今さら聞けないサイバー関連海外法制

2024/11/26

PwCコンサルティング合同会社　パートナー
丸山　満彦

自己紹介

丸山満彦

PwCコンサルティング合同会社 パートナー

情報セキュリティ大学院大学 客員教授

専門分野・担当業界

- サイバーセキュリティ、ITリスク

略歴

- 25年にわたり製造業、サービス業、金融機関、政府などの幅広い業種に対するサイバーセキュリティ、ITリスク分野のコンサルティング、監査に携わる。内閣官房に出向し、内閣官房サイバーセキュリティセンターの立ち上げ、政府統一基準の策定、改訂に関与。ISMS制度の立ち上げ、普及にも関わる。内閣官房、総務省、経済産業省などの有識者委員に多数就任しているほか、複数のセキュリティ関連団体の理事、監事も務める。
- 情報セキュリティ文化賞（2021年）受賞

資格

- 公認会計士（CPA）
- 公認情報システム監査人（CISA）

本日の概要

今さら聞けないサイバー関連海外法規制

海外の法規制は日本でビジネスを行なっている企業においても他人事ではなく、想定外のところでその規制の対象となることがあります。特に欧米の法規制では違反した場合に**厳しい罰則**が課せられる場合もあり、日本企業においても、そのような法規制の内容をしっかり把握し、備える必要があります。そこで今回は、日本企業におけるIT関連の実務担当者が最低限知っておくべき海外、特にヨーロッパを中心とした「今さら聞けない」法規制、例えば、**GDPR**（General Data Protection Regulation、EU一般データ保護規則）や**NIS2指令**（Network and Information Security Directive 2）などを、その背景も含めて概説します。

目次

1.この法律や規則、どういう内容か知っていますか？

1. この法律や規則、どういう内容か知っていますか？
2. インターネットを巡ってどのようなことが起こっているのか？

2. 各国・地域がインターネットに対してどのような思惑をもっているのか考えてみる

1. 米国の立場（インターネットの産みの親、IT企業を多数持つ自由と公正を大切にする合衆国）
2. 欧州の立場（貴族を倒して得た民主主義と戦禍を乗り越えて得た人権を重視する国々の連合体）
3. 中国の立場（共産党独裁による14億人の多民族国家）
4. 日本の立場

3. 個人データ保護の法律 ― デジタル時代だからこそ

1. 何から何を守りたいのか？
2. 欧州の高い人権意識が個人データ保護法制に影響している
3. 欧州で成功し、ブリュッセル効果で世界中に
4. GDPRはどのような法律か？
5. 日本の個人情報保護法との違い

4. 安全保障とサイバーセキュリティ ― ネット社会の宿命

1. 何から何を守りたいのか？
2. NIS2指令はどのような規制か？
3. 身代金支払報告義務を求める米国重要インフラ向けサイバーインシデント報告法
4. （参考）日本の経済安全保障推進法：リスク管理措置の概要

5. IoTに関わる規制 ― 普及と安全のバランス

1. 何から何を守りたいのか？
2. 欧州のアプローチ、米国のアプローチ、日本のアプローチ
3. IoTセキュリティは認証制度により担保される時代に
4. 簡易な基準で早期に規制にした英国
5. 法制化で網羅的に対応する欧州
6. マーケットの力で対応する米国
7. 日本は政府主導のガイドライン対応
8. さて、相互認証はできるのか？

6. AIに関わる規制 ― 本格的に普及する前に法制化

1. 何から何を守りたいのか？
2. AI規制を考えない国はない
3. 先行して原則を示したOECD
4. リスクに応じた法規制を導入したEU
5. 国家による総合的なAI規制を試みる中
6. 日本はガイドライン対応でどこまで耐えられるのか？

7. まとめ

1. ざっと挙げてみるだけでもこれだけの法令があります
2. なりたい社会になるように法律は作られる
3. 私たちはどのような社会を目指しているのか？

1

この法律や規則、どういう
内容か知っていますか？

この法律や規則、どういう内容か知っていますか？

EU: General Data Protection Regulation (GDPR)

EU：一般データ保護規則

米国：カリフォルニア州消費者プライバシー法

中国：個人情報保護法

EU: Network and Information Security Directive 2 (NIS2)

NIS2指令

US: Cyber Incident Reporting For Critical Infrastructure Act of 2022

米国：サイバーインシデント報告法

中国：ネットワークセキュリティ法

EU: Cyber Resilience Act

サイバーレジリエンス法

UK: Product Security and Telecommunication Infrastructure Act (PSTI)

英国：PSTI法

US: Executive Order on Improving the Nation's Cybersecurity

米国：大統領令14028

EU: AI Act

AI法

中国：インターネット情報サービス深度合成アルゴリズム管理規定

インターネットを巡ってどのようなことが起こっているのか？

インターネット上も実世界の法律
が適用できるので、
インターネットは公共空間として、
自由であるべき。

インターネットにも国家主権を
及ぼすべき。

2

各国・地域がインターネットに対してどのような思惑をもっているのか考えてみる

米国の立場

インターネットの産みの親、IT企業を多数持つ自由と公正を大切にする合衆国

民間主導

米国は、インターネットの管理を政府ではなく民間企業や非営利団体に委ねることを重視。特に、ICANNの設立により、インターネット資源の管理を民間主導で行う体制が整えられた

自由でオープン

表現の自由や情報の自由な流通を保護する。政府の介入を最小限に抑え、民間企業や個人が自由にインターネットを利用できる環境を維持することを目指す

技術革新と規制のバランス

技術の進化を妨げないようにしながらも、必要な規制を導入して消費者保護や市場の公正性を確保することを目指す

民主主義を守る

サイバー上の脅威から民主主義の社会を守る

サイバーセキュリティとプライバシーも配慮

サイバー攻撃からの国民の保護も重視する。政府、企業に対するセキュリティ基準の設定や、消費者のデータ保護も強化

国際協力と多国間アプローチ

マルチステークホルダーアプローチを推進し、政府、民間企業、技術コミュニティ、市民団体などが協力してインターネットの管理に関与する考え方。

サイバーを含むさまざまな活動を国際協力のもと実施する

欧州の立場

貴族を倒して得た民主主義と戦禍を乗り越えて得た人権を重視する国々の連合体

人権保護の重視

技術の不適切な利用による人権侵害などが起こらないようにする（個人データ保護、AI法）

デジタル市場の公正性

競争の促進による消費者保護。デジタル市場法（DMA）やデジタルサービス法（DSA）などの導入

民主主義を守る

サイバー上の脅威から民主主義の社会を守る

サイバーセキュリティも配慮

サイバー攻撃からの国民の保護も重視する。政府、企業に対するセキュリティ基準の設定も強化

国際協力と多国間アプローチ

マルチステークホルダーアプローチを推進し、政府、民間企業、技術コミュニティ、市民団体などが協力してインターネットの管理に関与する考え方。

サイバーを含むさまざまな活動を国際協力のもと実施する

EU Values（欧州の価値観）を守るため

EUの価値観
EU Values

人間の尊厳	自由
民主主義	平等
法の支配	人権

1600年代—1800年代

絶対王政　国王常備軍・王権神授説

- 大航海時代
- 重商主義
- 帝国主義

- 英国：　1688年：**名誉革命**・権利の章典（絶対王政から立憲君主制）
- フランス：　1789年：**フランス革命**（絶対王政から共和制）
- ドイツ：　1918年：**ドイツ革命**（ワイマール共和制、**ナチ**の台頭、**ホロコースト**）

The EU values　https://ec.europa.eu/component-library/eu/about/eu-values/

中国の立場

共産党独裁による14億人の多民族国家

中国共産党独裁の国家

中華人民共和国憲法は、中国共産党による国家や社会への指導が明記されており、政策は、中国共産党の決定に基づき、中央人民政府（国務院）と地方政府により執行される。

社会主義革新価値観の重視

社会主义核心价值观

1. 国家が目標とするべき価値観：**富強・民主・文明・和諧**
2. 社会で大事にするべき価値観：**自由・平等・公正・法治**
3. 一人ひとりが守るべき価値観：**愛国・敬業・誠信・友善**

サイバー主権

各国が自国のインターネット空間を管理・統制する権利を持つべきだという考え方。インターネットの管理は国家の主権の一部と位置づけ、国内のインターネット企業やユーザーに対する厳格な規制を行う。

