ペイメントトークン利用による決済セキュリティ強化の潮流

タレスジャパン株式会社 e- セキュリティ事業部
シニアテクニカルスペシャリスト　山神　真吾

1. はじめに

決済取引において、機密データを保護するための最も効果的な方法は何か。それはクレジットカードに関連する機密データを一切持たないことである。守るべきデータがなくなれば、攻撃を受ける可能性は低くなる。セキュリティ対策としては最も効果が高い。ただし、機密データを安全な形で伝送しなければ、決済取引は成立しない。決済取引を完了するためには、別の代替手段が必要となる。

スマートフォンやタブレット端末の普及により、決済取引を取り巻くセキュリティ環境にも大きな変化が見られた。専用線を前提としていた時代のセキュリティでは、もはやモバイル端末からの決済取引は保護できない。事業者向けのモバイル決済ソリューションとして mPOS が登場し、消費者・カード会員向けのソリューションとしてペイメントトークンの利用が始まった。この２つのソリューションはクレジットカードに関連する機密データを事業者側で保持しないこと、既存の決済ネットワークに影響を与えず決済取引が完結することで共通している。

2013 年ごろから、国内でも事業者・加盟店によるスマートフォンおよびタブレット端末を活用したクレジットカード決済サービスの取り扱いが始まった。このような決済サービスはm POS（mobile Point of Sales）と呼ばれている。では、決して安全とは言い切れないモバイルネットワーク環境でいかに機密データを保護しつつ、決済を完了するのか。m POS では、P2PE（ポイント TO ポイント暗号）により、カード受付から加盟店センターまで一貫して機密データを暗号化する。また DUKPT（Derive Unique Key Per Transaction）と呼ばれる鍵管理プロトコルで、トランザクションごとにユニークな暗号鍵を生成利用する。万が一暗号鍵が傍受されても、次の決済では異なる鍵で暗号化しているため、決済情報を復号化することはできない。決済情報はクレジットカードを受け付けたカードリーダで暗号化されるため、事業者・加盟店は決済情報を持たない。

2014 年 3 月、国際ブランド 6 社が参加し、EMV Payment Tokenization Specification/Technical Framework が発表された。ペイメントトークンをどのように安全に実装するのか、トークンの形式、トークン化システムの要件について基準を定めている。ここで定義されているペイメントトークンは特にモバイル端末を利用した決済での利用を想定している。Tokenization 自体はそれほど新しい技術ではないものの、決済向けのトークン化技術・ペイメントトークンの利用は始まったばかりで、今後利用が拡大する見込みだ。昨年 10 月から米国で本格利用が始まったペイメントトークンによる決済は、今年 7 月には大陸を超えイギリスでも開始されている。

この文章では、ペイメントトークンとは何か、ペイメントトークンのセキュリティ面での長所、決済取引におけるセキュリティの将来について、論考する。

2. ペイメントトークンとは

トークン化は暗号化と異なり、カード番号を元の番号と関連性のない番号・代理の値に置き換える技術である。したがって、トークンから元の番号を演算で割り出すことはできない。EMV.co の仕様書ではトークンは ISO の標準で定められた 13 桁から 19 桁の数値と定義されているが、既存の決済インフラでの取引に対応するため、影響を考慮し実カード番号と同じ桁数でトークンが生成される場合が多い。ただし、必須というわけではない。実カード番号：PAN での決済処理と同様、Luhn チェックと呼ばれる演算・検証に対応し、BIN（銀行識別番号）や Expiry Date といった要素も含まれる。ただし、既に発行済みのカード番号と重複してしまうと処理ができないため、実カード番号とは異なるトークン専用の BIN が割り当てられる。

3. ペイメントトークンのセキュリティ面での長所

ペイメントトークンを利用することで、実カード番号：PAN はモバイルデバイス内に保存されない。PAN はトークンサービスプロバイダ（TSP）側に安全な状態で保管されている。トークンサービスプロバイダ（TSP）はペイメントトークン＝デバイスアカウントナンバー（DAN）を生成し、DAN と PAN をマッピングする。DAN と PAN を紐づけて格納するデータベースを Token Vault と呼ぶ。Token Vault では非常に機密性の高いデータを取り扱うため暗号化されており、金融業界で実績のある方法でセキュリティ管理をするように、EMV.co のドキュメントでも言及されている。また、Token Vault には Token Requestor ID や Domain 情報も含まれ、DAN を利用できる場所を制限・管理することができる。

