米国サイバー・サプライチェーン・セキュリティ法政策の動向
－第117議会第1会期（2021-2022年）－

米国サイバー・サプライチェーン・セキュリティ法政策の動向
－第 117 議会第 1 会期（2021-2022 年）－

橘　雄介（社会環境学部社会環境学科）

Law and Policy on the Cyber Supply Chain Security in the United States
－117th United States Congress 1st Session－

TACHIBANA Yusuke （Department of Socio-Environmental Studies, Faculty of Socio-Environmental Studies）

Abstract

The first session of the 117th Congress (2021-2022) was a year of significant change for supply chain security in two ways. The supply chain security community made progress on the revision of NIST SP 800-161, the basic document in the area of supply chain security, and on the rapid development of key policies in response to major security incidents, such as the Colonial Pipeline incident and the Log4j vulnerability incident.

On the other hand, there have been the following room to do. The Cybersecurity Maturity Model Certification (CMMC), a framework for mandatory information security measures for contractors in the Department of Defense, was temporarily suspended. And a bill that would establish a new information sharing framework between the public and private sectors regarding security incidents did not reach an agreement. Those may indicate the difficulty of making information security management mandatory, which was originally based on the voluntary approach.

Keywords：Information Law, Information Security, Supply Chain Security, U.S. Law, Critical Infrastructure

1.　はじめに

サイバー・サプライチェーンとは、情報及び運用技術（IT/OT）に関するサプライチェーンのエコシステムのことであり、また、サイバー・サプライチェーン・セキュリティ（以下「サプライチェーン・セキュリティ」と省略することがある）はこのエコシステムのセキュリティ確保の取組み全般を指す(1)。

一般的に情報セキュリティ法政策は大まかに、以下の 3 種類に分類できる。

① クラッカーに対する制裁や営業秘密の保護（主として民事法及び刑事法による規制）、
② 情報セキュリティ・マネジメント（ISMS（Information Security Management System）など、主として法的には任意の取組み）及び
③ 消費者保護（主として個人情報保護法による行政的規制）。

これらは相互に補完し合い、情報の CIA（機密性（Confidentiality）、完全性（Integrity）及び可用性（Availability））を保護してきた(2)。

サプライチェーン・セキュリティの分野において、②はサイバー・サプライチェーン・リスク管理（Cyber Supply Chain Risk Management: C-SCRM）と呼ばれる(3)（特に ICT 製品に焦点を当てる場合には、従来から「ICT SCRM」ともいわれる(4)。他方、日本では「IT サプライチェーンリスクマネジメント」ともいわれる(5)）。

本報告書はサイバー・サプライチェーン・セキュリティのうち米国における②の施策、特に C-SCRM の動向を調査するものであり、期間としては第 117 議会第 1 会期（2021-2022 年）を調査対象とする（末尾で付記する通り、本稿は研究費の報告書である。そのため、助成期間以降の展開、すなわち、第 117 議会第 2 会期（2022-2023 年）における展開は反映できていない）。

第 117 議会第 1 会期（2021-2022 年）はサプライチェーン・セキュリティにとって大きな変化のあった年だった。二つある。一つは従来からの取組みが実施されまたは進展したことである。たとえば、サプライチェーン・セキュリティ分野の基本文書である NIST SP 800-161 の改訂作業が進んでいる（後掲 3.2）。もう一つは、大きなセキュリティ・インシデントを受け、重要政策が急遽、進展したことである。たとえば、Colonial Pipeline 事件を受け、米政府は重要インフラに対して、分野毎にではあるが、情報セキュリティ施策を義務づけるようになっている（後掲 3.4 及び 3.5）。また、特にサ

プライチェーン・セキュリティに特化したものとしては、ソフトウェア部品表（Software Bill of Material: SBOM）の取組みが形になった。これはソフトウェア・サプライチェーンを可視化する取組みであり、2018 年という早くから始まっていたが、ようやく 2021 年になって成果を得たものである。加えて、Log4j 脆弱性事件を受け、ホワイトハウス自らもこの取組みの舵取りに乗り出している（後掲 2.3.3）。

他方で、挫折もあった。一つは国防総省における請負事業者向けの情報セキュリティ施策の義務化の枠組みであるサイバーセキュリティ成熟度モデル認証（Cybersecurity Maturity Model Certification: CMMC）が一旦、中止されたことである（後掲 3.2）。このことは、本来、法的には任意が原則だった情報セキュリティ・マネジメントを義務化することの難しさを示しているのかもしれない。もう一つは官ー民のセキュリティ・インシデントに関する新たな情報共有枠組みを定める（要するに、事業者にセキュリティ・インシデントの届出義務を課す）法案が成立しなかったことである（後掲 4）。他方で、SolarWinds 事件や Microsoft Exchange 事件の対応について情報共有体制の欠陥が指摘されており、火種は未だくすぶっているようである。

なお、サプライチェーン・セキュリティに関する法的枠組みに関しては拙稿[6]で紹介しているため、以下ではそのアップデート（基本的に 2021 年の新たな動向）を紹介し、その解説に必要な限りで、背景となる法制度を説明する。

2.　安全保障を理由とした政府調達

2.1.　全体像

前述の通り、各事業者における情報セキュリティ・マネジメントは原則として任意で、各事業者が各事業者の事情に合わせた対応をとることで足りるとされてきた（ただし、結果的に情報セキュリティの対策が社会通念に照らして不備があったとして、セキュリティ・インシデントの際に損害賠償責任を負うことはある[7]）。もっとも、政府の情報システムを構築する事業者や政府に IT 製品を納入する事業者が勝手に情報セキュリティのレベルを設定するというのでは、政府の情報の CIA が確保できない[8]。そこで、米国法では政府調達における請負事業者に一定のセキュリティ基準の履行を求めており、これにより政府の情報システムのセキュリティ水準を確保している。

加えて、米国政府が政府調達に情報セキュリティ基準の履行を求めることはもう 1 つの意味がある。それは、米国政府の購買力を利用することで、米国政府が要求する情報セキュリティ基準を事実上の基準（デファクト・スタンダード）にするというものである。この典型例は IT 製品に係る ISO/IEC 15408（Common Criteria: CC）である。

以下ではこの両者の視点から、ハードウェア及びソフトウェアに関する政府調達基準（または一定のセキュリティ施策を直接義務づける制度）を紹介する。簡単に示すと、この分野には表 **1** の制度がある。本報告書では拙稿[9]以後の動きである強調部分について以下で紹介する。強調していない部分は既に拙稿で解説しているため、該当箇所を参照されたい。

2.2.　ハードウェア：ICT 製品に関する認証基準

従来から、米国政府は一部の ICT 製品について政府調達の基準を設けていた（連邦情報セキュリティ管理法（Federal Information Security Management Act of 2002: FISMA (2002)）に基づく FIPS 140-3 及び Common Criteria（CC））[10]。近時、以下の通り、この手法を拡げる動きがある。

表 1　政府調達または一定のセキュリティ施策の義務づけに関するマッピング

	ハードウェア	ソフトウェア
模造電子部品	➢ 政府調達からの排除（国防権限法）	
疑わしい製品の排除	➢ 政府調達からの排除（国防権限法） ➢ 事後的な排除（連邦情報セキュリティ現代化法（FISMA (2014)）、連邦調達サプライチェーン・セキュリティ法（FASCSA））	同左
一部の ICT 製品に関する認証基準	➢ 既存の枠組みとして、連邦情報セキュリティ管理法（FISMA（2002））・FIPS 140-3、Common Criteria（CC） ➢ **FISMA 改正案** ➢ **ハードウェア部品表** ➢ **IoT 製品に関する最低基準＋ラベル制度**	
ソフトウェアに対するセキュリティ基準		➢ **ソフトウェアに関する最低基準＋ラベル制度** ➢ **ソフトウェア部品表** ➢ **クラウドのセキュリティ基準**

○　FISMA 改正案

前述の通り、従来の政府調達基準の 1 つの大きな法的根拠が FISMA (2002)である。直近では、同法を改正する提案がなされている。すなわち、第 117 会期連邦議会下院に 2022 年連邦情報セキュリティ近代化法（Federal Information Security Modernization Act of 2021）（S.2902）が提出されている(11)。

報道によれば、法案は①情報セキュリティに関する連邦政府機関の権限を運用面ではサイバーセキュリティ・インフラセキュリティ庁（Cybersecurity and Infrastructure Security Agency: CISA）に、戦略面では国家サイバー・ディレクター（U.S. National Cyber Director）に集約し、②連邦政府機関が情報セキュリティ基準を履行することを義務づけ、また、③IT 資産を自動的に管理可能なものとするとされる(12)。

