経済産業省　平成18年度
流通システム標準化事業

通信プロトコル・セキュリティの検討プロジェクト

通信プロトコル・セキュリティの検討プロジェクト活動報告

財団法人 流通システム開発センター
株式会社 野村総合研究所

通信プロトコル・セキュリティの検討プロジェクトの目的

- 本年度の流通システム標準化事業で検討が進められている、新しい業界インフラである、流通ビジネスメッセージ標準および商品データ同期化（GDS）は、インターネットをベースとしたネットワークを活用するため、オープンなネットワーク環境での信頼性、安全性を確保した企業間通信が必要になる。
- そこで、本プロジェクトでは、流通ビジネスメッセージ標準と商品データ同期化（GDS）の両方について、国際標準化動向、技術動向を踏まえた上で、信頼性、安全性を確保した企業間通信を実現する、通信基盤、セキュリティ認証のあり方を検討した。
  - 流通ビジネスメッセージ標準も商品データ同期化（GDS）も、共通のルールに基づいた通信基盤・セキュリティ認証のしくみを利用することで、業界インフラごとの無意味な個別対応をなくし、新しい業界インフラの導入を促進させることを目指した。
- また、商品データ同期化（GDS）については、来年度以降の実用化を視野に入れ、海外（GS1）で行われているようなデータプール事業者の認証が、必要かどうかの検討を行った。

プロジェクトの全体概要

経済産業省　平成18年度
流通システム標準化事業

■ 各テーマにおける、検討テーマ、成果物、利用目的、及び利用者は、以下の通り。

テーマ	成果物	利用目的	利用者
相互セキュリティ基盤に関する検討・認証局構築	2006年度実証用の認証局構築基準、認証業務規定、及び証明書発行	・2006年度実証事業を通じた、認証局、認証業務、証明書機能等の評価 ・下記ガイドラインを検討するために、共同実証に向け証明書を発行し、評価を実施	2006年度実証参加企業（EDI・GDS）
	業界共通認証局構築・運営・利用ガイドライン	・来年度以降、認証局サービスを行う企業に対する業界共通認証局の基準の提示 ・登録局基本作業の規定 ・証明書利用者への取得・利用の指針提示	認証局サービスベンダー、協議会（仮称）、企業間通信実施ユーザ・ベンダー
通信プロトコル標準化に関する検討	インターネットを利用した通信プロトコルガイドライン	来年度以降、流通システム標準化事業（流通ビジネスメッセージ標準・GDS）の成果を活用する際の、各種通信プロトコルのパラメータ等の設定指針	企業間通信実施ユーザ・ベンダー
GDSにおけるデータプール事業者認証基準策定に関する検討	我が国におけるデータプール認証の今後のあり方の検討指針	次年度以降の流通システム標準化事業のデータプール事業者等のサービス検討の素材とする	次年度流通システム標準化事業の検討事業者

相互セキュリティ基盤に関する検討・認証局構築

相互セキュリティ基盤の必要性

■ 相互セキュリティ基盤の必要性

- 新しい業界インフラである、流通ビジネスメッセージ標準および商品データ同期化（GDS）は、インターネットをベースとしたネットワークを活用するため、オープンなネットワーク環境での信頼性、安全性を確保した企業間通信が必要である。
- インターネット上には、「盗聴」「改ざん」「なりすまし」等の危険性がつきまとう。このような危険を防止するために有効な、電子証明書を利用したセキュリティ基盤の検討が必要である。

