SII
Seiko Instruments Inc.

電子文書の存在証明に必要な時刻認証技術

２００３年３月０６日

セイコーインスツルメンツ㈱
クロノトラスト部
上畑正和　m.uehata@sii.co.jp

Chronotrust

アジェンダ

SII
Seiko Instruments Inc.

- タイムビジネスのトレンド
- なぜ時刻認証
- 時刻認証実現の３つのポイント
- 時刻の認証チェーン
- システム構成
- 運用規定
- 時刻認証サービスモデル
- 事例：電子認証インフラ

  エヌ・ティ・ティ・コミュニケーションズ（株）殿
- 事例：電子公証

  （株）日本電子公証機構殿
- 事例：ボイスロギングシステム

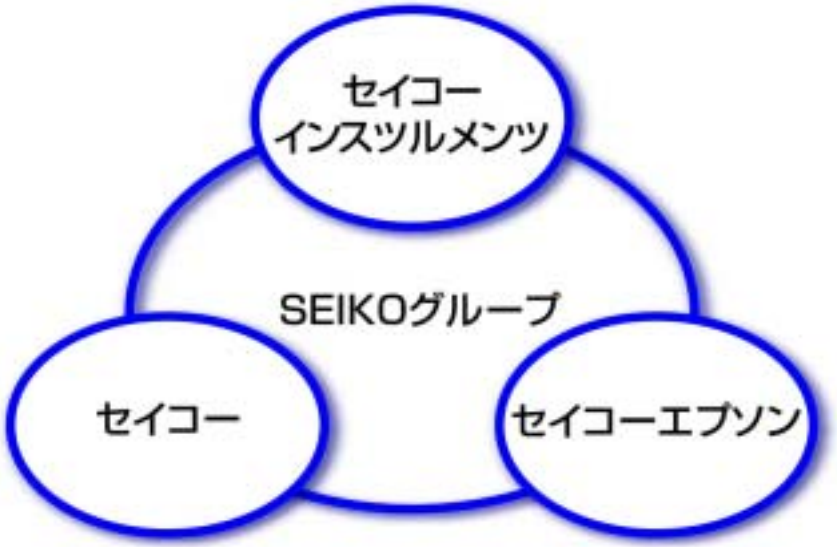
  ログイット（株）殿　，（株）日本電子公証機構殿

Chronotrust

SIIとセイコーグループ

SII
Seiko Instruments Inc.

1881年　服部金太郎服部時計店（現セイコー）を創業
1892年　時計製造工場精工舎（現セイコークロック、セイコープレシジョン）を創立
1937年　第二精工舎（現セイコーインスツルメンツ）を設立
1959年　第二精工舎諏訪工場が独立し、諏訪精工舎（現セイコーエプソン）を創立



Chronotrust

「時」と共に・・・120年

SII
Seiko Instruments Inc.

SEIKOグループ
「時」のあゆみ

“ 時の進化 ”

実社会から
ネット社会へ

Real World

1881　服部金太郎、京橋に服部時計店開く

1955　日本初の巻印付自動巻き「セイコーオートマチック」発売

1964　東京オリンピックの公式時計に（スイス時計メーカー以外初）

1974　世界初のクオーツデジタルウオッチ「セイコーデジタル」発売

1984　世界初の腕時計型コンピュータ「腕コン」発売

1992　バルセロナオリンピック公式時計

1994　リレハンメルオリンピック公式時計

1998　長野冬季オリンピック公式時計

1998　リスト型携帯情報端末「ラピュータ」発売

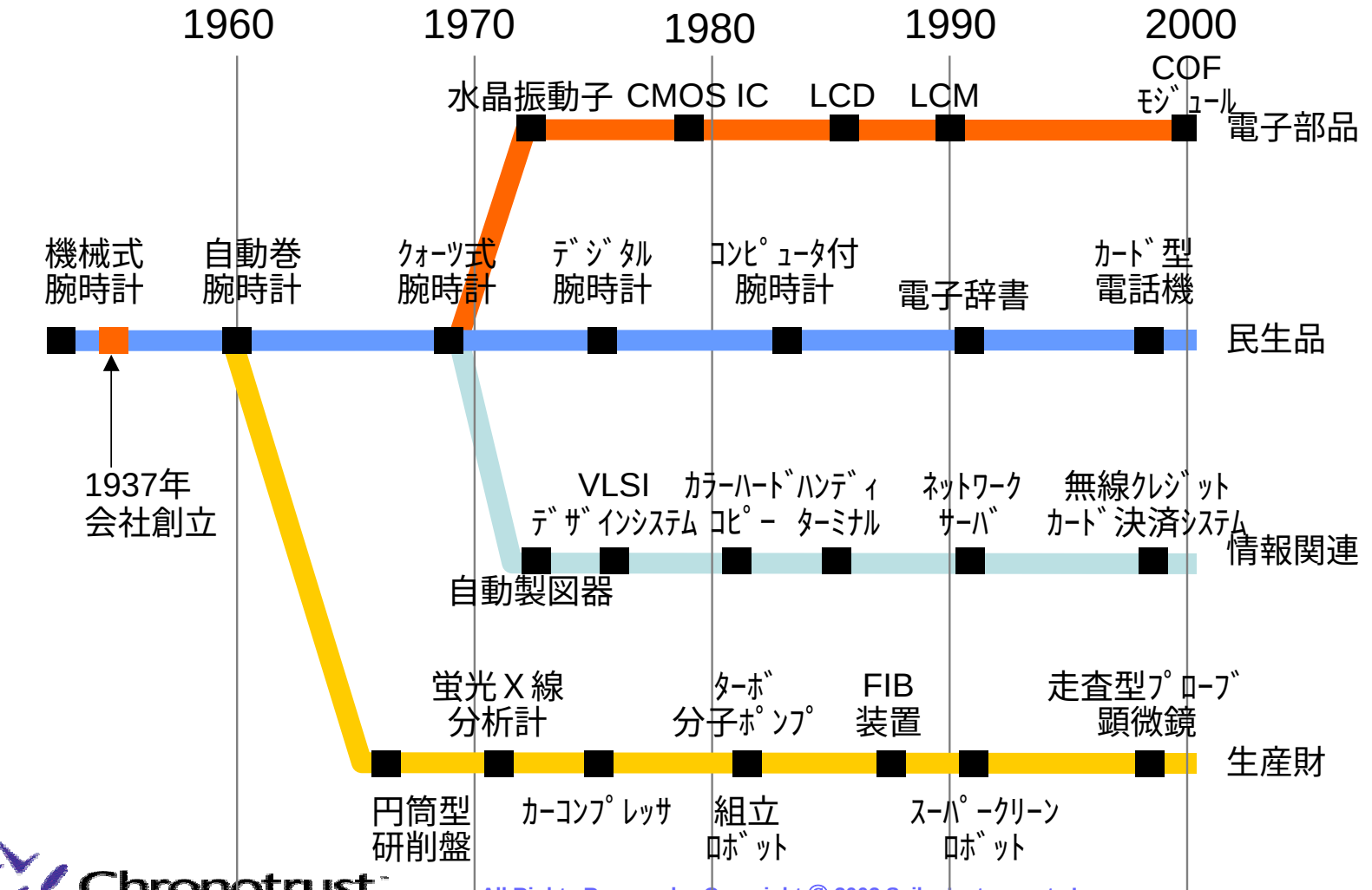
2002　ソルトレイクオリンピック公式時計

2002　タイムスタンプサーバー発売

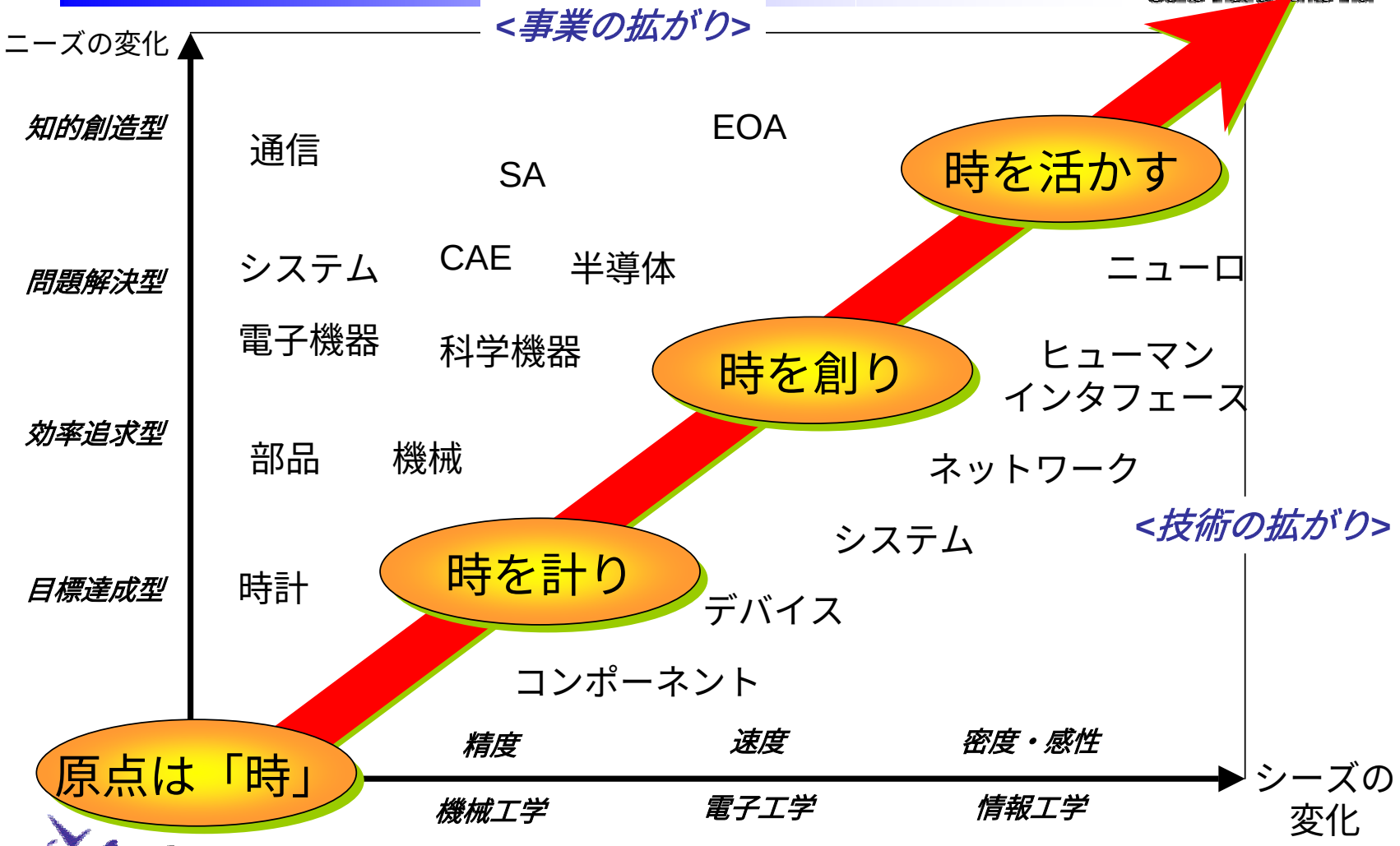
Net World

Chronotrust

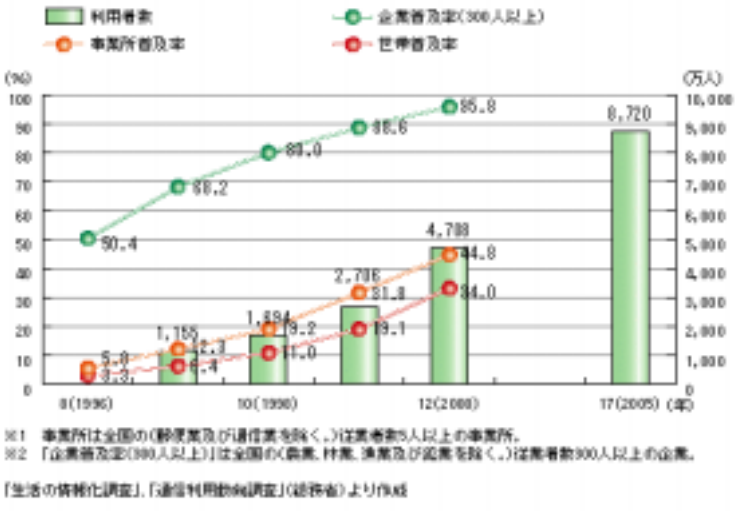
SIIの歴史 時計から多角化そして・・・



永遠のテーマ「時」これが私達の原点です

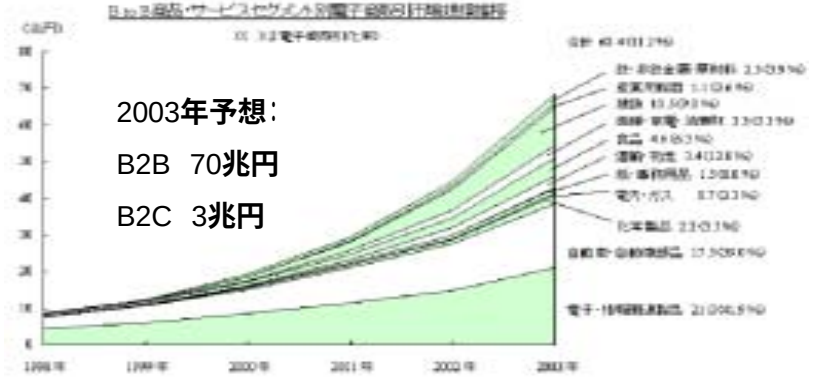


Network Security Infrastructure



※1 事業所は全国の(郵便業及び通信業を除く。)は従業者5人以上の事業所。
※2 「企業普及率(300人以上)」は全国の(農業、林業、漁業及び公務を除く。)は従業者数300人以上の企業。

「生活の情報化調査」、「通信利用動向調査」(総務省)より作成



2003年予想:

