世界にひとつ。あなたにひとつ。

W3CのPayment関連活動の概要

2018年6月

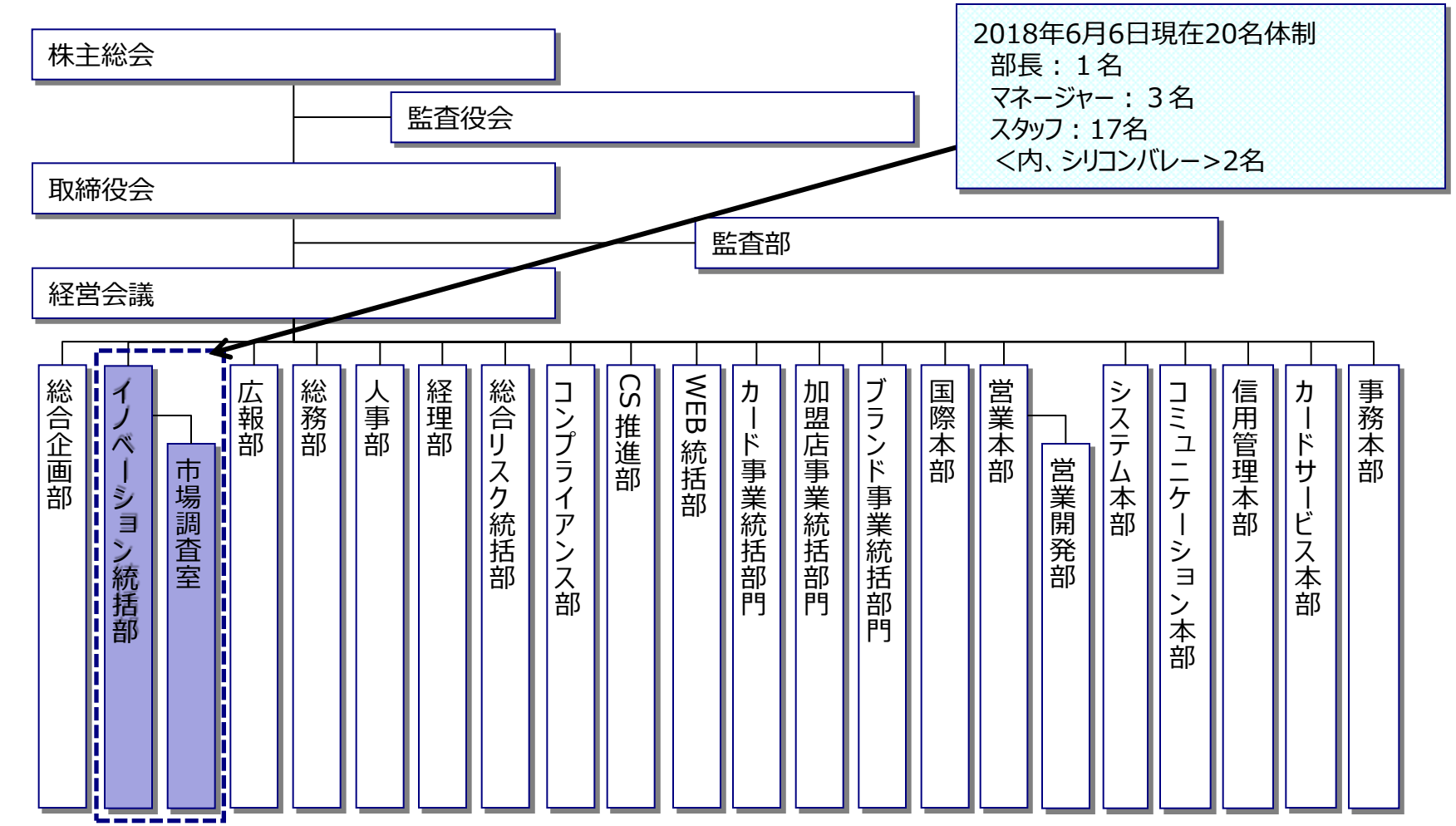
株式会社ジェーシービー

イノベーション統括部

※本資料は株式会社ジェーシービーとしての見解、意見を
表明するものではありませんので、ご留意ください

JCB イノベーション統括部のご紹介

R & D機能の強化に向けた組織改編としてテクノロジー等を活用した全社横断的なイノベーションの推進を企図



2020年のありたい姿

JCBをイノベーション体質の企業体に変革。
テクノロジーから強みを生み、ビジネスを進化させる。

JCB イノベーション統括部のご紹介

「全社R&Dの旗振り役」として、テクノロジー等を活用した全社横断的なイノベーションを推進するとともに、従来とは異なる新たなビジネスモデルの検討を進めている。

主なミッション

R	調査・研究	**高度なリサーチ活動実践による「洞察」** ・国内外の技術・市場についての最新動向調査・分析および将来予測・影響考察 ・重点イノベーション領域に対する、実効性を備えたシーズ探索と、具体的ニーズ掘り起し （VCを通じた出資案件等の調査を含む）

→ **市場調査室**

D	企画・統括・推進	**全社横断的なイノベーション促進による「攻め」** ・内外環境に即した重点イノベーション領域の見極め、選定 ・当社イノベーション戦略立案、戦略の全社統括・推進 ・オープンイノベーション促進 ・データビジネスの戦略立案・推進 ・全社イノベーション推進態勢構築 （仕組み／ヒト／意識）

→ **企画グループ**　**開発グループ**

R&D	研究・推進	**ビジネスモデルチェンジへの「備え」** ・将来想定されるコマース環境の変化を見据え、既存の事業体・アセットにこだわらず、当社の新たなビジネスモデル像を検討

→ **市場調査室・企画グループ**

JCB イノベーション統括部のご紹介

当社では、2017年度より4ヵ年の中期経営計画【Ｐｌａｎ　２０２０】に取り組んでおり、基本方針の1つに「ビジネスの進化・変革への挑戦」を掲げている。当部では、中期経営計画と前頁記載のミッションに基づき、「エンドユーザー様」「加盟店様」「社内事務」に関する短期課題と、将来に亘る中長期課題を設定し、検討すべき主要テーマを定めている。

重要課題