■ 電子証明書の利用状況

- 現状、取引先毎に複数の証明書を使い分ける必要が生じており、データ交換の開始時及び証明書の期限切れ時の運用が煩雑になっていた。

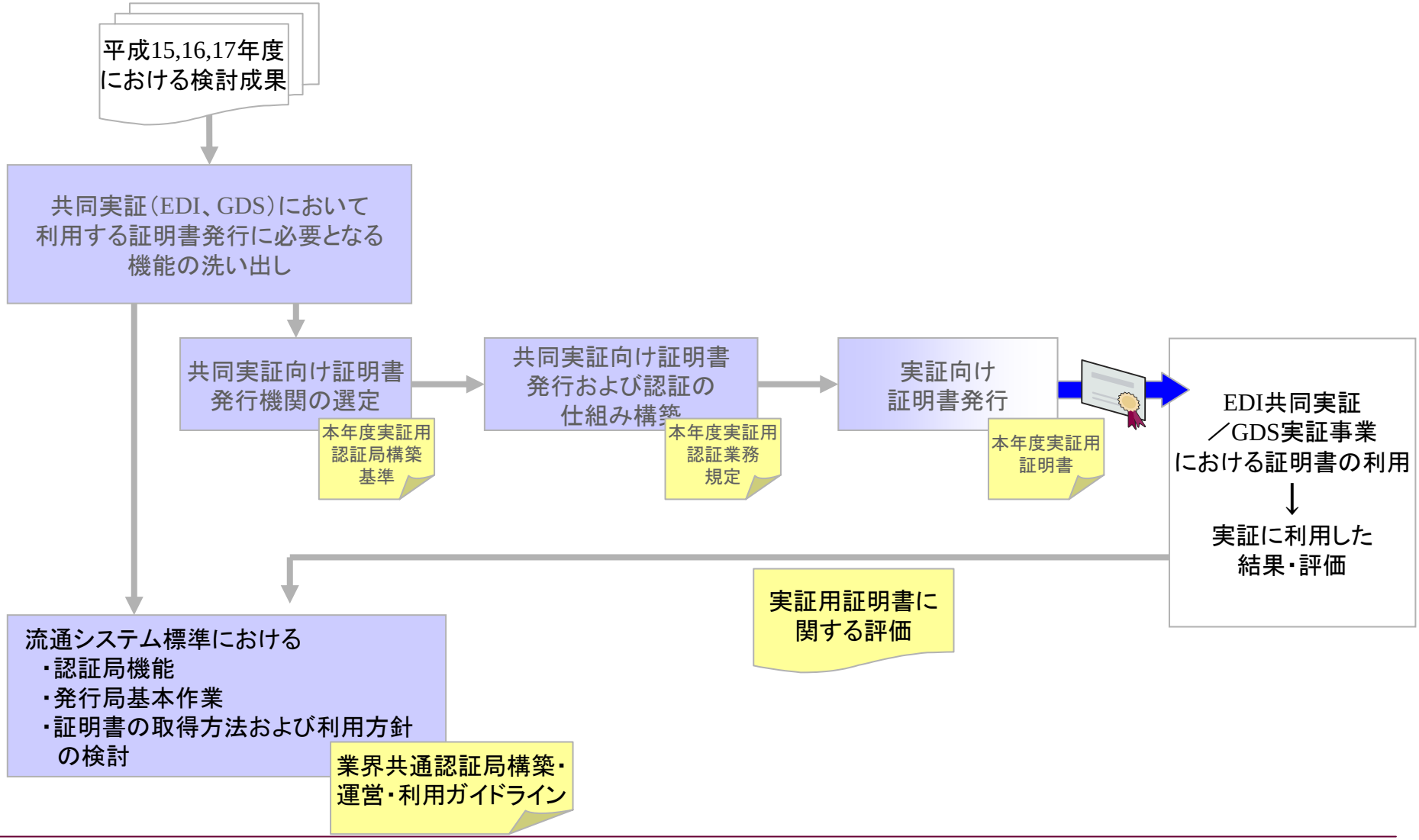
■ あるべき姿

- 一枚の証明書で複数取り引き先と電子商取引が実施できる、セキュリティ基盤の確立
- 証明書の有効期限が切れ、予期することなくB2B取引が中断することの無い、セキュリティ基盤の確立

相互セキュリティ基盤の検討が必要
- 業界共通認証局ガイドラインに基づく複数認証局間の相互通信

業界共通認証局構築ガイドラインWGの検討フロー

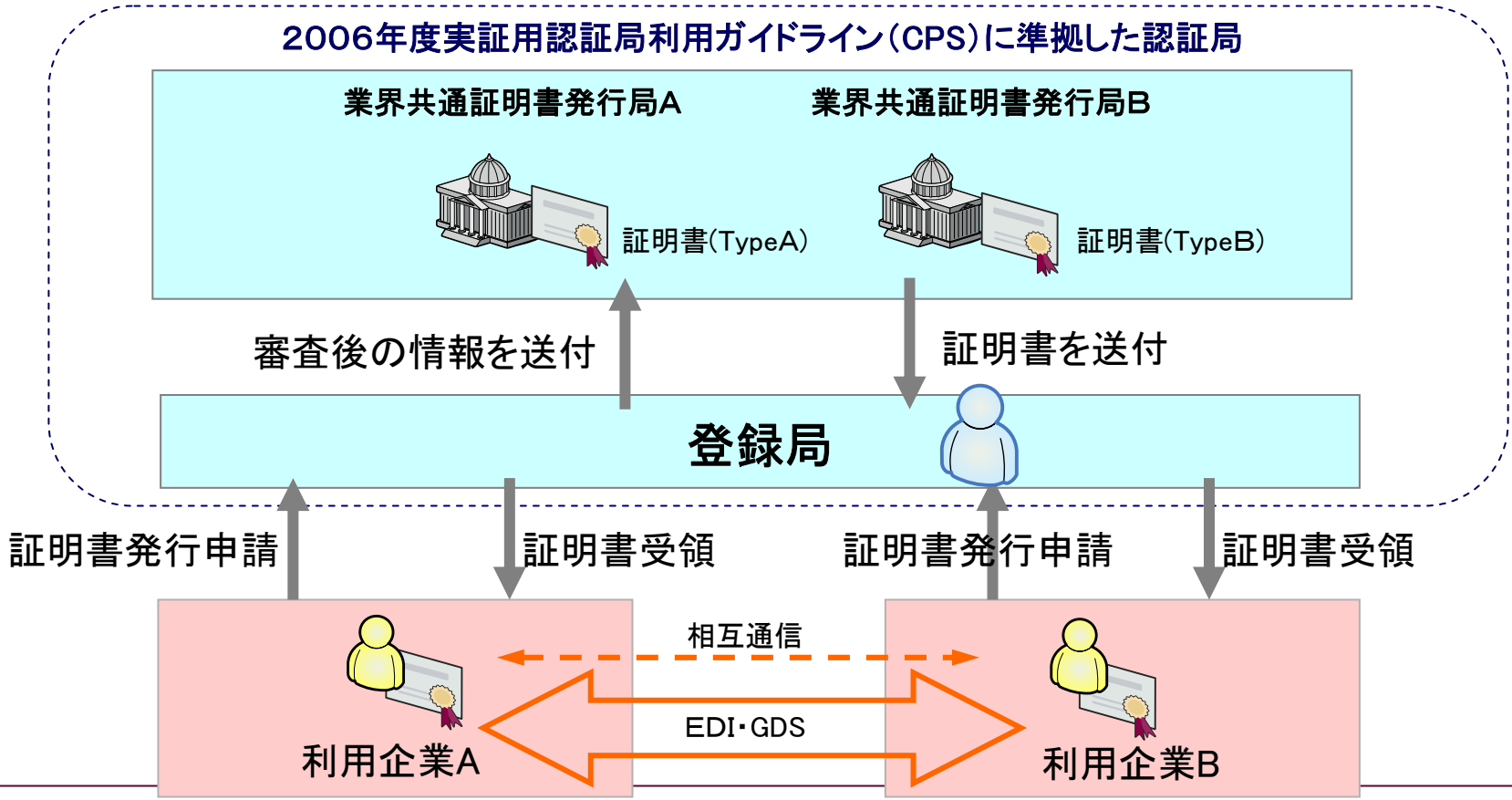
■ 業界共通認証局構築ガイドラインWGの検討フロー



【成果】共同実証向け証明書の発行

■ 2006年度実証用の認証局構築基準、認証業務規定、及び証明書

- 実証用の認証局構築基準、認証業務規定に基づいて、GDS実証及び流通ビジネスメッセージ標準共同実証向けに証明書を発行
- 2社の業界共通証明書発行局から証明書を発行することで、異なる証明書の相互通信を検証可能な環境を提供



【成果】共同実証における検証項目

分類	検証項目
相互通信	共同実証における通信パッケージによる業界共通証明書の利用の可能性
	異なる認証局から発行された証明書の相互通信
証明書の変更	期限切れ間近の証明書と継続証明書の自動切換え
	証明書の入れ替え（発行認証局は異なる）
証明書の失効	証明書効情報取得の各種アプリケーションの動作確認と新規有効証明書導入時の動作確認（相手先との通信遮断が正常動作）
	証明書失効後の新規証明書導入時の動作確認（発行認証局は異なる）
証明書のﾗｲﾌｻｲｸﾙ管理	証明書発行ライフサイクルのユーザビリティ検証

