

住基ネットに係る市町村ネットワークの脆弱性調査最終結果について

平成 16 年 2 月 29 日

住基ネット対応チーム

この調査は、住民基本台帳ネットワークが個人情報保護の観点から十分安全かどうかを確認するとともに、必要な対策に関する資料を得る目的で、住民基本台帳ネットワークの一部を構成している自治体のコンピュータネットワークに対して行われたものである。

なお、調査結果については、伊藤穰一氏による第三者評価を実施した。

調査を実施したのは、長野県本人確認情報保護審議会の委員である吉田柳太郎氏並びに吉田柳太郎氏を補助する目的で長野県と委託契約を締結した者 1 名及びその助手からなる調査チームである。

なお、長野県職員若干名が調査に立ち会った。

調査チームは、長野県内の 3 つの自治体のコンピュータネットワークにおいて、外部・内部のファイアウォール、DMZ 内の公開サーバ、既存住基サーバ、庁内WEBサーバ、住基ネットCS、住基ネットCS 端末等について調査を行い、いくつかの脆弱性を発見した。その主なものは次のとおりである。

- ・ パスワード設定等の問題があり、庁舎の内外から既存住基サーバや庁内WEBサーバに管理者権限でログインできたほか、データベースへのアクセス制限にも問題があり、住基コードなどの個人情報を含む重要なデータを閲覧できた。このことは、データの書き換えが可能であり、書き換えられた住民票データが住基ネットを経由して流通する可能性があることを意味している。
- ・ 住基ネットCSを含むコンピュータネットワーク上のサーバのOSが既知の脆弱性を含んだまま運用されており、一定の条件下においては、一般に入手可能なツールによる管理者権限奪取も可能であった。このことは、重要なデータの閲覧と書き換えが可能であり、書き換えられた住民票データが住基ネットを経由して流通する可能性があることを意味している。

また、住基ネットCSで得られたデータを利用してCS端末の管理者権限を奪取することが可能であった。

- ・ 既存住基サーバと CS との間に置かれた FW については、不要と思われるポートが空いている例があったほか、FW の OS のバージョンが古く、既知の脆弱性を利用した攻撃が行われる可能性が存在した。
- ・ 既存住基サーバと CS がデータ交換をする上で必要なアプリケーションに脆弱性のある関数が使われていることが類推された。

なお、DMZ 内の公開サーバの脆弱性は発見されていないが、これは調査対象の公開サーバが適切に運用されていたためであり、このことを以て運用状況の異なる自治体のコンピュータネットワークがインターネットに接続されていることの危険性は否定できない。

この調査では、脆弱性の指摘に併せて、自治体が今後取るべき対応に関する提案も行っている。その中には個々の自治体、とりわけ規模の小さな自治体では対応が難しいものも含まれているが、コンピュータシステムの共同運営などの方法により実現していくことも検討していく必要がある。

- 目次 -

1 この調査について

- 1 - 1 目的
- 1 - 2 調査方法
 - 1 - 2 - 1 概要
 - 1 - 2 - 2 内部からの侵入調査
 - 1 - 2 - 3 外部からの侵入調査
 - 1 - 2 - 4 留意した事項

2 調査概要

- 2 - 1 調査対象、調査環境、調査条件等
 - 2 - 1 - 1 調査対象
 - 2 - 1 - 1 - 1 下伊那郡阿智村
 - 2 - 1 - 1 - 2 諏訪郡下諏訪町
 - 2 - 1 - 1 - 3 東筑摩郡波田町
 - 2 - 1 - 2 調査環境
 - 2 - 1 - 2 - 1 下伊那郡阿智村
 - 2 - 1 - 2 - 2 諏訪郡下諏訪町
 - 2 - 1 - 2 - 3 東筑摩郡波田町
 - 2 - 1 - 3 調査条件
 - 2 - 1 - 3 - 1 下伊那郡阿智村
 - 2 - 1 - 3 - 2 諏訪郡下諏訪町
 - 2 - 1 - 3 - 3 東筑摩郡波田町
- 2 - 2 第三者による評価

3 調査結果・発見された脆弱性

- 3 - 1 庁内 LAN における脆弱性
 - 3 - 1 - 1 ネットワークの設定
 - 3 - 1 - 2 既存住基サーバ
 - 3 - 1 - 3 庁内WEBサーバ
- 3 - 2 CSセグメントにおける脆弱性
 - 3 - 2 - 1 既存住基サーバ / CS間のファイアウォール
 - 3 - 2 - 2 CS
 - 3 - 2 - 3 CS端末
 - 3 - 2 - 4 アプリケーション
- 3 - 3 インターネット側からの攻撃に関する脆弱性

