諸外国における
基幹的なインフラに対する妨害行為と
その対応の状況に関する調査

ボストン コンサルティング グループ
調査報告書　2024年2月8日

調査報告書の構成 (目次)

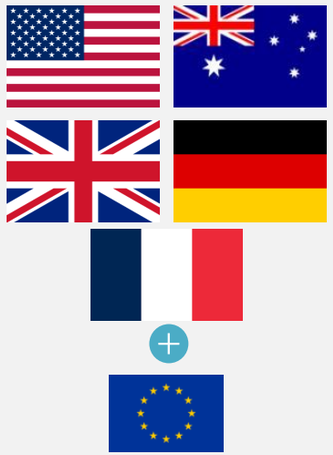
調査対象項目

各国の基幹インフラに対する妨害行為の防止のための制度を調査するとともに、
当該制度に基づき、実際に設備の導入等が認められなかった事例/懸念が示された事例について、情報を収集する

諸外国の制度調査

調査対象国の基幹インフラに対する妨害行為の防止のための制度の調査

対象5ヶ国 + EU



(概観のみ)

×

調査項目

インフラ防衛政策全体概観
(対内直投/サイバー含む)

内容・目的・趣旨	届出書等の記載事項
規制対象分野	審査スキーム
規制対象者	審査方法
規制対象行為	審査基準

事例の収集

調査対象国の基幹インフラに対する妨害行為の防止のための制度で設備の導入等が認められなかった事例等についての情報収集

事例 × 導入等が認められなかった理由について、公表情報から分析

調査の手法

政府機関等の公表情報や文献等の情報を基に調査を実施、
必要に応じ、当該制度等に関して知見を有する専門家にも調査を実施

調査内容

調査対象国の基幹インフラに対する妨害行為の防止のための制度について、以下を調査

- 内容・目的・趣旨
- 規制対象分野
- 規制対象者
- 規制対象行為
- 届出書等の記載事項
- 審査スキーム
- 審査方法及び審査基準

等

実施方法[1]

5ヶ国等の政府関連機関の公表資料を中心に文献調査 (下記は主なもの)

米国

- Federal register
- Congressional Research Service
- Department of Commerce

英国

- Legislation.gov.uk
- Department for Digital, Culture, Media & Sport
- Cabinet office

オーストラリア

- Legislation.gov.au
- Department of Home Affairs
- Cyber and Infrastructure Security Centre

ドイツ

- Bundessetzblatt
- Bundesministerium des Innern und für Heimat

フランス

- Légifrance
- Agence nationale de la sécurité des systèmes d'information

その他、政府機関等のレポートも補完的に参照 (以下は例示)

- 経済産業省
- 総務省　等

必要に応じ、専門家に対し、調査を実施

Note：各参照URLの最終アクセス日は2024年1月31日である

各国の主な制度の比較 [1/4]

		日本	米国	英国	オーストラリア	ドイツ	フランス
基本情報	法令名称	経済安全保障推進法	情報通信技術・サービス (ICTS) サプライチェーン保護規則	電気通信 (セキュリティ) 法 2021	重要インフラ安全保障法	ITセキュリティ法2.0	LOI n° 2019-810
	制定時期	2022年5月	2021年1月	2021年11月	2018年4月	2021年5月	2019年8月
	概要 (制度全体/妨害行為防止措置)	安全保障の確保に関する経済施策の総合的/効果的な推進のため、基本方針の策定とともに所要の制度を創設 • **基幹インフラ役務の安定的な提供確保** 等	外国敵対者が関連し、**米国に過度/許容できないリスクをもたらす**と判断した場合、**商務省による取引の禁止等を可能に**	通信事業者に対し、指定したハイリスクベンダーの**製品・サービスの使用禁止も含めた指示**を可能に **通信事業者に対し、セキュリティ義務遵守を求め、政府の関係機関に権限を付与**	**重要インフラ資産**を所有・運営する事業者等に関し、**資産登録/リスク管理プログラムの制度等**を導入し、**政府による指示/情報収集権限**を付与	**重要部品を新たに使用**する**重要インフラ事業者が事前に政府から許可を得る**仕組みを創設	5G以降の無線通信網を用いて接続する設備の使用に、**政府の許可を要するとする**もの
	類型 (審査/命令の方式)	事業者からの**事前届出の審査** • 一定の基準のもと対象とする事業/事業者を指定し、指定された重要設備の導入・維持管理等の委託をしようとする際、届出を行い審査を受ける必要あり • 国は、妨害行為の手段として使用されるおそれが大きいと認めるときは、勧告/命令	他省庁からの要請・裁量等を契機とした審査 • 関連する情報や他省庁からの要請、裁量により、照会の検討が可能 • 情報等を踏まえて審査を実施し、必要な場合は取引の禁止等を判断 • 違反した場合、罰則の対象	ハイリスクベンダーを指定、通信事業者に対し、当該ベンダーの製品の使用に要件等を設定 • 国家安全保障上、懸念がある事業者を主務大臣が指定 • 通信事業者による当該製品の使用等に関し、要件を設定	安全保障上のリスク低減等について、事業者に対して指示が可能 • 安全保障上のリスクを排除/低減するために合理的に必要であること • 誠実に交渉するための合理的な措置がとられていること • 事業者に安全性について不利な評価がなされていること　等を条件	事業者からの**事前届出の審査** • 重要な部品を新たに使用する重要インフラ事業者は、保証宣言と合わせ政府に届出を提出 • 政府は関係省庁間で審査基準に基づき審査 • 安全保障政策上の利益に反すると認めるときは、利用禁止の命令も可能	事業者からの**事前申請を審査、許可を付与** • 事業者は、対象機器の使用につき政府に事前に申請 • 政府は審査し許可を付与 - 最大8年間 - 条件が付与される場合や、却下される場合もあり

各国の主な制度の比較 [2/4]

		日本	米国	英国	オーストラリア	ドイツ	フランス
対象	対象インフラ分野	**14カテゴリーを指定** • 電気 • ガス • 石油 • 水道 • 鉄道 • 貨物自動車運送 • 外航貨物 • 航空 • 空港 • 電気通信 • 放送 • 郵便 • 金融 • クレジットカード	**6カテゴリーを指定** • 重要インフラ - 化学、商業用施設、情報通信、重要製造業 (自動車、金属 等)、ダム、防衛産業基盤、緊急サービス、エネルギー、金融、食品・農業、政府施設、ヘルスケア・公衆衛生、情報技術、原子力燃料・処分、交通システム、上下水道システム • 情報通信インフラ・衛星 • 機微な個人情報処理 • 監視、住宅管理、ドローン • 情報通信ソフトウェア • 最新技術 (AI、量子コンピューティング 等)	**公衆電子通信ネットワークまたは公衆電子通信サービスの提供者**	**11カテゴリーを指定** • 通信 • データ保管・処理 • 金融・証券 • 水道・下水 • エネルギー • ヘルスケア・医療 • 高等教育・研究 • 食品・食料品 • 交通 • 宇宙技術 • 防衛	**8カテゴリーを指定** • エネルギー • 水 • 食品 • 情報技術・通信 • 医療 • 金融・保険 • 交通・運輸 • 自治体廃棄物処理	**安全保障上、重要な通信事業者**
	対象機器/部品	分野毎に指定した**重要設備**に係る**設備の導入・維持管理等の委託**	米国の司法権の対象となる財産、活動等のうち、上記6カテゴリーに**分類される技術**に関するもの	**ハイリスクベンダーとして指定された事業者**が提供する製品・サービス	各分野それぞれにおいて設定された要件に該当する**重要インフラ資産**	重要インフラで用いられ、可用性、完全性等が損なわれることで**重要インフラの故障等が引き起こされるIT製品** 等	**5Gネットワーク関連装置** • 5Gネットワークにおける端末機器の認証、無線リソースの割当てや、機能実行/セキュリティ等に関連する装置 等

各国の主な制度の比較 [3/4]

プロセス

	日本	米国	英国	オーストラリア	ドイツ	フランス
事業者による主な情報提供の内容	**導入等計画書の提出** • 設備概要/導入内容/時期、供給者の名称/設立準拠法国 • リスク管理措置の実施状況	特段無し • 事業者からの申請プロセス/届出書等は未整理 • 商務省が得た情報/他機関からの要請/裁量等により審査を開始	対象ネットワーク/サービス/資産、関連する情報、自身のセキュリティ遵守状況を、**Ofcomに提出**	**資産の運用状況等を登録** • 所在地、サービスを提供する地域、事業体に関する情報 等 **リスク管理プログラムに係る年次報告をCISCに提出**	**重要部品の新たな使用の際、届出を実施** • 設備の安全性の保証の宣言 等	**対象機器の使用に際し、下記の情報を提出し申請** • 機器の概要・特性、使用目的 • 設置方法、運用手順 • 検査を受けることの確約 等
審査基準・考え方/審査期間	下記内容を基に判断 • 供給者への外部の主体からの強い影響の有無 • 事業者によるリスク評価、リスク管理措置の内容 • 脆弱性/不適切性や基準等の不遵守が指摘された例 等 審査期間は原則30日間(最長4か月)	下記内容を基に判断 • 対象製品・サービスの性質・特徴 • 関係者の所有態様/供述・行動 • リスク・脆弱性 照会/受理判断から、180日以内に最終判断 • 書面で決定した場合は延長可能	下記内容を基に判断 [ハイリスクベンダーの指定] • 提供される製品・サービスの性質や品質・信頼性・安全性 • 関係者の身元 等 [事業者に対する指示] • 国家安全保障上の必要性 • 指示内容と指示により達成しようとすることが比例していること 等 ※ 検討期間については法令上特段言及なし	下記内容を基に判断 • 当該事業者についての、安全性についての不利な評価の内容 • 指示に従うことにより発生する可能性のある費用/競争に及ぼす可能性のある影響 • 事業者/行政機関の意見 ※ 検討期間は、法令上、特段言及無し	下記内容を基に判断 • 製造者が第三国政府に支配されている可能性 • 製造者の悪影響を及ぼす活動の有無 • 安全保障政策の目的との合致 等 届出受領後2ヶ月経過するまで禁止/命令可能(4か月まで延長可能)	下記内容を基に判断 • 防衛と国家安全保障の利益への重大なリスクの懸念 • ネットワーク・サービスの永続性、品質、可用性、セキュリティの欠如 • 送信内容の機密性・中立性の担保 • セキュリティへの脅威・攻撃への対応 2か月間回答がない場合、却下とみなす規定あり

各国の主な制度の比較 [4/4]

		日本	米国	英国	オーストラリア	ドイツ	フランス
運用状況	当該制度に関連する命令等の事例	–	特段情報なし (参考) Huawei等の製品について、政府調達や認証が禁止されている例あり	**Huaweiを指定事業者とし、35事業者に対し、段階的に同社製品の使用を禁止**	**Huawei/ZTEの使用が禁止** • Huawei/ZTEが、政府より個別に通知があり、自社の製品が禁止された旨を開示 ※「重要インフラ安全保障法」と別の「電気通信法」の事例	特段情報なし • Huaweiの禁止に係る議論がなされている旨の報道等はあり	**Huawei製品が拒否された事例は存在** • 却下された申請が、Huawei関連製品である旨の議員の発言あり
	事例に係る情報の公開状況	–	特段情報なし (参考) Huawei等の製品について、安全保障上容認できないリスクがあることを理由に政府調達や認証が禁止されている例あり	**法令に基づき、Huaweiを指定し、事業者に対し使用を禁止した事実を、理由を含め詳細に公表** • 中国/関係者による英国へのサイバー攻撃の実績と今後の予測 • 国家情報法等、中国から中国に拠点を置く企業への指示があること • エンジニアリングプロセス上のサイバーセキュリティの評価 • 米国による経済制裁 等	**政府側からは個別企業の明確な名指しせず** • 安全保障上のリスクと対応を一般的に呼びかける「ガイダンス」に留まる ※「重要インフラ安全保障法」と別の「電気通信法」の事例 (参考) 重要インフラ安全保障法における資産の登録件数等を、報告書で公開	特段情報なし	**申請件数/拒否件数等は一部公になっている** • 政府は年次報告を通じ、申請/拒否件数と、その影響を議会に要提出 **個別事例の公表や、詳細な理由の公表はなし**

米国全体のポイント

2-2-1

注) 1 等の番号は、後述の制度パート(3-1-2) での対応番号を示す

制度の概要

政府機関に対する調達制限、民間企業に対する規制措置に加え、補助の要件も含め、重畳的に実施

- 「情報通信技術・サービス (ICTS) サプライチェーン保護規則」(以降、「ICTS規則」(1)) において、商務省による審査や指示を可能に

ICTS規則においては、インフラ事業者や情報通信関連事業者を幅広く対象。政府の裁量等で審査が可能

- 各重要インフラ、情報通信インフラ・衛星、監視・住宅管理・ドローン、情報通信ソフトウェア、最新技術

更に、対象国として中国/ロシア/北朝鮮等の6つの主体を特定した上で、審査の観点を示している

- 香港を含む中国、キューバ、イラン、北朝鮮、ロシア、およびベネズエラの政治家ニコラス・マドゥロ (マドゥロ体制) の6つの主体を指定
- 「① 技術・サービスの性質・特徴」や、「② 関係者の所有等の態様/供述・行動」、「③ リスク・脆弱性」を基に判断
- 特に「②」については、特定の供述及び行動も勘案するとされている

事例の概要

米国では、ICTS規則に基づく命令等の事例公表はないものの、制度自体は運用

- ICTS規則の施行前に、同規則に関し、複数の中国企業に召喚状が送られた旨の声明の発出あり (2021年3月)

上記以外に、安全機器法 (3) により、Huawei等中国企業5社の米国内での認証を不承認に (事実上の使用禁止)

- 安全で信頼できる通信ネットワーク法 (2) により政府補助金の利用は禁止されていた
- また、国防権限法2019 (4) により、政府による直接調達や規制対象機器を使用した企業と政府間との契約も禁止されていた
- これに加え、上述の安全機器法により、認証も不承認に
- なお、トランプ政権時代は、大統領令に基づきTikTok、WeChat、Alipay等を始めとする決済アプリを取り扱う中国企業の取引が制限 (いずれも撤廃)

なお、CHIPSプラス法 (8) における補助金の対象事業者は、受給日から10年間は、中国他懸念ある国で、重大取引に従事しない等の合意を商務長官と結ぶことを義務付け

英国全体のポイント

注) 1 等の番号は、後述の制度パート(3-2-2) での対応番号を示す

制度の概要

国内においてHuaweiのシェアが大きく、米国のHuaweiのエンティティリスト (Entity List：EL) への追加にも強い問題意識

- 英国は、通信市場においてHuaweiのシェアが非常に大きかった
- また、米国の貿易上の取引制限に係るELに追加されたことで、同社製品のセキュリティがより脆弱になることを懸念
- 英国は、中国からサイバー攻撃を受けていると認識しており、中国の近年の立法 (国家情報法) にも懸念

国内の情報通信のサプライチェーンのレビュー等も踏まえ、安全保障上の取引制限の観点から、情報通信インフラの制度を整備

- 「電気通信 (セキュリティ) 法 2021」(1) を制定し、通信法を改正
- これにより、情報通信事業者のセキュリティ義務を強化し、これを担保するため、所管省庁 (Ofcom) の権限を強化
- また、ハイリスクなベンダーを指定し、その製品等に関して通信事業者に対して指示を出すことも可能に

事例の概要

通信法により、"Huawei" の企業名も公に

- i) ハイリスクなベンダーを指定する「指定事業者の指定通知」において、Huaweiを指定
- ii) 35の通信事業者に対し、その機器の使用を制限する指示を発出

上記の i) 指定事業者の指定通知、ii) 提供者に対する指示 において、それぞれの理由を詳細に記載

- i) 指定事業者の指定通知において、中国・その関係者による英国へのサイバー攻撃の事実に言及
  - 政府として、中国及びその関係者が、英国にサイバー攻撃を実行しており、今後も実行すると評価
- ii) 提供者に対する指示においては、30頁弱に渡り、通信関連事業者に対し、Huaweiの機器使用を段階的に禁止する旨や対象、その根拠を詳細に記載

オーストラリア全体のポイント

注) 1 等の番号は、後述の制度パート(3-3-2) での対応番号を示す

制度の概要

重要インフラ安全保障法 (1) において、幅広い分野のインフラを対象に、関連する資産の登録やリスク管理を義務付けるとともに、安全保障上必要な場合は、政府による指示も可能としている

- 同法は11のセクターが対象
- 関連する資産や利害関係/支配の情報を登録する必要あり
- 自身でリスクを管理するためのプログラムも導入
- 安全保障上必要な場合は、政府が事業者に対し、何らかの行為を取るよう、「指示」を出すことも可能
  - 但し、政府と事業者が誠実に交渉することが前提であり、「指示」はそれが整わなかった場合、という建付け

加えて、電気通信分野においては、電気通信法に国家安全保障の要素を追加し (TSSR[1] ：電気通信部門の安全保障改革 (2))、通信事業者に対して措置 (導入自体は、TSSR が重要インフラ安全保障法に先立って実施)

事例の概要

上述のTSSRに基づき、政府から、「オーストラリアの法律に反する外国政府からの指示に従う可能性のあるベンダー」へのリスク喚起と、それへの対応を呼びかけるガイダンスが提供されている

- 同ガイダンス内では、通信事業者への5Gネットワークでのリスク喚起とTSSRに基づき通信事業者にリスクへの対応義務が課される旨の言及に留まり、「中国」や中国事業者名への言及はない

1. Telecommunication Sector Security Reforms：電気通信法を改正する形で導入された電気通信sectorのセキュリティ強化のための改革

ドイツ全体のポイント

注) 1 等の番号は、後述の制度パート(3-4-2) での対応番号を示す

制度の概要

ITセキュリティ法2.0 (1) において、幅広い分野の重要インフラを対象に、窓口の登録や不具合発生時の通知を義務付けるとともに、「重要な部品」の配備の前に事前届出を求め、必要な場合、政府が命令/禁止をすることが可能

- 同法は、エネルギー/情報通信/金融/医療等、幅広いセクターが対象
- 「重要な部品」を配備する前は、重要部品及びその配備計画の種類を届け出る必要あり
- 政府は、自国の安全保障を損なう懸念が高い場合は、命令/禁止を行うことが可能

更に、EUのNIS2指令の国内実施、及びサイバーセキュリティの更なる強化のため、ITセキュリティ法3.0 (2) も議論されているところ

- 対象分野等の更なる拡大等が予定

事例の概要

ITセキュリティ法2.0に基づく資産の登録等の運用は始まっているものの、個別事例の公表はされておらず、適用事例はない状況

- 一方で、Huawei製品の禁止の議論に係る報道等も見られる

フランス全体のポイント

注) 1 等の番号は、後述の制度パート(3-5-2) での対応番号を示す

制度の概要

通信事業者に対し、「LOI n° 2019-810」(これに基づく郵便・電子通信法の改正)(1) により、5Gに用いられるハードウェア/ソフトウェアについて審査/許可の制度を導入

- 政府は審査した上で、最大8年間の使用を許可 (条件を付けることも可能)
- 各通信事業者からの申請に基づき、審査/承認/許可された実績もある模様

加えて、EU NIS指令の国内実施のため、対応法令 (LOI n°2018-133 (2)) も制定

- 重要インフラ事業者を指定し、事業者に、情報提供/リスク管理/インシデント報告の義務を課すもの

また、2013年の段階から、国防の観点でCIIP法 (3) において、幅広い分野の重要インフラを対象に、監査の仕組みも導入済

更に、ドイツと同じく、EU NIS2指令 (4) への対応に向けた議論を行っているところ

- 一方で、現段階では、ドイツのように具体化までは至っていない状況

事例の概要

「LOI n° 2019-810」に基づき事前審査制度は導入され、運用されているものの、個別事例の公表はされていない状況

一方で、「LOI n° 2019-810」に基づき、拒否件数やその影響等は議会に提出され、一部公になっている

- 同法において、政府が国会に対し、適用状況について件数やコスト等を含む年次報告書を提出することが義務付けられている
- 上記に基づき、提出された報告書にて、申請件数等が記載

なお、**仏関連議員の発言に、"申請の拒否や承認の短縮が決定されたものは全てHuaweiのハードウェアに関わるものだった"、という趣旨**のものあり

3-1.米国

1. 政策の全体像

2. 制度の調査結果
   - ICTS規則 (1)
   - その他のインフラ防護等に関する法令 等

3. 事例

3-1.米国

1. 政策の全体像

2. 制度の調査結果
   - ICTS規則 (1)
   - その他のインフラ防護等に関する法令 等

3. 事例

米国の基幹インフラ妨害行為の防止に係る政策の全体像

政府機関に対する調達制限、民間企業に対する規制措置に加え、補助の要件も含め、重畳的に実施

主な対象行為		主な対象者		
		国内企業・政府機関		外国企業
		基幹インフラ関連事業者	政府機関	
取引規制	製品/役務の調達	① **ICTS[1] サプライチェーン保護規則** • 商務省が外国敵対者からの製品/サービスの調達を審査 主な制度 (詳細深掘)	④ **国防権限法2019 (NDAA2019)** • 中国5社について、米国政府による当該製品・サービスの調達等を禁止	
		② **安全で信頼できる通信ネットワーク法** • FCC[2]が、安全保障上のリスクをもたらす企業の製品/サービスを公表し、政府補助金の利用による中国通信機器企業等との取引を禁止		
		③ **安全機器法/同法に基づく行政命令** • 米国の安全保障上容認できないリスクがあるとされた対象機器へ米国内使用のための認証を全面的に禁止		
	対内直接投資			⑤ **外国投資リスク審査現代化法 (FIRRMA)** • 安全保障上懸念のある外国人による(非) 支配的投資や、空港・港湾/米軍施設に近接する土地等の取得を審査
サイバー攻撃への防護		⑥ **サイバーセキュリティー・パフォーマンス・ゴールズ (CPGs)** • インフラ事業者が取るべきセキュリティ対策について、具体的な対策等を提示	⑦ **サイバーセキュリティに関する大統領令14028** • 連邦政府のサイバーセキュリティに関する要件を設定。関連するガイドラインを策定	
補助要件 等		⑧ **CHIPSプラス法** • 補助金の対象事業者は、受給日から10年間は中国他懸念ある国で、重大取引に従事しないとの合意を商務長官と結ぶことを義務付け		

Note：上記分類は、本調査の目的から、関連が深いと考えられる法令を抽出し、主な目的/対象の相違等を強調するために整理をしたものであり、必ずしも上記各範囲の内容のみを含むとは限らない
特に、国内企業には、国内にて事業活動を行う外国企業も含まれうる

1. Information and Communications Technology and Services, 情報通信技術・サービス　2. Federal Communications Commission, 連邦通信委員会

3-1.米国

1. 政策の全体像

2. 制度の調査結果
   - ICTS規則 (1)
   - その他のインフラ防護等に関する法令 等

3. 事例

「ICTS規則」概要 [1/2]

法令等の名称

- "情報通信技術とサービスのサプライチェーンの保護"
  (商務省 規則)

制定時期

- 2021年1月19日 最終暫定規則公表/パブコメ開始
- 2021年3月22日 施行
- 2023年6月16日 大統領令14034に基づき改正
  (ソフトウェアアプリケーションが追加)

制定の経緯

- トランプ政権下、**連邦政府の調達**には、リスクの高い機器の**利用は禁止**されていた
- 更に、**民間取引**においても、リスクの高い機器を利用する場合に禁止する措置を取れるよう、2019年5月、**大統領令第13873号が公布**
  - 実施は**商務省の規則に委任**
- バイデン政権への移行直前 (2021年1月) に、**大統領令を実施する商務省規則が公表**
- パブコメを経て、同年3月に施行

妨害防止措置の概要

- 情報通信に関する取引に「**外国敵対者**」が関連し、米国に過度又は許容できないリスクをもたらす場合、**商務省**がこれを審査し、**取引中止**又は**リスクの軽減措置**を取る

外国敵対者

- **下記6主体と定義**
  - 中国 (香港を含む)
  - キューバ
  - イラン
  - 北朝鮮
  - ロシア
  - ベネズエラ (ニコラス・マドゥロ政権体制)

対象分野

- **重要インフラを中心に広範に対象に指定**
  - 重要インフラ (交通、金融、電力、基幹製造業 等)
  - 情報通信インフラ・衛星
  - 機微な個人情報処理
  - 監視、住宅管理、ドローン
  - 情報通信ソフトウェア
  - 最新技術 (AI、量子コンピューティング 等)

「ICTS規則」概要 [2/2]

審査プロセス

照会/受理判断

- **情報の受領/連邦機関の長からの要請/商務省の裁量**を契機に、商務省が照会準備を開始
- 取引が外国敵対者や、技術の要件を満たすかを判定し、受理するか否か判断

初期審査

- 受理後、当該取引が容認できないリスクをもたらすと判断した場合、**省庁間協議**を実施する

初期判断

- 初期審査で全面的に許可しない限り、**商務省は取引の当事者に通知**
- 当事者は**30日以内に回答**、改善策を提案

最終判断

- 商務省は、下記のいずれかに該当する**最終決定書**を**当事者に通知**する
  - 取引を**許可**する
  - 全面的に**禁止**する
  - **リスク軽減措置**を条件に許可する

審査基準

主に以下3つの観点で審査

- **対象となる製品・サービスの性質・特徴**
  - 問題となる情報通信技術又はサービスの性質及び特徴
- **関係者の所有等の態様/供述・行動**
  - 取引において問題とされている設計、開発、製造又は供給に対する外国敵対者による所有、支配、指示又は管轄の性質及び特徴 等
- **リスク・脆弱性**
  - 取引の個別的又は永続的な脅威をもたらす可能性 等

罰則

- 違反者には、行政罰、刑事罰が適用

「ICTS規則」詳細 [1/10]：名称/制定時期 等

「ICTS規則」は、大統領令を根拠に取引制限・禁止措置等を制定

法令等の名称	• **Securing the Information and Communications Technology and Services Supply Chain** (A Rule by the Commerce Department) - "情報通信技術とサービスのサプライチェーンの保護" (商務省 規則)
制定時期	• 2021年1月19日 最終暫定規則 (Interim Final Rule (IFR)) 公表/パブリックコメント開始 • 2021年3月22日 施行 • 2023年6月16日 大統領令第14034号に基づき、対象業種にソフトウェアアプリケーションを追加
制定の経緯	• 2019年5月15日、トランプ政権下にて、「大統領令第13873号」(情報通信技術及びサービスのサプライチェーンの安全確保) が発令 - 元々、国防権限法2019に基づき、連邦政府での調達は禁止されていた - 加えて、民間取引においても、国際緊急経済権限法 (IEEPA) に基づき、高いリスクがある機器等を利用する場合に一定の制限・禁止措置がとれるよう、本大統領令を公布 • その後、19年11月に最初の下位規則案が公表 (範囲が広範で曖昧との批判が産業界からなされ、更に検討) • 2021年1月19日 (トランプ政権最終日) に、暫定最終規則 (IFR) が公表 - 同年1 月のバイデン政権移行後も、産業界から反発あり (2月4日には、無期限停止を要請する共同書簡が提出) - モンド商務長官候補 (当時) が、1 月下旬段階では見直しの可能性に言及 • 特段の変更なく、3月22日に施行

Source: Congressional Research Service "The Information and Communications Technology and Services (ICTS) Rule and Review Process", Federal Register, Securing the Information and Communications Technology and Services Supply Chain, Executive Order on Securing the Information and Communications Technology and Services Supply Chain、Federal Register : Securing the Information and Communications Technology and Services Supply Chain; Connected Software Applications、Executive Order 14034、White House "FACT SHEET: Executive Order Protecting Americans' Sensitive Data from Foreign Adversaries"、CISTEC事務局「米国の民間分野における中国製IT機器の利用取引規制の経緯と内容について ―「情報通信技術・サービス・サプライチェーン・セキュリティ確保大統領令 13873」の下位暫定最終規則の施行」(2021.4.20)

(参考)「大統領令第13873号」の概要

名称	• **Securing the Information and Communications Technology and Services Supply Chain** (Executive Order 13873 of May 15, 2019)
制定年度	• 2019年 (トランプ政権)
制定の経緯	• 元々、国防権限法2019に基づき、連邦政府での調達は禁止されていた • 加えて、民間取引においても同様の規制の必要性が認識 • 国際緊急経済権限法 (IEEPA) を根拠に、高リスクの機器等を利用する場合に一定の制限・禁止措置がとれるよう措置
主な内容	• 下記の外国企業の情報通信技術・サービス (ICTS) を含む取引の禁止等を可能にする – (1) 米国内のICTSに妨害工作や破壊工作を行う不当なリスクをもたらすもの – (2) 米国の重要インフラやデジタル経済のセキュリティや回復力に壊滅的な影響を及ぼす過度のリスクがあるもの – (3) 米国の国家安全保障や米国人の安全保障に許容できないリスクがあるもの • 実施は、商務省 (Department of Commerce) に委任

Source: Executive Order on Securing the Information and Communications Technology and Services Supply Chain

(参考) ICTS規則の背景/制度趣旨

背景/制度趣旨

- 情報通信技術とサービス (ICTS) のサプライチェーンは、米国の国家安全保障に不可欠で、企業や政府は広範にICTSに依存している
- 外国の敵対者によるICTSの悪用は、国家安全保障に深刻な損害をもたらす可能性がある
  - これには、脆弱性の悪用によるデータ漏洩やサービスの停止などが含まれる

- 外国の敵対者がICTSを提供する際に潜在的な脆弱性を悪用することで、データの盗難やサービスの妨害が懸念されている
- これにより、個人の情報や機密データが流出する可能性やサービスの一時的または完全な中断も考えられる

- 2020年7月、中国国家安全省と協力する中国人ハッカー2名が、新型コロナウイルス感染症ワクチン研究を含む米国の知的財産と企業機密情報を標的とした世界的なコンピュータ侵入キャンペーンを実施した罪で米国司法省によって起訴された
- ドイツ当局は、連邦保安局と関係のあるロシアのハッキンググループが、ICTSサプライチェーンを悪用してドイツのエネルギー、水道、電力会社のネットワークを侵害したと発表した
- 日本の防衛省は、新しい最先端のミサイル設計の詳細が侵害された可能性のある三菱電機に対する大規模なサイバー攻撃を調査していると発表した

- 結果、大統領は、外国の敵対者が所有、管理する、あるいはその管轄や指示を受ける者によって設計、開発、製造、供給されたICTS の無制限の取得または使用は、国家安全保障に対して、異常かつ極端な脅威であると判断した
- 2019 年5月15日の大統領令第13873号「情報通信技術およびサービスのサプライチェーンの確保」は、米国憲法および法律に基づく大統領の権限に従って発出された

Source: Federal Register : Securing the Information and Communications Technology and Services Supply Chain

「ICTS規則」詳細 [2/10]：措置の内容/対象行為

商務省は、「外国敵対者」が関与するリスクある取引を審査し、中止等の命令をすることが可能

妨害防止措置の概要	商務省 (the Department of Commerce) に対し、「取引」(Transaction) に「外国敵対者」(Foreign Adversaries) が関連し、米国に過度又は許容できないリスクをもたらす場合、これを**審査**し、**取引中止又はリスクの軽減措置を取らせる権限**を与えるもの
規制対象行為	以下の条件に合致するICTS取引[1] • 米国の司法権の対象となる財産、または対象となる個人もしくは団体によって行われる活動に関わるもの • 外国または外国人が何かしらの利害関係を持つ資産に関わるもの • 2021年1月19日以降に開始、保留、完了したもの • 6つのカテゴリーに分類される技術に関するもの (後述の「審査対象分野」参照) 但し、以下は対象外 • 米国政府の産業安全保障プログラムの一環としての米国人によるICTSの買収 • 対米外国投資委員会 (CFIUS) が審査中または審査済みの取引

1. 情報通信技術又はサービスの取得・輸入・移転・設置・取引又は使用、と定義されている (マネージドサービス、データ送信、ソフトウェアアップデート等も含む)
Source: Congressional Research Service "The Information and Communications Technology and Services (ICTS) Rule and Review Process"

「ICTS規則」詳細 [3/10]：外国敵対者の定義

「外国敵対者」として、中国、ロシア等、6つの主体が指定されている

「外国敵対者」(Foreign Adversaries)の定義

- 米国の安全保障や米国人の安全にとって、著しく敵対的な行為の長期的なパターンや深刻な事例に関与している外国政府や外国人と定義
- 同規則において、米国商務省は、下記を外国敵対者としてリストアップ

中国
(香港を含む)

キューバ

イラン

北朝鮮

ロシア

ベネズエラ
(ニコラス・マドゥロ政権体制)

- 米国商務省は今後定期的に外国敵対者リストを見直す予定

Source: Congressional Research Service "The Information and Communications Technology and Services (ICTS) Rule and Review Process"

(参考) 政府による外国敵対者の決定

「外国敵対者」の決定	(「外国敵対者」の定義) 香港を含む中国、キューバ、イラン、北朝鮮、ロシア、およびベネズエラの政治家ニコラス・マドゥロ（マドゥロ体制）の6つの主体を指定 • 当初は「外国の敵対者」を特定しない方針を示していたものの、提出された意見によりリスク評価や貿易促進のために特定すべきとの要請があり再考 (特定理由) 特定理由としては、これらの国が米国の国家安全保障、あるいは米国人の安全保障や安全にとって著しく不利な行為を長期にわたって行っている、あるいは深刻な事例があることを挙げている • 上記判断は、**米国情報コミュニティ、米国司法省、国務省、国土安全保障省、その他の関連情報源からのリスク評価や報告書**など、複数の情報源に基づいて行われる • 長官は関係省庁の長と協議の上、このリストを定期的に見直し、追加、削除、補足、その他の修正を行うことができる

Source: Federal Register : Securing the Information and Communications Technology and Services Supply Chain

「ICTS規則」詳細 [4/10]：審査対象分野

対象業種として、インフラ事業者や情報通信関連業種が幅広く指定されている

審査対象分野 (全体像)

6カテゴリーにわたり、インフラ事業者や情報通信関連事業者が幅広く指定されている

1

大統領政策指令
第21号で指定された重要インフラ
Critical infrastructure

2

情報通信インフラ・衛星
Network infrastructure
and satellites

3

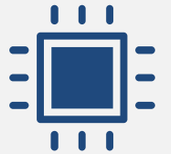
機微な個人情報処理
Sensitive personal
data processing

4

監視、住宅管理、ドローン
Monitoring, home networking,
and drones

5

情報通信ソフトウェア
Communication software

6

最新技術
Emerging technology

Source: Federal Register：Securing the Information and Communications Technology and Services Supply Chain

「ICTS規則」詳細 [5/10]：審査対象分野 詳細 [1/2]

対象業種として、インフラ事業者や情報通信関連業種が幅広く指定されている

審査対象分野 (詳細)

① 大統領政策指令第21号で指定された重要インフラ: Critical infrastructure

- 化学
- 商業用施設
- 情報通信
- 重要製造業 (自動車、金属 等)
- ダム
- 防衛産業基盤
- 緊急サービス
- エネルギー
- 金融
- 食品・農業
- 政府施設
- ヘルスケア・公衆衛生
- 情報技術
- 原子力燃料・処分
- 交通システム
- 上下水道システム

② 情報通信インフラ・衛星: Network infrastructure and satellites

下記に関連するハードウェアまたはその他の製品・サービス

- 無線ローカル地域ネットワーク
- モバイル・ネットワーク
- 人工衛星搭載物
- 人工衛星運用・制御
- ケーブル・アクセスポイント
- 無線アクセスポイント
- 有線アクセスポイント
- コア通信システム
- 光ファイバーを含む遠距離・短距離ネットワーク

Source: Federal Register：Securing the Information and Communications Technology and Services Supply Chain

(参考)「重要インフラ」に係る審査対象分野の具体的な内容 [1/5]

審査対象分野
(詳細)

大統領政策指令第21号に基づき、各連邦省庁の長官が重要インフラの特定に責任を有している

化学
- 基礎化学品
- 特殊化学品
- 農業化学品
- 消費者製品

商業用施設
- エンターテイメントおよびメディア (映画スタジオ、放送メディアなど)
- ゲーム (カジノなど)
- 宿泊施設 (ホテル、モーテル、カンファレンス センター、RV パーク、キャンプ場など)
- 屋外イベント (テーマパーク、遊園地、見本市、パレード、展示会、公園、マラソンなど)
- 公共の集会場 (アリーナ、スタジアム、水族館、動物園、博物館、コンベンションセンターなど)
- 不動産 (オフィスビル、アパートビル、マンション、複合施設、セルフストレージ)
- 小売 (小売センターおよび小売地区、ショッピング モールなど)
- スポーツリーグ (プロスポーツリーグや連盟など)

通信情報
- 放送
- ケーブル
- 衛星
- 無線ネットワーク
- 有線ネットワーク

Source:CISA "Critical Infrastructure Sectors", CISA, "Chemical Sector", CISA, "Commercial Facilities Sector", CISA, "2015 Communications Sector-Specific Plan"

(参考)「重要インフラ」に係る審査対象分野の具体的な内容 [2/5]

審査対象分野
(詳細)

[続き]

大統領政策指令第21号に基づき、各連邦省庁の長官が重要インフラの特定に責任を有している (続き)

重要製造業
- 一次金属製造(製鉄所および合金鉄製造業、アルミナ・アルミニウム製造・加工、非鉄金属製造・加工)
- 機械製造(エンジン・タービン製造、動力伝達装置製造、土木/鉱山/農業/建設機械製造業)
- 電気機器/家電製品/部品製造業(電気モーター製造、変圧器製造、発電機製造)
- 輸送機器製造(自動車および商船製造、航空宇宙製品・部品製造、機関車、鉄道車両、軌道設備製造業)

ダム
- 水力発電 / 都市・工業用水供給 / 農業灌漑 / 土砂・洪水調節 / 内陸大量輸送のための河川航行 / 産業廃棄物管理 / レクリエーション 等を提供

防衛産業基盤
- 研究開発
- 軍事兵器システム/サブシステム/部品/コンポーネントの設計/生産/納入/保守

緊急サービス
- 法執行機関
- 消防および救助サービス
- 救急医療サービス
- 緊急管理
- 公共事業

Source:CISA "Critical Infrastructure Sectors", CISA, "Critical Manufacturing Sector", CISA, "Dams Sector", CISA, "Defense Industrial Base Sector", CISA, "Emergency Services Sector"

(参考)「重要インフラ」に係る審査対象分野の具体的な内容 [3/5]

審査対象分野
(詳細)

[続き]

大統領政策指令第21号に基づき、各連邦省庁の長官が重要インフラの特定に責任を有している (続き)