＊現在、共同実証における検証中のため、検証結果は4月以降流通システム開発センターのホームページにて公開を予定しています。

【成果】相互セキュリティ認証基盤構築に関する検討

経済産業省　平成18年度
流通システム標準化事業

第一部　流通システムにおけるPKIを利用した総合セキュリティ基盤の考え方

1. インターネット環境における商取引のセキュリティ上の課題
   ・・・セキュリティインシデント、脅威の整理など
2. PKIを用いたセキュリティの確保
   ・・・電子署名、電子認証、暗号化、各種セキュリティプロトコルなど
3. 総合セキュリティ基盤
   ・・・目的、構成、認証の対象範囲、認証方法、電子証明書の利用用途[illegible]要件など
4. 総合セキュリティ基盤を構成する認証局の信頼性モデル
   ・・・PKIにおける認証局の信頼性モデル、現状の環境、採用すべき信頼性モデルなど
5. 既存認証局の利用と共存
   ・・・既存認証局の利用可能性など
6. 総合セキュリティ基盤の今後
   ・・・想定される総合セキュリティ基盤に関わる環境の変化、対応策、各対応策ごとの移行方式など

第二部　PKIを用いた総合セキュリティ基盤構築に向けた対応

1. 総合セキュリティ基盤を構成する認証局の認定制度の必要[illegible]
   ・・・認証局の信頼性を確保する仕組み、認証局認定機関による認定[illegible]
2. 総合セキュリティ基盤における認証局認定制度
   ・・・証局認定制度の目的、構成、業務、認定機関に関する要件、認定の取得・維持に関する要件
3. 認証局認定制度の今後の課題

第三部　平成17年度実証事業における評価結果

1. 相互セキュリティ基盤に関する相互通信の実用性検証
2. 証明書の変更について
3. 証明書の失効
4. 証明書のライフサイクル管理

認証局の信頼性モデルの検討

認証局の認定制度の検討

検証結果の評価

業界共通認証局ガイドライン（CP）への反映

【成果】業界共通認証局ガイドライン（CP）の構成

経済産業省　平成18年度
流通システム標準化事業

証明書の
プロファイル

証明書の
有効期限

認証局の監査
基準

証明書の失効
と一時停止

業界共通認証局
ガイドライン（CP）

認証局の瑕疵
責任

証明書の利用用途（例）

1.適切な証明書の利用用途

各流通業界共通認証局が発行する証明書の利用用途は以下の範囲に制限される。

(1)法人の証明書
- •GDSまたはEDI用途のメッセージ署名
- •GDSまたはEDI用途のSSLクライアント認証

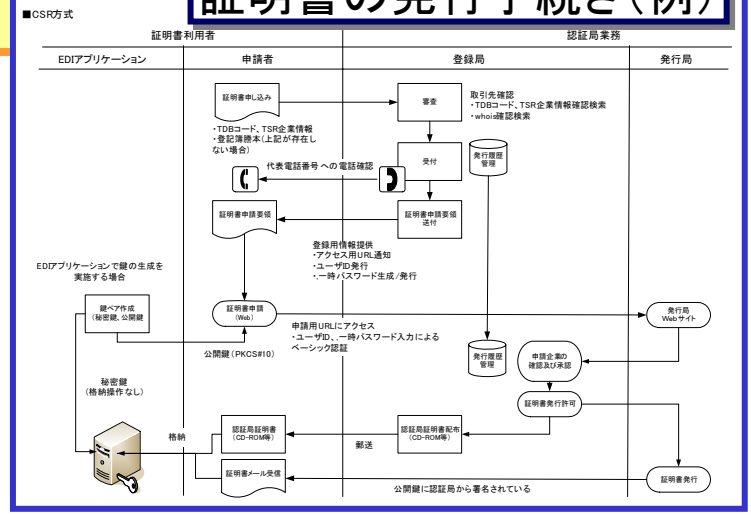
(2)法人に所属する役員・職員・契約社員の証明書
- •GDSまたはEDI用途のメッセージ署名
- •GDSまたはEDI用途のSSLクライアント認証

