# 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）

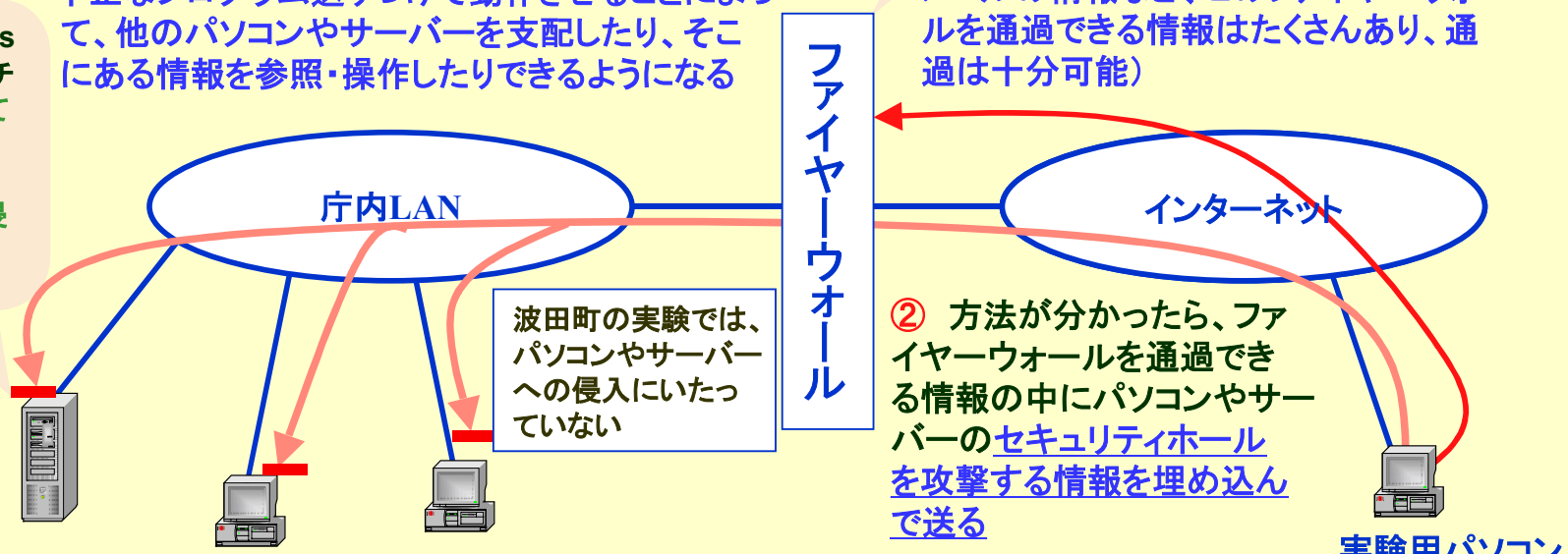
波田町の実験では、インターネットに接続している庁内LAN上のパソコンやサーバーに、セキュリティホールを見つけることができなかったため、庁内LAN上のサーバーやパソコンへの侵入にいたっていない

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）

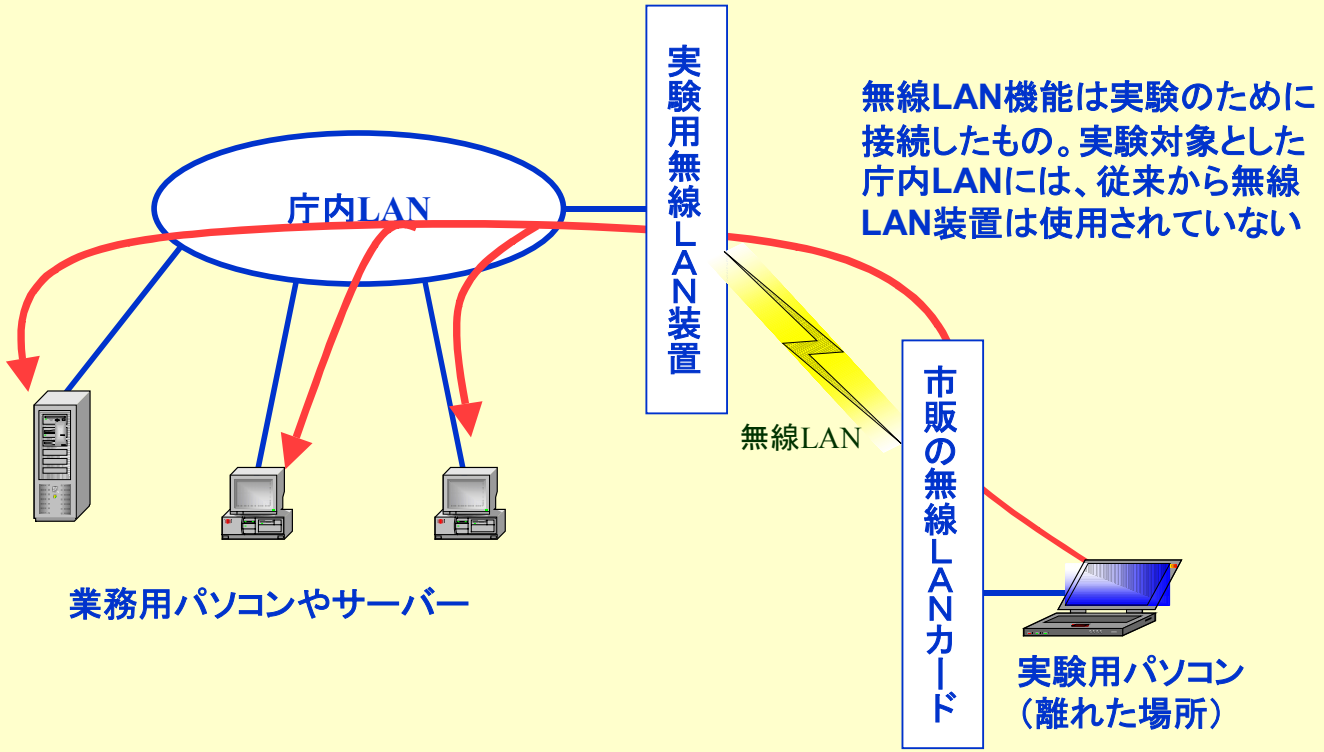
結果：実験用の無線LAN装置を庁内LANに接続して容易に動作させることができた。離れた場所にある実験用パソコンから、庁内LAN上の情報や機能を、正規職員が使っているパソコンと同様に利用することができた）

