金融分野のTPPsとAPIのオープン化：セキュリティ上の留意点※

※TPPs（Third Party Providers）

FinTechフォーラム資料

2016年11月8日

日本銀行
金融研究所
情報技術研究センター
中村　啓佑

- 本発表に示されている意見は、発表者個人に属し、日本銀行の公式見解を示すものではありません。

情報技術研究センター（CITECS）について

- 日本銀行金融研究所では、金融業界が情報化社会において直面する新たな課題に適切に対処していくことをサポートするために、2005年4月に設立。
  - 主に、①国際標準化の推進、②金融業界内の情報共有体制の整備、③新しい情報セキュリティ技術の研究開発といった役割を担う。

- 最近の主な研究テーマ
  - FIDOの活用と安全性上の留意点
  - 生体認証システムのセキュリティ
  - スマートフォンを用いた取引認証

研究成果は、金融研究所ディスカッション・ペーパーとして公表するほか、情報セキュリティ・シンポジウムにおいても発表。
（URL: http://www.imes.boj.or.jp/citecs/）

第17回情報セキュリティ・シンポジウム
（2016年3月2日開催）

アジェンダ

- APIとは
- TPPsサービスとそのアクセス/認証方式
- 金融機関におけるAPIのオープン化と標準化
- 金融機関のAPIを活用したサービスのリスクと対策

（参考）

本発表の内容は、以下の論文に基づいています。

中村啓佑 「金融分野のTPPsとAPIのオープン化：セキュリティ上の留意点」

『日本銀行金融研究所ディスカッション・ペーパー・シリーズ』No. 2016-J-14、2016年

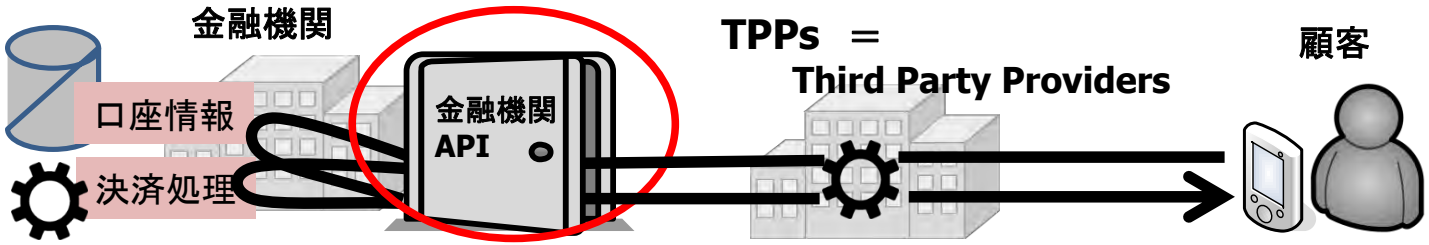
http://www.imes.boj.or.jp/research/abstracts/japanese/16-J-14.html

APIとは

- **API（Application Programming Interface）は、特定のプログラムを別のプログラムによって動作させるための技術仕様。**

APIの例

- 例1：インターネットを介し、Webブラウザに提供されるAPI
  —— 商店が所在地をウェブサイトで公開する際に、Google Maps APIを用いるケース
- 例2：金融機関からTPPsに提供されるAPI
  —— 顧客が、TPPsから提供された専用アプリを用いて金融機関APIを介して金融機関にアクセスするケース



