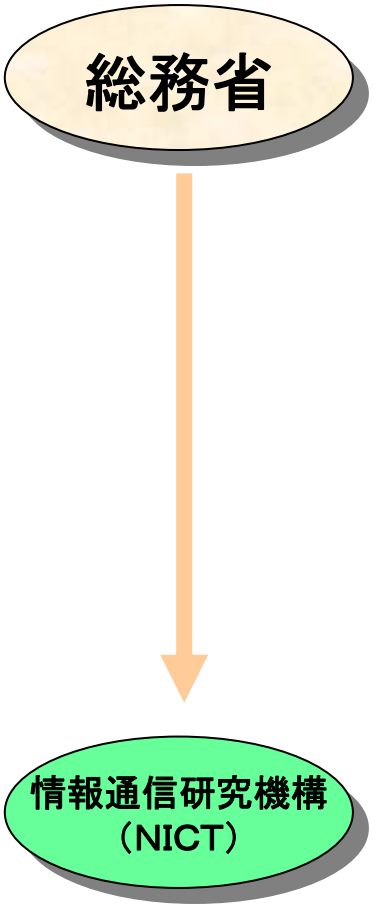
タイムスタンププラットフォーム技術の研究開発と実証実験

独立行政法人　情報通信研究機構

鳥山 裕史

NiCT 独立行政法人 情報通信研究機構
National Institute of Information and Communications Technology

「タイムスタンププラットフォーム技術の研究開発」



委託研究 （平成15～17年度）

日本標準時を利用して正確かつセキュリティの高いタイムスタンプを付与することができる「タイムスタンププラットフォーム技術」を確立し、安心して利用できる高度情報通信ネットワーク社会の実現に資する

・高精度時刻情報配信技術の開発
・高信頼時刻認証技術の開発
・高速時刻認証技術の開発
・プラットフォームシステムの構築
・プラットフォームシステムのセキュリティ分析実施
・実証実験の実施
など

研究開発開始の背景

タイムスタンプ技術が有効なことは理解されているが、広く使われている状態ではない

急速な電子化の流れ

安全確保は急務

利用者の抱える問題:

- ■必要であるが、使える状態にない
  - 個別用途への適用事例が少なく、独自開発を要する部分が多い
- ■使いたいが、コストが高すぎる

事業者の抱える問題:

- ■タイムスタンプ事業者の責任が明白でないので参入しづらい
  - 訴訟リスク、サービスの長期継続コストの分析が不十分
- ■ビジネスとして成立するか見通しが立たない

技術的、制度的な問題:

- ■長期にわたる安全性の確保
  - 安全であることは必要だが、早期に方式を絞らないとビジネスが成立しない
- ■法的な証拠性の確保
  - 条約、国内法令の整備、標準時刻とのトレーサビリティ確保

安全を確保しつつ、何らかの促進策が必要！

研究開発実施の基本スタンス

実証・具体化に重点を置く

■タイムスタンプ普及促進は急務である
■技術的な範囲が広く、すべてについて基礎研究を進める体制、時間を確保できない
　既存技術の検証、選択、改良を主とし、基礎研究項目は必要なものに限定

