住基ネットを通じた
他の自治体への不正侵入
（住民票の写しの広域交付不正請求）
についての検討

「長野県侵入実験速報から指摘できる住基ネットの脆弱性」補遺

Ver.1.1

2004. 1. 28

西邑　亨

＜もくじ＞

はじめに
1. 他の自治体への不正侵入ルートの例（広域交付の不正請求）
2. 不正な広域交付請求が可能になる条件
3. ICカードによる操作者認証の無力化について
4. 正規操作者に気づかれずに
受信した住民票写しの情報を取得する方法について
5. 自治体における有効な対策について
付記：並行して存在する「脅威」の問題
まとめ

はじめに

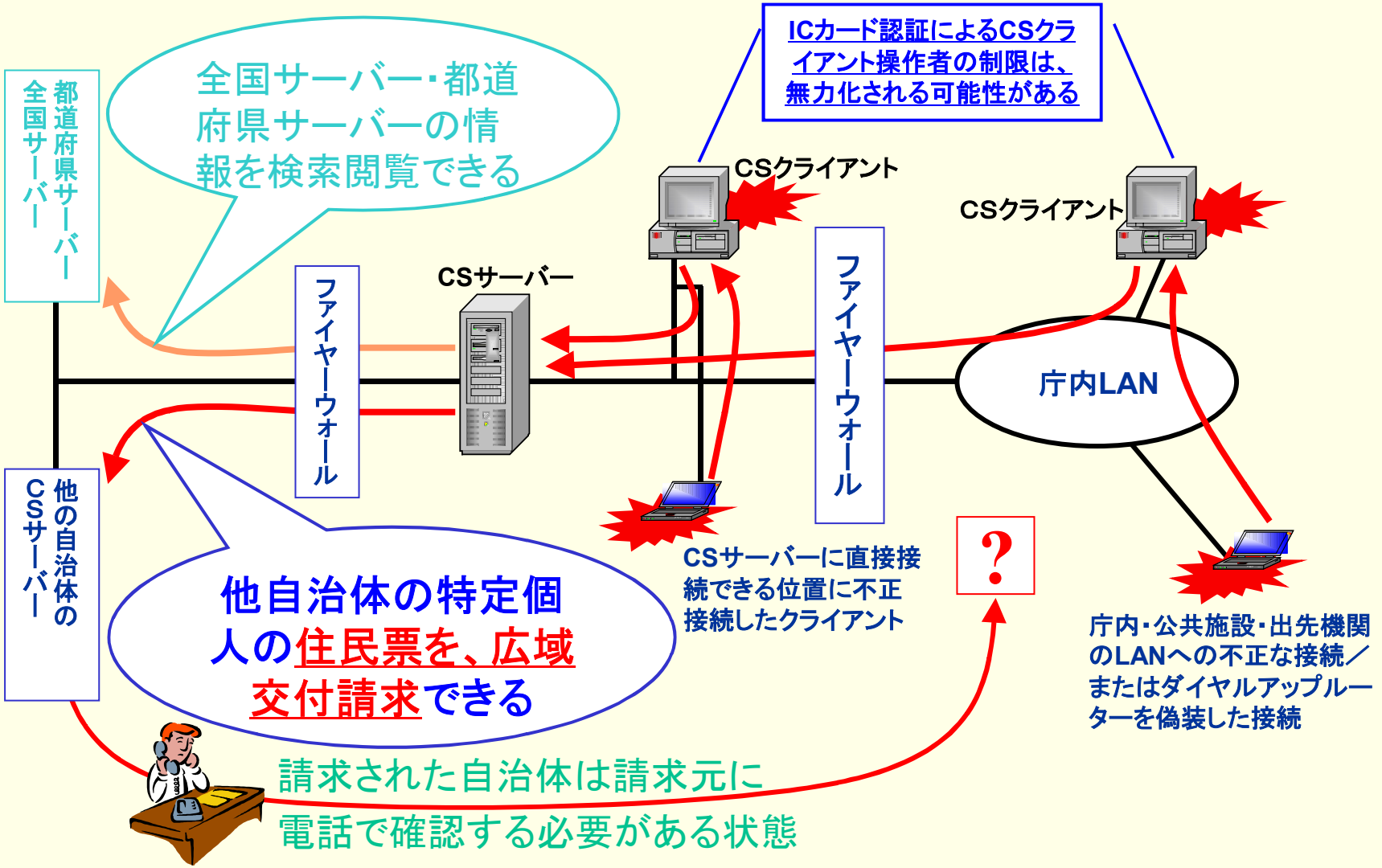
別途公開したレポート「長野県侵入実験速報から指摘できる住基ネットの脆弱性」では、他の自治体への不正侵入の可能性については「長野県の実験範囲を大幅に超える」ため、検討対象とはしていません。しかし、実験速報で指摘された住基ネットの脆弱性は、少なくとも「他の自治体の任意の個人の住民票の写し」を広域交付によって不正に取得できる可能性を強く示唆しています。

