株式会社研美社　御中

FeliCaスタンダードカード セキュリティの指摘について

- Maxell Confidential -

maxell
Within, the Future

2025/09/18

マクセル株式会社
光学・システム事業本部
ID&セキュリティ事業推進部

1．概要

はじめに

この資料は、この資料の内容に関する対応の目的にのみご使用いただき、その他の目的での使用や第三者への開示はお控えいただきますようお願い申し上げます。

報道内容について

「2017年以前に出荷された一部のFeliCa ICチップの脆弱性に関する指摘について」（ソニー株式会社）
https://www.sony.co.jp/Products/felica/business/information/2025001.html
「お知らせ」（フェリカネットワークス株式会社）
https://www.felicanetworks.co.jp/news/assets/9b1b34b8e71c9b1edc4bade8c0530ba93866bd8d.pdf

概要

・7/末、IPA(独立行政法人情報処理推進機構) 経由 JPCERT/CCから、ソニー(株)へFeliCaの脆弱性関連情報としてレポートが共有されました。
・FeliCa ICチップのうち、2017年以前に出荷された一部のICチップについて、IPAの「情報セキュリティ早期警戒パートナーシップガイドライン」に基づき外部(発見者)から指摘を受けました。
・報告された操作により、当該チップにおいてデータの読み取りや改ざんが実行される可能性があることが確認されました。

対応状況

・ソニー(株)にて、2017年以前に出荷された一部のFeliCa ICチップについて、報告された操作により、当該チップにおいてデータの読み取りや改ざんが実行される可能性があることを確認しました。
・本情報は機密性が高い情報として上記パートナーシップの枠組みの中のみで取り扱いがされ、一部のサービス事業者や公的機関と連携し、影響範囲・対応方針を協議中です。

2．対象製品と影響について

対象製品

種別	世代	カード型番	ICチップ型番	脆弱性指摘対象
A	第1世代	マクセルでの製造と販売はしておりません	2017年以前出荷の RC-S914 RC-S915 RC-S950	**対象**
B	第2世代	IE-4F(SP)***シリーズ	RC-S962	**対象外**
C	第3世代	IE-6F(SP)***シリーズ	RC-SA00	**対象外**

影響について

・対象となるチップでは、IPAから報告された手順を実施することにより、カード内に格納された各種暗号鍵が特定される可能性のある脅威が存在します。

・各種暗号鍵特定の手順については、発見者・IPA・JPCERT/CC・ソニー(株)の間のみで共有されており、公開されておりません。

・現時点、市場で各種暗号鍵の特定や被害発生の情報はありません。

・暗号鍵が特定されることで、秘匿データの読み出しやデータの改ざんが可能となります。

3．お客様へのご確認のお願い

・お客様もしくはエンドユーザー様にて、脆弱性が指摘されたFeliCa製品を過去ご使用された実績があるか、ご確認をお願い致します。

・脆弱性が指摘された対象となる第1世代のFeliCa製品（A）をご使用の場合、

1）Aの製品のみ使用されている場合

→ 暗号鍵(DES鍵)の特定、秘匿データの読み出し、データの改ざんなどの脅威が発生する可能性があります。

2）Aの製品をご使用のあと、Aの製品と同じ暗号鍵(DES鍵)をご使用した対象外のFeliCa製品（B）（C）を採用されている場合

→ **Aの製品**で暗号鍵(DES鍵)の特定、秘匿データの読み出し、データの改ざんなどの脅威が発生する可能性があります。

→ **B、Cの製品**で秘匿データの読み出し、データの改ざんなどの脅威が発生する可能性があります。

・対象となる第1世代のFeliCa製品（A）をご使用されていない場合

3）書き込まれている暗号鍵が事業者様の特定のサービスのみでご使用の場合

→ **セキュリティへの影響はありません。**

4）他の事業者様と暗号鍵を共有している場合

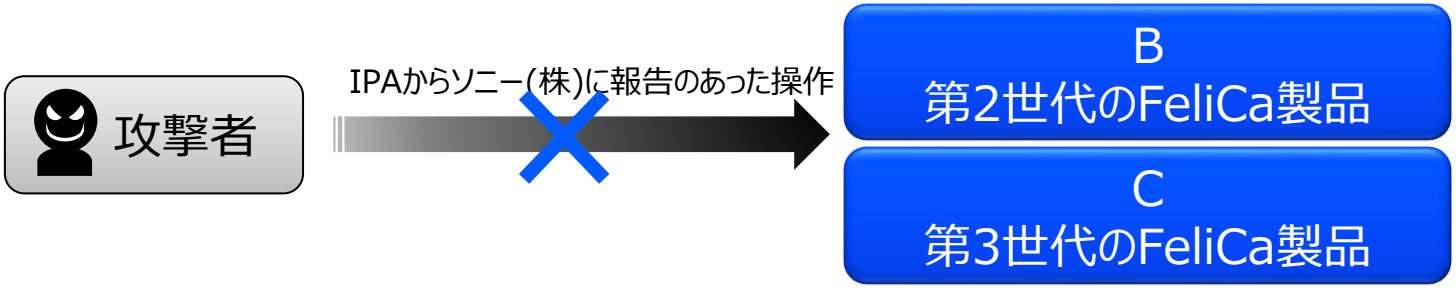
→ **B、Cの製品**で秘匿データの読み出し、データの改ざんの脅威が発生する可能性があります。

