

**インテル® アクティブ・  
マネジメント・テクノロジー:  
概要**

**リリース 4.0.3**

**2008年6月**

本資料に掲載されている情報は、インテル製品の概要説明を目的としたものです。本資料は、明示されているか否かにかかわらず、また禁反言によらずにかかわらず、いかなる知的財産権のライセンスを許諾するためのものではありません。製品に付属の売買契約書『Intel's Terms and Conditions of Sale』に規定されている場合を除き、インテルはいかなる責任を負うものではなく、またインテル製品の販売や使用に関する明示または黙示の保証（特定目的への適合性、商品適格性、あらゆる特許権、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。インテル製品は、医療、救命、延命措置などの目的への使用を前提としたものではありません。

インテル製品は、予告なく仕様や説明が変更される場合があります。

API とソフトウェアには、エラッタと呼ばれる設計上の不具合が含まれている可能性があり、公表されている仕様とは異なる動作をする場合があります。現在確認済みのエラッタについては、インテルまでお問い合わせください。

本書およびこれに記載されているソフトウェアはライセンスに基づいて提供されるものであり、そのライセンスの許諾範囲内でのみ使用または複製できます。本書の情報は情報提供の目的でのみ提供されるもので、予告なしに変更される場合があります。本書の情報はインテルが約定として構成したものではありません。本書の内容および本書の内容に関連して掲載されているソフトウェア製品の誤りに関して、インテルは一切の責任や義務を負いません。ライセンス契約で許可されている場合を除き、インテルからの文書による承諾なく、本書のいかなる部分も複製したり、検索システムに保持したり、他の形式や媒体によって転送したりすることは禁じられています。

最新の仕様をご希望の場合や製品をご注文の場合は、お近くのインテルの営業所または販売代理店にお問い合わせください。

本書で紹介されている注文番号付きのドキュメントや、インテルのその他の資料を入手するには、1-800-548-4725（アメリカ合衆国）までご連絡いただくか、<http://www.intel.co.jp/> を参照してください。

Intel、インテル、Intel ロゴ、Intel vPro は、アメリカ合衆国およびその他の国における Intel Corporation の商標です。

Microsoft、Active Directory、Windows は、米国 Microsoft Corporation の、米国およびその他の国における登録商標または商標です。

\*その他の社名、製品名などは、一般に各社の表示、商標または登録商標です。

© 2006-2008 Intel Corporation. 無断での引用、転載を禁じます。

## 1 はじめに

インテル® マネジメント・テクノロジー（インテル® AMT）は、インテル・ベースのプラットフォームに組み込まれている機能で、企業の PC を管理する IT 部門の能力を強化します。インテル® AMT は、PC 内部のプロセッサやオペレーティング・システム（OS）から独立して動作します。プラットフォームが電源コンセントと LAN に接続されていれば、プラットフォームの電源がオフの場合でも、リモート管理アプリケーションはインテル® AMT へ安全にアクセスできます。ソフトウェア・メーカーは、アプリケーション・プログラミング・インターフェイス（API）を使用して、インテル® AMT の機能を利用するアプリケーションを構築できます。

## 2 使用例

以下に、プラットフォームの管理および保護ツールとしてのインテル® AMT 機能の使用例を示します。

### すべてのコンピューティング資産を検出

インテル® AMT は、ハードウェアおよびソフトウェアの情報を不揮発性メモリーに格納します（ハードウェア情報は自動的に格納されます。ソフトウェア資産情報の取得と格納には、ホスト・プラットフォーム上で動作するソフトウェア・エージェントが必要です）。内蔵された管理機能により、IT スタッフは PC 電源がオフになっていても、ハードウェアおよびソフトウェア資産を検出することができます。

### システムの状態に関係なくリモートで修復

インテル® AMT に内蔵された管理機能は、IT 部門が OS 障害の後にシステムをリモートで修復できるようにするアウトオブバンド管理機能を提供します。IT 部門は、アラートとイベントログを利用して問題を素早く検出し、ダウンタイムを短縮できます。システムをリモートで診断し、リブートできるため、オンサイトサポートを削減します。

### 悪意のあるソフトウェア（マルウェア）攻撃から保護

インテル® AMT は、企業全体のソフトウェアやウイルス対策に一貫性を持たせ、常に最新の状態に保つことにより、企業のネットワークを保護します。サードパーティー・ソフトウェアは、バージョン番号やポリシーデータを不揮発性メモリーに格納することで、就業時間外に読み出しや更新を行うことができます。

### マルウェアとプラットフォーム悪用の影響を制限

インテル® AMT のシステム・ディフェンス機能は、管理対象クライアント上でのマルウェア発生やソフトウェア改ざんを封じ込め、感染したネットワーク要素を残りのネットワークから隔離することにより、ウイルスへの感染リスクを軽減します。エージェント・プレゼンス・チェック機能は、重要なアプリケーションが動作しているかどうかを検出します。これらのプログラムが動作していない場合、インテル® AMT は直ちに IT コンソールにレポートを送信し、必要に応じて IT スタッフが修正するまでそのプラットフォームを隔離します。

これらの使用例は、インテル® AMT で実現可能な最先端の企業コンピューティング管理の一部を紹介したものです。

### 3 アーキテクチャー

インテル® AMT のアーキテクチャーは、ファームウェア（製品の機能およびファームウェアを実行するためのハードウェア環境を実装する）、セキュリティーおよびネットワーク環境、インテル® AMT ソフトウェア開発キット（SDK）のコンポーネントで構成されています。

