

インテル・プロセッサの脆弱性に対応するアップデート (2016/06/13 購入の FMV LIFEBOOK AH53/X の例)

2018(H30).1.7

1. ハードウェアの脆弱性は Windows Update では対応が困難

2018/01/05 あたりから、マスコミで騒がれているインテル製 CPU の脆弱性^(※1)は、これまでのソフトウェア(OS、アプリ)の脆弱性とは異なり、ハードウェアの脆弱性(通称Meltdown^(※2)とSpecter^(※3)の2件)です。正確にはCPUの脆弱性ではなく

- (※1) ソフトウェアやハードウェアに脆弱性(安全上の欠陥)があると、その欠陥を外部からの不正アクセスや不正スソフトで攻撃されコンピュータやユーザが被害を受ける。
- (※2) Meltdown は、悪意のあるプログラムが許されている以上の権限レベルの情報を読み出せる脆弱性に付けられた名前
- (※3) Specter は、実行されているアプリから他のアプリデータ等を盗み出せる脆弱性に付けられた名前

ご存知の通りソフトウェアの脆弱性はソフトウェア更新(Windows Update やメーカーソフトの更新)を着実に実行することで被害を防ぐことができます。しかし今回のようなハードウェアの脆弱性はハードウェアメーカーが提供するファームウェアやドライバー等を更新して被害を防がなければなりません。

したがって今回のCPUの脆弱性は、自PCの製造メーカーが提供する「ユーザーサポート」を利用する必要があります。機種により異なる可能性があります。

【重要】今回の脆弱性は、^{インテル}INTEL互換の^{エーエムディー}AMDや^{アーム}ARMのプロセッサにもある

- AMD(米アドバンストマイクロデバイス社)プロセッサはINTELのセカンドソースであったが、現在は互換プロセッサとなっている
- ARM(英アーム社)プロセッサは低消費電力が特徴を持ち、モバイル機器で多く使われている

(参考)PC、タブレットの例ではプロセッサ(コアプロセッサ、Pentiumプロセッサ、Celeronプロセッサ、Atomプロセッサ等々)の高速化機能に脆弱性があ

る。このためファームウェアであるIntel ME(マネージメント・エンジン)のアップデートが必要である。

このアップデートはPC等の機種(型番)で異なるので各メーカーの対応も必要?

(注意) 今回の脆弱性はプロセッサの高速化策のために分岐命令の先行実施が要因であり、ファームウェアのアップデートで処理能力が若干低下する。

2. プロセッサの脆弱性に対するアップデートの確認

ここでは筆者のメインPC(富士通の2016春モデル)を例にして説明しますが、サブPC(NECの2010年秋モデル)は既にサポート終了でした。

(参考) 今回のCPUの脆弱性は、富士通は2012年春モデル以降、NECは2015年秋モデル以降、VAIOは第6世代CPU以降14機種限定、東芝は第3世代CPU以降だが提供時期未定

【アップデートの要否の確認手順】

- ① MS Edge を起動し「インテル ファームウェア 脆弱性」と入力して検索する
- ② 「インテル® マネジメント・エンジンの重要なファームウェア・アップデ…」をクリックして [インテル® マネジメント・エンジンの重要なファームウェア・アップデート (intel-sa-00086)] ページに移動する

サポートホーム > ソフトウェア



インテル® マネジメント・エンジンの重要なファームウェア・アップデート (intel-sa-00086)

最後のレビュー: 26-Dec-2017
 記事 ID: 000025619

インテル® マネジメント・エンジン (インテル® ME.x/8.x/10.x/x/9 11.X6.x/7)、インテル® トラステッド・エグゼキューション・エンジン (インテル® TXE3.0)、およびインテル® サーバー・プラットフォームサービス (インテル® SPS4.0) 脆弱性 (intel-sa-00086)

外部の研究者によって特定された問題に対応して、インテルは、包括的なセキュリティを実行の確認ファームウェア障害許容力の強化の目的で、次の:

- インテル® マネジメント・エンジン
- インテル® トラステッド・エグゼキューション・エンジン
- インテル® サーバー・プラットフォームサービス (SP)

インテルは特定の PC、サーバー、IoT プラットフォームへの影響の可能性があるセキュリティ上の脆弱性を特定します。

インテル® ME ファームウェアのバージョン 6.x を使用したシステム -11x、SPS ファームウェアのバージョン 4.0 を使用してサーバー、TXE を使用したシステムのバージョン 3.0 が影響されます。特定のプロセッサから、これらのファームウェアのバージョンを確認することができます。

