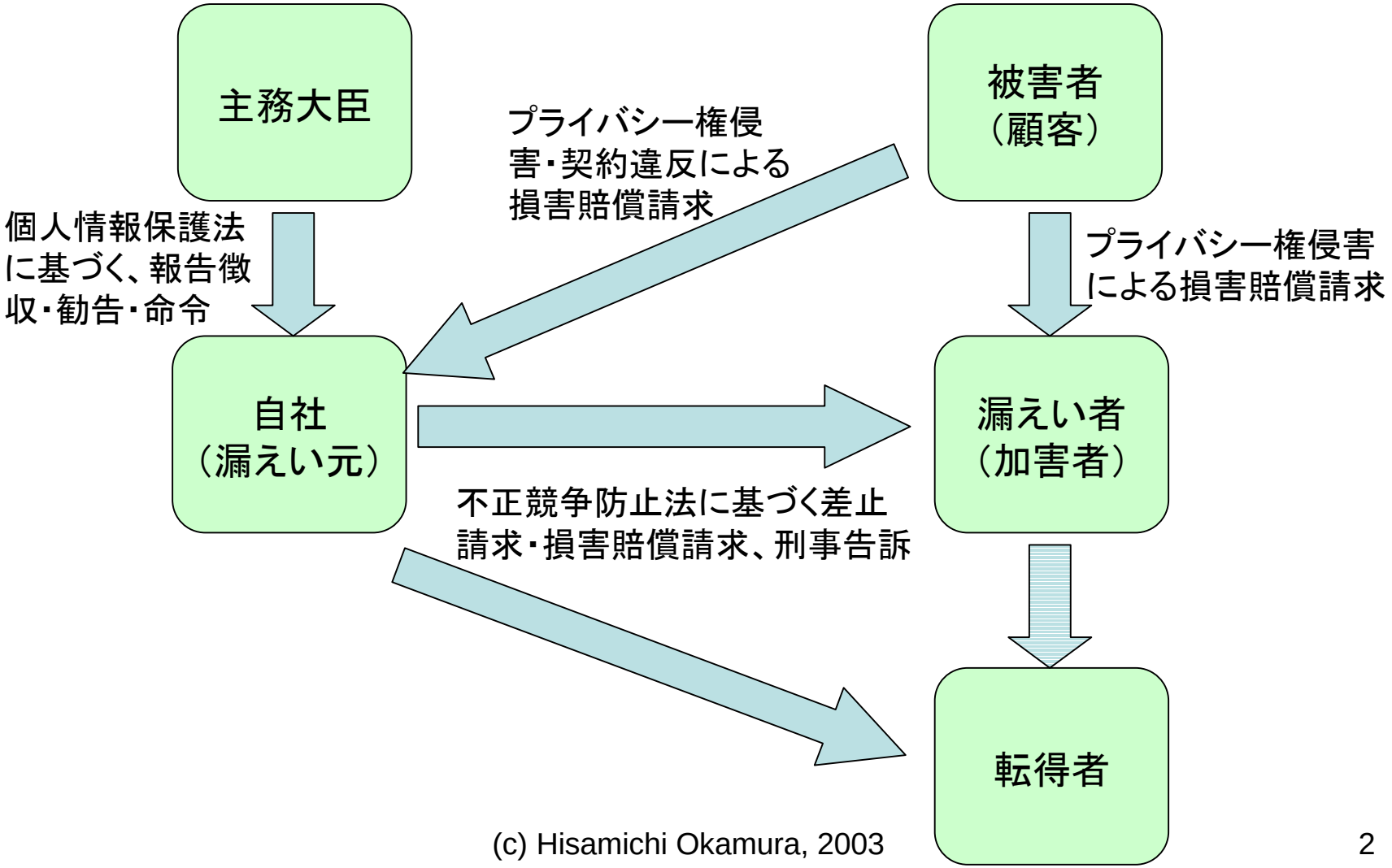
INTERNET WEEK 2003
2 - 5 December 2003 Yokohama / パシフィコ横浜

2003年12月4日

管理者が注意したい ネットワークの法律の最新動向2003

弁護士
岡村　久道

顧客名簿データ漏えい事案の法律関係（民事・行政）



業務用システム関連の漏洩事件ー機密性

- 日経マグロウヒル事件に関する東京地判昭和48年2月19日判時713号83頁（前述）
- 東京地判昭和62年9月30日判時1250号144頁（京王百貨店事件）
  - 百貨店に勤務するコンピューター技術者が、複写目的で同百貨店の顧客名簿が入力された磁気テープを、電算室から持出したときは、窃盗罪が成立する。
- 東京地判平成10年7月7日判時1683号160頁（さくら銀行顧客データ不正漏えい事件）
  - 都市銀行向けプログラム開発業務に従事していた者が、メイン顧客データをフロッピーディスクにコピーして、業務上預かり保管中の項目説明書等の資料4枚をコピーした上、名簿図書館に売却した事案で、資料に関する業務上横領罪の成立を認めた。
- 大阪高判平成13年12月25日サイバー法判例解説190頁（宇治市住民基本台帳データ不正漏えい事件 ）
  - 次ページ参照

宇治市住民基本台帳データ流出事件

- 事　案
  - 京都府宇治市の住民基本台帳データ約22万人分が不正流出した事実が判明。市がメンテナンスを委託していた電算業者（A社）の下請（B社）に児童検診用データを預けていたところ、B社のアルバイト大学院生Tが自分で持参した光磁気ディスク（MO）にコピーして持ち出し名簿業者に無断売却、インターネット上で販売されていた事案で、住民3名から市への損害賠償請求事件。
- 第一審（京都地判平成13年2月24日）
  - 請求一部認容（弁護士費用を含め総額計45000円の支払を命じた）
- 控訴審（大阪高判平成13年12月25日）
  - 市の控訴を棄却
  - 「控訴人は、A社がB社に再委託することを承認し・・・、控訴人の担当職員は、乳幼児検診システムの開発業務について、現にC社の代表取締役であるAや従業員であるBと打ち合わせを行い、従業員Tも、この打ち合わせに参加し・・・Bと従業員Tは、当初、控訴人の庁舎内で乳幼児検診システムの開発業務を行」い、「本件データを庁舎外に持ち出すことについても控訴人の承諾を求めたのである。これらの事実に照らすと、控訴人と従業員Tとの間には、実質的な指揮・監督関係があったと認め」られ、市は使用者責任を負う。」
- 上告審（最決平成14年7月11日）
  - 市の上告を棄却
- 問題点
  - 下請従業員の漏洩行為でも、発注者は使用者責任（一種の無過失責任）に基づき、損害賠償責任を負わされるリスク発生
  - 一人あたりに対する賠償額は少なくても、電子データの場合には大量漏洩で高額になるおそれ
  - 請負・下請などが作業に使うコピーの管理は難問

インターネットサイトからの主要な個人情報漏えい事件1

発覚時期	事件の概要
1997年6月	電話会社系のインターネット接続プロバイダがセキュリティ対策の甘さが原因で不正アクセスを受け、インターネット接続サービス会員約 7000人分のパスワードが外部漏えいしている可能性が判明した。
1998年1月	インターネット接続プロバイダが不正アクセスを受け、会員名簿データ約450人分が流出し無関係なウェブサイト上で公開されていた。翌月、電子計算機損壊等業務妨害罪などの被疑事実で都内在住の高校生が逮捕された。
1998年5月	三重県津市のインターネット接続プロバイダのTelnetサーバ上からクレジットカード番号を含んだ会員リスト299人分が漏えいした。
1998年10月	大手市場調査サイトのオンラインアンケートに回答したユーザーの個人情報約2500人分のリストがサーバから持ち出され、無関係なウェブサイト上で公開されていた。データが誰でもダウンロードできる状態であったことが原因。
2000年1月	パソコン周辺機器メーカーのウェブサイト上で、ウェブサーバ更新時のミスでパスワード機能が外れたことが原因で、アンケート回答者の個人情報約2000人分が、外部から閲覧可能な状態になっていた。
2000年2月	民間シンクタンクのウェブサイト上で、書籍を購入するなどした顧客1万6000人分以上の個人情報が外部から閲覧可能な状態になっていた。
2000年3月	管理を委託していた広告代理店の作業ミスにより、製薬会社のウェブサイト上で健康チェックのページに登録されていた顧客約9900人分の個人情報（氏名、年齢、電話番号、身長、妊娠の有無など）が外部から閲覧可能な状態になっていた。
2000年5月	更新作業中のミスが原因で、国際電話会社の子会社が管理するウェブサイトから、顧客の個人情報約1600人分が閲覧できるようになっていた。

