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

3. 実験の内容と結果

「管理者権限の取得」にもとづく「自由な操作」について
（レポーターによる注記）

「実験結果」では、しばしば「管理者権限を取得し、自由な操作ができた」という表現が使われていますが、これはそのまま住基ネットや庁内LANに対する無制限な操作が可能になったことを意味しません。

- 「管理者権限」とは、そのパソコンまたはサーバーのOS（基本ソフト）に対する自由な操作をする権限です。
- ソフト（プログラム）やファイルに操作権限（パスワード）などが設定されている場合、そのソフトやファイルを自由に操作するためには、設定されているパスワードなどを別に獲得する必要があります。
- 「住基ネットの業務用ソフト」では、OSの管理者権限やソフト（プログラム）の操作権限とは異なる、これらから完全に独立した「ICカード・パスワードによる操作者の認証」が行なわれています。OSの管理者権限だけでは、「住基ネットの業務ソフト」を自由に操作して本人確認情報の検索・閲覧・変更等をすることはできません。
- サーバー上の各種の「データベース」などについても、ソフト（プログラム）と同様の「パスワード」が設定されているます。
- 住基ネットの業務用ソフトの「操作者の認証」（CSクライアントで認証）と、「住基ネットのデータベースの操作権限」（データベースの内部で認証）は何らかの形で連携しているものとも考えられますが、詳細は不明。
- 管理者権限が取得できれば、ソフトやデータベースの操作権限を獲得する手がかり（情報）の収集がやりやすくなると考えられます。

3.1 庁内LANの安全性

- インターネットから庁内LANへの侵入
- 出先機関から庁内LANへの接続
- 無線LANによる庁内LANへの接続
- （付）実験対象外の問題点に関する指摘

(a)　インターネットから庁内LANへの侵入

対象：波田町

実験の方法：「インターネット側からのアクセス」（詳細不明）

結果：侵入にいたっていない

コメント：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）

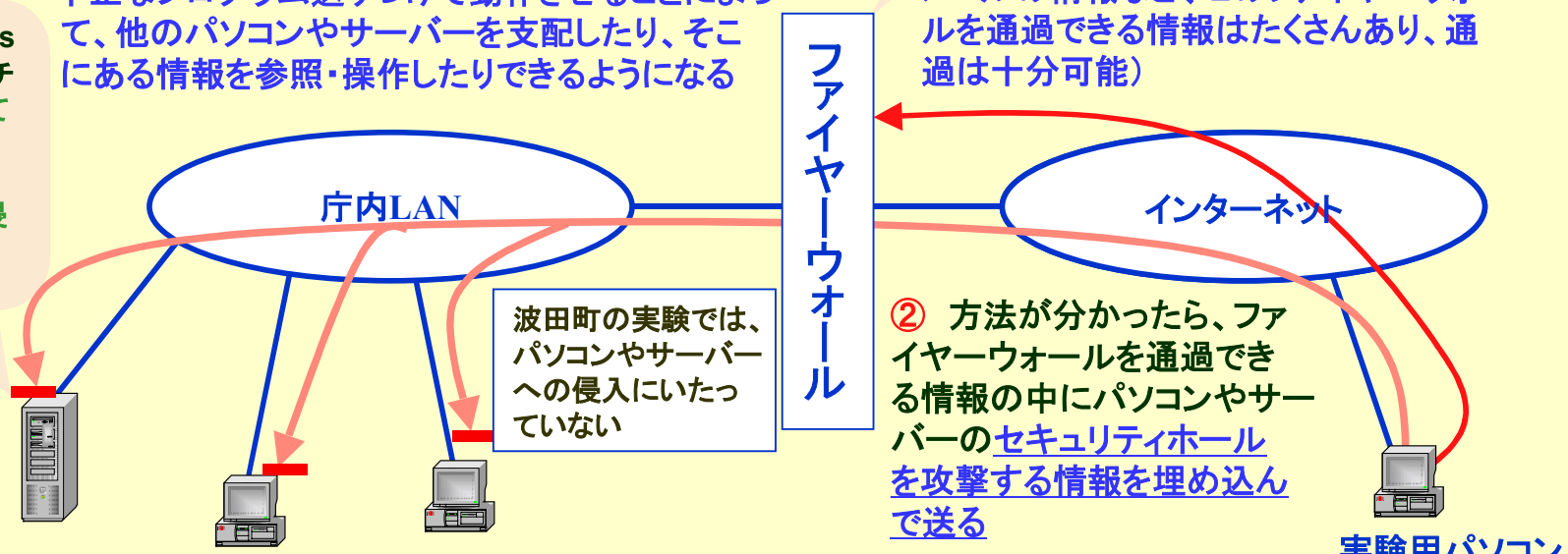
波田町の実験では、インターネットに接続している庁内LAN上のパソコンやサーバーに、セキュリティホールを見つけることができなかったため、庁内LAN上のサーバーやパソコンへの侵入にいたっていない

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、そこにある情報を参照・操作したりできるようになる

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）

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



(a-2) 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）

(b)出先機関から庁内LANへの不正な接続

対象：おそらく下諏訪町・阿智村（要確認）

実験の方法：出先機関のISDNダイヤルアップルーターのあいているLAN接続口に実験用のパソコンを接続して、本庁の庁内LANに接続できるか確認した

結果：庁内LANに接続し、本来の出先機関の業務用パソコンと同様に情報の参照や機能の利用ができた

コメント：既存の住基サーバのファイル共有フォルダの中身にはIDとパスワードというような設定はまったくなされていない状況だった。

出先機関のダイヤルアップルーターを偽装して、無関係の場所から本庁のダイヤルアップルーターに接続することも可能と考えられる。

出先機関には、小中学校・幼稚園・図書館が含まれる。

(c) 無線LANによる庁内LANへの不正な接続

対象：下諏訪町

実験の方法：庁内LANに、新たに市販の家庭用無線LAN装置（送受信局）を接続し、適合する無線欄カードを装着した実験用パソコンで離れたところから庁内LANへの接続が可能かを試みた。無線LANそのものの安全性のチェックはしていない。

（この実験は、無線LAN自体の安全性のテストではなく、無線LAN装置を意図的に持ち込むことによって、庁内LANへの接続・情報の参照などが容易に可能かどうかを確認することが目的）

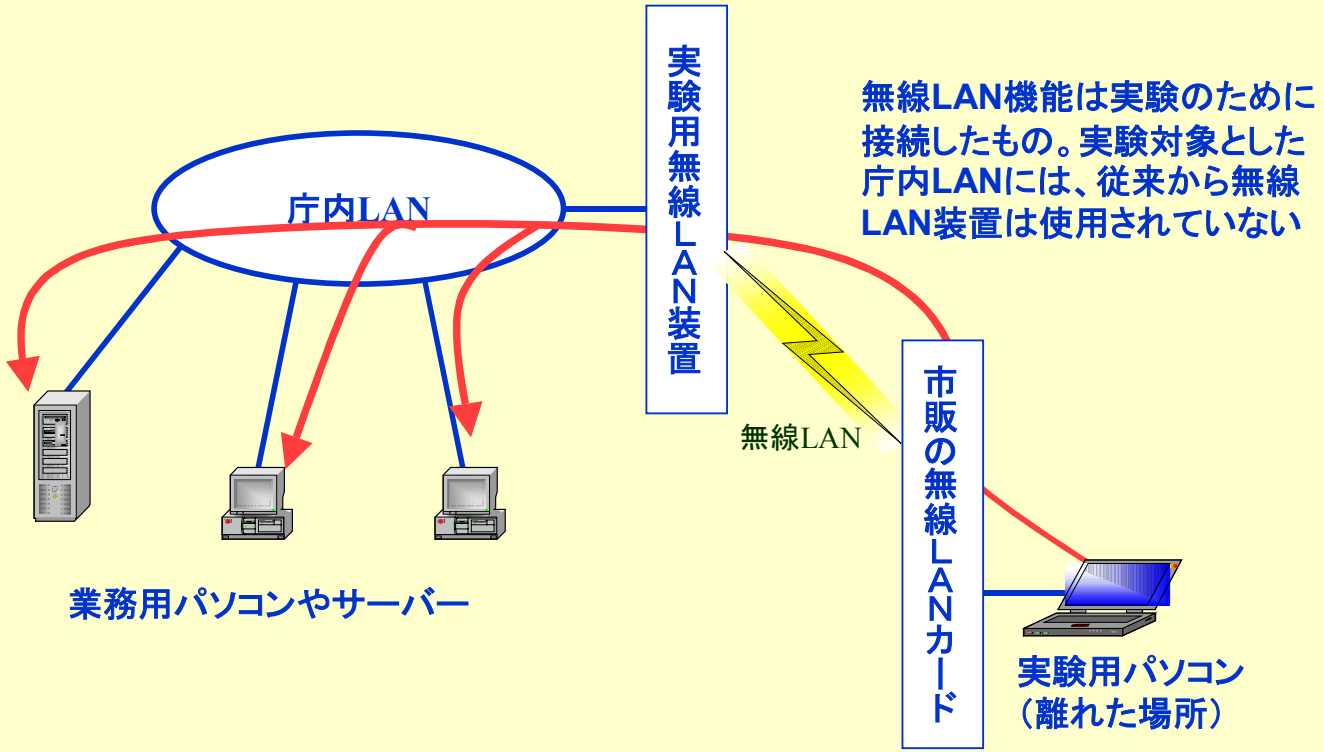
結果：実験用の無線LAN装置を庁内LANに接続して容易に動作させることができた。離れた場所にある実験用パソコンから、庁内LAN上の情報や機能を、正規職員が使っているパソコンと同様に利用することができた）

