電子政府推奨暗号リストの活用方法について

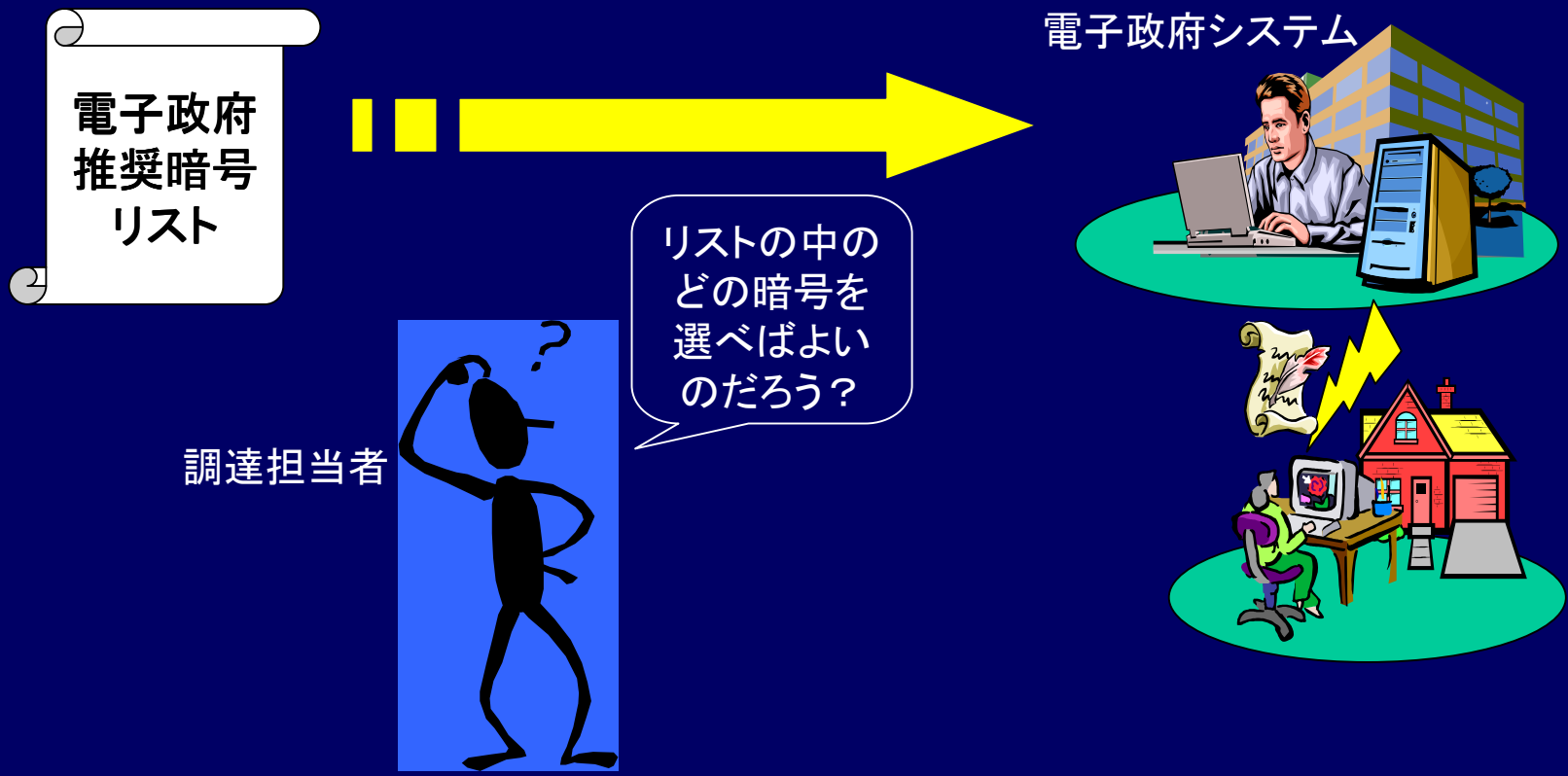
平成15年5月22日

暗号技術検討会
暗号調達ガイドブック作成WGリーダ
佐々木　良一（東京電機大学）

電子政府推奨暗号リストを用いた調達

電子政府推奨暗号リストの決定により、安全性及び信頼性に優れた暗号を電子政府システムに採用することが可能になった。

しかし、



調達対象システムにおける暗号の利用目的の抽出から、暗号アルゴリズムの選定までの手順を分かりやすく示す手引書が望まれる。

「暗号調達のためのガイドブック」の作成

- 各府省の調達担当者が、適切な電子政府推奨暗号を円滑に調達するための手引書として「暗号調達のためのガイドブック」を作成
- 暗号技術検討会の下に、暗号研究者、セキュリティの専門家、情報システムの専門家等から構成される「暗号調達ガイドブック作成ワーキンググループ」を設置
- ガイドブックの記述内容については、府省の調達担当者からのヒアリング結果を適宜反映
- また、全般にわたり、暗号技術評価委員会及び公開鍵暗号／共通鍵暗号評価小委員会の協力を得た。

暗号調達ガイドブックWG

・暗号アルゴリズム等に関する技術的評価の依頼
・その他、技術的事項に関する助言を求める

暗号技術検討会
（座長：今井秀樹 東京大学教授）
事務局：総務省、経済産業省

暗号技術評価委員会
（委員長：今井秀樹 東京大学教授）
事務局：通信・放送機構、
情報処理振興事業協会

・総務省及び経済産業省に対して暗号利用に関する助言を行う。
・電子政府における暗号利用に関する政策的判断を行う。
・具体的な暗号の評価依頼を行う。

・暗号アルゴリズム等に関する評価結果の報告
・その他、技術的事項に関する助言を行う

・具体的な技術的評価を行う
・電子政府における暗号利用に資する各種ガイドラインを作成する
・技術的事項に関する助言を行う

暗号調達ガイドブック作成WG
（リーダ：佐々木良一 東京電機大学教授）

共通鍵暗号評価小委員会
（委員長：金子敏信 東京理科大学教授）

公開鍵暗号評価小委員会
（委員長：松本 勉 横浜国立大学教授）

暗号調達ガイドブックWG　メンバー

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課企画役
	宇賀村直紀	社団法人電子情報技術産業協会 ITセキュリティセンター部長
	岡本　栄司	筑波大学電子・情報工学系教授
	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
	中村　逸一	株式会社NTTデータ　ビジネス開発事業本部 セキュリティ事業部　営業グループ部長
	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

