資料4

社会保障分野の情報セキュリティとICカードの活用について

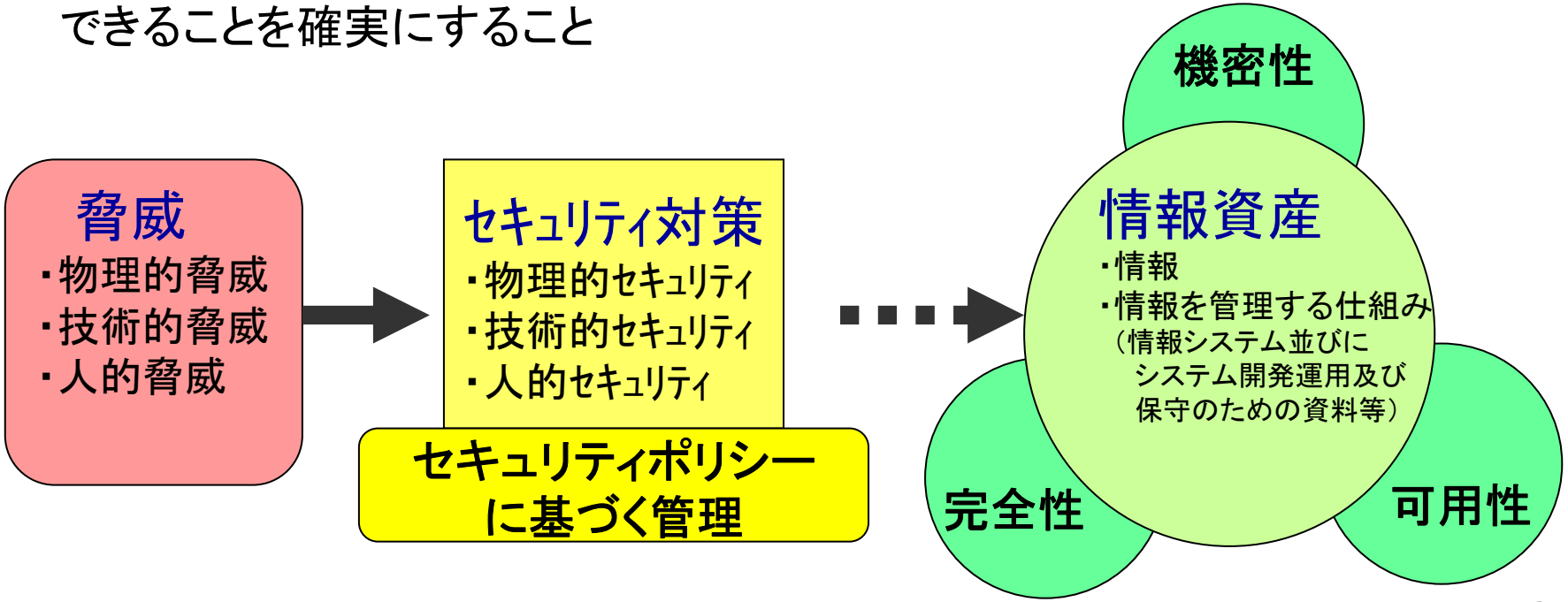
保健医療福祉情報システム工業会
セキュリティ委員会
茗原秀幸

１．情報セキュリティとは

3情報セキュリティとは

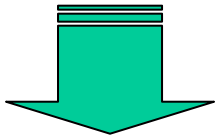
情報資産の機密性、完全性及び可用性を維持すること。

- 機密性（confidentiality）：情報にアクセスすることが認可された者だけがアクセスできることを確実にすること
- 完全性（integrity）：情報及び処理方法の正確さ及び完全である状態を安全防護すること
- 可用性（availability）：認可された利用者が、必要なときに情報にアクセスできることを確実にすること



情報の保護を行うために必要なこと

- セキュリティポリシーの策定と施行
  - 組織の情報資産を適切に保護するための対策について組織的に取り組む統一基準
- セキュリティ対策技術の利用
  - アンチウイルスソフトやファイア・ウォール等の製品



セキュリティ対策には、
①ポリシー策定、組織運用などの組織的もしくは運用的対策
②ファイアーウオール、暗号化などの技術的対策
が必要で、全体の対策レベルは一番低いものに引きずられる!!