次ページに図を示します。

3．お客様へのご確認のお願い2

1)、2)、4)のケース

3)のケース



今回の事象は発生せずセキュリティへの影響はありません。

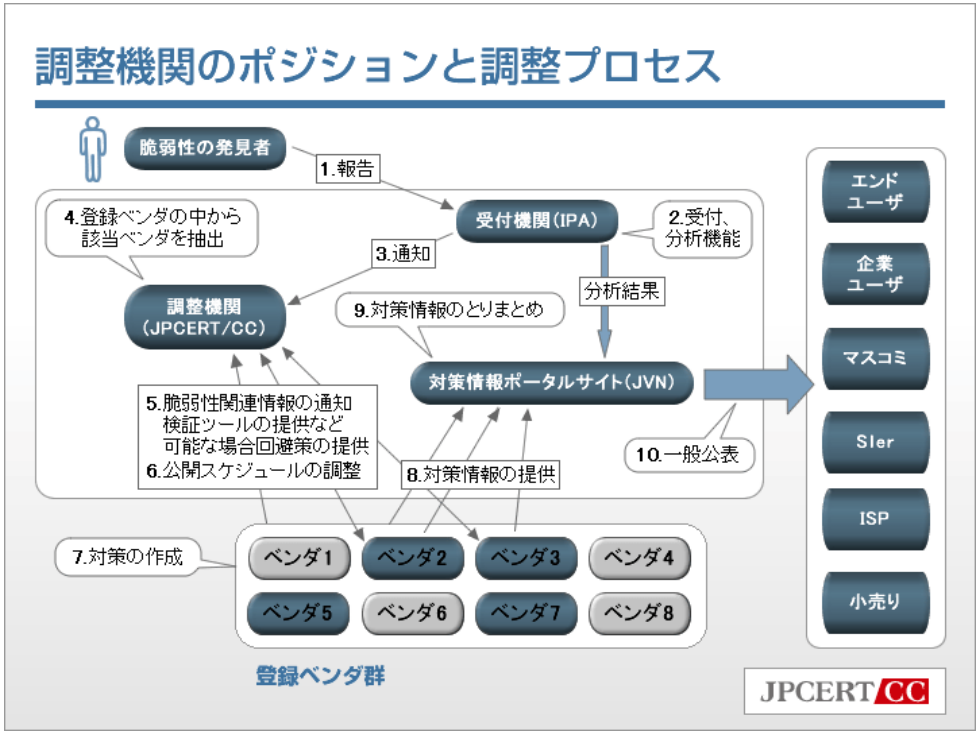
【参考１】 対策例に関して

前ページ1)、2)、4)のようなケースがあった場合を前提に、システムの構築・運用におけるセキュリティ機能の具体的な対策例は、以下となります。

- ⓪FeliCaカードやシステムの暗号方式をDESからAESへの移行
- ① サーバー側での取引ログの整合性検証
  例：各取引に一意の通番が付与され、サーバーでその整合性をチェックする仕組により、サーバー側で不正を検知できる。
- ② データを外部で暗号化してカードに格納
  例：カード内のデータが、事業者固有の暗号鍵で暗号化されているため、不正な書き換えを検知できる。
- ③ カード内データのMAC(またはデジタル署名)の付与
  例：カード内のデータの整合性を保証するために、MACや署名が付与され、R/W側で検証され、不正が検知できる。
- ④ 鍵の個別化
  例：カードごとに異なる鍵が設定されており、R/W側もその個別鍵を使って認証を行うため、他人のカードを対象とした不正行為の難易度が上がる。

【参考２】 IPAとJPCERT/CCについて

- 日本国内において、脆弱性関連情報の届け出を受け付ける機関がIPA(独立行政法人情報処理推進機構)で、開発者等との調整を行う機関がJPCERT/CCとなります。
- IPA、JPCERT/CCと開発者の間は、「情報セキュリティ早期警戒パートナーシップ」に基づき情報交換が行われています。
  また、IPAのガイドラインによれば、報告者はIPAへの報告時点で、対応をIPAに委ねる形となります。



JPCERTホームページより引用

- 報告内容について、一定期間においては、事前の連絡なく報告者から一方的に公開されることは、原則ありません。
- 本件でも報告者はIPAへの報告を行っており、同時に一部の報道機関に情報を提供している旨をIPAに伝えたとのことですが、IPAルールに従った対応がなされることが期待されます。


maxell
Within, the Future