資料3－3

HITACHI
Inspire the Next

次世代セキュリティ研究会資料

「主要な環境変化」による影響と新たな課題について

2007年12月20日

（株）日立製作所　手塚 悟

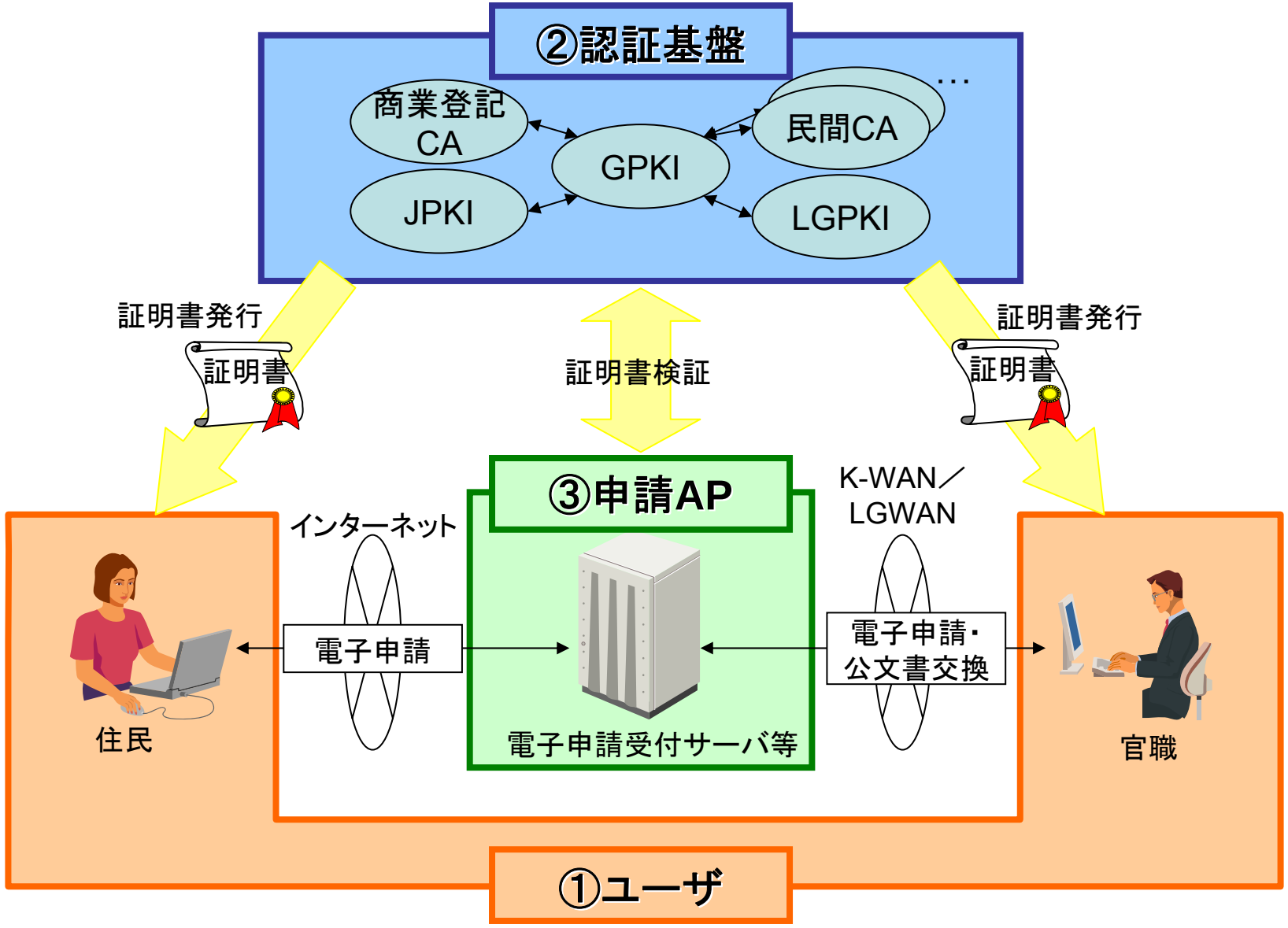
HITACHI
Inspire the Next

Contents

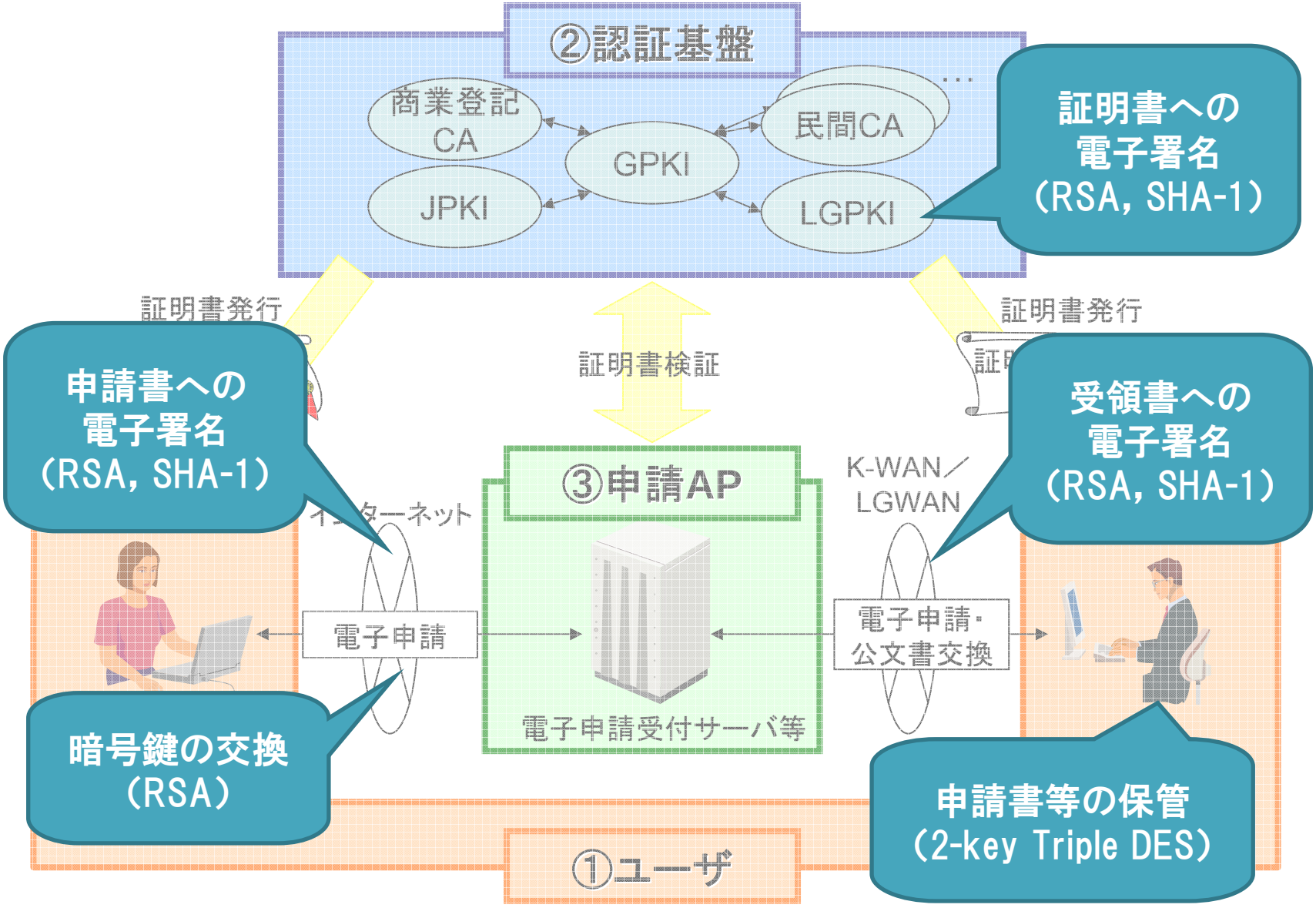
1. 暗号アルゴリズムの危殆化が
   電子政府システムに与える影響と対策

2. NGN時代の認証のあり方

1-1 電子政府システムの概要



1-2 電子政府システムにおける暗号利用



1-3 暗号アルゴリズムの危殆化

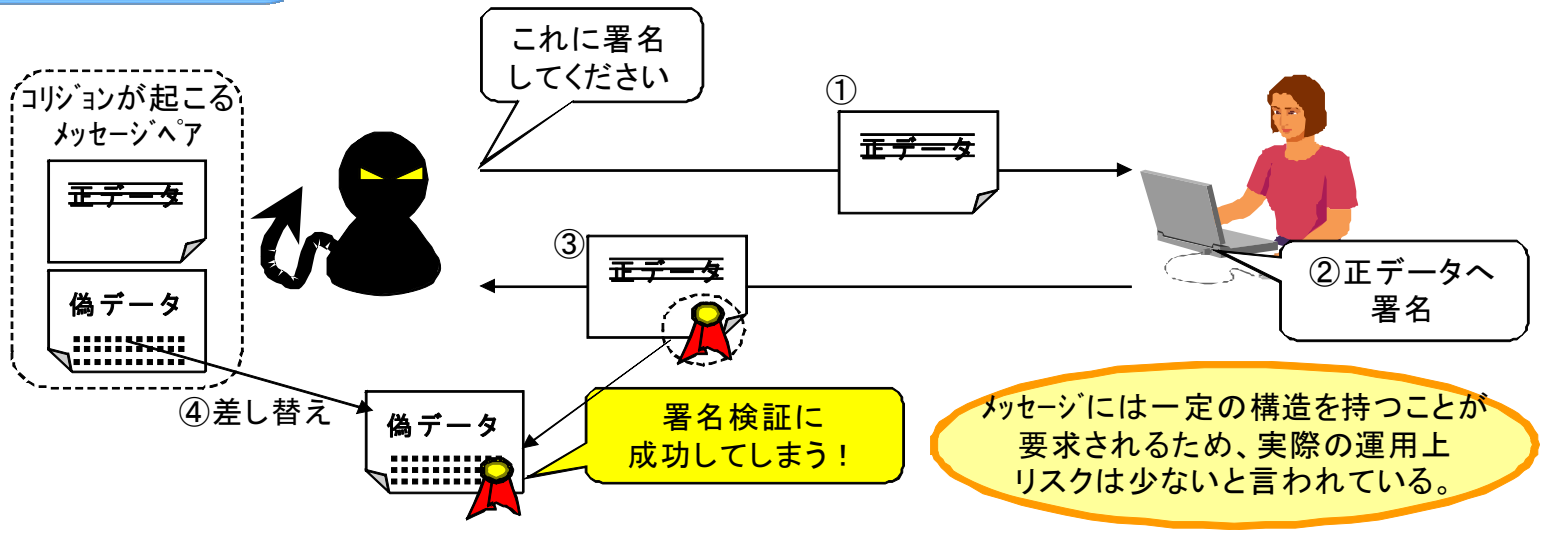
HITACHI
Inspire the Next

- 暗号アルゴリズムの危殆化とは？
  - その暗号アルゴリズムに期待する安全性のレベルが，何らかの原因により保てなくなること
- 暗号アルゴリズムの安全性
  - 現在利用されている多くの暗号アルゴリズムは，計算量的な安全性（解読するために莫大な時間・コストが必要であり，現実問題として解読不能）に依拠したもの
  - 時間経過に伴う計算能力の向上や解読技術の進展などにより，計算量的な安全性に基づく暗号アルゴリズムが徐々に危うくなるのは避けられない問題
    - DES（鍵長56bit） → AES（鍵長128bit,192bit,256bit）
  - 情報量的な安全性に基づく暗号アルゴリズムも考案されているが，制約条件が多く，まだ実用的なレベルに至っていない

