JPCERT/CC
重要インフラ情報セキュリティフォーラム2008
2008.2.20
於：秋葉原コンベンションホール

裁判例から考える
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

ケース1：Yahoo!BB情報漏えい事件

- 事案
  - BBテクノロジー株式会社はインターネット接続等の総合電気通信サービス「Yahoo!BB」を運営。
  - 社外からのメンテナンス作業のためにリモートメンテナンスサーバを設置。同サーバの中に同サービスの顧客データベースとして原告らの氏名・住所等の個人情報を保有管理。
  - 業務委託先から派遣されていた甲に、同サーバを含むサーバ管理業務を行わせ、共有アカウントを与えていた。
  - ところが、甲の退職後も同アカウント等の変更を行わなかったため、甲と第三者乙が共同もしくは単独で同アカウントを用いて不正アクセスして顧客データベースのデータを不正取得し、もって外部流出。
- 大阪地裁平成18年5月19日判決（（判タ1230号227頁）
  - ユーザー名・パスワードの管理が極めて不十分であったことなど、外部からの不正アクセスを防止するための相当な措置を講ずべき注意義務を怠った過失により原告らのプライバシーの権利が侵害されたとして、不法行為責任を認めた。
  - なお、同被告と共同して同サービスを提供していたとしてなされた被告ヤフー株式会社に対する請求について、本判決は、両被告は顧客情報をそれぞれ別個に管理しており、被告BBテクノロジー株式会社に対する監督義務も認められないとして棄却。

漏えい事件と企業の法的責任

- 漏えい情報が個人データなら個人情報保護法違反
  - 行政との関係による責任
  - 個人データが対象
  - 同法に基づく各省庁のガイドラインによって次の3つの措置必要
    1. 主務官庁への届出－漏えい内容・原因を含む
       →今まで何をしていたのか、再発防止策をどうするのかが問われる
    2. 被害者への連絡
    3. 経緯等の公表
  - 主務官庁から勧告、命令、命令違反には罰則。

- 業法違反に問われる場合もあり

- プライバシー権侵害の責任
  - 被害者との関係による責任
  - 漏えい情報が単なる個人情報でも責任
  - 差止請求と損害賠償請求
    - 従業者の行為について企業は民法715条に基づく使用者責任を負う
    - 雇用関係がなくても実質的な指揮・命令関係があれば責任

ケース2：TBC顧客情報漏えい事件

- 事案
  - エステサロンを経営する被告がウェブサイトで実施したアンケート等を通じて原告らから提供され保有管理していた原告らの個人情報を含む電子ファイルを，平成14年ころ，インターネット上において第三者が閲覧可能状態に置き，実際に第三者がそれにアクセスしてその個人情報を流出させたことによって原告らのプライバシーを侵害したとして，原告らが，被告に対し，不法行為に基づき慰籍料等の支払を求めた事案。本件当時，被告は，外部委託先に対し，本件ホームページ制作保守契約を締結して，本件ウェブサイトのコンテンツの内容の更新，修正業務等を委託するなどしていた。
- 東京地裁平成19年2月8日判決（判例時報1964号113頁）
  - 本件情報流出事故が発生した平成14年ころも，個人情報を取り扱う企業には，事業内容等に応じて，個人情報保護のために安全対策を講ずる法的義務が課せられていたが，外部委託先は，その提供する業務に関する技術的水準として，個人情報を含む電子ファイルについては，一般のインターネット利用者からのアクセスが制限されるウェブサーバの「非公開領域」に置くか，「公開領域」（ドキュメントルートディレクトリ）に置く場合でも，アクセスを制限するための「アクセス権限の設定」か「パスワードの設定」の方法によって安全対策を講ずる注意義務があったが，これを怠り，本件ウェブサイトを被告専用のサーバに移設する際，本件電子ファイルをサーバ内の公開領域に置いたうえ，第三者のアクセス権限を制限するような設定を講じなかったため，本件ウェブサイトにアクセスした第三者が本件電子ファイルを閲覧することができる状態にし，実際に，本件ウェブサイトを閲覧した第三者によって，本件情報がインターネット上に流出したのであるから，ネオナジーは不法行為責任を負うとした。そして，民法715条の使用者責任にいう使用関係の有無の判断は実質的な指揮，監督関係の有無によるが，被告は，本件ウェブサイトの管理を主体的に行い，外部委託先に委託したコンテンツの内容の更新，修正作業等についても実質的に指揮，監督していたとして，被告に使用者責任が成立するとした。
  - 認められた損害額は，原告ら一人あたり原則として慰謝料3万円と弁護士費用5000円。

