【アメリカ】連邦の IoT 機器のセキュリティ向上に関する法律

海外立法情報課　中川　かおり

＊2020 年 12 月 4 日、連邦政府が所有し、又はコントロールする IoT 機器のセキュリティ向上を目的とする最初の連邦法が成立した。

1　経緯

IoT は、‘Internet of Things’の略で、「モノのインターネット」と一般に訳され、「様々な物がインターネットにつながること」「インターネットにつながる様々な物」等を意味する。IoT 機器には、電源の投入や給湯により、離れて暮らす家族に動作状況が伝達される給湯ポットから、道路、信号機、他車等と通信しながら走行する自動運転車まで、様々なものがある。産業・市場の分析情報等を提供する IHS マークイット社の推計によれば、全世界に 2017 年に 270 億個あった IoT 機器が、2030 年には 1250 億個になるとされる[1]。連邦政府でも、装置のコントロール・監視、環境データの収集等様々な用途での IoT 機器の使用が増えており、現在 IoT 機器を使用し、又は今後 5 年以内に使用する計画があるとする省庁は 85%を超える[2]。一方で、IoT 機器は、ラップトップ、タブレット、ルータ等の汎用コンピュータ機器及びネットワークインフラと比べ、脆弱なセキュリティしか備えていないという問題があり[3]、実際に、IoT 機器を足掛かりにした大規模なサイバー攻撃も起きている[4]。そこで、連邦政府の所有等する IoT 機器のセキュリティ向上を目的とする最初の連邦法が、2020 年 12 月 4 日に成立した[5]。連邦政府は、単一の消費者としては世界で最大で、その定める基準は広範囲に影響を及ぼすとみられる。

2　概要

（1）IoT 機器の定義（15 U.S.C.（以下略）§ 278g-3a note.）

①物理的世界と直接に相互作用するために、1 以上の変換器（センサー[6]又はアクチュエータ[7]）、1 以上のネットワーク・インターフェイスを有し、かつ従来型の IT 機器（スマートフォン、ラップトップ等）ではない物であって、②単独で稼働でき、及びプロセッサのように他の装置の一部として稼働する場合のみに機能するものではない物

（2）連邦の IoT 機器に関する情報セキュリティ基準、セキュリティポリシー等（§ 278g-3b）

＊ 本稿におけるインターネット情報の最終アクセス日は、2021 年 6 月 9 日である。［］内は筆者の補記である。

1 “The Internet of Things is here and growing exponentially,” *IHS Markit Online Newsroom*, Oct. 24. 2017.

2 “New Federal Law for IoT Cybersecurity Requires the Development of Standards and Guidelines Throughout 2021,” *GIBSON DUNN*, Feb. 17, 2021.

3 H.R. Rep. No. 116-501, pt.1, at 13 (2020).

4 2016 年に東海岸の数百万人がインターネットにアクセスできなくなった事象は、IoT 機器の脆弱性を利用した分散型サービス拒否（DDoS）攻撃によりもたらされたものであった。*ibid*., at 5.

5 IoT Cybersecurity Improvement Act of 2020, P.L.116-207. <https://www.congress.gov/116/plaws/publ207/PLAW-116publ207.pdf>; IoT 機器に関する法律は、カリフォルニア州（SB327, 2018）とオレゴン州（HB2395, 2019）で制定されている。いずれも、IoT 機器の製造者に「合理的な」セキュリティ機能を備える機器の製造を求める。湯淺墾道「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」『情報法制研究』第 5 号, 2019.5, p.32.

6 システムの入力装置として、多様な情報を集めるために使われる。例えば、健康管理アプリにおいて、歩数、心拍、呼吸等を収集する物がある。渡辺晴美ほか編著『つながる!基礎技術 IoT 入門』コロナ社, 2020, p.3.

7 エネルギーを機械的な動きに変換する出力機器をいう。例えば、センサーから得た情報を元にエアコンの温度を自動的に調節する物がある。IoT 機器においては、インターフェースを介し、入力装置で得た情報を元に、コンピュータで計算、処理し、信号が出力装置に送られ、出力装置のアクチュエータが動作する。同上, pp.96, 99.

