



Zacta

Choose certainty.
Add value.

不正使用対策に向けて ～PCI、EMV対応による アプローチ～

Security Research & Consulting GmbHとの
パートナーシップとEMVの最新動向

- 日本でのセキュリティ認証試験について
- EMVの最新動向



Security Research & Consulting GmbH



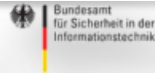
- 長い経験と高い実績
- 従業員約100名 30%以上がPhD取得者
- 設立: 2000年
- ドイツ国内に2拠点(ボン、ウィスバーデン)
- CEO: Gerd Cimiotti

主なセキュリティ評価実績

- コモンクライテリアの評価機関 (ITSEF) としてBSI (ドイツ連邦情報セキュリティ局)に認定 2002～
- EMVCo IC + ICC セキュリティ評価ラボ
- MasterCard CAST および Visa VCSP
- DK/GBIC (ドイツ銀行産業委員会; 2001～)
- PCI セキュリティ評価ラボ PCI-PTS, PCI-DSS, PCI P2PE
- POI セキュリティ評価ラボ UKCA, APCA, DPA



SRCのセキュリティ認証



Cards

POI

Background Processing

German Banking Industry (GBIC, formerly ZKA)
security evaluations

BNetzA: Electronic Signatures
National Network Regulation Body

Common
Criteria

Data Privacy
Protection

EMVCo
IC Evaluator

PCI PA-DSS

gematik
German Health
Care

MasterCard
Logical Audits

PCI PTS

BSI IT Baseline
Protection

MasterCard
Physical Audits

UKCA, APCA,
DPA

ISO 27001

gematik
German
Health Care

PCI
P2PE

PCI DSS



例えば: PCIでの対応範囲

スタンダード&プログラム	SRC
PCI DSS	✓
PCI PA-DSS	✓
PCI PIN	検討中(VISA)
PCI P2PE (QSAおよびPA-QSA)	✓
PCI TSP	手続き中(✓)
PCI CP	✓ (MasterCard)
PCI PTS	✓
PCI ASV	✓
PCI 3DS	✓