本レポートは、この問題について、上記レポートを補足するものです。
この問題は、住基法に規定されていないサービスに関わる脅威であり、他の住基ネットの問題点とは取り扱いが異なることについて、まず注意を喚起しておきたいと思います。

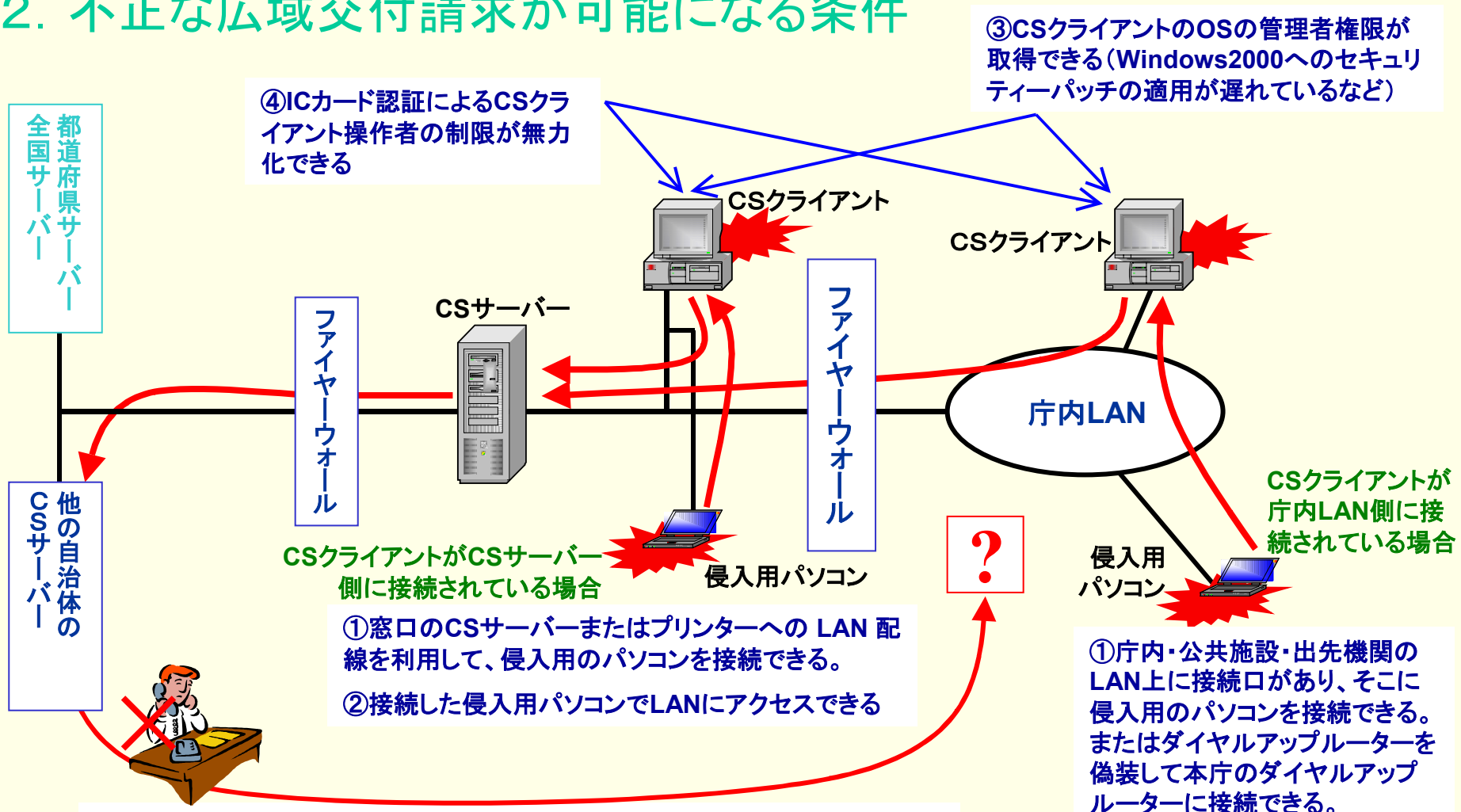
なお、以下で検討する「広域交付の不正請求」は、長野県速報から容易に指摘可能な他自治体への不正侵入手順の一例であり、他にもこうした手順が存在する可能性は、否定されていません。

