埼玉県社会保険労務士会大宮支部

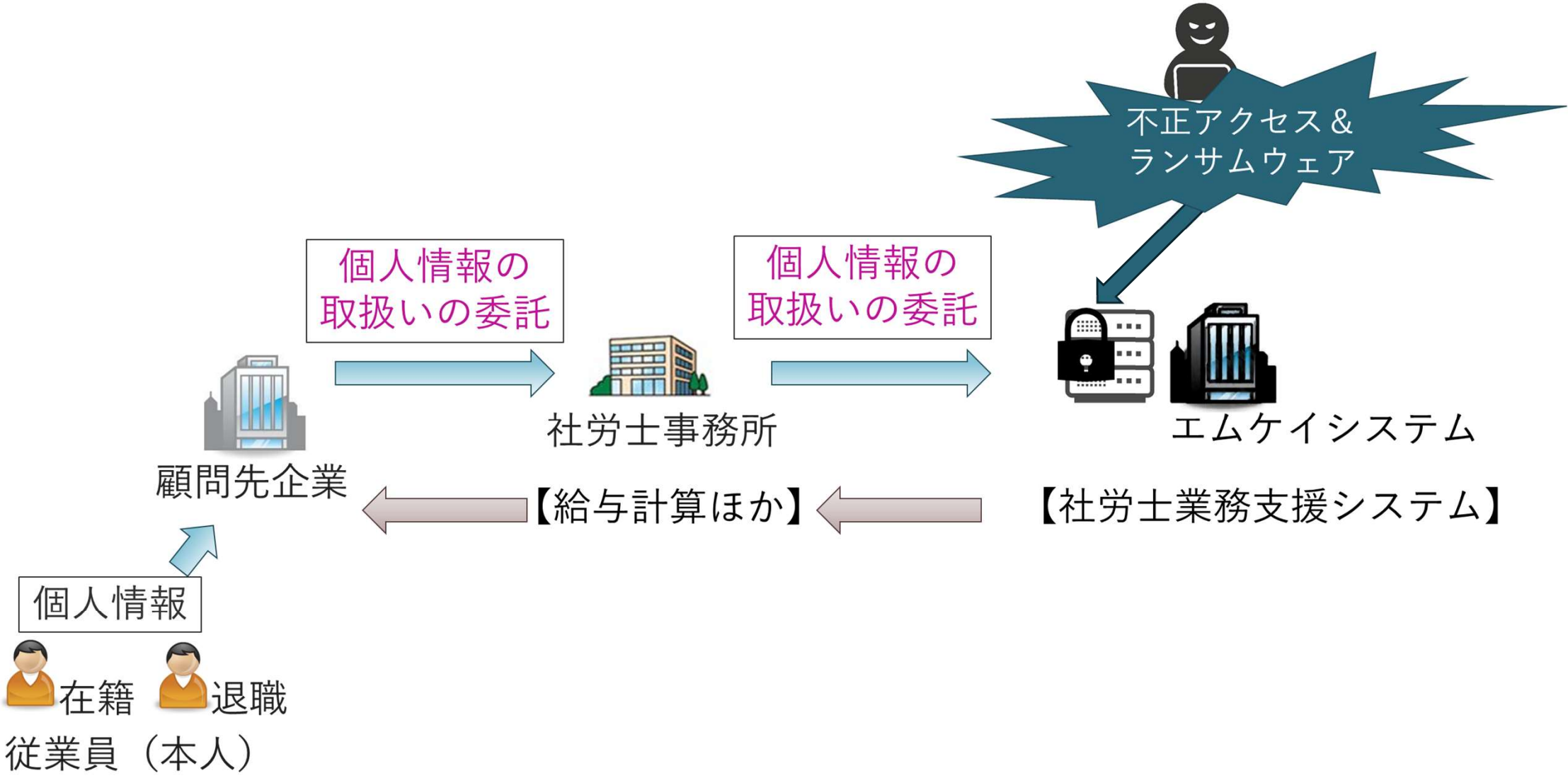
個人情報保護法関係研修会

令和２年改正個人情報保護法と社労士業務

情報漏えい対応を中心に

東京エクセル法律事務所
弁護士　坂　東　利　国

社労夢サーバのランサムウェア感染事件について



※ ランサムウェア
感染したコンピュータのシステムへのアクセスを制限し、制限を解除するための身代金を要求するプログラム

R2改正

漏えい等事案への対応

漏えい等の報告等

（漏えい等の報告等）

第26条　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、毀損その他の個人データの安全の確保に係る事態であって個人の権利利益を害するおそれが大きいものとして個人情報保護委員会規則で定めるものが生じたときは、個人情報保護委員会 規則で定めるところにより、当該事態が生じた旨を個人情報保護委員会に報告しなければならない。ただし、当該個人情報取扱事業者が、他の個人情報取扱事業者又は行政機関等から当該個人データの取扱いの全部又は一部の委託を受けた場合であって、個人情報保護委員会規則で定めるところにより、当該事態が生じた旨を当該他の個人情報取扱事業者又は行政機関等に通知したときは、この限りでない。

2　前項に規定する場合には、個人情報取扱事業者（同項ただし書の規定による通知をした者を除く。）は、本人に対し、個人情報保護委員会規則で定めるところにより、当該事態が生じた旨を通知しなければならない。ただし、本人への通知が困難な場合であって、本人の権利利益を保護するため必要なこれに代わるべき措置をとるときは、この限りでない。

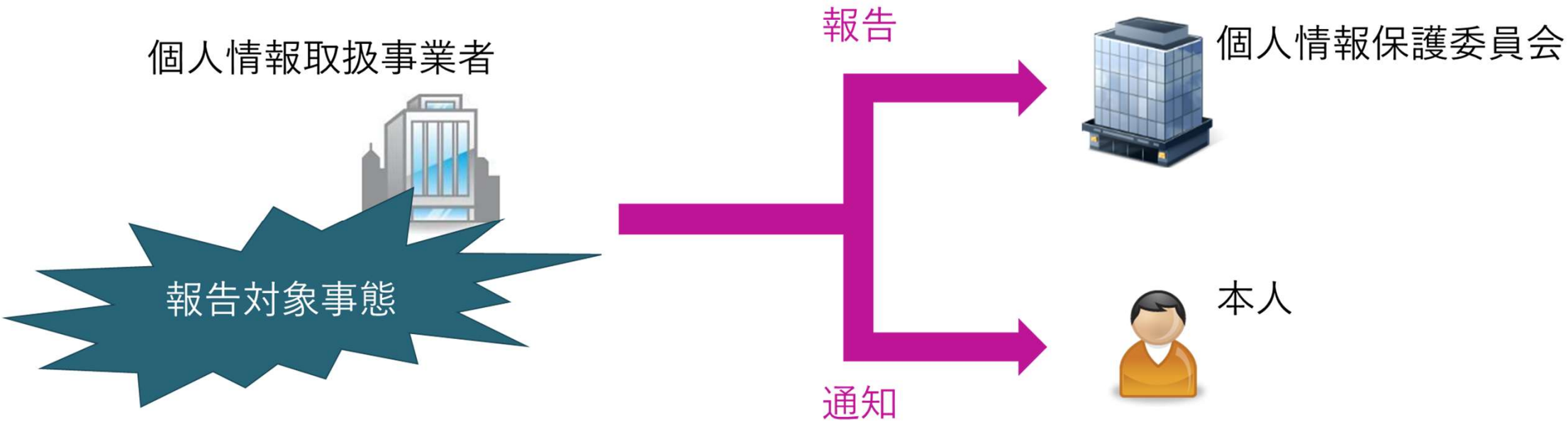
個人情報保護委員会への報告

BANDO Yoshikuni
Attorny at Law

個人データの漏えい等の報告等（法26条）

R2改正

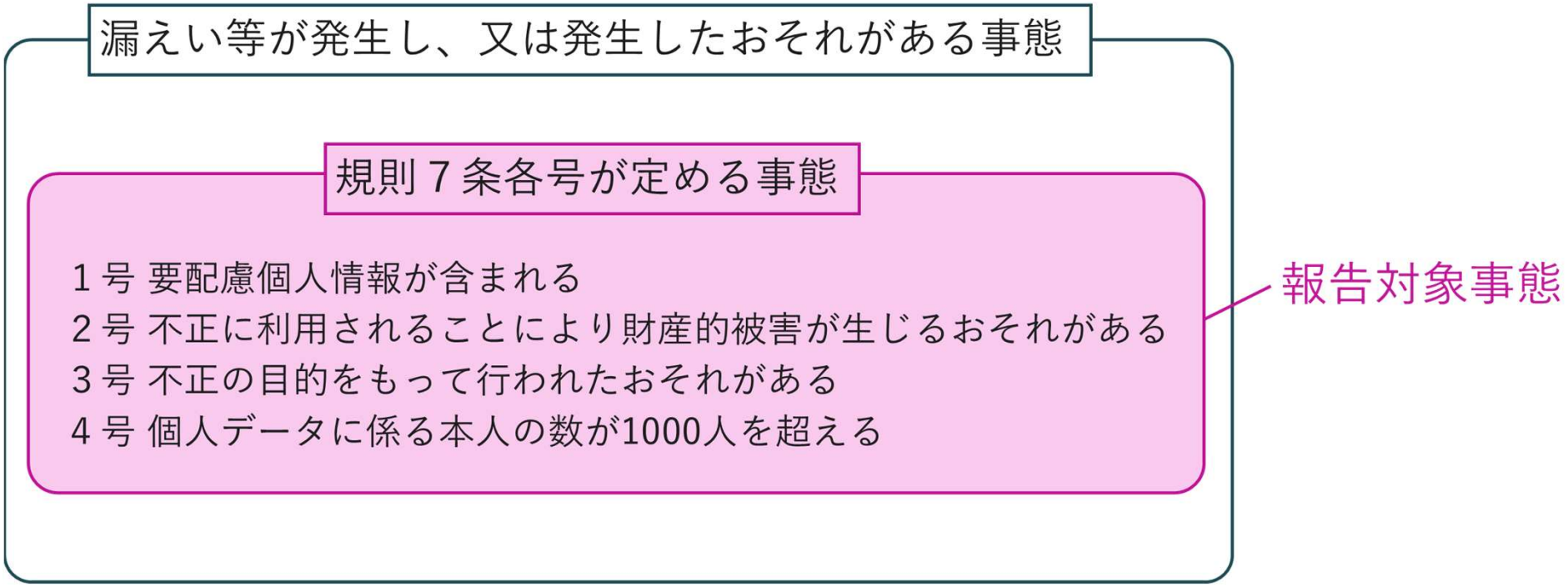
法26条	
1項	「報告対象事態」が生じたときは、当該事態が生じた旨を個人情報保護委員会に報告しなければならない
2項	報告対象事態を知った後、「通知事項」を本人に対し通知しなければならない



報告対象事態（法26条，施行規則7条各号）-1

● 報告対象事態

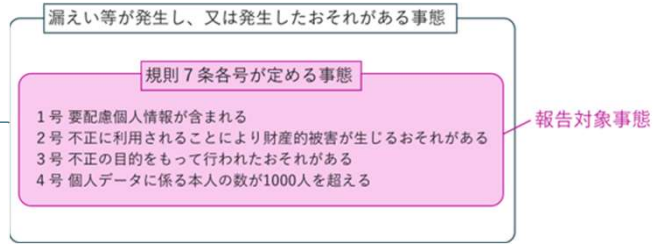
個人データの漏えい、滅失又は毀損（漏えい等）が発生し、又は発生したおそれがある事態のうち、個人の権利利益を害するおそれが大きい事態として個人情報保護委員会規則（施行規則7条各号）が定める事態



● 個人データの漏えい等が発生した「おそれ」

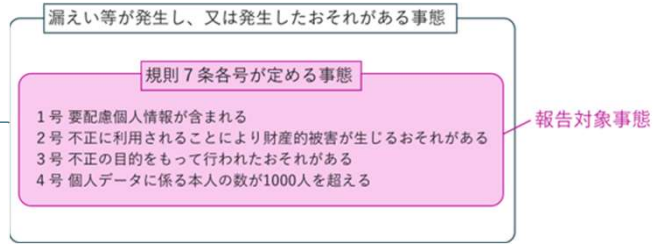
- ➢ その時点で判明している事実関係からして、漏えい等が疑われるものの漏えい等が生じた確証がない場合（通則ＧＬ）