4 対策

- 4 - 1 庁内LAN関係
 - 4 - 1 - 1 ネットワークの設定
 - 4 - 1 - 2 既存住基サーバ
 - 4 - 1 - 3 庁内WEBサーバ
- 4 - 2 CSセグメント関係
 - 4 - 2 - 1 既存住基サーバ/CS間のファイアウォール
 - 4 - 2 - 2 CS
 - 4 - 2 - 3 CS端末
 - 4 - 2 - 4 アプリケーション
- 4 - 3 インターネット側からの攻撃関係
- 4 - 4 その他
 - 4 - 4 - 1 セキュリティ監査
 - 4 - 4 - 2 SLA
 - 4 - 4 - 3 職員教育
 - 4 - 4 - 4 新たな技術等の導入
 - 4 - 4 - 5 ネットワーク・コンピュータシステムの共同運営

5 その他

- 5 - 1 調査日程
 - 5 - 1 - 1 第一次調査
 - 5 - 1 - 2 第二次調査
- 5 - 2 調査費用
 - 5 - 2 - 1 第一次調査
 - 5 - 2 - 2 第二次調査

付属資料(別添)

- 1 「住民基本台帳ネットワークシステムに係る市町村ネットワークの脆弱性調査」に係る第三者評価
- 2 調査環境(イメージ図)

1 この調査について

1 - 1 目的

この調査は、長野県本人確認情報保護審議会が平成 15 年 5 月 28 日に県に提出した第一次報告において指摘された事項を中心に、インターネット側から市町村の庁内ネットワークを経由した住基ネットシステムへの不正アクセス及び住基ネットシステムからの本人確認情報漏洩の可能性を確認し、有効な対策を講ずるための資料を得ることを目的として行われた。

1 - 2 調査方法

1 - 2 - 1 概要

調査を企画した時点で、住基ネットが庁内 LAN 経由でインターネットに接続されている市町村は既に県内にはほとんどなかったため、この調査では内部からの侵入（庁内 LAN から住基ネットへの侵入）と外部からの侵入（インターネットから庁内 LAN への侵入）との 2 種類の調査を行い、これらの結果を組み合わせることにより住基ネットに対するインターネットからの脅威を明らかにしようとした。

1 - 2 - 2 内部からの侵入調査

庁内 LAN に調査用コンピュータを接続して庁内 LAN 及び庁内 LAN 上に存在する各種サーバについての情報を収集し、その情報をもとにサーバの管理者権限奪取を試みた。

管理者権限を奪取した既存住基サーバから既存住基サーバ / CS 間の市町村設置ファイアウォールについての情報を収集するとともに、既存住基サーバに偽装した調査用コンピュータにより CS との通信を試みた。

また、CS セグメントに接続した調査用コンピュータにより、CS 及び CS 端末についての情報を収集し、既知の脆弱性を利用して CS 及び CS 端末の管理者権限奪取を試みた。

1 - 2 - 3 外部からの侵入調査

遠隔地からインターネットを経由してファイアウォール及び DMZ に置かれた公開サーバについての情報を収集し、得られた情報をもとに公開サーバへの侵入を試みた。

1 - 2 - 4 留意した事項

この調査は、調査対象自治体において実際に稼働しているコンピュータ・システムに関して行われたため、調査に当たってはコンピュータ・システム及びネッ

トワーク管理に支障が生じないように留意しつつ行われた。

また、不正アクセス行為の禁止等に関する法律への配慮から、全国の都道府県の委託を受けて LASDEC が管理している部分、すなわち CS の都道府県ネットワーク方向にあるファイアウォールから上流部分については、今回の調査対象とはしなかった。

2 調査概要

2 - 1 調査対象、調査環境、調査条件等

2 - 1 - 1 調査対象

2 - 1 - 1 - 1 下伊那郡阿智村

第一次調査を平成 15 年 9 月 22 日から 24 日まで、第二次調査を同年 11 月 25 日から 28 日まで実施した。第一次調査の調査対象は既存住基サーバ、庁内WEBサーバ、既存住基サーバ/CS間の市町村設置ファイアウォール。第二次調査の調査対象は既存住基サーバ、既存住基サーバ/CS間の市町村設置ファイアウォール、CS及びCS端末。

