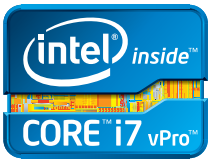
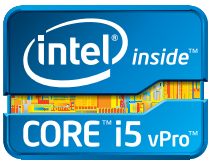
第 3 世代インテル® Core™ vPro™ プロセッサー・ファミリーの概要

ビジネスをより快適に、そしてよりセキュアに

ホワイトペーパー

第 3 世代インテル® Core™ vPro™ プロセッサー・ファミリー





エグゼクティブ・サマリー

今日、ビジネス PC に対する企業の要求はますます厳しくなっています。競合他社に負けない生産性と俊敏性を確保するためには、情報への素早いアクセスと、時間や場所を問わないレスポンス、多様なコミュニケーション手段が必要となります。その一方で企業は、自社を標的とする攻撃や、世界中に広く蔓延し、PC のバックグラウンドから絶えず侵入を試みてくる脅威に対しても注意を払わなければなりません。PC のパフォーマンス向上とさまざまなセキュリティー・リスクからの保護、この 2 点は企業の IT 部門にとって大きな課題となっています。第 3 世代インテル® Core™ vPro™ プロセッサー・ファミリーを搭載したビジネス・クライアント PC は、ビジネスをより快適に、そしてよりセキュアにすることを目的として設計されており、全く新しいレベルのパフォーマンスと最先端のセキュリティー・テクノロジーが組み込まれています。これを可能にしているのが、第 3 世代インテル® Core™ vPro™ プロセッサー・ファミリーが提供するハードウェア・ベース・テクノロジーの数々です。本ホワイトペーパーでは、これらのテクノロジーについて説明し、さらに、ビジネス PC に高い要求を持ち、俊敏性を追求する企業にとっての利点も紹介します。

第 3 世代インテル® Core™ vPro™ プロセッサー・ファミリー

速さとセキュリティーを追求して設計されたプロセッサー

ビジネスがボーダレス化した現在、モビリティーは必須となり、さらに扱うコンテンツもマルチメディアが主流となっています。ビジネスの生産性と俊敏性を維持するためには、情報への素早いアクセス、時間や場所を問わないレスポンス、多様なコミュニケーション手段が不可欠です。企業の IT 部門は、高性能なビジネス・クライアント PC によってこれらの要件を満たす必要があります。また、ビジネス向けのデスクトップ PC やノートブック PC にとってはセキュリティーも最優先事項であり、さらには管理コストを削減するための自動化されたリモート運用管理も求められています。

第 3 世代インテル® Core™ vPro™ プロセッサー・ファミリーを搭載したビジネス・クライアント PC には、インテル® vPro™ テクノロジーが組み込まれています。[1] これらの PC は、IT 部門の担当者が予防的、効率的、効果的、かつ迅速な対応を行うために必要なハードウェア・ベースの機能を内蔵しています。これらの機能はハードウェアに組み込まれているため、マルウェアの目には触れず、攻撃を受けることもなく、最先端の PC セキュリティーと、安全なアウトオブバンド（OOB）通信、リモートからの運用管理機能を実現します。こうした機能を利用することで、IT 部門はビジネス PC を保護し、トラブルシューティングや修復、メンテナンス作業を自動化するとともに、オンサイトでのサポート件数を減らすことができます。その結果、IT 部門は、ビジネス・クライアント PC の総保有コスト（TCO）を削減し、業務効率を向上させることで、企業収益にも貢献できます。

最先端のセキュリティー

第 3 世代インテル® Core™ vPro™ プロセッサー・ファミリーが内蔵するセキュリティー・テクノロジー [2] によって、これまでのビジネス PC にはなかった、高いレベルでの保護が可能になります。このテクノロジーは、OS やインストール済みのソフトウェア・エージェントおよびアプリケーションより下の階層で動作し、重要なビジネスとそのデータを守る上で必要不可欠な ID 管理および認証、データ保護、修復、レポート機能など、より深いレベルで脅威への対策を実現します。また、この内蔵機能は、ビジネス・クライアント PC 自身が自らを監視および保護することも可能にします。第 3 世代インテル® Core™ vPro™ プロセッサー・ファミリーのセキュリティー機能は、表 1 のとおりです。

表 1．第 3 世代インテル® Core™ vPro™ プロセッサー・ファミリーのセキュリティー機能

ユーザー /IT 部門が求める要件	ソリューション	インテルのテクノロジー
脅威への対策 不正なソフトウェア・エージェントが OS より下の階層へ侵入することを防ぐ。	▪ ルートキットなどのステルス手法を使用するウイルスやマルウェアによる高度な攻撃を防止します。ルートキットやマルウェアの侵入から、データセンターにホスティングされたデスクトップ仮想化やビジネス・クライアント PC 上の仮想化環境などの仮想領域を保護します。	▪ インテル® OS ガード [3] ▪ インテル® トラステッド・エグゼキューション・テクノロジー [4] ▪ インテル® バーチャライゼーション・テクノロジー [5]
ID およびアクセスの保護 ワンタイムパスワード（OTP）トークンおよび公開鍵基盤（PKI）証明書を保護する。 実在のアクセス権限を持つユーザーだけが認証情報にアクセスできるようにする。	▪ 運用管理の負荷を抑えながら、認証トークンおよび証明書を OS より下の階層のハードウェアで保護します。 ▪ 認証情報をネットワークへ送信する前に、キーロガーやスクリーン・スクレーパーからユーザー入力を保護します。	▪ 公開鍵基盤（PKI）およびワンタイムパスワード（OTP）を備えたインテル ® プロテクション・テクノロジー [6] ▪ ディスプレイへの表示を保護するインテル® アイデンティティー・プロテクション・テクノロジー
データ保護 意識せずに利用できる暗号化。より安全な暗号鍵や暗号化の基盤によって、盗難やコンプライアンス違反から PC を保護する。	▪ パフォーマンスを低下させることなく、高速な暗号化 / 復号が可能です。 ▪ さまざまな暗号化ソリューションを導入でき、データの安全性を確保します。 ▪ 真の乱数シードを、マルウェアから見えないところで生成します。 ▪ ノートブック PC が紛失または盗難に遭った場合に、データを保護します。 ▪ ノートブック PC が紛失または盗難に遭った場合、自動的にノートブック PC を無効にします。	▪ インテル® AES New Instructions [7] ▪ インテル® セキュアキー [8] ▪ インテル® アンチセフト・テクノロジー [9]
監視、修復、レポート クライアントへの安全なリモートアクセスを可能にし、迅速な診断、修復、およびトークン / 証明書の修復 / 破棄 / 再発行を実現する。	▪ 電源や OS の状態に関係なく、PC に対するリモートアクセスおよびトラブルシューティング / 修復を可能にします。 ▪ 感染した PC を自動的にネットワークから隔離します。 ▪ 復旧した PC をリモートから再有効化します。	▪ インテル® アクティブ・マネジメント・テクノロジー [10] ▪ ハードウェア・ベースのリモート KVM 制御 [11] ▪ アウトオブバンド通信の保護

