# 住民基本台帳ネットとは

- 住民基本台帳に記載されている国民全員に１１ケタの番号を割り当て
- 市町村、県、国のコンピューターで個人情報を一元管理するシステム

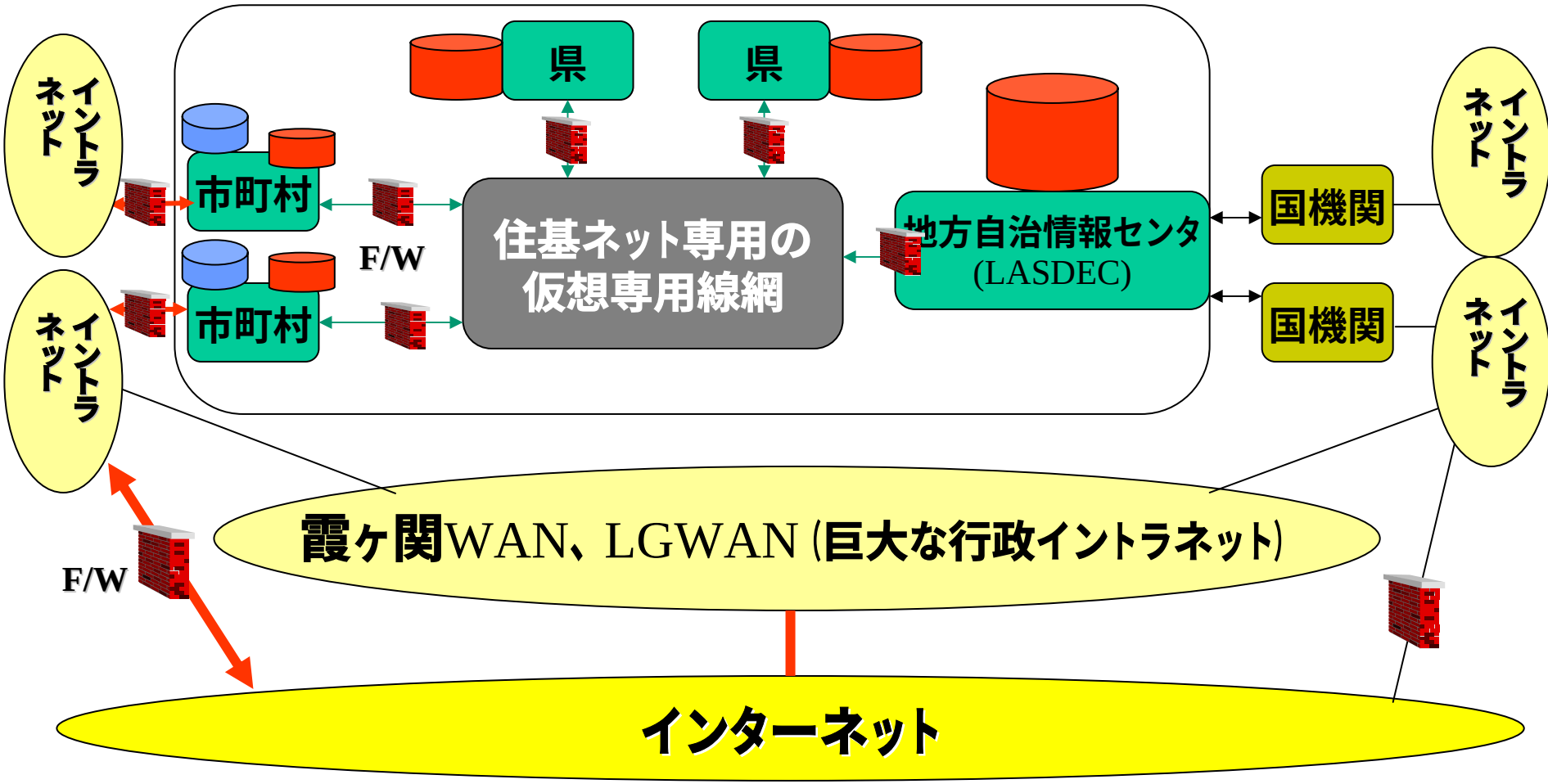
- ＩＣカードで居住地以外の自治体でも住民票の写しが取得できるなど、新しい行政サービスが可能になる
- 半面、「国民総背番号制に道を開く」との懸念も指摘

- ３６５億円の構築費と年間１９０億円＋αの運用経費
- 長野県分は、**初期：1億5千万円、運用：5億数千万円**
- 中途半端な開放型ネットのため、安全性に疑問あり、個人情報の漏洩につながる危険性がある