コメント：庁内LAN自体には、容易に無線LAN装置（送受信局）を接続できるLAN接続口が多数存在している

「（庁内LAN上には）パスワードのかかっていない共有エリアというのが沢山あったりということが、今回はっきりしました。」（吉田さん）

無線LANによる庁内LANへの不正な接続

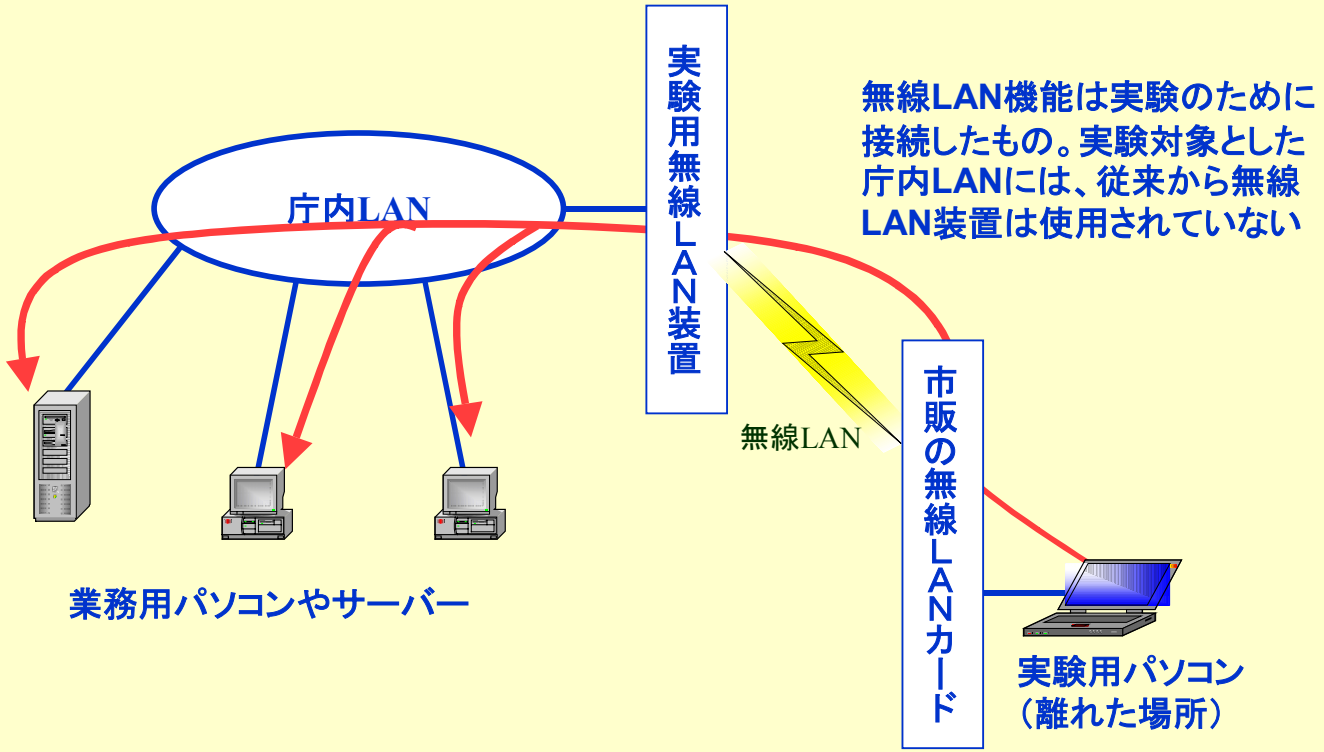
庁内LANに、市販の家庭用無線LAN装置を接続したら容易に動作させることができた。この状態で、離れた場所から家庭用無線LANカードを装着した実験用パソコンで庁内LANに接続でき、本来の業務用パソコンと同じように操作ができた



無線LAN機能は実験のために接続したもの。実験対象とした庁内LANには、従来から無線LAN装置は使用されていない

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



無線LAN機能は実験のために接続したもの。実験対象とした庁内LANには、従来から無線LAN装置は使用されていない

(d) 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

(e) 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）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：詳細不明）が適用されていなかった
- こうした状態にされていたひとつの要因は、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）

3.2 庁内LAN上の既存システムの安全性

- Webサーバーの安全性
- 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

  なお、実験対象2町村では、既存住基システムほか既存の事務処理システムは1台のサーバー上で動作し、また同じサーバー上の情報共有用の共有フォルダが存在しているものと考えられます（詳細不明）

(a)　Webサーバーの安全性

対象：下諏訪町・阿智村の庁内LAN上で稼働しているWebサーバー
（インターネット接続をしていない。各種の公共施設を含む庁内LAN内だけで閲覧するホームページを運用していると考えられる：要確認）

実験の方法：庁内LAN上に接続した実験用パソコンからWebサーバーにアクセスして、管理者権限が獲得できるか試した

結果：バッファーオーバーフローによって、Webサーバーの管理者権限を獲得できた（Webサーバーに対する自由な操作が可能になった）

コメント：Windows2000アドバンストサーバーを使用しており、公開されているセキュリティパッチ（の一部：詳細不明）が適用されていなかった

Webサーバーの安全性

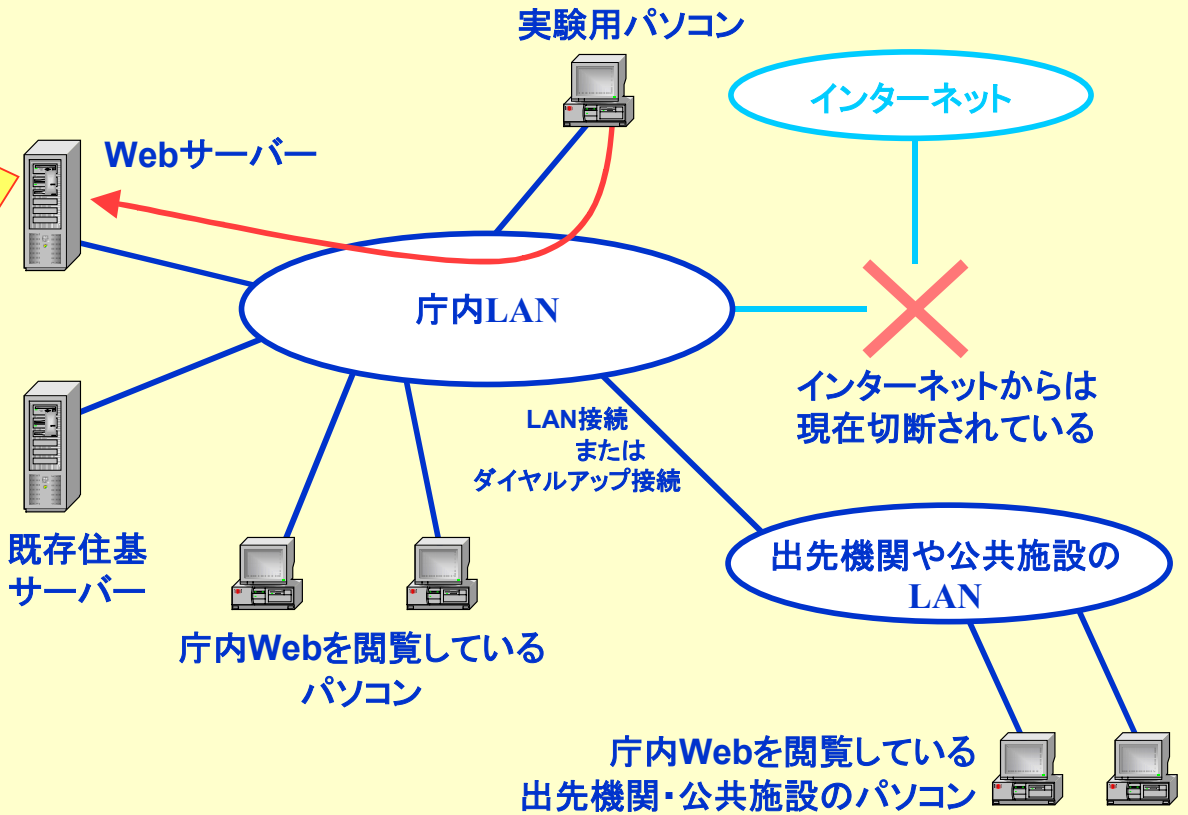
実験用パソコンによってWebサーバーの管理者権限を獲得し、Webサーバーを自由に操作することができた