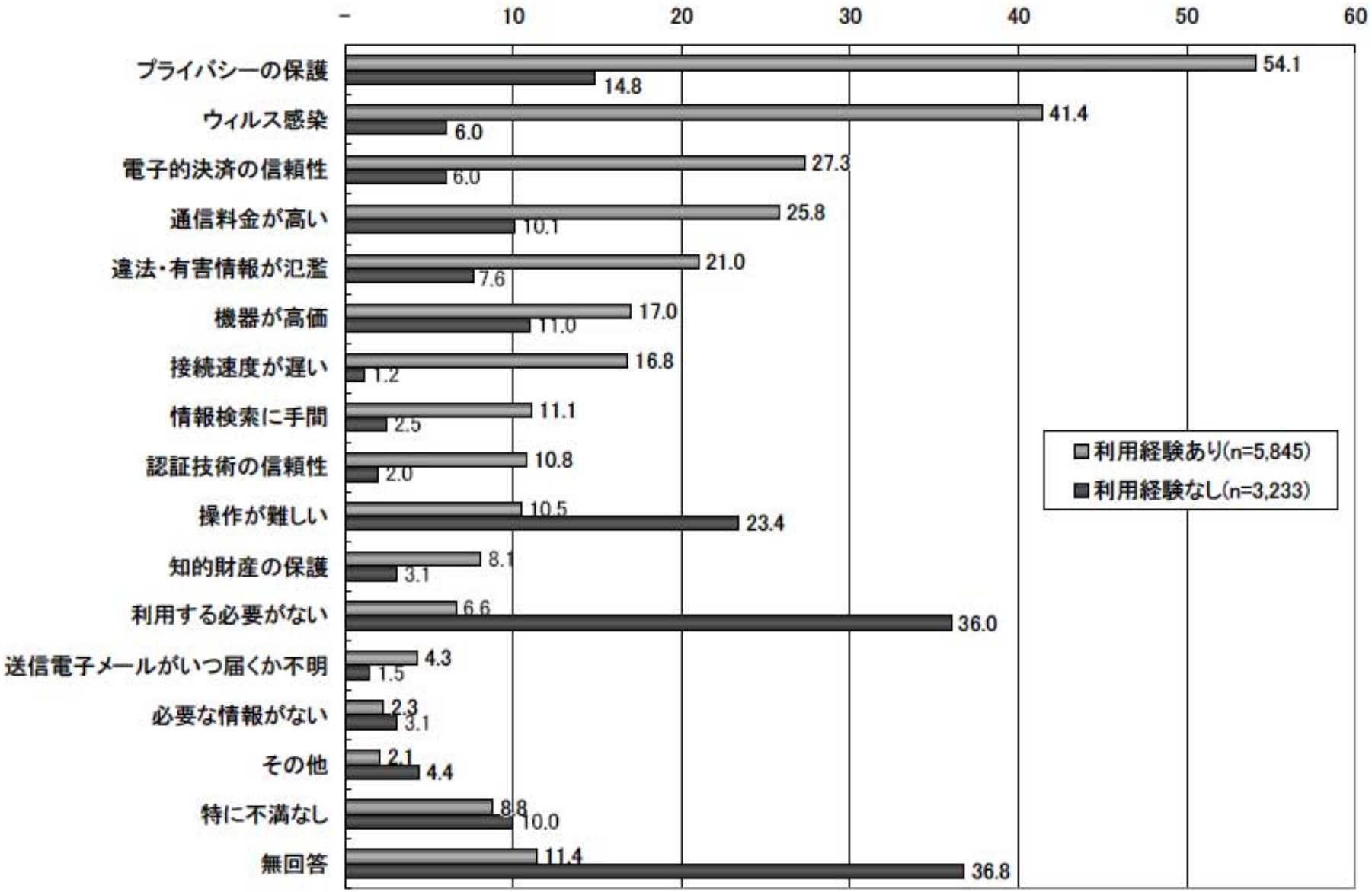
インターネットサイトからの主要な個人情報漏えい事件２

発覚時期	事件の概要
2000年8月	大手ファストフードチェーンのウェブサイト上で、プログラムの不具合が原因で、アンケート回答者の個人情報約100人分が、外部から閲覧可能状態になっていた。
2001年7月	化粧品会社の顧客約1万人の氏名、住所など個人データが、インターネット上で閲覧可能な状態になっていた。
2002年5月	岩手県のウェブサイト上に県条例に基づく情報公開請求者の実名8人分が請求内容とともに誤って掲載されていた。
2002年5月	エステティックサロン運営会社のウェブサイト上で、問い合わせやアンケート内容など顧客情報（当初発表の漏えい者数は３万7000人であったが後に約5万人分へと訂正）が外部から閲覧できる状態になっており、2002年12月、被害者の一部から損害賠償請求訴訟が提起された。
2002年6月	諏訪市が管理する原田泰治美術館のウェブサイト上で、来館者の住所・氏名などの個人情報約6700人分が閲覧可能な状態になっていた。
2002年6月	女性向けウェブサイト上でネット懸賞応募者の個人データ1101人分が閲覧可能な状態になっていた。
2002年7月	パソコン教室のウェブサイト上で就職希望者など個人情報約2000人分が閲覧可能な状態になっていた。
2002年7月	お見合い情報サービスのウェブサイト上で会員の写真など個人情報約200人分が閲覧可能な状態になっていた。
2002年8月	インターネットカフェの会員リスト約1万7000人分がインターネット上で閲覧可能な状態になっていた。

インターネットサイトからの主要な個人情報漏えい事件3

発覚時期	事件の概要
2002年8月	わさびなどを製造・販売する食品メーカーのウェブサイト上で、同社の管理する個人情報リスト約1200人分が閲覧可能な状態になっていた。
2002年8月	ソース等を販売する食品メーカーのウェブサイトから顧客の個人情報約4万9000人分が流出。
2002年8月	大手住宅販売企業のウェブサイト上で、システム移行時のプログラムミスが原因で、メールマガジン・パンフレット請求者の個人情報398人分が外部から閲覧可能状態になっていた。
2002年8月	菓子メーカーのウェブサイト上で顧客の個人情報3244人分が外部から閲覧可能状態になっていた。
2002年8月	学習塾を経営する企業のウェブサイト上に、アンケート回答者の住所や氏名など個人情報426人分が流出して掲載されていた。
2002年10月	東京都のウェブサイト上で、都から大道芸人の免許を受けた154人全員の個人情報が閲覧可能な状態になっていた。
2002年11月	私立大学の入学願書郵送希望者の個人情報3107人分がインターネット上で容易に閲覧可能な状態になっていた。
2002年11月	名古屋国税局のウェブサイトの「ご意見・ご要望コーナー」に意見を寄せた投稿者の個人情報約180人分が外部から閲覧可能な状態になっていた。
2002年12月	インターネット専業証券会社のシステムに障害が発生して、誤って顧客口座数百人分につき証券などの購入可能限度額が表示されていた。
2003年5月	損害保険会社が、自社の身体障害者採用試験に応募した38人に対し意思確認用のメールを送信する際、他の応募者98人分の障害の部位・等級などの社内管理用データを誤って送信。

図表 4- 22　インターネットを利用していて感じる不安・不満、利用しない理由



出典・総務省『2003年版通信利用動向調査』

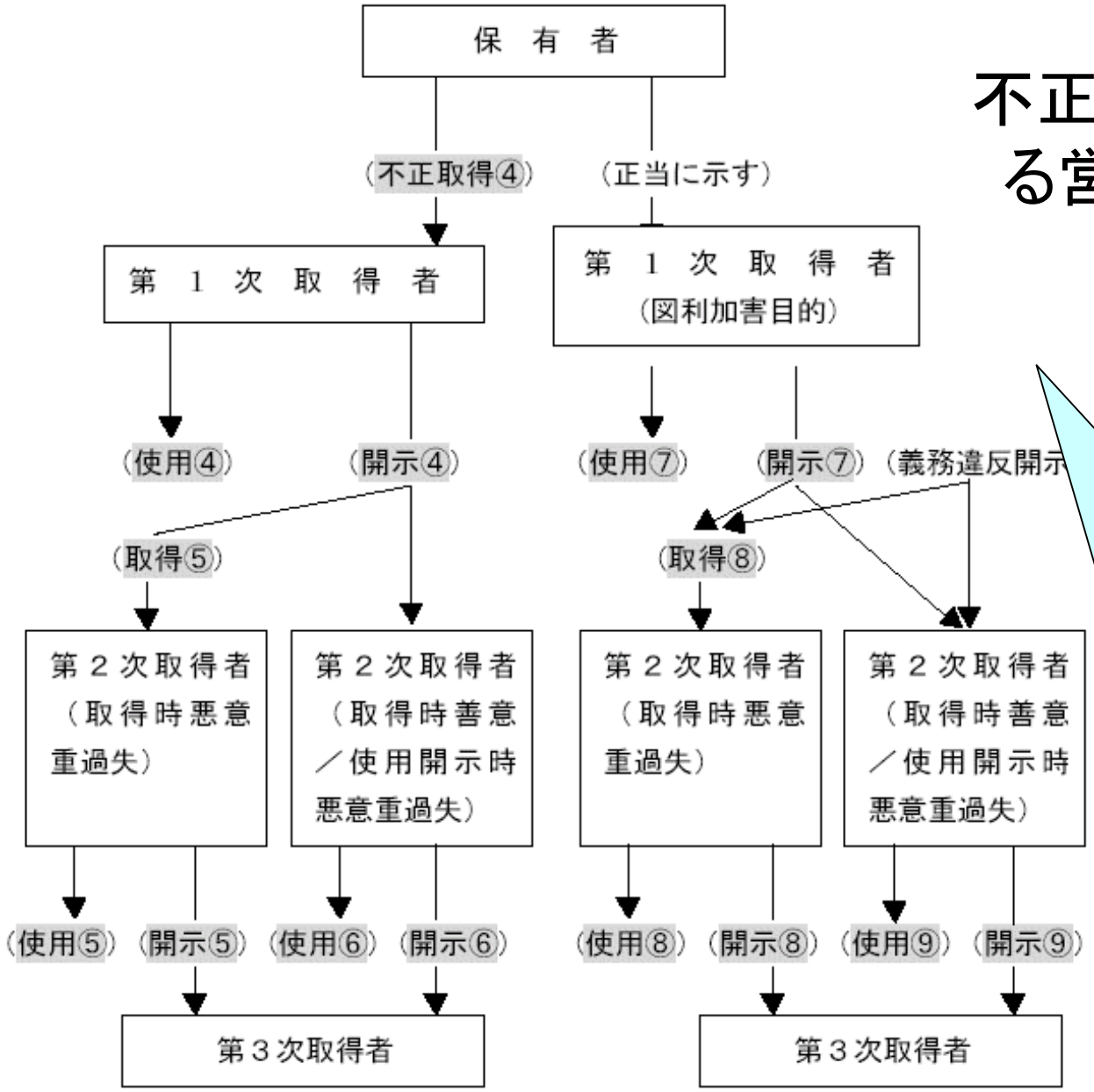
漏えい者の責任

- 顧客に対する民事責任
  - プライバシー権侵害に基づく損害賠償責任
- 漏えい元企業に対する民事責任
  - 不正競争防止法に基づく責任
- 刑事責任
  - 媒体ごと持ち出したような場合は刑法の窃盗罪などに該当するが、データだけ持ち出した場合には刑法の対象外
  - データだけ持ち出した場合も、2003年改正により不正競争防止法で、刑罰の対象となった（後述）
  - 不正アクセスによる場合は不正アクセス禁止法違反
  - 他に特別法で処罰規定がある場合あり
  - どちらにしても処罰を受けるのは故意犯の場合だけに限定される

機密性と刑法

- 情報が載った他人の管理する有体物（紙や媒体）を持ち出した場合には、刑法の窃盗罪が成立しうる。
  - 京王百貨店事件の東京地判昭和62年9月30日は、百貨店の顧客名簿データが入った磁気テープを、同百貨店に勤務するコンピュータ技術者が複写目的で持ち出した行為が窃盗罪に該当するとした。
- 情報が載った自己の管理する他人所有の有体物（紙や媒体）を持ち出した場合には、刑法の（業務上）横領罪が成立しうる。
  - 新潟鉄工事件の東京地判昭和60年2月13日（第一審）及び東京高判昭和60年12月4日は、コンピュータシステムに関する会社の機密資料を複写目的で持ち出した従業員に業務上横領罪の成立を認めた。
- 事前に共謀して持ち出させた者には共犯が成立し、事後に事情を知りながら当該財物を譲り受けた者には盗品譲受け罪（第256条）が成立しうる。
  - 富山化学・新薬産業スパイ事件の東京地判昭和59年6月15日では、会社部長の指示により、国立予防衛生研究所勤務の厚生技官が資料をコピー目的で密かに取り出して会社部長に手渡したという事案で、会社部長の行為について、厚生技官の窃盗罪との共謀共同正犯の成立が認められた。
  - 東洋レーヨン産業スパイ事件の神戸地判昭和56年3月27日では、会社の従業員が、上司から業務遂行上の参考として閲覧するようにとの指示を受けて交付された極秘書類たる製造設備に関する研究開発の報告書を無断で持ち出しライバル会社従業員に売り渡した事案で、持ち出した従業員には業務上横領罪、極秘書類と知って買い受けたライバル会社従業員には贓物故買罪（現在の盗品譲受け罪）が成立するとした。
- しかし自ら持参した媒体にデータを無断で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がある。データ自体はこれらの罪の客体たる「財物」や「物」に該当しないからである（宇治市住民基本台帳データ大量漏えい事件など）。
- それではまずいので、不正競争防止法で規制対象となった（後述）。

不正競争防止法による営業秘密の保護



（出典・経済産業省『営業秘密管理指針（平成15年1月30日）』5頁」）

- 差止め請求、損害賠償請求その他の措置が可能。
- しかし適用対象が故意の漏えい行為に限られていることに注意。過失による漏えいケースには使えない
- したがって、従業員・取引先に対して秘密保持誓約書などを徴収しておく必要がある