2 - 1 - 1 - 2 諏訪郡下諏訪町

平成 15 年 9 月 25・26 日に調査を実施した。調査対象は既存住基サーバ、既存住基サーバ/CS間の市町村設置ファイアウォール及びCS。

2 - 1 - 1 - 3 東筑摩郡波田町

平成 15 年 9 月 29 日から 10 月 1 日までの間調査を実施した。調査対象はファイアウォール及びDMZに置かれた公開サーバ。

2 - 1 - 2 調査環境

2 - 1 - 2 - 1 下伊那郡阿智村

第一次調査では役場サーバ室内のHUB、隣接する施設のLANポート、庁内LANにダイヤルアップで接続されている出先機関のルータに調査用コンピュータを接続して調査した。

第二次調査では、CSが格納されている役場サーバ室内のラックを開錠し、CSセグメントにあるHUBに調査用コンピュータを接続して調査した。

なお、同一セグメントに属するCS端末がラック外にあることから、必ずしもラック内のハブに接続する必要はないが、窓口業務への影響等を考慮してサーバ室で調査を実施したものである。

2 - 1 - 2 - 2 諏訪郡下諏訪町

調査用に構築した無線LANを利用して、町役場に隣接する建物から調査用コンピュータを庁内LANに接続して調査した。

2 - 1 - 2 - 3 東筑摩郡波田町

遠隔地(東京)からインターネットでファイアウォール及びDMZにある公開サーバを調査した。

2 - 1 - 3 調査条件

2 - 1 - 3 - 1 下伊那郡阿智村

第一次調査では役場の許可を得てサーバ室、隣接施設及び出先機関において調査を実施した。第二次調査では役場の許可を得てサーバ室のラックを開錠して調査を実施した。

第一次・第二次とも庁内WEBサーバ及び既存住基サーバのIPアドレスについての情報を得ていた。これは、調査に要する時間を短縮するためであり、事前にこの情報がなくても同様の調査は可能である。

なお、CSセグメントに関しての情報は無い状態で調査を実施した。

2 - 1 - 3 - 2 諏訪郡下諏訪町

役場の許可を得て無線LANを設置し、隣接した建物内から調査を実施した。

既存住基サーバのIPアドレスについての情報を得ていたが、CSセグメントに関しての情報は無い状態で調査を実施した。これは、調査に要する時間を短縮するためであり、事前にこの情報がなくても同様の調査は可能である。

2 - 1 - 3 - 3 東筑摩郡波田町

東京都内からインターネット経由で調査を実施した。調査対象ネットワークIPアドレスについては事前に情報を得ていた。これは、調査に要する時間を短縮するためであり、事前にこの情報がなくても同様の調査は可能である。

2 - 2 第三者による評価

客観的な第三者の評価により調査結果の信頼性を高めるため、本県の情報化施策推進に関するメンター(助言者)であるとともに総務省住民基本台帳ネットワークシステム調査委員会委員でもある伊藤穰一氏に評価を依頼した。

3 調査結果・発見された脆弱性

3 - 1 庁内 LAN における脆弱性

3 - 1 - 1 ネットワークの設定

庁内 LAN への接続に当たってのユーザ名及びパスワードの設定に問題があり、調査用コンピュータでネットワークに接続することができた。

また、住民が自由に出入りできる施設の LAN ポートや出先機関のダイヤルアップルータに接続した調査用コンピュータでネットワークに接続することができた。

3 - 1 - 2 既存住基サーバ

既存住基サーバの管理者権限のユーザ名及びパスワード設定に問題があり、庁内 LAN に接続した調査用コンピュータにより管理者権限で正規のユーザになりすましてログオンできた。

この際、データベースのユーザ名及びパスワード設定に問題があったので、データベースの内容を閲覧することができた。

また、既存住基サーバで使用されている OS には既知の脆弱性が存在しており、庁内 LAN に接続した調査用コンピュータにより、この脆弱性を利用して管理者権限を奪取した。

3 - 1 - 3 庁内 WEB サーバ

ファイル共有の設定に問題があり、庁内 LAN に接続した調査用コンピュータから個人情報を含む重要なデータファイルにアクセスすることができた。

庁内 WEB サーバが使用している OS には既知の脆弱性が存在しており、庁内 LAN に接続した調査用コンピュータにより、この脆弱性を利用して管理者権限を奪取し庁内 WEB サーバを支配することができた。

