INTEL-SA-00075 Detection and Mitigation Tool 使用ガイド

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)、インテル® スタンダード・マネジャビリティー (ISM)、およびインテル® スモール・ビジネス・テクノロジー (SBT)

INTEL-SA-00075 を検出して問題を緩和する方法

改訂 1.1 - 2017 年 7 月 20 日

はじめに

この文書では、INTEL-SA-00075 に記載されているセキュリティー脆弱性の問題を検出し、問題を緩和する複数のプロセスを手順ごとに説明します。詳細についてはパブリック・セキュリティー・アドバイザリー (https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00075&languageid=en-fr を参照してください。

1 台の PC のステータスを確認したいユーザーの場合：シングルまたはスタンドアロンのシステムをローカルで分析するために、インテルは INTEL-SA-00075 Detection GUI アプリケーション (Intel-SA-00075-gui.exe) を提供しています。

複数のコンピューターのステータスを確認または問題の緩和策を適用したい場合：インテルは INTEL-SA-00075 Detection and Mitigation Tool コンソール (Intel-SA-00075-console.exe) アプリケーションを提供しています。このツールは問題を検出し、その結果をローカル Windows レジストリに書き込むことができます。 また、あとで情報の収集と分析をするために (オプションで) XML ファイルに書き出すことも可能です。このコンソール ・ アプリケーションは、問題緩和にも補助的に利用できます。詳細については「*INTEL-SA-00075 Detection and Mitigation Tool の使用方法*」(2ページ) を参照してください。

インテル® セットアップ・アンド・コンフィギュレーション・ソフトウェア (インテル® SCS) を使用しているネットワーク管理者の場合：インテル® SCS スイートには別のコンソール・ツールである Intel® SCS System Discovery Utility が含まれています。インテル® SCS ツールをすでに使用している場合や、インテル® AMT の詳細データを取得したい場合には、このツールの使用を推奨します。詳細は「*Intel® SCS System Discovery Utility の使用方法*」 (11ページ) を参照してください1。

問題の緩和

本書で説明する問題の緩和手順は、この脆弱性に対処したファームウェア・アップデートが適用されていないインテルの管理機能 SKU (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)、 インテル® スタンダード・マネジャビリティー (ISM)、およびインテル® スモール・ビジネス・テクノロジー (SBT)) の不正な有効化と悪用を防止することを目的としています。

IT 専門家は、問題緩和手順の大規模な展開に使用する管理コンソール・スクリプトまたはタスクのベースとして、これらの手順説明を利用してください。緩和策の実施手順は以下の通りです。

1. インテルのマネジャビリティー SKU クライアントのアンプロビジョニングを実行し、権限を持たないネットワーク経由の攻撃者がシステム権限を取得するのを防ぎます。
2. Local Manageability Service (LMS) を無効化または削除して、権限を持たないローカルの攻撃者がシステム権限を取得するのを防ぎます。
3. 必要に応じてローカル管理機能の設定を制限します。

インテルでは、ネットワーク権限昇格の脆弱性に対処するために、どの緩和方法でも最初にインテルのマネジャビリティー SKU をアンプロビジョニングすることを推奨しています。プロビジョニング済みのシステムでは、LMS を無効化または削除する前にアンプロビジョニングを実行する必要があります。インテルのマネジャビリティー SKU の更新済みファームウェアがまだ利用可能になっていない現状では、LMS の削除または無効化によるローカルの権限昇格の問題を緩和することを推奨します。必要に応じて、LMS を不注意で再インストールまたは再度有効化してしまうことを防ぐ第 2 段階の対策として、OS を通じて実行する管理機能設定オプションの一部を OS で無効にすることができます。ただし、このようにローカル管理機能を追加で制限すると、後ほど設定を戻す際に制約が生じます。

注： AMT 6.0.*x* は Host Base Provisioning/Client Control Model に対応していないため、INTEL-SA-00075 Detection and Mitigation Tool を使用したローカル OS インターフェイスからのアンプロビジョニングは実行できません。マネジャビリティー・ファームウェア 6.0.*x*.*x* または 6.1.*x*.*x* プラットフォームを使用している場合、 Intel SCS Suite の ACUConfig /full またはシステムの MEBx を通じて完全にアンプロビジョニングする必要があります。

本書に記載されている問題の緩和手順のサポートについては、インテル ・ カスタマー ・ サポートにお問い合わせください ([テクノロジー] セクションで [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)] を選択します)。

INTEL-SA-00075 Detection and Mitigation Tool の使用方法

INTEL-SA-00075 Detection and Mitigation Tool とは？

INTEL-SA-00075 Detection and Mitigation Tool を使用すると、ローカルユーザーまたは IT 管理者は、インテル・セキュリティー・アドバイザリー INTEL-SA-00075 に記載されているエクスプロイトに対する脆弱性がシステムに存在するかどうか判断することができます。このツールのコンソール・バージョンでは、問題の緩和手順の実行にも使用できます。

Detection and Mitigation Tool は、次の 2 つのバージョンで提供されています。

- インタラクティブな GUI ツール：このバージョンを実行すると、デバイスのハードウェアとソフトウェアの詳細情報を検出し、リスク評価の結果を表示します。システムをローカルで評価する必要な場合はこちらのバージョンをお勧めします。
- コンソール実行可能ファイル：リスク評価を実行した上で、推奨される問題緩和手順を実行できます。オプションとして検出した情報を Windows* レジストリおよび/または XML ファイルに保存することが可能です。このバージョンは、複数のコンピューターで検出と緩和の一括操作を実施する IT 管理者に便利です。

INTEL-SA-00075 Detection and Mitigation Tool の入手方法

INTEL-SA-00075 Detection and Mitigation Tool のダウンロード・パッケージはこちらからダウンロードできます：
https://www.intel.com/content/www/jp/ja/support/technologies/000024133.html.