(3)法人が所有するサーバまたはシステム（の管理者）の証明書
- •GDSまたはEDI用途のSSLサーバ認証

(4)個人事業主の証明書
- •GDSまたはEDI用途のメッセージ署名
- •GDSまたはEDI用途のSSLクライアント認証

(5)個人事業主が所有するサーバまたはシステム（の管理者）の証明書
- •GDSまたはEDI用途のSSLサーバ認証

証明書の発行手続き（例）

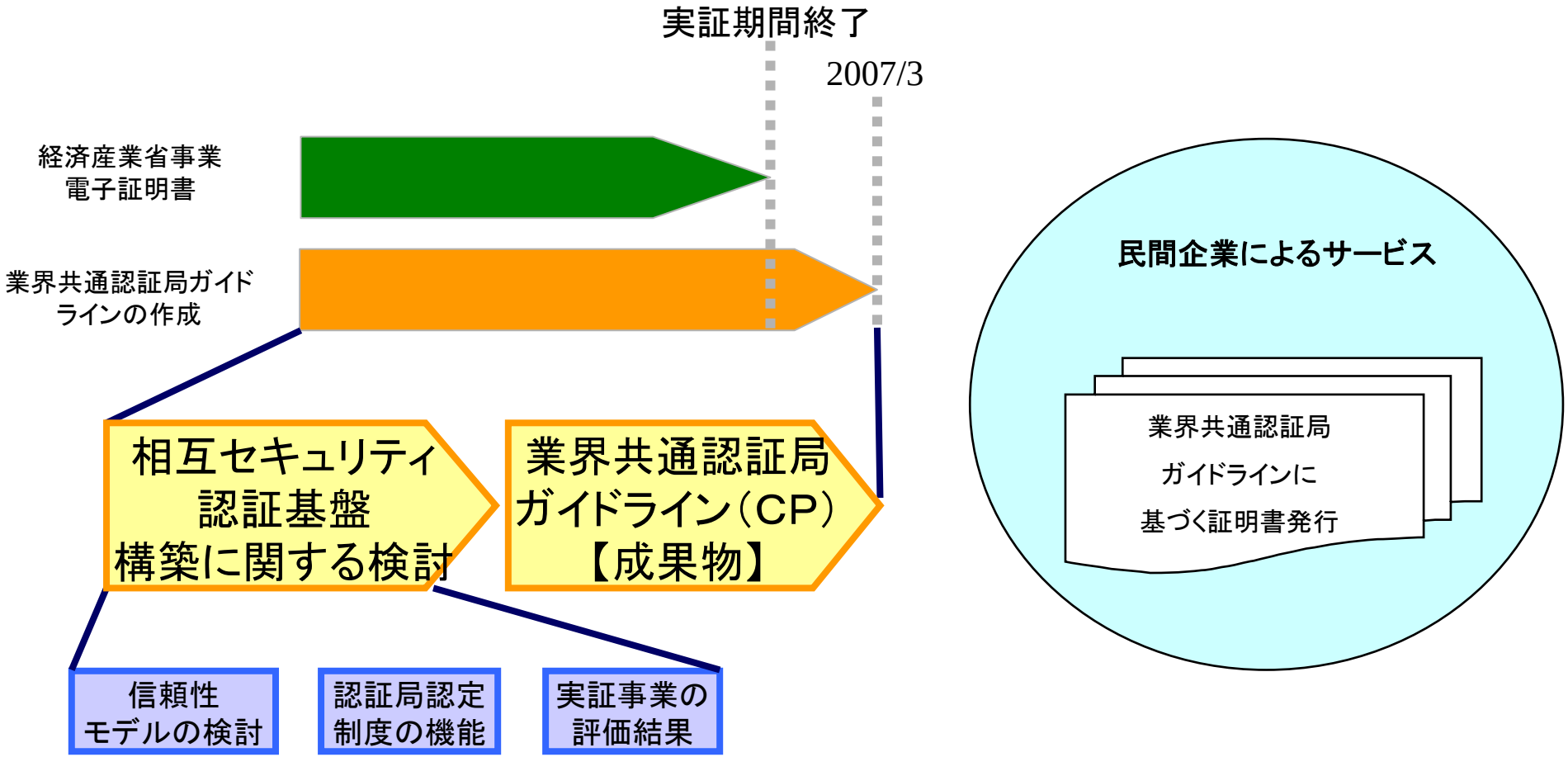


業界共通認証局ガイドライン（CP）をベースに各認証局運営企業は、認証局運営規定（CPS）を作成し、サービスを実施する

CP：証明書ポリシー、CPS：認証局運営規定

業界共通認証局ガイドライン（CP）の作成

■ 業界共通認証局ガイドラインを検討し、成果物を作成



＊CP：証明書ポリシー

通信プロトコル標準化に関する検討

通信プロトコル標準化の必要性①

■ 通信プロトコル標準化の必要性

- ネットワークを介してコンピュータ同士が通信を行ない電子商取引を実施する上で、通信プロトコルの標準化を進めることで、取引先毎に通信プロトコルが異なるという不具合を排除する。

■ 3種類の通信プロトコルを選択した理由

流通ビジネスメッセージ標準で使用するインターネット通信手順については、標準をひとつに絞らず、下記のような活用実績のある手順の中から各社が任意に選択することとした。

◆サーバ間通信

①ebXML MS(Message Service)
- ・OASISとUN/CEFACT策定したグローバル標準の一つ
- ・平成16年度実施された経済産業省実証実験で採用
- ・流通システム開発センターがガイドラインを公表
- ・日本チェーンストア協会が次期EDIプロトコルとしてガイドラインを公表（平成15年）
- ・アジア圏における利用が拡大している

②AS2（Applicability　Statement2）
- ・IETF（Internet Engineering Task Force）が策定したグローバル標準の一つ
- ・ウォルマートが推奨。2002年より拡大。海外での適用事例が増えている。
- ・GDSで、グローバルレジストリ及びデータプール間との通信プロトコルに採用されている。

◆クライアントーサーバ間通信

①SOAP　RPC(Remote　Procedure　Call)
- ・平成16年度に実施された経済産業省実証実験で採用
- ・中小企業向けに最適なPull型通信プロトコル

通信プロトコル標準化の必要性②

経済産業省　平成18年度
流通システム標準化事業

■ 通信プロトコルパラメータ設定の必要性

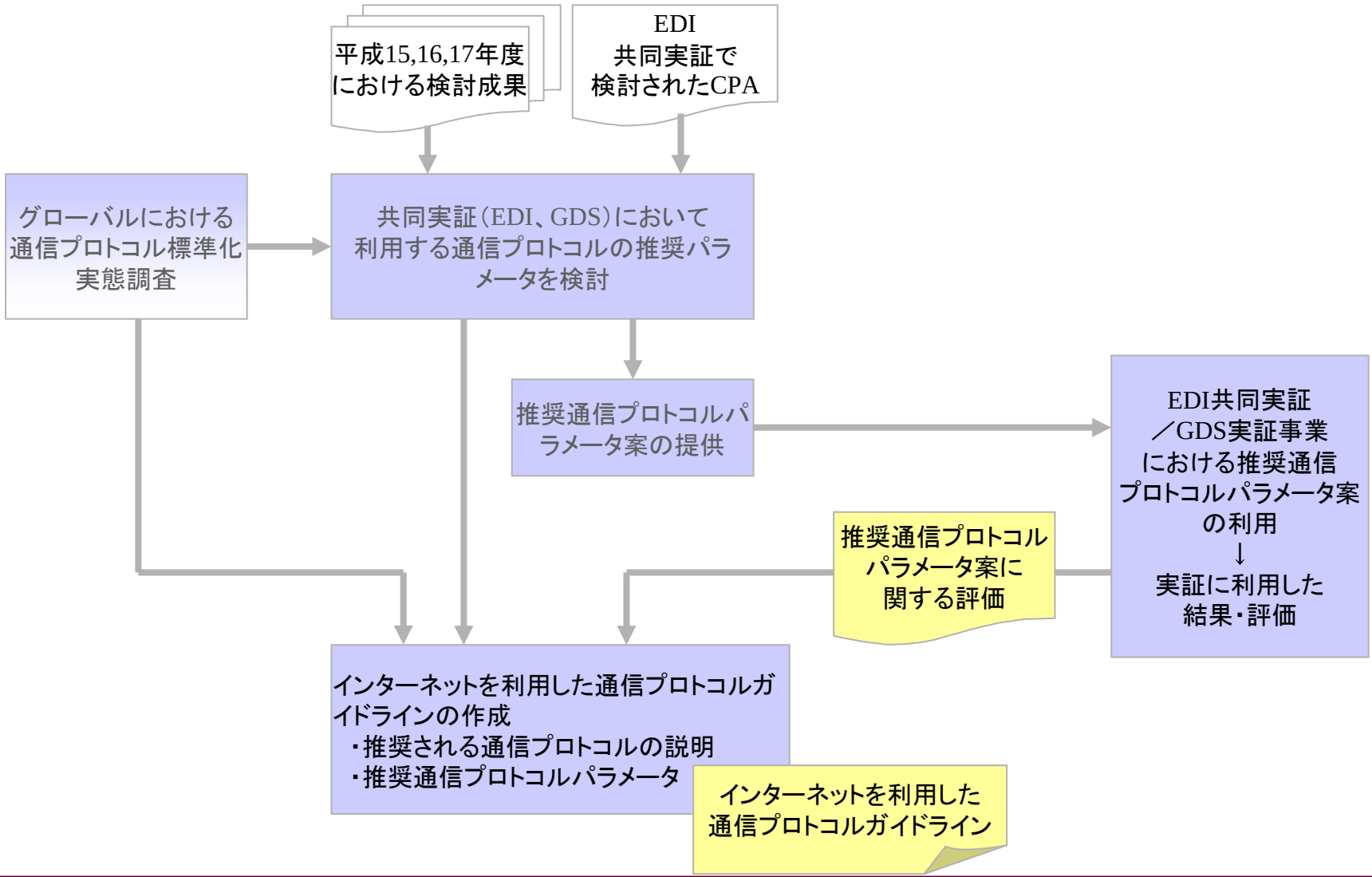
- インターネットの利用を前提とした通信プロトコルの設定パラメータは、出現して日も浅いため、相対で判断しながら確定する必要がある曖昧な設定項目が多かった。
- その為、経済産業省「流通システム標準化事業」では、相対で取り決めていた曖昧な設定項目をできるだけ固定値化することによって、相対での判断を少なくし、結果として企業間電子取引をスムースに開始できることを目的とした

