EU 一般データ保護規則

General Data Protection Regulation

HyTrust 製品の有用性

米コールファイア社による検証レポート

2018 年 5 月

株式会社クライム

目　次

エグゼクティブサマリー

HyTrust, Inc.（以下、HyTrust）は、一連の HyTrust ワークロードセキュリティ製品の欧州連合（EU）一般データ保護規則（General Data Protection Regulation、以下 GDPR）への準拠状況を技術的に検証するために、サイバーセキュリティアドバイザーとして評価の高いコールファイア（Caolfire）社を独立した審査機関として任用しました。

GDPR の要件を満たすには、欧州連合（EU）域内のデータ主体（当該個人）を対象に事業を行う団体は、組織的かつ技術的な予防策を新たに構築しなければならない可能性があります。その組織的かつ技術的な予防策は、GDPR に規定される個人データ保護要件に準じたものでなければならず、データの最小化、保管の制限、目的の限定、正確性、完全性、機密性、有用性、信頼性、適法性、公平性、透明性や、その他、諸々の項目が、その適用対象として定められています。適切な予防策を構築するには、GDPR の規定にもとづいて、保護すべきデータの処理を特定し、それにともなうリスクを理解する必要があります。

当文書は、HyTrust によって実現され得る、クラウドインフラストラクチャにおける個人データ保護に使用可能な技術的予防策に主な焦点を当てて論じます。GDPR の諸条件、特にデータ保護をサポートする上での HyTrust ソリューションの有効性を見極めることが、コールファイア社の調査目的です。調査対象の HyTrust ソリューションは、GDPR 準拠を目指す企業・団体がリスクを軽減し、データセキュリティを高めるための可視性や見識、制御機能を提供するものです。

コールファイア社の見解

HyTrust によってもたらされるソリューションは、保護対象のデータおよび機密データの処理に関する多くのリスクに対処する機能を備えている、というのがコールファイア社の見解です。

一般データ保護規則（GDPR）とは

一般データ保護規則（GDPR）は欧州連合（EU）議会によって 2016 年 4 月 14 日に採択されました。それにより、同規則が従来のデータ保護指令（Data Protection Directive 95/46/EC）に取って代わり、欧州全体の個人データ保護法令を統一的に定めることを目的としています。2018 年 5 月 25 日には、EU 加盟各国の個々の既存するデータ保護法例が GDPR に置き換えられ、個人データ処理のセキュリティに関し、各種の変更、法令適用およびその実効性の強化が見られることになります。これらの変更は、欧州内外の企業や公共機関に少なからず影響を与える可能性があります。

GDPR は、欧州全体のデータ保護法例を統一することにより全 EU 加盟国民に対するデータ保護を強化し、全 EU 加盟国民の個人情報保護の実効力を高め、データプライバシーに対する企業の取り組みを見直すことを、その趣旨としています。個人データがどのように管理され、処理されるべきか、そして、データ侵害に際して企業・団体がどのように対応すべきかの指針が、GDPR により示されます。

従来の規則は個人情報のセキュリティとプライバシーに関する人権を守る上で不十分でしたが、新規則では、EU および加盟各国の企業・団体（データの管理者および処理者）に対する実効力が高められました。それにより、規則の遵守を怠ったり、適切な処置を講じずに管理または処理すべき個人データを危険に晒した団体への取り締まりが強化されます。そのため、欧州領域内の適用範囲を広げると同時に、域外適用も定め、罰則、データ主体（当該個人）による承諾の条件も強化されました。

企業・団体は 2018 年 5 月 25 日までに自社のプロセスとセキュリティ戦略を見直し、GDPR の原則に準拠していることを確認する必要があります。準拠を怠り、データセキュリティ侵害が発生した場合は厳しい制裁が課され、刑事処分に加え、前年度の世界全体での総売上の 4%、あるいは 2,000 万ユーロのどちらか高額なほうが制裁金として課される可能性があります。

何が変わったのか？

新規則により、各種の変更と新たな法令適用が導入されました。GDPR を包括的に理解し、運用するには、法律上、技術上、そして、コンプライアンスにおける専門家との相談が推奨されます。GDPR により導入された主な変更点は以下の通りです。

欧州領域内の適用範囲拡大（域外適用の追加）

GDPR は、EU 域内に居住するデータ主体の個人データを処理するすべての会社に、その所在地にかかわらず適用されます。つまり、データの管理者および処理者による個人データの処理に対し、その管理者・処理者が EU 域内の事業者であろうが、EU 域外の事業者であろうが、データが EU 域内で処理されるか否かにかかわらず適用されます。該当するデータ処理には、支払の発生の有無を問わず、EU 加盟国民への製品やサービスの提供、EU 域内での行動の監視などの活動が含まれます。EU 域内に事業所を持たずに EU 加盟国民に対して事業を行っている事業者は、EU 域内に代表者を置く必要があります。