運用管理機能の強化

IT 部門の担当者は管理コンソールを使用して、PC のオペレーティング・システム（OS）から独立した内蔵運用管理機能にアクセスできます。電源、OS、ハードディスク・ドライブの状態に関係なく、管理機能は常に使用可能であるため、IT 担当者はビジネス PC のアップデート、トラブルシューティング、監視、安全性の確保を行うことができます。

第 3 世代インテル® Core™ vPro™ プロセッサー・ファミリーを搭載した PC により、IT 部門は有線または無線の企業ネットワークを介して管理機能に接続できます。さらに、PC がファイアウォールの外側で接続されていても、オープンな無線ネットワークを介して接続するという手段が用意されています。このようなビジネス・クライアント PC は、何らかの脅威が検出された場合、または IT 部門が事前に設定したポリシーと PC の状態が異なる場合、管理およびメンテナンスを目的としたコンソールとの通信をクライアント PC 主導で開始できます。第 3 世代インテル® Core™ vPro™ プロセッサー・ファミリーの運用管理機能を、表 2 に示します。

幅広いサポート

第 3 世代インテル® Core™ vPro™ プロセッサー・ファミリーを搭載した PC は、プロセッサー、チップセット、ネットワーク・コネクションに組み込まれた機能と、保護されたフラッシュメモリーを利用します。インテル® vPro™ テクノロジーとソフトウェア・ベンダー各社が提供するインテル® vPro™ テクノロジー対応の既存の管理コンソールを組み合わせることで、応答性と耐改ざん性を兼ね備えた包括的なセキュリティー / 運用管理ソリューションを実現できます。Microsoft、MOTEX、Sky など、主要な管理ソフトウェアの開発元である企業では、第 3 世代インテル® Core™ vPro™ プロセッサーの機能を活用するよう最適化された製品を提供しています。

定評ある信頼性の高い ROI

IT 部門において、ビジネス・クライアント PC への自動化されたリモートアクセスは、IT 効率や企業収益にかなり大きな影響を及ぼします。さらに、安全なコンソール・リダイレクションやリモート KVM 制御などの機能により、問題の診断と解決をリモートから適切に行うことができるため、ユーザーのダウンタイムを削減して生産性を向上できるほか、オンサイトサポートの回数を最小限に抑えて総保有コスト（TCO）を大幅に削減することもできます。以下に、具体的な例を挙げます。

- デスクトップ PC では、ソフトウェアに関連したオンサイトサポートの必要性が最大 56% 削減されます。[13]
- ノートブック PC では、これまで検出されなかったソフトウェア資産を検出する能力が最大 47% 向上し、ノートブック PC の資産管理の失敗件数が最大 62% 減少します。[13]
- ビジネス・アプリケーションの実行速度が最大 60% 向上し、マルチタスク処理速度が最大 2 倍に向上します。また、機密データの暗号化 / 復号処理速度が最大 4 倍に向上しており、明らかなパフォーマンスの向上を実感できます。[14]
- 電力コストが削減され、パッチ適用時間も最大 56% 短縮されます。[13]

適切に管理されていない PC は、無駄な消費電力を生む原因となります。使用していないシステムの電源をリモートからオフにするだけで、わずか 9 カ月で PC への投資を回収した企業もあります。[15] これ以外にもコストや時間を削減する機能を導入すれば、さらなる節約が可能となります。

表 2. 第 3 世代インテル® Core™ vPro™ プロセッサー・ファミリーの運用管理機能

必要とされる運用管理機能	利点 / 機能
コンソール・リダイレクションおよびリモート KVM 制御を利用した画面転送 [11,a,b]	**オンサイトサポートを削減し、ユーザーの生産性を向上させます。**クライアント PC へのリモートアクセスにより、IT スタッフが現地にいる場合と同様のサポート、トラブルシューティング、修復を可能にします。IT 部門は、PC の電源状態、OS 状態、またはハードディスク・ドライブを使用できるかどうかに関係なく、電源投入 / 切断、BIOS 設定や通常の操作など、あらゆる PC の状態を把握し、制御できます。また、他のクライアント・デバイスやローカルな IT ストレージ、またはネットワーク・ドライブから強制的にブートすることも可能です。
リモートからの電源管理 [a,b]	**オンサイトサポートを削減するとともに、電力コストを削減します。**IT 部門は、トラブルシューティング、アップデート / アップグレードのために PC の電源をリモートから投入または切断でき、使用していないときの電力を削減できます。
リモートからのソフトウェア・アップデート [a,b]	**オンサイトサポートを削減し、PC の健全性、パフォーマンス、信頼性の維持に役立ちます。**OS、エージェント、ソフトウェアのアップデート / アップグレードをリモートから実施します。従業員の生産性を落とさないように、夜間や休日にアップデートを実行できます。また、アップデートやパッチの適用を自動的に行うことも可能です。
クライアント PC 主導の自動起動とタスクの実行 [a,b]	**オンサイトサポートを行うことなく、PC の健全性を自動的に維持します。**クライアントは、事前に IT 部門により設定された時刻に自動的に起動します。PC が起動すると、PC 上のサードパーティー製ソフトウェア・エージェントが管理サーバーと通信し、アップデートやメンテナンスなどのタスクを業務時間外に実行します。[12]
エージェント動作チェックとアラート送信 [a,b,c]	**PC の健全性やコンプライアンスを自動的に維持します。**クライアント側のエージェントによる定期的なハードウェアとの通信により、重要なアプリケーションが実行されていることを確認し、一定時間通信が行われなかった場合は IT 部門に迅速に通知されます。[c]
ネットワーク・トラフィックの監視 [a,b]	**PC の健全性や信頼性を維持します。**プログラミング可能なフィルターが、ネットワーク・トラフィックを監視し、疑わしいパケットのヘッダーや頻度をチェックします。
システムの隔離と回復 [a,b]	**ネットワークでのウイルスの蔓延を防ぎます。**脅威が検出された場合、ローカル・ネットワーク接続は強制的に遮断されますが、運用管理のための管理コンソールとの接続は引き続き維持されます。
リモート診断 / 修復 [a,b]	**オンサイトサポートを削減するとともに、TCO も削減します。**アウトオブバンドのイベントログ、リモート起動および外部ディスクからの起動、コンソール・リダイレクション、リモート KVM 制御、BIOS 設定画面へのアクセスなどを利用して、問題をリモートから診断し修復します。
リモートからのハードウェア / ソフトウェア資産管理 [a,b,c]	**PC のコンプライアンスおよび健全性を維持します。**OS の状態や PC の電源状態に関係なく、ハードウェアやソフトウェアを監視します。[c] 資産情報は PC の不揮発性メモリーに格納され、いつでもアクセスできます。

