電子署名の検証モデル
–チェーンモデルは長期署名を不要とするか？–
【マニアック系？】

2016/10/26

宮崎

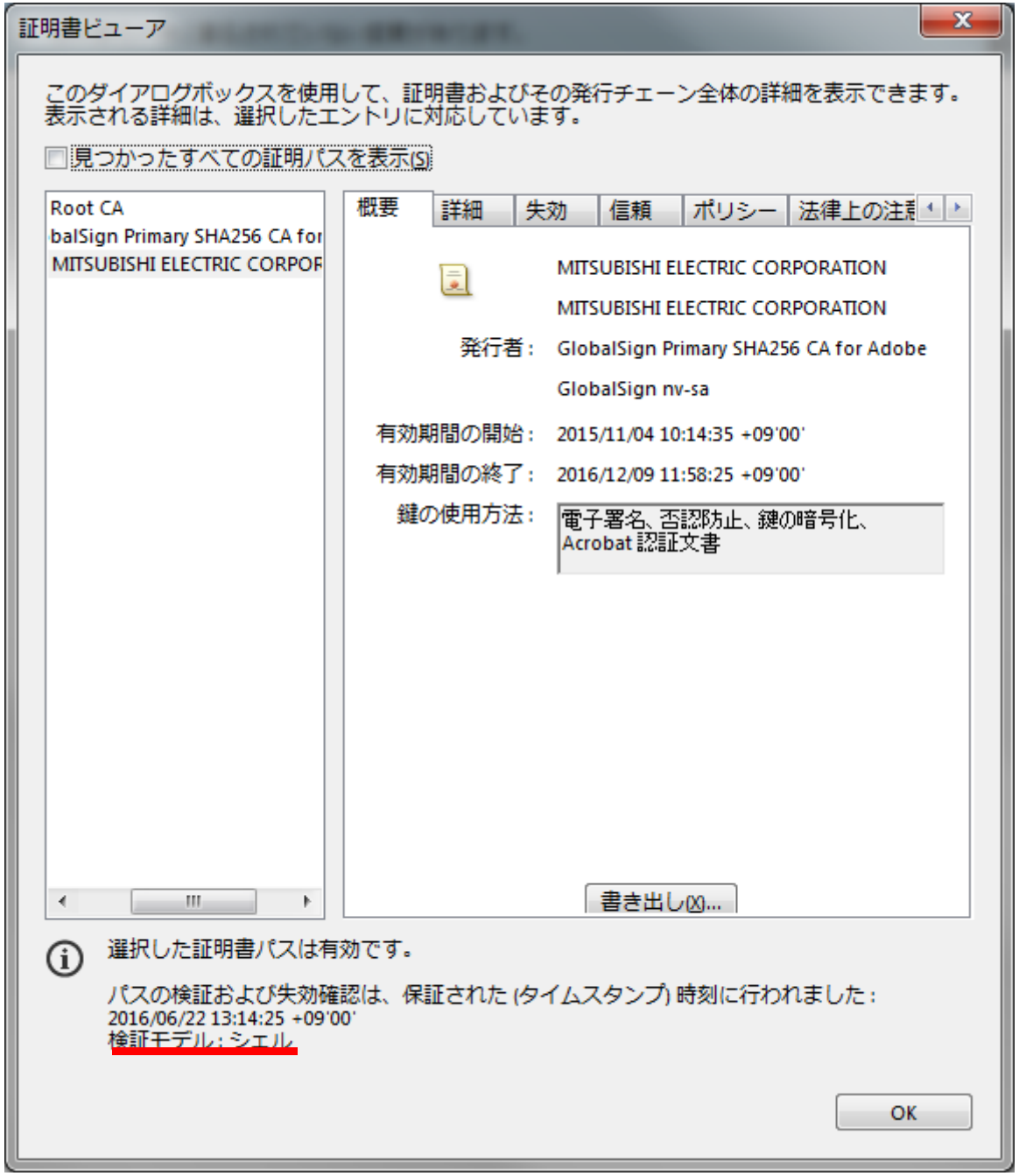
電子署名の検証モデル

- シェルモデル

