参考資料１

CA/SubCA鍵更新時の処理について

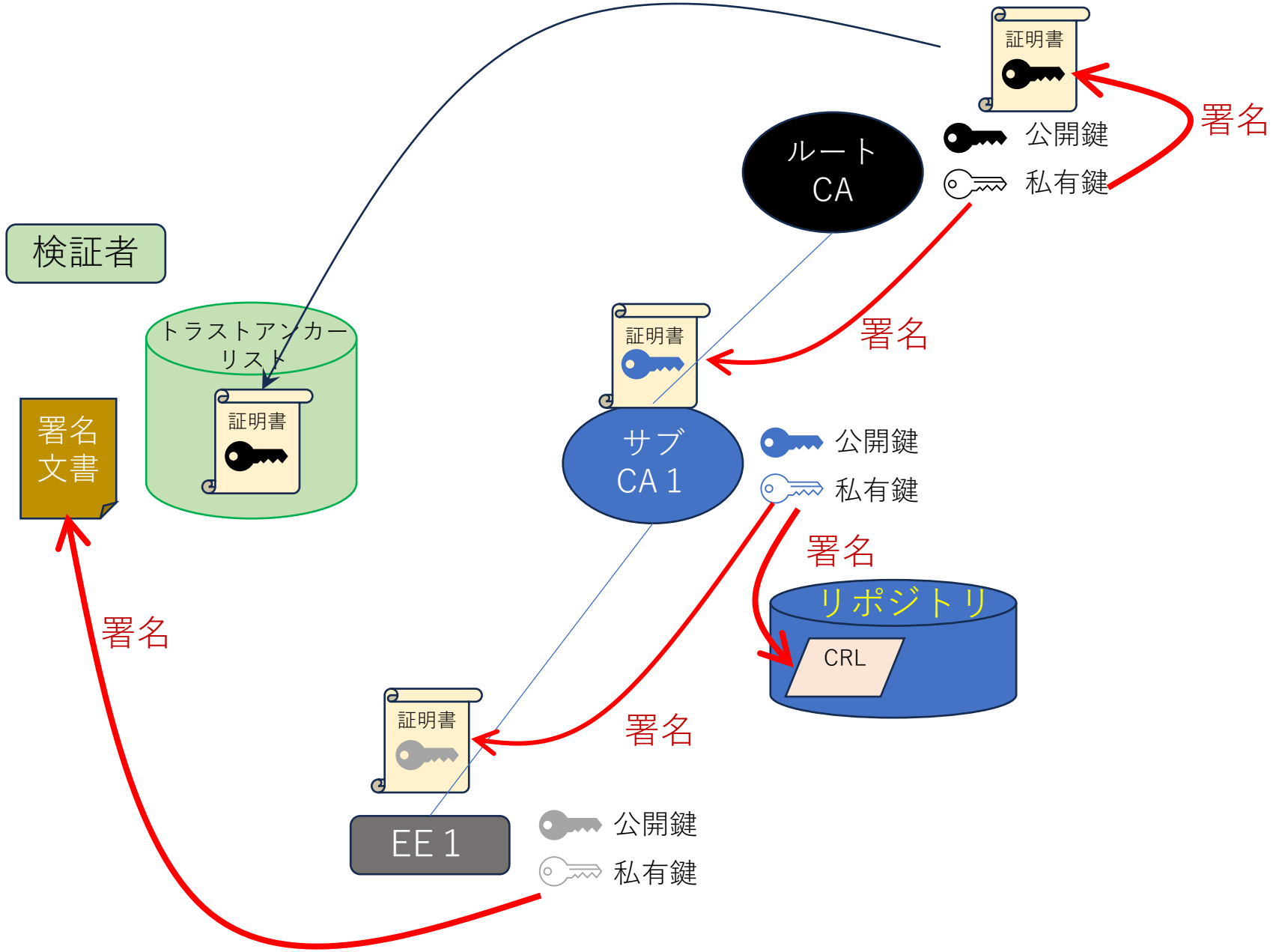
2024/5/16

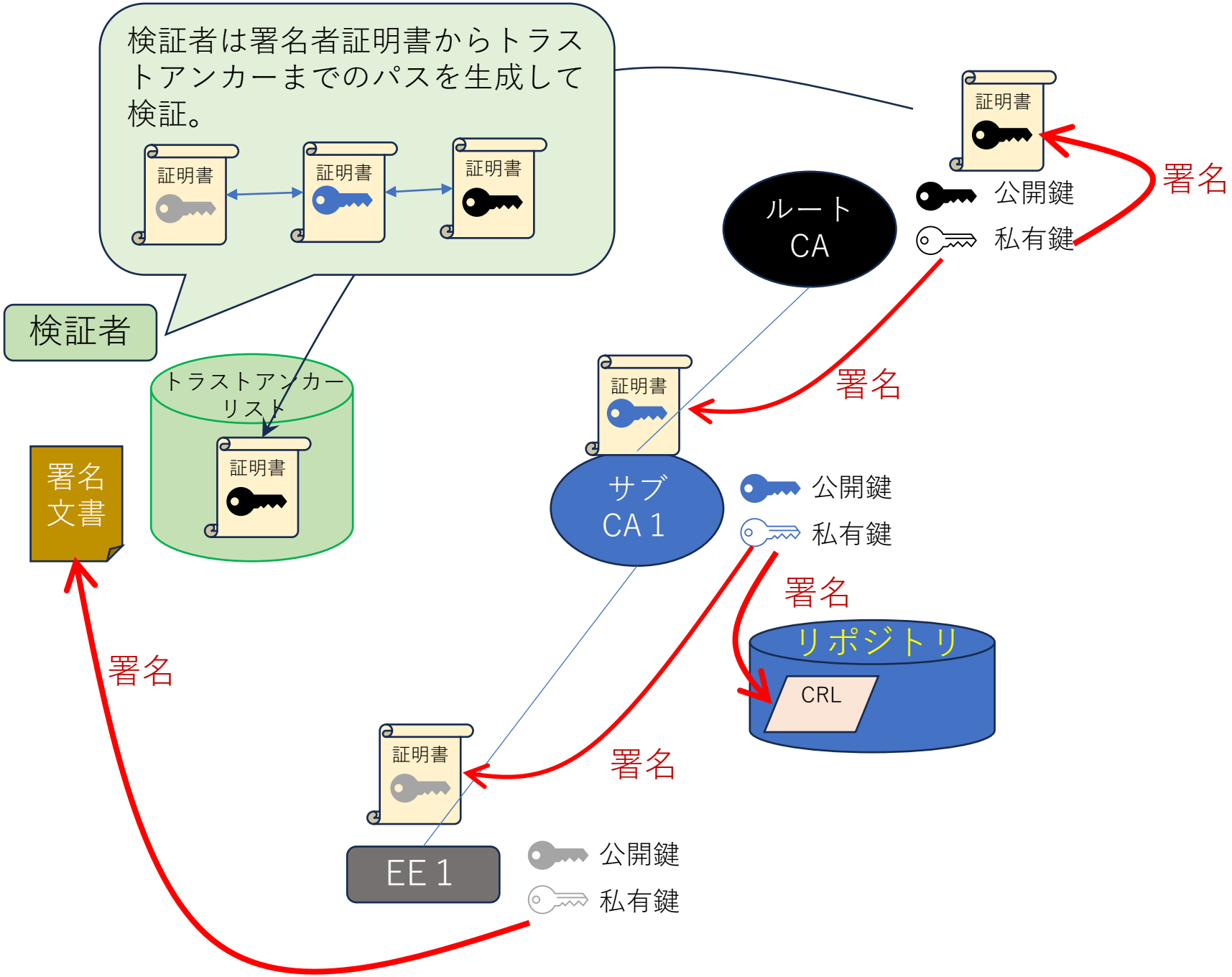