B2B 70兆円

B2C 3兆円

IT戦略本部の公開ホームページより

Phase1 ; Internet普及期（’94～’99）
1999年で企業普及率約90%=社会的市民権確保

サイバーセキュリティの重要性増大

-Chronotrust™

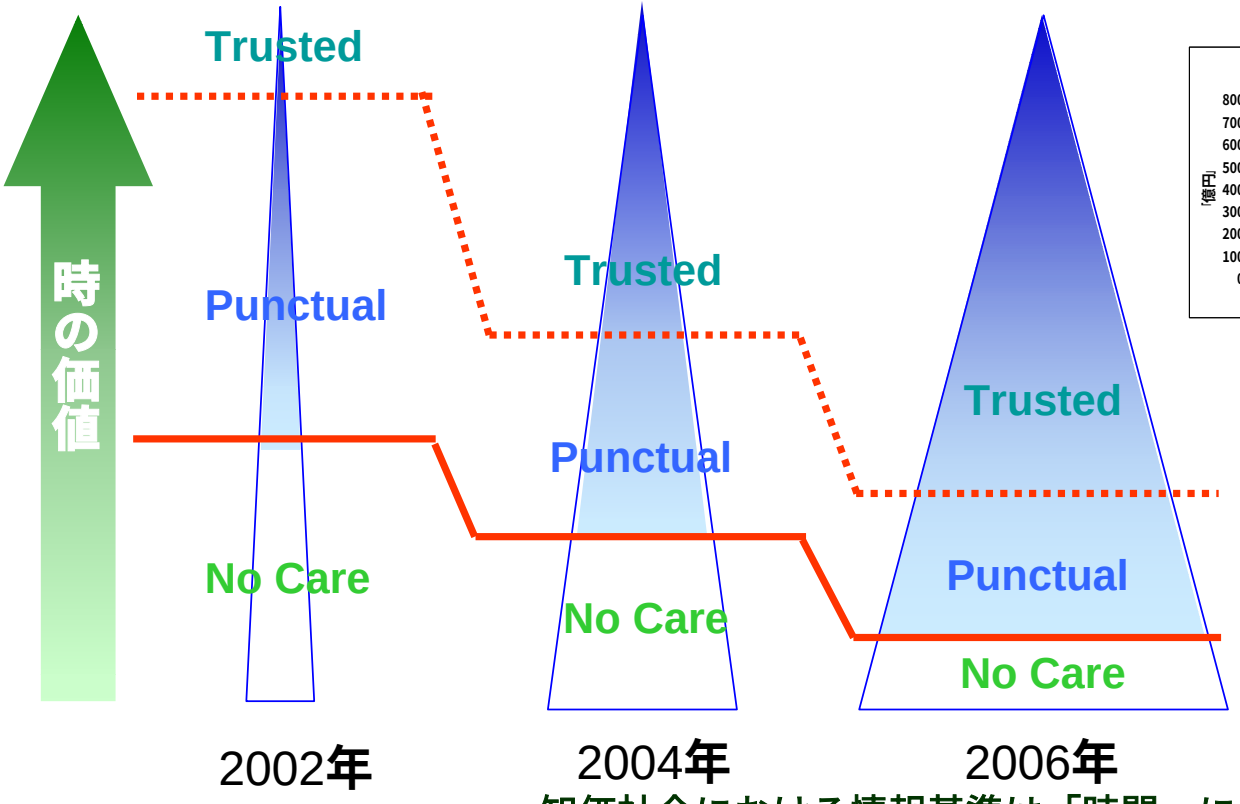
Phase2 ; Internetを利用したｻｰﾋﾞｽﾋﾞｼﾞﾈｽへの展開 (’99～)

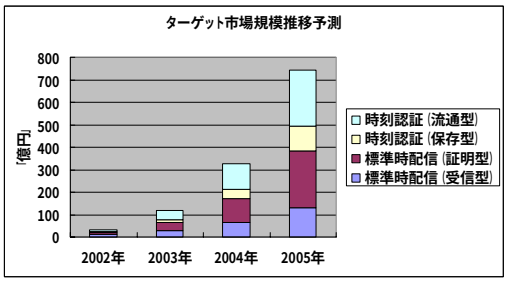
e-Commerce市場の拡大

タイムビジネスのトレンド

タイムビジネス市場全体の市場規模は２００５年で約1,５００億円、
関連産業も併せると、その周辺市場規模は3.2兆円と予測

出典： 総務省　タイムビジネス研究会報告書（2002年6月18日）

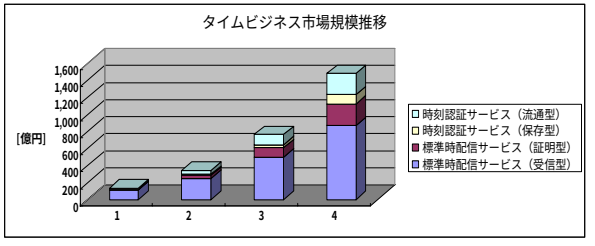




知価社会における情報基準は「時間」によって定まる。

時刻に関する世の中の動き

日本の動き



- タイムビジネス研究会（2002年1月～6月）
  - 政府・自治体等、公的機関への先行的導入の推進
  - 運用面・技術面を含めたガイドラインの策定
  - アジアのハブとしてのタイムビジネスの展開
  - 業界横断的な情報交換の場の設置
  - タイムビジネス推進協議会（ http://www.scat.or.jp/time/ ）
- ECOM（電子商取引推進協議会）　認証公証WG
  - 2002年度テーマ　「タイムスタンプ」
- ISO15408規定が日本政府調達基準となる（2001年4月）
  - **要求者はTSAの電子署名付TSと自身の電子署名を付けること。**
- 電子文書認証に関する法律　（2001年4月施行）
  - 電子署名法、IT書面一括法

世界の動き


Guidance for Industry

21 CFR Part 11; Electronic Records; Electronic Signatures

Time Stamps

- Authentidate社
  - USPS電子消印ﾌﾟﾛﾊﾞｲﾀﾞ（1500億Stamp/年）
- FDA　21CFR　Part11；電子記録/電子署名においてTimeStampの要求をDraftで規定（2002年2月）
- ETSI　102-023（2002-4）TSAのPolicy要求

タイムビジネス推進協議会

http://www.soat.or.jp/time/

SII Seiko Instruments Inc.

- 役員
  - 会長　中央大学教授　大橋正和
  - 副会長　東京大学教授　須藤　修
- 幹事
  - 日本電信電話（株)
  - （株）建設技術研究所
  - （独）通信総合研究所
  - セイコーインスツルメンツ（株）
  - （財）ﾃﾚｺﾑ先端技術研究支援ｾﾝﾀｰ
  - アマノ（株）
  - （株）ＮＴＴデータ
  - iDCイニシアティブ
  - 林俊樹（ﾒﾃﾞｨｱｺﾝｻﾙﾀﾝﾄ）

- 会員一覧（61社；発足時）
  - iDCｲﾆｼｱﾃｨﾌﾞ
  - **アマノ（株）**
  - アライド・ブレインズ（株）
  - （株）ｲﾝﾀｰﾈｯﾄｲﾆｼｱﾃｨﾌﾞ
  - （株）インフォシティ
  - （株）エイベック
  - **NTTコミュニケーションズ（株）**
  - **（株）NTTデータ**
  - （株）NTTデータ経営研究所
  - （株）エム研
  - **大橋正和（中央大学）**
  - （株）ガッツディト
  - （株）ゲーム
  - （株）建設技術研究所
  - コダック（株）
  - **サンマイクロシステムズ（株）**
  - （株）ジャストシステムズ
  - （株）ｽｸｳｪｱ
  - **須藤　修（東京大学）**
  - セイコーインスツルメンツ（株）
  - セイコープレシジョン（株）
  - ソラン（株）
  - **（独）通信総合研究所**
  - （財）ﾃﾚｺﾑ先端技術研究支援ｾﾝﾀｰ
  - 凸版印刷（株）
  - TIS（株）
  - （株)電通
  - 東京証券取引所
  - 東京都
  - （株)東京三菱銀行
  - **（株)東芝**
  - 西日本電信電話（株）
  - 日興コーディアルグループ
  - （社）日本医師会
  - 日本オラクル
  - （財）日本建設情報総合センター
  - 日本証券業協会
  - **日本電気（株）**
  - 日本電信電話（株）
  - **日本ボルチモアテクノロジーズ（株）**
  - 日本トレードマネージメント（株）
  - 野村證券（株）
  - （株）野村総合研究所
  - （有）バリアフリー
  - 林俊樹（メディアコンサルタント）
  - （株）ビットメディア
  - **富士ゼロックス（株）**
  - （株）富士総合研究所
  - **富士通（株）**
  - （株）フジテレビジョン
  - （株）ブイシンク
  - ブレインセラーズドットコム（株）
  - （株）マクニカ
  - **松本勉（横浜国立大学）**
  - **丸文（株）**
  - （株）みずほ銀行
  - （株）みずほコーポレイト銀行
  - **三菱電機（株）**
  - 大和証券SMBC（株）
  - （株）ＵＦＪ銀行
  - 郵政事業庁　貯金部

Chronotrust

なぜ時刻認証

■実社会では「何時」「どこで」「誰が」「何を」したのか？

行動の証拠が重要

■Internet社会でも「何時」、「誰が」、「何を」したのか？

意思表示の証拠が必要

- 電子データの存在証明
- 電子データの完全性証明
- 署名文書の長期保存
- 署名文書の重複検査

NetSecurityの基盤
時刻認証

Chronotrust

時刻認証実現の ３つのポイント

SII
Seiko Instruments Inc.

Time Source (時刻ソース)

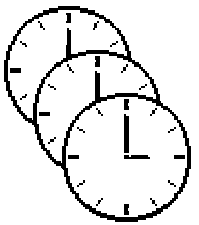
UTC協定世界時

・標準時刻（UTC協定世界時）と同期

・信頼できる第三者からの認証

→取引先に時刻を証明する基盤

Time Synchronization (時刻同期)



・認証された時刻ソース

・各機器の時刻同期

→時刻のばらつきによる
トラブルを回避

Time Stamp (タイムスタンプ)

・認証された時刻ソース

・時刻同期されたサーバ

・PKI技術

→文書・時刻の改ざん検出
取引の存在証明が可能

トレーサビリティの確保→認証のチェーン

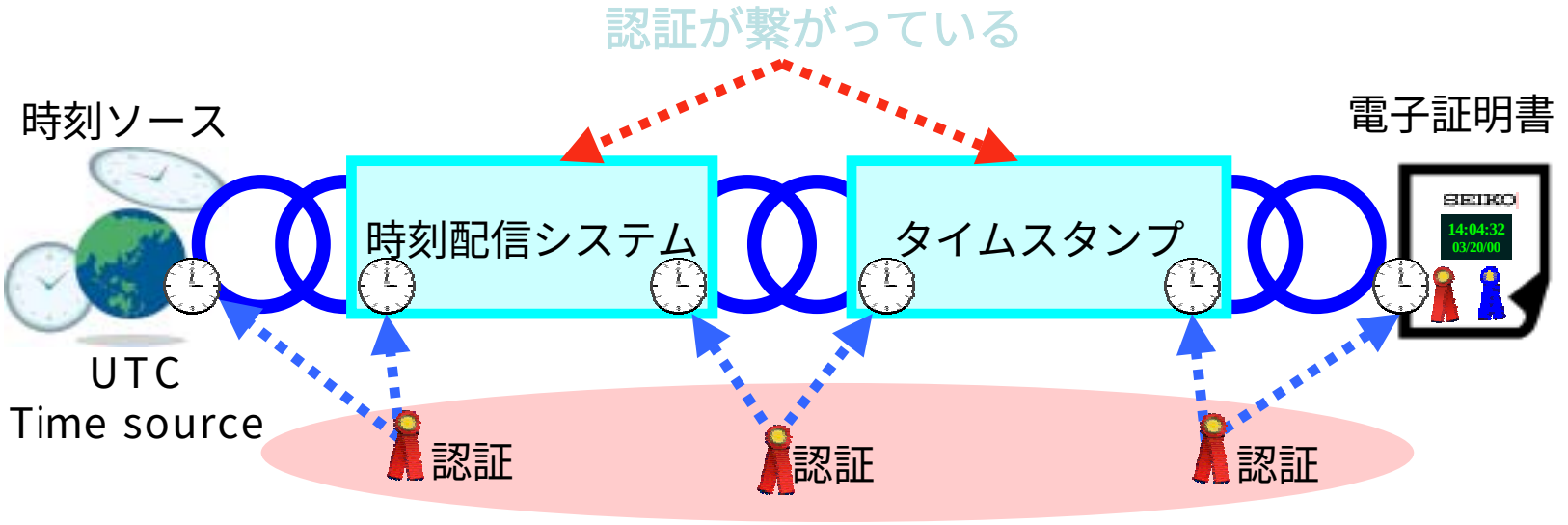
Chronotrust

時刻の認証チェーン

SII
Seiko Instruments Inc.

