資料 1-5

不正利用対策の考え方と対策例

ＮＲＩセキュアテクノロジーズ株式会社
マネジメントコンサルティング事業本部
決済セキュリティコンサルティング部

2025年4月11日

NRIセキュアテクノロジーズ
NRI SecureTechnologies

Envision the value,
Empower the change

01 はじめに（自己紹介）

02 現在の不正利用の状況

03 不正利用に関わる複層的対策に関する考察

04 不正利用に関わる対策の高度化に向けた考察

05 まとめ

1. はじめに（自己紹介）

プロフィール

須田 直亮（すだ なおあき）

経歴

- 2006年4月　外資系ITサービス会社入社
  カード決済向けミッションクリティカルシステムの
  要件定義・設計・構築・保守運用に従事
- 2014年7月　株式会社野村総合研究所入社
  NRIセキュアテクノロジーズ株式会社に出向
  セキュリティコンサルティング業務に従事
- 現在　決済セキュリティコンサルティング部 部長
  （日本カード情報セキュリティ協議会 副委員長）

専門

- 決済セキュリティ全般、情報セキュリティ・システム監査
- 暗号鍵の設計運用に対する評価・対策提言

資格等

- CISM公認情報セキュリティマネージャー
- CISA公認情報システム監査人
- QSA(Qualified Security Assessor)
- 3DS Assessor
- P2PE Assessor
- QPA(Qualified PIN Assessor)

主要プロジェクト

- 割販法対応含むEC加盟店向け不正利用対策の強化支援
- EMV 3Dセキュア提供に向けたPCI 3DSコンサルティング/準拠審査
- スマホ・EC決済サービスに関するセキュリティリスク評価/対策立案
- スマホ決済における本人認証システムのセキュリティ強度調査
- 決済サービスにおける暗号鍵管理システムの高度化支援
- インシデント発生EC加盟店におけるカード取扱業務の再開支援
- PCI DSSを始めとした各種認証取得支援（PCI DSS/P2PE/PIN/TSP）
- 新決済基盤のISO20022対応に向けたセキュリティアドバイザリ支援
- ブロックチェーンを利用したSTO発行における暗号鍵管理のセキュリティリスク評価

著書・論文等

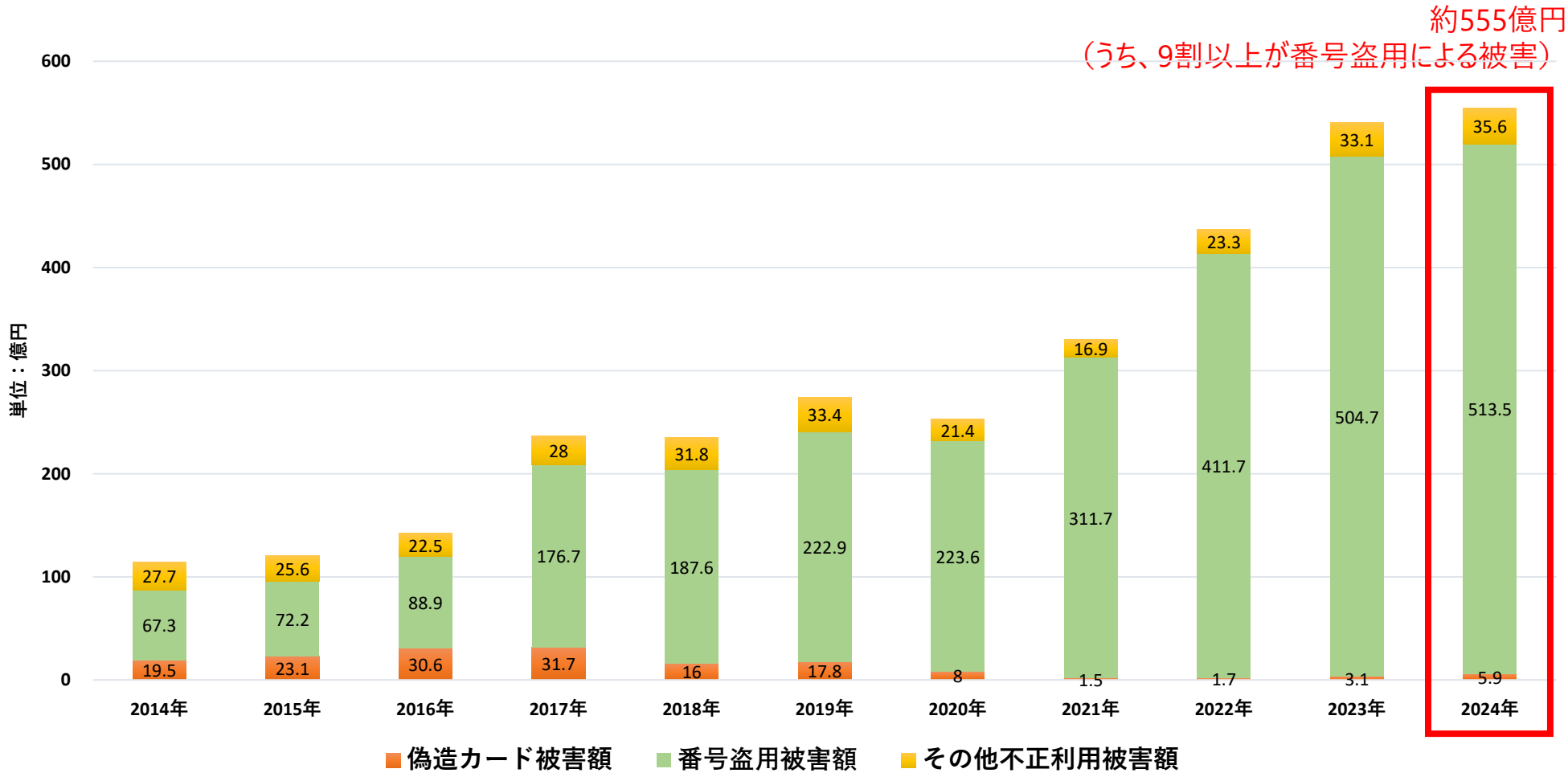
- 金融ITフォーカス 2017年1月号（野村総合研究所）
  - 『P2PEによって新たな局面を迎えるクレジットカード決済』
- NRIジャーナル（野村総合研究所）
  - 『デジタル時代の情報セキュリティを支える「暗号鍵管理」とは』
- ITロードマップ 2022（東洋経済新報社）
  - 『非接触決済に関する新たな取り組みとそれを支えるセキュリティ ～ グローバルトレンドからみえるキャッシュレス決済の新潮流』
- 日経xTECH（日経BP）
  - 『ITサービスの要「鍵管理」って何だ？キャッシュレスブームを陰で支える新技術 P2PEの威力を知る』
- 日経FinTech（日経BP）
  - 『暗号資産保護における「鍵管理」の重要性』

