用手順をいう。
- 「アルゴリズム」とは、ある特定の目的を達成するための演算手順をいう。
- 「暗号化」とは、第三者が復元することができないよう、定められた演算を施しデータを変換することをいう。

● 「暗号化消去」とは、情報を電磁的記録媒体に暗号化して記録しておき、情報の抹消が必要になった際に情報の復号に用いる鍵を抹消することで情報の復号を不可能にし、情報を利用不能にする論理的削除方法をいう。暗号化消去に用いられる暗号化機能の例としては、ソフトウェアによる暗号化（Windows の BitLocker 等）、ハードウェアによる暗号化（自己暗号化ドライブ（Self-Encrypting Drive）等）などがある。
● 「ウェブクライアント」とは、ウェブページを閲覧するためのアプリケーション（いわゆるブラウザ）及び付加的な機能を追加するためのアプリケーションをいう。
● 「運用手順書」とは、対策基準に定められた対策内容を個別の業務等において運用するため、あらかじめ定める必要のある具体的な手順や基準をいう。

【か】
● 書込 CD とは、データ授受用端末（Fat クライアント）から事務処理用端末（ノート PC（Surface））にデータを取り込む場合に使用する支払基金が支給する CD-R（Compact Disc Recordable）を指す。
● 「可用性」とは、情報へのアクセスを認められた者が、必要時に中断することなく、情報にアクセスできる特性をいう。
● 「完全性」とは、情報が破壊、改ざん又は消去されていない特性をいう。
● 「機器等」とは、情報システムの構成要素（サーバ装置、端末、通信回線装置、複合機、特定用途機器等、ソフトウェア等）、外部電磁的記録媒体等の総称をいう。（参考：図 1.4.-1）
● 「機密性」とは、情報に関して、アクセスを認められた者だけがこれにアクセスできる特性をいう。
● 「業務委託」とは、支払基金の業務の一部又は全部について、契約をもって外部の者に実施させることをいう。「委任」「準委任」「請負」といった契約形態を問わず、全て含むものとする。ただし、当該業務において支払基金の情報を取り扱わせる場合に限る。
● 「記録媒体」とは、情報が記録され、又は記載される有体物をいう。記録媒体において、文字、図形等人の知覚によって認識することができる情報が記載された紙その他の有体物を「書面」といい、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る記録であって、情報システムによる情報処理の用に供されるものを「電磁的記録」といい、電磁的記録に係る記録媒体を「電磁的記録媒体」という。また、電磁的記録媒体には、サーバ装置、端末、通信回線装置等に内蔵される内蔵電磁的記録媒体と、CD-R、外付けハードディスクドライブ、DVD-R 等（USB メモリ除く。）の外部電磁的記録媒体がある。
● 「共通利用型システム」とは、他の機関等含め共通的に利用することを目的として、一つの機関等が管理・運用する情報システムであって、他の機関等が整備する情報システムに対し、同情報システムと連携して、情報システムのセキュリティ機能を提供する情報シ

ステム及び他の機関等に機器等を提供し、他の機関等の職員等が利用する情報システムをいう。なお、共通利用型システムを構築・運用する機関等を「共通利用型システム管理機関」といい、共通利用型システムが提供するセキュリティ機能を利用して情報システムを構築・運用する機関等及び共通利用型システムが提供する機器等を利用する機関等を「共通利用型システム利用機関」という。

- 「緊急時対応計画」とは、情報セキュリティに係る緊急事態が発生した際又はその可能性を認知した際の迅速な対応を可能とするための手順をいう。
- 「クラウドサービス」とは、事業者によって定義されたインタフェースを用いた、拡張性、柔軟性を持つ共用可能な物理的又は仮想的なリソースにネットワーク経由でアクセスするモデルを通じて提供され、利用者によって自由にリソースの設定・管理が可能なサービスであって、情報セキュリティに関する十分な条件設定の余地があるものをいう。クラウドサービスの例としては、SaaS（Software as a Service）、PaaS（Platform as a Service）、IaaS（Infrastructure as a Service）等がある。なお、本ポリシーにおけるクラウドサービスは、支払基金以外の一般の者が一般向けに情報システムの一部又は全部の機能を提供するクラウドサービスであって、当該サービスにおいて支払基金の情報が取り扱われる場合に限るものとする。
- 「クラウドサービス管理者」とは、クラウドサービスの利用における利用申請の許可権限者から利用承認時に指名された当該クラウドサービスに係る管理を行う支払基金の職員等をいう。
- 「クラウドサービス提供者」とは、クラウドサービスを提供する事業者（クラウドサービスプロバイダ）をいう。
- 「クラウドサービス利用者」とは、クラウドサービスを利用する機関等の職員等又は業務委託した委託先においてクラウドサービスを利用する場合の委託先の従業員をいう。
- 「権限管理」とは、主体認証に係る情報（識別コード及び主体認証情報を含む。）及びアクセス制御における許可情報を管理することをいう。

【さ】

- 「サービス不能攻撃」とは、悪意ある第三者等が、ソフトウェアの脆弱性を悪用しサーバ装置又は通信回線装置のソフトウェアを動作不能にさせることや、サーバ装置、通信回線装置又は通信回線の容量を上回る大量のアクセスを行い通常の利用者のサービス利用を妨害する攻撃をいう。
- 「サーバ装置」とは、情報システムの構成要素である機器のうち、通信回線等を経由して接続してきた端末等に対して、自らが保持しているサービスを提供するもの（搭載されるソフトウェア及び直接接続され一体として扱われるキーボードやマウス等の周辺機器を含む。）をいい、特に断りがない限り、支払基金が調達又は開発するもの（共通利用型システムが提供するものを含む。）をいう。

- 「識別」とは、情報システムにアクセスする主体を、当該情報システムにおいて特定することをいう。
- 「識別コード」とは、主体を識別するために、情報システムが認識するコード（符号）をいう。代表的な識別コードとして、ユーザ ID が挙げられる
- 「事業継続計画」とは、支払基金において策定する社会保険診療報酬支払基金事業継続計画（ＢＣＰ：Business Continuity Plan）をいう。
- 「CSIRT(シーサート)」とは、支払基金において発生した情報セキュリティインシデントに対処するため、支払基金に設置された体制をいう。Computer Security Incident Response Team の略。
- 「実施手順」とは、本ポリシーに定められた対策内容を個別の情報システムや業務において実施するため、あらかじめ定める必要のある具体的な手順をいう。
- 「支払基金情報セキュリティポリシー」とは、支払基金が策定する情報セキュリティポリシーであり、情報セキュリティ対策の基本的な方針及び全ての情報資産に共通する情報セキュリティ対策の基準をいう（本ポリシーのことである。）。
- 「支払基金支給以外の情報システム」とは、支払基金が支給する情報システム以外の情報システムをいう。いわゆる私物の PC のほか、厚生労働省への出向者に対して支払基金が提供する情報システムも含むものとする。
- 「支払基金支給以外の情報システムによる情報処理」とは、支払基金が支給する情報システム以外の情報システムを用いて業務の遂行のための情報処理を行うことをいう。なお、直接装置等を用いる場合だけではなく、それら装置等によって提供されているサービスを利用する場合も含むものとする。ここでいうサービスとは、個人が契約している電子メールサービス等のことを指し、例えば支払基金の業務に要する電子メールを、個人で契約している電子メールサービスに転送して業務を行ったり、個人のメールから業務のメールを発信したりすることである。
- 「重要な設計書」とは、情報システムに関する設計書のうち、当該情報システムの適切な管理に必要なものであり、その紛失、漏えい等により、業務の遂行に支障を及ぼすものをいう。情報の格付では、要機密情報に相当する。
- 「主体」とは、情報システムにアクセスする者又は他の情報システムにアクセスするサーバ装置、端末等をいう。
- 「主体認証」とは、識別コードを提示した主体が、その識別コードを付与された主体、すなわち正当な主体であるか否かを検証することをいう。識別コードとともに正しい方法で主体認証情報が提示された場合に主体認証ができたものとして、情報システムはそれらを提示した主体を正当な主体として認識する。
- 「主体認証情報」とは、主体認証をするために、主体が情報システムに提示する情報をいう。代表的な主体認証情報として、パスワード等がある。
- 「主体認証情報格納装置」とは、主体認証情報を格納した装置であり、正当な主体に所

有又は保持させる装置をいう。所有による主体認証では、これを所有していることで、情報システムはその主体を正当な主体として認識する。代表的な主体認証情報格納装置として、IC カード等がある。

- 「支払基金内通信回線」とは、通信回線のうち、支払基金外通信回線以外のものをいう。
- 「支払基金外通信回線」とは、物理的な通信回線を構成する回線（有線又は無線、現実又は仮想及び支払基金管理又は他組織管理）及び通信回線装置を問わず、支払基金が管理していない電子計算機が接続され、当該電子計算機間の通信に利用する論理的な通信回線をいう。
- 「情報」とは、本ポリシーの「1.2.2 適用対象」の⑵に定めるものをいう（参考：図 1.4.-2)。
- 「情報資産」とは、情報（電子データ並びに電子媒体（フラッシュメモリ、フレキシブルディスク、光磁気ディスクその他これらに類する媒体をいう。以下同じ。）及び紙媒体（診療報酬請求書、診療報酬明細書、各種帳票、業務用文書等をいう。以下同じ。）に記録されたデータ)、情報システム及び情報システム開発・運用・保守のために必要な資料等。
- 「情報システム」とは、ハードウェア及びソフトウェアから成るシステムであって、情報処理又は通信の用に供するものをいい、特に断りのない限り、支払基金が調達又は開発するもの（管理を外部委託しているシステムや共通利用型システムを含む。）をいう（参考：図 1.4.-1)。
- 「情報セキュリティインシデント」とは、JIS Q 27000:2019 における情報セキュリティインシデントをいい、支払基金が保有する情報及びこれらを取り扱う情報システムの運用や情報セキュリティに影響を与える又は脅かす等の事故や事件（例：メール誤送信や電磁的記録媒体・書面の紛失・盗難等による情報漏えい、サービス不能攻撃等による情報システムの停止、ホームページ改ざん、マルウェア感染、不正アクセス）の発生や予告等をいう。

参考：JIS Q 27000:2019（抄）
・情報セキュリティインシデント
　望まない単独若しくは一連の情報セキュリティ事象、又は予期しない単独若しくは一連の情報セキュリティ事象であって、事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いもの。
・情報セキュリティ事象
　情報セキュリティ方針への違反若しくは管理策の不具合の可能性、又はセキュリティに関係し得る未知の状況を示す、システム、サービス又はネットワークの状態に関連する事象。

- 「情報セキュリティ関係規程」とは、本ポリシー及び本ポリシーに定められた内容を具

体的に実施するための実施手順書等をいう。

- 「情報セキュリティ対策推進体制」とは、支払基金の情報セキュリティ対策の推進に係る事務を遂行するため、支払基金に設置された体制をいう。
- 「情報取扱手順書」とは、情報の格付及び取扱制限についての定義、 情報の格付及び取扱制限の明示等についての手続及び情報の格付及び取扱制限の継承、見直しに関する手続等に関する運用手順をいう。
- 「情報の抹消」とは、電磁的記録媒体に記録された全ての情報を利用不能かつ復元が困難な状態にすることをいう。情報の抹消には、情報自体を消去することのほか、暗号技術検討会及び関連委員会（CRYPTREC）によって安全性が確認された暗号アルゴリズムを用いた暗号化消去や、情報を記録している記録媒体を物理的に破壊すること等も含まれる。削除の取消しや復元ツールで復元できる状態は、復元が困難な状態とはいえず、情報の抹消には該当しない。
- 「人事異動等の際に行うべき情報セキュリティ対策に関する手順書」とは、雇用の開始、終了及び人事異動時等に関する管理の運用手順をいう。
- 「セキュリティパッチ」とは、発見された情報セキュリティ上の問題を解決するために提供される修正用のファイルをいう。提供元によって、更新プログラム、パッチ、ホットフィクス、サービスパック等名称が異なる。
- 「ソーシャルメディア」とは、インターネット上において、ブログ、ソーシャルネットワーキングサービス、動画共有サイト等の、利用者が情報を発信し、形成していくものをいう。
- 「ソフトウェア」とは、サーバ装置、端末、通信回線装置等を動作させる手順及び命令を、当該サーバ装置等が理解できる形式で記述したものをいう。innta や OS 上で動作するアプリケーションを含む広義の意味である。

【た】

- 「対策基準」とは、支払基金における情報及び情報システムの情報セキュリティを確保するための情報セキュリティ対策の基準であり、本ポリシーのことである。
- 「対策推進計画」とは、情報セキュリティ対策を組織的・継続的に実施し、総合的に推進するための計画をいう。
- 「耐タンパ性」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。
- 「端末」とは、情報システムの構成要素である機器のうち、役職員等関係者が情報処理を行うために直接操作するもの（搭載されるソフトウェア及び直接接続され一体として扱われるキーボードやマウス等の周辺機器を含む。）をいい、特に断りがない限り、支払基金が調達又は開発するもの（共通利用型システムが提供するものを含む。）をいう。端末には、モバイル端末も含まれる。特に断りを入れた例としては、支払基金が調達又は開

発するもの以外を指す「支払基金支給以外の端末」がある。

- 「通信回線」とは、複数の情報システム又は機器等（支払基金が調達等を行うもの以外のものを含む。）の間で所定の方式に従って情報を送受信するための仕組みをいい、特に断りのない限り、支払基金の情報システムにおいて利用される通信回線を総称したものをいう。通信回線には、支払基金が直接管理していないものも含まれ、その種類（有線又は無線、物理回線又は仮想回線等）は問わない。
- 「通信回線装置」とは、通信回線間又は通信回線と情報システムの接続のために設置され、回線上を送受信される情報の制御等を行うための装置をいう。通信回線装置には、いわゆるハブやスイッチ、ルータ等のほか、ファイアウォール等も含まれる。また、物理的なハードウェアを有する通信回線装置を「物理的な通信回線装置」という。
- 「テレワーク」とは、情報通信技術（ICT＝Information and Communication Technology）を活用した、場所や時間を有効に活用できる柔軟な働き方のことをいう。テレワークの形態は、業務を行う場所に応じて、自宅で業務を行う在宅勤務、主たる勤務官署以外に設けられた執務環境で業務を行うサテライトオフィス勤務、モバイル端末等を活用して移動中や出先で業務を行うモバイル勤務に分類される。支払基金においては、役職員等関係者が自身の居宅（審査委員については勤務先医療機関）において業務を行うことをいう。
- 「特定用途機器」とは、テレビ会議システム、IP 電話システム、ネットワークカメラシステム、入退管理システム、施設管理システム、環境モニタリングシステム等の特定の用途に使用される情報システム特有の構成要素であって、通信回線に接続する機能を備えてている、又は内蔵電磁的記録媒体を備えているものをいう。
- 「電子署名」とは、情報の正当性を保証するための電子的な署名情報をいう。
- 「電子政府推奨暗号リスト」とは、CRYPTREC 暗号リストにおいて、安全性及び実装性能が確認された暗号技術について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリストをいう。
- 「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。
- 「電子メールサーバ」とは、電子メールの送受信、振り分け、配送等を行うアプリケーション及び当該アプリケーションを動作させるサーバ装置をいう。
- 「ドメインネームシステム（DNS)」とは、クライアント等からの問合せを受けて、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システムである。
- 「ドメイン名」とは、国、組織、サービス等の単位で割り当てられたネットワーク上の名前であり、英数字及び一部の記号を用いて表したものをいう。例えば、www.ssk.or.jp というウェブサイトの場合は、ssk.or.jp の部分がこれに該当する。

【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。

【は】

● 「複合機」とは、プリンタ、ファクシミリ、イメージスキャナ、コピー機等の機能が一つにまとめられている機器をいう。

● 「不正プログラム」とは、コンピュータウイルス、ワーム（他のプログラムに寄生せず単体で自己増殖するプログラム）、スパイウェア（プログラムの使用者の意図に反して様々な情報を収集するプログラム）等の、情報システムを利用する者が意図しない結果を当該情報システムにもたらすプログラムの総称をいう。

● 「不正プログラム定義ファイル」とは、不正プログラム対策ソフトウェアが不正プログラムを判別するために利用するデータをいう。

● 「踏み台」とは、悪意ある第三者等によって不正アクセスや迷惑メール配信の中継地点に利用されている情報システムのことをいう。

【ま】

● 「抹消」→「情報の抹消」を参照。

● 「明示等」とは、情報を取り扱う全ての者が当該情報の格付について共通の認識となるようにする措置をいう。明示等には、情報ごとに格付を記載することによる明示のほか、当該情報の格付に係る認識が共通となるその他の措置も含まれる。その他の措置の例としては、特定の情報システムに記録される情報について、その格付を情報システムの規程等に明記するとともに、当該情報システムを利用する全ての者に周知すること等が挙げられる。

● 「無線 LAN」とは、IEEE802.11a、802.11b、802.11g、802.11n、802.11ac、802.11ad 等の規格により、無線通信で情報を送受信する通信回線をいう。

● 「モバイル端末」とは、端末のうち、業務上の必要に応じて移動させて使用することを目的としたものをいい、端末の形態は問わない。

　令和 2 年 8 月 28 日付け本総厚総 009792「コミュニケーションサービスの導入について（通知）」に基づき、支払基金が職員等に貸与したノート PC 及び令和 4 年 5 月 13 日付け本シ基ネ 000032「在宅審査に使用するノート PC の配布について」等に基づき、支払基金が職員等に貸与した医療事務電算システム用ノート PC を指す。

● 「モバイル端末(要管理対策区域外における使用）及び支払基金支給以外の端末の使用に係る手順書」とは、要管理対策区域外にモバイル端末を持ち出して情報処理を行う場合及び支払基金支給以外の端末により情報処理を行う場合の安全管理措置及び手順をいう。

【や】

● 「役職員等関係者」とは、支払基金のすべての役職員等（審査調整役、役員、職員（非常勤嘱託、定年後再雇用者及び継続雇用職員を含む。）及び常任顧問）、審査委員、臨時職

員、派遣職員、委託業者（請負業者及び派遣業者を含む。）その他期間を定めて雇用している者をいう。

- 「要安定情報」とは、可用性 2 情報をいう。
- 「要管理対策区域」とは、支払基金が管理する施設等支払基金の管理下にある区域であって、取り扱う情報を保護するために、施設及び環境に係る対策が必要な区域をいう。
- 「要機密情報」とは、機密性 2 情報（重要性分類Ⅱ）及び機密性 3 情報（重要性分類Ⅰ）をいう。
- 「要保護情報」とは、要機密情報、要保全情報及び要安定情報をいう。
- 「要保全情報」とは、完全性 2 情報をいう。

【ら】

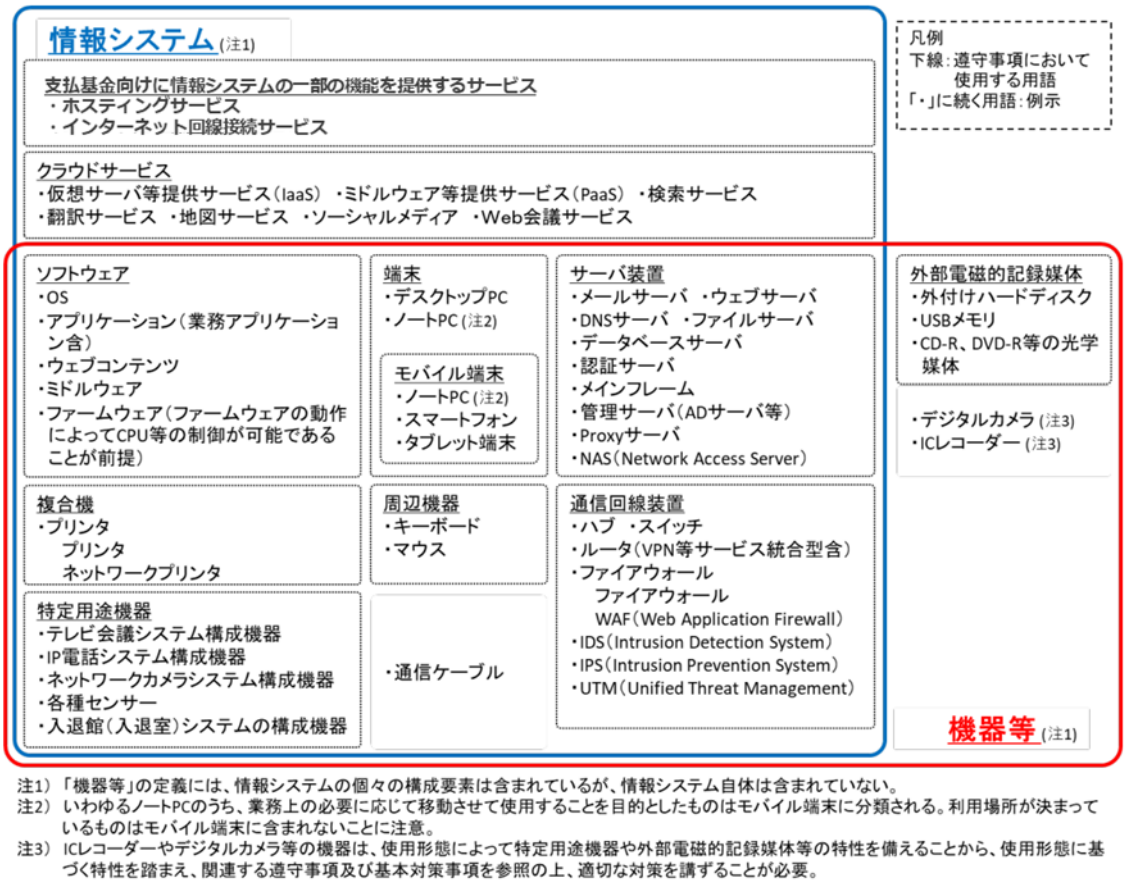
- 「リスク」とは、目的に対する不確かさの影響をいう。ある事象（周辺状況の変化を含む。）の結果とその発生の起こりやすさとの組合せとして表現されることが多い。
- 「ルートヒントファイル」とは、最初に名前解決を問い合わせる DNS コンテンツサーバ（以下「ルート DNS」という。）の情報をいう。ルートヒントファイルには、ルート DNS のサーバ名と IP アドレスの組が記載されており、ルート DNS の IP アドレスが変更された場合はルートヒントファイルも変更される。ルートヒントファイルは InterNIC（Internet Network Information Center）のサイトから入手可能である。
- 「例外措置手順書」とは、情報セキュリティ関係規程の適用が業務の適正な遂行を著しく妨げるなどの理由により、規定された対策の内容と異なる代替の方法を採用すること又は規定された対策を実施しないことを認めざるを得ない場合における対処手順をいう。

【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、暗号技術の適切な実装法・運用法を調査・検討するプロジェクトである。
- 「DNS サーバ」とは、名前解決のサービスを提供するアプリケーション及びそのアプリケーションを動作させるサーバ装置をいう。DNS サーバは、その機能によって、自らが管理するドメイン名等についての名前解決を提供する「コンテンツサーバ」とクライアントからの要求に応じて名前解決を代行する「キャッシュサーバ」の 2 種類に分けることができる。
- 「DNSSEC トラストアンカー」とは、DNSSEC 検証を行う際の、信頼の連鎖の起点情報をいう。
- 「IoT（Internet of Things）機器」とは、従来インターネットに接続していなかったが、インターネットに接続する機能を備えるようになった機器をいう。
- 「MAC アドレス（Media Access Control address）」とは、機器等が備える有線 LAN や

無線 LAN のネットワークインタフェースに割り当てられる固有の認識番号である。識別番号は、各ハードウェアベンダを示す番号と、ハードウェアベンダが独自に割り当てる番号の組合せによって表される。

- 「S/MIME（Secure Multipurpose Internet Mail Extensions）」とは、公開鍵暗号を用いた、電子メールの暗号化と電子署名付与の一方式をいう。
- 「VPN（Virtual Private Network）」とは、暗号技術等を利用し、インターネット等の公衆回線を仮想的な専用回線として利用するための技術をいう。
- 「Web 会議サービス」とは、専用のアプリケーションやウェブブラウザを利用し、映像又は音声を用いて会議参加者が対面せずに会議を行えるクラウドサービスをいう。なお、特定用途機器同士で通信を行うもの（テレビ会議システム等）は含まれない。



注1) 「機器等」の定義には、情報システムの個々の構成要素は含まれているが、情報システム自体は含まれていない。
注2) いわゆるノートPCのうち、業務上の必要に応じて移動させて使用することを目的としたものはモバイル端末に分類される。利用場所が決まっているものはモバイル端末に含まれないことに注意。
注3) ICレコーダーやデジタルカメラ等の機器は、使用形態によって特定用途機器や外部電磁的記録媒体等の特性を備えることから、使用形態に基づく特性を踏まえ、関連する遵守事項及び基本対策事項を参照の上、適切な対策を講ずることが必要。

図 1.4-1　「情報システム」、「機器等」及びその関係

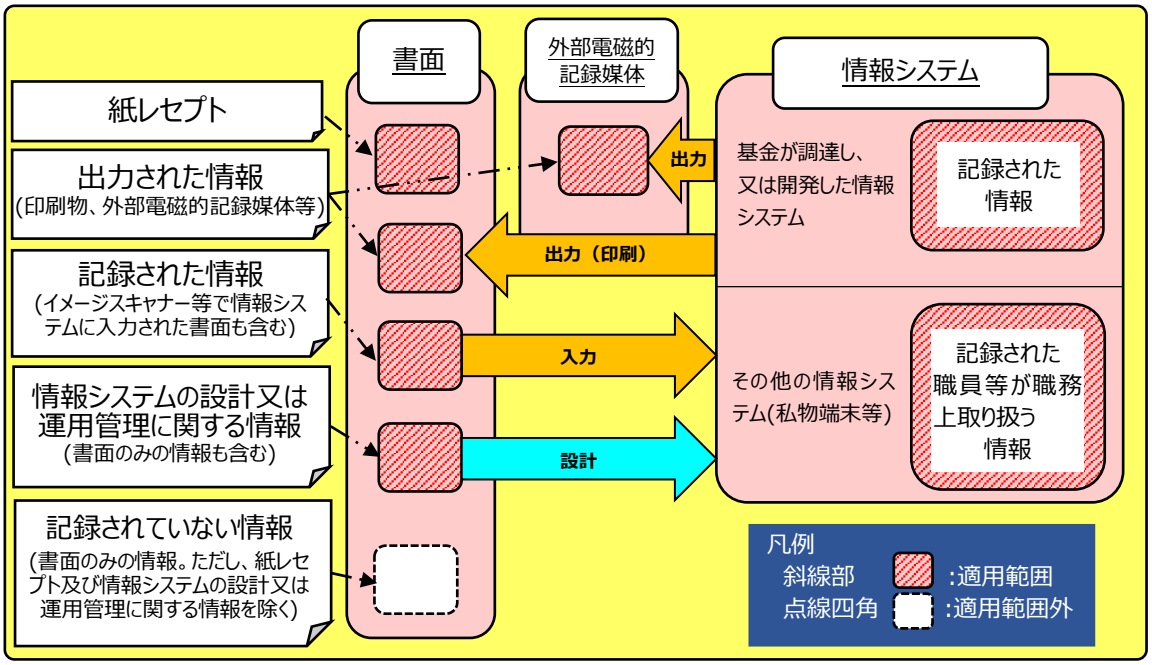


図 1.4-2　本ポリシーにおいて適用対象とする「情報」の範囲

第 2 部 情報セキュリティ対策の基本的枠組み

2.1 導入・計画

2.1.1 組織・体制の整備

目的・趣旨

情報セキュリティ対策は、それに係る全ての役職員等関係者が、職制及び職務に応じて与えられている権限と責務を理解した上で、負うべき責務を全うすることで実現される。そのため、それらの権限と責務を明確にし、必要となる組織・体制を整備する必要がある。特に最高情報セキュリティ責任者は、情報セキュリティ対策を着実に進めるために、自らが組織内を統括し、基金全体として計画的に対策が実施されるよう推進しなければならない。

なお、最高情報セキュリティ責任者は、本ポリシーに定められた自らの職務を、最高情報セキュリティ副責任者その他の本ポリシーに定める各責任者に担わせることができる。

遵守事項

⑴ 最高情報セキュリティ責任者及び最高情報セキュリティ副責任者等の設置

(a) 最高情報セキュリティ責任者

本ポリシーに基づき情報セキュリティ委員会を統括し、支払基金におけるすべての情報セキュリティに関する最終的な権限と責任を有する最高情報セキュリティ責任者１人を置く。最高情報セキュリティ責任者は、理事長とする。

(b) 最高情報セキュリティ副責任者

最高情報セキュリティ責任者は、最高情報セキュリティ副責任者１人を置く。最高情報セキュリティ副責任者は、専務理事とする。

(c) 情報セキュリティ責任者（審査支払等担当）

最高情報セキュリティ責任者は、審査支払等業務に関する情報セキュリティに係る事務を統括する情報セキュリティ責任者（審査支払等担当）を置く。情報セキュリティ責任者（審査支払等担当）は、システム部を所管する役員とする。

(d) 情報セキュリティ責任者（データヘルス担当）

最高情報セキュリティ責任者は、データヘルス業務に関する情報セキュリティに係る事務を統括する情報セキュリティ責任者（データヘルス担当）を置く。情報セキュリティ責任者（データヘルス担当）は、データヘルス業務を所掌する役員とする。

(e) 情報セキュリティ責任者（インシデント担当）

最高情報セキュリティ責任者は、情報セキュリティについて専門的な知識及び経験を有する情報セキュリティ責任者（インシデント担当）を置く。

【 基本対策事項 】

＜2.1.1(1)(a)関連＞

2.1.1(1)-1　最高情報セキュリティ責任者は、次に掲げる事務を統括する。

a)　情報セキュリティ対策推進のための組織・体制の整備

b)　本ポリシーの決定、見直し

c)　情報セキュリティ対策を総合的に推進するための計画(以下「対策推進計画」という。）の決定、見直し

d)　情報セキュリティインシデントに対処するために必要な指示その他の措置

e)　情報セキュリティ監査の結果を踏まえた改善計画の策定等の必要な措置の指示

f)　前各号に掲げるもののほか、情報セキュリティに関する重要事項

＜2.1.1(1)(b)関連＞

2.1.1(1)-2　最高情報セキュリティ副責任者は、次の事務を担う。

a)　最高情報セキュリティ責任者を補佐して支払基金における情報セキュリティに関する事務を整理し、最高情報セキュリティ責任者の指示を受けて支払基金の情報セキュリティに関する事務を統括する。

b)　最高情報セキュリティ責任者が不在の場合又は最高情報セキュリティ責任者の指示を受けた場合、その職務の全部又は一部を代理する。

＜2.1.1(1)(c)関連＞

2.1.1(1)-3　情報セキュリティ責任者（審査支払等担当）は、次の事務を担う。

a)　最高情報セキュリティ責任者及び最高情報セキュリティ副責任者を補佐し、最高情報セキュリティ責任者及び最高情報セキュリティ副責任者が不在の場合又は最高情報セキュリティ責任者及び最高情報セキュリティ副責任者の指示を受けた場合、審査支払等について、その職務の全部又は一部を代理する。

b)　審査支払等を担当する情報セキュリティ管理者を統括する。

c)　要管理対策区域における施設及び環境に係る対策の決定

d)　情報セキュリティ対策に関する実施手順の整備及び見直し並びに実施手順に関する事項

e)　情報セキュリティ対策に係る教育実施計画の策定及び当該実施体制の整備

f)　例外措置の適用審査記録の台帳整備等

g)　情報セキュリティインシデントに対処するための緊急連絡窓口の整備等

h)　前各号に掲げるもののほか、情報セキュリティ対策に係る事務

＜2.1.1(1)(d)関連＞

2.1.1(1)-4　情報セキュリティ責任者（データヘルス担当）は、次の事項を担う。

a)　最高情報セキュリティ責任者及び最高情報セキュリティ副責任者を補佐し、最高情報セキュリティ責任者及び最高情報セキュリティ副責任者が不在の場

合又は最高情報セキュリティ責任者及び最高情報セキュリティ副責任者の指示を受けた場合、データヘルス関係について、その職務の全部又は一部を代理する。

b) データヘルス関係の情報セキュリティ管理者を統括する。

c) データヘルス関係業務を行う要管理対策区域における施設及び環境に係る対策

d) データヘルス関係業務に係る情報セキュリティ対策に関する実施手順の整備及び見直し並びに実施手順に関する事項

e) データヘルス関係業務に係る教育実施計画の策定及び当該実施体制

f) データヘルス関係業務に係る情報セキュリティインシデントに対処するための緊急連絡窓口の整備等

g) 前各号に掲げるもののほか、データヘルス関係業務に係る情報セキュリティ対策に関する事項

＜2.1.1⑴(e)関連＞

2.1.1⑴-5 情報セキュリティ責任者（インシデント担当）は、次の事項を担う。

a) 情報セキュリティ責任者（インシデント担当）は、情報セキュリティインシデント発生時における実務対応を行い、専門的知見の提供、対応作業の実施支援・助言を行うとともに、情報セキュリティ関係規程に係る課題及び問題点を含む運用状況を適時に把握し、支払基金全体の情報セキュリティ対策の推進等について、最高情報セキュリティ責任者、最高情報セキュリティ副責任者、インシデント発生部署を所管する理事長特任補佐、システム運用推進役又は執行役（以下「インシデント発生担当理事長特任補佐等」という。）への助言を行う。

遵守事項

⑵ 情報セキュリティ委員会の設置

⑻ 最高情報セキュリティ責任者は、本ポリシー等の審議を行う機能を持つ組織として、情報セキュリティ委員会を設置し、委員長として委員会の議事を統括する。情報セキュリティ委員会の構成員、審議事項等は、情報セキュリティ委員会規程で定めるとおりとする。

【 基本対策事項 】

＜2.1.1⑵(a)関連＞

2.1.1⑵-1 情報セキュリティ委員会は、情報セキュリティに関する維持管理を推進するため、次に掲げる事項を審議する。

a) 本ポリシー

b） 対策推進計画
c） 前各号に掲げるもののほか、情報セキュリティに関し必要な事項

遵守事項
⑶ 情報セキュリティ監査責任者の設置
⒜ 最高情報セキュリティ責任者は、その指示に基づき実施する監査に関する事務を統括する者として、情報セキュリティ監査責任者１人を置く。情報セキュリティ監査責任者は、システム部長とする。

【 基本対策事項 】
＜2.1.1⑶⒜関連＞
2.1.1⑶-1 情報セキュリティ監査責任者は、次の事務を統括する。
a） 監査実施計画の策定
b） 監査実施体制の整備
c） 監査の実施指示及び監査結果の最高情報セキュリティ責任者への報告
d） 前各号に掲げるもののほか、情報セキュリティの監査に関する事項

遵守事項
⑷ 情報セキュリティ管理者等の設置
⒜ 情報セキュリティ管理者
情報セキュリティ管理者は、本部においては、部長及び室長とし、審査事務センター（以下「センター」という。）においては、センター長とし、審査事務センター分室（以下「分室」という。）においては、分室長とし、審査委員会事務局（以下「事務局」という。）においては、事務局長とする。
⒝ 情報セキュリティ管理補助者
情報セキュリティ管理補助者は、本部においては、次長、課長又は課長代理とし、センターにおいては、副センター長、室長又は課長とし、分室及び事務局においては、課長とする。
⒞ 情報セキュリティ管理担当者
情報セキュリティ管理担当者は、課長、課長代理又は係長のうち情報セキュリティ対策（所管する情報システムのセキュリティを含む。）に精通した者とする。

【 基本対策事項 】
＜2.1.1⑷⒜関連＞
2.1.1⑷-1 情報セキュリティ管理者は、情報セキュリティ対策を推進するため、次の事務を担う。

a)　所管する単位（本部の部、センター及び事務局）情報セキュリティ対策及び各担当が所管する情報システムにおける情報セキュリティ対策に関する事務の統括

b)　定められた区域の情報セキュリティ管理補助者の設置

c)　課の情報セキュリティ管理担当者の設置

d)　情報セキュリティインシデント発生時の適切な助言又は指示、原因調査、再発防止策等の実施

e)　情報セキュリティに係る自己点検計画の策定及び実施手順の整備

f)　所管する情報システムの情報セキュリティ対策に関する実施手順の整備

g)　所管するサーバ等の情報システムの設定が本ポリシーを遵守しているかどうかについて、また、問題が発生していないかについての定期的な確認

h)　前各号に掲げるもののほか、情報セキュリティ対策に関する事務（情報システムのセキュリティを含む。）

＜2.1.1(4)(b)関連＞

2.1.1(4)-2　本部における情報セキュリティ管理補助者は、自身の所属する部の本ポリシーの遵守状況、セキュリティ侵害、事故に関する情報を収集し、情報セキュリティ管理者に報告する。

2.1.1(4)-3　センター、分室及び事務局における情報セキュリティ管理補助者は、地方組織の本ポリシーの遵守状況、セキュリティ侵害、事故に関する情報を収集し、情報セキュリティ管理者に報告する。

2.1.1(4)-4　情報セキュリティ管理補助者は、定められた区域における施設及び環境に係る情報セキュリティ対策に関する事務を統括する。

2.1.1(4)-5　情報セキュリティ管理補助者は、情報セキュリティ対策（所管する情報システムのセキュリティを含む。）に関する職務について、情報セキュリティ管理者を補佐し、情報セキュリティ管理者が不在の場合又は情報セキュリティ管理者の指示を受けた場合、その職務の全部又は一部を代理する。

＜2.1.1(4)(c)関連＞

2.1.1(4)-6　情報セキュリティ管理担当者は、担当課における情報セキュリティ対策及び各担当が所管する情報システムに対する情報セキュリティ対策に関する事務を統括する。

遵守事項

(5)　最高情報セキュリティアドバイザーの設置

(a)　最高情報セキュリティ責任者は、情報セキュリティについて専門的な知識及び経験を有する者を最高情報セキュリティアドバイザー及び最高情報セキュリティアドバイザーを補佐する情報セキュリティアドバイザーを置き、自らへの助言を含む最高情報

セキュリティアドバイザーの業務内容を以下のとおり定める。

最高情報セキュリティアドバイザーは、情報セキュリティ責任者（インシデント担当）と兼務する。

(ｱ) 支払基金全体の情報セキュリティ対策の推進に係る最高情報セキュリティ責任者及び最高情報セキュリティ副責任者への助言

(ｲ) 情報セキュリティ関係規程の整備に係る助言、支援

(ｳ) 対策推進計画等、情報セキュリティ施策に係る各種計画の策定・実施に係る助言、支援

(ｴ) 教育実施計画の立案に係る助言並びに教材開発及び教育実施の支援

(ｵ) 情報システムに係る技術的事項に係る助言

(ｶ) 情報システムの設計・開発を外部委託により行う場合に調達仕様に含めて提示する情報セキュリティに係る要求仕様の策定に係る助言

(ｷ) 役職員等関係者に対する日常的な相談対応

(ｸ) 情報セキュリティインシデントへの対処の支援

(ｹ) 情報システムの分類に応じた情報セキュリティ対策に係る助言

(ｺ) 前各号に掲げるもののほか、情報セキュリティ対策全般に対する助言、支援

遵守事項

⑹ 情報セキュリティ対策推進体制の整備

ⓐ 最高情報セキュリティ責任者は、情報セキュリティ対策推進担当部署を本部の情報セキュリティを担当する課（以下、「セキュリティ担当課」という。）と定めるとともに、その役割を以下のとおり定める。

(ｱ) 情報セキュリティ関係規程及び対策推進計画の策定に係る事務

(ｲ) 情報セキュリティ関係規程の運用に係る事務

(ｳ) 例外措置に係る事務

(ｴ) 情報セキュリティ対策の教育の実施に係る事務

(ｵ) 情報セキュリティ対策の自己点検に係る事務

(ｶ) 情報セキュリティ関係規程及び対策推進計画の見直しに係る事務

(ｷ) 情報セキュリティインシデントに対する外部専門機関等からの情報収集及び他の機関への情報共有

(ｸ) 支払基金における情報セキュリティインシデントに関する情報の集約

ⓑ 最高情報セキュリティ責任者は、セキュリティ担当課の責任者を定める。セキュリティ担当課の責任者はセキュリティ担当課の課長とする。

遵守事項

⑺　兼務を禁止する役割

ⓐ　役職員等関係者は、情報セキュリティ対策の運用において、以下の役割を兼務しない。

(ｱ)　承認又は許可（以下本条において「承認等」という。）の申請者と当該承認等を行う許可権限者

(ｲ)　監査を受ける者とその監査を実施する者

ⓑ　役職員等関係者は、承認等を申請する場合において、自らが許可権限者であるときその他許可権限者が承認等の可否の判断をすることが不適切と認められるときは、当該許可権限者の上司又は次の表に定めた者に承認等を申請し、承認等を得る。

承認等を申請する者	許可権限者
情報セキュリティ管理者	情報セキュリティ管理補助者
情報セキュリティ管理担当者	情報セキュリティ管理者又は 情報セキュリティ管理補助者
書込 CD 管理者	書込 CD 管理者補助者

2.1.2　資産管理

目的・趣旨

支払基金が所管する情報システムの情報セキュリティ水準を維持するとともに、情報セキュリティインシデントに適切かつ迅速に対処するためには、支払基金が所管する情報システムの情報セキュリティ対策に係る情報を情報システム台帳で一元的に把握するとともに、情報システムの構成要素に関する調達仕様書や設定情報等が速やかに確認できるように、日頃から文書として整備しておき、その所在を把握しておくことが重要である。

遵守事項

⑴　情報システム台帳の整備

ⓐ　情報セキュリティ責任者（審査支払等担当又はデータヘルス担当）（以下、「情報セキュリティ責任者」という。）は、全ての情報システムのセキュリティ要件について、当該情報システムのセキュリティ要件に係る事項については、情報システム台帳に整備する。

ⓑ　情報セキュリティ管理者は、情報システムを新規に構築し、又は更改する際には、当該情報システム台帳のセキュリティ要件に係る内容を記録又は記載し、当該内容について情報セキュリティ責任者に報告する。

【 基本対策事項 】

＜2.1.2(1)(a)関連＞

2.1.2(1)-1　情報セキュリティ責任者は、以下の内容を全て含む台帳を整備する。

a)　情報システム名

b)　担当部及び課

c)　当該情報セキュリティ管理者、情報セキュリティ管理補助者及び情報セキュリティ管理担当者の氏名及び連絡先

d)　システム構成

e)　接続する支払基金外通信回線の種別

f)　取り扱う情報の格付及び取扱制限に関する事項

g)　当該情報システムの設計・開発、運用・保守に関する事項

h)　情報システムの利用目的

i)　情報システムの分類基準に基づいて実施した情報システムの分類結果

j)　連携する情報システム及び連携内容

また、民間事業者等が提供するクラウドサービス等を利用して情報システムを構築する場合は、前述の a)～j)に加え、以下を全て含む内容についても台帳として整備する。

k)　契約クラウドサービス等の名称

l)　クラウドサービス等の提供者の名称

m)　利用期間

n)　クラウドサービス等の概要

o)　ドメイン名

p)　クラウドサービス等で取り扱う情報の格付及び取扱制限に関する事項

q)　情報の暗号化に用いる鍵の管理主体（支払基金管理かクラウドサービス等の提供者管理か）

r)　クラウドサービス等で取り扱う情報が保存される国・地域

s)　サービスレベル

2.1.3　情報セキュリティ関係規程の整備

目的・趣旨

支払基金の情報セキュリティ水準を適切に維持し、情報セキュリティリスクを総合的に低減させるためには、支払基金として遵守すべき対策の基準を定めるとともに、情報セキュリティに係るリスク評価の結果等を踏まえた上で定めるとともに、計画的に対策を実施することが重要である。

また、対策基準に定められた対策を実施するためには具体的な運用手順書や実施手順を

定める必要があるが、それらが整備されていない、又は内容に漏れがあると、対策が適切に実施されないおそれがあることから、その場合には、最高情報セキュリティ責任者は、情報セキュリティ責任者に運用手順書等の整備を指示し、その結果について定期的に報告を受け、状況を適確に把握することが重要である。

遵守事項

⑴　リスク評価の実施

⒜　最高情報セキュリティ責任者は、支払基金の目的等を踏まえ、自己点検及び情報セキュリティ監査の結果等を勘案した上で、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを評価する。

遵守事項

⑵　対策基準の策定

⒜　最高情報セキュリティ責任者は、情報セキュリティ委員会における審議を経て、統一基準に準拠し、これと同等以上の情報セキュリティ対策が可能となるように対策基準である本ポリシーを定める。また、対策基準は、支払基金の業務、取り扱う情報及び保有する情報システムに関するリスク評価の結果を踏まえた上で定める。

