要件調査ワーキンググループ
活動報告

２００２年4月１６日

暗号技術検討会要件調査WG リーダ
佐々木　良一 (東京電機大学)

暗号技術検討会　要件調査ワーキンググループ

- 要件調査ワーキンググループ（要件調査WG）について

  - 2001年6月に設置
  - 暗号技術検討会の活動内容の一つである「電子政府で用いられる、または将来用いられるであろう暗号技術に求められる要求条件の調査及び検討」等を集中的に実施するためのサブグループ
  - 暗号技術の評価にあたり、評価精度の向上、評価の効率的な実施、評価結果の迅速な反映等に資することを目的
  - 2001年6月から2002年3月まで、計12回の会合を開催

要件調査WG　メンバー

(敬称略)

リーダ	佐々木良一	東京電機大学工学部情報メディア学科教授
	岩下　直行	日本銀行金融研究所研究第２課調査役
	岡本　栄司	東邦大学理学部情報科学科教授
	川村　信一	株式会社東芝　研究開発センター コンピュータ･ネットワークラボラトリー　主任研究員
	洲崎　誠一	株式会社日立製作所　システム開発研究所 第七部　Ｈ０１研究ユニット　研究員
	館林　誠	松下電器産業株式会社　マルチメディア開発センター メディア情報グループ　メディア情報第一チーム　リーダー
	米倉　昭利	財団法人日本品質保証機構 電子署名･認証調査センター所長
	渡辺　創	独立行政法人産業技術総合研究所　情報処理研究部門

要件調査WGの検討対象

- 以下の全ての条件を満たす電子政府システムを対象として調査及び検討。

  - 国の行政機関のシステム（大学、病院、地方自治体は対象外）

  - 国家の安全保障のため、又は国家の防衛上の目的のためのものを除く。

  - 国民との間で行政サービスとしてやりとりを行うもの、及びそのやりとりを安全に行うために必要な関連システム（下位層のシステムを含む）

要件調査WGにおける調査･検討項目

- 暗号技術を利用すると想定されるシステムの調査
  - 国の行政機関のシステムに関するヒアリング調査
  - メーカ、ベンダ等に対するアンケート調査
  - SSL(Secure Socket Layer) で用いられる暗号の安全性評価
- 電子政府に関連する海外の先行事例における暗号技術の取り扱いの調査
  - 海外電子政府システムにおける暗号要件に関する調査
- 暗号に対する技術的な要求条件の検討
  - 暗号技術を利用する電子政府システムのモデル化
  - 電子政府システムにおける暗号利用形態
  - 利用形態ごとに用いられる暗号技術
  - 電子政府における一般的要件
- 暗号技術を利用するにあたっての留意事項の検討

ヒアリング調査結果の概要

- 実施時期　　2001年7月～11月
- 実施方法　　面接（事前に質問票を送付）
- 対象システム　　計10システムの調査を実施
  【 電子申請、電子入札、電子納付、電子情報提供、など 】
- 要件に関する主な調査結果
  - クライアント側は、商用OS等に組み込まれたSSL等の既存ソフトを利用する場合が多い。（10システム中、半数以上（6システム）がSSLを採用）
  - 暗号の処理速度、ハッシュ関数の処理速度の高速化への要求は特になし。
  - 多く用いられている暗号アルゴリズムは以下の通り。

    公開鍵　　RSA（2048bit, 1024bit）
    共通鍵　　TDES，DES，RC2（128bit，40bit），RC4（128bit, 64bit）
    ハッシュ関数　SHA-1

アンケート調査結果の概要（1）

- 実施時期　2001年12月～2002年1月
- 実施方法　国内17社のメーカ及びベンダ等にメールで質問票を送付
- 回答企業数　計16社

- 主な調査結果

【暗号に求められる要件】

安全性（今後10年間利用可能）、実装性（処理速度、サイズ）、
暗号標準（デファクト又は国際標準）、を挙げる回答が多かった。

【10年後の要件の優先順位】

「現在と変わらない」「変わる」が半分ずつ。

（「変わらない」理由の例）
10年間で解読技術が進歩する一方、新たな暗号関連技術も登場するから
（「変わる」理由の例）
ハードウェア性能の向上により、実装性の順位が相対的に低下するから

【暗号の耐用年数】

一部の用途については10年以上必要、との意見が多かった。
（一部の用途：署名に使う暗号処理、認証局の共通鍵）

アンケート調査結果の概要 (2)

- 主な調査結果 (続き)

【推奨暗号の数】

推奨暗号を、利用形態別 (「署名・認証」「通信」「保存」等)、又は方式別 (「共通鍵」「公開鍵」等)、目的別 (「守秘」「認証」等)、に区分してリスト化する場合、区分毎の暗号数は、2～3個が望ましいとする意見がほとんど。

【政府調達における仕様の指定】

- 電子政府システムの調達仕様書に暗号アルゴリズムを指定することは「問題ない」とする意見が大多数
- 製品名を指定することには「望ましくない」「必要ない」とする意見が大多数

【市販ソフトに組み込まれている暗号を考慮すべきか】

「考慮すべき」「どちらかと言えば考慮すべき」とする意見が約半数。

【 ICカードシステムで利用する暗号の技術的要件 】

- 「実装サイズ、実装可能性」「処理速度」を挙げる回答が最も多い。
- ほか「標準暗号」「耐タンパ性」「鍵サイズ」「暗号強度」等。

SSLで利用される暗号の安全性評価結果の概要（1）

- ヒアリング及びアンケート、海外事例調査の結果、SSLが政府関係システムに用いられており、今後も用いられるケースが多いと判断。

- SSL自体の安全性及びSSLで用いられる暗号の安全性に関する評価を実施。（具体的な技術的評価は暗号技術評価委員会に依頼）

- 評価対象暗号　　公開鍵：RSA　　共通鍵：RC4, RC2, TDES

SSLで利用される暗号の安全性評価結果の概要（2）

SSL/TLSプロトコルに関する注意点

- SSL3.0を利用するにあたっては、既知のセキュリティホールを十分認識した上での設定（SSL2.0の利用を不可とする、等）を行うべき。
- 市販のSSLソフトを利用する場合、セキュリティホールにパッチの当てられた最新版を用いるべき。
- Internet Explorer及びNetscape Navigatorでは公開鍵証明無効化リスト（CRL）を不正に消去した上で不正な証明書を用いて認証を欺くという攻撃がありうる。よって、証明書を格納するファイルは厳密なアクセス管理を行うべき。
- 匿名認証モードの利用は推奨しない。（情報の盗聴、改ざんを受ける可能性）
- version rollback攻撃を防ぐため、特に理由がない限りSSL/TLSの最新版のみを使用するよう設定運用すべき。
- SSL3.0では、利用する暗号方式について変更出来ない。一方、TLS1.0は新しい暗号方式を追加することが可能であるため、既存の暗号技術に問題があった場合でも対応可能。
- TLSは機能追加を目的として拡張作業が行われているが、これらの拡張に伴って新たなセキュリティホールが発生する可能性もあるため、今後とも、TLSの動向に注目し、その安全性について継続的な調査、検討が必要。