2. 現在の不正利用の状況

国内におけるクレジットカード不正利用被害の状況

2024年も過去最高を更新（約555億円）し、うち9割以上が番号盗用による被害である。

クレジットカード不正利用被害の状況

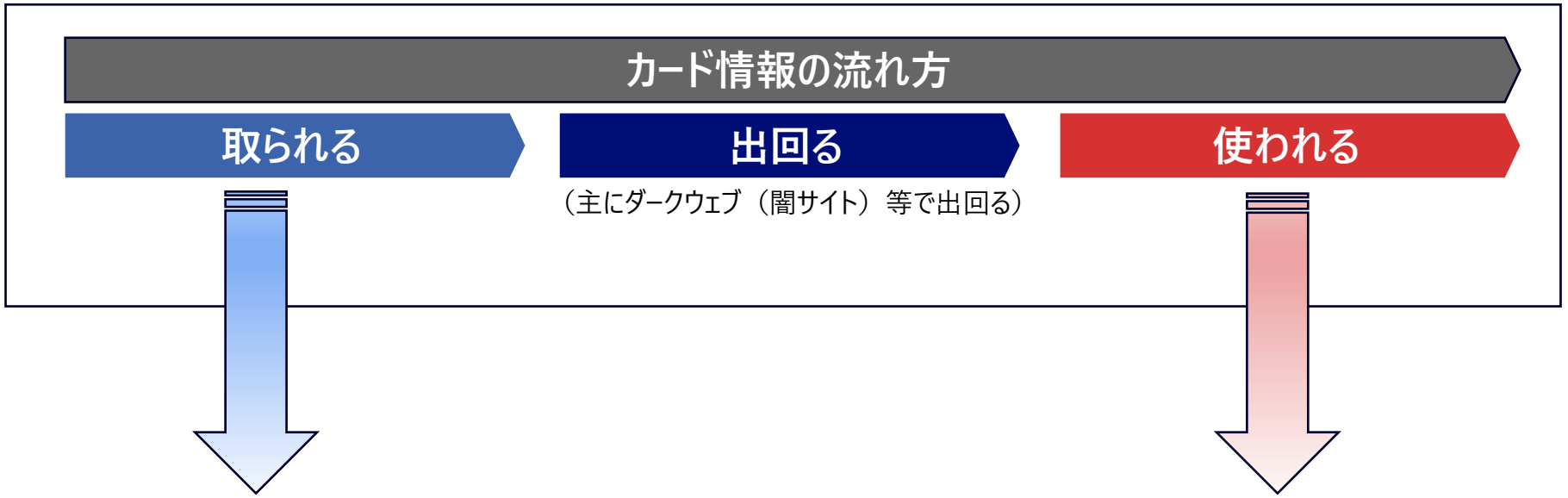


（出典：一般社団法人日本クレジット協会　クレジットカード不正利用被害額の発生状況　をもとにNRIセキュア作成）

非保持化/PCI DSS準拠済みのサービス・システムでも、不正利用対策はなぜ必要なのか？

カード情報を取られないようにすることと、使わせないようにすること、は異なる対策であるため。

カード情報の流れ（不正決済に至るまで）



カード情報を取られないようにする対策（漏洩防止）

クレジットカード・セキュリティガイドライン6.0では、
（非保持化orPCI DSS準拠）＋ 脆弱性対策

カード情報を使わせないようにする対策（不正利用防止）

クレジットカード・セキュリティガイドライン6.0では、
線の考え方に基づく各種対策

EC加盟店に対する攻撃（カード情報の不正窃取と不正利用）

どういった加盟店が、最も狙われやすいのか？

主に狙われやすい加盟店

カード情報を取られる（不正窃取）

システムセキュリティが脆弱なEC加盟店
（非保持化だけの対策に頼るEC加盟店）

カード情報が使われる（不正利用）

本人確認/認証などが甘いEC加盟店
高額や換金性の高い商材を扱うEC加盟店

悪意のあるものの心理（モチベーション）としては、以下のような状態になりやすい。

- ✓ **システムセキュリティが脆弱なEC加盟店（非保持化だけの対策に頼るEC加盟店）ほど、簡単にカード情報を窃取できるため、攻撃者視点では旨味がある。**
- ✓ **本人確認/認証が甘く、より高額や換金性の高い商材を扱っているEC加盟店で不正決済したい。**

※不正窃取されたカード情報はダークウェブ（闇サイト）上で転売され、最終的には様々なEC加盟店で不正利用されるケースが多い。
（必ずしも一つの加盟店で同一のカード情報の不正窃取・不正利用が、同時発生しているわけではない）

不正利用に関する手口やターゲットの変化

2024年度は、EMV 3Dセキュア認証回避や認証強度が弱い箇所を狙った攻撃が多く発生。今後は、リアルタイムフィッシングはじめ、より高度な攻撃が主流になる可能性もある。

2024年確認された主なクレジットカードの不正利用事案	概要
EMV 3Dセキュア認証を回避する攻撃	
ACSサーバに対するDDoS攻撃による3Dセキュア認証回避	業界全体でEMV 3Dセキュア導入が進む中で、カード情報だけでは不正利用が困難となった結果、**従来のサイバー攻撃と組み合わせた攻撃手口も確認**。
認証強度が相対的に弱い箇所を狙った攻撃	
Apple Pay/Google Payの不正利用、オフライン決済の悪用	業界全体でEMV3Dセキュア導入が進む中で、カード情報だけでは不正利用が困難となった結果、**EMV3Dセキュアより相対的に不正利用が容易な攻撃手口に移行**。
不正トラベル	2019年に一度流行った手口でもあり、2020年のコロナウイルス流行を受け一度減少したが、最近のインバウンド需要拡大に伴って再度流行。 **EMV 3Dセキュア未導入の旅行予約サイトが狙われた可能性がある**。
課金代行による不正利用	本スキームは過去から存在するが、今般はアダルトゲーム中心の事案が見られ、**不正利用対策が脆弱な小規模運営組織を狙っている可能性がある**。
デジタル地域通貨を使った不正利用	2023年-2024年にかけて複数のデジタル地域通貨にて盗難クレジットカードによる不正利用が発生。性質上、サービス提供期間が限定的であることから、**EMV 3Dセキュア導入を見送った自治体のデジタル地域通貨が狙われたと推察**。
その他（流行の変化を狙った攻撃など）	
トレーディングカードやシューズを狙った不正利用	流行の変化に伴い、盗難クレジットカードの**マネタイズ先としてこれまで比較的狙われてこなかった商品を狙った不正利用を確認**。

