NISC National Information Security Center

政府機関における安全な暗号利用の促進

内閣官房情報セキュリティセンター
産業技術総合研究所情報セキュリティ研究センター
繁富　利恵

暗号の安全性低下への対応

1　現状と課題

①電子政府システムでは，電子署名等のために暗号が使用されており，SHA-1及びRSA1024と呼ばれる暗号方式を広く使用.
②しかし，このSHA-1及びRSA1024は，安全性の低下が指摘されており，より安全な暗号方式への移行が必要.
③より安全な暗号方式への移行にあたっては，情報システムの相互運用性確保や政府全体の情報セキュリティの向上のため，政府統一的な移行指針を策定することが必要.

2　暗号の移行指針の概要

①技術的な対応

【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.

②制度的な対応

○ 各府省庁において次を実施
・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

③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.

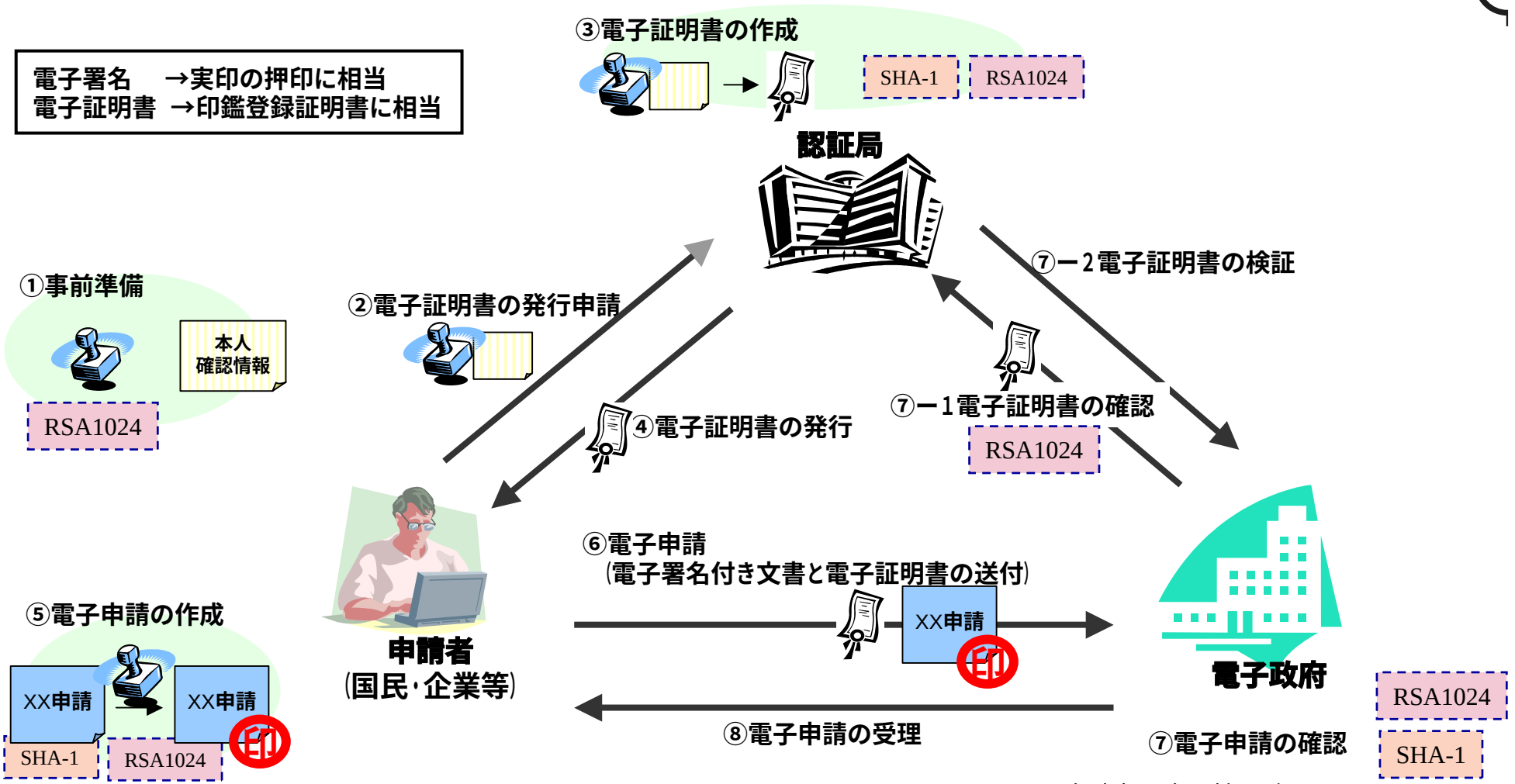
○ 内閣官房，総務省等
相互接続の技術要件，緊急避難対応等について2008年度中に検討.

