資料２

平成 15 年 12 月 16 日

市町村ネットワークの安全性調査について（速報）

１　調査の趣旨

・　８月１５日に知事が公表した「長野県の住基ネットに関する今後の方針」に基づき、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を行った。

２　調査日・調査町村

・　第１次は９月２２日から１０月１日まで、阿智村、下諏訪町、波田町を対象に実施した。
・　第２次は１１月２５日から２８日まで、阿智村を対象に実施。
・　調査終了後、発表までの間に、阿智村では緊急の安全措置を実施。

３　調査の実施主体等

・　調査の実施主体は、長野県。（３町村の協力を得て実施）
・　実際の調査は、本人確認情報保護審議会委員の吉田柳太郎委員（指揮監督）に、高度な専門的知識・技術を持つ補助者をつけて実施。補助者とは補助業務に係る委託契約を締結している。

４　調査内容

・　庁内 LAN に接続しての、庁内 LAN 及び住基ネットワーク（市町村管理部分）の安全性調査及びインターネットからの安全性調査。（協力を得た町村の内部ネットワークに対象を限定）
・　町村の業務に影響を与えない配慮をした上で調査を実施。

５　調査結果速報

別添１のとおり

6　第３者評価

（１）第３者評価の必要性

・ ネットワークの安全性調査という、評価の定まりにくい実験であることから第３者の評価を加えることにより、実験結果の信頼性を高めることとした。

（２）第３者評価の実施者

・ 伊藤穣一氏（ネオテニー代表取締役社長、総務省住民基本台帳ネットワークシステム調査委員会委員）に依頼

（３）第３者評価結果

・ 別添２のとおり

別添１

調査結果速報

平成１５年１２月１５日

総務省実験（10月17日品川区）との相違

	総務省	長野県
CS端末	×	○
CSサーバ	不明	○
住基ネット・CS間のFW	×	実験せず
CS・庁内LAN間のFW	×	通過の仕組発見

総務省（井上市町村課長の発言）

（８月５日公開討論会）

- 市町村のコミュニケーションサーバやその内側のファイアウォール、これは指定情報処理機関が24時間監視しているものですが、そこから内側で不正アクセスがないように、指定情報処理機関が十分監視している。

