個人情報保護委員会による近時の指導・助言等の事例で考えるコンプライアンスのポイント

2025年 6月19日

牛島総合法律事務所
弁護士　影島広泰
hiroyasu.kageshima@ushijima-law.gr.jp
03-5511-3233

お問い合わせ先

牛島総合法律事務所　弁護士　影島広泰

03-5511-3233
hiroyasu.kageshima@ushijima-law.gr.jp

東京都千代田区永田町2-11-1
　山王パークタワー14階

2003.10	弁護士登録（第56期）牛島総合法律事務所入所
2013.1	牛島総合法律事務所パートナー
2015.5	情報化推進国民会議 本委員（～2017.3）
2015.7	情報化推進国民会議 マイナンバー検討特別委員会委員（～2015.12）
2017.4	JIPDECプライバシーマーク付与適格性審査会委員

【個人情報の取扱い・情報管理に関する案件】
- **パーソナルデータを利用したビジネス構築のための法的スキームの助言**
- **内外企業がクロスボーダーにデータを移転する際の法的助言（GDPR・CCPA・アジア各国法）**

【システム・ソフトウェア開発に関する案件】
- **金融機関、流通、サービス業の各システム開発の中止に伴う訴訟・紛争**
- **システム開発プロジェクト遂行中のコスト増、品質問題、プロジェクト中断に関する交渉のアドバイス**

【著作等】
- **「個人情報関連法令スピードチェック」（商事法務）**
- **「法律家・法務担当者のためのIT技術用語辞典＜第2版＞」（商事法務）**
- **「座談会　システム開発取引はなぜ紛争が絶えないのか」（NBL1115～1117号）ほか多数**

【その他】
- **Thomson Reuters 2024年「ALB Asia Super 50 TMT Lawyers」に選出**
- **The Legal 500 Asia Pacific 2025のTMT（Technology, Media & Telecommunications）部門(independent local firms)におけるLeading partners**

目次

1. 個人情報保護委員会による監督（対 個人情報取扱事業者）

■ 監視・監督の実績（個人情報保護委員会「令和6年度年次報告」）

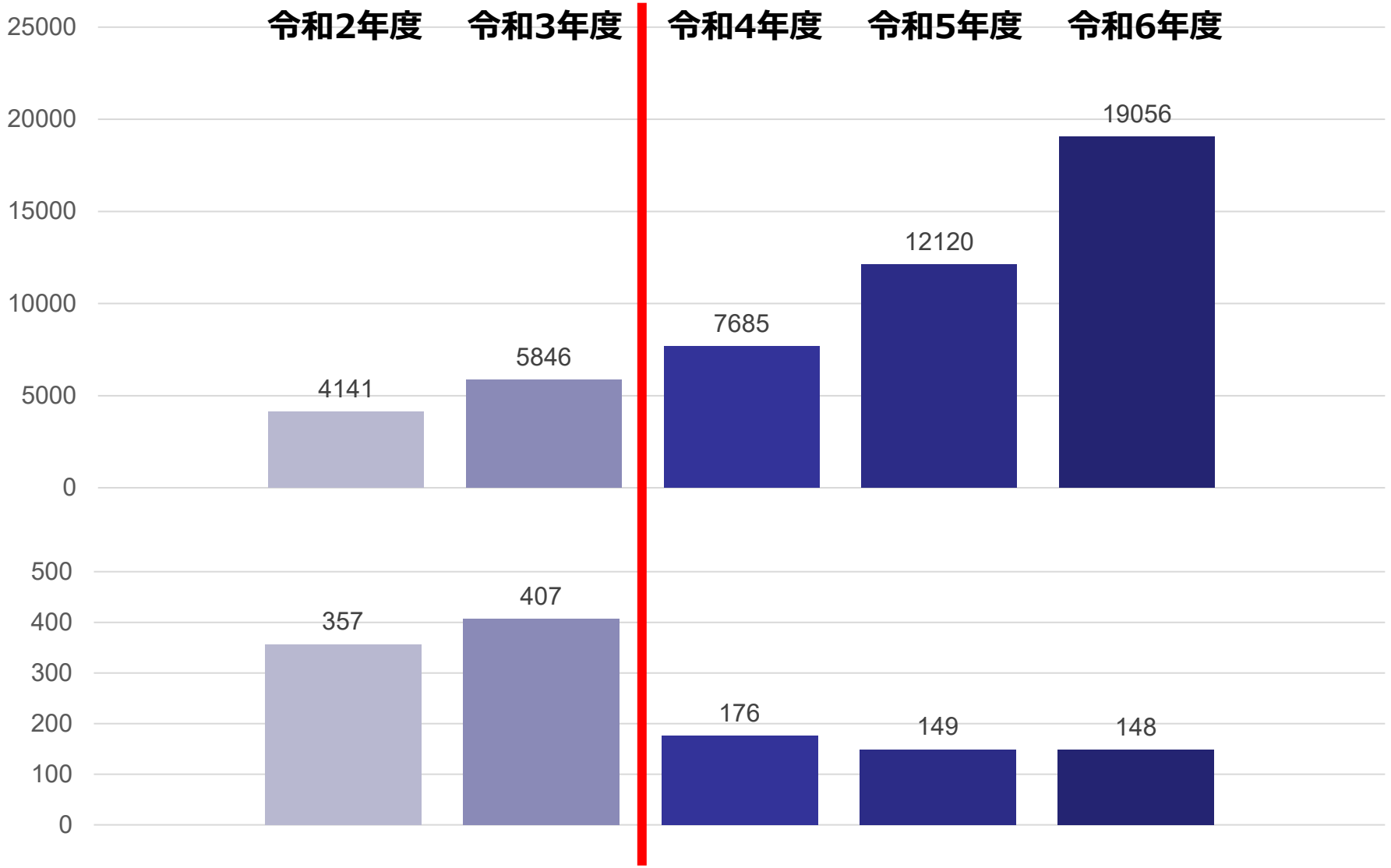
	合計		個人情報保護委員会		委任先省庁	
相談ダイヤルの苦情受付件数	7,358	(6,941)				
漏えい等報告の処理件数※	19,056	(12,120)	14,198	(7,075)	4,858	(5,045)
（うち域外適用分）	36	(13)				
任意の報告等	1,436					
報告徴収	148	(149)	67	(73)	81	(76)
立入検査	47	(31)	2	(0)	45	(31)
指導及び助言	395	(333)				
勧告	1	(3)				
命令	0	(0)				