短期						中長期	
A	顧客接点の強化	B	加盟店向け 機能・サービスの強化	C	社内事務の効率化・ 高度化	D	新たなビジネスモデル・ 事業基盤の構築

主要テーマイメージ

先端技術を駆使して、エンドユーザー様へ「心地よい決済」の提供を目指す	・「安全」「安心」な取引を実現するためのセキュアな環境構築を目指す ・加盟店様への新たな価値提供を目指す	・AI等を用いて社内事務のプロセスを革新し、低コストと共に業務品質向上を目指す ・全社的なデジタル変革によるコスト削減、ワークスタイル変革を目指す	当社データベースやネットワークインフラなどを活用・応用した新たなビジネスモデル・事業基盤構築を目指す
Ex.) モバイル決済、API活用、 チャットボット、生体認証　など	Ex.) 不正取引検知、 店舗支援ソリューション　など	Ex.) RPA、OCR、チャットボット、 予測業務自動化など	Ex.) 新たなフィービジネス、 新たな決済インフラ、VC出資 など

W3CのPayment関連活動の概要
Web Paymentに間する主要WG,IG

Web Payment WGが「至近の課題への対応」、Web Commerce IGが「将来的な課題の洗い出し」というように、時間軸の差異でWGとIGの検討内容を分けている。

	グループ名	主目的	Chair
Working Group (WG)	• **Web Payment WG**	• Payment Request APIなど、Web Paymentに関するフローやデータセット、API等の標準化を進める。 • 個別の課題はTask Forceを組成して対応。(※現在のTask ForceはTokenizationと3D Secure)	• Worldpay • Ripple
Interest Group (IG)	• **Web Commerce IG** (旧Web Payment IG)	• もともとは純粋にPaymentに関する将来的な議題を取り扱い、ユースケースの研究や課題の洗い出しを行う場であったが、Offering（例えばクーポン）など、Paymentに紐付くCommerce周りの議題やIoT周りの議題も扱うようスコープが拡大。	• Amex • Alibaba • NACS(The Association for Convenience & Fuel Retailing