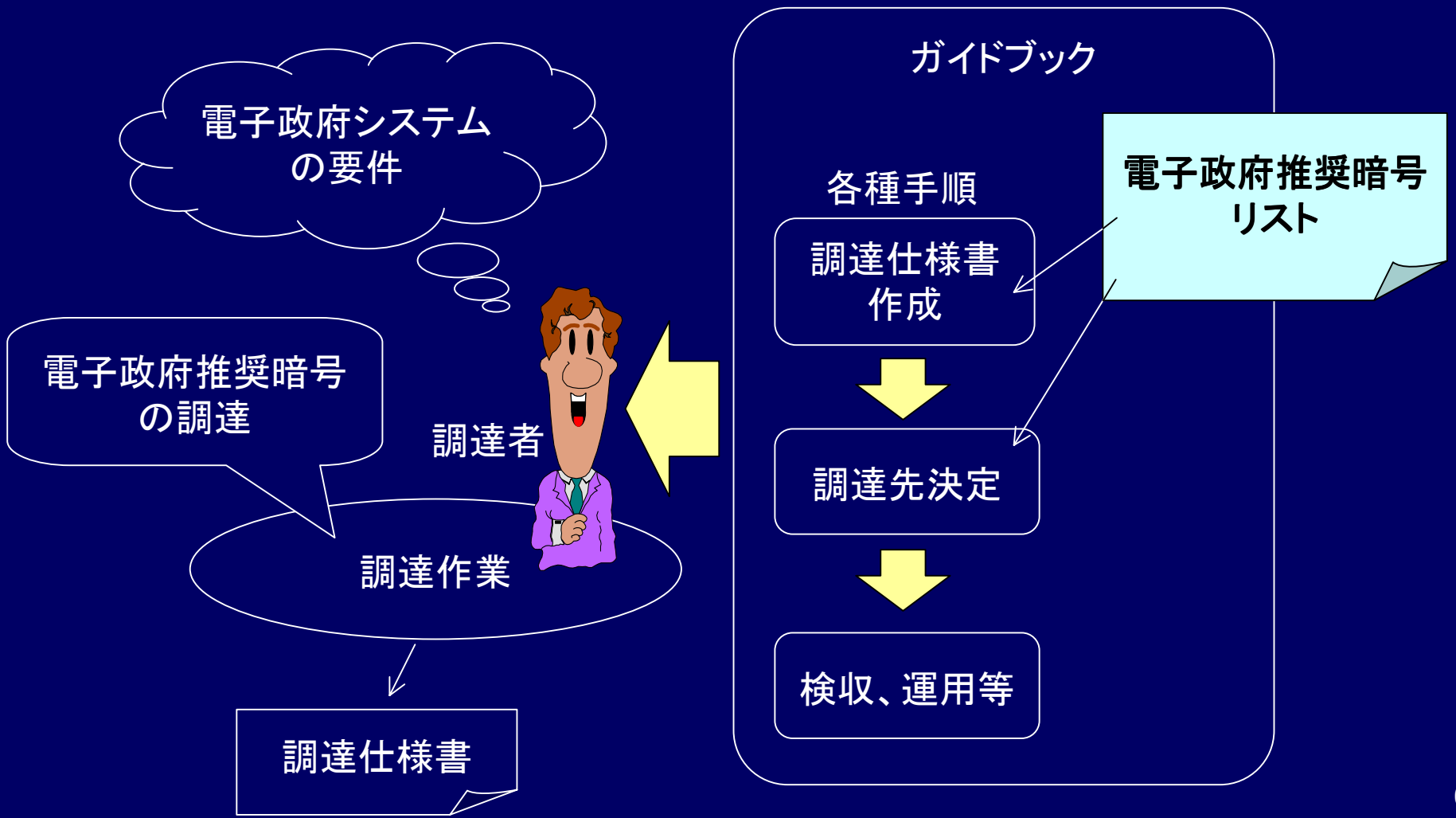
（敬称略）

ガイドブックの対象読者及び盛り込む内容

- 対象とする読者
  - 各府省における電子政府システムの調達担当者
  - 暗号やセキュリティに関する知識が豊富でない読者でも理解できるような記述レベルを目指した。
- 盛り込む内容
  - 暗号の利用目的の抽出から暗号アルゴリズムの選定までの手順の解説
  - 電子政府推奨暗号及び電子政府推奨暗号リストの解説
  - 調達仕様書作成にあたり、暗号に関連して留意すべき点

ガイドブックの位置付け

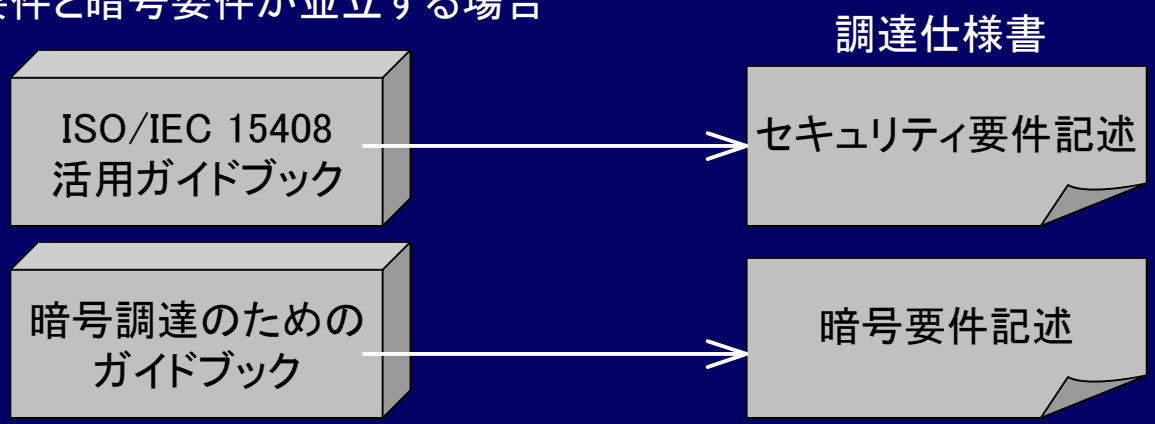
電子政府システムの調達担当者が、効率的に電子政府推奨暗号の調達を進められるよう、電子政府推奨暗号リストの利用手順や考え方等について説明



