2024年個人情報保護教育(PF-１１６）

個人情報保護の基礎知識

個人情報保護教育の４つの目的

１．個人情報保護方針を理解する
２．個人情報保護の重要性および利点を理解する
３．個人情報保護における自分の役割および責任を理解する
４．個人情報保護に違反した際に予想される結果を理解する

個人情報保護方針

内部向けと外部向けの2つ個人情報保護方針

内部向け個人情報保護方針

① 事業の内容と規模を考慮した適切な個人情報の取り扱いを行い、目的外の利用を行わないこと。及びその措置を講じること。
② 個人情報に関する法令、国が定める指針、その他の規範を遵守すること。
③ 個人情報の漏えい、滅失又はき損の防止及び是正に関すること。
④ 苦情及び相談への対応を行うこと。
⑤ 個人情報保護マネジメントシステムの継続的改善を行うこと。
⑥ 組織名及び代表者役職名・氏名

外部向け個人情報保護方針

① 制定年月日及び最終改訂年月日
② 外部向け個人情報保護方針の内容についての問い合わせ先

株式会社イカイコントラクト　個人情報保護方針

株式会社イカイコントラクトは、総合人材サービス事業を営む企業として、個人情報の重要性と多数の個人情報を取り扱う責任の重大性を深く認識し、以下のように個人情報を適正に取り扱うことにより、社会の信頼に応えていきます。

1.個人情報の保護に関する法令等の遵守

当社は、個人情報の保護に関する法令、国が定める指針その他の規範を遵守します。

2.個人情報の取得・利用及び提供

当社は、個人情報を取得・利用する場合には、利用目的を明確にし、その利用目的達成のために必要な範囲内において、適法かつ公正な手段によって取得し利用します。また、本人の同意を得ることなく、目的外の利用、第三者への提供は行いません。また、目的外の利用をおこなわないための措置を講じます。

3.個人情報に対する安全管理措置

当社は、個人情報への不正アクセス、個人情報の漏洩・紛失・棄損等のリスクに対し、万全の安全対策及び是正措置を講じます。従業者や委託先に対しても適切な監督を行います。

4.個人情報に関する請求、苦情・相談等への対応

当社は、本人からの個人情報の開示・訂正・削除等の請求、個人情報の取扱いに関する苦情・相談等に対し、専用の窓口を設け、適切かつ迅速に対応します。

5.個人情報の保護の継続的改善

当社は、個人情報に関して一層適切な取扱いをするため、個人情報の保護に関する規程類や管理体制を定期的に見直し、継続的に改善を行います。

平成29年4月1日　制定
令和2年4月1日　最終改訂

代表取締役　　伊海　剛志

個人情報とは

個人情報保護法の定義

・生存する個人に関する情報　（JISでは死者も含む）

・氏名、生年月日その他の記述により特定の個人を識別できるもの

・個人別につけられた番号、記号、
又は画像や音声によって個人を識別できるもの
（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できるものを含む）

