
# TENeT 概要書

Ver. 1.0

TEF950-S000-01.00.00/ja

2005 年 3 月

T-Engine フォーラム

 

# 目次



 

# 1. はじめに

## 1.1. 本書の目的

本書は，権利価値取引フレームワークを実現する TENeT（Trusted Environment with Networking eTRON）仕様について，仕様の目的と特徴を説明する資料である．なお TENeT 仕様は，その用途をモバイル環境における権利価値流通に特定した“権利価値流通用 eTRON 仕様”である．

## 1.2. TENeT の概要

近年の権利価値技術の進展や社会基盤としてのネットワークの普及により，貨幣やチケットなどの権利価値を電子的に発行・利用するサービスが提供されつつある．現在は扱える電子的な権利価値の種類は限られているが，権利価値流通サービスの現社会への浸透とともに，将来的には身分証明書などの個人情報の配布や，オークションなどによる利用者間の権利価値の取引市場が出現することなどが想定される．権利価値取引フレームワークである TENeT を用いた権利価値取引環境のイメージを図 1 に示す．

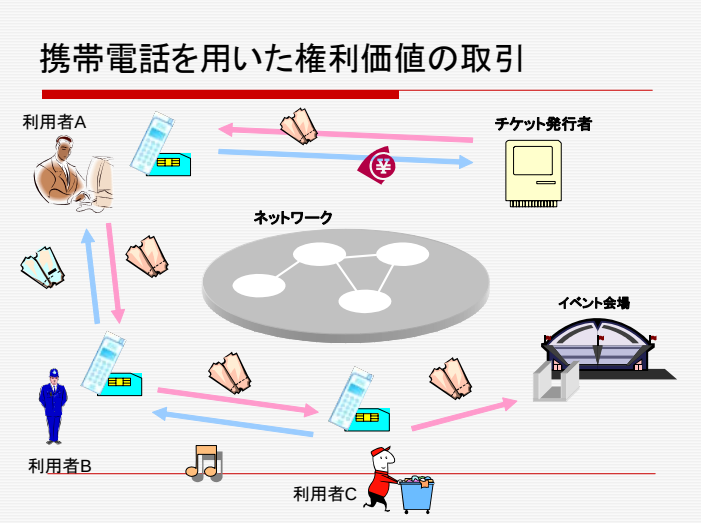


図 1 TENeT イメージ

しかし，権利価値流通サービスが浸透すると共に，権利価値の改竄や偽造など，不正な利用者や第 3 者による攻撃の機会も増加する．そのため，権利価値流通基盤の展開には，権利価値を不正な操作から守る技術が必須となる．

また，利用者が安全に権利価値を流通や取引させるためには，公平な取引ができることを保証することが重要となる．すなわち，たとえば利用者間で権利価値を売買する場合において，権利価値を持ち逃げされるなどの不正な行動を防がなくてはならない．特に携帯電話などの無線環境での利用を考慮すると，ネットワークの遮断や携帯電話の充電切れなどにより取引が途中で中断される可能性もあることから，取引の公平性の確保は非常に重要な要素となる．

TENeT は，この取引の公平性の問題を解決した，特にモバイル環境において安全な権利価値の取引を実現するためのフレームワークである．

 

### 1.3. TENeT 仕様の規定範囲

TENeT 仕様では，権利価値取引を実現する IC カードおよびアプリケーションプログラムの相互運用性を実現するために，以下の各種仕様を規定する．

- TENeT 権利価値取引 API 仕様
  アプリケーションプログラムから IC カードの権利価値を管理・流通させるための API
- TENeT メッセージング API 仕様
  アプリケーションプログラムから e2TP メッセージを送受するための API
- $e^2$TP (Extended eTRON Transfer Protocol) メッセージ仕様
  $e^2$TP メッセージのメッセージフォーマットおよび ISO7816-4 APDU へのマッピング方式
- TENeT メッセージ仕様
  TENeT 仕様 IC カードが備えるべき $e^2$TP メッセージのメッセージセット