SSLで利用される暗号の安全性評価結果の概要（3）

SSL/TLSで利用される暗号に関する注意点

- 鍵長40bitのDES及びRC2は、鍵総当りにより現実的な時間で解読可能
  → 安全性が必要なシステムにおいては、用いられるべきでない。
- 鍵長56bitのDESは、もはや現実的に解読可能な領域に達しつつある
  → 高い安全性が必要なシステムにおいては、用いられるべきでない。
- 鍵長168bitのTDESは、当面の間の使用には特に問題ない。しかし、TDESに替わる更に安全な暗号がSSLに採用されれば、それに置き替える方が望ましい。
- 鍵長128bitのRC2は、鍵総当りよりも効率の良い解読方法が存在
  → 新規に構築するシステムにおいては、採用することを勧めない。
- 64bitブロック暗号であるRC2, DES, TDESは、2^{32}ブロック以上を同じセッション鍵で暗号化すると、平文1bitの情報が漏れる恐れ
  → セッション鍵の更新に注意すべき
- 鍵長512bitのRSAは、現実的に素因数分解可能であり、安全でない。
  2001年度時点では、1024bit以上の鍵長を用いれば安全であると考えられる。

※ RC4は現在評価中であり、2002年度中に評価報告予定

海外電子政府システムにおける暗号要件に関する調査結果

- 調査実施時期　2001年11月 ～ 2002年2月
- 調査対象国　米国、カナダ、英国、ドイツ、韓国、シンガポール、オーストラリア等 13か国
- 調査内容　暗号利用事例、セキュリティ要件事例等
- 主な調査結果

【海外電子政府システムの暗号利用事例】

・通信の暗号化を行うシステムの大多数がSSLを利用

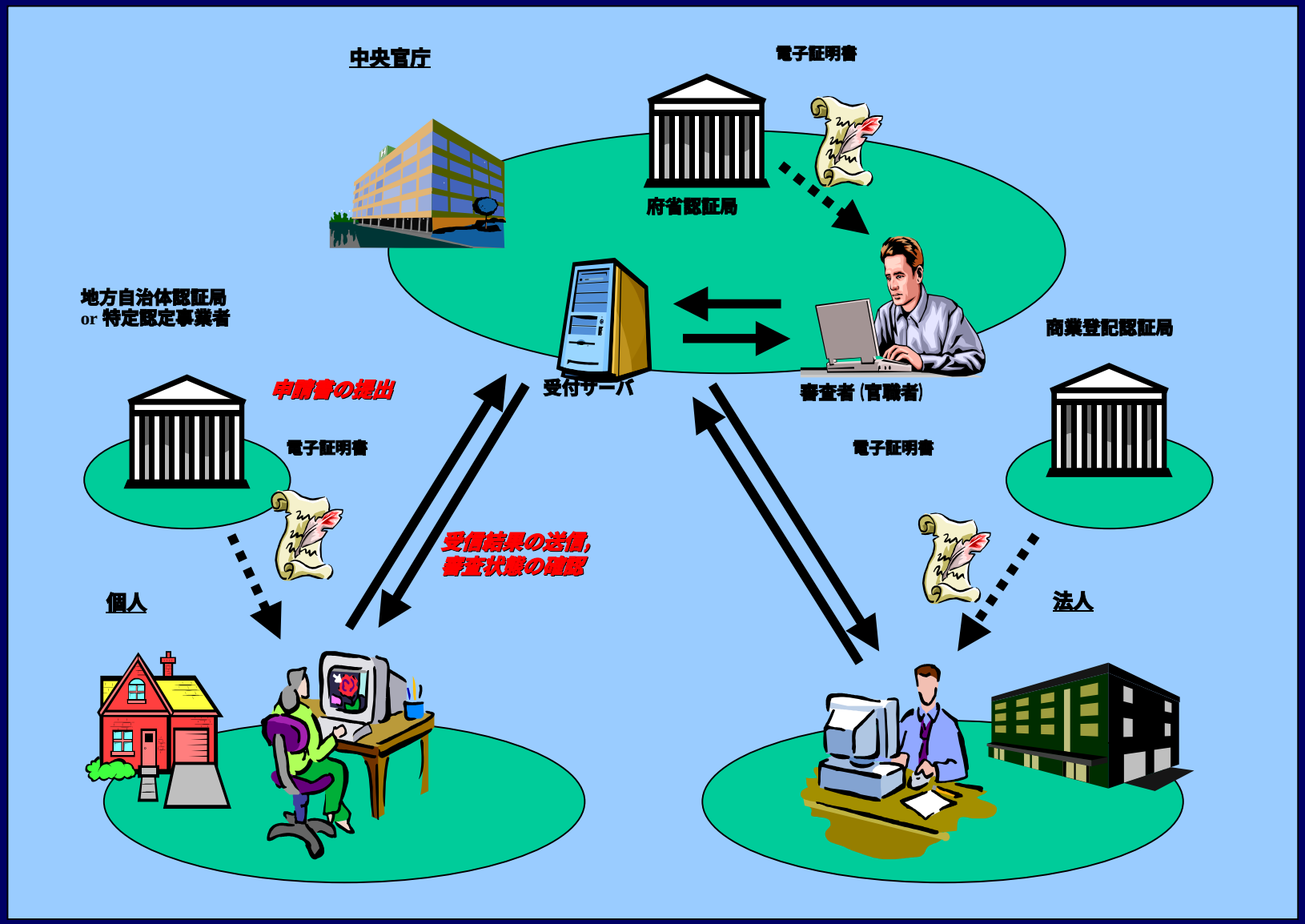
【セキュリティ要件事例】

・行政機関と外部との通信に関するセキュリティ要件を定めている国は少ない。

・オーストラリアDSD勧告におけるSSLパラメータ推奨設定
  - プロトコル：SSL 3.0（SSL2.0は禁止）
  - 共通鍵　：TDES(168) 又は RC4(128)
  - 公開鍵　：RSA 1024bit以上
  - ハッシュ　：SHA MAC　又は MD5 MAC

