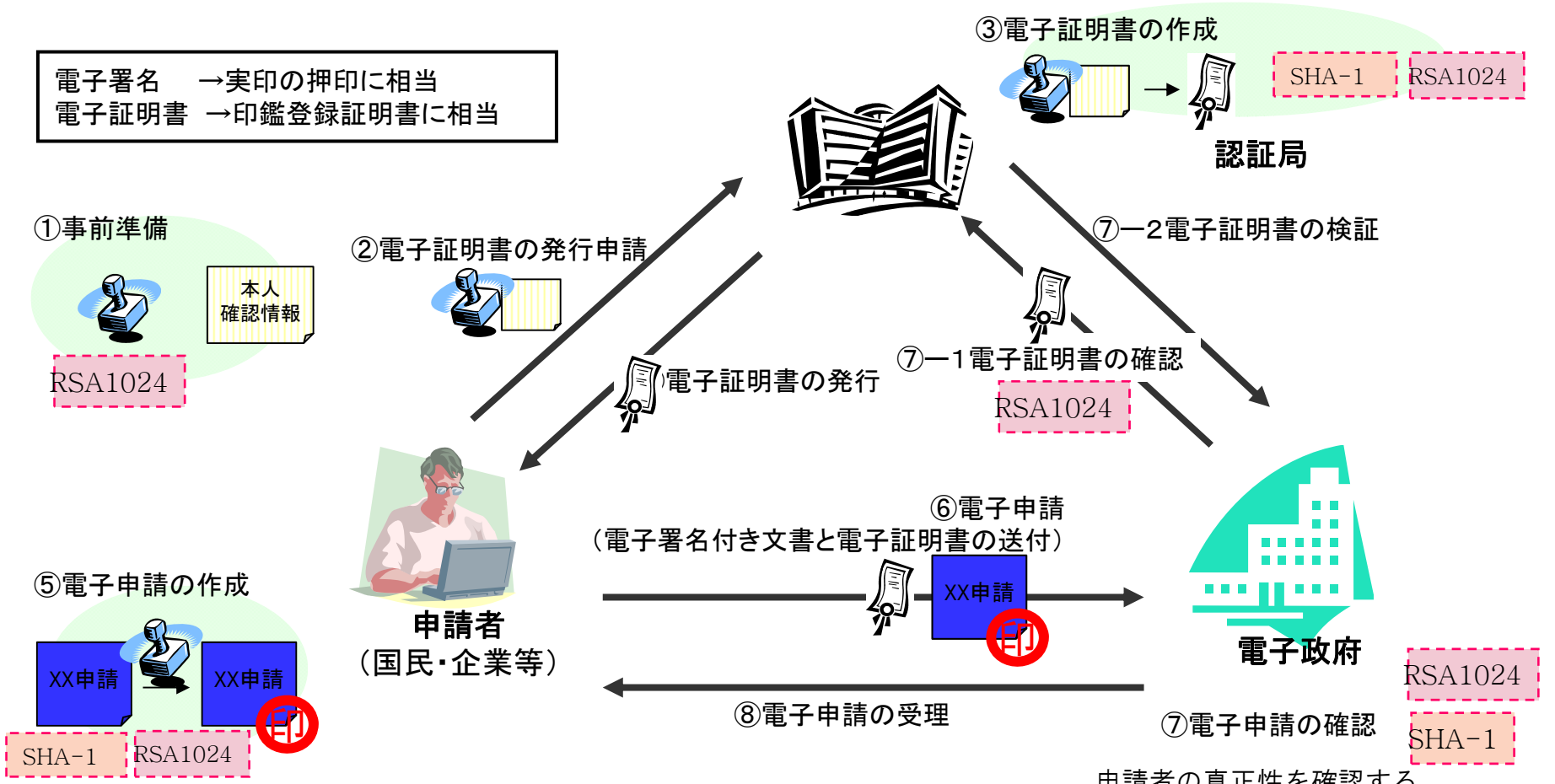
Research Center for Information Security

日本におけるRSA1024・SHA-1の移行に関する施策

（独）産業技術総合研究所
情報セキュリティ研究センター
山口（繁富）利恵

電子政府の一例(SHA-1及びRSA1024暗号の利用)

電子署名　→実印の押印に相当
電子証明書　→印鑑登録証明書に相当



電子申請や電子入札などにおいて，

- 申請者本人により作成された申請書であることを示す
- 申請者が申請した内容に相違ないことを担保する（情報の完全性）

申請者の真正性を確認する

- 本人が存在することを確認し，本人が実印に相当する鍵の持ち主であることを確認する．（印影照合）

我が国の戦略

- 2001年1月 e-Japan 戦略

「我が国は、すべての国民が情報通信技術（IT）を積極的に活用し、その恩恵を最大限に享受できる知識創発型社会の実現に向け、早急に革命的かつ現実的な対応を行わなければならない。市場原理に基づき民間が最大限に活力を発揮できる環境を整備し、５年以内に世界最先端のIT国家となることを目指す。」

