2021年10月28日

地域SECUNITY サイバーセキュリティセミナー
in FUKUOKA Overseas Trade（海外ビジネス編）

# サイバーセキュリティの各国法規制
## ～海外ビジネスにおける頻出論点の解説～

ＴＭＩ総合法律事務所　パートナー
弁護士・情報処理安全確保支援士
寺門　峻佑

# 講師紹介

## 寺門峻佑（てらかど　しゅんすけ）

TMI総合法律事務所　パートナー弁護士（日本・NY州）
情報処理安全確保支援士・情報セキュリティ監査人補

ご質問がありましたら、ご遠慮なく下記までご連絡ください。
E-mail：sterakado@tmi.gr.jp
URL：http://www.tmi.gr.jp/staff/s_terakado.html

- TMIプライバシー＆セキュリティコンサルティング株式会社取締役、内閣サイバーセキュリティセンタータスクフォース構成員、防衛省陸上自衛隊通信学校非常勤講師、経済産業省大臣官房臨時専門アドバイザー、滋賀大学データサイエンス学部インダストリアルアドバイザー、情報処理安全確保支援士会理事を歴任。
- データ利活用における個人情報保護法・各国データ保護法対応、情報セキュリティインシデント対応・情報セキュリティ管理体制構築を中心としたデータ・プライバシー・サイバーセキュリティ領域、システム/アプリ開発・ライセンスビジネスを中心としたIT法務・紛争、フォレンジックを含む不正調査案件を主に取扱う。
- ロサンゼルスのQuinn Emanuel Urquhart & Sullivan, LLPにおける国際紛争案件、サンフランシスコのWikimedia Foundation, Inc.法務部における各国データ保護法・各国著作権法・ドメイン保護案件、エストニアのLaw Firm SORAINENテクノロジーセクターにおけるeコマース・Fintech関連案件の経験も有する。

# アジェンダ

1．サイバーセキュリティの各国法規制

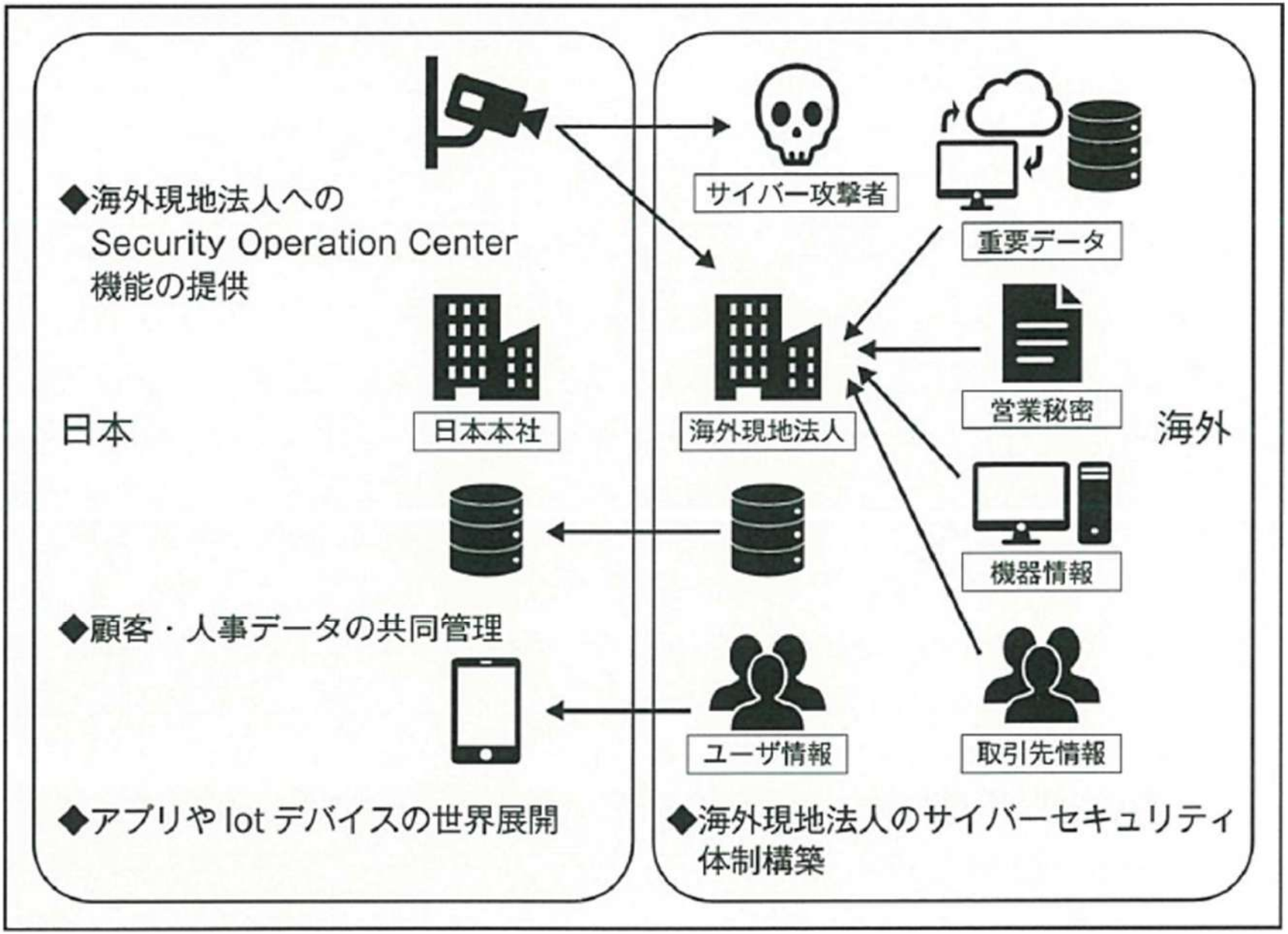
2．海外ビジネスにおけるインシデント対応

3．コンプライアンス体制整備の実務

# １．サイバーセキュリティの各国法規制

（１）EU一般データ保護規則(GDPR)
（２）カリフォルニア州消費者プライバシー法(CCPA)
（３）中国サイバーセキュリティ法・個人情報保護法
（４）基本的な対応事項まとめ
（番外）アジア各国におけるデータ保護法制
（番外）令和2年改正個人情報保護法
（番外）Cookie規制とCMP