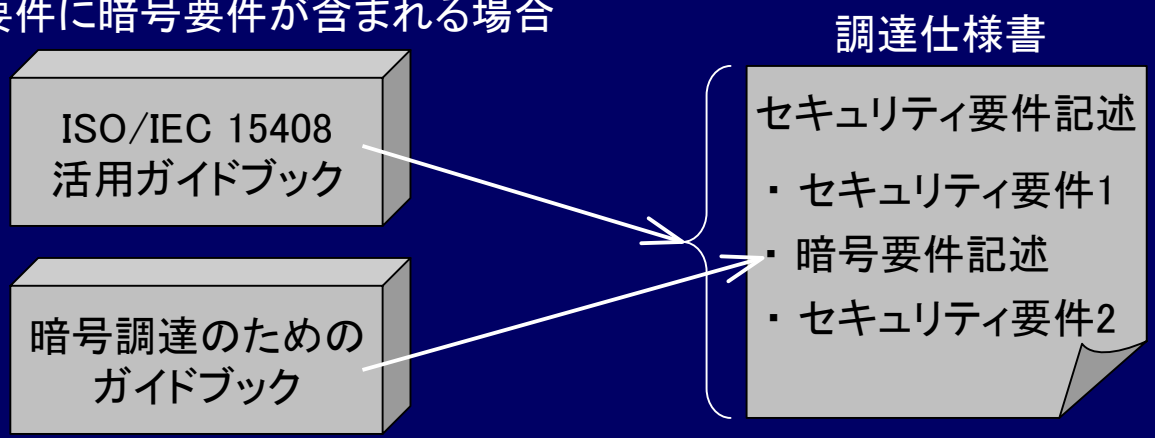
ISO/IEC 15408を活用した調達と暗号調達の関連

- ISO/IEC 15408では暗号技術の選択については触れていない。
- 「暗号調達のためのガイドブック」と「ISO/IEC 15408を活用した調達のガイドブック（経済産業省編）」を用いて電子政府システムの調達を行う際の、両ガイドブックの関係は以下のとおり。