この実現として・・・

- ミレニアム・プロジェクト「電子政府の実現」

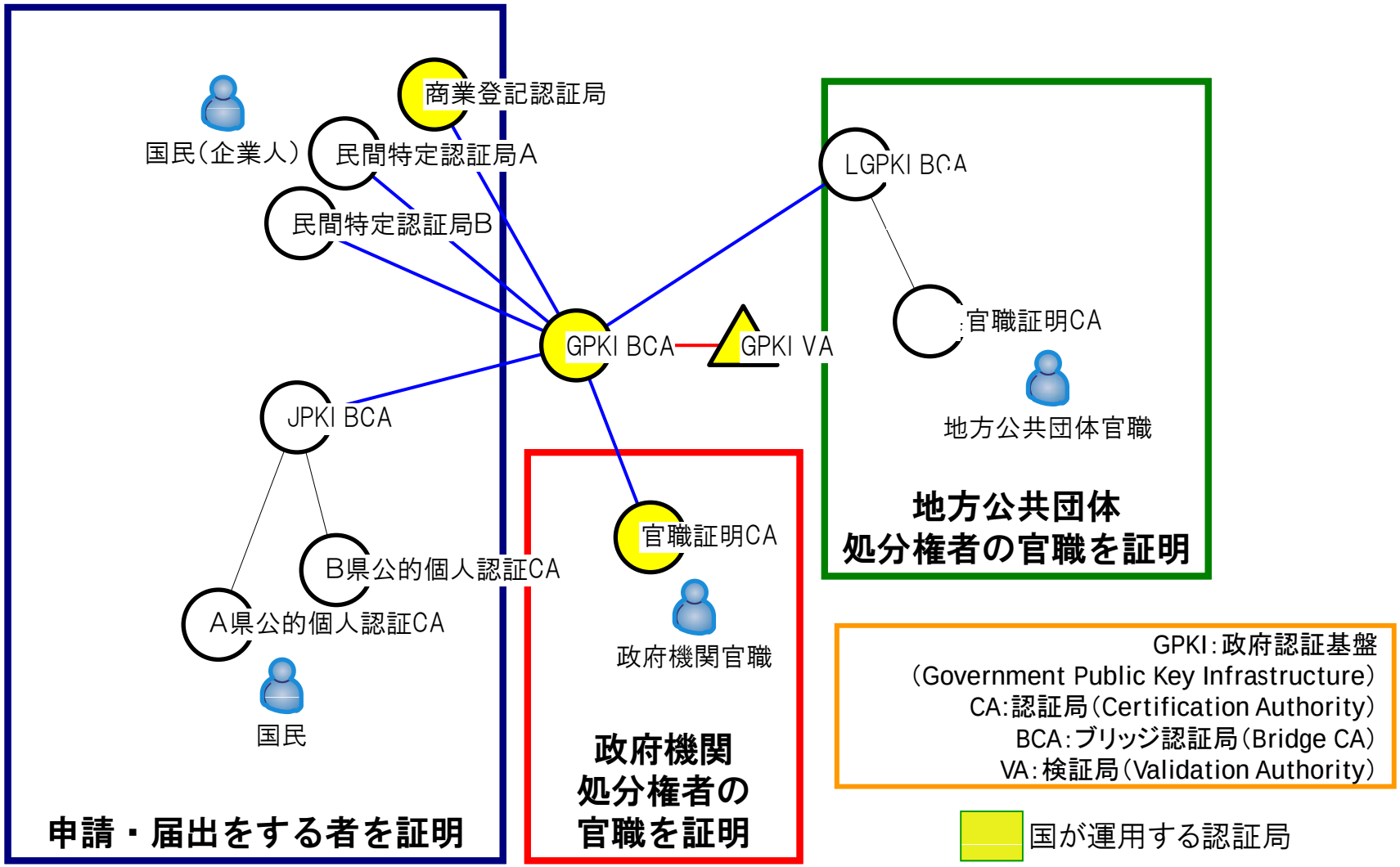
「2003年度までに、民間から政府、政府から民間への行政手続きをインターネットを利用してペーパーレスで行える電子政府基盤を構築する。」

我が国の認証基盤

- 公開鍵暗号に基づく認証基盤PKIの採用
  - オンラインでの電子申請における本人認証の仕組みとして採用。電子政府のための認証基盤の構築。

- 日本政府が運営するブリッジ認証局を相互認証のハブとして:
  - GPKI 政府認証基盤　…　官職証明等を認証
  - JPKI 公的個人認証サービス　…　住民基本台帳を基礎に置き、国民を認証
  - 商業登記認証局　…　商業登記認証局を基礎に起き、法人代表者等を認証
  - 民間認証局　…　電子署名法に基づいて、民間事業者が運営する認証局

各認証局と政府認証基盤(GPKI)ブリッジCAによる相互認証



暗号危殆化とその影響

- 米国政府の暗号移行
  - 2004年から、RSA1024やSHA-1に関して2010年末を期日に移行の取り組みを進めている。

⇨ 暗号の2010年問題

- 日本においては？
  - RSA1024やSHA-1が利用されているため、米国同様の移行が求められる。
  - CRYPTRECによって、2004年に暗号の移行の必要性について指摘があった。
  - 危殆化が起きた場合には、例えば、電子入札システムにおける入札金額の詐欺や、電子申請におけるなりすましなどが考えられる。
  - 一方、黄色い〇だけが、国が運営する認証局であり、一緒くたに移行、とは行かない。
  - アプリケーションシステム（e-taxシステム）、ICカード、利用者システムの移行も必要。

