cpl.thalesgroup.com

THALES
Building a future we can all trust

# QUADRAC株式会社：クレジットカードのタッチ決済で交通決済の利便性が大きく前進

## 画期的なMaaSサービスを支えるタレスの「決済用HSM」と「トークン化技術」

### サマリ

デジタルトランスフォーメーション（DX）のさらなる推進が社会全体で求められるなか、交通・移動のMaaS[1]領域では、より利便性の高い決済手段として海外では一般的である「クレジットカードのタッチ決済」の導入が、国内でも始まっています。

自動改札機や改札窓口又はバスに設置された専用リーダー端末にクレジットカードをかざすだけ。サインや暗証番号入力をすることなく[2]、スピーディにきっぷ購入や乗車ができるのがクレジットカードのタッチ決済です。

京都丹後鉄道、京福バス、北都交通ではすでに決済サービスを提供中。南海電気鉄道、福岡市交通局では、Visaカードのタッチ決済[3]と、スマホにインストールしたMaaSアプリを組み合わせた企画乗車券サービスなどの実証実験を2021年に行っています。

いずれの事例も、決済と認証の共通処理を一手に担っているのが、QUADRAC社の交通事業者向けSaaS 型プラットフォーム“Q-move”です。

“Q-move”は、タレスの決済用HSM、およびトークン化ソリューション「CipherTrust Tokenization」を採用したことで高セキュリティと運用コスト低減の両立に成功し、MaaS推進の切り札として注目されています。

### 選定のポイント

手軽に使えるタッチ決済は、サインや暗証番号の入力をする従来方式以上に、クレジットカードのデータを厳重に守る必要があります。QUADRAC社は、決済・認証センターを設計・開発するにあたって、DUKPT[4]の採用とPCI DSS[5]の認証取得を決断しました。

1 MaaS: Mobility as a Service
2 規定金額を超える支払いには、暗証番号入力やサインが必要
3 タッチ決済は、カードブランドごとに「Mastercard®コンタクトレス」、「JCBコンタクトレス」等があるが、現在の日本のMaaSでは「Visaのタッチ決済」が先行している
4 DUKPT - Delivered Unique Key Per Transaction
5 PCI DSS - Payment Card Industry Data Security Standard

「 “Q-move”は、交通決済の共通処理を集約し、クラウド化することで、ICカード等を使った既存の料金徴収システムに比べて大幅なシステム導入コスト低減に成功しました。多様な交通機関が横断的に導入する必要があるMaaS実現の切り札になると自負しています。特に海外からの訪日客は、空港バスからショッピング・宿泊・観光地移動などを、1枚のクレジットカードをかざすだけでシームレスに行えると便利です。その高評価がまたインバウンド拡大につながるような好循環を牽引していきたい。」

– QUADRAC株式会社　クラウド基盤担当マネージャ
伊藤 博貴氏

第1のDUKPTは、専用リーダ端末とセンター間の暗号通信に用いるプロトコルです。DUKPTのセキュリティレベルを維持するには、サーバーが保持する「システム鍵」を管理するために、暗号鍵保護の専用ハードウェア「HSM」の導入が必須でした。

QUADRAC社では各社のHSMを比較検討した結果、実績豊富で国内事例もたくさんあること、必要な機能がシンプルにそろっていてコストパフォーマンスに優れていること、導入後に性能をアップグレードできるため、スモールスタートしやすいことの3点を評価して、タレスの決済用HSMを採用しました。

第2のPCI DSSはクレジット業界における国際的データセキュリティ基準ですが、認証取得にあたっては、PCI DSS専門のコンサルティングを受けました。PCI DSSは審査の対象範囲が幅広く、認証取得に加えて毎年行われる監査へ確実に対応していくには、システム投資・運用管理費・人件費が膨大にふくらんでいく懸念があったからです。

最大の焦点は、DUKPT経由で受け取った暗号をセンターで復号化した後、その「生データ」を保存する方法です。

生データのままで保存すると、管理項目が広範囲にわたり、運用コストが増大します。再度暗号化して保存すると、暗号鍵を管理するところに運用負荷がかかります。

そこで注目したのがデータのトークン化、トークナイゼーション[6]です。トークナイゼーションは、高セキュリティなデータ保護の方法であると同時に、PCI DSS審査範囲の縮小と運用負荷軽減に貢献します。