エネルギー
- 電力(石炭、原子力発電所、天然ガス、水力発電、石油、再生可能エネルギー)
- 石油
- 天然ガス

金融
- 預金取扱機関
- 投資商品の提供者
- 保険会社
- その他の信用・融資機関
- 上記を支える重要な金融ユーティリティやサービスの提供者

食品・農業
- 農場
- レストラン
- 登録食品製造・加工・貯蔵施設

政府施設
- 一般的なオフィスビル
- 特殊用途の軍事施設
- 大使館
- 裁判所
- 国立研究所
- 重要な機器/システム/ネットワーク/機能を収容する可能性のある建造物
- 部門資産の保護に貢献するサイバー要素
- 重要な機能を実行したり、戦術的/作戦的/戦略的知識を有する個人

Source:CISA "Critical Infrastructure Sectors", CISA, "Energy Sector", CISA, "Financial Services Sector", CISA, "Food and Agriculture Sector", CISA, "Government Facilities Sector"

(参考)「重要インフラ」に係る審査対象分野の具体的な内容 [4/5]

審査対象分野
(詳細)

[続き]

大統領政策指令第21号に基づき、各連邦省庁の長官が重要インフラの特定に責任を有している (続き)

ヘルスケア・公衆衛生
- 公にアクセス可能な医療施設
- 研究施設
- 供給/製造業者
- その他の物理的資産/官民情報技術システム (健康増進活動拠点病院関連のデータを扱うもの)

情報技術
- インターネットを含むネットワークの維持と再構築を行う事業体

原子力燃料・処分
- 能動型動力炉
- 研究・試験用原子炉
- 活動中の核燃料サイクル施設

Source:CISA "Critical Infrastructure Sectors", CISA, "Healthcare and Public Health Sector-Specific Plan 2015", CISA, "Information Technology Sector", CISA, "Nuclear Reactors, Materials, and Waste Sector"

(参考)「重要インフラ」に係る審査対象分野の具体的な内容 [5/5]

審査対象分野
(詳細)

[続き]

大統領政策指令第21号に基づき、各連邦省庁の長官が重要インフラの特定に責任を有している (続き)

交通・運輸システム

- 航空 (航空機、航空交通管制システム、空港、ヘリポート、滑走路　等)
- 道路・車両 (道路、橋、トンネル、トラック、商用車両、車両、交通管理システム　等)
- 海上輸送システム (海岸線、港、水路、陸地間の複合輸送手段　等)
- 大量交通機関および旅客鉄道 (交通バス、トロリーバス、モノレール、地下鉄、ライトレール、旅客鉄道、バンプール/ライドシェアによる旅客サービスのためのターミナル、運用システム、サポート施設　等)
- パイプラインシステム
- 貨物鉄道 (航空、鉄道、貨車、機関車)
- 郵便・配送 (総合運送業者、地方および地域の宅配サービス、郵便サービス、郵便管理会社、チャーター便および配達サービス等)

上下水道システム

- 公共飲料水システム
- 公営廃水処理システム

Source:CISA "Critical Infrastructure Sectors", CISA, "Water and Wastewater Systems", CISA, "Transportation Systems Sector"

「ICTS規則」詳細 [6/10]：審査対象分野 詳細 [2/2]

対象業種として、インフラ事業者や情報通信関連業種が幅広く指定されている

審査対象分野 (詳細) [続き]

3 機微な個人情報処理: Sensitive personal data processing	提案されたICTS取引に先立つ時期に、12ヶ月以上にわたり、100万人を超える米国人の機微な個人情報を扱うデータホスト・コンピューティングサービスに関するソフトウェア、ハードウェアまたはその他いかなる製品・サービス
4 監視、住宅管理、ドローン: Monitoring, home networking, and drones	提案されたICTS取引に先立つ時期に、12ヶ月以上にわたり、米国人に100万を超える単位で販売されたネット通信可能なセンサー、ウェブカメラ、ルーター、ドローン等製品
5 情報通信ソフトウェア: Communication software	提案された ICTS 取引に先立つ時期に、12ヶ月以上にわたり 、100万人を超える米国人に利用されているインターネット通信用ソフトウェア • デスクトップアプリケーション • モバイルアプリケーション • ゲーミングアプリケーション • ウェブベースアプリケーション • 接続されたソフトウェアアプリケーション [2023年改正にて追加]
6 最新技術: Emerging technology	人工知能、機械学習、量子キーディストリビューション、量子コンピューティング、ドローン、自動運転システム、先端ロボットに関するICTS

Source: Federal Register : Securing the Information and Communications Technology and Services Supply Chain, Federal Register :: Securing the Information and Communications Technology and Services Supply Chain; Connected Software Applications

(参考) ICTS規則における機密な個人情報

機密な個人情報

(定義)
以下を含むものとして定義

- 個人を特定できる情報であって、12カ月間に100万人以上、特定の地域で事業を営む米国企業によって保持または収集されるもの
  - 個人の経済的困窮や苦境を示すために使用される可能性のある財務データ
  - 消費者報告書に含まれる一連のデータ
  - 健康保険や特定の金融保険の申請に使用される一連のデータ
  - 個人の身体的、精神的、または心理的な健康状態に関連するデータ
  - 個人の電子メールなどの非公開の電子通信情報
  - 特定の技術で使用される地理位置情報データ
  - バイオメトリクスデータ
  - 連邦、州、部族、準州、またはその他の政府の身分証明書を生成するために保存および処理されるデータ
  - 米国政府職員のセキュリティクリアランスの状態に関するデータ
  - セキュリティクリアランスまたは雇用申請からのデータ
- 個人の遺伝子検査の結果

Source: Federal Register : Securing the Information and Communications Technology and Services Supply Chain

「ICTS規則」詳細 [7/10]： 審査プロセス [1/2]

商務省の審査は大きく4段階からなり、情報の受領/他機関からの依頼/商務省の裁量で、審査を開始

審査プロセス [1/2]

照会/受理判断 (Referral) → 初回審査 (Initial review) → 初期判断 (Initial determination) → 最終判断 (Final determination)

商務省は下記の場合に照会準備を開始

- 商務省が、審査が必要であることを示す特定の情報を受領した場合
- 関連する連邦機関の長が要請した場合
- 商務省長官の裁量による場合

商務省は取引が、「外国敵対者」(Foreign Adversary) や技術要件を満たすかを判定し、以下を判断

- 照会を受理する
- 当事者にさらなる情報を求める
- 照会を拒否する

照会を受理した場合、商務省は初回審査を実施。その取引が不当な、あるいは容認できないリスクをもたらし得ると判断した場合、省庁間協議を実施

審査基準 (例) **[詳細後述]**

- 問題となっている技術やサービスの種類
- 脅威の性質
- 潜在的な被害の重大性

Source: Federal Register : Securing the Information and Communications Technology and Services Supply Chain, Federal Register :: Securing the Information and Communications Technology and Services Supply Chain; Connected Software Applications

(参考) 初回審査における審査基準

審査は、「技術/サービス」、「関係者」、「取引のリスク」に着目して実施されるとされている

審査基準[1]

対象となる技術・サービスの性質・特徴

- 当該ICTS取引 (以下、当該取引) において問題となる**情報通信技術又はサービスの性質及び特徴** (技術的能力、応用及び市場シェアに関する考慮事項を含む)

関係者の所有等の態様/供述・行動

- 当該取引において問題とされている**設計、開発、製造又は供給に対する外国敵対者による所有、支配、指示又は管轄の性質及び特徴**
- 当該取引において問題とされている**外国敵対者の供述及び行動**
- 当該取引において問題となった**設計、開発、製造又は供給に関与した者の供述及び行動**
- 当該取引の**当事者の供述及び行動**

リスク・脆弱性

- 当該取引が**個別的又は永続的な脅威をもたらす可能性**
- 当該取引が内包する**脆弱性の性質**
- 当該取引によりもたらされる**リスクを他の方法で軽減する能力の有無**
- 当該取引によってもたらされる危害のうち、少なくとも以下の1つについての**重大性**
  - 健康、安全及びセキュリティ/重要インフラ/機密データ/経済/外交政策/自然環境
  - 国家重要機能 (連邦継続指令-2 (FCD-2) により定義されているもの[2])
- 当該取引が実際に**脅威的損害をもたらす可能性**

1. 2023年改正で追加されたソフトウェアアプリケーションについては、別途、審査基準が設定されている (外国敵対者による所有・支配・管理、アプリケーションの監視の実施における使用等)
2. 政府形態の維持、米国の国際的信頼/信用、国民保護、外交、国土防衛、国土の復旧、米国経済の保護・安定化、国民の健康・安全・福祉

Source: Federal Emergency Management "AgencyFederal Continuity Directive 2: Federal Executive Branch Mission Essential Functions and Candidate Primary Mission Essential Functions Identification and Submission Process" Federal Register : Securing the Information and Communications Technology and Services Supply Chain; Connected Software Applications

「ICTS規則」詳細 [8/10]： 審査プロセス [2/2]

省庁間協議等のプロセスを経て、許可/禁止/リスク軽減措置等を決定

審査プロセス [2/2]

照会/受理判断 (Referral) → 初回審査 (Initial review) → 初期判断 (Initial determination) → 最終判断 (Final determination)

初期判断 (Initial determination)

最初の省庁間協議後、下記のいずれかについて、初期判断を実施

- 取引を許可する
- 禁止する
- リスク軽減措置を提案する

取引を全面的に許可しない限り、商務省は取引の当事者に決定書を提出、
当事者は30日以内に回答し、改善策を提案

- 当事者が回答した場合、商務省は2回目の省庁間協議を行わなければならない
- 当事者が回答しない場合、商務省は2回目の協議を経ずに最終決定を下すことが可能

最終判断 (Final determination)

初期判断の後、当事者に対し、商務省は最終的な決定書を発行

- 取引を許可する
- 全面的に禁止する
- リスク軽減措置の合意を条件として許可する

商務省は、さらに時間が必要であると書面で決定しない限り、**180日以内に全プロセスを完了**しなければならない

当事者が最終判断に違反した場合、行政罰 (Civil penalty)・刑事罰が科される可能性あり

Source: Federal Register : Securing the Information and Communications Technology and Services Supply Chain

「ICTS規則」詳細 [9/10]： 事前許可申請

事前の許可申請を求める手続きも議論されていたが、現時点では未整備

IFRのパブリックコメント時 (2021年3月) は、2021年5月19日までに、事前許可申請取引を公表する旨、記載あり

[米国Federal Register :2021年3月]
On January 19, 2021, the Department of Commerce (the Department) published a interim final rulemaking, "Securing the Information and Communications Technology and Services Supply Chain," which became effective on March 22, 2021. It allows the Secretary of Commerce, in accordance with Executive Order 13873, to prohibit certain information and communications technology and services transactions (ICTS Transactions) to address national security threats. In the January 19 notice, the Department stated it would implement a licensing process by May 19th for entities seeking pre-approval before engaging in or continuing to engage in ICTS Transactions. The Department is now seeking public input on such a licensing or other pre-clearance process.

仮訳
2021年1月19日、商務省は暫定最終規則案「情報通信技術・サービスのサプライチェーンの安全確保」を公表し、2021年3月22日に発効した。これは、商務長官が大統領令13873号に従い、国家安全保障上の脅威に対処するため、特定の情報通信技術・サービス取引(ICTS取引)を禁止することを認めるものである。**同省は1月19日の通知の中で、ICTS取引に従事する前、または継続的に従事する前に事前承認を求める事業体に対し、5月19日までにライセンス・プロセスを実施する**と述べている。同省は現在、このようなライセンスまたはその他の事前承認プロセスについて、一般からの意見を求めている。

事前審査に関する細則は未整備

Source: Federal Register : Securing the Information and Communications Technology and Services Supply Chain: Licensing Procedures

「ICTS規則」詳細 [10/10]： 届出書/罰則

商務省が得た情報/裁量により審査を開始するスキームであるため、届出書等は未整備

届出書/フォーマット	(特段存在せず) • 企業がICTS取引について、事前の許可を申請する仕組みは未整備
罰則	最終的な決定、指示、または緩和協定に違反した者は、IEEPA (国際緊急経済権限法) に基づく行政罰または刑事罰について米国連邦政府に対して責任を負う可能性がある • 行政罰: 罰金 最高額25万ドル 等 • 刑事罰: 罰金 最高額100万ドル 等

Source: Federal Register : Securing the Information and Communications Technology and Services Supply Chain

(参考) 政府による審査に関する規定内容

過度または容認できないリスクの考慮要素	ICTS取引が過度なリスクまたは容認できないリスクをもたらすかどうかを判断する際、長官と適切な省庁の長は以下のような要素を考慮する • (1) 大統領令 第 5 項 (a) に従って国家情報長官が作成した脅威評価および報告書 • (2) 米国連邦法典第 41 編第 1323 条に基づき、連邦調達安全評議会の勧告に従って、国土安全保障長官、国防長官、又は国家情報長官 (又はその被指名人) が発した排除命令又は除外命令 • (3) 国防連邦調達規則および連邦調達規則の関連規定、ならびにそれぞれの補足規定 • (4) 国土安全保障省サイバーセキュリティ・インフラ安全保障局「情報通信技術サプライチェーン・リスク管理タスクフォース」の報告、大統領令第5条(b)に従い、国土安全保障長官が決定した、米国における脆弱性を提示する事業体、ハードウェア、ソフトウェア、およびサービス • (5) 国土安全保障省サイバーセキュリティ・インフラ安全保障局によって特定された「国家重要機能」の実行に対する実際および潜在的脅威 • (6) ICTSの脆弱性が悪用された場合に発生し得る米国の公共部門および民間部門に対する結果の性質、程度、可能性 • (7) 長官が適切とみなすその他の情報源または情報
審査プロセス	ICTS 取引の**最初の審査を開始してから 180 日以内に最終決定を下す**ものと規定 • 追加の期間が必要であると書面で決定すれば延長可能

Source: Federal Register : Securing the Information and Communications Technology and Services Supply Chain

3-1.米国

1. 政策の全体像

2. 制度の調査結果
   - ICTS規則 (1)
   - その他のインフラ防護等に関する法令 等

3. 事例

米国のその他のインフラ防護等に関する法令 等

ICTS規則以外にも、様々な制度により、米国はインフラ防護等を図っている

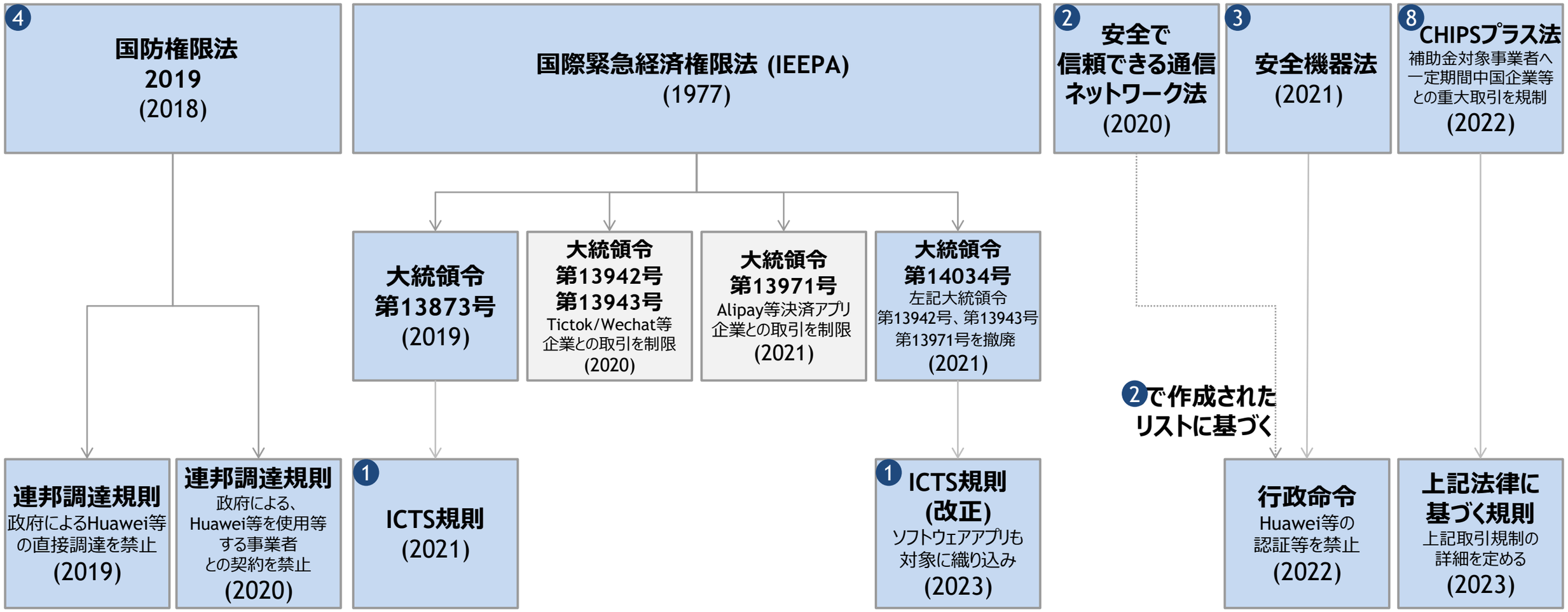
	法令名	制定年	法令の概要
2	安全で信頼できる通信ネットワーク法	2020年	• FCC[1]が、安全保障上のリスクをもたらす企業の製品/サービスを公表し、政府補助金の利用による通信機器企業 (中国Huawei、ZTE、ハイテラ、ハイクビジョン、ダーファ、チャイナモバイル、チャイナテレコム、露カスペルスキー) との取引を禁止
3	安全機器法/同法に基づく行政命令	2021年	• 安全機器法とそれに基づく行政命令により、米国の安全保障上、容認できないリスクがある企業の通信機器・サービスやビデオ監視システムについて、FCCによる米国内使用のための認証を禁止
4	国防権限法2019 (NDAA2019)	2018年	• Huawei、ZTE、ハイテラ、ハイクビジョン、ダーファの中国情報通信技術関連5社について、米国政府による当該製品・サービスの調達を禁止
5	外国投資リスク審査現代化法 (FIRRMA)	2018年	• NDAA2019を受け、安全保障上懸念のある外国人による (非) 支配的投資や、空港・港湾/米軍施設に近接する土地等の取得を審査 • 外国の敵対者による脅威を防ぐために、CFIUS[2]の権限が強化され、外国投資家は、特定の産業分野の取引については、事前にCFIUSに届け出を行う法的義務が課せられた
6	サイバーセキュリティー・パフォーマンス・ゴールズ (CPGs)	2022年	• インフラ事業者が取るべきサイバーセキュリティ対策について、達成すべき成果/対処すべきリスク、事業者が対策の成熟度を測定・改善するための基準を提示
7	サイバーセキュリティに関する大統領令14028	2021年	• 連邦政府の各機関にサイバーセキュリティ上、遵守する必要がある基準等を定めるもの • 政府機関に提供されるソフトウエアに関して、サプライチェーン上の安全性を向上する目的で、事業者が順守すべきガイドラインを策定
8	CHIPSプラス法	2022年	• 補助金の対象事業者は、受給日から10年間は中国他懸念ある国で、半導体製造施設の拡張を伴う重大取引に従事しないとの合意を商務長官と結ぶことを義務付け

1. Federal Communications Commission, 連邦通信委員会　2. The Committee on Foreign Investments in the United States, 対米外国投資委員会

(参考) 各制度の関係性 (上位法令/下位法令等の関連があるものを抜粋)

政府調達関係

民間事業者関係



Note：括弧内は施行年
Source：GovInfo "Public Law 95-223 95th Congress An Act"

米国のその他のインフラ防護等に関する法令 等　詳細 [1/3]

ICTS規則以外にも、様々な制度により、米国はインフラ防護を図っている

		② 安全で信頼できる通信ネットワーク法	③ 安全機器法
正式名称		Secure and Trusted Communications Networks Act of 2019	Secure Equipment Act of 2021
時期	施行日	2020年3月12日	2021年11月11日
概要		FCC[1]が、安全保障上のリスクをもたらす企業の**機器/サービス**を公表し、政府補助金の利用を禁止 • 当該法令に基づき安全保障上のリスクをもたらす可能性のある「対象機器・サービス」のリスト公表 - 24年1月時点、中国Huawei、ZTE、ハイテラ、ハイクビジョン、ダーファ、チャイナモバイル、チャイナテレコム等の中国企業や、露カスペルスキーが記載されている - リストは後述 • 「対象機器・サービス」に指定された場合、補助金を使ってそれら機器・サービスを購入、リース、維持することなどが禁じられる	米国の**安全保障上容認できないリスクがあるとされた対象機器**に対し、米国内での使用のための認証を全面的に禁止 • FCCに対し、対象となる通信機器・サービスのリストに掲載されている機器について、今後いかなる認可申請も審査・承認しないという規則を定めることを要求 - リストは、安全で信頼できる通信ネットワーク法に基づき公表される - 2022年11月に当該規則を実行するための行政命令が公表され、リストに掲載された**対象機器**への認証が禁止された

1. Federal Communication Commission

Source:H.R.4998 - 116th Congress (2019-2020): Secure and Trusted Communications Networks Act of 2019 | Congress.gov | Library of Congress, H.R.3919 - 117th Congress (2021-2022): Secure Equipment Act of 2021 | Congress.gov | Library of Congress、FCC "FCC Bans Authorizations for Devices That Pose National Security Threat"

(参考)「安全で信頼できる通信ネットワーク法」に基づく機器・サービスのリスト

Huawei等の中国企業の製品については、トランプ政権時代に政府調達等が禁止されたのに加え、バイデン政権において、
米連邦通信委員会 (FCC) の安全機器法に基づく行政命令により、使用に必要な認証がなされないこととなり、事実上使用が禁止された

リスト掲載の対象機器を判断する際の情報源

「安全で信頼できる通信ネットワーク法」第3条(c)にて記載された
以下4つを情報源とする

- (1) 合衆国法典第41編第1322条(a)に基づき設立された連邦調達安全評議会を含む、適切な国家安全保障の専門知識を有する行政府の省庁間機関による具体的な決定
- (2) 大統領令第13873 号に従って商務省が下した特定の決定
- (3) 2019年NDAA第889条(f)(3)に定義される、対象となる電気通信機器またはサービスである通信機器またはサービス
- (4) 適切な国家安全保障機関が行った具体的な決定

これらの機器については、安全機器法に基づく2022年11月の行政命令において、FCCによる認証がなされないこととなった

リストの内容 (2024年1月31日確認)

対象となる機器またはサービス	登録日
Huaweiが製造した電気通信機器	2021/3/12
ZTEが製造する電気通信機器	2021/3/12
国家安全保障目的のために使用される範囲でハイテラが製造するビデオ監視および電気通信機器	2021/3/12
国家安全保障目的のために使用される範囲でハイクビジョンが製造するビデオ監視および電気通信機器	2021/3/12
国家安全保障の目的で使用される限りにおいてダーファが製造するビデオ監視および電気通信機器	2021/3/12
カスペルスキーまたはその関連会社が直接的または間接的に提供する情報セキュリティ、ソリューション、サービス	2022/3/25
中国移動（チャイナモバイル）インターナショナルUSAが提供する国際電気通信サービス	2022/3/25
中国電信（チャイナテレコム）アメリカスが提供する電気通信サービス	2022/3/25
Pacific Networks Corpおよびその完全子会社のComNet (USA) LLCが提供する国際電気通信サービス	2022/9/20
China Unicom (Americas) Operations Limitedが提供する国際電気通信サービス	2022/9/20

Source: H.R.4998 - 116th Congress (2019-2020): Secure and Trusted Communications Networks Act of 2019 | Congress.gov | Library of Congress, FCC "List of Equipment and Services Covered By Section 2 of The Secure Networks Act"、FCC "FCC Bans Authorizations for Devices That Pose National Security Threat"

米国のその他のインフラ防護等に関する法令 等 詳細 [2/3]

ICTS規則以外にも、様々な制度により、米国はインフラ防護を図っている

		④ 国防権限法2019	⑤ 外国投資リスク審査現代化法2018
正式名称		National Defense Authorization Act for Fiscal Year 2019	Foreign Investment Risk Review Modernization Act 2018
時期	施行日	2018年8月13日	2018年8月13日 (NDAA2019に盛り込まれる形で成立) • 段階的に施行され、2020年2月13日に主要規定が施行
概要		規制対象機器について、米国政府による調達を禁止 • 米国政府機関に対し、(A)規制対象機器の直接調達と、(B) 規制対象機器を使用した企業との契約を禁止 – 当該法令に基づき規則が発出されており、Huawei・ZTEの電子通信機器、ハイテラ・ハイクビジョン・ダーファの監視ビデオおよび電気通信機器のうち、国家安全保障に関連する取引に規制が課せられている (詳細次頁) • 加えて、「外国投資リスク審査現代化法」及び「輸出管理改革法」も一部として制定	安全保障上懸念のある外国人による (非) 支配的投資や、空港・港湾/米軍施設に近接する土地等の取得を審査 (詳細後述) • 審査に当たっては具体的な基準も規定 • 規制例外国規定も規定 外国の敵対者による脅威を防ぐために、対米外国投資委員会 (CFIUS[1]) の権限が強化され、外国投資家は、特定の産業分野の取引については、事前にCFIUSに届け出を行う法的義務が課せられた • 従来は、投資者によるCFIUSへの任意の通知制度があるのみで義務ではなかったなかったものの、新たに外国政府関連投資家による投資や重要技術ビジネスへの投資のうち一定のものにつき事前の申告義務を規定

1. The Committee on Foreign Investments in the United States

Source:H.R.5515 - 115th Congress (2017-2018): John S. McCain National Defense Authorization Act for Fiscal Year 2019 | Congress.gov | Library of Congress, H.R.5841 - 115th Congress (2017-2018): Foreign Investment Risk Review Modernization Act of 2018 | Congress.gov | Library of Congress, H.R.5515-538, TITLE XVII-REVIEW OF FOREIGN INVESTMENT AND EXPORT CONTROLS, The Committee on Foreign Investment in the United States (CFIUS) | U.S. Department of the Treasury

(参考) Huawei製品等の政府調達に関する規制

Huawei等の中国製製品については、トランプ政権時代において、政府の直接の調達やそれらの製品を使用する企業からの調達が禁止されている

(A) 政府による直接調達の禁止

名称
- Federal Acquisition Regulation: Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment

時期
- 2019年8月13日施行

内容
- NDAA2019の第889条(a)(1)(A)に関する規則として公表
- 米政府機関が、規制対象機器等を使用している機器・サービスを**直接、調達・契約すること**を禁止する
- 規制対象機器として、以下の中国通信企業5社の通信・監視ビデオ関連の製品・サービスを指定
  - Huawei・ZTEの電子通信機器、ハイテラ・ハイクビジョン・ダーファの監視ビデオおよび電気通信機器のうち国家安全保障に関連するもの

(B) Huawei機器等使用企業からの政府調達の禁止

名称
- Federal Acquisition Regulation: Prohibition on Contracting With Entities Using Certain Telecommunications and Video Surveillance Services or Equipment

時期
- 2020年7月14日施行

内容
- NDAA2019の第889条(a)(1)(B)に関する規則として公表
- 米政府機関が、規制対象機器等を使用している機器・サービスを**使用する企業と契約をすることを禁止**する
- 規制対象機器として、以下の中国通信企業5社の通信・監視ビデオ関連の製品・サービスを指定
  - Huawei・ZTEの電子通信機器、ハイテラ・ハイクビジョン・ダーファの監視ビデオおよび電気通信機器のうち国家安全保障に関連するもの

1. Federal Communication Commission
Source: Federal Acquisition Regulation: Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment
FEDERAL REGISTER"Federal Acquisition Regulation: Prohibition on Contracting With Entities Using Certain Telecommunications and Video Surveillance Services or Equipment"

(参考) 外国投資リスク審査現代化法 (⑤) の詳細

「外国投資リスク審査現代化法」においては、安全保障上の考慮要素や、除外国/その判断要素が記載されている

国家安全保障の考慮要素 (和訳)

- (1) 米国の国家安全保障に関連する分野におけるリーダーシップに影響を及ぼす重要技術・重要インフラの取得を掲げている「特別懸念国」の関与の有無
- (2)重要インフラ、エネルギー、重要原料、重要技術の外国政府又は外国人による支配による安全保障への影響
- (3) 米国ビジネスに対する当該外国投資家の米国法規制遵守状況
- (4) 米国の安全保障の能力（人材、製品、技術、材料及びその他の供給品やサービスを含む）を脅かすような産業や商業活動の支配
- (5) 個人情報、遺伝子情報、その他の米国市民の機微なデータへのアクセス
- (6) サイバーセキュリティの脆弱性を新たに生じるような影響

CFIUS除外国

- オーストラリア（2020年2月13日）
- カナダ (2020 年2月13日)
- ニュージーランド (2022 年1月5日)
- グレートブリテン及び北アイルランド連合王国（2020年2月13日）

判断の要素 (和訳/一部要約)

(a) 当事者の企業形態にかかわらず、外国投資取引を審査する法的権限をどの程度保有しているか
(b) その国の防衛産業基盤、先端技術、デュアルユースおよび軍事物資、ネットワーク技術、重要インフラを含む、分野横断的な対外投資取引の審査メカニズムをどの程度整備し、効果的に活用しているか
(c) 自国の国家安全保障を保護するために、外国投資取引に条件を課したり、阻止したり、あるいは完了取引を解消する法的権限を有しているか、どの程度有効に活用しているか
(d) その国の取引や重要な権利者や国家安全保障上のリスク等に関する情報を入手する法的権限を有しているかどうか
(e) 当該外国の国家安全保障投資審査制度によって審査される取引の当事者から提供される機密商業情報の機密性をどの程度保持するか
(f) 外国投資取引の当事者による、当該取引に課した条件の遵守をどの程度監視し執行しているか
(g) 外国投資取引の当事者が外国政府当局に届け出ていない外国投資取引をどの程度監視し、特定するか
(h) その外国が、外国投資に関連する国家安全保障を保護するために、米国政府と実質的に取り決めを行っているかどうか
(i) 外国が、国家安全保障上必要な範囲において、適切な機密保持および分類要件に従い、外国投資の国家安全保障上の分析に重要な情報を米国政府と共有する法的権限を有しているかどうか
(j) 米国の国家安全保障上の利益を含め、一般的に、または特定の外国に関連して、国家安全保障上のリスクに対する外国投資の審査に関連する外国のプロセスに関して、委員会が適切とみなすか

Source: H.R.5841 - 115th Congress (2017-2018): Foreign Investment Risk Review Modernization Act of 2018 | Congress.gov | Library of Congress 、U.S. DEPARTMENT OF THE TREASURY"CFIUS Excepted Foreign States"、FACTORS FOR DETERMINATIONS UNDER § 800.1001(a) / § 802.1001(a)

米国のその他のインフラ防護等に関する法令 等 詳細 [3/3]

ICTS規則以外にも、様々な制度等により、米国はインフラ防護を図っている

	⑥ サイバーセキュリティー・パフォーマンス・ゴールズ	⑦ サイバーセキュリティに関する大統領令第14028号
正式名称	Cybersecurity Performance Goals (CPGs)	Executive Order 14028: Improving the Nation's Cybersecurity
時期 公表日	初版：2022年10月27日、Ver.1.0.1：2023年3月21日	2021年5月12日 (大統領令発出) 2022年9月14日 (上記に基づく覚書の発出)
概要	インフラ事業者が採るべきサイバーセキュリティ対策について、達成すべき成果/対処すべきリスク、事業者が対策の成熟度を測定・改善するための基準を提示 • サービスを確実に提供、サイバーセキュリティに関する事象発生を特定するための適切な保護措置を策定・実施 • 検出されたサイバーセキュリティに関する事象に関する措置を講じるための適切な活動を策定・実施 • 回復のための計画を維持し、サイバーセキュリティ事象によって損なわれた能力やサービスを回復するための適切な活動を策定・実施	サイバーセキュリティを向上させるため、各組織が遵守する必要がある基準等を定めるもの • 連邦政府と契約する情報通信サービス企業は、政府機関への情報共有等を行う必要あり 加えて、政府機関に提供されるソフトウェアに関して、サプライチェーン上の安全性を向上する目的で、事業者が順守すべきガイドラインを策定

Source: Cross-Sector Cybersecurity Performance Goals | CISA, Executive Order on Improving the Nation's Cybersecurity | The White House、 Enhancing the Security of the Software Supply Chain through Secure Software Development Practices、MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES"Enhancing the Security of the Software Supply Chain through Secure Software Development Practices"

(参考) CHIPSプラス法の詳細 (⑧)

CHIPSプラス法により、補助金等の要件として、中国関連事業者との取引の制限等の条件が課される

概要

名称
- CHIPS and Science Act of 2022

発出日

CHIPSプラス法：2022年8月9日成立

上記に基づく規則：
2023年9月25日公表、11月24日施行

内容
- 米国の半導体研究、開発、製造、労働力開発のために補助金や投資税額控除制度を用意
- 受給者には中国やその他の懸念国またはその関連事業者との取引の制限等の条件が課される

内容詳細 (本調査に関連する部分)

CHIPSプラス法に基づき商務省により出された規則において、CHIPSプラス法での補助金受給者に対して、中国・ロシア・イラン・北朝鮮など懸念国に関連する規制が課されている

- 受給者が外国に最先端・先端技術施設を新設・拡張することを阻止するため、**補助金等授与日から10年間、懸念される外国における最先端・先端技術施設の半導体製造能力の大幅な拡張を伴う重要な取引を禁止**
  - これらの制限に違反する取引を事業者が行った場合、**同省は提供資金の全額の返還を要求することが可能**
  - 大幅な拡張とは5%以上の拡張、重要な取引とは10万ドル以上の取引を指す
- 懸念される外国にある既存施設に、生産ラインの追加・施設の生産能力を10%以上拡張することを禁止
  - 生産物の85%以上が現地で消費される場合のみ可能
  - 上記制限の例外に該当する取引を行う場合も、商務省に報告することが必要

Source: FACT SHEET: CHIPS and Science Act Will Lower Costs, Create Jobs, Strengthen Supply Chains, and Counter China | The White House, Commerce Department Outlines Proposed National Security Guardrails for CHIPS for America Incentives Program | U.S. Department of Commerce、NIST" Frequently Asked Questions: Preventing the Improper Use of CHIPS Act Funding"、Federal Register：Preventing the Improper Use of CHIPS Act Funding

3-1.米国

1. 政策の全体像

2. 制度の調査結果
   - ICTS規則 (1)
   - その他のインフラ防護等に関する法令 等

3. 事例

ICTS関連の対応に関する政府のプレスリリース

ICTS規則の施行直前に、複数の中国企業に対して召喚状を送付した旨、政府がプレスリリースを行っている

概要

プレスリリース名
- U.S. Secretary of Commerce Gina Raimondo Statement on Actions Taken Under ICTS Supply Chain Executive Order

発出日
- 2021年3月17日

発出者
- 商務省

詳細

大統領令第13873号に基づく取引審査に必要な事項の確認のため、商務省が複数の中国企業に召喚状を送達

(和訳全文)

本日、**商務省は米国で情報通信技術およびサービス (ICTS) を提供する複数の中国企業に召喚状を送達**した。取引審査の必要事項の確認のため、商務省が複数の中国企業に召喚状を送達。

本日行われた措置は、これらの企業が関与する取引が大統領令に定められた基準を満たしているかどうかを調査する上で重要なステップとなる。

ジーナ・M・ライモンド米国商務長官は次の声明を発表した。

「バイデン・ハリス政権は、信頼できない ICTS の無制限の使用が国家安全保障上のリスクを引き起こすことを明確にしている。**中国政府は、我が国の技術的優位性を鈍らせ、同盟関係を脅かす行為を取っている。**

本日召喚状を発行することで、米国企業、米国労働者の安全、米国国家安全保障を最大限に守るために考えられる行動を決定するための情報収集における重要な一歩を踏み出している。私たちはこれらの企業と協力して徹底的な検討を行いたいと考えている。

信頼できる情報通信技術とサービスは国家と経済の安全保障に不可欠であり、バイデン・ハリス政権にとって引き続き最優先事項である。政府は、**信頼できない企業によるデータの流用や悪用を確実に防止し、米国の技術が中国やその他の主体による悪意のある活動を支援しないよう**に、政府全体のアプローチを取ることに断固として取り組んでいる。」

Source: U.S. Department of Commerce"U.S. Secretary of Commerce Gina Raimondo Statement on Actions Taken Under ICTS Supply Chain Executive Order"

(参考) 安全機器法/行政命令に基づき、認証が禁止されている機器等のリスト

Huawei等の中国企業の製品については、バイデン政権において、2022年11月に発出された米連邦通信委員会 (FCC) の安全機器法に基づく行政命令により、使用に必要な認証がなされないこととなり、事実上使用が禁止された

リストの内容 (2024年1月31日確認) [再掲]

対象となる機器またはサービス	登録日
Huaweiが製造した電気通信機器	2021/3/12
ZTEが製造する電気通信機器	2021/3/12
国家安全保障目的のために使用される範囲でハイテラが製造するビデオ監視および電気通信機器	2021/3/12
国家安全保障目的のために使用される範囲でハイクビジョンが製造するビデオ監視および電気通信機器	2021/3/12
国家安全保障の目的で使用される限りにおいてダーファが製造するビデオ監視および電気通信機器	2021/3/12
カスペルスキーまたはその関連会社が直接的または間接的に提供する情報セキュリティ、ソリューション、サービス	2022/3/25
中国移動（チャイナモバイル）インターナショナルUSAが提供する国際電気通信サービス	2022/3/25
中国電信（チャイナテレコム）アメリカスが提供する電気通信サービス	2022/3/25
Pacific Networks Corpおよびその完全子会社のComNet (USA) LLCが提供する国際電気通信サービス	2022/9/20
China Unicom (Americas) Operations Limitedが提供する国際電気通信サービス	2022/9/20

これらの機器については、安全機器法に基づく2022年11月の行政命令において、FCCによる認証がなされないこととなった

Source: H.R.4998 - 116th Congress (2019-2020): Secure and Trusted Communications Networks Act of 2019 | Congress.gov | Library of Congress, FCC "List of Equipment and Services Covered By Section 2 of The Secure Networks Act"、FCC "FCC Bans Authorizations for Devices That Pose National Security Threat"

(参考) 中国企業に対する規制概要 (いずれも撤回済)

トランプ政権時代は、大統領令に基づきTikTok、WeChat、Alipay等を始めとする決済アプリを取り扱う中国企業の取引が制限されていた (いずれも撤回)

