

* グローバルでIDマネジメントを行う際の考慮点 ~EU指令への対応~

日本電信電話株式会社
内部統制室 ITガバナンス担当
駒沢 健

*自己紹介

➤ 私はだれ

- ✓ 氏名：駒沢 健(こまざわ けん)
- ✓ 会社：日本電信電話株式会社
- ✓ 仕事：IT戦略の立案と推進を中心に従事

➤ ID管理WG参加の経緯

- ✓ とある企業へのID管理提案したが、全然まとまらない。専門家集団の門をたたくことに
- ✓ JNSA ID管理-WG 7年生

*突然質問 何の一覧??

企業名

- * 積水ハウス株式会社
- * アサヒグループホールディングス株式会社
- * 東レ株式会社
- * 株式会社エフピコ
- * 株式会社ブリヂストン

業種

- 建設業
- 食料品
- 繊維製品
- 化学
- ゴム製品

2016年度攻めのIT経営銘柄

経済産業省

トヨタ・フォード株式会社

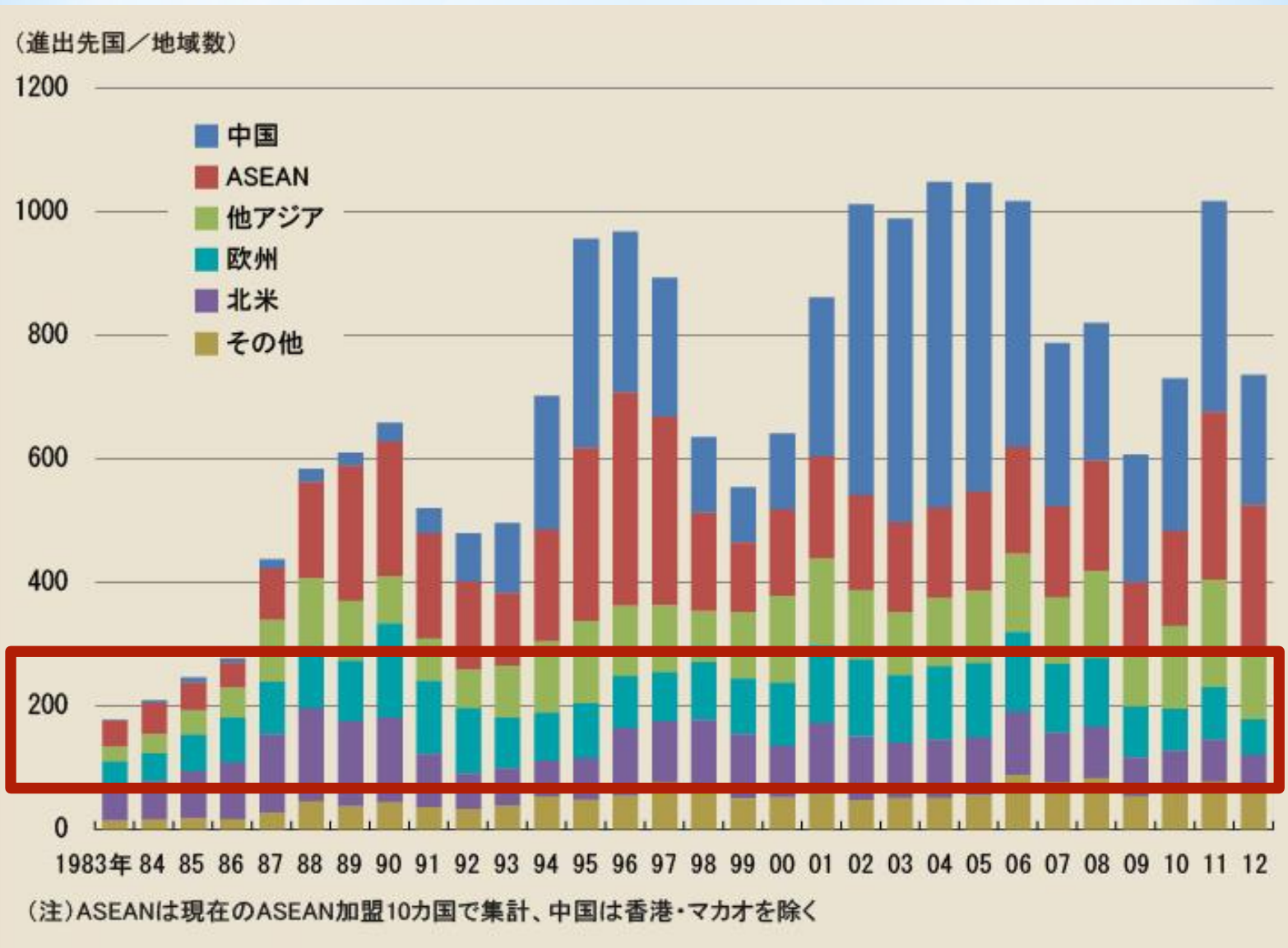
- * 大阪ガス株式会社
- * 東日本旅客鉄道株式会社
- * 株式会社アルファポリス
- * 三井物産株式会社
- * 株式会社三井住友フィナンシャルグループ
- * 東京海上ホールディングス株式会社
- * 東京センチュリーリース株式会社

