

NO&T U.S. Law Update

米国最新法律情報

2020 年 6 月 No.48

ニューヨーク州におけるデータセキュリティ～SHIELD Act の施行～

弁護士 塚本 宏達

弁護士 加藤 嘉孝

はじめに

2019 年 7 月、ニューヨーク州住民のプライバシー情報保護及び企業におけるサイバーセキュリティの強化を内容とする、Stop Hacks and Improve Electronic Data Security Act (以下、「SHIELD Act」といいます。))が制定され、2020 年 3 月 21 日に全面施行となりました。2018 年 6 月にカリフォルニア州消費者プライバシー法 (California Consumer Privacy Act (以下、「CCPA」といいます。)) が、2019 年 1 月にマサチューセッツ州における消費者データプライバシーに関する法律 (An Act Relative to Consumer Data Privacy) がそれぞれ制定されており、現在米国の各州において包括的な個人情報保護を目的とした州法が成立又は施行されたり、州議会において議論が行われたりしています。連邦レベルにおける包括的な個人情報保護に関する法律に関しても、現在連邦議会において議論が行われていますが、上記のとおり州法による対応が先行しているため、米国において事業を行う日本企業としては、個人情報保護に関する各州法について、保護される個人情報の範囲や適用のある事業者の範囲に注意して適用の有無及び課せられる義務の内容を検討する必要があります。

SHIELD Act も、上記州法と同様に、個人情報保護を目的とした州法ですが、米国経済の中心地であるニューヨーク州で制定された州法であることに加えて、後述するとおり広範な適用範囲を有することから、ニューヨークに拠点を構えている日本企業のみならず、米国において事業を営んでいる日本企業のサイバーセキュリティの実務に広く影響を与える可能性があるため、本ニュースレターにてその概要を紹介します。

SHIELD Act の概要

SHIELD Act は、①従前から存在するプライバシー情報に関するデータ侵害を防止するニューヨーク州データ侵害通知法 (New York Data Breach Notification Law) の改正及び②プライベート情報に対するセキュリティ、守秘性及び完全性の保護のための合理的なセーフガードの構築義務、という主に二つの内容で構成されています。

1. SHIELD Act の概要①～データ侵害通知法の改正

データ侵害通知法は、プライバシー情報を含むコンピュータ化されたデータを保有又は使用する人又は事業者が「システムセキュリティの侵害」(breach of the security of the system) があったことを認識した場合には、侵害されたプライベート情報 (private information) を有するニューヨーク州住民に対して、通知をしなければならない旨を定めています¹。SHIELD Act はデータ侵害通知法を以下のとおり改正し、その適用範囲を拡大しています。なお、下

¹ New York General Business Law §899-aa Section 2

記データ侵害通知法の改正に関する内容は 2019 年 10 月 23 日より施行されています²。

(1) プライベート情報の定義の拡大

改正前のデータ侵害通知法は、「プライベート情報」(private information) について、下記で述べるデータ要素の一つ又は複数と組み合わせられた情報から構成される個人情報 (personal information)³ であって、当該個人情報又はデータ要素が暗号化されていないか又は既に取得された暗号キーによって暗号化されているもの、と定義されていました⁴。列挙されているデータ要素は以下のとおりです。

- (a) ソーシャルセキュリティナンバー
- (b) 免許証番号又はノンドライバライセンス (non-driver identification card) の番号
- (c) 個人の金融口座にアクセスすることが可能になるセキュリティコード、アクセスコード、又はパスワードと結びついた口座番号、又はクレジットカード若しくはデビットカードの番号

しかし、SHIELD Act によって、プライバシー情報の定義が改正され、以下のとおりその範囲が拡大されることになりました。

- ① 暗号化に関する要件について、既に取得された暗号キーのみならず、アクセスされた暗号キーによって暗号化されている場合もプライベート情報に該当することとなりました⁵。
- ② データ要素について、上記(a)乃至(c)に加えて新たに以下の内容が追加されました⁶。
 - (d) 追加の識別情報等なく個人の金融口座にアクセスすることができる状況が存在する場合における、口座番号、又はクレジットカード若しくはデビットカードの番号
 - (e) 生体情報 (個人の特定に使用される指紋、声紋等の個人特有の身体的特徴を電子的に計測することによって生じたデータを意味します。)
- ③ オンラインアカウントにアクセスすることができるパスワード等と結びついたユーザーネーム又は E メールアドレスは個人情報やデータ要素と関連付けることなく、プライバシー情報として定義されました⁷。

