＜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。

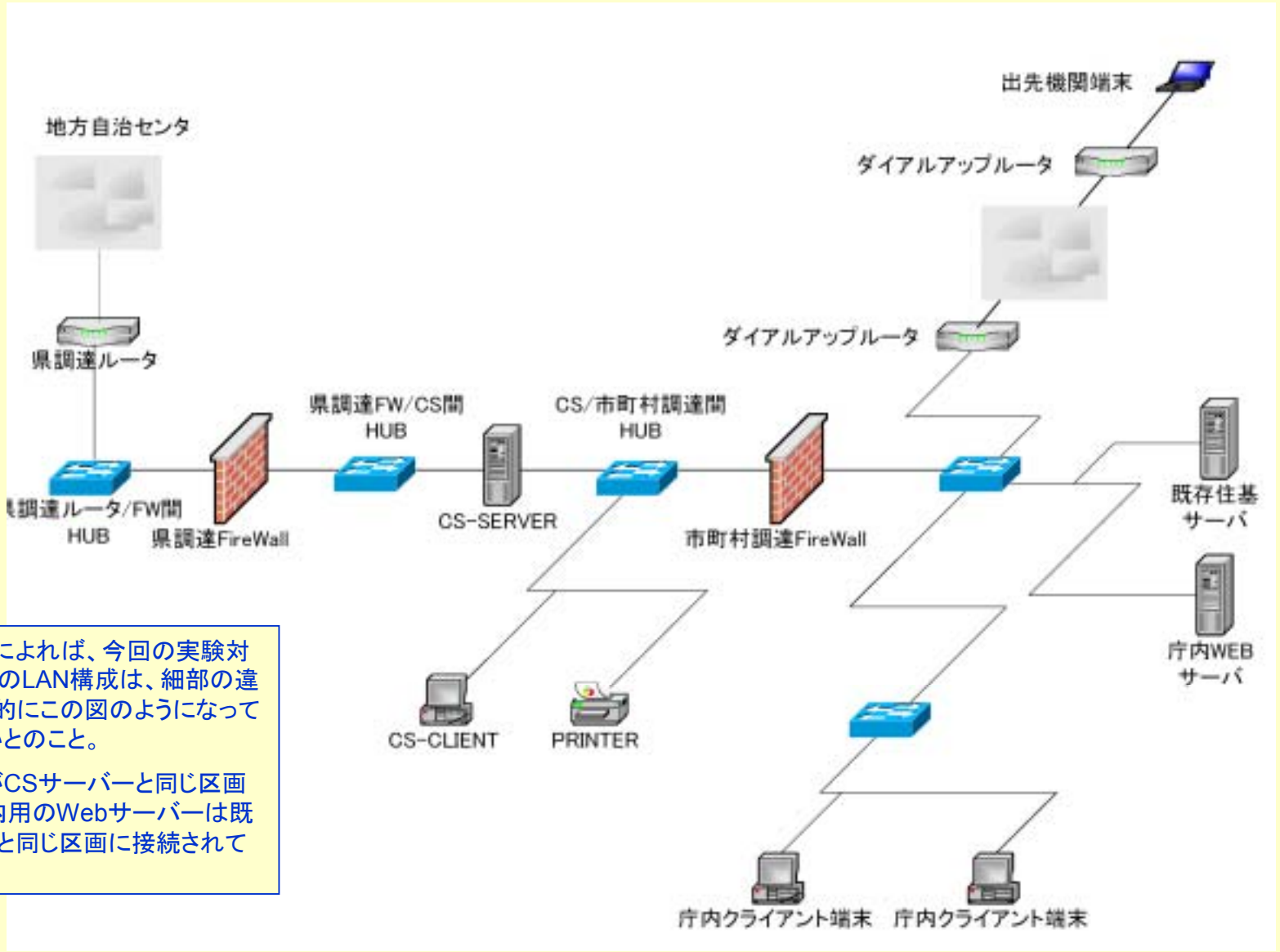
  ダイヤルアップルーターは発信機能と着信機能の両方を持っているため、セキュリティ設定を確実にしないと、想定しなかった相手からの情報を無差別に着信してLANに接続してしまう場合がある（侵入を受けやすい）。これを防止する一般的な手法として、「コールバック」がよく使われている。着信して相手を確認したら一度電話を切り、着信側から改めて発信側の（あらかじめ登録されていた）電話番号を呼び出して接続し、通信を開始する方式。自治体で使われているダイヤルアップ・ルーターでは、このコールバック方式の利用が徹底していない場合があるといわれている。