後述 4 の通り、同法案は 2022 年度国防権限法には含まれなかったため、第 117 議会第 1 会期で成立していない。

○　ハードウェア部品表作業部会（2022 年 1 月）

サプライチェーン・セキュリティにおいて重要なこととして、政府や事業者が調達の際に製品の脆弱性や信頼できないベンダーの介在を検証することがある(13)。しかし、そもそも脆弱性の有無の検知は容易ではなく、また、ICT 製品は数多の部品から構成されており、介在したベンダーを確認することも容易ではない。そこで、サプライチェーンを可視化する取組みとして、ソフトウェアの分野ではソフトウェア部品表の取組みが進んでいる（後掲 2.3.3）。そして、直近では、同様の取組みをハードウェアの分野でも行うことが米国政府において始まっている。

2021 年 1 月、「情報通信技術（ICT）サプライチェーンリスク管理（SCRM）タスクフォース（Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force)」の政府及び産業界のメンバーが集まり、新メンバーを発表するとともに、タスクフォースの 2022 年の作業計画を策定した。今後、タスクフォースにおける「ハードウェア部品表作業部会（Hardware Bill of Materials Working Group)」は、組織が ICT 製品を調達または導入する際に使用できる基本的なハードウェア部品表のテンプレートを作成するための適切な情報を特定することに焦点を当てるとされる(14)。

当該タスクフォースは後述のソフトウェア部品表に関するタスクフォースであり、米国政府がソフトウェアの手法をハードウェアへ応用することが予想される。今後の展開が期待される。

○　IoT 製品に関する最低基準＋ラベル制度

現在、米国政府が政府調達の手法を拡張させようとしている領域はモノのインターネット（Internet of Things: IoT）である。米国政府は IoT について米国立標準技術研究所（National Institute of Standards and Technology: NIST）に IoT 製品に関する最低基準を定めさせ、同時にそれを満たすラベル制度を考案させる計画である。そして、米国政府の購買力を利用して、IoT 製品のセキュリティ水準を全体的に引き上げようとしている。もっとも、第 117 議会第 1 会期時点で、後述の通り IoT メーカー向けのベストプラクティスの提供（NISTIR8259 シリーズ）と政府機関向けの情報セキュリティ・マネジメントに関するガイダンス（SP 800-213 シリーズ）にとどまり、政府調達への紐付けには至っていないとされる(15)。

・立法及び政府の動き

後述のように、NIST における IoT のセキュリティ基準策定自体は 2020 年前半から形になっているが、それと併行するように、立法及び大統領令においても IoT のセキュリティ基準に関するものが成立し、NIST に権限を与え、かつ、政府調達への接続を行っている。

一つは、トランプ政権末期の「IoT サイバーセキュリティ改善法（Internet of Things Cybersecurity Improvement Act of 2020)」である。トランプ大統領は 2020 年 12 月、同法案（HR 1668）(16)に署名した。これは連邦政府が購入する IoT 機器についてセキュリティ要件を定めるよう、NIST に指示するものである。この法律の下では、政府機関は、パスワードの変更や、ベンダーが提供するパッチのインストールなどのセキュリティ機能を備えた IoT デバイスしか利用できないことになる(17)。

もう一つは、2021 年 5 月にバイデン政権下で成立した大統領令 14028 号「国家のサイバーセキュリティの向上（Improving the Nation's Cybersecurity)」(18)である。大統領令は NIST に対し、IoT 及びソフトウェアに関連する二つのラベリング・プログラムを開始し、消費者に製品のセキュリティについて知らせるよう指示する。これらのプログラムの期限は 2022 年 2 月 6 日までとなっている(19)。

・NISTIR8259 シリーズ（2020 年 5 月～2021 年 8 月）

NIST は 2020 年 5 月、IoT デバイスに関する文書、NIST Interagency Reports (NISTIRs) 8259 A 及び NISTIR 8259 を発表した。その後、2020 年 12 月に 8259 B、8259 C 及び 8259 D のドラフト版を発表し、2021 年 8 月に確定版となっている(20)。

これらは、IoT 機器メーカーに対して、顧客のセキュリティ目標をサポートするために必要なガイダンスとベストプラクティスを提供することを目的としたものとされる。そして、そこでいう「コアベースライン」は組織のデバイス、データ、システム及びエコシステムを保護することを目的としたサイバーセキュリティ管理策である。NIST はこれが業界や市場に特化したベースラインを策定するための重要な基盤になるとする。もっとも、前述の通り、第 117 議会第 1 会期時点で政府調達への紐付けはなされていないとされる(21)。

・SP 800-213 シリーズ（2021 年 11 月）

NIST は 2021 年 11 月、政府機関向けの IoT 機器のマネジメント・ガイダンスを策定した。これは、これらのデバイスを入手する際に何を要求すべきかについて連邦政府機関にガイダンスを提供するものである。

＜参考情報＞

IoT に一定のセキュリティ措置の搭載を求める連邦法ないし規則は、本文の通り、第 117 議会第 1 会期時点で存在しないが、州法では動きがある。もっとも、情報セキュリティの観点からではなく、消費者のプライバシー保護の観点からのものである点には注意が必要である。

○　カリフォルニア州 IoT 法（2019 年）

カリフォルニア州は 2019 年 9 月、米国初の IoT セキュリティ立法を行った。法案の名称は「情報プライバシー：接続機器（Information privacy: connected devices）」であり[22]、民法の一部とされているようである。2020 年 1 月 1 日に施行されており、カリフォルニア消費者プライバシー保護法（California Consumer Privacy Act: CCPA）の姉妹法とされている。

規律の対象となるのは“connected device”であり、具体的には、「インターネットに直接または間接に接続でき、IP アドレスまたは Bluetooth アドレスが付与されている」機器とされ、広い定義となっている。規律対象者はカリフォルニア州で販売等される“connected device”の“manufacturer”である、小売り事業者やアプリ・プラットフォームなどは含まれない。対象事業者は対象機器に“reasonable security”措置を施す義務を負う。具体的には、次の要件を満たす必要があるとされる。

- 装置の性質・機能につりあうこと、
- 収集等する情報につりあうこと及び
- 機器及び収集等する情報を不正なアクセス等から防ぐよう設計すること。

義務違反を追求できるのは、カリフォルニア州の司法長官などの行政官だけであり、市民の私的な請求権は認められていない。

○　ハワイ州法（未成立）

また、こういった IoT に関する一定のセキュリティ機能の義務づけは他の州にも広がりつつある。たとえば、第 117 議会第 1 会期時点で、ハワイ州議会に法案（SB 2427）[23]が提出され、IoT デバイスのメーカーに対し「合理的なセキュリティ機能」をデバイスに装備することを求め、不正アクセスなどから消費者を守ることが定められている。

2.3.　ソフトウェア

2.3.1.　問題の所在

ソフトウェアの分野でもサプライチェーン・セキュリティの取組みが進んでいる。特に、2021 年はサプライチェーンないしオープンソースを介した 2 つの大きな事件があった。一つは SolarWinds 事件である。これは米国や欧州の政府機関などで広く使われている SolarWinds 社のソフトウェア「Orion」への攻撃である。攻撃者は、まず、SolarWinds 社のネットワークに侵入し、Orion に悪意のあるソフトウェアを注入した。次に、顧客がそのソフトウェアをダウンロードし、攻撃者が顧客のネットワークに侵入可能となった。このようにソフトウェアのサプライチェーンが狙われた（日本における同種の事件として、富士通 ProjectWEB 事件（2021 年 5 月）がある）[24]。また、同様に広く利用されているサービスが攻撃の対象となったものとして、2021 年 3 月の Microsoft Exchange 事件があり、やはり大きな問題となった[25]。

もう一つは Log4j 事件である。Log4j はプログラミング言語である Java のライブラリの一つで、ロギング（logging）の機能を担っていた。問題の脆弱性は Log4Shell と呼ばれるもので、リモートコード実行（remote code execution: RCE）に関するものである。この脆弱性を利用すれば、ハッカーが任意のコードを実行できたとされる。問題は二つあった。一つは、これがいわゆる「ゼロデイ（zero-day）」脆弱性で、発見時に緩和策が提供されていなかった。もう一つは、Log4j はオープンソースで、広く利用されていたことである[26]。

以上の事件を受け、後述のソフトウェア部品表に関するホワイトハウスの会合につながっている。

2.3.2.　ソフトウェアに関する最低基準＋ラベル制度

・大統領令 14028 号（2021 年 5 月）

2021 年 5 月、バイデン政権は前述の大統領令 14028 号を発した。大統領令は NIST を含む複数の機関に、ソフトウェアのサプライチェーンのセキュリティと整合性に関連するさまざまな取り組みを通じて、サイバーセキュリティを強化する義務を課している。また、大統領令 4 条では、NIST に対し、民間企業、学界及び政府機関などから意見を募り、ソフトウェアのサプライチェーンのセキュリティを強化するための既存の基準、ツール、ベストプラクティスもしくはその他のガイドラインを特定しまたは新たに開発することを指示している。また、前述の通り、大統領令は IoT 及びソフトウェアに関するラベリング・プログラムを定める[27]。

