2017 年 10 月 23 日

「KRACKs」WPA2 脆弱性に関する弊社対応について

平素は弊社製品のご愛顧を賜り、誠にありがとうございます。

「KRACKs」WPA2 脆弱性に関する弊社対応につきまして、本日までの調査結果及び今後の対応をご報告させていただきます。

1. 弊社製品が、本脆弱性（KRACKs）の対象となる利用方法

基本的に、WPA/WPA2 を利用した無線子機として利用する場合が該当します。
ただし、アクセスポイントとして利用する場合でも、以下の場合は該当します。

- WDS（複数のアクセスポイント間を通信する機能）を利用して、他のアクセスポイントに　接続して利用する場合
- IEEE 802.11R による高速ローミングを利用する場合

上記に該当しない場合は、本脆弱性の対象外です。
WDS 機能を搭載していても、利用していなければ対象外です。
同様に、IEEE 802.11R の利用設定をしなければ、対象外となります。

2. 本脆弱性に対応していない無線子機を接続する場合

弊社製品に、本脆弱性に対応していない無線子機を接続する場合、無線子機側の対策が必要となります。対策については、各ベンダにご確認ください。
Windows、Mac、iOS、Android 等は、各 OS ベンダより、対策パッチが配布されております。

3. 主な対象製品

製品名/型式	影響の有無	対策時期
SX-AP-4800AN	WDS, 802.11R 使用時に影響あり	順次対策予定
SX-AP-4800AN2	WDS 使用時に影響あり	順次対策予定
AP-500AC	WDS 使用時に影響あり	11 月中旬
SX-570	無線子機使用時に影響あり	11 月中旬
SX-580	無線子機使用時に影響あり	11 月中旬
SX-582	無線子機使用時に影響あり	順次対策予定
SX-BR-4600WAN	影響あり	順次対策予定
BR-300AN	影響あり	順次対策予定
BR-310AC	影響あり	順次対策予定

上記以外の製品に関しては、確認出来次第情報更新いたします。

お問い合わせ窓口

本件に対するお問い合わせは、下記窓口、又は弊社営業担当までお願いいたします。

サイレックス・テクノロジー カスタマサポートセンター

電話：0774-98-3981

詳細なご質問は、メール（support@silex.jp）や Web フォームからお願いいたします。

https://www.silex.jp/contact/products.html

以上