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。

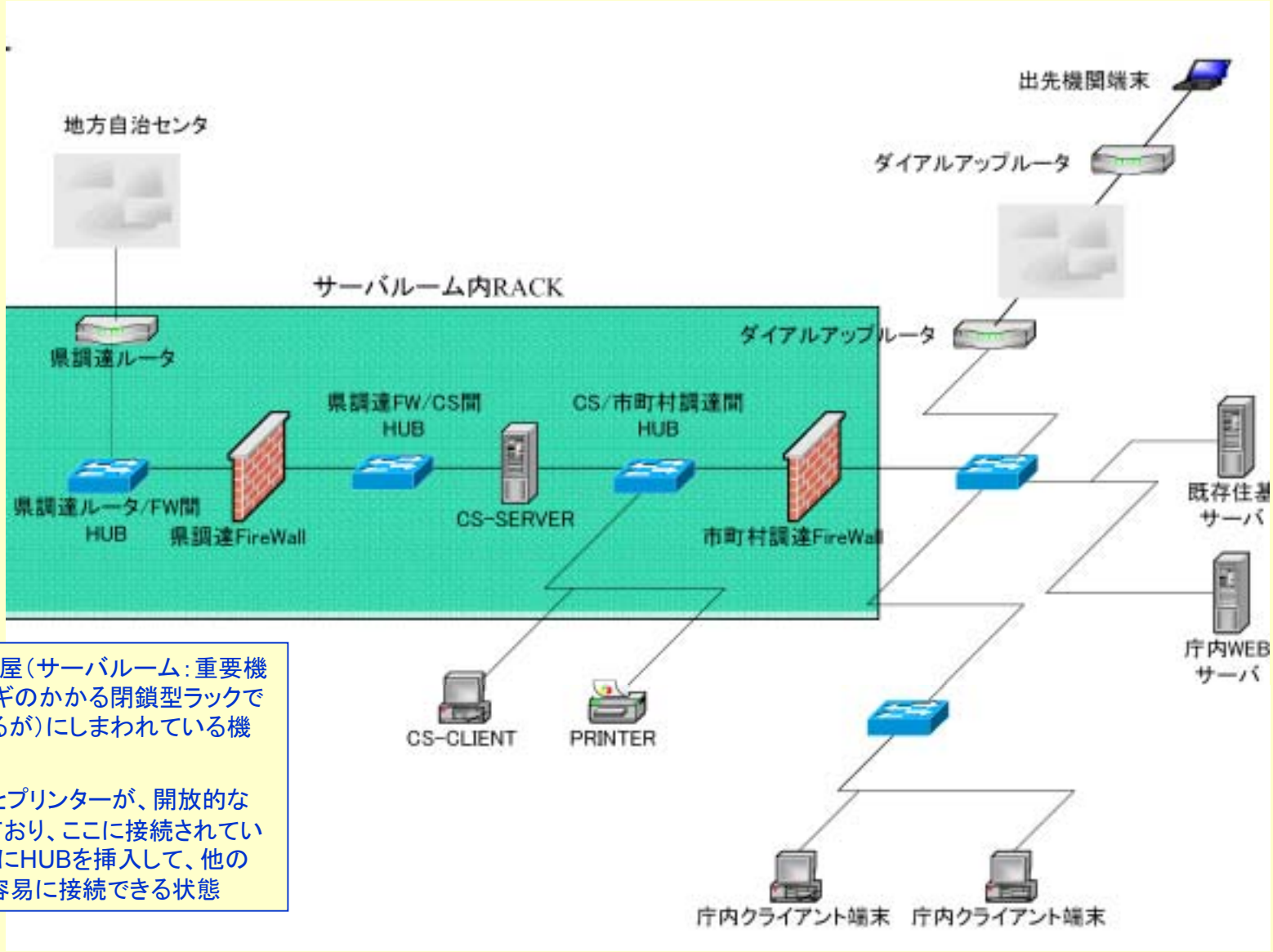
ネットワーク図1（吉田さん配布資料）



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。