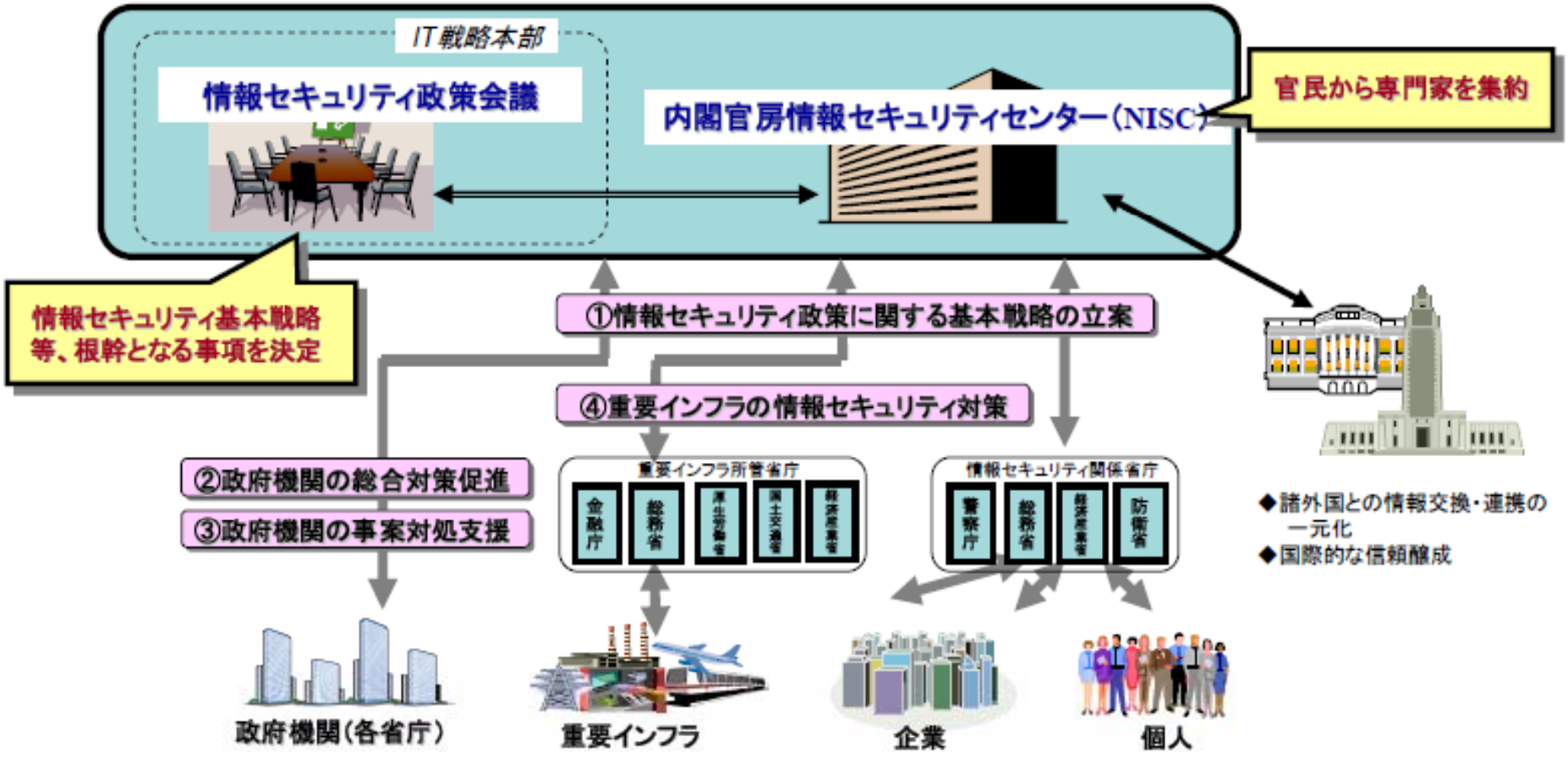
⇨ それぞれの影響や負担を抑えスムーズに移行するためには、関係者間の密接な連携及び慎重な移行計画の策定が求められる。

NISC ホームページより

情報セキュリティ政策会議及び内閣官房情報セキュリティセンター(NISC)の設置

NISC

- 「情報セキュリティ問題に取り組む政府の役割・機能の見直しに向けて」(2004年12月7日IT戦略本部決定)を受け、情報セキュリティ問題に関する政府中核機能の強化に向けて機能・体制等を整備中
  - 2005年4月25日、内閣官房情報セキュリティセンター(NISC:National Information Security Center)を設置
  - 2005年5月30日、IT戦略本部の下に「情報セキュリティ政策会議」を設置



NISC ホームページより

情報セキュリティ政策の推進体制

内閣官房を中心に関係省庁も含めた横断的な体制を整備

高度情報通信ネットワーク社会推進戦略本部（IT戦略本部）

本部長　内閣総理大臣
副本部長　内閣特命担当大臣（科学技術政策）
内閣官房長官
総務大臣
経済産業大臣
本部員　本部長及び副本部長以外のすべての国務大臣
民間有識者（8人）

（事務局）
内閣官房IT担当室
室長（官房副長官補（内政））

情報セキュリティ政策会議　（2005年5月30日　IT戦略本部長決定により設置）

議長　内閣官房長官
議長代理　内閣府特命担当大臣（科学技術政策）
構成員　国家公安委員会委員長
総務大臣
経済産業大臣
防衛大臣
→ 関係が参画

小野寺　正　KDDI株式会社代表取締役社長兼会長
黒川　博昭　富士通株式会社相談役
土屋　大洋　慶應義塾大学大学院准教授
野原　佐和子　株式会社イプシ・マーケティング研究所代表取締役社長
前田　雅英　首都大学東京法科大学院教授
村井　純　慶應義塾大学教授

（事務局）
内閣官房情報セキュリティセンター（NISC）
センター長（官房副長官補（安危））
副センター長（内閣審議官）2名
内閣参事官5名

協力

協力4省庁
- 警察庁（サイバー犯罪の取締り）
- 総務省（通信・ネットワーク政策）
- 経済産業省（情報政策）
- 防衛省（国の安全保障）

その他の関係省庁
- 重要インフラ所管省庁
  - 金融庁（金融機関）
  - 総務省（地方公共団体、情報通信）
  - 厚生労働省（医療、水道）
  - 経済産業省（電力、ガス）
  - 国土交通省（鉄道、航空、物流）
- その他
  - 文部科学省（セキュリティ教育）　等

重要インフラ事業者　等

政府機関（各府省庁）

企業

個人

移行指針の策定方針

- 移行指針には3つのポイント:

【移行対象】政府機関においてPKIを利用するシステム及び組織は広範に渡り、移行にはある程度の年数を要すると予想されることから、SHA-1の数年遅れではあるものの同様に危殆化が予想されるRSA1024をSHA-1と同時に移行すること。

【移行方法】実効性を確保するため、移行後に用いるアルゴリズムについては、製品化等の実績を重視する等して移行の確実性を高めること。

【移行期日】暗号移行のみのための追加的なシステム更改は非合理的であり、また利用者及び利用システムがかなり多いことから、各システムが従来から予定している更改時の対応及び利用者側の円滑な移行を考慮した移行期日とすること。

政府機関の暗号移行に関する経緯

- 平成20年2月4日　第16回情報セキュリティ政策会議
  - 政府機関の情報システムにおいて使用されている暗号アルゴリズムSHA-1及びRSA1024に係る移行指針 （案）について審議を実施，パブリックコメントに付すことを決定.
  - その際，構成員から「移行した暗号自体の安全性の監視も重要である」等の意見もあり，パブリックコメントとともに検討することとした.