#### 3.1 ハードウェア/プラットフォーム・アーキテクチャー

インテル® AMT の基本アーキテクチャーは製品リリースごとに異なり、各リリースの新機能を実装しています。

インテル® AMTリリース 2.0 は、インテル® vPro™ プロセッサー・テクノロジー搭載ワークステーション・プラットフォームのコンポーネントです。インテル® vPro™ プロセッサー・テクノロジーは、プラットフォーム・アーキテクチャーの多くのコンポーネントを使用しています。図 1は、これらのコンポーネントの関連付けを示しています。

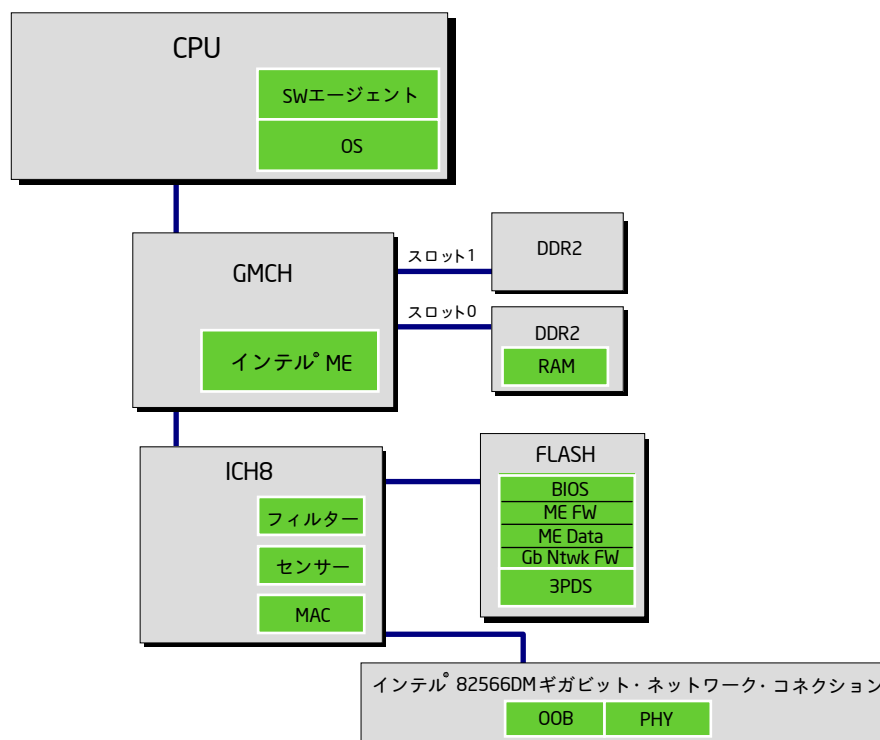


図1 インテル® AMT リリース 2.0 のアーキテクチャー

インテル® AMT の機能はファームウェア（ME FW）に格納されています。

- ファームウェア・イメージはフラッシュメモリーに格納されています。
- インテル® AMTの機能は、PCメーカーにより実装されるインテル® マネジメント・エンジン（インテル® ME）拡張BIOSを使用して有効にします。大規模組織向けのセットアップと構成はリモート・アプリケーションによって実行されます（「[認証と権限](#)」を参照）。
- 電源がオンになると、ファームウェア・イメージが DDR RAM にコピーされます。
- ファームウェアは、インテル® ME プロセッサー上で動作し、実行中に DDR RAM（スロット 0）のごく一部をストレージとして使用します。ファームウェアが動作するためには、RAM スロット 0 は設定済みで、電源がオンになっていなければなりません。

インテル® AMT は、以下の情報をフラッシュメモリー (**ME Data**) に格納します。

- OEM-configurable パラメーター
- パスワード、ネットワーク構成、証明書、アクセス制御リスト (ACL) などのセットアップ・構成パラメーター
- アラートやシステム・ディフェンス・ポリシーのリストなど、その他の構成情報
- 起動時に BIOS によって取得されたハードウェア構成

インテル® AMT は、サードパーティー・データ・ストレージ (3PDS) も管理します。ストレージ領域は、アプリケーションに関する重要な情報のローカルストレージとして、ソフトウェア・メーカーによって割り当てられます。

フラッシュメモリーには、BIOS 実行コード (**BIOS**) とインテル® 82566DM ギガビット・ネットワーク・コネクション (**GbE ネットワーク FW**) も格納されます。

フラッシュメモリーは、製造時に PC メーカーによって有効にされるハードウェア・メカニズムによってホストへの不正アクセスから保護されています。

**ICH8 インターフェイス・コントローラー**は、インバンドの入出力ネットワーク・トラフィック (プロセッサとの間のメッセージ・トラフィック) に適用されるフィルターの定義を保持します。これには、内部定義フィルターとシステム・ディフェンスおよびエージェント・プレゼンス・チェック機能を使用した ISV により定義されたアプリケーション・フィルターの両方が含まれます。

**インテル® 82566 ギガビット・ネットワーク・コネクション**は、アウトオブバンド (OOB) ネットワーク・トラフィック (インテル® AMT のトラフィック) を検出し、プロセッサではなくインテル® ME にルーティングします。インテル® AMT トラフィックは、IANA に登録されている専用のポート番号によって識別されます。