[a] これらのインテリジェントなセキュリティー機能やリモート運用管理機能を利用するには、インテル® vPro™ テクノロジーを有効にするアクティベーションの作業が必要になります。インテル® vPro™ テクノロジー（インテル® AMT を含む）のアクティベーションの方法については、http://www.intel.com/content/www/us/en/remote-support/implementation-of-intel-vpro-technology.html（英語）を参照してください。

[b] ユーザー OS がダウンした場合に無線で操作するには、WPA または WPA2/802.11i セキュリティーとコントローラー・リンク 1 が必要です。

[c] ホスト OS ベースの VPN を使用している場合にも利用できます。

内蔵されたセキュリティー機能による最先端の保護

近年のセキュリティー脅威には、ユーザーが企業データやシステムにアクセスする瞬間を狙ったものが少なくありません。企業は常に、自社を標的とした限定的な攻撃にさらされており、従来の無差別的なウイルス攻撃よりも大きなダメージを受ける可能性があります。さらに、サイバー犯罪者はターゲットに気付かれにくいステルス手法を駆使しているため、脅威の検出、予防、除去がより困難になっています。

第 3 世代インテル® Core™ vPro™ プロセッサー・ファミリーを搭載したビジネス PC は、セキュリティー・テクノロジーをソフトウェア・レベルでなく、ハードウェア・レベルで組み込むことで、最先端のセキュリティー機能を提供します。このハードウェア・ベースの内蔵テクノロジーにより、脅威に対する管理能力の拡張、ID およびアクセス保護の強化、データ・セキュリティーの向上、およびリモートからの自動的なイベント監視、修復、レポート機能が実現されます。

ハードウェア・ベースの脅威対策と、ID およびアクセスの保護

第 3 世代インテル® Core™ vPro™ プロセッサー・ファミリーに備わるハードウェア・ベースの内蔵セキュリティー・テクノロジーは、OS、ソフトウェア・エージェント、アプリケーション・ソフトウェアより下の階層で動作し、さまざまな攻撃や不正侵入がもたらす脅威を防止します。さらに、データやマシンの保護にも威力を発揮します。トークンや PKI 証明書が OS より下の階層のハードウェアで保護されており、ハードウェア・ベースのセキュリティーならではの堅牢性に加えて、ソフトウェア・ベースのソリューション並みの導入の容易さや日々の管理のしやすさを実現します。

脅威の管理や、ID の盗難および不正アクセスに対する保護を可能にする第 3 世代インテル® Core™ vPro™ プロセッサー・ファミリー搭載ビジネス・クライアント PC の内蔵セキュリティー・テクノロジーには、以下のものがあります。

- **OTP または PKI を備えたインテル® アイデンティティー・プロテクション・テクノロジー** [6] **:** ハードウェア・アシストにより、マルウェアや OS から影響を受けないレイヤーでワンタイムパスワード（OTP）トークンおよび公開鍵基盤（PKI）証明書を保護。ハードウェア・ベースならではの強力なセキュリティー機能を、ソフトウェア・ベース並みの利便性および応答性で提供します。
- **ディスプレイへの表示と入力を保護するインテル® アイデンティティー・プロテクション・テクノロジー** [6] **:** ハードウェア・ベースの認証により安全な入力を保証し、ユーザーの存在を証明します。
- **インテル® OS ガード** [3] **:** マルウェアが OS より下の階層に常駐することを防ぎます。
- **インテル® トラステッド・エグゼキューション・テクノロジー** [4] **:** 仮想マシンを起動する際に、信頼できる環境かどうかを検証します。
- **インテル® バーチャライゼーション・テクノロジー** [5] **:** 仮想化環境の特定のタスクを強化し、安全を確保することで、PC のさらなる保護を実現します。
- **インテル® アンチセフト・テクノロジー** [9] **:** モバイル環境で利用されるノートブック PC を保護します。

あらゆる場所でデータと PC を保護

第 3 世代インテル® Core™ vPro™ プロセッサー・ファミリー搭載ビジネス・クライアント PC には、データをサイバー犯罪者の手の届かない場所に置いたり、モバイル環境で利用される PC を保護するなど、さまざまなハードウェア・ベースのセキュリティー・テクノロジーが内蔵されています。

インテル® AES New Instructions

暗号化によってデータを保護できますが、旧来のリアルタイム暗号化には高い PC パフォーマンスが必要で、生産性低下の要因となってきました。しかし、プロセッサーに内蔵されたインテル® AES New Instructions（インテル® AES-NI）により [7]、暗号化と復号の処理速度は最大 4 倍に高速化されます。[14] こうしたパフォーマンスの向上により、第 3 世代インテル® Core™ vPro™ プロセッサー・ファミリーを搭載したビジネス・クライアント PC では、ユーザーは意識せずに暗号化機能を利用できます。

インテル® セキュアキー

暗号化に乱数が必要となる場合も、高品質の乱数がマルウェアの目の届かないところで生成されるため、安全性がより高まります。インテル® セキュアキー [2,8] は、真の乱数命令を使用して、独立したハードウェア上で乱数を自動生成する機能です。乱数の生成プロセスが非可視化されているため、ソフトウェアの乱数生成命令に影響を及ぼす恐れがあるエージェントからプロセスを隔離することができます。