デバイスの例



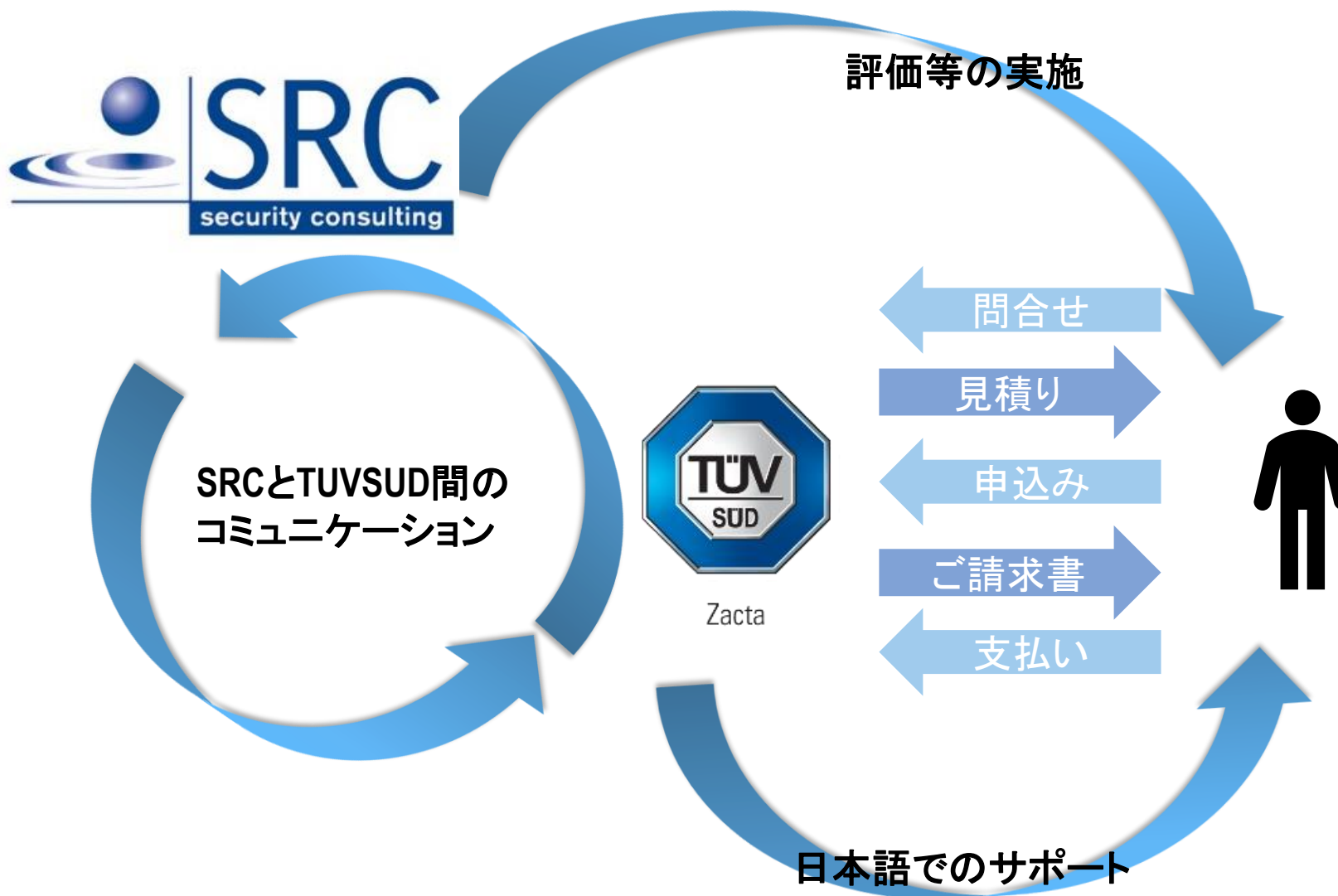


デバイスの例

- PED (PIN入力装置)または UPT POI(普通の決済端末)デバイス
- POS端末やATMに統合される暗号化PINパッド
- POS端末のセキュアコンポーネント (POS端末の中身、プリント基板やモジュール)
- Non-PED: PINを使用しない取引用のもの
- HSM(Hardware Security Module): PIN処理、カードパーソナライゼーション、暗号鍵管理、データ保護に使用されるセキュアな暗号デバイス。

A blue-tinted globe showing the continents of Asia and Australia, with a grid of latitude and longitude lines. The globe is centered in the background of the text.

