Wondowsのセキュリティホールを利用した個人情報漏洩の手法

住基ネットの
セキュリティとプライバシーの問題について
（対多摩市行政不服審査請求のための意見陳述）

補佐人
西邑　亨

2003年 9月 10日（東京都に提出）

MSブラスターウイルス感染が明らかにした個人情報漏洩ルートの存在

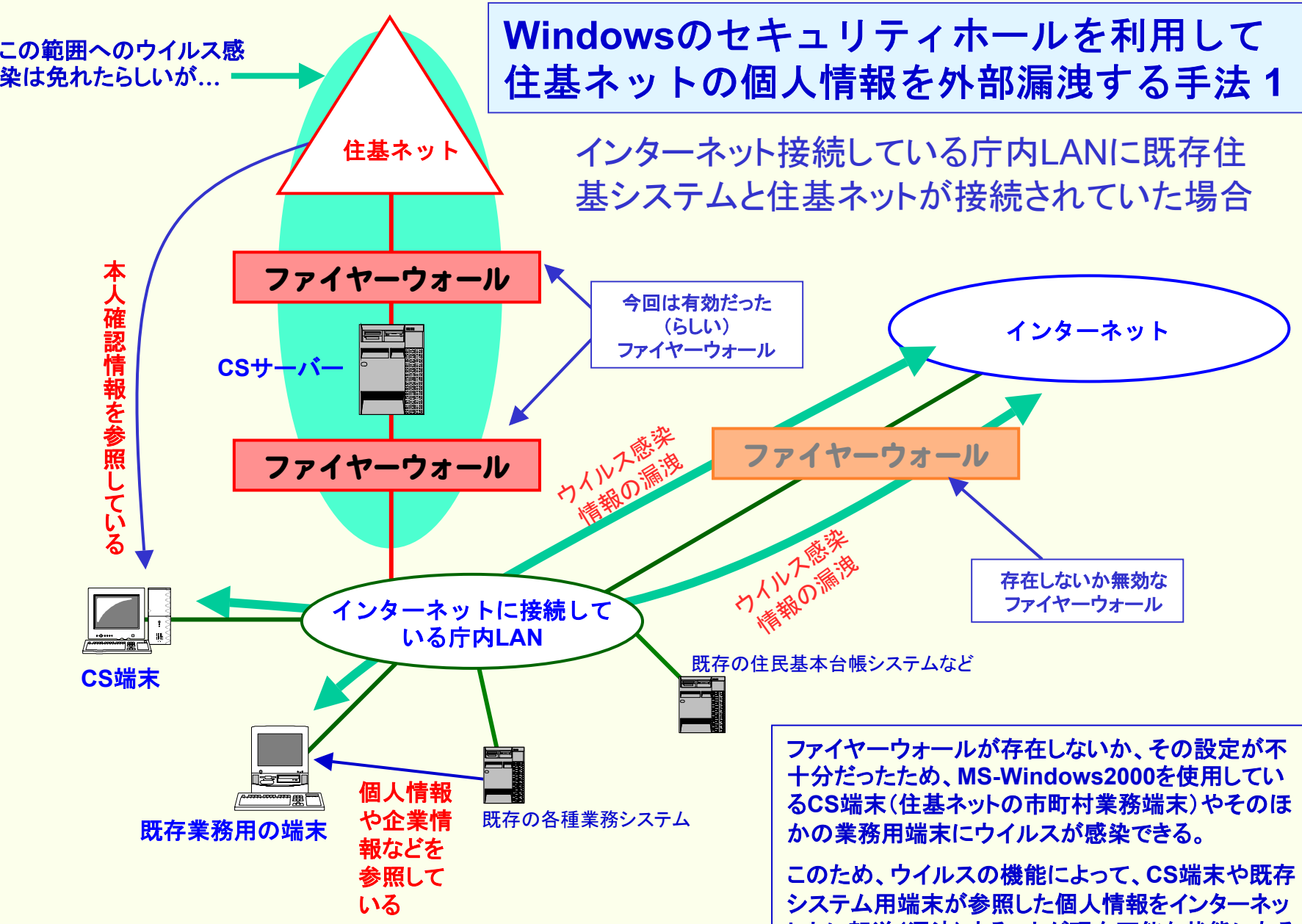
- 住基ネットのCSサーバー・業務端末に採用されたMS-Windows2000（MS-Windows NT系OS）は、技術の特性から見てセキュリティ的に脆弱であり、潜在的にセキュリティーホールが存在しうることは、以前から指摘されていた
- MS-Windows2000のセキュリティホールは、過去において年間数件が新たに発見されている
- MSブラスターウイルスが利用したMS-Windows2000のセキュリティホールは、事件の1か月前にMicrosoft社のセキュリティパッチが配布されていたが、住基ネットでは適用されていなかった