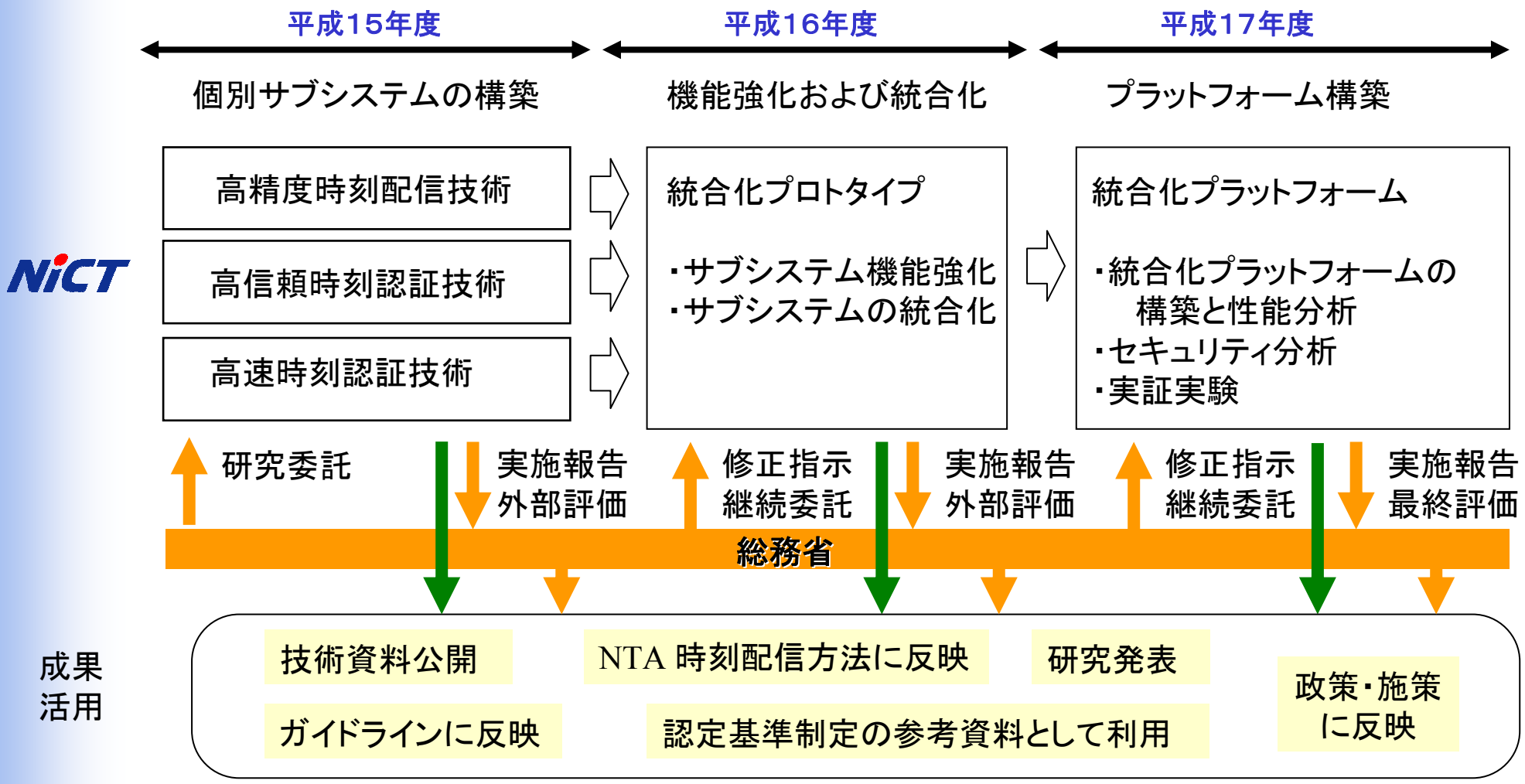
他研究プロジェクトとの連携

■日本標準時関係のノウハウ、設備の活用
　所内にGPSコモンビュー装置の開発、運用などの実績がある
■ネットワーク系プロジェクトとの連携
　システム統合、実証の際に高速バックボーンでの実験を実施

外部組織との連携

■装置製造担当会社のノウハウ活用
　ノウハウのある会社に発注し、製造のみではなく、実装上の選択肢などの提案を受ける
■タイムビジネス推進協議会での実証実験
　タイムビジネス協議会に参加する多数の事業者、大学等と連携し、実利用に
　近い形での実証実験を行う

各年度の実施内容概要


平成15年度
平成16年度
平成17年度
個別サブシステムの構築
機能強化および統合化
プラットフォーム構築
NiCT
高精度時刻配信技術
高信頼時刻認証技術
高速時刻認証技術
統合化プロトタイプ
・サブシステム機能強化
・サブシステムの統合化
統合化プラットフォーム
・統合化プラットフォームの構築と性能分析
・セキュリティ分析
・実証実験
研究委託
実施報告
外部評価
修正指示
継続委託
実施報告
外部評価
修正指示
継続委託
実施報告
最終評価
総務省
成果
活用
技術資料公開
NTA 時刻配信方法に反映
研究発表
ガイドラインに反映
認定基準制定の参考資料として利用
政策・施策
に反映

