令和４個人番号利用事務系ネットワークにおける

セキュリティ対策業務　詳細仕様書（案）

令和4年5月

三重県デジタル社会推進局デジタル改革推進課

目　次

1.　セキュリティ対策システムの概要 1
1.1.　セキュリティ対策システムの概要 1
1.2.　個人番号利用事務系ネットワークの概要 1
2.　各種詳細設計 1
2.1.　セキュリティ対策システムにかかる設計 1
2.2.　その他機能に関する設計 9
3.　ハードウェア・ソフトウェア要件 11
3.1.　基本的な考え方 11
3.2.　性能要件 11
3.3.　ハードウェア設置要件 12
3.4.　冗長化にかかる要件 14
3.5.　ソフトウェア要件 14
3.6.　三重県が用意するシステム等 15
4.　セキュリティ対策システム導入及び各種設定要件 15
4.1.　基本的な考え方 15
4.2.　セキュリティ対策システム導入及び設定 15
4.3.　その他機能に関する設定 17
4.4.　バックアップ設定 18
4.5.　稼働監視設定 18
4.6.　アカウント設定 18
4.7.　セキュリティ対策 18
5.　パソコン及びプリンタ更新要件 18
5.1.　基本的な考え方 18
5.2.　パソコン交換配布 18
5.3.　プリンタ交換配布 22
6.　Windows OS 及び Microsotf Office のバージョンアップ作業 23
6.1.　業務目的・範囲 23
6.2.　作業日程 23

6.3. 対象パソコン 24
6.4. 作業概要 24
7. 運用保守要件 25
7.1. 基本的な考え方 25
7.2. 運用業務 25
7.3. 保守業務 29
8. 機器の撤去・設定情報及びログ情報等の抽出 31
8.1. 基本的な考え方 31
8.2. 撤去する機器について 31
8.3. 抽出する情報について 31

1. セキュリティ対策システムの概要

1.1. セキュリティ対策システムの概要

個人番号利用事務系ネットワークにおいて個人番号利用事務を行うパソコン等について、認証の強化や情報漏えいの防止などセキュリティ対策を行うため、以下のアからキの機能を実現するためのセキュリティ対策システムを導入すること。

(ア) パソコン管理機能

(イ) パソコン認証機能

(ウ) 利用者認証（生体認証）機能

(エ) パソコン操作ログ記録機能

(オ) 外部媒体使用制限機能

(カ) 外部媒体暗号化機能

(キ) パソコン暗号化機能

なお、現行システムにおいては、（ア）（イ）（エ）（オ）（カ）の機能については同一のエージェントソフトウェアで実現し、（ウ）及び（キ）はそれぞれ単独の機能を有するソフトウェアで実現している。

1.2. 個人番号利用事務系ネットワークの概要

個人番号利用事務系ネットワークの概要（物理構成図・論理構成図）は別紙「個人番号利用事務系ネットワーク概要」のとおり。

令和４年５月時点での構成としては､データセンタから本庁舎･総合庁舎に延伸するVLAN（別紙(A)）と、3 拠点に設置するセグメント（別紙(B)）の 4 セグメントで構成しているが、本委託業務における運用期間中に接続パソコンやサーバ等の増加により、本庁・総合庁舎に延伸する VLAN を分割する可能性や、その他ネットワーク構成変更の可能性がある。

個人番号利用事務系ネットワークと他のセグメントとの通信は管理用の限られた通信のみ認めることとし、各パソコンから直接他のセグメントに通信することは想定していない。

2. 各種詳細設計

2.1. セキュリティ対策システムにかかる設計

各機能について、以下の方針及び機能要件を踏まえて必要な設計をもれなく行うこと。設計内容についてはレビュー会を設けて三重県に対して十分な説明を行い、内容の承認を得てから次の工程に進むこと。

2.1.1. 基本方針

ア．各機能について共通して求める要件は以下のとおり。

(ア) 各機能について、設定情報等を一元管理できること。

(イ) 各機能の設定情報やログ情報について、機器の故障等に伴う消失を防ぐため、必要なバックアップを取得すること。

(ウ) パソコンの OS として、Windows 10 Pro、Windows 11 Pro で利用できること。

(エ) パソコンにインストールするエージェントのインストール等について、ドメインへのログイン時に自動的に行うなど、パソコンへの導入が容易に行えること。

(オ) 各種ログは本委託業務において用意するログ記録用サーバに記録できること。ただし、サーバ障害時に備え、一時的にパソコンに記録し一定のタイミングでサーバに転送する方式としてもよい。一時的にパソコンに記録する際には、改ざん等が行われないよう暗号化等の対策を行うこと。

(カ) ログ記録用サーバに障害が発生した場合でも継続してログが記録できること。

イ．現行のセキュリティ対策システムで採用されている機能（ソフトウェアや導入機器等）について必ずしも後継品を選択する必要はないが、後継品以外による機能構築を行う場合は、各機能にかかる移行作業についても設計を行うこと。

2.1.2. パソコン管理機能

2.1.2.1. 方針

ア．個人番号利用事務系ネットワークに接続されたパソコン及びサーバにインストールされた OS、ソフトウェア、ウイルス対策ソフトのパターンファイル等を最新に保つため、インストールされたソフトウェアの情報等を管理するとともに、セキュリティパッチやウイルス対策ソフトのパターンファイル等を配信できる環境を構築すること。

イ．パソコンへのプログラム等の配信や障害発生時のリモート操作等、パソコンの管理に必要な環境を構築すること。

2.1.2.2. セキュリティパッチの管理

ア．マイクロソフト社製の OS で動作するパソコン、サーバに対し、任意のセキュリティパッチ、サービスパック等の配信が可能なこと。

イ．対象とするプログラムは下記のとおりとするが、新たな製品・クラスが追加された場合はその都度配信対象とするか検討を行うこと。

製　品：Office（すべてのバージョン）、Windows（すべてのバージョン）

クラス：Service Packs、セキュリティ問題の修正プログラム、更新、修正プログラム集、重要な更新

ウ．各パソコンのパッチ適用状況の出力ができること。

エ．セキュリティパッチは、個人番号利用事務系ネットワークに新たな Windows Server Update Services（WSUS）サーバを設置し、配信することとする。なお、更新プログラムは三重県が別途契約を行う自治体情報セキュリティ向上プラットフォームから配信を受けることとする。

オ．Windows Server Update Services（WSUS）でセキュリティパッチを配信できない Office または Windows のバージョンがある場合は「2.1.2.6. プログラム等配信機能」で本機能を実現すること。

2.1.2.3. ウイルス対策ソフトの管理

ア．パソコン及びサーバにインストールされたウイルス対策ソフトのパターンファイルやプログラム等を最新に保つため、パターンファイル・プログラム等の配信が可能なこと。

イ．パターンファイル等は、自治体情報セキュリティ向上プラットフォームから配信を受けること

とする。

2.1.2.4. Adobe 社製品ソフトの管理

ア．パソコン及びサーバにインストールされた Adobe 社製品に対し、セキュリティパッチの配信が可能なこと。

イ．個人番号利用事務系ネットワークはインターネットに直接接続できない為、必要なセキュリティパッチファイルについては、受託事業者が運用保守業務において別途準備すること。

2.1.2.5. パソコン情報の取得・出力

ア．任意のタイミングに任意のパソコンに対してパソコン情報（インベントリ）の取得が行えること。

イ．インベントリ取得のタイミングは、スケジュール設定できること。

ウ．取得するインベントリの種類は取得タイミング毎に設定できること。また、インベントリ取得に際してパソコンへの通知、またはパソコンへの負荷状況を考慮したインベントリ収集の制御が可能なこと。

エ．取得したインベントリ情報をリアルタイムで確認でき、任意の項目について、CSV 形式でエクスポートできること。

オ．各パソコンのインベントリ情報は 3 世代以上保有または変更履歴の確認ができること。

カ．以下のインベントリが取得できること。

(ア) ハードウェア情報（CPU、メモリ、HDD 容量等）

(イ) ウイルス対策ソフト情報（種類、パターンファイル等）

(ウ) OS 情報（バージョン、適用パッチ等）

(エ) アプリケーション情報（インストールされているアプリケーション名）

(オ) ソフトウェア情報（保存しているプログラムファイル名等）

(カ) レジストリ情報（指定した任意のレジストリ値）

(キ) 外部接続機器情報（USB にて接続されているデバイスの種類等）

(ク) その他（ログオンユーザ名、IP アドレス等）

キ．取得したインベントリ情報等をもとに条件に合致するパソコンを抽出することができること。また、抽出条件は保存することが可能なこと。

2.1.2.6. プログラム等の配信機能

ア．任意のパソコンもしくはグループ（サーバ・パソコン等の種別やパソコンの設置された拠点等によりグループ化することを想定）に対し、任意のタイミングでプログラムやファイルの配信ができること。

イ．プログラムの配信に際してパソコン利用者への通知またはパソコンの負荷状況を考慮した配信ができること。

2.1.2.7. パソコン設定管理機能

ア．個人番号利用事務系ネットワーク内のパソコンやサーバをグループ分けし、必要なグループポリシー（WSUS サーバの指定、ログオンスクリプトの指定、ブラウザのセキュリティ設定の指定など、Active Directory（AD）サーバにて設定が可能なものを、別セグメントに既設の AD