# 海外のサイバーセキュリティ関係法令の適用場面




出典：株式会社商事法務「法律実務のためのデジタル・フォレンジックとサイバーセキュリティ」寺門執筆担当稿より抜粋

# 海外のサイバーセキュリティ関係法令の適用場面

## 各国法規制対応の検討の切り口

① 法令の概要と自社への適用可能性

② 各国法で求められる情報セキュリティ水準

③ データの移転規制の内容

④ 罰則の内容

＋個人データ保護法規制の検討
（個人への情報提供・個人の権利行使対応など）

# 海外のサイバーセキュリティ関係法令の調査

## 個人データ保護法規制とサイバーセキュリティ法規制の法令調査

- 個人データ保護法規制
- サイバーセキュリティ法規制（民間企業に対して義務等を課す包括的なもの）
- サイバーセキュリティ法規制（IoT機器に関するもの）

＋規則・ガイドライン等

**⇒データマッピングも重要**

# （1）GDPR

## General Data Protection Regulation(GDPR)
## 2018年5月25日施行

### 基本情報

- 広範な適用範囲
  **域外適用**
- 高額な制裁金
  **2000万ユーロ or**
  **世界総売上高の4%**
  **いずれか高い方**
- 迅速な当局報告
  **データ侵害認識時から**
  **72時間以内**

### 主な遵守事項

- データ処理の正当化根拠
- データ主体への情報提供
- データ主体の権利行使対応
- **データの安全管理措置**
- **データ侵害時報告・通知**
- **個人データの越境移転対応**

