

情報セキュリティの社会技術

土屋俊
(千葉大学)

情報セキュリティとは(古典的定義) (1992年、OECD)

- 利用可能性(Availability)
 - データ、情報および情報システムが、要求された方法で適時にアクセス可能かつ利用可能であること
- 秘匿性(Confidentiality)
 - データおよび情報が、正当と認められるときに、正当と認められる方法で、正当と認められる個人、組織、およびプロセスにのみ開放されること
- 一貫性(Integrity)
 - データおよび情報が、正確で完全であること

古典的情報セキュリティを実現する技術

- 利用可能性
 - バックアップ(ファイル二重化)技術、フォールトトレラント技術
- 秘匿性
 - 暗号、相手認証(なりすまし検出)、アクセス制御、デジタル署名、ファイアウォール構築技術
- 一貫性
 - 改竄検出技術、取引証明技術

これらはたしかに利用されてはいるが、予想されるほどには普及していない(なぜか?)

新しいセキュリティ概念(入替でなく追加)

(ISO/IEC JTC 1/SC 27)

- 追跡可能性(accountability)
 - 主体の行為からその主体にのみ至る形跡をたどれることを保証すること
- 真正性(authenticity)
 - 利用者、プロセス、システム、および情報、または資源の身元(identity)が主張通りであることを保証すること
- 信頼性(reliability)
 - 意図した動作と結果に整合性があること

システムへの要求ではなく、システムと利用者との関係への要求であることが特徴

情報セキュリティの技術の3レベル

要素技術・システム技術・社会技術

- 要素技術(特定個別の問題を解決する技術)
 - 暗号、公開鍵、フィルタリング、電子透かし、など
- システム技術(要素技術を組み合わせて、制約条件のもとで課題解決する技術)
 - 侵入阻止、個人認証、ファイアウォール、侵入阻止・探知
- 社会技術(現実の人間が関与する場面で基礎的技術を活用する技術)
 - 信頼・信用形成、ポリシー策定・実現、大規模シミュレーションによる予測

研究開発の現状

- 要素技術は、急速な進歩を遂げた。とくに、暗号技術の進歩は著しい。しかし、先端技術はそれほど活用されていない。
- システム技術も、近年、急速に開発されつつあり、製品も数多くでるようになった。しかし、有効に活用されているかは疑問(たとえば、ファイアウォール)
- 社会技術は、ほとんど手がつけられていない。しかし、これなしには現実の社会で情報セキュリティを実現できない

情報セキュリティの社会技術の4レベル

- 個人レベルの情報セキュリティ
 - 個人およびその情報環境に危害が加えられない
- 団体レベルの情報セキュリティ
 - 団体(会社、学校、地方自治体などの結社)がその目的の体制を持続的に行い得る情報環境が維持される
- 国レベルの情報セキュリティ
 - 国レベルの政治・経済の情報インフラがその機能を持続的に果たす
- 国際社会レベルの情報セキュリティ
 - 国際社会が平和に永続する情報インフラが確保される

情報セキュリティの実現が守るもの

- 個人レベルの情報セキュリティ
 - 個人の身体生命、情報環境、プライバシー、
- 団体レベルの情報セキュリティ
 - 団体(会社、学校、地方自治体などの結社)がその目的の体制を持続的に行い得る情報環境が維持される
- 国レベルの情報セキュリティ
 - 国レベルの政治・経済の情報インフラがその機能を持続的に果たす
- 国際社会レベルの情報セキュリティ
 - 国際社会が平和に永続する情報インフラが確保される

情報セキュリティの社会技術の特徴

- 同時進行的社会設計
- Social designとしての「社会技術」
- その対象
 - 法律、経済制度
 - 慣行、慣習、ポリシー、ガイドラインetc
 - 倫理、意識、考え方、態度
- 上記の具体的技術開発への反映

研究開発方法の特殊性

- 情報社会を捉える、国際的に通用する新しい概念の提唱
- それにもとづくセキュリティ概念、セキュリティ技術の開発と、セキュリティシステムデザインへの反映
- 多様な分野の若手研究者を中心にした取り組み
 - 情報学(計算機科学、人工知能、ネットワークなど)
 - 社会科学(法律、経済、社会学など)
 - 人文科学(哲学、倫理学、言語学、図書館学など)
 - 認知科学(心理学、社会心理学、人類学など)
- 成果の随時公開、コメント受付、随時修正

方法

- 人々の考え方、態度の調査
 - 定量より定性調査の重視
 - アンケート手法よりインタビューを重視する「深い調査」
- 実験的方法
 - 比較的大規模の社会実験
 - 行動科学、認知科学的実験室実験によるモデル設計
- シミュレーション
 - 意識や規範を組み込んだ社会・経済モデル
 - 意識や規範を反映したセキュリティ対策技術開発
- Request for Comments方式
 - 提案、提唱に対するパブリックコメントを求める (Web利用)

