第3回 タイムスタンプ認定制度に関する検討会

資料３－２

各論点について

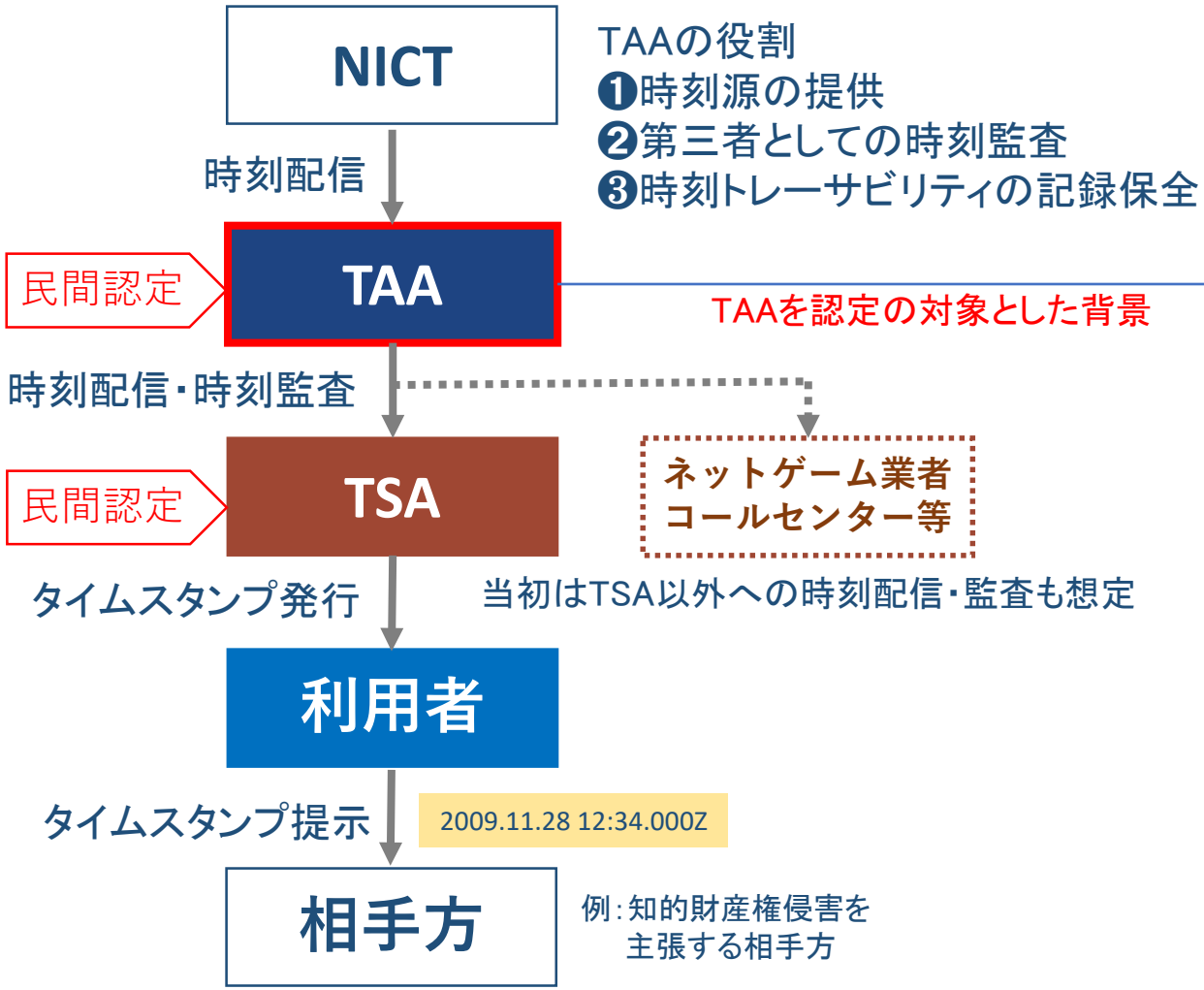
2020年5月29日

タイムビジネス認定センター長
伊地知　理

一般財団法人
日本データ通信協会

1．認定の対象　②TAAの扱い

検討の前提（タイムビジネスの仕組みと背景）



e文書法制定に向けて電子化のリスクを徹底排除

民間TSAがタイムスタンプ時刻の不正（バックデート）を強要されたとしても実施できない仕組みとしてTAAモデルに強い期待が寄せられた。

IT社会が進展し、時刻配信・監査サービスのニーズ拡大に期待

総務省「タイムビジネスの指針」にも示されている通り、ネットゲームや証券取引のコールセンターはじめ、様々な領域で時刻配信・監査が必要と考えられた。

1．認定の対象　②TAAの扱い

現状の課題（事業者ヒアリングに基づく）