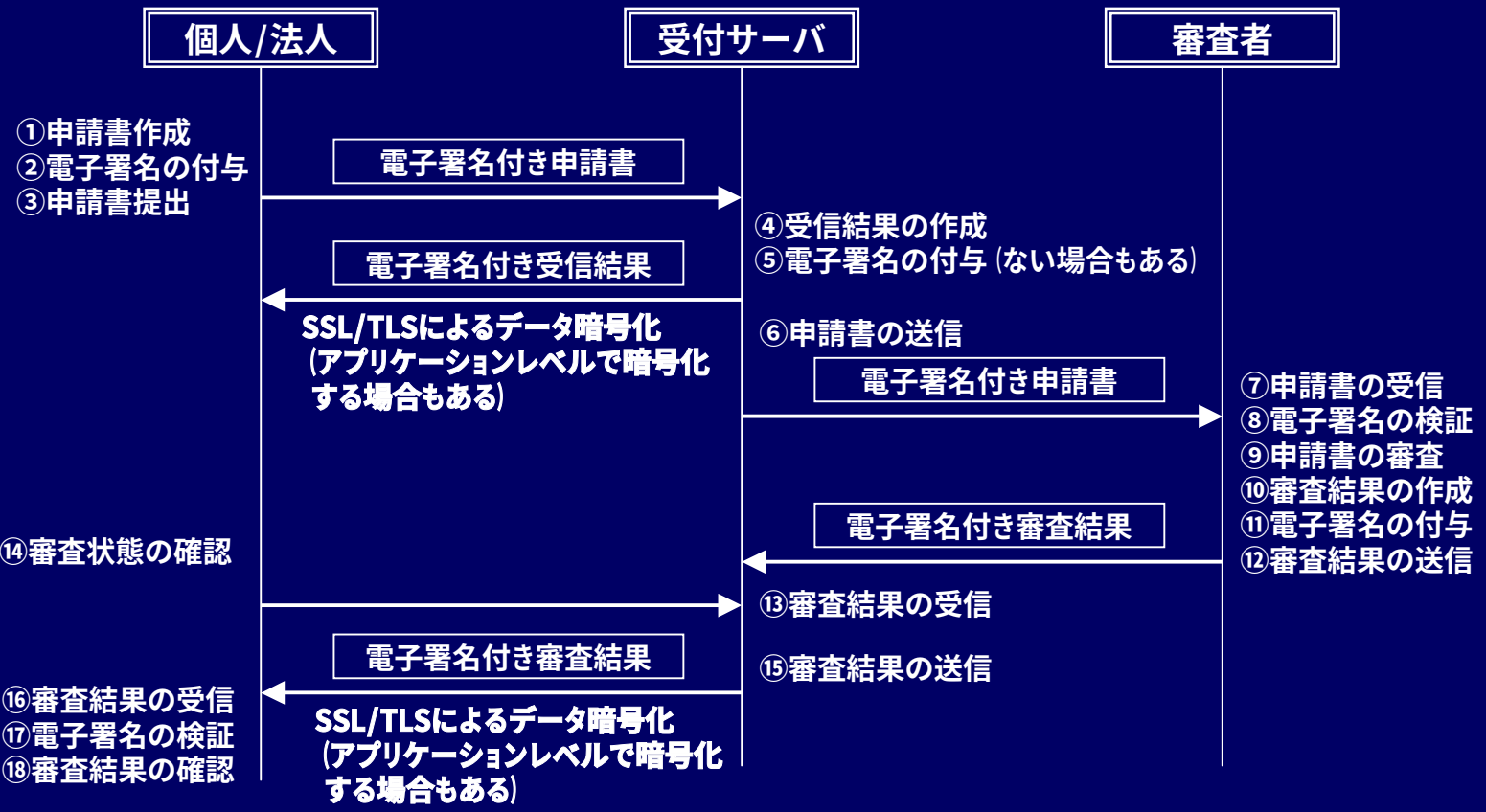
・米国NISTが公共Webサーバのセキュリティ確保に関するガイドラインを公表

電子政府システムのモデル化（電子申請システム）(1)



電子政府システムのモデル化（電子申請システム）(2)

- 電子申請システムにおける処理フローは、以下の3フェーズで構成
  1. 個人/法人が申請書を作成し、受付サーバに提出
  2. 提出された申請書を審査者が審査（受理/却下）
  3. 個人/法人が審査結果を確認

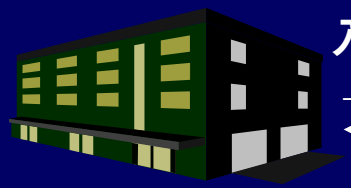


電子政府システムのモデル化（電子調達システム）(1)

