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うけ、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システムの脆弱性を、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、当該の場所においての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、調査チームはそ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アルアップ・アカウントがあり、これらのダイアルアップ・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ア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こ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あ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を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と。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　穣一