# 住基ネットワーク構成

住民・戸籍台帳

基本情報（住所、氏名、年齢、性別、住基コード、変更履歴）



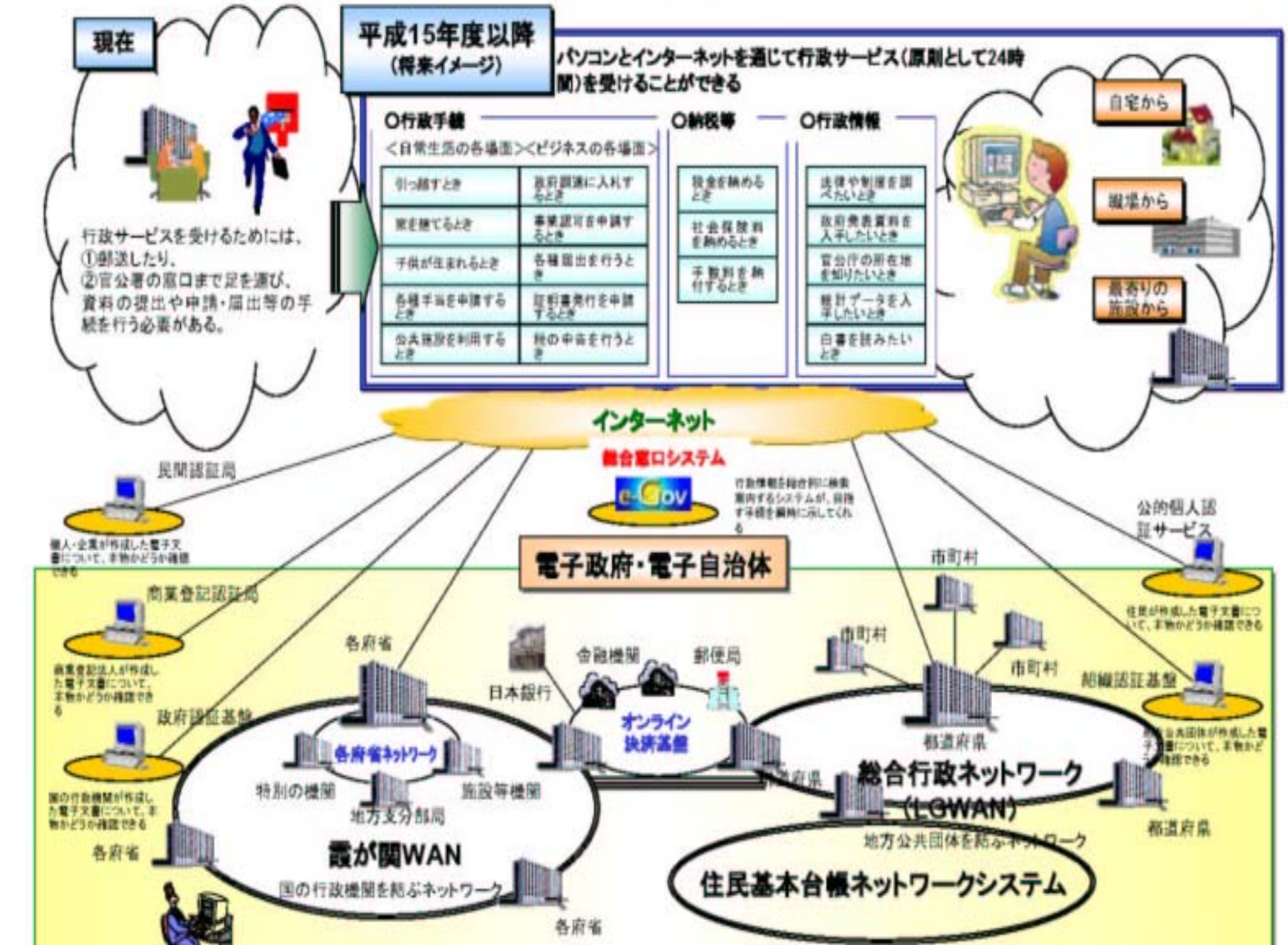

イントラネット：庁内LAN、内部限定の情報系LAN　（基幹業務系とは別LANが基本）、
F/W（ファイアーウォール、障壁：関所、守衛に相当）経由でインターネットと接続

# 誰が便利になるのか

- 住民への恩恵ー現時点では、ほとんどなし
  - 住民票の広域交付？
  - 転出時に、転出元の役所に行かないで済む？
  - 身分証証書としての住基カード？
  - 時間外の印鑑登録証明書、住民票自動発行？
  - 市町村自身が1％しか普及しないと予想して予算化

- 国の利便性ーあります
  - 際限のない拡大（93ー＞171ー＞264ー＞＞）
  - 例えば、警察、税務署、自衛隊、保険･医療、、など
  - 統合DB化可能（電子政府、電子自治体の目標）
  - これは国民総背番号制そのものになる可能性を秘めている

# 電子政府・電子自治体のイメージ

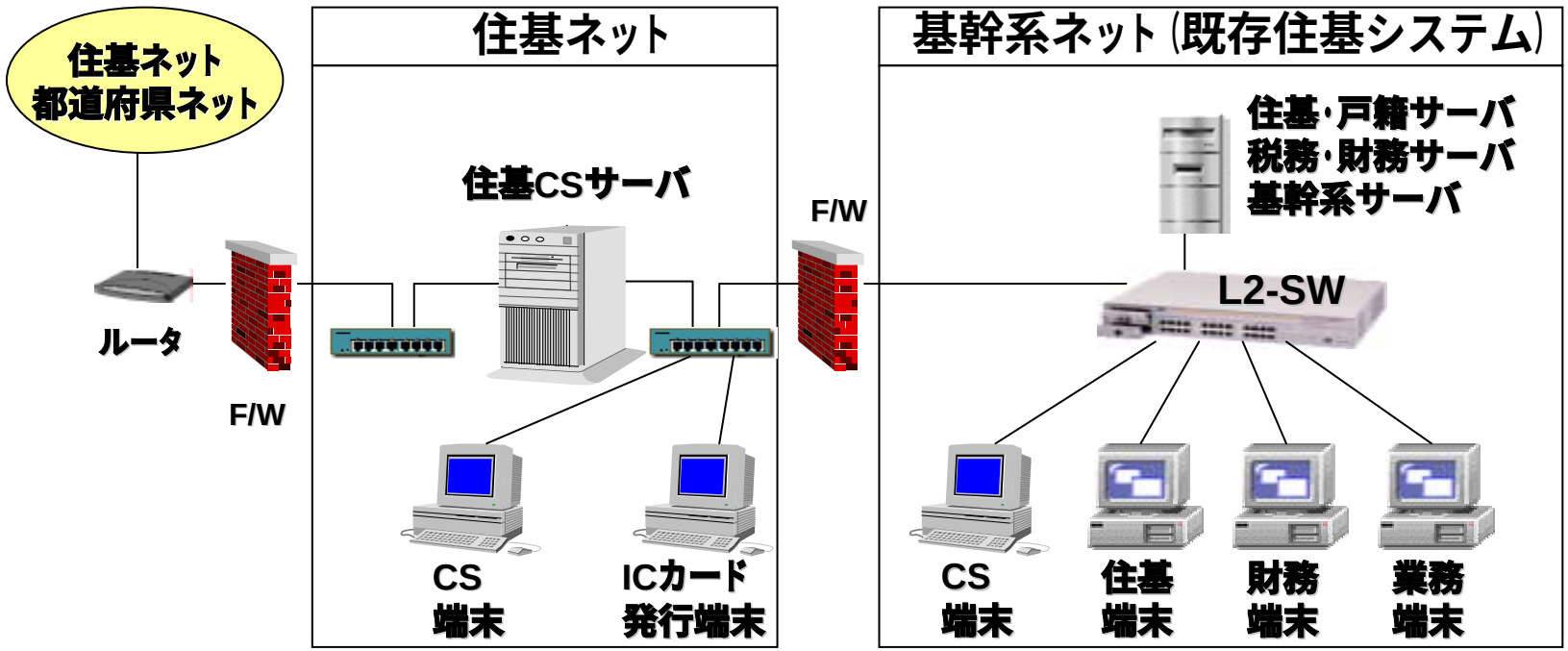


# 漏洩するのは　住所･氏名･年齢･性別･コード　だけか？

- **市町村役場で管理している個人情報例**
  - 納税状況、年金の支払い状況
  - 介護を受けている人は…要介護度やサービスの詳細･ねたきりになった年月･食事状況
  - 町主催の健康診断を受けた人は…現病歴･生活習慣の内容･身長･体重･体脂肪･血液･尿･体力検査の結果
  - 公立学校に通った人は…所属クラブ名、教科単位の得点から身体検査の結果、体力検査の結果
  - 公立保育園に通った人は…家族の職業･収入･勤務時間
  - 公立図書館を利用する人は…貸出資料名

