キャッシュレス決済サービスの
セキュリティ総点検タスクフォース報告書

2020年11月6日

ゆうちょ銀行

はじめに

この報告書は、ゆうちょ銀行が提供するキャッシュレス決済サービスについて、同サービスに関する各種ガイドライン等に定めるセキュリティ対策に基づき、対策の充足度を点検するとともに、現状を踏まえた強化策を取りまとめたもの

また、点検結果については、国内大手サイバーセキュリティ・コンサルティング会社による第三者評価を実施し、以下の見解を得ているもの

貴行が実施したセキュリティ総点検について、その計画から点検実施結果および今後の改善計画についてセキュリティ専門家としての客観的な観点で評価を行った。

その結果、一部事業者（サービス停止中である事業者）について貴行による点検が完了していない状況があるものの、それを除き総点検は適切に履行されたと評価できる。

今後、未了となっている事業者に係る点検を完了させるとともに、本総点検において識別された課題対応および更なるセキュリティ強化・高度化に向けた取り組みを継続実施されたい。

セキュリティ総点検タスクフォース報告書　目次

1. キャッシュレス決済サービスのセキュリティ総点検タスクフォースの設置　・・・　1

2. 不正取引事案概要　・・・　4

3. セキュリティ総点検プロセス・点検対象サービス　・・・　9

－　各サービスのセキュリティ総点検結果概要　－

4. 即時振替サービス　・・・　12

5. ゆうちょPay　・・・　25

6. mijica　・・・　28

7. JP BANK カード　・・・　32

１．キャッシュレス決済サービスのセキュリティ総点検タスクフォースの設置

1-1. セキュリティ総点検タスクフォース概要

◆ 目的

即時振替サービス、mijica会員間送金等における不正利用の発生を踏まえ、各種キャッシュレス決済サービスのセキュリティの堅牢性および利用状況のモニタリング態勢について、総点検を実施。

点検結果を受け、ゆうちょ銀行キャッシュレス決済サービスのセキュリティ向上に向け、セキュリティ強化策を決定。

◆ 点検対象（スコープ）

総点検は、金融庁「資金移動業者の決済サービスを通じた不正出金への対応について（要請）」を踏まえるとともに、以下各種ガイドライン等※に基づき実施。

※各種ガイドライン等
- 「コード決済における不正な銀行口座紐づけの防止対策に関するガイドライン」（以下、「キャッシュレス推進協議会ガイドライン」という。）および「コード決済に関する統一技術仕様ガイドライン」【店舗提示型】【利用者提示型】
- キャッシュレス推進協議会ガイドラインおよび不正取引事案をもとに策定したチェックリスト（以下、「ゆうちょ銀行チェックリスト」という。）
  ※ゆうちょ銀行チェックリストは第三者評価者確認済

(1) 点検対象（ゆうちょ銀行が提供しているキャッシュレス決済サービス）
- 即時振替サービス（双方向即時振替サービス含む）、ゆうちょPay、mijica、JP BANK カード

(2) 点検事項

点検項目は以下の2項目とし、各種ガイドライン等に即してサービスの登録から利用後に至る各フェーズ単位に点検
- 本人認証に係る検知、防御態勢
- 取引データに基づく不正取引の検証態勢

フェーズ（登録から利用後まで）				
①アカウント作成	②銀行口座紐づけ	③チャージ	④決済・送金	⑤取引後

(3) 成果物
- セキュリティ総点検タスクフォース報告書（ギャップ分析結果、現状分析結果、評価および対策等）
  ※　第三者の評価を受けたもの

1．キャッシュレス決済サービスのセキュリティ総点検タスクフォースの設置

1-2. セキュリティ総点検スケジュール

- 週次で進捗状況の打合せを実施
- 日程：以下のとおり
- 参加者：セキュリティ総点検タスクフォースメンバー

日付	イベント	打合せ内容
9/25 (金)	第１回会合	• セキュリティ総点検タスクフォースの設置
9/30 (水)	第２回会合	• 定例会日程 • ワーキングメンバーの選定 • 情報連携 【現状分析】着手
10/7 (水)	第３回会合	• 【現状分析】結果整理
10/12 (月)	第４回会合	• 【課題整理】中間一次整理
10/19 (月)	第５回会合	• 【対応策検討】中間二次整理
10/26 (月)	第６回会合	• 【対応策策定】第一次案整理
11/2 (月)	第7回会合	• セキュリティ総点検タスクフォース最終案報告
11/5 (木)	第8回会合	• 第三者評価結果報告

11/6 (金)	内部統制会議	• 会議報告後、社長決裁 セキュリティ総点検タスクフォース報告書（第三者評価結果報告を含む）

1-3. 検討体制

セキュリティ総点検タスクフォース

責任者：池田社長
（責任者補佐：萩野副社長）

＜事務局＞
IT戦略部　　：執行役部長、担当部長
監査企画部　　：執行役部長

システム部門　　：執行役、システム統括部長
営業部門　　：常務執行役、デジタルサービス事業部執行役部長、同企画役、
法人営業部長、同担当部長
コンプライアンス部門：常務執行役、マネー・ローンダリング対策部長
経営企画部　　：部長
（オブザーバー）
日本郵政　　：執行役

第三者評価者
（国内大手サイバーセキュリティ・コンサルティング会社）

2. 不正取引事案概要

本点検に至った不正取引の一覧

即時振替サービス、mijicaにおいて下記不正取引被害が報告されたため、原因・課題分析、対応策を取りまとめるため包括的にセキュリティ総点検を実施

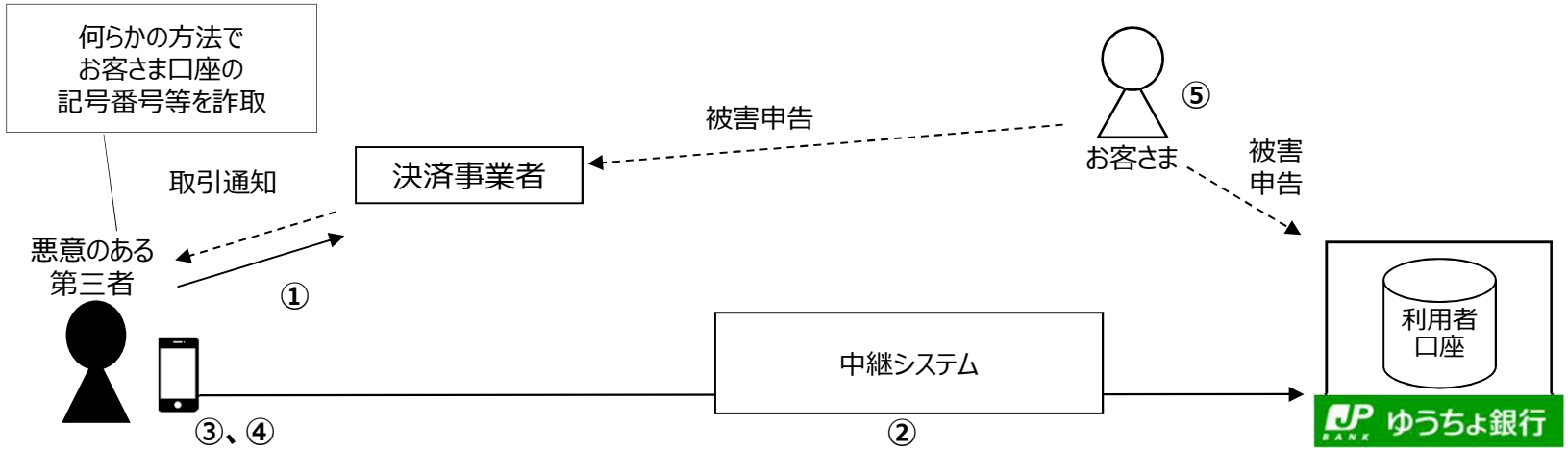
不正取引概要

即時振替サービス	2-1. 不正利用	■ 悪意のある第三者が、お客さまになりすましてアカウントを不正に新規登録 ■ 何らかの方法で詐取した記号番号等を用いて、お客さまの口座と当該アカウントを不正に紐づけ ■ 紐づけたお客さまの口座から当該アカウントにチャージのうえ、不正に取引
mijica	2-2. 不正ログイン	■ 悪意のある第三者が、リスト型攻撃等により特定したID、パスワードを入力し、mijica専用WEBサイト（以下「mijicaWEB」という）へ不正にログインし、お客さま情報を盗取した可能性
	2-3. 会員間不正送金	■ 悪意のある第三者が、リスト型攻撃等で特定したID、パスワードを入力し、mijicaWEBへ不正にログイン ■ お客さまの登録済みメールアドレスを悪意のある第三者のアドレスに変更 ■ ブルートフォース攻撃等により、送金に必要なカード番号を特定し、お客さまのmijicaから当該第三者のmijicaへ不正送金
	2-4. カードの不正作成・不正利用	■ 悪意のある第三者が、お客さまになりすましてアカウントを作成。何らかの方法で詐取した記号番号等によりお客さまの口座を当該アカウントに不正に紐づけ、mijicaを不正に申し込んだ可能性 ■ お客さまにカードが届くまでの期間にmijicaWEBへ不正にログインし、カード情報の一部を盗取した可能性 ■ お客さまの口座から不正に申し込んだmijicaへチャージ ■ 何らかの方法で必要なカード番号を特定し、不正に取引を行った可能性

