資料４－１

eSIMのセキュリティについて

2021年1月27日

大日本印刷株式会社
情報イノベーション事業部
ICTセンター
セキュア・エレメンツ・デザイン本部　第3部

DNP

DNPについて

DNP独自の「P&I」（印刷と情報）の強みを掛け合わせ、
多くのパートナーとの連携を深めて、
社会課題を解決するとともに、人々の期待に応える
「**新しい価値**」の創出に取り組んでいます。

常に変革に挑戦し続け、各種情報サービスや
包装・建材、写真プリントやエネルギー関連、エレクトロニクス
や医療・ヘルスケアなどに事業領域を広げています。

スマートフォンにおけるeSIMについて

MNO様が提供する一部のスマートフォンでは、SIMスロットが存在しない製品があります。

NTTドコモ様 SH-03M

楽天モバイル様 Rakuten Mini

スマートフォンや携帯電話は販売される地域や価格帯などに違いはありますが、
SIMスロットが存在せずeSIMのみの製品も増えていく可能性があります。

MNO様、MVNO様の継続的なビジネスのため、
eSIMにセキュリティ上の懸念がある場合には対策が必要ではないでしょうか。

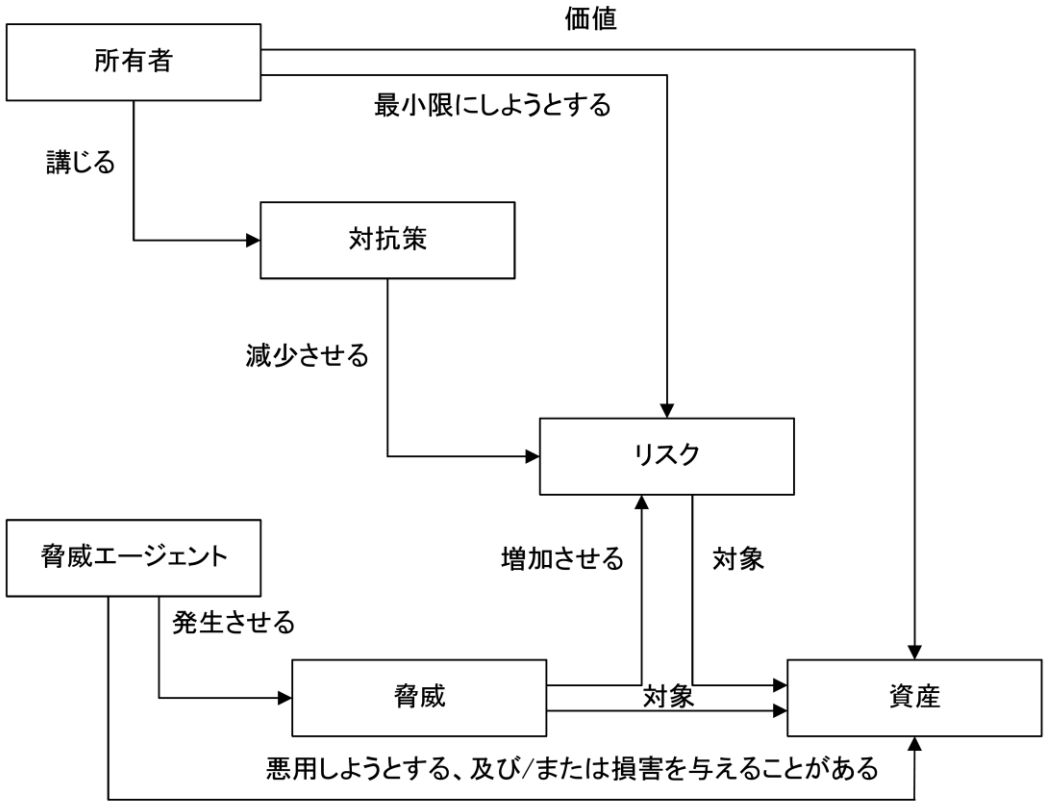
情報セキュリティの目的について

ISO/IEC 15408(Common Criteria)では、資産を脅威から守る対抗策の評価が求められます。

eSIMのセキュリティを検討するにあたっては、

・**資産**　（例えば、通信用認証鍵）
・**脅威**　（例えば、クローンSIMが作られること）

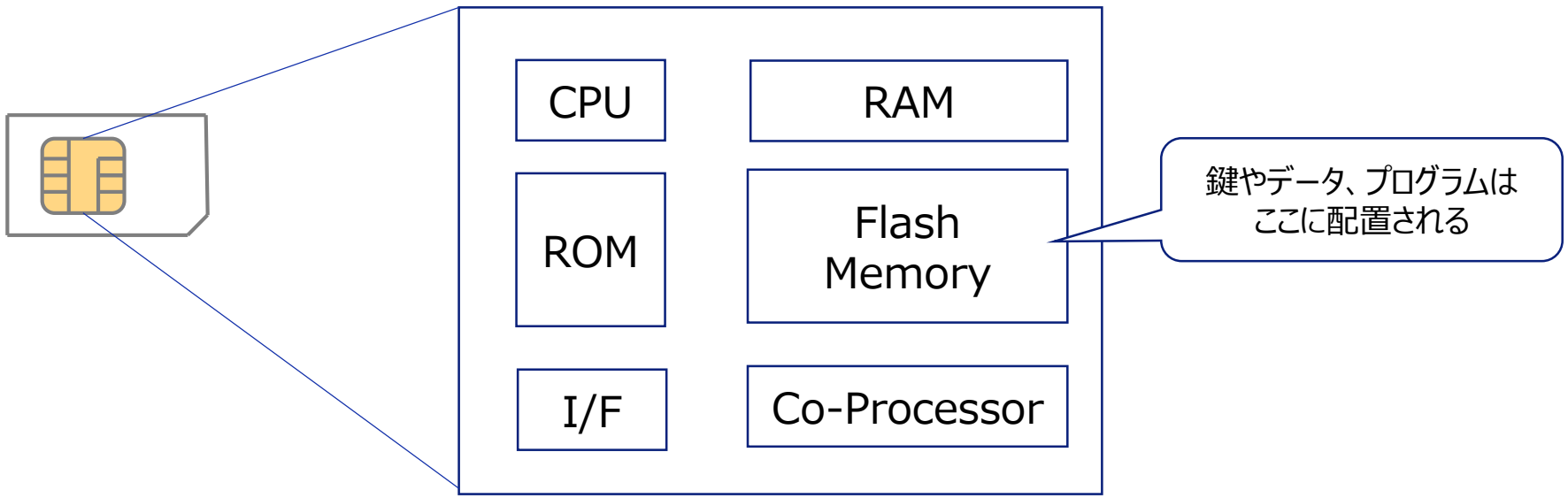
を明確化することで、必要かつ十分なセキュリティがどのようなものであるか、認識を共通化出来ると弊社では考えています。



(Common Criteria 3.1 Part1(日本語翻訳版) “図2セキュリティの概念と関係”より)

ICカードの内部構成について

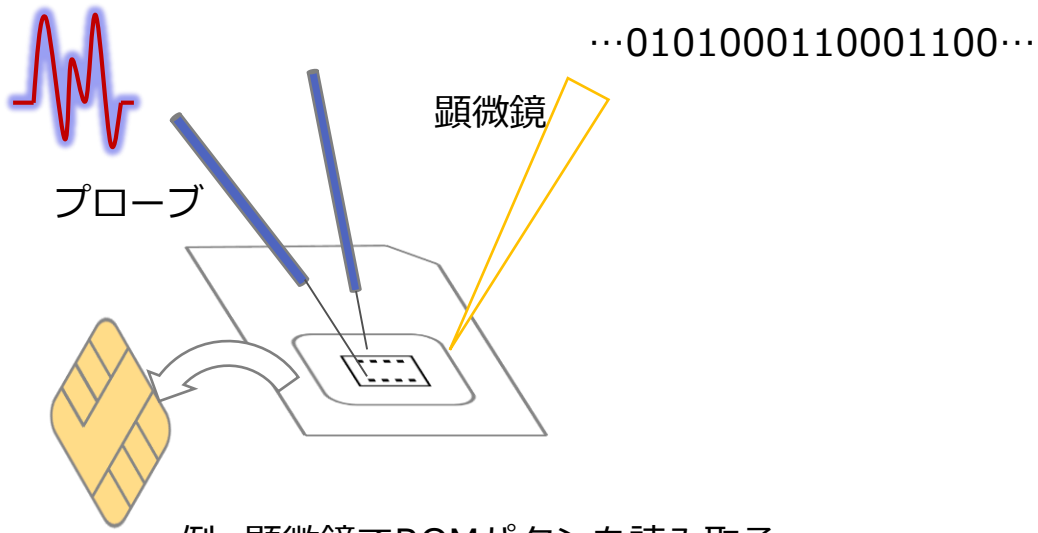
SIMを含むICカードは1chipのマイクロコンピュータで構成されており、暗号用のコプロセッサやセキュリティ異常検出回路など、一部の機能を除き、プログラムで動作を定義しています。