	大統領令13942	大統領令13943	大統領令13971
名称	• Executive Order 13942	• Executive Order 13943	• Executive Order 13971
発出日	• 2020年8月6日		• 2021年1月5日
内容	• 国際緊急権限法等に基づき米国個人及び法人に対して **ByteDance社** (TikTokの運営会社) 並びに **その子会社との取引を制限**	• 国際緊急権限法等に基づき米国個人及び法人に対してTencent Holdings (WeChat提供会社の親会社) 並びにその子会社との **WeChatに関する取引**を制限 – WeChat以外の取引の制限はない	• 国際緊急権限法等に基づき米国個人及び法人に対してAlipay、CamScanner、QQ Wallet、SHAREit、Tencent QQ、VMate、WeChat Pay、WPS Officeの開発・運用会社及びその関係会社との取引を制限

いずれも2021年6月9日の大統領令第14034により撤回、追加対策が指示。
2023年3月にICTS規則の対象範囲にアプリが追加された

Source: Executive Order 13942、Executive Order 13943、Executive Order 13971、Executive Order 14034、White House "FACT SHEET: Executive Order Protecting Americans' Sensitive Data from Foreign Adversaries"、U.S Department of Commerce "Securing the Information and Communications Technology and Services Supply Chain; Connected Software Applications"

(参考) 大統領令第13942号 (撤回済) の詳細

大統領令第13942号に基づき、米国の個人及び法人に対してTikTokおよびその関連会社との取引を制限（現在は撤回）

概要

名称
- Executive Order 13942

発出日
- 2020年8月6日

内容
- トランプ政権が、国際緊急権限法等に基づき米国個人及び法人に対してByteDance社(TikTokの運営会社)並びにその子会社との取引を制限

詳細

中国への警戒、及び、TikTokを通じた中国政府への情報提供やTikTokの政治的悪用を理由に、取引を制限

- 中国の企業が開発・所有するモバイルアプリケーションの米国内での普及が、米国の国家安全保障、外交政策、経済を脅かし続けている
- TikTok は、インターネット等から膨大な情報 (位置データ、閲覧履歴、検索履歴など) をユーザーから自動的に取得しており、このデータ収集により、中国共産党が、米国人の個人情報や専有情報にアクセスできるようになる恐れがある
  - 中国が連邦職員や請負業者の位置を追跡したり、脅迫用の個人情報の文書を作成したり、企業スパイ活動を行ったりできるようになる可能性がある
- TikTokはまた、香港での抗議活動や中国によるウイグル人や他のイスラム教徒少数民族の扱いに関するコンテンツなど、中国共産党が政治的にデリケートだとみなしたコンテンツも検閲していると伝えられている
  - 2019 年の新型コロナウイルスの起源に関する誤りが暴かれた陰謀論を TikTok 動画で広める場合など、中国共産党に利益をもたらす偽情報キャンペーンにも使用される可能性がある

Source: Executive Order 13942、White House"Executive Order on Protecting Americans' Sensitive Data from Foreign Adversaries"

(参考) 大統領令第13943号 (撤回済) の詳細

大統領令第13943号に基づき、米国の個人及び法人に対してWeChatに関するTencentとの取引を制限（現在は撤回）

概要

名称
- Executive Order 13943

発出日
- 2020年8月6日

内容
- トランプ政権が、国際緊急権限法等に基づき米国個人及び法人に対してTencent Holdings (WeChat提供会社の親会社) 並びにその子会社との**WeChatに関する取引**を制限した
  - WeChat以外の取引の制限はない

詳細

中国への警戒、及び、WeChatを通じた中国政府への情報提供やWeChatの政治的悪用を理由に取引を制限

- 中国の企業が開発・所有するモバイルアプリケーションの米国内での普及が、米国の国家安全保障、外交政策、経済を脅かし続けている
- WeChatもTikTokと同様に、ユーザーから膨大な情報を自動的に収集しており、中国共産党が米国人の個人情報や専有情報にアクセスできるようになる恐れがある
  - 2019年3月に、ある研究者が、中国だけでなく米国、台湾、韓国、オーストラリアのユーザーから送信された数十億件の WeChat メッセージを含む中国のデータベースを発見したと報告されている
- WeChatもTikTokと同様に中国共産党が政治的にデリケートだとみなしたコンテンツも検閲していると伝えられており、中国共産党に利益をもたらす偽情報キャンペーンにも使用される可能性がある
- オーストラリアやインドを含む他の国は、WeChatの使用を制限または禁止し始めている

Source: Executive Order 13943、White House"Executive Order on Protecting Americans' Sensitive Data from Foreign Adversaries"

(参考) 大統領令第13971号 (撤回済) の詳細

大統領令第13971号に基づき米国の個人及び法人に対してAlipay等決済取引を扱う企業との取引を制限（現在は撤回）

概要

名称
- Executive Order 13971

発出日
- 2021年1月5日

内容
- 国際緊急権限法等に基づき米国個人及び法人に対してAlipay、CamScanner、QQ Wallet、SHAREit、Tencent QQ、VMate、WeChat Pay、WPS Officeの開発・運用会社及びその関係会社との取引を制限

詳細

中国への警戒、及び、アプリケーションを通じた中国政府への情報提供やAlipay等の政治的悪用を理由に取引を制限

- 中国共産党が個人のデータを盗んだり入手したりする活動は、大量のデータ収集を利用して中国の経済と国家安全保障の課題を拡大する意図がある
- 上記に基づき、米国政府では中国に接続されるソフトウェアの使用禁止を課しており、インド全土でも禁止されている
  - インド電子情報技術省は声明で、これらのアプリケーションは「インド国外にあるサーバーに不正な方法でユーザーのデータを盗み、密かに送信している」と主張
- 中国に接続されるアプリケーションでは、ユーザーから膨大な情報を自動的に収集しており、中国共産党が米国人の個人情報や専有情報にアクセスできるようになる恐れがある

Source: Executive Order 13971、White House"Executive Order on Protecting Americans' Sensitive Data from Foreign Adversaries"

3-2. 英国

1. 政策の全体像

2. 制度の調査結果
   - 電気通信 (セキュリティ) 法 (1)
   - その他のインフラ防護等に関する法令 等

3. 事例

3-2. 英国

1. 政策の全体像

2. 制度の調査結果
   - 電気通信 (セキュリティ) 法 (1)
   - その他のインフラ防護等に関する法令 等

3. 事例

英国の基幹インフラ妨害行為の防止に係る政策の全体像

主な対象行為		主な対象者			
		国内企業			外国企業
		基幹インフラ事業者		通信関連製品製造/輸入業 等	
		通信事業者	その他事業者		
取引規制	製品/役務の調達	① **電気通信 (セキュリティ) 法** • 通信事業者に対するセキュリティ義務の遵守 等 **主な制度 (詳細深掘り)**			
	対内直接投資				② **国家安全保障および投資法** • 特定の種類の事業体および資産に対する支配権の取得に対して、政府への通知を義務付ける
サイバー攻撃への防護		③ **2018年ネットワークおよび情報システム規制 (NIS規制)** • 経済・社会にとって重要なデジタル・インフラ事業者等の重要な基盤サービス提供事業者に対して、適切なセキュリティ対策の実施や重大インシデントに関する当局への報告を義務付け		④ [参考:消費者向けIoT製品等] **製品セキュリティ・通信インフラストラクチャ法 (PSTI法)** • 消費者向けIoT製品の製造/輸入等について、最低限のセキュリティ基準を要求	
		⑤ **サイバーアセスメントフレームワーク (CAF) ※ ガイダンス用フレームワーク** • 国家の重要なインフラ (Critical National Infrastructure)の事業者は、本評価基準に沿って、評価することが推奨 (なお、政府機関/独立行政法人は、本CAFに基づき、GovAssureという機関によるレビューが義務付けられた)			

Note：上記分類は、本調査の目的から、関連が深いと考えられる法令を抽出し、主な目的/対象の相違等を強調するために整理をしたものであり、必ずしも上記各範囲の内容のみを含むとは限らない
特に、国内企業には、国内にて事業活動を行う外国企業も含まれうる

Source: Telecommunications (Security) Act 2021 (legislation.gov.uk), 総務省「英国（United Kingdom of Great Britain and Northern Ireland）」, Product Security and Telecommunications Infrastructure Act 2022 (legislation.gov.uk), The Network and Information Systems Regulations 2018 (legislation.gov.uk), National Security and Investment Act 2021 - GOV.UK (www.gov.uk), NCSC CAF guidance - NCSC.GOV.UK

3-2. 英国

1. 政策の全体像

2. 制度の調査結果
   - 電気通信 (セキュリティ) 法 (1)
   - その他のインフラ防護等に関する法令 等

3. 事例

電気通信 (セキュリティ) 法の概要 [1/2]

法令等の名称

電気通信 (セキュリティ) 法
(Telecommunications (Security) Act 2021)

※ 通信法 (Communications Act 2003) を改正するもの

制定時期

- 2020年11月　議会提出
- 2021年11月　成立

制定の経緯

- 情報通信サプライチェーンに関する課題意識から、**サプライチェーンをレビュー、ハイリスクベンダーの管理の必要性を認識**
  - 情報通信関連事業者の業界の慣行では、セキュリティ対策が不十分と認識
  - 英国はHuaweiに大きく依存しており、米国におけるHuaweiのエンティティリスト追加により、更に問題が深刻化したと認識
- 政府として、**2027年末までにHuawei製品を排除する**、という計画を公表するとともに、ハイリスクベンダーに対して措置を行う権限や、事業者のセキュリティ義務強化を法制化

妨害防止措置等の概要

- **公衆電子通信網または公衆電子通信サービスの提供者に対してセキュリティ強化の義務**を課すとともに、**セキュリティ評価に必要な情報のOfcom (通信庁) への提供**を求める
- 国家安全保障上の懸念がある事業者に対し、**主務大臣が、その旨を指定した上で、提供者に対して、当該事業者の製品の使用等に関し、要件を設定することができる (違反した場合は罰金)**

対象者

公衆電子通信網または公衆電子通信サービスの提供者
(以下、「提供者」)

Source: Telecommunications (Security) Act 2021 (legislation.gov.uk), 総務省「英国（United Kingdom of Great Britain and Northern Ireland）」

電気通信 (セキュリティ) 法の概要 [2/2]

運用プロセス[1)]

指定事業者の指定通知

主務大臣は、**国家安全保障上必要であると判断**した場合に限り、**指定通知**を発することが可能

指示に関する業界等との協議

主務大臣は、指定事業者との取引制限等、指示を行う場合、指示により影響を受けることになる**提供者**や**指定事業者**と、合理的に可能な限り、**協議を実施**

提供者に対する指示

主務大臣は、**国家安全保障のために必要**であり、**指示の内容が達成しようとすることと比例している場合**に限り、**指示を出すこと**が可能

運用基準

事業者の指定等では、以下の項目を考慮

- 事業者が提供する商品、サービス又は施設の**性質**、それらの**品質**、**信頼性、安全性**、 他国での使用状況
- **開発者・製造者・提供者等の身元、国** 等

罰則

主務大臣は、事業者に対し、罰金を科すことが可能

- 通信事業者がセキュリティ義務を遵守していない場合
  - 関連する売上高の最大10% / 1日あたり10万ポンド

1) Huaweiが指定事業者として通知された際には、指定事業者の指定通知と提供者に対する指示が同時に実施された

Source: Telecommunications (Security) Act 2021 (legislation.gov.uk), 総務省「英国（United Kingdom of Great Britain and Northern Ireland）」、Huawei Designation Notice (publishing.service.gov.uk)

「電気通信 (セキュリティ) 法」詳細 [1/9]：名称/制定時期 等

電気通信 (セキュリティ) 法は、ハイリスクベンダーへの対策を含む、通信事業のセキュリティ強化のために制定

法令等の名称

- **The Telecommunications (Security) Act 2021**
  - 電気通信 (セキュリティ) 法 2021
  - 通信法 (Communications Act 2003) を改正するもの

制定時期

- 2020年11月　議会提出
- 2021年11月　成立

制定の経緯

- 2019年7月公表の「ⅰ **電気通信サプライチェーンレビュー**」において、より多様で競争力のある**電気通信ネットワークの供給基盤を構築する必要性が指摘**
  - 業界のセキュリティ慣行の不十分さ、サイバーセキュリティの改善を促進する規制の枠組みの無いこと、リスク管理のインセンティブが欠如していることに起因していることを確認
  - **ハイリスクベンダーに起因するリスクを管理・軽減し、**新たな強固なセキュリティフレームワークの導入の必要性を指摘
- 2020年7月公表の「ⅱ **NCSCによる助言**」を受け、**英国政府は、ハイリスクベンダーのリスクを管理・軽減するために、2027年末までにHuaweiを5Gネットワークから排除する方針**を発表
- 2020年11月、「ⅲ **5Gサプライチェーンの多様性戦略**」を公表 (**電気通信事業者への新たな強固なセキュリティの枠組みを導入**、**Ofcomのセキュリティ権限の強化**等を内容)。同月、**法案を議会に提出**。
- 2021年11月　**成立**

Source: UK Telecoms Supply Chain Review Report (publishing.service.gov.uk), 5G Supply Chain Diversification Strategy, Parallel Parliament, ukpgaen_20210031_en.pdf (legislation.gov.uk)、国立国会図書館ウェブサイト（【イギリス】[立法情報]2021年電気通信（セキュリティ）法の制定 (ndl.go.jp)）

(参考) 「電気通信サプライチェーンレビュー (2019) 」の概要 [1/2]

名称	• The Telecoms Supply Chain Review
作成主体	• Department for Digital, Culture, Media and Sport[1]
作成時期	• **2018年10月 検討開始** • **2019年7月　レポート公表**
目的	• 5G等の次世代ネットワーク普及により、セキュリティーリスクと経済的機会が更に増す状況を踏まえ、**電気通信ネットワークのセキュリティーを重要視** • これを背景に、**英国政府は、**電気通信重要インフラの供給体制を包括的に見直すため、**以下3つの議題を調査：** - **1) 5Gとフルファイバーネットワークにおけるセキュリティの標準と慣行を改善するために、通信事業者にどのようなインセンティブを与えるべきか** - **2) ベンダーがもたらすセキュリティ上の課題にどのように対処すべきか** - **3) 電気通信サプライチェーンにおける持続可能な多様性をどのように創出するか** • 本レビューの結果に基づき、政府が、**電気通信サプライチェーン**について、セキュリティ・サービス品質・経済的・戦略的要素を考慮し、**エビデンスに基づく政策枠組み**を確立することを目的 (直近2019年5月、米国においてHuaweiがEntity Listに追加されたことにも度々言及)

1. 現在は省庁再編により別組織に統合
Source: UK Telecoms Supply Chain Review Report (publishing.service.gov.uk)

(参考) 「電気通信サプライチェーンレビュー (2019) 」の概要 [2/2]

課題認識	• 5Gとフルファイバーネットワークの広範な展開は、英国の主要な政策目標 • また、これらのネットワークのセキュリティーは英国の経済的利益に繋がると認識 • 一方で、5G等次世代ネットワークについて、**以下の課題を認識**： - **5Gの技術特性により、潜在的な攻撃の可能性がより大きくなること** (高速通信 / コモディティのハードウェア) - **ネットワークの接続範囲拡大により、リスクも大きくなること** - **敵対的な脅威が増すこと** (英国政府は過去2年間以上、露・中・北朝鮮・イランよりサイバー攻撃を受けており、今後ネットワークの弱点に付け込まれる可能性)
検討対象	**電気通信に係る国家の重要なインフラ (CNI[1]) について懸念あり** • リスク管理のインセンティブ不足に起因し、産業界の対応が不十分であること • 少数のサプライヤーに対し国家的に依存していること (Huawei、Ericsson、 Nokia)
提言	• **通信事業者への新たな電気通信セキュリティー必須要件** (TSR[2]) の設定 • **電気通信セキュリティのための強化された法的枠組みの確立** - TSRの効果的な実施を可能にするためのOfcomへの権限付与 • **ベンダーがもたらすセキュリティリスクの管理** - 調達と契約管理を通じたベンダの厳格な監視 (新TSRの遵守含む) - 事業者とベンダーの緊密な協力の要求 (機器/システム/ソフトウェアに対する効果的な保証試験、検証) - **セキュリティ・レジリエンスリスクが著しく高い特定の類型のベンダーへの追加的な規制** (当該時点では、英国政府は個々のハイリスクベンダーへの規制については最終決定を下すことはできないという結論)
ネクストステップ	• Ofcomとともに、**TSRのドラフトについて業界との協議** • TSR施行のために**必要な政策と規制変更**のため、**最も適切な法的手段の検討** • 世界の通信市場全体のサイバーセキュリティの水準を向上させるために、**国際的なパートナーとの協力を継続** 等

1. Critical National Infrastructure　2. Technical Security Requirement:通信事業者に対し、新たな電気通信セキュリティー必須要件を設定
Source: Department for Digital, Culture, Media & Sport "UK Telecoms Supply Chain Review Report"

(参考) ii 「NCSCによる助言」の概要

名称	• NCSC[1] advice on the use of equipment from high risk vendors in UK telecoms networks
年度	• 2020年1月 発表 • 2020年7月 内容更新 (NCSCによるUS Entity List等に係る分析を踏まえたもの)
主な内容	**ハイリスクベンダーについて、下記のとおり助言** • 英国内ネットワークにおいて、ハイリスクベンダー (以下HRV) の機器の使用に制限を設けるべき • HRVが、NCSCによって設計・監督された特定のリスク軽減戦略を導入している場合にのみ、HRV製品を使用すべき • HRVの製品は、5Gネットワークの最も機密性の高い「コア」部分への使用を禁止、 2023年までにアクセス・ネットワークにおける市場シェアを最大35%まで制限 **更に、Huaweiについて、個別に項を設けてリスクについて言及** • Huaweiは英国で大きな市場シェアを持つ一方、2017年制定の中国の国家情報法に基づき、英国に有害な行動を取るよう命じられる可能性を指摘 • また、中国国家がサイバー攻撃を実行し、今後も実行すると評価 • 更に、Huaweiのサイバーセキュリティとエンジニアリングの品質は低いと評価 • また、米国の追加制裁により、同社が現在依存している技術へアクセスできなくなるため、英国に供給する製品に大幅な変更をせざるを得ないと指摘 **=> NCSCの助言も踏まえ、英国政府は、2027年末までに、Huawei製品を排除する方針を公表**

1. National Cyber Security Centre：国家サイバーセキュリティセンター
Source: NCSC"NCSC advice on high risk vendors in UK telecoms",NSCS"Summary of the NCSC analysis of May 2020 US sanction", GOV.UK"Huawei to be removed from UK 5G networks by 2027"

(参考) ii 「5Gサプライチェーンの多様性戦略」の概要

名称	• 5G Supply Chain Diversification Strategy
作成者	• Department for Digital, Culture, Media and Sport[1]
年度	• 2020年11月発表
背景/目的	• 英国は、**ハイリスクベンダーのリスクを管理・軽減し**、セキュリティフレームワークを導入してきた – "我々は、世界で最も厳しい通信セキュリティ体制を導入するために、大胆な措置を講じている (大臣による序言)" • 加えて、**多様性ある供給基盤を構築する必要あり、という認識** • このため、**世界の電気通信市場の多様化**を進めるべく、**3つの軸で戦略を検討**： – **1) 既存事業者**の足元での市場供給能力の強化と新規市場への参入支援 – **2)** 英国市場の弾力性・競争力向上のために**新規事業者の誘致** – **3) 特定事業者への依存**を避けるため、**オープンインターフェイスソリューションの加速化**
主な内容	• **1) 既存事業者関連** – グローバル・サプライチェーン全体への業務能力分散の奨励 – サプライチェーン多様化機会の特定 – 関連する研究開発活動の促進 / 中長期的な技術ロードマップに沿った役割遂行の確保 • **2) 新規事業者の誘致** – ネットワークサービスの長期使用/提供のためのロードマップ策定 – Ofcomとの協力を通じた多様化に有益な周波数帯の割り当て、克服すべき障壁の特定 – 新規事業者の参入を妨げうる要件に係る適切な規制の調整 – 新規事業者の参入に伴うコスト増を支援するためのインセンティブ • **3) オープンインターフェイスソリューションの加速** – 英国における大規模なOpen RAN試験等を通じた研究開発エコシステムの確立 等

1. 現在は省庁再編により別組織に統合

Source:Department for Digital, Culture, Media & Sport "5G Supply Chain Diversification Strategy"

「電気通信 (セキュリティ) 法」詳細 [2/9]：妨害防止措置/対象者

通信事業者に対してセキュリティ強化の義務を課し、更に、特定製品・サービスの使用の禁止も含めた措置も可能に

妨害防止措置等の概要

通信法 (Communications Act) 2003を改正するもの

提供者関連

- **公衆電子通信網又は公衆電子通信サービスの提供者 (以下「提供者」) に対し、セキュリティ強化の義務**を課す
  - 主務大臣に、より具体的なセキュリティ義務を提供者に課すための**規則** (regulations) の発行権限を付与 (第1-2条)
  - 主務大臣に、セキュリティ義務を果たすために提供者が取るべき措置に関する**実施要綱** (Code of Practice) を発行する権限を付与 (第3条)
- **提供者**に、**Ofcom[1]等**に対して、**セキュリティインシデントを通知する義務**を課す (第4条)
- **Ofcom**に対し、**提供者によるセキュリティ義務遵守を確保する義務**や、**当該義務の遵守状況を評価**し、**義務を強制する権限 (罰金)** を付与する (第5-7条)

指定事業者関連

- **指定事業者[2]**が**提供等を行う商品・サービス等**に関して、**提供者に対し要件を課す指示 (指定事業者指示/Designated vendor directions) を出す権限、**及び、**事業者を指定する権限を主務大臣**に付与する (第15-16条)
- **提供者による「指定事業者指示」の遵守に関する情報入手**、及び**主務大臣への当該情報の報告をOfcomに求める「監督通知」**を出す権限を主務大臣に付与 (第18条)、**提供者に検査を求める通知 (検査通知/inspection notices) を出す権限をOfcomに付与**する (第19条)
- **「指定事業者指示」**の遵守を**提供者に強制する権限 (罰金)**(第20条)、及び**「指定事業者指示」の要件に違反している者等**に対し、**違反が国家安全保障に対する深刻な脅威もしくはセキュリティに対する重大な損害を与える又はその危険性がある場合に、「緊急執行指示」(Urgent enforcement direction)** を出す権限を主務大臣に付与する (第21条)

対象者

公衆電子通信網または公衆電子通信サービスの提供者
(the provider of a public electronic communications networks or a public electronic communications service)

- なお、「指定事業者指示」に基づく商品・サービスの使用制限については、指示を受けた提供者のみが対象

1. Office of Communications　2.主務大臣が国家安全保障のために必要であると判断した場合に、通知 (指定通知/Designation Notice) を出して指定することができる事業者
Source: Telecommunications (Security) Act 2021、国立国会図書館ウェブサイト（ 【イギリス】[立法情報]2021年電気通信（セキュリティ）法の制定 (ndl.go.jp)

「電気通信 (セキュリティ) 法」詳細 [3/9]：対象分野

通信ネットワークやサービスの提供者に対し、セキュリティ義務の強化が求められている

対象分野

公衆電子通信網または公衆電子通信サービスの提供者
The provider of public electronic communications network of a public electronic communications service

電子通信ネットワーク

- データ通信または関連するあらゆる装置または装置群、電気的磁気的または電気磁気的エネルギーの使用により信号を伝達するための伝送システム

電気通信サービス

- 電気通信ネットワークにより提供される下記のサービス
  - インターネット・アクセス・サービス
  - 番号ベース (number-based) の対人通信サービス
  - 機械対機械サービスまたは放送に使用される伝送サービスなど、信号の伝送からなり、または信号の伝送を主要な特徴とするその他のサービス

Source: Telecommunications (Security) Act 2021 、Communications Act 2003

(参考)「電気通信 (セキュリティ) 法」における対象事業者

通信ネットワークやサービスの提供者全般に対してセキュリティ義務の強化が求められる一方で、
具体的に指示が出された事業者のみに対し、指定事業者の製品・サービスの使用が禁止される

提供者の義務	対象者	
	提供者 (右記を除く)	指示を受けた提供者
セキュリティ強化	✓	✓
セキュリティインシデントの通知	✓	✓
指定事業者の製品・サービスの使用禁止等の指示		✓

Source: Telecommunications (Security) Act 2021 、Communications Act 2003

「電気通信 (セキュリティ) 法」詳細 [4/9] : Ofcomの概要　[1/2]

Ofcom (通信庁) は、「科学・イノベーション・技術省」と連携し、通信サービスの規制に取り組む組織

Department for Science, Innovation and Technology

- 英国を世界的な科学技術先進国に位置付けること
- 生活を変え経済成長を持続させるイノベーションの推進
- 経済、安全保障、公共サービスを支えるための人材育成プログラム、物理的・デジタルインフラ、規制
- 研究開発のファンディング

連携

15の機関

Executive Agency	Building Digital UK
	Intellectual Property Office
	Met Office
	UK Space Agency
Executive non-departmental public body	Advanced Research and Invention Agency
	Information Commissioner's Office
	UK Research and Innovation
Tribunal	Copyright Tribunal
Public Corporation	National Physical Laboratory
	Ordnance Survey
Other	British Technology Investments Ltd
	Government Office for Science
	Ofcom
	Phone-paid Services Authority
	UK Shared Business Services Ltd

Source: Departments, agencies and public bodies - GOV.UK (www.gov.uk), Ofcom.org.uk"What is Ofcom?"

「電気通信 (セキュリティ) 法」詳細 [5/9]：Ofcomの概要　[2/2]

会長	• Michael Grade（2022年5月就任）
人数体制	• 1353人（2023年3月時点）
設立時期	• 2002年
背景/目的	• Office of Communications Act 2002に基づいて独立した公的機関として設立 • 主要な義務は下記のとおり 　– 通信に関連する市民の利益の促進 　– 関連市場における、適切な場合は競争の促進を通じた、消費者の利益の促進
主な活動内容	• ブロードバンドを含む通信サービスを利用できるようにすること • 多様な企業が、多様な視聴者にアピールできる質の高いテレビ・ラジオ番組を提供できるようにすること • 視聴者・聴取者を、テレビ・ラジオ・オンデマンドで、有害/不快なものから保護すること • 番組によるプライバシー侵害等の不当な扱いから保護すること • ユニバーサル郵便サービスを、英国全土で標準的な料金でカバーすること • 電波を最も効果的な方法で利用すること 等

Source: Departments, agencies and public bodies - GOV.UK (www.gov.uk), Ofcom.org.uk"What is Ofcom?" (HC 1506) - Ofcom Annual Report and Accounts 2022-2023, Communications Act 2003 (legislation.gov.uk)

(参考) 通信事業者とOfcomとの関係性

Ofcomは、対象事業者からのインシデント報告や必要に応じて実施する関連情報の開示を通じ、①事業者のコンプライアンス遵守の監視、②義務不履行時の措置の執行、③Ofcomの役割・義務の内容等に関するガイダンスを実施

Ofcom役割	内容詳細
① 事業者のコンプライアンス遵守を監視	• 新しい電気通信セキュリティフレームワークへのコンプライアンス遵守状況の監視 – 産業界とアプローチを協議した上で、関連情報の要求・技術/管理スタッフへのインタビュー、企業内での業務の観察 – 敵対的なサイバー攻撃をシミュレートする「侵入テスト」の実施 • 指定事業者指示の遵守状況の監視 – 通信事業者に対し「検査通知」を発行し、ネットワークの調査・職員への聞き取り、調査・権限のある者によるネットワーク運用の監視等を実施 – Ofcomは事業者より該当情報を入手し、主務大臣にレポートを提出
② 事業者が義務を果たしていない場合の措置を執行	• 重大なセキュリティ侵害があった、あるいはその危険が差し迫っている場合の対応 – 通信事業者に対して、Ofcomが調査をしている間の暫定的な措置、インシデント報告後の影響軽減措置を要求 – 影響を受けた対象者と情報を共有・通知するよう事業者に要求 – 違反があった場合、違反に比例した厳しい制裁金 (年間売上高の10%まで) を科す
③ 義務の内容、Ofcomの役割等に関する事業者向けガイダンスを提供	• 法令上事業者に課される義務の内容・Ofcomの役割等を解説したガイダンスを公表 – 法律の説明を行ったり、Ofcomの役割を紹介する等、複数のガイダンスを出している

Source:Gov.uk"Factsheet 4: Ofcom and Telecoms Security", Ofcom.org.uk"Monitoring direction under s.105Z12", Ofcom guidance on resilience requirements imposed by or under sections 105A to D of the Communications Act 2003

「電気通信 (セキュリティ) 法」詳細 [6/9]：運用プロセス (提供者関連)

提供者は、セキュリティを評価・強化し、インシデント発生時には当局への報告が必要
- 詳細は、"Regulations"や"Code of Practices", "Ofcom Guidance"等で詳述

運用プロセス

提供者による
セキュリティ対策

**各事業者による
セキュリティ対策の実施**

提供者は自身で、**外注先・サプライチェーン**を含めた**適切なリスクアセスメントやセキュリティ対策を実施**
- ネットワーク・サービスのアクセス、パフォーマンス・機能性を損なうインシデントのリスク特定・低減
- ENISA[1]のガイドラインに従うことも推奨

**Ofcomによる評価/
義務の強制**

Ofcomは、**提供者がセキュリティ義務を遵守しているか評価し、義務を強制する権限あり**

なお、提供者は、ネットワーク・サービスのレジリエンスに影響を与える可能性がある変更を計画する場合、早期に当局と協議することが強く推奨
- 法令上、事業者はネットワークおよびサービスのレジリエンスを維持する義務を負っている
- OfcomのGuidance上、Ofcomと事前に協議を行うことが"strongly encourage"

インシデント発生時の報告

提供者はインシデント発生時、Ofcomへの報告が求められる

1. The European Union Agency for Cybersecurity

Source: Ofcom guidance on resilience requirements in sections 105A to D of the Communications Act 2003, Telecommunications (Security) Act 2021, Electronic Communications (Security Measures) Regulations and Telecommunications Security Code of Practice - GOV.UK (www.gov.uk)

(参考)「通信事業者への新たな電気通信セキュリティー必須要件 (TSR)」詳細

2022年3月より10週間にわたりTSR[1]のドラフトへのパブリックコメントを実施。意見を取り入れ、2022年10月にはTSRについて定めた規則が、12月には具体的な手法について記載した規範が施行

各規則等の検討経緯

- 2022年3月1日より5月10日
  - 通信事業者への新たな電気通信セキュリティー必須要件 (TSR) について定めた**「電気通信 (セキュリティ) 規則草案」**と、**「電気通信 (セキュリティ) 実施規範草案」**に対して、**10週間にわたりパブリックコメント**を実施
  - 電気通信事業者を中心に**38件の回答**あり
- 2022年8月30日
  - 上記コメントに対する政府の対応方針が公表
- 2022年10月1日
  - **「電気通信 (セキュリティ) 規則」**施行
  - 電気通信法における電気通信事業者の義務に加えて、講じる必要のあるセキュリティ対策を規定
- 2022年12月1日
  - **「電気通信 (セキュリティ) 実施規範」**施行
  - 電気通信事業者が規則を遵守するための方法に関するガイダンスを記載
  - 規則の基礎となる重要な概念と、通信事業者が講じることができる具体的な措置を説明
- 2024年3月31日
  - 事業者側の実装期限

1. Technical Security Requirement

Source:GOV.UK"Proposals for new telecoms security regulations and code of practice - government response to public consultation、GOV.UK"Electronic Communications (Security Measures) Regulations and Telecommunications Security Code of Practice"

「電気通信 (セキュリティ) 法」詳細 [7/9]：セキュリティ強化義務の内容

「電気通信 (セキュリティ) 規則」において、具体的な義務の内容が記載されている

事業者に課される義務

「電気通信法」にて、通信事業者は以下を講じることが義務付けられている

- セキュリティ侵害が発生するリスクの特定
- セキュリティ侵害の発生リスクの低減
- セキュリティ侵害の発生への備え

内容詳細

具体的な義務については「電気通信 (セキュリティ) 規則」において記載されている

- パブリックネットワークを安全に設計および構築 (または既存のネットワーク アーキテクチャの場合は再設計および開発) して**セキュリティ侵害のリスクを低減する方法で開発し、維持**すること
- パブリックネットワークの運用に関連する**データを適切な方法で保存し、機能を保護**すること
- 高リスクで敵対的な国家主体から**監視と分析**を可能にするツールを保護すること
- 記録/ログを少なくとも 13 か月間保持することにより、ネットワークまたはサービスへのアクセスと変更を**監視および分析**すること
- 第三者との関係性において生じたセキュリティ侵害のリスクを特定し低減するために、**契約上の取り決めや計画の文書化などのサプライチェーンと連携した措置を講じる**こと
- 不正アクセスまたはセキュリティ侵害のリスクを低減するために、**多要素認証やデフォルト認証情報の使用を避けるなどの防止措置を講じる**こと
- セキュリティ侵害の発生に備え、悪影響を抑制し、回復を可能にするために、**情報のオンラインコピーやその交換などの修復と復旧の準備を行う**こと
- 責任者の設定やポリシーの策定など適切な管理体制といった**ガバナンスを構築**すること
- リスクに対する関連動向を考慮し、**定期的なレビューを実施**すること
- 適切な期間内にパッチまたは緩和策を展開し、セキュリティ更新プログラムを**アップグレードおよび実装**すること
- 適切な技術と能力を有した責任者が第三者であるサプライヤーの活動やリスクを低減する目的でその実施事項等について保証すること
- セキュリティのリスクを特定するために**適切な間隔でテストを実施**すること
- 他のプロバイダーと情報を共有し、**セキュリティ上の問題の影響を修復または軽減**すること
  - ただし、情報共有は、セキュリティ リスクの特定と軽減を目的とする場合に限る

Source： GOV.UK "The Electronic Communications (Security Measures) Regulations 2022"

(参考) Ofcomによる評価/義務の遵守の確認の流れ

Ofcomによる提供者に対する義務の実施に関するモニタリングの流れや想定期間については、ガイダンスにて詳細に説明されている

Ofcomによる実施事項の詳細と想定期間

		類型[1] (Tier) の決定	情報収集 (初回)	情報収集 (追加)
Ofcomの 実施事項		事業者がどの階層 (Tier 1～3) に該当するかを確認。 Tier 1およびTier 2に該当する事業者には、その旨を通知 • 流れを説明するための会議を設定 • 3か月以内の終了を想定しているものの、時期によりそれ以上も想定	対象となるネットワーク/サービス/資産と、それらが構成する資産の詳細な情報を収集 • 事業者がセキュリティ義務を遵守しているかを確認	情報収集のリクエストを管理可能な規模に保ちつつ、措置の執行の判断に足る妥当なレベルの詳細を収集 必要に応じてフォローアップミーティングを実施する
想定 期間	Teir1	3か月	4か月	6か月に1回実施 • 事業者からの回答に4か月を要する • 約4回程度必要と想定
	Teir2	3か月	6か月	9か月に1回実施 • 事業者からの回答に6か月を要する • 約4回程度必要と想定

1. Tier1：関連売上高10億ポンド以上、Teir2：関連売上高5,000万ポンド以上10億ポンド未満、Tier3：関連売上高5,000万ポンド未満 (Teir3に対するモニタリングは想定していない) で区分されている
Source：Ofcom "Annex 5: Draft general statement of policy under section 105Y of the Communications Act 2003"

「電気通信 (セキュリティ) 法」詳細 [8/9]：運用プロセス (指定事業者関連)

主務大臣は、国家安全保障上、必要な場合、特定の者 (ベンダー) を指定しつつ、提供者に対して、指示を出すことが可能

運用プロセス

- 指定事業者関連

指定事業者の指定通知

主務大臣は、**国家安全保障上必要であると判断**した場合に限り、**指定通知**を発することが可能
- 商品、サービス又は施設の性質、それらの品質等が考慮要素 **[詳細次頁]**

通知には指定の理由を明記する必要あり (安全保障上の利益に反する場合は適用なし)

また、合理的に可能な限り、**指定される者と協議**する必要あり

指示に関する業界等との協議

主務大臣は、指定事業者との取引制限等、指示を行う場合、指示により影響を受けることになる**提供者**や**指定事業者**と、合理的に可能な限り、**協議を実施**

提供者に対する指示

主務大臣は、**国家安全保障のために必要**であり、**指示の内容が達成しようとすることと比例している場合**に限り、**指示を出すこと**が可能
- 指定事業者が供給/提供/利用可能にする商品、サービス、または施設の**使用に対する制限 等** (取引禁止措置を含む)
- 指定事業者が指示要件に違反している場合、**罰金を科し、また、緊急執行指示を出すことも可**
  - 関連する売上高最大10%/最大1日10万 £ 等

Note：必ずしも上記の順番で実施されるとは限らない
Source: Legislation.gov.uk "Telecommunications (Security) Act 2021"

(参考) 指定事業者に関する審査プロセスとその期間

指定事業者に関する審査プロセスについて、法令上は期間に関し、特段明記はされていない。
なお、Huaweiを指定事業者に指定したケースにおいては、正式な協議から最終的な指定/指示までは、約8か月を要している

方針の発表

- **2020年7月14日 政府としてHuawei機器の撤去方針の発表**
  - 英国政府は国家サイバーセキュリティセンター(NCSC)の調査・アドバイスに基づき、Huawei機器を2027年までに英国の5Gネットワークから撤去すると発表
  - NCSCは米国のHuawei規制の影響を調査・分析し、「リスクは十分に高く、NCSCはアメリカによるHuaweiの輸出管理規則後の機器を英国で一切使用しないよう勧告する」と公表

法案提出/通知書草案公表

- **2020年11月30日 Huawei・通信事業者への通知書草案を公表**
  - 同月に、電気通信 (セキュリティ) 法案が提出されていたところ、同法案に基づく通知書等の草案も策定
    (事業者を指定する通知の草案は10ページ、通信事業者への指示の草案は23ページに渡り、詳細を記載)
  - 草案は、該当者に直接送付されつつ、GOV.UKでも公表

法案成立/協議/指定通知

約8か月

- **2021年11月19日 電気通信 (セキュリティ) 法案が成立**
- **2022年2月18日～2022年3月21日 指示の内容について産業界等との協議**
  - 規制内容やタイムラインの公平性・妥当性等を協議するための35個の質問を公表し、4週間の回答受付期間を設定
  - Huawei・対象通信事業者は、所定のメールに返信することで回答を提出することが可能
- **2022年10月13日 指定事業者・通信事業者への最終通知を公表**
  - 2020年7月のHuawei機器撤去宣言を法的根拠に基づいて有効化
  - 協議の結果、草案で公表された2027年Huawei機器撤去に向けた段階的規制のうち8つの期限は変更がないものの、残り2つの規制の期限については、一部事業者においてネットワークの停止と顧客の混乱につながる可能性が認められた
  - 最終通知では、ネットワークの不必要な不安定化を避けつつ、Huaweiをできるだけ迅速に排除する必要性のバランスを保つ段階的期限を正式に設定