○ 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.

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）

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.

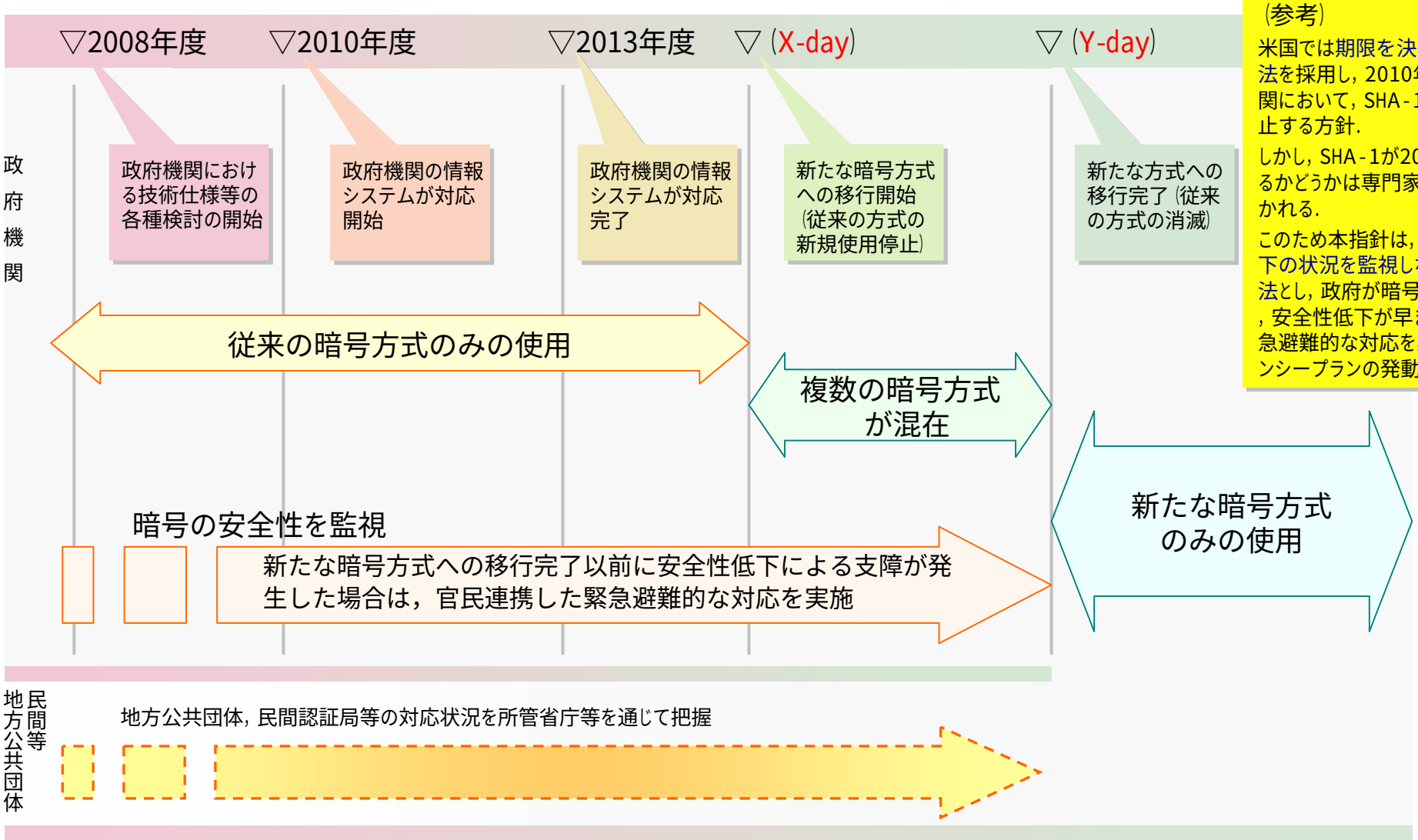
- 平成20年2月4日～3月7日 パブリックコメント
  - パブリックコメント総数　：　14件【内訳　企業・団体・大学　：　14件，　個人　：　0件】
  - 施策実施にあたっての配慮・要望として，民間との協調や2008年度の具体的検討に当たっての要望等について意見の提出あり.