# （1）GDPR：適用範囲

## 1．EU域内の拠点の活動の過程におけるデータ処理

✓欧州子会社の顧客データ・従業員データの日本における保存

## 2．EU域内に拠点のない場合、以下と関連する処理

- **EU域内のデータ主体への商品・サービスの提供**

  ✓欧州顧客向けECサイト運営

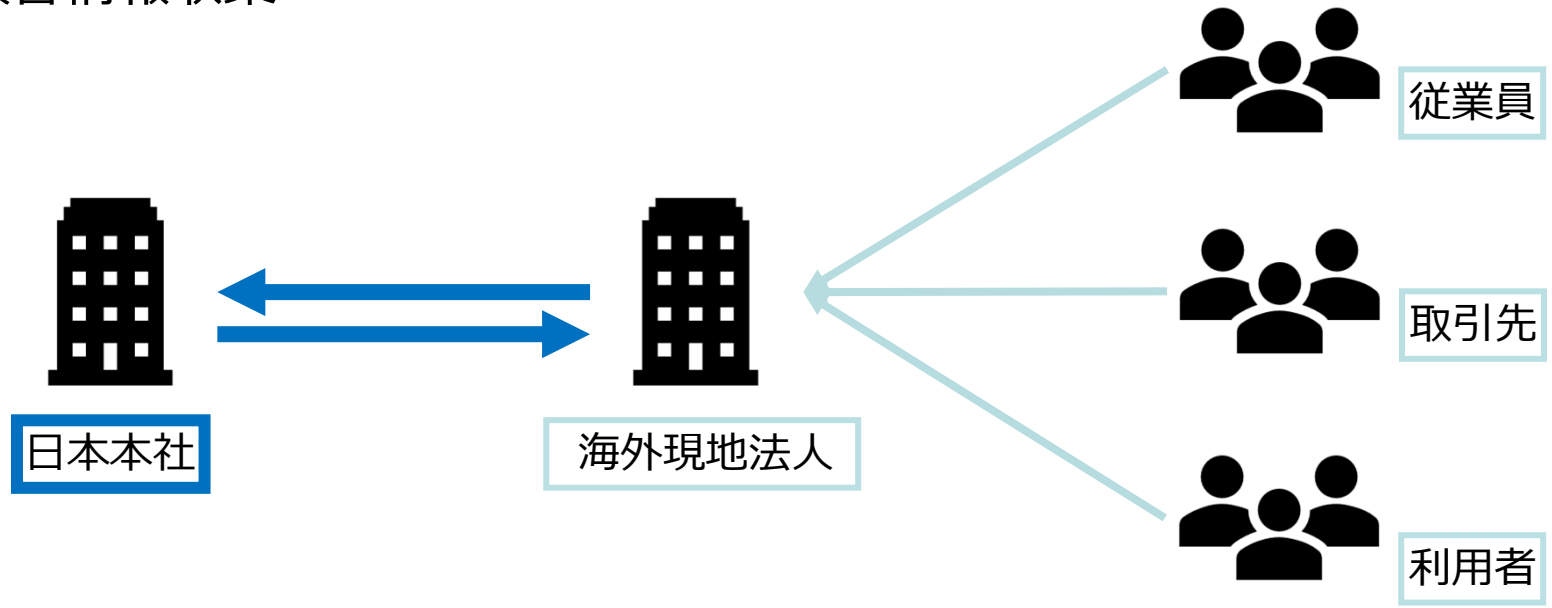
- **EU域内のデータ主体の行動監視を行う場合**

  ✓ウェブサイトにおけるCookie取得によるターゲティング広告

# （１）GDPR：頻出事例のご紹介①

## 海外現地法人保有パターン

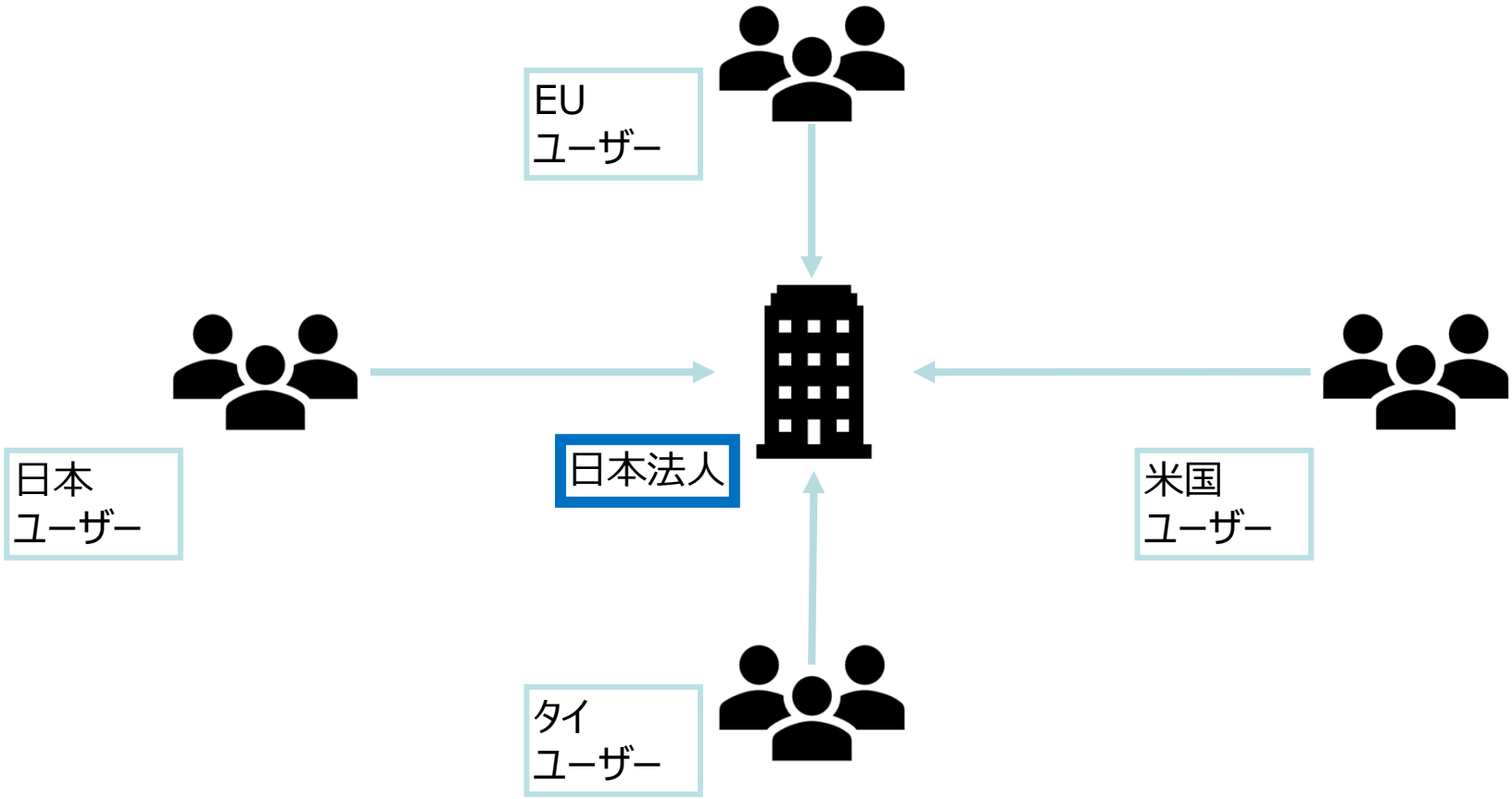
- 海外現地法人で商品を製造し、日本や世界各国に輸出
- 現地法人にて従業員と取引先担当者の個人データを取得
- BtoCビジネスにおける顧客情報の収集
- BtoBビジネスにおけるウェブサイトやFacebookアカウントを通じた顧客情報収集



# （１）GDPR：頻出事例のご紹介②

## 世界展開パターン

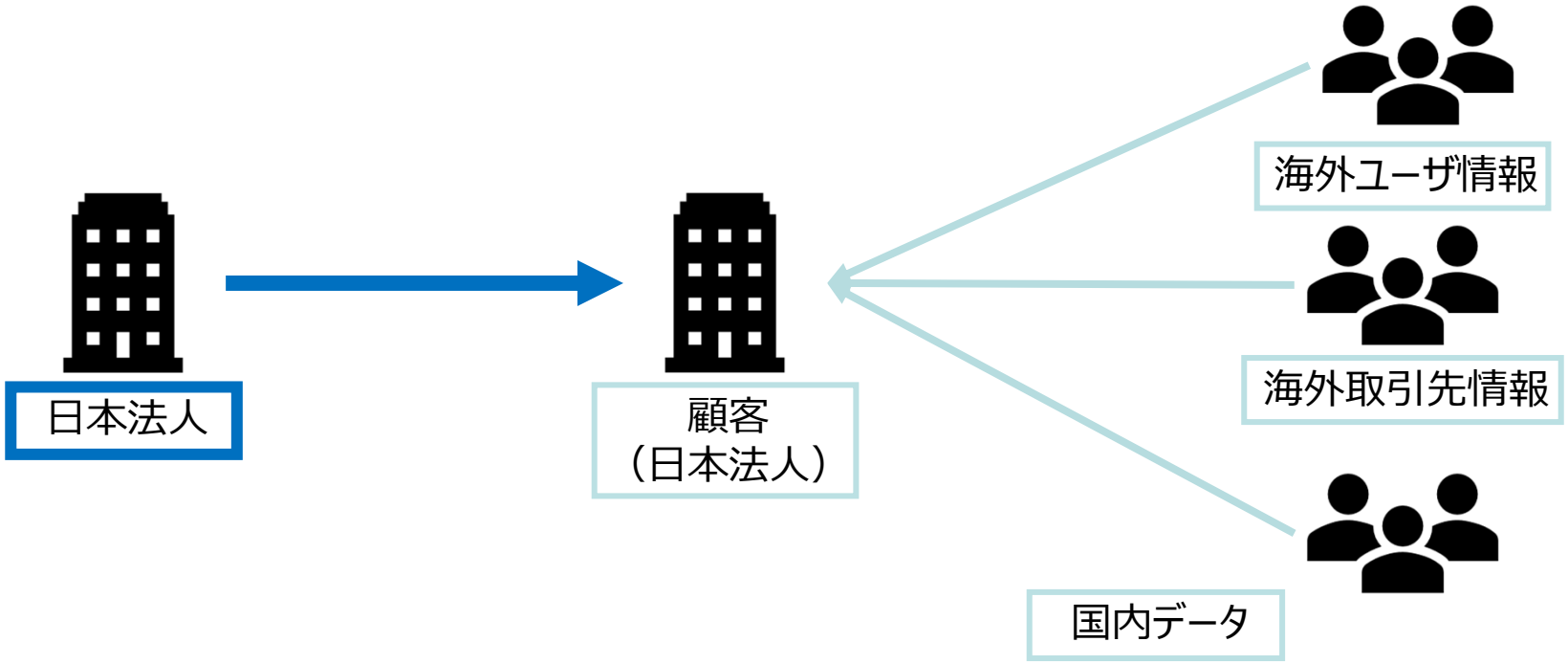
- 海外現地法人はない
- 他方、世界各国にスマホ用アプリを配信し、アカウント情報を取得