＜関連資料の所在＞
http://www.jca.apc.org/~nisimura/juki/Nagano/03Test/
「長野県侵入実験速報から指摘できる住基ネットの脆弱性」（西邑）
「長野県侵入実験速報の概要と整理」（西邑）
http://www.pref.nagano.jp/keiei/seisakut/happyou/kaiken/s-kaiken.htm
長野県知事会見（速報の発表）配付資料
http://www.pref.nagano.jp/hisyo/press/20031216n.htm
「市町村ネットワークの安全性調査について 」（長野県知事会見速記録）

1．他の自治体への不正侵入ルートの例（広域交付の不正請求）



2. 不正な広域交付請求が可能になる条件

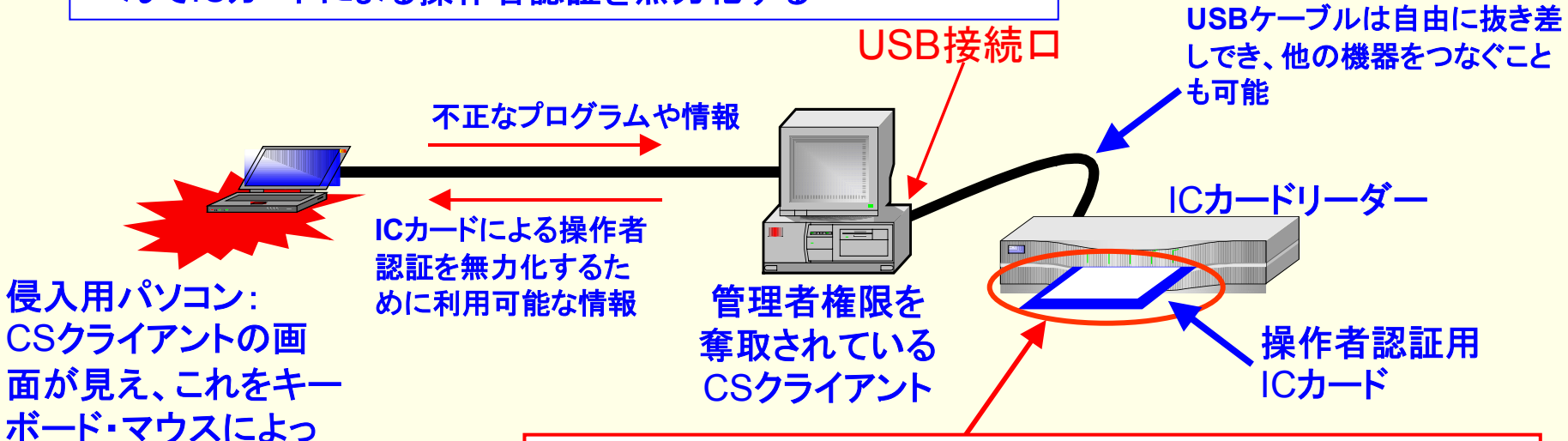


①から⑤までの条件が満たされれば、とりあえず広域交付の不正請求が可能になると考えられます

3. ICカードによる操作者認証の無力化について

容易に想定できる手法の例

✧USB接続口に干渉する方法（時間と技術能力が必要）
①別の機器を接続したり、不正なプログラムを実行して、USB接続口を通過する情報を調べ、分析する
②分かった方法をもとに、不正なプログラムやデータを送り込んでICカードによる操作者認証を無力化する



✧もっと簡単な方法（誰にでもできるが発見される可能性は高い）
ICカードを挿入したまま正規操作者が席を離れた場合、侵入者は自由に住基ネットの機能を利用できる（パスワードは侵入用パソコンから知ることが可能）

3. ICカードによる操作者認証の無力化について

- CSクライアントの管理者権限が侵入用パソコンの側で取得されている状態について、速報は、CSクライアントの画面をそのまま侵入用パソコンに表示し、そのキーボードとマウスを使ってCSクライアントの操作ができる状態だと報告しています。

  従って、住基ネットの業務アプリケーションが起動している状態で管理者権限が取得され、ICカードが挿入されていれば、侵入用パソコンの側で自由に住基ネットの操作ができることになります。侵入用パソコンの側からパスワードの入力が必要であっても、CSクライアントのキーボードを監視してパスワード（画面表示されない）を取得することは、インターネット上で無料配布されている一般向けツール（プログラム）を流用することで可能になります。