遵守事項

⑶　運用手順書及び実施手順の策定

⒜　情報セキュリティ責任者は、支払基金における情報セキュリティ対策に関する運用手順書（本ポリシーで最高情報セキュリティ責任者が整備すべきとされている場合を除く。）及び実施手順（本ポリシーで整備すべき者を別に定める場合を除く。）を整備し、運用手順書及び実施手順に関する事務を統括し、整備状況について最高情報セキュリティ責任者に報告する。

⒝　情報セキュリティ責任者は、情報セキュリティ対策における雇用の開始、終了及び人事異動時等に関する管理の運用手順を「人事異動等の際に行うべき情報セキュリティ対策に関する手順書」に整備する。

⒞　役職員等関係者は、雇用の開始、終了及び人事異動に当たり、「人事異動等の際に行うべき情報セキュリティ対策に関する手順書」を確認する。

遵守事項

⑷　対策推進計画の策定

⒜　最高情報セキュリティ責任者は、情報セキュリティ委員会における審議を経て、情報セキュリティ対策を総合的に推進するための対策推進計画を定める。また、対策推進計画には、支払基金の業務、取り扱う情報及び保有する情報システムに関するリスク評価

の結果を踏まえた全体方針並びに以下に掲げる取組の方針・重点及びその実施時期を含める。

(ｱ) 情報セキュリティに関する教育

(ｲ) 情報セキュリティ対策の自己点検

(ｳ) 情報セキュリティ監査及び過年度の情報セキュリティ監査結果を踏まえた取組

(ｴ) 情報システムに関する技術的な対策を推進するための取組

(ｵ) 前各号に掲げるもののほか、情報セキュリティ対策に関する重要な取組

2.2 運用

2.2.1 情報セキュリティ関係規程の運用

目的・趣旨

支払基金は、本ポリシーに定められた対策を実施するために定める具体的な運用規程及び実施手順を適切に運用する必要がある。

情報セキュリティ関係規程の運用において、当該規程に係る課題及び問題点を含む運用状況を適時に把握することが重要である。

遵守事項

(1) 情報セキュリティ対策の運用

(a) 情報セキュリティ対策推進部署は、最高情報セキュリティ責任者が規定した役割に応じて必要な事務を遂行する。

(b) 情報セキュリティ管理担当者は、役職員等関係者より情報セキュリティ関係規程に係る課題及び問題点の報告を受けた場合は、情報セキュリティ管理者に報告する。情報セキュリティ管理者は、課題及び問題点を含む運用状況を適時に把握し、必要に応じて情報セキュリティ責任者にその内容を報告する。

(c) 情報セキュリティ責任者は、情報セキュリティ関係規程に係る課題及び問題点を含む運用状況を適時に把握し、必要に応じて最高情報セキュリティ責任者にその内容を報告する。

遵守事項

(2) 違反への対処

(a) 役職員等関係者は、情報セキュリティ関係規程への重大な違反を知った場合は、情報セキュリティ管理担当者にその旨を報告する。

(b) 情報セキュリティ管理担当者は、本ポリシーの遵守状況、セキュリティ侵害、事故、情報セキュリティ関係規程への重大な違反に関して、役職員等関係者から報告を受けた場合及び自らがセキュリティ侵害等を知った場合は、速やかに情報セキュリティ管

理者を通じて、最高情報セキュリティ責任者へ報告し、情報セキュリティ管理者の指示により、適切に対処する。

(c) 情報セキュリティ管理者は、情報セキュリティ関係規程への重大な違反の報告を受けた場合及び自らが重大な違反を知った場合には、最高情報セキュリティ責任者及び情報セキュリティ責任者にその旨を報告し、違反者及び必要な者に情報セキュリティの維持に必要な措置を講じさせる。

(d) 本ポリシー及び情報セキュリティ関係規程に違反する行為を行った役職員等及び審査委員は、別に定める罰則の対象となる場合がある。

2.2.2 例外措置

目的・趣旨

例外措置はあくまで例外であって、濫用があってはならない。しかしながら、情報セキュリティ関係規程の適用が業務の適正な遂行を著しく妨げるなどの理由により、規定された対策の内容と異なる代替の方法を採用すること又は規定された対策を実施しないことを認めざるを得ない場合がある。このような場合に対処するために、例外措置の手続を定めておく必要がある。

遵守事項

(1) 例外措置手続の整備

(a) 最高情報セキュリティ責任者は、例外措置の適用の申請を審査し、許可する者（以下本款において「許可権限者」という。）を定め、審査手続を「例外措置手順書」に整備する。なお、許可権限者はシステム部長とする。

(b) 許可権限者は、例外措置の適用審査記録の台帳を整備する。

(c) 情報セキュリティ責任者は、許可権限者に対して、定期的に申請状況の報告を求める。

(d) 役職員等関係者は、例外措置の適用の申請に当たり、「例外措置手順書」を確認する。

【 基本対策事項 】

＜2.2.2(1)(a)関連＞

2.2.2(1)-1 最高情報セキュリティ責任者は、例外措置について以下を全て含む手順を「例外措置手順書」に定める。

a) 例外措置の許可権限者

b) 事前申請の原則その他の申請方法

c) 審査項目その他の審査方法

・申請者の情報（氏名、所属、連絡先）

・例外措置の適用を申請する情報セキュリティ関係規程の該当箇所（規程名と条

項等）

・例外措置の適用を申請する期間

・例外措置の適用を申請する措置内容（講じる代替手段等）

・例外措置により生じる情報セキュリティ上の影響と対処方法

・例外措置の適用を終了した旨の報告方法

・例外措置の適用を申請する理由

＜2.2.2(1)(b)関連＞

2.2.2(1)-2　許可権限者は、例外措置の適用審査記録に以下の内容を記載し、適用審査記録の台帳として保管するとともに、情報セキュリティ責任者へ定期的に報告する。

a)　審査した者の情報（氏名、役割名、所属、連絡先）

b)　申請内容

・申請者の情報（氏名、所属、連絡先）

・例外措置の適用を申請する情報セキュリティ関係規程の該当箇所（規程名と条項等）

・例外措置の適用を申請する期間

・例外措置の適用を申請する措置内容（講じる代替手段等）

・例外措置の適用を終了した旨の報告方法

・例外措置の適用を申請する理由

c)　審査結果の内容

・許可又は不許可の別

・許可又は不許可の理由

・例外措置の適用を許可した情報セキュリティ関係規程の該当箇所（規程名と条項等）

・例外措置の適用を許可した期間

・許可した措置内容（講じるべき代替手段等）

・例外措置を終了した旨の報告方法

遵守事項

(2)　例外措置の運用

(a)　役職員等関係者は、定められた審査手続に従い、許可権限者に規定の例外措置の適用を申請する。ただし、業務の遂行に緊急を要し、当該規定の趣旨を十分尊重した扱いを取ることができる場合であって、情報セキュリティ関係規程の規定とは異なる代替の方法を直ちに採用すること又は規定されている方法を実施しないことが不可避のときは、事後速やかに届け出る。

(b)　許可権限者は、役職員等関係者による例外措置の適用の申請を、定められた審査手続

に従って審査し、許可の可否を決定する。

(c) 許可権限者は、例外措置の申請状況を情報セキュリティ責任者及び情報セキュリティ委員会へ定期的に報告する。

(d) 情報セキュリティ責任者は、例外措置の申請状況を踏まえた情報セキュリティ関係規程の追加又は見直しの検討を行い、最高情報セキュリティ責任者に報告する。

2.2.3 教育

目的・趣旨

情報セキュリティ関係規程が適切に整備されているとしても、その内容が役職員等関係者に認知されていなければ、当該規定が遵守されないことになり、情報セキュリティ水準の向上を望むことはできない。このため、全ての役職員等関係者が、情報セキュリティの教育を通じ、情報セキュリティ関係規程への理解を深められるよう、適切に教育を実施することが必要である。

また、近年の情報セキュリティインシデントの増加等に鑑み、情報セキュリティの専門性を有する人材を育成することも求められる。

遵守事項

(1) 教育体制の整備・教育実施計画の策定

(a) 情報セキュリティ責任者は、情報セキュリティ対策に係る教育について、対策推進計画に基づき教育実施計画を策定し、その実施体制を整備する。

(b) 情報セキュリティ責任者は、情報セキュリティの状況の変化に応じ役職員等関係者に対して新たに教育すべき事項が明らかになった場合は、教育実施計画を見直す。

【 基本対策事項 】

＜2.2.3(1)(a)関連＞

2.2.3(1)-1 情報セキュリティ責任者は、役職員等関係者の役割に応じて教育すべき内容を検討し、教育のための資料を整備する。

2.2.3(1)-2 情報セキュリティ責任者は、役職員等関係者が毎年度最低 1 回は教育を受講できるように、教育実施計画を立案するとともに、その実施体制を整備する。

2.2.3(1)-3 情報セキュリティ責任者は、役職員等関係者の着任又は異動後に、3 か月以内に受講できるように、その実施体制を整備する。

遵守事項

(2) 教育の実施

(a) 情報セキュリティ管理担当者は、教育実施計画に基づき、役職員等関係者に対して、

情報セキュリティ関係規程に係る教育を適切に受講させる。

(b) 役職員等関係者は、教育実施計画に従って、適切な時期に教育を受講する。

(c) 情報セキュリティ責任者は、情報セキュリティ対策推進担当課及び CSIRT に属する者に教育を適切に受講させる。

(d) 情報セキュリティ管理担当者は、教育の実施状況を記録し、情報セキュリティ管理補助者及び情報セキュリティ管理者に報告する。

(e) 情報セキュリティ責任者は、教育の実施状況を分析、評価し、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に対して、役職員等関係者の情報セキュリティ教育の実施状況について報告する。

(f) 情報セキュリティ管理担当者は、情報セキュリティ教育についての受講状況や役職員等関係者の理解度を確認し、必要に応じて役職員等関係者を指導する。

(g) 情報セキュリティ管理者は、臨時職員、委託業者及び派遣職員に対し、雇用及び契約時に必ず本ポリシーのうち、臨時職員、委託業者及び派遣職員が守るべき内容を理解させ、実施及び遵守させる。なお、雇用及び契約に当たっては、本ポリシーを遵守する旨の同意書を必要とする。

2.2.4 情報セキュリティインシデントへ対処のための事前準備及び体制整備

目的・趣旨

情報セキュリティインシデント又はその可能性を認知した場合には、最高情報セキュリティ責任者に早急にその状況を報告するとともに、被害の拡大を防ぎ、回復のための対策を講じる必要がある。そのためには、連絡経路を整備し、セキュリティインシデント発生時に適切に動けるよう訓練し、対応手順を備えることが重要である。

遵守事項

(1) 緊急時対応計画の策定

(a) 情報セキュリティ責任者は、情報セキュリティに係る緊急事態が発生した際又はその可能性を認知した際の迅速な対応を可能とするため、「緊急時対応計画」を定める。

(b) 「緊急時対応計画」では、情報セキュリティインシデントの定義、緊急事態への対応及び対応の組織体制等について定める。

【 基本対策事項 】

＜2.2.4(1)(a)関連＞

2.2.4(1)-1 役職員等関係者は、情報セキュリティインシデント発生に備え、「緊急時対応計画」に定められた手順を事前に確認する。

遵守事項

⑵　情報セキュリティインシデント対応に関する最高情報セキュリティ責任者の役割

⑷　最高情報セキュリティ責任者は、外部の専門家等による必要な支援を速やかに得られる体制を構築する。

⑹　最高情報セキュリティ責任者は、情報セキュリティインシデントが発生した際、直ちに自らへの報告が行われる体制を整備する。

【 基本対策事項 】

＜2.2.4⑵⑷関連＞

2.2.4⑵-1　最高情報セキュリティ責任者は、情報セキュリティインシデント発生が発生した場合、必要に応じ、情報セキュリティ責任者（インシデント担当）又は厚生労働省等に随時支援を求める。

＜2.2.4⑵⑹関連＞

2.2.4⑵-1　最高情報セキュリティ責任者は、情報セキュリティインシデントが発生した際の報告経路を整備することについて指示する。

遵守事項

⑶　情報セキュリティインシデント対応に関する情報セキュリティ管理者の役割

⑷　情報セキュリティ責任者（インシデント担当）は、情報セキュリティインシデント発生時の対処手順のうち、意思決定の判断基準や決定権者、判断に応じた対応内容、緊急時の意思決定方法等を事前に確認する。

⑹　情報セキュリティ管理者は、情報セキュリティインシデントへの対処にかかる円滑な連絡・連携を図るため、平素より情報交換や訓練の必要性を検討し、情報セキュリティ上の脅威や技術動向も踏まえ、業務の遂行のため特に重要と認めた情報システムについて、その訓練の内容及び対応手順を整備する。

⑻　情報セキュリティ管理者は、情報セキュリティインシデントについて支払基金外の者から報告を受けるための窓口を整備し、その窓口への連絡手段を支払基金外に明示する。

【 基本対策事項 】

＜2.2.4⑶⑷関連＞

2.2.4⑶-1　情報セキュリティ責任者（インシデント担当）は、情報セキュリティインシデントに備え、業務の遂行のため特に重要と認めた情報システムについて、緊急連絡先、連絡手段、連絡内容を含む緊急連絡網を整備する。＜2.2.4⑶⑹関連＞

2.2.4⑶-3　情報セキュリティ管理者は、対処手順が適切に機能することを訓練等により確認する。

遵守事項

⑷　CSIRT 体制の整備

ⓐ　最高情報セキュリティ責任者は、情報セキュリティインシデントに対応できるよう、インシデント発生担当理事長特任補佐等を CSIRT 責任者とする CSIRT 体制の整備を指示する。CSIRT 責任者は、情報セキュリティインシデント発生時、支払基金本部に CSIRT を立ち上げ、CSIRT 構成員を招集し、情報セキュリティインシデント対応を指示する。

【 基本対策事項 】

＜2.2.4⑷ⓐ関連＞

2.2.4⑷-1　情報セキュリティインシデントに対応する CSIRT 構成員は、次のとおりとする。

a)　インシデント発生担当理事長特任補佐等

b)　情報セキュリティ責任者（インシデント担当）

c)　セキュリティ担当課の課長（CSIRT 事務局責任者）

d)　情報セキュリティ管理者（インシデント発生担当部長）

e)　情報セキュリティ管理担当者（インシデント発生担当課長・課長代理・係長）

f)　セキュリティ担当課職員（CSIRT 事務局）

遵守事項

⑸　情報セキュリティインシデント対策本部の整備

ⓐ　最高情報セキュリティ責任者は、重大な情報セキュリティインシデントに該当すると判断した場合は、情報セキュリティインシデント対策本部を設置する。

【 基本対策事項 】

＜2.2.4⑸ⓐ関連＞

2.2.4⑸-1　最高情報セキュリティ責任者は、以下の事象に該当する場合、重大な情報セキュリティインシデントであると判断する。

a)　CSIRT が対応する事例のうち、情報システムの停止（障害含む。）による保険者又は医療機関等のほか、利用者に及ぶ影響（診療報酬支払の遅延、オンライン資格確認等の利用停止）が広範囲又は長時間（予測されるものを含む。）にわたる場合

b)　CSIRT が対応する事例のうち、サイバー攻撃、ウイルス感染又は情報システムの不正利用（要管理対策区域内への不正侵入等）による情報システム内に保有する情報資産が侵害（毀損、滅失、改ざん又は漏えい）された場合

c)　CSIRT が対応する事例のうち、重要性分類Ⅰの情報が情報流失した場合

【重要性分類Ⅰの情報】

・個人及び個別保険医療機関等が特定できる情報の含まれているもので、役職員等の間でも厳重な管理が必要なもの。(職員台帳等の個人情報、電子審査録、審査分担、レセプト等)

・オンライン資格確認等システムで管理する資格情報、診療情報、薬剤情報等

・医療保険者等向け中間サーバー等で管理する特定個人情報

2.2.4(5)-2　情報セキュリティインシデント対策本部の構成員は、次のとおりとする。

a)　最高情報セキュリティ副責任者（専務理事）

b)　情報セキュリティ責任者（審査支払等担当）

c)　情報セキュリティ責任者（データヘルス担当）（常勤理事）

d)　情報セキュリティ責任者（インシデント担当）

e)　理事長特任補佐、システム運用推進役及び執行役（インシデント発生担当）

f)　情報セキュリティ管理者（インシデント発生担当部長）

g)　関係部長（必要に応じて参画）

2.2.5　情報セキュリティインシデントへの対応等

目的・趣旨

情報セキュリティインシデントが発生した場合には、早急に対策を講じる必要がある。そのためには、CSIRT が情報セキュリティインシデントに適切に対応するとともに、被害が保険者及び医療機関等に及び、影響が大きい場合は、最高情報セキュリティ責任者が迅速に判断を下すことが重要である。

遵守事項

⑴　役職員等関係者の対応

(a)　役職員等関係者は、情報セキュリティインシデント又はその可能性を認知した場合には、「緊急時対応計画」に基づき、情報セキュリティ管理担当者にその旨を報告し、指示に従う。

遵守事項

⑵　最高情報セキュリティ責任者の対応

(a)　最高情報セキュリティ責任者は、本ポリシー及び緊急時対応計画に則り、インシデント発生担当理事長特任補佐等に情報セキュリティインシデントに対応するために必要な指示を行う。

遵守事項

⑶　CSIRT の対応

⑷　CSIRT 責任者は、報告された情報セキュリティインシデントの可能性について状況を確認し、サイバー攻撃又は情報漏えいによる情報セキュリティインシデントであるかの評価を行う。

⑸　CSIRT 責任者は、情報セキュリティインシデントに関係する情報セキュリティ管理者に対し、被害の拡大防止等を図るための応急措置の実施及び復旧に係る指示又は勧告を行う。また、CSIRT 責任者は、同様の情報セキュリティインシデントが別の情報システムにおいても発生している可能性を検討し、必要に応じて当該情報システムを所管する情報セキュリティ管理者へ確認を指示する。

⑹　CSIRT は、CSIRT 責任者の指示を受けて速やかに対処・復旧にあたる。

＜2.2.5⑶⑸関連＞

2.2.5⑶-1　CSIRT 責任者は、認知した情報セキュリティインシデントの種類や規模、影響度合い等を勘案し、情報セキュリティインシデント対処中にあっても、必要に応じて、CSIRT、情報セキュリティインシデントの当事者のいる部課、その他関連部において事前に定められた役割分担を随時見直す。

＜2.2.5⑹関連＞

2.2.5⑶-2　CSIRT 構成員の役割は次のとおりとする。

a)　インシデント発生担当理事長特任補佐等

・CSIRT 責任者として支払基金に関わる情報セキュリティインシデント発生時における対応の一元管理を行う。

・最高情報セキュリティ責任者への報告及び指示を仰ぐ。

・情報セキュリティ責任者（インシデント担当）からの報告により、情報セキュリティインシデント対象事例に該当するかの判断を行う。該当する場合は、CSIRT を招集する。

・情報セキュリティ責任者の事象解析・評価を参考にシステム停止又は運用再開の判断を行う。

b)　情報セキュリティ責任者（インシデント担当）

・情報セキュリティインシデントへの対処に係る専門的知見の提供、対応作業についてインシデント発生担当理事長特任補佐等に助言を行う。

c)　セキュリティ担当課の課長（CSIRT 事務局責任者）

・インシデント発生担当部の補佐（役員報告含む。）を行う。

・セキュリティ担当課職員への情報セキュリティインシデント対応の指示を行う。

・インシデント発生担当部との情報共有を行う。

・情報セキュリティ責任者（インシデント担当）の補佐及び状況報告を行う。
・厚生労働省保険局保険課への状況報告を行う。

d) 情報セキュリティ管理者（インシデント発生担当部長）
・インシデント発生担当理事長特任補佐等及び情報セキュリティ責任者（インシデント担当）の指示による担当部における情報セキュリティインシデント対応、ベンダへの指示事項等の実行責任者
・システム停止を伴う場合における業務代替措置の検討及び最高情報セキュリティ責任者、最高情報セキュリティ副責任者又はインシデント発生担当理事長特任補佐等への報告
・CSIRT への状況報告及び指示事項に対するベンダ及び担当課職員への指示

e) 情報セキュリティ管理担当者（インシデント発生担当課長・課長代理・係長）
・情報セキュリティインシデントの可能性の報告受付
・インシデント発生担当理事長特任補佐等及び情報セキュリティ責任者（インシデント担当）の指示の下における情報セキュリティインシデント対応
・インシデント発生担当理事長特任補佐等及び情報セキュリティ責任者（インシデント担当）の指示のベンダへの連絡
・情報セキュリティインシデントに関する対処の内容の記録

f) セキュリティ担当課職員（CSIRT 事務局）
・情報セキュリティインシデントの可能性の報告受付
・インシデント発生担当理事長特任補佐等及び情報セキュリティ責任者（インシデント担当）の指示の下における情報セキュリティインシデント対応
・CSIRT 事務局としての情報セキュリティ責任者（インシデント担当）との連絡担当
・情報セキュリティ責任者の指示事項に対するインシデント発生担当部との連携
・情報セキュリティインシデントに関する対処の内容の記録
・その他情報セキュリティインシデントに関する事項

遵守事項

⑷ 情報セキュリティインシデント対策本部の対応

⑷ (a) 情報セキュリティインシデント対策本部は、重大な情報セキュリティインシデントに対し、迅速に対応する。

⑷ (b) 最高情報セキュリティ責任者は、情報セキュリティインシデント対策本部が設置された際は、構成員を招集し、対応策等について指示を行う。

【 基本対策事項 】

＜2.2.5⑷(a)関連＞

2.2.5⑷-1　情報セキュリティインシデント対策本部は、情報セキュリティインシデントによる保険者又は医療機関等のほか、利用者への影響を低減するための対応を行う。

2.2.5⑷-2　情報セキュリティインシデント対策本部の構成員は、最高情報セキュリティ責任者が適切な判断を下すための情報を提供する。

2.2.5⑷-3　CSIRT に属する情報セキュリティインシデント対策本部の構成員は、CSIRT に対し指示を行い、CSIRT はその指示に従い、情報セキュリティインシデントに対応する。

遵守事項

⑸　情報セキュリティインシデントに係る情報共有等

(a)　CSIRT は、情報システムにおいて、情報セキュリティインシデントを認知した場合には、当該事象について速やかに、厚生労働省に連絡する。

(b)　CSIRT は、情報セキュリティインシデントに関して、関係者等に情報共有を行う。

(c)　情報セキュリティインシデントにより、個人情報・特定個人情報の漏えい等が発生した場合、最高情報セキュリティ責任者の指示に従い必要に応じて個人情報保護委員会へ報告を行う。

(d)　共通利用型システムの情報セキュリティ管理担当者は、認知した情報セキュリティインシデント又はその可能性が、共通利用型システムに関するものである場合には、情報セキュリティ関係規程に加えて、共通利用型システム等の情報セキュリティ対策に係る運用手順に従い、適切に対処する。

(e)　CSIRT 責任者は、情報セキュリティインシデントではないと評価した場合であっても、注意喚起等が必要と考えられるものについては、関係者等に情報共有を行う。

(f)　情報セキュリティ管理者は（インシデント発生担当部長）は、認知した情報セキュリティインシデントがサイバー攻撃又はそのおそれのあるものである場合には、最高情報セキュリティ責任者の指示により、警察への通報・連絡等を行う。

遵守事項

⑹　情報セキュリティインシデントの再発防止・教訓の共有

(a)　情報セキュリティ管理者は、情報セキュリティインシデント対処の結果を報告書として最高情報セキュリティ責任者及び情報セキュリティインシデント対策本部に報告する。

(b)　最高情報セキュリティ責任者は、情報セキュリティ管理者から情報セキュリティインシデントについての報告を受けた場合には、その内容を確認し、本ポリシー及び実施

手順の改善等再発防止策を実施するために必要な措置を指示する。

(c) CSIRT 責任者は、情報セキュリティインシデント対処の結果から得られた教訓及び再発防止策を、役職員等関係者に周知する。

(d) セキュリティ担当課は、発生した情報セキュリティインシデントのうち、CSIRT で対応した事案について、情報セキュリティ委員会規程に基づき、当該事案の概要報告を行う。

2.3 点検

2.3.1 情報セキュリティ対策の自己点検

目的・趣旨

情報セキュリティ対策の実効性を担保するためには、情報セキュリティ関係規程の遵守状況等を点検し、その結果を把握・分析することが必要である。

自己点検は、役職員等関係者が自らの役割に応じて実施すべき対策事項を実際に実施しているか否かを確認するだけではなく、基金全体の情報セキュリティ水準を確認する目的もあることから、適切に実施することが重要である。

また、自己点検の結果を踏まえ、各当事者は、それぞれの役割の責任範囲において、必要となる改善策を実施する必要がある。

遵守事項

(1) 自己点検計画の策定・手順の準備

(a) 情報セキュリティ責任者は、対策推進計画に基づき年度自己点検計画を策定し、最高情報セキュリティ責任者の承認を得る。

(b) 情報セキュリティ責任者は、年度自己点検計画に基づき、役職員等関係者ごとの自己点検票及び自己点検の実施手順を整備する。

(c) 情報セキュリティ責任者は、情報セキュリティの状況の変化に応じ、役職員等関係者に対して新たに点検すべき事項が明らかになった場合は、年度自己点検計画を見直す。

遵守事項

(2) 自己点検の実施

(a) 情報セキュリティ管理者は、年度自己点検計画に基づき、役職員等関係者に自己点検の実施を指示する。

(b) 役職員等関係者は、情報セキュリティ管理者から指示された自己点検票及び自己点検の手順を用いて自己点検を実施する。

遵守事項

⑶　自己点検結果の評価・改善

(a)　情報セキュリティ管理者は、自己点検結果について、自らが担当する組織のまとまりに特有の課題の有無を確認するなどの観点から自己点検結果を分析、評価する。また、評価結果を情報セキュリティ責任者に報告する。

(b)　情報セキュリティ責任者は、支払基金に共通の課題の有無を確認するなどの観点から自己点検結果を分析、評価する。また、評価結果を最高情報セキュリティ責任者に報告する。

(c)　最高情報セキュリティ責任者は、自己点検結果を全体として評価し、自己点検の結果により明らかになった問題点について、情報セキュリティ責任者及び情報セキュリティ管理者に改善を指示し、改善結果の報告を受ける。

2.3.2　情報セキュリティ監査

目的・趣旨

情報セキュリティ対策の実効性を担保するためには、情報セキュリティ対策を実施する者による自己点検だけでなく、独立性を有する者による情報セキュリティ対策の監査を実施することが必要である。支払基金において実施する情報セキュリティ監査は、業務や情報システムへの理解度が高く、効率的に監査の深掘りができ、組織の情報セキュリティ対策の改善に係るPDCAサイクルを円滑に機能させるためにも重要である。

また、監査の結果で明らかになった課題を踏まえ、最高情報セキュリティ責任者は、情報セキュリティ管理者に指示し、必要な対策を講じさせることが重要である。

遵守事項

⑴　監査実施計画の策定

(a)　情報セキュリティ監査責任者は、対策推進計画に基づき監査実施計画を策定する。

(b)　情報セキュリティ監査責任者は、情報セキュリティの状況の変化に応じ、対策推進計画で計画された以外の監査の実施が必要な場合には、追加の監査実施計画を定める。

【 基本対策事項 】

＜2.3.2⑴(a)関連＞

2.3.2⑴-1　情報セキュリティ監査責任者は、対策推進計画に基づき、以下を例とする監査実施計画を策定する。

a)　監査の目的（例：情報セキュリティ対策の実際の運用が情報セキュリティ関係規程に準拠していること等）

b)　監査の対象（例：監査の対象となる組織、情報システム、業務等）

c) 監査の方法（例：情報セキュリティ対策の運用状況を検証するため、査閲、点検、観察、ヒアリング等を行う。監査の基準は、本ポリシー及び実施手順とする。）

d) 監査の実施体制（例：監査実施者）

e) 監査の実施時期（例：対象ごとの実施時期）

2.3.2(1)-2 情報セキュリティ監査責任者は、組織内における監査遂行能力が不足等している場合には、支払基金外の者に監査の一部を請け負わせる。

遵守事項

(2) 監査の実施

(a) 情報セキュリティ監査責任者は、監査実施計画に基づき、監査の実施を情報セキュリティ監査人に指示し、結果を監査報告書として最高情報セキュリティ責任者に報告する。

【 基本対策事項 】

＜2.3.2(2)(a)関連＞

2.3.2(2)-1 情報セキュリティ監査責任者は、監査業務の実施において必要となる者を、被監査部門から独立した者又は専門的知識を有する支払基金外の者から選定し、情報セキュリティ監査人に指名する。

2.3.2(2)-2 情報セキュリティ監査責任者は、以下の事項を全て含む監査の実施を監査実施者に指示する。

a) 本ポリシーに統一基準を満たすための適切な事項が定められていること。

b) 運用手順書及び実施手順が整備されている場合、運用手順書及び実施手順が対策基準に準拠していること。

c) 被監査部門における実際の運用が情報セキュリティ関係規程に準拠していること。

遵守事項

(3) 監査結果に応じた対処

(a) 最高情報セキュリティ責任者は、監査報告書の内容を踏まえ、指摘事項に対する改善計画の策定等を情報セキュリティ責任者及び情報セキュリティ管理者に指示する。また、措置が完了していない改善計画は、定期的に進捗状況の報告を指示する。

(b) 情報セキュリティ責任者は、最高情報セキュリティ責任者からの改善の指示のうち、支払基金内で横断的に改善が必要な事項について、必要な措置を行った上で改善計画を策定し、措置結果及び改善計画を最高情報セキュリティ責任者に報告する。また、措置が完了していない改善計画は、定期的に進捗状況を最高情報セキュリティ責任者に報告する。

(c) 情報セキュリティ管理者は、最高情報セキュリティ責任者からの改善の指示のうち、自らが担当する組織のまとまりに特有な改善が必要な事項について、必要な措置を行った上で改善計画を策定し、措置結果及び改善計画を最高情報セキュリティ責任者に報告する。また、措置が完了していない改善計画は、定期的に進捗状況を最高情報セキュリティ責任者に報告する。

2.4 見直し

2.4.1 情報セキュリティ対策の見直し

目的・趣旨

情報セキュリティを取り巻く環境は常時変化しており、こうした変化に的確に対応しないと、情報セキュリティ水準を維持できなくなる。このため、支払基金の情報セキュリティ対策の根幹をなす情報セキュリティ関係規程は、実際の運用において生じた課題、自己点検・監査等の結果や情報セキュリティに係る重大な変化等を踏まえ、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び顕在時の損失等を分析し、リスクを評価し、適時見直しを行う必要がある。

また、情報セキュリティに係る取組をより一層推進するためには、上記のリスク評価の結果を本ポリシー及び対策推進計画に反映することも重要である。

遵守事項

(1) 情報セキュリティ対策の見直し

(a) 最高情報セキュリティ責任者は、リスク評価に変化が生じた場合には、情報セキュリティ委員会による審議を経て、対策基準や対策推進計画の必要な見直しを行う。

遵守事項

(2) 情報セキュリティ関係規程の見直し

(a) 最高情報セキュリティ責任者は、情報セキュリティの運用及び自己点検、情報セキュリティ監査等の結果等を総合的に評価するとともに、情報セキュリティに係る重大な変化等を踏まえ、情報セキュリティ委員会の審議を経て、本ポリシーについて必要な見直しを行う。

(b) 情報セキュリティ責任者は、情報セキュリティの運用及び自己点検、情報セキュリティ監査等の結果等を踏まえて情報セキュリティ対策に関する運用手順書及び実施手順を見直し、又は整備した者に対して規定の見直しを指示し、見直し結果について最高情報セキュリティ責任者に報告する。

(c) 情報セキュリティ責任者は、情報セキュリティの運用及び自己点検、情報セキュリティ等の結果等を踏まえて支払基金内で横断的に改善が必要となる情報セキュリティ

対策の運用見直しについて、支払基金内の職制及び職務に応じた措置の実施又は指示し、措置の結果について最高情報セキュリティ責任者に報告する。

遵守事項

⑶　対策推進計画の見直し

ⓐ　最高情報セキュリティ責任者は、情報セキュリティ対策の運用及び自己点検、情報セキュリティ監査等を総合的に評価するとともに、情報セキュリティに係る重大な変化等を踏まえ、情報セキュリティ委員会の審議を経て、対策推進計画について定期的な見直しを行う。

第 3 部 情報の取扱い

3.1　情報の取扱い

3.1.1　情報の取扱い

目的・趣旨

業務の遂行に当たっては、情報の作成、入手、利用、保存、提供、運搬、送信、消去等（以下「利用等」という。）を行う必要があり、ある情報のセキュリティの確保のためには、当該情報を利用等する全ての役職員等関係者が情報のライフサイクルの各段階において、当該情報の特性に応じた適切な対策を講じる必要がある。このため、役職員等関係者は、情報を作成又は入手した段階で当該情報の取扱いについて認識を合わせるための措置として格付及び取扱制限の明示等を行うとともに、情報の格付や取扱制限に応じた対策を講じる必要がある。

遵守事項

⑴　情報の取扱いに係る運用手順書の整備

⒜　情報セキュリティ責任者は、以下を全て含む情報の取扱いに関する運用手順を「情報取扱手順書」に整備する。

(ｱ)　情報の格付及び取扱制限についての定義

(ｲ)　情報の格付及び取扱制限の明示等についての手続

(ｳ)　情報の格付及び取扱制限の継承、見直しに関する手続

⒝　役職員等関係者は、支払基金の情報を取扱うに当たり、「情報取扱手順書」を確認する。

【 基本対策事項 】

＜3.1.1⑴⒜関連＞

3.1.1⑴-1　情報セキュリティ責任者は、情報の取扱いに関する運用手順として、以下を全て含む内容を「情報取扱手順書」に含めて整備する。

a)　情報のライフサイクル全般にわたり必要な手順（業務の遂行以外の目的での情報の利用等の禁止等）

b)　情報の入手・作成時の手順

c)　情報の利用・保存時の手順

d)　情報の提供・公表時の手順

e)　情報の運搬・送信時の手順

f)　情報の消去時の手順

g)　情報のバックアップ時の手順

＜3.1.1(1)(a)(ｲ)関連＞

3.1.1(1)-2　情報セキュリティ責任者は、情報の格付及び取扱制限の明示の方法について、以下を例とする内容を「情報取扱手順書」に含めて整備する。

a)　電磁的記録として取り扱われる情報に明示する場合

(ｱ)　電磁的記録の本体である文書ごとにヘッダ部分又は情報の内容へ直接記載

(ｲ)　電磁的ファイル等の取扱単位ごとにファイル名自体へ記載

(ｳ)　フォルダ単位等で取り扱う情報は、フォルダ名に記載

(ｴ)　電子メールで取り扱う情報は、電子メール本文又は電子メール件名に記載

b)　外部電磁的記録媒体に保存して取り扱う情報に明示する場合

(ｱ)　保存する電磁的ファイル又は文書等の単位ごとに記載

(ｲ)　外部電磁的記録媒体本体に記載

c)　書面に印刷されることが想定される場合

(ｱ)　書面のヘッダ部分等に記載

(ｲ)　冊子等の単位で取り扱う場合は、冊子の表紙、裏表紙等に記載

d)　既に書面として存在している情報に対して格付や取扱制限を明示する場合

(ｱ)　手書きによる記入

(ｲ)　スタンプ等による押印

3.1.1(1)-3　情報セキュリティ責任者は、情報の格付及び取扱制限の明示を省略する必要がある場合には、これらに係る認識が共通となるその他の措置の実施条件や実施方法について、「情報取扱手順書」に含めて整備する。

＜3.1.1(1)(a)(ｳ)関連＞

3.1.1(1)-4　情報セキュリティ責任者は、情報の加工時、複製時等における格付及び取扱制限の継承、見直しについて、以下を例とする内容を「情報取扱手順書」に含めて整備する。

a)　情報を作成する際に、参照した情報又は入手した情報の機密性に係る格付及び取扱制限を継承する。

b)　既存の情報に、より機密性の高い情報を追加するときは、格付及び取扱制限を見直す。

c)　機密性の高い情報から機密に該当する部分を削除したときは、残りの情報の機密性に応じて格付及び取扱制限を見直す。

d)　情報を複製する場合には、元となる情報の機密性に係る格付及び取扱制限を継承する。

e)　完全性及び可用性については、作成時又は複製時に適切な格付を決定する。

f)　他者が決定した情報の格付及び取扱制限を見直す必要がある場合には、その決定者（決定について引き継いだ者を含む。）又はその上司（以下「決定者等」という。）に確認を求める。

遵守事項

⑵　情報の目的外での利用等の禁止

ⓐ　役職員等関係者は、自らが担当している業務の遂行のために必要な範囲に限って、情報を利用等する。

遵守事項

⑶　情報の格付及び取扱制限の決定・明示等

ⓐ　役職員等関係者は、情報の作成時及び支払基金外の者が作成した情報を入手したことに伴う管理の開始時に、格付及び取扱制限の定義に基づき格付及び取扱制限を決定し、明示等する。

　なお、情報は、当該情報の作成を行った課の情報セキュリティ管理担当者が管理責任を有する。ただし、別途、特別の定めがある場合はこの限りでない。

ⓑ　役職員等関係者は、情報を作成又は複製する際に、参照した情報又は入手した情報に既に格付及び取扱制限の決定がなされている場合には、元となる情報の機密性に係る格付及び取扱制限を継承する。

ⓒ　役職員等関係者は、修正、追加、削除その他の理由により、情報の格付及び取扱制限を見直す必要があると考える場合には、情報の格付及び取扱制限の決定者等に確認し、その結果に基づき見直す。

遵守事項

⑷　情報の利用・保存

ⓐ　役職員等関係者は、利用する情報に明示等された格付及び取扱制限に従い、当該情報を適切に取り扱う。

ⓑ　役職員等関係者は、要機密情報について要管理対策区域外で情報処理を行う場合は、情報セキュリティ管理担当者の許可を得る。

ⓒ　役職員等関係者は、要保護情報について要管理対策区域外で情報処理を行う場合は、必要な安全管理措置を講じる。

ⓓ　役職員等関係者は、保存する情報にアクセス制限を設定するなど、情報の格付及び取扱制限に従って情報を適切に管理する。

ⓔ　役職員等関係者は、CD-R 等の外部電磁的記録媒体を用いて情報を取り扱う際、定められた利用手順に従う。

ⓕ　役職員等関係者は、要機密情報について、インターネットに接続されている環境に保存しない等によりリスクが最小限となるよう取り組む。

【 基本対策事項 】

＜3.1.1⑷(a)(d)関連＞

3.1.1⑷-1　役職員等関係者は、情報の格付及び取扱制限に応じて、情報を取り扱う際は、以下を全て含む対策を講じる。

a)　要保護情報を放置しない。

b)　要機密情報を必要以上に複製しない。また、複製する場合は、情報セキュリティ管理担当者の許可を得なければならない。

c)　電磁的記録媒体に要機密情報を保存する場合には、重要度に応じ整理を行い、主体認証情報を用いて保護するか又は情報を暗号化する。要機密情報が記録された記録媒体は、施錠のできる執務室や書庫・保管庫等に保存したりするなどの措置を講じる。

d)　電磁的記録媒体に要保全情報を保存する場合には、電子署名の付与を行うなど、改ざん防止のための措置を講じる。

e)　情報の保存方法を変更する場合には、格付、取扱制限及び記録媒体の特性に応じて必要な措置を講じる。

3.1.1⑷-2　役職員等関係者は、入手した情報の格付及び取扱制限が不明な場合には、情報の作成元又は入手元への確認を行う。

＜3.1.1⑷(e)関連＞

3.1.1⑷-3　役職員等関係者は、データ授受用端末（Fat クライアント）から事務処理用端末（ノート PC（Surface））にデータを取り込む場合、書込 CD を利用する。

遵守事項

⑸　情報の提供・公表

(a)　役職員等関係者は、情報を公表する場合には、当該情報が機密性 1 又は機密性 0 情報（重要性分類Ⅲ又はⅣ）に格付されるものであることを確認する。

(b)　役職員等関係者は、閲覧制限の範囲外の者に情報を提供する必要が生じた場合は、当該格付及び取扱制限の決定者等に相談し、その決定に従う。電子媒体及び紙媒体の情報提供依頼の対応については、情報セキュリティ管理者に相談し、的確に行う。また、提供先において、当該情報に付された格付及び取扱制限に応じて適切に取り扱われるよう、取扱い上の留意事項を確実に伝達するなどの措置を講じる。

(c)　役職員等関係者は、電磁的記録を提供又は公表する場合には、当該電磁的記録の付加記録（更新の履歴、文書のプロパティ等をいう。）等からの不用意な情報漏えいを防止するための措置を講じる。

(d)　役職員等関係者は、閲覧制限の範囲外の者に要機密情報を提供する必要が生じた場合は、情報セキュリティ管理担当者の許可を得る。また、提供先において適切に取り扱われるよう、取扱い上の留意事項を確実に伝達するなどの措置を講じる。

【 基本対策事項 】

＜3.1.1⑸(c)関連＞

3.1.1⑸-1　役職員等関係者は、電磁的記録媒体を他の者へ提供する場合は、当該電磁的記録媒体に保存された不要な要機密情報を抹消する。

遵守事項

⑹　情報の運搬・送信

(a)　役職員等関係者は、要保護情報が記録又は記載された記録媒体を要管理対策区域外に持ち出す場合には、当該情報を管理する情報セキュリティ管理担当者の許可を得た上で、安全確保に留意して運搬方法を決定し、情報の格付及び取扱制限に応じて、安全確保のための適切な措置を講じる。

(b)　役職員等関係者は、要保護情報である電磁的記録を電子メール等で送信する場合には、安全確保に留意して送信の手段を決定し、情報の格付及び取扱制限に応じて、安全確保のための適切な措置を講じる。また、要保護情報を支払基金外通信回線（インターネットを除く。）を使用して送信する場合には、暗号化措置を施した上で、情報セキュリティ管理担当者が指定する方法により送信する。

(c)　役職員等関係者は、紙媒体の管理について、紛失、混入等がないよう整理を行い、必要に応じ紐で綴じる等の措置を講じる。また、台車等で移動する際は、紛失のないよう確実に移動する。

【 基本対策事項 】

＜3.1.1⑹(a)関連＞

3.1.1⑹-1　役職員等関係者は、要保護情報が記録又は記載された記録媒体の要管理対策区域外への運搬を第三者へ依頼する場合は、セキュアな運送サービスを提供する運送事業者により運搬する。なお、保険者等への送達に当たっては、信頼できる業者を選定するとともに、貨物追跡システムを構築し、コンテナ等施錠のできる車輌を使用する等セキュリティの確保について、契約書に規定する。

＜3.1.1⑹(a)(b)関連＞

3.1.1⑹-2　役職員等関係者は、要機密情報である電磁的記録を要管理対策区域外に運搬する場合には、以下を例とする情報漏えいを防止するための対策を講じる。

a)　運搬する情報を暗号化する。

b)　分割後の個別の情報から分割前の情報が容易に復元あるいは推測できないように要機密情報を複数の情報に分割し、それぞれ異なる経路及び手段を用いて運搬する。

c)　主体認証機能や暗号化機能を備えるセキュアな外部電磁的記録媒体を利用す

る。

＜3.1.1(6)(b)関連＞

3.1.1(6)-3　役職員等関係者は、要機密情報である電磁的記録を、支払基金外通信回線を使用して送信する場合には、以下を例とする情報漏えいを防止するための対策を講じる。

a)　送信する情報を暗号化する。

b)　通信経路全般が暗号化されている通信経路を用いて送信する。

c)　分割後の個別の情報から分割前の情報が容易に復元あるいは推測できないように要機密情報を複数の情報に分割し、それぞれ異なる経路及び手段を用いて送信する。

3.1.1(6)-4　役職員等関係者は、要保護情報である電磁的記録を送信する場合は、安全確保に留意して、以下を例に当該情報の送信の手段を決定する。

a)　支払基金管理の通信回線を用いて送信する。

b)　信頼できる通信回線を使用して送信する。

c)　VPN を用いて送信する。

d)　S/MIME 等の暗号化された電子メールを使用して送信する。

e)　支払基金独自で運用している又は支払基金が利用を承認しているなどセキュリティが十分確保されたウェブメールサービス又はオンラインストレージ環境を利用する。

遵守事項

(7)　情報の消去

(a)　役職員等関係者は、電磁的記録媒体に保存された情報が職務上不要となった場合は、速やかに情報を消去する。

(b)　役職員等関係者は、電磁的記録媒体を廃棄する場合には、当該記録媒体内に情報が残留した状態とならないよう、全ての情報を復元できないように抹消する。

(c)　役職員等関係者は、要機密情報である書面を廃棄する場合には、情報セキュリティ管理担当者の許可を得た上で、復元が困難な状態にする。

【 基本対策事項 】

＜3.1.1(7)(a)関連＞

3.1.1(7)-1　役職員等関係者は、情報の抹消を外部の民間事業者等へ業務委託する場合は、情報が適切に抹消されたことを証明する資料の提出を求める、職員等による立会いを行う等、委託先での履行状況を確認する。