- 時刻配信・監査サービス（TAA）を利用する社は、TSAのみ（現状6社）であり、TAAはビジネスとして成立し得ない状況
- 時刻配信・監査サービスを受けるTSAの機器は、それぞれのTAAに紐づいており、乗り換えが困難
  - 利用するTAAが業務廃止する場合など、TSAは別のTAAに乗り換えるための費用負担や移行作業が生じる
- TAAが25時間※停止した場合、時刻監査を受けるすべてのTSAのタイムスタンプサービスが停止

※ TAAによるTSAの時刻監査は数時間毎に行われる。監査結果が正常な場合、25時間有効な時刻監査証が発行され、TSAはその有効時間内のみタイムスタンプを発行することが出来る。時刻監査が25時間以上行われなかった場合や、監査結果が異常な場合、TSAのタイムスタンプ発行機能は直ちに停止される。

- 時刻配信・監査サービスの利用コストは、タイムスタンプサービス利用料に影響

1．認定の対象　②TAAの扱い

EUにおけるTSAの時刻の信頼性確保の要件

EUでは、TSA自らタイムスタンプの時刻の信頼性を確保する方式を採用している

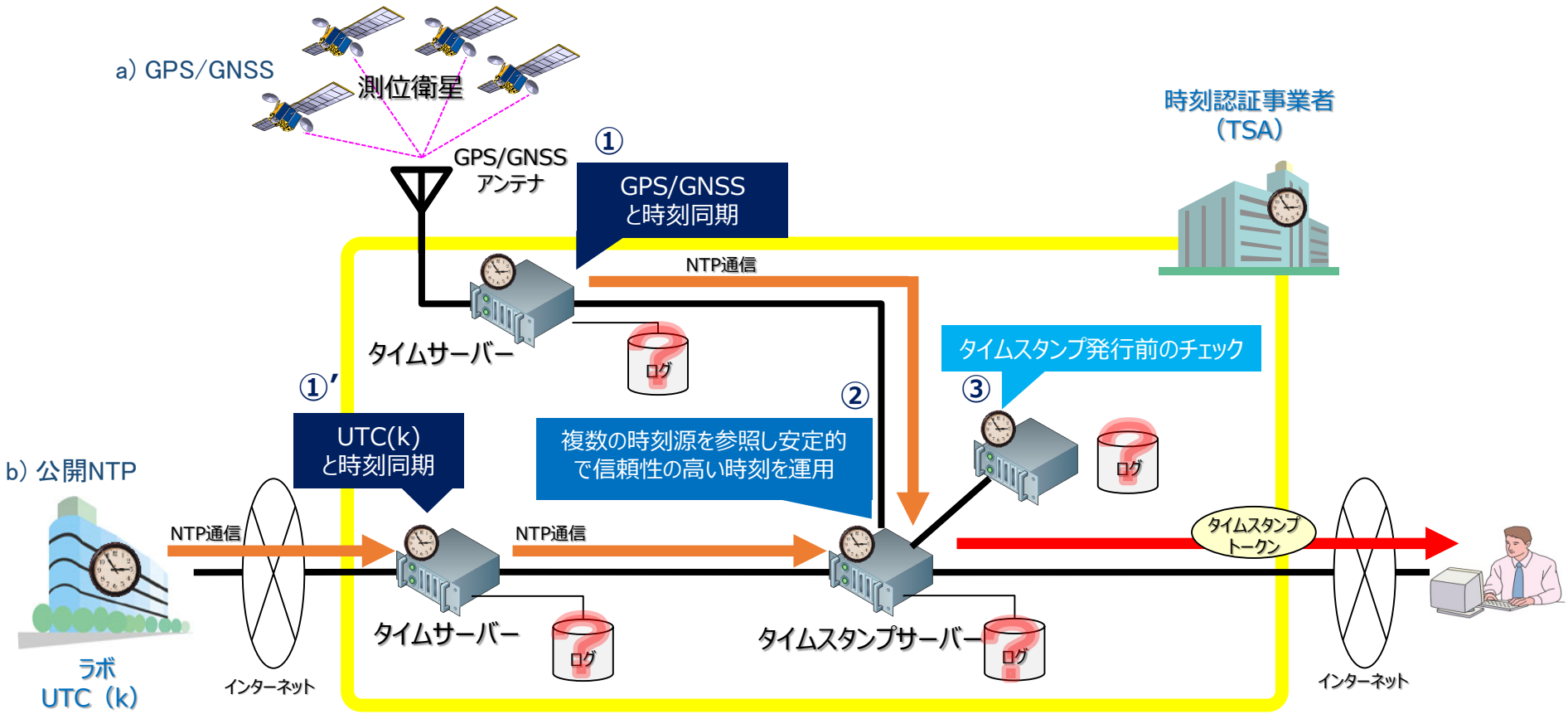
- 時刻のトレーサビリティ
  - タイムスタンプの時刻は、研究機関(k)によって運用される一つ以上のUTC※1(k)にトレーサビリティが確保されていなければならない。
- 時刻源と時刻同期精度
  - TSAは、以下を宣言しなければならない。
    ①トレーサビリティを確保する対象の時刻源UTC(k)
    ②時刻源との同期精度(±1秒以内)
- 時刻の較正と脅威からの保護
  - TSAは、宣言した時刻精度から外れないように時刻を維持しなければならない。
  - TSAは、権限のない人員による時刻の改ざんや妨害電波等の攻撃の脅威から時刻を保護しなければならない。
- 時刻精度を満たさないタイムスタンプの発行防止
  - TSAは、宣言した時刻精度から外れていることを検出した場合、タイムスタンプの発行を停止しなければならない。