・NIST・ベースライン基準案＋ラベル案（2021 年 11 月）

上記大統領令を受け、NIST は 2021 年 11 月、ソフトウェアのベースライン基準とラベルの枠組みに関する文書案[28]を発表した。NIST はこのラベルにより製品間の比較を可能にし、消費者の IoT 購入決定を支援するとする。また、最終的には関連するサイバーセキュリティのリスクを低減させ

るとする。公開諮問が 12 月 16 日まで行われ、その後、NIST は他の機関と協力して、ラベル表示制度の実装に向けた試験を開始するとされる(29)。

2.3.3. ソフトウェア部品表

○ NTIA の取組み（2018 年～）・取りまとめ文書の発表（2021 年 11 月）

ソフトウェア部品表に関する取組みは、国家電気通信情報局（National Telecommunications and Information Administration: NTIA）における前述のタスクフォース（情報通信技術（ICT）サプライチェーンリスク管理（SCRM）タスクフォース）において、2018 年から進められてきた。ソフトウェア部品表とはソフトウェアの構成要素を列挙した台帳であり、サプライチェーンの透明化に寄与する。

NTIA は 2021 年 10 月、ソフトウェア部品表の開発と使用に関する基本文書(30)を策定した(31)。これは 2018 年からの作業の集大成となる。これは NTIA を中心とするタスクフォースが作成した文書で、ソフトウェア部品表の作成方法などが記載されている。もっとも、単にガイダンスの作成だけではなく、医療分野、エネルギー分野及び自動車部門において概念実証がなされているようである。

なお、この取組みの法的基盤は前掲大統領令 14028 号であり、この大統領令は NTIA にソフトウェア部品表に対する権限を与えている。そして、将来的には、これを政府調達と義務づけ、政府の購買力を利用してソフトウェア部品表の採用を促進することが意図されているようである。

○ Log4j 脆弱性の影響：ホワイトハウス会議（2022 年 1 月）(32)

直近では、Log4j 事件を受け、バイデン政権はソフトウェア部品表の実装をさらに促進する動きに出ている。すなわち、2022 年 1 月、ホワイトハウスは政府機関及び民間事業者（Microsoft や Google など）を招き、オープンソースソフトウェアのセキュリティに関する会議を開催した。ここでは、ソフトウェア部品表によって消費者に対しソフトウェアにオープンソースのコンポーネントが含まれていることを警告することが合意された(33)。

2.3.4. クラウドのセキュリティ基準

○ 政府機関に対するガイダンス

・CISA・クラウドセキュリティ技術参照アーキテクチャ（2021 年 8 月～未確定）

クラウドのセキュリティ基準についても米国政府は具体的な行動をとっている。やはり前掲大統領令 14028 号は CISA に対し、行政管理予算局（Office of Management and Budget : OMB）及び連邦リスク認可管理プログラム（Federal Risk and Authorization Management Program : FedRAMP）と連携して、クラウドセキュリティ技術参照アーキテクチャを作成するよう指示した。その目的は、連邦政府がクラウド・スマートの追求を続ける中で、クラウドへの移行とデータ保護に関する推奨事項を各機関に提供することにある(34)。

これを受け、CISA は、2021 年 8 月、「クラウドセキュリティ技術参照アーキテクチャ（Cloud Security Technical Reference Architecture）」を発表した。これは堅牢な多要素認証かデバイス管理、クラウドベースのセキュリティサービスへの依存などを求めている(35)。これは「ゼロトラスト」の概念を採用したものとされている(36)。

・行政管理予算局・ゼロトラスト覚書（2021 年 12 月）・ゼロトラスト・アーキテクチャ (ZTA) 戦略（2022 年 1 月）

加えて、行政管理予算局は 2021 年 12 月、ゼロトラスト・セキュリティに関する覚書を発表した(37)。覚書は今後、連邦行政機関にゼロトラストの情報セキュリティ義務を課すとする。覚書はゼロトラストを境界防御に依存するのではなくネットワーク内の活動を監視する新たな実践であると定義している。

続く 2022 年 1 月、行政管理予算局は 「連邦ゼロトラスト・アーキテクチャ (ZTA) 戦略（Federal zero trust architecture (ZTA) strategy）」 を発表した(38)。戦略は連邦行政機関に対し 2024 会計年度末（2024 年 9 月末）までにゼロトラストの概念を踏まえた情報セキュリティ施策を実装することを義務付ける。

これらは第 117 議会第 1 会期時点で連邦行政機関向けの義務であるが、今後、どのように政府調達などへ展開していくのか注目される。

○ NSA・CISA・Security Guidance for 5G Cloud Infrastructures（2021 年 10-12 月）

通信分野については 5G とクラウド環境が密接に関係することから、個別の取組みがある。米国家安全保障局（National Security Agency: NSA）と CISA は “Enduring Security Framework: ESF”イニシアチブの一環として、2021 年 10 月から 12 月にかけて 5G クラウドインフラストラクチャ内でのサイバー脅威を緩和するためのガイダンスを公開している。ガイダンスは以下の全 4 部が発表されている(39)。

- Security Guidance For 5G Cloud Infrastructures Part IV: Ensure Integrity of Cloud Infrastructure (12/16/2021)(40) ;
- Security Guidance for 5G Cloud Infrastructures Part III: Data Protection (12/2/2021)(41) ;
- Security Guidance for 5G Cloud Infrastructures Part II: Securely Isolate Network Resources (11/18/2021)(42) ; and
- Security Guidance for 5G Cloud Infrastructures Part I: Prevent and Detect Lateral Movement (10/28/2021)(43).

3. 重要インフラ整備に関する規制

3.1. 全体像

米国法上、重要インフラ（Critical Infrastructure）とは「そ

れが物理的か論理的かを問わず、米国にとって極めて重要なシステム及び資産であり、これらのシステム及び資産の機能停止または破壊が安全保障、国家経済の安全、国民の健康もしくは安全またはこれらの事柄の組み合わせを弱体化させるものである。」（USA Patriot Act of 2001 (42 U.S.C. 5195c(e)) 1016 条(e)）[44]。

米国の情報セキュリティ法においてはインフラやネットワークが政府に属するか民間に属するかで制度が大きく異なる。前者の政府に属するインフラについては政府調達と似た手法が用いられている。すなわち、請負事業者に一定のセキュリティ基準の履行を求める手法である（後掲 3.2）。サイバー・サプライチェーン・リスク管理は典型的にはこの取組みを指している。この背景には、米国政府や米軍自体のセキュリティがいかに堅牢であっても、その請負事業者のセキュリティが脆弱であれば、このサプライチェーンを利用して攻撃が可能になってしまうという問題意識がある[45]。後者の民間に属するインフラについてはこういった直接的なセキュリティ基準の履行という手法は原則として用いられない。そこで、従来、重要インフラに対する政府の補助金の条件として一定のセキュリティ基準を定め、政府が間接的に重要インフラのセキュリティ水準をコントロールするという手法が用いられてきた（後掲 3.3）。他方で、2021 年以降、この間接的な手法が変わりつつある。その原因は後述の Colonial Pipeline 事件であり、この事件以後、米国政府は重要インフラ部門に直接、一定のセキュリティ施策の履行を求めるようになってきている（後掲 3.4 及び 3.5）。その意味で、現在は規制手法の転換期にあるかもしれず、注目される。

3.2.　政府ネットワークにおけるサプライチェーン・セキュリティの取組み[46]

○　NIST SP 800-161 の改訂作業の進捗

米国の法政策においてサイバー・サプライチェーン・セキュリティ分野における 2021 年の最大の目玉は NIST SP 800-161 の改訂である。これは政府機関向けの情報セキュリティ・マネジメントの基本文書である NIST SP 800-53 について特にサプライチェーン・セキュリティの観点から管理策を詳述したものである。後述の CMMC においてもサプライチェーン・マネジメントの箇所で参照されている。

今回の改訂は納入先、サプライヤー、開発者、システムインテグレーター、外部システムサービスプロバイダーまたはその他の情報通信技術（ICT）／運用技術（OT）関連のサービス・プロバイダーのために、実装ガイダンスをよりモジュール化し、利用しやすくすることに重点を置いているとされる[47]。2021 年 4 月に第 1 案[48]、10 月に第 2 案が発表され[49]、最終的な採択は 2022 年第 3 四半期が予定されている[50]。

