Vol.2021-EIP-91 No.1
2021/2/19

欧米における侵害通知の状況と日本への示唆

金子啓子†

概要： 2020 年個人情報保護法改正により、日本においても個人情報の侵害通知が義務化される。日本においては 2004 年から基本方針などで本人通知、官庁等への届出、公表が推奨され、小さな事故でも報告していた個人情報取扱事業者も相当数あった。しかし、法律上の義務となれば、その条件等が厳密に検討されるべきである。そこで、既に義務化されている欧米の状況を整理し、日本の今後の運用の実務視点からの参考としたい。

キーワード：個人情報、侵害通知

Data breach notification in US and EU and its lesson to the operation in Japan

KEIKO KANEKO†

Abstract: The revision of APPI in Japan will make the data breach notification mandatory.
In Japan, it's recommended in Basic Policy and other governmental guidelines to notify the principal, to report to the ministry and to disclose publicly, and certain number of personal information handling operators conducted these actions even if a small incident. Now it becomes legal obligation. The requirement should be more specific. Thus, this paper discusses the situation of US and EU where the data breach notification is already legal obligation and try to seek some lesson to the operation in Japan.

Keywords: personal information, data breach notification

1. はじめに

2020 年個人情報保護法（以下個情法）改正により、日本においても個人情報の侵害通知が義務化される。日本においては 2004 年から基本方針で公表が重要とされ、それを受けた経済産業省のガイドライン[a]では、本人への二次被害を防止するための通知と謝罪、主務大臣への報告、事実関係・再発防止策等の公表が推奨されていた。また、プライバシーマーク制度でも事故発生時のマーク付与機関への報告が義務づけられていた。生真面目でこれらの知識を有していた個人情報取扱事業者は小さな事故でも対応していたが、多くの個人情報取扱事業者は何もしない、という二極化の状況があった。

生真面目な事業者が行ってきたような小さな事故についての通知報告までが義務化されると、社会的な負担が大きくなりすぎる心配もあったが、改正個情法では、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に定めるものについて、個人情報保護委員会への報告と本人通知が義務付けられ、公表は原則として義務付けられていない[b]。2020 年 12 月 25 日、個人情報の保護に関する法律施行規則の一部を改正する規則(案)が公開されたが、そこでは①要配慮情報を含む個人データの漏洩等②財産的被害が生じる恐れがある個人データの漏洩等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洩等④1000 人を超える個人データの漏洩等の 4 類型が定められており[c]、概ね妥当と思われる。

しかし更に詳細な実務を検討するにあたり、先行する米国、EU の状況を概観することは実務上も有益なものと考えられる。また、本人通知は、二次被害を防止するために本人が自衛することを促すことができる、という意味で必要・有用であることは理解できるが、個人情報保護委員会への報告を義務付けることにどのような意味があるのか、単に、安全管理義務違反の処分を促進するためではないか、など、実務視点では心配でもあり、この点についても参考になることが期待される。

そこで、米・欧それぞれの概要を説明し、日本における運用への示唆を検討する。なお、本稿では、既に執筆した公表済み及び未発表の原稿も引用する。

† 大阪経済大学経営学部 Osaka University of Economics

[a] 平 16･4･2-個人情報の保護に関する基本方針
経済産業省、「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」(平成 26 年 12 月 12 日厚生労働省・経済産業省告示第 4 号)28 頁

[b] 改正 個情法 22 条の２

[c] 個情法施行規則改正案 6 条の２

2. 米国

2.1 州法

2.1.1 カリフォルニア州

最初に侵害通知を法で義務付けたのは、2002 年成立したカリフォルニア州のセキュリティ侵害情報法[d]である[e]。当時、他人の個人情報を盗用したクレジットカード口座の開設、小切手の発行、車の購入、その他のなりすましによる経済的犯罪が急増していたため、カリフォルニア州議会は、これらの源となる個人情報の漏洩等が派生した際には、なりすましの被害者が迅速に損害を最小化できるように、個人情報の悪用の可能性を通知することを義務付けるべく、立法した[f]。この法律では公的機関の義務と民間の事業者の義務が定められているが、侵害通知の内容については、ほぼ同内容のため、以下、民間の事業者の義務に着目して述べる[g]。

①通知が義務付けられる個人情報

侵害通知のセクション内に、そのセクションにおける「個人情報」の定義が以下の通り定められている[h]；

（１）氏名と以下の情報の組合せ（どちらかが暗号化されていない場合）

(A)ソーシャルセキュリティ番号

(B)運転免許証番号、又はカリフォルニア州 ID カード番号、納税者番号、パスポート番号、軍人番号等、政府文書により発行される ID で本人確認に共通して使用されるもの

