

日本インターネット協会
セキュリティ・フォーラム

IT Solution Innovator **iSiD**

電子認証の新たな国際標準 アイデントラス identrus

2001年3月8日
電通国際情報サービス
e-テクノロジー統括部長
渥美 俊英 atu@isid.co.jp

アジェンダ

- ✓ アイデントラスとは 概要
- ✓ 技術要素、主要ベンダ、製品
- ✓ アプリケーションモデル
- ✓ 動向

会社概要

- ✓ 株式会社電通国際情報サービス
Information Services International - Dentsu, Ltd
- ✓ 設立: 1975年 2000年11月 東証1部上場
- ✓ 主要株主: 電通、GEインフォメーション・サービス



1971年

株式会社電通TSS局としてGEの提供するリモート・コンピューティング・サービスの提供を開始

1975年
電通とGE
のJVとして
iSiD設立

70~80's

日本企業の海外進出を支援する形で、金融業、製造業を中心に約1,000社の利用

80~90's

金融業、製造業、流通・サービス業全般向けにシステム・インテグレーションとアウトソーシングを提供

- 電通グループの一員として、マーケティング面を含むトータルなインターネット・ビジネス支援
- GEグループの一員としてグローバルなシステム・インテグレーション支援

アイデントラス 続々と発表記事

- ✓ 三和銀が電子認証、ネット取引の安全性を保証、欧米銀と規格統一（日経 8/18夕刊）
- ✓ 三和銀、興銀、東京三菱、アイデントラス基盤の新決済サービスを来年中に開始（日経 9/12）
- ✓ 住友・さくら銀も参加、日米欧主要行ネット決済共通仕様でシステム構築（日経金融 9/22）
- ✓ SWIFT 銀行間通信網、電子商取引に開放
アイデントラスと提携（日経1/11 第1面トップ）

アイデントラスとは

- ✓ 世界のトップ銀行37行が出資・参加
- ✓ 本格的B2B市場形成に向けて
- ◆ 取引相手を認証し、信用できるか？
- ✓ 銀行が「信頼できる第3者機関」となり、
e-コマースの基盤システムを支えるのがねらい
- ✓ この仕組みを、アイデントラス社が提供する。
 - 1) そのための、システム仕様を策定し
 - 2) ソフトウェアの相互稼働性を認定し
 - 3) 電子認証のサービス基盤を提供する。