主な話題

- 「情報セキュリティに関する人々の意識のデザイン」
- 「情報セキュリティにおけるヒューマンインターフェイスのデザイン」
- 「情報セキュリティに関するポリシーとそのバランスのデザイン」
- 「情報化社会の人間活動予測に基づくセキュリティ対策モデルのデザイン」
- 「セキュアな世界実現のための社会モデルデザイン(社会レベル / 1 社会の枠を越えた国際レベル)」

現在の研究状況

- 情報インフラを信頼し、安心して社会生活を営めるようになる(個人レベル)チェックリスト
- セキュリティ意識が向上する(個人レベル)
- 不要な社会的利害対立に巻き込まれることなく情報技術を活用して、設立の目的を遂行できる(団体レベル)(企業は利益を、公共団体は公共サービスを)情報管理、公開、技術利用ポリシー、教育カリキュラム・方法・教材
- 社会的カタストロフィの回避(国レベル)
- 暗号政策の基本理念、(国際レベル)

インターネットの「匿名性」(信頼の根拠)

- 何を信じてよいのか
 - 名乗る必要のないコミュニケーション
 - 通常は、名乗る、顔を見せる、「生の」声を聞かせる
 - コミュニケーションの内容のみが真正性の保障
 - 状況要素が希薄になる
- 教訓：
 - 状況的内容を内容に含ませる
 - 署名は原則としてつける
 - 状況要素の明示化
 - ヘダー部を慎重に
 - 転送、返信などに配慮を(自分のコメントをつけるなど)

ヘダールの要素と注意点

- To:ここに羅列しない。
- Cc:誰が何を知っているかを知らせる
- Bcc:誰が何を知っているかを他人にしらせずに知らせる
- From:自分のメールソフトの設定できまる
- Subject:返信しないときは返信しない
- Date:時計は合わせる
- X-Mailer:文字化け解決のヒント
- Reply-To:思わぬ人に送らないように！
- Attachment:添付ファイルの種類を確認！

メール文化論

- 日本のメール
 - まず名乗る。
 - 用件を切り出す。
- 英文手紙の世界
 - まず呼びかける。
 - 最後に署名する。

聞き手がコミュニケーションの成否を支配することが大事

土屋です。

今日はもう10月なのに、ずいぶん暑い土曜日を過ごしています。来週中にお目にかかって、ご相談したいことがあるのですが、ご都合はいかがでしょうか。当方は、木曜日と金曜ならあいています。

