

# 米国・EUのサイバーセキュリティ法制

2020年11月29日 @九州大学SECKUN  
弁護士（日本・ニューヨーク） 有本真由

## 経歴

---

- 2005年 東京大学法学部卒
- 2010年 弁護士登録（東京弁護士会）
- 2010年 小川綜合法律事務所 入所
- 2017年 米Columbia Law School法学修士（LLM）修了
- 2018年 米ニューヨーク州弁護士 登録
- 2020年 アレシア国際法律事務所 開所
- 



## 所属団体

---

情報ネットワーク法学会会員

CSAジャパン運営委員

一般社団法人スタートアップレ  
ディ協会理事 など

---

# 内 容

1. サイバーセキュリティとは
2. 米国とEUの基本的な法律と組織
3. 電子署名の話～eIDAS規則など
4. 電子証拠の越境アクセス

# 1. サイバーセキュリティとは

# 「サイバーセキュリティ」の定義

## ■ サイバーセキュリティ基本法2条

「電子的方式、磁気的方式その他の知覚によっては認識することができない方式（以下この条において「電磁的方式」という。）により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置（情報通信ネットワーク又は電磁的方式で作られた記録に係る記録媒体（以下「電磁的記録媒体」という。）を通じた電子計算機に対する不正な活動による被害の防止のために必要な措置を含む。）が講じられ、その状態が適切に維持管理されていることをいう。」

# 「サイバーセキュリティ」の定義

## ■ CISAにおける定義

..., the term “**cybersecurity threat**” means an action, not protected by the First Amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system. (6 U.S.C. § 1501)

「サイバーセキュリティ脅威」は、合衆国憲法修正第1条で保護されていない行動であって、情報システム、または情報システムに保存、処理、または情報システムを通過する情報のセキュリティ、可用性、機密性、または完全性に悪影響を与える可能性のある、情報システム上または情報システムを介した行動を意味する。

# 「サイバーセキュリティ」の定義

## ■ EU Cybersecurity Actにおける定義

‘**cybersecurity**’ means the activities necessary to protect network and information systems, the users of such systems, and other persons affected by **cyber threats**; (ネットワーク及び情報システム、そのようなシステムの利用者、並びに、サイバー脅威による影響を受けるその他の者の防護のために必要となる活動)

‘**cyber threat**’ means any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons; (「サイバー脅威」とは、ネットワーク及び情報システム、そのようなシステムの利用者及び影響を受けるその他の者に対し損害、危殆またはそれ以外の負の影響を与え得る可能性のある状況、出来事または行動のことを意味する)

(翻訳は[夏井高人先生](#)による)

# 「情報セキュリティ」と「サイバーセキュリティ」

## ■ 情報とデータに関する三分法（西貝吉晃先生「サイバーセキュリティと刑法」）

- 情報：内容に着目した概念
- データ：表現形式（デジタルデータとアナログデータ）
- 存在形式：（有体物か、電磁的形式か）





# 情報セキュリティにおけるCIA

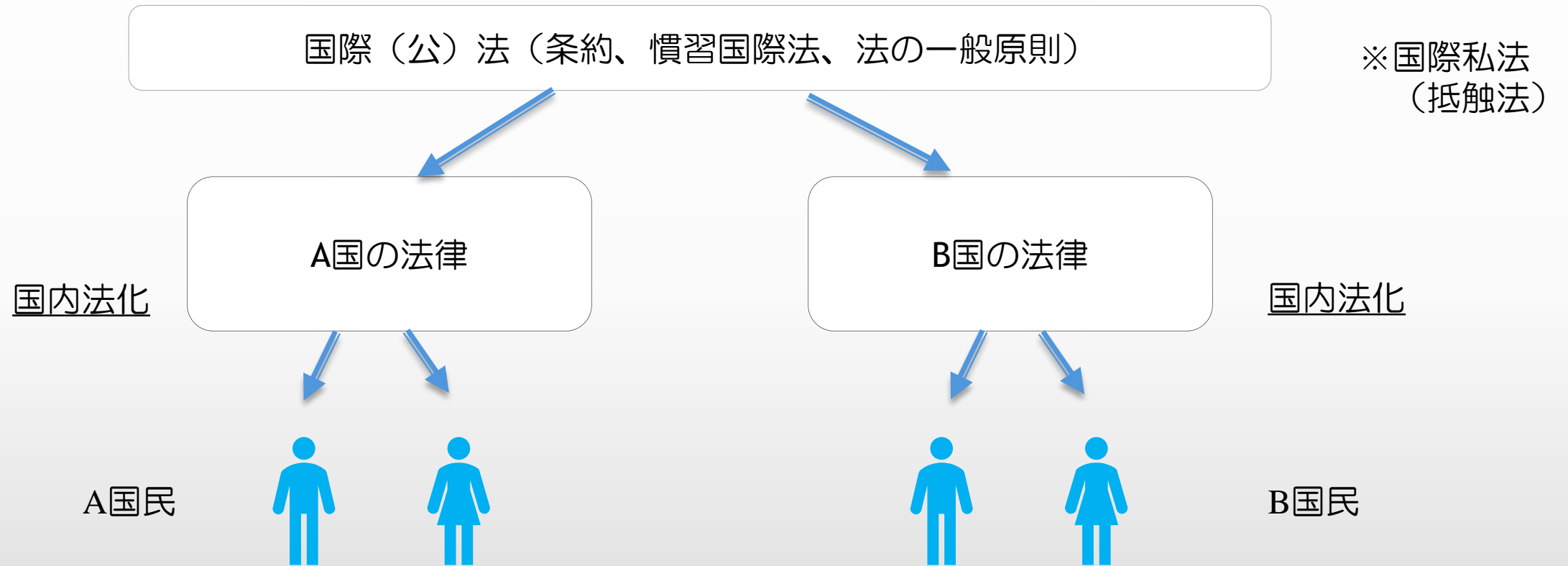
- 情報セキュリティ：「情報の機密性、完全性、可用性を維持すること」

機密性	Confidentiality	無権限者に情報が取得されないこと
完全性	Integrity	情報の不可変更改性（情報内容の同一性） と情報の真正性（作成名義の同一性）
可用性	Availability	権限のある主体が要求したときに、アクセス及び使用が可能であること

