安全で
コンプライアンスに
準拠した
クラウドへの道のり

安全でコンプライアンスに準拠したクラウドへの道のり

インテル、IBM Cloud SoftLayer*、VMware*、HyTrust* が提供するソリューション・スタックを活用し、信頼できるインフラストラクチャーを構築

テクノロジー・イノベーションは、企業の運用形態ばかりか、従業員の働き方も変革します。変革プロセスにおいて、企業はコラボレーション・パートナーとしての IT 部門に依存しています。

統合ソリューション：俊敏性、柔軟性、信頼性、コンプライアンス

企業は、かつてないほど厳しい競争に直面しています。革新的なビジネスモデルが市場を席捲し、大企業でさえも事業のやり方を変えざるを得ない状況です。企業はイノベーションを進めて競争上の優位に立ち、新しいサービスを提供して新規顧客を引きつけ保持し、運営コストをできる限り低く抑える必要があります。

企業が掲げる目標の中心には、ビジネスプロセスと知的財産、すなわちワークロードとデータが据えられています。こうしたワークロードとデータのセキュリティーおよびコンプライアンスを実現するインフラストラクチャーが、仮想クラウドです。よく考えて設計された仮想クラウドは、ワークロードとデータとして利用可能なリソースに関して、意思決定者に優れた俊敏性を提供します。その結果、新しいサービスとビジネスモデルの迅速な展開を繰り返すことで、イノベーションの機会が生まれます。また、IT 部門は運用効率を高め、一方で企業に求められるパフォーマンス、コスト、柔軟性の要件も満たすことができます。

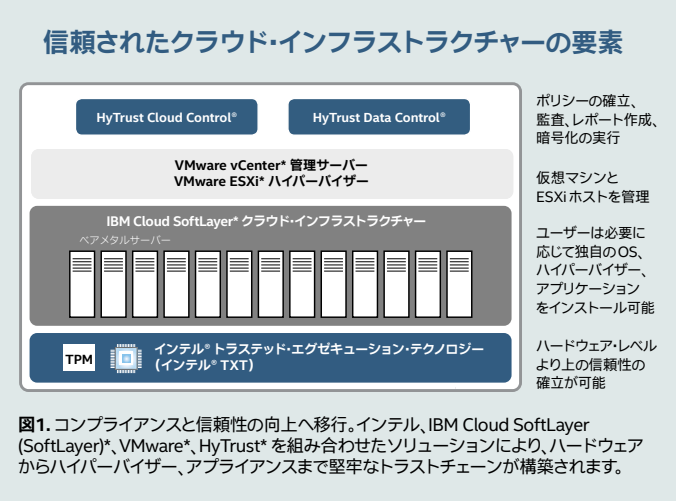

図1. コンプライアンスと信頼性の向上へ移行。インテル、IBM Cloud SoftLayer (SoftLayer)*、VMware*、HyTrust* を組み合わせたソリューションにより、ハードウェアからハイパーバイザー、アプライアンスまで堅牢なトラストチェーンが構築されます。

仮想クラウドの新しい課題

仮想化の利点には、セキュリティーおよびコンプライアンスに関する新たな課題と独自のリスクも伴います。例えば、仮想クラウドでは、設定や場所さえ認証されていないホスト間で、ワークロードとデータの移行ができてしまいます。

機密情報のセキュリティー侵害は、ビジネスに壊滅的な打撃を与え、訴訟問題に発展しかねません。データ漏えいが発生すると、IT部門はできる限り迅速に漏えい元を特定し、事態の解決を図る全責任を負います。ところが、従来のITソリューションでは、自動的に仮想化の課題を管理、解決したり、現代のリスクに対して効率的に保護したりすることはできません。したがって、企業は、他の規則や規制に対して社内セキュリティーとコンプライアンスを保証する新しく堅牢なソリューションを導入して、仮想クラウドを構築する必要があります。

データ・プライバシー、地理的位置（データ保存場所）、バウンダリー・コントロール、ジオフェンシング（仮想的な地理的境界）、インテリジェント復号などのユースケースで、企業はハードウェアからハイパーバイザーまで、あらゆるマネージドシステムで信頼することのできるソリューションの探求に躍起になっています。