また、不必要なサービスの提供が行われていたほか、OS レベルでのパケットフィルタリングによるアクセス制限も行われていなかった。

3 - 2 CS セグメントにおける脆弱性

3 - 2 - 1 既存住基サーバ / CS 間のファイアウォール

不要と思われるポートが開放されているものがあつた。今後このポート関連の脆弱性が発見される可能性は否定できない。

なお、ファイアウォールの OS のバージョンが古く、既知の脆弱性を利用した攻撃が行われる可能性がある。

3 - 2 - 2 CS

CSが使用しているOSには既知の脆弱性が存在しており、CSセグメントに接続した調査用コンピュータから、この脆弱性を利用して管理者権限を奪取することができた。

この際、CSのデータベースのユーザ名及びパスワードがCS内部のバッチファイルに暗号化されずに記述されていたので、データベースにアクセスできた。

さらに、このデータベース自体も暗号化されていなかったことから、当該自治体住民の住基ネット情報を閲覧することができた。

また、不必要なサービスの提供が行われていたほか、OSレベルでのパケットフィルタリングによるアクセス制限も行われていなかった。

3 - 2 - 3 CS端末

CS端末が使用しているOSには既知の脆弱性は存在していなかったが、管理者権限を奪取したCSで得られたデータを利用することにより、CSセグメントに接続した調査用コンピュータから、管理者権限でログオンすることができた。

また、CSセグメントに含まれる機器の大部分は施錠したラック内に格納されているが、CS端末は役場の窓口に設置されているため、ここがCSセグメントへの進入経路となる可能性がある。

3 - 2 - 4 アプリケーション

既存住基サーバとCSが通信するために使うと思われるアプリケーションには、脆弱性のある関数が使われている可能性があった。

3 - 3 インターネット側からの攻撃に関する脆弱性

今回の調査では脆弱性は発見されなかったが、一般にDMZにある公開サーバの管理者権限が奪取された場合、公開されている情報の破壊・改竄が可能なほか、DMZと庁内LANの間のファイアウォールの設定によっては、庁内LAN上に存在するデータも危険にさらされる可能性が存在する。

