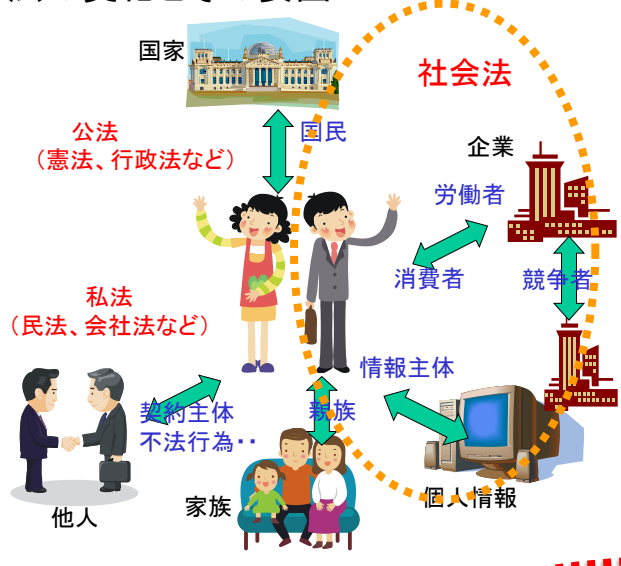
日本経営倫理士協会　第5回シンポジウム2014　　2014年3月5日

情報コンプライアンスと企業力

～企業情報の利活用と保護～

関西大学 社会安全学部
教授・博士（法学） 髙野 一彦

法の変化とその要因



特に社会法分野

社会の変化と共に「社会・公共の利益」も変化するため、その時代の社会的な課題に対応して、法も変化する

1. 欧米先進諸国の法制度との整合
2. 訴訟及び社会的課題

同様に消費者保護、環境法、公正競争、労働法、プライバシー・個人情報保護など・・

「個人情報」に関する国内外の諸課題と法規制

① 情報流出事件

1999年　宇治市　約22万件
：
2004年　ヤフーBB　460万件
2006年　防衛庁「秘」情報流出
2007年　大日本印刷　863万件
2007年　警視庁捜査情報　1万件
2009年　アリコ生命　13万件
2009年　三菱UFJ証券　148万件
2011年　ソニーPSN　7000万件
：

1999年
JIS Q 15001（Pマーク）
2003年
個人情報保護法成立

1998年
EUデータ
保護指令施行

② ICT発展に伴って顕在化した様々な課題

③ 国際的整合

2012年
EU一般データ
保護規則提案
米国消費者プライバシー権利憲章

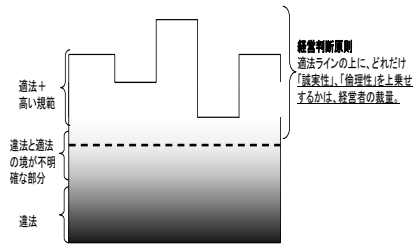
2013年
行政手続番号法成立
2015年
個人情報保護法の改正？

経営者の経営判断の適法性に関する判断基準

株主代表訴訟判決の違法性判断の類型

類型	役員の責任	判断基準
経営判断原則	○～×	**①前提事実の認識に重要かつ不注意な誤認がない ②意思決定及びその過程が著しく不合理でない**
内部統制システム構築義務	×	構築していなかった （ただし判例少ない）
監視義務違反	×	知ってたのに止めなかった 知り得たのに止めなかった
具体的法令違反	×	社内規定違反
	×	法令違反・定款違反

経営判断における「合理性」とは？



・経営者は、適法ラインの上に、どの程度「倫理性」、「誠実性」を上乗せして判断すれば良いのか？

・従業員は、ファジーな分野のどこに判断基準を設ければ良いのか？

① 情報流出事件に関して

企業防衛の視点から情報流出への対応

―わが国の情報法制の「間隙」―

頻発する情報流出事件

2004年　ヤフーBB顧客情報流出事件　460万件（内部者の窃取）

2006年　防衛庁／自衛隊「秘」扱い情報流出事件（ウイニー）

2007年　大日本印刷個人情報流出事件　863万件（委託先社員の窃取）

2007年　デンソー技術データ流出事件　13万点の図面（内部者の窃取）

2007年　警視庁捜査情報流出事件　1万件（ウイニー）

2009年　アリコ顧客情報漏えい事件　13万件（委託先からの流出？）

2009年　三菱UFJ証券顧客情報流出事件　148万件（部長代理の窃取）

2010年　尖閣諸島沖ビデオ映像流出、警視庁国際テロ捜査資料流出

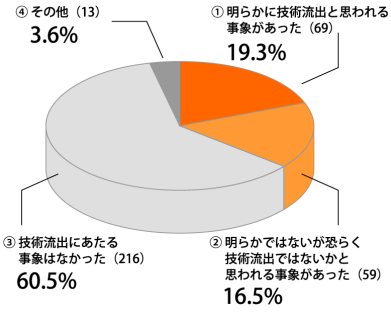
2011年　ソニーPSNから7000万人を超える個人情報が流出

2012年　新日鐵、営業秘密の不正取得で韓国鉄鋼大手パスコなどを提訴
（方向性電磁鋼板）

内部者からの「情報流出」が多く、損害は多額

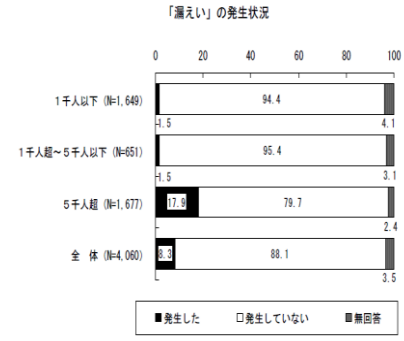
情報流出の発生頻度

技術情報の流出



出典：経済産業省「製造業関係企業に対するアンケート調査」2006年
<http://www.gov-online.go.jp/useful/article/200805/4.html>

個人情報の流出



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）」（H19.4）

「情報流出」は、他のリスクに比べて、
発生頻度が極めて高い

個人情報　漏えいと企業のリスク

情報漏えいと損害

①訴訟リスク　＝　本人のプライバシー侵害
②罰則リスク　＝　個人情報保護法違反
③損害賠償リスク　＝　契約違反により取引先より請求
③株主代表訴訟リスク　＝　管理体制の不備による損害
④その他　＝　被害者への補償、業務ストップ、信用喪失など