TBC顧客情報漏えい事件が残した教訓

- 委託先の監督の重要性
  - この事件では、委託先の過失行為について、委託元が民法の使用者責任に基づく損害賠償義務を負わされた。
    - 使用者責任にいう使用関係の有無の判断は実質的な指揮・監督関係の有無によるので、雇用関係は不要。
    - それに対する選任・監督に落ち度がないことを立証しなければ責任を免れない。そのため、責任を免れることは実際には困難。
  - 個人情報保護法22条は、個人データの安全管理措置につき、委託元の委託先に対する監督義務を課している。
- 委託先に対する監督方法
  - 個人情報保護法22条を受けて、多くの省庁のガイドラインでは、委託先に対する監督方法として、次の措置を求めている。この手法は、個人データ以外の情報管理全般に活用できる。
    1. 委託先選定基準の確立と、それに即した選定
    2. 適正な事項を盛り込んだ委託契約の締結
       資本関係がある会社なら、それに基づいてコントロール可能。しかし、独立した企業同士なら、契約によってコントロールするほかない。
    3. 委託契約が遵守されているかどうかの確認
    4. （以上の事項の見直し）

参考ー個人情報保護法・経済産業分野ガイドライン「委託先の監督」(法22条関連)

「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、法第20条に基づく安全管理措置を遵守させるよう、受託者に対し必要かつ適切な監督をしなければならない(中略)。その際、本人の個人データが漏えい、滅失又はき損等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の性質及び個人データの取扱状況等に起因するリスクに応じ、必要かつ適切な措置を講じるものとする。『必要かつ適切な監督』には、委託契約において、当該個人データの取扱に関して、必要かつ適切な安全管理措置として、委託者、受託者双方が同意した内容を契約に盛り込むとともに、同内容が適切に遂行されていることを、あらかじめ定めた間隔で確認することも含まれる。」(同ガイドライン37頁、なお傍線著者)

【個人データの取扱いを委託する場合に契約に盛り込むことが望まれる事項】

- 委託者及び受託者の責任の明確化
- 個人データの安全管理に関する事項(個人データの漏えい防止、盗用禁止に関する事項・委託契約範囲外の加工、利用の禁止・委託契約範囲外の複写、複製の禁止・委託契約期間・委託契約終了後の個人データの返還・消去・廃棄に関する事項)
- 再委託に関する事項(再委託を行うに当たっての委託者への文書による報告)
- 個人データの取扱状況に関する委託者への報告の内容及び頻度
- 契約内容が遵守されていることの確認(例えば、情報セキュリティ監査なども含まれる。)
- 契約内容が遵守されなかった場合の措置
- セキュリティ事件・事故が発生した場合の報告・連絡に関する事項

ケース3：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生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（京都地裁平成13年2月24日判決）
  - 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（大阪高裁平成13年12月25日判決）
  - 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って」おり、「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」られるので、市は使用者責任を負う。
- 上告審（最高裁平成14年7月11日決定）
  - 市の上告を棄却

宇治市住民基本台帳データ流出事件が残した教訓

- 宇治市から見れば委託先の監督の問題
  - 民法の使用者責任に基づく損害賠償義務を負わされた点でTBC顧客情報漏えい事件と同様。
  - 委託の連鎖は困難な問題。
    - 委託契約に対応策を盛り込む必要。
    - 具体的には、再委託の際の同意取得義務、再委託先に対する監督義務、再委託先の行為について委託先は責任を負うことなど。
- 委託先からみれば従業者管理の問題
  - 個人情報保護法21条は、従業者に対する監督義務を課す。これを受けて、多くの省庁のガイドラインでは、委託先に対する監督方法として、次の措置を求めている。この手法も、個人データ以外の情報管理全般に活用できる。
    1. 従業者からの誓約書・覚書等の徴収
    2. 内部規程の整備
    3. 遵守されているかどうか、確認のための措置
    4. 教育・啓発
    5. （以上の事項の見直し）