● セキュリティ要件と暗号要件が並立する場合



● セキュリティ要件に暗号要件が含まれる場合



WGにおける検討方法

- 調達担当者及び情報システム担当者へのヒアリング

  ・システム調達（特に暗号調達）についての現状、及び、ガイドブックに対する要望を把握するため、各府省の調達担当者及び情報システム担当者にヒアリングを実施

  ・ガイドブック原案を作成した時点で、再びヒアリングを行い、記述内容に関するコメントを求めた。

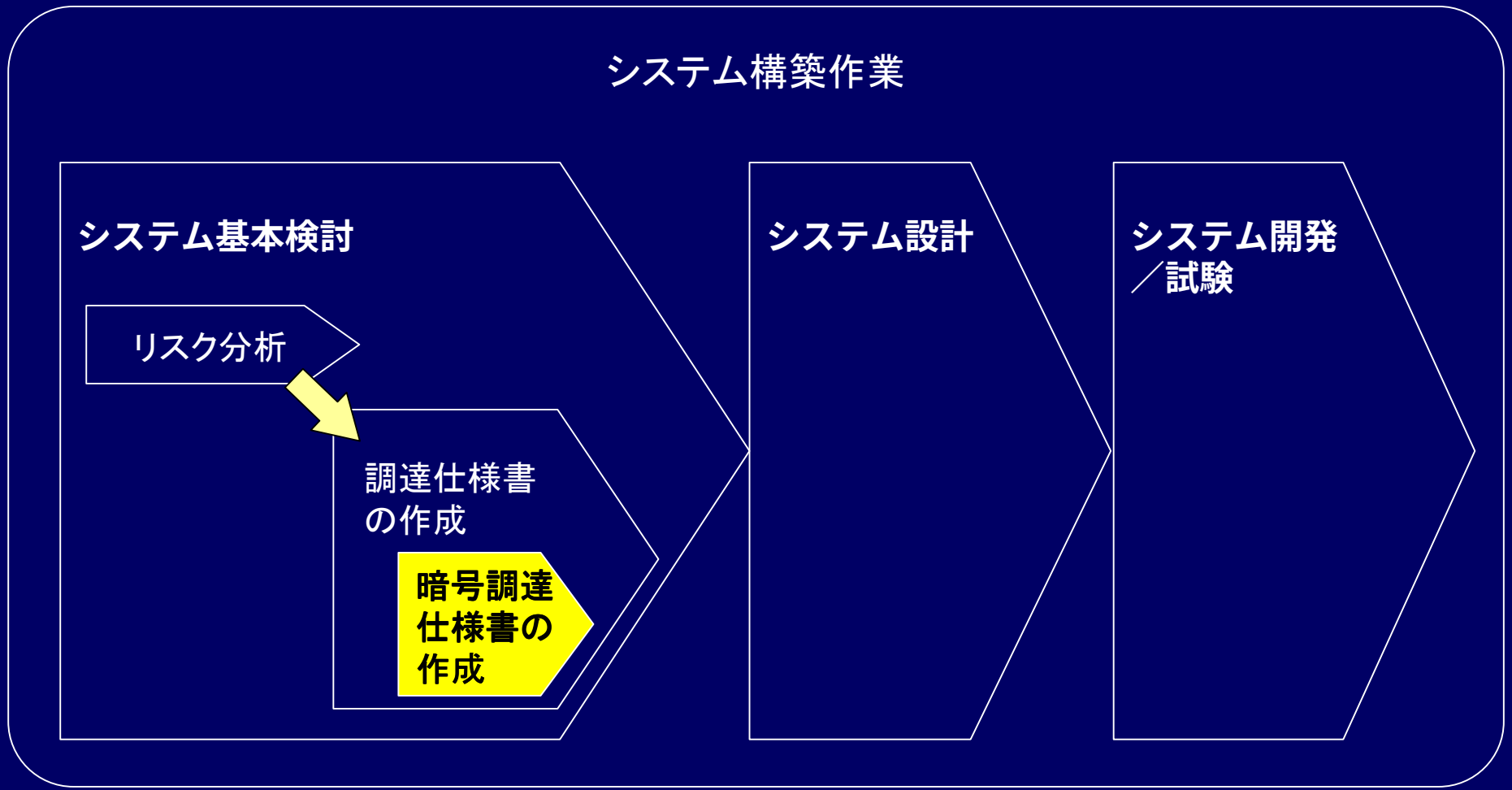
- 海外の電子政府事例に関する調査

  海外の電子政府システムにおける暗号調達ガイドラインの事例を調査

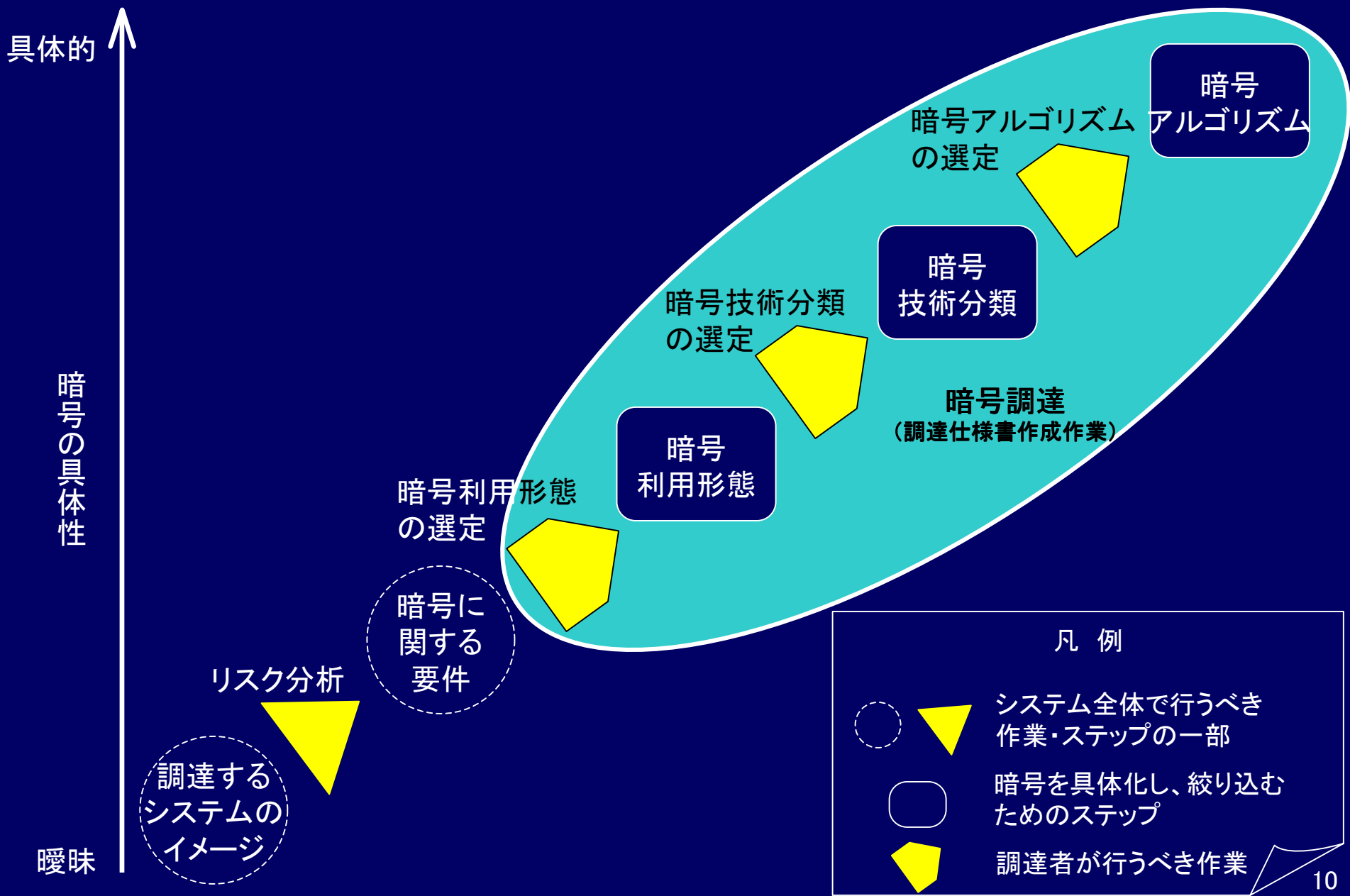
- 作業委員会による原案の編集

  ガイドブックWGの下に作業委員会を設置し、ヒアリング及び事例調査の結果等に基づいてガイドブック原案を作成（2002年6月～8月、計7回開催）

システム構築の作業全体に占める暗号調達の位置付け



暗号の具体化及び絞り込みのためのステップ



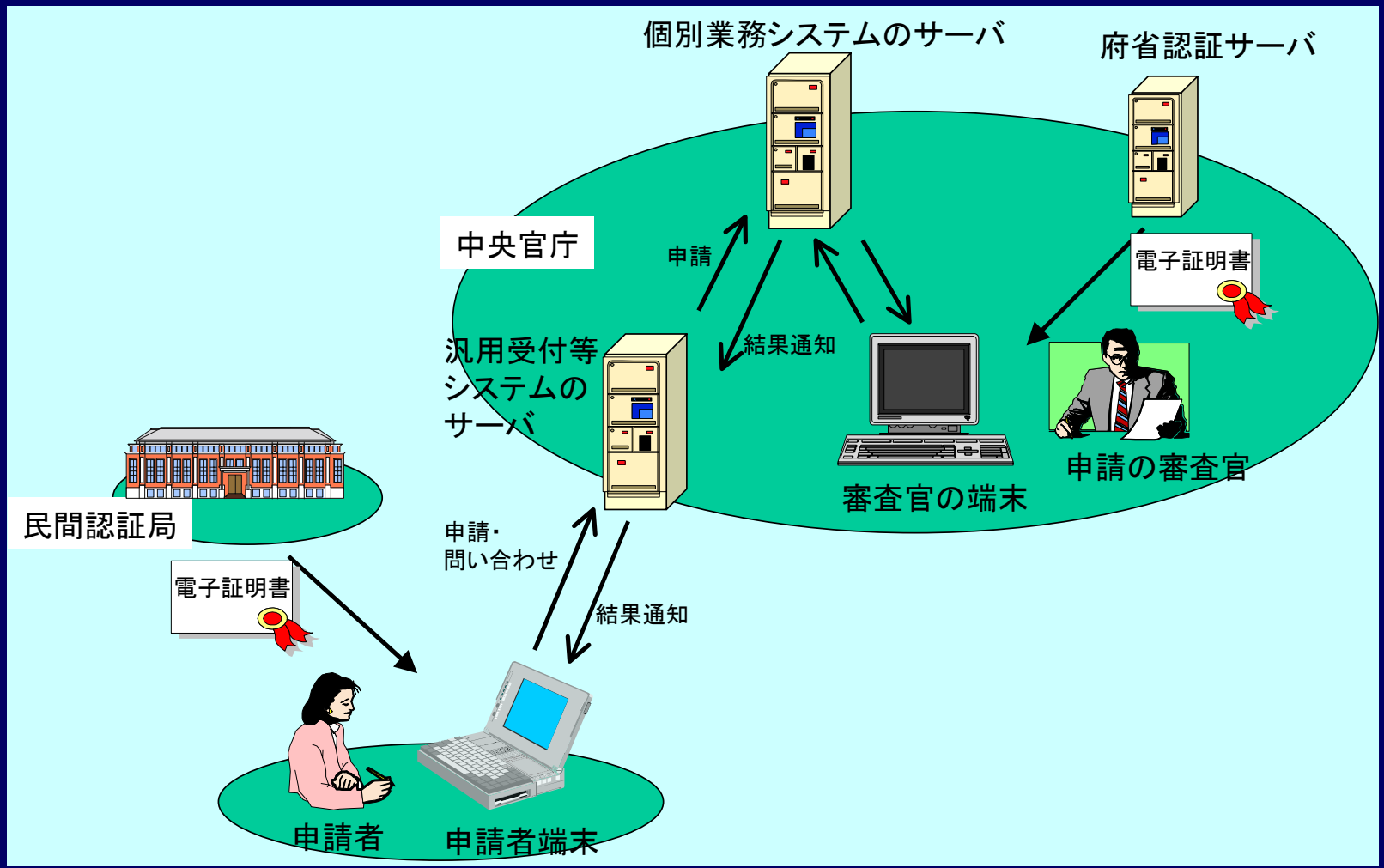
電子政府システム

（「e-Japan重点計画」「e-Japan重点計画 - 2002」より）

