セキュリティに関する検討

セキュリティの検討概要

■検討のポイント

ＯＳＳに係る行政手続は、自動車の所有権の公証と行政上の実態把握（登録）、安全の確保（検査）、自動車保管場所の確保、納税といった、極めて重要であり、不正があった場合の影響が大きなものである。そのため情報の漏洩や不正アクセスの防止等、さまざまな脅威から、いかにＯＳＳのセキュリティを確保するかについて以下の検討を行った。

①セキュリティレベルの設定
②セキュリティ確保のための運用方法

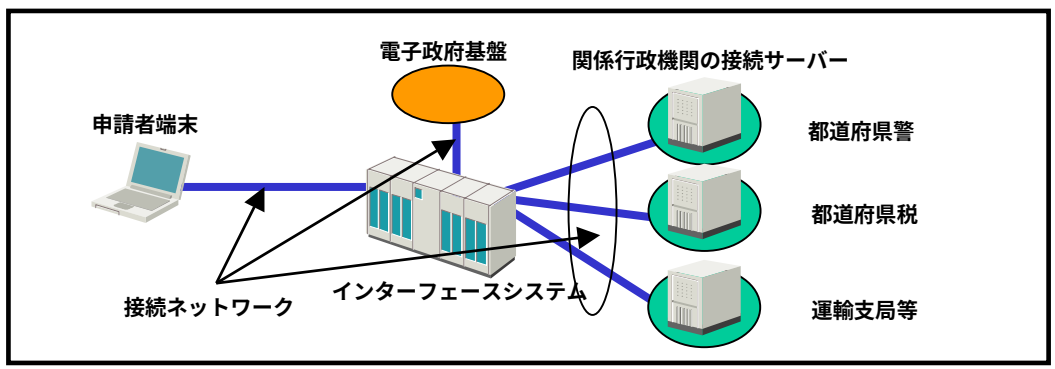
■検討の方向性

①セキュリティレベルの設定

設定対象として検討したのは、申請者端末、インターフェースシステム、接続ネットワーク、関係行政機関の接続サーバーとした。他に接続が予定されている機関（自動車メーカー等）については、接続方法等が明確になった上で検討する。検討は、ＩＳＯ／ＩＥＣ１５４０８やＩＳＯ／ＩＥＣ１７７９９等の国際標準規格を参考にして以下の２つの側面から行った。セキュリティレベルは電子政府にふさわしい高い水準のものとした。

・技術の側面：システムに採用するセキュリティ機能等、技術面から見たセキュリティレベル

・管理の側面：申請者、運用者、関連行政機関職員等の人及びシステムの管理面から見たセキュリティレベル



次ページ以降に、設定したセキュリティレベルの概要について示す。

ＩＳＯ／ＩＥＣ１５４０８：情報システムや製品に対して信頼できるセキュリティ機能を装備するための国際標準。１９９９年に制定。

ＩＳＯ／ＩＥＣ１７７９９：情報セキュリティマネジメント実践のための国際標準化されたガイドライン。情報セキュリティ対策を実現するための１０管理分野、１２７項目の詳細管理対策で構成される。２０００年１１月に制定。

(a) 申請者端末

区分	セキュリティレベル
技術の側面	・住民基本台帳ICカード等による公的認証に加えて、利用者が事前に登録したID／パスワードによりアクセスを制限 ・申請者端末に保管されるデータは暗号化し、第三者から読み出せないよう制御
管理の側面	・申請者端末の利用のためにID／パスワード等による管理を検討 ・申請データ等、入力データの控えは申請者が管理 ・一の端末を複数の者が利用するような場合（共同利用型端末）については、共同利用型端末管理者による管理とともに、システム的に管理することも含め、特に厳重な管理の仕組みも検討

（b）インターフェースシステム

区分	セキュリティレベル
技術の側面	・運用者用ユーザーID／パスワード等による厳重なシステムへのログイン確認によりアクセスを制限 ・運用者等に対してその業務・運用内容に対応したアクセス権限を設定 ・通信相手（関係行政機関や民間機関、共同利用型端末等）の正当性の検証のためのサイト間認証の実施 ・最新のセキュリティパッチの適用、セキュリティホールとなる不要プログラムやサービスのシステム上からの排除及び監視 ・ウィルス等の不正情報の早期検出、除去
管理の側面	・設置施設の施錠及び入退出の監視・管理 ・守秘義務 ・ＯＳＳ関係情報の取扱いに関わる場所・手順の限定と第三者の立会いによる確認とその記録の管理 ・障害時、セキュリティ侵害時に備えた定期的バックアップの実施 ・不正行為等の早期発見のため各種ログの取得と監査の実施

(c) 関係行政機関の接続サーバー

区分	セキュリティレベル
技術の側面	・運用者用ユーザーID／パスワード等による厳重なシステムへのログイン確認によりアクセスを制限 ・運用者等に対してその業務・運用内容に対応したアクセス権限を設定 ・通信相手（関係行政機関や民間機関、共同利用型端末等）の正当性の検証のためのサイト間認証の実施 ・最新のセキュリティパッチの適用、セキュリティホールとなる不要プログラムやサービスのシステム上からの排除及び監視 ・ウィルス等の不正情報の早期検出、除去 ・原本性保証装置の設置
管理の側面	・設置施設の施錠及び入退出の管理・監視 ・守秘義務 ・ＯＳＳ関係情報の取扱いに関わる場所・手順の限定と第三者の立会いによる確認とその記録の管理 ・行政職員・運用者へのセキュリティに関する訓練・教育の実施（定期的） ・障害時、セキュリティ侵害時に備えた定期的バックアップの実施 ・不正行為等の早期発見のため各種ログの取得と監査の実施

(d) 接続ネットワーク

区分	セキュリティレベル
技術の側面	・接続ネットワークの両端に不正侵入を抑止する装置（ファイアウォール）、検知する装置（ＩＤＳ）を設置 ・接続ネットワークの両端のルータ、ファイアウォール、ＩＤＳ等による送信元／先アドレス、プロトコル、サービス、接続時間、通信量の監視・制御 ・各サイト内部に接続ネットワークと隔離された領域を設置し、不正アクセスを排除およびセキュリティ被害拡散を防止 ・ネットワーク上の全送受信データは暗号化し、第三者から読み出せないよう制御
管理の側面	・不正行為等の早期発見のため各種ログの取得と監査

②セキュリティ確保のための運用方法

・技術、管理の側面におけるセキュリティ確保に当たっては、ISO/IEC15408、ISO/IEC17799等の国際標準規格を基準としたＯＳＳ用のセキュリティ運用規則を制定し、それに準拠する。

・関係行政機関をメンバーとした情報セキュリティ委員会（仮称）を設置する。

情報セキュリティ委員会（仮称）は以下の役割を担う。

(a) 情報セキュリティポリシーの策定、導入、周知徹底

(b) 情報セキュリティポリシー中のセキュリティレベル、体制・組織及び運用の定期的な評価・見直し

(c) 関係する職員・運用者に対するセキュリティに関する定期的な訓練・教育の企画／実施

(d) ＯＳＳ利用者、運用者の登録・管理

・情報セキュリティ委員会（仮称）メンバー外のＯＳＳ利用者（接続するシステムを含む）については、ＯＳＳにおけるセキュリティ確保のための接続要件や利用規程に準拠させる。

・システム設計等において、セキュリティに関して高度な知見を有する客観的な複数の第三者からＯＳＳにおけるセキュリティ確保への取組の評価を受ける。