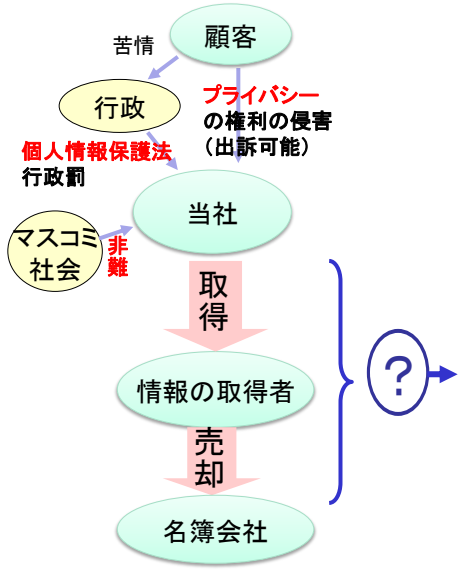
近年の情報漏えい事件

ヤフーBB　＝　450万人顧客情報流出（2004）⇒　損失29億円
アリコジャパン　＝　13万件顧客情報流出（2009）⇒　損失69億円

損失額：ヤフーBBは経産省資料、アリコは報道による

企業の『情報セキュリティー』は経営上の重要マター

情報の不正取得への処罰



情報の不正取得行為への法的制裁

	法律名	禁止行為
刑事	刑法	窃盗,業務上横領,背任など
	不正競争防止法（刑事的保護）	**営業秘密の不正取得**
	不正アクセス禁止法	不正アクセス行為
	電気通信事業法、電波法など	通信事業者による通信の秘密の侵害
	秘密保持法	職務上の秘密の漏示（公務員,弁護士など）
民事	民法	不法行為
	不正競争防止法（民事的保護）	**営業秘密の不正取得**

不正競争防止法

「不正競争防止法」による、「営業秘密」の保護

民事： 差止請求権、損害賠償請求権、信用回復措置請求権
刑事： 個人：10 年以下の懲役又は1000 万円以下の罰金 （法人：罰金3 億円以下）

「営業秘密」の概念

①秘密管理性： 秘密として管理している
②有用性： 経済的に有用な情報であること
③非公知性： 公に知られていない情報であること

争点は、「秘密管理性」

①アクセス制限： 情報にアクセスできる者を特定すること
②客観的認識可能性： 情報にアクセスした者が、それが秘密であると認識できること

※ 営業秘密の秘密管理性が争点になった81 件の裁判で、秘密管理性を認めた判例は23 件（28.4%）。（経済産業省「営業秘密管理指針」2010年、8頁）

情報の不正取得者への法的制裁は「間隙」

わが国における情報の不正取得者への刑事罰

1．情報の不正取得に対し、有体性説を有力説とする刑法の財産犯規定の適用は困難であった。

ex.大日本印刷事件東京地判昭40.6.26、京王百貨店事件昭62.9.30など
1974（昭和49）年 企業秘密漏示罪（改正刑法草案318条）の議論

2．2003年改正不正競争防止法における営業秘密侵害罪は、「秘密管理性」の要件が厳しく、実効性に乏しかった。

法的な保護を受けるために「個人情報」を「営業秘密」として管理せざるを得ず、利活用を過度に制限する「過剰反応」を生んでいる

【例】緊急連絡名簿に、㊙と書いて金庫に保管し、鍵は部長だけが使える

個人情報の不正取得者への刑事罰が必要との議論

欧米諸国との比較

営業秘密： アメリカ 96年 経済スパイ法 （Economic Espionage Act）
経済スパイ罪、トレード・シークレット窃盗罪の創設
ex.U.S. v. Okamoto, Serizawa(2001年)、U.S. v. Zhu, Kimbara（2002年）

個人データ： UK 98年 データ保護法（Data Protection Act 1998）
第55条 個人データの違法な取得等への刑事罰

Graduate School and Faculty of Safety Science FSS
© Kazuhiko.Takano

② ICTの発展に伴って顕在化した様々な課題

ICTの発展に伴って顕在化した様々な課題

(1) 行動ターゲティング広告 (Behavioral Targeting AD, BTA)

アクセスログなどを分析して最適な広告を表示する
新たなマーケティング手法だが、個人特定情報でないため、個人情報保護法の適用外

(2) ビックデータ問題

・G社 は2012年3月1日にプライバシーポリシーの統合を実施。
60以上のサービス(メール、カレンダー、Map、chromeなど)で収集する個人データを統合
・交通系カード:個人識別情報を削除した使用履歴の他社への販売の違法性、適正性に関する議論

(3) ポイントカードに紐付いた購買履歴情報

購買時にC社 のポイントカードを提示すると、購買履歴がC社に送信
⇒ 医薬品の購入履歴情報などが、販促に使われるという問題など

(4) ソーシャルメディアによる情報発信

Facebook、Twitterなどの「SNS」による従業員個人の情報発信が原因となり、企業が社会的非難を浴びる事案が急増。
⇒個人の就業時間外の行動の自由と企業秩序定立権のコンフリクト

○ポイントカード、購入医薬品データを取得 提携先企業から

朝日新聞2012年7月17日

(略)共通ポイントサービス「○ポイント」が、ドラッグストアで会員が買った医薬品の商品名をデータとして取得し、**会員に十分な説明をしないまま**販促活動などに使っていることがわかった。医薬品の購買履歴には、**本人が他人に明らかにしたくない情報**が含まれることが多い。日本薬剤師会などは「育毛剤を買った人にかつらの広告を送ったり、関節の痛みを和らげる薬を買った人に健康食品を勧めたりしないか」と懸念。厚生労働省も問題視している。

出典:朝日新聞Web版http://digital.asahi.com/articles/NGY201207160031.html?ref=comkiji_txt_end

1. 薬剤師や医薬品販売業者が正当な理由なく業務上知り得た人の秘密を漏らすことを禁じる刑法134条に抵触し秘密を漏らした罪に当たり得る。(新潟大学教授 鈴木正朝氏)