報告対象事態-規則７条各号が定める事態- 1



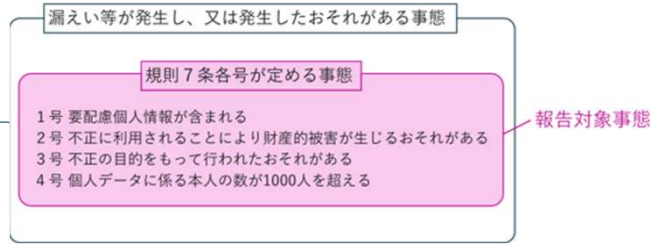
規則7条	
１号 （例）	要配慮個人情報が含まれる個人データの漏えい等が発生し、又は発生したおそれがある事態
	◯ 病院における患者の診療情報や調剤情報を含む個人データを記録したUSBメモリーを紛失した ◯ 従業員の健康診断等の結果を含む個人データが漏えいした

報告対象事態-規則７条各号が定める事態- 2



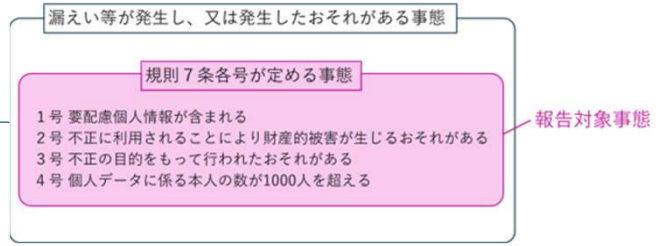
規則7条	
2号	不正に利用されることにより財産的被害が生じるおそれがある個人データの漏えい等が発生し、又は発生したおそれがある事態 ※漏えい等した個人データを利用し、本人になりすまして財産の処分が行われる場合が想定されている（Q&A）
（例）	◯送金や決済機能のあるウェブサービスのログインIDとパスワードの組み合わせを含む個人データが漏えいした ◯個人データであるクレジットカード番号のみが漏えいした（Q＆A） ✕住所、電話番号、メールアドレス、SNSアカウントといった個人データのみが漏えいした（Q&A） ✕ 個人データである銀行口座情報（金融機関名、支店名、預金種別、口座番号、口座名義等）のみが漏えいした（Q&A） ➢ ◯銀行口座情報がインターネットバンキングのログインに用いられている場合で、銀行口座情報とインターネットバンキングのパスワードの組み合わせが漏えいした場合は、該当する（Q&A） ✕ 個人データであるクレジットカード番号の下４桁のみとその有効期限の組合せが漏えいした（Q&A）

報告対象事態-規則７条各号が定める事態- 3



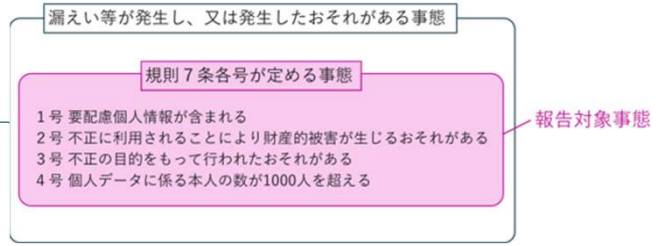
規則7条	
３号 （例）	不正の目的をもって行われたおそれがある個人データの漏えい等が発生し、又は発生したおそれがある事態
	［漏えい等が発生した事態］ ◯ 不正アクセスにより個人データが漏えいした場合 ◯ ランサムウェア等により個人データが暗号化され、復元できなくなった場合 ◯ 個人データが記載又は記録された書類・媒体等が盗難された場合 ◯ 従業者が顧客の個人データを不正に持ち出して第三者に提供した場合 ［漏えい等が発生したおそれがある事態］ ◯ 個人データを格納しているサーバや、当該サーバにアクセス権限を有する端末において外部からの不正アクセスによりデータが窃取された痕跡が認められた場合 ◯ 個人データを格納しているサーバや、当該サーバにアクセス権限を有する端末において、情報を窃取する振る舞いが判明しているマルウェアの感染が確認された場合 ➢ 単にマルウェアを検知したことをもって直ちに漏えいのおそれがあると判断するものではなく、防御システムによるマルウェアの実行抑制の状況、外部通信の遮断状況等についても考慮する（Q&A）

報告対象事態-規則７条各号が定める事態-４



規則7条	
３号	不正の目的をもって行われたおそれがある個人データの漏えい等が発生し、又は発生したおそれがある事態
（例）	［漏えい等が発生したおそれがある事態］ ◯ マルウェアに感染したコンピュータに不正な指令を送り、制御するサーバ（C&Cサーバ）が使用しているものとして知られているIPアドレス・FQDN（Fully Qualified Domain Name ：サブドメイン名及びドメイン名からなる文字列であり、ネットワーク上のコンピュータ（サーバ等）を特定するもの）への通信が確認された場合 ◯ 不正検知を行う公的機関、セキュリティ・サービス・プロバイダ、専門家等の第三者から、漏えいのおそれについて、一定の根拠に基づく連絡を受けた場合 ◯ 個人データを格納しているサーバや、当該サーバにアクセス権限を有する端末において、通常の業務で必要としないアクセスによりデータが窃取された痕跡が認められた場合

報告対象事態-規則７条各号が定める事態- 5



規則7条	
４号 （例）	個人データに係る本人の数が1000人を超える個人データの漏えい等が発生し、又は発生したおそれがある事態 ※ 「本人の数」は、漏えい等が発生し、又は発生したおそれがある個人データに係る本人の数（通則GL） ※ 本人の数が確定できない場合でも、漏えい等が発生したおそれがある個人データに係る本人の数が最大1,000人を超える場合には4号に該当する（通則GL） ※ 発覚当初は1,000人以下であっても、その後1,000人を超えた場合には、1,000人を超えた時点で4号に該当する（通則GL）
	◯ システムの設定ミス等によりインターネット上で個人データの閲覧が可能な状態となり、当該個人データに係る本人の数が1,000人を超える場合

※ １号から３号までの報告対象事態は、漏えい等の対象となった個人データに係る本人の数にかかわらない（１人でも報告対象事態に該当しうる）

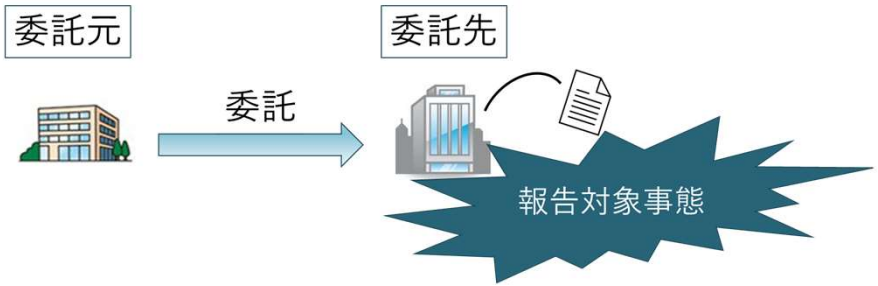
速報と確報（報告期限と報告内容）

● 個人情報保護委員会（PPC）への速報と確報（規則8）

	報告期限	報告内容
速報	報告対象事態を知ったとき※から、「速やかに」（規則8①） ➢ 当該事態を知った時点から概ね3～5日以内（通則GL）	報告をしようとする時点において把握している内容を報告すれば足りる（通則GL）
確報	• 報告対象事態を知ったとき30日以内（規則8②） • 規則７条3号の報告対象事態（不正の目的をもって行われたおそれがある場合）は、報告対象事態を知ったときから60日以内（規則8②）	全ての報告事項を報告しなければならない ➢ 合理的努力を尽くしても、全ての事項を報告できない場合は、判明次第、報告を追完する（通則GL）

※ 法人の場合は、いずれかの部署内の従業者が報告対象事態を知った時点が、報告期限となる「知った」時点（Q＆A）

個人データの取扱いを委託している場合の報告



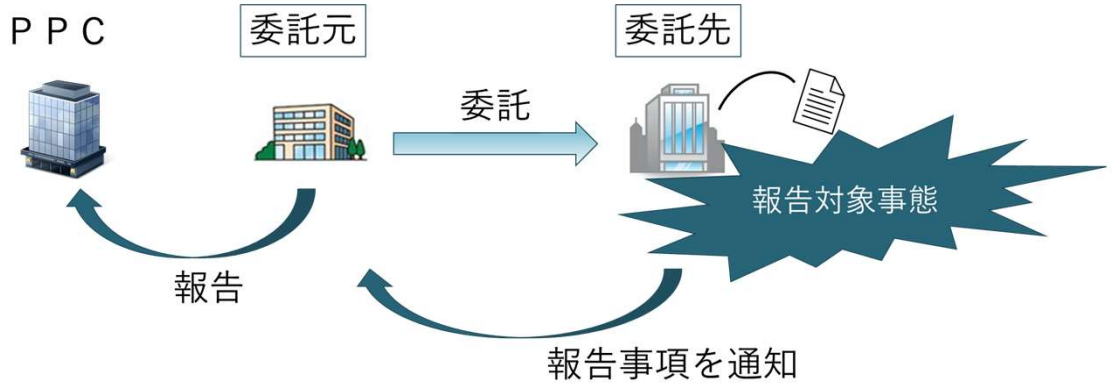
委託を受けて委託先が管理する個人データは委託先・委託元双方が取り扱っている

- 委託先で報告対象事態が発生したら、原則として、委託元・委託先の双方が報告義務を負う
  - ➢ 連名での報告は可能（通則ＧＬ）

  ※委託元で報告対象事態が発生した場合は、委託先は報告義務を負わない（Ｑ＆Ａ）

- 委託元への通知による例外（法26①但書）

  委託先が、委託元に対し、その時点で把握している報告事項を通知したときは、委託先は報告義務を免除される
  - ➢ 後述する本人への通知義務も免除（法26②かっこ書）



社労夢の場合

PPC

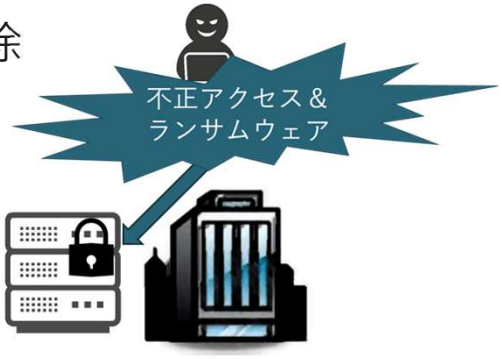
【報告】　【報告（免除可）】　【報告（免除可）】

委託元 ― 委託先

報告事項を通知すれば
PPCへの報告義務は免除

委託元 ― 委託先

報告事項を通知すれば
PPCへの報告義務は免除



顧問先企業

社労士事務所

エムケイシステム

個人情報

在籍

退職

従業員（本人）

報告事項（規則8①各号）

1号	概要	発生日、発覚日、発生事案、発見者、報告対象事態該当性、委託元及び委託先の有無、事実経過等
2号	漏えい等が発生し、又は発生したおそれがある個人データの項目	媒体や種類（顧客情報、従業員情報の別等）とともに報告
3号	漏えい等が発生し、又は発生したおそれがある個人データに係る本人の数	
4号	当該事態が発生した原因	当該事態が発生した主体（報告者又は委託先）とともに報告
5号	当該事態に起因して発生する二次被害又はそのおそれの有無及びその内容	クレジットカードの不正利用，ポイントサービスにおけるポイントの不正利用，漏えいしたメールアドレス宛てに第三者が不審なメール・詐欺メールを送信すること 等
6号	本人への対応の実施状況	当該事態を知った後、本人に対して行った措置（通知を含む。）の実施状況
7号	当該事態に関する公表の実施状況	
8号	再発防止のための措置	実施済みの措置と今後実施予定の措置に分けて報告
9号	その他参考となる事項（個人情報保護委員会が当該事態を把握する上で参考となる事項）	他の行政機関等への報告状況（捜査機関への申告状況も含む。），外国の行政機関等への報告状況，当該個人情報取扱事業者が上場会社である場合、適時開示の実施状況・実施予定，既に報告を行っている漏えい等事案がある中で、同時期に別の漏えい等事案が発生した場合には、両者が別の事案である旨 等

個人情報保護委員会（PPC）への報告の方法

- PPCのHPの報告フォームに入力して報告（通則GL）

漏えい等の対応とお役立ち資料

漏えい等の報告について

報告対象となる事態

下記の要件に該当する場合、漏えい等報告が義務付けられています。

（1）要配慮個人情報が含まれる個人データの漏えい等（又はそのおそれ）

（2）不正に利用されることにより財産的被害が生じるおそれがある個人データの漏えい等（又はそのおそれ）

（3）不正の目的をもって行われたおそれがある個人データの漏えい等（又はそのおそれ）

（4）個人データに係る本人の数が1,000人を超える漏えい等（又はそのおそれ）※民間事業者
保有個人情報に係る本人の数が100人を超える漏えい等（又はそのおそれ）※行政機関等