- 市町村設置のファイアウォールも、指定情報処理機関の工事であれば脆弱性はない。

24時間監視の実態

- ＣＳサーバー・ＣＳ端末
  →管理者権限取得（１１月２５日）

- CS・庁内LAN間のFW
  →実験により通過の方法発見（１１月２５日）

  地方自治情報センターから通報なし

- 住基ネット・ＣＳ間のＦＷ
  →１１月２８日にプラグの抜き差し

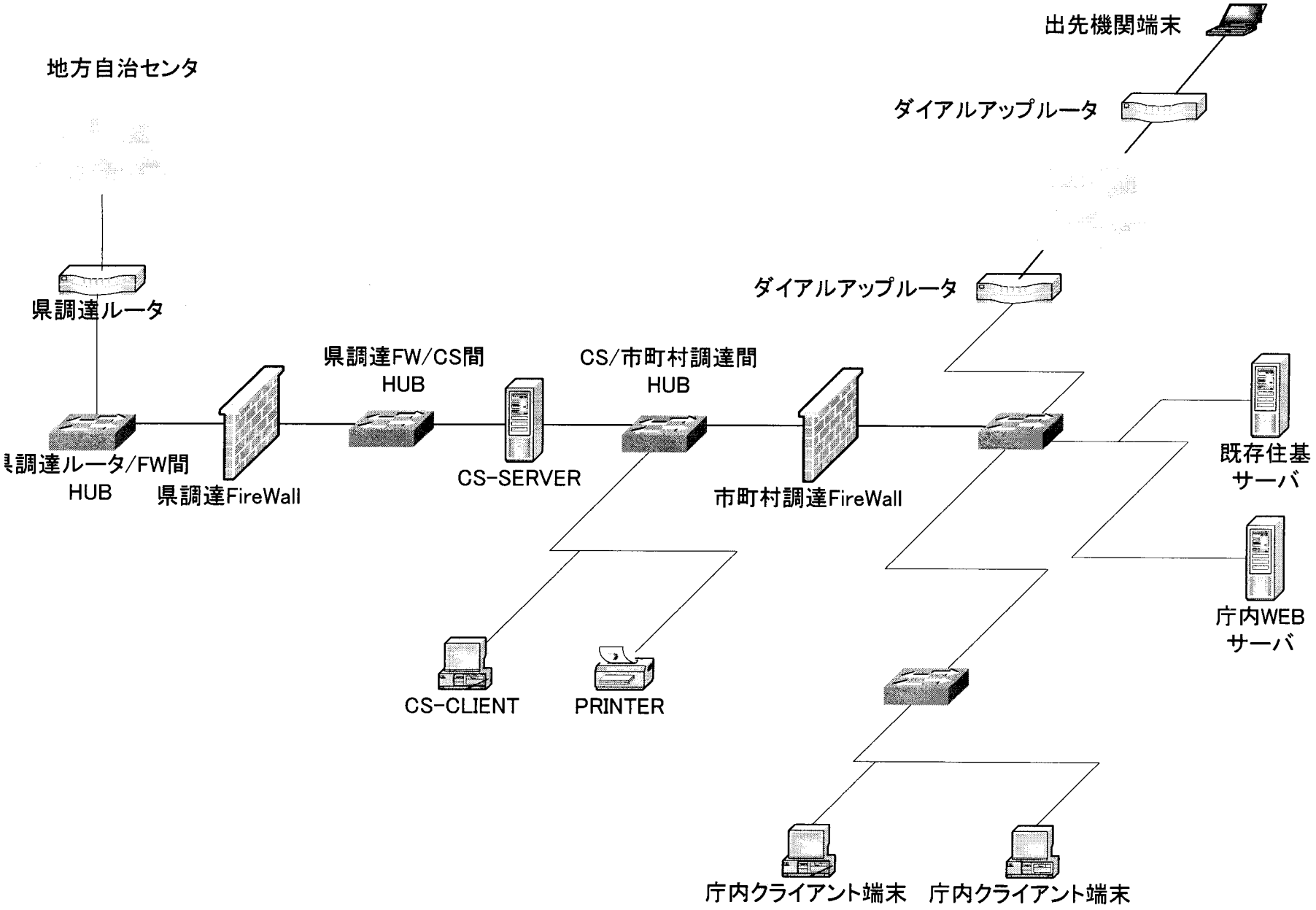
  地方自治情報センターから通報あり

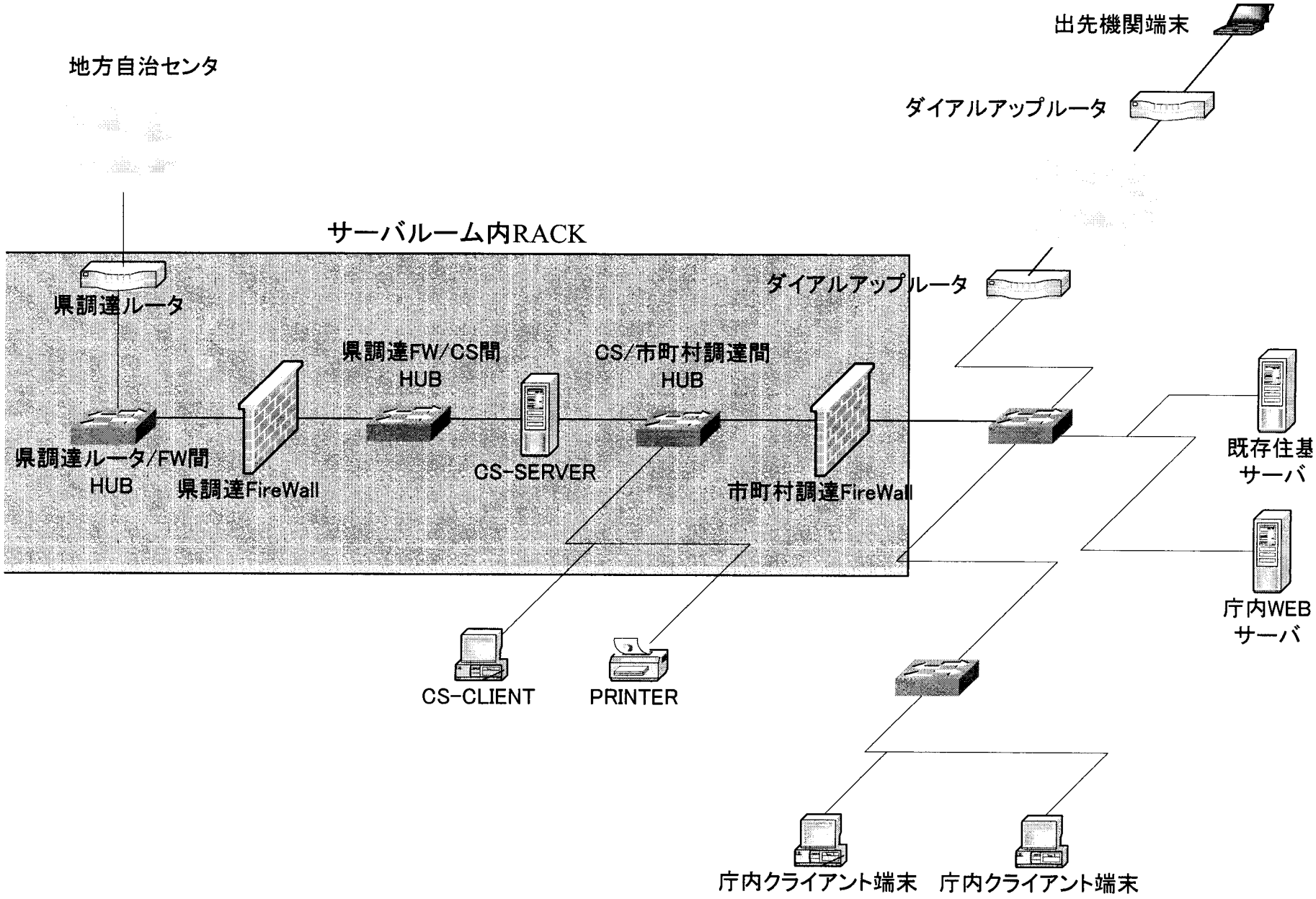
何がわかったのか？