インテル® アンチセフト・テクノロジー

PC の紛失や盗難は、企業にとって大きな損害につながる可能性があります。インテル® アンチセフト・テクノロジー [2,9]（インテル® AT）に対応したビジネス・ノートブック PC は、紛失や盗難による損害のリスクを大幅に軽減します。インテル® AT は、PC 上で何らかの脅威が検出されると、自動的に PC の安全性を確保し、ハードディスク・ドライブと内蔵セキュリティー・キーをロックして、ユニットを使用できない状態にします。たとえハードディスク・ドライブが取り外されたとしても、データにアクセスすることはできません。さらに、3G ネットワーク経由で、GPS で取得した位置情報を送信したり、MAC アドレスをサーバーに転送するなど、PC の現在位置の特定をサポートします。PC が見つかった場合には、IT 部門の担当者はリモートからユニットを再有効化できます。

監視、修復、レポート

脅威が検出された場合に迅速な対応を行うため、第 3 世代インテル® Core™ vPro™ プロセッサー・ファミリーを搭載した PC では、自動監視、自動および手動によるリモート修復、レポートが可能となっています。IT 部門はこの内蔵機能により、リモートから迅速に脅威に対処できます。

自動的なネットワーク監視と脅威の検出

IT 管理者は、インバウンドおよびアウトバウンドのネットワーク・トラフィックを監視して、ウイルスや悪意のある攻撃を防ぐ防御フィルターをプログラミングできます。脅威が検出されると、管理サーバーに対して自動的に通知され、PC はネットワークから安全に切断されます。この時点でも、修復チャネルは開かれた状態にあるため、IT 部門はその PC にアクセスして修復を試みることができます。

連続的で自律的なエージェント・チェック

第 3 世代インテル® Core™ vPro™ プロセッサー・ファミリーを搭載したノートブック PC やデスクトップ PC は、管理コンソールからセキュリティー・エージェントの動作をチェックするのではなく、自律的に独自のセキュリティー・エージェント・チェックを定期実行するように設定できるため、不必要なネットワーク・トラフィックは発生しません。そして、セキュ

リティー・チェックが成功すると、結果はイベントログに記録されます。PC 自体が特定のタイプのマルウェアや悪意のある攻撃に対して独自に内部チェックを実行するため、余計なトラフィックによってネットワークに負担をかけることもありません。

エージェントがチェックインしないまま一定の時間を経過した場合は、エージェントが削除、改ざん、または無効化されたとみなされます、不揮発性メモリーにアラートが即座に記録されます。さらに、IT ポリシーに指定されている場合は、クライアントは管理コンソールにアクセスし、ネットワークから管理サーバーにアラートを送信します。

企業ネットワーク内外の PC からのアラートの受信

第 3 世代インテル® Core™ vPro™ プロセッサー・ファミリーを搭載した PC には、ポリシーベースの監視機能およびアラート機能が組み込まれています。すべてのアラートは、不揮発性メモリー上の保護されたイベントログに記録されます。IT 管理者は、受信対象とするアラートのタイプを指定できるため、重要性の低いアラートがネットワーク・トラフィックを圧迫することはありません。すべてのアラートが記録された状態でイベントログが保存され、ネットワークからリモートでアクセスできます。

このアラート機能により、システム上でコンプライアンス違反が発生すると、IT 管理者に自動的に通知されます。また、ハードウェアで障害が発生しそうな場合にも自動的に通知されるため、ユーザーが問題に気付く前、またはアプリケーションがフリーズする前に、IT 管理者が問題を把握できる確率が高まります。

自動化されたリモート運用管理機能によるコスト削減

業界の調査によると、一般的な企業で発生する PC 関連の問題のうち、オンサイトサポートやサービスセンターへの問い合わせが必要となる問題の割合はわずかですが、そのコストはサポート費用の大半を占めています。第 3 世代インテル® Core™ vPro™ プロセッサー・ファミリーを搭載した PC は、オンサイトサポートの件数を大幅に減らし、メンテナンス作業を自動化し、ポリシーに対するコンプライアンスを保証することにより、メンテナンス・コストを簡単に削減できます。内蔵されている運用管理機能によって、以下の操作を行うことができます。

- システムが応答しない場合でも、リモートから PC の設定、診断、隔離、修復が可能。
- 通常の業務時間の終了後、あるいは PC の電源がオフの場合でも、PC を自動的に起動させ、ソフトウェアおよびエージェントのアップデートが可能。
- ハードウェアおよびソフトウェアの自動的な資産管理。
- アプリケーションや OS の Windows* 7 への自動的なアップグレード。

IT 効率や TCO の削減に貢献するだけでなく、PC が常に健全な状態に保たれ、ユーザーのダウンタイムを減らすことができるので、生産性も向上します。

ソフトウェアの自動化および PC のコンプライアンス強化

主要なソフトウェア・ベンダーの多くは、第 3 世代インテル® Core™ vPro™ プロセッサー・ファミリーを搭載した PC 内の機能を自動化する管理コンソールを提供しています。例えば、管理コンソールが提供するソフトウェア・エージェントによって古いソフトウェアが検出された場合、ソフトウェア資産情報の収集、ネットワーク・ポートの一時的な遮断、システムのアップデートという一連の処理を、サードパーティー製の管理アプリケーションを利用して自動的に実行できます。もしくは、休日や夜間など、より適切なタイミングでアップデートするようスケジューリングすることもできます。処理が完了したら、管理アプリケーションは、リモートからシステムの電源を元の状態に戻すことができます。IT 部門が直接介入することなく、PC は常に健全な状態に保持され、企業ポリシーに基づくコンプライアンスが保証されます。

Microsoft* Windows PowerShell* 向けインテル® vPro™ テクノロジー・モジュールによる直接アクセス

IT スタッフは、コンソール経由で管理を行うだけでなく、管理コンソールでは利用できないスクリプトや自動化機能も独自に作成できます。Windows PowerShell* と Microsoft* Windows PowerShell* 向けインテル® vPro™ テクノロジー・モジュールを使用して、IT 部門の担当者は運用管理機能に直接アクセスし、必要とする独自の機能を作成できます。

より多くの問題をリモートから解決

第 3 世代インテル® Core™ vPro™ プロセッサー・ファミリーの以下のような機能により、IT 管理者はオンサイトサポートの件数を最大 56%[13] 削減することができます。

- **リモート起動およびブートイメージのリダイレクション：**リモートから PC を起動したり、問題のある PC のブートデバイスを管理コンソールのローカルストレージ上に存在するクリーンなイメージやヘルプデスクの CD、または別のリモートドライブ上のイメージなど、他のデバイスをブートイメージとしてリダイレクションできます。
- **Serial-Over-LAN（SOL）コンソール・リダイレクション：** OS の管理外でも、リモートからキーボードを使って PC を操作できるため、BIOS 設定の変更などの作業もユーザーの手を借りずにサービスセンターから行うことが可能となります。
- **リモート KVM 制御：**実際に PC の前にいるかのように PC を制御して、非常に複雑なソフトウェア障害もリモートから解決できます。