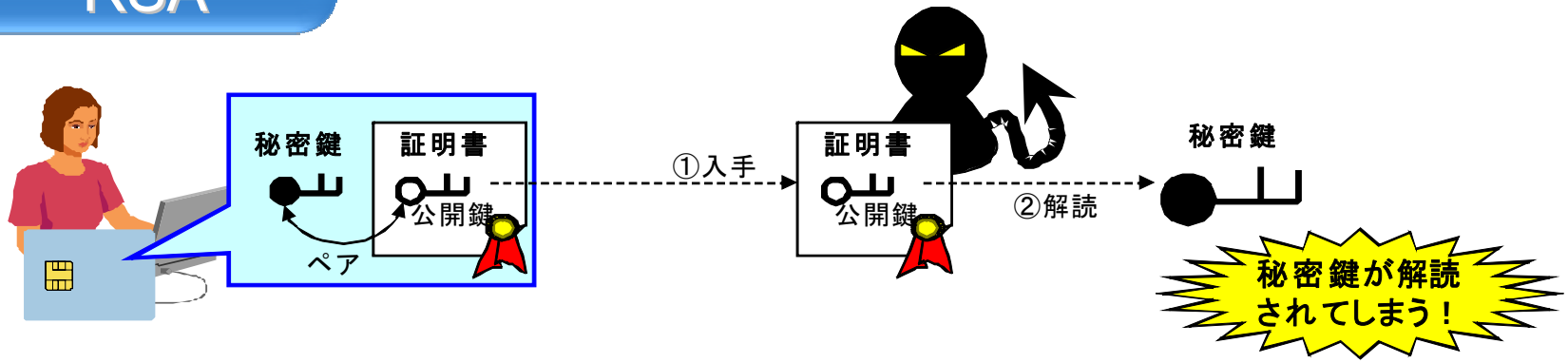
1-3 暗号アルゴリズムの危殆化

HITACHI
Inspire the Next

SHA-1



RSA



1-4 暗号2010年問題

HITACHI
Inspire the Next

- 暗号2010年問題
  - 米国NIST（国立標準技術研究所）が示した暗号アルゴリズムの移行方針（SP800-78，SP800-57等で公開）
  - 2010年以降，現在広範囲で使用されている下記暗号アルゴリズム等の使用を推奨しない（政府系システムの調達仕様から外れる）
    - SHA-1
      - 近い将来Collision（衝突）が発見される可能性大
      - ディジタル署名，ハッシュ値のみ使用するアプリケーションでは2010年以降使用を推奨しない
    - 1024bit RSA
      - 1024bitでは近い将来解読される可能性大
      - 2010年以降は使用を推奨しない（2048bit以上）
    - 160bit ECDSA
      - 1024bit RSA相当であり，2010年以降は使用を推奨しない（224bit以上）
    - 2-key Triple DES
      - 2010年以降は使用を推奨しない（3-key Triple DES or AES）

HITACHI
Inspire the Next

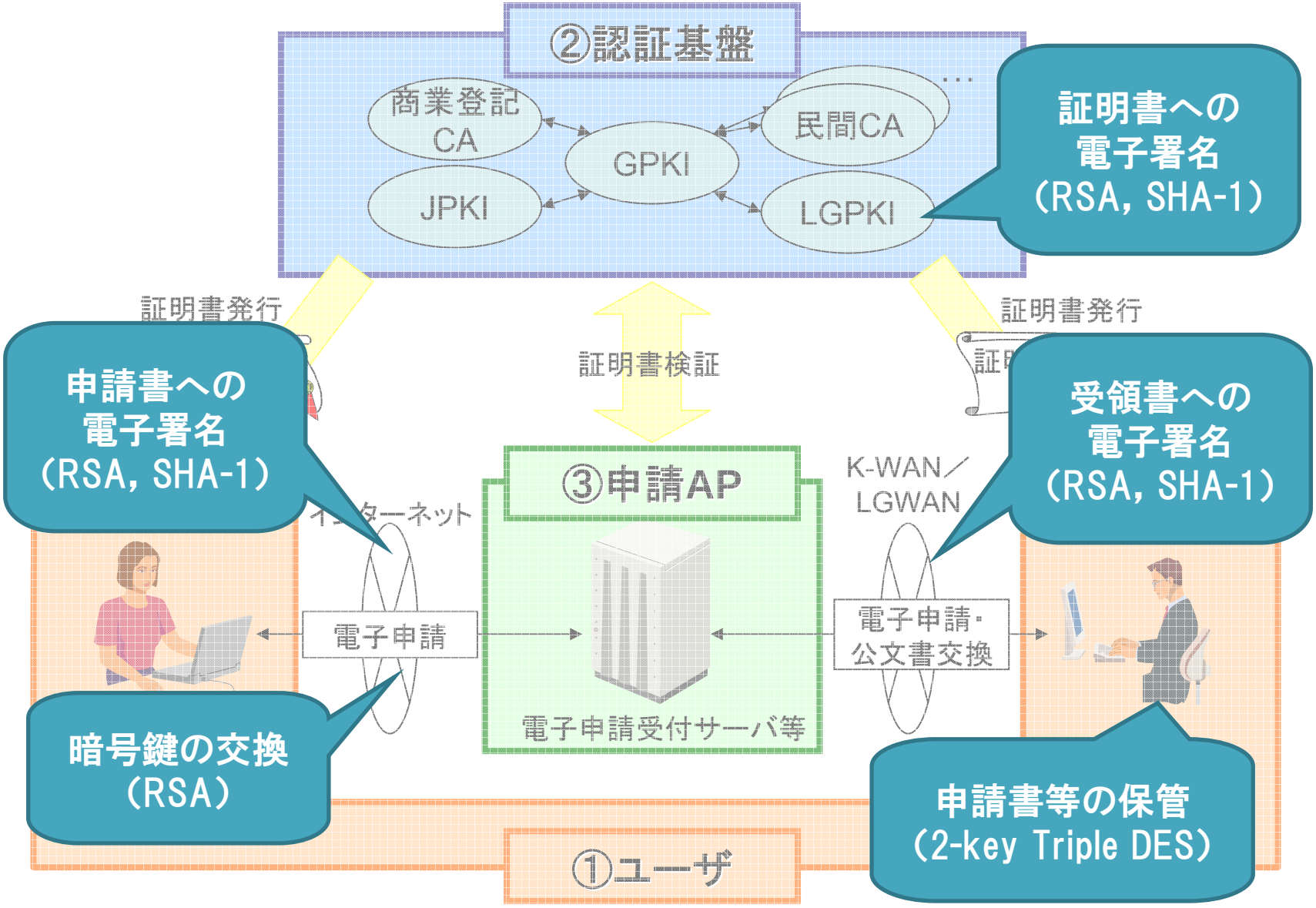
- 暗号2010年問題
  - 米国NIST（国立標準技術研究所）が示した暗号アルゴリズムの移行