漏えい等報告はこちら

■ 漏えい等報告フォーム

【報告方法と留意点】

- 以下の質問の回答ボタンをクリックしていただきますと、ご報告いただく種類のフォームが開きます。
- 報告者の氏名又は名称の欄は、報告実務をされる担当者の氏名ではなく、事業者等の名称等をご入力ください。
- ご報告の際は以下の記載例をご覧いただいた上で、ご報告ください。
- 記載例
  ：民間事業者用　① （委託先事例）（PDF：229KB） ② （不正アクセス事例）（PDF：291KB）
  ③ （要配慮個人情報）（PDF：191KB）
  ：行政機関等用　④ （誤送付事例）（PDF：188KB）

[出典]
個人情報保護委員会（PPC）のサイト内の「漏えい等の対応とお役立ち資料」
https://www.ppc.go.jp/personalinfo/legal/leakAction/

報告フォーム

別記様式第一（第八条第三項関係）

受付日	年　月　日
受付番号	

報告書

個人情報の保護に関する法律第 26 条第 1 項の規定により、次のとおり報告します。

令和●年 5 月 15 日

個人情報保護委員会　殿

報告者の氏名又は名称　　株式会社〇〇工業
住所又は居所　　〇〇県△△市××－××

1．報告種別（該当する□に印を付けること。）
新規又は続報の別：□ 新規　☑ 続報　前回報告：令和●年 4 月 2 日
速報又は確報の別：□ 速報　☑ 確報

2．報告をする個人情報取扱事業者（以下「報告者」という。）の概要

報告者の氏名又は名称	（フリガナ）カ）●●●●コウギョウ 株式会社〇〇工業
法人番号（13 桁）	● ● ● ● ● ● ● ● ● ● ● ● ●
業種・業種番号	●●●●業　● ● ● ●
報告者の住所又は居所	〇〇県△△市 ××－××
代表者の氏名（報告者が法人等の場合に限る。）	（フリガナ）コジョウイ　イチロウ 代表取締役 個情委　一郎
事務連絡者の氏名	（フリガナ）カ）●●●●コウギョウ　ソウムブ　〇〇カ　ホゴホウ　ジロウ 株式会社〇〇工業 所属部署　総務部〇〇課　保護法　二郎 電話　●●●●（　●●　）　●●●● E-mail　●●●●@●●.jp

3．報告事項
（1）事態の概要（該当する□に印を付けること。）
発生日：令和●年 2 月 1 日
発覚日：令和●年 4 月 1 日
発生事案：☑ 漏えい　□ 漏えいのおそれ　□ 滅失
□ 滅失のおそれ　□ 毀損　□ 毀損のおそれ
発見者：□ 自社/委託先　□ 取引先　□ 顧客/会員
☑ カード会社/決済代行会社　□ その他（　　）
規則第 7 条各号該当性：□ 第 1 号（要配慮個人情報）
☑ 第 2 号（財産的被害）
☑ 第 3 号（不正の目的）
□ 第 4 号（千人超）
□ 非該当（上記に該当しない場合の報告）
報告者に個人データの取扱いを委託した者（委託元）の有無：
□ 有（名称：　　）
（住所：　　）
（電話：　　）
☑ 無
報告者から個人データの取扱いの委託を受けた者（委託先）の有無：
☑ 有（名称：株式会社●●●●　　）
（住所：●●県●●市●●●●　　）
（電話：●●-●●●●-●●●●　　）
□ 無

事実経過：

概要：
弊社が運営するショッピングサイト「●SHOP」（△△（オープンソースの EC サイト構築用プログラム（※製品名等を補記ください）で構築））がクロスサイトスクリプティング（XSS）攻撃による不正アクセスを受けクレジットカード情報等が漏えいした。

発覚の経緯・発覚後の事実経過（時系列）：
R●.4.1　決済代行会社より、当社ショッピングサイト上でカード決済を行った顧客のカードが不正利用されている可能性があるとの連絡あり、顧客情報の漏えいのおそれがあるため、カード決済を停止した。
当該サイトの保守運用を委託しているベンダーへ調査を依頼する。
この時点では詳細な原因等は判明せず。
R●.4.3　決済代行会社の要請により外部業者へフォレンジック調査を依頼する。
R●.5.27　調査の結果、下記のとおり外部からの侵入の痕跡が確認された。

報告フォーム（続き）

R●.2.1　△△のXSSに関する脆弱性を悪用され、注文システム内に悪性のスクリプトが挿入される。
R●.2.2　挿入された悪性スクリプトが実行され、ショッピングサイト「●SHOP」内に悪性ファイルが設置される。
R●.2.4～R●.4.1　悪性ファイルを利用し、この期間中にショッピングサイト「●SHOP」上で決済を行った顧客のカード情報が収集される。

※発覚の経緯・発覚後の事実経過欄には下内容をご記入ください。
・発覚日、発生日、発覚に至る経緯（いつ、どのように）被害の拡大防止のためにとった措置を時系列に記載
・結果（ランサムウェアでデータを暗号化された、カード情報を取られた、他の攻撃（スパムメール送信）への踏み台にされた）を含む

外部機関による調査の実施状況（規則第７条第３号に該当する場合のみ記載）：
☑ 実施済（実施中）【依頼日：令和●年４月３日】
☐ 実施予定【依頼予定日：　　年　　月　　日】
☐ 検討中
☐ 予定なし
（詳細：　　）

（2）漏えい等が発生し、又は発生したおそれがある個人データの項目（該当する□に印を付けること。）

媒体：	☐ 紙	☑ 電子媒体	☐ その他（　　）
種類：	☑ 顧客情報	☐ 従業員情報	☐ その他（　　）
項目：	☑ 氏名	☐ 生年月日	☐ 性別
	☐ 住所	☐ 電話番号	☐ メールアドレス
	☑ クレジットカード情報		☐ パスワード
	☑ その他（購入商品　　）		

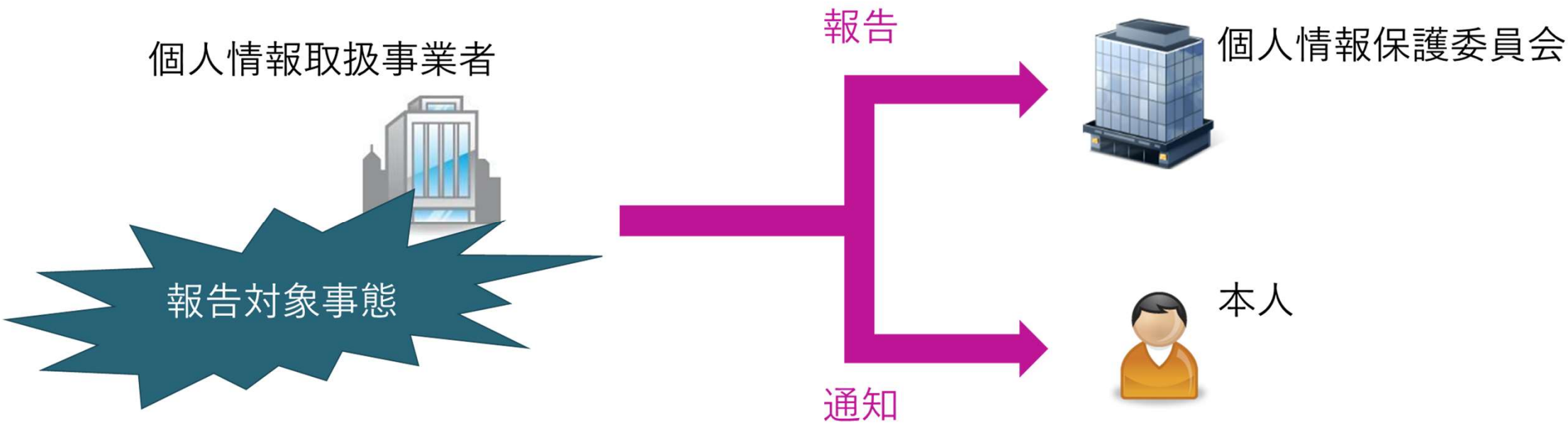
（3）漏えい等が発生し、又は発生したおそれがある個人データに係る本人の数
（　500）人　　うちクレジットカード情報含む（　500）人

本人への通知

個人データの漏えい等の本人への通知（法26条2項）

R2改正

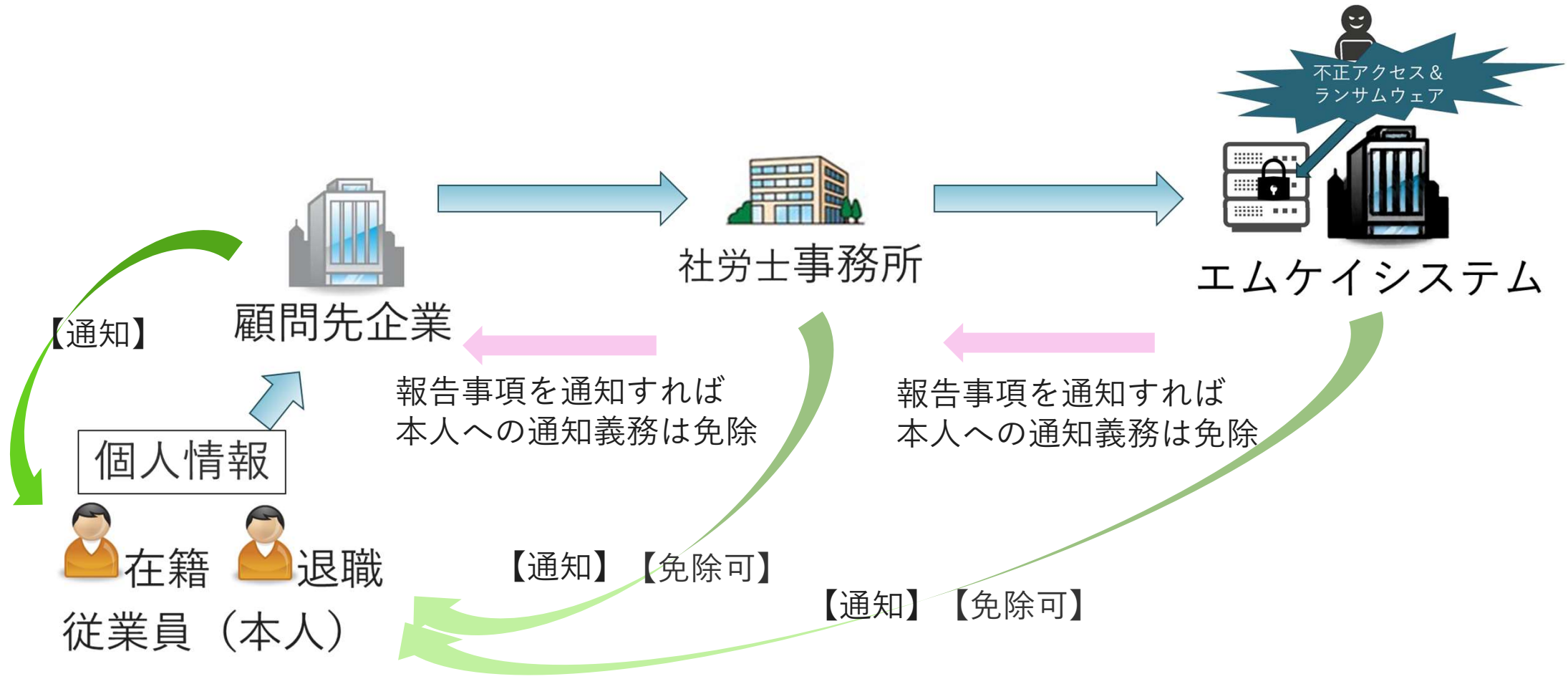
法26条	
1項	「報告対象事態」が生じたときは、当該事態が生じた旨を個人情報保護委員会に報告しなければならない
2項	報告対象事態を知った後、「通知事項」を本人に対し通知しなければならない



社労夢の場合

委託元 ― 委託先

委託元 ― 委託先



通知事項（規則10条）

「報告対象事態」を知った後、当該事態の状況に応じて速やかに、当該本人の権利利益を保護するために必要な範囲において、「通知事項」を本人に通知しなければならない（規則10）