こうした機能によって、IT スタッフは以下の操作が可能となります。

- **資産情報にいつでもアクセス**して、不足または故障したハードウェア部品を特定したり、ソフトウェアのバージョン情報を確認する。
- BIOS の問題、ブルースクリーン、フリーズ、パッチ適用の失敗、ソフトウェアに関する重大な問題など、複雑な問題が発生した場合でも、ユーザーの手を借りずに**トラブルシューティング・セッションを実行する**。
- **システムをクリーンな状態にリブート**したり、PC のブートデバイスを診断用サーバーまたは修復用サーバー（あるいはその他のデバイス）にリダイレクションする。
- **BIOS、ドライバー、OS のロード状況を監視**して、ブートプロセスの問題を特定する。
- **BIOS 設定の更新、BIOS バージョンの確認、新しいバージョンの BIOS のプッシュ配信**により、PC の問題を解決する。
- **不揮発性メモリーに保存されたイベントログをアップロード**して、システムの故障前に発生した一連のイベント（温度の急上昇や不正なソフトウェアのダウンロードなど）を確認する。

- 不足したファイルや破損したファイル（.DLL ファイルなど）の新しいコピーをプッシュ配信して **OS を復旧する**。
- **OS の再ビルド**やハードディスク・ドライブ全体のイメージの再構築をリモートから実行する。
- **OS の移行やアプリケーションのアップグレード**、またはアップグレードの問題解決をリモートから実行する。
- **より効果的な電源管理**により、消費電力を抑えて電力コストを削減する。
- **完全な電源オフの状態から自動的に起動するようにスケジューリング**して、社員が出社したときにすぐシステムを利用できるようにする。

リモート KVM 制御

これまでは、高度な管理ツールを利用しても、トラブルチケットの約 20% では、ユーザーの手を借りる必要がありました。[16] たとえリモートからの運用管理機能が内蔵されていても、こうした複雑なトラブルは解決できず、IT スタッフがオンサイトでサポートを行ったり、ユーザーに操作をしてもらう必要がありました。ハードウェア・ベースのリモート KVM 制御によって、IT スタッフはヘルプデスクを離れることなく「あたかもユーザーのキーボードを背後から操作するような」ことが可能となり、その結果、複雑なソフトウェア問題の解決時間が約 20%[16] 短縮されることが報告されています。

ソフトウェア・ベースのリモート・デスクトップとは異なり、ハードウェア・ベースのリモート KVM 制御を利用すると、IT スタッフは PC の状態を確認し、PC がどのような状態であっても確実に制御できます。そのため、対象となる PC が企業ファイアウォールの外側にある場合でも、有線 / 無線接続された PC 上のソフトウェア障害を解決できます。

第 3 世代インテル® Core™ vPro™ プロセッサー・ファミリーを搭載した PC のリモート KVM 制御はユーザー同意コードの表示画面が 27 カ国の言語で提供され、ポートレート・モードとランドスケープ・モードで最大 3 台のモニター（最大 16 ビット・カラーの 1920 x 1200）をサポートしています。

重要なシステム情報へのリモートからのアクセス

第 3 世代インテル® Core™ vPro™ プロセッサー・ファミリーを搭載したビジネス PC は、起動時の BIOS 構成データ、ハードウェアおよびソフトウェアの管理データ、アラート、そのほか重要なシステム情報を不揮発性メモリーに格納することが可能です。こうしたデータは、システムが企業ファイアウォールの外側にある場合でも利用できます。これにより、IT 部門は、OS が動作していない場合、ハードディスク・ドライブが故障している場合、あるいは PC の電源がオフの場合でも、システム情報にリモートからアクセスして、トラブルシューティング、診断、修復を行うことができます。

企業ネットワークの内外からの安全な通信

ソフトウェア・ベースの管理アプリケーションは OS と同じ階層にインストールされるため、そのエージェント（常駐ソフト）は攻撃に対して無防備なままとなります。また、ネットワーク上で暗号化されていない状態で通信すると、運用管理トランザクションは無防備な状態となり、安全性は確保されません。第 3 世代インテル® Core™ vPro™ プロセッサー・ファミリーを搭載した PC は、アウトオブバンド（OOB）通信と、OS や他のソフトウェアの目の届かない、ハードウェアに組み込まれた強固なセキュリティー・テクノロジーを使用して、一連の運用管理の操作を保護し、その安全性を確保します。

OOB チャネルは、OS のネットワーク・スタックではなく、ファームウェアに組み込まれた特別な TCP/IP スタックを使用します。このチャネルは、OS、アプリケーション、またはハードディスク・ドライブに障害が発生した場合も含め、ほぼいつでも利用でき、重要なシステム通信（アラート送信など）や各種タスク（エージェント動作チェック、リモート起動、コンソール・リダイレクションなど）をより安全に続行できます。運用管理はハードウェア・ベースであるため、問題が発生した場合でも、IT 部門はビジネス・クライアント PC と通信を続け、PC をトラブルシューティングし、修復して、再起動できます。IT スタッフは、運用管理エージェントが見つからない場合でも、PC に内蔵された保護されているメモリー領域を読み取ることで、リモートから PC の資産情報を取得できます。

第 3 世代インテル® Core™ vPro™ プロセッサー・ファミリーを搭載した PC は、企業ファイアウォールの外側においても安全性が確保された経路を介してリモートの運用管理コンソールと通信を行います。このため、サテライトオフィス、あるいはオンサイトのプロキシーサーバーや管理アプライアンスを設置していない拠点（小規模なビジネス・クライアントのリモート拠点など）に設置された PC に対しても、IT スタッフは運用管理やメンテナンス作業を行うことが可能となります。その結果、オンサイトサポートの件数が減るため、IT 部門の効率性は向上し、TCO の削減につながります。

クライアント PC 主導の安全な接続により、IT 部門は以下の操作を行うことができます。

- **クライアントがコンソールに定期的にアクセスするタイミングをスケジューリングできます。** IT 部門は休日や夜間などでも、安全に PC をアップデートおよび保守できます。
- **リモート PC が自動的に起動するようにスケジューリングできます。** スケジューリングされたチェック作業や管理作業を実行した後、コンソールに接続して、新たなタスクやアップデートを行うことができます。
- **クライアントのキーボードのホットキーを設定できます。** ヘルプやシステム保守のために、ユーザーはホットキーを押すだけで PC を IT コンソールに迅速に接続できるので、ユーザーの不安が解消されるとともに、IT 部門は電話をかけることなく、遠隔地から簡単にサポートを提供できます。