※1 UTC(Coordinated Universal Time):協定世界時。情報通信研究機構(NICT)はじめ世界の80機関程度の原子時計を用いて決定される。

1．認定の対象　②TAAの扱い

EUにおけるTSAの時刻の信頼性確保イメージ

Qualified time stampを発行するTSA（9社）の運用規程の調査結果



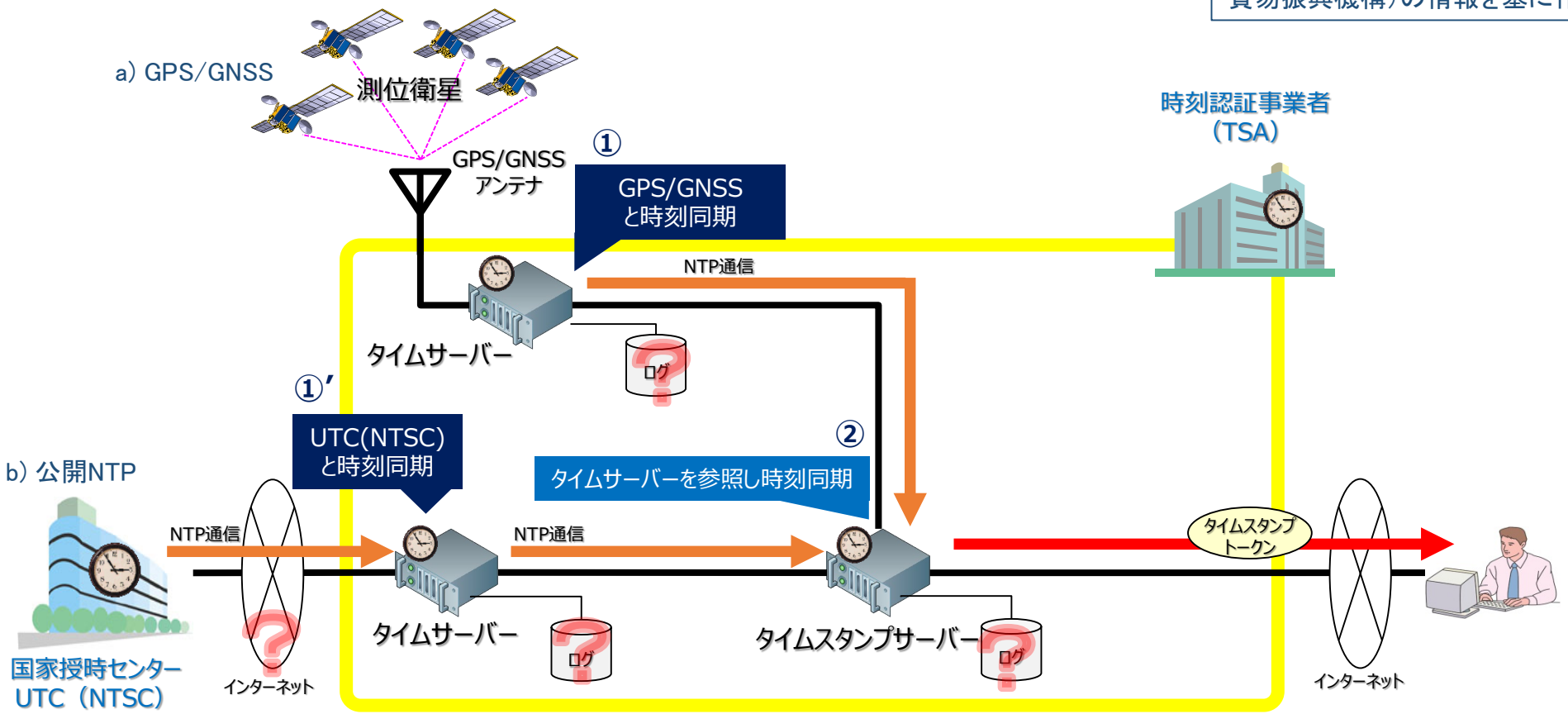
時刻同期	a) GPS/GNSS	b) 公開NTP	a) b) 両方
	2社	2社	5社

時刻監査	記載あり	記載なし
	0社	9社

1．認定の対象　②TAAの扱い

中国におけるTSAの時刻の信頼性確保イメージ

「中国におけるタイムスタンプの活用について」(2019年9月 日本貿易振興機構)の情報を基に作成



時刻同期	a) GPS/GNSS	b) 公開NTP	a) b) 両方
	1社	3社	0社

時刻監査	記載あり	記載なし
	0社	4社

1. 認定の対象　②TAAの扱い

TSAが発行するタイムスタンプ時刻の信頼性確保※1の方法

項目	第三者（TAA）が保証する方式	TSAが自ら立証する方式
1) 時刻同期の方法	TAAからの時刻配信	GPS/GNSS、公開NTPサーバー、光テレホンJJY等
2) 基準となる時刻	UTC(NICT)※2	UTC(NICT)、UTC(UNSO)※2、他
3) 時刻同期の精度	数十ミリ秒程度の誤差	数マイクロ秒程度～数十ミリ秒程度の誤差
4) 時刻トレーサビリティの証明方法	TAAによる時刻監査結果 エビデンス： ①NICT−TAA間の時刻比較結果 ②TAA−TSA間の時刻比較結果 （時刻監査証）	時刻同期の仕組みの説明とログ等による結果の証明 エビデンス： ①時刻同期の仕組みを表す文書 ②各機器の時刻同期ログ ③専門家による鑑識報告等
5) TSAの費用比較イメージ※3	100	10～20

※1 タイムスタンプ時刻の信頼性確保とは：基準となる時刻及びその時刻との誤差範囲（許容範囲）が予め明確に示され、発行された全てのタイムスタンプの時刻がその誤差範囲（許容範囲）におさまっていることを証明できること

※2 UTC（協定世界時）に付された（　）内は、原子時計を用いて協定世界時の運用に協力する機関の略称。NICTは情報通信研究機構。UNSOは米国海軍天文台でGPSに搭載されている原子時計はこれと同期している。