国家によるインターネットの管理と監視

国家によるインターネットの管理と監視を強化するための法律や規制を導入。サイバーセキュリティ法やデータセキュリティ法などによる国家の安全と社会の安定の確保を図る。

日本の立場

基本は、民主主義国家である、**米国、欧州と同じ**スタンス。

しかし、**安全保障の観点から、個人の権利利益の保護がおろそかにならないように注意**が必要？

欧米と同程度、民主主義に対する意識が高いのか？

欧米と同程度、プライバシー保護の意識が高いのか？

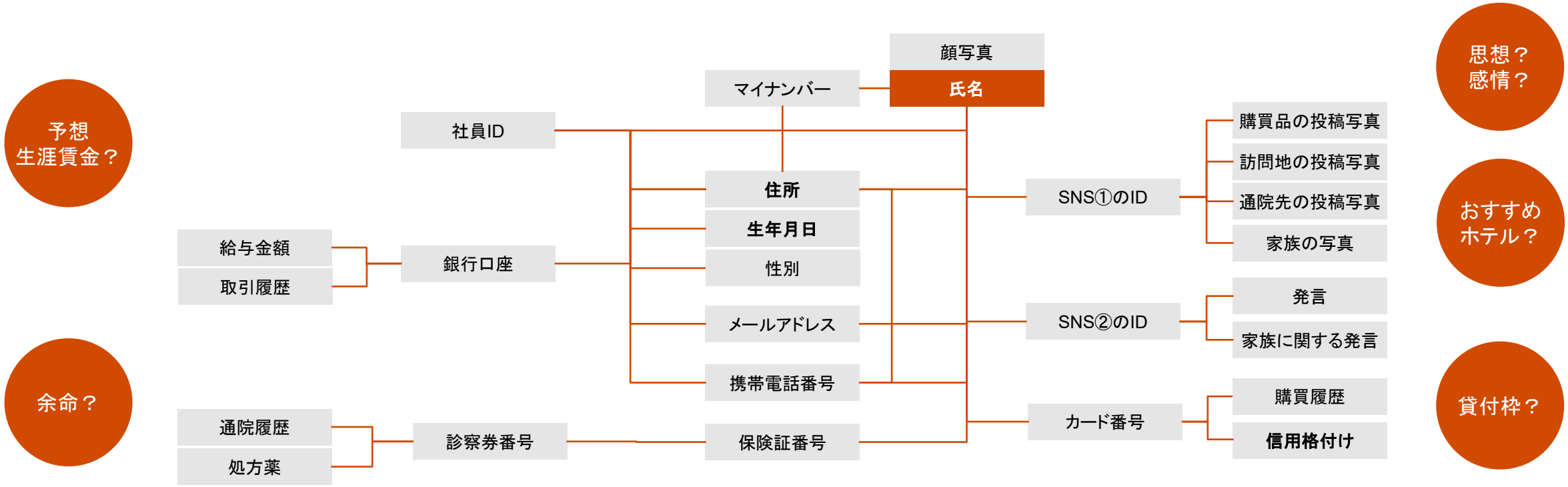
3

個人データ保護の法律

デジタル時代だからこそ

何から何を守りたいのか？

デジタル社会では、個人データを紐づけて収集蓄積し、評価を含むさまざまな分析に利用できるが、その結果が本人の意思と反する場合…



欧州の高い人権意識が個人データ保護法制に影響している

欧州人権条約

第8条

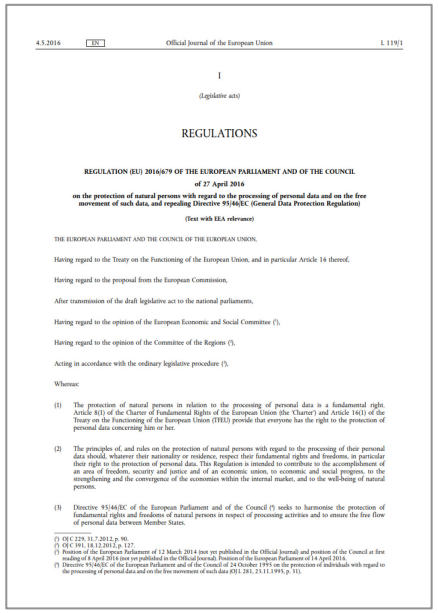
私生活及び家族生活の尊重を受ける権利

1　すべての者は、その私的及び家族生活、住居ならびに通信の尊重を受ける権利を有する。

2　この権利の行使に対しては、法律に基づき、かつ、国の安全、公共の安全もしくは国の経済的福利のため、また、無秩序もしくは犯罪の防止のため、健康もしくは道徳の保護のため、または他の者の権利及び自由の保護のため、民主的社会において必要なもの以外のいかなる公の機関による介入もあってはならない。

欧州人権条約（European Convention on Human Rights, ECHR）は、1950年に欧州評議会（Council of Europe）によって採択され、1953年に発効した。

1995年に採択されたデータ保護指令（Data Protection Directive, 95/46/EC）を改正する形で、個人データ保護規則 (General Data Protect Regulation) が、2016年に制定され、2018年に施行された。



4.5.2016 EN Official Journal of the European Union L 119/1

I

(Legislative acts)

REGULATIONS

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 27 April 2016

on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee (1),

Having regard to the opinion of the Committee of the Regions (2),

Acting in accordance with the ordinary legislative procedure (3),

Whereas:

(1) The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.

(2) The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data. This Regulation is intended to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons.

(3) Directive 95/46/EC of the European Parliament and of the Council (5) seeks to harmonise the protection of fundamental rights and freedoms of natural persons in respect of processing activities and to ensure the free flow of personal data between Member States.

(1) OJ C 229, 31.7.2012, p. 90.
(2) OJ C 391, 18.12.2012, p. 127.
(3) Position of the European Parliament of 12 March 2014 (not yet published in the Official Journal) and position of the Council at first reading of 8 April 2016 (not yet published in the Official Journal). Position of the European Parliament of 14 April 2016.
(5) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).

個人データ保護規則

第1 条

対象事項及び目的

1. 本規則は、個人データの取扱いと関連する自然人の保護に関する規定及び個人データの自由な移動に関する規定を定める。

2. 本規則は、自然人の基本的な権利及び自由、並びに、特に、自然人の個人データの保護の権利を保護する。

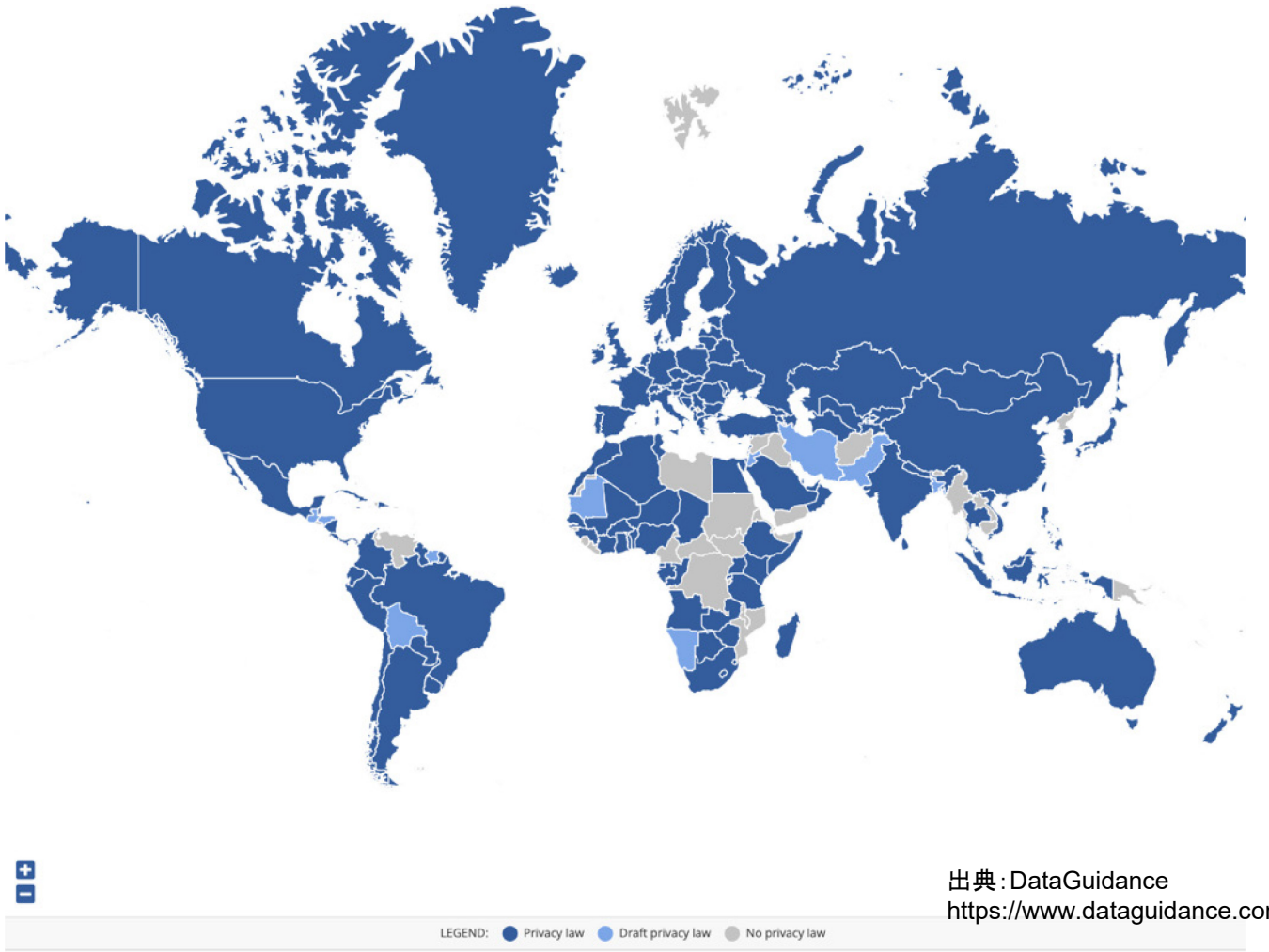
3. EU 域内における個人データの自由な移動は、個人データの取扱いと関連する自然人の保護と関係する理由のゆえに制限されることも禁止されることもない。

