

個人情報保護に係る主要課題に関する海外・国内動向調査

概要資料

令和5年11月15日

株式会社日本総合研究所
リサーチ・コンサルティング部門
融合戦略グループ

※概要資料の内容、意見などは個人情報保護委員会の公式見解を示すものではありません。

1. 国内における漏えい等事案の推移/近年の傾向

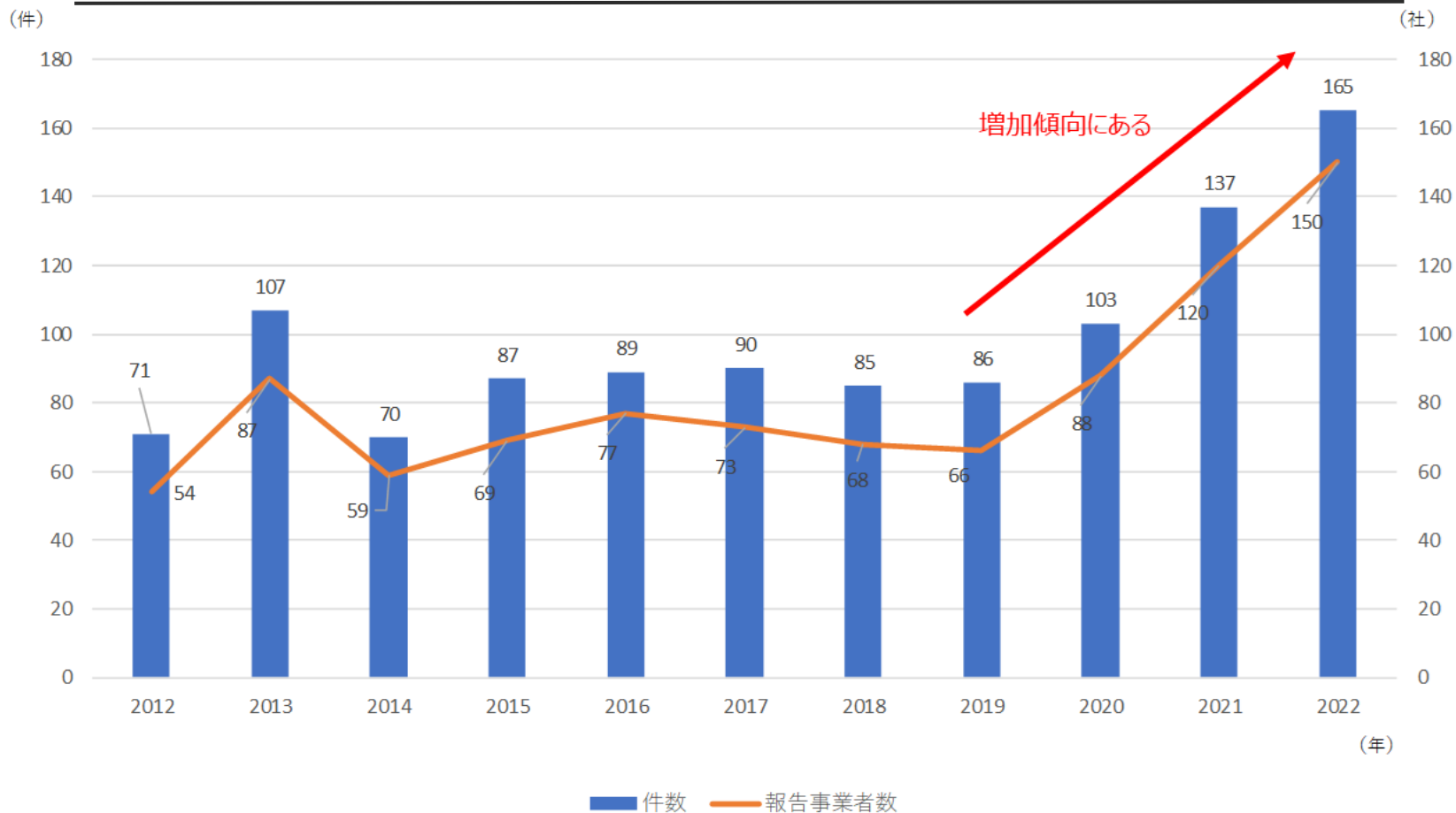
【調査結果の要旨・所感】

- 個人情報保護委員会が公表している漏えい等事案の報告件数等も踏まえると、ここ数年の漏えい等事案の発生件数は全体として増加傾向にあると考えられる。
- 上記に比例して、漏えい等事案に対する社会の関心も高まっていると考えられる。
- 漏えい等の発生経路は、かつては紙媒体が多くを占めていたが、近年はインターネット・電子メール等の電子媒体が多くを占めるに至っている。
- 漏えい等の発生原因も、かつては紛失・置忘れによるものが多くを占めていたが、2014年以降、不正アクセスを原因とする漏えい等の件数及び割合が増加している。

