長野県が実施した「市町村ネットワークの安全性調査」を受けての対応

平 成 １ ５ 年 １ ２ 月 ２ ６ 日
住民基本台帳ネットワークシステム調査委員会

○　長野県は、１２月１６日、速報として「市町村ネットワークの安全性調査」を発表した。この発表において、実際に住基ネット本体へは侵入されておらず、また、指定情報処理機関の本人確認情報は全く問題ない状況であるにもかかわらず、庁内ＬＡＮの脆弱性を住基ネット本体の安全性の問題であるかのように取り上げるなど、事実と異なる情報が喧伝されている。

○　この調査は、上述のような問題点を含んでいるものの、総合的に判断すれば、住基ネット本体の本人確認情報に対する危険性は確認されなかった一方で、一部の市区町村において、庁舎内に違法な物理的な侵入がなされた場合に、庁内ＬＡＮ上にある当該市区町村住民の個人情報について一定の危険性が存在することが報告されたものと考えるべきであろう。

○　なお、長野県は、本年８月５日、「住民基本台帳ネットワークシステムのセキュリティに関する公開討論会」において、ファイアウォールの侵入実験を行う必要性を強調し、また、８月１５日、住基ネットと接続している庁内ＬＡＮが物理的にインターネットと接続している市町村について、侵入実験を行ったうえでインターネットと切り離すよう要請すると記者発表を行っている。

○　他方、本調査委員会では、これまで住基ネット自体の安全性は高いものの、セキュアな電子自治体を構築する観点からも、市区町村の庁内ＬＡＮのセキュリティレベルの維持・向上が課題であると指摘してきたところである。

○　以上を踏まえ、今回の長野県の調査結果も冷静に分析しつつ、今後の市区町村のセキュリティ対策の向上を図るため、総務省・指定情報処理機関においては、以下のような取り組みを行うべきである。

（庁内ＬＡＮ）

①　「地方公共団体における情報セキュリティ監査の在り方に関する調査研究会報告書」で示されたセルフチェックリストを利用した庁内ＬＡＮのセキュリティ点検の普及を図るとともに、市区町村におけるセキュリティ監査の実施について積極的な財政支援及び技術支援を行う。

②　市区町村における庁内ＬＡＮ－インターネット間のファイアウォールについて、希望する市区町村に対し、遠隔でセキュリティ診断を実施する（平成１５年度中に実施）。

③　ＬＧＷＡＮ－ＡＳＰ（アプリケーションサービスプロバイダー）を利用した地方公共団体の庁内ＬＡＮのセキュリティ診断の実現に向けて検討を行う。

④　地方公共団体職員に対するセキュリティ研修について、質・量ともに、さらなる充実を図る。

⑤　庁内ＬＡＮの委託事業者（ベンダー）に対し、セキュリティパッチの適用、強固なパスワードの設定、ソフトウェアにおけるセキュリティ強化措置等について周知徹底を図るとともに、セキュリティ意識の向上を図るための研修会を実施する。

⑥　万一庁内ＬＡＮ上の個人情報の改ざんが行われた場合に、極めて可能性は少ないものの、住基ネットに改ざんされた情報が反映される危険性を防止するため、当面、市区町村において、定期的に住民異動届と住基ネット上の本人確認情報の変更を照合する等、運用面での確認作業を実施してもらう方向で検討する。

（ＣＳ等）

⑦　指定情報処理機関において、ＣＳ・ＣＳ端末のセキュリティパッチの適用について、動作確認を迅速に実施する体制を強化し、さらなる早期の適用を図る。また、住基ネット関係のソフトウェアにおけるセキュリティ強化措置についても、継続的に確認作業を実施する。

⑧　第２回目の住基ネットに関するチェックリストによる自己点検、セキュリティ監査を実施する（平成１６年度できるだけ早期に実施）。

チェックリストによる点検にあたっては、ＦＷ管理状況に加えて、強固なパスワードの設定、物理的な侵入に対する防御等を重点項目とする方向で検討する。

⑨　住基ネットに関するデータ送受信において高度なセキュリティレベルの維持、向上を図るための方策を実施する（平成１６年度できるだけ早期に実施）。

⑩　ペネトレーションテストを継続的に実施する（平成１６年度も実施）。

ペネトレーションテストの実施にあたっては、テストの範囲や体制のあり方について検討を行う。

（別紙）

長野県が実施した「市町村ネットワークの安全性調査」についてのＱ＆Ａ

Ｑ１　長野県が実施した「市町村ネットワークの安全性調査」で何がわかったのか。

（Ａ）

１　長野県が実施した「市町村ネットワークの安全性調査」で確認できた事項は、次のとおりである。

①　インターネットからＦＷ経由での庁内ＬＡＮへの侵入に失敗

②　ＣＳ－庁内ＬＡＮ間のＦＷを突破できず

③　そこで、厳重に管理されているサーバ室やラックの鍵をあけ、ＦＷで防御された区画内に攻撃端末をつなぎこむ等、物理的な侵入を伴う形での実験に切り替えて、ＣＳ、ＣＳ端末の管理者権限を取得

