電子認証局会議
Certification Authority Conference

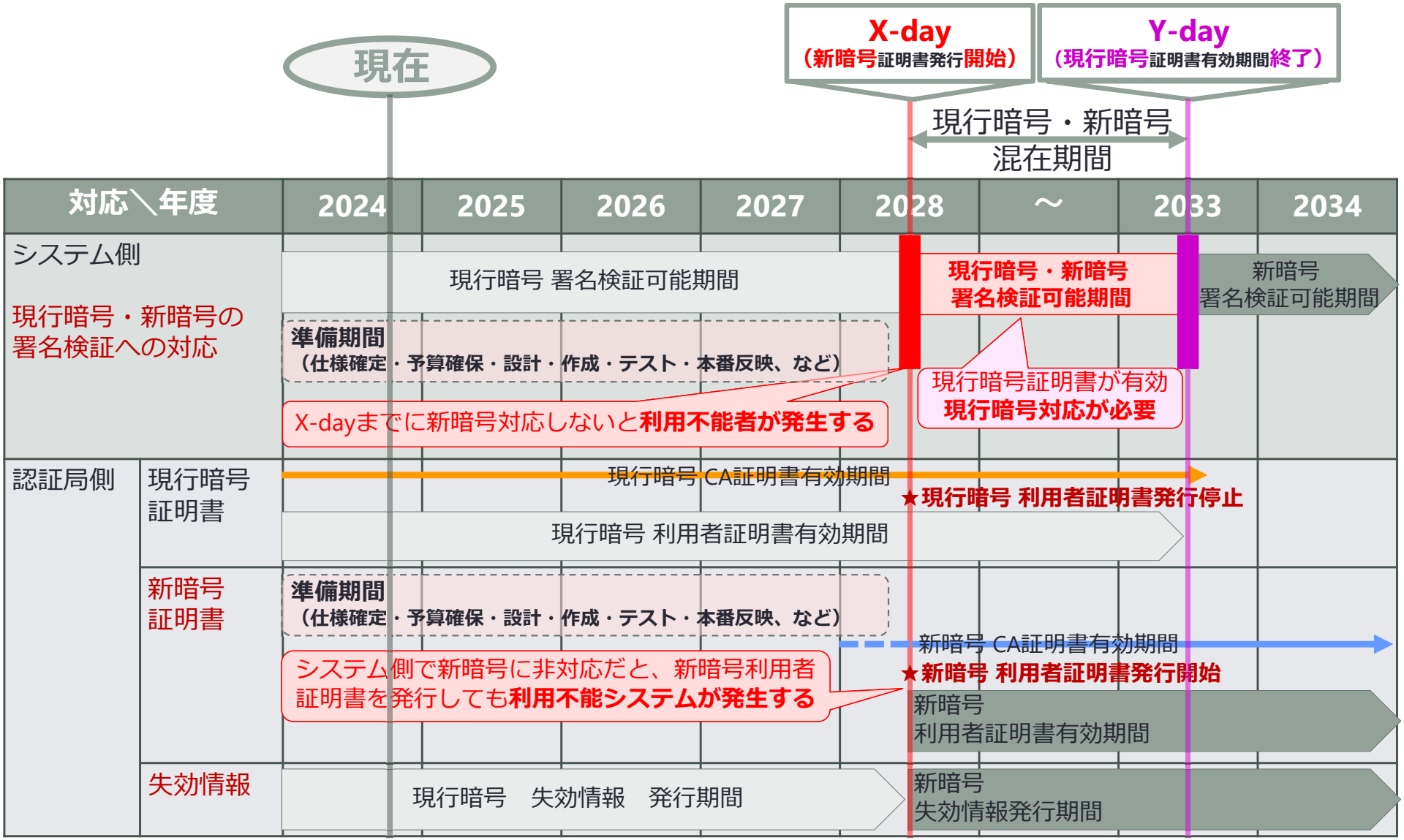
2028年暗号移行に関する説明

2025年3月18日
電子認証局会議

暗号移行のポイント

電子認証局会議
Certification Authority Conference

- 暗号移行は、証明書を利用するシステム側と証明書を発行する認証局側での**連携・調整**が不可欠。
- 暗号移行を円滑に実施するため、**イベントを意識した準備**や綿密な**関係者連携**が最重要課題。