メモリサイズなどの違いはありますが、SIMもeSIMもハードウェアの構成は大きな違いはありません。

ICカード製品のセキュリティについて

ICカード技術を利用した製品について、様々な攻撃方法が知られています。



例: 顕微鏡でROMパタンを読み取る

これらの製品においては**ハードウェアだけではなく、ソフトウェアのセキュリティ対策も重要**となります。

次ページ以降に具体例を示します。

PIN照合における分岐処理

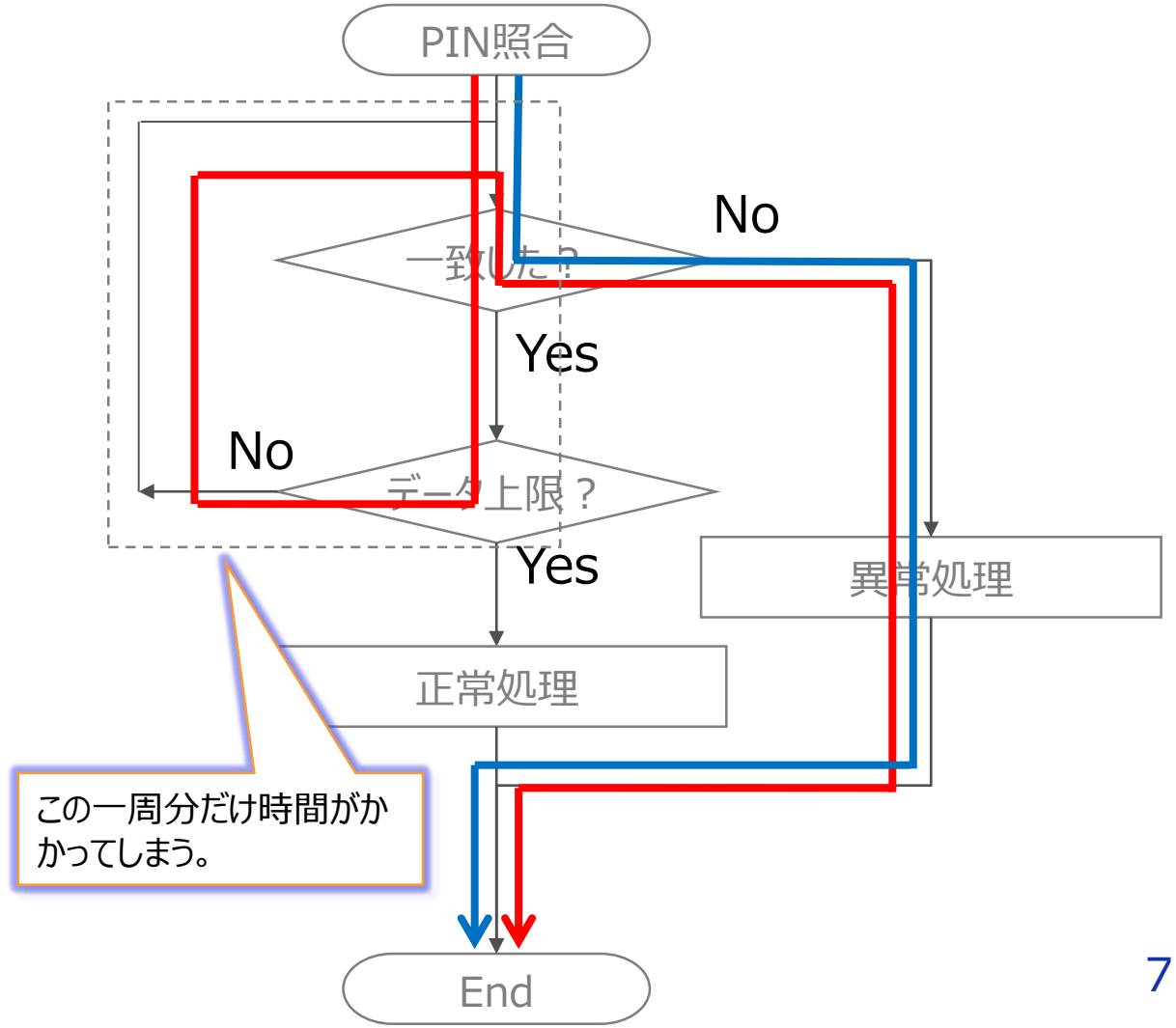
①PIN照合処理の実装次第では入力によって処理の流れが変わります。

正しいPIN=1234

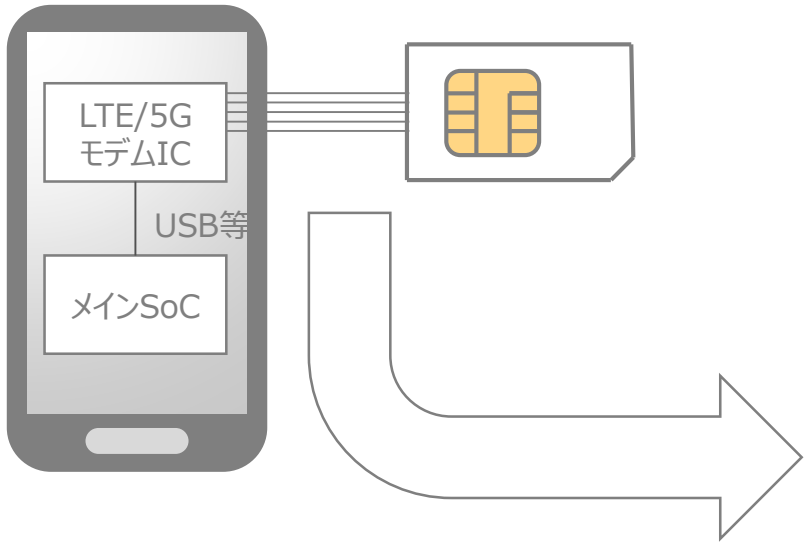
青矢印：9999
赤矢印：1999（先頭バイトは正しい）

②オシロスコープでI/Oを測定すると

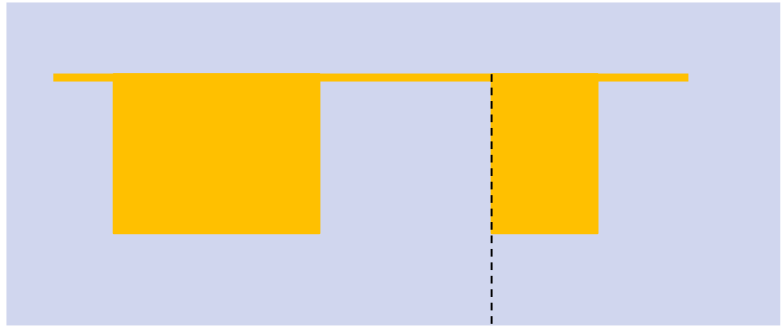
→次ページへ



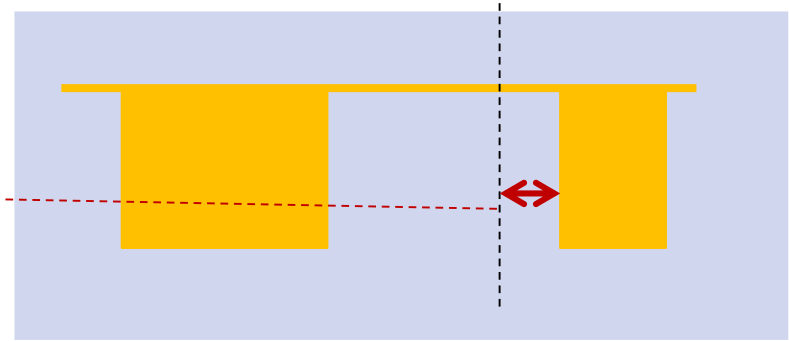
PIN照合のオシロスコープによる計測結果



通信波形A: 全データ不一致



通信波形B: 先頭バイトが一致



③ループ1回分だけレスポンスが遅れるため、波形の違いから、PINの先頭バイトの正否がわかってしまいます

これはTiming Analysisと呼ばれるサイドチャネル解析の1つであり、ソフトウェアを含めた対策をしない限り、**脅威**から**資産**を守ることが出来ません。

eSIMのセキュリティ課題と対応について