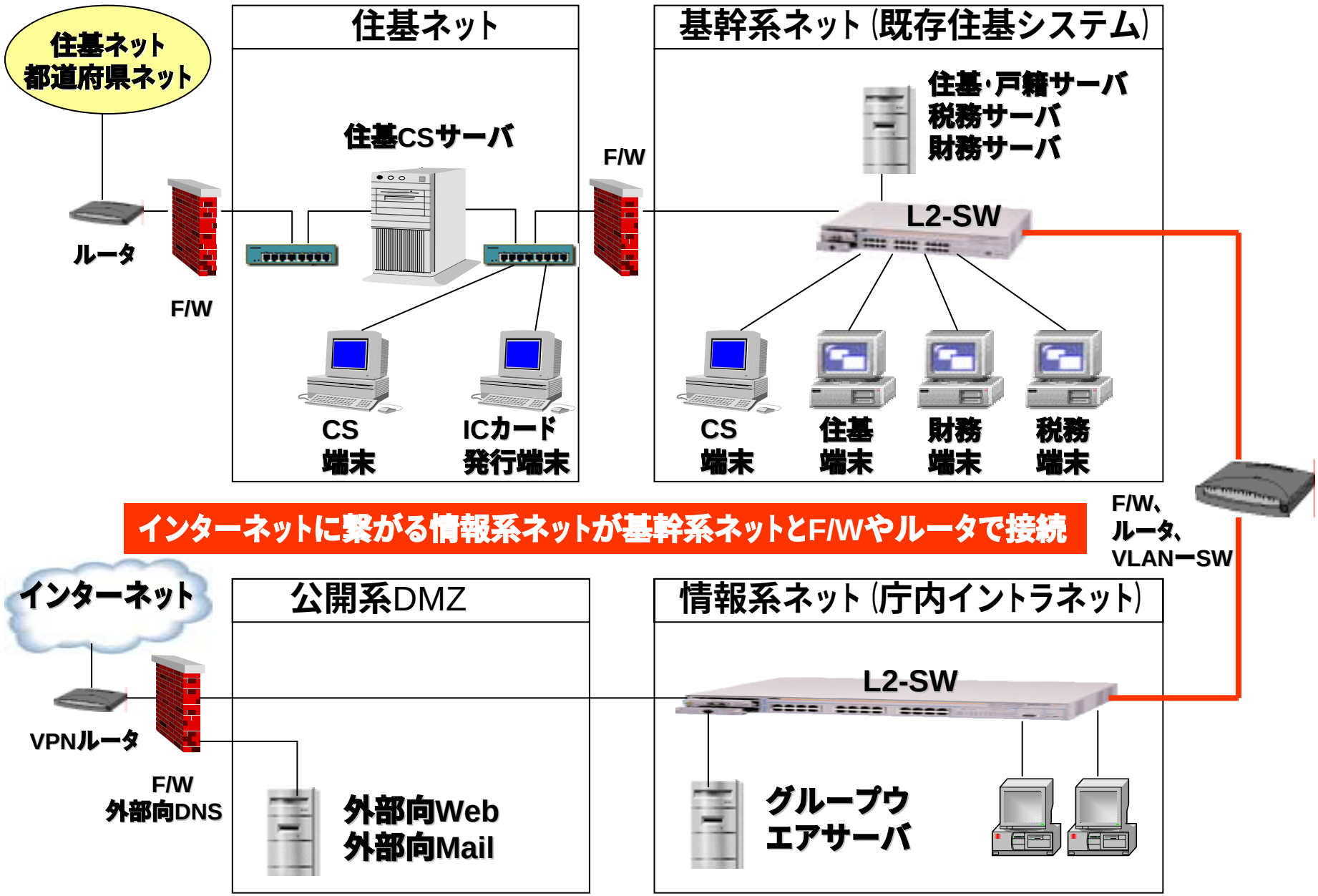
- **電子自治体構想では、これら情報を統合DB管理を目指す**
- **これらの情報は原則として各自治体内で限定運用するもの**
- **しかし、検索コード（住基コード）の全国共通化、行政間ネットワーク連携により、その保証がなくなる可能性がある**
- **単なる11桁の個人番号が、各情報をつなぐ役割を持つことの意味は大きい**