欧州で成功し、ブリュッセル効果で世界中に

プライバシー法制は外交手段の一つ

世界に先駆けて**個人データ保護指令**を作成、その後**個人データ保護規則（GDPR）**に改正。欧州との取引のためには、GDPRに従わざるを得ず、結果的に各国とも**GDPRと同等の法律**の整備が必要となっている。

ブリュッセル効果



出典：DataGuidance
https://www.dataguidance.com/

GDPRはどのような法律か？

個人データの取り扱いと関連する**自然人の保護**に関する規定および**個人データの自由な移動**に関する規定を定める。

自然人の**基本的な権利**および**自由**、並びに、特に、自然人の**個人データの保護**の権利を保護する。

データ主体の権利保護

データ主体に自身のデータへの**アクセス**、**修正**、**削除**、**ポータビリティ**などの権利の付与など

透明性と責任

データ保護**影響評価**の実施、**データ保護オフィサー（DPO）**の任命など

遵守体制の構築

技術的、組織的措置を講じるためのコンプライアンス体制を構築する。

データ保護ポリシーの策定、**データ侵害通知義務**。

罰則

罰則として、違反に対して、最大で**世界年間売上高の4%**または2,000万ユーロのいずれか高い方が科される。

国際的な影響

EU域外の企業に対しても、EU市民のデータを処理する場合には適用される。（**域外適用**）

日本の個人情報保護法との違い

	法の適用範囲	データ主体の権利	同意要件	データ保護責任者	罰則
	域外適用あり EU市民のデータを扱うEU域外の企業にも適用される	**広範で明確な権利** アクセス権、修正権、削除権、データポータビリティ権、処理の制限、異議申立権	**厳格な同意要件** 明示的な同意が必要。また、同意を取り消す権利も明記	**データ保護責任者の設置と責任** 一定の要件の企業には設置が義務付けられ、監視と指導を行う権限がある	**厳しい罰則** 最高額は、世界年間売上の4%または2,000万ユーロのいずれか高い額
	域外適用なし 海外の日本国民は保護されない	**一部権利は限定的** アクセス権や訂正権はあるが、削除権は制限付き、データポータビリティ権、処理の制限、異議申立権は明記されていない	**同意要件の厳格さは不明瞭** 同意要件はあるものの、厳格な定義はない	**データ保護責任者の概念はない** 義務付けられていない	**緩い罰則** 最高額は、法人で5,000万円、個人で50万円。 懲役1年未満の刑事罰もある

4

安全保障と
サイバーセキュリティ

ネット社会の宿命

何から何を守りたいのか？

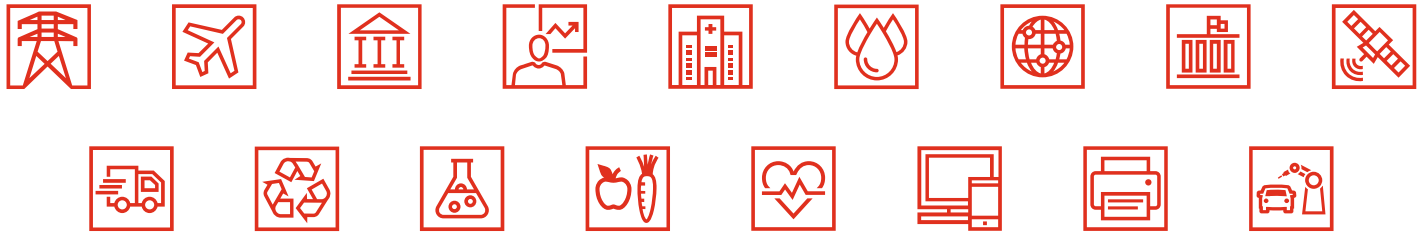
社会活動が、データ、情報処理、インターネットの依存度をますます高めていることから、サイバー空間の安全を高めることが、我々の社会生活を維持するためにも必要不可欠となってきている。

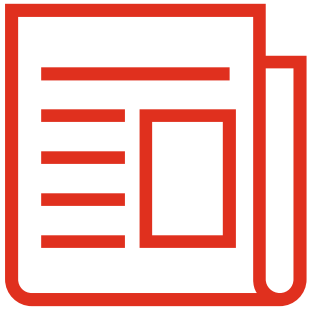
社会インフラを攻撃する意欲が高いと思われる団体は、競争関係にある国家（およびその支援をうけている組織などを含む）、ハクティビストと想定される。

1組織で守ることは難しい。そのため、同様の立場にある組織が連携、協力して対応することが効果的である。

また、政府も1ユーザであるが、このような活動が円滑に行えるような支援をすることが重要となる。

そのため、インシデントの報告義務が課されている。





NIS2指令 (Network and Information Security Directive 2) はどのような規制か？

EU全体でサイバーセキュリティ能力を構築し、重要インフラなどの必須サービスを提供するために用いられるネットワークと情報システムの脅威を緩和し、インシデントに直面しても当該サービスの継続性を確保し、もってEUの安全と経済社会の有効な機能に寄与することを目指している。

重要インフラ保護

重要インフラ組織として、主要事業者とその他の重要な事業者に分けて、レジリエンスの向上のための規制を規定

セキュリティ対策の強化

ガバナンス

セキュリティ対策を承認し、その実施を監督し、かつ、当該事業体が同条を侵害した場合に責任を負うことができるようにする

対策

方針、インシデントハンドリング、事業継続、サプライチェーン、開発、有効性評価、訓練、暗号、人的セキュリティ、アクセス管理、資産管理など

インシデント報告

早期通知：24時間以内

インシデント通知：72時間以内

（**中間報告**）

最終報告：**1ヶ月**以内

罰則

罰則として、違反に対して、最大で**世界年間売上高の2（1.4）%** または1,000（700）万ユーロのいずれか高い方が科される。

カッコ書は主要事業者以外の重要事業者

NIS2指令 はどのような規制か？（補足）

規制開始

2024年10月18日から各国で施行

規制対象

主要事業者

- エネルギー、運輸、銀行、金融市場インフラ、医療、上下水道、デジタルインフラ、ICTサービス、行政、宇宙

重要事業者

- 郵便・配送、廃棄物管理、化学製品製造など、食品製造など、製造（医療機器、コンピュータ、電気機器など、自動車など）

（SaaS事業者など※）

- 実施規則により別途規制をする

※
- DNS service providers,
- TLD name registries,
- cloud computing service providers,
- data centre service providers,
- content delivery network providers,
- managed service providers,
- managed security service providers,
- providers
  - of online market places,
  - of online search engines and
  - of social networking services platforms, and
- trust service providers

セキュリティ対策

- リスク分析および情報システム・セキュリティに関する方針
- インシデントハンドリング
- バックアップ管理、災害復旧、危機管理などの事業継続
- サプライチェーンのセキュリティ
- ネットワークと情報システムの取得、開発および保守におけるセキュリティ（脆弱性の取り扱いおよび公開など）
- 有効性を評価するための方針および手続。
- 基本的なサイバー衛生の実践および訓練。
- 人的セキュリティ、アクセス制御方針および資産管理

インシデント通知

早期通知：24時間以内

インシデント通知：72時間以内

- 重大性や影響に関する評価を通知

（中間報告）：必要に応じて

最終報告：1ヶ月以内

- インシデントの詳細（原因や緩和措置策、影響範囲など）

身代金支払報告義務を求める米国重要インフラ向けサイバーインシデント報告法

成立

2022年10月18日から各国で施行

規制対象

重要インフラ事業体（小規模事業体除く）

大統領指令21（2013.02.12）で定義されている重要インフラ事業体

16分野（化学、商業施設、通信、重要製造、ダム、防衛、救急サービス、エネルギー、金融サービス、食料と農業、政府、医療、情報技術、原子炉・核物質、輸送システム、上下水道システム）のうち小事業体以外