これも個人情報？

- 入室監視カメラの録画映像

  例えば、社員名簿に写真が登録されていて照合すれば特定できる場合。

- 留守番電話に架かって来た録音音声

  個人の特定が可能な場合で録音した情報

- 番号だけの情報

  預金番号、クレジットカード番号、社員番号、保険証番号などは、当該企業では容易に照合して特定可能

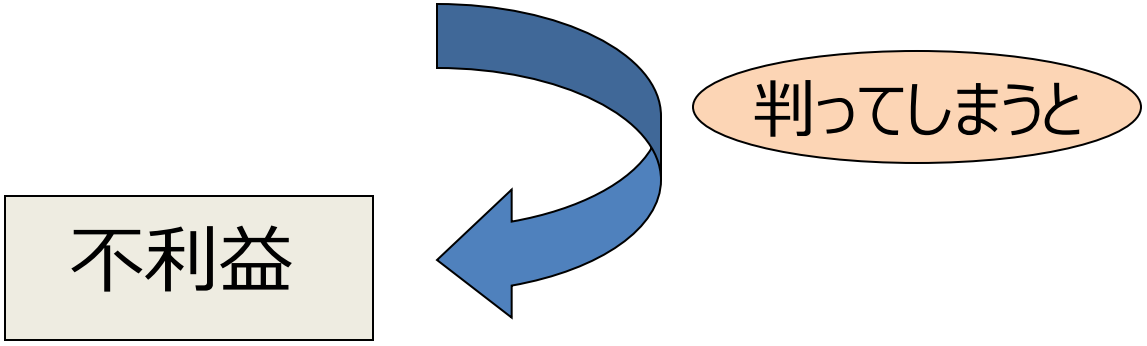
- 電話帳の情報

  住所、氏名、電話番号が公開されている情報

個人情報はなぜ大切

個人情報

《その情報があれば誰のことかわかってしまう一切の情報》



・個人が特定される → **情報の伝達、拡散**

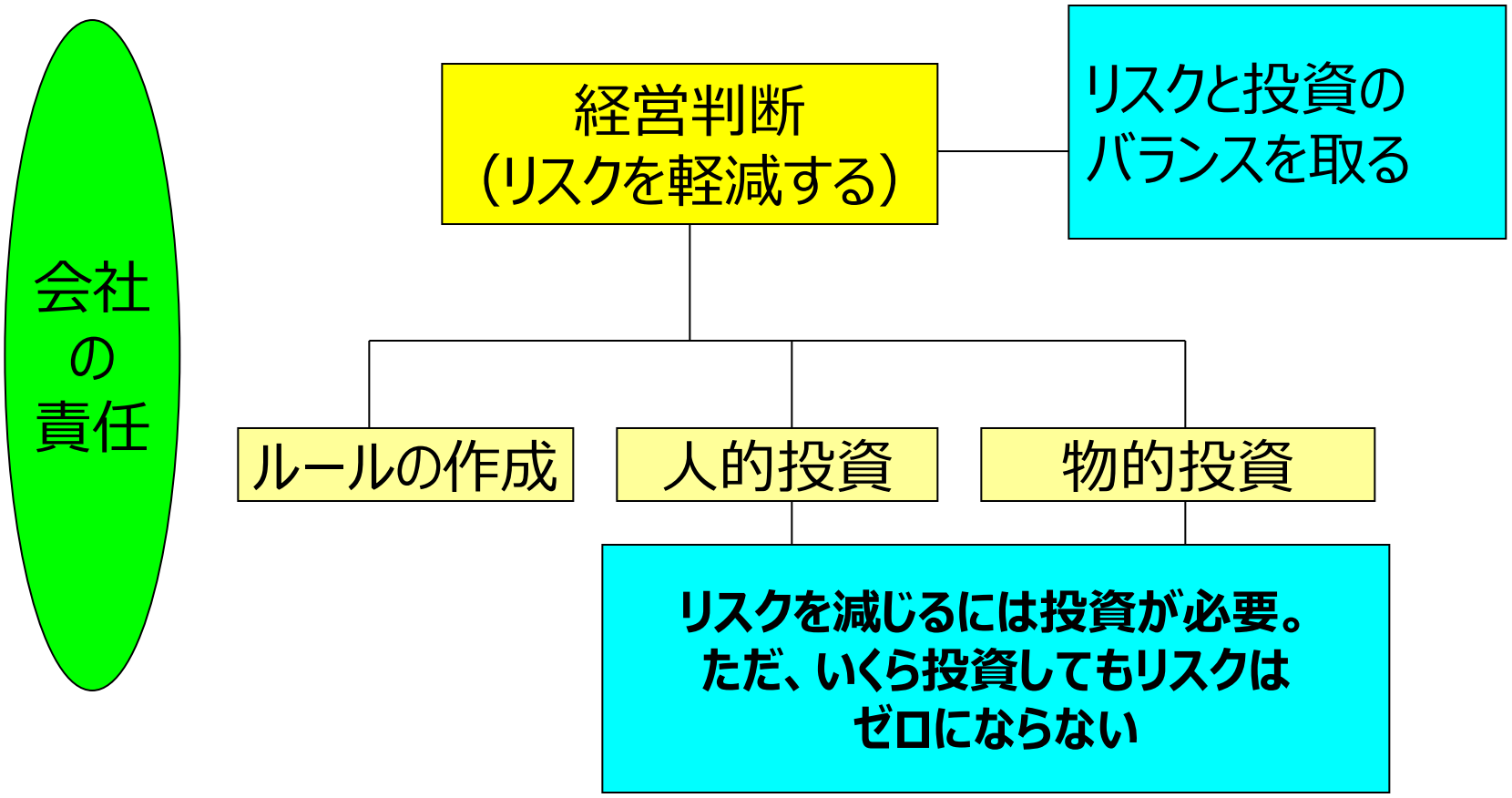
・個人に連絡、接触 → **セキュリティへの脅威（悪用される）**

個人情報保護に関する私達の役割と責任

私達
の
責任

- 個人情報保護のルールを理解して守る
- 上司の指示を守る
- おかしいと思ったことやリスクを放置せずに
  報告や対策を実施する

個人情報保護に関する私達の役割と責任



ＰＭＳにおける役割と責任

個人情報保護体制上の役割	責任
代表者 伊海　剛志	当社PMSの最高責任者として、管理責任者、監督責任者を指名し、PMSを実施させる。
個人情報保護管理者 小林　高晃	当社PMSの統括責任者として、PMSの構築、維持および個人情報取扱いの管理全般について責任を負う。
個人情報保護監査責任者 大川　洋二	内部監査について規程に従い、全部門の監査を計画、実行し、代表者に報告する。
個人情報保護教育責任者 室伏　智信	個人情報保護教育について規程に従い、全従業者に対するPMS教育を計画、実行し、個人情報保護管理責任者に報告する。
苦情相談管理責任者 神尾　俊明	開示請求や苦情等の問合せ対応全般について責任を負う。