W3CのPayment関連活動の概要
Web Payment　WGの主な参画企業

GoogleやMicrosoftなどブラウザを手掛ける企業と、国際ペイメントカードブランドが主な参加者になると考えられがちだが、Rippleが”Chief Standardization Officer”のAdrain HBをほぼ専担者として置き、積極的に活動を行っている点が特徴として挙げられる。

IT事業者（ブラウザ、OS等）	• Google • Facebook • Apple	• Microsoft • Mozilla • Opera
決済周辺プレイヤー（EC/Payment Service Priovider）	• Alibaba • AirBnB • Samsung Pay	• WorldPay • Stripe
国際ペイメントカードブランド	• Mastercard • Visa • American Express	• JCB • Discover
仮想通貨等	• Ripple	

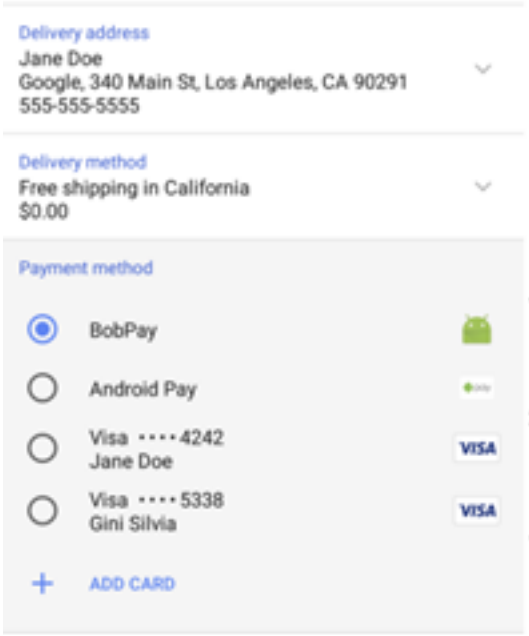
W3CのPayment関連活動の概要
W3C内の関連するWG

- 至近では特に決済における本人確認強化の流れ（後述）を受け、Web Authentication WGとの関係が特に重要視されている。
- 今年4月のWeb Payment WGの会合（シンガポール）でも、Web Authentication WGとの取り組み強化の方針を改めて確認。

	グループ名	主目的	Chair
Working Group (WG)	• **Web Authentication WG**	• 「Web認証仕様」の標準化を目指す。（主にFIDO2の仕様を参照）	• Yubico • Microsoft
	• **WoT (Web of Things) WG**	• IoTにおいて発生するSecurity / Interoperability / Connectivityなどの懸念（特にサイロ化による分断）の解決を目指す。	• Siemens • Panasonic • Intel
	• **Verifiable Claim WG**	• 資格や成績などの属性のデジタル証明を保存、送信、受信ができるための標準化や相互運用性の実現を目指す。	• Pearson • ETS
	• **Automotive WG**	• IoT時代の入り口として、データセットの標準化/APIの仕様策定により相互運用性の実現とオープン化を目指す。	• Jaguar Land Rover • 三菱電機（米）
	• **Web VR WG**	• VRに関するブラウザレベルのAPIの仕様策定を行う。	• Intel • TBD

W3CのPayment関連活動の概要
Web Payment WGの最近の動向①：Payment Request API

- Payment Request APIは要約すると「決済に係るフォーム入力に関する部分を代替する」機能。
- あくまで決済処理を行うための機能ではなく、決済を行うのに必要となる各種情報を、決済代行業者などにスムーズに受け渡すためのもの「橋渡し」をしている。
- ここが標準化されることで、加盟店（イーコマースのサイトなど）が決済に係る機能を簡単に実装できるようになると共に、ユーザーが決済に係る情報を入力する「手間」を省くことによって、イーコマースでのCVRの改善を見込むことが出来る。




```
const methodData = [
  {
    supportedMethods: "basic-card",
    data: {
      supportedNetworks: ["visa", "mastercard"],
      supportedTypes: ["debit", "credit"],
    },
  },
  {
    supportedMethods: "https://example.com/bobpay",
    data: {
      merchantIdentifier: "XXXX",
      bobPaySpecificField: true,
    },
  },
];
```

