



インテル® vPro® プラットフォーム： 非常時でも、通常どおりのビジネスニーズに 応える設計

自宅学習とリモートワークをサポートするためのヒント

在宅勤務の従業員が急増し対応に追われている場合も、オンライン学習の環境を整えて配信する場合も、インテル® vPro® プラットフォームを基盤とするPC資産ならば管理の心配はありません。すでに所有しているこのプラットフォームには、今必要なテクノロジーがすべて組み込まれています。

インテルは長年にわたり、仕事の本質の変化とリモートワーカーの増加に注目してきました。その結果として、インテル® vPro® プラットフォームには、リモートワーク、教育、技術サポート、ますます巧妙化するセキュリティ脅威に対する保護に必要なテクノロジーの多くがすでに組み込まれています。PC資産をインテル® vPro® プラットフォーム対応デバイスで構成している場合、リモートPCを継続的に稼働させるために必要なものはすでに用意されているはずです。

インテル® vPro® プラットフォームでは、Windows* ベースのすべてのデバイスで、実際の問題をすぐに解決できる優れたツールを利用できます。ここでは、インテル® vPro® プラットフォームを最大限に活用するうえで役立つリソースをまとめました。

リモート管理機能

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)

まず実行できるアクションは、インテル® vPro® プラットフォーム対応デバイスでインテル® AMTを有効にすることです(まだ有効にしていない場合)。リモートワーク中は、自分のマシンをオンサイトに持ち込んでサポートを受けるのも難しく、技術者が自宅に派遣されることもないと考えられます。そのため、リモート管理機能はこれまで以上に重要になります。インテル® アクティブ・マネジメント・テクノロジーによって可能になります。

ハードウェア・ベースのインテル® アクティブ・マネジメント・テクノロジーは、OSから独立して機能する安定したアウトオブバンド接続を提

供し、OSがダウンした場合でも、システムのさまざまな問題を修復できます。システムが応答せず、実行も起動もできない場合は、破損したドライバー、アプリケーション・ソフトウェア、OSを修復します。また、KVMを使用して、OSのアップグレードを監視したり、システムBIOSを起動することもできます。

インテル® AMTは、IT部門と端末ユーザーを直接つなぐトンネルです。インテル® AMTを使用すると、PCの電源がオフになっていたりオペレーティング・システムがダウンしている場合でも、PCにリモート接続して、ネットワーク接続されたコンピューティング資産を検出、修復、保護することができます。

OSよりも下の層で動作するハードウェア・ベースのこの独自のテクノロジーにより、技術者は、OSとドライバーの修復やアップグレードが可能になります。つまり、OSよりも下の層に入ることができるということです。これは、チームがVPNにログオンできない場合でも機能します。ヘルプデスクは、チームの生産性をリモートから引き続きサポートできます。

通常の状況では、この機能によってIT部門の時間が節約され、管理の負担も軽減されます。最近の状況では、インテル® AMTは、従業員が業務を継続し、生産性を維持するための最良の選択肢と言えます。

インテル® AMTによるITチームの支援：

ハードウェアKVMでは、キーボード/ビデオ/マウスのリダイレクション操作によって、リモートPCに安全に接続して管理します。このKVMはソフトウェア・ベースではなくハードウェア・ベースであるため、OSが稼働していないときでも機能し、再起動中やBIOS内でもKVMセッションを維持できます。



マネージドITサービス・プロバイダーは、**ブート・リダイレクション**を使用してリモートPCを一時的な環境で再起動できます。これには診断ツールからウイルススキャン、OSインストール・イメージまで、サポート技術者がUSBキーに保持しているISOイメージが考えられ、例えばデスクトップPCのハードディスク・ドライブが故障し、技術者が新しいハードディスクを持って到着するまでに数時間かかるといった場合は、ブート・リダイレクションによるリモート再起動を実行すると、別の方法では操作できないPCが一時的な作業環境に配置されます。そのため、従業員は新しいハードディスク・ドライブが届くのを待っている間も、ウェブページからメールやインターネット・サービスに引き続きアクセスできるので、ハードウェア障害が発生した場合でも高い生産性を維持できます。新しいドライブが届いたら、技術者はリカバリー/再インストール・プロセスをリモートから開始できます。

その他のさまざまなメリット:

- リモートで電源をオンにしてPC資産全体を管理: 修復やバッチ適用のために、単一のシステム、またはすべての職場のあらゆるシステムの電源をオンにできます。
- 起動時間を設定し、更新のスケジュールを設定: ユーザーがデバイスの前にいなくても、メンテナンスを確実に実行できます。
- 無人システムをリモートから管理: デジタルサイネージ、Intel Unite® ソフトウェア搭載システム、小売業のPOSシステムなどをリモートから管理できます。
- OSアップグレードへの対応: Windows* 10など、OSアップグレードの起動プロセスを監視します。

インテル® アクティブ・マネジメント・テクノロジーをまだ設定していない場合

インテルでは、リモートワーカーのサポートに役立つハウツービデオが含まれたYouTube*のプレイリストを用意しました。
<https://bit.ly/2UKCObl> を参照してください。

インテル® AMTを使用すると、マネージドITサービス・プロバイダーは、現場にいる場合と同様にPCをリモートから制御できるため、サポートコストとダウンタイムを削減できます。



