資料4

公的個人認証サービスにおける
暗号アルゴリズムの安全性低下に伴う
リスク整理の考え方

2008年12月18日

NTTコミュニケーションズ（株）

1．暗号アルゴリズムの安全性低下に伴うリスク整理

	利用者の電子署名に関するリスク	都道府県知事の電子署名に関するリスク
RSA1024 の安全性低下に伴うリスク	２－２．利用者秘密鍵が漏洩するリスク	※都道府県知事の鍵ペアはRSA2048を使用しているため、リスクの想定なし
SHA-1 の安全性低下に伴うリスク	２－１．風評被害のリスク ２－３．衝突計算攻撃（※１）によるリスク 第二原像計算攻撃（※2）は安全性を脅かす実用的な攻撃方法が報告されていないため、<u>今回はリスク整理の対象外とする</u>	

（※１）メッセージダイジェストが同一となる異なる2つのメッセージを生成する
（※2）あるメッセージとそのメッセージダイジェストから、同一のメッセージダイジェストを算出する、異なるもう1つのメッセージを特定する

２－１．風評被害のリスク

●リスクの内容

安全性の低下が指摘されている暗号アルゴリズム（RSA1024、SHA-1）を利用していることによって、風評被害に遭うリスクが考えられる。

【事例】

オーストラリアでの交通違反に関する裁判の事例。スピード違反取締用に設置されていた交通カメラでハッシュ関数のMD5が利用されていた。当時、MD5は暗号学会において衝突計算攻撃が成功する事例が報告されていたため、交通違反の証拠は無効だという被告側の主張を認める判決が下された。

●発生確率に関する見解

発生確率を算出するのは困難だが、風評被害が広がる要素として、以下の3点が挙げられる。

① 計算時間が劇的に短縮された暗号解読手法が発表される

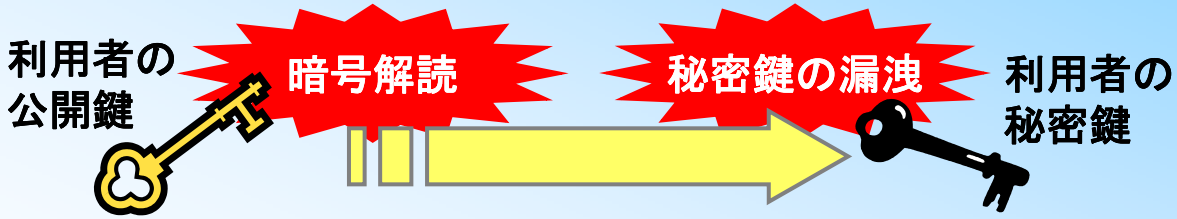
② アメリカでは政府システムにおいて2010年にRSA1024およびSHA-1の新規使用が終了する

③ ある国でRSA1024およびSHA-1を利用した電子データに対して、訴訟上の証拠能力を認めない判例が出される

２－２．利用者秘密鍵が漏洩するリスク

●リスクの内容

暗号アルゴリズム（RSA1024）の安全性低下により、利用者の公開鍵（電子証明書）から利用者の秘密鍵が解読され、漏洩してしまうリスクが考えられる。この結果、利用者の電子署名の改ざんや、電子申請時のなりすまし等のリスクが発生すると考えれる。



【事例】

1999年、フランスの全銀行で発行されていた銀行カード（ICカード）では、当時の技術レベルでも古いとされていたRSA暗号が利用されていた。その暗号アルゴリズムを解読した銀行機関の技術者が、カード発行機関に対して注意を促すために、実際に暗号解読を行って偽造ICカードを作成して見せた。

