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

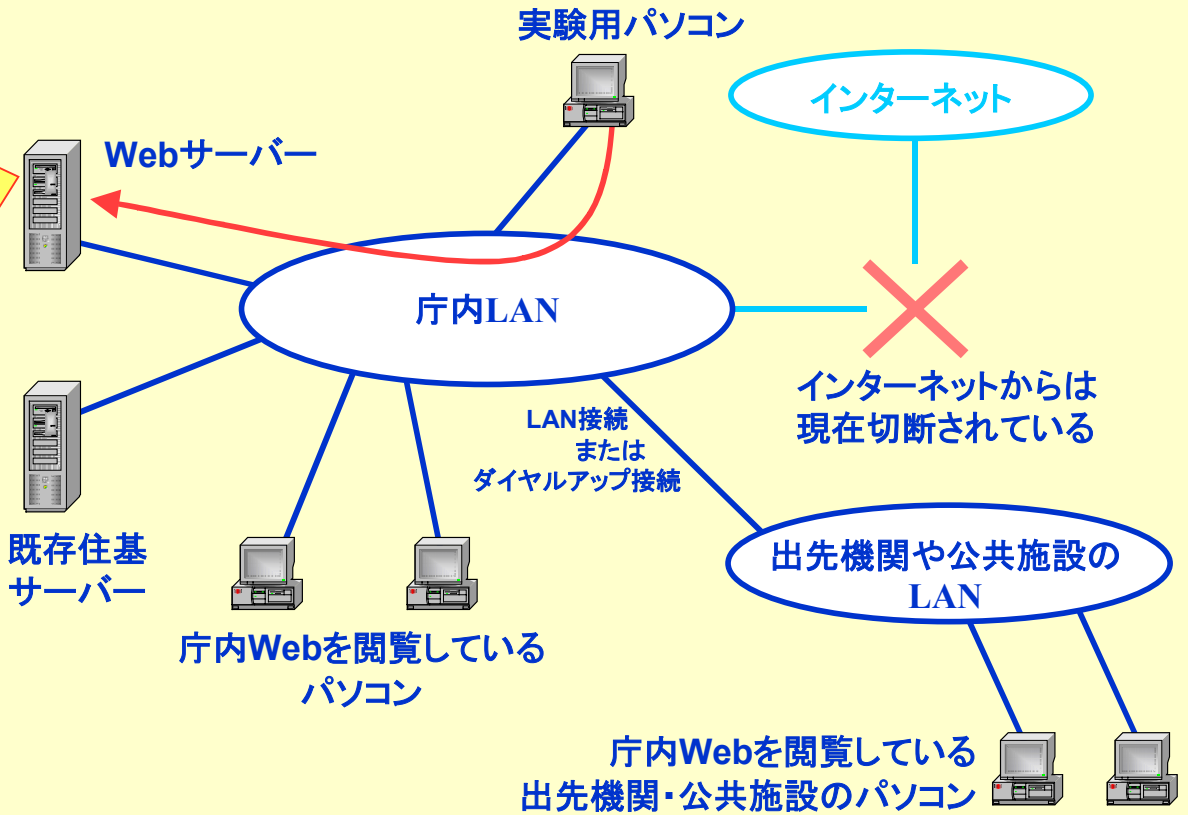
実験用パソコンによってWebサーバーの管理者権限を獲得し、Webサーバーを自由に操作することができた