(C)銀行口座、クレジットカード又はデビットカード番号がセキュリティコード、暗誦番号など使用に必要な情報と共に

(D)医療情報

(E)健康保険情報

(F)認証に用いるバイオメトリックスデータ

(G)自動ナンバープレート認識システムにより収集されたデータ

（２）ユーザー名や e メールアドレスと、パスワードやセキュリティの質問と答えの組合せ

公的機関によって法に基づいて公表されている情報は、「個人情報」ではない[i]。

立法当初は（１）(A)～(C)のなりすましによる経済犯罪につながりやすいものだけであった[j]が、現在はその他のなりすましのリスクのある情報などに拡大している。

②報告が義務付けられている場合

事業者は、これらの「個人情報」が権限のない者に窃取されたとき、又は窃取されたと合理的に信じられるときは、「システムのセキュリティ侵害」を迅速に公表するか、情報主体であるカリフォルニア州住民に通知しなければならない。データが暗号化されている場合は免除されるが、暗号化したデータと鍵などが窃取された場合は免除されない[k]。他人から受託して「個人情報」を持っている事業者はそのオーナーである委託元に通知する義務がある[l]。捜査当局が通知が捜査の妨げになると判断したときは、通知を遅らせることができる。なお、「システムのセキュリティ侵害」は「セキュリティ、機密性、完全性が損なわれたこと」と定義されているが、通知の義務があるのは acquire された時だけなので、完全性が損なわれただけでは通知義務はないと考えられる。

③通知の記載事項

通知の記載事項も細かく定められている；

事業者名、漏洩したと思われる個人情報の種類、可能なら発生したと思われる時期、捜査によって通知が遅れたかどうか、可能なら事故の概要、ソーシャルセキュリティ番号や運転免許諸番号やカリフォルニア州 ID カード番号の漏洩の際はクレジットレポーティング業者のフリーダイヤルと住所、もし、「個人情報」の定義の(A)(B)に該当する情報が通知者において侵害された場合、発生した場合、なりすまし防止と被害緩和対策を 12 か月無償で提供せねばならず、それを受けるために必要な情報を通知する義務がある。また、個人を守るために何をしたか、個人が自衛するためにとれる手段、バイオメトリックス認証データが漏洩した場合、その情報を認証に使用する他の事業者に使用中止を要請する方法、も任意で通知することができる。

④様式

タイトルは ““Notice of Data Breach”とし、“What Happened,” “What Information Was Involved,” “What We Are Doing,” “What You Can Do,” and “For More Information.”といった見出しで、平易な言葉で書かなければならない。重要性がわかるように表示し、10 ポイント以上の文字を使用すること、とし、書面での通知の際のフォーマットも掲載されている[m]。

⑤通知手段

通知手段は、以下のいずれかによる；

(1)文書

(2)連邦法に定める文書の電子化についての条件[n]を満たした消費者の同意を得た場合は、電子的通知

---

[d] California Security Breach Information Act (Senate Bill 1386)

[e] INFORMATION SECURITY AND PRIVACY, A PRACTICAL GUIDE FOR GLOBAL EXECUTIVES, LAWYERS AND TECHNOLOGISTS, 64 (Thomas J. Shaw Esq. Ed., 2011)64

[f] California Security Breach Information Act　§ 1
湯淺墾道「アメリカにおける個人情報漏洩通知法制に関する考察」情報ネットワーク・ローレビュー第 11 巻(2012 年 11 月) 72-87、74

[g] 公的機関については Cal. Civ. Code 1798.29、民間事業者については Cal. Civ. Code 1798.82 に定めがある。

[h] Cal. Civ. Code 1798.82 (h)

[i] Cal. Civ. Code 1798.82 (i)

[j] (B)は、運転免許証番号、又はカリフォルニア州 ID カード番号だけであった。

[k] Cal. Civ. Code 1798.82(a)

[l] Cal. Civ. Code 1798.82 (b)

[m] Cal. Civ. Code 1798.82 (d)

[n] 15 USC 7001　紙の文書も選択できることなどを事前に説明し、電子的に同意を得れば、電子的な文書も有効とする。

(3)上記いずれかの実施に 25 万ドル以上必要、50 万人以上への通知が必要、又は十分なコンタクト情報を有しない場合は、代替手段として以下のすべてを実施；
(A)電子メールアドレスを有する場合は電子メールでの通知
(B)web サイトがある場合は、30 日間の目立った掲載
(C)州の主要なメディアへの通知
(4)ユーザー名や電子メールアドレスとパスワードなどの組合せのみが漏洩した場合は、被害者にその旨とパスワードなどの変更の指示を電子的又は他の方法で提供することでも可。
(5)電子メールアドレスのログイン認証情報が漏洩したときは、そこへの通知では不十分で、他の方法によるか、その世帯がインターネットのオンラインアカウントを持っていれば”resident online”に目立つ表示を掲出する[o]。
もしも、事業者が情報セキュリティポリシーで通知方法を定めている場合は、それによることでもよいとしている[p]。

