長野県侵入実験速報から指摘できる
住基ネットの脆弱性

第1.2版

2004.1.17 Ver.1.0

2005.4.14 Ver.1.2

西邑　亨

はじめに

このレポートは、別途作成・公開したレポート「長野県侵入実験速報の概要と整理」（第2.1版）にもとづいて、長野県侵入実験速報から指摘可能な「住基ネットの脆弱性」について検討したものです。あわせて、これらの脆弱性を利用した場合、どのような条件が満たされれば個人情報の不正な参照・操作・利用が可能になるかを、比較的容易に想定できるいくつかのシナリオにもとづいて検討しています。

想定されたシナリオは、一般的な市町村の庁内LANおよび住基ネットの市町村サブシステム、都道府県ネットワーク、全国ネットワークを想定対象とするものです。したがって、シナリオ検討の内容は、長野県侵入実験における実験環境の範囲を超えている場合があります。

本レポートでは、侵入実験速報の内容を詳細に引用していません。必要な場合は上記「長野県侵入実験速報の概要と整理」（第2.1版）およびその1次資料である「長野県侵入実験速報」（長野県本人確認情報保護審議会のホームページで公開されている資料類）を参照してください。

ここで示した住基ネットとその周辺システムの脆弱性が、現実の社会やそこで暮らしている個人にとって、どの程度の脅威であるかを定量的に評価することは、レポーターの能力（情報通信技術の情報に接する機会は多いが、技術的な専門訓練を受けたことがない非専門家の能力）を超えています。ここで検討の対象とした脅威は、原則として「特定の条件を前提とすれば、論理的にあり得る」こと（定性的な評価）」として指摘しているものです。

したがって、本レポートで示される脅威のシナリオは、必ずしも脅威度の大きなシナリオを例示しているわけでもありません。また、長野県侵入実験速報から想定できるすべてのケースを網羅するものでもありません。

なお、シナリオ想定にあたって、技術的な脆弱性にとくに注目したため、セキュリティ確保を目的として制定されているシステム運用上の規則・規準・制度などは前提としていないことも指摘しておきます。この種の規則・制度等は、その絶対的な効果が担保されているわけではないと考えるのが、セキュリティ対策を実施する上での前提です。制度の絶対的な効果が担保されるなら、セキュリティ対策の大部分は必要がなくなりますが、そのように考えることは現実的ではありません。