アイデントラスの経過

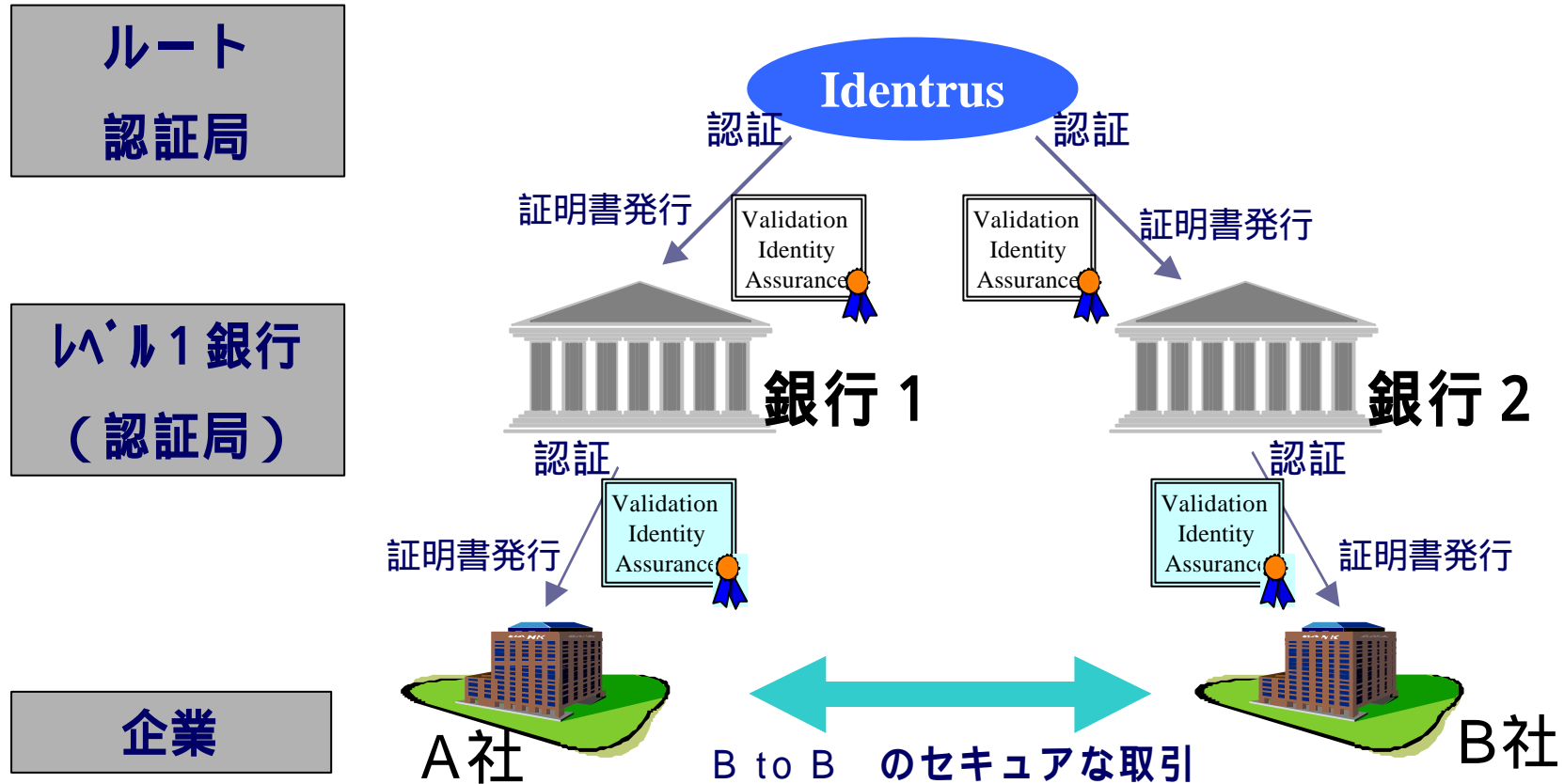
- ✓ 99年春、世界のトップ銀行8行が設立
 - ◆ ABNアムロ、BOA、チェース、シティ、ドイツ銀、バークレー等
 - ◆ 現在37行、三和、興銀、東京三菱、住友/さくら
 - ✓ 00年春、認証局の商用稼動開始
 - ✓ 00年、電子署名取引、決済、の仕様策定
 - ✓ 01年秋には、各銀行の共通システム稼動の予定
- 初の銀行間共通アプリケーション**