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

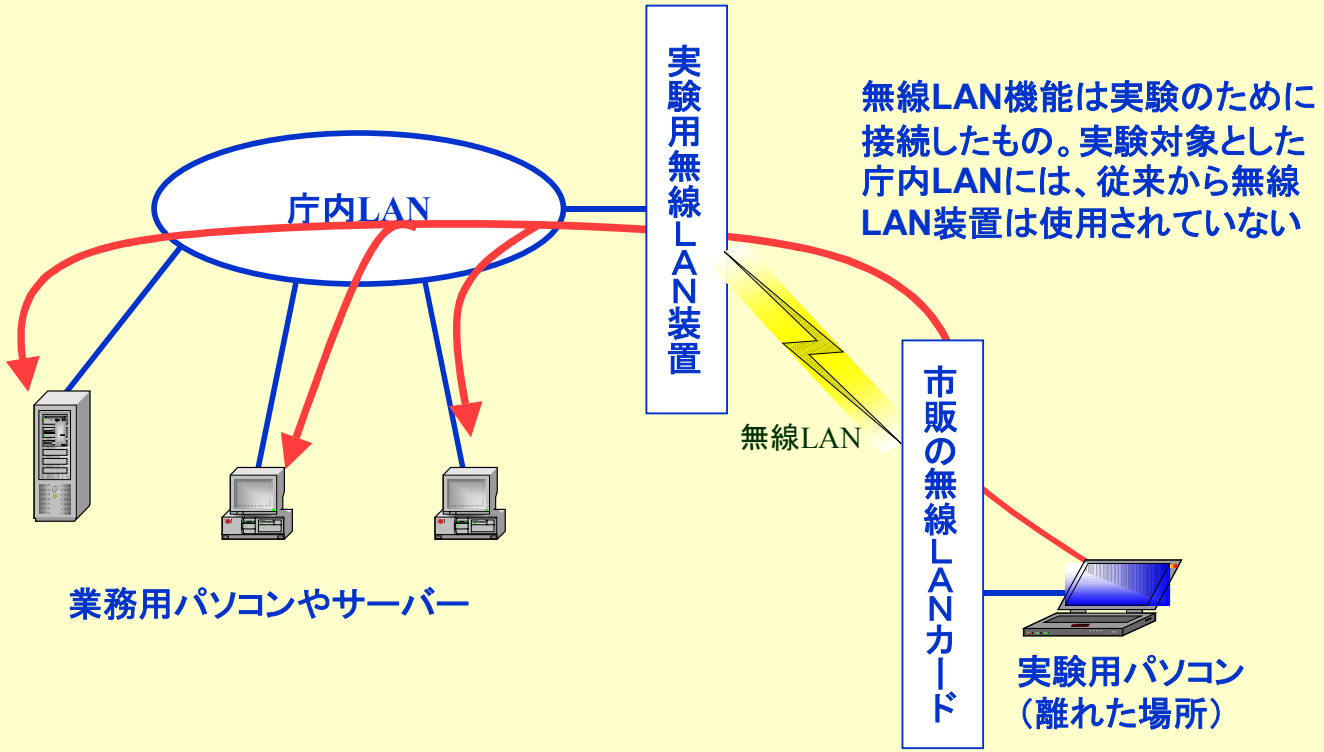
庁内LANに、市販の家庭用無線LAN装置を接続したら容易に動作させることができた。この状態で、離れた場所から家庭用無線LANカードを装着した実験用パソコンで庁内LANに接続でき、本来の業務用パソコンと同じように操作ができた




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）