セキュリティ侵害の例

- データの盗難・搾取・流出
  - サーバ内部のデータを盗む、ネットワークの通信経路上で盗聴する、等
- サービス妨害（DoS：Denial of Services）
  - サーバの処理能力を超えるような大量のリクエストやデータを送信する、セキュリティホールをついてシステムをダウンさせる、等の業務妨害行為
- 不正なリソースの使用
  - サーバ・ネットワーク等の不正な利用
    権利がないのに使う
- データの改ざん
  - サーバ内部のデータを権限がないにもかかわらず不正に改ざんする（ホームページの改ざん等）

セキュリティ侵害がもたらすもの

- サービスの低下と利益の喪失
  - システム停止による利用者への影響や機会喪失の発生
- 信用・ブランドイメージの低下
  - 社会保障機関としての信頼の喪失
- 復旧コストの発生
  - システムを復旧するための時間と労力がコストとして発生
- 訴訟・賠償請求
  - 個人情報やその他情報が漏洩した場合にその被害者から訴訟を提起され損害賠償責任を負う可能性
- 法的責任
  - 個人情報保護法などによる罰則規定

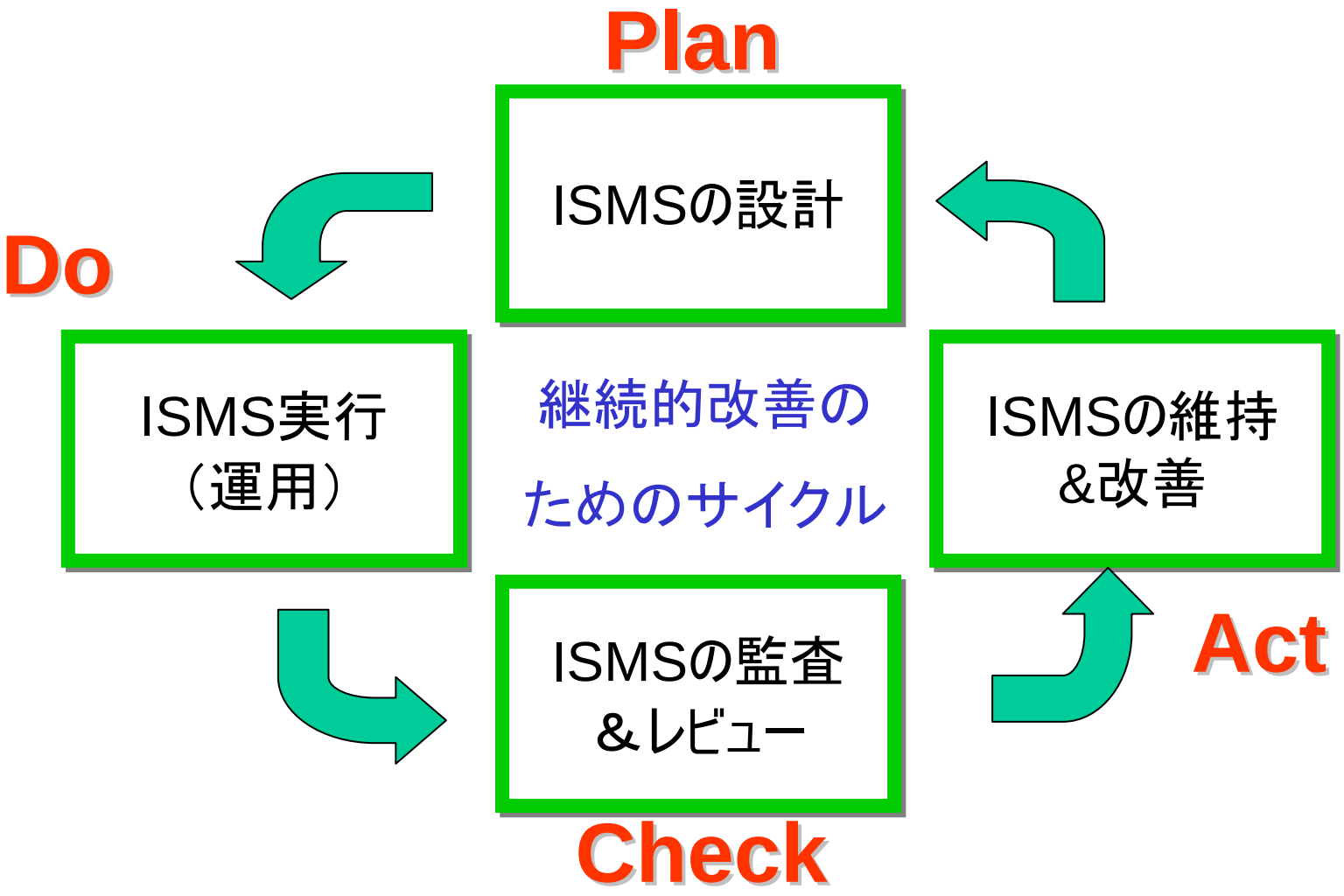
2.情報セキュリティ
マネジメントシステムとは

情報セキュリティマネジメントシステム（ISMS）

- 技術的対策から総合的なマネジメントへ
- ISO17799制定、JIPDECの認証制度スタート、OECDセキュリティ9原則の制定、BS7799のISO9000シリーズとの整合性確保のための大幅改訂などトレンドは情報セキュリティマネジメントにシフト→ISO27000シリーズとして体系化
- ISOにおける医療分野向けISMSの標準化
- JIPDEC、MEDISによる国内の普及検討

ISO9001（生産管理）、14001（環境管理）に次いで第三の柱に！

■ PDCAサイクルによるプロセスモデルの概要



セキュリティ対策の実施

＜リスクアセスメント＞

- 情報資産の価値評価
- 想定される脅威の分析
- 存在するぜい弱性の分析
- リスクの評価

どの情報資産をどの程度のコストで保護すべきか

＜セキュリティポリシー策定＞

- どのような方針で：ポリシー
- どのような基準で：スタンダード
