セキュリティ要件

# 認証

## クライアントアプリケーションの認証方式

ActiveDirectoryによりユーザー認証する。

## ログイン方式

クライアントアプリケーションに、自動ログインの設定機能を付加する。自動ログインの設定はデフォルトではOFFにする。また、設定はPC毎でかつPCのログインユーザー毎に保持する。

自動ログインの設定がOFFの場合、ユーザーIDとパスワードの入力によりユーザーはログインする。

自動ログインの設定がONの場合、アプリケーション起動時に自動的にWindowsにログインしているユーザーのユーザーIDを取得し、ActiveDirectoryに問合せを行う。ユーザーの有無および有効/無効にて、アプリケーションの実行可否を判断する。ユーザーIDやパスワードの入力はユーザーに対して求めない。

## 認証を必要とする箇所

クライアントアプリケーション起動時。

## 認証を必要としない箇所

APIへの各リクエストについては、認証を必要としないこととする。

## 再認証を必要とする箇所

なし。

# セッション管理

## セッションの破棄について

* 認証済みのセッションが一定時間以上アイドル状態にあるときでもセッションタイムアウトとしない

## CSRF（クロスサイトリクエストフォージェリー）対策の実施について

* CSRF対策を実施すべき箇所では再認証の実施すること
* CSRF対策を実施すべき箇所で再認証の実施を提供することが困難な場合にはアクセスを POSTに限定し秘密情報の埋め込みと確認を実施すること

# パラメータ

* URL パラメーターにユーザーID やパスワードなどの秘密情報を格納しないこと
* パラメーターにパス名を含めないこと
* アプリケーション要件に基づいて入力値の文字種や文字列長の検証を行うこと

# 文字列処理

## クロスサイトスクリプティング（XSS）対策

* ユーザーの入力など、外部から入力した URL を出力するときは「http://」や「https://」で始まるもののみを許可すること
* 要素の内容やイベントハンドラ（onmouseover=””など）を動的に生成しないようにすること

## 実装ルール

* HTTP レスポンスヘッダーの Content-Type に文字コードを指定すること

# 暗号化

* https://で指定すべき画面を特定すること
* サーバー証明書はアクセス時に警告が出ないものを使用すること