IEEE 802.1x、Cisco* SDN、Microsoft* NAP 環境でも利用可能なアウトオブバンド管理

第 3 世代インテル® Core™ vPro™ プロセッサー・ファミリーを搭載した PC は、IEEE 802.1x、Cisco* SDN、または Microsoft* NAP を使用して、高度なネットワーク・セキュリティーをサポートしています。この機能により、IT 管理者は OOB アクセスを利用してメンテナンス、セキュリティー、管理、PXE などのタスクを実行しながら、アウトオブバンドの詳細なコンプライアンス・チェックなど高度なネットワーク・セキュリティーも維持できます。

コンプライアンスの保持

資産管理機能と不揮発性メモリーに格納された資産情報により、これまで長い時間を要していた手作業での資産管理が簡易化され、人件費が

大幅に削減されます。さらに、使われていないソフトウェア・ライセンスの他リソースへの割り当て、ハードウェア資産の有効活用、製品保証の適切な管理なども可能になります。同時に、企業にとって、監査結果が内部統制関連法規に違反する心配もなくなります。

生産性の維持

マルチメディアやビデオ会議の多用、データ暗号化の幅広い利用、デスクトップ・ベースの仮想化環境の登場、要求の厳しいアプリケーションなど、今日のビジネス環境には、ビジネス PC のプロセッサーにとって負荷となるさまざまな要因が存在します。第 3 世代インテル® Core™ vPro™ プロセッサー・ファミリーは、ビルトイン・ビジュアル機能やその他多くのインテル® テクノロジーを備えており、生産性および応答性の維持に役立ちます。

第 3 世代インテル® Core™ i5 vPro™ プロセッサーでは、以下のようにパフォーマンスと効率性が向上しています。

- インテル® AES-NI により暗号化 / 復号が最大 4 倍高速化。[14]
- より高いパフォーマンスが必要になったときにプロセッサーの動作速度を引き上げる、新しいインテル® ターボ・ブースト・テクノロジー 2.0 による適応性に優れたパフォーマンスの実現。[14]
- インテル® ハイパースレッディング・テクノロジーによりマルチタスク処理速度が最大 2 倍に向上。[14]
- ビジネス・アプリケーションの動作速度が最大 60% 向上。[14]

インテル® ターボ・ブースト・テクノロジー 2.0 による適応性の高いパフォーマンス

インテル® ターボ・ブースト・テクノロジー 2.0 [17] では、電力と温度の余裕を管理してパフォーマンスを最適化します。要求の厳しいアプリケーションには、より多くの処理能力がインテリジェントに割り当てられます。インテル® ターボ・ブースト・テクノロジー 2.0 は現在のワークロードとプロセッサーの動作状態を比較し、問題なければプロセッサー・コアの動作周波数を基本周波数から自動的に引き上げて高いパフォーマンスを実現します。

インテル® ハイパースレッディング・テクノロジーによるスマートなマルチタスク処理

インテル® ハイパースレッディング・テクノロジー [18] により、第 3 世代インテル® Core™ vPro™ プロセッサー・ファミリーは余剰リソースを使用して、より多くのタスク（2 コアの場合は最大 4 スレッド、4 コアの場合は最大 8 スレッド）を実行できます。ユーザーにとっては、異なるアプリケーション間の切り替えがシームレスに行われるため、生産性が向上します。

ビルトイン・ビジュアル機能で実現される驚異的なビジュアル・パフォーマンス

第 3 世代インテル® Core™ vPro™ プロセッサー・ファミリーにはビルトイン・ビジュアル機能 [19] が含まれています。これは、今日のビジネス PC に必要不可欠なマルチメディア処理、3D イメージ、メディア変換機能を備えたハードウェア・ベースのテクノロジーで、コラボレーションやデジタルコンテンツの作成、実行を支援します。このビルトイン・ビジュアル機能により、専用のグラフィックス・カードを別途用意する必要がなくなるため、カードの追加購入に伴うコストや電力要件も発生しません。

短時間で簡単に実行できるアクティベーション

第 3 世代インテル® Core™ vPro™ プロセッサー・ファミリーを搭載したビジネス・クライアント PC の内蔵テクノロジーは、セキュリティー、運用管理機能、省電力を可能にする、IT インフラストラクチャー全般におよぶ包括的なシステム・ソリューションを実現します。ただし、このソリューションの構成および導入についての解説は、本ホワイトペーパーの対象範囲外です。構成の詳細については、http://www.intel.com/go/scs/（英語）を参照してください。

ひとたび PC が導入されると、未動作状態にある運用管理機能やセキュリティー・サービスのアクティベーションは数分で完了します。インテル® セットアップ・コンフィグレーション・ソフトウェア 8.0 により、IT 部門の担当者は迅速にサービスを構成できるため、サードパーティー製のソリューションと合わせて利用することで、企業もユーザーも、内蔵セキュリティー機能、リモート管理、およびパフォーマンス向上の利点をすぐに手にすることが可能となります。運用管理機能およびセキュリティー・サービスの実装については、http://www.intel.co.jp/vpro/ を参照してください。

トップレベルのはっきりスマートなパフォーマンスでビジネスを支援

第 3 世代インテル® Core™ vPro™ プロセッサー・ファミリーは、シリーズ最高の内蔵セキュリティー、自動化されたリモート運用管理、コスト効率を実現します。このプロセッサー・ファミリーは、企業ファイアウォールの内外にある PC への常時可能なアクセス、強化されたリモート運用管理機能、ヘルプデスクを離れずに高度で複雑な問題も解決できるリモート制御など、最先端のセキュリティーを提供します。

第 3 世代インテル® Core™ vPro™ プロセッサー・ファミリー搭載 PC の導入によって、問題解決やソフトウェア・アップデートに関する IT サービスコストを大幅に削減できることが、すでに多くの事例で報告されています。業界別の具体的な事例については、インテルの Web サイト（http://www.intel.com/references/ecm/（英語））を参照してください。