以下のコンポーネントはインテル® AMT とやり取りをします。

- **BIOS** を使用して、インテル® AMT の初期化、または初期状態へのリセットを行うことができます。プラットフォームのハードウェア構成情報を取得し、不揮発性メモリーに格納して、インテル® AMT がこの情報をアウトオブバンドで利用できるようにします。
- **ICH8 センサー機能**は、温度、ファンの状態、シャーシの保全性など、各種プラットフォーム・センサーの状態を検出します。選択されたセンサーの状態に変更があった場合やしきい値を超えた場合、アラートを格納または送信するようにインテル® AMT を構成することができます。
- プロセッサ上で実行される**ソフトウェア・エージェント** (通常、管理ソフトウェア・メーカーによって作成される) をインテル® AMT に登録して、「ハートビート」によりインテル® AMT と管理コンソールにその存在を知らせることができます。インテル® AMT はハートビートを監視し、エージェントの実行に問題がある場合は対処することができます。
- プロセッサ上の**ソフトウェア・メーカー製アプリケーション**は、ホスト・オペレーティング・システムと互換性のある専用ドライバーを使用して、インテル® AMT とローカルで通信することができます。

**インテル® AMT リリース 2.1** では、省電力オプションが強化されています。Sx 電力状態でスリープ中にネットワーク・インターフェイスがメッセージ受信した場合、インテル® AMT デバイスが起動されます。

**インテル® AMT リリース 2.2** では、リモート構成 (Zero-Touch Configuration または ZTC とも呼ばれる) が追加されています。これにより、インテル® AMT デバイスのセキュリティーを確保しながら、セットアップと構成プロセスを簡略化することができます。

### 3.1.1 インテル® AMTリリース 2.5 のアーキテクチャー

インテル® AMTリリース 2.5 では、エンタープライズ・ワイヤレス・モバイル・コンピューティングをサポートするようにAMTが拡張されています。図 2に示すように、アーキテクチャーにはモバイル用のICH8、CrestlineGM/PM965 MCH、ワイヤレスNICが含まれています。

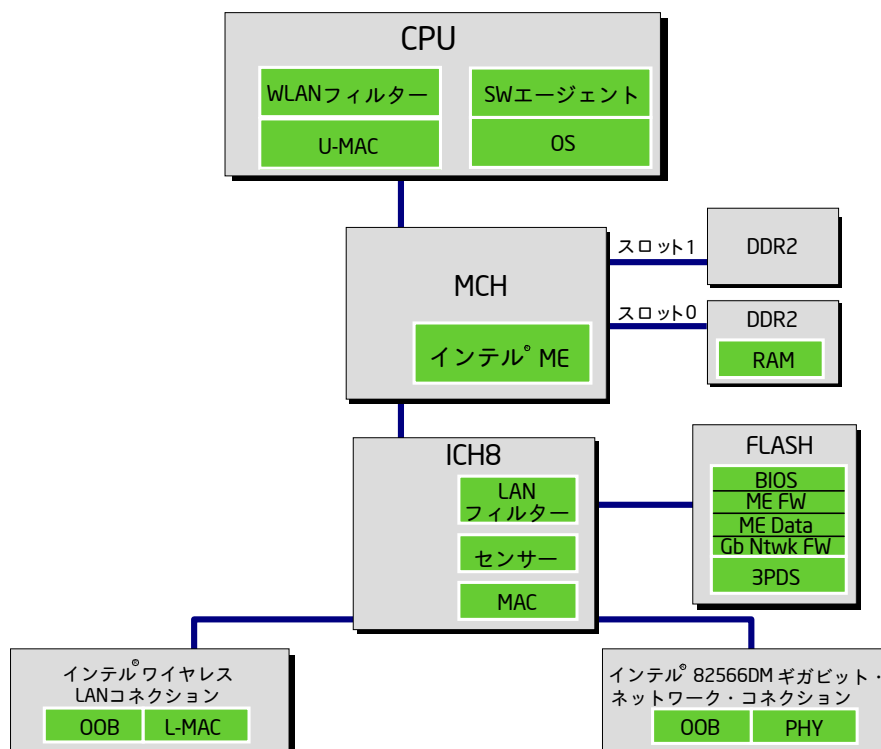


図2 インテル® AMT リリース 2.5 のアーキテクチャー

インテル® AMT リリース 2.5 では、リリース 2.0/2.1 に以下の機能が追加されています。

- ワイヤレス・ネットワーク・インターフェイスのサポート。インテル® AMT のアウトオブバンド管理は、このインターフェイスを介して行うことができます。また、このインターフェイスを介して送受信されるトラフィックに対してシステム・ディフェンスの packets フィルターを行うこともできます。
- IEEE802.1x EAP オプションのサポート。これにより、OS がアクティブでない場合でも、インテル® AMT はインバンドと OOB のワイヤレス・トラフィック処理を続行することができます。
- ワイヤレス接続が企業ネットワーク内のものかどうかを検出します。
- ローカル・プロセッサでアラートの登録と受信が可能なユーザー通知機能。インテル® AMT リリース 2.5 には、UNS (User Notification Service) が含まれています。これは、インテル® AMT アラート (システム・ディフェンス・アラートなど) を定義する Windows\* サービスです。インテル® AMT からアラートを受信すると、UNS は表示可能な Windows\* のイベントログに記録します。
- Cisco\* Network Admission Control (Cisco\* NAC) 規格に対応。このリリースには、ポスター情報を取得して、Cisco\* NAC デバイスに送信するプラグインが含まれています。

