カリフォルニア州 IoT セキュリティ法に関する若干の考察

情報セキュリティ大学院大学教授
湯　淺　墾　道
YUASA Harumichi

Ⅰ　はじめに

本稿は，2018 年９月に制定され 2020 年１月から施行される予定のカリフォルニア州法である「接続される機器（コネクテッド・デバイス）のセキュリティに関する法律」[1]（以下，「IoT セキュリティ法」）の内容を紹介すると共に，若干の考察を加えることを目的とする。

IoT セキュリティ法は，インターネットに接続される機器（コネクテッド・デバイス）のセキュリティを規制するものとしては全米初の州法であり，コネクテッド・デバイスの製造者に対して，合理的な（reasonable）セキュリティ機能を装備させることを義務づけるものである。また接続される機器がローカルエリアネットワークの外部に認証手段を備えている場合，製造者に対して，１台１台の機器の固有のパスワードを割り当てるか，デフォルトのパスワードのままでは接続して使用することができないようにすることを求めている。本法は，カリフォルニア州民法第３節第４部に追加されることとされており，事業者の義務を規定しているが違反した場合の罰則は置かれていない。

本法をセキュリティ・バイ・デザイン，またはプライバシー・バイ・デザインを具現化するものとして評価する議論がある一方で，本法はわずか３条を民法典について追加するものであって，条文の文言の曖昧さや規制の実効性への疑念も指摘されている。

このため，本稿では IoT セキュリティ法について，内容や定義について検討すると共に，わが国の立法化に向けた示唆についても若干の考察を加えることにしたい。

なお本法については本稿末に仮訳を示したが，他にも仮訳が公表されている[2]。

Ⅱ　本法の概要

本法は，インターネットに接続される機器をカリフォルニア州内で販売するために製造する事業者に対して，機器の性質及び機能に適するもので，収集・包有又は発信することができる情報にふさわしく，かつ機器及び機器に含まれる情報を不正アクセス・破壊・使用・改変または開示から保護するように設計された合理的なセキュリティ機能を装備させることを義務づけるものである。

以下に本法の概要を紹介すると共に，論点について検討を試みたい。

１　本法の適用対象事業者

本法でいう接続される機器とは，「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，インターネットプロトコル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」と定義される。また本法の規制の対象となるのは，当該機器の製造者であるが，

1）　2018 Cal. Legis. Serv. Ch. (S.B. 327)(to be codified at Cal. Civ. Code § 1798.91.04(a)).

2）　福岡真之介＝北條孝佳＝沼澤周（訳）「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）」。https://www.jurists.co.jp/sites/default/files/newsletter_pdf/ja/ja_newsletter_1810_2_robotics-artificial-intelligence.pdf

「カリフォルニアにおいて販売または販売の申込がなされている接続機器を製造する者，または他人と契約して当該他人のために製造する者を意味するものとする。」とされており，カリフォルニア州で販売する製造者はすべて規制対象となる。また，OEM その他の形態によって製造する場合も，規制の対象となる。

一方で，本法における製造事業者の規制対象には例外も多い。

まず，「接続される機器にユーザーの選択によって追加される無連携のサードパーティーのソフトウェアまたはアプリケーションに関連する接続される機器の製造者に義務を課すものとは解釈されないものとする。」とされており，製造事業者は無連携のサードパーティーのソフトウェアまたはアプリケーションには責任を負わない。しかし，ここでいう「無連携の」の定義は示されていないので，どのような状態が「無連携」となるのかが明らかではない。ユーザーが機器を購入した後，新たに当該機器にソフトウェアまたはアプリケーションをインストールした場合には製造事業者は責任を負わないと解するのが自然ではあるが，サードパーティーのソフトウェアまたはアプリケーションに認証制度を有しているような場合「無連携」といえるのかどうかが問題となる。たとえば，Amazon の Connected Device Certification program[3] のようにサードパーティーのソフトウェアまたはアプリケーションを認証するプログラムがある場合，単に自社の基準を充たしているかどうかを認証するだけであって当該ソフトウェアやアプリケーションのインストールを促すものではないから「無連携」なのか，インストールすることを前提として認証しているのであるから連携しているものとして規制対象となるのか，現時点では明らかではない[4]。