（西貝吉晃先生「サイバーセキュリティと刑法」）

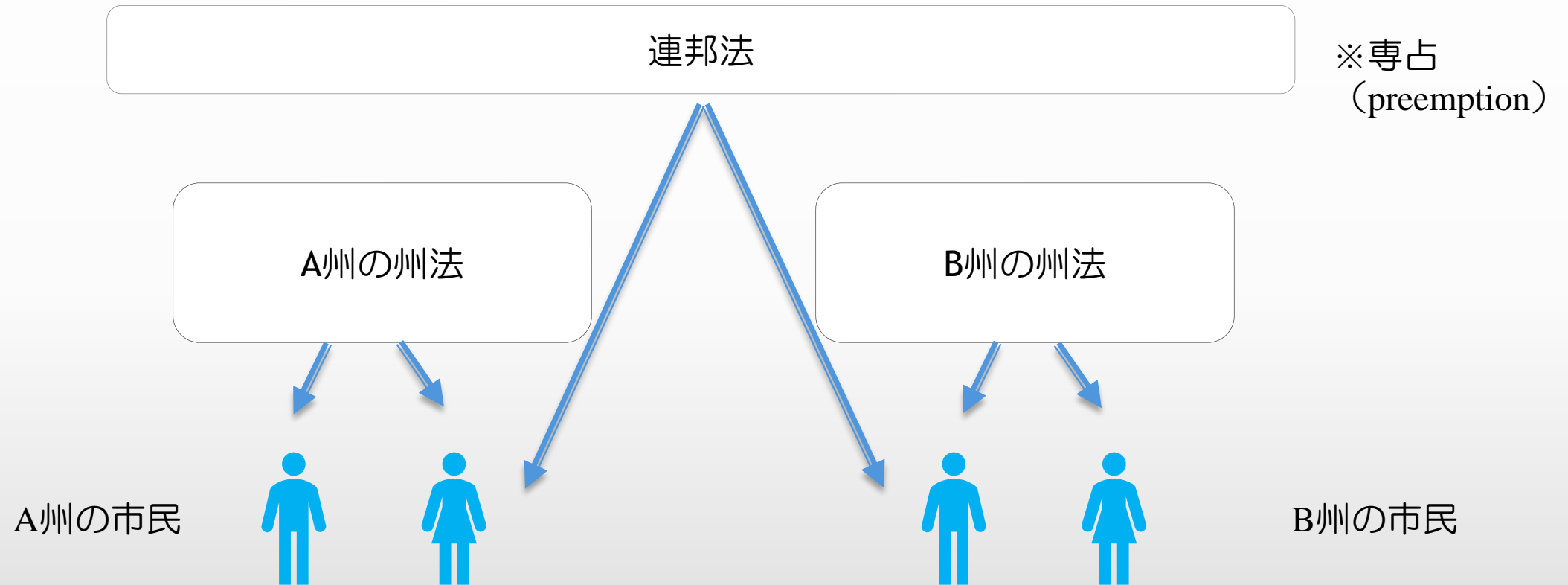
## 2. 米国とEUの基本的な法律と組織

# 国際法と各国法の関係



※国際弁護士？

# 連邦法と州法の関係（米国）



※ Uniform Acts（統一法）

※ 横出し、上乗せ（Security breach notification lawsなど）

# 連邦の法令（米国）

## ■ Act（法律）

- Bill（法案）
- U.S.C.（United States Code; 合衆国法典）
  - Ex. 44 USC § 3551

## ■ 大統領令

- Executive Order

## ■ Regulation（規則）

- 連邦規則集（Code of Federal Regulations; CFR）
  - Ex. 連邦調達規則（Federal Acquisition Regulation; FAR）

立法府

行政府

司法府

## USC

Title 1

Title 2

Title 3

Chapter 1～

Section 1～

- 
- 
- 
- 
- 

Title 54

# コモンローと大陸法

- コモンロー（common law）：判例法中心
- 大陸法（civil law）：制定法中心

両者の違いのセキュリティ法に対する影響

- 裁判所の権限が大きい
- セキュリティ法は比較的新しい
- 基本法？

# 米国のセキュリティ法（連邦法）

## ■ Federal Information Security Modernizing Act of 2014 (FISMA)

- 44 USC § 3551～
- Federal Information Security Management Act of 2002を改正
- 連邦機関において省庁内全体に及ぶ情報セキュリティプログラムを策定、文書化、実装することを義務づけ。
- risk-based policy for cost-effective security

# 米国のセキュリティ法（連邦法）

## ■ Federal Information Security Modernizing Act of 2014 (FISMA)

- **FIPS** (Federal Information Processing Standards): 連邦の公式規格
- **NIST SP** (special publications): NISTが発表するガイドライン等
  - **FIPS 199**: “Standards for Security Categorization of Federal Information and Information Systems”
    - 情報とシステムの影響値を、low, moderate, highに分類
    - このガイドラインとして、**NIST SP800-60** “Guide for Mapping Types of Information and Information Systems to Security Categories”
  - **FIPS 200**: “Minimum Security Requirements for Federal Information and Information Systems”
    - **NIST SP800-53** “Recommended Security Controls for Federal Information Systems”
    - FISMAに基づく連邦情報システムのセキュリティ標準及びガイドラインを提供する