Source: GOV.UK"Huawei to be removed from UK 5G networks by 2027", NCSC.GOV.UK "Summary of the NCSC analysis of May 2020 US sanction", GOV.UK"Telecommunications (Security) Bill: Illustrative designated vendor direction and designation notice", GOV.UK"Telecommunications (Security) Act 2021: draft designated vendor direction consultation", GOV.UK"Huawei legal notices issued"

「電気通信 (セキュリティ) 法」詳細 [9/9]：指定の際の考慮要素

主務大臣は、指定事業者を、商品・サービスの性質や品質、信頼性、その者の身元等に基づき判断

指定通知の際の考慮要素

特定の者を指定するかどうかを検討する際、主務大臣が考慮することができる事項には以下が含まれる。

(a) その者によって供給され、提供され、または利用可能となる商品、サービス、または施設の性質
(b) 商品、サービスもしくは施設またはそれらの構成要素の品質、信頼性および安全性
　(それらの開発もしくは生産またはそれらの供給、提供もしくは利用可能化の方法の品質、信頼性および安全性を含む)
(c) 商品、サービスまたは施設の供給の信頼性
(d) 商品、サービス、施設に対するメンテナンスまたはサポート提供の質と信頼性
(e) その者が供給、提供、または利用可能とする商品、サービス、または施設が、英国内で使用される、または使用される可能性のある範囲および方法
(f) その者によって供給、提供、または利用可能になった商品、サービス、または施設が、他の国や地域でどの程度、どのような方法で使用されているか、または使用される可能性があるか
(g) 関係者の身元
　(i) その者またはそれを構成するものが供給、提供、または利用可能にする商品、サービス、または施設の開発または生産
　(ii) 当該商品もしくはサービスの供給もしくは提供、または当該施設を利用可能にすること
　(iii) 当該商品、サービスまたは施設の保守またはサポートの提供
(h) 所有者、管理者、またはその関係者の身元

Source: Telecommunications (Security) Act 2021 、Communications Act 2003

3-2. 英国

1. 政策の全体像

2. 制度の調査結果
   - 電気通信 (セキュリティ) 法 (1)
   - その他のインフラ防護等に関する法令 等

3. 事例

英国のその他のインフラ防護等に関する法令 等

	法令名	制定年	法令の概要
2	国家安全保障及び投資法 (National Security and Investment Act)	2021年	• 国家安全保障を脅かす可能性がある外国企業や投資家による英国企業に対する買収を精査し、介入する権限を強化した法律 • 17の主要分野 (先端素材、先進ロボット、人口知能等) での取引を対象に、これらの分野に関わる取引を行う企業や投資家が、対象となる英国企業の株式または議決権を25%以上取得する場合、政府から承認を得る必要あり
3	ネットワーク及び情報システム規則 (NIS規制) (The Security of Network & Information Systems Regulations : NIS regulations)	2018年	• 経済・社会にとって重要なデジタル・インフラ事業者等の重要な基盤サービス提供事業者に対して、適切なセキュリティ対策の実施や重大インシデントに関する当局への報告を義務付け - デジタルサービス (オンラインマーケットプレイス、オンライン検索エンジン、クラウドサービス) - 基盤サービス (交通、エネルギー、水道、医療、デジタル・インフラ・サービス)
4	[参考]消費者向けIoT製品等 PSTI法 (Product Security and Telecommunications Infrastructure Act 2022)	2022年	• 製品/製品メーカーのセキュリティサポートに関する要求事項を設定 - デフォルトのパスワード設定の禁止 - 脆弱性情報の報告 - 製品のセキュリティアップデートの期間の透明化
5	[参考] ガイダンス用フレームワーク サイバーアセスメントフレームワーク (CAF)	2018年	• 国家の重要なインフラ (Critical National Infrastructure) の事業者は、本評価基準に沿って、サイバー対策の状況を評価することを推奨 - なお、政府機関/独立行政法人は、本CAFに基づき、GovAssureという機関によるレビューが義務付けられている

Source: National Security and Investment Act 2021 - GOV.UK (www.gov.uk) , The NIS Regulations 2018 - GOV.UK (www.gov.uk), Product Security and Telecommunications Infrastructure Act 2022 (legislation.gov.uk), The Product Security and Telecommunications Infrastructure (PSTI) Bill – product security factsheet - GOV.UK (www.gov.uk), Cyber Assessment Framework (CAF) changelog - NCSC.GOV.UK, Government Cyber Security Strategy: 2022 to 2030 - GOV.UK (www.gov.uk), GovAssure - UK Government Security, Government launches new cyber security measures to tackle ever growing threats - GOV.UK (www.gov.uk)

3-2. 英国

1. 政策の全体像

2. 制度の調査結果
   - 電気通信 (セキュリティ) 法 (1)
   - その他のインフラ防護等に関する法令 等

3. 事例

Huaweiに対する「指定通知」

国家安全保障上のリスクからHuaweiを指定事業者に指定 (2022年10月12日付文書)

指定文書の内容 (抄)

- 政府は、**中国及びその関係者が、英国にサイバー攻撃を実行しており、今後も実行すると評価**
  - 中国の法律・慣行が、中国に拠点を置く企業やその従業員に対し、英国にとって有害な活動を要求する可能性

- **Huawei**の製品とサービスの**サイバーセキュリティとエンジニアリングの品質について懸念**を表明
  - Huaweiは英国のFTTPおよびモバイルアクセスネットワークにおいて大きな市場シェアを有しており、2019年7月時点では、それぞれ**44%**および**35%**と推定
  - 国家安全保障上の懸念により、**Huaweiへの依存**は、**システム障害や敵対的悪用の潜在的影響を著しく増大させるため、国家安全保障に対する容認できないリスクが発生**
  - 上記の**Huaweiがもたらす累積的な国家安全保障リスク**を、他のベンダーが提供する機器やサービスがもたらす**国家安全保障リスクより大きく評価**

Source: Huawei Designation Notice (publishing.service.gov.uk)

(参考) Huaweiに対して発出した指定通知書 (和訳) [1/4]

2003年通信法第105Z8条に基づく指定通知、指定事業者指示のためのHuaweiの指定

背景

1. 2003年通信法（「法」）第105Z8条(1)は、国務大臣が指定事業者指示の目的のために者を指定する通知を発行することができると規定している。指定事業者指示は、同法第105Z1条(1)によって与えられる意味を有する。法第105Z8条(2)は、指定通知が複数の者を指定できることを規定している。

指定通知

2. 国務大臣は、本通知により、Huawei Technologies (UK) Co., Ltd.および本通知の付属文書に指定されたその関連会社のリスト（以下、総称して「Huawei 企業グループ」または「Huawei」）のそれぞれを、指定事業者指示の目的のための者として指定する。

3. 法第 105Z8 条(3)に基づき、国務大臣は、本通知が国家安全保障のために必要であると考え、本通知を発出する。

Source: Designation Notice under section 105Z8 of the Communications Act 2003, designating Huawei for the purposes of a designated vendor direction

(参考) Huaweiに対して発出した指定通知書 (和訳) [2/4]

通知の理由

4. 法第105Z8条5項に従い、国務大臣は以下の理由により、本通知が国家安全保障のために必要であると考える。

a. Huaweiの企業グループは中国に本社を置き、中国を拠点として支配されている。政府は、中国国家およびその関係者が、英国および英国の利益に対するサイバー攻撃を実行し、今後も実行することが予想されると評価している。特に、中国国家とその関連行為者は、電気通信サービス機器の弱点、および／または公衆電子通信ネットワークのプロバイダーがそのネットワークを構築・運用する方法の弱点を悪用し、そのセキュリティを侵害しようとし続けている。

b. 中国国家の慣行は、中国国家情報法2017（2018年改正）などの法律の運用方法と相まって、国家が中国に拠点を置く企業およびその従業員に対し、英国にとって有害な活動に従事するよう要求することを可能にする可能性がある。規則が運用される方法は、そのような企業が英国に有害な活動に従事するよう子会社に指示することを要求できることを意味する。また、Huaweiの従業員は、Huaweiの知らないところで中国国家が出した指示に従うよう求められることもある。これらの権限により、Huaweiの機器に秘密裏に悪意のある機能が組み込まれるリスクが生じる。英国がFTTP（Fiber to the Property）やモバイル・ネットワークの提供においてHuaweiへの依存度を高めた場合、このリスクはさらに高まるだろう。

c. Huaweiの製品とサービスのサイバーセキュリティとエンジニアリングの品質は、敵対的な悪用やシステム障害の現実的なリスクを生じさせる。この点に関して、Huawei・サイバーセキュリティ評価センター監督委員会は、2018年、2019年、2020年、2021年の年次報告書で、Huaweiのエンジニアリング・プロセスについて重大な懸念を提起している。2020年の報告書では、「NCSCは現在、数年にわたってHuaweiの製品品質に重大な問題がある証拠を目にしている」と述べている。2021年版報告書では、「NCSCが期待する製品ソフトウェアエンジニアリングとサイバーセキュリティの品質を満たすために、2020年の間に全体的な改善が見られないことを示す問題が引き続き発覚している」と述べている。

Source: Designation Notice under section 105Z8 of the Communications Act 2003, designating Huawei for the purposes of a designated vendor direction

(参考) Huaweiに対して発出した指定通知書 (和訳) [3/4]

通知の理由（続き）

d. Huaweiの製品とサービスの品質に関する国務大臣の懸念は、米国がHuaweiに対して科した制裁措置によって悪化している。これらの制裁により、一部のHuawei製品の製造が変更され、信頼性が低下し、欠陥の改善が難しくなった可能性がある。さらに：

i. 米国の輸出管理改革法2018に基づき作成された輸出管理規則に規定された、2020年5月および2020年8月の米国の外国生産直接製品規則の変更の結果、Huaweiは、米国の特定技術を使用して設計または製造された機器、特に半導体を購入または製造することができない。ライセンスの申請は、法的には拒否されるものと推定される。国務大臣は現在、5G機器に関してそのようなライセンスが付与されたことを認識していない。Huaweiの製造工程とサプライチェーンに深刻な影響を与えた結果、Huaweiは未知のテストされていないツールを使用して半導体やその他の機器を製造することを余儀なくされており、このような方法で製造された製品に対する適切な保証を提供することは著しく困難であり、不可能な可能性がある。

ii. 制裁措置の継続的な影響、将来的な制裁措置の実施および強化のリスク、ならびに米国が付与した「一時的一般ライセンス」（Huaweiへの一部供給を許可）の2020年8月の失効は、Huaweiがマネージドサービス（ネットワークの継続的な日常運用を確保するためのサポートおよびメンテナンスサービス）を合法的に提供する能力に、事前の通知なしに影響を及ぼしており、今後も影響を及ぼす可能性がある。

iii. 米国の制裁措置の影響により、Huaweiはサプライチェーンの重要な部分を中国に移転しており、中国技術の使用への依存度を高めている。その結果、英国のFTTP（Fiber to the Property）およびモバイル・ネットワークへの関与において、Huaweiは未知で未検証のコンポーネントへの依存度を高めている。これは、国家安全保障上の重大な懸念を引き起こす。

Source: Designation Notice under section 105Z8 of the Communications Act 2003, designating Huawei for the purposes of a designated vendor direction

(参考) Huaweiに対して発出した指定通知書 (和訳) [4/4]

通知の理由（続き）

e. Huaweiは、英国のFTTPおよびモバイルアクセス（MA）ネットワークにおいて、2019年7月時点でそれぞれ44%および35%と推定される大きな市場シェアを有している。Huaweiの規模とその事業規模を考慮すると、HuaweiはFTTPとMAネットワークにおいて、国家依存の重大なリスクを生み出す形で市場シェアを拡大する能力を有している。介入がなければ、英国は3つのFTTPおよびMAネットワークの提供においてHuaweiに依存するようになる可能性が高い。これらのネットワークは、英国の重要な国家インフラの一部を形成している。
上記 4(a)から(d)で述べた国家安全保障上の懸念により、Huaweiへの依存は、システム障害や敵対的悪用の潜在的影響を著しく増大させるため、国家安全保障に対する容認できないリスクが生じる。

f. 上記のHuaweiがもたらす累積的な国家安全保障リスクは、他のベンダーが提供する機器やサービスがもたらす国家安全保障リスクを大幅に上回る。Huaweiのリスクプロファイルは、指定ベンダーの指示に従った特定の強化措置によってのみ管理できる。

Source: Designation Notice under section 105Z8 of the Communications Act 2003, designating Huawei for the purposes of a designated vendor direction

指定事業者指示 (提供者に対する指示) [1/2]：概要

国家安全保障上のリスクから、関連する通信事業者にHuawei規制の通知を実施 (2022年10月12日付文書)

指示の内容 (抄)

- 28ページにわたる資料を通じて、通信事業者に対し、Huaweiの機器使用を段階的に禁止する旨や対象の詳細を記載

- 指示の理由も詳細に記載
  - 政府として、中国及びその関係者が、英国にサイバー攻撃を実行しており、今後も実行すると評価
  - 2017年国家情報法など、中国に拠点を置く企業等へ中国国家の指示へ従うよう要求する慣習
  - サーバーセキュリティ評価センターによるHuaweiのエンジニアリング・プロセスへ重大な懸念があるという評価
  - 米国による経済制裁　等

Source: Huawei Designated Vendor Direction (publishing.service.gov.uk)

指定事業者指示 (提供者に対する指示) [2/2]：対象事業者

以下の35の事業者は、Huaweiの使用に関連する指定事業者の指示を受けており、提供者はその指示に従わなければならない

- Openreach
- BT/EE
- VMO2
- Vodafone
- Sky
- TalkTalk
- Three
- AT&T
- Bharti Airtel
- CenturyLink Communications (now Lumen)
- CityFibre
- Cellnex
- Colt Technology Services
- Daisy Group Holdings
- Dixons Carphone
- Elitetele
- Fujitsu
- KCOM Group
- Nasstar
- Neos Networks
- Shell Energy
- Tata Communications
- Telia Carrier UK
- Tesco Mobile
- Telstra
- Gamma
- Verastar
- Verizon
- XLN Telecom
- Zayo
- China Telecom
- China Mobile
- Airwave Solutions
- Hyperoptic
- Gigaclear

上記35事業者は、提供者の規模が非常に大きい、または地域的な重要性が高い提供者

上記以外の指示を受けていない提供者に対しても、独自のセキュリティ基準を検討する際に、指定事業者であるHuaweiの影響を考慮することを推奨している

Source: Proposals to issue a designation notice and designated vendor direction for Huawei - government response to consultation - GOV.UK (www.gov.uk)

(参考) 提供者に対する指示の理由 [1/2]

理由についても、詳細に記載。中国やHuawei製品への安全性の懸念や他国動向が挙げられている

方針決定の理由 (和訳抜粋)

法第105Z1条(5)(b)に従い、国務大臣は以下の理由により、本指示が国家安全保障のために必要であると考える。

(1) Huaweiの企業グループは、中国に本社を置き、中国で経営されている。政府は、**中国国家およびその関連行為者は、英国および英国の利益に対するサイバー攻撃を実行し、今後も実行することが予想されると評価**している。特に、中国国家とその関連行為者は、電気通信サービス機器の弱点、公衆電子通信ネットワークのプロバイダーがそのネットワークを構築・運用する方法の弱点を悪用し、そのセキュリティを侵害しようとし続けている。

(2) **中国国家の慣行は、中国国家情報法2017 (2018年改正) などの法律の運用方法と相まって、中国に拠点を置く企業およびその従業員に対し、英国に有害な活動に従事するよう要求することを可能にする**。規則が運用される方法は、そのような企業が英国に有害な活動に従事するよう子会社に指示することを要求できることを意味する。また、**Huaweiの従業員は、Huaweiの知らないところで中国国家が出した指示に従うよう求められることもある**。これらの権限により、Huaweiの機器に秘密裏に悪意のある機能が組み込まれるリスクが生じる。このリスクは、英国がFTTP（Fiber to the Property）やモバイル・ネットワークの提供においてHuaweiへの依存度を高めた場合、さらに高まるだろう。

(3) **Huaweiの製品とサービスのサイバーセキュリティとエンジニアリングの品質は、敵対的な悪用、システム障害の現実的なリスクを生じさせる**。この点に関して、Huawei・サイバーセキュリティ評価センター監督委員会は、2018年、2019年、2020年、2021年の年次報告書で、Huaweiのエンジニアリング・プロセスについて重大な懸念を提起している。2020年の報告書では、「NCSCは現在、数年にわたってHuaweiの製品品質に重大な問題がある証拠を目にしている」と述べている。2021年版報告書では、「NCSCが期待する製品ソフトウェアエンジニアリングとサイバーセキュリティの品質を満たすために、2020年の間に全体的な改善が見られないことを示す問題が引き続き発覚している」と述べている。

Source: Proposals to issue a designation notice and designated vendor direction for Huawei - government response to consultation - GOV.UK (www.gov.uk)

(参考) 提供者に対する指示の理由 [2/2]

理由についても、詳細に記載。中国やHuawei製品への安全性の懸念や他国動向が挙げられている

方針決定の理由 (和訳抜粋)

(4) Huaweiの製品とサービスの品質に関する国務大臣の懸念は、**米国がHuaweiに対して科した制裁措置**によって悪化している。この制裁により、一部のHuawei製品の製造が変更され、信頼性が低下し、欠陥の改善が難しくなった可能性がある。加えて、以下の懸念がある

- (a) 米国輸出管理改革法2018に基づき作成された輸出管理規則に規定された、2020年5月および2020年8月の米国の外国生産直接製品規則の変更の結果、Huaweiは、米国の特定技術を使用して設計または生産された機器、特に半導体を購入または製造することができない。ライセンスの申請は、法的には拒否されるものと推定される。国務大臣は現在、5G機器に関してそのようなライセンスが付与されたことを認識していない。Huaweiの製造工程とサプライチェーンに深刻な影響が及んだ結果、Huaweiは未知でテストされていないツールを使用して半導体やその他の機器を製造せざるを得なくなり、このような方法で製造された製品に対する適切な保証を提供することが著しく困難になり、不可能になる可能性がある
- (b) 制裁の継続的な影響、将来的な制裁の実施と拡大のリスク、そして米国が付与した「一時的一般許可」の2020年8月の失効 (これは、米国による制裁の継続的な影響であり、一部Huaweiへの供給が許可されている) は、Huaweiがマネージドサービス (ネットワークの継続的な日常運用を確保するためのサポートおよびメンテナンスサービス) を適法に提供する能力に、事前の通知なしに影響を及ぼし、今後も影響を及ぼす可能性がある
- (c) 米国の制裁措置の影響により、Huaweiはサプライチェーンの重要な部分を中国に移し、中国技術の使用への依存度を高めている。その結果、英国のFTTP (Fiber to the Property) やモバイル・ネットワークへの関与において、Huaweiは未知の未検証部品への依存度を高めている。これは、国家安全保障上の重大な懸念を引き起こす。

(5) Huaweiは英国のFTTPおよびモバイルアクセス (MA) ネットワークにおいて大きな市場シェアを有しており、2019年7月時点ではそれぞれ44%および35%と推定される。Huaweiの規模と事業規模を考慮すると、HuaweiはFTTPとMAネットワークの市場シェアを拡大する能力を有しており、これは**国家依存の重大なリスク**を生み出す。介入がなければ、英国は FTTP と MA ネットワークの提供においてHuaweiに依存するようになる可能性が高い。これらのネットワークは、英国の重要な国家インフラの一部を形成している。上記 (1)から(4)に記載された国家安全保障上の懸念により、Huaweiへの依存は、システム障害や敵対的悪用の潜在的影響を著しく増大させるため、国家安全保障に容認できないリスクが生じる

(6) 上記の**Huaweiがもたらす累積的な国家安全保障リスクは、他のベンダーが提供する機器やサービスがもたらす国家安全保障リスクを大幅に上回る**。Huaweiのリスクプロファイルは、指定ベンダーの指示に従った特定の強化措置によってのみ管理できる。

Source: Proposals to issue a designation notice and designated vendor direction for Huawei - government response to consultation - GOV.UK (www.gov.uk)

(参考) 段階的な規制内容

2027年にかけて、段階的に規制内容 (対象) を拡大させ、2027年12月末までに禁止

段階的規制の内容とそれぞれの効力発生日 [ANNEX C]

- **本指令の施行日 (2022年10月14日)**
  - 2020年12月31日より後に調達されたHuawei機器の使用禁止 [5Gネットワーク]
  - 米国規則の変更 (2020/5/19, 8/17) により、製造工程/サプライチェーンが変更されたHuawei機器の使用・設置禁止
  - Huawei機器の設置禁止 (既に設置済の場合とHuawei機器を直接保守するために必要な場合は除く) [5Gネットワーク]
  - Huaweiによるサービスの利用の禁止 (既に設置された機器に対するHuawei専門の維持サービスは除く)
- **2023年1月28日**[1]
  - 国家安全保障上重要な場所に所在する加入者にサービスを提供する可能性のあるモバイル・アクセス・ネットワークにおけるHuawei機器またはサービス利用の禁止
  - 但し、公衆通信事業者が、本指令の日付以前に、影響を及ぼす当該サイトのリストを提供された場合に限る
- **2023年7月末**[1]
  - Huawei機器の使用に35%の上限を設定 [5Gアクセスネットワーク]
- **2023年10月末**[1]
  - Huawei機器の使用に35%の上限を設定 [FTTP、およびその他のギガビット以上のアクセス・ネットワーク]
- **2025年12月末**[1]
  - Huawei機器 (ハイデータレート伝送装置) の使用禁止 [ネットワーク全体]
- **2027年12月末**[1]
  - Huawei機器・サービスの使用禁止 [5Gネットワーク全体]

1. 実際に使用等が禁止されるのは、各日付の翌日から

Source: Huawei Designated Vendor Direction (publishing.service.gov.uk)

(参考) 対象機器

対象となるコアネットワーク機能は、本指令にて細かく指定

5Gネットワークを含む、すべてのモバイルおよび固定ネットワーク：

- インターネット・プロトコル・コア (プロバイダーのネットワークのコア内でインターネット・プロトコル／マルチプロトコル・ラベル・スイッチングまたはルーティングを行う機能を含む)
- セキュリティ機能
- 運用サポートシステム (OSS) (プロバイダーのネットワークに配備されたHuawei機器をサポートするために必要な範囲を除く)
- 管理と認証
- 認証・監査 (AAA) 機能
- 仮想化インフラ (ネットワーク機能仮想化インフラ (NFVI)) を含む
- オーケストレーターおよびコントローラー機能 (MANO (Management and Network Orchestration) およびSDN (Software Defined Network) オーケストレーター/コントローラーを含む)
- ネットワークの監視と最適化
- 相互接続機器 (高データレートのイントラコアおよび事業者間伝送機器は、独自の管理の対象となるため、この定義から除外されている)
- インターネット・ゲートウェイ機能
- 合法的インターセプト関連機能

すべての5Gネットワーク：

- 5Gコアデータベース機能
- 5Gコア関連サービス
  - 認証サーバー機能 (AUSF) 、アクセス＆モビリティ管理機能 (AMF) 、非構造化データ保存機能 (UDSF) 、ネットワークエクスポージャーファンクション (NEF) 、中間NEF (I-NEF) 、ネットワークリポジトリ機能 (NRF) 、ネットワーク・スライス選択機能 (NSSF) 、ポリシー・コントロール・ファンクション (PCF) 、セッション管理機能 (SMF) 、統合データ管理 (UDM) 、ユニファイド・データ・リポジトリ (UDR) 、ユーザープレーン機能 (UPF) 、UE radio Capability Management Function (UCMF) 、アプリケーション機能 (AF) 、5G-Equipment Identity Register (5G-EIR) 、ネットワークデータ分析機能 (NWDAF) 、充電機能 (CHF) 、サービス・コミュニケーション・プロキシ (SCP) 、セキュリティ・エッジ保護プロキシ (SEPP) 、非3GPPインターワーキング機能 (N3IWF) 、信頼された非3GPPゲートウェイ機能 (TNGF) 、有線アクセスゲートウェイ機能 (W-AGF)
- 3GPP TS 23.501で規定されている将来の5Gコア機能

Source: Huawei Designated Vendor Direction (publishing.service.gov.uk)

3-3.
オーストラリア

1. 政策の全体像

2. 制度の調査結果
   - 重要インフラ安全保障法 (1)
   - 電気通信法 (2017年改正) (2)

3. 事例

3-3.
オーストラリア

1. 政策の全体像

2. 制度の調査結果
   - 重要インフラ安全保障法 (1)
   - 電気通信法 (2017年改正) (2)

3. 事例

オーストラリアの基幹インフラ妨害行為の防止に係る政策の全体像

主な対象行為		主な対象者		
		国内企業		外国企業
		電気通信事業者	基幹インフラ事業者	
取引規制	製品/役務の調達	1 **重要インフラ安全保障法** • インフラ妨害のリスクが想定される場合、政府が事業者に対し、指示を出すことが可能 **主な制度（詳細深掘り）**		
		2 **電気通信法（2017年改正）** • 電気通信ネットワーク・サービスの変更等について事業者に通知を求め、安全保障を害する可能性ある特定の状況で事業者に指示を与えることを可能に **主な制度（詳細深掘り）**		
	対内直接投資			3 **外資買収法** • 国家安全保障の観点から重要とされる土地や事業に対する外国投資を政府の審査対象とするもの
サイバー攻撃への防護		1 **重要インフラ安全保障法** • 重要インフラ資産の保有者等は、資産に関する情報について、当局に対して登録 • 重要インフラ資産保有者に対し、リスクの予防・最小化のためのプログラム作成やインシデント発生時の報告を義務付け **主な制度（詳細深掘り）**		
		2 **電気通信法（2017年改正）** • 国家安全保障に影響を及ぼす可能性のある電気通信ネットワーク・サービスの変更案について、事業者は通知 **主な制度（詳細深掘り）**		

Note：上記分類は、本調査の目的から、関連が深いと考えられる法令を抽出し、主な目的/対象の相違等を強調するために整理をしたものであり、必ずしも上記各範囲の内容のみを含むとは限らない
特に、国内企業には、国内にて事業活動を行う外国企業も含まれうる

Source: Security of Critical Infrastructure Act 2018, Federal Register of Legislation "Telecommunications and Other Legislation Amendment Act 2017"、Federal Register of Legislation" Foreign Acquisitions and Takeovers Act 1975 "

3-3.
オーストラリア

1. 政策の全体像

2. 制度の調査結果
   - 重要インフラ安全保障法 (1)
   - 電気通信法 (2017年改正) (2)

3. 事例

「重要インフラ安全保障法」概要 [1/2]

法令等の名称

重要インフラ安全保障法
Security of Critical Infrastructure Act 2018

制定時期/主な改定の経緯

- 2018年4月　制定
- 2021年12月　改正
- 2022年4月　改正

制定の経緯

- オーストラリアにおけるサイバー攻撃の増加を背景に、重要インフラに関する国家安全保障上のリスクを管理するための枠組みを提供することを目的に制定
  - オーストラリアにおける重要インフラの所有権および運営管理の透明性を向上させ、これらのリスクを明らかとする
  - 重要インフラのリスクを特定し管理するために、政府のあらゆるレベル、および規制当局、所有者、運営者間の協力と連携を促進する

妨害防止措置の概要

- 重要インフラ資産を所有・運営する事業体・個人またはそれらの直接利害関係者 (以下、責任事業体等) に関し、下記を導入
  - 重要インフラ資産の登録
  - 事業者によるリスク管理プログラムの導入
  - 事業者によるインシデント発生時の報告義務
  - 政府による指示/情報収集の権限の付与
  - 政府によるインシデント発生時の必要な対応の権限
- 更に、国家的に重要なシステムに関連する、サイバーセキュリティの強化義務の設定

対象分野

以下の分野に属する責任事業体等

- 通信、データ保管・処理、金融・証券、水道・下水、エネルギー、ヘルスケア・医療、高等教育・研究、食品・食料品、交通、宇宙技術、防衛

Source: Security of Critical Infrastructure Act 2018, Reporting and Compliance (cisc.gov.au)

「重要インフラ安全保障法」概要 [2/2]

運用の方法 (政府による指示)

- 政府が事業者に特定の行動を求める場合、下記が条件
  - 安全保障上のリスクを排除または低減するため、**合理的に必要であること**
  - 指示を出すことなくリスクを排除または低減する結果を達成するため、当該事業者と**誠実に交渉するための合理的な措置**が取られていること
  - 当該事業体について、**安全性について不利な評価**がなされていること
  - 既存の規制制度が、リスクを排除または低減するため、**代わりに使用され得ない**と認識していること
- また、大臣は指示を与える前に、**関係する大臣等と協議**を行い、**事業者や大臣等から書面にて意見を陳述**させなければならない

指示を出す際の考慮要素

- 当該事業体についての、**安全性についての不利な評価の内容** (これを最も重視)
- 当該事業体が、指示に従うことにより発生する可能性のある費用
- 当該指示が、関連する重要インフラ部門における競争に及ぼす可能性のある影響
- 当該指示が当該事業体の顧客又は当該事業体が提供するサービスに及ぼす可能性のある影響
- 指定された期間内に、事業体または諮問を受けた大臣が行った意見表明

罰則

法令で定める義務を責任事業体が遵守しなかった場合等、罰金が発生
- 違反者が個人/法人かや、違反内容により相違[1]

1. 例えば、リスク管理プログラムの義務を怠った法人の場合の最高罰金額は、1,000 ペナルティユニット (罰金単位。オーストラリア議会HPによれば、2022年3月時点で22万豪ドルに相当)
Source: Security of Critical Infrastructure Act 2018, Risk assessments (homeaffairs.gov.au), Parliament of Australia

「重要インフラ安全保障法」詳細 [1/19]：制定時期/経緯等

重要インフラ安全保障法は、サイバーセキュリティへの対応を強化するために2018年に制定され、
その後も、順次、内容が追加された

法令等の名称

- Security of Critical Infrastructure Act 2018
  - 重要インフラ安全保障法

制定時期/主な改正

- 2018年4月　制定、 同年7月施行
- 2021年12月　改正
- 2022年4月　改正

経緯

- **2018 年4月：増加するサイバーセキュリティへの脅威に対応するために重要インフラ安全保障法を制定**
  - オーストラリアにおけるサイバー犯罪の件数は増加しており、**報告されたサイバーセキュリティ・インシデントの約4分の1が重要インフラや重要サービス**に関連
  - **民間企業/州政府等**によって大部分が所有・運営されている重要インフラ施設のサイバーセキュリティに対して、**連邦政府が関与することを目的**
- **2021年12月**、2018 年法を一部改正する法律が制定
  - 当初案は幅広い事項が盛り込まれており、一部を先行して成立
    - 「**対象資産の拡大**」、「**インシデント報告義務**」、「**政府への新たな権限付与 (情報収集、作業指示等)**」
    - 豪州法制審議会 (Law Council of Australia) が、法案に対し「委任立法の数、範囲、重大性から見て、本法案は極めて異例」と懸念を示したため、法案を分割、サイバーセキュリティ対応から緊急性の高い内容を優先
- **2022 年4月**、2021年改正で先送りした内容 (「**リスク管理プログラム**」、「**サイバーセキュリティ強化義務**」) を成立させ、2018年法を改正

Source: Submissions and discussion paper : Security Legislation Amendment (Critical Infrastructure Protection) Act 2022
出典: 国立国会図書館ウェブサイト（「【オーストラリア】2018 年重要インフラ安全保障法の改正 」）

「重要インフラ安全保障法」詳細 [2/19]：妨害防止措置/分野

重要インフラ資産の所有・運営者等は、関連する資産を登録するとともに、リスク管理やインシデント等の報告の義務あり。
加えて、政府に対し、国家安全保障に関し、情報収集や事業者への命令等の権限を付与

対象分野/ 対象者/資産 **[詳細次頁以降]**	重要インフラ資産を所有・運営する事業体・個人または重要インフラの直接利害関係者 (当該企業の10%の持分保有者) (以下、責任事業体等) • **本法の対象分野は、下記の11分野 (2022年法にて、当初の4分野[1]から拡大)** - 通信、データ保管・処理、金融・証券、水道・下水、エネルギー、ヘルスケア・医療、高等教育・研究、食料・食料品、交通、宇宙技術、防衛 • **それぞれの分野に関連する「重要インフラ資産」が詳細に定義**
妨害防止措置の概要 **[詳細後述]**	**重要インフラ資産を所有・運営する者、又はそれらの直接利害関係者 (以下、責任事業体等) に下記制度を導入** • 重要インフラ資産の登録 (1) • 事業者によるリスク管理プログラムの導入 (2) • 事業者によるインシデント発生時の報告義務 (3) • 政府による指示/情報収集の権限の付与 (4) • 政府によるインシデント発生時の必要な対応の権限の付与 (5) 更に、**国家的に重要なシステムの非公開の指定、**及びそれに関連する、強化されたサイバーセキュリティの義務の設定 (6)
対応すべき妨害行為	下記のサイバーセキュリティインシデント • コンピュータデータ・プログラムに対する不正なアクセスや改変 • コンピュータ同士の通信に対する不正な障害 • コンピュータの本体・データ・プログラムの可用性・信頼性・安全性及び使用自体への不正な障害

1. 当初は、電力、水道、港湾、ガスが対象
Source: Security of Critical Infrastructure Act 2018 、Security of Critical Infrastructure Act 2018 (SOCI) (cisc.gov.au), Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023 (legislation.gov.au)

「重要インフラ安全保障法」詳細 [3/19]：対象分野 (全体像)

本法においては、通信・エネルギーから金融、ヘルスケア、交通、防衛まで、幅広い分野のインフラが、
重要インフラ分野として定義されている
- 一部措置は、対象資産を限定 (資産の登録義務[1]、インシデント通知義務[2])

対象分野 (全体像)

1. 通信 *Communications*
2. データ保管・処理 *Data storage or processing*
3. 金融・証券 *Financial Services and Markets Sector*
4. 水道・下水 *Water and Sewerage Sector*
5. エネルギー *Energy*
6. ヘルスケア・医療 *Healthcare and Medical Sector*
7. 高等教育・研究 *Higher Education and Research*
8. 食品・食料品 *Food and grocery*
9. 交通 *Transport*
10. 宇宙技術 *Space Technology*
11. 防衛 *Defence Industry*

1. 登録義務は右記資産が対象：放送、ドメインネームシステム、データ保管・処理、金融市場インフラ、食料・食料品、病院、貨物インフラ、貨物サービス、公共交通、液体燃料、エネルギー市場運営、電気、ガス、港湾、水道
2. インシデント通知義務は右記資産が対象： 放送、ドメインネームシステム、データ保管・処理、銀行、年金 (Superannuation)、保険、金融市場インフラ、食料・食料品、病院、教育、貨物インフラ、貨物サービス、公共交通、液体燃料、エネルギー市場運営、港湾、電気、ガス、水道、空港

Source: Federal Register of Legislation "Security of Critical Infrastructure Act 2018", CISC Factsheet - Register of Critical Infrastructure Asset Guidance , CICS Factsheet" Cyber Security Incident Reporting Factsheet "、CISC Factsheet"Register of Critical Infrastructure Assets Guidance"

「重要インフラ安全保障法」詳細 [4/19]：対象分野 (詳細) [1/8]

対象分野	重要インフラ資産の分類	定義 / 重要インフラ資産の該当要件 (概要)
① **通信** *(Communications)* 	放送 *Broadcasting*	• 重要な放送送信設備として定める場所に位置し、同一事業者により所有または運営される放送送信資産 • 少なくとも50の異なる施設を保有し、同一事業体により所有または運営される放送送信資産 (放送再送信資産 (broadcasting re-transmission asset)でないもの) • 放送サービスの送信に不可欠な事業体により所有または運営される放送送信資産
	ドメインネーム *Domain Name Systems*	• オーストラリア政府のドメインネームシステムの管理にとって重要な事業体によって管理されている資産 • オーストラリア政府のドメインネームシステムの管理に関連して使用される資産 • オーストラリアのドメインネームシステムの管理にとって重要な資産 - 例えば、以下の管理を実施する事業者 - 登録データベース - WHOISサービス - .au に関するトップレベルのDNSネームサーバ - 次に掲げるDNSネームサーバー (-.com.au -.asn.au -.edu.au -.net.au -id.au -.gov.au)
	電気通信 *Telecommunications*	• 以下の資産のうち、通信事業者によって保有され通信事業に使用されるもの - 誘導/非誘導電磁エネルギーによって通信を行う、または行うことができるシステム - 電気通信ネットワークとその関連に使用される線・機器・装置・タワー・マスト・アンテナ・トンネル・ダクト・穴・ピット・ポールその他の構造物もしくは物

Note: 重要インフラ資産についてのガイダンス公表時点 (2023年4月) の情報
Source: Security of Critical Infrastructure Act 2018 , Critical Infrastructure Asset Class Definition Guidance

「重要インフラ安全保障法」詳細 [5/19]：対象分野 (詳細) [2/8]

対象分野	重要インフラ資産の分類	定義 / 重要インフラ資産の該当要件 (概要)
② **データ保管・処理** *(Data Storage or Processing Sector)* 	データ保管・処理 *Data Storage or Processing Sector*	• データ保管又は処理プロバイダーである事業体によって所有又は運営されている資産のうち、事業上重要なデータに関連するデータ保管または処理サービスを提供しエンドユーザーに提供するために、全部または主として使用される資産 • 事業上重要なデータとは以下を指す - 少なくとも20,000人の個人に関する個人情報 - 重要インフラ資産に関する研究開発に関する情報 - 重要インフラ資産の運用に必要なシステムに関する情報 - 重要インフラ資産のリスク管理および事業継続に関する情報

Note: 重要インフラ資産についてのガイダンス公表時点 (2023年4月) の情報
Source: Security of Critical Infrastructure Act 2018 , Critical Infrastructure Asset Class Definition Guidance

「重要インフラ安全保障法」詳細 [6/19]：対象分野 (詳細) [3/8]

対象分野	重要インフラ資産の分類	定義 / 重要インフラ資産の該当要件 (概要)
❸ **金融・証券** *(Financial Services and Markets)*	銀行 *Banking*	• 金融サービス・市場部門の安全性と信頼性に不可欠な公認預金受入機関である法人によって、所有または運営され、銀行事業に関連するもの - 500億ドル以上の資産を有する場合、安全性と信頼性に不可欠な公認預金受入機関とみなされる
	金融市場インフラ *Financial Market Infrastructure*	• オーストラリアの市場ライセンスを保有するオーストラリアの法人またはその関連事業体によって所有または運営されているもの • オーストラリアの清算・決済施設ライセンスを保有するオーストラリアの法人またはその関連事業体によって所有または運営されているもの • ベンチマーク管理者ライセンスを保有するオーストラリア法人またはその関連事業体によって所有または運営されているもの • オーストラリアのデリバティブ取引リポジトリ・ライセンスを保有するオーストラリア法人またその関連会社によって所有または運営されているもの • 金融サービスおよび市場部門の安全性と信頼性に不可欠な決済システムの運営に関連して使用されているもの
	保険 *Insurance*	• 保険事業を営む事業体またはその関連事業体によって所有または運営されているもの • 生命保険事業を営む事業体またはその関連事業体が所有または運営しているもの • 健康保険事業を営む事業体またはその関連事業体によって所有または運営されているもの
	年金制度 *Superannuation*	• Registerable Superannuation Entity (RSE) のライセンシーによって所有または運営され、200億ドル以上の資産を保有し、年金制度の運営関連で使用されているもの