また，「本項の目的に照らし，他人に代わって製造することに係る他人との契約は，接続される機器の購入，または接続される機器の購入及びブランド付与のみの契約を含まない。」としているので，自らは製造せずに他の事業者が製造した製品を購入して販売するのみの事業者は，本法の規制の対象を免れることになる。このため，輸入販売事業者，再販売事業者は本法の「本法の遵守の審査または執行」に関する義務の適用対象外となると解される。

2　本法の適用対象機器と例外

本法は，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，インターネットプロトコル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適用対象とする。IoT 機器類は，産業用の大規模なものから家庭で使用されるような小規模なものまで規模の大小差があり，種類もさまざまであるが，本法では特に限定は付していない。このため，本法の条文を読むかぎりでは，適用例外とされているものを除いて IoT 機器類は一律に規制に服することになる。しかし，産業用の IoT 機器やコネクテッド・カーのようなものまで本法の適用対象となるのかについては，疑念の声も上がっている。ただし「その機能性が，その執行権限に従って連邦政府機関により公布された連邦法，規則またはガイダンスに基づくセキュリティ要件の対象となる接続機器には，適用されない。」とも規定されているため，これらの産業用の IoT 機器やコネクテッド・カーのような大型 IoT 機器については何らかの連邦法やガイドライン等の規制対象となっていることから，本法の適用対象とはならないものと思われる。

また本法は，医療に関する機器のセキュリティについて定める連邦法及び州法の規制に服する機器類を適用対象外とする。具体的には，連邦法である 1996 年連邦医療保険のポータビリティと説明責任に関する法律（HIPAA 法）と，カリフォルニア州法である医療情報の機密保持法によって規制される機器類は，本法の規制に服さない。

3）https://developer.amazon.com/ja/alexa/connected-devices/launch/works-with-alexa

4）Amy Grant, *California IoT Security Law: A Nearsighted, Toothless Guard Dog or a Wolf in Sheep's Clothing?*. https://www.tripwire.com/state-of-security/security-data-protection/iot/california-iot-security-law/

３　「合理的な」セキュリティ対策

本法の解釈をめぐり，最も議論の対象となっているのは，「接続される機器の製造者は，当該機器に次のすべての基準を満たす一の合理的なセキュリティ機能または諸機能を装備しなければならない。」とする条文である[5)]。基準としては，(1)機器の性質及び機能に適するもの，(2)収集し，包有し，又は発信することができる情報に適するもの，及び(3)機器及び機器に含まれる情報を，不正アクセス，破壊，使用，改変または開示から保護するように設計したもの，が挙げられており，これらをすべて充足しなければならない。

しかし，本法は「合理的」ということについて何ら定義しておらず，(1)及び(2)の「適する」についても具体的な規定を置いていない。機器の性質及び機能に適するセキュリティ機能とは具体的にはどのようなものなのか，収集し，包有し，又は発信することができる情報に適するセキュリティ機能とは何を意味するのか，本法の条文からは読み取ることができないのである。さらに，(3)の不正アクセス，破壊，使用，改変または開示から保護するように設計したものについても，どの程度のレベルの保護対策を講じれば足りるのかについての言及を欠いている。

他方で，本法は(1)から(3)の基準を充足している場合にかぎって，接続される機器がローカルエリアネットワークの外部に認証手段を備えている場合，あらかじめプログラムされたパスワードは製造された機器ごとに固有のものであること，または当該機器の初回アクセスが許可される前にユーザーが新しい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ときには，合理的なセキュリティ機能とみなされるものとすると規定している。つまり，接続される機器の使用に際してインターネット経由で外部の認証手段によってユーザー認証を行うような場合には，１台１台の機器に固有のパスワードを振るか，出荷時のデフォルトのパスワードのままで使用できないようにするか，どちらかの対策を講じていれば，合理的とみなされるという規定になっているのである。

たしかに，出荷時のデフォルトのパスワードのままで使用したり，「password」「1234」のような簡単なパスワードを設定したりすることはセキュリティ上危険であり，IoT 機器のセキュリティの上での問題点の一つとされているが，その点を解消したからといって「合理的」なセキュリティ対策を講じていると判断することができるのかについては，疑問の余地が大きい。セキュリティ対策は，適切なパスワード設定にとどまるものではないからである。