● 通知事項 ：「報告事項」のうち、以下の事項（規則10）

1号	概要	発生日、発覚日、発生事案、発見者、報告対象事態該当性、委託元及び委託先の有無、事実経過等
2号	漏えい等が発生し、又は発生したおそれがある個人データの項目	媒体や種類（顧客情報、従業員情報の別等）とともに報告
~~3号~~	~~漏えい等が発生し、又は発生したおそれがある個人データに係る本人の数~~	
4号	当該事態が発生した原因	
5号	当該事態に起因して発生する二次被害又はそのおそれの有無及びその内容	クレジットカードの不正利用，ポイントサービスにおけるポイントの不正利用，漏えいしたメールアドレス宛てに第三者が不審なメール・詐欺メールを送信することなど
~~6号~~	~~本人への対応の実施状況~~	
~~7号~~	~~当該事態に関する公表の実施状況~~	
~~8号~~	~~再発防止のための措置~~	
9号	その他参考となる事項	

通知の時期（規則10条）

「報告対象事態」を知った後、当該事態の状況に応じて速やかに、当該本人の権利利益を保護するために必要な範囲において、「通知事項」を本人に通知しなければならない（規則10）

- **当該事態の状況に応じて速やかに**（法26②・規則10）

  その時点で把握している事態の内容、通知を行うことで本人の権利利益が保護される蓋然性、本人への通知を行うことで生じる弊害等を勘案して判断（通則GL）

  （その時点で通知の必要があるとはいえない事例：通則GL）

  - インターネット上の掲示板等に漏えいした複数の個人データがアップロードされており、個人情報取扱事業者において当該掲示板等の管理者に削除を求める等、必要な初期対応が完了しておらず、本人に通知することで、かえって被害が拡大するおそれがある場合
  - 漏えい等のおそれが生じたものの、事案がほとんど判明しておらず、その時点で本人に通知したとしても、本人がその権利利益を保護するための措置を講じられる見込みがなく、かえって混乱が生じるおそれがある場合

通知の範囲（規則10条）

「報告対象事態」を知った後、当該事態の状況に応じて速やかに、当該本人の権利利益を保護するために必要な範囲において、「通知事項」を本人に通知しなければならない（規則10）

● 当該本人の権利利益を保護するために必要な範囲（法26②・規則10）

（本人の権利利益を保護するために必要な範囲において通知を行う事例：通則GL）

- 不正アクセスにより個人データが漏えいした場合において、その原因を本人に通知するに当たり、個人情報保護委員会に報告した詳細な内容ではなく、必要な内容を選択して本人に通知すること
- 漏えい等が発生した個人データの項目が本人ごとに異なる場合において、当該本人に関係する内容のみを本人に通知すること

通知の方法

「報告対象事態」を知った後、当該事態の状況に応じて速やかに、当該本人の権利利益を保護するために必要な範囲において、「通知事項」を本人に通知しなければならない（規則10）

● 本人への通知（法26②）

- 本人に直接知らしめること
  - ➢ 事業の性質及び個人データの取扱状況に応じ、通知すべき内容が本人に認識される合理的かつ適切な方法によらなければならない（通則ＧＬ）
- 通知の様式についての法令上の定めはない

（例：通則ＧＬ）

- 文書を郵便等で送付することにより知らせる
- 電子メールを送信することにより知らせる
- 口頭で知らせる
  - ➢ 必要に応じて書面又は電子メール等による通知を併用することが望ましい（Ｑ＆Ａ）

本人への通知が困難である場合の代替措置

本人への通知が困難な場合であって、本人の権利利益を保護するため必要なこれに代わるべき措置をとるときは、この限りでない。（法26条２項）

	具体例（通則GL）
通知が困難	◯ 保有する個人データの中に本人の連絡先が含まれていない ◯ 連絡先が古いために通知を行う時点で本人へ連絡ができない ✕ 複数の連絡先を保有している場合に、１つの連絡先に連絡したが本人に連絡が取れなかった（Q＆A）
代替措置	• 事案の公表 ➢ 公表すべき内容は、本人へ通知すべき内容を基本とする ➢ 特定の個人が識別されるおそれがある事項については公表しなくてよい（Q＆A同旨） • 問合せ窓口を用意してその連絡先を公表し、本人が自らの個人データが対象となっているか否かを確認できるようにする ➢ 常設している個人情報の取扱いに関する相談を受け付ける窓口を利用することは可能（Q＆A）

社労夢事件における通知が困難な場合の公表の例

過去に当社と雇用関係にあった方へのお知らせ

2023.06.20

当社委託先使用システム（社労夢）への不正アクセス事案について

この度、当社の委託先において利用するシステムのサーバーがランサムウェアによる第三者からの不正アクセスを受けたことが判明いたしましたので、お知らせいたします。

現時点において情報漏えいの事実は確認されていませんが、この事態を重く受け止め、対象となる可能性のある皆様には、メールや書面等で順次ご連絡を差し上げており、併せて本ページでもお知らせいたします。

今後、漏えい等の事実が判明するなど、追加情報がありましたら、改めてお知らせいたします。なお、監督官庁への報告は適正に対応しております。

1.事態の概要および当該事態が発生した原因等

本年6月9日に、当社が労務業務の一部を委託している社会保険労務士事務所より、同事務所が使用する業務支援システム「社労夢」（本件システム）の運営ベンダー会社である株式会社エムケイシステムのデータサーバーが、ランサムウェアによるサイバー攻撃を受け、情報流出の可能性を否定できないことが判明したとの報告を受けました。

株式会社エムケイシステムより、現時点において、個人情報が外部へ送信された痕跡については発見されておらず、本件にかかわる個人情報の不正利用等の事実も確認されていないとの報告を受けております。引き続き、委託先である社会保険労務士事務所を通じて、対象となる個人情報の範囲や漏えい等の有無等の事実確認を行ってまいります。

なお、本ページ記載の内容は、委託先である社会保険労務士からの報告及びエムケイシステム社の

社労夢事件における通知が困難な場合の公表の例（続き）

リリース（※）等に基づくものが含まれ、現時点で判明している事実に限られることにご留意ください。

※エムケイシステム社の「第三者によるランサムウェア感染被害への対応状況のお知らせ」（6月9日付）および「東京新聞に掲載された記事ついて」（6月16日付）をご確認ください。

2.対象者

当社と過去に雇用関係にあった方（従業員・アルバイト・契約社員など）

3.漏えい等のおそれがある個人データの項目

名前（本人及び家族）、住所、電話番号、本人の給与及び賞与金額、生年月日、基礎年金番号等

なお、マイナンバーは本件システムに保存されていません。

4.二次被害について

二次被害の有無やおそれについて現在調査中ですが、現時点において、情報漏えい等の事実や情報の悪用等による二次被害は確認されておりません。二次被害が確認された場合、必要な情報についてお知らせいたします。

皆様には大変ご心配とご迷惑をおかけいたしますが、個人情報の不正利用や被害防止のために、不審な連絡等にはご注意いただきますようお願い申し上げます。

5.本件に関する問い合わせ先

〇〇対応窓口：aaaa@bbcorp.com

なお、本件に関する最新の情報については、エムケイシステム社のリリース等をあわせてご確認ください。

R2改正

漏えい等事案への対応

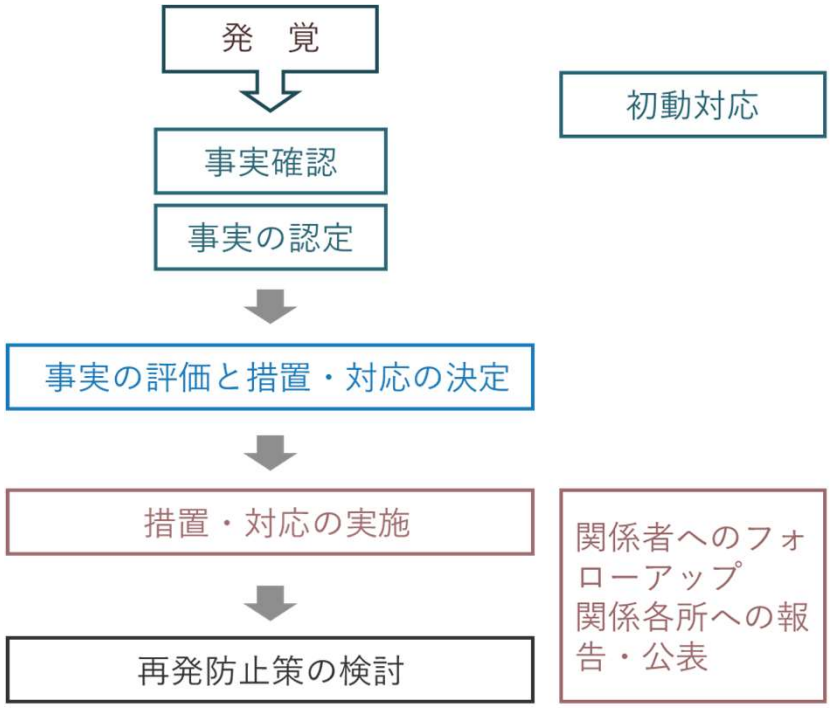
漏えい等事案が発覚した場合に講ずべき措置

漏えい等事案が発覚した場合に講ずべき措置（通則ＧＬ）

漏えい等事案が発覚した場合は、漏えい等事案の内容等に応じて、次の(1)から(5)に掲げる事項について、必要な措置を講じなければならない（通則ＧＬ）

(1) 事業者内部における報告及び被害の拡大防止
(2) 事実関係の調査及び原因の究明
(3) 影響範囲の特定
(4) 再発防止策の検討及び実施
(5) 個人情報保護委員会への報告及び本人への通知

- 危機対応（不祥事対応）の基本的な流れ



(1) 事業者内部における報告及び被害の拡大防止

責任ある立場の者に直ちに報告するとともに、漏えい等事案による被害が発覚時よりも拡大しないよう必要な措置を講ずる（通則ＧＬ）

● 責任ある立場の者

- 役職は限定されていない（Ｑ＆Ａ）
- 取扱規程等により、漏えい等事案が発覚した場合の適切かつ迅速な報告連絡体制を整備しておくことが必要（Ｑ＆Ａ）

● 初動対応

（被害拡大防止のための初動対応の例）

- 外部からの不正アクセスや不正プログラムの感染が疑われる場合に、当該端末等のLANケーブルを抜いてネットワークからの切り離しを行う又は無線LANの無効化を行うなどの措置を直ちに行う（Ｑ＆Ａ）
- 問題が発生しているシステムを休止する

（その他の初動対応の例）

- 役員等社内人員で構成する事故対策本部を設置する
- 外部専門家に相談する
- 初期公表の必要性を検討する

(2) 事実関係の調査及び原因の究明

漏えい等事案の事実関係の調査及び原因の究明に必要な措置を講ずる（通則ＧＬ）

● 事実関係の調査等

（例）

- 事故対策本部の指揮のもと、漏えい等の原因（経路等）と漏えい等した情報（漏えい等の範囲）を特定するための調査を実施する
  - ➢ 漏えい等が発生した端末の記憶媒体の調査（削除されたデータの復元，基本ソフトウェアが管理している情報の解析など）
  - ➢ （ツールが導入されている場合）漏えい等が発生した端末のソフトウェアの利用状況等を記録するツールの調査
  - ➢ （不正プログラムによる場合）不正プログラムの確保・解析
  - ➢ （端末がシャットダウンされていない場合）漏えい等が発生した端末のメモリの調査
  - ➢ サーバ等（ファイルサーバ・認証サーバや、経路交換機等の通信機器）の履歴調査
  - ➢ （専用機器が導入されている場合）ネットワークの通信内容の調査
- コンサル会社、漏えい事故調査会社等の外部専門家に調査を依頼して、事実の調査と原因の究明に努める

(3) 影響範囲の特定

事実関係の調査及び原因の究明で把握した事実関係による影響範囲の特定のために必要な措置を講ずる（通則ＧＬ）

（影響範囲の特定のために必要な措置の例）

- 漏えいした個人データに係る本人の数、漏えいした個人データの内容、漏えいした手段、漏えいした原因等を踏まえ、影響の範囲を特定する（Ｑ＆Ａ）
- 事故対策本部や外部専門家等により、漏えい等が疑われる情報の内容（漏えいした個人情報の件数や項目等）、事故の影響を受ける本人、二次被害の有無等、事故の影響範囲を特定する

(4) 再発防止策の検討及び実施

事実関係の調査及び原因の究明の結果を踏まえ、漏えい等事案の再発防止策の検討及び実施に必要な措置を講ずる（通則ＧＬ）

（再発防止策の検討及び実施に必要な措置の例）

- 役員、外部専門家等で構成された事故調査委員会を設置して、事実調査、原因の究明および影響範囲の特定の結果に基づいて事故の再発防止策を検討し、実施する
- 二次被害防止策を講ずる