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。

営業秘密とは？

- 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にある

情報セキュリティマネジメントを講じていなければ保護されないことに注意

健康食品通信販売顧客データ事件
東京地判平成14（2002）年4月23日

- 健康食品の通信販売等を業とする原告会社から、元従業員の被告A，同B，同Cが原告の営業秘密である顧客データを持ち出し、このデータを利用して被告会社が原告の事業の乗っ取りをしたと主張して顧客データの使用の禁止及び損害賠償請求をした事案で、請求を棄却。
- 「秘密として管理されているというためには，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，当該情報にアクセスできる者が制限されていることが必要である。そこで，本件について検討するに，原告の顧客データの管理方法については，…顧客データは，原告のメインコンピューターのハードディスクに，アクセス（マイクロソフト社のデータベースソフト）のデータとして収録されていた。原告には他に4台のコンピューターがあり，他のコンピューターからもメインコンピューターにアクセスしてこのデータにアクセスすることが可能であった。このコンピューターを操作し得る立場にあるのは，被告A…，被告Cのほか，入力作業等に携わっている4名ほどのパートタイマーがいたが，原告の顧客データへのアクセスについてはパスワード等による保護はされておらず，事務所にいる者なら誰でもこのデータを見ることができる状態にあった。また，顧客データをコピーすることも禁じられておらず，かえって顧客データを使用する場合はコピーしてから行うこととされていた。また，コンピュータを操作し得る上記の各人と原告との間では，秘密保持契約も締結されていなかった。」「これらの認定事実からすれば，原告では，顧客データを他のデータと一応識別できる形で保管してあったものと認められるが，これにアクセスできる者は特に制限されておらず，コピーも禁じられておらず，パスワード等による保護もされていなかったため，事務所にいる者であれば誰でも見ることができ，また，これらの者との間に秘密保持契約も締結されていなかったのであるから，秘密としての管理がされていたと認めることはできない。したがって，原告の顧客データは，不正競争防止法にいう営業秘密の要件を備えているということはできない。」

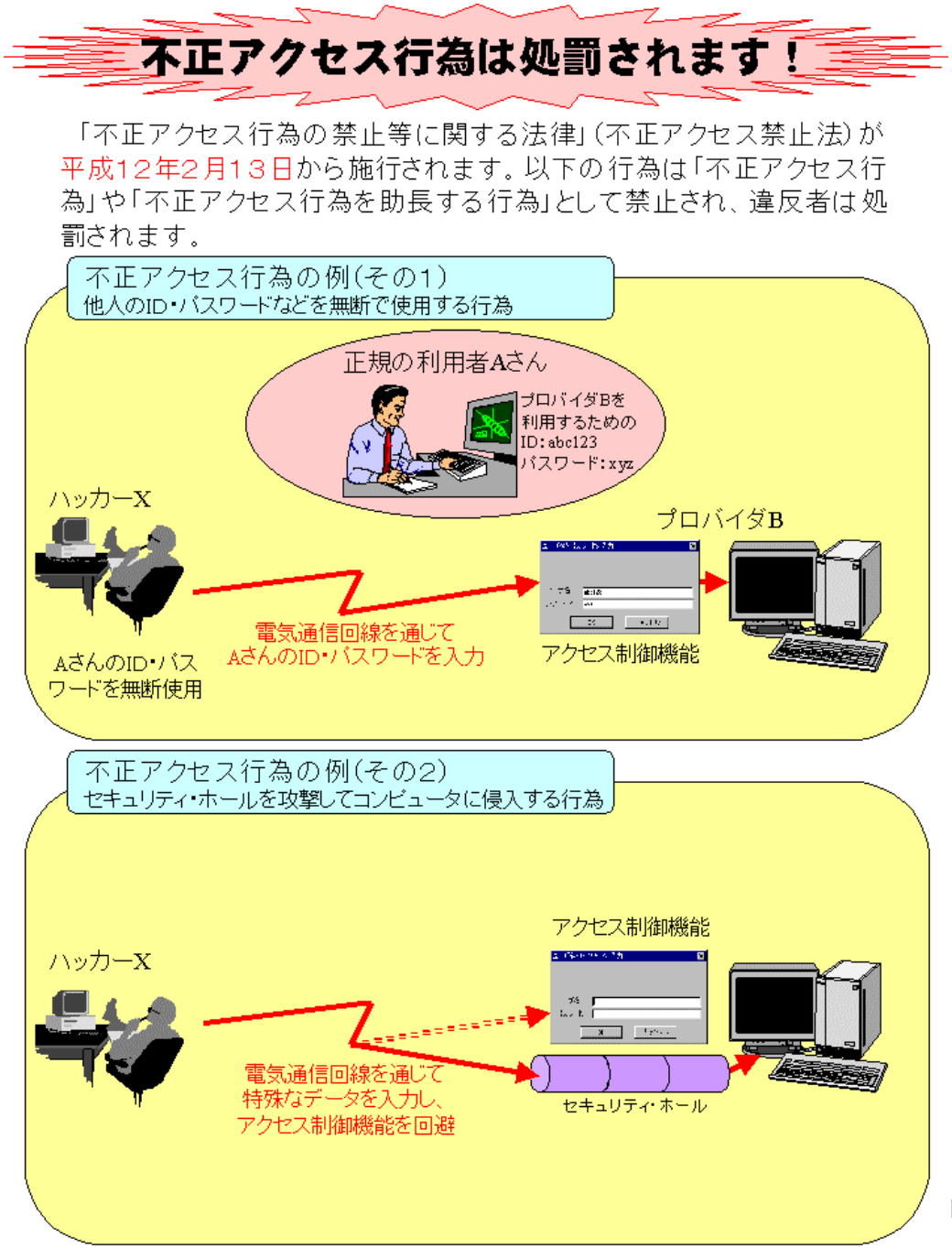
メディカルサイエンス事件
東京地判平成15(2003)年5月15日

- 健康器具関連会社である原告らが、パソコンにより管理していた営業秘密の会員情報を被告らが不正に取得するなどしたとして、差止請求、損害賠償請求を行った事案で、請求を棄却。
- 不正競争防止法2条4項にいう「秘密として管理されているというためには，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，当該情報にアクセスできる者が制限されていることが必要である。…コンピュータを立ち上げるにはパスワードが必要であったが，パスワードは…付箋に記載されてコンピュータに貼ってあったため，従業員は，上記事務担当者以外の，商品発送に関わる者も含め，全員がパスワードを知っていた。また，コンピュータが立ち上がった後は，事務所に居合わせた者は，誰でもその画面で会員情報を見ることができた。…会員登録の際に提出される会員の情報を記載した登録申請書の紙片…を見て事務処理をすることがしばしばであった。…この紙片は，原告両社の事務所の鍵も掛けていない棚や，出窓のところや段ボール箱に入れられて無造作においてあり，従業員その他，事務所に居合わせた者は，誰でも見たり持ち出したりすることが可能であった。そのほか，会員は，地方で講演会を開くときなどに，原告両社の事務担当者からその地方の会員の名簿の写しをもらってそれらに案内状を出したり，原告両社の事務所に電話をして，従業員から会員名を教えてもらったりすることが可能であった。…特に紙片の形で存在する会員情報(登録申請書)について，その管理の仕方は無造作といわざるを得ず，これにアクセスできる者は特に制限されておらず，事務所にいる者であれば誰でも見たり持ち出したりすることができ，また，電話での問い合わせにも特に制限なく会員情報が伝えられ，これらの者との間に秘密保持契約も締結されていなかったのであるから，秘密としての管理がされていたと認めることはできない。したがって，原告両社の会員情報は，不正競争防止法にいう営業秘密の要件を備えているということはできない。」

通信の秘密の保護規定の内容

法律名	保護対象	義務の名宛人	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	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）
	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	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	×	○	○	×
有線電気通信法	有線電気通信の秘密	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）
電波法	特定の相手方に対して行われる無線通信	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。	×	○	○	○（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）

（禁止行為中の○は対象で×は対象外）



警察庁「不正アクセス行為の禁止等に関する法律の概要」

http://www.npa.go.jp/hightech/fusei_ac1/main.htm

- 不正アクセス行為とは、識別符号（※1）を入力することで利用（※2）できるようになっているコンピュータ（※3）にネットワークを通じて（※4）アクセスし、このような利用ができる状態にしてしまう行為（※5）です。コンピュータ以外の端末から行うもの（※6）も禁止・処罰されます。
- 他人の識別符号を無断で第三者に提供する行為は、不正アクセス行為を助長する行為として禁止・処罰されます。提供手段に限定はなく、オンラインで行っても、オフラインであっても禁止・処罰されます。提供行為によって金銭的な利益を得たかどうかは関係ありません。

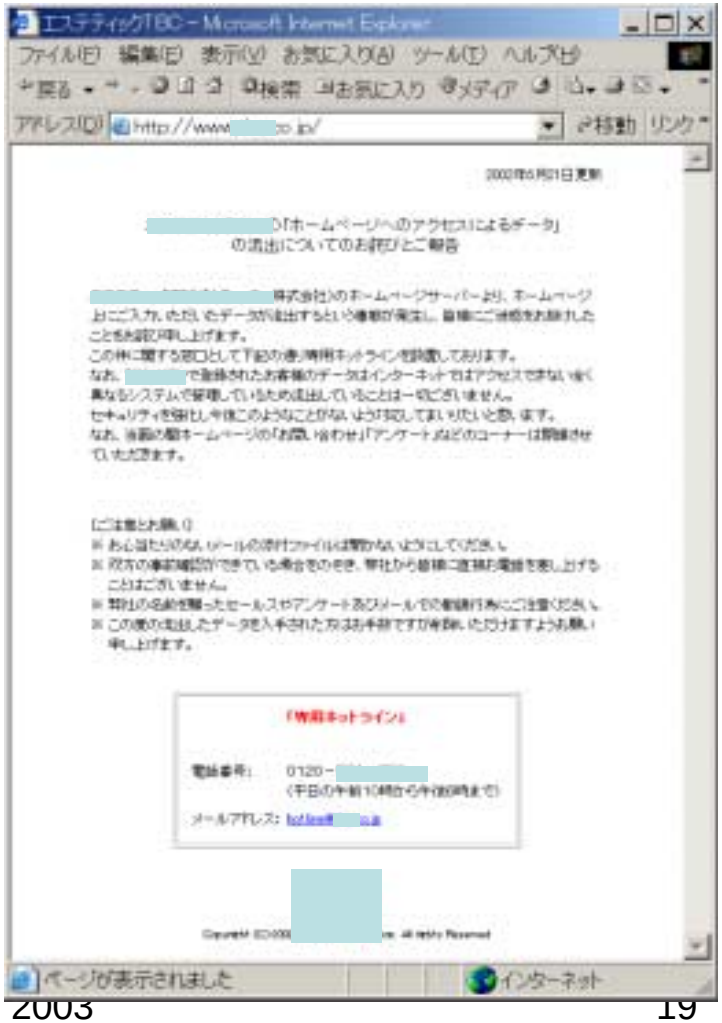
※1 ID・パスワードのほか、指紋、虹彩、音声、署名などを用いるものも含まれます。
※2 ホームページの書き換え、インターネット・ショッピングの注文、データ閲覧、ファイル転送など利用内容に限定はありません。
※3 企業のものも個人のものも広く含まれます。
※4 インターネットなどのオープンネットワークのほか、企業内LANで外部と接続していないものなども含まれます。
※5 利用してしまう行為も含まれます。
※6 例えば、電話機から口座番号と暗証番号をプッシュボタンで入力する行為などです。