その他製品

- 電気・ガス業
- 陸運業
- 情報・通信業
- 卸売業
- 銀行業
- 保険業
- その他金融業



日経企業のグローバル進出状況



* グローバル化に伴う経営者の課題感

2015 年の最重要リスク

- | | |
|----|---|
| 1 | 法規制や規制当局の 監視 強化 |
| 2 | マーケットの状況（例えば、不安定なエネルギー価格、国際情勢など） |
| 3 | サイバー攻撃／情報セキュリティ・ リスク への対応不十分 |
| 4 | 後継者選定の課題／才能ある人材の獲得やつなぎとめ |
| 5 | 組織の文化が、重要なリスクの適時の認識及び報告を助長していない可能性 |
| 6 | 変革に対する社内の抵抗がビジネスモデルと中核事業に対する必要な調整を阻害する可能性 |
| 7 | 想定外の危機（例えば、レピュテーション・ リスク ） |
| 8 | 顧客ロイヤリティの維持が困難になっている可能性 |
| 9 | 競合他社との競争 |
| 10 | 新たなテクノロジーによりビジネスモデルが破壊的な影響を受ける可能性 |

*たかだか、EUの人員管理

*されど、当局とか言われるとどうすりゃいいの

*本日は、そんなめんどくさいEU指令を踏まえたアイデンティティ管理のお話しです。

*EU指令にどう向き合うか

I. EU指令って？

II. 何がだめなの？

III. 対策を講じている国ってどこ？日本は大丈夫？

IV. 誰が判断するものなの？

V. 何をしないといけないの？

VI. 選択肢があるらしいけど、どれ選ぶのがいいの？

*EU指令って？

- *欧州連合（EU）が誕生したのは、1993年
- *それぞれの加盟国には、個人情報保護（プライバシー保護）について、独自の法律がある。
- *加盟国間の違いを埋めるために、EUは1995年（平成7年）10月24日、『個人データの取扱いに係る個人の保護及び当該データの自由な移動に関する欧州議会及び理事会の指令』を採択しました。

