電子署名・PKI利活用のメカニズム

2017年5月22日

政本　廣志
JNSA 電子署名WG
NTTアドバンステクノロジ

はじめに

電子署名・PKIのメカニズム

ではなく、

電子署名・PKI利活用のメカニズム

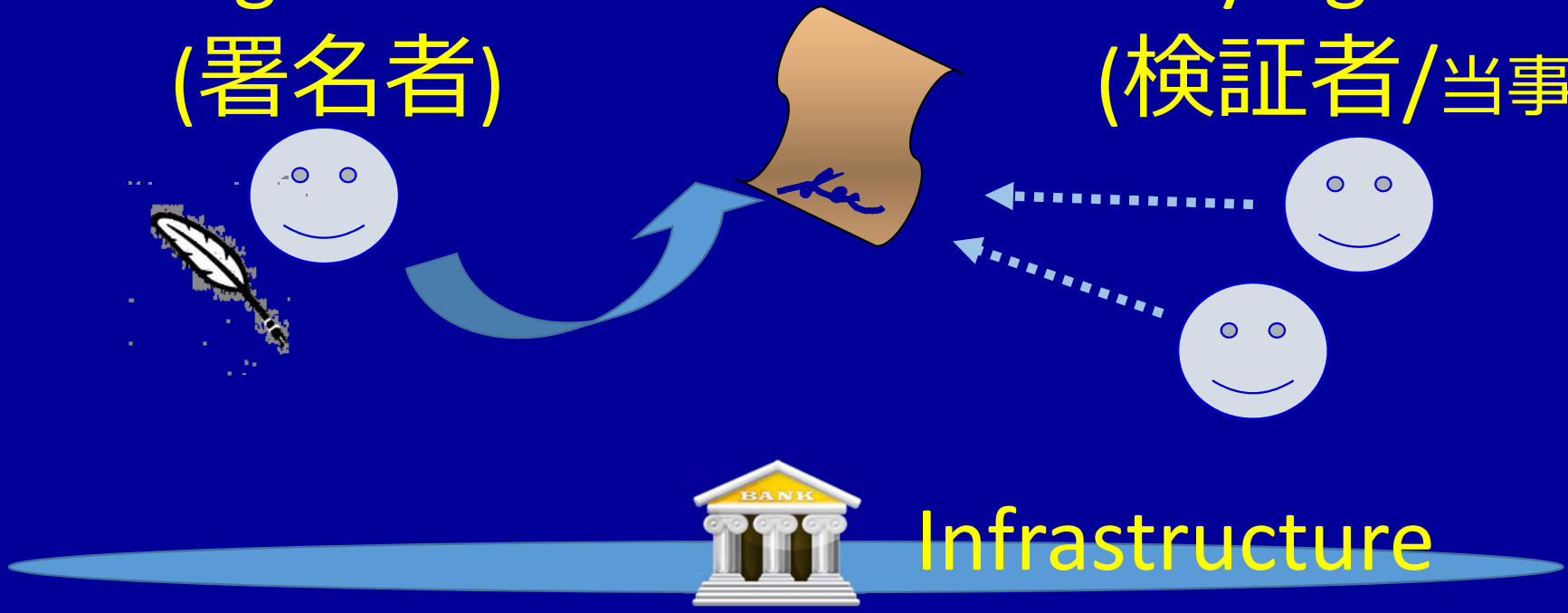
です

電子署名の仕組み

SignerとRelying PartiesとInfrastructure

Signer
(署名者)

Relying Parties
(検証者/当事者)