●発生確率に関する見解

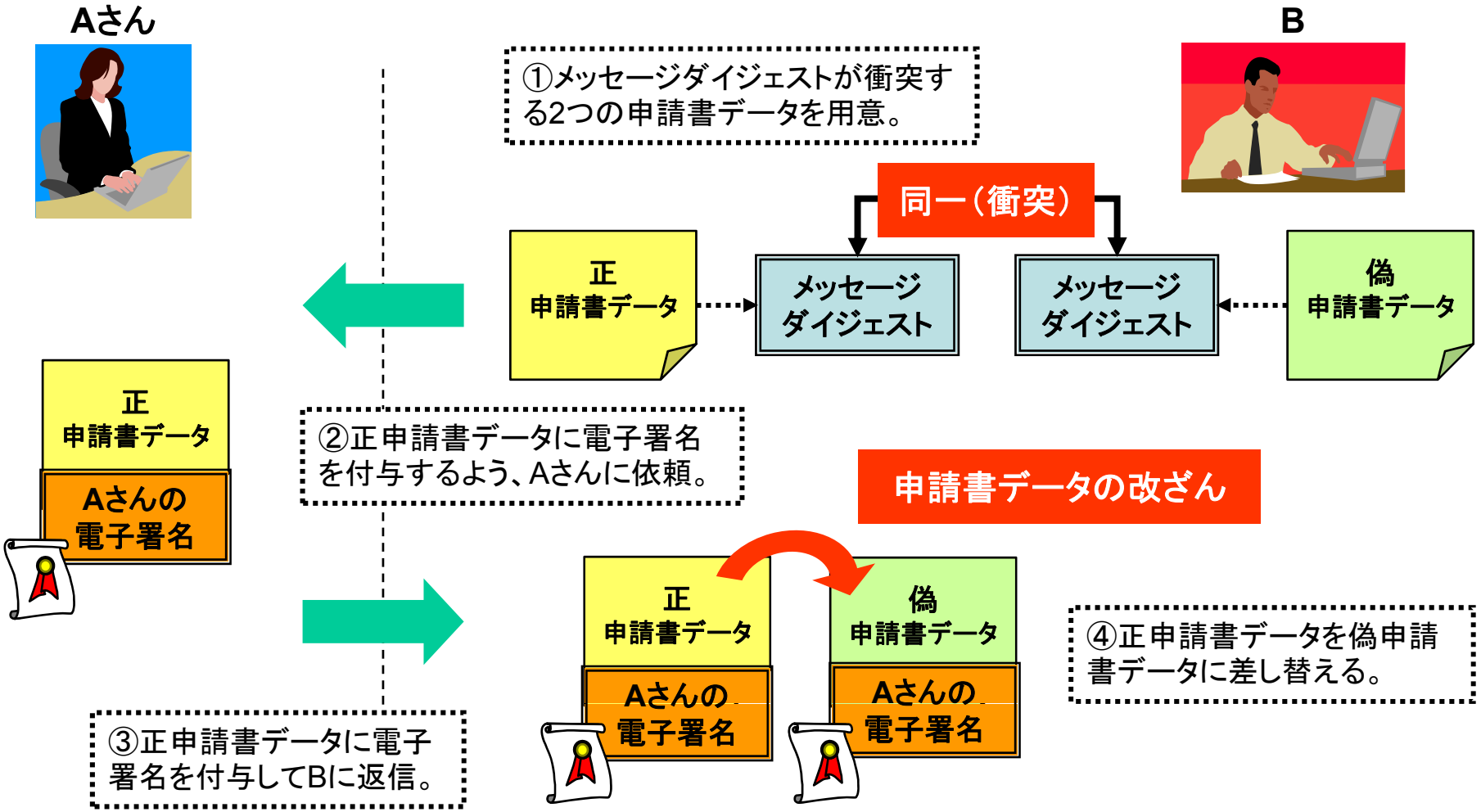
世界でも処理能力が高いスーパーコンピュータを用いて、RSA1024が1年間の計算によって攻撃可能になる時期については、2010年～2020年の間と推定されている。したがって、その時期に汎用的なPCを用いて瞬時に暗号が解読される可能性は極めて低いと考えられる。

ただし、暗号アルゴリズムの新たな解読手法が発見される可能性は、留意しておく必要がある。

２－３．衝突計算攻撃によるリスク（1/2）

●リスクの内容

SHA-1の安全性低下により、将来同一のメッセージダイジェストを持つ異なる申請書データが作成され、オンラインでの申請・届出等において申請書データの改ざんが行われる可能性がある。



２－３．衝突計算攻撃によるリスク（2/2）

●発生確率に関する見解

世界でも処理能力が高いスーパーコンピュータを用いて、SHA-1の衝突計算攻撃による脅威が現実的になることが想定される時期は2015年前後とされており、その時期に汎用的なPCを用いて瞬時に衝突計算攻撃が成功する可能性は極めて低いと考えられる。