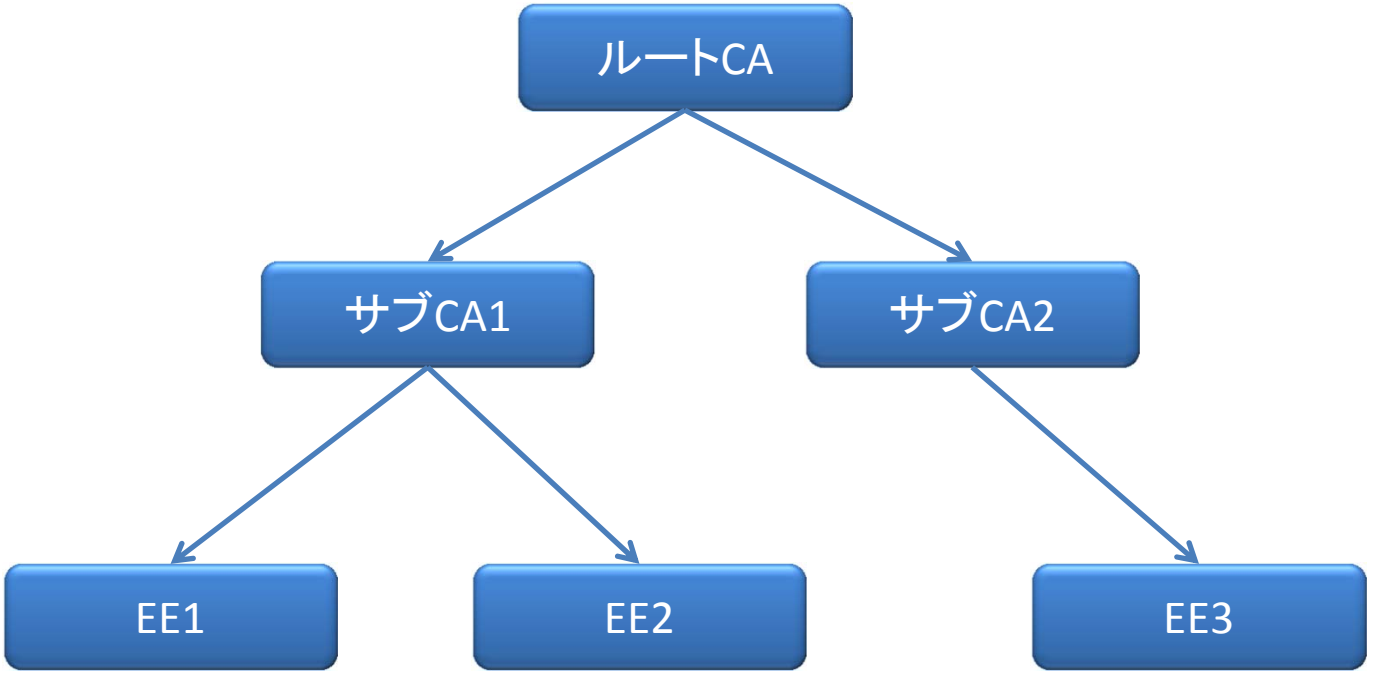
⇒普通

- チェーンモデル

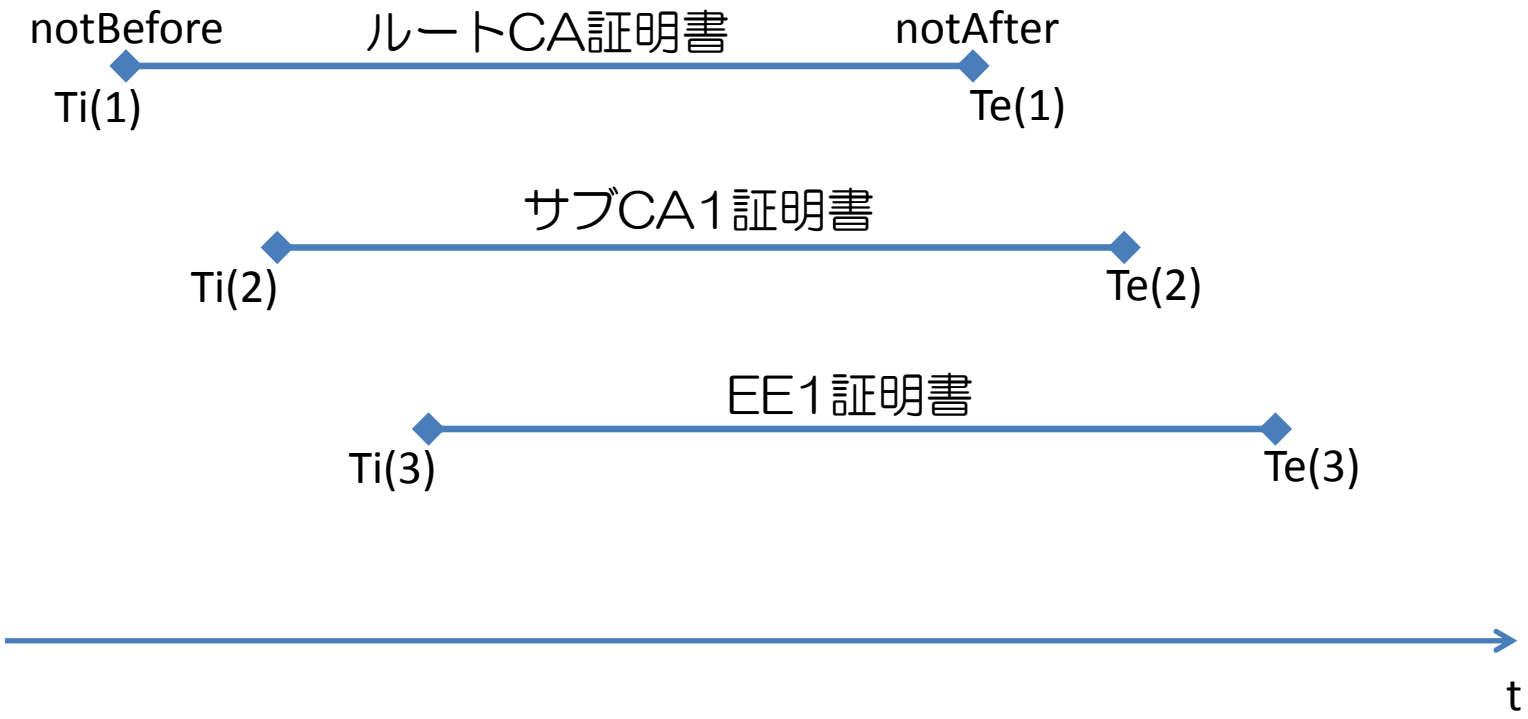
⇒独のQC（適格証明書）による署名の検証
　他に，イタリア、ポーランド、エジプト
　でも利用されているらしい。