このSRC社の知識と経験
評価・サポートの申し込みを
日本で受付可能に





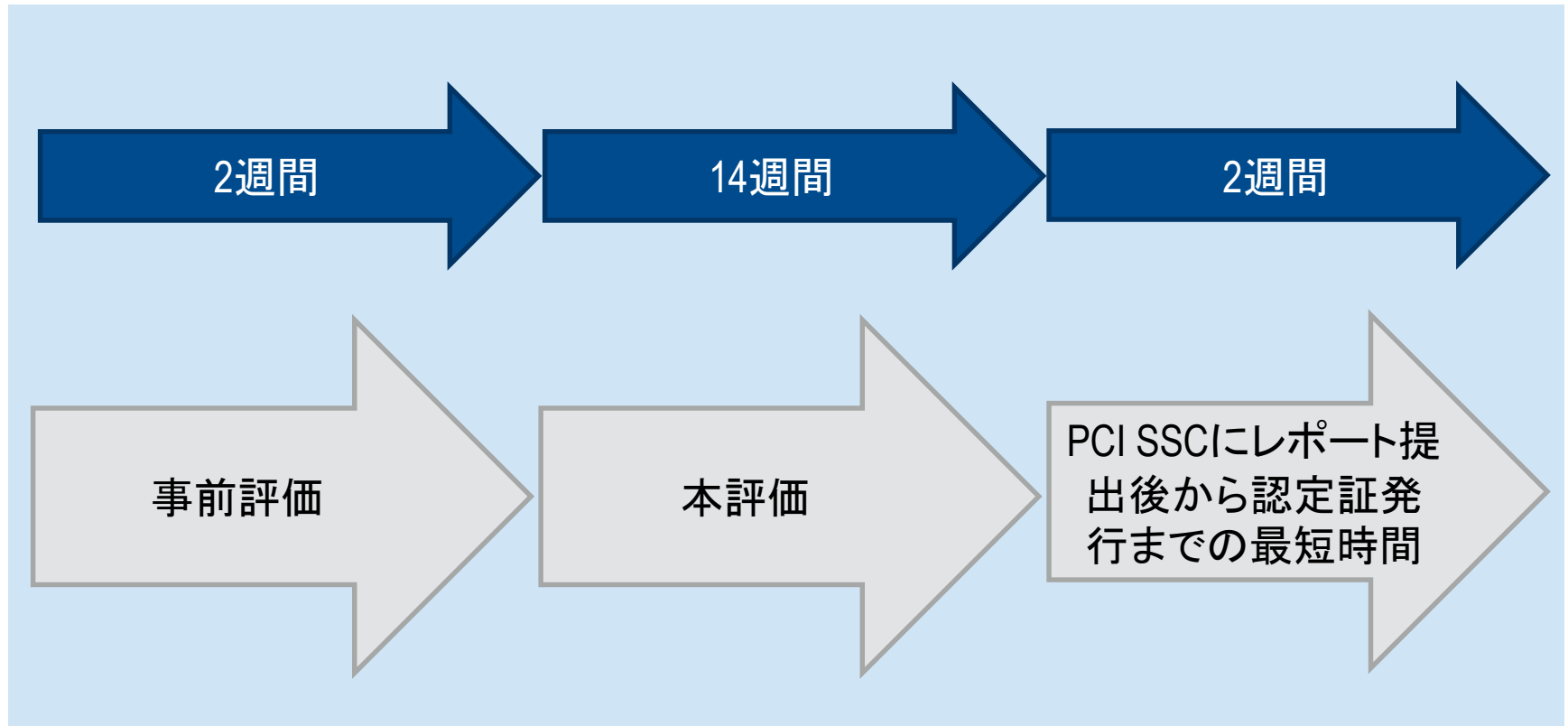
PCI PTSについて

- PCI PTS (PIN Transaction Security)
 - ユーザーのPINデータの盗難からの保護が目的
 - 決済端末とコンポーネントの物理的・論理的セキュリティ

認定について

- SRCが評価を行い、レポートを作成します。認定自体はPCI Security Standard Councilが行います。
- ベンダーはラボに対して必要資料と実機を提出する
- SRCでは適用される全てのセキュリティ要求事項に対する評価を実施しレポートを作成する
- 部分的な認定は不可 (例: マイクロプロセッサに対してのみの認定)

- 認定の所要時間例





- EMVの生体認証
- 2nd Genから：セキュアチャネル
- 2nd Genから：対リレーアタック





- 接触型が対象
- 仕様書上有効になったのは2018年1月1日から
- PINやサインと同様の本人確認手段の一つ
- EMV認定はEMVレベル2カーネルの一部として実施される