なおかつ、衝突計算攻撃において、２つのメッセージが意味を持つように意図的に作成することは、単に衝突計算攻撃を成功させる以上に困難なことであると予想されるため、実害を及ぼすリスクが顕在化する可能性は、極めてゼロに近いものと考えられる。

ただし、暗号アルゴリズムの新たな解読手法が発見される可能性は、留意しておく必要がある。

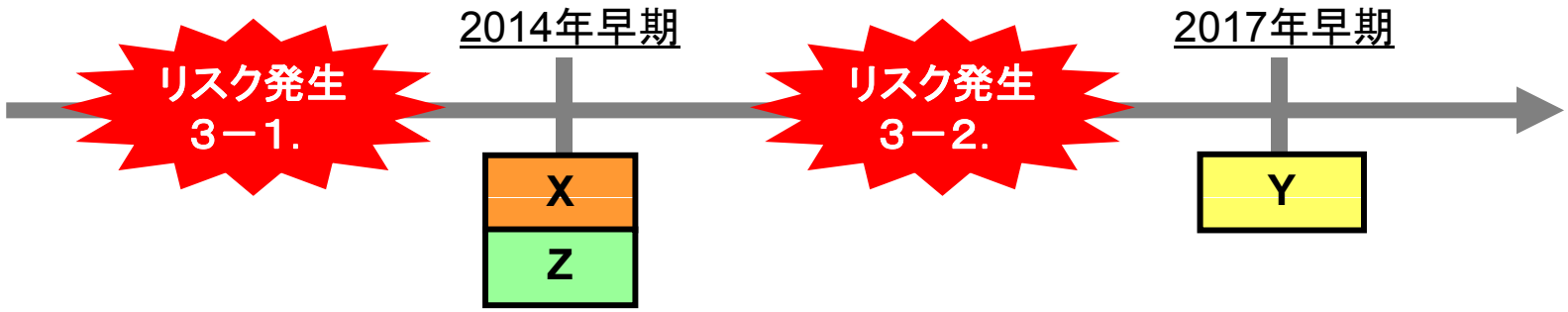
3. リスクが顕在化した場合の対処策（案）

暗号アルゴリズムの安全性低下に伴うリスク（風評被害や電子署名の偽造等）が顕在化した場合に備え、リスクの影響範囲およびリスクの発生時期を鑑みた対処策を用意しておく必要がある。ここでは、検討会報告書の移行スケジュールに基づき、以下のリスク発生時期で整理した対処策（案）を提示する。