サーバの設定に準拠して設定することを想定）が設定可能なこと。

イ．ホワイトリスト、ブラックリスト等によりアプリケーションの実行を許可または禁止し、不正アプリケーションの利用を防ぐことが可能なこと。

2.1.2.8. リモート操作機能

ア．パソコンのリモート操作が可能なこと。

イ．リモート操作時には、操作者・被操作者の双方でパソコン画面の閲覧・操作が可能なこと。

ウ．リモート操作開始時にパソコン側での操作が不要であること。

2.1.3. パソコン認証機能

2.1.3.1. 方針

ア．個人番号利用事務系ネットワークへの不正接続を防止するため、個人番号利用事務系ネットワークへの接続を許可されていない不正パソコンの接続を拒否する環境を構築すること。

2.1.3.2. 不正接続の検知

ア．不正パソコンが個人番号利用事務系ネットワークに接続されたことを検知できること。検知したパソコンに関する情報、日時等をログとして記録できること。

イ．検出方法については電子証明書による認証もしくは MAC アドレスによる認証を想定しているが、不正パソコンの接続防止に効果が高い方法であればその他の方法での実現としてもよい。

2.1.3.3. 不正パソコン接続の禁止（拒否）

ア．不正パソコンの接続を検知した場合は、他のパソコン、サーバとの通信ができないよう接続を禁止（拒否）できること。

2.1.3.4. 許可パソコンの追加・削除

ア．新たに接続を許可するパソコンの情報をセキュリティ対策システムに登録することが可能なこと。

(ア) 電子証明書による認証の場合には、新たな証明書を発行すること。パソコンへの証明書のインストールは三重県が行うが、インストール方法等のマニュアルを整備すること。

(イ) MAC アドレス認証の場合には、パソコンから取得した MAC アドレス情報をセキュリティ対策システムに登録すること。この場合、MAC アドレスの取得方法等についての操作マニュアル等を整備すること。

イ．パソコンを廃棄する場合など、パソコンの接続が不要となった場合にはパソコンの情報をセキュリティ対策システムから削除することが可能なこと。

(ア) 電子証明書による認証の場合には、削除するパソコン用に発行していた電子証明書を無効化できること。

(イ) MAC アドレス認証の場合には、パソコンの MAC アドレス情報をセキュリティ対策システムから削除できること。

2.1.3.5. ログの抽出・分析

ア．記録されたログについて、対象パソコンの情報や日時等により抽出・分析が可能なこと。

2.1.4. 利用者認証（生体認証）機能

2.1.4.1. 方針

利用を許可されていない第三者による不正使用を防止するため、個人番号利用事務系ネットワークの利用の際に生体情報による認証を求める環境を構築すること。

2.1.4.2. 認証機能

ア．Active Directory サーバにより、利用者の認証を行うこと。

イ．Active Directory の利用者情報は、別のセグメント上に既設の Active Directory サーバから取得すること。

2.1.4.3. 生体認証機能

ア．ID・パスワードによる認証とは別に、利用者の生体情報（静脈等）を用いた認証を実現すること。

イ．生体認証の方法や読み取り装置については、精度の高いもの（本人拒否率（FRR）が低く（0.1%以下）、他人受入率（FAR）が低い（0.001%以下）もの）を採用すること。また、登録非対応率についても低い（0.1%以下）ものであること。

ウ．生体認証の方法については、偽造等が容易でない方式を採用すること。

エ．認証のタイミングはパソコン（ドメイン）へのログイン時に行うこととし、Active Directory との連携を想定している。

オ．認証に関する情報は管理者側にて一元管理できること。ただし、サーバ障害時にも引き続き業務が行えるような構成とすること。

カ．Active Directory のログイン ID を複数の利用者で共有している場合でも、個々の利用者が特定できること。

キ．生体情報が読み取れないなどの事態に備えて、複数個所の生体情報が登録できること。

ク．生体情報を用いた方法以外でのログインは原則禁止とするが、不測の事態に備え、例外的に ID・パスワードによるログインを可能とすること。

2.1.4.4. 新規利用者の生体情報の収集・登録

ア．新規利用者の生体情報の登録フローは以下のいずれかの方法によること。

(ア) セキュリティ対策システム管理者（運用保守担当者）が認証情報を登録後、各拠点の管理者の権限により生体情報の登録（ログイン情報との結びつけ）を行う。この場合、各拠点の管理者には認証システムの管理権限は与えず、生体情報の登録権限のみを与えることとする。

(イ) 各拠点で新規利用者が仮登録を行い、各拠点からの申請に基づきセキュリティ対策システム管理者（運用保守担当者）が本登録を行う。

イ．新規利用者に関する Active Directory のログイン情報は、連携するサーバから取得すること。

2.1.4.5. ログの記録・抽出・分析

ア．ログインの成功・失敗等について、日時、利用者、パソコン等のログが記録できること。

イ．ログインの記録について、成功・失敗の区分、利用者、利用パソコン、日時等の条件により抽出・分析が可能なこと。

2.1.4.6. 他システムとの連携

ア．Active Directory サーバとの連携により認証情報を取得するシステムを除き、他システムとの連携については想定していない。

2.1.5. パソコン操作ログ記録機能

2.1.5.1. 方針

ア．不正な情報の持ち出しが行われた際やマルウェアによる被害を受けた際等における証拠保全を行うとともに、情報漏えいを未然に防止するため、パソコンの操作情報（パソコンへのログイン、外部媒体へのファイルコピーや印刷等）を記録できる環境を構築すること。

2.1.5.2. パソコン操作の記録

ア．パソコンの操作情報を、日時、操作パソコン、利用者情報等とともに記録できること。記録操作内容は以下を基準とし、運用設計において記録する項目を決定すること。

(ア) パソコン（ドメイン）へのログイン、ログオフ（ログインしたユーザ情報を含む）

(イ) ファイルの作成（保存）、移動、コピーなどのファイルの操作記録（ファイルサーバや外部媒体へのアクセスを含む）

(ウ) ファイルの印刷などファイルの出力記録

(エ) スクリーンショットの取得（PrintScreen）など、クリップボード操作に関する記録（取得した内容までの記録は行わない）

(オ) 外部媒体の接続

(カ) プログラムによるファイル生成や編集、コピーなど

(キ) 通信デバイスの接続

2.1.5.3. パソコンの不正操作に関する通報

ア．不正操作の恐れのある操作（例えば、容量の大きなファイルや多数のファイルのコピー、印刷等を想定）が行われた場合、管理者へ通報することが可能なこと。

イ．なお、個人番号利用事務系ネットワークは他セグメントとの通信は管理用の限られたものしか許可されていない為、通報方法について検討すること。

2.1.5.4. エージェント等未インストールパソコンの検出

ア．管理対象パソコンのうち三重県が指定するエージェント等がインストールされていない、またはインストールされているが動作していないパソコンの検出が可能なこと。なお、検出方法については、インベントリ取得日時等による把握も可とする。

2.1.5.5. 管理対象パソコンの追加・削除

ア．管理対象となるパソコンが追加・削除された際に、当該パソコンに関する情報を追加・削除できること。

イ．新たな管理対象パソコンへのエージェント等のインストールマニュアル等を整備すること。

2.1.5.6. ログの抽出・分析

ア．記録されたログについて、外部媒体へのファイル保存・コピーや印刷等の操作内容の他、対象のパソコン、利用者、日時等の情報により抽出・分析が可能なこと。

イ．外部媒体へのファイル保存やコピーなど、不正な情報持ち出しや情報漏えい等につながる可能

性のある操作について、拠点、パソコン、利用者別などに集計した月次レポート等の作成が可能なこと。

ウ．パソコン操作ログについては膨大な量になることが予想されるため、大量のログについて効率よく検索・分析等が可能なこと。

2.1.6. 外部媒体使用制限機能

2.1.6.1. 方針

ア．パソコンからの不正な情報持ち出し、不正な外部媒体の使用によるマルウェア被害や情報漏えいを防止するため、使用できる外部媒体を限定するとともに使用できるパソコン、使用できる職員を限定できる完了を構築すること。

2.1.6.2. 対象とする外部媒体

ア．以下に掲げるようなパソコンから切断しても情報が保持される記録媒体について、外部媒体単位での使用許可・禁止が制御可能なこと。

(ア) USB メモリ

(イ) 外付けハードディスク（USB 接続のもの）

2.1.6.3. 対象とする外部媒体読み取り・書き込み装置

ア．以下に掲げるような外部媒体の読み取り・書き込み装置については、個々の外部媒体の管理が困難であるため、パソコン単位、接続インターフェースまたは読み取り・書き込み装置単位での使用許可・禁止が制御可能なこと。

(ア) PC カード、Express Card スロットに接続された外部媒体読み取り・書き込み装置

(イ) CD/DVD 読み取り・書き込み装置

(ウ) メモリカード読み取り・書き込み装置

(エ) その他、USB 以外のインターフェースに接続された外部媒体及び外部媒体読み取り・書き込み装置

2.1.6.4. 使用可能な媒体の制限

ア．許可された媒体以外は使用できないような制限が可能であること。

イ．個々の媒体について、「2.1.6.5. 使用可能なパソコンの制限」「2.1.6.6. 使用可能な利用者の制限」との組み合わせによる使用制限・使用許可が可能なこと。

ウ．許可されていない外部媒体について、マウントや読み書きを禁止できること。

2.1.6.5. 使用可能なパソコンの制限

ア．個々の外部媒体及び外部媒体読み取り・書き込み装置について、使用できるパソコンの制限をかけることが可能なこと。

イ．使用が許可された媒体であっても、許可されていないパソコンで使用しようとした際には、マウントや読み書きを禁止できること。

2.1.6.6. 使用可能な利用者の制限

ア．個々の外部媒体について、使用できる利用者について制限をかけることが可能であること。

イ．使用が許可された媒体であっても、許可されていない利用者が使用しようとした際には、マウントや読み書きを禁止できること。

2.1.6.7. 許可媒体の追加・削除・アクセス権の変更

ア．新規媒体を追加する場合は、以下のいずれかのフローによること。

(ア) 申請者が別途ツール等を用いて取得した媒体情報及び申請書類等を送付し、セキュリティ対策システム管理者（運用保守担当者）が登録を行う。なお、個人番号利用事務系ネットワークは他セグメントとの通信は管理用の限られたものしか許可されていない為、連絡方法について検討すること。