④　実際に住基ネット本体へは侵入されておらず、また、指定情報処理機関の本人確認情報は全く問題ない

※　住基ネットに関しては、操作者用ＩＣカードによる認証を経ないと住基ネットの一切の操作を行えないようにする等、各般のセキュリティ対策をすでに講じており、ＣＳ、ＣＳ端末の管理者権限を取得されても、当該市区町村以外の住民の本人確認情報を盗取することはできない。

⑤　別途、庁内ＬＡＮ側から、ＦＷで防御された区画内に攻撃端末をつなぎこむ等、物理的な侵入を伴う形での実験に切り替えて、庁内ＬＡＮ上にある既存住基サーバ等の管理者権限を取得

⑥　なお、出先機関につなぎこんだ攻撃端末からダイアルアップ・アカウント経由で侵入が行われているが、これは物理的な侵入であって、一般的に指摘されている無線ＬＡＮやダイアルアップ・アカウントの危険性についての調査は行っていない

※　無線ＬＡＮやダイアルアップ・アカウントの危険性とは、物理的な侵入を伴わず、かつ、ＦＷを回避して、攻撃端末が庁内ＬＡＮにつなぎこまれる危険性をいう。

２　したがって、長野県の調査では、住基ネット本体の本人確認情報（当該市区町村以外の市区町村の住民の個人情報）に対する危険性は確認されなかった一方で、一部の市区町村において、庁舎内に違法な物理的な侵入がなされた場合に、庁内ＬＡＮ上にある当該市区町村の住民の個人情報について一定の危険性（改ざん等）が存在することが示されていると考えられる。

Ｑ２　ＣＳ－庁内ＬＡＮ間のＦＷの通過の方法を発見したとあるが、見解如何。

（Ａ）

１　長野県の調査結果では、ＣＳ－庁内ＬＡＮ間のＦＷの通過の方法を発見したとあるが、当該ＦＷはＣＳ－既存住基サーバ間の特定の通信とＣＳ－ＣＳ端末間の特定の通信のみを許可する設定となっており、その内容は攻撃端末をつなぎこめば容易に知ることができるものである。

２　しかしながら、このようなＦＷの通過の方法がわかったからと言って、ＦＷ越しにＣＳ、さらには住基ネットに対する攻撃はできない。

なお、ＣＳ－庁内ＬＡＮ間のＦＷが指定情報処理機関の提示にそった設定となっていればＦＷ攻略ができないことは、品川区において指定情報処理機関が実施したペネトレーションテストで実証済みである。

Ｑ３　住基ネットに改ざんされたデータを反映することが可能とあるが、見解如何。

（Ａ）

１　庁舎内に違法な物理的な侵入等がなされ、万一庁内ＬＡＮ上にある当該市区町村住民の個人情報について改ざんがなされた場合、極めて可能性は少ないものの、その改ざんされたデータが住基ネットに送信されることにより、結果的に住基ネットに改ざんされた情報が反映される危険性はあり得るものと考えられる。

なお、この場合でも、他の市区町村の本人確認情報には全く影響はない。

２　これを防止するためには、各市区町村の庁内ＬＡＮについてセキュリティ対策の強化を図っていく必要があるが、当面、住基ネットに関しては、市区町村に対し定期的に住民異動届と住基ネット上の本人確認情報の変更を照合する等、運用面での確認作業を実施してもらう方向で検討する。

Ｑ４　ＣＳ、ＣＳ端末に侵入し管理者権限を取得したとあるが、見解如何。
**　　また、全国の本人確認情報が閲覧可能と報道されたが、見解如何。**

（Ａ）

１　長野県の調査結果では、ＣＳ、ＣＳ端末の管理者権限を取得したとのことであるが、インターネットから侵入するとしながら、ＦＷで防御された区画内に攻撃端末をつなぎこむ等、物理的な侵入を伴う形で実験がなされている。
**　さらに、厳重に管理されているサーバ室やラックの鍵をあけて攻撃端末が接続されており、侵入実験としての的確性を欠いていると考えられる。**