特定の施設・設備又は特定の機能を果たす事業体

報告すべきインシデント

重大インシデント

- 機密性・完全性・有用性の重大損失
- 安全性とレジリエンスへの深刻な影響
- ビジネスやオペレーションを阻害
- 第三者やサプライチェーンを経由した不正アクセス（マネージドサービスなどを含む）

報告事項と報告期限

- インシデント報告：インシデントの認識から72時間以内
- 身代金支払報告：身代金支払いから24時間以内
- 補足的報告：インシデント報告の更新やインシデント報告後に身代金の支払いがあった場合は速やかに提出

（参考）日本の経済安全保障推進法：リスク管理措置の概要

特定社会基盤事業者

参考 リスク管理措置の概要

特定重要設備・構成設備を供給する方等のご協力のもと、特定社会基盤事業者において、講じられるリスク管理措置の例について、概要を以下に記載しておりますので、ご確認ください。
※全ての項目を常に実施することを求めるものではありません。
※詳細は主務省令をご確認ください。
※以下はこれらの措置を行うことが主に想定される方を記載したものです。その他の事項についても、特定社会基盤事業者から協力を求められることがありますので、特定社会基盤事業者と協議を行ってください。

1 特定重要設備の供給者の方のご協力のもと取組む事項
（※⑦については導入に携わる方も該当）　届出様式上の番号↓

（第三者による）受入検査等の検証体制の構築、脆弱性検査の実施	①－1
情報セキュリティ要件（最新のセキュリティパッチや不正プログラム対策ソフト等）の実装	②－1
品質保証体制の確立	③－1
開発・製造過程における不正な変更等の定期的又は随時の確認	④－1
開発・製造環境への物理的(入退室管理)及び論理的な制御(システムへのアクセス制御)	⑤－1
供給者・導入に携わる者が、設備設置時に不正な変更等を加えることを防止する体制	⑦
不正な変更のおそれの原因究明体制の担保	⑧－1
供給者によるサービス保証（故障対応や脆弱性対応等）	⑨－1
サービス保証が受けれられなくなった場合の代替手段の検討	⑩－1
設備に対するアクセスの制御及び不正アクセスの監視の仕組みの実装	⑬
過去３年間の国内関連法規・国際的な基準の違反の確認	⑭－1
外国の法的環境等による契約違反が生じたおそれがある場合の報告義務	⑮－1
供給者に関する詳細な情報提供の担保	⑰

2 構成設備の供給者の方のご協力のもと取組む事項

（第三者による）受入検査等の検証体制の構築、脆弱性検査の実施	①－2
情報セキュリティ要件（最新のセキュリティパッチや不正プログラム対策ソフト等）の実装	②－2
品質保証体制の確立	③－2
開発・製造過程における不正な変更等の定期的又は随時の確認	④－2
開発・製造環境への物理的(入退室管理)及び論理的な制御(システムへのアクセス制御)	⑤－2
不正な変更のおそれの原因究明体制の担保	⑧－2
供給者によるサービス保証（故障対応や脆弱性対応等）	⑨－2
サービス保証が受けれられなくなった場合の代替手段の検討	⑩－2
過去３年間の国内関連法規・国際的な基準の違反の確認	⑭－2
外国の法的環境等による契約違反が生じたおそれがある場合の報告義務	⑮－2
供給者に関する詳細な情報提供の担保	⑰

（参考）特定社会基盤事業者が自ら対応する事項

（第三者による）受入検査等の検証体制の構築、脆弱性検査の実施	①
インターネット接続時の不正アクセス防止機能実装、マニュアル整備	⑥
サービス保証が受けれられなくなった場合の代替手段の検討	⑩
不正な妨害が行われた場合でも役務の提供を継続できる体制の整備	⑪
インシデント発生時の対応方針や体制の整備	⑫
不正なアクセスの制御及び監視の仕組みの実装	⑬
映像機器の情報の取扱いの適切性確認（特定重要設備の設置場所）	⑯

8

重要維持管理等の委託先など

参考 リスク管理措置の概要

重要維持管理等の委託先や再委託先の方のご協力のもと、特定社会基盤事業者において、講じられるリスク管理措置の例について、概要を以下に記載しておりますので、ご確認ください。
※すべての項目を常に実施することを求めるものではありません。
※詳細は主務省令をご確認ください。
※以下はこれらの措置を行うことが主に想定される方を記載したものです。その他の事項についても、特定社会基盤事業者から協力を求められることがありますので、特定社会基盤事業者と協議を行ってください。

1 重要維持管理等の委託先の方のご協力のもと取組む事項　届出様式上の番号↓

操作ログや作業履歴等の保管や不正な変更の有無の定期的又は随時の確認	①
保有している設計書・設備等の情報への物理的(入退室管理)及び論理的な制御（システムへのアクセス制御）	③
実施環境における物理的(入退室管理)及び論理的な制御（システムへのアクセス制御）	④
サイバーセキュリティ教育	⑤
再委託を行う場合における特定社会基盤事業者の承認等	⑥
再委託を行う場合の委託先と同等のサイバーセキュリティ対策の確保	⑦
事業計画等による事業の安定性の確認	⑧
過去３年間の国内関連法規及び国際的な基準の違反の確認	⑨－1
外国の法的環境等による契約違反が生じたおそれがある場合の報告義務	⑩－1
供給者に関する詳細な情報提供の確保	⑫

2 重要維持管理等の再委託先の方のご協力のもと取組む事項

操作ログや作業履歴等の保管や不正な変更の有無の定期的又は随時の確認	①
保有している設計書・設備等の情報への物理的(入退室管理)及び論理的な制御（システムへのアクセス制御）	③
実施環境における物理的(入退室管理)及び論理的な制御（システムへのアクセス制御）	④
サイバーセキュリティ教育	⑤
再委託を行う場合における特定社会基盤事業者の承認等	⑥
再委託を行う場合の委託先と同等のサイバーセキュリティ対策の確保	⑦
過去３年間の国内関連法規及び国際的な基準の違反の確認	⑨－2
外国の法的環境等による契約違反が生じたおそれがある場合の報告義務	⑩－2
供給者に関する詳細な情報提供の確保	⑫

（参考）特定社会基盤事業者の方が自ら対応する事項

最新のセキュリティパッチ適用等の定期的な資産管理	②
再委託を行う場合における特定社会基盤事業者の承認等	⑥
事業計画等による事業の安定性の確認	⑧
映像機器の情報の取扱いの適切性確認（重要維持管理等の場所）	⑪

9

経済安全保障推進法で、基幹的なインフラ事業を行う事業者（特定社会基盤事業者として指定された者）が、特定の重要設備（特定重要設備）について、導入や重要な維持管理等の委託をしようとする際に、事前に国に届 出を行い、審査を受ける制度が設けられた。

確認書類の1つとして、リスク管理措置を講じていることを証する書類が必要となった。

経済安全保障推進法の特定社会基盤役務の安定的な提供の確保に関する制度のパンフレット（令和6年7月3日時点）
【特定重要設備の導入版（主に設備の供給者の方向け）
https://www.cao.go.jp/keizai_anzen_hosho/suishinhou/infra/doc/pamphlet_dounyu.pdf
【重要維持管理等の委託版（主に委託先の方向け）】
https://www.cao.go.jp/keizai_anzen_hosho/suishinhou/infra/doc/pamphlet_itaku.pdf

5

IoTに関わる規制

普及と安全のバランス

何から何を守りたいのか？

家庭にウェブカメラ、ルータなどの多くのIoT機器が利用されるようになった。家庭用機器では、ユーザによるセキュリティ対策に頼ることが難しいので、製品自体の脆弱性を減らし、デフォルトの設定がセキュアな状態になっているようにすることが必要。また、上市後の脆弱性の管理も重要。そのためSBOMなどの作成が重要。

セキュリティが弱い機器などを悪用

消費者用ネットワーク機器など

セキュア・バイ・デザイン

セキュア・バイ・デフォルト

脆弱性管理（SBOM含む）

欧州のアプローチ、米国のアプローチ、日本のアプローチ

法律
（罰則）

認証制度

大統領令
（マーケットパワー）

英国、欧州

- 法律で規制
- 法律で罰則を規定
- 違反者に罰則

米国

- ガイドラインで事業者に協力要請
- 政府調達で優先
- 認証取得製品をマーケットで推奨
- 認証製品を買うように消費者を誘導

?