参考ー事業者からの個人情報漏えい事案の状況
（内閣府平成18年度調査）

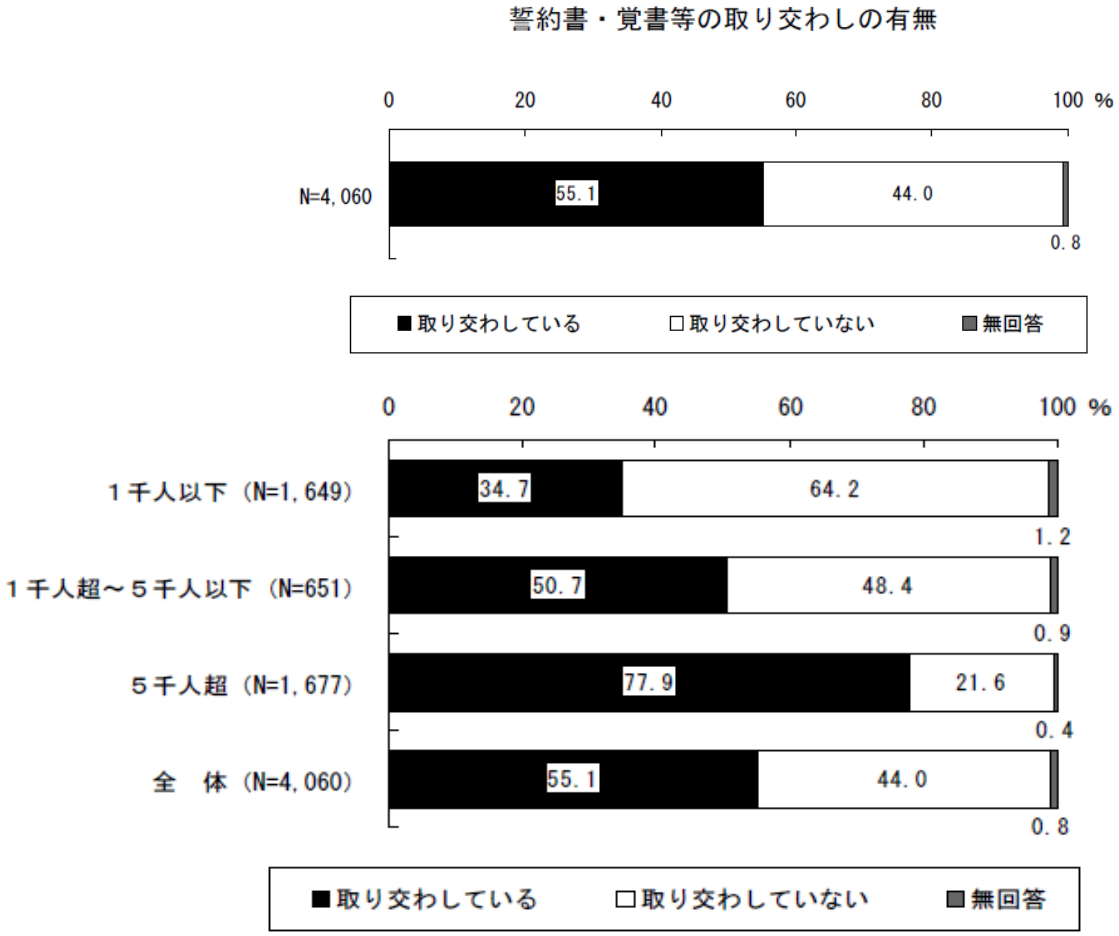
漏えいした者 ＼ 漏えい元	従業者				第三者				その他	不明	合計
	意図的	不注意	不明	計	意図的	不注意	不明	計			
事業者	6 (0.7%)	492 (55.1%)	5 (0.6%)	503 (56.3%)	101 (11.3%)	0 (0.0%)	1 (0.1%)	102 (11.4%)	4 (0.4%)	7 (0.8%)	616 (69.0%)
委託先	37 (4.1%)	164 (18.4%)	1 (0.1%)	202 (22.6%)	50 (5.6%)	3 (0.3%)	2 (0.2%)	55 (6.2%)	5 (0.6%)	4 (0.4%)	266 (29.8%)
不明	－	－	－	－	－	－		－	－	11 (1.2%)	11 (1.2%)
合計	43 (4.8%)	656 (73.5%)	6 (0.7%)	705 (78.9%)	151 (16.9%)	3 (0.3%)	3 (0.3%)	157 (17.6%)	9 (1.0%)	22 (2.4%)	893 (100.0%)

（注）（ ）内は、漏えい事案全体（893 件）に対する割合。

① 漏えい元は、「事業者」から直接漏えいした事案が全体の約7割、「委託先」から漏えいした事案が全体の約3割。
② 「事業者」及び「委託先」の中で、実際に漏えいに関わった者（以下「漏えいした者」という。）についてみると、「従業者」が全体の8割近くを占める。
③ 漏えい原因は、「従業者」については「意図的」なものが43件、「不注意」によるものが656件。ほとんどが「不注意」によるもの。「第三者」については、「意図的」なものが151件、「不注意」によるものが3件。ほとんどが「意図的」なもの。