2．不正取引事案概要

2-1. 即時振替サービスの不正利用

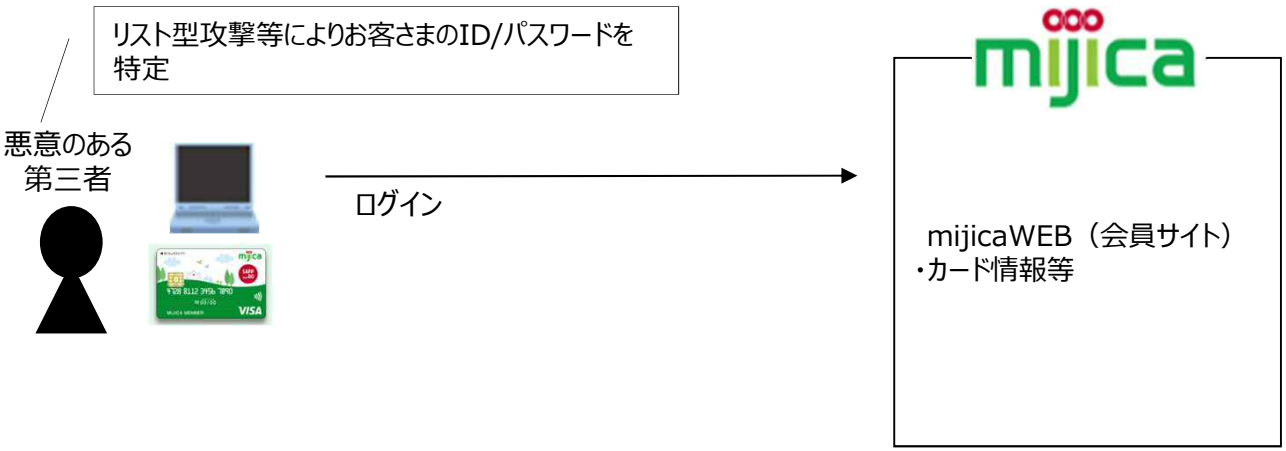
【不正・被害発覚の流れ】



	①アカウント作成	②口座紐づけ	③ チャージ	④決済	⑤取引後
犯行手口	悪意のある第三者が、お客さまになりすましてアカウントを不正に新規登録	何らかの方法で詐取した記号番号等を用いて、お客さまの口座と当該アカウントを不正に紐づけ	紐づけたお客さまの口座から当該アカウントにチャージ	不正に物品等を購入しチャージ金で決済	不正な取引に気づいたお客さまからの被害の申告により発覚

2-2. mijica専用WEBサイトへの不正ログイン

【不正・被害発覚の流れ】



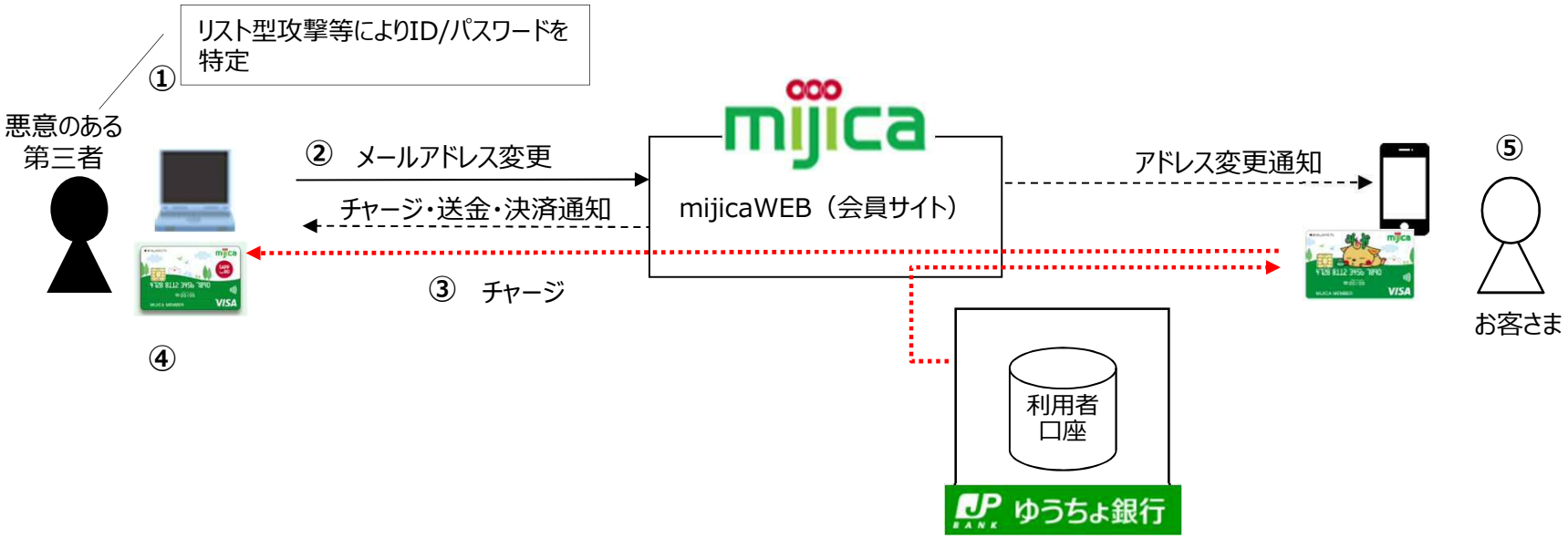
ログイン

犯行手口

悪意のある第三者が、リスト型攻撃等により特定したID、パスワードを入力し、mijicaWEBへ不正にログインし、お客さま情報を盗取した可能性

2-3. mijica会員間の不正送金

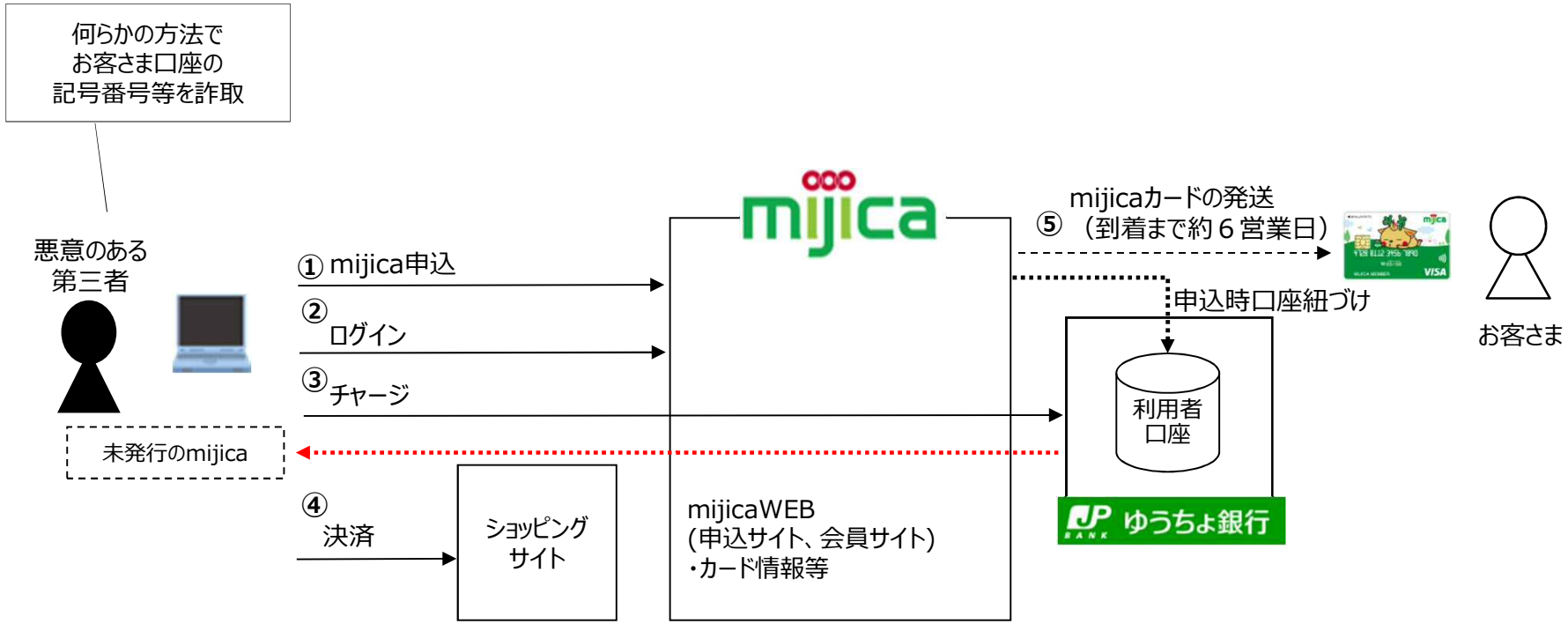
【不正・被害発覚の流れ】



	①ログイン	②メールアドレス変更	③チャージ・送金	④決済	⑤決済後
犯行手口	悪意のある第三者が、リスト型攻撃等で特定したID、パスワードを入力し、mijicaWEBへ不正にログイン	お客さまの登録済みメールアドレスを悪意のある第三者のアドレスに変更	ブルートフォース攻撃等により、送金に必要なカード番号を特定し、お客さまのmijicaから当該第三者のmijicaへ不正送金	不正に物品等を購入しチャージ金で決済	ゆうちょ銀行側の調査、不正な取引に気づいたお客さまからの被害申告により発覚

