IHE :
ATNA
(Audit Trial and Node Authentication)
CT
(Consistent Time)

IHE-J ベンダワークショップ2010

（２０１０・０５・２７）

接続検証委員会

IHE での PHI（健康情報）保護

- User Identity（ユーザ識別）→ PWP, EUA
- User Authentication（ユーザ認証） → EUA, XUA
- Node Authentication（ノード認証）→ ATNA
- Security Audit Trails（監査証跡） → ATNA
- Data Integrity Controls（データ完全性）→ CT, ATNA TLS option
- Data Confidentiality（データ機密性）→ ATNA TLS option
- Access Controls（アクセス制御）→ BPPC、IHE技術白書

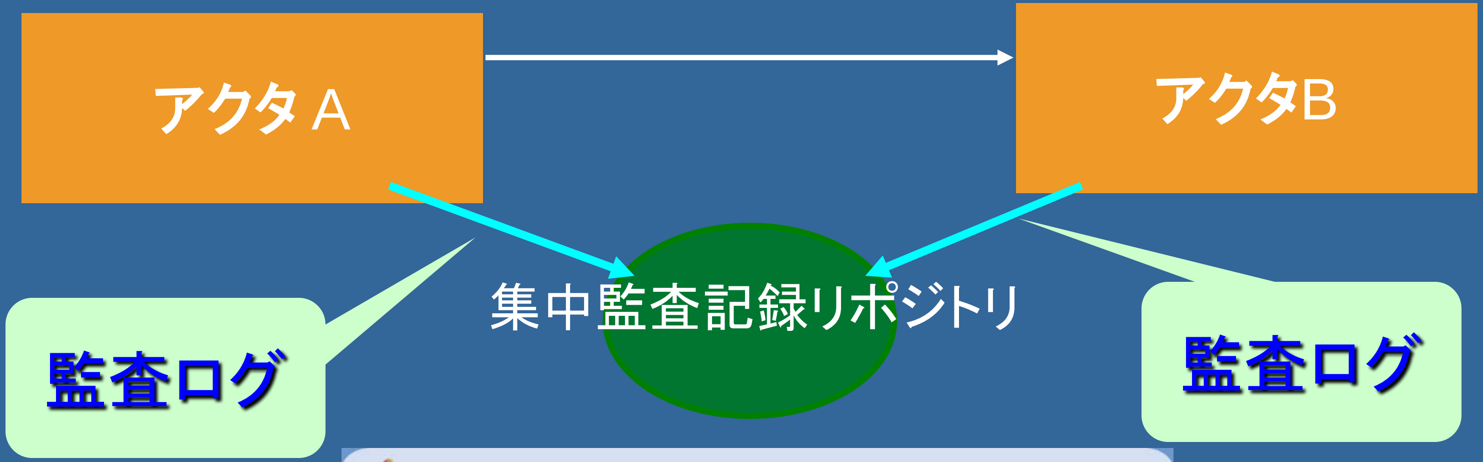
ATNA＝Audit Trail + Node Authentication
監査証跡　ノード認証

ATNAの目的

- **ユーザへの説明責任（監査証跡）**
  - 組織のセキュリティ責任者による監査に基づく、安全性に関する領域内のポリシーの遵守の評価
  - 保護すべきPHI（健康情報）データに対する不適切な生成、アクセス、修正、削除の発見
- **ノード認証によるアクセス制御**
  - ネットワークアクセスをノード（システムや機器）間に制限し、各ノードに対して認可されたユーザにアクセスを制限する方法でのアクセス制御
- **集中監査記録リポジトリ**
  - 全てのIHEアクタから、監査記録リポジトリへ監査記録を送る。監査記録リポジトリは監査記録を保存する
- **PHIデータの完全性**
  - PHI情報（生成、変更、削除、所在）の有効期間とその過程におけるデータの完全性の追跡

ATNA:AT(監査証跡)

- 監査は常に選択したアクセス制御と認証方法とは独立していなければならない
- 記録は単に個々のIHEアクタに相当する個々のコンポーネントだけではなく、全体のプロセスに対するイベントの記述を捕まえなければならない。
- 監査記録メッセージは、集中監査記録リポジトリへログ採取が行われる。仕組みは、Reliable Syslog Cooked Profile(RFC-3195)に使い方を規定している。BSD Syslog(RFC-3164)も使用可能だが制約がある。