*何がダメなの？

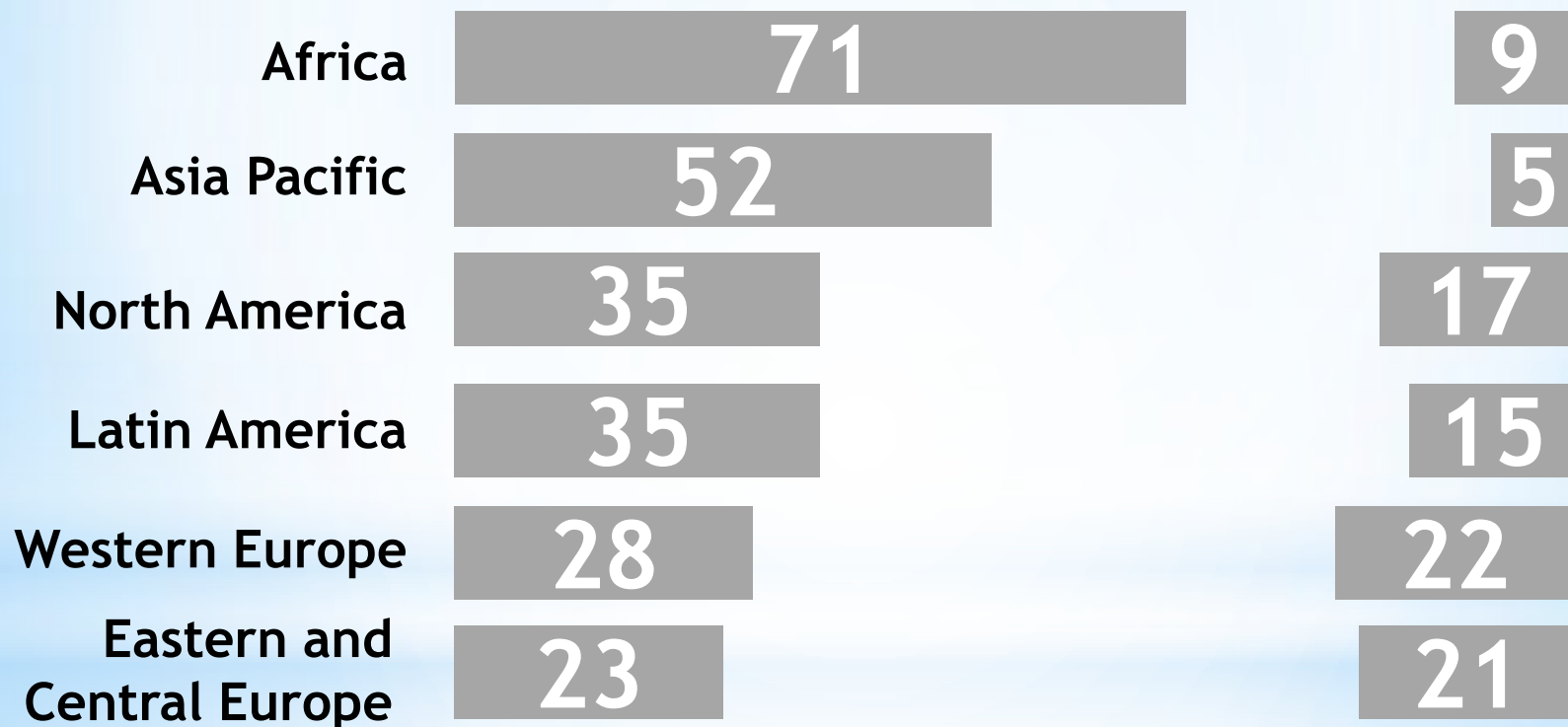
*対策を講じている国および、個別に対策を取らない限り、個人情報の移転が禁止されている



* グローバル化に対する世論(全世界)

Good

Bad



「グローバリゼーションは自国にとって良いことか」という問いに対する回答%
Gallup International (2006)

* 移転とは？

* 非常に重要な話

* IT目線で表現すると

* EUからデータを持ち出して、EU圏外のサーバに蓄積すること。

* EU圏外からアクセスすること。

* 結構キビシイ

* 対策を講じている国は？



2012年10月現在

ニュージーランドおよびモナコについては「十分なレベルの保護措置を行っている」と認定済み(欧州委員会の決定待ち)

* アメリカのセーフハーバーは大丈夫か？



アメリカ
(セーフハーバー)

