MIZUHO

Channel to Discovery

IC・IDカードの相互運用可能性の向上に係る基礎調査
「ニーズ編」

～IC・IDカードを巡るニーズのギャップについて～

みずほ情報総研株式会社

出口　太郎

発表内容

1. IC・IDカードシステムの概要
2. 調査概要
3. IC・IDカードの相互運用へのニーズ
4. 国内のIC・IDカードの現状
5. 各プレーヤの現状とニーズ
6. 標準化が進まない背景
7. 危惧される事態と影響
8. あるべき標準化の姿

注：この資料は独立行政法人情報処理推進機構(IPA)の「IC・IDカードの相互運用可能性の向上に係る基礎調査」結果に基づいて作成されています。

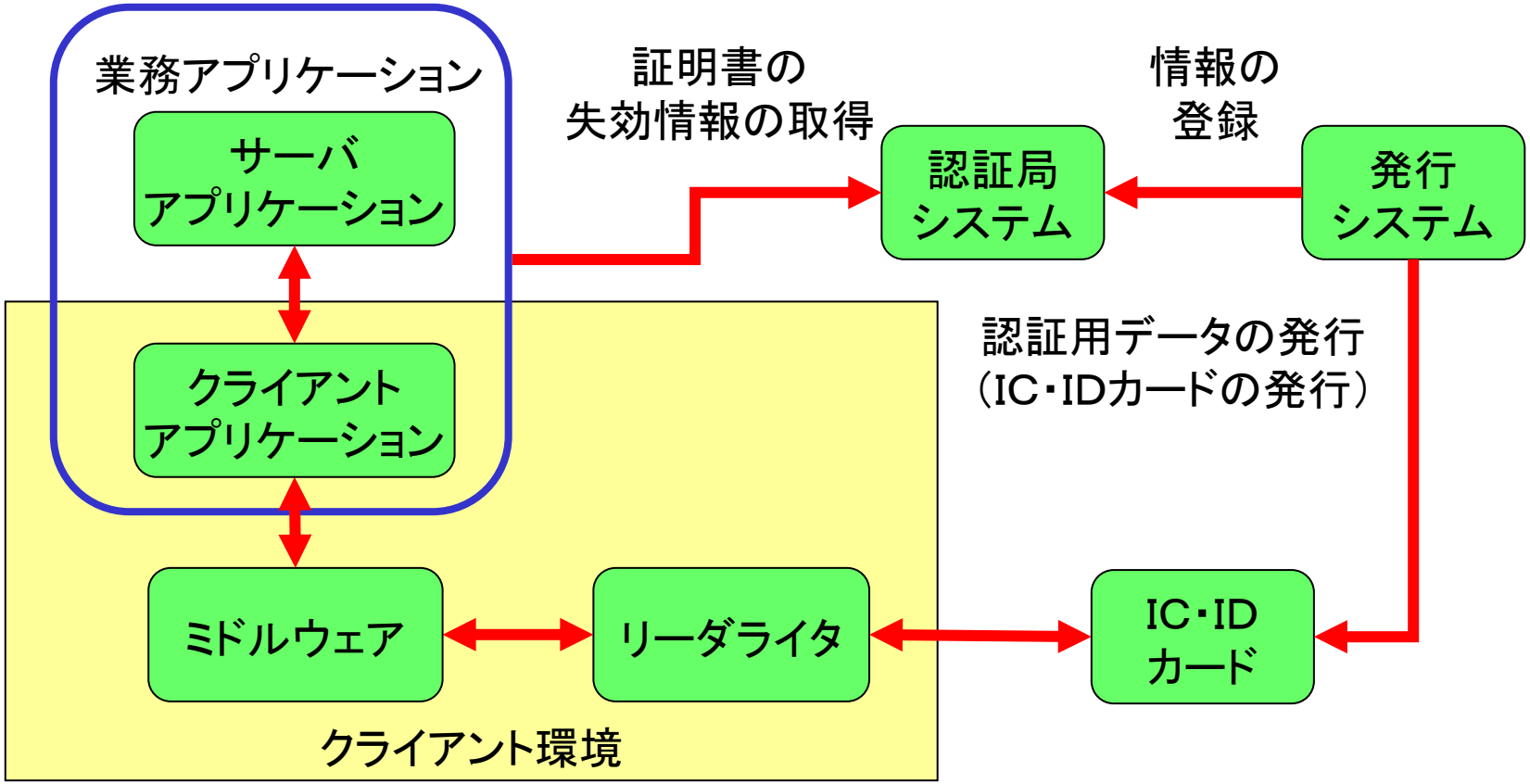
1．IC・IDカードシステムの概要

(1) IC・IDカードシステムの構成

(2) プレーヤと役割

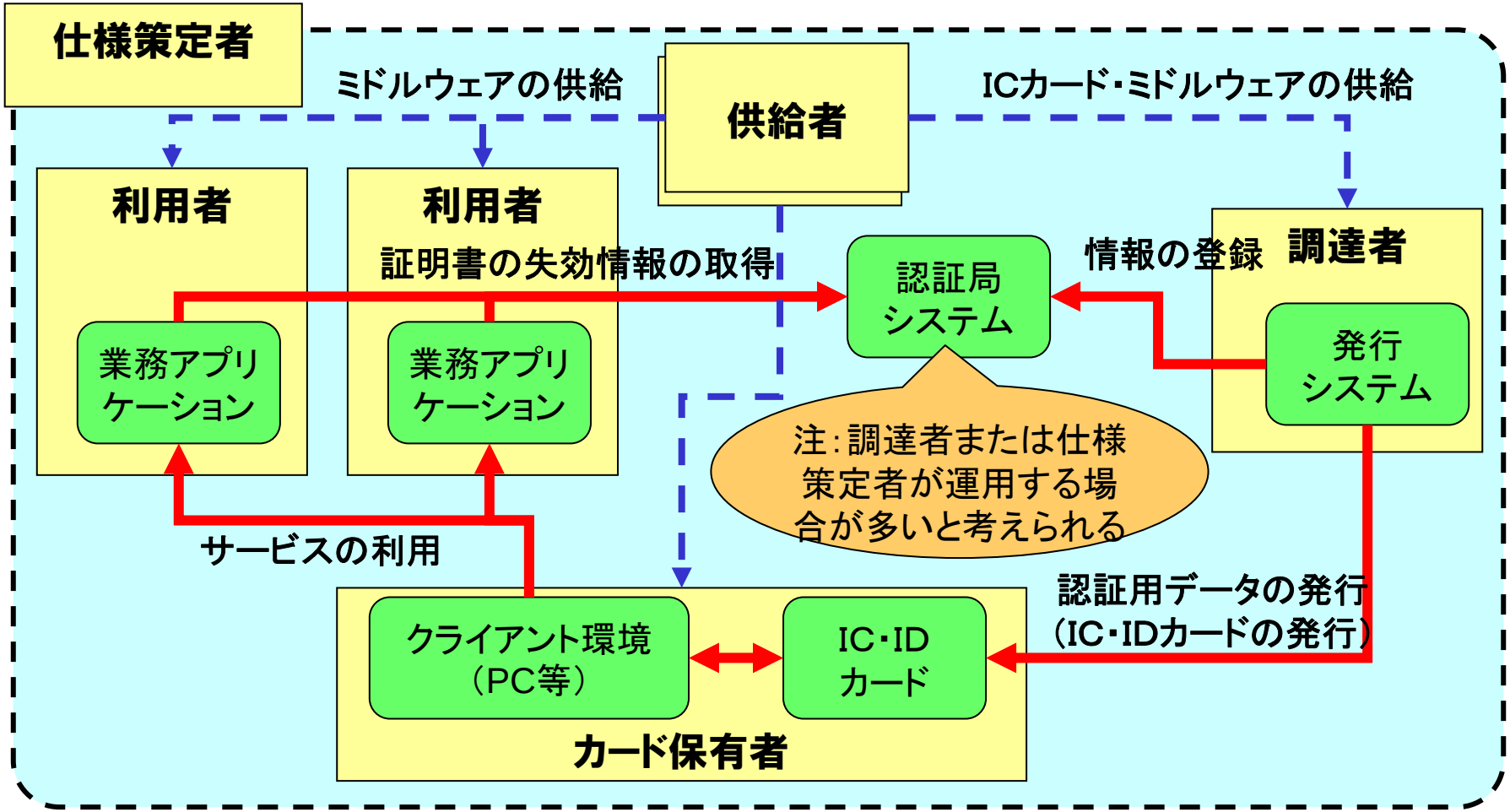
(3) クライアントシステムの構成

(1) IC・IDカードシステムの構成



注:この資料は独立行政法人情報処理推進機構(IPA)の「IC・IDカードの相互運用可能性の向上に係る基礎調査」結果に基づいて作成されています。

(2) プレーヤと役割



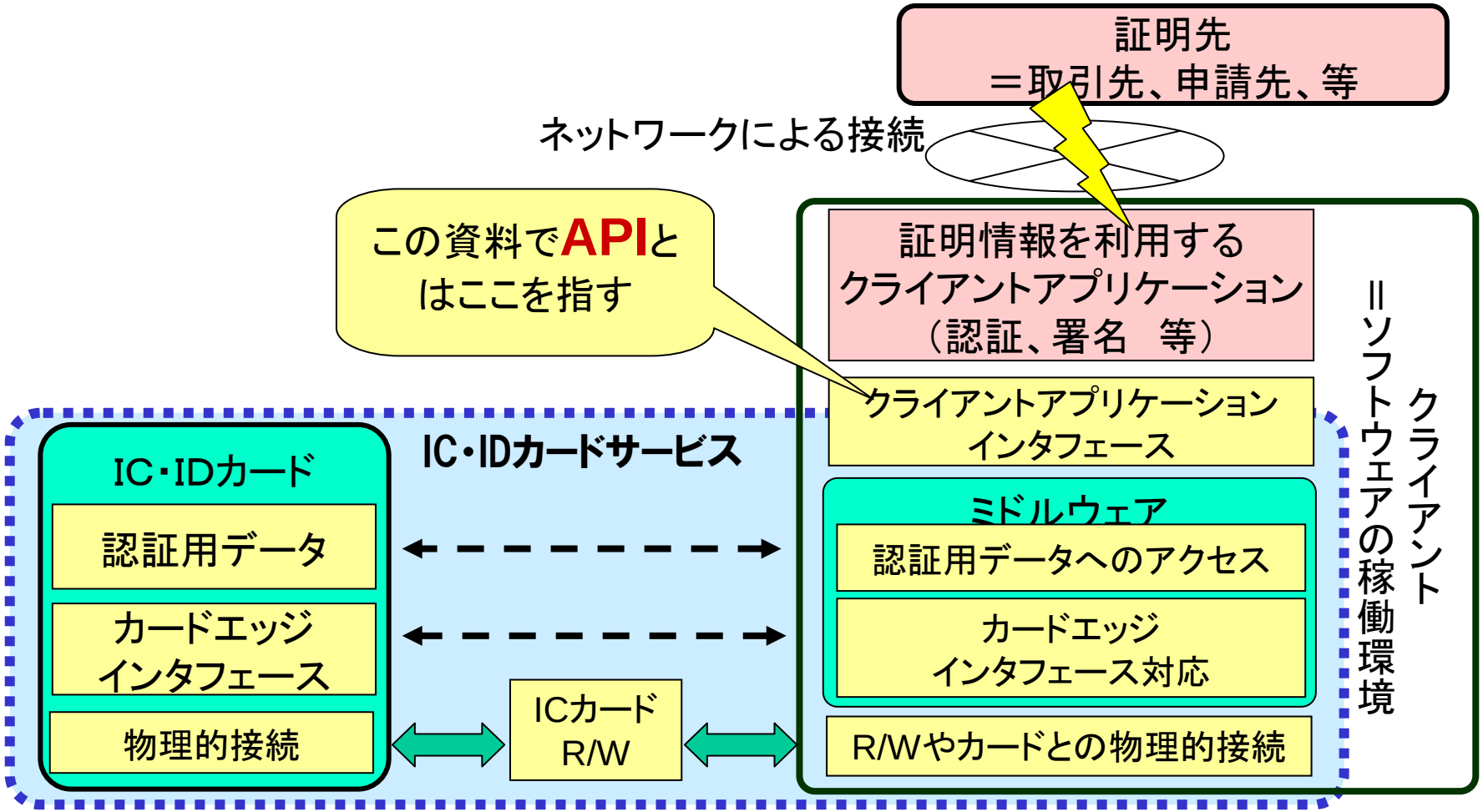