上流から下流まで厳正な認証連鎖で、
時刻の真正性を証明

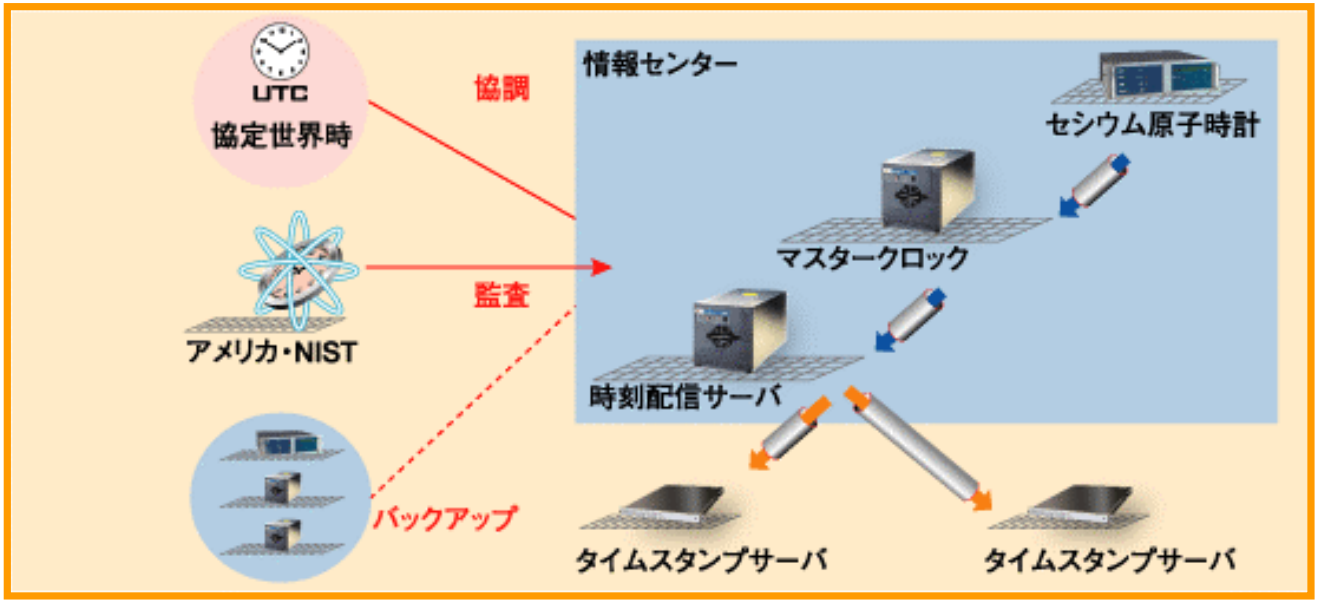
厳正な時刻認証サービス



Chronotrust

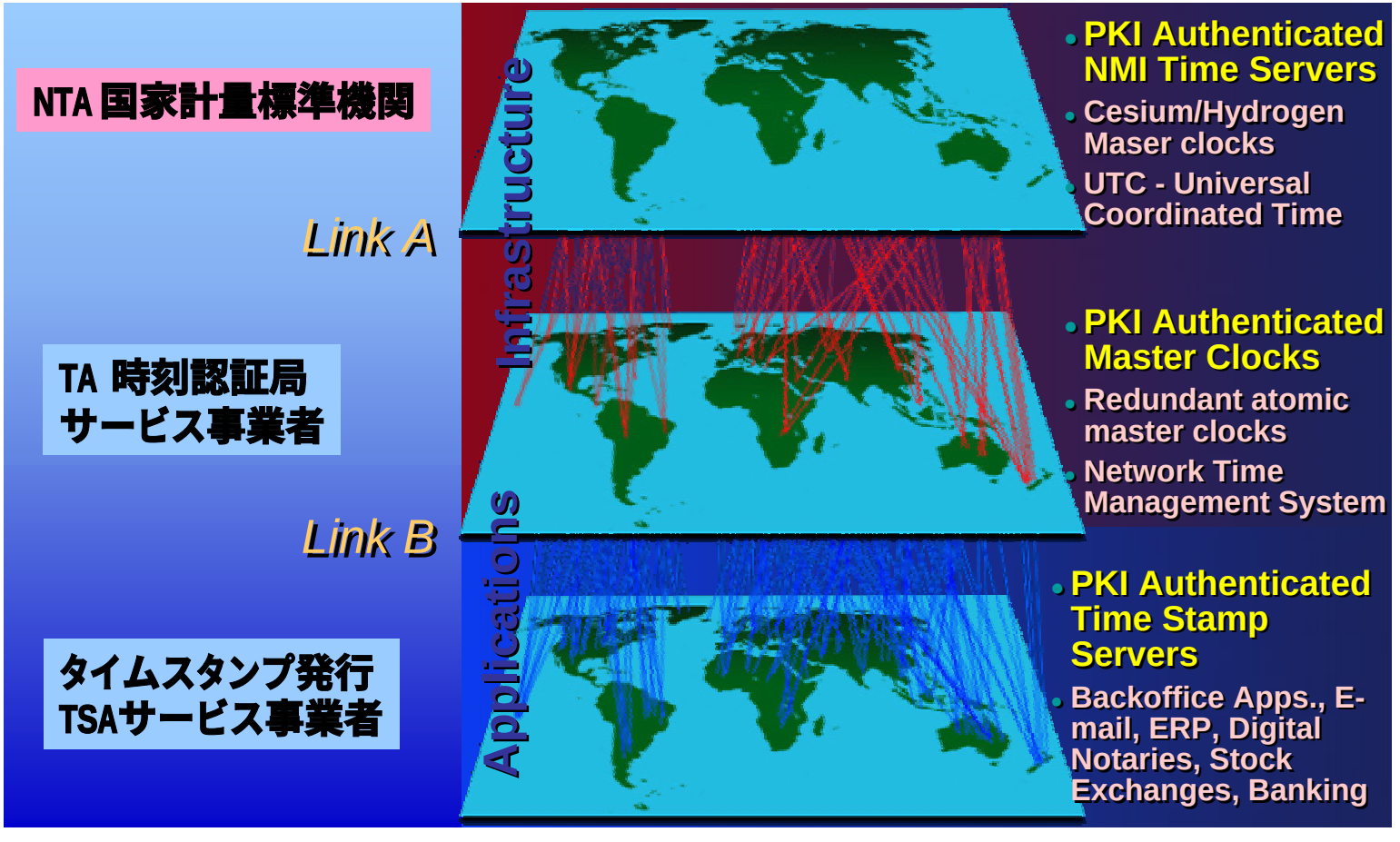
SEIKOブランドが保証する厳正な時刻とは

- 時刻ソースが明確である
- 国家計量機関の標準時とのつながりを証明できる
- 複数の原子時計で相互検証している
- 改ざんができない時刻である
- 第三者機関で認証した時刻である



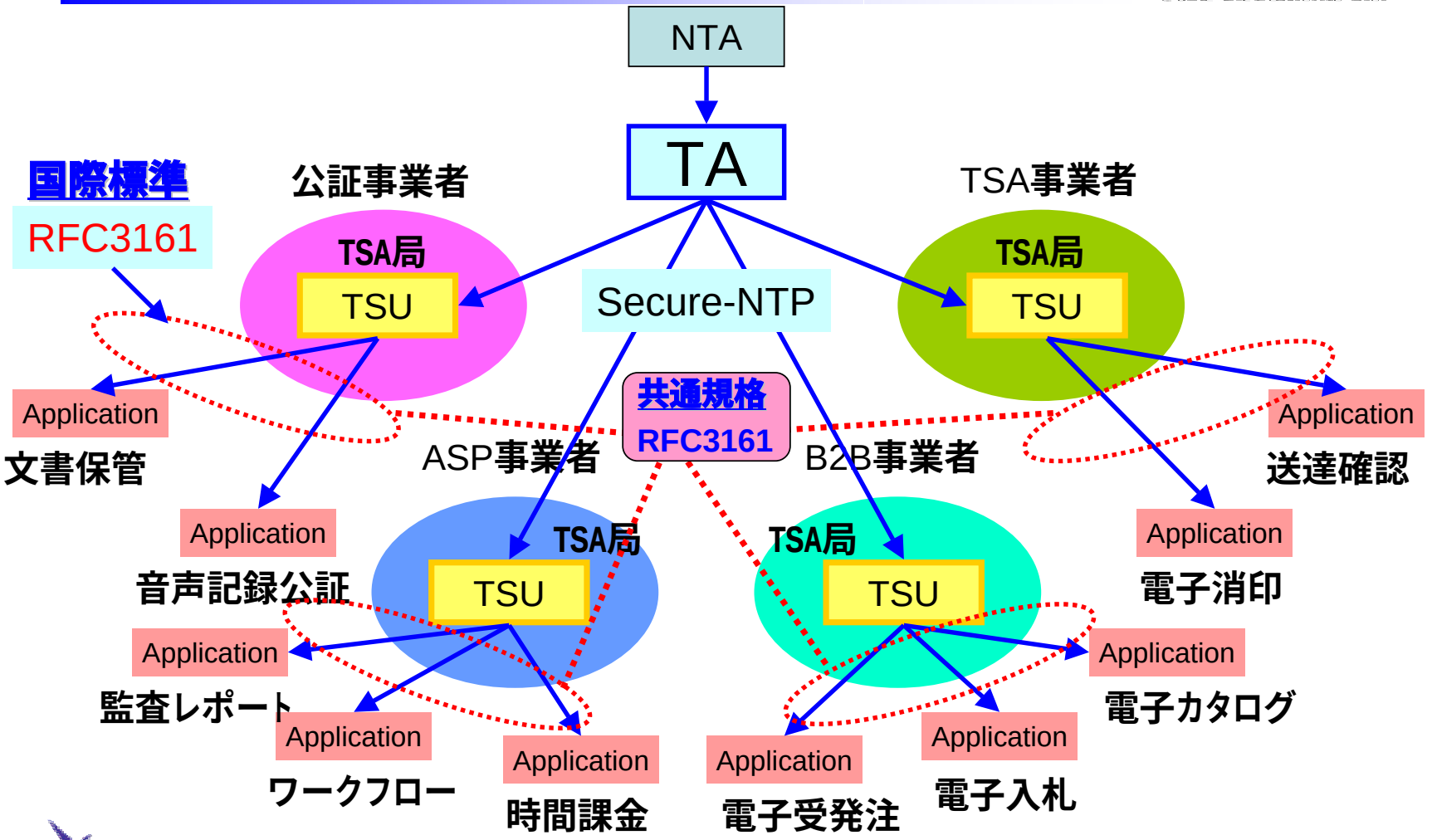
厳正かつ公正な時刻認証基盤

SII
Seiko Instruments Inc.



Chronotrust™

システム構成



タイムスタンプの概要

SII
Seiko Instruments Inc.

※RFC3161 abstract

- タイムスタンプの生成サービスは、あるデータが特定時間以前に存在していたことを証明するものである。
- TSAは信頼のおける第三者機関により運営されるものである。
- 組織内部で利用するタイムスタンプも必要になる。（TSAとTSUの関係）

Chronotrust

TSA:Time Stamping Authority TSU:Time-Stamp Unit

RFC3161の重要な機能

SII Seiko Instruments Inc.

- 否認防止サービスは、あるデータが特定時間以前から存在していたことを立証する能力を必要とする。
- タイムスタンププロトコルは、否認防止サービスを実施するための構成要素として使われる。

- タイムスタンプは、デジタル署名の失効前に付与することで、有効性を証明することができる
- 例えばデジタル署名が失効した後であっても、タイムスタンプと公開鍵証明書を利用すれば失効前に付与されていたことを証明することができる。

公開鍵基盤の最も重要な機能のひとつ

Chronotrust

TSAの要件

SII
Seiko Instruments Inc.

1. **信頼できる時刻ソースを利用すること**
2. **各TSTに信頼できる時刻を提供すること**
   TSTに含まれる情報：時刻、精度、順序性フラグ、シリアル番号・・・
3. **完全唯一なTSTを生成すること**
   署名鍵のバックアップ禁止、完全性の保証
4. **TSTが生成された時のセキュリティポリシを示す識別子をTSTに付与する。**
   例＞監査サービスモデル(SII定義)
   OID = 0.2.440.200125.1.3.2
   id-kp-timeStamping.タイムスタンプOID[1.3.6.1.5.5.7.3.8]
5. **データのハッシュ値に対してのみTSTを付与する**
   機密性を保持するための必須条件

Chronotrust

RFC3161のデータ構造

SII Seiko Instruments Inc.

Time Stamp Request

version
hashAlgorithm
hashedMessage
reqPolicy
nonce
certReq
extensions

Time Stamp Response

status
statusString
failInfo
timeStampToken

Time Stamp Token

contentType
version
digestAlgorithms
eContentType
eContent (= TSTInfo)
certificates
crls
signerInfos

TSTInfo

version
policy
hashAlgorithm
hashedMessage
serialNumber
genTime
accuracy
ordering
nonce
tsa
extensions

SignerInfos

version
sid
digestAlgorithm
signedAttrs
signatureAlgorithm
signature
unsignedAttrs

TSR

TSResp

CA局

Certificate

version
serialNumber
signature
validity
issuer
subject
subjectPublicKeyInfo
extensions

Hashed

RFC3281

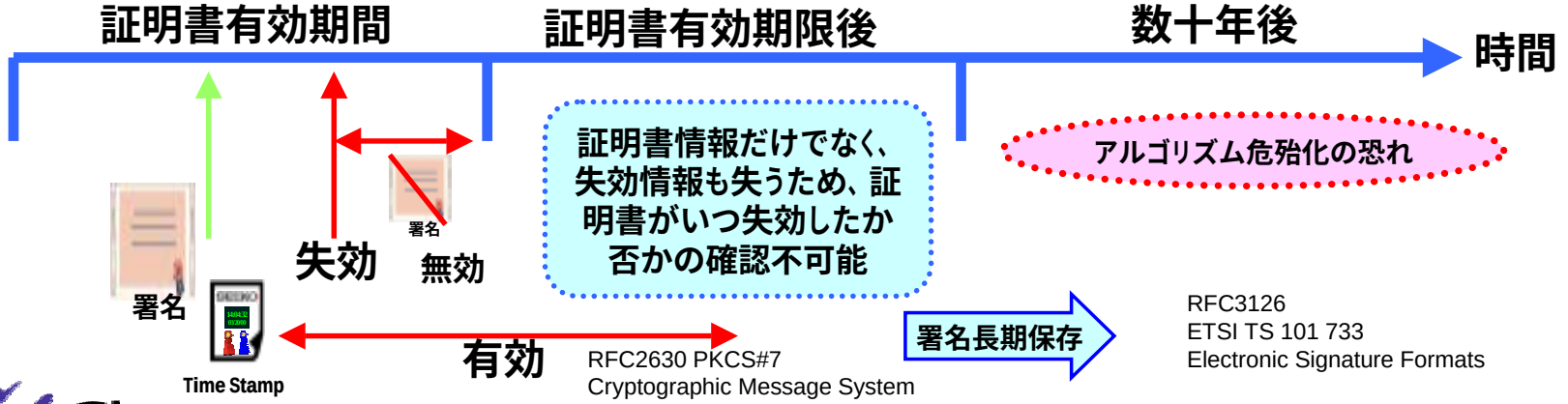
Time Attribute Certificate

version
holder
issuer
signature
serialNumber
attrCertValidityPeriod
attributes
issuerUniqueID
extensions
signatureAlgorithm
signatureValue