# （１）GDPR：頻出事例のご紹介③

## 処理者として適用されるパターン

- 海外現地法人・海外ビジネスなし
- 日本企業を中心にプラットフォームを提供し、当該顧客がプラットフォーム内に、海外個人データを取得・保有
- 顧客側から、海外データ保護規制に基づいて、個人情報の取扱いに関する契約（Data Processing Agreement）の締結を求められる



# （１）GDPR：主な対応事項

## General Data Protection Regulation(GDPR)
## 2018年5月25日施行

### 基本情報

- 広範な適用範囲
  **域外適用**
- 高額な制裁金
  **2000万ユーロ or**
  **世界総売上高の4%**
  **いずれか高い方**
- 迅速な当局報告
  **データ侵害認識時から**
  **72時間以内**

### 主な対応事項

１．個人データ処理の基本原則
２．プライバシーポリシー策定
３．データ主体の権利行使対応
４．処理業務の記録
５．安全管理措置の実装
６．データ侵害報告・通知の対応
７．DPAの締結
８．データ越境移転対応
（SCC/十分性認定の補完的ルール）
９．EU代理人の設置（必要な場合）
１０．DPOの設置（必要な場合）
１１．DPIAの実施（必要な場合）

# （１）GDPR：近時の注目すべきUpdate

## SCC（Standard Contractual Clauses）の改定版採択

7.6.2021 EN Official Journal of the European Union L 199/31

COMMISSION IMPLEMENTING DECISION (EU) 2021/914

of 4 June 2021

on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to 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) (1), and in particular Article 28(7) and Article 46(2)(c) thereof,

Whereas:

(1) Technological developments are facilitating cross-border data flows necessary for the expansion of international cooperation and international trade. At the same time, it is necessary to ensure that the level of protection of natural persons guaranteed by Regulation (EU) 2016/679 is not undermined where personal data is transferred to third countries, including in cases of onward transfers (2). The data transfer provisions in Chapter V of Regulation (EU) 2016/679 are intended to ensure the continuity of that high level of protection where personal data is transferred to a third country (3).

(2) Pursuant to Article 46(1) of Regulation (EU) 2016/679, in the absence of an adequacy decision by the Commission pursuant to Article 45(3), a controller or processor may transfer personal data to a third country only if it has provided appropriate safeguards, and on condition that enforceable rights and effective legal remedies for data subjects are available. Such safeguards may be provided for by standard data protection clauses adopted by the Commission pursuant to Article 46(2)(c).

(3) The role of standard contractual clauses is limited to ensuring appropriate data protection safeguards for international data transfers. Therefore, the controller or processor transferring the personal data to a third country (the 'data exporter') and the controller or processor receiving the personal data (the 'data importer') are free to include those standard contractual clauses in a wider contract and to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, the standard contractual clauses or prejudice the fundamental rights or freedoms of data subjects. Controllers and processors are encouraged to provide additional safeguards by means of contractual commitments that supplement the standard contractual clauses (4). The use of the standard contractual clauses is without prejudice to any contractual obligations of the data exporter and/or importer to ensure respect for applicable privileges and immunities.

(4) Beyond using standard contractual clauses to provide appropriate safeguards for transfers pursuant to Article 46(1) of Regulation (EU) 2016/679, the data exporter has to fulfil its general responsibilities as controller or processor under Regulation (EU) 2016/679. Those responsibilities include an obligation of the controller to provide data subjects with information about the fact that it intends to transfer their personal data to a third country pursuant to Article 13(1)(f) and Article 14(1)(f) of Regulation (EU) 2016/679. In the case of transfers pursuant to Article 46 of Regulation (EU) 2016/679, such information must include a reference to the appropriate safeguards and the means by which to obtain a copy of them or information where they have been made available.

(1) OJ L 119, 4.5.2016, p. 1.
(2) Article 44 of Regulation (EU) 2016/679.
(3) See also judgment of the Court of Justice of 16 July 2020 in Case C-311/18, *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems* ('Schrems II'), ECLI:EU:C:2020:559, paragraph 93.
(4) Recital 109 of Regulation (EU) 2016/679.

- 2021年6月4日、欧州委員会は、SCCの改定版を採択。
- **2021年9月27日以降は旧SCCは利用不可**
- **2021年9月27日以前に締結済の旧SCCは2022年12月27日まで有効（18か月間のtransition period）**
- 改定SCCは一般条項＋４モジュールの契約条項の構成。
  ①Controller to Controller
  ②Controller to Processor
  ③Processor to Processor
  ④Processor to Controller
- なお、日本－EU間は、十分性認定に基づく移転が可能。
  ※ただし、補完的ルールの遵守が前提。
  https://www.ppc.go.jp/files/pdf/Supplementary_Rules.pdf

出典：https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021D0914&from=EN

# （２）CCPA

## California Consumer Privacy Act (CCPA)
## 2020年1月1日施行

### 基本情報

- 広範な適用範囲
  **①CAで事業実施**
  **②CA個人情報を収集**
  **③３基準**
  **・売上2500万米ドル**
  **・5万人以上の取扱い**
  **・年間売上の50%**
- 法定損害賠償
  **消費者1人あたり1件につき**
  **100米ドル～750米ドル**

### 主な遵守事項

- CCPA対応プラポリ策定
- 消費者の権利行使（削除・開示・制限・移転等）対応
- ウェブサイトやフリーダイヤルによる窓口設置

### 関連遵守事項

- **データセキュリティ対策**
- **データ侵害報告・通知**

# （２）CCPA：主な対応事項

## California Consumer Privacy Act (CCPA)
## 2020年1月1日施行

### 基本情報

- 広範な適用範囲
  **①CAで事業実施**
  **②CA個人情報を収集**
  **③３基準**
  **・売上2500万米ドル**
  **・5万人以上の取扱い**
  **・年間売上の50%**