注：この資料は独立行政法人情報処理推進機構(IPA)の「IC・IDカードの相互運用可能性の向上に係る基礎調査」結果に基づいて作成されています。

(2) プレーヤと役割

関係者	主な役割
仕様策定者	当該サービスにおけるICカードの仕様を策定する
調達者	策定された仕様に沿ってICカードの調達を行い、カード保有者向けにICカードを発行する
利用者	また、カード発行時に鍵ペアの発行とICカードへの認証用データの登録を行う
カード保有者	調達者が調達したIC・IDカードを持つカード保有者に対して、IC・IDカードの認証用データを利用したサービスを提供する
供給者	IC・IDカードの発行を受け、サービスを利用する

注:この資料は独立行政法人情報処理推進機構(IPA)の「IC・IDカードの相互運用可能性の向上に係る基礎調査」結果に基づいて作成されています。

(3) クライアントシステムの構成



注：この資料は独立行政法人情報処理推進機構(IPA)の「IC・IDカードの相互運用可能性の向上に係る基礎調査」結果に基づいて作成されています。

2. 調査概要

(1)インタビュー調査の概要

(2) インタビュー調査対象のIC・IDカード

(3) 報告書の構成

(1)インタビュー調査の概要

- 2006年8月～11月　述べ13回のインタビュー調査
- 関係者へのヒアリングを実施
  - 仕様策定者 （7者）
  - 調達者 （4者）
  - 利用者 （4者）
  - 供給者　 （4者）
  - 国際標準化関係者 （2者）