警察庁「不正アクセス行為の禁止等に関する法律の概要」

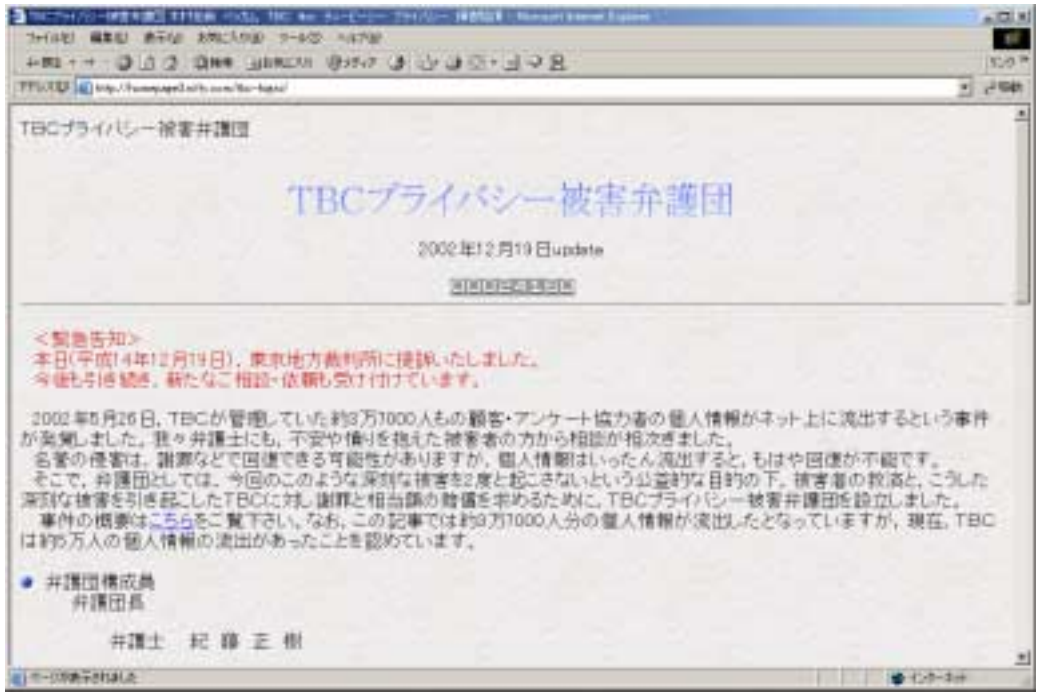
http://www.npa.go.jp/hightech/fusei_ac1/main.htm

自社の責任

- 顧客に対する民事責任
  - プライバシー権侵害に基づく損害賠償責任（罰則なし）
  - 漏えい者が自社の従業員であるとき又は実質的な指揮・命令関係がある者である場合には、民法715条の使用者責任を負う（実質的な無過失責任）
  - 契約上の義務を怠った場合は契約責任に基づく損害賠償責任
- 個人情報保護法上の責任
  - 主務大臣の報告徴収・勧告・命令など
  - 報告懈怠・虚偽報告、命令違反には罰則
  - 従業者・委託先に対する監督責任の規定あり
  - 個人情報保護法には顧客に対する民事責任の定めがないことに注意
- 謝罪文をサイト上に掲載したり、被害者（顧客）に送付する企業も多い（右図）



参考－TBCプライバシー弁護団



エステサロン大手の「TBC」を経営するコミーのサーバーから、約5万人分の個人データが流出。漏えいにより精神的苦痛を被ったとして、10人が「コミー」(新宿区)に1150万円の損害賠償を求め、東京地裁に提訴した。

http://homepage3.nifty.com/tbc-higai/

法律での情報セキュリティ遵守義務付け

- 不正アクセス禁止法
  - 第5条は、「アクセス管理者による防御措置」という表題で、ネットワーク・サーバなどのコンピュータ管理者に対し、いわゆるハッカーなどの不正アクセス被害を受けないようにセキュリティを保つべき義務を課している。但し、法文の「努めるものとする」という文言からも明らかなように、この義務は単なる努力義務にすぎず、これを遵守しなくとも法的なペナルティは課せられない。
- 労働者派遣法
  - 「派遣元事業主は、労働者の個人情報を適正に管理するために必要な措置を講じなければならない」と規定しており（第24条の3第2項）、違反行為には、厚生労働大臣の指導、助言及び勧告（第48条）、改善命令（第49条）などが用意され、第49条による処分に違反した者は罰則の対象となる（第60条）。
- 個人情報保護法案
  - 次に述べる

大阪地判平成12年9月20日

- さまざまなリスクに対する企業の対応について、「健全な会社経営を行うためには、目的とする事業の種類、性質等に応じて生じる各種のリスク‥‥の状況を正確に把握し、適切に制御すること、すなわちリスク管理が欠かせず、会社が営む事業の規模、特性等に応じたリスク管理体制(いわゆる内部統制システム)を整備することを要する。そして重要な業務執行については、取締役会が決定することを要するから(商法260条2項)、会社経営の根幹に係わるリスク管理体制の大綱については、取締役会で決定することを要し、業務執行を担当する代表取締役及び業務担当取締役は、大綱を踏まえ、担当する部門におけるリスク管理体制を具体的に決定するべき職務を負う。」と判示して、これを怠った当時の経営陣に対し、当時の為替レートで約計830億円もの支払いを命じた。
- 本判決は情報セキュリティが直接対象となった事案ではない。しかし本判決は、さまざまな種類のリスクと並んで「システムリスク」を摘示しているので、その対象は情報セキュリティ分野にも及んでいる。すなわち、金融庁の「金融検査マニュアル」では、システムリスクとは、コンピュータシステムのダウン又は誤作動等、システムの不備等に伴い金融機関が損失を被るリスク、さらにコンピュータが不正に使用されることにより金融機関が損失を被るリスクとして定義されている。この定義は情報セキュリティに関する前述の定義とはやや異なっているが、大筋において実質的に一致する部分が多い。こうした分野において、本判決がいう「リスク管理体制(いわゆる内部統制システム)」の整備は、本稿のテーマである情報セキュリティマネジメントを意味している。また、本判決が経営陣に求める「会社経営の根幹に係わるリスク管理体制の大綱」こそが、セキュリティポリシーなのである。

個人情報保護法の安全管理措置

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）

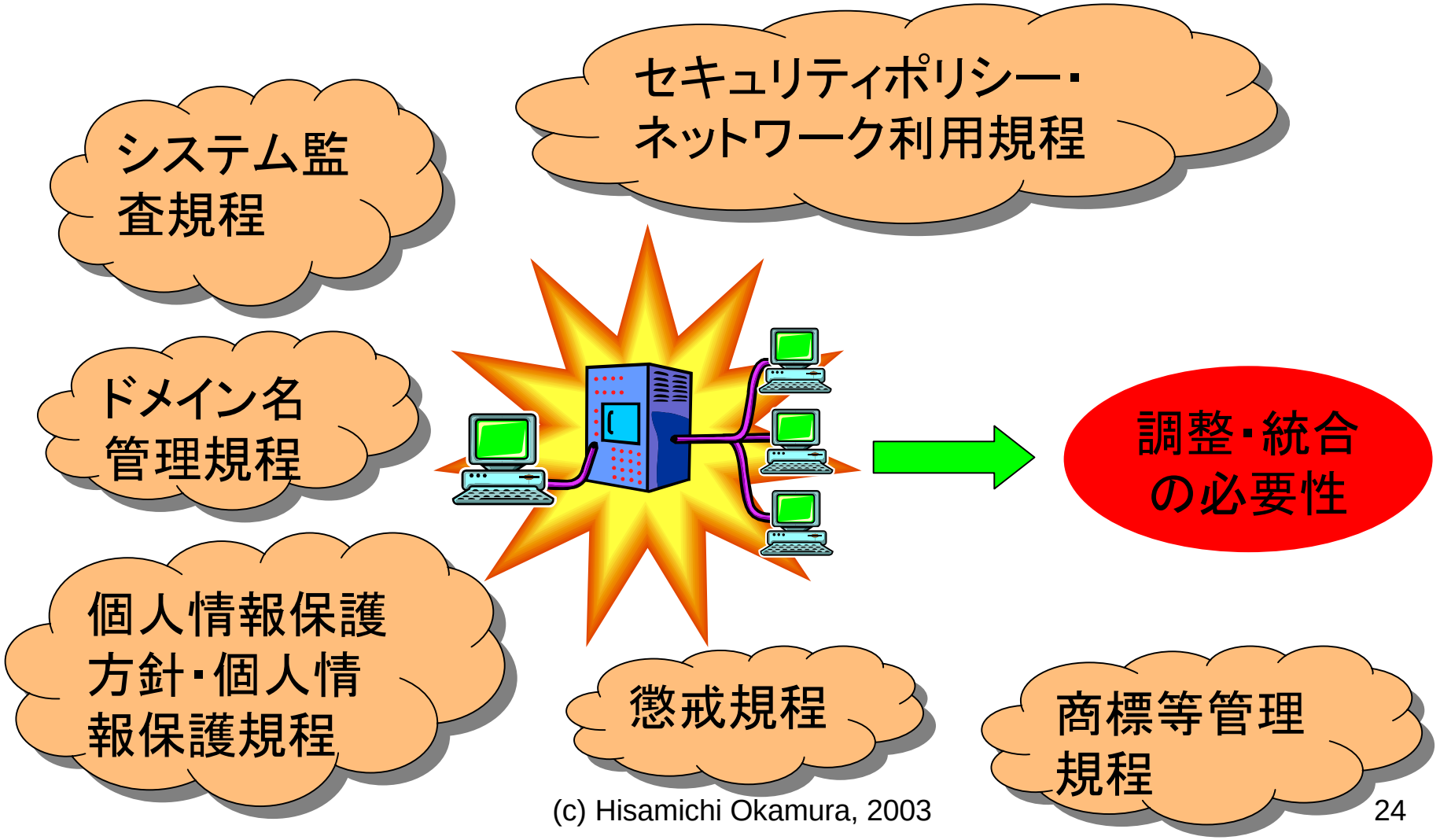
個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない。