証明書ビューア
このダイアログボックスを使用して、証明書およびその発行チェーン全体の詳細を表示できます。
表示される詳細は、選択したエントリに対応しています。
見つかったすべての証明パスを表示(S)
Root CA
balSign Primary SHA256 CA for
MITSUBISHI ELECTRIC CORPOR
概要
詳細
失効
信頼
ポリシー
法律上の注意
MITSUBISHI ELECTRIC CORPORATION
MITSUBISHI ELECTRIC CORPORATION
発行者：
GlobalSign Primary SHA256 CA for Adobe
GlobalSign nv-sa
有効期間の開始：
2015/11/04 10:14:35 +09'00'
有効期間の終了：
2016/12/09 11:58:25 +09'00'
鍵の使用方法：
電子署名、否認防止、鍵の暗号化、
Acrobat 認証文書
書き出し(X)...
選択した証明書パスは有効です。
パスの検証および失効確認は、保証された (タイムスタンプ) 時刻に行われました：
2016/06/22 13:14:25 +09'00'
検証モデル：シェル
OK

PKI信頼モデル例



各証明書の有効期間


notBefore
ルートCA証明書
notAfter
Ti(1)
Te(1)
サブCA1証明書
Ti(2)
Te(2)
EE1証明書
Ti(3)
Te(3)
t