3. 不正利用に関わる複層的対策に関する考察

不正利用対策の考え方の推移

「4つの方策」から「線の考え方」へと移行

クレジットカード・セキュリティガイドラインに見る不正利用対策における指針整理

クレジットカード・セキュリティガイドライン	EC加盟店に求められる不正利用対策における指針	今後の対策への期待
5.0まで	**4つの方策** 本人認証（3Dセキュア認証、認証アシスト） 券面認証（セキュリティコードによる認証） 属性・行動分析（不正検知） 配送先情報（不正検知）	カード決済の一連の流れを踏まえて適切な対策を講じる。 ※点での対策ではなく、線の概念に基づく対策（複層的な対策）
6.0以降	**線の考え方（概念図）** 	

（出典：一般社団法人日本クレジット協会　クレジットカード・セキュリティガイドライン6.0 をもとにNRIセキュア作成）

なぜ複層的な対策が必要なのか？

単一点のみの対策（点での対策）では、巧妙化する攻撃を防ぎ切れない。

A社事例（チケット販売サイト）

不正利用の発生状況

概要

＜サービスおよび被害状況＞
- A社は、チケット販売サイトを運営。チケット購入含むサービスの利用には、会員登録が必須。
- 特に高額チケットを狙った不正被害の件数が、急増（払い戻しや風評被害などの影響もあり）。

＜手口＞
- ログイン画面を突破され、予め登録された正規会員のカードで購入。または不正入手されたカードを紐づけられ、不正に購入。

原因と対策

原因

- **主たる不正利用対策がEMV 3Dセキュアのみ**

対策案

① 会員登録時とログイン時の認証強化
② 不審なIPアドレスからのアクセス制限
※ 別途、不正検知ソリューション導入も検討。

ポイント

割賦販売法に基づく実務指針に沿った対応として、決済時のEMV 3Dセキュアだけでは、不十分となる場合が多く存在。
カード決済の一連の流れの入口部分（カード決済前の会員登録/ログイン/属性情報変更など）で、適切な不正ログイン対策を合わせて検討・実施しておくべき。

単純に複数の対策を組み合わせればよい？

複層的な対策をする上でも、リスクに応じて個々の対策の実施範囲を見極める必要がある。

B社事例（Webショッピングサイト/スマホ決済サービス）

不正利用の発生状況

概要

＜サービスおよび被害状況＞
- B社はショッピングや各種会員向けサービスを提供するWebサイトと対面店舗向けのスマホ決済アプリを提供。
- スマホ決済アプリはクレジットカードなどの決済手段と紐づけが可能。

＜手口＞
- Webサイトを通じて電話番号を書き換えられ、スマホアプリのSMS認証が突破されて、不正決済される。

原因と対策

原因

- **スマホアプリ側ではSMS認証が実装されており強固であったが、アカウントを共有している「Webサイト」側の認証が相対的に脆弱（依然としてID/パスワードによる認証のみ）であった。**

対策案

Webサイト側での認証強化
①ログイン時の多要素認証
②電話番号の変更時の認証強化

ポイント

サービス全体において、電話番号変更が可能な導線がどの程度存在するか、導線毎に認証強度の差がないかを把握する必要がある。特に、Webサイト、スマホアプリ、コールセンター、書面による郵送、etc、の決済チャネルや会員属性の変更に関わる導線を正しく把握し、リスクに応じて対策の実施範囲を決めていく必要がある。

4. 不正利用に関わる対策の高度化に向けた考察

不正利用に関わる対策の高度化に向けた考察

仕組みづくり（システム）と、態勢づくり（組織態勢）、両観点からの考察

不正利用対策の高度化に向けた考察の観点

	観点	本日お話しする内容
①	仕組みづくり（システム）	不正検知を想定した属性・行動分析の考え方
②	態勢づくり（組織態勢）	①を適切に回していくための態勢整備に向けた考え方

観点①仕組みづくり：不正検知が求められる理由その１

サイバー攻撃の巧妙化により、本人認証の厳格化だけでは防ぎ切れない事案も多く発生。

- 近年、商取引や金融・決済サービスのWeb化が進む過程において、「なりすましログイン・不正決済」、「換金性の高い商品へのポイント交換・転売」等のサービス不正利用被害が多発。
- 本人認証の厳格化に加え、ユーザーの行動パターンや取引内容における不正検知の必要性が高まってきている。

背景

サイバー攻撃の手口が変化／特殊詐欺・不正利用が多発

- システム停止や情報窃取ではなく、金銭獲得や詐欺を目的とした業務・サービスの仕様を悪用した被害が増加
- システム上のエラーではなく、業務ロジック上の盲点を突いた詐欺行為のため、既存のセキュリティ対策では予防・検知が困難

必要な取り組み

業務・サービスの不正利用防止に係る包括的な検討が必要

- 業務・サービス利用時の本人確認のプロセス強化や多要素認証等の導入による本人認証の厳格化
- 業務・サービス内におけるユーザー行動や取引内容に関する不正およびリスクの検知