- どのような手順で：プロシージャ

組織と運用

システムで防御できない脅威に組織と運用で対策を講じる

システムにおける対策・運用規定

パスワード管理
アクセス権限付与基準
監査の条件　など

システムに対する要件

情報セキュリティの目標（例）
【何のためにISMSを実施するのか】

（１）個人情報の保護

社会保障情報は個人情報のなかでも特に重要な情報であり、情報の漏洩が本人の人生を大きく左右することも考えられる。情報提供機関は取り扱う情報の重要性を認識し、適切に管理しなければならない。

特に重要な対策（管理策）例としては以下のようなものがあげられる

個人情報保護の観点から社会保障情報の機密性の維持をおこなうこと

（２）誤った情報による事故の予防

社会保障情報の完全性が維持されない場合、誤った情報に基づく業務が実施される恐れがある。情報提供機関は事故防止の観点から社会保障情報の完全性の維持に努めなければならない。

特に重要な対策（管理策）例としては以下のようなものがあげられる

適切な業務を行なう観点から社会保障情報の完全性の維持をおこなうこと

（３）サービス機能の維持

情報提供機関は社会インフラが多大なダメージを受けても速やかに機能回復し、継続して業務を行なえるようにする必要がある。また、悪意を持った攻撃に対する適切な防御手段を用意し、サイバーテロなどに対処できるようにしなければならない。

特に重要な対策（管理策）例としては以下のようなものがあげられる

情報提供機関の機能維持のために情報システムの可用性の維持をおこなうこと

脅威とは

リスクが発生する要因のことを「脅威」という。

脅威とは、より厳密に言えば、「情報資産や組織に損失や損害をもたらす不測の事態の潜在的な要因」のことである。

脅威の分類

脅威			
偶発的脅威		意図的脅威	環境的脅威
過失	故障	故意	災害
データ入力誤り 運用誤り 誤接続 その他	H/W障害 S/W障害 回線障害 その他	情報の盗用、改ざん なりすまし、不法侵入 ウィルス、サイバーテロ 物理的破壊、その他	地震 火災 水害 その他

これらの脅威はあくまで「不測の事態の潜在的な要因」であり、脅威があるだけでは問題とはならない。これら脅威を顕在化し、具体的な損害を与える要因があって初めて脅威はリスクとなる。