- フォームデータをStripe等の決済代行業者に受け渡し。
- 各社モバイルウォレットの他、クレジットカードを直接利用することも可能。
- 将来的には振込/振替、各種電子マネー、仮想通貨への対応も視野に入れている。

（出典）W3C、Google

W3CのPayment関連活動の概要
Web Payment WGの最近の動向②：セキュリティ強化に向けた対策

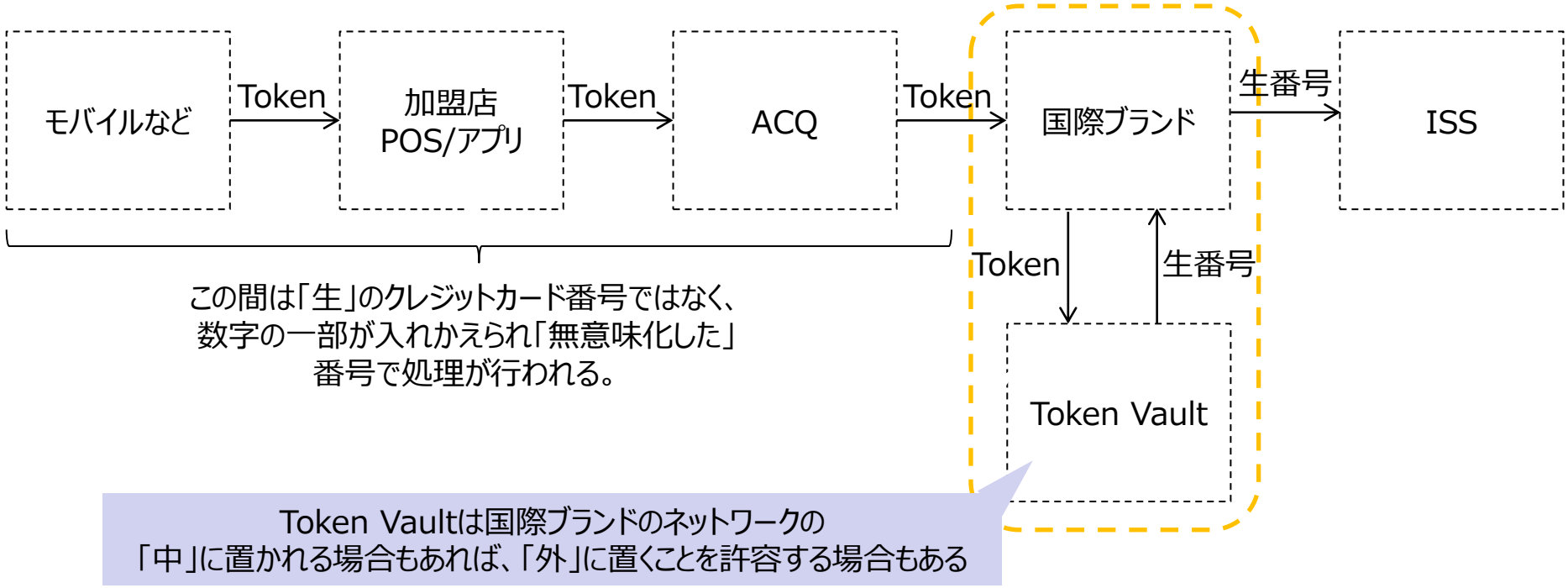
- カードペイメントに係るセキュリティ強化策として国際ブランドが提供しているものは主に以下の2点が存在するが、Web Payment WGでもこの2点についてはセキュリティ強化対策の一環として対応する動きとなっており、対応の為のTask ForceがWG内で設置されている。

	主な目的	概要
Tokenization	**「カード番号盗難」の防止**	• カード番号の一部を「でたらめな番号」に置き換え「無効化」することにより、カード番号を盗難された際の不正利用を防ぐ。 • 「無効化」された番号は、Token Vaultで元の番号に戻されてイシュアに渡される。 そこまでの処理は「無効化」された番号に基づいて行われる。
3D Secure	**「成りすまし」の防止**	• イシュアによる本人確認、国際ブランドによるイシュア/加盟店の正当性確認を追加。 • 3D Secure 1.0では（基本機能としては）ECでの毎決済時にパスワード（Static）の入力が求められていたが、CVRの低下要因となるという点から採用されないケースも多くみられた。 • その為2.0ではリスクベースの考え方を導入することで、成りすまし等の不正が行われている可能性が高い取引にのみ、パスワード(Dynamic/OneTime)の入力も求める方式にアップデート。