インテル® AMT リリース 2.6 では、モバイル・プラットフォーム向けのリモート構成とその他のいくつかの機能が追加されています。

### 3.1.2 インテル® AMTリリース 3.0 のアーキテクチャー

インテル® AMT リリース 3.0 のアーキテクチャーは、リリース 2.0 のアーキテクチャーに似ています。MCH は GMCH に、ICH8-DO は ICH9-DO にアップグレードされています。インテル® AMT リリース 2.5 の全機能（ワイヤレスとモバイル関連の機能は除く）に加えて、これらの変更と新しいバージョンのファームウェアは、以下の追加機能を提供します（詳細は、『ネットワーク・インターフェイス・ガイド』を参照してください）。

- ヒューリスティックなシステム・ディフェンス：企業ネットワーク全体に被害が拡大する前に、ホスト・プラットフォームからのワーム攻撃を発見し拡散を阻止するための基本機能です。
- WS-Management のサポート：この新しい規格は、以前のバージョンの SOAP ベースの API とともに、インテル® AMT プラットフォームの管理の手法として利用できます。関連ドキュメントについては、Documents フォルダの WS-Management\_Class\_\_Reference ディレクトリーを参照してください。
- リモート構成：インテル® AMT デバイスのセキュリティーを確保しながら、セットアップと構成のプロセスを簡略化します。

### 3.1.3 インテル® AMTリリース 4.0 のアーキテクチャー

リリース 4.0 では、モバイル・プラットフォームの機能に以下の機能が追加されています。

- 監査ログ：このログは、監査人権限を持つユーザーだけが監視できる、重要なインテル® AMT 監査可能イベントを記録します。監査ログは、「不正な管理者」がインテル® AMT ベースのシステムに損害を与えたり乗っ取ったりしようとした場合に備えて監査証跡を残し、こうした試みに対する抑止力になります。
- WS-Management：リリース 3.0 に含まれている DASH 1.0 のサポートが、モバイル・プラットフォームに拡張されています。
- リモート管理機能で Management Presence Server をサポート。
- Microsoft\* NAP のサポート：エンドポイント・アクセス制御機能が、Microsoft\* Network Access Protection (NAP) をサポートするように拡張されています。

### 3.1.4 インテル® AMTリリース 5.0 のアーキテクチャー

リリース 5.0 には、ワイヤレス機能を除くリリース 4.0 の全機能が含まれています。

## 3.2 リモートアクセス

インテル® AMT には、リモート・インターフェイス（インテル® AMT リリース 2.5/2.6/4.0 は、ワイヤレスおよび有線接続によるリモート・インターフェイスをサポート）とローカル・インターフェイスの 2 種類のインターフェイスがあります。リモート・インターフェイスは、LAN コネクションを介してトラフィックを送受信します。インテル® AMT のファームウェアは、ローカルユーザーやアプリケーションが重要な設定を変更してしまわないように、リモート・インターフェイスからのみ設定することができます。

リモート・アプリケーションは、以下の3つの方法を使用してインテル® AMT と通信します。

### SOAP (Simple Object Access Protocol) メッセージ

SOAP は、非集中型の分散環境で情報交換を行うための軽量なネットワーク・プロトコルです。XML ベースのプロトコルで、以下の3つの部分で構成されています。

- メッセージ内容とその処理方法について記述するためのフレームワークを定義するエンベロープ
- アプリケーション定義のデータ型のインスタンスを表す一連のエンコーディング規則
- リモート・プロシージャ・コールとレスポンスを表す規約

インテル® AMT のプログラマティック・インターフェイスは、インテル® AMT のファームウェアによって呼び出される SOAP ベースの API で、リモートホストで動作しているソフトウェア・メーカー製管理コンソール・アプリケーション・ソフトウェアと通信します。API は WSDL (Web Service Description Language) で記述されています。ファームウェア・サービス (インターフェイスとも呼ぶ) ごとに WSDL ファイルがあります。

### 独自のリダイレクション・プロトコル

インテル® AMT の機能を使用して、ソフトウェア・メーカーのアプリケーションは、コンソールテキストをリモートの接続先に送信したり、リモートの接続先からキーストロークを受信するようにプラットフォームを構成できます。これは Serial Over LAN (SOL) と呼ばれます。プラットフォームの IDE インターフェイスをリダイレクションして、リモートの FD/CD への読み書きを行うようにプラットフォームを構成することもできます。どちらの場合も、独自プロトコルを使用します。SDK に含まれているリダイレクション・ライブラリーを使用して、このプロトコルを実装できます。

インテル® AMT SDK には、リモート・インターフェイス機能の使用例を示すサンプルコードが多数含まれています。

### WS-Management

WS-Management (Web Services for Management) は、ネットワークのデバイス管理にオブジェクト指向アプローチを使用する DMTF の新しい規格です。この規格は、CIM (Common Information Model) に基づいており、インテル® AMT の全機能をサポートするように拡張されています。リリース 3.0 以降では、CIM オブジェクトとカスタム AMT オブジェクトを使用して、管理機能すべてをサポートしています。インテル® AMT は、DASH 1.0 暫定仕様を実装しています。WS-Management は、SOAP の上の別のレイヤーである点に注意してください。詳細は、SDK WS-Management ドキュメントを参照してください。