罰則

GDPR に違反した企業・団体は最高で、前年度の世界全体での総売上の 4%か、2,000 万ユーロのどちらか高いほうの罰金を課せられる可能性があります。これは、もっとも深刻な GDPR 違反を犯した場合に課される最高額の制裁金です。そのような罰金が課される違反例としては、顧客の承諾なしにデータを処理したり、プライバシー保護

の原理に反するような設計ミスが考えられます。制裁金は段階的なしくみで構成され、より深刻度の低い違反に対しては、総売上の 4%ではなく 2%の制裁金が課されます。記録を正しく保管していない場合や、データ侵害発生時に管轄行政やデータ主体（対象となる個人）への通知を怠ったり、影響評価を行わなかった場合などに、そのような制裁が課されます。

サプライチェーン

従来の規則では、データ管理者（controller）のみが個人データ保護の全責任を負い、仮にデータの一部がデータ処理者（processor）としての第三者に処理されていても関係ありませんでした。しかし、GDPR においては、管理者と処理者がともに GDPR 要件を満たす必要があり、コンプライアンスの責任を共有する形になります。これは、すなわち『クラウド』も GDPR 適用の例外ではなくなることを意味します。

承諾

GDPR は、データ処理の承諾条件をわかりやすく（平易で明快な言葉により）、アクセスしやすい形で提示することを義務付けています。承諾条件には、データ処理の目的が必ず含まれていなければなりません。さらに、データ主体（対象となる個人）が承諾を撤回することは、承諾を供与するのと同じぐらいに容易でなければなりません。

データ保護責任者（Data Protection Officer）

GDPR においては、すべての公共機関、ならびに、その主要事業が個人の機密データの大規模な処理、あるいは定期的かつ組織だった個人の監視を大規模に行う私企業は、データ保護コンプライアンスの管理責任を負う者として、データ保護責任者（DPO）を任用しなければなりません。DPO の役割は、コンプライアンス責任者と似ていますが、個人データの処理と保持に関して、IT プロセス、データセキュリティ（サイバー攻撃対策を含む）、事業継続に関わるその他の重要事項に精通していなければならない点が異なります。

データプライバシー影響評価（Data Privacy Impact Assessment）

個人データのアクセスや保管に新システムが使用される場合や、個人データが新規の、または予期せぬプロセスに使用される場合、あるいは、単にデータベースが単一リポジトリに統合される場合など、諸般の状況において、企業・団体はデータプライバシー影響評価（DPIA）を実施することが義務付けられます。それにより、データの取り扱い手順や処理（個人データの用途を含む）が個人データとその主体のプライバシーとセキュリティにどのような影響を及ぼすかを検証しなければなりません。

アクセス権

透明性の向上とデータ主体の権利保護の観点から、データ主体はデータ管理者に対し、その関連データの処理状況、どの範囲まで、どのような目的で処理されるのか、確認を得る権利を有します。データ管理者は、依頼があれば、個人データのコピーをデータ主体に無料で、電子フォーマットで提供できるようにしておくことが義務付けられます。

削除権（忘れられる権利）

データ主体はデータ管理者にその個人データの消去、データ流布の停止、第三者によるデータ処理の中止を要求することができます。

データの可搬性

アクセス権の延長として、データ主体はその関連データを一般的に使用されるフォーマットで受け取る権利を有します。そのフォーマットは機械で読み取れる形式でなければなりません。それにより、データ主体は自分のデータを他のデータ管理者に移転することが可能になります。

データ侵害の遅滞なき通知

GDPR は、データ管理者によるデータ侵害セキュリティ報告の必須要件を規定しています。それによると、（i）可能な限り、72 時間以内に遅滞なく監査当局に通知することと、（ii）当該データ主体に不当な遅れなく通知すること（被害のリスクが低い場合は不要）が義務付けられています。データ処理者はデータ管理者に不当な遅れなく通知しなければなりません。GDPR により、データ侵害発生時に事業者が被る法律上、財務上、あるいは風評上のリスクは極めて高まったと言えます。

設計・初期設定からデータ保護

「プライバシー バイ デザイン」は決して新しいコンセプトではありませんが、GDPR によって初めて義務付けられました。プライバシー バイ デザインでは、個人データの保護を考慮した設計が、後から検討し、追加するのではなく、システム設計の最初の段階から組み込まれている必要があります。適切で効果的な、技術的かつ組織的方策がシステム設計の一部として実装され、GDPR の要件および、その規定に則ったデータ主体の権利保護が考慮されていなければなりません。

HyTrust によるデータ保護

HyTrust の使命は、クラウドインフラストラクチャの信頼性を高めることです。マルチクラウドを追及する企業に、ワークロードがクラウド上のどこにあっても、その安全を積極的に確保するために欠かせない機能を提供します。この使命を全うするために、HyTrust は Cloud Security Policy Framework（クラウドセキュリティポリシーフレームワーク、