JDTF　宮崎

説明の流れ

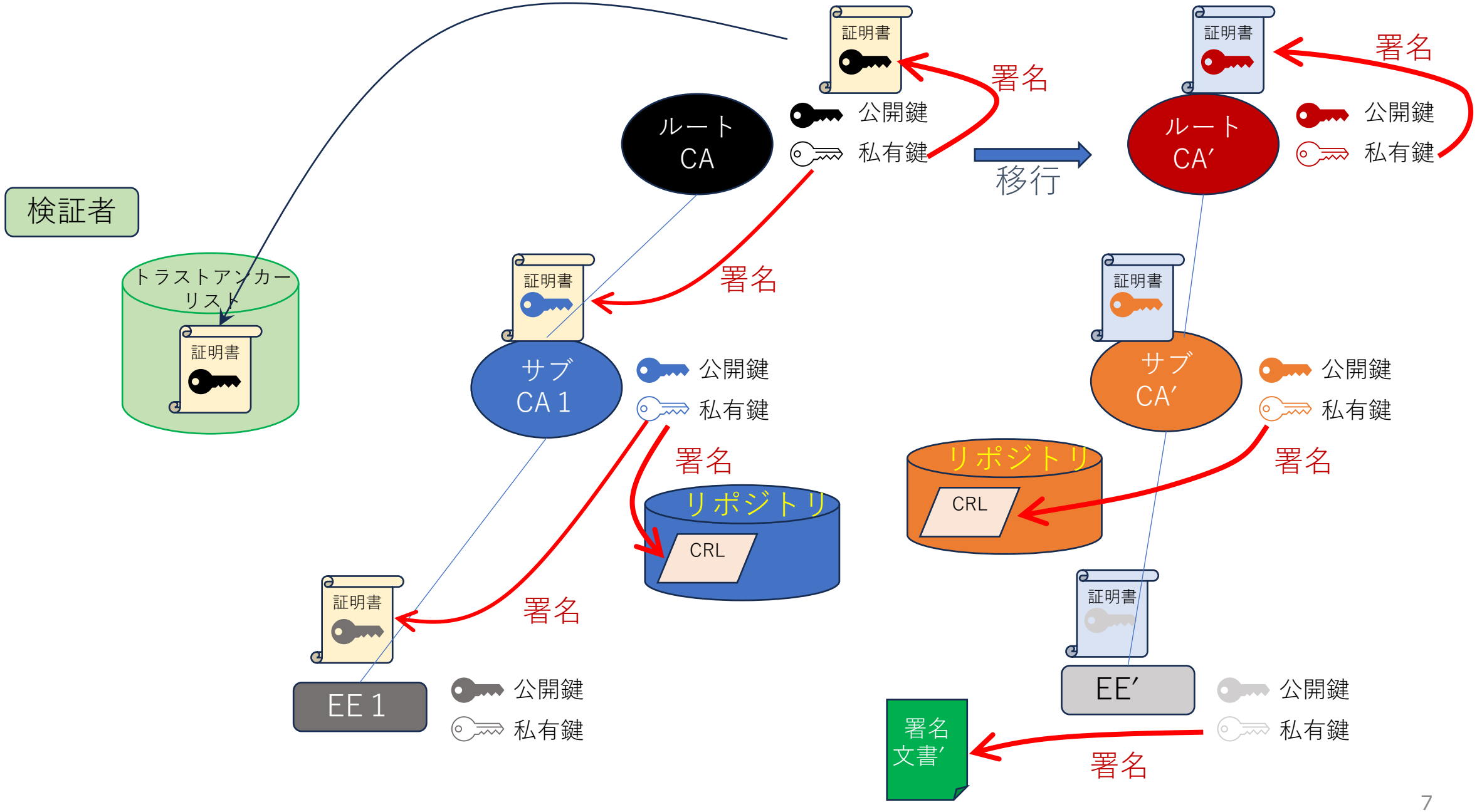
- 証明書検証処理の基本
- ルートCA移行に伴うリンク証明書の必要性
- サブCA移行に伴うリンク証明書の不必要性
- 問題となりそうな点