Note: 重要インフラ資産についてのガイダンス公表時点 (2023年4月) の情報
Source: Security of Critical Infrastructure Act 2018 , Critical Infrastructure Asset Class Definition Guidance

「重要インフラ安全保障法」詳細 [7/19]：対象分野 (詳細) [4/8]

対象分野	重要インフラ資産の分類	定義 / 重要インフラ資産の該当要件 (概要)
④ **水道・下水** *(Water and Sewarage)*	水道 *Water*	• 単一の水道事業者が管理する1つまたは複数の上下水道システムまたはネットワークのうち、最終的に少なくとも10万の水道/下水道接続にサービスを提供するもの
⑤ **エネルギー** *(Energy)*	電気 *Electricity*	• 最終的に少なくとも10万以上の需要家または規則が定めるその他の需要家に供給するための、送電または配電のためのネットワーク、システム、または相互接続設備 • 州または準州の電力ネットワークまたは電力系統の安全性と信頼性を確保するために重要な発電所のうち、以下に該当するもの - 州または準州の発電事業者のうち、設置要領が30メガワット以上であり卸電力市場に接続されているもの - 州または準州においてシステム再稼働付帯サービスの提供を契約している事業者が所有または運営するもの
	市場運営 *Energy Market Operator*	• エネルギー市場運営会社 (AEMO)・電力水道会社・地域電力会社・電力会社に所有または運用されている資産のうち、以下の全てに該当するもの - エネルギー市場またはシステムの運営に関連して使用されている - エネルギー市場やシステムの安全性と信頼性を確保するために不可欠である - 重要な電力資産、重要なガス資産、または重要な液体燃料資産に該当しない

Note: 重要インフラ資産についてのガイダンス公表時点 (2023年4月) の情報
Source: Security of Critical Infrastructure Act 2018 , Critical Infrastructure Asset Class Definition Guidance

「重要インフラ安全保障法」詳細 [8/19]：対象分野 (詳細) [5/8]

対象分野	重要インフラ資産の分類	定義 / 重要インフラ資産の該当要件 (概要)
❺ **エネルギー (続き)** *(Energy)*	ガス *Gas*	• 1日当たりの最大取出容量が75 テラジュール以上のガス貯蔵施設、または規則で定められるその他の1日当たりの最大取出容量を有するガス貯蔵施設 • 1日あたり300テラジュール以上の処理能力、または規則が定めるその他の処理能力を有するガス処理施設 • 少なくとも10万件の需要家に、またはその他の規則で定める需要家に供給するガスの配給のためのネットワークまたはシステム • 重要なガス輸送パイプラインを運転するために必要な制御室やその他の資産 • ガス市場の安全性と信頼性を確保するために重要なガス輸送パイプライン – ガス送電パイプラインは、下記以上の規模であれば重要： - 東部: 200 TJ/日- 北部：80 TJ/日- 西部：150 TJ/日 – タスマニア・ガス・パイプラインとカーペンタリア・ガス・パイプラインは重要ガス資産に該当
	液体燃料 *Liquid Fuel*	• 液体燃料市場の安全性と信頼性に不可欠な液体燃料精製所 – ビクトリア州コリオとクイーンズランド州リットンにある液体燃料精製所は、重要な液体燃料精製所に該当 • 50メガリットル以上の液体燃料を貯蔵できる液体燃料貯蔵施設 • 液体燃料市場の安全性と信頼性を確保するために重要な液体燃料パイプライン – シドニー・メトロポリタン・パイプライン、ゴアベイ・パイプライン、ウェスタンポート・アルトナ・ジーロング・パイプライン、ロングフォード～ヘイスティングス パイプライン、メルボルン空港ジェット燃料パイプライン、ジェット燃料パイプライン (カーネル～シドニー空港) 、ブリスベン空港ジェット燃料パイプライン、 パース空港ジェット燃料パイプラインが該当

Note: 重要インフラ資産についてのガイダンス公表時点 (2023年4月) の情報
Source: Security of Critical Infrastructure Act 2018, Critical Infrastructure Asset Class Definition Guidance

「重要インフラ安全保障法」詳細 [9/19]： 対象分野 (詳細) [6/8]

対象分野	重要インフラ資産の分類	定義 / 重要インフラ資産の該当要件 (概要)
⑥ ヘルスケア・医療 *(Healthcare and Medical)*	病院 *Hospital*	• 一般集中治療室(ICU)を有する病院 ※ 一般集中治療室（ICU）とは、数日間の機械的人工呼吸と侵襲的心血管系モニタリングが可能な設備と人員を備え、以下のような支援を受けることができる病院内の区域をいう： • 通常の勤務時間中-少なくとも1名の集中治療専門の専門医または顧問医が、その区域に即座に配置され、専属で勤務していること • 常時-病院に常駐し、その領域で即座に対応可能な開業医が少なくとも1人いること • 毎日少なくとも18時間、少なくとも1人の看護師がいること • 入退院方針が運用されていること
⑦ 高等教育・研究 *(Higher Education and Research)*	教育 *Education*	• 全国高等教育機関登録簿 (National Register of Higher Education Providers) のオーストラリアの大学カテゴリーに登録されている団体によって所有または運営されているもののうち、以下のいずれかに該当するもの - (高等教育・研究以外の) 重要インフラ部門にとって重要な研究プログラムの実施に関連して使用されているもの - オーストラリアの防衛に不可欠な研究プログラムの実施に関連して使用されているもの - オーストラリアの国家安全保障に不可欠な研究プログラムの実施に関連して使用されているもの

Note: 重要インフラ資産についてのガイダンス公表時点 (2023年4月) の情報
Source: Security of Critical Infrastructure Act 2018 , Critical Infrastructure Asset Class Definition Guidance

「重要インフラ安全保障法」詳細 [10/19]：対象分野 (詳細) [7/8]

対象分野	重要インフラ資産の分類	定義 / 重要インフラ資産の該当要件 (概要)
⑧ **食料・食料品** *(Food and Grocery)* 	食料・食料品 *Food and Grocery*	• 必要不可欠な食料・食料品の流通又は供給に使用されるネットワークのうち、以下のいずれかの主体により運用されるもの - 重要なスーパーマーケット小売業者 (Aldi Pty Ltd、Coles Group Ltd、Woolworths Group Ltdが該当) - 重要な食料品卸売 (Metcash Trading Ltdが該当) - 重要な食品卸売業者
⑨ **交通** *(Transport Sector)* 	航空 *Aviation*	• 航空サービスの提供に関して使用されているもののうち、以下のいずれかに該当するもの - 航空機運航会社が所有または運営しているもの - 空港運営会社が空港の運営に関連して使用しているもの - 2004年航空運送安全法第44条C上に基づく規制航空貨物代理店によって所有または運営されているもの
	貨物インフラ *Freight Infrastructure*	• 州・準州等の間の物品輸送の重要な通路として機能する道路網・鉄道網・複合一貫輸送施設
	貨物サービス *Freight Services*	• 次のいずれかまたはすべてによる物品の輸送に不可欠な事業を営む企業が使用するネットワークのうち、年間収益が少なくとも1.5億ドルであり、道路・鉄道・水上等の貨物サービスを提供しており、以下のいずれかの運送・保管を実施すること - 食料品の輸送が重要インフラに該当するもの、液体燃料　等

Note: 重要インフラ資産についてのガイダンスが出された2023年4月時点
Source: Security of Critical Infrastructure Act 2018 、Critical Infrastructure Asset Class Definition Guidance

「重要インフラ安全保障法」詳細 [11/19]：対象分野 (詳細) [8/8]

対象分野	重要インフラ資産の分類	定義 / 重要インフラ資産の該当要件 (概要)
9 交通 [続き] *(Transport)* 	港 *Port*	• オーストラリア指定の安全保障上の規制対象の港湾の一部を構成する土地： – Broome Port, Port Adelaide, Port of Brisbane 等
	公共交通機関 *Public Transport*	• 単一事業体によって管理され、1ヶ月あたり少なくとも500万人の旅客の移動を処理する能力がある公共交通網またはシステム (航空に該当するものは除く)
10 宇宙技術 *(Space Technology)* 	宇宙関連サービス *Space Related Services*	• 宇宙関連サービスの商業的提供を伴うオーストラリアの経済主体[1] – 宇宙物体に関する位置/航法/計時サービス・宇宙状況認識サービス・宇宙気象の監視及び予報・ 宇宙物体に関する通信/追跡/遠隔測定/制御・宇宙からのリモートセンシングによる地球観測・宇宙へのアクセスを容易にするサービス等
11 防衛 *(Defense Industry)* 	防衛 *Defense Industry*	• 契約に基づいて国防省またはオーストラリア国防軍に提供されている、または提供される予定のもののうち、重要な防衛能力で構成されている、またはそれを可能にするもの – 資材、技術、プラットフォーム、ネットワーク、システム、サービス

Note: 重要インフラ資産についてのガイダンス公表時点 (2023年4月) の情報　1. 法令上の「宇宙技術」としての定義のみ記載あり
Source: Security of Critical Infrastructure Act 2018 , Critical Infrastructure Asset Class Definition Guidance

「重要インフラ安全保障法」詳細 [12/19]：資産登録 [1/3]

事業者は、インフラ資産に関する運用の情報や利害に関する情報を登録/更新し、政府はこれを保管 (登録簿は非公開)

主体

- **責任主体 (responsible entity)[1]：**
  - **当該資産に関する運用情報**を提供する義務あり

  (注) 重要インフラ資産を保有・運用する主体

- **重要インフラ資産に関わる直接利害関係者 (direct interest holder) [1]：**
  - **利害及び支配に関する情報**を長官に提供しなければならない

  (注) 直接利害関係者 (direct interest holder)：
  - 関連会社とともにその資産の少なくとも10%の直接又は共同の持ち分を保有する場合
  - その資産に直接的または間接的に影響を与え、または支配する立場にある持分を保有している場合

情報提供

- 資産取得等の後、**6ヶ月以内**に資産の運用情報を提供する必要あり (提供の必要がある情報の内容は後述)
- また、**継続的に情報提供が必要**
  - 運用情報が不正確/不完全になった場合、資産の報告主体が変更された場合は、更新情報を提供
  - これらの更新は、事象発生から30日以内に行わなければならない

(情報提供が必要となる例)
- 連絡先の変更、報告主体の変更、オペレータ又はデータに係る取決 (arrangement) の変更

政府機関の対応

- **内務次官 (Secretary) は、重要インフラ資産に関する情報を記載した、重要インフラ資産登録簿を保管**
  - 登録簿は非公開[2]

1. 一つの事業者が両方に該当する場合もあり得る 2. 重要インフラ安全保障法における資産の登録件数等は、報告書で公開されている (下記Annual Report参照)
Source: Security of Critical Infrastructure Act 2018, Department of Home Affairs 2021-22 Annual Report

「重要インフラ安全保障法」詳細 [13/19]：資産登録 [2/3]

「運用」に関する情報については、資産の所在地や事業体に関する情報を提供する必要がある

運用に関して登録が必要な情報

- 資産の**所在地**
- 当該資産が**サービスを提供する地域**
- **事業体に関する情報**：
  - 事業体の名称
  - その事業体の ABN[1]
    (その事業体がオーストラリア国外で設立された場合は、その他の類似の事業体番号)
  - 事業体の本社、又は主たる事業所の住所；
  - 事業体が法人化/設立/設立された国
- 資産に責任を負う**事業体の経営責任者**に関する情報
  - 役員のフルネーム
  - 当該役員が国籍を有する国又は地域
- 各事業者が**資産または資産の一部を運用する際の取決め**の説明
- 当該資産に関する**規則で定めるデータが維持されている取決**の説明 等

次頁にて詳細記載

1. Australian Business Number
Source: Security of Critical Infrastructure Act 2018

「重要インフラ安全保障法」詳細 [14/19]：資産登録 [3/3]

説明事項の具体的な内容については、ガイダンス上で明示されている

「各事業者が資産または資産の一部を運用する際の取決め」の詳細

- 責任主体がその資産の独占的な運営者である場合は、その旨を記述
- 他の事業体がその資産、またはその資産の異なる部分の運営に関与している場合は、それぞれの運営者について以下の情報を提供
  - 事業体名
  - ABN（または国際的に同等のもの）
  - 事業体の本社または主たる事業所の住所
  - 事業体が運用する資産の部分
  - 事業者が提供する役割または機能
  - 資産の各運営者との取り決めの説明
- 運営者とは、重要インフラ資産の日常的な運営について、ある程度の運営管理を行う立場にある事業体または個人
  - 責任主体から、資産または資産の一部を独立して運用する権限を与えられている
  - アセットがその機能を確実に果たすことに直接貢献する

「当該資産に関する規則で定めるデータが維持されている取決め」の詳細

- 責任主体は、指定された種類のデータを管理する第三者との取り決めに関連して情報を提供することが求められる
  - 第三者とは、責任主体以外の事業体であり、資産に代わってデータの保存や処理を請け負うデータセンターやクラウドサービスプロバイダを含む
- データが極めて重要であり、スパイ行為や妨害行為に利用される可能性があることから、この義務によりデータ関連の外部委託の取決めが可視化
- 取決めについて提供する必要のある情報には以下が含まれる
  - データを管理する事業体に関する以下の情報
    - 名前
    - ABN（または国際的に同等のもの）
    - 事業体の本社または主たる事業所の住所
    - 事業体が設立された国
  - データが保管されている住所（可能な限り、データを保管するサーバーのコンピュータの所在地の住所を含む）
  - クラウドサービスの一部であるかどうか
    - クラウドサービスを利用して保有されるデータについては、クラウドサービスの名称
    - 事業体が保持するデータの種類

Source: Register of Critical Infrastructure Assets Guidance

「重要インフラ安全保障法」詳細 [15/19]：リスク管理プログラム

事業体は、重要インフラリスク管理プログラム (CIRMP[1]) を策定し、これを遵守する必要あり (免除される場合もあり)

目的/内容

- ハザードの発生が資産に影響を及ぼす重大なリスクがある場合、**各ハザードを特定**

  (「重要なリスク」は、下位規則において下記のとおり規定)
  - コントロールできない長さの期間における、重要インフラ資産の機能停止・大幅な低下
  - 重要インフラ資産の重要な構成要素への実質的なアクセス不能、または意図的もしくは偶発的な操作
  - 情報資産の運用技術または情報資産の機能に不可欠な情報通信技術への干渉
  - オーストラリア国外における業務上の機密情報の保管、送信または処理 (レイアウト図等、機密情報 等)
  - 情報資産の運用管理システムまたは運用監視システムへのリモートアクセス
- 合理的に実行可能な限りにおいて、そのようなハザードが発生する**重大なリスクを最小化または排除**
- 合理的に実行可能である限りにおいて、**ハザードが資産に及ぼす関連する影響を軽減**

CIRMPのプロセス

- **責任主体は、自身のCIRMPにおいてプロセス/システムを確立し、これを維持する必要あり**
  - 情報資産の運用状況の特定
  - 重要インフラ資産に対する重要なリスクの特定
  - 合理的に実行可能な限りにおいて、
    - (i) 重要なリスクを最小化または排除
    - (ii) 各ハザードが 重要インフラ資産に与える影響の緩和
  - CIRMPの見直し/最新の状態の維持
- **年次報告書の作成義務あり。責任主体に運営機関がある場合は、年次報告書はその承認を得る必要あり**

1. Critical Infrastructure Risk Management Program：重要インフラ事業者のうち対象の責任主体に対し、ハザードの発生が資産に影響を及ぼす重大なリスクがある場合の各ハザードの特定や、合理的な実行可能な範囲におけるそのハザードが発生する重要なリスクの最小化や排除、関連する影響の権限を求めるもの

Source: Security of Critical Infrastructure Act 2018, Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023、CISC Fact Sheet – Risk Management Program

(参考) リスク管理プログラムによる義務

対象事業者は13資産の責任主体であり、CIRMPの策定と規則の遵守、報告書の提出や継続的な見直しが求められる

対象

重要インフラにて、以下の資産に該当する13資産の
責任主体に適用

- 放送
- ドメインネーム
- データ保管・処理
- 金融市場インフラ
- 水道
- 電気
- 市場運営
- ガス
- 液体燃料
- ヘルスケア・医療
- 食料・食料品
- 貨物インフラ
- 貨物サービス

重要インフラリスク管理プログラム (CIRMP) の義務

対象事業者は以下の3つを実施することが求められる

1. CIRMPの策定と規則の遵守

- 重要インフラ資産に適用されるハザード、重大なリスクの特定
- 資産への影響の検討
- リスクの軽減や排除の実施/活動の検討

2. CISCへの年次報告書の提出

- 取締役会等で承認された年次報告書を会計年度終了後90日以内に規制当局に提出
- サンプルの審査を受けることも可能

3. 継続的義務

- CIRMPの維持、定期的な見直し

なお、CIRMPには定められた書式はなく、また、既存のリスク管理プロセスにとって代わることを意図しているわけではない
むしろ、**対象となる責任主体は、既存のリスク管理の枠組みやプロセスをCIRMPに組み込むことが期待されている**

Source: CISC Fact Sheet – Risk Management Program 、Guidance for the Critical Infrastructure Risk Management Program

(参考) リスク管理プログラムによる義務 [1/2]：CIRMPの策定と規則の遵守

CIRMPの策定と規則の遵守では、重要なリスクを特定し、最小限に抑えることができるような対策検討が求められる

CIRMPの策定と規則の遵守

事業者は以下を通じて、CIRMPプロセスまたはシステムを確立し、維持することが義務付けられている

- 資産の運用状況を確認する
- 資産に対する重大なリスクの特定
- 合理的に実行可能な限りで重大なリスクを最小化/排除する
- 合理的に実行な限りでハザードに関連する影響を緩和する
- CIRMPを見直し常に最新の常態に保つ

また、「**合理的に実行な限りでハザードに関連する影響を緩和する**」ために、以下が求められている

- 合理的に実行可能な範囲で、CIRMPにプロセスまたはシステムを確立し、維持する
  - **サイバーおよび情報セキュリティ上の危険が発生するリスクを最小化・排除する**
  - **サイバー/セキュリティ・ハザードが重要インフラ資産に及ぼす影響を軽減する**
- 12か月の猶予期間 (2024年8月18日) までに、**CIRMPのフレームワークまたは規則第8条第4項に規定される同等のフレームワークに準拠**する

事業者が遵守すべきフレームワーク

事業者はハザードに関連する影響緩和のために、以下のフレームワークを遵守することが求められる

例) サイバーセキュリティ関連

- オーストラリア規格AS ISO.IEC 27001:2015
- オーストラリア通信局「Essential Eight Maturity Model」
  - 成熟度レベル1を満たすことが必要
- NIST「Framework for Improving Critical Infrastructure Cybersecurity」
- 米国エネルギー省「Cybersecurity Capability Maturity Model」
  - 成熟度レベル1を満たすことが必要
- 豪州エネルギー市場運営会社「The 2020-21 AESCSF Framework Core」
  - セキュリティ・プロファイル1を満たすことが必要

Source: CISC Fact Sheet – Risk Management Program , Guidance for the Critical Infrastructure Risk Management Program

(参考) リスク管理プログラムによる義務 [2/2]：年次報告書の提出

CISCへの年次報告書の提出においては、年次報告書においてCIRMPが適切に実施されたことを記載することを義務化

年次報告書の内容

年次報告書において以下の内容を記載する (重要インフラ法第30AG条)

- 会計年度末においてCIRMPが最新であったか否かの記載
- 会計年度中に重要インフラ資産に重大な影響を及ぼすハザードが発生した場合には以下を記載
  - ハザードの内容 (現在解消しているのか否か)
  - CIRMPがハザードの緩和のために有効であったか否か
  - ハザードが発生した結果、年度内にCIRMPの変更を行ったか否か、その内容は何か
- 責任主体が理事会/取締役会等を有する場合、年次報告書がその承認を受けたか

ただし、**年次報告書にCIRMPそのものを記載する必要はない**
また、プログラムが最新かつ適切であることを保証しなければならない

事業者による政府への自主的な事前審査

CIRMP に基づく年次報告書について、事業者に提出義務はあるが、**現時点ではまだ提出期限を迎えてはいない**

- 2023年2月17日に施行済
- 2024年8月18 日までに、 CIRMPで特定されたサイバーセキュリティフレームワークに準拠し、報告書を提出する必要がある

一方で、希望する事業者は、**自主的にCIRMPに基づく年次報告書の提出が可能**であり、**政府側で確認を行っている**

- 2023年9月22日の時点で、CISCは27件の年次報告書を受領
- これらのレポートでは、102の重要なインフラストラクチャ資産がカバー
- このうち4件の報告書において、実際に重要なインフラ資産が重大なハザードに見舞われたことの記載があった

Source: CISC Fact Sheet – Risk Management Program , Guidance for the Critical Infrastructure Risk Management Program, CIRMP voluntary annual report update, Regulatory obligations

「重要インフラ安全保障法」詳細 [16/19]：政府による指示/情報収集

大臣は、重要インフラ資産の運用又はこれによるサービスの提供に関して、安全保障を害する行為または不作為のリスクがある場合、指示を出すことが可能

指示の概要

- **内務大臣**は、重要インフラ資産の責任主体に対し、**当該主体が指定された期間内**に特定の行為または事項を行うこと、または行わないことを**要求する指示**を与えることができる
- 以下の場合を除き、指示を与えてはならない：
  - 事業体に対して特定の行為または事柄を行うこと、または行わないことを要求することが、安全保障上のリスクを排除または低減することに関連する目的のため、**合理的に必要である**こと
  - 指示が行われることなくリスクを排除または低減する結果を達成するために、当該事業者と**誠実に交渉するための合理的な措置**が取られていること
  - 当該事業体について、**安全性について不利な評価**がなされていること
  - 既存の規制制度が、リスクを排除または低減するため、**代わりに使用され得ない**と認識していること
- 大臣は指示を与える前に、**関係する大臣等と協議**を行わなければならない

考慮事項

- 当該事業体についての、**安全性についての不利な評価[1]の内容 [これが最も重視される]**
- 当該事業体が、その指示に従うことによって発生する可能性のある費用
- 当該指示が、関連する重要インフラ部門における競争に及ぼす可能性のある影響
- 当該指示が当該事業体の顧客又は当該事業体が提供するサービスに及ぼす可能性のある影響
- 指定された期間内に、事業体または諮問を受けた大臣が行った意見表明

※ その他、必要な場合は、政府が情報収集できる権限も規定

1. Australian Security Intelligence Organization Actにおいて、「ある者に関する安全性の評価であって、その者の利益を害する/害する恐れのある情報等や、その者に対して特定の行政措置を講じる/講じることを勧告すべきもののうち、その実施によりその者の利害が害されるもの」と定義

Source: Security of Critical Infrastructure Act 2018

「重要インフラ安全保障法」詳細 [17/19]：インシデントの通知の義務

事業体は、サイバーセキュリティのインシデントが発生した場合、ASD/ACSC[1]に通知の義務あり

[重大なサイバーセキュリティインシデントの場合]

- **重大なインシデント**が発生した、又は発生しつつあり、かつそのインシデントが**資産の可用性に重大な影響**を与えた、または与えつつあることを認識した場合、インシデントを認識してから**12時間以内にACSC[1] に通知義務あり**
  - **重大な影響**とは、重要なインフラ資産が必要不可欠な商品やサービスの提供に関連して使用されており、インシデントがそれらの必要不可欠な商品やサービスの利用可能性を著しく中断させる場合を指す
  - 口頭で報告する場合は、ACSCに通知してから84時間以内に、書面でも通知の義務あり

[その他のサイバーセキュリティインシデントの場合]

- **インシデントが発生した**、または発生していることを認識した場合、かつインシデントが資産に**関連する影響**を与えた、与えている、または与える可能性がある場合、認識後、**72時間以内にACSCに通知の義務あり**
  - **関連する影響**とは、資産またはシステムの完全性、信頼性、または機密性への影響のこと
  - 口頭で報告する場合は、ACSCに通知してから48時間以内に、書面でも通知の義務あり

1. ASD：Australian Signal Directorate (豪州通信情報局), ACSC：Australian Cyber Security Centre。ASDは、情報収集、サイバーセキュリティ、攻撃的サイバー作戦等を実施

Source: Security of Critical Infrastructure Act 2018, Report a cyber security incident | Cyber.gov.au, 国立国会図書館ウェブサイト（「オーストラリア連邦議会による情報機関の監視」）

「重要インフラ安全保障法」詳細 [18/19]：インシデント時の政府の対応

インシデント発生時、政府は、情報提供や命令等、必要な対応を行うことも可能

インシデント発生時の対応

情報提供命令
Information-gathering

- インシデントが発生した場合、当該資産に関する**情報**を指定期間内に**提供**することを命令できる
  - 但し、電気通信法で禁じられている行為を伴う情報提供は指示してはならない

対応命令
Action Direction

- 当該責任事業体がインシデントに対する合理的な対応を講じる意志・手段がない場合、責任事業体に対して、指定された期間内に特定の対応を取るよう**命令**できる

介入要請
Intervention Request

- 上記の対応命令 (Action Direction) がインシデントに対して十分な効果を持たず、責任事業体が合理的な対応を取る意思又は手段を持たない場合、他の政府機関に対し、**介入**することを要請できる

具体的な内容

- コンピュータ及び周辺機器へのアクセス・改変
- コンピュータ本体・データ・プログラム及び周辺機器の解析
- 対象のコンピュータへの特定のプログラムのインストール
- コンピュータ及び周辺機器に格納されているデータ・プログラムへのアクセス・追加・復元・複製・変更・削除
- コンピュータ及び周辺機器の機能変更
- コンピュータ及び周辺機器の対象資産群からの切断、除却または接続
- コンピュータ及び周辺機器の敷地からの除却

Source: Security of Critical Infrastructure Act 2018

「重要インフラ安全保障法」詳細 [19/19]：セキュリティ強化義務

内務大臣が特定の資産を、「国家的に重要なシステム」(Systems of National Significance) として非公開で指定し、サイバーセキュリティを強化する義務を課すことも可能

国家的に重要なシステムの指定

- 内務大臣は、以下を満たす場合、特定の資産を「**国家的に重要なシステム**」(**Systems of National Significance: SoNS**) と、**書面で非公開で指定** (**Privately Declare**) できる
  - 当該資産が、国家安全保障に影響する重要インフラであること
  - 当該資産が、国家安全保障に影響する重要インフラであることが公に知られた場合、国家安全保障にリスクがあること
- 内務大臣は、指定後30日以内に、**当該資産の責任主体等に、指定の事実を通知**しなければならない。
  ※ 当該資産が指定されたことの公表は、法律で罰せられる行為に該当

指定された資産のセキュリティ強化義務

- SoNSの責任主体等は、下記のとおり、**サイバーセキュリティ強化の義務あり** (下記のうち、状況に応じ必要なもののみを要求)

インシデント対応計画策定の義務	SoNS の責任事業体等は、SoNS に影響を与える可能性のあるインシデントへの対応計画を策定・維持し、更に当該計画の遵守・定期的見直し・更新の義務を負う
サイバーセキュリティ演習の実施	内務次官は、書面による通知により、SoNS 及び 1 種類以上のインシデントに関してサイバーセキュリティ訓練(以下「訓練」)を実施するよう要求できる • 訓練は、インシデントへの適切な対応能力、準備態勢、SoNS への影響を軽減する能力のテストを目的
脆弱性アセスメントの実施	内務次官は、責任事業体等に、インシデントに対するSoNSの脆弱性を評価するため、脆弱性評価の実施を要求できる • 責任事業体等は、評価後 30 日以内に報告書を作成し、提出の必要あり

※ コンピュータが国家的に重要なシステムである場合、または国家的に重要なシステムを運用するために必要な場合、システムの関連組織は、ASDへのシステム情報の定期的な報告/レポート/システム情報を送信するソフトウェアのインストールを要求される場合がある

Source: Security of Critical Infrastructure Act 2018

(参考) Cyber and Infrastructure Security Centre：CISC の概要

CISCは、重要インフラの所有者/運営者がリスクを理解し、規制要件を満たせるよう支援する、内務省の組織

長官	• Jim Anderson（2023年8月就任）
設立時期	• 2021年9月1日
背景/目的	• 下記を目的に、内務省[1] (Department of Home Affairs) に設置 – オーストラリアの重要インフラの安全性・継続性・強靭性を共同で確保 – オーストラリアの所有者と事業者がベストプラクティスの基準を満たし、重要インフラの強靭性を向上させるため、以下の取組を実施： – エンゲージメント・パートナーシップ・助言・演習・モデリング・規制
主な活動内容	• ハザード/リスク/脅威/脆弱性/機会を特定・対応 • 基準・認定・規制改革をサポート • オーストラリアの政府関連機関等の身元調査 • 重要インフラの継続的な提供を損なう可能性のある危機に備えるための支援 • 革新的な規制とコンプライアンス：セキュリティ・リスクを共同で管理するために、産業界や政府と協力するための情報源・検証機関として存在

1. 内務省は、サイバーと重要インフラの強靭性と安全保障、出入国管理、国境警備と管理、テロ対策、主権保護、市民権と社会的結束、を主な役割とする
Source: Cyber and Infrastructure Security Centre (cisc.gov.au), Home Affairs: The Fourth Year, Who we are (homeaffairs.gov.au)

3-3.
オーストラリア

1. 政策の全体像

2. 制度の調査結果
   - 重要インフラ安全保障法 (1)
   - 電気通信法 (2017年改正) (2)

3. 事例

電気通信法におけるセキュリティ改革の概要 [1/2]：全体概要

電気通信法を改正するかたちで、電気通信セクターのセキュリティ強化のための改革 (TSSR) を導入

法令等の名称

電気通信法
Telecommunications Act 1997

※ 上記法令を、"the Telecommunications and Other Legislation Amendment Act 2017"にて改正し、"Telecommunications Sector Security Reforms" (TSSR) を実施

制定時期/主な改定の経緯

- 2017年9月 改正
- 2018年9月 TSSR関連部分施行

制定の経緯

- 電気通信ネットワークのセキュリティと強靭さは、国民の社会的・経済的厚生にとって不可欠である一方、サイバー侵入等、悪意ある行為による妨害の脅威が増大
- このため、通信事業者等に対し、無許可アクセス/妨害からネットワークを保護するために最善を尽くすよう求めるとともに、産業界と政府間の情報共有を正式化することを目的に設定

妨害防止措置の概要

- 電気通信セクターに対し、下記を導入するもの
  1. **安全保障上の義務を追加**[1]
     - 各事業者は、ネットワーク・設備が犯罪に利用されることを防止するために最善を尽くす (元々存在した他の義務に追加)
  2. **システムの変更の場合の通知** **[詳細後述]**
     - 上記義務を遵守する能力に影響を及ぼす可能性ある変更を政府に通知
  3. **政府による情報収集の権限の付与**
     - 安全保障上の観点から、政府による情報収集を可能とする
  4. **政府による指示等の権限の付与** **[詳細後述]**
     - 安全保障を害する可能性がある特定の状況において、事業者に対して指示を出すことが可能

対象分野

- 電気通信セクターに限定

1. 情報通信に関する独立した機関であるACMA (Australian Communications and Media Authority) も安全保障を目的とした義務を有している

Source: Telecommunications sector security (homeaffairs.gov.au), Telecommunications Sector Security Reforms come into force (homeaffairs.gov.au), Federal Register of Legislation "Telecommunications and Other Legislation Amendment Act 2017"

電気通信法におけるセキュリティ改革の概要 [2/2]：主な措置

② システムの変更の場合の通知

- 電気通信事業者等が、**電気通信サービス/システム**に対して**変更が実施**されることにより、**義務を遵守する能力に重大な悪影響を及ぼす可能性があることを認識**した場合、**事前に、CISC[1]を通じCAC[2]に通知する必要あり**
  - 拘束力のある契約締結前、事業計画/交渉の初期段階、計画時点等に実施
  - 悪影響とは、ネットワーク/施設を、無許可アクセス・干渉から保護するセキュリティ義務を遵守する能力への影響
    - 例：新たなサービスの提供、通信機器・ネットワーク管理機器の設置場所の変更 (国外への移動含む)・調達、アウトソーシング契約の締結、機密データ/情報へのアクセス又は管理レベルの変更、サービスの変更管理
    - 不要な場合の例：同クラスの機器の交換、ネットワークに接続されていない試験/試用でデータ保護が適用されている場合
- 30日以内にCACから、「追加情報の提供依頼」、「関連リスクの通知/議論」、「リスクなし」のいずれかの通知あり

④ 政府による指示等の権限の付与

- 内務大臣は、通信事業者等に、指示を与えることが可能 (指示権限は、「最後の手段」として意図されている)
  - 通信サービスの利用/提供が安全保障を害する場合
    - サービスの使用/供給の中止
    - 安全保障情報機構 (ASIO[3]) が当該事業者に対し、不利な安全保障評価を発していることが条件
  - ネットワーク/施設に関わる無許可の干渉/アクセスのリスクがあり、安全保障を害する場合
    - 通信事業者等に対し、特定の行為/事項を行う又は行わないよう指示を与えることが可能
    - ASIOによる不利なセキュリティ評価 (これを最も重視)、事業者が指示に従うコスト、業界の競争

  ※ 指示を与える前に、法令を管理する大臣と協議し、事業者に対して意見を述べる機会を提供する必要あり (サービスの使用/供給の中止の場合は、首相にも協議が必要)
- 加えて、政府が事業者の義務遵守に関する評価・安全保障のリスク評価にアクセスするため、事業者に情報/文書の提供を求めることも可能

1. Cyber and Infrastructure Security Centre：重要インフラの所有者/運営者がリスクを理解し、規制要件を満たせるよう支援する、内務省の組織, 2. Communications Access Co-ordinator：重要インフラ事業者の通知受領やそれに対する免除の実施等を行う内務省の組織　3. Australian Security Intelligence Organisation：オーストラリア及び同国国民を外国の干渉等から防護することを目的とした組織
Source: Telecommunications Sector Security Reforms come into force (homeaffairs.gov.au), Notification Requirement factsheet - CISC branding, TSSR Admin Guidelines (cisc.gov.au)

② 電気通信法に基づく通知義務

通信事業者等に対し、セキュリティに重大な悪影響を与える可能性のあるシステムの変更がある場合の通知を義務付け

事業者側のプロセス

重要な悪影響を与える可能性があるか否かを判定

以下に変更がある場合「重大な悪影響」を与える可能性が高いものと列挙
- リスクの高いベンダーの関与
- 新しいアクセス技術
- IPコア
- 仮想化インフラ、オーケストレータ、コントローラー
- セキュリティ関連/暗号
- 非雇用者への特権的なアクセス権の付与
- 通信機器の新規調達
- アウトソーシング契約の締結 等

通知を行わないことを決定した場合、その旨の記録の保持を行うことを推奨
- 質問がある場合CISCへ問い合わせ

CISC[1]との協議

変更を行う前に、CISCへ連絡を実施し確認をすることを推奨
- 具体的には、調達について決定する前、ベンダに情報要求書を発行したタイミングを推奨

上記の確認を行い、変更についての十分な情報と確実性が確保されたのちに、変更を実施し、CAC[2]へ通知書を出すことを推奨

通知後の対応

通知をCACへ提出したのちに、30日以内にCACからの以下の通知あり、内容に応じた対応が必要
- 追加情報の要求
  - 追加の情報提供を実施
- 関連するリスクの通知
  - 最善のリスク対応方法についてCACと議論
- リスクなし

1. Cyber and Infrastructure Security Centre：重要インフラの所有者/運営者がリスクを理解し、規制要件を満たせるよう支援する、内務省の組織, 2. Communications Access Co-ordinator：重要インフラ事業者の通知受領やそれに対する免除の実施等を行う内務省の組織
Source: TSSR Admin Guidelines (cisc.gov.au)

(参考) ACMAの概要 [1/2]

ACMAは、オーストラリアの通信およびメディアサービスを規制しているオーストラリア連邦の独立した機関

Australian Communications and Media Authority (ACMA)

- 業界のパフォーマンスを高めるための規制の維持・執行・改善・消費者保護
- 産業界が地域社会にサービスを提供できるよう、公的資源を管理

部門

5つの部門

Communications Infrastructure	Licensing & Infrastructure Safeguards
	Spectrum Allocations
	Spectrum Planning & Engineering
Consumer	Telecommunications Safeguards & Numbers
	Unsolicited Communications & Scams
Content	Content Safeguards
	Gambling & Mis/Disinformation
Corporate & Research	Digital & Technology Services
	Finance, Reporting & Operations
	Research, Data, Regulation & Governance
	Human Resources & Communications
Legal Service	

Source: ACMA HPより

(参考) ACMAの概要 [2/2]

会長	• Nerida O'Loughlin（2017年10月就任）
設立時期	• 2005年
背景/目的	• オーストラリアの通信インフラとコンテンツ・サービスがもたらす経済的・社会的利益の最大化に貢献するため、以下に取り組む - 業界の業績を促進するための規制の維持・執行・改善・消費者保護 - 産業界が地域社会にサービスを提供できるよう、公的資源を管理
主な活動内容	• 通信・メディアサービスおよび市場に関する規則の設定と管理 • オーストラリアで活動する人・組織・製品の認可 • 苦情・問題を調査し、規則が守られていない場合に措置を実施 • 電波を計画・管理し、5Gのような新しいサービスのためのスペースを確保

Source: ACMA HPより

3-3.
オーストラリア

1. 政策の全体像

2. 制度の調査結果
   - 重要インフラ安全保障法 (1)
   - 電気通信法 (2017年改正) (2)

3. 事例

政府による通信事業者に対するガイダンス [1/2]

オーストラリア政府から発出されたガイダンスにおいては、通信事業者への5Gネットワークでのリスク喚起と、TSSRに基づき、通信事業者にリスクからの保護の義務が課される旨の言及に留まり、特定の事業者に係る言及は無し

概要

名称
- GOVERNMENT PROVIDES 5G SECURITY GUIDANCE TO AUSTRALIAN CARRIERS

発出日
- 2018年8月23日

内容
- 政府として5G技術を保護する一方で、セキュリティリスク増大の可能性や現在の安全対策では不十分である旨を指摘
- あわせて、豪州法に抵触する外国政府からの指示を受ける可能性が高いベンダーの関与への危険性を指摘

記載内容詳細

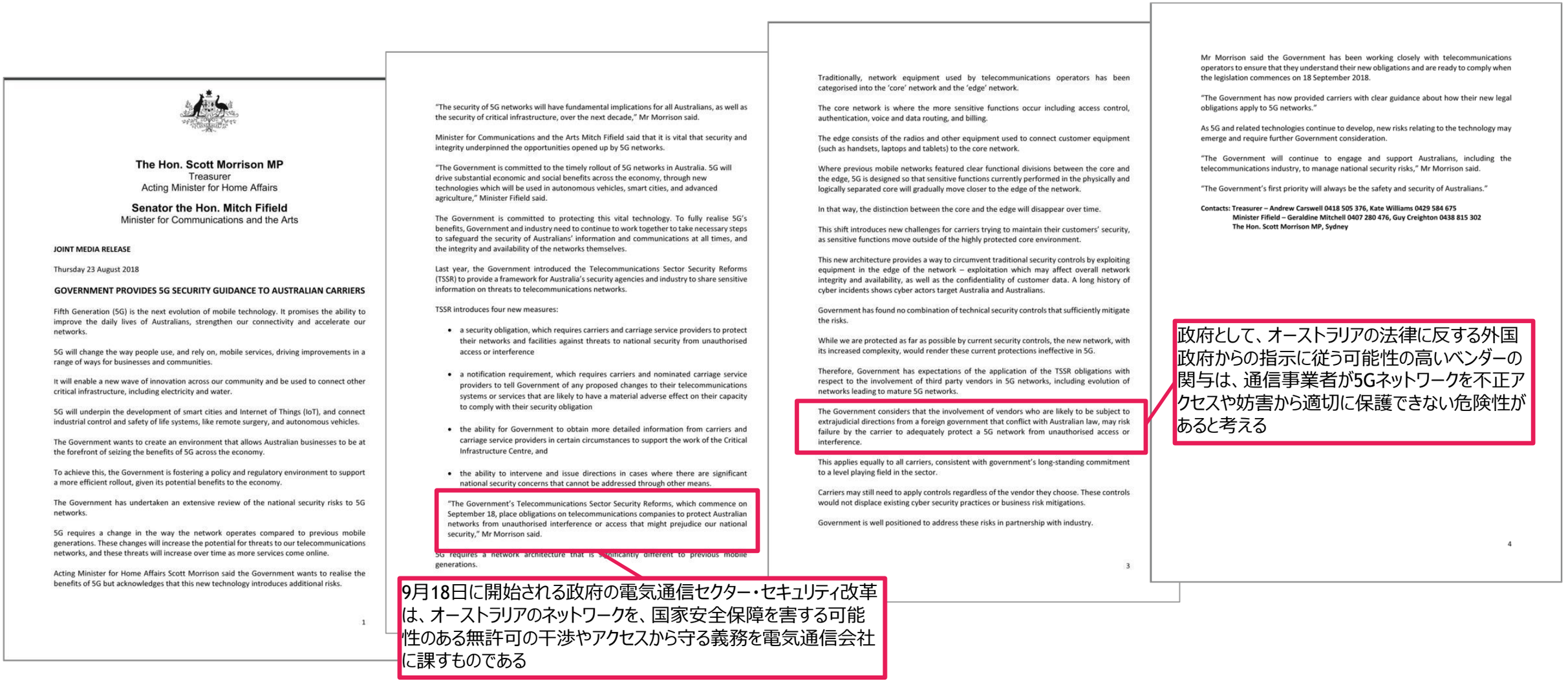
5Gネットワークを通じたセキュリティリスク増大の可能性とそれへの対策の必要性を指摘

(本文関連部分和訳 抜粋)
- 5Gではネットワークの運用方法が変わる。この変化は、通信ネットワークに対する脅威の可能性を増大させ、こうした脅威は、より多くのサービスがオンライン化されるにつれて、時間の経過とともに増加する
- 5Gの利点を完全に実現するためには、政府と産業界が協力して、オーストラリア国民の情報と通信のセキュリティを常に保護し、ネットワーク自体の完全性と可用性を守るために必要な措置を講じ続ける必要がある
- 9月18日から適用されるTSSRは、オーストラリアのネットワークに対し、国家安全保障を害する可能性のある無許可の干渉やアクセスから守る義務を通信事業者に課すもの
- 政府として、**オーストラリアの法律に反する外国政府からの指示に従う可能性の高いベンダーの関与は、通信事業者が5Gネットワークを不正アクセスや妨害から適切に保護できない危険性**があると考える

Source: GOVERNMENT PROVIDES 5G SECURITY GUIDANCE TO AUSTRALIAN CARRIERS

政府による通信事業者に対するガイダンス [2/2]

ガイダンスは4頁で、5Gネットワークを通じたセキュリティリスク増大の可能性とそれへの対策の必要性を指摘



The Hon. Scott Morrison MP
Treasurer
Acting Minister for Home Affairs

Senator the Hon. Mitch Fifield
Minister for Communications and the Arts

JOINT MEDIA RELEASE

Thursday 23 August 2018

GOVERNMENT PROVIDES 5G SECURITY GUIDANCE TO AUSTRALIAN CARRIERS

Fifth Generation (5G) is the next evolution of mobile technology. It promises the ability to improve the daily lives of Australians, strengthen our connectivity and accelerate our networks.

