西村あさひ法律事務所
NISHIMURA & ASAHI
個人情報保護・データ保護規制ニューズレター

Ⅰ. 個人データの漏えい事案における実務対応
Ⅱ. 個人情報保護・データ保護規制 各国法アップデート

2020年
8月27日号

Ⅰ. 個人データの漏えい事案における実務対応

執筆者：河合 優子、北條 孝佳

1. はじめに

近年、様々な機器やシステムがネットワークに接続されることで、利便性が向上する反面、サイバー攻撃の対象領域が拡大している。金融や電気、交通といった重要インフラに対するサイバー攻撃がなされれば、人命を脅かすことにもつながりかねない。また、ある企業がサイバー攻撃の被害に遭えば、その企業に留まらず、接続されたネットワークを経由して、他の企業に被害が拡大する可能性もある。

サイバー攻撃の手法や被害内容は様々である。個人情報やクレジットカード情報、営業秘密情報などの漏えい(窃取)事件は世間に大きなインパクトを与えている。他にも、大量の接続要求を受信してウェブサイトが停止する、ウェブサイトに対する不正なアクセスによりコンテンツが改ざんされる、ランサムウェアにより業務ファイルが窃取された上に暗号化され、業務ファイルを復元したければ又は公開されたくなければ暗号資産(仮想通貨)を支払えと脅迫されるといった被害もみられる。これらの被害は、企業の評価や事業継続性に大きく影響を与える場合もある。

そこで、本稿では、サイバー攻撃により個人データ[1]の漏えい、滅失又は毀損(以下「漏えい等」という。)が発生した場合における実務対応のポイントを概説する。なお、セキュリティ対策を徹底して攻撃を回避することが重要なのは言うまでもないが、100%の防御は不可能である以上、サイバー攻撃を受けてしまった場合を見据えて、事前に社内体制や対応方法を準備しておくことも欠かせない。ひとたびサイバーセキュリティインシデント(以下「インシデント」という。)が発生すれば、状況は刻一刻と変化し、重要な情報と雑多な情報が混在し、複数の作業や判断を迅速かつ的確に行う必要があるためである。

2. 実務対応のポイント

(1) 初動対応

個人データの漏えい等事案は、その対応を誤れば、マスメディア等から多くの批判を浴び、経営トップの責任まで問われる事案

[1] 「個人データ」とは、個人情報データベース等を構成する個人情報をいう(個人情報保護法 2 条 6 項)。

に発展する可能性がある。そのため、事前にコンティンジェンシープラン(緊急時対応計画)等を策定しておき、初動から適切な対応をとることが肝要である。

初動対応では、予め指定されたインシデント対応部門[2]が速やかに被害状況を把握し、被害拡大を防止することに主眼が置かれる。この段階で、インシデント対応部門だけでは対処しきれないと考えられる場合、外部のインシデント対応事業者に依頼することもある。初動対応で行う事項の一例を挙げると、次のとおりである。

- アクセス履歴等の痕跡データの収集
- 個人データが保管されている領域(データベースやファイルが保存されているサーバ等)をネットワークから遮断し、又はアクセス権設定を変更する
- サイバー攻撃手法の推測
- 個人データが漏えい等した経路及び原因の特定
- 漏えい等した個人データの種類、件数等の大まかな把握
- インシデントの重大性の判断(レベル分け)、及びそれに応じた部門連携の開始
- 社内の関係メンバーの限定(情報管理の観点から)

初動対応の段階で被害状況をある程度明らかにできるように、あらかじめ、各ユーザのログイン履歴やファイルへの全てのアクセス履歴、ネットワークの通信履歴等、多数の痕跡データを一括して集約するシステムを導入しておくことが望ましい[3]。

(2) 詳細調査(デジタル・フォレンジック)

初動対応だけでは被害状況や被害経路が判然としない場合には、より詳細な調査や解析を行い、漏えい等した個人データの内容や件数、被害端末やサーバ、システム等の被害状況や、漏えい等のきっかけとなった被害経路、攻撃手法等の詳細な内容を把握する[4]。初動対応においてインシデント対応部門が被害端末の特定やログの集約を実施している場合には、これらを活用し詳細な調査を実施するが、外部のインシデント対応事業者に依頼するケースもみられる。