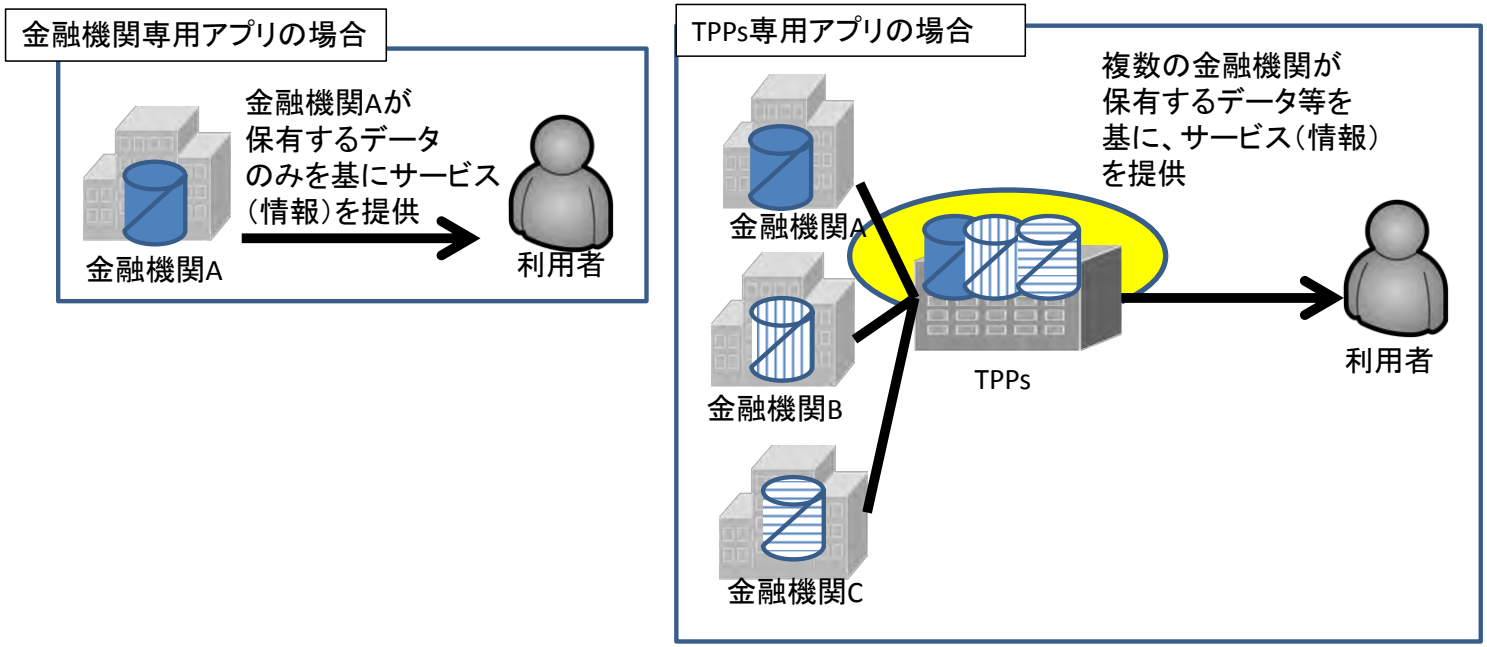
オープンAPIの形態（＊）

※ European Banking Association WG on Electronic Alternative Payments "Understanding the Business Relevance of Open APIs and Open Banking for Banks" を基に作成。

APIの形態	パブリックAPI	アクウェインタンスAPI	メンバーAPI	パートナーAPI	プライベートAPI
提供対象	不特定多数	資格を有する法人、個人	規範性のあるコミュニティ	個別契約締結先	会社内部
European Banking Association	←	対象		→	