このため，この規定はセキュリティ対策を適切なパスワード対策に矮小化する恐れがあり，事業者に対する一種のセーフ・ガードとして機能するとする指摘もある[6)]。結果的に，事業者は，上記の(1)から(3)の要件を充たし，接続される機器に外部認証機能を装備して各機器固有のパスワードを設定するかユーザーが自ら設定したパスワードを使用させるようにすれば「合理的」と判断されるわけであるから，外部認証機能の利用に傾くようになることも予想される。

また本法は「本法は，接続される機器の製造者に対し，ユーザーの裁量で機器上で動作するソフトウェアまたはファームウェアを修正する能力を含めて，ユーザーが接続される機器に対して完全な制御を行うのを防止する義務を課すものと解釈されてはならない。」とも規定している。この点につき，事業者はユーザーに対してソフトウェアまたはファームウェアのアップデートも含めて当該機器へのアクセス及び管理権を完全に与えなければならないと解する見解がある[7)]。この見解に

---

5)　本条につき，福岡＝北條＝沼澤（訳）・前注２）の訳文は，「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。」としており，この訳文では合理的なセキュリティ機能又は以下のすべての機能（(1)号から(3)号まで）のいずれかを選択的に備えることを要求しているようにも見える。しかし，合理的なセキュリティ機能又は(1)号から(3)号までのすべての機能のいずれかの実装を要求しているのではなく，(1)号から(3)号までのすべての要件を充たした合理的なセキュリティ機能を備えることを求めていると解するべきであろう。本法を解説するウェブサイト等の多くはそのように解するが，今後の議論が待たれる。

6)　Grant, supra note 4.

7)　Lisa Lifshitz, *Security by Degish: California's New IoT Security Laws*. https://businesslawtoday.org/2018/11/security-design-californias-new-iot-security-laws/

よれば，事業者はユーザーによる独自のセキュリティ対策が行えるような手段を残しておかなければならない，ということになる。他方で，事業者はユーザーに対して当該機器へのアクセス及び管理権を完全に与えなければならないというわけではなく，ユーザーが当該機器のアクセス・管理ができないような仕様とする義務を負うものではないことにとどまるという見方もありうる。

事業者に出荷後のソフトウェアまたはファームウェアのアップデートの提供を義務づけるものとはなっておらず，ユーザー側にもソフトウェアまたはファームウェアのアップデートを求める規定は存在しない。

4　実効性

本法は，昨年の 9 月末に州知事が署名したばかりということもあって，本稿執筆時点では，法的な議論はまだ必ずしも多くはないが，本法への批判は文言が広範かつ曖昧であり法の規制の実効性を欠くという点であろう。本法を紹介するウェブサイト等の多くが，「合理的（reasonable）」と「適する（appropriate）」という文言が具体的に何を意味しているのか，本法だけでは読み取ることができない点を指摘している。

また実効性に関する本法の問題点として指摘されているのは，訴訟提起の権利を否定していること，違反した事業者に対する罰則がないこと，輸入事業者と再販売事業者を適用除外としているためカリフォルニア州裁判所が管轄権を認定しないかぎり海外事業者と州外事業者には本法を適用できないこと，である。

特に消費者保護の観点からは，「本法は，民事訴訟を提起する権利を付与するものと解釈されてはならない。司法長官，市検事，郡法律顧問又は地方検事は，この法律を執行する排他的権限を有する。」としているため，消費者が本法に違反して製造された IoT 製品を購入して使用した結果サイバー攻撃を受けて被害が発生したというような場合，どのような法的救済が受けられるのかという問題が残っている。

他方で，サイバーセキュリティ法の研究者である Jeff Kosseff アメリカ海軍大学校准教授は，本法の意図は適切であると評価する。Kosseff は 2017 年に連邦議会に提案された Active Cyber Defense Certainty Act 法案[8] の賛同者でもあるが，連邦政府による積極的なサイバーセキュリティ対策を主張しており，サイバーセキュリティに関する事項はカリフォルニア州だけに適用される州法ではなく連邦法で規律すべきであるとする[9]。

Ⅲ　わが国の立法化に向けた示唆

IoT のセキュリティ及びプライバシーに関する懸念はわが国でも高まっており，すでに IoT セキュリティにさまざまなガイドラインが存在するが，IoT セキュリティに特化した法は存在しない。その点では，本法が参考となるところは多い。