システム必要条件

- Microsoft Windows* 7、8、8.1 または 10
- ローカルのオペレーティング・システムの管理者アクセス

ツールのインストール方法

インタラクティブ・インストール

INTEL-SA-00075 Detection and Mitigation Tool.msi を実行し、画面の指示に従います。

サイレント・インストール

```
msiexec.exe /i INTEL-SA-00075 Detection and Mitigation Tool.msi /qn
```

これにより INTEL-SA-00075 Detection and Mitigation Tool をデフォルトのディレクトリーにインストールします。
`C:\Program Files (x86)\Intel\Intel-SA-00075 Detection and Mitigation Tool\`

ツールのアンインストール方法

インタラクティブ・アンインストール

INTEL-SA-00075 Detection and Mitigation Tool.msi を実行し、画面の指示に従います。

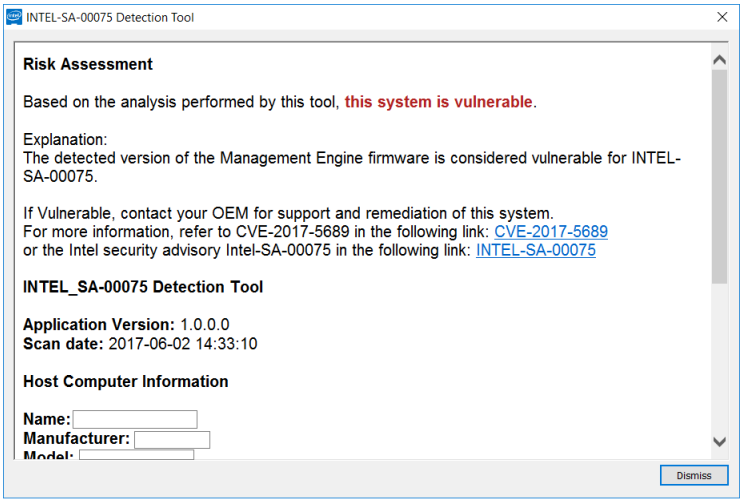
サイレント・アンインストール

```
msiexec.exe /x INTEL-SA-00075 Detection and Mitigation Tool.msi /qn
```

GUI ツールの実行方法

INTEL-SA-00075-GUI.exe は、単一システム上で実行することを目的としています。実行すると、画面に検出した情報を出力します。

図 1 : INTEL-SA-00075-GUI の画面への出力例



コンソール・ツールの実行方法

`INTEL-SA-00075-console.exe` を管理者権限を持つユーザーでコマンドプロンプトから実行します。

使用方法：

```
Intel-SA-00075-console.exe [[command] | [option...]]
```

1 度に 1 つのコマンドのみ実行できます。コマンドを指定しないと、検出コマンドが実行します。

表 1 : INTEL-SA-00075 コンソールのコマンドライン・スイッチ

コマンドラインのコマンド	機能
-Discover	コンソールに結果を出力し、データをレジストリーに書き込みます。
-Unprovision [password], -u [password]	インテル® AMT の設定をすべて削除し、インテル AMT の機能を無効にします。インテル AMT デバイス用の管理者ユーザーのパスワードを使用でき、必要とされる場合があります。 注：このコマンドをパスワードなしで呼び出すのは、INTEL-SA-00075 の影響があるファームウェアのバージョンのみで機能します (6.1.*x.x*～11.6.*x.x* でビルド番号は 3000 未満)。ファームウェアのバージョンが 6.1.*x.x*～11.6.*x.x* でビルド番号が 3000 以上の場合、アンプロビジョニングにはパスワードの入力が必須です。
-DisableClientControlMode, -DisableCCM	インテル AMT デバイスのクライアント・コントロール・モード・オプションを恒久的に無効化します。このコマンドを実行すると、デバイスをクライアント・コントロール・モードに設定できなくなります。注：この操作を取り消す CLI コマンドはありません。 警告：プラットフォームによっては、いったん無効にした CCM を再度有効化することはできません。
-DisableLMS	LMS サービスを無効にします。

コマンドライン・オプション	機能
-n, -noregistry	レジストリーへの結果書き込みを禁止します。
-c, -noconsole	コンソールへの結果表示を禁止します。
-d, -delay <seconds>	実行を開始するまでの遅延 (秒) を設定します。値を指定しない場合、ツールは遅延なく実行します。

-f, -writefile	ファイルへの結果書き込みを指定します。ファイル名の形式：<computername>.xml
-p <filepath>, -filepath <filepath>	出力ファイルを保存するパスです。パスを指定しないと、ファイルはツールと同じディレクトリーに保存されます。
-h, -help, -?	コマンドライン・スイッチと機能を表示します。

-Discover
検出コマンドは、コンソールに検出した情報を出力します。デフォルトでは、レジストリーにも検出データを書き込みます。コンソール・ツールでコマンドを指定しないと、検出コマンドが実行します。

-Unprovision
インテル® AMT の設定をすべて削除し、インテル AMT の機能を無効にします。オプションのインテル AMT デバイス用の管理者ユーザーのパスワードを使用できます。

設定すると、インテル® AMT および ISM は自動的にコンピューター・ネットワーク上の管理トラフィックをリッスンします。既知の権限昇格問題に対する脆弱性のあるシステムは、マネジャビリティー機能に対する不正アクセスを防ぐためにアンプロビジョニング・コマンドを使用してアンプロビジョニングを実行する必要があります。