米国NISTは，現在連邦政府で利用している暗号アルゴリズム（鍵長）を変更することに決定

日本の電子政府システムは？

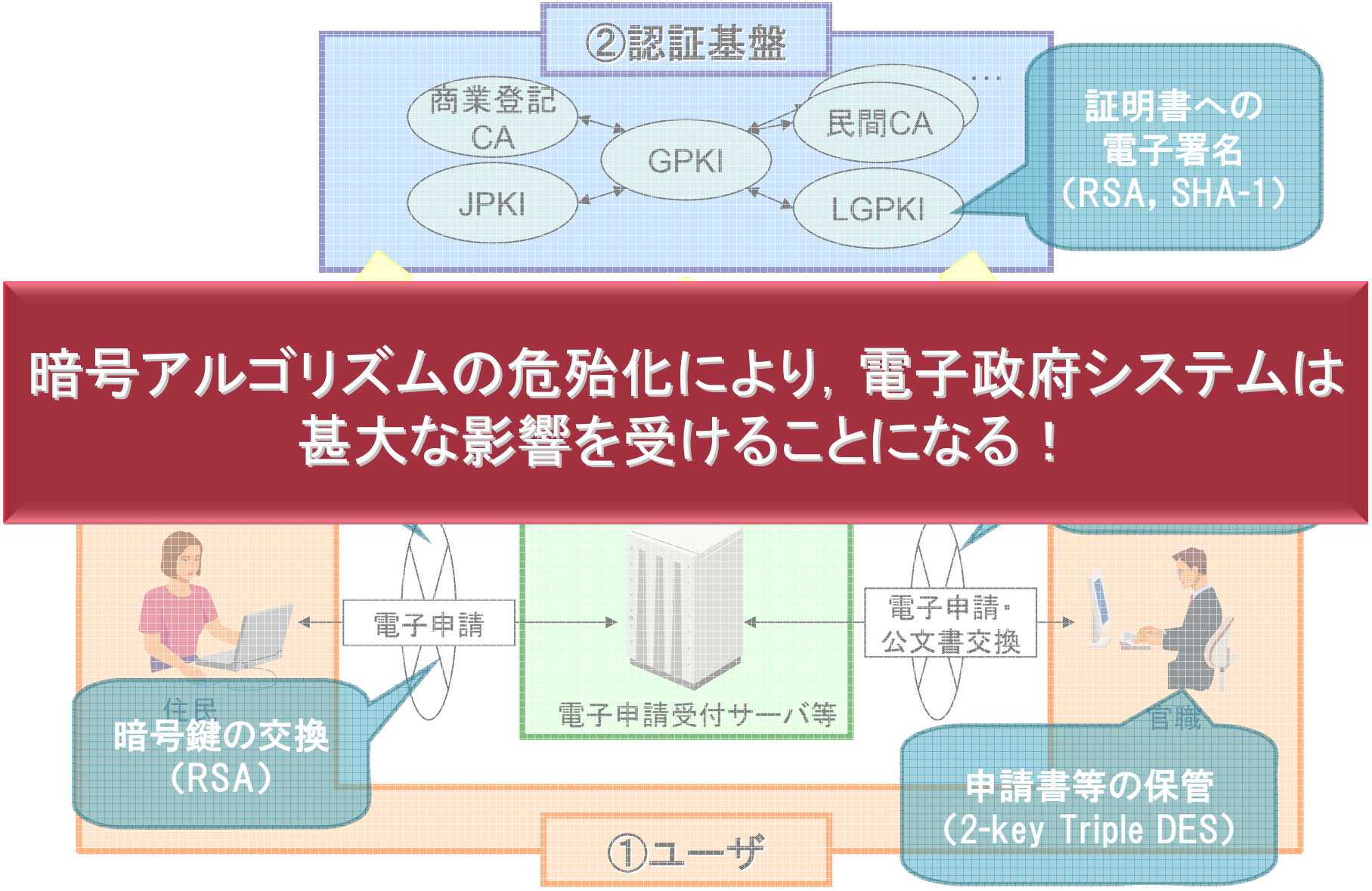
    - 1024bit RSA相当であり，2010年以降は使用を推奨しない（224bit以上）
  - 2-key Triple DES
    - 2010年以降は使用を推奨しない（3-key Triple DES or AES）

1-5　電子政府システムへの影響（概要）



1-5　電子政府システムへの影響（概要）

HITACHI
Inspire the Next



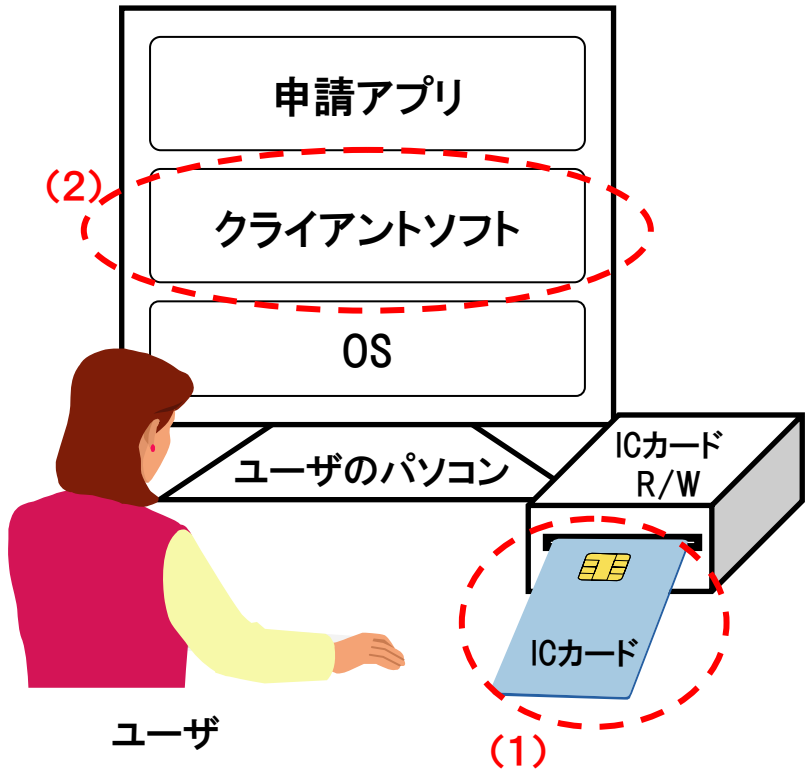
1-6 電子政府システムへの影響(詳細)