（　）内は令和5年度

※社会保険／人事労務業務支援システムの事業者がランサムウェアの攻撃を受けた事件の報告2,845件が含まれる

1. 個人情報保護委員会による監督（対 個人情報取扱事業者）

- **漏えい等事案に関する報告の処理件数**

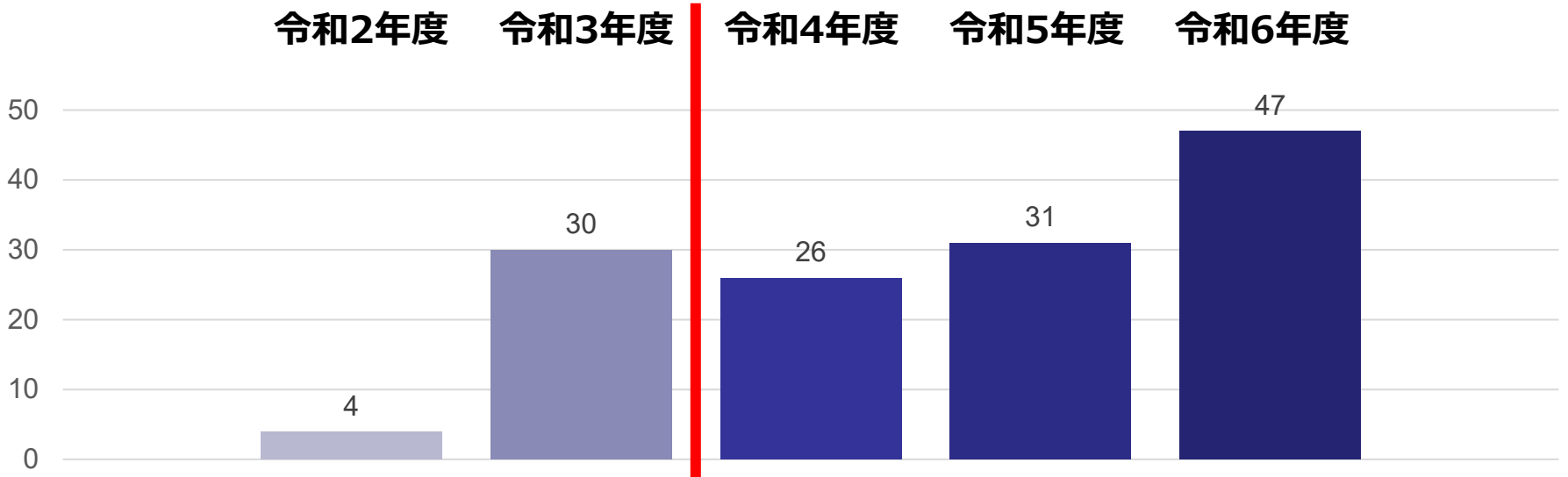


- **報告徴収**

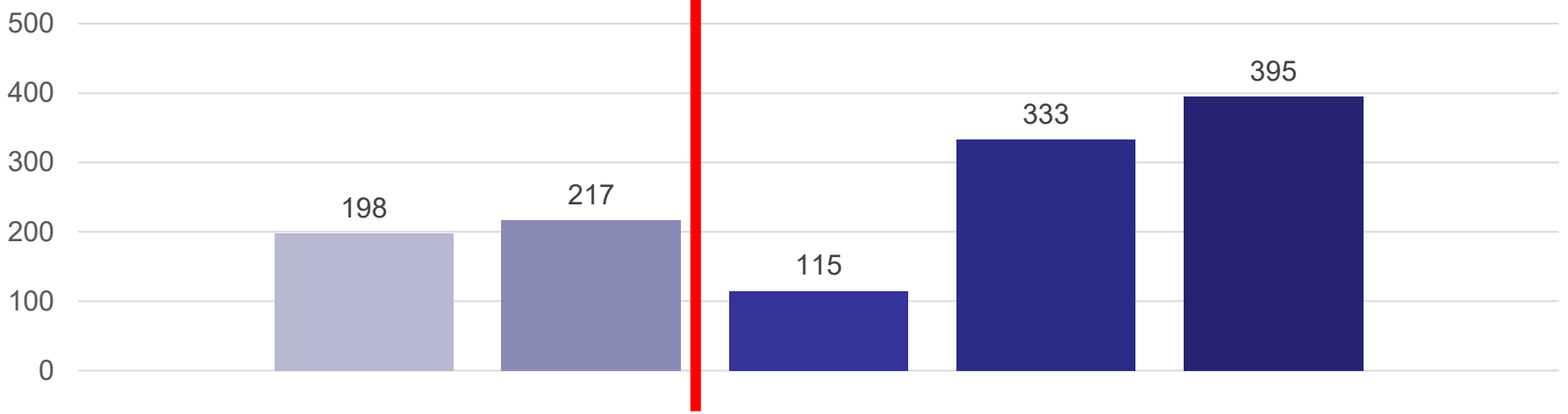
令和2年改正（漏えい等報告の義務化）施行

1. 個人情報保護委員会による監督（対 個人情報取扱事業者）

■ 立入検査



■ 指導・助言

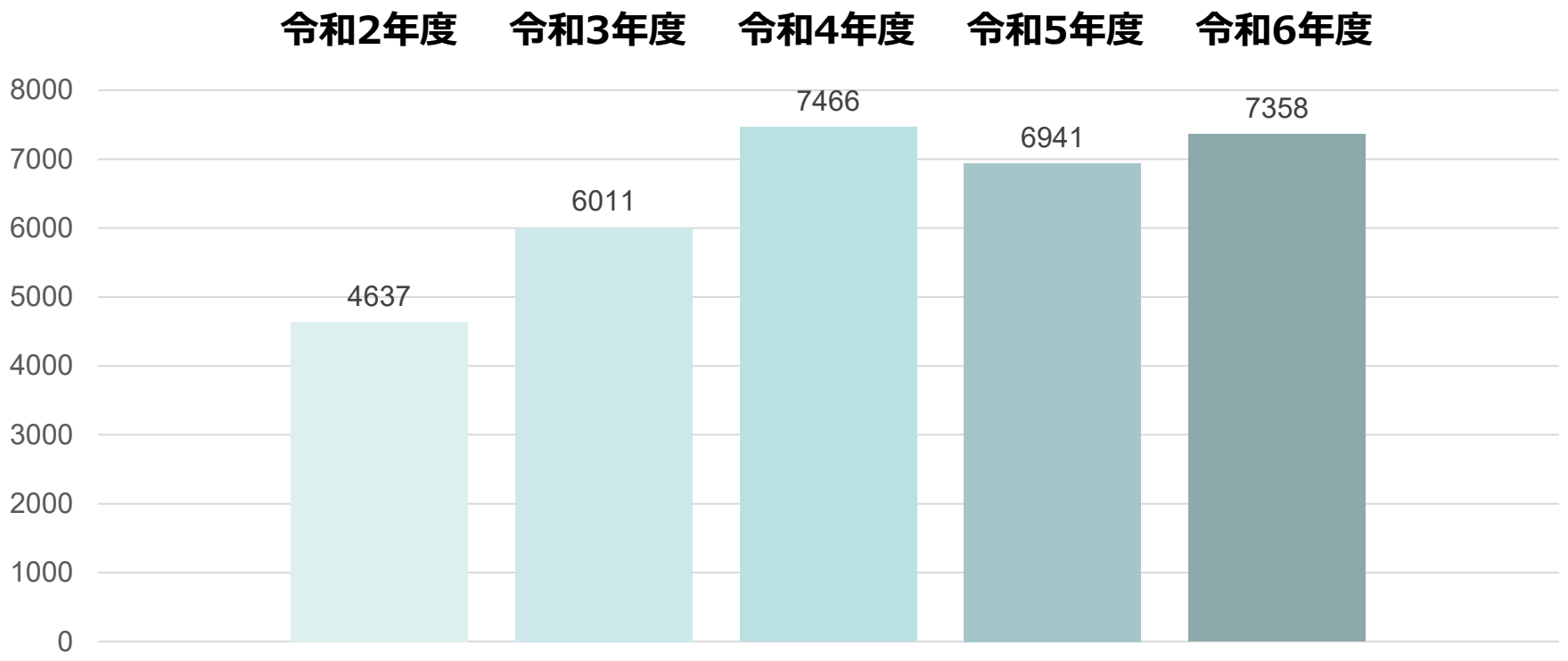


令和2年改正（漏えい等報告の義務化）施行

2. 個人情報保護法相談ダイヤル（民間部門）における受付件数

■ 相談ダイヤルにおける「苦情」の受付件数

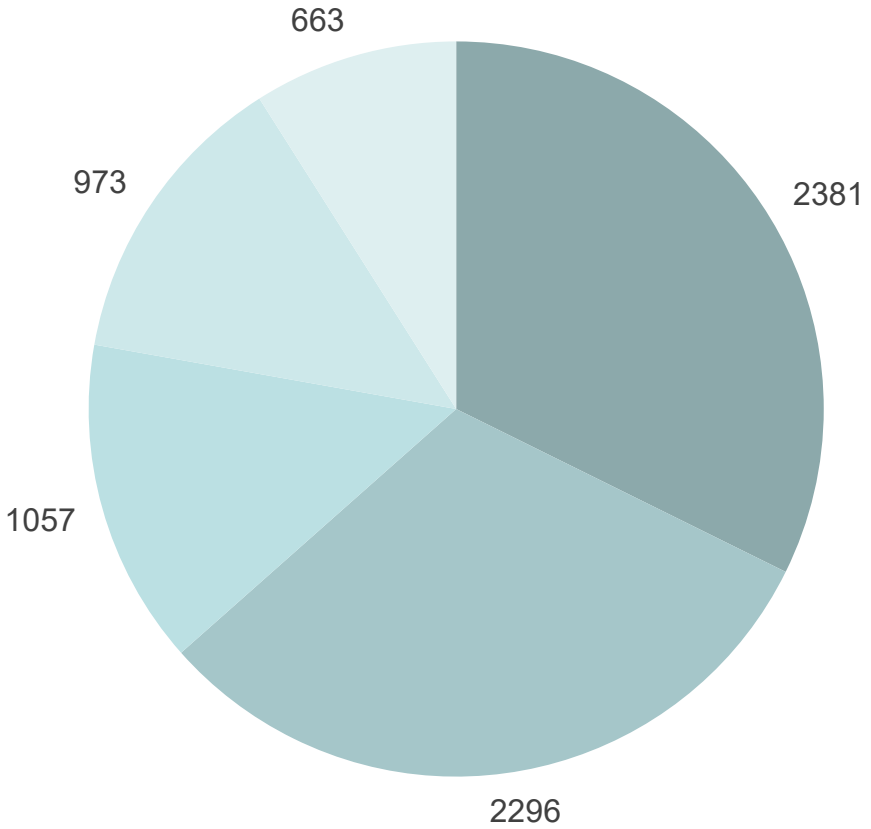
- ➢ **年間7,000件程度**で高止まり



2. 個人情報保護法相談ダイヤル（民間部門）における受付件数

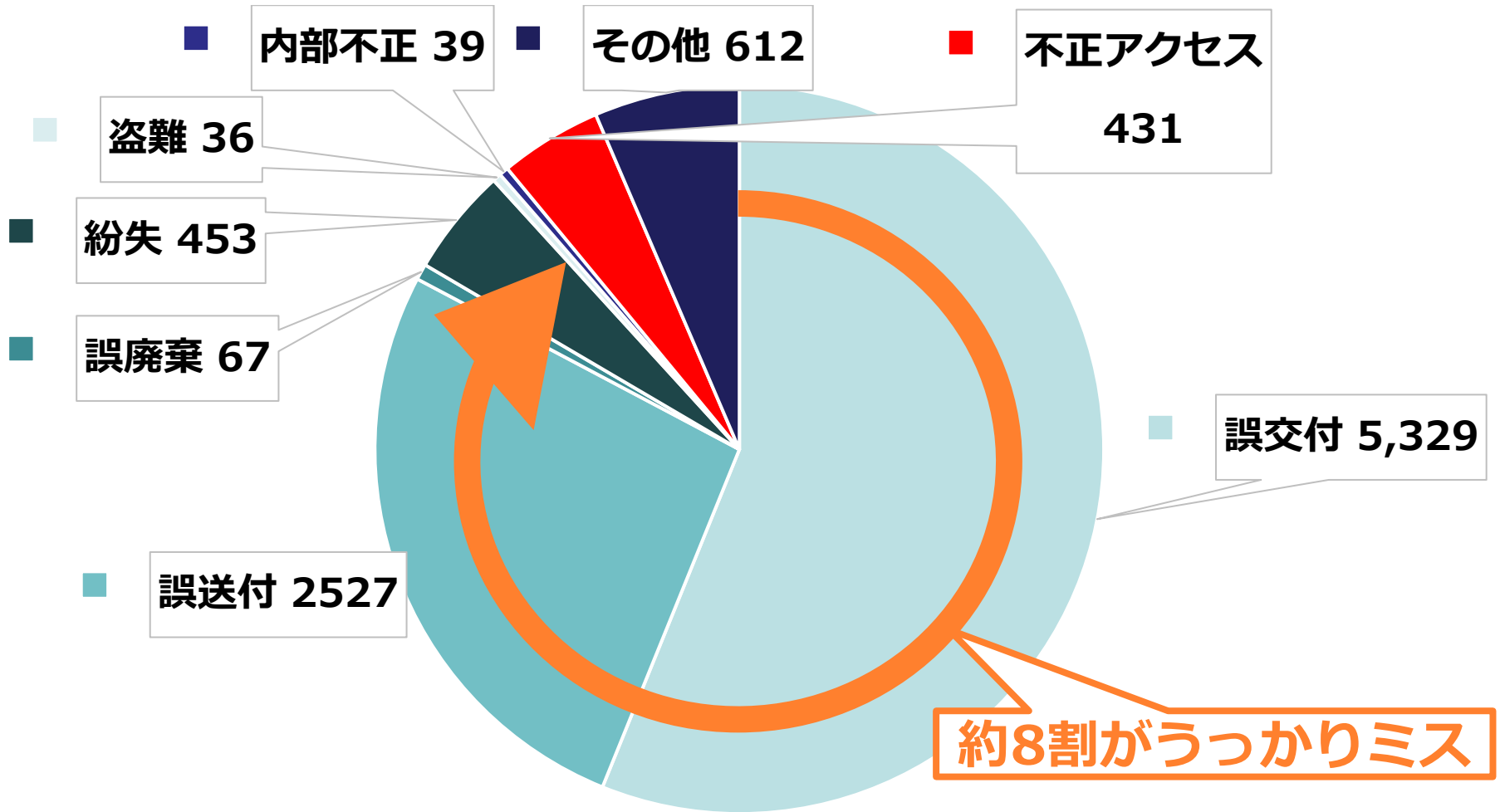
「苦情」の問い合わせ内容上位5項目

- 第三者提供
- 利用目的
- 開示等
- 漏えい等の報告等
- 正確性の確保



3. 漏えい等の原因

■ 漏えい等の原因（報告者からの漏えい）（令和6年度個人情報保護委員会年次報告書）



「病院や薬局における要配慮個人情報を含む書類の誤交付等のほか、フィッシング詐欺によるものなどが多かった」

目次

Case 1：クラウドサーバの誤設定

Case 1: 車両の位置情報等の漏えいに関する事案（指導・2023.7.12）

自動車会社が、関連会社に車両利用者へのサービスに関する個人データの取扱いを委託していたところ、クラウド環境の誤設定により車両利用者に対するサービスのためのサーバが公開状態に置かれ、車両から収集した約230万人分の車載器ID、車台番号、車両の位置情報等が、約10年間にわたり、外部から閲覧できる状態にあり、個人データの漏えいが発生したおそれが生じた

