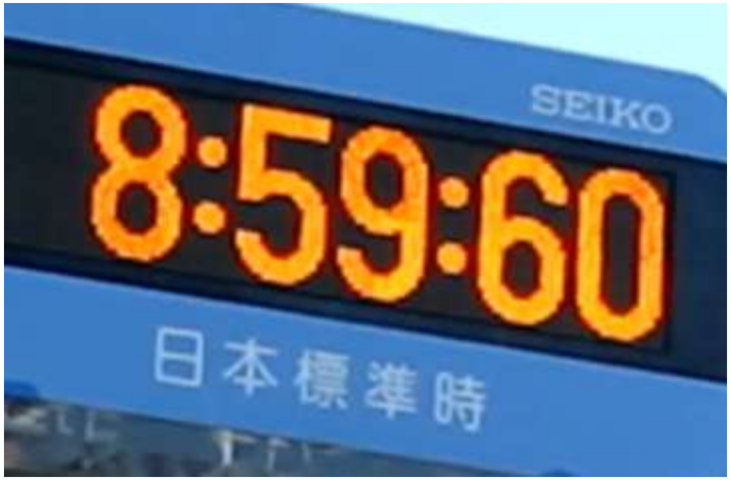
ITU/BIPM workshop

The Leap Second's Effect on Society



Sep 19th, 2013

Japan Data Communications Association

Time **B**usiness **F**orum

Steering Committee Chair Koichi Shibata

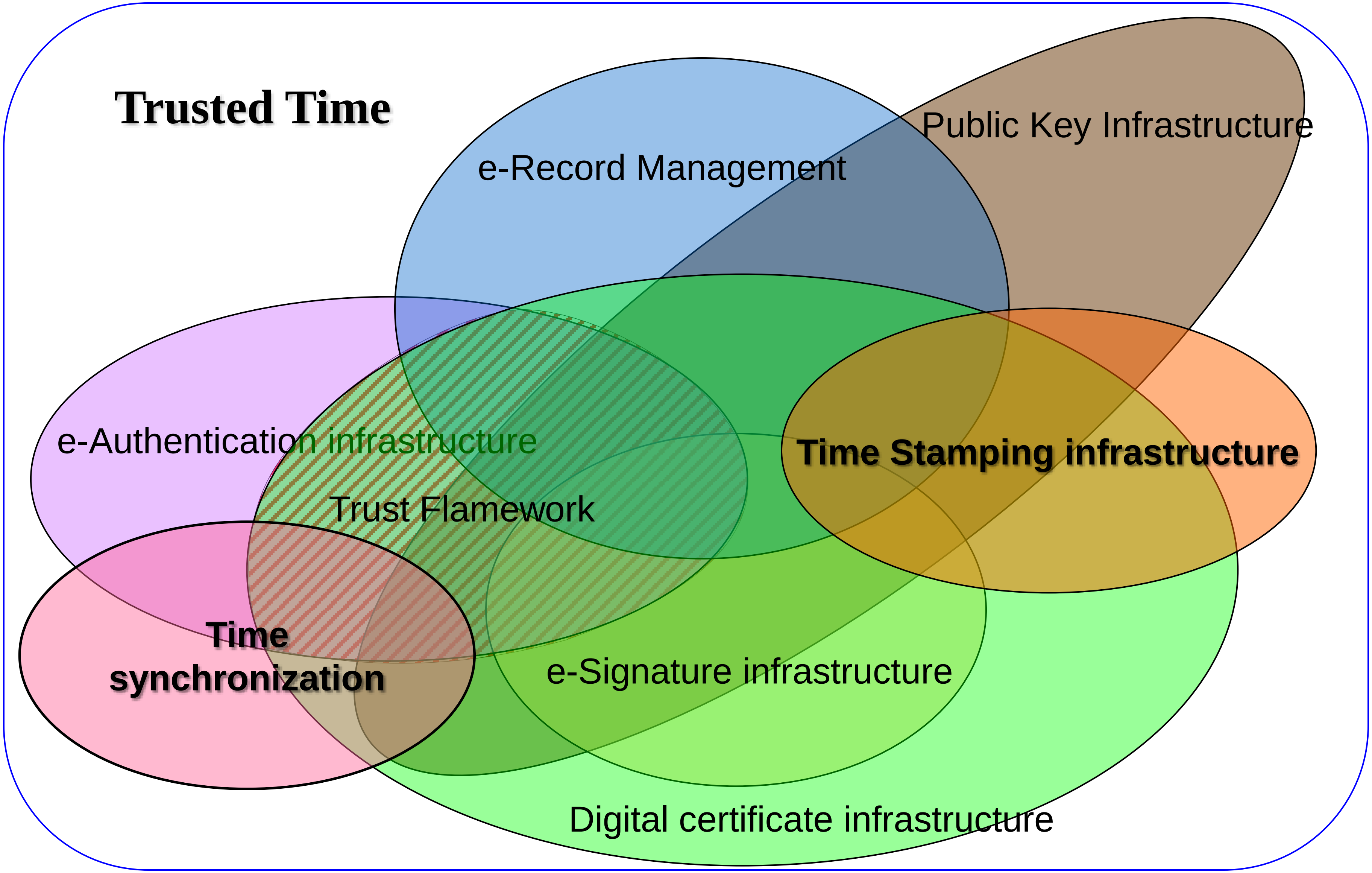
AGENDA

- The importance of TrustedTime to the ICT
- Japan's Time Business
- Accidents caused by the "Leap Second" in Japan
- The "Leap Second" in Time Business
- Review