もくじ

1. 速報から指摘可能な住基ネットの脆弱点

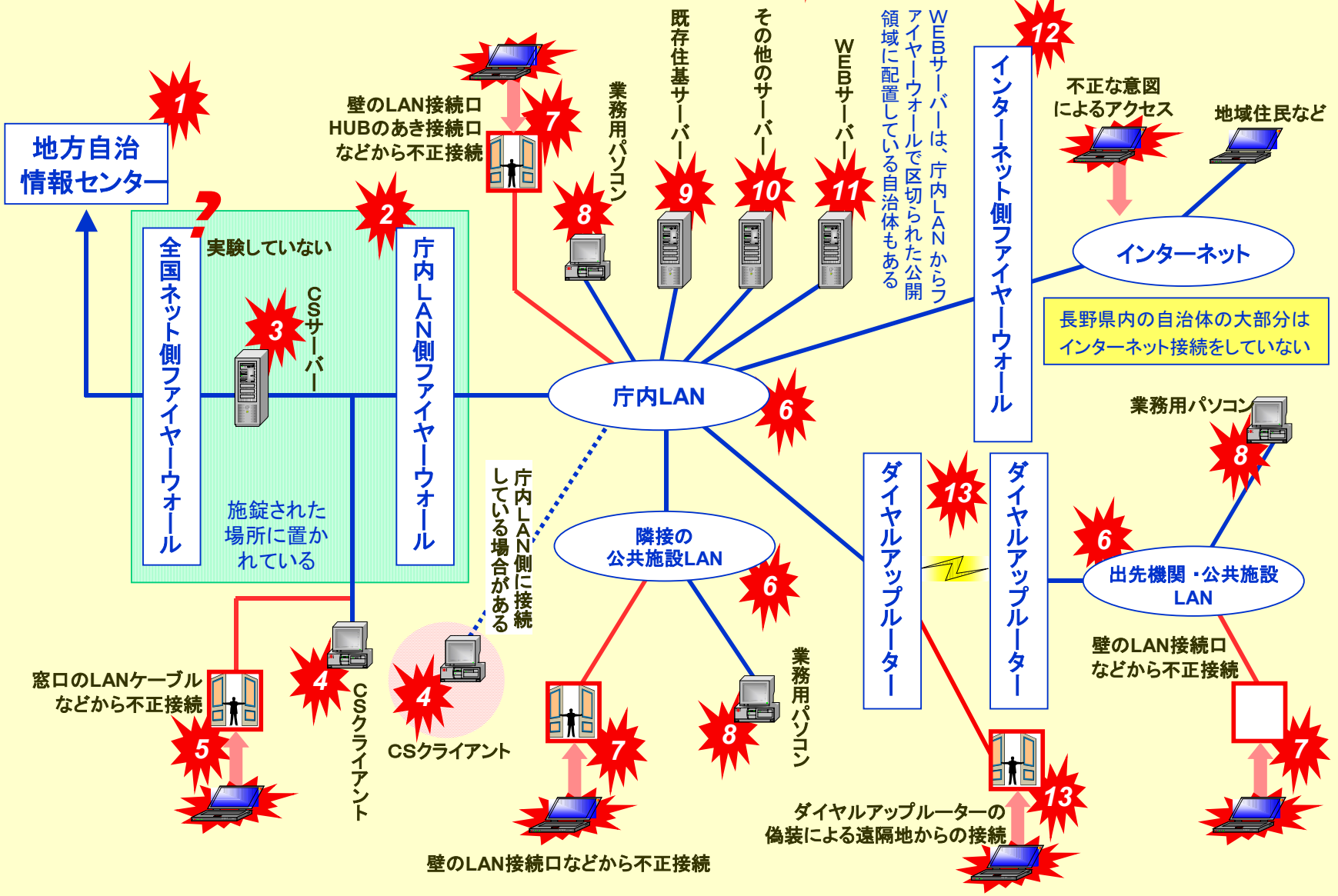
速報の結果を、住基ネット、および全国の市町村の多様なLANの状況を考慮して適用しています。
したがって以下は、長野県の速報結果そのものではなく、より一般化された可能性を示す内容になっています。

*

ここで指摘する「住基ネットの脆弱点」は、すべての自治体が一律に持っているものではありません。人口規模（予算規模）の大きな自治体は、インターネットに接続した「公開系庁内LAN」と、より高いセキュリティを確保するためにインターネットとは接続していない「閉鎖系庁内LAN」の2系またはそれ以上の庁内LANを、分離運用している場合も少なくありません。
一方では、今回実験対象とされた長野県波田町のように、人口規模（予算規模）がそれほど大きいとはいえない自治体でも、高いセキュリティレベルを確保している例はあります。

以下の指摘は、長野県の侵入実験が明らかにした脆弱点が、全国の一定範囲の自治体で共通しているものと推定しています。また、インターネットと（ファイヤーウォールを介した）庁内LANの接続が行われていることを前提として説明図などは作成されています。

速報から指摘可能な住基ネットの脆弱点 0 （脆弱点の詳細は次ページ以降を参照）



Windowsのセキュリティパッチの適用についての注

【 下諏訪町・阿智村のセキュリティパッチ適用状況 】 長野県の侵入実験が実施された03年９月２２日から１０月１日（1次実験）には、Windowsのセキュリティパッチの適用が迅速に行われる体制が確立されていたと判断できる資料はありません。従って、庁内LANの諸システムとは別に、総務省・地方自治情報センターからの指示に基づいてセキュリティパッチの適用が行われていたとしても、既知のセキュリティホールがCSサーバー・CSクライアントに存在していることは、十分予想されたことです。

