

# InternetWeek2021 C24 思ったより側にある国際標準

振り返ったら側にあった標準化(電子署名関連)

2021年11月25日

セコム株式会社 IS研究所

コミュニケーションプラットフォームディビジョン

暗号・認証基盤グループ 主任研究員

佐藤雅史

# 自己紹介



## 佐藤 雅史

- 情報セキュリティ、暗号を応用した電子認証や電子署名、ブロックチェーンなどが専門
- 日本ネットワークセキュリティ協会、日本トラストサービスフォーラムなど、様々な業界団体に活動
- ISO/TC 154 (Processes, data elements and documents in commerce, industry and administration) WG6
- ISO/TC 307 (Blockchain and distributed ledger technologies), 国内審議委員会, JWG4国内主査

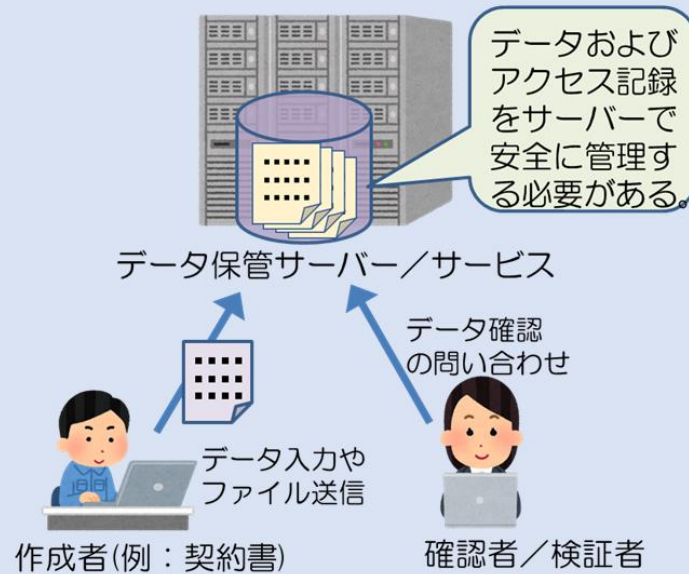
# 本日午前の部で…

「C19 電子契約, 公開鍵基盤(PKI), 証明書, リーガルテックの基盤技術」より

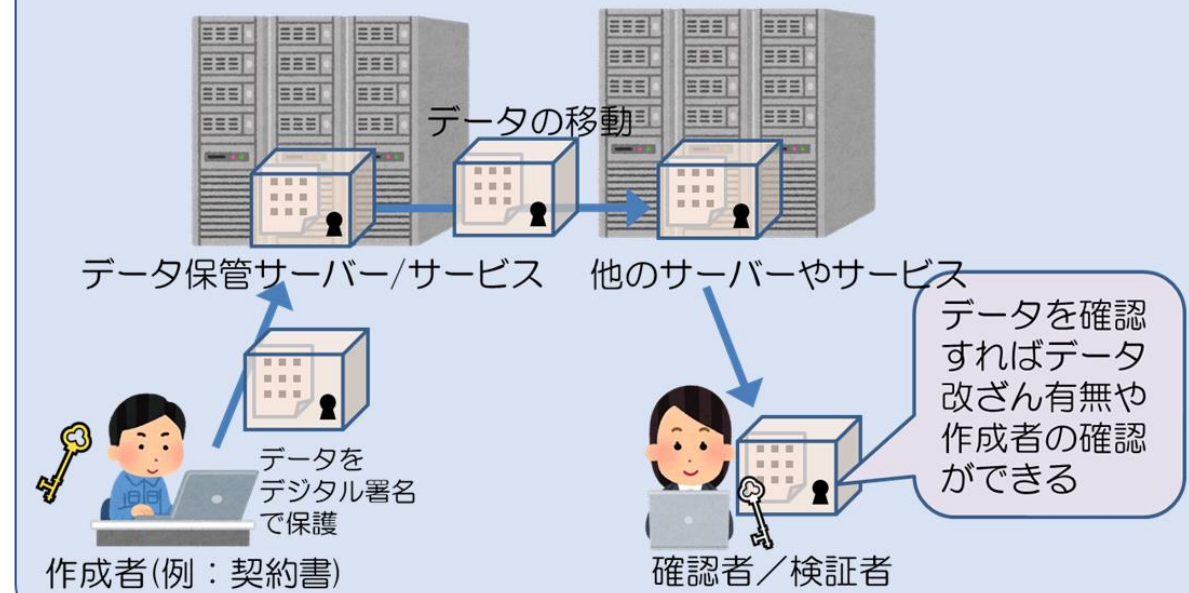