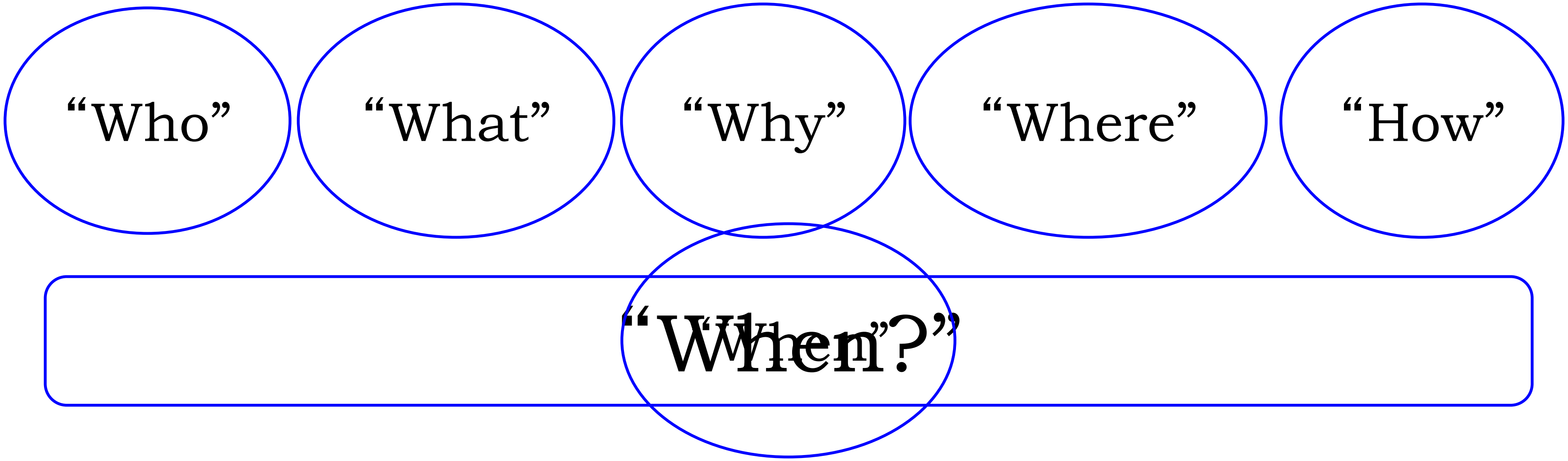
With "Time Business", your information will be protected

~ Trustworthy Information is Essential ~

Scope：ICT infrastructure for secure information society


Trusted Time
e-Record Management
Public Key Infrastructure
e-Authentication infrastructure
Time Stamping infrastructure
Trust Flamework
Time synchronization
e-Signature infrastructure
Digital certificate infrastructure

Information = the past phenomenon



Can’t share unless be there

We must Record it!

Civilization of Info Recording ⇒ Writing, Printing, Microphone, Camera

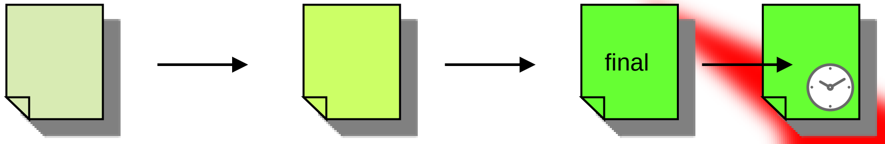
Is it Correct?

Culture of Info Management ⇒ Signatures, Stamps, Seals,
Archives, Memorandum, Contracts

The **Risks** and **Fixes** to Info Management

As Time Flows

Create Register Update Verify Finalize Store Use Discard



Fraud

Aging

Error

Tampering

Decay/Destruction

Loss of Legibility

Leakage/Misplacement

Searching Difficulties

Accidental Deletes

Explosive Increase in Information
Involvement of Stakeholders
Absence of Authors
Secondary, Tertiary use
Is it all accurate?

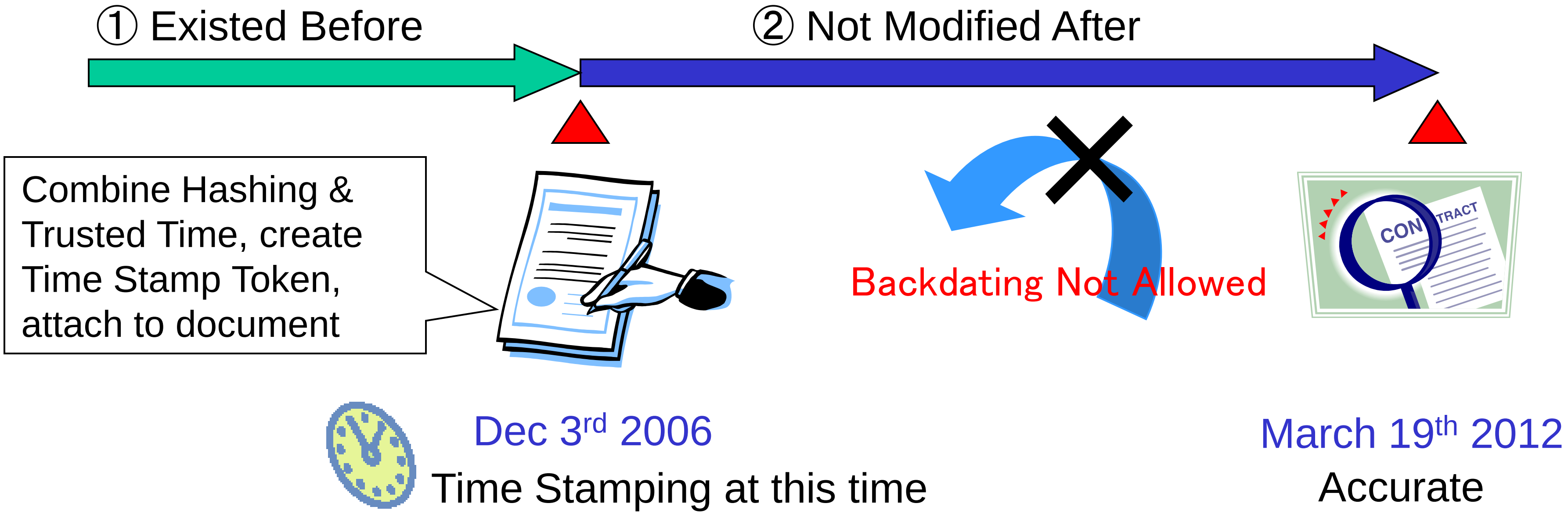
Coat information with the universal measure, Trusted Time
= Time Stamping

Time Stamp: Digital can Prove the "When"

