IoTセキュリティ法制をめぐって

湯淺　墾道
（情報セキュリティ大学院大学）

IDF第１５期第４回「法務・監査」分科会
２０１９／３／１１（月）

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

IoTセキュリティ

NICT法改正

- 電気通信事業法及び国立研究開発法人情報通信研究機構法の一部を改正する法律
  - 「国立研究開発法人情報通信研究機構（以下「機構」という。）は、平成三十六年三月三十一日までの間、特定アクセス行為を行い通信履歴等の電磁的記録を作成すること、特定アクセス行為による電気通信の送信先の電気通信設備に係る電気通信事業者に対し、送信型対電気通信設備サイバー攻撃のおそれへの対処を求める通知を行うこと等の業務を行うこととすること。」
- 国立研究開発法人情報通信研究機構法の一部改正
  - 第二条
  - (略)
  - 2 機構は、第十四条及び前項に規定する業務のほか、平成三十六年三月三十一日までの間、次に掲げる業務を行う。
  - 一 特定アクセス行為を行い、通信履歴等の電磁的記録を作成すること。

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- 機構の端末設備又は自営電気通信設備を送信元とし、アクセス制御機能を有する特定電子計算機である電気通信設備又は当該電気通信設備に電気通信回線を介して接続された他の電気通信設備を送信元とする電気通信の送信をおこなう行為であって、当該アクセス制御機能を有する特定電子計算機である電気通信設備に電気通信回線を通じて当該アクセス制御機能にかかる他人の識別符号(当該識別符号について電気通信事業法第52条第1項または第70条第1項第1号の規定により認可を受けた技術的条件において定めている基準を勘案して不正アクセス行為から防御するため必要な基準として総務省令で定める基準を満たさないものに限る。)を入力して当該電気通信設備を作動させ、当該アクセス制御機能により制限されている当該電気通信設備又は当該電気通信設備に電気通信回線を介して接続された他の電気通信設備の特定利用をし得る状態にさせる行為をいう。
- 不正アクセス禁止法の定める不正アクセスの構成要件から除外

カリフォルニア州 IoTセキュリティ法

カリフォルニア州IoT セキュリティ法

■カリフォルニア州法
「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」

- 2018年9月制定、2020年1月施行予定
- 2018 CAL. LEGIS. SERV. CH. (S.B. 327)(TO BE CODIFIED AT CAL. CIV. CODE § 1798.91.04(a)).

■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

- 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
- 民法典に追加
- 罰則無し
- 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いう評価
- 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

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

適用対象事業者

■「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

- 規制の対象となるのは、当該機器の製造者
- 「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。」
- カリフォルニア州で販売する製造者はすべて規制対象、OEM製造も規制の対象

適用除外

■「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。」

- ●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責任を負わない
- ●どのような状態が「無連携」となるのかが明らかではない

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- 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
  - ■ 製造事業者は責任を負わないと解するのが自然
  - ■ 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
  - ■ AmazonのConnected Device Certification program 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

■「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およびブランド付与のみの契約を含まない。」

- 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
- 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。

適用対象機器と例外

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

■「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。」

- 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
  - ◆連邦法の下でのガイドライン等の規制対象となっている場合は、本法の適用対象とはならない
- 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は適用対象外

「合理的な」セキュリティ対策

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

■「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

- （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）機器およ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」

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

■福岡真之介・北條孝佳・沼澤周「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.

■「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。」

■合理的なセキュリティ機能又は以下のすべての機能（(a)項から(c)項まで）のいずれかを選択的に備えることを要求？

●「合理的なセキュリティ機能」、または（a）項から（c）項までのすべての機能のいずれかを備えていればよい

■（a）項から（c）項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？

■「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」

■（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）機器およ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

- 「合理的」ということについて定義なし
- (1)(2)の「適する」の具体的な規定なし
  - 機器の性質及び機能に適するセキュリティ機能とは
  - 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
- (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
  - 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

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- 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
  - 事業者セーフ・ガード?
  - セキュリティ対策をパスワード対策に矮小化?

■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

- 「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。」
- HIPPA法、医療情報の機密保持法規制対象となる場合は適用除外

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

■「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。」

- 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あり

- ●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く義務?
- ●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

■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義務なし

■ユーザー側にアップデートを求める権利なし

実効性

■文言が広範かつ曖昧

- ●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

■訴訟提起の権利を否定

■違反した事業者に対する罰則がない

■輸入事業者と再販売事業者は適用除外、カリフォルニア州裁判所が管轄権を認定しないかぎり本法を適用できない

消費者保護

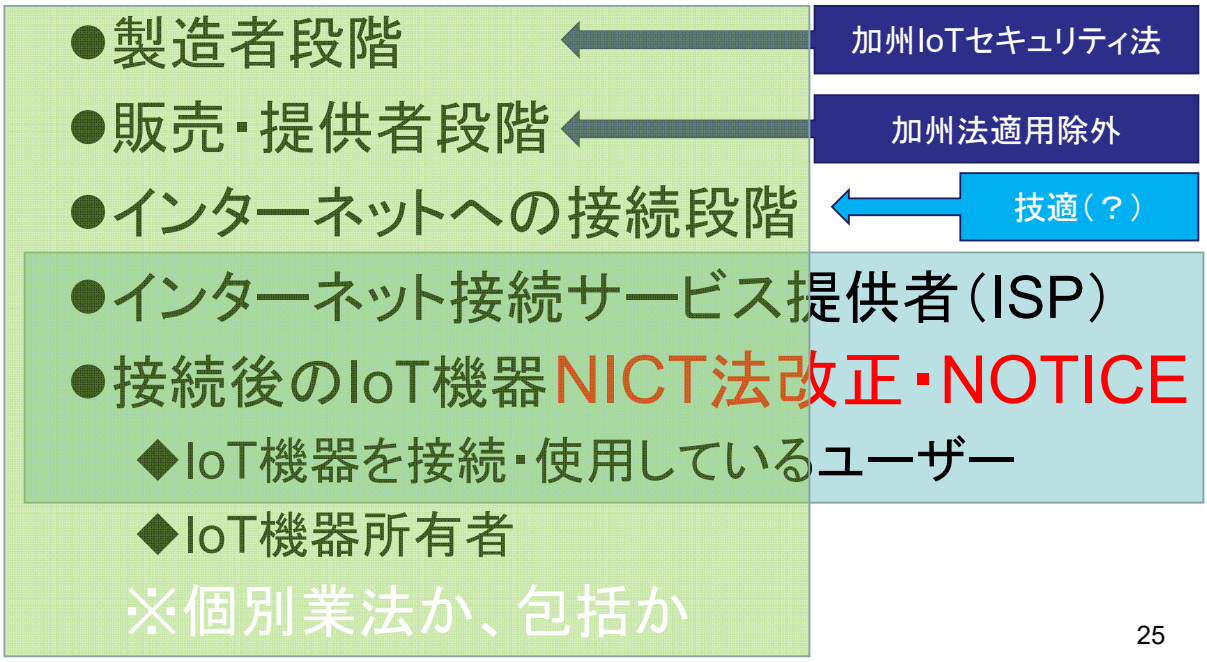
■「本法は、民事訴訟を提起する権利を付与するものと解釈されてはならない。司法長官、市検事、郡法律顧問又は地方検事は、この法律を執行する排他的権限を有する。」

- 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
- 訴訟提起は不可能
- ユーザーはどのような法的救済が受けられるのか

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

IoTセキュリティ法規制の今後

■IoTセキュリティ法規制のあり方



情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

■ 本報告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）の成果の一部です