ATNA：ATで監査すべきイベント（1）

トリガーイベント	詳細
Actor-start-stop	Startup and shutdown of any actor. Applies to all actors. Is distinct from hardware powerup and shutdown.
Audit-log-used	The audit trail repository has been accessed or modified by something other than the arrival of audit trail messages
Begin-storing-instances	Begin storing SOP Instances for a study. This may be a mix of instances.
Health-service-event	Health services scheduled and performed within an instance or episode of care. This includes scheduling, initiation, updates or amendments, performing or completing the act, and cancellation. See note below.
Instances-deleted	SOP Instances are deleted from a specific study. One event covers all instances deleted for the particular study.
Instances-stored	Instances for a particular study have been stored on this system. One event covers all instances stored for the particular study. .
Medication	Medication orders and administration within an instance or episode of care. This includes initial order, dispensing, delivery, and cancellation.
Mobile-machine-event	Mobile machine joins or leaves secure domain.
Node-authentication-failure	A secure node authentication failure has occurred during TLS negotiation, e.g. invalid certificate.

ATNA:ATで監査すべきイベント（２）

トリガーイベント	詳細
Order-record-event	Order record created, accessed, modified or deleted. Involved actors: Order Placer. This includes initial order, updates or amendments, delivery, completion, and cancellation. See note below.
Patient-care-assignment	Staffing or participant assignment actions relevant to the assignment of healthcare professionals, caregivers attending physician, residents, medical students, consultants, etc. to a patient It also includes change in assigned role or authorization, e.g., relative to healthcare status change, and de-assignment
Patient-care-episode	Specific patient care episodes or problems that occur within an instance of care. This includes initial assignment, updates or amendments, resolution, completion, and cancellation. See note below
Patient-care-protocol	Patient association with a care protocol. This includes initial assignment, scheduling, updates or amendments, completion, and cancellation. See note below.
Patient-record-event	Patient record created, modified, or accessed.
PHI-export	Any export of PHI on media, either removable physical media such as CD-ROM or electronic transfer of files such as email. Any printing activity, paper or film, local or remote, that prints PHI
PHI-import	Any import of PHI on media, either removable physical media such as CD-ROM or electronic transfers of files such as email.

