2017 年 10 月 17 日公開

2017 年 12 月 18 日更新

お客様各位

東芝メモリ株式会社

（続報）FlashAir™における「WPA2 の鍵情報の生成・管理に関する脆弱性」について

平素は、弊社製品をご愛用いただき、誠にありがとうございます。

弊社製 FlashAir™ SDHC/SDXC メモリカード（SD-UWA シリーズ＜W-04＞）、FlashAir™ SDHC メモリカード（SD-WE シリーズ＜W-03＞）、FlashAir™ SDHC メモリカード（SD-WD/WC シリーズ＜W-02＞）、FlashAir™ SDHC Class6 メモリカード（SD-WB/WL シリーズ）（以下、合わせて「対象製品」）で使用している WPA2（無線 LAN の暗号化方式）において、送受信するデータを暗号化する際の鍵情報の生成・管理に関する脆弱性が発見されました。FlashAir™と無線 LAN で接続した機器との間で送受信されているデータを盗み見られるおそれがあります。対象製品の中でソフトウェアの更新が必要な製品（以下、「ソフトウェア更新対象製品」）があります。ソフトウェア更新対象製品をお使いのお客様は、ソフトウェア更新ツールをご使用いただき、お手持ちのソフトウェア更新対象製品のソフトウェアを更新してください。

なお、ソフトウェア更新の実施／未実施に関わらず、ソフトウェア更新対象製品を含む、対象製品をお使いの場合、接続相手の機器に本脆弱性がある場合は、送受信されているデータを盗み見られるおそれがあるため、接続相手の機器に脆弱性がないことをご確認の上、接続してください。接続相手の機器の脆弱性の有無や対応状況につきましては、機器のメーカにお問い合わせください。

記

KIOXIA

ソフトウェア更新対象製品とバージョン

製品名	型番	容量表示	ソフトウェアバージョン
 FlashAir™ SDHC/SDXC メモリカード（SD-UWA シリーズ＜W-04＞）	SD-UWA064G	64GB	V4.00.01 およびそれ以前
	SD-UWA032G	32GB	
	SD-UWA016G	16GB	

ソフトウェアバージョンの確認方法

＜FlashAir™ Android / iOS アプリを使用して確認する場合＞

FlashAir™と接続した状態で、FlashAir™アプリの「FlashAir 情報」で確認することができます。

<FlashAir™ 設定ソフトウェアを使用して確認する場合>

パソコンの SDHC / SDXC 対応 SD カードスロットまたはパソコンに接続した SDHC/SDXC メモリカード・リーダ・ライターに FlashAir™を挿入し、FlashAir™ 設定ソフトウェアを起動します。FlashAir™ 設定ソフトウェアのメインメニュー画面右下にソフトウェアバージョンが表示されます。

KIOXIA

脆弱性の説明

FlashAir™で使用している WPA2（無線 LAN の暗号化方式）において、送受信されているデータを暗号化する際の鍵情報の生成・管理に関する脆弱性が発見されました。

脆弱性がもたらす脅威

FlashAir™と無線 LAN で接続した機器との間で送受信されているデータを盗み見られるおそれがあります。

対策方法

以下のソフトウェア更新ツールをご使用いただき、お手持ちのソフトウェア更新対象製品のソフトウェアを更新してください。修正版のソフトウェアのバージョンは、V4.00.02 です。

- ソフトウェア更新ツール（SD-UWA シリーズ＜W-04＞）

関連情報

本脆弱性に関連する情報は、以下の通りです。

- Wi-Fi Protected Access II（WPA2）ハンドシェイクにおいて Nonce およびセッション鍵が再利用される問題

更新履歴

- 2017/10/17

以上