(2) 適用のある事業者の範囲

データ侵害通知法は、プライベート情報を含むコンピュータ化されたデータを所有又はライセンスされているニューヨーク州において事業を営む人又は事業者に適用されると定めていましたが、SHIELD Act では、「ニューヨーク州において事業を営む (conducts business in New York state)」という要件が削除されました⁸。

(3) 権限のないアクセスの追加

データ侵害通知法は、「セキュリティシステムの侵害」を、事業者によって保持されているプライベート情報⁹のセキュリティ、守秘性又は完全性を構成するコンピュータ化されたデータを権限なく取得することと定義されていました。しかし、SHIELD Act は、権限のない取得に加えて、権限なく当該データにアクセスすることを「セキュリティシ

² SHIELD Act §6

³ 自然人に関するものであり、氏名、番号、個人的マーク又はその他識別子によって当該自然人を特定するために使用することができる情報を意味するとされています (改正前の New York General Business Law §899-aa Section 1 (a))。

⁴ 改正前の New York General Business Law §899-aa Section 1 (b)

⁵ New York General Business Law §899-aa Section 1 (b)(i)。また、暗号化の対象が個人情報又はデータ要素のいずれかとされていたものが、データ要素又は個人情報とデータ要素が組み合わせられたものとされました。

⁶ New York General Business Law §899-aa Section 1 (b)(i) (4)及び(5)

⁷ New York General Business Law §899-aa Section 1 (b)(ii)

⁸ New York General Business Law §899-aa Section 2

⁹ SHIELD Act 改正前は個人情報と規定されていましたが、SHIELD Act による改正によってプライベート情報と修正されました。

システムの侵害」に追加しました¹⁰。

(4) 制裁金の増額と出訴制限期間の延長

データ侵害通知法では、州司法長官が、同法に違反した事業者に対して、違反行為の差し止め、そして故意又は未必の故意をもって同法に違反した場合には制裁金 (civil penalty) を求めて、裁判所に提訴することを認めています¹¹。制裁金は、5,000 ドル又は 1 件につき 10 ドル (但し、上限は 15 万ドル) のいずれか大きい金額とされており、提訴期限は、申立てのあった行為があった日又は当該行為が明らかとなった日から 2 年とされていました。

SHIELD Act は、州司法長官の権限を強化し、1 件当たりの制裁金の額を 20 ドル、上限 25 万ドルに増額し、提訴期限についても、州司法長官が違反の事実について認識した日又はニューヨーク州住民から同法に基づく通知があったことを州司法長官に知らせる通知が送られた日のいずれか早い日から 3 年と延長されました¹²。

2. SHIELD Act の概要②～合理的なセーフガードの構築

データ侵害通知法の改正に加えて、SHIELD Act は、事業者に対して、事業者が保有するプライベート情報の保護を目的とした合理的なセーフガードの構築を義務付けています。具体的には、ニューヨーク州住民のプライベート情報を含むコンピュータ化されたデータを保有する人又は事業者は、プライベート情報のセキュリティ、守秘性及び完全性を保護するために合理的なセーフガードを構築し、それを実施及び維持することが義務付けられています (以下、「セーフガード構築義務」といいます。)¹³。したがって、SHIELD Act においては、具体的なプライバシー情報の侵害がなくても、事業者が合理的なサイバーセキュリティシステムを構築していない場合に罰則が適用されうることに留意する必要があります。

SHIELD Act では、データセキュリティに関する連邦法又は州法¹⁴の対象となりこれらを遵守しているエンティティ以外は、以下に掲げるデータセキュリティプログラムを実施している場合に、セーフガード構築義務を遵守しているとみなされる旨を定めています¹⁵。