2. 本人の同意の有効性が揺らぐと、プライバシーの権利侵害としての訴訟リスク、個人情報保護法違反による行政行為のリスクが顕在化する。

顧客が、カード番号のみならず商品名も送信されることを、カードの申込・提示をもって「同意」とみなせるかが論点 **(法的な「同意」の効果≠社会的な納得感)**

カード提示の際、商品名・購入価格などの情報が、カード発行会社に送信される旨の明確な(納得性の高い)同意が必要 ⇒ 会員規約に明記、チェックボックス＆サイン等

乗車履歴、事前説明せず外部販売
○社「匿名化で個人特定恐れなし」と説明　産経新聞2013年 7月18日

IC乗車券△△の利用者に事前説明しないまま、乗車履歴などのデータを日立製作所に販売していたことが、○社への取材で分かった。「名前や住所を匿名化しており、個人が特定される恐れがないため」としている。

個人情報保護法は、第三者に個人情報を提供する場合、利用者の同意を義務付けている。○社は「個人情報に当たらない」との見解だが、国土交通省は「違法でなくても、利用者が不安に思う可能性がある。○社の今後の対応などを確認したい」としており、プライバシー保護の面で論議を呼びそうだ。

産経新聞Web版より抜粋　http://sankei.jp.msn.com/life/news/130718/trd13071821130008-n1.htm

氏名
○○○○
△△△△
□□□□

付番	1	2	3	4	5	・・・
A001	○駅A入札 9/1 09:30:21	△駅C出札 9/1 10:21:31	△駅G入札 9/1 19:21:50	□駅B出札 9/1 20:30:11	□駅B入札 9/1 23:50:11	○駅A出札 9/2 0:31:55
B012	☆駅X入札 8/9 06:31:35	※駅Y出札 8/9 07:10:55	※駅Y入札 8/9 14:44:55	☆駅Z出札 8/9 15:15:54		
C765						

符合表 ⇨ 廃棄

事業化した場合のリスク

プライバシーの権利　（判例上確定した定義）

1964年　「宴のあと」事件　（東京地判昭和39年9月28日判時385号12頁）

「私生活をみだりに公開されないという法的保障ないし権利」

（1）私生活上の事実
（2）一般人の感受性を基準に、本人なら公開を望まない内容
（3）一般の人々に未だ知られていない

出訴可能な権利

個人情報の定義　（個人情報保護法の定義）

「個人情報」とは（略）、**①特定の個人を識別することができるもの**（他の情報と　②容易に照合することができ、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。）

事業者に勧告・命令など

「識別可能」になった場合、個人情報保護法違反（同意のない第三者提供）となり、プライバシーの侵害となる。

Netflix社のコンテスト （米国最大の映画配信・DVDレンタル事業者）

2006年、Netflix社は顧客の嗜好にあわせて映画を勧める独自のアルゴリズムの精度を10%以上向上した人に100万ドルの賞金を与えるという「Netflix Prize」を実施。

このコンテストに186カ国の5169チームが参加を申込んだ。Netflix社はコンテスト応募者に匿名化した50万人の会員の視聴履歴データを提供した。

コンテスト開始2週間後に、テキサス大学のグループが、その匿名データから、一部の個人の特定に成功したと発表。その結果、連邦取引委員会（FTC）は、Netflix社の会員のプライバシーへの影響に関する調査を行い、また訴訟も提起された。

2009年8月6日、同社は2回目のコンテストの実施を発表したが、2010年3月12日これを取りやめると発表した。

近年のICT技術は「再識別可能性」を高めている

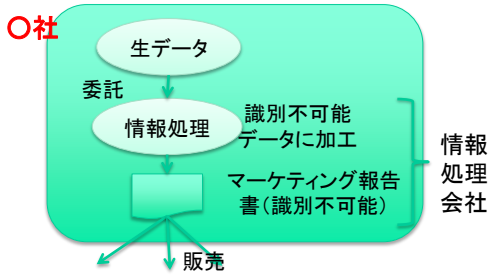
判断の基準をどこに求めるか

違法性判断→社会受容性（社会的責任）判断→経営判断の手順で検討を行うとすると・・

①「容易照合性」は提供元基準か、又は提供先基準か？
②再識別化のリスクは？
③本人（社会）の納得感は？

現行法制下で可能とされるモデル （新潟大学 鈴木正朝教授 資料より）

① ○社が情報処理会社に対し、情報処理＋マーケティング報告書の販売を含めて委託



② その他、
○社が情報処理会社に対し、
再識別不可能データを販売

但し、技術的な再識別可能性が残る

図の出所：鈴木正朝「個人情報保護法の改正動向とビッグデータ対応－政府IT総合戦略本部「パーソナルデータに関する検討会」を踏まえて」BERCコンプライアンス担当者の為の法令研究会資料、2013年11月25日、30頁。

ソーシャルメディアの課題

種類	具体例
SNS	Facebook、Mixiなど
クチコミサービス	価格.com、食べログなど
匿名コミュニティー	2ちゃんねるなど
動画・写真共有	You Tube、ニコニコ動画、Ustreamなど
ブログ	ココログ、Yahoo!ブログなど
マイクロブログ	Twitterなど
:	:

世代間格差が顕著
・10代・20代の利用率が多く、年齢が上がるにつれて利用率が低下
・企業は採用・事業活動にFacebook等のSNSを利用しており、10代・20代の利用率が更に上昇する可能性

ソーシャルメディアに関する資料は、筆者が主宰するBERC「コンプライアンス担当者の為の法令研究会」において、2012年11月5日及び2013年6月14日に実施した研究会の発表資料、岡野秀穂氏「ソーシャルメディアの個人利用と会社の対応」、及び早川一郎「ホテル従業員の事例の時系列」、並びに拙論、高野一彦「ソーシャルメディアのリスク管理」所収『経営倫理 第71号』（経営倫理実践研究センター、2013年7月）13-15頁をもとに作成。

事例1　アルバイト従業員がお客様のプライベート情報を投稿

サッカー選手Aと、タレントBがホテルでお泊りデート!?
2011年1月11日深夜、ホテルレストランのアルバイト女子大生がTwitterで「顔ちっちゃくて可愛かった…今夜は2人で泊まるらしいよお、これは…（どきどき笑）」と書き込みし、インターネット上で炎上

・インターネット上の声
「バイトの書き込みが事実なら、ホテルとして謝罪コメントを出さにゃならんだろうな」
「単なるバイトにしては色んな情報入りすぎだから、従業員の間では客の情報とか筒抜けなんだろう」
「ホテルとしては絶対にやっちゃいけないことだよね」
「金払いのいい芸能人、スポーツ選手、政治家なんかはもうこのホテル絶対使わないだろうね」

