モバイル決済とトークン技術

「簡単」で「安全」な決済の新手法

2016年10月から日本で「Apple Pay」のサービスが開始され、財布からカードを取り出すことなく、スマートフォンに搭載された非接触ICカードで電車に乗ったりコンビニで支払いができるようになり、モバイル決済がより身近になってきました。本稿では、簡単かつ安全にカード番号の漏えいを防ぐことができることから、近年のモバイル決済に採用されているトークン技術である「トークナイゼーション（トークン化）」の仕組みについて解説します。また、セキュアなトークン変換サービスの提供に求められる機能と役割を紹介するとともに、近い将来におけるモバイル決済とその顧客購買の変化について展望します。

1. はじめに：モバイル決済の本格展開へ

「もし家にお財布を忘れても一日中気づかないかもしれません。しかし、携帯電話がなかったら、私の生活は地下鉄に乗るところからつまずくでしょう。」――これは、リテール金融サービスの将来像を書いたブレット・キングの著書「Bank3.0」のモバイル決済の章で紹介された韓国の女子大生の言葉です[1]。

2016年10月から日本で「Apple Pay」のサービスが開始されました。新型iPhoneに搭載された非接触ICカード（FeliCaチップ）で電車に乗ったり、コンビニでの支払いを経験したiPhoneユーザーも多いのではないでしょうか。日本の電子マネー決済は、2001年のJR東日本の「Suica」採用を契機として、その後、全国のコンビニなどにFeliCa仕様の非接触POS端末数十万台が設置されるまで発展してきました。そしてモバイル決済は、2004年にNTTドコモの「おサイフケータイ」が開始されたのが最初です。

一方で、スマートフォンの個人保有は、2016年末の総務省の調査によると、20代で92.9%、40代でも74.8%まで拡大しています[2]。カード1枚を登録できるおサイフケータイに加えて、Android端末やiPhoneといったスマートフォンがNFC仕様やFeliCa仕様になることで、複数のカードや電子マネーが簡単な操作で支払い可能となり、財布を必要としないモバイル決済が、現実となる可能性がでてきました。

欧米への海外旅行で、カードがあればほとんど現金を使わずに過ごせるのを経験した方も多いでしょう。日本は、欧米や韓国と比較して、まだ現金による支払いの割合が高く、2016年現在で8割近くを占めています[3]。そのため、この10年間においても年率8～10%でカード決済や電子マネーの利用による非現金決済へのシフトが進んでいます。どこでも使えて簡便かつ安全な決済の登場は、それをさらに加速させるきっかけになると予想され、スマートフォンを利用したモバイル決済は、決済の非現金化への大きな牽引役になると考えられます。

2. モバイル決済の種類

モバイル決済とは、携帯電話、スマートフォン、タブレット、またはスマートウォッチなどのモバイル端末を利用した決済のことです。この数年、スマートフォンやタブレットの急速な普及により、多くの人が手元に保持するこれらのモバイル端末を使用した決済のニーズが拡大しています。

モバイル決済の種類を、**表1**に示します。1つは米スターバックスに代表されるような「スマホアプリ決済」があります。スマホアプリの画面に表示されたバーコードなどを店舗で読み取ることで、利用者の情報を読み取り決済を行う方法です。モバイル端末側の制約が少ないため小売店などで独自の導入がしやすいものの、その反面、標準化が進んでおらず利用店舗が限定されること、また利用者は決済アプリの事前登録が必要で、決済時にまちまちのアプ

リ操作をしなければならないという課題があります。

もう1つは非接触タイプのモバイル決済で、世界共通の「NFC仕様」(Type-A、Type-B方式)と、日本国内の電子マネーの標準といえる「FeliCa仕様」があります。どちらも店舗やコンビニ、駅のキオスクなどでかざすだけでピッと決済されるインターフェースですが、生い立ちの違いでモバイル端末や読み取り装置は別々の装備になります。現時点において、日本国内でFeliCa仕様の読み取り装置は、iD約65万台、QUICPay約51万台、Suica約36万台にのぼります。