シェルモデルの定義

【シェルモデル】

1. 及び2. を満たす場合、時刻T_v における署名検証結果は「有効」となる：

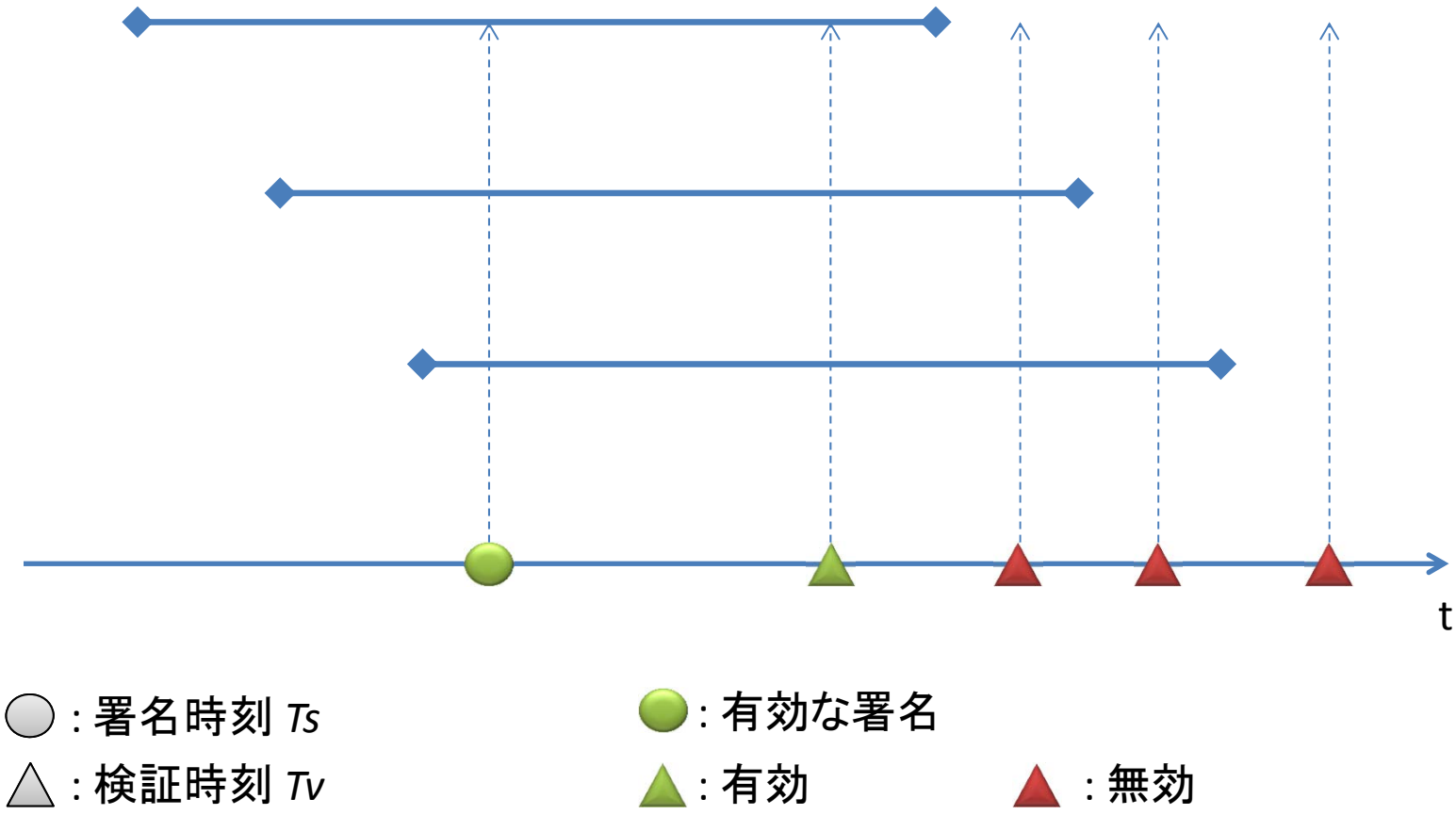
1. EE証明書 $Cer(N)$が署名時刻T_s において有効：

   $[T_i(N) \leq T_s \leq T_e(N)] \wedge [Cer(N)$が$T_s$に失効していない$]$

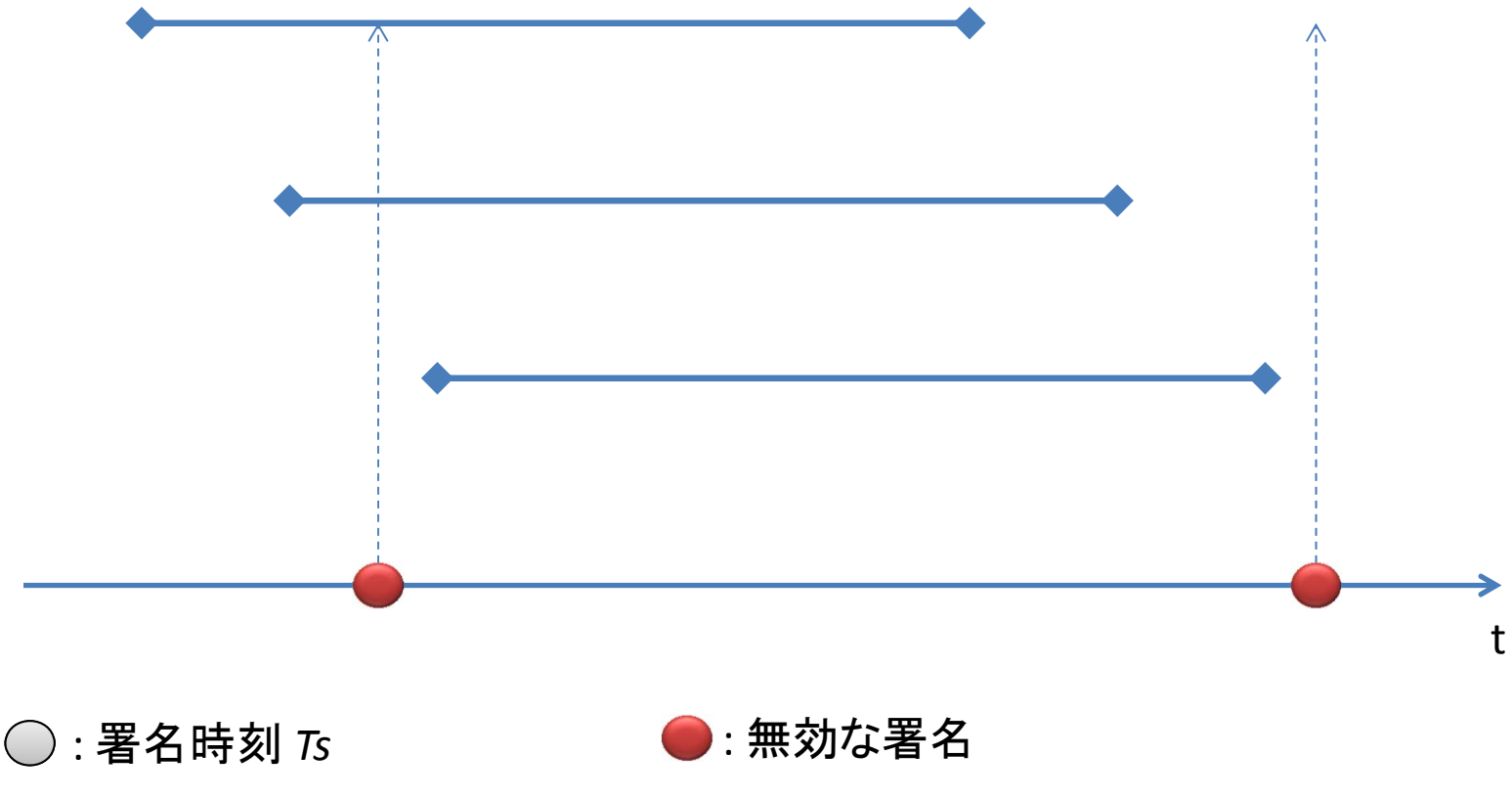
2. 証明書チェーンのすべての証明書$Cer(k)$がT_v において有効：

   $[T_i(k) \leq T_v \leq T_e(k)$ for all $1 \leq k \leq N]$
   $\wedge$
   $[T_v$に$Cer(k)$ for all $1 \leq k \leq N$が失効していない$]$