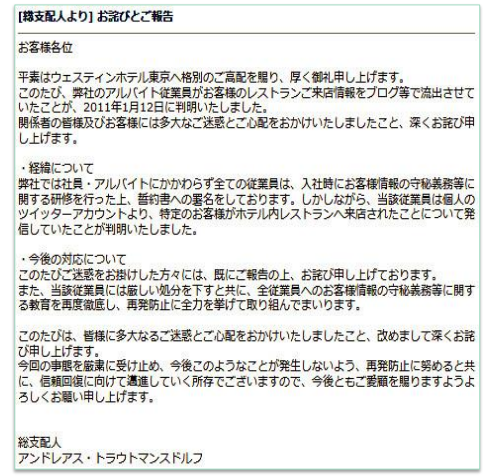
出典：岡野秀穂「ソーシャルメディアの個人利用と会社の対応」BERCコンプライアンス担当者の為の法令研究会資料、2012年11月5日
原典はロケットニュース24「〇〇と〇〇がお泊りデートか!?　女子大生バイトがTwitterでバラして炎上」　http://rocketnews24.com/

事例1の展開

2011年1月11日～12日

22:50　ツイッターで有名人の来店を発言
02:40　「2ちゃんねる」に掲載
03:15　「mixi」のアカウントが発見され大学名・クラブ名が推定
03:58　「Facebook」アカウント発見、顔写真がネットに出回る
05:30　ネットのニュースサイト掲載
16:48　産経新聞ニュースサイト掲載
21:14　ホテルHPに支配人の「お詫び」掲載

出典：早川一郎「ホテル従業員の事例の時系列」
BERCコンプライアンス担当者の為の法令研究会資料2012年11月5日



[総支配人より] お詫びとご報告

お客様各位

平素はウェスティンホテル東京へ格別のご高配を賜り、厚く御礼申し上げます。
このたび、弊社のアルバイト従業員がお客様のレストランご来店情報をブログ等で流出させていたことが、2011年1月12日に判明いたしました。
関係者の皆様及びお客様には多大なご迷惑とご心配をおかけいたしましたこと、深くお詫び申し上げます。

・経緯について
弊社では社員・アルバイトにかかわらず全ての従業員は、入社時にお客様情報の守秘義務等に関する研修を行った上、誓約書への署名をしております。しかしながら、当該従業員は個人のツイッターアカウントより、特定のお客様がホテル内レストランへ来店されたことについて発信していたことが判明いたしました。

・今後の対応について
このたびご迷惑をお掛けした方々には、既にご報告の上、お詫び申し上げております。
また、当該従業員には厳しい処分を下すと共に、全従業員へのお客様情報の守秘義務等に関する教育を再度徹底し、再発防止に全力を挙げて取り組んでまいります。

このたびは、皆様に多大なるご迷惑とご心配をおかけいたしましたこと、改めまして深くお詫び申し上げます。
今回の事態を厳粛に受け止め、今後このようなことが発生しないよう、再発防止に努めると共に、信頼回復に向けて邁進していく所存でございますので、今後ともご愛顧を賜りますようよろしくお願い申し上げます。

総支配人
アンドレアス・トラウトマンスドルフ

出典：ガジェット通信　http://getnews.jp/archives/93256

Graduate School and Faculty of Safety Science FSS © Kazuhiko.Takano

事例2．アルバイト従業員の投稿による近時の炎上事案

弁当チェーン店

出典：IT Media ニュース「「ほっともっと」従業員が冷蔵庫に入って写真をTwitterに」
http://www.itmedia.co.jp/news/articles/1308/03/news016.html

2013年8月3日
「食材などが保管されている冷蔵庫に男性が入り込んでおり、「今日暑くね？」というコメントとともにTwitterに投稿」
同弁当チェーン本部は、自社HP上に「不適切な行為」として謝罪文を掲載した。

コンビニエンスストア

出典：IT Media ニュース「「コンビニのアイスケースに入ってみた」写真炎上でローソンが謝罪」
http://nlab.itmedia.co.jp/nl/articles/1307/15/news010.html

2013年7月15日
コンビニの従業員がアイス用冷蔵庫に入った写真をFacebookに投稿して炎上。
チェーン本部は同店とのFC契約を解約し、同社HP上に謝罪文を掲載した。
※投稿⇒炎上は、FC契約を継続し難い信頼関係の破壊、と捉えている。

各企業とも、役員・正社員、派遣社員、内定者などの教育をすすめてきたが、アルバイトやフランチャイジーへの教育・浸透は今後の課題として残っている。

企業の対応における課題

（1）既存の規程類との整合

ソーシャルメディアに特化した規程類の策定は、既存規程類との整合、および職務分掌上の横断性から困難。

・従前の規程類で対応し、従業員教育ではソーシャルメディアの特徴とリスクの理解を促す、いわゆる「ネチケット」的なケースブック・ガイドライン等で対応。

・具体的な事案への対応は従前の（リアルな世界の）ルールで対応

①企業の営業秘密の投稿⇒秘密情報管理規程、非開示契約、守秘義務
②個人情報の投稿⇒個人情報保護規程、プライバシー権の侵害
③企業の信用棄損⇒名誉棄損、信用棄損を根拠とした懲戒規定
④インサイダー情報⇒インサイダー情報管理規程
⑤その他、職務専念義務違反、など

（2）従業員の私生活における行為への会社の関与

プライベートな時間の投稿に対して会社が関与すべきかどうかの判断基準

日本鋼管事件（最判昭和49年3月15）

在日米軍の立川基地拡張に反対する運動に加担して逮捕、起訴された従業員に対して、就業規則などに基づき懲戒解雇をした事件。

「当該行為の性質、情状のほか、会社の事業の種類・態様・規模、会社の経済界に占める地位、経営方針及びその従業員の会社における地位・職種等諸般の事情から綜合的に判断して、右行為により会社の社会的評価に及ぼす悪影響が相当重大であると客観的に評価される場合でなければならない。」

※本件は「懲戒解雇又は諭旨解雇の事由とするのには、なお不十分」と判断

（3）課題

・従業員の私的な投稿で炎上した場合の企業の広報対応
・アルバイト・パートの教育、フランチャイズ契約の相手方の教育

③ 国際的整合に関する課題

Graduate School and Faculty of Safety Science FSS © Kazuhiko.Takano

EU及び諸外国との関係

EUデータ保護指令 （1995 年10 月24 日採択, 1998 年10 月24 日発効）

個人データ処理に係る個人の保護及び当該データの自由な移動に関する欧州議会及び理事会の指令

指令25条1項:
第三国が「十分なレベルの保護」(adequate level of protection)を確保している場合に限りデータ移転を行うことができる。

