

eTRON: Entity and Economy TRON

越塚登^(*1, 3) 坂村健^(*2, 3)

^(*1) 東京大学 情報基盤センター
^(*2) 東京大学 大学院情報学環・学際情報学府
^(*3) YRP ユビキタスネットワークング研究所

本稿は、価値情報を流通させるためのセキュアな広域分散システムアーキテクチャ、Entity and Economy TRON (eTRON) について述べる。近年、ユビキタスコンピューティングに代表されるように、身の回りの様々なところにコンピュータが入り込むようになっている。それにもかかわらず、インターネットを経由したクラッキングや不正アクセスの被害が、年々増加している。eTRON は、こうしたコンピュータ化社会において、誰もが簡単に用いることのできるセキュリティー基盤を提供することを目的としている。本稿では、eTRON の基本的な考え方とアーキテクチャ、またキーコンポーネントである耐タンパー性を備えた eTRON チップに関する概要を述べる。

キーワード：セキュアコンピューティング、スマートカード、TRON

eTRON: Entity and Economy TRON

KOSHIZUKA, Noboru^(*1, 3) SAKAMURA, Ken^(*2,3)

^(*1) Information Technology Center, The University of Tokyo
^(*2) Interfaculty Initiative in Information Studies, The University of Tokyo
^(*3) YRP Ubiquitous Networking Laboratory

This article proposes a wide area distributed system architecture, called Entity and Economy TRON, eTRON, which incorporates with distributing value entities in secure. Recently, computers are embedded in various equipments for our everyday use, as seen in various ubiquitous computing scenarios. However, the number of cracking and illegal accesses for computers via the Internet is increasing in these years. For the improvement of this situation of computerized society, we are developing eTRON for providing an infrastructure for secure computing and networking that everyone can use it without difficulty. This article overviews basic concepts and architecture of eTRON, as well as its key components, eTRON chips, tamper resistant nodes in the eTRON architecture.

Keywords: Secure computing, Smart cards, TRON

1. はじめに

近年、情報技術の進展やネットワーク基盤の普及、更にユーザ層の拡大に伴い、社会のあらゆる場面をコンピュータ化することで、社会を効率化することが試みられている。政治、経済、文化といった人間社会のあらゆる活動を、コンピュータやコンピュータネットワークの上で実現しようとしている。

社会の重要な仕組みの一つに価値情報の流通がある。例えば、現代社会における重要な価値情報の一つに貨幣があり、その他にも各種証書、証券、チケットなどもある。これらが実効性を持つためには、流通時に改変されていないことが保証されなければならない。ところが、デジタル情報は、本来、情報品質を劣化させず、完璧に内容を複製したり変更できるため、価値情報を改変させないメカニズムは根本的に難しい。

デジタル情報に対する操作を制限し、不正を防ぐことは、ソフトウェアだけでは不十分であり、ハードウェアによる支援が不可欠である。現在は、一般的に耐タンパー性をもったハードウェアを使うことで、こうした支援を行っている。

トロンプロジェクトは、情報化社会で用いるデジタル化された価値情報を安全に格納し、流通させるために、耐タンパー性をもったチップを核技術とした、セキュアな分散広域システムアーキテクチャとして **eTRON (Entity and Economy TRON)** を構築している。

耐タンパー性をもったハードウェアはスマートカードとして実装されたものが多く、銀行のキャッシュカード、クレジットカード、公共交通システムのパスといった、貨幣価値に関連する情報を格納するデバイスとして広く使われている。スマートカードを使ったセキュアシステムは、応用を限定した専用システムとして構築され、アーキテクチャや全体システムの構成がクローズなものが多い。ところが、近年インターネットのようなオープンでかつ信頼性が必ずしも高くはない情報基盤が普及するに伴い、オープンな環境でも価値情報を安全に流通させたいという要求が高まっている。eTRON は、オープンな情報基盤上における価値情報の安全な流通の実現を目標としている。そこで用いられる耐タンパーデバイス