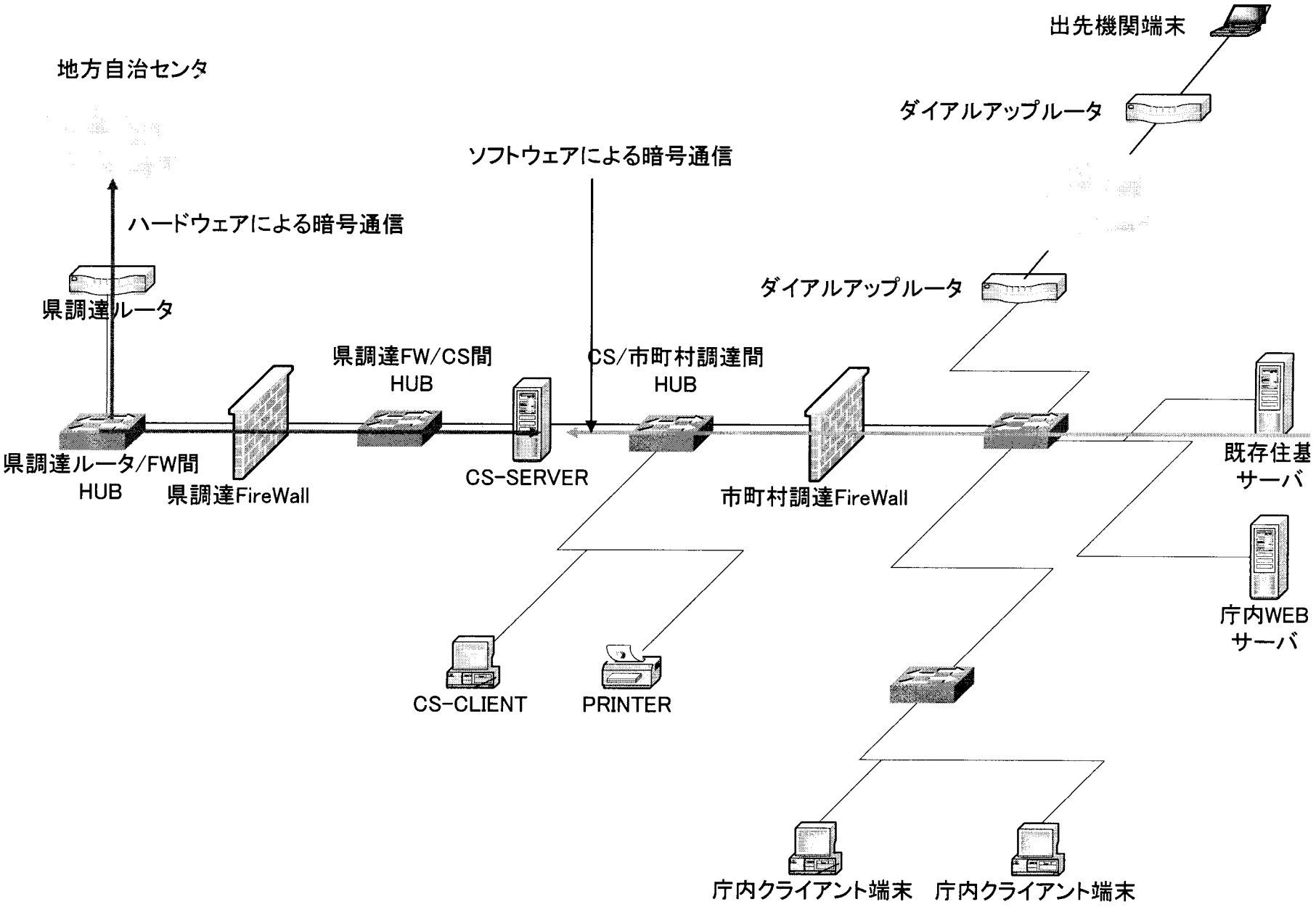
- CSサーバ、既存住基サーバデータの改ざんが可能である。
- FWを通過するのは、どのようなデータかがわかった。
- 改ざんしたデータは、日本中どこの自治体でも正当なデータとして扱われる。
- CSサーバへのアクセスを地方自治情報センターは検知できなかった。