○　国防総省：CMMC の実施中止（2021 年 5 月）及び 2.0（2021 年 11 月）

サプライチェーン・セキュリティ分野での 2021 年の最大の驚きの 1 つは国防総省における CMMC の実施中止である。CMMC は国防事業の請負事業者が履行すべきセキュリティ基準を定めたものである。このような請負事業者のセキュリティ対策義務は従前からあったが（NIST SP 800-171 に基づいていた）、CMMC は画期的なものであった。すなわち、従前はセキュリティ対策義務の履行をモニタリングするのは請負事業者自身、つまり、自己申告だったが、CMMC は一定の国防事業については第三者の認証を受けることを入札の条件とした[51]。

CMMC はこのように鳴り物入りで 2020 年に策定され、2021 年からの実施が予定されていたが、小規模事業者にとっては要件が煩雑すぎること、審査員が恣意的に認証を拒否できること、また、従前と異なり NIST の基準そのものを使っているわけではないため、国防事業と連邦行政機関の事業とで満たすべきセキュリティ基準が異なることなどの問題が指摘されていたとされる。そのため、2021 年 5 月に実施が中止された[52]。その後、12 月に改訂版（CMMC 2.0 と呼ばれている）が公表されているが、一部にとどまっている[53]。

3.3.　連邦補助金の用途を通じた通信インフラ規制[54]

前述 2 で概説した通り、米国の情報セキュリティ法においては国防権限法などに基づき一定の疑わしい製品を政府調達から排除している。Huawei 製品などもこれに含まれており、政府の事業の請負事業者は Huawei 製品などを「システムの実質的もしくは不可欠な構成要素としてまたはシステムの一部のための重要な技術として」使用することはできない（詳細は拙稿[55]の解説に譲る）。

では、通信事業者のネットワークはどのようになっているのだろうか。前述の通り、米国の情報セキュリティ法では政府ネットワークと民間ネットワークとの規律は異なり、直接に Huawei 製品などを禁じているわけではない。厳密には、連邦通信委員会（Federal Communications Commission: FCC）が所管する通信事業者に対する補助金の支給要件として一定の通信機器の使用禁止を定めている（もっとも、後述の通信機器の認可を通じて直接的な禁止にも展開している）。ここでは、その展開を追う。

・背景としての国防総省・5G レポート（2019 年）

後述の通り、政府及び議会は Huawei などの中国通信ベンダーを米国の 5G ネットワークから排除していく。その表向きの理由は安全保障だが、実際には 5G ネットワークのスタンダード争いという側面が指摘されている。それを示すのが 2019 年の国防総省によるレポートである。

すなわち、国防総省の助言機関である Defense Innovation Board は 2019 年 4 月、5G ネットワークにおける国防上のリ

スク関する報告書を公表している(56)。報告書は 5G 関連市場での米国の一人負けを警戒する。というのも、以下の事情があるからである。当時、通信機器市場で欧州勢（Ericsson 及び Nokia）が劣勢である一方、中国勢が急伸していた。他方、5G 周波数において、米国は高周波数帯を中国は中周波数帯を推進しているが、高周波数帯では多数の基地局を必要とするため、米国の方式だとどうしても費用負担が大きくなってしまう。そのため、中国ベンダーの方が市場においても、周波数政策においても安上がりで、ひいて、中国の周波数・製品がデファクトになるおそれがあるということが指摘された。そのため、報告書は中国企業への輸出規制などを提言していた。後述の Huawei の排除につながる大統領令 13873 号はこれを受けたものだとされている(57)。

・FCC による Huawei 等の排除（2019 年）

FCC は 2019 年 11 月、ユニバーサルサービス基金（Universal Service Fund: USF）の対象から Huawei 及び同じく中国の通信機器ベンダーである ZTE を排除するよう全会一致で決議した(58)。これにより、USF の支援を受けている通信事業者が、通信ネットワークに国家安全保障上の脅威を与えるとみなされる「対象企業」から購入した機器やサービスの購入、保守またはその他のサポートにその基金を利用することを禁止されることとなった。

また、FCC は、USF の制限決議と同時に、機器の交換規則案も発表した(59)。これを後押しするように、2020 年 3 月、米議会でも信頼できない機器の撤去・取替に資金を拠出する法案が可決され、トランプ大統領もこれに署名している(60)。

その後、FCC の動きを立法でも明確に裏付ける立法が成立している（ユニバーサル基金を利用した通信機器の取得規制として、Secure 5G and Beyond Act of 2020(61)）。

・Huawei 製品等の認可禁止法（2021 年 11 月））

以上は通信事業者が Huawei 製品等を利用することに単にお金を出さないという話だった（もちろん、特に中小の通信事業者にとっては死活問題であるが）。連邦議会は更に進んで、Huawei 製品等をそもそも米国内で使える通信機器として認可しないという方策を採用した。

バイデン大統領は 2021 年 11 月、「安全な機器法（Secure Equipment Act of 2021）」 (HR 3919・S 1790)(62)に署名し、同法は成立した。これは FCC が国家安全保障上の脅威と見なされる「対象機器・サービスリスト」を作成し、FCC がリスト内の機器等に新たにライセンスを与えることを禁止するものである。現在、対象となっているのは Huawei や ZTE など中国企業 3 社である。

＜参考情報＞

本文の FCC の補助金をてこにした情報セキュリティ施策の他にも通信インフラに関する情報セキュリティ施策がある。一つは商務省の通商に関する権限を用いて信頼できない通信機器ベンダーをサプライチェーンから排除するものであり、もう一つは FCC の通信免許に関する権限を用いて信頼できない通信事業者を米国内の通信ネットワークから排除するものである。

○　商務省による信頼できない通信ベンダーの排除

米国はより一般的に敵対国の影響下にある情報通信技術及びサービス（Information and Communications Technology or Services: ICTS）の取引制限を定めるに至っている。トランプ政権は 2019 年 5 月、ICT サプライチェーンに関する大統領令 13873 号を発布した(63)。これは、ICT サプライチェーンに対する外国勢力からの脅威を理由とする、国家緊急事態宣言である。同日、商務省は Huawei 及び関連企業を輸出禁止リストへ追加した(64)。その後、トランプ政権は 2020 年 5 月、2019 年 5 月の大統領令を延長する大統領令を発布し、輸出禁止製品を Huawei が設計したチップセットなどに拡大するとともに、期間を 2021 年 5 月 15 日まで延長した(65)。

さらに、2021 年、商務省は暫定最終規則(66)を策定した。これは輸出禁止リストと異なり、ケース・バイ・ケースで取引の禁止を判断する内容になっている。すなわち、同規則による制限対象取引は中国に限られず、ロシアやイランなど 6 カ国が指定されている。また、Huawei や ZTE との取引制限のように、一般的な制限ではなく、事業者・技術／サービスごとの制限となっている。規制を受ける ICTS 取引は、米国の管轄下にある人物／財物が関与するものであり、連邦機関や請負人による調達以外も含まれる。

もっとも、当該取引制限に対しては履行状況に懸念が示されている。すなわち、上院の共和党議員らは 2021 年 10 月、報告書を公表し、Seagate Technology Holdings plc が商務省による上記制限にもかかわらず Huawei にハードディスクを販売していたとして、非難している(67)。

○　FCC による信頼できない通信事業者の排除

FCC は、近時、1934 年通信法 214 条に基づく国内及び国際業務認可の枠組みに基づき中国の以下の通信事業者などの免許を取り消している。その理由として、中国政府が中国の通信事業者に対する影響力を有していることが各手続きにおいて指摘されている。

- Pacific Networks 及び ComNet（2021 年 3 月命令）(68)
- China Telecom (Americas) Corp.（2021 年 11 月命令）(69)
- China Unicom（2022 年 1 月命令）(70)

3.4.　重要インフラの制御システム向けのセキュリティ基準

重要インフラの制御システムは直近のセキュリティ政策の目玉である。すなわち、2021 年 5 月、Colonial Pipeline 事件が発生した。この事件では石油事業者 Colonial Pipeline 社がランサムウェア攻撃を受け（ロシアのハッカー集団だとされる）、1 週間程度石油パイプラインが停止した。このパイプラインは米国東海岸の燃料消費の半分近くのシェアを占めるものとされ、石油価格が高騰するなど、社会経済活動に大きな被害を与えた。サイバー攻撃が成功した原因として Colonial Pipeline 社のセキュリティ施策の不徹底があるとされ、制御システムに対するサイバー攻撃が実社会のインフラに被害を与えることが現実化した(71)。また、Colonial Pipeline 事件に比べると目立たないが、重要なものとして水道分野でも事件があった。2021 年 2 月、フロリダ州オールズマールの飲料水システムがサイバー攻撃を受け、水中のアルカリの量を制御するシステムが一時的に乗っ取られた(72)。これらを受け、バイデン政権は後述の国家安全保障覚書を発し、これを受け、各政府機関が重要インフラのセキュリティ対策を強化している。