# 安全性の高いネットワーク接続形態

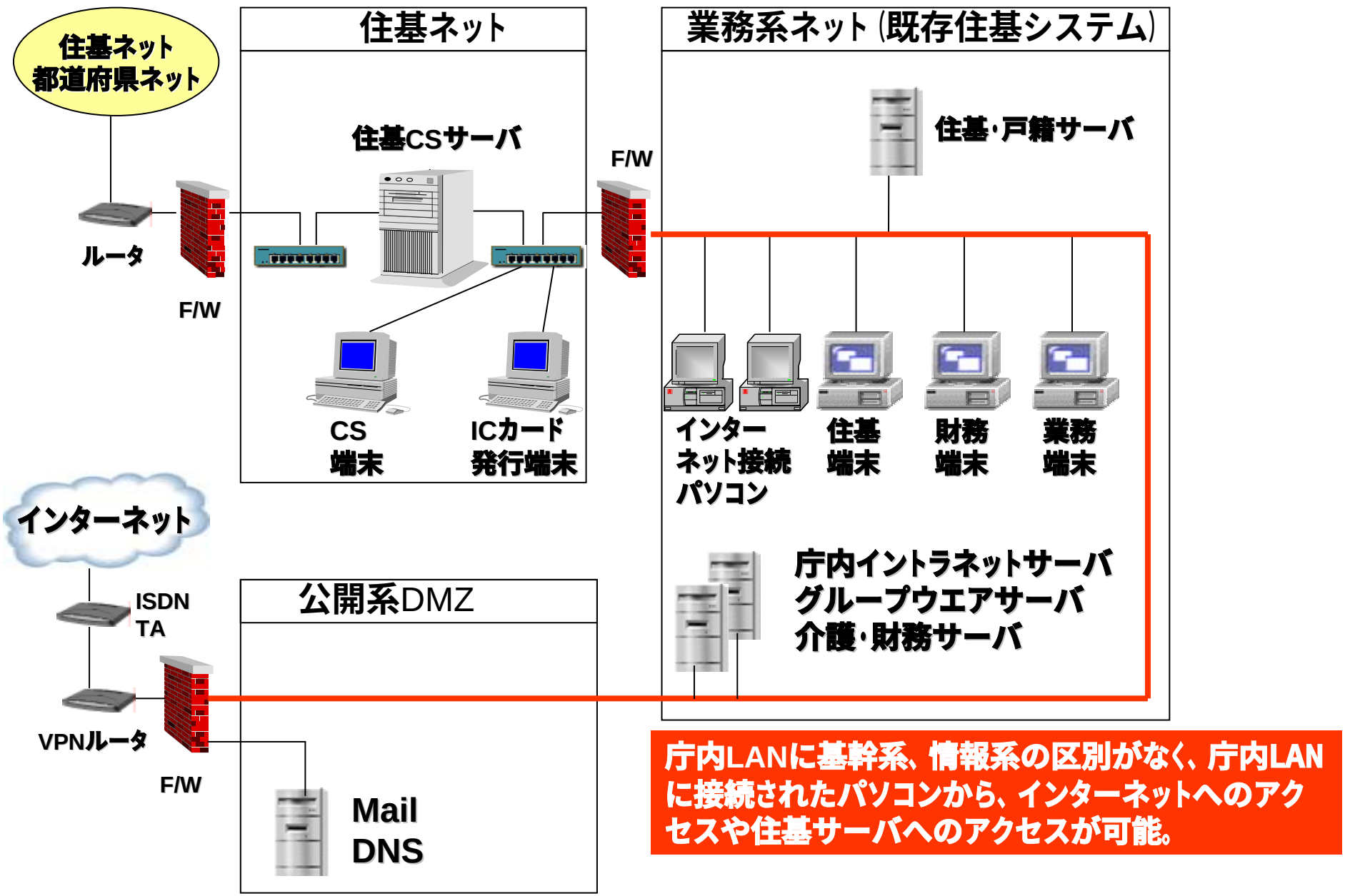



**住基ネットに繋がる基幹系と、インターネットに繋がる情報系は分離する**

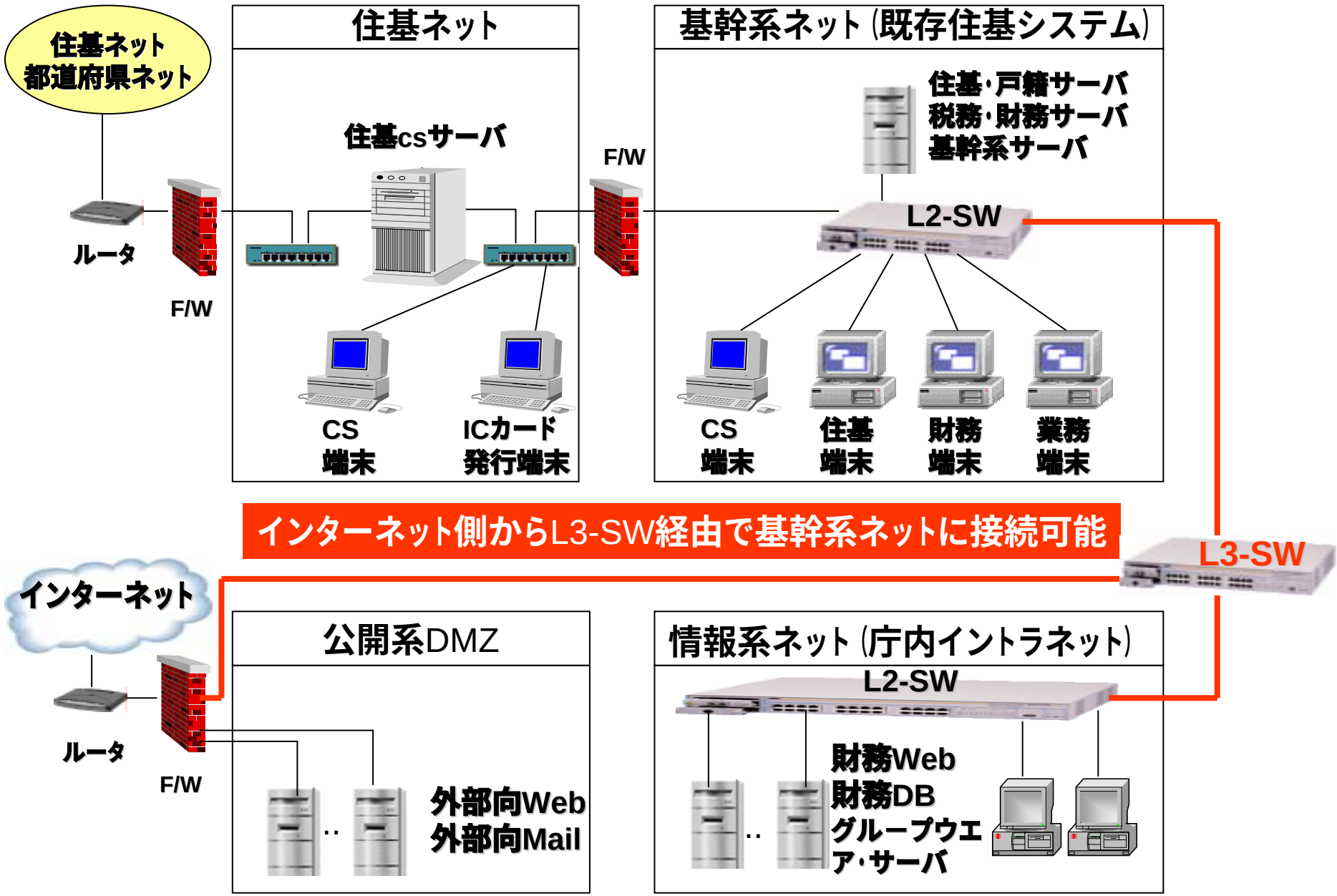
# 危険性のあるネットワーク接続事例－１



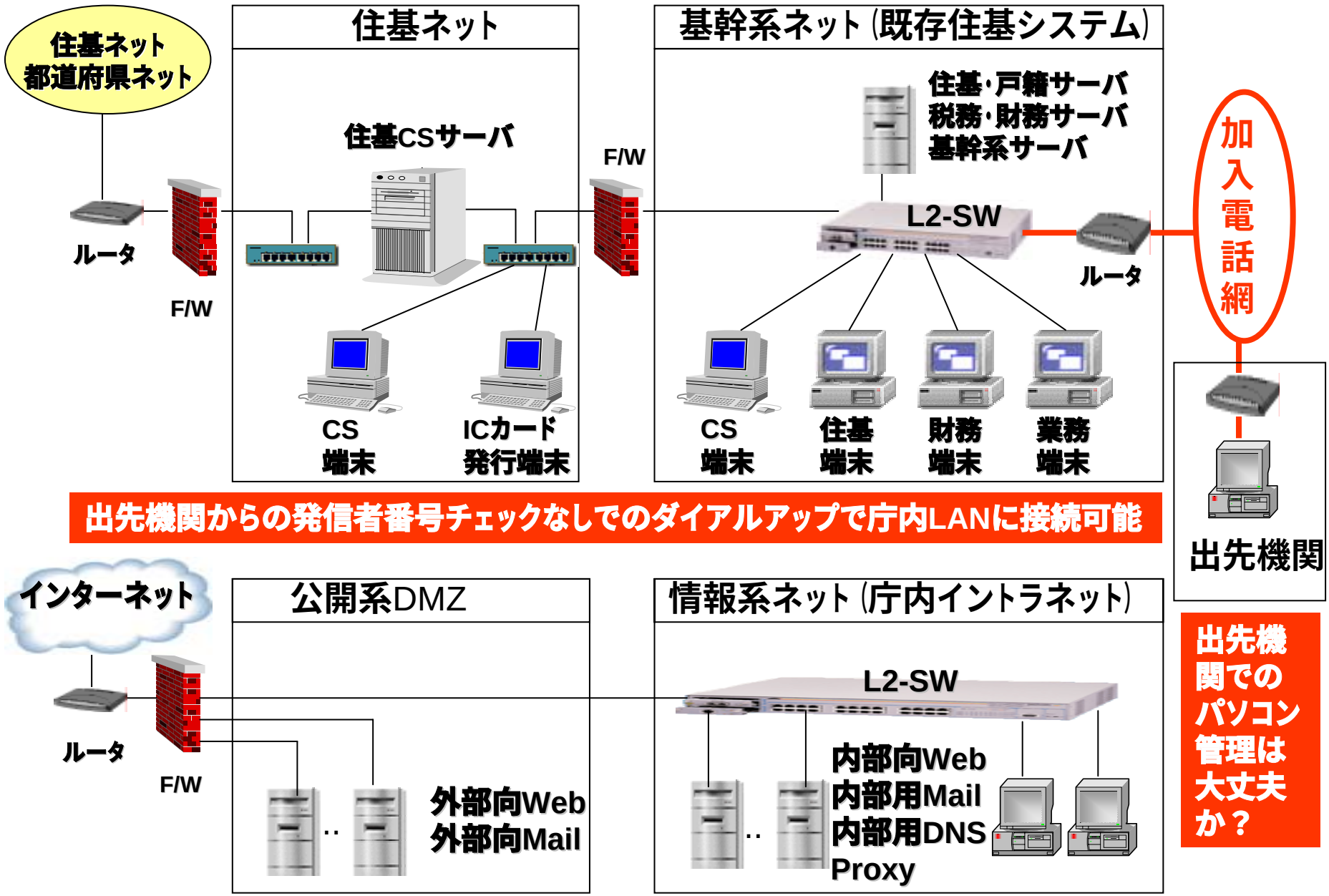
# 危険性のあるネットワーク接続事例－２



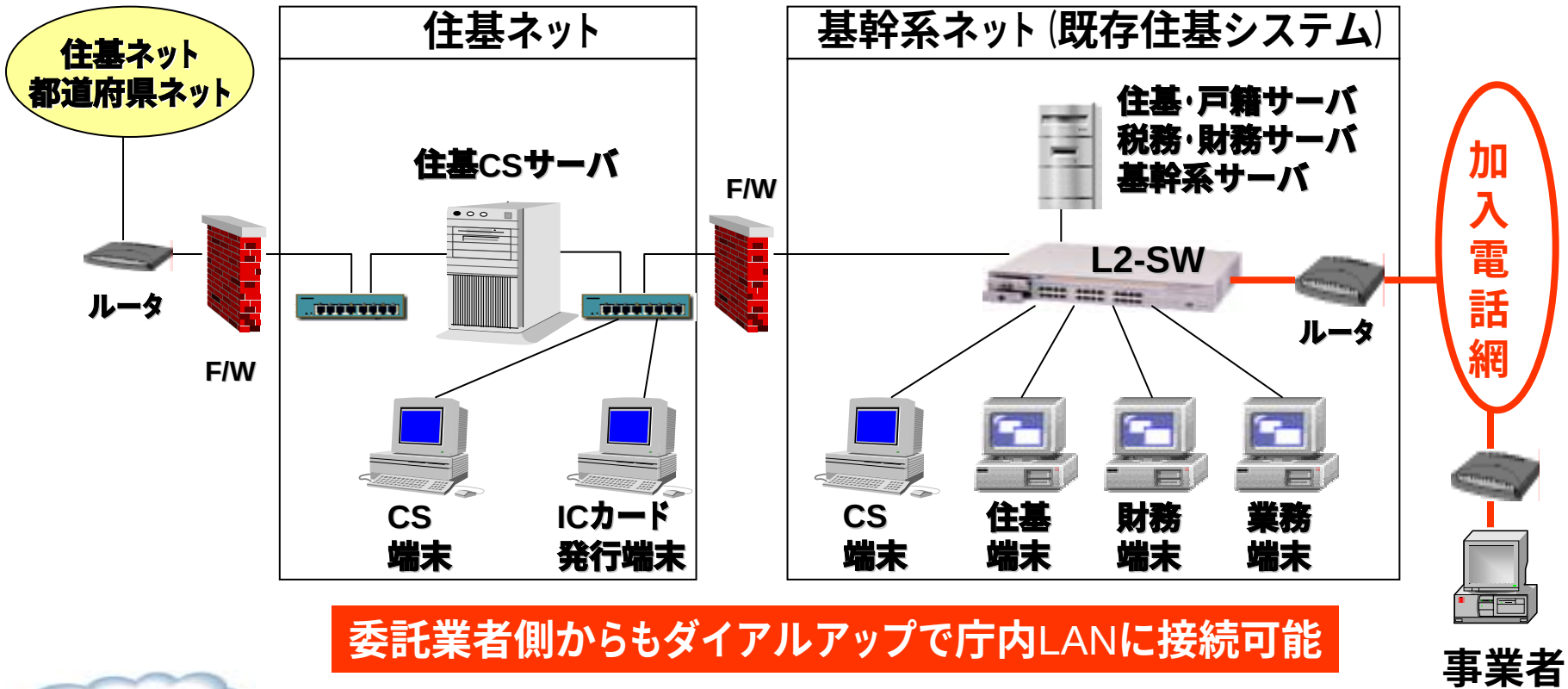
# 危険性のあるネットワーク接続事例－３



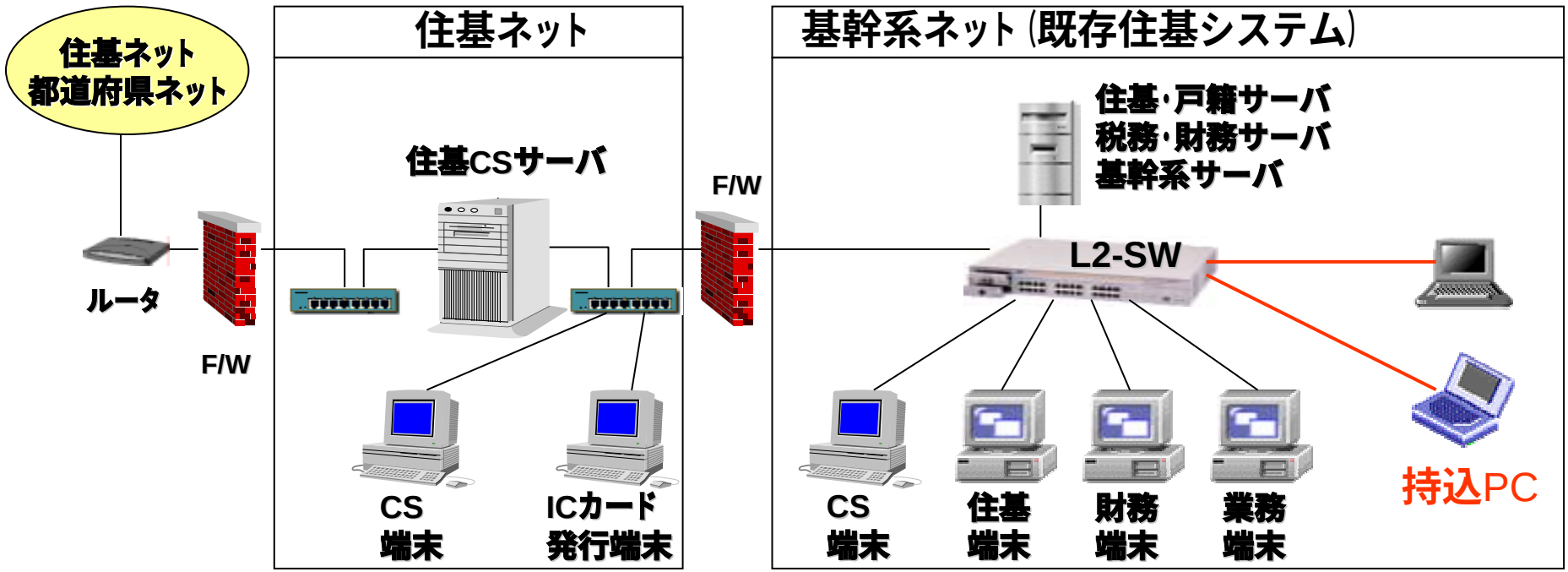
# 危険性のあるネットワーク接続事例－４



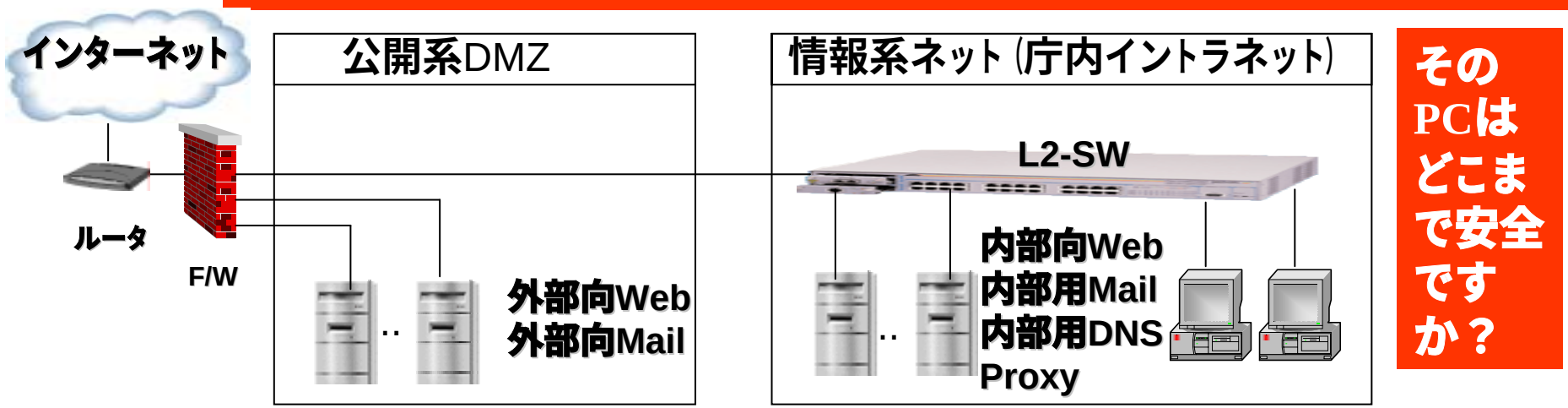
# 危険性のあるネットワーク接続事例－５



# 危険性のあるネットワーク接続事例－6




住基ネットに繋がる基幹系HUBに空きがあり、持ち込んだパソコンを接続可能




**そのPCはどこまで安全ですか？**

# 全国約400の市区町村で、住基とインターネットが接続

(2003.6.7毎日新聞)

全国の市区町村のうち1割以上の約400の団体で、住民基本台帳ネットワーク(住基ネット)と接続している庁内LANが、インターネットと接続していることが、総務省の資料で分かった。総務省は「直ちに危険とはいえない」としているが、片山虎之助総務相のこれまでの発言と食い違う部分もあり、批判が高まりそうだ。