Verifies that an digital document…

① Has existed before the stamped time

② Has not been modified after the stamped time



① Existed Before

② Not Modified After

Combine Hashing & Trusted Time, create Time Stamp Token, attach to document

Backdating Not Allowed

Dec 3rd 2006

Time Stamping at this time

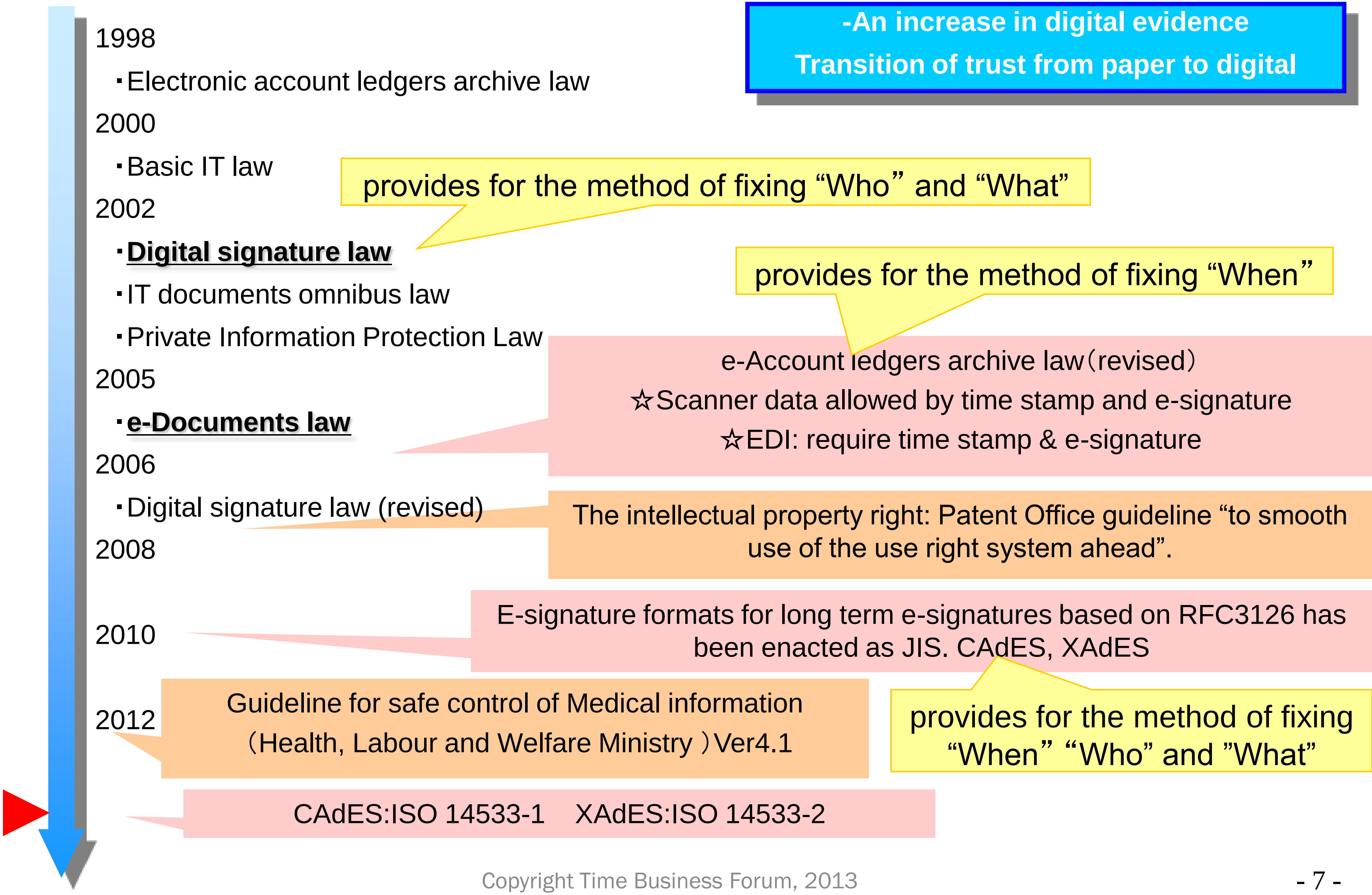
March 19th 2012

Accurate

Time Stamping protects the integrity of digital documents using the trustworthy resource, Trusted Time

Market Trend in Japan

-An increase in digital evidence
Transition of trust from paper to digital



1998

- Electronic account ledgers archive law

2000

- Basic IT law

2002

- **Digital signature law**
- IT documents omnibus law
- Private Information Protection Law

2005

- **e-Documents law**

2006

- Digital signature law (revised)

2008

2010

2012

provides for the method of fixing “Who” and “What”

provides for the method of fixing “When”

e-Account ledgers archive law（revised）
☆Scanner data allowed by time stamp and e-signature
☆EDI: require time stamp & e-signature

The intellectual property right: Patent Office guideline “to smooth use of the use right system ahead”.