したがって、以下に述べる「Windowsのセキュリティホールを利用して　住基ネットの個人情報を外部漏洩する手法 」の存在は、住基ネットの1次稼働時点ですでに技術的には可能であり、1年後の2次稼働以後も本質的な問題は何ら変わっていない。

今回の自治体・政府機関のLANに対するMSブラスターウイルス感染の経過において明らかとされたことは、今回問題となったWindowsNT系OS（基本ソフト）のセキュリティホールを利用する個人情報窃取の具体的な手法が、2003年9月10日現在も「住基ネット」全体に存在しているという事実である。

Windowsのセキュリティホールを利用して住基ネットの個人情報を外部漏洩する手法１

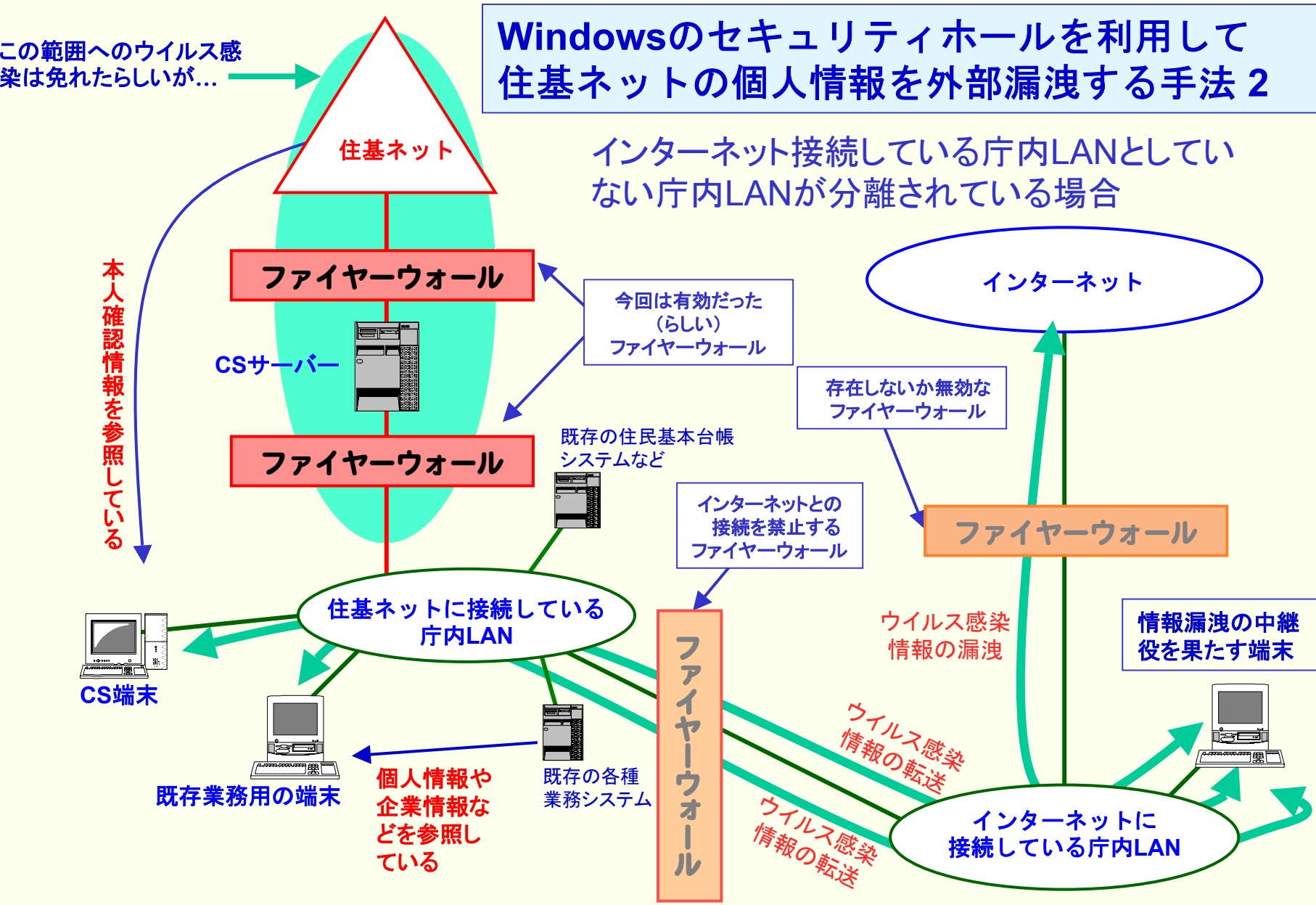
インターネット接続している庁内LANに既存住基システムと住基ネットが接続されていた場合