※EU加盟国27か国および欧州経済領域(European Economic Area, EEA)構成国であるノルウェイ、リヒテンシュタイン、アイスランドに対して同指令に従った国内法の整備を求めている

海外法規への日本企業の対応

EUデータ保護指令26条1項、2項及び4項の例外的措置

①情報主体の明確な同意
②標準契約条項(SCC)⇒データ保護当局の承認
③拘束的企業準則(BCR)⇒ 域内3当局の承認
又は、そもそもデータを移転せずEU域内で完結

⇒ 実質的な経済障壁として機能している

わが国の個人情報保護法の十分性評価

①EUデータ保護指令との比較
②十分性を評価されなかった、オーストラリアの2000年プライバシー修正法へのEU委員会コメントから類推
③2012年1月20日 欧州委員会「プライバシー比較研究」（後掲）

	EUデータ保護指令	日本の個人情報保護法
適用の対象	個人、法人、公的機関等	5000件を超える個人情報を保有する事業者
情報の種類	特別な種類のデータの取扱いを制限 ※人種又は民族、政治的見解、宗教又は思想的信条、労働組合への加入、健康又は性生活に関するデータの取扱い禁止等	情報の質による法律上の義務の違いはない ※個人情報＝特定の個人を識別することができる情報等
開示請求等	出訴可能な権利（right）	事業者の義務
第三国への移転	「十分なレベルの保護」でない第三国への情報の移転を制限	なし
監視機関	独立した監視機関が官民双方を監視 **※独立性要件**	主務大臣が民間を監視 行政の監視機関はない
制裁	規定違反への法的制裁	事業者への行政行為

EUにおける新たな動き

EU一般データ保護規則提案

2012 .1.25　改定案を公表、
2013.10.21　LIBE委員会で改訂案承認

クラウドコンピューティング（EU 域外へのアウトソーシング）、SNSにおけるデータ保護のあり方、多国籍企業への過度な負担の軽減などを目的とした改訂

「プライバシー・バイ・デザイン」の原則

①新サービスの導入時にデータ保護への考慮の義務（第23条）
②個人データの取扱いを行うに当たって、データ保護影響評価（Data Protection Impact Assessment）を実施する必要がある旨の規定（第33条）、など

透明性が高く容易に入手可能な方針を用意する義務（第11条）

「同意の条件（Conditions for Consent）」における明確な同意取得（第7条2項）

公表文などの中で示される場合は、区別して明示（explicit）する義務、同意撤回の権利を保障する義務を追加。（「黙示の同意」、「約款の条項」などは明示的でない）
⇒わが国の現行法制における「同意」の適法性とは異なる

消去する権利（Right to erasure）（第17条）

本人は、当該企業・団体の保有する個人データのみならず、第三者のリンク、コピー・複製についても消去する権利を有する。
※2013.10.21　LIBE委員会で「忘れ去られる権利」を削除し、消去する権利のみ承認した。

「指令（Directive）」から「規則（Regulation）」へ

「規則（regulation）」は自動的に全加盟国の国内法の一部となり、「指令（directive）」は全加盟国が指令に基づき国内法として立法義務を有する。規則への格上げにより、加盟国へ直接適用し、EU域内でのデータ保護ルールの一元化を図る。

現データ保護指令26条1、2及び4項の例外規定 ⇒ 新規則案では‥
①標準契約条項（SCC） ⇒ データ保護当局の承認不要
②拘束的企業準則（BCR）⇒ 域内一当局の承認でOK、など

⇒ 多国籍企業の負担軽減

「地域的な範囲」におけるEU域外適用（3条2項）

EUデータ保護規則案は、EU域外企業であっても、① EU居住者への商品・サービスの提供、② EU居住者の行動の監視、を行っている管理者に対して適用される。

「監督機関への報告」（31条）

個人データ違反を発見した場合、24時間以内に監督機関に報告する義務
⇒危機管理体制の整備

「データ保護ルール遵守を確実にする、独立した監視機関」の設置（41条2項(b)）

監督機関による課徴金（第79条）

監督機関は、EUデータ保護規則に反した管理者・処理者に対して最高1億ユーロ（約130億円）または全世界での年間売上高の最大5%まで過料として科す。

※2013.10.21 LIBE委員会で当初提案から引き上げて承認された

事業者にとっての影響は多大 ⇒ グローバルなデータ保護ルールを！

Graduate School and Faculty of Safety Science FSS © Kazuhiko.Takano

新プライバシー保護法制の潮流

2013年5月24日 行政手続き番号法 成立

同法に採用された「世界レベル」のプライバシー保護

独立性が高い監視機関の設置、情報の不正取得への刑事罰、
プライバシー影響評価の実施と運用、マイポータルなど

※「国際的にも通用する強度」（堀部政男一橋大学名誉教授）との評価

今後・・・

・「番号法」における特定個人情報保護委員会の設置と人事
・医療等個人情報保護委法案の議論は収束
・2013年9月～12月「パーソナルデータに関する検討会」
⇒2015年通常国会にて個人情報保護法改正

企業の個人情報保護コンプライアンスの見直しが必要

① グローバルに展開する企業は国際水準の保護ルールを採用
② 人事・労務、健康診断情報などは番号法に基づく対応
③ 個人情報を取扱うビジネス・スキームの適法性・適正性の確認
⇒ 適法、かつ社会的受容性の両面を充足する「同意」

④ 法改正の動向

わが国の個人情報保護法制の「有効性」

―欧州委員会「プライバシー比較研究」（2012.1.20）の分析から―

Graduate School and Faculty of Safety Science FSS © Kazuhiko.Takano

わが国の個人情報保護違法性の国際的評価

2012年1月20日 欧州委員会「特に技術発展に焦点をあてた、新たなプライバシーの課題への異なるアプローチの比較研究」における、ニューサウスウエールズ大学のグレアム・クリーンリーフ教授の報告「Country Studies B.5–Japan」におけるわが国の評価

