資料４

プラットフォームビジネスと情報セキュリティ

弁護士･国立情報学研究所客員教授
岡村久道

情報セキュリティ（Information Security）

	意　義	侵害の典型例
機密性（Confidentiality）	アクセスを認可（authorized）された者だけが、情報にアクセスできることを確実にすること	情報の漏えい
完全性（Integrity）	情報および処理方法が完全かつ確実であることを保護すること	情報のき損・改ざん行為
可用性（Availability）	許可された利用者が、必要な際に情報および関連資産にアクセスできることを確実にすること	情報のき損・滅失

- 情報セキュリティとは、情報の①機密性、②完全性、③可用性の確保（3要素の頭文字を取って「CIA」という言葉で総称）という意味。
- 1992年のOECD情報セキュリティガイドラインに登場
  - その後の情報セキュリティマネジメントの英国規格である「BS 7799　パート1」、それをベースに国際標準化した「ISO/IEC 17799」、さらに日本国内標準化した「JIS X 5080」、JIPDEC「ISMS認定基準Ver.2」でもほぼ共通
  - 1980年のOECDプライバシーガイドラインの「安全保護の原則」がベース
- 2002年の改訂OECD情報セキュリティガイドライン
  - 情報システムをとりまく環境は劇的な変化を迎えたとして、個人も含めて新しい情報社会のすべての参加者がセキュリティの担い手（「セキュリティ文化」の提唱）
- 法律もシステム運営者やデータ利用者に責任を負わせる方向へ

情報セキュリティと法律

- 情報セキュリティ概念は技術に由来しているので、法律との整合性に関する議論に乏しい
- 国際標準のISO/IEC 17799 なども法律領域を前提にしていない。元になったBS7799は一定限度英国の法律に触れていたが、ISO化する際に除去して2つに分け、パート1がISO/IEC 17799となった。
- これまで法律領域は独自に情報セキュリティ侵害行為を規制してきたこれまで法律領域は情報ではなく物を対象に組み立てられてきた
  - フロッピーを盗むと窃盗罪で有罪だが、データだけコピーして持ち出しても窃盗罪にならない
- 最近では、法律で、システム運営者に情報セキュリティを守るべき責任を負わせる傾向にある　←具体例：個人情報保護法（後述）
- しかし、法律でシステム運営者に課せられた情報セキュリティを遵守するために、何をどうすればいいのか分からず、これから混乱が広がる可能性がある。
- 他方、技術領域でも、これから法律を念頭に置いて進めることが必須であるが、この点に関する啓蒙が進んでいないこともあり、法律違反のセキュリティポリシーすら見受けられる状況にある。

個人情報保護法と情報セキュリティ

- 個人情報保護法は、対象を個人データに限定しつつ、CIA全体を保護
- 管理する側に責任を持たせる
- 個人情報漏えい事故などでは、純然たる外部者の不正行為よりも、従業員など純然たる内部者、もしくは委託先によるケースが大半を占めていることを踏まえ、第21条（従業者に対する監督）および第22条（委託先に対する監督）が置かれた。
- 現行法は管理する側に責任を持たせるが、不正漏えい行為に対する直罰規程の導入に向けた法改正を検討中

第２０条（安全管理措置）

個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人 データの安全管理のために必要かつ適切な措置を講じなければならない。