(イ) 各拠点で仮登録を行い、各拠点からの申請に基づきセキュリティ対策システム管理者（運用保守担当者）が本登録を行う。

イ．不要となった外部媒体については、許可媒体から削除し、使用不可とできること。

ウ．媒体を使用できるパソコンや利用者の変更に対応できること。

エ．媒体を使用できる期間の指定ができること。

2.1.6.8. ログの記録・抽出・分析

ア．外部媒体の使用を拒否した際には、日時、外部媒体に関する情報、利用パソコン、利用者に関する情報をログとして記録できること。

2.1.7. 外部媒体暗号化機能

2.1.7.1. 方針

ア．「2.1.6.2. 対象とする外部媒体」で指定する外部媒体の紛失や盗難時の情報漏えいを防止するため、外部媒体への情報記録時に暗号化を必須とする環境を構築すること。

2.1.7.2. 外部媒体の暗号化

ア．外部媒体にファイルをコピーする際には、暗号化を必須とし、平文での保存は禁止できること。

イ．暗号化方式はパスワードつきの ZIP 形式を基本とするが、他の形式を採用してもよい。他の形式を採用する場合は、他の団体へのデータ受け渡し等を考慮した形式での保存も可能であること。

2.1.7.3. パソコンや利用者による制限の緩和

ア．特定のパソコン、特定の利用者に対しては、暗号化せずに媒体に出力できること。

2.1.8. パソコン暗号化機能

2.1.8.1. 方針

ア．パソコンの不正持ち出しやパソコンの盗難時の情報漏えいを防止するため、パソコン自身に記録された情報を暗号化できる環境を構築すること。

2.1.8.2. パソコン暗号化

ア．パソコンのハードディスクに記録された情報を自動的に暗号化できること。

イ．暗号化する領域は、ハードディスク全体もしくは OS、プログラムフォルダ以外のいずれかで可能なこと。

ウ．パソコンの使用時には暗号化を意識せずに使用できること。

エ．管理者側で一元管理可能な製品であること。

オ．OS 起動前にパスワード要求を行えること。また、パスワードの初期化を管理者側で可能なこと。

2.1.8.3. 対象外フォルダやパソコンの設定

ア．OS、プログラムフォルダ以外を暗号化する方式を採用する場合は、既存システムの動作要件等により、特定のフォルダ・ファイルや特定のパソコンについて暗号化を行わない設定が可能なこと。

イ．パソコンの暗号化を行う、行わないなどの設定について一元管理が可能なこと。

2.2. その他機能に関する設計

その他機能については以下の方針及び機能要件を踏まえて設計を行うこと。

2.2.1. 名前解決（DNS）

ア．セグメント内の名前解決を行うため、DNS サーバを構築すること。

イ．DNS 機能はいずれかの機能を実現するために導入するサーバが兼ねることとしてよい。

ウ．セグメント外のサーバ等の名前解決については、必要に応じて手動で登録できること。また、特定のドメインに対しては、指定の DNS サーバを参照するよう設定できること。

エ．外部のセグメントに設置されている DNS サーバと連携させることは想定していない。

2.2.2. 時刻同期（NTP）

ア．セグメント内のパソコン、サーバ等の時刻同期を行うため、NTP サーバを構築すること。

イ．NTP サーバは AD サーバが兼ねることを想定している。

ウ．NTP サーバについて、外部のセグメントに既設の NTP サーバと時刻同期するよう設計すること。

2.2.3. バックアップ

2.2.3.1. 基本的な考え方

ア．機器等の故障によるデータ消失に備えるため、各機能の設定情報、認証等に関する情報、ログ等についてバックアップを取得できること。

イ．バックアップは自動的に取得できること。バックアップは各機能の動作に支障がないよう、夜間に行うことを想定している。

ウ．バックアップの取得は、バックアップ用サーバでの集中管理を想定しているが、アプライアンスサーバ等で集中管理が困難な機器等についてはこの限りではない。

エ．バックアップ媒体（テープ等）を用いる場合は適宜交換を行うこと。なお、テープ交換はオートローダ等を用いて自動化すること。

2.2.3.2. バックアップの取得頻度及び世代数の考え方

ア．セキュリティ対策システムにかかる設定情報等

セキュリティ対策システムにかかる設定情報等のバックアップは､週に 1 回フルバックアップ、その他の日は必要に応じて差分もしくは増分によるバックアップを取得すること。バックアップデータを集中管理する場合は、サーバごとにリストアが可能なこと。また、複数世代の管理を行うこと。

イ．ログ等

ログ等のバックアップについては日次で取得し、セキュリティ対策システムの運用期間内にお

けるすべてのログを保持できること。バックアップしたログについても必要に応じて参照や検索が可能なこと。

2.2.4. 稼働監視

2.2.4.1. 基本的な考え方

ア．導入する機器のうち、サーバ、ネットワーク機器等障害時にセキュリティ対策システム全体に影響が及ぶ機器については、稼働状況の監視を行うこと。

イ．監視項目については、死活監視のほか、障害の前兆をとらえられる情報（CPU、メモリ等の使用率、プロセスの稼働状況、その他ハードウェア、ソフトウェア障害等）等、安定稼働に有用なものがあれば対象とする。

2.2.4.2. 監視方法及び監視項目

ア．監視対象

サーバ、ネットワーク機器等、障害時にセキュリティ対策システム全体に影響が及ぶ機器を対象とする。

イ．監視項目

監視項目については、セキュリティ対策システムの安定稼働に有用なものを受託事業者が選定し、三重県の承認を得ること。

ウ．通報の方法

本委託業務で業務系セグメントに障害情報を集約する機器等を設置し、業務系セグメントより通報する方式または三重県が別途構築し運用を行っている監視システムにより監視を行う方式を想定しているが、ガイドライン等の趣旨に反しない方法であれば他の方式の採用も可能である。

2.2.5. アカウント

ア．本セキュリティ対策システムを使用・運用するために必要となる、管理者アカウント、利用者アカウント等の設計を行うこと。

イ．利用者アカウントは連携する Active Directory サーバの情報を引き継ぐこととするが、生体認証情報との紐づけ設定が実施できること。

2.2.6. 運用業務

ア．各機能の運用にあたって必要となる運用設計（パソコン・利用者・媒体の追加・変更・削除時の対応など）を行うこと。

イ．運用設計に基づき、運用マニュアルを整備すること。

2.2.7. セキュリティ対策

ア．マルウェア等からの被害を防止するため、導入するソフトウェア等は既知の脆弱性等に対応した最新のものとすること。

イ．マルウェアへ対応するため、導入するサーバ機器等（運用管理用パソコンを含む）にはウイルス対策ソフトを導入するとともに、パターンファイルが常に最新となるよう設計を行うこと。

ウ．Windows OS で動作するサーバ、パソコンについては、本業務で構築するパソコン管理機能における WSUS サーバからセキュリティパッチの配信を受けるよう設計すること。

エ．ウイルス対策ソフトについて、本業務で構築するパソコン管理機能によりパターンファイル等の配信を受けるよう設計すること。

3. ハードウェア・ソフトウェア要件

3.1. 基本的な考え方

ア．本セキュリティ対策システムの設計、構築、導入及び運用に伴い必要となる全てのハードウェア、ソフトウェア等の物品（以下、納入物品という。）の取得、設定に関することを業務範囲とする。

イ．納入物品の設置に伴って必然的に必要となる物品（ラック取り付け金具や、ケーブル等の接続部品等）についても提供すること。

ウ．落札決定後速やかに業務計画書の一部として納入物品の一覧を提出することとするが、納入時点での製品状況が業務計画書提出時点より変わった場合は、三重県の承認を得たうえで最新の製品状況に従い最適な物品を納入すること。

エ．納入物品は原則「国際エネルギースタープログラム」に適合するものであること。適合外の機器を納品する場合は、事前に三重県の承認を得たうえで納入すること。

オ．納入物品は、新品、買い取りで提供すること。

カ．納入物品等に伴うマニュアル、技術資料等については、必要部数を提供すること。

キ．納入に際して、梱包材、三重県が不要と判断する付属品、マニュアル等を撤去すること。

ク．バックアップ及びクリーニングに必要な外部媒体等がある場合は、委託期間内において必要な量を見積り、確保するとともに、三重県の要請に応じ納入すること。

ケ．運用期間終了後、本委託業務範囲に係る物品（本委託業務で導入したハードウェア等）については、三重県が指示するものを除き、受託事業者側で撤去を行うこととし、データの消去と機器の廃棄を証明する書類を提出すること。ただし、全ての HDD 及び SSD は三重県にて物理破壊を行ってから処分することとする。

コ．納入したソフトウェアは本委託業務終了後も三重県にて利用できるものとすること。

サ．納入物品のすべてを保守対象とし、一つの窓口で対応すること。

3.2. 性能要件

3.2.1. サーバ要件

以下の要件を満たす機器の構成・性能とすること。

ア．サーバ構成について

本委託業務で導入するセキュリティ対策システムの各機能を実現するために必要となるサーバを用意すること。CPU、メモリ、ディスク容量等に関しては、性能要件を満たす構成とすること。なお、複数の機能を 1 台のサーバで実現してもよい（仮想化技術による統合も可とする）。