# 米国のセキュリティ法（連邦法）

## ■ Cybersecurity Information Sharing Act of 2015 (CISA)

- 6 U.S.C.（合衆国法典） § 1501～
- 企業間、企業・政府間のサイバー脅威の情報共有を推進（AISなど）

## ■ Cybersecurity Enhancement Act of 2014 (CEA)

- 6 U.S.C. § 7421
- サイバーセキュリティに関する研究・人材・教育の支援
- National Institute of Standards and Technology (NIST)による技術要件の作成

※ NIST（国家標準技術研究所）

# 米国のセキュリティ法（連邦法）

## ■ The Federal Trade Commission Act（連邦取引委員会法）

- 15 U.S.C. § § 41-58、1914年
- 連邦レベルの消費者保護法。商取引（commerce）における不公正又は詐欺的取扱い（unfair or deceptive practices）を根拠に禁じる。オフライン及びオンラインのデータセキュリティポリシーに適用される。FTCは、同法に基づき、ポリシーの不遵守を取り締まっている。

## ■ Gramm-Leach-Bliley Act（GLBA又は金融サービス近代化法）

- 15 U.S.C. § § 6801-6809, § § 6821-6827、1999年
- 金融機関による非公開個人情報（Non-Public Personal Information; NPI）の収集・使用・開示を規制。各種金融機関及び金融商品を扱う事業会社に適用される。

# 米国のセキュリティ法（連邦法）

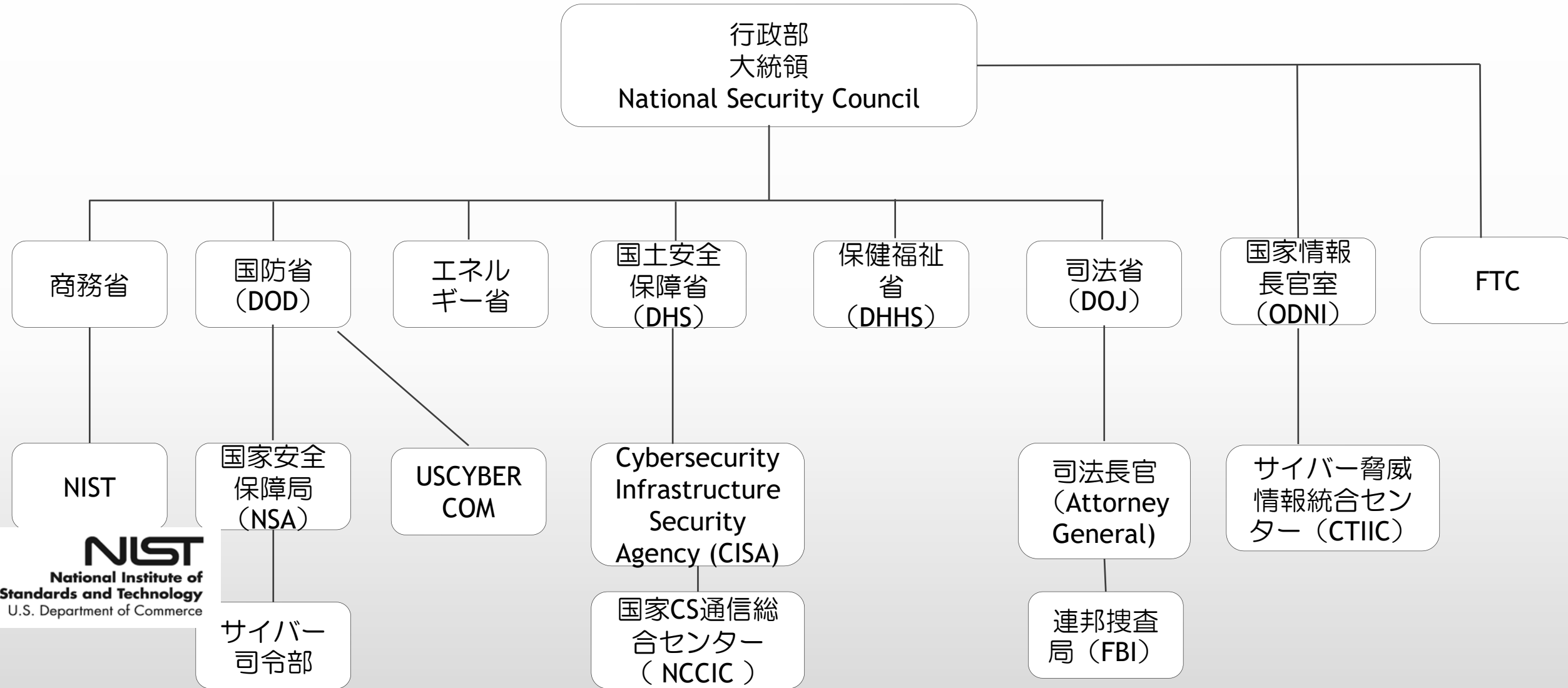
- The Health Insurance Portability and Accountability Act (HIPAA)
  - 42 U.S.C. §1301 et seq., 1996年
  - 医療情報の収集・使用・開示を規制。医療情報を保有しうるすべての団体に適用される。
  - HIPAA Omnibus Rule: 保護対象健康情報（protected health information (PHI)）の収集・使用に関する下位規則
    - HIPAA Privacy Rule
    - Protection of Electronic Protected Health Information (HIPAA Security Rule)