  - 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

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

(X,Y-day)：関係機関との調整を図りながら，2008年度中に時期を検討



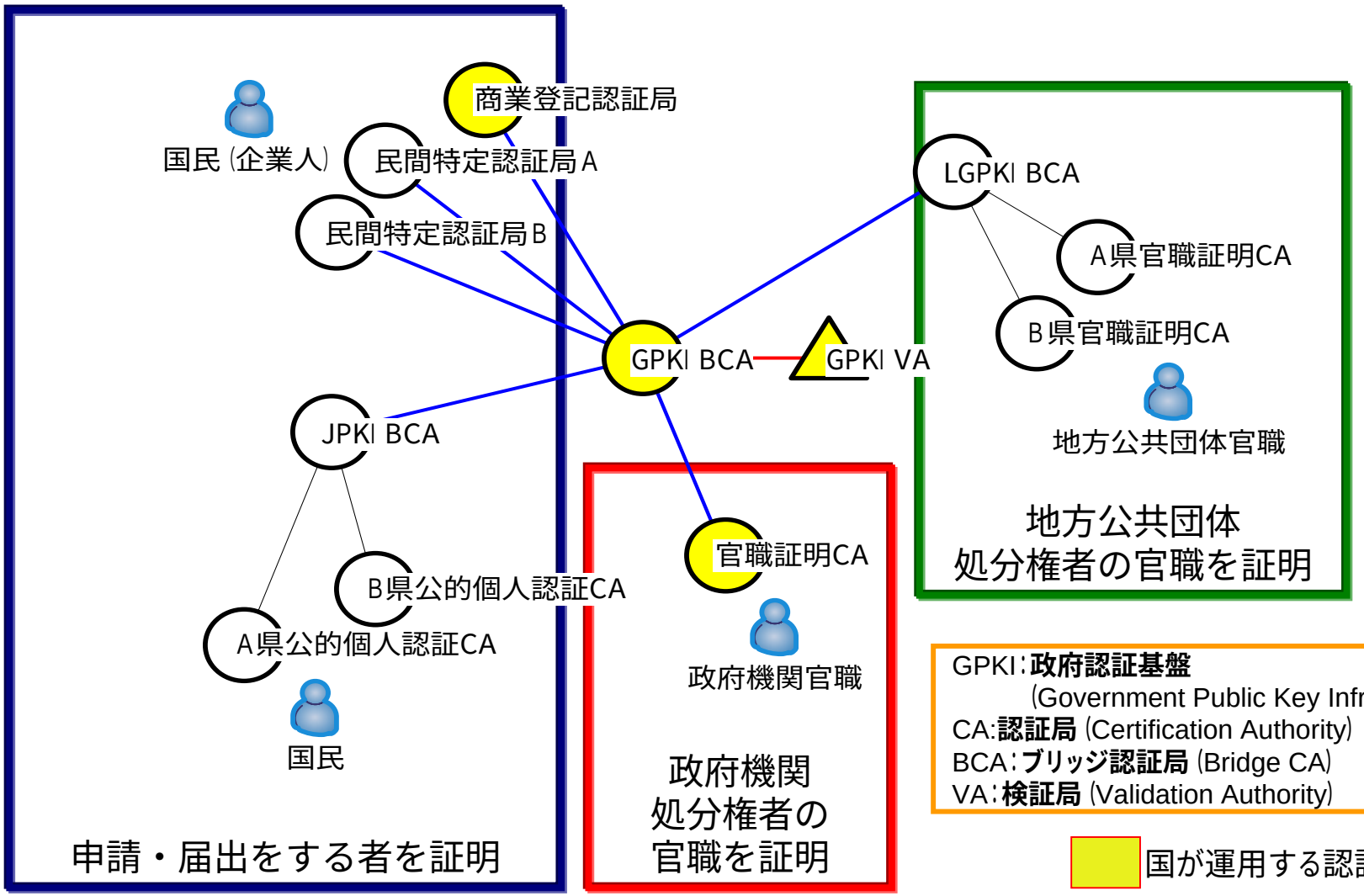
(参考)