※複数の立場からの回答を頂いているインタビュー先多数

注：この資料は独立行政法人情報処理推進機構(IPA)の「IC・IDカードの相互運用可能性の向上に係る基礎調査」結果に基づいて作成されています。

(2) インタビュー調査対象のIC・IDカード

- 公的個人認証
- 国家公務員ICカード
- 電子入札コアシステム
- 国立大学における認証基盤
- ヘルスケアPKI

注:この資料は独立行政法人情報処理推進機構(IPA)の「IC・IDカードの相互運用可能性の向上に係る基礎調査」結果に基づいて作成されています。

(3) 報告書の構成

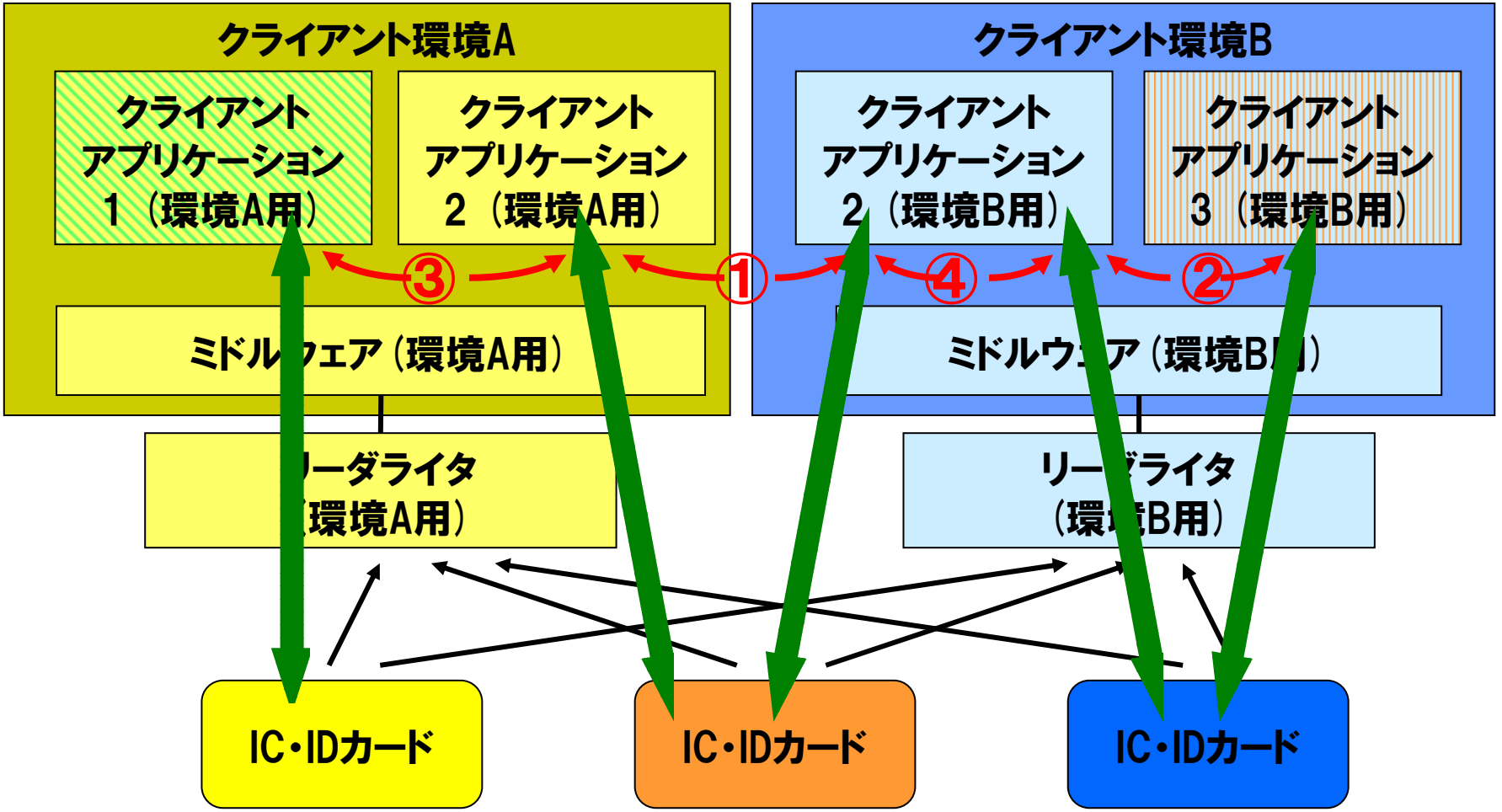
- IC・IDカードシステムの概要(2章)
- IC・IDカードの相互運用可能性に関するニーズ(3章)
- 標準化の動向(4章)
- 国内でのIC・IDカードの導入動向(5章)
- IC・IDカードの相互運用可能性に関する課題(6章)
- IC・IDカードの標準化及び普及に向けた提言(7章)

注:この資料は独立行政法人情報処理推進機構(IPA)の「IC・IDカードの相互運用可能性の向上に係る基礎調査」結果に基づいて作成されています。

3. IC・IDカードの相互運用へのニーズ

(1) 全体概要
(2) ケース①　異なるクライアント環境での利用
(3) ケース②　1枚のカードの複数用途への利用
(4) ケース③　複数のカードとアプリケーション
(5) ケース④　1アプリケーションに複数のカード

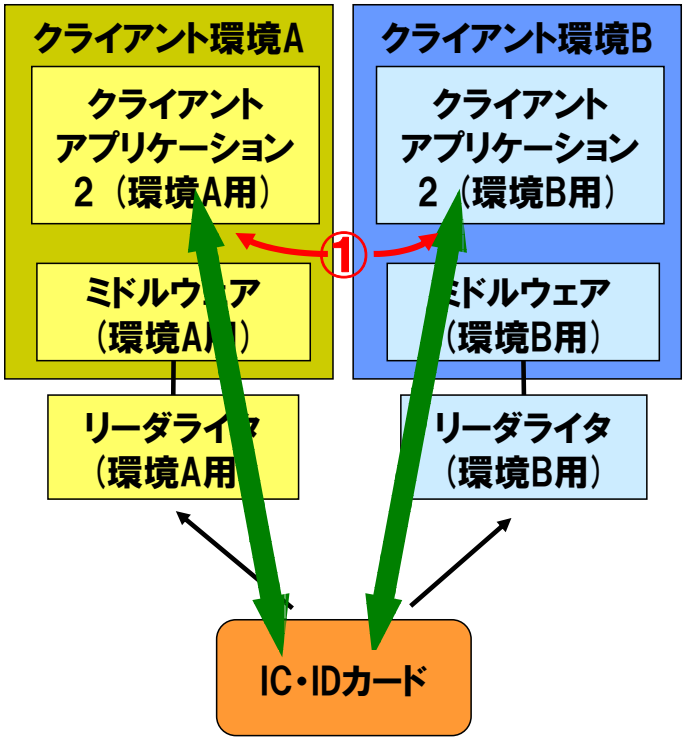
(1) 全体概要



注：この資料は独立行政法人情報処理推進機構(IPA)の「IC・IDカードの相互運用可能性の向上に係る基礎調査」結果に基づいて作成されています。

(2) ケース①　異なるクライアント環境での利用

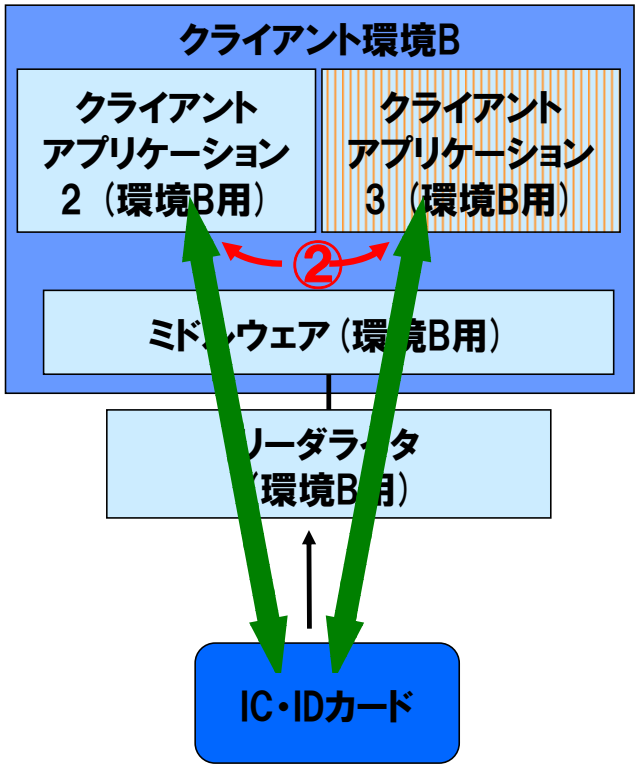
- 複数種のクライアントOS、さまざまなバージョンが混在
  - 大学などの研究環境で、研究環境、研究資源への接続時の認証に
  - 医療機関で電子カルテシステムやレセプトシステムとの連動で
  - 個人の自宅から、日常的に利用しているパソコンで利用される場合