＜3.1.1(7)(b)関連＞

3.1.1(7)-2　役職員等関係者は、端末やサーバ装置等をリース契約で調達する場合は、契約

終了に伴う返却時の情報の抹消方法及び履行状況の確認手段について、以下を例とする対策を行う。

a) リース契約の調達仕様書に記載し、契約内容にも含める。

b) リース契約終了に伴う情報の抹消について、役務提供契約を別途締結する。

遵守事項

⑻ 情報のバックアップ

(a) 役職員等関係者は、情報の格付に応じて、適切な方法で情報のバックアップを実施する。

(b) 役職員等関係者は、取得した情報のバックアップについて、格付及び取扱制限に従って保存場所、保存方法、保存期間等を定め、適切に管理する。

(c) 役職員等関係者は、保存期間を過ぎた情報のバックアップについては、本款(7)の規定に従い、適切な方法で消去、抹消又は廃棄する。

【 基本対策事項 】

＜3.1.1(8)(a)関連＞

3.1.1(8)-1 役職員等関係者は、要保全情報又は要安定情報である電磁的記録若しくは重要な設計書について、バックアップを取得する。

＜3.1.1(8)(b)関連＞

3.1.1(8)-2 役職員等関係者は、要保全情報又は要安定情報である電磁的記録のバックアップ若しくは重要な設計書のバックアップについて、災害や情報セキュリティインシデント等の危機的事象により生ずる業務上の支障を考慮し、適切な保管場所を選定する。要保全情報又は要安定情報である電磁的記録のバックアップについて、危機的事象として情報システムや情報が破壊される情報セキュリティインシデントを想定する場合は、必要に応じて、以下を例とする情報システムや情報とバックアップが同時に破壊されない保管場所を選定する。

a) バックアップ取得元の情報システムが接続するネットワークから物理的に隔離された保管場所

b) バックアップ取得元の情報システムが接続するネットワークから論理的に隔離された保管場所

3.2 情報を取り扱う区域の管理

3.2.1 情報を取り扱う区域の管理

目的・趣旨

サーバ装置、端末等が、不特定多数の者により物理的に接触できる設置環境にある場合に

おいては、悪意ある者によるなりすまし、物理的な装置の破壊のほか、サーバ装置や端末の不正な持ち出しによる情報の漏えい等のおそれがある。その他、設置環境に関する脅威として、災害の発生による情報システムの損傷等もある。

したがって、執務室、会議室、サーバ室等の情報を取り扱う区域に対して、物理的な対策や入退管理の対策を講じることで区域の安全性を確保し、当該区域で取り扱う情報や情報システムのセキュリティを確保する必要がある。

遵守事項

⑴　要管理対策区域における対策の基準の決定

⑻　情報セキュリティ責任者は、要管理対策区域の範囲を定める。

⑼　情報セキュリティ責任者は、要管理対策区域の特性に応じて、以下の観点を全て含む対策を講じる。

(ｱ)　許可されていない者が容易に立ち入ることができないようにするための、施錠可能な扉、間仕切り等の施設の整備、設備の設置等の物理的な対策。

(ｲ)　許可されていない者の立入りを制限するため及び立入りを許可された者による立入り時の不正な行為を防止するための入退管理対策。

【 基本対策事項 】

＜3.2.1⑴⑼(ｱ)(ｲ)関連＞

3.2.1⑴-1　情報セキュリティ責任者は、要管理対策区域の安全性を確保するための段階的な対策の水準（以下「クラス」という。）を定める。下表のとおり、３段階のクラスとする。要管理対策区域へのクラスの割当ての例を図3.2.1-1～2に示す。

クラス	説明
クラス３	一部の限られた者以外の者の立入りを制限する必要があるなど、クラス２より強固な情報セキュリティを確保するための厳重な対策を実施する必要がある区域
クラス２	役職員等関係者以外の者の立入りを制限する必要があるなど、情報セキュリティを確保するための対策を実施する必要がある区域
クラス１	クラス３、クラス２以外の要管理対策区域

※便宜上、要管理対策区域外の区域はクラス０と呼び、クラス０＜クラス１＜クラス２＜クラス３の順位を設ける。すなわち、クラス０が最も下位のクラス、クラス３が最も上位のクラスとなる。

3.2.1⑴-2　情報セキュリティ責任者は、クラス１の区域について、施設の整備、設備の設置等の物理的な対策及び入退管理対策の基準として以下を定める。

a)　不特定の者が容易に立ち入らないように、壁、施錠可能な扉、パーティション等で囲むことで、下位のクラスの区域と明確に区分する。

b) 不特定の者が容易に立ち入らないように、立ち入る者の身元、訪問目的等の確認を行うための措置を講じる。また、出入口が無人になるなどにより立入りの確認ができない時間帯がある場合には、確認ができない時間帯に施錠するための措置を講じる。

c) 要管理対策区域に不正に立ち入った者を容易に判別することができるように、以下を全て含む措置を講じる。

(ｱ) 役職員等関係者は、支払基金支給の職員証（ネックストラップ付）を着用、明示する。クラス２及びクラス３の区域においても同様とする。

(ｲ) 一時的に立ち入った者に入館カード等を貸与し、着用、明示させる。クラス２及びクラス３の区域においても同様とする。この際、一時的に立ち入った者と継続的に立入りを許可された者に貸与する入館カード等やそれと併せて貸与するストラップ等の色分けを行う。また、悪用防止のために一時的に立ち入った者に貸与したものは、退出時に回収する。

3.2.1(1)-3 情報セキュリティ責任者は、クラス２の区域について、施設の整備、設備の設置等の物理的な対策及び入退管理対策の基準として以下を定める。

a) クラス２の区域への立入りを許可されていない者が容易に立ち入らないように、壁、施錠可能な扉、パーティション等で囲むことで、下位のクラスの区域と明確に区分する。ただし、窓口のある執務室等の明確に区分できない区域については、不特定の者が出入りできる時間帯は役職員等関係者が窓口を常に目視できるような措置を講じる。

b) クラス２の区域への立入りを許可されていない者が容易に立ち入らないように、施錠可能な扉を設置し全員不在時に施錠する。

c) クラス２の区域へ許可されていない者が容易に立ち入らないように、立ち入る者が許可された者であることの確認を行うための措置を講じる。

3.2.1(1)-4 情報セキュリティ責任者は、クラス３の区域について、施設の整備、設備の設置等の物理的な対策及び入退管理対策の基準として以下を定める。

a) クラス３の区域への立入りを許可されていない者の立入り等を防止するために、壁、常時施錠された扉、固定式のパーティション等強固な境界で下位のクラスの区域と明確に区分する。

b) クラス３の区域へ許可されていない者が立ち入らないように、立ち入る者が許可された者であることの確認を行うための措置を講じる。

c) クラス３の区域への立入りを許可されていない者に、不必要に情報を与えないために、区域の外側から内部の重要な情報や情報システムが見えないようにする。

d) 一時的に立ち入った者が不正な行為を行うことを防止するために、一時的に立ち入った者を放置しないなどの措置を講じる。業者が作業を行う場合は立会

いや監視カメラ等により監視するための措置を講じる。

e) 情報の持ち出し等を防止するため、私用の携帯電話、スマートフォン及びタブレット端末の区域内への持ち込みを制限する。

3.2.1(1)-5 情報セキュリティ責任者は、区域へのクラスの割当ての基準として以下を定める。

a) サーバ室や日常的に機密性が高い情報を取り扱う執務室には、一部の限られた者以外の者が立ち入り盗難又は破壊をすること、情報システムを直接操作して情報窃取すること等を防止するために、クラス３を割り当てる。

b) 一般的な執務室や執務室内の会議室には、役職員等関係者以外の者が立ち入り、情報システムを盗難又は破壊すること、情報システムを直接操作して情報窃取すること等を防止するために、クラス２を割り当てる。

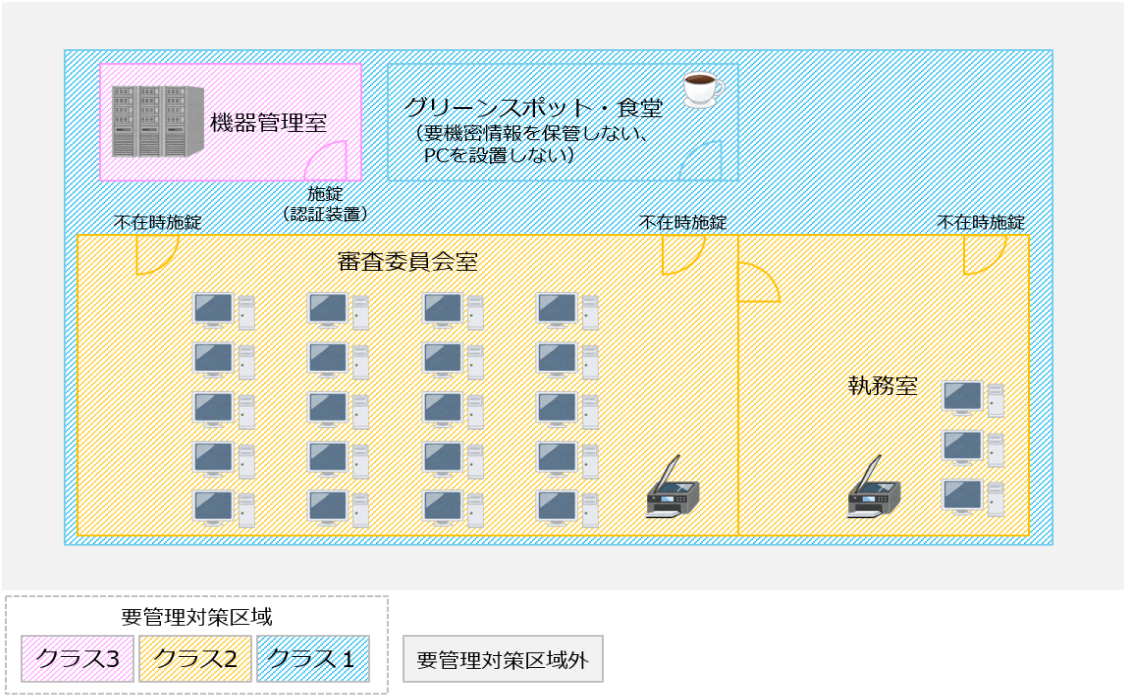


図 3.2.1-1 要管理対策区域へのクラスの割当ての例１（事務所）

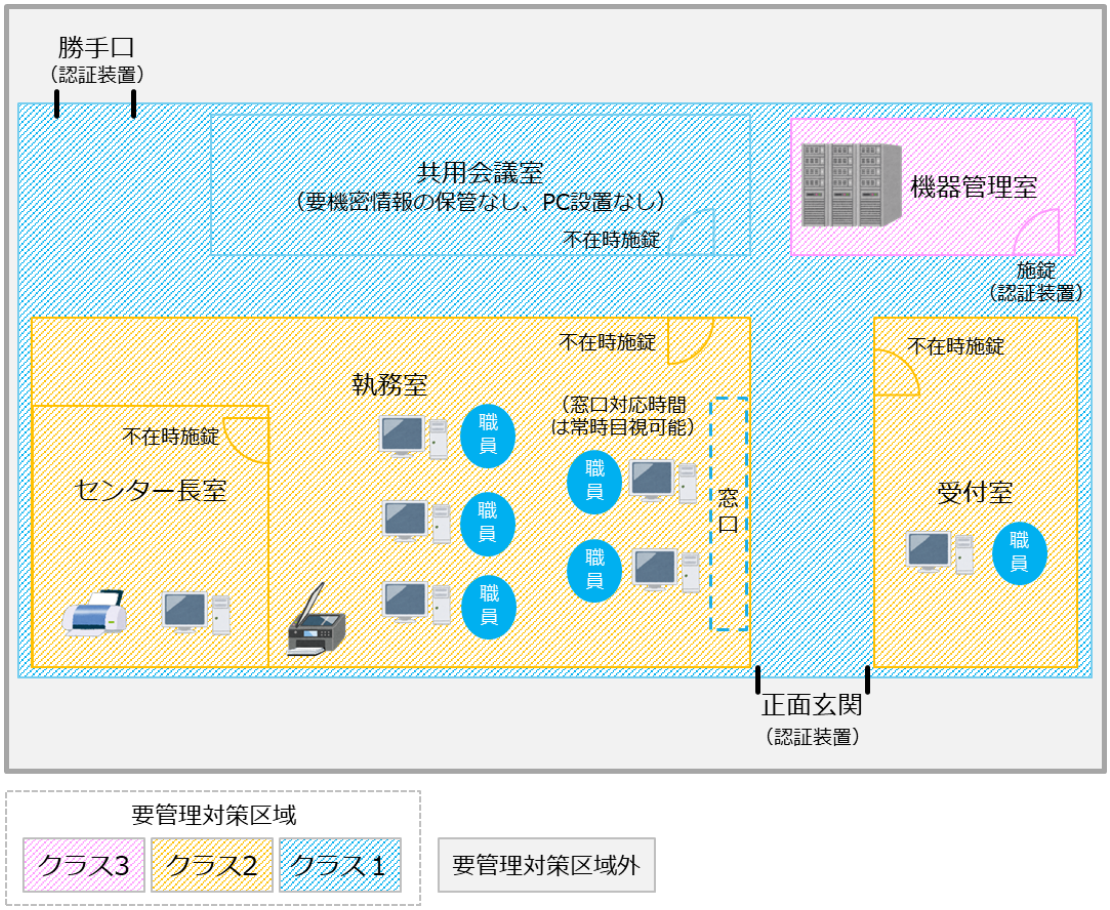


図 3.2.1-2 要管理対策区域へのクラスの割当ての例２（窓口のある執務室）

遵守事項

⑵　区域ごとの対策の決定

(a)　情報セキュリティ管理者は、情報セキュリティ責任者が定めた対策の基準を踏まえ、施設及び執務環境に係る対策を行う単位ごとの区域を定める。

(b)　情報セキュリティ管理補助者は、管理する区域について、情報セキュリティ責任者が定めた対策の基準と、周辺環境や当該区域で行う業務の内容、取り扱う情報等を勘案し、当該区域において実施する対策を決定する。

【 基本対策事項 】

＜3.2.1⑵(b)関連＞

3.2.1⑵-1　情報セキュリティ管理補助者は、管理する区域において、クラスの割当ての基準を参考にして当該区域に割り当てるクラスを決定するとともに、決定したクラスに対して定められた対策の基準と、周辺環境や当該区域で行う業務の内容、取り扱う情報等を勘案し、当該区域において実施する対策を決定する。この際、

決定したクラスで求められる対策のみでは安全性が確保できない場合は、当該区域で実施する個別の対策を含め決定する。

遵守事項

⑶　要管理対策区域における対策の実施

⒜　情報セキュリティ管理補助者は、管理する区域に対して定めた対策を実施する。役職員等関係者が実施すべき対策については、役職員等関係者が認識できる措置を講じる。

⒝　情報セキュリティ管理補助者は、災害から要安定情報を取り扱う情報システムを保護するために物理的な対策を講じる。

⒞　役職員等関係者は、利用する区域について情報セキュリティ管理補助者が定めた対策に従って利用する。また、役職員等関係者が支払基金外の者を立ち入らせる際には、当該支払基金外の者にも当該区域で定められた対策に従って利用させる。

【 基本対策事項 】

＜3.2.1⑶⒜関連＞

3.2.1⑶-1　情報セキュリティ管理補助者は、管理する区域について、以下を例とする利用手順等を整備し、当該区域を利用する役職員等関係者に周知する。

a)　扉の施錠及び開閉に関する利用手順

b)　一時的に立ち入る者が許可された者であることを確認するための手順

c)　一時的に立ち入る者を監視するための手順

第 4 部 外部委託

4.1 業務委託

4.1.1 業務委託

目的・趣旨

支払基金外の者に、調査・研究等の業務を委託、あるいは情報システムやアプリケーションプログラムの開発・運用・保守等を委託する際に、役職員等関係者が当該委託先における情報セキュリティ対策を直接管理することが困難な場合は、委託先に提供する要保護情報等を適切に保護するための情報セキュリティ対策が確実に実施されるよう、委託先への要求事項を調達仕様書等に定め、委託の際の契約条件とする必要がある。

業務委託には以下の例のように様々な種類があり、また、契約形態も、請負契約や委任、準委任、約款への同意等様々であるが、いずれの場合においても、前述のように委託先に提供した情報が適切に保護されるための情報セキュリティ対策が確実に実施される必要のある業務委託の契約時には、委託する業務の範囲や委託先の責任範囲等を明確化し、契約者双方で情報セキュリティ対策の詳細について合意形成することが重要である。

なお、委託業務でクラウドサービスを利用する場合は、委託先においてもクラウドサービス特有のリスクがあることから、4.2「クラウドサービス」で規定する内容についても取り扱う情報の格付、委託する業務や利用するクラウドサービスの特性等に応じて委託先への要求事項に含める必要がある。また、情報システムに関する業務を委託する際は、情報システムに関する別のリスクがあることから、4.1.2「情報システムに関する業務委託」に規定する内容についても実施する必要がある。さらに、機器等を調達する場合には、調達する機器等におけるサプライチェーン上のリスクがあることから、4.3「機器等の調達」で規定する内容についても実施する必要がある。

＜業務委託の例＞

- 情報システムの開発及び構築業務の委託
- アプリケーション・コンテンツの開発業務の委託
- 情報システムの運用業務の委託
- 業務運用支援業務（統計、集計、データ入力、媒体変換等）の委託
- プロジェクト管理支援業務の委託
- 調査・研究業務（調査、研究、検査等）の委託
- ウェブサイトの運用業務の委託

遵守事項

⑴　業務委託に係る対策の整備

⒜　情報セキュリティ責任者は、業務委託に係る以下の内容を全て含む対策を講じる。

(ｱ)　委託先への提供を認める情報及び委託する業務の範囲を判断する基準（以下「委託判断基準」という。）は次のとおりとする。

a　既存のシステム又は契約中の外部サービスでは代替できない等、業務を遂行する上で委託する必要性がある。

b　委託契約で個人情報を取り扱う場合、保存された情報に対して国内法令のみが適用される。

c　重要な情報（重要性分類Ⅱ以上）を提供する場合は、提供する情報を必要最小限とし、安全な方法で提供する。提供した情報が委託先にて不要となった場合は、確実に返却又は抹消させる。

d　その他、法令に違反しない。

(ｲ)　委託先の選定基準は、次のとおりとする。

a　委託先は、事業の継続性を有し存続する可能性が高く、本ポリシーと同等の対策が講じられていると判断できる。

b　委託先は、本ポリシーを遵守し得る者である。

c　委託先は、本ポリシーと同等の情報セキュリティ管理体制を整備している。

d　委託先は、事業従事者に対して、本ポリシーと同等の情報セキュリティ対策の教育を実施している。

e　委託業務において取り扱われる情報が重要な情報（重要性分類Ⅱ以上）である場合、委託先の第三者による認証について確認する。

遵守事項

⑵　業務委託実施前の対策

⒜　情報セキュリティ管理者は、業務委託の実施までに、以下を全て含む事項を実施する。

(ｱ)　委託する業務内容の特定

(ｲ)　委託先の選定条件を含む仕様の策定

(ｳ)　仕様に基づく委託先の選定

(ｴ)　契約の締結

(ｵ)　委託先に要機密情報を提供する場合は、秘密保持契約（NDA）の締結

⒝　情報セキュリティ管理者は、業務委託の実施までに、委託の前提条件として、以下を全て含む事項の実施を委託先に求める。

(ｱ)　仕様に準拠した提案

(ｲ)　契約の締結

(ｳ)　委託先において要機密情報を取り扱う場合は、秘密保持契約（NDA）の締結

【 基本対策事項 】

＜4.1.1⑵(a)(ｲ)関連＞

4.1.1⑵-1　情報セキュリティ管理者は、以下の内容を全て含む情報セキュリティ対策を実施することを委託先の選定条件とし、仕様等にも含める。

a)　委託先に提供する情報の委託先における目的外利用の禁止

b)　委託先における情報の適正な取扱いのための情報セキュリティ対策の実施内容及び管理体制

c)　情報セキュリティインシデントへの対処方法(情報セキュリティインシデント検知からの報告時間の定めを含む)

d)　情報セキュリティ対策その他の契約の履行状況の確認方法

e)　情報セキュリティ対策の履行が不十分な場合の対処方法

4.1.1⑵-2　情報セキュリティ管理者は、委託する業務において取り扱う情報の格付等を勘案し、以下の内容の全てを必要に応じて仕様等に含める。

a)　監査の受入れ

b)　サービス品質の保証

＜4.1.1⑵(a)(ｲ)(ｴ)関連＞

4.1.1⑵-3　情報セキュリティ管理者は、委託先との情報の受渡し方法や委託業務終了時の情報の廃棄方法等を含む情報の取扱手順について委託先と合意し、定められた手順により情報を取り扱う。

＜4.1.1⑵(a)(ｳ)関連＞

4.1.1⑵-4　情報セキュリティ管理者は、委託先がその役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、基本対策事項 4.1.1⑵-1 及び 2 の措置の実施を委託先に担保させるとともに、再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を支払基金に提供し、支払基金の承認を受けるよう、仕様に含める。また、委託判断基準及び委託先の選定基準に従って再委託の承認の可否を判断する。

＜4.1.1⑵(b)(ｱ)関連＞

4.1.1⑵-5　情報セキュリティ管理者は、以下の内容を全て含む委託先における情報セキュリティ対策の遵守方法、情報セキュリティ管理体制等に関する確認書等を提出させる。また、変更があった場合は、速やかに再提出させる。

a)　当該委託業務に携わる者の特定

b)　当該委託業務に携わる者が実施する具体的な情報セキュリティ対策の内容

遵守事項

⑶　業務委託実施期間中の対策

⒜　情報セキュリティ管理者は、業務委託の実施期間において以下を全て含む対策を実施する。

(ｱ)　委託判断基準に従った要保護情報の提供

(ｲ)　契約に基づき委託先に実施させる情報セキュリティ対策の履行状況の定期的な確認

(ｳ)　委託した業務において、情報セキュリティインシデントの発生若しくは情報の目的外利用等を認知した場合又はその旨の報告を役職員等関係者より受けた場合における、委託事業の一時中断などの必要な措置を含む、契約に基づく対処の要求

⒝　情報セキュリティ管理者は、業務委託の実施期間において以下を全て含む対策の実施を委託先に求める。

(ｱ)　情報の適正な取扱いのための情報セキュリティ対策

(ｲ)　契約に基づき委託先が実施する情報セキュリティ対策の履行状況の定期的な報告

(ｳ)　委託した業務において、情報セキュリティインシデントの発生若しくは情報の目的外利用等を認知した場合における、委託事業の一時中断などの必要な措置を含む対処

【 基本対策事項 】

＜4.1.1(3)(b)(ｱ)関連＞

4.1.1(3)-1　情報セキュリティ管理者は、委託業務における情報の適正な取扱いを委託先に担保させるため、以下の内容を全て含む情報セキュリティ対策について、あらかじめ委託先との契約に含めた上で、委託期間を通じて、情報の格付等に応じた実施を求める。

a)　情報セキュリティインシデント等への迅速・的確な対処能力の確立・維持（情報セキュリティインシデント検知からの報告時間の定めを含む）

b)　情報へアクセスする主体の識別とアクセスの制御

c)　ログの取得・監視

d)　情報を取り扱う機器等の物理的保護

e)　情報を取り扱う要員への周知と統制

f)　セキュリティ脅威に対処するための資産管理・リスク評価

g)　委託先が取り扱う情報及び当該情報を取り扱うシステムの完全性の保護

h)　セキュリティ対策の検証・評価・見直し

＜4.1.1(3)(b)(ｲ)関連＞

4.1.1(3)-2　セキュリティ担当課は、毎年度、業務委託事業者に対し、4.1.1(2)-1 b)等の内容について報告を求める。

遵守事項

⑷　業務委託終了時の対策

(a)　情報セキュリティ管理者は、業務委託の終了に際して以下を全て含む対策を実施する。

(ｱ)　業務委託の実施期間を通じてセキュリティ対策が適切に実施されたことの確認を含む検収

(ｲ)　委託先に提供した情報を含め、委託先において取り扱われた情報が確実に返却、廃棄又は抹消されたことの確認

(b)　情報セキュリティ管理者は、契約に基づき、業務委託の終了に際して以下を全て含む対策の実施を委託先に求める。

(ｱ)　業務委託の実施期間を通じてセキュリティ対策が適切に実施されたことの報告を含む検収の受検

(ｲ)　提供を受けた情報を含め、委託業務において取り扱った情報の返却、廃棄又は抹消

4.1.2　情報システムに関する業務委託

目的・趣旨

支払基金以外の者に、情報システムやアプリケーションプログラムの開発・運用・保守等の情報システムに関する業務を委託する際は、4.1.1「業務委託」で規定する内容に加え、委託先によって情報システムに支払基金の意図しない変更が加えられないための対策や、情報システムの構築の段階や運用・保守の段階において、脆弱性の混入を防止するための対策等の情報システムに関する業務委託に特有の対策を講じる必要があるこれらについても、委託先への要求事項として調達仕様書等に定め、委託の際の契約条件とする必要がある。

＜情報システムに関する業務委託の例＞

・情報システムの開発及び構築業務の委託
・アプリケーション・コンテンツの開発業務の委託
・情報システムの運用業務の委託
・支払基金内でのみ利用される共通基盤システム（情報システムのリソースやソフトウェアの一部又は全部を共有する基盤を提供する情報システム）の運用業務の委託（ホスティング型プライベートクラウド）

遵守事項

⑴　情報システムに関する業務委託における共通的対策

(a)　情報セキュリティ管理者は、情報システムに関する業務委託の実施までに、委託先の

選定条件に情報システムに支払基金の意図しない変更が加えられないための対策に係る選定条件を加え、仕様を策定する。

【 基本対策事項 】

＜4.1.2⑴⒜関連＞

4.1.2⑴-1　情報セキュリティ管理者は、以下の内容を全て含む情報セキュリティ対策を実施することを情報システムに関する業務委託の委託先の選定条件に加え、仕様にも含める。

a)　委託先企業若しくはその従業員、再委託先又はその他の者によって、情報システムに支払基金の意図しない変更が加えられないための管理体制

b)　委託先の資本関係・役員等の情報、委託事業の実施場所、委託事業従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供

遵守事項

⑵　情報システムの構築を業務委託する場合の対策

⒜　情報セキュリティ管理者は、情報システムの構築を業務委託する場合は、契約に基づき、以下を全て含む対策の実施を委託先に求める。

(ｱ)　情報システムのセキュリティ要件の適切な実装

(ｲ)　情報セキュリティの観点に基づく試験の実施

(ｳ)　情報システムの開発環境及び開発工程における情報セキュリティ対策

【 基本対策事項 】

＜4.1.2⑵⒜(ｲ)関連＞

4.1.2⑵-1　情報セキュリティ管理者は、情報セキュリティの観点に基づく試験の実施について、調達仕様書に記載するなどして、以下を全て含む事項の実施を委託先に求める。

a)　ソフトウェアの作成及び試験を行う情報システムについては、情報セキュリティの観点から運用中の情報システムに悪影響が及ばないように、運用中の情報システムと分離する。

b)　情報セキュリティの観点から必要な試験がある場合には、試験項目及び試験方法を定め、これに基づいて試験を実施する。

c)　情報セキュリティの観点から実施した試験の実施記録を保存する。

＜4.1.2⑵⒜(ｳ)関連＞

4.1.2⑵-2　情報セキュリティ管理者は、開発工程における情報セキュリティ対策として、調達仕様書に記載するなどして、以下を全て含む事項の実施を委託先に求める。

a) ソースコードが不正に変更・消去されることを防ぐために、以下の事項を含むソースコードの管理を適切に行う。

・ソースコードの変更管理

・ソースコードの閲覧制限のためのアクセス制御

・ソースコードの滅失、き損等に備えたバックアップの取得

b) 情報システムに関連する脆弱性についての対策要件として定めたセキュリティ実装方針に従う。

c) セキュリティ機能が適切に実装されていること及びセキュリティ実装方針に従った実装が行われていることを確認するために、設計レビュー及びソースコードレビューの範囲及び方法を定め、これに基づいてレビューを実施する。

遵守事項

⑶ 情報システムの運用・保守を業務委託する場合の対策

⑷ 情報セキュリティ管理者は、情報システムの運用・保守を業務委託する場合は、情報システムに実装されたセキュリティ機能が適切に運用されるための要件について、契約に基づき、委託先に実施を求める。

⑸ 情報セキュリティ管理者は、情報システムの運用・保守を業務委託する場合は、委託先が実施する情報システムに対する情報セキュリティ対策を適切に把握するため、当該対策による情報システムの変更内容について、契約に基づき、委託先に速やかな報告を求める。

【 基本対策事項 】

＜4.1.2⑶⑷関連＞

4.1.2⑶-1 情報セキュリティ管理者は、情報システムの運用・保守を業務委託する場合は、情報システムに実装されたセキュリティ機能が適切に運用されるために、以下を全て含む要件を調達仕様書に記載するなどして、契約に基づき、委託先に実施を求める。

a) 情報システムの運用環境に課せられるべき条件の整備

b) 情報システムのセキュリティ監視を行う場合の監視手順や連絡方法（情報セキュリティインシデント検知からの報告時間の定めを含む）

c) 情報システムの保守における情報セキュリティ対策

d) 運用中の情報システムに脆弱性が存在することが判明した場合の情報セキュリティ対策

遵守事項

⑷　支払基金向けに情報システムの一部の機能を提供するサービスを利用する場合の対策

⑷(a)　情報セキュリティ管理者は、支払基金以外の一般の者が支払基金向けに要機密情報を取り扱う情報システムの一部の機能を提供するサービス（クラウドサービスを除く。）（以下「業務委託サービス」という。）を利用するため、情報システムに関する業務委託を実施する場合は、委託先の選定条件に業務委託サービスに特有の選定条件を加える。

⑷(b)　情報セキュリティ管理者は、業務委託サービスに係るセキュリティ要件を定め、業務委託サービスを選定する。

⑷(c)　情報セキュリティ管理者は、委託先の信頼性が十分であることを総合的・客観的に評価し判断する。

⑷(d)　情報セキュリティ管理担当者は、業務委託サービスを利用する場合には、情報セキュリティ管理者へ当該サービスの利用申請を行う。

⑷(e)　情報セキュリティ管理者は、業務委託サービスの利用申請を受けた場合は、当該利用申請を審査し、利用の可否を決定する。

⑷(f)　情報セキュリティ管理者は、業務委託サービスの利用申請を承認した場合は、承認済み業務委託サービスとして記録する。なお、業務委託サービスの管理者は、情報セキュリティ管理担当者とする。

【 基本対策事項 】

＜4.1.2⑷(a)関連＞

4.1.2⑷-1　情報セキュリティ管理者は、業務委託サービスの中断や終了時に円滑に業務を移行するための対策として、以下を例とするセキュリティ対策を実施することを委託先の選定条件に加え、仕様にも含める。

a)　取り扱う情報の可用性区分の格付に応じた、業務委託サービス中断時の復旧要件

b)　取り扱う情報の可用性区分の格付に応じた、業務委託サービス終了又は変更の際の事前告知の方法・期限及びデータ移行方法

4.1.2⑷-2　情報セキュリティ管理者は、業務委託サービスの利用を通じて支払基金が取り扱う情報に対して国内法以外の法令及び規制が適用されるリスクを評価して委託先を選定し、必要に応じて支払基金の情報が取り扱われる場所及び契約に定める準拠法・裁判管轄を委託先の選定条件に加え、仕様にも含める。

＜4.1.2⑷(b)関連＞

4.1.2⑷-3　情報セキュリティ管理者は、取り扱う情報の格付及び取扱制限に応じてセキュリティ要件を定め、業務委託サービスを選定する。また、業務委託サービスのセキュリティ要件としてセキュリティに係る国際規格等と同等以上の水準を求

める。

＜4.1.2(4)(c)関連＞

4.1.2(4)-4　情報セキュリティ管理者は、監査による報告書の内容、各種の認定・認証制度の適用状況等から、業務委託先の信頼性が十分であることを総合的・客観的に評価し判断する。

4.2　クラウドサービス

4.2.1　クラウドサービスの選定（要機密情報を取り扱う場合）

目的・趣旨

支払基金が委託先に取扱いを委ねる情報は、当該委託先によって適正に取り扱われなければならないが、クラウドサービスにおけるセキュリティ対策の詳細を直接確認することは一般に容易ではない。このため支払基金がクラウドサービスを利用して要機密情報を取り扱う場合は、クラウドサービスの特性を理解し、支払基金によるクラウドサービス提供者へのガバナンスの有効性や、利用の際のセキュリティ確保のために必要な事項を十分に考慮し、支払基金とクラウドサービス提供者の役割や責任分担を明確にした上で、クラウドサービスが選定基準及びセキュリティ要件を満たすことを確実にすることが求められる。

＜クラウドサービスの例＞

・仮想サーバ、ストレージ、ハイパーバイザー等提供サービス（IaaS）
・データベースや開発フレームワーク等のミドルウェア等提供サービス（PaaS）
・Ｗｅｂ会議サービス
・ソーシャルメディア
・検索サービス、翻訳サービス、地図サービス

なお、民間事業者等が不特定多数の利用者に対して提供する、定型約款や規約等への同意のみで利用可能となるクラウドサービスでは、セキュリティ対策やデータの取扱いなどについて支払基金への特別な扱いを求めることができない場合が多く、要機密情報を取り扱う上で必要十分なセキュリティ要件を満たすことが一般的に困難であることから、原則として要機密情報を取り扱うことはできないため、4.2.3「クラウドサービスの選定・利用（要機密情報を取り扱わない場合）」の規定を遵守する必要がある。

遵守事項

(1)　クラウドサービスの選定に係る運用手順書の整備

(a)　情報セキュリティ責任者は、以下を全て含む要機密情報を取り扱う場合のクラウドサービス（要機密情報を取り扱う場合）の選定に関する運用手順書を整備する。

(ｱ)　クラウドサービスを利用可能な業務及び情報システムの範囲並びに情報の取扱い

を許可する場所を判断する基準（以下 4.2 節において「クラウドサービス利用判断基準」という。）

(ｲ) クラウドサービスの選定基準

(ｳ) クラウドサービスの利用申請の許可権限者（情報セキュリティ管理者）と利用手続

(ｴ) クラウドサービス管理者（情報セキュリティ管理担当者）の指名とクラウドサービスの利用状況の管理

【 基本対策事項 】

＜4.2.1(1)(a)(ｱ)関連＞

4.2.1(1)-1 情報セキュリティ責任者は、遵守事項 4.1.1(1)(a)(ｱ) で整備を求めている「委託判断基準」と同等の基準とするとともに、クラウドサービス特有の脅威やクラウドサービスで利用する業務等を踏まえた上でクラウドサービス利用判断基準を策定する。

＜4.2.1(1)(a)(ｲ)関連＞

4.2.1(1)-2 情報セキュリティ責任者は、クラウドサービスの選定基準について、遵守事項 4.1.1(1)(a)(ｲ) で整備を求めている「委託先の選定基準」と同等の基準とするとともに、ISMAP クラウドサービスリストから選定することを求める。

＜4.2.1(1)(a)(ｳ)関連＞

4.2.1(1)-3 情報セキュリティ責任者は、支払基金において要機密情報を取り扱う場合のクラウドサービスの利用手続を、以下を全て含める内容を定める。

a) 利用申請の許可権限者

b) 申請内容

・ISMAP クラウドサービスリストの登録番号
・クラウドサービスの名称（必要に応じて機能名までを含む）
・クラウドサービスの種類
・クラウドサービス提供者の名称
・利用目的（業務内容）
・取り扱う情報の格付
・利用期間
・利用申請者（所属・氏名）
・利用者の範囲（支払基金内に限る、部内に限る など）
・選定時の確認結果

＜4.2.1(1)(a)(ｴ)関連＞

4.2.1(1)-4 情報セキュリティ責任者は、支払基金におけるクラウドサービスの利用状況の管理について、以下を例に運用手順書を整備する。

a) 利用申請の許可権限者（情報セキュリティ管理者）は、申請ごとにクラウドサービス管理者（情報セキュリティ管理担当者）を指名する。

b) 利用承認したクラウドサービスは、その内容を遅滞なく記録するよう運用ルールを定め、常に最新のクラウドサービスの利用状況を把握できるようにする。記録する際は、以下を例とする項目を記録し支払基金内で共有する。

・ISMAP クラウドサービスリストの登録番号
・クラウドサービスの名称（必要に応じて機能名までを含む）
・クラウドサービスの種類
・クラウドサービス提供者の名称
・利用目的（業務内容）
・取り扱う情報の格付
・利用期間
・利用申請者（所属・氏名）
・利用者の範囲（支払基金内に限る、部内に限る など）
・クラウドサービス管理者（情報セキュリティ管理担当者の所属・氏名）

遵守事項

⑵ クラウドサービスの選定

⑻ 情報セキュリティ管理者は、取り扱う情報の格付及び取扱制限を踏まえ、クラウドサービス利用判断基準に従って業務に係る影響度等を検討した上でクラウドサービスの利用を検討する。

⑼ 情報セキュリティ管理者は、取り扱う情報の格付及び取扱制限並びにクラウドサービス提供者との情報セキュリティに関する役割及び責任の範囲を踏まえて、以下を全て含むセキュリティ要件を定める。

(ｱ) クラウドサービスに求める情報セキュリティ対策
(ｲ) クラウドサービスで取り扱う情報が保存される国・地域及び廃棄の方法
(ｳ) クラウドサービスに求めるサービスレベル

(c) 情報セキュリティ管理者は、クラウドサービスの選定基準に従い、前項で定めたセキュリティ要件を踏まえて、原則として ISMAP クラウドサービスリストからクラウドサービスを選定する。

【 基本対策事項 】

＜4.2.1⑵(b)(ｱ)関連＞

4.2.1⑵-1 情報セキュリティ管理者は、クラウドサービスに求めるセキュリティ要件策定に当たっては、ISMAP の管理策基準が求める対策と同等以上の水準を求める。

＜4.2.1⑵(b)(ｱ)(ｲ)(ｳ)関連＞

4.2.1(2)-2　情報セキュリティ管理者は、業務に特有のリスクを踏まえ、クラウドサービスで取り扱う情報が保存される国・地域及び廃棄の方法、クラウドサービスに求める情報セキュリティ対策やサービスレベル等をクラウドサービスに求めるセキュリティ要件に含める。

＜4.2.1(2)(c)関連＞

4.2.1(2)-3　情報セキュリティ管理者は、クラウドサービスを選定するに当たっては、ISMAP クラウドサービスリストの詳細情報等を用いて、(2)(b)で定めたセキュリティ要件を満たしていることを確認する。

遵守事項

(3)　クラウドサービスの利用に係る調達

(a)　情報セキュリティ管理者は、クラウドサービスを調達する場合は、クラウドサービス提供者の選定基準及び選定条件並びにクラウドサービスの選定時に定めたセキュリティ要件を調達仕様に含める。

(b)　情報セキュリティ管理者は、クラウドサービスを調達する場合は、クラウドサービス提供者及びクラウドサービスが調達仕様を満たすことを契約までに確認し、利用承認を得る。また、調達仕様の内容は、契約に含める。

【 基本対策事項 】

＜4.2.1(3)(b)関連＞

4.2.1(3)-1　情報セキュリティ管理者は、調達仕様の内容を契約に含める際、クラウドサービス提供者との情報セキュリティに関する役割及び責任の範囲が明確になっていることを確認する。

遵守事項

(4)　クラウドサービスの利用承認

(a)　情報セキュリティ管理担当者は、クラウドサービスを利用する場合には、利用申請の許可権限者へクラウドサービスの利用申請を行う。

(b)　利用申請の許可権限者（情報セキュリティ管理者）は、役職員等関係者によるクラウドサービスの利用申請を審査し、許可の可否を決定する。

(c)　利用申請の許可権限者（情報セキュリティ管理者）は、クラウドサービスの利用申請を許可した場合は、承認済みクラウドサービスとして記録し、クラウドサービス管理者（情報セキュリティ管理担当者）を指名する。

【 基本対策事項 】

＜4.2.1⑷(b)関連＞

4.2.1⑷-1　利用申請の許可権限者（情報セキュリティ管理者）は、クラウドサービスの利用申請の審査においては、以下を全て含む内容を審査し、利用の可否を決定する。

a)　クラウドサービス提供者が、業務に特有のリスクを踏まえたクラウドサービス提供者の選定条件を満たしていること。

b)　利用するクラウドサービスのセキュリティ要件が、ISMAP 管理基準の管理策基準が求める対策と同等以上の水準であること。

c)　クラウドサービスで取り扱う情報が保存される国・地域及び情報の廃棄方法が、支払基金が求めるセキュリティ要件を満たしていること。

d)　クラウドサービスに求めるサービスレベルが、支払基金が求めるセキュリティ要件を満たしていること。

4.2.2　クラウドサービスの利用（要機密情報を取り扱う場合）

目的・趣旨

クラウドサービスを利用する際のセキュリティ対策は、選定や契約時における対策だけでなく、契約後のクラウドサービスを利用した情報システムの導入・構築、運用・保守、更には契約終了時に至るまで情報システムのライフサイクル全般において行う必要がある。

クラウドサービスのサービス内容は非常に早いサイクルで変化しており、新たに追加される機能を活用することで業務の効率化や情報セキュリティの向上を図ることができる。一方で、構築時には想定していなかった脅威や脆弱性が発生する可能性もある。したがって、クラウドサービスの利用においては、情報セキュリティ対策の定期的な確認による見直しをすることで、セキュリティ要件の追加及び修正を漏れなく実施することが求められる。さらに、クラウドサービスへのアクセス権限については、支払基金の業務やクラウドサービスの利用環境等の変化に応じて、定期的な確認による見直しをすることが重要である。

なお、本款ではクラウドサービスを利用する場合のライフサイクルの各段階において、特に必要となる情報セキュリティ対策を示しており、情報システム全体のライフサイクルの各段階で必要な情報セキュリティ対策については、5.2「情報システムのライフサイクルの各段階における対策」で定める遵守事項についても併せて遵守する必要がある。

遵守事項

⑴　クラウドサービスの利用に係る運用手順書の整備

(a)　情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方等を踏まえ、クラウドサービスを利用して情報システムを導入・構築する際のセキュリティ対策の基本方針を運用手順書として整備する。

⑹　情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、クラウドサービスを利用して情報システムを運用・保守する際のセキュリティ対策の基本方針を運用手順書として整備する。

⑹　情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、以下を全て含むクラウドサービスの利用を終了する際のセキュリティ対策の基本方針を運用手順書として整備する。