万が一、DAN を不正に傍受されたとしても、次の決済取引には利用できない。DAN 単体では決済処理されない。動的な暗号文が決済処理の承認に必要だからである。また、小売店のメリットとして、決済に利用する POS 端末が攻撃を受けたとしても、POS からクレジットカード番号が漏洩することはない。小売店では実カード情報を取り扱わないからだ。小売店、加盟店センターではペイメントトークンが通過するだけなので、負担が軽くなる。

ペイメントトークンを利用した NFC 決済フロー例について、図 1 にまとめている。消費者がスマートフォンをタップし、NFC 決済取引を開始する。小売店の POS 端末、加盟店センターを経由し、決済ネットワークへ DAN と動的暗号文が送信される。決済ネットワークは DAN に紐づいた PAN を取得するため、トークンサービスプロバイダ（TSP）へ照会を実施する。TSP は Token Vault 内の DAN/PAN マッピング情報を確認し、PAN を決済ネットワークに返却する。この一連の照会作業を De-tokenization と呼ぶ。決済ネットワークは返却された PAN と動

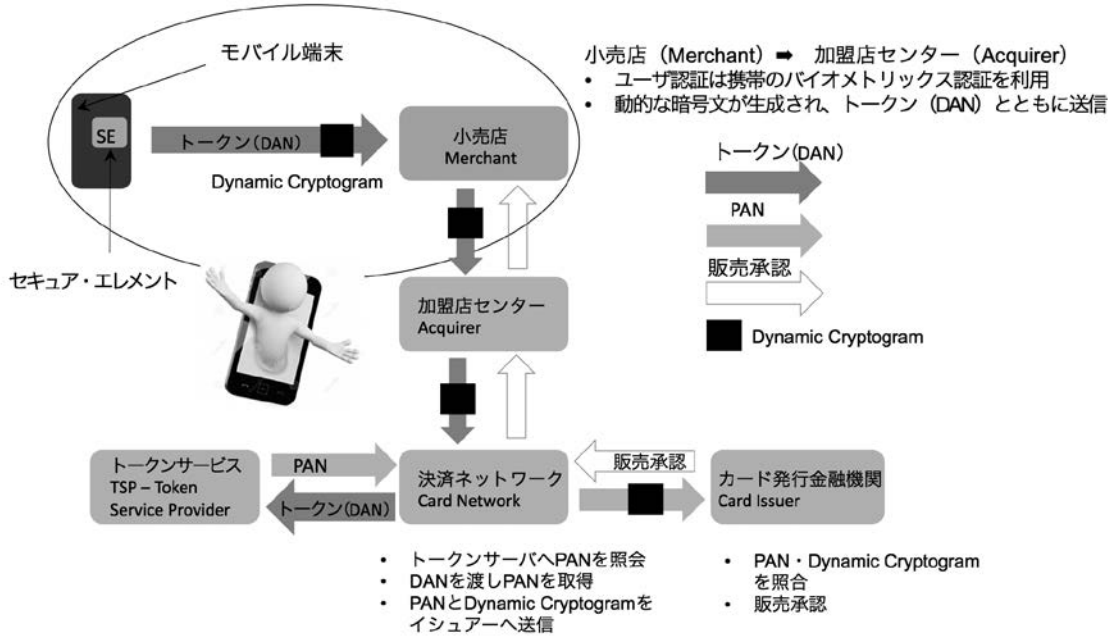

図 1：ペイメントトークンによる NFC 決済フロー例

的な暗号文をカード発行金融機関に送信し、販売承認を取得する。販売承認は加盟店センターを経由し小売店へ送信され、決済処理が完了する。

4. HCE とペイメントトークン

決済トークンはモバイルデバイスの安全が確保された領域に保管されるのが一般的である。eSE（組み込み型の IC チップ）や UICC（SIM カード）などセキュアエレメント（SE）を利用する方法、TEE（汎用 OS とは区切られた信頼されたアプリケーション実行環境）など実装方法は様々だ。そうした方法の中で特に注目を集めている技術がある。HCE：ホストカードエミュレーションである。既に国際カードブランドの各社が HCE への対応を表明している。さて、HCE とは何で、いったいなぜ注目を浴びているのか。

HCE とはクラウドベースのモバイル決済ソリューションである。モバイル端末側のセキュアエレメントを利用するのではなく、クラウド上でカードをエミュレーションする技術である。CE（カードエミュレーション）モードを利用すると、モバイルアプリが直接 NFC コントローラにアクセスできるようになる。HCE ではモバイル端末からの決済処理にペイメントトークンが利用される。ペイメントトークンや認証情報はセキュリティが強化されたクラウド上に保管される。これまでモバイル端末側に配置されていたセキュアエレメント（SE）がクラウドに移動したようなイメージである。