- 第 1、第 2、第 3、第 4、第 5、第 6、第 7、第 8 世代インテル® コア™ プロセッサ・ファミリー
- インテル® ジーオン™ プロセッサ E3-1200V5 および V6 製品ファミリー
- 拡張性の高いインテル® ジーオン™ プロセッサ・ファミリー
- W インテル® ジーオン™ プロセッサ・ファミリー
- インテル® Atom™ C3000 プロセッサ・ファミリー
- Apollo Group がどのように 22Lake インテル® Atom™ プロセッサ E3900 シリーズ
- Apollo Group がどのように 22Lake インテル® Pentium™ プロセッサ
- インテル® Pentium™ プロセッサ G シリーズ
- インテル® Celeron™ プロセッサ G、N、J シリーズ

お使いのシステムは、特定された脆弱性の影響かどうかを確認するには、次のリンクを使用して intel-sa-00086 検出ツールをダウンロードして実行します。

[よくある質問 \(FAQ\) J](#)

利用可能なリソース

- [インテルの公式セキュリティアドバイザリ: 脆弱性の技術的な詳細情報](#)

Microsoft と Linux® ユーザー向けのリソース

- [intel-sa-00086 検出ツール](#)

注: INTEL-sa-00086 検出ツールのバージョンよりも以前の 1.0.0.146 CVE-2017-5711、CVE-2017-5712 を確認していませんでした。これらの cves インテル® アクティブ・マネジメント・テクノロジー (インテル® AMT)-10 バージョン 8.X.X を搭載したシステムのみを対象とします。インテルアクティブ・マネジメント・テクノロジーを搭載したシステムのユーザーは -10.X8.x | 1.0.0.146、またはそれ以降のバージョンをインストールすることをお勧めします。INTEL-sa-00086 セキュリティアドバイザリに関しては、システムのステータスを確認するには、このバージョンをインストールします。INTEL-sa-00086 検出ツールのバージョンを確認ことができ、ツールを実行していると、出力ウィンドウにバージョン情報を表示しています。

リソースからシステム / マザーボードの製造元によっては

注: 利用可能になった場合は、他のシステム / マザーボードの製造元のリンクが提供される予定です。ご利用の [メーカー](#) が表示されていない場合は、アップデートに必要なソフトウェアの対応状況についてはお問い合わせください。

- Acer: [サポート情報](#)
- ASRock: [サポート情報](#)
- ASUS: [サポート情報](#)
- compulab: [サポート情報](#)
- Dell クライアント: [サポート情報](#)
- Dell サーバー: [サポート情報](#)
- 富士通: [サポート情報](#)
- getac: [サポート情報](#)
- GIGABYTE: [サポート情報](#)
- HP Inc.: [サポート情報](#)
- Hpe サーバー: [サポート情報](#)
- インテル® ネット・ユニット・オブ・コンピューティングは、インテル® Compute Stick、インテル® コンピュータ・カード: [サポート情報](#)
- Intel® サーバー: [サポート情報](#)
- Lenovo: [サポート情報](#)
- Microsoft の表面: [サポート情報](#)
- MSI: [サポート情報](#)
- NEC: [サポート情報](#)
- Oracle: [サポート情報](#)
- Panasonic 製: [サポート情報](#)
- Quanta/qct: [サポート情報](#)
- Supermicro: [サポート情報](#)
- 東芝: [サポート情報](#)
- VAIO: [サポート情報](#)



- ③ この Web ページの中段にある [リソースからシステム/マザーボードの開発元によっては] 欄の下に列挙されている PC メーカーから自 PC のメーカーサポート情報 (例: 富士通サポート) を探し出しクリックしてメーカーのサポートページを開く

URL : <https://www.intel.co.jp/content/www/jp/ja/support/articles/000025619/software.html>

FUJITSU グローバル | 変更

サービス | 製品 | ソリューション | サポート | 富士通について

ホーム > サポート > 製品 > ソフトウェア > セキュリティ > 富士通パッチ & TA 情報 > このページは、セキュリティ情報を提供します。

セキュリティ

> 富士通パッチ & TA 情報

> Oracle Solaris パッチ & TA 情報

インテル第3四半期 17年私 TXE、SPS 4.0 11.x 3.0 セキュリティレビューの累積的な更新

インテル コーポレーションは、チップセットのいくつかのセキュリティの脆弱性を発表しました。

詳細についてはインテルの web サイトを参照してください:
<https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00086&languageid=en-fr>