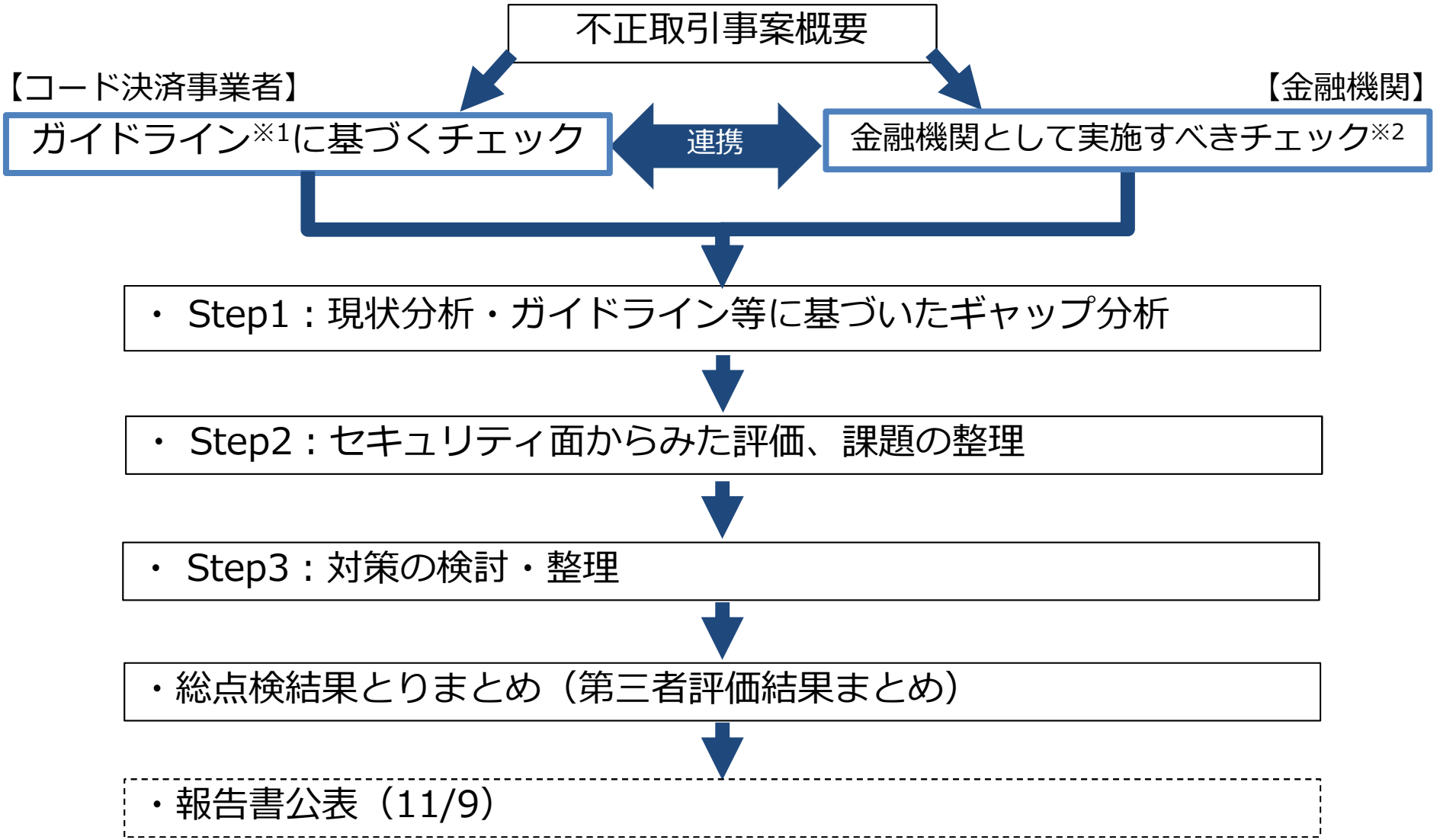
2-4. mijicaカードの不正作成・不正利用

【不正・被害発覚の流れ】



	①mijica申込	②ログイン	③チャージ	④決済	⑤mijicaカードの発送
犯行手口	悪意のある第三者が、お客さまになりすましてアカウントを作成。 何らかの方法で詐取した記号番号等によりお客さまの口座を当該アカウントに不正に紐づけ、mijicaを不正に申し込んだ可能性	お客さまにカードが届くまでの期間にmijicaWEBへ不正にログインし、カード情報の一部を盗取した可能性	（お客さまの口座から不正に申し込んだmijicaへチャージ）	ショッピングサイトで、何らかの方法でカード番号を特定。物品等を購入し決済	お客さまに身に覚えがないカード申込により発覚 注　総点検の過程にて被害発覚

3-1. セキュリティ総点検プロセス



※1 キャッシュレス推進協議会ガイドライン等
※2 キャッシュレス推進協議会ガイドライン等およびゆうちょ銀行チェックリスト

3-2. セキュリティ総点検対象サービス

項番	サービス/事業者			
4	即時振替サービス	決済事業者	コード決済事業者（6社）	PayPay
				LINE Pay
				ドコモ口座（NTTドコモ）
				メルペイ
				ファミペイ(ファミマデジタルワン)
				pring
			その他決済事業者（6社）	Kyash
				支払秘書（ウェルネット）
				PayPal
				ゆめか（ゆめカード）
				楽天Edy
				PayB（ビリングシステム）

項番	サービス/事業者			
4	即時振替サービス	決済事業者以外の事業者	ECサイト	郵便局のネットショップ（日本郵便）
			公営競技（7社）	日本中央競馬会（JRA）
				全国競輪施行者協議会
				南関東4競馬場
				BOAT RACE振興会
				オッズ・パーク
				ケイドリームス
				WinTicket
			証券会社（6社）	マネックス証券
				野村證券
				いちよし証券
				あかつき証券
				松井証券
				One Tap BUY
			ノンバンク（3社）	SMBCモビット
				トヨタファイナンス
				SMBCファイナンスサービス（プロミスのアプリローン）
5	ゆうちょPay			
6	mijica			
7	JP BANK カード	JCB		
		VISA/Master		

各サービスのセキュリティ総点検概要

【点検・評価方法】
- サービス形態・内容により、該当するキャッシュレス推進協議会ガイドライン等の必須項目が異なるため、該当する項目について点検
- 点検にあたっては各事業者に必要項目の充足状況を問合せ、その回答に基づき評価を実施。

＜即時振替サービス＞
- 事業者側（チェック項目の詳細はP15参照）
  - ① コード決済事業者(6社)　：キャッシュレス推進協議会ガイドライン等に定める必須項目を全て点検
  - ② その他の決済事業者(6社)　：サービス形態・内容に合わせてキャッシュレス推進協議会ガイドラインに定める必須項目から該当する項目について点検
  - ③ 決済事業者以外の事業者(17社)：サービス形態・内容に合わせてキャッシュレス推進協議会ガイドラインに定める必須項目から該当する項目について点検

  ⇒ 上記で定めた必須項目を全て充足することを評価する。

- ゆうちょ銀行側（チェック項目の詳細はP16参照）

  サービス形態・内容に合わせて、ゆうちょ銀行チェックリストに定める必須項目から該当する項目について点検

  ⇒ 決済事業者(12社)向けに実施する以下のセキュリティ強化策（高度化項目を含む）を評価に含める。
  - ① 預金者保護の観点から業界水準に照らし先駆的な高度な対応（高度化項目）に該当する2項目（口座紐づけ・チャージ時の監視機能および不正モニタリング態勢の整備）
  - ② ガイドラインから導出されたゆうちょ銀行チェックリストには含まれていないが、預金者保護の観点から実施することが望ましいと考えられる3項目（セキュリティ強化策）

