資料４

（財）地方自治情報センターへの照会事項について

○照会内容

＜住基ネットのセキュリティについて＞（平成１５年７月１０日照会、１５日一部追加）

１．ＣＳ内のデータについて
：ＣＳ内で、住基６情報自体は暗号化された状態で保持されているのか。暗号化されている場合は，鍵管理はどこで行っているか．また，操作用ＩＣカードと鍵の関連はどうなのか。

２．操作者用ＩＣカードによるＣＳ端末へのログインの仕組みについて
：端末ＯＳへのログインなのか、端末で動作している住基操作用アプリケーションへのログインなのか、ＣＳ本体のアプリケーションにより認証を受けるためのログインなのか。端末・ＣＳアプリケーションの認証として利用している場合，ＩＣカードデータを鍵としてアプリケーションでデータの暗号の復号化等を行っているのか，単にアプリケーションを起動させるか否かの判断にＩＣカードデータを利用しているのか。

３．ＣＳ端末が専用機であることについて
：他のアプリをインストールすることの、規定上、技術上の可否。
：Windows の添付アプリとしてインターネットエクスプローラー等があるが、Ｅメールなど、それを利用したインターネット閲覧等の可否。

４．ＣＳが専用機であることについて
：ＣＳに住基以外の業務アプリ等をインストールすることの規定上、技術上の可否。
：万が一、市町村がＣＳを住基以外の業務に使うサーバにも利用した場合、全国センターでは認知できるか。

５．ＦＷの監視について
：住基ネットで利用しているＦＷについて，それぞれ全国センターから常時何を監視しているのか．監視項目と監視体制と監視範囲について。

６．ＩＤＳによる監視について
：ＩＤＳの設置場所は、全国センターのファイアウォールの全国ネットワーク側か。
：ＩＤＳで監視できる通信は全国サーバに届くものだけか、都道府県ネットワーク内を流れる市町村－県間通信も含むのか、また、２次稼働で発生する市町村間通信は。
：ＩＤＳのアラートの分析は行っているのか
：ファイアーウォールのログとの相関分析はおこなっているか
：なにをもって不正進入と判断しているか

７．「住民基本台帳ネットワークシステム」の範囲は
：市町村のＣＳを含むか。
：庁内ＬＡＮを利用して接続するＣＳ端末を含むか。

８．媒体交換方式を採用する市町村の２次稼働の際の手順等について
：他市町村からのデータ送信要求への対応は、随時媒体交換により既存住基とＣＳのデータを連携させる必要があるか。
：他市町村からのデータ送信要求は、ＣＳ端末上で認知されると考えるが、媒体交換方式の場合のＣＳ端末はそもそも、庁内ネットワークを利用して接続する形態はあり得ないと考えて良いか。

＜住基カードについて＞（平成１５年７月１７日照会）

１．住基カードは、予め内部の読み出し不可能な領域に秘密鍵を格納した状態で供給され、外部からデータを与えると内部の演算回路によりこの秘密鍵を使ってデータを暗号化して出力する機能があります。この場合の暗号方式は、公開鍵暗号方式なのでしょうか。共通鍵暗号方式なのでしょうか。

２．公開鍵暗号方式である場合、ＲＳＡ暗号なのでしょうか。楕円鍵暗号なのでしょうか。また、鍵のビット長はどれだけでしょうか。秘密鍵、公開鍵のペアはだれが作成するのでしょうか。さらに、この公開鍵はだれが知っているのでしょうか。利用者はこの鍵ペアを知ることが出来るのでしょうか。また、自分で独自に鍵を生成してカード内の鍵を交換出来るのでしょうか。

３．共通鍵暗号方式である場合、暗号方式は何でしょうか。この場合、鍵のビット長はどれだけでしょうか。鍵はだれが作成するのでしょうか。鍵を利用者が知ることは出来ないのでしょうか。また、自分で独自に鍵を生成してカード内の鍵を交換出来るのでしょうか。

４．カード内の演算回路を使って暗号化する際のデータの受け渡し方等のインターフェース規格は公開されているのでしょうか。

○回答内容

＜住基ネットのセキュリティについて＞

週明けに文書で回答する旨の連絡あり。（平成１５年７月２５日）

＜住基カードについて＞

別紙のとおり（非公開のため掲載しておりません。）