4 対策

4 - 1 庁内LAN関係

4 - 1 - 1 ネットワークの設定

不正なログオンを防止するため、パスワードに関するポリシーを確立し、このポリシーに沿ってネットワークを運用する。

不正な接続が行われないようLANポート、HUBに物理的な措置を行うとともに、ダイヤルアップルータは運用時間外の電源遮断を行う。

4 - 1 - 2 既存住基サーバ

不正に管理者権限でログオンできないようにするため、パスワードに関するポリシーを確立し、このポリシーに沿ってシステムを運用する。

OSの脆弱性を利用した攻撃を回避するため、常に適切なセキュリティパッチを適用する。

4 - 1 - 3 庁内WEBサーバ

データファイルの共有設定を安易に行わない。

OSの脆弱性を利用した攻撃を回避するため、常に適切なセキュリティパッチを適用する。

不必要なサービスを停止するとともに、OSレベルでのパケットフィルタリングを利用する。

4 - 2 CSセグメント関係

4 - 2 - 1 既存住基サーバ/CS間のファイアウォール

システムが利用しないポートを閉鎖する。

OSの脆弱性を利用した攻撃を回避するため、OSのバージョンを最新にする。

4 - 2 - 2 CS

OSの脆弱性を利用した攻撃を回避するため、常に適切なセキュリティパッチを適用する。

不必要なサービスを停止するとともに、OSレベルでのパケットフィルタリングを利用する。

4 - 2 - 3 CS 端末

不正に管理者権限でログオンできないようにするため、パスワードに関するポリシーを確立し、このポリシーに沿ってシステムを運用する。

不正な接続が行われないように、CS 端末を設置している場所での LAN ポートに物理的な措置を行う。ラック内に CS 端末専用ファイアウォールを設置する。

4 - 2 - 4 アプリケーション

アプリケーションに脆弱性が含まれる場合があるため、第三者がソースコードをチェックできる仕組みを作る必要がある。

4 - 3 インターネット側からの攻撃関係

DMZ に置かれた公開サーバに対しては、常に適切なセキュリティパッチを適用する。

公開サーバの管理者権限が奪取された場合を想定して、ファイアウォールの設定、庁内 LAN のコンピュータへのセキュリティパッチ適用を適切に行う。

4 - 4 その他

4 - 4 - 1 セキュリティ監査

一部の構成要素に限定せずにシステム全体について実施する。
第三者により定期的に実施する。

4 - 4 - 2 SLA

管理を委託している業者との間で SLA (サービスレベル・アグリーメント) を結び、ネットワーク管理、セキュリティパッチの動作検証及び適用の責任の明確化を図る。

4 - 4 - 3 職員教育

職員がネットワークシステムの脆弱性を正しく理解することにより、不正なアクセスを防止する。

4 - 4 - 4 新たな技術等の導入

情報漏洩防止のためのモニタリングシステム、IDS・IDP、インベントリソフトによる端末管理、L3 スイッチ等による経路制御、認証 VLAN など、新しい技術の導入を図る。

4 - 4 - 5 ネットワーク・コンピュータシステムの共同運営

上記の対策を講じる際に多大なコストが発生することが予想されることから、県域WANを整備した上でサーバ群を共同管理するなど、複数の自治体によるネットワーク・コンピュータシステムの共同運営を検討する。

5 その他

5 - 1 調査日程

5 - 1 - 1 第一次調査

調査日程	調査対象
平成 15 年 9 月 22 日 (月) ~ 24 日 (水)	下伊那郡阿智村
平成 15 年 9 月 25 日 (木) 26 日 (金)	諏訪郡下諏訪町
平成 15 年 9 月 29 日 (月) ~ 10 月 1 日 (水)	東筑摩郡波田町

5 - 1 - 2 第二次調査

調査日程	調査対象
平成 15 年 11 月 25 日 (火) ~ 28 日 (金)	下伊那郡阿智村

5 - 2 調査費用

5 - 2 - 1 第一次調査

報酬・旅費 194,113円 (調査指揮監督者に対する報酬等)
委託料 2,782,500円 (調査補助者に対する委託料)

5 - 2 - 2 第二次調査

報酬・旅費 229,400円 (調査指揮監督者に対する報酬等)
委託料 3,600,000円 (調査補助者に対する委託料)

長野県知事 田中康夫 殿

「住民基本台帳ネットワークシステムに係る市町村ネットワークの脆弱性調査」 に係る第三者評価

市町村ネットワークの調査の実施方法に対する評価

私は、今回の長野県が行った市町村ネットワークの安全性調査に関して、長野県より調査を委託された調査チームに詳細にわたりインタビューをし、調査チームによって使用されたデータ、ログおよび方法を再調査した。

私は、この多少困難な状態下で行われた調査の技術的な要件は論理的に整合性がとれており、非常に高いクオリティを持った調査であったと評価する。

また、私は、実施手順について実施者からの十分な説明を受け、それを基にして評価しており、そのため、調査に実際に立ち会わずとも正当な評価ができるものである。

私は、この調査の制約条件を考えれば、調査チームの最終報告書とそれに対する私の評価は、地方自治体ネットワーク、および地方自治体ネットワークへつながる住基ネットワークの脆弱性を、公平かつ正確な視点で指摘していると言える。

また、より多く時間をかけ、より多くのアクセスをし、リソースとコストを加えることにより、この調査結果はより精度を増すと信じる。

市町村ネットワークの調査全体に対する分析

私は調査チームが長野県の3つの自治体において行ったセキュリティ調査に関して、調査チームのメンバーと調査のプロセス、データと分析について再検討し、彼らの方法論と結論についてもディスカッションした。

総合的に言って、当該の場所におけるセキュリティレベルは平均以下であり、住民についての様々な個人情報は盗まれたり改竄されることに対して危険な状態にあると言える。

調査チームはインターネットからと地方自治体オフィスの内部から調査を行った。その調査は非常に限定された時間の中で行われた。インターネットからの侵入テストは成功しなかったが、自治体オフィスの中からの侵入テストは成功した。調査は、地方自治体オフィスの中にあるコンピュータに限定されていたため、総務省が管理する住基ネットには直接アタックしなかった。しかしながら、直接に住基ネットに接続するコンピュータである「CS」、「CS 端末」及び「既存住基サーバー」は、すべて地方自治体ネットワーク内部にあるが、これらのすべてが攻撃されやすい状態であり、調査チームはこれらのコントロールを奪取することが可能だった。「CS」及び「既存住基サーバー」は当該自治体に住んでいる住民の住基ネットデータのデータベースを持っている。これは理論的には、彼らが住民の記録を編集したり消去したり新しく作ることを可能にするということである。テストでは行われなかったが、このデータベースを編集することは偽の記録を中央の住基ネットシステムに送る事態を引き起こす原因となることはありえるであろう。