また、盗難・紛失によるカード利用を停止するような場合も、クラウド上に DAN や認証情報があることから即時に停止させることが可能で、運用面のメリットも非常に高い。万が一、不正取引が発生した場合も決済ごとに生成される動的な暗号文と認証プロセスにより、リアルタイムでの検知が可能で、取引の無効化とモバイルデバイスのブロックが可能である。

ビジネス面でも、HCE を導入するメリットがある。現状、セキュアエレメント（SE）と NFC を利用した決済には、MNO、MNO-TSM、SP と様々なプレーヤーが存在し、関係者間の調整、書類作成、交渉などに多くの時間を費やしてきた。HCE ではカード発

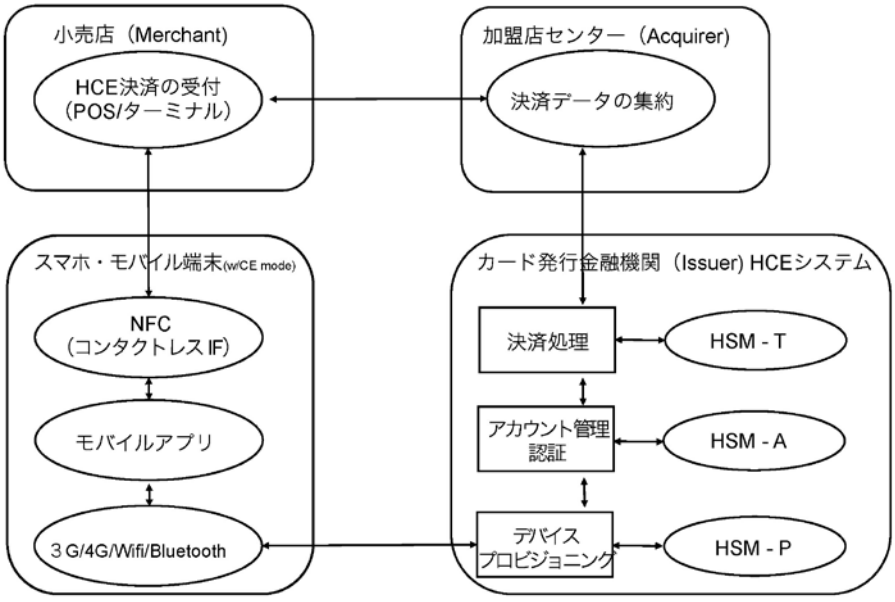

図2：HCE を構成する要素

行金融機関（Issuer）主導で、プロジェクトを進めることができることから、複雑化していたプロセスをシンプルにすることが可能で、導入までの時間と費用を削減することが可能である。

一方、HCE の利用にあたり、「クラウド環境ではセキュリティが十分でない」と警鐘をならす人々が一部に存在する。もちろん鍵管理がアプリケーションレイヤで実施されていると仮定するとその考え方は正しい。ソフトウエアの脆弱性を突いた攻撃により、鍵や決済データが漏洩してしまう可能性がある。しかし、金融機関や決済サービス事業者はそうしたセキュリティ面のリスクを理解して、バックエンドにある HCE システムに HSM（ハードウエア・セキュリティ・モジュール）を配置しセキュリティレベルを高めている。決済処理、アカウント管理・認証、モバイルデバイスとのセキュアセッションの確立、デバイス認証情報の割り当て（プロビジョニング）と HSM は活躍している。また、現状、弊社把握している範囲では、ソフトウエアベースの鍵管理を採用しているカード発行金融機関は存在しない。

5. HCE やペイメントトークンの将来

もちろん、市場の将来について、完璧に予測することは困難だ。ただ、今後 HCE やペイメントトークンが近い将来復旧していく好材料が存在しているのは事実で、新しい潮流に乗り遅れないように、準備を進めていくべきである。2014 年閣議決定された「日本再興戦略」改訂で、日本政府は 2020 年までにキャッシュレス対応を完了することを、日本クレジット協会がクレジットカードは 2016 年 12 月末までにクレジットカードの 80％を EMV 化すること、2020 年に EMV 化 100％を目標に掲げている。もちろん EMV 化＝コンタクトレス化ではない。

簡単な説明にとどめるが、EMV には接触型と非接触型の決済取引が存在する。実装方法は異なるもののカード偽造や盗難・紛失カードの不正利用を防止するという目的で共通している。接触型の EMV ではチップを利用した強力な暗号処理と動的な暗号文を活用したカード認証手順で、偽造カードの不正利用を効果的に防止してきた。