※3 第三者（TAA）が保証する方式の「TAAのサービス料金」を100とした場合のTSAが自ら立証する方式の「TSAのハードウェア費用、保守料金、雑費」の年額（概算値）比率を推定。

1．認定の対象　②TAAの扱い

TAAの扱いに関する方向性

・タイムスタンプの信頼性を確保するためには、①時刻の正確性、②時刻のトレーサビリティ　の担保が重要。

・第三者（TAA）が保証する方式によらずとも、

①は、GPS/GNSSや公開NTPサーバー等の時刻源と同期した時刻を用いることで担保することが可能であり、

②は、サーバーのログ等を活用することで担保することが可能。

・EUや中国においても、「TSAが自ら立証する方式」が主流であり、十分なタイムスタンプの信頼性を備えている。

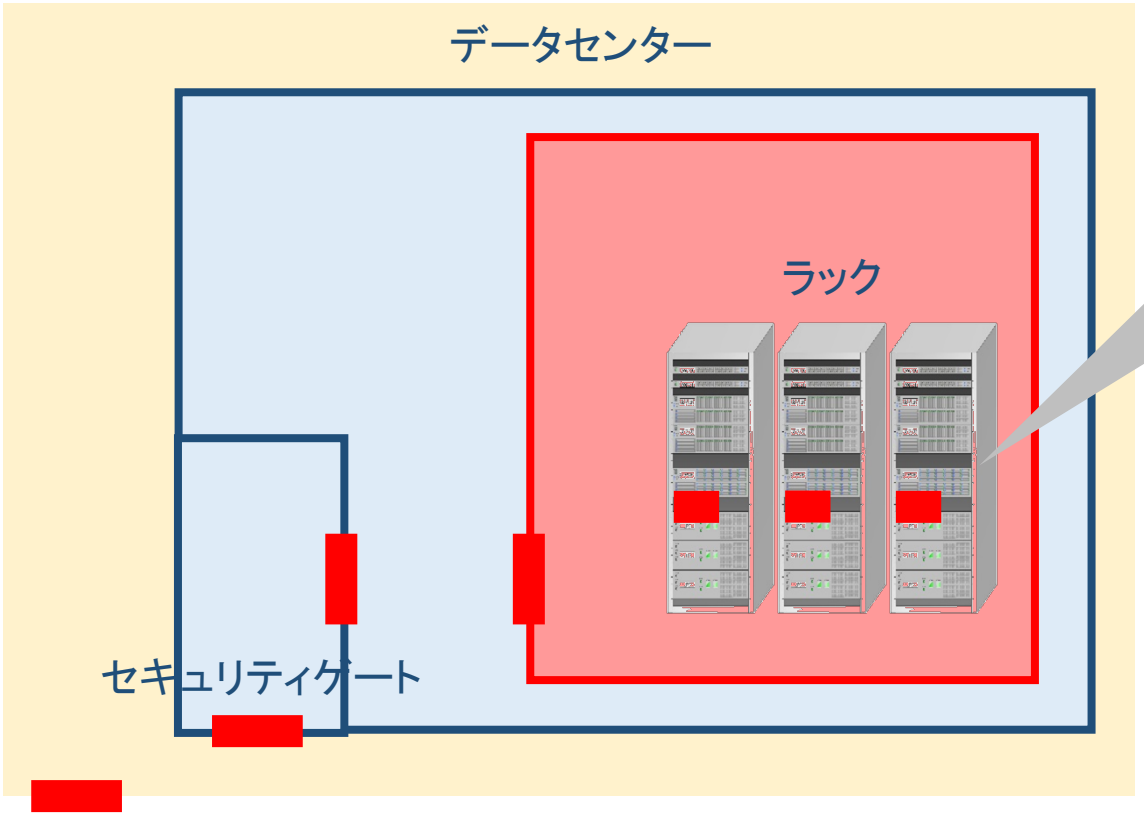
・「TSAが自ら立証する方式」により、TSAのコストを削減、ひいては利用者のサービス料を低減できる余地がある。