「CIA」全部が対象

社内規程で対処

委託契約で対処

関連する社内諸規定の調整・更新

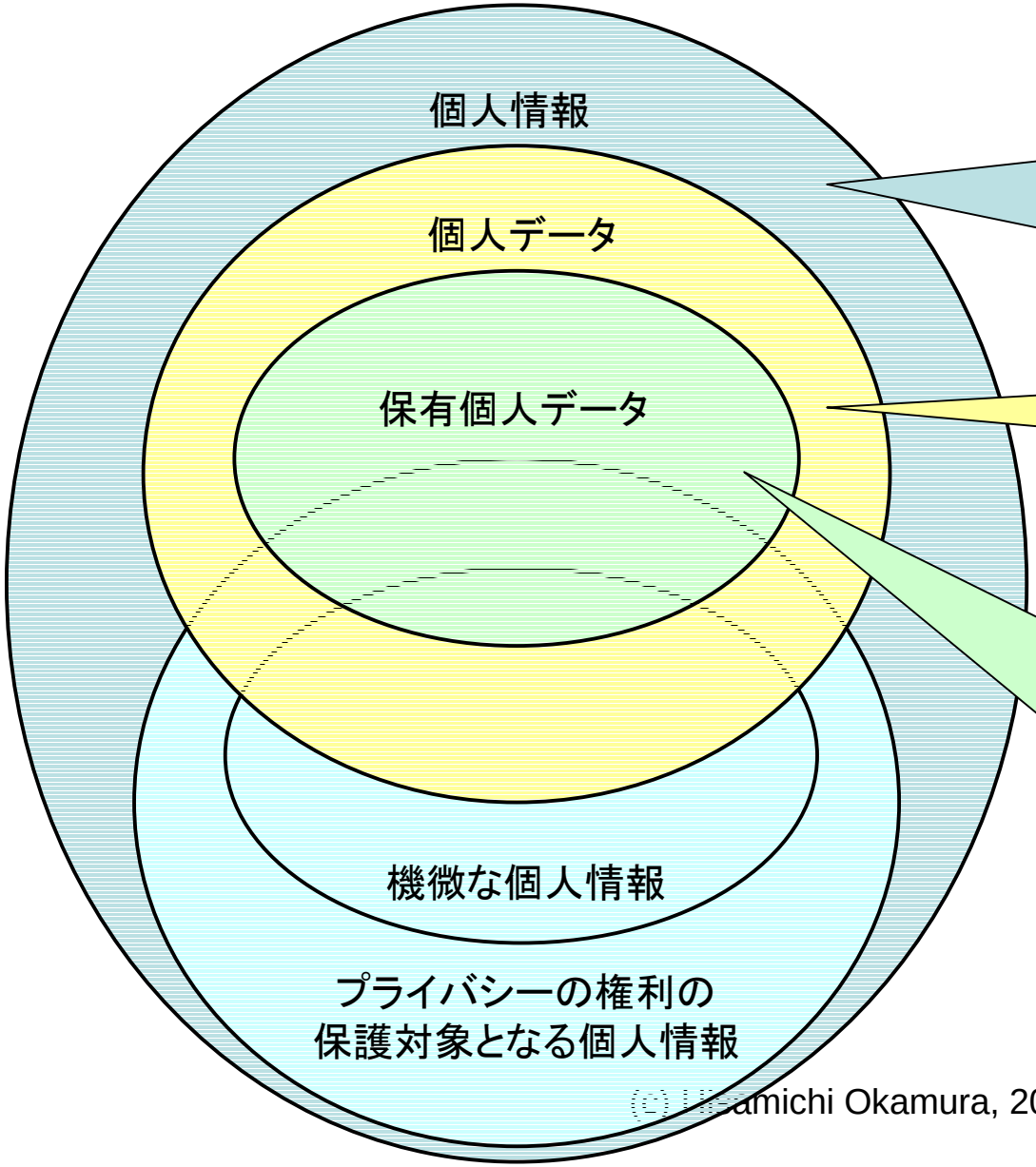


個人情報保護法制の全体像

<table>
<tr><td></td><td colspan="3">公的部門</td><td>民間部門</td></tr>
<tr><td></td><td>国の行政機関</td><td>独立行政法人、特殊法人及び認可法人であって行政機関と同様に取り扱うべきもの</td><td>地方公共団体</td><td rowspan="2"></td></tr>
<tr><td>基本法</td><td colspan="3">〔基本理念など基本法部分〕　　個人情報保護法</td></tr>
<tr><td rowspan="2">一般法</td><td>行政法人個人情報保護法</td><td>独立行政法人等個人情報保護法</td><td rowspan="2">個人情報保護条例</td><td rowspan="2">〔個人情報取扱事業者の義務など一般法部分〕</td></tr>
<tr><td colspan="2">情報公開・個人情報保護審査会設置法
行政機関の保有する個人情報の保護に関する法律等の施行に伴う関係法律の整備等に関する法律</td></tr>
<tr><td rowspan="2">個別法</td><td></td><td></td><td></td><td>電気通信事業法、貸金業法、労働者派遣法など</td></tr>
<tr><td colspan="4">クローン技術規制法、職業安定法など</td></tr>
</table>

（図表中の網がけ部分が今回行われた法整備。なお国の機関のうち立法府及び司法府を適用対象とする個人情報保護に関する一般法は存在せず。）

個人情報とプライバシーの権利

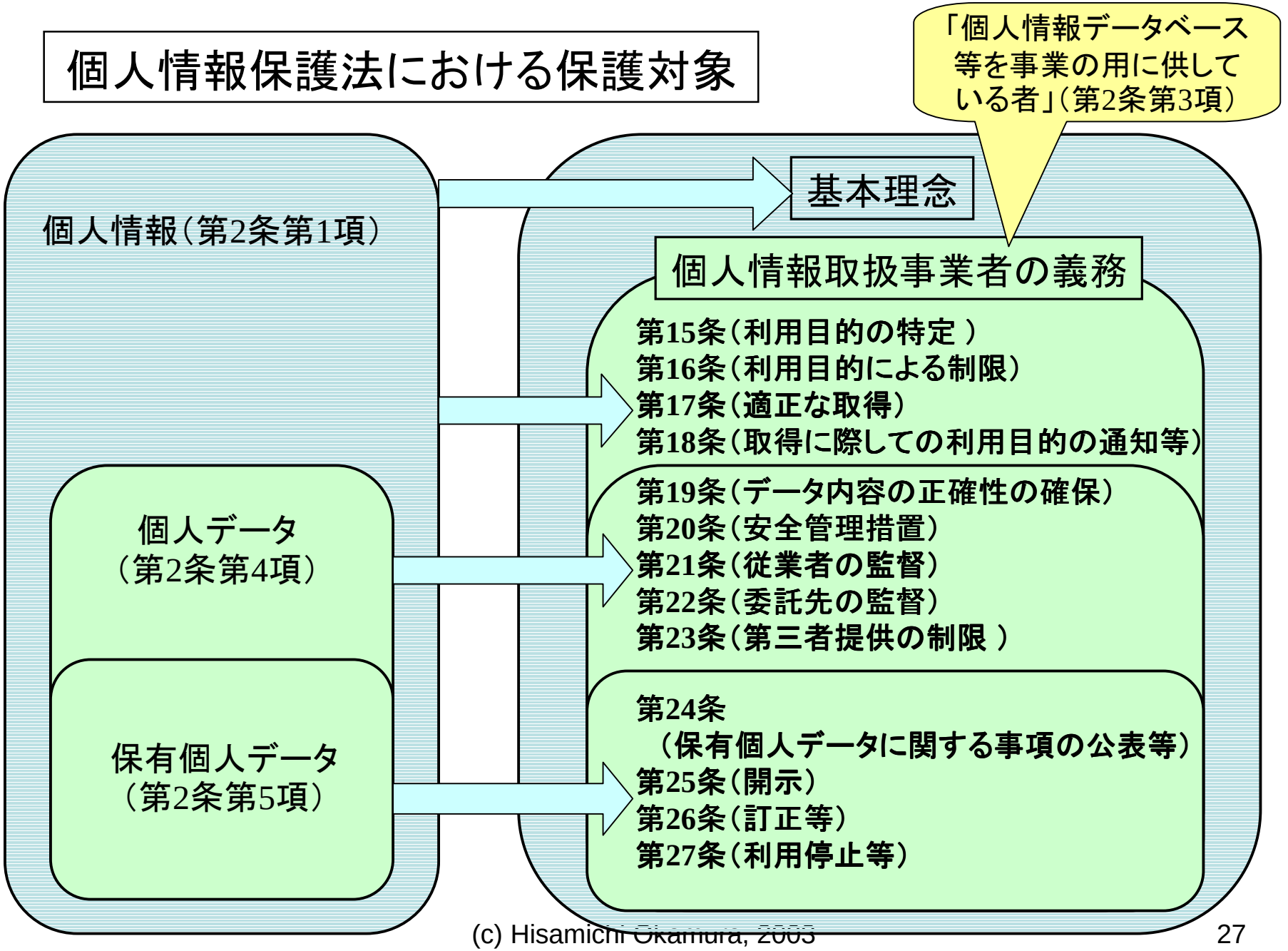


「生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）」（第2条第1項）

「個人情報データベース等を構成する個人情報を含む情報の集合物」（第2条第4項）

「個人情報取扱事業者が、開示、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提供の停止を行うことのできる権限を有する個人データであって、その存否が明らかになることにより公益その他の利益が害されるものとして政令で定めるもの又は一年以内の政令で定める期間以内に消去することとなるもの以外のもの」（第2条第5項）

個人情報保護法における保護対象



「個人情報取扱事業者」（第２条第３項）概念

- 義務規定の適用主体
- 「個人情報取扱事業者」とは個人情報データベース等を事業の用に供している者

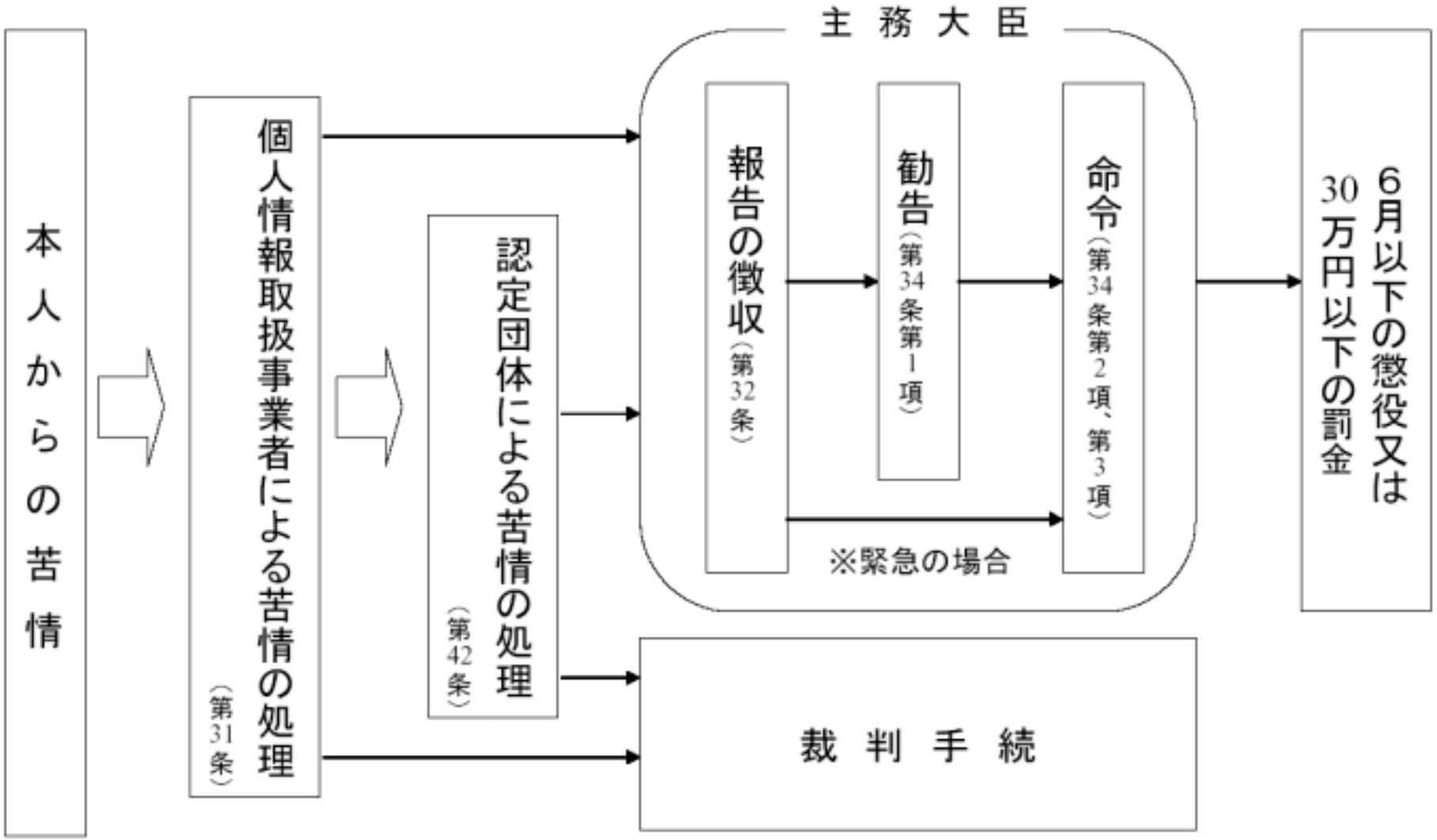
  「個人情報データベース等」とは、個人情報を含む情報の集合物であって、次に掲げるものをいう（第２条第２項）。