⑥政府への報告

500 件以上のカリフォルニア州住人の情報が侵害された場合は州の司法長官に侵害通知のコピーを電子的に提出する義務がある[q]。

⑦罰則等

侵害通知を含め顧客情報の節の条文の違反については、損害賠償請求や差止請求が可能だが、罰則などは定められていない[r]。

2.1.2 その他の州

現在は、50 州すべてで同様の侵害通知法を定めている[s]。各州は、カリフォルニア州法をモデルにしている。対象となる個人情報については、氏名と共に流出した情報等で、微妙にバリエーションがあるが、いずれもなりすましのリスク等の高い情報に限られている[t]。暗号化された情報はすべての州で免責となっている。
数に関わらず州の司法長官等の機関への報告を義務付けている州も、ニューヨーク州をはじめ、いくつかある[u]。また、ペナルティが定められている州もいくつかある。例えば、ニューヨーク州では、侵害通知違反に対し司法長官は仮処分の父権訴訟を提起でき、更に、侵害通知がなかったことによる実損の賠償も結果損害も含め請求できる。裁判所は故意または重過失により違反したと判断したときは、5000 ドル又は 1 件につき 25 ドル(総額 25 万ドル以下)の民事罰を科すこともできる[v]。

[o] Cal. Civ. Code 1798.82 (j)
[p] Cal. Civ. Code 1798.82 (l)
[q] Cal. Civ. Code 1798.82 (f)
[r] Cal. Civ. Code 1798.84
[s] https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx （2021 年 1 月 7 日最終閲覧）
[t] 前掲注 s。Shaw・前掲注 e 64 頁
[u] ニューヨーク州、インディアナ州、メリーランド州、マサチューセッツ州など
[v] GEN.BUS. §899-AA 6 条

2.2 連邦法

2.2.1 民間の義務

連邦法においても、侵害通知義務を定めるものがいくつかある。金融事業に関するグラム・リーチ・ブライリー法において顧客のプライバシーの保護が問題となり、2003 年、FTC が金融機関等に適用されるグラム・リーチ・ブライリー・セーフ・ガード規則によりセキュリティを義務付け、管轄する当局が顧客情報の保護に関する官庁間統一ガイダンスを定め、この中で侵害通知が義務付けられている[w]。その中で、タイムリーな通知は機関のレピュテーションリスクを管理するために重要であり、顧客のなりすましの被害からの自衛を可能にすることによって法的リスクも下げ、顧客との良い関係も維持できる、恥ずかしいとか面倒などの理由で見合わせてはいけない、としている。そのうえで、氏名が社会保険番号、運転免許証番号、口座番号、クレジットカード又はデビットカード番号、個人 ID 番号と共に流出した場合や、アカウントへのパスワードやオンラインバンキングの認証情報の漏洩時には通知を義務付けている[x]。

オバマ政権の 2009 年には、なりすましによる経済被害以外の目的での侵害通知義務も登場した。経済的・客観的な健康情報技術に関する法律において、医療機関、健康保険を扱う事業者、および個人健康記録を扱うサービスベンダーは、健康情報のセキュリティが侵害され又は合理的に侵害されたと信じられるときは、その個人に対し通知する義務を負う旨、定められた。通知は侵害の発見から 60 日以内に出されなければならず、通知したことの立証責任を負う。通知は郵送によるが本人が意向によっては電子メールでもよい。古い住所等しかない、など、それらの方法で通知できない時は、10 人以上通知できない個人がいる場合は、その事業者の Web サイトのホームページへの目立った掲載又は主要なマスメディアへの通知という代替手段を取ることができる。しかし、差し迫った誤用があり得るので緊急を要すると判断するときは、郵送等での通知に加え電話での通知も可能である。また、500 人以上の情報が侵害されたときは、州の有名なメディアに通知する必要がある。更に保険福祉長官への報告も義務付けられ、500 人以上の侵害時は直ちに、それ以外は記録を残し年間まとめて報告しなければならない。保険福祉省はそれを Web サイトに掲出し、議会に年次報告する[y]。

2.2.2 政府機関の義務

連邦政府における個人情報保護は 1974 年制定のプライバシー法[z]で規制されており、その実施のためのガイドライン制定は行政予算局が制定することになっている[aa]。2017

[w] 湯淺・前掲注 f 77 頁
[x] 12 C.F.R. Part 30, App. B
[y] 42 U.S.C.17932、湯淺・前掲注 f 75 頁
[z] Privacy Act of 1974, Pub. L. No.93-579
[aa] 5 U.S.C.S 552a (v)

年 1 月行政予算局は連邦機関において侵害が発生した時の対応に関するポリシーを改定した[bb]。この中の VII.事故対応計画の中に、侵害通知の規定がある。通知するか否かについて、民間より判断の幅があるが、それだけに通知の手段などの説明には、参考になる点が多い。

