Climb Inc.
Growing to Meet Your Needs

クラウド サービス プロバイダが
データセキュリティを武器にする方法

2019年7月

株式会社 クライム

目　次

概要

一般的には、「セキュリティ」という言葉と「投資収益率（ROI）」という言葉が同じ文章で同時に使われることはほとんどありません。しかし、クラウド サービス プロバイダ（CSP）のビジネスプランでは、その 2 つの用語が同時に使われるのが当たり前になりつつあります。新規の顧客を開拓するには、データセキュリティへの取り組みが重要な意味を持つようになったからです。広くセキュリティ技術を運用して、セキュリティ対策と安全基準を満たすことに真剣に取り組む CSP こそが、セキュリティの懸念からクラウドへの移行を躊躇していた顧客の信頼を勝ち取っています。当ホワイトペーパは、CSP がデータセキュリティをビジネスの必須要件に加え、顧客ベースを拡大する方法について論じます。

データセキュリティがクラウドの要件に

セキュリティ製品が放っておいても飛ぶように売れたことなど一度もありません。顧客が自ら進んで購入し、それをインスールして管理するには、それ相当の強い動機づけが必要です。そうでなければ、セキュリティ製品が自ずと採用されることはありません。その状況は現在も変わりありませんが、仮想環境とクラウド インフラストラクチャの普及で、データセキュリティの制御が不可欠となる状況が格段に増えてきました。各種市場調査において、セキュリティに精通した IT 部門の責任者や IT 担当者がデータセキュリティをクラウドを採用する上での最大の懸念、と指摘する例が後を絶ちません。

セキュリティ ソフトウェアやアプライアンスはこれまで、データセンターに余計に追加しなければならなかったオーバーヘッドと見られる向きがありました。たとえセキュリティのメカニズムが生むパフォーマンス上のオーバーヘッドがゼロあるいはゼロに近かったとしても、付加的な IT 管理の重荷と見なされます。しかし、セキュリティはユーザーにとって、パブリック クラウドへの移行に不可欠な要件となりつつあります。

顧客のプライベート データセンターでかつて受け入れられていたセキュリティの基準が変わりつつあります。メディアで頻繁に報道されるデータ侵害の件数も増加し、企業の IT セキュリティ責任者のみならず、一般の耳目も集めるようになり、セキュリティのハードルも上がってきています。顧客はクラウドサービスの契約を決める際、セキュリティの保証を求めるようになってきました。クラウドを採用する上での足枷であったセキュリティが、クラウドに移行する最大の理由になる日もそう遠くありません。これは、ハイブリッド クラウドを採用する大企業にこそ、もっとも顕著な傾向です。CSP のネットワークは企業ネットワークの延長のようなものであり、企業は強固なセキュリティと責任の共有を根本的な要件として期待します。先見性のある CSP はデータセキュリティを競合他社との差別化の武器として重視し、要求の高い顧客企業を獲得していくことになるでしょう。

当ホワイトペーパーで論じるデータセキュリティ ソリューションは、クラウド上でのデータ保護を対象としています。データと、それを処理する仮想マシン（VM）要素を自動的に暗号化することによって、データを保護します。これは、顧客

が IaaS（Internet as a Service）のパブリック クラウドで自社 VM を稼働させている場合や、SaaS（Software as a Service）プロバイダが個々の顧客に独立した VM（あるいは独立した仮想ディスク）を運用している場合にも適用されます。その両方のケースで CSP は複数インスタンスの VM（顧客ごとに 1 件またはそれ以上の VM）を作り、顧客のインフラストラクチャを拡張可能にしています。CSP は安全なマルチテナント環境を確立しなければならなず、データがクラウドで保管、運用、バックアップされるたびに個別に暗号化され、高いセキュリティが確保されることを顧客に保証しなければなりません。

このようなソリューションは、CSP と顧客が VM のセキュリティに関して簡単なポリシー選択を行い、その上で通常のタスクを処理するという管理型モデルを採用しています。暗号化（エンクリプション）、キー管理、監査レコード、その他の機能の透明性が保たれ、顧客も CSP もアプリケーションを変更したり、運用方法を変えたりする必要がありません。