加えるなら、住基ネットとは無関係だが、センシティブな個人情報を含んでいる多数のファイルが、保護がないままの地方自治体ネットワークの上にアクセス可能な状態で存在した。

インターネットから地方自治体ネットワークに侵入することは可能ではなかったが、遠距離のオフィスのためユーザーが地方自治体のネットワークに接続することを許したダイヤルアップ・アカウントがあり、これらのダイヤルアップ・アカウントが何者かの支配下に置かれた場合ネットワークにダイヤルインすることは可能である。加えて、ある自治体では庁舎以外の施設で直接ネットワークに接続していた。自分のコンピュータをそのネットワークと接続することができるならば、「ハッカー技能」を持たない何者でも容易にこれらの端末上に「共有されて」いる機密なファイルをダウンロードすることができる。

CSと、地元の住民の住基ネットデータを収容している既存住基サーバーに侵入することは非常に容易であった。それらは適切なセキュリティパッチが当てられないままシステム運用を行っていた。既存住基サーバーのパスワードは、データベースのものと同様に非常に判りやすく、解明するのに時間はかからなかった。

そのサーバー上で走っているソフトウェアは「バッファオーバーフロー」の弱点が含まれた状態で書かれていた。これはソフトウェア・コードのデベロッパーのセキュリティ

への理解の欠如を示すものである。コンピュータ・エンジニアならば、住基ネットのデータにアクセスを得るために、自由に入手可能なツールを使ってこれらの脆弱性のどれでも自分の制御下に置くことが可能である。

私は当該ネットワークのセキュリティレベルが平均以下であったと考える。そして平均的コンピュータ・ネットワークエンジニアなら誰でも侵入することが可能で、住基ネット情報を含む様々な個人情報盗んだり損害を与えることができるであろう。オフィスで働く人々と、特にシステム・セキュリティを提供している業者は、セキュリティとプライバシー問題に敏感ではない。サーバーは適切に保守されてはいなかったし、パスワードの選択（多くが既定パスワードあるいは容易に推測できるパスワードを用いていた）は無責任であり、そしてセキュリティに関する注意の完全な欠如を示していた。私は、地方自治体オフィスとこれらの地方自治体に対するソリューションを供給しているベンダーの双方に、プライバシーの目的のためにセキュリティの優先順位が明確に上げられるべきことを強く主張したいと思う。私は、住民と彼らの情報を守るべき担当者が、際立って危険な状態にさらされていると考える。

市町村ネットワークの調査の最終審査に基づく勧告

1. 地方自治体ネットワークのセキュリティ強化に関する勧告

a. 地方自治体ネットワークに接続されたサーバー、およびそれに接続されているすべてのコンピュータ上で起動しているすべてのソフトウェアのバッファオーバーフローを調べる。これらの監査の能力を有する第三者機関が存在するので、地方自治体に販売されたアプリケーションはこの第三者機関もしくは地方自治体に属する能力のあるグループにより調査されることを必要とする。

b. ハードウェアのメンテナンスに関する合意書に加えて、サービスレベルに関する合意書 (Service Level Agreements/SLAs) も必要とすること。多くのネットワークは、その機器を販売する地方の業者によるネットワーク管理責任を明示する合意書を、当該業者と交わしていなかった。

c. 時宜を得たプログラムの更新および修正(パッチをあてるなど)を行うこと。誰が

この要求を実施すべきかが明らかではなく、CSの場合など多くの場合、誰がそのような更新に責任があるかも明らかではなかった。ネットワークのすべての部分について責任を負うべき者をはっきりさせるべきである。それが民間業者の場合には、更新の適用と怠慢について契約上の責任を負わせるべきである。