基本的な考え方としては、セキュリティ侵害は、事実によるので、通知をするかどうかは状況により異なる、としている。その上で、政府機関が通知をするかどうかは、個人へのリスクを評価して機関の長が決定するとし、透明性と過剰通知のバランスを取る、としている。通知は機関の長の名前で出すべきとするが、委託先で発生した場合は、委託先に侵害通知を出させることもできる。タイミングは実務的に迅速に遅滞なく出すべきとしており、具体的な期日には言及していない。むしろ、一つの事故について複数回の通知を出すことを避けるべきであり、事実調査に要する時間と本人へのリスクの可能性をバランスすべきとする。通知の内容としては、事故の概要と漏洩した情報の種類、暗号化その他の保護措置があったかどうか、もしあれば、個人が損害を緩和する手段や機関が取っている対策や被害者に提供しているサービス、もしあれば機関が取りつつある調査、緩和策、将来の侵害の防止策、個人から連絡が取れる機関の窓口情報が挙げられている。FAQ も有益だがアップデートや翻訳が容易なように Web に出す方が良い、フリーダイヤルのコールセンターを設置し侵害対応に慣れたオペレーターを使う、被害者が英語以外を使う人が多いなら複数の言語で通知すべき、など、実務上の Tips のような事項も記載されている。通知方法については、最新の住所への普通郵便が優先、とし、もしも転居などで古くなっていることがわかっていたら、郵便局など他の機関に問い合わせるなど、合理的な手段でアップデートすることとされている。広告と間違えて捨てられないよう、封筒には機関名を記載し受領者の注意を惹くラベルを表示する。配達不能で返送された場合に次の通知をいかに行うかに関する手続きを決めておく。緊急性があるときは電話も適切だが、郵送と併用すべきである。電子メールは事故のことを知った攻撃者が悪用することが多いため、推奨しない。スパムやジャンクメールフォルダに自動的に入ることもあるし、メールの合法性を疑い、開封しないこともある。十分な連絡先を持っていない場合は代替手段も取ることができる。新聞と放送のメディアに通知するが、その中には個人が自分の情報が含まれているかどうかを問い合わせることができるフリーダイヤルや電子メールアドレスを掲載する。調査中で今後事態の詳細が判明していく場合は、アップデート情報が欲しい人が情報を受信できる方法も検討する。代替手段は、大きな事故が発生した際の第一報としても活用できる、とする。

[bb] OMB Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifia-ble Information (January 3, 2017)
https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-12_0.pdf

3. EU

3.1 GDPR 及び侵害通知に関するガイドライン

欧州において、侵害通知が初めて規定されたのは、2002 年の EU 電子通信プライバシー指令の 2009 年改正である。しかし、対象は通信プロバイダであった。これに対し、2016 年に成立し 2018 年 5 月から施行されている一般データ保護規則（以下 GDPR という）では、全事業者に報告を義務付けている[cc]。

前文の趣旨によれば、「個人データ侵害は、適切かつ適時の態様で対応が行われないと、自然人の個人データに対する管理の欠落又は自然人の権利制限の喪失、差別、ID 盗取又は ID 詐欺、金銭上の損失、無権限による仮名の復元、信用の毀損、職務上の守秘義務によって保護された個人データの機密性の喪失、又は、関係する自然人に対するその他の重要な経済的若しくは社会的不利益といったような、自然人に対する物的な損失、財産的な損失若しくは非財産的な損失をもたらしうる。」ため、監督機関に対し迅速な通知が必要であり、「当該個人データ侵害が自然人の権利及び自由に対する高いリスクを発生させるおそれがあるときは、当該個人が予め必要な予防策を講じることができるように、データ主体に対し、不当な遅滞なく、個人データ侵害について連絡[dd]」する必要がある。

2016 年、29 条作業部会は GDPR における侵害通知に関するガイドライン（以下ガイドラインという）を制定し、EDPB の第 1 回会合において承認されている[ee]。以下では、このガイドラインでの解説も含めて説明する。

3.1.1 監督機関への報告

まず、第 33 条で、個人情報保護の監督機関への報告を義務付け、第 34 条で本人への通知を義務付けている。

管理者は、本人の権利と自由にリスクを与えない場合を除き、不当な遅滞なく、できれば個人データ侵害に気づいた時から 72 時間以内に監督機関に通知が必要である。72 時間以内に報告されなかった場合は、その理由を付さなければならない。委託先である処理者は、侵害発見後、不当な遅滞なく、委託元である管理者に通知しなければならない。管理者は、すべての個人データ侵害を文書化し、監督機関が遵守を検証できるようにしなければならない。

[cc] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) 33 条、34 条
[dd] 前文 85、86
[ee] Guidelines on Personal data breach notification under Regulation 2016/679, WP250 rev.01
https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en （最終閲覧 2021 年 1 月 7 日）
なお、2021 年 1 月 19 日、報告すべき侵害についてガイドライン案が開示され、パブコメ募集中だが、本稿では取り上げない。

「『個人データ侵害』とは、偶発的又は違法な、破壊、喪失、改変、無権限の開示又は無権限のアクセスを導くような、送信され、記録保存され、又は、その他の取扱いが行われる個人データの安全性に対する侵害を意味する」、と定義されており、機密性、完全性だけでなく、可用性も含まれている。ガイドラインによれば、バックアップからリストアできる一時的な可用性喪失であっても個人データ侵害であり、管理者は文書化しなければならないが、個人の権利と自由に与えるリスクを分析評価して通知の要否を判断する[ff]、というステップになる。

どの時点で個人データ侵害に「気づいた」ことになるのか、について、ガイドラインは、事業者が「合理的な程度の確信を持った時」とし、前文で「その個人データ侵害の性質及び重大性、その結果として生じる事態及びデータ主体に対する悪影響を考慮に入れた上で、不当な遅滞なく通知」とされていることから「タイムリーに妥当なアクションを取れるようにどんな侵害にも気づけるように体制を整える義務がある[gg]、としている。そのうえで、いくつかの事例を挙げている；

