

クレジットカードの不正を防止する技術

Yuta Horii (@yutadayo)

YAPC::Fukuoka 2025

2025-11-14

今日お話しすること

 決済電文の技術仕様

 決済データを活用した不正検知 / 防御システムの紹介

 イシューが行なっている日々の運用



堀井 雄太

SmartBank, Inc.

CTO

 @yutadayo

 @yutadayo



スマートバンクという会社を創業し
ワンバンクの開発をしています



磁気・ICカードの製造に関する開発や
プロジェクトに長く関わっています



YAPC::Hakodate 2024 に続き
登壇させてもらっております

※ クレジットカードを製造する技術というタイトルで発表



頑張らなくていいお金の管理

— AI家計簿アプリ —

 ワンバンク

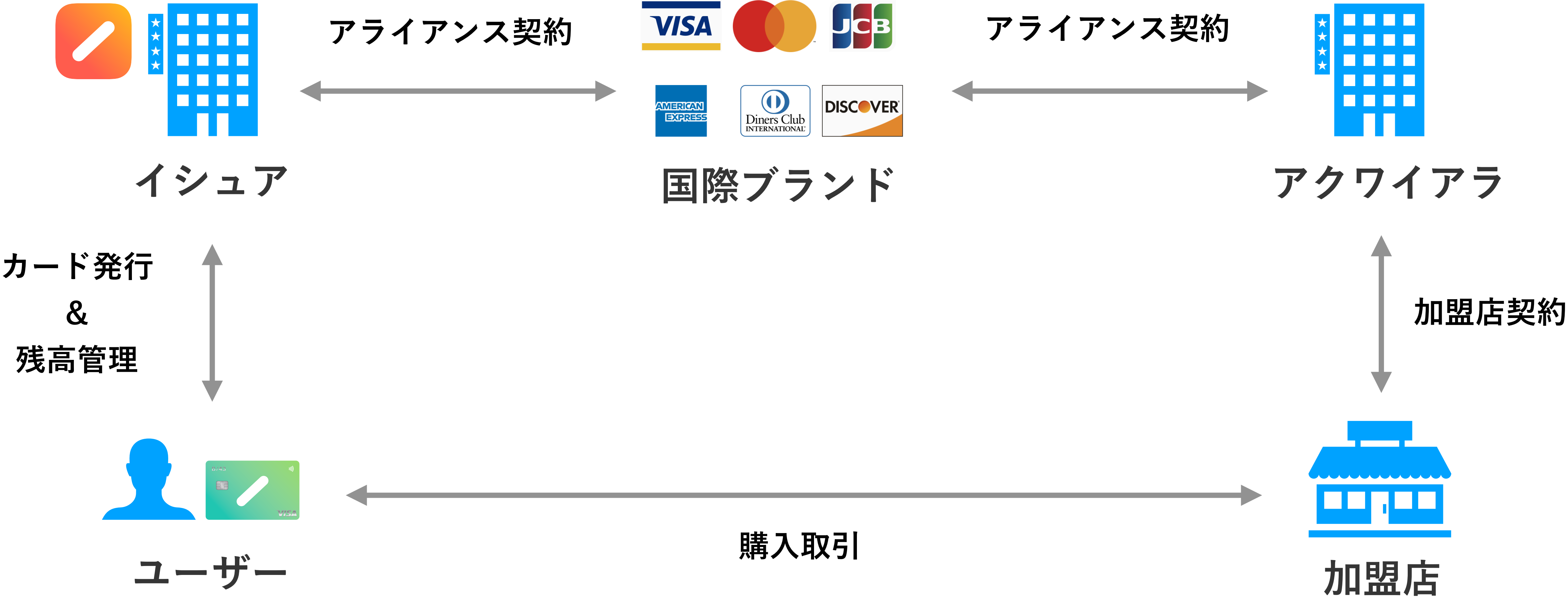


アジェンダ

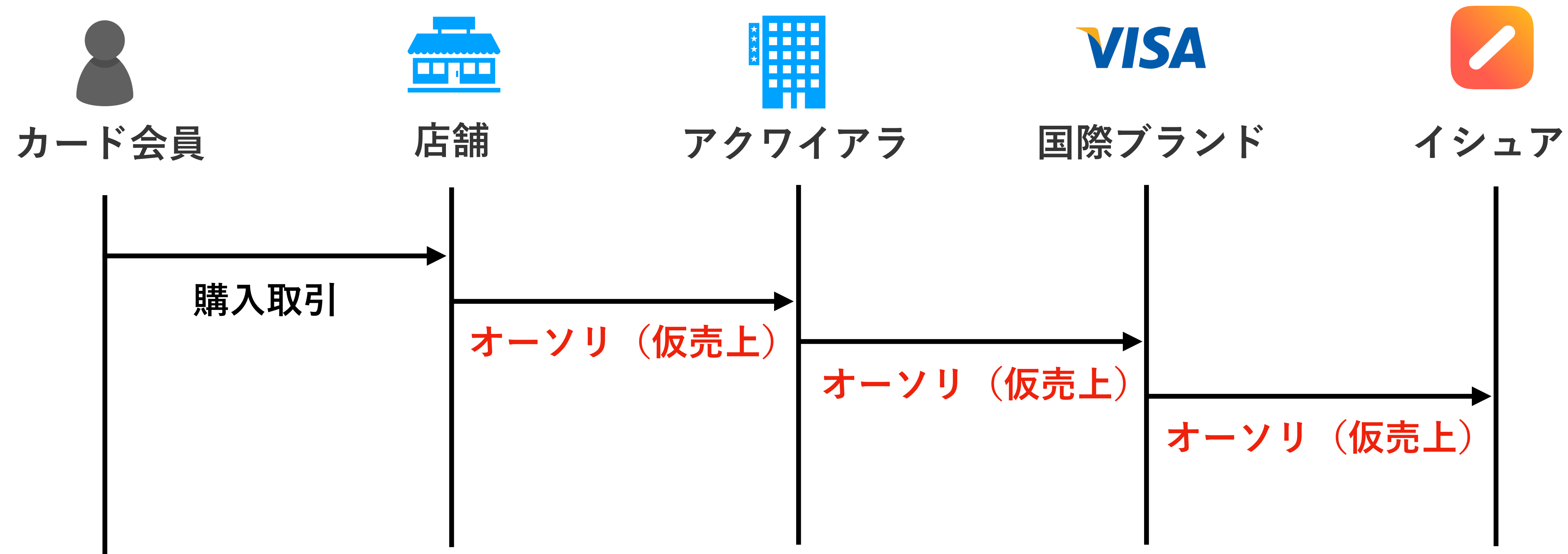
1. 決済電文の仕様
2. 決済データを用いた不正判定ロジックについて
3. ルールベースの不正検知の仕組み
4. 不正攻撃への対策