W3CのPayment関連活動の概要
【参考】Tokenizaionの仕組み

- 国際ブランド、もしくは国際ブランドが認定したToken Service ProviderがPayment Tokenを発行し、その番号を使って決済処理を行う。
  （カード番号の真ん中8ケタが、元の数字と数学的に全く関係性の無い数字に置き換えられる）
- TokenはToken Vaultで「元の番号」に戻され、その番号がカードイシュアに伝達されることで、カード決済が実行される。

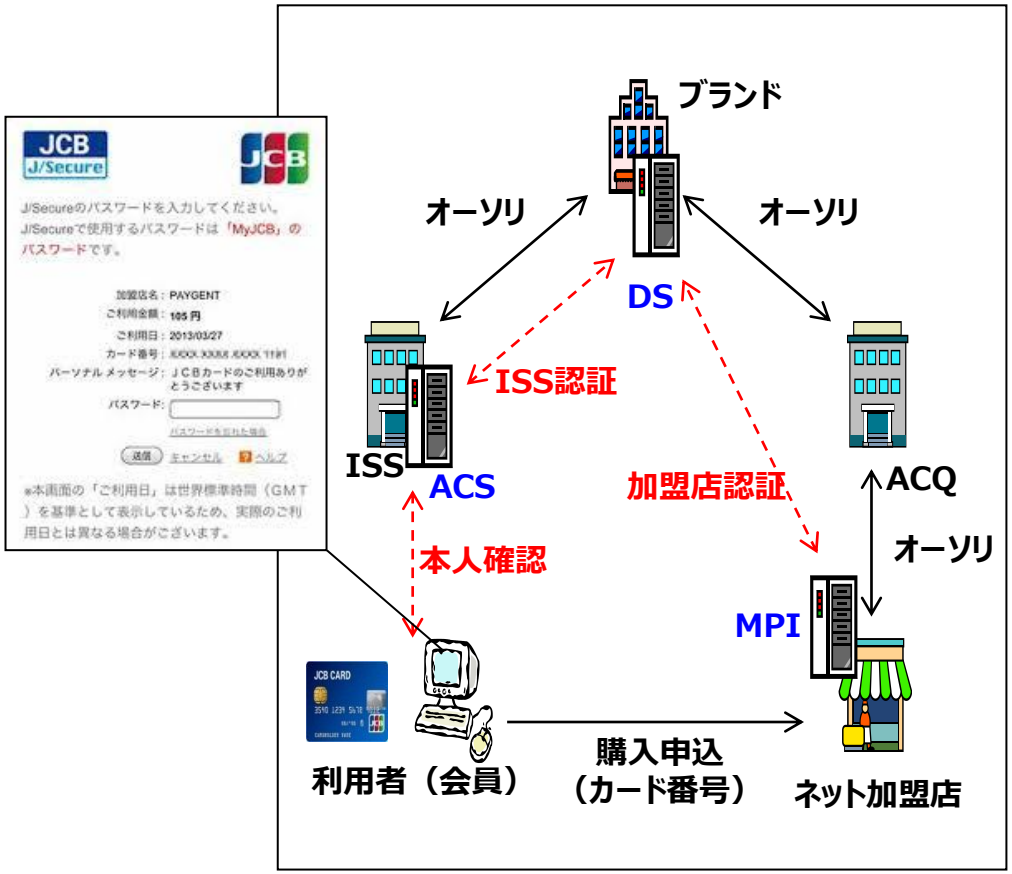
Tokenizationを利用する際のフローイメージ



W3CのPayment関連活動の概要
【参考】3D Secureの仕組み

- インターネット上での本人確認、正当性認証を強化した取引手段。
- 従来のオーソリ（ACQ **D**omain）に加え、ISSによる本人確認（ISS **D**omain）と、ブランドによるISS/加盟店の正当性確認（Brand **D**omain）を実施。　（⇒なので「**3D** Secure」という名称）