注：この資料は独立行政法人情報処理推進機構(IPA)の「IC・IDカードの相互運用可能性の向上に係る基礎調査」結果に基づいて作成されています。

(3) ケース②　1枚のカードの複数用途への利用

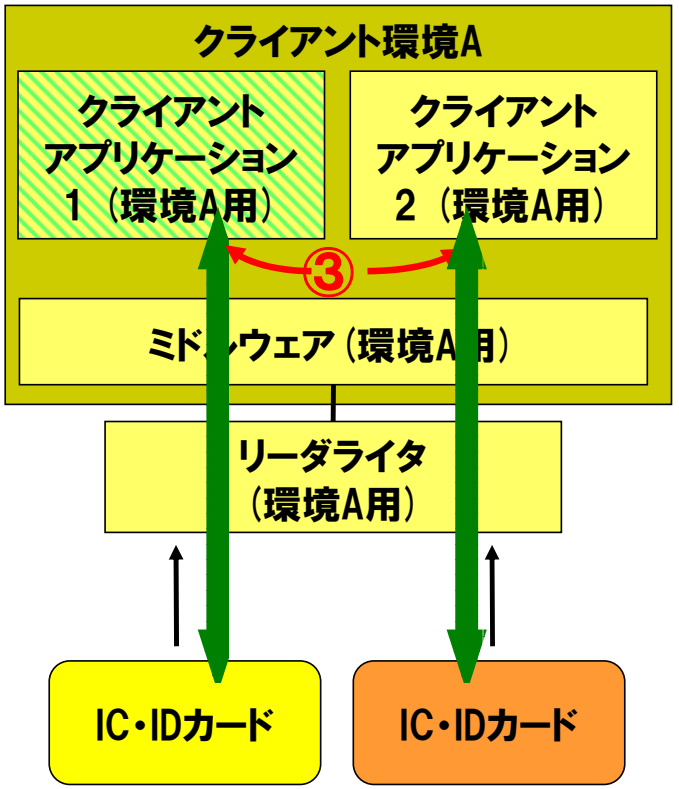
- 1枚のIC・IDカードを新たな業務アプリケーションにも利用
  - 電子入札システム用ICカードで他の行政機関の電子調達や電子申告を行いたい
  - 研究機関の内部で利用者認証に使っているIC・IDカードで、他の研究機関との共同研究でも利用者認証に使いたい



注：この資料は独立行政法人情報処理推進機構(IPA)の「IC・IDカードの相互運用可能性の向上に係る基礎調査」結果に基づいて作成されています。

(4) ケース③　複数のカードとアプリケーション

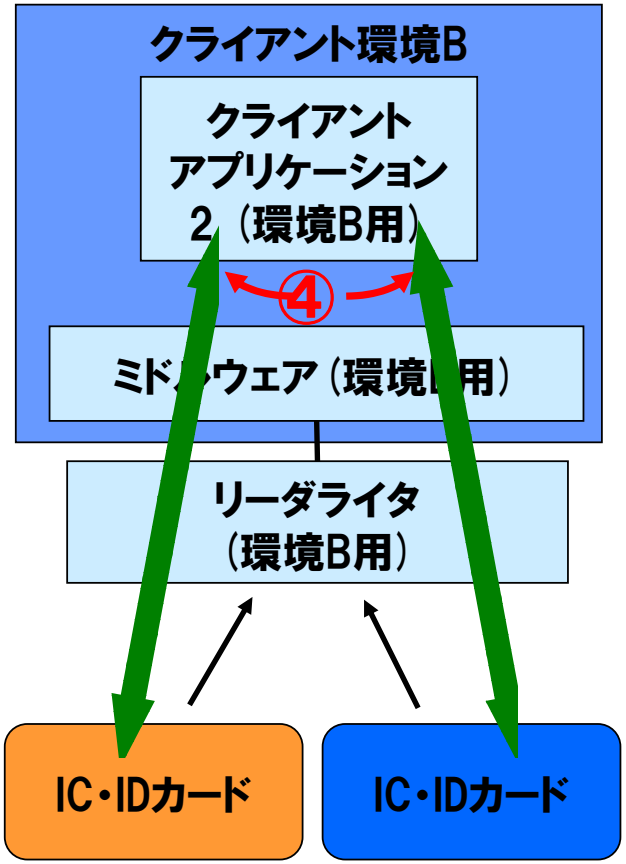
- 複数種のIC・IDカードを用途に応じて使い分ける
  - 営業担当者が入札を行うクライアントで、会計担当者の電子申告や技術担当者の資格に基づく業務を行う
  - 医療機関で電子紹介状を扱うクライアントで電子申告も実施



注：この資料は独立行政法人情報処理推進機構(IPA)の「IC・IDカードの相互運用可能性の向上に係る基礎調査」結果に基づいて作成されています。

(5) ケース④　1アプリケーションに複数のカード

- 複数種のIC・IDカードを利用
  - 別々の発行者が発行した医師が勤務する病院
  - 長期間利用される間にカードのバージョンアップや調達先の変更が発生
  - 行政書士等の代理申請
  - 医師が紹介状と患者のカード提示による同意に基づいて紹介医師の電子カルテにアクセス



注：この資料は独立行政法人情報処理推進機構(IPA)の「IC・IDカードの相互運用可能性の向上に係る基礎調査」結果に基づいて作成されています。

4. 国内のIC・IDカードの現状

(1) 国際標準の限界

(2) 事例での相互運用への配慮

(3)事例での標準化と公開の現状

(1) 国際標準の限界

		ISO/IEC 7816シリーズ	ISO/IEC 24727シリーズ	PKCS#11
カードエッジインタフェース	物理的接続	明確に規定。相互運用可能性〇	ISO/IEC 7816及び14443を参照	規定せず
	コマンド	実装は基本的にオプション。相互運用可能性△	左記からコマンドを抽出・定義　相互運用可能性〇	規定せず
データモデル		標準を定義もオプション多くコマンドも限定されず。相互運用可能性△	規定せず	規定せず
クライアントアプリケーションインタフェース		規定せず	汎用の関数を定義もIC・IDカードにはやや不足。相互運用可能性△	認証用データを扱う機能群の関数を詳細に定義。相互運用可能性〇

注：この資料は独立行政法人情報処理推進機構(IPA)の「IC・IDカードの相互運用可能性の向上に係る基礎調査」結果に基づいて作成されています。

(2) 事例での相互運用への配慮

	公的個人認証	国家公務員（PKIなし）	電子入札コア	国立大学	HPKI (整備中)
(1)複数クライアント環境	△Mac対応は遅れているが整備中	×調達府省次第として考慮せず	×Windowsに限定	△Mac OSは一部のみ対応	○WindowsとLinux双方へ対応必須
(2)1枚を複数用途	○APIを公開して幅広い行政手続きに利用	△カードにアプリケーションを追加可能	×APIを認証業者のみ公開、他業務考慮せず	○学内での認証インフラとしてAPIを整備	△将来に向け様々な用途を念頭にAPIを検討
(3)1環境で複数カード・用途	×考慮していない	×考慮していない	×考慮していない	×カードを発行しなおし	△電子申請等との共存か
(4)1環境に複数種のカード	○複数市町村のカードを利用	△入退館は全府省カードに対応必須	×考慮していない	×考慮していない	○患者カードとの組合せを検討