出典・内閣府「平成18年度個人情報保護法施行状況の概要」（平成19年4月）

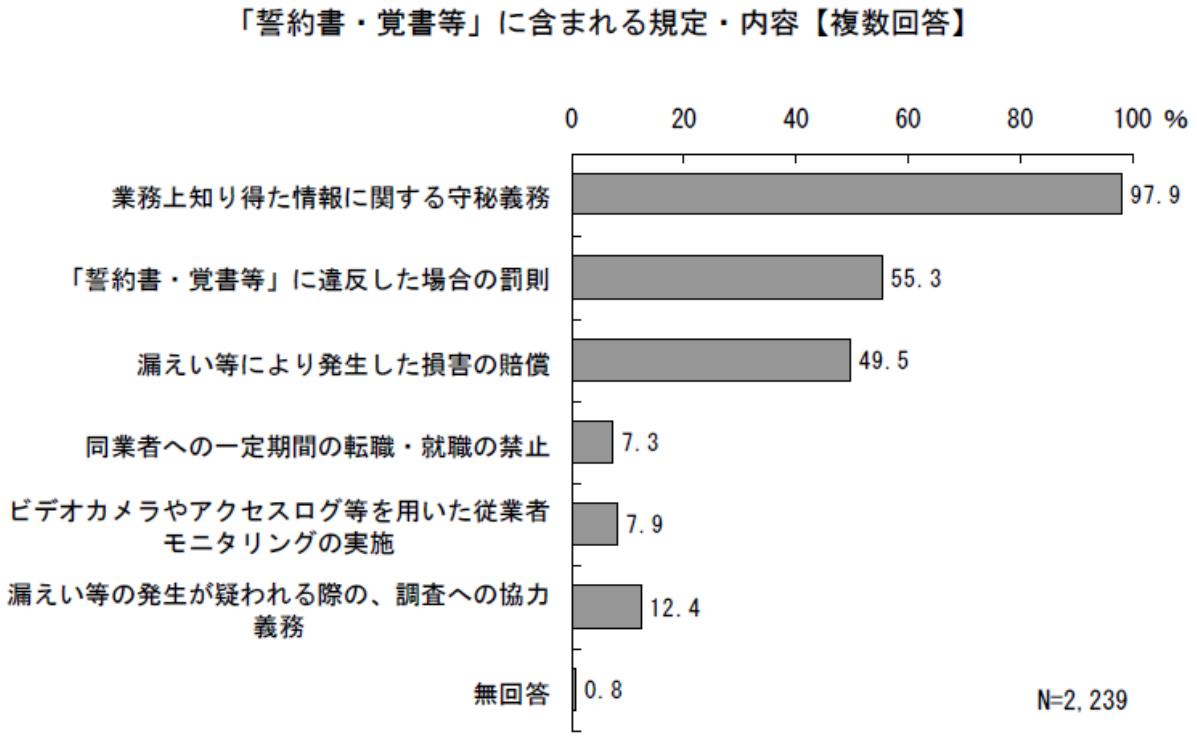
参考－従業員との個人情報保護関連の「誓約書」・「覚書」等の締結状況（内閣府平成18年度調査）



○従業者と個人情報保護に関する「誓約書・覚書等」を「取り交わしている」事業者は6割弱。
○保有個人情報数が多い事業者ほど、「誓約書・覚書等」を「取り交わしている」事業者の割合は高い。
○保有個人情報数が「5千人超」の事業者は「誓約書・覚書等」を「取り交わしている」事業者が8割弱である一方、「1千人以下」の事業者は3割強。

出典・内閣府「個人情報の保護に関する事業者の取組実態調査（概要）」（平成19年4月）
http://www5.cao.go.jp/seikatsu/shingikai/kojin/20th/20070425kojin2.pdf

「誓約書・覚書等」に含まれる規定・内容（平成18年度調査）



○「誓約書･覚書等」には、ほぼすべての事業者で「業務上知り得た情報に関する守秘義務」に関する事項が含まれている。

○「『誓約書･覚書等』に違反した場合の罰則」、「漏えい等により発生した損害の賠償」に関する事項が含まれている事業者は5割前後であり、相対的に多い。

出典･内閣府「個人情報の保護に関する事業者の取組実態調査（概要）」（平成19年4月）
http://www5.cao.go.jp/seikatsu/shingikai/kojin/20th/20070425kojin2.pdf