IoTセキュリティは認証制度により担保される時代に

英国では今年の4月より認証制度が義務付けられており、米国、欧州での導入も決まっている。

地域・国	英国	欧州	米国	日本
法令など	製品セキュリティ・通信インフラ（PSTI）法	サイバーレジリエンス法	（大統領令） サイバートラスト制度	（ガイドライン）
特徴	義務	義務	義務（検索、ネット販売事業者） 任意（製造事業者）：ラベル制度	任意：ラベル制度
	自己適合宣言	自己適合宣言とサイバーセキュリティ認証スキーム（EUCC）	検討中	自己適合宣言と第三者認証の組み合わせ？
対象	消費者向け	消費者から産業用まで	消費者向け	検討中 （消費者から産業用まで？）
	IoT製品	デジタル製品	IoT機器	IPを使用したデータの送受信機能を持つ機器
対象除外	PC、タブレット、医療機器、EV充電ステーション	PC、スマートフォン、タブレット、医療機器、自動車、航空機	検討中（PC、スマートフォン、タブレット、医療機器、自動車？）	検討中
開始時期	2024年4月	2027年？	2024年予定	検討中

U.S. CYBER TRUST MARK

簡易の基準で早期に規制にした英国

製品セキュリティ・通信インフラ (PSTI) 法の概要

目的	製品（IoT機器を含む）メーカーに対するセキュリティ対応の意識改革を求める
要件	**コンプライアンス宣言** ● 製造業者、またはその代理人によって作成されたもので、担当大臣の規定する形式を用いて、適用されるセキュリティ要件に準拠していると自ら宣言
	脆弱性管理 ● 脆弱性を報告する方法の明確化、市場からのフィードバックの受領、また脆弱性開示ポリシーの開示など、セキュリティ対応体制の構築
	サポート期間 ● 製品がセキュリティサポート（セキュリティ問題に対する案内や修正アップデート）を受けられる最低期間やサポート終了期間を明示すること
	デフォルトパスワード禁止サポート期間 ● 機器固有のパスワード設定で出荷するか、製品を使用する前にユーザが強固なパスワードを設定しなければ使い始められない仕様とすること
罰則など	1,000万ポンドまたは、全世界売上高の4%のうち高い金額
施行日	2024年4月29日

対象製品	2021年11月にデジタル・文化・メディア・スポーツ省が発表したファクトシートに基づくと以下が対象の製品となる • スマートフォン • スマートカメラ、スマートTV、スマートスピーカー • 子ども向けおもちゃや幼児モニタ • 煙探知機やドアロックといった安全関連製品 • IoTのベースとなる複数機器をつなぐ機器やハブ • ウェアラブルヘルストラッカ • アウトドア用のGPS機器などの製品 • ホームオートメーションや警戒システム • 洗濯機や冷蔵庫といったスマート家電 • スマートホーム支援機器類
対象	製造業者（および代表者）：在英国の製品製造者、製品に商標などを付して製造者であることを示す者、または製品を市場に適するように調整する者 輸入業者：英国内で製品の輸入をおこなうもの（該当製品の製造業者ではないこと） 販売業者：英国内で製品を流通するオンライン販売者を含むディストリビュータ（当該製品の製造業者または輸入業者でないこと）

出所：
Guidance The UK Product Security and Telecommunications Infrastructure (Product Security) regime
https://www.gov.uk/government/publications/the-uk-product-security-and-telecommunications-infrastructure-product-security-regime
を元にPwC が作成

法制化で網羅的に対応する欧州

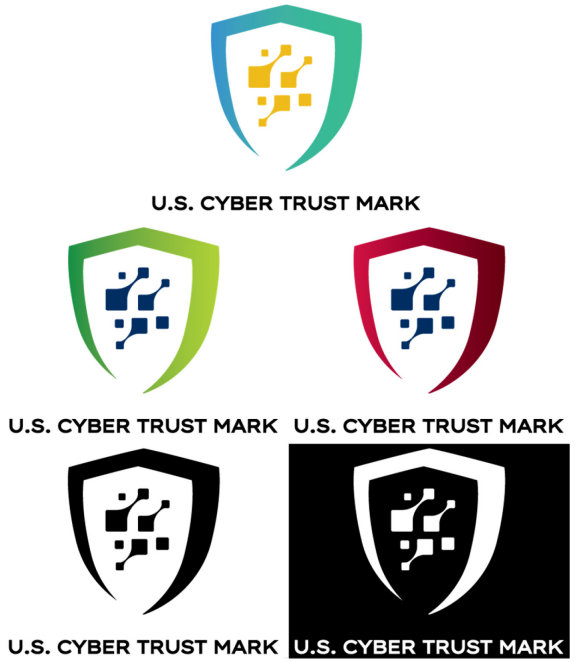
サイバーレジリエンス法 （CRA）の概要

法的根拠	EU運営条約(TFEU)の114条 *EU域内の単一マーケットの構築（単一デジタルマーケット）
EU戦略的位置づけ	2020 EU Cybersecurity Strategy Link 2020 EU Security Union Strategy Link *Cyber Resilience Act はEuropean Cyber Defence Policy Link に依拠しています。
目的	接続されたデバイスとソフトウェアのサイバーセキュリティ強化
主な内容	• デジタル要素を含む製品のサイバーセキュリティを確保するための製品の上市に関する規則 • デジタル要素を含む製品の設計、開発、製造に関する必須要件、およびこれらの製品に関連するサイバーセキュリティに関する経済事業者の義務 • デジタル要素を含む製品のサイバーセキュリティを全ライフサイクルにわたって確保するために製造者が実施する脆弱性処理プロセスに関する必須要件、およびこれらのプロセスに関連する経済事業者の義務 • 上記の規則および要件の市場監視および執行に関する規則
経済事業者の定義	製造者、輸入者、販売者

対象製品の定義	ソフトウェアまたはハードウェア製品およびその遠隔データ処理ソリューション、市場に個別に投入されるコンポーネントなど、**「デジタル要素を含む製品」**
対象製品	• すべてのIoT製品を含む、接続可能なソフトウェアとハードウェア • 遠隔データデータ処理ソリューション • 単独でマーケットに投入するコンポネントなど *例えば、アプリケーション、スマートスピーカー、スマート家電など • AnnexⅢ記載の二つのカテゴリの重要な製品リスト
対象企業	EU圏内で、アプリケーション、スマートスピーカー、スマート家電など、上記対象製品を生産、輸入、販売する企業が対象となります。
適用除外	• EU Regulation (EU) 2017/745（医療機器およびその付属品） • EU Regulation (EU) 2017/746（体外診断用医療機器およびその付属品） • EU規則2019/2144（自動車とトレーラー、およびその自動車を意図したシステム、コンポーネント、個別の技術ユニットに対する型式承認要件） • Regulation (EU) 2018/1139（民間航空）により認証済みの機器 • 他のRegulationにより同等のセキュリティ要件に達している場合 （セキュリティ要件未達成の以下の製品） • 展示会出展用製品 • 試験用の製品
CEマーク	対象製品はCEマークの取得が必要。 CEマークLink

マーケットの力で対応する米国

サイバートラストマークの概要



適用するラベル	• Federal Communications Commissionの「U.S. Cyber Trust Mark」を使用、QRコードで詳細なセキュリティ情報を確認可能	**政府支援**	• CISAが消費者意識向上、対応済み製品の優先陳列を支援 • 司法省など規制当局が実効性保障
対象製品	• スマート冷蔵庫、電子レンジ、テレビ、空調制御システム、スマート・フィットネス・トラッカーなど一般的な機器	**ルーター**	• NISTはコンシューマルーターのセキュリティに関するガイドラインを2023年中に完成させ、欧州に展開
目的	• IoT製品セキュリティの強化 • 消費者のセキュリティ意識を高め、製品セキュリティ競争を促す	**エネルギー省**	• スマートメーターと電力インバーターのサイバーセキュリティ表示要件を研究・開発する予定
適用ガイドライン	• NISTのガイドライン	**参加企業**	• アマゾン、ベスト・バイ、グーグル、LGエレクトロニクスU.S.A.、ロジテック、サムスン電子など
コメント	• 法的義務付け、高い制裁金の設定はないものの、競合他社の参加により対応を迫られることになる可能性が高い。		