○　重要インフラ制御システムのサイバーセキュリティ改善に関する国家安全保障覚書（2021 年 7 月）

バイデン政権は、2021 年 7 月、「重要インフラ制御システムのサイバーセキュリティ改善に関する国家安全保障覚書（National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems）」（以下「覚書」という）を発した(73)。これは既に試行されていた電力会社の産業用制御システムの改善を目的としたパイロットプログラム(74)を他の分野に広げるものである。すなわち、覚書は水や交通システムなどの「国家的に重要な機能」を支えているあらゆる事業体が基本的な保護機能を導入するよう奨励するものである。その意味で、情報セキュリティ・マネジメントを原則として任意なものとするアプローチからの画期となる。

覚書を受け、国土安全保障省及び商務省はセキュリティ・ベースラインの策定を義務づけられた(75)。具体的には、商務省傘下の NIST は産業用制御システム（Industrial Control Systems: ICS）のセキュリティ・ガイドラインである NIST SP 800-82 を改訂している(76)。

また、覚書を受け、これ以降、各部門ごとに行動計画などが定められ、情報セキュリティ施策の実施が分野毎に推進されていく。以下、各分野毎にみてみよう。

3.5.　その他の分野別の展開

【水道・下水分野】

○　水・廃水セクター行動計画（2022 年 1 月）

環境保護庁（Environmental Protection Agency: EPA）、国家安全保障会議（United States National Security Council: NSC）、CISA、水セクター調整協議会（Water Sector Coordinating Council: WSCC）及び水政府調整協議会（Water Government Coordinating Council: WGCC）は 2022 年 1 月、「産業用制御システム・サイバーセキュリティ・イニシアティブ - 水・下水セクター行動計画（Industrial Control Systems Cybersecurity Initiative – Water and Wastewater Sector Action Plan）」を策定した(77)。これは前掲覚書に基づいている。

ホワイトハウスのファクトシートによれば、「この計画は、電気やパイプラインのアクションプランと同様に、所有者や運営者がシステムを監視し、ほぼリアルタイムで状況認識や警告を提供する技術の導入を支援するものである。また、この計画では、サイバーセキュリティに関連する情報を政府やその他の関係者と迅速に共有することで、悪意のある行為を検知する能力を向上させる。」とされる(78)。

【鉄道分野】

○　運輸保安庁：鉄道事業者に対するセキュリティ施策の義務づけ（2021 年 12 月）

運輸保安局（Transportation Security Administration: TSA）は 2021 年 12 月、旅客・貨物鉄道事業者にサイバーセキュリティ保護の制定を義務付ける 3 つのセキュリティ指令(79)を発行した(80)。鉄道事業者は、サイバーセキュリティ調整員を任命し、24 時間以内にサイバーセキュリティ事件を CISA に報告し、サイバーセキュリティ事件対応計画を策定し、サイバーセキュリティ脆弱性評価を実施しなければならない。

【電力分野】

○　連邦エネルギー規制委員会・規則制定案（2022 年 1 月）

連邦エネルギー規制委員会（Federal Energy Regulatory Commission: FERC）は 2022 年 1 月、規則制定通知案（Notice of Proposed Rulemaking: NOPR）を採択した(81)。これは一部の電力会社についてゼロトラストの情報セキュリティ対策を義務づけ、サイバー攻撃対策を強化するものである。

4.　今後の動向と影響：2 つの GAO 報告書からの示唆

○　良い特徴

以上、拙稿(82)以降の、具体的には 2021 年以降のサプライチェーン・セキュリティ分野の動きを追った。規制手法としての特徴は、政府ネットワークと民間ネットワークを区別した上で、前者については政府調達や請負事業者に対するセキュリティ基準をてこに情報セキュリティ水準を引き上げ、他方、後者については原則として任意のアプローチを採用しつつも、政府資金をてこに一定のセキュリティ基準を事実上要求するというやり方だった。これに対して、近時はより劇的な動きがあることも見えてきた。それは前述の通り、Colonial Pipeline 事件以降の重要インフラ部門に対する直接的なセキュリティ対策の要求である。

表 2　成立した NDAA から除外された主なサイバー関連法案ないし条項

	下院法案	上院法案
官民情報共有	H.R.5440：重要インフラ事業者にサイバー・インシデントを CISA に報告することを義務づける。	
インシデント対応		S.2902：FISMA の改正法案。連邦行政機関に対しすべてのサイバー攻撃を CISA に報告し、主要な事件を議会に報告することを義務付ける。これにより CISA が連邦行政機関のネットワークにおける主導機関であることを保証する。
政府調達		S 3099：連邦政府がクラウドを安全に導入するプログラムを成文化する法案。

また、セキュリティ対策の内容としても進展がみられる。ハードウェアとソフトウェアなどの製品・サービスに対する基準に関してはいずれも一定のセキュリティ基準＋ラベル制度と部品表という手法を志向している。前者は最低限のセキュリティ水準を確保するもので、後者はそれ以上の部分をサプライチェーンの透明化により達成しようとする趣旨と理解できるかもしれない。さらに、Log4j 事件が部品表の必要性を一層高めたようである。他方、ネットワークの情報セキュリティ基準に関しては、ゼロトラストへの移行が進んでいる。これも背景には Colonial Pipeline 事件を象徴とするランサムウェアへの対抗という側面があるものと思われる。

では、以上は我が国の情報セキュリティ法政策にどのような示唆を与えるのだろうか。まず、以上の良い特徴のうち、我が国の法体系に整合する法政策のいずれもが参考になり得る。その意味で、ここで改めて良い特徴の示唆を強調する必要はないだろう。次に、むしろ、将来を予測する意味で重要なことは、米国にも足りないところはある、つまり、悪い特徴ないし欠点から得られるところかもしれない。この点を以下で敷衍して、本報告書の示唆としたい。

○　情報セキュリティ基準はどのくらい守られているか？

前項までにさまざまな情報セキュリティ基準を紹介したが、本当のセキュリティ対策はここからである。すなわち、実際に各連邦行政機関や民間事業者がセキュリティ基準を遵守しなければ、意味はない。そして、この点は米国会計検査院（Government Accountability Office: GAO）の報告書によって批判されている。すなわち、実は、NIST や CISA がいくら情報セキュリティ基準を定めても、実施はそれほど進んでいないとされる。その背景として、サプライチェーン・セキュリティの分野で調達ルールが十分に確立されていないことが指摘されており、連邦調達セキュリティ理事会（Federal Acquisition Security Council: FASC）による統一的な調達ルールの策定が期待されているとされる(83)。

この観点から見ると、上記の良い特徴を見ても、この統一的な調達ルールという点には未だいたっていないものの、着実に前進している印象を受ける。たとえば、製品・サービスに対する基準の方では、ハードウェアとソフトウェアの一定のセキュリティ基準＋ラベル制度は統一ルールに資する。他方で、ネットワークの情報セキュリティ基準に関しては、解決の方向性が見えているか疑問である。というのも、国防総省の CMMC は請負事業者の情報セキュリティ対策を認証するという点で、この解決策になった可能性があるが、結局、批判にさらされた。その意味で、情報セキュリティ対策を認証するという方策がうまくいくかどうかは CMMC 2.0 の今後の成否に関わってくるのかもしれない。その意味で、今後、我が国への示唆を考えるという意味でも、注視すべきだろう。

○　インシデント対応は十分か？

もう 1 つは特に SolarWinds 事件及び Microsoft Exchange 事件からの反省である。GAO の報告書(84)は省庁間のサイバー統合調整グループ（Cyber Unified Coordination Groups: UCG）が官－官及び官－民の情報共有及び協力に一定の役割を果たしたとしつつも、それは不十分だったとした。すなわち、特に官－民の情報共有は同時に機密情報の管理の問題も生じるため、共有が制限されていたとされる。また、技術的な問題としても、ネットワーク活動に関するデータを記録及び保存する方法が異なり、迅速な対応ができなかったとされる。その上で、報告書は連邦政府機関のサイバーセキュリティ義務を更新する法律の必要性を指摘している。

この官－民の情報共有については直近で下院から法案が提出されていたが、上院がこれを飲まず、第 117 議会第 1 会期では成立しなかったという経緯がある。すなわち、2022 年会計年度国防権限法案（S 1605）(85)は 2021 年 12 月、バイデン大統領が署名し、成立した。しかし、それまでに議会で紆余曲折があった。特に、情報セキュリティ分野においては重要な規定が削除された（参照、表 **2**）(86)。その 1 つが、下院版 NDAA（HR 4350）(87)に存在した重要インフラ事業者にサイバー・インシデントを CISA に報告することを義務づける