＜ゆうちょPay、mijica、JP BANK カード＞

サービス形態・内容に合わせて、キャッシュレス推進協議会ガイドライン等およびゆうちょ銀行チェックリストに定める必須項目から該当する項目について点検

4. 即時振替サービス

4-1. 決済事業者

4-1-1.ガイドライン等に基づくチェック項目の概要

4-1-2.サービスフローとチェック項目の対応関係

4-1-3. 決済12事業者の現状分析結果とセキュリティ面から見た評価・対策

4-1-4. ゆうちょ銀行側の現状分析結果とセキュリティ面から見た評価・対策

4-2. 決済事業者以外の事業者

4-2-1. 現状分析の結果とセキュリティ面から見た評価・対策

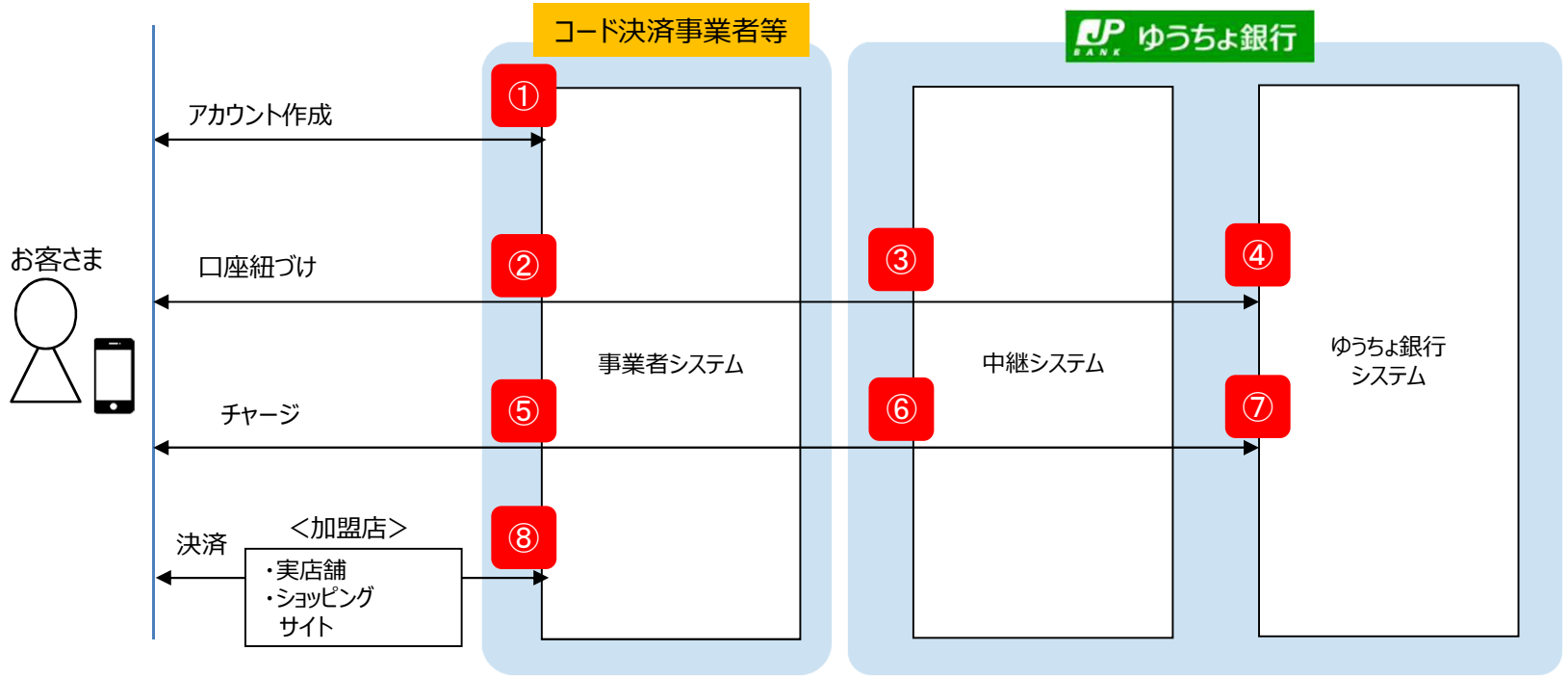
4-1-1. ガイドライン等に基づくチェック項目の概要

チェックリストの全体像は下表のとおり。

	(1) アカウント作成	(2) 口座紐づけ	(3) チャージ	(4) 決済	(5) 常時
コード決済事業者（必須18項目）	1：アカウント作成時に取得する情報の内容やその内容を基礎づける資料の確認方法等を検討・判断【必須】 2：アカウント作成時に取得可能な周辺情報の活用を検討・判断【必須】 3：モニタリング結果の活用【考慮】 4：過去に不正が行われたアカウントに関する情報を蓄積してブラックリスト化し、アカウント作成において、当該ブラックリストと突合する【必須】 5：アカウント作成時において、利用者又はモバイルデバイスを一意に特定できる手段での認証の実施【必須】 6：不正利用の傾向に合わせたアカウント作成の制御の実施【考慮】	7：利用者がコード決済事業者に提供した利用者のうち金融機関から求められる情報を金融機関に提供し、金融機関が保有する紐づけようとされている銀行口座についての情報と一致するとの回答を金融機関から得た場合にのみ当該銀行口座の紐づけを認める【必須】 8：１つのアカウントに複数名義の不正な銀行口座が紐づけられることの防止【必須】 9：１つの銀行口座を複数のアカウントに紐づけることに対する制限【推奨】 10：モニタリング結果の活用【考慮】	11：チャージ額の制限【必須】 ※ただし、13の決済額の制限のいずれかの実施が必須とする 12：モニタリング結果の活用【考慮】	13：決済額の制限【必須】 ※ただし、11のチャージ額の制限のいずれかの実施が必須とする 14：モニタリング結果の活用【考慮】 **【抜粋:コード決済に関する統一技術仕様ガイドライン】** ＜利用者提示型＞ #26：決済時における本人認証【推奨】 #27：QR コード等の有効時間の設定【必須】（目安：5 分） #29：QR コード等の再発行の際の従前のQR コード等の無効化【必須】 ＜店舗提示型＞ (第1部) #21：決済完了画面の偽造防止等【必須】 #22：契約店への取引確認手段の提供【必須】 (第2部) #18：決済時における取引検証【必須】 #22：利用者への取引完了通知【必須】	15：モニタリング体制の構築【必須】 16：モニタリング精度向上・強化【必須】 17：不正を検知した場合の対応体制の整備【必須】 18：事後的な調査によって再発防止へつなげること【必須】
	【必須】4項目	【必須】2項目	【必須】1項目	【必須】7項目	【必須】4項目
ゆうちょ銀行（必須3項目）	-	b：ユーザ認証強度の強化【必須】 d：監視体制の整備【高度化】 e：不正検知、お客さまからの問い合わせ時の停止・復旧対応【必須】	f：異常なチャージが行われていないかの監視体制の整備【高度化】	-	h：不正検知、お客さまからの問い合わせ時の停止・復旧対応【必須】
	-	【必須】2項目	-	-	【必須】1項目

凡例：「1~18」は、キャッシュレス推進協議会ガイドラインの必要要件チェックリストのチェック項目を引用
「b~h」は、ゆうちょ銀行チェックリスト

4-1-2. サービスフローとチェック項目の対応関係



チェック項目との対応関係	(1) アカウント作成	(2) 口座紐づけ	(3) チャージ	(4) 決済	(5) 常時
	① コード決済事業者 チェック項目番号：1,2,4,5	② コード決済事業者 チェック項目番号：7,8	⑤ コード決済事業者 チェック項目番号：11	⑧ コード決済事業者 チェック項目番号：13, #27～第2部#22	① ② ⑤ ⑧ コード決済事業者 チェック項目番号：15~18
	–	③ ゆうちょ銀行(中継システム) チェック項目番号：b, e	–	–	③ ⑥ ゆうちょ銀行(中継システム) チェック項目番号：h
	–	④ ゆうちょ銀行 チェック項目番号：b, e	–	–	④ ⑦ ゆうちょ銀行 チェック項目番号：h

