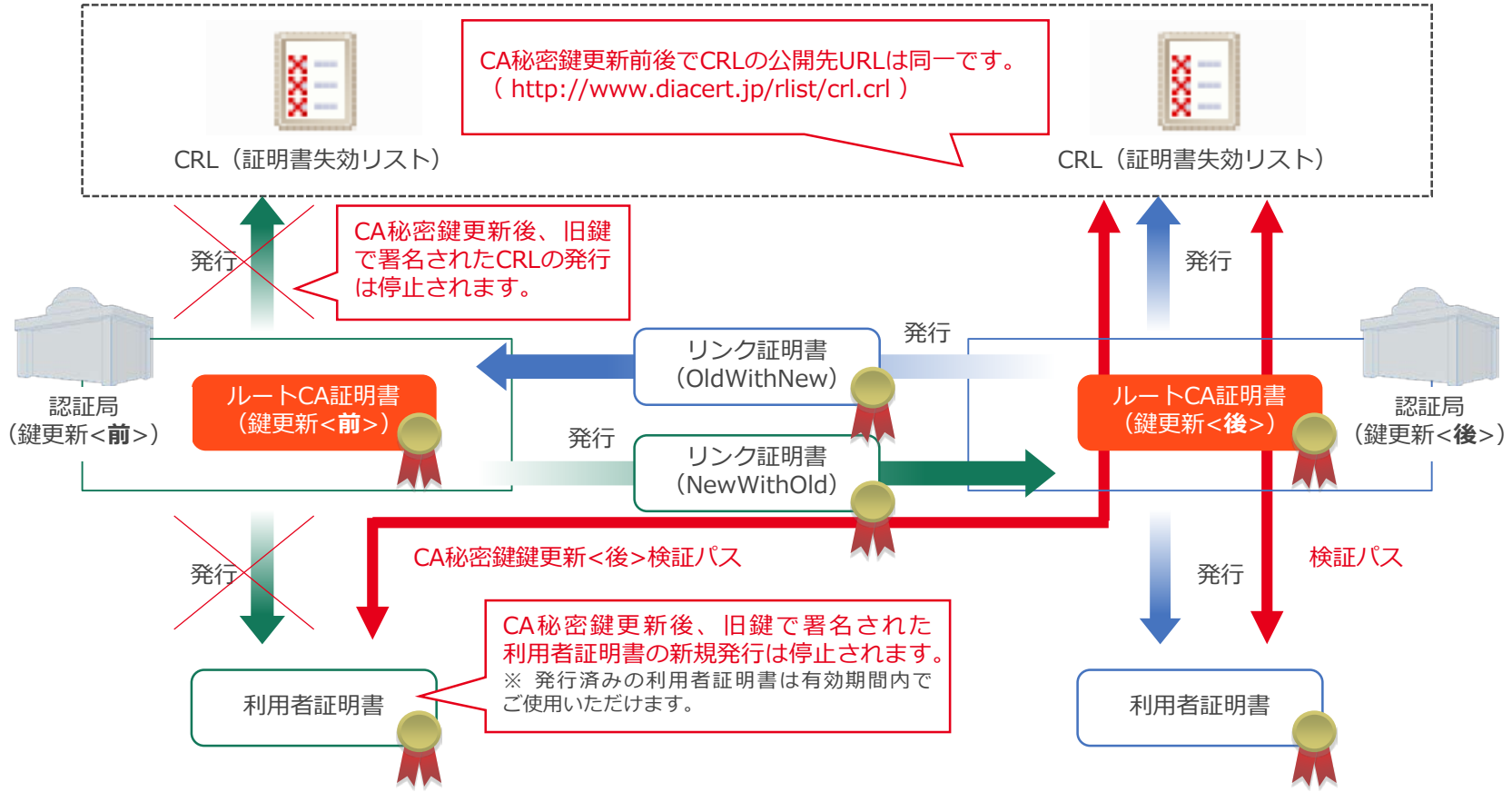
認証局秘密鍵更新時の有効性検証パスイメージ

- 認証局（以下、CA）秘密鍵更新時は、新しいルートCA証明書と共に古い世代のルートCA証明書と新しい世代のルートCA証明書を紐付けるリンク証明書を作成し、リポジトリに公開します。
  - CA秘密鍵更新前に発行した利用者証明書の有効性検証を行う場合は、リンク証明書の検証パスを辿ってCA秘密鍵更新後のCAから発行されたCRLの検証を行う形となります。



※ CRL（Certificate Revocation List）…認証局が失効させたエンドエンティティ証明書のリストです。 CRLを確認することで、 電子証明書が失効していないかどうかを確認することができます。

※ リンク証明書…認証局の鍵更新時に、同時に存在することとなる新しい認証局の鍵ペアと古い認証局の鍵ペアの関係を保証するために発行される電子証明書です。