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



(b) 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

対象：下諏訪町・阿智村の庁内LAN上で稼働している既存住基サーバー
（同じサーバー上で、他の既存事務処理システムのサーバー・情報共有用のための共有フォルダも運用されている：詳細不明）

実験の方法：庁内LAN上に接続した実験用パソコンからサーバーにアクセスして、既存住基サーバー（既存事務処理システムを含む）の管理者権限が獲得できるか試した。またサーバー上の各種ファイルやデータベースの参照・書き換え・削除などが可能か確認した

結果：バッファーオーバーフローによって、サーバーの管理者権限を獲得できた（既存住基サーバーおよび他の事務処理システムのサーバーに対する自由な操作が可能になった）。
また、各種データベースのID・パスワードは容易に推定でき、共有フォルダ内の個人情報ファイルはパスワードで保護されていなかったため、それらの内容を参照できた、書き換え・削除も可能であることが確認できた。

コメント：Windows2000サーバーを使用しており、公開されているセキュリティパッチ（の一部：詳細不明）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攻撃が有効に実行できた

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

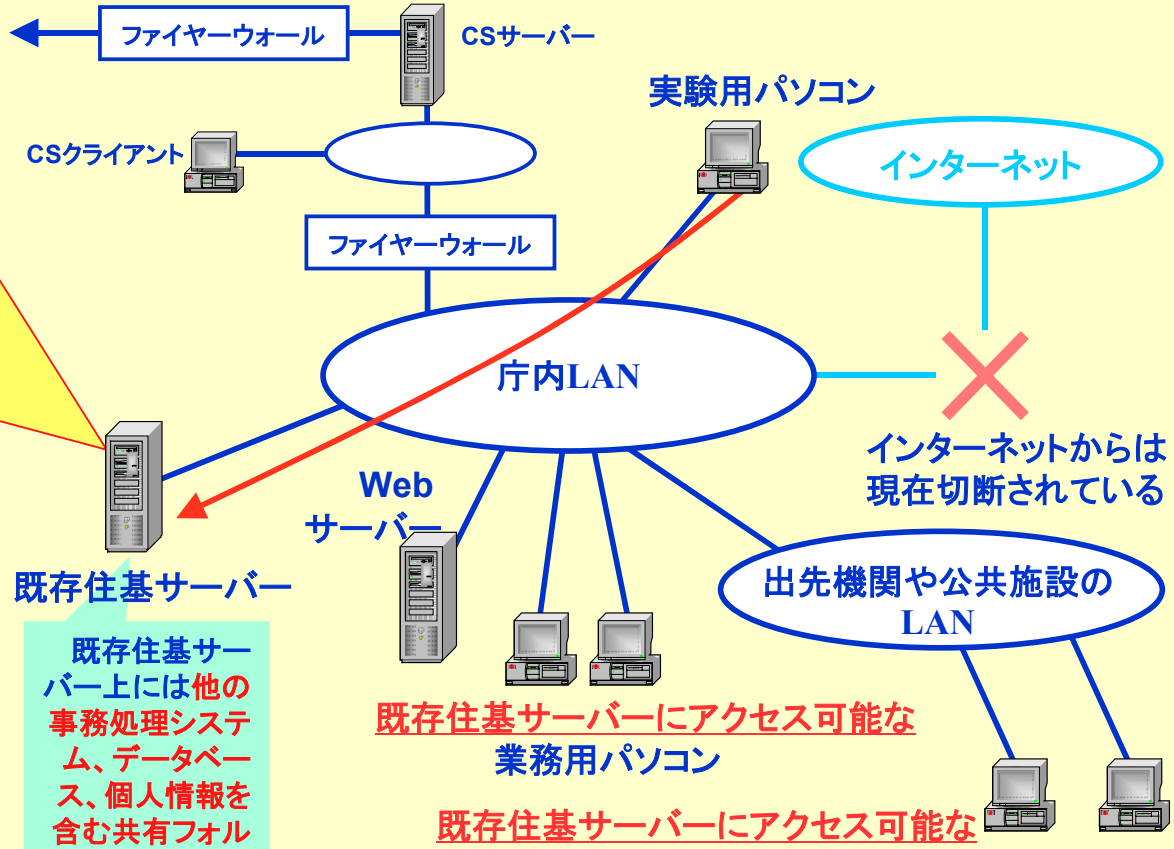
実験用パソコンによって既存住基サーバーの管理者権限・データベース等のID・パスワードを獲得できた。サーバーを自由に操作し、サーバー上の各種の個人情報を参照し、また個人情報が書換・削除可能であることを確認した

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



既存住基サーバー上には他の事務処理システム、データベース、個人情報を含む共有フォルダも存在する

3.3 CSクライアントの安全性

対象：下諏訪町・阿智村のCSクライアント（いずれも、庁内LANとはファイヤーウォールで区切られたCSサーバー側にある）

実験の方法：庁内LANとはファイヤーウォールで区切られたCSクライアント側のLAN上に、実験用パソコンを接続して、CSクライアントの管理者権限が取得できるか試みた。また、ICカードによる操作者の認証無しで、CSクライアントが操作できるかを確認した

結果：CSクライアントの管理者権限を獲得でき、ICカード・パスワードなしでCSクライアント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を検索するなどの操作については不明:＊注）

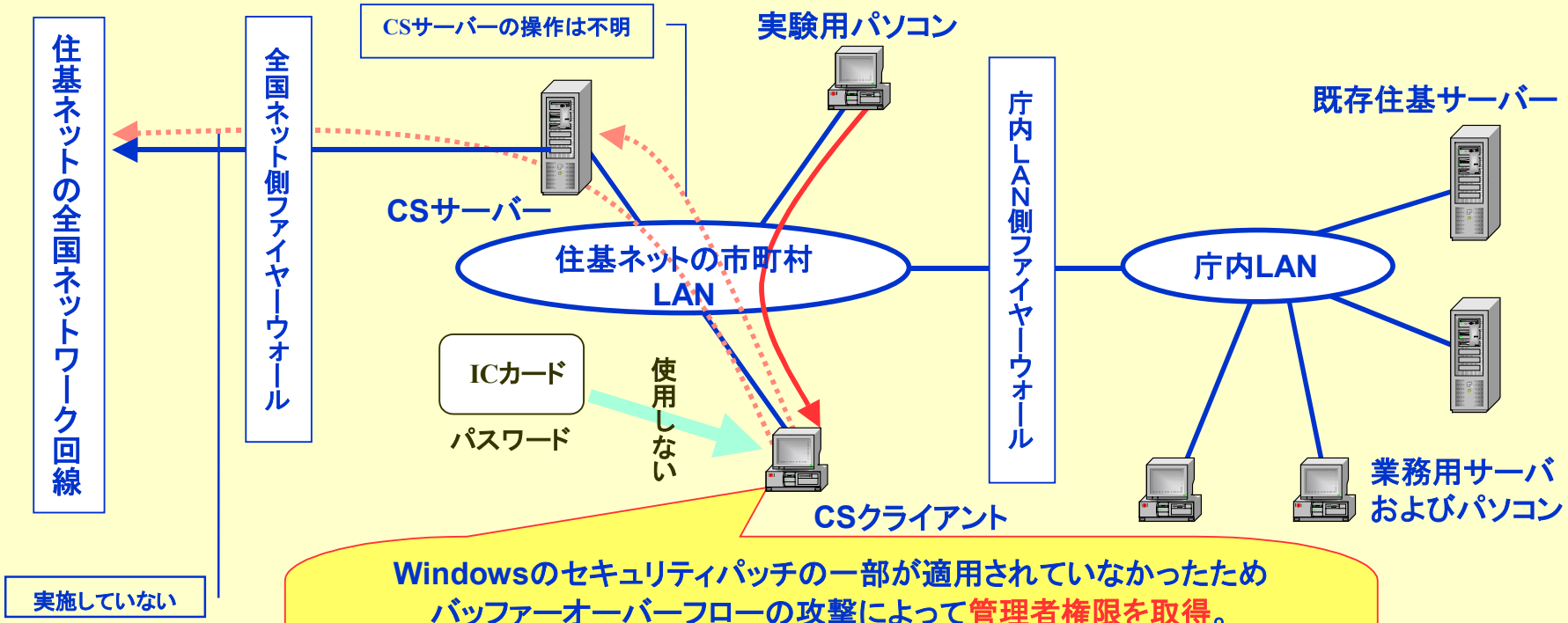
コメント：Windows2000サーバーを使用しており、公開されているセキュリティパッチの一部が適用されていなかったため、バッファーオーバーフロー攻撃が有効に実行できた