キャッシュレス推進協議会ガイドライン等をもとに、サービス特性を考慮し、必須項目を設定。

通番	チェック項目			決済事業者（コード決済事業者）	決済事業者（その他決済事業者）			決済事業者以外	
	＊チェック項目番号	フェーズ	内容		–	チャージ機能なし	アプリ無し（利用時カード要）	ECサイト	公営競技、証券、ノンバンク
1	1	アカウント作成	アカウント作成時に取得する情報の内容やその内容を基礎づける資料の確認方法等を検討・判断	必須	必須	必須	必須	必須	—
2	2		アカウント作成時に取得可能な周辺情報の活用を検討・判断	必須	必須	必須	—	—	
3	4		過去に不正が行われたアカウントに関する情報を蓄積してブラックリスト化し、アカウント作成において、当該ブラックリストと突合する。	必須	必須	—	—	—	
4	5		アカウント作成時において、利用者又はモバイルデバイスを一意に特定できる手段での認証の実施	必須	必須	必須	—	—	
5	7	口座紐づけ	利用者がコード決済事業者に提供した利用者のうち金融機関から求められる情報を金融機関に提供し、金融機関が保有する紐づけようとされている銀行口座についての情報と一致するとの回答を金融機関から得た場合にのみ当該銀行口座の紐づけを認める	必須	必須	必須	必須	—	
6	8		１つのアカウントに複数名義の不正な銀行口座が紐づけられることの防止	必須	必須	必須	必須	必須	
7	11	チャージ	チャージ額の制限 ※ただし、13の決済額の制限のいずれかの実施が必須とする。	必須	必須	—	必須	—	
8	13	決済	決済額の制限 ※ただし、11のチャージ額の制限のいずれかの実施が必須とする。	必須	必須	必須	必須	—	
9	15	常時	モニタリング体制の構築	必須	必須	—	—		—
10	16		モニタリング精度向上・強化	必須	必須				
11	17		不正を検知した場合の対応体制の整備	必須	必須			必須	
12	18		事後的な調査によって再発防止へつなげること	必須	必須			必須	
13	利用者#27	QRコード決済	QR コード等の有効時間の設定（目安：5 分）	必須	—				
14	利用者#29		QR コード等の再発行の際の従前のQR コード等の無効化	必須					
15	店舗１#21		決済完了画面の偽造防止等	必須					
16	店舗１#22		契約店への取引確認手段の提供	必須					
17	店舗2#18		決済時における取引検証	必須					
18	店舗2#22		利用者への取引完了通知	必須					
	必須項目数			18	12	6	5	4	0

＊チェック項目番号は、キャッシュレス推進協議会ガイドライン等に掲載されているチェックリストの必須項目番号

ゆうちょ銀行チェックリストをもとに、サービス特性を考慮し、必須項目および高度化項目を設定。

通番	チェック項目			決済事業者（コード決済事業者）	決済事業者（その他決済事業者）			決済事業者以外	
	＊チェック項目番号	フェーズ	内容		–	チャージ機能なし	アプリ無し（利用時カード要）	ECサイト	公営競技、証券、ノンバンク
1	a	アカウント作成	サービス利用登録時の本人確認※	–	–			–	–
2	b	口座紐づけ	ユーザー認証強度の強化（二要素認証）	必須	必須			–	–
3	c		不正な口座紐づけの防止（アカウント情報と口座情報の突合）※	–	–			–	–
4	d		監視体制の整備	高度化	高度化			–	–
5	e		不正検知、お客さまからの問い合わせ時の停止・復旧対応	必須	必須			必須	必須
6	f	チャージ	異常なチャージが行われていないかの監視体制の整備	高度化	高度化	–	高度化	–	–
7	g	常時	異常な決済が行われていないかの監視体制の整備※	–	–			–	–
8	h		不正検知、お客さまからの問い合わせ時の停止・復旧対応	必須	必須			必須	必須
9	i		対策状況の定期的な確認※	–	–			–	–
	必須項目数			3	3			2	2
	高度化項目数			2	2	1	2	0	0

＊チェック項目番号は、ゆうちょ銀行チェックリストの番号
※ 事業者側のプロセスのため即時振替の場合は対象外

4-1-3. 決済12事業者の現状分析結果とセキュリティ面から見た評価・対策

4-1-3-1. コード決済事業者（6社）サービス名：PayPay、LINE Pay、ドコモ口座、メルペイ、ファミペイ、pring

キャッシュレス推進協議会ガイドライン等に定める必須項目について、点検を実施。

＜評価・対策＞

- 6社中5社については必須項目を全て充足していることを確認
- 6社中1社については回答を受領後、追加確認を要する事項があったため、現在評価を実施中

	必須項目の現状分析						評価結果
	アカウント作成	口座紐づけ	チャージ	決済	常時	トータル	
コード決済事業者（5社）	4/4	2/2	1/1	7/7	4/4	18/18	・必須項目全ての充足を確認

4-1-3-2. その他決済事業者（6社）サービス名：Kyash、支払秘書、PayPal、ゆめか、楽天Edy、PayB

サービス形態・内容に合わせて、キャッシュレス推進協議会ガイドラインに定める必須項目から該当する項目について、点検を実施。

＜評価・対策＞

- 6社中3社は必須項目を全て充足していることを確認
- 6社中1社については、充足していない項目を本年12月中に対応予定
- 6社中1社については、回答を受領後、追加確認を要する事項があったため、現在評価を実施中
- 6社中1社については、回答内容を同社と協議中

その他決済事業者	必須項目の現状分析						評価結果
	アカウント作成	口座紐づけ	チャージ	決済	常時	トータル	
－（１社）	4/4	2/2	1/1	1/1	4/4	12/12	・必須項目全ての充足を確認
チャージなし（１社）	3/3	2/2	-	1/1	-	6/6	・必須項目全ての充足を確認
アプリなし（１社）	1/1	2/2	1/1	1/1	-	5/5	・必須項目全ての充足を確認

4-1-4. ゆうちょ銀行側の現状分析結果とセキュリティ面から見た評価・対策

キャッシュレス推進協議会ガイドラインおよび不正取引事案をもとに、ゆうちょ銀行チェックリストを策定の上、当該リストを適用し点検を実施。

＜評価・対策＞

- 口座紐づけ時の本人認証の強化機能（二要素認証）を決済事業者12社に導入済み（2020年9月）であり、必須項目全てを充足していることを確認

＜セキュリティ強化策＞（高度化項目であるモニタリング態勢の整備を含む）

- 口座紐づけ時の監視機能の構築およびモニタリング態勢を整備
- 口座紐づけ時におけるお客さまあて通知（お手紙）の実施
- 口座紐づけ時の二要素認証において、残高認証を導入している決済事業者(1社)に対し、IVR認証(自動音声応答)の導入に向けた協議を実施
- チャージ時の異常な取引の監視体制の構築およびモニタリング態勢の整備
- 不正取引の確認をお願いするお手紙が、宛先不明等によりお届けできなかったお客さまについて、口座紐づけを解除

⇒ 上記のセキュリティ強化策は、2020年12月を目途に準備

	現状分析等				評価結果
	口座紐づけ	チャージ	常時	トータル	
現状	2/2	-	1/1	3/3	・必須項目全ての充足を確認
対策後	6/6	1/1	1/1	8/8※	■高度化項目 d：口座紐づけ時の監視体制の整備 f：異常なチャージが行われていないかの監視体制の整備 ※以下のセキュリティ強化策を含む ・口座紐づけ時の郵送通知 ・IVR認証必須（残高認証導入済み事業者を含む） ・宛先不明等お客さまの口座紐づけの解除

4-2-1.現状分析の結果とセキュリティ面から見た評価・対策

4-2-1-1. ECサイト

キャッシュレス推進協議会ガイドラインに定める必須項目から該当する項目について、点検を実施。

＜評価・対策＞

- ECサイトは必須項目4項目、全てを充足していることを確認
- ゆうちょ銀行は必須項目2項目、全てを充足していることを確認

＜セキュリティ強化策＞

- 不正が発生するリスクは相対的に低いものの、お客さまの預金保護の観点から、セキュリティをより高めるため、二要素認証（IVR認証）の導入に向け協議

サービス	必須項目の対応状況						評価結果
	アカウント作成	口座紐づけ	チャージ	決済	常時	トータル	
ECサイト	1/1	1/1	-	-	2/2	4/4	・必須項目全ての充足を確認。
ゆうちょ銀行	-	1/1	-	-	1/1	2/2	・必須項目全ての充足を確認。

4-2-1.現状分析の結果とセキュリティ面から見た評価・対策

4-2-1-2. 公営競技、証券会社およびノンバンク（16社）

日本中央競馬会（JRA）、全国競輪施行者協議会、南関東4競馬場、BOAT RACE振興会、オッズ・パーク、ケイドリームス、WinTicket、マネックス証券、野村證券、いちよし証券、あかつき証券、松井証券、One Tap BUY、SMBCモビット、トヨタファイナンス、SMBCファイナンスサービス

＜評価・対策＞

- 公営競技、証券会社およびノンバンク（16社）は、キャッシュレス推進協議会ガイドラインをもとに、サービス特性を考慮して、必須項目を検討した結果、対象となる必須項目なし
- ゆうちょ銀行は必須項目2項目、全てを充足していることを確認

＜セキュリティ強化策＞

- 事業者は特定目的の資金移動のサービス等であり、不正が発生するリスクは相対的に低いものの、お客さまの預金保護の観点から、セキュリティをより高めるため、二要素認証（IVR認証）の導入に向け協議

サービス	必須項目の対応状況						評価結果
	アカウント作成	口座紐づけ	チャージ	決済	常時	トータル	
ゆうちょ銀行	-	1/1	-	-	1/1	2/2	・必須項目全ての充足を確認。