1. 決済電文の仕様

1. 決済電文の仕様



決済データの流れ



決済電文は ISO8583 という規格をベースにしたデータとしてやりとりされる

ISO8583とは？

- カード決済メッセージの国際標準フォーマット※
- 基本構造として以下の内容で構成されている
 - メッセージタイプ
 - ビットマップ
 - データエレメント
- ブランドによって ISO8583 の形式を独自にカスタマイズされている
 - スマートバンクの場合はVisa仕様にカスタムされた決済データを処理している

ISO8583の基本構造

MT	Bitmap	Data	Data	Data	Data	Data	Data	Data
----	--------	------	------	------	------	------	------	------

- メッセージタイプ
 - 4桁の値で、何のメッセージなのかを表す（0100 / 0110 etc…）
 - 1桁目はバージョン、2桁目はメッセージの目的、3桁目はメッセージの種類、4桁目はメッセージの発信元
 - 例えば 0100 は加盟店取引の承認要求（オーソリ）を指す
- ビットマップ
 - データエレメントのうち、どのBit位置のデータが存在するかを示す64Bitの値
 - 7224048000808000 → Bit位置 2,3,4,7,11,14,22,25,41,49 のデータエレメントが存在する
- データエレメント
 - カード番号や決済金額などが含まれていて、どのBit位置の値かでデータの種類が決まっている

データエレメントサンプル

Bit位置	フィールド名	値	意味
2	PAN	43232100xxxx0001	カード番号
3	Processing Code	000000	取引種別識別値（00000 = 購入取引）
4	Amount, Transaction	000000001000	決済金額
7	Transmission Date & Time	0525022201	アクワイアラが送信した取引時刻
14	Expiration Date	2511	カード有効期限
18	Merchant Category Code（MCC）	5399	業種コード
22	POS Entry Mode	051	カードの読み取り方式（051=PIN有りIC決済）
32	Acquiring Institution ID Code	476135	アクワイアラ識別値
41	Card Acceptor Terminal ID	00235799	決済端末ID
42	Card Acceptor ID Code	235737000762203	加盟店ID

イシュアは電文のパース処理を行い、それぞれの値の内容や組み合わせと
保有している会員情報を使って決済処理を行う

2. 決済データを用いた不正判定ロジックについて

不正な取引とは？

 不正な決済カテゴリ	海外送金などマネーロンダリングに使われやすい決済 ホテル / ガソリンスタンドなどカードの用途に合っていない決済
 不正な決済国	北朝鮮やイラン、ミャンマーなど取引を許可していない国からの決済
 不正な加盟店	デートサイト、オンラインカジノといった不正被害の多い加盟店からの決済
 不正なカード	カード情報が流出したカード、有効化前のカード、etc
 不正なユーザー（口座）	決済金額上限等の閾値を超えた口座での決済、悪意あるユーザーによる不正補償申請

ワンバンクの決済処理フロー

1. 決済可能な決済カテゴリの判定

2. 不正な加盟店の判定

3. 本人確認が必要な加盟店かの判定

4. 指定している決済NGな加盟店の判定

5. クレジットマスター攻撃判定

6. 3DS取引の確認

7. 有効なカードの判定

…の判定

```
def validation_methods
  %i[
    check_presentment_enable_mcc
    check_scam_merchant
    check_kyc_require_merchant
    check_block_rule
    check_no_authorization_merchant
    check_credit_master_rule
    check_fraud_authorization_rule
    check_online_casino_rule
    check_card_activated
    check_expired_card
    check_card_available
    check_account_ready_to_pay
    check_three_d_secure
    check_valid_validation_result
    check_valid_params
    check_amount_exceed_limit
    check_balance_sufficient
    check_total_payment_amount_limit
    check_monthly_payment_amount_limit
    check_high_value_prepaid_payment_amount_limit
    check_monthly_high_value_prepaid_payment_amount_limit
  ]
end
```

不正な決済カテゴリの判定

- Merchant Category Code (MCC) を利用して判定
- 決済NGなMCCを予めDBに登録しておき、データと照合
- 該当した場合に決済不承認にする

```
# 売上オーソリを承認可能な mcc かチェックする
# マスタで定義されていない mcc は許可する方針とする
def presentment_authorization_enable_mcc?(mcc)
  find_by(code: mcc).exists?
end
```

MCC	業種
4829	Money Transfer / Remittance
5967	Direct Marketing – Inbound Teleservices
6011	ATM・Cash Disbursements
6051	Non-Financial Institutions – Quasi Cash
7273	Dating and Escort Services
7995	Betting / Gambling

不正な加盟店の判定

- MCCだけで不正な決済を防げる訳ではない
 - MCCはアクワイアラが設定するため 이슈アにコントロールできない
- ワンバンクでは不正な**加盟店のブロックリストを作成**し、決済処理の中で判定ロジックとして使用している
- 加盟店の一意のリストを作るのは決済電文の特性上難しい
 - 加盟店IDが時間経過で変わる
 - 日本では同じ加盟店でもアクワイアラが複数存在している（マルチアクワイアリング）
 - デパートなどの集合施設の場合に加盟店のIDが重複することも

不正な加盟店の判定のためのブロックリスト

アクワイアラID	加盟店ID	端末ID	ブロック理由
451899	9666125	45821729	詐欺
479338	479338000667103	99999999	決済NG加盟店
439702	70013028	70013028	オーソリ無し決済

- **アクワイアラID / 加盟店ID / 決済端末ID の組み合わせで登録**
 - 加盟店名だけで判定すると巻き込みが発生してしまう
 - アクワイアラや決済した端末情報もセットにしないと一意な加盟店と判断できない

3. ルールベースの不正検知の仕組み

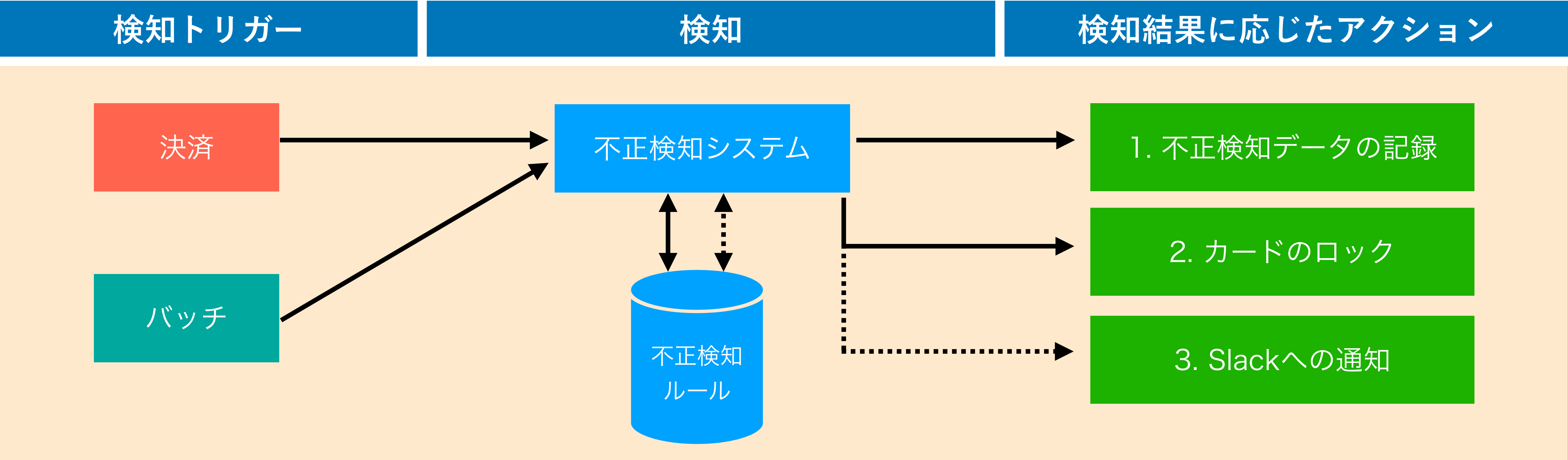
不正の実績から不正取引の傾向をルール化、該当する取引を検知し、ブロックリストへの反映や取引のキャンセル、不正取引の返金対応を行なっています👮