1) 暗号化されていない USB メモリの紛失は、まだ、漏洩したかどうかわからないが可用性は失われているので「気づいて」いる。

2) 1 件の個人情報の誤送信をその受領者が証拠を示して連絡してきたときは、明確な証拠があるので「気づいて」いる。

3) 侵入の痕跡を見つけ、個人情報が侵害されていないかチェックしたところ、やはり侵害されたことを確認した。その時点で、明確な証拠があるので「気づいて」いる。

4) 身代金要求があって、システムをチェックしたところ確かに攻撃されていたことが確認されれば「気づいて」いる。外部からの連絡があって、本当に攻撃されたかどうか調査をしている間は「気づいて」いないが、連絡があってすぐに調査を始め、侵害されたかどうかが判明することが期待されている。

72 時間以内に報告できない事態は例外的なはずである理由として、下記のように説明している；

1) リスク評価：そもそも管理者は予め侵害が発生した場合のリスク評価を DPIA で実施しているはずである。

2) 前文 87 にあるように、管理者は侵害を検知し注意を向けることができるような技術的・組織的なプロセスを持つべきである。事故対応計画を含むガバナンスを実施し、社内や委託先において、事故や兆候となる事象が検知されればしかるべきレベルに報告されるようにすべきである。

処理者の管理者への報告について、ガイドラインは、具体的な期限がないのは、リスクの判断が不要だからであり、侵害に気づいたら遅滞なく通知すればよいからとする。管理者は処理者から通知を受けた時点で侵害に気づいたことになる。管理者は影響を評価するために自ら調査を希望するかもしれない、としている。そして管理者と処理者の間の契約にはどのようにこの通知を履行するか、についても規定されるべき、としている[hh]。

監督機関への報告事項は、タイムリーさ重視でよく、正確な数などの詳細は追って報告することでもよいが、通知は最終的には情報主体の損害を緩和することが目的なので、個人へのリスクを検討できるように流出した情報の種類は重要である。第一報の後、調査をして実は漏洩がなかった、ということでも、それを報告すればよい。

ガイドラインは、監督機関への報告が不要になる「本人の権利と自由にリスクを与えない場合」についても解説する。まず、既に公知となっている情報の漏洩でその開示が情報主体にリスクを生じさせない場合である。次に暗号化されている場合は鍵も窃取されていなければ、実際には読みだせないので機密性についてのリスクはないと考えられるとする[ii]。同様に、パスワードなどが高度な暗号鍵によるハッシュ関数でハッシュ化されソルトが施されている場合も解読できないのでリスクがない。しかしバックアップがなくて可用性に問題が生じるようであれば報告は必要である。暗号化されていても脆弱性のあるアルゴリズムによるものや、変更しなければデフォルト鍵で復号できるものもあるので、技術的な仕様も把握しておく必要がある[jj]。

3.1.2 情報主体への通知

ガイドラインは、情報主体への通知の主な目的は、自分を守るためのステップについての情報提供としている[kk]

①通知内容

34 条 2 項は、最低限の通知内容として以下を挙げている；

1) データ保護オフィサーの名前及び連絡先、又は、より多くの情報を入手することのできる他の連絡先

2) 侵害の結果として発生する可能性のある事態

3) 適切な場合、起こりうる悪影響を低減させるための措置を含め、その個人データ侵害に対処するために管理者によって講じられた措置又は講ずるように提案された措置

②リスク評価

情報主体への通知義務は、情報主体の権利と自由に高リスクがある場合に限られ、監督機関への報告より閾値が高い。ガイドラインは、リスク評価は、侵害の拡大防止の効果的なステップの検討と、通知の要否の判断のために必要、としている。高リスクの例として、差別、なりすまし、詐欺、財産的損害、信用失墜を挙げており、特に特別な種類の個人データとされるものの漏洩については高リスクとな

[ff] ガイドライン　8 頁
[gg] ガイドライン　11 頁
[hh] ガイドライン　14 頁
[ii] ガイドライン　18 頁。2014 年版のガイドラインでは暗号化されていても個人情報なので報告すべし、としていた。
[jj] ガイドライン　19 頁
[kk] ガイドライン　20 頁

るとしている。評価の要素としては以下のものを挙げている[ll]；

1)侵害のタイプ

2)個人情報の性質、機微さと量

単なる 1 人の氏名と住所の開示は通常は実質的な損害を起こさないが、もし養親の氏名と住所が実の親に開示されれば、養子と養親に厳しい結果となり得る、と例示している。

健康データや身分証明書、クレジットカード情報などの財務的情報の侵害もなりすましのリスクがありその組合せはよりリスクが高い。一見当たり障りのない情報でも脈絡によっては犯罪者に有益になり得る。

3)個人の特定の容易さ

単独での特定だけでなく、他の情報との組合せによる特定の容易さも考慮する。仮名化され特定するための情報が守られているので有れば、特定の可能は低い。

4)結果の重大性

なりすましや詐欺、身体への危害、精神的苦痛、信用失墜や汚辱等が引き起こされる場合や意図が不明か悪意の者が手にしているときはリスクが高い。信用できる者への誤送信で、すぐに連絡して、相手が返却するか開封しないで削除すると信用できる場合は、リスクが低く、監督機関への報告も不要かもしれないが、事故の記録は必要である。影響の永続性も判断要素である。