## なぜデジタル署名を使おうとするの？

署名者本人に対して発行された証明書+デジタル署名付きデータにより、そのデータ自身で本人の電子署名(意思)であることを確認できるようにする。

### サーバー保管/記録のケース



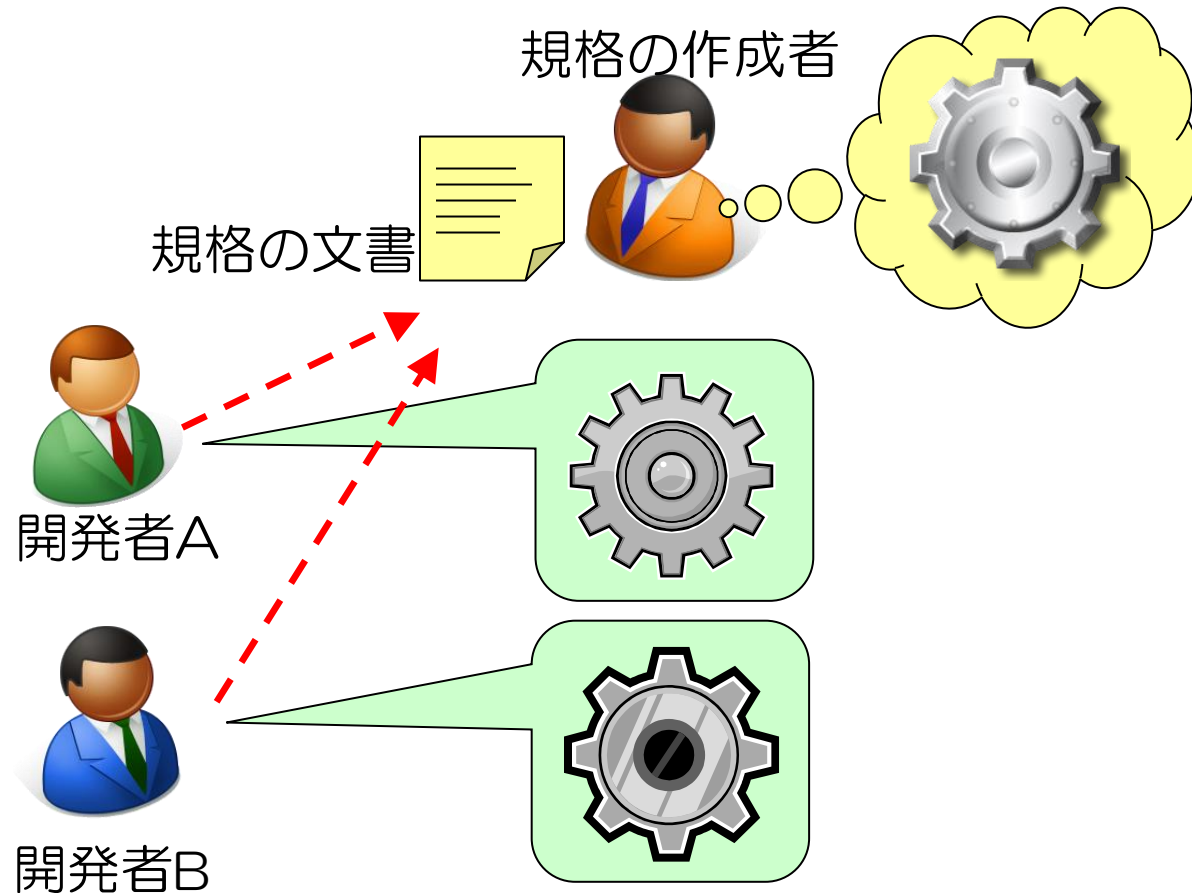
### デジタル署名のケース



(第三者)検証可能性、相互運用性、移行可能性でメリットがある

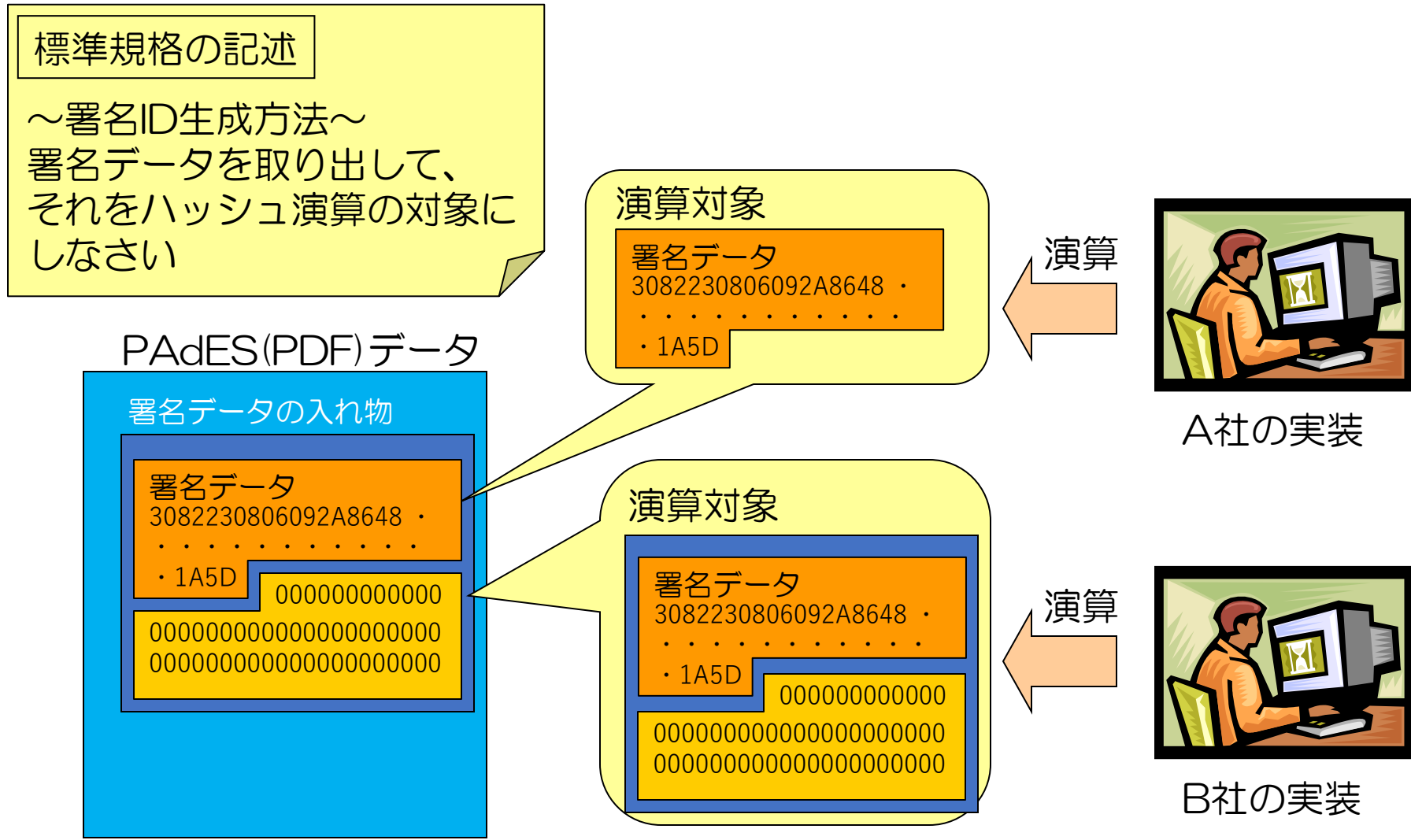
# 相互運用性 (Interoperability) の問題

標準規格さえあれば皆が同じようにモノを作れる？  
(というわけでもない…)



