【別紙６】　情報セキュリティ要件

本調達における情報セキュリティ対策は、情報に対する不正アクセスや情報漏洩、改ざんを防止するため、機密性・完全性・可用性の観点から実施すること。

なお、本調達においては、適用徴収システムの開発及び導入、システム環境の構築までが調達の範囲であるが、サービスレベル要件等を確実に達成できるシステム環境を構築する必要があるため、ハードウエア・ソフトウエア等の要件についても併せて記載する。

第１　基本方針

本システムは、労働保険料の債権管理をはじめとして労働保険の適用徴収事務の即時処理を行うと共に、e-Gov や官庁会計事務データ通信システム等の連携する他システムに対する影響度の高いシステムであり、高度な情報セキュリティレベルが要求される。以下の方針に従った情報セキュリティ対策を行うこと。

１　情報セキュリティ対策は以下の文書を含む情報セキュリティ関連の文書又は仕様に準じること。参照する資料は常に最新版を用いること。「厚生労働省情報セキュリティポリシー」等の非公開情報については、契約後に開示する。

(1)「政府機関の情報セキュリティ対策のための統一基準」（以下、政府機関統一基準という。）

(2)「厚生労働省情報セキュリティポリシー」

(3)「各府省の情報システム調達における暗号の利用方針」

２　ファイアウォールや不正侵入保護システムを利用する場合には ISO/IEC15408 セキュリティ評価基準の認定を受けているものを採用すること。その他の製品についても、リスク分析・評価の結果により必要と判断された場合には、ISO/IEC15408 セキュリティ評価基準の認定を受けている製品を優先して採用することを検討すること。

３　本システム稼働時点での本システム導入ハードウエア及びアプリケーションシステムに関する種類やバージョン情報、すべての設定項目について文書化すること。また、設定項目が正しく設定されていることについて、確認を行うこと。

４　情報システムの可用性維持のための対策については、サービスレベル要件を基に検討を実施し、十分な可用性を維持すること。

５　調達時点の技術で実現可能な対策を現実的な方法にて実施すること。

６　稼働時点での必要機能の組み込みに加えて、稼働期間全体に亘っての継続的な更新（最新かつ実証済みの情報セキュリティパッチ等を遅延なく取り込む等）のための仕組みを実現すること。

７　厚生労働省が別途実施する第三者機関による情報セキュリティ監査において改善の必要性が指摘された場合には、受注者の負担と責任において迅速に対応すること。

８　情報セキュリティ評価及び認証制度に基づく ST を作成するとともに、ST 確認を受けること。

９　受注者は厚生労働省と機密保持契約を締結すること。

第２　クライアント端末セキュリティ

クライアント端末に対する情報セキュリティ対策を行い、ウィルス等の技術的な脅威や情報の持ち出し等の物理的な脅威に対し､情報システムに対する機密性､完全性、可用性を確保する。

１　基本要件

(1) NTP サーバ（インターネット標準の時刻情報プロトコルを実装したサーバ）との時刻同期を図ること。

(2) OS の機能を最大限に活かしたセキュアな設定を行うこと（パッチ適用、不要なサービスの停止等)。また、設定内容の集中的な管理及び変更が容易に行える仕組みを設けること。具体的な設定事項として、OS ベンダーが提供している推奨設定をベースとした設定を検討すること。