5)情報主体の特別な特徴

例えば子供や脆弱性のある個人やよりリスクが高くなる。

6)管理者の特徴

例えば医療機関は侵害による個人への影響が大きい

ガイドラインは、別紙に、具体的な例と、監督機関への通知、情報主体への通知、それぞれについての判断例を掲載している。また、ENISA の推奨する侵害による被害の評価方法も参考になる、としている。

③通知方法等[mm]

基本は直接の通知が必要だが、それが不相応な努力を要する場合は、本人が同様に知ることができるなら公表で代替可能である。ガイドラインは、透明性のある通知手段の例として、電子メールや SMS、ダイレクトメッセージの他、Web サイトでの目立つ告知やバナー、郵送、印刷メディアへの目立つ広告を挙げており、単なるプレスリリースや事業者のブログへの記載は個人への効果的な通知ではない、としている。影響を受ける全個人に伝達される可能性を最大化する方法を考えるべきとし、複数の手段を組み合わせてもよい、としている。

また、言語については通常のコンタクトで使われている言語とし、通常コンタクトがないか世界的に発信している場合はリソースを考えて管理者の国の言語でも許容される。侵害された通信手段を使う場合は、攻撃者によりなりすまされる可能性がることも考慮する。

④通知の時期

情報主体への通知は具体的な期限がない。前文は「そのようなデータ主体に対する連絡は、監督機関から提供されたガイダンス又は法執行機関のような監督機関以外の関連機関から提供されたガイダンスを尊重しつつ、可能な限り速やかに合理的に実現できるように、かつ、監督機関と密接に協力して、行われなければならない。」とし、情報主体の自衛のためには早期に必要だが捜査に支障があるのであれば遅らせることも正当化される、としている。また、もし、連絡先などがわからず情報主体に通知できなかったときは、可能な限り早い通知でよいとし、15 条に基づき情報主体がコンタクトしてきたときを例に挙げている。

⑤通知が不要な場合

34 条 3 項は、通知が不要な場合を規定しているが、ガイドラインは少し解説している[nn]；

1)　暗号化のように他者が判読できない場合。これにはトークン化も含まれる

2)　管理者が事後的にリスクが発生しない対策をした場合。例えば侵害発見後直ちにアクセスした者に対応する等。

3)通知に「過大な負担を要する[oo]」又は連絡先情報がない場合。通知はデータ主体が平等に効果的な態様で通知されるような広報又はそれに類する方法に変更される。この場合、オンディマンドで情報が伝わる技術的な手段も想定される、とする。

⑥処分等

管理者は第 5 条第 2 項に定める説明責任に基づき、監督機関に対しこれらを示す必要があり、監督機関は通知が必要と判断すればそれを要請することもでき、また、権限を行使し処罰することも可能である。

事業者が、これらの通知をしなかった場合、83 条 4 項に基づき、1000 万ユーロ又は全世界の売上総額の 2%以下の金額のいずれか高額の方以下の制裁金が科される可能性がある。また、GDPR の義務違反については、それによって発生した損害の賠償義務もある[pp]。

3.2 執行状況

2018 年 5 月 25 日発効後、加盟国は、侵害通知について、どのような執行をしているだろうか。

EDPB では、加盟国の決定を正式にまとめてはいないが、加盟国の監督機関が発表した記事等をまとめて掲載しているのでこれらを参考に、また、2020 年については参考まで

[ll] ガイドライン 22 頁以下
[mm] ガイドライン 21 頁
[nn] ガイドライン 22 頁　D.
[oo] 29 条委員会は、脚注で透明性についてのガイドラインを参照、としてる。
[pp] GDPR　82 条

にフランスと英国の状況[qq]も合わせて整理したのが表 1 である。

表 1　GDPR 執行状況

			2018	2019	2020			
			EDPB	EDPB	EDPB	CNIL	ICO	合計
発表された執行数			2	56	62	7	24	93
	内、セキュリティ違反		1	21	17	1	4	22
		内、侵害通知が契機			5	0	0	5
	内、侵害通知義務違反		0	2	5	1	0	6

2018 年 5 月の発効から 1 年間で 89,271 件の侵害通知が監督機関に提出されている[rr]が、セキュリティ違反の執行数がせいぜい 2 桁、ということは、通知が必ずしもセキュリティ違反に対する処分を促進する目的で義務付けられているわけではなさそうである。しかし、安全管理義務違反が問われたもののうち、侵害通知が契機となったものは、2020 年では 1/4 弱ある。侵害通知義務違反についての執行例のほとんどが、安全管理義務違反が問われると同時に通知もなかった又は遅かったことが問題になっているだけだが、侵害通知をメインに取り上げたケースが 2 件あるので、それを紹介する。