米国では期限を決めて対応する方法を採用し，2010年末以降，政府機関において，SHA-1の新規使用を停止する方針．

しかし，SHA-1が2010年に危殆化するかどうかは専門家の間でも意見がわかれる．

このため本指針は，暗号の安全性低下の状況を監視しながら対応する方法とし，政府が暗号の安全性を監視し，安全性低下が早まった場合は，緊急避難的な対応を実施(コンテンジェンシープランの発動)．

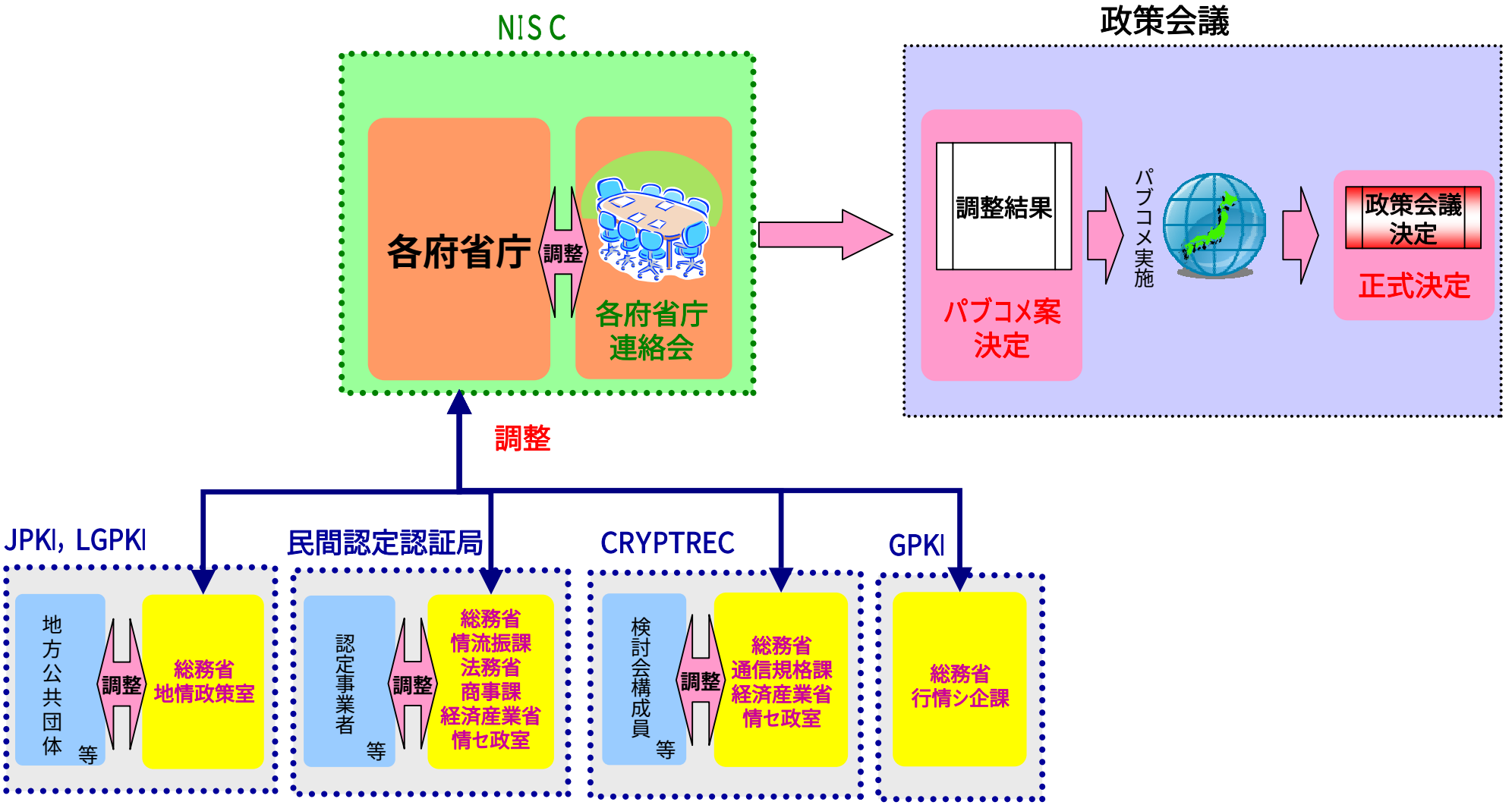
各認証局と政府認証基盤（GPKI）ブリッジＣＡによる相互認証



GPKI：**政府認証基盤**
（Government Public Key Infrastructure）
CA:**認証局**（Certification Authority）
BCA：**ブリッジ認証局**（Bridge CA）
VA：**検証局**（Validation Authority）

国が運用する認証局

関係者全体図



移行指針より抜粋：スケジュール

(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．

各府省庁による移行に関する検討

- GPKI
  - 総務省情報システム企画課
  - 対応移行計画：GPKI相互運用要件及び検証環境構築を計画中

- 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）
  - 「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

- JPKI：公的個人認証サービス
  - 総務省自治行政局
  - 「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」において検討中

- 住基カード
  - 総務省自治行政局市町村課において検討中

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

  - 目的
    - 「電子署名及び認証業務に関する法律」（電子署名法）は．平成１２年第１４７回国会の審議を経て，同年5月に公布，平成１３年4月１日に施行された．
    - 電子署名法附則第3条においては，施行後5年を経過した場合に，同法の施行の状況について検討を行うものとされており，総務省，法務省及び経済産業省は，平成18年度以降，外部有識者のヒアリングを行うなどして同法施行上の課題の抽出等を実施してきた．