# 米国のセキュリティ法（連邦法）

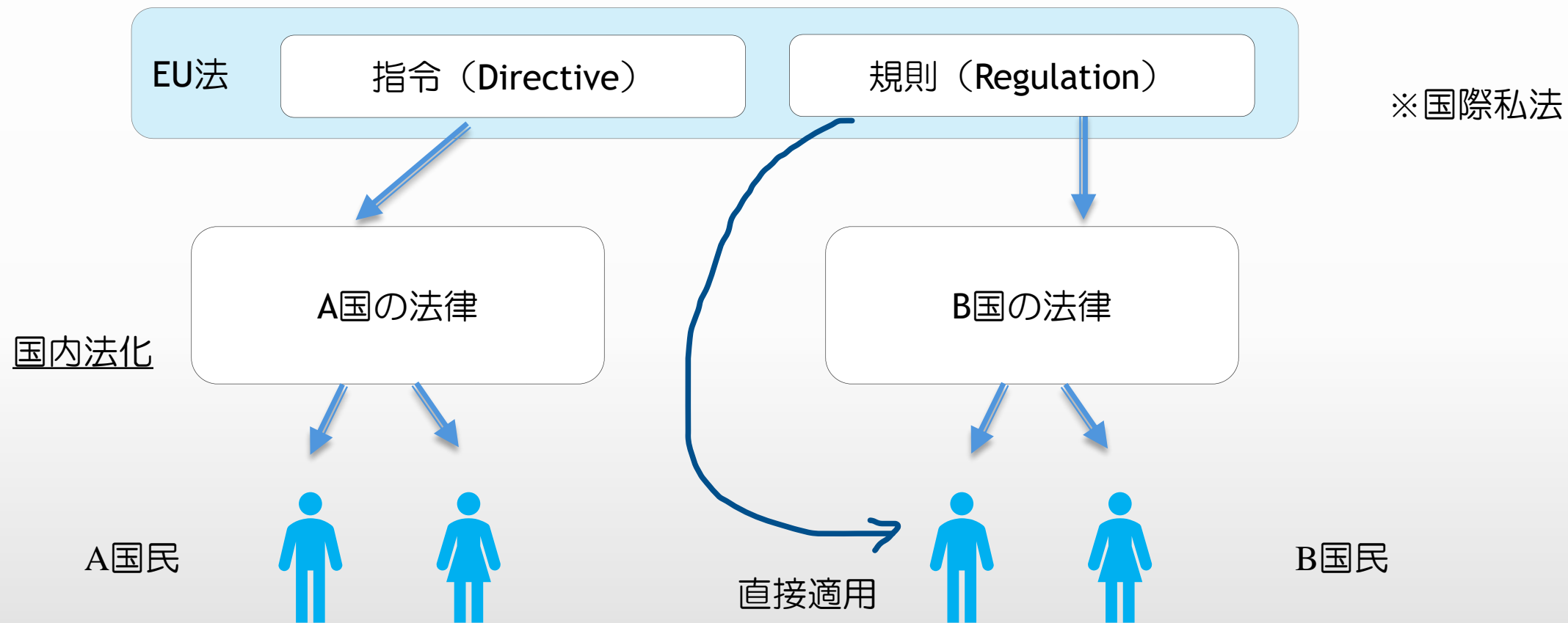
## ■ The Computer Fraud and Abuse Act (CFAA)

- 18 U.S.C. § 1030、1986年
- コンピュータにかかる詐欺及び不正アクセスを規制。

## 【組織図】



# EU法と加盟国法の関係



# EUのセキュリティ法

## ■ NIS Directive

- ネットワーク・情報システムに係るEU共通の高度な安全水準のための措置に関する指令
- 指令(EU) 2016/1148
- サイバーセキュリティ対策に関する初めての共通立法
- 加盟国におけるCS関連のリスクやインシデントに対する対処能力の向上、情報共有・域内の協力促進、重要インフラを保有する企業に対するリスク管理・インシデント報告の義務付け

# EUのセキュリティ法

## ■ GDPR

- 規則(EU) 2016/679
- 個人データ保護
- EDPB (欧州データ保護委員会)

## ■ Cybersecurity Act

- 規則(EU) 2019/881
- ENISA (European Agency for Network and Information Security) の権限強化 (EU Cybersecurity Blueprint)
- ICT製品のCS証明書フレームワークの導入
- ECCG (European Cybersecurity Certification Group)の導入