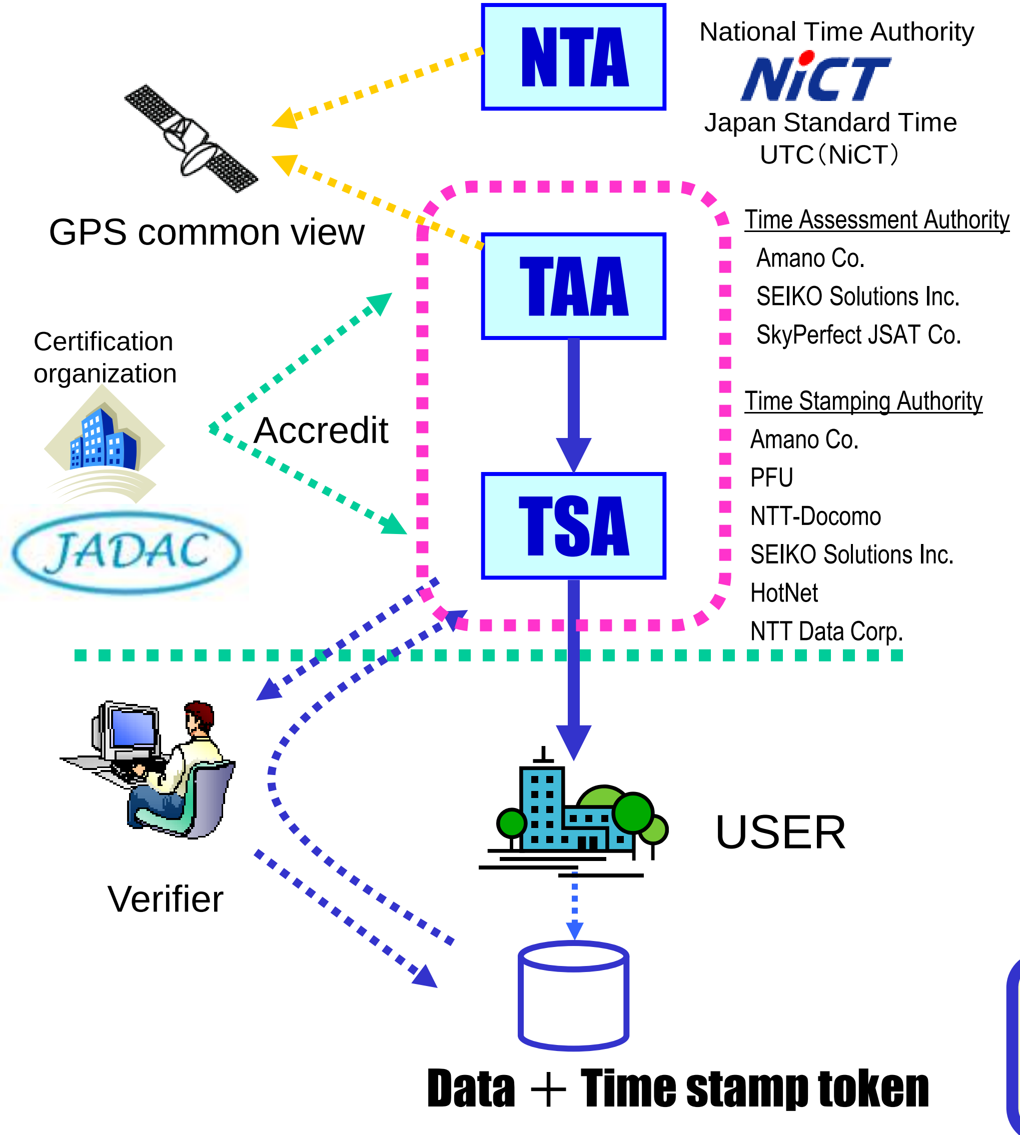
E-signature formats for long term e-signatures based on RFC3126 has been enacted as JIS. CAdES, XAdES

Guideline for safe control of Medical information
（Health, Labour and Welfare Ministry ）Ver4.1

provides for the method of fixing “When” “Who” and ”What”

CAdES:ISO 14533-1　XAdES:ISO 14533-2

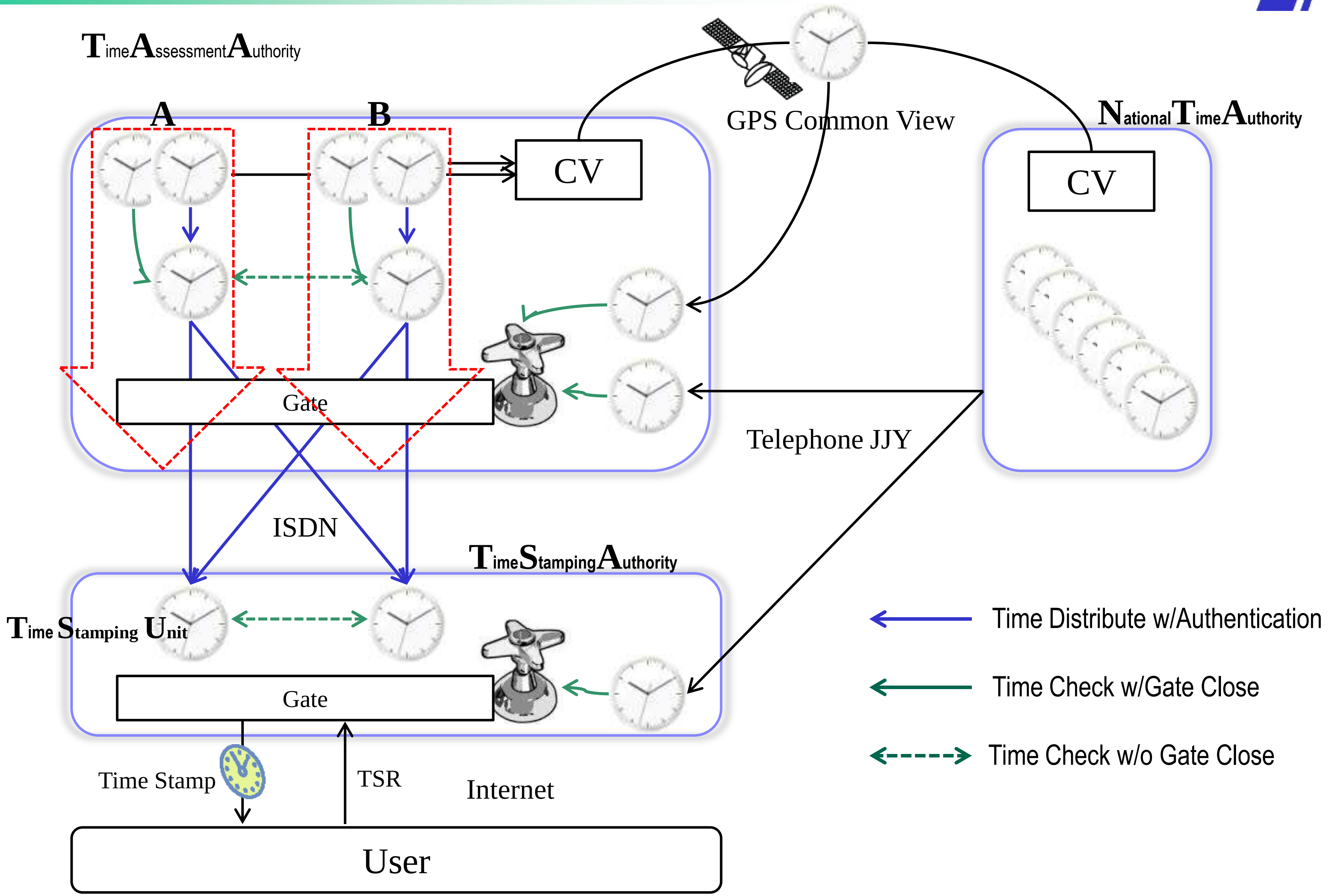
Accreditation Program for Time Stamping Services