  一　特定の個人情報を電子計算機を用いて検索することができるように体系的に構成したもの

  二　前号に掲げるもののほか、特定の個人情報を容易に検索することができるように体系的に構成したものとして政令で定めるもの
- 取り扱う個人情報の量及び利用方法からみて個人の権利利益を害するおそれが少ないものとして政令で定める者は除外→5000件で調整予定
- 国会審議で問題となったもの（個人でも該当するのではないか？）
  - –カーナビゲーションシステム
  - –オンラインのデータベースサービス
  - –インターネットの検索エンジン
  - –年賀状ソフト

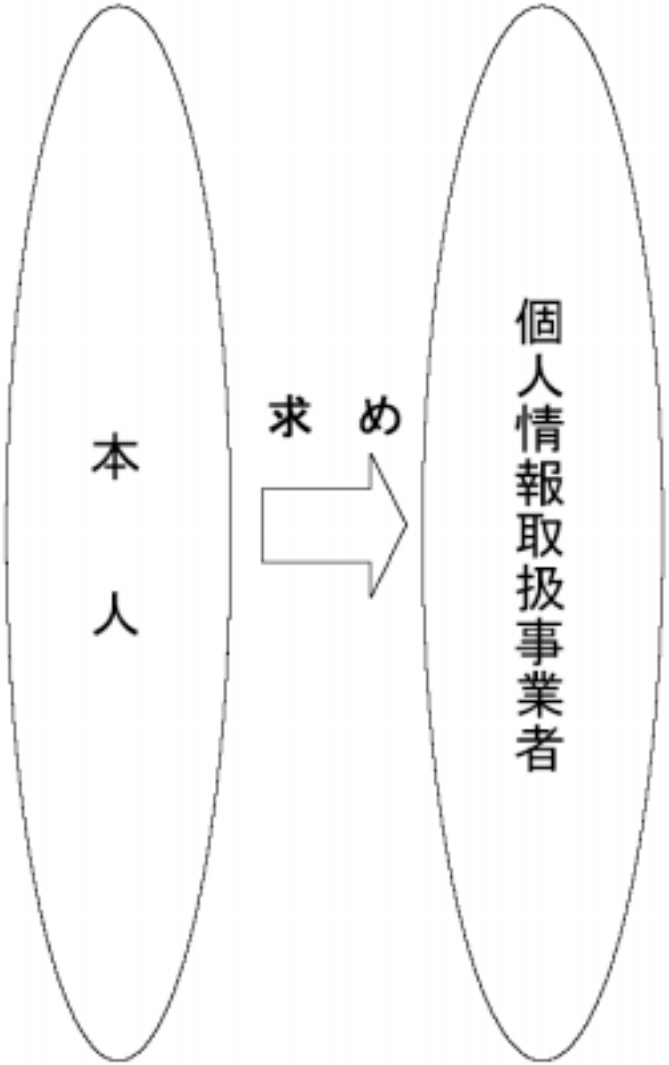
出典・内閣官房個人情報保護室「法案の論点解説」

実効性担保の仕組み



出典・内閣官房個人情報保護室「法案の論点解説」

本人の関与の仕組み



利用目的の通知（第24条第2項）

保有個人データがどのような目的で利用されているのかについて、原則として、本人に通知しなければならない。

開　　示（第25条第1項）

保有個人データについて、原則として、本人に開示しなければならない。
（開示しないことができる場合の例）
① 本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合
② 個人情報取扱事業者の業務の適正な実施に著しい支障を及ぼすおそれがある場合　など

訂　正　等（第26条第1項）

保有個人データの内容が事実でないときは、利用目的の達成に必要な範囲内において、訂正等を行わなければならない。

利用停止等（第27条第1項、第2項）

①利用目的による制限、②適正な取得、③第三者提供の制限に違反していることが判明したときは、違反を是正するために必要な限度で、原則として、利用停止等を行わなければならない。

窓口設置に関する実務上の留意点

- 従来の苦情処理窓口では対応不能
- 本人確認が必要（成りすましによる漏えい避ける）
- 法的判断が必要（拒絶できる事由に該当するか）
- 対応を間違えると主務大臣から調査を受けたり裁判を提起されるおそれ
- 常に相談できるように弁護士との連携
- 担当者のトレーニング
- 対応マニュアル作成
- 本部の保有情報か、加盟店の保有情報か（双方の保有情報であり得る）
- 台帳の作成
- 子会社の窓口との一本化（子会社では対応困難で、別々に窓口作るとお金がかかる）
- 開示しても問題がない情報なのか整理が必要
- 不要な情報は捨てる（捨て方に注意）

参考－電子メール社内モニタリングとプライバシー権

- 電子メール無断モニタリング事件（東京地判平成13年12月3日）
  - 会社の上司に電子メールを無断モニタリングされ、プライバシー権を侵害されたことを理由とする損害賠償請求訴訟の事案
  - 会社における職務遂行の妨げとならず、会社の経済的負担も極めて軽微な場合には会社のネットワークシステムを用いた私的電子メールの送受信は社会通念上許され、従業員にプライバシー権が一切ないとはいえないとしつつ、通常の電話装置による場合よりもプライバシー保護は狭く、事業部の最高責任者による監視は相当であり、原告の私的使用の程度は限度を超えていたと判示して、請求棄却。
- 日経クイック情報電子メール事件（東京地判平成14年2月26日労判825号50頁）
  - 従業員に対する誹謗中傷メールの調査過程でメールサーバから偶然発見された別の従業員（原告）による多量の私的メールを理由として、被告会社が原告に対して行った懲戒処分が、プライバシー侵害に該当するか否かが争われた事案で、私用メールは職務専念義務違反で企業秩序違反行為として懲戒処分の対象となり、サーバ上のデータ調査は業務関連情報が保存されていると判断されるから社会的に許容しうる限界を超えていないとして、請求棄却。
- 厚生労働省「労働者の個人情報保護に関する行動指針」（平成12年12月20日）
  - 使用者は、職場において、労働者に関しビデオカメラ、コンピュータ等によりモニタリングを行う場合には、原則として労働者に対し実施理由、実施時間帯、収集される情報内容等を事前に通知するとともに、個人情報保護に関する権利を侵害しないよう配慮すること、常時のモニタリングは労働者の健康及び安全の確保又は業務上の財産の保全に必要な場合に限り認められること、使用者は原則としてモニタリングの結果のみに基づいて労働者に対する評価又は雇用上の決定を行ってはならないことを求めている。

漏えい事案への対処に関するポイント

- 機密性については、すでに法整備が一応完了しているので、すでに技術問題であるのと同時に法律問題としてコンプライアンス（法令遵守）経営上の課題であることを自覚すべき。
- 社内モニタリングのような技術的コントロール策を講じるにしても、法令に照らして適法か、社内規程上の裏付けがあるかなど、法的側面からの検討が不可欠。
- 個人情報保護法第20条（安全管理措置）を遵守しているというためにも、また不正競争防止法上の「営業秘密」として保護を受けるためにも、日頃から自社で情報セキュリティマネジメント（ISMS）を実践している必要がある。
- 開示請求などへの対応の必要もあり、IT領域にも精通している顧問弁護士などと協議して個人情報保護法対策を進める必要がある。技術系のコンサルタントに任せる場合、責任をもった法的な検討ができるところを選定することが不可欠。

ワン切り事件と有線電気通信法改正

- ワン切りが社会問題化する一方、2002年7月、ワン切り業者がコンピュータで自動ダイヤルした大量発呼が原因で、電話交換機に過負荷が生じて輻輳状態となり、大阪府下一帯と兵庫県尼崎市で500万回線以上の電話回線が一時不通となった。
- 12月4日に有線電気通信法改正が国会で可決成立。
- この改正でワン切り行為は実質的に刑罰付きで禁止対象となり、ひとまず沈静化。
- 第13条の2

  営利を目的とする事業を営む者が、当該事業に関し、通話（音響又は影像を送り又は受けることをいう。以下この条において同じ。）を行うことを目的とせずに多数の相手方に電話をかけて符号のみを受信させることを目的として、他人が設置した有線電気通信設備の使用を開始した後通話を行わずに直ちに当該有線電気通信設備の使用を終了する動作を自動的に連続して行う機能を有する電気通信を行う装置を用いて、当該機能により符号を送信したときは、一年以下の懲役又は百万円以下の罰金に処する。

関連ーワン切り事件
東京地判平成14(2002)年10月18日

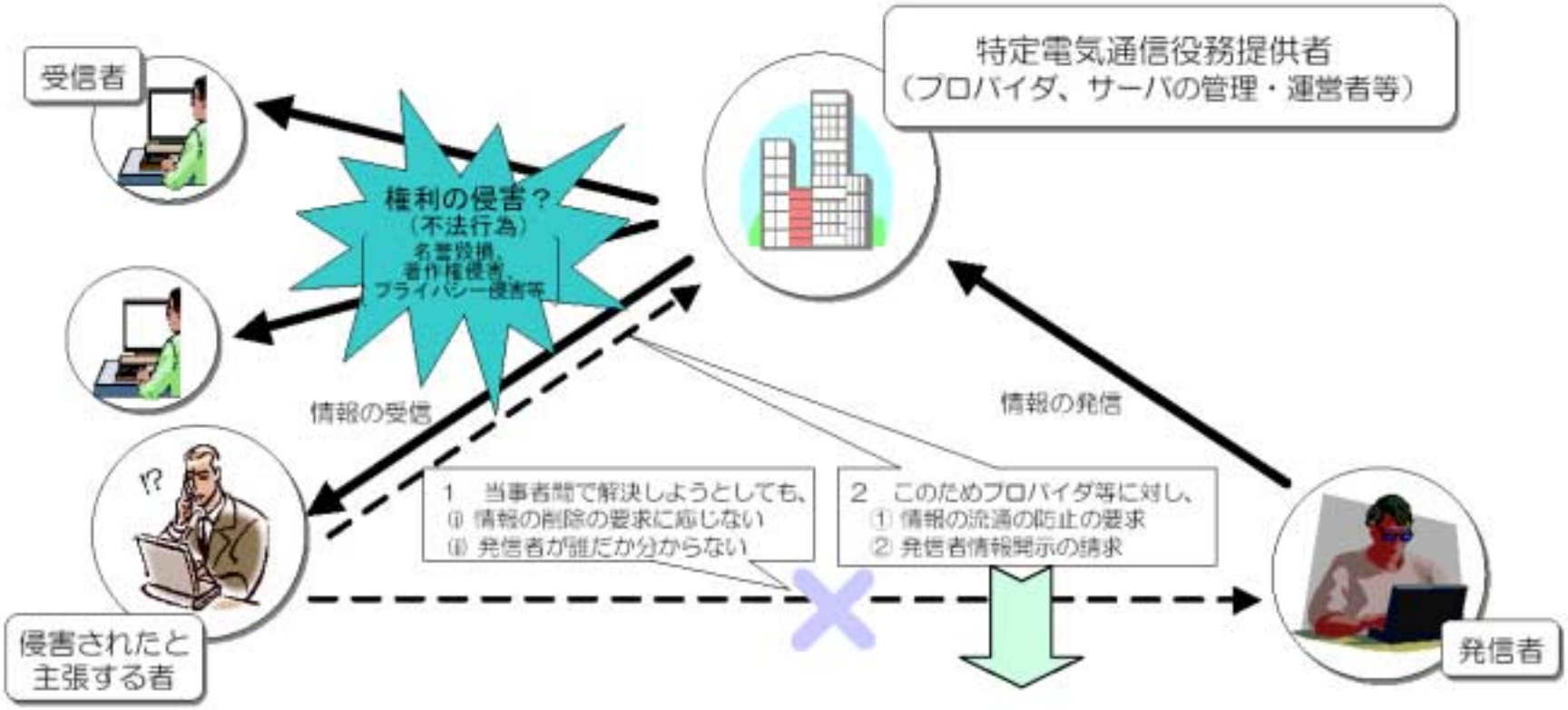
- 録音再生機と電話回線の連動した装置(コミュニケーションサーバ)を設置し、ワン切りコールや迷惑メールにより同サーバの電話番号等を広く宣伝した上、同サーバに電話をかけてきた不特定多数人に対し、同サーバに記憶させた前記わいせつな音声を再生して聴取させた行為につき、わいせつ物陳列罪の成立を認めた事例。
- 「サーバの電話番号を広く宣伝し、多数の者にその番号に電話をかけてくるよう勧誘するために用いた手口をみても、…瞬時に、膨大な数の携帯電話にあててその電話番号等を送信し、これらの携帯番号の保有者の関心を引いた上、折り返しその番号に電話をかけてきた者に対し、短時間、無料でわいせつな音声の一部を電話口に流してその好奇心をかき立て、引き続き有料でわいせつな音声を聴取させるという、甚だ巧妙なものである。このように、被告人らは、本件に際し、さしたる抵抗感もなく、他人の迷惑を顧みない通信手段の悪用であるとして社会的に強い避難を受けている、いわゆる『ワン切りコール』あるいは『迷惑メール』と称される手段まで用いていたばかりか、実際に上記音声を聴取しながらその利用料金を支払わない者に対し、次々と電話をかけて、利用料金のほかに延滞料金等の名目で法外な金員をも支払うよう執拗に督促し、これにより多額の利益を得ていたというのであって、金儲けのためにはあくどい手段を用いることさえ辞さないという被告人らの規範意識の希薄さも、厳しい非難を免れない」