（参考）国内における主な不正利用被害の事例

■ **証券業**

✓ なりすましログイン・不正出金による約1億円の流出

■ **小売業**

✓ 不正アクセス・なりすましチャージ・商品購入により、約5500万円の流出、当該サービスの廃止

■ **銀行業**

✓ なりすましによる約330万円の不正送金被害および氏名、カード番号、購買履歴等の情報流出、当該サービス廃止

■ **通信業**

✓ なりすましによる約3000万円の不正な預金引き出し・商品の不正購入

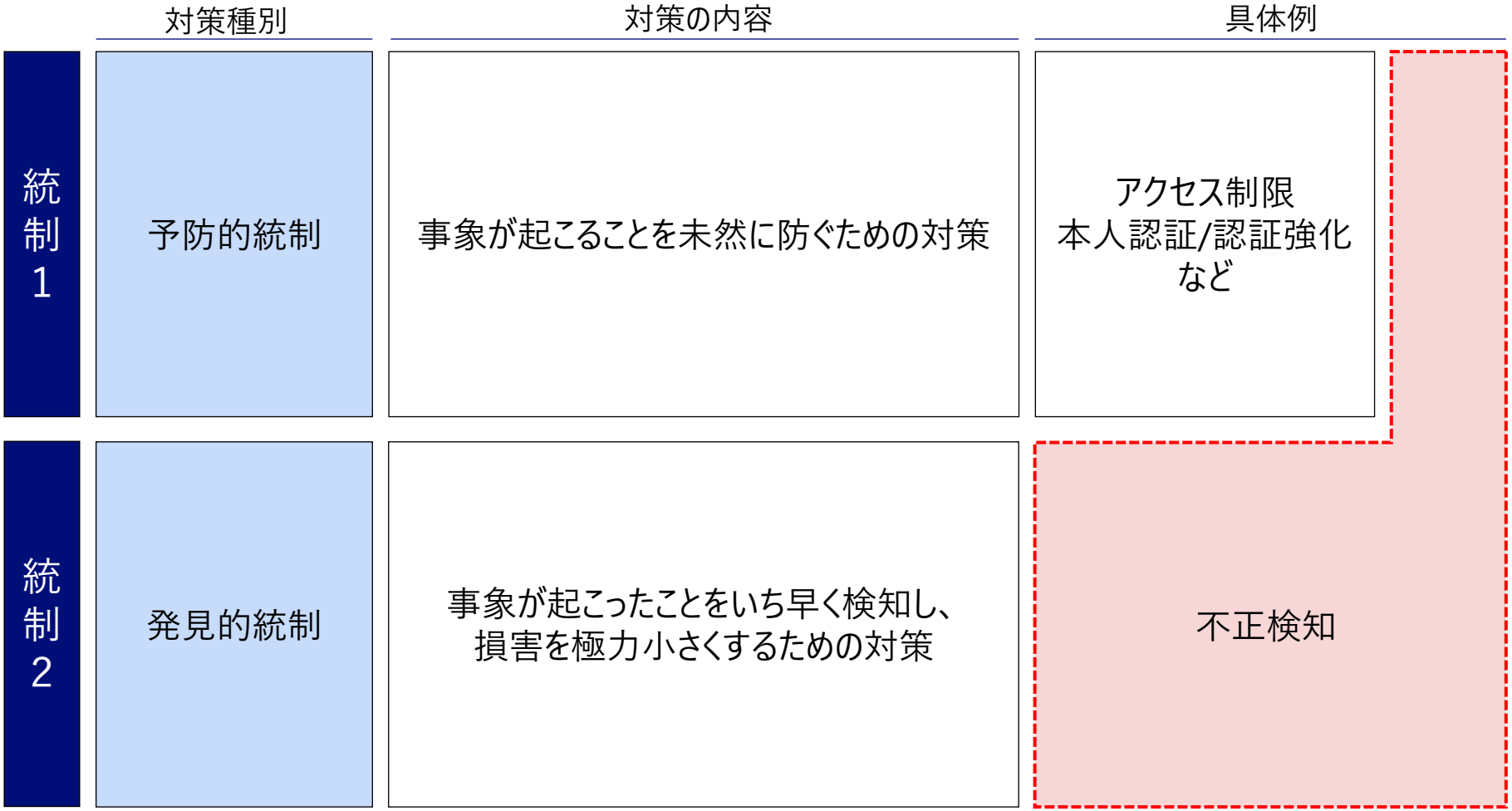
■ **運送業**

✓ なりすましログインによる約3400件のID、メールアドレス、氏名、電話番号、性別、郵便番号、住所、クレジットカード情報等の流出

観点①仕組みづくり：不正検知が求められる理由その２

不正利用対策を考える上で、不正検知は予防的/発見的統制の両方の観点で有効である。

不正に対する対策の基本的考え方

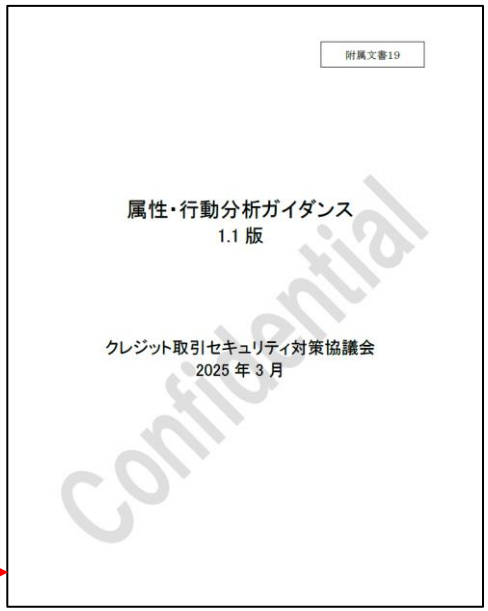


観点①仕組みづくり：不正検知による対策の高度化に向けて

属性・行動分析は不正検知による対策を考える上で、事業者毎のレベルに違いが生じやすい。

- 世の中におけるクレジットカードの不正利用対策について、現状で検討可能な対策項目単位で見た場合、おおよその洗出し自体は、既にされている状況にあると思慮。
- EMV 3Dセキュア以外の対策が備わってないEC加盟店に今後いかに追加対策（複層的対策）を広く求めていくか、という課題がある一方、個々の対策の深掘り方に応じて、不正が一定程度抑えられているEC加盟店とそうでないEC加盟店とに違いが生じているケースがあるものと推察。
- 特に、属性・行動分析は、不正検知の対策を考える上で、対策レベルに違いが生じやすい。