※ ワンバンクは決済以外に入金や出金機能もあるので、それらもルール化して不正を検知しています。

不正検知ルール※

検知ロジック	検知タイミング
30 分以内に 5 件以上、海外通貨で決済された加盟店	オンライン
30分以内に 2 回以上、100,000 円以上のクレジットカード入金	オンライン
1週間で50件以上の決済失敗	日時
1週間で海外加盟店での有効性確認が10件以上あり、 それらが3件以上の異なる決済カテゴリで使われているカード	1時間毎
当月の決済金額の合計が10万円以上のユーザー	非同期Job実行

3. ルールベースの不正検知の仕組み



- 不正検知システムは決済 or バッチから呼び出され、登録されているルールに応じて取引内容や会員データを評価する
- 検知結果に応じて設定されているアクションを実行する

3. ルールベースの不正検知の仕組み

- 検知システム

- 決済時に即時に検知実行するものもあれば、決済レスポンスの制約上、**時間のかかる検知ロジックは非同期で実行**する
- 即時での検知が必要ないものはバッチ時間や日時で実行する

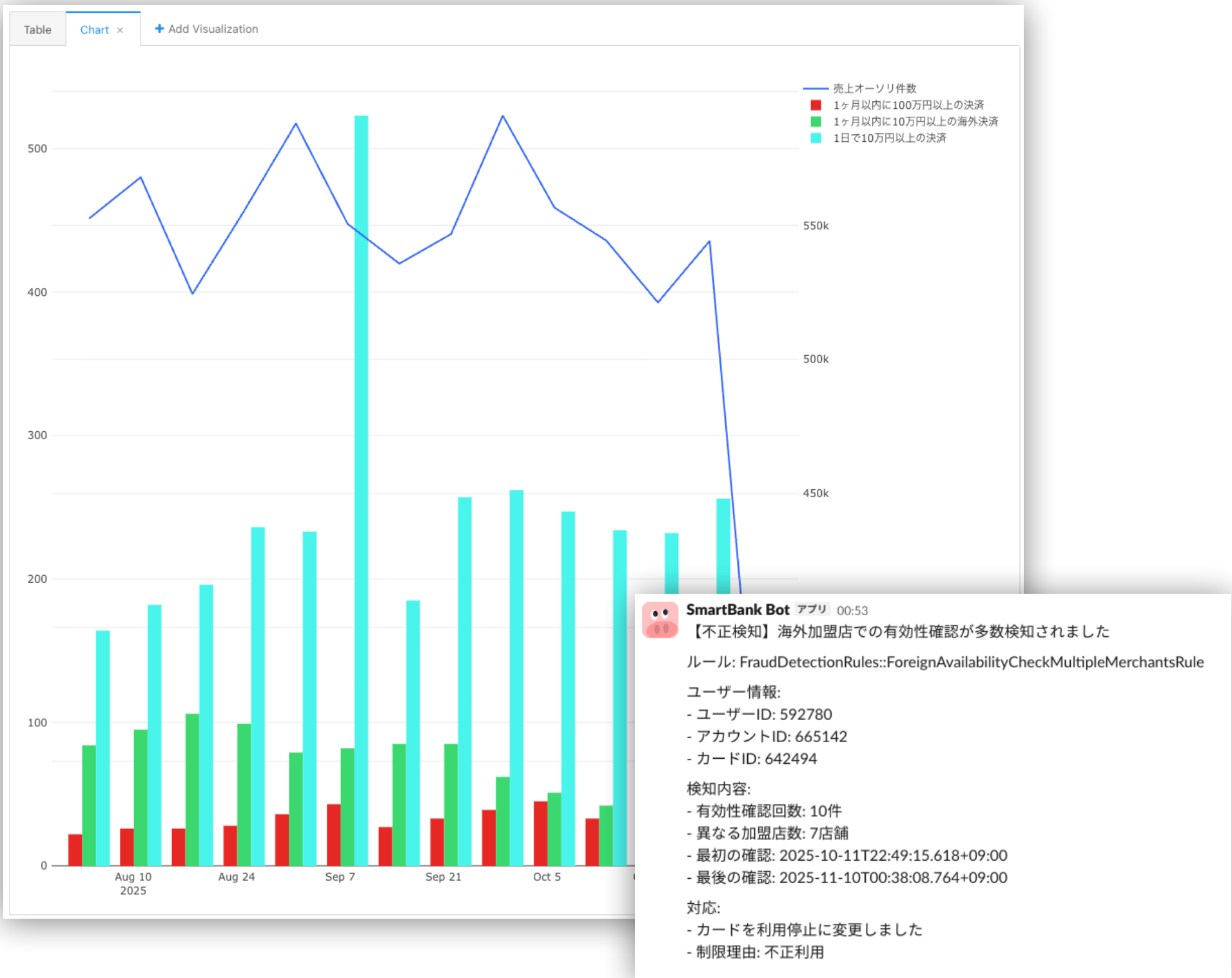
- 検知アクション

- 検知後のアクションは汎用的な実装になっており、ルール毎にどのようなアクションを取るかを任意に設定できる
- アクション自体も同期 / 非同期で実行されるように設定できる
- 検知のON/OFF、検知無効間隔の設定や、特定のユーザーを除外する機能など運用に合わせて割と多機能な実装になっている

不正検知ルール運用

- 管理画面から検知件数や取引詳細を確認しルールの評価を実施
- 不正確定した後は取引やユーザーにタグをつけることでルール自体の評価を行う
- Redashで集計のダッシュボードを作り定期的なモニタリング
- 不正の手口は頻繁に変わるので検知件数の傾向などを確認し、ルール自体を更新 / 停止
- 緊急性が高いルールでの検知はSlackに通知
- 専任のオペレーターが取引確認