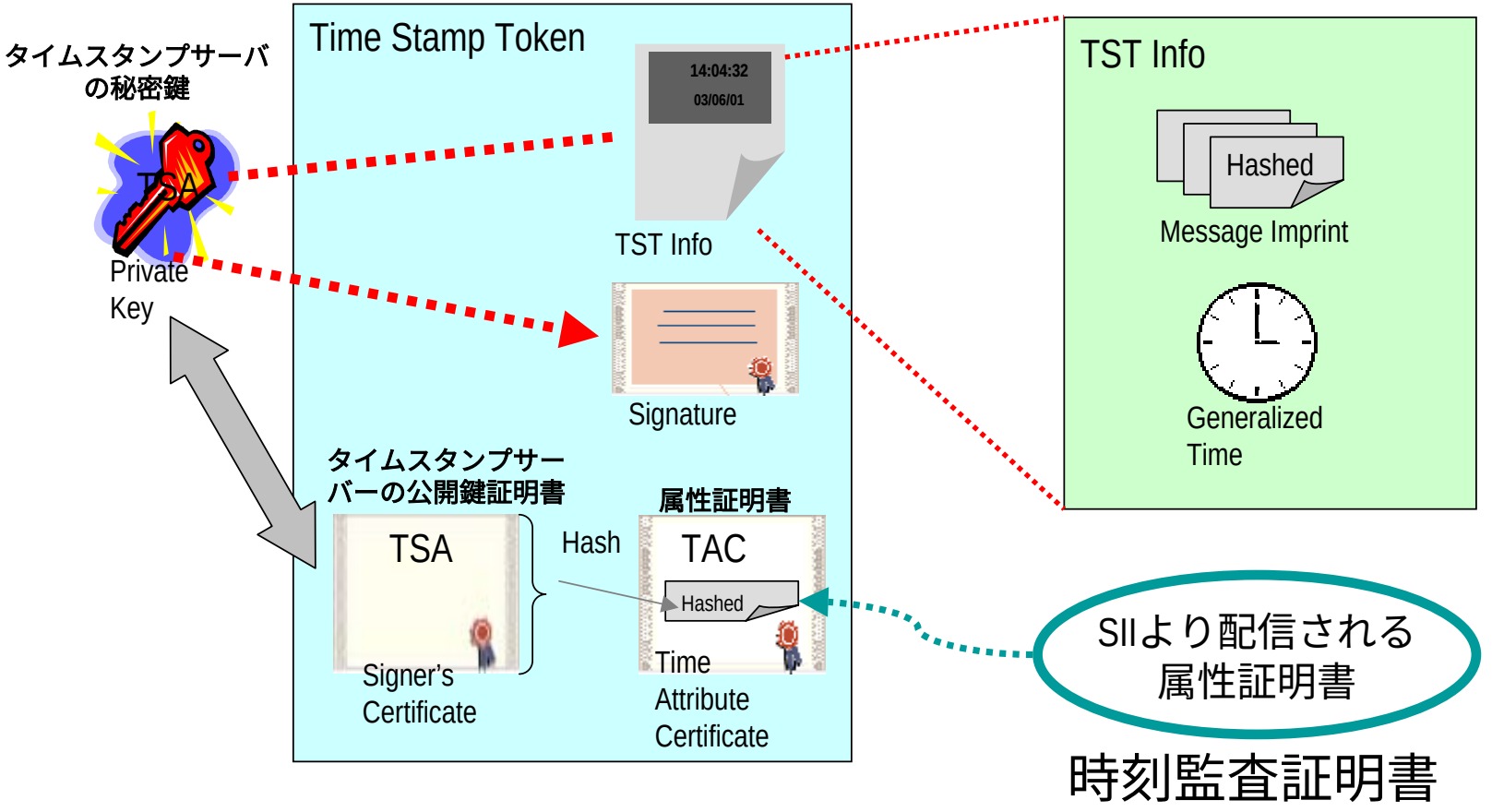
Chronotrust

CMS&タイムスタンプ属性

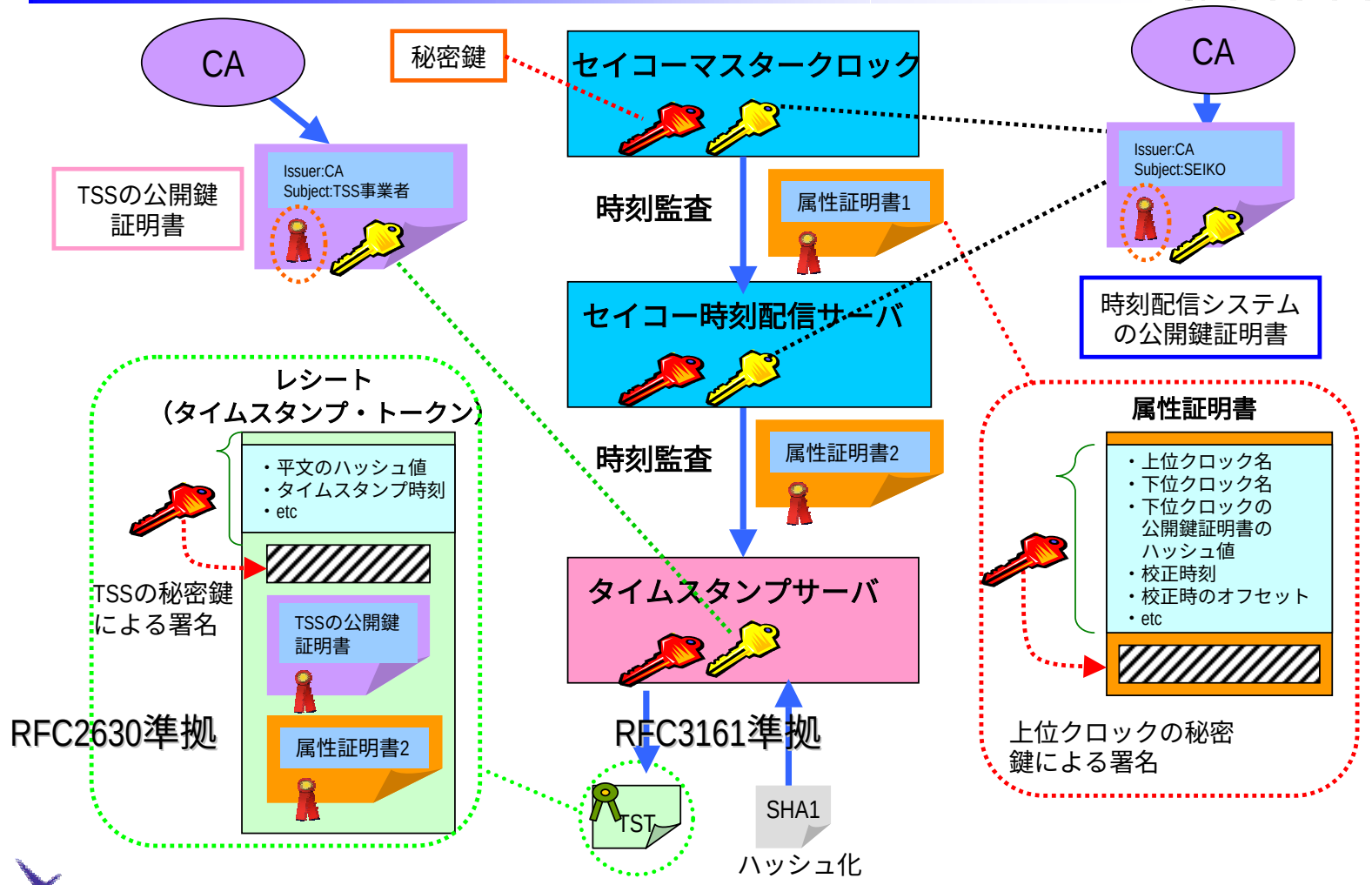
- タイムスタンプの主要な用途のひとつは、デジタル署名が**特定の時間以前**に生成されたことを証明する。
- 検証者は、証明書が失効された場合であってもデジタル署名の署名日と失効日の前後関係を知ることが出来る。
- 署名タイムスタンプ属性
  - Id-aa-timeStampToken OBJECT IDENTIFIER
    - OID 1.2.840.113549.1.9.16.2.14
    - ※CMSのSignerInfos unsignedAttrs（非署名属性）にTSTを含める