このコマンドをパスワードなしで呼び出すのは、INTEL-SA-00075 の影響があるファームウェアのバージョンのみで機能します (6.1.*x.x*～11.6.*x.x* でビルド番号は 3000 未満)。ファームウェアのバージョンが 6.1.x.*x*～11.6.*x.x* でビルド番号が 3000 以上の場合、アンプロビジョニングにはパスワードの入力が必須です。

-DisableClientControlMode
-DisableClientControlMode による設定の制限は、OS の管理者権限を取得した不正な攻撃者による緩和対策の取り消しからコンピューターを保護する第 2 段階の対策としてお客様に提供されているオプションの手順です。これらのオプションを取り消すのは難しく、コンピューターの製造元が対応していない可能性があります。場合によっては、システムへの物理的アクセスが必要となります。この設定の制限を実行する場合は、LMS サービスを無効にする前に実行する必要があります。

CCM を再度有効にする方法
お使いのシステムの製造元が対応している場合は、BIOS からインテルのマネジャビリティー SKU のリセットを実行し、CCM を再度有効にすることができます。この機能の対応状況と、実行する手順については、製造元にお問い合わせください。

注：お使いのシステムの製造元では OS から BIOS を設定できるツールを提供している場合があります。このようなツールが利用可能な場合は、コンピューターに物理的にアクセスせずに、BIOS でインテルのマネジャビリティー SKU をリセットできることがあります。この機能を持つツールが利用可能かどうかは、製造元にお問い合わせください。

-DisableLMS

DisableLMS コマンドは、問題の緩和手順として LMS サービスを無効にします。

LMS とは?

Intel® Management and Security Application Local Management Service (LMS) は、インテル® AMT、インテル® SBA またはインテル® スタンダード・マネジャビリティー対応デバイス上で実行しているローカル・アプリケーションが、共通の SOAP および WS マネジメント機能を使用できるようにするサービスです。インテル® マネジャビリ ティー・エンジン (ME) ポート (16992、16993、16994、16995、623 および 664) をリッスンし、インテル® MEI ドライバーを介してファームウェアにトラフィックを送ります。

その他の注意事項

OS の管理者権限を持つユーザーなら誰でも削除された LMS を再インストールする、または無効になった LMS を再度有効にすること

ができます。したがって、システムに脆弱性が存在している際には、LMS を不注意で再インストールまたは再有効化しないように十分に注意することが大切です。例えば、あとからインテル・マネジャビリティー・ソフトウェア・インストーラーを実行すると、LMS が再インストールされる可能性があります。

図 2 : INTEL-SA-00075-Console の出力例

```
INTEL-SA-00075 Discovery Tool
アプリケーションのバージョン： <アプリのバージョン>
スキャン日： <日時>

*** ホスト・コンピューターの情報 ***
コンピューター名： <コンピューター名>
製造元： <コンピューターの製造元>
モデル： <コンピューターのモデル>
プロセッサー： <プロセッサーのモデル>
Windows のバージョン： <Windows* のバージョン>

*** ME 情報 ***
バージョン： <インテル ME ファームウェアのバージョン>
SKU： <マネジャビリティー機能、ある場合>
状態： <ME プロビジョニングの状態>
ドライバー・インストール済み： <True/False>
コントロール・モード： <なし/ACM/CCM>
CCM が無効： <True/False/不明>
EHBC 有効 <True/False>
LMS の状態： <実行中/停止/存在しない>
LMS スタートアップの種類： <起動/システム/自動/手動/無効/存在しない>
MicroLMS の状態 <実行中/停止/存在しない>
MicroLMS スタートアップの種類： <起動/システム/自動/手動/無効/存在しない>
SPS である： <True/False>


*** リスク評価 ***
このツールの分析に基づい評価結果
< このシステムには脆弱性があります /
このシステムに脆弱性はありません /
このシステムに脆弱性はありません。インテル以外の SKU です /
このシステムに脆弱性はありません。この ME FW のバージョンに影響はありません /
このシステムに脆弱性はありません。この ME SKU に影響はありません /
このシステムに脆弱性はありません。SMBIOS によるとこれはコンシューマー向け SKU です /
このシステムに脆弱性はありません。システムは SPS FW（サーバー・プラットフォーム・サービス・ファームウェア）を実行しています /
このシステムのファームウェアが更新され、システムがアンプロビジョニング済みの状態です /
このシステムのファームウェアが更新され、システムがプロビジョニング済みの状態です /
OEM にお問い合わせください /
このシステムのリスクは不明です>

脆弱性が見つかった場合、このシステムのサポートと修正方法については OEM にお問い合わせください。

*** 詳細情報 ***
CVE-2017-5689 を参照してください：
     https://nvd.nist.gov/vuln/detail/CVE-2017-5689

またはインテル・セキュリティー・アドバイザリー Intel-SA-00075 を参照してください：
```