  （二次被害防止策の例）

  - 顧客名簿が名簿業者に渡った場合は名簿業者に警告し回収する
  - 個人情報が掲示板等に掲載された場合は掲示板等へ削除要請する
  - クレジットカード等の情報が漏えいした場合は、専門業者への不正利用のモニタリング依頼をする

(5) 個人情報保護委員会への報告及び本人への通知

個人情報保護委員会への報告は法26条１項、本人への通知は法26条２項に従って実施する（通則ＧＬ）

● ＰＰＣへの報告，本人への通知

- 前述

● 事案の公表

漏えい等事案の内容等に応じて、二次被害の防止、類似事案の発生防止等の観点から、事実関係及び再発防止策等について、速やかに公表することが望ましい（通則ＧＬ）

過去の大量漏えい事案にみる対応モデル

□ 事故の可能性の把握と初期対応

- 役員会等で当面の処置を決定（システム休止等）
- 事故対策本部設置（役員等社内人員で構成）
- 外部専門家（コンサル会社，調査会社等）に相談・調査依頼
- 二次被害防止策を講ずる（名簿業者に警告・回収，掲示板等への削除要請，クレジットカード等不正利用のモニタリング依頼等）

□ 公表（できるだけ早く）

- 事故調査委員会設置（役員，外部専門家=コンサル会社・弁護士等）
- お問い合わせ窓口設置
- 警察に相談
- 漏えいが疑われる情報の本人に連絡・お詫び

□ 中間報告

- 調査結果を受けて対応策の検討
- 関係機関（個人情報保護委員会・監督官庁等）への報告
- 警察に被害届，刑事告訴
- 漏洩した顧客への各種対応（金券交付，無償サービス提供等）
- 社内処分（懲戒処分，役員の減給等）
- 検証委員会設置（再発防止策の検討）（社外取締役，外部専門家）

□ 最終報告

- 安全管理措置の見直し・改善（再発防止策の検討・実施）
- クレーム，訴訟への対応

R2改正

保有個人データに関する義務

法35条５項の要件を満たす場合の利用停止等又は第三者提供の停止（法35条5項）

本人は、個人情報取扱事業者に対し、当該本人が識別される保有個人データを当該個人情報取扱事業者が利用する必要がなくなった場合、当該本人が識別される保有個人データに係る第26条第１項本文に規定する事態が生じた場合その他当該本人が識別される保有個人データの取扱いにより当該本人の権利又は正当な利益が害されるおそれがある場合には、当該保有個人データの利用停止等又は第三者への提供の停止を請求することができる（法35条５項）

個人情報取扱事業者は、前項の規定による請求を受けた場合であって、その請求に理由があることが判明したときは、本人の権利利益の侵害を防止するために必要な限度で、遅滞なく、当該保有個人データの利用停止等又は第三者への提供の停止を行わなければならない。ただし・・・（法35条６項）

法35条5項の利用停止等・第三者提供停止の請求（法35条5項・6項）の概要

利用停止等の対象	請求への対応	制限等
次の場合には、当該本人が識別される保有個人データの利用停止等または第三者提供の停止を請求できる（法35⑤） • 当該保有個人データを当該個人情報取扱事業者が利用する必要がなくなった場合 • 個人情報保護委員会に漏えい等の報告をしなければならない場合（法26①） • 本人の権利又は正当な利益が害されるおそれがある場合	1. 法35⑤の請求に理由があることが判明したときは、本人の権利利益の侵害を防止するために必要な限度で、遅滞なく、当該保有個人データの利用停止等・第三者提供停止を行い（法35⑥）、遅滞なく、その旨を通知（法35⑦） 3. 利用停止等・第三者提供停止を行わない旨の決定をしたときは、遅滞なく、その旨を通知（同）	◯ 当該保有個人データの利用停止等・第三者提供停止に多額の費用を要する場合その他の利用停止等を行うことが困難な場合であって、本人の権利利益を保護するため必要なこれに代わるべき措置をとるときは、この限りでない（法35⑥但書） ◯ 請求を受け付ける方法を定めることができる（法37） ✕ 手数料は徴収できない

要件

● 個人情報取扱事業者が利用する必要がなくなった場合

- 法22条後段（不要な個人データの消去）と同様に、利用目的が達成され当該目的との関係では当該保有個人データを保有する合理的な理由が存在しなくなった場合や利用目的が達成されなかったものの当該目的の前提となる事業自体が中止となった場合等をいう（通則GL）

【利用する必要がなくなった場合の例】

- ダイレクトメールを送付するために保有していた情報について、ダイレクトメールの送付を停止している場合
- 電話勧誘のために保有していた情報について、電話勧誘を停止している場合
- キャンペーンの懸賞品送付のために保有していた当該キャンペーンの応募者の情報について、懸賞品の発送が終わり、不着対応等のための合理的な期間が経過した後
- 採用応募者のうち、採用に至らなかった応募者の情報について、再応募への対応等のための合理的な期間が経過した後

要件

- 当該本人が識別される保有個人データに係る法26条１項本文に規定する事態が生じた場合
  - 個人情報保護委員会への報告対象事案が生じた場合
- 当該本人の権利又は正当な利益が害されるおそれがある場合
  - 「おそれ」は、一般人の認識を基準として、客観的に判断する（通則GL）
  - 個人情報取扱事業者に本人の権利利益の保護の必要性を上回る特別な事情がない限り、個人情報取扱事業者は請求に応じる必要がある（通則GL）

【本人の権利又は正当な利益が害されるおそれがある場合の例】

◯ ダイレクトメールの送付を受けた本人が、送付の停止を求める意思を表示したにもかかわらず、個人情報取扱事業者がダイレクトメールを繰り返し送付している場合

◯ 電話勧誘を受けた本人が、電話勧誘の停止を求める意思を表示したにもかかわらず、個人情報取扱事業者が本人に対する電話勧誘を繰り返し行っている場合

◯ 個人情報取扱事業者が、安全管理措置を十分に講じておらず、本人を識別する保有個人データが漏えい等するおそれがある場合

要件

【本人の権利又は正当な利益が害されるおそれがある場合の例】

◯ 個人情報取扱事業者が、法27条１項に違反して第三者提供を行っており、本人を識別する保有個人データについても本人の同意なく提供されるおそれがある場合

◯ 個人情報取扱事業者が、退職した従業員の情報を現在も自社の従業員であるようにホームページ等に掲載し、これによって本人に不利益が生じるおそれがある場合

【本人の権利又は正当な利益が害されるおそれがない場合の例】

✕ 電話の加入者が、電話料金の支払いを免れるため、電話会社に対して課金に必要な情報の利用停止等を請求する場合

✕ インターネット上で匿名の投稿を行った者が、発信者情報開示請求による発信者の特定やその後の損害賠償請求を免れるため、プロバイダに対してその保有する接続認証ログ等の利用停止等を請求する場合

✕ 過去に利用規約に違反したことを理由としてサービスの強制退会処分を受けた者が、再度当該サービスを利用するため、当該サービスを提供する個人情報取扱事業者に対して強制退会処分を受けたことを含むユーザー情報の利用停止等を請求する場合

✕ 過去の信用情報に基づく融資審査により新たな融資を受けることが困難になった者が、新規の借入れを受けるため、当該信用情報を保有している個人情報取扱事業者に対して現に審査に必要な信用情報の利用停止等又は第三者提供の停止を請求する場合

漏えい事故の法的問題

事業者の法的責任

BANDO Yoshikuni
Attorny at Law

事業者の民事責任

※ 漏えい事故等について個人情報保護法違反はなくても、プライバシーの侵害や、個人情報の漏えいによる不快感・漏えいによる影響に対する不安感が生ずることにより、精神的損害が発生したとして、本人からの損害賠償（慰謝料）請求が認められる可能性

- 事業者自身に過失（落ち度）がある

  ➡ 事業者は民法709条による不法行為責任を負う

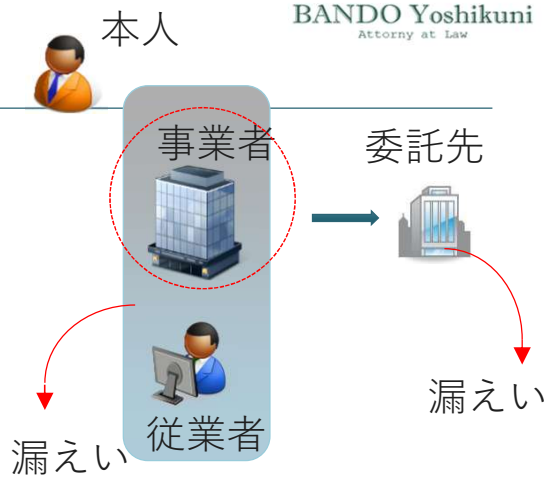
  - 事業者のサーバのセキュリティ管理ミスによる顧客情報漏えい
  - 消費者金融が人違いで誤った延滞情報を信用情報機関に提供し、本人から誤りを指摘されたにもかかわらず１年数ヶ月間にわたって放置したことについて、消費者金融に11万円の損害賠償を命じた裁判例あり（京都地判H15.10.3）
  - 委託先のサーバからの漏えい等の場合でも、委託先に対する適切な監督をすべき注意義務に違反したとして委託元の損害賠償を命じた裁判例あり（東京高判R1.6.27：ベネッセ事件）

- 従業者の漏えい行為による：従業者は不法行為責任を負う（民法709条）

  ➡ 事業者は民法715条による使用者責任を負う（従業者と連帯責任）

> 「ある事業のために他人を使用する者は，被用者がその事業の執行について第三者に加えた損害を賠償する責任を負う」（民法715条本文）

事業者の個人情報保護法上の責任



- 事業者の管理ミスによる場合　→ 安全管理措置義務（法23条）違反
- 従業者の漏えい行為による場合 → 従業者の監督義務（法24条）違反
- 委託先の漏えい行為による場合 → 委託先の監督義務（法25条）違反

➢ 個人情報保護委員会による報告徴収・立入検査，指導・助言，勧告，命令の対象（法143条・145条）

- 罰則：「両罰規定」（法184条）により、行為者とともに事業者も処罰される　※故意の場合
  - 個人情報保護委員会の命令違反（法178条）
    - ➢ 事業者が個人の場合は、行為者と同じ100万円以下の罰金だが、
    - ➢ 事業者が法人の場合は、１億円以下の罰金
  - 故意による漏えい：個人情報データベース等提供罪（法179条）
    - ➢ 事業者が個人の場合は、行為者と同じ50万円以下の罰金だが、
    - ➢ 事業者が法人の場合は、１億円以下の罰金
  - 個人情報法保護委員会による報告徴収・立入検査の妨害等（法182条）
    - ➢ 事業者が個人・法人いずれの場合も、行為者と同じ50万円以下の罰金

安全管理措置を講ずる義務－ 個人情報保護法23条とガイドライン

- **必要かつ適切な措置を講じなければならない**（法23条）
  - 安全管理措置を講ずるための具体的な手法は、個人データが漏えい等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、事業の規模及び性質、個人データの取扱状況、取り扱う個人データの性質及び量、個人データを記録した媒体の性質等に起因するリスクに応じて、必要かつ適切な内容とすべき（通則GL）