TPPsサービスのアクセス方式と認証方式

- TPPsは、個々の金融機関よりも利用者の金融取引にかかる情報を多く保有するケースがある。



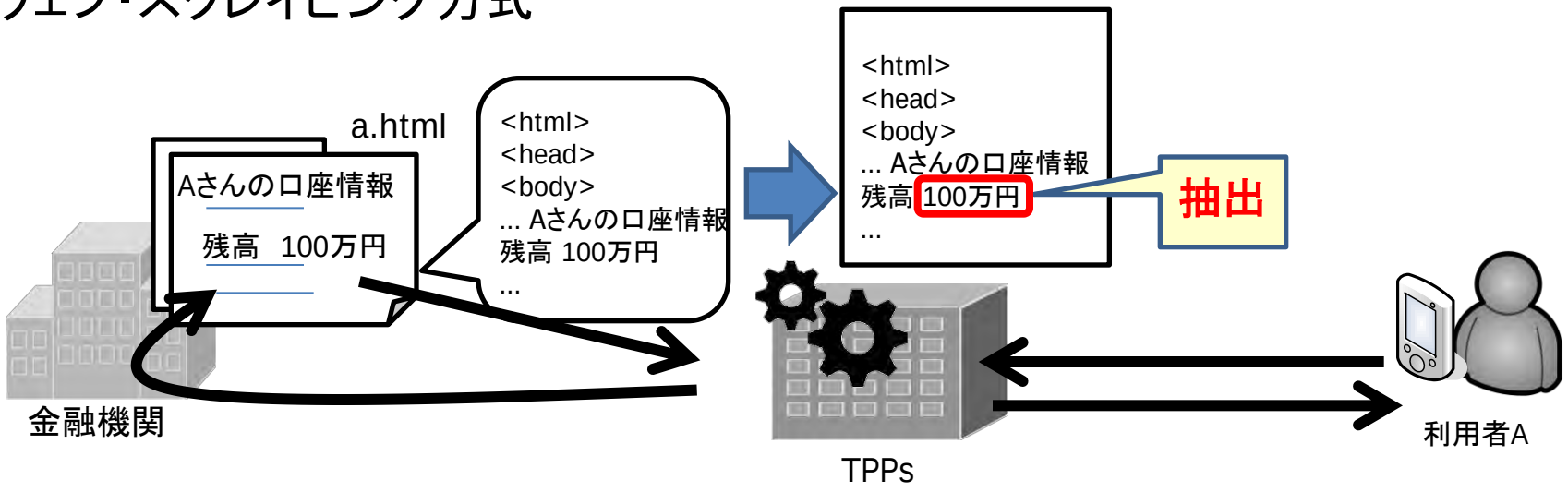
- 金融機関へのアクセス方式と認証方式は、2種類に大別される。

- サービス毎の組合せ

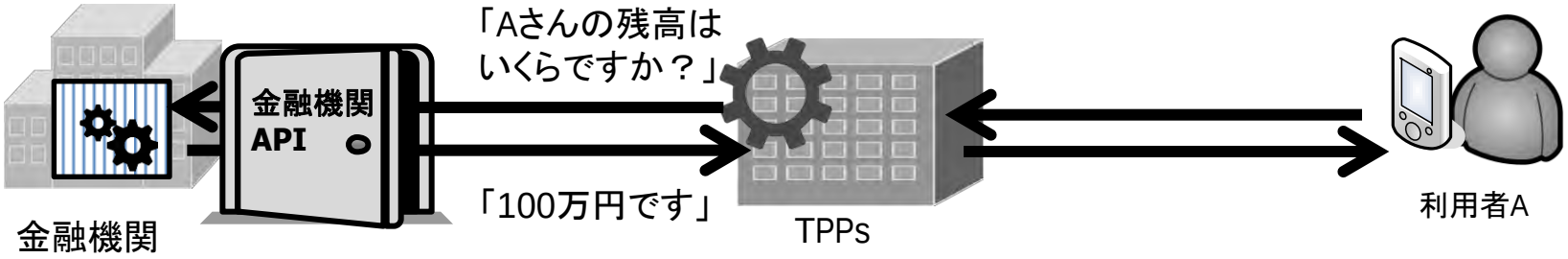
TPPsサービス	アクセス方式	認証方式
口座情報サービス（Account Information Service）	ウェブ・スクレイピング方式	レガシー認証（本人認証）
	API方式	トークン認証（本人認証＋認可）
決済指図伝達サービス（Payment Initiation Service）	API方式	トークン認証（本人認証＋認可）