しかしわが国においては，次のような検討課題が残っていることを認識した上で，IoT のセキュリティ及びプライバシーの法規制の可能性について検討すべきであろう。

まず，IoT の法的定義が固まっていないという問題がある。

本稿執筆時点で IoT に関係する法的定義を置いているのは，国立研究開発法人情報通信研究機構法及び特定通信・放送開発事業実施円滑化法の一部を改正する等の法律[10] と，官民データ活用推進基本法[11] である。

改正特定通信・放送開発事業実施円滑化法では，附則 5 条 2 項 1 号で IoT について次のように定義している。

8）2017 年 10 月には，民間事業者によるアクティブ・ディフェンスを合法化するアクティブ・ディフェンス確実化法案（Active Cyber Defense Certainty Act）が連邦議会に提出された。同法案はサイバー攻撃被害者に hack back（逆侵入）を許容するものであり，論議を呼んだものの，可決に至らなかった。H.R.4036 - 115th Congress (2017-2018). アクティブ・ディフェンスによる積極的対抗を主張するものとして，Scott Jasper, Strategic Cyber Deterrence: The Active Cyber Defense Option, 165-185 (2017) などを参照。

9）Jeff Kosseff, *Hamiltonian Cybersecurity* (August 19, 2018). Wake Forest L. Rev., Vol. 54, Forthcoming. Available at SSRN: https://ssrn.com/abstract=3234758.

10）平成 28 年法律第 32 号。

11）平成 28 年法律第 103 号。

「新技術開発施設供用事業　インターネット・オブ・シングスの実現（インターネットに多様かつ多数の物が接続され，及びそれらの物から送信され，又はそれらの物に送信される大量の情報の円滑な流通が国民生活及び経済活動の基盤となる社会の実現をいう。）に資する新たな電気通信技術の開発又はその有効性の実証のための設備（これを設置するための建物その他の工作物を含む。）を他人の利用に供する事業をいう。」

一方，官民データ活用推進基本法2条3項は，次のように定義している。

「この法律において『インターネット・オブ・シングス活用関連技術』とは，インターネットに多様かつ多数の物が接続されて，それらの物から送信され，又はそれらの物に送信される大量の情報の活用に関する技術であって，当該情報の活用による付加価値の創出によって，事業者の経営の能率及び生産性の向上，新たな事業の創出並びに就業の機会の増大をもたらし，もって国民生活の向上及び国民経済の健全な発展に寄与するものをいう。」

改正特定通信・放送開発事業実施円滑化法は，インターネット・オブ・シングスの実現にあたり，「インターネットに多様かつ多数の物が接続され，及びそれらの物から送信され，又はそれらの物に送信される大量の情報の円滑な流通が国民生活及び経済活動の基盤となる社会」がIoTであるとしているのに対して，官民データ活用推進基本法では「インターネットに多様かつ多数の物が接続されて，それらの物から送信され，又はそれらの物に送信される大量の情報の活用に関する技術」がIoTであるとしており，両者のあいだには若干の相違がある。「インターネットに多様かつ多数の物が接続されて，それらの物から送信され，又はそれらの物に送信される大量の情報」という点では両者の定義は共通するが，前者がその流通によって実現する国民生活及び経済活動の基盤となる社会までを射程に入れていると考えられるのに対して，後者はそれを活用に関する技術までにとどめている。

もとより両者ともに特に義務規定などを伴うものではないので，両者の定義の相違は特に大きな問題を生じさせていないともいえるが，IoTのセキュリティやプライバシーを考える際に，技術にとどめるのか社会までを射程に入れるのかという点は，IoTセキュリティ対策を考える上では無視できない。

またわが国においては，セキュリティ侵害通知（security breach notification）法に相当する規定が存在しない。本稿執筆時点で，アメリカにおいては特定領域の連邦法のほか，46州でセキュリティ侵害通知法が制定されており，個人データを含むデータのセキュリティ侵害が発生したときには当該本人，データの所有者や権限を有する者に通知しなければならないとしている[12)]。これに対して，わが国では行政手続における特定の個人を識別するための番号の利用等に関する法律29条の4が特定個人情報の漏えい等に関する報告義務を個人番号利用事務等実施者に課しているのみで，個人情報の漏えい等について本人に通知する法的義務は存在しない。また不正アクセス行為の禁止等に関する法律8条も，アクセス管理者に「不正アクセス行為から防御するため必要な措置を講ずるよう努めるものとする。」という努力義務を定めているが，実際に不正アクセスが発生した場合の通知公表義務は規定していない。