以下、CloudSPF）を構築しました。CloudSPF により、プライベートおよびパブリッククラウドのワークロードに対するセキュリティポリシーの作成と適用、そして実行が自動化されます。CloudSPF は、発見、分析、実行、報告といったセキュリティライフサイクルの各段階に対応する HyTrust Workload Security Solution によってサポートされます。HyTrust Workload Security Solution は、HyTrust CloudControl、HyTrust DataControl、HyTrust CloudAdvisor の三本柱から構成されます。

これらの HyTrust ソリューションは、GDPR の規制対象となるワークロードに対し、そのデータプライバシー保護のための各種規制事項に柔軟に対応します。Intel®プロセッサーの機能と組み合わされ、VMware NSX for vSphere と統合されれば、セキュリティポリシーの設計、作成、適用、実行の各機能が拡充され、多種多様なより幅広いセキュリティ効果をもたらします。下図 1 は、HyTrust CloudSPF の GDPR ライフサイクルへの対応（左）と、ワークロード保護のための般的なワークロードセキュリティ項目に沿った機能性を表しています。

図 1. クラウドセキュリティポリシーフレームワーク（CloudSPF）をサポートする HyTrust ワークロードセキュリティ

個人データの収集、処理、保管を行うビジネスアプリケーションのビルトイン機能として、データプライバシーが徹底されることの重要性は疑う余地がありません。セキュリティ制御が慎重かつ計画的に設計され、個人データの適切な取り扱い基準やポリシー、手順に沿ったアプリケーションに統合されれば、技術的予防策への GDPR 要件は大半が満たされるはずです。データを取り扱うアプリケーションは、GDPR の規定事項に沿ってデータプライバシーを確立する制御機能を備えている必要があります。しかし、データプライバシーを全面的に GDPR 基準で処理する機能がビジネスアプリケーションに備えられていたとしても、土台となるインフラの設計にリスクが潜んでいることもあります。そのインフラがサポートする事業において、機密データプのライバシーが脅かされる結果になりかねません。「セキュリティ バイ デザイン」

を確立するための包括的なアプローチは、アプリケーションの機能としてのセキュリティ制御と、アプリケーションとデータをサポートするインフラに機能として組み込まれ、統合されたセキュリティ制御の両面を考慮することが重要です。

> 『コンピュータシステムに充分なセキュリティ制御を備えられるかどうかは、システム設計の課題である。包括的なセキュリティは、ハードウェア、ソフトウェア、通信、物理的、人的、管理手続き上の防御策が組み合わされなければ実現しない。特筆すべきは、ソフトウェアのみの防御策では充分ではないということである』 ― The Ware Report（米国防省国防科学委員会タスクフォースによるコンピュータセキュリティに関する報告書、1970 年）

CloudSPF は、企業が必要とするインフラやプラットフォームセキュリティのあらゆる要素を考慮して構築されました。人、データ、インフラの要素に適用されたセキュリティのライフサイクルは、「セキュリティ バイ デザイン／バイ デフォルト」のモデルとなるものです。そこには、セキュリティ設計の多くの課題を解決するために特別に考案された HyTrust ソリューションが組み込まれています。

HyTrust CloudControl

クラウドおよびソフトウェアデファインドのデータセンターを採用した企業は、効率性、柔軟性、コスト節約など、多くの利点を享受しています。例えば、柔軟性は、ワークロードをいつでも必要なときに動的に拡大することを容易にします。仮想化によって実現する、基盤となるハードウェアからの抽象化も、ワークロードの可搬性を高めます。ワークロードが特定のハードウェアに縛られないので、効率的なリソースの分散が可能になり、ワークロードの可用性が向上します。ワークロードが複数の場所に容易に移行または拡張できるので、顧客により近く、効率的なサービスが可能になる点も見逃せません。

これら柔軟性から得られる利点も多い反面、それによる複雑化も否めません。ソフトウェアデファインドデータセンター本来の絶えず変化する特性が運用上の死角を生み、セキュリティの状態をいつ何時でも識別可能にすることは難しくなります。ワークロードが分散されたインフラに点在して、動的に拡大または縮小でき、仮想ネットワークは簡単に構築または破壊が可能です。このような環境では、ソフトウェアデファインドのインフラから得られる利点をサポートしつつ、同時に、セキュリティへの意識、ポリシーの施行を疎かにせず、監査要件のサポートや迅速な修復を可能にする制御メカニズムが必要とされます。

VMware vSphere および VMware NSX、そして VMware ESXi との統合が可能な HyTrust CloudControl は、セキュリティを重視し、ポリシーの施行、監査サポート、セキュリティ問題の修正機能を、仮想ワークロードにもたらします。さらに、アクセス権限の高度な制御とポリシーの徹底、フォレンジック分析、コンプライアンスの自動化などの機能が、仮想環境とプライベートクラウドインフラに活用でき、セキュリティライフサイクルの各ステップが発見から報告まで継続的にサポートされます。