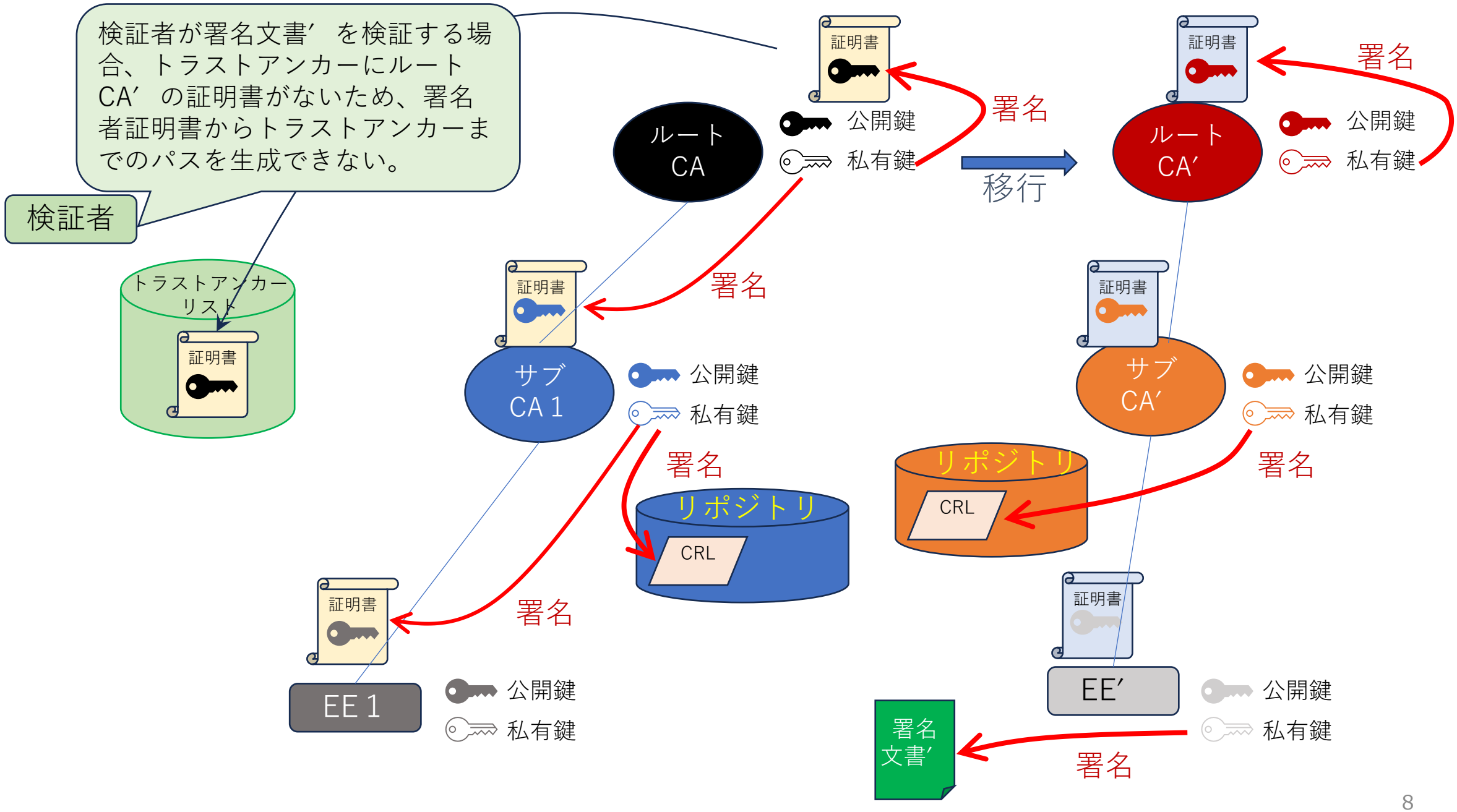
証明書検証処理の基本

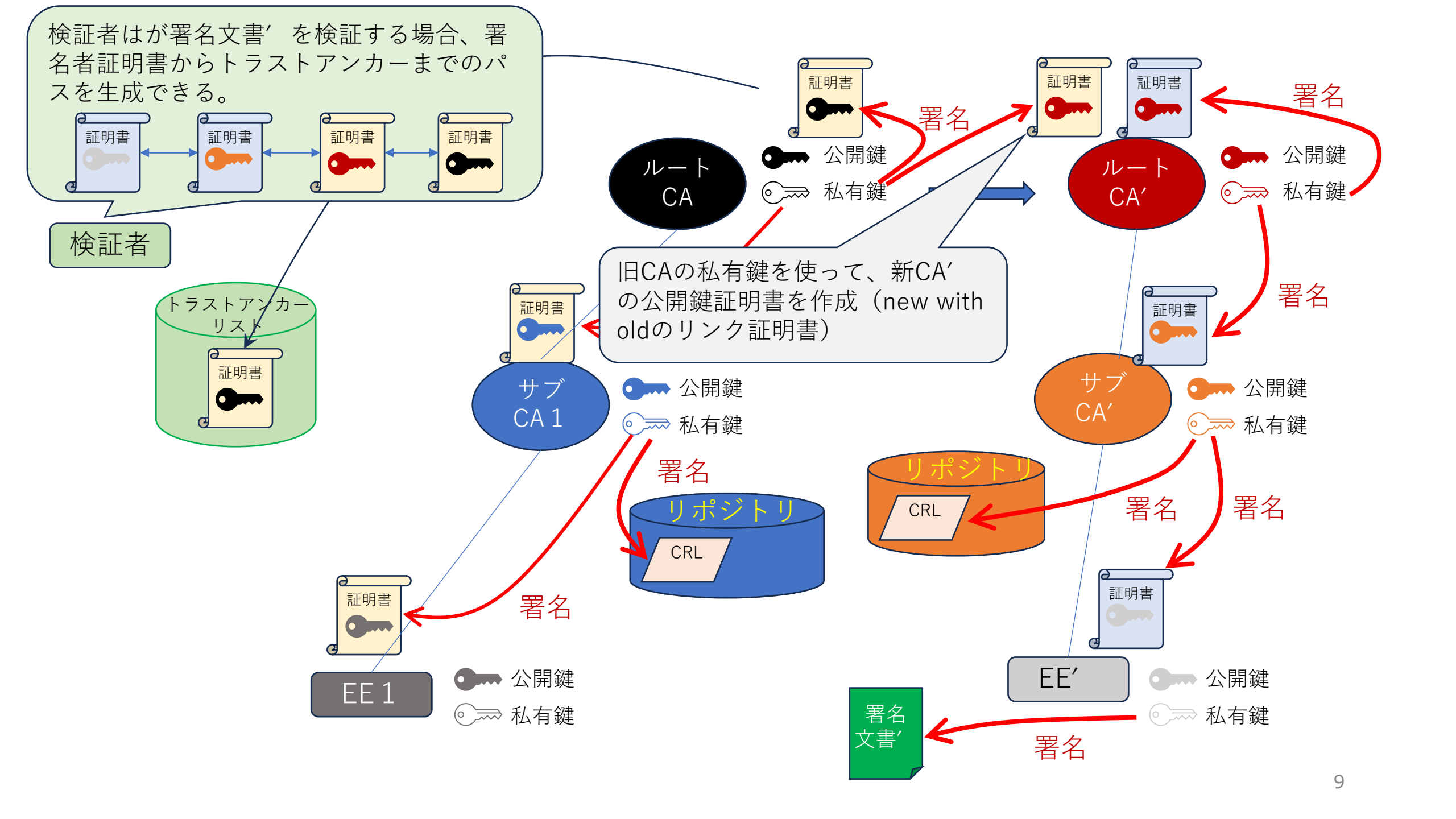

証明書
署名
ルート
CA
公開鍵
私有鍵
検証者
トラストアンカー
リスト
証明書
署名
文書
証明書
サブ
CA 1
公開鍵
私有鍵
署名
リポジトリ
CRL
署名
証明書
署名
EE 1
公開鍵
私有鍵
署名

