ふろく

- 速報された侵入実験の内容・結果・コメント（「長野県侵入実験速報の概要と整理」より抜粋）
- 長野県による速報の評価
- 第三者による速報の評価（要旨）
- 実験対象町村のネットワーク図

インターネットから庁内LANへの侵入（一般的な方法の解説）

波田町の実験では、インターネットに接続している庁内LAN上のパソコンやサーバーに、セキュリティホールを見つけることができなかったため、庁内LAN上のサーバーやパソコンへの侵入にいたっていない

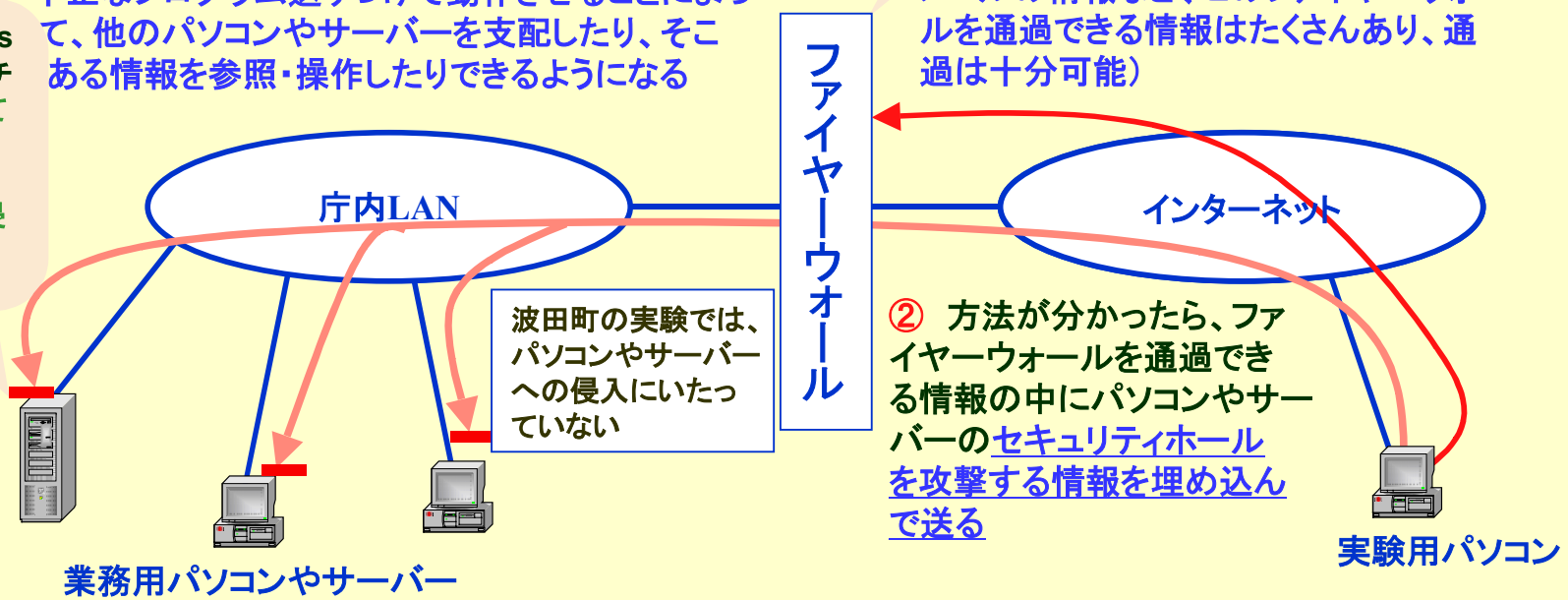
インターネットと庁内LANを分離しているファイヤーウォール

① ファイヤーウォールを通過する方法を調べる（例えば、ホームページや電子メールの情報など、このファイヤーウォールを通過できる情報はたくさんあり、通過は十分可能）

② 方法が分かったら、ファイヤーウォールを通過できる情報の中にパソコンやサーバーのセキュリティホールを攻撃する情報を埋め込んで送る

③ 庁内LAN内のパソコンやサーバーに、セキュリティホールがあれば侵入が成功する場合がある。
その結果、そのパソコンやサーバーに対して
- インターネット上から操作ができるようになる
- 持っている情報を見たり、加工したり、削除したり追加したりできるようになる
- 不正なプログラム送りつけて動作させることによって、他のパソコンやサーバーを支配したり、そこある情報を参照・操作したりできるようになる

たとえば、Windowsのセキュリティパッチをあてるのが遅れていれば、そのパソコン・サーバーを拠点として庁内LANに侵入されてしまう



インターネットから庁内LANへの侵入（補足説明）

ここまでやれば、みだりに侵入されないというレベルに達成されておられました。波田町さんのレベルに到達することができれば、ある程度の安全性を確保できる。（吉田さんの報告より）

予算なり、担当者の勉強する時間だとか、コンピュータに明るい方が非常に少ない中で業務を兼務されている方にですね、同じレベルの知識を今すぐ持てというのはかなり物理的に無理があるんだろうと思います。よってですね、波田町さんというのは、しかるべきスキルをお持ちになって、それをまた業者さんと一体となって運用されているからこそできる業であって、基本的にインターネット側からの脅威というのは何ら変わりなく危険で、相変わらず危険であると、それだけお金をかけないといけないし、知識も磨きつづけないといけない。（同じく吉田さんの報告より）

インターネット接続を中止している市町村についてのコメント

長野県下の市町村さんにつきましてはインターネットの接続は直ちにやめていただきたい、こう再三お話しさせてきていただいておりまして、その意味では安全性という認識を非常に高くお持ちいただいたことによってですね、