信頼できるソリューションの内幕

信頼性とコンプライアンスを保証してサービスを提供するには、適切なアーキテクチャーをベースに仮想クラウドを構築する必要があります。この重要な課題を解決するため、インテル、IBM Cloud SoftLayer（SoftLayer）、VMware、HyTrustが統合されました。その結果、広範囲に及ぶコラボレーションによって、信頼されたプロセッサー・プールなどの最新のコンセプトと優れた新しいユースケースを実現するソリューション・スタックが生まれました。IT部門や企業のリーダーたちは、信頼性と安全性が高く、コンプライアンスに準拠したインフラストラクチャーを構築し、同時に仮想化とクラウドのメリットを最大限に活用できるようになりました。この信頼できるクラウド・アーキテクチャーは、次のものをベースに構築されています。

- インテル® Xeon® プロセッサー
- 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）
- トラステッド・プラットフォーム・モジュール（TPM）1.2
- インテル® AES New Instructions（インテル® AES-NI）
- IBM Cloud SoftLayer（SoftLayer）* ベアメタルサーバー
- VMware vCenter* 管理サーバー
- VMware ESXi* ハイパーバイザー（仮想OS）
- HyTrust CloudControl（HTCC）*
- HyTrust DataControl（HTDC）*

SoftLayerベアメタルサーバーとインテル® TXTおよびTPMを注文すると、SoftLayerは自動的に初期設定を実行し、サーバーのプロビジョニングを開始します。これにより、展開環境に合わせて信頼できるテクノロジーに対応した設定が可能になります。設定が完了すると、インテル® TXTは常時「オン」状態になり、各サーバーに信頼のルートを自動的に提供します。

ハードウェアに加え、HyTrustとVMwareソリューションがセキュリティー管理を一元化し、IT管理とデータの可視化を強化します。最初に、VMwareがVMware vCenter管理サーバーとVMware ESXiハイパーバイザー（OS）によってクラウドの仮想レイヤーを提供します。VMwareが提供するのは、強力かつ全体的な仮想化機能と、シンプルな統合ハイパーバイザー管理機能です。多くの企業がすでにVMwareによる仮想化を採用し、クラウド環境を管理しているため、HyTrustは既存のVMwareインフラストラクチャーへとシンプルに統合されます。

HyTrustは、仮想クラウドの管理をポリシーに基づいて自動化します。この管理レイヤーは、HyTrust CloudControl（HTCC）およびHyTrust DataControl（HTDC）コンポーネントから構成されます。HTCCにより、IT部門は構成設定をカスタマイズし、ポリシーを設定して、内外の脅威からの仮想化環境の保護をより強固なものにすることができます。これには、仮想管理者用の認証オプションの設定、VMware vCenter Server* およびホストの管理、管理およびセキュリティー・ポリシーの確立が含まれます。HTCCはポリシーを実行し、仮想データセンターにおいて試行、却下、または承認された管理者の行動を克明に記録した詳細ログも取り込みます。これにより、厳密な監査およびコンプライアンス要件を効率よく遵守し、できる限り迅速にセキュリティー脅威を抑止できるようになります。

VMware機能には、インテル® TXT、TPM 1.2、HTCC、HTDC用の直接統合サポートが含まれます。また、HTCCおよびHTDCには、インテル® TXT、TPM、VMwareソリューション用の直接統合サポートが含まれます。HTCCは、管理しやすいようにVMware vCenterに統合されました。HTCCは、仮想クラウド・インフラストラクチャーと仮想マシン管理者の中間に位置する機能です。仮想マシン管理者リクエストが送信されると、HTCCはそのリクエストがセキュリティー・ポリシーに準拠しているかどうかを判定し、その結果に応じてリクエストを許可または却下します（図2を参照）。また、HTCCは、アクションに追加承認が必要かどうかも判定できます（「Four Eyes Principle（複数人による確認原則）」など）。

なお、すべてのリクエストをログに記録することで、HTCCは監査、トラブルシューティング、分析に利用可能なフォレンジック品質の詳細な記録を作成します。このソリューション・スタックでは、HTCCが信頼に基づいたログサポート、Active Directoryサービス、仮想インフラストラクチャー・セグメンテーション、ハイパーバイザー強化、マルチテナント型ポリシー実行を担当します。

HyTrustの2つ目のコンポーネントであるHTDCは、堅牢かつ柔軟性に富んだデータ・セキュリティーおよび暗号化/復号ソリューションです。HTDCにより、IT部門は軍事レベルの暗号化のほか、扱いやすく拡張可能なキー管理も実行できます（Hytrust暗号化およびキー管理はNIST FIPS 140-2認定を受けています）。HTDCキー管理は、暗号化ポリシーの一元管理を自動化します。仮想マシン内にHTDCエージェントがインストールされるため、暗号化状態も物理ホスト間で仮想マシンとともに移動します。これにより、ワークロードはあらゆるオンプレミスまたはクラウド・プラットフォームで確実に暗号化されます。また、独特なキー管理機能により、データ所有者はキーの全所有権を保持できますが、これはクラウドに欠かせない機能です。