3. モバイル決済の使い易さと安全性を保つには

これまでのカード決済は、財布から取り出したカードをカード専用装置で読み取って、さらに利用者が暗証番号の入力かサインをするという方法でした。モバイル決済では、クレジットカードやデビットカード(本人の銀行口座から即時に引き落とされる)でも、スマートフォン操作で支払うカードを選んで非接触POSリーダーにかざすという「簡単で使い易い」方法が主流となっています。しかしながら、個人所有が前提のスマートフォンも、紛失や盗難により簡単に悪用される心配があり、安心して利用できません。また、カード情報のスマートフォンの登録・保持も安全性の考慮が必要です。ここで、カードのモバイル決済のセキュリティーについて解説します。

(1)個人を特定するユーザー認証:指紋など生体認証の利用

これまでクレジットカードやデビットカードの店舗利用は、プラスチックカード情報の確認とともに、暗証番号(4桁のPIN)を入力することで利用者を確認していました。しかし、この4桁の暗証番号は、推測されやすい、盗み見されやすいなど第三者に不正利用されるリスクがあります。電子マネーは、使い勝手を優先して暗証番号を不要としていますが、本人でなくとも誰でも使えるリスクがある上に決済できる金額の上限が低くなります。

ユーザー認証の強化策の一つとしては、その場での二次元バーコードの読み取りやワンタイム・パスワード(OTP)の採用がありますが、支払いのシーンで提示や照合にそれなりの時間がかかることになります。

もう一つの強化策は、本人を特定するために生体認証を使って個人を認証する方法です。生体認証には、声による声紋認証、手のひらや指などの静脈認証、目の彩虹の画像パターンによる彩虹認証などいくつかの選択肢があります。モバイル決済で現在注目されているのは、モバイル端末による本人の指紋認証です。Apple Payで採用された「Touch ID」は、カード決済時にスマートフォン(iPhone)に指をつけながら非接触装置にタップするもので、米国をはじめとして英国、豪州、中国、そして2016年に日本でリリースされました(腕時計のApple Watchは、本人のiPhoneと電波でリンクしている限りは指紋不要)。

iPhoneおよびAndroid端末などで広く生体認証を利用できるようにするために、Google、PayPal、Samsungなど100社以上が参加する標準化団体「FIDO Alliance (Fast IDentity Online Alliance)」は、モバイル端末と指紋認証の標準仕様「FIDO 1.0」を規定しました。これにより、指紋情報の管理をデバイスから出さないなどの生体認証の標準仕様が採用されていくと推測します。

(2)カード番号そのもののブロック手法 :カード番号のトークナイゼーション

2016年5月、全国のコンビニATMから一斉にカード不

表1. モバイル決済の種類と特性

モバイル決済の区分	利用者のモバイル端末	店舗側の読取方法	利用可能な店舗	決済用インターフェースの標準化対応	決済事例
①スマホアプリ決済	スマートフォン	POS接続のバーコードリーダー等でスマートフォンに表示された利用者の情報を読み取り	少ない(小売店単位に個別のアプリ仕様)	なし	スターバックス、CurrentC
②-1モバイル決済(NFC仕様)	iPhone 6以降、NFC対応おサイフケータイ等のAndroid端末	NFC(Type-A、Type-B)リーダーで、非接触でカード情報を読み取り	少ない(イクスピアリなど対応端末が限定的)	EMVCoによるカード決済の標準仕様あり	Apple Pay、Andoroid Pay、Samsung Pay、PayPass、PayWave
②-2モバイル決済(FeliCa仕様)	iPhone 7(FeliCa仕様)、FeliCa対応おサイフケータイ等のAndroid端末	FeliCaリーダーで、非接触でカード情報を読み取り	多い(コンビニ、スーパー、駅内など)	FeliCaは国内市場における電子マネーの標準	Apple Pay、Suica、iD、QUICPay、楽天Edy、nanaco、WAON