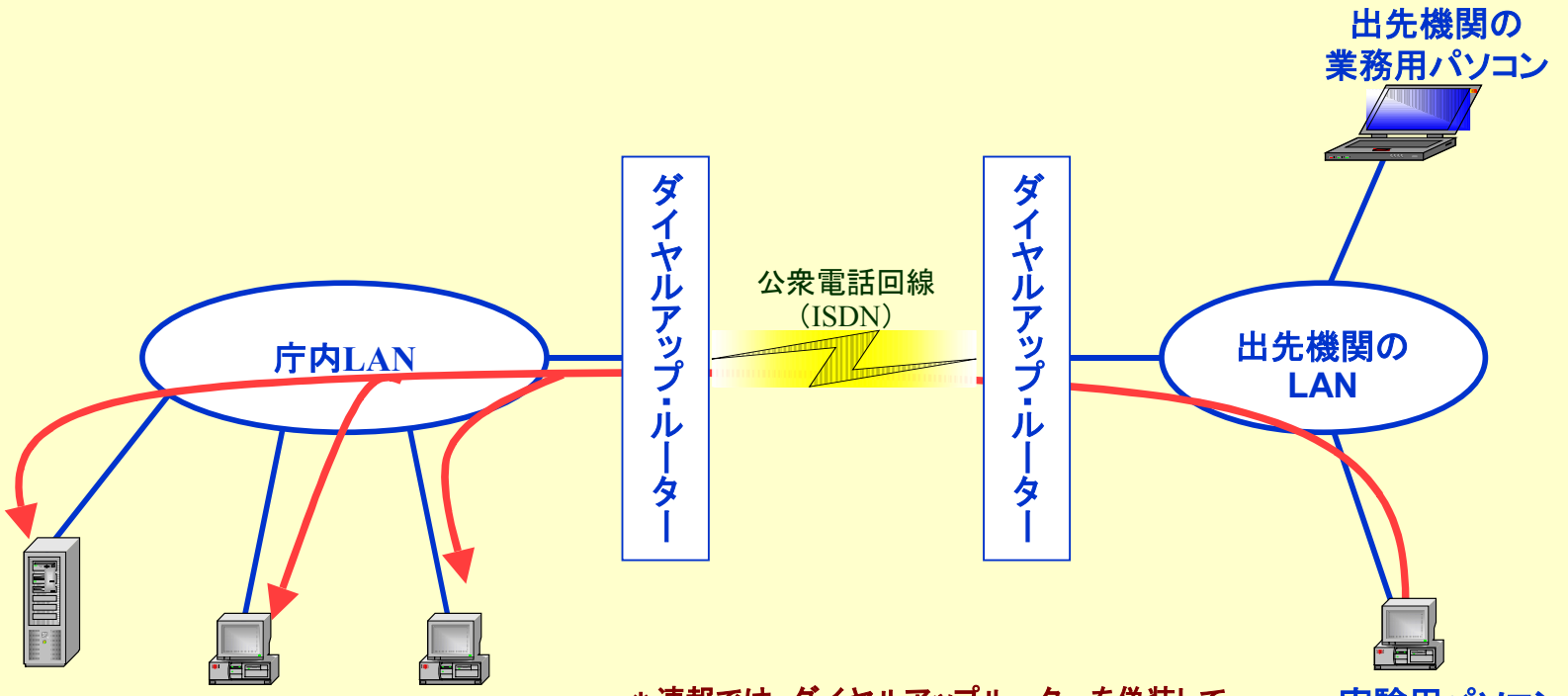
インターネットからの接続を切断いただいていた。

よってですね、インターネットから直接的に庁内ネットワークに入ってこられるという脅威は、ありがたいことに、長野県下ではですね、ほとんどゼロに近い状態。

（吉田さんの報告より）

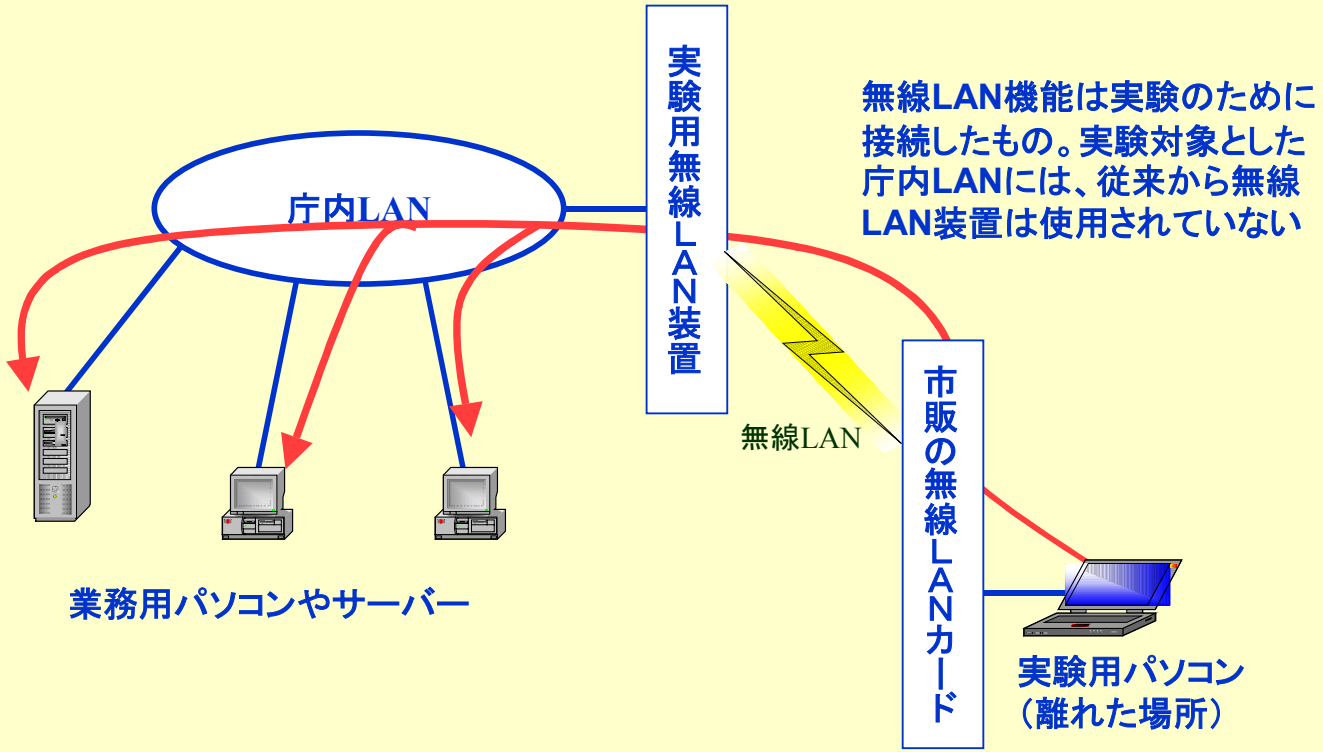
出先機関から庁内LANへの不正な接続

実験用パソコンを出先機関のLANに接続したら、容易に、本庁の庁内LANに接続でき、出先機関の本来の業務用パソコンと同じように操作ができた



無線LANによる庁内LANへの不正な接続

庁内LANに、市販の家庭用無線LAN装置を接続したら容易に動作させることができた。この状態で、離れた場所から家庭用無線LANカードを装着した実験用パソコンで庁内LANに接続でき、本来の業務用パソコンと同じように操作ができた



実験対象外の接続方法についての指摘

以下のような危険な要素が多数存在している

- 庁内LANは、近隣の公共施設（コミュニティセンター・公民館・図書館・スポーツ施設など）に接続されていて、施設の壁など（ 外来者にも手の届く場所）に接続口がもうけられている
- 同じく、ダイヤルアップルーターで接続されている遠方の出先機関（図書館・小中学校・幼稚園などを含む）のLAN接続口についても同様である
- 庁内LANや出先機関のHUBには、あいた接続口があり、外来者にも手の届くところに置かれている場合がある
- 庁内LANに接続されたパソコンの裏側では、むき出しの状態でLANやUSB（住基ネットの操作者認証用ICカードリーダーライターを接続）が接続されていて、誰にでも簡単に抜き差しできる状態になっていた。これは、窓口付近に置かれたCSクライアントでも同様で、ここには操作者認証用のICカードリーダーが接続されている
- ダイヤルアップルーターを偽装することによって、遠方の第3者が庁内LANに接続できる可能性がある。これを防御するには、通常採用される「コールバック方式」では十分といえない