(3) ウィルス対策ソフトウエアの導入を前提とした情報システムの構築を行うこと。

(4) ソフトウエア及びソフトウエアの修正モジュールの自動配布・適用状況の管理が迅速かつ容易に行える環境を整備すること。

(5) クライアント端末に対するソフトウエアのインストールは管理者の管理で行うこととし、職員によるソフトウエアのインストールを禁止する措置をとること。

(6) クライアント端末には指定された方法以外の起動ができない措置をとること。

(7) サーバと通信を行うクライアント端末は、通信の暗号化を実現すること。

(8) データの持ち出し制御に係る以下の機能を有する情報を構築すること。

ア　外部記憶媒体に格納する際、格納の可否を制御する機能

イ　外部記憶媒体に格納する際、情報を暗号化する機能

ウ　ネットワーク共有サーバに格納する際、格納を制御する機能

エ　プリンタに出力する際、プリンタ出力を制御する機能
（印刷者を一意に特定可能な文書 ID を印字する機能を含む）

オ　上述のクライアント端末に対するデータの持ち出し制御を行うため、管理サーバにてログを取得・管理する機能

(9)クライアント端末にはセキュリティケーブルを配備すること。

２　アクセス権限

権限管理を実施し、不正アクセス等の技術的な脅威に対し、アプリケーションシステムへのログイン制御を行い情報システムの機密性、完全性、可用性を確保すること。

(1) 契約後に示す権限定義表に基づく権限管理が実現可能であること。

(2) 権限の種類は、主に「登録」、「参照」、「更新」、「削除」の４種の組合せとする。

第３　サーバセキュリティ

サーバに対する情報セキュリティ対策を行い、不正アクセス等の技術的な脅威に対し、情報システムに対する機密性、完全性、可用性、安全性を確保すること。

1　NTP サーバ（インターネット標準の時刻情報プロトコルを実装したサーバ）との時刻同期を図ること。
2　ウィルス対策を行うこと。
3　情報セキュリティ監査ソフトエージェントを導入し、適宜監査できる環境を整備すること。
4　クライアント端末と通信を行うサーバは、通信の暗号化を実現すること。
5　ソフトウエア及びソフトウエアの修正モジュールの自動配布・適用状況の管理が迅速かつ容易に行える環境を整備すること。配布されるソフトウエア及びソフトウエアの修正モジュールは、電子署名により配布元を確認できること。
6　運用･保守時に担当職員に指定された任意のクライアント端末のみが､指定されたサーバへアクセスできること。
7　OS の機能を最大限に活かしたセキュアな設定を行うこと（パッチ適用、不要なサービスの停止、リモートログイン時の管理者権限への昇格停止等)。また、設定内容の集中的な管理及び変更が容易に行える仕組みを設けること。具体的な設定事項として、OS ベンダーが提供している推奨設定をベースとした設定を検討すること。
8　修正モジュール適用管理環境を整備すること。
9　サーバ上のファイルやフォルダ･アプリケーションシステム等の情報システムに対し、アクセス証跡を取得する機能を有すること。
10　サーバに、ファイルやアプリケーションシステムに対するアクセス制御を行うことができる機能を搭載すること。また、ファイルやアプリケーションシステムに対するアクセス制御を行う機能については、本システム稼働時点で制御内容を検討し、設定項目について文書化すること。また、設定項目が正しく設定されていることについてテストを行うこと。

第４　ネットワークセキュリティ

ネットワークに対する情報セキュリティ対策を行い、不正接続やネットワーク障害等の物理的な脅威や不正アクセス等の技術的な脅威に対し、情報システムに対する機密性、完全性、可用性を確保すること。

1　不正接続対策

不正接続による物理的な脅威に対し、情報システムの機密性、完全性、可用性を確保すること。不正接続対策の例を以下に示す。

(1) 許可されたクライアント端末以外の不正なクライアント端末（ハブやルータを含む）が LAN に接続されたことを検知し、排除する。
(2) 不正なクライアント端末は、IP アドレスや MAC アドレス等によって検知する。

2　アクセス制御

アクセス制御を実施することにより、サービス不能攻撃等の技術的な脅威に対し、情報システムの機密性、完全性、可用性を確保すること。

(1) ファイアウォール

ア　適用徴収システムに関連する業務サーバを設置するLANには、ファイアウォールを設置し、通信を制御すること。

イ　ファイアウォールの設定内容について文書化すること。

ウ　調査時等に必要な大容量のログを蓄積可能とすること。また、少なくとも過去1年分のログは即時に参照可能な状態とし、それより以前のログは電子媒体に保管可能とすること。

エ　調査時等に利用するために、ログを分析可能な仕組みを設けること。

(2) 不正侵入保護システム

ア　適用徴収システムに関連する業務サーバを設置するLANには、不正侵入保護システム（IPS：Intrusion Prevention/Protection System）を設置し、不正なアクセスから保護すること。

イ　不正侵入保護システムの設定内容について文書化すること。

ウ　調査時等に必要な大容量のログを蓄積可能とすること。また、少なくとも過去1年分のログは即時に参照可能な状態とし、それより以前のログは電子媒体に保管可能とすること。