本人の数	約230万人
個人データの項目	車載器ID、車台番号、車両の位置情報等
その他	外部から閲覧できる状態だった期間が約10年間。 委託元への行政指導のみ公表。委託先への行政指導の有無は不明。

Case 1：クラウドサーバの誤設定

■ 個情委が指摘した「個人情報保護法上の問題点」

問題点	①サーバのクラウド環境設定を行う従業員に対する個人情報に関する**研修内容が不十分**であったため、**車載機ID、車台番号及び位置情報等が個人情報として認識されていなかった** ②**委託先のサーバのクラウド環境**におけるアクセス制御の観点からの**監査・点検を実施しておらず**、**委託先の個人データの取扱い状況を適切に把握していなかった**。

■ 個情委による指導（概要）

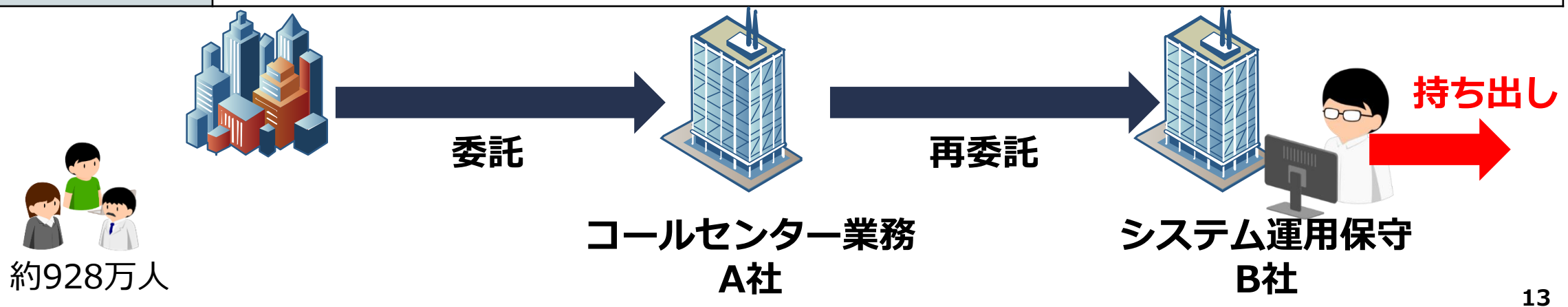
指導1	23条及び25条並びに通則ガイドラインに基づき、下記の通り個人データの安全管理のために必要かつ適切な措置を講ずること • 従業者に個人データを取り扱わせるにあたって、個人データの取扱いを**周知徹底**するとともに適切な**教育**を行うこと（人的安全管理措置）。 • 本来アクセスすべきでない者が本件サーバにアクセスすることがないよう、**適切なアクセス制御**を実施すること（技術的安全管理措置）。 • 委託先に対して、自らが講ずべき安全管理措置と同等の措置が講じられるよう、必要かつ適切な監督を行うこと（**委託先の監督**）。
指導2	事業者が策定した以下の**再発防止策を確実に実施**すること ① 従業者に対し、クラウド環境設定における個人データ取扱いのルールに関する**社内教育**を徹底する、 ② **クラウド設定を監視するシステムを導入**し、設定状況を継続的に監視するとともに、**技術的に公開設定ができないようにする**、 ③ **委託先に対して**、**クラウド環境設定**に関する個人データの取扱い状況を**定期的に監査**する等