イ．処理能力及びライセンス

本委託業務で導入する機器を除き、パソコン 170 台、サーバ 60 台、職員数 500 人の利用を想定し十分な処理能力を有すること。また、製品により適切なライセンスを導入すること。

なお、将来の拡張性を考慮し、ソフトウェア等のライセンス、パソコンに接続する生体情報等の読み取り装置を追加購入するだけで、本委託業務で導入する機器を除き、パソコン 500 台、サーバ 100 台、職員数 1,000 人程度の規模でも運用可能な処理能力を有すること。

ウ．容量

パソコン操作ログ等のログ情報について、1 年分のログが保存できる容量を確保すること。また、バックアップ領域に 6 年分のログが保存できる容量を確保すること。

エ．クライアント

Windows 10 Pro、Windows 11 Pro のパソコンに対応していること。

Web ブラウザを使用する場合には、Microsoft Edge に対応していること。

オ．ディスプレイ

ラックマウントタイプとすること。

3.2.2. 運用管理パソコン要件

本セキュリティ対策システムの管理を行うために必要となる運用管理パソコンを導入すること。

ア．パソコン構成について

本委託業務で導入するセキュリティ対策システムの各機能の管理のために必要となるパソコンを 2 台以上用意すること。

イ．ソフトウェア

運用管理パソコンには、セキュリティ対策システムの運用管理に必要となるソフトウェアをインストールすること。

3.3. ハードウェア設置要件

3.3.1. 共通事項

ア．機器の導入にあたり、各機器の搬入、設置、設定作業は原則受託事業者が全て行うこと。

イ．通信ケーブル等に負荷の掛からない配線とすること。

ウ．サーバのディスプレイ、キーボード等に関しては複数サーバ間で共用するなどの省スペースに配慮した構成とすること。

エ．各機器についてソフトウェア等のインストール及び必要な設定を行った後に設置場所へ納入すること。

オ．設置場所への納入および設置作業、配線作業ならびにネットワークへの接続作業の実施においては、事前に実施日時を三重県と調整すること。また、搬入時は三重県が別途指示する搬入口およびエレベータを使用し、設備、器物破損を防止するための措置を講じること。

カ．ハードウェアの納入を円滑に進めるため、事前に三重県にスケジュール等を説明し、協議のうえ三重県の指示に従い実施すること。

3.3.2. データセンタ設置機器

3.3.2.1. サーバ設置場所

サーバ機器については三重県が指定するデータセンタ（三重県津市内）に設置すること。

3.3.2.2. データセンタ契約

三重県は個人番号利用事務系ネットワークにおけるセキュリティ対策システム用にラックを契約しているが、現行セキュリティ対策システムの機器を撤去（令和 4 年 10 月末予定）するまでは本委託業務で導入する機器の設置スペースを確保していない。よって、三重県が契約するラックを利用できるタイミングまでは、三重県が指定するデータセンタにおけるラック契約を、本委託業務の受託事業者の負担で行うこと。その後、現行セキュリティ対策システムの機器が撤去された後に、三重県が契約するラックへ機器の移設を行うこと。なお、移設日程については三重県と受託事業者で協議して決定することとするが令和 4 年 11 月中を想定している。また、業務への影響を考慮し、作業は夜間または閉庁日に実施すること。

なお、「基本仕様書 2.3 イ」により運用開始時期を遅らせる場合は、受託事業者によるラックの利用契約期間が長くなるため注意すること。

3.3.2.3. 三重県が準備するデータセンタ概要

ア．データセンタの使用ラックスペースは最大 16U（機器間の空きスペースを含む）とする。なお、ラックの規格は H2,000mm×W700mm×D1,000mm(42U)である。

イ．ラックに機器をマウントする際には、空調・ファンの稼動など、ラック内の温度を考慮した設置を行うこと。

ウ．ラックの設置位置においては、必要に応じてブランクパネル等を使用し通気通路を考慮すること。

エ．ラックにマウントできない機器に関しては耐震バンド等により耐震・免震措置を施すこと。

オ．本業務の契約期間中、追加ラックが必要な場合、そのハウジング契約は、本調達の契約範囲で用意すること。

カ．機器、ラック、分電盤、電源ケーブル及び通信ケーブルにラベル表記すること。

キ．データセンタに設置する機器類は、入力電圧として 5-15R AC100V に対応していること。

ク．ラックで提供する電源は、20A までとする。なお、それ以上に必要な場合は受託事業者にて追加電源の費用を負担すること。

ケ．指定データセンタにおいては停電対策がとられており、UPS 等による個別の停電対策は不要である。

3.3.3. 生体情報読み取り装置

ア．各パソコンに接続する生体情報読み取り装置については、三重県本庁舎 7 階サーバ室内へ納入した後にパソコンとともに利用者へ配布すること。

イ．現行セキュリティ対策システムにて利用中の生体情報読み取り装置（120 台）も継続して利用可能であるが、契約期間中は全て保守を行うこと。なお、台数の不足分については新たに納品すること。

3.3.4. 運用管理パソコン

ア．セキュリティ対策システムの運用管理のために必要となる管理用パソコンについては、三重県本庁舎 7 階サーバ室内へ納入すること。

3.3.5. その他機器

ア．各拠点等に設置する機器がある場合には、それぞれ必要な拠点に機器を設置すること。

3.4. 冗長化にかかる要件

ア．利用者認証サーバを除くサーバ機器については、ディスクの冗長化のみを必須とし、機器を複数台用意するなどの冗長化については必要に応じて実施すること。

イ．なお、利用者認証サーバについて、Active Directory サーバと生体認証を行うサーバ（以下、「生体認証サーバ」という。）が異なるサーバであり、生体認証サーバの障害時においてもパソコンにおいて引き続き認証を行うことが可能な場合は、生体認証サーバについての冗長化も不要とする。

3.5. ソフトウェア要件

3.5.1. 共通

ア．使用するソフトウェアはセキュリティ対策システムへの影響がない限り、最新のセキュリティパッチの適用を行ったうえで納入すること。

イ．新規にソフトウェアを納入する場合は、実際に使用するバージョンに関わらず、最新バージョンの使用権を確保すること。

ウ．使用するソフトウェアとして、要件を満たすソフトウェアを選定し、納入すること。

3.5.2. 必要ライセンス

必要ライセンス数は、本委託業務で導入する機器等を除き、以下のとおりとする。

ア．管理対象端パソコンは 170 台、サーバは 60 台とする。

イ．パソコンを利用する職員（利用者数）は 500 人とする。

ウ．運用管理用ソフトウェアの運用管理担当者は 15 人とする（受託事業者が利用するライセンス 1 を含む）。

エ．その他、各種ソフトウェアについて必要なライセンスを確保すること。

3.5.3. マイクロソフト製品のライセンス

三重県では以下のクライアントライセンスを全職員分保有しており、本セキュリティ対策システムにおいても利用可能である。ただし、以下のクライアントライセンス以外のライセンスが必要となる場合は、受託事業者にて準備すること。

CAL の種類
Windows Server 2019 ユーザ CAL

3.5.4. ウイルス対策ソフトライセンス

ウイルス対策ソフトのライセンス調達も本委託業務の範囲内とする。なお、パターンファイル取得の関係上、別紙「個人番号利用事務系ネットワークで利用可能なウイルス対策ソフト」から選定すること。

3.6. 三重県が用意するシステム等

3.6.1.1. 障害監視システム

各種サーバやネットワーク機器を監視するための障害監視システム（zabbix）を利用できる。利用には、対象となる機器の設定追加や、警告時の対応等についても決定する必要がある為、注意すること。

3.6.2. 自治体情報セキュリティ向上プラットフォーム

個人番号利用事務系ネットワークで利用する Microsoft 社製品やウイルス対策ソフトの更新プログラム、パターンファイルは「自治体情報セキュリティ向上プラットフォーム」より取得すること。「自治体情報セキュリティ向上プラットフォーム」の契約は別途三重県が行う。

4. セキュリティ対策システム導入及び各種設定要件

4.1. 基本的な考え方

ア．導入する各パッケージソフトウェアの機能の範囲内で運用し、カスタマイズ等は実施しない。

イ．「２．各種詳細設計」で策定した設計に基づき必要な構築及び設定を行うこと。

4.2. セキュリティ対策システム導入及び設定

4.2.1. 共通要件

ア．各機能に共通する要件は以下のとおりとする。

(ア) 各機能を実現するために必要となる機器を導入し、必要な設定を行うこと。

(イ) 必要なログが取得できるよう設定を行うこと。

4.2.2. パソコン管理機能

ア．セキュリティパッチの管理

(ア) ネットワーク内のパソコン、サーバに対し、Microsoft 社製品及び Adobe 社製品のセキュリティパッチの配信ができるよう設定を行うこと。

(イ) ネットワーク内のパソコン、サーバ等をグループ化し、グループごとにパッチ配信が行えるよう設定すること。

(ウ) Microsoft 社製品についてはセキュリティパッチを自治体情報セキュリティ向上プラットフォームから配信を受けるよう設定すること。

イ．ウイルス対策ソフトの管理

(ア) ネットワーク内のパソコン、サーバに対し、ウイルス対策ソフトのパターンファイル、プログラム等の配信ができるように設定を行うこと。

(イ) ウイルス等が検出された際に、ウイルス名、コンピュータ名、パス名及び対処結果を管理者側で確認ができるよう設定を行うこと。

(ウ) パソコンについては、週に１回程度の定期的なウイルススキャンの設定を行うこと。

(エ) パターンファイルについては自治体情報セキュリティ向上プラットフォームから配信を受けるよう設定すること。

ウ．パソコン情報の取得・出力

(ア) ネットワーク内のパソコン、サーバの情報が取得できるよう設定を行うこと。

(イ) あらかじめ、動作している OS 別や、エージェント等がインストールされていないパソコン、ウイルス対策ソフトがインストールされていないパソコン等のグループ設定を行うこと。