## 3.3 ローカルアクセス

プラットフォーム上でローカルに動作しているアプリケーションは、SOAP over HTTPまたは SOAP over HTTPSを使用するWS-Managementと同じ方法でインテル® AMTリリース2.0以降と通信します。以下の図 3に示すように、ローカル・アプリケーションがローカルのインテル® AMT ホスト名宛てのSOAP/HTTPSメッセージを送信すると、ホスト名へのトラフィックを待機するLMS (Local Manageability Service) はメッセージを読み取り、インテル® マネジメント・エンジン・インターフェイスにルーティングします。

LMS には以下の利点があります。

- ローカル・インターフェイスとリモート・インターフェイスを SOAP/WSDL ベースに統一して、API を簡略化します。
- ユーザー名とパスワードの認証、証明書ベースの認証機能と暗号化機能を追加するための HTTPS の使用の可能性など、HTTP 内蔵機能をフル活用します。

このインターフェイスは、インテル® ME と通信するマルチスレッド接続ベースのドライバーを組み込みます。対応するドライバーは、情報を受信して、インテル® AMT に組み込まれた IP スタックに渡します。

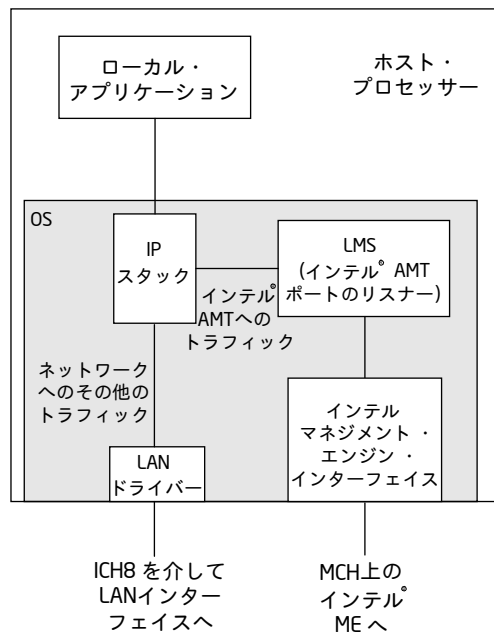


図3 インテル® AMT へのローカルメッセージのルーティング

ローカル・アプリケーションはストレージ・ライブラリーを使用して、リモート管理コンソールが後で読み出せるように、不揮発性メモリーに情報（ソフトウェア・インベントリーなど）を保存することができます。

### 3.4 UNS (User Notification Service)

UNS (User Notification Service) は、インテル® AMT リリース 2.5 以降がインストールされているプラットフォーム上のホストにインストールされる Windows\* サービスです。UNS は、アラートを受信するためにインテル® AMT デバイスに登録されます。UNS はアラートを受信すると、Windows\* のアプリケーション・イベント・ログに記録します。アラートを表示するには、[マイ コンピュータ] を右クリックして、[管理] - [システム ツール] - [イベント ビューア] - [アプリケーション] を選択します。

[ソース] は「インテル(R) AMT」です。定義されているすべてのアラートの [分類]、[イベント]、[説明] は以下の通りです。

分類	イベント	説明
System Defense (システム・ディフェンス)	1001	Security policy invoked. Some or all network traffic (TX) was stopped. (セキュリティ・ポリシーが起動されました。送信側ネットワーク・トラフィックの一部またはすべてが停止されました。)
System Defense (システム・ディフェンス)	1002	Security policy invoked. TX Network connectivity was reduced. (セキュリティ・ポリシーが起動されました。送信側ネットワーク接続が制限されました。)
System Defense (システム・ディフェンス)	1003	Security policy invoked. Some or all network traffic (RX) was stopped. (セキュリティ・ポリシーが起動されました。受信側ネットワーク・トラフィックの一部またはすべてが停止されました。)
System Defense (システム・ディフェンス)	1004	Security policy invoked. RX Network connectivity was reduced. (セキュリティ・ポリシーが起動されました。受信側ネットワーク接続が制限されました。)
Remote Diagnostics (リモート診断)	1201	A remote Serial Over LAN session was established. (リモート Serial Over LAN セッションを確立しました。)
Remote Diagnostics (リモート診断)	1202	Remote Serial Over LAN session finished. User control was restored. (リモート Serial Over LAN セッションを終了しました。ユーザー・コントロールが復帰しました。)
Remote Diagnostics (リモート診断)	1203	A remote IDE-Redirection session was established. (リモート IDE リダイレクション・セッションを確立しました。)
Remote Diagnostics (リモート診断)	1204	Remote IDE-Redirection session finished. User control was restored. (リモート IDE リダイレクション・セッションを終了しました。ユーザー・コントロールが復帰しました。)
WLAN	1102	WLAN Profile insufficient for management session over WLAN interface. (WLAN インターフェイスを介する管理セッションの WLAN プロファイルが不十分です。)
WLAN	1104	Management session was established over WLAN interface. (管理セッションは WLAN インターフェイスを介して確立しました。)
WLAN	1103	Security parameters insufficient for management session over WLAN interface. (WLAN インターフェイスを介する管理セッションのセキュリティ・パラメーターが不十分です。)
WLAN	1105	Management session over WLAN interface has finished. (WLAN インターフェイスを介した管理セッションを終了しました。)