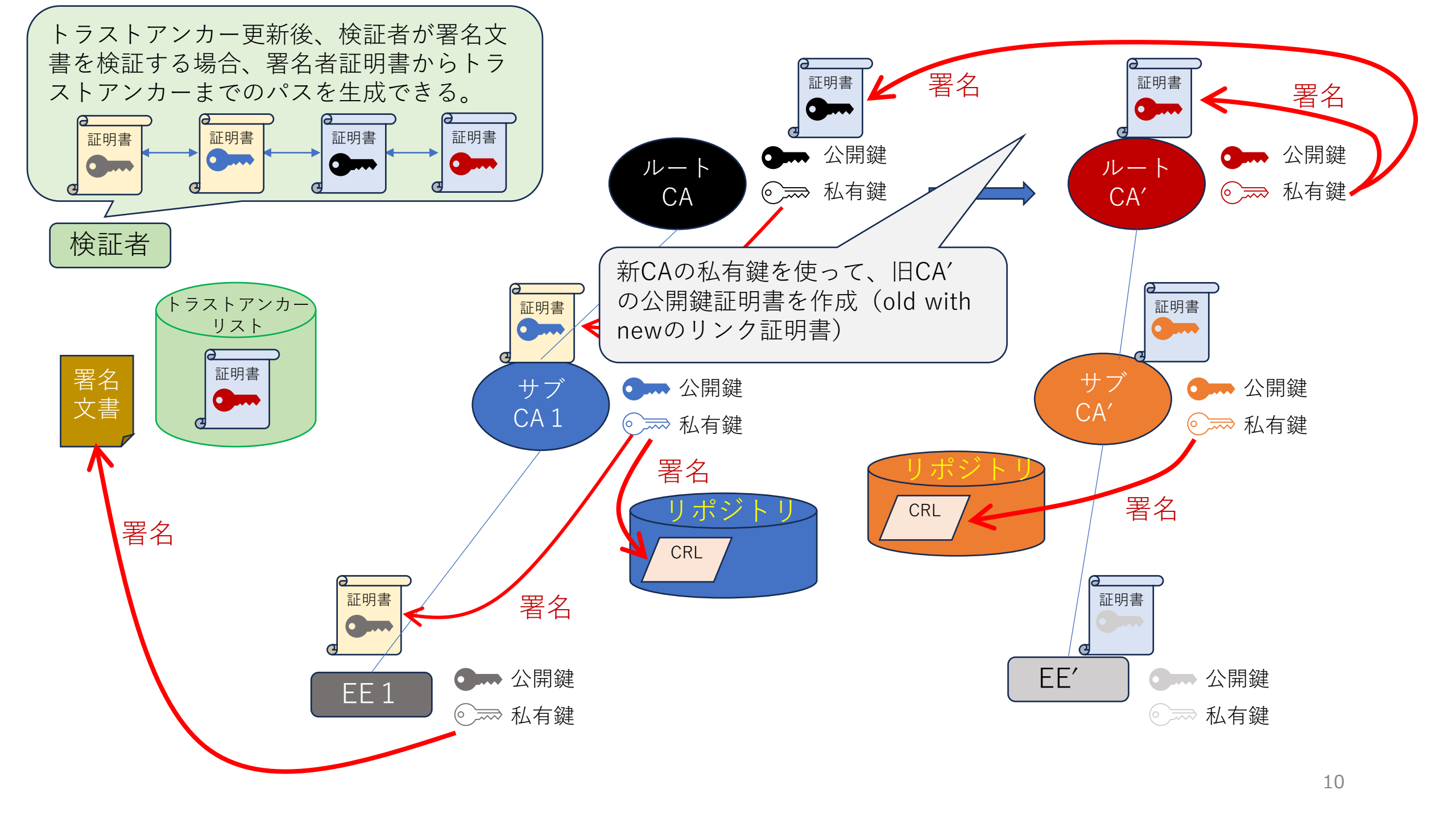

検証者は署名者証明書からトラストアンカーまでのパスを生成して検証。
証明書
証明書
証明書
検証者
トラストアンカーリスト
証明書
署名文書
署名
ルートCA
証明書
公開鍵
私有鍵
署名
署名
証明書
サブCA 1
公開鍵
私有鍵
署名
リポジトリ
CRL
署名
証明書
EE 1
公開鍵
私有鍵