正による現金引き出しがあり、海外の特定銀行の口座からわずか数時間のうちに、およそ18億円もの被害がありました。偽造団による犯罪で、デビットカードのカード情報の漏えいによる、偽造カードによるキャッシング不正です。個人の暗証番号はハッキングでシステム迂回されて現金が引き出されました。この例のように、カード番号は小さな利用店舗の端末からリテーラーのPOSデータベース、インターネット販売企業等に散らばり絶え間なく不正利用があるため、VisaやMasterCardといったブランドでは、カード情報を流出させた加盟店や企業に被害額を課すという方針転換（ライアビリティー・シフト）が行われました。米国では2015年から、日本でも2017年から、まずATM利用取引からのライアビリティー・シフトが開始されます。

これに関連して、カードに記載される16桁のカード番号（PAN）の不正取得そのものを防ぐため、乱数などでカード番号とは別の固有番号に置き換える「トークナイゼーション（トークン化）」という技術が使われ始めています。モバイル端末とカード発行会社や銀行との間では、カード番号（PAN）の代わりに固有のトークン番号でやり取りすることで、万一このトークン番号が不正行為で漏えいしてもカード番号は漏えいされないというものです。

トークナイゼーションの技術は、2014年に国際カードブランドによる共同設立機関「EMVCo」が制定するEMV標準として、「決済トークナイゼーション仕様書 - 技術フレームワーク[4]」が定められました。そして同年10月、iPhoneのモバイル決済「Apple Pay」が、商用としてこのトークナイゼーションを正式採用し、それに合わせてカードブランドのVisa、MasterCard、AMEXが米国でトークナイゼーションのサービス提供を開始しました。翌2015年には「Android Pay」「Samsung Pay」のモバイル決済においても、トークナイゼーション技術が採用されました。モバイル端末にカード番号を保持することなくモバイル決済を行うことで、モバイル端末から決済ネットワークまでカード番号の漏えいを防ぐことができるため、セキュリティー効果が高い手法だと言えます。

4. トークナイゼーション技術とトークン変換の流れ

ここではモバイル決済の主要スキームに採用され、国際カードブランド認定機関でEMV標準化された決済トークナイゼーションの仕様とそのトークン変換の仕組みについて解説します。

(1)決済におけるトークナイゼーションの流れ

顧客がクレジットカード支払いをする際に、いくつかの箇所でカード情報が漏えいする可能性があります。カード支払いでは、カード加盟店の店舗は顧客から代金を受け取る代わりにカード情報を受け取り、このカード情報および決済情報をカード会社に送付することで、カード会社から代金を受け取ります。スマートフォン～店舗POS～アクワイアラー（加盟店管理会社）～決済ネットワーク～カード発行会社とカード情報が伝わっていく過程で、カード情報が第三者に漏えいするリスクが生じます（**図1**上図）。

これに対してEMV仕様のトークナイゼーションを採用した場合、クレジットカード番号やデビットカード番号などのカード情報をトークンに置き換えてカード決済されます。スマートフォンから決済ネットワークまで、カー