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

リスク評価の判断に使用されるロジックについては、「表 2」で説明しています。

表 2：出力のリスク評価の意味

メッセージ	意味
脆弱性があります	検出されたバージョンのマネジメント・エンジン・ファームウェアは、INTEL-SA-00075 で脆弱性があると見なされます。
脆弱性がありません	システムは「*INTEL-SA-00075 Discovery Tool を使用して影響のあるシステムを識別する方法*」(8 ページ) で説明している「脆弱性がありません」の基準を満たしています。
このシステムのファームウェアが更新され、システムがアンプロビジョニング済みの状態です	このシステムで検出されたファームウェアは、INTEL-SA-00075 のフィックスが適用済みです。再度プロビジョニングを実行する前に、INTEL-SA-00075 ツールを使用してシステムの完全なアンプロビジョニングが実行済みであることを確認してください。許可されていない構成設定がすべて削除されます。
このシステムのファームウェアが更新され、システムがプロビジョニング済みの状態です	このシステムで検出されたファームウェアは、INTEL-SA-00075 のフィックスが適用済みです。ファームウェアの更新前にシステムがプロビジョニングされた場合、完全なアンプロビジョニングと再プロビジョニングにより許可されていない構成設定が削除されます。
OEM にお問い合わせください	OEM 提供の SMBIOS で検出された情報にマネジャビリティー SKU が表示されていますが、ツールがコンピューターの詳細データをリクエストしても応答がありませんでした。マネジメント・エンジン・インターフェイス・ドライバーの不足により生じている可能性があります。お使いのコンピューターのモデルが影響を受けているか、OEM にお問い合わせください。
不明	ツールがお使いのコンピューターのハードウェア・インベントリ・データをリクエストしても、有効な応答がありませんでした。このシステムの脆弱性を判断するには、お使いのシステムの製造元にお問い合わせください。 このメッセージは、PMX ドライバーがインストールされていないサーバー・プラットフォームで受け取る場合があります。Windows OS のバージョンによっては、このドライバーが利用できないことがあります。ドライバーが存在しない場合に推奨される回避方法は、SPS ファームウェアのリリースに含まれる spsInfo または spsManuf アプリケーションを実行することです。どちらのアプリケーションも PMX ドライバーをインストールします。

結果

注：INTEL-SA-00075 Discover コマンドが返すデータの量は、インテル・マネジャビリティー・ドライバーがシステムに読み込まれているかどうかに依存します。インテル® マネジメント・エンジン・インターフェイス (MEI) ドライバーと Intel® Management and Security Application Local Management Service (LMS) がある場合、より詳細なデータセットが利用可能です。製造元によっては一部のフィールドに対応していない場合があります。

レジストリーの場所

結果の表の値は、次のレジストリー・キーで参照できます。

- 32 ビット版オペレーティング・システムの場合：HKLM\SOFTWARE\
  `Intel\Setup and Configuration Software\INTEL-SA-00075 Discovery Tool`
- 64 ビット版オペレーティング・システムの場合：`HKLM\SOFTWARE\WOW6432Node\`

```
Intel\Setup and Configuration Software\INTEL-SA-00075 Discovery Tool
```

XML

XML ファイルに結果を書き出すことを選択した場合、そのファイルは INTEL-SA-00075-console.exe の実行場所、またはコマンドライン・オプションで指定したパスのいずれかに保存されます。ハードウェアのインベントリー、OS、LMS の有無などの情報が記録されます。AMT がある場合、見つかったデフォルトおよびカスタム証明書ハッシュのリストも含まれます。このリストは、AMT に保存されているハッシュに対して予想されるハッシュの監査に使用される場合があります。

コンソールが返すコード

表 3 : INTEL-SA-00075 コンソールの返すコード

番号	意味
0	NOTVULNERABLE (If Discover command was run) | STATUS_OK
2	MACHINE_STATE_UNCONFIGURED
30	CLIENT_CONFIG_NOT_SUPPORTED
39	DISABLE_CCM_IN_ADMIN_MODE
83	HECI_NOT_INSTALLED
111	HECI_ERROR
500	DISCOVERY__VULNERABLE
501	DISCOVERY_POTENTIALLYVULNERABLE_PROVISIONED
502	DISCOVERY_POTENTIALLYVULNERABLE_UNPROVISIONED
503	DISCOVERY_CHECKWITHOEM
504	DISCOVERY_UNKNOWN_RISK
505	DISCOVERY_UNKNOWN
506	DISCOVERY_UNKNOWN_CPU

表 4 : INTEL-SA-00075 コンソールの出力する値

値	位置	説明
Application Version (アプリケーションのバージョン)		使用したスキャンツールのバージョン
Scan Date (スキャン日)		スキャンを実行した日時
Computer Name (コンピューター名)		スキャンしたコンピューターの名前
Computer Manufacturer (コンピューターの製造元)	ハードウェアのインベントリー	コンピューターの製造元
Computer Model (コンピューターのモデル)		コンピューターのモデル
Processor (プロセッサー)		コンピューターのプロセッサー・モデル
ME Version (ME バージョン)	ME ファームウェアの情報	以下の形式の完全な ME ファームウェアのバージョン番号の文字列値 : Major.Minor.Hotfix.Build
ME SKU		ある場合、システムのマネジャビリティー機能
ME Provisioning State (ME プロビジョニングの状態)		ME 設定の状態 未検出 プロビジョニングされていません プロビジョニング中 プロビジョニング済み
ME Driver Installed (ME ドライバーのインストールの有無)		True/False 値 (MEI ドライバーがコンピューター上に存在するかどうか)
EHBC Enabled (EHBC 有効)		True/False 値 (システムで組込み機器向けホストベース構成方法が有効かどうか)
LMS state (LMS の状態)		LMS サービスが実行中、実行されていない、または存在しないかどうか