実験対象外の庁内LANに関する安全性一般についての指摘

- 庁内LAN上のパソコンやサーバーには、多くの場合ID・パスワードの設定がされていないか、設定されていても「デフォルトID」から変更されていなかったり、簡単に推定できるID・パスワードを使っている（実際にパスワードを推定できた）
- 既存の各種事務処理システムの情報を蓄積したデータベースについても、アクセスを制限するパスワードについても、簡単に推定できる状態だった
- センシティブな個人情報を含むサーバー上の共有フォルダ（情報共有領域）が、パスワードによって保護されていなかったため、庁内LANから誰にでも見える状態になっていた
- 庁内LANのIPアドレス割り当てが自動化されている（DHCPを使用しているなどと考えられますが、速報では詳細不明）ため、庁内LANへの接続はきわめて容易にできた
- 庁内LAN上のサーバー、パソコンに、公開されているWindowsのセキュリティパッチ（の一部：＊注1）が適用されていなかった。
- こうした状態にされていた要因は、これらの庁内LANが「インターネットに接続されていない、閉じたLANである」ことを理由として、納入業者や自治体の担当者が意識的に「安全だから使い勝手を優先した使い方」をいしていること。
  あるいは、「閉じたLANになっているため、インターネットから簡単にセキュリティパッチのインストールができない」こと。

- 業者が開発・納入した業務用のプログラム（各種業務用アプリケーション）に、バッファー・オーバーフローのセキュリティ・ホールが存在している（この指摘は伊藤穣一さんのコメントによるもの）

注1：「Asahiパソコン」誌04年3月1日号（p.20）によれば、「吉田氏は『実験に使用したセキュリティーホールはMS03-026』と明かした。ほかに、MS03-039とMS03-046も、修正プログラムが当たっておらず、利用可能だったという」。