このように，わが国のIoTセキュリティ規制の可能性については，立法化を考える前に検討すべき論点が数多く残っている。本法の施行は2020年1月からとなっており，施行前後にはさまざまな法的議論が起こることが予想される。今後の動向が注目されよう。

12）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11巻（2012年）72頁以下。なお各州のセキュリティ侵害通知法は，医療情報，バイオメトリクス情報も対象に含むかどうかでかなり異なっている。Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 Tex. L. Rev. 85, 138 (2014).

〈付録〉

カリフォルニア州接続される機器（コネクテッド・デバイス）のセキュリティに関する法律　仮訳

【接続される機器のセキュリティ】

1798.91.04 条

(a)　接続される機器の製造者は，当該機器に次のすべての基準を満たす一の合理的なセキュリティ機能または諸機能を装備しなければならない[13]。

(1)　機器の性質及び機能に適するもの

(2)　収集し，包有し，又は発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情報を，不正アクセス，破壊，使用，改変または開示から保護するように設計したもの

(b)　接続される機器がローカルエリアネットワークの外部に認証手段を備えている場合，(a)項の要件を全て満たすことを条件として，以下のいずれかの要件が満たされている場合は(a)項に基づく合理的なセキュリティ機能とみなされるものとする。

(1)　あらかじめプログラムされたパスワードは，製造された機器ごとに固有のものであること

(2)　当該機器は，初回アクセスが許可される前にユーザーが新しい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 条

本法の目的に照らして，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ー，プロセスまた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，インターネットプロトコル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いうものとする。

(c)「製造業者」とは，カリフォルニアにおいて販売または販売の申込がなされている接続機器を製造する者，または他人と契約して当該他人のために製造する者を意味するものとする。本項の目的に照らし，他人に代わって製造することに係る他人との契約は，接続される機器の購入，または接続される機器の購入及びブランド付与のみの契約を含まない。

(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に設計された機器の特徴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，消費者が許可していないアクセス，破壊，使用，変更又は開示をいうものとする。

1798.91.06 条

(a)　本法は，接続される機器にユーザーの選択によって追加される無連携のサードパーティーのソフトウェアまたはアプリケーションに関連する接続される機器の製造者に義務を課すものとは解釈されないものとする。

(b)　本法は，電子ストア，ゲートウェイ，マーケットプレイスまたはその他のソフトウェアもしくはアプリケーションの購入もしくはダウンロード手段の提供者に対し，本法の遵守の審査または執行につき，何らかの義務を課すものと解釈されてはならない。

(c)　本法は，接続される機器の製造者に対し，ユーザーの裁量で機器上で動作するソフトウェアまたはファームウェアを修正する能力を含めて，ユーザーが接続される機器に対して完全な制御を行うのを防止する義務を課すものと解釈されてはならない。

(d)　本法は，その機能性が，その執行権限に従って連邦政府機関により公布された連邦法，規則またはガイダンスに基づくセキュリティ要件の対象となる接続機器には，適用されない。

(e)　本法は，民事訴訟を提起する権利を付与するものと解釈されてはならない。司法長官，市検事，郡法律顧問又は地方検事は，この法律を執行する排他的権限を有する。

(f)　本法により課される義務および義務は，他の法律に基づいて課されるその他の義務に重複するものであり，いずれの当事者も他の法律に基づいて課される義務から除かれるとは解釈されないものとする。

(g)　本法は，法律また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釈されないものとする。

(h)　1996 年連邦医療保険のポータビリティと説明責任に関する法律（HIPAA 法）または医療情報の機密保持法（第 1 章 2.6 条（第 56 項以降））の適用対象となる企業，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，またはその他の個人は，これらの法律により規制される活動に関して，本法の適用を受けない。

---

13)　本項につき，(1)号から(3)号までのすべての機能を充たしただけでは，合理的とは評価されるには不十分である可能性がある。

（i） 本法は，2020 年 1 月 1 日に施行する。

※　本稿は，科学研究費補助金「自動走行の自動車における個人情報・プライバシーの保護の法的検討」（18K01396）の研究成果の一部である。