- 平成20年2月4日～3月7日 パブリックコメント
  - パブリックコメント総数　：　14件【内訳　企業・団体・大学　：　14件，　個人　：　0件】
  - 施策実施にあたっての配慮・要望として，民間との協調や2008年度の具体的検討に当たっての要望等について意見の提出あり.
  - 2008年度における検討事項に対するコメント等の理由により，**文章の修正に至らず.**
  - **移行した暗号自体の安全性の監視について，指針に追加.**

- 平成20年4月22日 第17回情報セキュリティ政策会議
  - 政府機関の情報システムにおいて使用されている暗号アルゴリズムSHA-1及びRSA1024に係る**移行指針を決定**

- 平成21年2月3日　第20回情報セキュリティ政策会議
  - 政府機関の情報システムにおける**X-dayを2014年度早期、Y-dayを2015年度早期とした**が、政府機関以外との調整があるため、引き続き状況の確認を行っているところ

移行指針概要(技術)

- 【政府認証基盤とそれに依存する各府省庁の情報システム】
  - 相互運用性確保のため，新旧暗号方式の双方に対応し，適切な時期に暗号方式を切り替える運用を可能に.
  - 新たな暗号方式として，SHA-256及びRSA2048を採用.
  - 移行完了前に安全性低下の影響が発生する場合に備え，緊急避難的な対応も想定.

- 【上記以外の情報システム】
  - 現実的な脅威となる攻撃手法が示された時点で，速やかに別の暗号方式に変更する等の対応措置を可能とする.
  - 新たな暗号方式は，より安全なものを各府省庁において判断し決定する.

- Webのサイト証明書に関しての移行は範囲外
  - あくまでも政府機関で運営している認証局及び認証基盤に関わる暗号移行.

移行指針概要(制度、スケジュール)

- 制度的な対応
  - システムの移行時期を踏まえ，必要な対応の取りまとめ
  - 移行手順書の整備

- 移行に関わるスケジュール
  - 内閣官房，総務省，法務省，経済産業省等
    - 新たな暗号方式へ切り替える時期等を2008年度中に検討.
  - 内閣官房，総務省等
    - 相互接続の技術要件，緊急避難対応等について2008年度中に検討.
  - 各府省庁
    - 2010年から2013年までの間に，各情報システムの対応を完了.
  - 内閣官房，総務省，経済産業省
    - 安全性の状況を監視し，必要な情報を速やかに各府省庁に提供.

（参考）移行指針より抜粋

(2) 計画等の策定

ア 各府省庁は，(1)に定める暗号アルゴリズムの安全性向上に必要な対応について，情報システム全体の更改前の部分的な実施も検討した上で，情報システムごとの移行時期を踏まえ，必要となる対応を2008年度中にとりまとめる．

イ 既に発行済みの電子署名付き文書ファイル及び電子証明書について，暗号アルゴリズムの移行に伴い，失効，再発行等の対応が必要となる場合に備え，それぞれの手続きごとに，当該対応に係る手順書の整備等必要な措置を講ずる．

ウ 新たな暗号アルゴリズムへの移行が完了する以前に，SHA-1又はRSA1024の安全性の低下による影響が発生する状況に備え，情報システムの停止等に伴う国民への影響を最小限とするために必要な措置を講ずる．

(3) スケジュール

ア 各府省庁は，(2)アにおいて取りまとめた内容の概要について，2008年度中に内閣官房に報告する．

イ 内閣官房，総務省，法務省，経済産業省及び関係府省庁は，アの報告等を基に，新たな暗号アルゴリズムへの切替時期並びにSHA-1及びRSA1024の使用停止時期について，2008年度中に検討する．

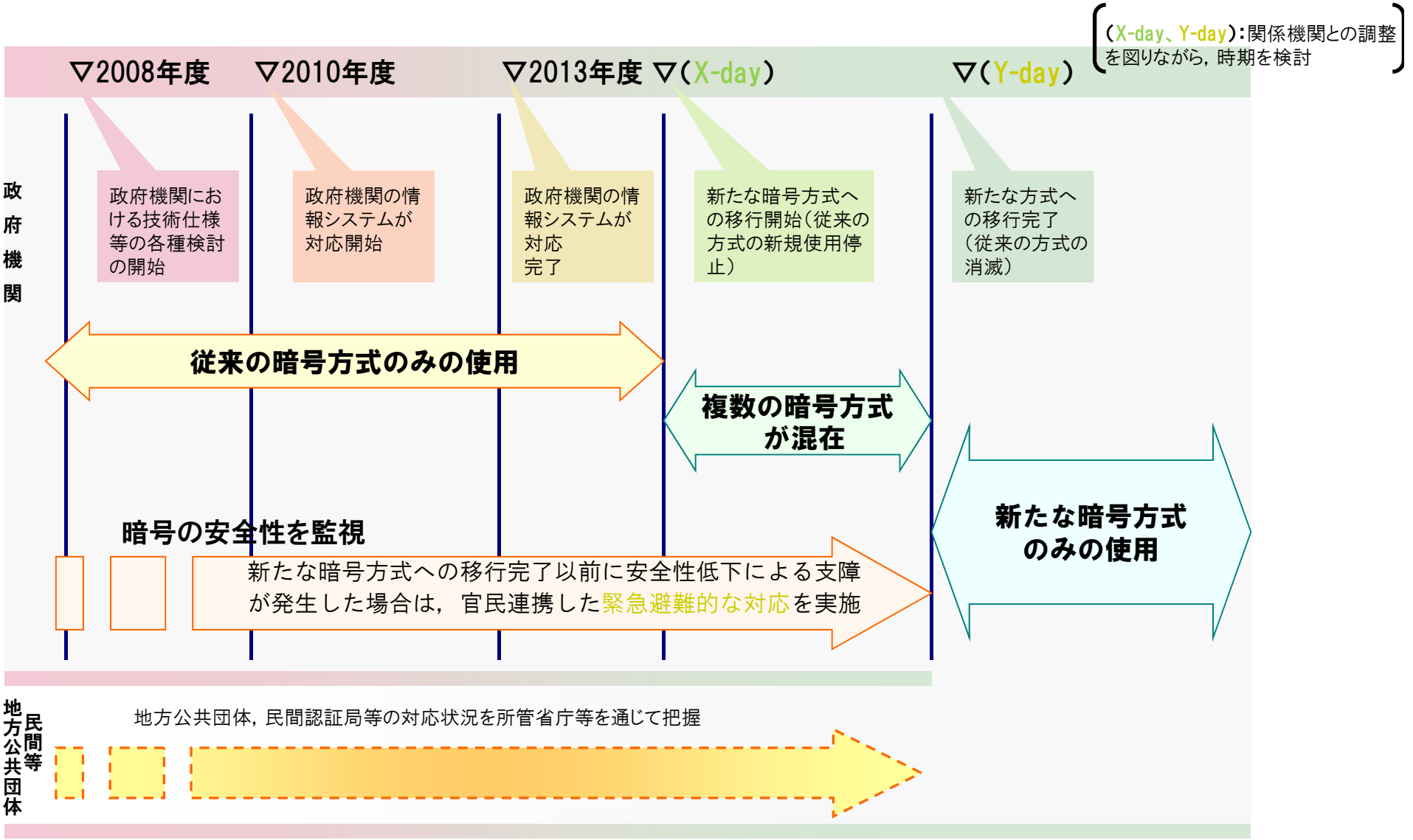
ウ 内閣官房，総務省及び関係府省庁は，政府認証基盤と他の認証局との相互接続に必要となる技術要件及び新たな暗号アルゴリズムへの移行が完了する以前に安全性の低下による影響が発生する状況に備えた官民共同の電子証明書の失効等の仕組みについて，2008年度当初に検討に着手する．