HyTrustには、インテル® AES New Instructions（インテル® AES-NI）用の直接統合サポートが含まれます。インテル® AES-NIは、パフォーマンス・オーバーヘッドがほぼゼロのままより迅速かつ効率的なスマート暗号化を可能にするため、インテル® Xeon® プロセッサーに統合されています。HyTrustは、プロセッサー内のインテル® AES-NIを自動的に検出し、それを最大限に活用してHyTrust暗号化、復号、再キー発行プロセスを強化します。企業は、最重要機密以外にも、すべてのワークロードとデータを暗号化し、保護できるようになりました。

仮想インフラストラクチャーにおける信頼性の重要さ

インフラストラクチャーに信頼を置くためには、ホスト、データストア、ハイパーバイザー、ガバナンスを信頼できるようになる必要があります。つまり、ホストは期待どおりの場所にあり、設定は認証されていることを把握することが肝要です。これは、機密性の高いワークロードとデータは、信頼されたホストでのみ実行され、適切な場所にある信頼されたホスト間でのみ転送されること。仮想データストアの復号は、ワークロードとそのデータを保持するホストも信頼され、そのデータを処理する認証を受けている場合にのみ許可されること。そして、管理者は認証されたアクションのみを実行し、クラウドで要求または実行されたアクションは、計画的であれ、事故であれ、不正によって起こされたものであれ、すべてログに記録されるという状況を把握することも意味します。信頼できるクラウド・ソリューションのカギを握るのは、信頼のルート、そしてそれが可能にするユースケースです。

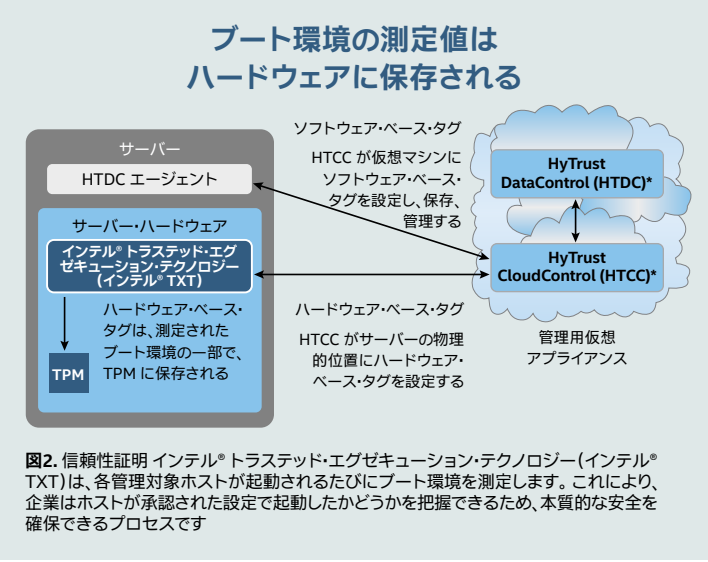

図2. 信頼性証明 インテル® トラステッド・エグゼキューション・テクノロジー（インテル® TXT）は、各管理対象ホストが起動されるたびにブート環境を測定します。これにより、企業はホストが承認された設定で起動したかどうかを把握できるため、本質的な安全を確保できるプロセスです

信頼のルート（Root of Trust）

現在のセキュリティーおよび規制要件を遵守するには、仮想クラウドに信頼のルートが必要です。これはハードウェアをベースとし、インテル® TXTおよびTPMによって実現します。信頼できるクラウドでは、サーバーが起動するたびにインテル® TXTがブート環境を測定します。BIOS、OS、ハイパーバイザー、VMkernel*、読み込まれたモジュールセット（VMware vSphere* インストール・バンドル（VIB））など、すべてのブート環境要素が測定されます。各測定値は、本質的に安全なプロセスでTPMに保存されます。