【 総務省のパッチ適用の迅速化 】 総務省・地方自治情報センターが東京・品川区で実施した侵入実験（10月10日から12日）の時期には、セキュリティパッチの公開後迅速にパッチの適用が行われている形跡があります。総務省の報告書には「④セキュリティパッチについて、動作確認を迅速に実施し、引き続き早期の適用に努める」（4ページ）と記載されています。品川区でCSクライアントへの攻撃が成功しなかったのは、実験の直前に公開されたセキュリティパッチまでが、総務省・地方自治情報センターの指示に基づいて適用された後に実験が行われたと考えざるを得ません（従来はパッチの公開から数か月以上、パッチ適用が遅れるのは常態でした。03年8月のMS-ブラスターウイルスのCSクライアントへの感染を受けて、このウイルスを防御するパッチについては1か月程度で動作確認がされたことが確認されていますが、それでも1か月かかっていました）。

この「パッチの早期適用」という新しい方針が、動作確認と全国での適用完了までにどれだけの期間を要する体制であるかは不明ですが、CSクライアントにMSブラスターウイルスが感染した事実に衝撃を受けて、地方自治情報センター内にセキュリティパッチ動作確認の体制が創設されたものと思われます。

【 セキュリティパッチ公開の間隔が長期化された問題 】マイクロソフト社は、それまでセキュリティ情報および対応するパッチ公開の迅速な随時実施の方針を変更して、03年10月以降は1か月に１回まとめて公開すると発表しました。このことは、住基ネットが使用しているマイクロソフト社のソフトウェア製品のセキュリティホールが発見された場合、最大で1か月間程度対応が遅れることを意味しています。従来、多くのセキュリティホールは社外で発見され、マイクロソフト社に通告されていました。つまり、未対応のセキュリティホールは、一部のネットワーク技術者などの間では暫定的な防御対応を実施するために情報が流布されながら、根本的な対策が一般に提供されるまでに最大1か月程度（1か月を越える場合も当然予想される）かかることを意味しています。

総務省・地方自治情報センターが「ほとんど即時適用」の方針を採用していたとしても、その迅速性は十分生かされなくなっているともいえる状態で、「事実上既知のセキュリティホール」は住基ネットの中で長期にわたって放置されることになります。

【 波田町の場合 】 なお、波田町でのインターネットからの侵入実験が「侵入にいたらなかった」のは、波田町が独自の判断でセキュリティパッチを適用していたWebサーバーなどにセキュリティホールが発見できなかったためです。Webサーバーなどへのセキュリティパッチの適用は、総務省・地方自治情報センターの指示とはまったく無関係です。また波田町ではCSサーバー・CSクライアントへの攻撃実験は行われていません。

1 地方自治情報センターによる監視の脆弱点

「24時間監視」への過剰な依存

- センターが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。
- センターは、CSサーバー・CSクライアントへの攻撃、管理者権限取得を検知できない
- センターは、庁内LAN側ファイヤーウォールの通過条件を調べるための攻撃を検知できない

2 庁内LAN側ファイヤーウォールの脆弱点

「ファイヤーウォール」への過剰な依存

- このファイヤーウォールを通過する具体的な方法が確認されている
- このファイヤーウォールに「保守用裏口」がある可能性が指摘されている。この場合、ファイヤーウォールの設定を変更することで、ファイヤーウォール自体を無効化できる可能性がある。
- このファイヤーウォールへの攻撃を地方自治情報センターは検知できない

3 CSサーバーの脆弱点

- Windows2000サーバーのセキュリティ・ホール対策が不十分な可能性が高く、その場合管理者権限が取得できる（OSレベルでの自由な操作ができるようになる）。
- CSサーバーへの攻撃を地方自治情報センターの監視は検知できない。

4 CSクライアントの脆弱点

- Windows2000のセキュリティ・ホール対策が不十分な可能性が高く、その場合管理者権限が取得できる（OSレベルでの自由な操作ができるようになる）。
- CSクライアントへの攻撃を地方自治情報センターの監視は検知できない。
- クライアント上で住基ネット業務アプリケーションを操作して、住基ネット上の本人確認情報を検索・閲覧できる可能性がある。