ケース4：F社Z事業部事件判決

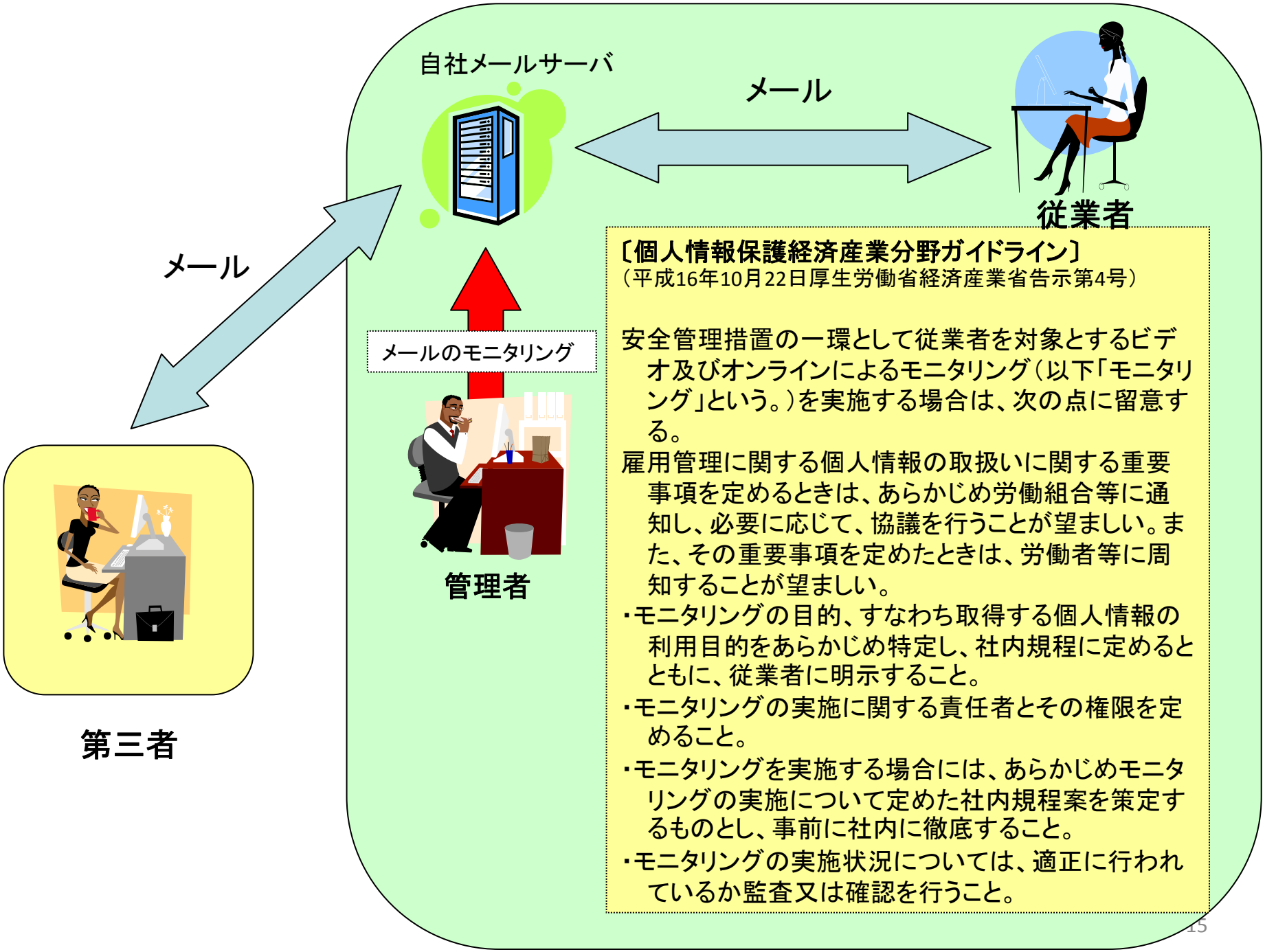
- 事案
  - 会社の事業部長である被告から，直属のアシスタントである女性がセクシャルハラスメントを受け，社内ネットワークシステムを用いて送受信した女性と夫との私用メールを被告が監視して許可なく閲読したとして，前記夫婦が不法行為に基づき損害賠償請求した事案である。私用メールに関するプライバシー権の有無を判断する前提として，私用メールの許容性が問題となった。
- 東京地裁平成13年12月３日判決（労判826号76頁）
  - セクシャルハラスメントの事実は認められないとしたうえ，「F社の米国本部には，会社のネットワークシステムを用いた電子メールの私的使用の禁止等を定めたガイドラインがあったものの，日本国内のZ事業部においてはこれが周知されたことはなく，社員による電子メールの私的使用の禁止が徹底されたこともなく，社員の電子メールの私的使用に対する会社の調査等に関する基準や指針，会社による私的電子メールの閲読の可能性等が社員に告知されたこともない」という事実を認定した。そして，前記「事実関係の下では，会社のネットワークシステムを用いた電子メールの私的使用に関する問題は，通常の電話装置におけるいわゆる私用電話の制限の問題とほぼ同様に考えることができる。すなわち，勤労者として社会生活を送る以上，日常の社会生活を営む上で通常必要な外部との連絡の着信先として会社の電話装置を用いることが許容されるのはもちろんのこと，さらに，会社における職務の遂行の妨げとならず，会社の経済的負担も極めて軽微なものである場合には，これらの外部からの連絡に適宜即応するために必要かつ合理的な限度の範囲内において，会社の電話装置を発信に用いることも社会通念上許容されていると解するべきであり，このことは，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に関しても基本的に妥当する」とした。そして，保護の範囲は通常の電話装置の場合よりも相当程度低減され，社会通念上相当な範囲を逸脱した監視の場合に限りプライバシー権侵害となるが，本件では原告らの私的使用の程度が許容限度を超えていること等を理由に，監視行為が前記範囲を逸脱したといえないとして，請求を棄却した。