通信プロトコルガイドラインの作成

通信プロトコルガイドライン利用によるインターネットを利用した電子商取引へのスムースな導入

通信プロトコルの利用WGの検討フロー

■ 通信プロトコルの利用WGの検討フロー



【成果】通信プロトコルガイドライン概要

- 「平成17年3月リリースのメッセージ交換ガイドライン」の改訂を実施
  - 3種の通信プロトコルを同じ目次立てで解説することで、読み手における分かり易さに重点を置いた
  - 推奨通信プロトコルパラメータやメッセージサンプルを掲載することで、実用性を向上した
- 新たに「インターネット利用を前提とした電子商取引における一般的なセキュリティ要件」を追加し、企業が電子商取引を開始する際に必要なセキュリティポリシーの雛形を提供

通信プロトコルガイドライン目次

【成果】通信プロトコルガイドライン
推奨通信プロトコルパラメータ①

■ 3種類（AS2、ebXML MS、SOAP-RPC）の通信プロトコルのパラメータ値を出来るだけ共通に推奨値を設定する事を目標に作業を実施し、以下のような成果物を作成

		統一推奨値	備考
トランスポート層情報			
認証方式	サーバ認証	SSLサーバ認証有り	
	クライアント認証	一部検討中	SOAP-RPCはサーバ側セキュリティポリシーに準拠
	ベーシック認証		SOAP-RPCは必須
EDI関連通信仕様情報			
同期／非同期モード		同期応答	SOAP-RPCは該当無し
応答要求		あり（受領確認）	
応答への署名		なし（受領確認への署名）	
重複検出		あり（二重送信防止）	

＊主なものを掲載

【成果】通信プロトコルガイドライン
推奨通信プロトコルパラメータ②

		統一推奨値	備考
信頼性メッセージ交換			
	再送回数	3回	送信に失敗した際のリトライ回数
	再送間隔	3分	再送時にあける間隔
	配信順序保証	無し	配信する順序の保証の有無
	重複検出時間	30分	受信済みメッセージに対する重複検出可能な時間
ビジネスメッセージ特性		一部検討中	
	セキュリティ仕様 送信否認拒否		SOAP-RPCはサーバ側セキュリティポリシーに準拠
	セキュリティ仕様 受信否認拒否	無し	
	セキュリティ仕様 メッセージ暗号化	無し	

■ 通信プロトコルのパラメータ値を共同実証プロジェクトに引渡し、実効性について検証を行った

＊現在、共同実証における検証中のため、検証結果は4月以降流通システム開発センターのホームページにて公開を予定しています。

【成果】通信プロトコルガイドライン 推奨通信プロトコルパラメータ③

経済産業省　平成18年度
流通システム標準化事業

■ 推奨通信プロトコルパラメータの検討に当たっては、技術面ばかりでなく、グローバルスタンダードの状況、ベンダーの実装状況、ユーザの実装状況を加味した上で、最適値を選定し 、以下のような成果物を作成