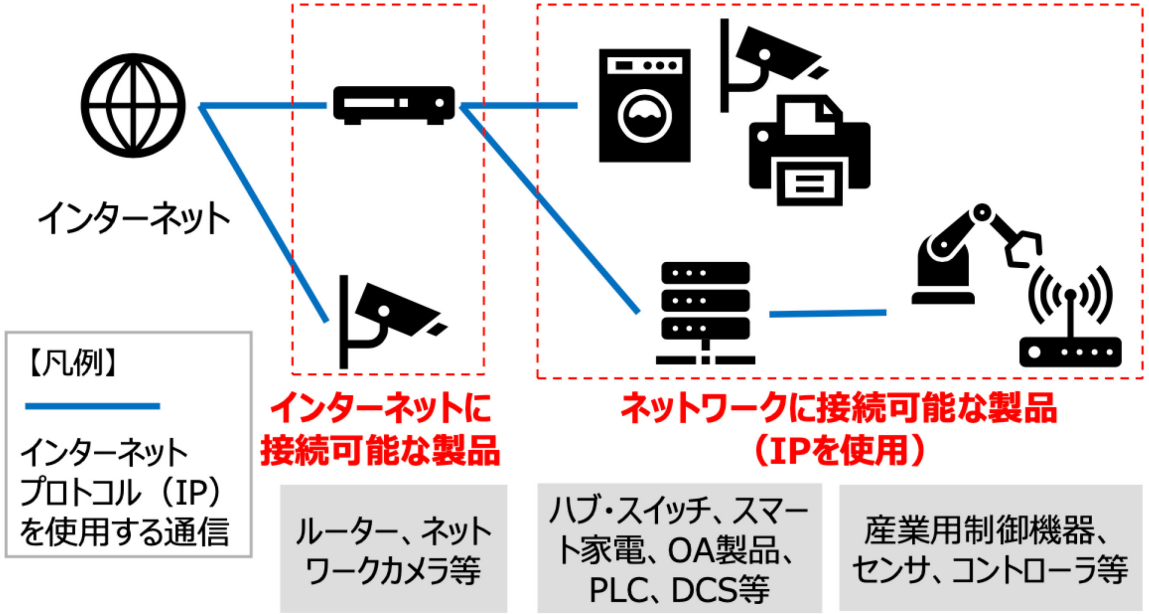
出所：Federal Communications Commission
https://www.fcc.gov/cybersecurity-certification-mark

日本は政府主導のガイドライン対応

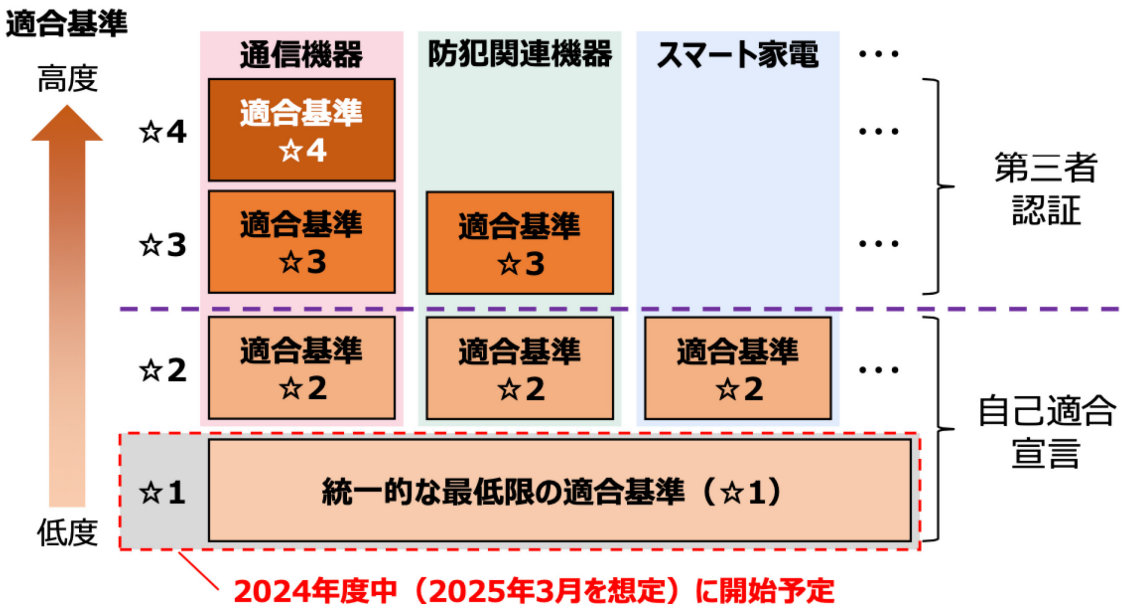
IPを使用する通信機能を持つIoT製品が対象

最低限の脅威に対応するための基準（☆1）およびIoT製品類型ごとの特徴に応じた基準（☆2～☆4）を定め、求められるセキュリティ水準に応じた複数の適合性評価レベルを適用することを想定

対象製品の概要(※1)



適合性評価レベル（☆1～☆4）のイメージ



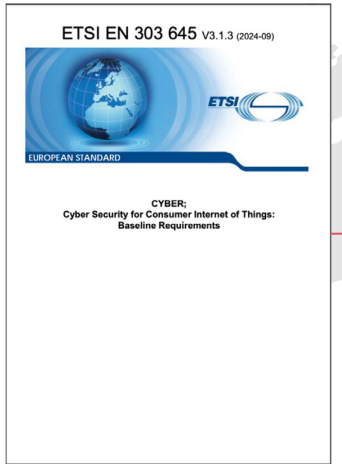
出所：経済産業省 IoT 製品に対する セキュリティ適合性評価制度 構築方針案（2024.05.26確認）
https://www.meti.go.jp/press/2023/03/20240315005/20240315005-3r.pdf

さて、相互認証はできるのか？

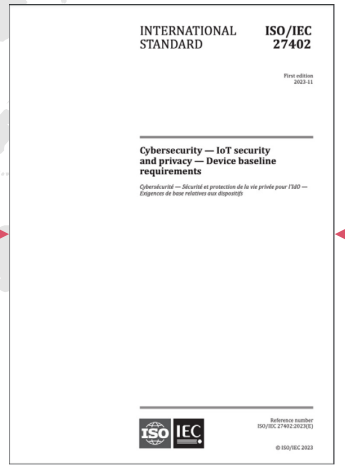
それぞれの国・地域で独自の認証制度をつくっている。認証のための制度（スキーム、規準）が異なる。ベンダーはそれぞれに国・地域ごとに認証を取らなければならないのか？

英国、欧州、シンガポール

認証規準：ETSI EN 303 645



?

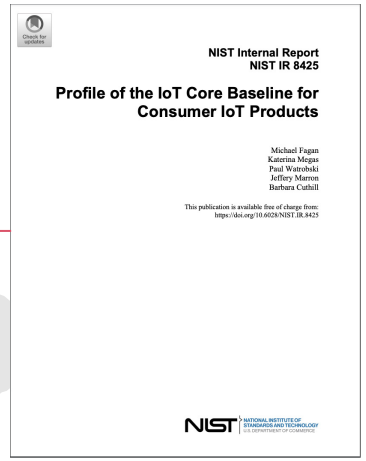


ISO/IEC 27402:2023

?

米国

認証規準：NIST IR 8425



6

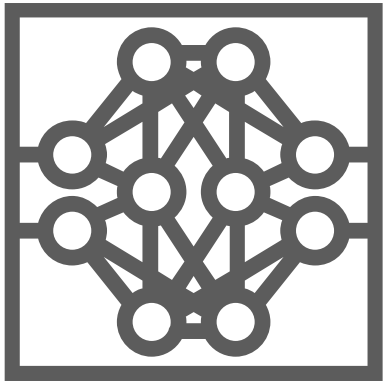
AIに関わる規制

本格的に普及する前に法制化

何から何を守りたいのか？

AIとりわけ、生成AIにより、

- プライバシー、知的財産権などが侵されやすくならないのか？
- 公正な社会を維持できるのか？
- 競争が歪められないのか？
- 民主主義は守られるのか？



AI規制を考えない国はない

AIの利用促進のためには適切な利用ルールの設定が不可欠

OECD

生成AIのための初期政策検討

G7広島サミット

AIにおけるアカウンタビリティの高度化
(2023.02.23)

米国

大統領令（EO14110）

AI権利章典のための草案

1. 安全効果的なシステム、
2. アルゴリズムの差別からの保護
3. データプライバシー
4. 通知と説明
5. 人間による代替措置

欧州

AI法

AIをリスクに応じて4つに分類。容認できないリスクのAIは使用禁止。

1. 人的監視
2. 技術的な堅牢性と安全性
3. プライバシーとデータガバナンス
4. 透明性
5. 多様性、被差別、公平性
6. 社会的・環境的福祉

英国

AI規制法案

AI安全サミット

2023年12月に委員会、議会などで政治的合意。

2024年成立し、2026年に施行が想定される。

中国

グローバルAIガバナンス・イニシアティブ (2023.10.19)

