政府認証基盤(GPKI)における暗号方式等の移行について

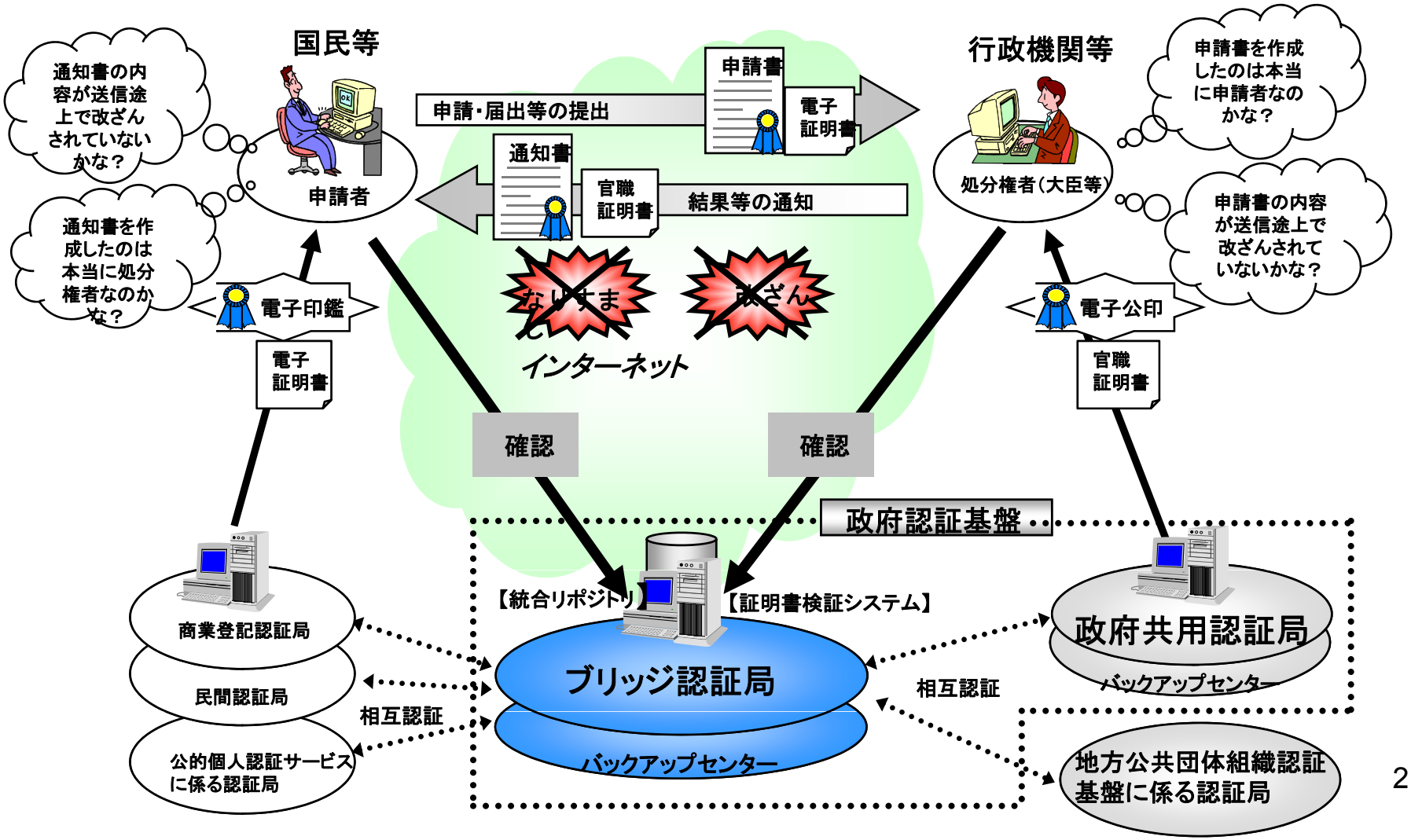
総 務 省 行 政 管 理 局
行政情報システム企画課

政府認証基盤（GPKI：Government Public Key Infrastructure）

－GPKIを利用した申請・届出のオンライン化－

国民等と行政機関との間でインターネット等を利用してやり取りされる申請・届出等手続に係る電子文書について、その文書が真にその名義人によって作成され、内容に改変がないことを相互に確認できるようにするための仕組み。

公開鍵暗号方式による電子署名を用いた認証システムにより実現しており、ブリッジ認証局及び政府共用認証局から構成されている。（平成13年４月～運用）



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

「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（平成20年4月22日　情報セキュリティ政策会議決定）」においては、政府認証基盤等に以下の対応が求められている。