＜参考 即時振替サービス（公営競技、証券会社およびノンバンク）のサービス概要等＞

#	区分		サービス概要	お客さま・事業者間の入出金	リスク
1	即時振替サービス	公営競技(7社)	PC・スマートフォンから馬券等を購入および当選金を受け取るための資金移動	同一名義人口座との入出金のみ（勝馬投票券等の購入資金のための出金、当選金受取のための入金）	特定目的の資金移動のサービス等であり、不正が発生するリスクは相対的に低い
2		証券会社(6社)	証券口座への株式購入等のための資金移動	同一名義人口座への出金のみ（金融商品購入資金）	
3		ノンバンク(3社)	借入金の返済	同一名義人口座への出金のみ（借入金の返済金）	

5. ゆうちょPay　6. mijica　7. JP BANK カード

- ガイドラインに基づくチェック項目の概要
- ゆうちょ銀行側に必須として適用するチェック項目

チェックリストの全体像は下表のとおり。

	(1) アカウント作成	(2) 口座紐づけ	(3)会員サイトログイン／チャージ／送金	(4) 決済	(5) 常時／その他
ゆうちょ銀行	1：アカウント作成時に取得する情報の内容やその内容を基礎づける資料の確認方法等を検討・判断【必須】 ①：会員サイトの登録時に複雑なID・PWの設定を強制する【必須】 2：アカウント作成時に取得可能な周辺情報の活用を検討・判断【必須】 3：モニタリング結果の活用【考慮】 4：過去に不正が行われたアカウントに関する情報を蓄積してブラックリスト化し、アカウント作成において、当該ブラックリストと突合する【必須】 5：アカウント作成時において、利用者又はモバイルデバイスを一意に特定できる手段での認証の実施【必須】 6：不正利用の傾向に合わせたアカウント作成の制御の実施【考慮】	7：利用者がコード決済事業者に提供した利用者のうち金融機関から求められる情報を金融機関に提供し、金融機関が保有する紐づけようとされている銀行口座についての情報と一致するとの回答を金融機関から得た場合にのみ当該銀行口座の紐づけを認める【必須】 8：１つのアカウントに複数名義の不正な銀行口座が紐づけられることの防止【必須】 9：１つの銀行口座を複数のアカウントに紐づけることに対する制限【推奨】 10：モニタリング結果の活用【考慮】 ②：カード到着前の決済・会員サイトの利用を不可とする【必須】	(会員サイトログイン) ③：ログイン時における本人認証【推奨】 ④：ログイン時に閲覧できる情報を必要最小限とする【必須】 ⑤：ログイン試行の防止【必須】 (チャージ) 11：チャージ額の制限【必須】 ※ただし、13の決済額の制限のいずれかの実施が必須とする 12：モニタリング結果の活用【考慮】 (送金) ⑥：送金実行時における追加認証、送金額の制限を必須とする【必須】 ⑦：モニタリング結果の活用【推奨】	13：決済額の制限【必須】 ※ただし、11のチャージ額の制限のいずれかの実施が必須とする 14：モニタリング結果の活用【考慮】 **【抜粋:コード決済に関する統一技術仕様ガイドライン】** ＜利用者提示型＞ #26：決済時における本人認証【推奨】 #27：QR コード等の有効時間の設定【必須】(目安：5 分) #29：QR コード等の再発行の際の従前のQR コード等の無効化【必須】 ＜店舗提示型＞ (第1部) #21：決済完了画面の偽造防止等【必須】 #22：契約店への取引確認手段の提供【必須】 (第2部) #18：決済時における取引検証【必須】 #22：利用者への取引完了通知【必須】	15：モニタリング体制の構築【必須】 16：モニタリング精度向上・強化【必須】 17：不正を検知した場合の対応体制の整備【必須】 18：事後的な調査によって再発防止へつなげること【必須】 (その他) ⑧：重要な諸届における追加の本人認証【必須】 ⑨：諸届のモニタリング態勢の構築【推奨】
	a：サービス利用登録時の本人確認【高度化】	b：ユーザ認証強度の強化【必須】 c：不正な口座紐づけの防止【必須】 d：監視体制の整備【高度化】 e：不正検知、お客さまからの問い合わせ時の停止・復旧対応【必須】	f：異常なチャージが行われていないかの監視体制の整備【高度化】		g：異常な決済が行われていないかの監視体制の整備【高度化】 h：不正検知、お客さまからの問い合わせ時の停止・復旧対応【必須】 i：コード決済事業者における対策状況の接続時・定期的な確認【必須】

凡例：「1～18」は、キャッシュレス推進協議会ガイドラインの必要要件チェックリストのチェック項目を引用
「a～i」および「①～⑨」は、ゆうちょ銀行チェックリストの項目
（「a～i」は、キャッシュレス推進協議会ガイドラインをもとに策定。「①～⑨」は、不正事案取引をもとに策定。）

キャッシュレス推進協議会ガイドライン等およびゆうちょ銀行チェックリストをもとに、サービス特性を考慮し、必須項目を設定。

通番	チェック項目			ゆうちょPay	mijica	JP BANK カード
	チェック項目番号	フェーズ	内容			
1	1	アカウント作成	アカウント作成時に取得する情報の内容やその内容を基礎づける資料の確認方法等を検討・判断	必須	必須	必須
2	①		会員サイトの登録時に複雑なID・パスワードの設定を強制する	–	必須	必須
3	2		アカウント作成時に取得可能な周辺情報の活用を検討・判断	必須	–	–
4	4		過去に不正が行われたアカウントに関する情報を蓄積してブラックリスト化し、アカウント作成において、当該ブラックリストと突合する	必須	必須	必須
5	5		アカウント作成時において、利用者又はモバイルデバイスを一意に特定できる手段での認証の実施	必須	必須	–
6	7	口座紐づけ	利用者がコード決済事業者に提供した利用者のうち金融機関から求められる情報を金融機関に提供し、金融機関が保有する紐づけようとされている銀行口座についての情報と一致するとの回答を金融機関から得た場合にのみ当該銀行口座の紐づけを認める	必須	必須	必須
7	8		１つのアカウントに複数名義の不正な銀行口座が紐づけられることの防止	必須	必須	必須
8	②		カード到着前の決済・会員サイトの利用を不可とする	–	必須	必須
9	b		ユーザー認証強度の強化（二要素認証）	必須	必須	必須
10	c		不正な口座紐づけの防止（アカウント情報と口座情報の突合）	必須	必須	必須
11	e		不正検知、お客さまからの問い合わせ時の停止・復旧対応	必須	必須	必須