# 実装が食い違う例

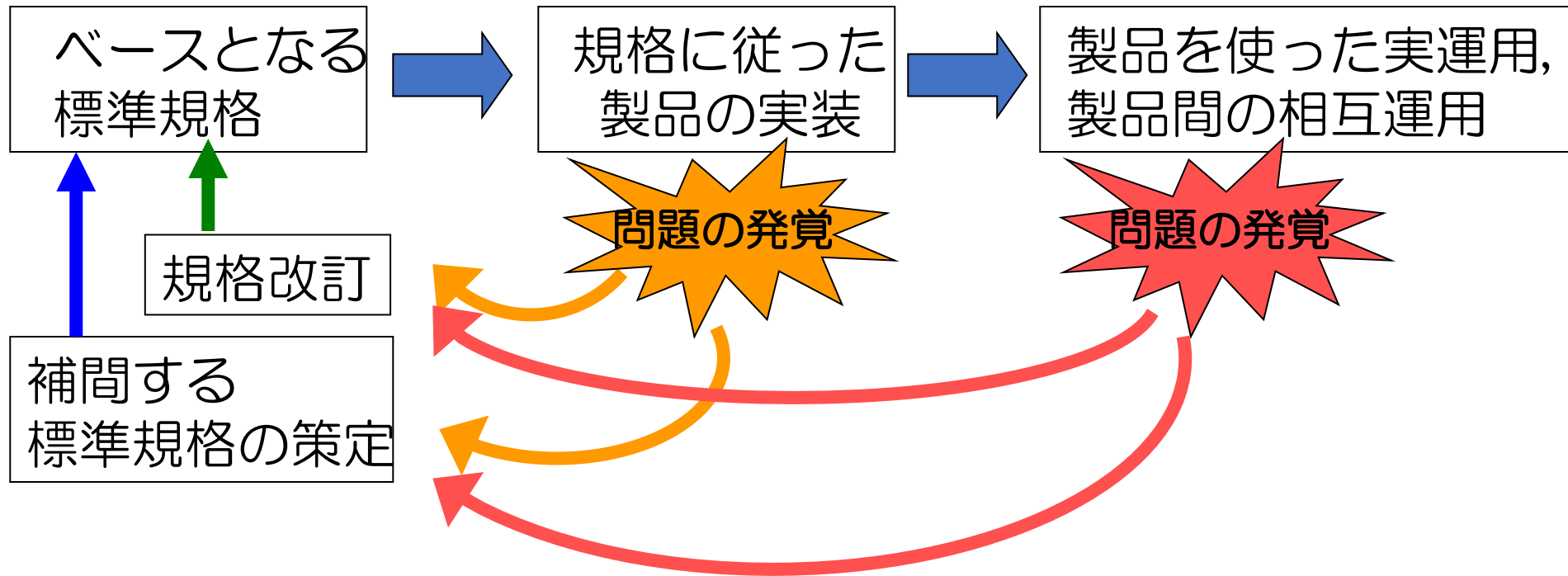
～同じ規格を読んでも同じ理解になるとは限らない～



# 相互運用性の問題が生じる要因いろいろ

- 標準規格の記述が曖昧、記述のミス
  - 標準規格の作成者は必ずしも開発経験者ではない・・・
  - 実装して相互運用してみても発覚する問題もある
- 選択可能な要素（オプション要素）
  - オプション要素を利用する製品、サポートしない製品
  - オプション要素をサポートしない場合の挙動
  - SHOULD(推奨)の扱い
- 開発者の独断、思い込み
  - 規格をよく読んでいない。参照規格を見ていない。

# 使える標準規格にするには…



実装と実運用で得られた知見をフィードバックすることが重要



# デジタル署名(電子署名用途)に関する 標準化の考え方

使える標準規格をめざそう！  
相互運用性の確保が重要課題！

- JNSA Challenge PKI Project (2001-2004頃)
- ECOM 電子署名プラグテスト (2005)
- 日欧 電子署名プラグテスト (2007)
- ETSI 電子署名プラグテスト (2008年～)

※ETSI (European Telecommunications Standards Institute)