ルートCA移行に伴うリンク証明書の必要性

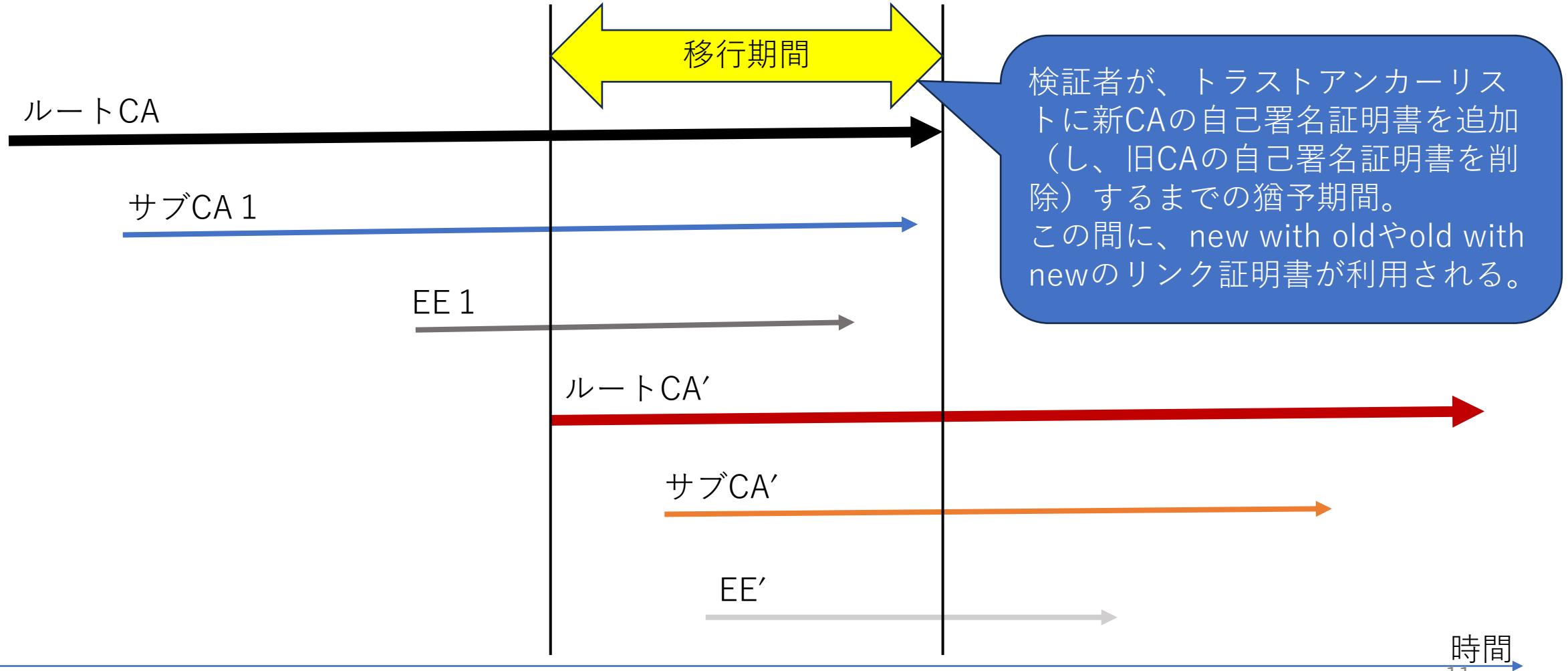

検証者
トラストアンカー
リスト
証明書
ルート
CA
証明書
公開鍵
私有鍵
署名
移行
ルート
CA′
証明書
署名
公開鍵
私有鍵
サブ
CA 1
証明書
署名
公開鍵
私有鍵
リポジトリ
CRL
署名
サブ
CA′
証明書
公開鍵
私有鍵
署名
リポジトリ
CRL
EE 1
証明書
署名
公開鍵
私有鍵
EE′
証明書
公開鍵
私有鍵
署名
署名
文書′
署名


検証者が署名文書′を検証する場合、トラストアンカーにルートCA′の証明書がないため、署名者証明書からトラストアンカーまでのパスを生成できない。
検証者
トラストアンカーリスト
証明書
ルートCA
証明書
公開鍵
私有鍵
署名
移行
ルートCA′
署名
公開鍵
私有鍵
証明書
サブCA 1
公開鍵
私有鍵
署名
リポジトリ
CRL
署名
証明書
EE 1
公開鍵
私有鍵
署名
証明書
サブCA′
公開鍵
私有鍵
署名
リポジトリ
CRL
証明書
EE′
公開鍵
私有鍵
署名文書′
署名