- ① 合理的な運営上のセーフガード (reasonable administrative safeguard)
セキュリティプログラムを調整するための 1 人以上の従業員を任命すること、合理的に予測可能な内部的及び外部的リスクを特定すること等。
- ② 合理的な技術上のセーフガード (reasonable technical safeguard)
ネットワーク及びソフトウェアデザインにおけるリスクを評価すること、情報処理、送信及び保存におけるリスクを評価すること等。
- ③ 合理的な物理上のセーフガード (reasonable physical safeguard)
不法アクセスの発見、防止及び対応、事業目的上不要になってから合理的期間内におけるプライベート情報の処分等。

SHIELD Act は、小規模事業者 (small business)¹⁶におけるセーフガード構築義務の遵守に関しては、小規模事業

¹⁰ New York General Business Law §899-aa Section 1 (c)

¹¹ 改正前の New York General Business Law §899-aa Section 6 (a)。さらに、差し止め訴訟において、裁判所は、通知を受けることができた者が通知をなされなかった場合に被った現実の損害に対する損害賠償を命じることができるとされています。

¹² New York General Business Law §899-aa Section 6 (a) 及び (c)

¹³ New York General Business Law §899-bb Section 2 (a)

¹⁴ SHIELD Act では、金融機関における個人情報の保護に関するルールを定めているグラム・リーチ・ブライリー法 (Gramm-Leach-Bliley Act)、患者のセンシティブな健康情報の保護に関するルールを定めている医療保険の相互運用と説明責任に関する法律 (Health Insurance Portability and Accountability Act) 等が列挙されています (New York General Business Law §899-bb Section 2 (b) (i))。

¹⁵ New York General Business Law §899-bb Section 2 (b) (ii)

¹⁶ 従業員が 50 人未満、直近 3 年における年間総売上が 300 万ドル未満、又は GAAP に基づき計算された事業年度末における総資産の額が 500 万ドル未満の人又は事業者を意味すると定義されています (New York General Business Law §899-bb Section 1 (c))。

者が、その事業の規模及び複雑性、活動の性質及び範囲並びに小規模事業者が顧客から収集する個人情報又は顧客に関する個人情報のセンシビリティに応じて適切かつ合理的な運営上、技術上及び物理上のセーフガードを含むセキュリティプログラムを有していれば、当該義務を遵守したとされる旨を規定しています¹⁷。日本企業の米国子会社では、小規模事業者に該当する場合もあるかと思われますが、その場合に必要とされるセーフガードの具体的内容は、上記事情を考慮の上、小規模事業者が営む事業の内容に応じて判断することになると思われます。

セーフガード構築義務に違反した場合、州司法長官は、違反行為の差し止め及び各違反につき 5,000 ドル以下の制裁金を求めて、訴訟を提起することが認められています¹⁸。上記内容については 2020 年 3 月 21 日から施行されました¹⁹。

実務上のポイント

1. CCPA との相違点

2018 年 6 月に成立し、その後の修正を経て、2020 年 1 月 1 日から施行されている CCPA²⁰は、これまでの米国企業が一般に行ってきた消費者プライバシー保護の実務よりも厳格な内容が規定されており、加えてプライバシー情報を侵害された消費者によるクラスアクションの提訴が可能となっていることから、米国において事業を営む企業に大きな影響を与えています。そこで、SHIELD Act と CCPA の主要な相違点を紹介します。

(1) 個人の権利規定

CCPA では、事業者の情報収集時の通知義務、プライバシーポリシーの開示義務等のみならず、消費者が、収集された個人情報の種類及び具体的な情報、収集・販売の事業・商業上の目的等の開示を事業者に対して請求する権利や個人情報の削除を請求する権利等が規定されています。一方で、SHIELD Act の主な内容は、セキュリティシステムの侵害があった場合の事業者による NY 州住民に対する通知及び事業者における合理的なセーフガードの構築義務であり、プライバシー情報の主体である個人に対して、事業者に対する具体的な請求権等を与える内容は規定されていません。