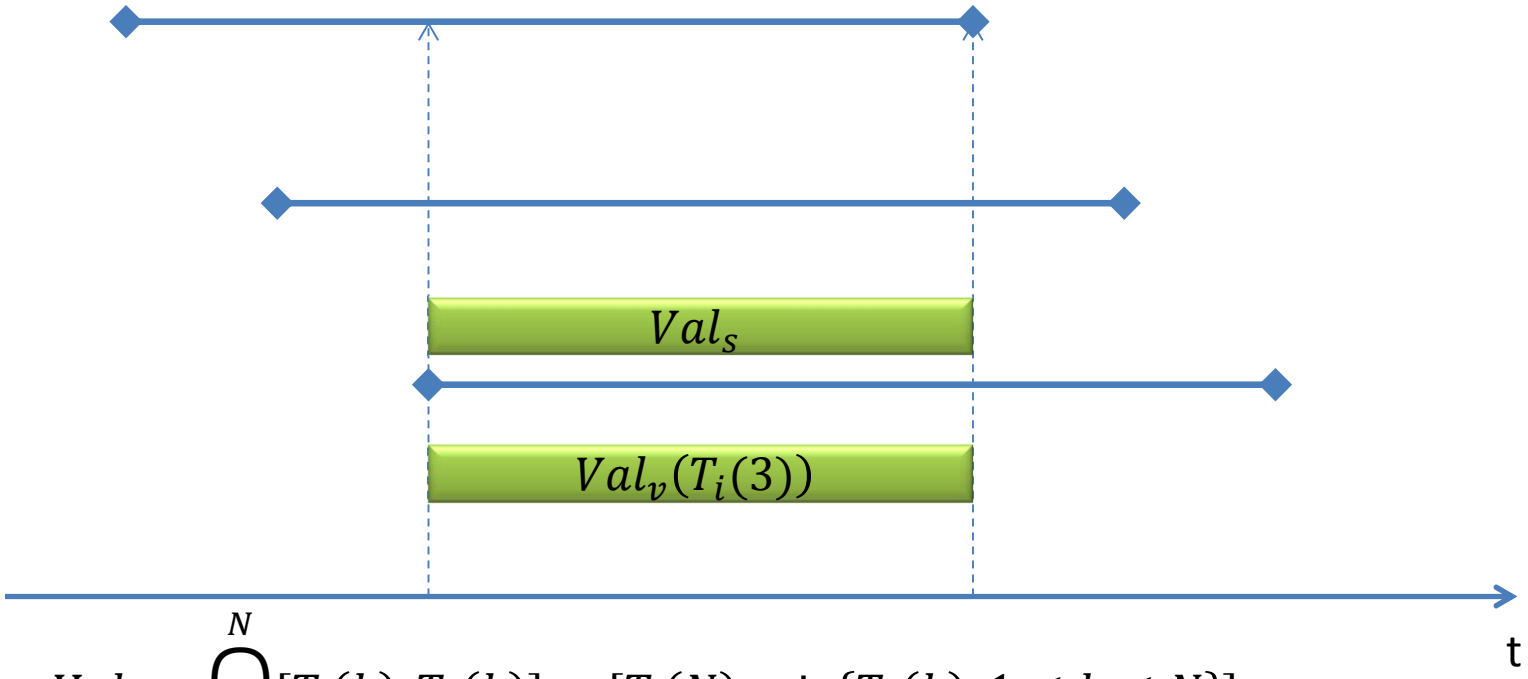
シェルモデルにおける検証結果



シェルモデルにおける署名の生成時の有効性



シェルモデルにおける有効期間



$$Val_s = \bigcap_{k=1}^{N} [T_i(k), T_e(k)] = [T_i(N), \min\{T_e(k): 1 \le k \le N\}]$$

$$Val_v(T_s) = [T_s, \min\{T_e(k): 1 \le k \le N\}] \quad \text{for all } T_s \in Val_s$$