キャッシュレス推進協議会ガイドライン等およびゆうちょ銀行チェックリストをもとに、サービス特性を考慮し、必須項目を設定。

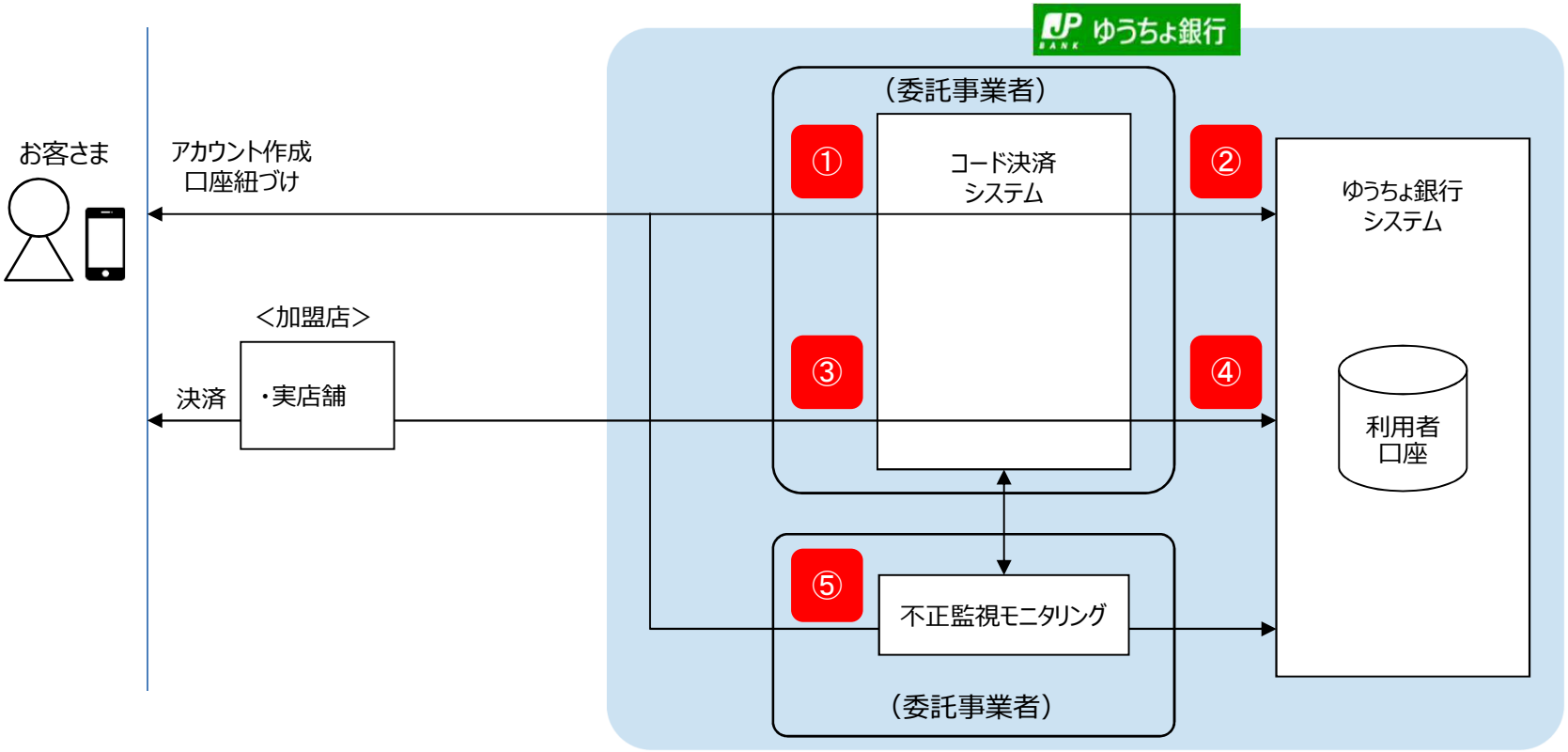
通番	チェック項目			ゆうちょPay	mijica	JP BANK カード
	チェック項目番号	フェーズ	内容			
12	④	会員サイトログイン/チャージ/送金	会員サイトのログイン時に閲覧できる情報を必要最小限とする	–	必須	必須
13	⑤		会員サイトのログイン試行の防止	–	必須	必須
14	11		チャージ額の制限 ※ただし、13の決済額の制限のいずれかの実施が必須とする	–	必須	–
15	⑥		送金実行時における追加認証、送金額の制限を必須とする	–	必須	–
16	13	決済	決済額の制限 ※ただし、11のチャージ額の制限のいずれかの実施が必須とする	必須	必須	必須
17	15	常時／その他	モニタリング体制の構築	必須	必須	必須
18	16		モニタリング精度向上・強化	必須	必須	必須
19	17		不正を検知した場合の対応体制の整備	必須	必須	必須
20	18		事後的な調査によって再発防止へつなげること	必須	必須	必須
21	⑧		重要な諸届における追加の本人認証	–	必須	必須
22	h		不正検知、お客さまからの問い合わせ時の停止・復旧対応	必須	必須	必須
23	i		対策状況の定期的な確認	必須	必須	必須
24	利用者#27	QRコード決済	QR コード等の有効時間の設定（目安：5 分）	必須	–	–
25	利用者#29		QR コード等の再発行の際の従前のQR コード等の無効化	必須		
26	店舗１#21		決済完了画面の偽造防止等	必須		
27	店舗１#22		契約店への取引確認手段の提供	必須		
28	店舗2#18		決済時における取引検証	必須		
29	店舗2#22		利用者への取引完了通知	必須		
必須項目数				22	22	19

5. ゆうちょPay

5-1. サービスフローとチェック項目の対応関係

5-2. 現状分析の結果とセキュリティ面から見た評価・対策

5-1. サービスフローとチェック項目の対応関係



	(1) アカウント作成/口座紐づけ	(4) 決済	(5) 常時
チェック項目との対応関係	①⑤ **ゆうちょ銀行(委託事業者)** チェック項目番号（アカウント作成）：1,2,4,5 （口座紐づけ）：7,8	③ **ゆうちょ銀行(委託事業者)** チェック項目番号：13,#27～第2部#22	①③⑤ **ゆうちょ銀行(委託事業者)** チェック項目番号：15～18
	② **ゆうちょ銀行** チェック項目番号（利用登録時）：b, （口座紐づけ）：c,e	④ **ゆうちょ銀行** チェック項目番号： -	②④ **ゆうちょ銀行** チェック項目番号：h,i

サービス形態・内容に合わせて、キャッシュレス推進協議会ガイドライン等およびゆうちょ銀行チェックリストに定める必須項目から該当する項目について、点検を実施。

＜評価・対策＞
- 必須項目22項目、全てを充足することを確認

サービス	必須項目の対応状況						評価結果
	アカウント作成	口座紐づけ	チャージ	決済	常時	トータル	
ゆうちょPay	4/4	5/5	-	7/7	6/6	22/22	・必須項目全ての充足を確認。

6. mijica

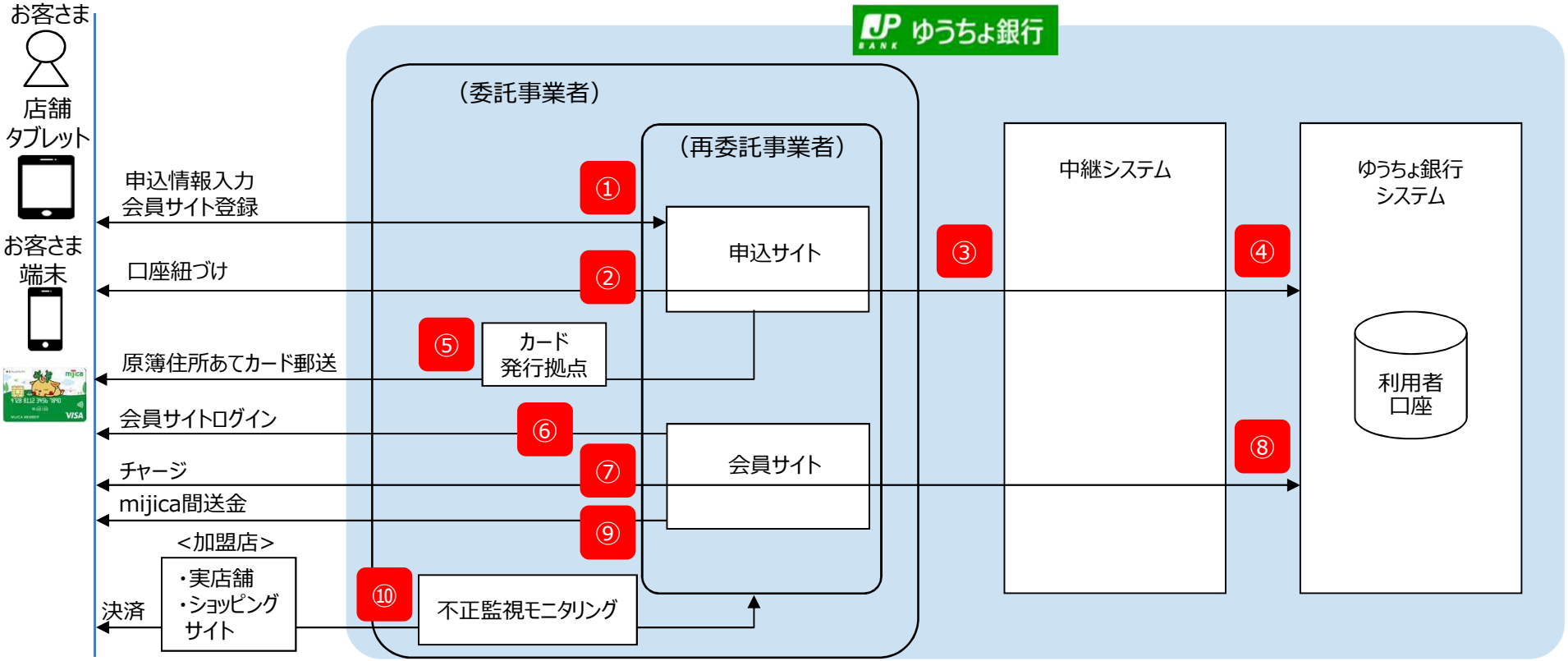
6-1. サービスフローとチェック項目の対応関係

6-2. 現状分析の結果とセキュリティ面から見た評価

6-3. 対策・まとめ

6-1. サービスフローとチェック項目の対応関係

【6. mijica】



	(1) アカウント作成	(2) 口座紐づけ	(3) 会員サイトログイン／チャージ／送金	(4) 決済	(5) 常時／その他
チェック項目との対応関係	① **ゆうちょ銀行（再委託事業者）** チェック項目番号：1,4,5,①	② **ゆうちょ銀行（再委託事業者）** チェック項目番号：7,8,②	⑥⑦ **ゆうちょ銀行（再委託事業者）** チェック項目番号:④,⑤,11	⑨ **ゆうちょ銀行（再委託事業者）** チェック項目番号:⑥	－	①②⑥⑦⑨ **ゆうちょ銀行(再委託事業者)** チェック項目番号:15～18,⑧
	－	－	－	－	⑩ **ゆうちょ銀行（委託事業者）** チェック項目番号：13	⑩ **ゆうちょ銀行（委託事業者）** チェック項目番号：15～18
	－	③ **ゆうちょ銀行（中継システム）** チェック項目番号：c,e	－	－	－	③ **ゆうちょ銀行（中継システム）** チェック項目番号：g,h
	－	④⑤ **ゆうちょ銀行** チェック項目番号：b,c,e	－	－	－	④⑧ **ゆうちょ銀行** チェック項目番号：g,h,i