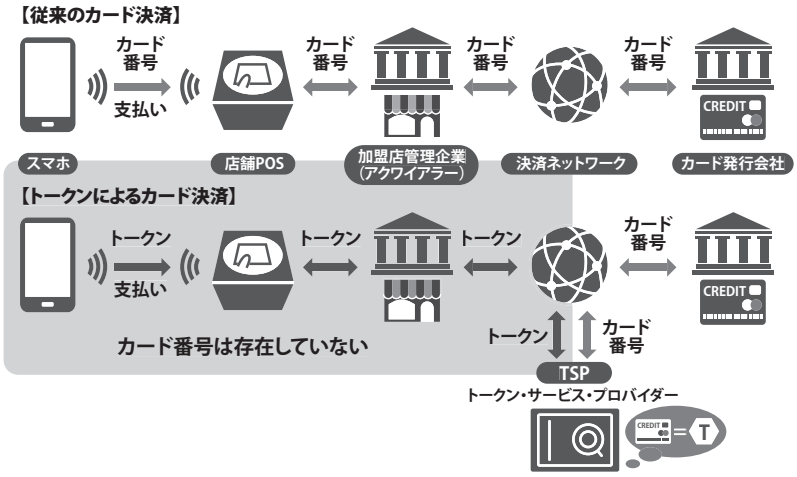

図1. 従来のカード決済の流れとトークンによるカード決済の流れ

図2. カード番号とトークン番号の発行例

ド番号でなくトークンがやり取りされます。**図1**下図の「トークン・サービス・プロバイダー(TSP)」は、トークン番号の関係が分かるため、アクワイアラーからのトークンがカード番号に置き換わってカード発行会社に伝わるためカード決済ができるのです。

EMV仕様のカードのトークン番号の発行例を**図2**に示します。カード番号16桁のうち最初の6桁は、カード発行会社に固有に割り振られた範囲(BINレンジ)と共通の番号をトークンに割り振ります。BINレンジを共通にすることで、加盟店やアクワイアラー、決済ネットワークにおいて、どのカード発行会社のカードかが分かります。このように、従来のカード番号体系を維持させることで、加盟店からアクワイアラー、決済ネットワークにおいて、本物のカード番号かトークンかを意識せずに処理できるようにしています。

2016年10月、日本でリリースされた「Apple Pay」では、EMV仕様のクレジットカード決済に加えて、国内の電子マネーの標準であるFeliCa仕様の「Suica」「iD」「QUICPay」決済にて、トークナイゼーション技術を採用しました。指紋認証「Touch ID」とともに、利用者の利便性とセキュリティーの強化を実装して、モバイル決済に進出しました。

(2)トークン・サービス・プロバイダーの役割と機能

ここまで、カード番号とトークンの番号の変換を行う役割として、トークン・サービス・プロバイダーについて紹介してきました。ここでは、トークン・サービス・プロバイダーに必要なそのほかの役割と機能について解説します(**表2**)。

①トークン発行

カード保有者のモバイル端末からのカード登録要求に基づいて、モバイル決済スキーム会社、およびカード発行会社とオンラインAPI接続にて、本人情報やカード状況を確認(ID&V)の上、モバイル決済用のトークンを発行します。このトークン発行ではどうしてもカード番号を含むカード情報が連携されるため、トークン発行のAPI接続の相互認証には、厳重な暗号化手法を用いる必要があります。

②ID&V(Identification & Verification)

トークン発行要求の際に、カード保有者の確認を行う機能を提供します。ID&Vおよびトークン発行までの処理フローでは、カード番号を含むカード保有者情報が連携されるため、トークン発行のAPI接続の相互認証には厳重な暗号化手法を用いる必要があります。

③オーソリゼーション/売上処理でのトークン変換(De-Token)

トークンによるカード決済の流れで示したように、モバイル決済のタイミングでオーソリ処理や売上処理のために、トークンとカード番号を紐付けしたマッピング情報によりリアルタイムに変換する基本機能で、トークンからカード番号に戻すことを「デトークン(De-Token)」と呼びます。クレジットカードの利用は休日・夜間を問わないため、デトークンは24時間365日無停止の可用性が求められます。

④トークンのライフサイクル・マネジメント

トークンのライフサイクル・マネジメントは、発行済トークンのステータスや情報の更新を行う管理機能です。日本のカードは、クレジットカードに電子マネーが付帯されて1枚のカードになっていることも多く、その関連を含むサービス利用者の利便性の考慮が必要となります。