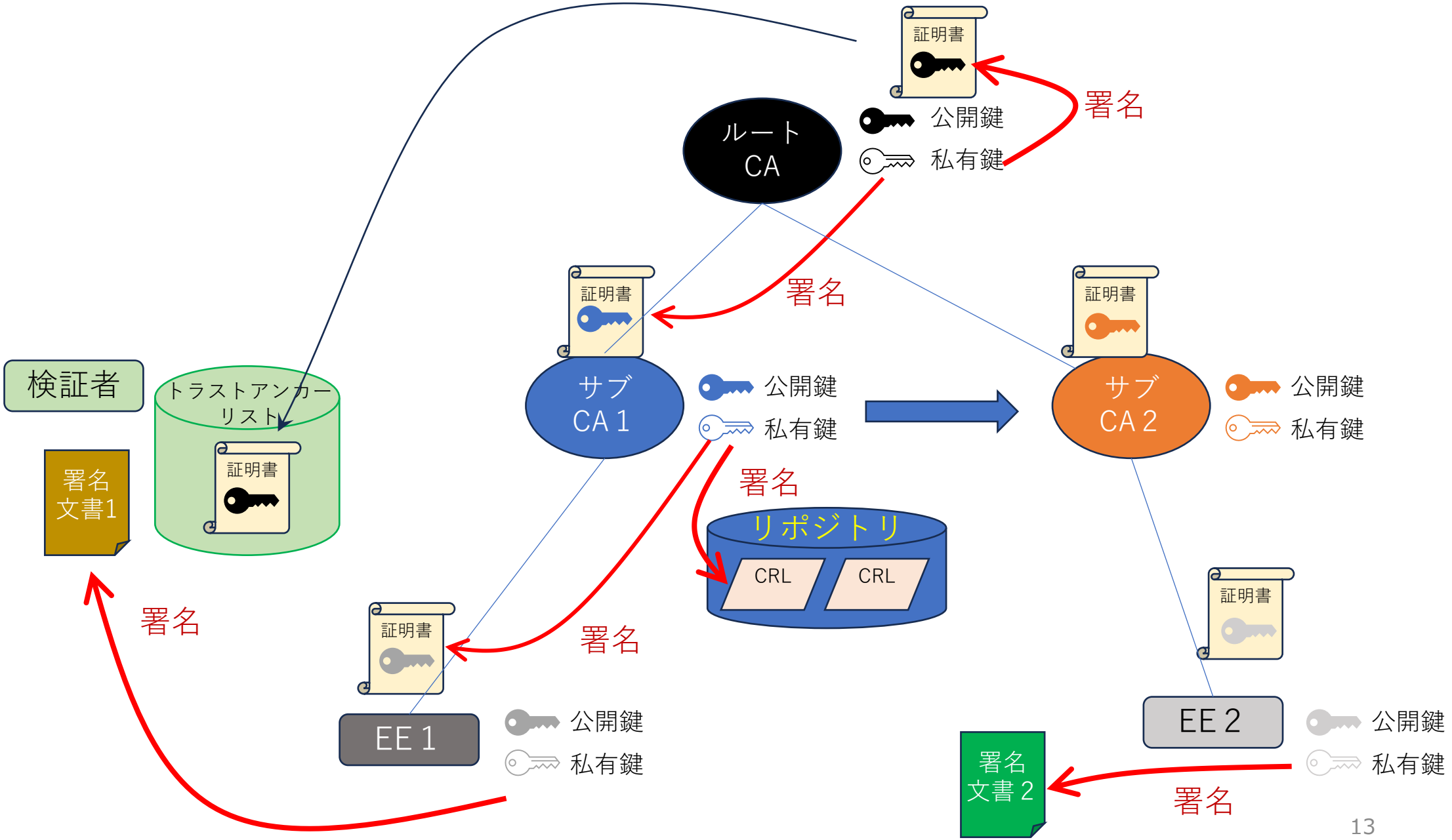

検証者はが署名文書′を検証する場合、署名者証明書からトラストアンカーまでのパスを生成できる。
証明書
証明書
証明書
証明書
検証者
トラストアンカーリスト
証明書
ルートCA
公開鍵
私有鍵
署名
証明書
証明書
ルートCA′
公開鍵
私有鍵
署名
旧CAの私有鍵を使って、新CA′の公開鍵証明書を作成（new with oldのリンク証明書）
証明書
サブCA 1
公開鍵
私有鍵
署名
リポジトリ
CRL
証明書
サブCA′
公開鍵
私有鍵
署名
リポジトリ
CRL
署名
署名
証明書
EE 1
公開鍵
私有鍵
署名
証明書
EE′
公開鍵
私有鍵
署名
署名文書′
署名


トラストアンカー更新後、検証者が署名文書を検証する場合、署名者証明書からトラストアンカーまでのパスを生成できる。
証明書
証明書
証明書
証明書
検証者
ルート CA
証明書
公開鍵
私有鍵
署名
ルート CA′
証明書
公開鍵
私有鍵
署名
新CAの私有鍵を使って、旧CA′の公開鍵証明書を作成（old with newのリンク証明書）
トラストアンカーリスト
証明書
署名文書
サブ CA 1
証明書
公開鍵
私有鍵
署名
リポジトリ
CRL
サブ CA′
証明書
公開鍵
私有鍵
署名
リポジトリ
CRL
署名
証明書
EE 1
公開鍵
私有鍵
署名
証明書
EE′
公開鍵
私有鍵

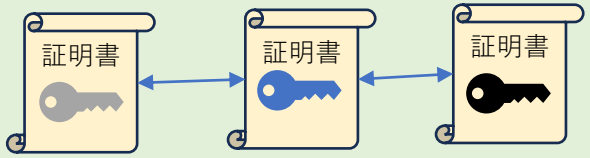
CAの移行タイミングとリンク証明書



サブCA移行に伴うリンク証明書の不必要性


証明書
署名
ルート
CA
公開鍵
私有鍵
証明書
署名
検証者
トラストアンカー
リスト
証明書
サブ
CA 1
公開鍵
私有鍵
証明書
サブ
CA 2
公開鍵
私有鍵
署名
署名
文書1
署名
リポジトリ
CRL
CRL
証明書
署名
証明書
EE 1
公開鍵
私有鍵
EE 2
公開鍵
私有鍵
署名
文書 2
署名