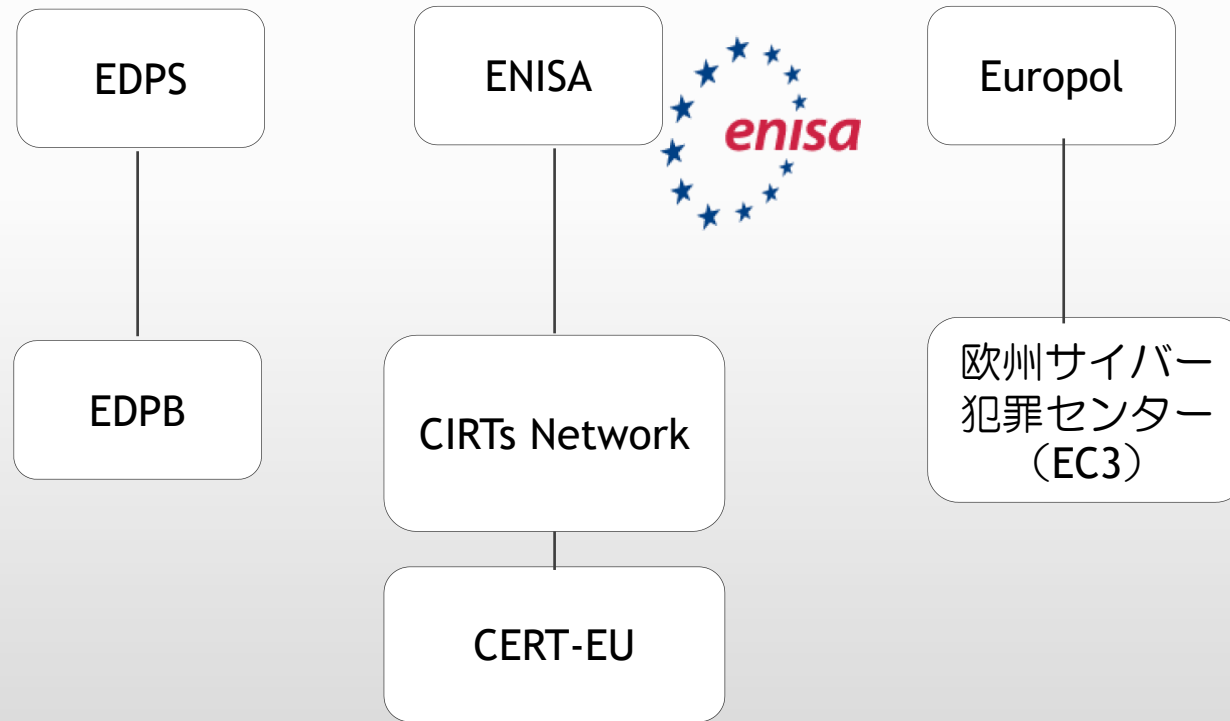


# EUのセキュリティ法

## ■ サイバー犯罪条約

- 欧州評議会が発案
- 米国、日本も加盟
- 不正アクセス、オンライン上の児童ポルノ、著作権侵害等を規制

【組織図】



### 3. 電子署名の話～ eIDAS規則など

# 電子署名（米国）

## ■ E-Sign Act of 2000 (Federal Electronic Signature in Global and National Commerce Act)

- **electronic signature**
- an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record. (15 USC § 7006(5))
- 法的効果
  - (a) 署名や記録は、電子形式であることを理由に法的効果を否定されない。
  - (b) 契約は、電子記録であることを理由に法的効果を否定されない。
  - (c) 法律上何らかの記録が書面に基づくことが必要である場合、電子文書で足りる（例外あり）。
  - (d) 法律上何らかの署名が必要である場合、e-signatureで足りる（例外あり）。

## ■ Uniform Electronic Transaction Act (UETA)

- 州の統一法、47州が採択

# 電子署名（米国）

- E-signatureとして認められる場合
  - Sign and scan
  - I agree, I consent
  - 署名を写真で撮ってそれを文書に貼る
  - DocuSign, Adobe Signなど

# 電子署名（米国）

- 金融機関に対しては消費者保護の措置（明白な同意など）
- Wet ink署名が必要な場合
  - 遺言
  - 家族法に関する書面（離婚、養子縁組など）
  - 不動産にかかる重要書類
  - 判決など

# E-signatureとdigital signature（米国）

## ■ Digital signature

- “[t]he result of a **cryptographic** transformation of data that, when properly implemented, provides a mechanism for verifying origin authentication, data integrity and signatory non-repudiation” (NIST, Federal Information Processing Standards Publication, Digital Signature Standard)
- 暗号化によって非改変性

# 電子署名の松竹梅

- E-signature（一般的なe署名）
- Advanced electronic signature（認証と本人確認において一定の要件）
- Digital signature（暗号化技術を伴う）
- Qualified electronic signature（本人確認、認証、非改変性について政府等による認定あり、多要素認証や暗号化など）



# 電子署名（日本）

## ■ 電子署名及び認証業務に関する法律（2000年制定）

（定義）

2条1項 この法律において「**電子署名**」とは、電磁的記録（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるものをいう。以下同じ。）に記録することができる情報について行われる措置であって、次の要件のいずれにも該当するものをいう。