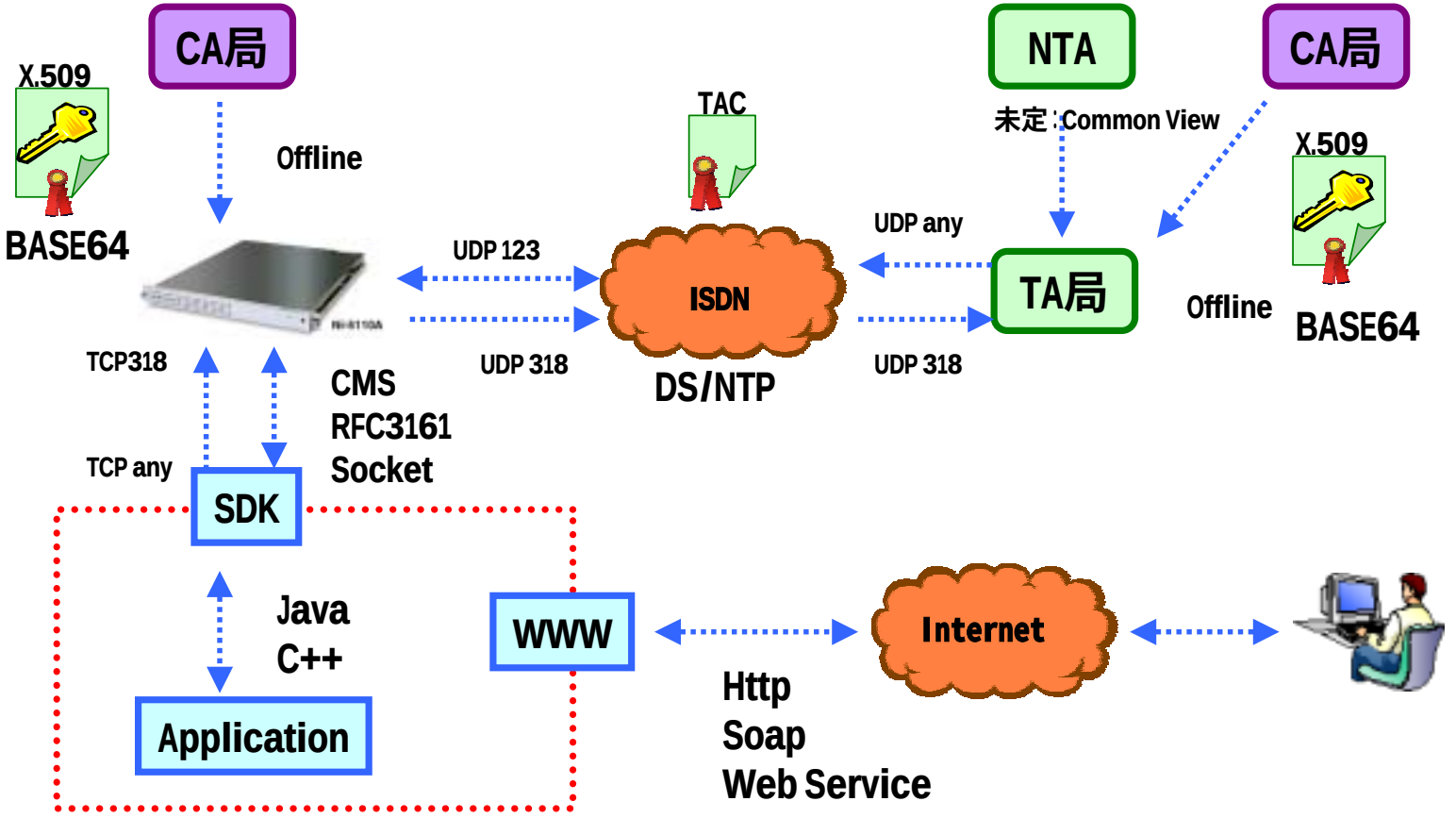
Time Stamp Tokenの構造について



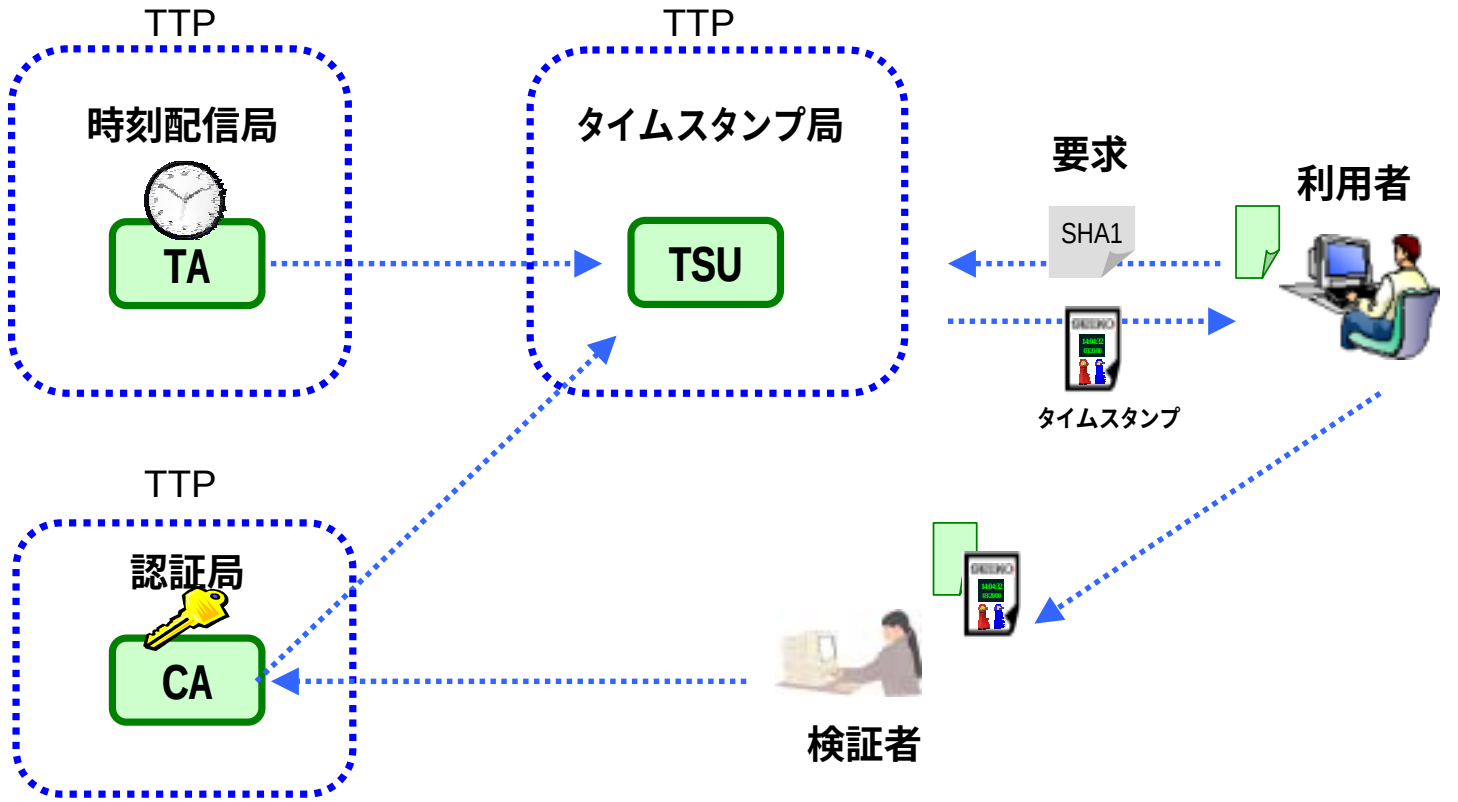
タイムスタンプサーバーの仕組み



TSUの通信環境とAP開発環境

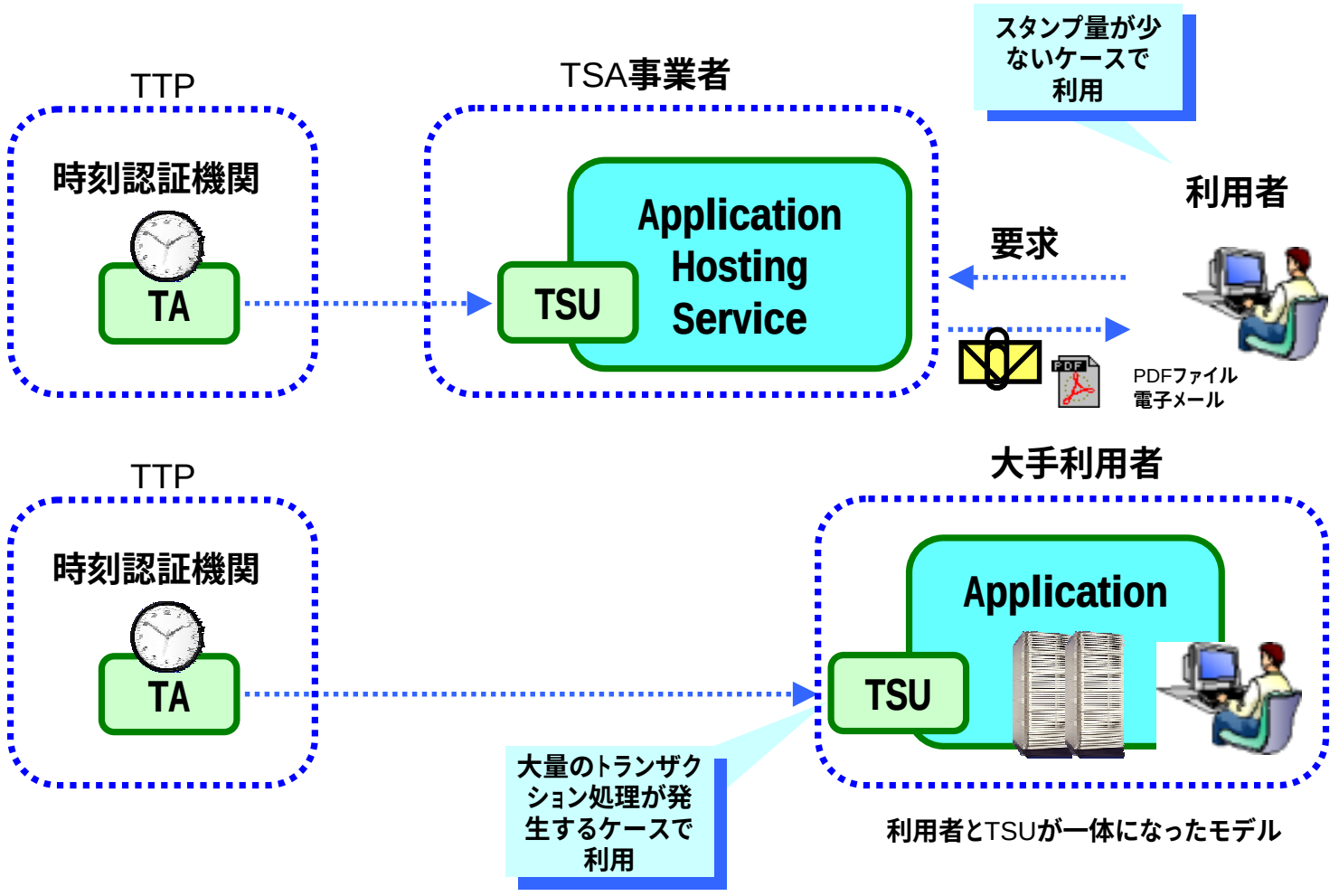


TSUシステム構成(基本)



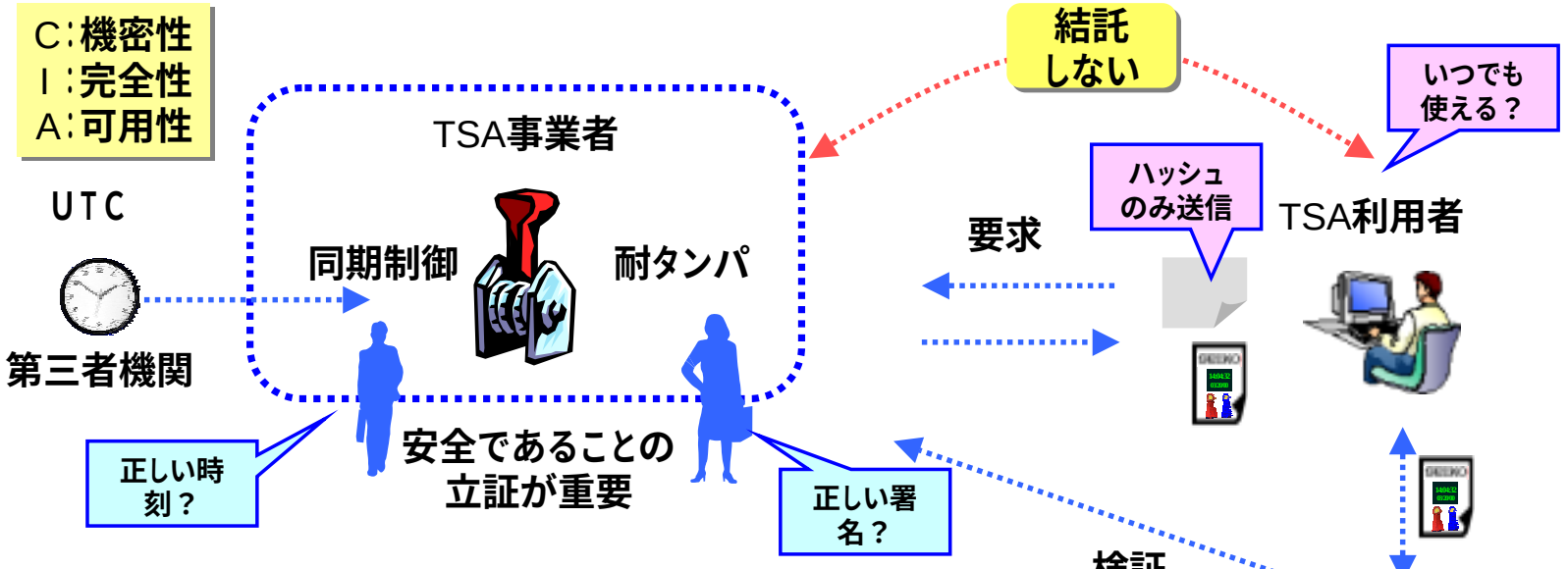
TTP:Trusted Third Party

TSUシステム構成(応用)



TSAのセキュリティ要件

SII
Seiko Instruments Inc.

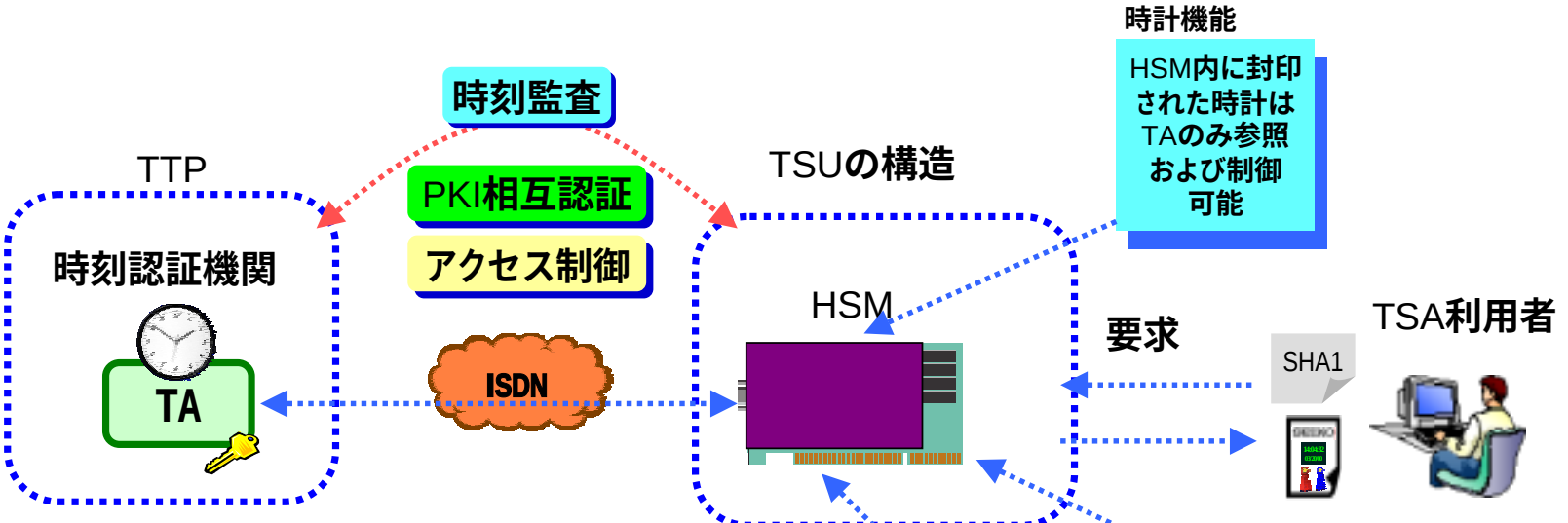


- TSA事業者とTSA利用者が結託した場合の脅威
  - 電子文書の改ざんが可能
  - 時刻をバックデートし、原本のすり替えが可能

対策が重要

Chronotrust

安全なTSUの要件



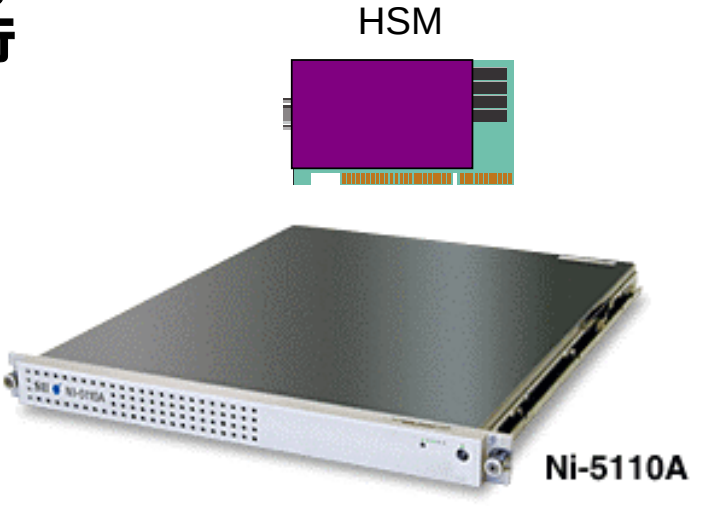
- 相互認証によるTSUとTAの関係を特定
- 時刻監査によるTSUの時計精度保証
- ユニークなシリアル番号管理
- 第三者からの時刻配信･監査
- HSMモジュールの採用による耐タンパ性
- 定期的な時刻監査の実施
- 監査結果に対する厳正なアクセス制御

タイムスタンプサーバ Ni-5110A

SII Seiko Instruments Inc.

高精度な時計機能 (TMC同期型)
ハッシュデータに対するタイムスタンプの付与
タイムスタンプトークン (デジタル署名) の発行
耐タンパー構造 (秘密鍵保護)

- サポート鍵長 ⇒ RSA,DSA 1024bit長
- Hashアルゴリズム ⇒ SHA-1 160-bit
- Time Stamp Protocol :RFC3161
- Time Stamp Token :RFC2630
- Co-Processボード (FIPS 140-1 Level3取得)



時刻認証サービス

- クロノトラスト時刻配信センタを自社運営／管理
- Cesium原子時計を用いた正確な時間
- Tractabilityのある時刻リソース
- ﾀｲﾑｽﾀﾝﾌﾟｻｰﾊﾞに対しての時刻校正履歴を提供可能
- バックアップ環境による高信頼性 (バックアップ機の2重化システム)

Chronotrust

ＴＴＰ＆運用規定

SII
Seiko Instruments Inc.

Chronotrust

時刻配信・監査サービス用
クロノトラスト時刻認証局運用規定
http://www.sii.co.jp/ni/repository/index.html

時刻配信局

ポリシ
運用規定

タイムスタンプ局

ポリシ
運用規定

CPとCPSのガイドラインはRFC2527 にて公開

認証局

ポリシ
運用規定

証明書ポリシ	証明書の目的や利用用途を規定。CPは証明書の拡張領域にOID形式で記載される。
認証局運用規定	CPをどのように実施するかという、CAの運用規定を定めたもの。CAのシステムや運用手順を明示的な文書にして、利用者に公開する。

Chronotrust

クロノトラスト 3種のサービス

SII
Seiko Instruments Inc.