ファイヤーウォールが存在しないか、その設定が不十分だったため、MS-Windows2000を使用しているCS端末（住基ネットの市町村業務端末）やそのほかの業務用端末にウイルスが感染できる。

このため、ウイルスの機能によって、CS端末や既存システム用端末が参照した個人情報をインターネット上に転送（漏洩）することが現在可能な状態にある

Windowsのセキュリティホールを利用して住基ネットの個人情報を外部漏洩する手法 2



インターネットに接続している庁内LAN上のパソコンにウイルスが感染し、これを個人情報漏洩の中継ポイントとして利用すれば、住基ネットがインターネットから分離されていても、CS端末や既存の業務用端末の個人情報を外部漏洩可能な状態

住基ネットのセキュリティ的な問題点
（MSブラスターウイルス事件が明らかにした現状）

- CSサーバー・都道府県サーバー・全国サーバーを他から分離しているファイヤーウォールの設定が十分であったとしても、本人確認情報を参照するクライアント（CS端末）がMS-WindowsNT系OSを採用していれば、前述のような個人情報漏洩ルートは利用可能である
- この手法で漏洩する（窃取可能な）情報は、当該自治体住民の本人確認情報だけでなく、CS端末が参照した他自治体の本人確認情報、および当該自治体のWindowsNT系OSを使用した業務端末等が参照するすべての個人情報や企業情報・行政情報
- 自治体や国の機関のファイヤーウォールは、必要なポイントに設置されていないか、設置されていてもその設定がきわめて不十分な状態にあることが、今回の事件で明らかになった
- 住基ネットのCSサーバー・CS端末のWindowsセキュリティパッチは、1か月前に一般配布されていたにも係わらず、知られている限りでは現在もまだ適用されておらず、現時点で住基ネット上の個人情報を窃取する手法は周知された状態にある
- MS-WindowsNT系OSのセキュリティホールは、未知のものが多数存在していると考える必要があるとされており、現在のセキュリティパッチが適用されても十分な安全が確保されるわけではない

結論（１） セキュリティ問題について

（1）現実に、セキュリティ上の問題は多数存在している

住基ネットは技術的な視点から見て、多くのセキュリティ上の問題点を抱えている。その多くは、狭い意味での「住基ネット」（ファイヤーウォールによって分離されているCSサーバー・都道府県サーバー・全国サーバーとそれらを結ぶネットワーク回線の範囲）ではなく、ファイヤーウォールによって「接続」されている自治体や国のLAN／WANの中に存在している。

自治体や国のLAN／WANを含む「住基ネット」全体のセキュリティ構築が十分でなければ、「個人情報（本人確認情報）」は自治体・国の機関のLANなどから漏洩する。その意味で「住基ネットのセキュリティ構築」は、当初の計画段階から失敗していたことは、前述した情報漏洩ルートが現に存在していることを見ても明らかである。