3D Secureのフロー概要



DS
(Directory Server)

- 各カードブランドが運営するサーバー
- 認証サービスに参加するカード発行会社と加盟店の情報を保持

MPI
(Merchant Plugin Server)

- 個人認証サービスを運用するにあたり必要になるプラグインソフトウェア
- 加盟店及びpayment gatewayのサーバーに導入が必要

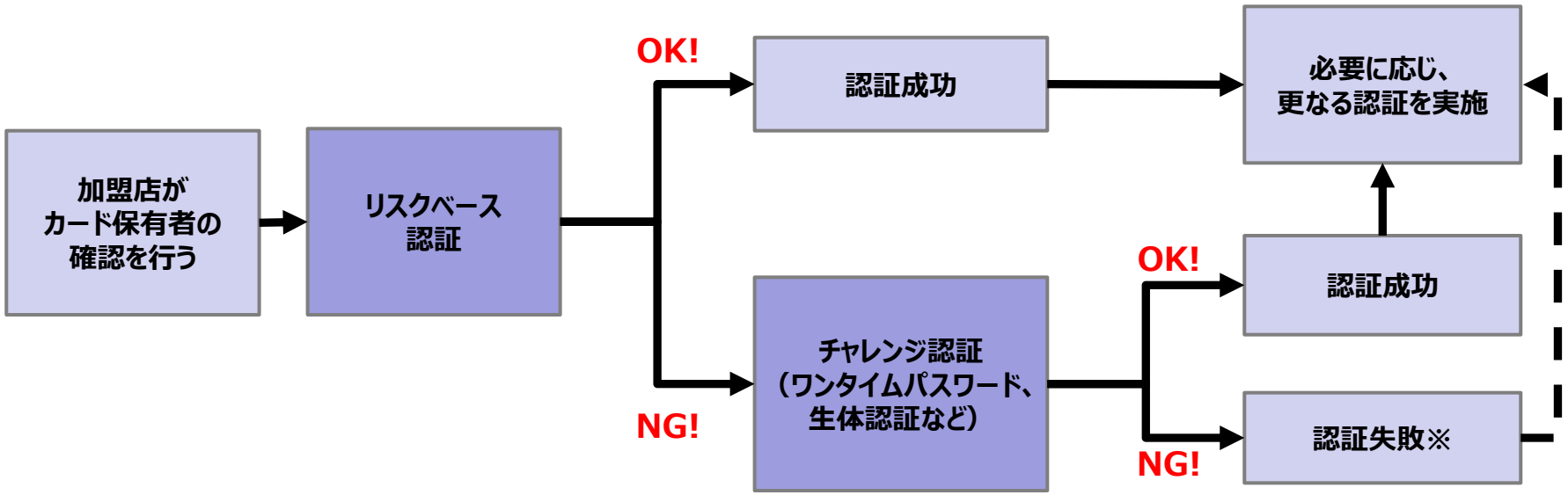
ACS
(Access Control Server)

- カードイシュア、又はプロセッサーが運営するサーバー
- 会員認証を行うために必要な情報の保持と、会員とのパスワード認証を実行

W3CのPayment関連活動の概要
【参考】3D Secure 2.0での大きな変更点

- 3D Secure 1.0では（基本機能としては）ECでの毎決済時にパスワードの入力が求められていたが、CVRの低下要因となるという点から採用されないケースも多くみられた。
- その為2.0ではリスクベースの考え方を導入することで、成りすまし等の不正が行われている可能性が高い取引にのみ、ワンタイムパスワード等の入力を求める方式にアップデート。
- また、1.0はブラウザでの利用を前提としていたが、2.0ではネイティブアプリにも対応。

3D Secure　2.0で想定する認証フロー



*場合により、違う認証要素を用いて再度認証のトライを行う

W3CのPayment関連活動の概要
欧州PSD2（第2次欧州決済指令）のRTSの概要

- EBA（欧州銀行監督機構）はPSD2に関するインターフェースの要件としてRTS（規制技術基準）を以下2項目に関して定めており、PSD2の対象となる決済および金融プロセスに関与する企業はこれに準拠することが求められている。（RTSは2019年9月から正式施行となる予定）
- PSD2では未準拠であることへのペナルティは各国法で規定されることとなる。（未準拠の場合は、罰金/域内ライセンスはく奪などのペナルティが科せられる）