生成的AIサービス管理暫定弁法 施行 2023.08.15

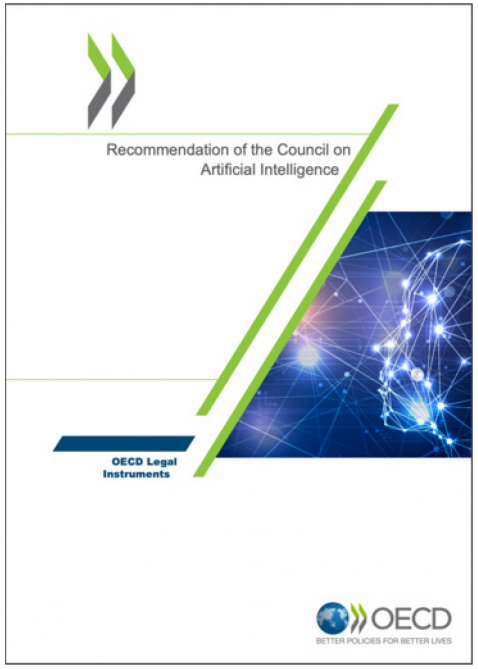
インターネット情報サービス深層合成管理規定

画像生成AIに「AI生成マークの表示」の義務化とAIユーザの実名登録制の規制

先行してAIの原則を示したOECD

AIは社会に大きな影響を及ぼす可能性がある。（良い意味でも、悪い意味でも）

差別・偏見　著作権　偽情報



包摂的な成長、持続可能な開発および幸福	人々と地球にとって有益な結果を追求することにより、信頼できるAIの責任ある スチュワードシップに積極的に取り組むべき
人間中心の価値観および公平性	法の支配、人権および民主主義の価値観を尊重すべきである。 状況に適した形で、かつ技術の水準を踏まえたメカニズムとセーフガードを実装すべき
透明性および説明可能性	AIシステムに関する透明性と責任ある開示に積極的に関与すべき
頑健性、セキュリティおよび安全性	ライフサイクル全体にわたって頑健で、セキュリティが高く、かつ安全であるべき 状況に適した形で、かつ技術の水準を踏まえたトレーサビリティを確保すべき 役割、状況および能力に基 づき、系統化されたリスクマネジメントのアプローチをAIシステムのライフスタイル の各段階に絶え間なく適用すべき
アカウンタビリティ	役割と状況に基づき、かつ技術の水準を踏まえた形で、AIシステムが 適正に機能していることおよび上記の原則を尊重していることについて、アカウンタビリティを果 たすべき

出典：2019.05.22 OECD 人工知能に関する理事会勧告（2023.11.27確認）
https://legalinstruments.oecd.org/api/download/?uri=/public/83072497-5c4a-4e23-8ba9-8e5c6eb863cc.pdf

リスクに応じた法規制を導入したEU

個人の権利利益の尊重、政府に対する規制

リスクレベル	利用
許容できないリスク	禁止 （EUの価値観に矛盾）
ハイリスク	要件と事前適合性評価の準拠を条件
限定リスク	情報・透明性の義務を条件
最小リスク	制限なし

リスクの分類（EUの規制案に基づく例）

リスクレベル	リスクレベルの概要
1 許容できないリスク	● 人の生命や基本的人権に対して、直接的に脅威をもたらすと考えられるAIシステム ● 政府による個人の社会的格付け、危険な行動を促す音声アシストなどが挙げられる
2 ハイリスク	● 人の健康や安全、基本的人権、または社会的／経済的な利益に影響を与える可能性があるAIシステム ● 製品のセーフティコンポーネント、雇用・労働者の管理、必要不可欠な民間・公共サービスなどが挙げられる
3 限定リスク	● 深刻なリスクはないが、透明性に関する特定の要件を満たす必要があるAIシステム ● コンテンツや応答が、対話型AIによって生成されたことを明らかにする要件などが挙げられる
4 最小リスク	● リスクがごくわずか、またはリスクの伴わないAIシステム ● AIを利用したビデオゲーム、スパムフィルターなどが挙げられる

出典：https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/generative-ai-regulation03.html

国家による総合的なAI規制を試みる中国

社会秩序の維持、政府による規制

アルゴリズムの認定登録制度など、実名インターネット環境を踏まえた、政府ができるだけ関与できるようにする規制設計がされる。

国務院
2017年 新一代人工知能発展規画

工業情報化部
2017年 新一代人工知能産業発展促進
三年行動計画（2018-2020）

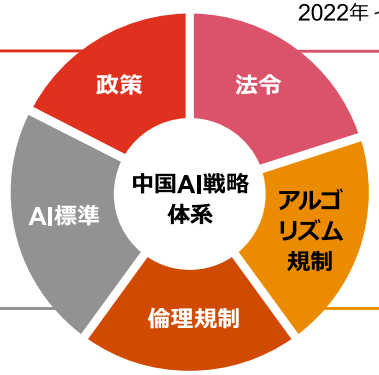
科学技術部
2019年 国家新一代人工知能開放イノベーション
プラットフォーム建設工作ガイド

全人代
2017年 サイバーセキュリティ法
2021年 データセキュリティ法
2021年 個人情報保護法

国家インターネット情報弁公室
2019年 インターネット情報
コンテンツ生態治理規定
2022年 インターネットコメントサービス管理規定

国家標準化管理委員会など
2020年 国家新一代人工知能
標準体系建設ガイド

全国信標委人工知能サブ技術委員会
2023年 人工知能倫理治理標準化ガイド



国家インターネット情報弁公室
2022年 インターネット情報
サービスアルゴリズム・
レコメンデーション管理規定
2022年 インターネット情報サービス
深度合成アルゴリズム管理規定
2023年 生成人工知能サービス
管理暫行弁法

国務院
2022年 科技倫理ガバナンス強化に関する意見
2019年 新一代人工知能ガバナンス準則ー責任ある人工知能の発展

科学技術部（人工知能ガバナンス専門委員会）
2021年 新一代人工知能倫理規範
2023年 科技倫理審査弁法（試行）（パブコメ）

セキュリティ三法

- 2017: サイバーセキュリティ法
- 2021: データセキュリティ法
- 2022: 個人情報保護法

標準・倫理規制

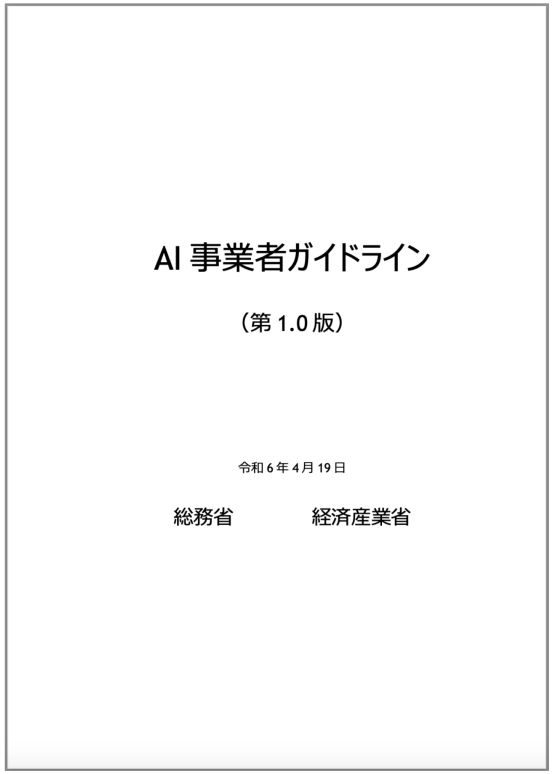
- 2020: 国家新一代人工知能標準体系建設ガイド
- 2021: 新一代人工知能倫理規範
- 2023: 人工知能倫理治理標準化ガイド
- 2023: 科技倫理審査弁法（試行）

アルゴリズム規制

- 2022: インターネット情報サービスリコメンデーション管理規定
- 2022: インターネット情報サービス深度合成アルゴリズム管理規定
- 2023: 生成人工知能サービス管理暫行弁法