詳細調査には相当の時間を要する場合もあるため、個人情報保護委員会や本人等への通知・報告や公表等の対応に並行して実施する。また、詳細調査を実施しても、被害の一部しか判明せず、漏えい等した個人データの件数が不明な場合には、侵害された端末等に保存されていた個人データの全件数を被害の最大件数とみなして対応することが望ましい。

加えて、漏えい等した個人データがダークウェブ等で販売・配布されることもある。ダークウェブ等を観測する事業者の協力を得て、一定期間、個人データの不適切な販売・配布がなされていないかを観測したり、二次被害防止のため対象者に注意喚起を行うなどの措置を講じる場合もある[5]。

(3) 通知・報告等

初動対応や詳細調査の過程で被害状況等を把握できた場合、詳細調査の完了を待たずに、インシデント発生前に策定しておいた情報開示基準やマニュアル、行動計画等に沿って、通知・報告等の対応を進めることになる。

---

2 このようなインシデント対応部門として、CSIRT(Computer Security Incident Response Team)を構築し、対応する組織も増えている。

3 具体的には、SIEM(Security Information and Event Management や EDR：Endpoint Detection and Response)等。事前対策を適切に行わず、インシデント発生後の初動対応だけでは、詳細な被害状況を把握することは非常に難しい。また、詳細調査を行っても最後まで被害状況が不明なまま終了するインシデント事例は後を絶たない。システムを導入し、早期の初動調査対応ができることをファスト・フォレンジックともいい、「早急な原因究明、侵入経路や不正な挙動を把握するため、必要最低限のデータを抽出及びコピーし、解析すること」と定義されている(特定非営利活動法人デジタル・フォレンジック研究会)。

4 詳細調査のことをデジタル・フォレンジックともいい「インシデントレスポンス(コンピュータやネットワーク等の資源及び環境の不正使用、サービス妨害行為、データの破壊、意図しない情報の開示等、並びにそれらへ至るための行為(事象)等への対応等をいう。)や法的紛争・訴訟に際し、電磁的記録の証拠保全及び調査・分析を行うとともに、電磁的記録の改ざん・毀損等についての分析・情報収集等を行う一連の科学的調査手法・技術」と定義されている(特定非営利活動法人デジタル・フォレンジック研究会)。

5 ただし、観測を依頼する企業は、観測事業者や観測方法・報告方法の適法性を確認する等、慎重な対応が必要である。「ダークウェブから、例えばサイバー攻撃により不正に入手された個人データを取得するような場合、それが不正な手段によらない個人情報の取得といえるか…など、情報の取得が適法かどうか…等を個別の事例に即して慎重に検討する必要があると考えられる」とされている(内閣サイバーセキュリティセンター「サイバーセキュリティ関係法令 Q&A ハンドブック Ver1.0」Q69 参照)。

①　現行法における報告及び連絡

個人データが漏えい等した場合、現行法の下では、個人情報保護委員会等への報告及び本人への連絡は努力義務にとどまる[6]。報告・連絡の要否や内容については、外部の専門家とも相談のうえ事前に一定の基準を策定しておくことが望ましい。

本人への連絡を行う場合、二次被害の防止や類似事案の発生防止等の観点からは、メール、電話又は書簡等、本人に直接通知することが望ましいが、事案の規模や性質によっては、ウェブサイトへの掲載等、本人が容易に知り得る状態に置くこともある(その場合は、後述する公表との整合性も考慮する必要がある)。また、問合せ専用のメールアドレスの作成や、インシデント発生から一定期間は、24 時間対応の電話窓口を設置すること等も検討すべきであろう。その場合、応対者によって対応や回答が異ならないよう、対応マニュアルや想定 Q&A 集も作成する。