２　住基ネット業務を行うためには操作者用ＩＣカードによる認証が必要であるため、ＣＳ、ＣＳ端末の管理者権限が取得されたとしても、住基ネットの全国サーバや県サーバの本人確認情報を不正に閲覧することはできないし、実際に閲覧されていない。
**　なお、ＣＳは市区町村が管理するＦＷで防御し、重要機能室に設置する等権限のない者がアクセスできないように市区町村で管理を行っており（平成１５年に実施したチェックリストにより、全市区町村での実施を確認済み）、そもそも攻撃端末のつなぎこみができないようになっている。**

３　今回、ＣＳ、ＣＳ端末の管理者権限取得の要因は、推測容易なパスワードの不正取得、セキュリティパッチの適用時間差によるセキュリティホールの悪用等によると考えられることから、指定情報処理機関において、動作確認実施体制を強化しセキュリティパッチの適用時間差をさらに縮小する取り組みなどを引き続き行うとともに、住基ネット関係のソフトウェアにおけるセキュリティ強化措置について継続的に確認作業を実施することとする。
**　あわせて、ＣＳについて権限のない者がアクセスできないように厳重な管理を行う、操作者用ＩＣカードの適切な管理を行う、強固なパスワードを設定する等、市区町村に対し引き続き技術的支援を行うこととする。**

（参考）
**　品川区において指定情報処理機関が実施したペネトレーションテストでＣＳ端末への侵入ができなかった要因として、その時点ではセキュリティパッチの適用時間差がなかったこと、強固なパスワードが設定されていたこと等が考えられる。**

Ｑ５　既存住基サーバに侵入し管理者権限を取得したとあるが、見解如何。

（Ａ）

１　長野県の調査結果では、既存住基サーバの管理者権限を取得したとのことであるが、インターネットから侵入するとしながら、ＦＷで防御された区画内に攻撃端末をつなぎこむ等、物理的な侵入を伴う形で実験がなされており、侵入実験としての的確性を欠いていると考えられる。

２　既存住基サーバは、税、国民健康保険等、これまで各市区町村において独自に電算化を行ってきた庁内ＬＡＮの一部であり、各市区町村において適切な管理がなされるべきものであって、住基ネットと直接的な関係はない。（なお、住基ネットと直接的な関係はないにしても、当該市区町村の多くの個人情報が保有されており、もとよりセキュリティ対策の強化が強く求められている。）

ただし、万一庁内ＬＡＮ上にある当該市区町村住民の個人情報について改ざんがなされた場合、極めて可能性は少ないものの、その改ざんされたデータが住基ネットに送信されることにより、結果的に住基ネットに改ざんされた情報が反映される危険性はあり得るものと考えられる。

３　今回、既存住基サーバの管理者権限取得の要因は、推測容易なパスワードの不正取得、セキュリティパッチの適用時間差によるセキュリティホールの悪用等によると考えられることから、ベンダー各社に対して、各市区町村において独自に電算化を行ってきた庁内ＬＡＮについても、セキュリティパッチを適用する、強固なパスワードを設定する、ソフトウェアにおけるセキュリティ強化措置を実施する等、セキュリティ対策の徹底を求める必要がある。

また、各市区町村に対しても、セキュリティ対策の強化について財政的支援及び技術的支援を行う必要がある（平成１６年に「地方公共団体における情報セキュリティ監査の在り方に関する調査研究会報告書」に基づき、セルフチェックリストを市区町村に配布する予定）。

当面、住基ネットに関しては、市区町村に対し定期的に住民異動届と住基ネット上の本人確認情報の変更を照合する等、運用面での確認作業を実施してもらう方向で検討する。

Ｑ６　指定情報処理機関による２４時間監視が不十分とあるが、見解如何。
（ＣＳへの不正アクセスを指定情報処理機関は検知できなかった。）

（Ａ）

指定情報処理機関は、住基ネット－ＣＳ間のＦＷまでを責任領域とし、当該領域について２４時間監視を行っており（ＣＳについては稼働状況のみ監視）、ＣＳについては、各市区町村において管理がなされている。

なお、この点については、住基ネットの設計段階において、指定情報処理機関から地方公共団体に通知しており、また、総務省及び指定情報処理機関の各種説明資料等でも公表されている事実である。