総務省が5日、長野県の本人確認情報保護審議会の報告に反論する形で、全国の市区町村に通知した文書で分かった。同文書のなかで、総務省は、1割強の市区町村で住基ネットと物理的に接続している庁内LANがネット接続していることを認めた。そのうえで、「接続していたとしていても、直ちにセキュリティー上危険とはいえず、FWの設定など適切なセキュリティー措置の実施により、個人情報の保護を図ることが可能」と説明している。

また、仮に庁内LANにウイルスやハッカーが侵入しても「住基ネットに入り、他の市区町村のCS(コミュニケーションサーバー)、都道府県サーバー、指定情報処理機関サーバーに到達する恐れはない」と明言している。

しかし、片山総務相は、2月13日の衆議院予算委員会などで「ご存知のように住基ネットは閉じたネットワークですよね。インターネットなんかと接続していないんですよ。接続しているものは切ってもらうんですよ」などと発言している。

この点について、総務省市町村課では、「閉じたネットワークというのは、FWでセグメントとして区画されているという意味。住基ネットと庁内LAN、庁内LANからインターネット接続しているもので、セキュリティー上問題があると考えた約200団体については、昨年8月の段階で、いったん住基ネットと常時接続を行わないよう指導しており、大臣発言はその意味だ」と説明している。

# 最新の InternetExplorer バグベア.B 情報 (2003.6.5)

- 悪意のあるユーザーによる攻撃 (毎日新聞ニュース シマンテック MS社のHP)
- Web サーバーから返されるオブジェクトの種類を判断する処理に存在する脆弱性を悪用し、バッファのオーバーラン攻撃が行われる可能性がある問題です。
  ファイルのダウンロード時にダイアログ ボックスでブロックできず、ユーザーのコンピュータ上で任意のコードが実行される可能性があります。