参考資料(1) 国内における漏えい等事案の推移/近年の傾向 —上場企業とその子会社における個人情報の漏えい等の公表件数—

- 上場企業とその子会社における個人情報の漏えい・紛失事故公表件数は、2020年から毎年件数及び社数が増加傾向にある。

上場企業とその子会社における個人情報の漏えい・紛失事故公表件数遷移（2012年～2022年）

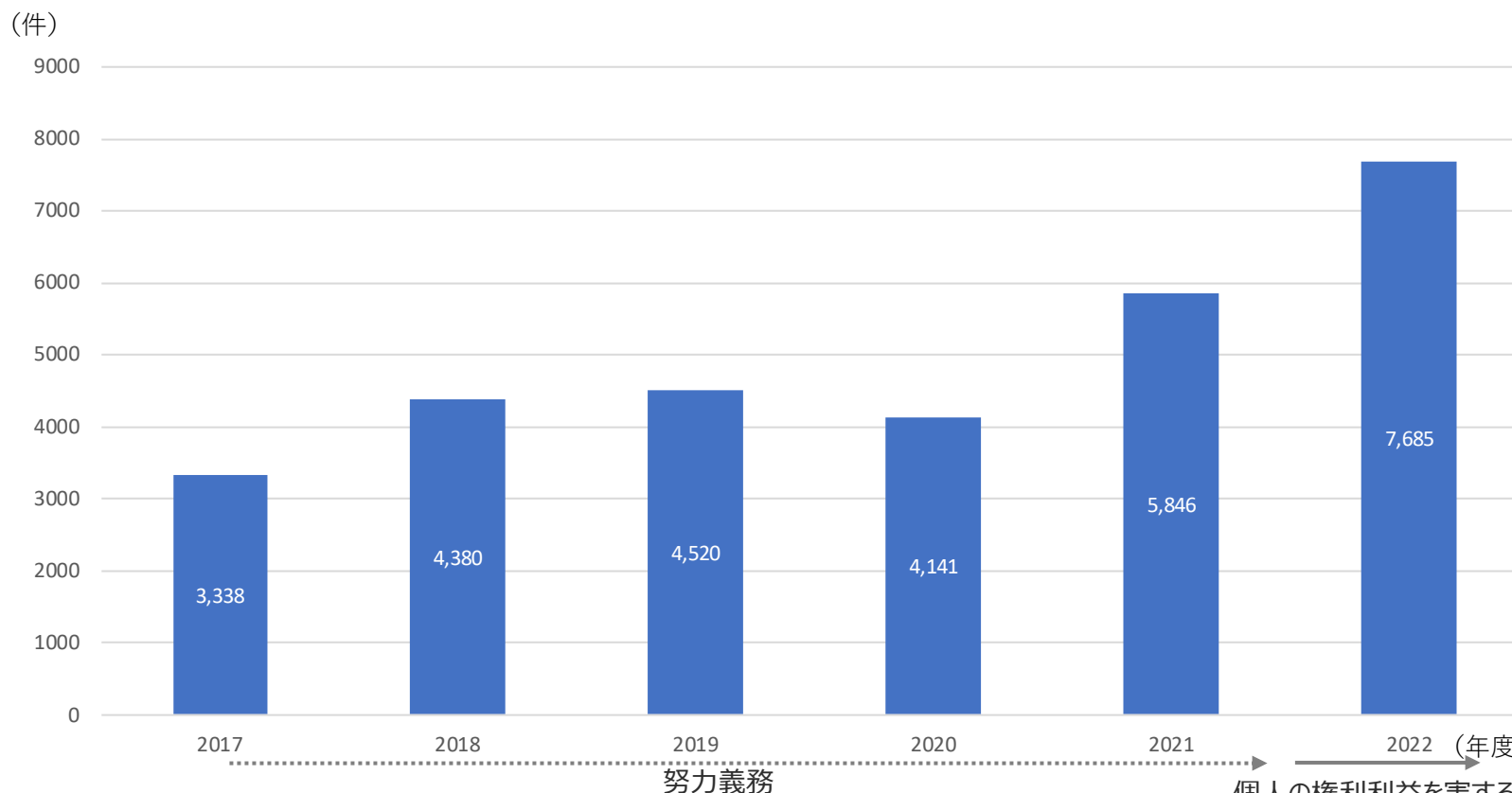


(出所) 株式会社東京商工リサーチ「上場企業の個人情報漏えい・紛失事故」調査結果をもとに日本総研作成

参考資料(2) 国内における漏えい等事案の推移/近年の傾向 —個人情報保護委員会への報告数—

- 個人情報保護委員会事務局において個人情報の漏えい等事案に関する報告を受け処理した件数の推移は以下の通り。
- 報告が努力義務となった2017年度から、ほぼすべての年度で前年比増加している。