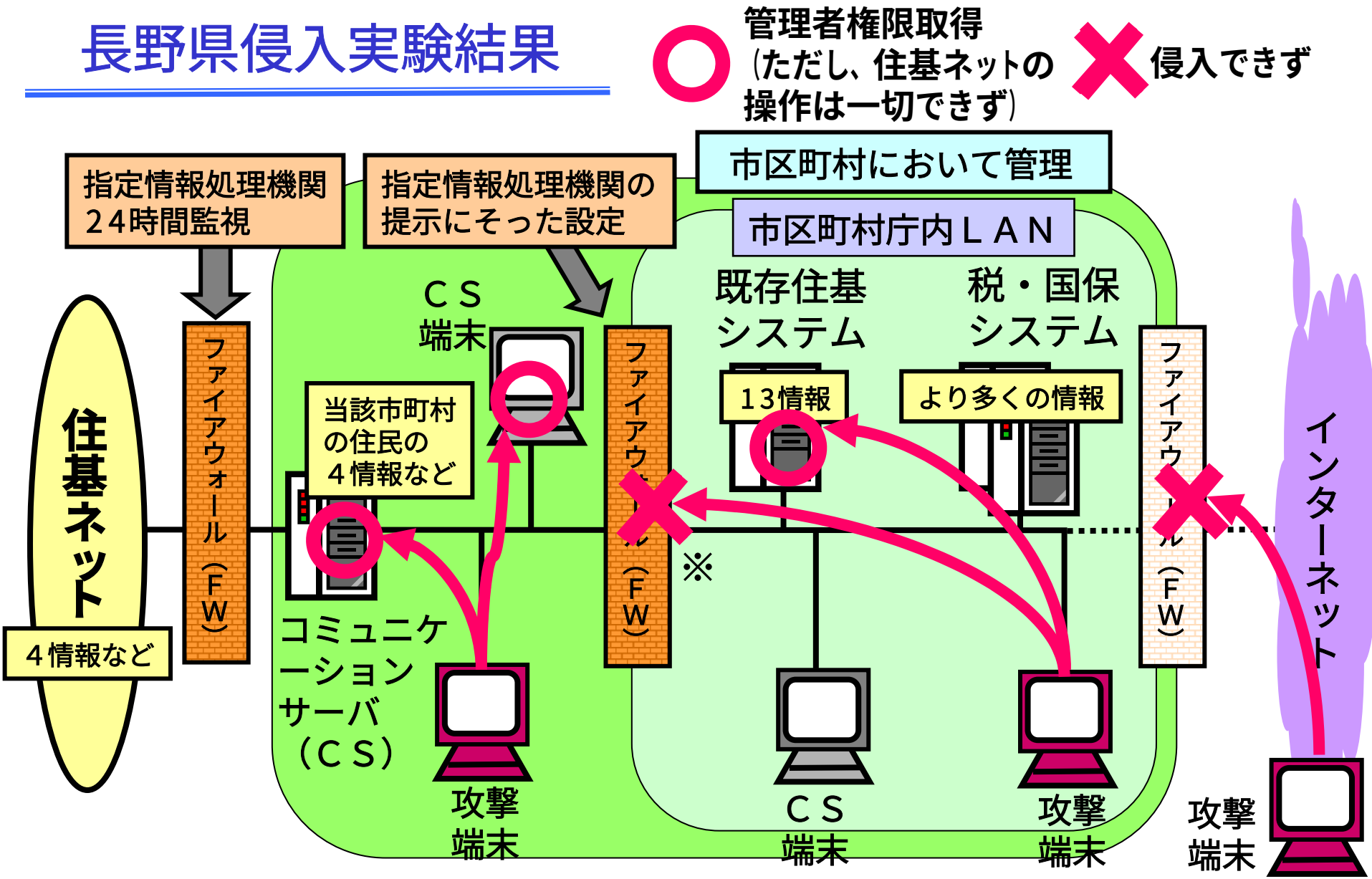
Ｑ７　次のような事例が起こりえるとしているが、見解如何。
・選挙人名簿に登載されていないことにして選挙をできなくさせる
・国民年金データを改ざんして転居させ、転居した場所でより多い年金額をもらう
・介護保険や児童手当の受給データを改ざんして、本来の受給者をもらえなくする
・税金の滞納データを消去し、そのデータを持たせて、勝手に転出させる

（Ａ）

１　住基ネットは、全国共通の本人確認を行う仕組みであり、４情報（氏名・住所・性別・生年月日）、住民票コードとこれらの変更情報のみを保有するシステムである。

２　したがって、長野県が例示している内容は、すべて各市区町村の庁内ＬＡＮに関わるものであり、住基ネットと全く関係ない。

長野県侵入実験結果



※　長野県では、通過の仕組みを発見したとしているが、実際の侵入はなされていない。