A 時刻認証サービス

タイムスタンプサービス事業者向けのトラステッドな時刻認証。
最も厳正かつ公正な時刻認証サービス。タイムスタンプサーバで
発行されたデジタル署名にSEIKOの時刻監査証が添付される。

B 時刻配信サービス

一般企業およびIDC事業者向けのトラステッドな時刻配信。
厳正な時刻配信による企業内の安全な時刻同期システムを構築する。
採用企業については、SEIKOのSecure-Site-Seal表示が可能。

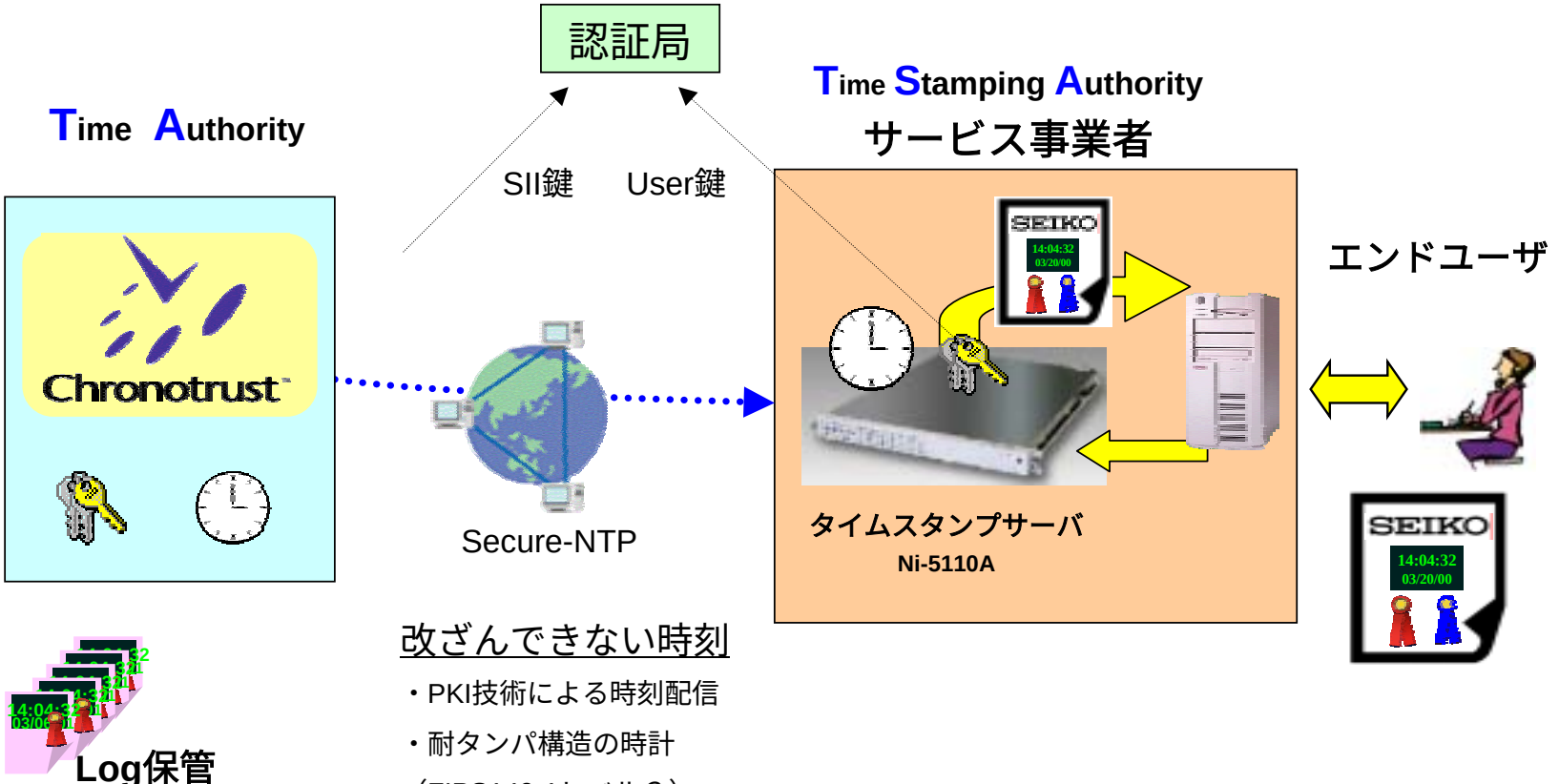
C 時刻監査サービス

一般企業および一般サービス事業者向けの時刻監査・監視。
一般企業のNet時刻がUTC標準時と比べて、どれだけ誤差があるのかを
監査・監視するサービス。

Chronotrust™

時刻認証 サービスモデル

SII
Seiko Instruments Inc.



改ざんできない時刻

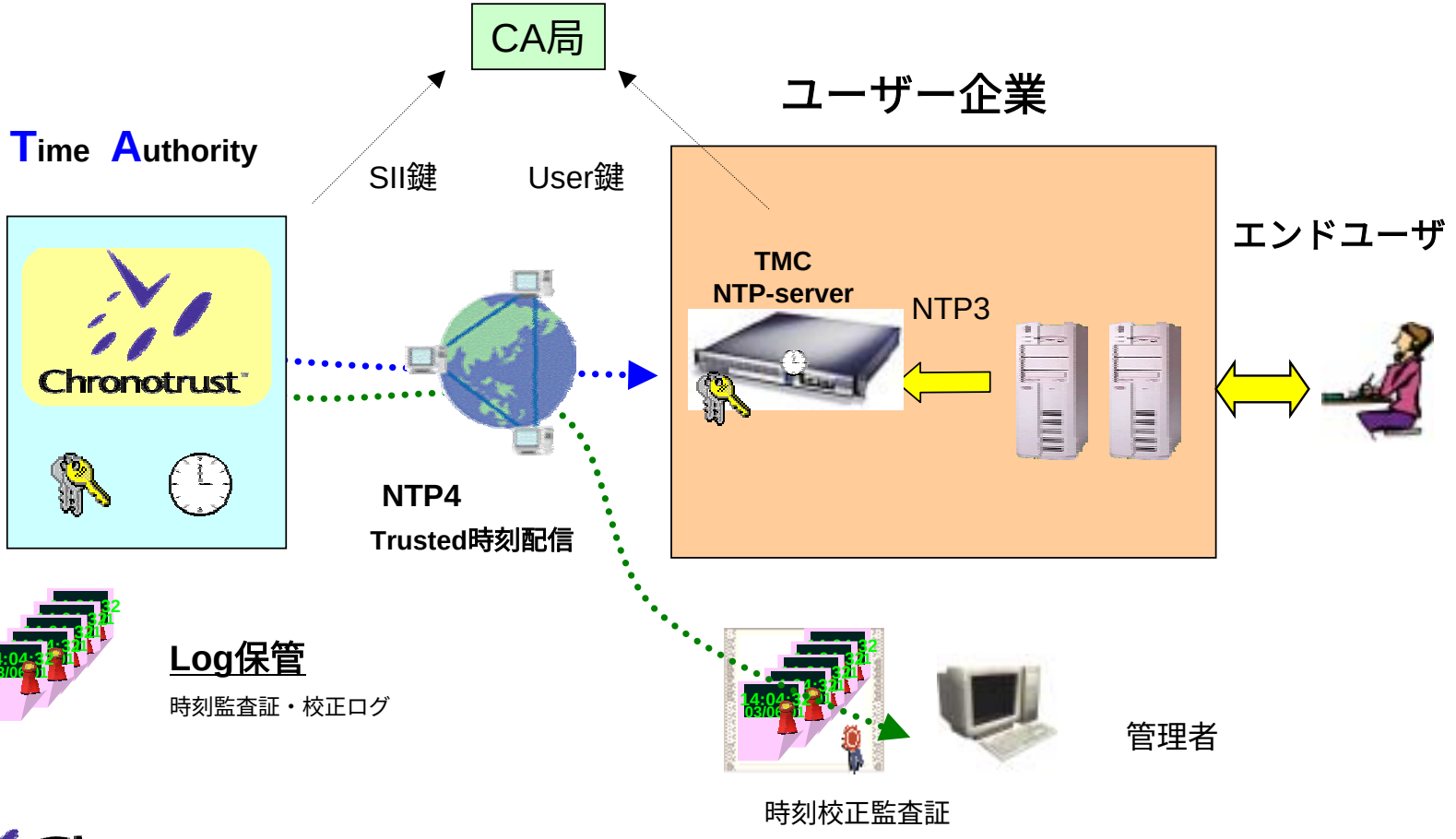
- PKI技術による時刻配信
- 耐タンパ構造の時計
（FIPS140-1レベル３）