研究開発項目（平成15年度）

高精度時刻配信技術の研究開発

■一般家庭、一般企業で使われるインターネット接続に適した時刻配信技術の開発・検証
→ ローコストな通信手段でも、安心して使える技術の確立

■高速バックボーンでの高精度時刻配信技術の開発・検証
→ NTA－TA，TA－TA，TA－TSA間高精度時刻配信のローコスト化

高信頼時刻認証技術の研究開発

■トレーサビリティ検証可能な時刻配信基盤技術の調査・開発・検証
→ NTA－TA－TSA間で日本標準時を安全に配信する技術の確立

■タイムスタンプ検証技術の調査・開発・検証
→ 安心して利用できる検証技術の確立

高速時刻認証技術の研究開発

■安全な鍵長でも十分な処理能力を持つタイムスタンプ装置の開発
→ サービスコストの低減
サービス普及時に想定される大量処理の実現

研究開発項目（平成16年度）

高精度時刻配信技術の研究開発

■配信時刻の十分な精度と信頼性を保証するための技術を開発

高信頼時刻認証技術の研究開発

■時刻情報トレース機能の強化

高速時刻認証技術の研究開発

■タイムスタンプ処理性能を向上させる技術の設計･検証

高速時刻認証技術の研究開発

■平成15年度に開発した各システムを統合し、連携動作させるプロトタイプシステムを構築

研究開発項目（平成17年度）

統合化プラットフォームシステムの構築と性能分析

■認証連鎖方式による時刻配信の配信経路と誤差が確認できること
■時刻リンク方式による時刻配信の配信経路と誤差が確認できること
■時刻同期精度として、NTA−TA間で1ミリ秒以内、NTA−TSA間で数ミリ秒以内を達成する

統合化プラットフォームシステムを用いた実証実験

■実アプリケーションを実験運用し、実用性に関する評価と技術・運用等の課題を明らかにする
■有効期間が切れる前あるいは脆弱化する前にタイムスタンプの効力を延長保証する技術、
運用面の方策について検証を行い、課題を明らかにする