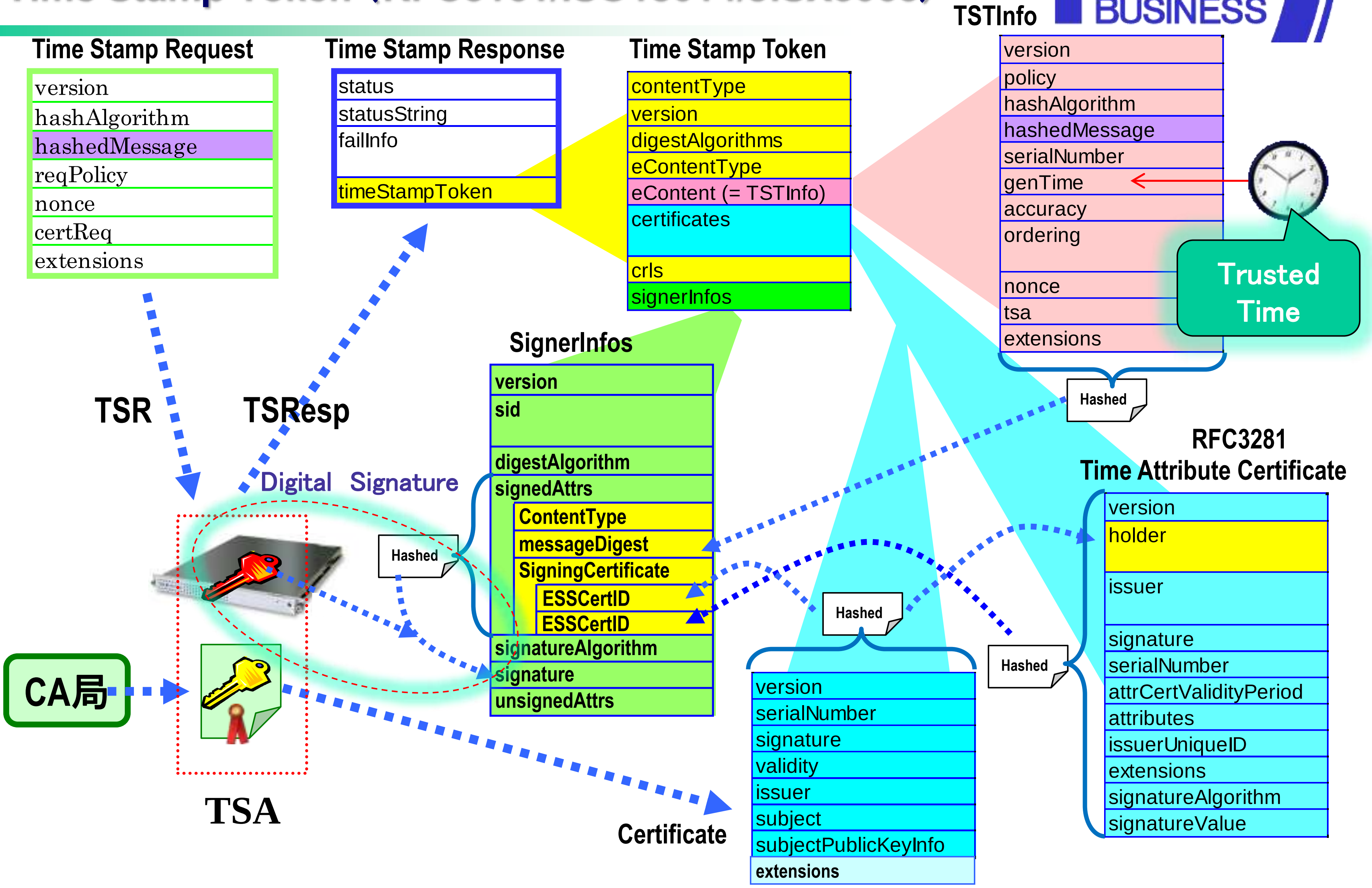
February 2005, the Nippon Information Communications Association (NIC) established the voluntary accreditation program for time-stamping services. The program is based on the guideline of “time business” issued by MIC (Ministry of Internal Affairs and Communications) in November 2004, and is to approve if the services of a TA (Time Authority) and a TSA (Time Stamping Authority) meet the required criterions of the program. The criterions cover five fields, (1) technology, (2) operation, (3) facilities, (4) network security and (5) information obligations. Requirements for accreditation are : (1) Accredited TA & TSA must have business footholds and facilities & equipments for time business within JAPAN. (2) Accreditation is valid for 2 years and accredited TA & TSA must submit an application to NIC for the renewal.
＜http://www.dekyo.or.jp/tb/english/index.html＞

To enhance levels of time-stamping service provision and to contribute to the technical infrastructure of IT societies.

Trusted Time Traceability



Time Stamp Token（RFC3161/ISO18014/JISX5063）



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

Trusted Time

Hashed

SignerInfos

- version
- sid
- digestAlgorithm
- signedAttrs
  - ContentType
  - messageDigest
  - SigningCertificate
    - ESSCertID
    - ESSCertID
- signatureAlgorithm
- signature
- unsignedAttrs

TSR

TSResp

Digital Signature

Hashed

CA局

TSA

Hashed

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

Standardize the traceability of trusted time

Trusted time source for Time Stamping Authority : **TAA (Time Assessment Authority)** has been defined as the international recommendation.

ITU-R

Trusted time source for Time Stamp Authority

In April 2010, recommendation from Japan has been authorized as ITU-R **TF.1876** by ITU-R (International Telecommunication Union Radiocommunication Sector) SG7(Business Science).