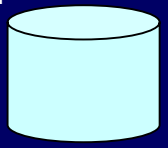
入札者

①参加資格審査申請

②参加資格認定通知書



入札書保管



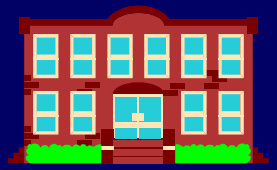
国の行政機関（発注者）

⑥認証書により入札に参加

⑦落札結果の通知

③電子認証書発行申請

④電子認証書発行（ICカード）



電子認証局

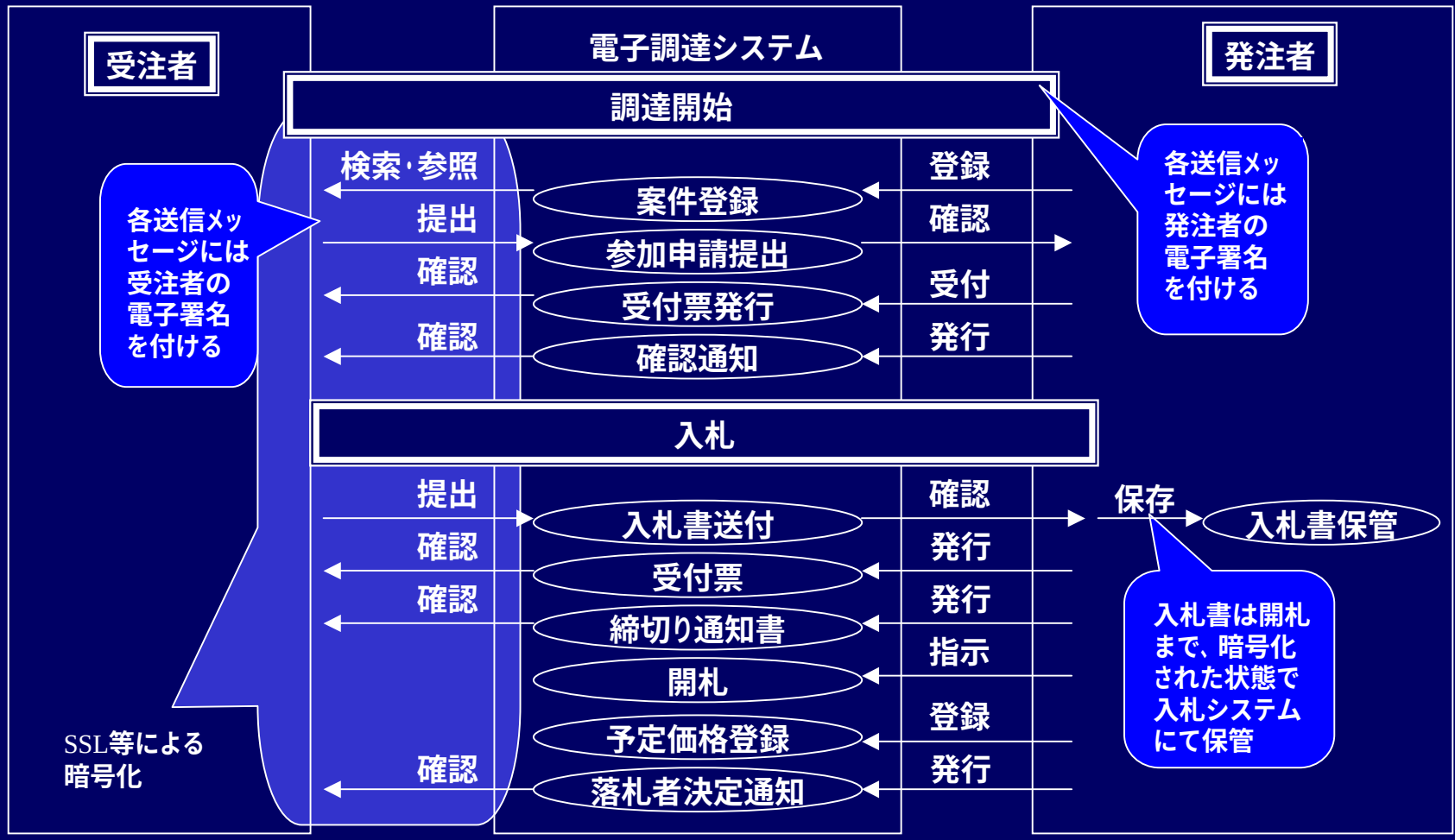
⑤認証書発行情報

電子入札システム

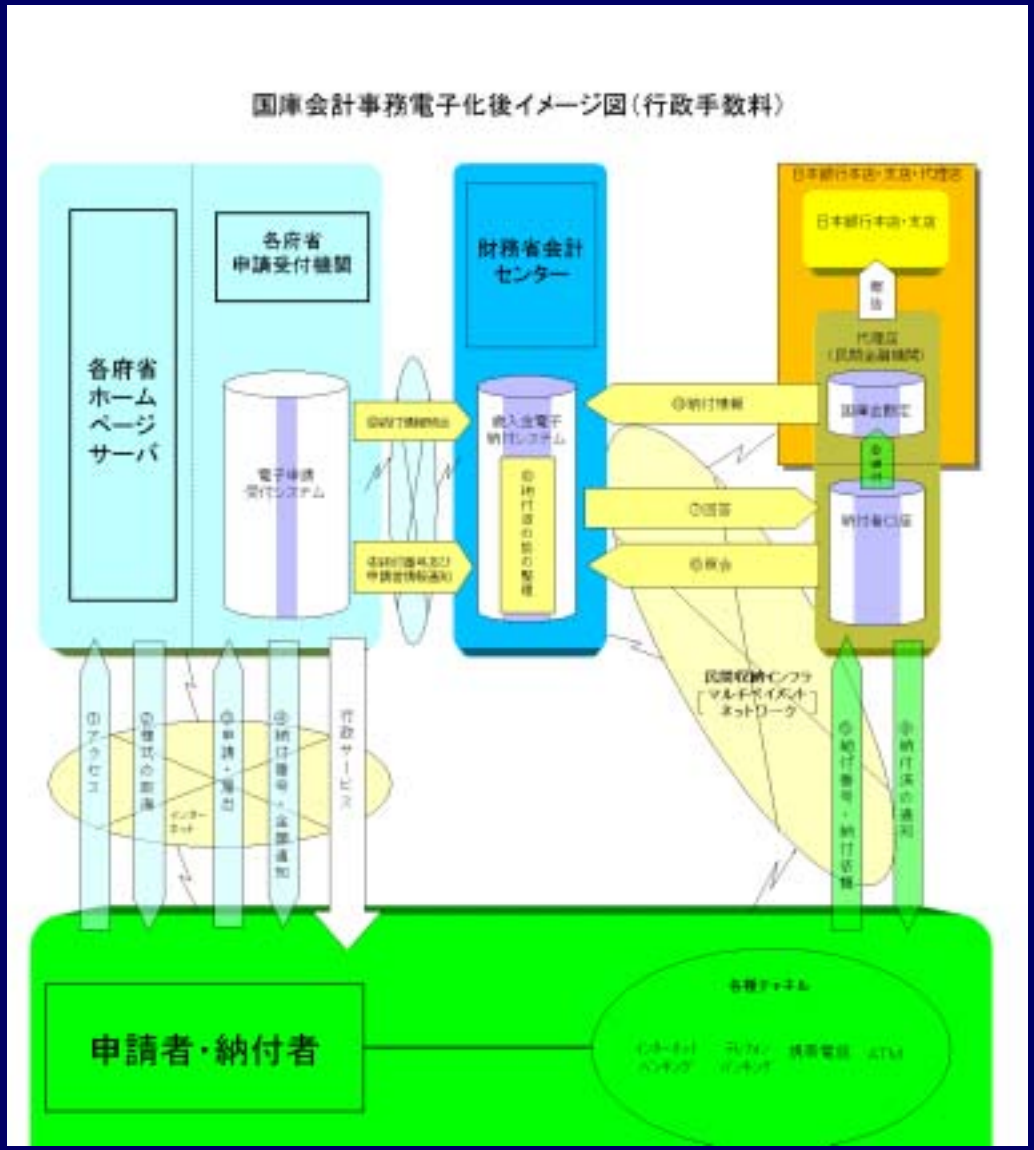
電子政府システムのモデル化（電子調達システム）(2)