エ．プログラム等の配信機能

(ア) ネットワーク内のパソコン、サーバに対し、セキュリティ対策システムの運用のために必要となるエージェント等が自動的にインストールされるよう設定を行うこと。

(イ) ウイルス対策ソフトについても未インストールのパソコンにインストールされるよう設定を行うこと。

オ．パソコン設定管理機能

(ア) 別セグメントに既設の Active Directory サーバで設定しているグループポリシーに準じた設定を適用すること。

(イ) 個人番号利用事務系ネットワーク内のパソコンに対して、個人番号利用事務系ネットワーク独自の設定について適用を行うこと。独自の設定としては以下を想定しているが、個人番号利用事務系ネットワークの特性に応じて有用な設定等があれば、三重県の了承を得たうえで設定を行うこと。

- Microsoft 社製品に対するセキュリティパッチ配信サーバの設定
- Adobe 社製品に対するセキュリティパッチ配信設定
- ウイルス対策ソフト管理サーバの設定
- 本業務で利用するエージェント等のインストールに関する設定

カ．リモート操作機能

(ア) ネットワーク内のパソコンに対してリモート操作が行えるよう設定を行うこと。

4.2.3. パソコン認証機能

ア．個人番号利用事務系ネットワークに接続を許可するパソコンについて、初期登録作業を実施すること。登録するパソコンについては三重県から提示する。

イ．許可されたパソコン以外は接続できないよう設定を行うこと。

ウ．不正パソコンが接続された際にログ等が記録されるよう設定を行うこと。

4.2.4. 利用者認証（生体認証）機能

ア．別セグメントに既設の Active Directory サーバと連携し、ユーザ情報が取得できるよう設定を行うこと。

イ．既設の Active Directory サーバの設定に準じ、ログイン時のウイルス対策ソフトのインストールや各種ソフトウェアのバージョンチェック等が行えるよう設定を行うこと。

ウ．現行セキュリティ対策システムで使用を許可されている利用者について、次期セキュリティ対策システムへの登録作業（生体情報の登録を含む）を行うこと。なお、登録にあたっては、生体情報の収集までは三重県が行うため、必要な支援等を行うこと。

エ．生体認証装置について、あらかじめ複数人を対象とした動作検証を行い、「2.1.4.3. 生体認証機能（イ）」に定める精度が実現できることを確認すること。精度が低い場合には、必要に応じてチューニング等を行うこと。

オ．生体認証読み取り装置の展開（ドライバインストール方法など）について支援を行うこと。

カ．原則として、生体認証を行った利用者以外は個人番号利用事務系ネットワークに接続することができないよう設定を行うこと。

4.2.5. パソコン操作ログ記録機能

ア．実際に記録する操作内容について検討し、設計及び設定を行うこと。

イ．レポートとして出力する条件や内容について検討し、設定を行うこと。

4.2.6. 外部媒体使用制限機能

ア．利用を許可する媒体について、利用を許可するパソコン及び利用者の情報を含めて設定を行うこと。媒体のリストは三重県より提示する。

イ．外部媒体を追加・削除する場合、利用を許可するパソコンや利用者を追加・削除する際の業務フローについて検討し、必要な設計・設定を行うとともに、三重県が作業する部分についてマニュアル等を整備すること。

4.2.7. 外部媒体暗号化機能

ア．外部媒体へファイルをコピーする際に暗号化を必須とする設定を行うこと。

イ．例外とする条件（パソコン、利用者、媒体）の設定を行うこと。

ウ．例外設定を追加・削除する際の業務フローについて検討し、必要な設計を行うとともに、三重県が作業する部分についてマニュアル等を整備すること。

4.2.8. パソコン暗号化機能

ア．管理対象パソコンを暗号化するための設定を行うこと（既設のパソコン、新規設置するパソコンについても同様とする）。

イ．暗号化にあたっては、既存システムへの影響を考慮すること。

ウ．OS、プログラムフォルダ以外を暗号化する方式を採用する場合は、以下についても対応すること。

（ア）既存システムの動作に支障がある場合にはフォルダ・ファイル単位やパソコン単位での除外を行うこと。

（イ）除外設定を追加・削除する際の業務フローについて検討し、必要な設計を行うとともに、三重県が作業する部分についてマニュアル等を整備すること。

4.3. その他機能に関する設定

4.3.1. 名前解決（DNS）

ア．セグメント内のパソコン、サーバ等の名前解決について、本委託業務で構築する DNS サーバを参照するよう設定すること。

イ．DNS サーバによる名前解決を行わないサーバがある場合（外部セグメントのサーバ等）については、必要に応じて Hosts ファイル等により名前解決を行うよう設定すること。

4.3.2. 時刻同期（NTP）

ア．セグメント内のパソコン、サーバ等の時刻同期について、本業務で構築する NTP サーバと同期するよう設定すること。

イ．パソコンについては、ドメインへのログイン時に時刻同期することを想定している。

4.4. バックアップ設定

ア．「2.2.3 バックアップ」に基づき必要なバックアップが取得できるよう設定を行うこと。

4.5. 稼働監視設定

ア．障害時にセキュリティ対策システム全体に影響が及ぶサーバ等の稼働監視ができるよう設定すること。

4.6. アカウント設定

ア．セキュリティ対策システムを使用・運用するために必要となる管理者アカウント、利用者アカウント等を登録すること。

イ．利用者アカウントのリストは三重県より提示する。

4.7. セキュリティ対策

ア．本委託業務で導入するサーバ（運用管理パソコンを含む）において、WSUS サーバ、ウイルス対策ソフト管理サーバ、パソコン管理ソフトウェア等からセキュリティパッチ、パターンファイルを受信できるよう設定すること。

5. パソコン及びプリンタ更新要件

5.1. 基本的な考え方

ア．セキュリティ対策システムの構築完了後、令和 4 年 9 月 1 日から令和 4 年 9 月 30 日までを移行期間とし、全拠点におけるパソコン及びプリンタにおいて。次期セキュリティ対策システムを利用できるようにすること。

イ．三重県が別途準備するパソコン（大半は新規購入品となる予定）を対象にキッティング作業を行い、本業務で導入するセキュリティ対策システムを利用可能な状態にすること。

ウ．職員が現在使用しているパソコンからデータを移行し交換配付を行うこと。

エ．現在利用中で一部更新しないパソコンについては本委託業務で導入する次期セキュリティ対策システムを利用可能な状態に設定すること。

オ．三重県が新たに購入するプリンタに設定を行い、パソコンの交換配布時にあわせてプリンタの交換配布を行うこと。

カ．移行期間中に、運用に支障が生じることが判明した場合には、設定や運用の見直しを行うこと。

キ．移行期間中は、十分な検証を実施し、検証結果について三重県の承認を得ること。

5.2. パソコン交換配布

5.2.1. 作業内容の確認

「5.1 基本的な考え方」を踏まえて事前に全ての作業内容を三重県に提出し承認を得ること。

5.2.2. 履行場所別概数

履行場所別概数は下記の通りである。修理・交換等により台数、設置場所が変動することがあるが、若干の台数増減には対応すること。

利用場所	数量
本庁	50
吉田山会館	1
桑名庁舎	7
四日市庁舎	9
鈴鹿庁舎	5
津庁舎	7
松阪庁舎	4
伊勢庁舎	15
伊賀庁舎	5
尾鷲庁舎	12
熊野庁舎	11
北勢児童相談所	1
中勢児童相談所	1
障害者相談支援センター	11
計	140

5.2.3. 作業台数

パソコン作業台数の内訳は下記の予定である。ただし、数台程度の増減には対応すること

ア．新規購入パソコンのキッティング（セキュリティ対策システム導入を含む)、交換配布　120 台

イ．利用中のパソコンに本業務で導入するセキュリティ対策システムを導入　20 台

5.2.4. 作業計画

ア．令和4年9月27日までに対象パソコン交換等の作業が終了するように作業計画を作成すること。

イ．交換配付作業は、1 台あたり 3 時間以内を目安と見込んでいる。

ウ．キッティング作業の時間は、平日 8 時 45 分から 17 時 15 分までとして、作業を計画すること。

エ．パソコン運搬の時間は、 原則として平日 8 時 45 分から 17 時 15 分までとする。ただし、時間外の受け渡しが必要な場合は、事前に県と協議すること。

オ．交換配付は平日 9 時 00 分から 16 時 00 分までとする。

カ．履行場所は、原則として 1 日 1 ヶ所とする。ただし、進捗によっては最大 3 ヶ所までの同時作業を行う場合がある。

キ．気象条件、交通事情、停電または履行場所の都合等により更新作業を延期する場合がある。更新作業期間とは別に予備日を設定する等、スケジュールを工夫すること。

ク．各パソコンには個人番号利用事務系ネットワークで利用する各種システムが入っている。このため、必要に応じて、三重県がシステムのインストール作業等を交換配布スケジュールに合わせて関係事業者と調整するため、この調整結果をふまえて作業計画を再調整すること。