②　2020 年改正個人情報保護法における報告及び本人通知の義務化、利用停止請求等への対応

2020 年 6 月に改正された個人情報保護法(以下「2020 年改正法」という。)の下では、個人データの漏えい等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への報告及び本人への通知が義務付けられる(2020 年改正法 22 条の 2 第 1 項本文、第 2 項本文)。これらの義務違反は勧告、命令、違反の事実の公表等の処分の対象となる(同法 42 条 1 項、3 項及び 4 項)。また、2020 年改正法の下では、報告義務が生じることとなるインシデントが発生した場合は、本人から、利用停止又は消去、あるいは第三者提供の停止の請求を受ける可能性があるため(同法 30 条 5 項)、当該請求に速やかに対応できる体制を整備しておく必要もある。

報告義務が生じることとなるインシデントは、今後改正予定の施行規則に定められるが、①一定数以上の大規模な個人データの漏えい等、②要配慮個人情報の漏えい等、③不正アクセスによる個人データの漏えい等、④財産的損害に至るおそれのある個人データの漏えい等、といったものが含まれると考えられる。また、2020 年改正法の下では、報告の提出先が個人情報保護委員会に一元化され、速報と確報の二段階の報告が求められる見込みである。現行法の下では、本人への連絡方法は、直接の通知・ウェブサイトへの掲載等のいずれでも構わないが、2020 年改正法では、本人への通知が困難な場合に限ってウェブサイトへの掲載等が認められる。

(4)　各国法対応

GDPR を筆頭に、各国のデータ保護法制の適用がある場合には、個人データの漏えい等に伴って海外当局に報告を行う必要がある。GDPR のように、漏えい等の発生を認識してから 72 時間以内に報告することを原則とする等、時間的な限定付けがなされる場合もあるため、平時から、国内外の法律事務所との連絡体制を構築しておくことが望ましい。

また、実務的には、平時から自社の取り扱っている個人データを把握し、それらに各国のデータ保護法制の適用があるのか整理しておかないと対応が困難である。例えば、EU 域内の子会社から日本の本社に移転された個人データが漏えい等した場合、当局への通知義務は生じるのだろうか、生じるとして EU 域内の子会社と日本の本社の何れが当局に通知するのだろうか。また、EU 域内に出張したときに取得した名刺を格納したデータベースから個人データが漏えい等した場合、当局への通知義務は生じるのだろうか。これらの問いに答えが用意されていなければ、個人データが漏えい等した際に適切に対応することは不可能である。

(5)　警察への相談・報告等

サイバー攻撃による個人データ漏えい等事案の場合、不正アクセス禁止法違反や不正競争防止法違反の可能性があるため、警察への被害相談の実施や被害届の提出を検討する。警察署への訪問時には、詳細調査によって作成された解析結果報告書等があればこれを持参して説明する。サイバー攻撃を行った攻撃元が日本国内の IP アドレスである場合には、警察は、当該 IP アドレスが割り当てられた端末を差し押さえるために裁判所へ捜索差押令状を請求する必要があり、システム担当者の供述調書が作成されることもある。

6　平成 29 年個人情報保護委員会告示第 1 号「個人データの漏えい等の事案が発生した場合等の対応について」

(6) 適時開示・インサイダー取引規制対策

上場企業において個人データの漏えい等の事案が発生した場合には、有価証券上場規程や同施行規則に従い、適時開示の要否を検討する必要がある。また、当該事案の発生が、インサイダー取引規制上の「重要事実」に該当する場合には、当該事実の公表前に会社関係者が当該企業の株式等の取引を行うことは、インサイダー取引規制に該当し得るため(金融商品取引法 166 条 1 項柱書)、社内の情報管理及び株式取引制限の徹底が重要である。

なお、個人データ漏えい等の事案に限った問題ではないが、適時開示について、インターネット上に公開している自社ウェブサイト等に会社情報を掲載するにあたり、公表予定時刻より前に資料を自社ウェブサーバ内の「公開ディレクトリ」に情報セキュリティ措置を講ずることなく保存したため、公表予定時刻より前に外部の者が容易に閲覧できるケースがあることが明らかになったとの指摘があり[7]、この点に留意する必要がある。