電子調達システムの処理フローは、以下の3フェーズにより構成

1. 入札資格の申請/審査/認定通知
2. 入札書の提出/保管
3. 開札及び落札通知



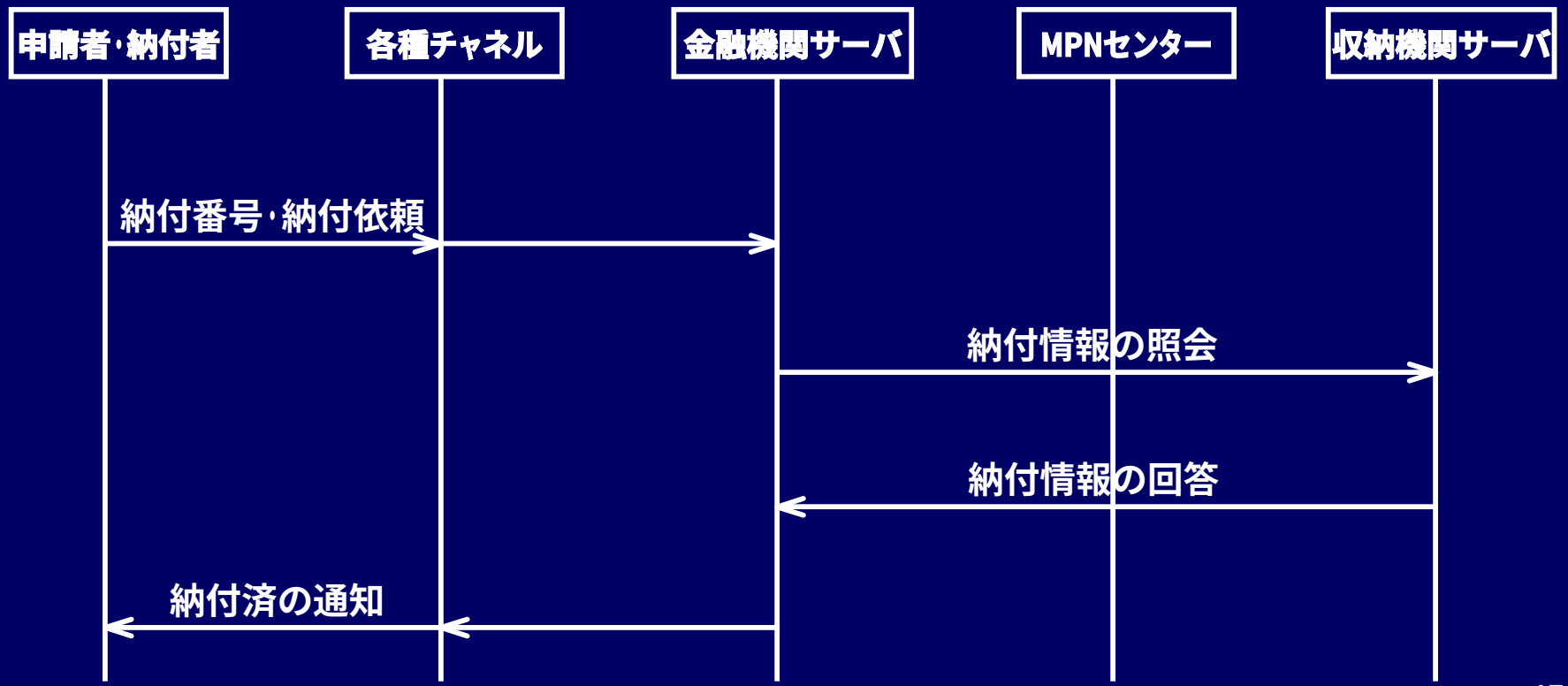
電子政府システムのモデル化（電子納付システム）(1)