統合化プラットフォームシステムに係るセキュリティ分析

■総合的なセキュリティ要件や必要となるセキュリティ対策等を明らかにする
■2つのタイムスタンプ方式に関し、セキュリティ面の妥当性を分析する

統合化プラットフォームシステム（NICT内設置分）

検証用クライアント
（Client）

認証局（CA）

ハードウエア
セキュリティモジュール
HSM

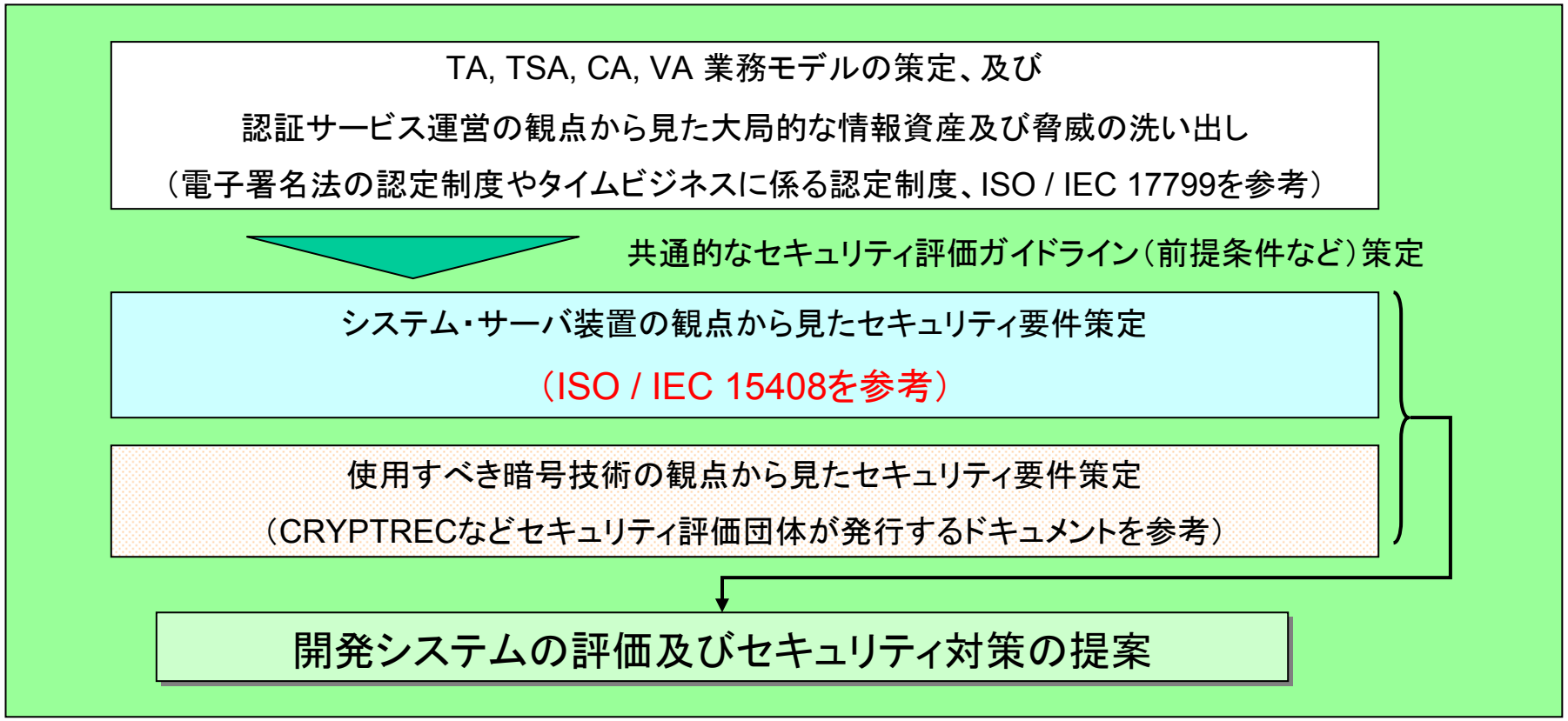
検証局 （VA）

国家時刻標準局1
NTA1

国家時刻標準局2
NTA2

TA2
標準時配信局2

タイムスタンププラットフォームのセキュリティ評価

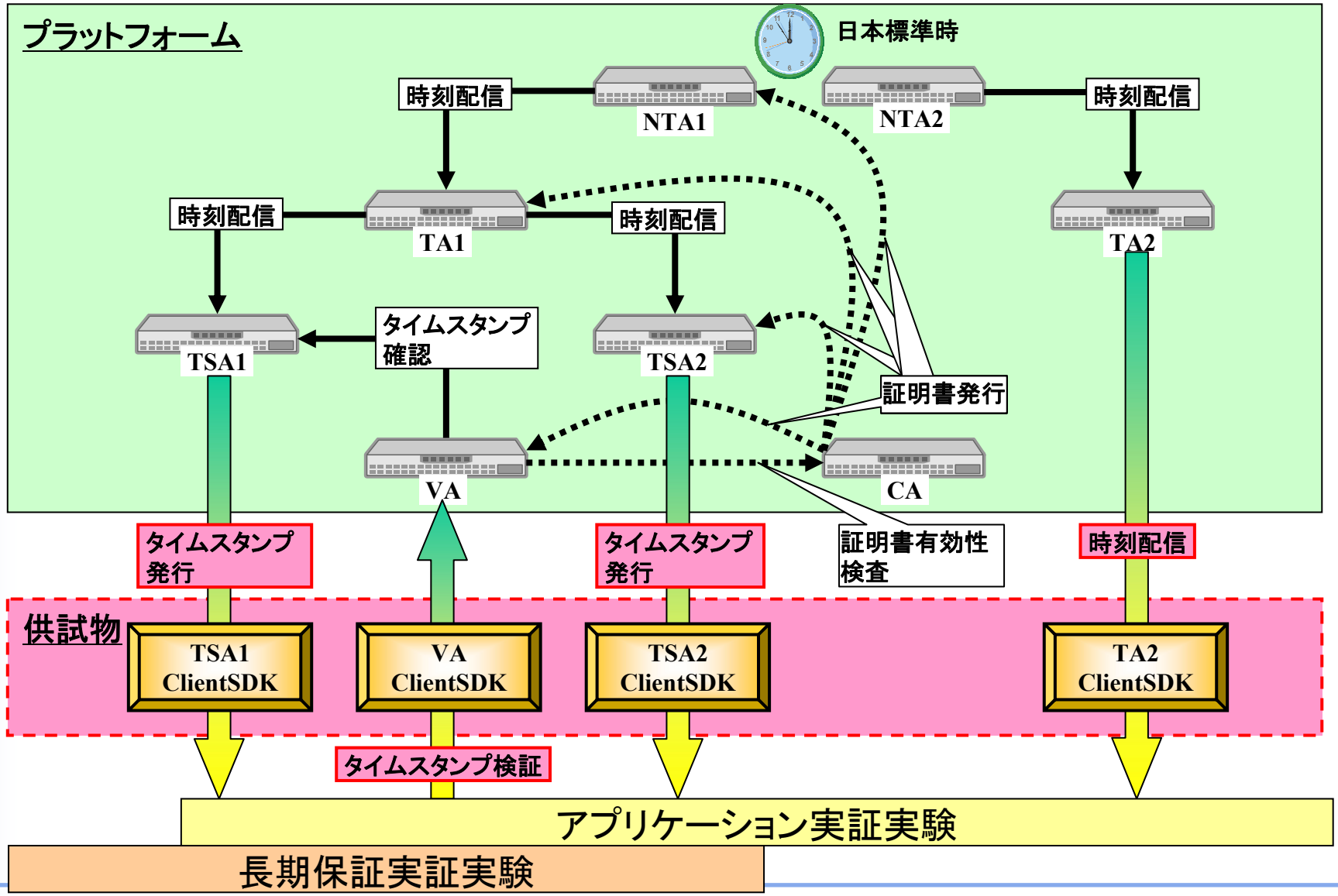


セキュリティ評価実施手順