ユーザーID	不正検知ルールID		 検知無視設定		
最終検知日	ユーザーID	不正検知ルールID	検知タイトル	検知回数	検知無視設定
2025-11-09 15:50:08	1001893	11	1日で10万円以上の決済	1	×
2025-11-09 15:50:07	1000039	11	1日で10万円以上の決済	4	×
2025-11-09 14:49:59	1363038	11	1日で10万円以上の決済	1	×
2025-11-09 13:53:14	1081671	46	直近1ヶ月で海外加盟店での有効性確認が10件以上あり、それらが3件以上の異なる加盟店で行われているカード	1	×
2025-11-09 13:50:20	662338	34	GMO入金から1時間以内の出金	3	×
2025-11-09 13:49:42	331178	11	1日で10万円以上の決済	2	×



4. 不正攻撃への対策

カード決済にはいくつかの攻撃のパターンがあり、それぞれの攻撃の内容と防御している対策について解説していきます 🖐

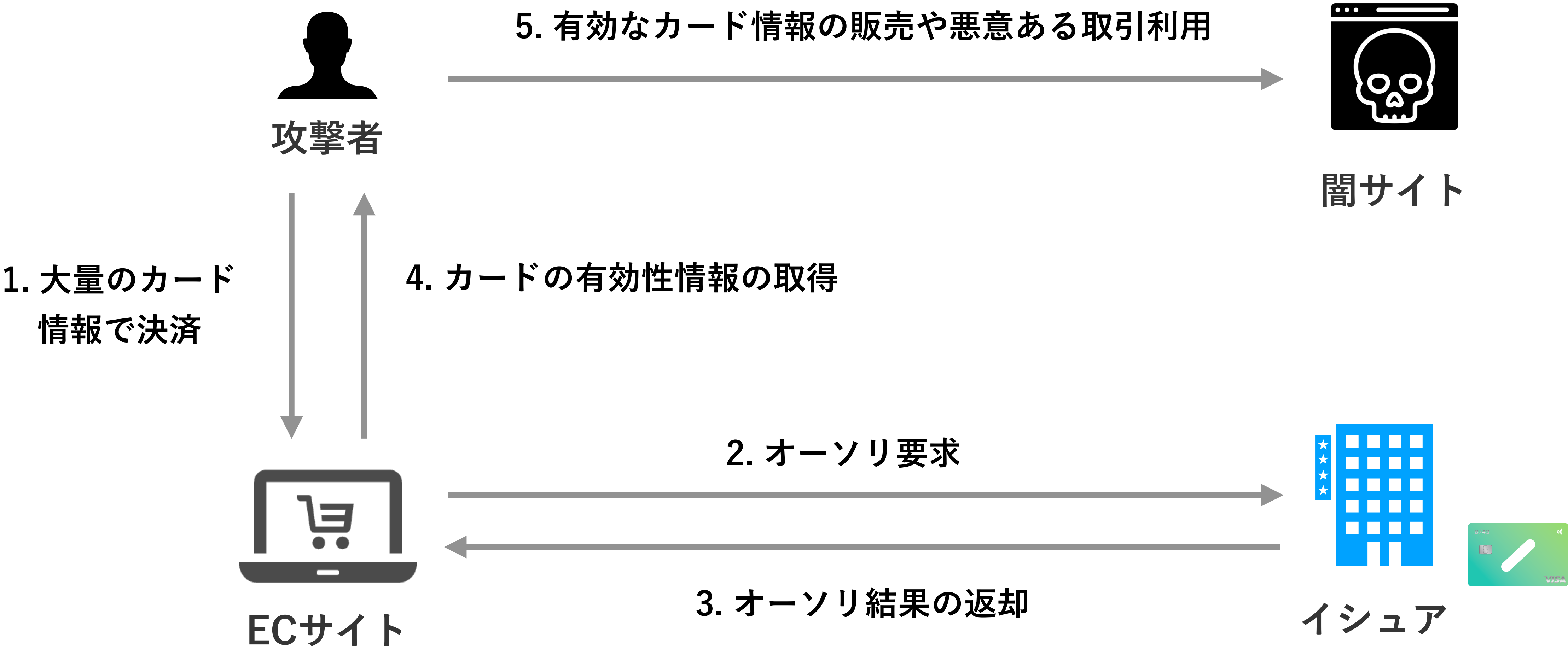
1. クレジットマスター攻撃

2. なりすまし攻撃

クレジットマスター攻撃（クレマス）

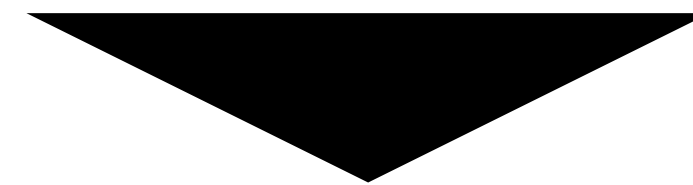
- カードの規則性を利用し同一のBIN（カード番号の先頭数桁）帯に対して決済取引を行いカード番号を取得する攻撃
- 主にプログラムによるランダムで大量な攻撃が多い
- BINはイシュアによって固定化されているので、有効期限やセキュリティコードなどの組み合わせで何度もアタックすることでカード情報を割り出すのが特徴
- 有効と判断されたカードでさらに不正な決済に使われる