また、詳しくて使いやすいセキュリティポスチャーダッシュボードにより、コンプライアンスに対するコンフィギュレーションの状態や、システム管理者の行動に対する監査証跡、さらにリソースの保護状態がすべての仮想マシン（VM）に対して可視化され、わかりやすく表示されます。セキュリティの状態を目で確かめられるので、クラウドおよびセキュリティ管理者のとるべき措置が情報として示されます。そのため、コンフィギュレーションのずれやコンプライアンスの問題にいち早く対処でき、環境に変更が生じた原因やそのワークロードへの影響を確認することができます。セキュリティおよび運用の担当者は、セキュリティの問題やコンフィギュレーションのずれにボタン一つで対応でき、継続的なコンプライアンスが確保されます。

HyTrust CloudControl には、30 以上のあらかじめ定義された使いやすいテンプレートが備えられ、様々なセキュリティとコンプライアンスの枠組みに対応することができます。コンフィギュレーションをテンプレートと比較すれば、コンプライアンスに影響する問題の有無が直ちにわかるしくみになっています。これらのテンプレートをリスクベースの枠組みでコンプライアンスを追求するための土台とし、そこに新たなポリシーを追加し、コンフィギュレーションを調整して、企業独自のニーズに見合うようにカスタマイズすることができます。コンプライアンスの問題が見つかれば、コンプライアンス違反事項やそのコンフィギュレーションを一回クリックするだけで簡単に修正できます。

さらに、HyTrust CloudControl には、仮想環境のアクセスを制御するきめ細かな機能があり、ハイパーバイザーに内蔵された役割ベースの従来型アクセス制御がもたらす機能を上まわる制御、セキュリティ、監査機能を提供します。それにより、システム管理者のスコープが定義され、アクセスを限定できるようになります。スコープまたはドメインを特定のアクション、さらに特定のオブジェクトに制限できます。加えて、プライベートクラウド環境の管理機能へのアクセス権限に、より強力な認証制御がもたらされます。例えば、複数ファクタによる認証、ルートアカウントのパスワード保管とローテーション、エンクリプション（暗号化）、キー管理などが活用できます。

セキュリティに重大な影響を与える変更には、二次的認証も可能となり、より強力な制御が実現します。各種コンプライアンスで推奨されるツーパーソン（二名照合）ルールもサポートされます。権限のあるユーザーが実行した処理に関するセキュリティでは、このツーパーソンルールがベストプラクティス（最適手順）とされており、信頼性をより高めると同時に、誤用の危険を減らし、システム管理者による不正、認証情報の悪用など、内部の不正にも対処することができます。さらに、システム管理者の実行した処理が二重に確認され、コンフィギュレーションを誤る危険性も減り、ダウンタイムやセキュリティ侵害の防止につながります。

Boundary Control（境界制御）

ワークロードのセキュリティを確保するために、HyTrust CloudControl は Boundary Control（境界制御）を適用することができます。それにより、VM を置くホストや、VM の起動または移行先ホストを、ワークロードのコンプライアンス維持に必要なセキュリティ要件を満たすホストだけに制限できます。信用できるプラットフォーム、地理的な場所、

ハイパーバイザーのコンフィギュレーションなどを対象に境界制御を適用し、ワークロードを適正に管理するしくみです。VM がどこで稼動し、どのようなデータがアクセスされるのかを、HyTrust がしっかり制御します。

HyTrust CloudControl は、Intel®の Trusted Execution Technology（Intel® TXT[1]）を活用して、ハイパーバイザーの Root of Trust（信頼の起点）を構築します。Intel TXT はプラットフォームを堅牢にして、ハイパーバイザー攻撃、BIOS や他のファームウェア攻撃、悪意あるルートキット、その他のソフトウェア攻撃など、新しい脅威から防御するしくみを備えています。ブートプロセスを隔離して、Measured Launch Environment（MLE）を活用できるのが、Intel TXT の強みです。この MLE において、起動環境のクリティカルな全要素を、正しく稼動することが確認済みのソースと正確に比較し、承認済みコードと合致しないものはすべてブロックすることができます。つまり、HyTrust CloudControl は Intel TXT と連携し、ワークロードが確認済みの健全なホストでのみ稼動するように規制することができます。下図 2 は、Intel TXT の機能を具現化する第三者ソフトウェア（つまり HyTrust など ）と Intel プロセッサーの構成を図示したものです。