注：この資料は独立行政法人情報処理推進機構(IPA)の「IC・IDカードの相互運用可能性の向上に係る基礎調査」結果に基づいて作成されています。

(3)事例での標準化と公開の現状

	公的個人認証	国家公務員(PKIなし)	電子入札コア	国立大学	HPKI(整備中)
アプリケーション開発	○行政機関が任意に可	△府省ごと自由に可	×コアシステム専用	○各種を接続予定	△各種を想定し検討中
API	○複数種を公開(PKCS# 11, CSP 等)	△入退管理のみ統一。非公開	△統一されているが非公開	○整備(PKCS #11, CSP)	△公開あるいは開示の見通し
ミドルウェア機能	△統一されているが非公開	△入退管理のみ統一	×認証局別カードとセット	×ベンダ独自仕様	△認証局別に検討中
リーダライタ IF	△統一されているが非公開	△入退管理のみ統一	×認証局別カードとセット	×ベンダ独自仕様	△認証局別に検討中
カードエッジ IF	△統一されているが非公開	△入退管理のみ統一	×認証局別カードとセット	×ベンダ独自仕様	○ガイドライン検討中

注:この資料は独立行政法人情報処理推進機構(IPA)の「IC・IDカードの相互運用可能性の向上に係る基礎調査」結果に基づいて作成されています。

5. 各プレーヤの現状とニーズ

(1) 仕様策定者

(2) 調達者

(3) 利用者

(4) 供給者

(1) 仕様策定者

- 公共分野でもサービス個別の仕様策定
  - 公共、民間を問わず幅広く活用させる意図はない
  - 類似の分野でも公開を通じた標準化はされていない
  - 個別に策定したIC・IDカードの仕様は一般には開示しない
- 複数企業から調達可能な公開仕様が存在しない
  - 実現するサービスのために自ら仕様策定が必要
  - セキュリティ構造の明確化ができないと「全面非公開」
  - 相互運用が不要ならば「ベンダ任せ」でも困らない

注:この資料は独立行政法人情報処理推進機構(IPA)の「IC・IDカードの相互運用可能性の向上に係る基礎調査」結果に基づいて作成されています。

(2) 調達者

- IC・IDカードの調達先は限定されることが多い
  - 仕様が個別策定かつ非公開
  - 仕様策定時の参加者が有利に
- ICカードとミドルウェアはセットで調達する必要がある
  - 利用できるクライアントOSが限定される
  - クライアントに複数のミドルウェアが共存できない場合も
    - 保有者に他社製IC・IDカードを共用しないよう求める必要が生じる
    - 別のベンダからIC・IDカードを調達したら、ミドルウェアとIC・IDカード全て交換が必要な場合がある

注:この資料は独立行政法人情報処理推進機構(IPA)の「IC・IDカードの相互運用可能性の向上に係る基礎調査」結果に基づいて作成されています。

(3) 利用者

- ベンダ固定でも短期的には困らないケースが大半
  - アプリケーションプログラムだけ考えればAPI以下は「IC・IDカードサービス」としてブラックボックス化も可
  - サービス提供対象が固定的ならば対象のIC・IDカードも固定的に考えればよい
- 長期的には困るケースが生じる
  - サービス追加時／対応IC・IDカードの変更・追加時／サービス対象者を広げたい時／．．．

注：この資料は独立行政法人情報処理推進機構(IPA)の「IC・IDカードの相互運用可能性の向上に係る基礎調査」結果に基づいて作成されています。

(4) 供給者

- IC・IDカードはニーズ少ない
  - プライベート用途ならPKIはいらない
  - せいぜいSSLのクライアント認証
- 相互運用よりも独自製品としての最適化を優先
  - ミドルウェア仕様やカードエッジインタフェースは非公開
  - APIをPKCI#11やCSP対応にして汎用性を高める
  - 最低限の機能、限定的な利用環境に絞り込む
  - 制限の大きなリソースで性能と価格の維持を図る
  - 国際標準同様の機能でも、独自コマンドもある

注:この資料は独立行政法人情報処理推進機構(IPA)の「IC・IDカードの相互運用可能性の向上に係る基礎調査」結果に基づいて作成されています。

6. 標準化が進まない背景

(1) 仕様策定及び調達の視点

(2) 製品供給の視点

(3) 構造的背景

(1) 仕様策定及び調達の視点

- 相互運用可能性を確保できる調達仕様が存在しない
  - 国際標準に丸ごと対応する製品は存在しない
  - 実績のあるICカードは多くがミドルウェア一体で仕様非公開
- 相互運用へのニーズ・モチベーションが低い
  - 公共分野の仕様策定者、調達者でも、仕様を公開して幅広く普及させる意図を持っておらず、非開示が通例
- ベンダ間相互運用を求めるサービスの規模が小さい
  - 相互運用の問題は「局地的問題」として対処されている

注:この資料は独立行政法人情報処理推進機構(IPA)の「IC・IDカードの相互運用可能性の向上に係る基礎調査」結果に基づいて作成されています。

(2) 製品供給の視点

- 相互運用可能性は既得市場喪失の脅威
  - アプリケーションとのセットに他社が参入する余地ができる
- 技術的難易度が高い
  - 他社製品との通信を保証するのは容易ではない
- 市場規模が小さい
  - 数万枚の規模では新製品の市場としては小さい
- 相互運用タイプの処理性能の向上が遅れ気味
  - ユーザの性能向上ニーズに供給の多い個別仕様で対応

注:この資料は独立行政法人情報処理推進機構(IPA)の「IC・IDカードの相互運用可能性の向上に係る基礎調査」結果に基づいて作成されています。

(3) 構造的背景

- 分野別での情報化の推進
  - 公的個人認証、法人登記、電子調達等が個別に整備
  - PKIを利用した認証のしくみについて、省庁横断的な技術体系、仕様体系の整理が行われてこなかった
- 垂直統合的な供給体制
  - アプリケーション・ミドルウェア・カード・リーダライタのセットを一貫した製品として供給
  - セット製品としてのメンテナンス性は高い
  - 独自仕様で他の製品との連係は考慮されない