(2) 事業者の範囲

CCPA が適用される事業者は、消費者の個人情報を取得し、その処理の目的と手段を決定する営利企業であり、一定の事業規模水準又は個人情報の利用等の要件²¹を満たす事業者とされています。一方で、SHIELD Act はニューヨーク州において事業を営んでいるか否かを問わず、プライベート情報をコンピュータ化している事業者に対して適用があります。したがって、SHIELD Act では、事業者が事業上個人情報をどのように利用しているかという点を要件にしておらず、また、小規模事業者であっても、SHIELD Act の適用があることに留意する必要があります。

(3) 雇用関連情報に対する適用

CCPA では、2021 年 1 月 1 日までの時限措置として雇用関連情報への適用が除外されています。一方で、SHIELD Act にはそのような適用除外規定がないため、たとえば、消費者から個人情報を取得する機会が乏しい BtoB ビジネスであっても、ニューヨーク州住民を雇用する場合には SHIELD Act が適用される可能性があることに留意する必要があります。

¹⁷ New York General Business Law §899-bb Section 2 (c)

¹⁸ New York General Business Law §899-bb Section 2 (d)及び§350-d

¹⁹ SHIELD Act §6

²⁰ なお、2020 年 6 月 1 日付で、カリフォルニア州司法長官局から CCPA の最終規則案がカリフォルニア州行政法局に提出されました。カリフォルニア州行政法局によって当該規則が承認されれば、カリフォルニア州務長官に提出され、施行される予定です (<https://www.oag.ca.gov/privacy/ccpa>)。

²¹ 具体的には、年間売上高が 2,500 万ドル超、年間合計 5 万件以上の消費者、世帯若しくはデバイスの個人情報を商業目的で購入し、受領し、販売し又は共有している、又は年間売上高の 50%以上を個人情報の販売から得ている企業とされています。

(4) 私的訴権 (Private Right of Action)

CCPA では、一定の場合に消費者が事業者に対してクラスアクションを提起することが可能とされています。しかし、SHIELD Act では、データ侵害通知法において私的訴権は明示的に規定されておらず、セーフガード構築義務に関しては、法律上明示的に私的訴権を否定しています²²。

(5) 合理的なセキュリティの内容

CCPA では、直接的に事業者に対して合理的なセキュリティを構築する義務を規定しているわけではありませんが、個人情報保護のために個人情報の性質上適切な合理的セキュリティプラクティス及び手続きを実施及び維持する義務に違反した場合には、クラスアクションの対象となる旨が規定されています。しかしながら、かかる合理的セキュリティプラクティスの内容は具体的に規定されていません。一方で、SHIELD Act では、上記で述べたとおり、合理的なセーフガードの内容について、三つのカテゴリーに分けて具体的な例示が法律上規定されています。

2. セーフガード構築義務への対応

前述のように、SHIELD Act は合理的なセーフガードの内容について具体的な例示がなされていますが、そのうち合理的な物理上のセーフガードの具体的な内容として、事業目的上不要となった情報の処分が規定されています。しかし、企業の情報管理上、事業目的上不要となったか否かにかかわらず、一定期間は取得した情報を保存しておくことを義務付けている場合が多いと考えられ、また、リティグレーション・ホールドによる訴訟関連文書の保存義務のように法令上一定期間の情報保存義務が課せられる場合も考えられます。これらの情報保存義務と上記セーフガードの関係についてどのように調整するのか今後検討が必要と思われます。

3. 新型コロナウイルスによる影響とサイバーセキュリティ

新型コロナウイルスの影響によって、米国ではリモートワークによる在宅勤務を行っている企業が急増しており、サイバー犯罪者らが新たにリモートワークに取り組んでいる従業員をターゲットにすることも危惧されています。合理的なセーフガードの構築義務は2020年3月21日より施行されていますので、米国において新型コロナウイルスのパンデミックが本格化する以前から、SHIELD Act の適用を受ける事業者は必要な準備を進めていたと思われますが、在宅勤務下におけるサイバーセキュリティの構築、従業員に対するセキュリティ意識の教育・強化等の必要性がより高まっていると考えられます。

