ＩＡＪセキュリティフォーラム　2002.11.7

情報セキュリティにおける法的責任

～個人情報保護、電子署名制度を中心に～

概要　　情報の取り扱いが重要なテーマとなっている。「物」の取り扱いと異なり、情報そのものをどう守るか、が問われる。個人情報処理の過程での漏洩事故が多発し、対策が急務とされる。より合理的対策の体系として、電子署名制度などの確立が求められている。

ポイント

情報セキュリティの重要性
　情報の価値、情報破壊にまつわる被害の拡大

　存在を覚知できない・・・どう認識し、管理するのか
　　管理されているかの監督は、誰が、どうやって？
　テクニカル・ギャップに対する対処は

情報セキュリティの問題点・課題
　情報の適正管理ということ
　　個人情報の価値の把握
　　個人情報の利用形態
　　個人情報の適正管理とは

　事故の事前対策ができているのか
　　どのような事前対策が考えられるか
　　免責

第１　個人情報漏洩を中心に

１　情報漏洩のポイント

個人情報の価値

客観的な価値　　交換価値　情報売買の裏マーケットが存在する事実
ネットの中で、誰でもが売主になれる

司法判断による価値
交換価値や、実質的財産損害ではない

むしろ、プライバシー侵害を中心にした精神的損害（慰謝料）などを中心に構成

☆　２００２年1月１６日　東京高等裁判所　第１事件

早稲田大学（東京都新宿区、奥島孝康総長）が 1998 年 11 月に中国の江沢民・国家主席を招いて開催した講演会の参加者名簿 1400 人分を、本人に無断で警察に提供したのはプライバシー侵害行為だとして、早大生ら 6 人が早大を相手に総額約 198 万円の損害賠償を求めていた事件。東京高裁は 16 日、学生側の訴えを棄却した昨年 4 月の東京地裁（加藤新太郎裁判長）の判決を取り消し、早大に対して１人あたり１万円の支払いを命じる逆転判決を言い渡した。判決では、「同意を得ずに名簿を警視庁に提出した行為はプライバシー侵害にあたる。あらかじめ同意を得ようとしなかったのは大学の手抜かりで、配慮に欠ける」と判示

１審判決　早稲田大学江沢民講演会名簿提出事件
（東京地裁平成１３年４月１１日判決判時１７５２号３頁）

プライバシー侵害を認め、被害が抽象的だとして、警察への提出は社会通念の範囲内だとして適法と判断していた。

☆7月１７日　東京高等裁判所　第２事件

前記同内容の事件で、元学生３人が計３３０万円の損害賠償を求めた訴訟の控訴審で、東京高裁は請求を棄却した一審東京地裁判決を支持し、訴えを退けた。

雛形要松裁判長は「個人識別の単純な情報であり、警備に万全を期すという目的のために名簿を提出したのは正当」と認定した。

高裁判決は判断が分かれるという結果となった。

2　個人情報漏洩の基本構造

①　わが国の産業構造

発注者（無責任・管理能力なし、処理能力なし）

受注者（合理化して、ほとんど外注=商社機能＝手配師機能のみ）

ひどいときは自分が下請け発注した企業すら正確に把握せず、

まして、孫に関しては、一切認識していないことが多い

下請け企業　小規模商社（実質は取次店）

孫受け　　企業としての実体がない・・・アルバイト集団

派遣社員による構成

②　情報処理の万全対策のためのバックアップ

受注者、下請け企業、孫請け企業、担当アルバイトなど全員が

無断バックアップ

情報処理後、バックアップのみ返納することなく、留保・・・漏洩

③　秘密保持義務契約・情報処理に関する合意があるのか

そもそも、発注書・受注書、納品書で完結していることが多い。

契約書など作っていない。利用しているのは、他企業の意味不明の契約書

のコピーであることも多い。

秘密保持の必要性、重要性の認識がまったく存在しない。

④　法的責任と対策

個人情報保護法案における委託先管理義務

情報アウトソーシングの場合の法的責任

京都・宇治市事件を参考に

京都宇治市個人情報漏洩事件

京都宇治市の個人情報21万7617人分の漏洩事件が発生した。

宇治市が児童健康診断用にシステムを構築すること、それに対応して市民のデータ処理を行うべく住民データの打ち込みを行う作業を外注したところ、複数の外注先の内１社が、これを受注したものの、守秘義務契約など締

結しなかった。右下請け企業は、さらに同作業を孫請け企業発注し、その代表者とアルバイト学生が作業中、データ処理に時間を要した為、住民情報データをMOにコピーの上、持ち出し、孫請企業社屋で作業した。そのとき学生アルバイトが、このデータをコピーして、当該名簿を２５万８０００円で名簿業者に販売した。この業者は同データを加工、選別して、女性適齢期名簿、一人暮らし名簿等を作成、結婚相談所、婚礼衣装業者、名簿業者などに順次転売し、さらには同事業者がネット販売を行ったという事件。