ケース5：グレイワールドワイド事件判決

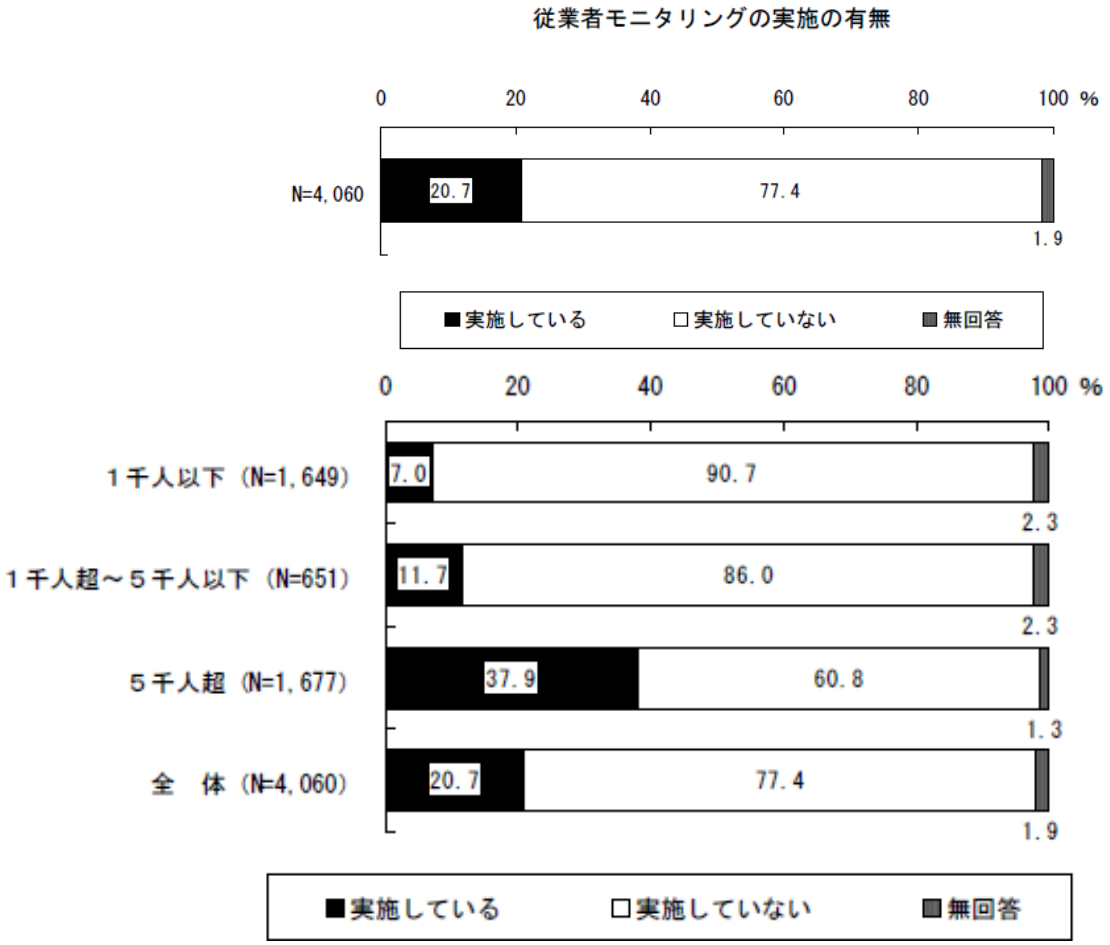
- 事案
  - –就業時間中に私用メールを行ったこと等を理由とする解雇の効力を，労働者側が争った事案 。
- 東京地裁平成15年9月22日判決（労判870号83頁）
  - –労働者は職務専念義務を負うとしたうえ，「労働者といえども個人として社会生活を送っている以上，就業時間中に外部と連絡をとることが一切許されないわけではなく，就業規則等に特段の定めがない限り，職務遂行の支障とならず，使用者に過度の経済的負担をかけないなど社会通念上相当と認められる限度で使用者のパソコン等を利用して私用メールを送受信しても上記職務専念義務に違反するものではない」とした。
  - –本件では「就業時間中の私用メールが明確には禁じられていなかった上，就業時間中に原告が送受信したメールは１日あたり2通程度であり，それによって原告が職務遂行に支障を来したとか被告に過度の経済的負担をかけたとは認められず，社会通念上相当な範囲内にとどまる」ことを理由に，職務専念義務違反を認めなかった。
  - –さらに，本判決は，他に解雇事由として主張された点を検討しても本件解雇が客観的合理性・社会的相当性を備えているとは評価し難いとして，解雇権の濫用にあたり解雇は無効であるとした。