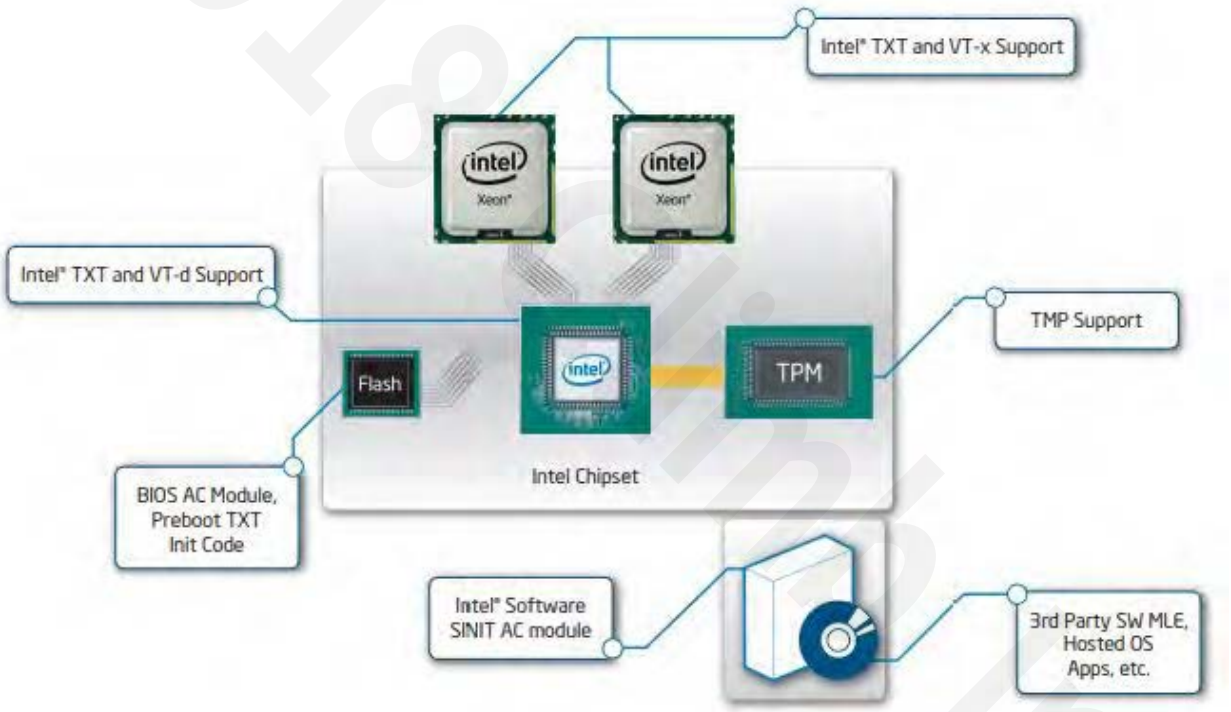

図 2. Intel® TXT の構成（ジェームズ･グリーン、Intel Corporation、2012 年）

[1] Intel は Intel Corporation およびその子会社、関連会社の米国およびその他の国における商標です。

下図 3 は、HyTrust CloudControl が MLE での結果を踏まえて、トラステッド（安全確認済み）プールを構築し、VM のホスト先を見極める環境を図解したものです。