（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の対応として）

・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する。

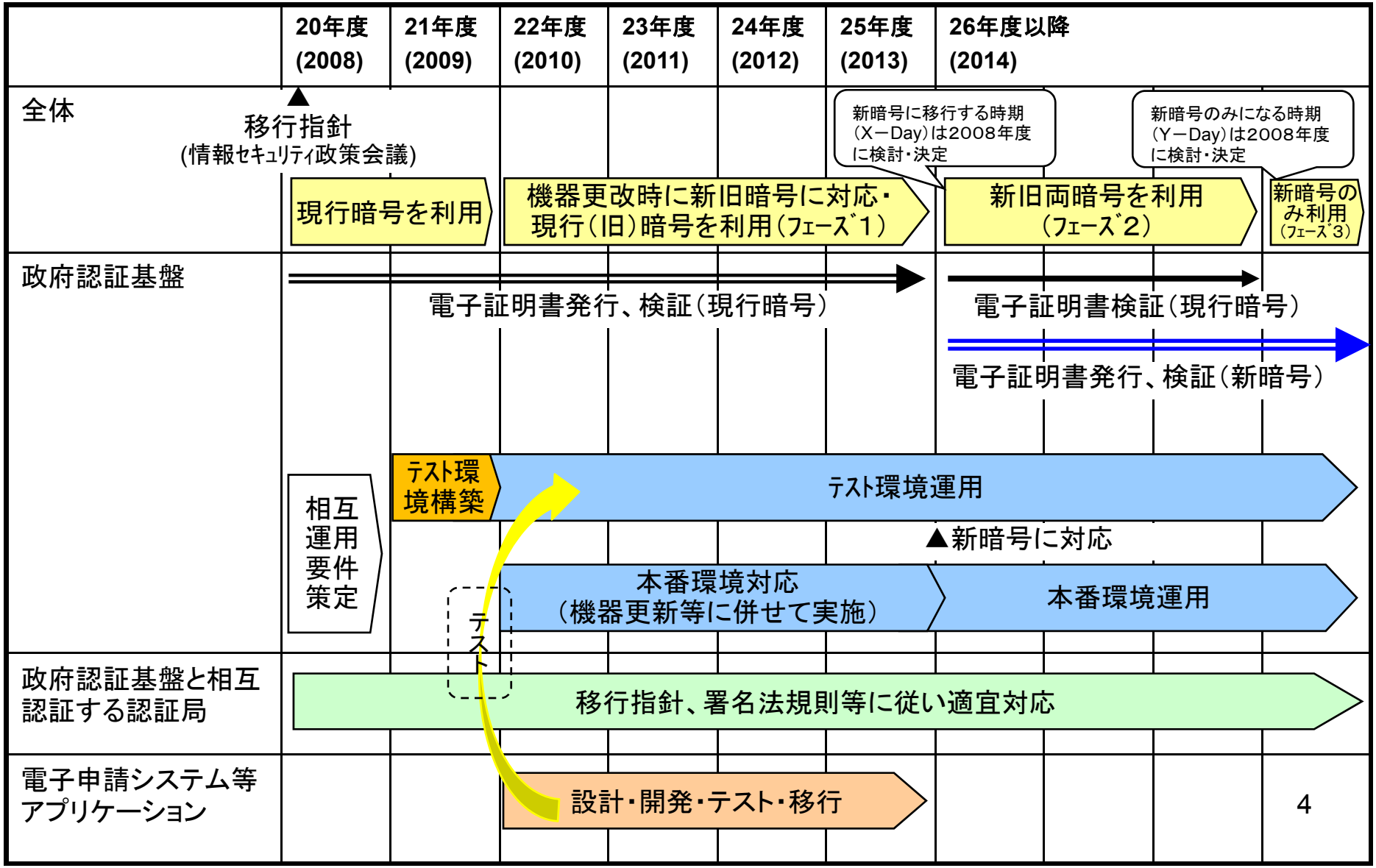
・新たな暗号方式として、SHA-256及びRSA2048を採用する。

（移行スケジュールとして）

・内閣官房、総務省等は、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整備を2008年度中に検討、2009年度の構築を目指す。

暗号アルゴリズム移行スケジュール（想定）

「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に係る移行指針から想定される移行スケジュールは、下図のとおり。



政府認証基盤ブリッジ認証局の暗号アルゴリズム移行の流れ

- フェーズ2開始時点（X-day）で、新たな暗号アルゴリズムへの移行を鍵更新により行う。鍵更新後に発行する電子証明書及び失効リストは、新たな暗号アルゴリズム（SHA-256及びRSA2048）により発行する。

- フェーズ2（X-dayからY-dayまで）において、ブリッジ認証局の鍵更新時に発行されるリンク証明書の関連付けにより、現行の暗号アルゴリズムで発行された電子証明書の検証を可能とする。

- フェーズ3開始時点（Y-day）で、現行の暗号アルゴリズムで発行された電子証明書を失効する。