クレジットマスター攻撃図解



クレジットマスター攻撃に対する防御策

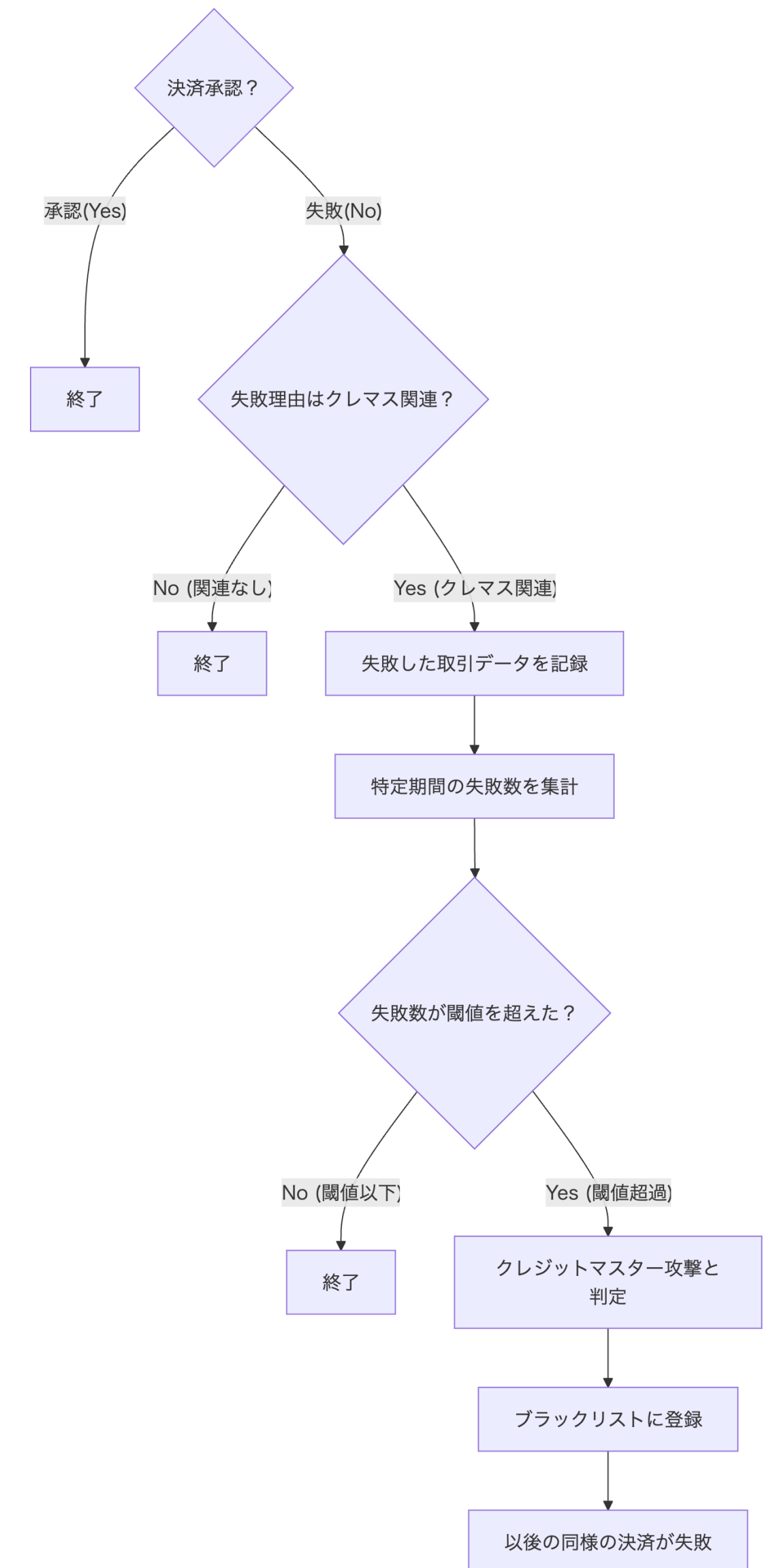
1. 攻撃中は特定の加盟店 / アクワイアラが指定されることが多い
2. 攻撃の特性上、大量に失敗も発生し失敗理由の多くが存在しない
カード番号、有効期限やセキュリティコードの間違い
3. 一定の期間内に大量に取引が行われることが多い



特定の期間、特定の加盟店で大量に取引が発生し且つ
カード情報の相違で失敗している取引を検知する

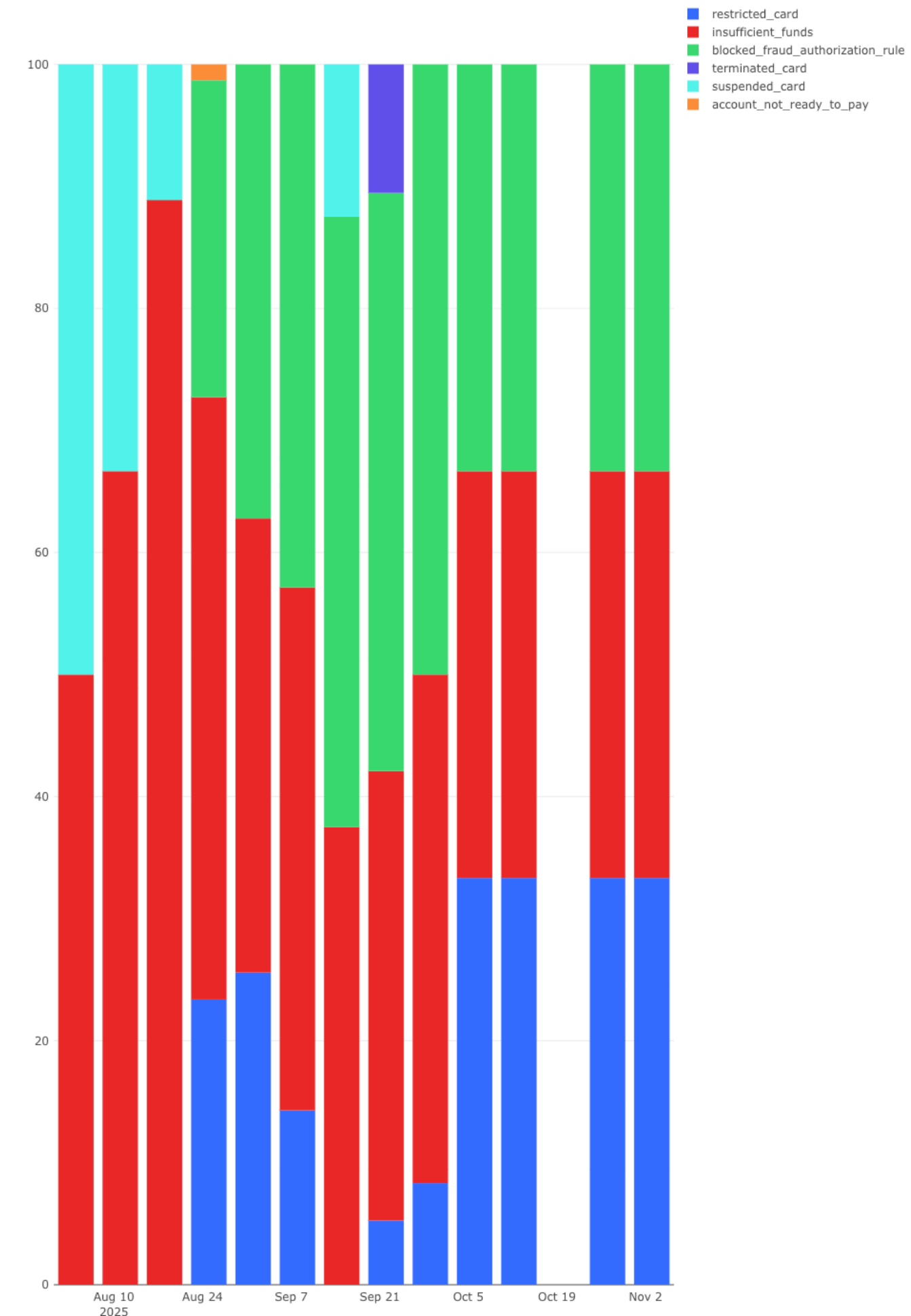
クレマス攻撃に対するシステムの対応

- ワンバンクは決済に失敗した理由の全てをDBに記録している
- クレマス時に起きる**失敗理由で不承認になった取引を記録**
 - 有効期限、PIN、セキュリティコードの間違いなど
- 失敗決済毎に遡って**特定の期間で集計し失敗数の閾値を超えていればクレマス判定**としている
- クレマス判定された取引は攻撃加盟店としてブロックリストに登録され以後の取引が失敗する
 - 失敗数が閾値以下になった場合は、ブロックリストから解除される