国の行政機関においては、行政の情報化により、事務・事業及び組織の改革を推進するとともに、セキュリティの確保に留意しつつ、「紙」による情報の管理から**ネットワークを駆使した電子化された情報の管理へ移行し、高度に情報化された行政、すなわち以下のような「電子政府」を実現**する。

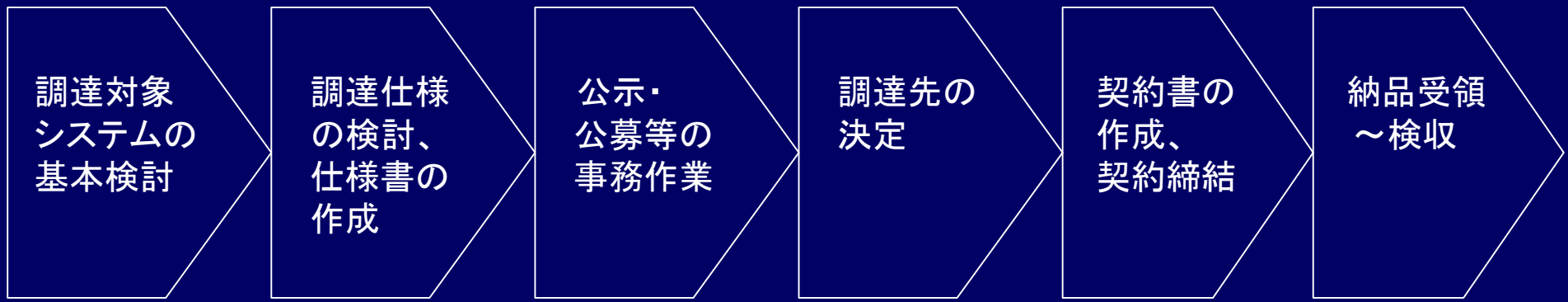
（主な項目）		（システム名）
・行政情報の電子的提供	→	**電子情報提供システム**
・申請・届出等手続の電子化	→	**電子申請システム**
・歳入・歳出の電子化	→	**電子納付システム**
・調達手続の電子化	→	**電子調達システム**
・ペーパレス化（電子化）		
※ほか、電子政府の共通基盤	→	**政府認証基盤（GPKI）**

システムモデルの例 （電子申請システム）



システム調達の流れ及び概要

【システム調達の流れ】



【概要】

- 調達を進める基本的事項の整理
- リスク分析、等

- システム要件の具体化検討
- 仕様書の作成

（必要に応じてパブコメ実施）

調達システムに適合する提案をした業者を選定

特記事項等を盛り込んで、契約書を作成、契約締結

システム受領、仕様と相違ないことを確認、検収

暗号調達の進め方

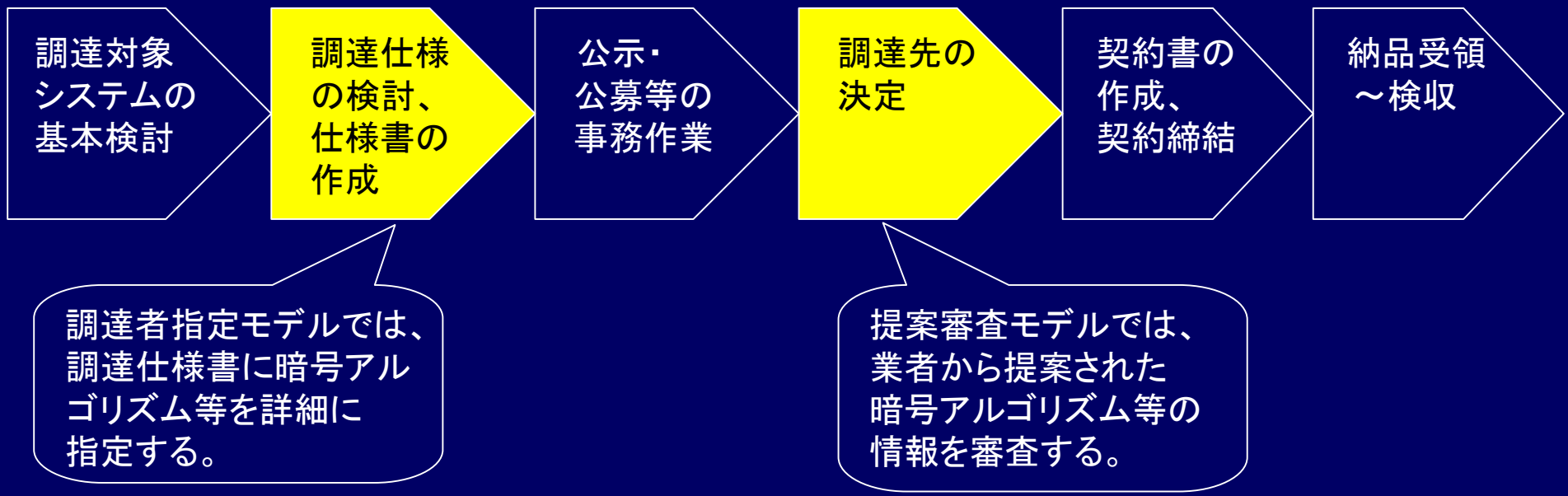
ガイドブックでは、暗号選定のための作業を以下の2通りに分類し、各々について解説した。