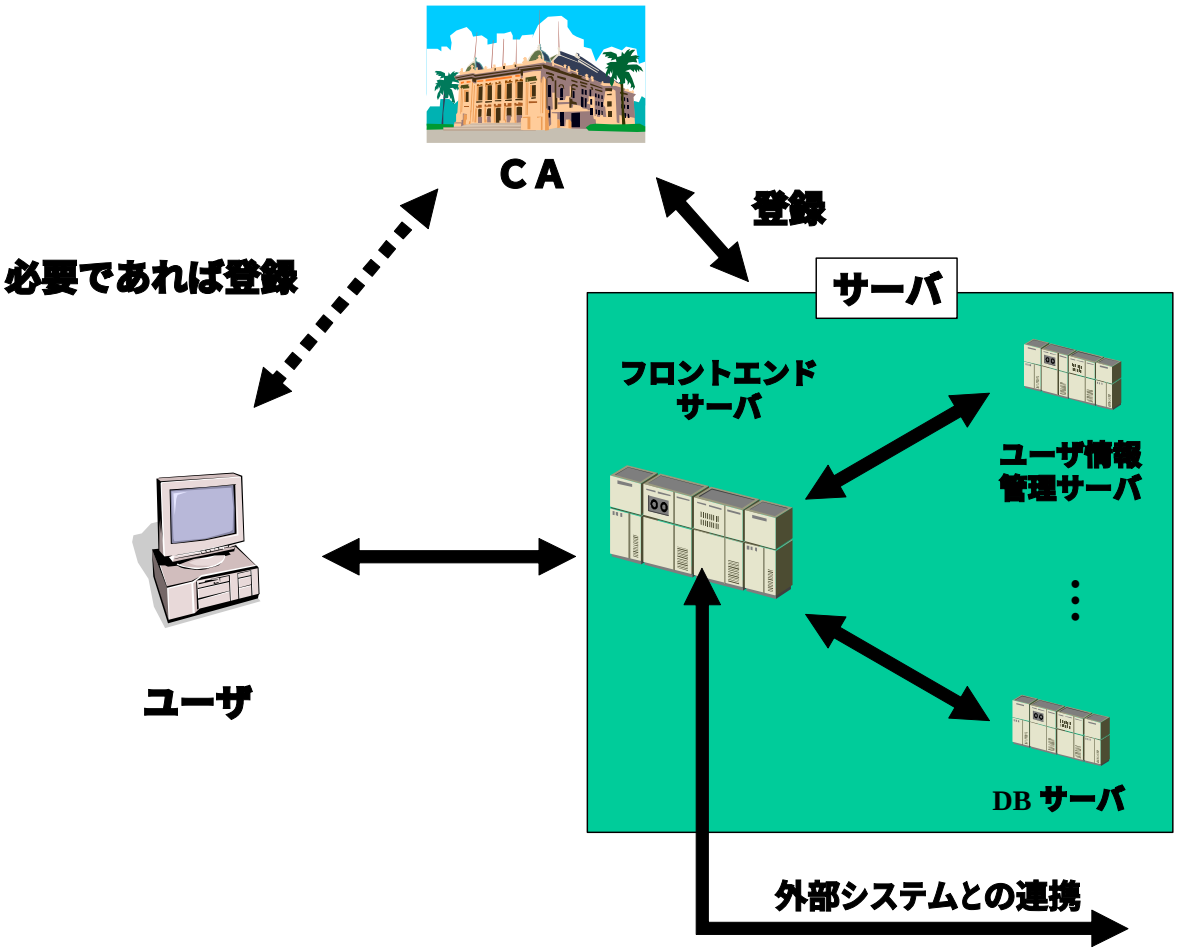
電子政府システムのモデル化（電子納付システム）(2)

電子納付システムの処理フローは、基本的には、金融機関側から送られてきた納付情報を、各府省（収納機関）側のシステムに配信する作りであり、以下の3フェーズから構成

1. 申請者及び納付者が金融機関に納付番号及び金額を依頼するフェーズ
2. 金融機関が、収納機関に納付情報を照会し、その回答を受け取るフェーズ
3. 金融機関が、申請者及び納付者に納付済の通知を行うフェーズ

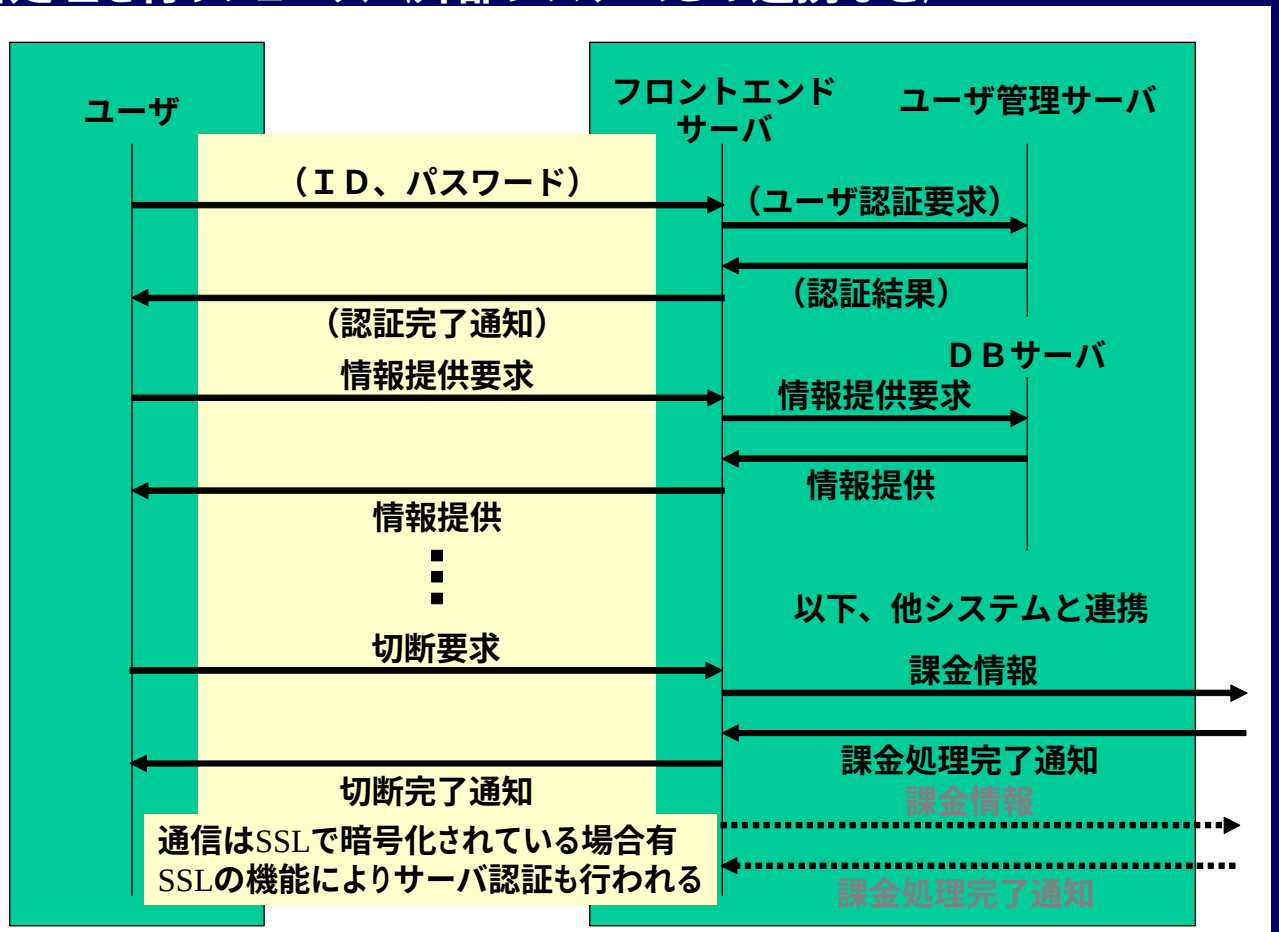


電子政府システムのモデル化（電子情報提供システム）(1)