ATNA:ATで監査すべきイベント（3）

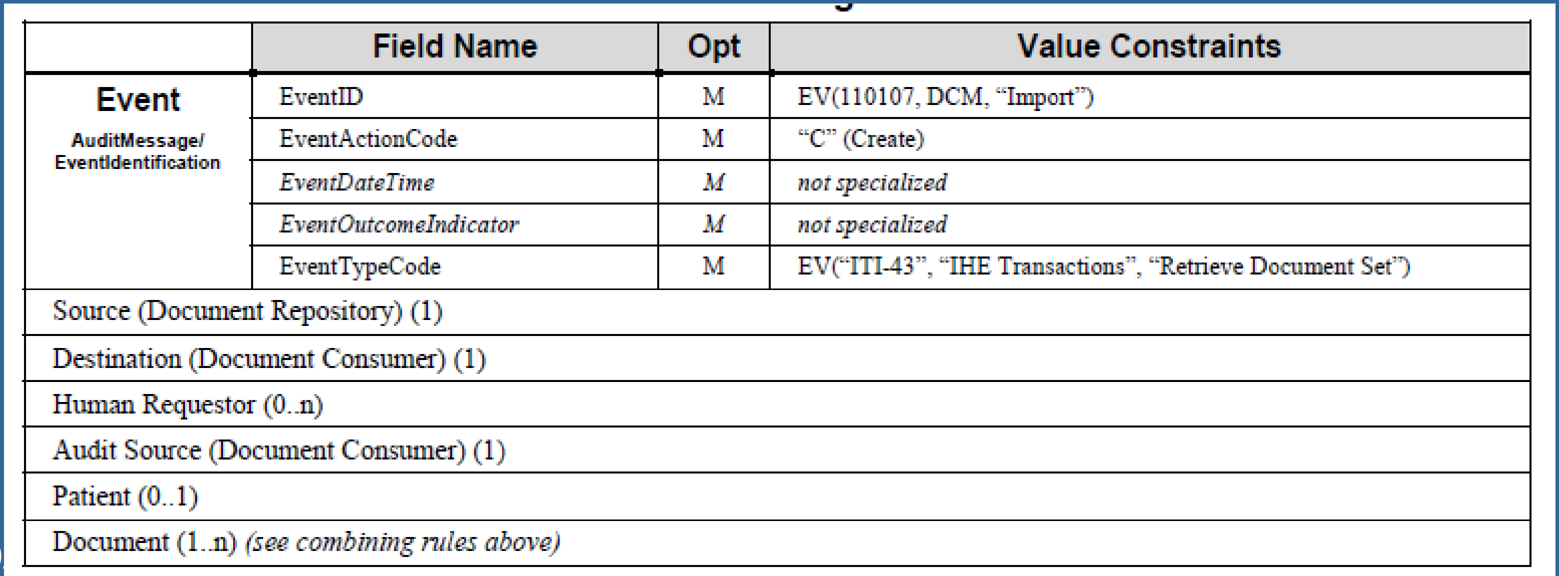
トリガーイベント	詳細
Procedure-record-event	Procedure record created, modified, accessed or deleted
Query-information	A query has been received, either as part of an IHE transaction, or as part other products functions. For example: 1) Modality Worklist Query 2) Instance or Image Availability Query 3) PIX, PDQ, or XDS Query
Security Alert	Security Administrative actions create, modify, delete, query, and display the following: 1. Configuration and other changes, e.g., software updates that affect any software that processes protected information. Hardware changes may also be reported in this event. 2. Security attributes and auditable events for the application functions used for patient management, clinical processes, registry of business objects and methods **(e.g. WSDL, UDDI)**, program creation and maintenance, etc. 3. Security domains according to various organizational categories such as entity-wide, institutional, departmental, etc. 4. Security categories or groupings for functions and data such as patient management, nursing, clinical, etc.

ATNA:ATで監査すべきイベント（4）

トリガーイベント	詳細
Security Alert **（前頁のつづき）**	5. The allowable access permissions associated with functions and data, such as create, read, update, delete, and execution of specific functional units or object access or manipulation methods. 6. Security roles according to various task-grouping categories such as security administration, admissions desk, nurses, physicians, clinical specialists, etc. It also includes the association of permissions with roles for role-based access control. 7. User accounts. This includes assigning or changing password or other authentication data. It also includes the association of roles with users for role-based access control, or permissions with users for user-based access control. 8. Unauthorized user attempt to use security administration functions. 9. Audit enabling and disabling. 10. User authentication revocation. 11. Emergency Mode Access (aka Break-Glass) Security administration events should always be audited.
User Authentication	This message describes the event of a user attempting to log on or log off, whether successful or not. No Participant Objects are needed for this message.
Study-object-event	Study is created, modified, accessed, or deleted. This reports on addition of new instances to existing studies as well as creation of new studies.
Study-used	SOP Instances from a specific study are created, modified or accessed. One event covers all instances used for the particular study.