Eleanor エレノアペイメント

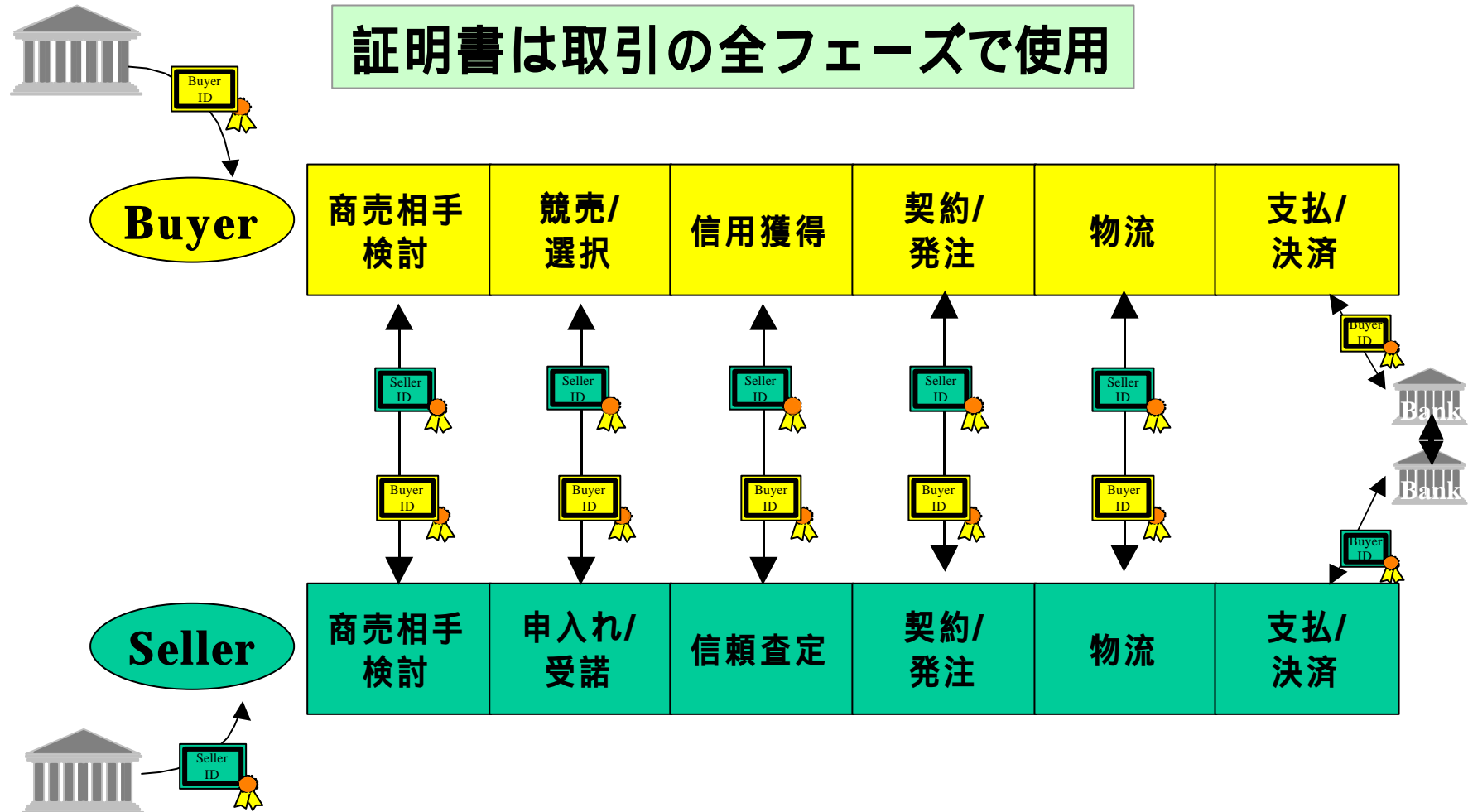
アイデントラスの仕組み

✓ 4 者間電子認証モデル

PKIをベースにしたシステム
全て、インターネット経由



電子商取引と認証

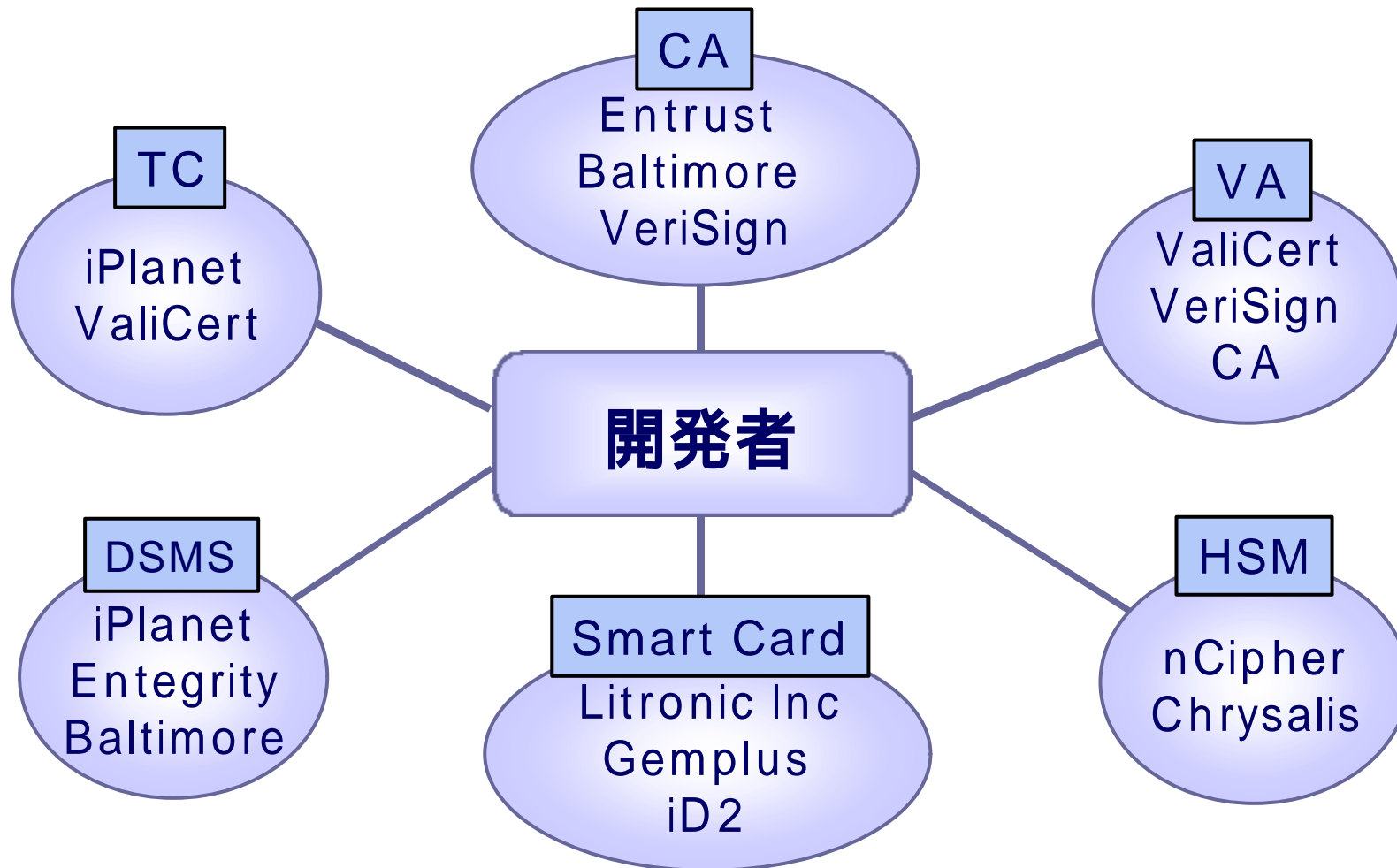


アイデンティティの要素技術

PKI(公開鍵暗号基盤)の厳格な応用

- ✓ CA(Certificate Authority) 認証局/証明書発行管理
- ✓ VA (Validation Authority) 証明書有効性確認
- ✓ TC(Transaction Coordinator) 電子署名電文制御
- ✓ DSMS 電子署名メッセージ管理
- ✓ HSM 秘密鍵の管理ハードウェア
- ✓ ICカード 個人の秘密鍵の管理
- ✓ 署名アプリ ブラウザでの証明書管理、署名