ウェブ・スクレイピング方式とAPI方式

ウェブ・スクレイピング方式



API方式



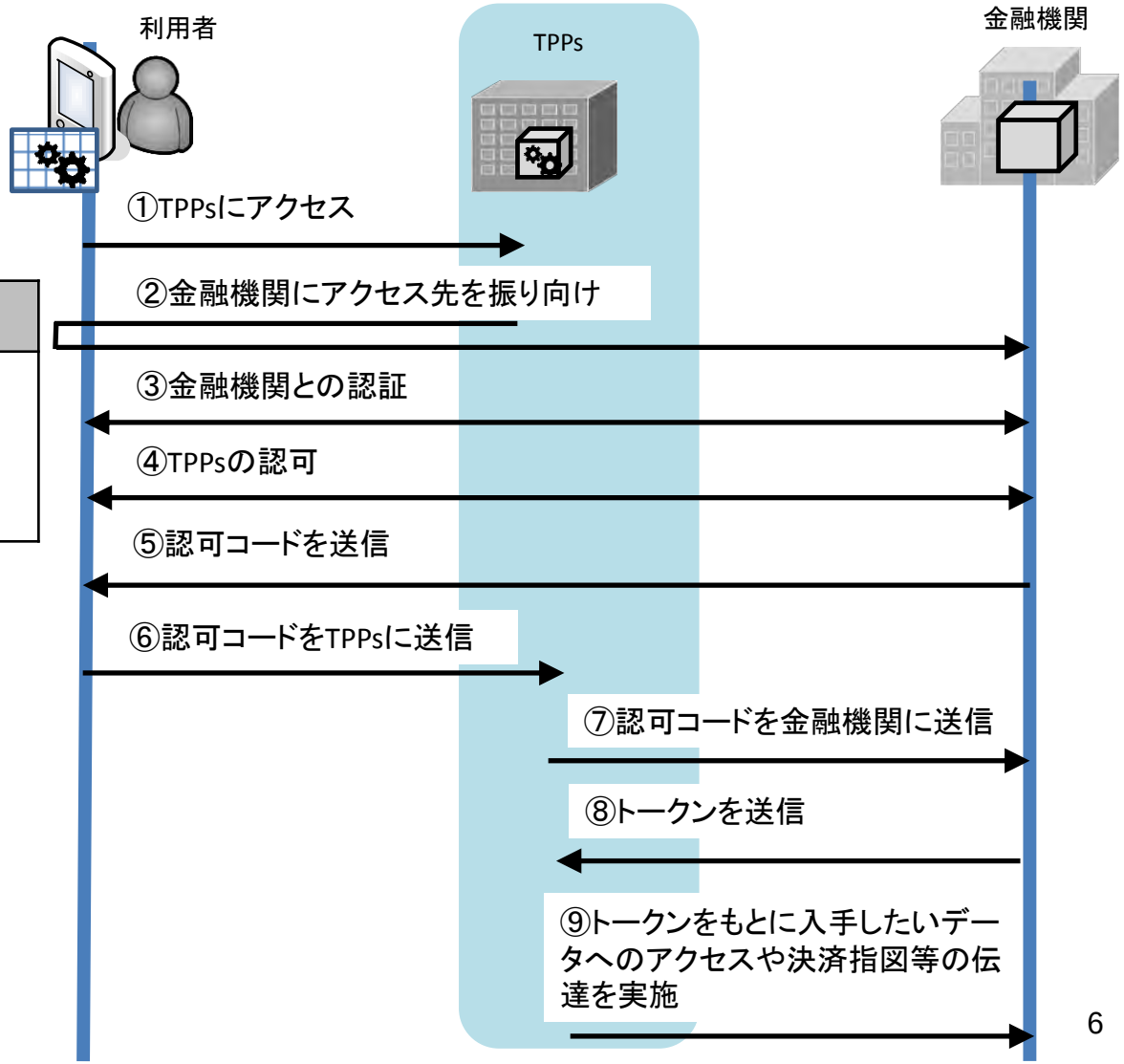
トークン認証（OpenID Connectのフロー）

- 利用者が、金融機関から認可コードを受領してTPPsに渡し、TPPsはそのコードを用いてトークンを取得し、金融機関から情報を取得、または金融機関に決済指図等を伝達する。