表2. トークン・サービス・プロバイダー(TSP)の主な機能

区分	機能	説明	接続方法
基本機能	①トークン発行	モバイル端末のカード登録要求に対して、モバイル決済スキーム、カード発行会社と連携して、トークン発行する機能	API機能、バックエンド機能
	②ID&V(Identification & Verification)	カードホルダーの本人確認、カード状況の確認等を実施する機能	API機能
	③オーソリゼーション/売上でのトークン変換(De-Token)	加盟店POSなどの支払いにおけるオーソリゼーション、および売上の際に実施されるデトークン処理	API機能
	④トークンのライフサイクル・マネジメント	カード番号および発行済トークンのステータス管理や情報更新を行う管理プロセス	バックエンド機能
拡張機能	⑤カスタマー・サービス・ポータル	利便性のため端末やカードの利用停止・再開およびカード情報の更新に伴うトークンのステータスを変更するための操作画面	ポータル画面
	⑥プロビジョニング用アプリの提供	カード発行会社専用のプロビジョニング用のアプリの提供	アプリ形態

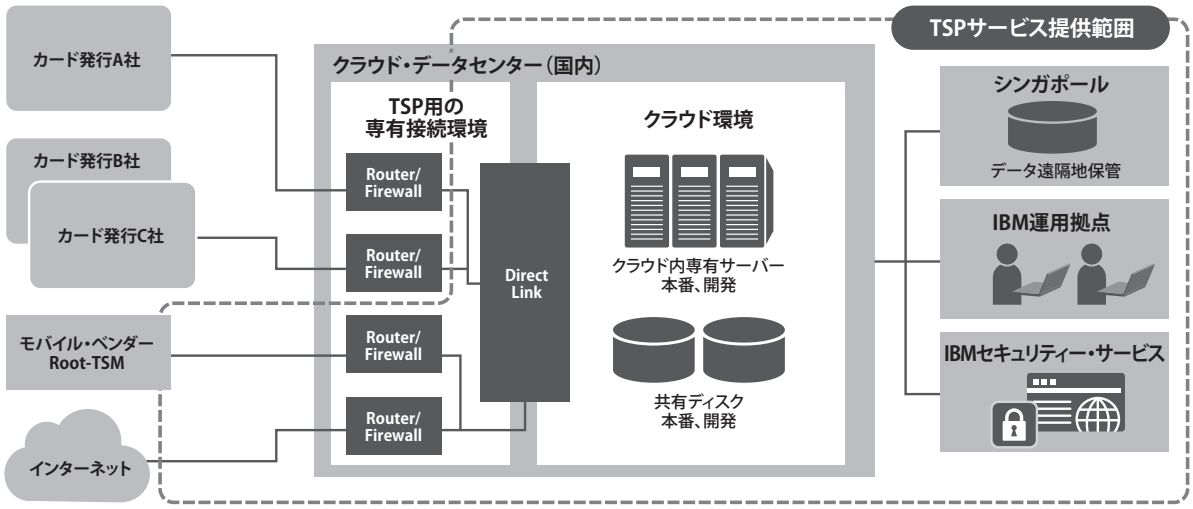

図3. クラウド利用による日本IBMのTSPデータセンター

登録端末の紛失やカード本体の利用停止・再開、およびカードの更新に伴いトークン情報の保管庫（トークンボルト）のステータスを変更するAPI機能です。

⑤カスタマー・サービス・ポータル

カード会社のオペレーターが、登録端末の紛失やカード本体の利用停止・再開、およびカードの更新に伴うトークン情報の照会、ステータスを変更する操作画面のポータル機能です。

⑥プロビジョニング用のアプリの提供

モバイル提供の標準ウォレット画面のカード登録でなく、カード発行会社のアプリとして、カード会社のWebシステムなどとID認証を行い本人確認までを連携するモバイル用アプリの機能です。