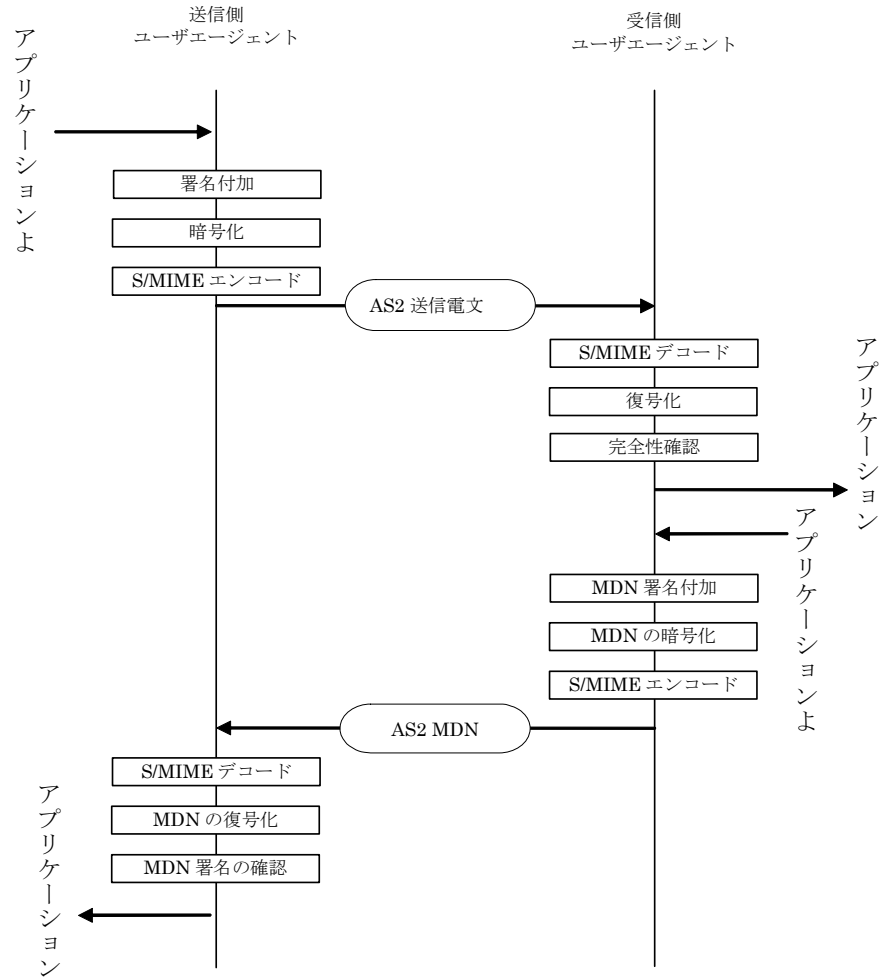
3種類の通信プロトコルのパラメータ値を共通化出来なかった事例

通信プロトコル	一次局（送信元）における接続先の確認	二次局（送信先）における接続元の確認	選定の理由
ebXML MS	SSLサーバ認証	接続認証（ベーシック認証→SSLクライアント認証）	データ送信前に、送信元の確認可能 ユーザID、パスワードを入れ替える必要なし
AS2	SSLサーバ認証	メッセージ署名	GS1にて認証方式が「メッセージ署名」に規定されている S-MIMEベースのプロトコルのためメッセージ署名との親和性が高い
SOAP-RPC	SSLサーバ認証	ベーシック認証	SSLクライアント認証対応製品が普及していない 製品の対応が出来次第、SSLクライアント認証に移行を推奨

＊現在、共同実証との検討の最中のため、推奨通信プロトコルパラメータは4月以降流通システム開発センターのホームページにて公開を予定しています。

【成果】通信プロトコルガイドライン
対象通信プロトコルの概要①：AS2の特徴

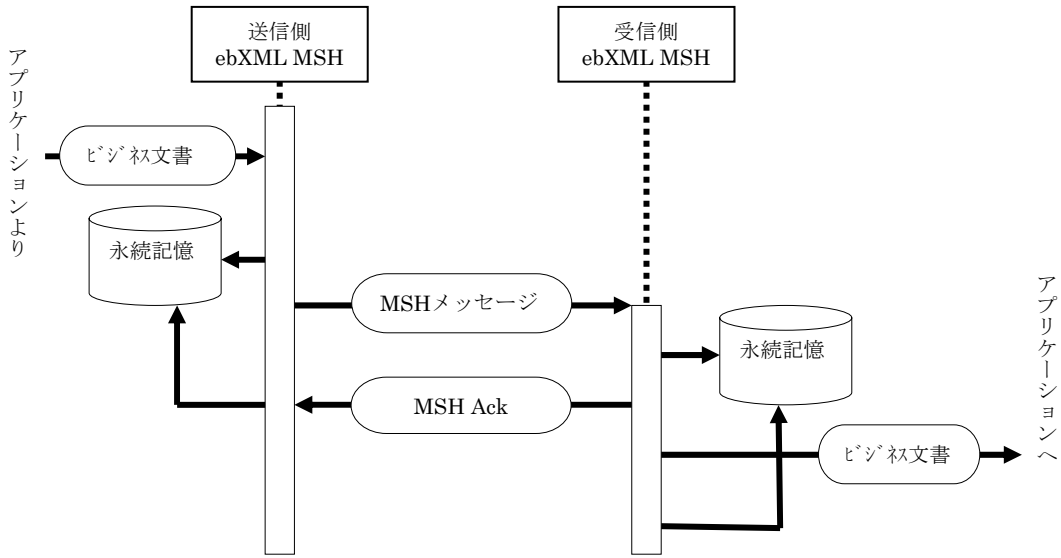
- AS(Applicability Statement)の特長はMDNの設定である。MDNは送達確認にために使用される。
- AS2には同期モデルと非同期モデルがある。同期モデルの場合は、元のAS2文書を送受信したHTTPセッションと同一のセッション内でMDNの返信が実行される（今回の推奨値は同期モデル）。
- セキュリティは、電子署名による認証と暗号化、いわゆるSecure MIME(S/MIME)の形式を選択することができる。



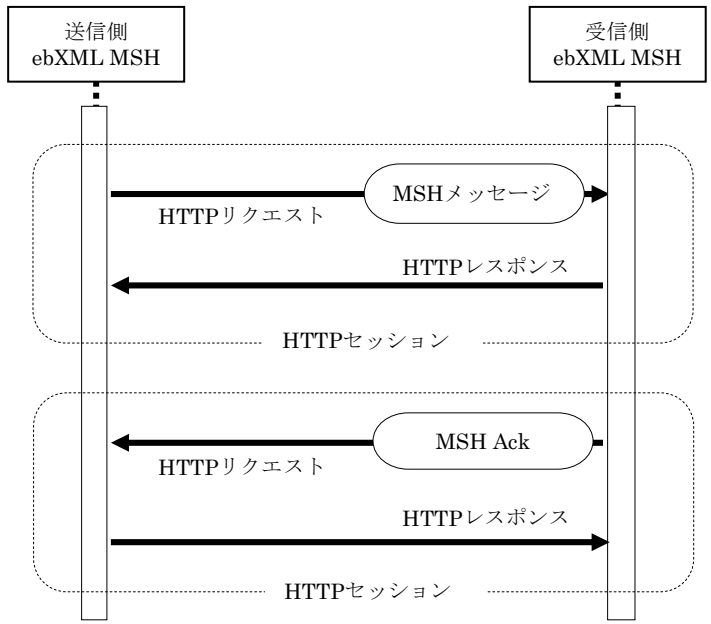
【成果】通信プロトコルガイドライン
通信プロトコルの概要②：ebXML MSの特徴

- ebXML v2.0 では電子署名による認証と暗号化が可能。また、否認防止の機能を実現するために、Acknowledgement Message（Ack）を返信することを規定している。
- ebXMLもAS2と同様にHTTPトランスポートを選択した場合には同期モデルと非同期モデルがある。