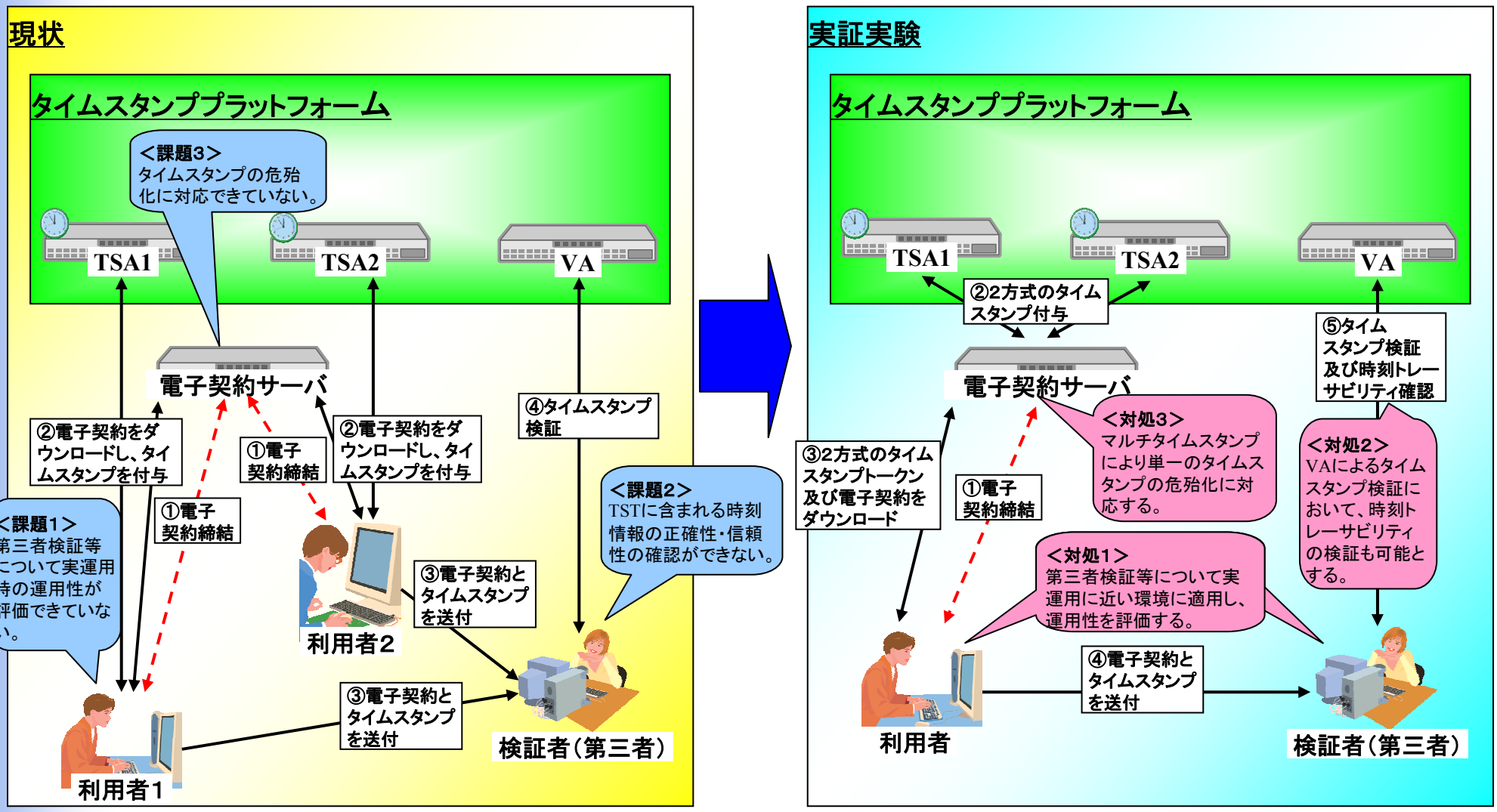
作業項目	説　明
業務モデル策定	TA、TSA、VA、CAの想定業務モデルを策定 ・サービスシステム構成（物理的な環境含む）の明確化 ・サービス利用者/提供者などの関与者の明確化 ・業務フローの明確化 ・可能であれば、大局的に見た情報資産及び脅威の抽出
セキュリティ評価ガイドライン策定	ISO/IEC 15408の考え方を踏まえたセキュリティ評価ガイドライン ・評価対象(TOE※)の検討及び評価対象定義のガイドライン ・脅威抽出及びリスク評価のガイドライン ・セキュリティ目標決定、セキュリティ要件・機能の策定に係るガイドライン
セキュリティ評価	上記の「セキュリティ評価ガイドライン」に従い、**セキュリティ評価を実施** セキュリティ評価の観点から**開発システムを評価**