クレマス攻撃のチューニングポイント

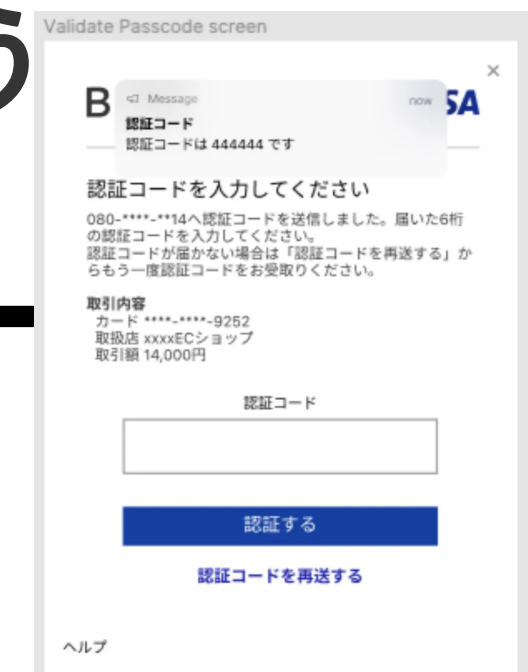
- Amazonセールなど、特定期間に多く取引され、クレマス判定されるなど巻き込みが発生してしまう場合がある
- 一部の問題ない加盟店はブロックリストに入れないなどの対処をしている
- 集計タイミングを広く取ると本当は問題なかった場合もクレマス判定される場合がある（偽陽性）
- ブロック後にクレマス判定理由と同様の理由で決済失敗が発生していないかを社内のツールで確認している



なりすまし攻撃 (漏洩したカード情報を用いた決済)

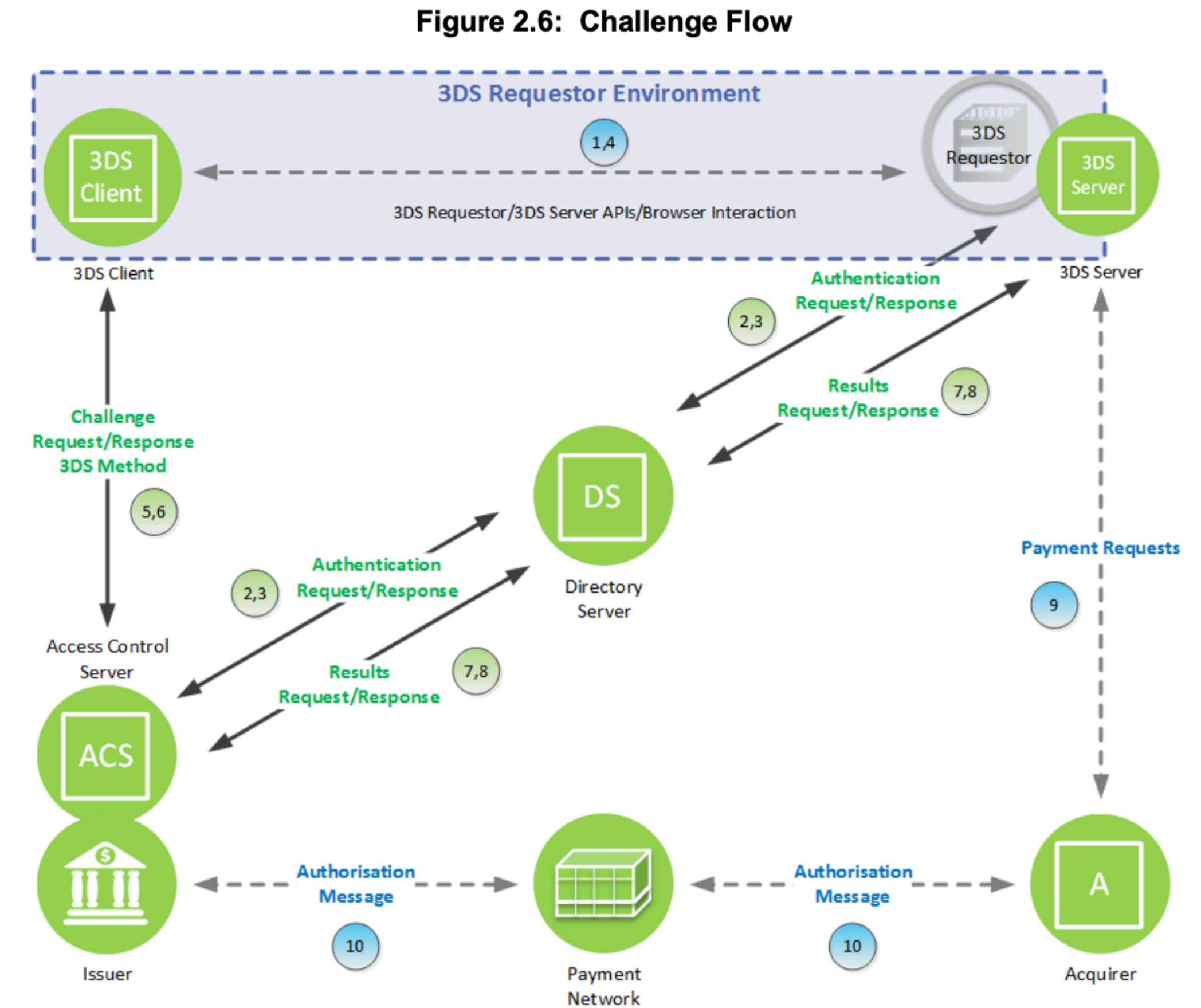
- 既に攻撃者にカード情報が漏れており、高額な取引や海外決済などで不正利用される
 - 主にユーザーからの問い合わせなどで発見され、漏洩後の検知は非常に難しい
- カード情報が漏洩される経路も様々
 - 海外でのスキミング被害
 - クレマスによるカード情報の特定
 - 脆弱な加盟店ECサイトからの情報流出