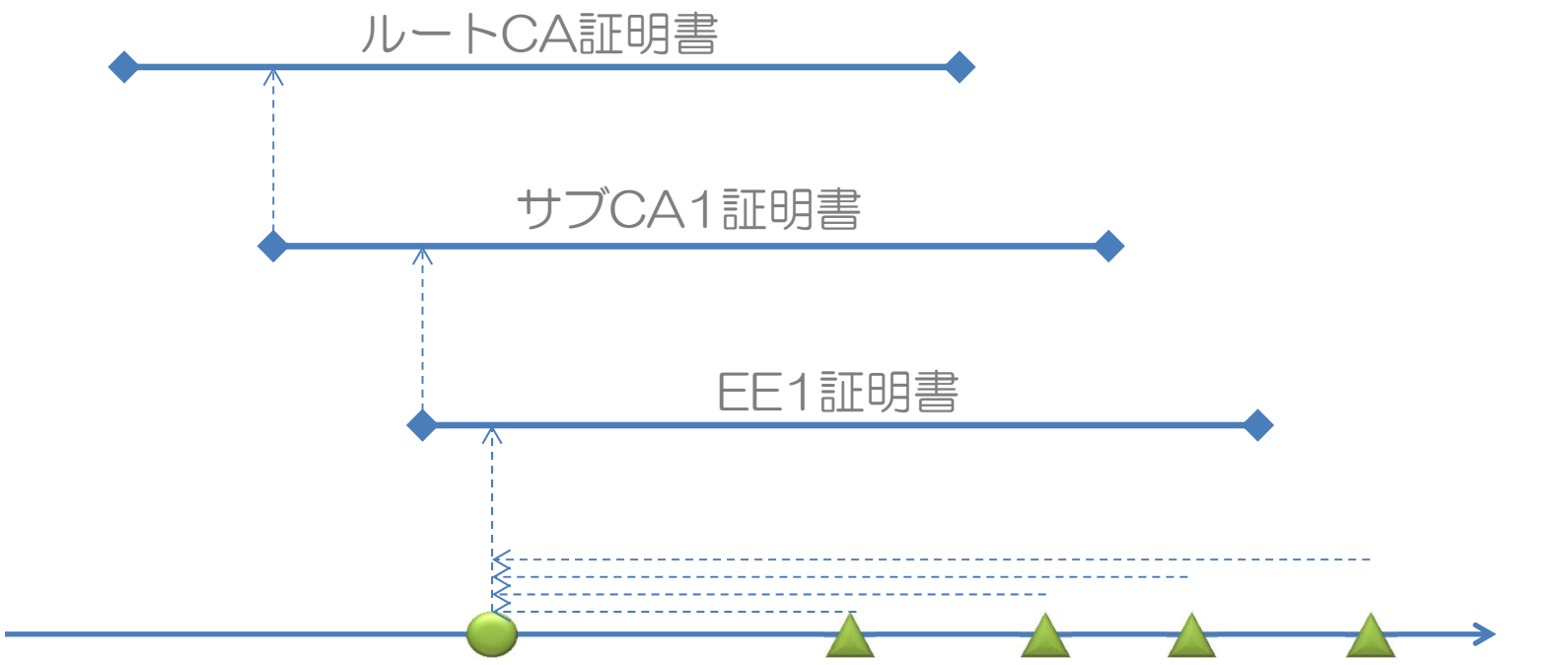
Val_s : 有効な署名が生成できる期間
$Val_v(T_s)$: 生成時に有効な署名が検証時に有効である期間
仮定 : 証明書は失効しない

チェーンモデルの定義

【チェーンモデル】
1及び2を満たす場合、時刻T_v における署名検証結果は「有効」となる：

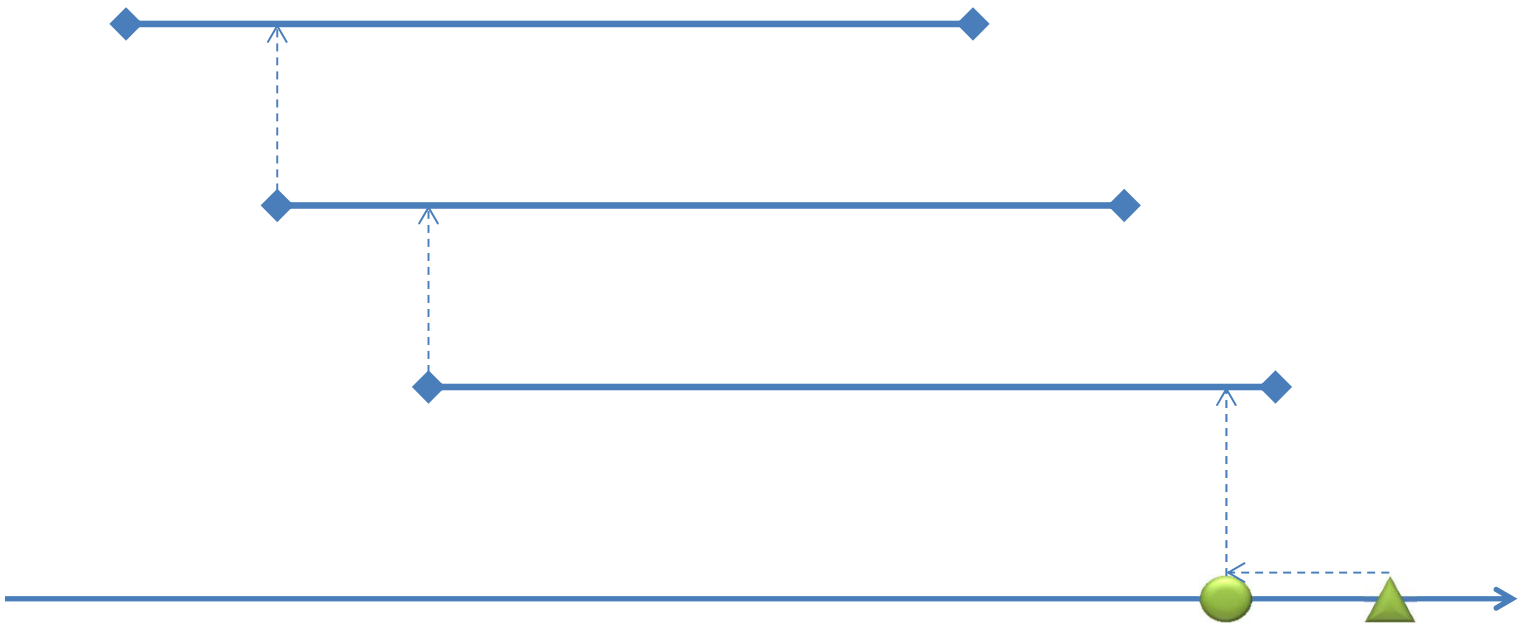
1. EE証明書 $Cer(N)$が署名時刻T_s において有効：
   $[T_i(N) \leq T_s \leq T_e(N)] \wedge [T_s$に$Cer(N)$が失効していない$]$
2. 証明書チェーンのすべての証明書$Cer(k)$が自身の発行時刻において有効：
   $[T_i(k-1) \leq T_i(k) \leq T_e(k-1)]$
   $\wedge$
   $[T_i(k)$に$Cer(k-1)$for all $2 \leq k \leq N$が失効していない$]$