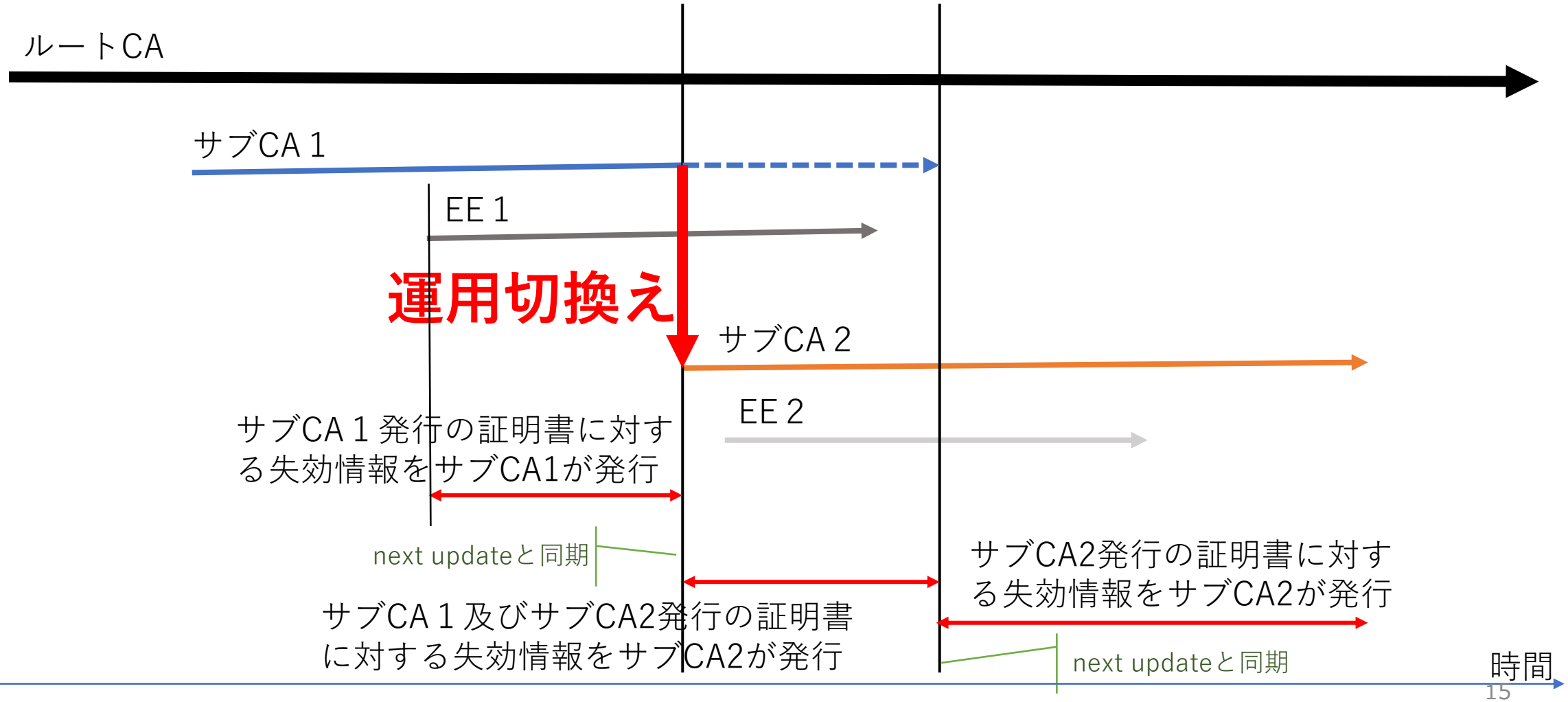
トラストアンカーは同じなので、文書1の検証では、

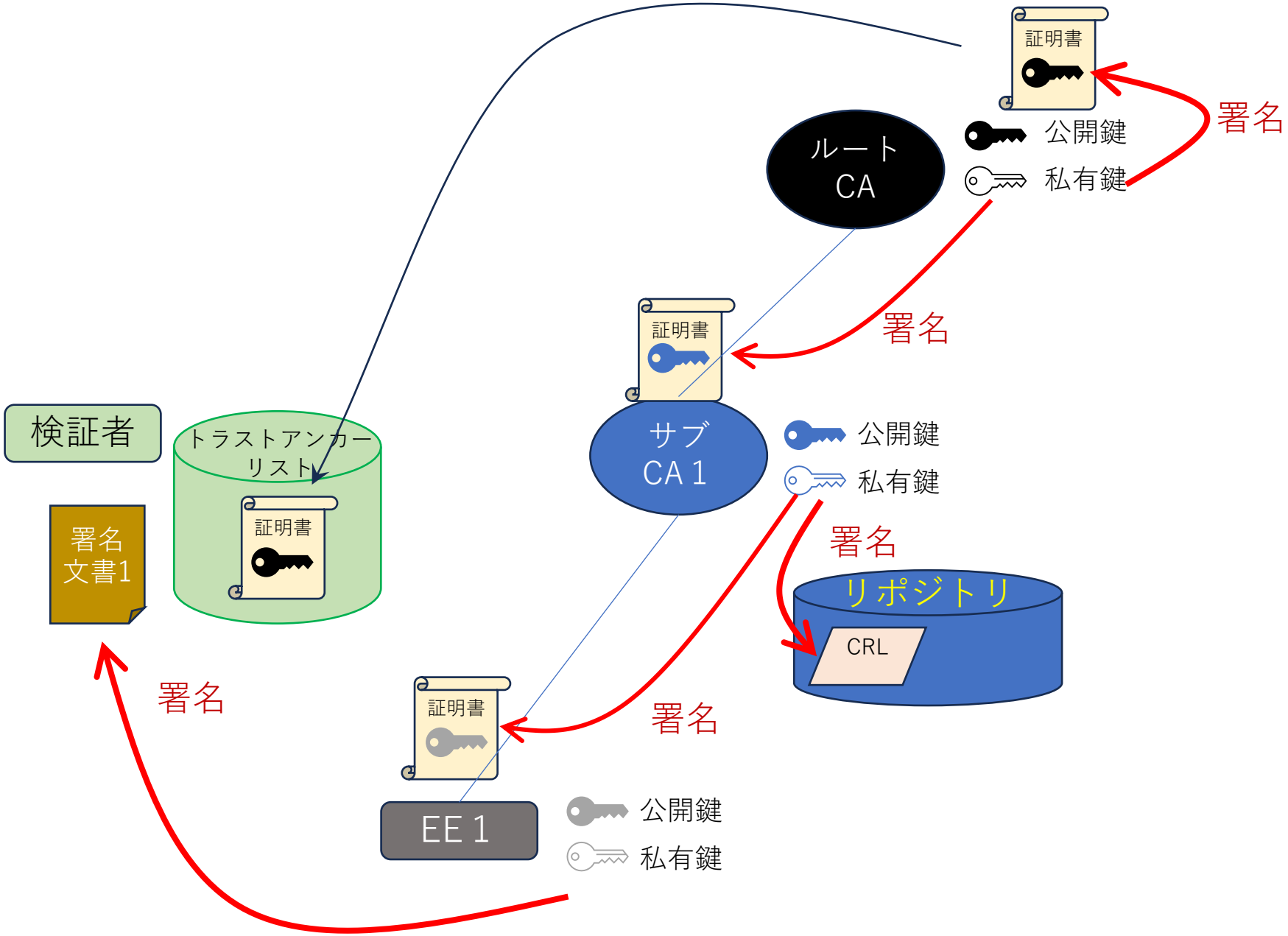


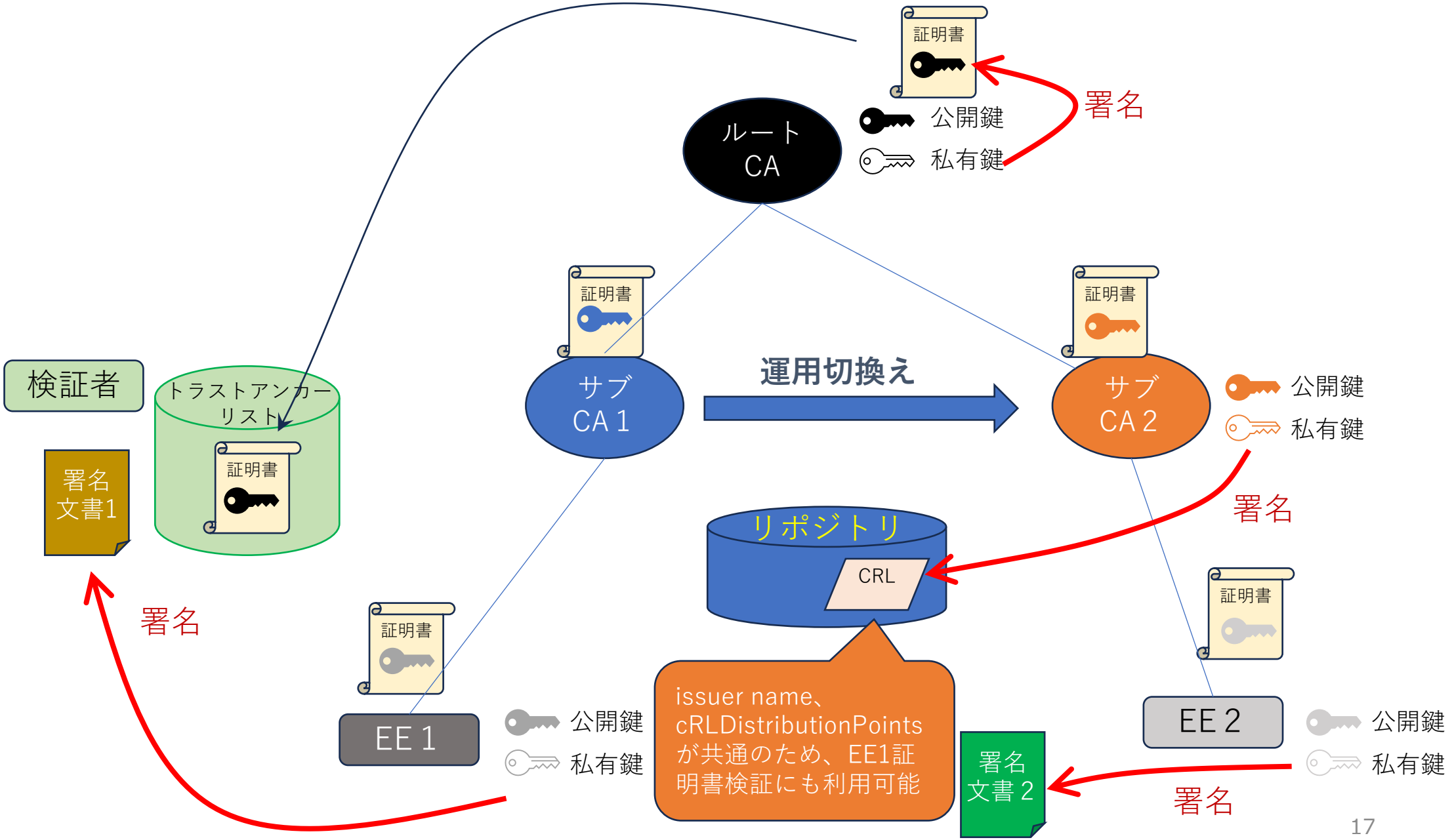
文書２では、

とパスが構築可能。従ってリンク証明書は不要。

失効情報の検証


ルートCA
サブCA 1
EE 1
運用切換え
サブCA 2
EE 2
サブCA 1 発行の証明書に対する失効情報をサブCA1が発行
next updateと同期
サブCA 1 及びサブCA2発行の証明書に対する失効情報をサブCA2が発行
サブCA2発行の証明書に対する失効情報をサブCA2が発行
next updateと同期
時間


証明書
署名
ルート
CA
公開鍵
私有鍵
証明書
署名
検証者
トラストアンカー
リスト
証明書
サブ
CA 1
公開鍵
私有鍵
署名
署名
文書1
署名
リポジトリ
CRL
証明書
署名
EE 1
公開鍵
私有鍵


証明書
署名
ルート
CA
公開鍵
私有鍵
検証者
トラストアンカー
リスト
証明書
署名
文書1
署名
サブ
CA 1
運用切換え
証明書
サブ
CA 2
公開鍵
私有鍵
署名
リポジトリ
CRL
証明書
証明書
EE 1
公開鍵
私有鍵
issuer name、
cRLDistributionPoints
が共通のため、EE1証
明書検証にも利用可能
署名
文書 2
EE 2
公開鍵
私有鍵
署名

問題となりそうな点

ただし、RFC5280には、、、

4.2.1.13. CRL Distribution Points

The cRLDistributionPoints extension is a SEQUENCE of DistributionPoint. A DistributionPoint consists of three fields, each of which is optional: distributionPoint, reasons, and cRLIssuer. While each of these fields is optional, a DistributionPoint MUST NOT consist of only the reasons field; either distributionPoint or cRLIssuer MUST be present. If the certificate issuer is not the CRL issuer, then the cRLIssuer field MUST be present and contain the Name of the CRL issuer. If the certificate issuer is also the CRL issuer, then conforming CAs MUST omit the cRLIssuer field and MUST include the distributionPoint field.