F社Z事業部事件・グレイワールドワイド事件が残した教訓

- 違反した従業者に対する懲戒が、実効性を保つための有効な方法となる。
  - これらのケースは、就業中の私用メールにつき、主として会社における職務遂行の支障となるか、会社の経済的負担はどの程度かという基準によって、社会通念上の相当性について判断。その限度内では私用メールにも許容性が認められる半面、限度を超せば懲戒処分の対象になりうるとしている。
- しかし、これらのケースは、内部規程が定められていなかった事例。
- F社Z事業部事件判決
  - 「F社の米国本部には，会社のネットワークシステムを用いた電子メールの私的使用の禁止等を定めたガイドラインがあったものの，日本国内のZ事業部においてはこれが周知されたことはなく，社員による電子メールの私的使用の禁止が徹底されたこともなく，社員の電子メールの私的使用に対する会社の調査等に関する基準や指針，会社による私的電子メールの閲読の可能性等が社員に告知されたこともない」
- グレイワールドワイド事件判決
  - 「就業規則等に特段の定めがない限り，職務遂行の支障とならず，使用者に過度の経済的負担をかけないなど社会通念上相当と認められる限度で使用者のパソコン等を利用して私用メールを送受信しても上記職務専念義務に違反するものではない」
- 事前に内部規程を定めておけば、もっとスムーズに処分できた可能性。
- ISO/IEC 17799:2005（JIS Q 27002:2006）
  - 組織の情報資産を適切に保護し，維持するという管理目的のために，情報および情報処理システムと関連する情報資産の利用の許容範囲に関するルールを明確化したうえ，文書化して実施すべきこと（箇条7.1.3）、従業員のセキュリティ違反に対する正式な懲戒手続を備えること（8.2.3）を求めている。


自社メールサーバ
メール
従業者
メール
メールのモニタリング
管理者
第三者
〔個人情報保護経済産業分野ガイドライン〕
（平成16年10月22日厚生労働省経済産業省告示第4号）
安全管理措置の一環として従業者を対象とするビデオ及びオンラインによるモニタリング（以下「モニタリング」という。）を実施する場合は、次の点に留意する。
雇用管理に関する個人情報の取扱いに関する重要事項を定めるときは、あらかじめ労働組合等に通知し、必要に応じて、協議を行うことが望ましい。また、その重要事項を定めたときは、労働者等に周知することが望ましい。
・モニタリングの目的、すなわち取得する個人情報の利用目的をあらかじめ特定し、社内規程に定めるとともに、従業者に明示すること。
・モニタリングの実施に関する責任者とその権限を定めること。
・モニタリングを実施する場合には、あらかじめモニタリングの実施について定めた社内規程案を策定するものとし、事前に社内に徹底すること。
・モニタリングの実施状況については、適正に行われているか監査又は確認を行うこと。

参考－従業者モニタリングの実施の有無（内閣府平成18年度調査）



○従業者モニタリングを「実施している」事業者は約2割。
○ 保有個人情報数が多い事業者ほど、従業者モニタリングを「実施している」事業者の割合は高い。
○保有個人情報数が「５千人超」の事業者は従業者モニタリングを「実施している」事業者が4割弱である一方、「１千人以下」、「１千人超～５千人」の事業者は１割前後。

出典・内閣府「個人情報の保護に関する事業者の取組実態調査（概要）」（平成19年4月）
http://www5.cao.go.jp/seikatsu/shingikai/kojin/20th/20070425kojin2.pdf

ケース6：北海道警察江別署捜査情報漏えい事件

- 北海道警察江別署捜査情報漏えい事件
  - 道交法違反容疑で逮捕、不起訴となった江別市の社員（原告）を被疑者とする捜査関係文書が、北海道江別署の男性巡査の私物パソコンからインターネットを通じて外部に流出したとして、原告の被った精神的損害の賠償200万円を北海道（被告）に請求した訴訟。ファイル交換ソフト「Winny」を私有パソコンにインストールしており、パソコンがアンティニーウイルスに汚染されていることを知らずに、私的な目的でWinnyを起動させインターネットに接続した結果、パソコンのデスクトップ画面上に保存されていた捜査関係文書がアンティニーによってパソコンの公開用フォルダに複写され、他のWinny利用者に閲覧可能な状態となり、そのことがインターネット利用者の情報交換を目的とするホームページに掲載されたこともあって、捜査情報が不特定多数のWinny利用者によって閲覧され、ダウンロードされるに至った。
- 第一審（札幌地裁平成17年4月28日判決）
  - 巡査がパソコンを使用して本件捜査関係文書を作成した際に作成途中の同文書をハードディスクに保存した行為は職務行為そのものであり、また、同巡査が上記文書をパソコン内に保存したままパソコンを自宅に持ち帰り、インターネットに接続させた行為は、作成途中の本件捜査関係文書の保存、管理という点において捜査関係文書の作成という職務行為と関連して一体不可分のものというべきであるから、巡査の上記原因行為は「職務を行う」についてのものということができるとして、慰謝料40万円の支払を北海道に命じた。
- 控訴審（札幌高裁平成17年11月11日判決）
  - 原判決を取り消し、請求棄却。報道によれば、自宅でネット接続した行為を「職務とは無関係の行為」と判断。道警の管理責任については「当時、このウイルスは広く知られておらず、流出の予見可能性はなかった」とした。