法律の制定日から 90 日以内に、商務省の下で科学技術に関する標準の研究等を行う国立標準技術研究所（NIST）所長は、省庁が所有し、又はコントロールする IoT 機器であって、省庁が所有し、又はコントロールする情報システムに接続される物の適切な利用及び管理につき、最低情報セキュリティ要件を含めた連邦政府の基準等を作成し、公表する[8]。この基準等は、①IoT 機器のセキュリティ脆弱性の管理の検討等、②IoT 機器の a)安全な開発、b)ID 管理、c)パッチ適用、d)構成管理[9]等に関する NIST の基準、民間部門の基準等と合致するよう作成される。NIST 所長が基準等を作成してから 180 日以内に、行政管理予算局（OMB）局長は、省庁の情報セキュリティポリシー等を、上記 NIST 所長の基準等と合致させるよう審査する。NIST 所長は、基準等を 5 年に 1 度審査し、改訂する。情報セキュリティポリシー等及び連邦調達規則もこれらに合わせて改訂される。

（3）IoT 機器等のセキュリティ脆弱性等に関する公表指針（§ 278g-3c）

法律の制定日から 180 日以内に、NIST 所長は、次の事項に関する指針を作成し、公表する。①省庁が所有し、又はコントロールする情報システム（IoT 機器を含む。）のセキュリティ脆弱性の報告、公表等、②当該脆弱性の解決策の報告、公表等、③省庁に情報システム（IoT 機器を含む。）を提供する契約者等による、情報システムの潜在的なセキュリティ脆弱性に関する情報の受領、④当該契約者等による、当該脆弱性の解決策についての情報の配布。

上記指針を、産業界のベストプラクティス、国際標準規格（ISO29147［脆弱性の開示］及び ISO30111［脆弱性取扱手続］）等に合致させる。OMB 局長は、上記指針の実施を監視する。

（4）IoT 機器等のセキュリティ脆弱性に取り組むために必要となり得るポリシー等（§ 278g-3d）

法律の制定日から 2 年以内に、OMB 局長は、国土安全保障長官と協議の上で、情報システム（IoT 機器を含む。）のセキュリティ脆弱性に取り組むために必要となり得るポリシー、基準等を作成し、実施を監視する。同長官は、OMB 局長と協議の上で、情報システム（IoT 機器を含む。）のセキュリティ脆弱性についての情報を報告、公表等するために、省庁に運営上及び技術上の支援を提供する。その際、同長官は、当該支援が(2)の NIST 所長による基準等と合致することを保障する。連邦調達規則もこれらに合わせて改訂される。

（5）一定の IoT 機器に関する調達等の禁止（§ 278g-3e）

省庁の情報統括責任者（CIO）は、IoT 機器の契約の審査を通じて、当該機器の利用が、(2)の NIST 所長による基準等及び(3)の NIST 所長による指針を順守できないと判断する場合には、省庁の長に、当該機器の調達又は入手、調達又は入手のための契約の更新等を禁じる。この禁止は、単純調達基準（simplified acquisition threshold）[10]を超えない額の契約に適用され、法律の制定日から 2 年後［2022 年 12 月 5 日］に効力を生じる。

ただし、CIO が、国家安全保障の利益若しくは研究目的による必要性又は代替的かつ効果的な手法による当該機器のセキュリティの確保を認める場合には、省庁の長は、契約等の禁止を免除される。OMB 局長は、CIO が免除の付与を判断するための標準手続を作成する。

---

[8] 2020 年 12 月、この規定に基づき、次の 4 つの基準案が公表されたが、最終基準の策定には至っていない。①NIST SP 800-213［連邦政府の IoT 機器サイバーセキュリティ指針］、②NISTIR 8259B［IoT 中核基準に必要な非技術的支援］、③NISTIR 8259C［IoT 中核基準及び非技術的基準を利用するプロファイルの作成］、④NISTIR 8259D［連邦政府のための IoT 中核基準及び非技術的基準を利用するプロファイルの事例］

[9] 組織の全ての構成機器を、そのライフサイクル、調達、処分を通じて、IT により追跡し、管理するプロセスで、各構成機器の状況につきデータを収集し、更新するデータベースの設計・実施を含む。Mike Alley, “IoT Configuration Management - 3 Crucial Questions,” *CXO Unplugged*, March 26, 2018.

[10] 連邦政府が、少額の物品、サービス等を購入するための簡易な契約手法が適用される上限額をいう。