5.2.5. 準備作業

ア．受託事業者は、キッティングおよびデータ移行作業の手順書を作成し、三重県に説明すること。

イ．Ghost solution suite を使用した OS イメージを、受託事業者にて作成すること。
OS イメージは、 以下の ソフトウェアを含むこととする。

・Windows 10 Pro
・Microsoft Office Standard 2016 または Professional Plus 2016
・Microsoft Edge
・Adobe Acrobat Reader DC
・ウイルス対策ソフト

なお、Ghost solution suite は三重県保有のライセンスを利用すること。

ウ．実機を使用し、手順及び時間配分を検証すること。実機については三重県が指定するものを利用すること。

エ．履行場所別、作業日別の対象パソコンの割り当ては、作業計画に従い三重県が行う。

オ．受託事業者は、キッティングおよび交換配付作業に必要となるハブ等ネットワーク機器、LAN ケーブル及び OA タップ等を準備すること。

5.2.6. キッティング作業

ア．作業スペースは、パソコン保管場所と同階に三重県が準備した長机約 2 台分のスペースを利用可能。パソコンを庁外に持出して受託事業者が準備した場所でキッティング作業を行う場合は、県と事前に協議をすること。

イ．Windows ログイン用のパスワードは県が指示するものを利用すること。

ウ．Ghost solution suite を利用したイメージの展開後、コンピュータ名の設定、Windows のライセンス認証、ウイルス対策ソフト及び本委託業務で導入するセキュリティ対策システムのインストール、その他必要となる設定等を行うこと。コンピュータ名は、三重県が指定する管理番号とすること。

エ．三重県ドメインへの参加およびグループポリシーの適用を行うこと。ドメイン参加時のアカウント情報は三重県が指示するものを利用すること。

オ．デバイスの起動順序（BIOS 設定）は、 1 USB 、2 SSD または HDD とすること。

カ．三重県指定の管理番号をラベルシールに印刷し、パソコン本体に 2 か所、AC アダプターに 1 か所に貼付すること。

キ．パソコン本体の製造番号、管理番号 の一覧を作成すること。

ク．「ウ」および「エ」の作業は、交換配付作業時に実施しても構わない 。

5.2.7. 交換配布会場

ア．交換配付場所は、本庁舎 7 階会議室、各総合庁舎情報機器室、児童相談所及び障害者相談支援センター会議室または各庁舎執務室で行うことを想定している。

イ．作業場所の利用方法（机、電源、LAN ポート等）については、三重県の指示に従うこと。

ウ．交換配付時の設定作業及びデータ移行は全て有線 LAN を使用すること。

5.2.8. パソコンの運搬等

ア．パソコン運搬用の車両は受託事業者が用意し、所要台数のパソコンを交換配付会場まで運搬すること。

イ．執務室から更新会場までの運搬は、三重県（対象パソコンの使用者）が行う。ただし、拠点によっては執務室で行う場合もあるため、執務室での対応も想定しておくこと。

ウ．履行場所の更新会場におけるパソコンの受付及び返却は原則、三重県が行うが、三重県から指示があった場合は、受託事業者で対応すること。

エ．パソコンの梱包材等は受託事業者が処分すること。

5.2.9. 交換配布作業前の確認

ア．対象パソコンごとにチェックシートを準備し、開始時刻を記録すること。

イ．交換配付作業前に、本体の破損、故障及び異音の有無を確認すること。

ウ．対象パソコンの異常を見つけた場合は、作業を中断し県に報告すること。

エ．旧パソコンの CD ドライブ内を確認し、ディスクが残っていないか確認すること。ディスクが発見された場合は、三重県に報告すること。

5.2.10.ユーザデータ移行

ア．三重県が指定した ID で PC にログインすること。

イ．移行するユーザデータは、ユーザーフォルダ（デスクトップ、マイドキュメント等）、Microsoft Edge のお気に入りとする。詳細は三重県が別途指示する。

ウ．ユーザデータについて、正確に移行するため、保存フォルダのファイル数及びファイルサイズを確認し記録すること。

エ．ユーザデータの移行は、LAN 経由で旧パソコンから新パソコンにコピーする方法を想定している。なお、他に効率的な方法があれば、検証を行ったうえで認める。いずれの方法であっても、使用する機器及びソフトウェア等は受託事業者が準備すること。

オ．初期設定（ローカル ID、IP アドレス設定等）については、三重県からの指示に従い確実に実施すること。

カ．Windows 及び Office のライセンス認証を行うこと。ただし、電話認証等インターネット以外での方法で認証を行うこと。

キ．三重県が指定したプリンタドライバのインストール、設定を行うこと。

5.2.11. データ移行以外の作業

ア．配布前に Microsoft Edge、セキュリティ対策ソフト等が正常に動作しているか確認すること。

イ．更新プログラムや修正パッチを適用すること。

ウ．BIOS を最新化すること。

エ．交換配付作業用のユーザプロファイルを削除すること。

オ．除菌シート等でパソコンの消毒を行うこと。

カ．作業終了後に、三重県に報告し、Active Directory や WSUS 上でコンピュータが適切な状

態となっているか確認すること。

5.2.12. 作業に関する注意事項

ア．受託事業者が持ち込み使用できるソフトウェアは、開発元が明確であり、実績を有するものであること。また、使用について三重県の許可を得ること。

イ．個人番号利用事務系ネットワークは専用のネットワークで運用している為、他のネットワークと接続することは認めない。

ウ．パソコンに保存されているファイル、画像等について、内容の閲覧及び撮影、記憶媒体への複写及び移動を禁止する。

エ．対象パソコンのハードウェア不良を発見した場合は、ただちに三重県に連絡すること。

オ．ユーザデータのコピーまたは復元において、不具合または異常が発生した場合は、ただちにファイル損失の回避策を行い、その後すみやかに三重県に連絡すること。

5.2.13. 作業に関する注意事項

ア．回収したパソコンを更新会場から本庁舎へ運搬すること。

イ．本庁舎に到着後、損傷等が無いか確認し、チェックシートへ記入すること。

5.2.14. サポートデスク業務

ア．交換配布に関するパソコンの使用者からの問い合わせは三重県が対応する。その内容によっては、受託事業者に調査と回答を依頼することがある。

5.3. プリンタ交換配布

5.3.1. 履行場所別概数

現在のプリンタ利用状況は下記の通りである。修理等により台数、設置場所が変動することがあるが、若干の台数増減には対応すること。

履行場所	数量
本庁	7
桑名庁舎	2
四日市庁舎	2
鈴鹿庁舎	2
津庁舎	2
松阪庁舎	1
伊勢庁舎	4
伊賀庁舎	2
尾鷲庁舎	4
熊野庁舎	2
北勢児童相談所	1
中勢児童相談所	2
障害者相談支援センター	2

計	33

5.3.2. 作業計画

イ．令和 4 年 9 月 27 日までに対象プリンタの交換等の作業が終了するように作業計画を作成すること。

ウ．交換配布作業はパソコンの交換配布と同日に実施すること。

5.3.3. 準備作業

ア．三重県指定の管理番号をラベルシールに印刷し、プリンタ本体に 1 か所貼付すること。

イ．三重県指定の IP アドレスをプリンタに設定すること。

5.3.4. 交換配布会場

ア．パソコン交換配布会場と同一とする。

5.3.5. プリンタの運搬等

ア．運搬用の車両は受託事業者が用意し、所要台数の新プリンタを交換配付会場まで運搬すること。

イ．執務室から更新会場までの運搬は、三重県（対象プリンタの使用者）が行う。ただし、拠点によっては執務室で行う場合もあるため、執務室での対応も想定しておくこと。

ウ．履行場所の更新会場におけるプリンタの受付及び返却は原則三重県が行うが、三重県から指示があった場合は、受託事業者で対応すること。

エ．新プリンタの梱包材等は受託事業者が処分すること。

5.3.6. 交換配布作業前の確認

ア．対象プリンタごとにチェックシートを準備し、開始時刻を記録すること。

イ．交換配付作業前に、本体の破損の有無を確認すること。

5.3.7. 交換配布作業後の作業

ア．回収したプリンタを更新会場から本庁舎へ運搬すること。

イ．本庁舎に到着後、損傷等が無いか確認し、チェックシートへ記入すること。

6. Windows OS 及び Microsotf Office のバージョンアップ作業

6.1. 業務目的・範囲

ア．三重県が準備するパソコンの OS（Windows 10 Pro）及び Microsoft Office Professional Plus 2016 または Standard 2016 はサポート期限が令和 7 年 10 月 14 日の予定である。別途三重県が指定するタイミングで、個人番号利用事務系ネットワーク内の全パソコンに対して Windows OS、Microsoft Office のバージョンアップを行うこと。アップデート後のバージョンは令和 7 年に三重県が決定する予定である。

イ．Windows OS および Microsoft Office のライセンスは三重県が準備する。

6.2. 作業日程

令和 7 年度に実施予定である。詳細は三重県と受託事業者で協議して決定することとする。

6.3. 対象パソコン

個人番号利用事務系ネットワークで利用する全てのパソコンを対象とする。パソコン台数は令和 7 年度時点で 160 台程度を見込んでいる。

6.4. 作業概要

6.4.1. 作業計画

ア．サポート期限内に余裕をもって全てのパソコンの更新が終了するように三重県と協議のうえ作業計画を作成すること。

イ．作業は、1 台あたり 3 時間以内を目安と見込んでいる。なお、各パソコンには個人番号利用事務系ネットワークで利用する各種システムが入っている。このため、必要に応じて、三重県がシステムのインストール作業等をバージョンアップスケジュールに合わせて関係事業者と調整するため、この調整結果をふまえて作業計画を再調整すること。