アイデントラス 主要コンポーネント・ベンダ



データの流れ

4者間電子認証モデル

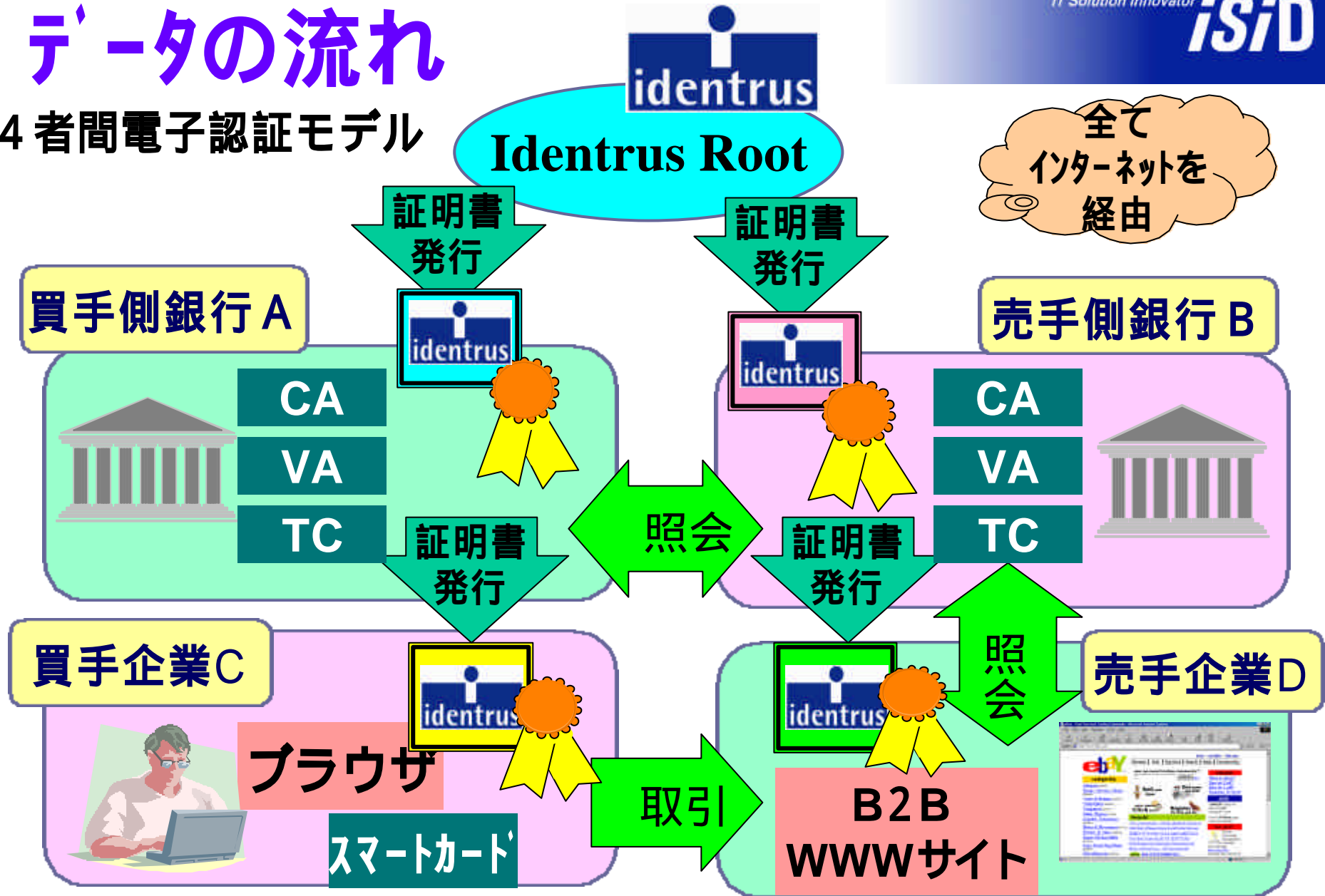


図1 TCの役割

1=注文 2=証明書の照会 3a=自行OCSP
