データ・セキュリティ NEWSLETTER

2022 年 3 月号（Vol.8）

ニューヨーク州 SHIELD Act に基づく最近の違反事例

森・濱田松本法律事務所
弁護士　林　浩美
TEL. 03 5220 1811
hiromi.hayashi@mhm-global.com
弁護士　田中 浩之
TEL. 03 6266 8597
hiroyuki.tanaka@mhm-global.com
弁護士　湯川 昌紀
TEL. 03 6266 8764
masaki.yukawa@mhm-global.com

日本国外に居住する個人のデータを保有する場合に当該個人が居住する法域のデータ保護法制の適用を受けることに留意が必要ですが、米国ニューヨーク州に居住する個人のデータについては、2019 年 10 月（一部は 2020 年 3 月）に施行された SHIELD (Stop Hacks and Improve Electronic Data Security) Act に対応する必要があります。

SHIELD Act では、違反について民事制裁金が科され得ることとなっていますが、違反事例が最近公表されており、実務上参考になる点もありますので解説致します。

Ⅰ. ニューヨーク州 SHIELD Act の概要

1. 対象となる「private information」

対象となる「private information」には、personal information（自然人に関する当該自然人を特定することができる情報）に加えて、以下の情報が含まれます。

- Social Security Number
- 運転免許証等の番号
- 口座番号、クレジットカード番号等
- 生体認証情報

2. 対象となる事業者

対象となる事業者は、private information を含むコンピュータ化されたデータを保有又はライセンスする者とされており、事業者がニューヨーク州に拠点を有する等の

要件は定められていませんので[1]、日本法人であってニューヨーク州で事業を営んでいない場合でもニューヨーク州に居住する個人のデータを保有する場合には適用され得ることになります。

なお、Gramm-Leach-Bliley Act、Health Insurance Portability and Accountability Act その他の連邦又はニューヨーク州のデータ保護法の適用を受ける場合には適用対象外になる場合があります。

３．義務の内容

対象となる事業者は、不正アクセスを本人に通知する義務と、セキュリティ対策を講じる義務を負います。

不正アクセスを本人に通知する義務[2]

対象となる事業者は、ニューヨーク州の居住者の private information が正当な権限なく取得され若しくはアクセスされ、又はこれらがあったものと合理的に考える場合には、可能な限り迅速に本人に通知する必要があります。

正当な権限を有する者が意図せず private information を開示した場合で、当該情報が不正に利用され、又は開示として経済的若しくは感情的な害を生じさせるものではないであろう場合には、本人への通知は不要とされています。ただし、本人への通知を不要とした意思決定について書面化し、少なくとも 5 年間保存すること、500 人を超えるニューヨーク州の居住者が影響を受ける場合は意思決定後 10 日以内にニューヨーク州司法長官に対して当該意思決定を届け出ることとされています。

セキュリティ対策を講じる義務[3]

対象となる事業者は、ニューヨーク州の居住者の private information の安全性（security）、機密性（confidentiality）及び完全性（integrity）を保護するために合理的な措置（private information の処分を含む。）を講じる必要があります。

具体的には、下記の(A)から(C)の措置を講じる場合には遵守すると見做すこととされています。

(A) 合理的な組織的安全管理措置

(1) 安全管理措置を管理する責任者の選任

(2) 合理的に予想される内部的及び外部的リスクの特定

[1] SHIELD Act では、それ以前の Information Security Breach and Notification Act に存在していた、ニューヨーク州で事業を営む者(any person or business or business which conducts business in New York state)という要件が削除されています。

[2] New York General Business Law（以下「NYGBL」といいます。）の Section 899-AA 2 項。https://www.nysenate.gov/legislation/laws/GBS/899-AA 参照。

[3] NYGBL の Section 899-BB 2 項。https://www.nysenate.gov/legislation/laws/GBS/899-BB 参照。

(3) 特定されたリスクをコントロールするための安全管理措置の十分性の評価
(4) 安全管理措置にしたがった従業員の教育研修と監督
(5) 外部委託先の適切な選定及び管理
(6) 業務及び環境の変化に照らした安全管理措置の見直し

(B) 合理的な技術的安全管理措置
(1) ネットワークとソフトウェアの設計におけるリスク評価
(2) 情報の処理、移転及び保存におけるリスク評価
(3) 攻撃又はシステム障害の検知、防止及び対応
(4) 主要な統制、システム及び手順の有効性の検証と監視

(C) 合理的な物理的安全管理措置
(1) 情報の保存と処分のリスク評価
(2) 侵入の検知、防止及び対応
(3) 情報の取得、移転、破棄及び処分における不正なアクセス又は利用の防止
(4) 情報が不要になった後合理的期間内の、情報の読取り又は復元ができないような処分

４．制裁の内容

義務に違反した場合には以下の制裁の対象になります。

<u>不正アクセスを本人に通知する義務の違反</u>

不正アクセスを本人に通知する義務に違反した場合、5,000 ドル又は 1 件当たり最大 20 ドル（最高 250,000 ドル）のいずれか高い方の金額の民事制裁金を科すこととされています[4]。

<u>セキュリティ対策を講じる義務の違反</u>

セキュリティ対策を講じる義務に違反した場合、1 件当たり最大 5,000 ドルの民事制裁金を科すこととされています[5]。

Ⅱ．最近公表された違反事例

2022 年 2 月 16 日、ニューヨーク州司法長官は、SHIELD Act に基づくセキュリティ対策を講じる義務の違反を行った企業との間で、当該企業がセキュリティ対策を講じること、及び 600,000 ドルを支払うという内容での和解をすることを公表しています。