個人情報保護委員会事務局への事業者等からの漏えい等事案報告の処理件数推移（2017年度～2022年度）



(注1) 2017年度「個人データの漏えい等」の件数は、報告が努力義務となった5月30日以降のデータを集計している。

(注2) 2022年度7,685件は義務報告のみ。任意報告837件、行政機関等からの報告件数114件は含んでいない。

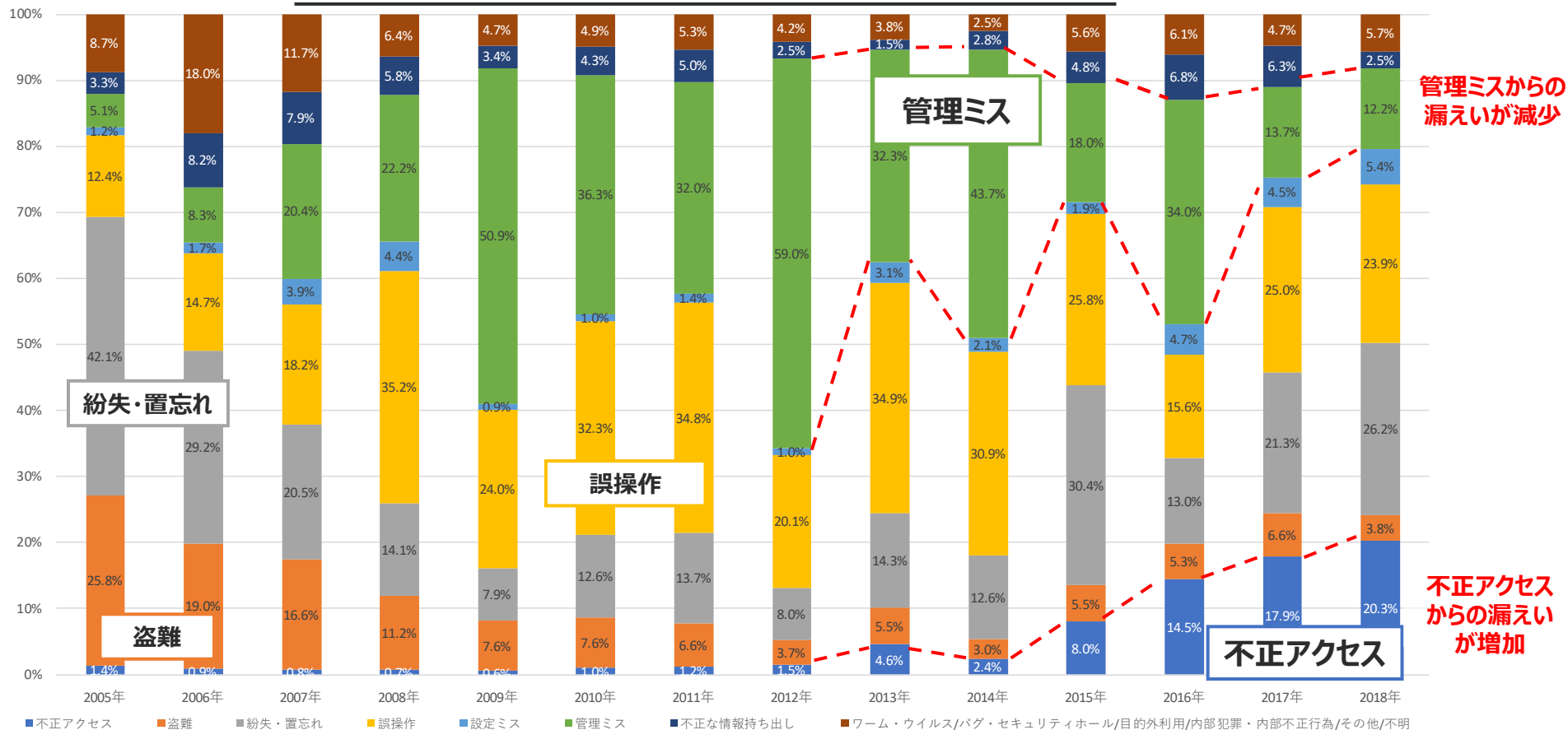
個人の権利利益を害する恐れがあるときは、報告が義務化

(出所) 個人情報保護委員会各年度年次報告をもとに日本総研作成

参考資料(3) 国内における漏えい等事案の推移/近年の傾向 —漏えい等の発生原因の推移—

- 漏えい件数の割合を比較すると、2012年には漏えい原因の半分以上を占めていた「管理ミス」は減ってきている一方で、不正アクセスによる漏えい事案が徐々に増加している。

原因別 漏えい件数の経年変化 (2005年～2018年)