5G will change the way people use, and rely on, mobile services, driving improvements in a range of ways for businesses and communities.

It will enable a new wave of innovation across our community and be used to connect other critical infrastructure, including electricity and water.

5G will underpin the development of smart cities and Internet of Things (IoT), and connect industrial control and safety of life systems, like remote surgery, and autonomous vehicles.

The Government wants to create an environment that allows Australian businesses to be at the forefront of seizing the benefits of 5G across the economy.

To achieve this, the Government is fostering a policy and regulatory environment to support a more efficient rollout, given its potential benefits to the economy.

The Government has undertaken an extensive review of the national security risks to 5G networks.

5G requires a change in the way the network operates compared to previous mobile generations. These changes will increase the potential for threats to our telecommunications networks, and these threats will increase over time as more services come online.

Acting Minister for Home Affairs Scott Morrison said the Government wants to realise the benefits of 5G but acknowledges that this new technology introduces additional risks.

1

"The security of 5G networks will have fundamental implications for all Australians, as well as the security of critical infrastructure, over the next decade," Mr Morrison said.

Minister for Communications and the Arts Mitch Fifield said that it is vital that security and integrity underpinned the opportunities opened up by 5G networks.

"The Government is committed to the timely rollout of 5G networks in Australia. 5G will drive substantial economic and social benefits across the economy, through new technologies which will be used in autonomous vehicles, smart cities, and advanced agriculture," Minister Fifield said.

The Government is committed to protecting this vital technology. To fully realise 5G's benefits, Government and industry need to continue to work together to take necessary steps to safeguard the security of Australians' information and communications at all times, and the integrity and availability of the networks themselves.

Last year, the Government introduced the Telecommunications Sector Security Reforms (TSSR) to provide a framework for Australia's security agencies and industry to share sensitive information on threats to telecommunications networks.

TSSR introduces four new measures:

- a security obligation, which requires carriers and carriage service providers to protect their networks and facilities against threats to national security from unauthorised access or interference
- a notification requirement, which requires carriers and nominated carriage service providers to tell Government of any proposed changes to their telecommunications systems or services that are likely to have a material adverse effect on their capacity to comply with their security obligation
- the ability for Government to obtain more detailed information from carriers and carriage service providers in certain circumstances to support the work of the Critical Infrastructure Centre, and
- the ability to intervene and issue directions in cases where there are significant national security concerns that cannot be addressed through other means.

"The Government's Telecommunications Sector Security Reforms, which commence on September 18, place obligations on telecommunications companies to protect Australian networks from unauthorised interference or access that might prejudice our national security," Mr Morrison said.

5G requires a network architecture that is significantly different to previous mobile generations.

Traditionally, network equipment used by telecommunications operators has been categorised into the 'core' network and the 'edge' network.

The core network is where the more sensitive functions occur including access control, authentication, voice and data routing, and billing.

The edge consists of the radios and other equipment used to connect customer equipment (such as handsets, laptops and tablets) to the core network.

Where previous mobile networks featured clear functional divisions between the core and the edge, 5G is designed so that sensitive functions currently performed in the physically and logically separated core will gradually move closer to the edge of the network.

In that way, the distinction between the core and the edge will disappear over time.

This shift introduces new challenges for carriers trying to maintain their customers' security, as sensitive functions move outside of the highly protected core environment.

This new architecture provides a way to circumvent traditional security controls by exploiting equipment in the edge of the network – exploitation which may affect overall network integrity and availability, as well as the confidentiality of customer data. A long history of cyber incidents shows cyber actors target Australia and Australians.

Government has found no combination of technical security controls that sufficiently mitigate the risks.

While we are protected as far as possible by current security controls, the new network, with its increased complexity, would render these current protections ineffective in 5G.

Therefore, Government has expectations of the application of the TSSR obligations with respect to the involvement of third party vendors in 5G networks, including evolution of networks leading to mature 5G networks.

The Government considers that the involvement of vendors who are likely to be subject to extrajudicial directions from a foreign government that conflict with Australian law, may risk failure by the carrier to adequately protect a 5G network from unauthorised access or interference.

This applies equally to all carriers, consistent with government's long-standing commitment to a level playing field in the sector.

Carriers may still need to apply controls regardless of the vendor they choose. These controls would not displace existing cyber security practices or business risk mitigations.

Government is well positioned to address these risks in partnership with industry.

3

Mr Morrison said the Government has been working closely with telecommunications operators to ensure that they understand their new obligations and are ready to comply when the legislation commences on 18 September 2018.

"The Government has now provided carriers with clear guidance about how their new legal obligations apply to 5G networks."

As 5G and related technologies continue to develop, new risks relating to the technology may emerge and require further Government consideration.

"The Government will continue to engage and support Australians, including the telecommunications industry, to manage national security risks," Mr Morrison said.

"The Government's first priority will always be the safety and security of Australians."

Contacts: Treasurer – Andrew Carswell 0418 505 376, Kate Williams 0429 584 675
Minister Fifield – Geraldine Mitchell 0407 280 476, Guy Creighton 0438 815 302
The Hon. Scott Morrison MP, Sydney

4

9月18日に開始される政府の電気通信セクター・セキュリティ改革は、オーストラリアのネットワークを、国家安全保障を害する可能性のある無許可の干渉やアクセスから守る義務を電気通信会社に課すものである

政府として、オーストラリアの法律に反する外国政府からの指示に従う可能性の高いベンダーの関与は、通信事業者が5Gネットワークを不正アクセスや妨害から適切に保護できない危険性があると考える

Source: GOVERNMENT PROVIDES 5G SECURITY GUIDANCE TO AUSTRALIAN CARRIERS

HuaweiによるTSSRに関連する声明

HuaweiはHuaweiの使用禁止に対し、TSSRの見直しを求める声明を文書を議会に対して出している

文書概要

文書名
- Review of Part 14 of the Telecommunications Act 1997 – Telecommunications Sector Security Reforms

発出日
- 2020年11月27日

発出者
- Huawei Australia

内容詳細

HuaweiはTSSRに基づく5GへのHuawei機器の使用禁止がオーストラリアの5Gにおける競争力低下やコストの上昇につながっており、Huaweiの使用について安全上の問題がない旨を記載

(和訳を一部抜粋)
- TSSRはオーストラリアの世界的なモバイルネットワークのリーダーシップを破壊し、ベンダーの競争を低下させ、通信事業者と消費者間の価格を強制的に引き上げた
  - TSSRはHuaweiを始めとした中国企業の市場からの排除のツールになっている
  - その結果、オーストラリアでは1つのベンダーの独占状態となり、セキュリティ脆弱性やコストが増加している
  - ガイドライン上で述べられたテクノロジーに関する調査結果は誤っており、5Gの規制を管理する世界的な業界標準化団体によって完全に反論されている
- オーストラリア政府は全てのベンダーが独立したテストと検証を可能にするような政策を実施すべき
  - 5Gに接続されている機器は中国製であり、独立したテストや評価もない
  - Huaweiは何も隠すことをなく独立したテストを実施している

Source: Parliament of Australia, "Submissions received by the Committee", Submission 6. Huawei Australia

3-4. ドイツ

1. 政策の全体像

2. 制度の調査結果
   - ITセキュリティ法2.0 (1)
   - ITセキュリティ法3.0 (2)

3. 事例

3-4. ドイツ

1. 政策の全体像

2. 制度の調査結果
   - ITセキュリティ法2.0 (1)
   - ITセキュリティ法3.0 (2)

3. 事例

ドイツの基幹インフラ妨害行為の防止に係る政策の全体像

主な対象行為		主な対象者		
		国内企業		外国企業
		基幹インフラ事業者 (通信事業者を除く)	通信事業者	
取引規制	製品/役務の調達	① **ITセキュリティ法2.0** • 重要インフラ事業者による重要部品の配備を事前に審査 **主な制度 (詳細深掘り)**		
		② **ITセキュリティ法3.0 (EU NIS2指令の国内実施に向け、現在検討中)** • 対象範囲の拡大 等		
	対内直接投資			③ **対外経済法** • 分野特定的審査及び分野横断的審査により、対内直接投資を規制
サイバー攻撃への防護		① **ITセキュリティ法2.0** • 重要インフラ事業者/デジタルサービス提供者/特別な公益を有する企業等に、セキュリティに係る取組の状況の申告や、インシデントに関する報告を義務付け **主な制度 (詳細深掘り)**		
		② **ITセキュリティ法3.0 (EU NIS2指令の国内実施に向け、現在検討中)** • 対象範囲の拡大 等		

Note：上記分類は、本調査の目的から、関連が深いと考えられる法令を抽出し、主な目的/対象の相違等を強調するために整理をしたものであり、必ずしも上記各範囲の内容のみを含むとは限らない
特に、国内企業には、国内にて事業活動を行う外国企業も含まれうる

3-4. ドイツ

1. 政策の全体像

2. 制度の調査結果
   - ITセキュリティ法2.0 (1)
   - ITセキュリティ法3.0 (2)

3. 事例

「ITセキュリティ法2.0」概要 [1/2]

法令等の名称

- ITセキュリティ法2.0 (通称)
  (Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0))

制定時期

- 2020年12月16日　閣議決定
- 2021年4月23日　連邦議会で可決
- 2021年5月7日　連邦参議院(上院)で承認
- 2021年5月28日　施行

制定の経緯

- 2020年1月 **欧州委員会**が、各国に対し、5Gネットワークのサイバーセキュリティーリスクを評価しこれに基づいて必要な対策を**2020年4月末までに整備するよう呼び掛け**
- 2020年12月16日 ドイツ政府がITセキュリティ法2.0を閣議決定
- 2021年5月7日に連邦議会が承認し、同年5月28日に施行

主な妨害行為防止措置の概要

- **重要部品 (ソフトウェア、ITサービスを含む)**を新たに使用する重要インフラ事業者は、**重要部品を新たに使用する際、事前に政府から認可を得る**ことを義務化
- ドイツ国内の公序や公共の安全を損なう恐れがある場合は、**連邦内務・国土省は、使用を禁止することも可能に**

※ BSI[1]法等、関連する法令を改正するもの

対象者

以下に掲げる分野に属し、その障害や不全が重大な供給のボトルネックや公共の安全に脅威をもたらす、**重要インフラ事業者**

- **エネルギー、水、食品、情報技術・通信、医療、金融・保険、交通・運輸、自治体廃棄物処理**

1. 連邦情報セキュリティー庁 (Bundesamt für Sicherheit in der Informationstechnik)

Source: Bundesamt für Sicherheit in der Informationstechnik, "What are Critical Infrastructures?" , Bundesamt für Sicherheit in der Informationstechnik, "Second act on increasing the security of IT systems (German IT Security Act 2.0)"、 Bundesgesetzblatt, "Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme", Deutscher Bundestag, "Drucksache 19/26106", European Commission, "Secure 5G networks: Commission endorses EU toolbox and sets out next steps", Bundesministerium des Innern und für Heimat, "Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme" Bundesamt für Sicherheit in der Informationstechnik, "Gesetz über das Bundesamt für Sicherheit in der Informationstechnik"

「ITセキュリティ法2.0」概要 [2/2]

審査プロセス

届出の受理

- 重要インフラ事業者から、重要部品を使用する前に**設備の安全性を製造元が保証した宣言とともに連邦内務・国土省に届け出を提出**

関係省庁間の協議

- 関係省庁間で審査基準に抵触するかを協議
  - 連邦内務・国土省、外務省、経済・エネルギー省、財務省、国防省、交通・デジタルインフラ省、保健省等

最終判断

- 関係省庁間の協議結果を踏まえて、連邦内務・国土省が認可/否認
  - 当該部品の利用が**ドイツの安全保障政策上の利益に反すると認めるときは、当該部品の利用禁止を命ずる**ことができる

審査基準

主に以下3つの観点で審査

1. 製造者が第三国政府(その他の政府機関や軍隊を含む)に直接または間接的に支配されていること
2. 製造者が自国、EU、NATO等の加盟国・機関の公序良俗や治安に悪影響を及ぼす活動を行っていること
3. 重要部品の使用が、自国、EU、NATOの安全保障政策の目的に合致していること

罰則

違反した場合、内容に応じ、最大で200万/100万/50万ユーロ等の罰金が科される

Source: Bundesamt für Sicherheit in der Informationstechnik, "What are Critical Infrastructures?", Bundesamt für Sicherheit in der Informationstechnik, "Fragen und Antworten zu Bußgeldern (§ 14 BSIG)", Deutscher Bundestag, "Kleine Anfrage der Fraktion der CDU/CSU"

「ITセキュリティ法2.0」詳細 [1/9]：制定時期/経緯等

「ITセキュリティ法2.0」は、5Gネットワークにより増大するサイバーセキュリティーのリスクに対応するために制定された

法令等の名称	• Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0) – ITセキュリティ法2.0
制定時期	• 2021年1月 法案が連邦議会に提出 • 2021年4月23日 連邦議会で可決 • 2021年5月7日 連邦参議院(上院)で承認 • 2021年5月28日 施行
制定の経緯	• 2020年1月 欧州委員会が、5Gネットワークのサイバーセキュリティーリスクに対処するため、そのリスクを評価し、必要な対策を2020年4月末までに整備するよう呼びかけ (それに先立ち欧州理事会は、5Gのセキュリティに関する協調的アプローチの呼びかけ/2019年3月に勧告を実施) • 2020年12月16日 ドイツ政府がITセキュリティ法2.0を閣議決定 • 2021年4月23日 連邦議会で可決 (審議過程で政府原案に対し一部修正。重要部品の使用届出について使用を禁ずる場合の判断の基準の追加 等) • 2021年5月7日 連邦参議院 (上院) で承認 • 2021年5月28日 施行

Source: Bundesgesetzblatt, "Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme", Deutscher Bundestag, "Drucksache 19/26106", European Commission, "Secure 5G networks: Commission endorses EU toolbox and sets out next steps", Bundesministerium des Innern und für Heimat, "Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme",

(参考) ITセキュリティ法2.0の構成

ITセキュリティ法2.0において改正されるBSI法においては、特に5Gのモバイルネットワークのセキュリティを強調

改正概要

- 第1条
  BSI(連邦サイバーセキュリティ庁-Bundesamt für Sicherheit in der Informationstechnik)法の改正
- 第2条
  電気通信法の改正
- 第3条
  エネルギー経済法の改正
- 第4条
  対外経済法施行令の改正
- 第5条
  社会法典の改正
- 第6条
  評価
- 第7条
  法律の発効

ITセキュリティ法2.0により、改正後のBSI法には、以下の観点が盛り込まれている
(BSIによるIT セキュリティ法2.0の解説 (概要))

- 検出と防御
  - セキュリティ脆弱性の検出/サイバー攻撃に対する防御能力の強化
- モバイル ネットワークのサイバーセキュリティ
  - ドイツの公共の秩序や安全保護のための重要部品の使用を禁止する規制
    - 通信事業者は、高度なセキュリティ要件も満たす必要があり、重要部品は許可されている必要あり
    - **特に、5Gモバイル ネットワークにおける情報セキュリティを保証**
- 消費者保護
  - 特に連邦レベルでの独立した中立的なアドバイスと警告を通じ、情報技術のセキュリティ分野におけるデジタル消費者保護と消費者情報の任務を付与
- 企業のセキュリティ
  - 重要インフラの範囲が都市廃棄物処理セクターを含むように拡大され、他の公益の利益をもたらす企業 (武器製造業者、経済的に重要な企業等) も特定のITセキュリティ対策を実装する必要があり、BSIと信頼ある情報交換を実施
- サイバーセキュリティ認証に関する国家機関
  - 欧州のサイバーセキュリティ認証制度に基づく規制の監視と施行を担当

Source: Bundesamt für Sicherheit in der Informationstechnik, "Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme"、Bundesgesetzblatt, "Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme"

「ITセキュリティ法2.0」詳細 [2/9]：妨害防止措置の概要等

重要インフラ事業者は、重要部品を新たに使用する際に政府からの許可の取得が必要

妨害防止措置の概要

重要インフラ事業者は、「**重要部品**」を新たに使用する際、**事前に政府から許可を得ることを義務化**

更に、**連邦内務・国土省**が、ドイツ国内の公序や公共の安全を損なう恐れがある場合に**使用を禁止**

同省管轄下の**連邦情報セキュリティー庁 (BSI)** に対し、サイバーセキュリティ上の権限を付与

- 通信サービス事業者からの情報収集に係る権限の強化
- ネットワークにおけるセキュリティリスクの検出
- サイバーセキュリティに係る認証 等

対象者[1]

以下に掲げる分野に属する重要インフラ事業者[2]

- **エネルギー、水、食品、情報技術・通信、医療、金融・保険、交通・運輸、自治体廃棄物処理**
  - 「重要インフラ」とは、国家社会にとって重要な意味を持つ組織や施設であり、その障害や機能不全が、供給のボトルネックや、公共の安全への重大な脅威をもたらすもの

規制対象行為

重要インフラ事業者による自国の公共の秩序や安全が損なわれる可能性がある**重要部品の使用を制限**する

連邦内務・国土省が、以下の観点から審査を実施

- 製造者が、第三国政府 (その他の政府機関や軍隊を含む) に直接または間接的に支配されている
- 製造者が自国、EU、NATO等の加盟国・機関の公序良俗や治安に悪影響を及ぼす活動を行っている
- 重要部品の使用が、自国、EU、NATOの安全保障政策の目的に合致している

1.この他、本法においては、「デジタルサービス提供者」と「特別な公益性を有する企業」(武器製造業者、経済的重要性が特に高い企業等)も規定があり、それぞれインシデント通知義務や、ITセキュリティに関する自己申告書の提出が求められている　2. 事業者の数について、連邦内務・国土省による「ITセキュリティ法2.0の評価に関する報告書」(23年5月)によると約1,800事業者が登録されている旨の言及あり

Source: 内閣府「経済安全保障法制に関する有識者会議 基幹インフラに関する検討会合 第一回資料」, Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, "Kritische Infrastrukturen", Bundesministerium des Innern und für Heimat, "Evaluierung des IT-Sicherheitsgesetzes 2.0"、 Bundesamt für Sicherheit in der Informationstechnik, "Gesetz über das Bundesamt für Sicherheit in der Informationstechnik"

(参考) デジタルサービス提供者の義務

「デジタルサービス提供者」には、技術的・組織的な措置や、インシデント発生時の通知、当局への情報提供等が求められる

定義

- この法律にいう「デジタルサービス提供者」とは、デジタル・サービスを提供する法人をいう
- 本法にいうデジタルサービスとは、情報社会サービスに関する技術的規制及び規則の分野における情報提供のための手続を定めた2015年9月9日の欧州議会及び理事会の指令に定めたサービスであり、以下を指す
  - オンラインマーケットプレイス
  - オンライン検索エンジン
  - クラウドコンピューティングサービス　等

デジタルサービス提供者に対する特別要件 (概要)

(1) セキュリティのリスク管理のために、適切かつ相応の技術的および組織的措置を講じる

(2) 上記措置は、最新の状況および以下の点を考慮
- 1. システムと設備の安全性
- 2. セキュリティ・インシデントの検出・分析・軽減
- 3. 事業継続マネジメント
- 4. 監視・検査・試験
- 5. 国際規格への準拠

(3) EU内で提供するデジタルサービス提供に重大影響を及ぼすセキュリティインシデントを直ちに連邦事務局に通知

(4) EU指令の要件等を遵守していない兆候がある場合、当局からの求めに応じ、必要な情報提供や要件充足の不備を排除

(EU内の他加盟国に主たる事業所やネットワーク/情報システムを有する場合、ドイツの当局は、当該他加盟国の当局と連携し、情報提供や要請を実施)

Source: Bundesamt für Sicherheit in der Informationstechnik, "Gesetz über das Bundesamt für Sicherheit in der Informationstechnik

(参考) 特別な公益性を有する企業の義務

「特別な公益性を有する企業」には、連絡先の登録やITセキュリティ宣言の導入等の追加的な義務が求められている

定義

特別な公益性を有する事業とは、重要インフラの事業者には該当しない事業のうち、以下を指す

- UBI1：武器等製造企業
  - 武器、弾薬、兵器の分野、または製品の分野で事業を行う企業
- UBI2：価値創造企業
  - 国内付加価値の点でドイツにとって重要な企業であり、これらの企業の主要サプライヤー
- UBI3：危険物質取り扱い企業
  - 危険物質を取り扱う事業者等

法律上の義務 (概要)

- 連絡先の登録義務 [UBI1及びUBI2 ※ UBI3は任意]
  - 問い合わせ先等の登録
- セキュリティインシデントの報告義務 [UBI1-UBI3]
  - ITシステムのセキュリティインシデントについて報告
    - 価値創造の提供の障害を引き起こした又はこれにつながる可能性のあるもの (UBI1及びUBI2)
    - 可用性/完全性/真正性/機密性に対する障害で、インシデントにつながった、又はインシデントにつながる可能性のある重大な障害 (UBI3)
- ITセキュリティ宣言 [UBI1及びUBI2]
  - 認証/セキュリティ監査/ITセキュリティテスト/重要なシステムの保護対策の情報提出
  - 提出すべき内容：
    - 過去2年のITセキュリティ認定資格
    - 過去2年のその他のITセキュリティ監査およびテスト
    - 特に保護する価値があるITシステム、コンポーネント、プロセスの保護に関する情報

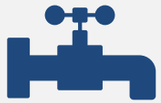
Source: Bundesamt für Sicherheit in der Informationstechnik, "Gesetz über das Bundesamt für Sicherheit in der Informationstechnik"、Bundesamt für Sicherheit in der Informationstechnik, "Unternehmen im besonderen öffentlichen Interesse (UBI)"、Bundesamt für Sicherheit in der Informationstechnik, "Registrierung"、Bundesamt für Sicherheit in der Informationstechnik, "FAQ zu UBI: Allgemein"

「ITセキュリティ法2.0」詳細 [3/9]：対象分野 (全体像)

本法令の対象として、8カテゴリーに渡るインフラ分野が定義されている

対象分野
(全体像)

1. 
エネルギー
Energy

2. 
水
Water

3. 
食品
Food

4. 
情報技術・通信
Information technology and telecommunications

5. 
医療
Health

6. 
金融・保険
Finance and insurance

7. 
交通・運輸
Transport and traffic

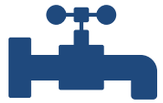
8. 
自治体
廃棄物処理
Municipal waste disposal

Source: Bundesamt für Sicherheit in der Informationstechnik, "Gesetz über das Bundesamt für Sicherheit in der Informationstechnik", Bundesamt für Sicherheit in der Informationstechnik, "Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz",Bundesamt für Sicherheit in der Informationstechnik, "What are Critical Infrastructures?"

「ITセキュリティ法2.0」詳細 [4/9]：対象分野 (詳細) [1/3]

本法の下位法令 (法令の附属書) において、各分野の詳細な対象者 (事業毎の閾値含む) が規定されている

対象分野 (詳細)

①	エネルギー Energy		• 電力供給[1] • ガス供給 • 燃料または灯油の供給 • 地域冷暖房供給
②	水 Water		• 飲料水供給 • 下水処理
③	食品 Food		• 食品供給 (生産/流通/貿易)

1. 例えば、電力供給であれば、発電プラント、電力制御設備/システム、送電網、配電網 等の区分に更に分かれており、それぞれに閾値 (扱うエネルギー量の水準等) が設定されている

Source：Bundesamt für Sicherheit in der Informationstechnik, "Gesetz über das Bundesamt für Sicherheit in der Informationstechnik", Bundesamt für Sicherheit in der Informationstechnik, "Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz", Bundesamt für Sicherheit in der Informationstechnik, "What are Critical Infrastructures?"

「ITセキュリティ法2.0」詳細 [5/9]：対象分野 (詳細) [2/3]

対象分野
(詳細)
[続き]

④ ICT Information technology and tele communications

- 音声とデータの送信
  (アクセスネットワーク、伝送ネットワーク、海底ケーブル陸揚げ局 等)
- データの保存と処理

⑤ 医療 Health

- 入院医療
- 生命を直接維持する医療機器の供給
- 医薬品・ワクチンの供給 (処方箋医薬品、血液・血漿濃縮物の供給)
- 臨床検査診断

⑥ 金融・保険 Finance and insurance

- 現金の供給
- カード決済取引
- 伝統的な決済
- 証券およびデリバティブ取引の清算・決済
- 保険サービス

Source: Bundesamt für Sicherheit in der Informationstechnik, "Gesetz über das Bundesamt für Sicherheit in der Informationstechnik", Bundesamt für Sicherheit in der Informationstechnik, "Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz", Bundesamt für Sicherheit in der Informationstechnik, "What are Critical Infrastructures?", Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, "Kritische Infrastrukturen"

「ITセキュリティ法2.0」詳細 [6/9]：対象分野 (詳細) [3/3]

対象分野 (詳細) [続き]

7 交通・運輸 Transport and traffic		• 旅客輸送サービス (航空、海運、内陸水路) • 貨物輸送サービス (鉄道輸送、道路輸送、物流)
8 自治体廃棄物処理 Municipal waste disposal		–

Source: Bundesamt für Sicherheit in der Informationstechnik, "Gesetz über das Bundesamt für Sicherheit in der Informationstechnik", Bundesamt für Sicherheit in der Informationstechnik, "Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz", Bundesamt für Sicherheit in der Informationstechnik, "What are Critical Infrastructures?", Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, "Kritische Infrastrukturen"

(参考) 重要部品　詳細

「重要部品」とは法令上で重要インフラにて使用されるIT製品を指し、情報技術・通信分野についてのリストが公開されている

定義 (第2条13項)

この法律にいう重要部品とは、以下のIT製品をいう

- 1.重要インフラで使用されているもの
- 2.可用性、完全性、真正性、機密性が損なわれることにより、重要なインフラが故障したり、その機能が著しく損なわれたり、公共の安全が脅かされる可能性があるもの
- 3.この規定を参照した法律に基づいて発行されたもの
  - a) 重要部品として決定されているもの
  - b) 法律に基づいてクリティカルと判断された機能

重要部品を決定する重要機能の概要 (情報技術・通信分野：5Gネットワークのリスト)

カテゴリー	機能
a) コア・ネットワーク機能	• エンドユーザーの認証、ローミング、セッション管理 • エンドユーザー施設のデータ転送 • アクセスポリシー管理 • ネットワークサービスの登録と認可 • エンドユーザーおよびネットワークデータのストレージ • サードパーティのモバイルネットワークへの接続 • コアネットワーク機能を外部アプリケーションの公開 • ネットワークスライスへのエンドデバイスの割り当て
b) NFV 管理とネットワークオーケストレーション (MANO)	仮想化されたネットワーク機能の管理とオーケストレーション
c) 管理体制とサポートサービス	管理システムのセキュリティ機能
d) 無線アクセスネットワーク (RAN)	5G RAN管理
e) 輸送と伝送	関連性が高まる音声とデータの転送
f) インターネットワーク交換	MNO外のIPネットワーク（サードパーティネットワークサービス）

Source: Bundesamt für Sicherheit in der Informationstechnik, "Gesetz über das Bundesamt für Sicherheit in der Informationstechnik" , Bundesnetzagentur, "Katalog von Sicherheitsanforderungen"

「ITセキュリティ法2.0」詳細 [7/9]：審査のプロセス [1/2]

重要インフラ事業者からの届出を関係省庁間で協議・審査し、認可・否認を判断する。

審査プロセス [1/2]

事業者による届け出の受理 → **関係省庁間の協議** → **最終判断**

重要インフラ事業者は、「重要な部品[1]」を新たに使用する前に、**設備の安全性を製造元が保証した宣言とともに、連邦内務・国土省に届け出を提出 [詳細後述]**

- 設備の安全性を製造元が保証した宣言
  - 部品が破壊工作、スパイ活動、テロリズムの目的で悪用される可能性が特に高い技術的特徴を有していないことの保証方法

関係省庁間で審査基準に抵触するかを協議

- 外務省、経済・エネルギー省、財務省、国防省、運輸・デジタルインフラ省、保健省 等
- 2~4か月の審査期間中は部品を使用不可

主に以下3つの観点で審査

- 製造者が第三国政府(その他の政府機関や軍隊を含む)に直接または間接的に支配されている
- 製造者が自国、EU、NATO等の加盟国・機関の公序良俗や治安に悪影響を及ぼす活動を行っている
- 重要部品の使用が、自国、EU、NATOの安全保障政策の目的に合致している

1. 重要なインフラで使用されており、可用性、完全性、真正性、機密性が損なわれることにより、重要なインフラが故障したり、その機能が著しく損なわれたり公共の安全が脅かされる可能性があり、関連規定上、重要部品又は重要な機能を持つとされるもの

Source: Bundesamt für Sicherheit in der Informationstechnik, "Gesetz über das Bundesamt für Sicherheit in der Informationstechnik", Bundesamt für Sicherheit in der Informationstechnik, "Fragen und Antworten zu Bußgeldern (§ 14 BSIG)", 内閣府「経済安全保障法制に関する有識者会議」

「ITセキュリティ法2.0」詳細 [8/9]：審査のプロセス [2/2]

重要インフラ事業者からの届出を関係省庁間で協議・審査し、認可・否認を判断する。

審査プロセス [2/2]

届け出の受理 → **関係省庁間の協議** → **最終判断**

関係省庁間の協議結果を踏まえて、**連邦内務・国土省が認可/否認**

- 当該部品の利用がドイツの安全保障政策上の利益に反すると認めるときは、**当該部品の利用禁止を命ずることができる (届出受領から2か月以内(4か月まで延長可能))**
- **製造者が信頼に値しないことが判明した場合、重要なコンポーネントのさらなる使用を事後的に禁止することが可能**

Source: Bundesamt für Sicherheit in der Informationstechnik, "Gesetz über das Bundesamt für Sicherheit in der Informationstechnik" Bundesamt für Sicherheit in der Informationstechnik, "Fragen und Antworten zu Bußgeldern (§ 14 BSIG)"

「ITセキュリティ法2.0」詳細 [9/9]：製造者の製品使用の禁止

重要な部品の「製造者」が「信頼できない」場合、その製品の使用を禁止する旨の規定も存在

下記に該当する兆候がある場合、製造業者は「信頼できない」と判断される

1. (政府が最低要件を示す) 保証宣言に記載された義務に違反している
2. 保証宣言に記載されている事実が正しくない
3. 製品および製造環境における安全性チェックとペネトレーション分析が、必要な範囲で適切にサポートされていない
4. 脆弱性や操作を認識し、重要インフラの運用者に報告した後も、直ちにそれを排除していない
5. 重要な部品が、その欠陥のため、重要インフラのセキュリティ、機密性、完全性、可用性または機能性に不適切な影響を及ぼす可能性が高い、またはその可能性が現に高まった
6. 重要な部品が、重要なインフラのセキュリティ、機密性、完全性、可用性、または機能性を悪用するために特に適した技術的特性を有している、または有していた

Source: Bundesamt für Sicherheit in der Informationstechnik, "Gesetz über das Bundesamt für Sicherheit in der Informationstechnik"

(参考) 保証宣言の内容

保証宣言については、記載すべき事項の最低要件を記載した命令が出されている

重要部品の製造者による以下を確約する旨の声明を記載する必要がある (概要)

1. 重要部品に関して、重要インフラ事業者とBSI等と協力し、**重要部品の製造・運用に関する情報の提供、必要な支援を提供、重要インフラ事業者が重要部品の情報セキュリティ管理システムを監査できる状況にする**こと
2. 重要部品のセキュリティテストや侵入分析をする際に、**重要インフラ事業者を支援する**ことを確約すること
3. システムのセキュリティ関連の**生産及び提供計画の変更について、重要インフラ事業者に事前通知**を行うこと、及び重要インフラ事業者の要請に応じセキュリティ関連部分の**製品開発に関する情報提供を行う**こと
4. 重要部品に**脆弱性がされ次第、重要インフラ事業者へ通知**をすることを約束すること
5. 重要部品に**適切な情報セキュリティ管理システムを適用する**ことを約束すること
(関連情報の文書化、最新の技術水準による保護、変更の監視等も含まれる)
6. 会社に適用される法律に違反した場合、会社の構造を前提とし、欧州連合(EU) 加盟国ではない国の政府/政府機関/軍にとって、重要インフラのセキュリティ、機密性、完全性、可用性または操作性に影響を及ぼすことが可能かどうか、可能である場合、どのような方法で可能であるかについての宣言
7. 会社の本社情報や商業登記番号、代表者の氏名・住所・生年月日
8. 運用プロセスに関する**秘密情報等の開示を拒否すること**を法律上/事実上保証すること
9. 保証宣言を履行することが不可能になった場合には、直ちに政府や重要インフラ事業者へ報告すること

Source: Garantieerklärung - declaration of guarantee

3-4. ドイツ

1. 政策の全体像

2. 制度の調査結果
   - ITセキュリティ法2.0 (1)
   - ITセキュリティ法3.0 (2)

3. 事例

「ITセキュリティ法3.0」の概要：議論の状況/ディスカッションペーパー概要

NIS2指令の実施とサイバーセキュリティの強化のため、国内法の草案を策定中 (昨年9月にディスカッションペーパーが発表)

法令等の名称	• Wirtschaftsbezogene Regelungen zur Umsetzung der NIS-2-Richtlinie in Deutschland – ドイツにおけるNIS2指令実施のための経済規制 – 正式名称ではないが、「ITセキュリティ法3.0」と呼称される場合もあり – 連邦政府内で正式には調整されていないディスカッション ペーパーとの位置づけ
検討の経緯	• 2020年12月 欧州委員会がNIS (ネットワーク情報システム) 指令の改訂案(NIS2)を発表 • 2022年12月 NIS2指令が官報掲載 • 2024年10月18日の施行に向けて、対応する国内法の策定に向け、草案作成中 – 2023年9月　ドイツ連邦内務省よりディスカッションペーパーが発表
主な変更点 (内務・国土省が言及しているもの)	• 特に重要な施設/重要な施設及び重要インフラ運用者に対する監督・検証体制の再構築 • BSI法へのNIS2指令との定義の入れ込み • NIS2指令の要件に基づく対象範囲の設定 – 中規模以上 (従業員数50名以上又は年間売上高1000万ユーロ超等) の企業の対象化 等

