タブレット導入に関するセキュリティの対応について

【生活保護システム】
・生保システム側で、「誰が、いつ、誰の情報を度の端末で持ち出し、いつ返却したか」を持出したか一元で確認することができます。
・個人情報を持ち出す際にも氏名や住所に対して「0%」から「100%」の間で任意にマスク（●●●）をかける機能を備えております。

【タブレット端末】
・標準の「パスコードロック」を設定することでハードウェアの暗号化をすることができます。
・「パスコードロック」を一定回数失敗すると、初期化しなければいけなくなります。
　万が一、タブレットを紛失場合も内部のデータを参照される可能性は低くなります。
・iPad の電源オフ、規定時間経過、ホームボタンを押すごとにログイン画面に戻りますので、開いている途中のデータを他者に見られる心配はなし。

※機能の制限について※
・iPad の一般設定で、「アプリケーションのインストールを許可しない」「Safari（Web 閲覧）を許可しない」などの機能制限を行うことができます。
　→機能制限を行うと、トップ画面のアイコンが消え起動できないようになります。

【訪問支援アプリ】
・アプリ起動時の認証を規定回数間違えると持出し中の内部データを消去する機能を備えております。
・データ持出し後、規定日数以内に訪問後のデータを生保システム側に取り込まなければ内部のデータを消去する機能を備えております。

【無線 LAN AP（アクセスポイント）】
・無線 LAN のステルスモードを利用することで、
・デバイスの MAC アドレスでフィルタリングして無許可の端末の接続を防止します。
・無線 LAN の手順が複雑な「WPA2（無線 LAN の暗号化方式の規格）」を採用し、悪意のある人が認証情報を取得できないようにすることができます。
・暗号化方式に「AES」を採用し、暗号データの解読を防止します。

【認証機器（NetAttest EPS）】
・端末に証明書をインストールすることで、証明書がインストールされた端末のみの接続を許可し、それ以外の端末の接続を防止します。

【ファイアウォール】
・ファイアウォールでサーバーへの通信のみに制御をかけます。