顧客はその貴重なデータがプライベート データセンターを離れるときは当然セキュリティに過敏になります。変わらずデータを制御し続け、そのプライバシーを保つことを求めます。業務上重要なワークロードをクラウドに移す顧客にとって、データプライバシーが最大の懸念であることは周知の事実です。

顧客はセキュリティをビジネスの一部と考える

顧客企業（特に、取締役レベルのセキュリティ責任者がいるような企業）は、IT セキュリティを「リスク対ベネフィット」の視点から捉えます。そのような企業は、クラウド サービスのビジネス上の利点を理解すると同時に、その利点に対して、セキュリティ リスクを天秤にかけます。そこでは、以下のようなセキュリティの技術的問題がビジネスリスクと見なされます。

- データセキュリティ上、物理サーバーと仮想サーバーの間に重大な違いがある

物理的に施設を構える従来型のデータセンターは物理サーバーを基盤としており、セキュリティ戦略は境界防御型がほとんどです。物理的なマシンは固定されていて、鍵のかかった部屋に置かれ、一部のシステム管理者だけがアクセスできるのが一般的です。一方、サーバーの仮想化は、プライベート データセンターにおいても、セキュリティに対する考え方を大きく変えました。仮想化のモバイルな特性と分散型のメカニズムは、管理プロセスやセキュリティへの懸念など、従来型の固定されたデータセンターでは限定的であった新しい課題を生み出しました。仮想マシン（VM）を管理されたホストやパブリック クラウド サービスに移動することは、様々なセキュリティの懸念を生み、本来クラウドがもたらす様々な利点を覆しかねません。そのような問題については後述します。

- 混在型インフラストラクチャの費用的な利点が、不十分なデータ分離／データプライバシーを誘発

コンピューティングとストレージの柔軟な活用は、仮想化の価値がもっとも認められる一側面です。VM はパフォーマンスや許容量のニーズに応じて、1 つのハードウェアから別のハードウェアに、システムを中断せずに移動することがで

きます。これは往々にして、VM が他の VM と並行して同じホスト上に、通常は混在型のストレージにおいて同時に稼働することを意味します。パブリック クラウドで VM を使用することは、大抵の場合、混在型のインフラストラクチャに依存します。その混在環境では、データ分離を確保することが重要であり、決して軽視できることではありません。ほとんどのプロバイダはそれを認識し、最低でも、マルチテナントのデータ分離が必要だと理解しているようです。それは別々の物理デバイスを提供することによって実現可能ですが、コストがかかり、プロバイダと顧客の双方にとり、せっかくのクラウドの効率性と費用効果が損なわれてしまいます。そこで、混在する VM とデータを暗号化によって分離してデータプライバシーを確立するのが理想的な解決策となります。ただし、それが高パフォーマンスで自動的に行われ、暗号化とキー管理が VM の移動をライフタイムを通してサポートしなければなりません。

- 物理サーバーに比べ、VM のアクセス媒体が多すぎる（管理者、ホスト、ストレージなど）

VM にアクセスするホストやユーザーは次第に増加します。物理サーバーと異なり、仮想サーバーやその仮想ディスクにはモバイルの特性があり、複製やストレージでのレプリケーション、災害復旧（DR）アーカイブへのコピー、データセンター間の移動が簡単です。例えば、VMware の仮想ディスクは単純な Storage VMotion コマンドで、稼働中でも 1 つのデバイスから他の場所へ移動できます。その場合、移動先ストレージのセキュリティは元のストレージのセキュリティと同じなのか？移動先には誰がアクセスするのか？その管理やバックアップは誰が担当するのか？などの疑問が生じます。つまり、モバイルの柔軟性と簡単さが潜在的なセキュリティ リスクにつながる可能性があります。