(7) 公　表

適時開示事由に該当しない場合、実務上、ステークホルダーへの公表を行うことが多いが、その内容や時期は、事案に応じて慎重に検討する必要がある。例えば、公表後、詳細調査によって新たな別の被害が判明した場合には、適切な初期対応ができていなかったのではないかと指摘を受けたり、株価の下落や取引関係の変更など、企業活動に少なからず影響を与えるおそれがある。また、公表により二次被害の拡大が惹起される場合もある。そのため、法務部門、広報部門及び経営陣は、IT システム管理部門や情報セキュリティ管理部門等と緊密に連携し、必要に応じて外部専門家も起用して、公表の要否や内容を検討する必要がある。

公表を行う場合には、経緯、漏えい等した個人データの種類・件数、原因、対応状況、二次被害の状況、再発防止策、問合せ窓口等を記載することが一般的である。

(8) 再発防止策の検討

上記の各対応に並行して、同種事案の再発防止策を検討する必要がある。特に、事案の公表や個人情報保護委員会への報告、本人への連絡等を行う場合は、この再発防止策も公表・連絡事項に含めるべきであるため、速やかな検討が求められる。

また、同種事案の再発防止策という、いわば短期的な対策にとどまらず、企業としてのセキュリティ体制の評価や抜本的な見直し等、長期的な対策も必要となり得る。デジタルトランスフォーメーション(DX)が促進され、デジタル化された社会を狙うサイバー攻撃の手法が複雑化・高度化することに伴い、各企業は、時代に合わせたセキュリティ体制を構築すべく、定期的・継続的に見直すことも考えられる。

かわい　ゆうこ
河合　優子
西村あさひ法律事務所　パートナー弁護士
y_kawai@jurists.co.jp

2006年弁護士登録。2013年コロンビア大学ロースクール卒業(LL.M.)、2014年ニューヨーク州弁護士登録。M&A、ジョイントベンチャー、各国データ関連法制への対応、ライセンス、電子商取引、株主総会対応その他企業法務全般について、クロスボーダー案件を中心に数多く担当。日本の個人情報保護法制については、多国籍企業を含む国内外の企業・組織をクライアントとし、データの域外移転、M&A に伴うデータの取扱い、医療・遺伝子関連データの取扱い等、多岐に渡る問題点について、多くのアドバイスを継続的に提供。情報法制学会会員。一般社団法人遺伝情報取扱協会監事。

ほうじょう　たかよし
北條　孝佳
西村あさひ法律事務所　カウンセル弁護士
ta_hojo@jurists.co.jp

危機管理、企業不祥事などの企業法務に従事。特に様々なサイバーセキュリティ事案の調査・法的措置・再発防止策に関する法的アドバイスを行っている。2000年警察庁入庁。元警察庁技官。デジタルフォレンジックやマルウェア解析等に従事し、数多くのサイバー攻撃事案に対応。2015年弁護士登録、日本シーサート協議会専門委員、情報通信研究機構招聘専門員、総務省発信者情報開示の在り方に関する研究会構成員等を務める。

[7] 「上場会社等が法定開示書類及び適時開示事項を自社ウェブサイト等に掲載する場合の留意事項について」(2013 年 4 月 5 日、金融庁)

Ⅱ. 個人情報保護・データ保護規制　各国法アップデート

執筆者：岩瀬　ひとみ、松本　絢子、石川　智也、河合　優子

1.　日　　本

2020 年 7 月 29 日、個人情報保護委員会は、違法に個人データをウェブサイトに掲載している 2 事業者に対し、個人情報保護法 42 条 2 項に基づき、当該ウェブサイトを直ちに停止等するよう命令を行った。同法に基づく初の命令事案である。本件は、利用目的の通知・公表の不実施(同法 18 条違反)及び同意に基づかない第三者提供(同法 23 条 1 項違反)が問題とされている。