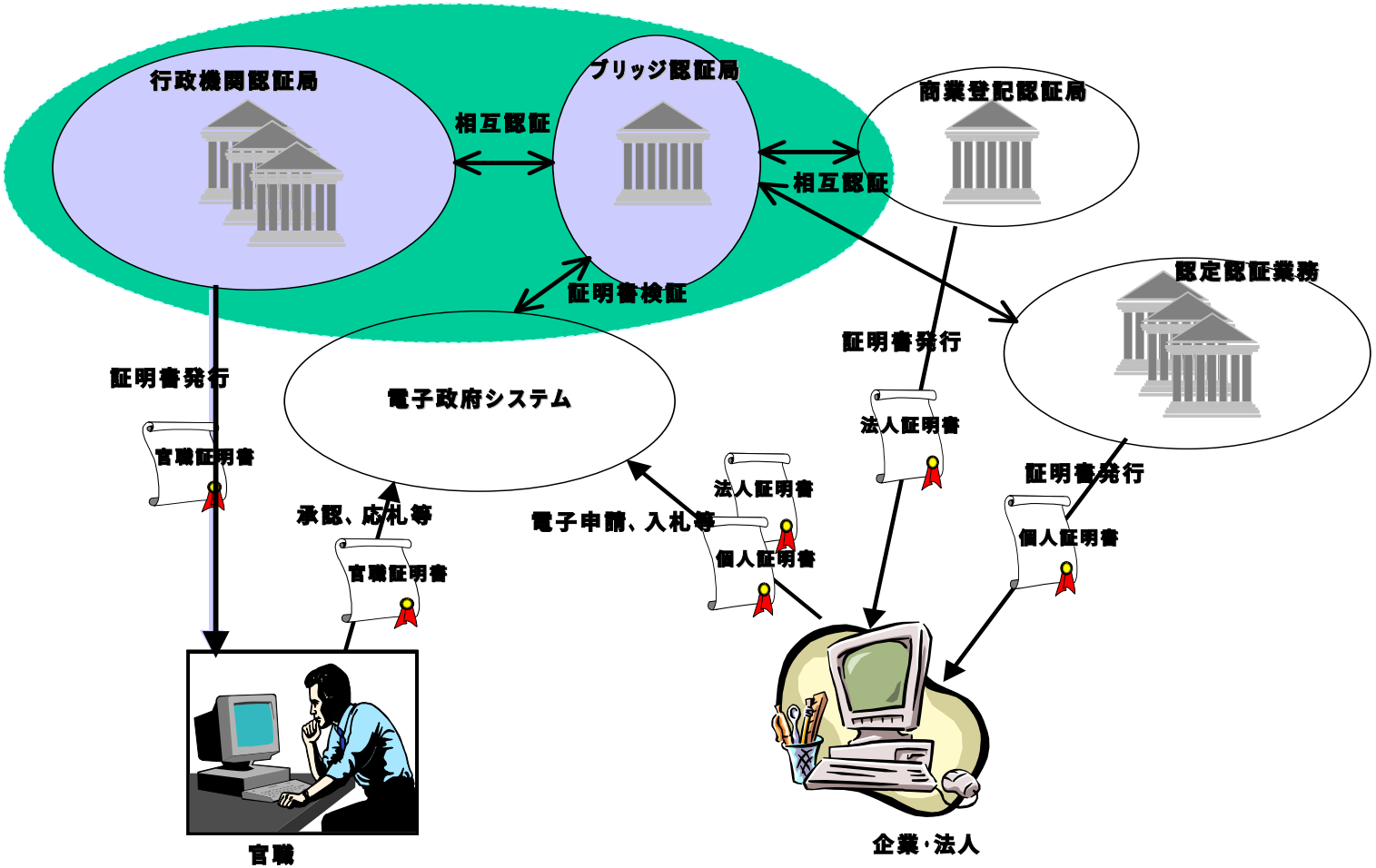


電子政府システムのモデル化（電子情報提供システム）(2)

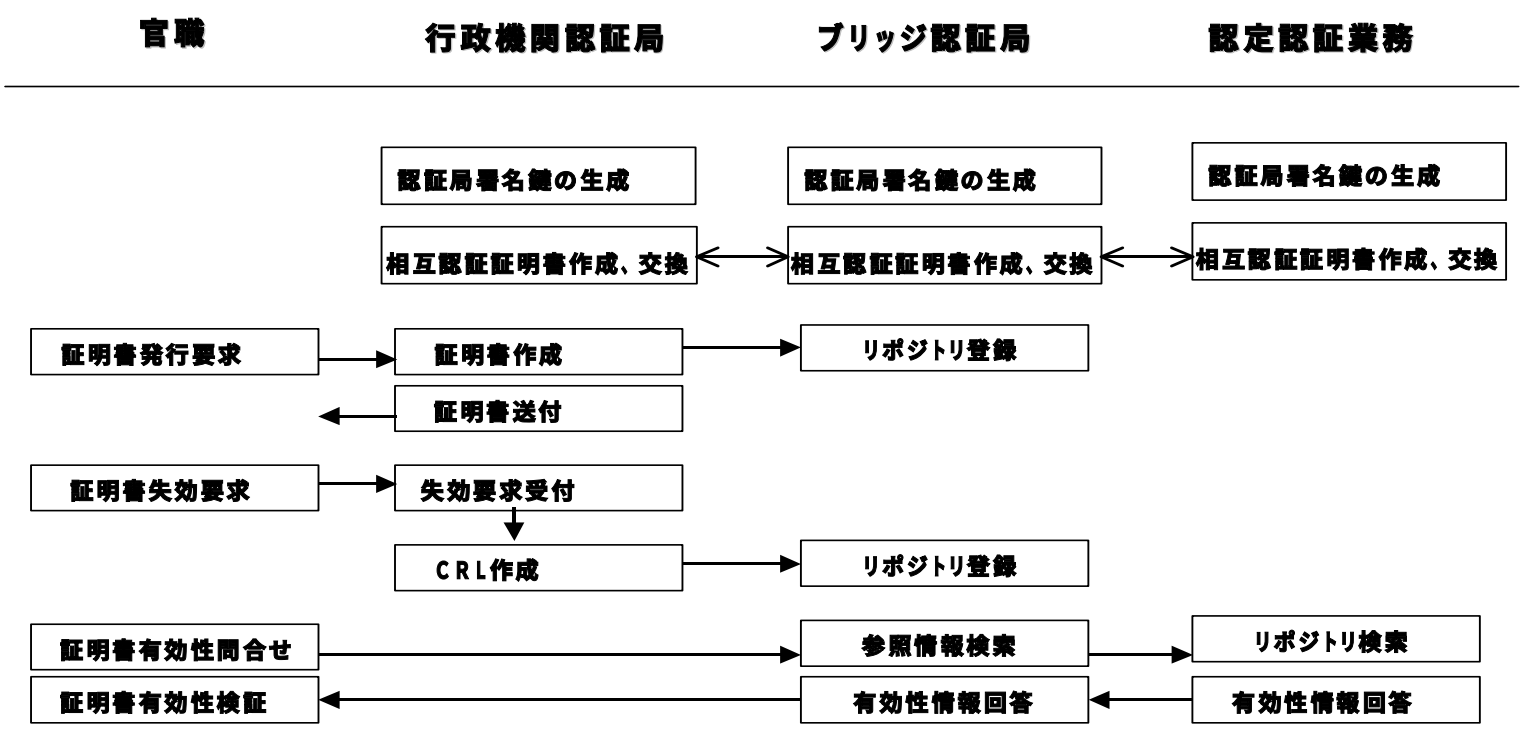
- 電子情報提供システムにおける処理は以下の3フェーズによって構成
  - 個人/法人が前もって利用者登録するフェーズ　（※ない場合もあり）
  - 個人/法人が情報を要求し、システムがそれを提供するフェーズ
  - 決済処理を行うフェーズ（外部システムとの連携など）