ウ．１日の作業は、平日 8 時 45 分から 17 時 15 分までとして、作業を計画すること。当日受け付けた全パソコンを返却した時点で終了とする。

エ．履行場所は、原則として 1 日 1 ヶ所とする。ただし、進捗によっては最大 3 ヶ所までの同時作業を行う場合がある。

オ．気象条件、交通事情、停電または履行場所の都合等により更新作業を延期する場合がある。更新作業期間とは別に予備日を設定する等、スケジュールを工夫すること。

6.4.2. 準備作業

ア．受託事業者は、更新作業の手順書を作成し、三重県に説明すること。

イ．作業にあたっては、Ghost solution suite のライセンスを保有しているため、これを利用してもよい。ただし、ライセンス以外に必要な機器類があれば準備すること。また、イメージの作成も実施すること。

ウ．実機を使用し、手順及び時間配分を検証すること。実機については三重県が指定するものを利用すること。

エ．更新作業に必要となるハブ等ネットワーク機器、LAN ケーブル及び OA タップ等を準備すること。

6.4.3. 更新会場の設営と片付け

ア．バージョンアップ作業は本庁舎 7 階会議室、各総合庁舎情報機器室、児童相談所及び障害者相談支援センター会議室または各庁舎執務室で行うことを想定している。。

イ．作業場所の利用方法（机、電源、LAN ポート等）については、三重県の指示に従うこと。

ウ．バージョンアップ作業は全て有線 LAN を使用すること。

6.4.4. 対象パソコンの受け渡し等

ア．執務室から更新会場までの運搬は、三重県県（対象パソコンの使用者）が行う。ただし、拠点によっては執務室で行う場合もあるため、執務室での対応も想定しておくこと。

イ．履行場所の更新会場におけるパソコンの受付及び返却は原則、三重県が行うが、三重県から指示があった場合は、受託事業者で対応すること。

ウ．作業に関するパソコンの使用者からの問い合わせは三重県が対応する。その内容によっては、受託事業者に調査と回答を依頼することがある。

6.4.5. 更新作業前の確認

ア．対象パソコンごとにチェックシートを準備し、開始時刻・終了時刻を記録すること。

イ．更新作業前に、本体の破損、故障及び異音の有無を確認すること。

ウ．対象パソコンの異常を見つけた場合は、作業を中断し三重県に報告すること。

6.4.6. ユーザデータの確認と退避

ア．ユーザデータのバックアップ、復元についても対応すること。

6.4.7. バージョンアップ作業

ア．三重県が指定した ID で PC にログインすること。

イ．Windows OS の更新は、Ghost solution suite を利用するか、クリーンインストール作業を行うことを想定している。以降の記載は、クリーンインストールを想定して記載しているが、Ghost solution suite を利用することにより省略できるものがあれば、省略してもよい。

ウ．初期設定（ローカル ID、IP アドレス設定等）については、三重県からの指示に従い確実に実施すること。

エ．Office のインストール作業を行うこと。

オ．Windows 及び Office のライセンス認証を行うこと。ただし、電話認証等インターネット以外での方法で認証を行うこと。

カ．三重県指定のドメインを設定、参加すること。

キ．必要に応じて、修正パッチまたは更新プログラムを適用すること。

ク．本委託業務で導入するセキュリティ対策システム、ウイルス対策ソフト等をインストールし、設定すること。インストールに必要な情報・メディアについては三重県から提供する。

ケ．三重県が指定したプリンタドライバのインストール、設定を行うこと。

コ．作業終了後に、三重県に報告し、Active Directory や WSUS、パソコン管理ソフト上でコンピュータが適切な状態となっているか確認すること。

7. 運用保守要件

7.1. 基本的な考え方

ア．運用保守に必要なハードウェア、ソフトウェア等の準備はすべて受託事業者の作業範囲とする。

イ．サーバ機器、ネットワーク機器等、障害発生時にセキュリティ対策システム全体に影響が出る機器については、速やかに復旧させる必要があるため、オンサイト保守とする。

ウ．パソコンに接続する機器（生体情報読み取り装置）についてはオンサイトもしくはセンドバック保守とする。

7.2. 運用業務

7.2.1. ヘルプデスク

ア．　三重県では、セキュリティ対策システムに関する日常的な設定作業等を行う要員として「ヘ

ルプデスク」を別途契約しており、運用保守業務の一部を担当することが可能である。

イ．業務を実施するためには、締結済みの契約内容の範囲に限られる、マニュアルや手順書を作成する必要がある、業務引継ぎや研修を実施する必要がある、ヘルプデスク担当者を後方支援する体制が整備されている、など、一定の条件があるため、注意すること。

ウ．本委託業務の契約期間中において、ヘルプデスクにかかる契約期間が終了するが、その後も同種の契約を実施する予定のため、継続して業務が実施できる想定である。

7.2.2. 業務分担

セキュリティ対策システムの運用業務における受託事業者、三重県、ヘルプデスクの業務分担は以下のとおりとする。管理対象パソコン追加・削除時、利用者追加・削除時、外部媒体追加・削除時のサーバ設定作業については、年度末に多くの変更作業が発生すると予想されることから、3 月 31 日、4 月 1 日及び年度末を挟んだ 5 開庁日については受託事業者が対応し、それ以外の期間はヘルプデスクで対応することとする。

作業内容	受託事業者	三重県	ヘルプデスク
管理対象パソコン追加･削除時のサーバ設定作業	○（年度末）		○（それ以外）
新規管理パソコンへのエージェント､生体認証読み取り装置ドライバ等インストール作業	△（支援）		○
利用者追加・削除時のサーバ設定作業	○（年度末）		○（それ以外）
新規利用者にかかる情報の収集		○	
外部媒体追加・削除時のサーバ設定作業	○（年度末）		○（それ以外）
新規外部媒体にかかる情報の収集		○	
パッチによる影響等の情報提供	○		△（協力）
パッチインストール、パソコンへの展開	○	△（協力）	△（協力）
Windows OS 大型アップデート	○	△（協力）	△（協力）
稼働監視	○	△（協力）	△（協力）
障害一次切り分け	○	△（協力）	△（協力）
障害対応	○	△（協力）	
障害後予防措置・是正措置	○	△（協力）	
マニュアル等の改訂	○		
月次報告	○	△（出席）	
操作研修	○	△（出席）	△（出席）

7.2.3. 受託事業者が行う作業

7.2.3.1. 管理対象パソコン追加・削除時のサーバ設定作業（各年度末のみ）

ア．三重県からの依頼に基づき、管理対象パソコン情報の追加・削除を行うこと。

イ．具体的には、パソコン認証機能における許可パソコンの追加・削除、パソコン暗号化機能における暗号化範囲の反映等を想定している。

7.2.3.2. 利用者追加・削除時のサーバ設定作業（各年度末のみ）

ア．三重県からの依頼及び三重県が収集・仮登録した情報等に基づき、人事異動等に伴う利用者情報の追加・削除を行うこと。

イ．具体的には、利用者認証（生体認証）における対象者の追加・削除、外部媒体使用制限機能における許可の有無の反映等を想定している。

ウ．利用者のアカウントに関する情報は連携先の Active Directory サーバから入手し、利用者の生体情報と紐づける運用を想定している。

エ．年度末の人事異動時には利用者のうち最大 3 分の 1 程度の設定を短期間で変更することが必要となるため、必要な対応を行うこと。

7.2.3.3. 外部媒体追加・削除時のサーバ設定作業（各年度末のみ）

ア．三重県からの依頼及び三重県が収集・仮登録した情報等に基づき、外部媒体情報の追加・削除を行うこと。

イ．具体的には、外部媒体使用制限機能における許可の有無の反映等を想定している。

7.2.3.4. パッチによる影響等の情報提供

ア．セキュリティ対策システムで使用するソフトウェア製品（ファームウェア等を含む。三重県が別途インストールしたものを除く）に関するバグフィックス、セキュリティ対応等のパッチがリリースされた場合、速やかにその内容の調査を行い、適用の要否及び適用の可否を三重県に報告すること。

イ．適用が必要だがセキュリティ対策システムに影響がありすぐに適用できない場合は、適用するために必要となるセキュリティ対策システム改修の内容を三重県に報告すること。

ウ．パッチリリースから情報の提供までの期間は 1 週間以内とする。

7.2.3.5. パッチインストール、パソコンへの展開

ア．サーバ、運用管理パソコン等の機器について、適用が必要なパッチのインストールを行うこと。

イ．三重県が適用後の影響有無の確認作業を短時間に行えるよう必要な支援を行うこと。

ウ．パッチ適用により障害が発生した場合は、受託事業者にて障害対応を行うこと。

エ．パソコンにインストールするエージェントやドライバ等について、適用が必要なパッチの展開（パソコン管理機能による配信を想定）を行うこと。

7.2.3.6. Windows OS 大型アップデート

ア．個人番号利用事務系ネットワークで利用するパソコンに対して定期的（年 1 回程度の予定）に Windows OS の大型アップデートを行うこと。

イ．アップデートファイルを三重県へ提供すること

ウ．アップデート作業の手順書を作成すること

エ．三重県が保有する検証機において先行してアップデート作業行い、セキュリティ対策システムの動作確認を実施すること。

オ．各パソコンにアップデートファイルの配布を行うこと。

カ．アップデートの実行は三重県にて実施する。

キ．利用者からの問い合わせ対応は三重県またはヘルプデスクが行うが、必要に応じて支援を行うこと。

7.2.3.7. 稼働監視

ア．障害時にセキュリティ対策システム全体に影響が及ぶサーバ等の稼働監視を行うこと。

イ．障害発生時は三重県に報告し、「7.2.3.7 障害一次切り分け」「7.2.3.8 障害対応」「7.2.3.9 障害対応」等を実施すること。

7.2.3.8. 障害一次切り分け

ア．障害の発生原因の切り分けを行い、結果を三重県に報告すること。なお、受託事業者のみで原因の特定が困難な場合は三重県に報告したうえで、必要に応じて他事業者等と協力し切り分けを行こと。