北海道警察江別署捜査情報漏えい事件が残した教訓

- 無理な内部ルール策定は、かえって命取り
  - 本件では……
    1. 私物パソコン持ち込みを許可制とする
    2. 私物パソコン内蔵ハードディスクに業務（職務）データを保管してはならない
    3. 持ち帰り時には上司のチェックを受けなければならない

    ……という内部ルールが設けられていたが、2と3に違反していたことが過失の認定事由となった。しかし、
    1. 許可するかどうかの基準をどうするか？
    2. それならどこに保管せよというのか？
    3. 上司には、チェックできる時間とスキルがあるのか？
  - 結局、無理な内部ルールを作っても結局は守られないので、責任を重くするおそれを発生させるだけで終わる。
  - むしろ、私物パソコンの持ち込みを禁止する方が現実的
- 「私物パソコンに対してもWinnyインストール禁止」という内部ルールは可能か？
- インシデント発生時に、持ち込み私物パソコン内部を、所有者の意に反してチェックできるか？
  - 所有権の問題－窃盗とならないか？
  - プライバシー権の問題

ケース7：前橋信金事件

- 事案
  - この信用金庫の労働組合が事実上分裂。その後も新旧執行部の対立。分裂前の組合には多額の組合費が設立以来蓄えられ、この信用金庫に預金。ところが、新執行部は組合員旅行を企画。それによって預金の大部分が費消されることが予想。旧執行部は、旅行への支出により組合財政が破綻することを恐れ、組合財産を守るため、組合預金の払戻などを禁止する仮処分を申請するしかないと考えた。そのためには預金残高を確認する必要。ところが、組合口座の名義人として通帳・印鑑を握っていた会計担当者は、新執行部側の支持者。その結果、旧執行部が残高を確認しようとしても、協力を得ることが難しい状況。信用金庫では当時、すでに預金処理についてオンラインシステムを導入。そのための内部ルールとして、オンライン事務取扱要領も定めていた。「取扱要領」には、オンライン端末機の管理に関し、担当職員は操作に必要なオペレーターキーの貸与を禁止すること、担当職員のみがこれを操作すべきことなどが規定。旧執行部の代表である執行委員長は困り果てた末、端末機の操作方法を知っている部下に依頼して、組合預金の残高を確認してもらうことにした。しかし、この部下には端末機操作の権限はなかった。彼は、操作担当者がオペレーターキーを装着したまま離席したすきに、端末機を使って組合預金の残高を確認した。まもなく事態は露見した。端末機操作を目撃した職員から通報があった。設置された防犯カメラは部下の行為をとらえていた。そのため、わずか数カ月後、執行委員長らは就業規則に基づいて信用金庫から懲戒処分を受けた。執行委員長は自らが受けた停職処分を不服に思った。そこで、停職処分が無効であるとして、信用金庫を相手取って裁判を起こした。信用金庫側は、就業規則の「規定違反」「秘密漏洩」「職員としての不適格非行」に該当するので停職処分は有効であるとして争った。
- 前橋地裁昭和61年5月20日判決（判例時報1253号136頁）
  - 原告の執行委員長側が勝訴し、停職処分は無効であるとされた。
- 東京高裁昭和62年8月31日判決（判例時報1253号134頁）
  - 信用金庫側が逆転勝訴、停職処分を有効とした。

前橋信金事件が残した教訓

- 地裁判決
  - 「端末機の操作に関しては、現実には、被告が想定していたその取扱要領に反する運用がなされていたため、原告において、端末機操作担当者以外の従業員が、被告に何らの損害を及ぼすおそれのないような操作をすることについて、さほど重大な非違とは考えていなかったこと」を指摘。
  - つまり、「取扱要領」が有名無実化しかけていたことが重視。そのため、重い懲戒処分をもってのぞむのは「著しく不合理であり、社会通念上相当性を欠いたものといわざるをえない。」とした。実効性を欠いた社内ルールは、裁判の場でも意味が乏しいという判断。
- 高裁判決
  - 「取扱要領」が有名無実化しかけていたことは事実であると認めている点では、地裁判決と変わらない。しかし、それを危惧した信用金庫側が「取扱要領」に従った扱いを周知徹底させるべく努力していたことを重視。それにもかかわらず、その矢先に違反行為をおこなったのだから、違反した責任は重いとした。
- 教訓
  - せっかく社内ルールを作っても、日ごろから、きちんとした教育啓発活動をおこなっていなければ、ルールの実効性は保てない。これでは「絵に描いたモチ」。それだけでなく、万一の場合に裁判所で保護してもらうことも困難になる。そうした教訓を、この事件は示している。内部点検・監査なども同様であるはず。

おわりに