2003.12.16 長野県知事会見にもとづく

長野県侵入実験速報の概要と整理

第2.2版

2005.4.14 Ver.2.2

西邑　亨

もくじ

本レポートにおける資料の範囲と整理の方針

＜資料の範囲＞

- 本レポートは、長野県が県のホームページで公開している、03年12月16日長野県知事会見の速記録および配付資料に、もとづいて整理した「速報概要」です。
  一部は、12月20日さいたま市での日弁連シンポジウムでの吉田さんの報告およびその後の交流会でのヒアリング、12月24日の長野県本人確認情報保護審議会での発言（県のホームページで公開されている録音）も参照し、必要な場合はこれらから補足しています。
- 関連するマスコミ報道等は参照していません

＜整理の方針＞

- 主として会見における吉田柳太郎さんの発言をもとに、実験課題ごとにその内容と結果を整理した（図解はレポーターが作成し、ネットワーク機器の細部は省略した）。
- 吉田さんの報告は、一定の技術的正確さを意識した内容であるため一般向けではない内容を含んでいる。これらの点についてはわかりやすさを優先した要約、言い換えなどを行なっている
- 上記資料から直接指摘できる内容以外のレポーターによる評価はできるだけ加えないようにしたが、結果を理解する上で最小限必要と考えられる事項については、一部レポーターの評価を追加した部分がある
- 不明な事項については、気づいた範囲でこれを指摘した

◆本レポートの文責は西邑にあります。速報の誤読等があれば、西邑までご指摘いただけますようお願いします

1. 実験の目的と実験環境

- 侵入実験の目的:

  市町村ネットワークのさらなる安全性の確保のため、市町村の庁内ネットワークを通じた住基ネットシステムへの不正アクセス及び住基ネットシステムからの情報漏洩の可能性の有無について確認するための調査（県配布速報の「実験の主旨」より）

  ＊今回の実験速報では、インターネットを通じた「外部侵入の脅威」よりも、庁内LANに不正に接続して「操作権限を奪取する、「内部からの侵入の脅威」が、より注目されています（レポーターのコメント）

実験の目的と実験環境

- 実験環境：市町村が日常使用している状態で、とくに実験のための整備はしていない

  実際に稼働している3町村の庁内LAN及び市町村の住基ネット（市町村管理部分）。
  波田町では、インターネットからの接続に関する実験だけを実施、下諏訪町、阿智村ではそれ以外の実験項目を実施した。ただし実験項目によって実施対象町村が下諏訪町・阿智村のいずれかであるか、または両方であるかは必ずしも明らかではない。

  地方自治情報センターから指示されたファイヤーウォールの設定をしている。
  CSサーバー・CSクライアントのOSのセキュリティパッチ適用範囲については、地方自治情報センターの指示通りであるか不定。そのほかのサーバー・パソコンについても既知のセキュリティパッチがあてられているかについては不定

  実験実施時刻は、町村の事務が行なわれていない（深夜などの）時間帯。このため、LAN上には、日常的な事務処理の情報は流れていない。
  実験用のパソコンや装置は、あいているHUBの接続口を介して庁内LANなどに接続した。
  無線LANの実験には、市販の家庭用無線LAN装置を新たに庁内LANに接続して動作させ、無線LANカードを装着した実験用パソコンを使用した。

2. 速報にもとづく結果と評価

2.1　指摘された危険性の概要

＜県配付「何が分かったのか？」:一部順序を入替えた＞

- CSサーバ、既存住基サーバデータの改ざんが可能である。
- 改ざんしたデータは、日本中どこの自治体でも正当なデータとして扱われる。
- ファイヤーウォールを通過するのは、どのようなデータかがわかった。
- CSサーバへのアクセスを地方自治情報センターは検知できなかった。

（以上は県担当者の評価によるまとめ。吉田さんが県に提出した速報原文には記載されていないとのこと）

管理者権限・管理者用パスワードの取得

CS-CERVER	リモートからのbufferoverflowによる管理者権限取得
CS-CLUENT	リモートからのbufferoverflowによる管理者権限取得
既存住基サーバ	容易に推測可能な管理者用パスワード
庁内webサーバ	リモートからのbufferoverflowによる管理者権限取得

吉田さん配布「ネットワーク図4」より

無線LANから庁内LANに接続可能

出先機関に持ち込みパソコンを接続して庁内LANに接続可能

2.2 評価（想定できる不正行為の例）

＜県配布「何が起こりえるのか？」＞

- 選挙人名簿に登載されていないことにして、選挙をできなくさせる。
- 国民年金データを改ざんして転居させ、転居した場所でより多い額の年金をもらう。
- 介護保険や児童手当の受給データを改ざんして、本来の受給者をもらえなくさせる。
- 税金の滞納データを消去し、そのデータを持たせて、勝手に転出させる。

（上記は県担当者の評価による記載。吉田さんが県に提出した速報原文にはこの指摘はないとのこと）

◆県は今回の実験結果の内とくに既存住基サーバーなど既存システム上のデータ書換えが可能だった点に、重大な関心を寄せていることがわかる

2.3　評価（第3者コメントの結論部分抜粋）

＊伊藤穣一さんの第3者コメントより

- 当該ネットワークのセキュリティレベルが平均以下
- 平均的コンピュータ・ネットワークエンジニアなら誰でも侵入することが可能
- 様々な個人情報を盗んだり損害を与えることができる
- サーバーは適切に保守されてはいません
- 多くが既定パスワードあるいは容易に推測できるパスワードを用いていた
- セキュリティに関する注意の完全な欠如
- プライバシーの目的のためにセキュリティの優先順位が明確に上げられるべき