トラストチェーンがHyTrustによって拡張され、信頼性証明サービス（Trust Attestation Service：TAS）が実行されます。HyTrustは、TPM内の測定値をTASに保存されたホワイトリストと比較します。ホストのブート測定値がTASホワイトリストの測定値と一致する場合、HyTrustはそのホストに信頼済みのラベルを付けます。基本的に、ホストが起動して認証済みと認識されている設定で実行されると、そのホストは信頼済みとみなされます。それ以外の場合は、HyTrustはそのホストを信頼できないものとしてラベルを付けます。HyTrustは、ホストの信頼状態を参照し、ワークロードおよびデータの移行、管理、復号用にIT部門が定義したポリシーを実行します。例えば、IT部門のポリシーは、信頼できないホストをメンテナンスのため排除し、下位レベルのアプリケーションのみの実行許可を出すなどの指定が可能です。

信頼性が実現するパワフルなユースケース

信頼されたプロセッサー・プール: インテル® TXT および HyTrust は連動し、ホストが信頼、認証された設定で起動するかどうかを検証します。これが、インテル® TXT および TPM によって実現される信頼性証明プロセスです。IT 部門は、どのホストが信頼できるかを把握した後、HyTrust を使用して対象ホストを信頼されたプロセッサー・プールとしてグループ化できます。これは、コンプライアンスに準拠した仮想クラウド管理の最新コンセプトの 1 つです。信頼性に基づいたプロセッサー・プールにより、IT 部門はワークロード、機密データ、クラウドリソースに関するさまざまなビジネス、セキュリティー、コンプライアンス要件を満たすことが可能になります。例えば、機密性の高いワークロードは、特定の信頼されたグループ内にある、特定の信頼されたサーバーのみで実行されるように、IT 部門はインテリジェント・ポリシーをワークロードに適用することができます。商品アプリケーションのワークロードは、より標準的に安全が確保された、他のホストに割り当てることができます。信頼されたプロセッサー・プールは、企業に動的クラウド環境のメリットをもたらし、機密性の高い重要なワークロードには高レベルの保護を実行します。

正確なデータ・ロケーション: データ・ロケーションとは、ホストの実際の物理的な位置を把握することです。信頼性証明とハードウェア・ベースのポリシータグにより、IT 部門は仮想クラウド全体の実際のサーバー位置を可視化できるようになりました。ハードウェア・ベースのポリシータグとは、場所、機能、コンプライアンス要件、その他の論理識別子を基準として、ホストに「タグ」を付けることを可能にする HyTrust 記述子です。ハードウェアに基づく記述子であるため、ホストのブート環境に含まれ、ホストが起動するたびにインテル® TXT によって測定されます。サーバーは起動するたびに、設定だけではなく、実際の物理的位置も検証できるようになります。

検証後のバウンダリー・コントロール: バウンダリー・コントロールは、ワークロードやデータが特定の境界内だけで実行されるように制限する機能です。この場合の境界とは、国境などの地理的境界を指しますが、論理的なグループ、機能、コンプライアンス・ファクターに基づいた境界などの論理的境界を同時に指すこともできます。バウンダリー・コントロールは、ソフトウェア・ベース・タグ、またはインテル® TXT、ハードウェア・ベース・タグ、HyTrusによる堅牢性の高いセキュリティー・オプションを利用して実行できます。IT 部門が各ホストの実際の物理的位置を把握すると、HyTrust ポリシーを適用してデータおよびワークロードを認証された場所のみに制限し、各制限についてエビデンスに基づいたレポートを作成できます。

追加ジオフェンシング: ジオフェンシングは、信頼されたプロセッサー・プール内のワークロードを分離する機能です。例えば、信頼されたプロセッサー・プールとバウンダリー・コントロールを活用すると、特定の地域内の信頼されたサーバーだけをグループ化できます。次に、ジオフェンシングを使用し、そのプール内のワークロード・タイプを分離できます(会計ワークロードを監査ワークロードから隔離するなど)。信頼されたプロセッサー・プール内でサーバーをグループ化できるジオフェンシングにより、管理の精度を上げることができます。