最先端の内蔵セキュリティー機能、強力なリモート管理機能、はっきりスマートなパフォーマンスを備えた第 3 世代インテル® Core™ vPro™ プロセッサー・ファミリーは、俊敏性を必要とする企業にとって理想的なビジネス・クライアント PC の基盤となります。第 3 世代インテル® Core™ vPro™ プロセッサー・ファミリーを搭載したビジネス・クライアント PC の詳細については、http://www.intel.co.jp/vpro/ を参照してください。

[1] インテル® vPro™ テクノロジーは高度な機能であり、利用するにはセットアップと有効化を行う必要があります。利用できる機能と得られる結果は、ハードウェア、ソフトウェア、IT 環境のセットアップと構成によって異なります。詳細については、http://www.intel.com/technology/vpro/ (英語) を参照してください。

[2] すべての条件下で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。内蔵セキュリティー機能は、一部のインテル® Core™ プロセッサーで提供されているものであり、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。

[3] 絶対的なセキュリティーを提供できるシステムはありません。第 3 世代インテル® Core™ vPro™ プロセッサーと対応するオペレーティング・システムを搭載したインテル® OS ガード対応システムが必要です。詳細については、各システムメーカーにお問い合わせください。

[4] すべての条件下で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。インテル® トラステッド・エグゼキューション・テクノロジー (インテル® TXT) を利用するには、インテル® バーチャライゼーション・テクノロジー、インテル® TXT に対応したプロセッサー、チップセット、BIOS、Authenticated Code モジュール、インテル® TXT に対応した Measured Launched Environment (MLE) を搭載するコンピューター・システムが必要です。さらに、インテル® TXT を利用するには、システムが TPM v1.s を搭載している必要があります。詳細については、http://www.intel.com/technology/security/ (英語) を参照してください。

[5] インテル® バーチャライゼーション・テクノロジーを利用するには、同テクノロジーに対応したインテル® プロセッサー、BIOS、および仮想マシンモニター (VMM) を搭載したコンピューター・システムが必要です。機能性、性能もしくはその他の特長は、ご使用のハードウェアやソフトウェアの構成によって異なります。ご利用になる OS によっては、ソフトウェア・アプリケーションとの互換性がない場合があります。各 PC メーカーにお問い合わせください。詳細については、http://www.intel.com/go/virtualization/ (英語) を参照してください。

[6] すべての条件下で絶対的なセキュリティーを提供できるシステムはありません。インテル® アイデンティティー・プロテクション・テクノロジー (インテル® IPT) を利用するには、インテル® IPT に対応した第 2 世代または第 3 世代インテル® Core™ プロセッサーを搭載したシステム、および同テクノロジーに対応したチップセット、ファームウェア、ソフトウェア、インテル® IPT に対応した Web サイトが必要です。各システムメーカーにお問い合わせください。データやシステムの紛失や盗難など、サービス利用の結果生じたいかなる損害に対してもインテルは責任を負いません。詳細については、http://ipt.intel.com/ (英語) を参照してください。

[7] インテル® AES New Instructions (インテル® AES-NI) を利用するには、インテル® AES-NI に対応したプロセッサーを搭載したコンピューター・システム、および命令を正しい手順で実行する他社製ソフトウェアが必要です。インテル® AES-NI は、一部のインテル® Core™ プロセッサーで利用できます。提供状況については、各 PC メーカーなどにお問い合わせください。詳細については、http://software.intel.com/en-us/articles/intel-advanced-encryption-standard-instructions-aes-ni/ (英語) を参照してください。

[8] 絶対的なセキュリティーを提供できるシステムはありません。第 3 世代インテル® Core™ vPro™ プロセッサーとインテル® セキュアキーをサポートするために最適なソフトウェアを搭載したインテル® セキュアキー対応 PC が必要です。詳細については、各システムメーカーにお問い合わせください。

[9] すべての条件下で絶対的なセキュリティーを提供できるシステムはありません。インテル® アンチセフト・テクノロジーを利用するには、同テクノロジーに対応したチップセット、BIOS、ファームウェア、ソフトウェアを搭載したシステムと、同テクノロジーに対応したサービス・プロバイダーのサービスへの加入が必要です。対応状況と機能については、各システムメーカーとサービス・プロバイダーにお問い合わせください。データやシステムの紛失や盗難など、サービス利用の結果生じたいかなる損害に対してもインテルは責任を負いません。詳細については、http://www.intel.com/go/anti-theft/ (英語) を参照してください。

[10] 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) によって可能となるセキュリティー機能は、インテル® AMT に対応したチップセット、ネットワーク・ハードウェア、ソフトウェア、および企業 LAN へ接続されていることが必要です。ホスト OS ベースの VPN 上や、ワイヤレス接続時、バッテリー駆動時、スリープ時、ハイバネーション時、電源切断時には、インテル® AMT を利用できないことや、一部の機能が制限されることがあります。セットアップには構成が必要となり、管理コンソールへのスクリプトや既存のセキュリティー・フレームワークへの統合、新しいビジネスプロセスの変更や導入を必要とする場合もあります。詳細については、http://www.intel.co.jp/amt/ を参照してください。

[11] リモート KVM (キーボード、ビデオ、マウス) 制御を利用できるのは、インテル® Core™ i5 vPro™ プロセッサーおよびインテル® Core™ i7 vPro™ プロセッサーでプロセッサー・グラフィックスを有効にした場合のみです。ディスクリート・グラフィックスはサポートされません。

[12] システム上で Client Initiated Remote Access (CIRA) を利用するには、有線または無線 LAN に接続する必要があります。この機能は、公衆無線 LAN スポットや、接続に「click to accept (クリックによる同意)」が必要な場所では利用できない場合があります。

[13] 結果は、インテルの依頼で LeGrand と Salamasick の第三者監査が実施した、さまざまな企業 IT 環境に対するインテル® Centrino® Pro プロセッサー・テクノロジーの 2007 EDS ケーススタディーとインテル® vPro™ テクノロジーの 2007 EDS ケーススタディー、およびインテルの依頼で作成された Wipro Technologies の調査レポート『The Benefits of Intel® Centrino® Pro Processor Technology in the Enterprise』(2007) からのものです。EDS のケーススタディーでは、インテル® vPro™ テクノロジーを搭載した PC のテスト環境とインテル® vPro™ テクノロジー非搭載の環境を比較しています。PC は一般的なビジネス環境を反映してさまざまな OS や電力ステートでテストを行っています。Wipro の調査では、インテル® vPro™ テクノロジーを導入した場合に予測される ROI (費用対効果) のモデリングを行っています。実際の結果は異なる場合があり、より小規模な企業で得られる結果は反映されていない場合があります。これらの調査結果については、http://www.intel.co.jp/jp/gopro/、http://www.eds.com/ (英語)、http://www.wipro.com/japanese/ を参照してください。