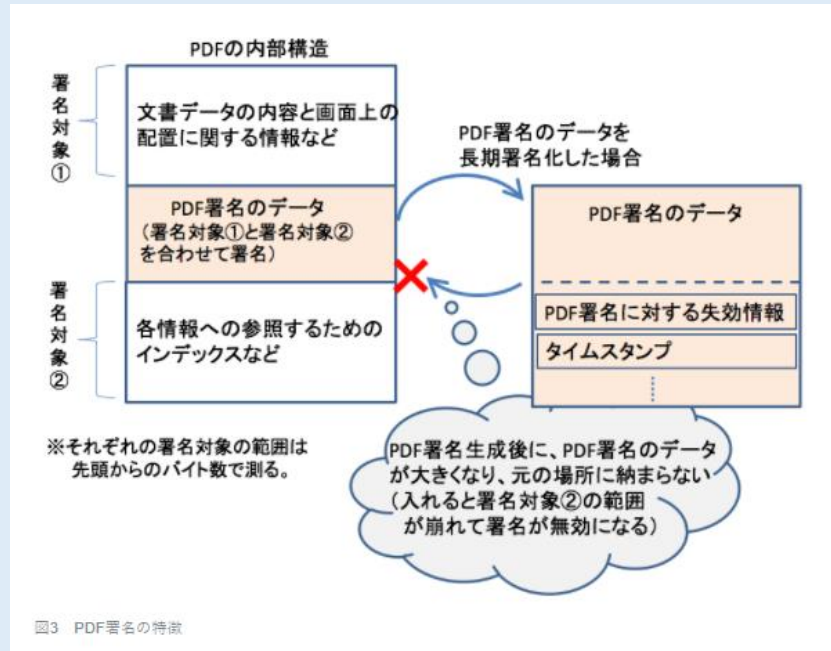


# デジタル署名(電子署名用途)の標準

署名フォーマット	ベース規格	長期署名プロファイル (長期保存用) ISO/JIS	業界別プロファイル
CAdES (ASN.1ベース)	EN 319 122 (CAdES digital signatures)	ISO 14533-1 JIS X 5092	【ヘルスケア】 ISO 17090-4
XAdES (XMLベース)	EN 319 132 (CAdES digital signatures)	ISO 14533-2 JIS X 5093	【ヘルスケア】 ISO 17090-4
PAdES (PDFベース)	EN 319 142 (PAdES digital Signatures) ISO 32000-2 (PDF 2.0)	ISO 14533-3	【ヘルスケア】 ISO 17090-4
JAdES (JSONベース)	ETSI TS 119 182 (JAdES digital signatures)	—	—

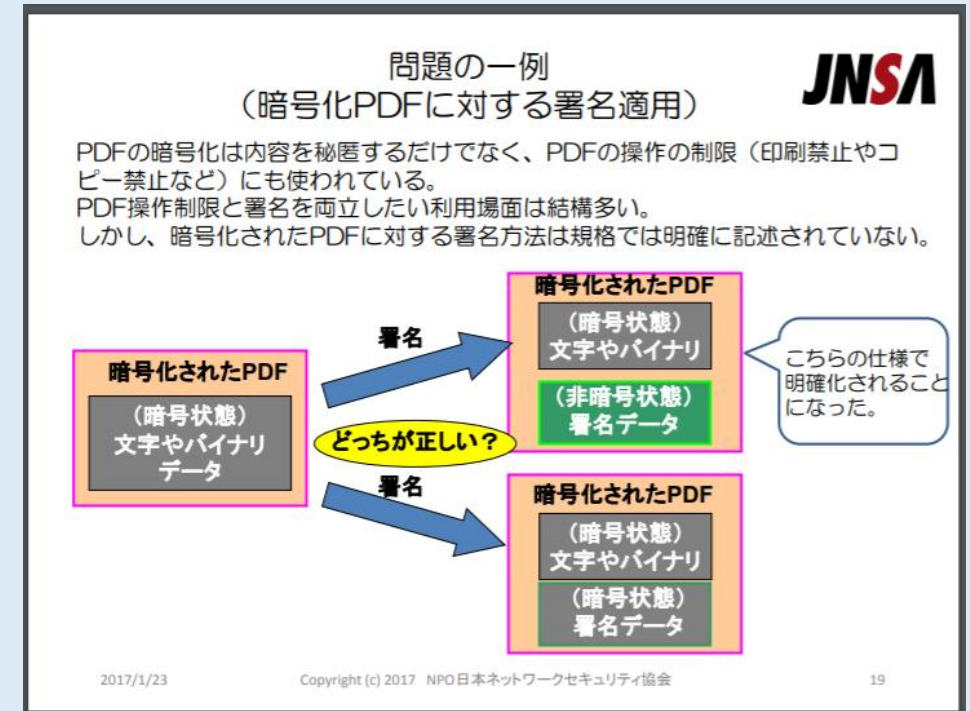
# 最初は問題提起から…

## ①PDF署名適用における課題共有から PAdES仕様の誕生のきっかけへ



情報処理学会 デジタルプラクティス Vol.9 No.3 (July 2018),  
特集号招待論文「デジタル社会のトラストを支える電子署名」より

## ②PAdES仕様での問題共有から PDF2.0議論への参画, プロファイル規格策定へ



JNSA Network Security Forum 2017  
「PDF長期署名プロファイルの国際標準化を振り返って」より

# きみが思うより側にある国際標準

まずは…

- 標準規格に覗いてみよう！触れてみよう！

何かに気付いたら？

- 聞いてみよう！相談してみよう！提案してみよう！（まずは関係のある日本の団体や専門家でもOK）

一歩踏み出すと…

- その道の第一人者達と良い出会いがあるかも！