エ 内閣官房，総務省及び関係府省庁は，新たな暗号アルゴリズムに対応した情報システムの相互運用性の検証を可能とする環境の整備について2008年度当初に検討に着手し，2009年度の構築を目指す．

オ 各府省庁は，上述の検討結果を踏まえ，原則として，2010年度に新規に構築（更改を含む．以下同じ．）する情報システムから3(1)の設計要件を組み入れ，2013年度までに各情報システムを当該要件に適合させるものとする．ただし，2009年度に構築する情報システムについては，3(1)ウの仕様を適用する．

カ 総務省及び経済産業省は，現在使用されているSHA-1及びRSA1024並びに新たに使用するSHA-256及びRSA2048の安全性について監視し，内閣官房は，必要な情報を速やかに各府省庁に提供する．

移行指針に基づく暗号方式の移行完了までのスケジュール



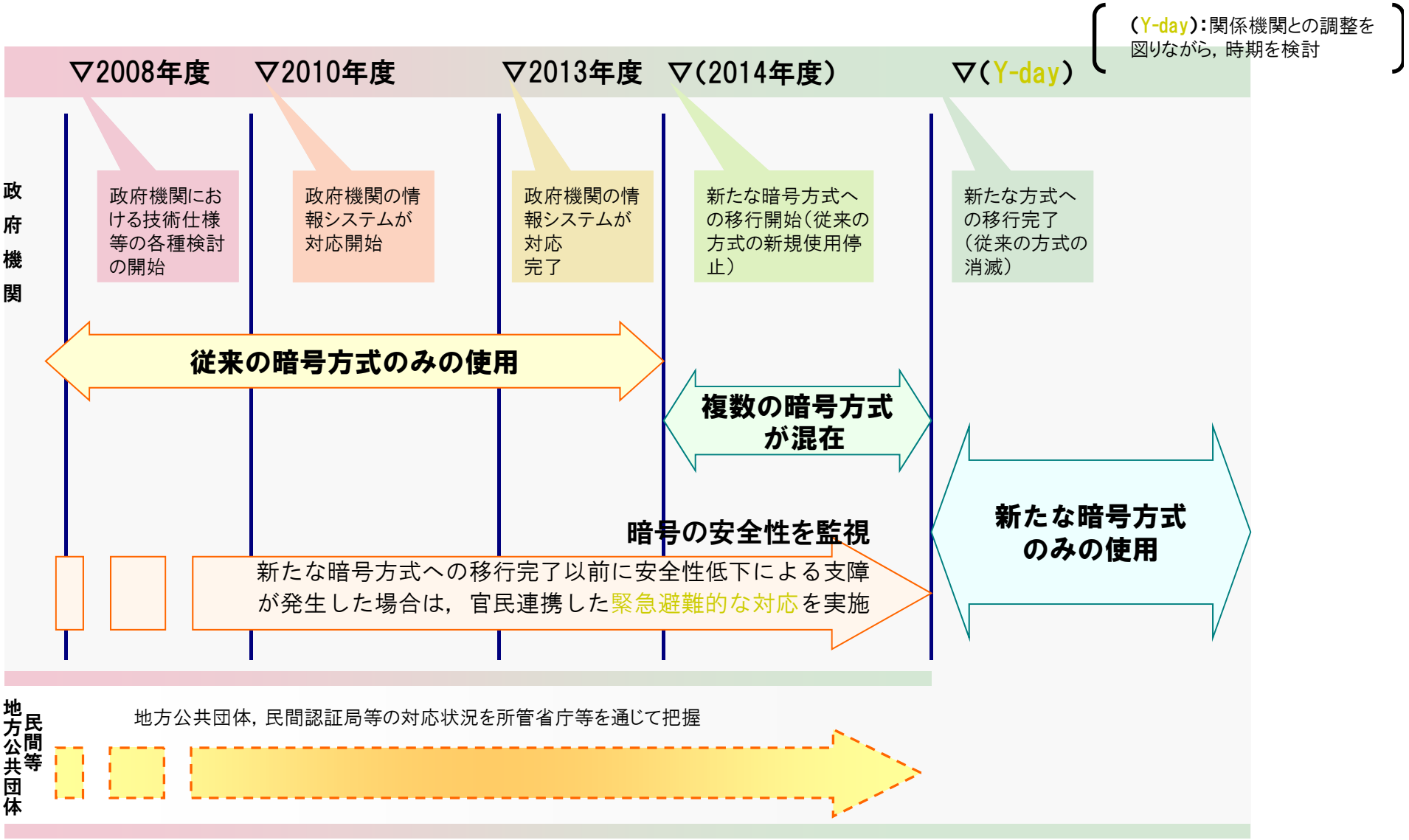
移行の現状

- 切り替え時期の検討
  - 政府機関の情報システムの対応を2013年度末に完了したあと、新暗号アルゴリズムによる運用を開始する時期を2014年度早期。
  - 電子署名が付与された文書の検証が必要となる期間を1年程度。

⇨ 政府機関とつながる情報システムは多岐にわたるため、今後調整。

  - 安全性予測：
    - CRYPTRECの安全性予想によると、問題ないと考えられる。
    - この予想を外れる急激な安全性の低下については、緊急対応計画で対応。

