

Google Cloud Platform 向け タレス ソリューション



Google Cloud Platformを含む ハイブリッドクラウド全体の ワークロードを保護

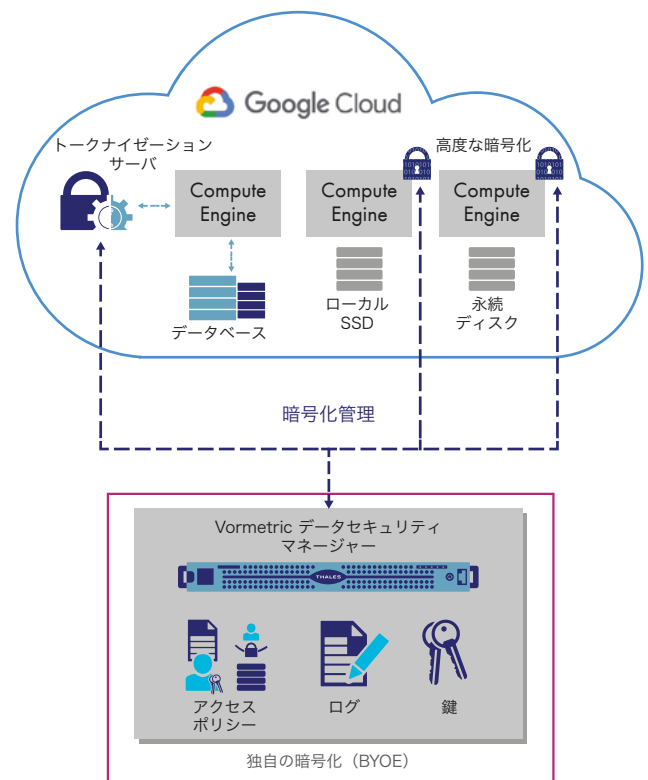
Google Cloud Platform (GCP) の情報技術ワークロードを活用すると、利便性が高まり、コストを削減することができます。ただし、データを保護するためには、セキュリティ、プライバシー、コンプライアンスに関するルールやベストプラクティスに準拠する必要があります。また、現在使用しているすべてのクラウド間、および将来使用するすべてのクラウド間で、高速なデータモビリティが必要となりますが、クラウドベンダー固有の暗号化ソリューションでは十分に対応できない場合があります。

包括的な鍵管理機能を備えた 高度な暗号化ソリューション

クラウドを効果的かつセキュアに使用するには、クラウド内で機密データを使用するかどうかなど、次々と重要な決断を下さなければなりません。タレスであれば、デジタルトランスフォーメーションをセキュアに進めることができます。タレスの高度な暗号化ソリューションと一元的鍵管理ソリューションを活用することで、オンプレミスや、Google Cloud Platform、その他各種クラウドプロバイダー内に保存しているデータを保護し、管理できるようになります。タレスのテクノロジーは、以下のようなメリットをもたらします。

- 暗号化をクラウドベンダーに依存しないことで必要なデータモビリティを確保しつつ、独自の一元的暗号化管理により、Google Cloud Platform を含むさまざまなクラウドベンダー全体に、ワークロードやデータを効率的かつセキュアに展開することができます。

- 業界最先端の SIEM アプリケーションに対応したデータアクセスログ機能により、攻撃を迅速に検出できます。
- 特権ユーザーアクセス制御を含む高度な暗号化により、クレデンシャルの悪用から生じるリスクを軽減できます。
- ボルトレストークナイゼーションと動的なデータマスキングにより、クラウドおよび PCI-DSS のいずれにも対応したアプリケーションを設計できます。



お客様のプライベートクラウド

Google Cloud Platformや各種サービスのワークロードに対応するデータ暗号化

全面的に Google Cloud Platform ベースで厳格なデータセキュリティ管理を行っている場合でも、オンプレミスのプライベートクラウドや、複数のクラウドプロバイダー、Google Cloud Platform を横断してデータが分散しているハイブリッドクラウドを運用している場合でも、高度な暗号化ソリューションが必要です。Google Cloud Platform はデフォルトで保存データを暗号化しますが、暗号化されていないデータをオペレーティングシステムに提供するため、OS レベルでデータのリスクが発生します。タレスの Vormetric 透過暗号 (VTE) は、ファイルやデータベースが Google Cloud Platform にある場合でも、それ以外の場所にある場合でも、すべて保護します。既存のアプリケーションやデータベース、インフラストラクチャ、ビジネスプロセスを変更する必要はありません。