管理ミスからの漏えいが減少

不正アクセスからの漏えいが増加

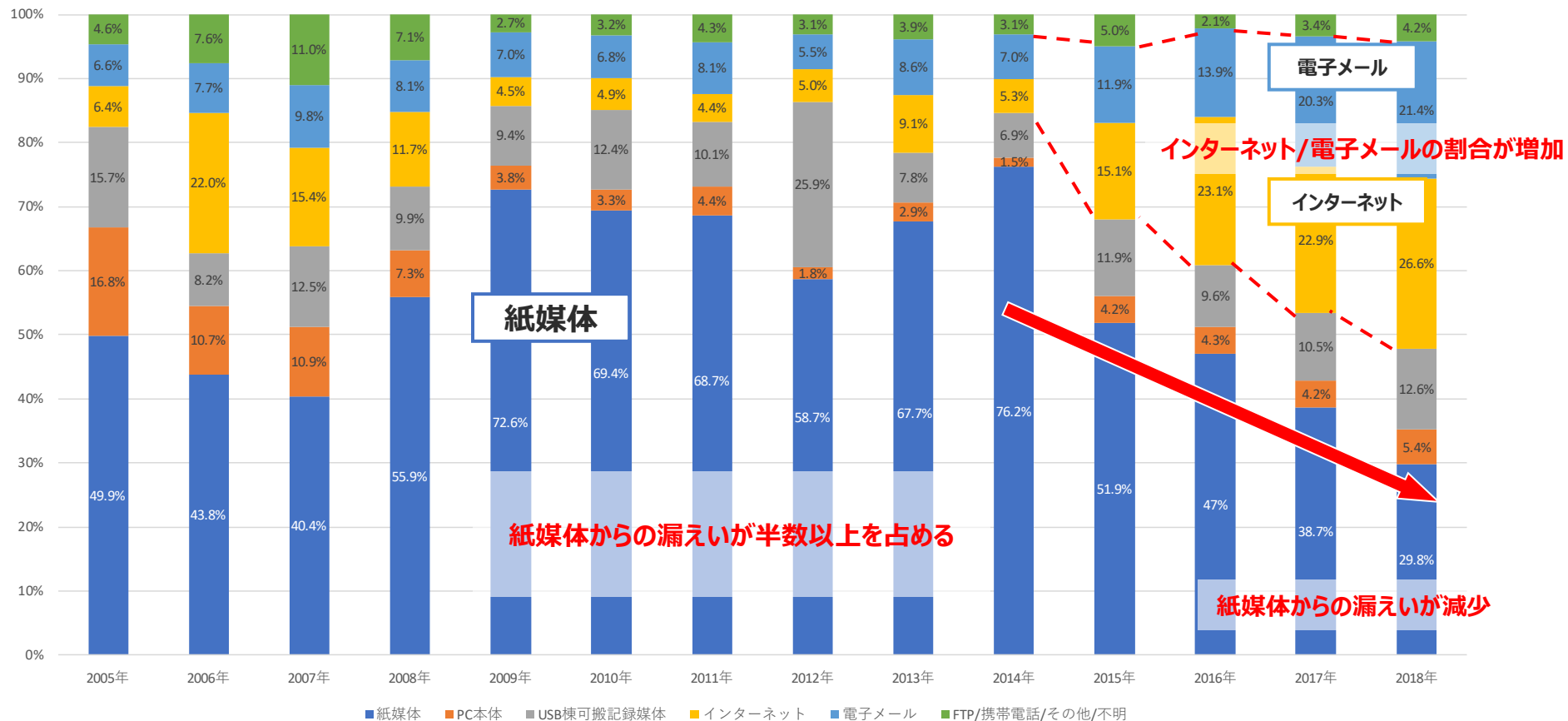
(注) 発生原因別の推移は、各年集計公開後、修正内訳データが改めて公開されていないため、2018年公開資料をもとにしており、元資料から個別数値が読み取れない部分があったワーム・ウイルス/バグ・セキュリティホール/目的外利用/内部犯罪・内部不正行為/その他/不明はまとめて記載している。

(出所) NPO日本ネットワークセキュリティ協会「2018年情報セキュリティインシデントに関する調査結果～個人情報漏えい編～(速報版)」を参考に日本総研作成

参考資料(4) 国内における漏えい等事案の推移/近年の傾向 —漏えい等の発生経路—

- 漏えいの原因となった媒体・経路の割合を比較すると、2014年まで紙媒体からの漏えいが大半を占めていたが、翌年からインターネット、電子メールの割合が急増しており、不正アクセスを原因とする漏えい増加と同時期であることが分かる。

媒体・経路別 漏えい件数の経年変化（2005年～2018年）



(注) 発生経路別の推移は、各年集計公開後、修正内訳データが改めて公開されていないため、2018年公開資料をもとにしており、元資料から個別数値が読み取れない部分があったFTP/携帯電話/その他/不明はまとめて記載している。

(出所) NPO日本ネットワークセキュリティ協会「2018年情報セキュリティインシデントに関する調査結果～個人情報漏えい編～（速報版）」を参考に日本総研作成

2. 海外における個人情報・プライバシーに関する直近の執行状況の要旨（1）

英国 | ICO (Information Commissioner's Office)