線の考え方（概念図）と属性・行動分析ガイダンス（付属文書19）



（出典：一般社団法人日本クレジット協会　クレジットカード・セキュリティガイドライン6.0 ）

属性・行動分析を考える上で参考となる専用の付属文書（属性・行動分析ガイダンス）が用意されている。

観点①仕組みづくり：不正検知による対策の高度化に向けて

カード取引の不正検知の仕組み考える上でのレベル段階分け（参考例）

レベル段階分け（参考例）

不正検知のレベル	利用する主な分析項目	特徴
6	属性（個人属性情報、加盟店ECサイト会員情報） ＋行動（購買情報、決済情報、位置情報、デバイス情報、ビヘイビア情報） ＋**外部情報（自社外での不正実績情報、脅威情報など）**	外部の不正データを利用することで、自社外ですでに不正実績のある利用者を事前に弾くことができる
5	属性（個人属性情報、加盟店ECサイト会員情報） ＋行動（購買情報、決済情報、位置情報、デバイス情報、**ビヘイビア情報**）	ビヘイビア情報を利用することで、機械的操作や流れ作業といった一般利用者ではない動きを検知できる
4	属性（個人属性情報、加盟店ECサイト会員情報） ＋行動（購買情報、決済情報、位置情報、**デバイス情報**）	デバイス情報を利用することで、一般利用者ではない設定やなりすましによる利用・再入会を検知できる
3	属性（個人属性情報、加盟店ECサイト会員情報） ＋行動（購買情報、決済情報、**位置情報**）	位置情報を見ることで、サービス対象外のエリアからのアクセスや不自然なアクセスが検知できる
2	属性（個人属性情報、加盟店ECサイト会員情報） ＋**行動（購買情報、決済情報）**	主に加盟店側で保有している情報で実現できる
1	**属性（個人属性情報、加盟店ECサイト会員情報）**	仕組みがシンプルであり、最も低コストで実現できる

高 ↑ 中 ↓ 低

現行のガイダンスにおける属性・行動分析の期待値（推測）↑

ポイント

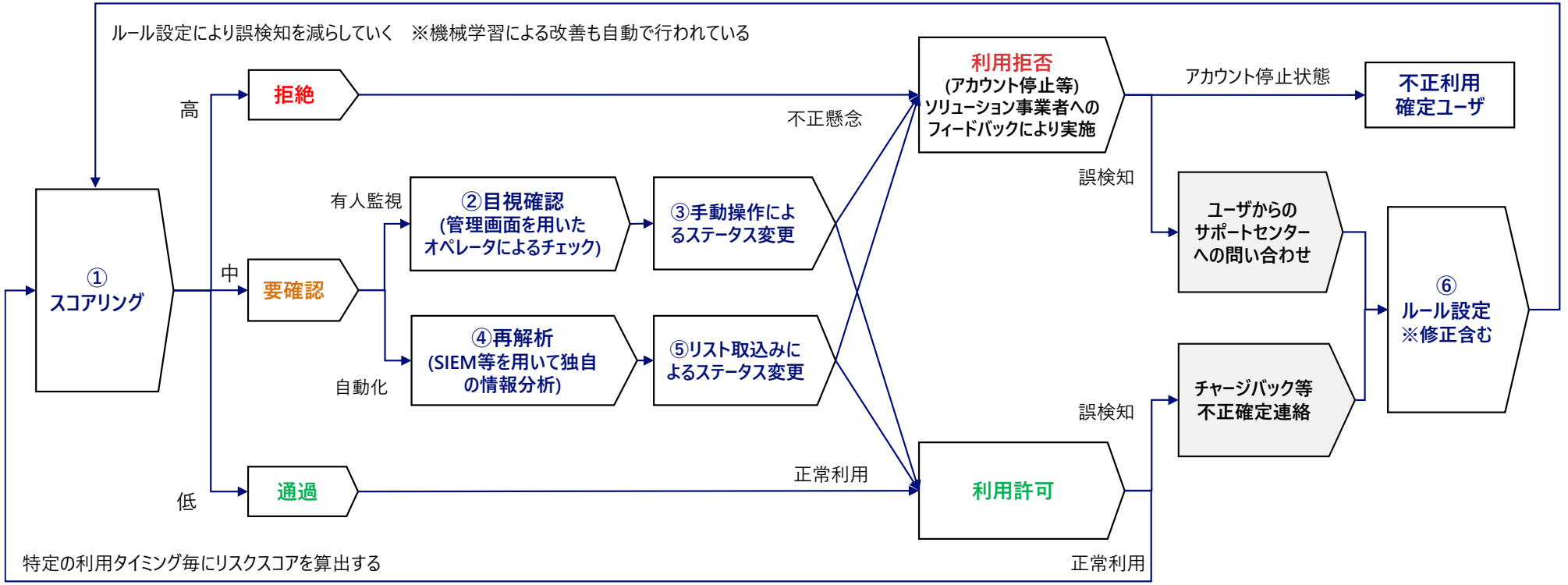
- Lev1（単純パターンマッチング）では、回避されやすく、また、利用阻害（誤検知）に繋がるといった可能性も高いため、より多くの分析項目を用いてスコアリングする方式が推奨される。
- Lev2以上からは、属性情報に加えて、行動情報の分析が行われ、レベルに応じて分析項目の要素が追加されていく。
- Lev4以上が、現行のガイダンスにおける属性・行動分析としての本来の期待値と推測（弊社推測）
- 日々変化する不正利用への対応が求められることになるため、定期的な検知ルールの見直しが必要（次頁参照）。

観点①仕組みづくり：不正検知による対策の高度化に向けて

日々の不正監視の運用フローを回し、検知ルールの見直しを図り、誤検知を減らしていく。

■ ユーザが利用するたびにスコアリングが行われ、判定結果に応じた対応を行い、ルールの見直し（設定・修正）を行うことで、検知精度を上げていくことを継続して繰り返していく。

