

RC-S500

AES暗号方式およびDES暗号方式に対応したリーダー向けFeliCa™ SAMです。

本製品を使用することで、さまざまな機器・用途でFeliCaのセキュリティー機能を利用することができます。

AES対応

高セキュリティー

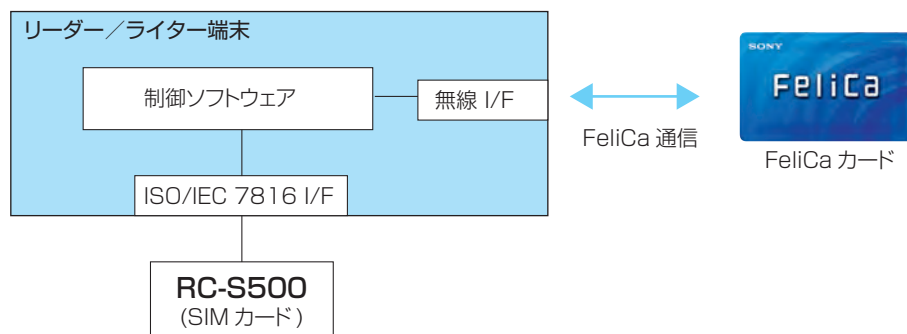
高速通信

現行製品との
互換性

概要

AES/DES両方の暗号方式に対応した、リーダー向けFeliCa SAM(Secure Application Module)です。AES暗号方式およびDES暗号方式のFeliCaカードに対して、セキュアにアクセスするために必要な機能を提供します。リーダー/ライター装置のSIMカード用スロットに装着して使用することで、FeliCaのセキュリティー機能を使用したシステムを開発できます。

RC-S500を用いたリーダー/ライターの構成例



特長

● 新世代標準暗号化方式AESに対応

本製品は、カードとリーダー/ライター端末間およびRC-S500とリーダー/ライター端末間の暗号通信において、従来のDES(Data Encryption Standard)暗号方式に対応しました。さらに、AES(Advanced Encryption Standard)暗号方式を備えることで、セキュリティーの向上を実現しました。

● 高セキュリティー

本製品に搭載しているセキュリティーICチップはコモンクライテリア (ISO/IEC 15408) EAL5+を取得予定です。セキュリティーICチップ内に暗号アルゴリズムを搭載し、また鍵を格納することができます。これらにより、高セキュリティーなシステムの構築が可能です。

● 高速通信

本製品は、リーダー/ライター端末との通信において、最大1.25Mbps*の高速通信を実現しました。高速な処理が求められるシステムでもご利用頂けます。

*入力クロック10MHz時

● 現行製品との互換性を確保

本製品は、RC-S251との互換性 (電気特性/コマンド) を有しており*、AESカード対応システムへの移行が容易です。

*初期設定など管理用のコマンドを除く

主な機能

	RC-S500
通信	・ ISO/IEC 7816-4に準拠した Command/Response APDUでのコマンド送受信
セキュリティ	・ リーダー/ライター端末とRC-S500間の暗号通信 ・ カードとRC-S500間の暗号通信
鍵管理	・ FeliCaカードのシステム、エリア、サービス鍵およびグループ鍵の管理
FeliCaカードアクセス	・ FeliCaカードとの相互認証 ・ カードコマンドパケットの暗号化 ・ カードレスポンスパケットの復号 ・ カードレスポンスのタイムアウト時間の計算 ・ パッケージ生成 ・ グループ鍵生成

主な仕様

	RC-S500	
外部インターフェース/通信方式	ISO/IEC 7816準拠 (T=1プロトコル)	
入力クロック	1~10 MHz	
通信速度	最大1.25 Mbps (入力クロック10 MHz時)	
使用温度/保存温度	-25℃ ~ +85℃ (10% RH ~ 90% RH)	
カード外形寸法 (プラグイン部)	ISO/IEC 7810 ID-1/000カード (25 mm × 15 mm)	
不揮発性メモリー	書き換え耐性	10万回
	最大鍵登録数	512 (システム/エリア/サービス鍵、DES/AES合計) 32 (グループ鍵、DES/AES合計)
電源電圧/消費電力	ISO/IEC 7816 ClassA (5 V)、ClassB (3 V) に対応	

- 仕様および外観は改良のため、予告なく変更されることがありますのであらかじめご了承ください。
- FeliCaは、ソニー株式会社の登録商標です。
- その他本カタログに記載されているシステム名、製品名は一般に各開発メーカーの登録商標または商標です。なお、本文ではTM、®は明記していません。

ソニー株式会社

ソニーシティ大崎

プロフェッショナル・ソリューション事業本部
FeliCa事業部
営業部

東京都品川区大崎2-10-1 〒141-8610

URL: <http://www.sony.co.jp/Products/felica/>

カタログの記載内容：2014年5月現在
J2013J-07-00