＊注：「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 」（会見での質問に対する吉田さんの説明）

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

3.4 CSサーバーの安全性

対象：下諏訪町・阿智村のCSサーバー

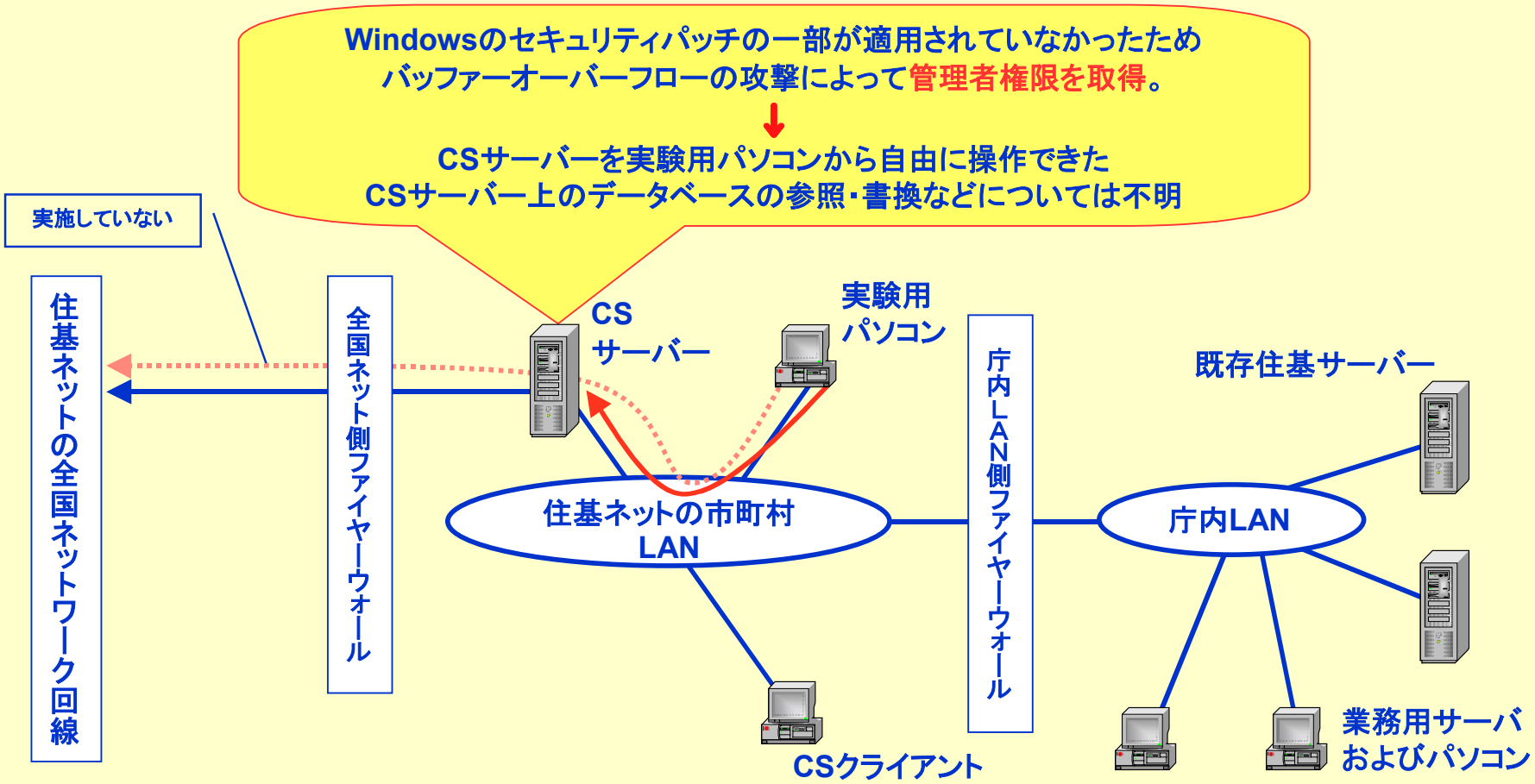
実験の方法：庁内LANとはファイヤーウォールで区切られたCSサーバー側のLAN上に、実験用パソコンを接続して、CSサーバーの管理者権限が取得できるか試験した。（CSサーバー上の本人確認情報データベースに対する試験については不明）。

結果：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サーバー上の本人確認情報データベースに対する操作については不明）

コメント： Windows2000サーバーを使用しており、公開されている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攻撃が有効に実行できた

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）



3.5 住基ネットファイヤーウォールの安全性

- 庁内LAN側ファイヤーウォールの安全性
- 全国ネット側ファイヤーウォールの安全性

(a)　庁内LAN側ファイヤーウォールの安全性

対象：下諏訪町・阿智村の、CSサーバーと庁内LANの間にあるファイヤーウォール（市町村調達ファイヤーウォール）

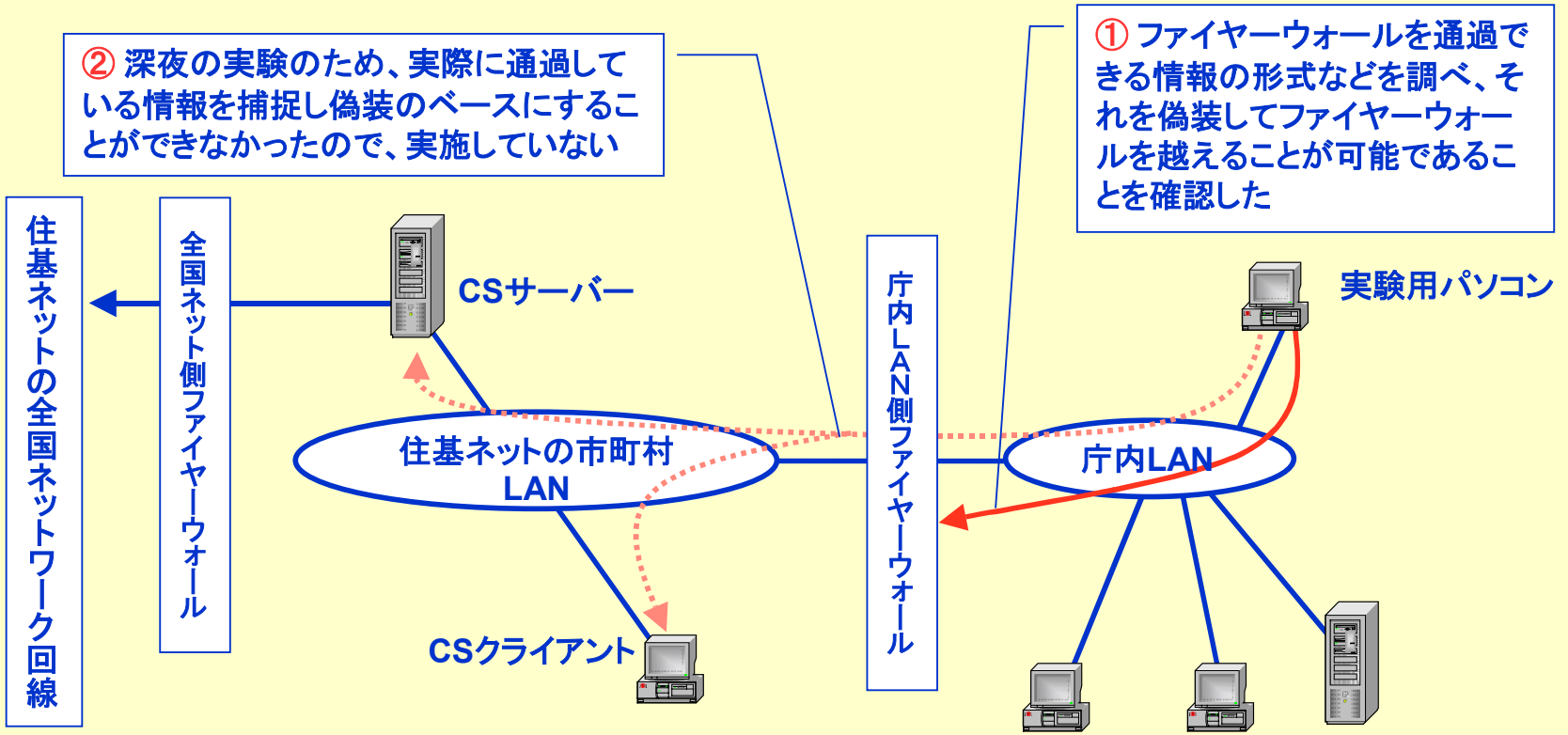
実験の方法：庁内LANに接続した実験用パソコンから、ファイヤーウォールを通過して不正情報を送りCSサーバーまたはCSクライアントに不正に接続できるかを調べた