- 法定損害賠償
  **消費者1人あたり1件につき**
  **100米ドル～750米ドル**

### 主な対応事項

1. CCPA対応プライバシーポリシーの策定
2. 消費者による権利行使の対応
3. オプトアウト・オプトインへの対応
4. 消費者の権利行使に関する差別的取扱禁止
5. 合理的なセキュリティ施策構築
6. インシデント対応準備
7. 委託先との契約見直し（必要な場合）
8. CPRA対応（必要な場合）

# （２）CCPA：近時の注目すべきUpdate

## California Privacy Rights Act（CPRA）の可決

- 2020年11月3日、カリフォルニア州の住民投票で、CCPAを改正する内容のCPRAが可決。
- 2023年1月1日から適用開始予定であり、2022年1月1日以降に収集された個人情報が対象となる予定。

## CPRAによる主な追加規制の概要

1．対象事業者の範囲を拡大：40%以上の持分を有するJV等
2．対象情報につき「センシティブ個人情報」の概念を新設
3．「プロファイリング」の概念を新設
4．個人情報の「共有」の概念を新設（CCPAの「売却」とは異なる）
5．「コントラクター」の概念の新設

# （３）中国サイバーセキュリティ法

## Cybersecurity Law /2017年6月1日施行

- 中国国内におけるネットワークの構築、運営、維持及び使用並びにサイバーセキュリティの監督管理について適用
- 重要情報インフラ運営者：公共通信・情報サービス、エネルギー、交通、金融等の重要な産業及び分野の運営者
- ポイント
  - **安全保護義務の履行（21条）**
  - **インシデント対応策の制定（25条）**
  - **個人情報の安全管理措置・インシデント発生時の通知報告義務（42条）**
  - **国内データの国内保管（37条。ネットワーク運営者は意見募集稿段階）**
  - **国内データの国外移転時のセキュリティ評価の実施（同上）**
  - 罰則・主管部門による是正命令（59条～75条）

# （３）中国個人情報保護法

**2021年11月1日施行予定**

## 基本情報

- 広範な適用範囲
  **域外適用**
- 強力な行政権限
  **業務停止命令**
  **業務・営業許可の取消命令**
  **制裁金**
- 詳細が未定
  **ガイドライン等が未公表**

## 主な遵守事項

- 中国個人情報保護法対応プライバシーポリシー策定
- 個人情報取扱の正当化事由
- 本人による権利行使対応
- 自動的決定のオプトアウト
- 個人情報の第三者提供に係る本人同意の取得
- **個人情報の国内保存義務と個人情報の越境移転対応**
- **安全管理措置の実施**
- **セキュリティインシデント対応（救済措置・報告・通知）**

# （３）中国個人情報保護法：適用範囲

**１．中国国内で自然人の個人情報を処理する活動**

**２．中国国外で中国国内の自然人の個人情報を処理する活動であって、以下のいずれかと関連する処理**

- **中国国内の自然人への商品・役務の提供**
  - ✓中国国内顧客向けECサイト運営
- **中国国内の自然人の行為を分析又は評価する行為**
  - ✓ウェブサイトにおけるCookie取得によるターゲティング広告
- **法律、行政法規に規定されたその他の場合**
  - ※現状、特別な規定がない

# （４）基本的な対応事項まとめ

- プライバシーポリシーの各国法対応版策定
- 個人情報取扱規程の各国法対応特則策定
- 情報セキュリティポリシーの各国法対応特則策定
- インシデント対応フローの各国法対応版の策定
- データの越境移転規制への対応
- データの処理委託に関する契約の整備

# （番外）アジア各国におけるデータ保護法制

## アジア各国におけるデータ保護法制

タイ： Cybersecurity Act B.E. 2562 (2019)
Personal Data Protection Act 2019

ベトナム：The Law on Cybersecurity
Draft Decree on Personal Data Protection

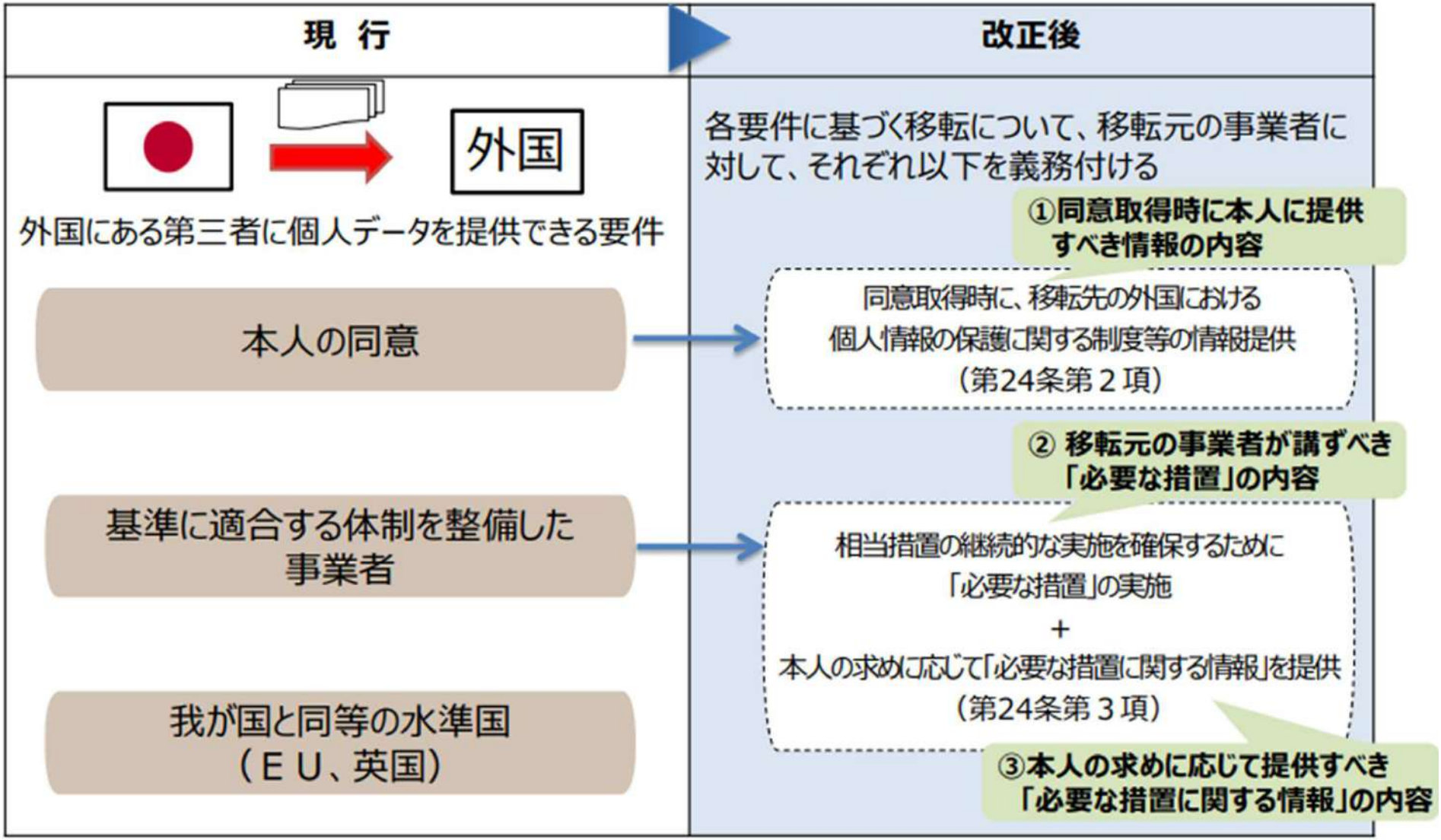
シンガポール：Personal Data Protection Act 2020