LMS startup type (LMS スタートアップの種類)		LMS スタートアップの種類が存在しない、起動、システム、自動、手動、無効かの情報
MicroLMS state (MicroLMS の状態)		MicroLMS サービスが実行中、実行されていない、または存在しないかどうか
MicroLMS startup type (MicroLMS スタートアップの種類)		MicroLMS スタートアップの種類が存在しない、起動、システム、自動、手動、無効かの情報
Control Mode (コントロール・モード)		ME 設定のモード なし、ACM、CCM
Is CCM Disabled (CCM が無効)		クライアント・コントロール・モードが無効かどうか：True/False/不明
Is SPS (SPS である)		プラットフォームが脆弱性のあるサーバー・プラットフォーム・サービス (SPS) システムかどうか
*** リスク評価 ***	リスク評価	*表 2：「出力のリスク評価の意味」を参照してください。*

INTEL-SA-00075 Discovery Tool を使用して影響のあるシステムを識別する方法

影響を受けるシステムとは、影響を受けるインテル® マネジメント・エンジン (ME) ファームウェアのバージョンを使用していて、「表 5」に定義されているマネジャビリティー機能セット 3 つのうちいずれか 1 つを含むものと定義されます。

注： サーバー・プラットフォーム・サービス (SPS) プラットフォームは、 INTEL-SA-00075 に対する脆弱性はありません。SPS プラットフォームには、サーバー・プラットフォーム上のマネジャビリティー・エンジン (ME) (PCH の一部) で実行するファームウェアがあります。このファームウェアは、PC/ワークステーション・プラットフォーム上のインテル・マネジャビリティー・ファームウェア (ME 上で実行) とは異なります。

表 5：INTEL-SA-00075 Discovery Tool を使用してシステムが INTEL-SA-00075 に対して脆弱かどうか判断する基準

値の名前	脆弱性があります	脆弱性がありません
ME SKU	インテル® フル AMT マネジャビリティー インテル® スタンダード・マネジャビリティー インテル® スモール・ビジネス・アドバンテージ (SBA)	ME SKU の値が左側の脆弱性リストにない または 左側の ME SKU の値が脆弱性のないファームウェア・バージョンと共に記載されている
ME バージョン	ME バージョン 6.x.x.x ～ 11.7.x.x ME でビルド番号が 3000 未満 例: 9.5.22.**1760**	ME バージョン： • 6.x.x.x ～ 11.7.x.x でビルド番号が 3000 以上 ○ 例: 11.6.27.**3264** • 2.x.x.x.～ 5.x.x.x • 11.7.x.x より大きい

注：インテル® スモール・ビジネス・テクノロジー (SBT) は、インテル® スモール・ビジネス・アドバンテージ (SBA) 用のマネジャビリティー SKU です。

INTEL-SA-00075 コンソール・ツールの実行結果を含めるように Microsoft* SCCM ハードウェア・インベントリーを拡張する方法

Intel-SA-00075 コンソール・ツールの結果を Windows レジストリーに保存する場合、Microsoft* SCCM ハードウェア・インベントリー拡張機能を使用して結果をインポートすることができます。これで、目標のコンピューターの修正またはファームウェアの更新に使う、SCCM にコレクションを構築することができます。これには、次の手順を実行する必要があります。

1. SCCM configuration.mof ファイルにハードウェア・インベントリー・クラスを追加します。

2. クライアント設定でこれらの新しいハードウェア・インベントリー・クラスを有効にします。
3. 展開するソフトウェア・パッケージを作成し、INTEL-SA-00075 Console Tool (`Intel-SA-00075-console.exe`) を実行します。
4. ソフトウェア・パッケージを実行するタスク・シーケンスを作成します。

MOF ファイルの変更

注：ご利用の環境に中央管理用サーバーがある場合、MOF ファイルに変更を加えます。そのようなサーバーがない場合は、プライマリー・サーバー全てで変更を加えてください。

1. configuration.mof ファイルを参照します。通常は \Program Files\Microsoft Configuration Manager\inboxex\clifiles.src\hinv\ に存在します。
2. バックアップ・コピーを作成します。
3. Configuration.mof ファイルを編集します。ファイルの最後までスクロールして、次の行の上にカーソルを合わせます。

```
//=========================
// Added extensions end
//=========================
```

4. 本書の 13〜14 ページの MOF ファイルの変更点のコンテンツを、手順 3 の行の上に貼り付けます。
5. ファイルを保存して閉じます。
6. configuration.mof のあるディレクトリーで、管理者権限を持つユーザーとしてコマンドプロンプトを実行します。
7. 変更した configuration.mof ファイルをターゲットにして、スイッチを使用しないで mofcomp を実行します。

ハードウェア・インベントリーの変更

注：これらの変更を加えてから、新しい項目がハードウェア・インベントリーに表示されるまでに、クライアントに配布する必要があります。変更が反映されるまでの時間は、お使いの環境の設定方法に依存します。

1. INTEL-SA-00075.mof という新しいファイルを作成します。
2. 「INTEL-SA-00075 ハードウェア・インベントリーのインポート」(165 ページ) のコンテンツを新しく作成したファイルに貼り付けて保存します。
3. Configuration Manager Console を起動します。
4. Administration > Client Settings > Default Client Settings の順に選択します。
5. Default Client Settings を右クリックして、Properties を選択します。
6. Hardware Inventory > Set Classes の順に選択します。
7. [インポート] をクリックします。
8. INTEL-SA-00075.mof ファイルに移動して開きます。
9. 「Import both hardware inventory classes and hardware inventory class settings」(ハードウェア・インベントリー・クラスとハードウェア・インベントリー・クラス設定の両方をインポートする) オプションが選択されていることを確認します。
10. [インポート] をクリックします。
11. OK > OK の順に選択します。
12. SCCM は変更内容を dataldr.log ファイルのハードウェア・インベントリーに記録します。