ジオフェンシング:信頼されたプール内の特定のサーバーにワークロードを制限

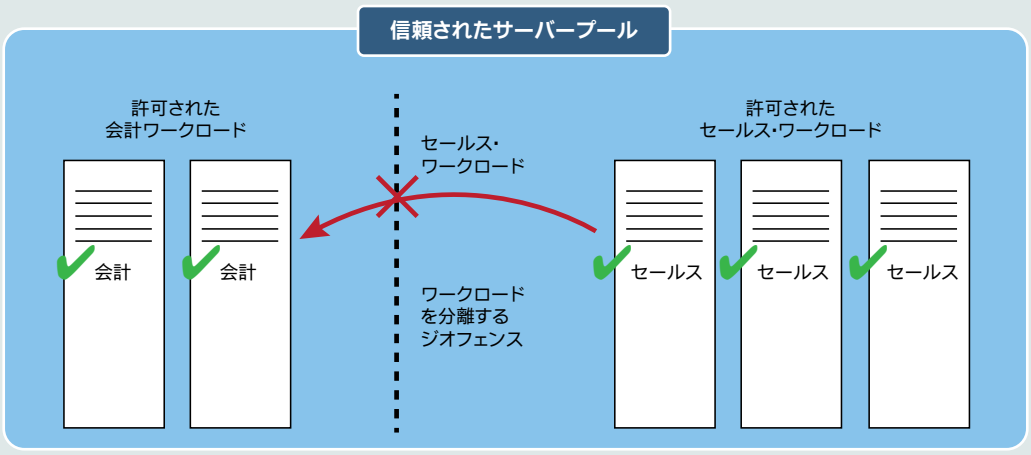

図3. 信頼性証明などの機能を活用することで、信頼されたプロセッサー・プール、バウンダリー・コントロール、ジオフェンシングでは、信頼された正式なサーバーのみでデータとワークロードが確実に処理されます。

迅速なスマート復号：インテル、SoftLayer、VMware、HyTrustのソリューション・スタックを利用すると、IT部門は復号の実行場所を信頼された場所にある認証されたサーバーに限定できます。例えば、従来のクラウドでは、仮想ワークロードを外部ドライブに読み込み、信頼されていないホストに移動して復号することができます。対照的に、信頼できるクラウドでは、暗号化を仮想マシン本体に関連付け、仮想マシンとともに移動させることができます。ワークロードが信頼できないホストに移動されても、認証がなければ復号はできません。また、信頼性証明とデータ・ロケーションを活用し、HyTrustポリシーを実行すると、物理的に認証された場所に位置する認証されたホストに対してのみ、復号リクエストを承認できます。

エビデンスベースのコンプライアンス：一般的に、規制要件においては、データ損失やデータ漏えいなどのリスクを軽減するため、データ保護が義務付けられています。また、コンプライアンスでも、データの場所と移動に関する管理と、データのアクセスおよび使用に関するエビデンスに基づいた監査の実施が義務付けられています。このソリューション・スタックでは、インテル® TXTおよびHyTrustを活用することで、管理者は仮想ワークロード・レベルで統一されたインテリジェント・ポリシーを設定、適用し、すべての仮想化アクティビティーを可視化し、ログに記録することができます。克明なログ記録により、セキュリティー分析に不可欠な詳細情報を参照して、特権を持つ管理者のアクションを確認することができます。また、HyTrustは、IT部門がエビデンスに基づいた監査や報告を実施し、必要に応じてフォレンジックに使用可能なレベルの詳細な分析を実施できるように、管理者のアクションを個別のログに記録します。

まとめ

インテル、SoftLayer、VMware、HyTrustにより信頼性が証明されると、信頼されたプロセッサー・プール、ハードウェア・ベースのポリシータグ、データ・ロケーション、バウンダリー・コントロール、ジオフェンシング、ポリシーベースの復号など、最新の優れたコンセプトやユースケースを実現できます。こうした堅牢なソリューション・スタックを活用することで、管理者は、仮想ワークロード・レベルにおいて統一された信頼性に基づくポリシーを設定、適用、実行できます。信頼性証明により、IT部門は、機密性の高いワークロードの処理を認証された場所の認証されたサーバーに限定できるように、仮想インフラストラクチャー全体の物理的サーバーを可視化できます。信頼性に基づき、IT部門は認証された管理者アクションのみを適切に実行し、承認/却下に関係なく、要求されたすべてのアクションを正確にログに記録して、レポートやコンプライアンス向けに利用することが可能となります。

IT部門がどのホストを信頼できるかを把握すると、より効率的にリスクを低減し、セキュリティーを高めることができます。インテル、SoftLayer、VMware、HyTrustのソリューション・スタックを活用すると、信頼できるクラウド・インフラストラクチャーを構築し、社内のセキュリティー要件はもちろん、ミッション・クリティカルなビジネス・オペレーションに関するコンプライアンス要件にも対処しやすくなります。IT部門や企業のリーダーたちは、ビジネスを守るために必要な最高レベルのデータ保護、可視化、監査を維持しつつ、クラウド・コンピューティングの利点を最大限に活用することができるようになります。

このソリューションおよびSoftLayerでの展開方法の詳細は、以下を参照してください。
https://knowledgelayer.softlayer.com/learning/intel-trusted-execution-technology-txt/