移行指針に基づく暗号方式の移行完了までのスケジュール



政府機関の対応状況

- GPKI
  - 政府認証基盤のブリッジ認証局に接続するすべての認証局は、総務省が定める政府認証基盤相互運用性仕様書に準拠する必要がある。
  - 仕様書は、すでに改訂をおえ、現在は、相互認証を検証するためのシステム構築に取り組んでいる。

- 法務省：商業登記認証局
  - 2013年度末を期日として、移行の準備中。

- アプリケーションシステム
  - 各認証局が発行する公開鍵証明書を利用するシステムのこと。
    - 例：e-tax、電子申請システム、電子入札システム
  - 2013年度末を期日として、準備中。

暗号の「急激な危殆化」が発生した場合に備えた「緊急対応計画」

- NISC作成の緊急対応計画の「**雛形**」を参考にして、各府省庁にて「**対象システム**」ごとに緊急対応計画を策定（2009年中）
- SHA-1及びRSA1024の安全性がどの程度かということを「危険度*1」によって表現し、現状は危険度1だと想定。
- 新たな暗号方式への移行完了以前に安全性低下による支障が発生した場合は、官民連携した緊急対応計画の策定

危険度があがる判断はNISCより発信

危険度0：安全	暗号として十分に利用できる状態	
現在はここ → 危険度1：危険	理論的な暗号解読アルゴリズムが公開された状態	体制整備
危険度2：Y年で危殆化	高性能計算機などの利用によって危殆化が実証された状態	状況判断 対策の周知 システム対応
危険度3：危殆化	十分に短い時間で署名の偽造ができる状態	利用停止 もしくは 別の業務を利用する方法

緊急対応計画をそれぞれの段階ごとに事前に策定

JPKI：公的個人認証サービス

- 「公的個人認証サービスにおける暗号方式等の移行に関する検討会」
  - 目的：公的個人認証サービスについても，その信頼性を引き続き確保するため，「公的個人認証サービスにおける暗号方式等の移行に関する検討会」を開催し，暗号方式等の移行について学識経験者・関係機関等による検討を行う．
  - 開催時期：平成20年9月～12月
  - 結論：NISC移行指針と同様の移行を実施することが公表

- 「公的個人認証サービス普及拡大検討会」
  - 開催時期：2009年4月～8月（中間報告）
  - 中間報告：有効期限を5年に延長する方向性が打ち出されるが、最終決定はなされていない。

- 地方公共団体組織認証基盤（LGPKI)
  - 総務省において検討中

住民基本台帳カードの対応について

- 住基カードの対応は，総務省自治行政局市住民制度課において検討中
- 住基カードのシステム開発に係るスケジュール（イメージ）は下記の通り

平成20年中期	検討（暗号アルゴリズム決定）
平成20年度後期～平成21年度中期	カード開発：仕様検討
平成21年度中期～平成23年度後期	カード開発：製品開発/ISO評価/ 動作確認
平成24年度	カード発行

第一回公的個人認証サービスにおける暗号方式等の移行に関する検討会資料より抜粋

特定認証業務を行う民間認定認証局：検討会概要

- 「電子署名及び認証業務に関する法律の施行状況に係る検討会」において検討

  【論点】

  - 電子署名の仕組みの基礎となる暗号技術は，コンピュータの能力の向上などにより安全性が低下する宿命にあり，世代交代は避けられない．
  - 現在電子署名法施行規則及び告示で規定されている暗号のうち，ハッシュ関数SHA-1及び公開鍵暗号RSA1024bitについては安全性の低下が指摘されているが，どのような対応を採るべきか．

  - 開催時期：平成19年12月～平成20年3月

- 検討結果
  - 告示第3条（特定認証業務に係る電子署名の基準）に規定する特定認証業務に係る電子署名の基準においても，より安全性の高い暗号技術への移行を促すため，速やかにSHA-2を追加し，SHA-2及びRSA2048bitによる電子署名について行う認証業務も特定認証業務に含めることが適当．
  - 主務省においては，以下のスケジュール案を基本として，制度改正作業等を進めていくことが適当．また，今後主務省は，暗号技術検討会等の意見等を踏まえ，早急にコンティンジェンシープランを作成し，暗号の急速な危殆化に備えるべき．