SCCM パッケージの作成

1. 15 ページのバッチファイルを作成し、INTEL-SA-00075 コンソール・ツールのファイルと共に特定のフォルダーに保存します。
2. Configuration Manager Console を起動します。
3. Software Library > Packages の順に選択します。
4. Packages を右クリックして、Create Package を選択します。
5. 名前：Intel-SA-00075.
6. 「This package contains source files」(このパッケージにはソースファイルが含まれます) にチェックマークを入れます。
7. 手順 1 のパッケージ・フォルダーを参照します。
8. Next を選択します。
9. Do not create a program (プログラムを作成しない) を選択します。
10. Next > Next > Close の順に選択します。
11. パッケージを適切な配布ポイントに配布します。

SCCM タスク・シーケンスの作成

1. Configuration Manager Console を起動します。
2. Software Library > Operating Systems の順に選択します。
3. Task Sequences を右クリックして Create Task Sequence を選択します。
4. Create a new custom task sequence (新しいカスタム・タスク・シーケンスを作成する) を選択します。
5. Next を選択します。
6. Intel-SA-00075 の名前を入力します。
7. Next > Next > Close の順に選択します。
8. Intel-SA-00075 タスク・シーケンスを右クリックし、Edit をクリックします。
9. Add > General > Run Command Line の順に選択します。
10. Command Line フィールドに Intel-SA-00075.bat を入力します。
11. Package ボックスにチェックマークを入れて Browse を選択します。
12. 作成済みの Intel-SA-00075 パッケージを選択して OK をクリックします。
13. [OK] をクリックします。

Intel® SCS System Discovery Utility の使用方法

Intel® SCS System Discovery Utility とは？

Intel® SCS System Discovery Utility とはインテル® セットアップ・アンド・コンフィグレーション・ソフトウェア (インテル® SCS) スイートのコンポーネントで、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)、インテル® スタンダード・マネジャビリティー (ISM) またはインテル® スモール・ビジネス・テクノロジー (インテル® SBT) をサポートするシステム上で、ハードウェアとソフトウェアの詳細情報を提供します。実行すると、Microsoft Windows レジストリーおよび/または XML ファイルに結果を保存することができます。この情報は、ファームウェアの更新のターゲットにするシステムを見つけ、問題の緩和を実行するために使用することができます。

Intel® SCS System Discovery Utility の入手方法

Intel® SCS System Discovery Utility のダウンロード・パッケージは以下から入手できます。
https://downloadcenter.intel.com/download/26691/Intel-SCS-System-Discovery-Utility.

Intel® SCS System Discovery Utility を使用してマネジャビリティー・ファームウェアのバージョンを確認する方法

Intel® SCS System Discovery Utility の出力を使用して、システムのファームウェアのバージョンを確認し、システムにマネジャビリティー SKU が存在しているか確認することができます。この情報は、出力の `ManageabilityInfo` セクションに記載されています。このツールの実行方法については、12 ページの「*Intel® SCS System Discovery Utility の実行方法*」セクションを参照してください。

`FWVersion` 値には、デバイスの現在のファームウェアのバージョンが含まれます。`AMTSSKU` 値は、ある場合サポートされているマネジャビリティー SKU を示します。「表 6」で説明しているように、`FWVersion` と `AMTSKU` の値をチェックしてシステムの脆弱性を判断してください。

表 6：IIntel® SCS System Discovery Utility を使用してシステムが INTEL-SA-00075 に対して脆弱かどうか判断する基準

値の名前	脆弱性があります	脆弱性がありません
`AMTSKU`	インテル(R) Full AMT Manageability インテル(R) スタンダード・マネジャビリティー インテル(R) スモール・ビジネス・アドバンテージ (SBA) 出力の例： <ManageabilityInfo> <AMTSKU>**Intel(R) Full AMT Manageability**</AMTSKU> <AMTversion>**11.0.0**</AMTversion> <FWVersion>**11.0.0.1202**</FWVersion>	AMTSKU 値が出力にない または 左側の AMTSKU の値が脆弱性のないファームウェア・バージョンと共に記載されている 出力の例： <ManageabilityInfo> <FWVersion>**9.0.13.1402**</FWVersion>
`FWVersion`	インテル® マネジャビリティー SKU ファームウェアのバージョン 6.x.x.x ～ 11.7.x.x ME でビルド番号が 3000 未満 例: 9.5.22.**1760**	インテル® マネジャビリティー SKU ファームウェアのバージョン： • 6.x.x.x ～ 11.7.x.x でビルド番号が 3000 以上 　○ 例: 11.6.27.**3264** • 2.x.x.x.～ 5.x.x.x • 11.7.x.x より大きい

注：インテル® スモール・ビジネス・テクノロジー (SBT) は、インテル® スモール・ビジネス・アドバンテージ (SBA) 用のマネジャビリティー SKU です。

Intel® SCS System Discovery Utility の実行方法

レジストリーのみにデータを保存

管理者権限を持つユーザーとしてコマンド・プロンプトで次のコマンドを実行してIntel® System SCS Discovery Utility を実行し、データをレジストリーに書き込みます。

```
SCSDiscovery.exe SystemDiscovery /nofile
```

XML ファイルのみにデータを保存

次のコマンドを使用して Intel® SCS System Discovery Utility を実行し、XML ファイルにデータを保存します。

```
SCSDiscovery.exe SystemDiscovery <filename and path> /noregistry
```