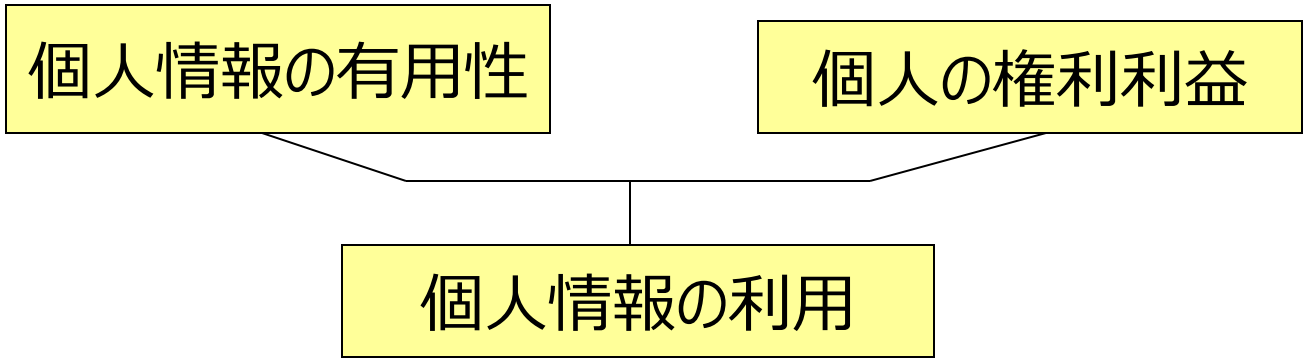
個人情報保護に関する発展経緯

プライバシー保護という考え方で発展

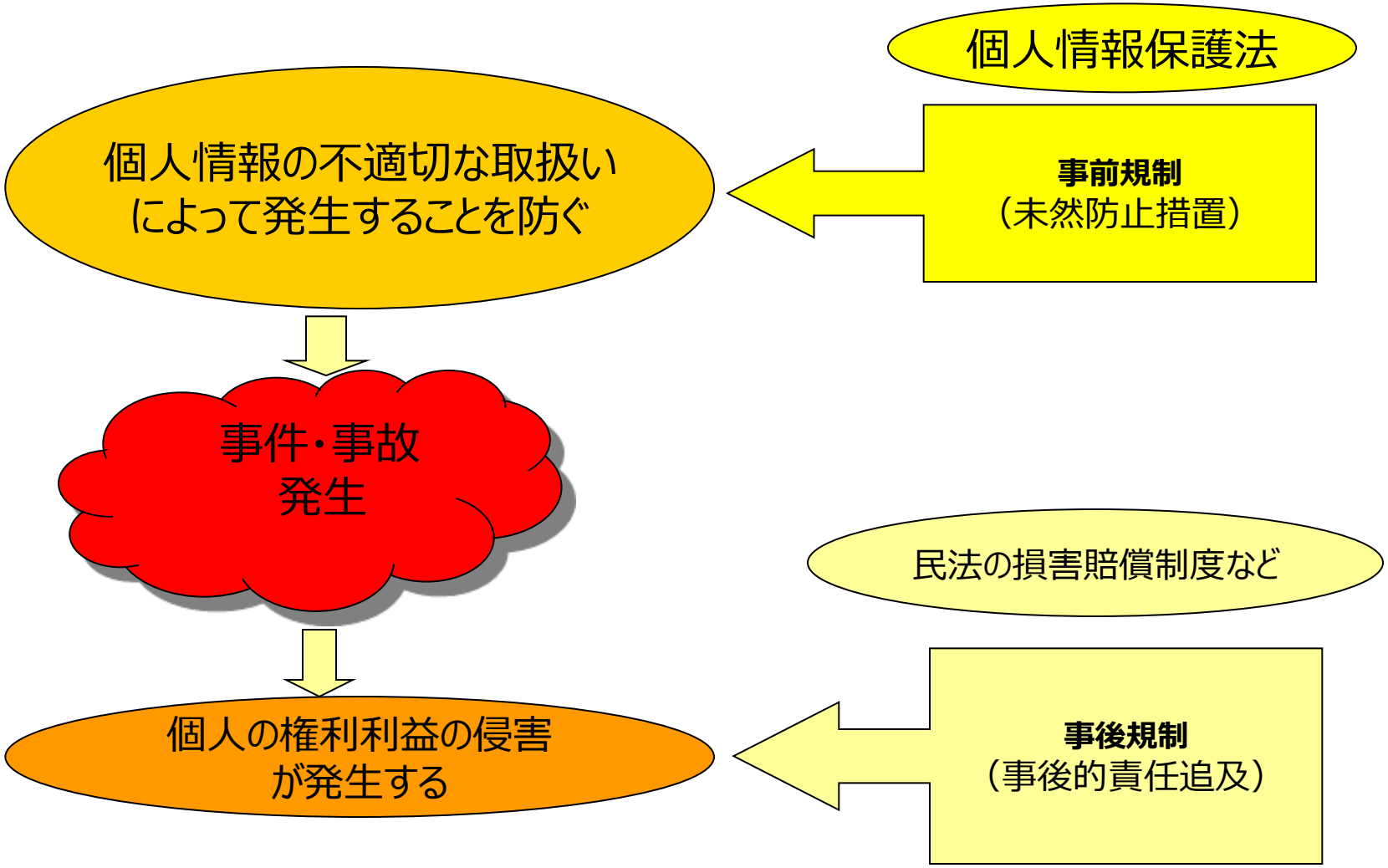
・1890年　米国　「プライバシーの権利」という書物の中で
「一人にしておいてもらう権利」と定義
・1971年　米国　「自己に関する情報の流れをコントロールする
個人の権利」と定義
・1964年　日本　「宴のあと」（三島由紀夫著）裁判で
「プライバシーの保護とは私生活をみだりに公開されない
という法的保障」とした。
・1980年　ＯＥＣＤ8原則採択
「プライバシー保護と個人データの
国際流通についてのガイドライン」
・2005年　「個人情報保護に関する法律」施行