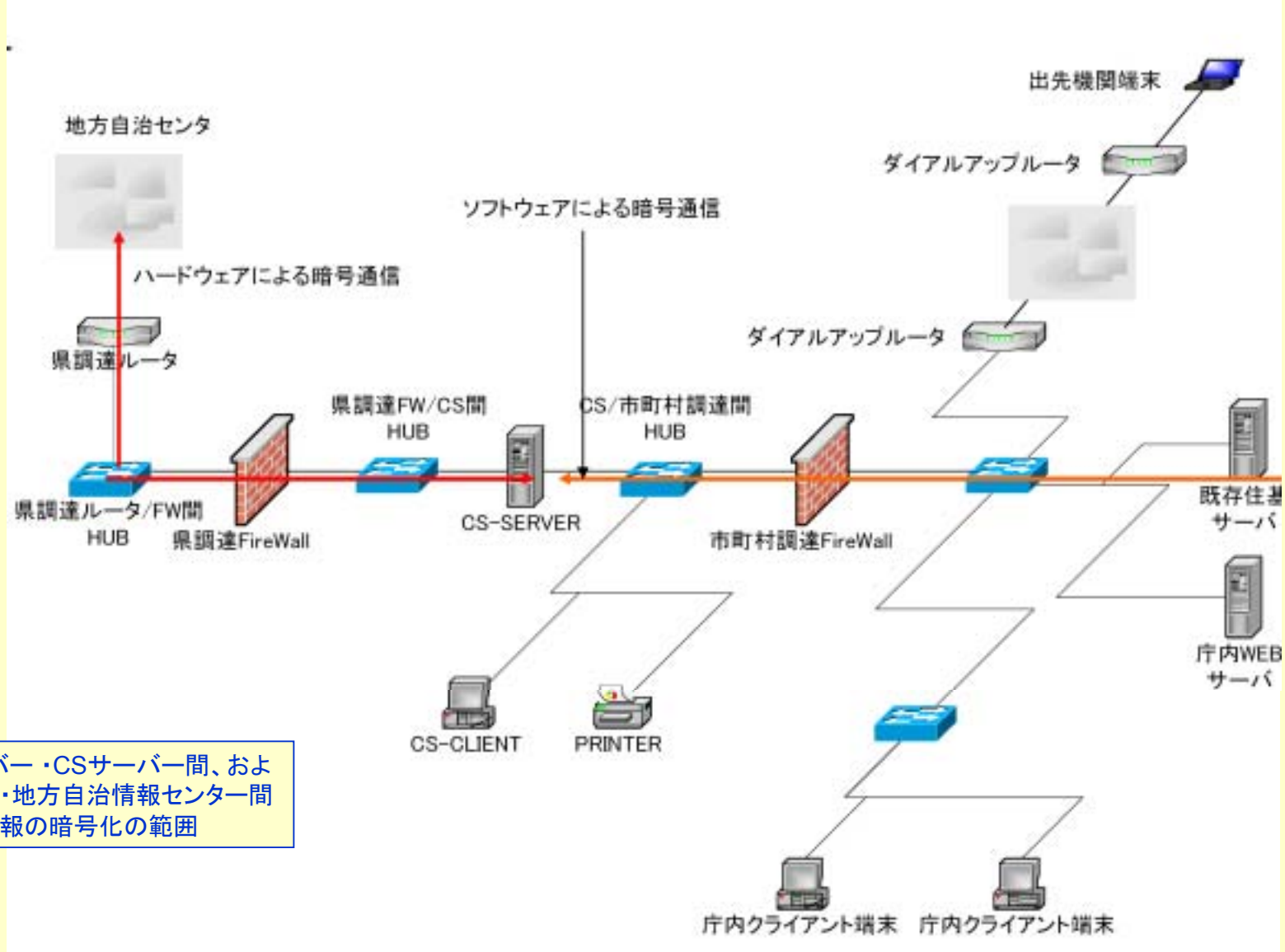
ネットワーク図2（吉田さん配布資料）



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。