ぜい弱性とは

脅威を顕在化するシステムの弱点のことを「ぜい弱性」という。

ぜい弱性の例

ぜい弱性の例	
環境	ドアや窓、電源供給、災害を受けやすい立地など
ハードウェア	駆動部分の経年劣化、バックアップ回路の不備など
ソフトウェア	仕様書の欠如、アクセス制御の不備、プログラムのバグなど
ネットワーク	非暗号化、通信経路の保護の不備、バックアップ回線の不備など
組織	教育プログラムの不備、部外者の管理の不徹底など
個人	スキル不足、低いモラル、誤った理解など
マネジメント	予算不足、情報セキュリティマネジメント意識の欠如など

ぜい弱性はその存在自体が障害となるわけではない。

脅威とぜい弱性が組み合わせられることでリスクが発生するのである。

リスクマネジメント

リスクに対処する方法

リスクコントロール
　積極的に損害を小さくするための対策（管理策）を採用する
・リスク予防
　脅威や脆弱性を少なくするための対策を実施する
・損害の極小化
　リスクが発生したときの損害を少なくするための対策を実施する

リスク移転
　契約等により他社に移転する対策
・リスクファイナンス
　損害保険や責任賠償保険などに加入しリスクを移転する
・アウトソーシング
　情報資産そのものや情報セキュリティ対策を外部に委託する

リスク保有
　組織としてリスクを受容する対応
・リスクファイナンス
　引当金を積むなどの対応を行う
・何もしない

リスク回避
　適切な対策が見出せない場合の対応
・業務の廃止
　業務そのものをやめてしまう
・情報資産の破壊
　管理対象物をなくしてしまう

通常のリスクマネジメントにおいては、これらのどれか一つを選択するということではなく、リスクの重要度や対策の容易性などから総合的に判断し、これらの対策を組み合わせて実施する。

3.PKIの利用に焦点を当てた場合におけるICカードの要件

重要な注意：
ICカードの利用方法にはPKIのための利用以外にも、
一般的なアプリケーションサービスのための利用方法がある。
本章ではPKIのための利用に焦点をあてて記述しており、
他のアプリケーションにおける要件については一切記載していない。

社会保障サービスで実現すべきこと

- ITを活用し、各種社会保障サービスを、安全、安心な環境で提供する
- ITを活用し、個人の各種情報を本人に対して可視化する
- ITを活用し、必要に応じて本人が社会保障関係の手続きを簡単に行えるようにする。

ITを活用した、安全、安心な仕組み

- 利用者が間違いなく本人だと確認するための手段の整備→なりすましの防止→アクセス時の本人認証手段の整備
- 各種申請などが本人の手により間違いなく行われたと確認するための手段の整備→偽造、改ざんの防止と否認防止→申請書類作成時の電子署名の手段の整備

情報セキュリティマネジメントの結果としての
管理策として選択されるべきもの

どのようなサービスが考えられるか

- 年金関連のサービス
- 予防医療関連のサービス
- 医療保険関連のサービス
- 各種電子申請のサービス
- etc

上記のようなサービスを提供するにあたり、セキュリティの確保は必須事項である。本人確認や否認防止のためのセキュリティ対策としてのアクセス認証と電子署名は安全、安心のためにはあったほうが良い。

セキュリティ対策としてのICカードの利用

- PKI技術を利用することにより、本人認証や電子署名を利用できる。
- PKI技術を利用するには私有鍵（秘密鍵）の管理が重要になる。
- 私有鍵（秘密鍵）は堅牢な、可般型の媒体に格納する必要がある。

堅牢な媒体としてはFIPSなどの規格を満たしたハードウェア・セキュリティ・モジュール（HSM）を活用すべきである。

可般型HSMとしてはICカードが有力

ICカードを利用した電子署名、認証

- ICカードに格納された秘密鍵、証明書を利用して電子署名やアクセス認証を行なう
- ICカードとのAPIは各社が独自仕様で用意
  - 現状はベンダ各社が専用のPKIドライバを用意している。
  - 異なるICカードを使うには、それぞれのドライバを用意する必要がある。