- **安全管理措置の具体的内容を策定する際に参照できる規範**

【一般】

- 通則ガイドライン「（別添）講ずべき安全管理措置の内容」（個人情報保護委員会）
- 特定個人情報の適正な取扱いに関するガイドライン（事業者編）（〃）

【Pマーク】

- JISQ15001「個人情報マネジメントシステム－要求事項」

【ISMS】

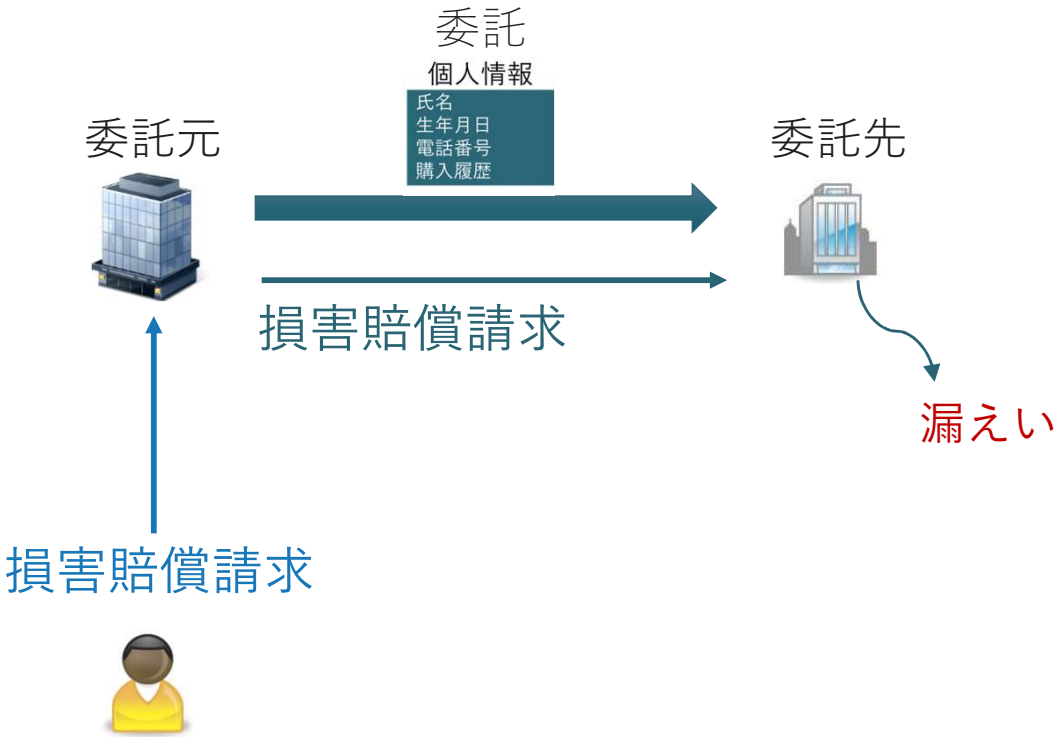
- JIS Q 27001「情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－要求事項」
- JIS Q 27002「情報技術－セキュリティ技術－情報セキュリティ管理策の実践のための規範」

委託元と委託先の関係

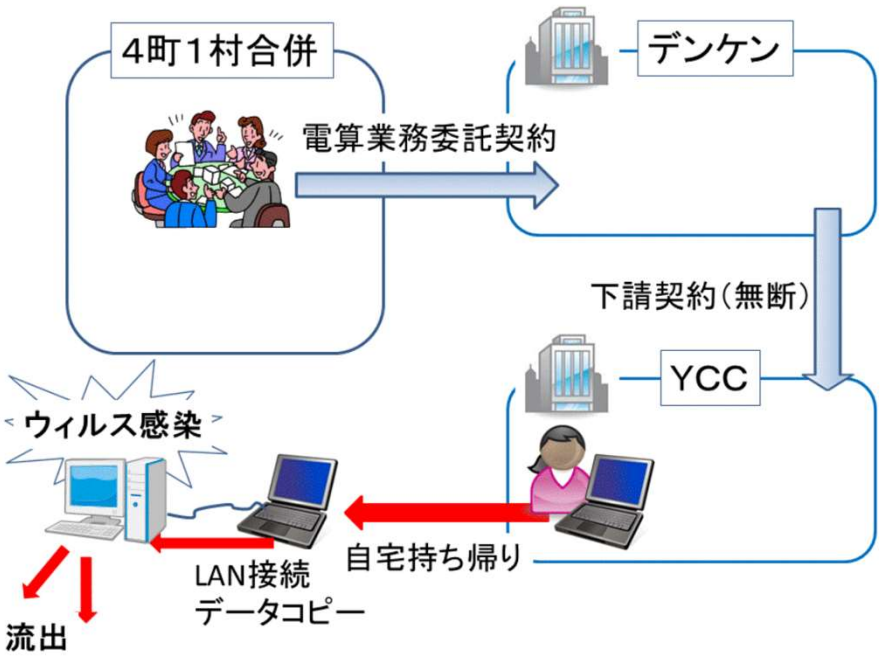
委託先の民事責任

● 委託先が漏えい事故を発生させた場合の委託元の責任

- 委託元から委託先に対し損害賠償請求（債務不履行責任or不法行為責任）
- 過失相殺が認められる可能性あり（民法418条・722条）



- 愛南町個人情報漏えい事件（山口地判H21.6.4）
  - 委託元（デンケン）の委託先（YCC）に対する損害賠償請求につき、委託元に4割の過失を認めて過失相殺した（6割認容）



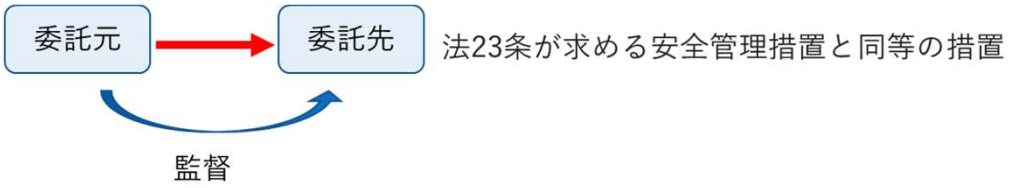
委託元の個人情報保護法上の責任（法25条，通則ＧＬ）-1

（委託先の監督）
第25条　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。

①　適切な委託先の選定

委託先の安全管理措置が、少なくとも法第23条で求められるものと同等であること※を確認するため、

「（別添）講ずべき安全管理措置の内容」に定める各項目が、委託する業務内容に沿って、確実に実施されることについて、あらかじめ確認しなければならない



※委託元が高い水準の措置を講じている場合でも、法律上は、委託先は 法23条が求める水準の安全管理措置を講じれば足りる（Q&A）

②　委託契約の締結

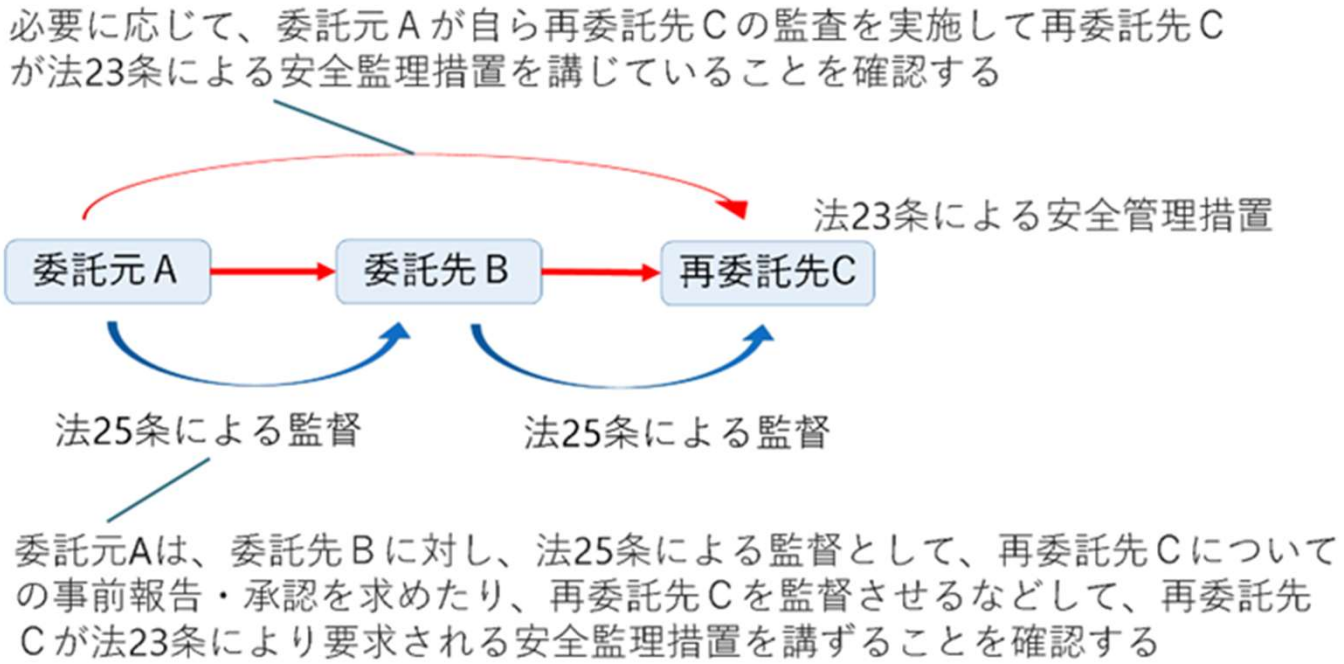
委託契約※には、当該個人データの取扱いに関する、必要かつ適切な安全管理措置として、委託元、委託先双方が同意した内容とともに、委託先における委託された個人データの取扱状況を委託元が合理的に把握することを盛り込むことが望ましい

※ 書式の類型（契約書、覚書、合意書の取り交わし、誓約書の差し入れ）を問わない（Q&A）

委託元の個人情報保護法上の責任（法25条，通則ＧＬ） -2

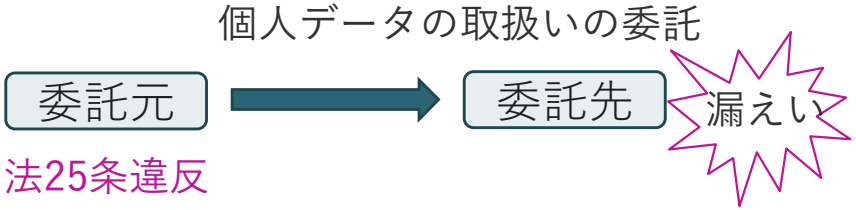
③	委託先における個人データ取扱状況の確認
	定期的に監査を行う等により、委託契約で盛り込んだ内容の実施の程度を調査した上で、委託の内容等の見直しを検討することを含め、適切に評価することが望ましい • 委託元が個人データを取り扱う場所に赴くこと（立入検査）は義務ではなく、取扱いを委託する個人データの内容や規模に応じて適切な方法（口頭による確認も含む。）を講じれば足りる（Q&A） • 委託先の従業員等から守秘義務等に係る誓約書を取得したり、委託先の従業員等の個人情報の提出を求めたりすることは義務ではない（Q&A）

［再委託の場合に実施することが望ましい措置（通則GL）］



委託先に対する必要かつ適切な監督を行っているといえない事例（通則GL）

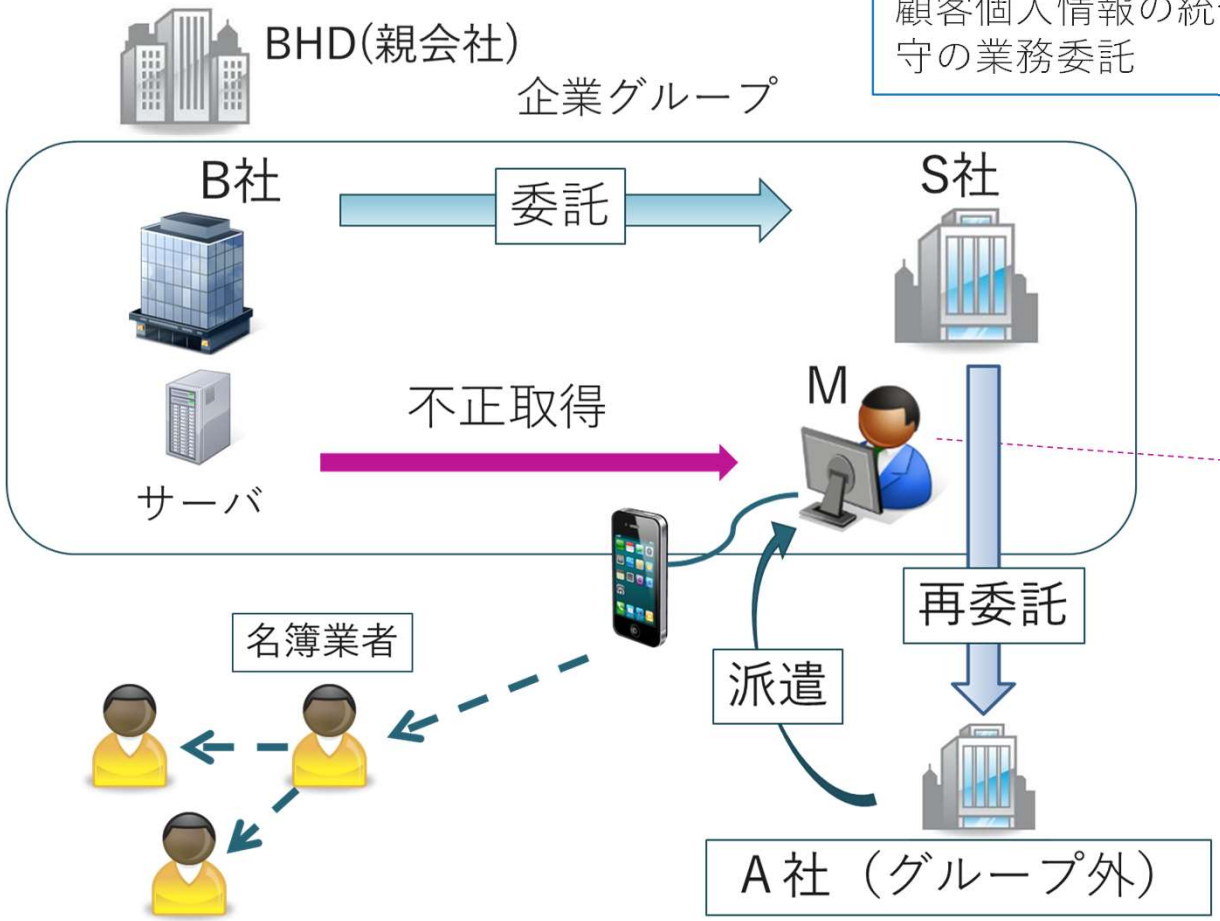
- 安全管理措置の状況を契約締結時及びそれ以後も適宜把握せず外部の事業者に委託した結果、委託先が個人データを漏えいした
- 個人データの取扱いに関して必要な安全管理措置の内容を委託先に指示しなかった結果、委託先が個人データを漏えいした