従来のSIMとeSIMとのセキュリティ上の違いとして以下が考えられます。

SIM: MNO様がセキュリティ要件を考慮し、どの製品を使うか選択が可能
eSIM: ユーザーがスマートフォン等を選択するため、どのeSIM製品を使うかMNO様は選択不可能

このためeSIMでは**第三者によるセキュリティレベルの保証が重要**となります。

ハードウェア及びソフトウェアのセキュリティ対策が十分かどうかを確認する方法としては、
Common Criteriaのような評価会社による評価とその結果に基づくセキュリティ認定や、
クレジットカードで用いられるブランド認定などがあります。

eSIMのセキュリティ要件

標準仕様上、eSIM製品化においてはCC認定の取得が必須となります。
但し、2019年9月までは、eSIM製造時に必要となる**eSIM工場証明書**取得の条件とはなっておらず、
実際に**CC認定を取得していない製品**が市場に出回っています。

eSIM工場証明書の取得条件は以下の通りです。

期間	工場監査	eSIMデバイス評価
2019年9月まで	必須	特になし
2019年9月～2020年6月	必須	HWとしてはCC取得 SWとしては次のいずれか ①CC認定、②暫定方式
2020年6月～2022年1月	必須	HWとしてはCC取得 SWとしては次のいずれか ①CC認定、②GSMAによる認定、③暫定方式
2022年1月以降	必須	HWとしてはCC取得 SWとしては次のいずれか ①CC認定、②GSMAによる認定

SGP24 v2.3におけるeSIMデバイス要件　詳細

DNP

eSIM製造時に必要となる工場証明書の取得について、eSIMのソフトウェア評価における認定取得の条件は以下の通りです。

種別	認定条件
CC認定	プロテクションプロファイル”BSI-CC-PP-0100-2018”を満たすこと
GSMA認定	“SGP.06”および“SGP.07”を満たすこと
暫定方式	**なし** (セキュリティ評価のみ)

暫定方式を採用した製品も、一旦市場に出たものについてeSIMとしての有効性を失うことはありません。

eSIMの情報について

DNP

eSIMの管理番号である**EID** (下表)を読み出すことで、**ベンダーやバージョンを識別**できます。

オフセット	値	意味、備考
1	8	Major Industry Identifier digit
2	9	Additional digit of 9 specifying telecommunications
3～5	**Country code**	Country codeが3桁未満の場合、後ろに0を連結
6～8	**Issuer identifier**	Issuer identifierが3桁未満の場合、後ろに0を連結
9～13	Version information	OSおよびプラットフォームのバージョン情報
14～18	Additional issuer information	OSおよびプラットフォームの追加情報
19～30	Individual identification number	個別番号
31～32	Check digit	チェックコード