- 調達者指定モデル

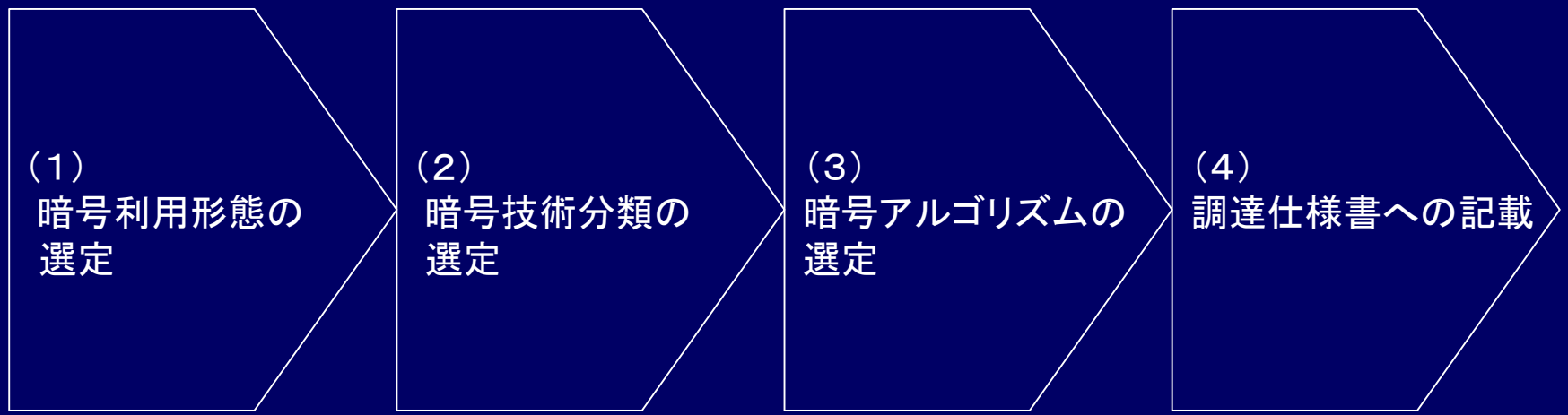
  調達仕様書作成時に、調達するシステムについて詳細に説明し、その中で、電子政府推奨暗号リストの中から暗号を選択する方法

- 提案審査モデル

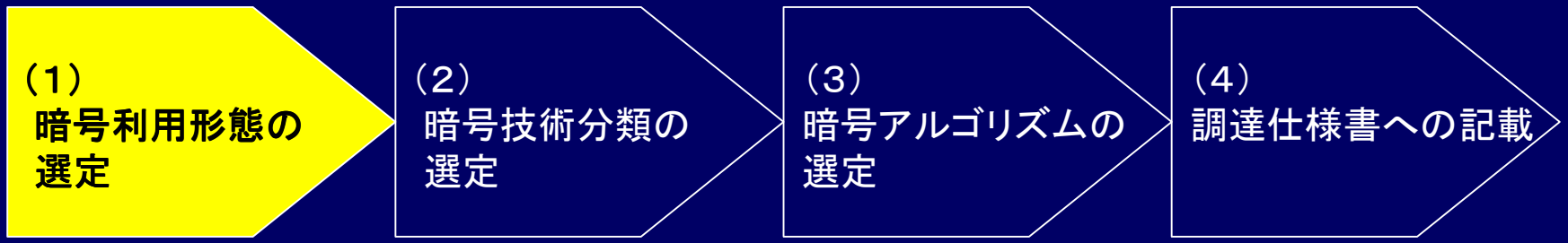
  調達仕様書では、暗号については概略を説明するに止め、業者に提案資料の中で電子政府推奨暗号リストの中から暗号を選択させ、それを審査する方法



「調達者指定モデル」による調達仕様書の作成



(1) 暗号利用形態の選定

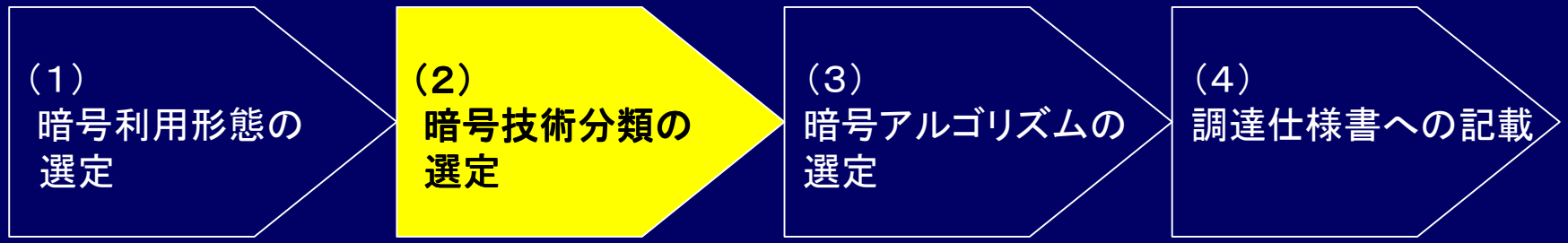


- 暗号利用形態 ： 電子政府システムにおける暗号の利用目的を整理、分類したもの
- 主な暗号利用形態は以下のとおり
  - ・相手認証　・鍵共有　・守秘　・署名
- 暗号による保護を必要とする情報に対応する暗号利用形態を選定する。