パスとファイル名は、システムまたはネットワーク共有上のローカルの場所にすることができます。ネットワーク共有を使用する場合は、Intel® SCS System Discovery Utility を実行するアカウントが、そのネットワーク共有上に書き込みアクセス許可を持つことを確認します。ファイル名とパスを指定しない場合、システムの FQDN が XML ファイル名に使用され、ファイルはIntel® SCS System Discovery Utility と同じディレクトリーに保存されます。

レジストリーと XML ファイルにデータを保存

次のコマンドを使用して Intel® SCS System Discovery Utility を実行し、データをレジストリーと XML ファイルに保存します。

```
SCSDiscovery.exe SystemDiscovery <ファイル名とパス>
```

前の例と同じく、ファイル名とパスを指定しない場合、システムの FQDN が XML ファイル名に使用され、ファイルはIntel® SCS System Discovery Utility と同じディレクトリーに保存されます。

Intel® SCS System Discovery Utility の結果

Intel® SCS System Discovery Utility が返すデータの量は、インテル・マネジャビリティー・ドライバーがシステムに読み込まれているかどうかに依存します。インテル® マネジメント・エンジン・インターフェイス (MEI) ドライバーと Intel® Management and Security Application Local Management Service (LMS) がある場合、より詳細なデータセットが利用可能です。以下に説明する結果は、既知の権限昇格の問題に関係のあるいくつかの主要データフィールドのみ説明しています。その他のデータフィールドの詳細については、Intel® SCS System Discovery Utility のマニュアルを参照してください。製造元によっては一部のフィールドに対応していない場合があります。

レジストリーの結果

レジストリーに保存された結果は、次の場所で参照できます。
`HKLM\Software\Intel\Setup and Configuration Software\SystemDiscovery`

キーの値 :

値の名前	レジストリーのサブキー	値の説明
FWVersion	ManageabilityInfo	インテル® マネジメント・エンジンのファームウェア・バージョン
AMTSKU	ManageabilityInfo	サポートされているマネジャビリティー機能 (ある場合)

XML ファイルの結果

インテル® マネジメント・エンジンのファームウェア・バージョンは XML の以下のパスで参照できます。

```
<SystemDiscovery>
       <ManageabilityInfo>
              <FWVersion> バージョン番号 </FWVersion>
```

システムでサポートされているマネジャビリティー機能 (ある場合) は XML の次のパスで参照できます。

```
<SystemDiscovery>
       <ManageabilityInfo>
              <AMTSKU> マネジャビリティー機能名 </AMTSKU>
```

システム検出データを SCCM ハードウェア・インベントリーにインポートする方法

システム検出データの収集プロセスは、Microsoft* System Center Configuration Manager (SCCM) 用の Intel® SCS Add-on を使用して自動化できます。このアドオンをインストールすると、システム検出データを含めるように SCCM ハードウェア・インベントリー機能の拡張と、システムのコレクションに対してシステムの検出を実行するために使用できるタスク・シーケンスの作成を自動化します。このプロセスで収集した情報は、影響のあるシステムにファームウェア更新をプッシュして問題の緩和を実行する SCCM コレクションを作成するために使用されます。

Microsoft SCCM 用 Intel® SCS Add-on ダウンロード・パッケージは、以下から入手できます。
https://downloadcenter.intel.com/download/26506/Intel-SCS-Add-on-for-Microsoft-System-Center-Configuration-Manager.

