NEC e-Trend Conference 2005

ユビキタス情報社会のセキュリティ確保と法的保護

明治大学法学部教授
あすか協和法律事務所弁護士
夏　井　高　人

講演概容

- ユビキタス・コンピューティングの技術を応用して情報社会がさらに拡大されようとしている。次世代の情報社会は，従来の有線通信技術に加え，ローカルな場面での無線通信技術の多方面にわたる応用利用が拡大し，それらが相互にネットワーク接続される情報環境が想定されている。
- このような情報基盤の変化は，情報基盤を守るセキュリティのあり方や法的保護についても全面的な見直しと再検討を迫っているということが言える。例えば，有線通信主体の時代に可能であったトラフィックの集中監視による侵害行為の防止だけでは効果的な防御ができなくなることが想定される。無線通信環境では，どこからでも誰でも侵入可能だし，トラフィックの増大が監視能力の限界を超えてしまうからである。そして，監視能力の相対的な低下は，法的保護とりわけ法の執行の場面において深刻な悪影響を生じさせることが懸念される。そのことは，結果的に，情報セキュリティや法が保護しようとする対象（法的利益）である情報資産やプライバシーなどの保護についても無視できない重大な脆弱性をもたらすことにもなり得る。
- この講演では，ユビキタス技術を基盤として情報社会を構築する際に想定される様々なリスク要素をあげ，それらについて情報セキュリティの面と法的保護の面からどのような対応を考慮すべきかについて検討し，いくつかの提案を試みる。

ユビキタス情報社会の特徴

- プロバイダ，プロシューマ，消費者の格差が拡大する社会になる。
  - 情報の消費者はますます単純消費者になる。
  - 情報の単なる生産者は疲弊する。
  - 情報の優位者がさらに優位な地位を確保する。
- 情報通信が重要な社会インフラになる。
  - 在来型の通信手段が衰退・消滅し，代替手段の構築が困難。
  - 在来型の物的設備の転用。
  - インフラとしての運用・保護のあり方が異なる。
- 無線による電気通信が多用される。
  - 電波出力の大きさの限界によるネットワークの多重化
- 規模・機種・大きさ・形状に関係なくすべての種類の電子機器が情報端末となり得る。
  - 情報家電
  - 各種感性装置，制御装置等
- 双方向の通信の可能性が拡大する。
- 細分化されたIDが統一的に管理可能となる。
  - 情報機器のID，個人ID，RFIDタグなど商品のID，サービスのID
- 監視が容易になる。
  - 事業者による監視，警察による監視，犯罪者による監視

問題点

- 利用環境
  - 電力消費量の増加（特に待機電力）
  - 環境保護・省エネルギー政策との矛盾が拡大
- 利用意識
  - 家庭・個人の内と外との区別が不鮮明化
  - 社会的なモラル感覚の変容（土足で他人の家に上がりこむ）
- セキュリティ
  - 情報家電等では脆弱性の解消やセキュリティ対応が困難
  - 大規模なDDoS攻撃やコンピュータウイルスの大増殖が可能な環境
  - 事業継続性への重大な支障
- 法令順守
  - 個々の機器・サービスの製造・販売・提供・運用にまでは手が回らない
- 結果
  - 情報セキュリティや人権保護の要請と現実との間の齟齬が極大化