HITACHI
Inspire the Next

ユーザへの影響

(1)ICカード
- 利用者の秘密鍵及び証明書を格納
- ICカード内で暗号演算を実施

(2)クライアントソフト
- ICカードを利用した署名生成，署名検証，証明書取得，証明書表示等を実施するために必要となるクライアントソフト

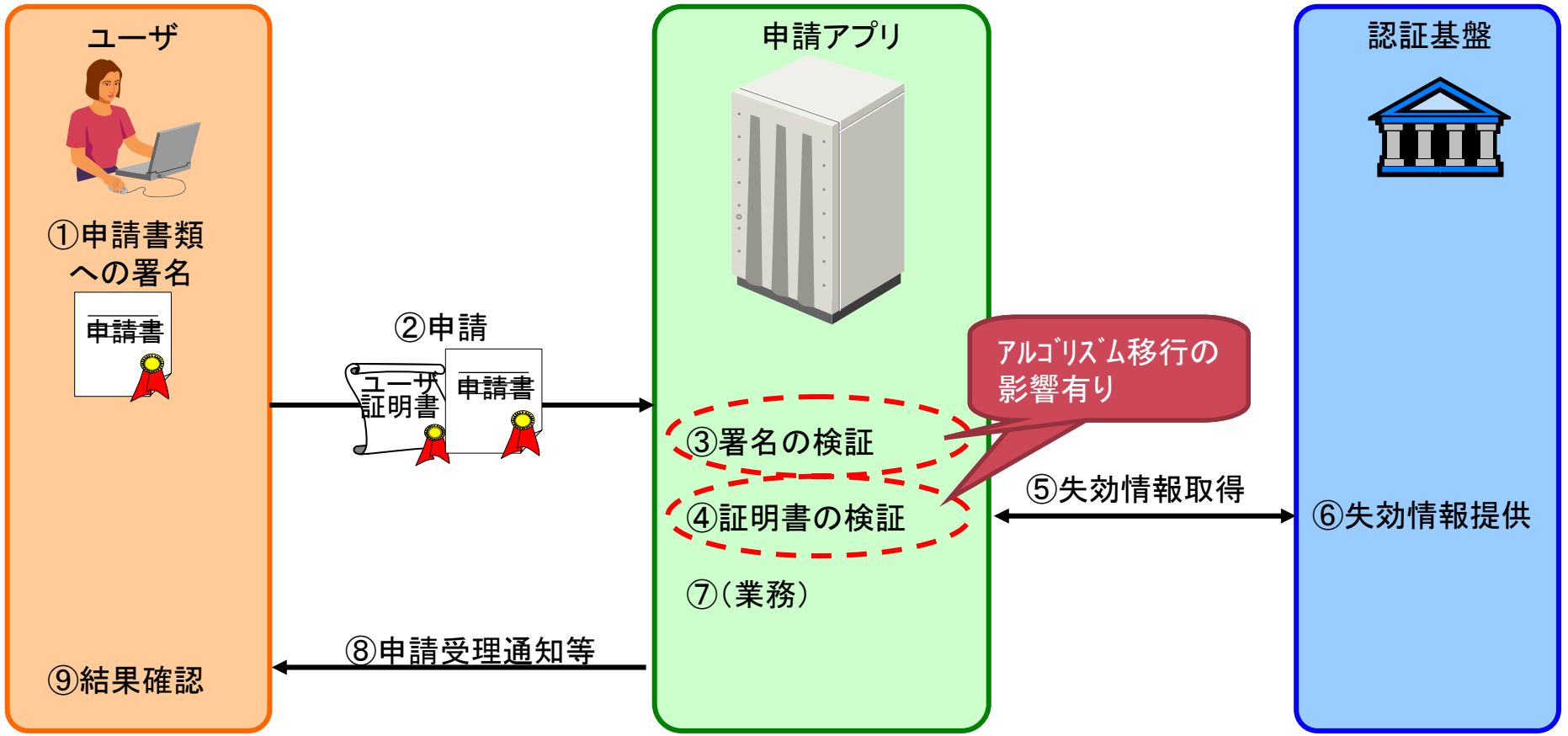


JPKIで利用されている住基カードをはじめとして，GPKIやLGPKI，商業登記CA，民間CAで利用されているICカードとクライアントソフトに影響がある

1-6 電子政府システムへの影響(詳細)