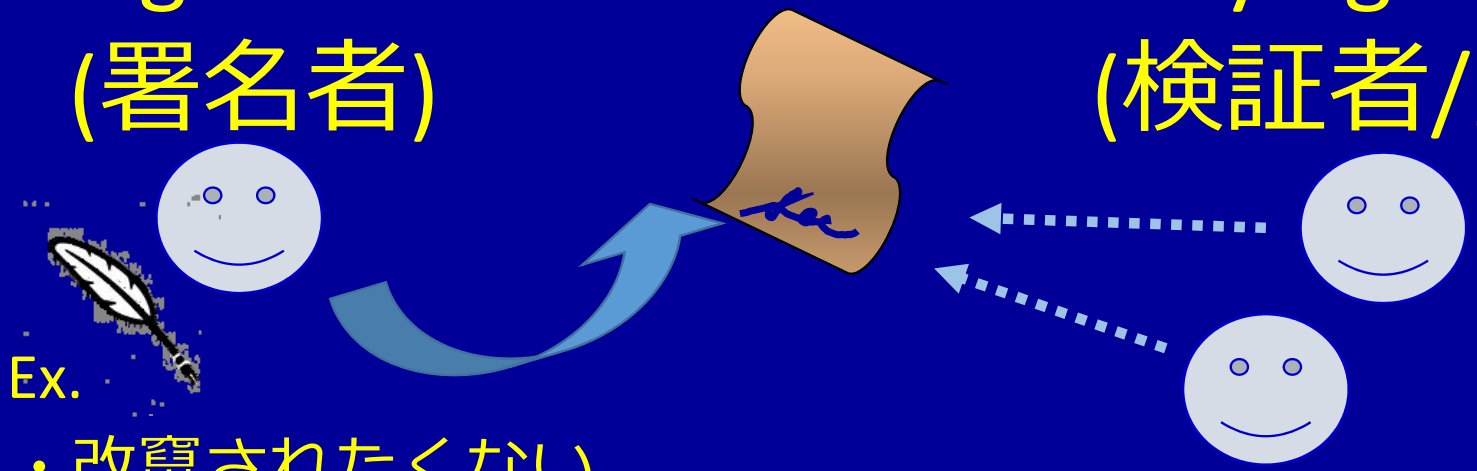
Infrastructure

【要因１】モチベーション（１）

Signerのモチベーション

Signer
(署名者)

Relying Parties
(検証者/当事者)



Ex.

・改竄されたくない
・自分のものと証明したい
・相手に信用してもらいたい

【要因１】モチベーション（２）

Relying Partyのモチベーション

Signer
(署名者)

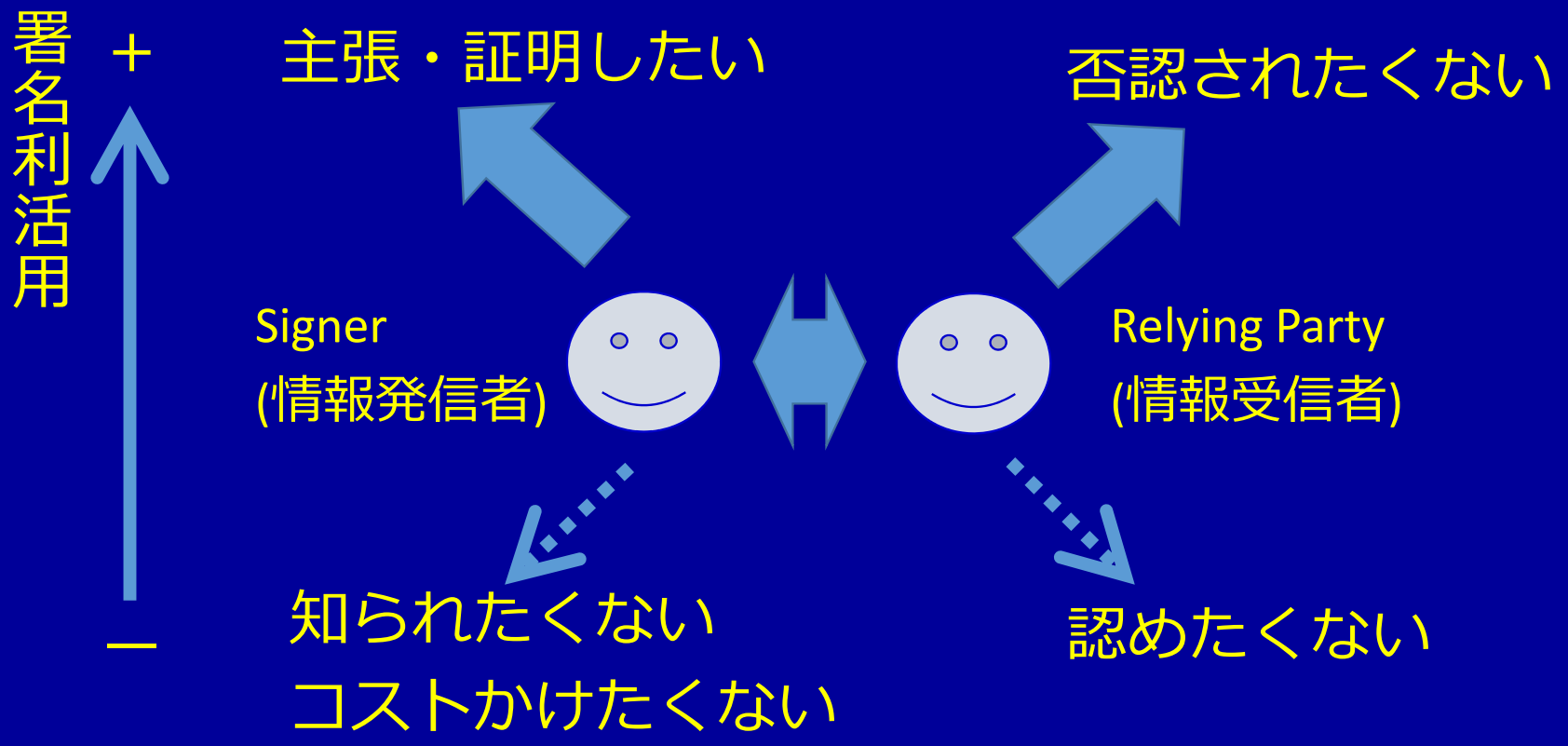
Relying Party
(検証者/当事者)

Ex.

