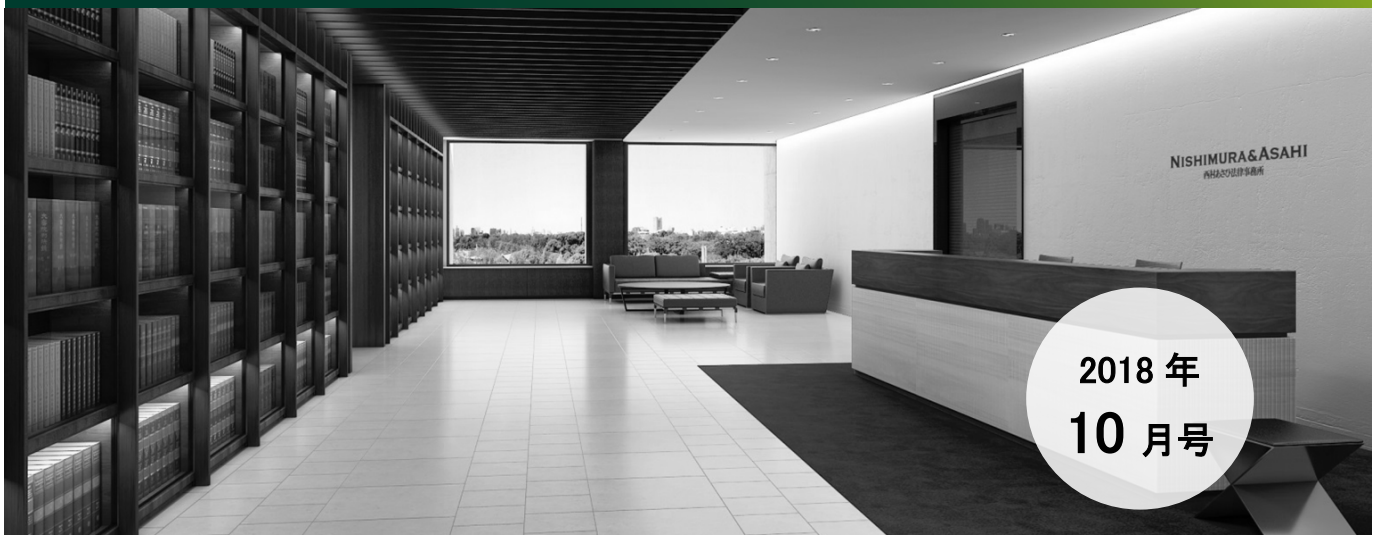
ロボット/AI ニューズレター



米カリフォルニア州の IoT セキュリティ法について(日本語仮訳)

執筆者:福岡 真之介、北條 孝佳、沼澤 周

1 カリフォルニア州において IoT セキュリティ法が成立

2018 年 9 月 28 日、アメリカのカリフォルニア州において、IoT 機器(コネクテッドデバイス:接続機器)に対するセキュリティ強化を目的とした新しい法律(IoT セキュリティ法)が成立しました。本法律は 2020 年 1 月 1 日から施行され、IoT 機器の製造業者は、IoT 機器ごとに異なるパスワードを設定するか、利用者が初めて使用する前に独自のパスワードを設定するなどの機能を付加することが義務付けられるようになります。本法律は、カルフォルニア州民法第 3 編第 4 部に追加されるものです。

本法律は、曖昧な部分も見られますが、それらは今後の適用や IoT 機器の製造業者の動向によって明確になっていくものと考えられます。

IoT 機器については、メモリ容量等のリソースが少なく、サイバー攻撃を受けたとしてもアクセスログ等のサイバー攻撃の痕跡が残りにくくなっています。セキュリティの設定も脆弱であり、IoT 機器そのもののハッキングにより、IoT 機器内の情報が窃取・改ざん・削除されるおそれや、IoT 機器を踏み台とした第三者に対するサイバー攻撃の問題点が指摘されているところであり、本法律は、これらの問題点の基礎的な対策を義務付けることになると考えられます。

シリコンバレーを含むカリフォルニア州の規模、影響力を考えますと、各州における IoT 機器のセキュリティに関するスタンダード基準が事実上設定されたに等しく、IoT 機器のセキュリティ強化の動きが活発化すること、さらには、世界各国の立法化にも波及する可能性もあるため、今後の動向に注視する必要があると考えられます。

日本企業であっても、カリフォルニア州において販売する接続機器を製造する者等には対象となりえますので(下記「製造業者」の定義参照)、本法律の影響を受けることになります。