この脆弱性の影響を受ける製品は以下を確認してください。

- PC
 - 日本 (富士通)
<http://www.fmworld.net/biz/common/intel/20171122/> (日本語)
 - ヨーロッパ/中東/インド/アフリカ (富士通テクノロジー・ソリューションズ)
http://support.ts.fujitsu.com/content/intel_firmware_SA86.asp
 - アジア太平洋地域 (富士通 PC アジア パシフィック (株) 建設中)
 - 米国/カナダ (富士通アメリカ株式会社) 建設中
 - オーストラリア/ニュージーランド (富士通オーストラリア) 工事
- x86 サーバー
 - 日本 (富士通)
<http://jp.fujitsu.com/platform/server/primergy/note/page31.html> (日本語)
 - 富士通技術 Solutions(English)
http://support.ts.fujitsu.com/content/intel_firmware_SA86.asp

改訂履歴

- 2017年12月5日: 第3回リリース
 - 追加日: x86 サーバー日本 (富士通) 情報
- 2017年11月22日: 第2弾発売
 - 日本の PC (富士通) 情報を追加しました。
- 2017年11月20日: 最初のリリース

- ④ [・日本 (富士通)] 下の URL をクリックして富士通の [インテル社のファームウェアに関する脆弱性 (INTEL_SA_00086) のお知らせ] ページに進む


Japan [国・地域を変更](#)

富士通サイト内検索

デジタルトレンド
サービス
業種/業務
製品
サポート
企業情報

[ホーム](#) > [コンピュータプラットフォーム](#) > [法人向けPC・タブレット・スマートフォン](#) > [サポート\(法人向けパソコン\)](#) > [ウイルス・セキュリティ関連情報](#) > [インテル社のファームウェアに関する脆弱性\(INTEL-SA-00086\)のお知らせ](#)

法人向けパソコン(PC)・
タブレット・スマートフォン

▼ サポート(法人向けパソコン)

サポート・サービス

- > サポート・サービスのご案内
- > 保証内容と修理について

サポート情報

- > セキュリティ関連情報
- > ドライブダウンロード
- > マニュアル
- > お使いになる上での注意事項
- > OS関連情報
- > よくあるQA一覧
- > 今までに発表した製品
- > お問い合わせ

[▶ 個人のお客様はこちら](#) **FMWORLD [法人]**

ツイート いいね! BI

富士通株式会社
2017年11月22日 掲載
2018年1月15日 更新

インテル社のファームウェアに関する脆弱性 (INTEL-SA-00086) のお知らせ

平素は、富士通製品をご愛顧いただきまして、誠にありがとうございます。

米国インテルコーポレーション(以下、インテル社)より、「Intel® マネジメントエンジンファームウェア」に脆弱性がある旨の報告がされております。以下の対処方法をご覧いただき、ご対応くださいますようお願いいたします。

» [個人のお客様はこちらをご覧ください。](#)

脆弱性の概要

インテル社が外部の研究者の報告を受けて調査を行った結果、Intel® マネジメントエンジンファームウェアに脆弱性があり、攻撃を受けるリスクがあることが確認されました。

対象機種

2012年以降に発売した以下のパソコンが対象になります。

>> [対象機種一覧\(ノートブック、タブレット\)](#)

⑥

>> [対象機種一覧\(デスクトップ\)](#)

対処方法

BIOS、またはファームウェアのアップデート、およびドライバソフトウェアのアップデートが必要です。

BIOS、またはファームウェアの提供時期については[対象機種一覧](#)を

BIOS、またはファームウェアのアップデート

⑤-1

1. ドライブダウンロードページで、機種を選択するか、型名を入力し、検索結果を表示します
>> [ドライブダウンロード](#)
2. 該当するBIOS書換データ、またはファームウェアをダウンロードします。
3. ダウンロードしたデータを解凍し、Readme.txtをよく読みアップデートします。

ドライバソフトウェアのアップデート

⑤-2

機種により以下のいずれかのドライバソフトウェアが搭載されていますので、該当するドライバソフトウェアをアップデートする必要があります。

- ・ Intel® マネジメント エンジン インターフェースドライバ
- ・ Intel® アクティブ マネジメント テクノロジードライバ

1. ドライブダウンロードページで、機種を選択するか、型名を入力し、検索結果を表示します。
>> [ドライブダウンロード](#)
2. 検索結果に表示されたいずれかのドライバソフトウェアをダウンロードします。
3. ダウンロードしたデータを解凍し、Readme.txtをよく読みアップデートします。