PKIドライバ（アクセス方式）が標準化できれば便利

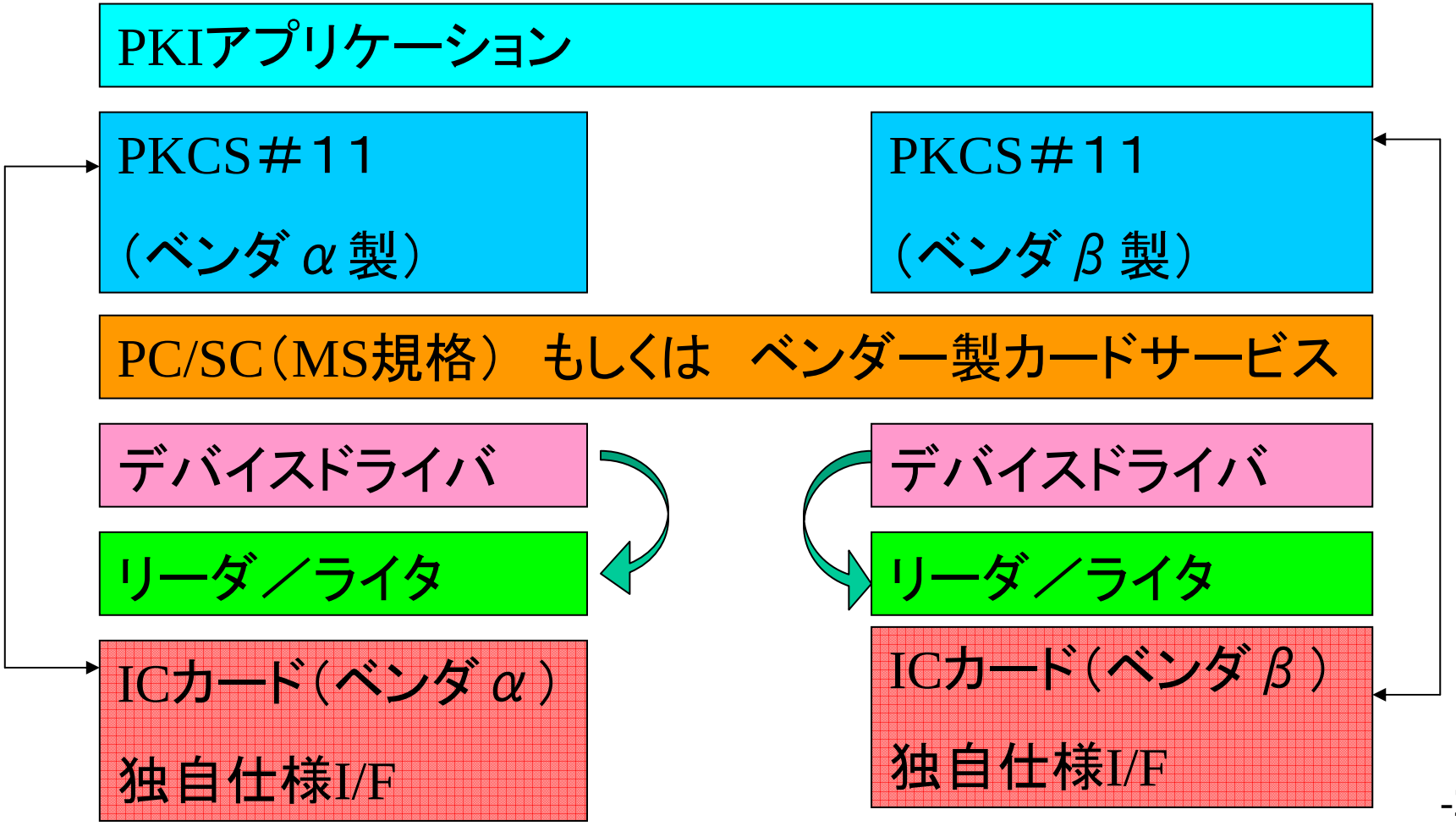
ISO/JTC1/SC17　においてICカードにおけるPKIの利用を標準化するための規格が整備されている。