- 対策が行われていないシステムがインターネットなどのネットワークを通じて他のコンピュータと接続している場合、この問題を悪用した攻撃を受けることがあります。この攻撃は、受動的攻撃という悪意のあるユーザーから送られた HTML 形式の電子メールからも攻撃を受ける可能性があります。この攻撃は、ハッカーまたはクラッカーと呼ばれる悪意のあるユーザーや、ワームといった自動的な攻撃を目的とした悪意のあるプログラムから行われることがあります。

- この脆弱性を悪用されることにより、以下のような実害を受ける事が考えられます。
  意図しないアプリケーションが動作させられる可能性があります。(ハードディスクのフォーマットやワームなど)
  意図しないスクリプトが動作させられる可能性があります。
  バックドア設定の危険性もあり

# いくつかの事例　－１

- MSのFTPサーバーから、顧客データベースなど大量の内部資料が流出（2002年11月20日） link
- 『アパッチ』使用サイトに深刻なセキュリティー危機：ロシア大統領サイトも（2002年6月21日） link
- 『ウィンドウズ2000』の脆弱性、米軍サーバーにも危険（2003年3月18日） link
- 『パスポート』のセキュリティー問題でMSに多額の罰金か（2003年5月8日） link
- マイクロソフト自身にも及んだ『SQLスラマー』ワームの被害（2003年1月28日） link
- 依然として残る米国政府コンピューター・システムの脆弱性（2002年11月19日） link
- 米政府審議会「ネットワークの複雑化で攻撃がますます容易に」（2002年12月9日） link