Case 2: 再委託先の内部不正

Case 2: 委託先（再委託先）の従業者による不正な持ち出し（勧告・2024.1.24）

多数の民間事業者及び地方公共団体等からコールセンター業務の委託を受けていた事業者が、コールセンター業務で用いるシステムの保守運用を委託していたところ、委託先（再委託先）でシステム保守運用業務に従事していた者が、委託元の顧客又は住民等に関する個人データ等合計約928万人分を不正に持ち出した事案

本人の数	約928万人
個人データの項目	氏名、住所、電話番号等
その他（勧告に至った理由）	• **2013年から2023年まで**の間という長期間にわたって反復的に行われていた • **2022年に委託元から個人データの漏えいに関する調査依頼があり、B社と共に調査したが、当時十分な調査が実施できておらず、不正な持ち出しによる漏えいを是正できなかった。**十分な調査が行われなかった経緯及び原因を未だに明らかにできておらず、個情委への報告もできていない



Case 2: 再委託先の内部不正

■ 個情委がA社（委託先）に指摘した「個人情報保護法上の問題点」

問題点	**①組織的安全管理措置（取扱状況の把握及び安全管理措置の見直し）** 過去調査の経緯等からして、**個人データ等の取扱状況の把握や安全管理措置の見直しが不十分** **②人的安全管理措置（従業者の教育）** **年１回定期的な研修**を行っていたが、委託先の監督が不十分だったことからして、適切な情報セキュリティの確保・個人データ等の適正な取扱いの重要性に関する**認識を醸成するところまでには到底至っていなかった** **③委託先の監督** **・個人データ等の取扱いに関する取り決めがなされていなかった** ・委託先における個人データ等の取扱状況の把握が不十分

Case 2: 再委託先の内部不正

■ 個情委がB社（再委託先）に指摘した「個人情報保護法上の問題点」

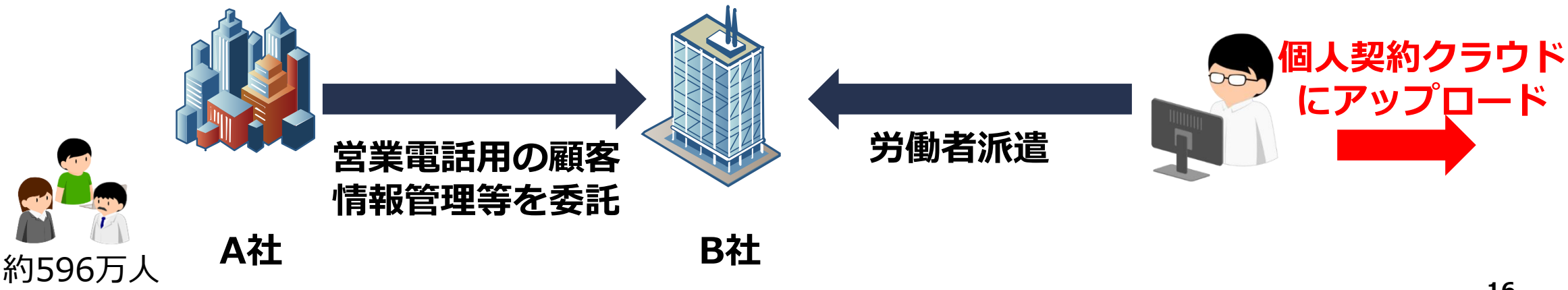
問題点	**①組織的安全管理措置（個人データの取扱いに係る規律に従った運用）** **規程に従わないUSBメモリの利用**が行われており、不正な持ち出しを発見することもできなかった。 社内規程ではアクセス記録等の分析・監視が必要であるとされていたが、実際にはされていなかった **②組織的安全管理措置（個人データの取扱状況の把握及び安全管理措置の見直し）** 監査：**アクセスログの分析・監視が実施されていなかった** 過去調査：不正な持ち出しを確認できなかった **③人的安全管理措置（従業者の教育）** 年1回研修等の取り組みを行っていたが、不十分 **④物理的安全管理措置（個人データを取り扱う区域の管理）** **入退室の管理や監視カメラの設置を行うにとどまり、USBメモリ等の外部記録媒体の持ち込みについてチェック及び制限を行わず** **⑤技術的安全管理措置** システム管理者アカウントのアクセス制御御が適切になされていなかった **システム管理者のアカウントの共用**によりアクセス者の識別と認証が適切に行われていなかった 情報システムの使用に伴う漏えい等の防止のための措置が不十分 ・**保守端末等への個人データ等のダウンロードが可能** ・私物 USB メモリの接続制限、検知もできず

Case 3: 委託先の派遣社員による漏えいのおそれ

Case 3: 委託先の派遣社員による漏えいのおそれ（指導・2024.2.15）

A社が、B社に対し、電話営業用の顧客情報管理を含む業務を委託していたところ、B社の派遣社員であったXが、顧客情報管理のために業務上使用するPCから、個人契約するクラウドサービスに合計約596万人分の個人データをクラウドサービスへアップロードすることにより、外部に流出させ、漏えいのおそれが発生

本人の数	約596万人
個人データの項目	氏名・住所・電話番号・メールアドレス・生年月日・回線 ID 等
その他	・「**大量の顧客個人データを取り扱っているシステム**である」 ・Xは、自ら作成したツールのソースコードをノウハウとして持ち出したかったものであり、当該個人データについて外部の第三者への提供は行っていないと説明している



Case 3: 委託先の派遣社員による漏えいのおそれ

■ 個情委がA社（委託元）に指摘した「個人情報保護法上の問題点」

問題点	**①物理的安全管理措置（個人データを取り扱う区域の管理）** 情報管理規程で、顧客の個人データを取り扱う場合はインターネット及びメールの利用が制限された専用のPCを利用することとし、それらを利用するPCとは取扱区域を分けて管理するルールであったが、本件PCはかかる制限がされていなかった **②技術的安全管理措置（情報システムの使用に伴う漏えい等の防止）** ネットワーク監視を行っており、本件も発生当日に検知し、ネットワークからの切断を行っており、一定の処置を講じていたといえる。しかし、**外部インターネットへのアクセス規制については、一部のサイトを接続不可と定めるブラックリスト方式で運用されており、ファイル共有サービス等のクラウドサービスも含めて、業務上不必要なサイトには接続できない設定とはしていなかった** **③組織的安全管理措置（個人データの取扱いに係る規律に従った運用）** 運用ルールの運用確保のための取組では、日次で行わせる自主点検の結果を月次で確認することで、確実に徹底されていることを確認することとしていたが、虚偽の申告に対応できていない **④委託先の監督の不備（委託先における個人データの取扱状況の把握）** 自ら又は外部の主体による監査を実施することはなく、**B社の自主点検に任せ**、月次で結果報告を受け取るだけであった。A社がB社に行わせていた自主点検は、**従業者にデータを削除したことを自己申告させ、他の従業者がデスクトップ上に不要なデータが残っていないかどうかを確認するという簡易な方法**にとどまっており、本件のように**意図的にデータ削除せず、自身しか把握していないデスクトップ以外の場所に保存した場合は、発見され得ないことは容易に想定可能である**から、点検項目や点検の方法が不十分であった

Case 3: 委託先の派遣社員による漏えいのおそれ

■ 個情委がB社（委託先）に指摘した「個人情報保護法上の問題点」

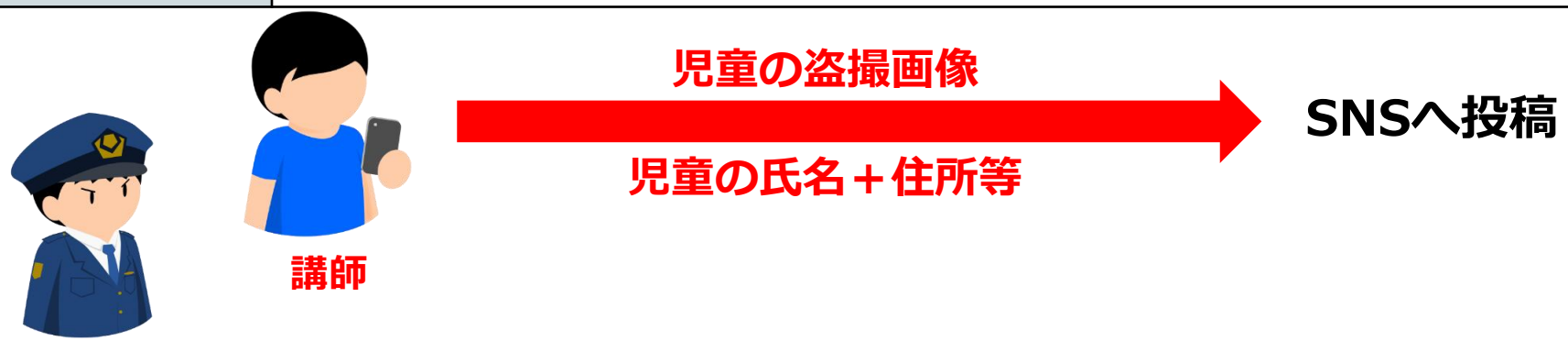
問題点	**①組織的安全管理措置（取扱状況の把握及び安全管理措置の見直し）** **自主点検は実施していたものの、他部署等による監査は実施していない** **②人的安全管理措置（従業者の教育）** 派遣社員であるＸを含む従業者に、情報セキュリティ遵守のため機密保持に関する**誓約書を提出**させ、また、**情報セキュリティ研修の実施**を行っていたものの、情報セキュリティ研修では、**一般的な情報セキュリティの考え方及び法の令和２年改正部分を紹介するにとどまっており、大量の顧客データを管理する事業者における研修としては十分とはいえない**。