JIS

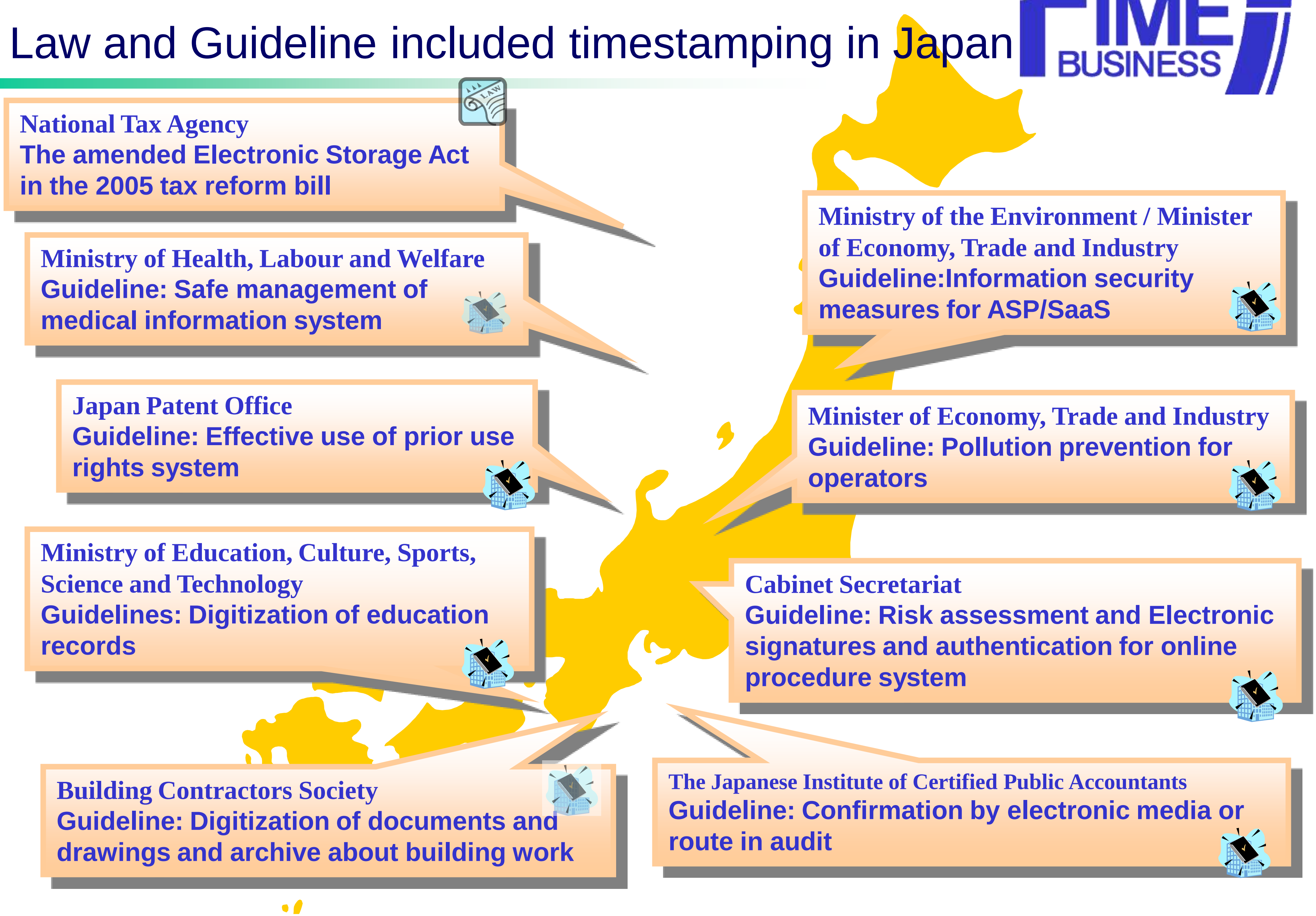
ISO/IEC
18014-4

JIS X 5094:2011…Technical requirements for TAA to certify TSA clocks of UTC-traceability

ISO/IEC 18014-4 …Information technology - Security techniques - Time-stamping services - Traceability of time sources

- STATUS: Under development
- Stage:40.00 (2013-06-13)
- TC/SC : JTC 1/SC 27 WG2

Law and Guideline included timestamping in Japan



National Tax Agency
The amended Electronic Storage Act in the 2005 tax reform bill

Ministry of Health, Labour and Welfare
Guideline: Safe management of medical information system

Japan Patent Office
Guideline: Effective use of prior use rights system

Ministry of Education, Culture, Sports, Science and Technology
Guidelines: Digitization of education records

Building Contractors Society
Guideline: Digitization of documents and drawings and archive about building work

Ministry of the Environment / Minister of Economy, Trade and Industry
Guideline:Information security measures for ASP/SaaS

Minister of Economy, Trade and Industry
Guideline: Pollution prevention for operators

Cabinet Secretariat
Guideline: Risk assessment and Electronic signatures and authentication for online procedure system

The Japanese Institute of Certified Public Accountants
Guideline: Confirmation by electronic media or route in audit

Case Summary

Time Stamps are used in various fields in Japan.

Users' needs are‥‥

non-Repudiation

Right of Prior Use

Accountability

Misappropriated application

Electronic document by scanner

Paperless

Record Authenticity

Lawsuit Aversion

Example of Timestamping Application (1)

>> Transaction Doc, e-commerce

User name	Purpose	Target data	Format	Commencing Year
JTB Corp.	Speedup operation and Operational efficiency	Written estimate	PDF	2005～
Murata Manufacturing Co., Ltd.	Speedup operation and Operational efficiency	From for foreign trade	PDF	2011～
AICHI Bank	Compliance for e-Doc law	Image Scanned….Request for account transfer, various notification, identification	PDF	2011～
NISHIJIN Hospital	Compliance for e-Doc law	Image Scanned….Receipt, agreement, written consent	PDF	2012～