専門知識のある IT 担当者は、セキュリティ リスクが外部のハッカーよりも内部に起因する場合が多いことを知っているはずです。ある調査では、データ漏洩などセキュリティ問題の 52%が内部での処理により、しかも、ほとんどが偶発的に生じていると判明しています。CSP のデータセンターも例外ではなく、故意によるか事故かにかかわらず、内部の脅威に晒されています。顧客が CSP に重要なデータ資産の管理を任せる場合、データプライバシーがサービスの最重要案件になることは言うまでもありません。顧客のデータを暗号化するだけでなく、プロバイダが顧客データはもちろん、関連する暗号化キーにもアクセスできないことが、クラウドのセキュリティにおいてはベストプラクティスの最優先事項となっています。

- VM イメージを構成するファイルはセキュリティ上、重要な保護対象

データと VM イメージの両方を保護することが重要です。例えば、物理サーバーと仮想サーバーの本質的な違いを表す以下の例を考えてみてください。

クレジットカード情報保護のためのセキュリティ基準（PCI DSS）を満たさなければならない物理サーバーにおいてデータベース アプリケーションが稼働しているとします。PCI DSS を満たすためには、カラム単位あるいはテーブルスペースの暗号化によって、データベース上のクレジットカード番号を保護するのが一般的です。物理ホストでそれを実践すれば、要件は満たされます。しかし、そのサーバーが仮想化されたらどうでしょうか。ホストが過度に使用されれば、ハイパーバイザーが仮想メモリーにアクセスするようになります。また、VM が一時停止すれば、暗号化キーを含

むメモリー イメージがディスクに書き込まれ、ストレージに保存されます。つまり、VM イメージ ファイルが保護されていない場合、暗号化キーを見つけ出すことが突然にたやすくなってしまう危険性があります。

VM イメージが保存されているストレージは保護されなければなりません。そのようなメモリーイメージの保護は、2011 年発行の PCI-DSS ガイドラインの最新アップデートにも明記されています。

データのオフサイト移管は社内のセキュリティ議論を健全化

データセキュリティの実践方法は従来、IT 部門の最高責任者、セキュリティ責任者、あるいは単にセキュリティに精通したスタッフが決定していました。それは、完全にプライベートなデータセンターでは、業務を中断しない程度に、あるいは予算を超過しない程度に、実践すべきベストプラクティスの度合いを決めることが中心でした。しかし、パブリック クラウドでは、技術的な実践方法にとどまらず、SLA（サービスレベル アグリーメント）契約や、法的、信託上の責任問題が関わってきます。よって、サーバーをパブリック クラウドに移すことは、セキュリティに関する決定を社内の IT チームにとどめず、上層部も巻き込んで、議論の透明化が図られます。

- ビジネスリーダーはクラウドを会社の生存／競争力強化の原動力と捉える

製品、サービス、ソリューションを供給しながら、成長を目指す企業は、そのためにどうクラウドを活用するか考える必要に迫られています。それを実践できなかった企業は淘汰され、できた企業だけが生き残ります。CEO や CFO、取締役会などは、クラウドの活用が IT コスト面だけでなく、サービスやシステムを迅速に発展させる柔軟性、競争力、戦略的目標の達成に重要な手段と認める傾向にあります。クラウドの活用がビジネスを補助するだけの IT 業務に留められていては、本来の価値が見出せません。クラウドの柔軟性が、企業運営の中心課題に据えられ、その応用範囲の広がりがビジネスの鍵を握ります。

セキュリティ上重大かつ業務上不可欠なデータをクラウドには任せられない、と主張する IT 管理者もいます。しかし、この言い訳は、クラウド サービスの採用が増加の一途をたどる中、通用しなくなっています。企業はいずれ大半の業務をクラウドに移動することになると自覚しています。重要な決断は、クラウドを活用するか否かではなく、どの CSP を信頼して、重要なアプリケーション ワークロードを任せるかという点です。

- データプライバシーの問題は企業トップの法律顧問が担当

米国だけでもデータ侵害に関する法律は 51 件ほどあります。プライベート データが漏洩した、あるいは漏洩が疑われる場合、すぐにこれらの法律の適用または法的な影響が生じます。データ漏洩がプライベート データセンターで起きたか、CSP サイトで起きたかは関係ありません。また、外部のハッカーの仕業か、内部犯の悪事によるものか、信頼する職員のミスによるものかも関係ありません。データ漏洩とその法的な影響はデータを所有する会社の責任であることに変わりはありません。だからこそ、法的リスクが甚大で、企業の法律顧問の活躍の場となっています。