- OpenID Connectのほか、代表的なトークン認証の方式として、SAML（Security Assertion Markup Language）が存在する。

OpenID Connect	SAML
ウェブサイト間の信頼関係に関係なくID連携を実現可能	相互に信頼関係を結んだウェブサイト間でのみID連携が可能

※OpenID Connectは、OAuth2.0の機能を拡張し、更に認証を付加したプロトコル。



主なアクセス/認証方式の組合せにおける比較

アクセス/認証方式		（組合せ①） ウェブ・スクレイピング方式＋レガシー認証	（組合せ②） API方式＋トークン認証
金融機関	対応負担	• **不要**	• **必要** ―― APIを介した外部からのアクセスを可能とするように情報システムの更改が必要。
	認可によるアクセス制御	• **不可**	• **可能** ―― 金融機関および利用者が認めたデータのみにアクセスを制御可能。
TPPs	対応負担	• （組合せ②に比べて）**重い** ―― ウェブサイトのURLやレイアウトの変更の都度プログラム等の変更が必要。 ―― 利用者のID、パスワード等を管理する必要。	• （組合せ①に比べて）**軽い** ―― APIの変更の都度プログラム等の変更が必要。 ⇒ 変更頻度はウェブサイトよりもAPIの方が低いため、対応負担はAPIの方が軽い。 ―― 利用者のトークン管理が不要。（ただし、利用者のトークンを保有するサービスの場合、その管理が必要。）
	取得可能なデータ	• ウェブサイト上で提供されているものに限られる。	• 金融機関、利用者の同意が得られれば、ウェブサイト上で提供されないものも可能。
利用者		• 認可によるアクセス制御ができないID・パスワード等をTPPsに登録することによる不安が存在する可能性。	• トークンをTPPsに預ける場合でも、認可によるアクセス制御が可能であるため、組合せ①ほど不安感が高くない可能性。

金融機関におけるAPIのオープン化と標準化

オープン化のメリット：TPPsの新規参入の促進や金融サービスの品質向上等

―― APIを公開している金融機関の例

フィドール・バンク（独）、ビルバオ・ビスカヤ・アルヘンタリア・バンク（西）、クレディ・アグリコル・バンク（仏）等

標準化の検討状況

組織	状況
The Open Banking Working Group（英）	EU加盟国によるPSD2の実施に先んじてAPIのオープン化を推進。 ―― 英国の金融機関やTPPsの競争力を強化することが目的。
Open Bank Project（独）	金融サービスに活用できるAPIの雛形を作成し、国内の銀行に対して提供。
ISO/TC68（金融サービス）	・SC2（セキュリティ分科委員会）とSC7（コア銀行業務分科委員会）に、TPPsにかかるスタディ・グループを設置し2016年9月から検討を開始。 ・再編が検討されているなか、新しく設置することが検討されている分科委員会の検討項目の候補に、APIの標準化が挙げられている。