>> e-contract

Username	Purpose	Target data	Format	Commencing Year
Tohoku Information Systems Company, Inc.	Stamp duty reduction	Contract	PDF	2007～
NS Solutions Corp.	Electric contract service	Contract	PDF	2010～
Toho Co., Ltd	Operational efficiency	Contract for movie contents	PDF	2011～
Edison Co., Ltd	Web Service of management for industrial wastewater	Contract for outsourcing of industrial wastewater treatment	PDF	2011～
Communication Plan	Electric contract service	Contract	PDF	2012～

Example of Timestamping Application (2)

>> Medical Information

User Name	Purpose	Target data	Format	Commencing Year
Teikyo Univ. Hospital	Compliance for e-Doc Law	Medical record(Scanned images….surgical consent form, letter of introduction)	PDF	2009～
Osaka Univ. Hospital		Medical Record (Scanned images)	PDF, XDW	2010～
Toyama Univ. Hospital		Medical Record	PDF	2011～
Japanese Red Cross Shizuoka Hospital		Medical Record (Letter of introduction medical certificate)	PDF	2011～
Social Institute Chukyo Hospital		Consent form, Letter of introduction, Interview sheet, Medical certificate	PDF, XDW	2011～
Daido Hospital				
NISHIJIN Hospital		Scanned images(Receipt, agreement, written consent)	PDF	2012～
Keio Univ. Hospital		Letter of introduction, Medical certificate	TIFF	2012～
Takara pharmacy		Prescription, Dispensing record	JPEG	2012～
St. Luke’s International Hospital		Letter of introduction, Medical certificate	PDF	2012～
Nagoya Memorial Hospital		Consent form, Letter of introduction, Interview sheet, Medical certificate	PDF, XDW	2012～
Takeda General Hospital			XDW	2012～

Example of Timestamping Application (3)

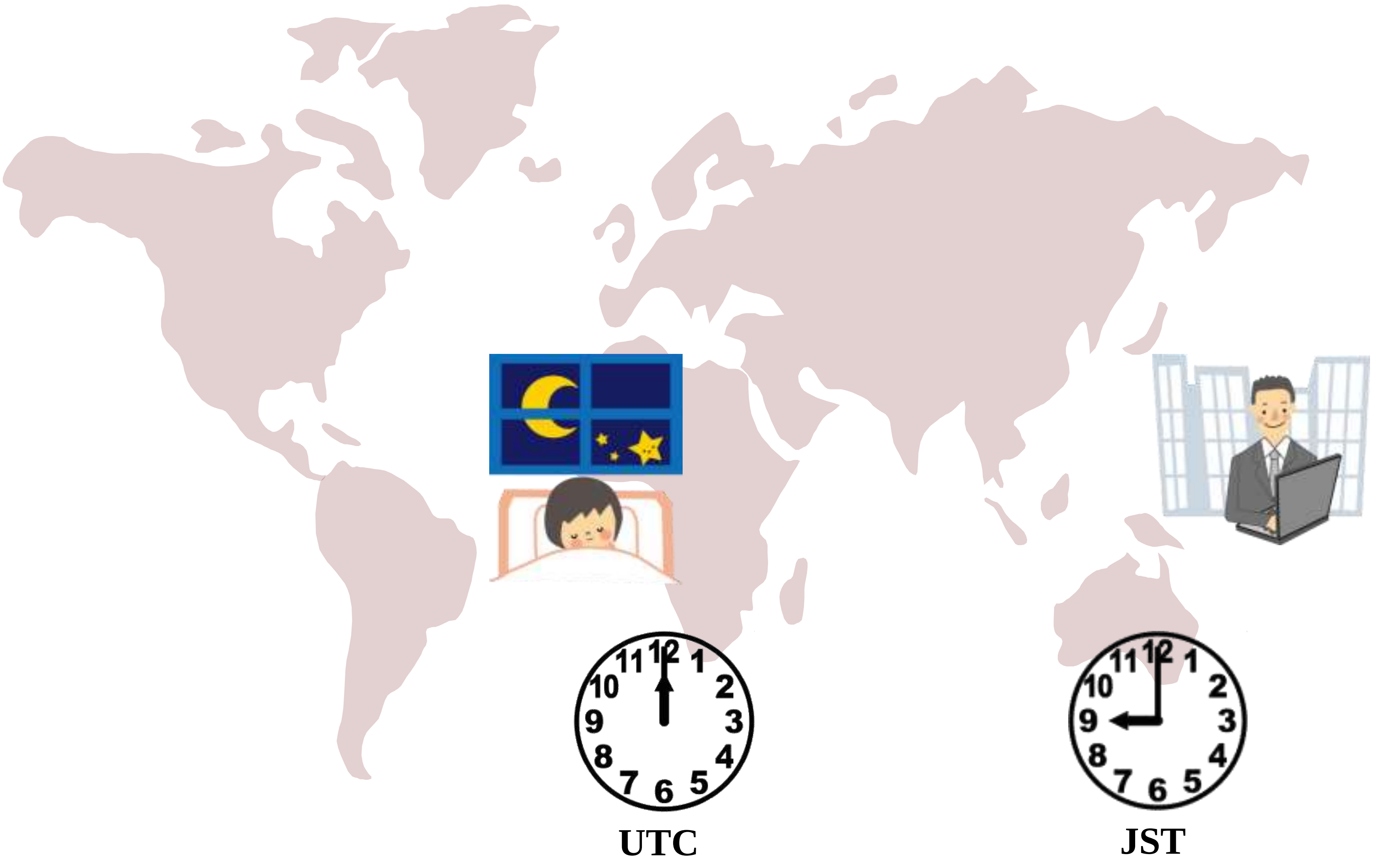
>> Intellectual Property

User name	Purpose	Target data	Format	Commencing Year
National Printing Bureau.	Responsibility of giving trusted information as national authority	Official Gazette	PDF, XDW	2003～
Japan Data Communications Association	Ensure the integrity	Privacy Mark certification	PDF	2007～
Ministry of Finance Japan	Ensure the integrity	IOU for Fiscal Loan Fund, Certificate for money on deposit	XML	2009～
UBE-NITTO KASEI Co.,Ltd	Prior use right, Rights reserved in joint study or development	Document and report and experiment data generated in study or development	PDF	2006～
Nippon Soda Co., Ltd			PDF	2006～
OMRON Corp.			PDF	2009～
NIPRO Corp.			PDF	2010～