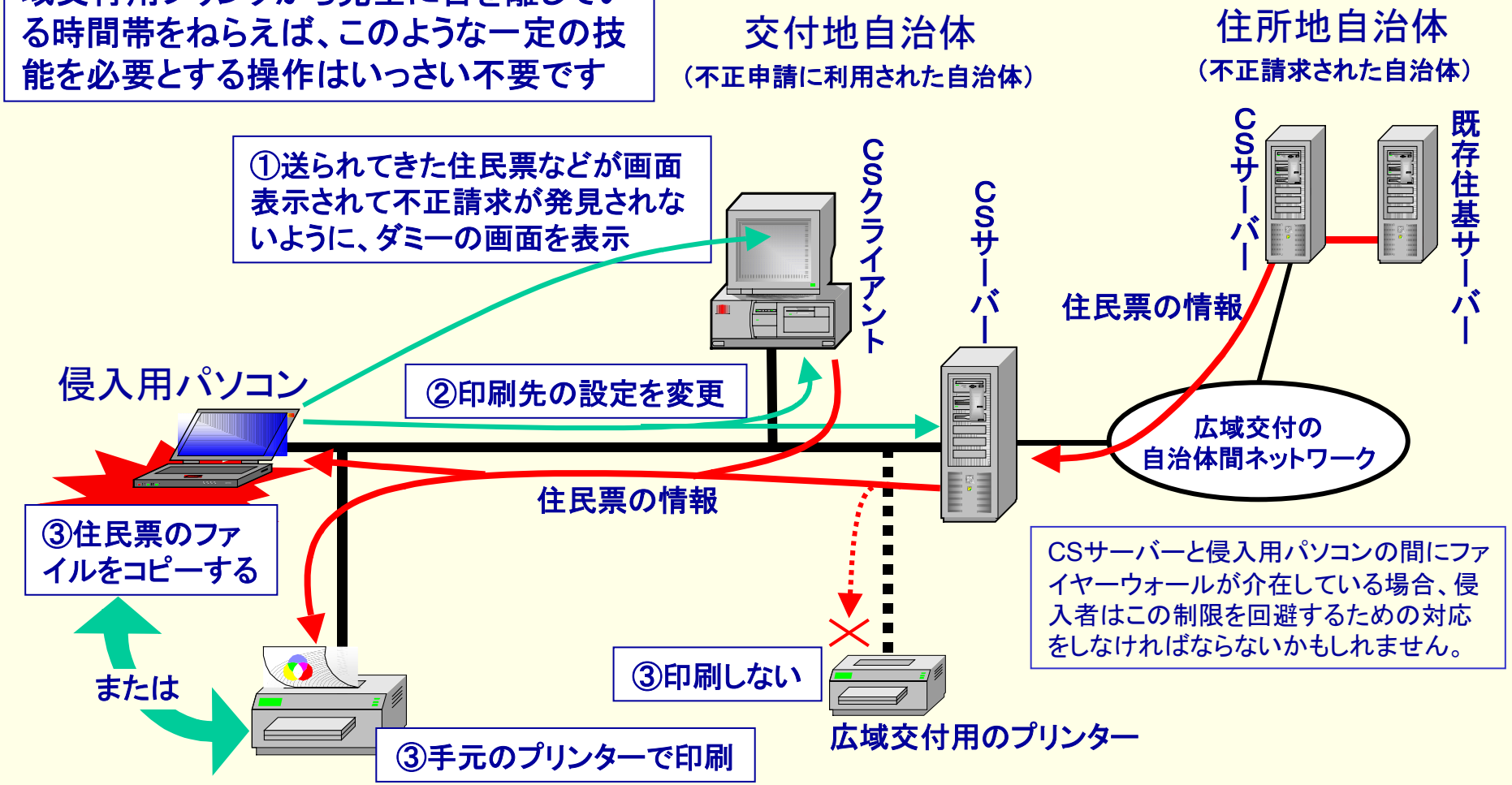
- また、CSクライアントの管理者権限が取得できており、あるいはICカードのリーダーライターが接続されているUSB接続口およびケーブルが容易に操作可能な状態になっていることから、USB接続口にソフト的にまたはハード的に干渉することで、ICカードによる操作者の認証を無力化する情報を入手することは十分可能といえます。

- 以上から、CSクライアントの管理者権限が取得できる状況では、ICカードによる操作者の認証によってCSクライアントの不正な操作を防止する対策は十分ではなく、これを無力化することは可能と考えられます。

4. 正規操作者に気づかれずに受信した住民票写しの情報を取得する方法

容易に想定できる手法の例

ただし、職員がCSクライアントの画面と広域交付用プリンタから完全に目を離している時間帯をねらえば、このような一定の技能を必要とする操作はいっさい不要です



4. 正規操作者に気づかれずに受信した住民票写しの情報を取得する方法について

「住基ネット基本設計書（第2.0版 2000.10） 本編 第3編 2章」p.2-83～2-84によれば、広域交付を請求した市町村（交付地市町村）には、CSクライアント上の手動による画面操作として、広域交付対象者選択（同一世帯者による請求の場合は世帯全員の情報が送られてくるため、この操作が必要になる）と住民票の写しの交付印刷（以上はCSクライアント上の画面操作）、および認証（内容確認や押印の作業）が行われるとされています。従って、CSクライアントの画面上にこれらの作業にともなう情報が表示されたりプリンタに出力されるため、正規操作者が不正請求の事実に気づき住民票の漏洩が阻止される可能性は高いと言えます。

これに対して、不正侵入者には

- ✧ 正規操作者が席を離れていることを確認して、広域交付請求を行う（発見される可能性は高い）
- ✧ 送られてきた住民票の写し情報は、侵入用パソコンのそばのプリンタに出力する、またはファイルの形で取得する

または、より発見されにくい手法として、

- ✧ これらの情報が表示されないよう、CSクライアントの画面表示に干渉する
- ✧ 送られてきた住民票の写し情報は、侵入用パソコンのそばのプリンタに出力する、またはファイルの形で取得する