Vormetric 透過暗号 (VTE) :

- ユーザー ID (root 権限管理者を含む) やプロセスなど、多くのきめ細かいアクセスポリシーに基づいて、オペレーティングシステムレベルで不正アクセスを制御することで、データセキュリティを強化します。
- 詳細なファイルアクセスログにより、セキュリティ侵害を迅速に検出し、コンプライアンス要件に対応します。ログは、セキュリティ情報 / イベント管理 (SIEM) システムに送ることができます。
- 既存環境の変更を必要としない柔軟な実装により、迅速な投資収益化を実現します。暗号化エージェントは、Google Compute Engine 上や、ストレージにアクセスする各種サーバ上で動作し、さまざまな Windows バージョンや Linux ディストリビューションで使用できます。

PCI-DSSコンプライアンスを促進

Google Cloud Platform に対応する Vormetric トークナイゼーションと動的データマスキング (VTS) は、データセンター、ビッグデータ環境、クラウド内の機密資産を保護し、匿名化することで、PCI-DSS コンプライアンスをシンプルにします。フォーマット維持トークン化やランダムトークン化により、データベース構造を維持しながら機密フィールドを保護し、システム中断を引き起こさない実装を実現します。そのため、ポリシーベースの動的データマスキング機能を簡単にアプリケーションに追加することができます。

セキュアな一元的鍵管理

Vormetric データセキュリティマネージャー (DSM) は、Vormetric 透過暗号や Vormetric トークナイゼーションサーバの鍵、ポリシー、ログを一元管理します。Vormetric データセキュリティマネージャー (DSM) は、FIPS140-2 Level2 または Level3 に準拠した物理アプライアンスとして、あるいは FIPS140-2 Level1 に準拠した仮想アプライアンスとして利用できます。物理アプライアンスはオンプレミスに適しており、Google Compute Engine インスタンス仮想マシンなどにインストールした暗号化エージェントを管理できます。仮想アプライアンスは、VMware、KVM、Amazon Web Services、Microsoft Azure など、さまざまな仮想化フォーマットで利用できます。

データ保護要件に対応するセキュリティ

タレスは、Google Cloud Platform ワークロードの保護をシンプルにし、組織内部や、政府、業界のデータセキュリティ規則の遵守を促進します。Vormetric 透過暗号エージェントと Vormetric トークナイゼーションサーバは、GCP 内やマネージドサービスプロバイダー内、オンプレミスのワークロード上でシームレスに連携し、ポリシー / 鍵を一元管理します。

タレスCPLについて

今日の企業は、重大な判断を下すうえで、クラウド、データ、ソフトウェアに依存しています。世界で最も尊敬されているブランドや世界で最も大きな規模の企業が、タレスを信頼しているのはそのためです。タレスは、クラウド、データセンター、デバイス、ネットワークを横断して、作成場所、共有場所、保存場所を問わず、最も機密性の高い情報やソフトウェアを保護し、セキュアなアクセスを実現します。タレスのソリューションを活用することで、各企業は、セキュアにクラウドに移行し、自信を持ってコンプライアンスを達成し、毎日膨大な数のユーザーが利用するデバイスやサービスに組み込まれた自社のソフトウェアから、優れた価値を生み出すことができます。

> [thalesecurity.com](https://www.thalesecurity.com) <



アメリカ大陸 - Thales eSecurity Inc. 2860 Junction Ave, San Jose, CA 95134 USA ・ 電話 : +1 888 744 4976 または +1 954 888 6200 ・ FAX : +1 954 888 6211 ・ 電子メール : sales@thalesecurity.com

アジア太平洋 - Thales Transport & Security (HK) Lt. Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong ・ 電話 : +852 2815 8633 ・ FAX : +852 2815 8141 ・ 電子メール : asia.sales@thales-security.com

ヨーロッパ / 中東 / アフリカ (EMEA) - Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ ・ 電話 : +44 (0)1844 201800 ・ FAX : +44 (0)1844 208550 ・ 電子メール : emea.sales@thales-security.com