不正監視の運用フロー（参考例）



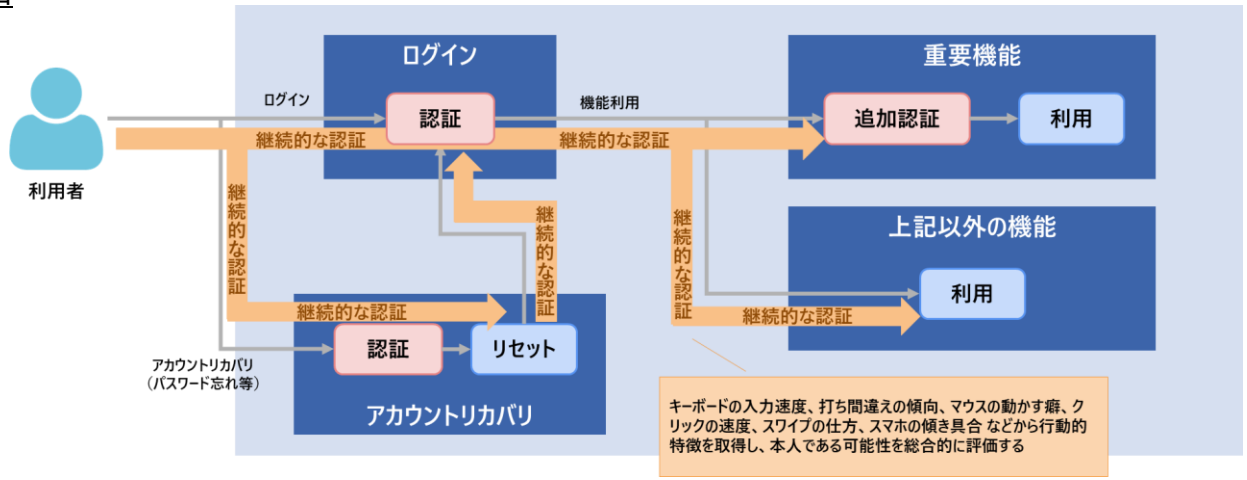
観点①仕組みづくり：ご参考

行動的生体認証について

■ PCやスマホなどの操作における癖や傾向といった利用者の行動に関わる特徴を、ビヘイビア情報として活用し、本人確認を行う仕組み。

■ ログインからログアウトまで継続して認証できるという利点を有する。

認証イメージ図



メリット/デメリット

● メリット

✓ **模倣および詐称への耐性**：行動的特徴を利用するため、模倣および詐称への耐性は高い

✓ **継続的な認証**：サービスを利用している間、行動的特徴を収集して本人確認を継続的に実施可能

✓ **利用者の負荷の低さ**：サービス利用者は認証を意識することがないため利便性を損なわない

● デメリット

✓ **誤判定のリスク**：誤判定リスクは少なからず存在（例：端末の機種変更やケガによる行動的特徴の変化などでの誤判定、等）

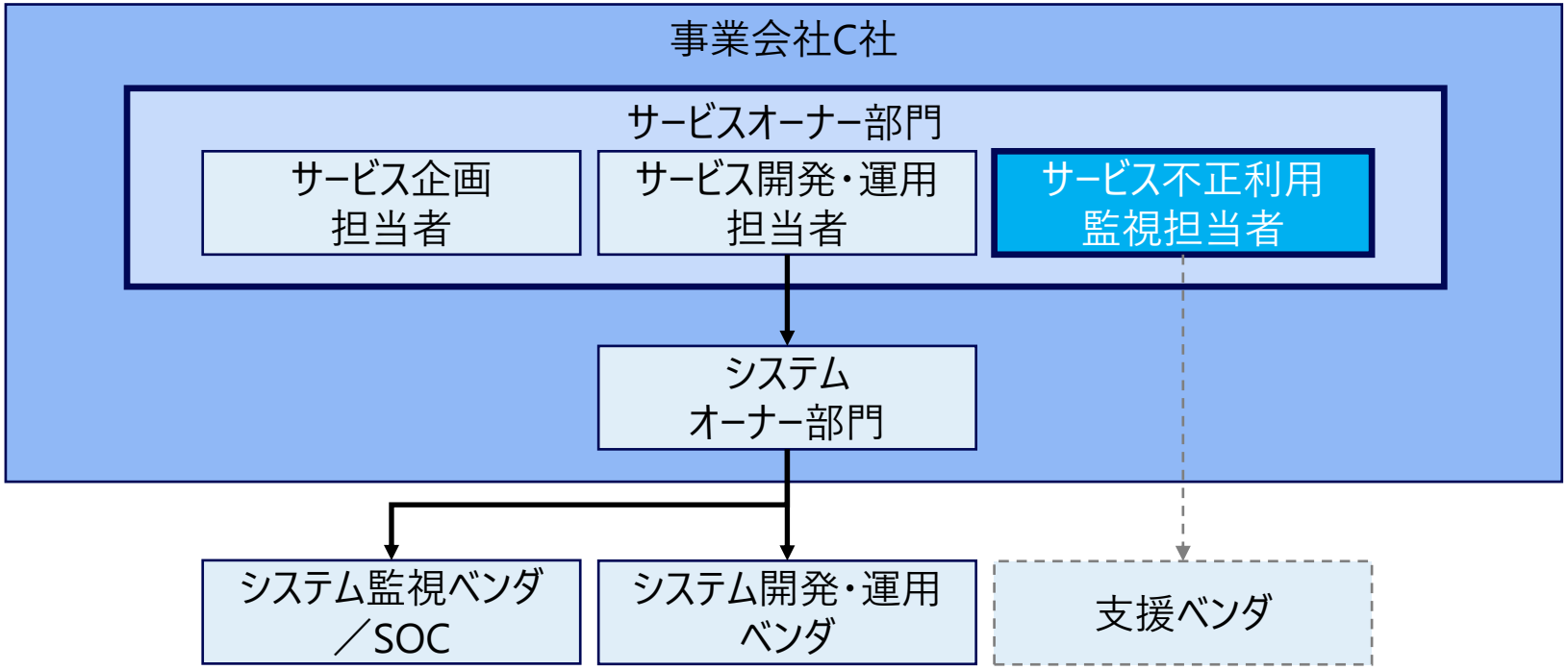
✓ **取得する情報のプライバシーリスク**：行動的特徴を収集するためプライバシー面での整理が必要となる

観点②態勢づくり：運用組織などの検討

不正監視の運用フローを回し、ルールの見直しによって不正検知の精度を上げていく上では、サービスオーナー部門に、不正利用の監視担当者を設置することが、より効果的。

- なりすましログインや不正決済等のサービス不正利用疑いは、対処として疑わしいユーザーのIPブロック、アカウント停止、トランザクション取り消し、身に覚えのある取引かの電話確認、パスワード強制変更等が考えられる。
- これらに迅速に対応する上での態勢づくりとして、サービス側の不正利用はビジネスとして何が対象かを定義する必要があるため、不正利用の監視担当者をサービスオーナー部門に設置する事例がある。属性・行動分析における不正検知において、ルールの見直しによる検知精度の向上を継続的に図っていく上では、より効果的となる。