フィリピン：Data Privacy Act of 2012

マレーシア：Personal Data Protection Act 2010

**消費者保護に手厚いデータ保護法の制定がトレンド**

# （番外）令和2年改正個情法：越境移転規制




出典：個人情報保護委員会「改正法に関連する政令・規則等の整備に向けた論点について（越境移転に係る情報提供の充実等）」令和2年11月4日　https://www.ppc.go.jp/files/pdf/201104_ekkyouiten.pdf

# （番外）Cookie規制とCMP

## CMP（Consent Management Platform）とは


- 同意管理プラットフォーム
- GDPR及びeプライバシー指令への対応で発展
- 日本においてもCMP導入は増加傾向

出典：
TMIプライバシー＆セキュリティコンサルティング株式会社
ウェブサイト
https://tmiconsulting.co.jp/

※試験導入しているもの

# （番外）Cookie規制とCMP


## CMPの機能

- ポップアップによる同意取得
- ユーザへの同意管理機能の提供
- 事業者への同意確認機能の提供
- ユーザへの情報提供

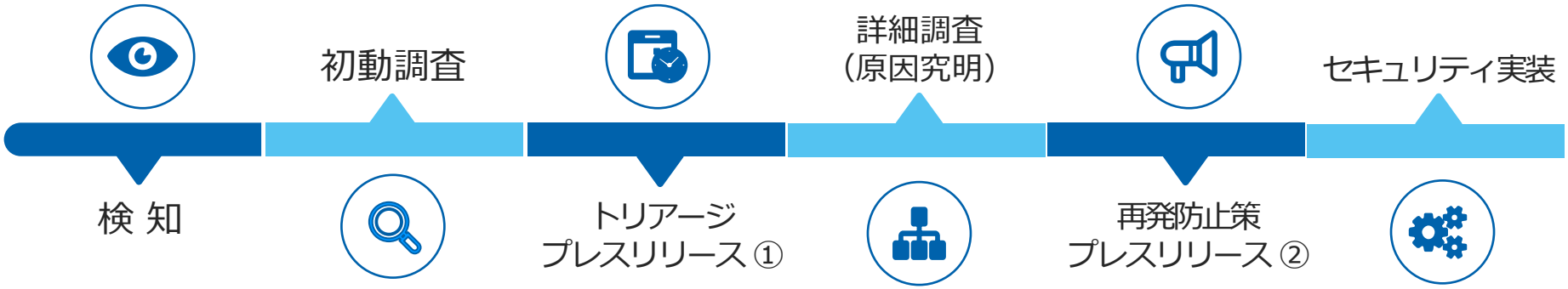
出典：
TMIプライバシー＆セキュリティコンサルティング株式会社
ウェブサイト
https://tmiconsulting.co.jp/

※試験導入しているもの

# ２．海外ビジネスにおけるインシデント対応

（１）情報漏えいインシデント対応の全体像
（２）海外におけるインシデント対応の留意点

# （１）情報漏えいインシデント対応の全体像




**初動調査支援**

- 初動対応アドバイス

**トリアージ、被害拡大防止支援**

- トリアージアドバイス
- フォレンジック業者選定
- フォレンジック調査のスコープ決定・ディレクション
- 第三者委員会組成
- 詳細調査実施

**再発防止策策定支援**

- 組織再編プラン
- セキュリティシステムプラン

**セキュリティ実装支援**

- 規程類見直し
- インシデント対応フロー見直し
- セキュリティシステム導入

**IR・広報お客様対応支援**

- 1次プレスリリース(初動版)作成
- 本人通知作成(メール・郵便)
- 記者会見セット・リハ
- 適時開示
- コールセンタのセット
- お客様対応アドバイス(クレーム処理方針)
- 2次プレスリリース(フル版)作成
- 本人通知作成
- 記者会見セット・リハ
- 適時開示

**当局対応支援**

- 1次報告 個人情報保護委員会
- IPA・JP-CERT
- サイバー犯罪対策課
- 当局対応
- 2次報告

**被害補償対応支援／被害回復支援**

- 被害補償対応
- ベンダへの請求
- 刑事告訴

# （２）海外におけるインシデント対応の留意点

- 日本法とは別途、海外法の検討が必要
- スピード重視：GDPRは認識後72時間以内
- フォレンジック業者選定の困難

**①各国ローファーム・フォレンジック業者との連携**

**②海外法令対応インシデント対応フローの策定**

**③想定事案を用いたリハーサル**

# ３．コンプライアンス体制整備の実務

# グローバル平時対応のポイント

- 適用法令の検討：**データマッピングの実施**
- 適用法令の内容把握：**法令調査の実施**
- 体制整備の検討：**Fit&Gapアセスメント実施**
- 実装：**各種ドキュメント作成・システム実装など**