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

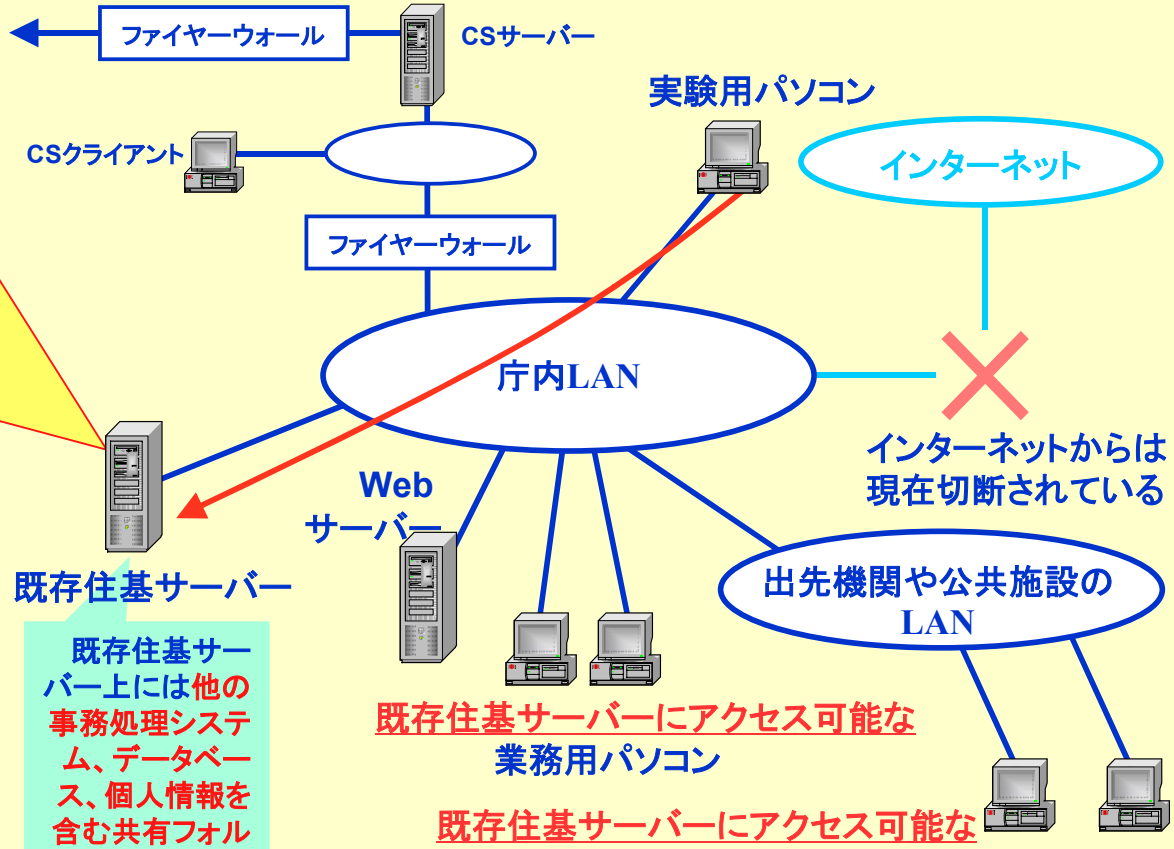
実験用パソコンによって既存住基サーバーの管理者権限・データベース等のID・パスワードを獲得できた。サーバーを自由に操作し、サーバー上の各種の個人情報を参照し、また個人情報が書換・削除可能であることを確認した

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）

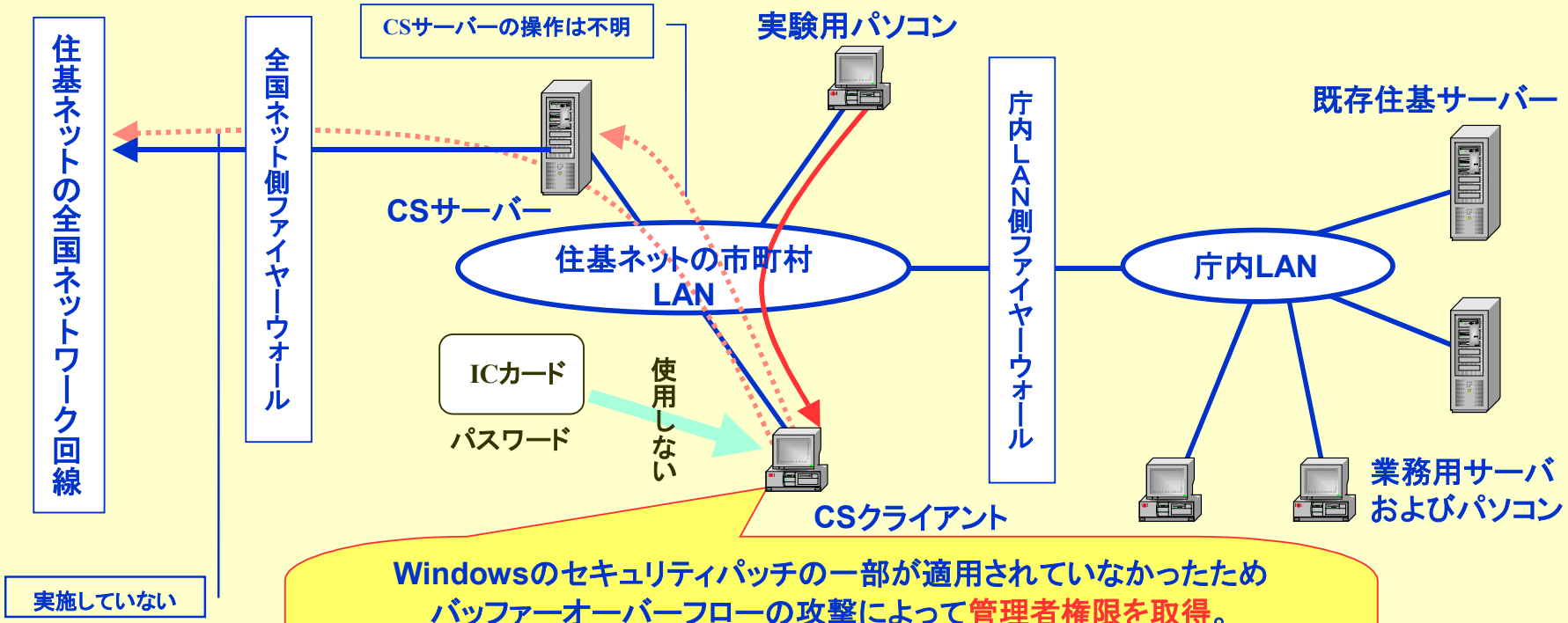
コメント：Windows2000サーバーを使用しており、公開されているセキュリティパッチの一部が適用されていなかったため、バッファーオーバーフロー攻撃が有効に実行できた