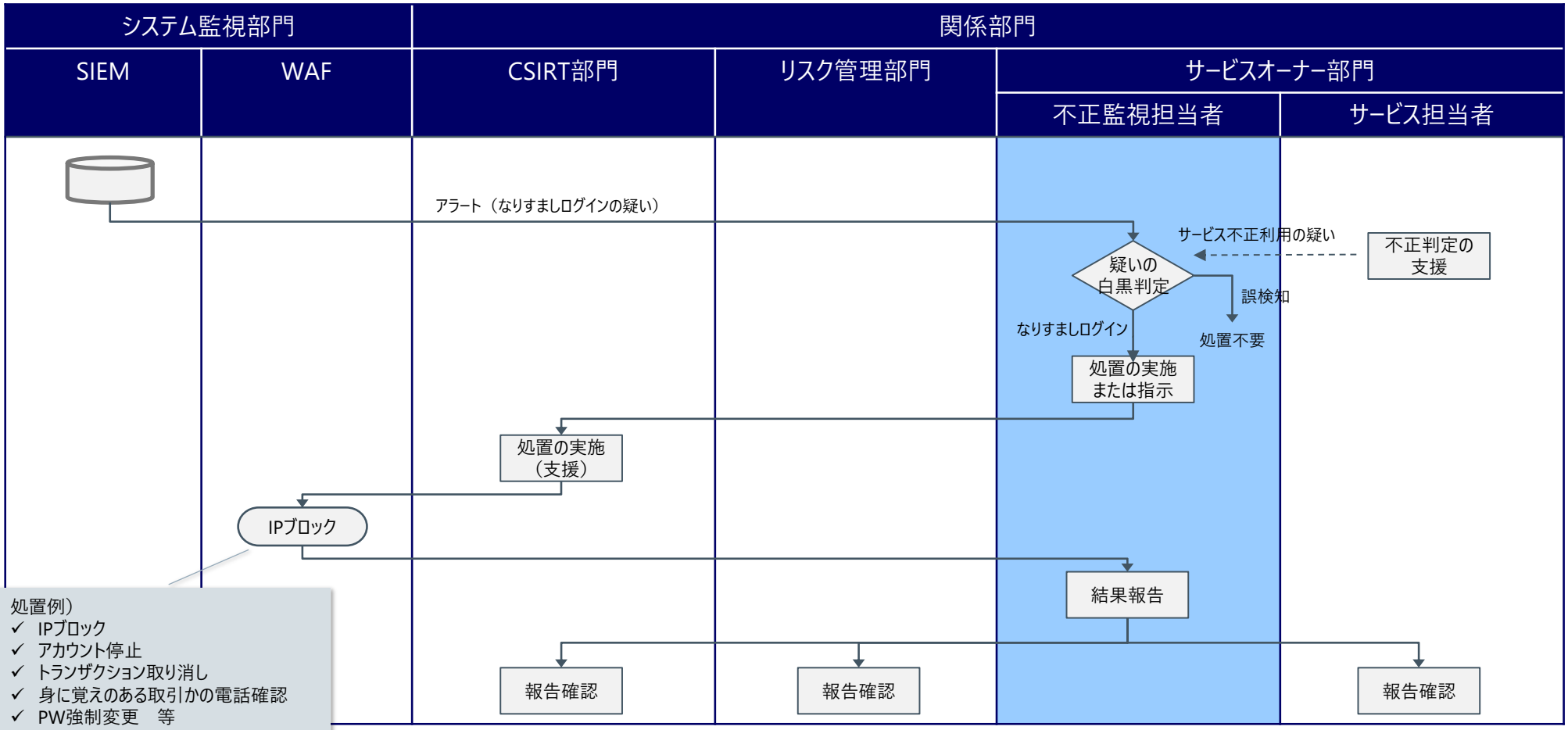
運用組織の検討イメージ



観点②態勢づくり：運用組織などの検討

不正利用監視担当者を介すことで、不正検知の結果やサービス影響に即した、素早い判断・対応が可能となり、結果に基づくルール見直しによって継続的な検知精度の向上にも繋がる。

組織間の連携イメージ



※一連の対応においてAI等も活用することにより、さらなる精度向上や運用負荷軽減につなげられる可能性もあり。

観点②態勢づくり：ご参考

外部情報を積極的に活用する高度なレベルの態勢づくりのご紹介（SSIRTのご紹介）

- SSIRTは「第1線」で、事業部門と同等の立場で、サービス守る専門組織。
- 「不正利用の監視」のみならず、サービスリスク分析や不正検知のための脅威情報収集など、サービスを提供する各事業部門に対して、全社横断的に対応する。
- 大企業かつ多角的に決済サービスを提供している事業者おいては、SSIRTのような専門組織が効果的に機能する。
  （特に、事業部門毎にセキュリティ対策の均一化やナレッジ共有などを高いレベルで維持できるといった効果など）

SSIRT = Service Security Incident Response Team
事業部門と同等の立場(第 1 線)で、事業部門におけるセキュリティ対応を支援

CSIRT：本社機構の立場(第 2 線)で、セキュリティガバナンスの実行を支援

ポイント

外部情報（自社外での不正実績情報・脅威情報など）を積極的に活用した、高度なレベルの不正検知の仕組みを目指す事業者*においては、SSIRTのような態勢づくりが効果的に機能する。