# いくつかの事例－２　ルータ

- [4] CIAC Bulletin N-083 Cisco Catalyst Enable Password Bypass Vulnerability
  http://www.ciac.org/ciac/bulletins/n-083.shtml

  Cisco Catalyst OS **バージョン** 7.5(1) **が稼動している** Cisco Catalyst 4000、6000 **および** 6500 **には、コマンドラインアクセスにおけるパスワード認証に 脆弱性があります。 結果として、遠隔から第三者が登録されているユーザ名を使って、パスワード なしに、そのユーザの権限を取得する可能性があります。更に、パスワードな しに管理者権限を取得する可能性があります。この問題は** OS **をバージョン** 7.6(1) **に更新することで解決します。ーー**2003.4.30　**ＪＰＣＥＲＴーー**

# いくつかの事例－３　電子メールソフト

- [1] CERT Advisory CA-2003-12 Buffer Overflow in Sendmail http://www.cert.org/advisories/CA-2003-12.html

sendmail には、電子メールアドレスの処理にバッファオーバーフローの脆弱 性があります。結果として、遠隔から第三者が管理者権限を取得する可能性が あります。この問題は、sendmail をバージョン 8.12.9 (またはそれ以降) に更新する、もしくはベンダや配布元が提供する修正済みのパッケージに更新するなどの方 法で解決します。

関連文書 (日本語) JPCERT/CC Alert 2003-03-31 新たな sendmail の脆弱性に関する注意喚起 http://www.jpcert.or.jp/at/2003/at030004.txt JPCERT/CC Vendor Status Note JVNCA-2003-12 Sendmail にバッファオーバーフローの脆弱性 http://jvn.doi.ics.keio.ac.jp/vn/JVNCA-2003-12.html Turbolinux Security Advisory TLSA-2003-24 バッファオーバーフローの問題　ーー2003.4.2　ＪＰＣＥＲＴーー

# いくつかの事例ー4　IIS

- [1] CERT Advisory CA-2003-09 Buffer Overflow in Core Microsoft Windows DLL http://www.cert.org/advisories/CA-2003-09.html CIAC Bulletin N-054 Microsoft Unchecked Buffer in Windows Component Could Cause Web Server Compromise http://www.ciac.org/ciac/bulletins/n-054.shtml

  Microsoft Windows 2000 に含まれる ntdll.dll には、バッファオーバーフローの脆弱性があります。結果として、遠隔から第三者が ntdll.dll を使用して いるアプリケーション (IIS 5.0 など) の実行ユーザの権限を取得する可能性 があります。※ 上記 CA-2003-09 の公開時のタイトルは「Buffer Overflow in Microsoft IIS 5.0」でしたが変更されました。この問題は、Microsoft が提供する修正プログラムを適用することで解決しま す。ただし、Windows 2000 Service Pack 2 を使用している場合には、注意が 必要です。詳細については、下記「関連文書」のうち、Microsoft による MS03-007 を参照してください。

  関連文書 (日本語) マイクロソフト セキュリティ情報 Windows コンポーネントの未チェックのバッファにより Web サーバーが侵害される (815021) (MS03-007) http://www.microsoft.com/japan/technet/security/bulletin/MS03-007.asp JPCERT/CC Alert 2003-03-18 Microsoft IIS 5.0 の脆弱性に関する注意喚起 http://www.jpcert.or.jp/at/2003/at030003.txt JPCERT/CC Vendor Status Note JVNCA-2003-09 Microsoft Windows DLL にバッファオーバーフローの脆弱性 http://jvn.doi.ics.keio.ac.jp/vn/JVNCA-2003-09.html

  ーー2003.3.26　ＪＰＣＥＲＴーー

# いくつかの事例ー5　ファイル共有

- [4] CIAC Bulletin N-055 Samba smbd Buffer Overrun Vulnerability http://www.ciac.org/ciac/bulletins/n-055.shtml

  Samba に含まれる smbd には、バッファオーバーフローの脆弱性があります。結果として、遠隔から第三者が root 権限を取得する可能性があります。対象となるのは以下のバージョンです。- Samba バージョン 2.0.x から 2.2.7a (2.2.7a を含む) この問題は、Samba をバージョン 2.2.8 (もしくはそれ以降) に更新する、または問題を修正したパッケージに更新することで解決します。※ 日本 Samba ユーザ会が提供している、Samba 日本語版 (2.2.7a-ja-1.0 およびそれ以前) にも同様の脆弱性があることが報告されており、既に この問題を修正したものとして、Samba 2.2.7a-ja-1.1 が公開されてい ます。