QUADRAC社は、各社のトークナイゼーションのソリューションを比較検討しました。

タレスのCipherTrust Tokenizationを選んだのは、決済用HSMと同様に、「実績」、「コストパフォーマンス」、「スモールスタートのしやすさ」を評価したからです。

また、トークナイゼーションにはボールト型とボールトレス型の2つのアーキテクチャがありますが、CipherTrust Tokenizationはどちらにも柔軟に対応可能。QUADRAC社は、ボールトレス型を選択して、この部分でも、監査範囲の削減と、コスト削減を追求しました。

## ソリューション

“Q-move”は予定どおりにPCI DSS認証を取得し、2020年から商用サービスを開始しました。交通事業者はリーダー端末の導入台数規模を気にすることなく、高速・高セキュリティな決済・認証機能を活用しています。

更に“Q-move”は、交通機関利用者が乗車履歴をスマートフォンで閲覧できるWebサービスを提供しています。また、別のベンダーがQRコードと組み合わせてサービスを提供できるように共通機能を整備しているのが特徴です。

順調なスモールスタートですべり出したQUADRAC社のクラウド型サービスは、MaaS基盤としての今後のビッグ展開が期待されます。

### 課題

- クレジットカードのタッチ決済機能を利用した交通決済システムのクラウドサービス基盤を、高セキュリティ、かつ低コストで構築したい
- 専用リーダー端末と決済・認証センターとの暗号通信には、DUKPTを採用。システム鍵を厳重に保管するため、HSMが必須に
- 決済・認証センターはPCI DSS認証を取得する。PCI DSS監査範囲を縮小し、運用負荷を軽減するため、生データのトークナイゼーションを採用

### ソリューション

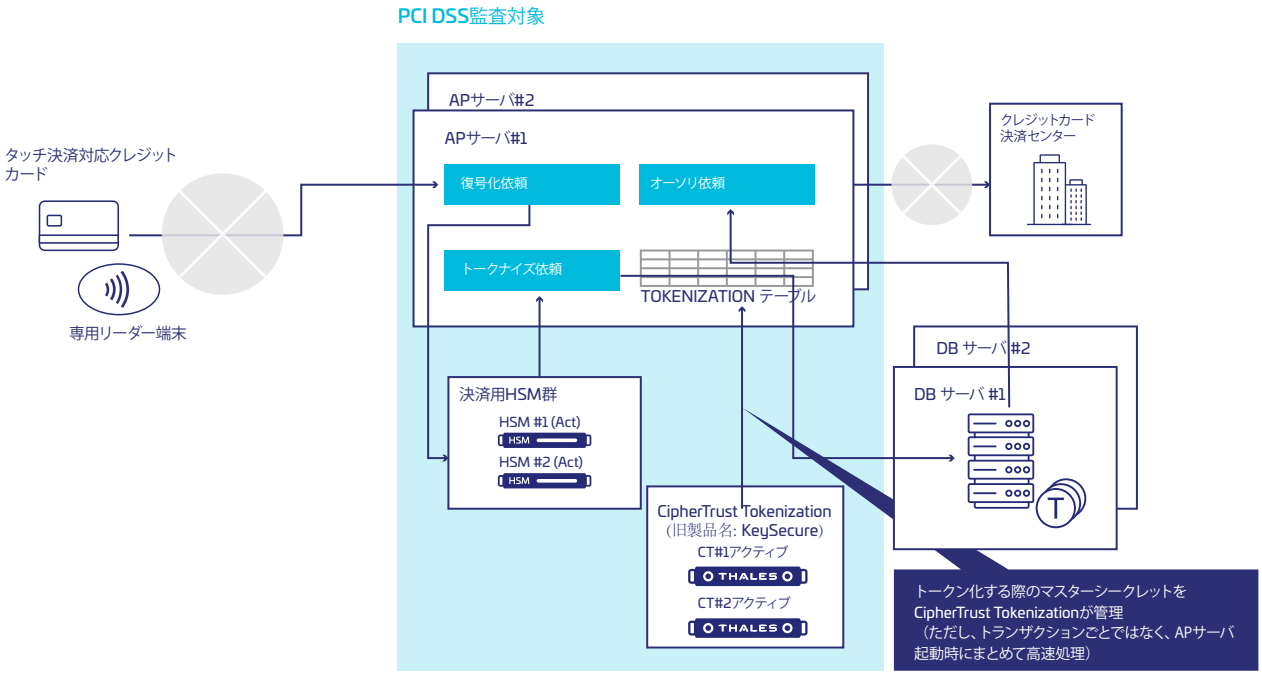
- DUKPTのシステム鍵管理には、タレスの決済用HSMを選定
  - —実績豊富、国内事例もたくさんある
  - —必要な機能がシンプルに網羅されていて、コストパフォーマンスが高い
  - —使用開始後に処理性能をアップグレードできるため、スモールスタートしやすい
- 生データのトークン化には、タレスのCipherTrust Tokenizationを選定
  - — 実績豊富でコストパフォーマンスも優れている
  - —CPU、メモリ等のリソースが最小限で済み、導入しやすい
  - —ボールトあり／ボールトなしの両アーキテクチャへ柔軟に対応する。“Q-move”はボールトなしを選択し、ここでもPCI DSS監査の簡素化と初期投資抑制を推し進めた