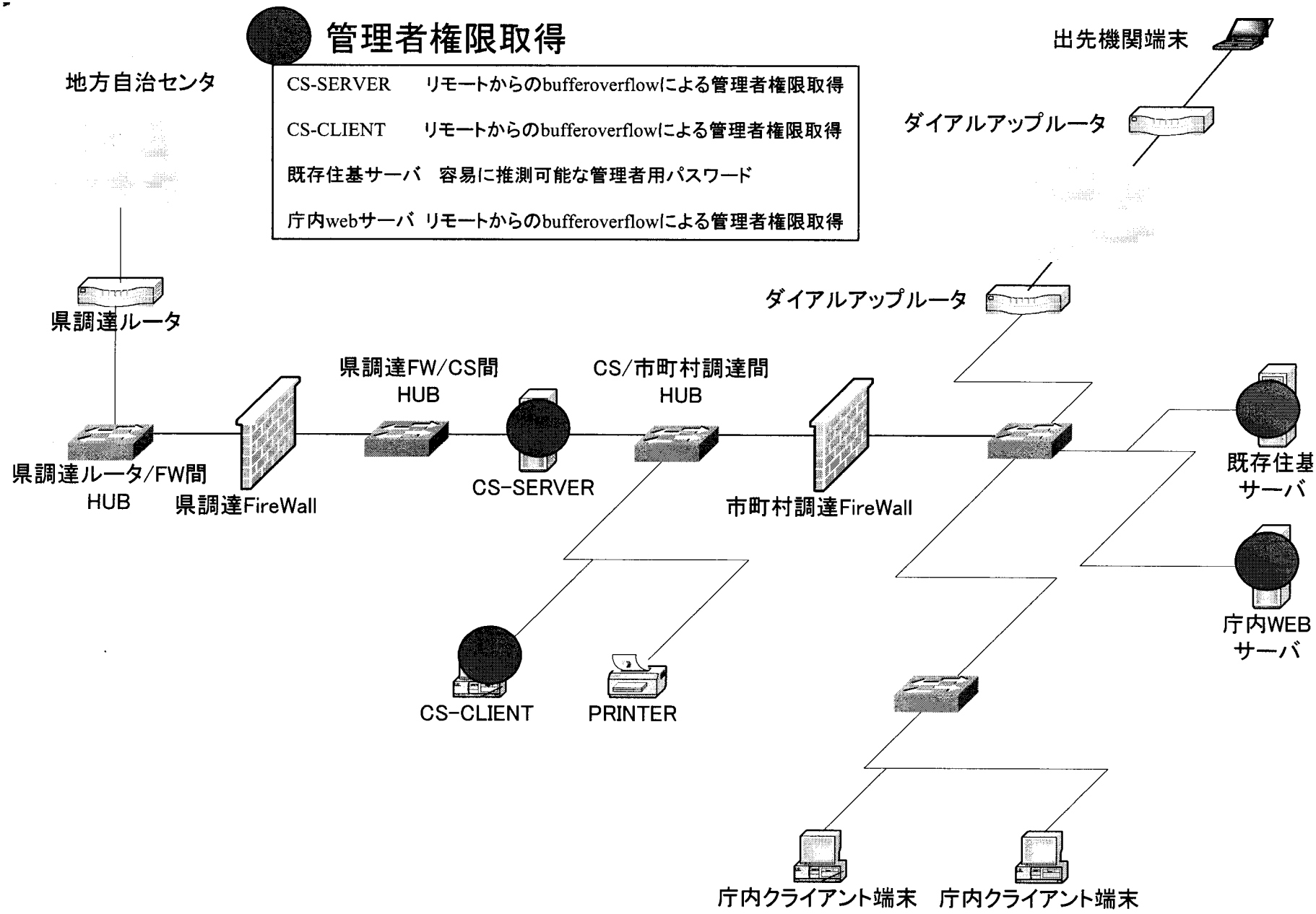
何が起こりえるのか？

- 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る。
- 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。


出先機関端末
地方自治センタ
ダイアルアップルータ
県調達ルータ
ダイアルアップルータ
県調達FW/CS間
HUB
CS/市町村調達間
HUB
県調達ルータ/FW間
HUB
県調達FireWall
CS-SERVER
市町村調達FireWall
既存住基
サーバ
庁内WEB
サーバ
CS-CLIENT
PRINTER
庁内クライアント端末
庁内クライアント端末


出先機関端末
地方自治センタ
ダイアルアップルータ
サーバルーム内RACK
県調達ルータ
ダイアルアップルータ
県調達FW/CS間
HUB
CS/市町村調達間
HUB
既存住基
サーバ
県調達ルータ/FW間
HUB
県調達FireWall
CS-SERVER
市町村調達FireWall
庁内WEB
サーバ
CS-CLIENT
PRINTER
庁内クライアント端末
庁内クライアント端末


出先機関端末
地方自治センタ
ダイアルアップルータ
ソフトウェアによる暗号通信
ハードウェアによる暗号通信
県調達ルータ
ダイアルアップルータ
県調達FW/CS間
HUB
CS/市町村調達間
HUB
県調達ルータ/FW間
HUB
県調達FireWall
CS-SERVER
市町村調達FireWall
既存住基
サーバ
庁内WEB
サーバ
CS-CLIENT
PRINTER
庁内クライアント端末
庁内クライアント端末


管理者権限取得
CS-SERVER　リモートからのbufferoverflowによる管理者権限取得
CS-CLIENT　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
地方自治センタ
出先機関端末
ダイアルアップルータ
県調達ルータ
ダイアルアップルータ
県調達FW/CS間
HUB
CS/市町村調達間
HUB
県調達ルータ/FW間
HUB
県調達FireWall
CS-SERVER
市町村調達FireWall
既存住基
サーバ
庁内WEB
サーバ
CS-CLIENT
PRINTER
庁内クライアント端末
庁内クライアント端末