インテル® AMTはファイアウォールの外側でも利用できることをご存知でしょうか。インテル® エンドポイント・マネジメント・アシスタント (インテル® EMA) により、ITチームはオンサイトデバイスと同様にリモートPCも制御できるため、従業員や学生のホーム・ネットワークが接続すれば、24時間365日、サポートが可能になります。インテル® EMAは、クラウドを介してインテル® AMTを最新化するように設計されており、既知のネットワークの範囲内にあるPCへのインバンド (OS/エージェント・ベース) 接続とアウトオブバンド (OSよりも下の層) 接続の両方に対応します。IT技術者は、PCのOSがクラッシュまたはハングアップした場合でも、ユーザーが技術的な問題を特定して解決できるようリモートから支援できます。

- 企業ファイアウォールの内外にあるデバイスに接続: IT部門はインテル® vPro® プラットフォーム用に構築されたソフトウェア・ツールを使って、企業ファイアウォールの内外にあるデバイスに、クラウド経由でリモートからより安全に接続できます。
- クラウドからデバイスを管理: インテル® エンドポイント・マネジメント・アシスタントにより、ITユーザーはインテル® AMTへのアクセスをカスタムまたはサードパーティーのコンソールに統合できます。これらの管理対象デバイスはクラウドに配置でき、パブリック・ネットワークでもプライベート・ネットワークでもかまいません。コンソールは、プライベート・ネットワーク、エッジ、またはパブリック・クラウドに配置できます。

これまでの懸念事項を解消:

PCのセキュリティー機能

リモートワーク、過密状態のVPN、クラウドアプリの使用が増えたからといって、セキュリティーの脅威まで増大するわけではありません。最新PCの一部で利用可能なインテル® ハードウェア・シールドでは、セキュリティー機能がハードウェアに組み込まれています。



従来のセキュリティ対策は一般にソフトウェアのみのアプローチであり、通常は「OSよりも上の層」で動作します。しかし、攻撃はますます巧妙になり、「スタックを下って」ハードウェアとソフトウェアの間を移動し、ITの従来のセキュリティ対策を脅かしています。インテル® ハードウェア・シールドは、デバイスを脅威からフルスタックで保護するハードウェア支援型セキュリティ機能の集合です。

インテル® ハードウェア・シールドを使用する場合、有効化は不要です。お使いのPCでメーカーがこのテクノロジーを有効にしていれば、すでに脅威から防御されています。

パフォーマンス

授業のストリーミング、ビデオ会議、クラウドベースのコラボレーションが増えれば、PCに負荷がかかりますが、究極のプロセッサが搭載されているので問題ありません。授業に参加するときも、電話会議をすぐに始めるときも、これらのPCは優れた応答性とパフォーマンスを発揮します。さらに、GPUオフロードによりCPUを生産性タスクに集中できるため、パフォーマンスを低下させることなくセキュリティ・スキャンを継続できます。

パフォーマンス = ユーザー体験の向上

ドッキング・ステーションや複数のモニターなどの周辺機器の追加も簡単に行うことができます。誰でもホームオフィスや自宅学習の環境を通常と同じ構成でセットアップでき、リモートの生産性がさらに高まります。

コネクティビティ

インテル® vPro® プラットフォームを基盤とする最新PCの一部には、Wi-Fi® 6が内蔵されています。Wi-Fi® 6は最新の規格として、公共施設、公共スペース、オフィス、家庭用サービス・プロバイダーで今後の展開が見込まれます。最新のインテル® vPro® プラットフォームにはこの規

格が組み込まれているので、Wi-Fi® 6対応のホームルーターの普及が進めば、PC資産の準備が整います。

まとめ

従業員の生産性の維持はビジネスに有益です。また、通常どおり業務を継続したい人々にとっても有益です。学習、共同作業、単独作業のいずれであっても、ほとんどの人はテクノロジーの問題に邪魔されたくはありません。インテル® vPro® プラットフォームなら、内蔵のテクノロジーにより、PCの効率と稼働時間を低下させることなく、企業資産を保護しながら、従業員のつながりと生産性を維持できます。

リソース:

最新の管理機能を提供するインテルのテクノロジーの詳細については、<http://www.intel.co.jp/amt/> を参照してください。

作業手順のビデオ、ガイド、専門家による支援など、インテル® アクティブ・マネジメント・テクノロジーの使用を開始するためのツールについては、<http://www.intel.co.jp/content/www/jp/ja/architecture-and-technology/implementation-of-intel-active-management-technology.html> を参照してください。

インテル® vPro® プラットフォームの詳細については、<http://www.intel.co.jp/vPro/> を参照してください。





すべての条件下で絶対的なセキュリティを提供できるコンピューター・システム、製品、コンポーネントはありません。一部のインテル® Core™ プロセッサ・ファミリーで利用できる内蔵セキュリティ機能を使用するには、別途ソフトウェア、ハードウェア、サービスまたはインターネットへの接続、あるいはその両方が必要となる場合があります。結果は、システム構成によって異なります。詳細については、各PCメーカーにお問い合わせください。

Intel、インテル、Intelロゴ、Intel Core、Intel Unite、vPro、Intel vProは、アメリカ合衆国および/またはその他の国におけるIntel Corporationまたはその子会社の商標です。

* 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。

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/>

©2020 Intel Corporation. 無断での引用、転載を禁じます。

2020年7月

342367-001JA
JPN/2007/PDF/SE/CS/KS