    - この検討会は，当該抽出した課題について議論を行い，今後の電子署名法の運用に反映していくため，開催したもの

  - 開催時期
    - 第1回平成１９年１２月１８日
    - 第2回平成２０年2月１９日
    - 第3回平成２０年3月３１日

【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．

- 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．

2008年度 早期	**暗号アルゴリズムの移行に向けた具体的な検討の開始，特定認証業務に係る電子署名の基準にSHA-2を追加．**
(2010年度)	**(政府機関システム暗号移行開始)*政府機関システム移行指針(案)による**
(2013年度)	**(政府機関システム新旧暗号アルゴリズム(SHA-1及びSHA-2，RSA1024bit及び2048bit)対応環境構築が完了)*政府機関システム移行指針(案)による**
2013年度末まで	**認定認証事業者に対して，暗号移行に係る変更認定のための調査が必要な場合は実施し，認定認証事業者は，RSA2048bitを用いた発行者鍵ペアを新たに生成する必要がある場合は，生成．**
2014年度 早期まで	**認定認証事業者は，RSA2048bitによる発行者鍵ペアを活性化させSHA-2及びRSA2048bitによる電子署名についての認証業務を開始．**
2014年度	SHA-1，RSA1024bitによる利用者電子証明書の有効期間後に，特定認証業務に係る電子署名の基準から，SHA-1，RSA1024bitを削除． （SHA-1，RSA1024bitによる利用者電子証明書の有効期間について，各認定認証事業者は，SHA-2，RSA2048bitによる利用者電子証明書への切替を考慮し，あらかじめ調整を図ること等が求められる．）

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」において検討中

- 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
  - 第一回 平成20年9月16日
  - 第二回 平成20年10月
  - 第三回 平成20年12月開催予定