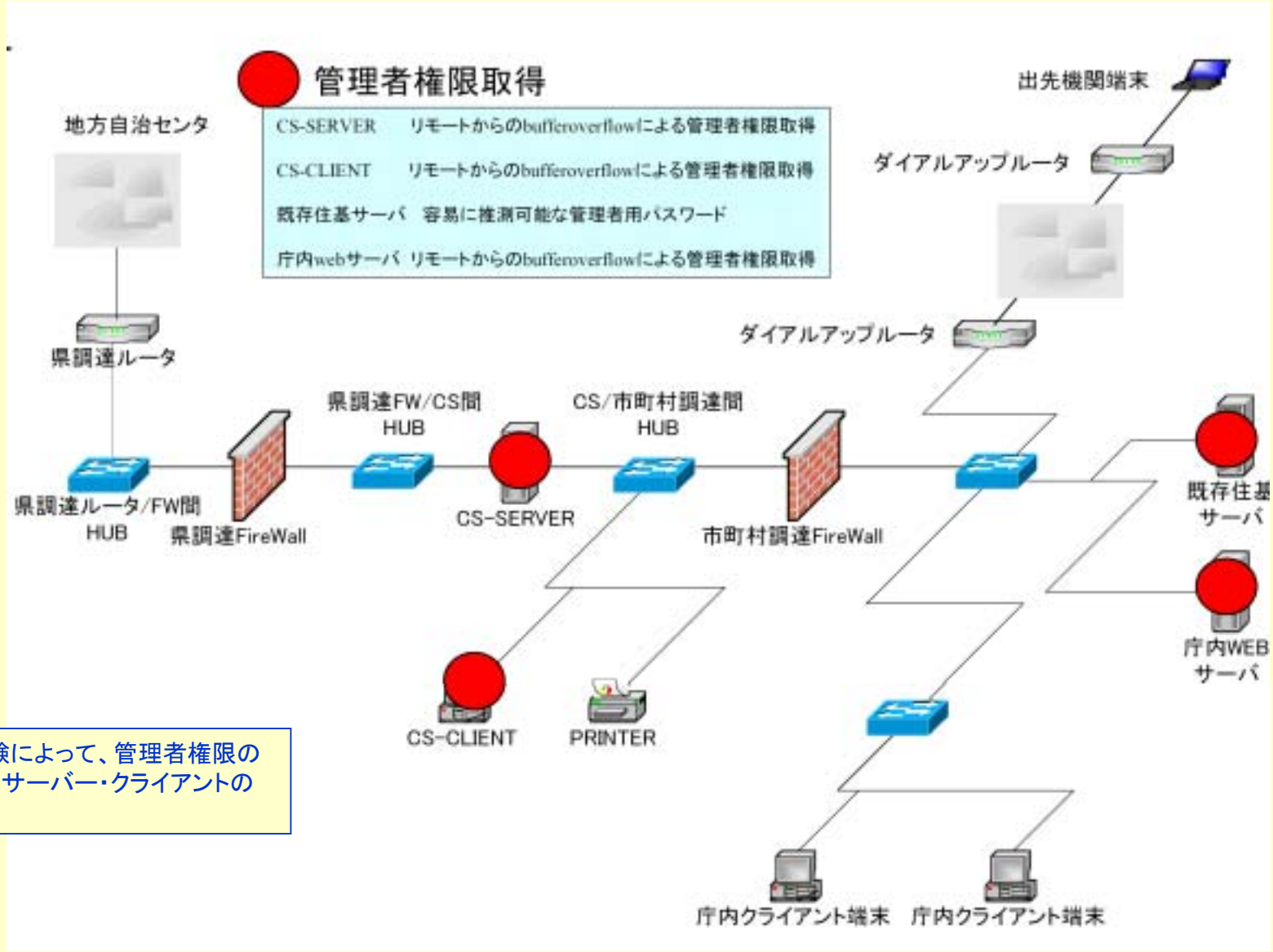
CSクライアントとプリンターが、開放的な場所に置かれており、ここに接続されているLANケーブルにHUBを挿入して、他のパソコンなどを容易に接続できる状態

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