エ　調査時等に利用するために、ログを分析可能な仕組みを設けること。

3　データ暗号化

ネットワーク上のデータ暗号化を実施することにより、盗聴等の技術的な脅威に対し、情報システムの機密性を確保すること。

(1) 業務サーバ～クライアント端末（アプリケーションシステム）間

業務サーバのアプリケーションシステムは、SSL/TLS等で通信できる仕様にすること。

(2) 業務サーバ間

サーバ室の業務サーバ間の通信は、暗号化を実施しない。

(3) クライアント端末間

クライアント端末間の通信は暗号化しない。

4　証跡取得

(1) 証跡管理を実施することにより、不正アクセス等の技術的な脅威に対し、情報システムの機密性を確保すること。

(2) 機密情報を保持するサーバが設置されたネットワークにおいて、そのサーバへのアクセス証跡を取得する機能を有すること。

(3) 調査時等に必要な大容量のアクセス証跡を蓄積可能とするとともに、調査時等に利用するために、アクセス証跡を分析可能な仕組みを設けること。また、少なくとも過去１年分のアクセス証跡は即時に参照可能な状態とし、それより以前のアクセス証跡は電子媒体に保管可能とすること。

第５　ウィルス対策要件

適用徴収システムのウィルス対策を実施するにあたり、以下の要件を満たすこと。

１　ウィルス対策全体方針

(1) システム稼働時において想定されるすべてのウィルス侵入経路に、ウィルスチェックを行う環境を整備すること。

(2) 全サーバ及びクライアント端末について、検収前に全ファイルに対するウィルスチェックを行い、書面にて報告を行うこと。

(3) ウィルス対策ソフトウエアを集中管理する管理サーバを設置し、設定情報、ウィルスチェックパターンファイル（以下、パターンファイル）の更新状況及びウィルス被害状況を確認できる環境を整備すること。

２　ウィルス対策ソフトウエア要件

(1) 機能要件

ア　管理サーバよりウィルス対策ポリシー、パターンファイル更新方法が一括して設定可能であり、その設定内容を個々の環境上で変更できないこと。

イ　ウィルスの検出・駆除は、基本的にクライアント端末上で行い、クライアント端末上で作成したファイルをサーバに格納する前にウィルスの検出･駆除を行うこと。

ウ　ウィルス対策ソフトウエアを搭載しないサーバであっても、そのウィルスが具体的にどこで検出・駆除されるかを明記すること。

エ　パターンファイルの更新については、ソフトウエアベンダー等において、パターンファイルが公開された時点で、迅速に省内に適用できる仕組みを用意すること。

オ　パターンファイルの更新については、利用者である職員や担当職員の作業負担にならない方法を実現すること。

(2) 運用要件

ア　ウィルス対策ソフトウエアは常駐させ、常駐ソフトウエアは一般利用者が解除できない仕組みとすること。

イ　ウィルス対策は、パターンファイルの更新を含め、自動化すること。

ウ　バージョンやウィルス定義ファイルが古いクライアント端末を検出し、ネットワークへの接続を制御する仕組みを組み入れること。

エ　担当職員が、ウィルス対策ソフトウエアを管理するサーバにアクセスし、操作するための専用クライアント端末を指定された場所に整備すること。

(3) クライアント端末・サーバでの個別要件

ア　すべてのクライアント端末上にウィルス対策ソフトウエアを導入すること。
イ　サーバにウィルス検知・駆除ソフトウエア又はそれに代わる機能を導入し、ウィルス混入に対するリスクを軽減すること。

第６　情報セキュリティ監査／監視

情報セキュリティ維持・運用管理を行い、盗難や障害等の物理的な脅威や管理の不備等の人的脅威、不正アクセス等の技術的な脅威に対し、情報システムに対する機密性、完全性、可用性を確保すること。

１　情報セキュリティ監視

情報セキュリティ監視を実施することにより、障害等の物理的な脅威に対し、情報システムの機密性・完全性・可用性を確保すること。

(1) 機能要件

ア　関連するファイアウォールと不正侵入保護システムは双方を連携して監視できること。
イ　不正侵入保護システムによる保護結果に基づき、必要に応じてファイアウォールのルールを変更し、不正侵入を防御できること。
ウ　サーバの生死監視、サーバのリソース消費状況の監視、サーバ上のアプケーションの稼働管理を行うための監視マネージャを導入すること。
エ　労働局、監督署及び安定所等にサーバを設置する場合は、監視エージェントを導入すること。
オ　監視マネージャには、各サーバ監視項目に対する閾値を設定し、正常／異常の判定を行えるようにすること。
カ　不正アクセスを判断するに至るまでの不正アクセス監視マニュアルを作成すること。
キ　ウィルス混入を検知した際の、ウィルス対応マニュアルを作成すること。
ク　各サーバ・アプリケーションシステムで取得した証跡を、一定期間保管し必要に応じ参照が可能な状態を保てること。