非接触型決済には現状①プラスチックカードに搭載された非接触型 IC チップを利用する方式②モバイル端末の NFC を利用する方式の２つがあり、②の場合、必ずしも安全とは言い切れない無線通信環境を利用するため、必然的にペイメントトークンを利用するケースが多い。①のプラスチックカードに実カード番号ではなく、ペイメントトークンを格納するようになるのかどうかはまだはっきりしていないものの、盗難・紛失時の損失を最小限にすることができるため、近い将来 EMV チップにペイメントトークンを格納する利用事例が出てくるかもしれない。

EMV 接触型決済の普及が一番の優先事項であるが、2020 年という目標まで残された時間はそれほど長くはない。米国と同様に、コンタクトレス化と EMV 化が同じタイミングで加速していく可能性は十分に有り得る。

近年の訪日旅行者（インバウンド）が増加しており、訪日旅行者が使い慣れない現地通貨のことを気にせず、小売店でスムーズな決済を実行することは重要である。ビジネスチャンスを逃さないのは商売の鉄則だ。販売機会の拡大と商取引の活性化はオリンピック開催に向けて、共通のゴールである。その準備にあたり、決済取引が安全で効率的になっていくのは間違いない。安全で効率的な決済実現に向け、HCE やペイメントトークンの利用が拡大する可能性が高い。HCE とペイメントトークンは対面決済の安全性を高めるだけでなく、オンライン・非対面決済でもセキュリティ強化に有効で、これから伸びていく技術であると考えられる。

一方、21 世紀の初めごろから 10 年以上 IC カードベースの電子マネーを利用し、「かざす」決済に慣れ親しんできた日本居住者にとって、スマートフォンを「タップしてかざす」決済への期待・要求は今のところそれほど強いものではないかもしれない。

また、NFC の Type-A / Type-B のカードリーダの設置、既存カードリーダのファームウエアの改修を進め、「タップしてかざす」決済が可能な場所を増やしていくことが一つの大きな課題となっている。日常生活の中で利用できることが普及の第一条件である。コンビニエンスストアやスーパーで利用できる状況になれば、消費者の利用は一気に加速する。

また、日本特有の決済環境、国内完結型取引（＝オンアス取引）も考慮しなければならない。トークンによる決済情報のルーティングが確実に実行されるようになるまでに、決済事業者間の微調整・協力も必要になる。

ビジネス面では日本居住者向けには、スムーズなクレジット決済プラスワンのサービス＝特典、リワードの提供等、消費者を引き付ける魅力、付加価値を高める必要がある。ただし、CLO（＝カード・リンクド・オファー）が即収益増加につながるわけではない点に注意すべきだ。プロモーション・キャンペーンの原資が乏しい小規模店舗が CLO による特典付与・キャッシュバックを実施するのは難しい。小規模小売店の経営改善に直結するのかどうかについては賛否両論がある。

6. モバイル決済における HSM の必要性

HCE やペイメントトークンを利用して安全な取引を実行するためには HSM が不可欠である。法律や規則で強制されるものではないものの、HCE やペイメントトークンを実装するにあたり HSM の利用はデファクトスタンダートとなっている。仮にペイメントトークン管理システムが攻撃を受けた場合、単に決済ができないだけではなく、企業は信用を失い、事業継続が困難な状態になりうる。国際ブランドは HSM の利用を推奨している。安全性が必ずしも確保されているとは言えない無線環境を利用することからも、HSM で鍵をアプリケーションから分離して管理するのは必然だ。また、ペイメントトークンは演算により元の値が解読されることがないよう、専用ハードウエアによる偏りのない乱数生成が必要である。

HSM はハードウエア・セキュリティ・モジュールの略称で、鍵管理と暗号・乱数処理を実行する。HSM は決済インフラの様々な場面で利用されていることはあまり知られていない。

- EMV チップ用のデータ生成
- EMV チップを搭載したクレジットカード発行
- 既存の決済インフラのトランザクション保護（PAN/PIN/MAC を含む決済取引データの保護）
- モバイルデバイスとのセキュアセッションの確立
- ペイメントトークン（DAN）の生成・乱数処理
- ペイメントトークン（DAN）のプロビジョニング

弊社は業界をリードする HSM メーカで、HCE や決済トークンの実装作業を支援する目的でコマンドや API を準備している。HCE を実装するサービスプロバイダとの導入事例も豊富で、標準化された仕様部分だけでなく、国際ブランド各社が定める独自実装・変更要求にも柔軟に対応し続けている。