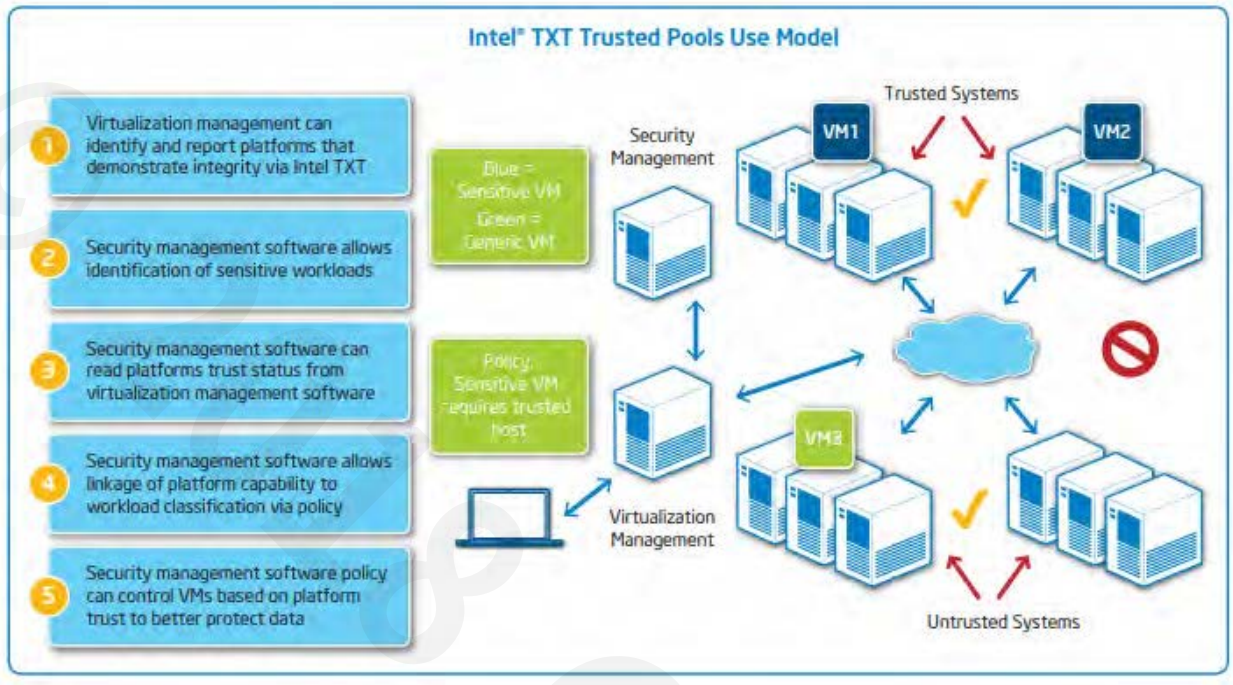

図 3. Intel® TXT トラステッドプールのユースモデル（ジェームズ・グリーン、Intel Corporation、2012 年）

HyTrust CloudControl は、VM を選別されたトラステッド（安全確認済み）ホストに対してのみ適用することができます。そのようなホストをトラステッドコンピュートプールと呼びます。セキュリティポリシーに違反するノードへの VM の移行、あるいは起動を試みても、許可されません。Intel TXT の MLE で審査に合格したホストでも、さらに HyTrust CloudControl で特定のコンフィギュレーション基準に照らして検証でき、そのホストがトラステッドコンピュートプールに加えてもよいものかどうかを決めることができます。

トラステッドホストの定義による境界制御に加え、VM にロケーション制御を適用することもできます。世界各地で事業展開する企業にとって便利な機能です。ワークロードおよびデータのジオロケーションタグにもとづいて、HyTrust CloudControl が VM にジオフェンスを適用し、場所ごとの制限を設けることができます。それにより、ワークロードはあらかじめ認められたロケーションでしか稼動することができません。たとえば、欧州の VM は欧州のホストでのみ起動可能というルールが規定されている場合、Intel TXT を用いたハードウェアタグ、あるいはソフトウェアタグによって European（欧州）と識別されるホストや VM に対して同ルールが適用されます。このしくみは、GDPR をはじめとする各種規制に応用することができます。データがどこで処理されるかを制限することによってデータ保護を強化し、コンプライアンスの徹底が図られます。

HyTrust DataControl

HyTrust DataControl は、マルチクラウド環境におけるエンクリプション（暗号化）とキー管理の自動化を実現します。HyTrust DataControl のエンクリプションは、Intel® Xeon プロセッサーファミリー[2]と Intel® Core™ プロセッサーファミリー[3]における Intel® Advanced Encryption Standard New Instructions（Intel® AES NI）との組み合わせで、高速化されます。プライベートまたはパブリッククラウドを利用する企業が、クラウド上でシステムを運用しながらも、暗号化キーの所有権と制御をプライベートで確保することができます。GDPR の観点から言えば、データ管理者がキー管理を専用に構築して機密データをより確実に制御できることになります。このキー管理機能は、ワークロードセキュリティのより強力な制御を可能にし、KeyControl の管理者はキーのデコミッション（撤収）も安全確実に行えるようになります。

HyTrust DataControl でワークロードが暗号化されると、そのワークロードがクラウド上を、あるいはクラウド間を移動するときも、完全に暗号化されたまま移動します。ワークロードのデクリプション（復号化）は、KeyControl および DataControl のポリシーエンジンを照会した結果、充分な近似性が確認されるときのみ可能になります。VM のデータは、認められている境界を越えて移行されたり、抽出されたもの、そして DataControl のポリシーエンジンに構築されたポリシーに違反するものはアクセスできなくなります。下図 4 は、機密ワークロードの安全確保を図る際の、DataControl と管理者のインタラクションを表しています。

図 4. DataControl を構成する各プロセス

[2] Intel および Intel Xeon は Intel Corporation およびその子会社、関連会社の米国およびその他の国における商標です。

[3] Intel および Intel Core は Intel Corporation およびその子会社、関連会社の米国およびその他の国における商標です。

HyTrust DataControl のポリシーエージェントは VM 内部にあり、機密データが存在するところに直接ポリシーが適用できるしくみになっています。これは、VM や VM ディスクの複製が権限なしに行われ、VM が盗み出されたり、ひいてはデータ全体の不正取得が図られる際に、データを保護し、アクセスを制限するための重要なしくみです。VM があるところはどこでも、そして VM が複製されるときはいつでも、暗号化が解かれないようになっています。

HyTrust DataControl は、一連のワークロード全体を VM ごと、あるいは仮想ディスクごと、さらにはパーティションごとに暗号化することができます。ブートパーティションも暗号化でき、DataControl ポリシーに違反する VM の起動を妨げることが可能です。企業は、機密データを含むディスクを暗号化し、不正アクセスを防止することにより、GDPR 対象のワークロードに防護壁を追加して、セキュリティを強化することができます。