Case 4: 従業員がSNSに個人データを投稿した事例

Case 4: 学習塾の講師が児童の写真・氏名等を投稿（指導・2024.2.29）

学習塾を運営する事業者において、従業員Xが、児童の写真及び動画とともに、事業者が管理する在校児童の個人データを検索して閲覧し、私用スマホに入力して記録し、６人分の個人データをXの SNSアカウントに掲載して漏えいさせた

本人の数	6人
個人データの項目	児童の氏名、年齢、生年月日、住所、所属小学校名、電話番号（＋盗撮画像も投稿）
その他	（報道）Xは個人情報データベース盗用・提供罪で懲役2年、保護観察付き執行猶予5年。事業者も書類送検。 ・「**こどもの個人データ**については、こどもの「安全」を守る等の観点から、**特に取扱いに注意が必要**であり、組織的、人的、物理的及び技術的という多角的な観点からリスクを検討し、必要かつ適切な安全管理措置を講ずる必要がある。」



Case 4: 従業員がSNSに個人データを投稿した事例

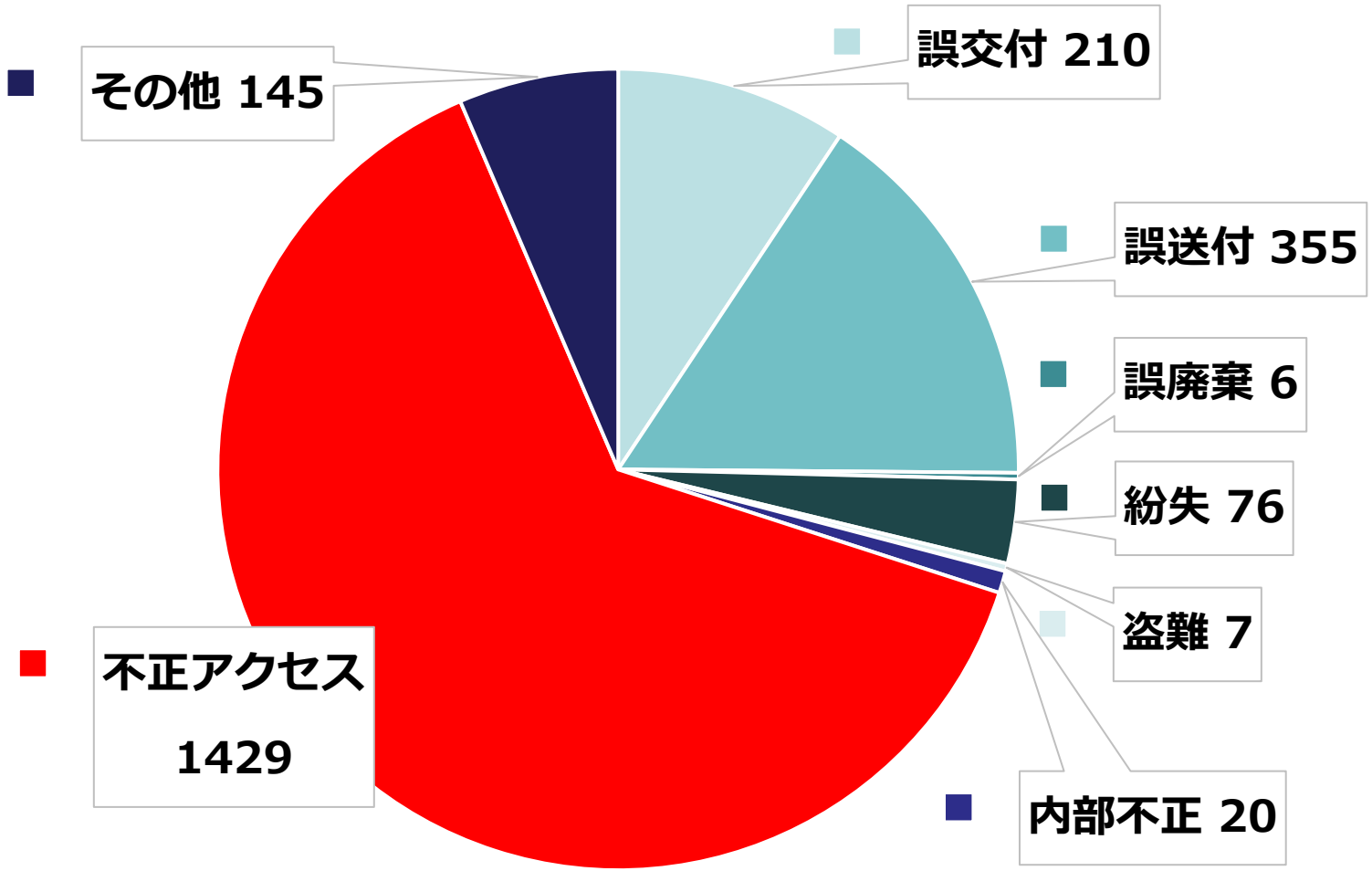
■ 個情委が指摘した「個人情報保護法上の問題点」

問題点	**①組織体制の整備及び漏えい等事案に対応する体制の整備** 大量の児童の個人データを保有及び管理しているにもかかわらず、人的なリソース不足を理由に**コンプライアンス及びリスク管理に関する部署を設置しておらず**、また、責任者の設置はしていたものの、漏えい等事案が発生した場合に**当委員会に報告するための体制が機能していなかった**。そのため、本件漏えい事態が**発覚してから約２か月後に速報を提出**した **② 取扱状況の把握及び安全管理措置の見直し** 責任者である塾長（会社全体を統括する者）が定期的に**内部監査**を実施していたとのことであるが、監査の項目は、研修の実施状況を確認するにとどまるものであり、**個人データの取扱状況については確認していなかった**