一 当該情報が当該措置を行った者の作成に係るものであることを示すためのものであること。 ←**本人性**

二 当該情報について改変が行われていないかどうかを確認することができるものであること。 ←**非改変性**

⇒ 公開鍵暗号（PKI）方式が主流だが、それに限定していない

# 前提として...

## ■ 契約の成立に必要なのは...（原則）

申し込み（意思）⇔ 承諾（意思）

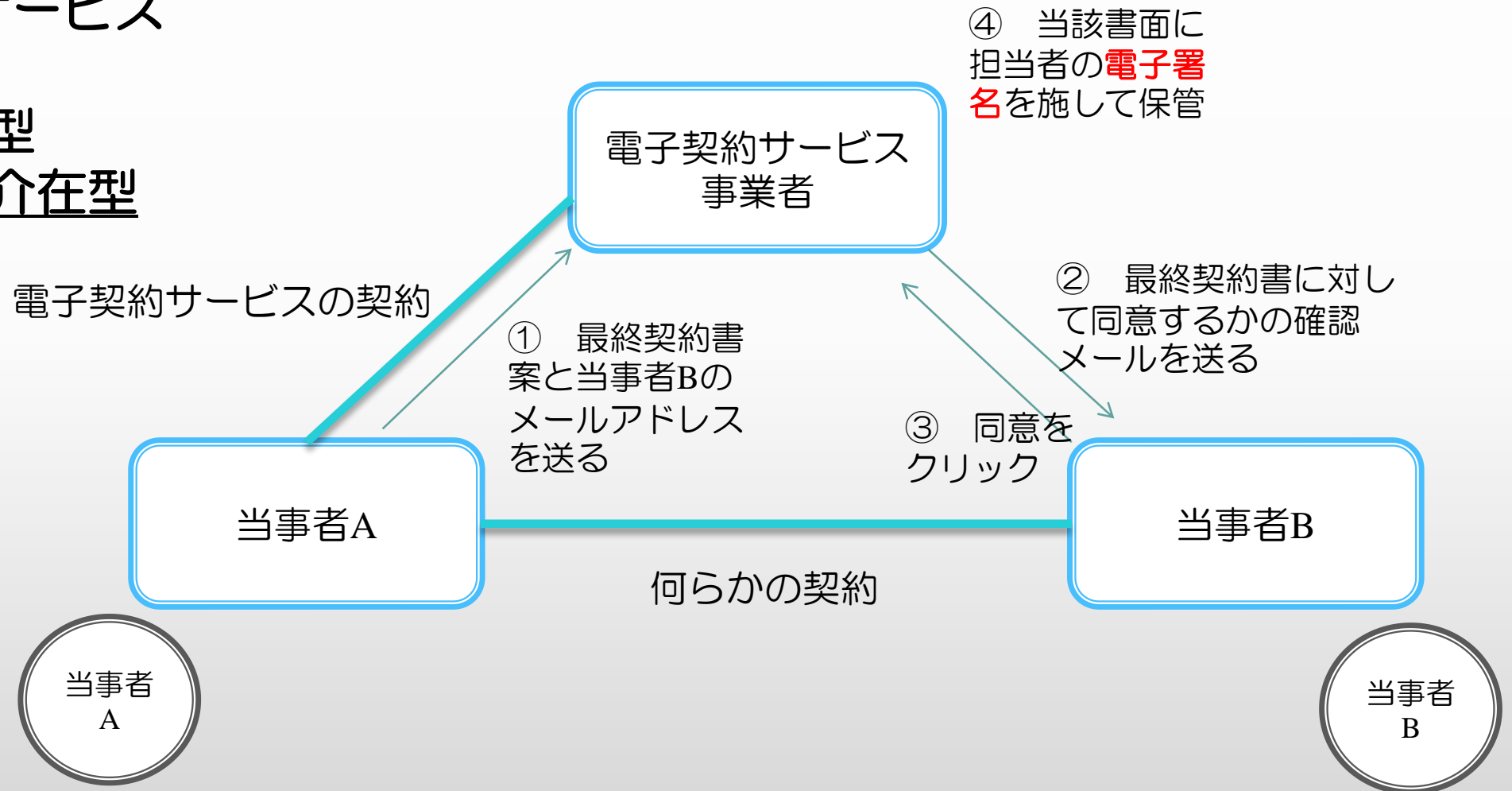
「意思の合致」があればよい。

署名も捺印も電子署名も不要。口頭でOK

# 三省見解（2020年）の背景

## ■ 電子契約サービス

- 当事者型
- 事業者介在型



## 2条1項に関する三省見解

### ■ 「電子署名法2条1項に関するQ&A」（2020年7月8日）

「電子署名法第2条第1項第1号の「当該措置を行った者」に該当するためには、必ずしも物理的に当該措置を自ら行うことが必要となるわけではなく、例えば、物理的にはAが当該措置を行った場合であっても、Bの意思のみに基づき、Aの意思が介在することなく当該措置が行われたものと認められる場合であれば、「当該措置を行った者」はBであると評価することができるものと考えられる。」

# 2条1項に関する三省見解

## ■ 「電子署名法2条1項に関するQ&A」（2020年7月8日）

- これで何が変わるか？
  - ⇒ 取締役会議事録など電子署名が要求されている文書について  
事業者型でもOKということに
- 問題は？

# 電子署名法3条

## ■ 電子署名及び認証業務に関する法律（2000年制定）

3条 電磁的記録であって情報を表すために作成されたもの（公務員が職務上作成したものを除く。）は、当該電磁的記録に記録された情報について**本人による電子署名（これを行うために必要な符号及び物件を適正に管理することにより、本人だけが行うことができることとなるものに限る。）**が行われているときは、真正に成立したものと推定する。

➤ 固有性の要件

➤ （参考）二段の推定

## 二段の推定とは

当該文書に本人の印鑑による印影（捺印）がある

↓ 経験則による推定（一段目の推定）

本人の意思に基づく押印であると推定される

↓ 民訴228条4項による推定（二段目の推定）

当該文書全体が本人の意思に基づいて作成されたこと（文書の成立の真正）が推定される

⇒ 文書の成立の真正が認められると、判例上、契約書については、特段の事情のない限り、記載されている法律行為の存在が認定される。

# 3条（文書の真正の推定）に関する三省見解

## ■ 「電子署名法3条に関するQ&A」（2020年9月4日）

事業者型のサービスが3条の固有性の要件を満たすためには、

- ①利用者の確認プロセス（2要素認証など）
- ②事業者内部のプロセス（暗号の強度や利用者毎の個別性を担保する仕組み（例えばシステム処理が当該利用者に紐付いて適切に行われること）を備えるなど）

において十分な水準の固有性を満たしていると言える必要。

⇒ ①②を満たせば、事業者型でも3条の推定が認められるとの見解



# キーポイント

- あくまでも行政府の見解にすぎない。  
裁判所が判断したわけではない。
- ハンコが撤廃される？  
選択肢が増えるだけ

# 電子署名 (EU)

- 電子署名に関する指令 [eSignature Directive 1999/93/EC]

“A Digital Agenda for Europe” (2010) : Digital Single Market構想



- **eIDAS規則** [Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market] (2016年7月1日施行)

electronic **I**dentification, Authentication and trust **S**ervices

# eIDAS規則の目的

- 個人や企業が国内で使用している電子ID（eID）スキームを使用して、eIDを使用している他のEU諸国の公的サービスにアクセスできるようにする。
- トラストサービス（電子署名、電子シール、電子タイムスタンプ、電子デリバリ、ウェブサイト認証）が、従来のペーパーベースのプロセスと同等の法的効果を有し、国内外で機能するようにして、当該サービスのための域内市場を創出する。

# 「トラストサービス」とは

- eIDAS規則に規定される電子署名、電子シール、電子タイムスタンプ、電子デリバリサービス、ウェブサイト認証にかかるサービスであって、電子取引の法的有効性を高めるものをいう。

（欧州委員会のdigital single marketのサイト：

[https://ec.europa.eu/digital-single-market/en/glossary#letter\\_t](https://ec.europa.eu/digital-single-market/en/glossary#letter_t)）