### 1.4. 本書の構成

本書の構成は以下のとおりである．2 章で TENeT 仕様の具体的な利用シーンを示し，3 章で利用シーンを実現するための要求条件を列挙する．4 章で TENeT 仕様の概要を示す．

 

# 2. TENeT の利用シーン

## 2.1. 利用シーン

モバイル環境を「携帯電話に代表される，ネットワークに接続可能な個人所有の携帯端末を常時持ち歩いている環境」と定義する．モバイル環境における権利価値流通には，IC カードなどの耐タンパ装置のみを携帯する権利価値流通と比較して，次のような特徴がある．

- 携帯端末のネットワーク機能を利用して他の利用者と権利価値のやり取りが可能
- 携帯端末のユーザインタフェースを利用して，所有している耐タンパ装置内の権利価値の制御が可能

上記の特徴から，モバイル環境における権利価値流通では表 1 に示す利用シーンが考えられる．

表 1　モバイル環境における権利価値流通の利用シーン

| 利用シーン | 詳細 |
|---|---|
| **権利価値の購入** | 改札の券売機など特定の場所で購入していた定期券やチケットの購入，電子マネーのチャージなどが携帯端末のネットワーク機能を利用していつでもどこでも行える． |
| **権利価値の譲渡** | 他の利用者に対して権利価値を譲渡する．従来は譲渡用に専用機器やネットワークに接続した PC 等が必要であったが，携帯端末のネットワーク機能を利用することで他の機器を必要なく権利価値を譲渡できる． |
| **権利価値の交換** | 他の利用者と権利価値を交換する．上記と同様に携帯端末のネットワーク機能を用いて，互いに権利価値を譲渡することで交換できる．交換が安全に実行できれば取引サービス全般に適用できる．たとえばネットワーク上のフリーマーケットなどの自由な取引サービスが実現できる． |
| **権利価値の使用** | 改札やゲート等では従来の近接型非接触 IC カードと同じく，携帯端末を翳すだけで権利価値を利用できる．たとえば，携帯端末のローカル通信機能を利用して自動車のインテリジェンスキーのように持っているだけで自動的に権利価値を使用してドアを開くなどの応用も可能である． |

TENeT 仕様は，2.1 節の利用シーンを実現するために，携帯端末上のアプリケーションが利用する API と，IC カードの入出力メッセージを規定している．3 章以降で権利価値流通への要求条件と，その要求条件を満たす TENeT の機能について述べる．

 

## 3. 権利価値流通への要求条件

本章では，2 章の利用シーンを実現するための権利価値流通への要求条件について整理する．

利用シーンを可能にするような権利価値は，RFC3506 において Electronic Voucher と呼ばれ，その満たすべき要件が定義されている[RFC3506]．RFC3506 およびその技術的背景である文献[TKHF00][TKHF01]によれば，権利価値が満たすべき要求条件は、図 2 のように整理される．

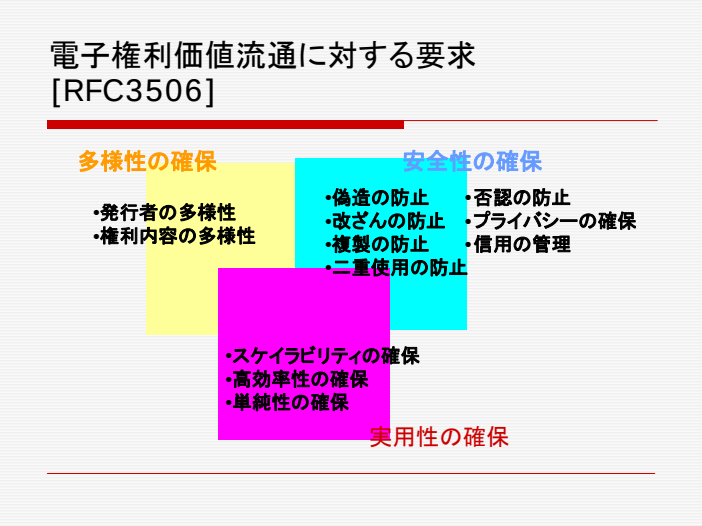


図 2　RFC の要求条件

図 2 の各要求条件について，以下に説明を加える．記述内容は，RFC3506 の記述に[TKHF00][TKHF01]を参考にしながら適宜補足を加えたものである．