規定である。問題の一つは規定の内容であり、インシデントの報告の義務化自体は超党派の支持を得ていたとされるが、報告の期限や報告の仕方について折り合えなかったとされる。逆に言えば、官ー民の情報共有の必要性自体は合意されていたということになる。我が国にも参考になる議論であろう。

［付記］

脱稿後、永野秀雄「大統領令第 14028 号「国家のサイバーセキュリティの向上」に基づき制定された諸規則等及び「2022 年重要インフラに関するサイバーインシデント報告法」について」CISTEC Journal 199 号 272-307 頁（2022 年）［大統領令 14028 号及びこれに基づいて制定された行政規則を網羅的に紹介するとともに、第 117 議会第 2 会期（2022-2023 年）において成立した「2022 年包括歳出法（Consolidated Appropriations Act, 2022）」（Public law 117–103）における第 Y 編「2022 年重要インフラに関するサイバー・インシデント報告法（Cyber Incident Reporting for Critical Infrastructure Act of 2022: CIRCIA）」を解説する］に触れた。

本研究は 2021 年度福岡工業大学研究スタートアップ支援制度の助成を受けたものであり、本稿は当該助成の報告書である。そのため、助成期間以降の展開、すなわち、第 117 議会第 2 会期（2022-2023 年）における展開は反映できていない。

その他、JSPS 科研費 JP18H05216、JSPS 科研費 JP 22K13319、旭硝子財団 2022 年度採択研究助成プログラム及び公益財団法人末延財団のオンラインデータベース提供事業の助成を受けた。

文　　献

(1) 一般的に参照、橘雄介「米国におけるサイバー・サプライチェーン・セキュリティ政策の動向」情報法制研究 9 号 119-120 頁（情報法制学会、2021 年 5 月）[https://www.jstage.jst.go.jp/article/alis/9/0/9_119/_article/-char/ja]。
(2) 情報の CIA の観点から情報セキュリティ法の体系を構築したものとして、参照、岡村久道『情報セキュリティの法律〔改訂版〕』（商事法務、2011 年 11 月）。この体系を受けて、サプライチェーン・セキュリティの法政策を CIA の観点からマッピングするものとして、橘・前掲注 1。
(3) NIST, *Cyber Supply Chain Risk Management* (Project, May 2022) [https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management].
(4) NIST, *NIST Special Publication 800-161: Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, 3 (April 2015).
(5) 情報処理推進機構（IPA）「IT サプライチェーンにおける情報セキュリティの責任範囲に関する調査　調査報告書」1 頁（2019 年 4 月）。
(6) 橘・前掲注 1。
(7) 日本の判決であるが、参照、最判平成 29.10.23 判時 2351 号 7 頁［ベネッセ事件］。
(8) インシデントの実例として、参照、橘・前掲注 1・120-121 頁。
(9) 橘・前掲注 1。
(10) 橘・前掲注 1・127-128 頁。
(11) S.2902 - Federal Information Security Modernization Act of 2021, 117th Congress (2021-2022) [https://www.congress.gov/bill/117th-congress/senate-bill/2902?s=1&r=20].
(12) House Committee on Oversight and Reform, *Cybersecurity for the New Frontier: Reforming the Federal Information Security Management Act* (January 11, 2022) [https://oversight.house.gov/legislation/hearings/cybersecurity-for-the-new-frontier-reforming-the-federal-information-security]; FEDSCOOP, *House lawmakers introduce FISMA modernization legislation* (January 25, 2022) [https://www.fedscoop.com/house-lawmakers-introduce-fisma-modernization-legislation/].
(13) 従前からセキュリティ要求事項として示すものとして、NIST, *supra* note 4; Department of Defense, *CMMC Appendices*, RM.4.148 (Version 1.02, March 2020).
(14) CISA, *Ict Supply Chain Risk Management Task Force Announces New Members and Working Group* (January 11, 2022) [https://www.cisa.gov/news/2022/01/11/ict-supply-chain-risk-management-task-force-announces-new-members-and-working-group].
(15) NIST, *Frequently Asked Questions (FAQs) for NISTIRs 8259 and 8259A (Final)* (June 1, 2020) [https://www.nist.gov/itl/applied-cybersecurity/frequently-asked-questions-faqs-nistirs-8259-and-8259a-final].
(16) H.R.1668 - IoT Cybersecurity Improvement Act of 2020, 116th Congress (2019-2020) [https://www.congress.gov/bill/116th-congress/house-bill/1668].
(17) NATIONAL LAW REVIEW, *Trump Signs IoT Cybersecurity Improvement Act into Law* (December 14, 2020) [https://www.natlawreview.com/article/trump-signs-iot-cybersecurity-improvement-act-law].
(18) Executive Order 14028 of May 12, 2021, Improving the Nation's Cybersecurity [https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity].
(19) NIST, *Improving the Nation's Cybersecurity: NIST's Responsibilities under the May 2021 Executive Order* [https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity].
(20) NIST, *NISTIR 8259 Series* [https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program/nistir-8259-series].
(21) NIST, *supra* note 15.
(22) SB-327 Information privacy: connected devices.(2017-2018) [https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB327].
(23) SB2427 [https://capitol.hawaii.gov/measure_indiv.aspx?billtype=SB&billnumber=2427&year=].
(24) ENISA, *Enisa Threat Landscape for Supply Chain Attacks* (July 2021) [https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks].
(25) Microsoft, *HAFNIUM targeting Exchange Servers with 0-day exploits* (March 2, 2021) [https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/]; FBI & CISA, *FBI-CISA Joint Advisory on Compromise of Microsoft Exchange Server* (March 10, 2021) [https://www.cisa.gov/uscert/ncas/current-activity/2021/03/10/fbi-cisa-joint-advisory-compromise-microsoft-exchange-server]. 実際の被害例を紹介するものとして、*see* ENISA, *ENISA Threat Landscape 2021: April 2020 to mid-July 2021* (October 2021) [https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021].
(26) NIST, *CVE-2021-44228 Detail*, National Vulnerability Database (October 10, 2021) [https://nvd.nist.gov/vuln/detail/CVE-2021-44228]; Cyber Safety Review Board, *Review of the December 2021 Log4j Event* (July 11, 2022) [https://www.cisa.gov/sites/default/files/publications/CSRB-Report-on-Log4-July-11-2022_508.pdf].
(27) NIST, *supra* note 19.
(28) NIST, *DRAFT Baseline Criteria for Consumer Software Cybersecurity Labeling* (November 1, 2021) [https://www.nist.gov/system/files/documents/2021/11/01/Draft%20Consumer%20Software%20Labeling.pdf].
(29) NIST, *NIST Seeks Public Input on Consumer Software Labeling for Cybersecurity* (November 1, 2021) [https://www.nist.gov/news-events/news/2021/11/nist-seeks-public-input-consumer-software-labeling-cybersecurity].
(30) NTIA, *Multistakeholder Process on Software Component Transparency Framing Working Group, Framing Software Component Transparency: Establishing a Common Software Bill of Materials (SBOM) Second Edition* (2021-10-21) [https://www.ntia.gov/files/ntia/publications/ntia_sbom_framing_2nd_edition_20211021.pdf].
(31) NTIA, *Software Bill of Materials* [https://www.ntia.gov/SBOM].
(32) 連邦取引委員会（Federal Trade Commission: FTC）及び CISA によるインシデント対応については、*see* Kimberly Peretti and Jon Knight, *The Log4j Vulnerability: What This Critical Vulnerability Means For Your Enterprise*, Alston & Bird (January 18, 2022) [https://business.cch.com/CybersecurityPrivacy/SPA&B1182022.pdf?utm_campaign=Cybersecurity%20Policy%20Report%20-%20%20January%2018%2C%202022&utm_medium=email&utm_source=Eloqua&elqTrackId=918841f2d163466086c9c9954cb2c346&elq=bf26fcdf5f0b416fab6f402ed28d6517&elqaid=44459&elqat=1&elqCampaignId=14617].
(33) White House, *Readout of White House Meeting on Software Security* (January 13, 2022) [https://www.whitehouse.gov/briefing-room/statements-releases/2022/01/13/readout-of-white-house-meeting-on-software-security/].
(34) *See* Chris Hughes, *CISA's Cloud Security Technical Reference Architecture: Where it succeeds and where it falls short* (September 28, 2021) [https://www.csoonline.com/article/3634449/cisas-cloud-security-technical-reference-architecture-where-it-succeeds-and-where-it-falls-short.html]; ITI（Information Technology Industry Council）のコメントとして、*see* ITI, *ITI Recommends Streamlined Approach to OMB's Federal Zero Trust Strategy* [https://www.itic.org/news-events/news-releases/iti-recommends-streamlined-approach-to-omb-s-federal-zero-trust-strategy].
(35) CISA, *Cloud Security Technical Reference Architecture* [https://www.cisa.gov/cloud-security-technical-reference-architecture]; CISA, *Cloud Security Technical Reference Architecture Version 1.0* (August 2021) [https://www.cisa.gov/sites/default/files/publications/CISA%20Cloud%20Security%20Technical%20Reference%20Architecture_Version%201.pdf].