セキュリティ評価報告書作成

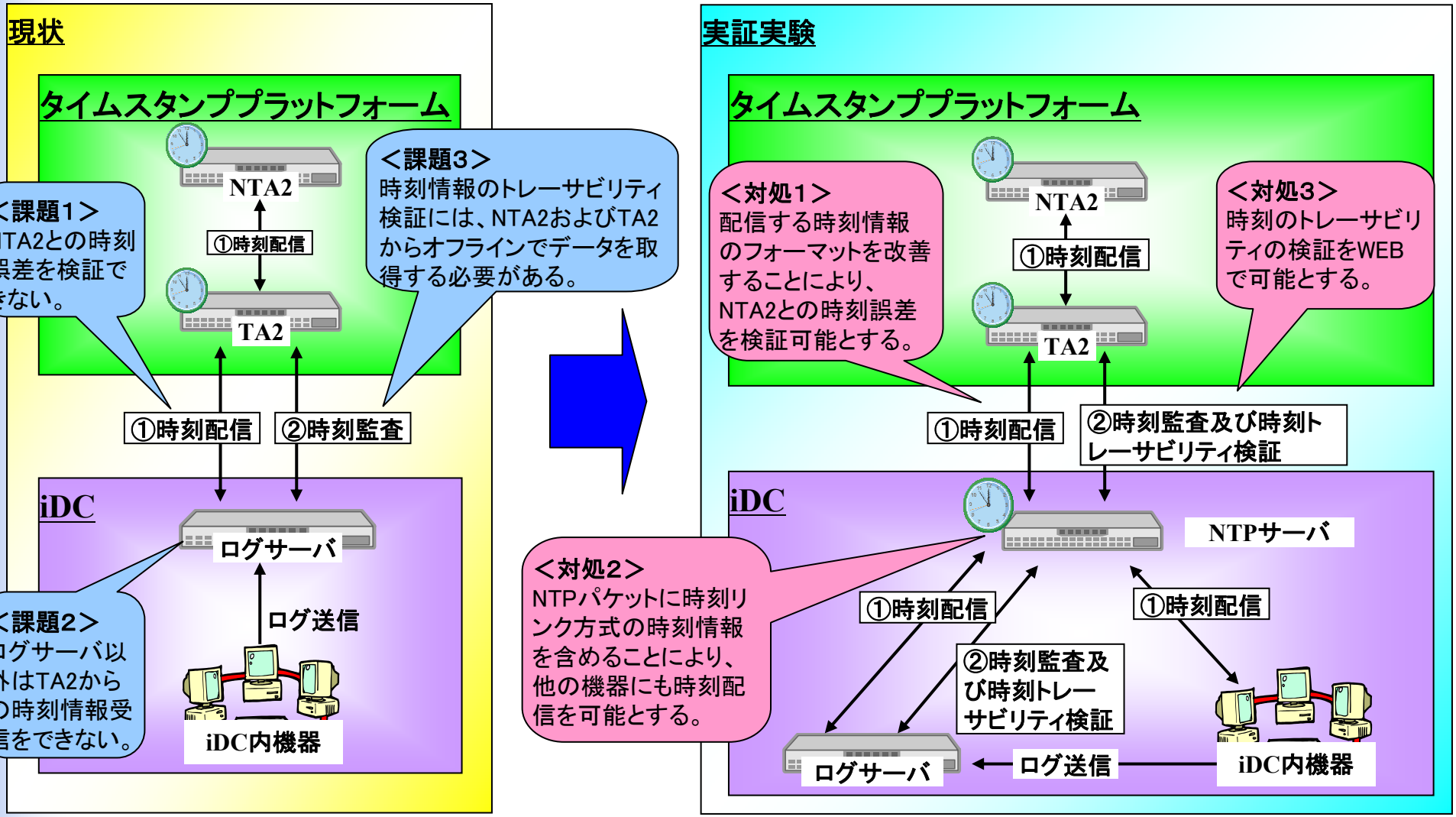
タイムスタンププラットフォーム実証実験



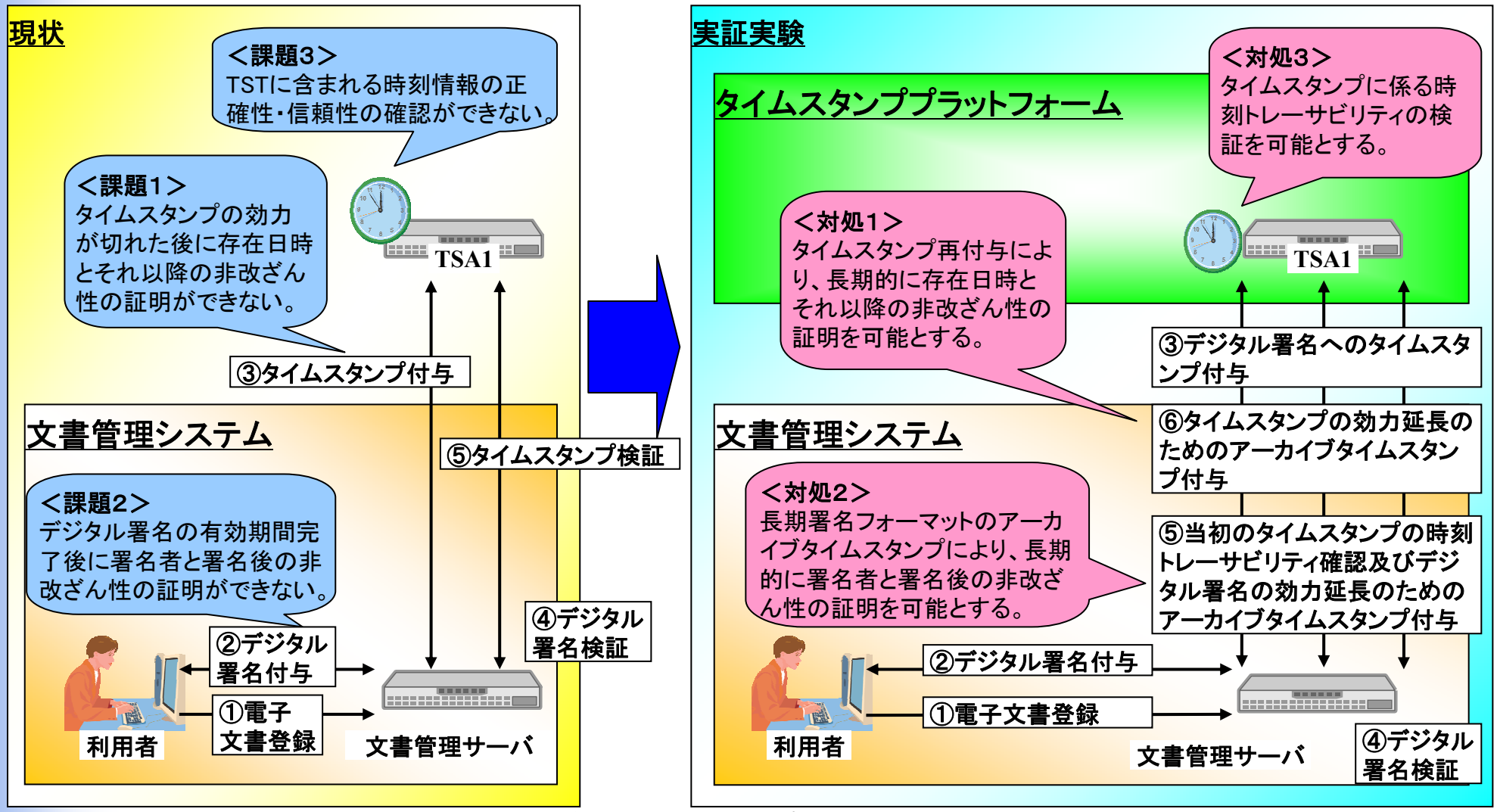
1　電子契約実証実験　システム構成



2　ログサーバ実証実験　システム構成

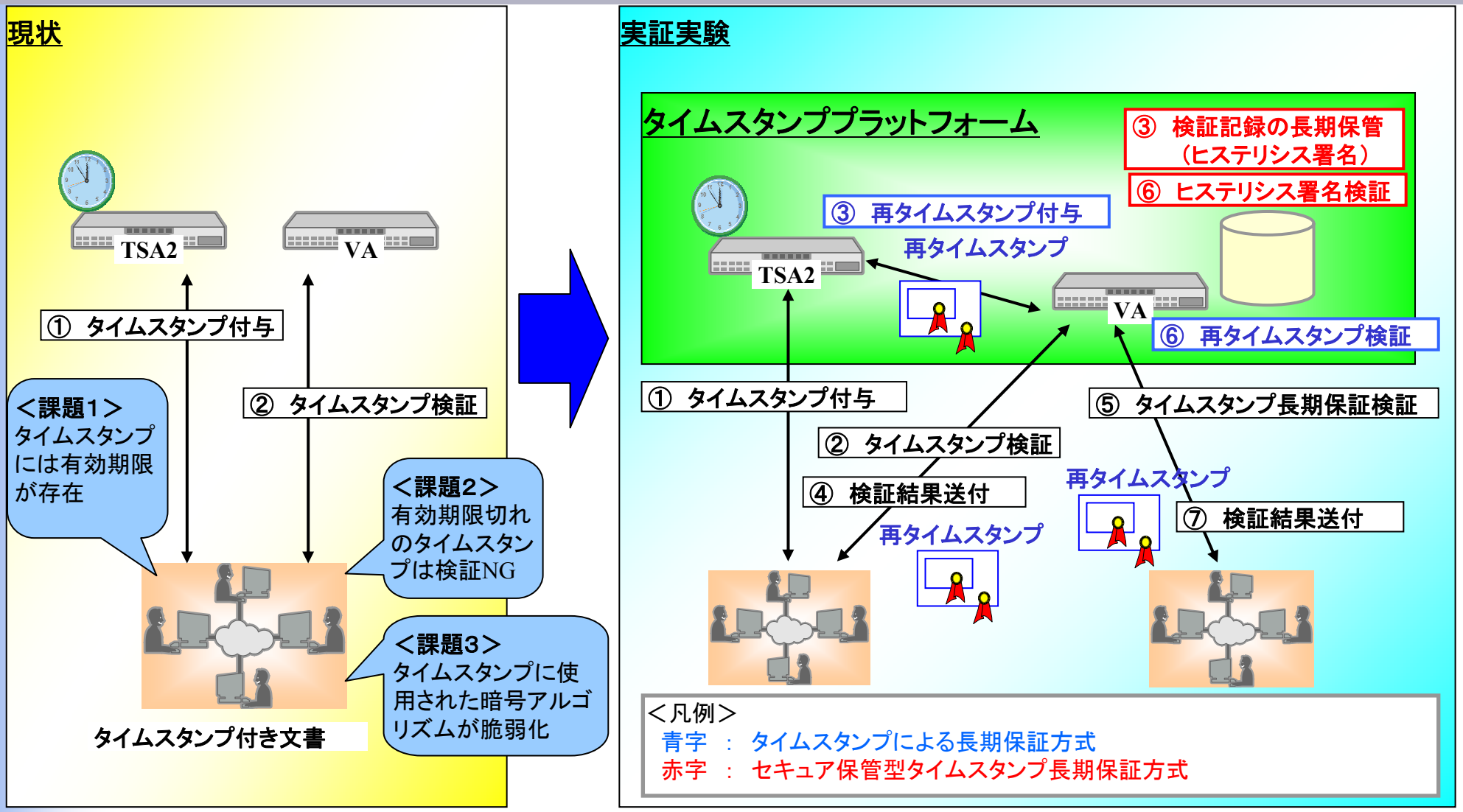


３　文書管理システム実証実験　システム構成



※　本実証実験は、リンク情報を使用するアーカイビング方式のタイムスタンプを対象をして実施。

4　VAによる長期保証　システム構成



※　本実証実験は、デジタル署名を使用する方式のタイムスタンプを対象として実施。

今後の展開について

NICT：18年度は、専用の予算なし

「時空標準技術（応用分野）の研究」
の一環として可能な部分を実施

これまでの成果の活用

■開発・実験結果を報告書として公開
■タイムビジネス協議会活動の中で、開発・実験結果を活用
■タイムスタンププラットフォームシステムを用いた新規実験の実施

検討段階

タイムスタンプの幅広い利用に向けた開発・実証

検討段階

■高速、ローコストな時刻認証サーバの開発
■ファイルサーバ、メール中継サーバへの時刻認証機能組込み

関連する要素技術の研究開発

検討段階

■時刻情報と共に、位置情報も認証する技術
■クライアント側機器で、安全に時刻認証を行う技術
■オンライン状態でない場合にも時刻認証を利用可能とする技術