	調査件数	処分の数		
		課徴金・罰金	命令	勧告
2022年	545	33	23	32
2021年	1,208	N/A (注)	N/A	N/A
2020年	1,857	N/A	N/A	N/A

(注) 公表資料上、処分の数に関する2020年、2021年の数値は不見当であった。

【執行例】2020年10月30日、ICOは、サイバー攻撃を受けていた会社を買収したMarriott International Inc社が買収時に適切なデューデリジェンスを行わず、また、適切な技術的又は組織的安全管理措置を講じていなかったことがGDPRに違反するとして、同社に対し、1,840万ポンドの制裁金を課した。なお、上記サイバー攻撃により全世界で3億件以上の宿泊者データ（氏名、住所、電話番号、パスポート番号等）の漏えいが推定されている。

フランス | CNIL (La Commission Nationale de l'Informatique et des Libertés)

	調査件数	処分の数	
		制裁措置	正式通知
2022年	345	21 (うち課徴金19件)	147
2021年	384	18 (うち課徴金15件)	135
2020年	247	14 (うち課徴金11件)	49

【執行例】2023年6月15日、CNILは、行動リターゲティングサービスを提供するCRITEO社がGDPRの個人の同意の証明義務（同7条1項）や情報提供義務（同12条・13条）等に違反していたとして、4,000万ユーロの制裁金を課した。

2. 海外における個人情報・プライバシーに関する直近の執行状況の要旨(2)

米国 | FTC (Federal Trade Commission)

調査件数 (注1)		公表されている執行事例 (注2)	
2022年度	541	2022年	6
2021年度	505	2021年	11
2020年度	561	2020年	12

(注1) プライバシー以外の分野の調査件数も含まれている。

(注2) FTCがプレスリリース上で公表している「Privacy and Security」に関する執行事例数であり、実際に執行された件数ではない。

【執行例】2023年6月27日、FTCは、親の同意を得ずに13歳未満の子どもから個人情報を収集する等のCOPPA (Children's Online Privacy Protection Act) に違反する行為を行ったEdmodo社に対して、600万ドルの民事制裁金の支払い等を命じた。

米国 | HHS (the U.S. Department of Health and Human Services)

	調査件数	民事制裁金が課された件数 (注2)
2021年 (注1)	2,177	14
2020年	2,171	19
2019年	1,832	10

(注1) 公表資料上、2022年の数値が見当であったことから、2021年以前の件数を記載している。

(注2) 和解に至った件数を含む。

【執行例】2023年2月2日、HHSは、患者の氏名、生年月日、社会保障番号、診断結果、関係する医療保険情報を含む約280万人の情報の漏えい事案を引き起こしたBanner Health社との間で、125万ドルの支払い等を内容とする和解が成立した旨を公表している。

2. 海外における個人情報・プライバシーに関する直近の執行状況の要旨(3)

カナダ | OPC (Office of the Privacy Commissioner of Canada)

公表資料上、OPCにおける調査件数や処分の数に関する数値は不見当であった。

オーストラリア | OAIC (Office of the Australian Information Commissioner)

	委員会主導の調査	
	開始された数	終了した数
2022年度	28	28
2021年度	7	4
2020年度	4	10

【執行例】OAICは、Facebook Inc社及びFacebook Ireland社が、両者のアプリケーションを通じてユーザーのデータを収集・提供していたことが、オーストラリアプライバシー法の開示制限や個人情報を保護するための措置を講じる義務に違反するとして、制裁金の支払いを求めて2020年3月にオーストラリア連邦裁判所に提訴しており、現在係争中である（なお、制裁金の上限は222万豪ドルと想定される。）。