(36) 米国政府におけるゼロトラストの基本的な考え方については、*see* NIST, *NIST SP 800-207* [https://csrc.nist.gov/publications/detail/sp/800-207/final].
(37) OFFICE OF MANAGEMENT AND BUDGET, *Memorandum for the Heads of Executive Departments and Agencies*, M-22-05 (December 6, 2021) [https://www.whitehouse.gov/wp-content/uploads/2021/12/M-22-05-FY22-FISMA-Guidance.pdf].
(38) White House, *Office of Management and Budget Releases Federal Strategy to Move the U.S. Government Towards a Zero Trust Architecture* (January 26, 2022) [https://www.whitehouse.gov/omb/briefing-room/2022/01/26/office-of-management-and-budget-releases-federal-strategy-to-move-the-u-s-government-towards-a-zero-trust-architecture/]; OFFICE OF MANAGEMENT AND BUDGET, *Memorandum for the Heads of Executive Departments and Agencies*, M-22-09 (January 26, 2022) [https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf].
参考文献として、まるちゃんの情報セキュリティ気まぐれ日記「米国 OMB M-22-09 米国政府のゼロトラスト・サイバーセキュリティ原則への移行についての覚書」（2022 年 1 月 28 日）[http://maruyama-mitsuhiko.cocolog-nifty.com/security/2022/01/post-18c0d5.html]。
(39) NSA, *NSA Cybersecurity Advisories & Guidance* [https://www.nsa.gov/Press-Room/Cybersecurity-Advisories-Guidance/].
(40) https://media.defense.gov/2021/Dec/16/2002910260/-1/-1/0/SECURITY_GUIDANCE_FOR_5G_CLOUD_INFRASTRUCTURES_PART_IV_20211216.PDF
(41) https://media.defense.gov/2021/Dec/01/2002901540/-1/-1/0/SECURITY_GUIDANCE_FOR_5G_CLOUD_INFRASTRUCTURES_PART_III_508%20COMPLIANT.PDF
(42) https://media.defense.gov/2021/Nov/18/2002895143/-1/-1/0/SECURITY_GUIDANCE_FOR_5G_CLOUD_INFRASTRUCTURES_PART_II_20211118.PDF
(43) https://media.defense.gov/2021/Oct/28/2002881720/-1/-1/0/SECURITY_GUIDANCE_FOR_5G_CLOUD_INFRASTRUCTURES_PART_I_20211028.PDF
(44) Presidential Policy Directive (PPD) 21: Critical Infrastructure Security and Resilience (February 2013) もこの定義を踏襲している。
(45) 詳しくは、橘・前掲注 1。
(46) 参考文献として、石黒正揮「サプライチェーンにかかわるセキュリティを確保するための仕組みと制度」情報処理 62 巻 3 号 e1-e6 頁（情報処理学会、2021 年 2 月）、情報処理推進機構（IPA）「各国政府のセキュリティ政策に関する 実施体制、法制度及び認証制度調査― 調査報告書 ―」(2021 年 4 月)、橘・前掲注 1、後藤厚宏「IoT とサプライチェーンのサイバーセキュリティ対策(第 5 回)IoT サプライチェーンのセキュリティガイドライン：グローバル動向」アイソス 26 巻 8 号 10-13 頁（システム規格社、2021 年 8 月）。
(47) NIST, SP 800-161 Rev. 1 (Draft), *Cyber Supply Chain Risk Management Practices for Systems and Organizations* (April 2021) [https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/draft].
(48) *Id.*
(49) NIST, *SP 800-161 Rev. 1 (Draft): Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (2nd Draft)* (October 28, 2021) [https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/draft].
(50) *Id.*
(51) 詳しくは、橘・前掲注 1・124-125 頁。その他、参考文献として、永野秀雄「米国国防総省によるサイバーセキュリティ成熟度モデル認証(CMMC)の導入：現行の NIST SP 800-171 の遵守制度を超えて」CISTEC journal 186 号 200-215 頁（安全保障貿易情報センター、2020 年 3 月）、久野保之＝亀田繁＝土橋俊夫「変化する米国防総省のセキュリティ対策：DFARS/NIST SP 800-171 から CMMC へ」月刊 JADI 878 号 4-16 頁（日本防衛装備工業会、2020 年 7 月）、久野保之＝亀田繁＝土橋俊夫「米国連邦政府のセキュリティ対策状況：防衛業界の DFARS/NIST SP 800-171 から CMMC へ」月刊 JADI 894 号 18-28 頁（日本防衛装備工業会、2021 年 11 月）。
(52) U.S. Department of Defense, *Strategic Direction for Cybersecurity Maturity Model Certification (CMMC) Program* (November 4, 2021) [https://www.defense.gov/News/Releases/Release/Article/2833006/strategic-direction-for-cybersecurity-maturity-model-certification-cmmc-program/].
(53) Acquisition & Sustainment, CMMC DOCUMENTATION [https://www.acq.osd.mil/cmmc/documentation.html].
(54) 参考文献として、佐藤仁「Global ICT Trend 米国議員、AT&T に Huawei との提携破棄を要求：続く米中のサイバーセキュリティをめぐる対立」InfoCom T&S world trend report 347 号 14-18 頁（情報通信総合研究所、2018 年 3 月）、谷田敏一「Special ICT Report 米中貿易戦争と通信機器製造業の最新動向(前編)Huawei 製通信機器を締め出す動き」InfoCom T&S world trend report 358 号 22-32 頁（情報通信総合研究所、2019 年 2 月）、同「Special ICT Report 米国による Huawei 製 5G 機器排斥の現状：EU、英国は Huawei 製品の使用を容認」InfoCom T&S world trend report 372 号 28-41 頁（情報通信総合研究所、2020 年 4 月）、同「Special ICT Report 新型コロナウイルス感染症とスマホ業界：米政府による対 Huawei 規制強化とスマホ向けチップセットの動向」InfoCom T&S world trend report 375 号 38-51 頁（情報通信総合研究所、2020 年 7 月）、同「Special ICT Report 激変する世界のネットワーク機器業界：Huawei 製ネット機器の排斥と急激な技術進歩」InfoCom T&S world trend report 376 号 30-42 頁（情報通信総合研究所、2020 年 8 月）、同「Special ICT Report 激変する世界のネットワーク機器市場：中国 Huawei が米規制で困窮、韓国 Samsung が台頭」InfoCom T&S world trend report379 号 30-43 頁（情報通信総合研究所、2020 年 11 月）、土屋大洋「ファーウェイ問題と米中サイバー戦争 (特集 米中は新冷戦に向かうか)」外交 54 巻 32-39 頁（外務省、2019 年 3 月）、富坂聰「ファーウェイ問題に翻弄される日本 (特集 総力研究 米中激突 通信覇権はどちらが優勢か)」海外事情 67 巻 4 号 68-82 頁（拓殖大学海外事情研究所、2019 年 7 月）、高橋陽一「世界の 5G 競争における米国の現状と課題」調査レポート R&A（KDDI 総合研究所、2020 年 9 月）[https://www.kddi-research.jp/topics/2020/090701.html]。
(55) 橘・前掲注 1・126-127 頁。
(56) DEFENSE INNOVATION BOARD, *The 5G Ecosystem: Risks & Opportunities for DoD* (2019) [https://media.defense.gov/2019/Apr/03/2002109302/-1/-1/0/DIB_5G_STUDY_04.03.19.PDF].
(57) Extreme Tech, *DOD Warns the US Could Be Left in the Dust During 5G Transition* (April 4, 2019) [https://www.extremetech.com/mobile/288947-dod-warns-the-us-could-be-left-in-the-dust-during-5g-transition]; Gizchina, *US Gov Report: The US Will Lose to China in 5G Competition* (April 8, 2019) [https://www.gizchina.com/2019/04/08/us-gov-report-the-us-will-lose-to-china-in-5g-competition/]; 高島康司「米国が中国に敗北宣言？米国防総省の報告書が明らかにした「5G 戦争」の結末」Money Voice（2019 年 11 月 22 日）[https://www.mag2.com/p/money/834971]、遠藤誉「ファーウェイのスマホは本当に「スパイ」可能か――米国が「禁輸」する真の狙い」ITmedia ビジネス（2019 年 11 月 21 日）[https://www.itmedia.co.jp/business/articles/1911/20/news038.html]、Buzzap「5G 基地局から Huawei 排除を進める理由、アメリカ国防総省のレポートから明らかに」（2019 年 12 月 15 日）[https://buzzap.jp/news/20191215-5g-huawei-purge-america-defense-report/]。
(58) FCC, *Protecting National Security Through FCC Programs* (Report and Order, November 22, 2019) [https://www.fcc.gov/document/protecting-national-security-through-fcc-programs-0].
(59) FCC, *FCC Proposes New Rules for Removing Bad Actors from FCC Programs* (Notice of Proposed Rulemaking, November 22, 2019) [https://www.fcc.gov/document/fcc-proposes-new-rules-removing-bad-actors-fcc-programs-0].
(60) H.R.4998 - Secure and Trusted Communications Networks Act of 2019, 116th Congress (2019-2020) [https://www.congress.gov/bill/116th-congress/house-bill/4998].
(61) S.893 - Secure 5G and Beyond Act of 2020, 116th Congress (2019-2020) [https://www.congress.gov/bill/116th-congress/senate-bill/893].
(62) H.R.3919 - Secure Equipment Act of 2021, 117th Congress (2021-2022) [https://www.congress.gov/bill/117th-congress/house-bill/3919].
(63) White House, *Executive Order on Securing the Information and Communications Technology and Services Supply Chain* (May 15, 2019) [https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/]; Executive Order 13873 of May 15, 2019, Securing the Information and Communications Technology and Services Supply Chain (84 FR 22689) (Executive order) [https://www.federalregister.gov/citation/84-FR-22689].
(64) DoC, *Department of Commerce Announces the Addition of Huawei Technologies Co. Ltd. to the Entity List* (Press release, May 15, 2019) [https://www.commerce.gov/news/press-releases/2019/05/department-commerce-announces-addition-huawei-technologies-co-ltd].
(65) Bureau of Industry and Security, *Export Administration Regulations: Amendments to General Prohibition Three (Foreign-Produced Direct Product Rule) and the Entity List* (May 19, 2020) [https://www.federalregister.gov/documents/2020/05/19/2020-10856/export-administration-regulations-amendments-to-general-prohibition-three-foreign-produced-direct].
Also see Mobile World Live, *Trump renews telecom trade ban* (May 14, 2020) [https://www.mobileworldlive.com/featured-content/top-three/trump-renews-telecom-trade-ban]; 日本貿易振興機構（ジェトロ）「米商務省、ファーウェイおよび関連企業への輸出管理を強化、米技術を用いた外国製造製品も対象」（2020 年 5 月 19 日）[https://www.jetro.go.jp/biznews/2020/05/53b8c3153447-25c7.html]。
(66) Department of Commerce, *Securing the Information and Communications Technology and Services Supply Chain*, Federal Register Vol. 86, No. 11 (January 2021, Docket No. 210113–0009).
(67) U.S. Senate Committee on Commerce, Science, & Transportation, *Committee Investigation Suggests Leading Technology Company Violated Huawei-related Rule* (October 26, 2021) [https://www.commerce.senate.gov/2021/10/committee-investigation-suggests-leading-technology-company-violated-huawei-related-rule].
(68) In the Matter of Pacific Networks Corp. and ComNet (USA) LLC GN Docket No. 20-111.
(69) China Telecom (Americas) Corp. v. FCC and U.S. (case 21-1233).
(70) FCC, *FCC Revokes China Unicom Americas' Telecom Services Authority* (January 27, 2022) [https://www.fcc.gov/document/fcc-revokes-china-unicom-americas-telecom-services-authority].
(71) 参考文献として、永野秀雄「重要インフラに対する標的型ランサムウエア攻撃と米国の対応：コロニアルパイプライン社事件後の展開」CISTEC journal 195 号 243-266 頁（安全保障貿易情報センター、2021 年 9 月）、日本経済新聞「米最大の石油パイプライン、サイバー攻撃で停止」（2021 年 5 月 9 日）[https://www.nikkei.com/article/DGKKZO71689440Z00C21A5EA2000/]、日本経済新聞「石油会社サイバー攻撃、「ダークサイド」の犯行 FBI」（2021 年 5 月 11 日）[https://www.nikkei.com/article/DGXZQOGN10DBA0Q1A510C2000000/?n_cid=NMAIL006_20210511_A]。
(72) IT Media「水道局の水処理システムにハッカーが侵入し、飲料水の汚染試み フロリダ州で」（2021 年 2 月 9 日）[https://www.itmedia.co.jp/news/articles/2102/09/news137.html]。
(73) White House, *National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems* (July 28, 2021) [https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorand

um-on-improving-cybersecurity-for-critical-infrastructure-control-systems/].
(74) Energy.gov, *Biden Administration Takes Bold Action to Protect Electricity Operations from Increasing Cyber Threats* (April 20, 2021) [https://www.energy.gov/articles/biden-administration-takes-bold-action-protect-electricity-operations-increasing-cyber-0].
(75) U.S. Department of Commerce, *Joint Statement by Secretaries Mayorkas and Raimondo on President Biden's New National Security Memorandum* (July 28, 2021) [https://www.commerce.gov/news/press-releases/2021/07/joint-statement-secretaries-mayorkas-and-raimondo-president-bidens-new].
(76) NIST, *White House National Security Memo Issued | NIST & DHS Developing Cybersecurity Performance Goals for Critical Infrastructure Control Systems* (July 29, 2021) [https://www.nist.gov/news-events/news/2021/07/white-house-national-security-memo-issued-nist-dhs-developing-cybersecurity].
(77) U.S. Environmental Protection Agency, *EPA Announces Action Plan to Accelerate Cyber-Resilience for the Water Sector* (January 27, 2022) [https://www.epa.gov/newsreleases/epa-announces-action-plan-accelerate-cyber-resilience-water-sector]; White House, *Fact Sheet: Biden-Harris Administration Expands Public-Private Cybersecurity Partnership to Water Sector* (January 27, 2022) [https://www.whitehouse.gov/briefing-room/statements-releases/2022/01/27/fact-sheet-biden-harris-administration-expands-public-private-cybersecurity-partnership-to-water-sector/].
(78) *Id.*
(79) Enhancing Rail Cybersecurity - SD 1580-21-01; Enhancing Public Transportation and Passenger Railroad Cybersecurity - SD 1582-21-01; Enhancing Surface Transportation Cybersecurity - IC 2021-01 [https://www.tsa.gov/for-industry/surface-transportation-cybersecurity-toolkit].
(80) TSA, *DHS Announces New Cybersecurity Requirements for Surface Transportation Owners and Operators* (December 2, 2021) [https://www.tsa.gov/news/press/releases/2021/12/02/dhs-announces-new-cybersecurity-requirements-surface-transportation].
(81) FERC, *FERC Moves to Close Gap in Reliability Standards for Electric Grid Cyber Systems* (January 20, 2022) [https://www.ferc.gov/news-events/news/ferc-moves-close-gap-reliability-standards-electric-grid-cyber-systems]; FERC, *Staff Presentation | Notice of Proposed Rulemaking (NOPR) Regarding Internal Network Security Monitoring for High and Medium Impact Bulk Electric System Cyber Systems* (January 20, 2022) [https://www.ferc.gov/news-events/news/staff-presentation-notice-proposed-rulemaking-nopr-regarding-internal-network-0].
(82) 橘・前掲注 1。
(83) GAO, *Information Technology ―Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risk*s, GAO-21-171, highlights (December 2020) [https://www. gao.gov/products/GAO-21-171#summary].
(84) GAO, *Cybersecurity: Federal Response to SolarWinds and Microsoft Exchange Incidents*, GAO-22-104746 (Jan 13, 2022) [https://www.gao.gov/products/gao-22-104746].
(85) S.1605 - National Defense Authorization Act for Fiscal Year 2022, 117th Congress (2021-2022) [https://www.congress.gov/bill/117th-congress/senate-bill/1605].
(86) *See* H.R.5440 - Cyber Incident Reporting for Critical Infrastructure Act of 2021, 117th Congress (2021-2022) [https://www.congress.gov/bill/117th-congress/house-bill/5440]; S.2902, *supra* note 11; S.3099 - Federal Secure Cloud Improvement and Jobs Act of 2021, 117th Congress (2021-2022) [https://www.congress.gov/bill/117th-congress/senate-bill/3099/all-actions?s=1&r=14&overview=closed].
(87) H.R.4350 - National Defense Authorization Act for Fiscal Year 2022, 117th Congress (2021-2022) [https://www.congress.gov/bill/117th-congress/house-bill/4350/text].