3D セキュア を導入し決済
時に本人認証を行う

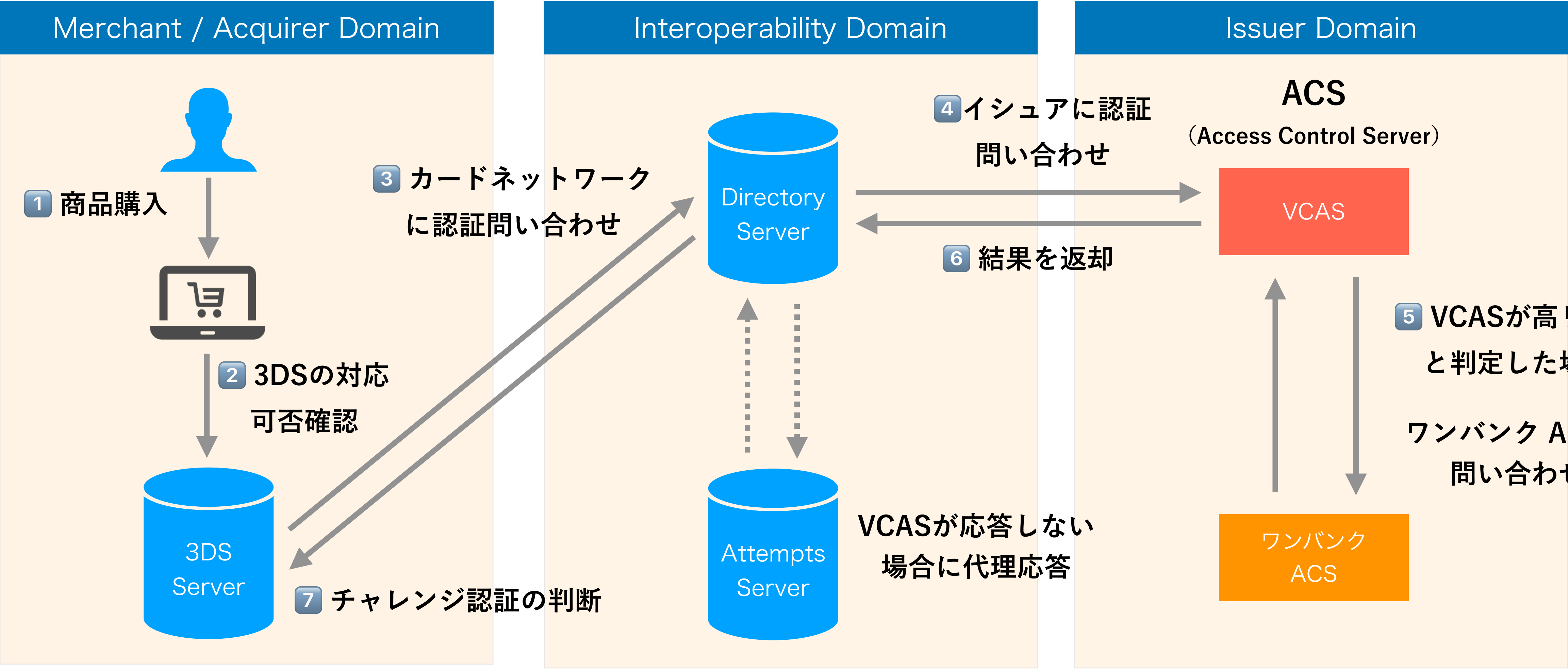


3D セキュアとは？

- EMVCo が規定するオンライン決済時に本人認証を行うための国際標準※
- オーソリ要求の前に実施される認証のフロー
- Ver 1系の際はパスワードを求められるのが主流
- Ver 2系で OTPや生体認証が採用されている
- 3Domain の通りイシュア / 加盟店・アクワイアラ / 決済NW が連携して行う認証の仕組み
- ワンバンクはVCASというVisaの本人認証の仕組みを導入することで実現している