HyTrust CloudAdvisor

CloudSPF の中心的な役割を担うのが、HyTrust CloudAdvisor です。HyTrust CloudAdvisor のサービス機能は、形式化されていない非構造データであっても機密データの識別を可能にします。機密データがどこにあるのか、誰がデータにアクセスし、変更を加えているのか、どのファイルが更新中なのか、いつデータが処理されるのか、など、状況の把握と対策を可能にする有益な情報をもたらします。監査・レポート機能により、機密データが当該環境において、なぜ露出しているのか、客観的な見識が得られ、機密データファイルに誰がアクセスしているかも判ります。このような HyTrust CloudAdvisor がもたらす可視性は、機密データをクラウド環境の保護された境界内で確実に防御することを可能にし、GDPR へのコンプライアンスを目指す企業の大きな力となります。運用ポリシーにもとづいて、機密データを検知し、レポートできるのが HyTrust CloudAdvisor の強みです。

HyTrust CloudAdvisor は、HyTrust CloudControl、HyTrust DataControl、VMware vSphere、そして VMware NSX と組み合わせることにより、機密データ保護の制御体制を万全にします。ポリシー違反への対応、複数の境界を的確に保護するセキュリティは言うまでもありません。境界の保護には、機密データを含むワークロードを安全確認済みの磐石な仮想ホストに移し、不正アクセスを防止することも含まれます。これらの境界において、機密データの暗号化によるセグメンテーションが実行され、境界内における管理体制が強化されます。それにより、権限のあるシステム管理者がセキュリティポリシーを遵守することを確実にします。

HyTrust による GDPR サポート概要

データ管理者（controller）および処理者（processor）が GDPR へのコンプライアンスを確立するに当たって、個人データ漏洩の危険性や深刻度を判定するためのリスク評価を行うことはとても重要です。さらに、データ管理者と処理者にとって、認識されたリスクを GDPR へのコンプライアンスが十分にサポートできる許容範囲まで下げるためのセキュリティ対策に、どの程度の実現性があるのかを判定することも重要です。当文書は、その実現性の要因（例えば、提案された解決策にかかる費用）について意見するものではありません。あくまで、データプライバシーに影響を及ぼすリスクへの対応策に関する意見を述べ、提案された解決策の利点を論じることを主旨としています。

また、当文書に書かれたコールファイア社の意見は、リスクに対応する上で同様に役立つ可能性のある組織的対策には考慮していません。さらに、プライバシー保護の観点から当文書内で述べられている意見は、それが組織的な性質のものか、技術的なものかにかかわらず、GDPR コンプライアンスの一環として個人データの収集や処理に携わるビジネスアプリケーションに組み込める、あるいは恐らく組み込むべき対策を考慮するものではありません。

GDPR の条項には、セキュリティ対策を設計や初期設定に組み込む「バイデザイン・バイデフォルト」のコンセプトに主眼を置くものが多くあります。もちろん、ここで提案される解決策を、セキュリティを中心要素とするインフラ設計の一端を担うものとして捉えることは可能です。同様に、GDPR の規制事項を満たすコンプライアンス要件や一定レベルのデータ保護を確立する追加措置として捉えることも可能です。しかし、セキュリティ対策の「バイデザイン」での実装を、組織の GRC（ガバナンス、リスク、コンプライアンス）プログラムに鑑みて特に示唆する GDPR 条項が多いのも事実です。したがって、セキュリティ対策および予防策の実装は、組織の GRC プログラムを考慮して行われるべきであり、単なる付け足しや臨時的措置として導入されるべきものではありません。ここで提案される解決策は、GDPR の規定条項を満たすために導入すべき、その他のプライバシーおよびセキュリティ対策を補強するものとして有効であると、コールファイア社は考えます。

コールファイア社の評価方法

コールファイア社はベンダーの顧客向けに、その製品やサービスが各種セキュリティおよびコンプライアンス要件をどのようにサポートしているか、顧客理解を助けるための意見書の作成を通常業務としています。当文書は、セキュリティとコンプライアンスの広範な議論に対し、対象範囲が狭く絞られています。

今回の評価において、コールファイア社は 2016 年 4 月 6 日付けの GDPR の法定条項を調査し、提案される解決策に関しては、HyTrust 製品のプレゼンテーションや各種文書の調査を実施しました。調査対象の文書には、製品データシート、リリースノート、インストールガイド、インプレメンテーション／インテグレーションガイド、アドミニストレーションガイド、ユースケースなど、HyTrust が提供する、あるいは HyTrust ウェブサイトで一般公開されている各

種情報が含まれます。さらに詳しい情報が必要な場合や不明な点の解明に、HyTrust 製品の専門家や GDPR の専門家に対する聞き取り調査も実施しました。これらの総合的な調査にもとづき、コールファイア社は、HyTrust に実現され、使用されるソリューションの各種機能が GDPR の規定事項にどのように対応するのかを評価し、その機能性を記述しました。

コールファイア社は、制御環境にモデル化したワークロードのセキュリティを確保し、GDPR コンプライアンスをサポートする各種機能を実演するために使用した参考アーキテクチャ自体の検証は行っていません。