2.　韓　　国

2020 年 8 月 5 日、個人情報の保護・活用に関する主要な法律である①個人情報保護法、②情報通信網の利用促進及び情報保護等に関する法律(情報通信網法)並びに③信用情報の利用及び保護に関する法律(信用情報法)の各改正法が施行された。同改正は、当事務所個人情報保護・データ保護規制ニューズレター2020 年 1 月 31 日号で紹介したとおり、個人情報の定義の明確化、委員会の独立性・執行機能の強化、金融分野におけるデータ経済の活性化等を意図しており、個人情報の保護と安全な活用の調和が期待されている。また、高画質カメラを搭載したドローンによる個人情報侵害への憂慮が増大していることを背景として、移動型映像情報処理機器で収集された個人情報も個人情報保護法の対象となるよう、更なる改正の議論がなされている。

3.　米　　国

2020 年 8 月 14 日に、CCPA(カリフォルニア州消費者プライバシー法)最終規則が Office of Administrative Law(OAL)によって承認され即日発効した。2020 年 6 月 1 日に OAL に提出された CCPA 規則最終案は、3 月 11 日に公表されたもの(当事務所個人情報保護・データ保護規制ニューズレター2020 年 2 月 14 日特別号及び同 2020 年 3 月 24 日号参照)から実質的な変更はなかったが、OAL によって一部修正がなされている。州司法長官による CCPA の執行開始日は 7 月 1 日であり、CCPA 規則が成立するのに先立ち、CCPA の規定を根拠としたエンフォースメントが開始されているようである。

4.　E　　U

欧州司法裁判所は、2020 年 7 月 16 日に Schrems II 事件の判決を下し、EU から米国に個人データを移転するための枠組みの 1 つであるプライバシーシールドを無効と判断した。また、EU から個人データの保護の水準が十分であるとの認定を受けていない国に個人データを移転するための枠組みの 1 つである標準契約条項(SCC)については、それ自体は有効であるものの、①当事者間で締結されている契約の内容のみならず、移転先の国の公的機関による移転されたデータへのアクセス(いわゆるガバメント・アクセス)に関して移転先の国の法制度を考慮した上で、EU 域内の保証と実質的に同等の水準の個人データの保護を保障することを求めるとともに、②SCC だけでは EU 域内の保障と実質的に同等の水準の個人データの保護が保障できないおそれがある場合には、補完的措置を講じて対応することを求めている。このため、SCC を締結して個人データの移転を行っている企業には、新たな対応事項が生じている状況である。

プライバシーシールドについては、2020 年 8 月 10 日、米国商務省と欧州委員会が共同で、上記判決に対応したプライバシーシールドの強化版の可能性を評価するための協議を開始したと公表している。

詳細は、当事務所ヨーロッパニューズレター2020 年 7 月 29 日号も参照されたい。

5.　中　　国

・ 2020 年 7 月 3 日、「中華人民共和国データ安全法」(草案)が公表され、2020 年 8 月 16 日まで意見募集が行われた。当該草案は、(1)レベル別、種類別によるデータ管理及びリスク評価、モニタリング・早期警報、応急措置等データ安全管理に関する各基本制度を創設、(2)データ活動を展開する組織及び個人のデータ安全保護義務を明確化、(3)データ安全と発展を両立させ促進・支持する措置を規定、(4)政務データ安全の保障と政務データ開示の推進に関する制度・措置の創設等の内容が含まれている。

・ 2020 年 7 月 25 日、中華人民共和国サイバーセキュリティ法の実施に関して、「ネット安全基準実践ガイドライン–アプリ(App)による個人情報の収集・使用に関する自己評価ガイドライン」が制定された。
・ 2020 年 7 月 27 日、「情報安全技術　情報技術製品サプライチェーン安全要求(意見募集稿)」が公表され、2020 年 9 月 26 日まで意見募集が行われている。
・ 2020 年 7 月 29 日、「ネット安全基準実践ガイドライン–アプリ(App)によるシステム権限の申請・使用に関する手引き(意見募集稿)」が公表され、2020 年 8 月 12 日まで意見募集が行われている。