APIのオープン化に関する標準化の留意点

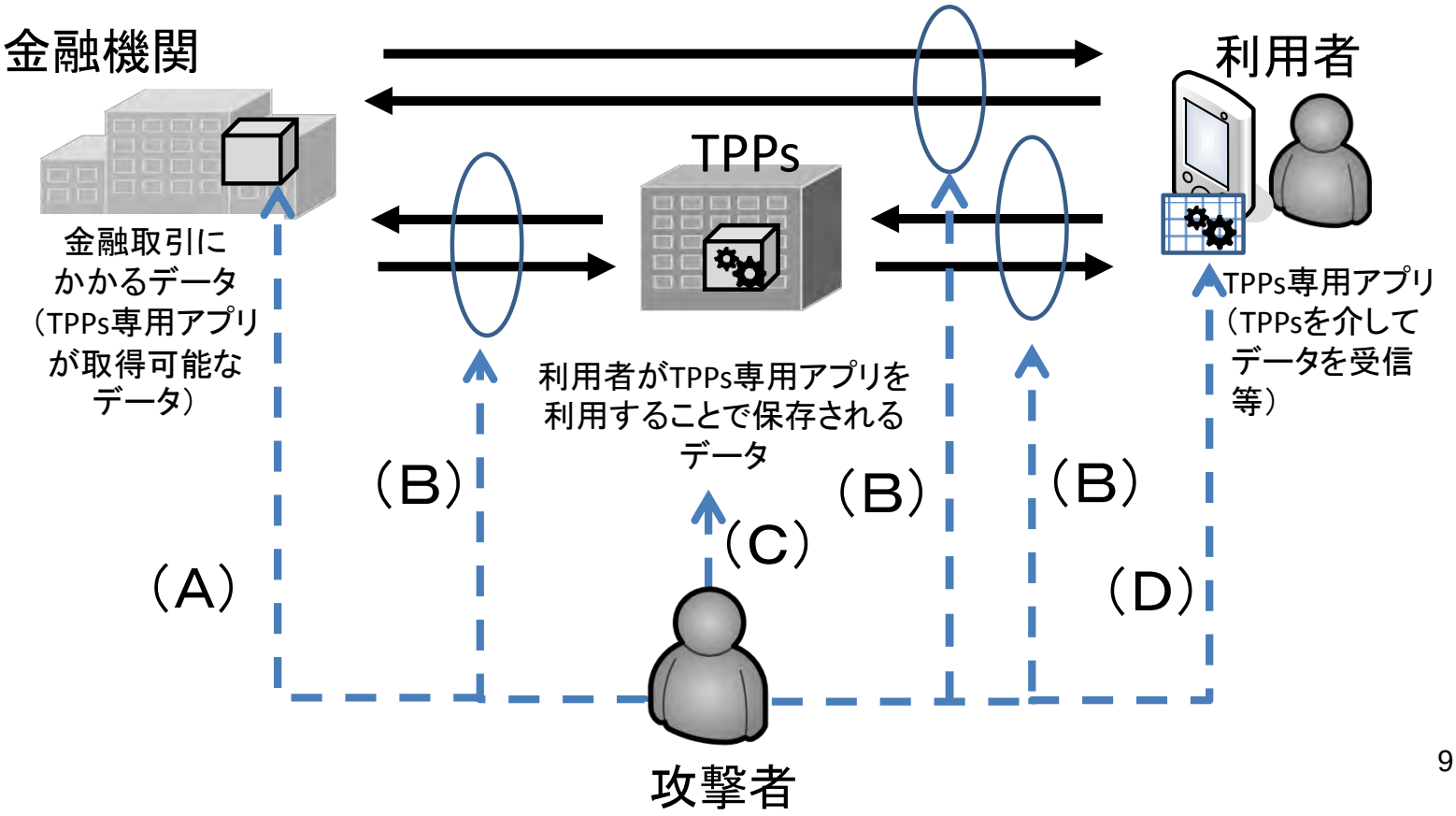
- **APIのプログラムを標準化すると、プログラムの脆弱性が発見された場合に、多くの金融機関が影響を受ける可能性。**
- 標準化する対象は、それ自体が脆弱性とならないものとした方が望ましい。