「データ保護の「十分性（adequacy）」を充足していると判断することは困難」

その根拠として「私企業にとっては、法律違反による多額の罰金や集団訴訟よりも、風評リスクによる損害（risk of reputational damage）のほうが重要」であり、わが国の法律が、「有効」であるとの根拠を見いだせない、との指摘。

グリーンリーフ報告では「有効性」を重視しているが、わが国のデータ保護法制は、特に小規模事業者・ネット事業者への有効性が低いことが課題

【参考】 EUデータ保護の「十分性」の基準

（1）「個人データの第三国への移転：EUデータ保護指令25条及び26条の適用の実務文書」「ルールへの優れたレベルのコンプライアンス」があることが要件

Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive, 24 July 1998

（2）オーストラリアの2000年プライバシー修正（民間部門）法の欧州委員会への認定申請第29条作業部会の意見では主に法制度の外形的要件と執行状況の評価

Article 29 Data Protection Working Party Opinion 3/2001 on the level of protection of the Australian Privacy Amendment (Private Sector) Act 2000, (5095/00/EN WP40 final) Adopted on 26th Jan. 2001」

企業から見た「有効性」

（1）株式会社の類型による違い

会社法 ⇒ 大会社及び委員会設置会社の「内部統制システム構築義務」

大会社及び委員会設置会社の取締役には内部統制システム構築義務がかかっている。体制整備の内容は会社法施行規則 100条1項「業務の適正を確保するための体制」に、使用人のコンプライアンス体制（4号）について、企業グループとしての体制の構築を親会社等の取締役の義務（5号）と規定している。

株主代表訴訟、第三者訴訟

金融商品取引法 ⇒ 有価証券報告書提出会社の「内部統制報告義務」

金融商品取引法において、有価証券報告書提出会社に「内部統制報告制度」が義務付けられている。その具体的な内容は、金融庁「財務報告に係る内部統制の評価及び監査の基準」および「同実施基準」に規定されており、「全社的な統制」としてリスク管理体制に関する自己評価を行い、外部監査人の内部統制監査を受け、内閣総理大臣に報告書を提出する義務を負う。

内部統制報告書の虚偽記載への刑事罰・罰金

大会社及び委員会設置会社、有価証券報告書提出会社（公開会社）の経営者にかかる法的義務は、コンプライアンス経営を促すモチベーションとなっている

Graduate School and Faculty of Safety Science FSS © Kazuhiko.Takano

（2）企業法務におけるリスク評価の問題

① 個人情報保護法における主務大臣の権限の行使

主務大臣による「勧告」「命令及び中止命令」至る可能性は低い

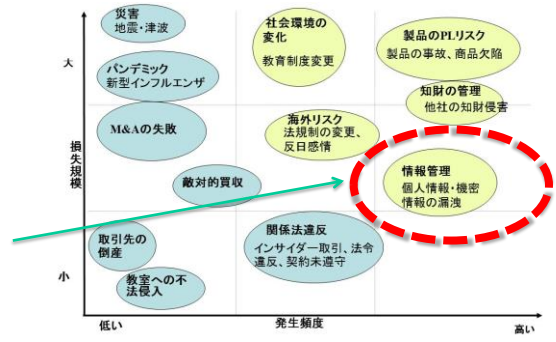
	苦情相談	漏えい事案	勧告、命令及び中止命令	備考
H23年度	5,267件	420件	0件	報告の徴収16件、助言1件
H22年度	6,212件	413件	0件	報告の徴収15件

出所：消費者庁「平成23年度個人情報の保護に関する法律施行状況の概要」2011年9月、43頁。

② 訴訟リスク

数多くのプライバシーの権利の侵害に関する判例が存在するが、おおむね賠償額は、数千～数万円の間。侵害行為への抑止力としての効果が極めて低い。

「発生頻度」と「損失規模」で優先順位をつける企業のリスク評価では、「情報法CP」の優先順位は低くなる



(3)事業形態による違い

法人顧客相手の事業と、個人顧客相手の事業では、企業のコンプライアンスへの取組みに違いが出る

個人顧客	不信を招く行為は不買運動につながり重要なリスク	適法かつ社会受容性を考慮したルール設定と運用
法人顧客	消費者の信用低下を重要なリスクと捉えない傾向	現行法制度の「間隙」をつく挑戦的なルール設定と運用

例:個人情報保護法における第三者提供の同意⇒法と社会受容性に乖離
⇒明確な同意を追及するか、約款の一条項として記載するか、など

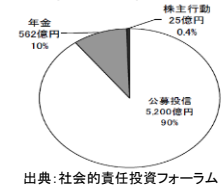
参考　社会的責任投資(Socially Responsible Investment, SRI)ファンド

米国におけるSRIの投資残高　(単位:10億ドル)　出典:SOCIAL INVESTMENT FORUM <http://www.socialinvest.org>

1995年	1997年	1999年	2001年	2003年	2005年	2007年	2009年
$639	$1,185	$2,159	$2,323	$2,164	$2,290	$2,711	$3,071

参考:国＝2400億ポンド(約45兆円、2007年)、日本＝8400億円(2009年)

伸び悩む日本のSRI残高



出典:社会的責任投資フォーラム <http://www.sifjapan.org/>

Dow Jones　Sustainability Assessment Questionnaire

Economic dimension　:　32問
Environmental dimension:　31問
Social dimension:　36問
→ コーポレートガバナンス
リスクマネジメント
コンプライアンス

まとめ　ー企業から見たわが国の個人情報保護法制の「有効性」ー

根拠	義務・誘因	対象	効果
会社法	内部統制システム構築義務	大会社・委員会設置会社の取締役	株主代表訴訟、第三者訴訟による損害賠償請求
金融商品取引法	内部統制報告制度	有価証券報告書提出会社の経営者	報告書の虚偽記載に刑事罰・罰金
個人情報保護法	主務大臣による権限の行使	個人情報取扱事業者	「勧告」「命令」等 但し、近年は0件
プライバシー侵害訴訟	民事訴訟の提起	全ての法人・個人	損害賠償額は概ね数千円～数万円
[参考] CSR評価	SRIファンドのインデックスとして採用	公開会社	企業価値の上昇 日本のSRI残高は伸悩む

非大会社かつ非公開会社であり、法人顧客対象の事業を行っている企業は、
法の「有効性」を担保するプレッシャーが全くかかっていない。

小規模事業者、小資本で起業できて多額な設備投資が不要なため株式公開による資金調達の需要が少ないインターネットビジネスのような業態が該当
＝国際的にみればデータ保護ルールが最も有効に機能して欲しい分野