Webサーバーの安全性

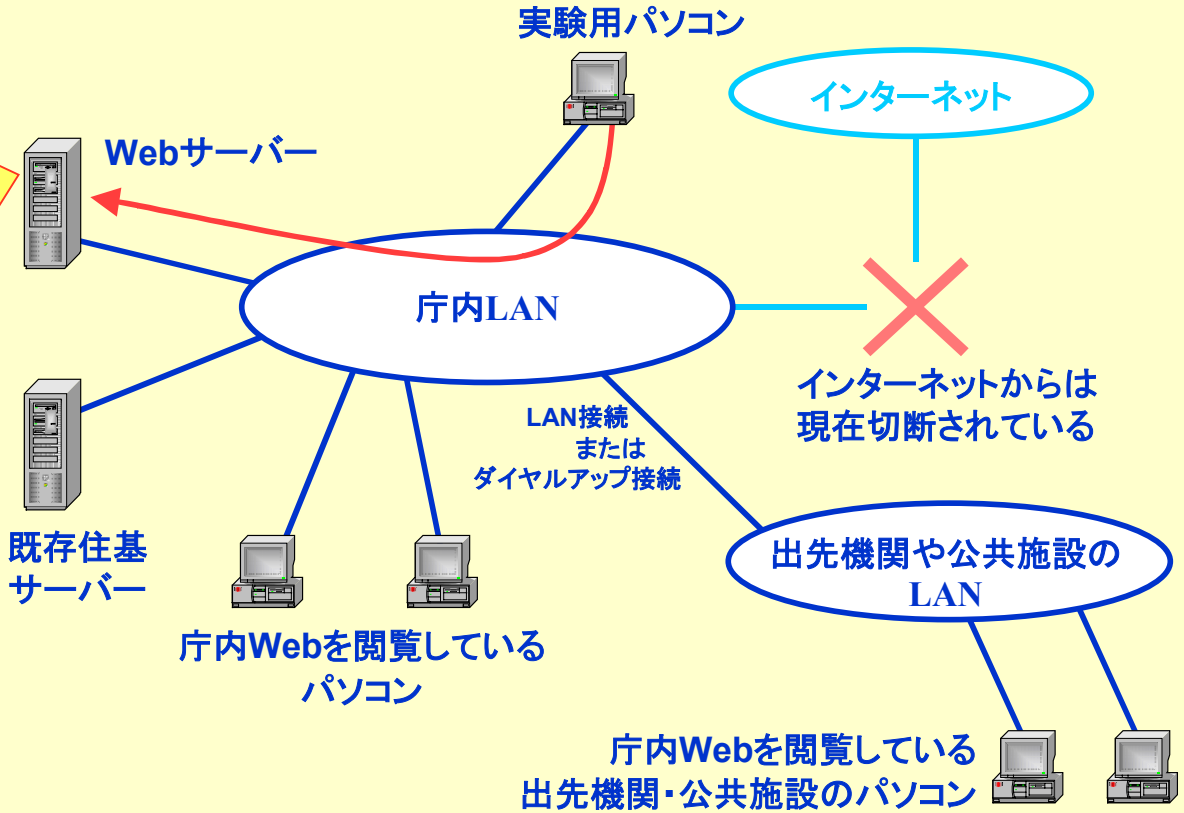
実験用パソコンによってWebサーバーの管理者権限を獲得し、Webサーバーを自由に操作することができた

セキュリティホールを
攻撃することにより
サーバーの管理者権限を
実験用パソコンが獲得

↓

Webの内容を書き換えることが自由にできる
ホームページ上に
ウイルスを仕込んで
他のパソコンに感染させる
ことができる、など

Webサーバー上で不正な
プログラムを動作させるなど
の方法により、
他のパソコン・サーバーに
侵入する拠点にできる



既存住基サーバーおよび既存事務処理システムなどの安全性

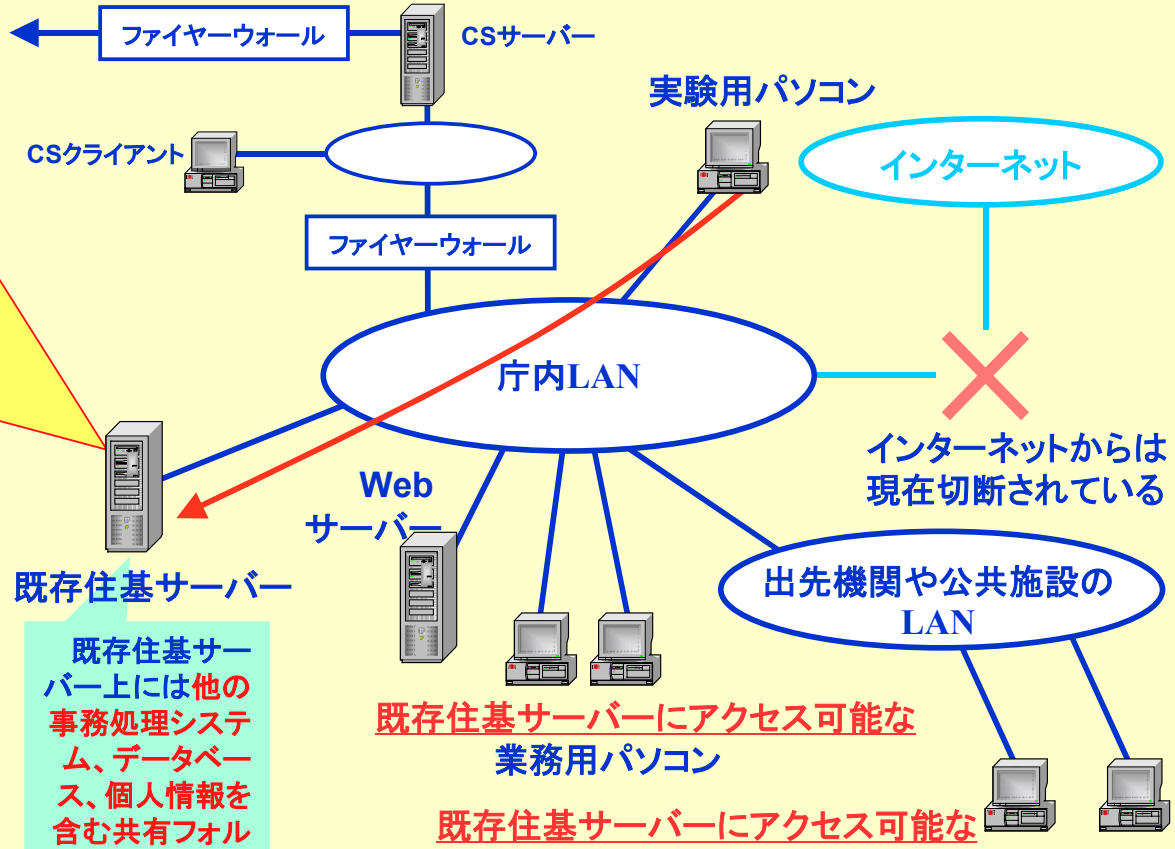
実験用パソコンによって既存住基サーバーの管理者権限・データベース等のID・パスワードを獲得できた。サーバーを自由に操作し、サーバー上の各種の個人情報を参照し、また個人情報が書換・削除可能であることを確認した