## 3.5 レガシー・アーキテクチャー

インテル® AMT リリース 1.0 アーキテクチャーは、リリース 2.0 以降のアーキテクチャーに似ていますが、リリース 2.0 以降の機能をすべて備えているわけではありません。また、インテル® AMT リリース 1.0 のローカル・インターフェイスは、ローカル通信に同期型のシングルスレッド・スキーム (KCS/WMI 準拠) を使用します。インテル® AMT リリース 1.0 SDK を使用して作成されたアプリケーションをサポートするために、リリース 2.0 以降のシステムをレガシーモードで構成することができます。このモードは、必要な下位互換性を提供します。インテル® AMT リリース 1.0 リリース 2.0 以降の機能の相違点およびレガシーモードに関する詳細は、『ネットワーク・インターフェイス・ガイド』を参照してください。レガシーモードは、インテル® AMT リリース 4.0/5.0 ではサポートされていません。

## 4 機能概要

上記のセクション2で紹介した各使用例は、ファームウェアの機能の一部に依存しています。ここでは、各使用例でソフトウェア・メーカーが使用しているファームウェア・サービスについて簡単に説明します。インテル® AMTのファームウェア・サービスとインターフェイスは以下の通りです。

### 検出

**ハードウェア資産インターフェイス**を使用して、プラットフォームの最新のハードウェア・インベントリを取得することができます。プラットフォーム上でローカルに動作しているソフトウェア・アプリケーションは、**ストレージ・インターフェイス**と**ストレージ・ライブラリー**を使用して、不揮発性のサードパーティー・データ・ストア (3PDS) に情報を格納できます。

### 修復

検出使用例によるプラットフォームの現在のハードウェア構成とソフトウェア構成の判断に加えて、IT スタッフはプラットフォームのパフォーマンスをリモートで監視することができます。**イベント管理インターフェイス**を使用して、イベントフィルターの作成、イベントの記録、重要なイベントが発生した場合のアラートの送信が可能です。また、**リダイレクション・インターフェイス**と**リモート・コントロール・インターフェイス**を使用して、プラットフォームの制御とブートをリモートで行うことができます。

### 保護

ローカル・アプリケーションは、**ストレージ・インターフェイス**を使用して、ファイアウォールとウイルススキャンのバージョン情報を保存することができます。リモート・アプリケーションは、この情報を読み取り、ファイアウォールとウイルススキャンが最新の状態にあるかどうかを判断します。最新の状態ではない場合、リモート・アプリケーションは、プラットフォームの電源がオフであっても、**リダイレクション・インターフェイス**と**リモート・コントロール**を使用して更新することができます。更新が完了するまで、**システム・ディフェンス (サーキットブレーカー) インターフェイス**は、プラットフォームのネットワーク・アクセスを制限することができます。また、リモート・アプリケーションは、ホストの電源がオフであっても、**ストレージ・インターフェイス**を使用してプラットフォーム上に情報を保存することができます。プラットフォームの電源がオンになると、ローカル・アプリケーションは保存されたデータを読み取り、指示された更新を実行します。

## 制限

IT 管理者は、**リモート・エージェント・プレゼンス・チェック・インターフェイス**を使用して、クライアント・プラットフォームでウイルススキャン、ファイアウォール、ソフトウェア・インストール・トラッキング・プログラムなどを実行するために IT ポリシーによって要求されるアプリケーションを登録します。ソフトウェア・メーカーは、これらのアプリケーションに**ローカル・エージェント・プレゼンス・チェック・インターフェイス**の呼び出しを組み込みます。アプリケーションは実行を開始すると、インテル® AMT に「ハートビート」メッセージを送信します。アプリケーションを起動できない場合、またはウイルスによる処理の中断やユーザーによるシャットダウンで実行が停止された場合、インテル® AMT は問題を検出し、**イベント管理インターフェイス**を使用して管理コンソールにアラートを送信します。**サーキット・ブレーカー・インターフェイス**を使用して作成されたシステム・ディフェンス・ポリシーは、中断されたアプリケーションが実行可能になるまでワークステーションのネットワーク・アクセスを制限することができます。

## インフラストラクチャー

**セキュリティ管理インターフェイス**、**ネットワーク管理インターフェイス**、**ネットワーク・タイム・インターフェイス**は、アクセス制御リスト (ACL)、ネットワーク設定、セキュリティ・パラメーターの構成に使用します。これらのインターフェイスに関連する関数のほとんどは、セットアップ・構成プロセスで使用されます。

## 5 サービス

インテル® AMTの機能は、サービス（インターフェイスとも呼ぶ）に分けられます。『ネットワーク・インターフェイス・ガイド』で説明しているように、各サービスはリモート・ネットワーク・インターフェイスとローカル・インターフェイスのどちらか一方、または両方を介してアクセスすることができます。サービスに含まれる関数を使用するためには、ユーザーは対応するレルムへのアクセス権を所有していなければなりません。インテル® AMTアクセス制御リスト (ACL) におけるレルムの説明は、以下の「[アクセス制御リスト \(ACL\) とレルム](#)」を参照してください。表 1 は、インテル® AMTサービスのリストです。以下の2つのサービスには注意が必要です。

- ストレージ・インターフェイスは、SDK の一部であるストレージ・ライブラリーによってサポートされています。ストレージ・ライブラリー関数は、インテル® AMT、ストレージの割り当て処理、サードパーティー・データ・ストア (3PDS) の読み書きに対するユーザー接続を管理します。ストレージのコマンドとレスポンスは SOAP 接続を使用しますが、バイナリーメッセージ形式は1つだけで、ストレージ・ライブラリーによって作成および解釈されます。ストレージ管理インターフェイスは、別のレルムにあり、IT 管理者によりソフトウェア・メーカー製アプリケーションのサードパーティー・データ・ストア (3PDS) への書き込み権限と読み取り権限を指定するために使用されます。ストレージ・ライブラリーの機能については、『ストレージ設計ガイド』を参照してください。
- リダイレクション・インターフェイスは、リダイレクション関数のデータ転送に独自のメッセージ形式を使用します。詳細は、『リダイレクション・ライブラリー設計ガイド』を参照してください。