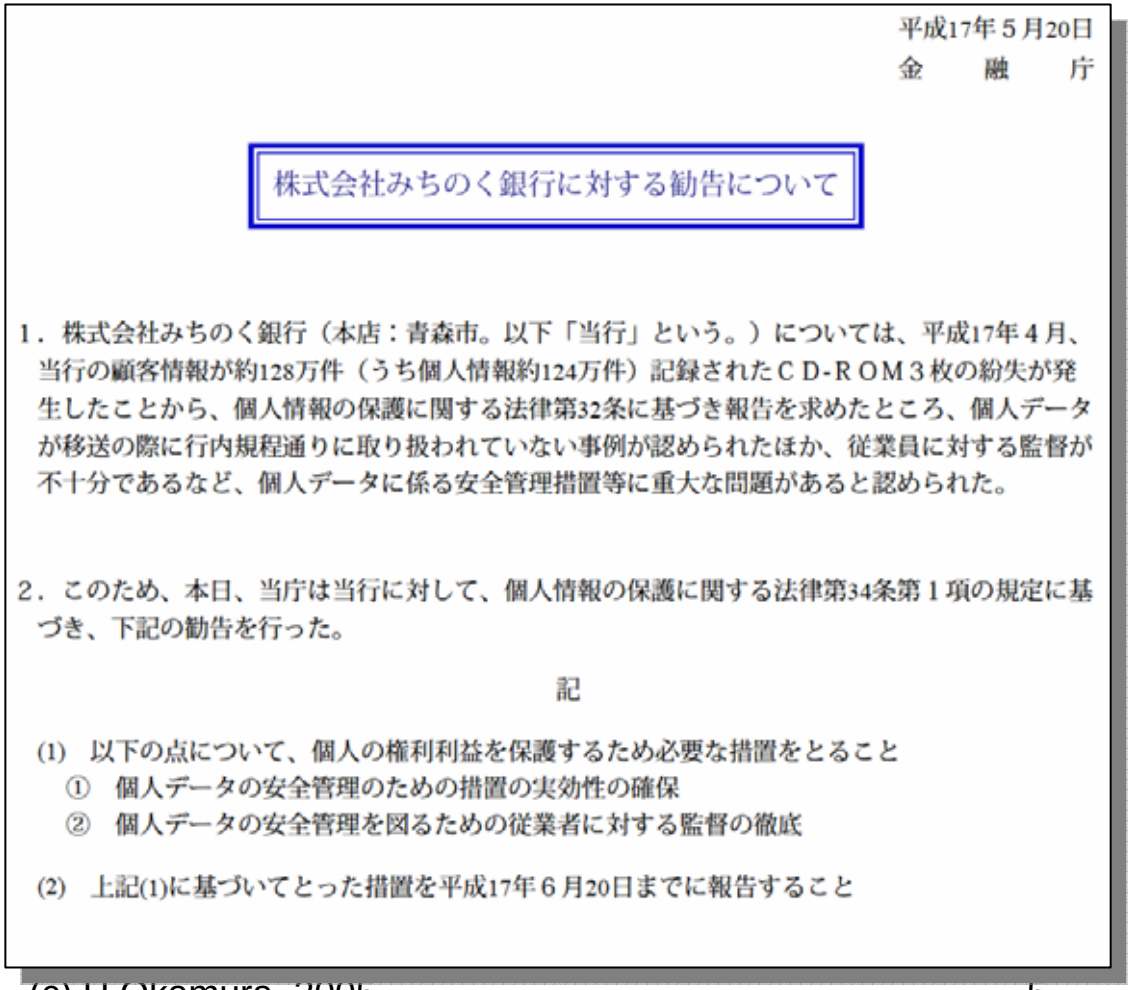
第２１条（従業者の監督）

個人情報取扱事業者は、その従業者に個人データを取り扱わせるに当たっては、当該個人データの安全管理が図られるよう、当該従業者に対する必要かつ適切な監督を行わなければならない。

第２２条（委託先の監督）

個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない。

- 個人情報保護法の実効性担保は、主として主務大臣の関与による。
- すでに金融庁が漏えい事件につき、全面施行後初の勧告を行っている。
- 間接罰にとどまる点、具体的な通信に関連していることを要しない点で、通信の秘密と異なる。



平成17年５月20日
金　　融　　庁

株式会社みちのく銀行に対する勧告について

１．株式会社みちのく銀行（本店：青森市。以下「当行」という。）については、平成17年４月、当行の顧客情報が約128万件（うち個人情報約124万件）記録されたＣＤ-ＲＯＭ３枚の紛失が発生したことから、個人情報の保護に関する法律第32条に基づき報告を求めたところ、個人データが移送の際に行内規程通りに取り扱われていない事例が認められたほか、従業員に対する監督が不十分であるなど、個人データに係る安全管理措置等に重大な問題があると認められた。

