インテル・プロセッサー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ー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る。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 の製造メーカが提供する「ユーザーサポート」を利用する必要があり、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、INTEL互換のＡＭＤやARMのプロセッサーにもある

- AMD（米アドバンスド マイクロ デバイス社）プロセッサーは INTEL のセカンドソースであったが、現在は互換プロセッサーとなっている
- ARM（英アーム社）プロセッサー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ー（コアプロセッサー、Pentium プロセッサー、Celeron プロセッサー、Atom プロセッサー等々）の高速化機能に脆弱性がる。
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の対応も必要？

（注意）今回の脆弱性はプロセッサー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. プロセッサー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。

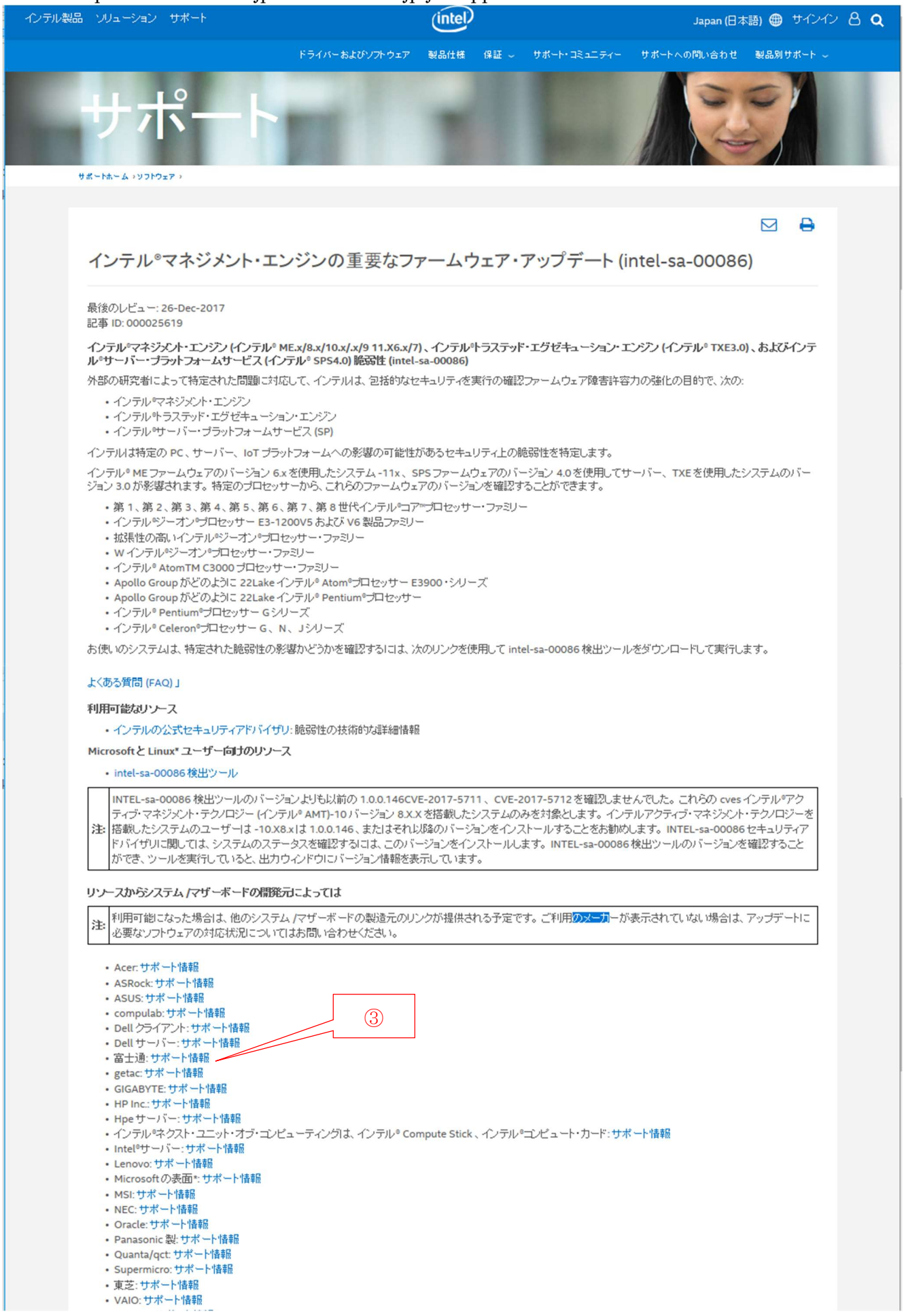
（参考）今回の CPU の脆弱性は、富士通は 2012 年春モデル以降、NEC は 2015 年秋モデル以降、VAIO は第 6 世代 CPU 以降 14 機種限定、東芝は第 3 世代 CPU 以降だが提供時期未定