1 件目は、2019 年イタリアの電子メールサービス電子メールサービスプロバイダが詐欺的な WiFi アクセスポイントにより Web で電子メールを読むための認証情報が盗まれた事件[ss]である。同社は、侵害発見後、まず、ユーザーが PW を変更せざるを得ないように設定し、事故の説明の Web 掲出。その後、電子メールで通知したが、イタリアの監督機関は順番が逆でまず通知すべきと指摘。更に、通知は「IT システムに異常が発生したので、不正アクセスを避けるために PW を変更して下さい」という文章だけだったため、監督機関はそれでは不十分として、侵害の種類、その結果のリスク、具体的な対応方法、他のサイトで同じ認証を利用している場合の変更要請などを再度通知させた。

2 件目は、2020 年 12 月のアイルランドの監督機関の決定で、Twitter の欧州の法人であるアイルランドの Twitter International Company(TIC)社に対し、50 万ドル相当の制裁金が科された事件[tt]である。問題となったのは、アンドロイドでツイッターを使用するユーザーが、ツイッターに紐づけている電子メールアドレスを変更した場合、開示先限定の投稿の開示範囲が無限定になるバグである。

米国の Twitter Inc.は、外部からバグの情報を受け付けるプログラムを持っている。2018 年 12 月 26 日、このプログラムの運営の委託先が、寄せられたバグ情報の検証の委託先である IT セキュリティ会社にこのバグを報告した。この IT セキュリティ会社は 12 月 29 日に検証し、low risk として Twitter Inc.の情報セキュリティチームに報告したが、年末休暇のため、情報セキュリティチームが見たのは 1 月 2 日だった。セキュリティ事案でなくプライバシー事案と判断し、法務部門に相談した。3 日、Twitter Inc.の法務は、個人情報事故に該当しうるため事故対応体制を取ることを要請し、4 日、体制を取ったが、グローバル DPO が情報共有先に加えられていなかった。7 日ツイッターグループの週次ミーティングでの報告で初めてグローバル DPO が本件を知り、同ミーティングに出席していた TIC の DPO も知ることとなった。TIC としてはこの時初めて本件を知ったとしてその 19 時間後である翌日、監督機関に電子メールで報告した。報告によれば、少なくとも 88726 人の EU,EEC のユーザーが影響を受けている。

TIC は本件を知ったのは 1 月 7 日と主張したが、監督機関は、侵害通知ガイドラインによれば、侵害通知義務は事故を知るための技術的、組織的な仕組み作りも含めた義務であり、管理者である TIC は処理者である Twitter, Inc.にタイムリーに報告させる義務がある。処理者の不備は、遅れや非通知の言い訳にはならない、とし、遅くとも Twitter, Inc. の法務がプライバシー事案とコメントした 1 月 3 日には気づくべきであったとして、1 月 3 日に constructive awareness（みなし気づき）があった、とした[uu]。また、事故対応記録義務についても、雑多なセキュリティ事故と同じレベルであり、リスク分析もなく、義務を果たしていない、と判断した。

そして、「是正効果があるように制裁金を増額すべく、違反の性質、スコープ、過失の程度を考慮すべし」、とする、EDPB からの拘束力のある決定[vv]に基づき、50 万ドルの制裁金を決定した。

4. 分析と日本への示唆

4.1 政府への報告の意味

本人通知の必要性は理解できるが政府への通知の意味は何か、という冒頭の疑問について、両地域は対照的なアプローチをとっているように見える。カリフォルニア州は基本的には政府への報告は義務付けられていないが、EU は、監督機関への報告義務の方が本人への通知より閾値が低く、実質的にほとんどの事故を報告しなければならない。

[qq] https://edpb.europa.eu/news/national-news/2018_en
https://edpb.europa.eu/news/national-news/2019_en
https://edpb.europa.eu/news/national-news/2020_en
https://www.cnil.fr/en/tag/Sanctions
https://ico.org.uk/action-weve-taken/enforcement/

[rr] EDPB, *GDPR in numbers*, May 2018
https://ec.europa.eu/info/sites/info/files/infographic-gdpr_in_numbers.pdf

[ss] *Italian SA: Users must receive specific, helpful information in case of a data breach*, 7 June 2019, https://edpb.europa.eu/news/national-news/2019_en (last visited Jan. 25, 2021)

[tt] Data Protection Commission (Ireland), In the matter of Twitter International Company, IN-19-1-1 (9th day of December 2020)
https://edpb.europa.eu/sites/edpb/files/decisions/final_decision_-_in-19-1-1_9.12.2020.pdf

[uu] Data Protection Commission (Ireland)　前掲注 tt88 頁

[vv] Decision 01/2020 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding Twitter International Company under Article 65(1)(a) GDPR
https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_bindingdecision01_2020_en.pdf

個人情報保護指令下で定めていた個人情報取扱すべてについての監督機関に対する通知義務が負担だけで効果を上げなかったことから、対象を絞って侵害通知制度を導入したものである、との説明wwは、EU の官僚主義的拘りとして理解できる。更に、ガイドラインによれば、その冒頭で、「侵害通知義務は、管理者が侵害に素早く対処し、影響を最小化し、可能なら侵害された情報を回復するためであり、監督機関に関連する助言を求めるためである。72 時間以内の報告義務により管理者に情報主体への通知の要否を正しく判断できるようになる[xx]。」と、情報主体や管理者のメリットも強調している。