2. 将来の監査に関する勧告

a. 「チェックリストによる監査」と、監査対象と友好関係にある機関によるセキュリティ監査が、第三者機関によるセキュリティ監査を凌ぐものでないことは明らかである。したがって、第三者機関によるセキュリティ監査が定期的に行われるべきである。

b. 詳細なログと監査担当者との面談は必要とされ、セキュリティ監査の質の評価が常になされるべきである。

c. 長野県のセキュリティ監査は不正アクセス禁止法に従うことが不可避であったために、地方自治体の管理するネットワークに限定された。本来あるべきセキュリティ監査はシステム全体にわたってなされるべきであり、システムのどの構成要素も除外すべきではない。重要なのは構成要素ではなく、システム全体のセキュリティであることが理解されるべきである。

3. 付加

a. セキュリティ監査、業者に対する新しい責任、セキュリティ強化は追加的コストを必要とすることになる。これらのコストと関係するコストから見たセキュリティ強化の実現可能性を評価すべきである。

b. メディアは、住基ネットシステム全体の脆弱性に焦点をあてず、インターネットからの侵入実験の失敗にのみ焦点をあてていた。彼らはセキュリティ監査のポイントを間違えており、ただ総務省と長野県の対立関係をあおり続けているだけである。しかし事実は、中央の住基ネットシステムが直接的には侵入されなかったとしても、住基ネットシステム全体に脆弱性があることが見つかったということである。何がセキュリティ強化のために必要とされるか、誰が設定の変更を実施しセキュリティ監査することに責任をもつべきか、そのようなセキュリティ強化にはどのようなコストがかかるか、これら