- タイムスタンプの信頼性確保に関し、第三者（TAA）が保証する方式に限定せず「TSAが自ら立証する方式（※）」も認める。

（※）日本で採用する具体的な方法については、次回検討

2. 認定の基準　①設備面の基準

検討の前提（HSM※1のセキュリティレベルの扱い）



タイムスタンプサーバー

（内蔵）

秘密鍵

HSM 秘

タイムスタンプの発行に用いる
秘密鍵が保護すべき対象

秘密鍵が漏えいすると

- **秘密鍵を取得した者が、不正なタイムスタンプを発行できる**
- **失効処理が行われ発行済みタイムスタンプの正しい検証ができなくなる**

※1　HSM（Hardware Security Module）は、耐タンパー機構による物理的な安全性が確保された鍵管理機能を備えた暗号処理装置。一般に、鍵の生成やデジタル署名の生成等の機能も備えています。

2. 認定の基準　①設備面の基準

検討の前提（HSMに関係する標準）

	FIPS140-2	コモンクライテリア（CC）
概要	米国連邦政府の省庁等各機関が利用する暗号モジュールに関する要件を規定したもの。	日米はじめ30か国以上が加盟する国際協定により、認証書は相互に通用する。
関連標準	ISO/IEC 19790, JIS X 19790	ISO/IEC 15408, JIS X 5070
対象	暗号モジュール	ITセキュリティ
機能要件	インターフェース、物理的セキュリティ、暗号鍵管理等10分野につき、レベル1～4の4段階で規定	備えるべきセキュリティ機能に関する要件を標準に記載された項目から選択する方式
保証要件※1	設計保証（モジュールが十分な設計がなされたことを明らかにする）	設計から製造の過程で、セキュリティ機能が実現されていることを確認する要件を7段階に分類しており、標準に記載された項目から選択する方式
認証制度	CMVP※2（米加） JCMVP（日）：IPA	加盟各国に認証制度がある JISEC（日）：IPA

※1　セキュリティ対策に必要となる機能が確実に動作することを確信するための根拠を「保証要件」として定めている。

※2　CMVP（Cryptographic Module Validation Program）は、米国・カナダの認証制度で、FIPSの規定に基づきセキュリティが確保されていることを評価する制度。

2. 認定の基準　①設備面の基準

現状（タイムビジネス信頼・安心）認定制度

- HSMのセキュリティレベルに関する要件

タイムビジネス信頼安心認定制度　時刻認証業務（デジタル署名を使用する方式）審査基準
（1）技術基準　12.タイムスタンプトークンの生成に用いる秘密鍵の保護装置
タイムスタンプトークンの生成に使う秘密鍵は、HSM（FIPS140-2のレベル3認証相当以上の製品）を用いて保護する。

➡具体的には、FIPS140-2 レベル3に定められる基準を用い、米加の認証制度であるCMVP（Cryptographic Module Validation Program）により認証された製品、又は、相当以上の製品を用いることを求めている

セキュリティ・レベル	物理的なセキュリティ要件	アクセス権限に関するセキュリティ要件
レベル1	暗号モジュールとしての基本的なセキュリティ要求事項のみが充足されることが求められる	なし
レベル2	レベル1に加え、物理的セキュリティのメカニズムを強化したレベルで、攻撃の痕跡を残す機能が求められる	オペレータの役割ベースでの認証
レベル3	レベル2に加え、高い確率で攻撃の検知または能動的に対抗するための機能（データ消去等）が求められる	オペレータのIDベースでの認証
レベル4	全ての攻撃の検知や能動的対抗機能に加え、高温等の規格外環境でも暗号モジュールの保護が求められる	

秘密鍵の漏えいを防ぐために必要最低限のレベル

2. 認定の基準 ①設備面の基準

現状の課題（事業者ヒアリングに基づく）

- 調達可能なHSM（FIPS140-2レベル3の基準でCMVPの認証を取得）は極めて限定的で**継続的な調達に不安**がある
  - 現在、調達条件に見合う製品の提供が確認できているのは、Thales社（仏）及びnCipher Security社（英）の2社のみ
- 障害が発生した際の調査や修理には相当な期間を要するため、予備機を多めに確保する必要がある
  - HSMは高価であり、コスト負担も重い
- タイムスタンプの発行には無関係な問題により、CMVPの認証リストから外れる場合もある
  - 認証された製品であっても、基準の変更等により認証ステータスが「Active」から「Historical」（政府調達の条件を満たさないステータス）に変更されることもある。