２　情報セキュリティ監査

情報セキュリティ監査を実施することにより、管理の不備や運用の不履行等の人的脅威、不正アクセス等の技術的な脅威に対し、情報システムの機密性・完全性・可用性を確保すること。

システム構築後に構築したシステムに対してシステム監査を実施し、結果及び結果に対する対応を報告すること。実施時期については、徴収業務室と調整し決定すること。なお、監査においては監査を実施する者と監査を受ける者が、その役割を兼務しないこと。

第７　暗号技術採用／利用

1　暗号技術採用／利用方針

(1) 暗号アルゴリズム及び製品選定

ア　暗号アルゴリズムの選定に際しては、「各府省の情報システム調達における暗号の利用方針（平成15年2月28日行政情報システム関係課長連絡会議了承）」に従うこと。

イ　製品の選定に際しては、FIPS140-2に準拠する製品、ISO/IEC15408セキュリティ評価基準においてEAL4以上の認定を受けているものの導入を検討すること。

ウ　採用する暗号アルゴリズム及び製品についての選定理由を明確にし、徴収業務室へ説明すること。

(2) 情報セキュリティ強度の均一化

ア　公開鍵暗号利用時の鍵長の基準値は1,024bit以上とすること。

イ　共通鍵暗号利用時の鍵長の基準値は256bit以上とすること。

(3) カスタマイズの回避

可能な限り市販の暗号技術製品を採用し、カスタマイズによる独自プログラムの作成は行わないこと。ただし、カスタマイズしなければ実現できない要件がある場合には、採用製品とカスタマイズ理由を説明すること。

2　暗号技術整備

(1) クライアント端末でのファイル／ディスク暗号化

ア　基本的にはクライアント端末上に重要な情報資産を格納しないことが前提であるが、クライアント端末上に機密情報が格納される可能性があること、そのクライアント端末が第三者に盗難されることを想定し、ハードディスクやファイルの暗号化の施策により、その情報が第三者によって参照ができないように考慮すること。

イ　ハードディスクやファイルの暗号化については、アプリケーションシステムのレスポンスに極力影響を与えないよう考慮すること。

ウ　暗号化した情報は正当な操作や処理において自動的に復号されること。

(2) サーバでのファイル暗号化

サーバ上の機密情報は暗号化しない。

第8　開発・テスト・検証環境に関する情報セキュリティ

開発・テスト・検証環境に関する情報セキュリティ確保を行い、盗難等の物理的な脅威や管理の不備等の人的脅威に対し、開発中のシステムに関する機密性を確保すること。

1　開発環境

開発環境に関する情報セキュリティ確保を行い、開発中のシステムに関する機密性を確保すること。

(1) 開発環境

ア　開発は許可された場所のみで行うこと。

イ　開発環境への入退室管理等の物理的アクセス制御を行うこと。

ウ　開発者が開発から離れる時にはアクセス権を完全に消去すること。

エ　開発環境に部外者が入室する際には、記録をとり、関係者による付添いを行うこと。

オ　開発に係る構成管理は自動化すると共に、許可されない変更が行われないように対策を実施すること。

カ　開発環境に係る情報セキュリティ対策の継続的適用を確実にするための組織・体制と役割を明確にするとともに、情報セキュリティ侵害対応マニュアルを作成し、徴収業務室の承認を得ること。

(2) 開発情報

ア　システム開発時に用いる情報は、許可を受けた場所のみで利用し、持ち出さないこと。

イ　システム開発時に用いたテストデータは､本番開始時までに完全に消去すること。

ウ　システム開発時に用いた ID 等は、完全に消去すること。

エ　厚生労働省を含む関係省庁より入手した資料については、プロジェクト内で保管し、外部に情報流出させないこと。

オ　入手した資料は識別可能な仕組みを設けて管理することとし、プロジェクト終了時に徴収業務室へ返却又は破棄するなどの処置をとること。

カ　厚生労働省等から提供した情報及び開発成果物を含むシステム開発に係る情報の運搬時には､データの暗号化や施錠可能な鞄を用いる等､情報漏洩対策を行うこと。

(3) 脆弱性診断

ア　開発環境にて脆弱性診断を実施し、本番環境が脆弱にならないようにすること。

イ　また、脆弱性診断の方法、結果及び対策を徴収業務室に明示すること。

(4) その他

納品に際して、開発物が一切の改変なく、厚生労働省が受け取れる保証を提供するシステム管理、配送の設備と手続をとること。