(ｱ)　クラウドサービスの利用終了時における対策

(ｲ)　クラウドサービスで取り扱った情報の廃棄

(ｳ)　クラウドサービスの利用のために作成したアカウントの廃棄

【 基本対策事項 】

＜4.2.2(1)(a)関連＞

4.2.2(1)-1　情報セキュリティ責任者は、不正なアクセスを防止するため、以下を全て含む構築時におけるアクセス制御に係る基本方針を運用手順書に含める。

a)　クラウドサービスを利用する際にクラウドサービス提供者が付与又はクラウドサービス利用者が登録する識別コードの作成から廃棄に至るまでのライフサイクルにおける管理

b)　クラウドサービスを利用する際に使用するネットワークに対するサービスごとのアクセス制御

c)　クラウドサービスを利用する情報システム許可権限者を保有するクラウドサービス利用者に対する強固な認証技術の利用

d)　クラウドサービス提供者が提供する主体認証情報の管理機能が要求事項を満たすことの確認及び要求事項を満たすための措置の実施

e)　クラウドサービス上に保存する情報やクラウドサービスの機能に対してアクセス制御できることの確認及び適切なアクセス制御の実施

f)　クラウドサービス利用者によるクラウドサービスに多大な影響を与える操作の特定と誤操作の抑制

g)　クラウドサービス上で構成される仮想マシンに対する適切なセキュリティ対策の実施

h)　インターネット等の支払基金外通信回線から支払基金内通信回線を経由せずにクラウドサービス上に構築した情報システムにログインすることの要否の判断と認める場合の適切なセキュリティ対策の実施

i)　クラウドサービスが正しく利用されていることの検証及び不正侵入、不正操作等がなされていないことの検証を行うための必要なログの管理

4.2.2(1)-2　情報セキュリティ責任者は、取り扱う情報の機密性保護のため、以下を全て含む構築時における暗号化に係る基本方針を運用手順書に含める。

a) クラウドサービス内及び通信経路全般における暗号化の確認及び適切な実施

b) 情報システムで利用する暗号化方式の遵守度合いに係る法令や規則の確認

4.2.2(1)-3 情報セキュリティ責任者は、以下を全て含む構築時における開発時のセキュリティ対策に係る基本方針を運用手順書に含める。

a) クラウドサービスを利用する場合のクラウドサービス提供者へのセキュリティを保つための開発手順等の情報の要求とその活用

b) クラウドサービス上に他ベンダが提供するソフトウェア等を導入する場合のそのソフトウェアのクラウドサービス上におけるライセンス規定

4.2.2(1)-4 情報セキュリティ責任者は、以下を全て含む構築時における設計・設定時の誤り防止に係る基本方針を運用手順書に含める。

a) クラウドサービスを利用する際のクラウドサービス提供者への設計、設定、構築等における知見等の情報の要求とその活用

b) クラウドサービスを利用する際の設定の誤りを見いだすための対策

c) クラウドサービス上に構成された情報システムのネットワーク設計におけるセキュリティ要件の異なるネットワーク間の通信の監視

d) 利用するクラウドサービス上の情報システムが利用するデータ容量や稼働性能についての監視と将来の予測

e) 利用するクラウドサービス上で要安定情報を取り扱う場合の可用性を考慮した設計

f) クラウドサービス内における時刻同期の方法の確認

＜4.2.2(1)(b)関連＞

4.2.2(1)-5 情報セキュリティ責任者は、以下を全て含む運用・保守時における利用方針に係る基本方針を運用手順書に含める。

a) 責任分界点を意識したクラウドサービスの利用

b) 利用承認を受けていないクラウドサービスの利用禁止

c) クラウドサービス提供者に対する定期的なサービスの提供状態の確認

d) 利用するクラウドサービスに係る情報セキュリティインシデント発生時の連絡体制

4.2.2(1)-6 情報セキュリティ責任者は、以下を全て含むクラウドサービス利用に必要な運用・保守時における教育に係る基本方針を運用手順書に含める。

a) クラウドサービス利用のための運用手順

b) クラウドサービス利用に係る情報セキュリティリスクとリスク対応について

c) クラウドサービス利用に関する適用法令や関連する規制等について

4.2.2(1)-7 情報セキュリティ責任者は、以下を全て含む運用・保守時におけるクラウドサービスで取り扱う資産の管理に係る基本方針を運用手順書に含める。

a) クラウドサービス上で利用する IT 資産の適切な管理

b) クラウドサービス上に保存する情報に対する適切な格付・取扱制限の明示

c) クラウドサービスの機能に対する脆弱性対策について、クラウドサービス利用者の責任範囲の明確化と対策の実施

4.2.2(1)-8 情報セキュリティ責任者は、不正アクセスを防止するため、以下を全て含む運用・保守時におけるアクセス制御に係る基本方針を運用手順書に含める。

a) 管理者権限をクラウドサービス利用者へ割り当てる場合のアクセス管理と操作の確実な記録

b) クラウドサービス利用者に割り当てたアクセス権限に対する定期的な確認による見直し

c) クラウドサービスのリソース設定を変更するユーティリティプログラムを使用する場合の機能の確認と利用者の制限

d) 利用するクラウドサービスの不正利用の監視

4.2.2(1)-9 情報セキュリティ責任者は、クラウドサービスで取り扱う情報の機密性保護のため、以下を全て含む運用・保守時における暗号化に係る基本方針を運用手順書に含める。

a) 暗号化に用いる鍵の管理者と鍵の保管場所等の鍵管理機能

b) 鍵管理機能をクラウドサービス提供者が提供する場合の鍵管理手順と鍵の種類の情報の要求とリスク評価

c) 鍵管理機能をクラウドサービス提供者が提供する場合の鍵の生成から廃棄に至るまでのライフサイクルにおける情報の要求とリスク評価

4.2.2(1)-10 情報セキュリティ責任者は、以下を全て含む運用・保守時におけるクラウドサービス内の通信の制御に係る基本方針を運用手順書に含める。

a) 利用するクラウドサービスのネットワーク基盤が他のネットワークと分離されていることの確認

4.2.2(1)-11 情報セキュリティ責任者は、以下を全て含む運用・保守時における設計・設定時の誤りの防止に係る基本方針を運用手順書に含める。

a) クラウドサービスの設定を変更する場合の設定の誤りを防止するための対策

b) クラウドサービス利用者が行う可能性のある重要操作の手順書の作成と監督者の指導の下での実施

4.2.2(1)-12 情報セキュリティ責任者は、以下を全て含む運用・保守時におけるクラウドサービスを利用した情報システムの事業継続に係る基本方針を運用手順書に含める。

a) 不測の事態に対してサービスの復旧を行うために必要なバックアップの確実な実施。又は、クラウドサービス提供者が提供する機能を利用する場合は、その実施の確認

b) 要安定情報をクラウドサービスで取り扱う場合の十分な可用性の担保、復旧

に係る手順の策定と定期的な訓練の実施

c) クラウドサービス提供者からの仕様内容の変更通知に関する内容確認と復旧手順の確認

d) クラウドサービスで利用しているデータ容量、性能等の監視

＜4.2.2(1)(c)(ｱ)関連＞

4.2.2(1)-13 情報セキュリティ責任者は、以下を全て含む更改・廃棄時における利用終了手順に係る基本方針を運用手順書に含める。

a) クラウドサービスの利用を終了する場合の移行計画書又は終了計画書の作成

b) 移行計画書又は終了計画書のクラウドサービス利用者への事前通知

＜4.2.2(1)(c)(ｲ)関連＞

4.2.2(1)-14 情報セキュリティ責任者は、以下を全て含む更改・廃棄時における情報の廃棄に係る基本方針を運用手順書に含める。

a) 情報の廃棄方法

b) 暗号化消去が実施できない場合の基盤となる物理機器の廃棄方法

＜4.2.2(1)(c)(ｳ)関連＞

4.2.2(1)-15 情報セキュリティ責任者は、以下を全て含む更改・廃棄時におけるアカウントの廃棄に係る基本方針を運用手順書に含める。

a) 作成されたクラウドサービス利用者アカウントの削除

b) 利用したクラウドサービスにおける管理者アカウントの削除・返却と再利用の確認

c) クラウドサービス利用者アカウント以外の特殊なアカウントの削除と関連情報の廃棄

遵守事項

(2) クラウドサービスの利用に係るセキュリティ要件の策定

(a) クラウドサービス管理者（情報セキュリティ管理担当者）は、クラウドサービスを利用する目的、対象とする業務等の業務要件及びクラウドサービスで取り扱われる情報の格付等に基づき、(1)各項で整備した基本方針としての運用手順書に従い、クラウドサービスの利用に係る内容を確認する。

(b) クラウドサービス管理者（情報セキュリティ管理担当者）は、クラウドサービスを利用する目的、対象とする業務等の業務要件及びクラウドサービスで取り扱われる情報の格付等に基づき、(1)各項で整備した基本方針としての運用手順書に従い、クラウドサービスの利用に係るセキュリティ要件を策定する。

【 基本対策事項 】

＜4.2.2⑵⒜関連＞

4.2.2⑵-1　クラウドサービス管理者（情報セキュリティ管理担当者）は、以下を全て含むクラウドサービスの利用に係る内容を確認する。

a)　クラウドサービス提供者が提供する主体認証情報の管理機能が支払基金の要求事項を満たすこと。

b)　クラウドサービス上に保存する情報やクラウドサービスの機能に対してアクセス制御できること。

c)　クラウドサービス利用者によるクラウドサービスに多大な影響を与える操作の特定

d)　クラウドサービス内及び通信経路全般における暗号化

e)　クラウドサービス上に他ベンダが提供するソフトウェア等を導入する場合のそのソフトウェアのクラウドサービス上におけるライセンス規定

f)　クラウドサービスのリソース設定を変更するユーティリティプログラムを使用する場合の機能

g)　鍵管理機能をクラウドサービス提供者が提供する場合の鍵管理手順と鍵の種類の情報の要求とリスク評価

h)　鍵管理機能をクラウドサービス提供者が提供する場合の鍵の生成から廃棄に至るまでのライフサイクルにおける情報の要求とリスク評価

i)　利用するクラウドサービスのネットワーク基盤が他のネットワークと分離されていること。

j)　クラウドサービス提供者が提供するバックアップ機能を利用する場合、求める要求事項が満たされること。

＜4.2.2⑵⒝関連＞

4.2.2⑵-2　クラウドサービス管理者（情報セキュリティ管理担当者）は、以下を全て含むクラウドサービスで利用するアカウント管理に関するセキュリティ機能要件を策定する。

a)　クラウドサービス提供者が付与又はクラウドサービス利用者が登録する識別コードの作成から廃棄に至るまでのライフサイクルにおける管理

b)　クラウドサービスを利用する管理者権限を保有するクラウドサービス利用者に対する強固な認証技術

c)　クラウドサービス提供者が提供する主体認証情報の管理機能が要求事項を満たすための措置

4.2.2⑵-3　クラウドサービス管理者（情報セキュリティ管理担当者）は、以下を全て含むクラウドサービスで利用するアクセス制御に関するセキュリティ機能要件を策定する。

a) クラウドサービス上に保存する情報やクラウドサービスの機能に対して適切なアクセス制御

b) インターネット等の支払基金外通信回線から支払基金内通信回線を経由せずにクラウドサービス上に構築した情報システムにログインすることを認める場合の適切なセキュリティ対策

4.2.2(2)-4 クラウドサービス管理者（情報セキュリティ管理担当者）は、以下を全て含むクラウドサービスで利用する権限管理に関するセキュリティ機能要件を策定する。

a) クラウドサービス利用者によるクラウドサービスに多大な影響を与える誤操作の抑制

b) クラウドサービスのリソース設定を変更するユーティリティプログラムを使用する場合の利用者の制限

4.2.2(2)-5 クラウドサービス管理者（情報セキュリティ管理担当者）は、以下を全て含むクラウドサービスで利用するログ管理に関するセキュリティ機能要件を策定する。

a) クラウドサービスが正しく利用されていることの検証及び不正侵入、不正操作等がなされていないことの検証を行うために必要なログの管理

4.2.2(2)-6 クラウドサービス管理者（情報セキュリティ管理担当者）は、以下を全て含むクラウドサービスで利用する暗号化に関するセキュリティ機能要件を策定する。

a) クラウドサービス内及び通信経路全般における暗号化の適切な実施

b) 情報システムで利用する暗号化方式の遵守度合いに係る法令や規則の確認

c) 暗号化に用いる鍵の保管場所等の管理に関する要件

d) クラウドサービスで利用する暗号鍵に関する生成から廃棄に至るまでのライフサイクルにおける適切な管理

4.2.2(2)-7 クラウドサービス管理者（情報セキュリティ管理担当者）は、以下を全て含むクラウドサービスを利用する際の設計・設定時の誤り防止に関するセキュリティ要件を策定する。

a) クラウドサービス上で構成される仮想マシンに対する適切なセキュリティ対策

b) クラウドサービス提供者へのセキュリティを保つための開発手順等の情報の要求とその活用

c) クラウドサービス提供者への設計、設定、構築等における知見等の情報の要求とその活用

d) クラウドサービスの設定の誤りを見いだすための対策

4.2.2(2)-8 クラウドサービス管理者（情報セキュリティ管理担当者）は、以下を全て含むクラウドサービス運用時の監視等の運用管理機能要件を策定する。

a) クラウドサービス上に構成された情報システムのネットワーク設計におけるセキュリティ要件の異なるネットワーク間の通信の監視

b) 利用するクラウドサービス上の情報システムが利用するデータ容量や稼働性能についての監視と将来の予測

c) クラウドサービス内における時刻同期の方法

d) 利用するクラウドサービスの不正利用の監視

4.2.2(2)-9 クラウドサービス管理者（情報セキュリティ管理担当者）は、以下を全て含むクラウドサービスの可用性に関するセキュリティ要件を策定する。

a) 利用するクラウドサービス上で要安定情報を取り扱う場合の可用性を考慮した設計

4.2.2(2)-10 クラウドサービス管理者（情報セキュリティ管理担当者）は、以下を全て含む利用するクラウドサービスにおいて情報セキュリティインシデントが発生した際の復旧に関する対策要件を策定する。

a) 不測の事態に対してサービスの復旧を行うために必要なバックアップの確実な実施

遵守事項

(3) クラウドサービスを利用した情報システムの導入・構築時の対策

(a) クラウドサービス管理者（情報セキュリティ管理担当者）は、(1)(a)で定めた運用手順書を踏まえて、(2)(b)において定めるセキュリティ要件に従いクラウドサービス利用における必要な措置を講じる。また、導入・構築時に実施状況を確認・記録する。

(b) クラウドサービス管理者（情報セキュリティ管理担当者）は、情報システムにおいてクラウドサービスを利用する際には、情報システム台帳及び関連文書に記録又は記載する。なお、情報システム台帳に記録又は記載した場合は、情報セキュリティ責任者へ報告する。

(c) クラウドサービス管理者（情報セキュリティ管理担当者）は、クラウドサービスの情報セキュリティ対策を実施するために必要となる文書として、クラウドサービスの運用開始前までに以下の全ての実施手順を整備する。

(ｱ) クラウドサービスで利用するサービスごとの情報セキュリティ水準の維持に関する手順

(ｲ) クラウドサービスを利用した情報システムの運用・監視中における情報セキュリティインシデントを認知した際の対処手順

(ｳ) 利用するクラウドサービスが停止又は利用できなくなった際の復旧手順

【 基本対策事項 】

＜4.2.2(3)(c)(ｱ)関連＞

4.2.2(3)-1　クラウドサービス管理者（情報セキュリティ管理担当者）は、以下を全て含むクラウドサービスで利用するサービスごとの情報セキュリティ水準の維持に関する手順を実施手順として整備する。

a)　クラウドサービス利用のための責任分界点を意識したクラウドサービス利用手順

b)　クラウドサービス利用者が行う可能性のある重要操作の手順

＜4.2.2(3)(c)(ｲ)関連＞

4.2.2(3)-2　クラウドサービス管理者（情報セキュリティ管理担当者）は、以下を全て含む情報システムの運用・監視中に発生したクラウドサービスの利用に係る情報セキュリティインシデントを認知した際の対処手順を整備する。

a)　クラウドサービス提供者との責任分界点を意識した責任範囲の整理

b)　利用するクラウドサービスのサービスごとの情報セキュリティインシデント対処に関する事項

c)　利用するクラウドサービスに係る情報セキュリティインシデント発生時の連絡体制

＜4.2.2(3)(c)(ｳ)関連＞

4.2.2(3)-3　クラウドサービス管理者（情報セキュリティ管理担当者）は、以下を全て含む利用するクラウドサービスが停止又は利用できなくなった際の復旧手順を実施手順として整備する。

a)　要安定情報をクラウドサービスで取り扱う場合の十分な可用性を担保した復旧に係る手順

遵守事項

(4)　クラウドサービスを利用した情報システムの運用・保守時の対策

(a)　クラウドサービス管理者（情報セキュリティ管理担当者）は、(1)(b)で定めた運用手順書を踏まえて、クラウドサービスに係る運用・保守を適切に実施する。また、運用・保守時に実施状況を定期的に確認・記録する。

(b)　クラウドサービス管理者（情報セキュリティ管理担当者）は、クラウドサービスの運用・保守時に情報セキュリティ対策を実施するために必要となる項目等で修正又は変更等が発生した場合、情報システム台帳及び関連文書を更新又は修正する。なお、情報システム台帳を更新又は修正した場合は、情報セキュリティ責任者へ報告する。

(c)　クラウドサービス管理者（情報セキュリティ管理担当者）は、クラウドサービスの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により見直しを適時検討し、必要な措置を講じる。

【 基本対策事項 】

＜4.2.2(4)(a)関連＞

4.2.2(4)-1　クラウドサービス管理者（情報セキュリティ管理担当者）は、以下を全て含むクラウドサービスの利用に関する情報セキュリティ対策を実施する。

a)　クラウドサービス提供者に対する定期的なサービスの提供状態の確認

b)　クラウドサービス上で利用する IT 資産の適切な管理

4.2.2(4)-2　クラウドサービス管理者（情報セキュリティ管理担当者）は、以下を全て含むクラウドサービスで利用するアカウント管理、アクセス制御、管理権限に関する情報セキュリティ対策を実施する。

a)　管理者権限をクラウドサービス利用者へ割り当てる場合のアクセス管理と操作の確実な記録

b)　クラウドサービス利用者に割り当てたアクセス権限に対する定期的な確認による見直し

4.2.2(4)-3　クラウドサービス管理者（情報セキュリティ管理担当者）は、以下を全て含むクラウドサービスで利用する機能に対する脆弱性対策を実施する。

a)　クラウドサービスの機能に対する脆弱性対策の実施

4.2.2(4)-4　クラウドサービス管理者（情報セキュリティ管理担当者）は、以下を全て含むクラウドサービスを運用する際の設定変更に関する情報セキュリティ対策を実施する。

a)　クラウドサービスのリソース設定を変更するユーティリティプログラムを使用する場合の利用者の制限

b)　クラウドサービスの設定を変更する場合の設定の誤りを防止するための対策

c)　クラウドサービス利用者が行う可能性のある重要操作に対する監督者の指導の下での実施

4.2.2(4)-5　クラウドサービス管理者（情報セキュリティ管理担当者）は、以下を全て含むクラウドサービスを運用する際の監視に関する対策を実施する。

a)　利用するクラウドサービスの不正利用の監視

b)　クラウドサービスで利用しているデータ容量、性能等の監視

4.2.2(4)-6　クラウドサービス管理者（情報セキュリティ管理担当者）は、以下を全て含むクラウドサービスを運用する際の可用性に関する情報セキュリティ対策を実施する。

a)　不測の事態に対してサービスの復旧を行うために必要なバックアップの確実な実施

b)　要安定情報をクラウドサービスで取り扱う場合の十分な可用性の担保、復旧に係る定期的な訓練の実施

c) クラウドサービス提供者からの仕様内容の変更通知に関する内容確認と復旧手順の確認

4.2.2(4)-7 クラウドサービス管理者（情報セキュリティ管理担当者）は、以下を全て含むクラウドサービスで利用する暗号鍵に関する情報セキュリティ対策を実施する。

a) クラウドサービスで利用する暗号鍵に関する生成から廃棄に至るまでのライフサイクルにおける適切な管理の実施

遵守事項

(5) クラウドサービスを利用した情報システムの更改・廃棄時の対策

(a) クラウドサービス管理者（情報セキュリティ管理担当者）は、(1)(c)で定めた運用手順書を踏まえて、更改・廃棄時の必要な措置を講じる。また、クラウドサービスの利用終了時に実施状況を確認・記録する。

【 基本対策事項 】

＜4.2.2(5)(a)関連＞

4.2.2(5)-1 クラウドサービス管理者（情報セキュリティ管理担当者）は、以下を全て含むクラウドサービスの利用終了に関する情報セキュリティ対策を実施する。

a) クラウドサービスで取り扱った情報の廃棄

b) 暗号化消去が行えない場合の基盤となる物理機器の廃棄

c) 作成されたクラウドサービス利用者アカウントの削除

d) 利用したクラウドサービスにおける管理者アカウントの削除又は返却

e) クラウドサービス利用者アカウント以外の特殊なアカウントの削除と関連情報の廃棄

4.2.3 クラウドサービスの選定・利用（要機密情報を取り扱わない場合）

目的・趣旨

要機密情報を取り扱わない場合であって、クラウドサービス提供者における高いレベルの情報管理を要求する必要がない場合においても、種々の情報を支払基金から送信していることを十分認識し、リスクを十分踏まえた上で利用の可否を判断して利用することが求められる。一方、要機密情報を取り扱う場合と同等のセキュリティ対策を求めることはクラウドサービスの利用推進を妨げるものであるため、要機密情報を取り扱わない前提でクラウドサービスを利用する場合は、本款で定めた遵守事項に従って情報セキュリティ対策を適切に講じることが求められる。

遵守事項

⑴　要機密情報を取り扱わない場合のクラウドサービスの利用に係る運用手順書の整備

⒜　情報セキュリティ責任者は、以下を含む要機密情報を取り扱わない場合のクラウドサービスの利用に関する運用手順書を整備する。

(ｱ)　クラウドサービスを利用可能な業務の範囲

(ｲ)　クラウドサービスの利用申請の許可権限者（情報セキュリティ管理者）と利用手続

(ｳ)　クラウドサービス管理者（情報セキュリティ管理担当者）の指名とクラウドサービスの利用状況の管理

(ｴ)　クラウドサービスの利用の運用手順

【 基本対策事項 】

＜4.2.3(1)(a)(ｲ)関連＞

4.2.3(1)-1　情報セキュリティ責任者は、支払基金において要機密情報を取り扱わない前提でクラウドサービスを業務に利用する場合は、以下を例に利用手続を定める。

a)　利用申請の許可権限者（情報セキュリティ管理者）

b)　利用申請時の申請内容

・クラウドサービスの名称（必要に応じて機能名までを含む）
・クラウドサービス提供者の名称
・利用目的（業務内容）
・取り扱う情報の格付
・利用期間
・利用申請者（情報セキュリティ管理担当者の所属・氏名）
・利用者の範囲（支払基金内に限る、部内に限る など）
・選定時の確認結果

＜4.2.3(1)(a)(ｳ)関連＞

4.2.3(1)-2　利用申請の許可権限者（情報セキュリティ管理者）は、支払基金における要機密情報を取り扱わない場合のクラウドサービスの利用状況について、以下を例に管理する。

a)　利用申請の許可権限者（情報セキュリティ管理者）は、申請ごとにクラウドサービス管理者（情報セキュリティ管理担当者）を指名する。

b)　利用承認したクラウドサービスは、その内容を遅滞なく記録するよう運用ルールを定め、常に最新のクラウドサービスの利用状況を把握できるようにする。記録する際は、以下を例とする項目を記録し支払基金内で共有する。

・クラウドサービスの名称（必要に応じて機能名までを含む）
・クラウドサービス提供者の名称

・利用目的（業務内容）
・取り扱う情報の格付
・利用期間
・利用申請者（情報セキュリティ管理担当者の所属・氏名）
・利用者の範囲（支払基金内に限る、部内に限る など)。
・クラウドサービス管理者（情報セキュリティ管理担当者の所属・氏名）

＜4.2.3(1)(a)(ｴ)関連＞

4.2.3(1)-3　情報セキュリティ責任者は、支払基金において要機密情報を取り扱わない前提でクラウドサービスを業務に利用する場合は、以下を全て含む運用手順定める。

a)　サービス利用中の安全管理に係る運用手順
・適切な主体認証、アクセス制御の管理の実施
・サービス機能の設定（例えば情報の公開範囲）に関する定期的な内容確認
・情報の滅失、破壊等に備えたバックアップの取得
・利用者への定期的な注意喚起（禁止されている要機密情報の取扱いの有無の確認等）

b)　情報セキュリティインシデント発生時の連絡体制

遵守事項

(2)　要機密情報を取り扱わない場合のクラウドサービスの利用における対策の実施

(a)　役職員等関係者は、要機密情報を取り扱わないことを前提としたクラウドサービスを利用する場合、利用するサービスの定型約款、その他の提供条件等から、利用に当たってのリスクが許容できることを確認した上で利用申請の許可権限者へ要機密情報を取り扱わない場合のクラウドサービスの利用を申請する。

(b)　利用申請の許可権限者（情報セキュリティ管理者）は、役職員等関係者による利用するサービスの定型約款、その他の提供条件等から、利用に当たってのリスクが許容できることの確認結果を踏まえて、クラウドサービスの利用申請を審査し、利用の可否を決定する。

(c)　利用申請の許可権限者（情報セキュリティ管理者）は、要機密情報を取り扱わないクラウドサービスの利用申請を承認した場合は、クラウドサービス管理者（情報セキュリティ管理担当者）を指名し、承認したクラウドサービスを記録する。

(d)　クラウドサービス管理者（情報セキュリティ管理担当者）は、要機密情報を取り扱わないクラウドサービスを安全に利用するための適切な措置を講じる。

【 基本対策事項 】

＜4.2.3⑵⑷関連＞

4.2.3⑵-1　クラウドサービス管理者（情報セキュリティ管理担当者）は、要機密情報を取り扱わないクラウドサービスの利用において以下を全て含む、適切な措置を講じる。

a)　要機密情報を取り扱わないクラウドサービスの利用に係る安全管理

b)　要機密情報を取り扱わないクラウドサービスで情報セキュリティインシデントが発生した際の連絡体制の整備

4.3　機器等の調達

4.3.1　機器等の調達

目的・趣旨

調達する機器等において、必要なセキュリティ機能が装備されていない、当該機器等の製造過程で不正な変更が加えられている、調達後に情報セキュリティ対策が継続的に行えないといった場合は、情報システムで取り扱う情報の機密性、完全性及び可用性が損なわれるおそれがある。また、不正な変更が加えられている機器等が組み込まれた情報システムにおいては、当該機器等が当該システムへの不正侵入の足がかりとされ、要機密情報の窃取や破壊、情報システムの機能停止等の原因となるおそれがある。

これらの課題に対応するため、対策基準に基づいた機器等の調達を行うべく、機器等の選定基準及び納入時の確認・検査手続を整備する必要がある。

遵守事項

⑴　機器等の調達に係る対策

⒜　情報セキュリティ責任者は、機器等の選定基準として以下を例とする確認を行う。必要に応じて、選定基準の一つとして、機器等の開発等のライフサイクルで不正な変更が加えられない管理がなされ、その管理を支払基金が確認できることを加える。

(ｱ)　開発工程において信頼できる品質保証体制が確立されていること

(ｲ)　設置時や保守時のサポート体制が確立されていること

(ｳ)　利用マニュアル・ガイダンスが適切に整備されていること

(ｴ)　脆弱性検査等のテストの実施が確認できること

(ｵ)　ISO 等の国際標準に基づく第三者認証が活用可能な場合は活用すること

⒝　情報セキュリティ責任者は、情報セキュリティ対策の視点を加味して、機器等の納入時の確認・検査に関する対策を講じる。

【 基本対策事項 】

＜4.3.1(1)(a)関連＞

4.3.1(1)-1　情報セキュリティ責任者は、機器等の選定基準に、サプライチェーン・リスクを低減するための要件として、以下を全て含める。

a)　調達した機器等に不正な変更が見付かったときに、必要に応じて追跡調査や立入検査等、支払基金と調達先が連携して原因を調査・排除できる体制を整備している。

4.3.1(1)-2　情報セキュリティ責任者は、機器等の選定基準に、機器等に必要なセキュリティ機能が適切に実装されていることを含める。

4.3.1(1)-3　情報セキュリティ責任者は、調達する機器等において、設計書の検査によるセキュリティ機能の適切な実装の確認、開発環境の管理体制の検査、脆弱性テスト等、第三者による情報セキュリティ機能の客観的な評価を必要とする場合には、ISO/IEC 15408 に基づく認証を取得しているか否かを、調達時の評価項目とすることを機器等の選定基準として定める。

4.3.1(1)-4　情報セキュリティ責任者は、ソフトウェア及びサイバーセキュリティリスクの高い機器等の調達における透明性の確認を必要とする場合には、SBOM（Software Bill of Materials：ソフトウェア部品表）の作成、提供等を、調達時の評価項目とすることを機器等の選定基準として定める。

＜4.3.1(1)(b)関連＞

4.3.1(1)-5　情報セキュリティ責任者は、機器等の納入時の確認・検査手続には以下を全て含む事項を確認する。

a)　調達時に指定したセキュリティ要件の実装状況

・調達時に指定したセキュリティ要件（機器等に最新のセキュリティパッチが適用されているか否か、不正プログラム対策ソフトウェア等が最新の脆弱性に対応しているか否か等にも留意）に関する試験実施手順及び試験結果を納品時に報告させて確認

・セキュリティ要件として調達時に指定した機能が正しく動作することを受入れテストにより確認

b)　機器等に不正プログラムが混入していないこと

・内部監査等により不正な変更が加えられていないことを確認した結果を納品時に報告させて確認

第 5 部 情報システムのライフサイクル

5.1 情報システムの分類

5.1.1 情報システムの分類基準等の整備

目的・趣旨

支払基金が所管する情報システムが多様化するなか、支払基金で所管する情報システムの情報セキュリティインシデントの発生リスクを低減させるためには、多様な情報セキュリティ対策からその情報システムに求められる対策を過不足無く適切に選択する必要がある。

そのためには、情報セキュリティを取り巻く様々な脅威動向や情報システムにインシデントが発生した際の業務影響度、社会的影響、取り扱う情報、支払基金の組織特性等を踏まえて、高度な情報セキュリティ対策が求められる情報システムを判別するための分類基準を定め、分類基準に応じた情報セキュリティ対策を規定することで、支払基金が所管する情報システムの分類に応じた適切な対策が講じられるようにすることが重要である。

遵守事項

⑴ 情報システムにおける分類

(a) 情報セキュリティ責任者は、情報システムの情報セキュリティインシデント発生時の業務影響度等を踏まえ、高度な情報セキュリティ対策が要求される情報システムを判別するための基準である情報システムの分類基準を整備する。

【 基本対策事項 】

＜5.1.1⑴(a)関連＞

5.1.1(1)-1 情報セキュリティ責任者は、情報システムに求める分類基準を以下のとおり定める。情報セキュリティ管理者は、分類基準に従い情報システムの重要度を決定し、対策を講じる。

情報システムの重要度	分類基準	基本セキュリティ対策	追加セキュリティ対策
高	・外部接続システムのうち、特定個人情報・個人情報を扱うシステム ・外部接続システムのうち、特定個人情報・個人情報以外の重要情報を取扱うシステム	必須	必須
中	・外部接続していないが要保護情報を取	必須	必要に応じて

	扱うシステム		実施
低	・情報システムの重要度「高」・「中」以外のシステム	必須	必要に応じて実施

※　外部接続システムとは、インターネット接続のあるシステム又は閉域網のシステムのうち、外部との境界にあるシステムをさす。

遵守事項

⑵　情報システムの分類基準に基づいた情報セキュリティ対策

(a)　情報セキュリティ責任者は、情報システムに求める分類基準に応じた情報システムのセキュリティ要件及び情報システムの構成要素ごとの情報セキュリティ対策の具体的な対策事項を整備する。

【 基本対策事項 】

＜5.1.1⑵(a)関連＞

5.1.1⑵-1　情報セキュリティ責任者は、取扱う情報の特性や国内外の情報セキュリティに関連する動向等を踏まえ、セキュリティベースラインとして全ての情報システムに対し対策を求める「基本セキュリティ対策」と、それに加え高度な情報セキュリティ対策を要求する情報システムに対し追加で対策を求める「追加セキュリティ対策」を定める。

遵守事項

⑶　情報システムの分類基準に基づいた分類の実施

(a)　情報セキュリティ責任者は、情報システムの分類基準に基づいた情報システムの分類を情報セキュリティ管理者に実施させ、実施した結果を報告させる。情報セキュリティ管理者から報告を受けた情報システムの分類結果については、情報セキュリティインシデント発生時の業務影響度や脅威動向等を踏まえて、上位又は下位の情報システムの分類の適用が望ましい場合には修正の指示を行う。

【 基本対策事項 】

＜5.1.1⑶(a)関連＞

5.1.1⑶-1　情報セキュリティ責任者は、以下の全ての場合、情報セキュリティ管理者に対して分類基準に基づいた情報システムの分類を行わせる。

a)　情報システムの構築又は更改が発生した場合

b)　情報システムで取り扱う情報の格付等に変更が発生した場合

c)　分類の再実施を指示する場合

5.1.1⑶-2　情報セキュリティ責任者は、支払基金で所管する情報システムの分類結果を

確認し、以下の例に該当する場合、報告を受けた情報システムの分類結果の上位への修正指示の要否を検討する。

a) 業務特性やシステム特性、取り扱う情報等を踏まえると上位の情報システムの分類の適用が望ましいと判断される場合

b) 類似する支払基金の情報システムで上位の情報システムの分類が適用されていた場合

遵守事項

⑷ 情報システムの分類基準と具体的な情報セキュリティ対策の見直し

⑷ 情報セキュリティ責任者は、情報システムの分類基準と分類基準に応じた具体的な情報セキュリティ対策について定期的な確認による見直しをする。

⑷ 情報セキュリティ責任者は、全ての情報システムが分類基準に基づいて適切に分類が行われていることを定期的に確認する。

【 基本対策事項 】

＜5.1.1⑷⑹関連＞

5.1.1⑷-1 情報セキュリティ責任者は、以下の全ての場合に分類基準に基づいた情報システムの分類が行われていることを確認する。

a) 情報システムの構築又は更改を把握した場合

b) 対策推進計画の各種施策や情報セキュリティ監査及び自己点検等の結果を踏まえ、定期評価や評価の再実施が必要と判断した場合

5.2 情報システムのライフサイクルの各段階における対策

5.2.1 情報システムの企画・要件定義

目的・趣旨

情報システムのライフサイクル全般を通じて、情報セキュリティを適切に維持するためには、情報システムの企画段階において、適切にセキュリティ要件を定義する必要がある。

セキュリティ要件の曖昧さや過不足は、過剰な情報セキュリティ対策に伴うコスト増加のおそれ、要件解釈のばらつきによる提案内容の差異からの不公平な競争入札、設計・開発工程での手戻り、運用開始後の情報セキュリティインシデントの発生といった不利益が生じる可能性に繋がる。

そのため、情報システムが対象とする業務、業務において取り扱う情報、情報を取り扱う者、情報を処理するために用いる環境・手段等を考慮した上で、当該情報システムにおいて想定される脅威への対策を検討し、必要十分なセキュリティ要件を仕様に適切に組み込むことが重要となる。

加えて、構築する情報システムへの脆弱性の混入を防止するための対策も、構築前の企画段階で考慮することが重要となる。

また、情報システムの構築、運用・保守を業務委託する場合については、4.1「業務委託」、クラウドサービスを利用して情報システムを構築する場合は 4.2「クラウドサービス」、情報システムで利用する機器等を調達する場合は 4.3「機器等の調達」、共通利用型システムを利用して情報システムを構築する場合は 5.4「共通利用型システム」を参照すること。

遵守事項

⑴ 実施体制の確保

(a) 情報セキュリティ管理者は、情報システムのライフサイクル全般にわたって情報セキュリティの維持が可能な体制の確保を、情報セキュリティ責任者に求める。

(b) 情報セキュリティ責任者は、前項で求められる体制の確保に際し、最高情報セキュリティ責任者の協力を得ることが必要な場合は、当該体制の全部又は一部の整備を求める。

遵守事項

⑵ 情報システムの分類基準に基づいた分類の実施

(a) 情報セキュリティ管理者は、情報システムを新規に構築し、又は更改する際には、情報システムの分類基準に基づいて情報システムの分類を行い、セキュリティ担当課に報告する。

遵守事項

⑶ 情報システムのセキュリティ要件の策定

(a) 情報セキュリティ管理者は、情報システムを構築する目的、対象とする業務等の業務要件及び当該情報システムで取り扱われる情報の格付等を勘案し情報システムの分類に基づき、情報システムに求める分類基準に応じた具体的な対策事項を踏まえて、以下の全ての事項を含む情報システムのセキュリティ要件を策定する。

(ｱ) 情報システムに組み込む主体認証、アクセス制御、権限管理、ログ管理、暗号化機能等のセキュリティ機能要件

(ｲ) 情報システム運用時の監視等の運用管理機能要件（監視するデータが暗号化されている場合は、必要に応じて復号する）

(ｳ) 情報システムに関連する脆弱性及び不正プログラムについての対策要件

(ｴ) 情報システムの可用性に関する対策要件

(ｵ) 情報システムのネットワーク構成に関する要件

(b) 情報セキュリティ管理者は、インターネット回線と接続する情報システムを構築する場合は、接続するインターネット回線を定めた上で、標的型攻撃を始めとするイン

ターネットからの様々なサイバー攻撃による情報の漏えい、改ざん等のリスクを低減するための多重防御のためのセキュリティ要件を策定する。

(c) 情報セキュリティ管理者は、機器等を調達する場合には、「IT 製品の調達におけるセキュリティ要件リスト」を参照し、利用環境における脅威を分析した上で、当該機器等に存在する情報セキュリティ上の脅威に対抗するためのセキュリティ要件を策定する。

(d) 情報セキュリティ管理者は、構築する情報システムが取り扱う情報や情報システムを利用して行う業務の内容等を踏まえ高度な情報セキュリティ対策を要求する情報システムについては、情報システムの分類に応じて策定したセキュリティ要件について、最高情報セキュリティアドバイザー等へ助言を求め、業務の特性や情報システムの特性を踏まえて、上位の情報セキュリティ対策をセキュリティ要件として盛り込む必要が無いかを確認する。

【 基本対策事項 】

＜5.2.1(3)(a)関連＞

5.2.1(3)-1 情報セキュリティ管理者は、「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」を活用し、情報システムが提供する業務及び取り扱う情報、利用環境等を考慮した上で、脅威に対抗するために必要となるセキュリティ要件を適切に決定する。

5.2.1(3)-2 情報セキュリティ管理者は、開発する情報システムが運用される際に想定される脅威の分析結果並びに当該情報システムにおいて取り扱う情報の格付及び取扱制限に応じて、セキュリティ要件を適切に策定し、調達仕様書等に明記する。

＜5.2.1(3)(a)(ｱ)関連＞

5.2.1(3)-3 情報セキュリティ管理者は、開発する情報システムが対抗すべき脅威について、適切なセキュリティ要件が策定されていることを第三者が客観的に確認する必要がある場合には、セキュリティ設計仕様書（ST：Security Target）を作成し、ST 確認を受ける。

＜5.2.1(3)(a)(ｲ)関連＞

5.2.1(3)-4 情報セキュリティ管理者は、情報システム運用時のセキュリティ監視等の運用管理機能要件を明確化し、情報システム運用時に情報セキュリティ確保のために必要となる管理機能や監視のために必要な機能を調達仕様書に明記する。

＜5.2.1(3)(a)(ｳ)関連＞

5.2.1(3)-5 情報セキュリティ管理者は、開発する情報システムに関連する脆弱性への対策が実施されるよう、以下を全て含む対策を調達仕様書等に明記する。

a) 既知の脆弱性が存在するソフトウェアや機能モジュールを情報システムの構成要素としない。

b) 開発時に情報システムに脆弱性が混入されることを防ぐためのセキュリティ実装方針。

c) セキュリティ侵害につながる脆弱性が情報システムに存在することが発覚した場合に修正が施される。

d) ソフトウェアのサポート期間又はサポート打ち切り計画に関する支払基金への情報提供。

5.2.1(3)-6 情報セキュリティ管理者は、開発する情報システムに支払基金の意図しない不正なプログラム等が組み込まれないよう、以下を全て含む対策を実施する。

a) 情報システムで利用する機器等を調達する場合は、支払基金の意図しない不正なプログラム等が組み込まれていないことを確認すること。

b)アプリケーション・コンテンツの開発時に支払基金の意図しない不正なプログラム等が混入されることを防ぐための対策を講じること。

c)情報システムの構築を委託する場合は、委託先において支払基金の意図しない変更が加えられないための管理体制を求めること。

＜5.2.1(3)(a)(ｴ)関連＞

5.2.1(3)-7 情報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を構築する場合は、許容される停止時間に応じた以下を全て含むセキュリティ要件について、情報システムを構成する要素ごとに策定し調達仕様書等に明記する。

a) 端末、サーバ装置及び通信回線装置等の冗長化に関する要件

b) 端末、サーバ装置及び通信回線装置並びに取り扱われる情報に関するバックアップの要件

c) 情報システムを中断することのできる時間を含めた復旧に関する要件

＜5.2.1(3)(a)(ｵ)関連＞

5.2.1(3)-8 情報セキュリティ管理者は、開発する情報システムのネットワーク構成に関する要件について、以下を全て含む要件を調達仕様書等に明記する。

a) インターネットやインターネットに接点を有する情報システム（クラウドサービスを含む。）から分離することの要否の判断とインターネットから分離するとした場合の要件

b) 端末、サーバ装置及び通信回線装置上で利用するソフトウェアを実行するために必要な通信要件

c) インターネット上のクラウドサービス等のサービスを利用する場合の通信経路全般のネットワーク構成

d) 支払基金外通信回線を経由して機器等に対してリモートメンテナンスすることの要否の判断とリモートメンテナンスすることとした場合の要件

＜5.2.1(3)(c)関連＞

5.2.1(3)-9 情報セキュリティ管理者は、構築する情報システムの構成要素のうち、製品と

して調達する機器等について、当該機器等に存在するセキュリティ上の脅威へ対抗するためのセキュリティ要件を策定するために、以下を全て含む事項を実施する。

a) 「IT 製品の調達におけるセキュリティ要件リスト」を参照し、リストに掲載されている製品分野の「セキュリティ上の脅威」が自身の運用環境において該当する場合には、「国際標準に基づくセキュリティ要件」と同等以上のセキュリティ要件を調達時のセキュリティ要件とする。ただし、「IT 製品の調達におけるセキュリティ要件リスト」の「セキュリティ上の脅威」に挙げられていない脅威にも対抗する必要がある場合には、必要なセキュリティ要件を策定する。

b) 「IT 製品の調達におけるセキュリティ要件リスト」に掲載されていない製品分野においては、調達する機器等の利用環境において対抗すべき脅威を分析し、必要なセキュリティ要件を策定する。

5.2.2 情報システムの調達・構築

目的・趣旨

情報システムを調達・構築する際には、策定したセキュリティ要件に基づく情報セキュリティ対策を適切に実施するために、選定基準に適合した機器等の調達や、情報システムの開発工程での情報セキュリティ対策の実施が求められる。

また、機器等の納入時又は情報システムの受入れ時には、整備された検査手続に従い、当該情報システムが運用される際に取り扱う情報を保護するためのセキュリティ機能及びその管理機能が、適切に情報システムに組み込まれていることを検査することが必要となる。

なお、情報システムの構築を委託する場合は 4.1「業務委託」、クラウドサービスを利用して構築する場合は 4.2「クラウドサービス」、情報システムで使用する機器等を調達する場合は 4.3「機器等の調達」を参照し遵守する必要がある。

遵守事項

(1) 情報システムの構築時の対策

(a) 情報セキュリティ管理者は、情報システムの構築において、情報セキュリティの観点から必要な措置を講じる。

(b) 情報セキュリティ管理者は、構築した情報システムを運用保守段階へ移行するに当たり、移行手順及び移行環境に関して、情報セキュリティの観点から必要な措置を講じる。

(c) 情報セキュリティ管理者は、情報システムを新規に構築し、又は更改する際には、情報システム台帳のセキュリティ要件に係る内容を記録又は記載し、当該内容についてセキュリティ担当課に報告する。

(d) 情報セキュリティ管理者は、所管する情報システムの情報セキュリティ対策を実施するために必要となる文書として、以下を全て含む情報システム関連文書を整備する。
(ｱ) 情報システムを構成するサーバ装置及び端末関連情報
(ｲ) 情報システムを構成する通信回線及び通信回線装置関連情報
(e) 情報セキュリティ管理者は、所管する情報システムの情報セキュリティ対策を実施するために必要となる文書として、以下を全て含む実施手順を整備する。
(ｱ) 情報システム構成要素ごとの情報セキュリティ水準の維持に関する手順
(ｲ) 情報セキュリティインシデントを認知した際の対処手順
(ｳ) 情報システムが停止した際の復旧手順

【 基本対策事項 】

＜5.2.2(1)(a)関連＞

5.2.2(1)-1 情報セキュリティ管理者は、情報システムの構築において以下を含む情報セキュリティ対策を行う。

a) 情報システム構築の工程で扱う要保護情報への不正アクセス、滅失、き損等に対処するために開発環境を整備する。

b) セキュリティ要件が適切に実装されるようにセキュリティ機能を設計する。

c) 情報システムで使用する機器やソフトウェア等においては、設定の誤りを防止するため、当該提供者が提示している推奨設定や業界標準、ベストプラクティス等を参照し、情報システムの各種設定を行う。

d) 情報システムへの脆弱性の混入を防ぐために定めたセキュリティ実装方針に従う。

e) セキュリティ機能が適切に実装されていること及びセキュリティ実装方針に従った実装が行われていることを確認するために、設計レビューやソースコードレビュー等を実施する。

f) 脆弱性検査を含む情報セキュリティの観点での試験を実施する。その際は、脆弱性検査ツールや点検基準を用いた第三者による検査の実施を検討し、必要な措置を講じる。

＜5.2.2(1)(b)関連＞

5.2.2(1)-2 情報セキュリティ管理者は、情報システムの運用保守段階へ移行するに当たり、以下を全て含む情報セキュリティ対策を行う。

a) 情報セキュリティに関わる運用保守体制の整備

b) 運用保守要員へのセキュリティ機能の利用方法等に関わる教育の実施

c) 情報セキュリティインシデント又はその可能性を認知した際の対処方法の確立

＜5.2.2(1)(d)(ｱ)関連＞

5.2.2(1)-3　情報セキュリティ管理者は、所管する情報システムを構成するサーバ装置及び端末に関連する情報として、以下を全て含む文書を整備する。

a)　サーバ装置及び端末を管理する役職員等関係者及び利用者を特定する情報

b)　サーバ装置及び端末の機種並びに利用しているソフトウェアの種類、名称及びバージョン、サポート体制等

c)　サーバ装置及び端末で利用するソフトウェアを動作させるために用いられる他のソフトウェアであって、以下を全て含むものの種類、名称及びバージョン、入手先、サポート体制等