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町村課において検討中

•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

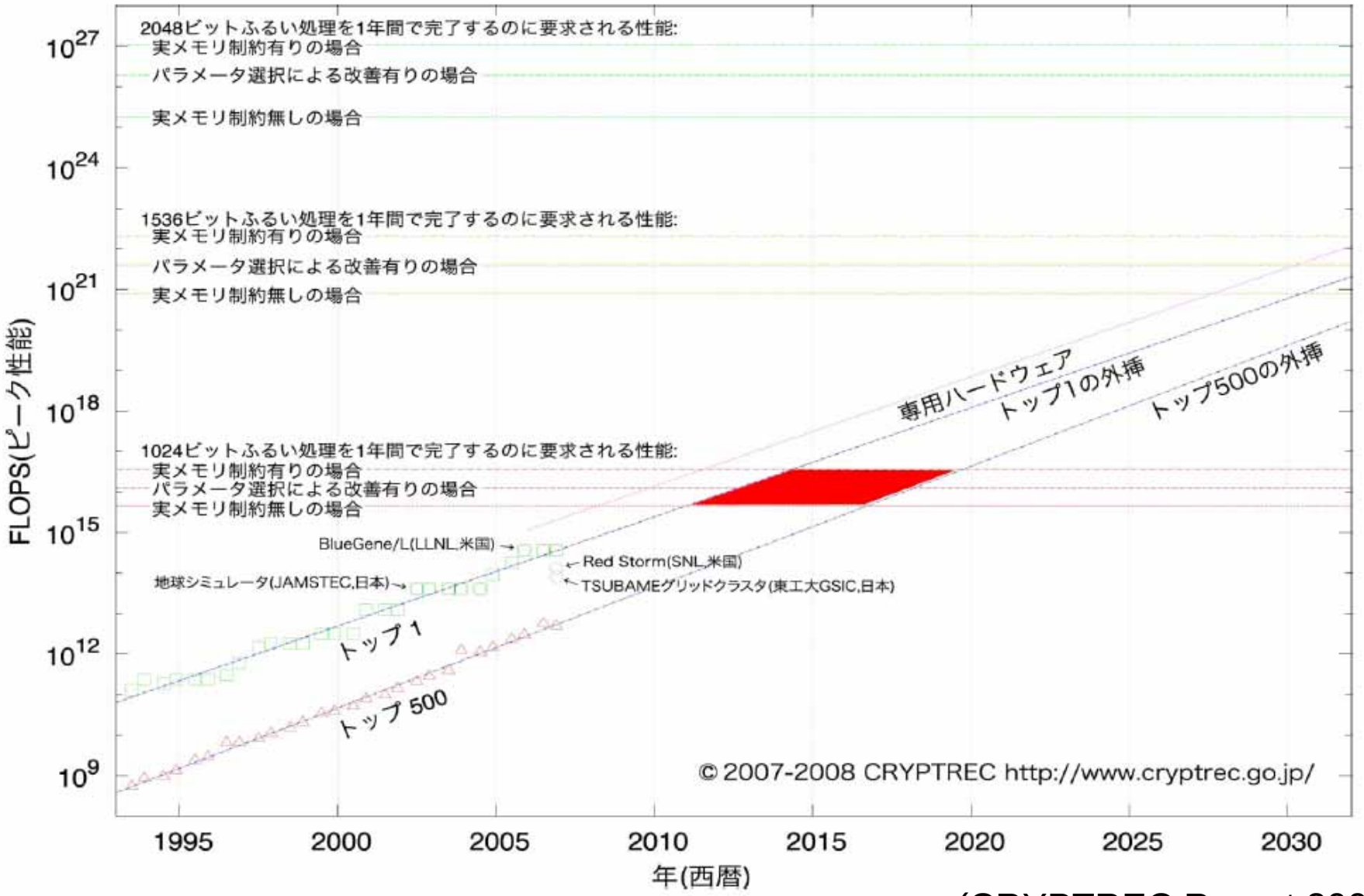
平成20年中期	検討（暗号アルゴリズム決定）
平成20年度後期～平成21年度中期	カード開発：仕様検討
平成21年度中期～平成23年度後期	カード開発：製品開発/ISO評価/ 動作確認
平成24年度	カード発行