韓国 | 個人情報保護委員会

	調査件数 (調査対象者の数)	処分の数		
		課徴金・罰金	命令	勧告
2022年	540	160 (うち課徴金 17、過料 143)	61	
2021年	1,209	168 (うち課徴金 22、過料 146)	126	
2020年	1,857	126 (うち課徴金 28、過料 98)	78	94

【執行例】2022年9月14日、韓国の個人情報保護委員会は、ユーザーの行動情報を収集、分析してユーザーの関心を推論し、カスタマイズされた広告などに使用する等していたにもかかわらず、その事実を利用者に明確に知らせず、また、事前に同意を得なかったことが韓国の個人情報保護法に違反するとして、Google Limited Liability Company社及びMeta Platforms, Inc社に対してそれぞれ約690億ウォン、約308億ウォンの課徴金を課した。

2. 海外における個人情報・プライバシーに関する直近の執行状況の要旨(4)

その他の執行事例

同意を得ることなく政治キャンペーンその他の広告のために個人データが利用された事例

2018年10月24日、イギリスのICOは、世論調査中の有権者に対するオンライン広告のターゲットを絞るために、データ主体の同意を得ることなく氏名、電子メールアドレスを含む個人データを利用してAggregage IQ Data Service Ltd.社に対し、データ分析、政治キャンペーンその他の広告目的のために、英国の政治団体などから入手した英国またはEU市民の個人データの処理を中止し、消去することを要求し、これに従わない場合、最高2,000万ユーロ又は全世界での総売上高の4%の高い方を罰金として科すことを通知した。なお、報道によれば、同社は、ブレグジットの国民投票キャンペーン中に有権者候補に対して広告を掲載するために、Vote Leave社から270万ポンド以上の支払いを受けていたとのこと。

公開情報から顔画像等を収集し、顔画像データベースを作成する等した事例

2022年5月18日、イギリスのICOは、インターネット等の公開情報から200億枚以上の顔画像等を収集し、オンライン顔認識データベースを作成する等していたClearview社に対して、UKGDPR違反を理由に約750万ポンドの制裁金を課した。同社は、利用者が同社のデータベースにアップロードした人物画像と類似した特徴を持つ画像のリスト及び出典リンクを提供するというサービスを提供していた。同様の事案について、フランス、オーストラリア及びカナダにおいても執行がなされている。

同意や合理的な必要性を欠いて顔画像が収集された事例

2021年9月29日、オーストラリアのOAICは、7-Eleven Stores Pty Ltd社が店舗に設置したタブレット端末で顧客に対してアンケートを実施し、アンケートに回答した顧客の顔画像を当該端末で撮影し、アンケート回答者の重複を除外するために無期限に利用し、サーバーに無期限に保存したことについて、機微情報である顔画像の同意や合理的な必要性を欠いた収集であり、オーストラリアプライバシー法に違反するとして、収集した顔画像の破棄等の命令を行った。

2. 海外における個人情報・プライバシーに関する直近の執行状況の要旨(5)

その他の執行事例

アプリサービス上で収集した会話履歴がAIモデルの開発等に利用された事案

2021年4月28日、韓国の個人情報保護委員会は、ScatterLab社が同社のアプリサービス上で収集した利用者のメッセージング会話を個人情報の削除又は暗号化措置をせずにAIモデルの開発と運営に利用する等したことが、個人情報の収集目的を超えた利用、法定代理人の同意を得ない14歳未満の児童の個人情報の収集、同意なき機密情報の処理に該当するなど個人情報保護法に違反するとして、課徴金5,550万ウォンの賦課、過料4,780万ウォンを科すなどの措置を採った。

ハッカーによる攻撃により80万人弱の個人情報が漏えいした事案

2023年6月14日、韓国の個人情報保護委員会は、ハッカーの攻撃により利用者の個人情報784,920件を流出させたインターパーク社について、異常なアクセスを遮断する遮断措置を講じておらず、安全措置義務を定めた個人情報保護法に違反するとして、課徴金10億2,654万ウォンの賦課、過料360万ウォンを科すなどの措置を採った。