法人向けパソコン(PC)・
タブレット・スマートフォン

- ・ タブレット ARROWS
- ・ ノートPC LIFEBOOK
- ・ デスクトップPC ESPRIMO
- ・ PCワークステーション CELSIUS
- ・ Android™ タブレット
- ・ シンククライアント FUTRO
- ・ ESPRIMO ロングライフシリーズ
- ・ 周辺機器
- ・ スマートフォン・携帯電話
- ・ WEB MART限定PC ダイレクトシリーズ

・ サポート(個人向けパソコン)

・ 導入事例

- ⑤ アップデート候補のファームウェアは「**BIOS** またはファームウェア」と「**ドライバーソフトウェア**」である

(補足) 「BIOS またはファームウェア」は GPT の 64 ビット Windows の場合は拡張 BIOS の UEFI (ファームウェア) であり。

「ドライバーソフトウェア」は Intel® Management Engine (通称 Intel ME)

(参考) BIOS、Intel ME のバージョンは次の手順で調べるコヨができる

BIOS : [コンパネ] → [管理ツール]

→ [システム情報] の「BIOS バージョン/日付

⇒⇒⇒ バージョン : **1.28**、日付 : **2017/10/31**

Intel ME : [コンパネ] → [デバイス マネージャ] → [システム マネージャ]

→ [Intel(R) Management Engine Interface] を右クリック

→ [プロパティ] → [詳細]

⇒⇒⇒ 日付 : **2017/07/18**、バージョン : **11.7.0.1040**

- ⑥ [対象機種] 欄の [≫対象機種一覧 (ノートブック、タブレット)] をクリックして、対応機種一覧のページを表示する

URL : <http://www.fmworld.net/biz/common/intel/20171122/note.html>

The screenshot shows the Fujitsu website interface. At the top, there is a navigation bar with 'Japan' and a search box. Below the navigation bar, there are several tabs: 'デジタルトレンド', 'サービス', '業種/業務', '製品', 'サポート', and '企業情報'. The main content area is titled '対象機種一覧 (ノートブック、タブレット)'. It features a search bar with the text '品名検索' and a '検索' button. Below the search bar, there is a note: '※半角英数字で入力してください。'. There is also an '更新情報' section with two bullet points: 'ソフトウェア提供情報を更新しました。(2018年1月15日)' and '2012年上期から2015年上期発表モデルの対象機種を追加しました。(2017年11月30日)'. At the bottom, there is a table titled '2017年上期モデル'.

品名	型名	提供時期	適用するソフトウェア		
			カテゴリ	ソフトウェア名	バージョン
ARROWS Tab Q737/R	すべての型名が対象	提供済	BIOS	ARROWS Tab Q737/P Q737/P-PV Q737/R Q737/R-PV 用 BIOS書換データ	V1.11以上
ARROWS Tab Q737/R-PV	すべての型名が対象	提供済	BIOS	ARROWS Tab Q737/P Q737/P-PV Q737/R Q737/R-PV 用 BIOS書換データ	V1.11以上
	FARR05001 FARR05002				

- ⑦ [品名検索] に自 PC の品名 (例 : LIFBOOK AH53/X) を入力した後、[検索] をクリックしてアップデートの要否を検索する

(参考) 富士通製のノート PC の場合は本体の裏面に貼られたラベルに、

品名 (LIFEBOOK AH53/X) と型名 (例 : FMVA53XR) が印刷されている

- ⑧ 「**LIFEBOOK AH53/X は見つかりませんでした。**」メッセージが表示されたので、この PC はファームウェアのアップデーが不要である。
- ⑨ [OK] をクリックして処理を終わる

【重要】この資料の作成を始めた 2018/01/07 時点では対象であった

- この資料の作成を始めた 2016/08/01/07 時点 (2017/12/26 更新) では、「2016 年 1 月発表モデル」欄に「LIFEBOOK AH53/X」が有ることが確認でき、BIOS の更新が必要とされていたのでインストール作業を行った
- 2018/01/19 時点 (2018/01/1 更新) では、[2016 年上期モデル]には「LIFEBOOK AH53/X」が無く「BIOS」も「Intel® Management Engine」のアップデートは記載がない