名誉毀損と
サイト運営者関連紛争

ー企業批判サイト問題を中心に

プロバイダ責任制限法（平成13年法律第137号）

プロバイダ等の自主的対応を促すための環境整備の必要性



(a)　情報の違法性の判断が困難等自主対応による措置の責任が不明確な場合がある

(b)　民事事件ではほとんど発信者情報の開示はされず、被害者救済が困難なことがある

⇨ プロバイダ等による自主的対応を促し、その実効性を高める環境整備の必要

出典・総務省資料

プロバイダ等の責任の明確化の概要

被害者（侵害されたとする者）に対する責任

以下の①、②の場合でなければ、**責任なし**

① 他人の権利が侵害されていることを知っていたとき

② 違法情報の存在を知っており、他人の権利が侵害されていることを知ることができたと認めるに足りる相当の理由があるとき

プロバイダ等による対応

削除せず

削除

発信者に対する責任

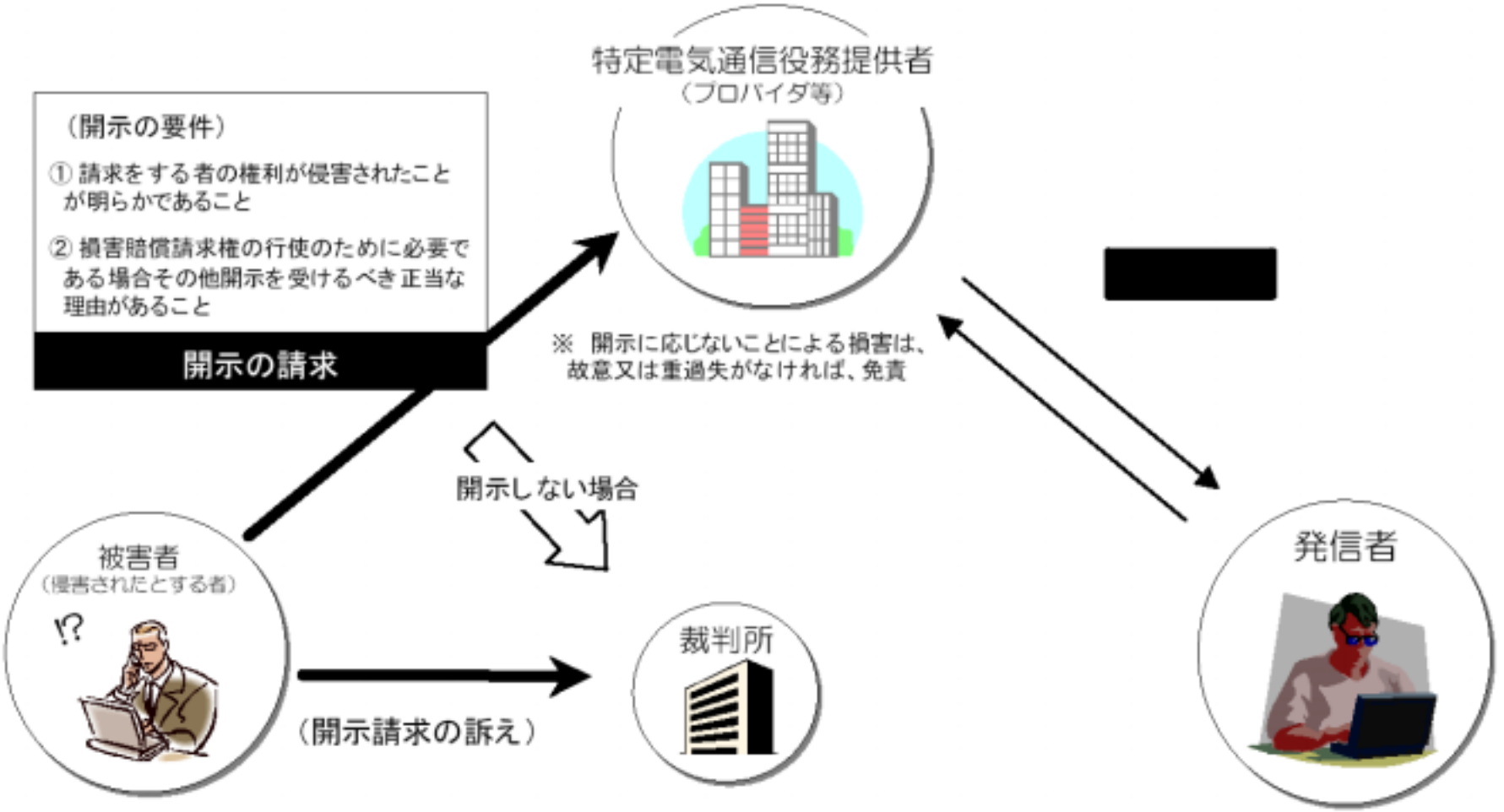
以下の①、②の場合は、いずれも**責任なし**

① 他人の権利が侵害されていると信じるに足りる相当の理由があったとき

② 権利を侵害されたとする者から違法情報の削除の申出があったことを発信者に連絡し、7日以内に反論がない場合

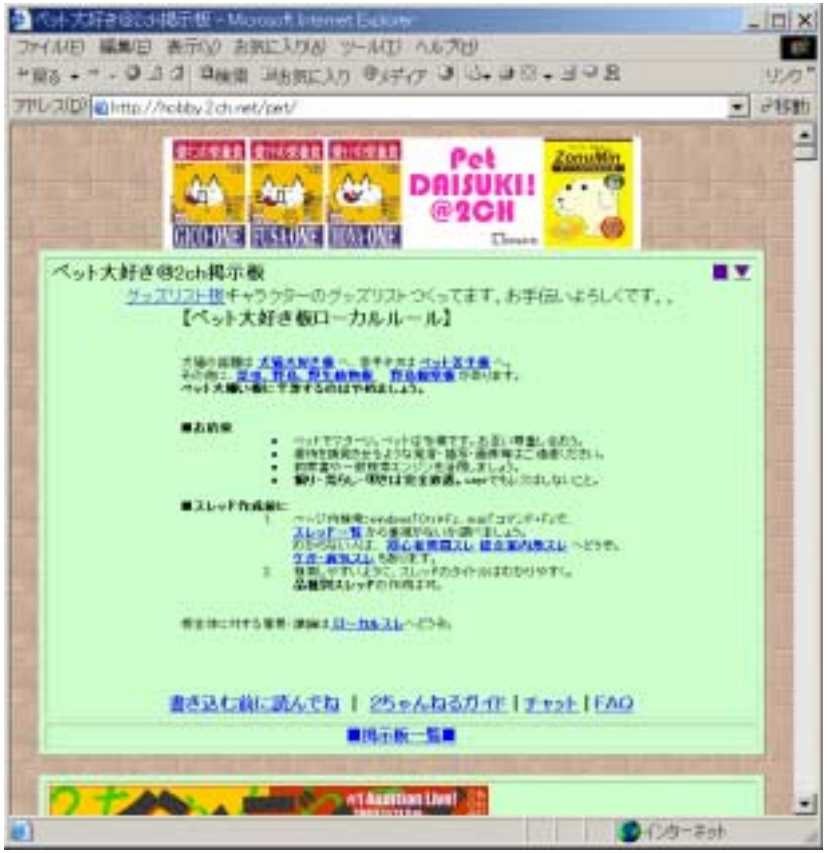
 出典・総務省資料　003

発信者情報開示の概要


特定電気通信役務提供者
（プロバイダ等）
（開示の要件）
① 請求をする者の権利が侵害されたことが明らかであること
② 損害賠償請求権の行使のために必要である場合その他開示を受けるべき正当な理由があること
開示の請求
※ 開示に応じないことによる損害は、故意又は重過失がなければ、免責
開示しない場合
被害者
（侵害されたとする者）
!?
（開示請求の訴え）
裁判所
発信者

2ちゃんねる動物病院事件第一審（東京地判平成14年6月26日サイバー判解42頁）1/2

- 被告の運営するインターネット上の電子掲示板「2ちゃんねる」（本件掲示板）において、原告らの名誉を毀損する発言が書き込まれたにもかかわらず、被告がそれらの発言を削除するなどの義務を怠り、原告らの名誉が毀損されるのを放置し、これにより原告らは精神的損害等を被ったなどとして、それぞれ被告に対し、不法行為に基づく損害賠償金の支払、人格権としての名誉権に基づき、本件掲示板上の名誉毀損発言の削除を認めた事案。



http://hobby.2ch.net/pet/

2ちゃんねる動物病院事件第一審（東京地判平成14年6月26日サイバー判解42頁）2/2

- 「被告は、遅くとも本件掲示板において他人の名誉を毀損する発言がなされたことを知り、又は、知り得た場合には、直ちに削除するなどの措置を講ずべき条理上の義務を負っている」。
- 「本件各発言に関する真実性の抗弁、相当性の抗弁についての主張・立証責任は、管理者である被告に存するものと解すべきであり、本件各発言の公共性、公益目的、真実性等が明らかではないことを理由に、削除義務の負担を免れることはできない」。
- 「正当な理由なく他人の名誉を毀損することが許されないのは当然であり、このことは匿名による発言であっても何ら異なるところではない」。
- 「被告は、本件にはプロバイダー責任法が適用され、同法の制定経緯、規制範囲等に照らすと、被告が本件各発言を削除しなかったことにつき削除義務違反はないと主張する」が、「被告は、‥‥本件掲示板上の発言を削除することが技術的に可能である上、通知書、本件訴状、請求の趣旨訂正申立書等により、本件1ないし3のスレッドにおいて原告らの名誉を毀損する本件各名誉毀損発言が書き込まれたことを知っていたのであり、これにより原告らの名誉権が侵害されていることを認識し、又は、認識し得たのであるから、プロバイダー責任法3条1項に照らしても、これにより責任を免れる場合には当たらない」。