2. 認定の基準　①設備面の基準

EUにおけるHSMのセキュリティレベルの要件

- 次のいずれかに準拠することを規定

ⅰ）コモンクライテリア

・対象はITセキュリティ
・加盟各国の認証制度

【機能要件】
トラストサービスプロバイダーが用いるHSMとして備えるべきセキュリティ要件
（備えるべきセキュリティ要件はプロテクションプロファイル※1としてEUで策定済み）

or

ⅱ）FIPS 140-2

・対象は暗号モジュール
・米加が行う認証制度（CMVP）

【機能要件】
レベル3以上
（高い確率で攻撃の検知または能動的に対抗するための機能（データ消去等）を備える）

※1　コモンクライテリアの要求事項から利用分野に適した項目を選択し、要求仕様として取りまとめたもの。

どちらも**秘密鍵の漏えいを防ぐために必要最低限のレベル**は備えている。

2. 認定の基準　①設備面の基準

設備面の基準に関する方向性

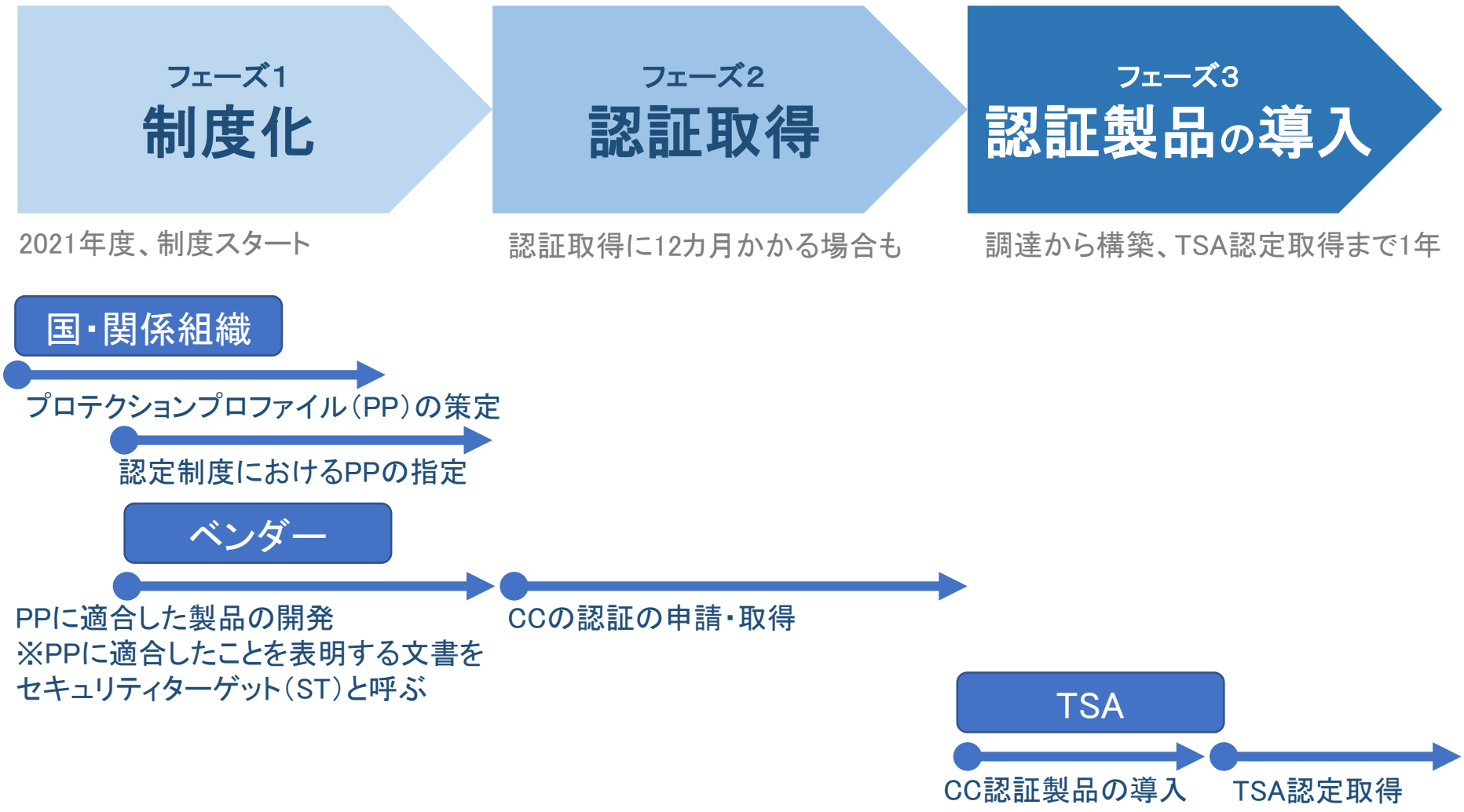
- HSMのセキュリティレベルの扱い

・FIPS140-2レベル3の基準でCMVPの認証を取得した調達可能な製品は限定的かつ高コスト
・他方、秘密鍵の漏えいを防止するために現状のセキュリィティレベルは必要最低限
・同等のセキュリティレベルを確保されたコモンクライテリアに基づく認証による規定を設けることで、調達可能な製品の裾野が広がる

- FIPS及びコモンクライテリアの基準及び対応する認証制度を用いた審査基準を策定する
  - コモンクライテリアについては、今後、備えるべき要件を選択しプロテクションプロファイルとして策定する必要がある

（参考）2. 認定の基準　①設備面の基準

コモンクライテリア（CC）認証活用へのステップイメージ



2. 認定の基準　②審査プロセス効率化

審査プロセス効率化の検討

- 既にISMS等の認証を取得しているTSAについて、当該認証と重複する調査項目を省略する余地があるのではないか。
- 電子署名法の認定認証業務の申請で提出した書類や調査の結果等を活用する余地があるのではないか。