総務省：次世代IPインフラ研究会第一次報告書
バックボーンの現状と課題
（2004年6月7日）

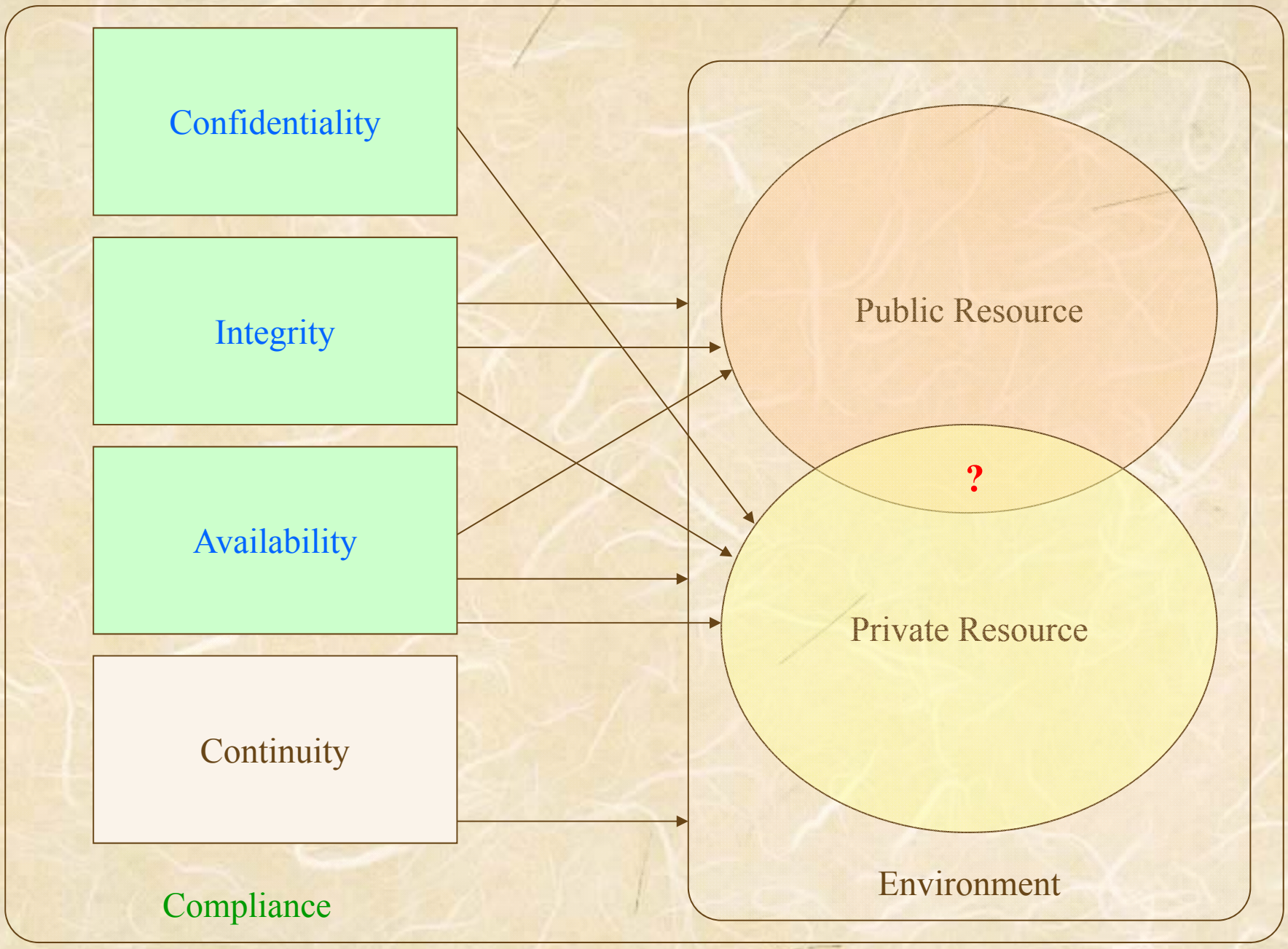
- ５　障害連鎖防止
  - インターネット全体の安定した運用を確保する観点から障害連鎖を防止するためには、①各ISP間の情報共有、②経路情報のフィルタリング、③経路情報等のデータベースであるIRRの活用が必要である。なお、このうちIRRについては、データベースの維持・更新・管理を随時行うこと等により、その信頼性を高めていくことが必要である。
  - 更に、ISPとして最低限守るべき運用方針やネットワーク品質の明確化については、現在JANOG等の任意団体において継続されている情報交換や技術交流が行われているが、事業を開始したばかりのISPやこれから事業を開始しようとするISPに対して、障害連鎖防止のための運用のノウハウを普及・啓蒙させていくための施策も必要と考えられる。
  - 端末設備側のセキュリティの向上も重要であり、端末設備やアプリケーション・ソフトそれ自体のセキュリティを高めるとともに、ISP、通信機器メーカ、システムインテグレータ等において、利用者のセキュリティ意識を高め、セキュリティ対策が適切に実行されるための方策を見出す必要がある。

具体例で考える

- RFIDチップ
  - 電力供給問題
    - *停電になれば何もできなくなってしまう*
  - 情報セキュリティ
    - *プライバシー侵害の懸念*
    - *個人情報保護上の困難性*
    - *無権限使用やサービス拒否*
  - 電波の混信等
    - *周波数帯の奪い合い*
    - *電波の相互干渉*
  - 製品の安全性保障
    - *重金属等の有害物質対策*
    - *粉塵被害等の防止*
    - *電波による身体への影響は本当にないのか？*
  - 環境保護・資源保護
    - *自然環境に対する影響は未知数*
    - *リサイクルは事実上不可能*

考え方の図式

- 経営倫理の基本
  - 適法な経営，製品開発と運用
- 個人情報保護
  - ユビキタス環境に対応する個人情報保護指針
  - 個人情報保護指針の周知と適正な運用
- 情報セキュリティ
  - 重要インフラと事業継続性の観点を基礎とする情報セキュリティ指針
  - すべてのタイプの事業者が電気通信事業者
  - 個人でも利用可能な超省エネ型のセキュリティ技術の開発
- 情報犯罪の防止
  - IDの偽装・偽造等の防止と検知・対応
  - 世界的な犯罪防止組織との連携
- 法
  - サイバー法とコンピュータ・フォレンジックス（Computer Forensics）
  - ユビキタス情報社会に対応可能な法律家（裁判官，検察官，弁護士）の養成
  - 警察による犯罪捜査機能の強化


Confidentiality
Integrity
Availability
Continuity
Compliance
Public Resource
?
Private Resource
Environment

ISO/IEC FCD 24743:2004-12-04

Information technology - Security techniques

Information security management system requirements specification

- **4. Abstract of objectives**
- The objective of this standard is to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS) this is designed to ensure adequate and proportionate security controls that adequately protect information assets and give confidence to customers and other interested parties.
- The standard is intended to be suitable for several different types of use, including:
  - use within organisations to formulate security requirements and objectives;
  - use within organisations as a way to ensure that security risks are cost effectively managed;
  - use within organisations to ensure compliance with laws and regulations;
  - use within an organisation as a process framework for the implementation and management of controls to ensure that the specific security objectives of an organisation are met;
  - the definition of new information security management processes;
  - identification and clarification of existing information security management processes;
  - use by the management of organisations to determine the status of information security management activities;
  - use by the internal and external auditors of organisations to demonstrate the information security policies, directives and standards adopted by an organisation and determine the degree of compliance with those policies, directives and standards;
  - use by organisations to provide relevant information about information security policies, directives, standards and procedures to trading partners and other organisations that they interact with for operational or commercial reasons;
  - implementation of a business enabling information security; and
  - use by organisations to provide relevant information about information security to customers.