２．このため、本日、当庁は当行に対して、個人情報の保護に関する法律第34条第１項の規定に基づき、下記の勧告を行った。

記

(1)　以下の点について、個人の権利利益を保護するため必要な措置をとること
　①　個人データの安全管理のための措置の実効性の確保
　②　個人データの安全管理を図るための従業者に対する監督の徹底

(2)　上記(1)に基づいてとった措置を平成17年６月20日までに報告すること

止まらない個人情報流出　全面施行前１

発覚時期	事件の概要
2004年1月	大手消費者金融から顧客情報約116万人分が漏えい。
2月	ブロードバンド接続サービスの全顧客約660万人分とIP電話通信記録約140万件漏えい。
3月	テレビ通販大手から顧客情報約30万人分が漏えい。
3月	プロバイダから顧客情報約34万人分が漏えい。
3月	鉄道会社のメール会員データ約13万人分流出。
3月	飲料会社のモニター応募者情報７万5000人分が名簿業者に流出。
3月	外資系銀行の日本の支店の約12万口座分の記録が外部漏えい。
4月	信販会社のカード会員約10万人分の情報流出。
4月	石油会社のカード会員情報最大92万人分流出。
6月	旅行代理店から顧客情報約62万人分が流出。
8月	クレジットカード会社から会員情報約48万人分が流出。
8月	大手中学受験塾から模試受験の小学生らの個人情報18万人分流出。

止まらない個人情報流出　全面施行前2

発覚時期	事件の概要
2004年8月	自動車メーカーから中古車保証サービスの加入者情報約4万人分流出。
11月	愛知県の村役場でパソコンが盗難され住民記録4400人分流出。
12月	ヨン様など韓国芸能人の個人情報がネットで大量流出。
12月	ブロードバンド接続サービスの全顧客約660万人分とIP電話通信記録約140万件漏えい。
12月	カタログ販売大手が顧客情報4418件入りPC紛失
2005年1月	大手テーマパークが年間パスなど個人情報14万人分が流出した可能性があると発表。最終的には16万人分と判明。
1月	個人情報約3万件を保存したPCが札幌市保健所で盗難
1月	化粧品会社のホームページから不正アクセスにより顧客情報約5万9000人分が流出。
1月	医師が患者情報1万4000人分を持ち出したとして横浜市が告訴へ。
2月	信託銀行が学生506人分のメールアドレスを誤送信。

止まらない個人情報流出　全面施行後

発覚時期	事件の概要
2005年4月	地方銀行が国内の全顧客約131万件の顧客情報を紛失。
5月	大阪府八尾市が所得額など個人情報を含む「市民税・府民税特別徴収税額決定通知書」1万686人分を盗まれた。
5月	岐阜県大垣市が水道利用者情報約2万人分入りの磁気テープを紛失。
5月	パソコン教室から社員（休職中）が受講生らの個人情報131人分入りファイルを持ち出し、ネットの個人情報売買業者にメール送信。
5月	価格比較サイトから不正アクセスでアドレス2万2000件流出。
5月	製薬会社で個人情報2万3444名分を含むパソコンが盗難。
6月	電話会社が業務委託先で顧客情報約8万4千件入りUSBメモリを紛失。
6月	信託銀行が顧客情報十数万人分を紛失。
6月	愛知県一宮市立小学校の2003年度の全児童535人分と教職員約30人分の個人情報などがWinny経由でネット上に流出。
6月	熊本の私立大学が学生情報4万2000人分を紛失。
6月	マスターカードのクレジットカード情報4000万枚分以上が流出