また、報告不要の場合は暗号化などで解読できない場合しか挙げられておらず、1 件の誤送信も、少なくとも記録し、リスク分析をし、監督機関への報告の要否について、説明責任を負うことになる。現に、Twitter 事件でも、事故の記録が不十分として 33 条 5 項違反も問題にされている。「個人情報の取り扱いは原則違法」と広く網をかけて管理者に説明責任、立証責任を負担させる[yy]、という GDPR の基本的姿勢にも通じるものがあり、米国のような事業者の予見可能性を重視した細かな規定よりも、広く網をかけて柔軟に取り締まれるようにする意図も感じられる。

とはいえ、本人に通知するという習慣がない事業者に行動を促すには政府への報告を義務付けるのが効果的であることも理解できる。通知という行為だけでなく、組織の一部での侵害への「気づき」から組織として素早く対処し影響を最小化するための技術的、組織的体制づくりまでを促進する、という意味では、72 時間以内の政府への報告のプレッシャーは意味があることであろう。Twitter の事件は、まさにその良い例である[zz]。

この点、日本の個情法は、個人情報取扱事業者の予見可能性を重視したアプローチになっていると考える。また、プライバシーマーク制度などで本人通知に慣れている事業者にとっては、社会的信用のために、法的な義務がなくても本人通知だけは行う、ということもあろう。

4.2 実務上の論点

米国もＥＵも、本人通知に必要な十分な情報を保有しない場合は、Web サイトへの目立つ掲載やマスメディアへの発表などの代替手段で通知できることとしている。連絡方法がないなら、その情報が悪用され本人に危害が加わる可能性も高くなさそうだが、たまたまその本人を知っている人が入手した場合や、旧住所からでも悪用する者もいるかもしれないので、それも必要だろう。その場合、本人が自分の情報が含まれているかどうかの問い合わせができる窓口の設置、とされているのも参考になる。なお、米国、EU とも、通知が到達したかどうかのトレースは義務付けていない。

通知の手段については、米国と EU では違いがある。米国は郵送を基本とし、電子メールは信用できないから代替手段の一要素として認めるだけだが、EU は電子メールや SMS は郵送と並列に例示されている。データ最小化原則を持つ EU では、住所まで保有しているとは限らないため、と思われる。日本において、本人通知は、社会的に丁寧とされる郵送又は訪問によるお詫びが多かったが、個情法の下、不要な情報を収集しない事業者も多いので、EU のようなアプローチが妥当であろう。米国においても州法ではそれぞれの事業者がセキュリティポリシーで通知方法を定めていればその方法でよい、と柔軟に対応している。

4.3 セキュリティ強化に向けて

GDPR 前文 87 は、「個人データ侵害が発生したかどうかを迅速に確定するため、そして、監督機関及びデータ主体に対して速やかに連絡するための全ての適切な技術的な保護及び組織上の措置が実装されているか否かが確認されなければならない。（後略）」と、事故の発見に向けた技術的な保護も求めているように見える。NRI の 2019 年日米星の比較調査によれば、米国とシンガポールでは発生したセキュリティインシデントの上位を占めるのはサイバー攻撃だが日本ではヒューマンエラーだった[aaa]。日本に攻撃がない訳がなく、単に検知していないだけではないか、と考えられる。であるならば、GDPR の求める体制づくりは日本にも参考になるであろう。

＊＊＊＊

（参考文献）

湯淺墾道「アメリカにおける個人情報漏洩通知法制に関する考察」情報ネットワーク・ローレビュー第 11 巻(2012 年 11 月) 72-87

INFORMATION SECURITY AND PRIVACY, A PTACTICAL GUIDE FOR CLOBAL EXECUTIVES, LAWYERS AND TECHNOLOGISTS (Thomas J. Shaw Esq. Ed., 2011)

EDPB, Guidelines on Personal data breach notification under Regulation 2016/679, WP250 rev.01

[ww] 石井夏生利『新版　個人情報保護法の現在と未来』（勁草書房、2017）140 頁。前文(89)を引用。(89)はプライバシーインパクトアセスメントの説明でもある。

[xx] ガイドライン　15 頁

[yy] 5 条 2 項

[zz] もちろん、米系国際プラットフォーマーに対する厳しい対応の側面もあろう。

[aaa] NRI Secure Insight 2019, https://www.secure-sketch.com/ebook-download/tag/%E8%AA%BF%E6%9F%BB%E3%83%AC%E3%83%9D%E3%83%BC%E3%83%88?__hssc=54303287.1.1593399865650&__hstc=54303287.88217294ccda08ddcfd534d0649e8cc4.1593399865650.1593399865650.1593399865650.1&__hsfp=194947021&hsCtaTracking=8f41f339-53b3-48d6-8f2a-5cd716041121%7C6e988249-1746-4a61-91bb-a6249f90ae71
金子啓子『バランスのとれた個人情報保護規範の実現に向けて』69 頁も NY 州と日本の比較において同様の推論。
http://lab.iisec.ac.jp/degrees/d/theses/iisec_d31_thesis.pdf