ATNA：監査ログ（１）

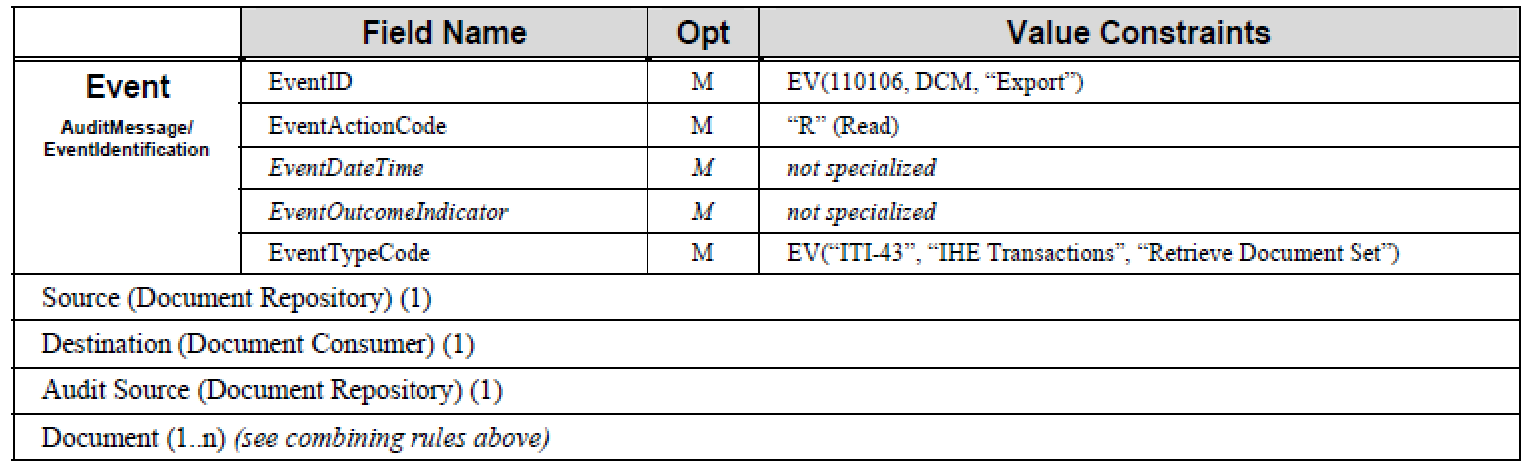
- 各トランザクションごとに、監査ログの項目に対する設定値の決め方が決まっている。
- 例：Retrieve Document Set [ITI-43]の場合
  - ドキュメントコンシューマ側
    - 監査イベント：PHI-Import
    - ドキュメントコンシューマが出力する監査ログ（一部）



	Field Name	Opt	Value Constraints
Event **AuditMessage/** **EventIdentification**	EventID	M	EV(110107, DCM, “Import”)
	EventActionCode	M	“C” (Create)
	EventDateTime	*M*	*not specialized*
	EventOutcomeIndicator	*M*	*not specialized*
	EventTypeCode	M	EV(“ITI-43”, “IHE Transactions”, “Retrieve Document Set”)
Source (Document Repository) (1)			
Destination (Document Consumer) (1)			
Human Requestor (0..n)			
Audit Source (Document Consumer) (1)			
Patient (0..1)			
Document (1..n) *(see combining rules above)*			

ATNA：監査ログ（２）

- 例：Retrieve Document Set [ITI-43]の場合（前頁の続き）
  - ドキュメントリポジトリ
    - 監査イベント：PHI-Export
    - ドキュメントリポジトリが出力する監査ログ（一部）



	Field Name	Opt	Value Constraints
Event AuditMessage/ EventIdentification	EventID	M	EV(110106, DCM, “Export”)
	EventActionCode	M	“R” (Read)
	EventDateTime	*M*	*not specialized*
	EventOutcomeIndicator	*M*	*not specialized*
	EventTypeCode	M	EV(“ITI-43”, “IHE Transactions”, “Retrieve Document Set”)
Source (Document Repository) (1)			
Destination (Document Consumer) (1)			
Audit Source (Document Repository) (1)			
Document (1..n) *(see combining rules above)*			

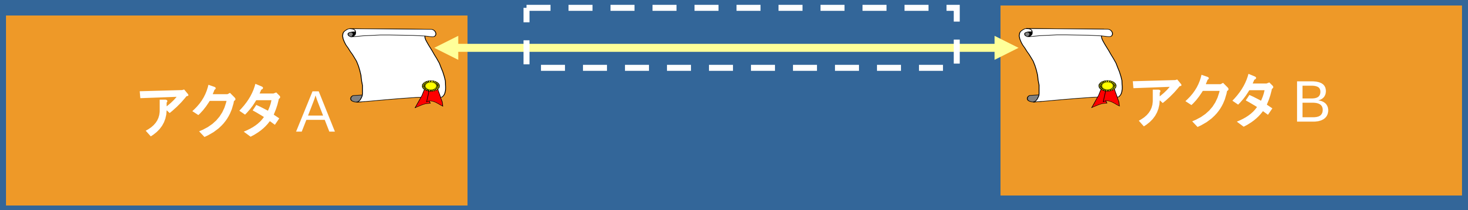
  - 監査ログの全項目とそれに対する設定値の決め方はITI-TF-2bの3.43.6.1.1、3.43.6.1.2にある。（ここではほんの一部を出しただけです）