SourceSource: 経済産業省「EU NIS2指令概要」, BMI - Gesetzgebungsverfahren - Diskussionspapier des Bundesministeriums des Innern und für Heimat für wirtschaftsbezogene Regelungen zur Umsetzung der NIS-2-Richtlinie in Deutschland

3-4. ドイツ

1. 政策の全体像

2. 制度の調査結果
   - ITセキュリティ法2.0 (1)
   - ITセキュリティ法3.0 (2)

3. 事例

事例調査結果

ITセキュリティ法2.0に基づく資産の登録等の運用は始まっているものの、個別事例の公表はされておらず、適用事例はない状況

一方で、内務省によるHuawei製品を禁止する動きもみられるものの、実行には至っていない

Source: Drucksache 20/9923 (bundestag.de)

3-5. フランス

1. 政策の全体像

2. 制度の調査結果
   - LOI n° 2019-810 (1)
   - LOI n° 2018-133 (2)
   - CIIP法 (3)
   - NIS2指令 国内実施法 (検討状況) (4)

3. 事例

3-5. フランス

1. 政策の全体像

2. 制度の調査結果
   - LOI n° 2019-810 (1)
   - LOI n° 2018-133 (2)
   - CIIP法 (3)
   - NIS2指令 国内実施法 (検討状況) (4)

3. 事例

フランスの基幹インフラ妨害行為の防止に係る政策の全体像

主な対象行為		主な対象者		
		国内企業		外国企業
		通信事業者	基幹インフラ事業者 (通信事業者を除く)	
取引規制	製品/役務の調達	1 **LOI n° 2019-810** • 5G以降のハード・ソフトウェア利用に際し、通信事業者が申請し、政府が許可するもの **主な制度 (詳細深掘り)**	2 **LOI n° 2018-133 (EU NIS指令の国内実施法)** • 重要インフラ事業者を指定し、セキュリティ対策実施等を義務化しつつ、当局による検査も可能に **主な制度 (詳細深掘り)**	
	対内直接投資			5 **通貨金融法典/PACTE法** • 投資家がフランスの特定業種の法人または事業へ投資する場合、経済大臣の事前承認が必要
サイバー攻撃への防護		3 **CIIP[1]法 (重要情報インフラ防護法)** • 重要なインフラ事業者に対し、国防を目的とするセキュリティ対策実施と、国家情報システム・セキュリティ庁 (ANSSI) やその認定委託事業者による監査を義務化		
		4 **EU NIS2指令の国内実施法 (現在検討中)**		

Note：上記分類は、本調査の目的から、関連が深いと考えられる法令を抽出し、主な目的/対象の相違等を強調するために整理をしたものであり、必ずしも上記各範囲の内容のみを含むとは限らない
特に、国内企業には、国内にて事業活動を行う外国企業も含まれうる

1. Critical Infrastructures Information Protection

Source: Légifrance, "LOI n° 2019-486 du 22 mai 2019 relative à la croissance et la transformation des entreprises (1)"、国立国会図書館ウェブサイト（【フランス】国による情報監視技術の使用を規定する法律(国立国会図書館調査及び立法考査局)）

3-5. フランス

1. 政策の全体像

2. 制度の調査結果
   - LOI n° 2019-810 (1)
   - LOI n° 2018-133 (2)
   - CIIP法 (3)
   - NIS2指令 国内実施法 (検討状況) (4)

3. 事例

「LOI n° 2019-810」概要 [1/2]

法令等の名称

- LOI n° 2019-810
  - LOI n° 2019-810にて、郵便・電子通信法典を改正し、第II部第1編第2章第7節を追加

制定時期

- 2019年6月　議会提出
- 2019年8月　郵便・電子通信法典改正

※ 郵便・電子通信法典自体は、1952年に電気通信分野の基本法令として法典化されたもの

制定の経緯

- 2019年6月　防衛と国家安全保障の利益の維持を目的に、5Gサービスのセキュリティ対策に関する法案を議会へ提出
- 2019年8月　「郵便・電子通信法典」が改正、無線通信ネットワークについて、国防・国家安全保障の観点が追加された

妨害防止措置の概要

- 5G以降の無線通信網関連のハード・ソフトウェア利用について、**通信事業者は、首相府の定める様式に従い、事前に審査を受け、許可を得る旨規定**

対象者/対象機器

対象者：国の安全保障上重要な通信事業者

対象機器：5G関連機器
(幅広いハードウェア/ソフトウェアが対象)

Source:総務省「フランス共和国　通信概要」, Légifrance, "Code des postes et des communications électroniques", Le Sénat, "Proposition de loi visant à préserver les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques mobiles"

「LOI n° 2019-810」概要 [2/2]

審査プロセス

申請書の提出/受理

- 対象となる機器リストが、ANSSI[1]等関係各省での協議を経て、作成され、公開
- 通信事業者は作成されたリストを元に保有している5G対応設備を確認し、申請書を作成・提出

政府による確認

- 政府は郵便・電子通信法典や関連法令に基づき、申請書を確認
- 国民に危害を及ぼす重大な危険があると判断した場合、許可や更新を拒否することが可能

最終判断

- 最大8年間の利用・運営権が認可
  - 条件が付く場合もあり
- 許可の更新は、有効期限の2か月前から可能

審査時に考慮する要素

国民に危害を及ぼす重大な危険があると判断した場合、許可や更新を拒否可能

- 防衛と国家安全保障の利益を損なう重大なリスクが懸念される利用
- ネットワークおよびサービスの永続性、品質、可用性、セキュリティを欠如する利用
- 送信されるメッセージおよび通信に関連する情報の機密性および中立性が担保されない利用
- 公的機関や事業者の情報システムセキュリティに対する脅威および攻撃に対応しない利用

1. Agence nationale de la sécurité des systèmes d'information（国家情報システム・セキュリティ庁）

Source:総務省「フランス共和国　通信概要」, Légifrance, "Code des postes et des communications électroniques", Le Sénat, "Proposition de loi visant à préserver les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques mobiles"

「LOI n° 2019-810」詳細 [1/5]：法令等の名称、経緯

電気通信分野においては随時改正がなされており、ANSSIに対する報告等が求められてきたところ、
更にLOI n° 2019-810において、国防・国家安全保障の観点から、機器の使用に関する審査も求められることとなった

法令等の名称	• **LOI n° 2019-810** – 郵便・電子通信法典は、電信・放送領域における行政法をまとめたもの[1] – 「LOI n° 2019-810」等により改正
改正時期	• 2019年6月　議会提出 • 2019年8月　「LOI n° 2019-810」により「郵便・電子通信法典」改正、「第Ⅱ部第1編第2章第7節」が追加、無線通信ネットワークについて、国防・国家安全保障の観点を盛り込み
改正までの経緯	• 2015年10年 「国家デジタル・セキュリティ戦略」において、セキュリティ関連政策の監督・執行機関をANSSI[2]とし、従来、国防・政府機関を中心としてきたセキュリティ対策を市民生活に拡張する方針が示される • 2016年11月 電子通信産業のサイバーセキュリティ対応に関する省令が発効 (ANSSIに対し、情報システムのリストを提出、年ごとに更新報告やセキュリティ・システムのトラブル時、報告する義務が課される) • 2018年7月　法典の改正により、通信事業者はANSSIの指示する技術的措置を取ること等が規定 • 2019年6月　防衛と国家安全保障の利益の維持を目的に、5Gサービスのセキュリティ対策の要素を法令へ追加する**「LOI n° 2019-810」**が議会へ提出 • 2019年8月　**「郵便・電子通信法典」が改正、**無線通信ネットワークについて、国防・国家安全保障の観点が追加

1. 「法律の部」、「国務院の議を経るデクレ (政令)の部」、「デクレ (政令) の部」の3部から構成されている、2. Agence nationale de la sécurité des systèmes d'information（国家情報システム・セキュリティ庁）
Source:総務省「フランス共和国　通信概要」, Légifrance, "Code des postes et des communications électroniques", Le Sénat, "Proposition de loi visant à préserver les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques mobiles"

「LOI n° 2019-810」詳細 [2/5]：妨害防止行為等の概要

5G以降のハード・ソフトウェアの利用に際して、通信事業者は、申請・許可が必要

妨害防止措置の概要	国内において、5G以降の無線通信網を用いてエンドユーザーに接続するハードウェア/ソフトウェアの設備は、**首相**の許可を受ける必要あり **許可**は、事業者から提出された申請書の審査後に付与 許可の期限は**最大8年間** (条件付きの場合あり) • 許可の更新には更新申請が必要。現行の許可が失効する2か月前までに要提出
対象者/設備	対象者：安全保障上、重要な通信事業者[1] 対象設備：5G通信に関わる全ての機器 (基地局、端末、ネットワークソフトウェア　等) • 但しエンドユーザーの敷地内に設置されるもの等は除く
規制対象行為	基準に準拠しない場合や、事前の審査・認可を得ないままの5G機器利用 • 防衛と国家安全保障の利益を損なう重大なリスクが懸念される利用 • ネットワークおよびサービスの永続性、品質、可用性、セキュリティを欠如する利用 • 送信されるメッセージおよび通信に関連する情報の機密性および中立性が担保されない利用 • 公的機関や事業者の情報システムセキュリティに対する脅威および攻撃に対応しない利用

1. 国防法典 L. 1332-1の定義も引用 (それが利用できないことにより、国家の戦争又は経済的潜在力、安全保障、生存能力を著しく低下させる施設を運営する事業者)
Source:総務省「フランス共和国　通信概要」, Légifrance, "Code des postes et des communications électroniques", Le Sénat, "Proposition de loi visant à préserver les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques mobiles"

「LOI n° 2019-810」詳細 [3/5]：事前申請のプロセス

通信事業者から提出された申請書を基に、政府により内容を確認
最大8年間の許可を付与

申請書の提出 / 受理

対象となる機器リストが、ANSSI等関係各省庁との協議後、首相の命令により作成・公開
[リストは次頁参照]

通信事業者は作成されたリストを元に保有している5G対応設備を確認し、申請書を作成し、国防・国家安全保障事務総長に提出

政府 (首相府/ANSSI[1]) による確認

郵便・電子通信法典/関係法令に基づき、申請書を確認/審査

国民に危害を及ぼす重大な危険があると判断した場合、許可や更新を拒否可能

[考慮する要素]
- 防衛と国家安全保障の利益を損なう重大なリスクが懸念される利用
- ネットワークおよびサービスの永続性、品質、可用性、セキュリティを欠如する利用
- 送信されるメッセージおよび通信に関連する情報の機密性および中立性が担保されない利用
- 公的機関や事業者の情報システムセキュリティに対する脅威および攻撃に対応しない利用

最終判断

最大8年間の利用・運営権が認可
- 期限付きでの認可となるケースも存在

許可の更新については、有効期限が切れる2か月前から対応

1. Agence nationale de la sécurité des systèmes d'information（国家情報システム・セキュリティ庁）
Source: 総務省「フランス共和国　通信概要」, Le Sénat, "Proposition de loi visant à préserver les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques mobiles"

「LOI n° 2019-810」詳細 [4/5]：対象となる機器のリスト

5Gネットワークについて、幅広い装置が対象となっている

第5世代移動無線ネットワークにおける下記のソフトウェア/ハードウェア装置[1]

- 端末機器の認証
- 当該端末機器への無線リソースの割当
- 端末機器相互または第三者ネットワークへの電子通信のルーティングの保証

第5世代移動無線ネットワーク内で機能を実行し、ネットワークのセキュリティ、完全性、または可用性を決定するソフトウェア/ハードウェア装置[1]

装置概要	3GPP規格における関連ネットワーク機能の命名
端末機器との無線通信と無線リソースの割り当てを提供する機器、または基地局	新しい無線基地局 (en-gNodeB and gNodeB)
端末機器の認証とネットワーク・アクセス認証を提供する機器	アクセス＆モビリティ管理機能（AMF）と認証サーバー機能（AUSF）
端末機器から第三者ネットワークへの通信をルーティングする装置	ユーザープレーン機能（UPF）
端末機器のセッションや接続を管理する機器	セッション管理機能（SMF）
ネットワーク・アクセス・ポリシーを実施・制御するデバイス	ポリシーコントロール機能（PCF）
移動無線ネットワークを構成する異なる分離ユニット間で端末装置とその通信を分配するための装置	ネットワーク・スライス選択機能（NSSF）
ネットワーク内での登録、承認、サービス継続のための機器	ネットワークリポジトリ機能（NRF）
ネットワーク情報をネットワーク外の機器に公開し、設定できるようにする機器	ネットワークエクスポージャー機能（NEF）
暗号データ記憶装置と加入者識別子	統合データ管理（UDM）
モバイル・ネットワークと他のネットワークを相互接続する機器	セキュリティ・エッジ保護プロキシ（SEPP）

1. 受動的なアンテナを含む受動的な電子機器やこれらの機器に組み込まれる特殊でないハードウェアおよびソフトウェア機器等、例外あり
Source: Légifrance, "Arrêté du 6 décembre 2019 fixant la liste des appareils prévue par l'article L. 34-11 du code des postes et des communications électroniques"

「LOI n° 2019-810」詳細 [5/5]：申請時の記載事項

事業者は、申請時、自身の情報、機器の目的や活用法・運用法等を記載する必要がある

- **申請者の情報**
  - 自然人の場合：申請者の氏名および住所
  - 法人の場合：申請者の氏名、登録事務所の住所および法定代理人の氏名
- **機器の目的、名称、バージョン、技術的特性**
  - 製造者から提供された機器の技術資料を添付
- **申請者の無線ネットワーク内での機器の使用目的**
- **装置の設置方法**
  - 装置のオプション機能の起動の有無、他のネットワーク要素との相互接続に採用された保護措置、装置・データがホストされる特殊化されていないコンピュータソフトウェア、オペレーティングシステムとあらゆる仮想化ソリューション、このソフトウェアの保護措置 等を明記すること
- **装置の運用手順**
  - 運用中またはコンピュータホスティング上で実施される可能性のある設定・監督・保守作業や、設定・監督・保守作業を実施する下請業者を明記すること
- **機器が刑法典R226-3に規定される認可の対象である場合は、当該認可への言及**
- **認可申請書に記載された情報への準拠を確認するために必要な検査を受けることの確約**

Source: Légifrance, "Décret n° 2019-1300 du 6 décembre 2019 relatif aux modalités de l'autorisation préalable de l'exploitation des équipements de réseaux radioélectriques prévue à l'article L. 34-11 du code des postes et des communications électroniques"

3-5. フランス

1. 政策の全体像

2. 制度の調査結果
   - LOI n° 2019-810 (1)
   - LOI n° 2018-133 (2)
   - CIIP法 (3)
   - NIS2指令 国内実施法 (検討状況) (4)

3. 事例

「LOI n° 2018-133」(NIS指令国内実施法) 概要 [1/2]

法令等の名称

- **LOI n° 2018-133**
  - NIS指令の国内実施法
- **Décret n°2018-384**
  - 「LOI n° 2018-133」を補足する政令

制定時期

- 2018年2月　LOI n° 2018-133 施行
- 2018年5月　Décret n°2018-384 施行

制定の経緯

- 2018年2月　EU NIS指令に準拠する形で「LOI n° 2018-133」を施行、大枠を決定
- 2018年5月　「Décret n°2018-384」にて詳細を規定
  - 対象分野の詳細等の規定
  - 対象事業者の指定に係る規定

妨害防止措置の概要

電力・石油・ガス等を始めとする重要インフラ事業者の
安全保障分野におけるEU NIS指令の実施

- 首相が、関係省庁及び国家情報システム・セキュリティ庁(ANSSI) の推薦に基づき、重要インフラ事業者を指定
- 指定された重要インフラ事業者に対し、セキュリティリスク管理や、インシデント報告の義務を課す
- 首相は、違反の疑いがある事業者に対し、遵守状況の検査を命令することも可能

対象者

下記の各セクターの重要インフラ事業者

- エネルギー、輸送、物流、銀行・金融、保険、福祉、雇用訓練、医療、水道・下水、デジタルインフラ、教育、食品産業

Source: Le Sénat, "Programmation militaire 2014-2019", 経済産業省「平成30年度 産業保安等技術基準策定研究開発等事業(電気分野におけるサイバーセキュリティ対策国際調査)報告書」, Secrétariat général de la défense et de la sécurité nationale, "THE CRITICAL INFRASTRUCTURE PROTECTION IN FRANCE"

「LOI n° 2018-133」(NIS指令国内実施法) 概要 [2/2]

運用の内容

事業者の指定

- 首相が、関係省庁/政府機関の提案を基に、事業者を指定
  - 事業者には、指定される旨、事前に通知し、意見を述べる機会を付与

事業者による義務遵守

- ネットワーク/システムのリストの作成・更新
- セキュリティ関連規則の遵守
- インシデント発生時の当局への報告

当局による検査

- 義務の遵守状況・セキュリティレベルの確認のための検査を実施することが可能
  - 首相が、関係閣僚の意見を事前に聴取
- 事業者は、検査に協力する義務/結果を遵守する義務あり

セキュリティ規則の概要

事業者が遵守すべき規則は、大きく下記から構成

- セキュリティに係るガバナンス
  - ポリシー策定と実施、セキュリティの認証
- ネットワーク/情報システムの保護
  - アーキテクチャ/管理のセキュリティ、アクセスの制御
- ネットワーク/情報システムの防御
  - インシデントの検知と対処
- 事業のレジリエンス
  - インシデント発生時の危機管理

罰則

セキュリティ関連規則を遵守しなかった場合、インシデント報告義務を遵守しなかった場合、政府による検査を妨害した場合のそれぞれで、事業者の種類に応じ、罰金が科される (12万5千ユーロ等)

1)2019年3月時点

Source: 経済産業省「平成30年度 産業保安等技術基準策定研究開発等事業(電気分野におけるサイバーセキュリティ対策国際調査)報告書」, ANSSI, "Appel public à commentaires sur la mise à jour du référentiel PASSI", ANSSI, "FAQ - opérateurs de services essentiels (OSE)"

「LOI n° 2018-133」詳細 [1/15]：名称/制定経緯 等

LOI n° 2018-133は、EU NIS指令を実施し、インフラ事業者のサイバーセキュリティを向上させることが目的

法令等の名称

- LOI n° 2018-133
  - NIS指令に対応する法律
- Décret n°2018-384
  - LOI n° 2018-133の詳細を規定する政令

制定時期

- 2018年2月　LOI n° 2018-133　施行
- 2018年5月　Décret　n°2018-384 施行

制定の経緯

- 2013年2月　　「EUサイバーセキュリティ戦略」が公表
  - サイバー攻撃を含むインシデントへの対処能力向上、サイバーセキュリティ対策に関する産業・技術開発等の取組が示される
- 2016年7月　　EUにおいて「ネットワーク・情報システムの安全に関する指令」(NIS指令) が制定
  - EU域内におけるサイバーセキュリティ対策に関する初めての共通立法
  - 加盟国に対し、2018年5月9日までに国内法制化することが義務付け
- 2018年2月　　EUのNIS指令に準拠するかたちで、「LOI n° 2018-133」を施行
- 2018年5月　　「Décret n°2018-384」施行、対象となる重要インフラ事業者の定義等の詳細を規定

Source: Le Sénat, "Programmation militaire 2014-2019", Assemblée Nationale, "Défense : loi de programmation militaire 2014-2019"),経済産業省「平成30年度 産業保安等技術基準策定研究開発等事業(電気分野におけるサイバーセキュリティ対策国際調査)報告書」、国立国会図書館ウェブサイト（ネットワーク・情報システムの安全に関する指令（NIS指令）―EU のサイバーセキュリティ対策立法― (ndl.go.jp)）

「LOI n° 2018-133」詳細 [2/15]：対象者/対象分野 等

社会/経済の観点から重要な、幅広いインフラ事業者が対象となっている

対象者

- **社会または経済の機能に不可欠なサービスを提供し、当該サービスの提供に必要なネットワーク及び情報システムに影響を及ぼす事故が発生した場合、その継続に重大な影響を及ぼす可能性がある公共または民間の事業者**[1]
  - 首相が事業者を指定
  - リストは定期的 (少なくとも2年ごと) に更新

対象分野/指定時の考慮要素

- **15の分野に渡り、幅広く対象 [詳細次頁]**
- **指定の際は、下記を考慮**
  - サービスの利用者の数
  - 他の対象セクターのサービスへの依存度
  - 重大性・期間の観点から、事故が経済や社会の機能、公共の安全に及ぼす可能性のある影響
  - 事業者の市場シェア
  - インシデントによって影響を受ける可能性のある地域という地理的範囲
  - 代替手段の利用可能性を考慮した、十分なサービスレベルを確保する上での事業者の重要性
  - (該当する場合) セクター固有の要因

1 一部例外あり (国防法典で別途規定がある事業者/システム等)。デジタルサービス事業者も対象となっており、類似の規定あり

Source: REPUBLIQUE FRANÇAISE"Décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique"、REPUBLIQUE FRANÇAISE"LOI n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité (1)"、経済産業省「平成30年度 産業保安等技術基準策定研究開発等事業(電気分野におけるサイバーセキュリティ対策国際調査)報告書」、国立国会図書館ウェブサイト（ネットワーク・情報システムの安全に関する指令（NIS指令）―EU のサイバーセキュリティ対策立法― (ndl.go.jp)）

「LOI n° 2018-133」詳細 [3/15]：対象分野 (全体像)

計15のカテゴリーにわたり、インフラ事業者を幅広く指定

対象分野 (全体像)

1. 
エネルギー
Energy

2. 
交通・運輸
Transport

3. 
物流
Logistics

4. 
銀行
Banks

5. 
金融市場インフラ
Finance market infrastructures

6. 
金融サービス
Finance services

7. 
保険
Insurance

8. 
福祉
Social

9. 
雇用と職業訓練
Employment and vocational training

10. 
健康
Health

11. 
飲料水の供給・配給
Supply and distribution of water

12. 
非飲料水の処理
Treatment of non-drinking water

13. 
デジタルインフラ
Digital Infrastructure

14. 
教育
Education

15. 
食品産業
Restaurant

Source: REPUBLIQUE FRANÇAISE"Décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique"

「LOI n° 2018-133」詳細 [4/15]：対象分野 (詳細) [1/9]

対象分野 (詳細)

セクター	サブセクター	概要
① エネルギー Energy 	電気	• 電力供給事業者 　- 販売・再販 (最終消費者/電力供給者への販売、電力取引所の運営) • 配電事業者 　- 配電 (配電網の管理と管理、消費者接続の管理、消費者メーターの管理) • 送電事業者 　- 送電 (送電網の運用・監督、需給調整、連系管理)
	石油	• 石油パイプライン事業者 　- 石油パイプラインの運営・監督 • 生産、精製、加工、保管、輸送施設の運営事業者 　- 生産 (生産施設の運営および監督)、精製 (製油所の運営および監督) 　- 保管 (貯蔵施設の運営および監督)、パイプライン外の輸送 (輸送計画、船舶またはトラックの運行) • デジタル物流データ転送プラットフォームの運営者 　- 石油事業者間/石油事業者と公的機関の間での物流データ転送サービス
	ガス	• ガス供給事業者 　- 販売・再販(顧客への販売、ガス供給者への販売、ガス取引所の運営) • ガス配電ネットワーク事業者 　- 配給 (運用と監視、消費者接続の管理、消費者メーターの制御) • ガス輸送事業者 　- 輸送(輸送ネットワークの運営・監視、需給調整、相互接続の管理) • ガス保管施設事業者 　- ガス貯蔵 (貯蔵施設の運営・監視)

Source:REPUBLIQUE FRANÇAISE"Décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique"

「LOI n° 2018-133」詳細 [5/15]：対象分野 (詳細) [2/9]

対象分野 (詳細)

セクター	サブセクター	概要
① エネルギー (続き) Energy 	ガス (続き)	• 液化天然ガス施設事業者 - 液化設備の運転・監視 - 荷揚げ・再ガス化 (荷揚げ設備の運転・監視、再ガス化設備の運転・監視) • 天然ガス事業者 - 天然ガスの供給、流通、輸送、貯蔵および処理 • 天然ガス精製および処理施設の運営事業者 - 精製 (精製設備の運転・監視) - 加工 (加工設備の運転・監視)
② 交通・運輸 Transport 	航空輸送	• 航空会社 - 旅客運送(旅客のチェックイン・搭乗、航空機の運航) - 貨物運送(貨物のチェックイン・搭乗、航空機の運航) • 空港管理事業者 - 空港施設の運営(検査・検査、貨物チェックイン、搭乗、旅客・手荷物管理) - 航空機の給油・装備 • 航空ナビゲーションサービスの提供事業者 - 飛行中の航空航行の管制と規制 - 空港の管制と規制 • 航空機整備事業者 - 航空機の整備・修理
	鉄道輸送	• 鉄道インフラストラクチャ事業者 - 鉄道交通制御・管理(交通監視・規制、信号、運行計画、経路管理) • 鉄道インフラメンテナンス事業者 - 鉄道インフラのメンテナンス

Source:REPUBLIQUE FRANÇAISE"Décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique"

「LOI n° 2018-133」詳細 [6/15]：対象分野 (詳細) [3/9]

対象分野 (詳細)

セクター	サブセクター	概要
② 交通・運輸 (続き) Transport	鉄道輸送 (続き)	• 鉄道会社 - 貨物・危険物輸送 (鉄道車両運行) - 旅客輸送 (車両運行、旅客案内・受付、旅客管理) • 車両整備事業者 - 車両のメンテナンス
	ガイド付き輸送	• 旅客の輸送会社 - 旅客輸送 (車両の運行、旅客の案内・受付、旅客動線の管理)
	水上輸送	• 河川、海運、沿岸の旅客および貨物運送事業者 - 旅客輸送 (旅客管理) - 貨物・危険物の輸送(予約、貨物登録) - 運行計画 • 船舶整備事業者 - 船舶のメンテナンス • 内陸水運インフラを運営する事業者 - 水上輸送インフラの運営 • 港湾または港湾施設の管理者および事業者 - 貨物サービス (積荷、荷降ろし、保管、警備、コンテナ管理) - 船舶の受付 (水先、曳航、係留、燃料補給) - 案内、受付、審査、旅客の乗降 - 港湾施設の管理

Source:REPUBLIQUE FRANÇAISE"Décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique"

「LOI n° 2018-133」詳細 [7/15]：対象分野 (詳細) [4/9]

審査対象分野 (詳細)

セクター	サブセクター	概要
② 交通・運輸 Transport 	水上輸送 (続き)	• 船舶交通事業者 　- 船舶交通サービス • 河川交通事業者 　- 河川交通サービス
	道路輸送	• 道路当局 (公的機関 / 事業者) 　- 道路管理 (メンテナンス、信号、インフラ管理、交通規制、監視) • 高度道路交通システムの運営事業者 　- 車両の集中管理 　- 交通管理の支援 　- 乗客情報の管理 　- オペレーションの支援 • 貨物運送会社 　- 危険物の輸送 • 公道輸送会社 　- 旅客管理、オペレーション • フォワーダー 　- フォワーダー、運送会社のチャーター
③ 物流 Logistics 		• 物流プラットフォームマネジャー 　- 物流プラットフォーム管理

Source:REPUBLIQUE FRANÇAISE"Décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique"

「LOI n° 2018-133」詳細 [8/15]：対象分野 (詳細) [5/9]

対象分野 (詳細)

セクター	サブセクター	概要
④ 銀行 Banks		• 信用機関・銀行 - 預金管理 - 信用業務 - 決済サービス - 投資サービス
⑤ 金融市場インフラ Financial market infrastructure		• 取引プラットフォーム運営者 - 金融商品取引プラットフォームの運営 • 中央清算機関 - 金融市場取引の中央清算サービス • 中央保管期間 - 担保管理 - 有価証券決済および受渡し
⑥ 金融市場サービス Financial Services		• 金融サービス・プロバイダー、決済機関、電子マネー機関 - 支払いサービス - 特別証券の発行 • 現金輸送会社 - 現金輸送業務の計画と運営 - 現金回収と供給依頼の管理

Source:REPUBLIQUE FRANÇAISE"Décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique"

「LOI n° 2018-133」詳細 [9/15]：対象分野 (詳細) [6/9]

対象分野 (詳細)

セクター	サブセクター	概要
7 保険 Insurance		• 保険会社、相互保険会社、積立保険会社、再保険会社 - 生命保険 - 損害保険 - 再保険
8 福祉 Social		• 社会保障機関 - 社会保障給付 (健康保険、老齢年金、家族手当、失業手当）の計算と支払い - 社会保障機関の徴収とキャッシュフローの管理
9 雇用と職業訓練 Employment and vocational training		• 決済事業者 - 雇用扶助の計算と支払い

Source:REPUBLIQUE FRANÇAISE"Décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique"

「LOI n° 2018-133」詳細 [10/15]：対象分野 (詳細) [7/9]

対象分野 (詳細)

セクター	サブセクター	概要
⑩ 健康 Health 	医療施設	• 医療従事者 - 予防、診断またはケア活動に貢献するサービス • 救急医療サービスの提供者 - 電話の受信と調整 - 移動式救急・救命サービス
	医薬品	• 医薬品卸・販売業者 - 医薬品流通
⑪ 飲料水の供給・配給 Supply and distribution of water 		• 飲料水の供給業者および販売業者 - ボトル水供給（図面作成、ボトリング、計画、流通、水質管理） - 配管水製造（集水、輸送、処理、貯蔵施設の運転、監督、維持管理、水質管理） - 配管水供給（配水施設の運転、監督、維持管理、流通、水質管理）

Source:REPUBLIQUE FRANÇAISE"Décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique"

「LOI n° 2018-133」詳細 [11/15]：対象分野 (詳細) [8/9]

対象分野 (詳細)

セクター	サブセクター	概要
12 非飲料水の処理 Treatment of non-drinking water		• 廃水の収集・処分・処理事業者 – 廃水回収 – 廃水処理 • 洪水および雨水の管理事業者 – 雨水の収集 – 避難誘導・管理
13 デジタルインフラ Digital Infrastructure		• インターネット・エクスチェンジ・ポイント（IXP） – インターネットトラフィックを交換するピアリング相互接続サービス • ドメインネームシステム（DNS）サービスプロバイダー – ドメイン名登録・管理 – ドメイン名ホスティング – ドメイン名解決サービス • トップレベル ドメイン名レジストリ – ドメイン名の割り当てとトップレベルドメイン名レジストリの管理 – トップレベルゾーンのホスティング

Source:REPUBLIQUE FRANÇAISE"Décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique"

「LOI n° 2018-133」詳細 [12/15]：対象分野 (詳細) [9/9]

対象分野 (詳細)

セクター	サブセクター	概要
14 教育 Education 		• 国の教育経路を担当する事業者 - 学校および学生の派遣先の管理 • 国家試験の実施を担当する事業者 - 国家試験の実施
15 食品産業 Restaurant 		• 医療、児童、 刑務所セクターへの食糧供給事業者 - 注文管理 - 調達、物流、保管、流通管理

Source:REPUBLIQUE FRANÇAISE"Décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique"

「LOI n° 2018-133」詳細 [13/15]：事業者の指定

関係省庁/政府機関と連携した上で事業者が指定される

事業者の指定

- 対象分野/サブセクターを所管する各大臣が、その分野で必須サービス事業者として指定される可能性のある事業者のリストを、上記の基準に照らしてその提案を正当化した上で、首相に提案
  - ANSSI (国家情報システム・セキュリティ庁) も提案可能
- 首相が、当該事業者を本法の事業者に指定する意向を各事業者に通知
- 事業者は、この通知から1ヶ月以内に意見を提出
- 指定された場合、2か月以内に、事業者はANSSIに対し、任命した代表者の情報を提供

Source: ANSSI, "FAQ - opérateurs de services essentiels (OSE)", Légifrance, "LOI n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité (1)"、Légifrance,"Décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique"

「LOI n° 2018-133」詳細 [14/15]：事業者の義務

指定された事業者は、情報提供やインシデント時の報告の義務あり

事業者の義務

[① ネットワーク/情報システムのリスト作成/更新、情報提供]

- 指定後3か月以内に、サービス提供に必要なネットワーク/情報システムのリスト・関連情報をANSSI (国家情報システム・セキュリティ庁) に送付 (その後も、年に1回、更新したものを送付)
  - 当局による検査 (後述) を目的に利用できるものとする必要
  - ANSSIは、関係大臣の意見を聴いた後、リスト/情報について、事業者に対して意見を述べることが可能
  - 事業者は2か月以内に、修正後のリスト/情報をANSSIに要通知

[② 事業者によるリスク管理]

- 下記に関するセキュリティ規則の遵守
  - セキュリティに係るガバナンス： ポリシー策定と実施、セキュリティの認証
  - ネットワーク/情報システムの保護： アーキテクチャ/管理のセキュリティ、アクセスの制御
  - ネットワーク/情報システムの防御： インシデントの検知と対処
  - 事業のレジリエンス： 重要サービスに重大影響を及ぼすインシデント発生時の危機管理

[③ インシデント時の報告]

- 事業者は、インシデント[1]を認識し次第、遅滞なくANSSIに報告
- インシデントの原因またはその結果に関連する追加情報を認識した場合、直ちにその情報を同庁に報告
- 進展に応じ、事故に関する情報を求める当局の要請に応じる必要あり

1) 必要不可欠なサービスの提供に必要なネットワークおよび情報システムに影響を及ぼす事態

Source: ANSSI, "FAQ - opérateurs de services essentiels (OSE)", Légifrance, "LOI n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité (1)"、Légifrance,"Décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique"

「LOI n° 2018-133」詳細 [15/15]：当局の検査

更に、指定された事業者は、当局による検査にも対応する義務あり

当局による検査

- **首相は関係閣僚の意見を聴いた後、義務の遵守状況・セキュリティレベルの確認のための検査を実施することが可能（暦年に1回を超える検査は不可）**
  - 現地で実施 (検査費用は事業者が負担)
  - 事業者は、検査者に対し、セキュリティ・ポリシーに関する文書、該当する場合はセキュリティ監査の結果など、検査の実施に必要な情報および要素を提供
  - また、分析・技術情報の記録実施のために、検査対象ネットワークおよび情報システムへのアクセスを許可することも要求
  - 遵守の不履行が発見された場合、当局が定める期間内に義務を遵守するよう、当該事業者の管理者に対して正式な通知を行うことが可能
  - 期限は事業者の操業状況および実施される措置を考慮して決定されるものとする
  - 検査の結果は、関係大臣に通知

Source: Source: ANSSI, "FAQ - opérateurs de services essentiels (OSE)", Légifrance, "LOI n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité (1)"、Légifrance,"Décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique"

(参考) ANSSI (国家情報システム・セキュリティ庁) の概要

名称	Agence nationale de la sécurité des systèmes d'information (国家情報システム・セキュリティ庁)
設立	2009 年7月
設立の背景・目的	• サイバー攻撃の潜在的な脅威に対応する目的で設立 • 軍事的な観点から創設・継承されてきた国家組織が前身 – 行政機関や運営者に対するアドバイスやサポートの役割が追加
行政機関における位置づけ	国防・安全保障について首相を支援する責任を負う、首相府 国防・国家安全保障総局 (SGDSN[1]) 下の組織
主な役割	• 情報通信技術の開発におけるセキュリティ意識の醸成への貢献 • 情報システムのセキュリティ機器・技術の研究、開発方針への参画 • 情報システムセキュリティ分野における国家技術とノウハウの促進

1. Secrétariat général de la Défense et de la Sécurité nationale

Source: Agence nationale de la sécurité des systèmes d'information,経済産業省「平成30年度 産業保安等技術基準策定研究開発等事業(電気分野におけるサイバーセキュリティ対策国際調査)報告書」, ANSSI, "Notre histoire"

3-5. フランス

1. 政策の全体像

2. 制度の調査結果
   - LOI n° 2019-810 (1)
   - LOI n° 2018-133 (2)
   - CIIP法 (3)
   - NIS2指令 国内実施法 (検討状況) (4)

3. 事例

「CIIP法」概要 [1/3]

CIIP法は、基幹インフラ事業者のサイバーセキュリティ対策が目的

法令等の名称	• CIIP法 (重要情報インフラ防護法) – 正式名称 (LOI no 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale)
制定時期	• 2013年8月　CIIP法を上院議会に提出 • 2013年12月　CIIP法制定
制定の経緯	• フランスでは、5年毎に軍事計画が策定、防衛・安全保障に関する法案も合わせて制定・更新 • 2013年8月　CIIP法案を上院議会に提出 – 2014~19年の軍事計画を策定するにあたり、国防大臣からサイバー防衛を強化するよう提案 – "この法案は、サイバー防衛を構成する新たな戦略的状況も反映している。それは、この分野における行動能力の強化と、この新たな課題への法律の適応を規定するものである" • 2013年12月　CIIP法制定

Source: Le Sénat, "Programmation militaire 2014-2019", Assemblée Nationale, "Défense : loi de programmation militaire 2014-2019",経済産業省「平成30年度 産業保安等技術基準策定研究開発等事業(電気分野におけるサイバーセキュリティ対策国際調査)報告書」

「CIIP法」概要 [2/3]

セキュリティ対策の徹底と監査の実施により、重要インフラ事業者のセキュリティを強化

妨害防止措置の概要	電力・石油・ガス等を始めとする国の重要なインフラ事業者に対し、**国防を目的とするセキュリティ対策実施と、国家情報システム・セキュリティ庁 (ANSSI) / 認定委託事業者による監査を義務化** 適切なセキュリティ対策を行わなかった場合、**罰金が科される**
対象者/資産	政府によって指定される重要インフラ事業者 (OIV) [1] • 食糧、水道、福祉・健康、民間活動、法的活動、軍事活動、エネルギー、交通・運輸、金融、通信・放送、宇宙、工業
規制対象行為	20カテゴリにわたる「サイバー衛生対策」を評価・審査した上で、**ANSSIが定める基準に満たしていない製品の使用・運用が行われている場合、罰金が科される** • 「サイバー衛生対策」のカテゴリ – 情報保証ポリシー、ネットワークマッピング、セキュリティ保守、セキュリティ認定、ログ取得、ログ相関分析、検知、セキュリティインシデント処理運用、セキュリティ警告処理運用、危機管理、ID特定、認証、アクセス制御と権限管理、管理者アクセス制御、管理システム、システムとネットワークの区分、トラフィック監視とフィルタリング、リモートアクセス、システム設置、痕跡情報

1. フランス語では、OIV (Opérateur d'importance vitale) と呼称。現時点で、12セクター、200事業者以上とのこと (ANSSI HP)
Source: 経済産業省「平成30年度 産業保安等技術基準策定研究開発等事業(電気分野におけるサイバーセキュリティ対策国際調査)報告書」, Secrétariat général de la défense et de la sécurité nationale, "THE CRITICAL INFRASTRUCTURE PROTECTION IN FRANCE", ANSSI, "CIIP FAQ"

「CIIP法」概要 [3/3]

12のセクターそれぞれに担当する大臣を割り当て、各大臣が策定した基準を基に、重要インフラが指定される

対象分野
(全体像)

1. 食糧 Food
2. 水道 Water management
3. 福祉・健康 Health
4. 民間活動 Civil activity of the State
5. 法的活動 Legal activity
6. 軍事活動 Military activity
7. エネルギー Energy
8. 交通・運輸 Transport
9. 金融 Finance
10. 通信・放送 Communications, NICT
11. 宇宙 Space & research
12. 工業 Industry

Source: Secrétariat général de la défense et de la sécurité nationale, "THE CRITICAL INFRASTRUCTURE PROTECTION IN FRANCE"

3-5. フランス

1. 政策の全体像

2. 制度の調査結果
   - LOI n° 2019-810 (1)
   - LOI n° 2018-133 (2)
   - CIIP法 (3)
   - NIS2指令 国内実施法 (検討状況) (4)

3. 事例

NIS2指令の国内実施法の検討状況

NIS2指令の国内適用に向け、国家情報システム・セキュリティ庁 (ANSSI) は、対象事業者含め関係者と協議を実施中、
並行して、法案やその関係法令を準備しており、2024年に、議会に法案を提出・採択することを目指している

関係者との協議

- NIS2指令の実施に向けた内容の協議
  - 法律の対象となる事業体の範囲（2023年第3四半期）
  - ANSSIと、対象事業者との間のコミュニケーションの方法（2023年第3四半期）
  - リスク管理の観点からのサイバーセキュリティ要件（2023年第4四半期）
- NIS2適用後に向けた支援策協議
  - 事業者が規制の影響をどのように受けるかを理解
  - 国内当局への報告義務の支援方法の検討
  - リスク管理要件を理解/実施

法令の作成

法案

- 法案準備 (2023年)
- 議会に法案を提出・採択 (2024年中)

下位法令 (政令・命令)

- NIS2の適用を補佐する政令・命令の作成
- 草案作成後、法律の公布後数か月の間に各省庁と協議の上公布

Source: ANSSI, "La directive NIS 2"

3-5. フランス

1. 政策の全体像

2. 制度の調査結果
   - LOI n° 2019-810 (1)
   - LOI n° 2018-133 (2)
   - CIIP法 (3)
   - NIS2指令 国内実施法 (検討状況) (4)

3. 事例

事例調査結果

「LOI no. 2019-810」に基づき事前審査制度は導入され、運用されているものの、**個別事例の公表はされていない状況**

一方で、「LOI no. 2019-810」に基づき、**拒否件数やその影響等は議会に提出され、一部公になっている**

- 同法第5条において、2020年7月1日より、政府が国会に対し、適用状況について件数やコスト等を含む年次報告書を提出することが義務付けられている
- 上記に基づき、首相府 国防・国家安全保障総局 (SGDSN) により2020年7月29日に提出された報告書にて申請件数と個別機器への影響が記載
  - 2019年12月～2020年7月において、4社からの申請に対し、157件の許可、22件の却下を実施。
    設置済み1,917台、新設4,548台の個別機器へ影響

なお、**上院外交・防衛・軍隊委員会の関連議員による、"申請の拒否や承認の短縮が決定されたものは全てHuaweiのハードウェアに関わるものだった"、との発言あり**

- "2020年の1年間で、フランスの通信事業者4社はANSSI[1]に157件の申請を行い、合計約6万5,000件のハードウェアを申請した。これらの申請の約半数 (82件) は、法律で認められている最長期間である8年間の認可を受ける結果となった。3分の1 (53件) は、許可された最長期間よりも短い期間の許可となった。最後に22件が却下された。
  却下または許可期間の短縮となった決定はすべて、**Huaweiハードウェア**に関するものであった"

1. Agence nationale de la sécurité des systèmes d'information（国家情報システム・セキュリティ庁）
Source: Bilan annuel de l'application des lois au 31 mars 2022、LA FRANCE S'ACCORDE DES MOYENS EN HAUSSE FACE À UNE MENACE CYBER QUI EXPLOSE !