（暗号利用形態選定表のサンプル）※電子申請システムの場合

暗号による保護を必要とする情報	**暗号利用形態**	暗号技術への要件
・申請データ ・申請内容確認で授受されるデータ ・到達確認通知 ・状況確認で授受されるデータ ・審査終了通知 ・許認可等公文書の取得要求データ ・許認可等公文書	**・相手認証** **・署名** **・守秘**	・通信速度は、利用者の負担とならない程度の速度であること ・多くの利用者にとって、利用が負担とならないように、暗号アルゴリズムは標準的なものであることが望ましい。
（・鍵情報）	**（・鍵共有）**	（必要となったときのための欄）

(2) 暗号技術分類の選定

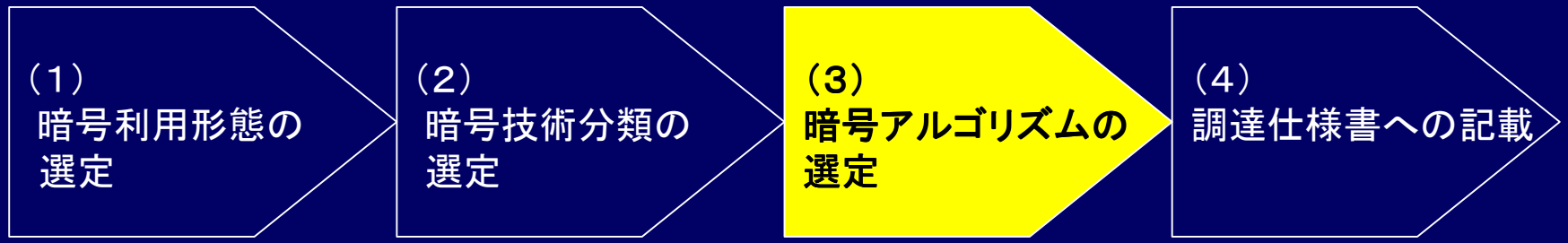


- 暗号技術分類：暗号アルゴリズムを機能的、技術的に類似するグループに分類したもの
- ガイドブックでは以下の4つに分類
  - ・公開鍵暗号　・共通鍵暗号　・ハッシュ関数　・擬似乱数生成系
- (1)で選定した暗号利用形態に対して適切と思われる暗号技術分類を選定する。

(暗号技術分類選定表のサンプル)※電子申請システムの場合

暗号による保護を必要とする情報	暗号利用形態	**暗号技術分類**	暗号技術への要件
・申請データ ・申請内容確認で授受されるデータ ・到達確認通知 ・状況確認で授受されるデータ ・審査終了通知 ・許認可等公文書の取得要求データ ・許認可等公文書	守秘	**共通鍵暗号**	・通信速度は、利用者の負担とならない程度の速度であること ・多くの利用者にとって、利用が負担とならないように、暗号アルゴリズムは標準的なものであることが望ましい。
	相手認証	**公開鍵暗号**	
	署名	**公開鍵暗号**	
(・鍵情報)	(・鍵共有)	**公開鍵暗号**	(必要となったときのための欄)

(3) 暗号アルゴリズムの選定



- (2)で選定した暗号技術分類に対して適切な暗号アルゴリズムを、電子政府推奨暗号リストから選択する。
- 主な留意点は以下のとおり。

（実装方法について）
- 実装方法に関しては、実装攻撃の脅威に対する十分な配慮、検討を行い、適切な実装を行うよう注意する必要がある。

（公開鍵暗号）
- 暗号利用形態に応じて、プロトコル標準への採用の有無等を考慮して選択する。
- 許容される処理速度の範囲内で使用される鍵長を長くする、等の検討が必要である。
- パラメータの選択に十分留意する必要がある。

（共通鍵暗号）
- 処理速度、メモリ制限環境での実装性、プロトコル標準への採用の有無等を考慮して選択する。
- ブロック暗号を採用する場合、今後は可能な限りブロック長128ビットのものを選択する。
- 暗号利用モードは、実装環境や利用用途に応じた適切なものを選択する。

など

(3) 暗号アルゴリズムの選定

（1）
暗号利用形態の
選定

（2）
暗号技術分類の
選定

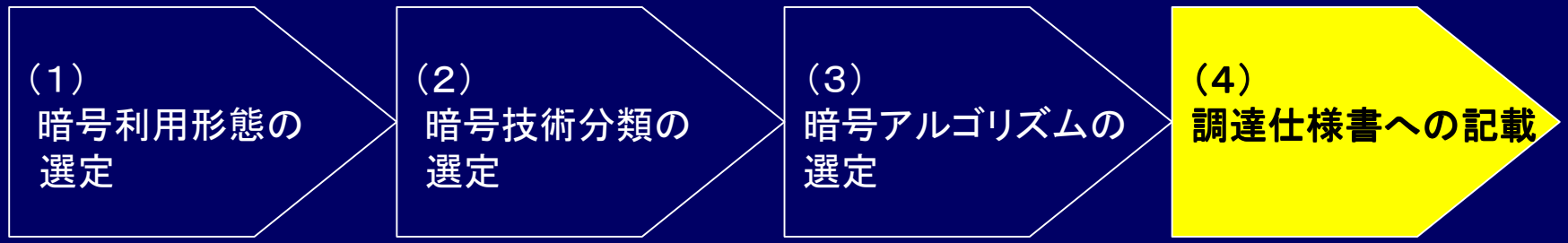
**（3）
暗号アルゴリズムの
選定**

（4）
調達仕様書への記載

（暗号アルゴリズム選定表のサンプル）※電子申請システムの場合

暗号による保護を必要とする情報	暗号利用形態	暗号技術分類	暗号アルゴリズム	暗号技術への要件
・申請データ ・申請内容確認で授受されるデータ ・到達確認通知 ・状況確認で授受されるデータ ・審査終了通知 ・許認可等公文書の取得要求データ ・許認可等公文書	守秘	共通鍵暗号	**共通鍵暗号その1**	・通信速度は、利用者の負担とならない程度の速度であること ・多くの利用者にとって、利用が負担とならないように、暗号アルゴリズムは標準的なものであることが望ましい。
	相手認証	公開鍵暗号	**公開鍵暗号その1 または 公開鍵暗号その3**	
	署名	公開鍵暗号	**公開鍵暗号その1 または 公開鍵暗号その3**	
（・鍵情報）	鍵共有	公開鍵暗号	**公開鍵暗号その2**	
上記暗号アルゴリズムにて特に指定のない場合は右記アルゴリズムを使用すること		ハッシュ関数	**ハッシュ関数その1**	
		擬似乱数生成	**擬似乱数生成その1**	