（2）住基ネットの導入は決定的な準備不足であった

前述したような問題に対応する手法としては、住基ネットだけでなく庁内LAN全体におけるセキュリティパッチの早期適用・ウイルス情報の頻繁な更新・ファイヤーウォール十分な設定などの基本的な対策を徹底した上で、長野県が示したように、自治体システムにおいて住基ネットに接続する庁内LANをインターネットに接続する庁内LANと物理的に切断した上で、両方のLANの運用状況を常時監視する体制を取ることは、一定の実効性があるものと考えられる。

しかし、住基ネット導入にあたって、「基本対策」すら十分に徹底できていないのが自治体および国のネットワークシステムの実情であり、長野県提案を有効に機能させるための基礎ができているとは言えない。稼働後1年をへた時点でのこうした状況から見て、「住基ネット」の導入は、システムの運用／利用のための自治体・国の機関の能力・体制・設備の準備が決定的に不足しており、計画自体に多数の問題が存在していたといわざるを得ない。

（3）多くの自治体財政から見て、セキュリティ対策の早期実施はありえない

長野県提案にあるような自治体・国の機関の段階での情報システム全般に対する総合的セキュリティ対策は、行政事務の電子化（電子自治体／電子政府）推進において、すべての自治体に必須の対策であると考えられる。しかし、こうした対策が必要とする高額の新規支出は、自治体の財政状態の改善に逆行するものであり、現実的ではない。

したがって、「住基ネット」全体における深刻なセキュリティ状況状況の改善の見通しは、中・短期的には存在しないと言える。

結論（2） プライバシーの保障について

（1）セキュリティ確保はプライバシー保障の基礎条件のひとつであり、その条件は現状において満たされていない

住民のプライバシーを保障すべき立場にある自治体にとって、「セキュリティ確保」はプライバシー保障のための基礎的条件のひとつである。十分なセキュリティ強度を確保することによって住民のプライバシーを高いレベルで保障することは、自治体首長に対して住民基本台帳法が求めている責務のひとつである。しかしながら、前述したように、CS端末から当該自治体住民だけでなく他自治体住民の個人情報が漏洩する可能性が明らかに存在することは、住基ネットが住民のプライバシー保障のための条件のひとつを満たしてていないことを示している。

（2）セキュリティ確保はプライバシー保障の十分条件ではない

しかし、セキュリティ強度の確保は、プライバシー保障の必要条件ではあっても、それだけでは十分ではない。とくに、今回の住民基本台帳法の改正によって付番されることになった「住民票コード」（国民固有のIDコード）は、プライバシー侵害の重大なキーとなりうることは、このコードの民間での利用が住民基本台帳法によって禁じられていることによって端的に示されている。

（3）住民票コードを利用したプライバシー侵害は、適切に防御されてはいない

ところが、本人確認情報の国や自治体における利用について規定した住民基本台帳法および行政機関個人情報保護法などには、こうした危険性を持つ「住民票コード」を含む本人確認情報の取り扱いについて、プライバシー保障の視点からは何ら規定しておらず、プライバシーを侵害する可能性の極めて高い「個人情報の結合」に住民票コードを利用することは、禁止されていない。したがって、住基ネットの運用において、高いセキュリティ強度が確保され得たとしても、自治体住民のプライバシーは保障されない。

（4）多摩市長は、個人情報保護条例にもとづいて、住民の利益を確保する義務を果たすべきであった

多摩市個人情報保護条例は第3条において、市長の責務として「この条例の解釈及び運用に当たっては、市民の基本的人権を尊重し、個人情報の保護に関して必要な措置を講じなければならない」と規定している。したがって、「目的外利用及び外部提供の制限」における例外を規定した同条例第14条の2（2）「法令等の規定の適用上必要があるとき」においても、「市民の基本的人権を尊重し、…必要な措置を講じる」責務を免れるものではない。

ところが、前述のように、住民票コードを含む本人確認情報の提供のための住基ネットの運用においては、プライバシー保障はきわめて不十分な状態にあり、市長は市民の利益のために、少なくとも同14条の6が規定する外部提供先における「使用方法の制限その他の必要な制限を付」すなどの措置を検討し実施すべきであったにもかかわらず、その様なことを検討・実施したとは、本件審査請求人に対して弁明していない。

（5）以上から、多摩市長は条例に反して必要な措置をとっておらず、本件審査請求人の主張には十分な正当性があるものといえる。