京都地裁平成13年3月は、宇治市と企業に対して賠償責任を認め、被害者である市民1名あたり1万円の損害賠償請求、弁護士費用5000円を認める判断を行い、その後平成13年12月大阪高裁は１審判決を支持、その後宇治市は上告するも最高裁はこれを認めず、判決確定。

・公開されている情報もあるが、明らかに個人的な公開されたくない情報も含まれていた。公開されていない情報、公開を欲しない情報に対してはプライバシーの保護が必要。
・誰でも閲覧できる情報にプライバシーはあるのか、については、請求者への事実上の制限、違法な閲覧禁止、取扱者による取得情報の濫用禁止、刑罰もあり、無制限公開ではなく、プライバシーであることを減殺しない。
・電話帳などで公開されている、としても限られた情報であって、電話帳情報を大きく超えるものであって、適法化しない。
・プライバシー侵害の有無
　・流失による具体的被害は指摘されていない
　・ネットによる不特定多数への販売は実現しなかった
　・しかし、今後の危険性は残る
　こうした事態が発生したことに、権利侵害がある。
・管理責任　使用者と被用者の実質的指揮監督関係の有無で判断
　　請負か委託か、といった形式論は重要でない
　　結局秘密保持契約がない、持ち出しを容認していた

第２　情報セキュリティの総合的対策

宇治市による改善策・対応策

アクセスコントロール

パイプ論

アクセス権限者認証　　アクセス記録の保持

情報の読み取り制限　　暗号化による解読制限

情報と個人の結びつき（個人認証）　　紐つけ論

情報そのものと権限との結びつき

個人の存在の確認と権限との照合

属性認証

第３　電子署名制度

１　電子署名制度の必然性

ＩＤ･パスワード神話の崩壊

既にＩＤ・パスは、氏名表示と同レベルに低下している

パスワードへの過信は危険である

生年月日、電話番号・・・・忘れない為の工夫は皆同じ

難しいパスワードはすぐ忘れ、ハードディスクのフォーマットなど、重要情報の抹消を意味しているのではないか？

本人であることの確認を第三者に委ねる仕組み

本人確認作業とアクセスコントロールの役割分担（分散処理）

確実性、客観性の第三者保証　　電子認証、認証局（登録局）の作業

この他にも電子公証の仕組みもある

結論　誰でも簡単に、安全に、利用できる本人確認、アクセス権限確認、意思確認のシステムを作る必要があること。

どう作る、だれが判断する、本当に安全？

2　電子署名の本質

データと人との紐付けと、データへの人の許容、データ内容の安全性確保を保証する制度

個人、法人について、第三者がその個人、法人の存在自体を確認・認証して、その申請内容に従って存在を証明する業務を行い（認証業務)、証明された本人（個人、法人）が、自らの意思表示やデータへのアクセスについて、自己の秘密鍵を利用して署名（電子署名）し、あるいはアクセス申請し、その証明された証明書によって第三者が本人であることを確認する（検証）ことで、真正な本人作成のデータであると認識できるという仕組み。

現行制度の限界？

・認証局が鍵を生成、ＰＧＰなどによる自己生成鍵の利用は制度として視野に入っていないと思われる。分散処理ではこまるとされている点（認証・証明の確実性･被告適格が保証されないのではないか、ＣＲＬ管理など）
・秘密鍵の管理は安全にできているか
・ＩＣカードは安全か、使いやすいか、経済性はどうか
・携帯電話との接合

3　課題

利用できるアプリケーションが少ない
安全性は高いが、使いにくい
ＩＣカードの重要性が増せば、ますます使えなくなる
目的別の分散処理か

わかりにくい
専門用語が多すぎる
従来業務との接合も、移動の必要性も、便利さもはっきりしていない

4　展望

情報処理技術と証拠保全

電子公証制度の発展

契約書、議事録、覚書、通信内容、電子メール、などの各種データの保存

商業登記簿を基礎におく公証制度に内在する課題

5　電子的処理の必要性

データ処理が基本となりつつあるという実態の存在

大量のデータの保存、大量の形式データの立証などに最適

多数の人の処理が加わったときのデータ保存と、記入の前後、権限の有無の確認が必要なとき

6　属性証明の発展が鍵

存在証明は、実はあまり役に立たない　　裁判は起こせるが・・・・

属性証明と保険とが接合して初めて実用化するのではないか

属性情報とは

法人の信用情報、権限･免許、歴史、手形情報、金融情報など

個人の資格、権限、地位、支払能力、第三者の支払保証など

存在証明に属性情報が付加される仕組みが必要だろう

以上