2 カリフォルニア州 IoT セキュリティ法の仮訳 [1]

TITLE 1.81.26. 接続機器(コネクテッドデバイス)のセキュリティ

[1] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327

1798.91.04

(a) 接続機器の製造業者は、当該機器に合理的なセキュリティ機能又は以下のすべての機能を備えていなければならない。
  (1) 機器の性質及び機能に適するもの
  (2) 収集し、保持し、又は送信することができる情報に適するもの
  (3) 機器及び機器に含まれる全ての情報を、不正アクセス、破壊、使用、変更又は開示から保護されるように設計されたもの

(b) (a)項各号の全ての要件を満たすことを条件に、接続される機器が LAN 外からのアクセスに対して認証機能を備えている場合には、以下のいずれかの要件が満たされる場合、当該認証機能は、(a)項に基づく合理的なセキュリティ機能であるとみなす。
  (1) あらかじめ設定されたパスワードが、製造された機器ごとに固有のものであること
  (2) 当該機器に初回アクセス時にユーザが新たな認証手段を生成しなければならないセキュリティ機能を備えていること

1798.91.05.

本章の目的に照らし、次の用語は、次の意味を有するものとする。

(a) 「認証」とは、情報システム内のリソースにアクセスするユーザ、プロセス又は機器の権限を検証する方法を意味するものとする。

(b) 「接続機器」とは、直接又は間接にインターネットに接続することができ、かつ、IP アドレス又はブルートゥースアドレスを割り当てられた機器その他の物理オブジェクトを意味するものとする。

(c) 「製造業者」とは、カリフォルニアにおいて販売若しくは販売の申込みがされている接続機器を製造する者又は第三者のために製造するために当該第三者と契約する者を意味するものとする。本項の目的に照らし、第三者のために製造することに係る当該第三者との契約は、接続機器の購入のみのための契約、又は接続機器の購入及びブランド付与のみのための契約を含まない。

(d) 「セキュリティ機能」とは、機器に対してセキュリティを提供するよう設計された機器の機能を意味するものとする。

(e) 「不正アクセス、破壊、使用、変更又は開示」とは、ユーザが許可していないアクセス、破壊、使用、変更又は開示を意味するものとする。

1798.91.06

(a) 本章は、ユーザが接続機器に追加することを選択した、関係のないサードパーティー製のソフトウェア又はアプリケーションに関連して、接続機器の製造業者に何らかの義務を課すものと解されてはならないものとする。

(b) 本章は、電子ストア、ゲートウェイ、マーケットプレイス又はその他のソフトウェア若しくはアプリケーションの購入若しくはダウンロードの提供業者に対し、本章の遵守の審査又は実施をすることについて、何らかの義務を課すものと解されてはならないものとする。

(c) 本章は、接続機器の製造業者に対し、ユーザの裁量により機器上で実行されるソフトウェア又はファームウェアを変更する機能を含め、ユーザが接続機器に対して完全に制御できないようにするための何らかの義務を課すものと解されてはならないものとする。

(d) 本章は、連邦政府機関がその規制権限に基づいて公布した連邦法、規則又はガイダンスに基づくセキュリティ要件の対象となる機能を有する接続機器には適用されないものとする。

(e) 本章は、訴訟を提起する私的権利の根拠を付与するものと解されてはならないものとする。司法長官、市検事、郡法律顧問又は地方検事は、本章を執行する排他的権限を有する。

(f) 本章により課される義務及び責任は、他の法律に基づいて課されるその他の義務又は責任に累積するものであり、いずれの当事者も他の法律に基づいて課される義務又は責任から免除されるものと解されてはならないものとする。

(g) 本章は、法令又は管轄裁判所の命令により権限を付与された、製造業者から接続機器情報を取得する法執行機関の権限を制限するものと解されてはならないものとする。

(h) 1996 年連邦健康保険継続責任法(HIPAA 法)又は医療情報の機密保持法(Div.1 Par.2.6 (Sec.56 以降))の適用対象となる法人、医療提供者、共同事業者、医療サービス計画、請負業者、雇用主、又はその他の個人は、これらの法律により規制される活動に関して、本章の適用を受けないものとする。

(i) 本章は、2020 年 1 月 1 日に施行する。

3　カリフォルニア州 IoT セキュリティ法の原文

TITLE 1.81.26. Security of Connected Devices

1798.91.04

(a) A manufacturer of a connected device shall equip the device with a reasonable security feature or features that are all of the following:
  (1) Appropriate to the nature and function of the device.
  (2) Appropriate to the information it may collect, contain, or transmit.
  (3) Designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure.