結果：この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

コメント：業務時間中に実験をしていれば、偽装のサンプルとなる情報を捕捉してこのファイヤーウォールを越えることは容易である

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

(b) 全国ネット側ファイヤーウォールの安全性

地方自治情報センターの監視範囲を確認する以外に、とくに安全性を調べる試験は実施していない

地方自治情報センターの監視については次項参照。

3.6 地方自治情報センターによる監視の有効性

対象：下諏訪町・阿智村（全国ネット側ファイヤーウォールについては阿智村のみ確認）

実験の方法：CSサーバー・CSクライアントおよび庁内LAN側ファイヤーウォール・全国ネット側ファイヤーウォールに対する攻撃や管理者権限の奪取などに対して、地方自治情報センターがどのような反応をするかを観察した。ただし、全国ネット側ファイヤーウォールについては、ネットワーク回線の切断、接続を行ない、反応を待った

結果：①CSサーバー・CSクライアントにアクセスした脆弱性の調査と、その結果にもとづく管理者権限の取得の攻撃に対して、地方自治情報センターは何らの反応を見せず、状況を把握していなかったことが確認された。

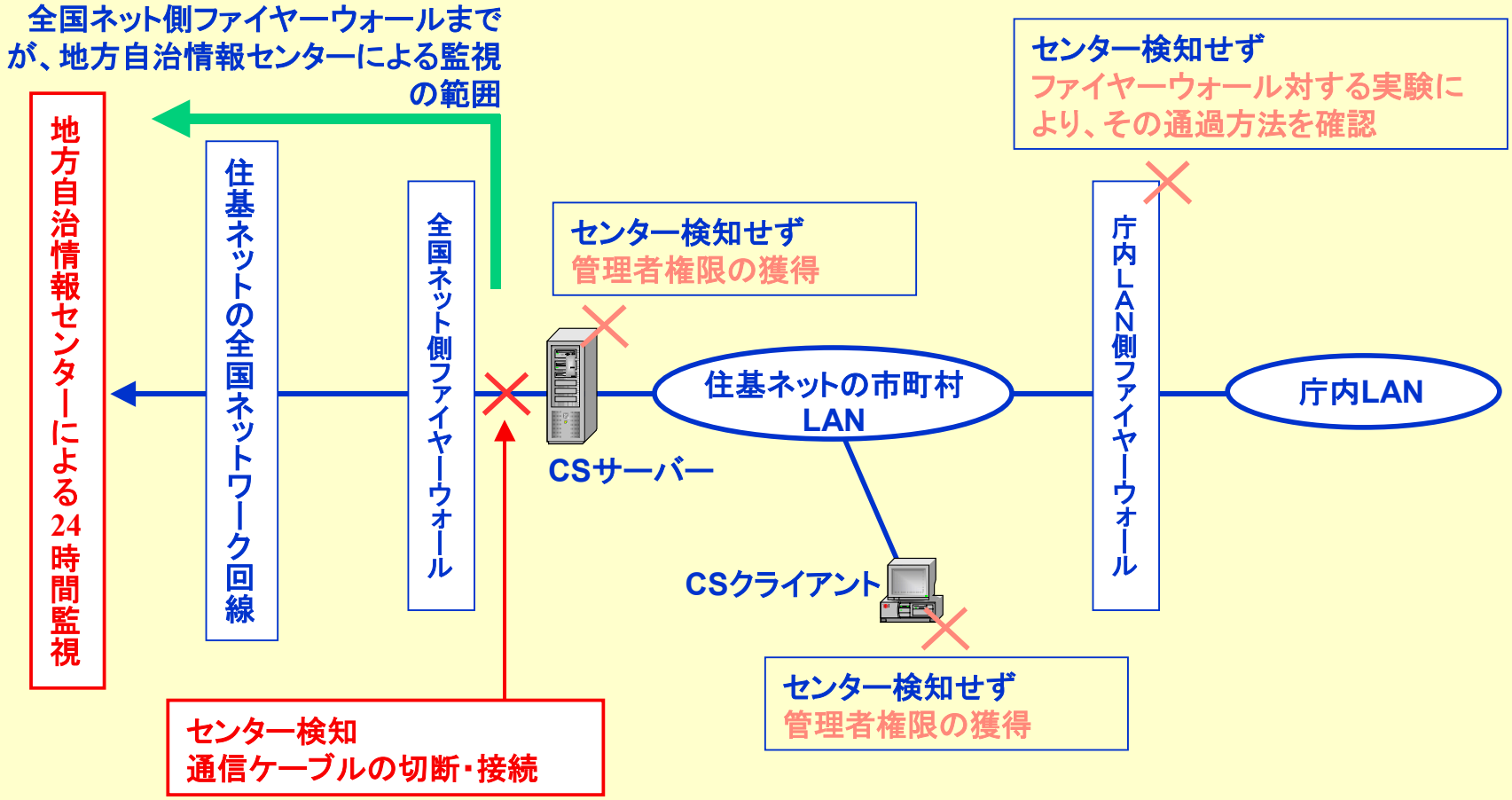
②庁内LAN側ファイヤーウォールにアクセスしてこのファイヤーウォールを通過する方法を確認したが、地方自治情報センターからは同じく反応がなく、状況を把握していなかったことが確認された。

③全国ネット側ファイヤーウォールのネットワーク回線の切断、接続に対しては、ただちに地方自治情報センターから電話による問い合わせがあり、切断の状況を把握していたことが確認された。

コメント：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（確認したのはファイヤーウォールの切断についての監視まで。全国ネットワーク側ファイヤーウォールの何を地方自治情報センターが監視しているのかは不明。詳細を知ることは今回の実験の対象外と考えられる）

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



＜ふろく＞

- 用語解説
- ネットワーク図（1～4）

用語解説 1

- **サーバー**：クライアントからアクセスを受けて、サービス（機能や情報）を提供するもの。厳密には「サービスを提供するソフト／システム」（ソフトウェア）を示すことばで、必ずしもコンピューター自体（ハードウェア）を指していない場合がある（1台のコンピューターで複数のサーバー機能を提供している場合がある）。サーバーには、通常のパソコンよりもやや高性能な機種が使われる場合が多く、とくにそうしたコンピューター（ハードウェア）を指す場合には「サーバー機」と呼ぶ。
- **クライアント**：利用者（個人）が操作してサーバーのサービスを受け、利用者の目的を達成するために使われている個人用コンピューター。通常は「パソコン」と同義。

  「端末」と呼ばれる場合があるが、「端末」は本来「大型コンピューター」（ホストコンピューター）の操作用装置を指すことばで、特定の目的の画面以外表示しないディスプレイとキーボードで構成されている。端末は「パソコン」（クライアント）のような独自の記憶装置や情報処理機能を持たないため、個人の自由な目的に利用することができない。近年、「パソコン」を「端末」として流用するケースが増えていたため混同されているが、端末として利用される「パソコン」は、決められた目的以外には利用できないように機能が制限され留のが普通である。

  住基ネットの「CS端末・業務端末」と呼ばれるコンピューターには「パソコン」が使われ、CSサーバーのサービスを利用している。厳密には「端末」ではない。吉田さんの報告では「CSクライアント」と呼ばれている。本レポートでは吉田さんの用語にしたがっている。