同様に、企業がデータをクラウドに移すときは、データ主権の問題も大きな法的影響を伴います。EU 加盟国の中には、特定の個人情報が国境を越えることを法律違反と認定する国もあります。米国では、CSP は個人のプライベート データを本人に通知なく、法的に転用が強制される可能性があります。例えば、英国の大手国防情報セキュリティ会社 BAE は Microsoft のクラウド コラボレーション ソフトウェア Office 365 の採用を、同社の法律顧問の指示により取りやめる事例がありました。Microsoft が BAE のデータ主権を保証できなかったことがその理由です。

- 企業経営者はデータセキュリティ リスクの説明責任を認識

企業の IT 運用にクラウドの占める割合が大きくなるにつれ、クラウドにおけるデータセキュリティが社内の取締役会でも議論されるようになりました。データ漏洩が公になった場合、会社が財務上および風評上に被る損害は膨大な額にのぼることがメディアでも再三取り沙汰され、企業の CEO は最終的な損害額は法的な処理に留まらず、それをはるかに上回ることを認識しています。データ漏洩の結果、顧客の信頼を失うことは取り返しのつかない大損害です。そのような脅威に対する CEO の対応はこれまで、IT 責任者を呼び出して机をより強く叩き、データセキュリティの重要さを説くことぐらいでした。しかし、今や CEO は、IT 責任者にデータセキュリティの保証を含むクラウド採用プランの提出を求めるようになりました。データセキュリティの問題が会社の将来や自身の地位に大きく影響することが、企業の最高経営責任者にも意識され出したのです。

顧客ニーズに応える CSP はセキュリティ懸念をビジネスに転換

クラウド サービス プロバイダ（CSP）にとって、顧客が抱くデータセキュリティの疑問を理解し、それに的確に答えることが重要になります。データセキュリティが重荷になる必要はありません。データセキュリティのソリューションは、適切に設計されれば、シンプルかつ自動的に運用でき、顧客が使用するアプリケーションの機能を混乱させるようなことはありません。簡単に管理でき、アプリケーションの動作を遅くさせたり、顧客や顧客サポートを継続的に悩ませるようなこともありません。セキュリティ ソリューション（特に暗号化ベースのソリューション）に疑問を抱く顧客は通常、オーバーヘッドとリスクについて心配しています。管理の複雑さとそれに要する時間はどれぐらいか？システム パフォーマンスへの影響はどのぐらいか？アプリケーションの動作は遅くなるのか？データを暗号化されていない状態で取得できるのか？できない場合のリスクは？暗号化キーを失くす危険は？正しく設計されたソリューションとは、このような顧客の懸念にきちんと応え、クラウドにおけるデータセキュリティの最重要ニーズを満たすものでなければなりません。

暗号化ベースのセキュリティ ソリューションが応えるクラウドの顧客ニーズ

- 混在型のクラウド環境でもデータのプライバシーが守られる
- クラウドへの保存、移動、レプリケーションに際した顧客データへのアクセス
- 未保護データを残すことなく、クラウドから顧客データを取得・引き上げ可能

- PCI-DSS（クレジットカード情報保護のためのセキュリティ基準）、HIPAA（医療保険の相互運用性と説明責任に関する法律）などのデータ規制要件を必要に応じて遵守
- データの安全確保に必要な措置が取られていることを示す監査レコードへのアクセス
- クラウドでデータ侵害が発生した際、その通知義務からのセーフハーバー（免責）要件を満たす
- 管理の複雑さ、オーバーヘッド、リスクを最低限に

上記の機能性を顧客に提供する CSP は、顧客が業務上不可欠でセキュリティ上重要な仮想ワークロードをクラウドに安心して配備できる環境を構築していると言えます。このようなサービスの提供が顧客の信頼を得ることはわかりましたが、では、CSP のビジネスや経済的・法律的ニーズを満たす形でこのようなサービスを実現するにはどうしたらよいでしょうか？