(4) 調達仕様書への記載



(調達仕様書に記載する暗号アルゴリズム指定表のサンプル) ※電子申請システムの場合

暗号による保護を必要とする情報	暗号利用形態	暗号技術分類	暗号アルゴリズム
・申請データ ・申請内容確認で授受されるデータ ・到達確認通知 ・状況確認で授受されるデータ ・審査終了通知 ・許認可等公文書の取得要求データ ・許認可等公文書	守秘	共通鍵暗号	共通鍵暗号その1
	相手認証	公開鍵暗号	公開鍵暗号その1 または 公開鍵暗号その3
	署名	公開鍵暗号	公開鍵暗号その1 または 公開鍵暗号その3
(・鍵情報)	鍵共有	公開鍵暗号	公開鍵暗号その2
上記暗号アルゴリズムにて特に指定のない場合は右記アルゴリズムを使用すること		ハッシュ関数	ハッシュ関数その1
		擬似乱数生成	擬似乱数生成その1

「提案審査モデル」による調達仕様書の作成

「提案審査モデル」により調達仕様書を作成する場合、暗号に関して以下のような指示を行う。

- 電子政府推奨暗号リストに掲載されている暗号の使用に関する指示

  調達するシステムでは、可能な限り、電子政府推奨暗号リストに記載されている暗号アルゴリズムを使用するよう、提案を行う業者に指示する。

- 暗号アルゴリズム選定理由の明記に関する指示

  暗号アルゴリズムの選定（公開鍵暗号のパラメータ選択、及び、共通鍵ブロック暗号の利用モードの選択を含む）が妥当であるか否かを審査するため、調達するシステムのイメージから暗号アルゴリズムの選定までの過程を、理由を付けて分かりやすく説明した文書を提案書に添付するよう、提案を行う業者に指示する。

複数の暗号を実装する場合の留意点

- 複数暗号実装のメリット

  電子政府推奨暗号に関して解読問題が発生する可能性は低いものの、1つの暗号が解読された場合に備えて複数の暗号を実装し、切り替えられるようにすることは、セキュリティを向上する上で有効である。

- 複数暗号実装のデメリット

  複数の暗号を同じシステムに実装し、これを切り替えて利用できるように作り込む場合、切り替え部分にセキュリティホールが混入する恐れがある。そのため、脆弱性が上昇する可能性がある。

- 対応策

  したがって、セキュリティ脆弱性の上昇により懸念されるリスクが、暗号が解読されるリスクに比べて小さいと判断された場合にのみ、複数暗号を実装すべきである。

※ なお、広く国民が利用するシステムにおいて、利用者（国民）側の暗号を全体として1つに特定できない場合などには、政府側のサーバで複数の暗号をいずれも扱えるようにしておかなければならない。このような場合、セキュリティホールを作り込まないよう、十分な配慮をしつつ複数の暗号を実装しておくことが、利用者の利便性を向上させる上でも望ましい。

暗号プログラムの配布と暗号輸出規制

- 不特定多数の利用者に、暗号機能を含むプログラムを配布する(*)ことは、外国為替及び外国貿易法による規制がある。

  (*) 例えば、政府が管理するサーバ上のホームページ等において、暗号アルゴリズムを含む通信プログラムを公開し、不特定多数の利用者が自由にそのプログラムをダウンロードし、使用できるようにすること

- 調達者は、不特定多数の利用者に通信プログラムを配布しないで済むよう配慮するか、配布する場合は、その通信プログラムが、以下の3点を満たしている必要がある。
  - 市販製品(購入に際して何ら制限されず販売されるもの)をそのまま組み込むか、プログラムが無償で提供されること
  - 暗号機能が利用者によって変更できないこと
  - プログラム使用に際して技術支援が不要であるように設計されていること

- 詳細は、「外国為替及び外国貿易法」、「外国為替及び外国貿易法第25条第1項第1号の規定に基づき許可を要する技術を提供する取り引きについて(役務通達)」等を参照のこと。

電子政府推奨暗号の評価・特徴一覧

電子政府推奨暗号に選定された全ての暗号について、以下の情報を一覧表にして掲載

- 安全性に関するコメント（リストに載せた根拠）
- ソフトウェア実装性能（共通鍵暗号、ハッシュ関数、擬似乱数生成系）
- 主なパラメータや補助関数に関する要件
- 国際標準等への採用状況
- 提案元が保有する知的財産権の実施の権利に関する考え方
- その他特記事項　　等

関連資料

- 暗号技術検討会2002年度報告書

（総務省ホームページ）
http://www.soumu.go.jp/s-news/2003/pdf/030331_4_1.pdf

（経済産業省ホームページ）
http://www.meti.go.jp/policy/netsecurity/index.html

- 暗号技術評価報告書（2002年度版） CRYPTREC Report 2002

（通信・放送機構ホームページ）
http://www.shiba.tao.go.jp/kenkyu/CRYPTREC/fy15/cryptrec200304_report02.html

（情報処理振興事業協会ホームページ）
http://www.ipa.go.jp/security/enc/CRYPTREC/fy15/cryptrec20030401_report01.html

問い合わせ先

- 「暗号調達のためのガイドブック」に関する問い合わせ先

  総務省 情報通信政策局 通信規格課
  cryptrec-inq@soumu.go.jp

  経済産業省 商務情報政策局 情報政策ユニット 情報セキュリティ政策室
  it-security@meti.go.jp

- 暗号に関する技術的な問い合わせ

  通信・放送機構（TAO） 研究企画管理部 研究企画課
  cryptrec@shiba.tao.go.jp

  情報処理振興事業協会（IPA） セキュリティセンター 暗号技術グループ
  cryptrec@ipa.go.jp