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

参考：CRYPTREC（暗号技術検討会・暗号技術監視委員会）による見解

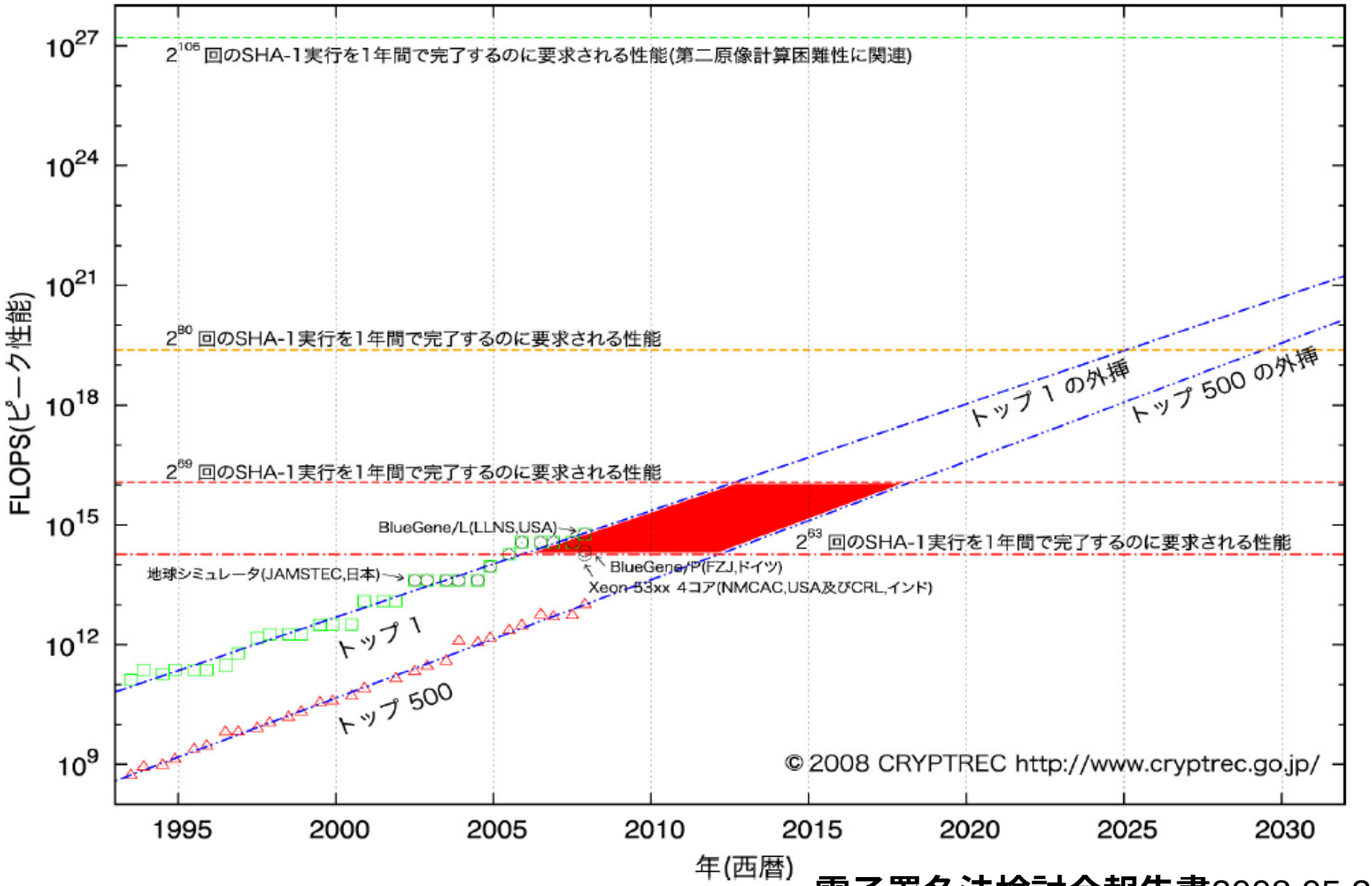
- 暗号技術検討会・暗号技術監視委員会などは，RSA1024及びSHA-1の安全性に懸念が生じる可能性を指摘
  - 暗号技術検討会は，総務大臣官房総括審議官及び経済産業省政務情報政策局長が開催
- 計算量による予測は困難
- SHA-1の安全性
  - 衝突発見困難性のレベルは，現時点で63ビット以下．
    - スーパーコンピュータ・レベルのテクノロジとの比較では．2015 年前後には脅威となることが想定される．
  - ターゲット型衝突発見困難性のレベルは，まだ不確定である．
  - 第2原像計算困難性のレベルは，現時点で106ビット以下．
- RSA1024の安全性
  - 素因数分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