暗号化ベースのセキュリティ ソリューションが満たす CSP のニーズ

- 見込み顧客からのデータセキュリティの質問に充分に答えることによって新規顧客を獲得
- 安全なインフラストラクチャをプレミアム価格で高額販売（任意）
- 各種規制（PCI-DSS、HIPAA など）へのコンプライアンスを必要とする顧客に適切なサポートを提供
- クラウド契約の一部として顧客に希望があった場合に、より高度な SLA を提供
- 顧客のプライベート環境から CSP のクラウドへ VM やデータを安全に移管する方法を提供
- 顧客データの漏洩、法的問題、政府からのディスクロージャー要請に対処するために顧客の暗号化キーを分離保持
- バックアップおよび災害復旧（DR）用に VM イメージの暗号化を実現
- 顧客の保存データが誤って漏洩した、あるいは漏洩が疑われる場合の一般通知義務からのセーフハーバー（免責）— データ侵害に関する法律が暗号化されたデータの通知にセーフハーバーを適用する場合
- データセキュリティのベストプラクティスを奨励することにより、自社のサービスを他社と差別化

CSP と顧客、双方のニーズを満たす機能性

前述の CSP および顧客ニーズの考察にもとづき、暗号化ベースのソリューションの特性や機能がニーズにどのように対応するかを以下に見ていきます。

クラウドの顧客に重要な機能

- **データセキュリティの制御が簡単かつ明瞭に、顧客企業が運用方法を変えなくても自動的に提供可能**

クラウド サービスの顧客の懸念を解消する最善策は、ソリューションをほぼ全般的に透明化することです。顧客はこれまで通り、CSP と普通に契約するだけで足り、特別なプロセスを必要とするべきではありません。単純なケースでは、顧客はデータの暗号化を希望するチェックボックスを選択するだけでよく、より高度なケースでは、顧客がポリシー上の選択をでき、特定の VM セットを誰が管理する権限を持つか規定できるしくみも有効です。そのような設定の後に顧客が普段と変わりなく VM を管理し、使用できる利便性が重要です。

- **暗号化が顧客企業の業務や使用するアプリケーションに悪影響を及ぼさない**

  従来の暗号化ソリューションは複雑過ぎて、システムへの影響が顕著でした。例えば、暗号化の導入を決めた企業は、最初に広範なデータストアを暗号化するのに、重要なアプリケーションをしばらくオフラインにしなければなりませんでした。さらに、暗号化による CPU への負担が重要なアプリケーションの動作を遅くさせ、効率性を損ない、ユーザーの使い心地が悪くなるケースがほとんどでした。暗号化ソフトウェアのアップグレード時やキー管理サーバーがオフラインになったとき、さらには各種規制への対応やセキュリティの強化にともなってデータの再キーが必要になったときなどは、業務への影響が一層顕著になりました。このような問題は、最新型の適切な暗号化ソリューションを採用することで解消され、ユーザーに余計な負担をかけることがなくなります。アプリケーションが稼働されるときにその場でデータを自動的に暗号化することが可能になり、同時に、ハードウェアに組み込まれた暗号化アクセラレータ機能が高速処理をサポートします。暗号化ソリューションのデプロイメントをサポートするキー管理システムの可用性も重要なポイントです。顧客がキーを使えずに困るようなことは絶対に避けなければなりません。

- **保護が必要なすべての仮想ワークロードに適用できる包括的な暗号化**

  かつて暗号化ソリューションはその複雑さのため、一定数のシステムだけを、どうしても必要な場合に暗号化するのが一般的でした。しかし、現在は仮想ワークロードやデータがクラウドとデータセンター間を移動する環境において、暗号化はあらゆるワークロードに適用可能であるのが、セキュリティの基本原則です。いかなる仮想化ワークロードとそのデータストアも暗号化でき、同時に VM 自体のシステムドライブ（ゲスト OS を含む）も暗号化できるような仮想化完全対応の暗号化ソリューションが必要です。そのような包括性が、VM とそのデータの保護には不可欠です。すべてを漏らさず暗号化し、しかも、それが自動的に実行されなければなりません。

