TEEを用いた安全かつ可用性の高いクレジットカード決済スキームの提案

寳代 晋太郎[1]　品川 高廣[1]

概要：クレジットカード決済をおこなう際には，カードを挿入した決済端末からカード発行会社であるイシュアのサーバーに対して, 決済のたびに決済電文を送信して決済の承認手続きを依頼する必要がある. しかし現在のカード決済スキームでは, 決済ネットワークに送られる決済電文が十分に保護されていないといった安全性の問題や, ネットワーク不調時に決済が遅延・中断するといった可用性の問題がある. 本稿では,Trusted Execution Environment (TEE) を用いた安全かつ可用性の高いクレジットカード決済スキームを提案する. 決済処理業者においてクレジットカード情報を平文で処理することを避けるために, イシュアの決済システムを決済処理事業者の提供する TEE 内で動作させる. また, ネットワーク不調時にも決済を安定して可能にするために, イシュアのサーバに接続せずに TEE 内の処理で一定額までの決済を可能にする.

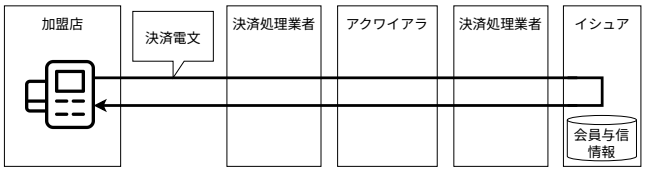

図 1　カード決済時の決済承認プロセス

1. はじめに

キャッシュレス決済が増加する中で，クレジットカード決済の重要性が年々大きくなっている．カード決済をおこなう際には、決済のたびにオーソリゼーションと呼ばれる決済承認手続が必要となる（**図 1**）．オーソリゼーションでは, まず加盟店の店頭でカードを挿入した決済端末から、決済ネットワークを介して決済電文が決済処理業者に送信され、次に加盟店と契約しているカード会社（アクワイアラ）へと転送され，最終的にカード会員と契約しているカード会社（イシュア）へ転送される．イシュアでは決済金額が当該カード会員の与信枠を超えていないか判定し, 決済端末へ判定結果を返却する．オーソリゼーションでやり取りされる決済電文には，決済日時や決済金額などの決済情報と共に，カード会員番号や有効期限などの重要なカード会員情報が含まれている．

しかし，現在のオーソリゼーションスキームにはいくつかの問題がある．第一に，決済ネットワークに送られる決済電文が十分に保護されていないといった安全性の問題である．現在のスキームでは，決済電文に決済処理業者やアクワイアラには必ずしも必要ないカード会員情報が含まれることがあり，決済処理業者などに悪意のある従業員がいた場合に、システムのルート権限を取得することでメモリダンプなどの手段によりカード会員情報が窃取される可能性がある．第二に，ネットワーク不調時に決済が遅延・中断するといった可用性の問題である．例えば，加盟店や決済処理業者，カード会社間で地理的に大きな距離がある場合には，ネットワーク遅延が大きくなる可能性がある．また，ネットワーク切断や帯域不足が発生した場合，オーソリゼーション自体が不可能になり，結果として決済が失敗する可能性がある [1].

安全性の問題に対しては，主に不正検知の手法が多数研究されている **?**．しかし，不正検知では事後対処となるため，カード情報の漏洩を未然に防ぐことが難しい．可用性の問題に対しては，完全オフラインで動作する決済手法 [2] が提案されている．しかし，この手法では既存の決済スキームとの互換性に課題がある．既存の決済スキームを改善することでこれらの問題に対処する場合には、セキュリティを十分に考慮した慎重な検討が必要となる．

本研究では，信頼できる隔離実行環境である Trusted Execution Environment (TEE) を活用した安全かつ可用性の高いクレジットカード決済スキームを提案する．まず，カード会員情報が決済システム内で平文で扱われることを避けるために，決済端末内や決済処理業者のシステムに TEE を導入し、カード情報が暗号化された状態で処理

[1] 東京大学
The University of Tokyo

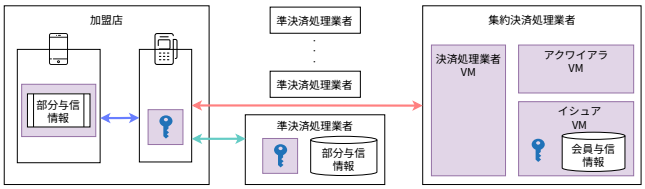

図 2 提案手法の概要

されるようにする．これにより、決済システム内に悪意のある人間が存在してもカード情報が窃取されないようにする。また，ネットワーク不調による決済の遅延・中断を防ぐため，準決済処理業者を分散配置し，地理的に近い決済端末と直接通信して決済を実行する．分散決済を可能にするために，カード会員情報を部分的に複製し，準決済処理業者間のデータ不整合を弱い一貫性制御で一時的に許容し，セキュリティリスクにはデジタル署名で対処する．さらに，ネットワークが分断された際も，スマートフォンと決済端末の直接通信によりオフライン決済を可能にすることで，ネットワーク不調時にも決済を安定して行える仕組みを実現する．