6. エジプト

エジプトでは、個人情報保護法が、2020 年 7 月 13 日に大統領の承認をもって最終的に成立し、7 月 15 日に公布され、2020 年 10 月 14 日から施行される。この新法は、エジプトの国内外を問わず、エジプトにいる個人に関する個人データの処理を行う企業に適用される。また、エジプト国外に所在する受領者に対する個人データの移転は、今後設立予定のエジプトデータ保護センターの許可がない限り、原則として禁止されている。個人データの越境移転に関するルールやガイドライン等は、2021 年 4 月 14 日までに制定予定の施行規則において定められることが想定されている（当事務所個人情報保護・データ保護規制ニューズレター2020 年 3 月 24 日号も参照）。

いわせ
岩瀬　ひとみ
西村あさひ法律事務所　パートナー弁護士
h_iwase@jurists.co.jp

1997 年弁護士登録、2004 年ニューヨーク州弁護士登録。1994 年早稲田大学法学部卒業、2003 年スタンフォード大学ロースクール卒業(LL.M.)。知財/IT 関連の各種取引や争訟(特許関連訴訟、商標関連訴訟、システム関連紛争等)を主に扱う。IT 分野では、国内・外国が絡む、様々な局面における個人情報・データ関連の規制その他の問題や、クラウド、AI、IoT 等新しい技術を用いたビジネスに絡む各種法律問題についてアドバイスを行う。

まつもと　あやこ
松本　絢子
西村あさひ法律事務所　パートナー弁護士
a_matsumoto@jurists.co.jp

2005 年弁護士登録、2013 年ニューヨーク州弁護士登録。2012 年ノースウェスタン大学ロースクール卒業(LL.M.)後、2012-2013 年ニューヨークの米国三菱商事会社および北米三菱商事会社に出向。国内外の M&A や企業組織再編のほか、コーポレートガバナンス、コンプライアンス、情報管理、ブランド戦略、保険等に関連する企業法務一般を幅広く扱う。情報管理関連では、個人情報や営業秘密、知財、インサイダー取引規制等に関する法律問題や、AI・クラウドに絡む法律問題等についてアドバイスを提供している。情報法制学会会員。

いしかわ　のりや
石川　智也
西村あさひ法律事務所　パートナー弁護士
n_ishikawa@jurists.co.jp

2006 年弁護士登録。2005 年東京大学法学部卒業、2015 年バージニア大学ロースクール卒業(LL.M.)、2016 年ミュンヘン知的財産法センター卒業(LL.M.)、Noerr 法律事務所ミュンヘンオフィスに出向、2017 年ニューヨーク州弁護士登録。GDPR を初めとするグローバルでの個人情報保護法制・データ規制へのコンプライアンス対応について多くの日本企業にアドバイスを提供しており、関連する講演・執筆記事も多数。日本経済新聞社による「2019 年に活躍した弁護士ランキング」の「データ関連分野」で、総合ランキング 1 位(企業票＋弁護士票)。情報法制学会会員、Certified Information Privacy Professional/Europe(CIPP/E)。2020 年にドイツのフランクフルト・デュッセルドルフに開設予定の西村あさひ法律事務所欧州拠点の代表に就任予定。

かわい　ゆうこ
河合　優子
西村あさひ法律事務所　パートナー弁護士
y_kawai@jurists.co.jp

2006年弁護士登録。2013年コロンビア大学ロースクール卒業(LL.M.)、2014年ニューヨーク州弁護士登録。
M&A、ジョイントベンチャー、各国データ関連法制への対応、ライセンス、電子商取引、株主総会対応その他企業法務全般について、クロスボーダー案件を中心に数多く担当。日本の個人情報保護法制については、多国籍企業を含む国内外の企業・組織をクライアントとし、データの域外移転、M&A に伴うデータの取扱い、医療・遺伝子関連データの取扱い等、多岐に渡る問題点について、多くのアドバイスを継続的に提供。情報法制学会会員。一般社団法人遺伝情報取扱協会監事。

（当事務所の連絡先）　東京都千代田区大手町 1-1-2 大手門タワー 〒100-8124
Tel: 03-6250-6200 (代) Fax: 03-6250-7200
E-mail: info@jurists.co.jp　URL: https://www.jurists.co.jp