- 再委託の条件に関する指示を委託先に行わず、かつ委託先の個人データの取扱状況の確認を怠り、委託先が個人データの処理を再委託した結果、当該再委託先が個人データを漏えいした
- 契約の中に、委託元は委託先による再委託の実施状況を把握することが盛り込まれているにもかかわらず、委託先に対して再委託に関する報告を求めるなどの必要な措置を行わず、委託元の認知しない再委託が行われた結果、当該再委託先が個人データを漏えいした

先例となる事案

B社顧客情報漏えい事件（2014） ※調査委員会報告及び報道より



顧客個人情報の統合・分析に使用するシステムの開発・運用・保守の業務委託

S社から貸与されたPCからB社のデータベースに正規のアカウントでアクセスし、顧客情報約3500万件分をPCに保存し、USB接続したスマホに転送

［漏えいした情報］
- 氏名，性別，生年月日
- 郵便番号，住所，
- 電話番号
- メールアドレス
- 出産予定日
- 保護者の氏名　など

△

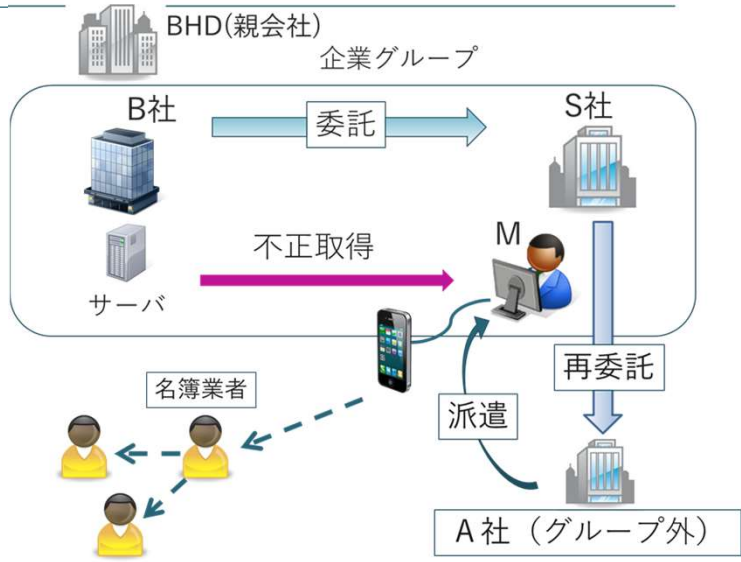
規則７条３号及び４号の「報告対象事態」に該当

名簿業者３社に顧客情報を売却して約400万円を得、顧客情報は最終的には500以上の業者に流出

名簿業者から約257万件分を購入したＪ社や約7万5000件分を購入したE社らがDM送付やセールス電話等に利用した

DM送付等のほかには、実害の発生は認められず（東京高判R1.6.27，報道）

B社顧客情報漏えい事件（2014） ※調査委員会報告及び報道より



● 脆弱性

技 クライアントPCとサーバ間の通信量が一定の閾値を超えた場合にS社の担当部長にメール送信されるアラートシステムの対象にMのクライアントPCとサーバ間の通信が設定されておらず、Mによる不正行為に対してアラートシステムが機能しなかった

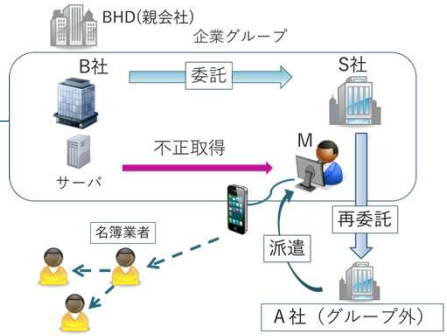
人 技 社内規程で社内PCのデータを外部メディアに書き出すことが原則禁止され、運用上も書出し制御システムが導入されていたが、

- クライアントPCのUSBポートは開放され、
- 制御システムも特定の新機種のスマートフォンへの書き出しについては機能しない状態であった

組 Bグループでは、全体の情報セキュリティの統括責任者が明確でなく、統括的に管理する部署も存在せず、個人情報管理の責任部門も不明確で、実効性ある監査は実施されていなかった

セキュリティソフトのバージョンアップにより、設定内容を変更すればデバイスの接続制御措置をとることが可能な状態だったが、設定変更がなされていなかった（東京高判R2.3.25）

事案の発覚と会社が講じた措置等 ※調査委員会報告及び報道より



6月末　B社のみに登録していた個人情報で、他社からDMやセールス電話が来ているとの問合せが急増

6/28　緊急対策本部設置（本部長はＢ社社長）

社内調査を開始，調査会社を起用（社外調査開始）

6/30　経産省に報告・相談

所轄警察署に報告・相談

お客様問合せ窓口設置

7/4　調査会社報告により名簿業者を把握し名簿を入手

- 保有データと名簿をマッチングさせた結果、Ｂ社しか保有していないデータが含まれていることが判明

7/7　社内調査の結果、データベースから顧客情報が持ち出されていることが判明

7/8　漏えいが疑われる顧客名簿を取り扱っている名簿業者及び名簿を利用してDMや電話をしている企業に名簿の利用・販売の中止を求める内容証明郵便を発送

7/9　顧客情報の漏えいを発表

△

(1) 事業者内部における報告及び被害の拡大防止

(2) 事実関係の調査及び原因の究明

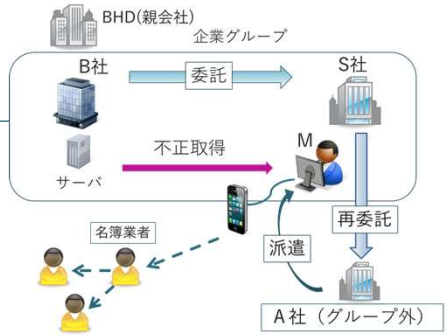
(3) 影響範囲の特定

(5) 個人情報保護委員会への報告及び本人への通知

△

（参考）
速報と確報

会社が講じた措置等 ※調査委員会報告及び報道より



7/10　顧客へのお詫びの文書発表

経産省が報告徴収を要請（報告書提出は7/17）

7/11　お詫びと対策状況に関する新聞広告

7/15　BHD社（親会社）に事故調査委員会を設置（弁護士，セキュリティ関連企業役員及びBHD役員ら計5名。メンバー決定は7/22）

警視庁に刑事告訴

7/17　Mを逮捕（8/7起訴）

⋮

9/17　経産省に最終報告書提出

9/25　調査委員会報告

9/26　BHDに外部監視機関設置（情報に関する法律・コンプライアンスに関する専門家，情報セキュリティに関する専門家などで構成）

経産省が個人情報保護法に基づき勧告

9月下旬　対象者にお詫び（500円分の金券交付又は新たに設立した「B社こども基金」への500円寄付の選択）

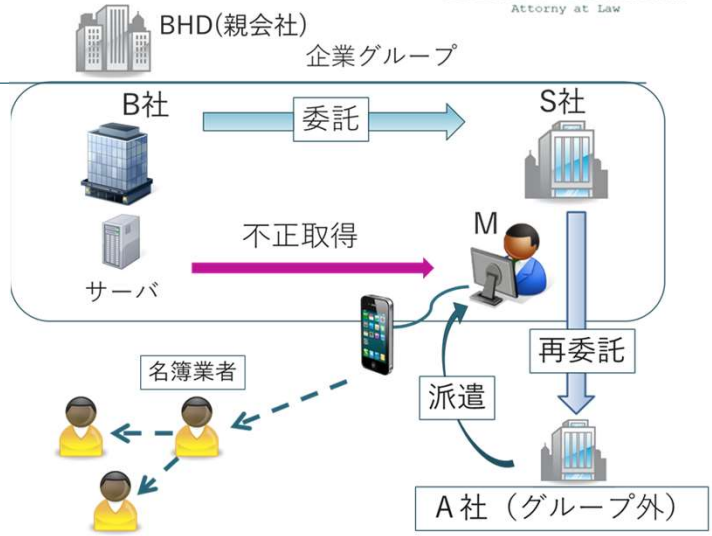
(1) 事実関係の調査及び原因の究明

(4) 再発防止策の検討及び実施

(5) 個人情報保護委員会への報告及び本人への通知

（参考）
速報と確報

漏えい事故の影響-1 ※調査委員会報告及び報道より



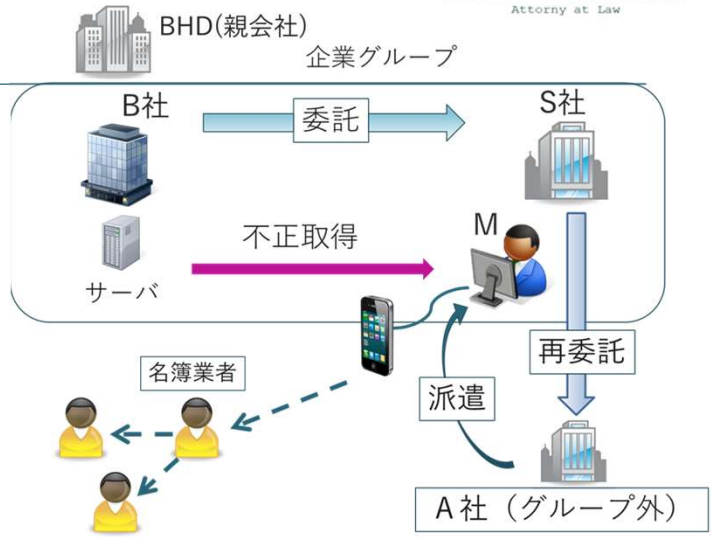
- BHDの代表取締役副会長と取締役1名が管理監督責任を重く受け止め辞任（7/31）
- JIPDECがＢ社のプライバシーマーク付与取消し措置を決定（11月）
  - ➢ JIPDECは名簿を購入してDM発送に利用した事業者に対しても勧告措置

- BHD発表の2014年第1四半期（4～6月期）決算で、特別損失を260億円計上（お客様へのお詫び200億，情報セキュリティ対応60億），最終損失が136億円と初めて赤字に転落
- Ｂ社が行う通信教育講座の会員数はピーク時の約420万人から2015年4月には約271万人に激減

- Mは、不正競争防止法違反（営業秘密の複製，開示。同法21条1項）の容疑で逮捕・起訴され、懲役2年6月（実刑）及び罰金300万円（東京高判H.29.3.21）
- Mから顧客情報を購入し転売した名簿業者と同社社長は不正競争防止法違反（営業秘密の取得・開示）の被疑事実で書類送検（社長は営業秘密の認識を否認）