# eIDAS規則の内容

## ■ Chapters

1. 一般規定 [General Provisions] (1-5条)
2. 電子本人確認 [Electronic Identification] (6-12条)
3. トラストサービス [Trust Services] (13-45条)
4. 電子文書 [Electronic Documents] (46条)
5. 権限委任及び実施規定 [Delegations of Power and Implementing Provisions] (47-48条)
6. 最終規定 [Final Provisions] (49-52条)

# eIDAS規則の内容

## ■ Chapter 3の内容（Sections）

1. 一般規定 [General provisions]
2. 監督 [Supervision]
3. 認定トラストサービス [Qualified trust services]
4. 電子署名 [Electronic signatures]
5. 電子シール [Electronic seals]
6. 電子タイムスタンプ [Electronic time stamps]
7. 電子書留送付サービス [Electronic registered delivery services]
8. ウェブサイト認証 [Website authentication]

# 各用語の定義

## ■ 電子署名

電子形式の他のデータに添付または論理的に関連付けられる電子形式データであって、署名者が署名するために使用するもの。

## ■ eシール

電子形式のデータであって、電子形式の他のデータに添付または論理的に関連付けられて、後者の送信元と完全性を保証するもの。

## ■ 電子タイムスタンプ

電子形式の他のデータを特定の時間に結びつける電子形式のデータであって、後者のデータがその時点で存在したという証拠を確立するデータ。

# 日本の法制との比較

サービスの内容	eIDAS	日本	
電子署名	電子署名（SES）：25条 高度電子署名（AES）：26条 適格電子署名（QES）：28条、別紙I	電子署名法	署名（民事訴訟法228条）
電子シール	電子シール：35条 高度電子シール：36条 適格電子シール：38条、別紙III	（電子委任状法と電子署名法）	代理人形式
電子タイムスタンプ	電子タイムスタンプ：41条 適格電子タイムスタンプ：42条	（公証人による電子認証（公証人法1条4号））	確定日付（民法施行法5条）
電子書留送付	電子書留送付：43条 適格電子書留送付：44条		
ウェブサイト認証	適格ウェブサイト認証：45条、別紙IV		



## 4. 電子証拠の越境アクセス

# 電子証拠の越境アクセスの必要性

## ■ 必要性

- サイバー犯罪の増加
- 通常犯罪でも電子証拠が増加

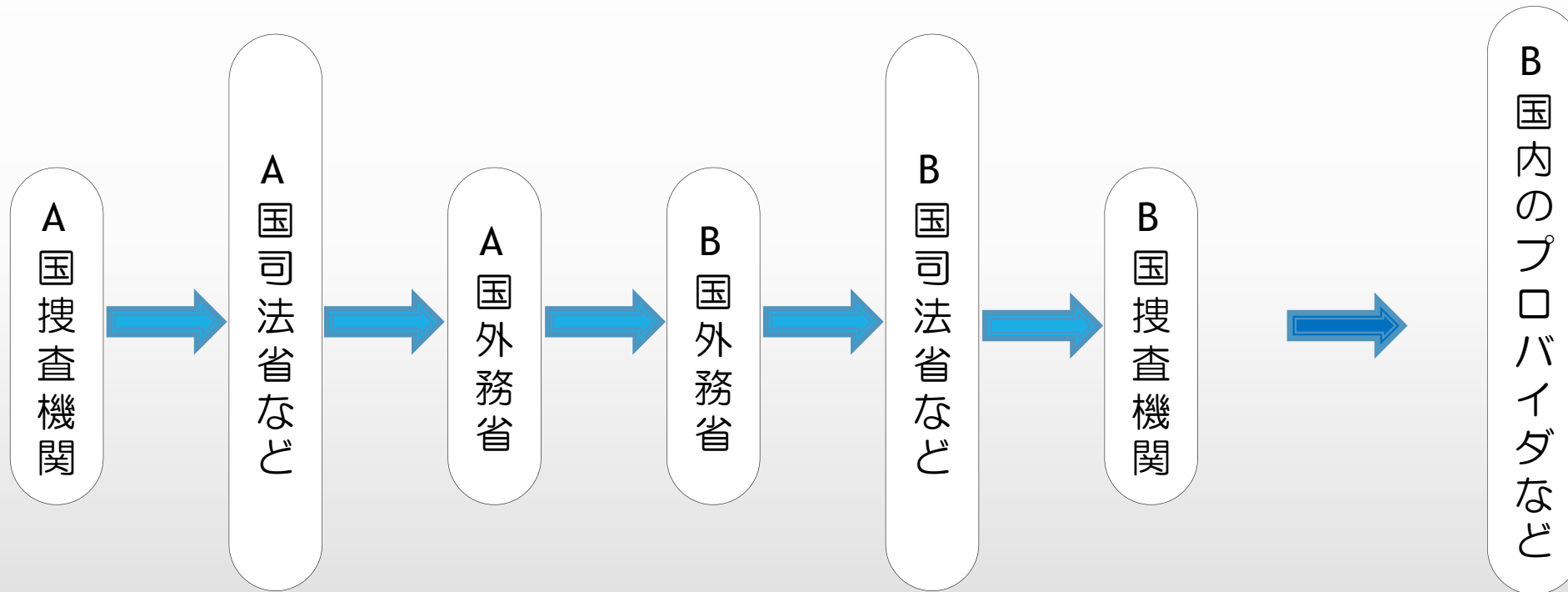
⇒ 捜査機関は海外サーバに蔵置されているデータにアクセスしたい

## ■ 現在存在する方法

- 刑事共助条約（MLAT）
- インターポール（EU内ではユーロポール）
- 法執行機関間の非公式の協力
- 24/7 point of contact networks（サイバー犯罪条約35条）