2ちゃんねる動物病院事件控訴審（東京地判平成14年12月25日サイバー判解58頁）

- 控訴棄却。
- 原審被告である控訴人による次の主張をすべて退けた事例。
  - 対抗言論の理論によれば名誉毀損が成立しない
  - 本件各発言の公共性、目的の公益性、内容の真実性が明らかではないから削除義務の負わない
  - 本件にプロバイダ責任法が適用され、同法の制定経緯等に照らすとプロバイダは直接名誉毀損に当たる発言をした者ではなく、発言の公共性、目的の公益性、内容の真実性を判断することができないから、名誉毀損における真実性等の存否についてもプロバイダの責任を追及する者が主張立証責任を負う
  - 匿名の発言も表現の自由の一環として保障されるべきである
  - 不正アクセス禁止法の立法過程において議論の結果接続情報の保存義務が否定されたということから、電子掲示板における匿名性は削除義務の根拠としてはならない

錦糸眼科事件（東京地判平成15年3月31日裁判所HP）1/2

- 近視矯正クリニック「錦糸眼科」を運営する医療法人がヤフー（被告）の電子掲示板に訴外人によって「患者が失明」などと虚偽の書き込みをされて営業上の損害を受けたと主張して行った、ヤフーに対するプロバイダ責任制限法に基づく発信者情報開示請求が認容された事例。近視矯正クリニック「錦糸眼科」を運営する医療法人「メディカルドラフト会」が電子掲示板に「患者が失明」などと虚偽の書き込みをされて営業上の損害を受けたと主張して行った、ヤフーに対するプロバイダ責任制限法に基づく発信者情報開示請求が認容された事例。訴え提起後ヤフーは、投稿者のメールアドレスだけを開示し、本人が原告側に身元を明らかにして謝罪したが、投稿者が競合する医療機関関係者だったので、組織ぐるみの疑いがあり、発信元パソコン特定の必要があるとして、IPアドレス及び発信時刻の開示を求めたもの。
- 「名誉毀損行為を理由とする不法行為については，その行為が①公共の利害に関する事実に係り，②専ら公益を図る目的に出た場合には，③摘示された事実がその重要な部分について真実であることの証明があったときには，上記行為の違法性が阻却され，不法行為は成立しないものと解されているが，発信者情報開示請求訴訟においては，権利侵害要件の充足のためには，当該侵害情報により原告（被害者）の社会的評価が低下した等の権利の侵害に係る客観的事実のほか，当該侵害情報による侵害行為には，上記の①から③までの違法性阻却事由……のうち，そのいずれかが欠けており，違法性阻却の主張が成り立たないことについても主張，立証する必要がある」。「しかしながら，名誉毀損行為を理由とする不法行為訴訟においては，主観的要件に係る阻却事由として，④摘示された事実が真実であることが証明されなくとも，その行為者においてその事実を真実と信ずるについて相当の理由があるときには，当該行為には，故意又は過失がなく，不法行為の成立が否定されると解されているが，このような主観的要件に係る阻却事由については，発信者情報開示請求訴訟における原告（被害者）において，その不存在についての主張，立証をするまでの必要性はない」。

錦糸眼科事件（東京地判平成15年3月31日裁判所HP）2/2

- 「被告は，訴外人が原告に対して損害賠償及び謝罪・訂正文の掲載を提案しているのであるから，原告には本件発信者情報の開示を受けるべき正当な理由はないと主張する」が，「原告と訴外人との間で和解が成立して損害の賠償が行われ，原告の損害賠償請求権が消滅した等の特段の事情が存する場合は格別，訴外人が原告に対して上記の損害賠償等の提案を行ったとしても，今後，原告，訴外人間の交渉がまとまらず，原告において訴訟等の法的手続をとらざるを得なくなることも十分あり得るのであるから，上記の訴外人の損害賠償等の提案の事実は，これをもって，原告について本件発信者情報の開示を受けるべき正当な理由を否定」できない。
- 「発信者情報開示請求訴訟において，原告（被害者）が既に発信者情報のうちの一部の情報を把握している場合であっても，……直ちにその余の発信者情報についての開示を受けるべき正当な理由の存在が否定されるものではない」。「４条１項……にいう『発信者』……を特定する場合には，当該侵害情報を流通過程に置く意思を有していた者が誰かという観点から判断すべきであり，例えば，法人の従業員が業務上送信行為を行った場合には，当該法人が『発信者』に当たるものと解すべきである……。したがって，……発信者情報開示請求訴訟において，原告（被害者）が既に発信者情報の一部を把握しており，送信行為自体を行った者が特定されているような場合であっても，その余の発信者情報の開示を受けることにより，当該侵害情報を流通過程に置く意思を有していた者，すなわち，当該送信行為自体を行った者以外の『発信者』の存在が明らかになる可能性があるのであるから，原告（被害者）が当該侵害情報の『発信者』を特定し，その者に対して損害賠償請求権を行使するためには，上記の総務省令が定めるすべての発信者情報の開示を受けるべき必要性がある」。

羽田タートルサービス発信者情報開示請求事件（東京地判平成15年4月24日 ）

- インターネット上のウェブサイトに掲載された「奴隷労働で酷使する」などの情報により名誉を毀損されたとする原告が、被告に対しプロバイダ（ウェブオンライン）がプロバイダ責任制限法4条1項にいう「開示関係役務提供者」に当たり、同社を被告（ソニーコミュニケーションネットワーク）が吸収合併したことで地位を承継したとして、同項に基づき発信者情報開示を求めた事案
- 本件名誉毀損サイトは、株式会社ゼロからレンタルサーバサービスの提供を受けて開設されたものなので、原告がゼロに情報の開示を求めたが、発信者のメールアドレスとID・パスワードしか情報開示を受けられず、他の情報は把握していないということであった。
- 本件メールアドレスはウェブオンラインが付与したものであったが、同社と合併した被告が開示要求を拒んだので本訴が提起された。
- 本判決は、「発信者とホームページ提供業者の1対1の電気通信に過ぎないから、それを媒介するにすぎない経由プロバイダをもって、特定電気通信役務提供者（開示関係役務提供者）と解することはできない」として、書き込みがあったサイトと直接の関係がない被告は「請求の対象にならない」、「通信の秘密にかかわる守秘義務を解除するもので、安易な拡張解釈は許されない」「発信者の特定が不可能となる場合でも、法解釈としてプロバイダに開示請求はできない」と判示した。

2ちゃんねる・DHC事件
東京地判平成15（2003）年7月17日

- インターネット上の電子掲示板において名誉及び信用の毀損に当たる発言が書き込まれた場合について，電子掲示板の運営・管理者には前記発言を削除すべき条理上の義務があるとし，運営・管理者の損害賠償責任が認められた事例。
- 「プロバイダー責任制限法との関係で，削除義務違反の有無について検討してみるに，同法3条1項は，インターネット上の電子掲示板の情報の流通により他人の権利が侵害された場合，プロバイダー等が当該情報の流通によって他人の権利が侵害されていることを知っていたとき，又は，そのような情報の流通を知っている場合であって，これによる他人の権利侵害を知ることができたと認めるに足りる相当な理由があるときでなければ，賠償の責めに任じない旨規定しているのであるが，本件のようにあるスレッドに他人の名誉や信用を毀損する多数の発言が書き込まれているような場合においては，その中の個々の発言を具体的に認識するまでの必要はなく，当該スレッド内に前判示のような危険性を有する発言が存在しているとの認識があれば，他人の権利を侵害するような性質の情報が流通しているとの認識があったといって差し支えない。そして，本件においては，被告にこのような意味での認識があった」

パワードコム発信者情報開示請求事件（東京地判平成15（2003）年9月12日）

- 「WinMX」によるインターネット経由の情報流通により自己のプライバシー権を侵害された旨主張する原告らが、当該情報の流通に当たり発信者側の通信設備とインターネットとの間の通信を媒介したインターネット・サービス・プロバイダ事業者（被告）に対し、プロバイダ責任制限法4条1項に基づき、上記発信者の氏名及び住所の開示を求めた事案で、開示請求が認められた事例。
- 「ウインエムエックスによる電子ファイルの送信は、プロバイダ責任制限法4条1項、2条1号にいう『特定電気通信』に該当する」
- 「被告は、①ウインエムエックスにより送信側コンピュータから受信側コンピュータに対して電子ファイルが送信される際、送信側プロバイダの通信装置は、送信側ユーザーと受信側ユーザーとの間の１対１の通信を媒介しているにすぎないから、ウインエムエックスによる電子ファイルの送信は、『不特定の者によって受信されることを目的とする電気通信の送信』に該当しない」と主張するが、「送信側ユーザーは、電子ファイルをウインエムエックス共有フォルダに記録することによって、だれでも当該電子ファイルを取得することができる状態に置いたのであり、送信側コンピュータと受信側コンピュータとの間の当該電子ファイルのやりとりが1対1の通信にみえることは、このように不特定の者へ向けられて送信された電子ファイルに含まれた情報が、実際に受信された時点における当該受信のみを基準としてみれば、1対1の通信であるようにみえることを意味するにすぎない」から、「1対1の通信にみえることは、何ら当該通信が『不特定の者によって受信されることを目的とする電気通信』であることを否定する理由となるものではない」。
- 「ウインエムエックスによる情報の流通により権利を侵害されたと主張する者は、ウインエムエックスによる電子ファイルの送信が『特定電気通信』であると主張して、送信側プロバイダに対し、送信側ユーザーに関する情報の開示を請求することができる。」

企業批判サイト・書き込みへの対処

- 意図的に「無視」することには一定の合理性がある
  - 挑発に乗れば、ますますエスカレートする危険。相手は「お祭り」と一緒。
  - 「内部告発」を装った場合など、経営陣の過剰反応に注意
- 「無視」することが困難なケースも存在
  - 具体性が高い内容の場合など、放置すれば損害が発生するようなケース
  - それが虚偽の内容であれば対処を要する
- まずは管理者に対する削除要請が先行
  - 「2ちゃんねる」では削除要請文が掲載され、被害増幅の危険
- 民事手続では発信者の特定が先行
  - プロバイダの場合はテレコムサービス協会が書式等を作っており、同協会のサイトで配布を受けられる
  - 一般にプロバイダは開示に慎重な姿勢
  - 経営陣が特定を強く求める場合がある
- 刑事手続が有効な場合もある
  - 発信者の特定が困難な場合など
- 本当の内部告発には日頃からの対応が必要
  - 内部告発用窓口の設置など
  - モニタリング（社内からの悪質な書き込み防止）
  - 社内から悪質サイトへの接続遮断措置の方が有効な場合もある

ご 質 問

- okamura@mail.law.co.jp
- http://www.law.co.jp/