# ServiceNow Platform Encryption

### ビジネス上の課題

アプリケーションや情報をオンプレミスシステムからクラウドに移行するお客様は、ますます増えています。サイバー攻撃はより複雑化し、攻撃者は複数の侵入経路を利用して機密データにアクセスしています。クラウドへのデータ移行が進む中、医療記録などの個人を特定できる情報 (PII)、クレジットカード番号、企業の財務情報、知的財産など、機密データを適切に保護できない場合、重大な財務的損失、風評被害、法的影響などが生じる可能性があります。さらに、組織はプライバシーに関する法律や、HIPAA、PCI DSS、GDPR などの業界規制に対するコンプライアンスを確保しなければなりません。

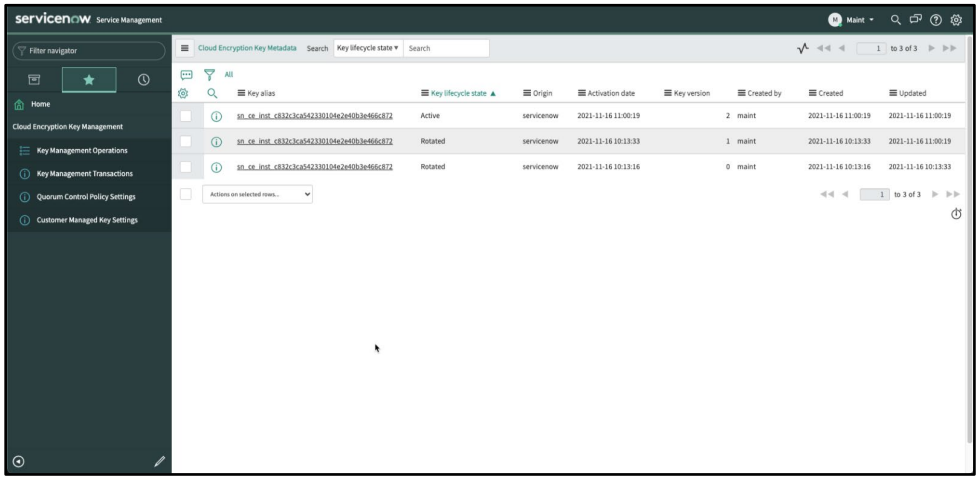
暗号化などのセキュリティソリューションを採用する際の懸念事項として、予算、パフォーマンスに関する懸念、展開に関するナレッジの不足などが挙げられますが、暗号化は何重もの保護を提供するサイバーセキュリティ戦略における主要な防御ポイントです。

### ServiceNow のソリューション

ServiceNow Platform Encryption は、機密データを保護し、プライバシーポリシー、規制要件、契約上の義務に対するコンプライアンスを確保する、複数の暗号化技術を組織に提供します。

Platform Encryption ソリューションは、次の 2 種類の暗号化機能で構成されています。

**Cloud Encryption** は、ボリュームベースの暗号化を提供し、FIPS 140-2 レベル 3 検証済みのハードウェアセキュリティモジュール (HSM) と、NIST 800-57 特別刊行物に準拠して構築された顧客制御のキー管理機能により、ServiceNow データセンターに保存中の機密データを常に保護することを保証します。