・動的リンクライブラリ等、ソフトウェア実行時に読み込まれて使用されるもの

・フレームワーク等、ソフトウェアを実行するための実行環境となるもの

・プラグイン等、ソフトウェアの機能を拡張するもの

・静的リンクライブラリ等、支払基金がソフトウェアを開発する際に当該ソフトウェアに組み込まれるもの

・インストーラー作成ソフトウェア等、支払基金がソフトウェアを開発する際に開発を支援するために使用するもの

d)　サーバ装置及び端末の調達仕様書又は設計書

5.2.2(1)-4　情報セキュリティ管理者は、前項b)及びc)の情報を収集するため、自動でソフトウェアの種類やバージョン等を管理する機能を有するIT資産管理ソフトウェアを導入するなどにより、これら情報を効率的に収集する手法を決定する。

＜5.2.2(1)(d)(ｲ)関連＞

5.2.2(1)-5　情報セキュリティ管理者は、所管する情報システムを構成する通信回線及び通信回線装置関連情報として、以下を全て含む文書を整備する。

a)　通信回線及び通信回線装置を管理する役職員等関係者を特定する情報

b)　通信回線装置の機種並びに利用しているソフトウェアの種類、名称及びバージョン、サポート体制等

c)　通信回線及び通信回線装置の調達仕様書又は設計書

d)　通信回線の構成

e)　通信回線装置におけるアクセス制御の設定

f)　通信回線を利用する機器等の識別コード、サーバ装置及び端末の利用者と当該利用者の識別コードとの対応

g)　通信回線の利用部門

＜5.2.2(1)(e)(ｱ)関連＞

5.2.2(1)-6　情報セキュリティ管理者は、所管する情報システムについて、情報システム構成要素ごとのセキュリティ維持に関する以下を全て含む運用手順を整備する。

a)　サーバ装置及び端末のセキュリティの維持に関する手順

b) 通信回線を介して提供するサービスのセキュリティの維持に関する手順
c) インターネット等の外部ネットワーク経由で利用するサービスのセキュリティの維持に関する手順
d) 通信回線及び通信回線装置のセキュリティの維持に関する手順
e) 端末、サーバ装置、通信回線装置等において利用するソフトウェアのセキュリティの維持に関する手順

遵守事項

⑵ 納品検査時の対策

⑻ 情報セキュリティ管理者は、機器等の納入時又は情報システムの受入れ時の確認・検査において、調達仕様書等定められた検査手続に従い、情報セキュリティ対策に係る要件が満たされていることを確認する。

⑼ 情報セキュリティ管理者は、情報システムが構築段階から運用保守段階へ移行する際に、当該情報システムの開発事業者から運用保守事業者へ引継がれる項目に、情報セキュリティ対策に必要な内容が含まれていることを確認する。

【基本対策事項】

＜5.2.2⑵⑻関連＞

5.2.2⑵-1 情報セキュリティ管理者は、情報システムの受入れ時の確認・検査を行う場合は、以下を全て含む内容を確認する。

a) 情報システムの構築時に使用し、運用時に不要となる識別コードが削除されていること。
b) 機器等において推測可能な初期値として設定されている主体認証情報等が変更されていること。
c) 機器等において公開された脆弱性について対策を実施していること。
d) 機器等において不要なポートが開放されていない、不要なサービスが起動していない、利用を認めていないソフトウェアが動作していないこと。

5.2.3 情報システムの運用・保守

目的・趣旨

情報システムの運用段階に移るに当たり、企画又は調達・構築時に決定したセキュリティ要件が適切に運用されるように、人的な運用体制を整備し、機器等のパラメータが正しく設定されていることの定期的な確認、運用・保守に係る作業記録の管理等を実施する必要がある。

情報システムにおける情報セキュリティインシデントは一般的に運用時に発生すること

が大半であることから、適宜情報システムの情報セキュリティ対策の実効性を確認するために、情報システムの運用状況を監視することも重要である。

また、情報システムの保守作業においても運用作業と同様に情報セキュリティ対策が適切に実施される必要がある。保守作業を個別に委託する場合等においても、本ポリシーに基づく情報セキュリティ対策について適切に措置を講じることが求められる。なお、情報システムの運用・保守を業務委託する場合は、4.1「業務委託」を参照のこと。

さらに、クラウドサービスを利用して構築された情報システムの運用・保守をする場合は、4.2「クラウドサービス」、共通利用型システムを利用して構築された情報システムを運用・保守する場合は、5.4「共通利用型システム」を参照すること。

遵守事項

⑴　情報システムの運用・保守時の対策

⑷　情報セキュリティ管理者は、情報システムの運用・保守において、情報システムに実装された監視を含むセキュリティ機能を適切に運用する。

⑹　情報セキュリティ管理者は、不正な行為及び意図しない情報システムへのアクセス等の事象が発生した際に追跡できるように、運用・保守に係る作業についての記録を管理し、運用・保守によって機器の構成や設定情報等に変更があった場合は、情報セキュリティ対策が適切であるか確認し、必要に応じて見直す。

⑹　情報セキュリティ管理者は、情報システムの運用・保守において、情報システム台帳及び関連文書の内容に変更が生じた場合、情報システム台帳及び関連文書を更新又は修正する。なお、情報システム台帳を更新又は修正した場合は、セキュリティ担当課へ報告する。

⑹　情報セキュリティ管理者は、情報システムの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により見直しを適時検討し、必要な措置を講じる。

⑹　情報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、危機的事象発生時に適切な対処が行えるよう運用をする。

【 基本対策事項 】

＜5.2.3⑴⑷関連＞

5.2.3⑴-1　情報セキュリティ管理者は、情報システムのセキュリティ監視について、以下の内容を全て含む監視手順を定め、適切に監視運用する。

a)　監視するイベントの種類や重要度

b)　監視体制

c)　監視状況の報告手順や重要度に応じた報告手段

d)　情報セキュリティインシデント又はその可能性を認知した場合の報告手順

e)　監視運用における情報の取扱い（機密性の確保）

5.2.3(1)-2　情報セキュリティ管理者は、情報システムに実装されたセキュリティ機能が適切に運用されていることを確認する。

5.2.3(1)-3　情報セキュリティ管理者は、情報システムにおいて取り扱う情報について、当該情報の格付及び取扱制限が適切に守られていることを確認する。

5.2.3(1)-4　情報セキュリティ管理者は、情報システムで不要となった識別コードや過剰なアクセス権限等の付与がないか適時見直す。

5.2.3(1)-5　情報セキュリティ管理者は、運用中の情報システムにおいて定期的に脆弱性対策の状況を確認する。

5.2.3(1)-6　情報セキュリティ管理者は、運用中の情報システムの脆弱性の存在が明らかになった場合には、情報セキュリティを確保するための措置を講じる。

＜5.2.3(1)(e)関連＞

5.2.3(1)-7　情報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、以下を全て含む運用をする。

a)　情報システムの各構成要素及び取り扱われる情報に関する適切なバックアップの取得及びバックアップ要件の確認による見直し

b)　情報システムの構成や設定の変更等が行われた際及び定期的に、情報システムが停止した際の復旧手順の確認による見直し

5.2.4　情報システムの更改・廃棄

目的・趣旨

情報システムの更改・廃棄において、情報システムに記録されている機密性の高い情報が廃棄又は再利用の過程において外部に漏えいすることを回避する必要がある。

情報システムに機密性の高い情報が記録されている場合や、格付や取扱制限を完全に把握できていない場合等においては、記録されている情報の完全な抹消等の措置を講じることが必要となる。

遵守事項

(1)　情報システムの更改・廃棄時の対策

(a)　情報セキュリティ管理者は、情報システムの更改又は廃棄を行う場合は、当該情報システムに保存されている情報について、当該情報の格付及び取扱制限を考慮した上で、以下を全て含む措置を適切に講じる。

(ｱ)　情報システム更改時の情報の移行作業における情報セキュリティ対策

(ｲ)　情報システム廃棄時の不要な情報の抹消

(ｳ)　設定、構成等の履歴を記録し、保存

遵守事項

⑵　情報システムを構成する機器等の修理・廃棄時の対策

(a)　情報セキュリティ管理者は、業者に機器の修理をさせる際、情報を消去することが難しい場合は、修理を委託する業者に対し、秘密を守ることを契約に定める。

(b)　重要な情報を含む機器について、業者に廃棄させる場合は、情報がいかなる方法によっても容易に復元できない方法で廃棄を行う。

5.2.5　情報システムについての対策の見直し

目的・趣旨

情報セキュリティを取り巻く環境は常時変化しており、新たに発生した脅威等に的確に対応しない場合には、情報セキュリティ水準を維持できなくなる。このため、情報システムの情報セキュリティ対策の定期的な確認による見直しや、外部環境の急激な変化等が発生した場合の適時確認を行うことによる見直しが必要となる。また、運用時における定期的な情報セキュリティ対策の確認による見直しの他、対策推進計画に基づく情報セキュリティ対策の見直しや自己点検及び情報セキュリティ監査等の結果等を踏まえた支払基金内で横断的に改善が必要となる情報セキュリティ対策についての見直しも併せて実施する必要がある。

遵守事項

⑴　情報システムについての対策の見直し

(a)　情報セキュリティ管理者は、対策推進計画に基づき情報システムの情報セキュリティ対策を適切に見直す。

(b)　情報セキュリティ管理者は、支払基金内で横断的に改善が必要となる情報セキュリティ対策の見直しによる改善指示に基づき、情報セキュリティ対策を適切に見直す。また、措置の結果については、情報セキュリティ責任者へ報告する。

5.3　情報システムの運用継続計画

5.3.1　情報システムの運用継続計画の整備・整合的運用の確保

目的・趣旨

業務の停止が国民の皆様に不利益や重大な影響をもたらす可能性のある業務は、地震、火災、感染症、情報セキュリティインシデント等の危機的事象発生時でも継続させる必要があり、支払基金においても、事業継続計画と情報システム運用継続計画を策定し運用する必要がある。

危機的事象発生時に情報システムの運用を継続させるためには、危機的事象発生時にお

ける情報セキュリティに係る対策事項及び実施手順を検討し、定めることが重要となる。

なお、こうした事業継続計画や情報システムの運用継続計画が定める要求事項と、情報セキュリティ関係規程が定める要求事項とで矛盾がないよう、それぞれの間で整合性を確保する必要がある。

遵守事項

⑴ 情報システムの運用継続計画の整備・整合的運用の確保

⒜ 情報セキュリティ責任者は、支払基金において非常時優先業務を支える情報システムの運用継続計画を整備する場合は、危機的事象発生時における情報セキュリティに係る対策事項及び実施手順の整備を検討する。

⒝ 情報セキュリティ責任者は、情報システムの運用継続計画に沿って、危機的事象発生時における情報セキュリティに係る対策事項及び実施手順が運用可能であるかを定期的に確認する。

⒞ 情報セキュリティ責任者は、情報システムの運用継続計画に沿って、危機的事象発生時における情報セキュリティに係る対策事項及び実施手順を定期的に見直す。

【 基本対策事項 】

＜5.3.1⑴⒝関連＞

5.3.1⑴-1 情報セキュリティ責任者は、危機的事象発生時における情報セキュリティに係る対策事項及び実施手順が運用可能であるかを確認するため、以下を例とする訓練の実施を検討する。

a) 情報システム復旧訓練

b) 情報システム切り替え訓練

5.3.1⑴-2 情報セキュリティ責任者は、危機的事象発生時における情報セキュリティに係る実施手順が運用可能であるかを確認するため、以下を例とする訓練の実施を検討する。

a) 手順書確認訓練

b) シナリオ非提示型訓練

＜5.3.1⑴⒞関連＞

5.3.1⑴-3 情報セキュリティ責任者は、以下を全て含む事項を踏まえ、危機的事象発生時における情報セキュリティに係る対策事項及び実施手順を見直す。

a) 危機的事象発生時における情報セキュリティに係る対策事項及び実施手順が運用可能であるかの確認結果

b) 危機的事象発生時の対処結果

c) 情報システムの構成や利用環境、利用方法、取り扱う情報の変化

5.4　共通利用型システム

5.4.1　支払基金が提供する場合における対策

目的・趣旨

共通利用型システムは、支払基金と共通利用型システム利用機関が連携して運用するものであることから、支払基金と共通利用型システム利用機関の間で情報セキュリティ対策の漏れが生じないようその防止を図る必要がある。また、共通利用型システムを利用する一部の情報システムで情報セキュリティインシデントが生じた場合に同システムを利用する他の情報システムにも影響が及ぶ可能性等も踏まえ、支払基金は、共通利用型システム全体としての情報セキュリティマネジメントを適切に実行し、情報セキュリティ水準を適切に確保する必要がある。

このため、支払基金と共通利用型システム利用機関の責任と役割分担を明確化し、情報セキュリティインシデントを認知時にこれに係る対処を連携して迅速・確実に実施できる体制にする必要がある。

遵守事項

⑴　情報セキュリティ対策に関する運用手順の整備

ⓐ　情報セキュリティ管理者は、共通利用型システムを構築する場合は、以下の内容を全て含む情報セキュリティ対策に関する運用手順書を整備し、共通利用型システム利用機関と十分な合意形成を行う。

(ｱ)　支払基金と共通利用型システム利用機関との間の責任分界

(ｲ)　平常時及び非常時の協力・連携体制

(ｳ)　非常時の具体的対応策

【 基本対策事項 】

＜5.4.1⑴ⓐ関連＞

5.4.1⑴-1　情報セキュリティ管理者は、共通利用型システムを構築する場合は、以下の内容を全て含む情報セキュリティ対策に関する運用手順を定める。

a)　支払基金と共通利用型システム利用機関がそれぞれ責任を追うべき情報セキュリティ対策の責任分界点

b)　共通利用型システム及び共通利用型システム利用機関の情報システムにおける情報セキュリティインシデントを認知した場合の、支払基金と共通利用型システム利用機関の間の情報共有や対処の方法を含む対処手順

c)　共通利用型システム利用機関が確保するべき管理体制や整備するべき運用手順書及び実施手順

d)　共通利用型システムが提供するセキュリティ機能を利用する情報システムが

備えるべきセキュリティ要件

e) 共通利用型システムが提供する機器等を利用する役職員等関係者への識別コード及び主体認証情報の付与や管理に関する手順並びにアクセスの権限の設定に関する手順

遵守事項

⑵ 情報システム台帳及び情報システム関連文書の整備

(a) 情報セキュリティ責任者は、遵守事項 2.1.2(1)(a)で整備する共通利用型システムに関する情報システム台帳について、共通利用型システム利用機関に関係するセキュリティ要件に係る事項を含めて整備する。

(b) 情報セキュリティ管理者は、遵守事項 5.2.2(1)(d)で整備する共通利用型システムに関する情報システム関連文書について、共通利用型システム利用機関に関係する情報を含めて整備する。

【 基本対策事項 】

＜5.4.1(2)(a)関連＞

5.4.1(2)-1 情報セキュリティ責任者は、セキュリティ機能を提供する共通利用型システムに関する情報システム台帳について、以下の内容を全て含めて整備する。

a) 当該共通利用型システムが提供するセキュリティ機能を利用する情報システム名

b) 上記共通利用型システム利用機関の名称及び管理部室

c) 上記情報システムの情報セキュリティ管理者の氏名及び連絡先

d) 上記情報システムの利用目的

5.4.1(2)-2 情報セキュリティ責任者は、機器等を提供する共通利用型システムに関する情報システム台帳について、以下の内容を全て含めて整備する。

a) 当該共通利用型システムが提供する機器等を利用する共通利用型システム利用機関

b) 上記共通利用型システム利用機関における当該共通利用型システム利用管理者の氏名及び連絡先

c) 上記共通利用型システム利用機関において当該共通利用型システムで取り扱う情報の格付及び取扱制限に関する事項

＜5.4.1(2)(b)関連＞

5.4.1(2)-3 情報システムの情報セキュリティ管理者は、共通利用型システムに関する情報システム関連文書のうち、共通利用型システム利用機関に提供した機器等に係る情報については、共通利用型システム利用機関の求めに応じ、必要な範囲で提供する。

5.4.2　支払基金が利用する場合における対策

目的・趣旨

支払基金が共通利用型システムを利用する場合、共通利用型システム管理機関が定める運用手順に基づき必要な体制を確保すると共に、責任と役割分担を踏まえ、適切に利用する必要がある。また、情報セキュリティインシデントを認知した際の対処においては両機関の協力が必要となることから、共通利用型システム管理機関が定める運用手順に基づき情報セキュリティインシデントを認知した際の支払基金と共通利用型システム管理機関の責任と役割分担を明確にしておき、対処に必要となる情報は支払基金と共通利用型システム管理機関で共有されている状態にしておくことが重要である。

遵守事項

⑴　支払基金における体制の整備

(a)　情報セキュリティ管理者は、共通利用型システムが提供するセキュリティ機能を利用して情報システムを構築する場合は、共通利用型システム管理機関が定める運用手順に応じた体制の確保を、情報セキュリティ責任者に求める。

(b)　情報セキュリティ責任者は、共通利用型システムが提供する機器等の提供を受けこれを支払基金の役職員等関係者が利用する場合は、共通利用型システムごとに共通利用型システム利用管理者として情報セキュリティ管理者を指名する。

(c)　共通利用型システム利用管理者（情報セキュリティ管理者）は、当該共通利用型システムの利用に際し、共通利用型システム管理機関が定める運用手順に応じた体制の確保を行う。

遵守事項

⑵　支払基金における情報セキュリティ対策

(a)　情報セキュリティ管理者は、共通利用型システムが提供するセキュリティ機能を利用する情報システムを構築する場合は、共通利用型システム管理機関が定める運用手順に基づき、共通利用型システムの情報セキュリティ水準を低下させることのないように、適切にセキュリティ要件を策定し、運用する。

(b)　情報セキュリティ管理者は、共通利用型システム管理機関が定める運用手順に基づき、共通利用型システムに関する情報セキュリティインシデントに適切に対処する。

遵守事項

⑶　支払基金における機器等の管理

(a)　共通利用型システム利用管理者（情報セキュリティ管理者）は、共通利用型システムが提供する機器等の提供を受けてこれを支払基金の役職員等関係者が利用する場合は、

当該共通利用型システムの利用に関する情報セキュリティ対策に係る運用手順書及び実施手順を整備する。

⑹　共通利用型システム利用管理者（情報セキュリティ管理者）は、提供を受けた共通利用型システムの機器等を把握するために必要な文書を整備する。

⑹　共通利用型システム利用管理者（情報セキュリティ管理者）は、共通利用型システム管理機関が情報システム台帳や情報システム関連文書を整備するために必要な情報について、共通利用型システム管理機関に提供するとともに、当該情報に変更が生じた場合は速やかに通知する。

⑹　共通利用型システム利用管理者（情報セキュリティ管理者）は、共通利用型システム管理機関が定める運用手順に基づき、共通利用型システムに関する情報セキュリティインシデントに適切に対処する。

【　基本対策事項　】

＜5.4.2⑶⒜関連＞

5.4.2⑶-1　共通利用型システム利用管理者（情報セキュリティ管理者）は、共通利用型システム管理機関が定める運用手順を踏まえ、以下の内容を全て含む情報セキュリティ対策に係る運用手順書及び実施手順を定める。

a)　共通利用型システムが提供する機能のうち、支払基金で利用を認める機能

b)　共通利用型システムが提供する端末で利用を認めるソフトウェアや接続を認める機器等

c)　共通利用型システムにおける情報セキュリティインシデントの可能性を認知した場合の報告手順及び対処手順

d)　共通利用型システムにおける業務委託サービスやクラウドサービスの利用申請の手順

e)　共通利用型システムを利用する役職員等関係者への識別コードや主体認証情報の付与、アクセス権限の設定等に関する手順。ただし、共通利用型システム管理機関において識別コードや主体認証情報の付与、アクセス権限の設定等を行わない場合は除く。

f)　前各号に掲げるもののほか、支払基金における共通利用型システムの利用に係る情報セキュリティ対策に関する事項

5.4.2⑶-2　共通利用型システム利用管理者（情報セキュリティ管理者）は、支払基金の対策基準や取り扱う情報の格付等を踏まえ、共通利用型システムに追加のセキュリティ対策が必要であると認める場合は、共通利用型システムにおける当該セキュリティ対策の追加的実施その他の措置について協議する。

＜5.4.2⑶⒝関連＞

5.4.2⑶-3　共通利用型システム利用管理者（情報セキュリティ管理者）は、支払基金に設

置している共通利用型システムの機器等を把握するため、以下の内容を全て含む文書を整備する。

a) 当該機器等を管理または利用する役職員等関係者を特定する情報

b) 当該機器等の設置場所並びにその区域のクラス及び当該設置場所の情報セキュリティ管理者

第 6 部　情報システムの構成要素

6.1　端末

6.1.1　端末

目的・趣旨

端末の利用に当たっては、不正プログラム感染や不正侵入を受けるなどの外的要因により、保存されている情報の漏えい等に注意する必要がある。また、役職員等関係者の不適切な利用や過失等の内的要因による不正プログラム感染等の情報セキュリティインシデントが発生するおそれもある。これらのリスクを考慮し役職員等関係者が利用する端末については適切なセキュリティ対策を講じるとともに、利用を認めるソフトウェアや接続を認める機器等を定めておくことが重要である。また、物理的な端末のモバイル利用に当たっては、盗難・紛失等による情報漏えいの可能性も高くなる。これらのことを考慮して、対策を講じる必要がある。

なお、本款の遵守事項のほか、7.1「情報システムのセキュリティ機能」において定める主体認証・アクセス制御・権限管理・ログ管理等の機能面での対策、7.2.1「ソフトウェアに関する脆弱性対策」、7.2.2「不正プログラム対策」、6.4.4「IPv6 通信回線」において定める遵守事項のうち端末に関係するものについても併せて遵守する必要がある。

遵守事項

(1)　端末の導入時の対策

(a)　情報セキュリティ管理者は、要保護情報を取り扱う端末について、端末の盗難、不正な持ち出し、第三者による不正操作、表示用デバイスの盗み見等の物理的な脅威から保護するための対策を講じる。

(b)　情報セキュリティ管理者は、多様なソフトウェアを利用することにより脆弱性が存在する可能性が増大することを防止するため、端末で利用を認めるソフトウェアを定め、それ以外のソフトウェアは利用させない。

(c)　情報セキュリティ管理者は、端末に接続を認める機器等を定め、接続を認めた機器等以外は接続させない。

(d)　情報セキュリティ管理者は、情報システムのセキュリティ要件として策定した内容に従い、端末に対して適切なセキュリティ対策を実施する。

(e)　情報セキュリティ管理者は、端末において利用するソフトウェアに関連する公開された脆弱性について対策を実施する。

【 基本対策事項 】

＜6.1.1(1)(a)関連＞

6.1.1(1)-1　情報セキュリティ管理者は、モバイル端末を除く端末について、原則としてクラス２以上の要管理対策区域に設置する。

6.1.1(1)-2　情報セキュリティ管理者は、端末の盗難及び不正な持ち出しを防止するために、以下を例とする対策を講じる。

a)　モバイル端末を除く端末を、容易に切断できないセキュリティワイヤを用いて固定物又は搬出が困難な物体に固定する。

b)　モバイル端末を保管するための設備（利用者が施錠できる袖机やキャビネット等）を用意する。

6.1.1(1)-3　情報セキュリティ管理者は、第三者による不正操作及び表示用デバイスの盗み見を防止するために、以下を例とする対策を講じる。

a)　一定時間操作が無いと自動的にスクリーンロックするよう設定する。

b)　要管理対策区域外で使用するモバイル端末に対して、盗み見されるおそれがある場合にのぞき見防止フィルタを取り付ける。

＜6.1.1(1)(b)関連＞

6.1.1(1)-4　情報セキュリティ管理者は、以下の全てを考慮した上で、端末で利用を認めるソフトウェアをバージョンも含め定める。なお、特定の業務や端末のみに利用を認めるなどの条件を付す場合は、その旨を含める。

a)　ソフトウェアベンダ等のサポート状況

b)　ソフトウェアと外部との通信の有無及び通信する場合は、プロトコル (バージョンを含む)、使用するポート、暗号化の有無

c)　インストール時に同時にインストールされる他のソフトウェア

d)　その他、ソフトウェアの利用に伴う情報セキュリティリスク

6.1.1(1)-5　情報セキュリティ管理者は、端末に対して、利用を認めるソフトウェア以外のソフトウェアを利用者が自由にインストールできない技術的な措置を講じる。

遵守事項

(2)　端末の運用時の対策

(a)　セキュリティ担当課は、利用を認めるソフトウェアについて、定期的な確認による見直しを行う。

(b)　情報セキュリティ管理者は、所管する範囲の端末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端末を検出等した場合には、改善を図る。

(c)　役職員等関係者は、端末にソフトウェアをダウンロードする場合は、電子署名により当該ソフトウェアの配布元を確認する。

また、ダウンロードに当たっては、セキュリティ担当課に事前に連絡する。

【 基本対策事項 】

＜6.1.1⑵(a)関連＞

6.1.1⑵-1　情報セキュリティ管理者は、利用を認めるソフトウェアの定期的な確認においては、引き続き利用を認めるか否かを判断し、利用を認めない場合は利用を認めるソフトウェアから削除する。

6.1.1⑵-2　情報セキュリティ管理者は、利用を認めるソフトウェア以外のソフトウェアについて役職員等関係者から利用申請があった場合には、当該ソフトウェアの利用を認める否かを判断し、利用を認める場合は利用を認めるソフトウェアに追加する。

遵守事項

⑶　端末の運用終了時の対策

(a)　情報セキュリティ管理担当者は、端末の運用を終了する際に、端末の電磁的記録媒体の全ての情報を抹消する。

6.1.2　要管理対策区域外での端末利用時の対策

目的・趣旨

テレワークの実施等により、役職員等関係者が支払基金の要管理対策区域外で業務を行うことが増え、支払基金支給端末を利用して要管理対策区域外で業務を行う場合は、盗み見や盗難・紛失などのリスクが増える。そのようなリスクに対抗するため、要管理対策区域外で支払基金支給端末を使用する場合は、利用手順や利用の許可手続等を定め、役職員等関係者に守らせる必要がある。また、端末においても盗難、紛失、不正プログラムの感染等による情報窃取を防止するため技術的な措置を講じる必要がある。

さらに、役職員等関係者が支払基金外通信回線を用いて情報システムにリモートアクセスをする場合は、リモートアクセス特有の攻撃等に対抗するためのセキュリティ対策を実施する必要がある。リモートアクセスについては、遵守事項 8.1.3(2)を参照のこと。

なお、支払基金外通信回線を用いて情報システムにリモートアクセス環境を構築する場合は、情報システムへのアクセスについて初回のアクセス要求時のみ制御を行うのではなく、アクセスの都度信用できるアクセスであるかを検証し、信用できない場合には追加の措置を講じるなど、アクセスの要求ごとに、主体等の状況を継続的に認証し認可する仕組みを実現する機能の一部である動的なアクセス制御を実施することも有効である。動的なアクセス制御については、7.3「ゼロトラストアーキテクチャ」を参照すること。

遵守事項

⑴　支払基金支給端末（要管理対策区域外で使用する場合に限る）の導入及び利用に係る手順書の整備

⒜　情報セキュリティ責任者は、役職員等関係者が支払基金支給端末（要管理対策区域外で使用する場合に限る）を用いて要保護情報を取り扱う場合について、これらの端末や利用した通信回線から情報が漏えいするなどのリスクを踏まえた利用手順及び許可手続を「モバイル端末(要管理対策区域外における使用）及び支払基金支給以外の端末の使用に係る手順書」に定める。

⒝　情報セキュリティ責任者は、要機密情報を取り扱う支払基金支給端末（要管理対策区域外で使用する場合に限る）について、盗難、紛失、不正プログラムの感染等により情報窃取されることを防止するための技術的な措置に関する手順を「モバイル端末(要管理対策区域外における使用）及び支払基金支給以外の端末の使用に係る手順書」に整備する。

⒞　情報セキュリティ責任者は、要管理対策区域外において支払基金外通信回線に接続した支払基金支給端末を要管理対策区域で支払基金内通信回線に接続することについての可否を判断した上で、可と判断する場合は、当該端末から支払基金内通信回線を経由して情報システムが不正プログラムに感染するリスクを踏まえた安全管理措置に関する手順及び許可手続を「モバイル端末(要管理対策区域外における使用）及び支払基金支給以外の端末の使用に係る手順書」に定める。

⒟　役職員等関係者は、支払基金支給端末（要管理対策区域外で使用する場合に限る）の利用に当たり、「モバイル端末(要管理対策区域外における使用）及び支払基金支給以外の端末の使用に係る手順書」を確認する。

【 基本対策事項 】

＜6.1.2⑴⒜関連＞

6.1.2⑴-1　情報セキュリティ責任者は、役職員等関係者が支払基金支給端末（要管理対策区域外で使用する場合に限る）を用いて要保護情報を取り扱う場合の利用手順を、以下を例として定める。

a)　端末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

b)　盗み見に対する対策（のぞき見防止フィルタの利用等）

c)　盗難･紛失に対する対策(不要な情報を端末に保存しない､端末の放置の禁止、利用時以外のシャットダウン及びネットワークの切断、モバイル端末を常時携帯する、常に身近に置き目を離さないなど)

d)　利用する場所や時間の限定

e)　端末の盗難・紛失が発生した際の緊急対応手順

6.1.2⑴-2　情報セキュリティ責任者は、役職員等関係者が支払基金支給端末（要管理対策

区域外で使用する場合に限る）を用いて要保護情報を取り扱う場合について、以下を含む許可手続を実施手順として定める。

a） 利用時の許可申請手続

b） 手続内容（利用者、利用期間、主たる利用場所、目的、利用する情報、端末、通信回線への接続形態等）

c） 利用期間満了時の手続

d） 許可権限者（情報セキュリティ管理担当者）による手続内容の記録

＜6.1.2(1)(b)関連＞

6.1.2(1)-3 情報セキュリティ責任者は、要機密情報を取り扱う支払基金支給端末（要管理対策区域外で使用する場合に限る）について、以下を例に、利用者が端末に情報を保存できないようにするための機能又は端末に保存される情報を暗号化するための機能を検討し、要管理対策区域外で使用する物理的な端末に求める技術的な措置について「モバイル端末(要管理対策区域外における使用）及び支払基金支給以外の端末の使用に係る手順書」に整備する。

a） シンクライアント等の仮想デスクトップ技術を活用した、端末に情報を保存させないリモートアクセス環境を構築する。利用者は専用のシンクライアントアプリケーションを利用端末にインストールし、業務用システムへリモートアクセスする。

b） セキュアブラウザ等を活用した、端末に情報を保存させないリモートアクセス環境を構築する。利用者はセキュアブラウザを利用端末にインストールし、業務用システムへリモートアクセスする。

c） ファイル暗号化等のセキュリティ機能を持つアプリケーションを導入する。

d） 端末に、ハードディスク等の電磁的記録媒体全体を自動的に暗号化する機能を設ける。

e） 上記の各号のいずれの機能も使用できない場合は、端末にファイルを暗号化する機能を設ける。

f) ハードディスク等の電磁的記録媒体に保存されている情報を遠隔からの命令等により暗号化消去する機能を設ける。

g） 高度なセキュリティ機能を備えた OS を搭載するスマートフォンやタブレット端末等を使用する。

＜6.1.2(1)(c)関連＞

6.1.2(1)-4 情報セキュリティ責任者は、要管理対策区域外において支払基金外通信回線に接続した支払基金支給端末について、支払基金内通信回線に接続する場合は、当該端末から支払基金内通信回線を経由して情報システムが不正プログラムに感染するリスクを踏まえ、以下を例とする技術的な措置について「モバイル端末(要管理対策区域外における使用）及び支払基金支給以外の端末の使用に係る手

順書」に整備する。

a) 支払基金内通信回線に接続する前に当該端末に対し、不正プログラム対策ソフトウェアを用いてスキャンを行う。

b) 支払基金内通信回線に接続した当該端末が、不正な通信を行っていないか、不要なアプリケーション、サービスやポートを使用していないか確認する。

c) 技術的な措置において不適切な状態を検知した場合は、支払基金内通信回線に接続させない措置を講じることや、支払基金内通信回線から直ちに切断するなどの措置を講じる。

遵守事項

⑵ 支払基金支給端末（要管理対策区域外で使用する場合に限る）の導入及び利用の対策

⑻ 情報セキュリティ管理者は、役職員等関係者が支払基金支給端末（要管理対策区域外で使用する場合に限る）を用いて要機密情報を取り扱う場合は、当該端末について 前条⑹の技術的な措置を講じる。

⑹ 情報セキュリティ管理者は、要管理対策区域外において支払基金外通信回線に接続した支払基金支給端末を支払基金内通信回線に接続させる際、当該端末について前条⑹の技術的な措置を講じる。

【 基本対策事項 】

＜6.1.2⑵⑻⑹関連＞

6.1.2⑵-1 要対策管理区域外においては、第三者による物理的なアクセスのリスクへの対策を実施する。

6.1.3 支払基金支給以外の端末の導入及び利用時の対策

目的・趣旨

支払基金の業務の遂行においては、支払基金から支給された端末を用いてこれを遂行すべきである。しかしながら、出張や外出等や危機的事象発生時の際に、やむを得ず支払基金支給以外の端末を利用して情報処理を行う場合も考えられるが、この際、当該端末の情報セキュリティ水準が対策基準を満たさないおそれがある。このため、支払基金支給以外の端末を業務において利用する可能性がある場合は、利用に当たって求められる情報セキュリティの水準が確保されるかどうかを適切に評価し、業務遂行可能なように、利用できる機能の制限や追加のセキュリティ対策を施した上で、役職員等関係者に対して支払基金における厳格な管理の下で利用させることが必要である。

また、支払基金支給以外の端末については、端末の管理を端末の所有者が行うこととなり、支払基金において管理ができないことへのリスクを勘案し、その利用の可否を判断する必

要がある。利用を認めたとしても、利用の許可手続を定めるとともに、情報の取扱いについての規定や手順を整備し遵守させる必要がある。

遵守事項

⑴　支払基金支給以外の端末の利用可否の判断

⑷　最高情報セキュリティ責任者は、支払基金支給以外の端末の利用について、取り扱うこととなる情報の格付及び取扱制限、支払基金が講じる安全管理措置、当該端末の管理は支払基金ではなくその所有者が行うこと等を踏まえ、求められる情報セキュリティの水準の達成の見込みを勘案し、支払基金における支払基金支給以外の端末の利用の可否を判断する。

遵守事項

⑵　支払基金支給以外の端末の利用に関する運用手順書の整備

⑷　情報セキュリティ責任者は、役職員等関係者が支払基金支給以外の端末を用いて支払基金の業務に係る情報処理を行う場合の許可等の手続を「モバイル端末(要管理対策区域外における使用）及び支払基金支給以外の端末の使用に係る手順書」に定める。

⑹　情報セキュリティ責任者は、役職員等関係者が支払基金支給以外の端末を用いて要保護情報を取り扱う場合について、盗難、紛失、不正プログラムの感染等により情報窃取されるなどのリスクを踏まえた利用手順及び許可手続を「モバイル端末(要管理対策区域外における使用）及び支払基金支給以外の端末の使用に係る手順書」に定める。

⑹　情報セキュリティ責任者は、要機密情報を取り扱う支払基金支給以外の端末について、盗難、紛失、不正プログラムの感染等により情報窃取されることを防止するための技術的な措置を含めた安全管理措置に関する手順を「モバイル端末(要管理対策区域外における使用）及び支払基金支給以外の端末の使用に係る手順書」に整備する。

⑹　情報セキュリティ責任者は、要管理対策区域外において支払基金外通信回線に接続した支払基金支給以外の端末を支払基金内通信回線に接続することについての可否を判断した上で、可と判断する場合は、当該端末から支払基金内通信回線を経由して情報システムが不正プログラムに感染するリスクを踏まえた安全管理措置に関する手順を「モバイル端末(要管理対策区域外における使用）及び支払基金支給以外の端末の使用に係る手順書」に整備する。

⑹　役職員等関係者は、支払基金支給以外の端末の利用に当たり、「モバイル端末(要管理対策区域外における使用）及び支払基金支給以外の端末の使用に係る手順書」を確認する。

【 基本対策事項 】

＜6.1.3(2)(a)関連＞

6.1.3(2)-1　情報セキュリティ責任者は、支払基金支給以外の端末を利用する際に、以下を全て含む許可等の手続を実施手順として整備し、役職員等関係者に周知する。なお、利用できる機能は、Microsoft365（Teams、Outlook 等）における情報及び資料の共有とする。

a)　以下を全て含む支払基金支給以外の端末利用時の申請内容

・申請者の氏名、所属、連絡先

・利用する端末の契約者の名義（スマートフォン等の通信事業者と契約を行う端末の場合）

・利用する端末の製造企業名、機種名、OS の種類及びバージョン

・利用目的及び利用を許可する業務、取り扱う情報の概要、要機密情報の利用の有無等

・主要な利用場所

・利用する主要な通信回線サービス

・利用する期間

b)　利用許諾条件

c)　申請手順

d)　利用期間中の不具合、盗難・紛失、修理、機種変更等の際の届出の手順

e)　利用期間満了時の利用終了又は利用期間更新の手続方法

f)　許可権限者（システム部長）

＜6.1.3(2)(b)関連＞

6.1.3(2)-2　情報セキュリティ責任者は、役職員等関係者が支払基金支給以外の端末を用いて要保護情報を取り扱う場合の利用手順を、以下を例とし実施手順として定める。

a)　端末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

b)　盗み見に対する対策（のぞき見防止フィルタの利用等）

c)　盗難・紛失に対する対策（不要な情報を端末に保存しない、端末の放置の禁止、利用時以外のシャットダウン及びネットワークの切断、モバイル端末を常時携帯する、常に身近に置き目を離さないなど）

d)　利用する場所や時間の限定

e)　端末の盗難・紛失が発生した際の緊急対応手順

6.1.3(2)-3　情報セキュリティ責任者は、要機密情報を取り扱う支払基金支給以外の端末について、以下を例とする利用時の措置を利用手順に加え、実施手順として定める。

a)　パスワード等による端末ロックの常時設定

b) OS やアプリケーションの最新化

c) 不正プログラム対策ソフトウェアの導入及び定期的な不正プログラム検査の実施（支払基金として不正プログラム対策ソフトウェアを指定する場合は当該ソフトウェアの導入も含める）

d) 支払基金提供の業務専用アプリケーションの利用（専用アプリケーションを提供する場合のみ）

6.1.3(2)-4 情報セキュリティ責任者は、要機密情報を取り扱う支払基金支給以外の端末について、以下を全て含む禁止事項を利用手順に加え、実施手順として定める。

a) 端末、OS、アプリケーション等の改造行為

b) 安全性が確認できないアプリケーションのインストール及び利用

c) 利用が禁止されているソフトウェアのインストール及び利用（利用を禁止するソフトウェアを定める場合）

d) 許可されない通信回線サービスの利用（利用する回線を限定する場合）

e) 第三者への端末の貸与

f) 利用承認を得ていないクラウドサービス等への端末内の要機密情報のバックアップ

g) Ｍｉｃｒｏｓｏｆｔ３６５の情報及び資料の端末へのダウンロード及び保存

h) 支払基金内通信回線への接続

i) 機密性３情報（重要性分類Ⅰ）の取扱い

6.1.3(2)-5 情報セキュリティ責任者は、役職員等関係者が支払基金支給以外の端末を用いて要保護情報を取り扱う場合について、以下を全て含む許可手続を実施手順として定める。

a) 利用時の許可申請手続

b) 手続内容（利用者、利用期間、主たる利用場所、目的、利用する情報、端末、通信回線への接続形態等）

c) 利用期間満了時の手続

d) 許可権限者（システム部長）による手続内容の記録

＜6.1.3(2)(c)関連＞

6.1.3(2)-6 情報セキュリティ責任者は、要機密情報を取り扱う支払基金支給以外の端末について、以下を例に、利用者が端末に情報を保存できないようにするための機能又は端末に保存される情報を暗号化するための対策の検討のほか、端末で機密性３情報（重要性分類Ⅰ）を取り扱うことができない対策についても検討し、要機密情報を取り扱う支払基金支給以外の端末に求める安全管理措置に関する運用手順のうちの技術的な措置として加える。なお、可能な限り端末に情報を保存させない機能を設ける。

a) シンクライアント等の仮想デスクトップ技術を活用した、端末に情報を保存

させないリモートアクセス環境を構築する。利用者は専用のシンクライアントアプリケーションを利用端末にインストールし、業務用システムへリモートアクセスする。

b) セキュアブラウザ等を活用した、端末に情報を保存させないリモートアクセス環境を構築する。利用者はセキュアブラウザを利用端末にインストールし、業務用システムへリモートアクセスする。

c) ファイル暗号化等のセキュリティ機能を持つアプリケーションを導入する。

d) 端末に、ハードディスク等の電磁的記録媒体全体を自動的に暗号化する機能を設ける。

e) 上記の各号のいずれの機能も使用できない場合は、端末にファイルを暗号化する機能を設ける。

f) ハードディスク等の電磁的記録媒体に保存されている情報を遠隔からの命令等により暗号化消去する機能を設ける。

g) 高度なセキュリティ機能を備えた OS を搭載するスマートフォンやタブレット端末等を使用する。

＜6.1.3⑵(d)関連＞

6.1.3⑵-7 情報セキュリティ責任者は、要管理対策区域外において支払基金外通信回線に接続した支払基金支給以外の端末を要管理対策区域で支払基金内通信回線に接続することの許可手続として、以下を全て含む手続を実施手順として整備し、役職員等関係者に遵守させる。

a) 利用時の許可申請手続

b) 手続内容（利用者、目的、利用する情報、端末等）

c) 利用期間満了時の手続

d) 支払基金内通信回線への接続時の手続（端末の事前検疫等）

e) 許可権限者（情報セキュリティ管理担当者）による手続内容の記録

遵守事項

⑶ 支払基金支給以外の端末の利用に関する責任者の策定

(a) 情報セキュリティ責任者は、支払基金支給以外の端末を用いた支払基金の業務に係る情報処理に関する安全管理措置の実施状況を管理する責任者（以下「端末管理責任者」という。）を定める。端末管理責任者はシステム部長とする。

遵守事項

⑷ 支払基金支給以外の端末の利用時の対策

(a) 役職員等関係者は、支払基金支給以外の端末を用いて支払基金の業務に係る情報処理を行う場合には、端末管理責任者（システム部長）の許可を得る。

⑹　役職員等関係者は、支払基金支給以外の端末を用いて要保護情報を取り扱う場合は、⑵⑹で定める利用手順に従う。

⑹　端末管理責任者（システム部長）等は、要機密情報を取り扱う支払基金支給以外の端末について、⑵⑹に定める安全管理措置を講じる又は役職員等関係者に講じさせる。

⑹　役職員等関係者は、情報処理の目的を完了した場合は、要保護情報を支払基金支給以外の端末から消去する。

6.2　サーバ装置

6.2.1　サーバ装置

目的・趣旨

電子メールサーバやウェブサーバ、ファイルサーバ等の各種サーバ装置には、大量の情報が保存されている場合が多く、当該情報の漏えいや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を受けるなどの可能性が高い。仮に支払基金が利用するサーバ装置が不正アクセスや迷惑メールの送信の中継地点に利用されるようなことになれば、国民の皆様からの信頼を大きく損なう。加えて、サーバ装置は、同時に多くの者が利用するため、その機能が停止した場合に与える影響が大きい。これらのことを考慮して、対策を講じる必要がある。

なお、本款の遵守事項のほか、7.1「情報システムのセキュリティ機能」において定める主体認証・アクセス制御・権限管理・ログ管理等の機能面での対策、7.2.1「ソフトウェアに関する脆弱性対策」、7.2.2「不正プログラム対策」、7.2.3「サービス不能攻撃対策」、6.4.4「IPv6 通信回線」において定める遵守事項のうちサーバ装置に関係するものについても遵守する必要がある。さらに、支払基金外通信回線を経由してサーバ装置の保守作業等を行う場合は、6.4.1「通信回線」のリモートメンテナンスについての対策も遵守する必要がある。また、特に電子メールサーバ、ウェブサーバ、DNS サーバ及びデータベースについては、本款での共通的な対策に加え、それぞれ本節において定める遵守事項についても併せて遵守する必要がある。