セキュリティホールを
攻撃することにより
サーバーの管理者権限を
実験用パソコンが獲得
サーバー上のデータベース・
ファイルのID/パスワードも
容易に推定できた

↓

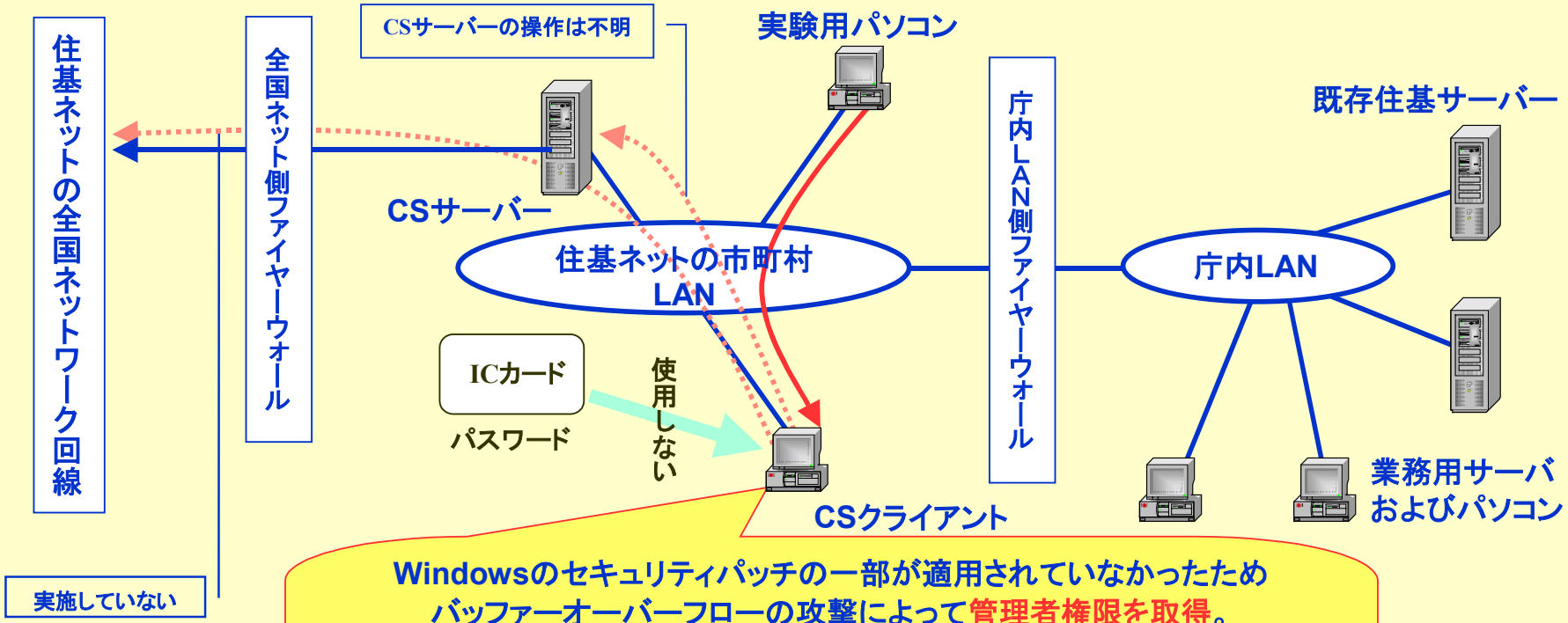
サーバー上の既存住基システム・他の事務処理システム（選挙人名簿・年金・介護保険・税など）や共有フォルダの個人情報を自由に参照・書換・削除できる

既存住基の情報を書き換えることによって、転出など住基ネットを通じて他の市町村にその情報を送付できる



CSクライアントの安全性

実験用パソコンによってCSクライアントの管理者権限を獲得できた。操作者認証用のICカード・パスワードがなくてもCSクライアントを自由に操作できた（住基ネットの業務プログラムを使ってCSサーバー・全国サーバー・県サーバー上の本人確認情報を検索するなどの操作については不明）