6-2. 現状分析の結果とセキュリティ面から見た評価

【6. mijica】

サービス形態・内容に合わせて、キャッシュレス推進協議会ガイドライン等およびゆうちょ銀行チェックリストに定める必須項目から該当する項目について、点検を実施。

＜評価＞

- 必須項目22項目のうち、14項目が未実施または不十分。

サービス	必須項目の対応状況						評価結果
	アカウント作成	口座紐づけ	会員サイトログイン／チャージ／送金	決済	常時／その他	トータル	未実施/不十分（注）
mijica	3/4	4/6	0/4	0/1	1/7	8/22	(アカウント作成時) ① 会員サイトの登録時に複雑なID・PWの設定を強制する (口座紐づけ時) ②カード到着前の決済・会員サイトの利用を不可とする b ユーザー認証強度の強化 (会員サイトログイン時) ④ ログイン時に閲覧できる情報を必要最小限とする ⑤ ログイン試行の防止 (チャージ時) 11 チャージ額の制限 (送金時) ⑥ 送金実行時における追加認証、送金額の制限を必須とする (決済時) 13 決済額の制限 (常時／その他) 15 モニタリング体制の構築 16 モニタリング精度向上・強化 17 不正を検知した場合の対応体制の整備 18 事後的な調査によって再発防止へつなげること ⑧ 重要な諸届における追加の本人認証 h 不正検知、お客さまからの問い合わせ時の停止・復旧対応

注：今回の総点検でセキュリティ対策が未実施または不十分であったサービスは停止中。
ただし、現在提供しているデビットカード機能等のサービスについては、今回の点検項目に該当するセキュリティ上の問題はなかったことから、引き続き利用可能。

＜対策＞

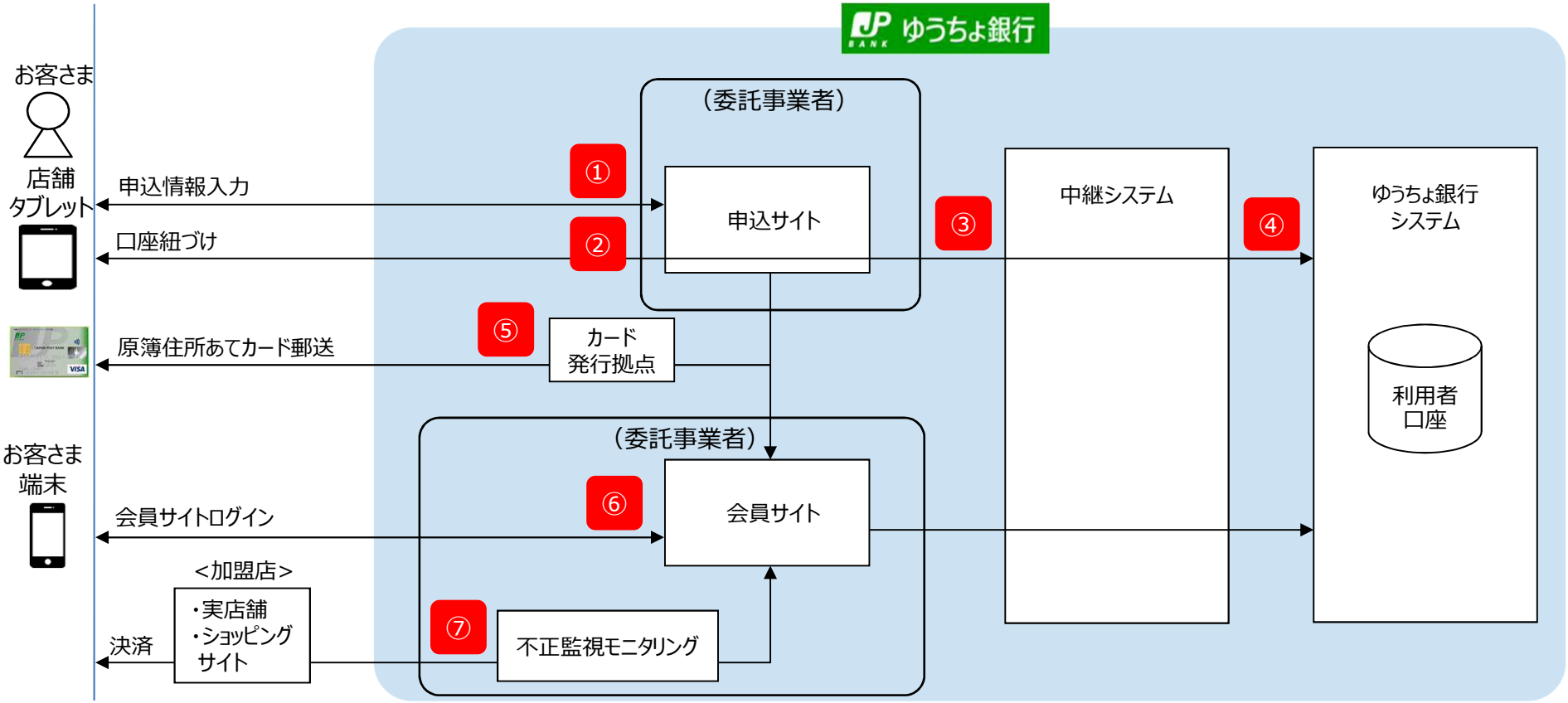
- mijicaは必須項目22項目のうち、14項目が未実施または不十分という評価

- 対応必須となる14項目については、対策が多岐にわたることから、スコープを今後のサービス戦略にまで広げ、ゆうちょ銀行のビジネスの方針を早急に整理

7. JP BANK カード

7-1. サービスフローとチェック項目の対応関係

7-2. 現状分析の結果とセキュリティ面から見た評価・対策



	(1) アカウント作成	(2) 口座紐づけ	(3) 会員サイトログイン	(4) 決済	(5) 常時／その他
チェック項目との対応関係	① **ゆうちょ銀行(委託事業者)** チェック項目番号：1,2,4,5,①	② **ゆうちょ銀行(委託事業者)** チェック項目番号：7,8,②	⑥ **ゆうちょ銀行(委託事業者)** チェック項目番号：④,⑤	⑦ **ゆうちょ銀行(委託事業者)** チェック項目番号：13	① ② ⑥ ⑦ **ゆうちょ銀行(委託事業者)** チェック項目番号：15～18,⑧
	–	③ **ゆうちょ銀行(中継システム)** チェック項目番号：b,c,e	–	–	
	⑤ **ゆうちょ銀行** チェック項目番号：b	④ **ゆうちょ銀行** チェック項目番号：b,c,e	–	–	④ **ゆうちょ銀行** チェック項目番号：h,i

サービス形態・内容に合わせて、キャッシュレス推進協議会ガイドライン等およびゆうちょ銀行チェックリストに定める必須項目から該当する項目について、点検を実施。

＜評価・対策＞

➢ JP BANKカード（JCB）、JP BANKカード（VISA/Master）ともに、必須項目19項目、全てを充足することを確認

事業者	必須項目の対応状況						評価結果
	アカウント作成	口座紐づけ	会員サイトログイン	決済	常時／その他	トータル	
JP-BANKカード（JCB）	3/3	6/6	2/2	1/1	7/7	19/19	・必須項目全ての充足を確認
JP-BANKカード（VISA/Master）	3/3	6/6	2/2	1/1	7/7	19/19	・必須項目全ての充足を確認

おわりに

○ 本報告書は、ゆうちょ銀行が提供する送金決済サービスのセキュリティ対策に係る点検結果であり、サービス提供（再開含む）に当たっての、判断の一要素となるもの

○ 総点検において策定した対策が、確実に実行されていることを確認するため、セキュリティ対策に係るフォローアップ会議（責任者：萩野副社長）を開催し、進捗等の実行管理、確認を行うこととする。

➢ フォローアップ対象の主な対策

＜即時振替＞

- 決済事業者　：点検、評価が完了していない3社の評価の実施
- ゆうちょ銀行（2020年12月目途に準備）

【高度化　2項目】

- 口座紐づけ時の監視機能の構築およびモニタリング態勢の整備
- チャージ時の異常な取引の監視体制の構築およびモニタリング態勢の整備

【セキュリティ強化策　3項目】

- 口座紐づけ時におけるお客さまあて通知（お手紙）の実施
- 口座紐づけ時の二要素認証における残高認証からIVR認証の導入に向けた協議
- 宛先不明等お客さまの口座紐づけの解除

- 決済事業者以外の事業者　：セキュリティ強化策1項目（口座紐づけ時の二要素認証（IVR認証）の導入に向け協議）

＜mijica＞

- 今後のビジネス方針決定に向けたセキュリティ対策の検討

○ お客さまに安全・安心なサービスを提供するため、巧妙化するサイバー攻撃や犯罪の動向を捉え、認証方法やモニタリング態勢などのセキュリティ対策の高度化を継続して進めていくこととする。