(b) Subject to all of the requirements of subdivision (a), if a connected device is equipped with a means for authentication outside a local area network, it shall be deemed a reasonable security feature under subdivision (a) if either of the following requirements are met:
  (1) The preprogrammed password is unique to each device manufactured.
  (2) The device contains a security feature that requires a user to generate a new means of authentication before access is granted to the device for the first time.

1798.91.05. For the purposes of this title, the following terms have the following meanings:

(a) "Authentication" means a method of verifying the authority of a user, process, or device to access resources in an information system.

(b) "Connected device" means any device, or other physical object that is capable of connecting to the Internet, directly or indirectly, and that is assigned an Internet Protocol address or Bluetooth address.

(c) "Manufacturer" means the person who manufactures, or contracts with another person to manufacture on the person's behalf, connected devices that are sold or offered for sale in California. For the purposes of this subdivision, a contract with another person to manufacture on the person's behalf does not include a contract only to purchase a connected device, or only to purchase and brand a connected device.

(d) "Security feature" means a feature of a device designed to provide security for that device.

(e) "Unauthorized access, destruction, use, modification, or disclosure" means access, destruction, use, modification, or disclosure that is not authorized by the consumer.

1798.91.06

(a) This title shall not be construed to impose any duty upon the manufacturer of a connected device related to unaffiliated third-party software or applications that a user chooses to add to a connected device.

(b) This title shall not be construed to impose any duty upon a provider of an electronic store, gateway, marketplace, or other means of purchasing or downloading software or applications, to review or enforce compliance with this title.

(c) This title shall not be construed to impose any duty upon the manufacturer of a connected device to prevent a user from having full control over a connected device, including the ability to modify the software or firmware running on the device at the user's discretion.

(d) This title shall not apply to any connected device the functionality of which is subject to security requirements under federal law, regulations, or guidance promulgated by a federal agency pursuant to its regulatory enforcement authority.

(e) This title shall not be construed to provide a basis for a private right of action. The Attorney General, a city attorney, a county counsel, or a district attorney shall have the exclusive authority to enforce this title.

(f) The duties and obligations imposed by this title are cumulative with any other duties or obligations imposed under other law, and shall not be construed to relieve any party from any duties or obligations imposed under other law.

(g) This title shall not be construed to limit the authority of a law enforcement agency to obtain connected device information from a manufacturer as authorized by law or pursuant to an order of a court of competent jurisdiction.

(h) A covered entity, provider of health care, business associate, health care service plan, contractor, employer, or any other person subject to the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Public Law 104-191) or the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) shall not be subject to this title with respect to any activity regulated by those acts.

(i) This title shall become operative on January 1, 2020.

ふくおか　しん の すけ
福岡　真之介
西村あさひ法律事務所　パートナー弁護士
s_fukuoka@jurists.co.jp

1996 年東京大学法学部第 1 類卒業。1998 年弁護士登録。2001 年西村あさひ法律事務所に所属。2006 年デューク大学ロースクール卒業(LL.M.)、2006-2007 年シュルティ・ロス・アンド・ゼイベル法律事務所(米国)勤務、2007-2008 年ブレーク・ドーソン法律事務所(オーストラリア)勤務。著書は、『AI の法律と論点』(商事法務・2018)、『IoT・AI の法律と戦略』(商事法務・2017)等多数。

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

2015 年弁護士登録。2016 年西村あさひ法律事務所に所属。危機管理、社内不祥事等の企業法務に従事。特に情報漏洩をはじめとする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アドバイスを行っている。2000-2014 年警察庁勤務。元警察庁技官。NTT 情報流通プラットフォーム研究所出向、警察大学校警察情報通信研究センター、東京大学生産技術研究所との共同研究等に従事し、数多くのサイバー攻撃事案を経験。

ぬまざわ　しゅう
沼澤　周
西村あさひ法律事務所　弁護士
s_numazawa@jurists.co.jp

2015 年弁護士登録。著書は、『AI の法律と論点』(商事法務・2018)等。知的財産権や技術関連(AI、自動運転関連技術等を含む)の取引・紛争、個人情報保護法等のデータ保護法制に係る案件、その他ベンチャー支援を含む一般企業法務を取り扱う。