今回の安全確認実験の目的

１．なにを目指した実験だったのか

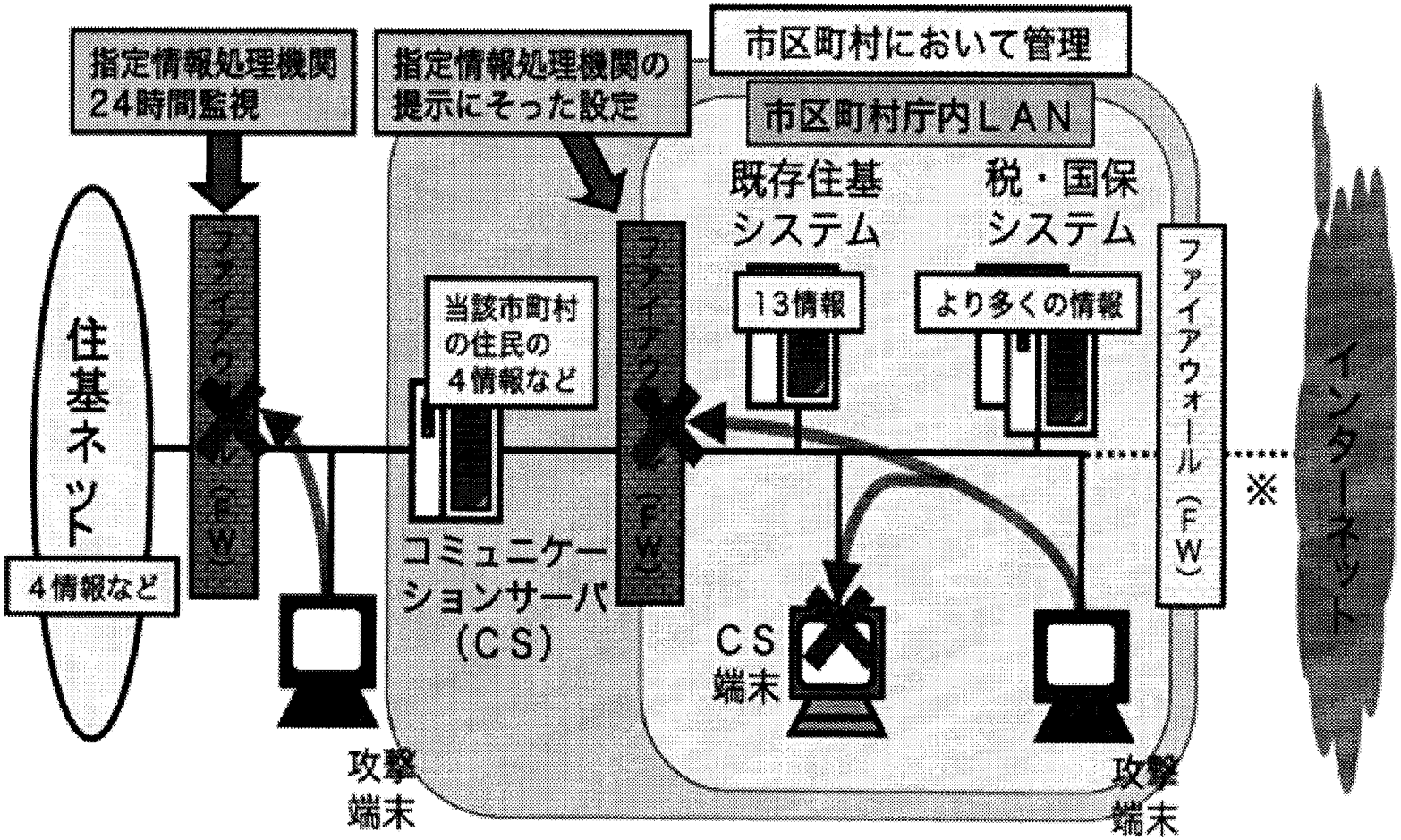
・８月の審議会で明らかにしたインターネットからの問題は
すでに指摘していたので多くの自治体ではコストをかけ
庁内ネットワークとインターネットを切断していた。