7.2.3.9. 障害対応

ア．必要に応じて障害発生拠点へ駆けつけ、不良部位の切り分け及び修理・修正・交換を行うこと。

イ．障害によりソフトウェア、データが破損した場合、バックアップデータ等から速やかに復旧を行うこと。また、必要に応じて、セキュリティ対策システムの再セットアップを行うこと。

7.2.3.10. 障害後是正措置・予防措置

ア．障害が発生した場合、障害に関する情報を収集したうえで、その障害情報をもとに原因を分析し、同様の障害が発生しないように是正措置・予防措置を検討し、三重県に報告すること。また、三重県の指示により、決定した措置を講じること。また、直ちに障害原因が判明しない場合は、三重県の了承を得たうえで、継続して調査を行い、障害原因の特定に努めること。

イ．障害情報、是正措置、予防措置の内容は障害記録として体系的に記録し、常に活用できるように保存すること。

7.2.3.11. マニュアル等の改訂

ア．稼働後の運用により、運用マニュアル等のドキュメントの修正が発生した場合には、履歴管理を行った上で速やかに各種ドキュメントを修正すること。

イ．ドキュメントの修正にあたっては三重県へ説明を行った上で、承認を受けること。

7.2.3.12. 月次報告

ア．各機能の運用状況について、出力されるレポート等に基づき報告を行うこと。報告頻度は月に 1 回以上とする。

イ．前回の報告以降に発生した障害等についても報告を行うこと。

7.2.3.13. 操作研修

ア．三重県の運用管理担当者及びヘルプデスクを対象とした操作研修を実施すること。実施回数は年 2 回を上限とする。

イ．現場担当者向けの操作研修については三重県で対応するが、必要に応じて機器の準備やサーバ等の設定などの支援を行うこと。

7.2.4. 三重県が行う業務

以下の業務については、三重県が行うことを想定しているが、その手順を受託事業者にて操作

マニュアルとして作成すること。

7.2.4.1. 新規利用者にかかる情報の収集

ア．新規利用者にかかる生体情報等の収集やセキュリティ対策システムへの仮登録は操作マニュアルに基づき三重県が行う。このために必要な機能を提供すること。詳細は「2.１.4. 利用者認証（生体認証）機能」を参照すること。

7.2.4.2. 新規外部媒体にかかる情報の収集

ア．新規外部媒体にかかる情報等の収集やセキュリティ対策システムへの仮登録は操作マニュアルに基づき三重県が行う。このために必要な機能を提供すること。詳細は「2.1.6. 外部媒体使用制限機能」を参照すること。

7.2.5. ヘルプデスクが行う業務

以下の業務については、ヘルプデスクが行うことを想定しているが、その手順については受託事業者にて操作マニュアルを作成すること。

7.2.5.1. 新規パソコンへのエージェント、生体情報読み取り装置ドライバ等インストール作業

ア．新規パソコンへのパソコン操作ログ記録等のためのエージェント、生体情報の読み取り装置のドライバ等のインストール作業は操作マニュアルに基づきヘルプデスクが行うが、必要に応じて支援を行うこと。

7.2.5.2. 管理対象パソコン追加・削除時、利用者追加・削除時、外部媒体追加・削除時におけるサーバ設定作業（年度末以外の期間）

ア．年度末以外の期間においては、ヘルプデスクがこれらの作業を行うため、必要な操作マニュアルを整備すること。また、ヘルプデスクによる対応が困難な場合は、必要に応じて支援を行うこと。

7.3. 保守業務

7.3.1. 保守対象の範囲

以下のとおり、本委託業務で導入した機器についてセキュリティ対策システムの保守業務を行うこと。保守業務とは、障害一次切り分け作業の結果、保守対象セキュリティ対策システムが障害の原因と推定される場合、受託事業者が「7.3.5. 保守業務対応時間帯及び保守方法」に定める時間帯に、次の諸作業を行うことをいうものとする。

ア．電話による障害連絡の受付

連絡先は契約締結後、三重県と協議のうえ決定することとする。

イ．障害機器が特定されたときの機器交換

機器交換にかかる費用は、受託事業者が負担するものとする。パソコンに接続する機器（生体情報読み取り装置）の輸送にかかる費用についても同様とする。

生体情報読み取り装置については、読み取り精度が低く運用に支障が生じる場合にも機器交換等を行うこと。

ウ．消耗品等の補充

セキュリティ対策システムの安定稼働に必要となる補充品は、受託事業者が必要に応じて準

備し、補充するものとする。

7.3.2. 保守対象機器

ア．保守対象とする機器は本委託業務で受託事業者が導入するすべての機器とする。

7.3.3. 保守業務における三重県の協力

三重県は受託事業者が保守業務を行なう上で必要とする次の各号の事項に対し、受託事業者のために環境を提供するものとする。

ア．状況確認のための必要なコンピュータ機器等のオペレーション作業を行う。

イ．代替品の受取作業及び交換作業を行う。

ウ．障害機器の受託事業者への返送作業を行う。

7.3.4. 保守業務対応時間帯及び保守方法

ア．セキュリティ対策システムの運用に重大な影響を与える機器の保守については、24 時間 365 日（オンサイト）とする。

イ．保守業務対応時間内において、対応依頼から初期対応を開始するまでの時間として、概ね 30 分以内として設計を行ったうえで対応を行うこと。なお、大規模災害発生時においては可能な限り当該時間を目標にして設計を行ったうえで対応を行うこと。なお、初期対応とは、障害発生箇所・原因の確認作業への着手、三重県などの関係者への連絡等を指す。

ウ．駆けつける必要があると判断してから、駆けつけ完了までの時間を開庁日の 8 時 30 分から 17 時 15 分までは 2 時間以内、上記以外の時間帯は 4 時間以内として設計を行ったうえで対応を行うこと。大規模災害発生時においては可能な限り当該時間を目標として設計を行ったうえで対応を行うこと。

エ．復旧方法が明らかになり、かつ復旧作業が必要な場所へ到着してから、復旧するまでの時間として概ね 2 時間以内となるように設計を行ったうえで対応を行うこと。なお、2 時間以内の復旧が困難と判明した場合における対応等についても設計行ったうえで対応を行うこと。

オ．障害が発生した場合でも、ハードウェア等が冗長化されており、機能提供に影響がないと判断される場合や、特段の機能停止が発生しないと確認できた場合は、翌開庁日の 8 時 30 分からの対応も可とするため、必要に応じて設計を行ったうえで対応を行うこと。

カ．パソコンに接続する機器（生体情報読み取り装置）等の保守については、開庁日の 8 時 30 分から 17 時までの保守（先出しセンドバック）とする。

7.3.5. 保守部品・消耗品

ア．オンサイトでの保守対応が不可能な部位がある場合を想定し、予備品の保有等についても設計を行ったうえで対応を行うこと。

イ．常時保有すべき保守部品（付属品、ソフトウェアを含む。）がある場合は、必要数の確保について設計を行ったうえで対応を行うこと。なお、履行期間中において、製造中止等に伴い保守部品の入手が困難になった場合は、三重県の承認を得たうえで、代替品による対応も可とする。

ウ．保守業務を実施するうえで、必要になる消耗品がある場合は、履行期間中における必要数について、設計を行ったうえで対応を行うこと。なお、履行期間中における消耗品の納入についても、本委託業務の範囲内とする。

7.3.6. SSD / HDD の取り扱い

保守業務により交換したサーバ機器等の SSD / HDD は受託事業者へ返却せず三重県にて物理破壊した後処分することとする為、あらかじめ必要な調整等を実施しておくこと。

8. 機器の撤去・設定情報及びログ情報等の抽出

8.1. 基本的な考え方

ア．本委託業務で導入した機器等のうち、次々期セキュリティ対策システムで継続使用しない機器について、次期セキュリティ対策システム運用終了後（本業務期間内）に撤去を行うこと。

イ．機器等の撤去にあたっては、機器等に保存された情報が復元できないよう消去すること。

ウ．各機能の設定情報及びログ情報等について、汎用的な形式で提出すること。

8.2. 撤去する機器について

サーバ機器等において SSD / HDD を内蔵する場合、全ての SSD / HDD は三重県へ提供すること。三重県にて物理破壊した後処分することとする。

8.3. 抽出する情報について

8.3.1. 設定情報

各機能の設定情報（接続を許可するパソコンに関する情報、利用を許可する媒体に関する情報等、随時変更され設計書等に記載のない内容を含む）について、次々期セキュリティ対策システムに反映できるよう、汎用的な形式で抽出すること。

抽出する形式や内容等については、本委託業務運用期間中に協議のうえ決定する。

8.3.2. ログ情報

各機能のログ情報（不正パソコンの接続ログ、認証に関するログ、パソコン操作ログ、外部媒体の使用に関するログ等）について、汎用的な形式（XML、CSV などのテキストファイルを想定）で抽出すること。

抽出する形式や内容等については、本委託業務運用期間中に協議のうえ決定する。

8.3.3. その他

その他、必要に応じて、次々期セキュリティ対策システムへの移行にあたり必要となる情報の提供を行うこと。