同期シーケンス



非同期シーケンス

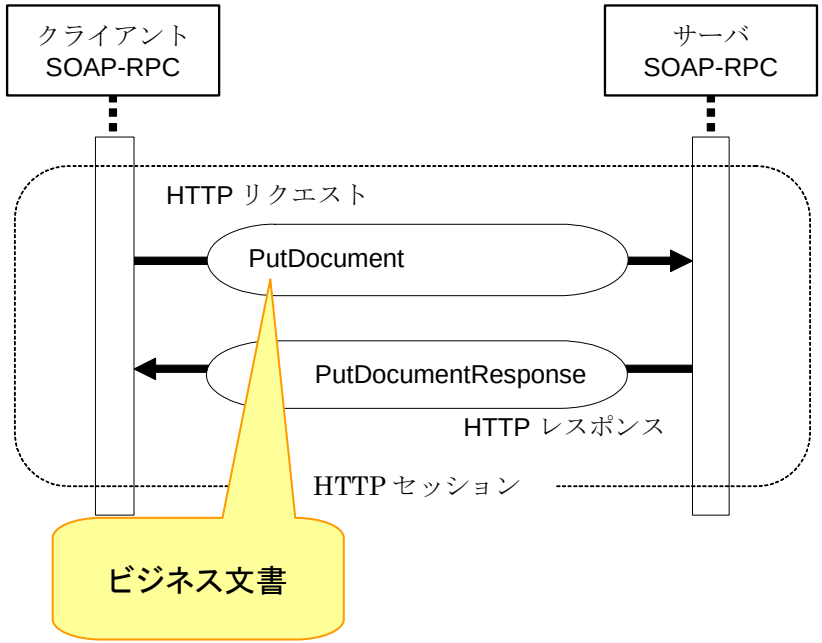


【成果】通信プロトコルガイドライン
対象通信プロトコルの概要③：SOAP-RPCの特徴

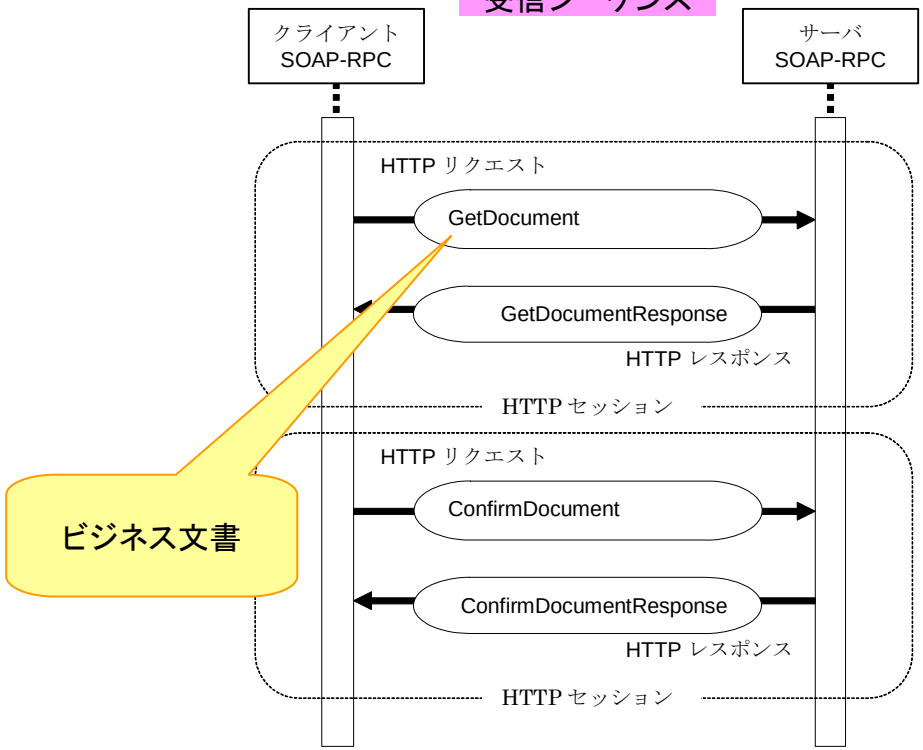
経済産業省　平成18年度
流通システム標準化事業

- データを転送するための3つのSOAP-RPCメソッドより構成されるシンプルな通信プロトコル。
  ①PutDocument　②GetDocument　③ConfirmDocument
- 通信の一次局（起点）はクライアント側であり、クライアントからサーバへの接続により処理が開始され、ビジネス文書の送信や受信を行う。
- 取引量が少なく、低コストでインターネットEDIを実現したい中小企向けに適している。