  ✧ 「大型コンピューター本体（ホスト）と操作用装置（端末）」の関係は「ホスト優位」で、「端末」は特定の「ホスト」にだけ専属している。これに対して「サーバーとクライアント」の関係は、その名称からも理解できるように「クライアント優位」で、ネットワーク上のクライアントはどのサーバーのサービスを利用するかをクライアント自身（それを操作する利用者）が決めるている（その意味では、「CSクライアント」にはサーバー選択の自由がなく、「端末」的であると言える）。

用語解説 2

- **CSサーバー**：住基ネットの一部として市町村に置かれているサーバー。本来はコミュニケーション・サーバーの略（CS）だが、慣習的に「CSサーバー」と呼ばれている。

  住基ネット上で自治体が都道府県サーバー・全国サーバーに本人確認情報を提供するための機能を、既存住基システムと通信・連携してはたしているほか、住民票の広域交付・転出時の通知などでは他の市町村と直接通信して情報を交換する。

- **CSクライアント**（CS端末・業務端末）：住基ネットの一部として市町村に置かれているクライアントで、通常は窓口業務担当者が操作するため窓口に配置されている。CSサーバーが提供しているサービスを、自治体職員が利用する場合は、すべてCSクライアントを通じて行なう。CS端末自体は、既存住基システムや都道府県サーバー、全国サーバー、他の自治体と通信することはない。

  CSクライアント上で住基ネットの機能（CSサーバーが提供するサービス）を利用するためには、その操作者専用の認証用「ICカード」と、その操作者だけが知っていることになっている「パスワード」が必要とされている。

- **既存住基サーバー**：電子化された住民基本台帳の情報を記録し、住民基本台帳を使う自治体事務のためのサービスを提供しているサーバー。小規模自治体では、同じサーバー機上に、他の事務処理のための機能（サーバー）が複数同時に稼働していることが、吉田さんの報告で指摘されている。

  自治体によっては、サーバーではなく「大型コンピューター＋端末」やその小型版である「オフコン」が現在でも使われている可能性がある。

用語解説 3

- **データベース**：住所録のような複数の項目をひとまとめにした「定型の情報」を、大量に保存・管理し、検索や自動的な事務処理などに効率よく利用できるようにした、コンピューター上の機能。既存住基サーバーは「住民基本台帳データベース」を中心としてそのサービスを提供している。CSサーバーは「本人確認情報データベース」を持っている。
- **共有フォルダー**：ネットワーク上で情報を共有する最も簡単な仕組みのひとつ。サーバー機のハードディスクに記録・保存されているファイルの内、特定のフォルダの中味をネットワークに接続した利用者に対して公開する仕組み。共有フォルダで情報の共有サービスを提供するサーバーを、「ファイル・サーバー」と呼ぶ。

  利用者を区別せずに誰にでも無制限に情報を公開する場合もあるが、利用者のID・パスワードを共有フォルダに登録して、公開範囲を制限することもできる。個人情報などを含む情報ファイルを共有フォルダで公開する場合は、利用できる個人の範囲をかなり厳しく制限するのが普通。

  そのサーバーの管理者権限を獲得できれば、共有フォルダの利用者制限に関係なく、すべての情報を閲覧・書換・削除できるようになる

用語解説 4

- **セキュリティホール**：コンピューターシステムに対してセキュリティ上の被害を及ぼす行為に対して十分な防御がされていない部分を「セキュリティホール」と呼んでいる。ソフト（プログラム）の中にあるだけでなく、コンピューター自体（ハードウェア）、ネットワークの配線や機器、それらの置かれている場所や置き方、システムを運用する人的な要素など、セキュリティホールは非常に多様な形態で存在している。
- **セキュリティパッチ**：ソフト（プログラム）上に存在しているセキュリティホールを修正するためのプログラムの「ツギあて」。これも一種のプログラム。通常、ソフトを開発した企業の責任で作成され、ソフト利用者に無料で提供される。Windowsのセキュリティパッチは、マイクロソフト社のホームページから誰でもが無料で入手できる。
- **バッファーオーバーフロー**：ソフト（プログラム）のセキュリティホールを攻撃して、プログラムを誤動作させる手法のひとつ。Windows系OSの場合、バッファーオーバーフロー攻撃によって管理者権限を奪取できる場合が多いが、プログラムが暴走してデータを壊したり、プログラムの動作が停止する場合もある。いずれにしてもセキュリティ上の問題になる。

  具体的には、プログラムが一度に処理しきれないきわめて大量の情報を集中して入力することによって、データの一時保存場所（バッファー）をあふれさせ、プログラムの一部を破壊するもの。十分なセキュリティ対策を講じているプログラムでは、こうした攻撃を予想して必要な対策をプログラム上で実施しているが、プログラム自体が非常に複雑になってきているため、攻撃を受ける可能性のある部分を見落として、未対策のまま一般に普及してしまう場合も多い。

用語解説 5

- **LAN**：ローカルエリア・ネットワーク。構内通信網などと訳される。建物内・事業所内など比較的狭い範囲のネットワークを指しているが、後述する広域のネットワークであるWANとの間での厳密な区分はなく、建物内などの複数の独立したLANを相互接続していてもLANと呼ばれている例は少なくない。
- **無線LAN**：通常のLANは電線や光ファイバーなどのケーブルでコンピューターを相互の接続するが、ケーブルの代わりに電波や赤外線などを使ってコンピューター間を接続するLAN。近傍に電波や赤外線などが漏れるので、セキュリティ上の問題が多く、防御対策が研究されているが、現在市販されている普及型の無線LAN装置のセキュリティ対策は十分ではないと言われている。
- **WAN**：ワイドエリア・ネットワーク。比較的広い地域に散在するLANを、相互に接続したネットワーク。インターネットは地球規模のWAN。身近な例としては、国の機関（省庁やその出先機関など）のLANを相互に接続した「霞ヶ関WAN」や、全国の自治体のLANを相互に接続した総合行政ネットワーク（LGWAN）などがある。WANのセキュリティ対策には、LAN単位で一定レベルのセキュリティ強度を確保した上でWANに接続するという原則が、必須のものとして採用されている（LGWANでも、形式的にはこの原則が適用されている）。

  住基ネットも一種のWANであるが、ネットワークの設計思想が大型コンピューターシステム（ホスト・端末型システム）に近いためか、今までWANと呼ばれれた例を見ていない。セキュリティ対策も接続するLAN単位のセキュリティ強度確保が軽視され、WANの原則は採用されていない（LAN間の接続は、日時を定めて強制的に実施された）。

用語解説 6

- **ルーター**：LAN間の接続をするとき、LANの出入り口に置かれる交換機の一種で、LANの独立性を確保する装置。LAN上を流れる情報についている「宛先」（アドレス）を常時チェックしていて、他のLAN宛の情報だけを、そのLANの外に送り出している。また、外部から受信した情報の宛先をチェックし、LAN内のどれかのコンピューターあての場合だけ、内部の独自の宛先（ローカルアドレス）に書き換えてLAN内に送信する。
- **ダイヤルアップ・ルーター**：LAN間は通常専用線などで接続されるが、公衆電話回線でLAN間接続を行なうために、ダイヤルアップ・ルーターには通常のルーター機能のほか「電話番号を指定して相手に接続する機能」（受信もできる）が追加されている（電話を使ってインターネット接続をする「モデム」は、ルーター機能を持っていない）。アナログ電話回線用とISDN用があるが、通信速度が早いISDN回線を使う方式が一般的。