ISO7816　part4,8,15　がそれにあたる。→JIS化もされている。

ICカード用PKIシステムの現状

各社が自社の独自I/Fを持っており、各社がそれにあわせたPKCS＃11などの

PKIアクセス用のドライバを用意している



ICカードのPKIドライバ標準化の必要性

現状の問題点

- 各社が専用ドライバを用意している場合
  - 仮に仕様の異なる複数社のICカードが採用されたら、全てのマシンに各社用のPKIドライバを組み込む必要がある。

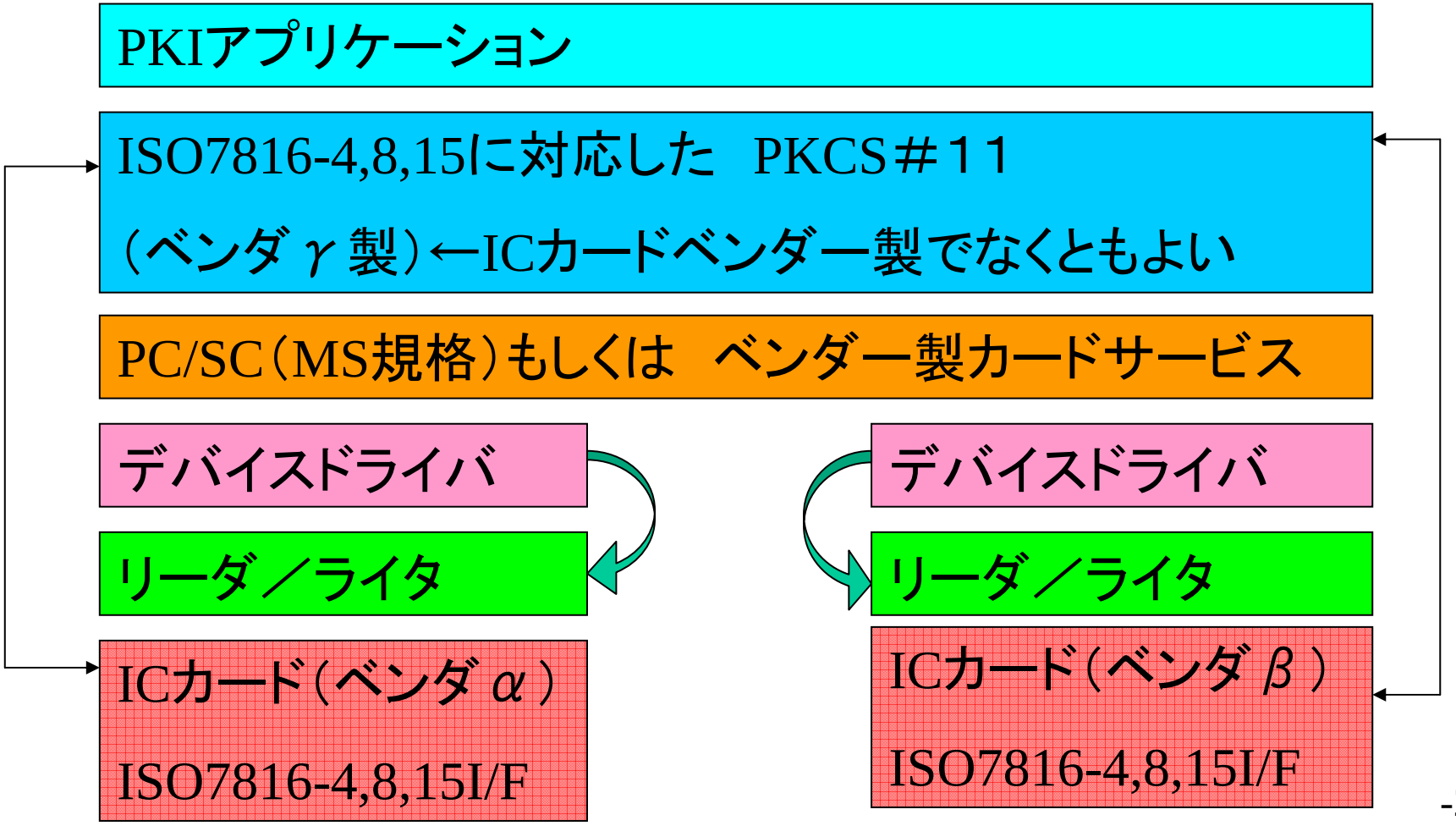
    →複数ドライバを共存させて動作保障できるのか
  - 一社独占の納入でない限り相互運用性が確保できない。
- 一社が提供するPKIドライバに各社が合わせる場合
  - 国際規格ISO7816やJIS規格が既にあるのに別の規約を策定する必要はない。
  - 政府調達ならばWTOを意識する必要がある。