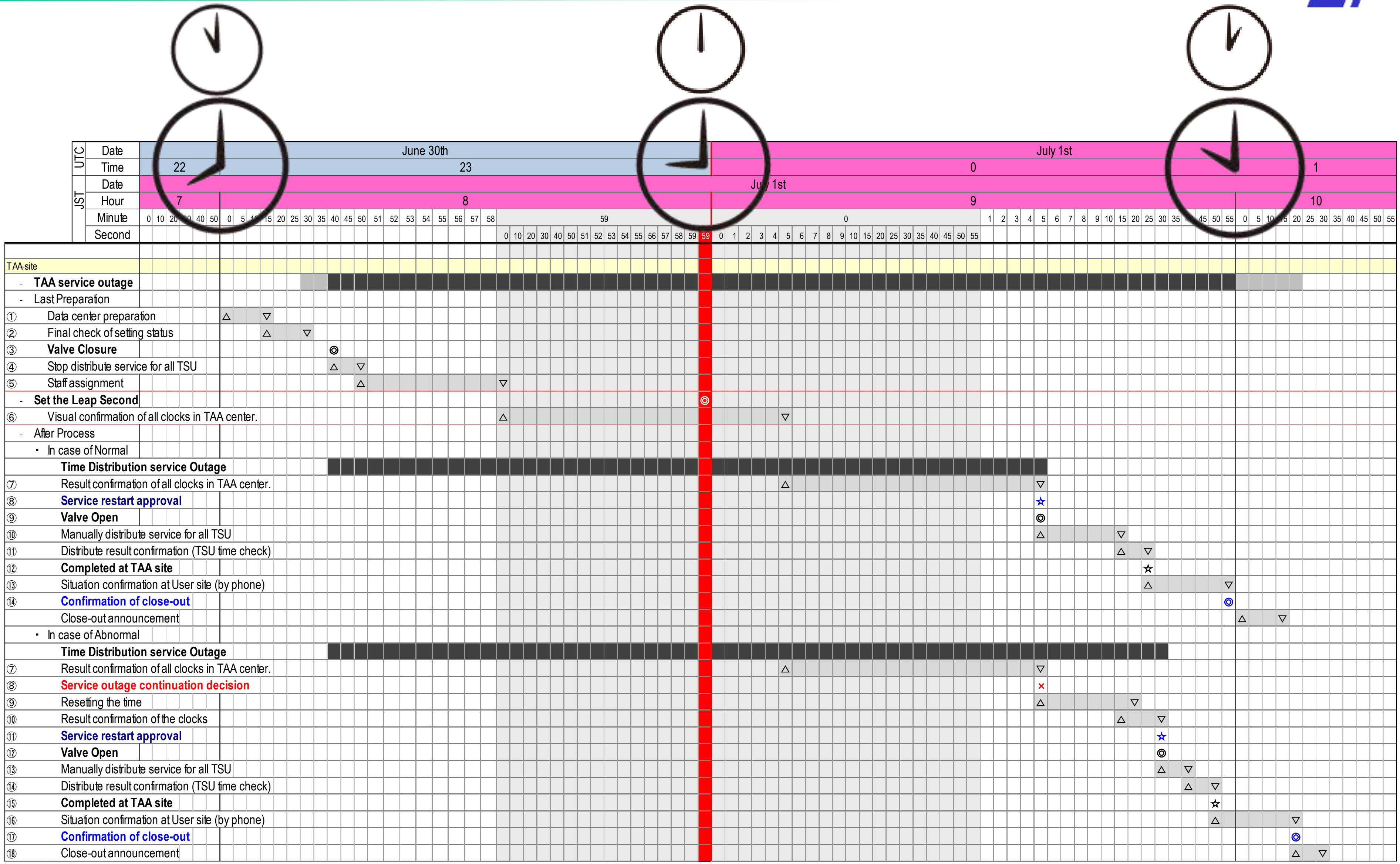
Incidents in Japan

- TAA
  - trouble after leap second pushed
    - Jan 2nd 2006: More Leap second pushed at 24hour after
    - July 1st 2012: Former i-Rig device‘s output time was 1second late
- Cybouz: Groupware Software Vender
  - trouble before leap second
    - A bug in the centeral server‘s OS prevented access to Cybouz.com
    - June 30th 2012 09:25am ～ 10:41pm
- Mixi: SNS site
  - trouble 4hours
    - July 1st 2012
    - Server slowed down, users could not login, or sometimes lost response.

Japan’s Timezone Situation



TimeSchedule on July 1st 2012



TAA-site

- TAA service outage
- Last Preparation

① Data center preparation
② Final check of setting status
③ **Valve Closure**
④ Stop distribute service for all TSU
⑤ Staff assignment

- **Set the Leap Second**

⑥ Visual confirmation of all clocks in TAA center.

- After Process
  - In case of Normal

Time Distribution service Outage
⑦ Result confirmation of all clocks in TAA center.
⑧ **Service restart approval**
⑨ **Valve Open**
⑩ Manually distribute service for all TSU
⑪ Distribute result confirmation (TSU time check)
⑫ **Completed at TAA site**
⑬ Situation confirmation at User site (by phone)
⑭ **Confirmation of close-out**
Close-out announcement

- In case of Abnormal

Time Distribution service Outage
⑦ Result confirmation of all clocks in TAA center.
⑧ **Service outage continuation decision**
⑨ Resetting the time
⑩ Result confirmation of the clocks
⑪ **Service restart approval**
⑫ **Valve Open**
⑬ Manually distribute service for all TSU
⑭ Distribute result confirmation (TSU time check)
⑮ **Completed at TAA site**
⑯ Situation confirmation at User site (by phone)
⑰ **Confirmation of close-out**
⑱ Close-out announcement

Review

- Time is a crucial measurement to the ICT Society.
- Irregular actions done with time causes confusion to the ICT Society.
- It is thought to be impossible to adjust every time label in the system by ±1 second at once.
- The side-effects to this problem cannot be predicted.
- Should we not prevent the possibility of confusion happening as much as we can?

Thank you.