 3b=自行業務 3c=他行OCSP 3d=他行業務

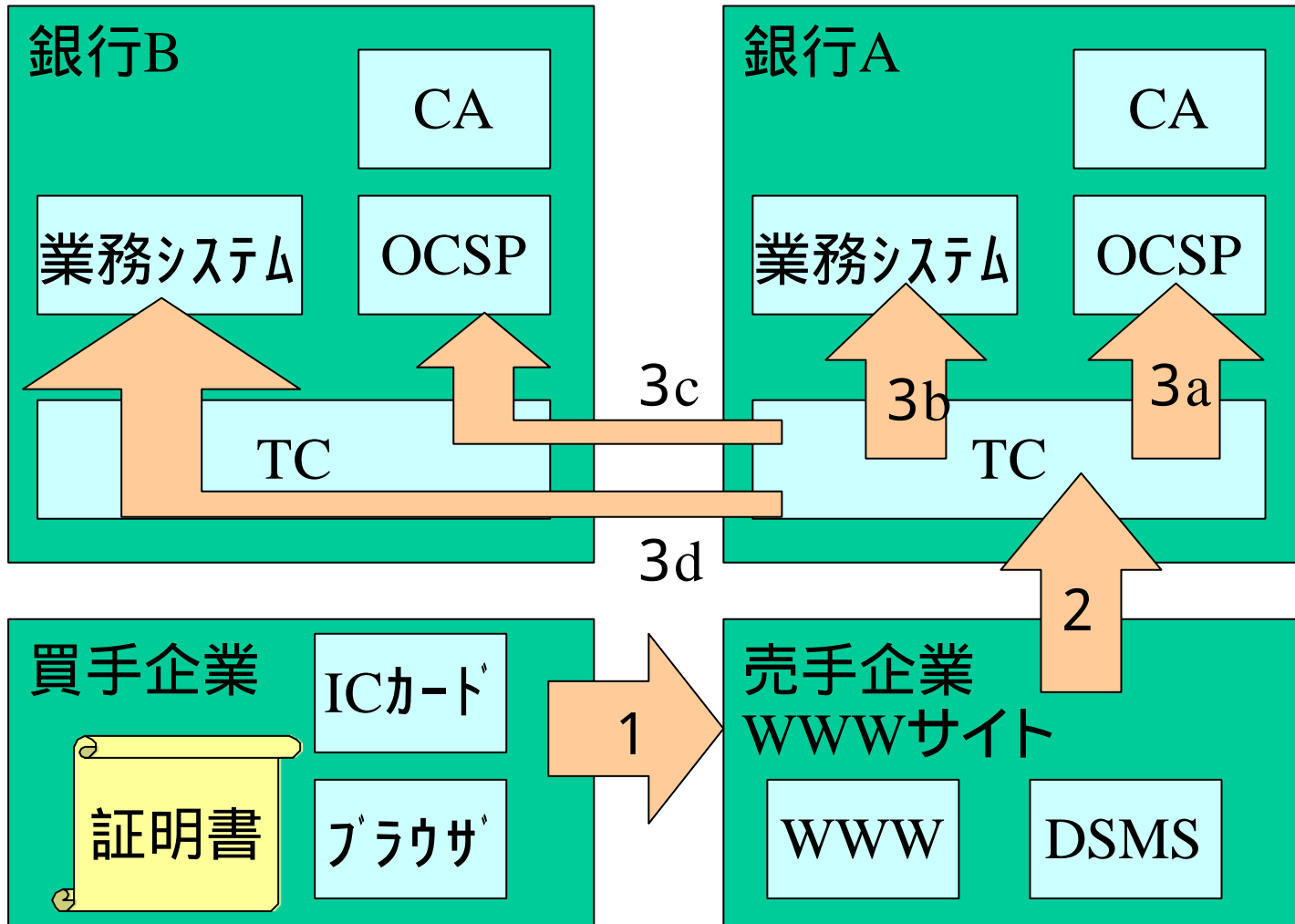
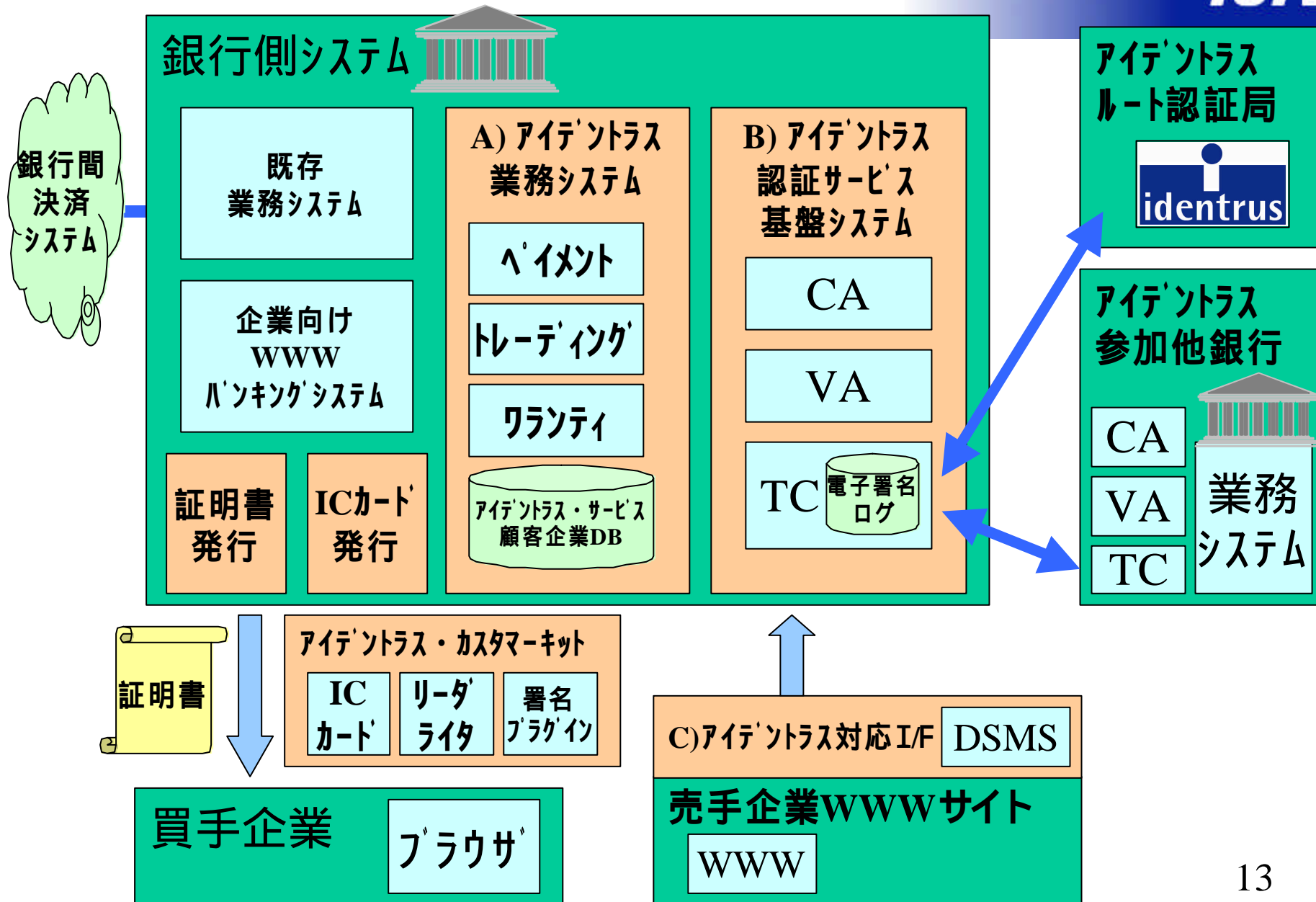