- 大きく5つのカテゴリーが規定されている

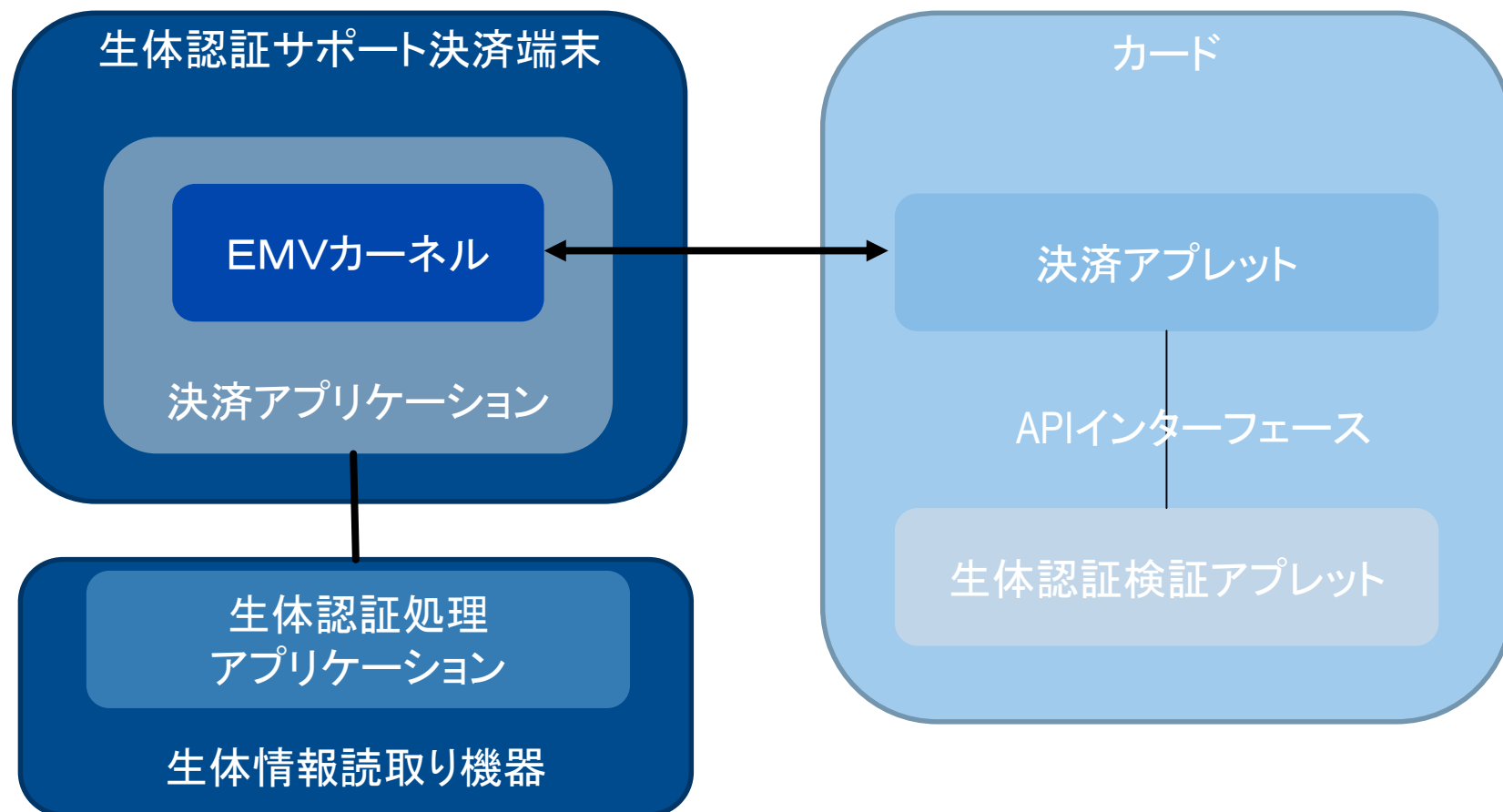
- 顔
- 指（指紋/静脈）
- 虹彩
- 掌
- 声紋

サブカテゴリ

- 右
- 左
- 親指
- 人差し指
- 中指
- 薬指
- 小指
- 掌
- 手の甲
- 手首

- オフライン生体認証とオンライン生体認証がある

生体認証の実装の例





2nd Genとは： EMVの次世代仕様

- 接触と非接触に共通なアプリケーション
- モジュール式でフレキシブル
- RSAから楕円暗号(ECC)へ
- 現在仕様のドラフト版のレビューとフィードバックをEMVCoで行っている。