個人情報保護法の目的

・高度な情報通信社会の発展により、
　個人情報の利用が著しく拡大した。
・個人情報を取り扱う事業者の
　遵守すべき義務等を定めた。
・個人情報の有用性に配慮しつつ、
　個人の権利利益を保護すること。



個人情報保護法は予防法



正確性の確保と安全管理措置

データ内容の正確性・最新性の確保

個人情報取扱事業者は、利用目的の達成に必要な範囲内で、
個人データを正確かつ最新の内容に保つように努めなければならない。

安全管理措置

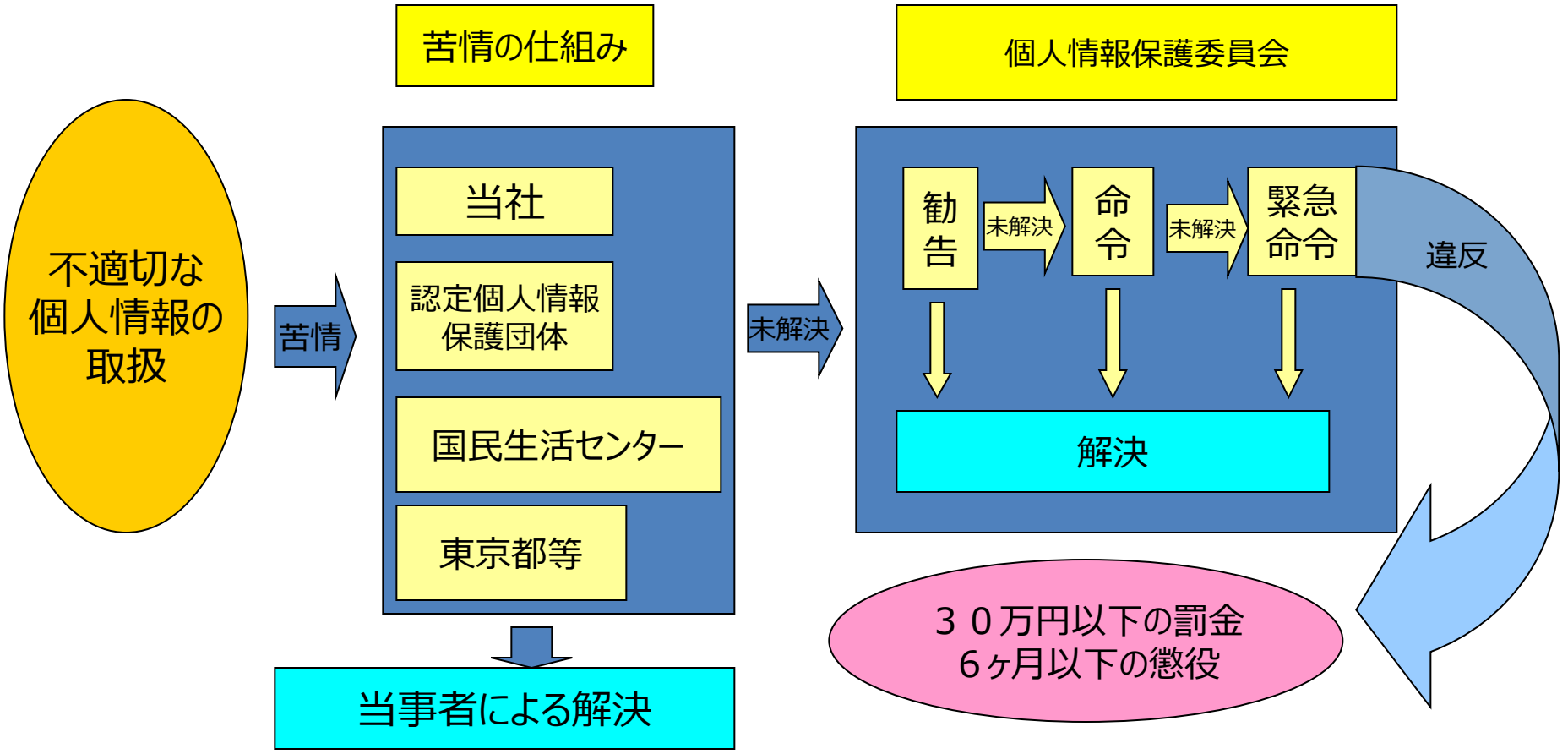
個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失、又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。

従業員の監督

①従業員の雇用時、派遣社員等の受け入れ時には
　個人情報の非開示契約（秘密保持誓約書等）を締結する。
　この契約には、雇用契約等の終了後においても非開示条項が
　一定期間有効である旨を定めること。