【想定するリスク発生時期】

3－1. 暗号アルゴリズムの移行前

3－2. 新旧暗号アルゴリズムでの並行運用期間中



【移行スケジュール関連時期】

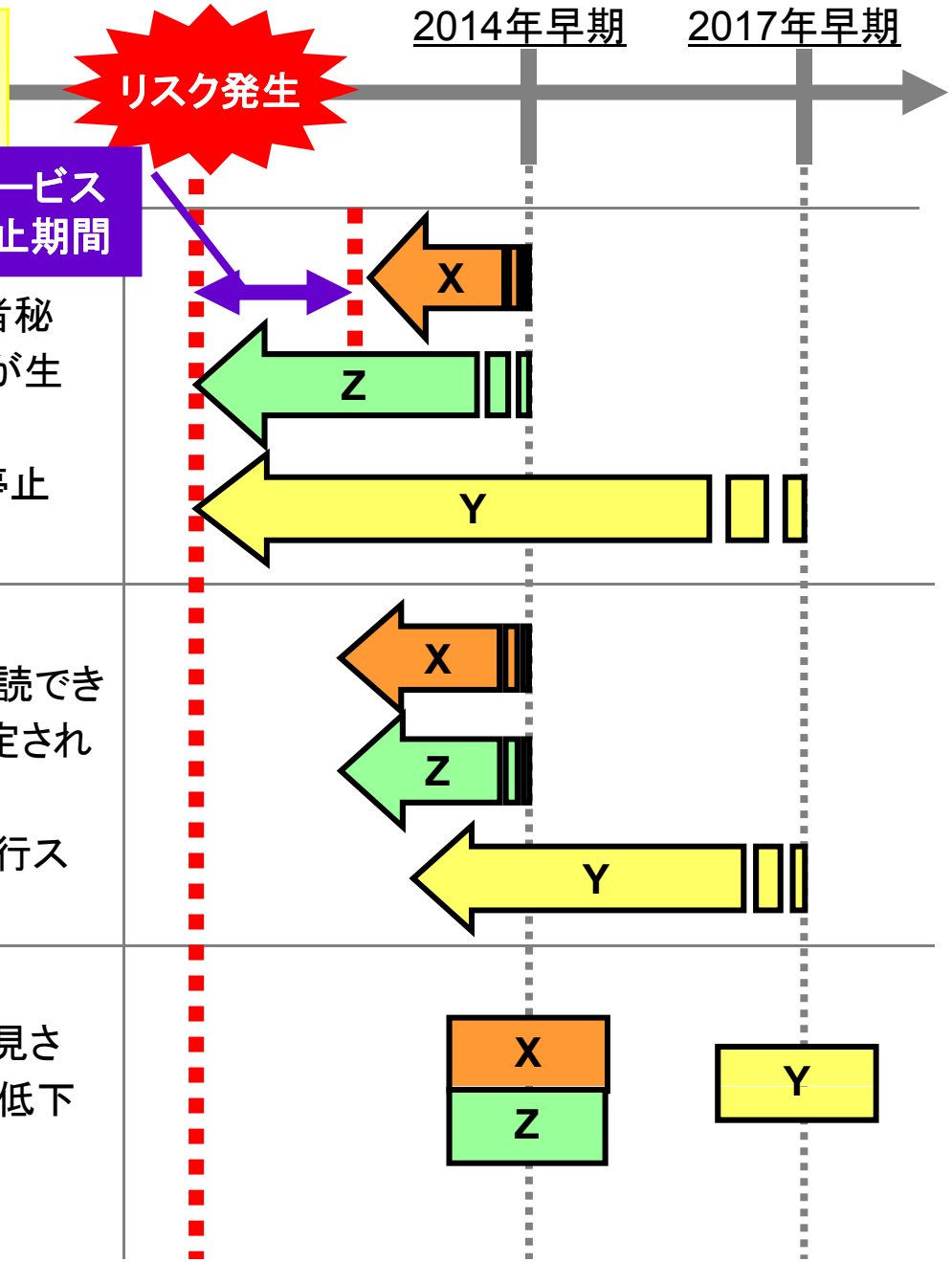
X ： 新電子証明書の発行開始時期

Z ： 旧電子証明書の発行停止時期

Y ： 旧電子証明書の使用停止時期

３－１．暗号アルゴリズムの移行前における対処策（案）

暗号アルゴリズムの移行前にリスクが顕在化した場合、リスクの内容により、当初の移行スケジュールを見直す必要がある



【対処案1】

暗号アルゴリズムの解読により、複数の利用者秘密鍵が漏洩し、電子署名の改ざんによる実害が生じる等、致命的なリスクが発生した場合

●緊急に電子証明書の強制失効、新規発行停止

●復旧策は事後検討

【対処案2】

汎用PCを用いて瞬時に暗号アルゴリズムを解読できる手法が研究機関で発見される等、実害が想定されるリスクが発生した場合

●電子証明書の運用は継続しつつ、当初の移行スケジュールを前倒して対応

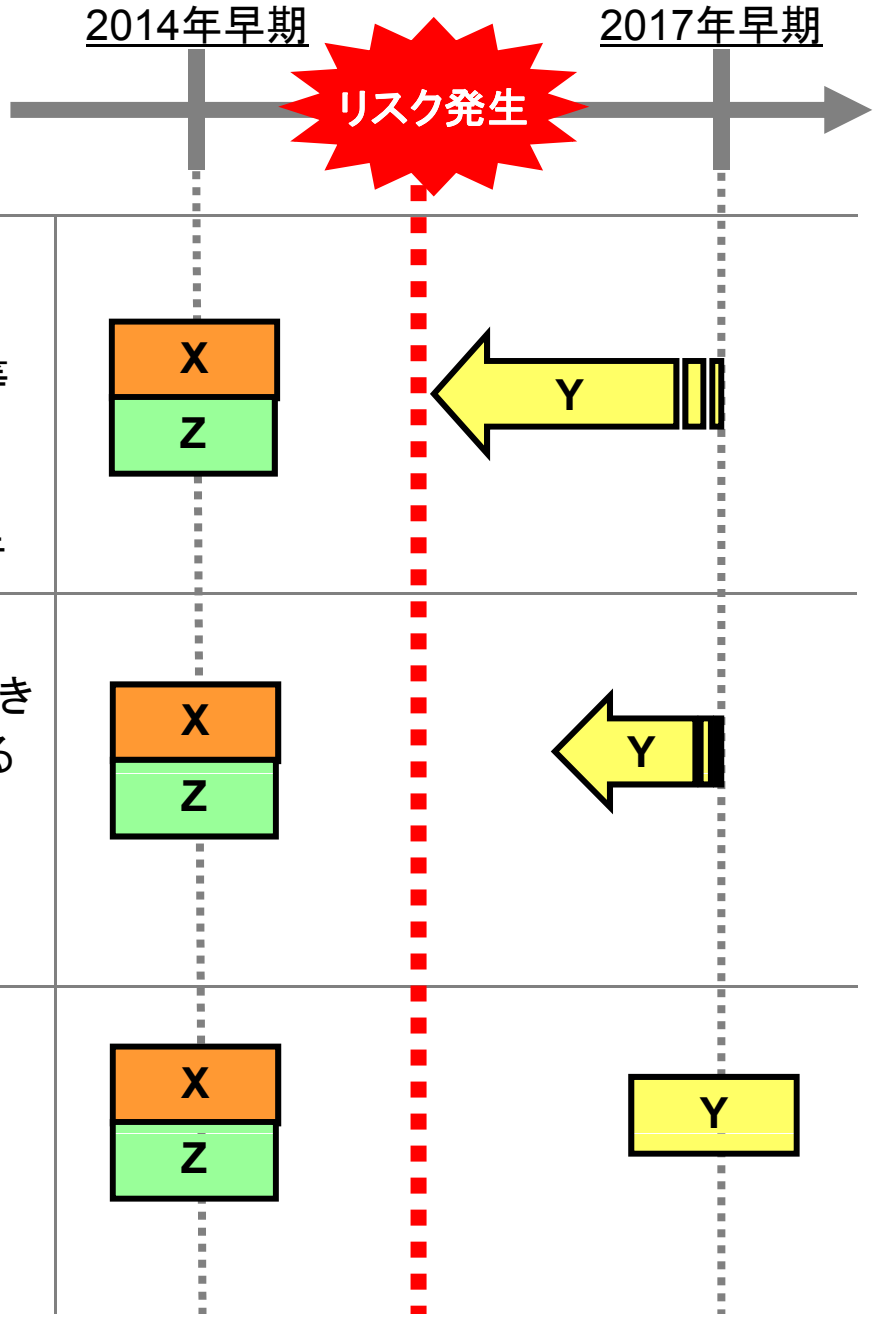
【対処案3】

より少ない計算量で暗号解読可能な手法が発見される等、現状よりも暗号アルゴリズムの安全性低下が指摘されたものの、実害が想定しにくい場合

●当初の移行スケジュール通りに対応

３－２．新旧暗号アルゴリズムの並行運用期間における対処策（案）

旧暗号アルゴリズムに関するリスクが顕在化した場合、リスクの内容により、当初の旧電子証明書の使用停止時期（Yの時期）を見直す必要がある



【対処案1】

旧暗号アルゴリズムの解読により複数の利用者秘密鍵が漏洩し、電子署名の改ざんによる実害が生じる等の致命的なリスクが発生した場合

●緊急に旧電子証明書の強制失効

●強制失効された利用者には新電子証明書を再発行

【対処案2】

汎用PCを用いて瞬時に旧暗号アルゴリズムを解読できる手法が研究機関で発見される等、実害が想定されるリスクが発生した場合

●旧電子証明書の有効期間を当初の移行スケジュールよりも前倒して終了

【対処案3】

より少ない計算量で暗号解読可能な手法が発見される等、現状よりも暗号アルゴリズムの安全性低下が指摘されたものの、実害が想定しにくい場合

●当初の移行スケジュール通りに対応