など、いくつかの手法を採用することが可能です。画面表示への干渉および情報をファイル形式で取得するなどのためには、CSクライアント上での不正プログラムの実行や印刷先などの変更（場合によってはCSサーバーでも）が必要になることも予想されます。これらは、CSクライアントの管理者権限を取得している（ということはCSサーバーの管理者権限が取得できる可能性も極めて高い）ので、実行可能と言えます。

5. 自治体における有効な対策について

「住基ネット基本設計書 本編 第3編 2章」p.2-83～2-84によれば、広域交付を請求された市町村（住所地市町村）には、CSクライアント上の手動による画面操作として、住所地職員確認と住民票写しの情報送信指示という、請求を目視で審査する機能が提供されています。

審査において却下となった場合は住民票の写しは送信されず、交付地市町村への連絡が行われます。問題がなければ住民票写しの情報が送信されます。ただし基本設計書には、この審査の処理を省略することも可能であることが注記されており、無審査で住民票写しの情報を送信する市町村もあると考えられます。

以上の住基ネット市町村業務アプリケーションの機能を見ると、前述してきた手法による不正な広域交付請求を、この審査の過程で発見することはできないことがわかります。
従って、「住基ネットの停止」以外で一定の実効性が期待できる不正請求被害の防御手法は、

- ✧広域交付において審査の処理を省略しない。かつ、
- ✧請求元市町村担当部署の正確な電話番号を調べて電話をかけ、正規に広域交付請求が行われたことを担当部署の責任者に直接確認する

加害側となることも同時に防御できる対策は、

- ✧住基ネットの安全が確認されるまで広域交付の機能を停止する

だと考えられます（システム上、この機能だけを停止できるかどうかは不明）。

]

付記：並行して存在する「脅威」の問題

本レポートで検討してきた広域交付の不正請求を可能とする条件は、すでに「長野県侵入実験速報から指摘できる住基ネットの脆弱性」でも述べてきたように、

- ✧ 全国サーバー・都道府県サーバーの不正な検索・閲覧

を可能とする条件を同時に含んでいるものです。

しかしながら、現在の住基ネットの運用状況では、全国サーバー・都道府県サーバーにおける不正な本人確認情報の検索を有効に防御する手法は、市町村に与えられていません。

この脅威を有効に防御するには、

- ✧ 住基ネットを停止する（市町村が停止を求めて切断する）

ことによる暫定的な安全を確保した上で、抜本的な制度的、技術的対策の検討・実施が必要であることを指摘しておきます。

まとめ

広域交付の不正請求は、どちらかといえば全国サーバー・都道府県サーバー上の本人確認情報に対する不正な検索・閲覧よりも手順は複雑になり、要求される条件も増えます。しかし、漏洩される個人情報の内容はより深刻なため、侵入者の側から見れば不正取得の魅力は格段に大きいことに注目する必要があると考えられます。

住基ネット上の広域交付は、自治体間の直接接続によるもので、この機能の実行には全国センター・都道府県センターは関与していません。不正な広域交付の脅威は、

- ✧ 自治体が加害側にも被害側にもなりうる問題
- ✧ 自治体独自の責任において対策を立案・実施する問題
  （地方自治情報センターの担当範囲を超えている問題）

です。別の視点から見れば、住基法に規定されていないサービスのため、自治体独自で脅威の大きさを評価し対策を決定・実施すべき（自治体以外は対策を実施しない）問題であることにも、注目する必要があるでしょう（自治体は広域交付を拒否できます）。

すべての自治体は、「侵入の入口」となりうると同時に、情報を盗まれる「ターゲット」にもなるため、自自治体のセキュリティを強化しただけでは、自治体の責任を果たしたことにはなりません。この脅威は、大規模なネットワークの相互接続におけるセキュリティ確保の困難を典型的に示しているものといえます。