注:この資料は独立行政法人情報処理推進機構(IPA)の「IC・IDカードの相互運用可能性の向上に係る基礎調査」結果に基づいて作成されています。

7. 危惧される事態と影響

(1)異なるクライアント環境で利用できない

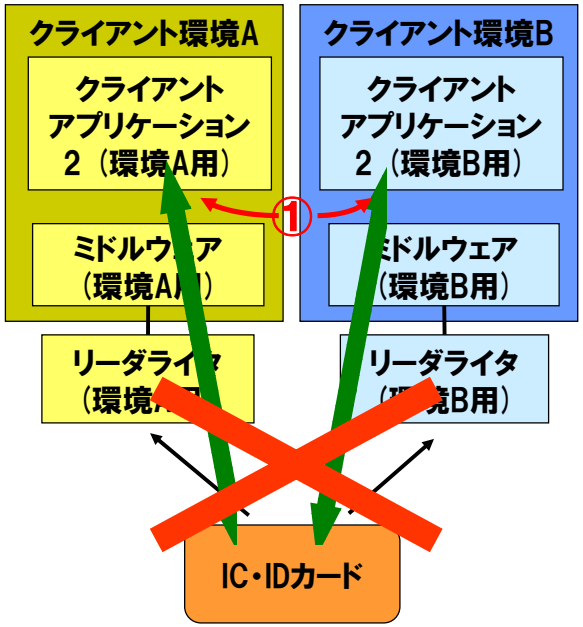
(2) 1枚のカードが複数用途に利用できない

(3) 別のIC・IDカードとアプリケーションが使えない

(4) 別のIC・IDカードが組み合わせられない

(1)異なるクライアント環境で利用できない

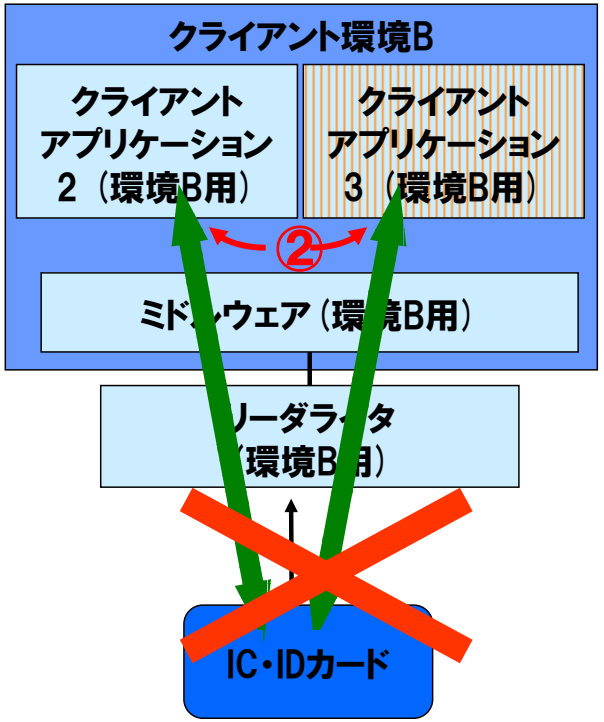
- カードベンダがサポートするOSでしか使えない
  - IC・IDカード用にPCを購入しなければならない
  - クライアントPCを買い換えるとIC・IDカードも新たに購入する必要が生じる
  - PCのOSバージョンアップ時に古いPCを使いつづける必要性



注：この資料は独立行政法人情報処理推進機構(IPA)の「IC・IDカードの相互運用可能性の向上に係る基礎調査」結果に基づいて作成されています。

(2) 1枚のカードが複数用途に利用できない

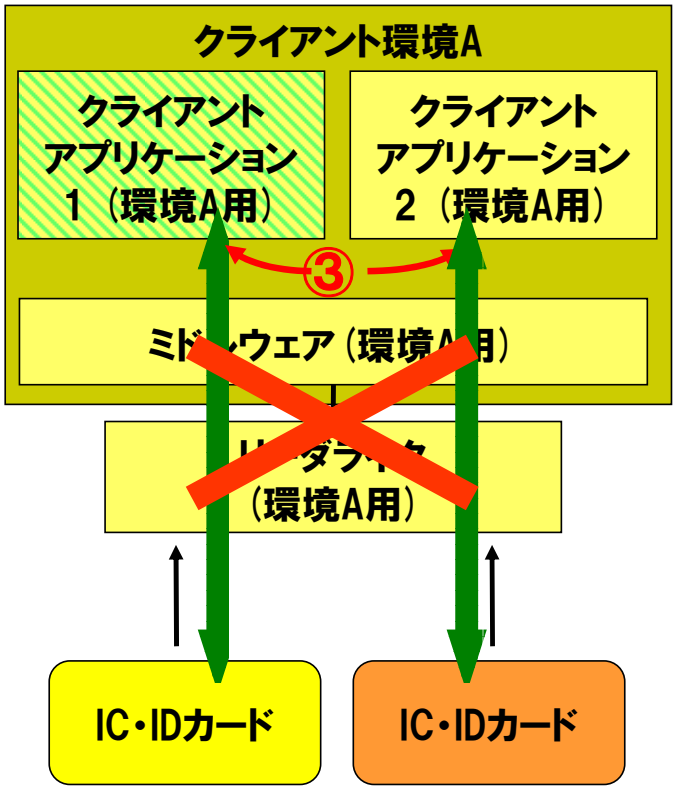
- IC・IDカードがあるのに別のサービスに使えない
  - APIが非公開で接続できない
  - データモデルが異なり認証できない
  - *IC・IDカード以外のミドルウェアが競合(ex. JREバージョン)*
- 追加アプリの開発先が限定の危惧
  - 非公開のミドルウェアを利用できる先が事実上限定されるケースも



注:この資料は独立行政法人情報処理推進機構(IPA)の「IC・IDカードの相互運用可能性の向上に係る基礎調査」結果に基づいて作成されています。

(3) 別のIC・IDカードとアプリケーションが使えない

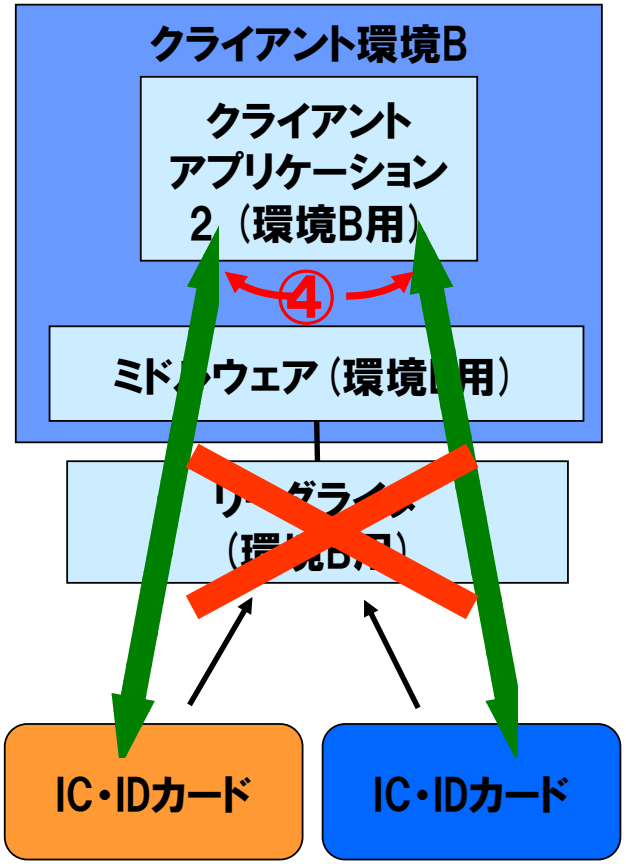
- 1台のクライアントで2種のカードが使えない
  - カードごとにミドルウェアが異なる
  - 複数のミドルウェアが1台のクライアントPCに共存できない
- サービス別にPCを買わなければならない



注：この資料は独立行政法人情報処理推進機構(IPA)の「IC・IDカードの相互運用可能性の向上に係る基礎調査」結果に基づいて作成されています。

(4) 別のIC・IDカードが組み合わせられない

- 新たに適用が求められるIC・IDカードに迅速に対応できない
  - アプリケーション側に開発費が発生
  - ミドルウェアの共存に費用が発生
- 発行するカードの変更で発行済みカード、リーダライタの総入替が必要になるケースも



注：この資料は独立行政法人情報処理推進機構(IPA)の「IC・IDカードの相互運用可能性の向上に係る基礎調査」結果に基づいて作成されています。

ここまでのまとめ

- IC・IDカードの相互運用ニーズは顕在化しつつある
  - 個別の「PKI用カード」からネットワーク上の「IDカード」へ
  - 「どこからでもつながる」「何にでも使える」
- 国内ではIC・IDカードの相互運用が進む環境にない
  - 個別に仕様を策定し、非公開で運営
  - ミドルウェア、リーダライタ、IC・IDカードをセットで提供
  - 国際標準だけでは相互運用できない
- このままでは「IC・ID」カードは普及しない
  - 個別サービスだけ見れば、標準化・公開されなくても短期的には困らない
  - 長期的には利用者ニーズを削ぎ普及を阻害する