- **キーの取り扱い、預託（エスクロー）、回復、保護などの複雑なキー管理が自動化**

  キー管理はわかりづらく、顧客企業（その IT スタッフの多く）にとって取っつきにくい作業です。暗号法の言語を理解できる人は限られ、キー保管や分配のしくみは IT 専門家にとっても難解とされます。キー処理のしくみに自動対応するポリシー管理モデルを提供し、CSP と顧客の負担を解消するソリューションが必要です。

- **暗号化キーを許可するのは顧客の特権**

  セキュリティに敏感な顧客企業の中には、データ主権の問題や、偶発的あるいは権限の誤用による暗号化キーの不正アクセスを懸念するユーザーも少なくありません。しかし、適正に設計されたシステムでは、顧客が暗号化

キーへのアクセス制御を保持します。そのようなキー管理のメカニズムが通常のシステム運用を阻害することなく、顧客だけが暗号化キーへのアクセスを許可できる体制が保証されます。その特権を CSP が無効化できるようなことはありません。

- **適正なアクセス許可にもとづく限り、データは暗号化されていない状態でいつでもアクセス可能**

  クラウド サービスの顧客には、いつでも自分のデータにアクセスできる安心感が重要です。充分なアクセス制御がシステムに組み込まれる必要があります。ハードウェアの不具合や他の問題でデータへのアクセスを永久に喪失してしまうような不安感を、ユーザーに微塵も抱かせるべきではありません。

- **管理作業やデータアクセスはすべて監査対象で、履歴の確認がいつでも可能**

  クラウド サービスの顧客は、保護されたデータが常に監視下に置かれることを望みます。その監査ログが保存され、そこからデータセキュリティやコンプライアンスを確立するために実践すべきことを確認できることが重要です。

クラウド サービス プロバイダ（CSP）にとって重要な機能

- **データセキュリティの制御が簡単かつ明瞭に、CSP がインフラに変更を加えなくても自動的に提供可能**

  CSP には、マルチテナントの混在環境で顧客データを自動分類できる暗号化システムが必要です。それは、顧客の VM とデータを自動的に保護し、その保護が VM のライフタイムを通じて VM とともに移動し、VM を保護し続けるものでなければなりません。つまり、VM が仮想ホスト間を移動したり、他のストレージに移されたり、バックアップや災害復旧（DR）システムにコピーされるたびに、それらを保護し続け、関連するセキュリティ ポリシーも併せた可搬性が必要とされます。同時に、そのソリューションは、CSP の既存する IT 管理方法やセキュリティ ツール、ストレージ、ネットワーク ハードウェアを阻害することがあってはなりません。

- **暗号化システムがパフォーマンスを著しく阻害しない**

  IaaS と SaaS のプロバイダは、ある意味、コンピュート サイクル（CPU の負担）を切り売りしていると言えます。データセキュリティ システムは過剰サイクルの消費をせず、CSP のインフラストラクチャへの過度の負担ががビジネスに響くようなことは避けなければなりません。そもそも暗号化（エンクリプション）とは、限定的な事例やデータセットにだけ用いられてきました。しかし、新しいテクノロジーやソフトウェア開発技術、異なる物理システム間を移動するデータの保護へのニーズの高まりによって、暗号化の適用範囲が拡大しました。

  暗号化技術自体も現在は高速化と汎用化が進んでいます。CPU の高速化も目覚ましく、暗号化の基盤となる数学的処理を支える力は以前とは比べものになりません。加えて、暗号化を支える特別なハードウェアも利用しやすくなっています。ほとんどの場合、仮想化をホストするサーバーにはすでにその機能が備わっています。例えば、AES-NI（Advanced Encryption Standard New Instructions）機能は標準的なインテルおよび