Case 5: SaaSベンダがランサムウェアの攻撃を受けたケース

■ 漏えい等の原因（委託先からの漏えい・令和6年度）

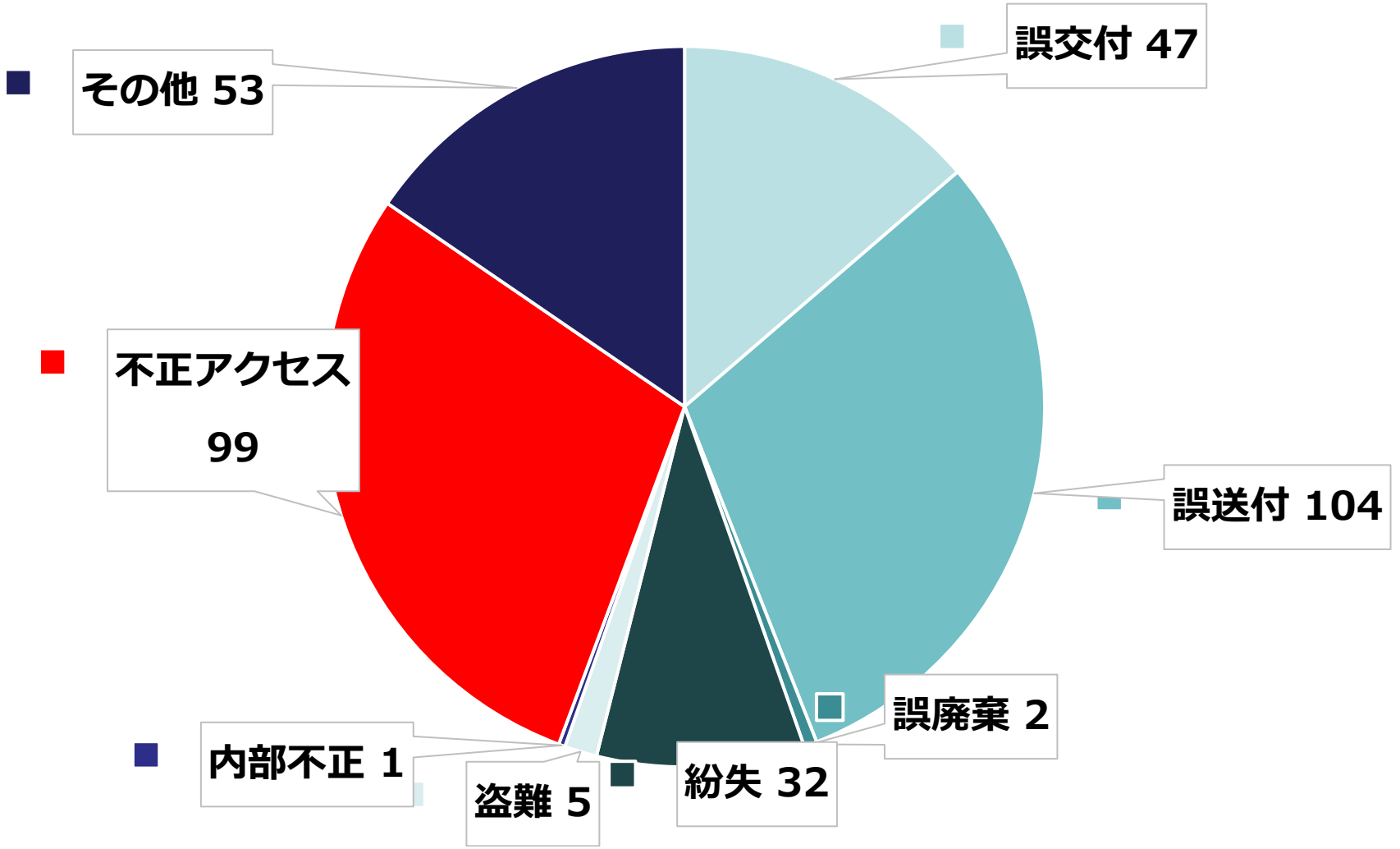
- ➢ 社会保険／人事労務業務支援システムのランサムウェア事案の報告2,845件が含まれる



Case 5: SaaSベンダがランサムウェアの攻撃を受けたケース

■ 漏えい等の原因（委託先からの漏えい・令和5年度）

- ➢ やはり不正アクセスの割合が多い



Case 5: SaaSベンダがランサムウェアの攻撃を受けたケース

Case 5: SaaSベンダがランサムウェアの被害（指導・2024.3.25）

社会保険/人事労務業務支援システムを、社会保険労務士の事務所等のユーザに対し、SaaS環境においてサービス提供していたところ、サーバが不正アクセスを受け、ランサムウェアにより、システム上で管理されていた個人データが暗号化され、漏えい等のおそれが発生

本人の数	社労士事務所：2,754事業所、管理事業所：約57万事業所 本件システムで管理する本人数：最大約2,242万人
個人データの項目	社労士の顧客である企業等の従業員等の氏名、生年月日、性別、住所、基礎年金番号、雇用保険被保険者番号及びマイナンバー等（取り扱っていたデータ）
その他	・「保守用 ID については、個人データの取得を防止するための技術的な措置は講じられていないことから、個人データの提供に該当し、**委託に基づき個人データを取り扱っている**ものと認められる。」

Case 5: SaaSベンダがランサムウェアの攻撃を受けたケース

■ 個情委がSaaSベンダに指摘した「個人情報保護法上の問題点」

問題点	**①技術的安全管理措置** **ユーザのパスワードルールが脆弱**であったこと、また、**管理者権限のパスワードも脆弱であり類推可能**であったことから、アクセス者の識別と認証に問題があった。 **ソフトウェアのセキュリティ更新が適切に行われておらず**、深刻な脆弱性が残存されていた **ログの保管、管理及び監視が適切に実施されておらず、不正アクセスを迅速に検知するには至らなかった**

■ 個情委が委託先（社労士）に指摘した「個人情報保護法上の問題点」

問題点	ユーザの多くは、個人データの取扱いの委託を行っていたとの認識が薄く、委託先の監督が結果的に不十分となっていた可能性がある

■ 個情委が委託元（クライアント）に指摘した「個人情報保護法上の問題点」

問題点	クライアントの多くは、社労士事務所に対して個人データの取扱いの委託及びSaaSベンダに対する再委託を行っていたとの認識が薄く、委託先等への監督が結果的に不十分となっていた可能性がある

■ マイナンバー法の問題点

問題点	**高度な暗号化による秘匿化がされた状態で保管されていた** →番号法の規定による**指導は行わない**こととする

Case 6：グループ会社間での個人データの不適切な共有

Case 6: 電力グループ会社間での個人データの共有（指導・2024.6.27）

一般送配電事業者であるA社及び関係小売電気事業者であるB社の顧客の個人情報についてグループ会社であるHD社・C社が閲覧できる状態になっており、HD社・C社の従業者の中には、システム画面上表示されていた顧客の個人データを、業務上の目的及び業務外の目的のため利用していた者がいた

＜接点情報システム＞

管理・運営：B社

共同利用　：A社

アクセス権限がB社の親会社であるHD社及びHD社の子会社であるC社に**誤って設定**され、顧客の個人データを、HD社及びC社から閲覧できる状態となっていた

＜要請応対システム＞

管理・運営：B社

共同利用　：A社

B社には「顧客検索機能」における**自社の顧客情報**及び「要請事項と対応結果の登録機能」へのアクセス権限**のみが設定されているはずであったが**、「顧客検索機能」における**A社の顧客情報へのアクセス権限も誤って設定されたままになっていた**。

本来、当該システムを利用しないはずのHD社及びC社にも両機能へのアクセス権限が誤って設定されたままになっていた。

Case 6：グループ会社間での個人データの不適切な共有

■ 個情委が指摘した「個人情報保護法上の問題点」

問題点	**①個人情報の適正な取得（20条１項）** HD及びC社は、電気事業法の規律と趣旨を知り又は容易に知ることができる立場にあったことを鑑みると、当該２社による顧客の個人データの閲覧及び利用は、社会通念上適正とは認められない行為といえ、「適正性を欠く」個人情報の取得行為であると認められ、「偽りその他不正の手段」による個人情報の取得に該当 **②安全管理措置（23条）** **技術的安全管理措置** **適切なアクセス制御**を実施できていなかった。 **組織的安全管理措置** 接点情報システム及び要請応対システムに関する個人データの取扱状況について、**定期的な点検や内部監査を実施していなかった** **人的安全管理措置** A社は**一般的な内容の研修を行うにとどまっていた**。 A社の従業者の中には、HD社及びC社がアクセス可能な状態となっていることを知りながら、適切な対応を講じなかった従業者も存在したことからすると、個人データの適正な取扱いの重要性に関する認識を醸成するには不十分なものであり、人的安全管理措置に不備が認められる。

Case 7: 個人情報の不適正取得

Case 7: 個人情報を不適正に取得していた事例（勧告・2025.1.29）

① 建設現場に掲示されている法定標識や公共工事の入札・落札情報検索サイト等の**公開情報から、建設会社等の従業者である者の個人情報を入手**

② ①で入手した情報を基に、当該建設会社等に**架電し**、架空の事業者名を名乗った上で、「貴社の××工事の現場監督である〇〇さんから弊社に電話で問合せをいただき、折り返しの電話が欲しいとのことだった」、「貴社の工事現場の近くで別の工事をすることとなったので、貴社の現場監督である〇〇さんに連絡したいことがある」等の**虚偽の事実を伝え、当該建設会社等の電話応答者を誘導し、当該現場監督者等の携帯電話番号を取得**