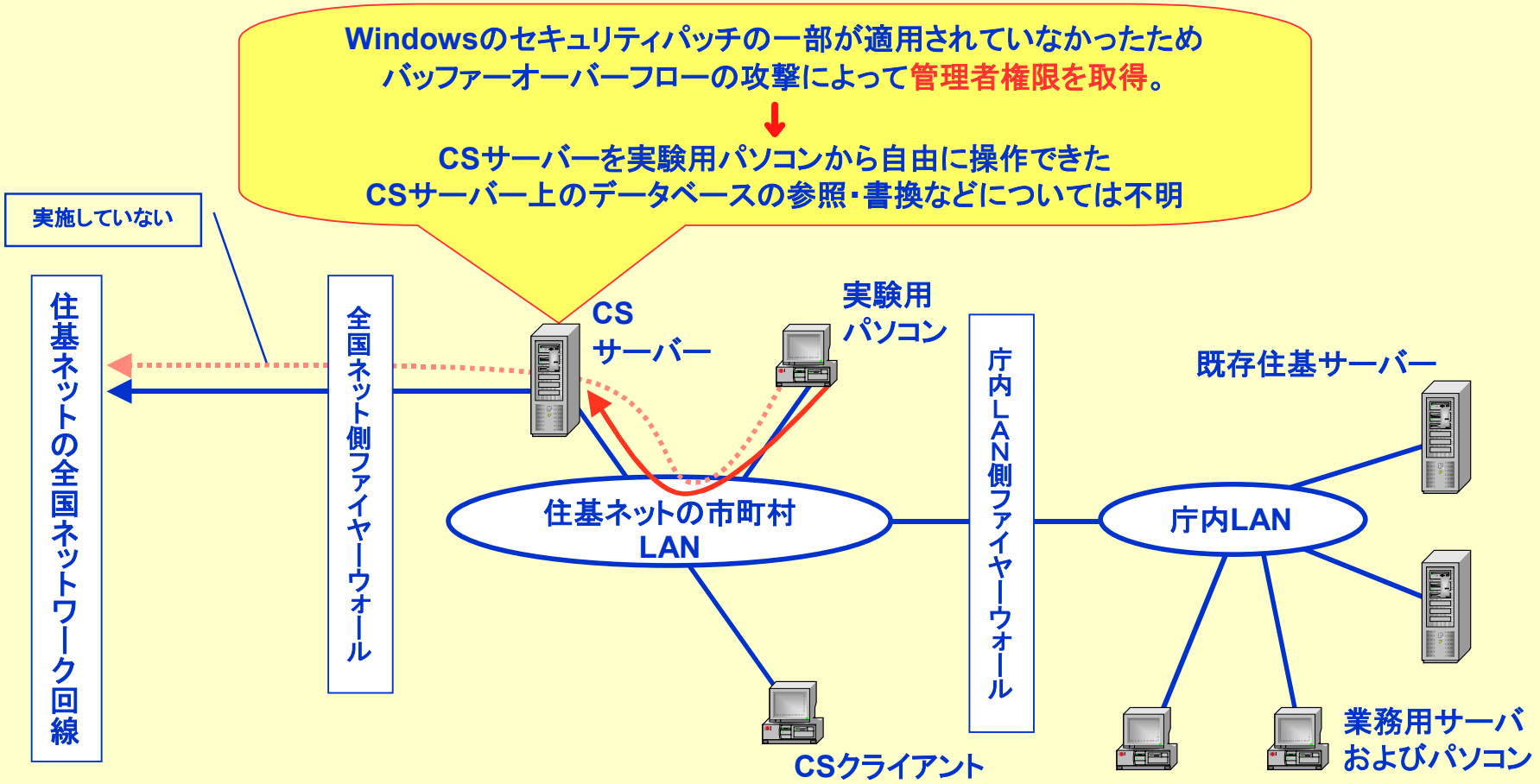
Windowsのセキュリティパッチの一部が適用されていなかったため
バッファーオーバーフローの攻撃によって管理者権限を取得。

↓

CSクライアントを実験用パソコンから自由に操作できた
CSサーバー・全国サーバー・県サーバー上の本人確認情報を検索する
などの操作については不明

CSサーバーの安全性

実験用パソコンによってCSサーバーの管理者権限を獲得でき、CSサーバーを自由に操作できた（CSサーバー・全国サーバー・県サーバー上の本人確認情報の参照や書換などの操作については実施していないため不明）