②定めた安全管理措置を順守させるように
　必要で適切な監督を行うこと。

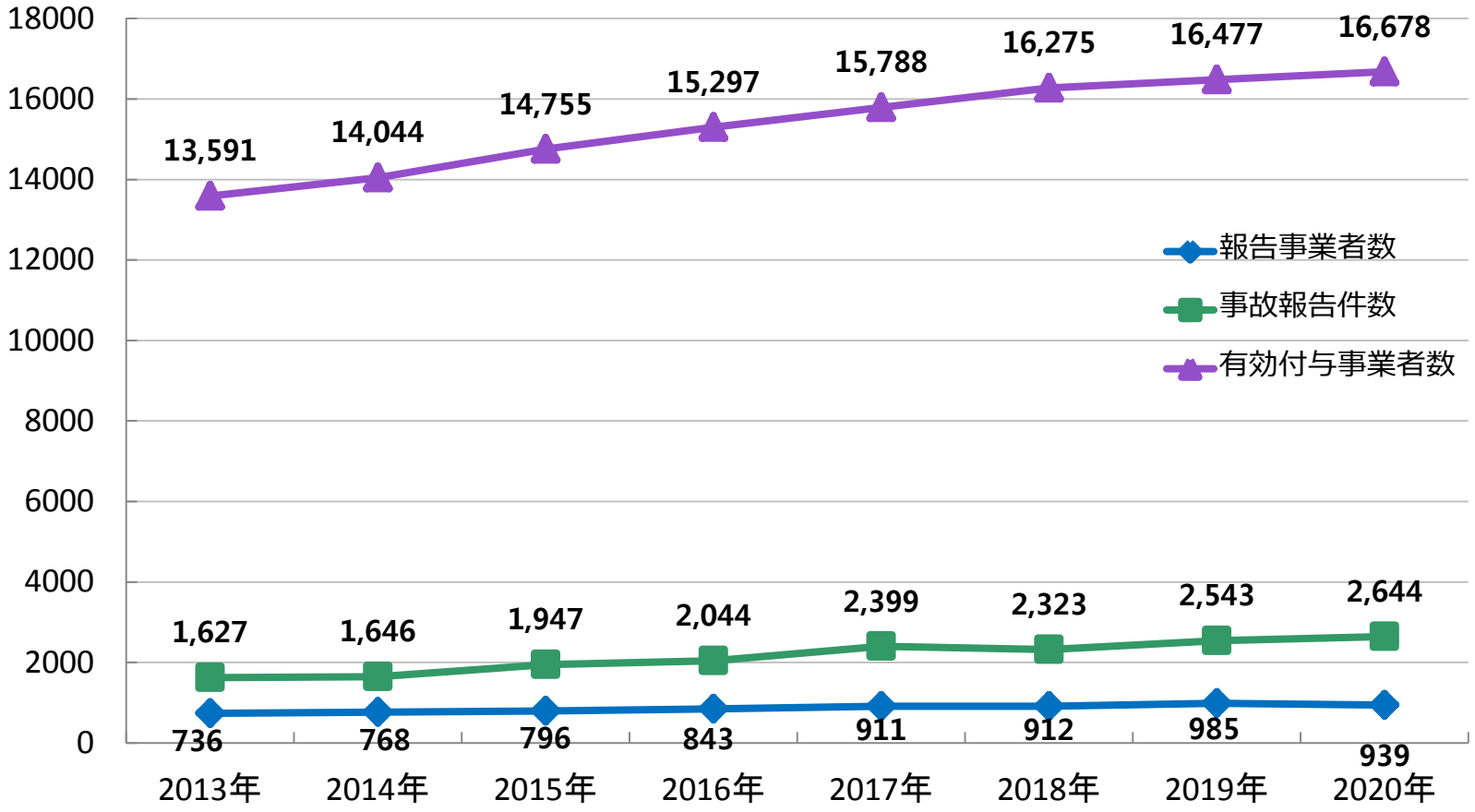
実効性担保の仕組み（罰則）



個人情報事故事例

個人情報の事故について
（JIPDEC2020年11月9日公表）

事故報告の状況

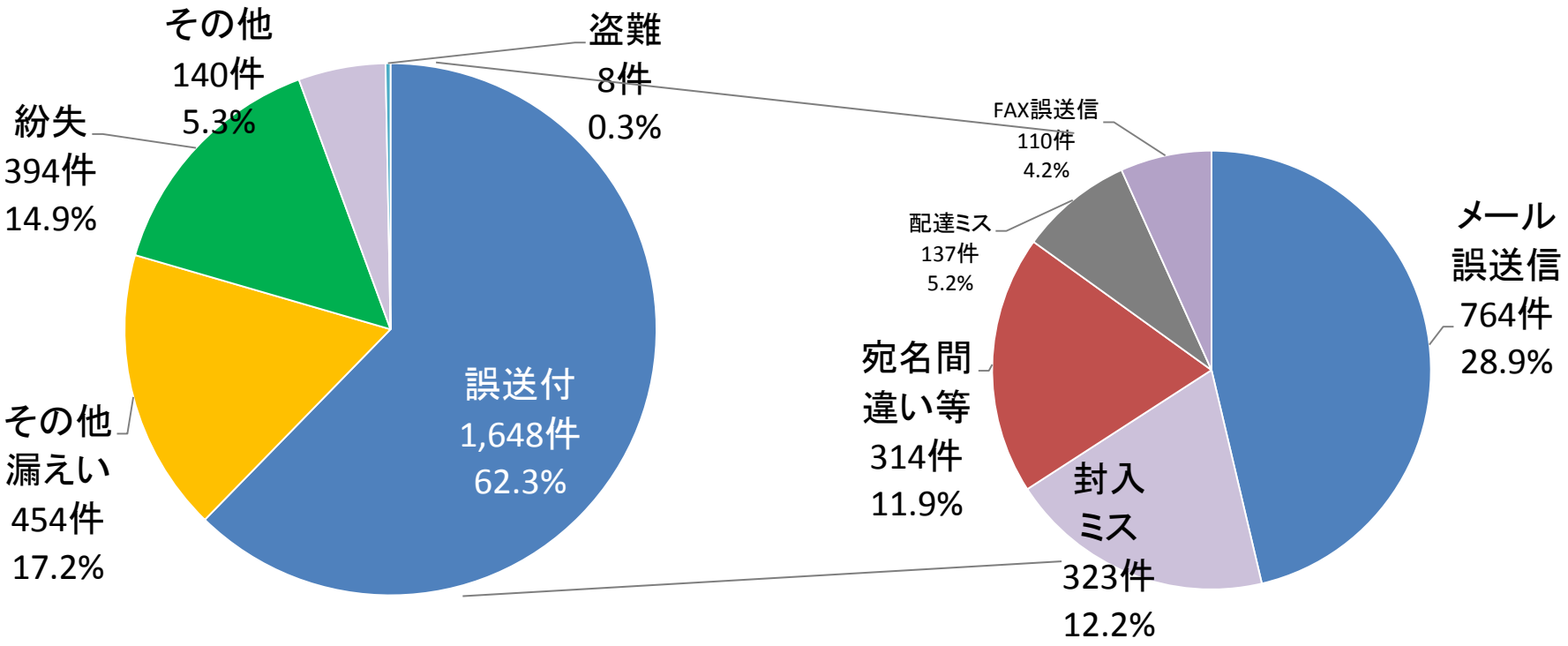


付与業者からの原因別事故報告
（JIPDEC2020年11月9日公表）

		漏えい							盗難・紛失			その他	合計
		誤送付					ｳｲﾙｽ感染	その他漏えい	盗難・紛失		紛失		
		宛名間違い	配達ミス	封入ミス	FAX	メール			車上あらし	置き引き			
2018年度	報告件数	346	0	305	108	586	1	329	5	31	478	134	2323
	割合	14.9%	0.0%	13.1%	4.6%	25.2%	0.0%	14.2%	0.2%	1.3%	20.6%	5.8%	100%
2019年度	報告件数	400	58	329	136	590	9	437	5	6	421	152	2543
	割合	15.7%	2.3%	12.9%	5.3%	23.2%	0.4%	17.2%	0.2%	0.2%	16.6%	6.0%	100%
2020年度	報告件数	314	137	323	110	764	0	454	5	3	394	140	2644
	割合	11.9%	5.2%	12.2%	4.2%	28.9%	0.0%	17.2%	0.2%	0.1%	14.9%	5.3%	100%

（注意）「宛名間違い」は、宛名書き間違い、誤登録、誤入力、渡し間違いなどである。
「配達ミス」は、配送を業とする付与事業者自らが配達した際の間違いである。
「その他の漏洩」は、システム設計上のミス、不正アクセスによる漏洩
その他ヒューマンエラーと考えられるのが含まれる。
「その他」は、誤廃棄、目的外利用、内部不正行為、同意のない提供などである。
「割合」は各媒体の「報告件数」を「合計」で割った値。
小数点以下第２位を四捨五入して出している為、
合計が100%にならないことがある。