このような手段により取得した個人情報を**データベース化**し、本来の業務である**職業紹介や転職支援に利用**するなどしていた

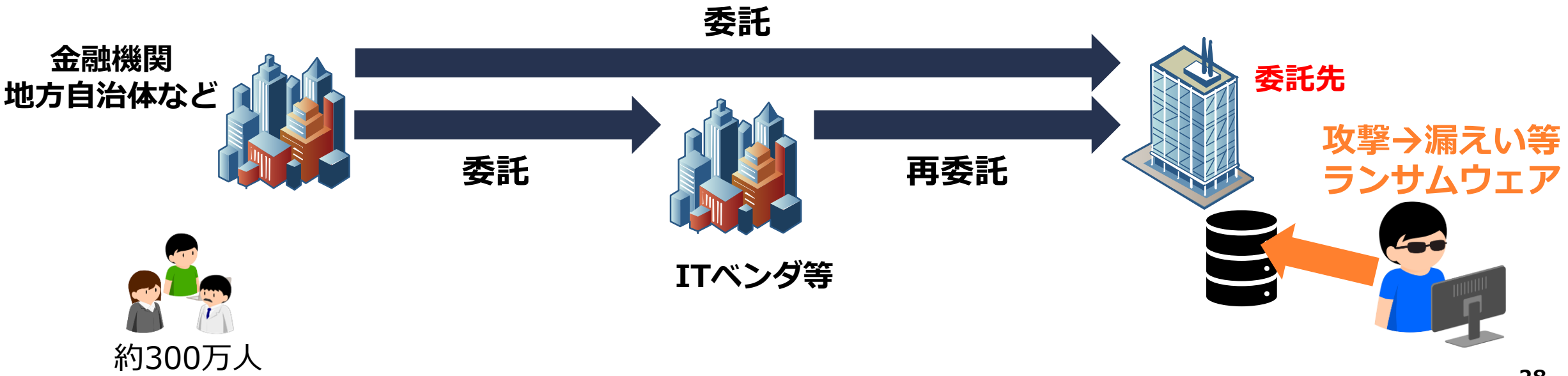
本人の数	1万人以上
個人データの項目	氏名・携帯電話番号
その他	少なくとも1年9か月間

Case 8: 委託先がランサムウェアの攻撃を受けたケース

Case 8: 委託先がランサムウェアの被害（指導・2025.3.19）

金融機関や地方公共団体等から委託を受けて、様々な通知書の印刷・発送業務を実施していた事業者が、第三者から不正アクセスを受け、通知書の内容及び発送先に関する個人データの漏えい及び毀損が発生。窃取されたファイルがダークウェブ上に公開された。

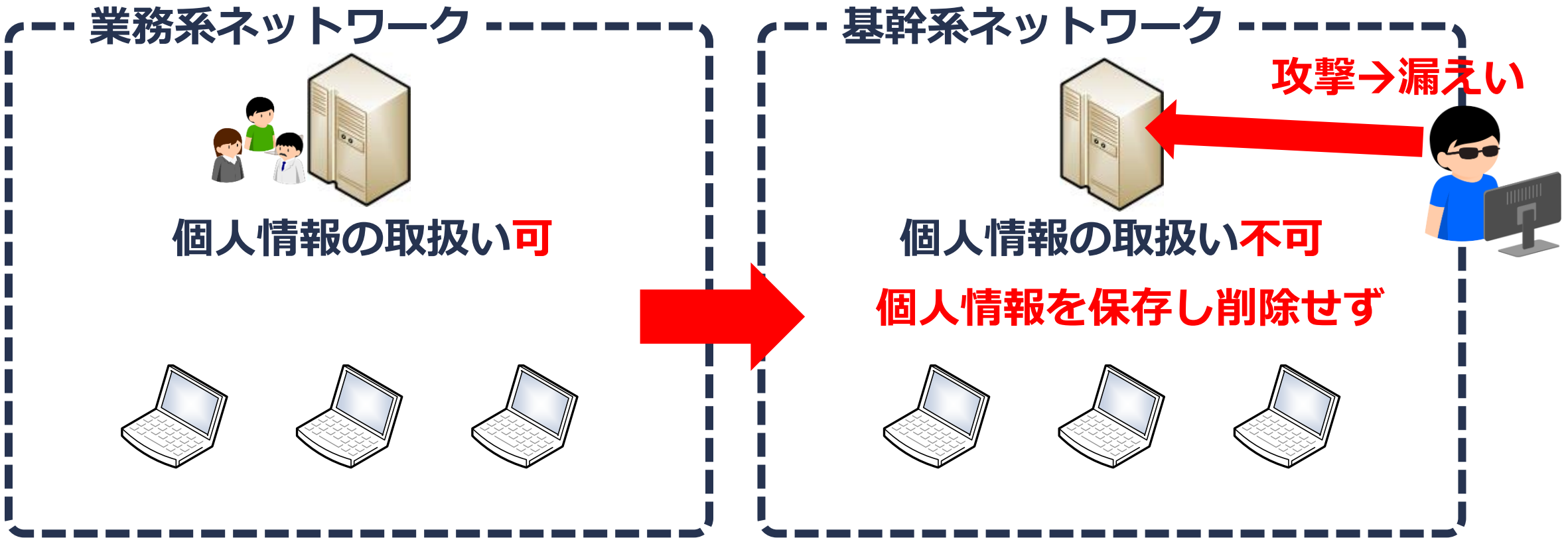
本人の数	3,076,477人（うち、要配慮個人情報13,150人） 委託元は100団体ほど
個人データの項目	氏名、住所のほか、確定拠出年金やローン残高等、税額情報、健康保険組合の要配慮個人情報等
その他	VPN 機器のログを適切に取得していなかったため、フォレンジック調査によっても真因は分かっていない



Case 8: 委託先がランサムウェアの攻撃を受けたケース

■ 流出の原因（豊田市のリリース）

1. A社が、委託業務において取り扱う個人情報データを「豊田市個人情報取扱い及び情報セキュリティに関する特記」の規定に反して**市の承諾なく複製し**、かつ、**社内規定の原則に反して本来は個人情報の取扱いをしないサーバ及びPCにデータを保管し**、**業務終了後も消去することなく残していました**。



Case 8: 委託先がランサムウェアの攻撃を受けたケース

■ 個情委が指摘した「個人情報保護法上の問題点」

問題点	**①外部からの不正アクセス等の防止（技術的安全管理措置）** **VPN 機器のアップデートを実施しておらず**、VPN 機器の認証に関連する脆弱性について対応が未了 基幹系ネットワークに関する管理者アカウントについて平成29年２月から同じパスワードを使用していた。そして、実際の**パスワードは推測がある程度容易な英小文字のみ11桁**であった。多要素認証未導入。 **②組織体制の整備（組織的安全管理措置）** 保管ルールという重要な業務ルールについて明文化なし。実際、**保管ルールが守られていなかった** VPN機器が約３年間アップデートされておらず、パスワードポリシーも桁数や文字についての制限がなく、更新日数についての規定は存在したものの遵守されておらず、約７年間、管理者アカウントのパスワード更新なし →**経営層を含む管理者が適切に状況を把握できていなかった**こと、また、個人データの取扱いに関する**責任分担や役割の明確化が不十分**であったことに起因する **③個人データの取扱いに係る規律に従った運用（組織的安全管理措置）** 個人データの保管場所について規律に沿った運用が実施されていなかった。**ログ取得が不十分**であった **④取扱状況の把握及び安全管理措置の見直し（組織的安全管理措置）** 定期的な監査や点検が十分に実施できていなかった **⑤従業者の教育（人的安全管理措置）** 定期的に一般的な情報セキュリティ等に関する研修を行っていたが、保管ルールを明文化することなく、日常業務における暗黙のルールとして、委託元からの個人データ等の取扱いを行っていた。そのため、**保管ルールは従業者が常時確認できる状態ではなく、同ルールを周知しているといえる状態ではなかった。**