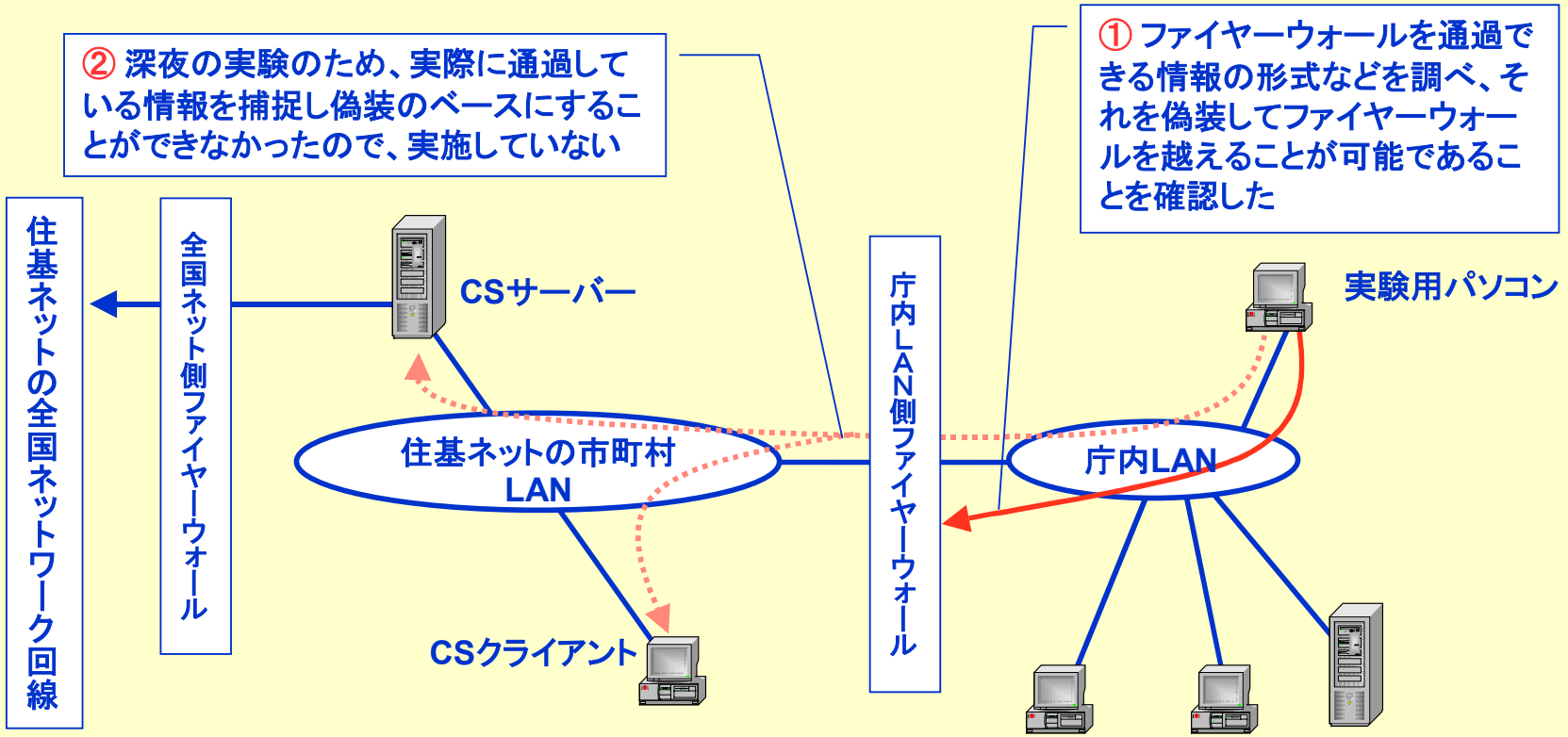
CSサーバーの安全性（補足）

「全国センター・都道府県センターの本人確認情報を検索できるか」との記者の質問に対して、吉田さんは以下のように回答している（検索の実施は法的な不正侵入に該当する可能性が配慮されたため、実施していないと推測できる）。

「答えは可能だということになります。ある特定要件を加えないとLASDEC側に置いてある全部の集約さた情報の検索はできないことになっていますけれども、その条件が手に入ればCS端末を正規に動作させているのと同じ環境が手に入るので、いわゆる検索はできるということですね 」（知事会見の場であった記者の質問に対する吉田さんの説明）

庁内LAN側ファイヤーウォールの安全性

ファイヤーウォールを通過する方法を確認した。ただし、実験時間帯が深夜であったため、実際にファイヤーウォールを通過している情報が存在しないため、これ捕捉して偽装のベースとすることができず、ファイヤーウォールを越えてCSサーバーないしCSクライアントに接続することはしていない