表 1. インテル® AMT のサービス

サービス	レルム	関数	ローカル	リモート	リリース
セキュリティ管理インターフェイス	PTAdministrationRealm	アクセス制御リスト (ACL)、Kerberos パラメーター、Transport Layer Security (TLS)、構成パラメーター、省電力オプション、パワーパッケージなど、セキュリティ管理データを管理します。		✓	1.0 以降
ネットワーク管理インターフェイス	PTAdministrationRealm	ローカル・ネットワーク・オプションを設定します。通常、DHCP サーバーを使用して設定されますが、このインターフェイスを使用して直接設定することも可能です。		✓	1.0 以降
ハードウェア資産インターフェイス	HardwareAssetRealm	プラットフォームのハードウェア・インベントリ情報を取得します。		✓	1.0 以降
リモート・コントロール・インターフェイス	RemoteControlRealm	リモートでのプラットフォームの電源オン/オフが有効になります。リモートでブートするために、リダイレクション機能と組み合わせて使用されます。		✓	1.0 以降
ストレージ・インターフェイス	StorageRealm	不揮発性ユーザーストレージの構成、書き込み、読み取りを行います。実際のコマンドは、ストレージ・ライブラリーにあります。	✓	✓	1.0 以降
イベント管理インターフェイス	EventManagerRealm	アラートの生成、リモートコンソールへの送信、ローカルでの記録を行うために、ハードウェアとソフトウェアのイベントを構成します。		✓	1.0 以降
	EventLogReader	インテル® AMT のシステムログの読み取り権限だけを持つユーザーを定義します。	✓	✓	2.6 以降
ストレージ管理インターフェイス	StorageAdminRealm	不揮発性メモリーの割り当てと使用を制御するグローバル・パラメーターを構成します。		✓	1.0 以降
リダイレクション・インターフェイス	RedirectionRealm	リダイレクション機能を有効または無効にし、リダイレクション・ログを取得します。リダイレクション・インターフェイス自体は、HTTP/SOAP に依存しない独自インターフェイスです。詳細は、『リダイレクション・ライブラリー設計ガイド』を参照してください。		✓	1.0 以降

サービス	レルム	関数	ローカル	リモート	リリース
ローカル・エージェント・プレゼンス・チェック・インターフェイス	AgentPresenceLocal レルム	ローカル・プラットフォームで動作するように設計されたアプリケーションによって使用されます。動作中であることを知らせ、定期的にハートビートを送信します。	✓		2.0 以降
リモート・エージェント・プレゼンス・チェック・インターフェイス	AgentPresenceRemote レルム	ローカル・エージェント・アプリケーションを登録し、アプリケーション実行中またはアプリケーションの実行が不意に停止された場合のインテル® AMT の動作を指定します。		✓	2.0 以降
サーキット・ブレーカー・インターフェイス	CircuitBreakerRealm	入出力ネットワーク・トラフィックを監視し、疑わしい状態が検出された場合にトラフィックを遮断するためのフィルター、カウンター、ポリシーを定義します (システム・ディフェンス機能)。		✓	2.0 以降
NetworkTime インターフェイス	NetworkTimeRealm	インテル® AMT デバイスのクロックを設定し、ネットワーク時間と同期します。		✓	2.0 以降
GeneralInfo インターフェイス	GeneralInfoRealm	全般設定とステータスの情報を返します。このインターフェイスを使用して、ほかのインターフェイスに関連付けられたパラメーターの読み取り権限をユーザーに与えることができます (パラメーターの変更権限は与えられません)。	✓	✓	2.0 以降
FirmwareUpdate インターフェイス	FirmwareUpdateRealm	PC メーカーによって、インテル® AMT のファームウェアを更新するために、インテルの提供するツールを介して使用されます。一般的にソフトウェア・メーカーが使用するものではありません。	✓	✓	2.0 以降
EIT	Admin	エンベディッド IT サービスを実装します (ソフトウェア・メーカー用ではありません)。	✓	-	2.1 以降
ワイヤレス構成 インターフェイス	Admin	ワイヤレス・インターフェイス設定を管理します。	-	✓	2.5、 2.6、 4.0 のみ
エンドポイント・アクセス制御 インターフェイス	EndpointAccessControl	NAC ポスチャーに関連付けられた設定を返します。	✓	-	2.5 以降

サービス	レルム	関数	ローカル	リモート	リリース
エンドポイント・アクセス制御管理インターフェイス	EndpointAccessControl Admin	NAC ポスチャを構成し、有効にします。	-	✓	2.5以降
ローカルユーザー通知インターフェイス	LocalUN	ローカル・インターフェイスのアラートをユーザーに提供します。	✓	-	2.5以降
セキュア監査ログ	Audit	システム監査人が重要なイベントを監視できるようにします。	-	✓	4.0以降
ユーザーアクセス制御	UserAccessControl	複数の ACL 管理コマンドを 1 つのレルムにまとめて、ユーザーが管理者権限を要求せずに自分のパスワードを管理できるようにします。	-	✓	4.0以降
リモートアクセス	RemoteAccess	インテル® AMT が Management Presence Server と連携して動作するのに必要なセットアップ・コマンドを提供します。	-	✓	4.0以降
WoX	WoX レルム	追加の「Wake on～」機能をサポートします。	✓	-	5.0以降