Case 9: 代理店・出向者と情報管理

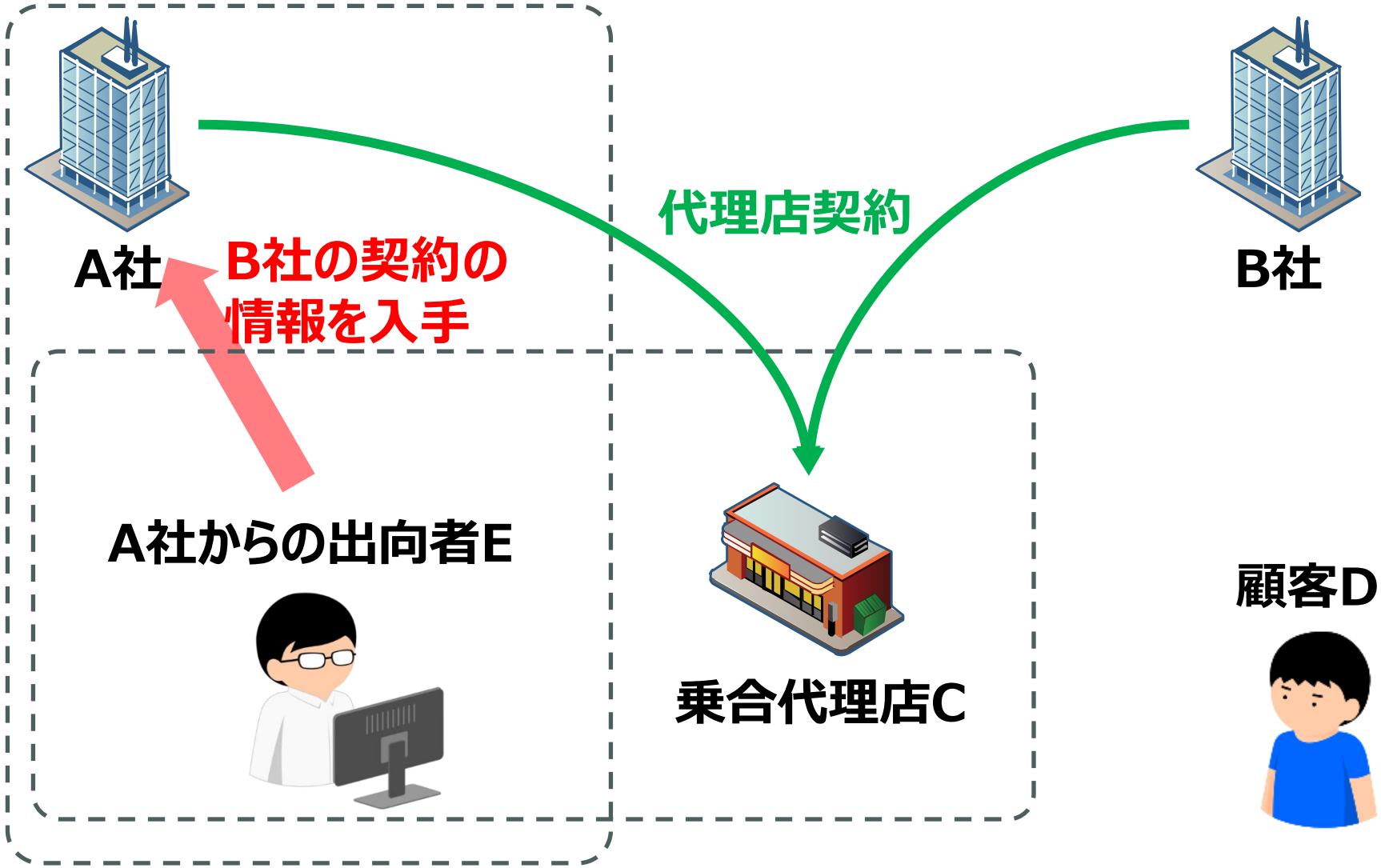
Case 9: 損保会社の代理店事案・出向者事案（指導・2025.4.30）

代理店事案：乗合代理店が、損保会社から保険契約の締結等の業務を委託されることに伴って取扱いを委託されていた保険契約者の個人データを、本人の同意なく、他の損害保険会社に提供

出向者事案：損保会社から代理店に出向している従業者が、出向先の保険代理店が管理する他の損害保険会社の保険契約者に関する個人データ等を、出向先保険代理店に無断で、かつ、本人の同意を得ることなく、出向元の損保会社にメール等により送付

本人の数	代理店事案：各社1,004,861人～221,144人、出向者事案：各社83,546人～39,290人
個人データの項目	契約者氏名、証券番号、保険料、契約した損害保険会社名、保険期間等
その他	• ディーラー等における保険販売状況のデータが、当該代理店に乗り合っている損害保険会社に対し、共有される慣習が存在した • 保険料収入の拡大のため、他社保険契約に係る情報や代理店内におけるシェアに関する情報の提供等により、少しでも自社の保険契約獲得に貢献することができれば、出向元から高い評価を受けられるかもしれないとの期待感を持つ者も少なからずいたものと推察されている

Case 9: 代理店・出向者と情報管理



Case 9: 代理店・出向者と情報管理

■ 代理店事案：個情委が指摘した「個人情報保護法上の問題点」

問題点	**①保険代理店：第三者提供の制限（27条１項）違反** **②損害保険会社：適正取得（20条１項）違反** **③損害保険会社：安全管理措置及び委託先の監督の不備** **組織的安全管理措置** **・営業部門（第1線）**：業務実態に即した情報管理の在り方に関する理解が十分ではなかった **・コンプライアンス部門・リスク管理部門（第２線）**：業務実態に即したリスクの把握・管理の状況をモニタリングし、牽制することが十分にできていなかった。**第１線の報告を基に情報管理に関する対応を講ずるにとどまっており、独立したリスクの特定・評価を十分に行う態勢となっていなかった** **・内部監査部門（第３線）**：問題認識が不足 **人的安全管理措置** **長年の慣習により行われてきた保険契約者に関する個人データの取扱いが、個人情報保護法の規定に違反する行為であると気付き是正する程度には至っておらず、研修内容の十分性に疑問を呈さざるを得ない** **委託先の監督**

Case 9: 代理店・出向者と情報管理

■ 出向者事案：個情委が指摘した「個人情報保護法上の問題点」

問題点	**①保険代理店：安全管理措置（23条）の不備** 保険代理店が**意図的に提供したものではないから**、保険代理店にとっては、個人データの**漏えいに該当** **②損害保険会社：適正取得（20条１項）違反** 出向元損害保険会社においても、少なくとも一部は、当該**持ち出し行為により得られた情報であることを知り、又は容易に知ることができるにもかかわらず、出向者から当該個人情報を取得した**ものといえる **③損害保険会社：安全管理措置及び委託先の監督の不備** **組織的安全管理措置・人的安全管理措置** 代理店事案と同じ **委託先の監督** 自社の一部の出向者により、保険代理店の了承を得ずに他社の保険契約者に関する個人情報が送付される事象が発生していたところでもあり、自社が保険代理店に委託している個人データの取扱いの状況について、委託先である保険代理店において、漏えい等の事象が存在していないかを確認し、必要に応じて委託の内容等を見直し、定期的な監査等を実施する等、保険契約者の個人データが適切に取り扱われるよう、保険代理店に対して監督を実施するべきであった。

目次

1. まとめ

■ 統計から

① **年間7,000件もの「苦情」あり**（第1位：第三者提供、第2位：利用目的）

② **漏えい等は「うっかりミス」が約8割**

■ 指導・勧告事例から

① **クラウドの誤設定**

② **社内研修の不十分さ**

③ **内部不正（故意犯）への対応**

- アクセスログの分析・監視
- USBメモリの持込みチェック
- 自己申告による確認

④ **個情委への報告の遅滞**

⑤ **委託先のランサムウェア被害**

- 委託終了後の消去の確認
- 暗号化の重要性

⑥ **慣例的に行われてきた情報共有の再確認**

2. 年次報告書の指摘を踏まえた、目下の留意点

■ サイバーセキュリティ（令和6年度年次報告書）

不正アクセスによる漏えい等の原因

① VPN機器の脆弱性やECサイトを構築するためのアプリケーション等の**脆弱性が公開され対応方法がリリースされていたにもかかわらず、事業者が放置**していたこと

② **ID・パスワードが容易に推測されやすいもの**とされていたこと

③ **設定ミス**によりデータベースへのアクセス制御が不適切な状態になっていたこと

など、安全管理措置に不備があったケースが多く見られた

■ 「指導」に至ったもの

- 26条1項に基づく**報告が著しく遅滞**したもの
- **公開済みの**ウェブサイトやネットワークの**脆弱性への対応を怠り不正アクセスを受けた**ことにより個人データの漏えい等を生じさせた場合等基本的な安全管理措置に不備があると認められるもの

3. 不備事項として指摘されているもの（行政機関等）

■ 個人情報保護法に基づき計画的に行われた実地調査等の結果

➢ 各調査等項目において不備事項が認められた割合（国：12、地方公共団体44）

検査項目	国の行政機関等	地方公共団体等
規程の整備状況	33%(4)	48%(21)
組織体制の整備状況	8%(1)	32%(14)
漏えい等事案等発生時等の対応体制	8%(1)	25%(11)
教育研修	**58%(7)**	**93%(41)**
監査・点検	**58%(7)**	**82%(36)**
委託及び再委託	**75%(9)**	**64%(28)**
書類の保管及び廃棄	42%(5)	36%(16)
漏えい等の防止及び外部からの不正アクセスの防止	8%(1)	7%(3)
電子媒体の管理及び使用	50%(6)	**55%(24)**
アカウント及びアクセス権の管理	33%(4)	**57%(25)**
端末及びサーバの管理	25%(3)	43%(19)
ログの分析	**67%(8)**	**89%(39)**
その他	17%(2)	11%(5)