cRLDistributionPoints拡張は、DistributionPointのシーケンスです。 DistributionPointは3つのフィールドで構成され、各フィールドはオプションです: distributionPoint、reasons、およびcRLIssuer。これらの各フィールドはオプションですが、DistributionPointは理由フィールドのみで構成してはなりません(MUST NOT)。 distributionPointまたはcRLIssuerのいずれかが存在する必要があります。証明書発行者がCRL発行者でない場合、cRLIssuerフィールドが存在し、CRL発行者の名前が含まれている必要があります。証明書の発行者がCRLの発行者でもある場合、準拠するCAはcRLIssuerフィールドを省略し、distributionPointフィールドを含める必要があります。

- 旧サブCAが発行した証明書に対するCRLが新サブCAから発行される場合、証明書発行者がCRL発行者と同等であるとみなすか否かが問題となる。対応としては次のA、Bが考えられる（OCSPの利用など、それ以外にもある可能性あり）。

  A）旧サブCAのSubjectと新サブCAのSubjectが同一であるため、同等とみなすのであれば、distributionPointが同一であるため、実装上問題とならないと思われる。
  - ただし、両者の相違を証明書レベルあるいは公開鍵レベルで比較し、同等性を処理するようなロジックが含まれれば、同一でないとみなされ、検証処理に失敗する可能性あり。EE証明書とCRL証明書のissureの比較で同一性を判断することが適当である。
  - このとき、サブCA間のリンク証明書を利用したとしても「同一でない」ため、解決とはならない。（一部の実装ではリンク証明書利用により処理に成功したと聞くが、これはリンク証明書を利用して検証を行った際の認証パス上に新サブCA証明書が含まれることをもって同一性の判断をしたためにこの結果となったと考えられる）

HPKIのEE証明書にはdistributionPointのみが存在しcRLIssuerが存在しないことが前提。

B) 旧サブCAの有効期限内（正確には旧サブCAが発行したEE証明書の有効期限内）は旧サブCAから発行された証明書向けのCRLを発行し続ける。
- これにより同一性解釈の問題は回避でき、リンク証明書も不要となる。
- ただし、新旧distributionPointに記載するHTTPやLDAPのURIを異なる値とする必要がある。

- いずれにしても、どのような対応をすべきかを、検証ポリシーや検証処理の実装ガイド等として明文化する必要がある。（B案なら不要か）

以上です。