図2 システム構築の実際

アイデントラス対応システムの構築範囲



アイデンティティの 今後の展開と影響

- ✓ 決済、取引、与信の業務/システム仕様確定
 - ◆ XMLベースの世界共通メッセージ仕様
- ✓ 欧米日トップ銀行が、共通アプリケーションを稼動
- ✓ e-マーケットプレイスのアイデンティティ対応
- ✓ B2Bコマースサーバのアイデンティティ対応
- ✓ アプリケーションサーバのアイデンティティ対応

参考資料

掲載雑誌		掲載内容
日経オープンシステム	00/04号	特集「WWWシステムはなぜ遅いのか」
日経オープンシステム	00/07号	特集「止まらないシステムへの挑戦」
インターロップマガジン	00/07号	「ベリサインOnSiteに見るPKIシステムのアウトソース構築」
日経コンピュータ	00/08/28号	特集「Java対COBOL」
日経オープンシステム	00/09号	特集「サーバーサイドJavaの実力を探る」
日経コンピュータ	00/09/25号	特集「大規模ECシステム“超短期開発”の実際」
日経オープンシステム	00/12号	特集「ネット時代を乗り越える、変化に強いシステム構築法」
日経システムプロバイダ	00/12/22号	特集「見えてきたITサービスの次世代人物像」
インターロップマガジン	00/11,12号	「アイデンティティとは何か～新たな電子認証の国際標準」
日経インターネット・テクノロジー	連載	連載「誰も教えてくれなかったセキュリティ対策」
日経コンピュータ	連載	連載「疑問に答えるe-ビジネスのIT」