＊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

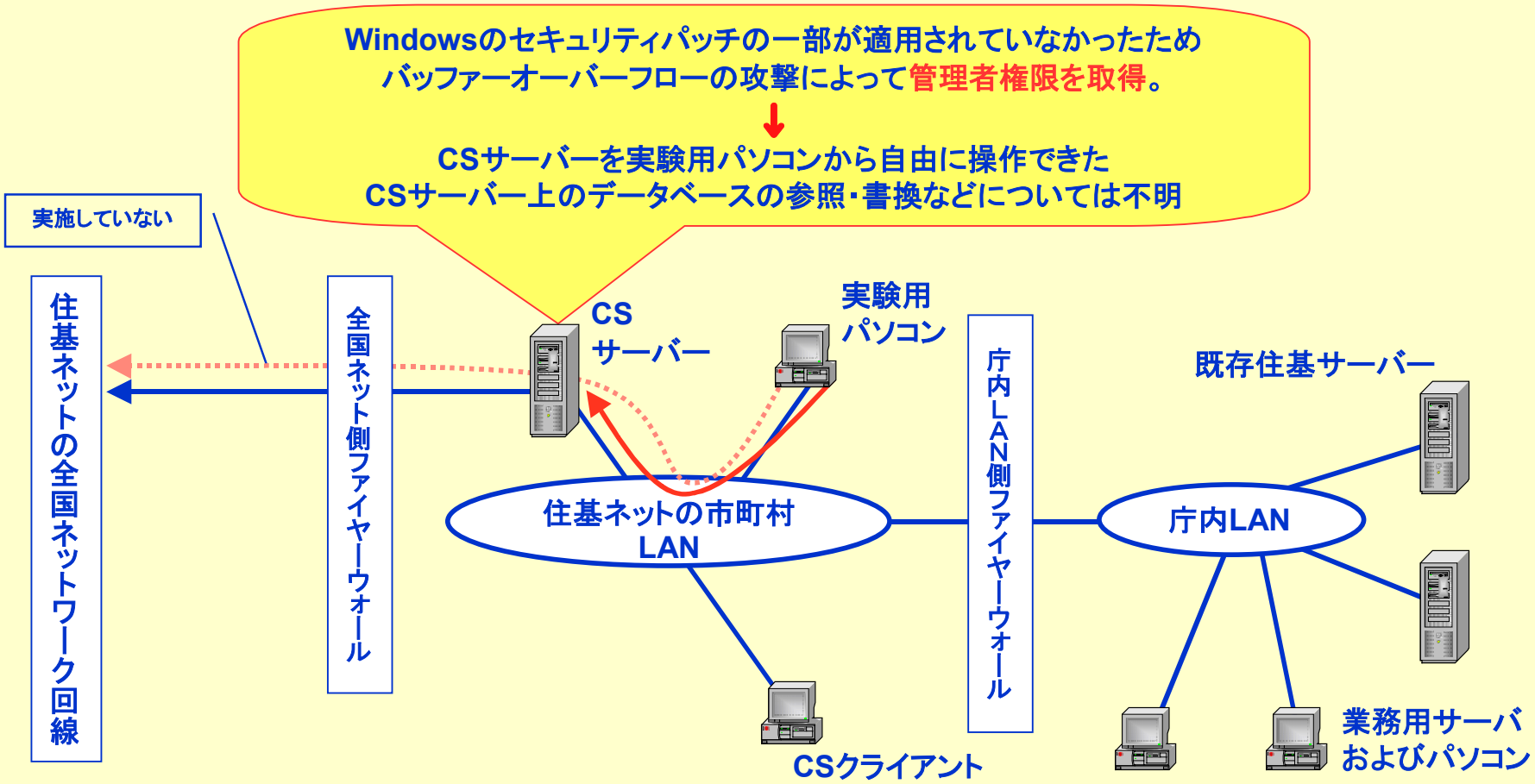
実験の方法：庁内LANとはファイヤーウォールで区切られたCSサーバー側のLAN上に、実験用パソコンを接続して、CSサーバーの管理者権限が取得できるか試験した。（CSサーバー上の本人確認情報データベースに対する試験については不明）。