ATNA：NA（ノード認証）

- 各ノードの接続に対して、双方向の証明書ベースのノード認証を要求する。
- DICOM,HL7,HTMLの各プロトコルは全て証明書ベースの決まった認証機構を持っている。
- ユーザではなく、ノード（システムや機器）を認証している。

（ユーザの認証はEUA、XUAで定義。ATNAと連携して使用できる）

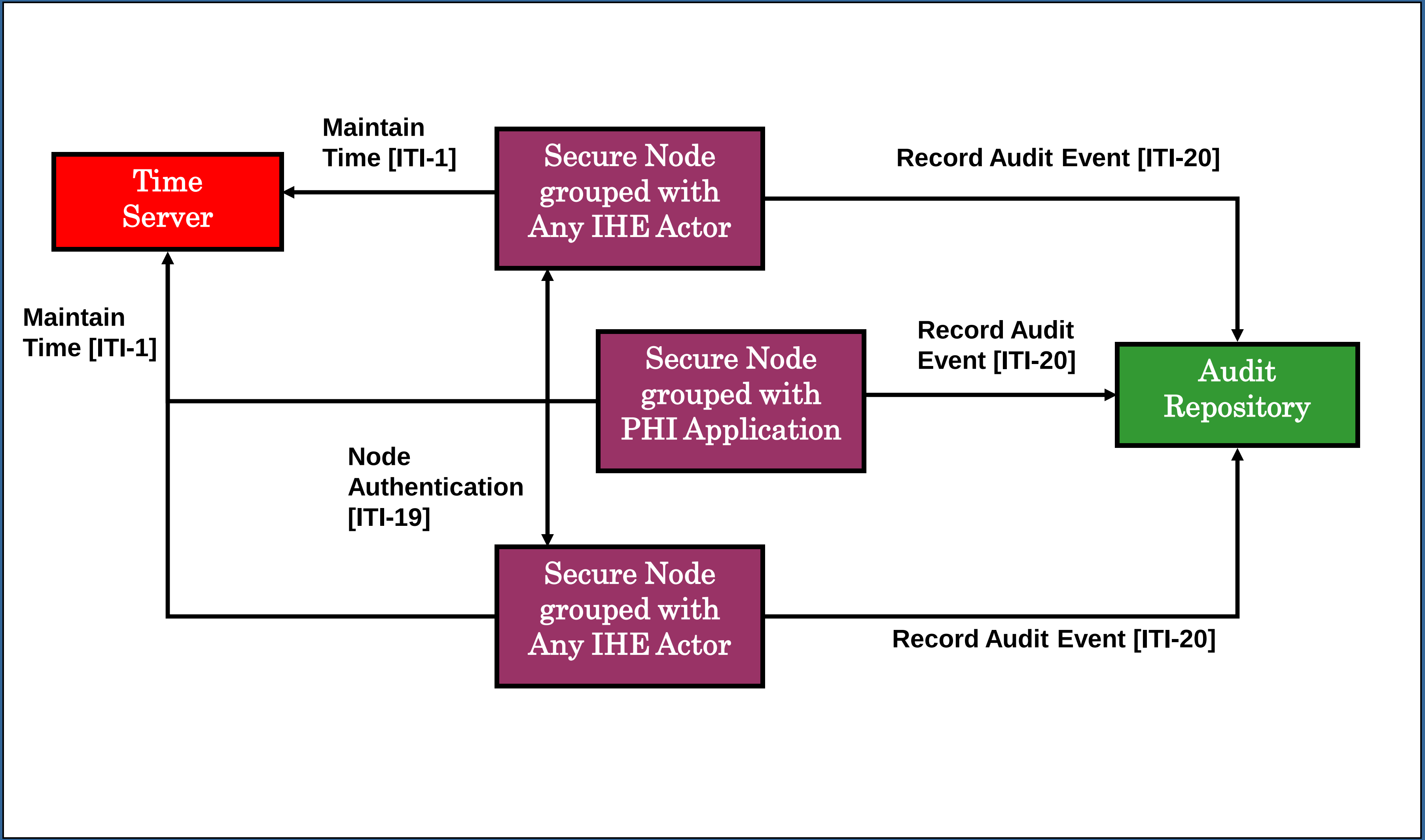
- 双方向のノード認証ができない機器の接続は禁止されるか、PHIアクセスを防ぐようにする。