	概要	
CSC (Common and Secure Communication)	• AISP(＝PFMなどの口座情報サービス提供者)、PISP（決済指図伝達サービス提供者）、CBPII（銀行以外のカードイシュア、主にデビットカードを想定）に対し、ASPSP（銀行など）のアカウントに対しアクセスすることを認める • ただし、その経路は安全で、かつデータはあらゆる局面で安全に保護されなければならない。	• APIに安全にアクセスし、活用するために、アクセストークンやeIDASなどを活用すべし
SCA (Strong Customer Authentication)	• アカウントに対してオンラインでアクセス、およびオンラインで支払指図等を行う場合には、強力な顧客認証手段を用いる必要がある。 • 認証に用いる要素は、少なくとも一つは再利用不可/コピー不可/インターネット等を通じた盗難不可のものを利用しなければならない。	• 原則、決済を行う際には独立した二要素による認証を行うべし • かつ、認証には上記を利用したワンタイムな認証コードを生成しなければならない。

W3CのPayment関連活動の概要
認証の3要素

- 前述のように、PSD2におけるSCAでは以下のうち、独立した2要素を組み合わせで、かつ少なくとも一つはワンタイムの認証コードを生成することが求められている。
- 例えば、非対面取引においてEMVで整備が進む3D Secure 2.0でSCAをクリアしようとする場合、「記憶」と「所持」（＝ワンタイムパスワード）もしくは「生体情報」による2要素認証の形を取ることが想定される。

認証の「3要素」

記憶 (Something you know)		• 本人のみが記憶しているデータに基づいて利用者を認証する方法であり、パスワード、パスフレーズ、PIN（Personal Identification Number）などがこれに当たる。 • これらの記憶データは他人に知られないようにしておかなければならない。
所持 (Something you have)		• 本人のみが所持している物によって利用者を認証する方法でありIC カードやスマートカード、ワンタイムパスワードのトークンなどがある。他人に貸与は厳禁。 • 所持物は紛失や盗難の危険性がある。紛失や盗難時の安全性のために利用に当たっては記憶要素と組み合わせることが多い。
生体情報 (Something you are)		• 本人の生体に基づくデータにより利用者を認証する方法であり、本人の特性としての指紋、音声、虹彩、顔の形などを識別することによる。 • この方法は本人に結びついたデータによるもので記憶忘れや所持物の紛失などの問題はない。

（出所）　独立行政法人情報処理推進機構
「オンライン本人認証方式の実態調査 報告書」

W3CのPayment関連活動の概要
RTSにおけるSCAの適用除外要件

- 前述のようにRTSでは原則二要素認証を推奨しているが、ユーザビリティにも配慮し、（RTSで定められている）トランザクションリスク分析を行っている前提で、「一定金額以下の金額については、SCAの対象外」とする規定となっている。（＝何が何でも二要素認証が求められているわけでは無い。）

	主な目的	1要素認証	1要素+リスクベース	2要素認証
アカウントへのアクセス（参照）	預金残高	○	○	○
	過去90日分の支払情報	○	○	○
	その他情報	×	×	○
アカウントへの支払指示（更新）	本人口座への送金	○	○	○
	無人端末での送金	○	○	○
	30ユーロ以下の送金	○	○	○
	500ユーロまでの送金	×	○	○
	500ユーロ以上の送金	×	×	○

W3CのPayment関連活動の概要
SCAをクリアするためのソリューションとしてのFIDO

- SCAをクリアするためには国際ブランドが準備する3D Secure2.0を用いる方法もあるが、全ての加盟店に対し対応を強制するものではない為、（ブランドとしては3D Secure2.0を用いて欲しい所ではあるが、用いない場合は）別の方法でSCAをクリアする必要がある。
- その為の有力な方法の一つとして、FIDOを用いた認証が挙げられる。
- FIDO仕様が一般化することで対応するソリューションが増加すれば、その分だけ「より強固な本人確認」を「より簡単」に利用することが可能になる。

fido ALLIANCE simpler stronger authentication

简体中文 English 日本語

What is FIDO? Blog Get Involved Search...