遵守事項

⑴　サーバ装置の導入時の対策

⑻　情報セキュリティ管理者は、要保護情報を取り扱うサーバ装置について、サーバ装置の盗難、不正な持ち出し、不正な操作、表示用デバイスの盗み見等の物理的な脅威から保護するための対策を講じる。

⑼　情報セキュリティ管理者は、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、要安定情報を取り扱う情報システムについて、サービス

提供に必要なサーバ装置を冗長構成にするなどにより可用性を確保する。

(c) 情報セキュリティ管理者は、多様なソフトウェアを利用することにより脆弱性が存在する可能性が増大することを防止するため、サーバ装置で利用を認めるソフトウェアを定め、それ以外のソフトウェアは利用させない。

(d) 情報セキュリティ管理者は、サーバ装置に接続を認めた機器等を定め、接続を認めた機器等以外は接続させない。

(e) 情報セキュリティ管理者は、情報システムのセキュリティ要件として策定した内容に従い、サーバ装置に対して適切なセキュリティ対策を実施する。

(f) 情報セキュリティ管理者は、サーバ装置において利用するソフトウェアに関連する公開された脆弱性について対策を実施する。

(g) 情報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、適切な方法でサーバ装置のバックアップを取得する。

【 基本対策事項 】

＜6.2.1(1)(a)関連＞

6.2.1(1)-1 情報セキュリティ管理者は、要保護情報を取り扱うサーバ装置については、クラス２以上の要管理対策区域に設置する。

6.2.1(1)-2 情報セキュリティ管理者は、サーバ装置の盗難及び不正な持ち出しを防止するために、以下を例とする対策を講じる。

a) 施錠可能なサーバラックに設置して施錠する。

b) 容易に切断できないセキュリティワイヤを用いて、固定物又は搬出が困難な物体に固定する。

6.2.1(1)-3 情報セキュリティ管理者は、第三者による不正操作及び表示用デバイスの盗み見を防止するために、以下を例とする対策を講じる。

a) 一定時間操作が無いと自動的にスクリーンロックするよう設定する。

＜6.2.1(1)(b)関連＞

6.2.1(1)-4 情報セキュリティ管理者は、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要安定情報を取り扱う情報システムについては、将来の見通しも考慮し、以下を例とする対策を講じる。

a) 負荷分散装置、DNS ラウンドロビン方式等による負荷分散

b) 同一システムを２系統で構成することによる冗長化

＜6.2.1(1)(c)関連＞

6.2.1(1)-5 情報セキュリティ管理者は、以下を考慮した上で、利用を認めるソフトウェアをバージョンも含め定める。

a) ソフトウェアベンダ等のサポート状況

b) ソフトウェアと外部との通信の有無及び通信する場合はその通信内容

c) インストール時に同時にインストールされる他のソフトウェア
d) その他、ソフトウェアの利用に伴う情報セキュリティリスク
e) セキュリティベンダ等の第三者が提供するソフトウェアの脆弱性等に関する情報が確認できること

遵守事項

⑵ サーバ装置の運用時の対策

⑻ 情報セキュリティ管理者は、利用を認めるソフトウェアについて、定期的な確認による見直しを行う。

⑼ 情報セキュリティ管理者は、所管する範囲のサーバ装置の構成やソフトウェアの状態を定期的に確認し、不適切な状態にあるサーバ装置を検出等した場合には改善を図る。

⑽ 情報セキュリティ管理者は、サーバ装置上での情報セキュリティインシデントの発生を監視するため、当該サーバ装置を監視するための措置を講じる。

⑾ 情報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、危機的事象発生時に適切な対処が行えるよう運用をする。

【 基本対策事項 】

＜6.2.1⑵⑼関連＞

6.2.1⑵-1 情報セキュリティ管理者は、所管する範囲のサーバ装置の構成やソフトウェアの状態を定期的に確認し、改善を図る場合は、作業日、作業を行ったサーバ装置名、具体的な作業内容（サーバ装置の構成等の変更、脆弱性管理、ソフトウェアのインストール等）及び作業者、正常動作を確認した者などを含む変更事項等を記録し、管理する。

＜6.2.1⑵⑽関連＞

6.2.1⑵-2 情報セキュリティ管理者は、サーバ装置への不正アクセス等の情報セキュリティインシデントの発生を監視するために、以下を例とする対策を講じる。

a) アクセスログ等を定期的に確認する。
b) IDS/IPS、WAF（Web Application Firewall）等を設置する。
c) 不正プログラム対策ソフトウェアを利用する。
d) ファイル完全性チェックツールを利用する。
e) CPU、メモリ、ディスク I/O 等のシステム状態を確認する。
f) ホスト型の IDS/IPS を利用する。
g) ユーザ、グループ、システムの管理者の追加、変更の有無を確認する。
h) 管理者、ユーザのパスワード漏洩の有無、大量のログオン失敗や、通常とは異

なる時間帯やアクセス元 IP アドレスからのログインがないか確認する。

＜6.2.1(2)(d)関連＞

6.2.1(2)-3　情報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、以下を全て含む運用をする。

a)　サーバ装置全体の適切なバックアップの取得及びバックアップ要件の確認による見直し

b)　サーバ装置の構成やソフトウェア等の設定の変更が行われた際及び定期的に、サーバ装置が停止した際の復旧手順の確認による見直し

遵守事項

(3)　サーバ装置の運用終了時の対策

(a)　情報セキュリティ管理者は、サーバ装置の運用を終了する際に、サーバ装置の電磁的記録媒体の全ての情報を抹消する。

6.2.2　電子メール

目的・趣旨

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などの機密性に対するリスクの他、悪意ある第三者等によるなりすまし等、電子メールが悪用される不正な行為の被害に電子メールを利用する役職員等関係者が巻き込まれるリスクもある。これらの問題を回避するためには、適切な電子メールサーバの管理が必要である。

なお、本款の遵守事項のほか、6.2.1「サーバ装置」において定めるサーバ装置に係る遵守事項についても併せて遵守する必要がある。

遵守事項

(1)　電子メールの導入時の対策

(a)　情報セキュリティ管理者は、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。

(b)　情報セキュリティ管理者は、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主体認証を行う機能を備える。

(c)　情報セキュリティ管理者は、電子メールのなりすましの防止策を講じる。

(d)　情報セキュリティ管理者は、インターネットを介して通信する電子メールの盗聴及び改ざんの防止のため、電子メールのサーバ間通信の暗号化の対策を講じる。

【 基本対策事項 】

＜6.2.2(1)(a)関連＞

6.2.2(1)-1　情報セキュリティ管理者は、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以下を例とする設定をする。

a)　送信元の電子メールサーバの IP アドレスによって中継を制限する設定

b)　送信元のメールアドレスのドメイン名によって中継を制限する設定

c)　宛先のメールアドレスのドメイン名によって中継を制限する設定

＜6.2.2(1)(b)関連＞

6.2.2(1)-2　情報セキュリティ管理者は、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、以下を例とする役職員等関係者の主体認証を行う機能を備える。

a)　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 認証等の主体認証機能を導入する。

＜6.2.2(1)(c)関連＞

6.2.2(1)-3　情報セキュリティ管理者は、以下を例とする電子メールのなりすましの防止策を講じる。

a)　 DMARC による送信側の対策を行う。DMARC による送信側の対策を行うためには、SPF、DKIM のいずれか又は両方による対策を行う必要がある。

b)　DMARC による受信側の対策を行う。DMARC による受信側の対策を行うためには、SPF、DKIM の両方による対策を行う必要がある。

6.2.2(1)-4　情報セキュリティ管理者は、必要に応じて、S/MIME 等の電子メールにおける電子署名の技術による電子メールのなりすましの防止策を講じる。

6.2.2(1)-5　情報セキュリティ管理者は、役職員等関係者が支払基金外の者と電子メールを送受信する場合には、支払基金のドメイン名を取得できない場合を除き、支払基金のドメイン名を使用した電子メールアドレスが利用される機能を備える。

＜6.2.2(1)(d)関連＞

6.2.2(1)-6　情報セキュリティ管理者は、以下を例とする電子メールの盗聴及び改ざんの防止策を講じる。

a)　SMTP によるサーバ間通信を TLS により保護する。

b)　S/MIME 等の電子メールにおける暗号化及び電子署名の技術を利用する。

6.2.3　ウェブ

目的・趣旨

インターネット上に公開するウェブサーバは、常に攻撃を受けるリスクを抱えている。様々な攻撃により、ウェブコンテンツ（ウェブページとして公開している情報）の改ざん、

ウェブサーバの利用停止、偽サイトへの誘導等の被害が想定されるため、適切な対策を組み合わせて実施することが求められる。

なお、本款の遵守事項のほか、6.2.1「サーバ装置」において定めるサーバ装置に係る遵守事項についても併せて遵守する必要がある。さらに、ウェブサーバにおけるウェブアプリケーションについては、6.6「アプリケーション・コンテンツ」を参照のこと。

遵守事項

⑴　ウェブサーバの導入・運用時の対策

⒜　情報セキュリティ管理者は、脆弱性が存在する可能性が増大することを防止するため、ウェブサーバが備える機能のうち、必要な機能のみを利用する。

⒝　情報セキュリティ管理者は、ウェブサーバからの不用意な情報漏えいを防止するための措置を講じる。

⒞　情報セキュリティ管理者は、ウェブコンテンツの編集作業を行う主体を限定する。

⒟　情報セキュリティ管理者は、インターネットを介して転送される情報の盗聴及び改ざんの防止のため、全ての情報に対する暗号化及び電子証明書による認証の対策を講じる。

【 基本対策事項 】

＜6.2.3⑴⒜関連＞

6.2.3⑴-1　情報セキュリティ管理者は、ウェブサーバが備える機能のうち、必要な機能のみを利用するために、以下を全て含むウェブサーバの管理や設定を行う。

a)　CGI 機能を用いるスクリプト等は必要最低限のものに限定し、CGI 機能を必要としない場合は設定で CGI 機能を使用不可とする。

b)　ディレクトリインデックスの表示を禁止する。

c)　ウェブコンテンツ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を制限する。

d)　ウェブサーバ上で動作するソフトウェアは、最新のものを利用するなど、既知の脆弱性が解消された状態を維持する。

＜6.2.3⑴⒝関連＞

6.2.3⑴-2　情報セキュリティ管理者は、ウェブサーバからの不用意な情報漏えいを防止するために、以下を全て含むウェブサーバの管理や設定を行う。

a)　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。

b)　初期状態で用意されるサンプルのページ、プログラム等、不要なものは削除する。

c)　ウェブサーバに保存する情報を特定し、サービスの提供に必要のない情報がウェブサーバに保存されないことを確認する。

＜6.2.3(1)(c)関連＞

6.2.3(1)-3　情報セキュリティ管理者は、ウェブコンテンツの編集作業を担当するアカウントの限定として、以下を全て含むウェブサーバの管理や設定を行う。

a)　ウェブサーバ上のウェブコンテンツへのアクセス権限は、ウェブ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。

b)　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、不要なものは削除する。

6.2.3(1)-4　情報セキュリティ管理者は、ウェブコンテンツの編集作業に用いる端末の限定、識別コード及び主体認証情報の適切な管理として、以下を例とするウェブサーバの管理や設定を行う。

a)　ウェブコンテンツの更新の際は、専用の端末を使用して行う。

b)　ウェブコンテンツの更新の際は、ウェブサーバに接続する接続元の IP アドレスを必要最小限に制限する。

c)　ウェブコンテンツの更新に利用する識別コードや主体認証情報は、情報セキュリティを確保した管理を行う。

＜6.2.3(1)(d)関連＞

6.2.3(1)-5　情報セキュリティ管理者は、通信時の盗聴による第三者への情報の漏えい及び改ざんの防止並びに正当なウェブサーバであることを利用者が確認できるようにするための措置として、以下を全て含むウェブサーバの実装を行う。

a)　TLS 機能を適切に用いる。

b)　TLS 機能のために必要となるサーバ証明書には、利用者が事前のルート証明書のインストールを必要とすることなく、その正当性を検証できる認証局（証明書発行機関）により発行された電子証明書を用いる。

c)　暗号技術検討会及び関連委員会（CRYPTREC）により作成された「TLS 暗号設定ガイドライン」に従って、TLS サーバを適切に設定する。

6.2.4　ドメインネームシステム（DNS）

目的・趣旨

ドメインネームシステム（DNS：Domain Name System）は、インターネットを使った階層的な分散型システムで、主としてインターネット上のホスト名や電子メールで使われるドメイン名と、IP アドレスとの対応づけ（正引き、逆引き）を管理するために使用されている。DNS では、端末等のクライアント（DNS クライアント）からの問合せを受けて、ドメイン名やホスト名と IP アドレスとの対応関係等について回答を行う。DNS には、支払基金が管理するドメインに関する問合せについて回答を行うコンテンツサーバと、DNS クライアントからの要求に応じてコンテンツサーバに対して問合せを行うキャッシュサーバが

存在する。キャッシュサーバ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、コンテンツサーバ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、端末等の DNS クライアントが悪意あるサーバに接続させられるなどの被害に遭う可能性がある。さらに、電子メールのなりすまし対策の一部は DNS で行うため、これに不備があった場合には、なりすまされた電子メールの検知が不可能となる。これらの問題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。

なお、本款の遵守事項のほか、6.2.1「サーバ装置」において定めるサーバ装置に係る遵守事項についても併せて遵守する必要がある（SaaS 系のクラウドサービスを利用する場合を除く）。

遵守事項

⑴　DNS の導入時の対策

⑷　情報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の名前解決を提供する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じる。

⑹　情報セキュリティ管理者は、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じる。

⑹　情報セキュリティ管理者は、コンテンツサーバにおいて、支払基金のみで使用する名前の解決を提供する場合、当該コンテンツサーバで管理する情報が外部に漏えいしないための措置を講じる。

【 基本対策事項 】

＜6.2.4⑴⑷関連＞

6.2.4⑴-1　情報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の名前解決を提供するコンテンツサーバにおいて、以下を例とする名前解決を停止させないための措置を講じる。

a)　コンテンツサーバを冗長化する。

b)　通信回線装置等で、コンテンツサーバへのサービス不能攻撃に備えたアクセス制御を行う。

c)　ISP 等が提供するマネージド DNS サービスや DDoS（Distributed Denial of Service）対策サービスを利用する。

d)　UDP 及び TCP の両方でサービスを提供する。

＜6.2.4⑴⑹関連＞

6.2.4⑴-2　情報セキュリティ管理者は、支払基金外からの名前解決の要求に応じる必要性があるかについて検討し、必要性がないと判断される場合は必要であれば支払基金内からの名前解決の要求のみに応答をするよう、以下を例とする措置を

講じる。

a) キャッシュサーバの設定でアクセス制御を行う。

b) ファイアウォール等でアクセス制御を行う。

6.2.4(1)-3 情報セキュリティ管理者は、DNS キャッシュポイズニング攻撃から保護するため、以下を例とする措置を講じる。

a) ソースポートランダマイゼーション機能を導入する。

b) DNSSEC を利用する。

＜6.2.4(1)(c)関連＞

6.2.4(1)-4 情報セキュリティ管理者は、支払基金のみで使用する名前の解決を提供するコンテンツサーバにおいて、以下を例とする当該コンテンツサーバで管理する情報の漏えいを防止するための措置を講じる。

a) 外部向けのコンテンツサーバと別々に設置する。

b) ファイアウォール等でアクセス制御を行う。

遵守事項

(2) DNS の運用時の対策

(a) 情報セキュリティ管理者は、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。

(b) 情報セキュリティ管理者は、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が正確であることを定期的に確認する。

(c) 情報セキュリティ管理者は、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維持するための措置を講じる。

【 基本対策事項 】

＜6.2.4(2)(c)関連＞

6.2.4(2)-1 情報セキュリティ管理者は、キャッシュサーバにおいて、ルートヒントファイル（DNS ルートサーバの情報が登録されたファイル）の更新の有無を定期的（3か月に一度程度）に確認し、最新の DNS ルートサーバの情報を維持する。

6.2.4(2)-2 情報セキュリティ管理者は、キャッシュサーバにおいて DNSSEC を利用する場合、電子署名を検証する起点となる DNSSEC トラストアンカーを最新の状態に保つため、自動更新機能を有効にする又は更新の有無を定期的（3か月に一度程度）に確認する。

6.2.5　データベース

目的・趣旨

本款における「データベース」とは、データベース管理システムとそれによりアクセスされるデータファイルから構成され、体系的に構成されたデータを管理し、容易に検索・抽出等が可能な機能を持つものであって、要保護情報を保管するサーバ装置とする。

要保護情報を保管するデータベースでは、不正プログラム感染や不正アクセス等の外的要因によるリスク及び役職員等関係者の不適切な利用や過失等の内的要因によるリスクに対して、管理者権限の悪用を防止するための技術的対策等を講じる必要がある。

特に大量のデータを保管するデータベースの場合、そのデータが漏えい等した際の影響が大きく、また、そのようなデータは攻撃者の標的となりやすい。

なお、本款の遵守事項のほか、7.1「情報システムのセキュリティ機能」において定める主体認証・アクセス制御・権限管理・ログ管理・暗号・電子署名等の機能面での対策、6.4.4「IPv6 通信回線」、7.2.1「ソフトウェアに関する脆弱性対策」、7.2.2「不正プログラム対策」において定める遵守事項のうち、データベースに関係するものについても併せて遵守する必要がある。

遵守事項

⑴　データベースの導入・運用時の対策

⒜　情報セキュリティ管理者は、データベースに対する内部不正を防止するため、管理者アカウントの適正な権限管理を行う。

⒝　情報セキュリティ管理者は、データベースに格納されているデータにアクセスした利用者を特定できるよう、措置を講じる。

⒞　情報セキュリティ管理者は、データベースに格納されているデータに対するアクセス権を有する利用者によるデータの不正な操作を検知できるよう、対策を講じる。

⒟　情報セキュリティ管理者は、データベース及びデータベースへアクセスする機器等の脆弱性を悪用した、データの不正な操作を防止するための対策を講じる。

⒠　情報セキュリティ管理者は、データの窃取、電磁的記録媒体の盗難等による情報の漏えいを防止する必要がある場合は、適切に暗号化をする。

【 基本対策事項 】

＜6.2.5⑴⒜関連＞

6.2.5⑴-1　情報セキュリティ管理者は、必要に応じて情報システムの管理者とデータベースの管理者を別にする。

6.2.5⑴-2　情報セキュリティ管理者は、データベースに格納されているデータにアクセスする必要のない管理者に対して、データへのアクセス権を付与しない。

6.2.5(1)-3　情報セキュリティ管理者は、データベースの管理に関する権限の不適切な付与を検知できるよう、措置を講じる。

＜6.2.5(1)(c)関連＞

6.2.5(1)-4　情報セキュリティ管理者は、業務を遂行するに当たって不必要なデータの操作を検知できるよう、以下を例とする措置を講じる。

a)　一定数以上のデータの取得に関するログを記録し、警告を発する。

b)　データを取得した時刻が不自然であるなど、通常の業務によるデータベースの操作から逸脱した操作に関するログを記録し、警告を発する。

＜6.2.5(1)(d)関連＞

6.2.5(1)-5　情報セキュリティ管理者は、データベースにアクセスする機器上で動作するプログラムに対して、SQL インジェクションの脆弱性を排除する。

6.2.5(1)-6　情報セキュリティ管理者は、データベースにアクセスする機器上で動作するプログラムに対して SQL インジェクションの脆弱性の排除が不十分であると判断した場合、以下を例とする対策の実施を検討する。

a)　ウェブアプリケーションファイアウォールの導入

b)　データベースファイアウォールの導入

＜6.2.5(1)(e)関連＞

6.2.5(1)-7　情報セキュリティ管理者は、データベースに格納されているデータに対して暗号化を実施する場合には、バックアップデータやトランザクションデータ等についても暗号化を実施する。

6.3　複合機・特定用途機器

6.3.1　複合機・特定用途機器

目的・趣旨

支払基金においては、プリンタ、ファクシミリ、イメージスキャナ、コピー機等の機能が一つにまとめられている複合機が利用されている。複合機は、支払基金通信回線や公衆電話網等の通信回線に接続して利用されることが多く、その場合には、ウェブによる管理画面を始め、ファイル転送、ファイル共有、リモートメンテナンス等多くのサービスが動作するため、様々な脅威が想定される。

また、支払基金においては、IP 電話システム等の特定の用途に使用される情報システムが利用されている。これらの特定用途機器がインターネットに接続する機能を備える、いわゆる IoT 機器となっている場合が多くある。例えばネットワークカメラシステムの構成要素である機器のうちインターネットに接続する機能を備えるカメラや、環境モニタリングシステムの構成要素である機器のうちインターネットに接続する機能を備えるセンサーが挙げられる。近年、IoT 機器の脆弱性をついた攻撃が数多く発生しており、IoT 機器が踏み

台となって他の情報システムへの攻撃に利用されるなど、社会的問題となってきている。このため、これらの機器に対する情報セキュリティ対策が必要となる。

したがって、複合機や IoT 機器を含む特定用途機器に関しても情報システムの構成要素と捉え、責任者を明確にして適切に対策を講じることが重要である。

遵守事項

⑴ 複合機

(a) 情報セキュリティ管理者は、複合機を調達する際には、当該複合機が備える機能、設置環境並びに取り扱う情報の格付及び取扱制限に応じ、適切なセキュリティ要件を策定する。

(b) 情報セキュリティ管理者は、複合機が備える機能について適切な設定等を行うことにより運用中の複合機に対する情報セキュリティインシデントへの対策を講じる。

(c) 情報セキュリティ管理者は、複合機の運用を終了する際に、複合機の電磁的記録媒体の全ての情報を抹消する。

【 基本対策事項 】

＜6.3.1(1)(a)関連＞

6.3.1(1)-1 情報セキュリティ管理者は、「IT 製品の調達におけるセキュリティ要件リスト」を参照するなどし、複合機が備える機能、設置環境並びに取り扱う情報の格付及び取扱制限に応じ、当該複合機に対して想定される脅威を分析した上で、脅威へ対抗するためのセキュリティ要件を調達仕様書に明記する。

＜6.3.1(1)(b)関連＞

6.3.1(1)-2 情報セキュリティ管理者は、以下を例とする運用中の複合機に対する、情報セキュリティインシデントへの対策を講じる。

a) 複合機について、利用環境に応じた適切なセキュリティ設定を実施する。

b) 複合機が備える機能のうち利用しない機能を停止する。

c) 印刷された書面からの情報の漏えいが想定される場合には、複合機が備える操作パネルで利用者認証が成功した者のみ印刷が許可される機能等を活用する。

d) 複合機をインターネットに直接接続しない。

e) リモートメンテナンス等の目的で複合機がインターネットを介して外部と通信する場合は、ファイアウォール等の利用により適切に通信制御を行う。

f) 利用者ごとに許可される操作を適切に設定する。

＜6.3.1(1)(c)関連＞

6.3.1(1)-3 情報セキュリティ管理者は、内蔵電磁的記録媒体の全領域完全消去機能（上書き消去機能）を備える複合機については、当該機能を活用することにより複合機内部の情報を抹消する。当該機能を備えていない複合機については、業務委託先

との契約時に業務委託先に複合機内部に保存されている情報の漏えいが生じないための対策を講じさせることを、契約内容に含むようにするなどの別の手段で対策を講じる。

遵守事項

⑵　IoT 機器を含む特定用途機器

⑻　情報セキュリティ管理者は、特定用途機器について、取り扱う情報、利用方法、通信回線への接続形態等により脅威が存在する場合には、当該機器の特性に応じた対策を講じる。

【 基本対策事項 】

＜6.3.1⑵⑻関連＞

6.3.1⑵-1　情報セキュリティ管理者は、特定用途機器の特性に応じて、以下を含む対策を講じる。ただし、使用している特定用途機器の機能上の制約により講じることができない対策を除く。

a)　特定用途機器について、主体認証情報を初期設定から変更した上で適切に管理する。

b)　特定用途機器にアクセスする主体に応じて必要な権限を割り当て、管理する。

c)　特定用途機器が備える機能のうち利用しない機能を停止する。

d)　インターネットと通信を行う必要のない特定用途機器については、当該特定用途機器をインターネットに接続させず、インターネットに接点を有する情報システムに接続する場合は、当該特定用途機器がインターネットに接続されないように適切に通信制御を行う。

e)　特定用途機器がインターネットを介して外部と通信する場合は、ファイアウォール等の利用により適切に通信制御を行う。

f)　特定用途機器のソフトウェアに関する脆弱性の有無を確認し、脆弱性が存在する場合は、バージョンアップやセキュリティパッチの適用、アクセス制御等の対策を講じる。

g)　特定用途機器に対する不正な行為、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。

h)　特定用途機器を使用しない場合は、特定用途機器の電源をオフにする。

i)　特定用途機器を廃棄する場合は、特定用途機器の内蔵電磁的記録媒体に保存されている全ての情報を抹消する。

6.4　通信回線

6.4.1　通信回線

目的・趣旨

サーバ装置や端末への不正アクセスやサービス不能攻撃等は、当該サーバ装置や端末に接続された通信回線及び通信回線装置を介して行われる場合がほとんどであることから、通信回線及び通信回線装置に対する情報セキュリティ対策については、情報システムの構築時からリスクを十分検討し、必要な対策を実施しておく必要がある。通信回線の運用主体又は物理的な回線の種類によって情報セキュリティリスクが異なることを十分考慮し、対策を講じる必要がある。

また、情報システムの運用開始時と一定期間運用された後とでは、通信回線の構成や接続される情報システムの条件等が異なる場合があり、攻撃手法の変化も想定されることから、情報システムの構築時に想定した対策では十分でなくなる可能性がある。そのため、通信回線の運用時においても、継続的な対策を実施することが重要である。

遵守事項

⑴　通信回線の導入時の対策

⑷　情報セキュリティ管理者は、通信回線構築時に、当該通信回線に接続する情報システムにて取り扱う情報の格付及び取扱制限に応じた適切な回線種別を選択し、情報セキュリティインシデントによる影響を回避するために、通信回線に対して必要な対策を講じる。

⑸　情報セキュリティ管理者は、通信回線において、サーバ装置及び端末のアクセス制御及び経路制御を行う機能を設ける。

⑹　情報セキュリティ管理者は、要機密情報を取り扱う情報システムを通信回線に接続する際に、通信内容の秘匿性の確保が必要と考える場合は、通信内容の秘匿性を確保するための措置を講じる。

⑺　情報セキュリティ管理者は、役職員等関係者が通信回線へ情報システムを接続する際に、当該情報システムが接続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じる。支払基金通信回線へ支払基金支給以外の端末を接続する際も同様とする。ただし、個人が所有する端末は接続してはならない。

⑻　情報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が接続される通信回線について、当該通信回線の継続的な運用を可能とするための措置を講じる。

【 基本対策事項 】

＜6.4.1⑴⑷⑸関連＞

6.4.1⑴-1　情報セキュリティ管理者は、通信回線を経由した情報セキュリティインシデ

ントの影響範囲を限定的にするため、通信回線の構成、当該通信回線に接続する情報システムにて取り扱う情報の格付及び取扱制限、拠点等の地理的事情に応じて、以下を例とする通信経路の分離を行う。

a) 外部等との通信を行うサーバ装置及び通信回線装置のセグメントを DMZ として構築し、内部のセグメントと通信経路を分離する。

b) 通信が必要な単位でセグメントを分割し、セグメント間の通信を必要最小限とするアクセス制御を行う。

c) 他の情報システムから独立した専用の通信回線を構築する。

＜6.4.1(1)(c)関連＞

6.4.1(1)-2 情報セキュリティ管理者は、通信経路における盗聴及び情報の改ざん等の脅威への対策として、通信内容の秘匿性を確保するための機能を設ける。通信回線の秘匿性確保の方法として、TLS、IPsec 等による暗号化を行う。また、その際に使用する暗号アルゴリズム及び鍵長については、「電子政府推奨暗号リスト」を参照し決定する。

＜6.4.1(1)(d)関連＞

6.4.1(1)-3 情報セキュリティ管理者は、支払基金通信回線への接続を許可された情報システムであることを確認し、無許可の情報システムの接続を拒否するための機能として、以下を例とする対策を講じる。

a) 情報システムの MAC アドレス等の端末を一意に識別できる情報により接続機器を識別する。

b) クライアント証明書により接続機器の認証を行う。

＜6.4.1(1)(e)関連＞

6.4.1(1)-4 情報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が接続される通信回線を構築する場合は、以下を例とする対策を講じる。

a) 通信回線の性能低下や異常の有無を確認するため、通信回線の利用率、接続率等の運用状態を定常的に確認、分析する機能を設ける。

b) 通信回線及び通信回線装置を冗長構成にする。

c) 端末等が情報システムと通信可能な代替手段を整備する。

遵守事項

(2) 支払基金外通信回線の接続時の対策

(a) 情報セキュリティ管理者は、支払基金内通信回線にインターネット回線、公衆通信回線等の支払基金外通信回線を接続する場合には、支払基金内通信回線及び当該支払基金内通信回線に接続されている情報システムの情報セキュリティを確保するための措置を講じる。

(b) 情報セキュリティ管理者は、支払基金通信回線と支払基金外通信回線との間及び支

払基金内通信回線内の不正な通信の有無を監視するための措置を講じる。

(c) 情報セキュリティ管理者は、保守又は診断のために、支払基金外通信回線から支払基金内通信回線に接続された機器等に対して行われるリモートメンテナンスに係る情報セキュリティを確保する。

(d) 情報セキュリティ管理者は、電気通信事業者の通信回線サービスを利用する場合には、当該通信回線サービスの情報セキュリティ水準及びサービスレベルを確保するための措置について、情報システムの構築を委託する事業者と契約時に取り決めておく。

【 基本対策事項 】

＜6.4.1(2)(a)関連＞

6.4.1(2)-1 情報セキュリティ管理者は、支払基金内通信回線に、インターネット回線や公衆通信回線等の支払基金外通信回線を接続する場合には、外部からの不正アクセスによる被害を防止するため、以下を例とする対策を講じる。

a) ファイアウォール、WAF、プロキシやリバースプロキシ、次世代ファイアウォール等により通信制御を行う。

b) 通信回線装置による特定の通信プロトコルの利用を制限する。

c) IDS/IPS により不正アクセスを検知及び遮断する。

d) 不審なメールの受信や不審なウェブサイトへのアクセスを遮断する。

e) サンドボックス型の標的型攻撃対策をする。

6.4.1(2)-2 情報セキュリティ管理者は、インターネット回線等の支払基金外通信回線を用いたクラウドサービスへのアクセスがある場合、クラウドサービスへのアクセスを可視化し、適切な利用を把握するための対策を検討する。

＜6.4.1(2)(b)関連＞

6.4.1(2)-3 情報セキュリティ管理者は、支払基金内通信回線と支払基金外通信回線との間及び支払基金内通信回線内の不正な通信の有無を監視するため、以下を例とする監視を行う。

a) 支払基金外と通信回線で接続している箇所における外部からの不正アクセスの監視

b) 不正プログラム感染や踏み台に利用されること等による支払基金外への不正な通信の監視

c) 不正プログラム等の感染による拡大防止のため、支払基金内通信回線の機器等における不審な通信の監視

6.4.1(2)-4 情報セキュリティ管理者は、特定した監視対象について、監視方法及び監視記録の保存期間を定め、監視記録を保存し、適切に保護、管理する。

＜6.4.1(2)(c)関連＞

6.4.1(2)-5 情報セキュリティ管理者は、支払基金外通信回線からの保守又は診断のため

の支払基金内通信回線に接続された機器等に対して行われるリモートメンテナンスのセキュリティ確保のために、以下を全て含む対策を講じる。

a) リモートメンテナンスを行う主体の認証において多要素主体認証を用いる

b) リモートメンテナンスを行う端末等を制限するアクセス制御

c) 主体認証によるアクセス制御

d) 通信内容の暗号化による秘匿性の確保

e) ファイアウォール等の通信制御のための機器に例外的な設定を行う場合は、その設定により脆弱性が生じないようにする。

遵守事項

⑶ 通信回線の運用時の対策

⒜ 情報セキュリティ管理者は、経路制御及びアクセス制御を適切に運用し、通信回線や通信要件の変更の際及び定期的に、経路制御及びアクセス制御の設定の確認及び見直しを行う。

⒝ 情報セキュリティ管理者は、支払基金内通信回線と支払基金外通信回線との間及び支払基金内通信回線内の不正な通信の有無を監視するための監視対象や監視方法等について、定期的な確認による見直しをする。

⒞ 情報セキュリティ管理者は、保守又は診断のために、支払基金外通信回線から支払基金内通信回線に接続された機器等に対して行われるリモートメンテナンスに係る情報セキュリティ対策について、定期的な確認による見直しをする。

⒟ 情報セキュリティ管理者は、情報システムの情報セキュリティの確保が困難な事由が発生した場合には、当該情報システムが他の情報システムと共有している通信回線について、共有先の他の情報システムを保護するため、当該通信回線とは別に独立した閉鎖的な通信回線に構成を変更する。

【 基本対策事項 】

＜6.4.1⑶⒞関連＞

6.4.1⑶-1 情報セキュリティ管理者は、支払基金外通信回線から保守又は診断のためのリモートメンテナンスに関する以下を全て含む事項について、定期的な確認による見直しを行う。

a) リモートからのアクセスが必要な主体

b) リモートメンテナンスを行う端末

c) ファイアウォール等の通信制御のための機器に例外的な設定を行った場合の設定

6.4.2　通信回線装置

目的・趣旨

インターネット等の外部ネットワークからアクセス可能な通信回線装置においては、ソフトウェアの脆弱性を悪用された不正アクセスの被害を受ける可能性がある。そのため、通信回線装置におけるソフトウェアの脆弱性対策は、迅速かつ適切に対処することが求められる。また、通信回線装置は端末やサーバ装置などの経路制御やアクセス制御に用いるため、情報システムの構築時からリスクを十分検討し、必要なセキュリティ対策を実施しておく必要がある。さらに運用時においても、脅威動向の変化等に応じた継続的な対策を実施することが重要である。

遵守事項

⑴　通信回線装置の導入時の対策

⒜　情報セキュリティ管理者は、物理的な通信回線装置を設置する場合、第三者による破壊や不正な操作等が行われないようにする。

⒝　情報セキュリティ管理者は、通信回線装置が動作するためのソフトウェアに関して、以下を含む対策を講じる。

(ｱ)　バージョン確認する。

(ｲ)　脆弱性についての影響度と緊急度を確認する。

(ｳ)　影響度や緊急度に応じて更新ソフトウェアを適用するまでの時間をできるだけ短くする。

(ｴ)　通信に影響を与えるような更新がなされる場合は、バックアップを用意する。

⒞　情報セキュリティ管理者は、情報システムのセキュリティ要件として策定した情報システムのネットワーク構成に関する要件内容に従って従い、通信回線装置に対して適切なセキュリティ対策を実施する。

⒟　情報セキュリティ管理者は、通信回線装置において利用するソフトウェアに関連する公開された脆弱性について対策を実施する。

【 基本対策事項 】

＜6.4.2⑴⒜関連＞

6.4.2(1)-1　情報セキュリティ管理者は、第三者による通信回線及び物理的な通信回線装置の破壊、不正操作等への対策として、以下を例とする措置を講じる。

a)　要管理対策区域に設置する。

b)　物理的な通信回線装置を施錠可能なラック等に設置する。

c)　支払基金の施設内に敷設した通信ケーブルを物理的に保護する。

d)　物理的な通信回線装置の操作ログを取得する。

＜6.4.2(1)(b)関連＞

6.4.2(1)-2　情報セキュリティ管理者は、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、ソフトウェアを変更する際の許可申請手順を整備する。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。

遵守事項

(2)　通信回線装置の運用時の対策

(a)　情報セキュリティ管理者は、通信回線装置の運用・保守に関わる作業等により通信回線装置の設定変更等を実施する場合は、情報セキュリティインシデント発生時の調査対応のための作業記録を取得し保管する。

(b)　情報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を構成する通信回線装置については、運用状態を復元するために必要な設定情報等のバックアップを取得し保管する。

(c)　情報セキュリティ管理者は、通信回線装置が動作するために必要なソフトウェアの状態等を調査し、認識した脆弱性等について対策を講じる。

【 基本対策事項 】

＜6.4.2(2)(c)関連＞

6.4.2(2)-1　情報セキュリティ管理者は、通信回線装置が動作するために必要なソフトウェアの状態を定期的に調査（脆弱性の確認を含む）し、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など、不適切な状態にある通信回線装置を認識した場合には、改善を図る。

遵守事項

(3)　通信回線装置の運用終了時の対策

(a)　情報セキュリティ管理者は、通信回線装置の運用を終了する場合には、当該通信回線を構成する通信回線装置が運用終了後に再利用された時又は廃棄された後に、運用中に保存していた情報が漏えいすることを防止するため、当該通信回線装置の電磁的記録媒体に記録されている全ての情報を抹消するなど適切な措置を講じる。

6.4.3　無線 LAN

目的・趣旨

無線 LAN は、有線の通信回線及び通信回線装置において想定される脅威に加え、電波を利用するために有線と比較して通信の傍受等が容易であることに起因する脅威への対策が必要である。

なお、本款の遵守事項の他、6.4.1「通信回線」及び 6.4.2「通信回線装置」において定める導入時の対策に係る遵守事項についても併せて遵守する必要がある。

遵守事項

⑴　無線 LAN 環境導入時の対策

⑷　情報セキュリティ管理者は、無線 LAN 技術を利用して支払基金内通信回線を構築する場合は、通信回線の構築時共通の対策に加えて、通信内容の秘匿性を確保するために通信路の暗号化を行った上で、その他の情報セキュリティ確保のために必要な措置を講じる。

【 基本対策事項 】

＜6.4.3⑴⑷関連＞

6.4.3⑴-1　情報セキュリティ管理者は、無線 LAN 技術を利用して支払基金通信回線を構築する場合は、通信回線の構築時共通の対策に加えて、情報システムの分類に基づき、以下の対策を講じる。

【基本セキュリティ対策】以下を全て含む対策を講じる。

a)　無線 LAN 通信の暗号化

b)　無線 LAN 回線利用申請手続の整備

c)　以下を例とする無線 LAN 機器の管理

・無線 LAN 機器の電波出力・周波数チャンネル等の管理

・無線 LAN 機器のファームウェア等の更新作業

・管理外の無線 LAN アクセスポイント、端末の検出及び除去

d)　来訪者等に提供する無線 LAN によるインターネット接続回線と業務で使用する支払基金 LAN の分離

【追加セキュリティ対策】基本セキュリティ対策の実施に加えて、以下を例とする対策を講じる。

e)　IEEE 802.1X による無線 LAN へのアクセス主体の認証

6.4.4　IPv6 通信回線

目的・趣旨

近年では、サーバ装置、端末及び通信回線装置等に IPv6 技術を利用する通信（以下「IPv6 通信」という。）を行う機能が標準で備わっているものが多く出荷されている。IPv6 通信プロトコルでは、グローバル IP アドレスによるパケットの直接到達性などを考慮する必要があり、設定不備によっては運用者が意図しない IPv6 通信が通信ネットワーク上で動作し、結果として、不正アクセスの手口として悪用されるおそれもある。このため、必要な対策を

講じていく必要がある。

遵守事項

⑴　IPv6 通信を行う情報システムに係る対策

⑷　情報セキュリティ管理者は、IPv6 技術を利用する通信を行う情報システムを構築する場合は、製品として調達する機器等について、IPv6 Ready Logo Program に基づく Phase-2 準拠製品を、可能な場合には選択する。

⑹　情報セキュリティ管理者は、IPv6 通信の特性等を踏まえ、IPv6 通信を想定して構築する情報システムにおいて、IPv6 通信による情報セキュリティ上の脅威又は脆弱性に対する検討を行い、必要な措置を講じる。

【 基本対策事項 】

＜6.4.4⑴⑹関連＞

6.4.4(1)-1　情報セキュリティ管理者は、以下を全て含む IPv6 通信による情報セキュリティ上の脅威又は脆弱性に対する検討を行い、必要な措置を講じる。

a)　グローバル IP アドレスによる直接の到達性における脅威

b)　IPv6 通信環境の設定不備等に起因する不正アクセスの脅威

c)　IPv4 通信と IPv6 通信を情報システムにおいて共存させる際の処理考慮漏れに起因する脆弱性の発生

d)　アプリケーションにおける IPv6 アドレスの取扱い考慮漏れに起因する脆弱性の発生

遵守事項

⑵　意図しない IPv6 通信の抑止・監視

⑷　情報セキュリティ管理者は、サーバ装置、端末及び通信回線装置を、IPv6 通信を想定していない通信回線に接続する場合には、自動トンネリング機能で想定外の IPv6 通信パケットが到達する脅威等、当該通信回線から受ける不正な IPv6 通信による情報セキュリティ上の脅威を防止するため、IPv6 通信を抑止するなどの措置を講じる。

6.5　ソフトウェア

6.5.1　情報システムの基盤を管理又は制御するソフトウェア

目的・趣旨

情報システムの基盤を管理又は制御するソフトウェアは、情報システムを制御する上でセキュリティ上の重要な機能を有している。そのようなソフトウェアは悪用や不正アクセスされた場合、被害が広範囲に及ぶ可能性がある。したがって、情報システムの基盤を管理

又は制御するソフトウェアを利用する端末やサーバ装置、通信回線装置等及びソフトウェア自体において、必要なセキュリティ対策を実施する必要がある。

本款では、情報システムの基盤を管理又は制御するソフトウェアを利用する場合に求めるセキュリティ対策として、7.1 情報システムのセキュリティ機能で求めている対策から特に必要と考えられるものを示しており、本款以外に 7.1.1「主体認証機能」で定める主体認証機能の導入、7.1.2「アクセス制御機能」で定めるアクセス制御機能の導入、7.1.3「権限の管理」で定める権限の管理、7.1.4「ログの取得・管理」で定めるログの取得に係る遵守事項についても併せて遵守する必要があるが、情報システムの基盤を管理又は制御するソフトウェアの機能や仕様等を踏まえて、適切な対策を講じることが重要となる。

また、当該ソフトウェアを利用する際の操作ミスや設定不備などを防ぐためには、当該ソフトウェアの利用者や管理者が利用するソフトウェアを利用するための手順を整備することも重要である。さらに、情報システムの基盤を管理又は制御するソフトウェアを悪用した攻撃を防ぐにはソフトウェアの脆弱性対策が特に重要となる。当該ソフトウェアに関係する脆弱性に関する情報を製品ベンダや脆弱性情報提供サイト等からの通知を受け取るようにするとともに、公開された脆弱性についての影響度と緊急度に応じてセキュリティパッチ等を適用するまでの時間をできるだけ短くするなどの対策を検討する必要がある。脆弱性対策については、7.2.1「ソフトウェアに関する脆弱性対策」を参照し確実な対策を実施することが重要である。

遵守事項

⑴ 情報システムの基盤を管理又は制御するソフトウェア導入時の対策

(a) 情報セキュリティ管理者は、情報セキュリティの観点から情報システムの基盤を管理又は制御するソフトウェアを導入する端末、サーバ装置、通信回線装置等及びソフトウェア自体を保護するための措置を講じる。

(b) 情報セキュリティ管理者は、利用するソフトウェアの特性を踏まえ、以下の全ての実施手順を整備する。

(ｱ) 情報システムの基盤を管理又は制御するソフトウェアの情報セキュリティ水準の維持に関する以下の手順

・設定や構成の文書化

・情報システム全体に影響を及ぼすような重要な操作の手順

・情報セキュリティに関する設定や構成を変更する際の手順

(ｲ) 情報システムの基盤を管理又は制御するソフトウェアで発生した情報セキュリティインシデントを認知した際の対処手順

遵守事項

⑵　情報システムの基盤を管理又は制御するソフトウェア運用時の対策

⑷　情報セキュリティ管理者は、情報システムの基盤を管理又は制御するソフトウェアを運用・保守する場合は、以下の全てのセキュリティ対策を実施する。

(ｱ)　情報システムの基盤を管理又は制御するソフトウェアのセキュリティを維持するための対策

(ｲ)　脅威や情報セキュリティインシデントを迅速に検知し、対応するための対策

【 基本対策事項 】

＜6.5.1⑵⑷(ｱ)関連＞

6.5.1⑵-1　情報セキュリティ管理者は、情報システムの基盤を管理又は制御するソフトウェアのセキュリティを維持するため、権限設定やアクセス制御、セキュリティ設定が適切であるか定期的な確認をする。