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）

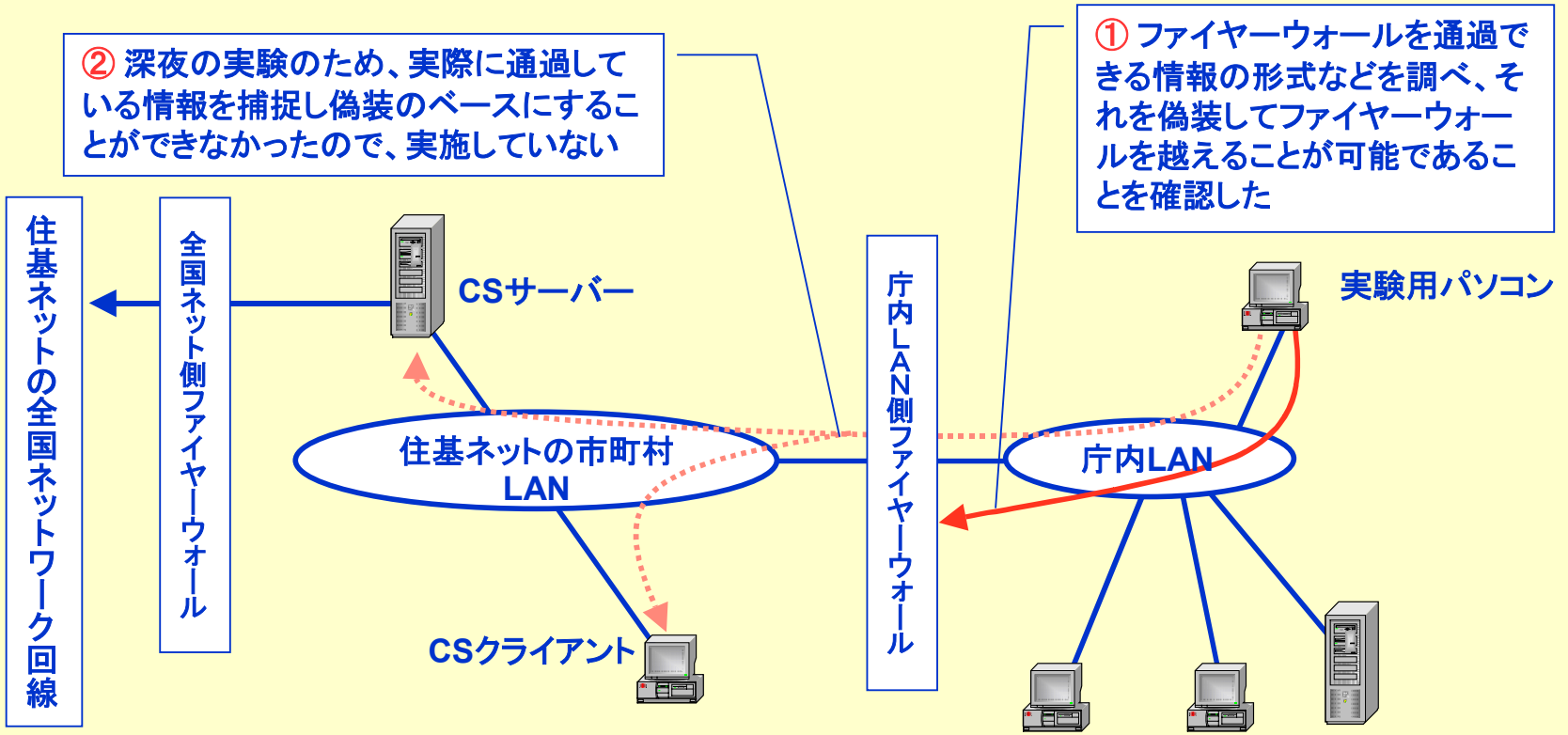
実験の方法：庁内LANに接続した実験用パソコンから、ファイヤーウォールを通過して不正情報を送りCSサーバーまたはCSクライアントに不正に接続できるかを調べた

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