個人情報の流出原因

- 車上荒らし被害
  - マンション管理会社の社員が車上荒らしで、管理する12棟409戸のマンション在住顧客の個人情報74件分が記載された書類を鞄ごと盗まれた(05/6/2)
  - たばこ会社の社員が車上荒らしで、たばこ販売店の個人情報74件分が記載された書類を鞄ごと盗まれた(05/6/3)
- 紛　失
  - 自動車ディーラーが顧客情報が記載されたリストを紛失 (05/6/3)
  - 熊本の私立大学が在学生と卒業生の個人情報を保存した業務用デスクトップ型パソコン1台を紛失 (05/6/3)
- 駐車場に置き忘れ
  - 百貨店の外回りの営業社員が、顧客名簿の入ったカバンを駐車場に置き忘れた (04/06/15)
- 電車の網棚に置き忘れ
  - 信託銀行営業職員が顧客情報入りカバンを電車網棚に置き忘れた (04/5/6)
- 誤って渡す
  - 銀行が支店において取引先の学校宛の書類の中に、誤って別の学校宛の書類を混入して渡す (05/4/22)
- 酔って寝込む
  - 酔った名古屋市内の税務署員が雑居ビルの階段で寝てしまい、目を覚ましたときにはパソコン用携帯メモリー入りカバンがなくなっていた (04/7/8)

機密性（Confidentiality）と刑法

- 機密性侵害の典型例は情報漏えい。
- 情報が載った他人の管理する有体物、つまり紙などの物理媒体を無断で持ち出して漏えいした場合には、刑法の窃盗罪が成立。情報が載った自己の管理する他人所有の有体物を持ち出したときには、刑法の業務上横領罪が成立。事前に共謀するなどして犯人に加功した者には共犯が、事後に当該媒体を犯人から譲り受けた者には盗品譲り受け等の罪が成立。
- ここでは、媒体という有体物に対して直接的な保護を与えることによって、それに載った情報が反射的に保護されているにすぎない。しかし、こうしたケースで価値があるのは情報そのもの。情報を保護する目的で、無価値に等しい紙切れなど媒体を保護するという方法を借用することは、きわめて不合理であり、技巧的にすぎる。
- 実際的な不都合も発生。まず、自ら持参した媒体にデータだけを無断コピーして持ち出した者には、これらの罪が成立しない点で限界。データ自体はこれらの罪の客体たる「財物」や「物」に該当せず、自ら持参した媒体も「他人」の財物や物にあたらないから。次に、無断で機密データをネットで外部送信する行為など、媒体と情報とが切断されている場合には、情報だけを保護することができない。
- こうした見地から、故意にデータを無断で持ち出す行為を「情報窃盗」として位置付け、立法で処罰規定を新設することを検討。ところが、実際に報道された個人情報漏えい事件を分析すると、むしろ過失による漏えい事件が大部分を占め、こうした過失のケースに対する歯止めにはならない。

機密性と民事責任

- 機密性侵害に対しプライバシー権侵害に該当するとして民事責任を負わせる。
- 故意･過失を問わず、不正行為者だけでなく管理者にも民事責任を負わせることが可能。
- 宇治市住民基本台帳データ流出事件の大阪高裁平成13年12月25日判決
  - 宇治市民の住民基本台帳データ約19万人分等を再々委託先アルバイト学生が漏えいしたことがプライバシー権侵害に該当、市が学生と実質的な指揮監督関係にあったことを理由に、使用者責任に基づく損害賠償義務を認める。
- 捜査情報漏えい事件の札幌地裁平成17年4月28日判決
  - 当時少年であった原告を被疑者とする捜査情報が、コンピュータウイルスへの感染により、北海道警察の警察官が私有するパソコンからインターネットを通じて外部流出した事故につき、被告北海道の損害賠償責任を認めた。

不正競争防止法による営業秘密の保護

- この法律では、①秘密管理性、②有用性及び③非公知性という3要件をすべて満たす必要がある。
- 要件①の判断基準として次の点を掲げる判例が多い。
  (1)当該情報にアクセスした者に当該情報が営業秘密であることを認識できるようにしていること（客観的認識可能性）
  (2)当該情報にアクセスできる者が制限されていること（アクセス制限）
- さらに具体的な認定要素として、コンピュータ処理用顧客データ社外持ち出し事案の判例では、パスワード等によるデータへのアクセス・閲覧制限、データのコピー・出力等の規制、保管場所の施錠・入退室制限、就業規則等による機密保持義務条項、社内教育・指導による周知徹底等の有無が総合的に判断される傾向