＜6.5.1⑵⑷(ｲ)関連＞

6.5.1⑵-2　情報セキュリティ管理者は、情報システムの基盤を管理又は制御するソフトウェアにおいて、脅威や情報セキュリティインシデントを迅速に検知し、対応するため、以下の全ての対策を実施する。

a)　情報システムの基盤を管理又は制御するソフトウェアの情報セキュリティ水準の維持に関する手順に基づく教育の実施

b)　情報セキュリティインシデントを認知した際の対処手順に基づく訓練

6.6　アプリケーション・コンテンツ

6.6.1　アプリケーション・コンテンツの作成・運用時の対策

目的・趣旨

支払基金では、情報の提供等のサービスのためにアプリケーション・コンテンツを用意し、広く利用に供している。利用者がこれらのアプリケーション・コンテンツを利用する際に、利用者端末の情報セキュリティ水準の低下を招いてしまうことは避けなければならない。支払基金は、アプリケーション・コンテンツの提供に際しても、情報セキュリティ対策を講じておく必要がある。

また、アプリケーション・コンテンツの開発・提供を業務委託する場合については、4.1「業務委託」についても併せて遵守する必要がある。

遵守事項

⑴　アプリケーション・コンテンツの作成に係る運用手順書の整備

⑷　情報セキュリティ責任者は、アプリケーション・コンテンツの提供時に支払基金外の

情報セキュリティ水準の低下を招く行為を防止するための運用手順を「アプリケーション・コンテンツの提供時に基金外の情報セキュリティ水準の低下を招く行為の防止に関する手順書」に整備する。

(b) 役職員等関係者は、アプリケーション・コンテンツの提供に当たり、「アプリケーション・コンテンツの提供時に基金外の情報セキュリティ水準の低下を招く行為の防止に関する手順書」を確認する。

遵守事項

(2) アプリケーション・コンテンツのセキュリティ要件の策定

(a) 情報セキュリティ管理者は、支払基金外の情報システム利用者の情報セキュリティ水準の低下を招かぬよう、アプリケーション・コンテンツについてのセキュリティ要件を定め、仕様に含める。

(b) 役職員等関係者は、アプリケーション・コンテンツの開発・作成を業務委託する場合において、前項に掲げる内容を調達仕様に含める。

【 基本対策事項 】

＜6.6.1(2)(a)関連＞

6.6.1(2)-1 情報セキュリティ管理者は、提供するアプリケーション・コンテンツが不正プログラムを含まないことを確認するために、以下を全て含む対策をセキュリティ要件として仕様に含める。

a) アプリケーション・コンテンツを提供する前に、不正プログラム対策ソフトウェアを用いてスキャンを行い、不正プログラムが含まれていないことを確認する。

b) 業務委託により作成したアプリケーションプログラムを提供する場合には、委託先事業者に、当該アプリケーションの仕様に反するプログラムコードが含まれていないことを確認させる。

6.6.1(2)-2 情報セキュリティ管理者は、提供するアプリケーション・コンテンツが脆弱性を含まないように開発することをセキュリティ要件として仕様に含める。

6.6.1(2)-3 情報セキュリティ管理者は、実行プログラムの形式以外にコンテンツを提供する手段がない場合を除き、実行プログラムの形式でコンテンツを提供しないことをセキュリティ要件として仕様に含める。

6.6.1(2)-4 情報セキュリティ管理者は、電子証明書を用いた署名等、提供するアプリケーション・コンテンツの改ざん等がなく真正なものであることを確認できる手段をアプリケーション・コンテンツの提供先に与えることをセキュリティ要件として仕様に含める。

6.6.1(2)-5 情報セキュリティ管理者は、提供するアプリケーション・コンテンツの利用時

に、脆弱性が存在するバージョンの OS やソフトウェア等の利用を強制するなどの情報セキュリティ水準を低下させる設定変更を、OS やソフトウェア等の利用者に要求することがないよう、アプリケーション・コンテンツの提供方式を定めて開発することをセキュリティ要件として仕様に含める。

6.6.1⑵-6　情報セキュリティ管理者は、サービス利用者その他の者に関する情報が本人の意思に反して第三者に提供されるなど、サービス利用に当たって必須ではない機能がアプリケーション・コンテンツに組み込まれることがないよう、以下を全て含む開発をすることをセキュリティ要件として仕様に含める。

a)　支払基金外のウェブサイト等のサーバへ自動的にアクセスが発生する機能が仕様に反して組み込まれていないことを、HTML ソースを表示させるなどして確認する。必要があって当該機能を含める場合は、当該支払基金外へのアクセスが情報セキュリティ上安全なものであることを確認する。

b)　本来のサービス提供に必要のない支払基金外へのアクセスを自動的に発生させる機能を含めない。

遵守事項

⑶　アプリケーション・コンテンツの開発時の対策

⑷　情報セキュリティ管理者は、ウェブアプリケーションの開発において、セキュリティ要件として定めた仕様に加えて、既知の種類のウェブアプリケーションの脆弱性を排除するための対策を講じる。

【 基本対策事項 】

＜6.6.1⑶⑷関連＞

6.6.1⑶-1　情報セキュリティ管理者は、以下を全て含むウェブアプリケーションの脆弱性を排除する。

a)　SQL インジェクション脆弱性
b)　OS コマンドインジェクション脆弱性
c)　ディレクトリトラバーサル脆弱性
d)　セッション管理の脆弱性
e)　アクセス制御欠如と認可処理欠如の脆弱性
f)　クロスサイトスクリプティング脆弱性
g)　クロスサイトリクエストフォージェリ脆弱性
h)　クリックジャッキング脆弱性
i)　メールヘッダインジェクション脆弱性
j)　HTTP ヘッダインジェクション脆弱性
k)　eval インジェクション脆弱性

l)　レースコンディション脆弱性

m)　バッファオーバーフロー及び整数オーバーフロー脆弱性

n)　サーバサイドリクエストフォージェリ（SSRF）脆弱性

6.6.1⑶-2　情報セキュリティ管理者は、ウェブアプリケーションを運用段階へ移行する前に情報システムの分類に基づき、以下の対策を実施する。

【基本セキュリティ対策】開発したウェブアプリケーションに対して脆弱性診断の実施を検討する。

【追加セキュリティ対策】高度な情報セキュリティ対策が要求される情報システムで実行するウェブアプリケーションに対して、脆弱性診断を実施する。

遵守事項

⑷　アプリケーション・コンテンツの運用時の対策

⒜　情報セキュリティ管理者は、利用者の情報セキュリティ水準の低下を招かぬよう、アプリケーション及びウェブコンテンツの提供方式等を見直す。

⒝　情報セキュリティ管理者は、運用中のアプリケーション・コンテンツにおいて、定期的に脆弱性対策の状況を確認し、脆弱性が発覚した際は必要な措置を講じる。

⒞　情報セキュリティ管理者は、ウェブアプリケーションやウェブコンテンツにおいて、アプリケーションやコンテンツの改ざんを検知するための措置を講じる。

【 基本対策事項 】

＜6.6.1⑷⒜関連＞

6.6.1⑷-1　情報セキュリティ管理者は、利用者に強制する OS やソフトウェア等のサポート状況や脆弱性情報等を確認し、サポートが終了する又は脆弱性が存在するバージョンの OS やソフトウェア等の利用を強制するなど情報セキュリティ水準を低下させる設定変更等を、OS やソフトウェア等の利用者に要求することがないよう、アプリケーション及びウェブコンテンツの提供方式等を見直す。

6.6.2　アプリケーション・コンテンツ提供時の対策

目的・趣旨

支払基金では、情報の提供等のサービスのためにウェブサイト等を用意している。これらのサービスは通常インターネットを介して利用するものであるため、そのサービス（クラウドサービス含む。）が実際の支払基金のものであると確認できることが重要である。また、支払基金になりすましたウェブサイトを放置しておくと、支払基金の信用を損なうだけでなく、利用者が不正サイトに誘導され、不正プログラムに感染するおそれがあるため、このような事態への対策を講じる必要がある。

遵守事項

⑴　支払基金ドメイン名の使用

⒜　情報セキュリティ管理者は、支払基金外向けに提供するウェブサイト等が実際の支払基金提供のものであることを利用者が確認できるように、支払基金ドメイン名（ssk.or.jp）を情報システムにおいて使用する。

⒝　役職員等関係者は、支払基金外向けに提供するウェブサイト等の作成を業務委託する場合においては、支払基金ドメイン名を使用するよう調達仕様に含める。

遵守事項

⑵　不正なウェブサイトへの誘導防止

⒜　情報セキュリティ管理者は、利用者が検索サイト等を経由して支払基金のウェブサイトになりすました不正なウェブサイトへ誘導されないよう対策を講じる。

【 基本対策事項 】

＜6.6.2⑵⒜関連＞

6.6.2⑵-1　情報セキュリティ管理者は、支払基金外向けに提供するウェブサイトに対して、以下を例とする検索エンジン最適化措置（SEO 対策）を講じる。

a)　クローラからのアクセスを排除しない。

b)　cookie 機能を無効に設定したブラウザでも正常に閲覧可能とする。

c)　適切なタイトルを設定する。

d)　不適切な誘導を行わない。

6.6.2⑵-2　情報セキュリティ管理者は、支払基金外向けに提供するウェブサイトに関連するキーワードで定期的にウェブサイトを検索し、検索結果に不審なサイトが存在した場合は、速やかにその検索サイト業者へ報告するとともに、不審なサイトへのアクセスを防止するための対策を講じる。

6.6.2⑵-3　情報セキュリティ管理者は、支払基金のウェブサイトなどになりすました不審なウェブサイト等が存在していることの連絡を受け付ける体制を整備するとともに、不審なウェブサイトに対し必要な措置を講じる。

遵守事項

⑶　アプリケーション・コンテンツの告知

⒜　役職員等関係者は、アプリケーション・コンテンツを告知する場合は、告知する対象となるアプリケーション・コンテンツに利用者が確実に誘導されるよう、必要な措置を講じる。

⒝　役職員等関係者は、支払基金外の者が提供するアプリケーション・コンテンツを告知

する場合は、告知する URL 等の有効性を保つ。

【 基本対策事項 】

＜6.6.2(3)(a)関連＞

6.6.2(3)-1　役職員等関係者は、アプリケーション・コンテンツを告知するに当たって、誘導を確実なものとするため、URL 等を用いて直接誘導することを原則とし、検索サイトで指定の検索語を用いて検索することを促す方法その他の間接的な誘導方法を用いる場合であっても、URL 等と一体的に表示する。また、短縮 URL を用いない。

6.6.2(3)-2　役職員等関係者は、アプリケーション・コンテンツを告知するに当たって、URL を二次元コード等に変換して印刷物等に表示して誘導する場合には、当該コードによる誘導先を明らかにするため、アプリケーション・コンテンツの内容に係る記述を当該コードと一体的に表示する。

＜6.6.2(3)(b)関連＞

6.6.2(3)-3　役職員等関係者は、支払基金外の者が提供するアプリケーション・コンテンツを告知する場合は、告知する URL 等の有効性を保つために以下の全ての措置を講じる。

a)　告知するアプリケーション・コンテンツを管理する組織名を明記する。

b)　告知するアプリケーション・コンテンツの所在場所の有効性（リンク先の URL のドメイン名の有効期限等）を確認した時期又は有効性を保証する期間について明記する。

第 7 部　情報システムのセキュリティ要件

7.1　情報システムのセキュリティ機能

7.1.1　主体認証機能

目的・趣旨

情報又は情報システムへアクセス可能な主体を制限するためには、主体認証機能の導入が必要である。その際、アクセス権限のある主体へのなりすましや脆弱性を悪用した攻撃による不正アクセス行為を防止するための対策を講じることが重要となる。

また、支払基金の情報システムにおいて、国民の皆様に向けてサービスを提供する場合は、国民の皆様が情報システムへのアクセスの主体となることにも留意して、主体認証情報を適切に保護しなければならない。

遵守事項

⑴　主体認証機能の導入

⑻　情報セキュリティ管理者は、情報システムや情報へのアクセス主体を特定し、それが正当な主体であることを検証する必要がある場合、主体の識別及び主体認証を行う機能を設ける。

⑼　情報セキュリティ管理者は、支払基金において申請、届出等のオンライン手続を提供する情報システムを構築する場合は、オンライン手続におけるリスクを評価した上で、主体認証に係る要件を策定する。

⑽　情報セキュリティ管理者は、主体認証を行う情報システムにおいて、主体認証情報の漏えい等による不正行為を防止するための措置及び不正な主体認証の試行に対抗するための措置を講じる。

【 基本対策事項 】

＜7.1.1⑴⑻関連＞

7.1.1⑴-1　情報セキュリティ管理者は、利用者が正当であることを検証するための主体認証機能を設けるに当たっては、以下を例とする主体認証方式を決定し、導入する。

a)　知識（パスワード等、利用者本人のみが知り得る情報）による認証

b)　所有（電子証明書を格納する IC カード、ワンタイムパスワード生成器、利用者本人のみが所有する機器等）による認証

c)　生体（指紋や静脈等、本人の生体的な特徴）による認証

7.1.1⑴-2　情報セキュリティ管理者は、支払基金内通信回線へリモートアクセスを必要とする主体やインターネット等から直接アクセスが可能なクラウドサービス等

の管理者権限を有する主体など厳格な主体認証が必要な場合、認証の強度として２つ以上の主体認証方式を組み合わせる多要素主体認証方式等の強固な認証技術を用いる。

7.1.1(1)-3　情報セキュリティ管理者は、主体認証情報としてパスワードを使用し、利用者自らがパスワードを設定することを可能とする場合には、辞書攻撃等によるパスワード解析への耐性を考慮し、強固なパスワードに必要な桁数や複雑さを利用者に守らせる機能を設ける。

＜7.1.1(1)(c)関連＞

7.1.1(1)-4　情報セキュリティ管理者は、主体認証を行う情報システムにおいて、主体認証情報の漏えい等による不正なアクセスを防止するため、以下を全て含む措置を講じる。

a)　原則として、機器等において初期値として設定されている識別コードを使用しない。

b)　不要な識別コードを無効にする。

7.1.1(1)-5　情報セキュリティ管理者は、主体認証を行う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、以下を例とする機能を設ける。

a)　利用者が定期的に変更しているか否かを確認する機能

b)　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

c)　利用者が主体認証情報を変更する際に、以前に設定した主体認証情報の再設定を防止する機能

7.1.1(1)-6　情報セキュリティ管理者は、主体認証を行う情報システムにおいて、主体認証情報が第三者に対して明らかにならないよう、以下を全て含む方法を用いて適切に管理する。

a)　主体認証情報を送信又は保存する場合には、その内容を暗号化する。

b)　主体認証情報に対するアクセス制限を設ける。

c)　主体認証情報に対するアクセスに関するログを保存し、アクセスした主体を確認する。

7.1.1(1)-7　情報セキュリティ管理者は、主体認証を行う情報システムにおいて、主体認証情報を他の主体に不正に利用され、又は利用されるおそれを認識した場合の対策として、以下を例とする機能を設ける。

a)　当該主体認証情報及び対応する識別コードの利用を停止する機能

b)　主体認証情報の再設定を利用者に要求する機能

遵守事項

⑵　識別コード及び主体認証情報の管理

⑻　情報セキュリティ管理者は、情報システムにアクセスする全ての主体に対して、識別コード及び主体認証情報を適切に付与し、管理するための措置を講じる。

⑼　情報セキュリティ管理者は、主体が情報システムを利用する必要がなくなった場合は、当該主体の識別コード及び主体認証情報の不正な利用を防止するための措置を速やかに講じる。

【 基本対策事項 】

＜7.1.1⑵⑻関連＞

7.1.1⑵-1　情報セキュリティ管理者は、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付与（発行、更新及び変更を含む。以下遵守事項 7.1.1⑵⑻において同じ。）する。

7.1.1⑵-2　情報セキュリティ管理者は、識別コードの付与に当たっては、以下を例とする措置を講じる。

a)　単一の情報システムにおいて、ある主体に付与した識別コード（共用識別コードを除く。）を別の主体に対して付与することの禁止

b)　主体への識別コードの付与に関する記録を消去する場合の情報セキュリティ管理者からの事前の許可

7.1.1⑵-3　情報セキュリティ管理者は、主体以外の者が識別コード又は主体認証情報を設定する場合に、主体へ安全な方法で主体認証情報を配布するよう、措置を講じる。

7.1.1⑵-4　情報セキュリティ管理者は、識別コード及び知識による主体認証情報を付与された主体に対し、初期設定の主体認証情報（必要に応じて、初期設定の識別コードも）を速やかに変更するよう促す。なお、主体認証情報の変更を確認できる機能がある場合は、変更日時を確認し変更がなされない（使用していない）識別コードについては無効にするなどの措置を講じる。

7.1.1⑵-5　情報セキュリティ管理者は、知識による主体認証方式を用いる場合には、他の情報システムで利用している主体認証情報を設定しないよう主体に注意を促す。

7.1.1⑵-6　情報セキュリティ管理者は、情報システムを利用する主体ごとに識別コードを個別に付与する。ただし、情報セキュリティ管理者の判断の下、やむを得ず共用識別コードを付与する必要がある場合には、利用者を特定できる仕組みを設けた上で、共用識別コードの取扱いに関して以下を例とする対策を講じる。

a)　当該情報システムにおける別途の認証手段を併用する。

b)　入退室管理装置等の物理的認証手段を併用する。

c)　第三者による承認を得てから利用する（その際、共用識別コードを使用したこ

とが通知される仕組みも併せて設ける)。

d) 主体認証情報を知る者を限定する。

＜7.1.1(2)(b)関連＞

7.1.1(2)-7 情報セキュリティ管理者は、主体認証情報の不正な利用を防止するために、主体が情報システムを利用する必要がなくなった場合には、以下を例とする措置を講じる。

a) 当該主体の識別コードを無効にする。

b) 当該主体に交付した主体認証情報格納装置を返還させる。

c) 無効化した識別コードを他の主体に新たに発行することを禁止する。

7.1.2 アクセス制御機能

目的・趣旨

アクセス制御とは、情報システム及び情報へのアクセスを許可する主体を制限することである。複数の主体が情報システムを利用する場合、当該情報システムにおいて取り扱う情報へのアクセスを業務上必要な主体のみに限定することによって、情報漏えい等のリスクを軽減することができると考えられる。

遵守事項

(1) アクセス制御機能の導入

(a) 情報セキュリティ管理者は、情報システムの特性、情報システムが取り扱う情報の格付及び取扱制限等に従い、権限を有する者のみがアクセス制御の設定等を行うことができる機能を設ける。

(b) 情報セキュリティ管理者は、情報システム及び情報へのアクセスを許可する主体が確実に制限されるように、アクセス制御機能を適切に運用する。

【 基本対策事項 】

＜7.1.2(1)(a)関連＞

7.1.2(1)-1 情報セキュリティ管理者は、主体の属性、アクセス対象の属性に基づくアクセス制御の要件を定める。また、情報システムの分類に基づき、以下の対策を実施する。

【基本セキュリティ対策】以下を例とするアクセス制御機能の要件を定める。

a) 利用時間や利用時間帯によるアクセス制御

b) 同一主体による複数アクセスの制限

c) IP アドレスによる端末の制限

d) ネットワークセグメントの分割によるアクセス制御

e)　ファイルに記録された情報へのアクセスを制御するサーバにおいて主体認証を受けたユーザのみが、暗号化されたファイルに記録された情報に対し、与えられた権限の範囲でアクセス可能となる制御

【追加セキュリティ対策】基本セキュリティ対策の実施に加えて、以下を例とするアクセス制御機能を用いることを検討する。

f)　認証・認可の統合管理基盤を用いたアクセス制御

g)　アクセスの要求ごとに、主体等の状況を継続的に認証し認可する仕組みを実現する機能の一部である動的なアクセス制御

＜7.1.2(1)(b)関連＞

7.1.2(1)-2　情報セキュリティ管理者は、主体の属性、アクセス対象の属性に基づくアクセス制御の要件の定期的な確認による見直しをする。

7.1.3　権限の管理

目的・趣旨

情報システムのアクセス制御機能を適切に運用するためには、主体から対象に対するアクセスの権限を適切に設定することが必要である。その際、アクセス権限は最小権限の付与とするため、全てにアクセスできないことを前提に、アクセスの必要がある主体に対してのみ権限を付与し、アクセスの必要のない主体に対しては権限を与えないことを原則とすることが重要である。また、情報に対して権限を付与する場合も同様に、知る必要のある主体に対してのみ権限を付与し、知る必要のない主体に対しては権限を与えないことを原則とすることが重要である。なお、権限の管理が不適切になると、情報又は情報システムへ不正アクセスされるおそれが生じる。

また、情報システムの管理機能として、一般的に管理者権限にはあらゆる操作が許可される特権が付与されている。当該特権が悪意ある第三者等に入手された場合、主体認証情報のみならず特権アクセスが可能な情報等の漏えい、改ざん、さらには情報システムや情報を破壊することを目的とした不正プログラムによって業務継続への影響もあり得る。また、これらの不正アクセスや不正プログラム等を検知又は防止するための設定情報等が不正に変更されることによる情報セキュリティ機能の無効化等が懸念されることから、限られた主体のみに管理者権限が付与されることが重要である。

遵守事項

(1)　権限の管理

(a)　情報セキュリティ管理者は、主体から対象に対するアクセスの権限を必要最小限の範囲で適切に設定するよう、措置を講じる。

(b)　情報セキュリティ管理者は、管理者権限の特権を持つ主体の識別コード及び主体認

証情報が、悪意ある第三者等によって窃取された際の被害を最小化するための措置及び、内部からの不正操作や誤操作を防止するための措置を講じる。

(c) 情報セキュリティ管理者は、主体から対象に対する不要なアクセス権限が付与されていないか定期的に確認する。

【 基本対策事項 】

＜7.1.3(1)(a)関連＞

7.1.3(1)-1 情報セキュリティ管理者は、初期値として利用可能な管理者権限を有する識別コードには、管理者権限を付与しない又は無効化にする。

＜7.1.3(1)(b)関連＞

7.1.3(1)-2 情報セキュリティ管理者は、主体に対して管理者権限を付与する場合、主体の識別コード及び主体認証情報が、第三者等によって窃取された際の被害を最小化するため、以下を例とする措置を講じる。

a) 業務上必要な場合に限定する

b) 必要最小限の権限のみ付与する

c) 管理者権限を行使できる端末を情報セキュリティ管理担当者等の専用の端末とする

7.1.3(1)-3 情報セキュリティ管理者は、管理者権限を有する識別コードの利用は権限を必要とする業務に限定し、一般の業務として使用させない。

7.1.4 ログの取得・管理

目的・趣旨

情報システムにおけるログとは、システムの動作履歴、利用者のアクセス履歴、通信履歴その他運用管理等に必要な情報が記録されたものであり、悪意ある第三者等による不正侵入や不正操作等の情報セキュリティインシデント及びその予兆を検知するための重要な材料となるものである。また、情報システムに係る情報セキュリティ上の問題が発生した場合には、当該ログは、事後の調査の過程で、問題を解明するための重要な材料となる。したがって、情報システムにおいては、仕様どおりにログが取得され、また、改ざんや消失等が起こらないよう、ログが適切に保全されなければならない。

遵守事項

(1) ログの取得・管理

(a) 情報セキュリティ管理者は、情報システムにおいて、情報システムが正しく利用されていることの検証及び不正侵入、不正操作等がなされていないことの検証を行うために必要なログを取得する。

⑹　情報セキュリティ管理者は、情報システムにおいて、その特性に応じてログを取得する目的を設定した上で、ログを取得する対象の機器等、ログとして取得する情報項目、ログの保存期間、要保護情報の観点でのログ情報の取扱方法、及びログが取得できなくなった場合の対処方法等について定め、適切にログを管理する。

⑹　情報セキュリティ管理者は、情報システムにおいて、取得したログを定期的に点検又は分析する機能を設け、悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施する。

【 基本対策事項 】

＜7.1.4(1)(a)関連＞

7.1.4(1)-1　情報セキュリティ管理者は、情報システムに含まれる構成要素（サーバ装置・端末等）のうち、時刻設定が可能なものについては、情報システムにおいて基準となる時刻に、当該構成要素の時刻を同期させ、ログに時刻情報も記録されるよう、設定する。

＜7.1.4(1)(b)関連＞

7.1.4(1)-2　情報セキュリティ管理者は、所管する情報システムの特性に応じてログを取得する目的を設定し、以下を例とする、ログとして取得する情報項目を定め、管理する。

a)　事象の主体（人物又は機器等）を示す識別コード
b)　識別コードの発行等の管理記録
c)　情報システムの操作記録
d)　事象の種類
e)　事象の対象
f)　正確な日付及び時刻
g)　試みられたアクセスに関わる情報
h)　電子メールのヘッダ情報及び送信内容
i)　通信パケットの内容
j)　操作する者、監視する者、保守する者等への通知の内容

7.1.4(1)-3　情報セキュリティ管理者は、取得したログに対する、不正な消去、改ざん及びアクセスを防止するため、適切なアクセス制御を含む、ログ情報の保全方法を定める。

＜7.1.4(1)(c)関連＞

7.1.4(1)-4　情報セキュリティ管理者は、取得したログ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、情報システムの分類に応じて以下の対策を実施する。

【基本セキュリティ対策】以下を例とする当該作業を支援する機能を導入する。

a) ログ情報をソフトウェア等により集計し、時系列で表示し、報告書を生成するなどの作業の自動化機能

【追加セキュリティ対策】基本セキュリティ対策の実施に加えて、以下を例とする当該作業を支援する機能の導入を検討する。

b) リアルタイムでのログの調査・分析を行うための機能

7.1.5 暗号・電子署名

目的・趣旨

情報システムで取り扱う情報の漏えい、改ざん等を防ぐための手段として、暗号と電子署名は有効であり、情報システムにおける機能として適切に実装することが求められる。

暗号化機能及び電子署名機能を導入する際は、使用する暗号アルゴリズム及び鍵長に加え、それを用いた暗号プロトコルが適切であること、運用時に当該アルゴリズム又は鍵長が危殆化した場合や当該プロトコルに脆弱性が確認された場合等の対処方法及び関連する鍵情報の適切な管理等を併せて考慮することが必要となる。

遵守事項

(1) 暗号化機能・電子署名機能の導入

(a) 情報セキュリティ管理者は、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、以下の全ての措置を講じる。

(ｱ) 要機密情報を取り扱う情報システムについては、暗号化を行う機能の必要性の有無を検討し、必要があると認めたときは、当該機能を設ける。

(ｲ) 要保全情報を取り扱う情報システムについては、電子署名の付与及び検証を行う機能を設ける必要性の有無を検討し、必要があると認めたときは、当該機能を設ける。

(b) 情報セキュリティ管理者は、暗号技術検討会及び関連委員会（CRYPTREC）により安全性及び実装性能が確認された「電子政府推奨暗号リスト」に基づき、情報システムで使用する暗号及び電子署名のアルゴリズム及び鍵長並びにそれらを利用した安全なプロトコルを定める。また、その運用方法について、実施手順を定める。

(c) 情報セキュリティ管理者は、支払基金における暗号化及び電子署名のアルゴリズム、鍵長及び運用方法に、電子署名を行うに当たり、電子署名の目的に合致し、かつ適用可能な公的な公開鍵基盤が存在する場合はそれを使用するなど、目的に応じた適切な公開鍵基盤を使用するように定める。

【 基本対策事項 】

＜7.1.5(1)(a)関連＞

7.1.5(1)-1 情報セキュリティ管理者は、暗号化又は電子署名を行う情報システムにおい

て、以下を例とする措置を講じる。

a) 情報システムのコンポーネント（部品）として、暗号モジュールを交換することが可能な構成とする。

b) 複数のアルゴリズム、鍵長及びそれに基づいた安全なプロトコルを選択することが可能な構成とする。

c) 選択したアルゴリズム及び鍵長がソフトウェア及びハードウェアへ適切に実装されており、かつ、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それに対応する主体認証情報等が安全に保護されることを確実にするため、「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。

d) 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は、耐タンパ性を有する暗号モジュールへ格納する。

e) 機微な情報のやり取りを行う情報システムを新規に構築する場合は、安全性に実績のあるプロトコルを選択し、長期的な秘匿性を保証する観点を考慮する。

＜7.1.5(1)(b)関連＞

7.1.5(1)-2 情報セキュリティ管理者は、役職員等関係者が暗号や電子署名を利用する場合、あるいは情報システムの新規構築や更新に伴い、暗号化又は電子署名を導入する場合において、情報システムで使用するアルゴリズム及び鍵長並びにそれらを利用した安全なプロトコルを、「電子政府推奨暗号リスト」に基づき定める。

7.1.5(1)-3 情報セキュリティ管理者は、基本対策事項 7.1.5(1)-2 で定めた事項の運用方法について、以下を全て含めて実施手順として定める。

a) 暗号化及び電子署名に使用するアルゴリズム又は鍵長が危殆化した場合又はそれらを利用した安全なプロトコルに脆弱性が確認された場合を想定した緊急対応手順を定める。

b) 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、管理手順を定める。

遵守事項

(2) 暗号化・電子署名に係る管理

(a) 情報セキュリティ管理者は、暗号及び電子署名を適切な状況で利用するため、以下の全ての措置を講じる。

(ｱ) 電子署名の付与を行う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、署名検証者へ安全な方法で提供する。

(ｲ) 暗号化を行う情報システム又は電子署名の付与若しくは検証を行う情報システムにおいて、暗号化又は電子署名のために選択されたアルゴリズム及び鍵長の危殆化及びプロトコルの脆弱性に関する情報を定期的に入手し、必要に応じて、役職員等

関係者と共有を図る。

【 基本対策事項 】

＜7.1.5(2)(a)(ｱ)関連＞

7.1.5(2)-1　情報セキュリティ管理者は、署名検証者が、電子署名の正当性を容易に検証するための情報を入手できるよう、以下を例とする方法により、当該情報の提供を可能とする。

a)　信頼できる機関による電子証明書の提供

b)　支払基金の窓口での電子証明書の提供

7.1.6　監視機能

目的・趣旨

情報システムにおける情報セキュリティインシデントや不正利用等の速やかな認知や、情報セキュリティ対策の実効性を確認するためには、適切に監視機能を実装し、運用することが重要である。また、監視機能の実装に当たっては、情報システムの特性や当該情報システムで取り扱う情報の格付等を踏まえて、監視対象や監視内容を定める必要がある。

遵守事項

(1)　監視機能の導入・運用

(a)　情報セキュリティ管理者は、情報システム運用時の監視に係る運用管理機能要件を策定し、監視機能を実装する。

(b)　情報セキュリティ管理者は、情報システムの運用において、情報システムに実装された監視機能を適切に運用する。

(c)　情報セキュリティ管理者は、新たな脅威の出現、運用の状況等を踏まえ、情報システムにおける監視の対象や手法を定期的に見直す。

【 基本対策事項 】

＜7.1.6(1)(a)(c)関連＞

7.1.6(1)-1　情報セキュリティ管理者は、監視のために必要な機能について、以下を例とする機能を調達仕様書等に明記する。

a)　支払基金外と通信回線で接続している箇所における外部からの不正アクセスやサービス不能攻撃を監視する機能

b)　不正プログラム感染や踏み台に利用されること等による支払基金外への不正な通信を監視する機能

c)　端末等の組織内ネットワークの末端に位置する機器及びサーバ装置において

不正プログラムの挙動を監視する機能

d) 支払基金内通信回線への端末の接続を監視する機能

e) 端末への外部電磁的記録媒体の挿入を監視する機能

f) サーバ装置等の機器の動作を監視する機能

g) ネットワークセグメント間の通信を監視する機能

7.1.6(1)-2 情報セキュリティ管理者は、暗号化された通信データを監視のために復号することの要否を判断し、要すると判断した場合は、当該通信データを復号する機能及び必要な場合はこれを再暗号化する機能を調達仕様書等に明記する。

＜7.1.6(1)(b)関連＞

7.1.6(1)-3 情報セキュリティ管理者は、情報システムのセキュリティ監視について、以下の内容を全て含む監視手順を定め、適切に監視運用する。

a) 監視するイベントの種類や重要度

b) 監視体制

c) 監視状況の報告手順や重要度に応じた報告手段

d) 情報セキュリティインシデントの可能性を認知した場合の報告手順

e) 監視運用における情報の取扱い（機密性の確保）

7.1.6(1)-4 【追加セキュリティ対策】情報セキュリティ管理者は、情報システム運用時の監視において、SOC や NOC 等のセキュリティ監視を専門の外部事業者に業務委託することを検討する。

7.2 情報セキュリティの脅威への対策

7.2.1 ソフトウェアに関する脆弱性対策

目的・趣旨

支払基金の情報システムに対する脅威としては、第三者が情報システムに侵入し支払基金の重要な情報を窃取・破壊する、第三者が過剰な負荷をかけ情報システムを停止させるなどの攻撃を受けることが想定される。特に個人情報等の重要な情報の漏えい等が発生した場合、国民の皆様等に多大な影響を及ぼすとともに支払基金に対する社会的な信用が失われる。

このような攻撃では、情報システムを構成するサーバ装置、端末及び通信回線装置のソフトウェアの脆弱性を悪用されることが多く見受けられる。したがって、支払基金の情報システムにおいては、ソフトウェアに関する脆弱性について、迅速かつ適切に対処することが求められる。

なお、情報システムを構成するハードウェアに関しても、同様に脆弱性が存在する場合があるので、5.2.2「情報システムの調達・構築」の規定も参照し、必要な対策を講じる必要がある。

遵守事項

⑴　ソフトウェアに関する脆弱性対策の実施

⒜　情報セキュリティ管理者は、サーバ装置、端末及び通信回線装置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脆弱性についての対策を実施する。

⒝　情報セキュリティ管理者は、公開された脆弱性の情報がない段階において、サーバ装置、端末及び通信回線装置上でとり得る対策がある場合は、当該対策を実施する。

⒞　情報セキュリティ管理者は、サーバ装置、端末及び通信回線装置上で利用するソフトウェアにおける脆弱性対策の状況を定期的及び適時に確認する。

⒟　情報セキュリティ管理者は、原則として、最新のセキュリティパッチを適用するものとし、脆弱性対策の状況の定期的な確認により、脆弱性対策が講じられていない状態が確認された場合並びにサーバ装置、端末及び通信回線装置上で利用するソフトウェアに関連する脆弱性情報を入手した場合には、セキュリティパッチの適用又はソフトウェアのバージョンアップ等による情報システムへの影響を考慮した上で、ソフトウェアに関する脆弱性対策計画を策定し、措置を講じる。

【 基本対策事項 】

＜7.2.1⑴⒜関連＞

7.2.1⑴-1　情報セキュリティ管理者は、サーバ装置、端末及び通信回線装置の設置又は運用開始時に以下の対策を実施する。

【基本セキュリティ対策】インターネット向けにサービスを公開しているサーバ装置や直接インターネットから到達可能なサーバ装置、端末及び通信回線装置に対し脆弱性診断を実施する。また、その他のサーバ装置、端末及び通信回線装置については、情報システムの分類や保有する情報、システム特性等を踏まえ、脆弱性診断の実施を検討する。

【追加セキュリティ対策】サーバ装置、端末及び通信回線装置に対し脆弱性診断を実施する。また、脆弱性診断の実施に当たっては、ペネトレーションテスト、TLPT（脅威ベースのペネトレーションテスト）等の高度な脆弱性診断の実施を検討する。

＜7.2.1⑴⒜⒞関連＞

7.2.1⑴-2　情報セキュリティ管理者は、対象となるソフトウェアの脆弱性に関して、以下を全て含む情報を適宜入手する。

a)　脆弱性の原因

b)　影響範囲

c)　対策方法

d) 脆弱性を悪用する不正プログラムの流通状況

7.2.1(1)-3 情報セキュリティ管理者は、利用するソフトウェアはサポート期間を考慮して選定し、サポートが受けられないソフトウェアは利用しない。

7.2.1(1)-4 情報セキュリティ管理者は、構成要素ごとにソフトウェアのバージョン等を把握し、当該ソフトウェアの脆弱性の有無を確認する。

7.2.1(1)-5 【追加セキュリティ対策】情報セキュリティ管理者は、情報システムを構成する機器へのセキュリティパッチの適時の適用を前提とした運用設計を行う。

＜7.2.1(1)(c)関連＞

7.2.1(1)-6 【追加セキュリティ対策】情報セキュリティ管理者は、サーバ装置、端末及び通信回線装置の運用時に、定期的な脆弱性診断（ペネトレーションテスト、TLPT 等の高度な脆弱性診断を含む）の実施を検討する。

7.2.1(1)-7 情報セキュリティ管理者は、脆弱性対策の状況を確認する間隔を、可能な範囲で短くする。

＜7.2.1(1)(d)関連＞

7.2.1(1)-8 情報セキュリティ管理者は、ネットワーク境界にある通信回線装置や認証サーバ、要機密情報を保有するサーバ等のサイバーセキュリティリスクが高い機器等に対しては、原則、セキュリティパッチの適用又はソフトウェアのバージョンアップ等の措置を講じる。リスク評価結果を踏まえ措置を講じないと判断した場合には、リスク評価結果の記録を残す。

7.2.1(1)-9 情報セキュリティ管理者は、ソフトウェアに関する脆弱性対策計画を策定する場合には、以下の全ての事項について判断する。

a) 対策の必要性

b) 対策方法。この際、自動でソフトウェアを更新する機能を有する IT 資産管理ソフトウェアを導入するなどにより、効率的に脆弱性対策を実施する手法をあらかじめ決定する。

c) 対策方法が存在しないゼロデイと呼ばれる状態の場合又は対策が完了するまでの期間に対する一時的な回避方法

d) 対策方法又は回避方法が情報システムに与える影響

e) 対策の実施予定時期

f) 対策試験の必要性

g) 対策試験の方法

h) 対策試験の実施予定時期

7.2.1(1)-10 情報セキュリティ管理者は、脆弱性対策が計画どおり実施されていることについて、実施予定時期の経過後、遅滞なく確認する。

7.2.1(1)-11 情報セキュリティ管理者は、脆弱性対策を実施する場合には、少なくとも以下の全ての事項を記録し、これらの事項のほかに必要事項があれば適宜記録す

る。

a) 実施日

b) 実施内容

c) 実施者

7.2.1(1)-12 情報セキュリティ管理者は、セキュリティパッチ、バージョンアップソフトウェア等の脆弱性を解決するために利用されるファイルは、信頼できる方法で入手し、完全性を検証する。

7.2.2 不正プログラム対策

目的・趣旨

情報システムが不正プログラムに感染した場合、情報システムが破壊される脅威や、当該情報システムに保存される重要な情報が外部に漏えいする脅威が想定される。さらには、不正プログラムに感染した情報システムは、他の情報システムに感染を拡大させる、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、標的型攻撃における拠点として利用されるなどが考えられ、当該情報システム以外にも被害を及ぼすおそれがある。このような事態を未然に防止するため、不正プログラムへの対策を適切に実施することが必要である。

遵守事項

(1) 不正プログラム対策の実施

(a) 情報セキュリティ管理者は、サーバ装置及び端末に不正プログラム対策ソフトウェア等を導入する。

(b) 情報セキュリティ管理者は、想定される不正プログラムの感染経路の全てにおいて、不正プログラム対策ソフトウェア等により対策を講じる。

(c) 情報セキュリティ管理者は、不正プログラム対策の状況を適宜把握し、必要な対処を行う。

【 基本対策事項 】

＜7.2.2(1)(a)関連＞

7.2.2(1)-1 情報セキュリティ管理者は、不正プログラム対策ソフトウェア等の導入に当たり、既知及び未知の不正プログラムの検知及びその実行の防止の機能を有するソフトウェアを導入する。

7.2.2(1)-2 情報セキュリティ管理者は、不正プログラム対策ソフトウェア等が常に最新の状態となるように構成する。

7.2.2(1)-3 情報セキュリティ管理者は、不正プログラム対策ソフトウェア等に定義ファ

イルを用いる場合、その定義ファイルが常に最新の状態となるように構成する。

7.2.2(1)-4　情報セキュリティ管理者は、不正プログラム対策ソフトウェア等の設定変更権限については、情報セキュリティ管理担当者が一括管理し、システム利用者に当該権限を付与しない。

7.2.2(1)-5　情報セキュリティ管理者は、不正プログラム対策ソフトウェア等について、定期的に全てのファイルを対象としたスキャンを実施するよう構成する。

＜7.2.2(1)(b)関連＞

7.2.2(1)-6　情報セキュリティ管理者は、想定される全ての感染経路を特定し、不正プログラム対策ソフトウェア等の導入による感染の防止、端末の接続制限及び機能の無効化等による感染拡大の防止等の必要な対策を行う。

7.2.2(1)-7　【追加セキュリティ対策】情報セキュリティ管理者は、EDR ソフトウェア等を利用し、端末やサーバ装置（エンドポイント）の活動を監視し、感染したおそれのある装置を早期にネットワークから切り離す機能の導入を検討する。

＜7.2.2(1)(c)関連＞

7.2.2(1)-8　情報セキュリティ管理者は、不正プログラム対策の実施を徹底するため、以下を例とする不正プログラム対策に関する状況を把握し、必要な対処を行う。

a)　不正プログラム対策ソフトウェア等の導入状況

b)　不正プログラム対策ソフトウェア等の定義ファイルの更新状況

7.2.3　サービス不能攻撃対策

目的・趣旨

インターネットからアクセスを受ける情報システムに対する脅威としては、第三者からサービス不能攻撃を受け、利用者がサービスを利用できなくなることが想定される。このため、支払基金の情報システムのうち、インターネットからアクセスを受けるものについては、サービス不能攻撃を想定し、システムの可用性を維持するための対策を実施する必要がある。近年ではインターネットに接続されたいわゆる IoT 機器で構成されたボットネットによる大規模な攻撃や、専門的な技術や設備がなくても攻撃を行うことのできる DDoS 代行サービスの存在も知られており、より一層の警戒が必要となっている。

遵守事項

(1)　サービス不能攻撃対策の実施

(a)　情報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（インターネットからアクセスを受ける情報システムに限る。以下本条において同じ。）については、サービス提供に必要なサーバ装置、端末及び通信回線装置が装備している機能又は民間事業者等が提供する手段を用いてサービス不能攻撃への対策を行う。

(b) 情報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、サービス不能攻撃を受けた場合の影響を最小とする手段を備えた情報システムを構築する。

(c) 情報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、サービス不能攻撃を受けるサーバ装置、端末、通信回線装置又は通信回線から監視対象を特定し、監視する。

【 基本対策事項 】

＜7.2.3(1)(a)関連＞

7.2.3(1)-1 情報セキュリティ管理者は、サーバ装置、端末及び通信回線装置について、サービス不能攻撃に対抗するための以下の機能を設けている場合は、これらを有効にしてサービス不能攻撃に対処する。

a) パケットフィルタリング機能

b) 3-way handshake 時のタイムアウトの短縮

c) 各種 Flood 攻撃への防御

d) アプリケーションゲートウェイ機能

7.2.3(1)-2 情報セキュリティ管理者は、以下を例とするサービス不能攻撃への対策を実施する。

【基本セキュリティ対策】以下を例とする対策を実施する

a) サービス不能攻撃の影響を排除又は低減するための専用の対策装置やサービスの導入

b) サーバ装置、端末及び通信回線装置及び通信回線の冗長化

【追加セキュリティ対策】基本セキュリティ対策に加え、以下を例とする対策を検討する。

c) インターネットに接続している通信回線の提供元となる事業者が別途提供する、サービス不能攻撃に係る通信の遮断等の対策

d) コンテンツデリバリーネットワーク（CDN）サービスの利用

＜7.2.3(1)(b)関連＞

7.2.3(1)-3 情報セキュリティ管理者は、サービス不能攻撃を受けた場合を想定し、直ちに情報システムを外部ネットワークから遮断する、又は通信回線の通信量を制限するなどの手段を有する情報システムを構築する。

7.2.3(1)-4 情報セキュリティ管理者は、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を想定し、攻撃への対処を効率的に実施できる手段の確保について検討する。

＜7.2.3(1)(c)関連＞

7.2.3(1)-5 情報セキュリティ管理者は、特定した監視対象について、監視方針及び監視方法を定める。

7.2.3(1)-6　情報セキュリティ管理者は、監視対象の監視記録の保存期間を定め、監視記録を保存する。

7.2.3(1)-7　情報セキュリティ管理者は、監視対象の平常時の負荷の状況を把握し、監視においてこれを著しく逸脱したと判断する目安を定める。

7.2.3(1)-8　情報セキュリティ管理者は、監視において、前項で定めた目安を超える負荷の状況が確認された場合は、サービス不能攻撃の可能性が排除される場合を除き、速やかに遵守事項 2.2.4(1)(a)で定める報告手順に基づき CSIRT に報告する。

7.2.3(1)-9　【追加セキュリティ対策】情報セキュリティ管理者は、脅威動向等の脅威情報を収集し、サービス不能攻撃を受ける可能性が予見される場合は、必要に応じて、CSIRT 等の関係者に通知する。