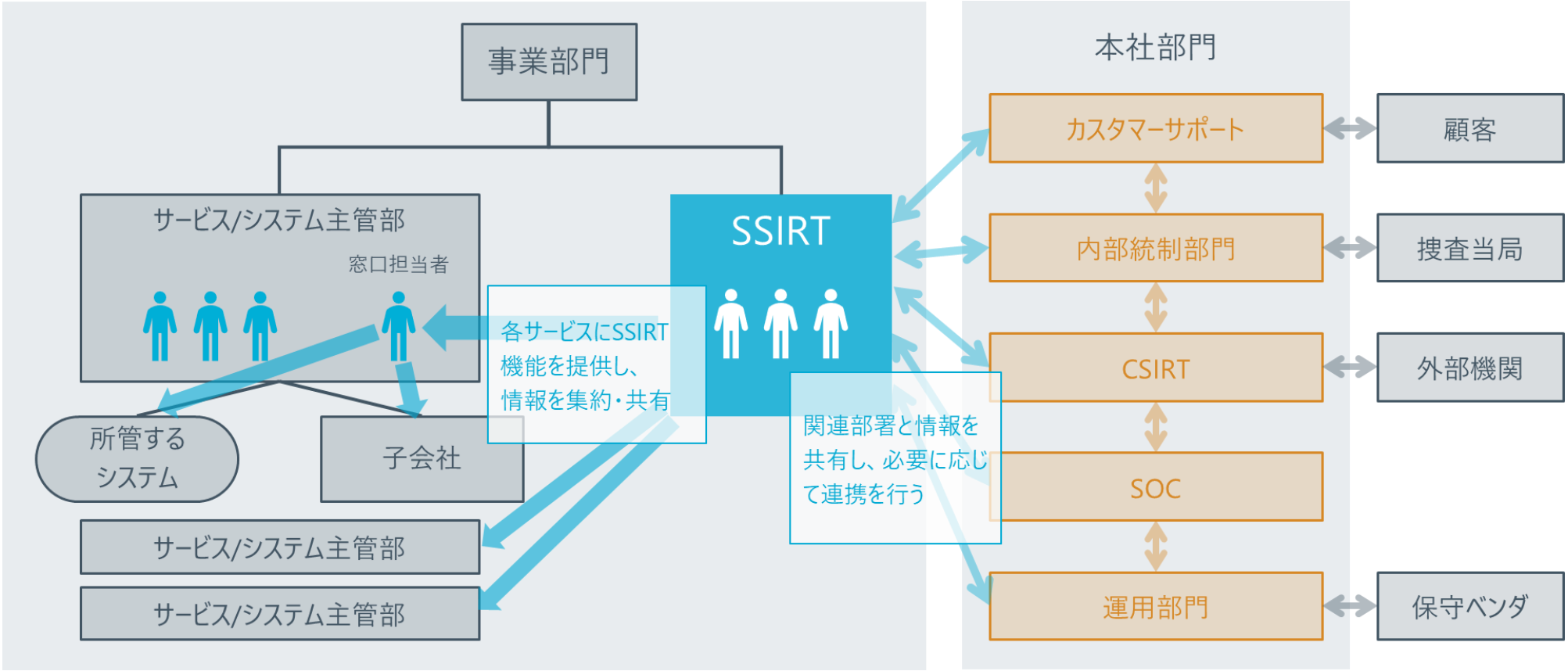
※前出の表（カード取引の不正検知の仕組み考える上でのレベル段階分け）のLevel5までの対応では、不正検知の仕組みにおいて期待する効果が得られない、またはリスクが十分に低減されない懸念がある事業者で、Level6以上を目指すような場合を主に想定。

観点②態勢づくり：ご参考

SSIRTの機能および連携のイメージ（複数事業部門を持つ大企業におけるSSIRT）

- SSIRTを中心とした組織にて、不正利用に繋がりうる脅威情報を収集し、関係部署に連携。
- SSIRTを介して、デジタルサービスリスク分析やデジタルサービスの不正利用の検知、大規模サービス悪用発生時の対応などをスムーズに行う。

SSIRTの機能および連携のイメージ（参考例）



5. まとめ

まとめ

本日お話したこと

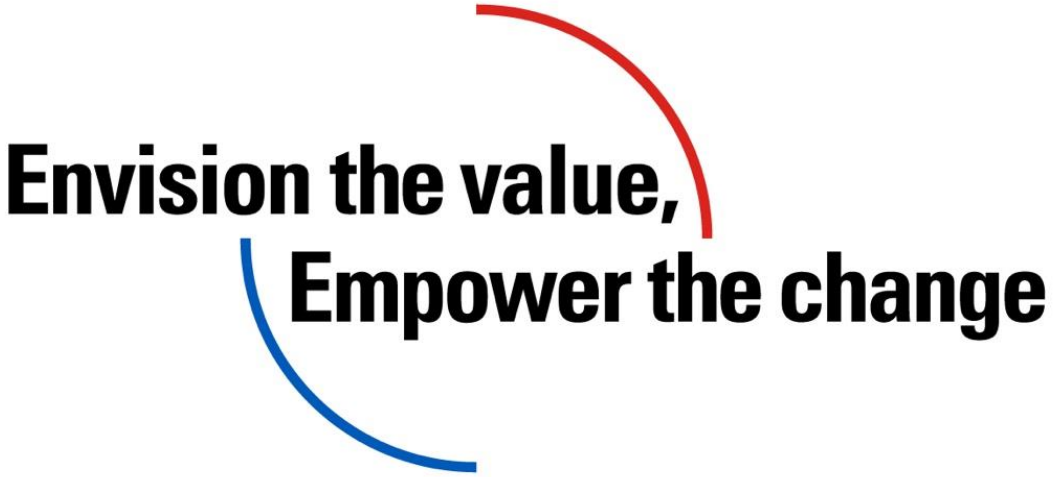
- カード情報を取られないようにすること（漏洩対策）、使わせないようにすること（不正利用対策）とは、それぞれ対策の観点が異なる。

- 2024年度は、EMV 3Dセキュア導入が一定程度進んだ一方で、EMV 3Dセキュア認証の回避や認証強度が弱い箇所を狙った攻撃が多く発生。

- 単一点のみの対策では、巧妙化する攻撃はもはや防ぎ切れず、「線の考え方」の概念に基づく対策（複層的な対策）が必要。決済時のEMV 3Dセキュアだけでは、対応として不十分となる場合が多く存在。

- 複層的対策についても、個々の対策の実施範囲（Web,スマホアプリ,etc を始めとした決済チャネルや会員属性の変更に関わる導線）を、リスクに応じて見極める必要がある。

- 不正利用対策の高度化に向けては、今後、仕組みづくり（属性・行動分析に基づく不正検知の仕組み、etc）と、態勢づくり（サービスオーナー部門に不正利用の監視担当の設置や全社横断的なSSIRT組織などの組成、etc）の両面で、具体的対策の進展が期待される。


Envision the value,
Empower the change