情報セキュリティ管理策を講じていなければ保護されないことに注意

不正競争防止法第14条第1項が定める営業秘密に関する罰則

号（類型）	行為類型	具体例（顧客名簿データが営業秘密に該当する場合）
第3号（不正取得・横領ケース（詐欺・窃盗類型1））	詐欺等行為により、又は管理侵害行為により取得した営業秘密を、不正の競争の目的で、使用し、又は開示	○競合他社から産業スパイが盗んできた顧客名簿データの購入者が、これを使用
第4号（不正取得・横領ケース（詐欺・窃盗類型2））	前号の使用又は開示の用に供する目的で、詐欺等行為又は管理侵害行為により、営業秘密を次のいずれかに掲げる方法で取得 イ　保有者の管理に係る営業秘密記録媒体等を取得すること。 ロ　保有者の管理に係る営業秘密記録媒体等の記載又は記録について、その複製を作成すること。	○競合他社に売却する目的で、顧客名簿データ入りフロッピーディスクを窃取（イ） ○競合他社に売却する目的で、フロッピーディスクの顧客名簿データを無断コピー（ロ）
第5号（不正取得・横領ケース（横領類型））	営業秘密を保有者から示された者であって、不正の競争の目的で、詐欺等行為若しくは管理侵害行為により、又は横領その他の営業秘密記録媒体等の管理に係る任務に背く行為により、次のいずれかに掲げる方法で営業秘密が記載され、又は記録された書面又は記録媒体を領得し、又は作成して、その営業秘密を使用し、又は開示 イ　保有者の管理に係る営業秘密記録媒体等を領得すること。 ロ　保有者の管理に係る営業秘密記録媒体等の記載又は記録について、その複製を作成すること。	○委託先従業員が、管理を委託された委託元の情報システムから、顧客名簿データ入りフロッピーディスクを無断で持ち出して競合他社に売却（イ） ○委託先従業員が、管理を委託されている委託元の情報システムから、顧客名簿データを自己所有のフロッピーディスクに無断コピーして持ち出し、競合他社に売却（ロ）
第6号（不正使用・開示（背任類型）ケース）	営業秘密を保有者から示されたその役員又は従業者であって、不正の競争の目的で、その営業秘密の管理に係る任務に背き、その営業秘密を使用し、又は開示（前号に掲げる者を除く。）	○取締役が、自社の顧客名簿データを、自己の経営する競合他社の宣伝広告用ダイレクトメール送付用宛名データとして無断使用

備　考

・「詐欺等行為」とは、人を欺き、人に暴行を加え、又は人を脅迫する行為をいう。

・「管理侵害行為」とは、営業秘密記録媒体等の窃取、営業秘密が管理されている施設への侵入、不正アクセス行為その他の保有者の管理を害する行為をいう。

・「営業秘密記録媒体等」とは営業秘密が記載され、又は記録された書面又は記録媒体をいう。

・「不正アクセス行為」とは、不正アクセス禁止法第3条に規定する不正アクセス行為をいう。

・「役員」とは、理事、取締役、執行役、業務を執行する無限責任社員、監事若しくは監査役又はこれらに準ずる者をいう。

※すべて親告罪（第14条第2項）。なお上記類型名は経済産業政策局知的財産政策室「不正競争防止法の一部を改正する法律案概要」に従った。

伝統的な機密性保護の中心は通信の秘密保護

法律名	保護対象	義務の対象	禁止行為	知得	漏えい	窃用	罰則
電気通信事業法	電気通信事業者の取扱中に係る通信の秘密（第４条第１項）	限定なし	侵してはならない	○	○	○	○（電気通信事業従事者には特に罰則加重）（第104条）
同　上	電気通信事業者の取扱中に係る通信に関して知り得た他人の秘密（第４条第２項）	電気通信事業に従事する者（退職後も同様）	守らなければならない	× **但し「通信の秘密」に該当するものは上記のとおり保護**	○	○	×但し「通信の秘密」に該当するものは上記のとおり罰則の対象
有線電気通信法	有線電気通信の秘密電気通信事業法適用の通信を除く）（第９条）	限定なし	侵してはならない	○	○	○	○（有線電気通信の業務従事者には特に罰則加重）（第14条）
電波法	特定の相手方に対して行われる無線通信（電気通信事業法適用の通信を除く）（第59条）	限定なし（何人も）	傍受してその存在若しくは内容を漏らし、又はこれを窃用してはならない。	△ **暗号通信の傍受等をした者が、漏えいまたは窃用の目的で内容を復元したときのみ処罰。**	○	○	○（無線局の取扱中に係る無線通信の秘密を漏えい又は窃用が対象、無線通信業務従事者には特に罰則加重）（第109条）