も、こうしたオープンな分散システムの一部として位置付けて設計している。

2. eTRON アーキテクチャ

eTRON は、耐タンパー性を有するハードウェアを活用し、インターネット等のオープンな通信基盤上で、価値情報を安全に流通させるための広域分散システムアーキテクチャである。eTRON アーキテクチャは特定の暗号・認証、ハッシュ等のアルゴリズムや、特定のアプリケーションに依存する枠組みではなく、価値情報の流通を実現するための、汎用的な枠組みである。

2.1 設計要件

eTRON アーキテクチャの設計要件は、次の通りである。

多目的

eTRON は、特定アプリケーション用のアーキテクチャではなく、価値情報を流通させるための汎用的なアーキテクチャである。この上で、複数の異なるアプリケーションを同時に扱う。

耐タンパーハードウェアの利用

各エンドユーザが持つ価値情報の格納デバイスには、耐タンパー性を有するハードウェアを用いる。携帯端末やカードに組込むための **eTRON チップ**、据え置き型の大容量ストレージとしての **eTRON ボックス**がある。

分散アーキテクチャ

eTRON では価値情報は、サーバに集約する方式ではなく、各ユーザが **eTRON チップ**や **eTRON ボックス**を使って、分散して保持する分散型アーキテクチャを利用できる。

価値情報の転々流通機能

eTRON では、**eTRON チップ**/**eTRON ボックス**に格納された価値情報をユーザ間でやり取りする際には、第三者サーバを介さずに当事者間で行うこと、つまり価値情報の**転々流通**、を可能にする。

Peer-to-Peer

eTRON チップ/eTRON ボックスは、Peer-to-peer で直接通信する。これにより、エンドノード間の通信経路途中での、暗号や署名のデコードが不要になるため、ノード間の通信基盤は単なる通信路を提供するだけになる。これによって、オープンな通信路上での価値情報の安全な流通が可能になる。

単一価値情報の分散分割格納機能

各ユーザが所有する耐タンパーデバイスに格納できない大きなサイズの情報を扱うために、eTRON では、単一価値情報を、複数のノードに分散して格納し、互いにリンクで接続することができる。各ユーザが所有する耐タンパーデバイスに格納できないような、大きい情報を扱う時に有用である。

PKI (Public Key Infrastructure)

eTRON アーキテクチャはノードが公開鍵暗号系の認証や暗号を扱うための PKI を含んでいる。

2.2 アーキテクチャの概要

eTRON は、価値情報を流通させるためのセキュアな広域分散システムである (図 1)。そのアーキテクチャは、以下の機能要素に分類できる。

eTRON コンテンツホルダ (Contents Holders)

eTRON コンテンツホルダ (以下 CH) は eTRON アーキテクチャが扱う価値情報を安全に格納する。以下で述べる eTRON サービスクライアント (以下、SCs) が CHs に格納されている情報をエンティティ転送プロトコル (Entity Transfer Protocol、以下、eTP) と呼ぶセッション層プロトコルにより安全に操作する。CHs は、実装方法に応じて、IC カード型の eTRON カード、携帯端末に埋め込むための eTRON チップ、据え置き型で多くの情報を格納できる eTRON ボックスなどがある。

eTRON サービスクライアント (Service Clients)