―― **データ記述言語、アーキテクチャ・スタイル、関数名、リターン値等。**

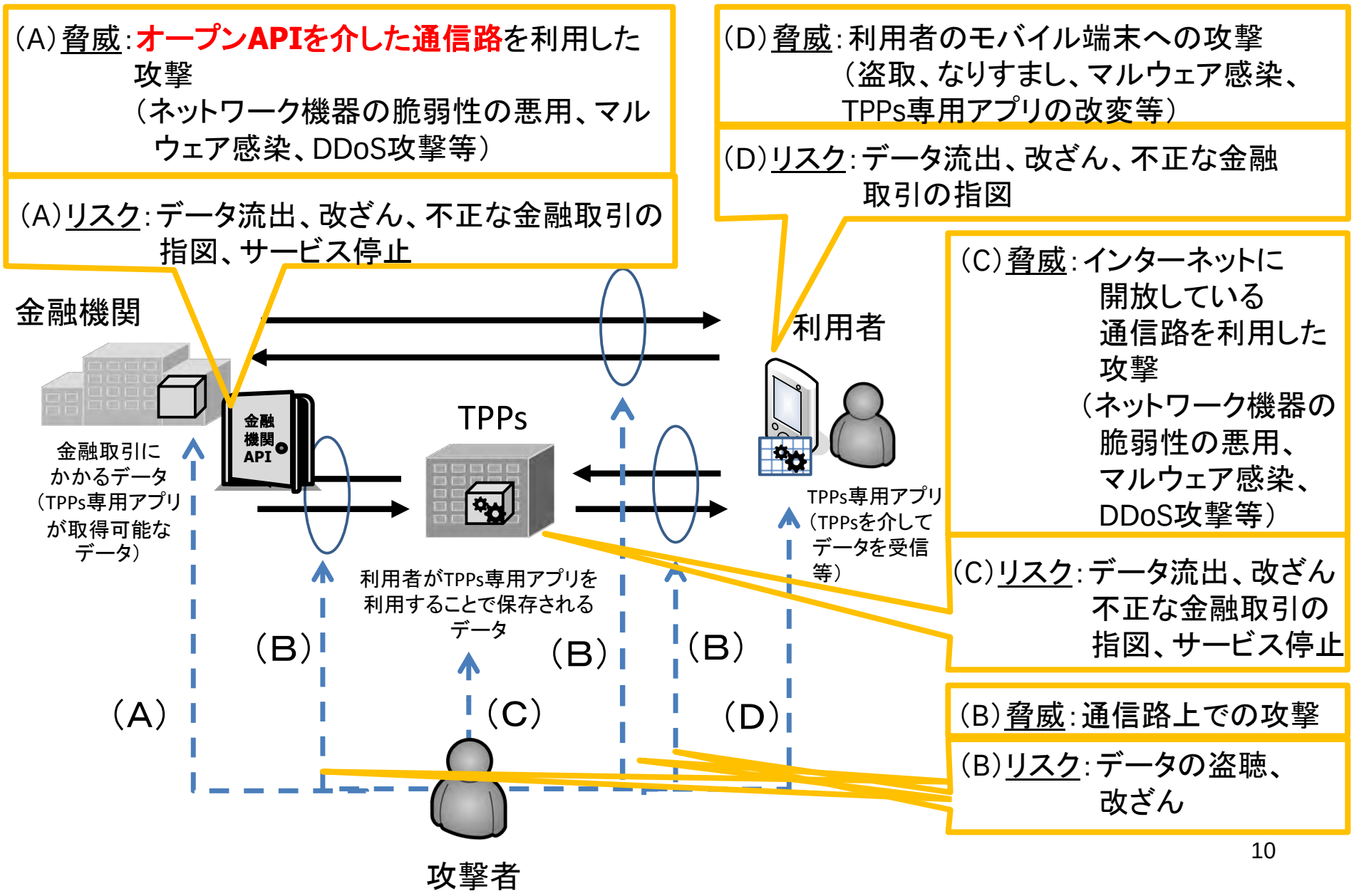
想定するモデル

- TPPsサービスの基本的なシステムのモデルを想定し、脅威やリスク、それらに対する対応策や論点等を考察する。

- 「金融機関」、「TPPs」、「利用者」のエンティティから構成されるモデルを想定。
  - —— 各エンティティはインターネットを経由して接続（または、通信）されている。
  - —— 攻撃者は、上記エンティティ以外を想定。ただし、金融機関やTPPsの内部者の一部と結託する場合も想定。