チェーンモデルにおける検証



○ : 署名時刻 *Ts*
△ : 検証時刻 *Tv*
● : 有効な署名
▲ : 有効

チェーンモデルにおける検証



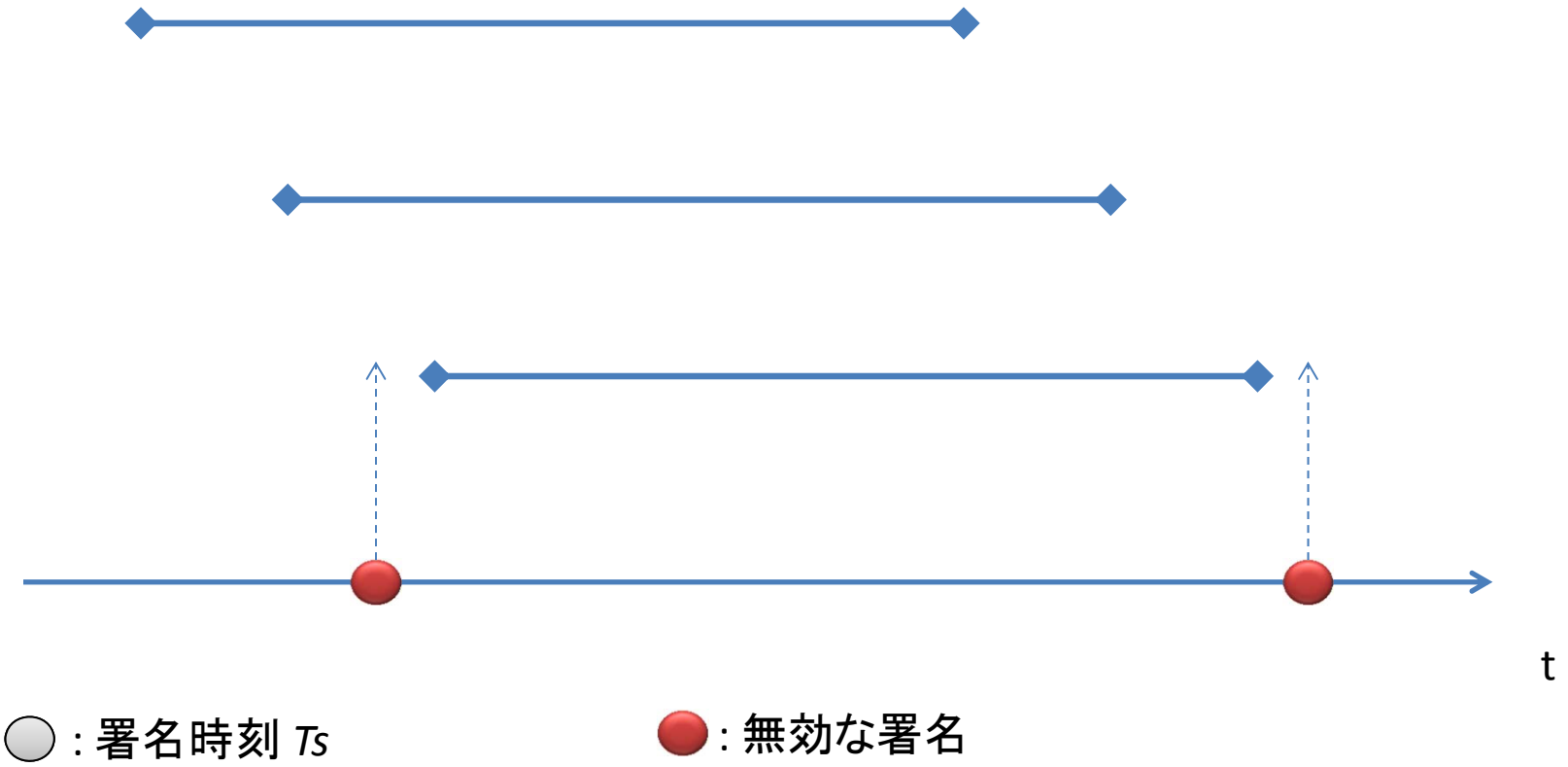
: 署名時刻 *Ts*

: 検証時刻 *Tv*

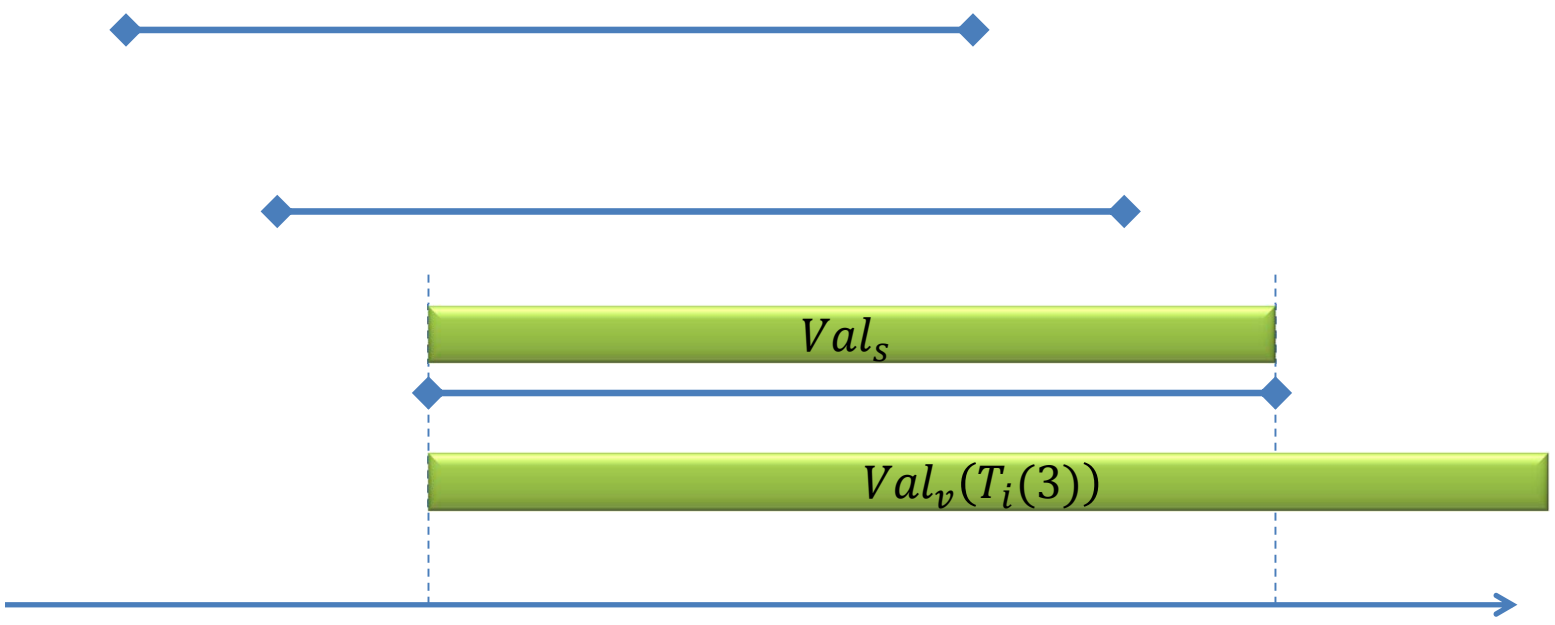
: 有効な署名

: 有効

チェーンモデルにおける検証



チェーンモデルにおける有効期間



$Val_s = [T_i(N), T_e(N)]$

$Val_v(T_s) = [T_s, \infty]$ for all $T_s \in Val_s$

チェーンモデルでの有効性の要件

- 署名生成時刻の証明⇒署名タイムスタンプが必要
- 署名鍵の漏洩⇒署名タイムスタンプあればOK
- 署名の公開鍵暗号の危殆化⇒署名タイムスタンプあればOK
- 署名のハッシュ関数の危殆化⇒アーカイブタイムスタンプが必要
- タイムスタンプのハッシュ関数の危殆化⇒アーカイブタイムスタンプが必要

⇒長期署名は必要だが，アーカイブタイムスタンプはハッシュ関数危殆化前に打てばよい。

⇒タイムスタンプの付与頻度は大幅に減らせる！

チェーンモデルでの有効性の要件

- 署名生成時刻の証明⇒署名タイムスタンプが必要
- 署名鍵の漏洩⇒署名タイムスタンプ有効期間内
- タイムスタンプのハッシュ関数の危殆化⇒アーカイブタイムスタンプが必要

ATSの頻度は某SSタイムスタンプ並みに。
しかも、検証を自分でできる！
？でもチェーンモデルじゃなくてもいい？

⇒長期署名は必要だが，アーカイブタイムスタンプはハッシュ関数危殆化前に打てばよい。

⇒タイムスタンプの付与頻度は大幅に減らせる！