電子政府システムのモデル化（政府認証基盤）(1)



電子政府システムのモデル化（政府認証基盤）(2)



電子政府システムにおける暗号利用形態（1）

➢ 各システムのモデルから抽出した暗号利用形態

・認証＝相手認証
・通信は方向に関わらず同じ取り扱い
・完全性保証と否認防止＝署名
・通信と保管を同じ取り扱い

➢ 電子政府システムに共通の暗号利用形態

利用形態	
＜利用者側＞　認証	
利用者から政府への通信	鍵共有
	守秘
	完全性保証
	否認防止
政府から利用者への通信	鍵共有
	守秘
	完全性保証
	否認防止
＜政府側＞　認証	
政府側データ保管	守秘
	完全性保証
	否認防止

相手認証

被認証者の正当性を検証者が確認する機能

鍵共有

公開の通信路を用いて共通鍵暗号を利用する際、送受信者間で鍵情報を共有する機能

守秘

公開の通信路又は記録媒体を介して正当な利用者以外には知られないようにして、電子情報を共有する機能

署名

電子情報の正当性を確認する機能。署名作成者の確認と、電子情報自体の改ざんの有無の確認の両方の機能

電子政府システムにおける暗号利用形態 (2)

- 「相手認証」「鍵共有」「守秘」「署名」の各利用形態で用いられる暗号技術

暗号技術 / 利用形態	公開鍵暗号				共通鍵暗号			その他	
	認証	鍵共有	守秘	署名	ブロック暗号		ストリーム暗号	ハッシュ関数	擬似乱数生成
					64ビット	128ビット			
相手認証	○				○	○		○**	○
鍵共有		○						○	○
守秘			○		○	○	○	○	○
署名				○	○*	○*		○	○

* MACを想定　** キードハッシュ関数を想定

暗号技術に求められる要件 (1)

行政機関システム向けヒアリング、企業向けアンケート、海外電子政府システム調査等から得られた、要件調査WGとして、電子政府で利用される暗号が満たすべきと考える一般的要件

- **暗号強度が十分高い**

  10年間、電子政府システムで安心して使えること。

  【10年間の根拠】

  - システムの置き換え周期は4～5年であり、そのシステムが完全に置き換わるまでに更に1周期かかることから、最低でも10年間は安心して使いたいという要望がある。
  - 供給者としては、コンピュータ性能の向上や解読手法の出現等により、暗号の安全性を非常に長期にわたって保証することが困難。非常に長期間にわたる安全性を考慮して暗号を選択しようとすると調達コストの上昇を招く可能性がある。

暗号技術に求められる要件 (2)

- **一般に使われる商用ソフトに予め入っているか、入る可能性の高いものが最低限一つは選ばれること。**

  - 広く国民との間でやりとりを行うシステムにおいては、クライアント側でのインストールを必要としないか、最小限のインストールで済むなど、ユーザに負担を掛けない方が望ましい。

  - よって、一般に使われる商用ソフトにあらかじめ入っているか、入る可能性の高いものが最低限1つは選ばれること。

暗号技術に求められる要件 (3)

その他、満たしていることが望ましい要件

- 処理速度が速いこと
- ICカードへの実装性が優れていること
- 何らかの暗号標準又はプロトコル標準になっていること

推奨暗号数に関する考察

➢ 推奨暗号数に関する選択肢

(1) 分類別に1つに絞り込む
(2) 分類別に複数個 (2～3個) に絞り込む
(3) 分類別に基準をクリアしたものを全てリストアップする

➢ 検討にあたっての指標

1. 社会的混乱が生じないか
2. 省庁の調達者が困らないか
3. 電子政府システムユーザが困らないか
4. CRYPTRECでの公正な選出が困難でないか

➢ 要件調査WGの結論

(3) 分類別に基準をクリアしたものを全てリストアップする

- CRYPTRECの当初の目的である「安全性等で問題のある暗号を選択しないようにする」は(3)で十分達成可能。
- 調達者は、市場が絞り込んだ暗号とリストアップされた暗号の両方に入っているものを選択すれば良い。
- クライアント側では、商用ソフトに入っている暗号から選択すれば良い。

その他の提案

- 署名された文書の有効期間の制約
  - 署名向け暗号の安全な運用のためには、暗号の使用期間（暗号化後、破られない期間）をある程度絞り込み、署名付き文書を再発行するなどの仕組みが必要。
- 標準化対応の必要性
  - 推奨暗号に選ばれても、実際のシステムに採用されるためにはISO、IETF等でオーソライズすることも必要。
- プロトコル、製品評価の必要性
  - 暗号プロトコルや暗号製品に関する安全性評価に対するニーズは高いので、今後対応していくことが望ましい。