HITACHI
Inspire the Next

申請APへの影響

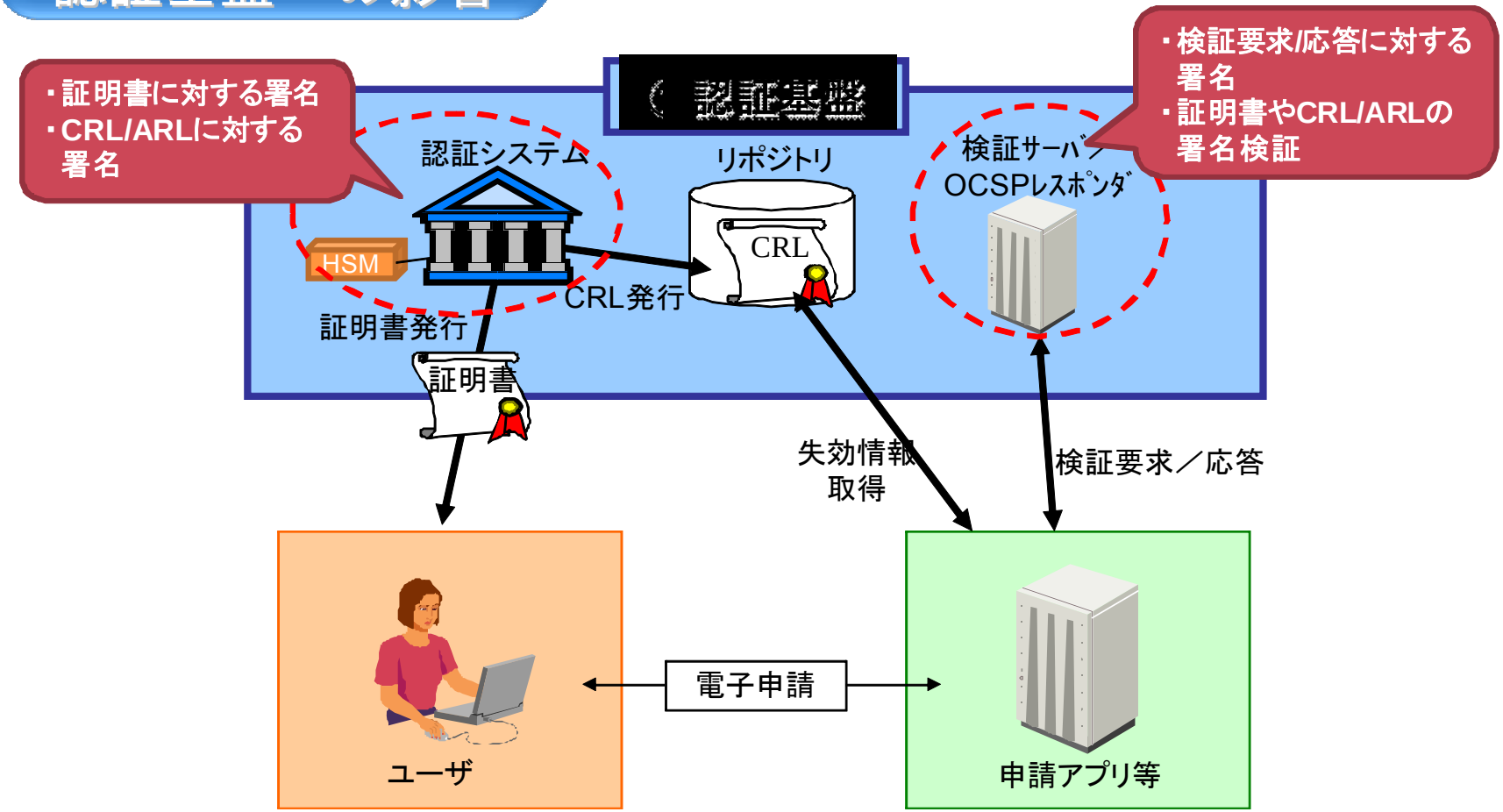


行政機関(府省)や地方公共団体(都道府県，市町村)が提供している申請アプリにおいて，それぞれ影響がある

1-6 電子政府システムへの影響(詳細)

HITACHI
Inspire the Next

認証基盤への影響

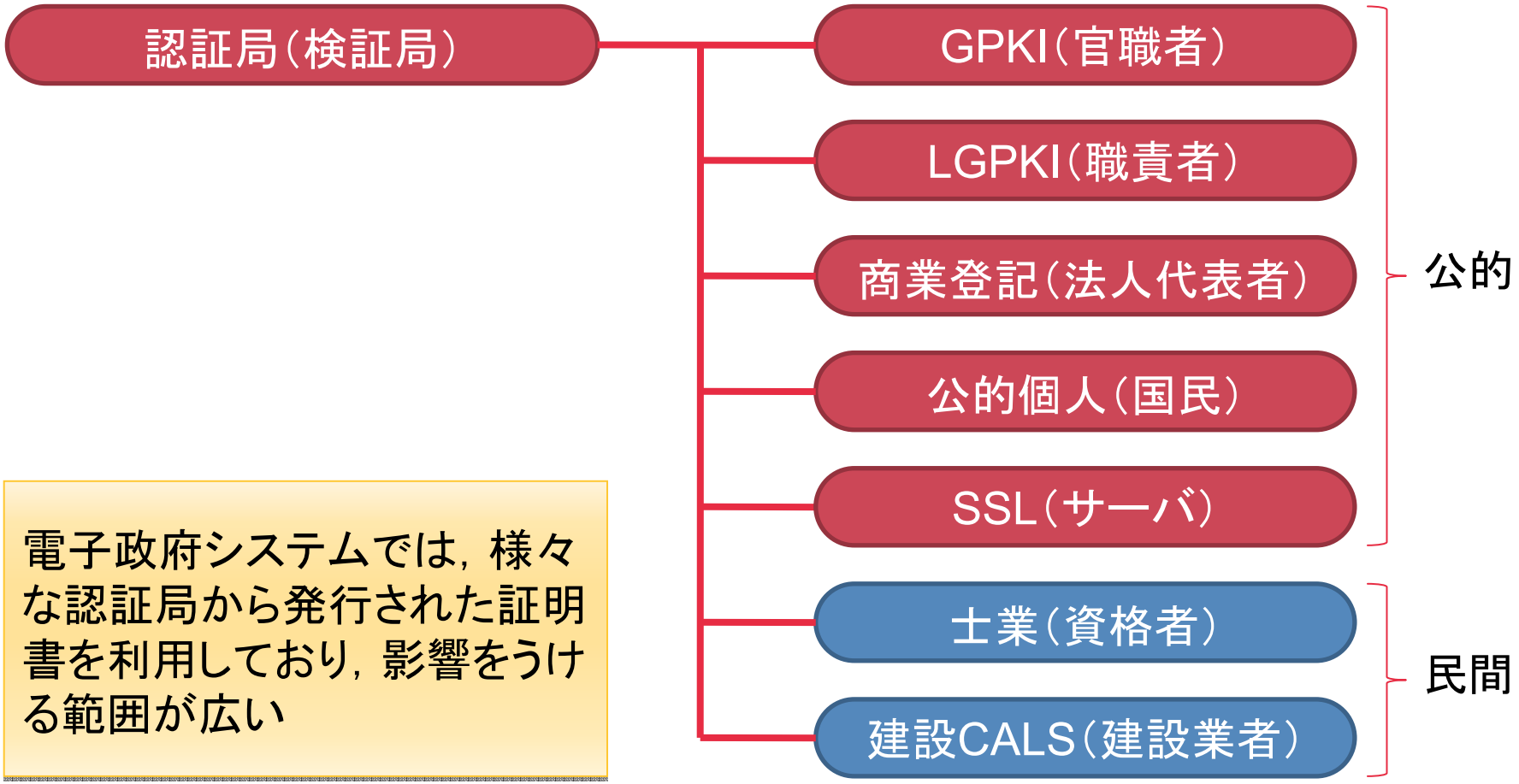


GPKI，JPKI，LGPKI，商業登記CA，民間認証局等において，それぞれ影響がある

1-6 電子政府システムへの影響(詳細)

HITACHI
Inspire the Next

認証基盤への影響



電子政府システムでは，様々な認証局から発行された証明書を利用しており，影響をうける範囲が広い

1-7 システム移行時の問題点

HITACHI
Inspire the Next

- 現在ユーザ（クライアントソフト），申請AP，認証基盤で使用している暗号アルゴリズムを，新たな暗号アルゴリズム（鍵長）に変更することは製品準備が済めば可能
- ただし，すべての既存システムを一斉に改修することは困難だと思われるので，並行運用期間が必要（どれくらいになるか不明）
- 上記状態だと，下記のような問題が生じる可能性大
  - 申請AP1と申請AP2が別の暗号アルゴリズムを利用している場合には，ユーザは二つの秘密鍵，証明書を使い分ける必要あり（ICカード2枚？）
  - 上記に合わせて認証基盤側は，暗号アルゴリズムが異なる複数種類の証明書，CRL/ARL等を発行する必要あり（ルート証明書も2枚？）
  - 同様に検証サーバ（OCSPレスポンダ）の検証結果（レスポンス）も，リクエスト相手に合わせる必要あり

認証基盤は最後まで影響を受ける

運用も含めて計画的にシステム移行しないと，いつまでたっても並行運用（システムの二重化）状態から脱却できない恐れあり！（単なるシステム改修（暗号モジュールの取替）では対応できない）