# グローバル平時対応のポイント

| | |
|---|---|
| 現状把握<br>データマッピング | ● 商流把握<br>● 取扱いデータの棚卸し |
| 各規制の洗い出し | ● 個人情報保護法及びプライバシー保護規制<br>● 海外データ保護規制<br>● 監督官庁等のガイドライン |
| Fit & Gap | ● 各規制の要求事項と現状の体制を比較<br>● あるべき姿と現状のGapを洗い出し |
| リスクアセスメント | ● Gap事項のリスク評価<br>● セキュリティリスクアセスメント |

# グローバル平時対応のポイント

| | |
|---|---|
| クリアランス計画 | ● Fit & Gap分析をベースにGap事項への対応方法を策定<br>● 同意取得方法の見直し<br>● サービス設計の見直し |
| 実装プロセス | ● プライバシーポリシーやクッキーポリシーの整備<br>● 社内規程・マニュアルの整備<br>● データ提供・連携契約の見直し<br>● システム実装 |
| 運用 | ● 教育<br>● 定期監査<br>● 法改正対応等の見直し |

# グローバル平時対応のポイント

- 法令の概要と自社への適用可能性の検証
- 外国法規制の遵守対応プロセスの実施

**SaaSプラットフォーム、アプリ、サービス展開における海外法令対応・認証取得対応がトレンド**

**∵ユーザー企業に選ばれるため**

**⇒要件定義・開発段階からのリーガルサポートが必須**

# （ご参考）データ利活用支援メニュー


## データの収集

- データマッピング作成
  （散在するデータを収集・集約）
- デジタルトランス
  フォーメーション（DX）支援
  （データ化されていないデータを発掘）
- 価値あるデータと無価値な
  データの分別
- プライバシーポリシーの整備
- クッキーポリシーの整備

## データ管理体制

- セキュリティ アセスメント
- クラウド利用のための
  アセスメント

## データ匿名化処理

- 匿名化処理などリスク
  低減化プラン策定
- 再識別化リスクアセスメント

## データの第三者との連携

- データ連携・提供契約の締結
- API 連携ポリシーの策定

## データの利用

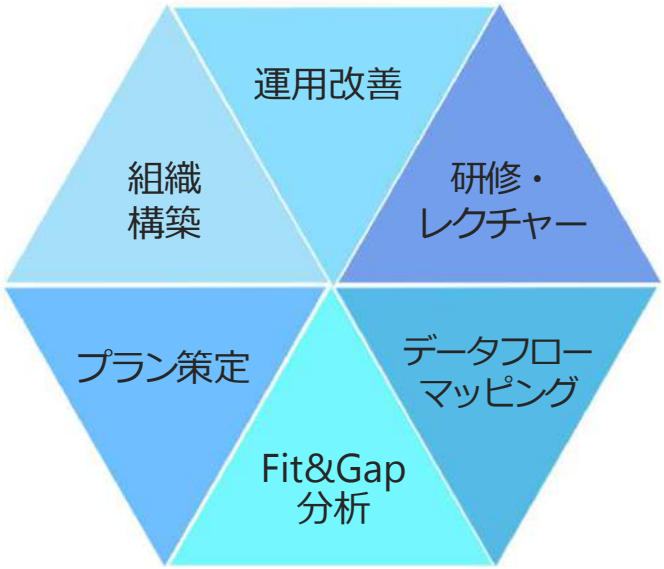
- ターゲティング広告
- CRM 施策の検討
- データの第三者への販売支援

## メディアの選別

- ブランド（レピュテーション）
  コントロール
  - 不適切なメディアへの掲載を防止
  - ブランドセーフティ
  - アドベリフィケーション
- アドフラウド（広告不正）
  防止対策