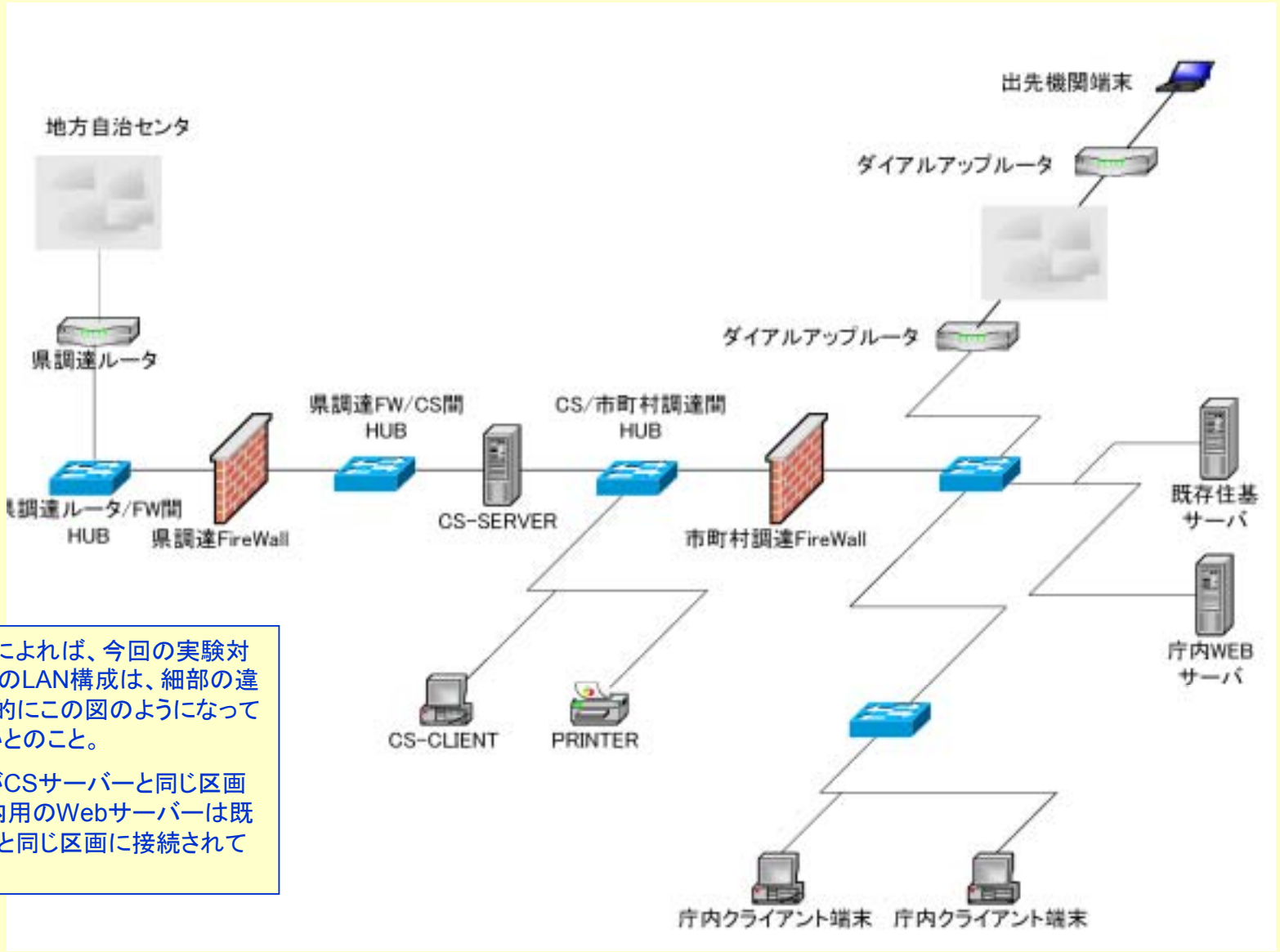
  ダイヤルアップルーターは発信機能と着信機能の両方を持っているため、セキュリティ設定を確実にしないと、想定しなかった相手からの情報を無差別に着信してLANに接続してしまう場合がある（侵入を受けやすい）。これを防止する一般的な手法として、「コールバック」がよく使われている。着信して相手を確認したら一度電話を切り、着信側から改めて発信側の（あらかじめ登録されていた）電話番号を呼び出して接続し、通信を開始する方式。自治体で使われているダイヤルアップ・ルーターでは、このコールバック方式の利用が徹底していない場合があるといわれている。

用語解説 7

- **HUB**：LAN内のコンピューターを、ケーブルを通じて相互に接続する中継装置の一種で、機能としては「集線装置」である。複数のLANケーブルの接続口を持ち、どれかひとつの接続口に受信した情報は、無差別に、他のすべての接続口に向けて送信される。ルーターのような情報の宛先（アドレス）などはまったくチェックしていない（最近は、LANが複雑化してきたために、宛先をチェックして特定の接続口にだけ送信する「スイッチングハブ」も使われ始めている）。
- **ファイヤーウォール**：LANやLANの一部分（セグメント）のセキュリティ確保を目的として、その入り口に設置されているサーバーの一種。基本動作としては、情報が持っている宛先などいくつかの形式をチェックして、あらかじめ登録されている特定の形式と一致する情報だけを通過させている（フィルタリング機能）。基本動作はルーターに似ているが、外部からの侵入・攻撃に対する高度な耐久性を持つように作られているなど、セキュリティ確保の目的に特化して作られ、使われている。

  ファイヤーウォールは情報の形式だけをチェックしているので、情報の内容は判断できない。このため、通過する情報にセキュリティ・ホールを攻撃するプログラムなどが含まれていても、ファイヤーウォールはこれを排除することができない。