ATNA：NA（ノード認証）

- **利用している規格**
  - ノードの識別及びキーとして、RSAキーをベースとしたX.509形式証明書を使用する
  - DICOM、HL7：TLSプロトコルを使用
    - TLS_RSA_WITH_NULL_SHA
    - TLS_RSA_WITH_AES_128_CBC_SHA（ATNA暗号化オプション）
  - HTTP：DICOMやHL7の場合と同じ方法でTLS接続を確立する。
    - HTTP通信では、暗号化オプションが必要となる
  - Webサービス：WS-I Basic Security Profile Version 1.1.
    - http://www.ws-i.org/Profiles/BasicSecurityProfile-1.1.html
    - TLS_RSA_WITH_NULL_SHAの不使用を勧告

ATNA: アクタとトランザクション



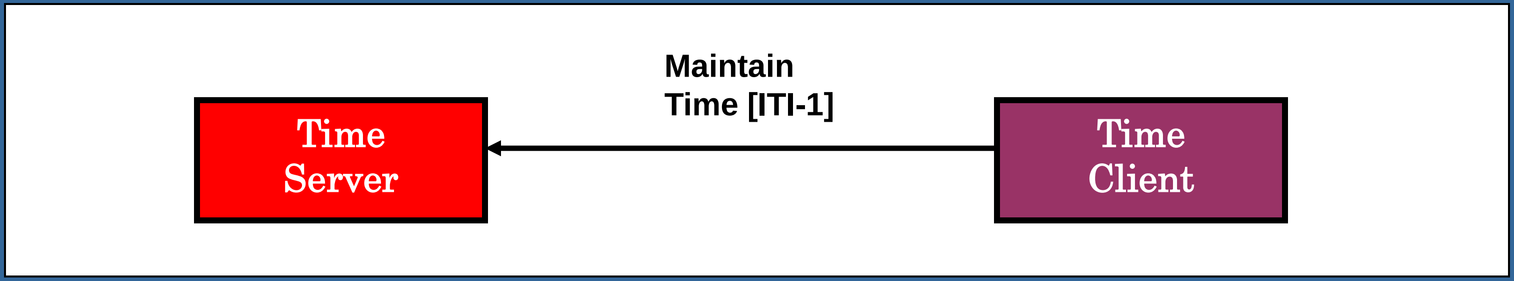
ATNA：アクタとトランザクション

アクタ	トランザクション	オプショナリティ	TFでの説明箇所
<any PHI application grouped with a Secure Node Actor>	Record Audit Event [ITI-20]	R	ITI-TF-2a 3.20
<any IHE actor grouped with a Secure Node Actor>	Record Audit Event [ITI-20]	R	ITI-TF-2a 3.20
Audit Record Repository	Record Audit Event [ITI-20]	R	ITI-TF-2a 3.20
Secure Node	Authenticate Node [ITI-19]	R	ITI-TF-2a 3.19
	Maintain Time [ITI-1]	R	ITI-TF-2a 3.1
Secure Application	Authenticate Node [ITI-19]	O	ITI-TF-2a 3.19
	Maintain Time [ITI-1]	O	ITI-TF-2a 3.1
	Record Audit Event [ITI-20]	O	ITI-TF-2a 3.20

CT (Consistent Time)

- 時刻の同期には、ネットワークタイムプロトコル（NTP）V3（RFC1305）を使用
- アクタは手動による構成調節をサポートしなければならない
- 要求される精度：1秒
- オプショナルとして、セキュアNTPを使用できる
- ATNA,EUA,XUAでは、CTが必要になる

CT： アクタとトランザクション



アクタ	トランザクション	オプショナリティ	TFでの説明箇所
Time Server	Maintain Time [ITI-1]	R	ITI-TF-2a 3.1
Time Client	Maintain Time [ITI-1]	R	ITI-TF-2a 3.1

Thank You.