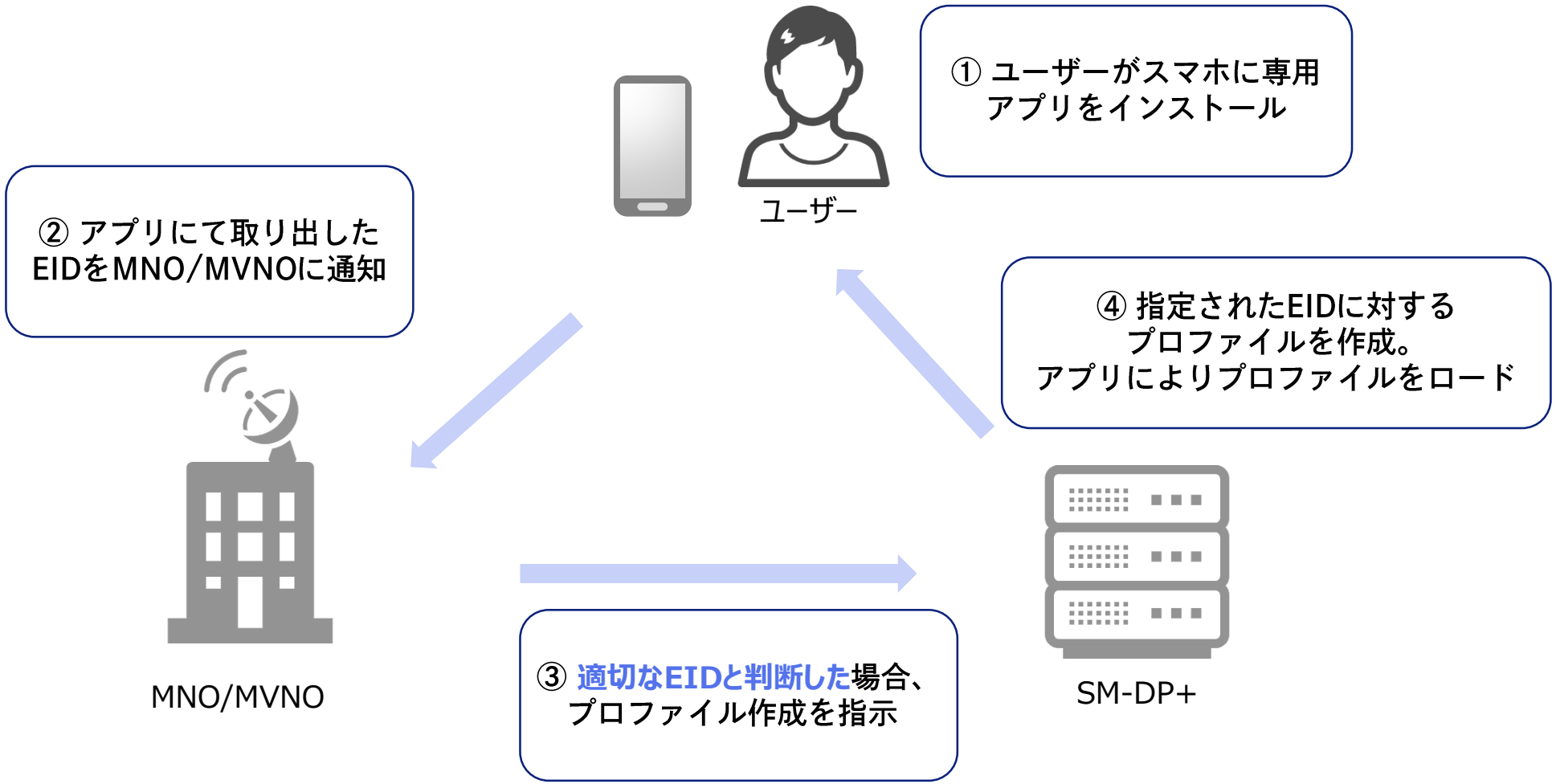
この値からベンダーを識別できます。(ITU-T T-SP-E.118)

(GSMA SGP.02 “2.2.2 Identification of eUICC: EID”より)

AndroidではEuiccManagerクラス　getEid()メソッドによりEIDを取得可能であり、Remote SIM Provisioningに用いる管理サーバー(SM-DP+)でもEIDを確認することが可能です。

もしeSIMを利用する場合には、必要となる費用、脅威、スマートフォン市場やユーザーの利便性などを考慮し、EIDによる利用可否の機能追加をご検討されてはいかがでしょうか。

EID確認　実施例


① ユーザーがスマホに専用
アプリをインストール
ユーザー
② アプリにて取り出した
EIDをMNO/MVNOに通知
④ 指定されたEIDに対する
プロファイルを作成。
アプリによりプロファイルをロード
MNO/MVNO
③ 適切なEIDと判断した場合、
プロファイル作成を指示
SM-DP+

ご清聴ありがとうございました