2017 年 5 月 16 日

お客様各位

株式会社東芝 ストレージ＆デバイスソリューション社

FlashAir™のフォトシェア機能におけるパスワードの固定の脆弱性について

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 メモリカード（SD-WE シリーズ＜W-03＞）および FlashAir™ SDHC メモリカード（SD-WD/WC シリーズ＜W-02＞）（以下、合わせて「対象製品」といいます。）でのブラウザを利用したフォトシェア機能において、パスワード固定の脆弱性があることがわかりました。ソフトウェア更新ツールをご使用いただき、お手持ちの対象製品のソフトウェアを更新し、フォトシェア機能をご利用の都度、FlashAir™ Android™ / iOS アプリにてフォトシェアモード用の SSID / パスワードを必ず初期値以外に変更してからご利用ください。
なお、ソフトウェア更新ツールは「FlashAir™のフォトシェア機能におけるアクセス制限不備の脆弱性について」でご案内しているものと同じです。

記

KIOXIA

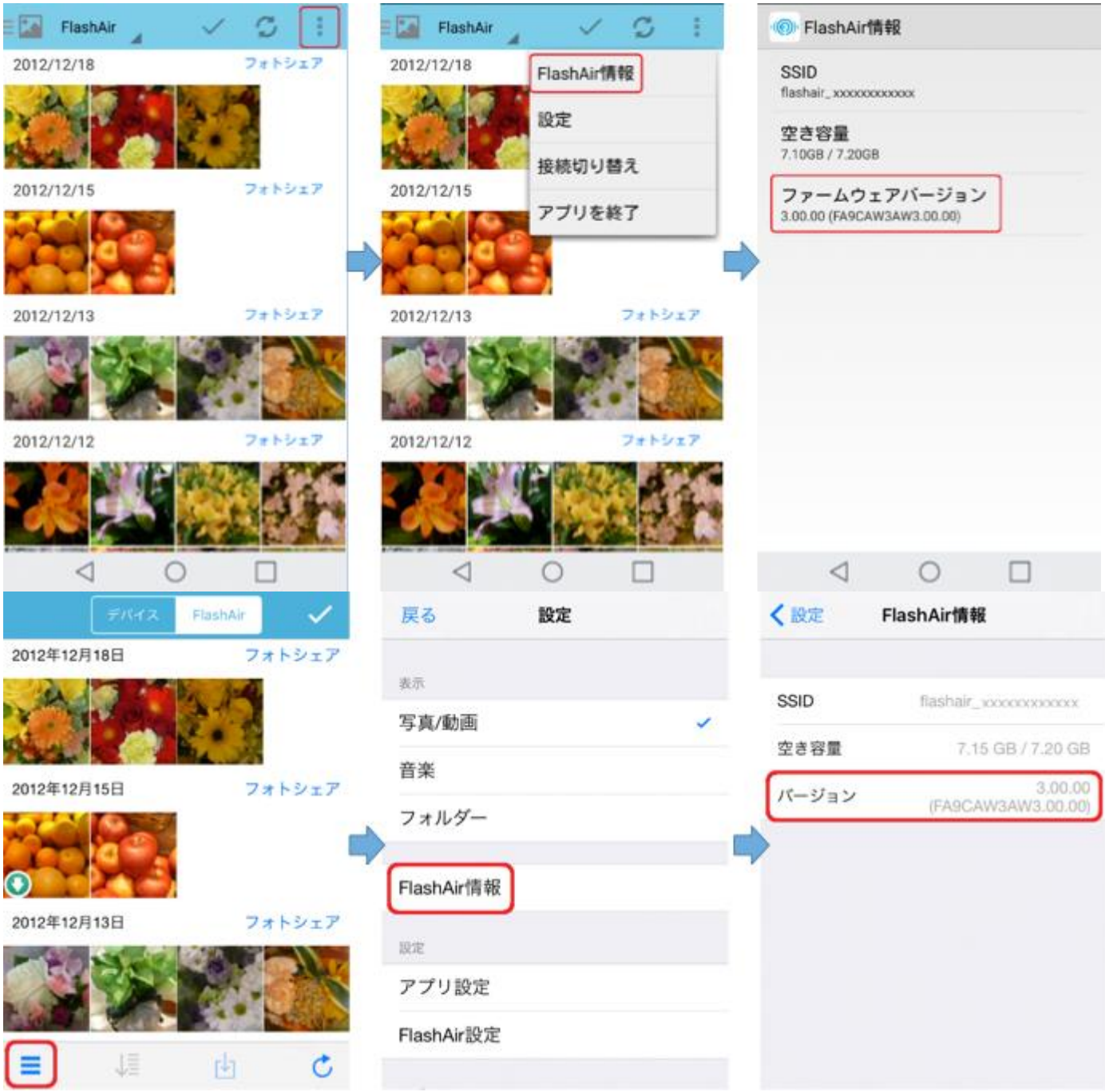
対象製品とバージョン

製品名	型番	容量表示	ソフトウェアバージョン
 FlashAir™ SDHC メモリカード （SD-WE シリーズ＜W-03＞）	SD-WE032G	32GB	V3.00.01 およびそれ以前
	SD-WE016G	16GB	
	SD-WE008G	8GB	
 FlashAir™ SDHC メモリカード （SD-WD/WC シリーズ＜W-02＞）	SD-WD032G	32GB	V2.00.03 およびそれ以前
	SD-WC016G	16GB	
	SD-WC008G	8GB	

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 対応 SD カードスロットまたはパソコンに接続した SDHC 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

脆弱性の内容

ブラウザで FlashAir™を使用する場合、設定メニューからフォトシェアを開始すると、フォトシェアモード用のパスワードが固定となります。

脆弱性のもたらす脅威

フォトシェアの実行中に、フォトシェア用の SSID / パスワードの初期値を知っていて接続を試みる第三者に接続され、写真を見られたり、保存されたりするおそれがあります。

対策方法

KIOXIA

下表のソフトウェア更新ツールをご使用いただき、お手持ちの対象製品のソフトウェアを更新し、フォトシェア機能をご利用の都度、FlashAir™ Android / iOS アプリにてフォトシェアモード用の SSID / パスワードを必ず初期値以外に変更してご利用ください。特にパスワードは、初期値やパスワードなし(空欄のまま設定)で使用しないでください。ソフトウェア更新後は、フォトシェア機能は FlashAir™ Android / iOS アプリからのみご利用いただけます。

対象製品	ソフトウェア更新ツールおよびバージョン	備考
FlashAir™ SDHC メモリカード（SD-WE シリーズ＜W-03＞）	無線 LAN 搭載 SDHC メモリカード FlashAir™ソフトウェア更新ツール（SD-WE シリーズ＜W-03＞） V3.00.02	2017 年 4 月 24 日公開
FlashAir™ SDHC メモリカード（SD-WD/WC シリーズ＜W-02＞）	無線 LAN 搭載 SDHC メモリカード FlashAir™ソフトウェア更新ツール（SD-WD/WC シリーズ＜W-02＞） V2.00.04	2017 年 5 月 15 日公開

関連情報

本脆弱性に関連する情報は、以下の通りです。

- FlashAir™のフォトシェア機能に SSID およびパスワード固定の脆弱性

謝辞

脆弱性発見者及び連絡をしていただいた JPCERT/CC の方々に感謝いたします。

脆弱性届出者：　三井物産セキュアディレクション株式会社　諫山貴由 様

以上