2. 設計

図 2 に本研究における提案手法の概要を示す．まず本手法では, イシュア以外でカード会員情報の読み取りができないように, 決済端末内で決済電文におけるカード会員情報を暗号化する．決済端末における暗号化は TEE 内部で行うことで, 攻撃者により決済端末の OS が乗っ取られた場合でも,TEE は独立した実行環境を提供するため, その鍵や暗号化されたデータへの不正アクセスを防ぐ．

ネットワーク遅延の軽減のため, 地理的に分散していた決済処理業者やアクワイアラ, イシュアを同一センタ内の異なる VM として集約決済処理業者内に統合する．この際, 集約決済処理業者のシステム管理者によるアクワイアラ VM やイシュア VM への不正なアクセスを防ぐため,SEV を使用し各 VM に割当てられたメモリと仮想ディスクを暗号化する．

また, 決済端末と決済処理業者が地理的に離れている場合のネットワーク遅延対策として, 広域ネットワーク上に準決済処理業者を分散配置する．決済端末は, 地理的に直近の準決済処理業者と集約決済処理業者の両方に接続させる. 準決済処理業者には, イシュア VM に所在するカード会員情報の一部が複製されるため, 決済端末は準決済処理業者とのみ通信を行うことでオーソリゼーションが可能となる．ただし, 準決済処理業者に全てのカード会員情報を複製するのではなく, 接続されている決済端末で決済が発生した会員のカード会員情報のみを準決済処理業者から集約決済処理業者へ要求する．これにより, 必要なカード会員情報のみが準決済処理業者へ複製されるようにする．

カード会員情報を保持する準決済処理業者を分散配置するこの方式には 2 つの潜在的な課題がある. まず同時刻に複数の準決済処理業者で同一の会員によるオーソリゼーションが発生した場合, 各センタ間でのデータ同期の遅延が生じることにより与信枠を超えて決済が行われる可能性がある．これを防ぐため,Gao らの研究 [3] で提案されている, 業務特性に応じてセンタ間でのデータ不整合を一時的に許容する弱い一貫性制御を用いる. 準決済処理業者には会員の与信枠の一部のみを部分与信枠として付与し, この部分与信枠を超える場合は, 集約決済処理業者までのオーソリが必須とさせる．このように弱い一貫性制御と集約決済処理業者の組み合わせによって, 結果整合性を担保する．

また準決済処理業者はロールバック攻撃のリスクもある．この攻撃が成功すると, 準決済処理業者で消費された部分与信枠が不正に回復され, 与信枠を超えた決済が可能となる．このような事態を回避するため, 準決済処理業者の TEE 内で, 保持しているデータに対し一意のデジタル署名を生成し, データが変更された場合, 署名の検証が失敗する. このデジタル署名の検証機能を用いて, ロールバック攻撃をリアルタイムで検知する事ができる. 検知された場合, 対象の準決済処理業者でのオーソリゼーションは即座に中断される．

ネットワーク分断が生じた際にも決済を実現するために, スマートフォンと決済端末間の通信のみでオーソリゼーションができるような仕組みを構築する．具体的には, スマートフォンの TEE 内に, 準決済処理業者と同様に当該カード会員の部分与信枠を付与する．これにより決済端末が準決済処理業者や集約決済処理業者への接続が不可能な場合においても, 決済金額が部分与信枠を超えない限り, オフラインでのオーソリゼーション及び決済が実現できる．

3. まとめと今後の予定

本稿では, TEE 技術を活用したセキュアで効率的なクレジットカード決済システムの新スキームを提案した．今後は各ノードでの具体的な決済条件の詳細策定及び実装を行う．最終的にはオーソリゼーションにおけるレイテンシを実測し, 提案システムの性能と効果を客観的に評価・検証する予定である．

参考文献

[1] Daza, V. et al.: FRoDO: Fraud Resilient Device for Off-Line Micro-Payments, *IEEE Transactions on Dependable and Secure Computing*, Vol. 13, No. 2 (2016).
[2] Daza, V. et al.: FORCE: Fully Off-line secuRe CrEdits for Mobile Micro Payments, *Proc. 11th International Conference on Security and Cryptography* (2014).
[3] Gao, L. et al.: Application specific data replication for edge services, *Proc. 12th International Conference on World Wide Web* (2003).