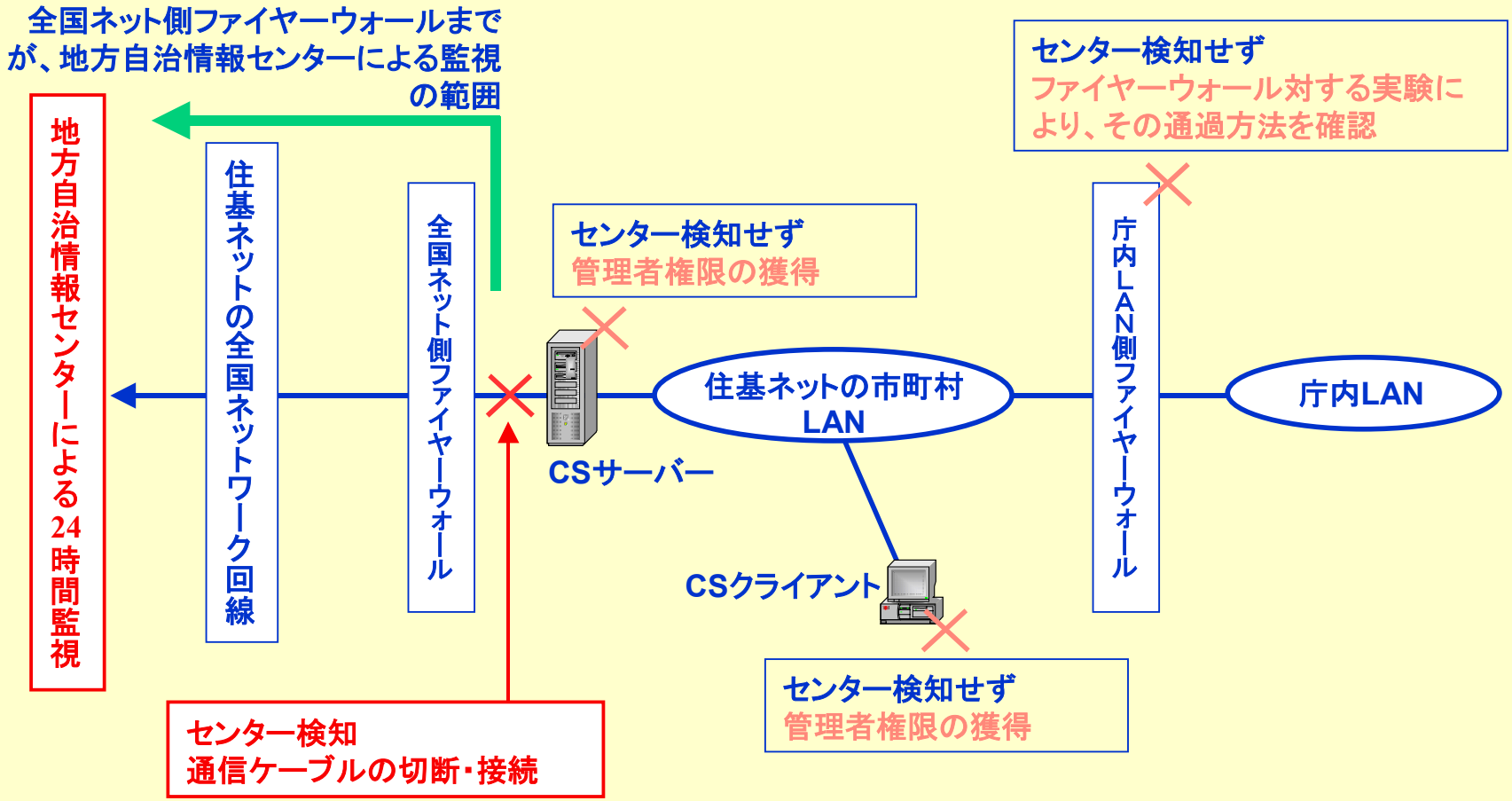


庁内LAN側ファイヤーウォールの安全性（補足）

- 12月24日の長野県本人確認情報保護審議会では、審議会委員の発言の中で「ファイヤーウォールの管理者権限」を取得できる可能性が高いと指摘されています。
  - ✧ これは「記者会見での発言」とされていますが、いつの記者会見でこの問題が言及されたのか未確認です（知事会見の速記録を見る限り、この場では言及されていなかったと思われます）。
  - ✧ また、「管理者権限が取得できる」可能性を指摘されたのが、どのファイヤーウォールであるか、今ひとつはっきりしません。発言を聞いている限りでは「庁内LANとCSサーバーの間に置かれたファイヤーウォール」であると理解可能ですが、明確に確認された議論ではありません。
- 吉田さんのその席での説明によると、このファイヤーウォールには、保守担当業者がネットワークを通じてメンテナンスをするための「裏口」がもうけられていることを根拠として指摘されたもの。そうした「裏口」の存在が実験の中で確認されたようです。
- ファイヤーウォールの管理者権限が不正に取得された場合、ファイヤーウォールの設定を変えて、入り口を新たに作る、働かないようにする、ログを書き換えて何が起きたのか分からないようにする、などが可能になると説明されています

地方自治情報センターによる監視の有効性

地方自治情報センターが24時間監視しているのは、
全国ネット側ファイヤーウォールまでであることが確認できた



県による 評価

＜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）

＜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。

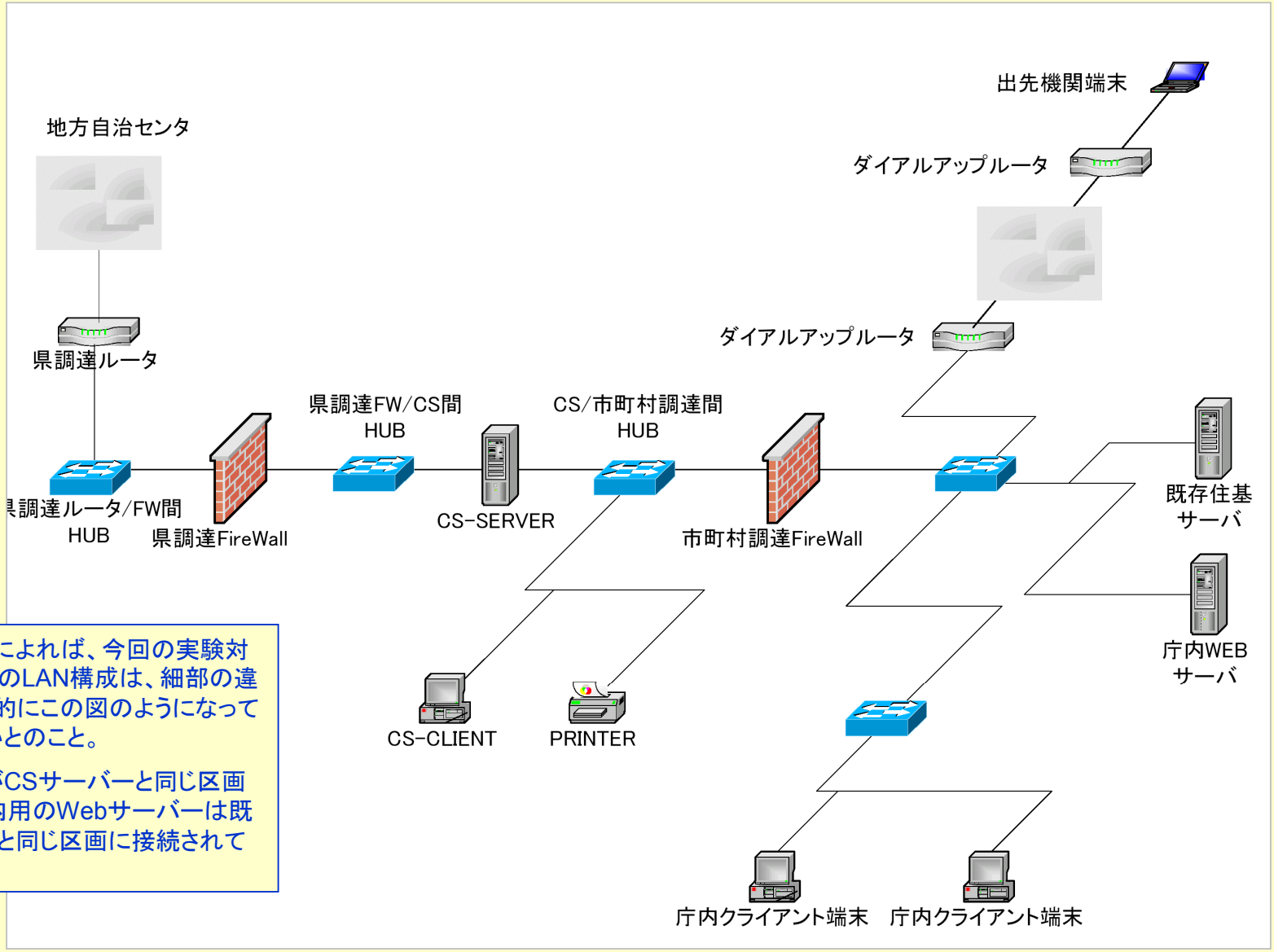
（以上は県担当者の評価によるまとめ。吉田さんが県に提出した速報原文には記載されていないとのこと

第3者による評価（要旨）

＊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

ネットワーク図（知事会見配付資料：吉田柳太郎さん作成）



吉田さんの報告によれば、今回の実験対象となった3町村のLAN構成は、細部の違いはあるが基本的にこの図のようになっていると考えてよいとのこと。

CSクライアントがCSサーバーと同じ区画に接続され、庁内用のWebサーバーは既存住基サーバーと同じ区画に接続されている。