# （ご参考）セキュリティ体制構築と支援メニュー

**経営責任 / 説明責任**




## 組織構築

- 各種規程の改定
- セキュリティ管理委員会組成
- セキュリティ施策実装
- サイバー保険の導入支援

成果物例：
・各種ポリシー
・各種規程・マニュアル

## 研修・レクチャー

- プロジェクト当初における経営層レクチャー
- プロジェクト最終における事業部レクチャー

成果物例：レクチャー資料

## Fit&Gap 分析

- セキュリティアセスメント
- プライバシーインパクトアセスメント

成果物例：Fit&Gap シート

## 運用改善

- セキュリティ管理委員会運用
- インシデント発生時の有事対応

成果物例：
セキュリティ管理委員会参加

## データフローマッピング

- ビジネスフローマッピング
- データフローマッピング

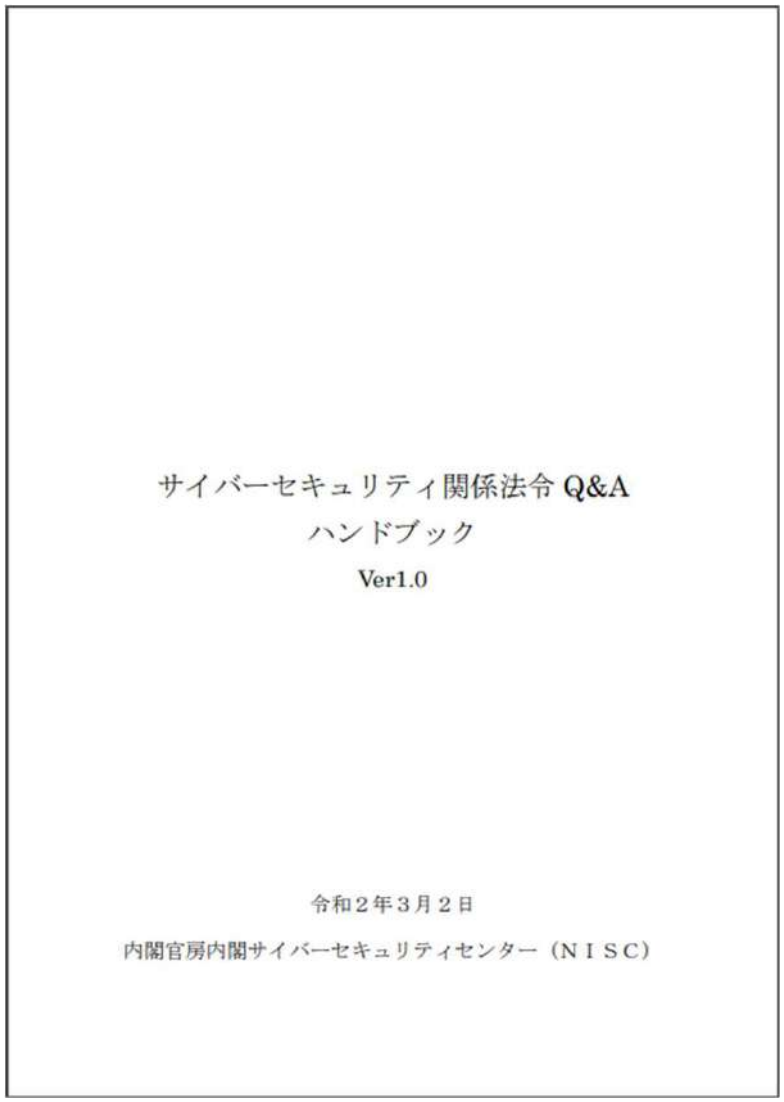
成果物例：
・ビジネスフローシート
・データマッピングシート

## プラン策定

- GAP 事項のクリアランス計画策定

成果物例：
クリアランス計画書

# （ご参考）サイバーセキュリティ関係法令Q&Aハンドブック

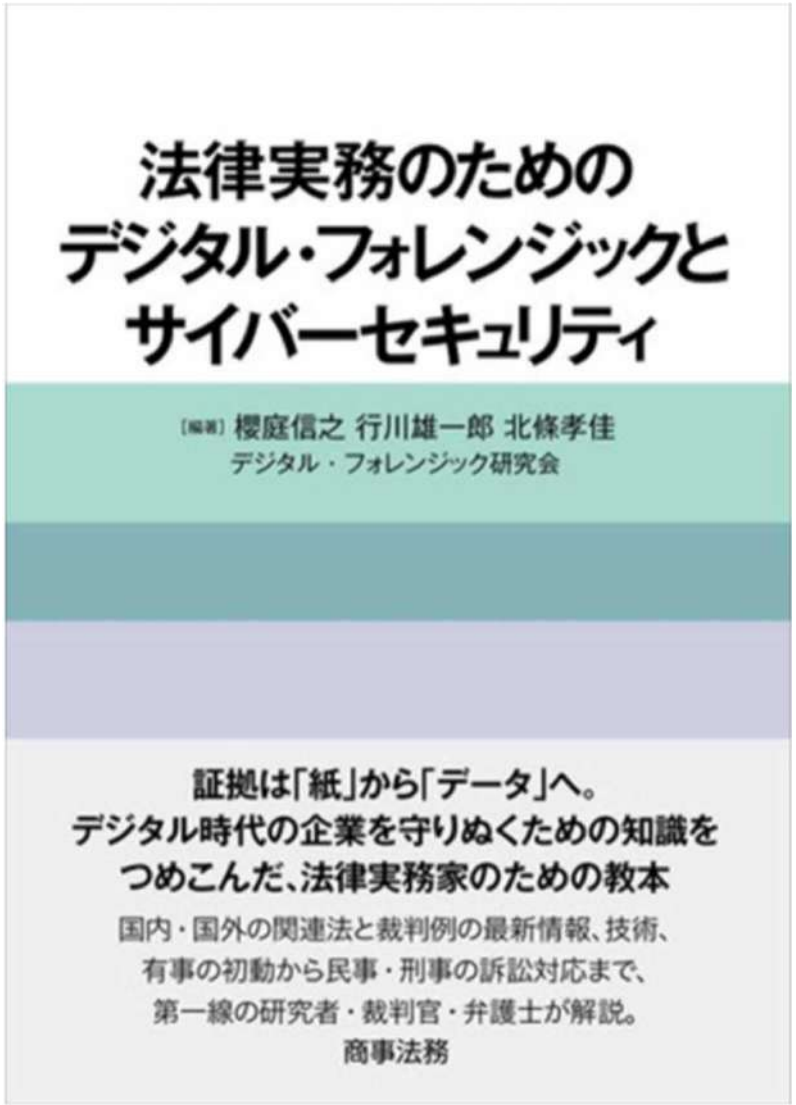



## ◆ Q&Aで取り上げている主なトピックス

1. サイバーセキュリティ基本法関連
2. 会社法関連（内部統制システム等）
3. 個人情報保護法関連
4. 不正競争防止法関連
5. 労働法関連（秘密保持・競業避止等）
6. 情報通信ネットワーク関連 （IoT関連を含む）
7. 契約関連（電子署名、システム開発、クラウド等）
8. 資格等（情報処理安全確保支援士等）
9. その他各論（リバースエンジニアリング、暗号、情報共有等）
10. インシデント対応関連（デジタルフォレンジックを含む）
11. 民事訴訟手続
12. 刑事実体法（サイバー犯罪等）
13. 海外法令（GDPR等）

出典：NISCウェブサイト「『サイバーセキュリティQ&Aハンドブック』について」参照
https://www.nisc.go.jp/security-site/law_handbook/index.html

# （ご参考）法律実務のためのデジタル・フォレンジックとサイバーセキュリティ




出典：株式会社商事法務ウェブサイト参照
https://www.shojihomu.co.jp/publication?publicationId=15551835

**第1章　国内法制**

サイバーセキュリティ基本法と関連法

**第2章　各種インシデント対応**

第1　不正アクセス事案等に対するデジタル・フォレンジックを含む諸対応

第2　テレワーク・IoT・脅威インテリジェンスサービスとリスク管理

第3　クラウドサービスのセキュリティと証拠収集

第4　海賊版サイト対策と応用可能性クロスボーダー型訴訟

第5　ブロックチェーンの仕組みとインシデント問題

第6　不祥事調査と法的責任

第7　サイバー・フィジカル・システムに対するサイバー攻撃と刑法的対応

**第3章　裁判手続**

第1　民事訴訟　　第2　刑事訴訟

**第4章　判例**

第1　デジタル・フォレンジック関連の民事裁判例

第2　サイバーセキュリティ関連の民事裁判例

**第5章　技術**

第1　コンピュータ概論

第2　デジタル・フォレンジックの手法

**第6章　外国法制**

サイバーセキュリティの外国法規制の概要

# ご清聴ありがとうございました

ご質問がありましたら、ご遠慮なく下記までご連絡ください。

E-mail：sterakado@tmi.gr.jp
URL：http://www.tmi.gr.jp/staff/s_terakado.html