ここで発行されたトークンボルトは、モバイル端末の登録者のトークンとカード番号のマッピングが保管されていることから、高度なセキュリティー基準下で管理・運営される必要があります。

Visa、MasterCard、AMEXなどの国際ブランドは、それぞれのブランドのトークン・サービス・プロバイダー機能を提供していますが、国際ブランドごとにAPI接続が必要となる上にそのブランドのトークン発行のみとなるため、付帯する電子マネーのトークン発行を含んだ運用管理が複雑となります。

日本IBMは2016年10月、モバイル決済のトークン・サービス・プロバイダーとして、EMVCo、およびPCI DSS[5]認定取得に加えて、採用カードの各ブランド認定、FeliCa仕様の電子マネー発行会社の認定を取得し、共同利用型のTSP事業サービス（**図3**）を開始しました[6]。

このトークン・サービス・プロバイダーとしての機能は、公益財団法人金融情報システムセンターが発行するFISCのセキュリティー基準で運営されるIBMのクラウド基盤上で構築され、今後の電子マネー、モバイル決済取引の急速な拡大や利用ケースの多様化に柔軟に対応するインフラ・アーキテクチャーで提供されています。

5. モバイル決済の将来

既に、ショッピングでのカード支払い、コンビニや駅の改札での電子マネーによる非接触決済は日常となっています。Apple Payに加えて、Android Payなどのモバイル決済のスキームも、欧米からアジアの各国に展開されつつあります。MasterCardやVISAは、2020年のオリンピック開催までにICカード仕様かつモバイルNFC（Type-A、Type-B方式）の端末100%化を目標として推進しています。

財布にプラスチックカードを入れて持ち歩くことはなくなり、利用カードをスマートフォンで選択し、NFCリーダーやアプリで簡単に、かつ生体認証や位置情報の確認などで安全に決済できるようになると予想されます。

近い未来、そうしたモバイル決済を取り巻く環境変化に対して、企業はどのような変革が必要なのでしょうか。**図4**に、決済のデジタル化、オンライン／オフラインの収束化、顧客行動のためのビッグデータ利用の変遷予測を示します。モバイル端末所有の日常化・一般化は、単