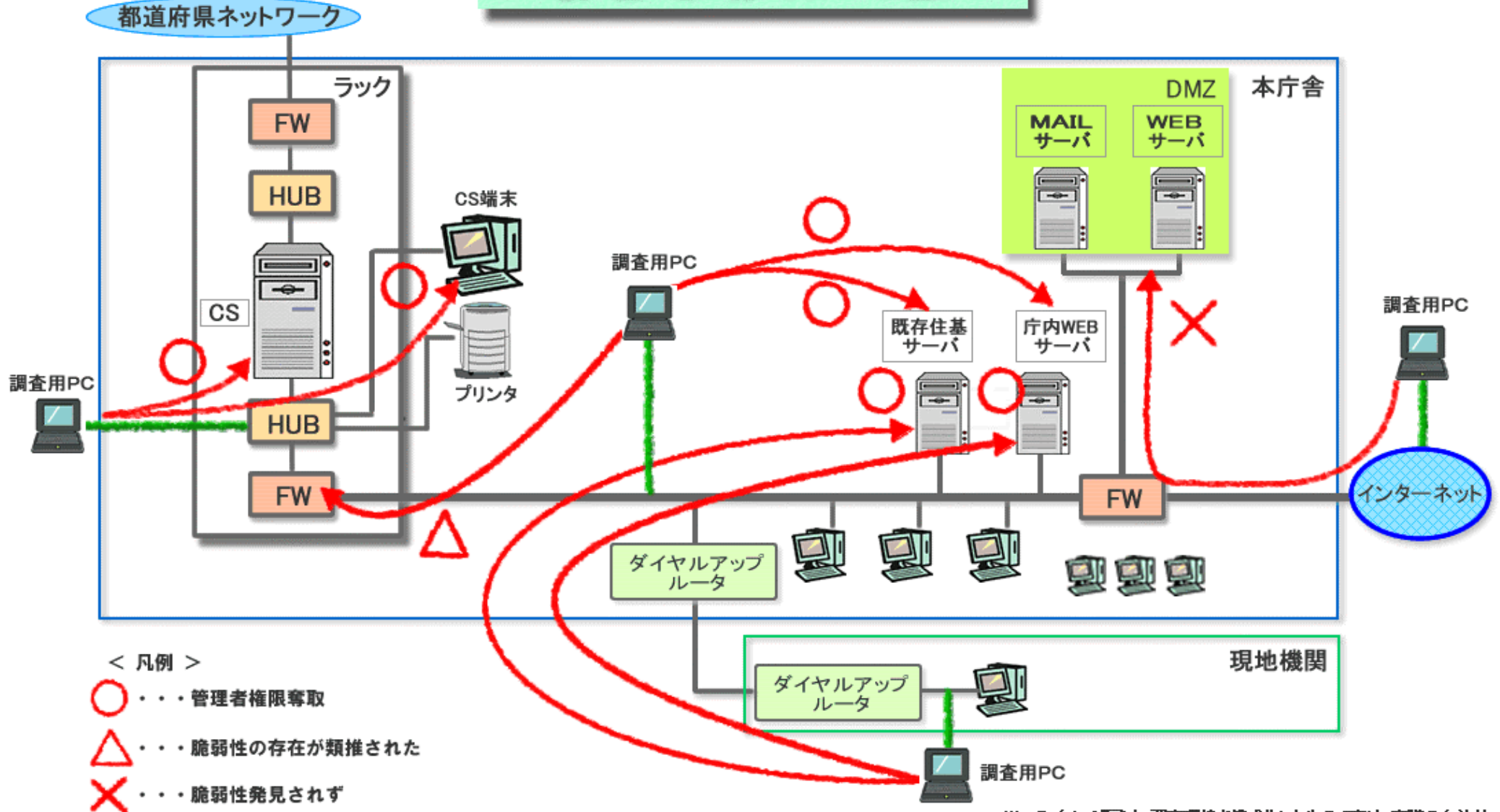
の3点についての議論こそが最も重要なのである。

c . セキュリティ調査チームは業者、中央政府、地方自治体に対して、見つかった脆弱性と推奨される対処法について任務終了後、報告をすべきである。この技術的な報告は迅速かつ徹底的に行われるべきである。

平成 16 年 1 月 30 日

伊藤 穰一

調査環境 (イメージ図)



※このイメージ図は、調査環境を模式化したものであり、実際の自治体コンピュータネットワークがこういう形態になっている訳ではない。

住民基本台帳ネットワークシステムに係る市町村ネットワークの脆弱性調査結果を踏まえた長野県の具体的対応について

今回の調査は住基ネットの一部を構成していると考えられる市町村のコンピュータネットワークを対象として行ったものであり、その結果については市町村によく理解していただくことが重要。その上で、調査実施者及び評価をした第三者からの提案を参考に、現時点で考えている対応を下記のとおり取りまとめた。なお、この対応についても市町村と十分協議しながら進めていくこととする。

1. セキュリティ研修

市町村ネットワークのセキュリティ強化支援のため、研修会等を開催する。

- (1) 調査結果を踏まえた市町村担当者向けセキュリティ研修会の実施
- (2) 住基ネットの運用及びセキュリティに関する研修会の実施
- (3) 市町村の必要に応じて、個別に庁内LANに関する相談やセキュリティ運用面でのアドバイス等を行う。
- (4) 市町村一般職員向けのセキュリティ研修機会の充実

2. セキュリティ監査等

全国的に進められるセキュリティ監査等を確実に実施できるよう支援する。

- (1) セルフチェックリストによる庁内LANのセキュリティ点検の実施
(平成15年度中)
- (2) 情報セキュリティ監査の実施(平成16年度 普通交付税措置予定)
- (3) 住基ネットに関するチェックリストによる自己点検、セキュリティ監査の実施
(平成16年度 地方自治情報センター)

3. より安全なネットワークシステム等の検討

市町村と十分協議しながら、長野県本人確認情報保護審議会から提案されている「より安全なネットワークシステム」等の具体化を進める。

- (1) 高速情報通信ネットワークの検討
 - ・高速情報通信ネットワークの整備・運営に関する方針(案)を県民に公表し、パブリックコメントを募る予定。
 - ・方針(案)を公表次第、市町村との協議()を進める。
- (2) 共同アウトソーシング(共同センター、ハウジング)の検討
 - ・共同アウトソーシングの枠組み、進め方等について市町村とともに検討()を行う
- (3) 庁内LANに関するセキュリティ対策会議()の開催
 - ・新たな技術等の導入の検討等を行う。

長野県電子自治体協議会及びセキュリティWGを想定。

4. その他

CS及びCS端末へのセキュリティパッチ早期適用のための体制強化等を地方自治情報センターに対して要請していく。

今後の具体的なスケジュールは別紙のとおり

(別紙)

- 3月上旬 市町村に対する説明会(県内2箇所)
- ・住基ネットに係る市町村ネットワーク脆弱性調査結果の説明
 - ・具体的なセキュリティ対策の提案
 - ・高速情報通信ネットワークの提案

セキュリティWG(市町村向けセキュリティ指針作成)

- 4月中旬 セキュリティ監査関係説明会・研修会

- 6月上旬 住基ネット担当者研修会

電子自治体協議会

セキュリティWG

(時期未定)

住基ネットに関するチェックリストによる自己点検