・よって残っていた内部からの脆弱性問題を確認した。

・内部の健康診断を行うことにより本人確認情報がどのように
安全に扱われているのかを確認することを目的とした。

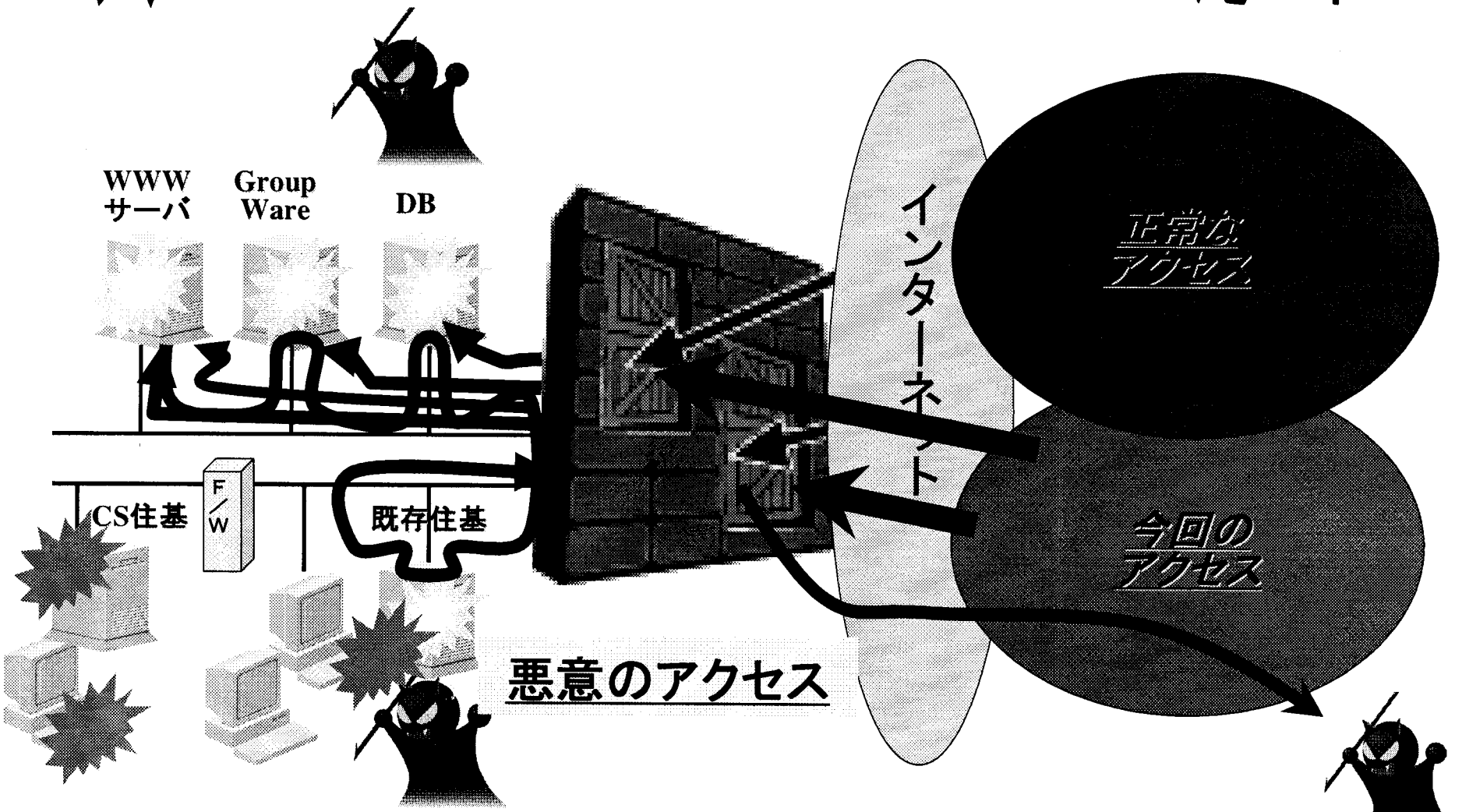
総務省の実験結果PDFより

住基ネットと市区町村庁内ＬＡＮ



※ 市区町村の中には、ファイアウォールを介して、庁内LANがインターネットと物理的に接続している団体がある。

ファイアーウォールが突破されていない？から安心？！



これを突破していないと表現するのが正しいのでしょうか

実験で浮き彫りになった問題点と対策

１．８月の審議会ですでに本人確認情報保護改善案を具体的に出している。

２．国の部分はテストしていないので安全かどうかは解らない。
　　そもそも、ドアもノックしていない。

３．LASDECの２４時間監視の質は民間業者で行えば年間３００万円以下で
　　有名大手が手がけているレベルでしかない死活監視のみとわかった。

４．このレベルでは不正なアクセスを検出できないことも明らかにできた。

５．国の部分が守られているから安全という話にはならない。
　　既存住基の内容を改竄し転出すればＣＳサーバーに１４情報が移動し
　　転出先の既存住基そのままコピーされ住基ネットのなかを４情報以外の
　　データーが流されている。

実験で浮き彫りになった問題点と対策

6. 出先施設の安全性は不十分であった。簡単に庁内LANに入れた。
庁内施設の安全性確保だけでは不十分で、遠隔施設の安全性も確保する必要がある。とくに出先からISDNによる公衆回線で庁内ＬＡＮ接続し
ており住基ネットが公衆回線に接続されていることが明らかになった。
発信者番号チェックやコールバック機能だけでは不十分である。

7．ラックの鍵を持ったことは実験の価値がないとの声が多いが国の実験もラックを開けて行っていたと、聞いている。アプローチは同じである。

8．他の都道府県では未だ長野県レヴェルには達していない。

9．今後より具体的な対応策を今回の実験を受けて精査して提案したい。

結論

1. 基礎自治体から他の都道府県の基礎自治体へ改竄された
   既存住基のデータが正規データーとしてＣＳサーバーに
   電送されそのデータが真のデーターとして他の市町村で
   扱われ既成事実化してしまう。
2. F/Wがあるから安全という技術神話は崩れた。
3. 波田町はなぜ今は安全だったのか
   インターネットと分離が無意味だったのではなく、
   サーバを完璧に守ったことが今回はたいへん有効だった。
   サーバやPCのセキュリティホール対策が重要ということ
   であり、不具合が見つかったら直せばいい、という考えは
   技術的には通用しない。