日本はガイドライン対応でどこまで耐えられるか？

法規制ではなく、ガイドラインによる方向づけ


AI 事業者ガイドライン

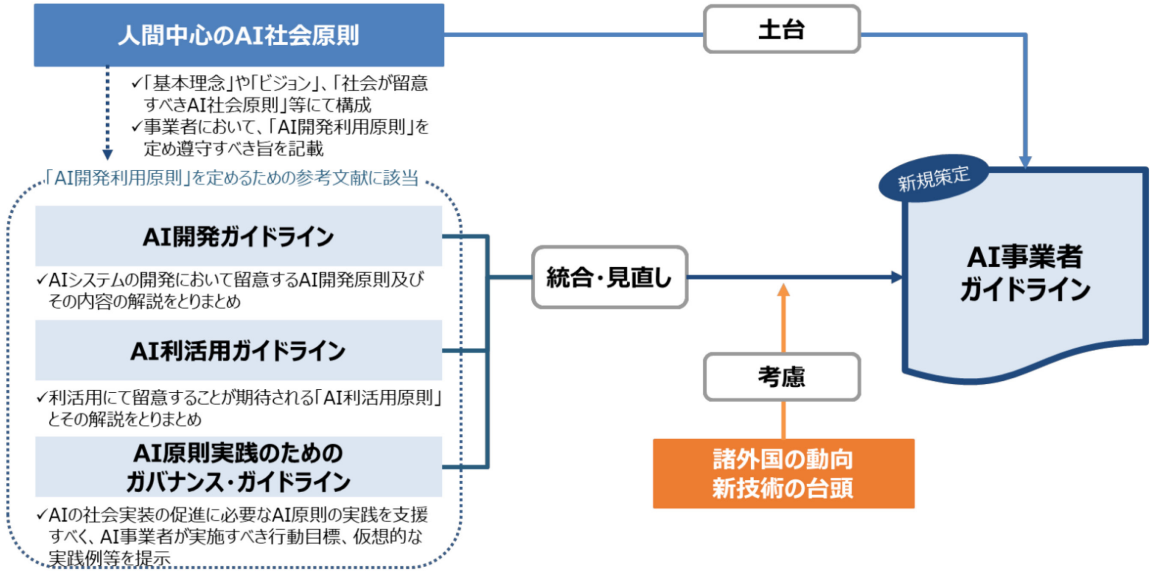
（第 1.0 版）

令和 6 年 4 月 19 日

総務省　　経済産業省

経済産業省、総務省が「AI事業者ガイドライン」をとりまとめた。(2024.01.19)

現在のところ法制化ではなく、ガイドラインで対応する方針のようである。



出典：内閣府
https://www8.cao.go.jp/cstp/ai/ai_senryaku/7kai/13gaidorain.pdf

7

まとめ

ざっと、あげてみるだけでもこれだけの法令があります

AI

- EU 欧州委員会：AI指針
- EU 欧州委員会：AI規則案
- 米国 WhiteHouse：大統領令
- 米国 WhiteHouse：AI権利章典
- 米国 国防総省：責任あるAIの指針の採用
- 米国 連邦取引委員会：ビジネス向けのAIアルゴリズム利用に係るガイダンス
- 米国 予算行政管理局：AI規制に係るガイダンス
- 米国 NIST：AIリスクマネジメント枠組み
- UK ICO：AIおよびデータ保護リスクツールキットv1.0
- 中国 国家インターネット情報弁公室（CAC）：インターネット情報サービスアルゴリズムレコメンデーション管理規定
- 中国 国家インターネット情報弁公室（CAC）：インターネット情報サービス深度合成アルゴリズム管理規定
- 中国 国家インターネット情報弁公室（CAC）：生成人工知能サービス管理弁法（パブコメ）

デジタルサービス

- EU 電子商取引指令
- EU デジタルサービス法
- EU デジタル市場法

IoT／OT

- 米国 IoTサイバーセキュリティ改善法
- 米国 カリフォルニア州 IoTセキュリティ法
- 米国 オレゴン州 IoT法
- EU サイバーセキュリティ法
- EU サイバーレジリエンス法
- EU RED委任規制2022/30（RE指令）
- 英国 製品セキュリティと通信インフラに関する法
- ブラジル 通信機器サイバーセキュリティ要件（法律第77号）

サイバーセキュリティ

- 日本 サイバーセキュリティ基本法
- 中国 サイバーセキュリティ法
- 米国 2022年重要インフラ向けサイバーインシデント報告法
- EU サイバーセキュリティ法
- EU 共通の高度サイバーセキュリティ措置に関する指令（NIS 2指令）
- EU サイバーレジリエンス法案
- EU デジタルオペレーションレジリエンス法
- 英国 ネットワーク・情報システム規則
- インド IT法2000／インフォメーション・テクノロジー・ルール2021
- インド 国家サイバーセキュリティポリシー
- インド インドCERT-Inサイバーセキュリティ指令2022
- 国連 UNECE規則サイバーセキュリティ（UN-R155）
- 国連 ソフトウェアアップデート（UN-R156）
- ISO ISO/SAE 21434

プライバシー

- 日本 個人情報保護法
- 中国 個人情報保護法
- 中国 データセキュリティ法
- 香港 個人情報保護法
- 台湾 個人情報保護法
- 韓国 個人情報保護法
- インド 個人情報保護法
- インドネシア 個人データ保護法
- オーストラリア 個人情報保護法
- シンガポール 個人データ保護法
- タイ 個人情報保護法
- フィリピン 個人情報保護法
- ブルネイ 個人データ保護規定草案
- ベトナム 個人データ保護法
- ニュージーランド プライバシー法2020
- マレーシア 個人情報保護法
- スリランカ 個人データ保護法2022年第9号
- EU 一般データ保護規則
- EU eプライバシー規制
- ベラルーシ 個人情報保護法
- ドイツ 電気通信およびテレメディアにおけるデータ保護およびプライバシーの規制に関する連邦法
- 英国 データ保護法
- 英国 一般データ保護規則
- スイス 改正連邦データ保護法1992
- イスラエ プライバシー保護法
- カタール データ保護規則2021

- モロッコ 個人データの処理に関する個人の保護に関する法律第09-08号
- チュニジア Organic law No. 63 - 2004
- トルコ 個人情報保護法
- ロシア 2006年7月27日付個人データに関する連邦法152-FZ号の改正法
- 南アフリカ 個人情報保護法
- アラブ首長国連邦 個人情報保護に関する2021年連邦政令第45号
- ケニア データ保護法
- ルワンダ 個人情報保護法とプライバシーに関する法律
- カナダ 個人情報保護および電子文書法
- カナダ 2022年デジタル憲章実施法
- 米国 カリフォルニア州消費者プライバシー法
- 米国 バージニア州消費者データ保護法
- 米国 コロラド州プライバシー法
- 米国 コネチカット州データ保護法
- 米国 ユタ州消費者プライバシー法
- チリ 私生活の保護に関する法律
- ブラジル データ保護法
- ペルー 個人情報保護法
- メキシコ 民間団体が保有する個人データの保護に関する連邦法
- パナマ データ保護法
- エクアドル 個人情報保護法
- アルゼンチン 個人情報保護法 25.326

出所：各国・地域の公的情報よりPwC作成

なりたい社会になるように法律は作られる

法律は社会を動かすプログラムコードのようなもの？

プログラム

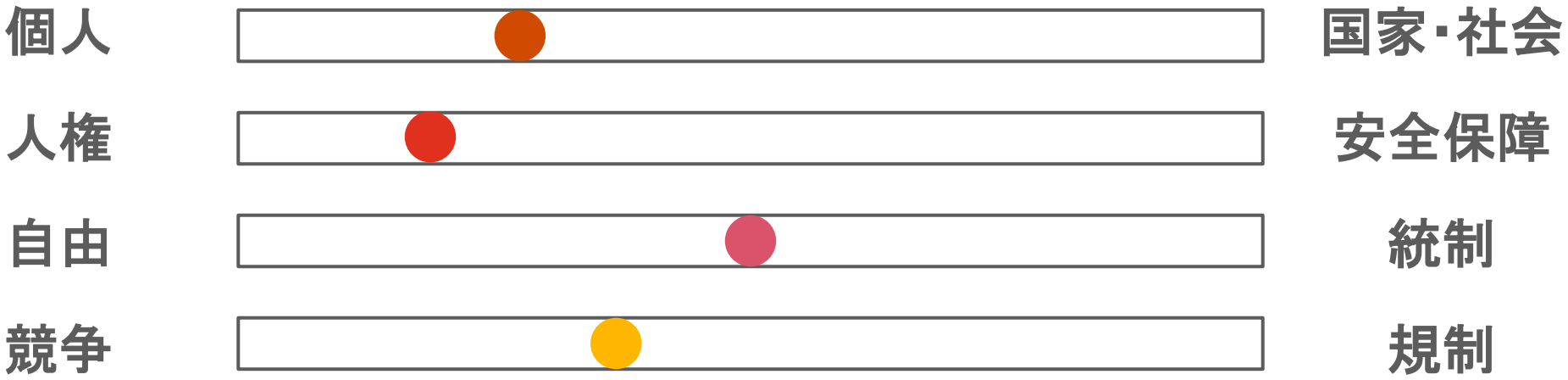
法律

コンピュータ

社会

私たちはどのような社会を目指しているのか？

正義　幸福



Thank you

www.pwc.com/jp

© 2024 PwC Consulting LLC. All rights reserved.
PwC refers to the PwC network member firms and/or their specified subsidiaries in Japan, and may sometimes refer to the PwC network. Each of such firms and subsidiaries is a separate legal entity. Please see www.pwc.com/structure for further details.
This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.