Log保管

時刻監査証明書・監査ログ

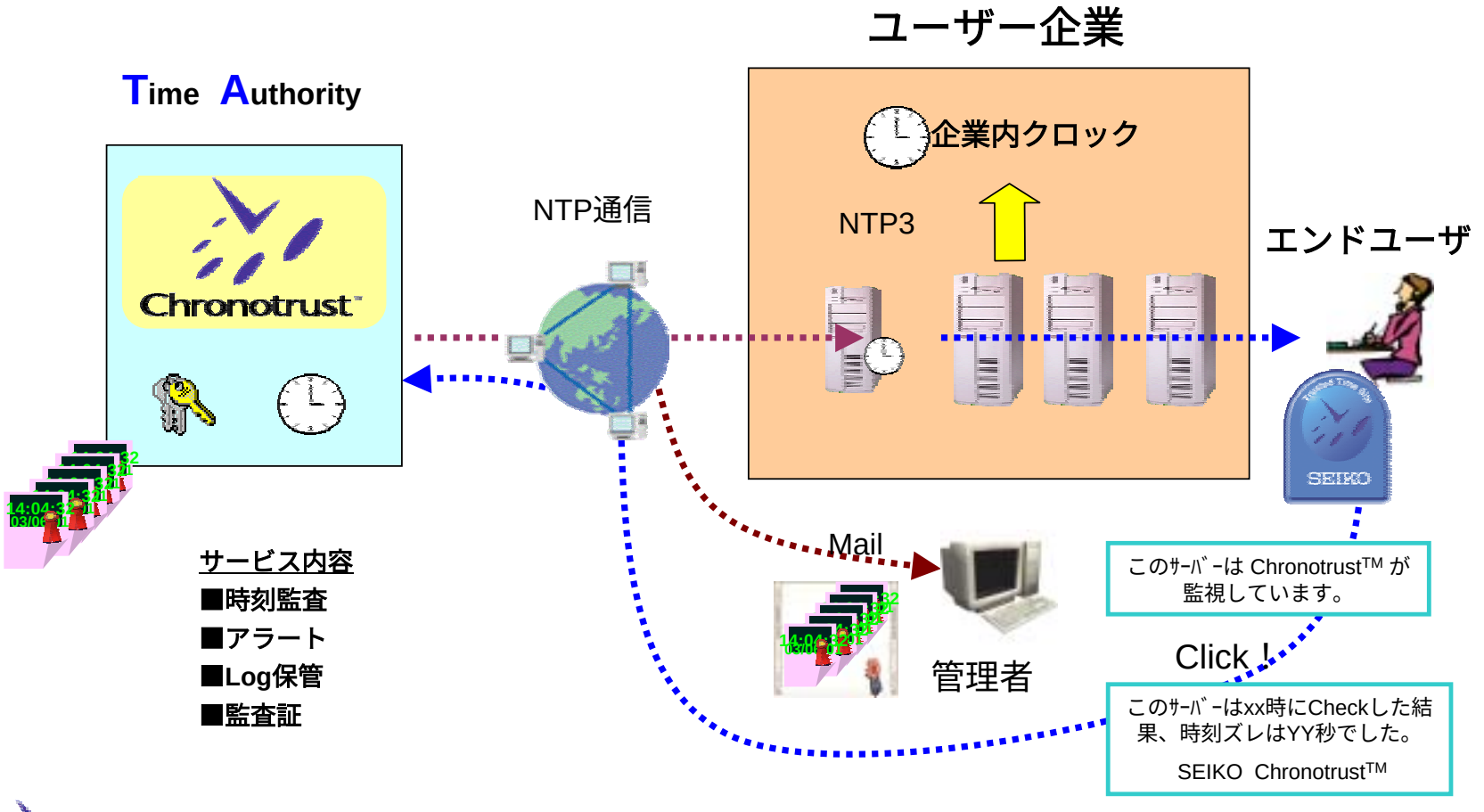
Chronotrust

時刻配信 サービス



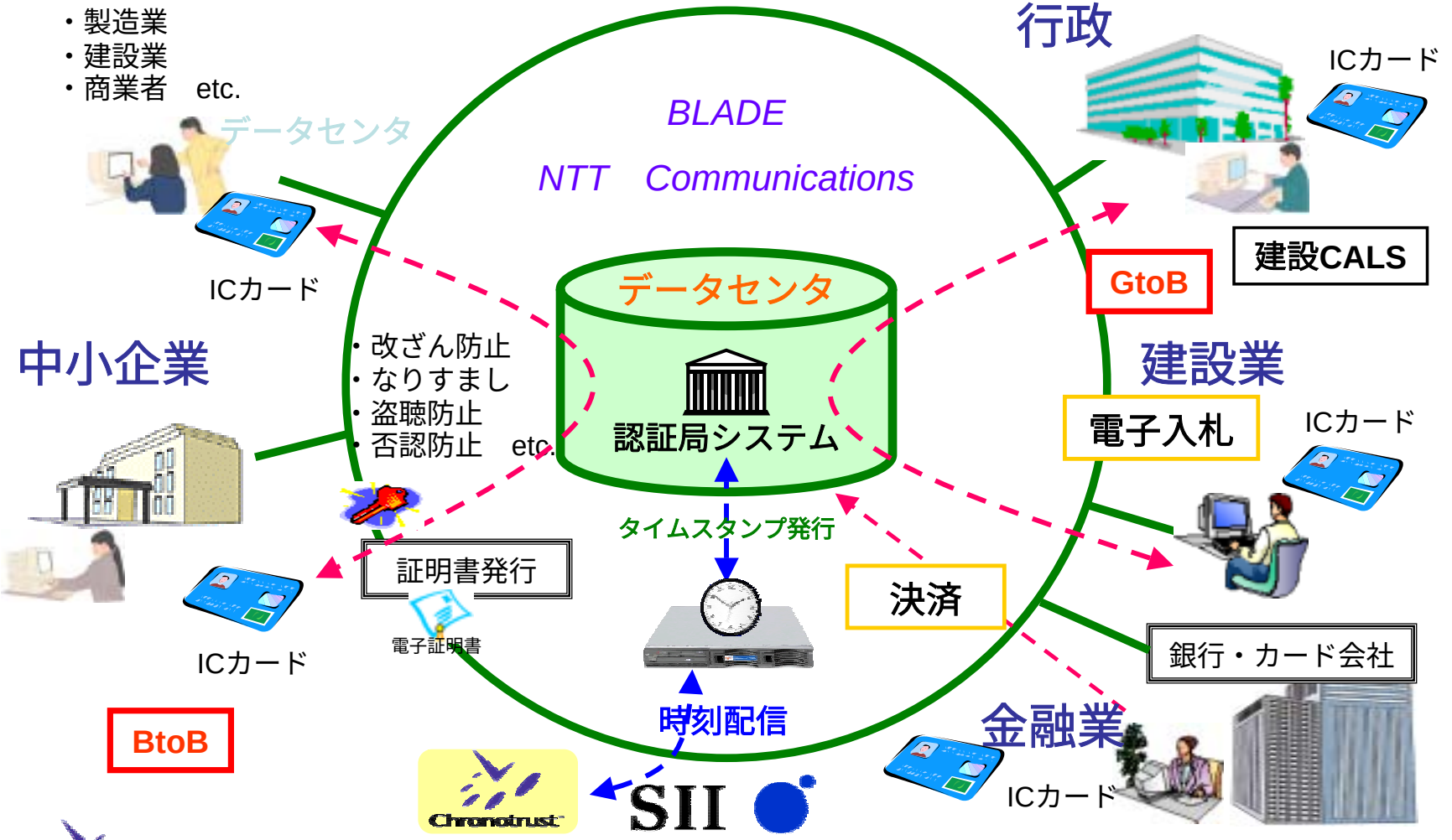
Chronotrust

時刻監査サービス

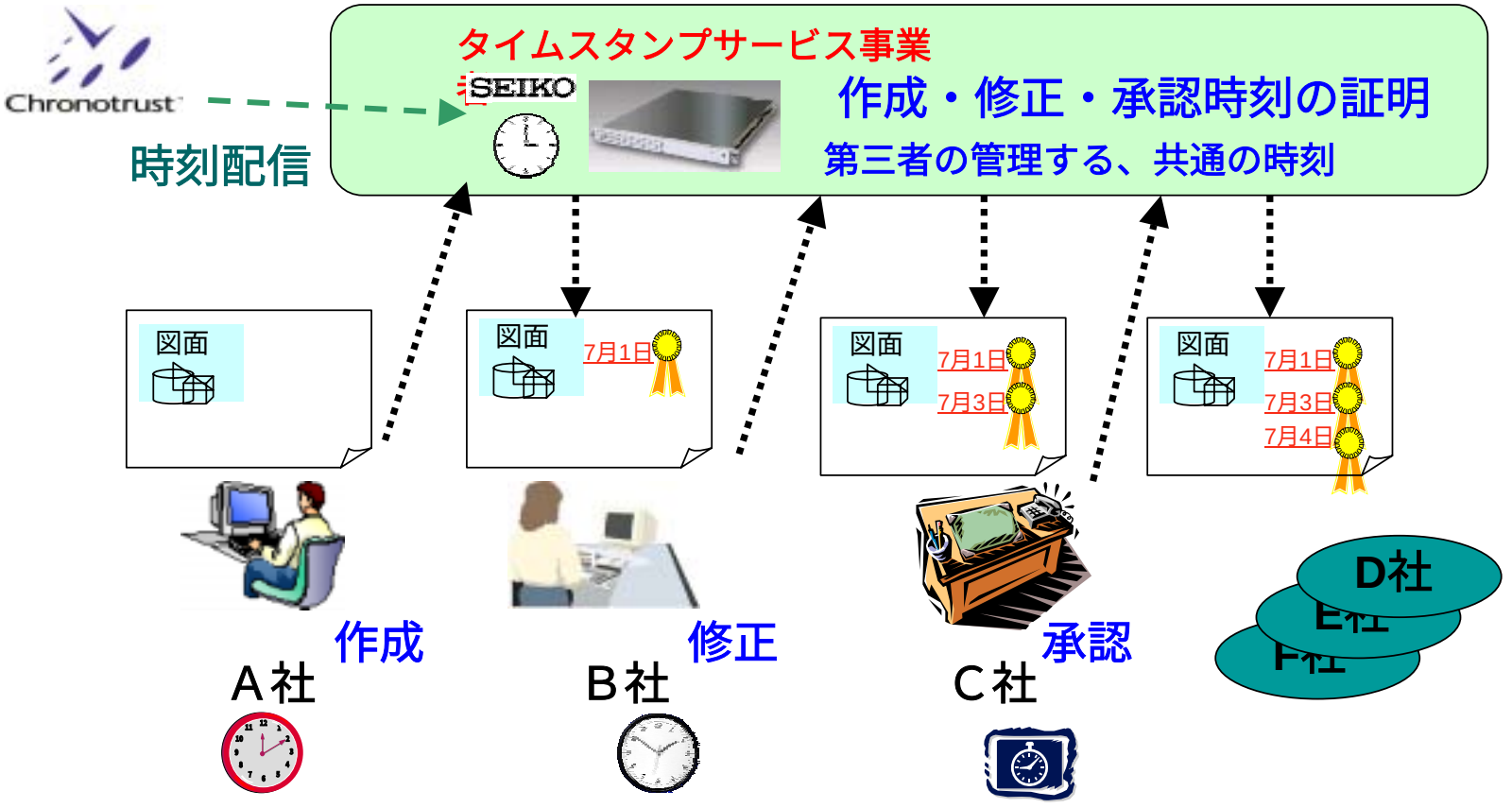


事例：電子認証インフラ

エヌ・ティ・ティ・コミュニケーションズ（株）殿



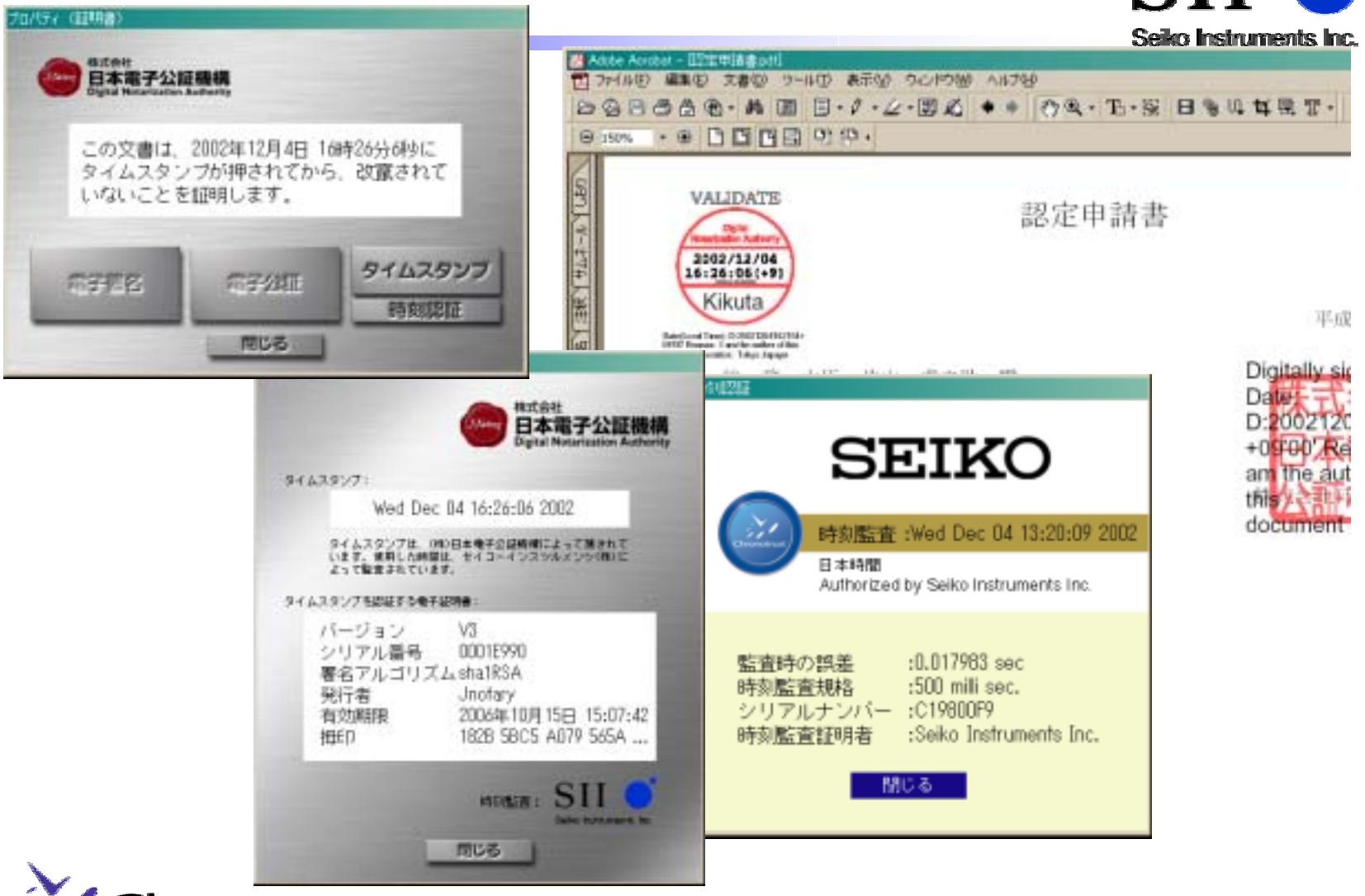
事例；企業間のドキュメントワークフロー



事業者間で流れる文書の時刻認証→文書の共有・版管理のトラブル防止

事例；電子公証　（株）日本電子公証機構殿

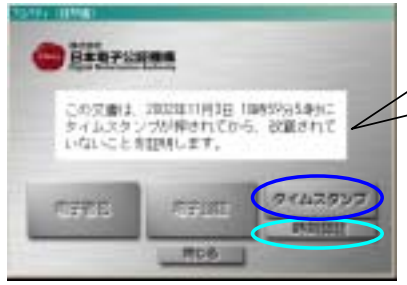
SII Seiko Instruments Inc.



Chronotrust

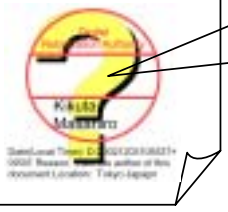
公証付きデータの検証方法　（株）日本電子公証機構殿

スタンプの個所をクリックすると、内容が表示されます。



さらに、クリックすると、この証明書が表示されます。

電子データ
(公証付き)