主な脅威とリスク


(A) 脅威：オープンAPIを介した通信路を利用した攻撃
（ネットワーク機器の脆弱性の悪用、マルウェア感染、DDoS攻撃等）
(A) リスク：データ流出、改ざん、不正な金融取引の指図、サービス停止
(D) 脅威：利用者のモバイル端末への攻撃
（盗取、なりすまし、マルウェア感染、TPPs専用アプリの改変等）
(D) リスク：データ流出、改ざん、不正な金融取引の指図
(C) 脅威：インターネットに開放している通信路を利用した攻撃
（ネットワーク機器の脆弱性の悪用、マルウェア感染、DDoS攻撃等）
(C) リスク：データ流出、改ざん 不正な金融取引の指図、サービス停止
(B) 脅威：通信路上での攻撃
(B) リスク：データの盗聴、改ざん
金融機関
金融機関API
金融取引にかかるデータ（TPPs専用アプリが取得可能なデータ）
TPPs
利用者
TPPs専用アプリ（TPPsを介してデータを受信等）
利用者がTPPs専用アプリを利用することで保存されるデータ
(A)
(B)
(B)
(B)
(C)
(D)
攻撃者

主な対策

（1）金融機関

■ **内部にアクセス可能な通信路**に対する対策が必要。

①データ流出・改ざんリスクへの対策

これまでと同様の対策が有効であるほか、トークンをTPPsに保存する場合、トークンを盗取する攻撃を迅速に検知したり、速やかに失効したりする仕組みの導入等が有効。

②不正な金融取引の指図のリスクへの対策

上述の「データ流出・改ざんリスクへの対策」で用いる対策のほか、**取引認証**を用いることも有効。

③サービス停止への対策

不正な通信によるDDoS攻撃への対策に加え、正規通信の頻度増加に伴う対策を行う必要。

―― メンバーAPI等である場合は、金融機関とTPPs間の通信に**VPNネットワーク**を用いることも有効。

（2）TPPs

- 基本的には、金融機関における上記①～③と同様の対策が必要。
  ―― TPPsが行うべき対策は、**金融機関が行うべき対策に劣るものではなく、第三者による情報セキュリティ監査**等を、定期的に受けることも検討に値する。
- TPPs専用アプリ自体や入出力が改変される状況を想定し、そうした状況を検知・回避可能とするように検討する。

（3）利用者

- モバイル端末および、起動時やTPPs専用アプリの使用時に求められる認証にかかる情報（ID、パスワード、生体情報等）を適切に管理。
- TPPs専用アプリ等の脆弱性に対応したパッチを速やかに適用。

リスク対策における重要な論点

①TPPsにおけるセキュリティ対策の適切な実施をどう担保するのか。

―― 金融機関は、金融情報システムセンターの定める「金融機関等コンピュータシステムの安全対策基準」に則ってセキュリティ対策を実施し、第三者による監査を受ける体制を整備している。

⇒ **TPPsも、対策のための一定の基準やモニタリング体制の必要性を検討することが重要。**

②利用者へのセキュリティ対策の啓発をどう進めていくのか。

―― TPPsは、金融機関と密に連携し、サービス利用時のリスクの所在、インパクト、講じているセキュリティ対策等に関して、利用者が理解できるように説明する必要。

③様々なリスクが顕在化した際の責任を、金融機関とTPPsとの間でどのように分担するか。

★**その他**（セキュリティ対策を講じたことによる副作用は今次分析の範囲外）

利用者の利便性の考慮は必要

―― セキュリティ対策を過度に実施すると、「スループットの低下」や「利用者に複雑な処理を強いる」など、利便性の低下が生じる可能性がある。利便性低下が利用者の許容範囲を超えないよう、セキュリティ対策は利便性とバランスを取りながら行う必要。

おわりに

- APIのオープン化により、金融機関の内部にアクセス可能な通信路を設定することになる。この通信路に対する対策が必要。

- APIの標準化を行う場合、その対象はそれ自体が脆弱性とならないもの（例えば、データ記述言語、アーキテクチャ・スタイル、関数名、リターン値等）とした方が望ましい。

- TPPsにおけるセキュリティ対策の適切な実施の担保（モニタリング等）、利用者へのセキュリティ対策の啓発、金融機関とTPPsとの間における責任分担等をどうするかを意識しつつ、APIをどこまでオープン化すれば良いかを検討する必要。