### メリット

- “Q-move”は、DUKPTに対応し、PCI DSS認証を取得。クレジットカードのタッチ決済機能を安心して利用できる高セキュリティなシステム基盤を構築できた
- クレジットカードのデータはトークン化して保存することで、PCI DSSの監査対象縮小に成功。初期投資を抑制、今後の運用コストも低減
- コスト低減と高セキュリティを両立させた“Q-move”は、交通事業者が参加・導入しやすく、数々の実用化と実証実験がすでに進行中。
- DUKPTのシステム鍵管理も、PCI DSS準拠のトークナイゼーションも、QUADRAC社の開発者にとって初めての取り組みだった。日本法人のタレスDIS CPLジャパンは、プリセールスの段階から、製品機能のみならず、他社での実装例、運用管理者のトレーニング方法などをレクチャー。初回の監査にも立ち会うなど、きめ細かいサポートを提供した
- QUADRAC社の今後のビジネス展開でも、幅広い製品ラインアップを誇るタレスは、多彩なサポートが可能

6 トークン化／トークナイゼーション - クレジットカード番号などの機密データを、乱数により生成する別の文字列に置き換え、保存・利用する技術。トークン化したデータは、元データと1対1で結びつき、元データの再取得が可能。一方でトークン化したデータそのものは、元データと数学的な関係性をまったく持たないため、万一漏えいしても単体では悪用ができない。したがって、トークン化したデータは、PCI DSSの審査範囲からはずすことができる

トークン化したデータを格納するデータベースサーバーは、PCI DSSの監査対象からはずすことができ、運用管理の負荷は大きく軽減した。




## ThalesのCipherTrust Tokenizationについて

CipherTrust Tokenizationは、Vaulted（トークンボルトあり）とVaultless（トークンボルトなし）の両方が用意されており、PCIDSSなどのデータセキュリティ要件を順守するコストと複雑さを軽減することができます。トークン化は、機密データを代理トークンに置き換えることで、機密データをデータベースや権限のないユーザーやシステムから切り離して保護します。Vaultless（トークンボルトなし）のソリューションには、ポリシーベースの動的データマスキング機能があります。どちらのソリューションも、トークン化をアプリケーションに簡単に追加できます。

## タレスについて

皆様がプライバシー保護を信頼して任せている相手は、そのデータを保護するためにタレスに頼っています。データセキュリティに関しては、組織が直面する決定的な局面は次々と増え続けています。その局面が暗号化戦略の策定、クラウドへの移行、コンプライアンス要件の順守のいずれであっても、デジタルトランスフォーメーションを保護するためにタレスに頼ることができます。

決断の瞬間のための、確実なテクノロジー。



> cpl.thalesgroup.com <

**お問い合わせ先 –** cpl.jpsales@thalesgroup.com すべてのオフィスの所在地と連絡先情報につきましては 、cpl.thalesgroup.com/ja/contact-usをご覧ください。