ABOUT TECHNOLOGY ADOPTION PARTICIPATE FIDO CERTIFICATION NEWS & EVENTS RESOURCES

FIDO Standards Provide Easy, Secure Way for European Payments Industry to Meet PSD2 Strong Authentication Requirements

September 20, 2017

The final draft Regulatory Technical Standards (RTS) on Strong Customer Authentication (SCA) under the revised Payment Services Directive (PSD2) mandates that financial institutions require multi-factor authentication for certain scenarios based on transaction amount and fraud level.

For a an industry that had been bracing for "old school" multi-factor authentication requirements that would have introduced unwanted friction into the online payment process, there is good news: with FIDO standards, you have an easy-to-deploy way to meet PSD2 SCA requirements, while meeting organizational and user demand for transaction convenience. In a paper released today, we detail exactly why and how. Read the paper, "FIDO & PSD2: Meeting the Needs for Strong Consumer Authentication," here.

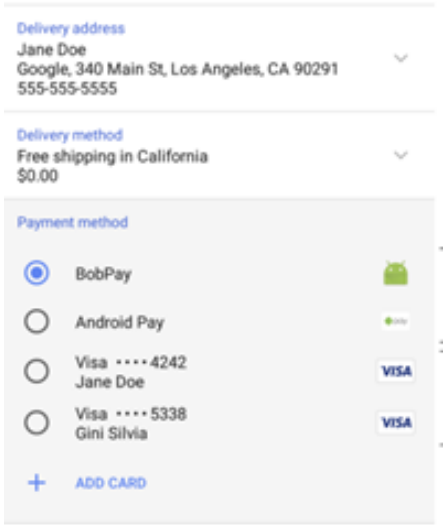
The final language in the regulation reflects a modern understanding of multi-factor authentication, thanks in large part to the outreach by FIDO Alliance and several of its members. Here's what is new and different in the final language and why payment service providers should be happy. While the final draft RTS requires two secure and distinct factors of authentication, it also recognizes that these factors can be housed in a single "multi-purpose" device – such as a mobile phone, tablet or PC – as long as "separate secure execution environments" are used (such as trusted execution environments (TEE), secure elements (SE) and trusted platform modules (TPM)).

（出典）FIDO Alliance

W3CのPayment関連活動の概要
W3C Web Payment WGでのデモ事例

- Web Payment WGの会議（@シンガポール）において、Web Payment とWeb Authenticationの具体的連携イメージとして、World Pay（UK）がYubico社のYubikeyを用いた2要素認証による支払のデモを実施。
- 今後、Web Payment ＷＧでは二要素認証対応/生体認証対応を利用するフローについてもPayment Request　APIでサポートを行う予定。

Web Paymentでの活用イメージ



支払方法を選択
（各種ウォレット、クレジットカード等）

パスワードを入力
（Something you know）

Yubikeyによる
ワンタイムパスワード入力
（Something you have）

この2段階で確実にSCAの要件をクリア

（出典）Google,Yubico

W3CのPayment関連活動の概要
最後に

- 「本人認証」は、対面取引/非対面取引両方で世界的に強化される傾向。
  ⇒**日本においても早晩、強化する方向に動くことが予想される。**

- 特に今後、決済も含め（API等を通じて）「銀行口座に直接アクセスする」ことが増加することになると考えると、「本人認証」はよりその重要性を増すことが予想される。
  ⇒**「安全」であることは前提として、よりサービスを広く利用してもらうためには、「安心感」をユーザーに持ってもらうことが重要。**
  ⇒**加えて「導入しやすさ」「使いやすさ」も必要。**

- **「導入しやすく」「使いやすい」FIDOのような仕組みが一般的に普及することで、より安全な決済が行われ、安心してショッピングを行うことが出来るようになることが期待される。**
  （そのためのWeb Payment, Web Authentication の取り組み）

世界にひとつ。あなたにひとつ。

ご清聴ありがとうございました

JCB 株式会社ジェーシービー