注：この資料は独立行政法人情報処理推進機構(IPA)の「IC・IDカードの相互運用可能性の向上に係る基礎調査」結果に基づいて作成されています。

8. あるべき標準化の姿

(1) 相互運用に必要な状況

(2) 支援環境整備の概要

(3) 機能及びセキュリティ構造の定義

(4) 実装規約

(5) 参照実装及びテスト環境

(6) 製品認定の仕組み

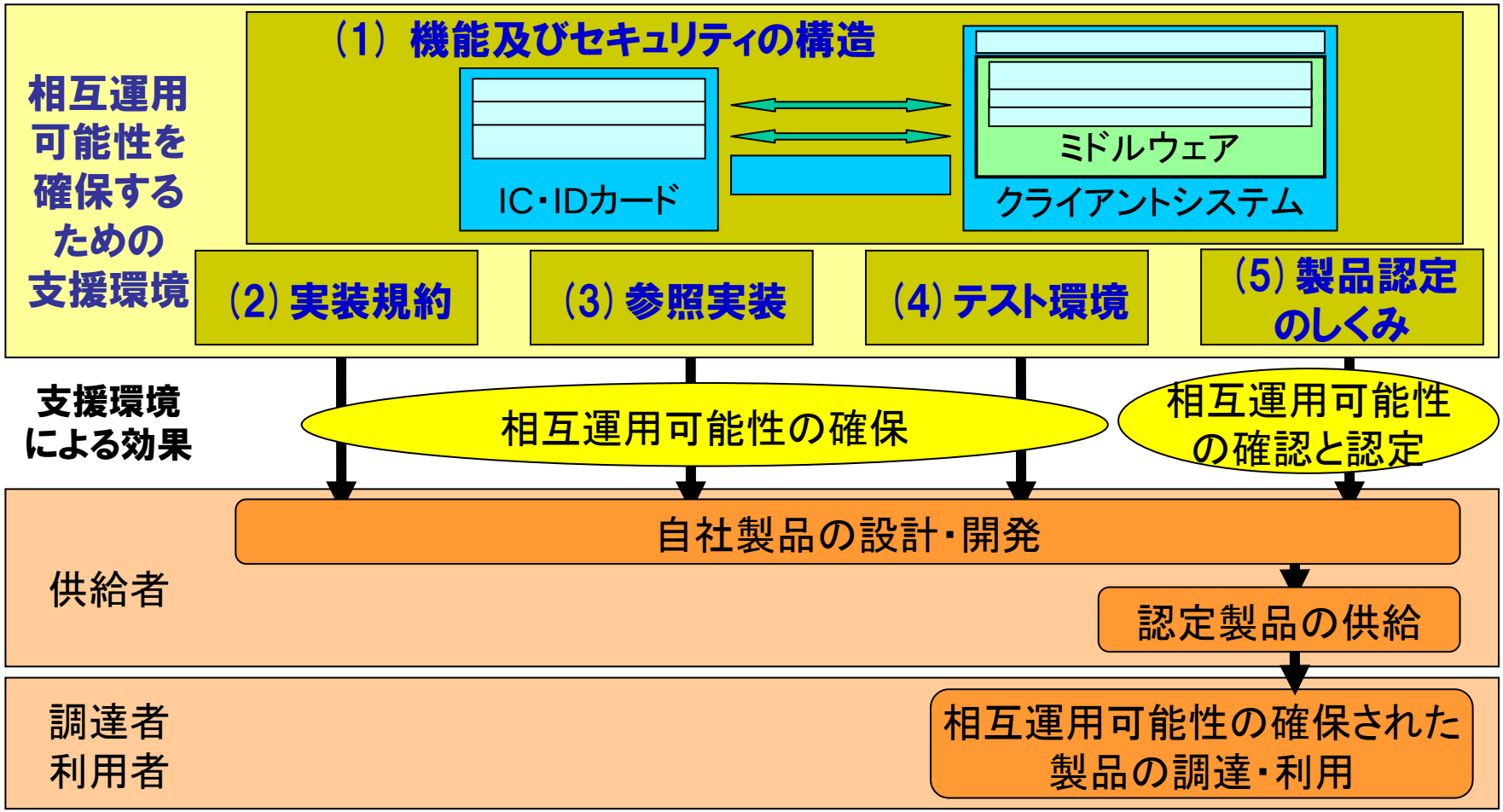
(7) 環境整備の進め方(案)

(1) 相互運用に必要な状況

- ユーザの視点
  - 仕様書に利用可能な一般的な仕様が整備されていること
  - 個別の要素ごとに導入可能であること
    (カードのみ／ミドルウェアのみ／リーダライタのみ)
  - クライアント環境の変化に対応できること
  - 相互運用可能性が保障された製品が調達できること
- ベンダの視点
  - 市場規模の明確化
  - 製品に対する責任範囲の明確化
  - 製品認定コストの軽減