各府省庁による移行に関する検討のまとめ

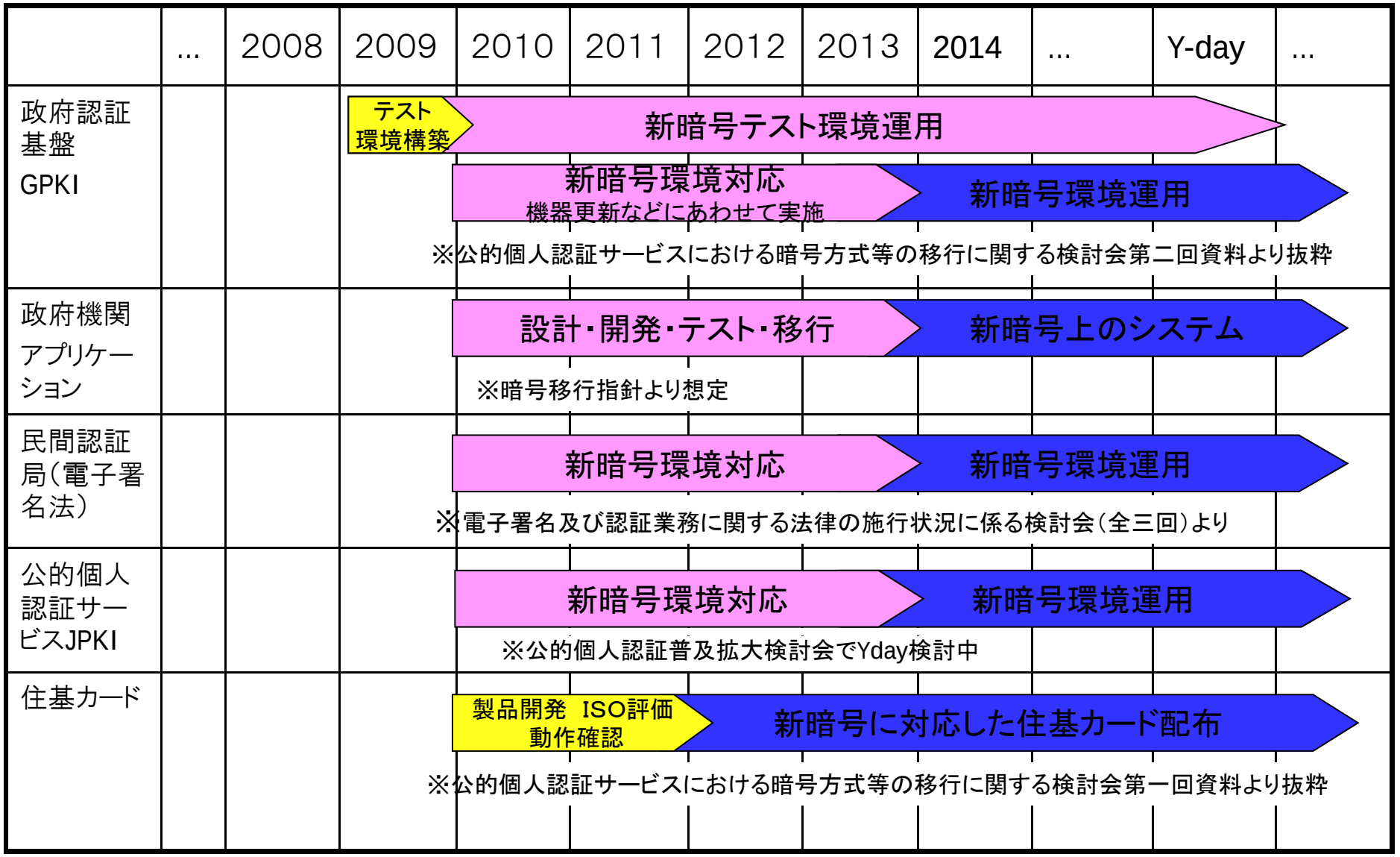
- GPKI
  - 総務省情報システム企画課
  - 対応移行計画：GPKI相互運用要件対応済み、検証環境構築中。

- 特定認証業務を行う民間認定認証局
  - 電子署名法主務三省（総務省，法務省，経済産業省）
  - NISCの移行とほぼ同じ時期に移行予定。

- JPKI：公的個人認証サービス
  - 総務省自治行政局
  - NISCの移行とほぼ同じ時期に移行予定。

- 住基カード
  - 総務省自治行政局住民制度課において検討。

暗号アルゴリズム移行スケジュール(想定)



今後に向けての課題

- 連携の重要性
  - 国の所管するシステムがすくなく、運営者の違う現状。
  - 移行が終わらない認証局があれば、セキュリティホールの可能性も。

- エンドユーザの意向
  - エンドユーザが多ければ多いほど。。。
  - ICカード（ハードウェアトークン）は？
    - クレジットカードは？
  - 移行を重視するか、安全性を重視するか
    - よくある話題ですが。

- 次世代移行
  - RSA2014＋SHA-1だけ。。。

まとめ

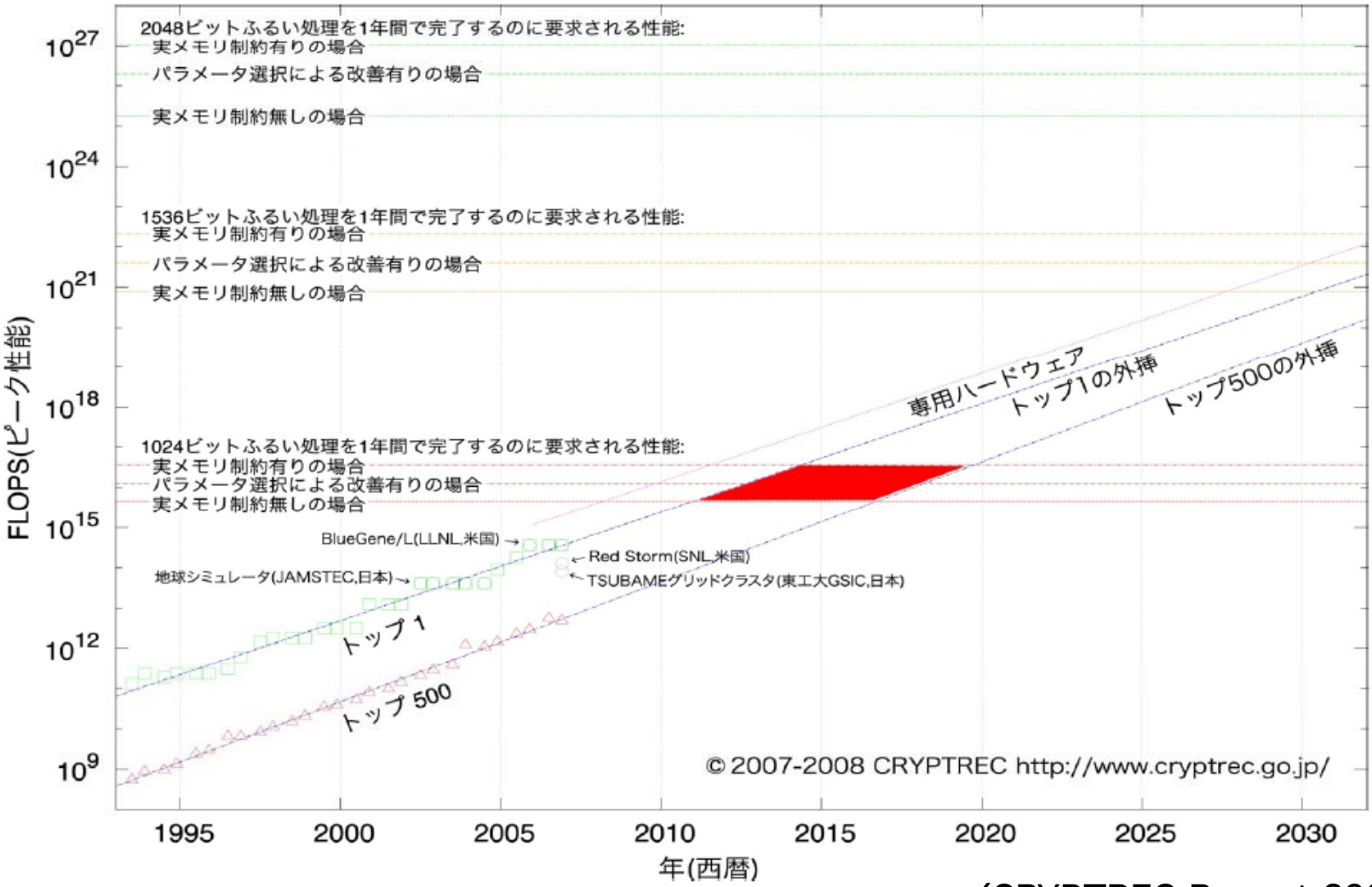
- PKIシステムの暗号移行について、NISCの移行指針を中心に解説
  - NISCの移行指針は、国の所管するシステムのみ。
  - それ以外のシステムは、所管ごとに検討をすすめているところ。

