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、伊藤穣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 －

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な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な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った。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）