1-7 システム移行時の問題点

HITACHI
Inspire the Next

- その他問題となりそうな事項
  - 既にユーザに配布しているICカードの回収と新たなICカードの配布
    - 格納された証明書の有効期限がバラバラ
    - 一斉交換　or 順次交換？
    - 住基カードの場合は，国民に市区町村役場に来てもらう必要あり
  - クライアントソフトには，OS等に付属の暗号ライブラリを利用しているケースあり
    - OSがサポートしている暗号しか利用できない（XPではNGの恐れあり）
    - クライアントソフトに暗号ライブラリを包含するように全面修正？

1-8 システム移行に向けた検討課題

HITACHI
Inspire the Next

- システム移行の期限
  - NISTと同様のRecommendationを日本としても発表するか？
    - CRYPTRECの評価結果を受け，国として決定？
  - 電子政府システムにおける暗号移行期限を設定するか？
    - 明確な移行期限がないといつまでも対応しないシステムが出てきてしまう恐れあり
- 製品の入手，システムの更新
  - Webブラウザ： Vista+IE7ならSHA-2, 2048bit RSAはすでにサポート
  - SSLサーバ： SHA-2未対応が多数（2048bit RSAはOK）
  - 認証局，HSM： SHA-2サポート製品も増えてきている（2048bit RSAはOK）
  - ICカード： SHA-2, 2048bit RSA未対応が多数
  - Java： 問題なし
- システム移行手順の策定
  - 所管省庁（開発ベンダ）が異なるが相互に依存関係にある既存電子政府システムをどのような手順で移行するか？
    - 整合性をとって移行しないと利用できなくなる危険性大！

1-9 システム移行に向けた施策(案)

HITACHI
Inspire the Next

- 所管省庁(開発ベンダ)が異なるが相互に依存関係にあるシステムを，ある時期に一斉に移行する際に，机上での検討だけで移行手順を決めるのでは不具合が生じる可能性が高い
- 移行期間前に処理した大量のデータ(署名付きデータ，暗号保管データ)を一括して変換(再署名，再暗号化)する必要がある

◆ テストベットの構築
  - シミュレーション，実証実験等を実施し，安全な移行手順(複数システム間での移行順序等も含む)を策定
  - 複数ベンダでの相互接続性テストに活用
  - 今後同様の事象が発生した場合にも利用可能

◆ 移行支援ツールの開発
  - 署名付きデータを再署名するツール
  - 暗号化されて保管されているデータを再暗号化するツール

1-10 （参考）海外状況

HITACHI
Inspire the Next

- 米国SP800-57 “Transitioning to New Algorithms and Key Sizes”で基本的な移行手順をガイダンス
  1. Sensitivity of information and system lifetime
  2. Algorithm selection
  3. System design
  4. Pre-implementation evaluation
  5. Testing
  6. Training
  7. System implementation and transition
  8. Transition
  9. Post-implementation evaluation

- 米国政府のIP v.6（2008年度に移行予定）の対応例では，調達仕様としてIP v.6対応機器を準備するよう記載されているのみ（ただし，厳密に期日までに用意することを求められているわけではなく，いつまでに用意できるかと約束すればいい案件も多い模様）

1-10 （参考）海外状況

HITACHI
Inspire the Next

- 欧州の状況
  - ECRYPT（欧州委員会FP6の情報テクノロジプログラムの一つ）
    - 攻撃者の能力の観点から暗号アルゴリズムのセキュリティレベルを分析（http://www.ecrypt.eu.org/documents/D.SPA.21-1.1.pdf）
  - フランス（DCSSI：Central Information Systems Security Division）

～ 2010年	2011年～2020年	2021年～
RSA: 1536bit以上 （2048bitを推奨） ECC: 160bit SHA: SHA-224,256	RSA: 2048bit ECC: 160bit SHA: SHA-256	RSA: 4096bit ECC: 256bit SHA: SHA-256

Me'canismes cryptographiques - Re`gles et recommandations "standards", Rev. 1.10, DCSSI , 12/2006

  - ドイツ（BSI：Federal Office for Information Security ）

2008年	2009年	2010年	2011年～2013年
RSA: 1280bit ECC: 180bit SHA: SHA-1※, -224,256	RSA: 1536bit ECC: 180bit SHA: SHA-1※, -224,256	RSA: 1728bit ECC: 224bit SHA:SHA-224,256	RSA: 1976bit ECC: 224bit SHA:SHA-224,256

※ 証明書のみ可
Algorithms for Qualified Electronic Signatures, BNetzA, BSI, 02/2007 updated with BSI Draft, 07/2007