- 多くの自治体などに見られるようにCSクライアントを庁内LAN側に接続している場合は、庁内LAN上などからより容易にCSクライアントを攻撃できるため、危険性ははるかに大きい。

5 全国ネット側／庁内LAN側両ファイヤーウォール間のLAN・配線の脆弱点

- CSクライアントやプリンターに対するLAN配線にHUB等を挿入して、侵入用のパソコンなどを容易に接続できる（施錠した場所にはいる必要がない）。
- IPアドレスが自動割り当てになっている可能性が高く、その場合はLAN内へのアクセスがきわめて容易にできる。
- 窓口業務用のCSクライアントの背面に接続されているUSBの配線が自由に抜き差しできるため、ここに何らかの装置を接続することが可能になっている。

6 本庁・出先機関・公共施設のLANの脆弱点

- 公開WEBサーバーが、内部業務用サーバーと同じLAN上に配置されている自治体が多い（公開LANと内部事務LANが区別されていないため、攻撃を受けやすい）
- IPアドレスが自動割り当てになっている可能性が高く、その場合はLAN内へのアクセスがきわめて容易にできる。

7 本庁・出先機関・公共施設のLAN配線の脆弱点

- 卓上などのHUBにあき接続口がある（パソコン等の不正接続が容易）
- 壁などにLAN接続口が設置されている（パソコン等の不正接続が容易）
- パソコン、プリンターのLAN接続などが容易に抜き差しできる（HUBなどを挿入してパソコン等を容易に接続できる）
- 無線LAN局を接続した場合も容易に動作し、無線LANカードを装着したパソコンから庁内LANにアクセスできる

8 本庁・出先機関・公共施設の業務用パソコンの脆弱点

- 既存事務処理システムのサーバーへのアクセス制限がされていない可能性が高い。
- OSのセキュリティ・ホール対策が不十分な可能性が高く、その場合管理者権限が取得できる（OSレベルでの自由な操作ができるようになる）。

9 既存住基サーバーの脆弱点

- Windows2000サーバー のセキュリティ・ホール対策が不十分な可能性が高く、その場合管理者権限が取得できる（OSレベルでの自由な操作ができるようになる）。
- 住基データベースのパスワードが容易に推定、取得できる可能性が高い。この場合住基台帳の内容を自由に閲覧・修正・削除できる。
- 業務用パソコンからのアクセス制限がされていない可能性が高い。

10 その他の事務処理システム用サーバーの脆弱点

＊実験対象町村では、これらのサーバーは既存住基サーバーと同じハードウェア上で動作している

- OSのセキュリティ・ホール対策が不十分な可能性が高く、その場合管理者権限が取得できる（OSレベルでの自由な操作ができるようになる）。
- データベースのパスワードが容易に推測、取得できる可能性が高く、この場合、データベースの内容を自由に閲覧・修正・削除できる。
- 業務用パソコンからアクセス可能な場所に多くの共有フォルダーが設定されている場合がある。パスワードは設定されていないか、容易に推定、取得できる可能性が高く、この場合これらの情報を自由に閲覧・修正・削除できる。

11 Webサーバーの脆弱点

- Windows2000サーバーのセキュリティ・ホール対策が不十分な可能性が高く、その場合管理者権限が取得できる（OSレベルでの自由な操作ができるようになる）。

  *インターネット接続がされていた場合、容易にインターネット上からWebサーバーの管理者権限を取得でき、他のサーバー等を攻撃するための拠点とすることができる。

12 インターネット側ファイヤーウォールの脆弱点

ファイヤーウォールへの過剰な依存

- 庁内LANが事務処理用LANと公開LANとに区分されていないため、このファイヤーウォールの効果は過大に期待することができない（長野県内の自治体の大部分はインターネット接続をしていないためこの問題は防御されているが ）。
- 庁内LAN側ファイヤーウォールと同様「保守用裏口」がある場合は、ファイヤーウォールの管理者権限が取得できる可能性がある（ファイヤーウォールを無効化できる可能性がある）。

13 ダイヤルアップルーターの脆弱点

- 出先機関等のダイヤルアップルーターを偽装して遠隔地から庁内LANに接続される可能性がある。