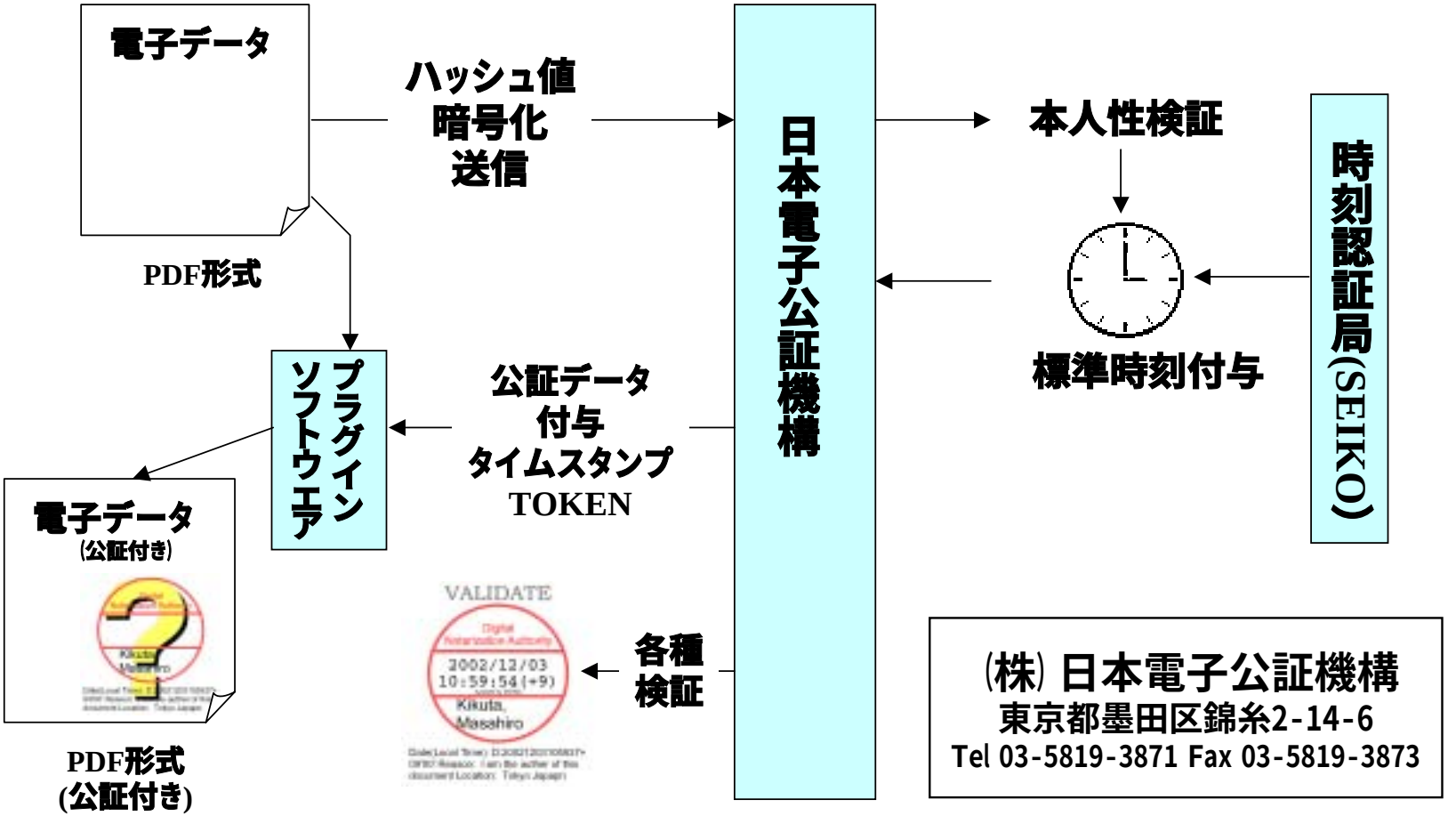
PDFファイル上に、**電子公証**のスタンプが付与されます。

タイムスタンプの個所をクリックするとタイムスタンプが表示されます。

時刻認証の個所をクリックすると時刻証明書が表示されます。

公証付与のフロー　（株）日本電子公証機構殿

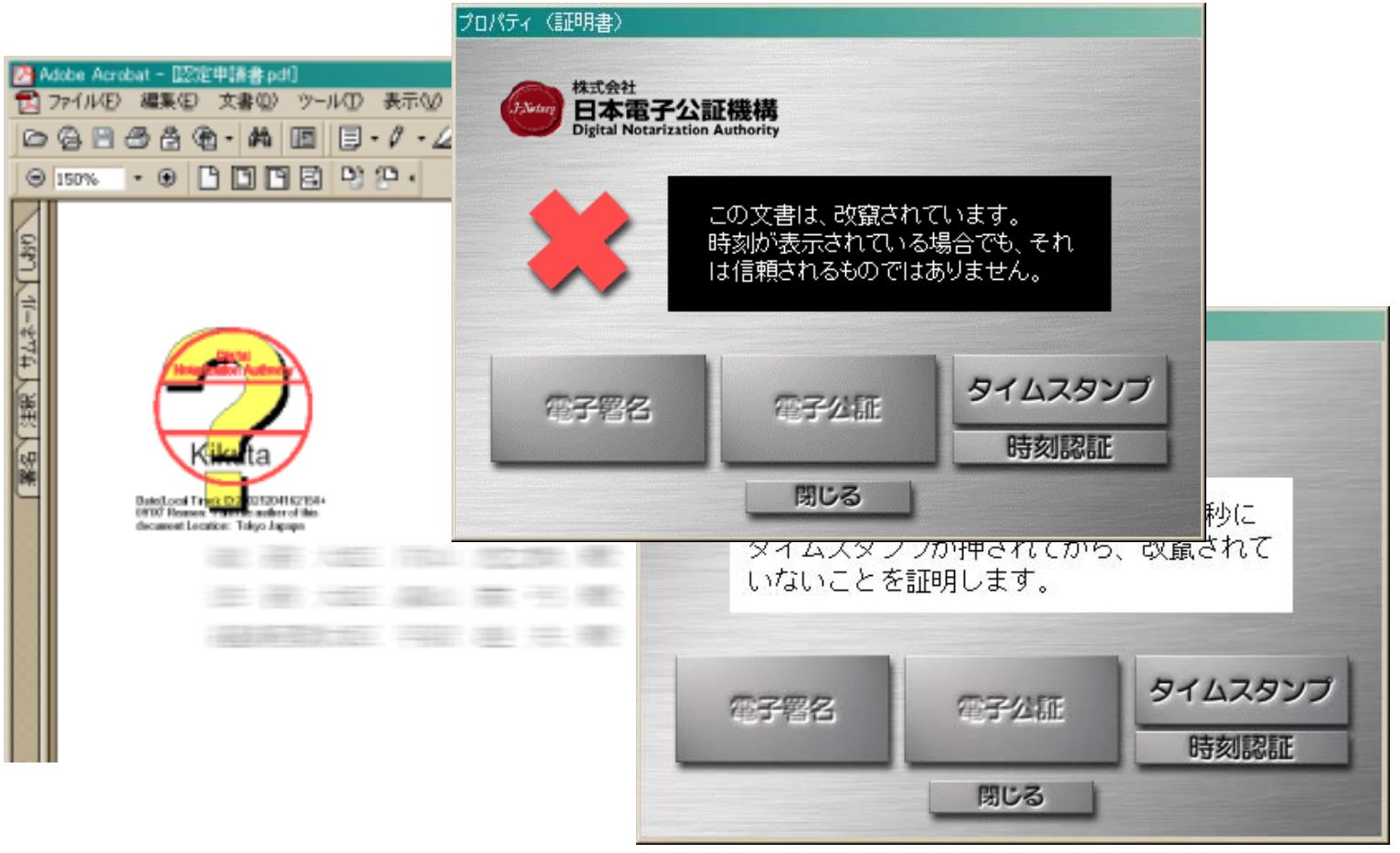
SII
Seiko Instruments Inc.



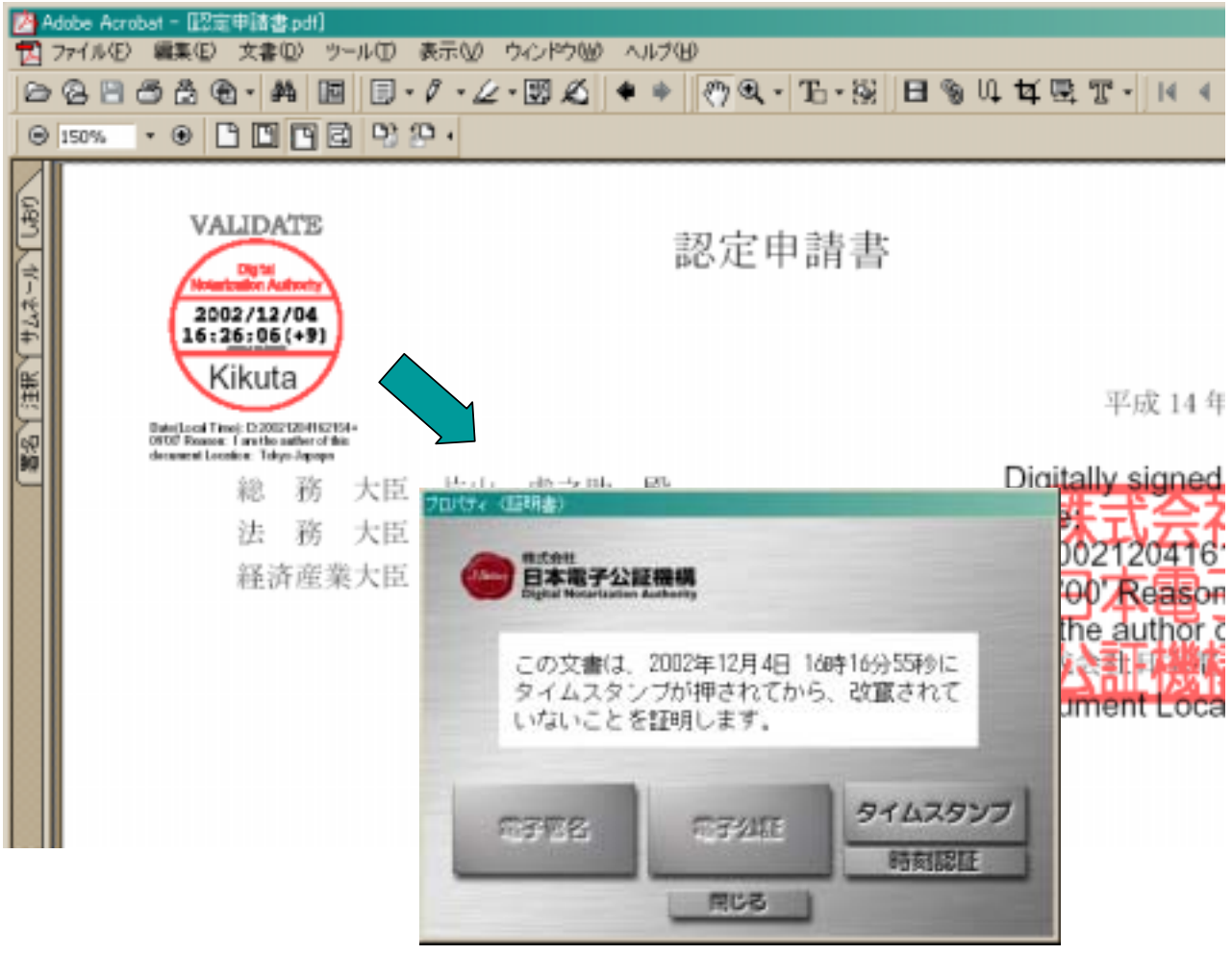
(株) 日本電子公証機構
東京都墨田区錦糸2-14-6
Tel 03-5819-3871 Fax 03-5819-3873

Chronotrust

改竄、非改竄証明書　（株）日本電子公証機構殿

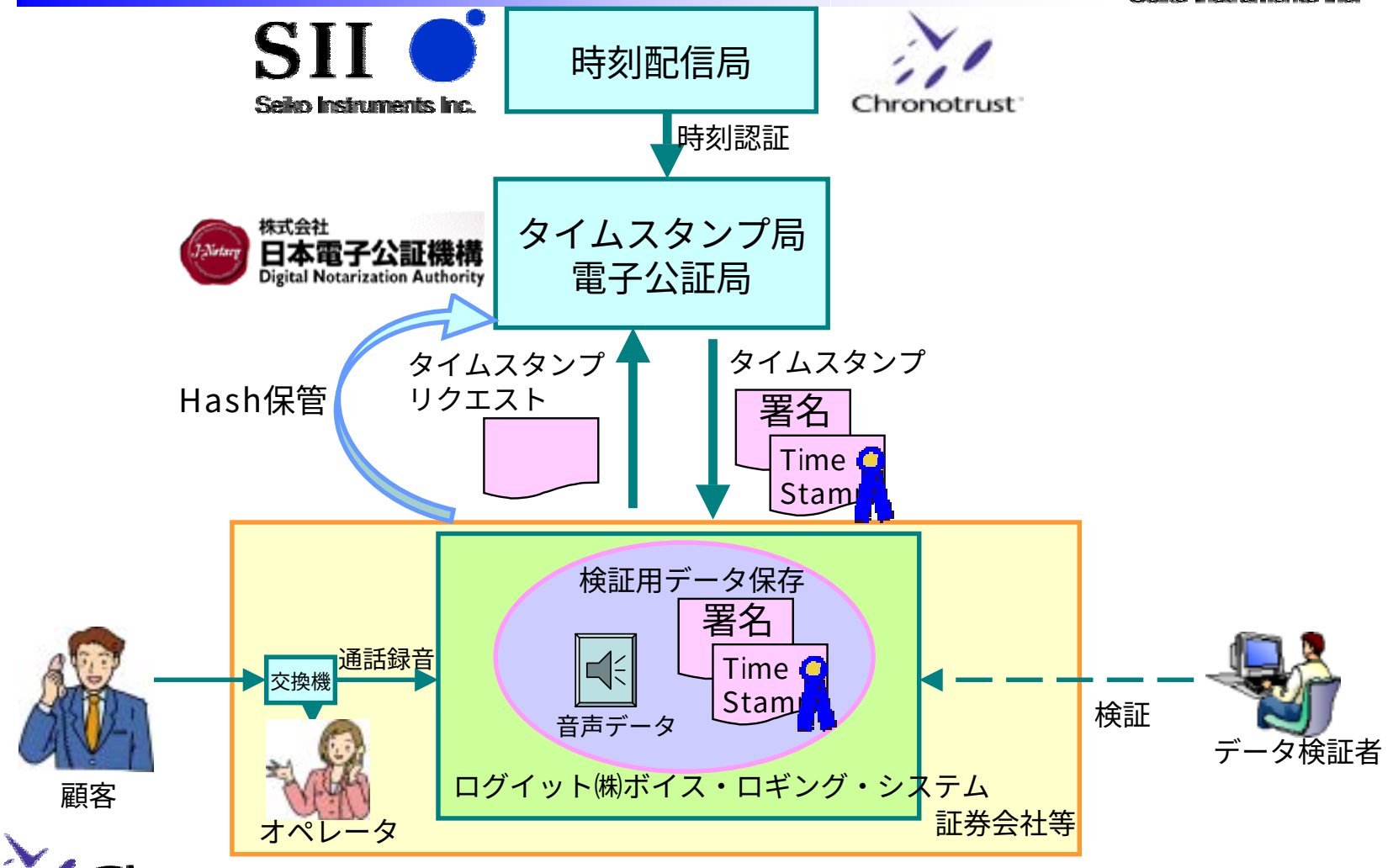


PDFファイルへのタイムスタンプ付与
（株）日本電子公証機構殿



事例；ボイスロギングシステム

ログイット（株）殿　，（株）日本電子公証機構殿



タイムスタンプ局の事例

SII Seiko Instruments Inc.

- 電子認証基盤サービス
  - デジタル署名
  - 証明書発行
- 業界向けアプリケーションサービス
  - 建設EDI
- 医療システム
  - 電子カルテ
  - 電子レセプト
- 電子公証サービス
  - タイムスタンプサービス

Chronotrust

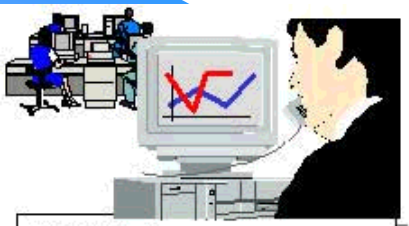
■応用例

出典: 総務省　タイムビジネス研究会ホームページ
http://www.soumu.go.jp/joho_tsusin/policyreports/chousa/time/index.html

SII Seiko Instruments Inc.

特許申請
・発明の日時を証明

電子入札
・電子政府における電子入札等の公平性を確保



証券取引
・取引日時の公平性を保証

ネットゲーム
・ネット利用の対戦等で
より多彩なゲームが実現

ネットオークション
・オークションにおける公平性の確保

電子カルテ
・医療機関におけるカルテ・レセプト等の日付正当性を保証

通信販売
・電子商取引における、信頼性の向上

Chronotrust™

E-mail:ni_info@sii.co.jp
Homepage:www.sii.co.jp/ni/tss/