明確で対象を限定しない罰則の規定が必要
独立監視機関による確実な権限行使と事業者へのコンサルテーションが必要

監視機関による確実な執行と事業者へのコンサルテーション

2011年8月10日～13日　トロントを訪問（IPC Office、CHEO、Kids Media Centerを調査）

1．Information and Privacy Commissioner of Ontario
Dr. Ann Cavoukian　⇒「Privacy by Design」提唱者

（1）Commissionerの職責

プライバシー保護と情報公開の両分野について、
独立した法執行機関として、官民双方を監視
・法の遵守監視と執行
・国民への情報提供、教育啓発、事業者の相談
・プライバシー影響評価と検査　（官民双方）など

（2）Commissionerの権限
・強制調査権＝市民からの不服申立に関する調査
・自己付託による調査、勧告、命令、訴訟提起と参加

（3）Commissioner Office
・140人のスタッフ中、約70名はプライバシー、約70名は情報公開
・行政機関との人事交流あり（情報公開担当の副委員長は行政出身）
・年間予算は約14億円（2010-11年度）、ほとんどは職員の人件費

参考：　イギリス インフォメーション・コミッショナー制度
ウイルムズローに所在、人員327人（IOCが独自採用）、年間予算は約30億（2017万£、2009-10年）
※出典：石井夏生利「英国におけるインフォメーション・コミッショナーの組織と権限」2010年8月21日、17頁。

Graduate School and Faculty of Safety Science FSS
© Kazuhiko.Takano

監視機関による確実な執行と事業者へのコンサルテーション

2011年8月10日～13日　トロントを訪問（IPC Office、CHEO、Kids Media Centerを調査）

2．事業者の意見

東オンタリオ小児病院（CHEO)のエルイーマム博士（Dr. Khaled El Emam）

オンタリオ州の新生児の登録情報のデータベースを新薬や治療後術の開発に利用
データベース構築にあたって、患者からの情報取得から研究者への情報提供の一連
のスキームについて、IPCに相談してプライバシー保護の仕組みを導入し、PIAと数回
の検査を経て運用

⇒「事業者にとっても時間と経費の低減につながり、相談は有益であった」
「コミッショナーによる監視と執行はオンタリオの事業者の意識を高めている」

その他、子ども向け優良サイトの認証を行っているKids Media CenteのMs. Gordonrも同意見

監督機関による監視と執行が事業者のコンプライアンス意識を高めている点は、
小規模事業者やインターネットビジネスにコンプライアンス経営を促すプレッ
シャーが低いわが国が「有効性」を高めるための示唆

企業における個人情報保護のもう一つの課題

国内法が企業に求める過剰な管理 （2000問題）

①重層的な法制度　個人情報保護法
個人情報保護法に基づく各省庁のガイドライン
47都道府県・1750市町村等の個人情報保護条例
JIS Q 15001（プライバシーマーク）

②個人情報＋利用目的の管理のためのデータベース構築

海外法規への日本企業の対応

EUデータ保護指令26条1項、2項及び4項の例外的措置

①情報主体の明確な同意
②標準契約条項（SCC）⇒データ保護当局の承認
③拘束的企業準則（BCR）⇒　域内3当局の承認
又は、そもそもデータを移転せずEU域内で完結

⇒ EU一般データ保護規則提案、への対応が予想される

その他、消費者プライバシー権利章典、改正OECDガイドラインへの対応も・・

わが国の会社法・金取法は海外法規の遵守も求めているため、**膨大なコストと労力**をかけて情報管理体制を構築している （しかしEUにおけるわが国の評価は低い）

非公開の小規模事業者やインターネットビジネスとのコンプライアンス経営への取組みの**格差がますます拡大**する傾向

グリーンリーフ報告からの立法上の示唆　―監督機関と罰則―

EUデータ保護指令 第24条「制裁」（Sanctions）

「加盟国は本指令の条文の完全な実行を確実にするために適切な措置を採択し、指令に従って採用された国内法規の条項の違反に対しする制裁を規定する」と規定

EU一般データ保護規則提案　第78条「刑罰」（penalties）

「加盟国は本規則の条項への違反に適用する刑罰をルールとして規定」し「刑罰は効果的（effective）で均衡が取れ（proportionate）、抑止的（dissuasive）でなくてはならない」と規定

1999年10月20日「高度情報通信社会本部個人情報保護部会（堀部政男座長）」の議論で個人情報保護法の立法過程で刑事罰の導入が検討されたが見送られた。その結果・・

①主務大臣の関与の少なさと相俟って抑止力としての効果が期待できない
②EUによる「十分性」の要件を充足しない
③企業防衛上の不都合⇒・不競法「営業秘密侵害罪」は構成要件が厳しく使えない
・営業秘密としての管理が過剰反応を促し、利用と流通を制限

一般法としての個人情報保護法の改正の観点は・・
①刑事罰の導入による不正取得事案の抑止効果
②独立監視機関による監視と権限の執行、事業者のコンサルテーション
⇒特定個人情報保護委員会の権限の拡大

⇒「有効性」を高める

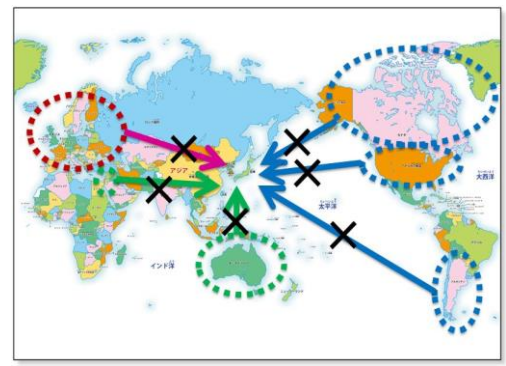
【参考】 成長戦略としてのパーソナルデータ制度設計の議論

① EUデータ保護指令第25条1項により、EU加盟27か国およびEEA構成3か国は、保護の十分性を認められていないわが国への個人データの移転は原則として禁止
② EUに保護の十分性を認められたカナダ、アメリカ（セーフハーバー）などの諸国は、同様に第三国への移転禁止条項を持っており、申請予定のオーストラリアなどの諸国も同様。
※EU規則提案（2013.10.21 LIBE委員会承認）では負担軽減が図られている。