•憲法上の通信の秘密保護を前提に法律で規定。他に不正アクセス禁止法など。

（禁止行為中の○は対象で×は対象外）

完全性 (Integrity)

- 情報および処理方法が完全かつ確実であることを保護することを意味。
- 紛争の典型例は、情報の不正な改ざん行為
- わが国の判例上では金融機関におけるオンライン詐欺の事案が多い。
  - 三和銀行事件の大阪地判昭和57年7月27日
  - 第一勧銀事件の大阪地判昭和63年10月7日
  - その他
  - 電子計算機使用詐欺罪によって処罰
- 金融機関以外における故意によって完全性が侵害された事例
  - 朝日放送クラッキング事件の大阪地判平成9年10月3日
  - 霞ヶ関中央省庁連続クラッキング事件 (2000年1月発生)
  - ニフティ電子掲示板詐欺事件の京都地判平成9年5月9日
  - パチンコ遊技台裏ロム事件の福岡高判平成12年9月21日
- 過失による完全性の侵害事例の典型例はコンピュータの誤操作事案
  - 日本相互銀行コンピュータ誤操作事件の福岡地判昭和53年4月
  - 三和銀行コンピュータ誤操作事件の札幌高判昭和55年6月
  - 預金者名コンピュータ誤入力事件の東京地判平成10年7月14日

可用性 (Availability)

- 許可された利用者が、必要な際に情報および関連資産にアクセスできることを確実にすること
- みずほフィナンシャルグループ大規模システム障害発生事件
- 世田谷ケーブル火災事件の東京高判平成2年7月12日
- ハードディスク・データ消失事件の広島地判平成11年2年24日
  - 原告がパソコン内蔵ハードディスク容量を増大させるために新たなハードディスクを購入し、販売店（被告）に旧ディスクから新ディスクへの交換を依頼したところ、被告の従業員が誤って旧ディスクを初期化したので、旧ディスク内に記録されていた原告の業務上不可欠な多量のデータがすべて消去された事案で、被告に損害賠償責任が認められた。
- レンタルサーバ・データ消滅事件の東京地判平成13年9月28日
  - 納入した製品が可用性を欠くとして取引先から訴えられた事案であり、インターネット接続プロバイダ（被告）のレンタルサーバ内に保管されていた原告の電子商取引サイト用コンテンツデータを、システム変更の際に被告が誤って消滅させたことを理由とする損害賠償請求を一部認容した。
- 東京電送センター事件の東京地判平成8年7月11日
  - コンピュータ機器の売買契約で、買主が機器に瑕疵を発見したときは直ちに売主に内容を通知すべき約定がある場合、通知を受ける都度、売主が機器を調査して代替品との交換又は修理等の必要な措置を行い、瑕疵ある状態を解消すれば、売主は債務不履行責任を負わないとした。

その他の問題

- 無線タグ･生体認証
  - 個人情報保護法とガイドラインで対応
- 無権限アクセスでの侵入行為
  - 無権限での侵入行為は不正アクセス禁止法で禁止。書き換え等を伴う場合やDdos攻撃は刑法の電算機損壊等業務妨害罪の対象。
- ウイルス
  - 配布行為は刑法の電算機損壊等業務妨害罪の対象
  - 処罰範囲拡張に向けて、現在、国会で刑法改正審議中
- 迷惑メール
  - 特定電子メール送信適正化法、特定商取引法等で規制
- ワン切り
  - 有線電気通信法で規制
- 架空請求メール、ワンクリック詐欺、振り込め詐欺
  - 刑法の詐欺罪、本人確認法等で対処
- フィッシング (Phishing) 詐欺
  - 著作権法違反で摘発
- 残された課題
  - ゾンビPC、ボットネット、スパイウェア等の規制