MOF ファイルの変更

```
       //======= Intel-SA-00075 Start ====

       #pragma namespace ("\\\\.\\root\\cimv2")
       #pragma deleteclass("INTEL_SA_00075_ME_Information", NOFAIL)
       [DYNPROPS]
       Class INTEL_SA_00075_ME_Information
       {
       [key] string KeyName;
       String MEVersion;
       Uint32 MEVersionMajor;
       Uint32 MEVersionMinor;
       Uint32 MEVersionBuild;
       Uint32 MEVersionRevision;
       String MEDriverInstalled;
       String MESKU;
       String MEProvisioningState;
       String LMSPresent;
       String MicroLMSPresent;
       String IsCCMDisabled;
       String ControlMode;
       String EHBCEnabled;
       };

       [DYNPROPS]
       Instance of INTEL_SA_00075_ME_Information
       {
```

```
KeyName="INTEL-SA-00075";
[PropertyContext("Local|HKEY_LOCAL_MACHINE\\SOFTWARE\\Intel\\Setup and Configuration
Software\\INTEL-SA-00075 Discovery Tool\\ME Information|ME
Version"),Dynamic,Provider("RegPropProv")] MEVersion;
[PropertyContext("Local|HKEY_LOCAL_MACHINE\\SOFTWARE\\Intel\\Setup and Configuration
Software\\INTEL-SA-00075 Discovery Tool\\ME Information|ME Version
Major"),Dynamic,Provider("RegPropProv")] MEVersionMajor;
[PropertyContext("Local|HKEY_LOCAL_MACHINE\\SOFTWARE\\Intel\\Setup and Configuration
Software\\INTEL-SA-00075 Discovery Tool\\ME Information|ME Version
Minor"),Dynamic,Provider("RegPropProv")] MEVersionMinor;
[PropertyContext("Local|HKEY_LOCAL_MACHINE\\SOFTWARE\\Intel\\Setup and Configuration
Software\\INTEL-SA-00075 Discovery Tool\\ME Information|ME Version
Build"),Dynamic,Provider("RegPropProv")] MEVersionBuild;
[PropertyContext("Local|HKEY_LOCAL_MACHINE\\SOFTWARE\\Intel\\Setup and Configuration
Software\\INTEL-SA-00075 Discovery Tool\\ME Information|ME Version
Revision"),Dynamic,Provider("RegPropProv")] MEVersionRevision;
[PropertyContext("Local|HKEY_LOCAL_MACHINE\\SOFTWARE\\Intel\\Setup and Configuration
Software\\INTEL-SA-00075 Discovery Tool\\ME Information|ME Driver
Installed"),Dynamic,Provider("RegPropProv")] MEDriverInstalled;
[PropertyContext("Local|HKEY_LOCAL_MACHINE\\SOFTWARE\\Intel\\Setup and Configuration
Software\\INTEL-SA-00075 Discovery Tool\\ME Information|ME
SKU"),Dynamic,Provider("RegPropProv")] MESKU;
[PropertyContext("Local|HKEY_LOCAL_MACHINE\\SOFTWARE\\Intel\\Setup and Configuration
Software\\INTEL-SA-00075 Discovery Tool\\ME Information|ME Provisioning
State"),Dynamic,Provider("RegPropProv")] MEProvisioningState;
[PropertyContext("Local|HKEY_LOCAL_MACHINE\\SOFTWARE\\Intel\\Setup and Configuration
Software\\INTEL-SA-00075 Discovery Tool\\ME Information|LMS
Present"),Dynamic,Provider("RegPropProv")] LMSPresent;
[PropertyContext("Local|HKEY_LOCAL_MACHINE\\SOFTWARE\\Intel\\Setup and Configuration
Software\\INTEL-SA-00075 Discovery Tool\\ME Information|Micro LMS
Present"),Dynamic,Provider("RegPropProv")] MicroLMSPresent;
[PropertyContext("Local|HKEY_LOCAL_MACHINE\\SOFTWARE\\Intel\\Setup and Configuration
Software\\INTEL-SA-00075 Discovery Tool\\ME Information|Is CCM
Disabled"),Dynamic,Provider("RegPropProv")] IsCCMDisabled;
[PropertyContext("Local|HKEY_LOCAL_MACHINE\\SOFTWARE\\Intel\\Setup and Configuration
Software\\INTEL-SA-00075 Discovery Tool\\ME Information|Control
Mode"),Dynamic,Provider("RegPropProv")] ControlMode;
[PropertyContext("Local|HKEY_LOCAL_MACHINE\\SOFTWARE\\Intel\\Setup and Configuration
Software\\INTEL-SA-00075 Discovery Tool\\ME Information|EHBC
Enabled"),Dynamic,Provider("RegPropProv")] EHBCEnabled;
};


//======= Intel-SA-00075 End ====
```

INTEL-SA-00075 ハードウェア・インベントリーのインポート

```
#pragma namespace ("\\\\.\\root\\cimv2\\SMS")
#pragma deleteclass("INTEL_SA_00075_ME_Information", NOFAIL)
[SMS_Report(TRUE),SMS_Group_Name("INTEL_SA_00075_ME_Information"),SMS_Class_ID("INTEL_SA_00075_ME_Information"),
SMS_Context_1("__ProviderArchitecture=32|uint32"),
SMS_Context_2("__RequiredArchitecture=true|boolean")]
Class INTEL_SA_00075_ME_Information: SMS_Class_Template
{
[SMS_Report(TRUE),key] string KeyName;
[SMS_Report(TRUE)] String MEVersion;
[SMS_Report(TRUE)] Uint32 MEVersionMajor;
[SMS_Report(TRUE)] Uint32 MEVersionMinor;
[SMS_Report(TRUE)] Uint32 MEVersionBuild;
[SMS_Report(TRUE)] Uint32 MEVersionRevision;
[SMS_Report(TRUE)] String MEDriverInstalled;
[SMS_Report(TRUE)] String MESKU;
[SMS_Report(TRUE)] String MEProvisioningState;
[SMS_Report(TRUE)] String LMSPresent;
[SMS_Report(TRUE)] String MicroLMSPresent;
[SMS_Report(TRUE)] String IsCCMDisabled;
[SMS_Report(TRUE)] String ControlMode;
[SMS_Report(TRUE)] String EHBCEnabled;
};
```

INTEL-SA-00075.bat バッチファイル

```
@echo off
.\Intel-SA-00075-console
SET EL=%ERRORLEVEL%
rem Schedule HW inventory
SET HWInventoryGUID="{00000000-0000-0000-0000-000000000001}"
wmic /IMPLEVEL:Impersonate /AUTHLEVEL:Pktprivacy /namespace:\\root\ccm path sms_client CALL
TriggerSchedule %HWInventoryGUID% /NOINTERACTIVE
echo Exit code: %EL%
exit %EL%
```

収集クエリーのサンプル

プロビジョニング済みのコンピューター

```
select *  from  SMS_R_System inner join SMS_G_System_INTEL_SA_00075_ME_Information on
SMS_G_System_INTEL_SA_00075_ME_Information.ResourceID = SMS_R_System.ResourceId where
SMS_G_System_INTEL_SA_00075_ME_Information.MEProvisioningState = "Provisioned"
```

LMS が実行中

著作権、その他知的財産権の非侵害性への保証を含む) に関してもいかなる責任も負いません。インテルが書面で同意した場合を除き、インテル製品はそのインテル製品の障害によって人身事故や死亡事故が引き起こされうるような用途に対して設計されておらず、そのような使用は意図されていません。

インテル® テクノロジーの機能と利点はシステム構成によって異なり、対応するハードウェアやソフトウェア、またはサービスの有効化が必要となる場合があります。実際の性能はシステム構成によって異なります。絶対的なセキュリティーを提供できるコンピューター・システムはありません。詳細については、各システムメーカーまたは販売店にお問い合わせいただくか、http://www.intel.co.jp/ を参照してください。