[4] NYGBL の Section 899-AA 6(a)項
[5] NYGBL の Section 899-BB 2(d)項が参照する Section 350-D。

当該事案では、98,632 人のニューヨーク州居住者の情報への不正アクセスがあった可能性があるとされています（下記のように、適切なログ記録がされていない等によって不正アクセスが実際に起こったかが判明せず、フォレンジックを行っても不正アクセスがあった可能性を排除できなかったとされています。）。

具体的な違反行為としては、以下の内容が指摘されています。

- メールアカウントに多要素認証を導入していなかったこと。
- メールアカウントのパスワードの長さが不十分であり（8 文字以上であることのみになっていた。）、6 回のパスワード間違いを許容していたこと。
- 90 日を超えるログ記録ができず、メールアカウントでの個人の動きをモニタリングできていなかったこと。
- 古いデータを保存領域に移さずにメールアカウントに残していたこと。

また、当該和解では、当該企業が講じることに合意したセキュリティ対策として、パスワード管理、認証のポリシー及び手続、暗号化、ペネトレーション・テスト、ログ及びモニタリング、データ削除等が具体的に定められています。当該企業は、セキュリティ対策を少なくとも毎年見直して合理的な変更を行うこと、セキュリティ対策の実施・維持・モニタリングを行う責任者をおくこと、セキュリティ対策の実施・維持・モニタリングに責任を負うマネジメント層の従業員に対して和解による要求事項を通知すること、当該マネジメント層の従業員に対するトレーニングを行うことについても合意しています。

Ⅲ. 実務上参考になる点

個人情報保護委員会の個人情報保護法ガイドライン（通則編）8-6 では、「個人データを取り扱う情報システムを外部からの不正アクセス・・・から保護する仕組みを導入し、適切に運用しなければならない。」とされており、日本の個人情報保護法 20 条（改正後は 23 条）で講じるべき安全管理措置としても外部からの不正アクセスの防止が含まれていますが、必ずしも具体的な対策の水準が定められていませんので、外国法に基づいて求められている水準も参考になると思われます（SHIELD Act が日本法人に適用され得ることについては、上記Ⅰ．２．をご参照下さい。）。

上記の事案では、メールアカウントに多要素認証を導入していなかったことが違反であるとされていますが、総務省のテレワークセキュリティガイドライン第 5 版（令和 3 年 5 月）においても、可能な限り多要素認証を利用することが推奨されています。

また、上記の事案ではログ保存が 90 日に限られていたことと、どのデータにアクセスがあったのかが分からなかったことから不正アクセスがあったかどうかが判明しなかったことが問題視されており、事案後に当該企業は 1 年までのログ保存ができること、及びメールへのアクセスがいつされたかを特定できるように是正した（より具体的には、システム提供会社との契約内容を変更した）とされています。個人情報保護委員会の個人情報保護法ガイドライン（通則編）8-6 の手法の例示では「ログ等の定期的な

分析により、不正アクセス等を検知する」とされており、具体的な期間やログの内容までには言及されていませんが、不正アクセス（又はその可能性）を特定するまでに期間を要することがあり得ることを踏まえた対応が必要になる点で参考になると思われます。

セミナー情報

- セミナー　『金融法務懇話会・サービサー業務研究会合同オンラインセミナー 改正個人情報保護法の概要と実務対応』
  開催日時　2022 年 3 月 16 日（水）14:00～17:00
  講師　小川 智史
  主催　一般社団法人金融財政事情研究会

- セミナー　『第 4828 回金融ファクシミリ新聞社セミナー「個人データ利活用規制の最新対応実務－第三者提供規制への対応を中心として」』
  開催日時　2022 年 3 月 28 日（月）13:30～16:30
  講師　田中 浩之
  主催　株式会社 FN コミュニケーションズ

文献情報

- 本　『令和 2 年改正個人情報保護法 Q&A〔第 2 版〕』
  出版社　株式会社中央経済社
  著者　田中 浩之、北山 昇

- 論文　「個人情報保護をめぐる実務対応の最前線（第 3 回）個人データの第三者提供と共同利用をめぐる論点(1)」
  掲載誌　NBL No.1208
  著者　岡田 淳、北山 昇、小川 智史

- 論文　「改正対応！「実務に役立つ」「対話で学ぶ」個人情報保護法の基礎 (20) 委託でできること・できないこと」
  掲載誌　会社法務 A2Z 2022 年 2 月号
  著者　田中 浩之、蔦 大輔、北山 昇

- 論文　「脅威を増すランサムウエア攻撃　身代金は支払っても問題ないのか」
  関連サイト　日経 Robotics 2022 年 1 月号
  著者　蔦 大輔

NEWS

- 2022 年 2 月 18 日：蔦 大輔 弁護士のコメントが、読売新聞 34 面『[サイバーテロ　病院の危機] ＜２＞「予算ない」「知らなかった」…脆弱性　見過ごし被害』と題した記事に掲載されました

- 2022 年 1 月 10 日：田中 浩之 弁護士のコメントが、日本経済新聞 17 面『2022 年 法律・ルールこう変わる』『管理状況、詳細に　個人情報保護法』と題した記事に掲載されました

（当事務所に関するお問い合せ）
森・濱田松本法律事務所　広報担当
mhm_info@mhm-global.com
03-6212-8330
www.mhmjapan.com