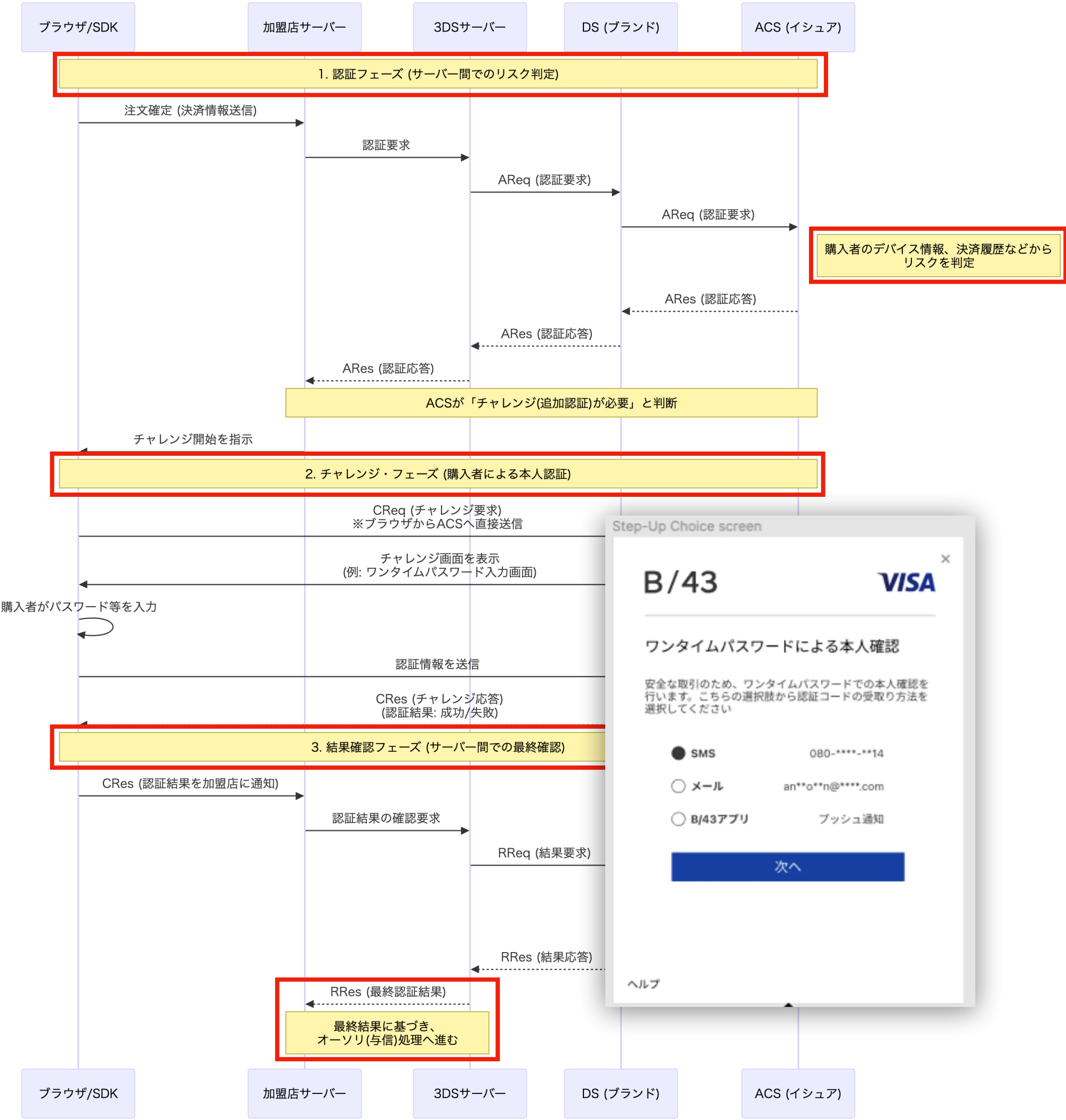


3D セキュア図解（認証フェーズ）



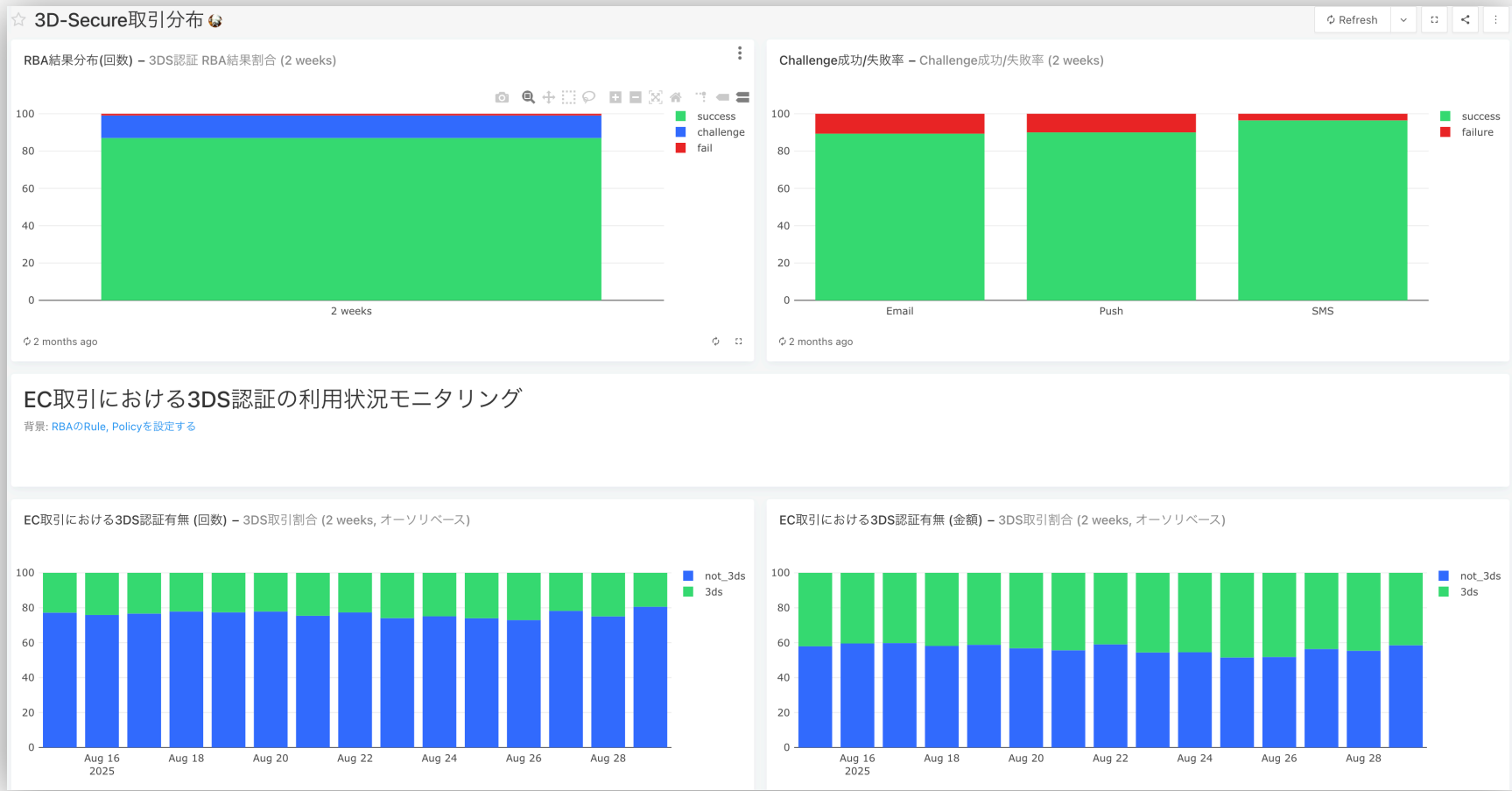
3D セキュア実装のポイント

- 認証フェーズではイシュアは予め設定しておいたリスク判定基準に基づいて本人確認の判定を行う
- VCASの管理画面でチャレンジ認証を発動するルールを設定できる
- チャレンジフェーズではユーザーが選択した認証方式に合わせてOTPなどを生成し送信する
- 結果フェーズで認証情報（ECI / CAVV※）を3DS Serverへ返却する
- 認証成功後、認証情報を含んだオーソリが送信される



3D セキュアの設定 & モニタリング

- 3D セキュアの結果をRedashでダッシュボード化して定期確認を行なっている
- 3D セキュアのチャレンジ率が 3 ~ 15%程度に収まっているか
- 各認証方式毎の成功 / 失敗率のチェック、失敗率が 20%以下に収まっているか
- VCASでの取引結果の確認
 - ユーザーからの不正申請時に3D セキュアが成功しているかのチェック
 - チャレンジ認証を実行するルールの定期見直し



Transaction Detail Report												
Date/Time (GMT)	Trans ID	PAN	Merchant Name	Local Amt.	USD *	Device Channel	Device Data	Risk Score	Authentication Type	Authentication Status	Confirmed Markings	
2025/11/18 02:54:16.835	6e5b075-4712-4...	402321*****8048	WotTicket	¥1,580 JPY	\$12.50 USD	SMW	IL	04	Risk Based	Fully Authenticated	Not Marked	
2025/11/18 02:54:16.725	4963255a-4b1a-4...	402321*****8048	WotTicket	¥1,720 JPY	\$13.68 USD	SMW	IL	04	Risk Based	Fully Authenticated	Not Marked	
2025/11/18 02:54:13.388	62441259-13ab-4...	402321*****8048	SQUARE ENIX	¥1,300 JPY	\$10.28 USD	SMW	IL	01	Risk Based	Fully Authenticated	Not Marked	
2025/11/18 02:54:04.891	9254309a-4053-4...	402321*****8052	PARFUM	¥20 JPY	\$0.12 USD	APP	IL	06	OTP - SMS	Merchant Cancelled	Not Marked	
2025/11/18 02:54:00.936	44f6a025-aab8-4...	402321*****8042	CHIBANK	\$17.00 GBP	\$22.35 USD	SMW	IL	02	OTP - SMS	Fully Authenticated	Not Marked	
2025/11/18 02:53:51.226	5a5777be-4b4d-4...	402321*****8018	SM JAPAN H3J20625	¥1 JPY	\$0.00 USD	SMW	IL	01	Risk Based	Fully Authenticated	Not Marked	
2025/11/18 02:53:40.086	3452a147-108b-4...	402321*****8028	Disney Mobile Order	¥1,580 JPY	\$12.50 USD	SMW	IL	02	Risk Based	Fully Authenticated	Not Marked	

まとめ

今日お話ししたこと

 イシュアはISO8583のVisa拡張された決済電文仕様を理解し
不正決済の判定ロジックに組み込んでいる

 過去の不正被害や攻撃情報からルールベースでの不正検知システムや
個別の対策する防御システムを構築し不正を抑制している

 不正は終わりになき戦い、運用の中で
モニタリングとロジックのチューニングを行っている

ご清聴ありがとうございました