「誤送付」の内訳
（JIPDEC2020年11月9日公表）



・メール・郵便物の宛先の確認
・添付ファイル・郵便物の中身の確認

事故の発生傾向

（JIPDEC2020年11月9日公表）

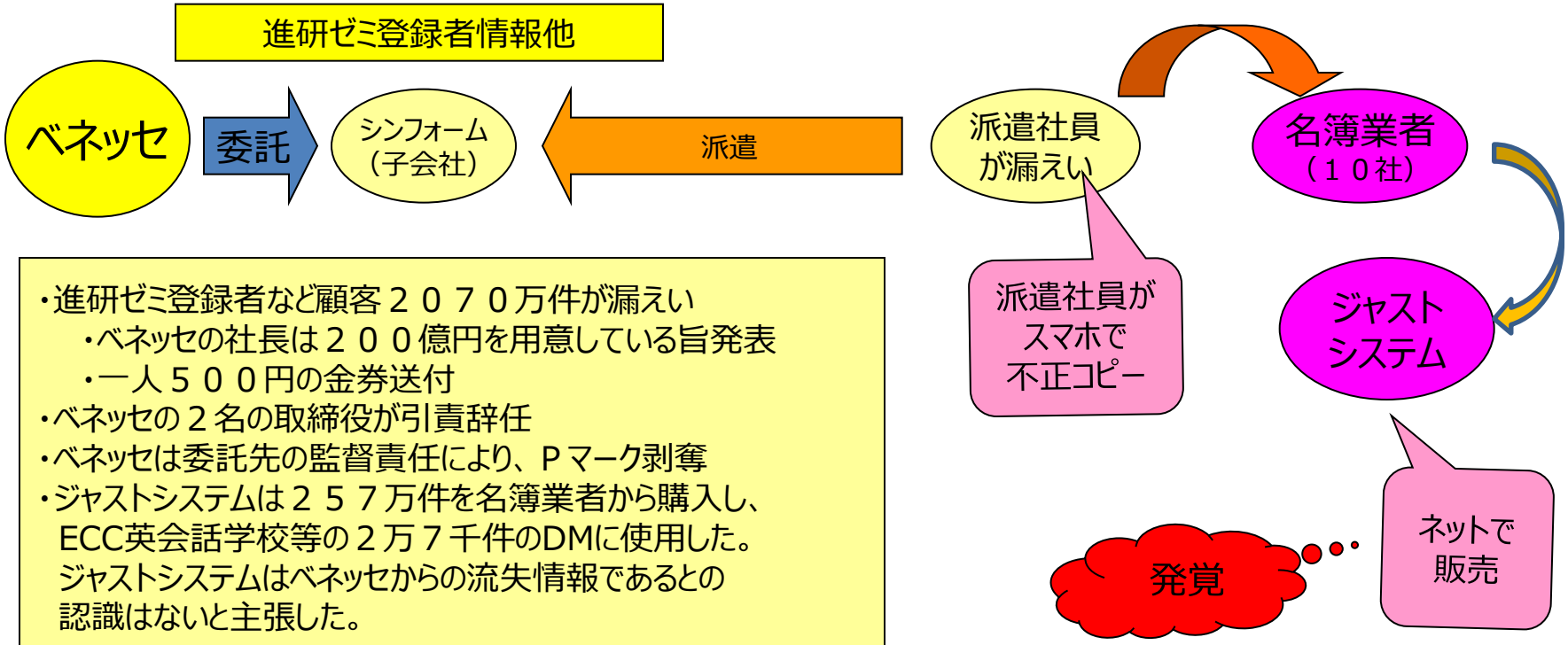
業種ごとの事故分類（イカイグループ関連業種抜粋）

	漏えい	滅失・き損・盗難等	目的外利用
01.製造・建設業	61%	**38%**	2%
03.貨物運送・倉庫・物流業	76%	24%	0%
10.BPO等業務代行業	84%	15%	1%
12.職業紹介・労働者派遣業	58%	10%	**32%**
全体	**73%**	**21%**	**6%**

・全体として「漏えい」が最も多く発生している。
　　⇒うっかりミスが多い、ミスを防ぐ手順を省略
・労働者派遣業においては「目的外利用」が多く発生している。
　　⇒間接スタッフの情報管理意識
・製造業においては「滅失・き損・盗難等」が多く発生している。
　　⇒現場でなくす・汚れる・壊れる

個別個人情報漏えい事例

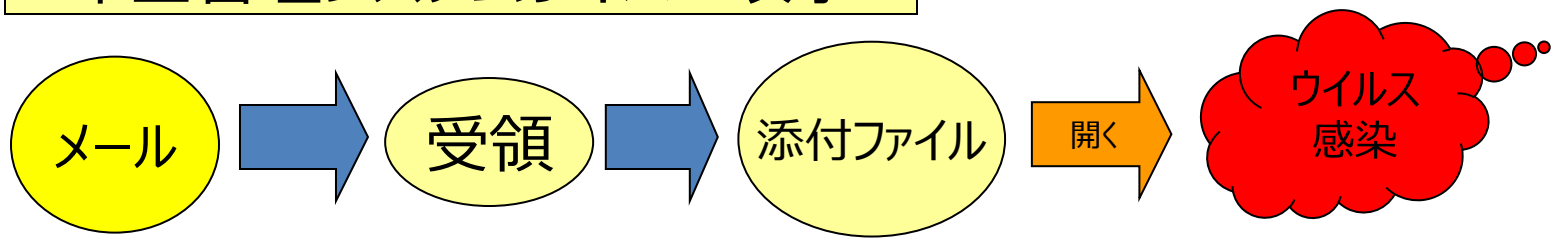
ベネッセ事件２０１４年７月発覚



・進研ゼミ登録者など顧客２０７０万件が漏えい
　・ベネッセの社長は２００億円を用意している旨発表
　・一人５００円の金券送付
・ベネッセの２名の取締役が引責辞任
・ベネッセは委託先の監督責任により、Ｐマーク剥奪
・ジャストシステムは２５７万件を名簿業者から購入し、ECC英会話学校等の２万７千件のDMに使用した。ジャストシステムはベネッセからの流失情報であるとの認識はないと主張した。
・個人情報保護法の改正で「第三者提供にかかわる記録の作成等」や「第三者提供を受ける際の確認等」に関する義務が導入された。

個別個人情報漏えい事例

年金管理システムサイバー攻撃



・2015年5月日本年金機構に大量の添付ファイル付メールが届く。
・メールのタイトルは『厚生年金基金制度の見直しについて(試案）』に関する意見」というタイトルで、
　添付ファイルが添付されていた。
・少なくとも２名の職員が添付ファイルを開く

・職員のPCは年金のデータの入ったサーバと接続されており、少なくとも10数台のPCにウイルスが感染した。
・感染したPCを通じて年金管理システムに対して不正アクセスがあり、125万件の個人情報が流出した。
　流出した情報は、氏名、住所、基礎年金番号、生年月日で、パスワードが付いていた情報は内70万件