**多様性の確保**

- 発行者の多様性　(Different Issuers)

いわゆる電子現金/電子貨幣システムと異なり，権利価値は個人から企業，政府まで様々な主体により生成され得る．これらの様々な主体が権利価値を生成・発行する手段を提供しなければならない．

- 権利内容の多様性　(Various types of vouchers)

電子現金/貨幣システムは単なる通貨単位の差異のみを扱えれば十分であるのに対して，電子権利価値はチケットやクーポンなど多種多様な内容を扱えなければならない．

**安全性の確保**

- 偽造の防止　(Preventing forgery)

権利価値は，発行者のみによって生成されることを保証しなければならない．すなわち，権利価値には（発行者の多様性から）それぞれ発行者が規定されているが，他者を発行者とする権利価値を勝手に偽造することがあってはならない．

- 改竄の防止 (Preventing alteration)

権利価値は，流通の過程でその内容が変更されることがあってはならない．ただし，譲渡によってその所有者が変更されることは許される．権利価値の譲渡は，（譲渡元である）所有者のみが実行することができる．

 

- 複製の防止（Preventing reproduction）

権利価値は，流通の過程で複製されることがあってはならない；すなわち，ある権利価値はある時点においてたかだか一人の所有者によってのみ所有されていなければならない．

- 二重使用の防止（Preventing duplicate-redemption）

一旦消費された権利価値は，それ以後行使されることがあってはならない．また権利価値の行使は，その所有者のみが実行することができる．

- 否認の防止（Non-repudiation）

発行者が権利価値の発行の事実を否認することを許すべきではない．また，所有者が譲渡若しくは消費の事実を否認することも同様に防ぐべきである．

- プライバシーの確保（Ensuring privacy）

ある権利価値の，現在もしくは過去の所有者は，その権利価値を入手しようとするものから隠蔽されるべきである．

- 信用の管理（Trust manageability）

様々な種類の権利価値が流通する環境を想定する場合，利用者にとってある権利価値が「信用」できるかどうか（実際に価値があるものであるかどうか）を判断することは困難となってくる．そのため，権利価値が「信用」できるかどうかを判定するような機能が提供されるべきである．

**実用性の確保**

- スケイラビリティの確保　（Scalability）

全ての権利価値を一手に売買するような集中ブローカーや，全ての発行者や所有者を認証する認証局の存在は，仮定されるべきではない．これらのような一局集中的な組織に依存するシステムは極めて脆弱である；このような組織において障害が発生すると，システム全体が破綻することになる．

- 高効率性の確保　（Efficiency）

イベントチケットや交通機関の切符など，高い性能を要求する応用に対応できるようにするため，権利価値を実現するシステムを効率的に実装可能でなくてはならない．

- 単純性の確保　（Simplicity）

（権利価値流通システムのための標準仕様は）実装が単純なものであるべきである．単純性は実装コストを削減するのみならず，システム自体を理解し信用するためにも重要である．

RFC3506 から抽出した要求条件は，権利価値を「価値」を持った有価物として安全に発行し，流通させるために求められる条件である．しかし，実際には権利価値の流通は，単なる一方向の発行や譲渡だけではなく，2.1 節の利用シーンで述べたように「取引」の一環として行われることが多い．

一般の消費者や商店がこのような取引を安心して行うためには，取引における公平性（fairness）が担保されている必要がある．すなわち，利用者の観点から見ると，商品（としての権利価値；興業チケットなど）を受け取ることなしに，対価(としての権利価値；貨幣や商品券など）だけを奪われることを避けなければならない．また，逆に商店の観点からは対価を受けとることなしに商品を渡してしまうことを避けなければならない[THIF03]．この要求条件は，特に通信が遮断し易いモバイル環境の取引において重要なものである．

 