eTRON サービスクライアント (以下、SCs) は CHs に格納された価値情報を操作する応用シ

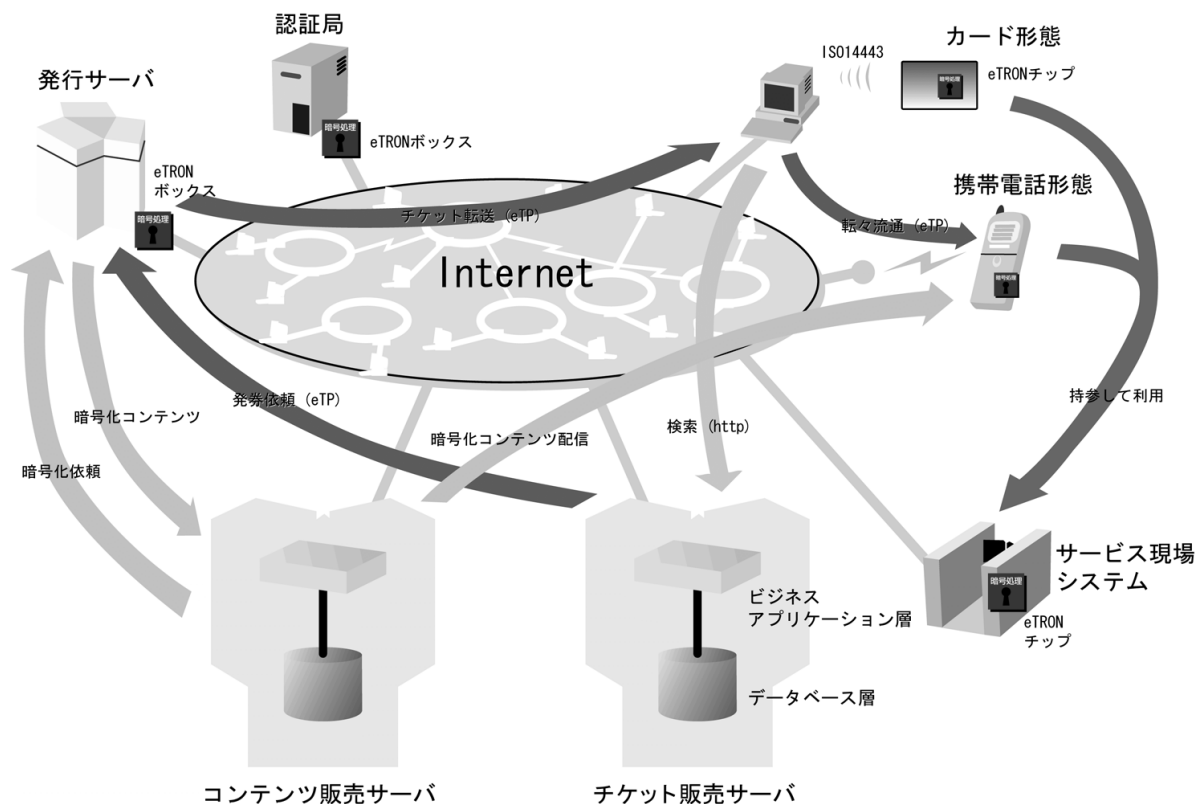


図 1 : eTRON アーキテクチャの概念図

テムが動作するコンピュータノードである。これは、CHs に格納する価値情報を発行・回収・変更・譲渡などを行う。CH の機能と SC の機能の両方を同時に有するノードもある。

この CH と SC 両方を合わせて、eTRON ノードと呼ぶ。eTRON ノードは eTRON アーキテクチャ内で有効なユニークな 128 bit 長の識別子 (eTRON ID) を持つ。

eTP 基盤

eTP 基盤 (eTP Infrastructure、以下、eTPI) は、CH と SC の間を eTP で通信するメカニズムを提供する。例えば、eTPI は、ユーザが携帯するモバイルノードである eTRON カードに対して、正しい通信経路を提供する。

eTRON 暗号認証基盤

eTRON 暗号認証基盤 (eTRON Authentication/Encryption Infrastructure、以下、AEI) は、eTRON アーキテクチャが認証や暗号の処理を行うときに用いられる PKI である。公開鍵を登録する認証サーバなどから構成される。

eTRON 応用ネットワーク基盤 (Application Network Infrastructure)

eTRON 応用ネットワーク基盤 (Application Network Infrastructure、以下、ANI) は eTRON アーキテクチャを使って価値情報を扱うユーザサービスを提供するためのアプリケーション依存のネットワーク基盤システムである。

3. eTRON チップ

eTRON チップは、上記の eTRON アーキテクチャのエンドノードを構成する重要な要素で、ユーザが価値情報を格納するために用いる。耐タンパー性をもったハードウェアを使って実装することが想定されている。eTRON チップは、カード型に実装したり (eTRON カード)、また携帯電話のようなモバイル端末や、家電製品などに組み込んで、それらの機器が安全に価値情報を扱うことを支援する。