暗号移行に関するシステムへの影響

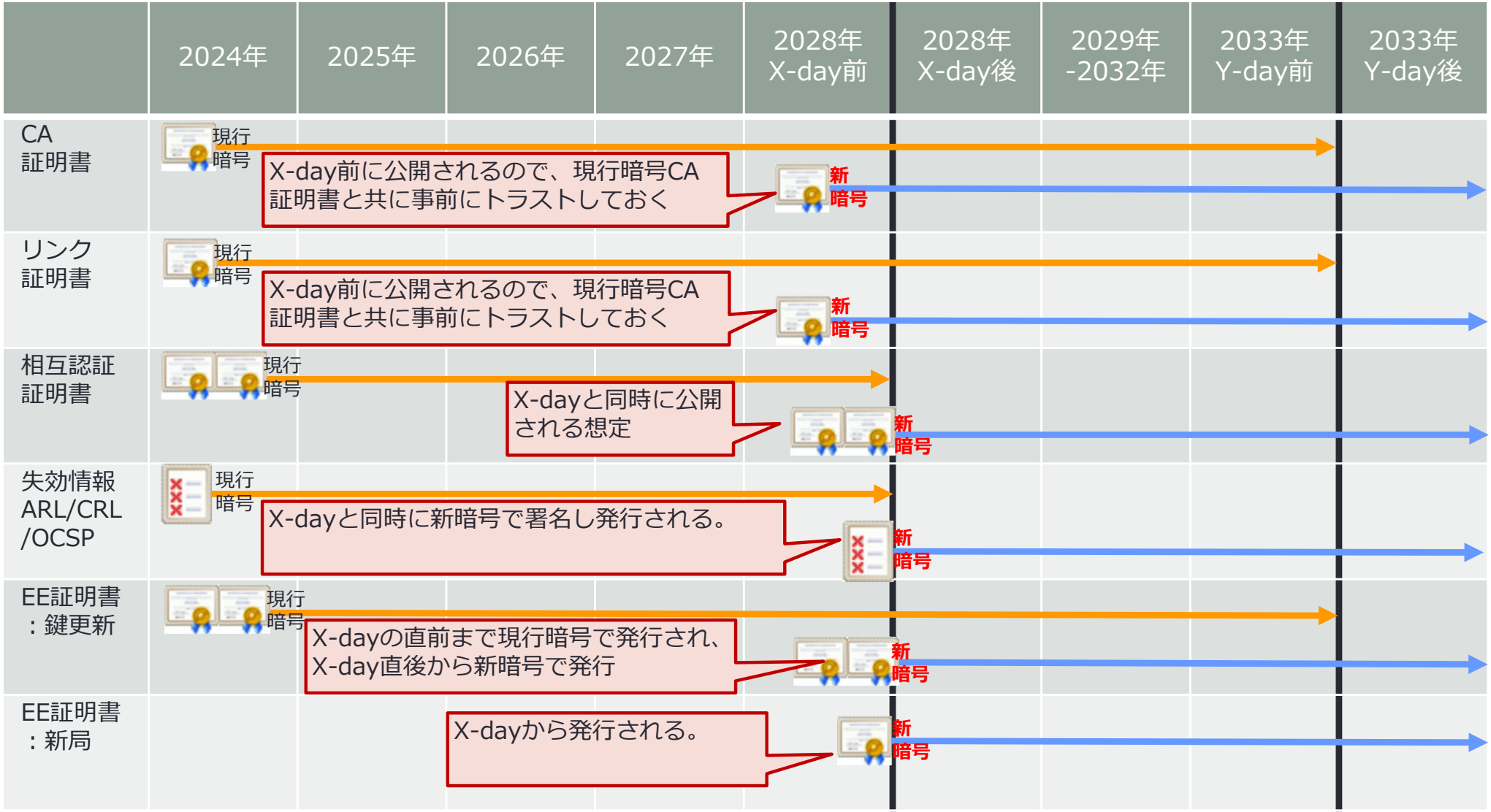
電子認証局会議
Certification Authority Conference

1. システム側で「新暗号方式の対応」が必須
   - ① X-day以降、システムで「新暗号方式での署名生成・署名検証」は必須
   - ② X-day以降Y-dayまでは現行暗号の電子証明書が残るため、「現行暗号方式での署名生成・署名検証も継続」して必須
2. 署名検証に必要な以下の内容に関して、X-dayと同時に新暗号方式で署名されるため新暗号での署名検証対応が必須
   - ① CA証明書類（自己署名証明書、リンク証明書、相互認証証明書）
   - ② 失効情報（ARL、CRL、OCSP）
   - ③ EE証明書は、現行暗号方式・新暗号方式が混在

参考：暗号移行前後における証明書等

電子認証局会議 Certification Authority Conference

■ EE証明書以外に署名検証で必要な内容に関しては以下のとおり。



現行暗号：現行暗号で署名　/　新暗号：新暗号で署名

関係者への依頼事項

電子認証局会議
Certification Authority Conference

- X-dayの実日程調整
  - GPKI、LGPKI、CACなどでの調整を実施。最終日程から、様々な事前調整の日程感が判明する。
- X-dayに向けた認定や審査の日程調整
  - X-day確定後、JIPDEC・GPKI・CACなど関係者間での調整を実施する。
- システム側における検証環境に基づくテストの実施
  - X-day以降の新暗号方式の署名生成・署名検証を実装し、検証環境でテストを実施する。
  - X-day以降Y-dayまでは現行暗号のEE証明書が残るため、現行暗号方式の署名生成・署名検証は継続的に必要なので両環境が混在する状況のテストも実施する。
  - システムによりEE証明書の暗号がいずれであるか確認する実装が必要であれば、当該実装を行ったうえでテストを実施する。
  - テスト日程はGPKIの新暗号移行検証環境の準備、およびLGPKI・CAC所属各社の同検証環境でのテスト実施日程を含めて調整する。