- 平成27年（2015年）の個人情報保護法改正に影響（29条：第三者提供に係る記録の作成等，30条：第三者提供を受ける際の確認等）

漏えい事故の影響-2 ※報道等より



- 「被害者の会」「被害者弁護団」のもと、Ｂ社，Ｓ社およびBHDに対する損害賠償請求の訴訟が第５次訴訟まで提起

（被害者の会HPより）

  - 着手金・実費0円で成功報酬制

    第1次訴訟は原告１人あたり5万5000円、総額9839万5000円を請求（原告1789名）

    第2次訴訟は総額9630万5000円を請求（原告1751名）

    第3次訴訟は総額2億7500万円を請求（原告5000名）

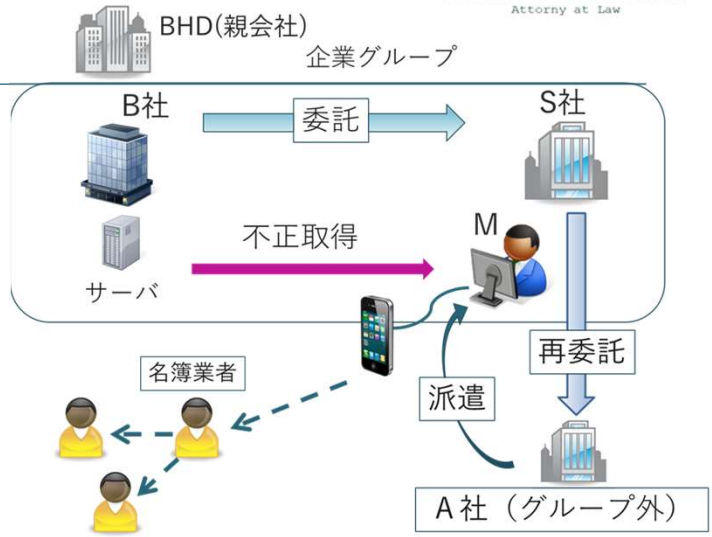
    第4次訴訟は総額5604万5000円を請求（原告1019名）

    第5次訴訟は総額6435万円を請求（原告1170名）

  - 東京地判R5.2.27は、Ｂ社およびＳ社の共同不法行為（民法719条1項前段）を認め、連帯して一人あたり3,300円（慰謝料3,000円＋弁護士費用300円。総額1300万円）の支払を命じた（B社が控訴）

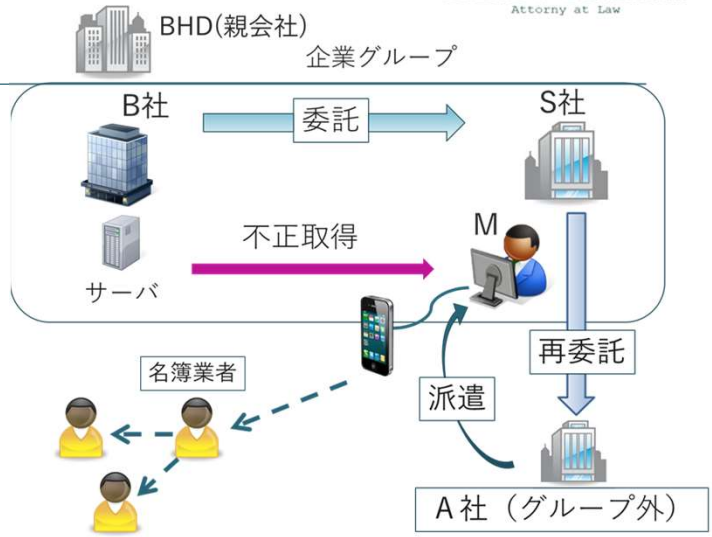
- この他にも、集団的訴訟や、弁護士等個人による訴訟提起もあり

漏えい事故の影響-3 ※報道等より



- 東京高判R1.6.27（2名がＢ社とＳ社に対して提訴し敗訴した東京地判と横浜地判の控訴審）
  - ➢ Ｂ社とＳ社の共同不法行為責任を認め、連帯して１人あたり2,000円の損害賠償を命じた
    - Ｓ社は、スマホによる書き出し制御措置を講ずべき注意義務違反の過失がある
    - Ｂ社は、委託先であるＳ社に対しセキュリティソフトの適切な設定を行っているか否かを監督する注意義務違反の過失がある
    - １人あたりの損害額を2,000円と認定（慰謝料のみで弁護士費用は認めず）
      - ✓ 漏えいした個人情報から何らかの重大なプライバシー情報が引き出されるとは想定しにくく、
      - ✓ 望まないDMが増えるかもしれないという危惧以上に何らかの実害が発生したとは認められない
      - ✓ 本件漏えいの発覚後にBHDが直ちに被害拡大防止措置を講じている
      - ✓ B社も顧客の選択に応じて500円相当の金券を配布する慰謝の措置を講じている

漏えい事故の影響-4 ※報道等より



- 東京高判R2.3.25（462人がB社とS社に対し合計約3590万円の損賠を求めたがB社の責任は否定された東京地判の控訴審）
  - ➢ Ｂ社とＳ社の共同不法行為責任を認め、連帯して１人あたり3,300円の損害賠償を命じた
    - Ｓ社は、セキュリティソフトを適切な設定内容に変更してデバイスの接続制御措置を講ずべき注意義務違反の過失がある
    - Ｂ社は、委託先であるＳ社に対しセキュリティソフトの適切な設定を行っているか否かを監督する注意義務違反の過失がある
    - １人あたりの損害額を3,300円と認定（慰謝料3,000円、弁護士費用300円）
      - ✓ 漏えいした個人情報は思想・信条，病歴，信用情報等とは異なり、個人の内面等に関わるような秘匿されるべき必要性が高い情報とはいえない
      - ✓ 財産的損害その他の実害が生じたことがうかがわれない
      - ✓ 本件漏えいの発覚後にBHDが直ちに被害拡大防止措置を講じている
      - ✓ B社も顧客の選択に応じて500円相当の謝罪品の交付を申し出ている

- 「被害者の会」による第３次訴訟を除く第１次～第５次訴訟（原告約5700名）の東京地判R5.2.23も、Ｂ社とＳ社の共同不法行為責任を認め、連帯して１人あたり3,300円の損害賠償を命じた

埼玉県社会保険労務士会大宮支部 個人情報保護法関係研修会

令和２年改正個人情報保護法と社労士業務

東京エクセル法律事務所
弁護士　坂　東　利　国

講演者（坂東利国）プロフィール

■経歴等

1989年　千葉県立千葉高校卒業　1994年　慶應義塾大学法学部法律学科卒業
2003年　弁護士登録（東京弁護士会・登録番号３０８９４）
2011年　ホライズンパートナーズ法律事務所（パートナー）
2020年　東京エクセル法律事務所（パートナー）

日本労働法学会　日本CSR普及協会　日本スポーツ法学会　所属
渋谷駅周辺地域ICT活用検討協議会法律顧問（2014年）
首都圏周辺地域ICT活用検討協議会法律顧問（2018年～）
働き方改革支援コンソーシアム顧問理事（2018年～）
日本ハラスメントカウンセラー協会顧問（2018年～）

《取扱業務》

コーポレート
・企業法務
・株主総会

人事・労務
・従業員関連の各種アドバイス
・就業規則その他の社内規程レビュー・作成
・社会保険労務士事務所の法律顧問

リスクマネジメント・危機管理
・ハラスメント関連（規程・組織体制の法適合性監査、社内研修）
・個人情報・マイナンバー関連（規程・組織体制の法適合監査、外部相談窓口、社内研修）
・コンプライアンス通報窓口
・社内調査サポート

家族関係
・離婚
・相続（遺言、遺言執行者、遺産分割等）

紛争解決
・交渉、あっせん、調停、労働審判、訴訟等

連絡先
メール：office@bando-law.com
事務所：東京エクセル法律事務所
東京都港区虎ノ門１－１－３
磯村ビル５階
（代表）03-3503-0921

職務経歴詳細
https://www.profile.bando-law.com

講演者（坂東利国）プロフィール

■顧問先企業の業種（坂東）

情報処理・システム開発、運送、服飾、資格・教育、薬局、コンサルティング、鉄鋼、自治体系、通信販売、医療法人、スポーツ協議連盟
社会保険労務士事務所、税理士事務所

■これまで担当した主な取扱案件の類型（事業者）

個別事案処理 （危機対応法務）	人事、労務の問題（交渉、仮処分、労働審判、訴訟等） 取引上のトラブル処理（交渉、調停、訴訟等）／不動産関連のトラブル処理（賃料請求・明渡し、契約条件変更などの内容証明郵便送付、交渉、調停、訴訟等） 会社組織上の問題（株主対応、株主総会指導、役員解任等、事業承継・事業譲渡の法務デューデリ等） 株式買取請求対応 会社、事業者の債務整理・倒産処理 不祥事対応（粉飾、情報漏えい、従業員の不正行為 等） 国税不服審判、行政不服審査／刑事告訴（横領、詐欺、背任）
コンサルティング （予防法務・リスク管理）	企業の法律顧問／士業向け顧問（税理士・社会保険労務士） 社内諸規程（就業規則、情報保護規程等）のレビュー、作成等／契約書や規約のレビュー、作成等 企業の人事労務に関連するアドバイス 株主総会・取締役会の準備アドバイス（取締役解任等）／株式会社以外の法人の社員総会・理事会の準備アドバイス 職場におけるハラスメント対策措置の法適合性監査／個人情報関連法令の適合性監査 内部通報窓口／ハラスメント相談外部窓口 事業承継準備／会社・事業者の倒産回避のためのアドバイス 破産管財人（東京地方裁判所）

講演者（坂東利国）プロフィール

《著作等》

『マイナンバー社内規程集』（日本法令 2015.5）
『中小企業のためのマイナンバー関連書式集』（日本法令 2016.1）
『改正個人情報保護法対応規定・書式集』（日本法令 2017.5）
『無期転換制度による法的リスク対応と就業規則等の整備のポイント』（DVD・日本法令 2018.2）
『同一労働・同一賃金の実務』（DVD・日本法令2019.2）
『働き方改革と労働法務』（マイナビ出版 2019.5）
『職場におけるハラスメントの理解とハラスメント相談窓口の実務』（全日本情報学習振興協会 2019.6）
『ハラスメントマネジメントの知識と実務』（全日本情報学習振興協会・2019.12）
『人事に役立つ ハラスメント 判例集50』（マイナビ出版・2020.3）
『管理職用 ハラスメント研修の教科書』（マイナビ出版・2020.9）
『TAX&LAW グループ会社の経営実務―法務・連結会計・税務― 』（共著・第一法規・2021.5） ほか

《記事等》

『マイナンバー法に対応した社内規程・書式の定め方』（SR-日本法令 2015.9）
『個人情報保護法ガイドライン』・体制整備＆規程見直し』（SR-日本法令 2017.2）
『無期転換ルール最終チェック（SR-日本法令 2018.2）
『従業員が反社会的勢力と関わっていた場合の企業対応」（月刊ビジネスガイド-日本法令 2019.11）
『これってハラスメント？ 定義・具体例・必要な防止対策を知ろう」（NISSAY Business INSIGHT 2021.4） ほか

《セミナー・研修の講師をさせていただいた企業の例（敬称略・社労士会・税理士会は多数のため除く。順不同）》

株式会社ISTソフトウェア，株式会社アイネット，旭商事株式会社，和泉運輸株式会社，伊藤忠テクノソリューションズ株式会社，医療法人社団総生会，Fホールディングス株式会社，NTT東日本，LVMHグループ，株式会社大阪エヌデーエス，株式会社京王設備サービス，株式会社光和コンピュータ，埼玉県産業労働部，SAPジャパン株式会社，山九株式会社，シェル商事株式会社，株式会社俊英館，株式会社タダノ，テレビ朝日映像株式会社，株式会社電通、東海カーボン株式会社，株式会社東急エージェンシープロミックス，東京ガスエンジニアリングソリューションズ株式会社，東芝テック株式会社，東和電気株式会社，凸版印刷株式会社，日曹エンジニアリング株式会社，株式会社ニッポンダイナミックシステムズ，日本水産株式会社，日本電気株式会社，株式会社日本法令，株式会社パルコスペースシステムズ，株式会社バンダイナムコエンターテイメント，株式会社富士通九州システムズ，フジモリ産業株式会社，ブリヂストンソフトウェア株式会社，ブリヂストンフローテック株式会社，HOYA株式会社，株式会社ワコム
学校法人あけぼの学院，学校法人大東文化学園，公益社団法人東京都看護協会，学校法人武蔵野大学
一般財団法人個人情報保護士会，埼玉SR経営労務センター，埼玉県（産業労働部人材活躍支援課），一般財団法人全日本情報学習振興協会，中小企業家同友会港支部，一般社団法人東京実業連合会，東京弁護士会法友会公正会，独独立行政法人都市再生機構（ＵＲ都市機構），一般社団法人長野県経営者協会，一般財団法人日本ハラスメントカウンセラー協会，日本労働組合総連合会埼玉県連合会，一般社団法人龍ケ崎労働基準協会