# 現状

## ■ 刑事共助条約（MLAT）による方法

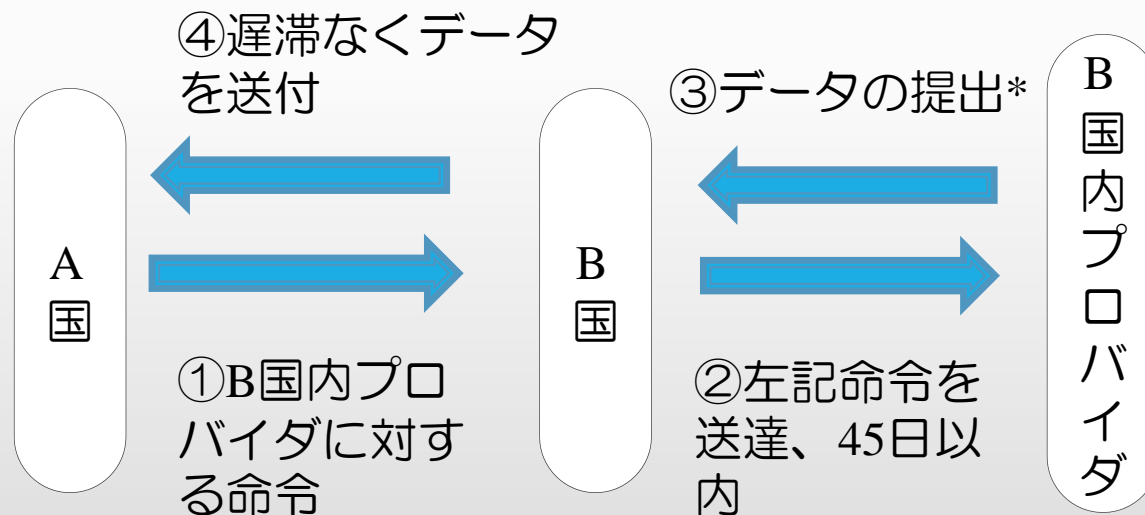


※平均10か月かかると言われている

# 国際条約による解決

## ■ サイバー犯罪条約第2追加議定書案（交渉中）

- 5.1条（仮）
- 相手国に対するデータ提出の方法



\* ユーザ情報（subscriber info）の場合は20日以内、トラフィックデータの場合は45日以内

# 国内法・域内法による解決

## ■ 米国CLOUD法とEUのe-evidence regulation（案）

国家 → 国家



国家 → プロバイダ

# E-evidence 規則（案）

## ■ E-evidence Regulation（案）

- 加盟国の司法機関は、直接、他の加盟国に所在するサービスプロバイダー又はその代理人に対し、一定の電子証拠（eメール、テキストメッセージ、識別情報等）を提出することを求める命令（European Production Order）を発付できる。プロバイダは、10日以内に応答する必要。
- 加盟国の司法機関は、直接、他の加盟国に所在するサービスプロバイダー又はその代理人に対し、一定のデータを保全することを求める命令（European Preservation Order）を発付できる。
- 個人情報保護など権利の保護措置

# CLOUD Act 制定の背景

## ■ Clarifying Lawful Overseas Use of Data Act of 2018

- 2018年3月成立
- Stored Communications Act of 1986（SCA、通信保存法）を改正
- 通信保存法 [18 U.S.C. § 2701-2713]  
第三者であるプロバイダー等の保有する “stored wire and electronic communications and transactional records” の任意/強制提出を定める
- CLOUD法制定の背景
  - SCAに基づく令状では、国外適用との関係で、海外のリモートサーバーにある情報を捕捉できない可能性がある（刑事共助条約（MLAT）を締結する必要）
  - Microsoft Corp. vs. United States, 829 F.3d 197 (2016)

# CLOUD Act

## ■ 主な内容

- ① プロバイダーに対する保有データの強制提出命令の発付・執行について、域外適用を認めた
- ② 外国政府との行政協定により、外国政府が外国国民について米国を拠点とするプロバイダーに対し令状を発付できることとした

- ## ■ ホワイトペーパー「[Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act](#)」（2019年4月）参照。



# 18 U.S.C. § 2713

## Required preservation and disclosure of communications and records

### ■ CLOUD法による改正

“A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider’s possession, custody, or control, regardless of whether such communication, record, or other information is located [within or outside of the United States](#).”

→令状による域外データの強制取得を明示的に認めた



当局

開示命令（令状）



データ

国外

プロバイダー

# ホワイトペーパーのQ&A

- 米国の管轄はどこまで及ぶのか？
  - 米国会社、米国に本社を有する会社、米国民の所有する会社に限られない。
  - 米国にサービスを提供していることによって管轄が生じるか否かは事実認定の問題。
  - 米国の管轄権の行使が根本的に公正であると認められる程度に十分な接触（sufficient contacts）を有しているかで判断。
  - 米国会社の外国所在の子会社の場合も同様のテストにかかる。米国会社が子会社を通じてデータを保持していると言えれば、令状が執行される可能性もある。

# 事業者が注意すべき事項

## ■ CLOUD法が適用されるか（管轄）

- 米国との関連性の程度、「十分な接触」があるか
  - 米国向けにサービスを提供、売上の程度、ユーザーの大半が米国民,etc.
  - 米国会社の子会社

## ■ 管轄が及ぶ可能性がある場合

- データを蔵置している国のデータ保護法において米国へのデータ移転が認められるかを検討しておく。
- 認められない可能性がある場合（特にGDPR）、米国における異議申立ての手續に精通しておく（14日以内に申立てを行う必要）。

## ■ 実際に命令の執行を受けた場合

- データが蔵置されている国の個人情報保護委員会に相談。

ご清聴ありがとうございました。

ご質問・ご意見等ございましたら  
以下までご連絡ください。

弁護士 有本真由  
アレシア国際法律事務所  
電話：03-6459-3502  
E-mail: [arimotomayu@gmail.com](mailto:arimotomayu@gmail.com)  
URL: <https://www.alesia-law.com>