- 全ての移行に関する項目が終わっているわけではない
  - 終了時期の問題が残っている（実は、終了時期は決まっていない）。

参考：CRYPTREC（暗号技術検討会・暗号技術監視委員会）による見解

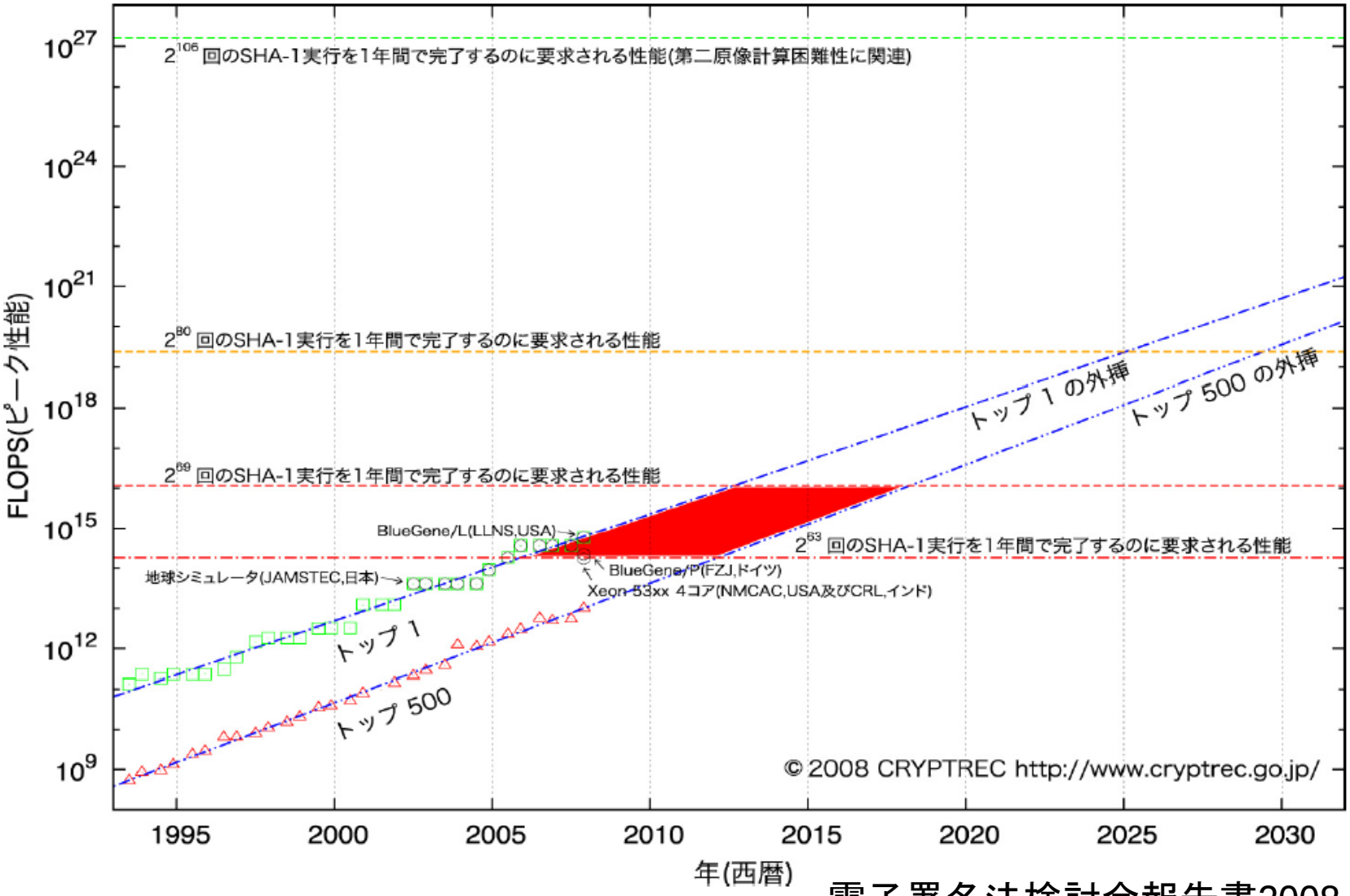
- 暗号技術検討会・暗号技術監視委員会などは，RSA1024及びSHA-1の安全性に懸念が生じる可能性を指摘
  - 暗号技術検討会は，総務大臣官房総括審議官及び経済産業省聖武情報政策局長が開催
- 計算量による予測は困難
- SHA-1の安全性
  - 衝突発見困難性のレベルは，現時点で63ビット以下．
    - スーパーコンピュータ・レベルのテクノロジとの比較では．2015 年前後には脅威となることが想定される．
  - ターゲット型衝突発見困難性のレベルは，まだ不確定である．
  - 第2原像計算困難性のレベルは，現時点で106ビット以下．
- RSA1024の安全性
  - 素因数分解問題の困難性のレベルは，現時点で70ビット以下．
    - スーパーコンピュータ・レベルのテクノロジとの比較では，概ね2015 年以降に脅威となることが想定される．

参考：1年間でふるい処理を完了するのに要求される処理性能の予測



(CRYPTREC Report 2006)

参考：1年間で衝突を計算するのに要求される処理性能の予測



電子署名法検討会報告書2008.05.30