ServiceNow Cloud Encryption

### メリット

**政府が承認した業界最強の** AES 256 ビット暗号化と FIPS 140-2 レベル 3 検証済みハードウェアセキュリティモジュール (HSM) を使用し、データを最大限に保護します。

**柔軟なキー管理と独自の暗号化キー** (BYOK) を使用して機密データの管理を強化し、必要に応じてキーの作成、取り消し、ローテーション、一時停止が可能です。ServiceNow サポートが介入する必要はありません。

**ビジネスや規制要件の**進化に応じたセキュリティの強化に柔軟に対応し、投資を保護 します。

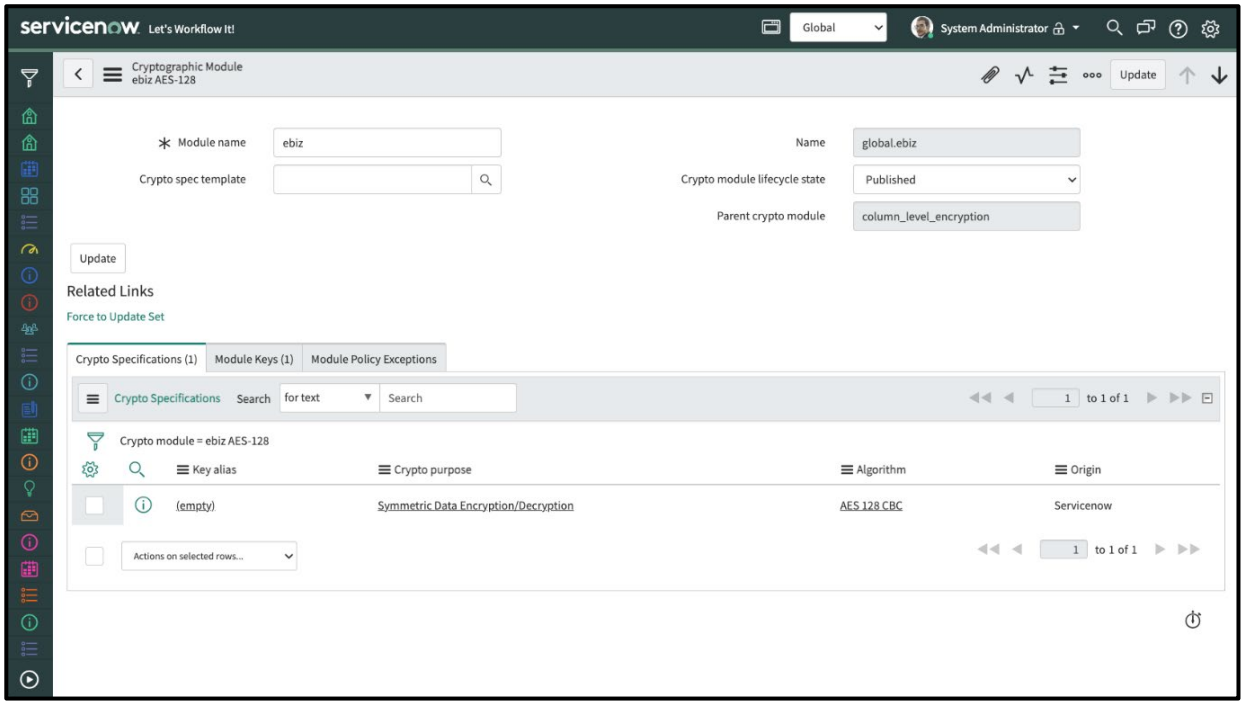
**業界の規制に準拠し、**機密データの保護と機密保持を保証することで、コンプライアンスを強化します。

**Cloud Encryption を使用すると、**アプリケーションのパフォーマンスに影響を与えることなくユーザーエクスペリエンスを向上させることができます。

**Column Level Encryption Enterprise** を使用して ServiceNow ワークフローにきめ細かいアプリケーション層のセキュリティを提供し、機密データを含む特定のフィールドとオブジェクトを保護します。

**保存中のデータと使用中のデータを対象とする**単一の暗号化ソリューションで複雑さとコストを削減 し、容易に調達および利用できます。

**Column Level Encryption Enterprise：**FIPS 140-2 レベル 3 検証済みのハードウェアセキュリティモジュールと、NIST 800-57 特別刊行物に準拠して構築された顧客制御のキー管理機能により、アプリケーションおよびデータベースレベルでデータを暗号化します。




ServiceNow Column Level Encryption Enterprise

Platform Encryption により、お客様は以下のことが可能になります。

- 機密データと規制対象データの機密性を確保し、不正な開示やデータ流出のリスクを低減する
- 政府や業界の認定要件と規制に準拠する
- 定義されたロール、定義されたスクリプト割り当て、システムユーザー、アプリケーションスコープ、ドメインメンバーシップに基づいて、機密データへのキーアクセスを制限する

**ServiceNow キーマネジメント**

Platform Encryption ソリューションには、NIST 800-57 ガイドラインに準拠して設計された包括的かつ直感的な KMF が付属しています。

ServiceNow の KMF は、柔軟な暗号化ポリシーと API サポートを可能にします。KMF には拡張キー管理機能が用意されており、お客様は自社のキーを使用するか (Bring Your Own Key、BYOK)、ServiceNow が管理するランダム生成キーを使用するかを選択できます。

KMF の中核となる機能は、キーの管理、暗号の管理と運用、監査、データ連携に関する専用のロールを持つ職務を分離するためのオプションを提供することです。

お客様のキーは、ServiceNow のインフラストラクチャ内にある FIPS 140-2 レベル 3 検証済みのハードウェアセキュリティモジュールに保管されます。

**キーのライフサイクル管理：**ServiceNow の担当者が介在することなく、お客様が定義したタイミングでキーの作成、取り消し、ローテーション、一時停止を行えます。

**モジュールのアクセスポリシー：**暗号化の各ユースケースに基づき、キーのアクセス権をスクリプト、ロール、システムにきめ細かく割り当てます。

**シンプルで直感的なユーザーインターフェイス：**使いやすいポイントアンドクリックで簡単に設定でき、最適なユーザーエクスペリエンスを提供します。

**ServiceNow Platform Encryption** は、新しいキー管理インフラ、HSM、サポートの調達および配備の必要性を排除します。Platform Encryption を使用すると、組織はリスクを最小限に抑え、攻撃対象領域を減らすことができるため、データ損失を防ぎ、保存中のデータを含め、常にデータが保護されていることを保証できます。シンプルで直感的なデータ保護ソリューションにより、組織全体で一貫したワークフローの展開と暗号の使いやすさを確保し、生産性を向上させることができます。

クラウドのセキュリティは、お客様がデータを所有し、その保護に責任を負うという共有責任です。データを暗号化することで、お客様はサイバーセキュリティ戦略の一環として何重もの保護を実現できます。

**ServiceNow Platform Encryption の詳細はこちら：**
**https://www.servicenow.com/jp/products/platform-encryption.html**

servicenow.


SN-DataSheet-Name-01012022