- セキュアチャネル

カードとの安全なコミュニケーションを担う

カード・端末間のコミュニケーションが暗号化される

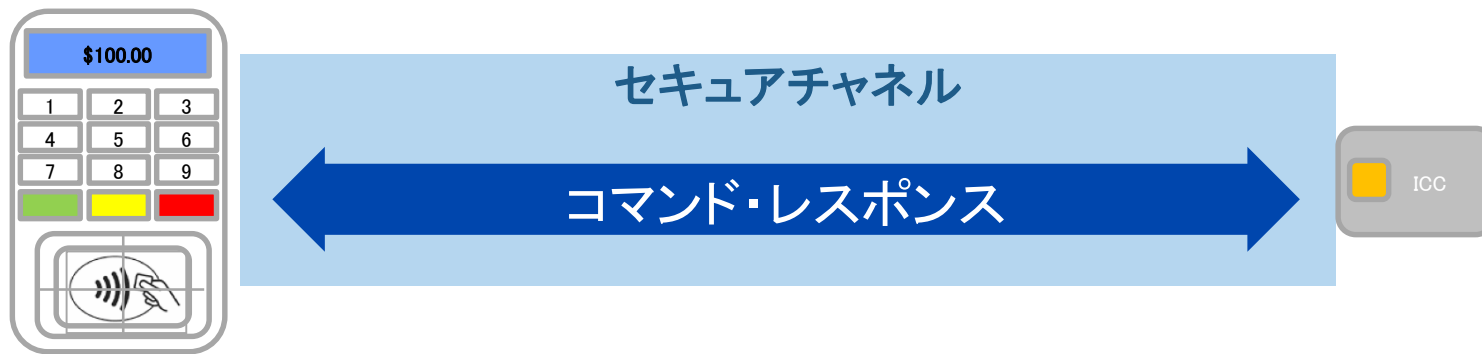
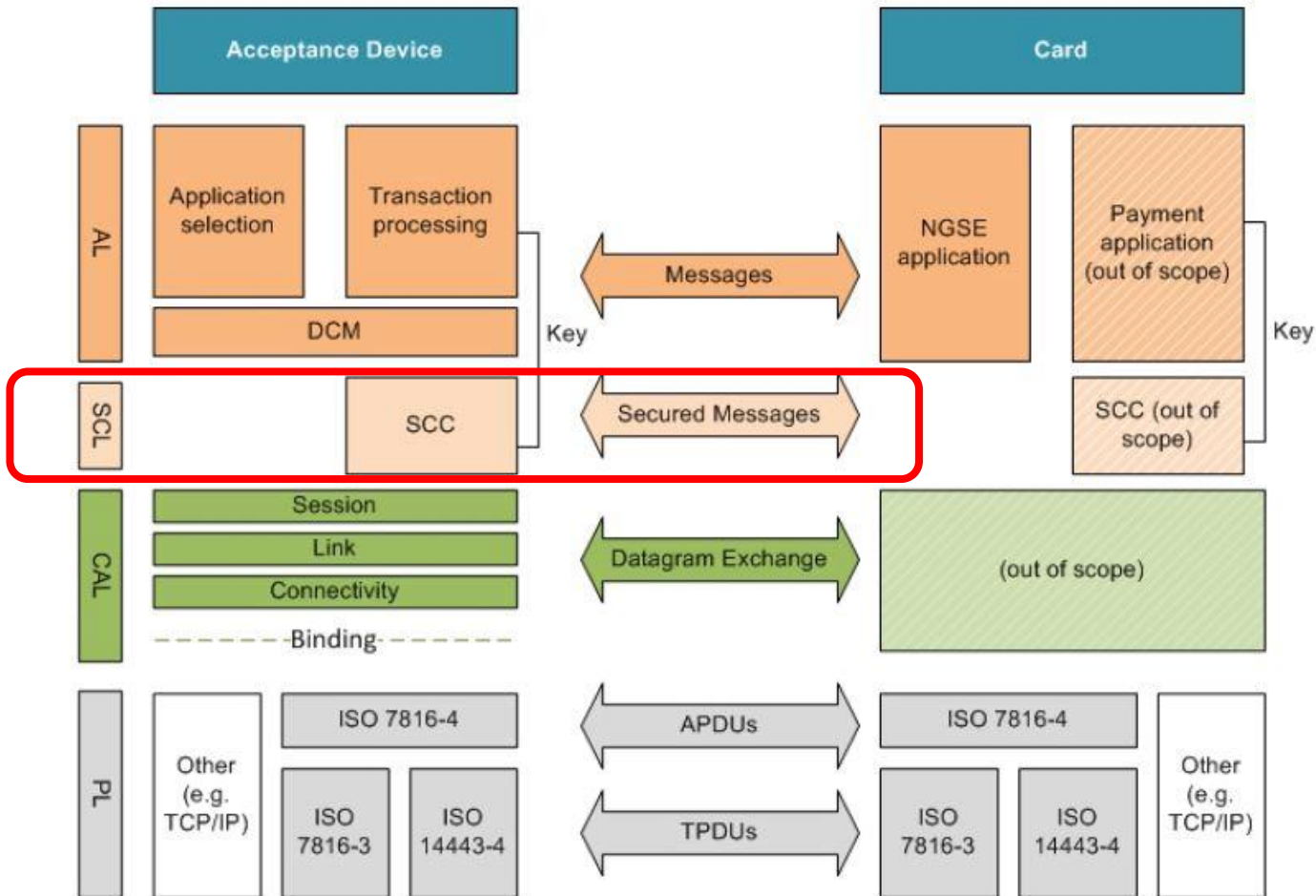