  ーー 2003.3.26　ＪＰＣＥＲＴーー

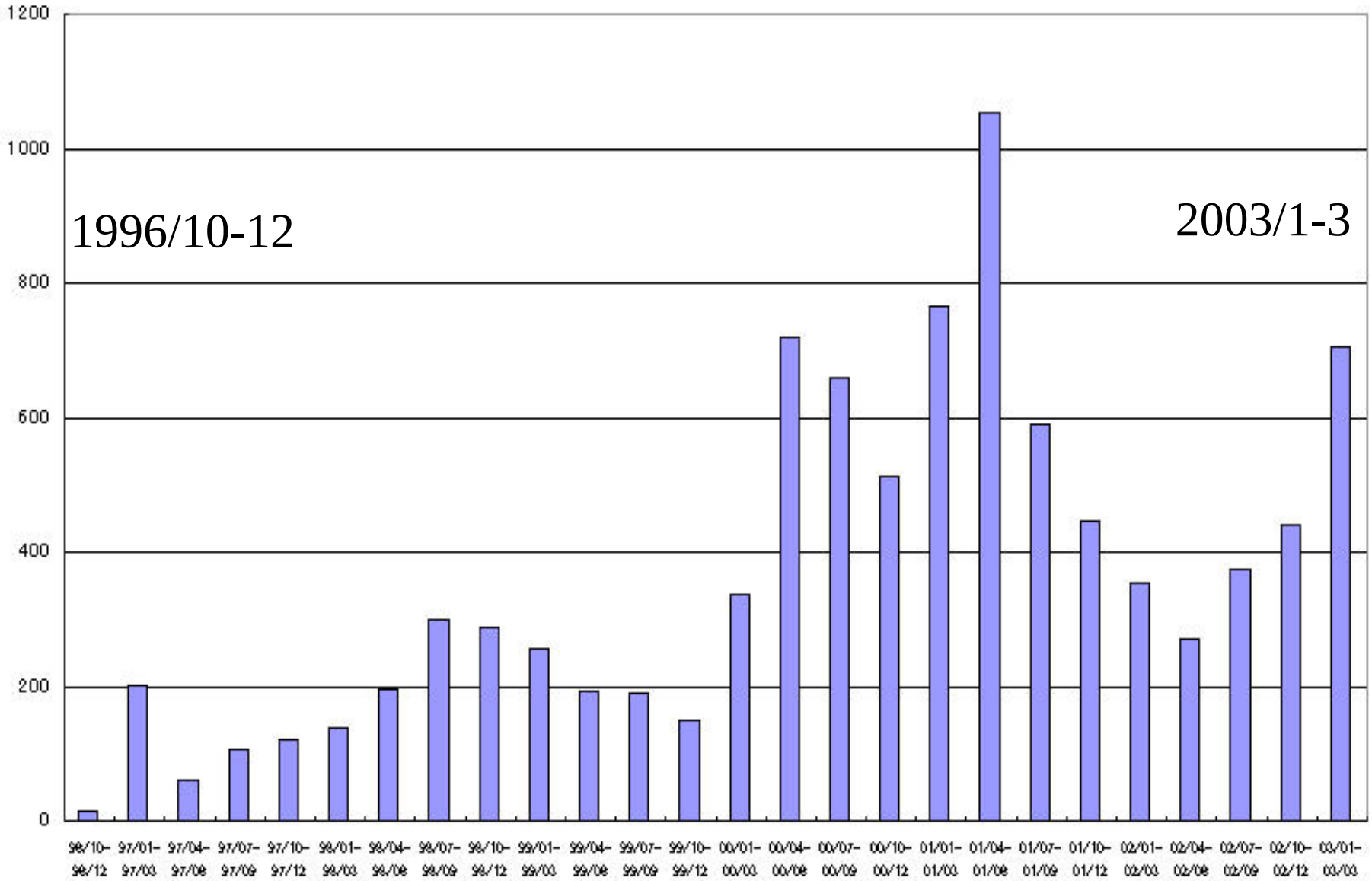
# いくつかの事例－6　データベース

- [1] CERT Advisory CA-2003-05 Multiple Vulnerabilities in Oracle Servers http://www.cert.org/advisories/CA-2003-05.html CIAC Bulletin N-046 Multiple Vulnerabilities in Oracle Servers http://www.ciac.org/ciac/bulletins/n-046.shtml

  Oracle 製品のいくつかには複数の脆弱性があります。結果として、遠隔から 第三者が Oracle サーバの実行権限を取得したり、データベースの内容を改ざ んするなどの影響を受ける可能性があります。対象となるのは以下の製品 (全 プラットフォーム) です。 - Oracle 8,8i,9i Database Server (8.0.x, 8.1.x, 9.0.1.x, 9.2.0.x) - Oracle9i Application Server (9.0.2, 9.0.3) ※ バージョン表記は日本オラクルのセキュリティ情報に基づいています。この問題は、Oracle が提供するパッチを適用することで解決します。 関連文書 (日本語) Oracle Technology Network - セキュリティ http://otn.oracle.co.jp/security/ JPCERT/CC Vendor Status Note JVNCA-2003-05 Oracle Server に複数の脆弱性 http://jvn.doi.ics.keio.ac.jp/vn/JVNCA-2003-05.html

  －－ 2003.2.26　ＪＰＣＥＲＴ－－

# JPCERT/CCが受理したインシデント報告件数の推移
# （セ キュリティ上の問題として捉えられる事象）



# 不完全を前提にセキュティ対策を

- **慶応大武藤教授** (2003-6-3)
  - 商用、オープンソースを問わず、OSとアプリケーションでは明らかに脆弱性の数に違いがある　(OSは高度なので手を加えられる技術者が少なく脆弱)
  - 全員が、完璧なソフト、完璧な仕組みなどありえないと認識することから始めなくてはならない。まずは“不完全である”と認めるべきだ
  - 同氏が批判するのは、現実に問題――大げさに過ぎるのであればリスク――が存在するにもかかわらず、それを積極的に認知させず、あたかも安全であるかのように見せかけるやり方だ
  - “こういった問題がある”ということを知り、その前提に立って使うことが重要だ。影の部分があることに触れた上で利益を語るべきではないか
  - 日本では政府を含め、とにかく守ることに力を注いでいる。しかし米国では9月11日のテロ事件の後、考え方が変わってきた。つまり、やられることを前提とし、そこからどう復帰させるか、リカバーするかがポイント
  - まず自らのシステムにどういった脆弱性があるかを検査し、どの程度リスクがあるかを把握しておく必要がある
  - 日本の仕組みは性善説に基づいたままだ。しかし、組織の内部犯行もありえるという性悪説に則って取り組みを進め、仕組み自身を変えていくしかない

# 用語解説

**種別：トロイの木馬**

増殖も自分のコピーもしませんが、データを損傷したり、セキュリティを危険にさらします。一般的に、何者かにより電子メールで送信されることを想定しており、自分で送信することはありません。ジョークプログラムまたは何らかのソフトウェアの形で届きます。

**種別：ウイルス**

感染対象となる媒体に自分自身を挿入または付着させることにより、他のプログラム、ブートセクタ、パーティションセクタ、マクロ対応のファイルに感染して増殖するプログラムまたは実行コード。ほとんどのウイルスは増殖するだけですが、中にはダメージを与えるものも多数存在します。

**種別：ワーム**

ハードディスクから他のハードディスクへ、あるいは、電子メールや他の転送メカニズムを介して自分のコピーを作成するプログラムで、コンピュータ上のデータを損傷したり、セキュリティを危険にさらしたりします。ジョークプログラムや何らかのソフトウェアの形で届きます。

**種別：ジョーク**

ユーザのコンピュータ上に様々な良性の現象を引き起こす無害なプログラム（予期せぬスクリーンセーバなど）。

# 住基コード占いページ　リンク

## 住民票コード占い(ベータ版)

お名前（フルネーム・カタカナ）

住民票コード（11ケタ）

占う　占わない

もどる

(since2002.8.14)

**騙されないように！！**

http://www.bb.wakwak.com/~■■■■/juminhyou-ur01.htm

# 中央集中管理から自治体主導の水平ネットへ

- 「住基ネット」の概念は古典的な中央集中型ネットワーク
  - 3段階のピラミッド構造　(市町村ー＞県ー＞国)
  - ならば、ただ1台だけのコンピュータに全ての情報を集め以下を徹底すべきであった
    - ・外部からの接続を完全に遮断し
    - ・限られた数の特定端末から
    - ・限られた人だけがアクセスしてこれを利用する
    - ・情報は外部に出さない　(現実には264組織の更なる拡大も)
- しかし、使う技術は開放型の水平・分散技術 (情報を秘密にしておく環境には適していない)
  - パソコン、Windows、インターネットなどの開放型技術
- 本質的には、一カ所に集めて強固にこれを守るのでなく、各自治体で分散管理し、必要に応じて「ネット」で問いあわせる。ー＞文字通り、住基ネットへ変更すべき