欧州司法裁判所によるセーフハーバー協定無効判決について

2015年10月6日、欧州司法裁判所は欧州委員会が米国と締結しているセーフハーバー協定は無効であるとの判決を下した。本判決は、欧州内で事業を展開している米国企業のビジネスにも大きな影響を及ぼすと見られている。今回の問題は、2013年のスノーデン事件によりNSA等の米国政府機関がFacebook Inc等のIT企業が保有するデータを監視していたことが発覚したことにより、オーストリア市民でFacebookのユーザーでもあるMax Schrems氏が、Facebookが十分な保護措置がなされていない米国に対して自身の個人データが転送されたとして、アイルランドのデータ保護機関に対して申立を行ったという事案である。

Microsoft、ドイツに新データセンター開設へ セーフハーバー問題対策か

欧州連合が米連邦政府とのセーフハーバールールの無効化を検討していることの対策

Microsoftは11月11日（現地時間）、独ベルリンにおいて、クラウドサービス提供のためのデータセンターをドイツ国内の2カ所に開設する計画を発表した。来年下半年に稼働を開始する計画。これらのデータセンター

では、Microsoft Azure、Office 365、Dynamics CRM Onlineなどのサービスを提供し、ユーザーデータを保持する。同社のサティヤ・ナデラCEOは発表文で「こ

*誰が判断するものなの？

一次法

EUの設立条約や改正条約にあたる基本条約

- ✓ EC条約（欧州共同体設立条約）
- ✓ ニース条約
- ✓ アムステルダム条約
- ✓ ローマ条約

二次法

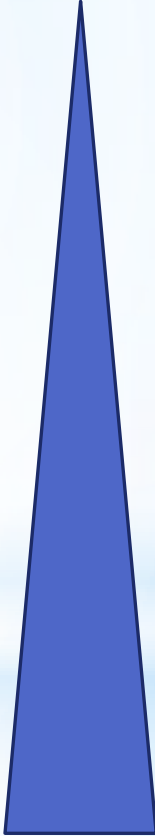
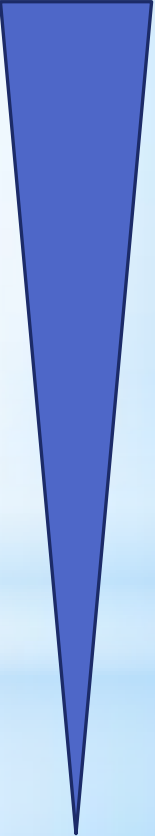
一次法（条約）を根拠に制定され、EU域内で直接・間接的に企業や個人を規制する法令

- 規則（Regulation）
- **指令（Directive）**
- 決定（Decision）
- 勧告（Recommendation）
- 意見（Opinion）