従って，2.1 節の利用シーンで述べた権利価値の安全な取引を実現するためには，以下の要求条件がさらに必要となる．

**公平性の確保**

それぞれの交換当事者は，対価として受領する対象の権利価値を受け取ることなく，譲渡する対象の権利価値を失うことがあってはならない．すなわち，交換の終了時において，受領する対象の権利価値，もしくは譲渡する対象の権利価値のいずれかを所有している状態でなければならない（取引終了時における公平性の確保）．また，交換は必ず有限時間内に終了しなければならない．

 

# 4. TENeT 仕様の概要

## 4.1. TENeT の特徴

TENeT は，権利価値を様々な環境，特にモバイル環境で安全に利用可能とするため，権利価値を IC カードや USIM などの耐タンパ装置に格納する．これを TENeT IC カードと呼ぶ．TENeT は，ネットワークを介して権利価値を安全かつ公平に流通・取引することを可能にするために，「公平な権利価値取引のための楽観的な交換プロトコル」の技術[THIF03]を採用している．これにより，サーバへの負荷集中を招くことなく，離れたところにある IC カード間で安全かつ公平に権利価値を取引することができる．

また TENeT は，上記の交換プロトコルのような IC カード間の分散処理をアプリケーションプログラムから容易に利用するために，IC カード間や IC カードとアプリケーションプログラム間で分散透過的にメッセージを送受するための機構を備えている．

これらの技術を採用することにより，TENeT はモバイル環境において，安心・安全な権利価値の流通や取引を行うための各種応用を容易に実現することを可能としている．

## 4.2. TENeT のアーキテクチャ

TENeT は，図 3 に示す各コンポーネントから構成される．それぞれのコンポーネントの概要を以下に述べる．

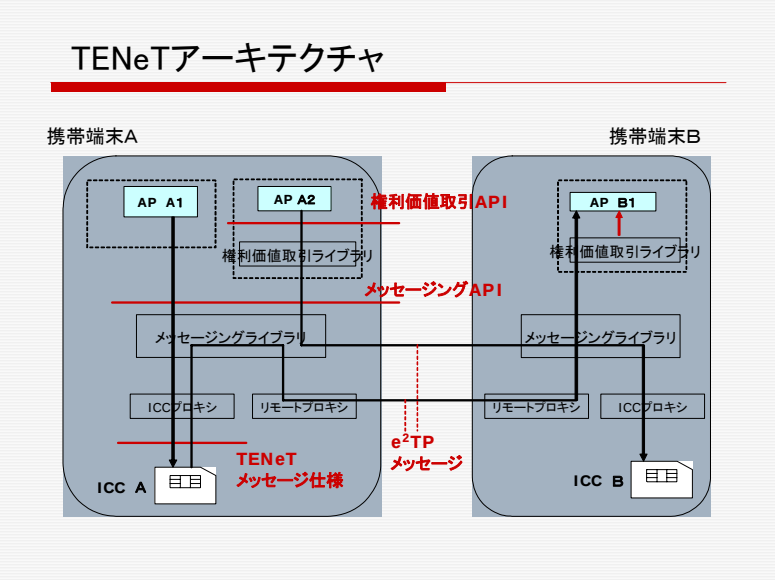


図 3　TENeT アーキテクチャ

## 4.3. 権利価値流通ライブラリ

権利価値流通ライブラリは，TENeT IC カードに格納された電子的な権利価値の操作や取引を行うための高レベルライブラリである．本ライブラリは，TENeT IC カードが提供する機能をアプリケーションプログラム（AP）に対して提供する．すなわち，TENeT 仕様を利用する一般的なアプリケーションの開発者は，IC カードとの間で授受される e2TP メッセージの構造や仕様などを意識することなく，本ライブラリが提供する API のみを用いて AP を開発することができる．

 

TENeT 仕様は，本ライブラリを利用するための API として権利価値取引 API 仕様を規定している．権利価値取引 API 仕様は Java 仕様として規定されている．

### 4.4. メッセージングライブラリ

メッセージングライブラリは，TENeT で用いられる通信メッセージである e2TP（Extended eTP）メッセージを，IC カードとの間や他の AP との間で送受するためのライブラリである．e2TP メッセージは，eTRON/16 仕様における eTP メッセージを拡張したメッセージである．