注:この資料は独立行政法人情報処理推進機構(IPA)の「IC・IDカードの相互運用可能性の向上に係る基礎調査」結果に基づいて作成されています。

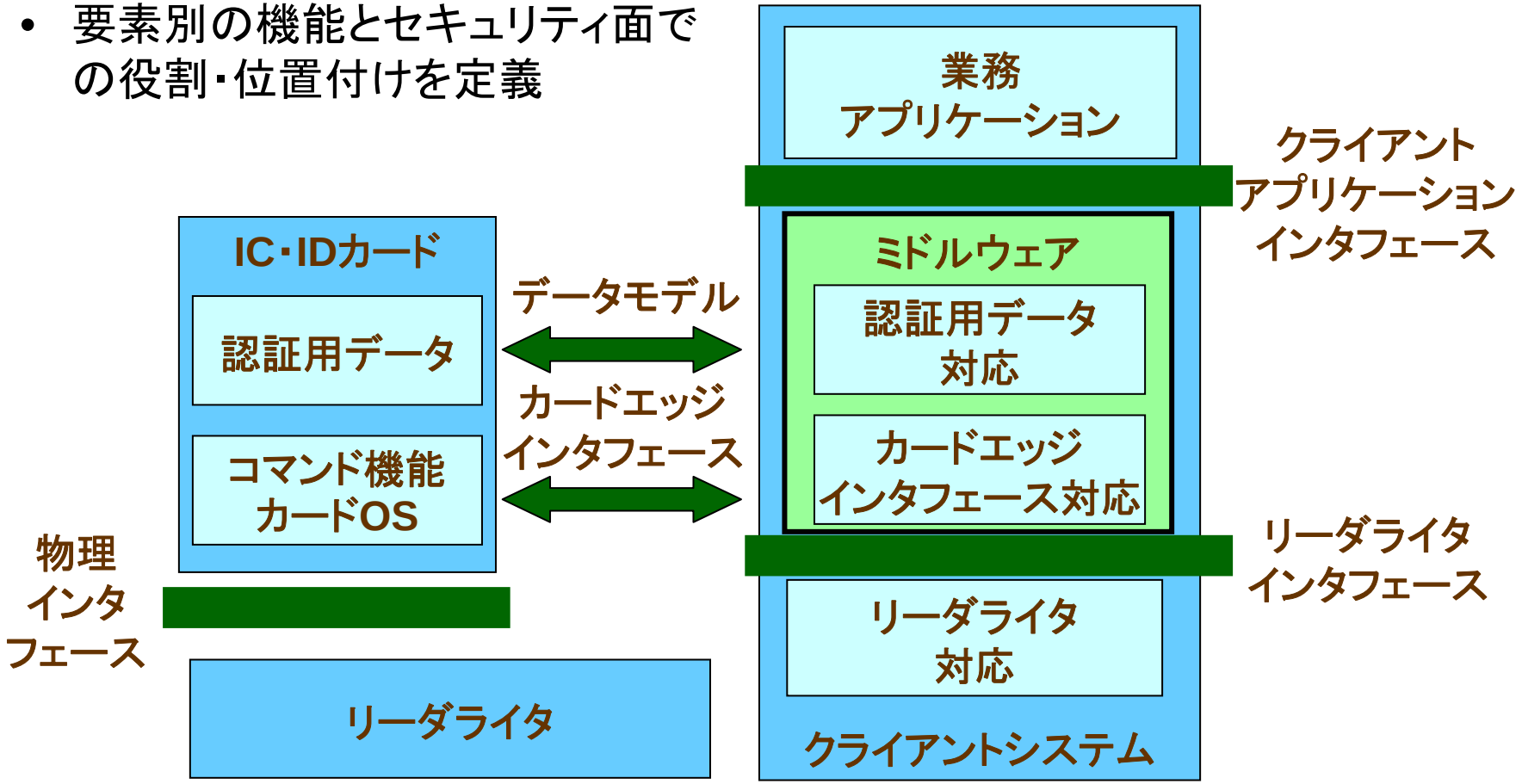
(2) 支援環境整備の概要



注:この資料は独立行政法人情報処理推進機構(IPA)の「IC・IDカードの相互運用可能性の向上に係る基礎調査」結果に基づいて作成されています。

(3) 機能及びセキュリティ構造の定義

- 要素別の機能とセキュリティ面での役割・位置付けを定義



注:この資料は独立行政法人情報処理推進機構(IPA)の「IC・IDカードの相互運用可能性の向上に係る基礎調査」結果に基づいて作成されています。

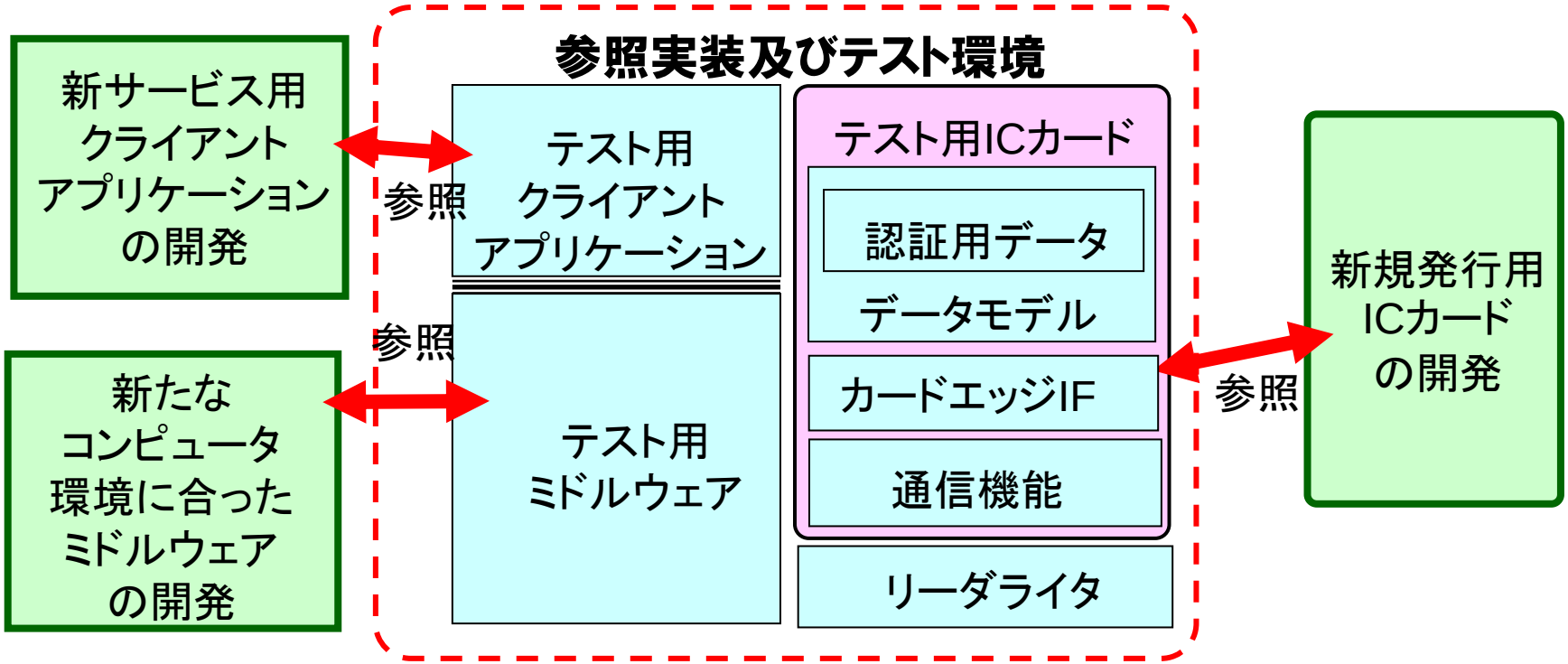
(4) 実装規約

- IC・IDカードシステムの仕様を定義
  - 国際標準に準拠
  - 国内で汎用的に利用可能
- 「これが決まればカードもアプリも作れる」公開仕様
  - クライアントアプリケーションインタフェース
  - リーダライタインタフェース
  - 物理インタフェース
  - カードエッジインタフェース
  - データモデル
  - 記録された認証用データへのアクセス手順

注:この資料は独立行政法人情報処理推進機構(IPA)の「IC・IDカードの相互運用可能性の向上に係る基礎調査」結果に基づいて作成されています。

(5) 参照実装及びテスト環境

- オープンソースソフトウェアによる参照実装
- 準拠性を確保するためのテスト環境・テストデータ



注:この資料は独立行政法人情報処理推進機構(IPA)の「IC・IDカードの相互運用可能性の向上に係る基礎調査」結果に基づいて作成されています。

(6) 製品認定の仕組み

- 何を買えばよいかが明確に分かる
  - 相互運用可能性が確保された製品を安心して調達できる
  - IC・IDカードやリーダライタ、ミドルウェア等を個別に調達可能にする
  - 公的機関での調達条件として採用される状況を目指す
  - 「安心して使えるカード」としてのブランドを確立
  - 製品認定を通じて国際標準に準拠
- 価格競争力が落ちない
  - 以上が、ICカードベンダ負担少なく実現されること

注:この資料は独立行政法人情報処理推進機構(IPA)の「IC・IDカードの相互運用可能性の向上に係る基礎調査」結果に基づいて作成されています。

(7) 支援環境整備の進め方(案)

- 今後導入されるIC・IDカードをターゲットに
  - 調達仕様書のサンプルまでできる
  - 導入時に有効性を示す
- まずは機能とセキュリティの構造を明確に
  - 公開可能な範囲が明確になる
  - カード技術者の検討範囲が明確になる
- ICカードの相互運用には日本ベンダは国際優位あり
  - JICSAP仕様　／電子パスポート　／住民基本台帳カード

注:この資料は独立行政法人情報処理推進機構(IPA)の「IC・IDカードの相互運用可能性の向上に係る基礎調査」結果に基づいて作成されています。

［発表者］
みずほ情報総研株式会社
情報・コミュニケーション部
出口太郎
taro.deguchi@mizuho-ir.co.jp
03-5281-5290

注：この資料は独立行政法人情報処理推進機構(IPA)の「IC・IDカードの相互運用可能性の向上に係る基礎調査」結果に基づいて作成されています。