7.2.4　標的型攻撃対策

目的・趣旨

標的型攻撃とは、特定の組織に狙いを絞り、その組織の業務習慣等内部情報について事前に入念な調査を行った上で、様々な攻撃手法を組み合わせ、その組織に最適化した方法を用いて、執拗に行われる攻撃である。典型的なものとしては、組織の情報システム内に何らかの手法で不正侵入・潜入し、権限の奪取等を通じて侵入範囲を拡大、重要な情報を窃取又は破壊する攻撃活動が考えられる。これら一連の攻撃活動は、未知の手段も用いて実行されることもあり、完全に検知及び防御することは困難との前提に立った対策が必要である。

標的型攻撃への対策としては、情報システム内部への侵入を低減する対策（入口対策）に加え、内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる（内部対策)、及び外部との不正通信を検知して対処する対策（出口対策）からなる、多重防御の情報セキュリティ対策体系によって、標的型攻撃に備える必要がある。

なお、近年は、組織に対する直接的な攻撃だけでなく、業務委託先等の関連組織への間接的な攻撃も確認されており、より幅広い対策の検討が求められる。

遵守事項

(1)　標的型攻撃対策の実施

(a)　情報セキュリティ管理者は、情報システムにおいて、標的型攻撃による組織内部への侵入を低減する対策（入口対策）を講じる。

(b)　情報セキュリティ管理者は、情報システムにおいて、内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、及び外部との不正通信を検知して対処する対策（内部対策及び出口対策）を講じる。

【 基本対策事項 】

＜7.2.4(1)(a)関連＞

7.2.4(1)-1　情報セキュリティ管理者は、サーバ装置及び端末について、組織内部への侵入を低減するため、以下を例とする対策を行う。

a)　不要なサービス機能やアプリケーションを削除又は停止する。

b)　不審なプログラムが実行されないよう設定する。

c)　パーソナルファイアウォール等を用いて、サーバ装置及び端末に入力される通信及び出力される通信を必要最小限に制限する。

d)　サービスは原則「標準ユーザ」の権限で実行する。

7.2.4(1)-2　情報セキュリティ管理者は、CD-R 等の外部電磁的記録媒体を利用した、組織内部への侵入を低減するため、以下を例とする対策を行う。

a)　出所不明の外部電磁的記録媒体を組織内ネットワーク上の端末に接続させない。接続する外部電磁的記録媒体を事前に特定しておく。

b)　外部電磁的記録媒体をサーバ装置及び端末に接続する際、不正プログラム対策ソフトウェアを用いて検査する。

c)　サーバ装置及び端末について、自動再生（オートラン）機能や自動実行機能を無効化する。

d)　サーバ装置及び端末について、使用を想定しない USB ポートを無効化する。

e)　組織内ネットワーク上の端末に対する外部電磁的記録媒体の接続を制御及び管理するための製品やサービスを導入する。

＜7.2.4(1)(b)関連＞

7.2.4(1)-3　情報セキュリティ管理者は、情報窃取や破壊等の攻撃対象となる蓋然性が高いと想定される、認証サーバやファイルサーバ等の重要なサーバについて、以下を全て含む対策を行う。

a)　重要サーバについては、組織内ネットワークを複数セグメントに区切った上で、重要サーバ類専用のセグメントに設置し、他のセグメントからのアクセスを必要最小限に限定する。インターネットに接続する必要がある場合は、必要最小限のプロトコルやポートのみに限定し、インターネットに接続する必要がない場合はインターネット分離を行う。

b)　認証サーバについては、利用者端末から管理者権限を狙う攻撃（辞書攻撃、ブルートフォース攻撃等）を受けることを想定した対策を講じる。

7.2.4(1)-4　情報セキュリティ管理者は、端末の管理者権限アカウントについて、以下を全て含む対策を行う。

a)　不要な管理者権限アカウントを削除する。

b)　管理者権限アカウントのパスワードは、容易に推測できないものに設定する。

7.2.4(1)-5　【追加セキュリティ対策】情報セキュリティ管理者は、以下を例とする内部対

策及び出口対策を行う。

a) プロキシサーバ等により、C&C サーバ等への不正な通信を監視し、遮断する。

b) 情報システムの管理者が利用する情報システム管理用の専用端末を用意し、他のセグメントと分離した運用管理セグメントを構築し、当該セグメントにシステム管理用の専用端末を接続する。

c) 認証サーバに管理者権限でログインできる端末をシステム管理用の専用端末に制限する。

d) 一般利用者が利用する端末間でのファイル共有機能を停止する又は一般利用者が利用する端末間の直接通信を遮断する。

7.3 ゼロトラストアーキテクチャ

7.3.1 動的なアクセス制御の実装時の対策

目的・趣旨

従来、組織内ネットワーク上の情報資産の保護においては、インターネット等の支払基金外通信回線と組織内ネットワークである支払基金内通信回線との境界にファイアウォール等を設置し防御を行い、組織内のネットワークに一定の信頼を置く「境界モデル」の対策が一般的であった。クラウドサービスの普及や、テレワークによる業務システム環境の変化等により、組織内の情報資産を取り巻く脅威は変化しており、このような新たな環境における脅威に対して境界モデルによる防御だけでは十分なセキュリティ対策の実施は困難になりつつある。特に、境界内部に設置されたサーバ装置等の情報資産について、境界での対策を過信しており、内部に侵入された際の横断的侵害（横方向の侵害やラテラルムーブメントとも呼称される）への情報セキュリティ対策が不足している可能性がある。

ゼロトラストアーキテクチャは、組織内外を問わずネットワークは常に侵害されているものであるとの前提のもと、情報資産を保護し、情報セキュリティリスクの最小化を図るための情報セキュリティ対策における論理的・構造的な考え方である。また、ゼロトラストアーキテクチャは中長期的な支払基金システムに係るライフサイクル全体にわたって適用されるものであり、特定の実装やソリューションを指すものではない。

ゼロトラストアーキテクチャに基づく情報資産の保護策の 1 つとして、情報資産へのアクセスの要求ごとに、アクセスする主体や、アクセス元・アクセス先となる機器、ソフトウェア、サービス、ネットワークなどの状況を継続的に認証し、認可する仕組みが考えられる。本款では、このような仕組みを実現する機能の一部と考えられる「動的なアクセス制御」を実装する場合に特に必要な対策について記載する。

動的なアクセス制御の機能を実装する場合は、本款以外に 7.1.1「主体認証機能」で定める主体認証機能の導入、7.1.2「アクセス制御機能」で定めるアクセス制御機能の導入、7.1.3「権限の管理」で定める権限の管理に係る遵守事項についても併せて遵守する必要がある

が、既存の情報システムの構成に動的なアクセス制御を実装する場合は、既存の情報システムの構成やアクセス制御に用いるソフトウェアなどを見直していくことが重要となる。

遵守事項

⑴　動的なアクセス制御における責任者の設置

(a)　情報セキュリティ責任者は、複数の情報システム間で動的なアクセス制御を実装する場合は、複数の情報システム間で横断的な対策の企画・推進・運用に関する事務の責任者として、情報セキュリティ管理者を選任する。

遵守事項

⑵　動的なアクセス制御の導入方針の検討

(a)　情報セキュリティ管理者は、動的なアクセス制御を導入する場合、動的アクセス制御の対象とする情報システムのリソースを識別し、動的なアクセス制御の導入方針を定める。

【 基本対策事項 】

＜7.3.1⑵(a)関連＞

7.3.1⑵-1　情報セキュリティ管理者は、動的なアクセス制御の対象とする情報システムの範囲や優先度を検討し、動的なアクセス制御の対象とする情報システムを特定する。

7.3.1⑵-2　情報セキュリティ管理者は、特定した情報システムの利用形態等を基に以下を例とする区分で情報システムのリソースを識別する。

a)　ユーザアカウント

b)　機器

c)　アプリケーション

d)　データ

7.3.1⑵-3　情報セキュリティ管理者は、識別したリソースを基にアクセスパターンを整理する。

7.3.1⑵-4　情報セキュリティ管理者は、整理したアクセスパターンに対するリスク評価を実施し、動的なアクセス制御を実装するアクセスパターンを特定する。

遵守事項

⑶　動的なアクセス制御の実装時の対策

(a)　情報セキュリティ管理者は、動的なアクセス制御の実装に当たり、リソースの信用情報の変化に応じて動的にアクセス制御を行うためのアクセス制御ポリシー（以下「アクセス制御ポリシー」という。）を作成する。

⑹　情報セキュリティ管理者は、アクセス制御ポリシーに基づき、動的なアクセス制御を行う。

【 基本対策事項 】

＜7.3.1⑶⑷関連＞

7.3.1⑶-1　情報セキュリティ管理者は、動的なアクセス制御を実現するための構成について検討する。

7.3.1⑶-2　情報セキュリティ管理者は、動的なアクセス制御の実装に当たり、動的なアクセス制御に活用する以下を例とするリソースの信用情報を整理する。

a)　ユーザアカウント

b)　機器

c)　アプリケーション

d)　データ

7.3.1⑶-3　情報セキュリティ管理者は、リソースの信用情報の変化に応じてアクセス制御ポリシーを作成する。

＜7.3.1⑶⑹関連＞

7.3.1⑶-4　情報セキュリティ管理者は、リソースの信用情報の変化を踏まえて、リソースの信用情報を収集する頻度・機会について定める。

7.3.1⑶-5　情報セキュリティ管理者は、リソースの認証・認可において、アクセス制御ポリシーに基づき、セッションが確立してない操作ごとにアクセス制御を行う。

7.3.2　動的なアクセス制御の運用時の対策

目的・趣旨

テレワークの拡大やクラウド・バイ・デフォルト原則によって、リソースの利用形態は日々変化していることを踏まえ、動的なアクセス制御の運用時には、実装時に検討した対策内容が正しく機能しているかどうか確認し、必要に応じてアクセス制御ポリシーを見直すことが重要である。また、動的なアクセス制御の前提となるリソースの信用情報を収集する中でリスクが検出された場合は、当該リスクを低減するための措置が必要となる。

本款では、支払基金が動的なアクセス制御を運用する場合に特に必要な対策についてのみ規定するため、本款以外に 7.1.1「主体認証機能」で定める識別コード・主体認証情報の管理、7.1.2「アクセス制御機能」で定めるアクセス制御の適切な運用、7.1.3「権限の管理」で定める権限の管理に係る遵守事項についても併せて遵守する必要がある。

遵守事項

⑴　動的なアクセス制御の実装方針の見直し

ⓐ　情報セキュリティ管理者は、動的なアクセス制御の運用に際し、情報セキュリティに係る重大な変化等を踏まえ、アクセス制御ポリシーの見直しをする。

【 基本対策事項 】

＜7.3.2⑴ⓐ関連＞

7.3.2⑴-1　情報セキュリティ管理者は、動的なアクセス制御の運用に際し、アクセスパターンやアクセス先のリソースの変化があった場合は、変化が影響する箇所に対し再度リスク評価を行い、アクセス制御ポリシーの見直しをする。

遵守事項

⑵　リソースの信用情報に基づく動的なアクセス制御の運用時の対策

ⓐ　情報セキュリティ管理者は、動的なアクセス制御の運用に際し、リソースの信用情報の収集により検出されたリスクへ対処を行う。

第 8 部 情報システムの利用

8.1　情報システムの利用

8.1.1　情報システムの利用

目的・趣旨

役職員等関係者は、業務の遂行のため、端末での事務処理のほか電子メール、ウェブ等様々な情報システムを利用している。これらを適切に利用しない場合、情報セキュリティインシデントを引き起こすおそれがある。

このため、情報システムの利用に関する運用手順書を整備し、役職員等関係者は運用手順書に従って利用することが求められる。

なお、支払基金支給端末（要管理対策区域外で使用する場合に限る）に係る運用手順書の整備については遵守事項 6.1.2⑴、支払基金支給以外の端末に係る運用手順書の整備については遵守事項 6.1.3⑵をそれぞれ参照すること。

遵守事項

⑴　情報システムの利用に係る運用手順書の整備

⒜　情報セキュリティ責任者は、支払基金の情報システムの利用のうち、情報セキュリティに関する実施手順を整備する。

⒝　情報セキュリティ責任者は、書込 CD を用いた情報の取扱いに関する利用手順を「書込 CD 等を用いた情報の取扱いに関する手順書」に定め、書込 CD 以外の外部電磁的記録媒体を用いた情報の取扱いに関する利用手順を「情報取扱手順書」に定める。

⒞　情報セキュリティ責任者は、要保護情報が記録された外部電磁的記録媒体（書込 CD を除く。）を要管理対策区域外に持ち出す際の許可手続を「情報取扱手順書」に定める。

【 基本対策事項 】

＜8.1.1⑴⒜関連＞

8.1.1⑴-1　情報セキュリティ責任者は、支払基金の情報システムの利用のうち、情報セキュリティに関する以下を例とする実施手順を定める。

a)　情報システムの基本的な利用のうち、情報セキュリティに関する手順

b)　端末（支払基金支給以外の端末を含む）の利用のうち、情報セキュリティに関する手順

c)　電子メール及びウェブの利用のうち、情報セキュリティに関する手順

d)　識別コードと主体認証情報の取扱手順

e)　暗号と電子署名の利用に関する手順

f)　不正プログラム感染防止の手順

g) アプリケーション・コンテンツの提供時に支払基金外の情報セキュリティ水準の低下を招く行為の防止に関する手順

h) ドメイン名の使用に関する手順

i) Web 会議サービス利用時の手順

j) クラウドサービスを利用した支払基金外の者との情報の共有時の手順

＜8.1.1(1)(b)関連＞

8.1.1(1)-2 情報セキュリティ責任者は、CD-R 等の外部電磁的記録媒体を用いた情報の取扱いに関する実施手順として、以下の事項全てを含めて定める。

a) 役職員等関係者は、支払基金が支給する外部電磁的記録媒体、又は遵守事項8.1.1(1)(b)に規定する実施手順において定められた外部電磁的記録媒体を用いた情報の取扱いの遵守を契約により支払基金との間で取り決めた支払基金外の組織から受け取った外部電磁的記録媒体を使用する。

b) 支払基金以外の組織から受け取った外部電磁的記録媒体は、支払基金と当該組織との間で情報を運搬する目的に限って使用することとし、当該外部電磁的記録媒体から情報を読み込む場合及びこれに情報を書き出す場合の安全確保のために必要な措置を講じる。

c) 要機密情報が記録された外部電磁的記録媒体を要管理対策区域外に持ち出す場合は、外部電磁的記録媒体に格納する情報を暗号化する、又は主体認証機能や暗号化機能等を備えるセキュアな外部電磁的記録媒体を利用する。

d) 要機密情報は保存される必要がなくなった時点で速やかに削除する。

e) 外部電磁的記録媒体を使用する際には、事前に不正プログラム対策ソフトウェアによる検疫・駆除を行う。

＜8.1.1(1)(c)関連＞

8.1.1(1)-3 情報セキュリティ責任者は、要保護情報が記録された書込 CD 以外の外部電磁的記録媒体を要管理対策区域外に持ち出す際の許可手続として、以下を全て含む手続を整備し、役職員等関係者に遵守させる。

a) 利用時の許可申請手続

b) 手続内容（利用者、利用期間、主たる利用場所、目的、記録する情報、機器名）

c) 利用期間満了時の手続

d) 許可権限者（情報セキュリティ管理担当者）による手続内容の記録

遵守事項

⑵ 情報システム利用者の規定の遵守を支援するための対策

⑻ 情報セキュリティ管理者は、役職員等関係者による規定の遵守を支援する機能について情報セキュリティリスクと業務効率化の観点から支援する範囲を検討し、当該機能を持つ情報システムを構築する。

【 基本対策事項 】

＜8.1.1⑵(a)関連＞

8.1.1⑵-1　情報セキュリティ管理者は、支払基金外のウェブサイトについて、役職員等関係者が閲覧できる範囲を制限する機能を情報システムに導入する。具体的には、以下を例とする機能を導入する。また、当該機能に係る設定や条件について定期的に見直す。

a)　ウェブサイトフィルタリング機能

b)　事業者が提供するウェブサイトフィルタリングサービスの利用

8.1.1⑵-2　情報セキュリティ管理者は、役職員等関係者が不審な電子メールを受信することによる被害をシステム的に抑止する機能を情報システムに導入する。具体的には、以下を例とする機能を導入する。また、当該機能に係る設定や条件について定期的に見直す。

a)　受信メールに対するフィルタリング機能

b)　受信メールをテキスト形式で表示する機能

c)　スクリプトを含む電子メールを受信した場合において、当該スクリプトが自動的に実行されることがない電子メールクライアントの導入

d)　受信メールに添付されている実行プログラム形式のファイルを削除等することで実行させない機能

遵守事項

⑶　情報システムの利用時の基本的対策

⑷　役職員等関係者は、業務の遂行以外の目的で情報システムを利用しない。

⑹　役職員等関係者は、情報セキュリティ管理者が接続許可を与えた通信回線以外に支払基金の情報システムを接続しない。

⑹　役職員等関係者は、支払基金通信回線に、情報セキュリティ管理者の接続許可を受けていない情報システムを接続しない。

⑹　役職員等関係者は、業務の遂行において、利用が認められていないソフトウェアを利用しない。当該ソフトウェア以外のソフトウェアを職務上の必要により利用する場合は、セキュリティ担当課の承認を得る。また、役職員等関係者は、支払基金の情報システム又は機器等を自動で動作させるソフトウェア、システム、アプリケーション、ツール又はプログラム等を無許可で作成・使用してはならない。

⑹　役職員等関係者は、接続が許可されていない機器等を情報システムに接続しない。また、あらかじめ許可された機器以外の機器等を職務上の必要により接続する場合は、情報セキュリティ管理者の承認を得る。

⑹　役職員等関係者は、情報システムの設置場所から離れる場合等、第三者による不正操

作のおそれがある場合は、情報システムを不正操作から保護するための措置を講じる。

⑹　役職員等関係者は、支払基金支給端末（要管理対策区域外で使用する場合に限る）及び支払基金支給以外の端末を用いて要保護情報を取り扱う場合は、定められた利用手順に従う。

⑹　役職員等関係者は、次の各号に掲げる端末を用いて当該各号に定める情報を取り扱う場合は、情報セキュリティ管理担当者の許可を得る。

(ｱ)　支払基金支給端末（要管理対策区域外で使用する場合に限る）　要保護情報

(ｲ)　支払基金支給以外の端末　要保護情報

⑹　役職員等関係者は、要管理対策区域外において支払基金外通信回線に接続した支払基金支給端末を要管理対策区域で支払基金通信回線に接続する場合には、定められた安全管理措置を講じる。

⑹　役職員等関係者は、要管理対策区域外において支払基金外通信回線に接続した支払基金支給端末を要管理対策区域で支払基金通信回線に接続する場合には、情報セキュリティ管理担当者の許可を得る。

⑹　役職員等関係者は、要保護情報が記録された外部電磁的記録媒体を要管理対策区域外に持ち出す場合には、情報セキュリティ管理担当者の許可を得る。ただし、外部電磁的記録媒体のうち、支払基金が支給する書込 CD については、要管理対策区域外に持ち出してはならない。

⑹　情報セキュリティ管理担当者は、臨時職員、委託業者及び派遣職員に、クライアントパソコン等による作業を行わせる場合において、必要に応じてその作業に必要のない機能を利用できないように設定する。

⑹　役職員等関係者は、業務の遂行において、利用承認を得ていないクラウドサービスを利用しない。

⑹　役職員等関係者は、業務の遂行において、USB メモリを利用しない。

【 基本対策事項 】

＜8.1.1(3)(d)関連＞

8.1.1(3)-1　役職員等関係者は、情報セキュリティ管理者の承認の有無にかかわらず、次のソフトウェアを利用しない。

a)　ピアツーピアで通信を行うソフトウェア

b)　ファイル交換ソフトウェア

c)　端末内の情報又は端末に入力した情報が自動で支払基金外のサーバ装置等に送信されるソフトウェア

＜8.1.1(3)(f)関連＞

8.1.1(3)-2　役職員等関係者は、第三者による不正操作のおそれがある場合は、情報システムを不正操作から保護するために、以下を例とする措置を講じる。

a) スクリーンロックの設定
b) 利用後のログアウト徹底
c) 利用後に情報システムを鍵付き保管庫等に格納し施錠

＜8.1.1(3)(n)関連＞

8.1.1(3)-3 役職員等関係者は、個人所有の USB メモリを要管理対策区域内に持ち込んではならない。また、個人所有の USB メモリを支払基金の端末及び情報システムに接続してはならない。

遵守事項

(4) 端末（支払基金支給以外の端末を含む）の利用時の対策

(a) 役職員等関係者は、支払基金が支給する端末（要管理対策区域外で使用する場合に限る）及び支払基金支給以外の端末を用いて要保護情報を取り扱う場合は、「モバイル端末(要管理対策区域外における使用)及び支払基金支給以外の端末の使用に係る手順書」に従う。

(b) 役職員等関係者は、次の各号に掲げる端末を用いて当該各号に定める情報を取り扱う場合は、情報セキュリティ管理担当者の許可を得る。

(ｱ) 支払基金が支給する端末（要管理対策区域外で使用する場合に限る）
機密性３情報（重要性分類Ⅰ）、要保全情報又は要安定情報

(ｲ) 支払基金支給以外の端末
要保護情報

(c) 役職員等関係者は、要管理対策区域外において支払基金外通信回線に接続した支払基金が支給する端末を要管理対策区域で支払基金内通信回線に接続する場合には、定められた安全管理措置を講じる。

遵守事項

(5) 電子メール・ウェブの利用時の対策

(a) 役職員等関係者は、要機密情報を含む電子メールを送受信する場合には、支払基金が運営し、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。

(b) 役職員等関係者は、支払基金外の者へ電子メールにより情報を送信する場合は、当該電子メールのドメイン名に支払基金ドメイン名を使用する。

(c) 役職員等関係者は、不審な電子メールを受信した場合には、あらかじめ定められた手順に従い、対処する。

(d) 役職員等関係者は、ウェブクライアントの設定を見直す必要がある場合は、情報セキュリティに影響を及ぼすおそれのある設定変更を行わない。

(e) 役職員等関係者は、ウェブクライアントが動作するサーバ装置又は端末にソフトウ

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。

(f) 役職員等関係者は、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、以下の全ての事項を確認する。

(ｱ) 送信内容が暗号化されること

(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

【 基本対策事項 】

＜8.1.1(5)関連＞

8.1.1(5)-1 役職員等関係者は、メールソフトを利用する場合、以下の措置を講じる。

a) 受信したメールが不用意に開封されないような対策(プレビュー表示の無効設定等)を実施する。

b) 実行形式のファイル（拡張子が「.ｅｘｅ」等のもの）が無効化されるよう設定する。

c) 添付ファイルのあるメールを送受信する場合は、不正プログラム対策ソフトウェアによる検査を実施する。

d) 差出人が不明なメール又は不自然に添付されたファイルは開かない。

e) メールの送受信が発生しないことが明らかなメールアドレスを削除する。

f) 情報セキュリティ管理者の許可を得た場合を除いて、個人的に利用している電子メールアドレス宛てに職場のメールを転送しない。

g) 実行形式のファイル（拡張子が「.ｅｘｅ」等のもの）を送信しない。

遵守事項

(6) 識別コード・主体認証情報の取扱い

(a) 役職員等関係者は、主体認証の際に自己に付与された識別コード以外の識別コードを用いて情報システムを利用しない。

(b) 役職員等関係者は、自己に付与された識別コードを適切に管理する。

(c) 役職員等関係者は、管理者権限を持つ識別コードを付与された場合には、管理者としての業務遂行時に限定して、当該識別コードを利用する。

(d) 役職員等関係者は、自己の主体認証情報の管理を徹底する。

【 基本対策事項 】

＜8.1.1(6)(b)関連＞

8.1.1(6)-1 役職員等関係者は、自己に付与された識別コードを適切に管理するため、以下を全て含む措置を講じる。

a) 知る必要のない者に知られるような状態で放置しない。

b) 他者が主体認証に用いるために付与及び貸与しない。

c) 識別コードを利用する必要がなくなった場合は、定められた手続に従い、識別コードの利用を停止する。

＜8.1.1(6)(d)関連＞

8.1.1(6)-2 役職員等関係者は、知識による主体認証情報を用いる場合には、以下を全て含む管理を徹底する。

a) 自己の主体認証情報を他者に知られないように管理する。

b) 自己の主体認証情報を他者に教えない。

c) 主体認証情報を忘却しないように努める。

d) 主体認証情報を設定するに際しては、推測されないものにする。

e) 異なる識別コードに対して、共通の主体認証情報を用いない。

f) 異なる情報システムにおいて、識別コード及び主体認証情報についての共通の組合せを用いない。(シングルサインオンの場合を除く。)

g) 情報セキュリティ管理者から主体認証情報を定期的に変更するように指示されている場合は、その指示に従って定期的に変更する。

8.1.1(6)-3 役職員等関係者は、所有による主体認証情報を用いる場合には、以下を全て含む管理を徹底する。

a) 主体認証情報格納装置を本人が意図せずに使われることのないように安全措置を講じて管理する。

b) 主体認証情報格納装置を他者に付与及び貸与しない。

c) 主体認証情報格納装置を紛失しないように管理する。紛失した場合には、定められた報告手続に従い、直ちにその旨を報告する。

d) 主体認証情報格納装置を利用する必要がなくなった場合には、これを情報セキュリティ管理担当者に返還する。

遵守事項

(7) 暗号・電子署名の利用時の対策

(a) 役職員等関係者は、情報を暗号化する場合及び情報に電子署名を付与する場合には、定められたアルゴリズム、鍵長及び方法に従う。

(b) 役職員等関係者は、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、定められた鍵の管理手順等に従い、これを適切に管理する。

(c) 役職員等関係者は、暗号化された情報の復号に用いる鍵について、鍵のバックアップ手順に従い、そのバックアップを行う。

遵守事項

⑻　不正プログラム感染防止

⒜　役職員等関係者は、不正プログラム感染防止に関する措置に努める。

⒝　役職員等関係者は、情報システムが不正プログラムに感染したおそれがあることを認識した場合は、感染した情報システムの通信回線への接続を速やかに切断するなど、必要な措置を講じる。

【 基本対策事項 】

＜8.1.1⑻⒜関連＞

8.1.1⑻-1　役職員等関係者は、不正プログラム対策ソフトウェアを活用し、不正プログラム感染を回避するための以下の全ての措置に努める。

a)　不正プログラム対策ソフトウェア等により不正プログラムとして検知された実行プログラム形式のファイルを実行しない。また、検知されたデータファイルをアプリケーション等で読み込まない。

b)　不正プログラム対策ソフトウェア等に係るアプリケーション及び不正プログラム定義ファイル等について、これを常に最新の状態に維持する。

c)　不正プログラム対策ソフトウェア等による不正プログラムの自動検査機能を有効にする。

d)　不正プログラム対策ソフトウェア等により定期的に全てのファイルに対して、不正プログラムの検査を実施する。

e)　不正プログラム対策ソフトウェアによる不正プログラム検査の実施中は、実行を途中で止めない。

8.1.1⑻-2　役職員等関係者は、外部からデータやソフトウェアをサーバ装置及び端末等に取り込む場合又は外部にデータやソフトウェアを提供する場合には、不正プログラム感染の有無を確認する。

8.1.1⑻-3　役職員等関係者は、不正プログラムに感染するリスクを低減する情報システム（支払基金支給以外の端末を含む）の利用方法として、以下のうち実施可能な措置を講じる。

a)　不審なウェブサイトを閲覧しない。

b)　アプリケーションの利用において、マクロ等の自動実行機能を無効にする。

c)　プログラム及びスクリプトの実行機能を無効にする。

d)　安全性が確実でないプログラムをダウンロードしたり実行したりしない。

e)　外部から入手した実行形式のファイル（拡張子が「．ｅｘｅ」等のもの）は、不用意にクリックしない。

f)　セキュリティ担当課が提供するコンピュータウイルスに関する情報を常に確認する。

遵守事項

⑼　Web 会議サービスの利用時の対策

ⓐ　役職員等関係者は、定められた利用手順に従い、Web 会議の参加者や取り扱う情報に応じた情報セキュリティ対策を実施する。

ⓑ　役職員等関係者は Web 会議を主催する場合、会議に無関係の者が参加できないよう対策を講じる。

【 基本対策事項 】

＜8.1.1⑼ⓐ関連＞

8.1.1⑼-1　役職員等関係者は、Web 会議サービスの利用に当たり、以下を全て含む情報セキュリティ対策を実施する。

a)　原則として、支払基金が支給する端末を利用する。

b)　原則として、支払基金が利用を許可した Web 会議サービスを利用する。

c)　利用する Web 会議サービスのソフトウェアが、最新の状態であることを確認する。

d)　要機密情報を取り扱う場合は、可能な限りエンドツーエンド（E2E）の暗号化を行う。

e)　要機密情報を取り扱う場合は、Web 会議サービスの議事録作成機能、自動翻訳機能及び録画機能等、E2E の暗号化を利用できなくなる機能を可能な限り使用しない。

＜8.1.1⑼ⓑ関連＞

8.1.1⑼-2　役職員等関係者は、会議に無関係な者を会議に参加させないために、以下を例とする対策を行う。

a)　会議室にアクセスするためのパスワード等をかける。

b)　会議の参加者に会議室にアクセスするためのパスワード等を通知する際は、第三者に知られないよう安全な方法で通知する。

c)　会議を非公開設定にする。

d)　待機室を設けて参加者と確認できた者だけを会議室に入室させる。

e)　Web 会議の主催者が事前に登録した者だけを会議室に入室させる。

f)　なりすましや入れ替わりが疑われるなどの不審な参加者を会議室から退室させる。

遵守事項

⑽　クラウドサービスを利用した支払基金外の者との情報の共有時の対策

ⓐ　役職員等関係者は、支払基金外の者と情報の共有を行うことを目的とし、クラウドサ

ービス上に要保護情報を保存する場合は、情報の共有を行う必要のある者のみがクラウドサービス上に保存した要保護情報にアクセスすることが可能となるための措置を講じる。

(b) 役職員等関係者は、支払基金外の者と情報の共有を行うことを目的とし、クラウドサービス上に要保護情報を保存する場合は、情報の共有が不要になった時点で、クラウドサービス上に保存した要保護情報を速やかに削除する。

8.1.2 ソーシャルメディアによる情報発信

目的・趣旨

国の行政機関、独立行政法人及び指定法人においても、積極的な広報活動等を目的としたソーシャルメディアの利用が一般的になっている。しかし、民間事業者等により提供されているソーシャルメディアでは支払基金ドメイン名を使用することができないため、真正なアカウントであることを国民等が確認できるようにする必要がある。また、支払基金のアカウントを乗っ取られた場合や、利用しているソーシャルメディアが予告なく停止した際に必要な情報を発信できない事態が生ずる場合も想定される。そのため、要安定情報を広く国民の皆様等に提供する際には、当該情報を必要とする国民等が一次情報源を確認できるよう、情報発信方法を考慮する必要がある。加えて、虚偽情報により国民の皆様等の混乱が生じることのないよう、発信元は、なりすまし対策等について措置を講じておく必要がある。

また、このようなソーシャルメディアは機能拡張やサービス追加等の技術進展が著しいことから、常に当該サービスの運用事業者等の動向等外部環境の変化に機敏に対応することが求められる。

なお、ソーシャルメディアは、定型約款や利用規約等への同意のみで利用可能となるクラウドサービスであることが考えられ、要機密情報を取り扱う上で必要十分なセキュリティ要件を満たすことは困難であることが一般的である。このことから、ソーシャルメディアの利用は、要機密情報を取り扱わず、委託先における高いレベルの情報管理を要求する必要が無い場合に限るものとする。ソーシャルメディアを利用の際は 4.2.3「クラウドサービスの選定・利用（要機密情報を取り扱わない場合)」の対策を参照すること。

遵守事項

(1) ソーシャルメディアによる情報発信時の対策

(a) 情報セキュリティ責任者は、支払基金が管理するアカウントでソーシャルメディアを利用することを前提として、以下を全て含む情報セキュリティ対策に関する情報セキュリティ対策を講じる。また、当該サービスの利用において要機密情報が取り扱われないよう対策を講じる。

(ｱ) 支払基金のアカウントによる情報発信が実際の支払基金のものであると明らかと

するために、アカウントの運用組織を明示するなどの方法でなりすましへの対策を講じる。

(ｲ) パスワード等の主体認証情報を適切に管理するなどの方法で不正アクセスへの対策を講じる。

(b) 役職員等関係者は、要安定情報の国民への提供にソーシャルメディアを用いる場合は、支払基金の自己管理ウェブサイトに当該情報を掲載して参照可能とする。

【 基本対策事項 】

＜8.1.2(1)(a)関連＞

8.1.2(1)-1 情報セキュリティ責任者は、ソーシャルメディアの閲覧者の信頼を確保し、その情報セキュリティ水準の低下を招かないよう、以下を全て含む対策を手順として定める。

a) アカウント運用ポリシー（ソーシャルメディアポリシー）を策定し、ソーシャルメディアのアカウント設定における自由記述欄又はソーシャルメディアアカウントの運用を行っている旨の表示をしている支払基金の当該ウェブサイト上のページに、アカウント運用ポリシーを掲載する。特に、専ら情報発信に用いる場合には、その旨をアカウント運用ポリシーに明示する。

b) URL 短縮サービスは、利用するソーシャルメディアが自動的に URL を短縮する機能を持つ場合等、その使用が避けられない場合を除き、原則使用しない。

8.1.2(1)-2 情報セキュリティ責任者は、支払基金のアカウントによる情報発信が実際の支払基金のものであると認識できるようにするためのなりすまし対策として、以下を全て含む対策を手順として定める。

a) 支払基金からの情報発信であることを明らかにするために、支払基金が支払基金ドメイン名を用いて管理している当該ウェブサイト内において、利用するソーシャルメディア名と、そのソーシャルメディアにおけるアカウント名又は当該アカウントページへのハイパーリンクを明記するページを設ける。

b) 支払基金からの情報発信であることを明らかにするために、アカウント名やアカウント設定の自由記述欄等を利用し、支払基金が運用していることを利用者に明示する。

c) 運用しているソーシャルメディアのアカウント設定の自由記述欄において、当該アカウントの運用を行っている旨の表示をしている支払基金の当該ウェブサイト上のページの URL を記載する。

d) ソーシャルメディアの提供事業者が、アカウント管理者を確認しそれを表示等する、いわゆる「認証アカウント（公式アカウント）」と呼ばれるアカウントの発行を行っている場合には、可能な限りこれを取得する。

8.1.2(1)-3 情報セキュリティ責任者は、第三者が何らかの方法で不正にログインを行い、

偽の情報を発信するなどの不正行為を行う、いわゆる「アカウント乗っ取り」を防止するために、ソーシャルメディアのログインパスワードや認証方法について、以下を全て含む管理手順を定める。

a) パスワードを適切に管理する。具体的には、ログインパスワードには強固なパスワードに必要な十分な桁数を備えた第三者に容易に推測できないパスフレーズ等を使用した容易に推測されないものを設定するとともに、パスワードを知る担当者を限定し、パスワードの使い回しをしない。

b) 二段階認証やワンタイムパスワード等、アカウント認証の強化策が提供されている場合は、可能な限り利用する。

c) ソーシャルメディアへのログインに利用する端末を紛失又は盗難に遭った場合は、当該端末を悪用され、アカウント乗っ取りの可能性があるため、当該端末の管理を厳重に行う。

d) ソーシャルメディアへのログインに利用する端末が不正アクセスされた場合、当該端末が不正に遠隔操作される又は、当該端末に保存されたパスワードが窃取される可能性がある。これらを防止するため、少なくとも端末には最新のセキュリティパッチの適用や不正プログラム対策ソフトウェアを導入するなど、適切なセキュリティ対策を実施する。

8.1.2(1)-4 情報セキュリティ責任者は、なりすましや不正アクセスを確認した場合の対処として、以下を全て含む対処手順を定める。

a) 自己管理ウェブサイトに、なりすましアカウントが存在することや当該ソーシャルメディアを利用していないこと等の周知を行い、また、信用できる機関やメディアを通じて注意喚起を行う。

b) アカウント乗っ取りを確認した場合には、被害を最小限にするため、ログインパスワードの変更やアカウントの停止を速やかに実施し、自己管理ウェブサイト等で周知を行うとともに、セキュリティ担当課に報告する。報告を受けたセキュリティ担当課は遵守事項 2.2.4(2)に従い適切な対処を行う。

8.1.3 テレワーク

目的・趣旨

働き方改革実行計画（平成 29 年 3 月 28 日　働き方改革実現会議決定）により、柔軟な働き方に対応しやすい環境整備が求められているところ、役職員等関係者が業務を遂行する上で、必ずしも事務所に出勤する必要はなく、自宅等から遠隔で業務を遂行する形態への対応が求められることとなった。また、大規模災害時や感染症対策として、事務所への出勤が抑制されるような状況下では、大半の役職員等関係者が事務所以外から業務を遂行できるようにテレワーク環境の整備が必要となる。

本款では、テレワークの実施に特に必要な対策についてのみ規定しているため、本款以外に、3.1.1「情報の取扱い」、6.1.2「要管理対策区域外での端末利用時の対策」、6.1.3「支払基金支給以外の端末の導入及び利用時の対策」、6.4.1「通信回線」、6.4.2「通信回線装置」、6.4.3「無線 LAN」、7.1.6「監視機能」及び 8.1.1「情報システムの利用」の各款を参照すること。

遵守事項

⑴　運用手順書の整備

⒜　情報セキュリティ責任者は、テレワーク実施時の情報セキュリティ対策を「モバイル端末(要管理対策区域外における使用）及び支払基金支給以外の端末の使用に係る手順書」に整備する。なお、原則としてテレワークは支払基金が支給する端末で行う。

⒝　役職員等関係者は、テレワーク実施に当たり、「モバイル端末(要管理対策区域外における使用）及び支払基金支給以外の端末の使用に係る手順書」を確認する。

【 基本対策事項 】

＜8.1.3⑴⒜関連＞

8.1.3(1)-1　情報セキュリティ責任者は、テレワークの実施に係る手順に盛り込むべき内容として、テレワークの実施申請及び承認並びにテレワークの実施報告のほか、以下を例とする項目を定める。

a)　テレワークの実施申請及び承認並びにテレワークの実施報告
b)　テレワークで取り扱うことができる情報の格付
c)　テレワークで取り扱う情報の保存場所
d)　要管理対策区域外での要機密情報の取扱手続
e)　テレワークに使用する端末に必要な情報セキュリティ対策
f)　支払基金が支給する端末の持出手続
g)　例外的に支払基金支給以外の端末の利用を認める場合
h)　支払基金支給以外の端末の利用許可手続及び安全管理措置
i)　テレワーク実施可能な場所
j)　テレワークに利用可能なネットワーク

遵守事項

⑵　実施環境における対策

⒜　情報セキュリティ管理者は、テレワークの実施により支払基金外通信回線を経由して支払基金の情報システムへリモートアクセスする形態となる情報システムを構築する場合は、通信経路及びリモートアクセス特有の攻撃に対する情報セキュリティを確保する。

⑹　情報セキュリティ管理者は、リモートアクセスに対し多要素主体認証を行う。
⑹　情報セキュリティ管理者は、リモートアクセスする端末を許可された端末に限定する措置を講じる。
⑹　情報セキュリティ管理者は、リモートアクセスする端末を最新の脆弱性対策や不正プログラム対策が施されている端末に限定する。

【 基本対策事項 】
＜8.1.3⑵⑷関連＞
8.1.3⑵-1　情報セキュリティ管理者は、VPN 回線を整備してリモートアクセス環境を構築する場合は、以下を例とする対策を講じる。
a)　利用開始及び利用停止時の申請手続の整備
b)　通信を行う端末の識別又は認証
c)　利用者の認証
d)　通信内容の暗号化
e)　主体認証ログの取得及び管理
f)　リモートアクセスにおいて利用可能な公衆通信網の制限
g)　アクセス可能な情報システムの制限
h)　リモートアクセス中の他の通信回線との接続禁止
i)　不正な通信の有無の監視
＜8.1.3⑵⑹関連＞
8.1.3⑵-2　情報セキュリティ管理者は、リモートから接続する端末が、許可されたものであるかどうかを確認するために、以下を例とする対策を行う。
a)　証明書による端末確認
b)　ソフトウェア認証による端末確認
＜8.1.3⑵⑻関連＞
8.1.3⑵-3　情報セキュリティ管理者は、リモートからの接続を最新の脆弱性対策や不正プログラム対策が施されている端末に限定するために、以下を例とする対策を行う。
a)　検疫ネットワークの整備
b)　IT 資産管理の自動化

遵守事項
⑶　実施時における対策
⑹　情報セキュリティ管理者は、テレワーク実施前及び実施後に役職員等関係者が確認するべき項目を定め、役職員等関係者に当該項目を確認させる。
⑹　役職員等関係者は、テレワーク実施場所については原則、居宅のみとし、画面ののぞ

き見を防止できるようテレワークの実施場所を選定する。審査委員が勤務先医療機関において在宅審査を実施する場合には、第三者が閲覧できない鍵付き個室を実施場所とする。

(c) 役職員等関係者は、原則として情報セキュリティ対策の状況が定かではない又は不十分な支払基金外通信回線を利用してテレワークを行わない。

【 基本対策事項 】

＜8.1.3(3)(b)関連＞

8.1.3(3)-1 役職員等関係者は、基本対策事項 6.1.1(1)-3 に示した対策のほか、以下の項目を例とする画面ののぞき見から発生する情報漏えい対策を講じる。

a) 背後に人が立たないよう背後に通路がない場所で壁を背にする位置に座りテレワークを行う。

b) Web 会議等、音声を扱う場合は、ヘッドホンを使用するなど、内容が周囲に漏れないよう注意する。

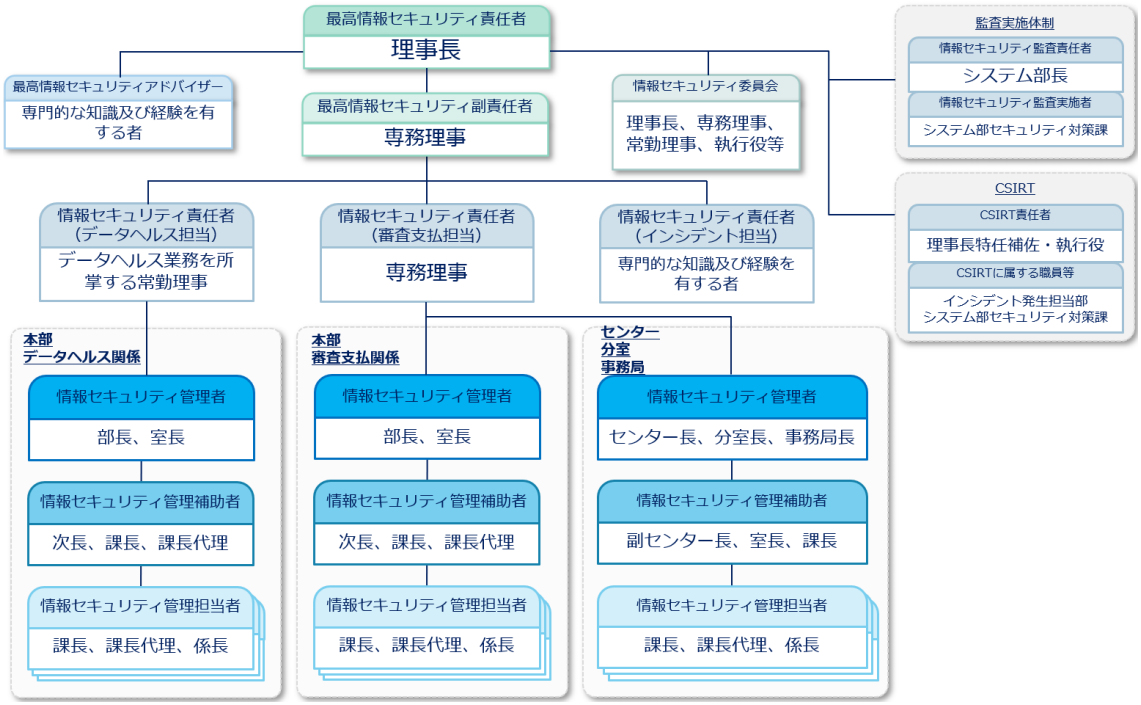
c) 同居する者に対し知り得た情報を他人に漏らさないよう協力を求める。

＜8.1.3(3)(c)関連＞

8.1.3(3)-2 役職員等関係者は、テレワークに情報セキュリティ対策の状況が不明又は不十分な支払基金外通信回線を利用しないために、以下を例とする対策を行う。

a) 公衆無線 LAN を利用しない。

b) 宿泊施設等が提供する無料ネットワークを利用しない。



A.1 組織・体制イメージ図

附　則

この規程は、令和３年１０月１日から施行する。

附　則

この規程は、令和４年１０月１日から施行する。

附　則

この規程は、令和５年１２月１３日から施行する。

附　則

この規程は、令和７年６月１８日から施行する。