原則として、通常はEU加盟国へは直接適用されず、国内法への置換えが必要によって、各国間で法令が異なる場合もあります。
（全く同一にはならないという意味）

➡ つまり、最終的には各国当局が判断することになる

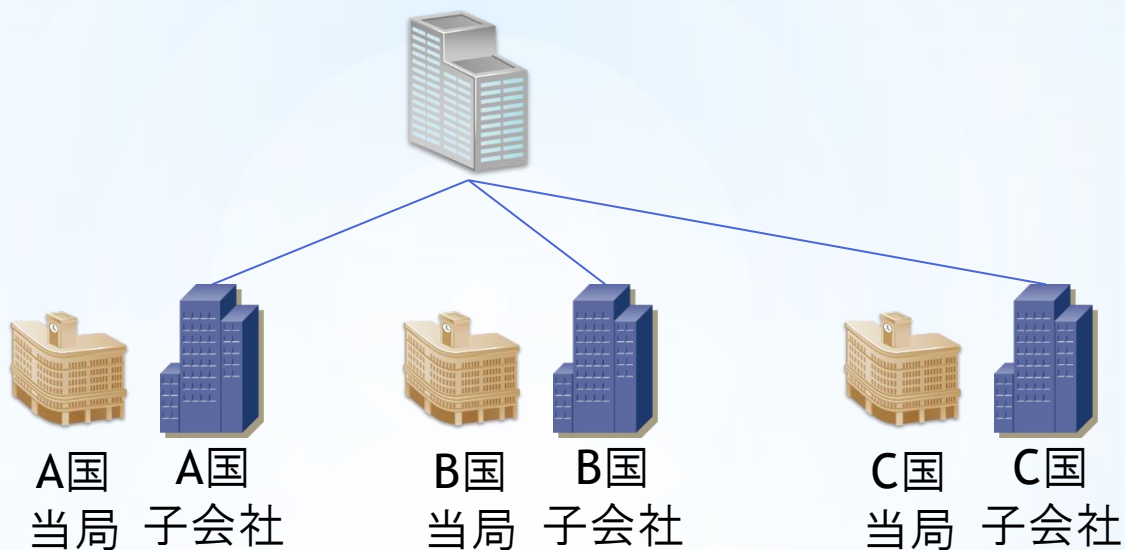
*何をしないといけないの？

方法	契約主体	内容	導入の負荷	範囲拡大時の 運用負荷
明確な同意 の取得	従業員個人 と企業	従業員個人から明確 な同意取得		
Standard Contractual Clauses (SCC)	現地法人 と本社	法人間でデータ移転契 約を締結※ (国によっては個別対 応要)		
Binding Corporate Rules (BCR)	グループ企業 包括	グループ内全法人を対 象として拘束力を有 する内部規定を策定 し、各国データ保護当 局の承認を得る		

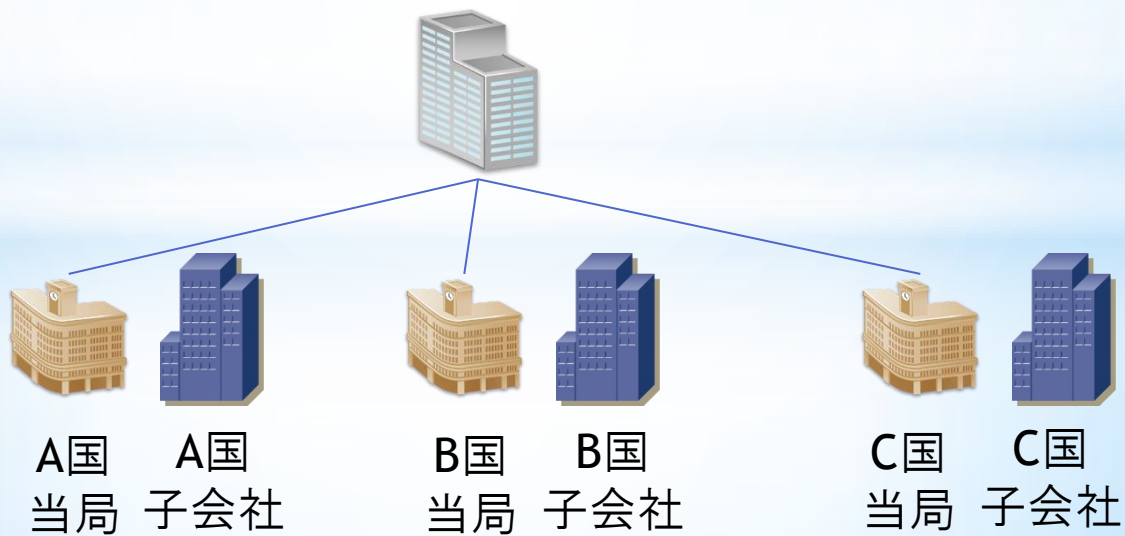
※Data Protection Authority(DPA)への申請・承認が必要

* SCCとBCRの大きな違い

Standard Contractual Clauses (SCC)



Binding Corporate Rules (BCR)



*ぶつちやけどれを選択するの？

- ✓ BCRは非常に期間と費用がかかり、実際に採用している企業は数少ない。
- ✓ SCCが現実的だが、準備に半年～2年かかる。また1千万程度の準備コストも必要
- ✓ 個人同意は小規模なら . . .

*おわりに

- ✓ 今後EU指令は、規則（Regulation）に変更する可能性がある
- ✓ 米国のセーフハーバー協定も無効になる可能性がある
- ✓ EU指令自体の動向を確認しつつ、余裕をもった準備期間が必要

*ご清聴ありがとうございました