世界の情報がわが国に集まる法制度へ
（世界のデータセンター）

パーソナルデータの扱いに関する制度設計は、成長戦略の一環

2015年通常国会に提出予定の法案は、国際的な整合が重要な課題となる

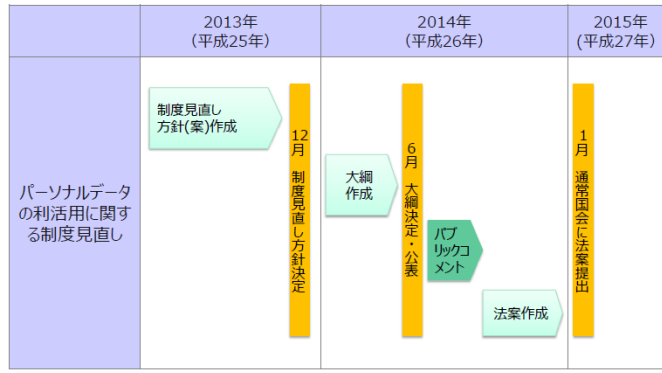


著者作成

【参考】 パーソナルデータに関する検討会　2013年9月2日 ～ 12月10日

パーソナルデータの利活用に関する制度見直し方針（案）

「平成26年（2014年）年6月までに、法改正の内容を大綱として取りまとめ、平成27年（2015年）通常国会への法案提出を目指すこととする」



※ 欧米を含めた諸外国の制度についても現在変更に向けた作業が行われているため、これらとの整合性を取るためにある程度の時間が必要となる。
（例：ＥＵデータ保護規則案 2014年4月に欧州議会本会議で採択の見込み）

出典：「パーソナルデータの利活用に関する制度見直し方針（案）」2013年12月10日、5～6頁
www.kantei.go.jp/jp/singi/it2/pd/dai5/gijisidai.html

【参考】 匿名化（非識別化）情報の利用に関する議論の概括

（1）EU

1995年 EUデータ保護指令、2012年 EUデータ保護規則提案は、「データ主体が識別できないような方法で匿名化されたデータについては利用可能」と規定。
（2013年 LIBE委員会で承認された修正案では、匿名化情報（pseudonymous data）が定義）

（2）アメリカ

アメリカにおいては包括的な規定なし
2013年3月に公開された、FTC（米連邦取引委員会）レポート「急速な変化の時代における消費者プライバシーの保護－企業と政策決定者への推奨※」では、以下の3要件を充足すれば企業は非識別化情報を利用可能と規定。

※Protecting Consumer Privacy in an Era of Rapid Change－Recommendations for Business and Policymakers－

①合理的な非識別化の措置を講ずる
②データを非識別状態で管理・利用し、再識別化を行わないことを公的に約束する
③非識別化データを他社などに提供する場合、提供先がデータの再識別化を行うことを契約上禁止する。

（3）わが国での議論

パーソナルデータに関する検討会では、FTC3要件をもとにわが国の匿名化情報の利用・管理ルールを策定してはどうかとの議論があるが、①合理的な措置（reasonable measures）の基準が不明確、②「公的な約束」に反する場合、アメリカはFTC法5条「不公正・欺瞞的な行為」として提訴可能だが、わが国に同様の法がない、③契約が履行される担保がない、などの課題がある。（技術検討WG 森亮二氏「「FTC3要件」を参考にした匿名化について」2013.11、14-16頁）

Graduate School and Faculty of Safety Science FSS
© Kazuhiko.Takano

まとめ

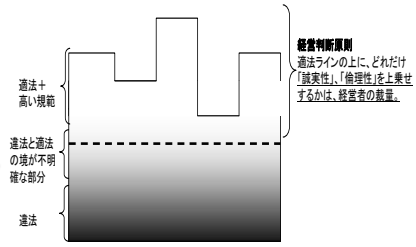
再掲出

経営者の経営判断の適法性に関する判断基準

株主代表訴訟判決の違法性判断の類型

類型	役員の責任	判断基準
経営判断原則	○～×	**①前提事実の認識に重要かつ不注意な誤認がない ②意思決定及びその過程が著しく不合理でない**
内部統制システム構築義務	×	構築していなかった （ただし判例少ない）
監視義務違反	×	知ってたのに止めなかった 知り得たのに止めなかった
具体的法令違反	×	社内規定違反
	×	法令違反・定款違反

経営判断における「合理性」とは？



・経営者は、適法ラインの上に、どの程度「倫理性」、「誠実性」を上乗せして判断すれば良いのか？

・従業員は、ファジーな分野のどこに判断基準を設ければ良いのか？

経営判断に必要な「法＋α」

1．企業の社会的責任

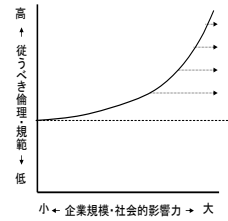
個々の基準を作り、運営する上で、適法であることは然ることながら、所属する企業の規模や特性に応じた規範性・倫理性が求められる

（1）社会的な影響が大きい
⇒ 売上やシェアが大きい企業

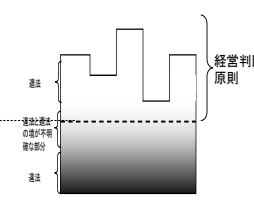
（2）国民の生命・身体に関係
⇒ 食品・医療品事業など

（3）事業の根幹が消費者の信頼
⇒ 教育事業など

企業の社会的影響力と倫理性・規範性の関係



企業のコンプライアンスルールのレベルと経営判断原則



2：長期的視座に立った判断

直近のコストや損失と、将来の利益（損失）を比較考量し、個々の判断を行う。

社会からの期待に応えること＝企業の社会的責任

グローバル企業の情報コンプライアンス

1. グローバルな「社会の変化」をWatchする、
   感度の高いアンテナを張り
2. 世の中より早目にコンプライアンス・プログラム
   に反映し
3. 社会の期待（立場）に見合った経営判断
   を行う、または企業体質を作る

必要があるのではないかと思います。これは結果として企業を守り、継続的な成長に寄与することになると思います。
そして、できれば企業して新たなフレームワークの制定過程に積極的に意見を発信されてはいかがでしょうか。

Graduate School and Faculty of Safety Science FSS © Kazuhiko.Takano

ご清聴、
ありがとうございました。