・この事件の専用窓口には15万８千件の問い合わせが発生した。

・パスワードが設定されていない部分があった。
・年金管理システムなど重要ファイルがインターネットと接続するPCでアクセス可能になっていた。
・標的型メールのウイルスについて教育等で学ぶこと。

個別個人情報漏えい事例

三菱UFJ証券顧客情報売却事件

・2009年1月システム部の部長代理が同社の全顧客情報148万件をCD-ROMに不正コピーし、名簿屋4社に5万人の個人情報（住所、氏名、勤務先、年収、携帯電話番号）を、加えて3月に122万件の企業情報を売却したが、買い叩かれて合計わずか33万円で売却。顧客情報は98社に転売され、回収できたのは28社のみである。

・顧客からのクレームが16000件、対応に当たった従業員は延2000人、該当の顧客5万人に1万円の商品券と詫び状を送付した。
しかし、何より信用の失墜が大きく、被害総額は70億円と見込まれる。（会社は損害賠償訴訟）

・犯人が使用したIDは異動の際に削除されるはずのものがそのまま使用された。
アクセス制御されていたが犯人はアクセス権限を保持しており、チェック体制が甘かった。
金融庁から業務改善命令を受けた。

《問題点》
・社内管理者の犯行は防止するのが難しい。

《教訓》
・失墜した信用の回復には膨大なコストが必要。
・一旦流出した個人情報は回収できない。
・犯行を起しにくいチェック体制を構築する。

最近の個人情報漏えい事故事例

２０１８年５月　エースコンタクト
会員向けWebサイト「A-Web倶楽部」のWebの脆弱性を突かれて氏名、クレジットカード番号等3412件漏洩。

→

２７人分６６８万円の被害

流出データに対する
架空請求が発生した。

脆弱性対策未実施。
社内でクレジットカードの情報を保持していた。

２０１８年５月　森永乳業
健康食品通販サイトからクレジットカードの名義、番号、有効期限、セキュリティコード等が漏洩。

→

２３万件

カードの不正使用により漏洩が発覚。
漏洩の経緯などは話せないとしている。
社内でクレジットカードの情報を保持していた。

事故例から見る事故防止策

① インターネットバンキング不正使用対策

・ID、パスワード、第2パスワードを安易に入力しない。

被害額：年間1495件・３0億円

（ IPAの2018年のセキュリティ脅威の第1位）

・フィッシング対策(ニセホームページにアクセスしない)

② クレジットカード不正使用対策

・信用度の低いサイトや店舗等でのクレジットカードを使用しない

・偽造カード・本人になりすましで2016年１４０億円の被害

③ Windowsアップデート(パッチ）を最新状態にする。

④ ウイルス対策ソフトのパターンファイルを最新状態にする。

⑤ 重要情報はインターネットから切り離して取り扱う。

⑥ 私物の情報機器類の企業への持ち込み禁止

最近の標的型攻撃メール事故について

標的型攻撃メールは特定の組織や人にしか送られないために
本物のメールと思い添付ファイルを開いてしまう恐れがある。
（年金機構など官公庁、大手企業から業界団体、中小企業へ拡大する恐れがある。IPA）

① 知らない人からのメールだが、新聞社からの取材申し込み、
就職活動の問合せ、製品やサービスの問い合わせやクレーム、
アンケート調査などになっており、うっかり開いてしまう。
② 心当たりのないメールだが、議事録などの内部文書、VIP訪問に関する
情報など興味をそそられる内容で、うっかり開いてしまう。
③ 届いたことがない公的機関からの、情報セキュリティに関する注意喚起
インフルエンザ等の感染症流行情報などで、うっかり開いてしまう。
④ 組織全体への案内で、人事情報、新年度の事業方針、資料の差し替え
などで、うっかり開いてしまう。
⑤ 心当たりのない航空券の予約確認や荷物の配送通知で、
うっかり開いてしまう。

標的型攻撃メールの見分け方

【おかしいと感じたメールは開けない、添付ファイルを開けない】

① 差出人のメールアドレスがフリーメールアドレスになっていたり、差出人のメールアドレスと本文のメールアドレスが異なっている。

② 不要なIDやパスワードなどの入力を要求するメールになっている。

③ 実在する名称を一部に含むURLが記載されている。

④ メール本文の日本語の言い回しが不自然である。
日本語では使用されていない漢字が使用されている。（中国語など）

⑤ 組織名や電話番号が存在しないものになっている。

⑥ 添付ファイルが添付されている。

（IPA資料より）

ランサムウエア（身代金要求型ウイルス）

感染させた端末を勝手に暗号化することにより使用出来なくし、元に戻すことと引き換えに「身代金」を要求するウイルス

・身に覚えのないメールを開き、添付ファイルを開けることによって感染する。
　感染した端末だけではなく、共有サーバーや外付けHDDに保存されているファイルも暗号化される。

・発生件数：2016年1月～12月　65,400件（日本）　（セキュリティ脅威第2位）

【対策】

・不自然なメール添付や、記載されたURLには“触らない”
・OSやソフトの“更新プログラムを速やかに適用”
・セキュリティソフトは常に“最新に”
・大切なデータは、複数の場所でこまめに“バックアップ”
・身代金を要求されても“支払わない”

以上です。

ご清聴ありがとうございました。