アプリケーションは e2TP メッセージを同期（送信メッセージに対する返答メッセージをブロック待ち受けする）もしくは非同期（メッセージの送信後，返答メッセージを待たずに処理を続行する）のいずれかにより送受信することができる．非同期メッセージ送信を行った場合，他のイベントドリブンシステム（GUI フレームワークなど）と同様に，受信メッセージはあらかじめ登録したリスナにより取得することとなる．

本ライブラリにより送信される e2TP メッセージの宛先として，TENeT 名前空間の eTRON ID を持つ任意の AP や IC カード，サーバなどを指定することができる．宛先がリモートであった場合には，メッセージは本ライブラリにより自動的にルーティングされ，ネットワークを介して適切な宛先に送信される．そのため，AP は宛先がローカルであるかリモートであるかを意識する必要はない．ただし，セキュリティ上の理由により，IC カードに対する一部のメッセージは，リモートから送信された場合は無効となる．リモート送信時に無効になるメッセージの種別については，TENeT IC カード仕様により定義されている．

本ライブラリにおいて，各 AP の eTRON ID は IC カードの eTRON ID を用いて自動的に生成および取得される．この値は送受信の窓口となるオブジェクトに格納され，メッセージ送信時に自動的にメッセージの送信元 ID として付与される．そのため，各 AP は eTRON ID の具体的な割り当てについて意識する必要はない．

TENeT 仕様は，本ライブラリを利用するための API としてメッセージング API 仕様を規定している．メッセージング API 仕様は Java で規定されている．

### 4.5. TENeT IC カード

TENeT IC カードは，TENeT において権利価値を格納・管理する役割を持つ．利用者は TENeT IC カードを用いて，権利価値の取引や生成・削除などを行うことができる．TENeT IC カードは複数の「フォルダ」を持ち，生成もしくは取引により受領された権利価値はいずれかのフォルダに格納される．また TENeT IC カードは利用者認証機能を有し，アクセス主体が権利価値に対して不正な操作を実行することを防止する．

以下に，TENeT IC カードが提供する機能を示す．

**認証機能**

- IC カードに対する認証

  利用者に対して，IC カードの所有者であることの認証を行う．

- フォルダ／ファイルのアクセス制御

  フォルダとファイルにアクセス権限を設定する．

 

**権利価値管理機能**

- フォルダの生成・削除

  カード内にフォルダを作成、あるいはフォルダを削除する

- フォルダの一覧取得

  カード内のフォルダ情報の一覧を取得する

- 権利価値の生成

  カード内の指定フォルダに権利価値を生成する

- 権利価値の削除

  カード内の指定された権利価値を削除する

- （フォルダに格納された）権利価値の一覧取得

  カード内のフォルダにあるすべての権利価値の情報を取得する

**権利価値流通機能**

- 権利価値の譲渡・交換

  カード内の指定された権利価値の譲渡、または他の権利価値との交換を行う

- 中断した取引の復旧

  上記交換・譲渡処理が中断したときに，取引の復旧を行い，処理を終了させる

**運用系機能**

- IC カードの内容のバックアップ・復元

  フォルダサイズの変更時などにカード内の情報をすべて外部にバックアップする

 

## 参考文献

[RFC3506] K. Fujimura, and D. Eastlake. RFC3506: Requirements and Design for Voucher Trading System (VTS), IETF, Mar. 2003.

[TKHF00] M. Terada, H. Kuno, M. Hanadate, and K. Fujimura. Copy Prevention Scheme for Rights Trading Infrastructure, In Proc. 4th Working Conference on Smart Card Research and Advanced Applications (CARDIS), pp. 51-70, IFIP, Sep. 2000.

[TKHF01] 寺田, 久野, 花舘, 藤村. 電子流通基盤のための汎用的な原本性保証方式, 情処論, Vol. 42, No. 8, pp. 2017-2029, Aug. 2001.

[THIF03] 寺田, 花舘, 井口, 藤村. 公平な権利価値流通のための楽観的な交換プロトコル, CSS2003, Sep. 2003.

 