Figure 5-1: Next Gen Kernel Communication Layering





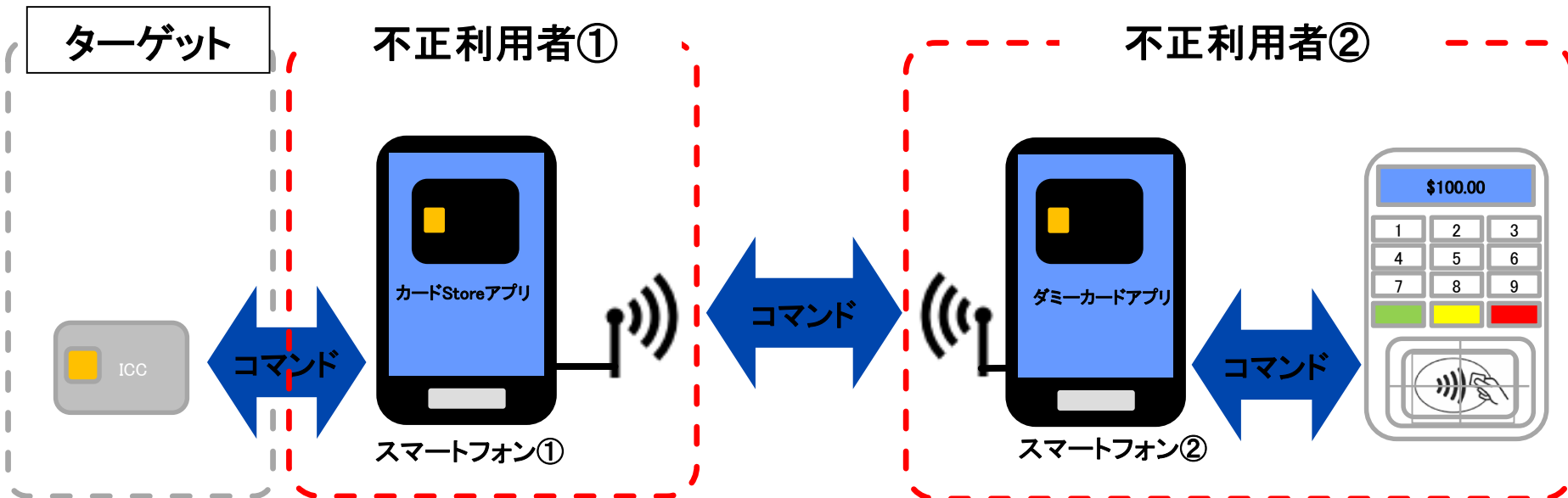
セキュアチャネルが有効な例として

- データの盗聴に対する防護として有効
- スキミングやシミングに対する防護として有効

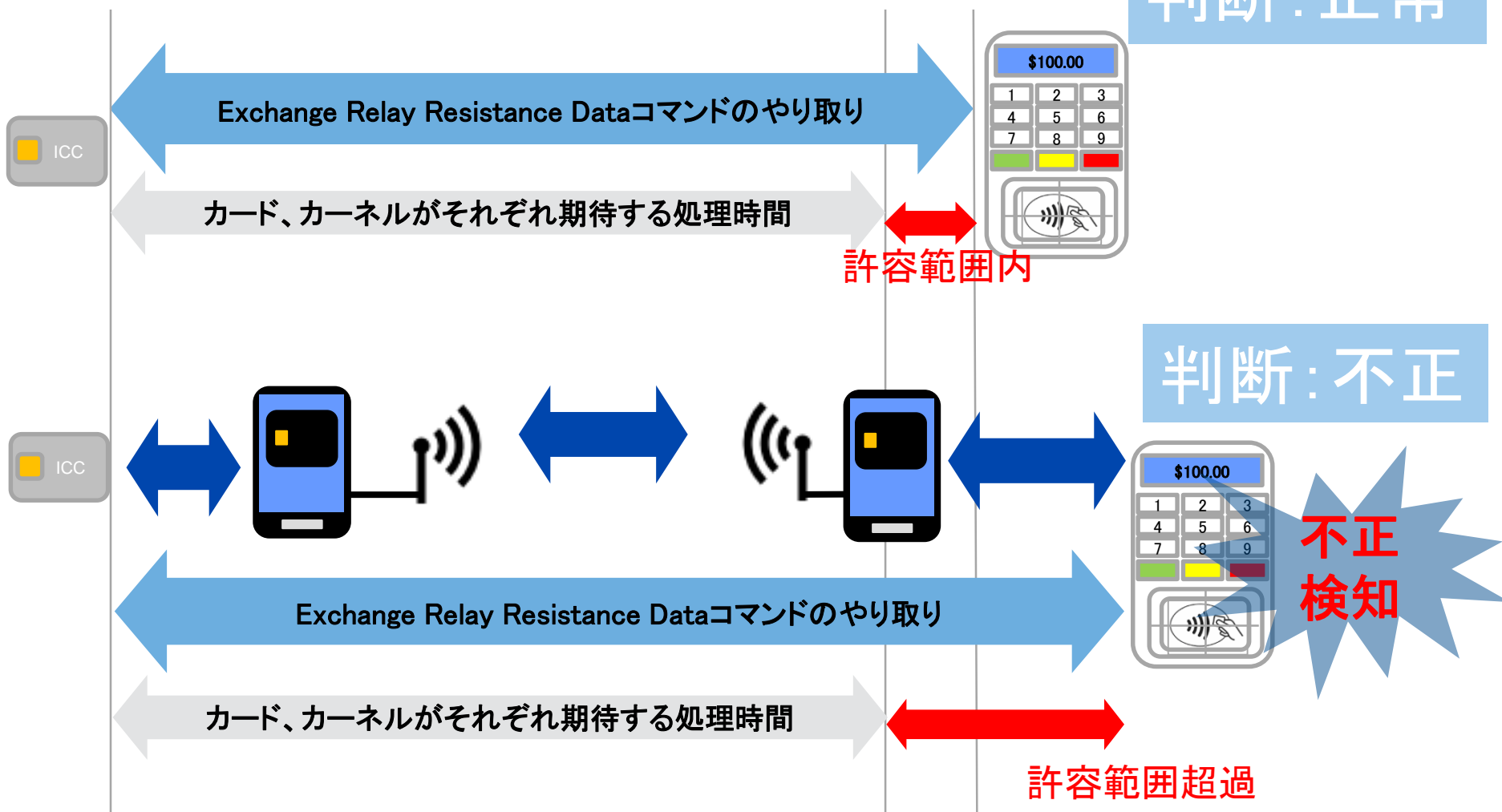
- 正常な取引



- リレーアタックによる不正取引の例



リレーアタックを防止する仕組み



EMV 非接触 無料セミナーを開催

2018年9月12日(水)
弊社新宿本社セミナールーム
近日ご案内配信予定



EMV・PCI各種オンデマンドセミナー
お問い合わせ先:

ペイメントサービス部 Tel:03-6858-9104

有路(アリジ) Takeshi.Ariji@tuv-sud.jp

森 Masashi.Mori@tuv-sud.jp

Web:<https://www.tuv-sud.jp/jp-jp>

Thank you



Thank you