従来のICカードとの違い

- 職員証、社員証、定期券など、一つの企業や企業グループで独占的に仕様を決めて運用できる事業
  - ICカードベンダーなどの差別化提案が有効
  - 国際調達基準を考慮する必要なし
- 年金手帳、健康保険証、介護保険証など、日本全国どこででも利用できることが求められる事業
  - 一社独占の場合、価格高止まりの危険性をはらむ
  - 健全な競争の促進による、価格低下と普及推進が重要
  - 国際的な調達基準への準拠（WTO対策）が必要

理想の状態

各社のICカードがISO準拠のI/Fを持っており、一つ（または複数）の
ISO準拠のI/Fに対応したPKIアクセス用のドライバが用意されている状態



このときICカードはどうあるべきか

- PKIを利用するという観点だけからみると以下のものが必要になる。
  - 標準的なPKIのI/Fをサポート
  - 鍵と証明書を必要な分だけ格納できる容量
  - 演算処理を現実的な時間で処理できる性能
- 国際標準に準拠した要求仕様であれば、自由競争による低価格化を促進できる。
  - 同一規格に対する、価格、性能、サポートの競争になる

このときPKCS#11ドライバはどうあるべきか

- ICカード各社は自らのドライバを用意する必要がない。
  - 莫大な開発負担から開放される
- PKIドライバ提供ベンダーによる自由競争
  - 品質、性能、価格、サポートなどの異なる各種製品をユーザーが自由に選択可能
  - 信頼できるベンダーによる性能保証のドライバが求められる可能性大
  - ドライバの動作保障に関する認定制度があれば安全なドライバの普及につながる。

他国における推進状況

- 国民IDカードでのICカードの利用はフィンランドとベルギーが先行
  - 国民用IDカードとしてICカードを発行している
  - ICカードの用途は認証・暗号用と署名用に限定
  - 今回説明のISO7816-4,8,15準拠の仕様
  - 既に大量発行の実績あり
- 米国では連邦従業員と契約業者向けのICカードを発行
  - 国立標準技術研究所（NIST）が政府調達基準（FIPS201）を策定
  - ISO完全準拠ではないものの対応を強く意識

フィンランドのFINEIDプロジェクト

- 国民用IDカードプロジェクトとして1998年スタート（1999年にカード発行開始）
- 国民登録局のDBと連動したカード発行
- 認証・暗号用と署名用の二種類のPKIを発行
- 対人としては、市民証明書と組織所属者証明書の二種類
- ICカード仕様が公開されており、ISO7816-4,8,15準拠
- 認証局の証明書ポリシ（CP）や認証実施規定（CPS）を公開

ベルギーのBELPICプロジェクト

- ベルギー電子政府プロジェクトの一環として始まった国民IDカードプロジェクト
- 2002年開始、2005年9月からBELPIC仕様のICカードに完全移行
- 認証用（6歳以上）と署名用（１８歳以上）の二種類のPKIを発行（暗号用はない）
- 年齢に応じてカードを分けている。（１２歳未満は子供用カード、１２歳からBELPICカード）
- ICカード仕様が公開されており、ISO7816-4,8,15準拠
- 認証局の認証実施規定（CPS）を公開（証明書ポリシ（CP）は非公開）

米国のPIVプロジェクト

- 政府調達基準としてFIPS201によって身分証の仕様を規定
- 対象は連邦政府職員および契約者
- 主目的は連邦政府へのアクセスに対するアクセス制御
- 認証用と署名用の二種類のPKIを発行（ただし署名用はオプション）
- ICカード仕様はISO7816-4,8に準拠。7816-15を強く意識している（将来的には移行？）
- PIV対応製品・サービスに対する認定制度を確立

他国の動向のまとめ

- 三例（フィンランド、ベルギー、米国）とも認証用、署名用のPKIカードに特化している
- ISO7816-4,8,15に完全準拠もしくは強く意識
- 仕様を公開し、広い参入機会を提供
- 米国では調達仕様だけでなく、認定制度を準備し、製品やサービスの安全を確保

ありがとうございました