2018 年 3 月 5 日

アドバンテック株式会社

産業用マザーボードAIMB-2XX/5XX シリーズ BIOS変更のお知らせ

平素は格別のご高配を賜り、厚く御礼申し上げます。
この度、産業用マザーボードAIMB-2XXシリーズ及びAIMB-5XXシリーズにおいて下記問題に対処するためにBIOS（MEファームウェアとマイクロコードを更新）の更新をここにお知らせ致します。

記

1. AIMB-2XX及びAIMB-5XXシリーズのBIOS更新によるIntelのセキュリティ脆弱性問題とハイパースレッディング問題に対応

- セキュリティ脆弱性問題

この脆弱性問題は、
① Intel® Active Management Technology (INTEL-SA-00075)
② Intel® Trusted Execution Engine (Intel® TXE 3.0) (INTEL SA-00086)
③ Intel® Server Platform Services (Intel® SPS 4.0) (INTEL SA-00086)
に関連した問題です。

- 特権を持たないネットワークハッカーが、プロビジョニング/アクティブ化されたインテルマネジャビリティSKUに対するシステム権限を取得する可能性がある問題。
- 特権を持たないローカルハッカーは、マネジャビリティの高い機能をプロビジョニングして、インテルマネジャビリティSKU上で特権のないネットワークまたはローカルシステムの特権を得る問題。

解決策：Intel MEファームウェアの更新で対応
Skylake & Kabylakeプラットフォームの更新：
① Intel® Management Engine (Intel®ME6.x/7.x/8.x/9.x/10.x/11.x) (INTEL-SA-00075)
② Intel® Trusted Execution Engine (Intel® TXE 3.0) (INTEL SA-00086)
③ Intel® Server Platform Services (Intel® SPS 4.0) (INTEL SA-00086)

*注１：インテルLAN搭載のMBのみMEファームウェアを更新する必要があり、

Realtek LANでのMBでは影響はありません。

*注2：インテルの資料によると、インテル®MEのプロビジョニングを解除または無効にすることでネットワークの脆弱性を緩和できます。 AIMB-2xxおよびAIMB-5xxのBIOSのデフォルト設定では、デフォルトのME設定はプロビジョニングを解除設定にしております。

*注3：INTEL-SA-00075及びINTEL SA-00086については下記URLを参照願います。

INTEL-SA-00075:
https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00075&languageid=en-fr
INTEL SA-00086:
https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00086&languageid=en-fr

- Skylake & Kabylakeプラットフォームにおけるハイパースレッディングの問題：

  解決策：マイクロコード更新で対応

*注：CPUがHT機能をサポートしていない場合、マイクロコードを更新する必要はありません。

BIOS変更による影響

項目	影響
機能	無
機構設計	無
ソフトウェア互換性	無
環境特性	無
ボード認証 注意 1	無
外観	無
発注型番	無
カットイン日程	新規発注より

注意 1：Advantech CE/FCC, UL/CB 認証への影響.

注意 2： 基本 BIOS 更新は標準型番へのみ対応し、お客様専用型番品やカスタム BIOS 仕様型番品には対応を致しません。 ただ、お客様から変更要望があれば案件内容に応じて検討させて頂きます。

各マザーボードシリーズ品の詳細については
別紙「AIMB-2xx_5xx BIOS Change Appendix.pdf」を参照願います。

尚、 本ご案内に関するお問合せは、以下のようにお願い致します。

- 販売代理店様から購入した場合
  販売代理店様へお問い合わせください。
- ご購入いただいた販売代理店様がわからない場合、および弊社から直接購入した場合
  以下弊社窓口へ直接お問い合わせください。
  アドバンテック株式会社 マーケティング部
  〒111-0032東京都台東区浅草6-16-3
  E-mail: ajp_callcenter@advantech.com
  TEL: 0800-500-1055 (フリーダイヤル)　FAX: :03-6802-1022

AIMB-2XX シリーズ

マザーボード フォームファクタ	製品シリーズ名	CPU SKU	ステータス	セリュリティ問題		ハイパースレッディング問題		セキュリティ問題
				INTEL-SA-0075	INTEL-SA-00086			INTEL-SA-00086
				ME更新		マイクロコード更新		ME更新
						0xBA (SKL)	0x5E (KBL)	
mini ITX	AIMB-275	KBL-S/SKL-S	V2.03	V	V	V	V	V
	AIMB-285	KBL-S/SKL-S	V2.04	No impact	V	V	V	V
	AIMB-205	KBL-S/SKL-S	V1.12	No impact	V	V	V	V
	AIMB-232 (B1)	KBL-U	V2.01	V	V2.01	V	No impact	V2.01
	AIMB-232	SKL-U	V1.11	V	No impact	V	No impact	No impact
	AIMB-242QG	SKL-H	V1.15	V	By request	V	No impact	By request
	AIMB-242WG	SKL-H		V	By request	V	No impact	By request
	AIMB-274	Haswell	V1.16	V	No impact	No impact	No impact	No impact
	AIMB-273	Ivy bridge	V1.13	V	No impact	No impact	No impact	No impact
	AIMB-272	Sandy bridge	V1.17	V	No impact	No impact	No impact	No impact
	AIMB-270	Calpella	V1.15	V	No impact	No impact	No impact	No impact

AIMB-5XX シリーズ

マザーボード フォーム ファクタ	製品シリーズ名	CPU SKU	ステータス	セキュリティ問題		ハイパースレッディング問題		Security issue
				INTEL-SA-0075	INTEL-SA-00086			INTEL-SA-00086
				ME更新		マイクロコード更新		ME update
						0xBA (SKL)	0x5E (KBL)	
micro ATX	AIMB-585QG	KBL-S/SKL-S	V2.04	V	V	V	V	V
	AIMB-585WG	KBL-S/SKL-S		V	V	V	V	V
	AIMB-585L	KBL-S/SKL-S		V	V	V	V	V
	AIMB-585WG2-SV	KBL-S/SKL-S	V1.11	V	V	V	V	V
	AIMB-505	KBL-S/SKL-S	V2.02	No impact	V	V	V	V
	AIMB-584QG	HSW-S	V2.01	V	No impact	No impact	No impact	No impact
	AIMB-584WG	Haswell		V	No impact	No impact	No impact	No impact
	AIMB-582QG	Ivy bridge	V1.12	V	No impact	No impact	No impact	No impact
	AIMB-582WG	Ivy bridge		V	No impact	No impact	No impact	No impact
	AIMB-502QG	Ivy bridge	V1.13	V	No impact	No impact	No impact	No impact
	AIMB-502WG	Ivy bridge		V	No impact	No impact	No impact	No impact
	AIMB-581QG	Sandy bridge	V1.17	V	No impact	No impact	No impact	No impact
	AIMB-581WG	Sandy bridge		V	No impact	No impact	No impact	No impact
	AIMB-580QG	Ibex Peak	V1.14	V	No impact	No impact	No impact	No impact
	AIMB-580WG	Ibex Peak	V1.11	V	No impact	No impact	No impact	No impact