送信シーケンス



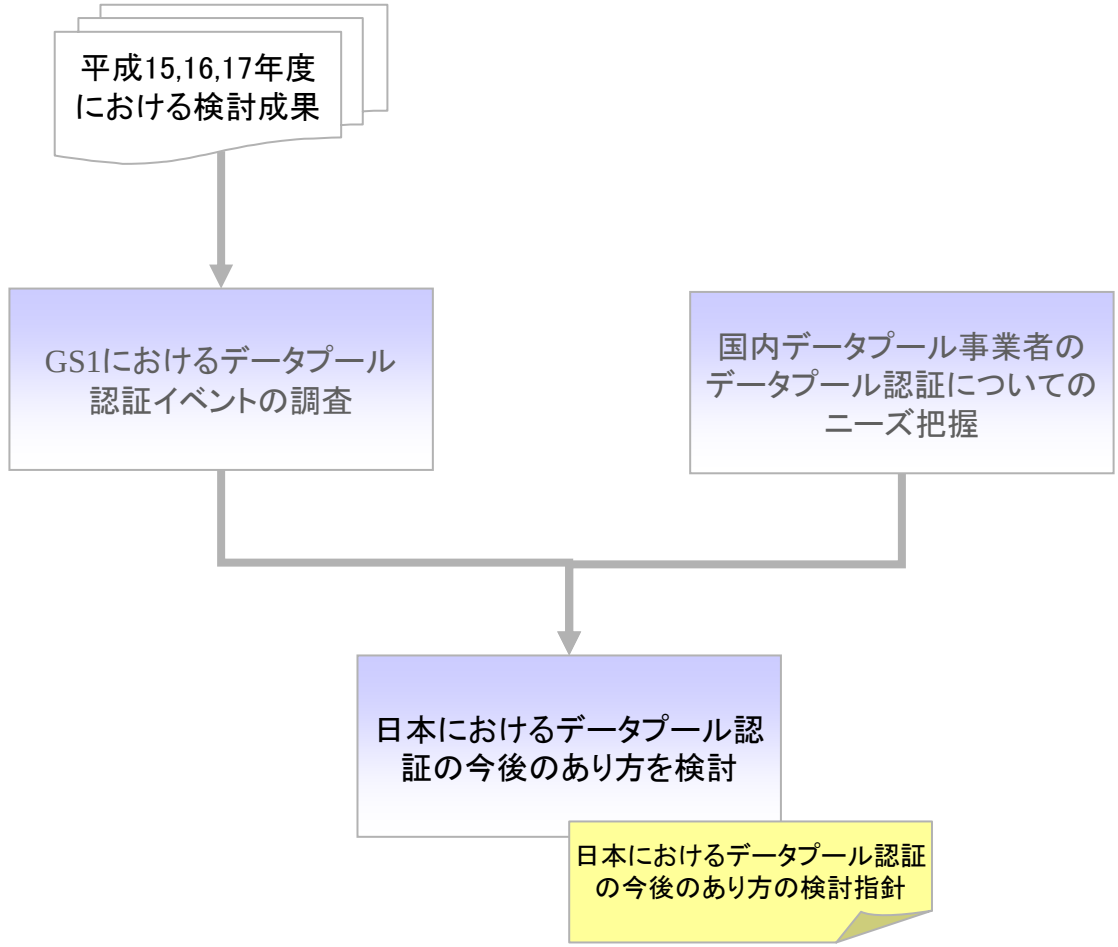
受信シーケンス



GDSにおけるデータプール事業者認証基準策定に関する検討

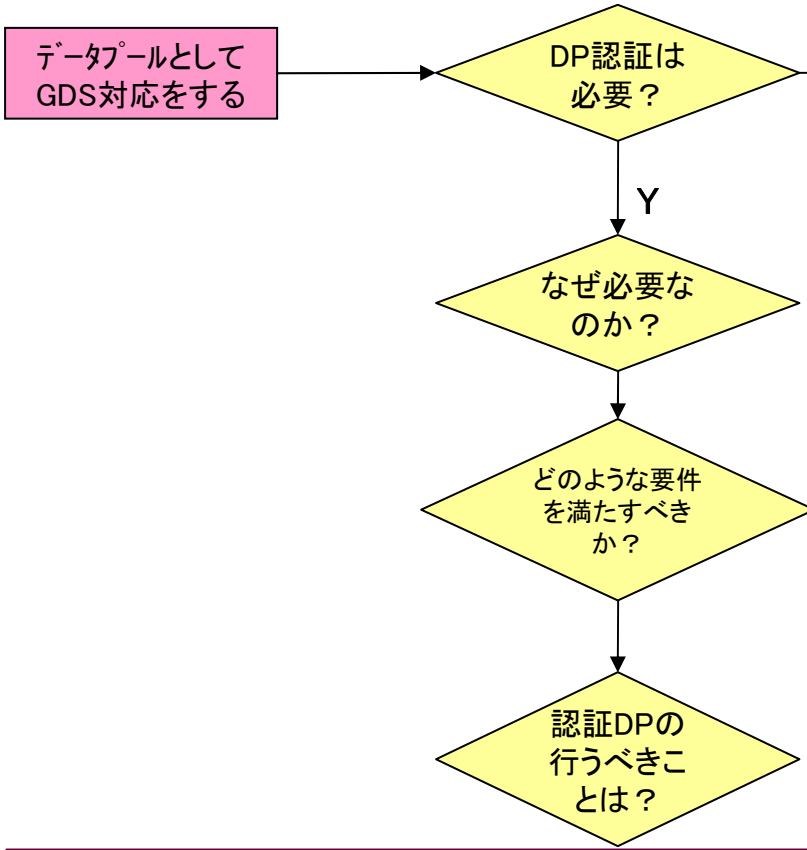
データプール認証検討WGの検討フロー

■ データプール認証定検討WGの検討フロー



データプール認証に関するWGの活動成果①

- 目標成果物：我が国におけるデータプール認定の今後のあり方の検討指針
- データプール認証に関するWGでの検討状況
  - 海外（GS1）で行っているDP認証に関する情報共有実施
  - 日本においてDP認証の必要性について判断するための材料は何かを確認
  - 日本のモデル（ナショナルレジストリにDPを接続）と似ているGS1フランスにおける認証業務を調査



検討すべき内容

・DPの定義づけ
・必要性：DP認証の目的・意義
・DP認証のメリット・デメリット（DP/ユーザーにとって）

各種　必要要件の検討
・業務面　・システム面　・サービスレベル　・セキュリティ
・守るべき義務　（必須機能等）　etc.

・認証DPの持つ権利/負うべき義務
・認証DPにならない商品DB事業者の扱いについて

データプール認証に関するWGの活動成果②

【検討の経過】

■ データプール認証は早い段階で必要である

【理由】

■ GDSプロセス標準に対する相互接続性を担保できないデータプール業者がサービスを開始した場合、GDSN全体の信頼性が揺らぐ可能性がある

■ GDSの業界拡大を進める上でも、信頼性が担保できるデータプール認証業務が必要である

【留意事項】

■ GDSプロセス標準を維持し、認定業務を実施するための機関が必要

■ データプールの負うべき責任と認証内容を明確にすべき

■ 認定業務、GDSプロセス標準の維持のためのコストとその負担モデルの確立が不可欠

＊具体的な、認証手段やデータプール認証の手順は検討の最中のため、4月以降流通システム開発センターのホームページにて公開を予定しています。

データプール認証についての目次（案）

1. データプール認証
   - I. GS1で行っているデータプール認証に関する情報共有
     - i. GS1の組織構造
     - ii. GSMPの組織構造
     - iii. GDSNの財政構造
     - iv. 認証機関
     - v. 認証基準
     - vi. 認証レベル
     - vii. 認証プロセス
     - viii. 認証テストの内容
     - ix. テスト基準
     - x. 認証合格通知
     - xi. データプール認証の取り消し
     - xii. 認証に関する問題
     - xiii. これからの認証業務について
   - II. GS1-Franceで行っているデータプール認証に関する情報共有

2. 日本におけるデータプール認証の必要性
   - i. 日本におけるデータプール認証の目的
   - ii. 日本におけるデータプール認証のメリット・デメリット
   - iii. データプール認証の定義と範囲
   - iv. 日本におけるデータプール認証の今後のあり方の検討指針
   - v. 今後検討すべき課題

本年度の成果の活用方針

本年度の成果の活用方針

- 次年度以降に実装する企業向けに、通信プロトコル・セキュリティの検討成果の活用を予定している。
- 検討成果は、「組織体の運営」「標準の維持」の2つの側面で、2007年度以降の協議会等の活動に引き継がれる予定である。

	組織体の運営	標準の維持	備考
相互セキュリティ基盤に関する検討・認証局構築	**認証局の認定** 認証局の運営業者の認定を左記ガイドラインに沿って認定	**ガイドラインのメンテナンス** 「業界共通認証局構築・運営・利用ガイドライン」のメンテナンス	
通信プロトコル標準化に関する検討		**ガイドラインのメンテナンス** インターネットを利用した通信プロトコルの標準化の検討および、ガイドラインのメンテナンス	