長野県の侵入実験に対する総務省コメント

１　本日（１２月１６日)、長野県において侵入実験の結果について発表があった。

　住基ネット本体へは侵入されておらず、全国センターの本人確認情報は全く問題ないところである。

　長野県の実験は、その手法に違法性のおそれがあることに加え、庁内ＬＡＮの小さな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ねじ曲げことさら誇大に取り上げた結果を公表しており、誠に遺憾である。

２　住基ネットはファイアウォールによる多重防御によってセキュリティを確保しているが、長野県の実験結果では、いずれのファイアウォールも突破することはできていない。８月１５日の長野県知事の発表ではインターネット接続が危険であるためインターネット接続団体で侵入実験を行うとしていたが、今回の実験ではインターネットからの侵入はできていない。

　したがって、長野県の意図した侵入実験は失敗したものである。

　ファイアウォールの安全性については、先般、指定情報処理機関が品川区の協力を得て実施した侵入実験でも同様の結果が得られている。

　住基ネットと接続している市区町村の庁内ＬＡＮがインターネットと物理的につながっていても、ファイアウォールの適切な設定、管理を通じてセキュリティを確保できることは明らかである。

３　長野県の実験結果では、ファイアウォールで防御された区画に攻撃端末を接続し、ＣＳ、ＣＳ端末と既存の住基システムに侵入したとあるが、今回の実験はサーバ室の鍵をあけサーバを設置しているラックの鍵をあける等、物理的な侵入を伴う実験としての的確性を完全に欠いた方法で行われている。

　これまで、ＣＳ、ＣＳ端末等の設置場所のセキュリティ強化を行うなど、チェックリストによる自己点検を踏まえた市区町村の庁内ＬＡＮのセキュリティ強化に継続的に取り組んでおり、攻撃端末が市区町村の庁内ＬＡＮ上に不正に接続されることがないよう対策を講じている。また、市区

町村のセキュリティ管理者のさらなる安全意識のレベル向上にも努力している。

　なお、第三者評価で指摘されているＣＳのセキュリティパッチの適用については、十分なシステムの動作検証を行い、早期にセキュリティパッチを適用するとともに、パスワードの設定が不十分等の指摘についても、市区町村に対し引き続き適切な技術的な支援を行う予定である。

　さらに、システム的には、操作者用ＩＣカードによる認証がないと住基ネットの個人情報を引き出すことができないようにする等、各般のセキュリティ対策を講じている。したがって、仮に市区町村の庁内ＬＡＮに攻撃端末を接続され、ＣＳやＣＳ端末の管理者権限を奪取されたとしても、住基ネット上の個人情報を盗み見ることはできない。

４　総務省としては、住基ネット調査委員会の提言、ペネトレーションテストを実施した監査法人の助言等を踏まえ、セキュアな電子自治体を構築する観点からも、引き続き、全国の市区町村における庁内ＬＡＮのセキュリティレベルの維持、向上を図るための取り組みを行ってまいりたい。