3.1 特徴

eTRON チップを、スマートカードとしてみると、以下の特徴がある。

分散環境ノード

eTRON チップは既存の多くのスマートカードとは異なり、コンピュータの周辺機器ではなく、分散環境におけるノードとして設計されている。サポートするプロトコルは、セッション層の eTP である。ネットワーク上のサーバーや他の eTRON カードと、eTP 基盤のネットワークを介して eTP で Peer-to-Peer 通信する。

eTRON ID で特定する相互認証方式

eTRON チップは eTRON ノードが持つユニークな識別子 (eTRON ID) を持つ。eTRON ID は eTRON チップを識別するだけでなく、遠隔地からチップへの通信の経路制御にも利用される。eTRON チップと通信セッションを構築する際には、相互認証がなされ、その結果として相互に確実に相手の eTRON ID が把握される。この相互認証の際の eTRON ID の正当性の確認は、その eTRON カードに与えられた AEI の認証局が付与した証明書とその署名を確認することでなされる。eTRON はこの認証の際に、何か特定のアルゴリズムを規定するものではなく、様々な方式を適用できる枠組みを提供する。既に、秘密鍵暗号アルゴリズムをベースとした方法や、PKI ベースの方法などの実装例がある。

eTRON ID に基づいたアクセス制御リスト方式による統合的な資源保護機構

eTRON チップは、相互認証によって通信相手の eTRON ID を特定する。そこで、eTRON がチップの持つ資源の保護機能として、eTRON ID に基づいたアクセス制御リスト (Access Control List、以下、ACL) を提供する。eTRON では、eTP によりセッションを構築した相手の eTRON ID に応じて、各資源に対して、発行者 (ISSUER)、所有者 (OWNER)、それ以外 (OTHERS) という立場が決まる。そこで、アクセス制御リストによって、発行者・所有者・それ以外が発行可能な命令を制限することができる。

価値情報の格納庫に対する操作権限として重要な性質は、価値情報の発行者と現在の所有者が相互に信頼しないことである。つまり、情報の発行者だけが可能な操作や、情報の所有者だけが可能操作というものを、ACL によって実現する。例えば、電子チケットの座席番号データのように、チケットの提供者であるチケットの発行者が変更できても、それを購入した情報の所有者には変更できない情報や、また所有者の個人情報のように、情報の所有者だけがアクセス制御できる情報などを実現することができる。

eTRON カードでは、アクセス制御リストの中で、所有者、発行者、その他、を統一的に扱い、それぞれのもつ権限に応じて、アクセス制御リストを変更する API を発行することによって、アクセス権限の制限や解放、委譲といった制御を柔軟に行うことを可能にしている。

転々流通のためのチップ間通信

eTRON では、サーバを介さず、価値情報を格納した eTRON ノード間で直接情報を交換する転々流通機能をもつ。

ロールバック可能なトランザクション機構

eTRON アーキテクチャ内での価値情報の移動はセキュアに行う必要があり、eTRON チップも例外ではない。eTRON チップは、価値情報の作成・削除処理の原始性を保証するために、トランザクション機構を提供している。トランザクション処理中にアボート命令が発行された場合、またコミット命令がタイムアウトした場合は、トランザクション処理はロールバックされる。ネットワーク上にトランザクションコーディネータを置ける場合は、二層コミットプロトコルも対応する。

リンク機能を持った記憶構造

種類 (リリース)	接触 I/F	非接触 I/F	暗号、認証機構	PTP*	RBT*	Link
eTRON/8 (2001)	—	ISO 14443 Type-C	Secret Key Based	無	無	無
eTRON/16 (2002)	ISO 7816		PKI	有	有	有
eTRON/32 (200X)						

PTP*: Peer-to-peer 通信機能

RBT*: Roll-Back Transaction (ロールバックトランザクション) 機能

表 1 : eTRON チップの実装状況

現在、耐タンパー性をもったチップは利用可能なハードウェア資源が乏しい。そこで、想定するアプリケーションの全ての価値情報をチップに格納できない場合もある。そこで、eTRON ではコンテンツを複数の eTRON CHs、例えば、eTRON チップとネットワーク上の eTRON ボックスの間で分散して保持し相互の間にリンクを設定できる。

3.2 開発状況

トロンプロジェクトでは 3.1 で述べた特徴を持った eTRON チップを用途に応じて開発している。これらは互いに外部インタフェースレベルができるだけ互換性を持つように設計している。