(参考)「LOI n° 2019-810」の規定報告事項

LOI n° 2019-810 第5条において、政府が国会に提出しなければならないレポートの調査項目が指定されている

第5条 (原文)

A compter du 1er juillet 2020, le Gouvernement remet au Parlement un rapport annuel sur l'application du régime d'autorisation préalable mis en place par la présente loi.
Ce rapport analyse les impacts de ce régime sur les opérateurs et l'ensemble de leurs prestataires et sous-traitants, sur le rythme et le coût des déploiements des équipements de quatrième et cinquième générations sur l'ensemble du territoire, sur l'accès des usagers aux services de communications électroniques rendus grâce aux réseaux radioélectriques mobiles et évalue le nombre d'appareils n'ayant pas pu être installés ou ayant dû être retirés à la suite d'une décision de refus.
La présente loi sera exécutée comme loi de l'Etat.

第5条 (仮訳)

2020年7月1日以降、政府は本法律により導入された事前認可制度の適用に関する年次報告書を議会に提出する。この報告書では、この制度が通信事業者、そのすべてのサービス・プロバイダーおよび下請け業者に与える影響、フランス全土への第4世代および第5世代機器の配備のペースとコスト、移動無線ネットワークを介して提供される電子通信サービスへの利用者のアクセスに与える影響について分析し、拒否決定後に設置できなかった、または取り下げざるを得なかった機器の数を評価する。

Source:Légifrance, "LOI n° 2019-810 du 1er août 2019 visant à préserver les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques mobiles (1)"

3-6. EU

1. 政策の全体像

2. 制度の調査結果
   - NIS2指令 (1)
   - サイバーレジリエンス法 (2)

3-6. EU

1. 政策の全体像

2. 制度の調査結果
   - NIS2指令 (1)
   - サイバーレジリエンス法 (2)

EUにおける主なサイバーセキュリティ関連の規制/政策

2016年7月	**NIS指令[1] 制定**	• サイバーセキュリティに関するEU全体の規制 - 各加盟国のサイバーセキュリティ関連のリスク/インシデントへの対処能力の強化 (所管官庁やCSIRTの指定等) - エネルギー・輸送・金融等の重要インフラを運営する企業等に対してセキュリティ要件・インシデント届出を義務化 - 情報共有などEU域内の協力の強化 (協力グループの設置)
2019年6月	**EUサイバーセキュリティ法**	• 欧州全域で高い共通レベルのサイバーセキュリティを実現することを目的とするENISA[2]の権限強化・サイバーセキュリティ認証制度の整備 - ENISAはEUレベルでのサイバーセキュリティインシデントへの対処・協力を支援 - ICT製品、サービス、プロセスに対するEU全体のサイバーセキュリティ認証枠組みを導入
2020年12月	**サイバーセキュリティ戦略**	• サイバー脅威への強靭性を構築し、信頼できるデジタル技術から便益を取得 • EUが技術的な主権を確立するための手段・資源の活用・強化策を説明 - NISの改正、欧州サイバーシールド（セキュリティ・オペレーション・センター設置）、5Gネットワーク/インターネットに接続する機器のセキュリティ強化 (サイバーセキュリティ認証制度の連携等) • EUの価値観を共有する世界のパートナーとの協力の強化 (EU Cyber Diplomacy Network等) 等
1 **2022年11月**	**NIS2指令 制定**	• 対象スコープの大幅な拡大、サイバーセキュリティリスクマネジメントの強化、インシデント報告内容/期限の明確化、加盟国間での協力体制の強化 **詳細後述**
2 **2023年11月**	**サイバーレジリエンス法 草案暫定合意**	• SBOM[4]作成や更新プログラム提供等セキュリティ要件への適合（自己適合宣言/第三者認証） • 重要なデジタル製品について、低リスク製品でEUCCやEN規格対象外の製品・高リスク製品には第三者認証を要求 • 脆弱性の悪用やインシデント発見後24時間以内にENISAへの報告を義務化 **詳細後述**
2024年1月	**EUCC[3]**	• EU市場におけるICT製品、サービス、およびプロセスのサイバーセキュリティのレベルの向上を目的とした共通の認証

1. Directive on Security of Network and Information System 2. European Union Agency for Cybersecurity 3. European Union Cybersecurity Certification 4. Software Bill of Materials
Source: 経済産業省「EU NIS2指令概要」, EU Commission, "The EU Cybersecurity Act" , European Parliament, "Directive on security of network and information systems (NIS Directive)" ネットワーク・情報システムの安全に関する指令（NIS指令）―EU のサイバーセキュリティ対策立法― (ndl.go.jp), An EU Prime! EU adopts first Cybersecurity Certification Scheme – ENISA (europa.eu), ENISA, "EU Cybersecurity Certification",

3-6. EU

1. 政策の全体像

2. 制度の調査結果
   - NIS2指令 (1)
   - サイバーレジリエンス法 (2)

「NIS2指令」概要 [1/2]

法令等の名称

NIS2指令
(Network and Information Systems Directive 2)

制定時期

- 2016年8月　NIS指令適用開始
- 2020年12月　NIS指令の改正案が提出
- 2022年12月　官報掲載
- 2024年10月　国内法化期限/適用開始

制定の経緯

- NIS指令への問題点の指摘あり
  - NIS指令の対象が限定的
  - EUで事業を行うサイバー攻撃への耐性や共同の危機対応体制が不足
- 上記を踏まえ、新たな規定を盛り込んだ指令案を提出、NIS2指令として制定

妨害防止措置の概要

- 対象スコープの大幅な拡大
- サイバーセキュリティリスクマネジメントの強化
- インシデント報告内容/期限の明確化
- 加盟国間での協力体制の強化

対象者

EU域内で下記分野のサービスを提供する中規模 (従業員50名以上等)以上の主要エンティティ/重要エンティティ[1]

- 特に重要な分野 (Sectors of High Criticality) :
  エネルギー、運輸、銀行、金融市場インフラ、ヘルスケア、飲料水、下水、デジタルインフラ、ICTサービスマネジメント、公的サービス、宇宙
- その他の重要分野 (Other Critical Sectors) :
  郵便・宅配、廃棄物管理、化学品、食品、製造業 (医療機器、コンピュータ・電気電子・光学製品、機械、自動車・トレーラー、輸送機器)、デジタルプロバイダー、研究

※ 下線は新たに追加されたセクター

1. 分野や従業員等の規模により、主要エンティティ (Essential Entity) と重要エンティティ (Important Entity) を区別 (特に重要な分野の大企業 (従業員250名以上) はEssential Entity 等)
Source: EUR-Lex, "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance)", 経済産業省「EU NIS2指令概要」、国立国会図書館ウェブサイト (【EU】高度な共通水準のサイバーセキュリティ指令 (NIS2指令)の制定)

「NIS2指令」概要 [2/2]

事業者に対する義務規定

事業者登録義務

- 対象の事業者は、以下の情報を管轄当局に提出
  - 組織名称・商業登録番号
  - 住所・連絡先
  - 属しているセクター
  - 自社がサービスを提供する加盟国リスト

リスク管理対策実施義務

- 最新の技術水準に準拠し、関連する欧州基準および国際基準を考慮に入れ、かつ、「オールハザードアプローチ」に基づくかたちで、リスク管理対策を実施

インシデント発生時の報告義務

- 発生時、24時間以内にCSIRT[1]、管轄当局に初期報告
- 72時間以内に、インシデント初期評価を報告
- 発生後、1ヶ月以内に最終報告を実施

「リスク管理対策」の要素

以下の要素を含んだ対策を講じる必要あり

- リスク分析及び情報システムセキュリティに関する方針
- インシデントの処理
- バックアップ、災害復旧、危機管理等の事業継続性
- サプライチェーンのセキュリティ
- 開発・保守におけるセキュリティ対策 (脆弱性管理、情報開示)
- リスク管理策の有効性評価のための方針及び手順
- サイバーセキュリティトレーニング
- 人材のセキュリティ、アクセス管理方針、資産管理 等

罰則

規定されているリスク管理対策・インシデント発生時の報告を怠った場合、事業者区分ごとに以下罰金が発生

- 主要エンティティ (Essential Entity)
  - 最大1,000万ユーロ、又は前会計年度における当該企業の全世界における総売上高の最大2%の罰金

- 重要エンティティ (Important Entity)
  - 最大700万ユーロ、又は前会計年度における当該企業の全世界における総売上高の最大1.4%の罰金

1. cybersecurity (single points of contact) and computer security incident response team：CSIRTとは、incident対応に責任を負う団体で、各加盟国が指定・設置する。国内におけるサイバー脅威、脆弱性、インシデントの監視及び分析等を任務とする

Source: EUR-Lex, "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance)"、国立国会図書館ウェブサイト (【EU】高度な共通水準のサイバーセキュリティ指令 (NIS2指令)の制定)

「NIS2指令」詳細 [1/12]：特に重要な分野

11セクターにわたり、特に重要な分野 (Sectors of high criticality) を特定
この分野の大企業 (従業員250名以上等) の企業が、主に主要エンティティ (Essential Entity) となる

対象分野
(特に重要な分野)

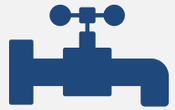
1. 
エネルギー

2. 
運輸

3. 
銀行

4. 
金融市場インフラ

5. 
医療

6. 
飲料水

7. 
下水

8. 
デジタルインフラ

9. 
ICTサービス
マネジメント

10. 
公的サービス

11. 
宇宙

Source: EUR-Lex, "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance)"

「NIS2指令」詳細 [2/12]：その他の重要な分野

7セクターにわたり、その他の重要分野が指定。前頁の「特に重要な分野」における中規模企業や、
下記「その他の重要な分野」の中規模以上の企業等が、主に重要エンティティ(Important Entity) となる[1]

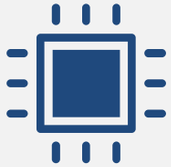
対象分野
(その他の重要分野)

1. 
郵便・宅配

2. 
廃棄物管理

3. 
化学品

4. 
食品

5. 
製造業

6. 
デジタルプロバイダ

7. 
研究

Source: EUR-Lex, "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance)"

「NIS2指令」詳細 [3/12]：特に重要な分野の詳細 [1/4]

セクター	サブセクター	エンティティの種類 (概要)
① エネルギー 	電気	• 電気事業/供給/配電/送電/発電に携わる事業者 • 指定された電気市場参加者
	地域冷暖房	• 地域冷暖房事業者
	石油	• 石油輸送パイプライン事業者 • 石油生産/精製/処理施設/貯蔵/配送事業者 • 緊急時用石油備蓄事業者(Central Stockholding Entity)
	ガス	• 供給事業/供給/配給/配送/貯蔵/施設運営事業者
	水素	• 水素の製造/貯蔵/分配に携わる事業者
② 運輸 	航空	• 航空会社 • 空港管理機関 • 交通管制事業者
	鉄道	• 鉄道・鉄道インフラ管理事業者/鉄道事業者
	海運	• 内陸・海上・沿岸の旅客・貨物水運事業者 • 湾岸を管理・運営する事業者 • 船舶交通事業者
	道路	• 交通管理を担当する道路当局 • 高度道路交通システムの運営事業者

Source: EUR-Lex, "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance)"

「NIS2指令」詳細 [4/12]：特に重要な分野の詳細 [2/4]

セクター	サブセクター	エンティティの種類 (概要)
③ 銀行 		• 信用機関 (Credit Institutions)
④ 金融市場インフラ 		• 取引所の運営者 • 中央清算機関 (CCPs)
⑤ 医療 		• 医療提供者 • EU基準研究所 (EU Reference Laboratories) • 医薬品の研究開発活動を行う事業者 • 基礎医薬品および医薬品製剤を製造する事業者 • 公衆衛生上の緊急時に重要と考えられる医療機器を製造する事業者
⑥ 水道インフラ 		• 飲料水の供給業者および販売業者 – 他の業務も行っており、業務全般において上記が主要なものでない事業者を除く

Source: EUR-Lex, "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance)"

「NIS2指令」詳細 [5/12]：特に重要な分野の詳細 [3/4]

セクター	サブセクター	エンティティの種類 (概要)
7 下水インフラ 		• 都市廃水/生活廃水/産業廃水を収集/処分/処理する事業者 – 業務全般において上記が主要なものでない事業者を除く
8 デジタルインフラ 		• インターネットエクスチェンジポイントプロバイダー • DNSサービスプロバイダー • TLDネームレジストリ • クラウドプロバイダー • データセンターサービスプロバイダー • コンテンツ配信ネットワーク運営者 • トラストサービスプロバイダー • 公衆電子通信ネットワーク事業者
9 ICTサービスマネジメント 		• マネージドサービスプロバイダー • マネージドセキュリティサービスプロバイダー

Source: EUR-Lex, "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance)"

「NIS2指令」詳細 [6/12]：特に重要な分野の詳細 [4/4]

セクター	サブセクター	エンティティの種類 (概要)
10 公的サービス 		• 中央政府の行政機関 • 地方自治体の行政機関
11 宇宙 		• 宇宙関連のサービス提供をサポートする地上インフラの事業者 – 電機通信ネットワークプロバイダーを除く

Source: EUR-Lex, "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance)"

「NIS2指令」詳細 [7/12]：その他の重要分野の詳細 [1/3]

セクター	サブセクター	エンティティの種類 (概要)
① 郵便・宅配 		• 郵便・宅配業者
② 廃棄物管理 		• 廃棄物管理活動を行う事業者 - 廃棄物管理活動が主要業務でない事業者は除く
③ 化学品 		• 化学物質の製造を行う事業者 • 化学物質・合成物質の流通を行う事業者
④ 食品 		• 卸売流通/工業生産/加工に従事する食品企業

Source: EUR-Lex, "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance)"

「NIS2指令」詳細 [8/12]：その他の重要分野の詳細 [2/3]

セクター	サブセクター	エンティティの種類 (概要)
5 製造業 	医療機器および体外診断用医療機器	• 医療機器製造事業者 • 体外診断用医療機器製造事業者 – 公衆衛生上の緊急時に重要と考えられる医療機器を製造する事業者を除く
	コンピューター/電子機器/光学製品	• コンピューター関連機器・電子機器・光学製品の製造事業者
	電気機器	• 電気モーター・発電機等電気関連機器の製造事業者
	機械および装置	• 金属成形機・パワーツール等機械および装置の製造事業者
	自動車/トレーラー/セミトレーラー	• 自動車/トレーラー/セミトレーラーの部品・車体等の製造事業者
	その他輸送機器	• 船舶・航空機等その他輸送機器の製造事業者
6 デジタルプロバイダ 		• オンライン・マーケットプレイスのプロバイダー • オンライン検索エンジンのプロバイダー • ソーシャル・ネットワーキング・サービス・プラットフォームのプロバイダー

Source: EUR-Lex, "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance)"

「NIS2指令」詳細 [9/12]：その他の重要分野の詳細 [3/3]

セクター	サブセクター	エンティティの種類 (概要)
7 研究		• 研究機関

Source: EUR-Lex, "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance)"

「NIS2指令」詳細 [10/12]：登録義務/リスク管理対策実施義務

事業者登録義務

- 対象事業者は、以下情報を当局に提出
  - 組織名称・商業登録番号
  - 住所・連絡先
  - 属しているセクター
  - 自社がサービスを提供する加盟国リスト

リスク管理対策実施義務

- 「オール・ハザード・アプローチ[1] (all-hazard approach)」に基づくかたちで、少なくとも以下の項目を含むリスク管理対策を実施。実施の際は、最新の技術水準に準拠し、関連する欧州基準・国際基準を考慮する必要
  - リスク分析及び情報システムセキュリティに関する方針
  - インシデント処理
  - 事業継続性 (バックアップ管理、災害復旧、危機管理等)
  - サプライチェーンセキュリティ
    (各組織とその直接のサプライヤ/サービス提供者との関係に係るセキュリティに関するものを含む)
  - ネットワーク及び情報システムの取得/開発/保守におけるセキュリティ・サイバーセキュリティリスク管理対策の有効性を評価するための方針及び手順
  - 基本的なサイバー衛生の実践とサイバーセキュリティ研修
  - Cryptography、及び適切な場合にはEncryptionの使用に関する方針及び手順
  - 人的資源のセキュリティ/アクセス管理方針/資産管理
  - 多要素認証又は継続的認証ソリューション、保護された音声/ビデオ及びテキスト通信/保護された緊急通信システムの使用等

1. 一般的には、ネットワークや情報システムを防護する際、物理的な防護も含め、サービス提供等の継続に必要なすべての要素を考慮すべき、というもの

Source: EUR-Lex, "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance)"

(参考) NIS2指令と国家安全保障の関係について

本指令は、サイバーセキュリティ達成を目的とした対策を定めるもの、という位置づけ
国家安全保障に関わる部分については、適用されない旨の規定あり

位置づけ (第1条　主題)

CHAPTER I　GENERAL PROVISIONS
Article 1　Subject matter
1.　This Directive lays down measures that aim to achieve a high common level of cybersecurity across the Union, with a view to improving the functioning of the internal market.
(仮訳)
1. この指令は、域内市場の機能を改善するために、**連合全体で共通の高いレベルのサイバーセキュリティを達成することを目的とした対策**を定めている

各国での取り扱い (第2条　範囲)

6.This Directive is without prejudice to the Member States' responsibility for safeguarding national security and their power to safeguard other essential State functions, including ensuring the territorial integrity of the State and maintaining law and order.
(仮訳)
6.本指令は、**国家安全保障を保護する加盟国の責任、および国家の領土保全の確保や法秩序の維持**など、国家のその他の**重要な機能を保護する加盟国の権限を損なうものではない**

7.
This Directive does not apply to public administration entities that carry out their activities in the areas of national security, public security, defence or law enforcement, including the prevention, investigation, detection and prosecution of criminal offences.
(仮訳)
7.
本指令は、国家安全保障、公安、防衛、法執行（犯罪の予防、捜査、摘発、訴追を含む）の分野で活動を行う行政機関には適用されない。

Source: EUR-Lex, "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance)"

「NIS2指令」詳細 [11/12]：インシデント発生時の報告義務

重大なインシデントが発生した場合の報告内容・タイムラインを規定

報告義務の概要

- 重大なセキュリティインシデントが発生した場合に、自国のCSIRT[1]または所管当局に報告する義務を負う
- 所管当局が通知を受領した場合、当該通知をCSIRTに転送しなければいけない
- 重大なセキュリティインシデントとは以下を指す
  - サービスの運営に深刻な混乱を引き起こした、または引き起こす可能性がある、あるいは当該組織に財務的損失をもたらした事象
  - 他の自然・人または法人に物質的・非物質的に重要な損害を与えた、または与える可能性がある事象

報告内容・タイムライン

- 重大なインシデント認識後、24時間以内
  - インシデントが不法行為または悪意ある行為による疑いがあるか、また国境を越えた影響を及ぼす可能性があるかどうかを含んだ、早期報告を実施
- 重大なインシデント認識後、72時間以内
  - 早期報告の情報を更新し、その重大性と影響についての初期評価を提供
- CSIRT・統括当局の要請に応じ、関連する状況の更新に関する中間報告を実施
- 重大なインシデント認識後、1ヶ月以内に以下の内容を含む最終報告を実施
  - インシデントの詳細な説明 (インシデントの重大性及び影響含む)
  - インシデントの契機となったと思われる脅威又は根本的な原因の性質に関する情報
  - 講じられた是正措置及び現在実施中の是正措置に関する情報
  - インシデントの国境を越えた影響 (該当する場合)

1) cybersecurity (single points of contact) and computer security incident response team;各加盟国に設置されたインシデント対応チーム

Source: EUR-Lex, "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance)"

「NIS2指令」詳細 [12/12]：罰則

リスク管理対策・インシデント発生時の報告を怠った場合、エンティティの類型ごとに罰則が設定されている

	対象者	
	主要エンティティ	重要エンティティ
罰則	最大1,000万ユーロ、又は前会計年度における当該企業の全世界における総売上高の最大2%の罰金	最大700万ユーロ、又は前会計年度における当該企業の全世界における総売上高の最大1.4%の罰金

Source: EUR-Lex, "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance)"

(参考) NIS2指令の各国国内法制化

NIS2指令の第41条1項に基づき、EU加盟国は2024年10月施行を目標に国内法制化を検討中である

NIS2指令 第41条1項

- By 17 October 2024, Member States shall adopt and publish the measures necessary to comply with this Directive. They shall immediately inform the Commission thereof.
- They shall apply those measures from 18 October 2024.

(仮訳)

- **2024年10月17日までに、加盟国は本指令を遵守するために必要な措置を採択し、公表**するものとする。加盟国は直ちにその旨を欧州委員会に通知しなければならない
- **加盟国は2024年10月18日より当該措置を適用**する

参考) EU指令の位置づけ (European Commissionサイト参照)

- **Directives** require EU countries to achieve a certain result, but leave them free to choose how to do so.
- EU countries must adopt measures to incorporate them into national law (transpose) in order to achieve the objectives set by the directive…
  - Transposition into national law must take place by the deadline set when the directive is adopted (generally within two years).

(仮訳)

- 指令は、EU諸国に一定の結果を達成することを求めるものの、達成方法を選択する自由を残している
- EU諸国は、指令が定めた目的を達成するために、**指令を国内法に組み込むための措置を採択**
  - 国内法への移管は、指令が採択された際に定められた期限（通常2年以内）までに行わなければならない

Source: EUR-Lex, "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance)", European Commission, "Types of EU law"

3-6. EU

1. 政策の全体像

2. 制度の調査結果
   - NIS2指令 (1)
   - サイバーレジリエンス法 (2)

サイバーレジリエンス法 (草案) の概要 [1/4]：名称/経緯等

法令等の名称

サイバーレジリエンス法
EU Cyber Resilience Act (CRA)[1]

制定時期

- 2022年9月　草案提出
- 2023年11月　暫定合意
- 2024年～　発効見込み
  ※ 発行後3年で適用

制定の経緯

- デジタル製品に関する国境を越えた**包括的なサイバーセキュリティ要件の規定**を目的
- **NIS-2指令を補完**するものであり、より安全なハードウェア及びソフトウェア製品を確保するためのサイバーセキュリティ要件を義務付けるもの

対象製品

- デジタル要素を備えた全ての製品
  (デバイス/ネットワークに直接的/間接的に接続されるもの含む)
- 以下の規則の対象製品は適用除外
  - 医療機器規則、体外診断用医療機器規則、民間航空機規則、自動車の型式承認規則の対象製品
  - 国家安全保障に関するデジタル製品や軍事目的・機密情報処理目的のもの
  - SaaSなどのソフトウェアサービス 等

主な規制の内容

- 製造事業者に対し、レベルに応じ下記の義務を課す
  - 「**デジタル製品**」は、**自己適合宣言**か**第三者認証**を選択
  - **「重要なデジタル製品」**は、**低リスク製品**かつEUCC/EN規格対象外の製品は**第三者認証**を、**高リスク製品**には、**第三者認証**を求める
  - 適合性評価証明書にはEU適合宣言書 (CEマーク)/EUCC証明書を活用
  - 脆弱性の悪用やインシデント発見後24時間以内にENISA[2]への報告を義務化

Note: 法案の内容等は、2022年9月時点のもの。次頁以降も同じ　1. 正式名称は、"Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020" であり、Regulation (規則) に分類され、国内法への移行は必要ない　2. 23年11月の暫定合意では、ENISAではなく各国当局が最初の通知先となる旨言及あり　Source: EUR-Lex, "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020", EU Council, "Cyber resilience act: Council and Parliament strike a deal on security requirements for digital products", Cyber resilience act: Council and Parliament strike a deal on security requirements for digital products - Consilium (europa.eu), 経済産業省「EUサイバーレジリエンス法 (草案概要)」,

サイバーレジリエンス法 (草案) の概要 [2/4]：製造事業者の義務 (概要) [1/2]

1. **[セキュリティ特性要件の遵守]** デジタル製品を市場に出す際、附属書IのSection 1に規定されている「セキュリティ特性要件」を遵守し、設計・開発・製造 されていることを確認する
2. **[リスクアセスメントの実施]** サイバーセキュリティ上のリスクアセスメントを実施し、リスクを最小化するため、その結果を設計・開発・製造・流通・メンテナンスの各段階において、考慮に入れる
3. **[アセスメントの技術文書への取り込み]** デジタル製品を市場に出す際、上記のリスクアセスメントの結果を、技術文書に含める
4. **[第三者提供品の取り扱い]** 第三者から提供された構成部品を組み込む際には、デューデリジェンスを実施し、その部品により製品のセキュリティを損なわないことを確保する
5. **[サイバーセキュリティに係る体系的な文書化]** 特性やリスクに比例した方法で、デジタル製品のサイバーセキュリティに係る側面を体系的に文書化する
6. **[脆弱性への継続的な対処]** 製品寿命又は市場に出した後5年間のうち短い期間の間、付属書 I のSection 2に適合するかたちで製品の脆弱性に効果的に対処する。製造業者は脆弱性開示ポリシー等、適切なポリシーや手続きを有するとともに、潜在的な脆弱性を処理し、是正する
7. **[技術文書の作成]** 市場に出す前に、技術文書を作成する。対応する適合性評価手続きを行い、適合性が実証された場合はCEマーキングを付する
8. **[関連文書の保存]** 市場に出した後10年間、技術文書と (該当する場合は) EU適合性証明書を、市場監視当局が用いることができるよう保管する
9. **[適合性維持のための手順の整備]** 製造工程の中で適合性を維持するための手順が整備されていることを確認する。製造事業者は、開発や製造工程や設計、製品の特性の変化や、関連する欧州の認証等に十分に考慮する
10. **[情報の表示]** 附属書IIに規定される情報と指示が、電子的又は物理的に製品に付属していることを確保する。それらの情報と指示は、わかりやすく言葉で明確に書かれていなければならない

Source: EUR-Lex - "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020", 経済産業省「EUサイバーレジリエンス法 （草案概要）」

サイバーレジリエンス法 (草案) の概要 [3/4]：製造事業者の義務 (概要) [2/2]

11. **[EU適合性証明書の提供]** EU適合性証明書を提供するか、その情報を記載したURLを提供する
12. **[製品のリコール]**製品寿命又は市場に出した後5年間のうち短い期間の間、附属書I「セキュリティ特性要件」を遵守しない場合、直ちに必要な是正措置を講じ、製品の撤回またはリコールを行う
13. **[監視当局への文書等の提出]** 市場監視当局からの要求に応じ、製品の適合性について証明する情報や文書を、わかりやすい言語で、紙又は電子的に提出する
14. **[操業停止前の通知]** 操業を停止することで本規制の義務を遵守できなくなる場合、操業停止前に市場監視当局に状況を報告するとともに、可能なあらゆる手段でユーザーに通知する
15. **[SBOM[1]]** 欧州委員会は実施法令 (implementing acts) の中で、SBOMの形式と要素を指定することができる

1. Software Bill of Materials

Source: EUR-Lex - "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020", 経済産業省「EUサイバーレジリエンス法 （草案概要）」

(参考) 項目1の付属文書

付属書 I のSection 1にて、デジタル製品のデザイン・製造・配布・運用等に関するセキュリティ特性要件を規定

付属書I Section1 セキュリティ特性要件（仮訳）

1. デジタル要素を含む製品は、**リスクに応じた適切なレベルのサイバーセキュリティを確保するように設計、開発、製造**されなければならない
2. デジタル要素を含む製品は、**悪用可能な既知の脆弱性がない状態で提供**されなければならない
3. **第10条(2)で言及されたリスクアセスメントに基づき**、該当する場合、デジタル要素を含む製品は以下の規定に従う
   - (a) 製品を**元の状態にリセットできる設定**を含め、**デフォルトで安全な設定**で提供する
   - (b) 適切な管理メカニズムにより**認証・アイデンティティ・アクセス管理システム等を不正アクセスから確実に保護**する
   - (c) 最新メカニズムや静止時・転送時の関連データ暗号化等により**保存・送信・その他の方法で処理された個人情報・その他の情報の機密性を保護**する
   - (d) 保存・送信・その他の方法で処理された個人またはその他の**データ・コマンド・プログラムおよび設定の整合性**を、**ユーザーによって許可されていない操作や変更から保護**し、**破損について報告**する
   - (e) 適切かつ関連性があり、**製品の使用目的に関して必要なものに限定**された**個人・その他のデータのみを処理**する(データの最小化)
   - (f) **サービス拒否攻撃に対する回復力と緩和**を含め、**必要不可欠な機能の可用性を保護**する
   - (g) **他のデバイスやネットワークが提供するサービスの可用性に与える悪影響を最小限**に抑える
   - (h) 外部インターフェイスを含む**攻撃面を制限するように設計、開発、製造**する
   - (i) 適切な悪用緩和の仕組みと技術を用いて、**インシデントの影響を軽減するように設計、開発、製造**する
   - (j) データ、サービス、機能へのアクセスや変更を含む**、関連する内部活動の記録/監視**により、**セキュリティ関連情報を提供**する
   - (k) **セキュリティ更新を通じて脆弱性に対処**できるようにする、また該当する場合は**自動更新や利用可能な更新のユーザーへの通知を通じて、脆弱性に対処**できるようにする

Source: EUR-Lex - "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020"

(参考) 項目6の付属文書

付属書I の Section 2にて、適切なポリシー・セキュリティアップデート・メカニズム等の脆弱性ハンドリング要件を規定

付属書I Section2 脆弱性ハンドリング要件（仮訳）

デジタル製品の製造者は以下の規定に従うこと：

1. **製品に含まれる脆弱性とコンポーネントを特定**し、**一般的に使用され、機械が読み取り可能な形式で、少なくとも製品の最上位レベルの依存関係を網羅するソフトウェア部品表を作成**する
2. デジタル要素を含む製品にもたらされるリスクに関連して、**セキュリティ更新プログラムを提供**することを含め、**脆弱性に遅滞なく対処・是正**する
3. デジタル要素を含む製品のセキュリティについて、**効果的かつ定期的なテストとレビューを実施**する
4. セキュリティ・アップデートが利用可能になったら、**修正された脆弱性に関する情報を公開**する。これには、**脆弱性の説明、影響を受けるデジタル要素を含む製品を特定するための情報、脆弱性の影響、深刻度、脆弱性を修正するための情報**を含む
5. **協調的な脆弱性開示に関するポリシーを導入・実施**する
6. デジタル要素を含む製品で**発見された脆弱性を報告するための連絡先を提供**することを含め、デジタル要素を含む製品およびその製品に含まれる**サードパーティコンポーネントの潜在的な脆弱性に関する情報の共有を促進する手段**を講じる
7. 悪用可能な脆弱性がタイムリーに修正または緩和されるよう、デジタル要素を含む製品の**アップデートを安全に配布する仕組みを提供**する
8. 特定されたセキュリティ問題に対処するための**セキュリティパッチやアップデートが入手可能な場合は、遅滞なく、かつ無償で配布**し、**潜在的な対処方法を含む関連情報をユーザーに提供する勧告メッセージを添付**する

Source: EUR-Lex - "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020"

サイバーレジリエンス法 (草案) の概要 [4/4]：インシデント報告義務

1. デジタル製品の中に積極的に悪用された脆弱性を発見してから24時間以内にENISA[1]に通知する
   - 通知には、その脆弱性の情報、講じられた是正措置・緩和措置を含む
   - ENISAは正当なサイバーセキュリティリスク等の事由が無い限り、NIS2指令に基づいて脆弱性開示目的で指定されているCSIRTに遅滞なく転送し、市場監視当局に知らせる
2. 製品のセキュリティに影響を与えるインシデントを認識してから24時間以内にENISAに通知する。インシデント通知には、インシデントの深刻度・影響、国境を越える影響があるか等を含む
   - ENISAは、正当なサイバーセキュリティリスク等の事由が無い限り、NIS2指令に基づいて指定されたコンタクト先に通知を遅滞なく転送し、市場監視当局にも知らせる
3. 運用レベルでの大規模なインシデントや危機管理に関する場合、ENISAはその情報を NIS2指令に基づいて設立されたEU CyCLONe (欧州サイバー危機連絡組織ネットワーク) に提出する
4. 製造業者は、上記インシデントを認識したのち、インシデントについて/必要に応じてインシデントの影響を緩和するための是正措置について、ユーザーに遅滞なく通知する
5. 欧州委員会は、通知された情報の種類、形式、手順を更に指定することができる
6. ENISAは、NIS2指令における「協力グループ」に対して、受領した情報を基に、サイバーセキュリティに関する最新の傾向を技術レポートとして2年に1度提出する
7. 製造業者が製品に統合されているオープンソースコンポーネント等の脆弱性を特定した場合、その脆弱性をコンポーネントを維持する個人/団体に報告する

1. The European Union Agency for Cybersecurity

Source: EUR-Lex - "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020", 経済産業省「EUサイバーレジリエンス法 （草案概要）」

(参考) ENISAの概要

名称	• ENISA (The European Union Agency for Cybersecurity)
長官	• Juhan Lepassaar（Executive Director）
設立時期	• 2004年
背景/目的	• 欧州全域で高い共通レベルのサイバーセキュリティを実現することを目的とするEUの機関 • EUのサイバー政策に貢献し、サイバーセキュリティ認証制度によってICT製品/サービス/プロセスの信頼性を高め、加盟国およびEU機関と協力し、欧州が未来のサイバー課題に備えることを支援 • 知識の共有/能力開発/意識向上を通じ、主要な利害関係者と協力/コネクテッド・エコノミーに対する信頼を強化/EUのインフラの回復力の向上を通じて欧州の社会と市民のデジタルセキュリティを維持
主な活動内容	• 加盟国のサイバーセキュリティ関係者とEUの諸機関・機関との積極的な協力の促進 • 欧州全体でサイバーセキュリティ政策の断片化を回避し、首尾一貫したアプローチを確保 • 迅速な対応とあらゆるレベル (戦略、作戦、技術、コミュニケーション) における取組の適切な調整のために、加盟国とEU機関との効果的な協力を確保 • サイバーセキュリティの能力と才能の育成への投資 • デジタル・ソリューションと広範なデジタル環境に対する信頼の向上 • ステークホルダー間のプロセス導入に繋がる構造化された対話の確保 • EUのサイバーセキュリティエコシステム内における情報と知識の共有・拡大

Source: ENISA HPより