以上

2020年6月10日

²² New York General Business Law §899-bb Section 2 (e)

[執筆者]

**塚本 宏達**（弁護士・NY オフィス共同代表）

hironobu_tsukamoto@noandt.com

1998 年京都大学法学部卒業。2005 年 The University of Chicago Law School 卒業(LL.M.)。2005 年～2007 年に Weil, Gotshal & Manges LLP（シリコンバレーオフィス）に勤務。2000 年弁護士登録（第一東京弁護士会）、長島・大野・常松法律事務所入所。2015 年より長島・大野・常松法律事務所ニューヨークオフィス（Nagashima Ohno & Tsunematsu NY LLP）共同代表。ニューヨークを拠点として、日系依頼者が米国において事業活動を行うことに関連して生じる様々な問題について、紛争対応を含めて継続的に助言をしている。

**加藤 嘉孝**（弁護士・アソシエイト）

yoshitaka_kato@noandt.com

2009 年大阪大学法務部卒業。2011 年京都大学法科大学院終了。2019 年 University of Virginia School of Law 卒業（LL.M.）。2012 年長島・大野・常松法律事務所入所。2019 年より長島・大野・常松法律事務所ニューヨークオフィス（Nagashima Ohno & Tsunematsu NY LLP）勤務。入所以来、M&A、ファイナンス取引、租税法分野を中心とした案件に携わる。近時はニューヨークを拠点として、日本及び米国のクライアントに対して、クロスボーダー取引を含む企業法務全般に関するリーガルサービスを提供している。

本ニュースレターは、各位のご参考のために一般的な情報を簡潔に提供することを目的としたものであり、当事務所の法的アドバイス構成するものではありません。また見解に亘る部分は執筆者の個人的見解であり当事務所の見解ではありません。一般的情報としての性質上、法令の条文や出典の引用を意図的に省略している場合があります。個別具体的事案に係る問題については、必ず弁護士にご相談ください。

www.noandt.com

NAGASHIMA OHNO & TSUNEMATSU NY LLP

450 Lexington Avenue, Suite 3700

New York, NY 10017, U.S.A.

Tel: +1-212-258-3333 (代表) Fax: +1-212-957-3939 (代表) Email: info-ny@noandt.com



Nagashima Ohno & Tsunematsu NY LLP は、米国における紛争対応や日米間の国際取引について効率的な助言を行うことを目的に、長島・大野・常松法律事務所のニューヨーク・オフィスの事業主体として 2010 年 9 月 1 日に開設されました。米国の法務事情について精緻な情報収集を行いつつ、米国やその周辺地域で法律問題に直面する日本企業に対して、良質かつ効率的なサービスを提供しています。

長島・大野・常松 法律事務所

〒100-7036 東京都千代田区丸の内二丁目 7 番 2 号 J P タワー

Tel: 03-6889-7000 (代表) Fax: 03-6889-8000 (代表) Email: info@noandt.com



長島・大野・常松法律事務所は、約 500 名の弁護士が所属する日本有数の総合法律事務所です。東京、ニューヨーク、シンガポール、バンコク、ホーチミン、ハノイ及び上海にオフィスを構えるほか、ジャカルタに現地デスクを設け、北京にも弁護士を派遣しています。企業法務におけるあらゆる分野のリーガルサービスをワンストップで提供し、国内案件及び国際案件の双方に豊富な経験と実績を有しています。

NO&T U.S. Law Update ～米国最新法律情報～の配信登録を希望される場合には、
<<https://legal-lounge.noandt.com/portal/subscribe.jsp>>よりお申込みください。本ニュースレターに関するお問い合わせ等につきましては、<newsletter-us@noandt.com>までご連絡ください。なお、配信先としてご登録いただきましたメールアドレスには、長島・大野・常松法律事務所からその他のご案内もお送りする場合がございますので予めご了承くださいます。