【アップデートの要否の確認手順】

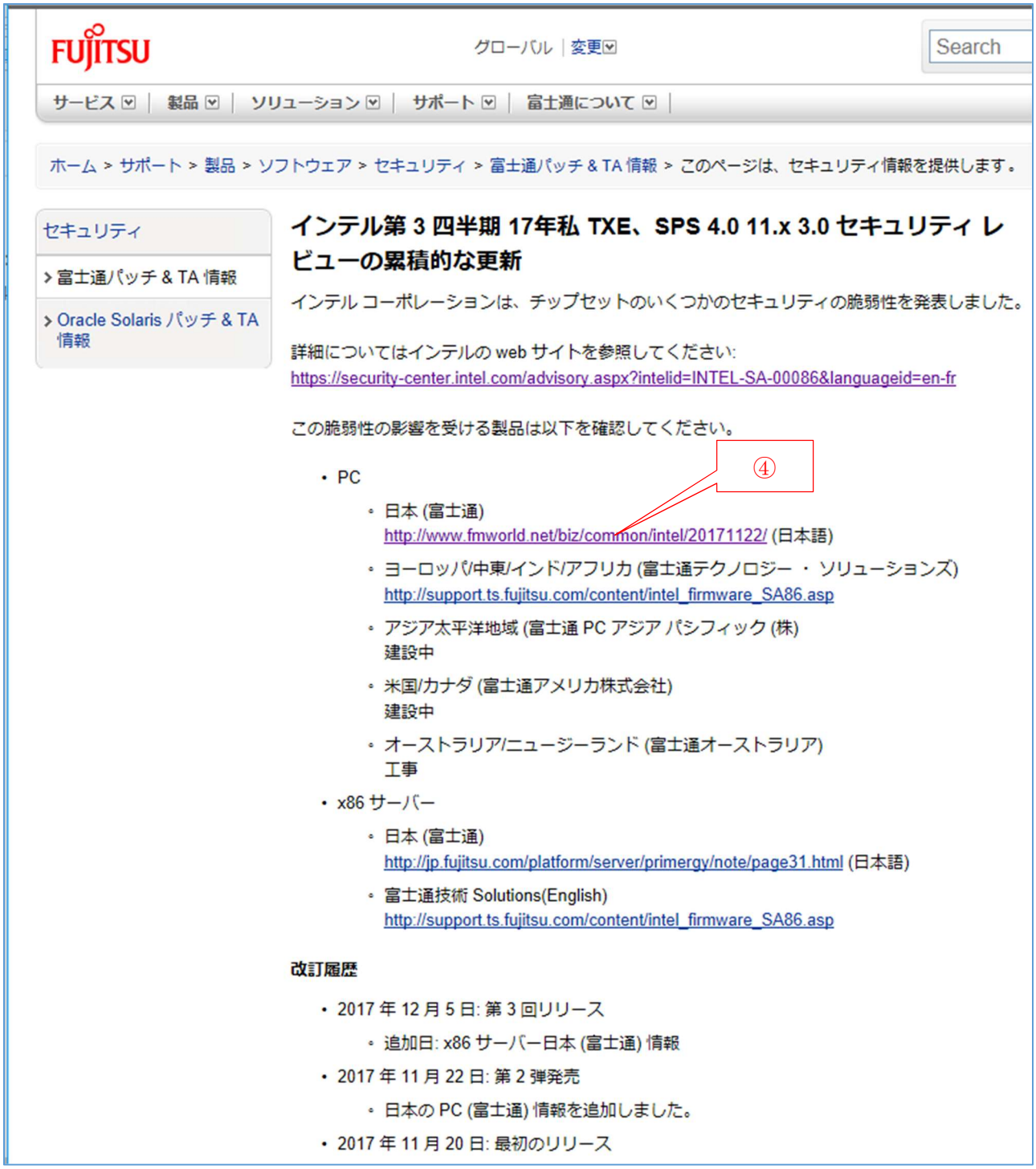
① MS Edge を起動し「インテル　ファームウェア　脆弱性」と入力して検索する

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

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



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 メーカから自 PC のメーカサポート情報（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



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

URL：http://www.fmworld.net/biz/common/intel/20171122/

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

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