2003年12月15日

田中康夫 知事

私はあなたと契約した外部調査者が長野県の３つの町村において行ったセキュリティ調査を詳細に再検討しました。私は、それらのプロセス、データと分析について再検討しました。

また私は調査チームの主要メンバーに数時間にわたってインタビューし、彼らの方法論と結論についてもディスカッションしました。

総合的に言って、当該の場所においてのセキュリティレベルは平均以下であり、様々な個人情報は盗まれたり改竄されることに対して危険な状態にあります。

調査チームはインターネットからと地方自治体オフィスの内部から調査を行いました。

このチームは、非常に限定された時間の中で調査を行いました。インターネットからの侵入テストは成功しませんでした。自治体オフィスの中からのテストは非常に成功していました。調査は、地方自治体オフィスの中のコンピュータに限定されていたため、総務省が管理する住基ネットは直接アタックされませんでした。しかしながら、直接に住基ネットに接続するコンピュータである「CSサーバー」と「既存住基サーバー」とは、共に地方自治体ネットワーク内部にあり、当該自治体に住んでいる市民の住基ネットデータのデータベースを持っています。これらのサーバーの両方ともが攻撃されやすい状態であり、調査チームはそれらのコントロールを奪取することが可能でした。これは理論的には、彼らが個人情報を編集したり消去したり新しく作ることを可能にするでしょう。テストでは行われませんでしたが、このデータベースを編集することは偽の記録を中央の住基ネット・システムに送る事態を引き起こす原因となることはありえるでしょう。

加えるなら、住基ネットとは無関係ですが、センシティブな個人情報を含んでいる多数のファイルが、保護がないままの地方自治体ネットワークの上にアクセス可能な状態にありました。

インターネットから地方自治体ネットワークに侵入することは可能ではありませんでしたが、遠距離のオフィスのためにユーザーが地方自治体のネットワークに接続することを許したダイアルアップ・アカウントがありました。これらのダイアルアップ・アカウントが何者かにより支配下に置かれた場合ネットワークにダイアルインすることは可能です。加えて、ある自治体では庁舎以外で直接ネットワークに接続していました。そのマシンを使うかあるいは自分のコンピュータをそこのネットワークと接続することができるならば、「ハッカー技能」を持たない何者でもこれらのマシンの上に「共有されて」いるセンシティブなファイルをダウンロードすることができます。

CS サーバーと、地元の市民の住基ネットデータを収容している既存住基サーバーに侵入することは非常に容易でした。それらは適切にセキュリティパッチが更新されないままシステム運用を行っていました。そのシステムでのパスワードは、データベースの上ものと同様に非常に判りやすく、解明するのに時間はかかりませんでした。

そのサーバー上で走っているソフトウェアなは「バッファー・オーバーフロー」の弱点が含まれた状態で書かれました。これはソフトウェア・コードのデベロッパーのセキュリティの理解の欠如を示すものです。私は、これらのシステム上で走っているソフトウェアに対し第三者によるセキュリティ調査を行うことを推薦します。コンピュータ・エンジニアならば、住基ネットのデータにアクセスを得るために、自由に入手可能なツールを使ってこれらの脆弱性のどれでも自分の制御下に置くことが可能です。

まとめとして、私は当該ネットワークのセキュリティレベルが平均以下であったと考えます。そして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で、住基ネット情報を含む様々な個人情報を盗んだり損害を与えることができるでしょう。オフィスで働く人々と、特にシステム・セキュリティを提供している売り手は、セキュリティとプライバシー問題に敏感ではありません。サーバーは適切に保守されてはいませんでしたし、パスワードの選択（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）は無責任であり、そしてセキュリティに関する注意の完全な欠如を

示していました。私は、地方自治体オフィスとこれらの地方自治体に対するソリューションを供給しているベンダー共に、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ことを強く主張したいと思います。私は、市民と彼らの情報を守るべき担当者が、際立って危険な状態にさらされていると考えます。

伊藤 穣一