まず、2001 年 7 月には、8bit のマイクロコントローラを使った非接触型の eTRON チップとして、eTRON/8 が開発された。eTRON/8 はカードとして実装され、非接触通信の ISO14443 Type-C による微弱誘導電流で動作する (図 2)。無電源で動作するという利点がある反面、大量の計算機資源を持たないため、一部の eTRON チップの特徴を備えていない、マイクロ eTRON チップであると位置付けている。3.1 で述べた特徴を



図 2 : eTRON/8 カードと μT-Engine

備えた、16 bits や 32 bits のマイクロコントローラを使った eTRON/16、eTRON/32 の開発を進めている (表 1)。

4. eTRON の利用

eTRON は、既に複数の場所で実際に採用され、30 万人以上が利用した実績を持つ。2001 年 7～9 月の約 2 ヶ月にわたって、神戸未来体験博覧会が開催され、その会場の入場券として、eTRON/8 カードが用いられ、神戸未来体験博は、未来の電脳都市を模擬的に体験することが目的とされており、博覧会場内は来館者に応じて多様な情報を提示するユビキタス情報空間となっていた^[2]。そこで、我々は、このユビキタス情報空間と来館者との間のインタフェースとして、安価で、かつ短時間でユビキタス情報空間に情報を与えたり、受け取ったりできるものを必要とした。こうした性質を満たすデバイスとして、非接触型スマートカードが最適であると考え、会場全体のユビキタス情報空間ー来館者インタフェースとして、eTRON/8 カードを用いた。会場には、店舗も含んでおり、本カードはセキュアでもあるため電子マネーのカードとしても用いられた。このユビキタス情報空間は、実世界型のアドベンチャーゲームになっている。eTRON/8 カードは来場者独自の経路の情報や、今まで会場内でみてきた展示物の履歴を記録するデバイスとして利用した。また、希望する来館者には、カードに設定された来館者の電子メールアドレスへ、博覧会からの提供情報を自動送付する機能も実現した。これらは、eTRON の多目的性を利用したアプリケーションとして構築したことになる。

同様の応用として、2001 年 7 月にオープンした、日本科学未来館の中の一部や、2002 年 1～2 月に開催された東京大学総合研究博物館のデジタルミュージアム III で、eTRON/8 カードが利用された^[5]。

現在、我々は PKI、Peer-to-Peer による価値情報の転々流通機能を有する eTRON/16 チップを利用した、モバイルアーキテクチャ上での価値情報の流通プラットフォーム STeP (Securely Transferable Entity Platform for Mobile Communications) を構築している^[3]。基盤となる

モバイルシステムのハードウェアとして、T-Engine^[4]を利用している。T-Engine は、組み込み型リアルタイムシステムの標準オープンプラットフォームとして、トロンプロジェクトが開発しているもので^[6]、eTRON チップインタフェースを標準で装備している。

5. まとめ

近年、インターネットを経由したクラッキングや不正アクセスの被害が、年々増加している。それにも関わらず、身の回りの様々なところにコンピュータが入り込むようになっている。こうしたコンピュータ化社会において、誰もが簡単に用いることができるセキュリティー基盤として、我々は eTRON アーキテクチャの構築に取り組んでいる。本稿では、この eTRON の基本理念やアーキテクチャの概要について述べた。

参考文献

- [1] Ken Sakamura and Noboru Koshizuka: "The eTRON Wide-Area Distributed-System Architecture for E-Commerce," *IEEE MICRO*, Vol. 21, No. 6, Dec., 2001, pp. 7-12.
- [2] Katsunori Shindo, Noboru Koshizuka, and Ken Sakamura: "Large-scale Ubiquitous Information System for Digital Museum," in *Proc. 21th IASTED*, Feb., 2003, 掲載予定.
- [3] 青野博, 他: 「モバイル向け電子価値流通プラットフォームの研究」, 第 19 回情報処理学会コンピュータセキュリティー研究会予稿集, 2002 年 12 月.
- [4] Ken Sakamura and Noboru Koshizuka: "T-Engine: The Open, Realtime Embedded-Systems Platform," *IEEE MICRO*, Vol. 22, No. 6, Dec., 2002, 掲載予定.
- [5] 坂村健 監修: 「デジタルミュージアム III」, 東京大学総合研究博物館, 2002 年.
- [6] T-Engine Forum, <http://www.t-engine.org/>