新規認定に係る審査や、更新認定に係る審査において、他の認証制度等の活用による審査の効率化を検討することが必要

2. 認定の基準　②審査プロセス効率化

ISMSの認証を活用した効率化イメージ

- ISMS認証で確認されている項目の審査簡素化
  - 省略の可能性のある内容
    - 職務の分離（相反する職務及び責任範囲の分離）
    - 関係当局との連絡（関係当局との適切な連絡体制を維持）
    - 情報セキュリティの意識向上、教育及び訓練
    - 情報の分類、情報のラベル付け
    - アクセス制御方針
    - ネットワーク及びネットワークサービスへのアクセス
    - 利用者登録及び登録削除
    - 物理的入退室管理　等

2. 認定の基準　②審査プロセス効率化

電子署名法の認定を活用した効率化イメージ

- 重複する提出書類の省略
  - 申請者の実在を証する公的書類（登記簿謄本等）や会社概要等の電子署名法の認定とタイムスタンプに係る認定で重複する提出書類を省略する。
- ファシリティに関するエビデンス確認の省略
  - 現状、使用するファシリティが建築基準法に適合していることを確認するために、建築確認通知書や建築確認済証の確認を行っている。
    - 申請事業者とファシリティを所有する者との間には複数の契約当事者が介在する場合もあり、機密情報であるデータセンターの所在地が記された書面の開示手続きには多大な労力を要する。
  - 電子署名法の特定認証業務の認定でも同じ確認を行っており、既に署名法の認定業務で用いられていることを証すれば、このエビデンス確認を省略する。

2. 認定の基準　②審査プロセス効率化

審査プロセス効率化の方向性

・ISMS等の認証を活用することで審査の効率化が期待
・電子署名法の認定認証業務の申請で提出した書類や調査の結果等を活用することで審査の効率化が期待

- 審査プロセス効率化の観点から他の認証制度等を活用する
  - 今後、具体的に活用し得る審査の項目・書類等について、精査する

END

各論点について

タイムビジネス認定センター