返事をすぐください

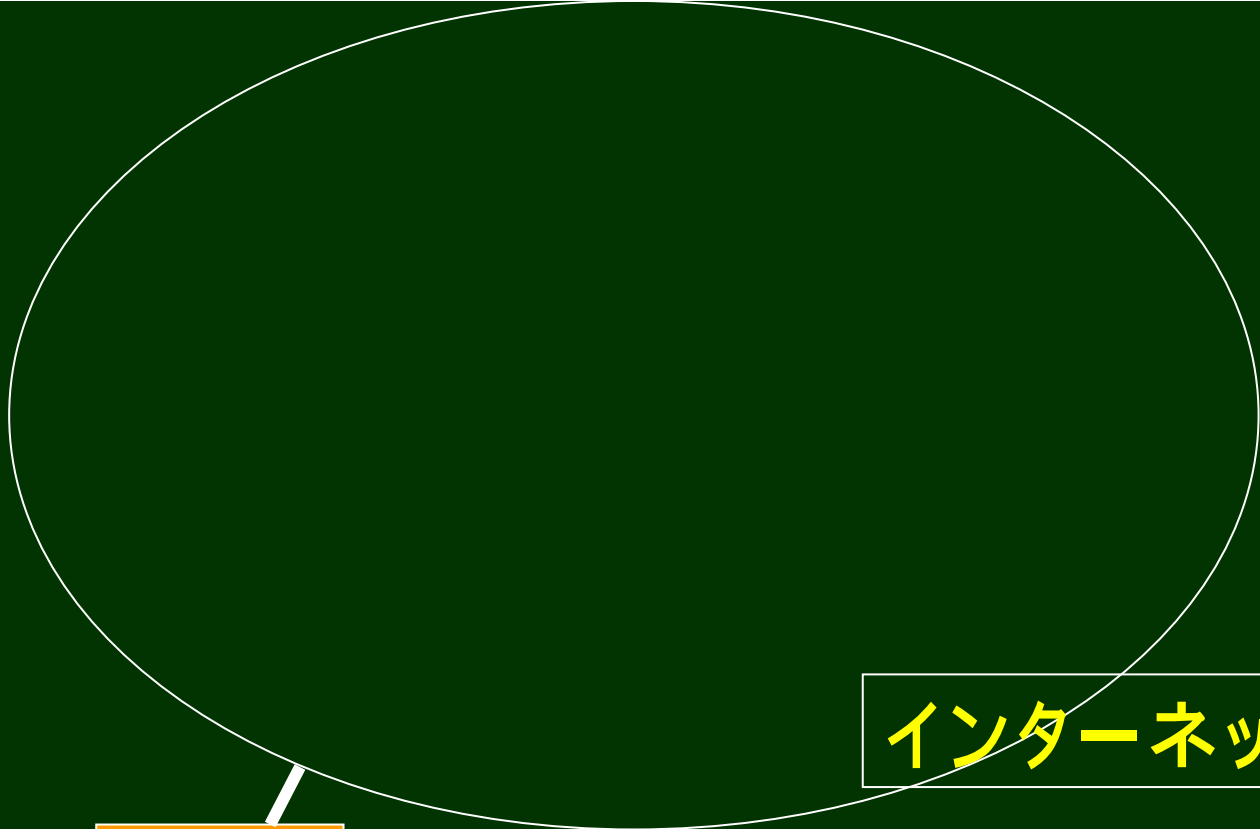
安西さん、

今日はもう10月なのに、ずいぶん暑い土曜日を過ごしています。来週中にお目にかかって、ご相談したいことがあるのですが、ご都合はいかがでしょうか。当方は、木曜日と金曜ならあいています。早めにお返事をいただければ、幸いです。

土屋

メールとプライバシー

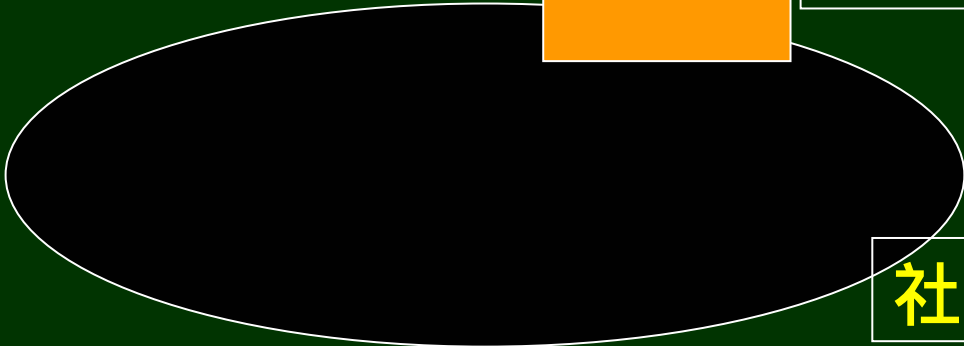
- 郵便・電話・電子メール
 - 事業法の整備がまだ不十分
 - 社会メールはsurveyable(ウェブ利用も同様)
 - したがって、電子メールに「信書の秘密」があるかはまだ、不明
- 相手に信用されるためには、プライバシーや個人情報の開示が必要？
 - 「裸になる」「裸の付き合い」
 - 顔をさらす
 - 電話番号を伝えるなど



インターネット



ゲートウェイ、ファイアウォール、各種サーバ



社内ネット

メーリングリストとフレームアップ

- Frame up でなく、Flame up
 - (もともとは、USENET Newsでの傾向)
 - メーリングリストは発火点が低い
 - 一人の人が犠牲者か、攻撃者になる傾向
 - 発言をやめると撤退とみなされて、残りの人に敗北と認識される(つまり、いい続けたほうが勝ち)
- 考えられる原因
 - 引用の容易さ(推論つきで理解しないで反応)
 - 別チャンネルによる参入手続きの不在
 - コミュニケーションの維持のみが存在を保証
 - 再参入手続きの不在

携帯電話の将来

- 機械が個人に属しているに思えるので、インターネットメールよりも「パーソナル」。同じ理由で、電話よりも「パーソナル」
- したがって、個人的コミュニケーションに中心になる(だろう)
- ここから、モバイル・ユビキタスへの展開？
 - 情報から知識への移行が困難
 - 「文書」を構築しない
 - その場限りの情報伝達
 - PDAも不十分か

情報の管理社会

- バーチャル・コミュニティ論、グローバル・ビレッジ論、ボランティア社会論など
- デジタルデバイド(情報格差が所得格差をもたらす)
- 情報の偏在化と「資本主義」の進行
 - 巨大メディアは存続
 - テレビネットワーク
 - メディア産業の独占傾向
 - 学術雑誌の独占傾向
 - アメリカへの情報集中
- そしてさらに、

情報セキュリティポリシーの社会技術

- ポリシー: 「一貫した態度」
- 情報セキュリティポリシー: 情報セキュリティに関する一貫した態度
 - 主として、団体、結社について
- 「慣習」とは違う: 明文化が必要
- [法律]とは違う: 策定手順は非民主的で、違反に対する制裁には法的強制力はない(「追放」などの制裁はある)
- 「倫理」とは違う: 個人が衡量する余地はない([倫理綱領]に近いが、厳密には違う)

その内容(結社の正確で多様)

- 結社の一員として要求される情報の利用方法に関する方針
 - 端末の利用
 - ネットワークの利用
 - サーバの利用
 - 外部との通信
 - 文書管理
 - 個人利用・プライバシー

ポリシーの実装(企業の場合)

- 服務規律、研修、テスト、資格
- Chief Information Security Officerの任命
 - そのもとに階層的構造のグループ化
 - 表彰と制裁
 - 対外的窓口の設定
- 倫理的問題との調整
 - プライバシー(ワークプレイス・サーベイランス)
 - 職能倫理
- 法律との調整