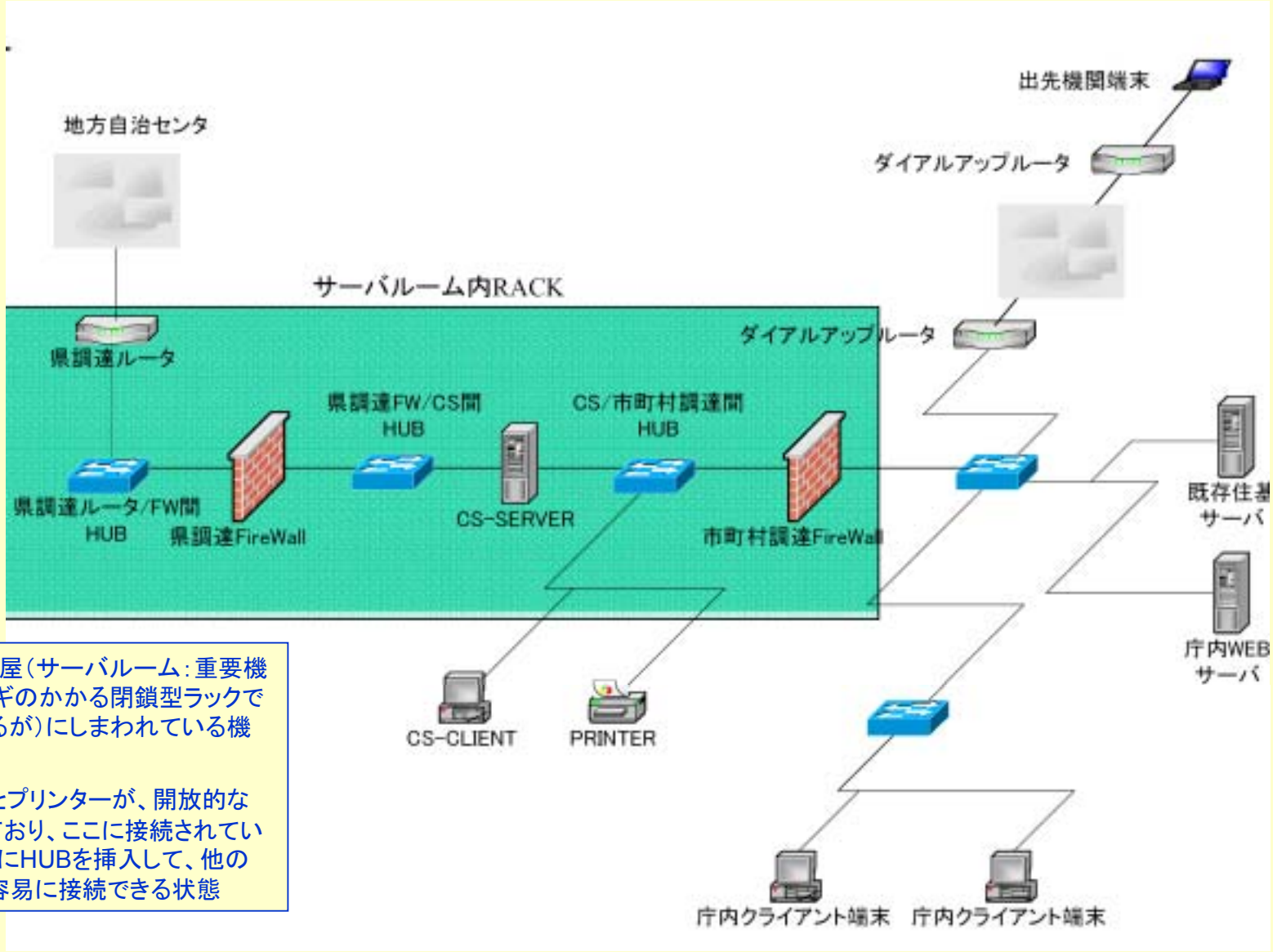
ネットワーク図1（吉田さん配布資料）



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。

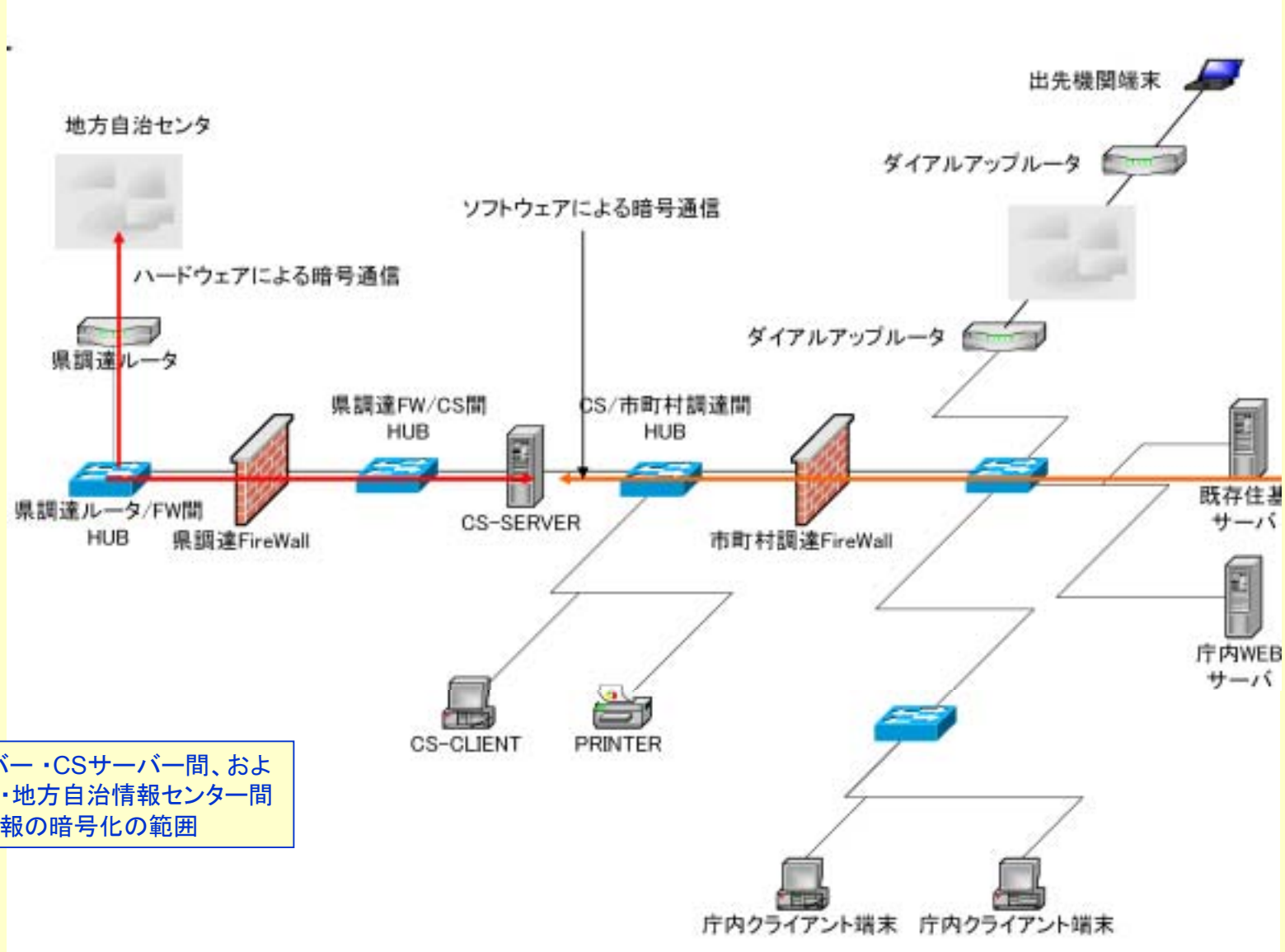
ネットワーク図2（吉田さん配布資料）



カギのかかる部屋（サーバルーム：重要機器室。またはカギのかかる閉鎖型ラックでも可とされているが）にしまわれている機器の範囲。

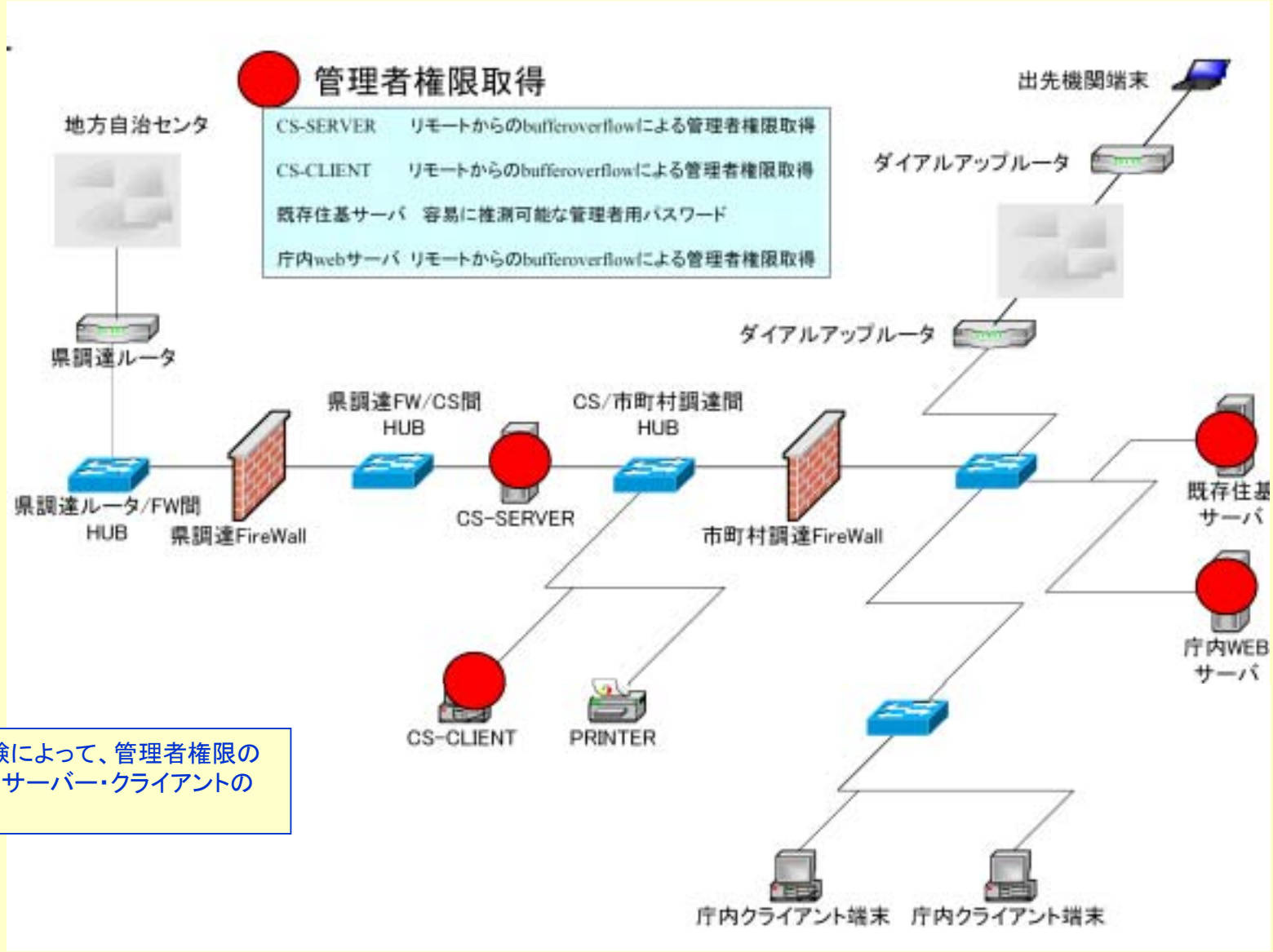
CSクライアントとプリンターが、開放的な場所に置かれており、ここに接続されているLANケーブルにHUBを挿入して、他のパソコンなどを容易に接続できる状態

ネットワーク図3（吉田さん配布資料）



既存住基サーバー・CSサーバー間、およびCSサーバー・地方自治情報センター間で交換される情報の暗号化の範囲

ネットワーク図4（吉田さん配布資料）



今回の侵入実験によって、管理者権限の取得に成功したサーバー・クライアントの範囲