AMD の x86 チップセットには組み込まれており、AES の包括的な暗号化処理をハードウェア仕様の速度（ソフトウェア ベースの暗号化に比べ 10 倍の高速）で実現します。このようなハードウェアの特性を自動的に検知し、活用する機能が暗号化ソリューションに備わっていることが重要になります。暗号化ソリューションのソフトウェアはスマート設計によって、その運用状況が分かりやすく、仮想化とストレージ インフラの基盤となるメカニズムと連携することが求められます。それにより、暗号化を必要なときだけ最適化された状態で実行でき、キャッシングのフル活用が可能になります。

- **API と CLI によるフル管理機能、使いやすい GUI（任意）を完備**

  CSP はインフラストラクチャをスケーラブルに運用しなければなりません。つまり、拡張性と可用性、回復力に優れ、完全に自動化された管理が可能であることが重要です。したがって、暗号化ソリューションには、一目でわかるぐらい単純で使いやすい GUI が、CSP と顧客の双方に必要です。同時に、CSP は API（アプリケーション プログラミング インターフェース）コールによってスクリプトでシステムを管理でき、スクリプトの実行はユーザーによる操作がまったく（あるいはほとんど）不要でなければなりません。API ファンクションは、顧客に対する初期のプロビジョニングから、その顧客の VM とデータの安全なデコミッショニングまで、すべての管理機能を網羅する必要があります。

- **顧客のコンプライアンスを満たす監査記録を生成でき、CSP の適正な運営を証明**

  CSP とは、言うなれば、顧客データの管財人であり、その適正な運営状況を顧客や政府機関または監査人に対して説明できなければなりません。暗号化ソリューションは、実行されたすべての管理作業がいつ、どこで、誰に行われたのか、一連の監査記録を提供する必要があります。そして、顧客がその監査履歴を簡単に閲覧でき、標準的なログ管理サーバーへのインポートとエクスポートも容易でなければなりません。

- **CSP がキー管理をホストし、顧客（またはサードパーティーサービス）が実際のキーへのアクセスを保持**

  CSP は、時として、顧客のデータ暗号化キーをいつでも管理できる状態に置いておきたいと考えます。必要なキーを自動的に使用できるシステムが必要ですが、その一方で、顧客データを暗号化した実際のキー自体も確実に暗号化され、キー管理システムに保管されることが大事です。さらに一歩進んだ、顧客と CSP の双方に有益なしくみは、保管されたデータ暗号化キーへのアクセスを顧客だけが許可できるようにキーを暗号化することです。それにより、顧客以外は誰もキーへのアクセスを制御できないという安心感が顧客にもたらされ、CSP が顧客のキーを晒してしまう危険や疑念も生じることがありません。

  同様のセキュリティは、サードパーティーのキー管理サービスをクラウド外で提供することによっても実現できます。顧客が直接そのサービスを使うことも、CSP が使うことも可能で、運用上の違いはありません。CSP が顧客のデータ暗号化キーに直接アクセスすることができず、キーを別のエージェントに受け渡すこともできません。VM やデー

タの所在地の法規制に敏感な顧客には特に有効な選択肢となります。データ暗号化キーへのアクセスを許可する権利を顧客が占有すれば、CSP がキーを外部に晒してしまう手段も動機も存在しないことになります。

まとめ

暗号化（エンクリプション）はデータのプライバシーを守る強力なツールです。もともとは特別な状況の選ばれたホストにだけ適用されてきました。しかし、データの処理とストレージがクラウドに移り、データプライバシーの需要と暗号化のニーズに大きな変化が生まれました。クラウド上の共有型の IT インフラストラクチャに、業務上重要なアプリケーションを移す企業が増え続けています。それができるのは、企業の法規制上のコンプライアンス ニーズならびにデータプライバシー ニーズを完全に満たすクラウド サービス プロバイダ（CSP）を通じてのみです。幸いなことに、適正に設計された最新の暗号化ソリューションは、そのような顧客ニーズと、CSP のビジネス要件を同時に満たすことができます。そして、そのようなソリューションを採用した CSP だけが他社との差別化に成功し、新規のクラウド顧客を獲得しています。

© 株式会社クライム

東京都中央区日本橋蛎殻町 1-36-7 蛎殻町千葉ビル 4F

TEL: 03-3660-9336 / 06-6147-8201

www.climb.co.jp Email: soft@climb.co.jp