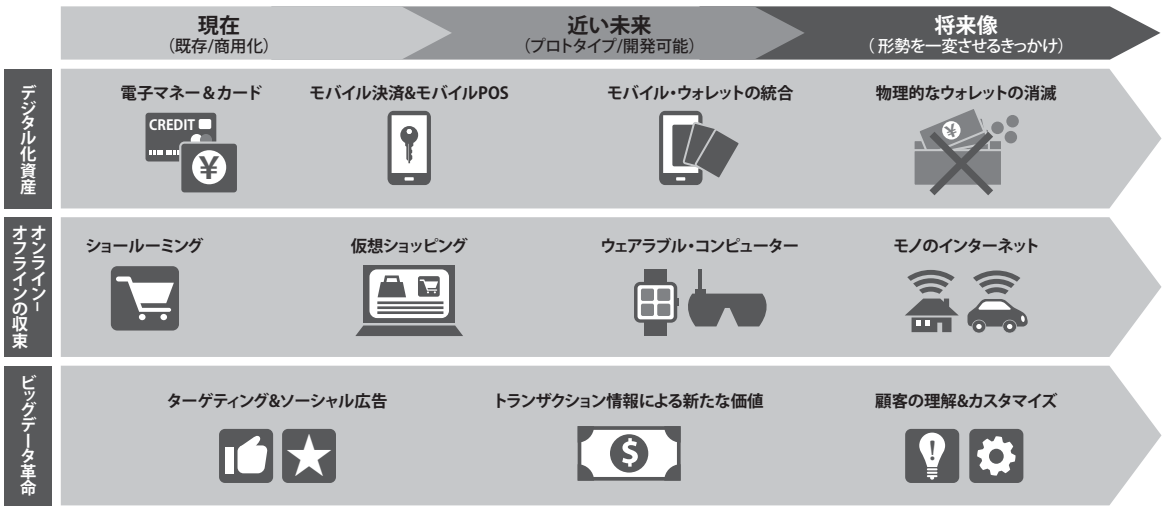

図4. 今後の決済と顧客購買の方向性

なる使いやすいモバイル決済の枠を超えて、顧客の購買行動から決済方法、さらには顧客のパーソナライズ化に向かうと考えられます。

こうした中で、企業がとるべき対応の1つ目のポイントは、企業が顧客との接点強化を行って、顧客の決済情報を把握することから、より親密な関係を強化することでしょう。また、2つ目のポイントは、購買の元となるリテーラー、決済会社、FinTech企業とアライアンスを組むことで、顧客が利用したいと望んでいる購買や決済のエコシステムに加わることです。

具体例としては、次のような強化施策が考えられます。

- 自社または企業グループのモバイル・ウォレット展開による顧客エンゲージメント／顧客接点の強化
- 顧客の決済・購買情報の把握と、顧客のカスタマイズ化・パーソナライズ化
- 顧客の便利な購買その他のサービスを目的とした、外部企業やFinTech企業とのエコシステムの強化

使い勝手の良い各種カード商品の発行に加えて、その決済手法の便利さの向上を図りつつ、さらに顧客が利用したいと望む購買や決済方法となるよう多方面の企業と連携してエコシステムを築いたり、顧客の購買情報の把握・分析からカスタマイズをすることで、顧客との関係を根本的に転換することが求められていきます。

6. おわりに

本稿では、カードや電子マネーによるモバイル決済の最近の状況とその種類、特性について紹介しました。さらに、近年、決済の安全性を保つ仕組みとしてEMV標準となり、モバイル決済のグローバル展開のスキームで採用が始まっている「決済トークナイゼーション」のトークン技術とその変換の仕組みを解説しました。

今後もIBMでは、カード決済に限らず個人間や企業間を含むさまざまな金融取引や決済の利便性と安全性を高めるために高度なセキュリティー・サービス事業や金融取引のソリューションを深化させて、皆様に提供し続けてまいります。

[参考文献]
[1] Bank 3.0 ブレット・キング. 上野博（訳）, 脱・店舗化するリテール金融戦略 , 東洋経済新報社（2015）
[2] 総務省: 平成27年通信利用動向調査, http://www.soumu.go.jp/main_content/000445736.pdf（2016）
[3] 株式会社三菱総合研究所 MRIマンスリーレビュー 2015年4月号 数字は語る10% - 成長続ける非現金決済市場, http://www.mri.co.jp/opinion/mreview/number/201504.html(2016)
[4] EMVCo:EMV Payment Tokenization Specification - Technical Framework, https://www.emvco.com/specifications.aspx?id=263(2014)
[5] PCI Security Council: PCI DSS Tokenization Guidelines, https://www.pcisecuritystandards.org/documents/Tokenization_Guidelines_Info_Supplement.pdf（2011）
[6] 日本IBM：Apple Payがもたらす変革-IBMのトークナイゼーション・サービスにより、Apple Payでの決済が簡単に, http://www.ibm.com/services/jp/gbs/mobile-consulting/apple-pay/(2016)

日本アイ・ビー・エム株式会社
グローバル・ビジネス・サービス事業
銀行・FMサービス事業部 決済トランスフォーメーション
インダストリー・スペシャリスト、シニア・アーキテクト

小宮山 光雄
Mitsuo Komiyama

1988年日本IBM入社。銀行・カード会社など金融担当のエンジニアとして、SOAオープン基幹系システム、24/365高可用性決済系のプロジェクトにアーキテクトとして従事。2011年より、金融の業界ソリューションの組織に異動。現在は、トークンサービスや決済系ソリューション、およびFinTechカード共通APIなどの活動を行っている。