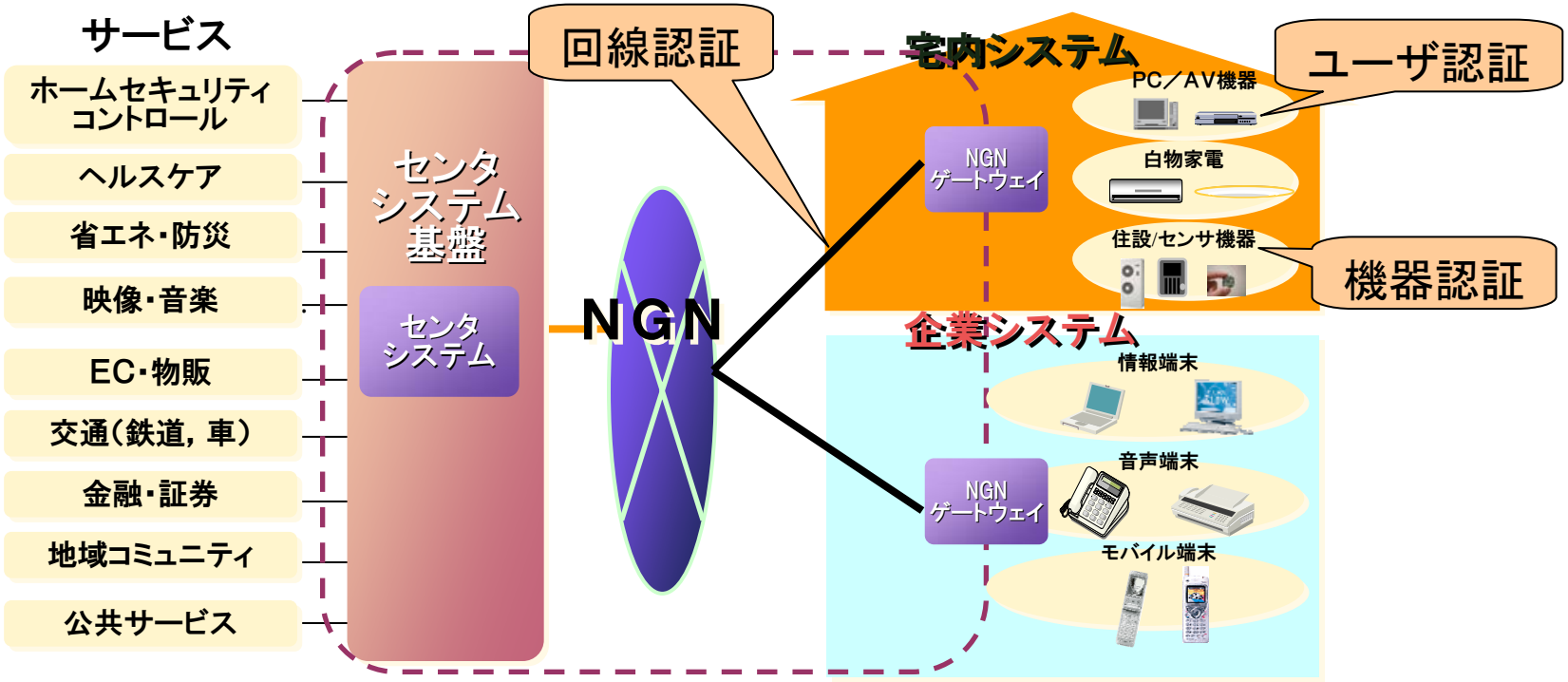
1. 暗号アルゴリズムの危殆化が
   電子政府システムに与える影響と対策

2. NGN時代の認証のあり方

2-1 NGNにおける回線認証

HITACHI
Inspire the Next

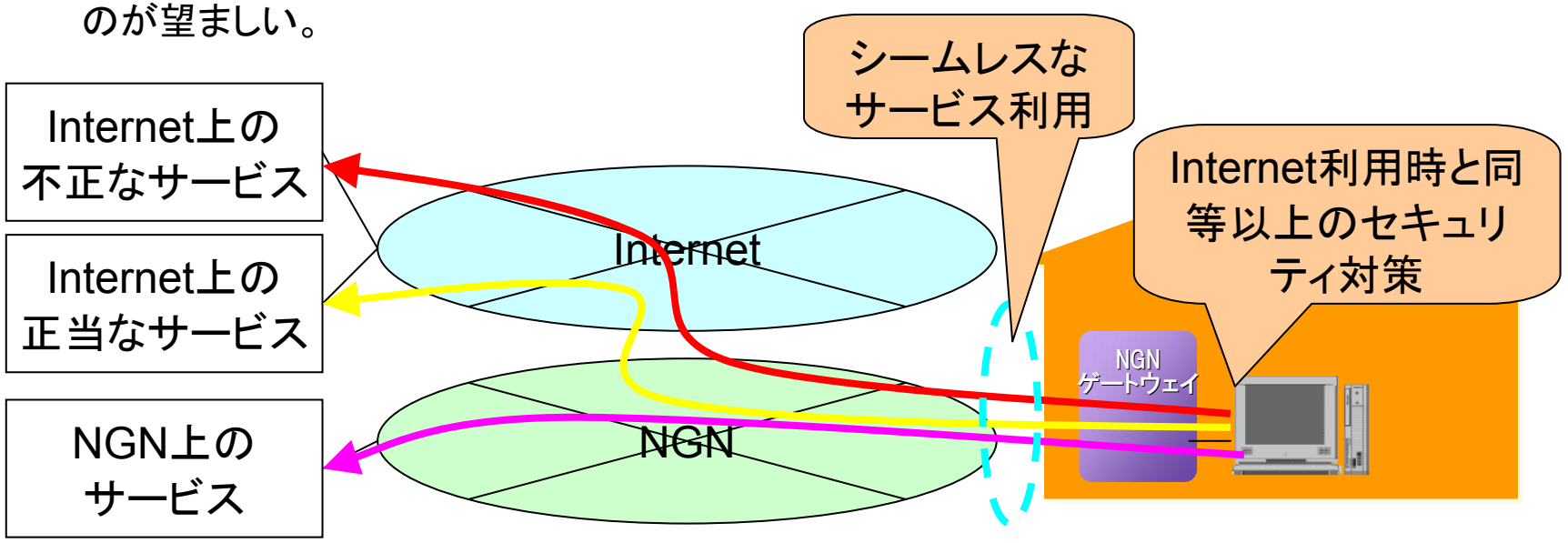
- NGNにおける認証のセキュリティ課題
  - NGNにおいては、認証機能によりセキュリティが向上するといわれているが、その認証の範囲は、回線認証(つまり、各家庭、SOHOなどの入り口まで)に留まっている。
  - しかしながら、アプリケーション、サービスによっては、回線認証では、不十分であり、実際のEnd機器、ユーザを対象とした認証機能が必要な場合がある。
  - 課題は、場合に応じてユーザ認証、機器認証が必要となること、またそれら認証機能と回線認証の連携を検討する必要があること。



2-2 NGN／Internetのシームレス利用

HITACHI
Inspire the Next

- NGNとInternetの同時利用時のセキュリティ課題
  - NGNでのネットワークアクセスはNGN内に閉じたアプリケーション、サービスへのアクセスだけに留まらず、Internetへアクセスするための、足回りとして利用される。
  - この場合、利便性の観点から、NGNサービスとInternetサービスのシームレスな利用が考えられる（一々回線を切り替えたりしない）。
  - したがって、Internet上の脅威は、NGNを利用していたとしても、依然として存在し続け、また、ユーザがNGNを使っていると安心している時に、実は、不正なInternetサイトにアクセスしているのかもしれない。(フィッシング、クロスサイトスクリプティング)
  - 前記、認証方式においてもNGNとInternetの双方のサービスで連携して提供されるのが望ましい。



2-3 NGN時代の認証の在り方

HITACHI
Inspire the Next

- 回線認証とユーザ認証／機器認証との連携
  - NGNにおける回線認証と、ユーザ認証／機器認証を連携させることにより、柔軟性、安全性の高い認証を実現することが望まれる。

- NGN／Internetのシームレス利用を可能とする認証方式
  - 依然存在し続けるInternet上の脅威に対応するため、NGN／Internet双方のサービスで連携して安全な認証方式が提供されることが望まれる。

END