- 本物か確認したい
- 誰のものか確認したい
- 否認防止の担保を取りたい

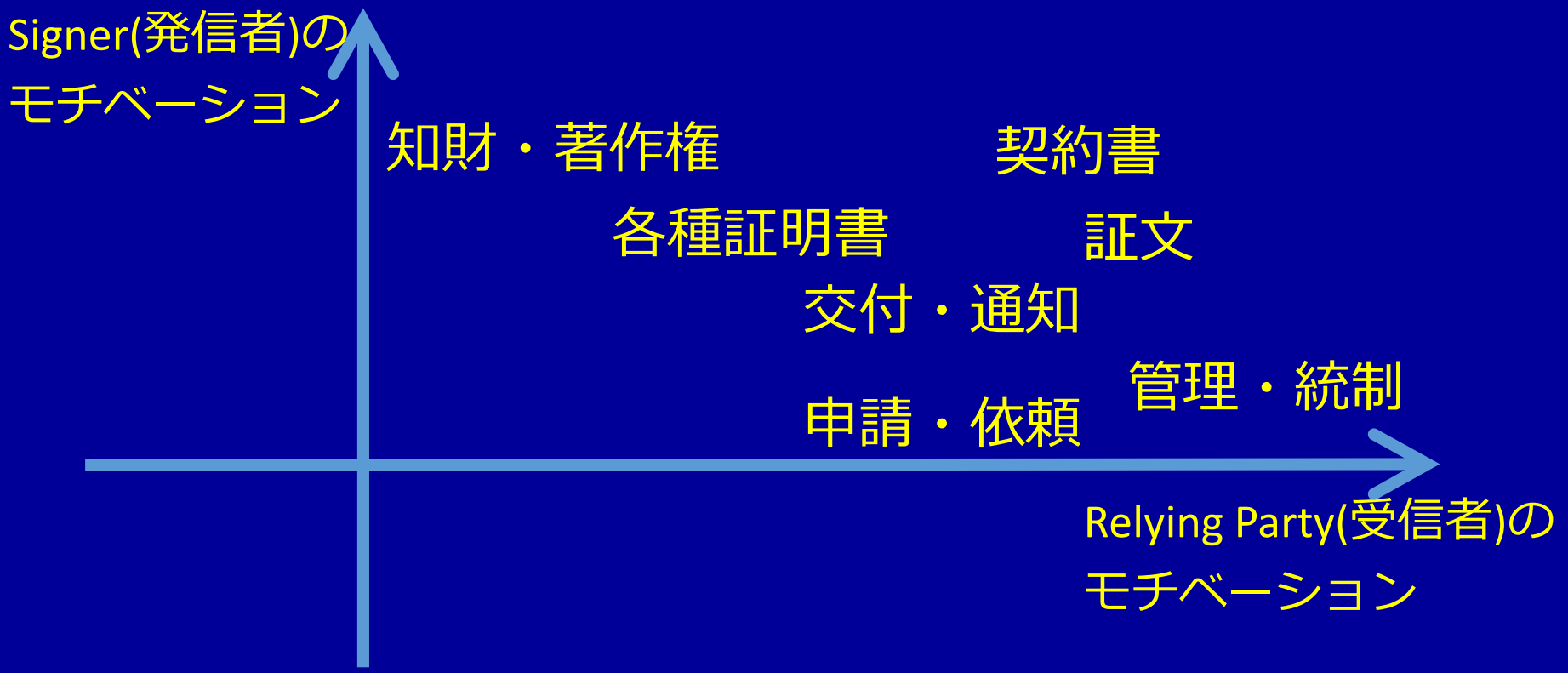
【要因１】モチベーション（３）

モチベーションの力学



【要因１】モチベーション（４）

モチベーションと用途の例



【要因２】強制力と代替性

- 規制型の用途における電子署名のニーズ：

利活用の意欲　≦　コスト重視

↑

法制度による強制力、代替手段の有無が大きく影響

【要因３】基盤(インフラ)の導入推進

- ここでの基盤：署名者を認証する組織、登録局RA
- 認証組織(コミュニティ)の大きさはさまざま
  - 国、業界、会社、資格認定組織、etc.
  - 広い範囲：PKI方式のメリットが生きる ／ 強制力が働きにくい
  - 狭い範囲：強制力が効きやすい ／ 署名が必要でないこともある

⇒ コミュニティの導入への取り組みに依存

【要因３】企業内における利用ニーズ例

- 社員証
- 社員DBに基づく発行
- サービス例
  - 出退勤管理（タイムカード、入退出カード）
  - 端末認証
  - 無線アクセス、リモートアクセス
  - 社員食堂、売店、図書館等施設利用
  - 社内システムアクセス
  - 決裁システム
  - 文責・著作者表示（署名）
  - 電子メール（署名メール）

【要因４】その他の環境要因

- 要因例：
  - 道具(ツール)の品揃え、使いやすさ
  - 利用シーンの多さ
  - 利用者数
  - 認知度

  etc.

まとめ

仮説：
署名利活用の推進力*P*は、

$$P = \Sigma \left(M_{Sig} \cdot E + M_{RP} \right) \times F \times C$$

M：モチベーションの高さ
E：コミュニティの取組み
F：強制力の強さ
C：環境要因