## 6 認証と権限

インテル® AMT 対応プラットフォームとのネットワーク通信は、最も安全な方法で行う必要があります。IT 管理者は、証明書ベースの認証と相互認証（オプション）を使用するように構成することができます。インテル® AMT には、すべてのアクセス要求の認証に使用されるアクセス制御リスト（ACL）があります。また、インテル® AMT では、認証プロセスを簡略化するために Microsoft\* Active Directory\* の Kerberos（オプション）を使用できます。インテル® AMT の処理の安全性を確保するためには、リモートのセットアップ・構成サーバーが必要です。

### 6.1 インテル® AMT セキュリティー・モデルの構成

インテル® AMT プラットフォームとセットアップ・構成サーバー（SCS）の通信は、2 つの共有情報（プラットフォーム ID と事前共有鍵（PSK））により開始されます。まず、インテル® AMT から SCS へ非暗号化形式の「hello」メッセージ（プラットフォーム ID を含む）が送信されます。SCS は、構成のためのトラフィックの認証と暗号化に PSK と TLS 事前共有鍵（TLS-PSK）プロトコルを使用して、セットアップ・構成プロセスを実行します。次に、SCS は、インテル® AMT プラットフォームに証明書をダウンロードし、不揮発性メモリーに格納します。この証明書は、企業内の証明機関によって発行されたもので、インテル® AMT が管理コンソール・アプリケーションを認証するために使用されます。インテル® AMT が相互認証向けに構成されている場合、SCS は、インテル® AMT と通信する各アプリケーションに、クライアント証明書を提供しなければなりません。

また、SCS はアクセス制御リスト (ACL) の設定、インテル® AMT の機能を有効化、デバイス設定の構成も行います。セットアップ・構成プロセスの最後に、プロセスで生成され、使用された鍵は削除されます。以降のすべての通信は、認証、秘匿機能 (暗号化)、保水性 (相互認証) に証明書と Transport Layer Security (TLS) を使用します。インテル® AMT は、以下で説明するように、アクセス制御リスト (ACL) を使用して許可を行います。HTTP Digest 認証は、SOAP over HTTP 通信に使用されます。リダイレクション機能は、SSL (Secure Sockets Layer) を使用して、リモートコンソールとインテル® AMT プラットフォーム間の安全な接続を確立します。詳細は、『サンプル・セットアップ・構成アプリケーション開発者ガイド』を参照してください。

## 6.2 アクセス制御リスト (ACL) とレルム

インテル® AMT のアクセス制御リスト (ACL) は、デバイス内の機能へのアクセス権を管理します。ACL エントリーには、ユーザー ID とユーザーがアクセス権を所有しているレルムのリストがあります。レルムに関連付けられた機能を使用するには、このアクセス権が必要です。上記の表では、各インターフェイスまたはサービスとそのレルムがリストされています。ユーザーは、1 つまたは複数のレルムへのアクセス権を所有することができます。

デフォルトのユーザーが 1 つ用意されており、ユーザー名は「admin」で、インテル® AMT のすべてのレルムへの権限が含まれる「PTAdministrationRealm」権限が与えられています。admin ユーザーは、セキュリティー管理インターフェイスのコマンドを使用して、追加ユーザーの ACL エントリーを作成することができます。セットアップ・構成プロセスの一環として、ソフトウェア・メーカー製アプリケーションに必要なユーザーを作成します。作成可能なユーザー数は、利用可能な ACL エントリーの数によって制限されます。

ACL エントリーには、Kerberos と Kerberos 以外の 2 種類があります。これらの主要な相違点は、Kerberos エントリーにはユーザーやユーザーグループを識別するための Microsoft\* Active Directory\* SID があるのに対して、Kerberos 以外のエントリーにはユーザーを識別するためのユーザー名とパスワードがあります。これらのエントリーの相違点については、『インテル® AMT と Active Directory\* の統合』を参照してください。

## 7 関連情報

『SDK ユーザーガイド』は、インテル® AMT ソフトウェア開発キット (SDK) について説明しています。関連ドキュメントや必要なシステム構成、インテル® AMT 機能の使用例を示すサンプルコードの要約が含まれています。

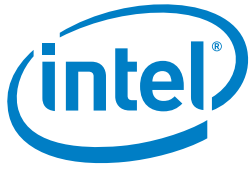
『ネットワーク・インターフェイス・ガイド』は、SOAP ベースのインターフェイスに関するドキュメントです。

『ストレージ設計ガイド』は、ソフトウェア・メーカーのストレージ・ライブラリーの構造、関数、使用方法について説明しています。

『リダイレクション・ライブラリー設計ガイド』は、このインターフェイスの関数とそれをサポートしているサンプル・アプリケーションについて説明しています。

インテル® AMT の WS-Management インターフェイスの詳細は、SDK Documents ディレクトリ内の **WS-Management\_Class\_Reference** フォルダーを参照してください。また、『インテル® AMT の WS-Management フロー』も参照してください。

SDK の各サンプルには、readme ファイルがあります。サンプルを使用する前に、必ず readme ファイルをお読みください。



インテル株式会社

〒 100-0005 東京都千代田区丸の内 3-1-1  
<http://www.intel.co.jp/>

©2008 Intel Corporation. 無断での引用、転載を禁じます。  
2008 年 11 月

318817-003JA  
JPN/0906/PDF/SE/DO/MH