[14] クロス・クライアントに関する記述は、デスクトップとモバイルのベンチマークのうち、値の低い方のパフォーマンス・データに基づいています。それぞれの構成とパフォーマンス・テストの内容は以下のとおりです。

ノートブック PC : 出荷前のインテル® Core™ i5-2410M プロセッサー (2 コア 4 スレッド、2.30GHz、3MB キャッシュ)、インテル® Emerald Lake CRB、4GB (2x2GB) PC3-10700 (DDR3-1333)-CL9、Hitachi* Travelstar 320GB HDD、インテル® HD グラフィックス 3000、ドライバー : 2185 (BIOS : v.34、インテル v.9.2.0.1009)、Microsoft* Windows* 7 Ultimate RTM 64 ビット版と、インテル® Core™2 Duo プロセッサー T7250 (2MB キャッシュ、2GHz、800MHz FSB)、Intel Silver Cascade Fab2 CRB、Micron* 4GB (2x2GB) PC3-8500F (DDR3-1066)-400、Hitachi* 320GB HDD、モバイル インテル® 4 シリーズ Express チップセット・ファミリー w/ 8.15.10.2182 (BIOS : American Megatrends AMVACRB1.86C.0104.B00.0907270557, 9.1.2.1008) を比較。

デスクトップ PC : 出荷前のインテル® Core™ i5-2400 プロセッサー (4 コア 4 スレッド、3.10GHz、6MB キャッシュ)、インテル® Los Lunas CRB、Micron* 4GB (2x2GB) PC3-10700 (DDR3-1333)-CL9、Seagate* 1TB、インテル® HD グラフィックス 2000、ドライバー : 2185 (BIOS : v.35、インテル v.9.2.0.1009)、Microsoft* Windows* 7 Ultimate RTM 64 ビット版と、インテル® Core™2 Duo プロセッサー E6550 (2 コア 2 スレッド、2.33GHz、4MB キャッシュ)、インテル® DG945GCL マザーボード、Micron* 2GB (2x1GB) DDR2 667MHz、Seagate* 320GB HDD、インテル® GMA 950、ドライバー : 7.14.10.1329、(BIOS : CL94510J.86A.0034、INF: 9.0.0.1011)、Microsoft* Windows* 7 Ultimate RTM 64 ビット版を比較。

ビジネス生産性に関する記述は SYSmark* 2007 に基づくものです。SYSmark* 2007 は、一般的なオフィスにおける生産性とインターネット・コンテンツ制作に照準を合わせたベンチマーク・ツールの最新版であり、ビジネス・クライアント PC の性能評価に利用されています。また、アプリケーションの専門家が開発したユーザー主導のワークロードと利用モデルを特色としています。マルチタスクに関する記述は PCMark* Vantage* に基づくものです。Windows* 7 または Windows Vista* 搭載 PC のハードウェア性能ベンチマークである PCMark* Vantage* は、各種のシングルスレッド / マルチスレッド CPU テスト、グラフィックス・テスト、HDD テストを集約したもので、Windows* 用アプリケーションのテストに重点を置いています。セキュリティー・ワークロードは、SiSoftware Sandra 2010 - AES256 で構成されます。CPU Cryptographic サブテストは、AES (Advanced Encryption Standard) の暗号化 / 復号アルゴリズムを実行中の CPU のパフォーマンスを測定します。詳細については、http://www.intel.com/performance/ (英語) を参照してください。

性能に関するテストに使用されるソフトウェアとワークロードは、性能がインテル® マイクロプロセッサー用に最適化されていることがあります。SYSmark* や MobileMark* などの性能テストは、特定のコンピューター・システム、コンポーネント、ソフトウェア、操作、機能に基づいて行ったものです。結果はこれらの要因によって異なります。製品の購入を検討される場合は、他の製品と組み合わせた場合の本製品の性能など、ほかの情報や性能テストも参考にして、パフォーマンスを総合的に評価することをお勧めします。詳細については、http://www.intel.com/performance/ (英語) を参照してください。

[15] 出典 : プリマス大学による ROI 分析 (http://communities.intel.com/docs/DOC-2020/ (英語))。インテルの依頼による調査。

[16] 出典 : 『Quantifying the Benefits of Intel KVM』 - Wipro、2009 年 11 月 (http://communities.intel.com/docs/DOC-3144/ (英語))。インテルの依頼による調査。

[17] インテル® ターボ・ブースト・テクノロジーに対応したシステムが必要です。インテル® ターボ・ブースト・テクノロジー 2.0 は次世代のインテル® ターボ・ブースト・テクノロジーであり、第 3 世代インテル® Core™ プロセッサーでのみ利用可能です。各 PC メーカーにお問い合わせください。実際の性能はハードウェア、ソフトウェア、システム構成によって異なります。詳細については、http://www.intel.co.jp/content/www/jp/ja/architecture-and-technology/turbo-boost/turbo-boost-technology.html を参照してください。

[18] インテル® ハイパースレッディング・テクノロジー (インテル ® HT テクノロジー) に対応したシステムが必要です。詳細については、各 PC メーカーにお問い合わせください。性能は、使用するハードウェアやソフトウェアによって異なります。インテル® HT テクノロジーは、一部のインテル® Core™ プロセッサーでは利用できません。詳細については、http://www.intel.co.jp/jp/products/ht/hyperthreading_more.htm を参照してください。

[19] 第 3 世代インテル® Core™ プロセッサー・ファミリーで利用可能です。インテル® HD グラフィックス、インテル® クイック・シンク・ビデオ、インテル® クリアー・ビデオ HD テクノロジー、インテル® InTru™ 3D テクノロジー、およびインテル® アドバンスト・ベクトル・エクステンションで構成されます。オプションにより、インテル® ワイヤレス・ディスプレイも含まれます (システム上で有効にされている場合)。ビルトイン・ビジュアルの利点が得られるかは、お選びの PC の設計によって決まります。ご使用のシステム上でビルトイン・ビジュアルが有効になっているかは、各 PC メーカーにお問い合わせください。ビルトイン・ビジュアルの詳細については、http://www.intel.com/jp/technology/visualtechnology/ を参照してください。

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/

2012 年 7 月

324823-002JA
JPN/1207/PDF/SE/MKTG/YM