コールファイア社の調査結果

当文書は主として、Intel プロセッサーを基盤とする VMware vSphere プラットフォームにおける HyTrust ソリューションの運用に焦点を当てています。それによって実現される技術的なセキュリティ対策の、GDPR の提示する各種要件の解決に向けた可能性を探ります。HyTrust の掲げるソリューションは、データプライバシーを推進する企業がセキュリティを確保するための技術的な方策の一部として論じられるのにふさわしいと、コールファイア社は考えます。GDPR のすべての規定条項に広範に適用できるわけではありませんが、IT インフラに対する数々の一般的な脅威への対策として有効な面もあり、企業システムが不正使用された場合に IT インフラが晒される脅威への予防策として検討に値します。

そのような脅威の一端に、機密データの所在が把握できていないという問題があります。形式化されていない非構造データとして環境内に存在する機密データは、どこにあるのか識別が困難です。HyTrust CloudAdvisor は、企業の制御領域内に潜む非構造の機密データを見つけ出し、データプライバシーのリスクに晒されている企業に以下の機能をもたらします。

- 機密データの場所を特定
- 機密データへのアクセス者を監視
- 機密データに関するコンプライアンスの監査レポート

機密データの場所を知ることにより、そのデータが設定された境界（バウンダリー）制御の域外にある場合など、GDPR コンプライアンス違反を確認・修正することができます。HyTrust CloudAdvisor は、機密データの企業インフラにおける論理的な場所と地理的な場所のどちらも識別可能です。論理的および地理的境界を設定し、EU 加盟国民のデータがそのいずれかの域外に保管・処理・転送されるときには、HyTrust CloudAdvisor によりポリシー違反が確認され、その修正が図られます。

HyTrust CloudAdvisor は、HyTrust DataControl、HyTrust CloudControl、VMware vSphere、そして VMware NSX との連携により、GDPR 準拠が必要な状況におけるセキュリティ制御を自動的に確立します。そ

れにより、企業・団体は、アプリケーションのアクセス制御や、エンクリプション（暗号化）、ジオフェンス、マイクロセグメンテーションを機密データに適用可能になり、セキュリティを強化できます。

HyTrust DataControl は、VM、VM ディスク、VM パーティション、さらには管理 VM 内の規制対象ワークロードの要素となるファイルを暗号化することができます。保存データが暗号化されていれば、たとえシステムが悪用され、暗号化済みのデータが不正に取り出されても、それを復号化するプライベートキーなしでは、データが不正利用されることはありません。企業インフラとそのデータの機密情報を暗号化すれば、個人データが不正に露出されるリスクが削減され、セキュリティ侵害の通知作業も削減される効果が期待できます。

GDPR においてデータ保持を論じる場合、それはファイルやファイルシステムではなく、レコード単位のデータ保持に主眼を置いています。ハードウェアの処分や再利用によるデータ漏洩リスクに対しては、HyTrust DataControl のキー裁断（シュレッディング）を用いることにより、データをディスクに残したまま取り出し不能にすることができます。データ保持ポリシーに準じた適正な消去メカニズムに時間制限を設ける必要がある場合、キーシュレッディングなら時間によるデータ消去を自動化できます。さらに、ポリシーに則った処理の記録がレポート機能によって残され、コンプライアンスを実証してくれます。

GDPR は、EU 加盟国民の個人データの処理が可能な場所を地理的に制限しています。そこで、HyTrust CloudControl は、Intel TXT との組み合わせにより、個人データを含むワークロードをジオセグメント化（地理的細分化）し、境界制御を適用することができます。クラウドコンピューティングがもたらした柔軟性は計り知れず、ワークロードのホストやプロビジョン、さらにスケールしたり拡充することが容易になりました。このようなクラウドコンピューティングの多くの機能に見られるダイナミックな特性は、コンプライアンスの管理やモニタリングを複雑化させています。特に、場所に関するコンプライアンスの複雑化は顕著です。ワークロードを発見・識別し、コンプライアンスに準じた運用環境でのみ稼動させる HyTrust CloudControl の機能は、このような課題への有効な対策となります。

そして、HyTrust CloudControl はコンプライアンスに準拠した環境を地理的な場所で定義するだけではなく、コンフィギュレーションチェック機能によって定義することも可能です。ハイパーバイザーと VM がワークロードを実行させるのに安全な環境であるか、最低基準を満たしているかどうか、確認することができます。つまり、ワークロードの起動、実行、移行が、総合的な判断によって決断されます。HyTrust CloudControl のポリシーが適用されている限り、制御対象の VM がコンプライアンスに準拠していないホストで起動、実行、移行されることはありません。制御の境界を越えての VM 移動では、HyTrust DataControl がデータの暗号化により、承認済みのホスト環境以外での許可のないアクセスを遮断します。そして、HyTrust CloudControl のログ機能が環境内の全処理を記録し、監査や報告の要件も満たされます。それにより、セキュリティ担当者がポリシー違反行為をすぐに発見し、それに対して発動される防止策を把握して個々の事例に的確に対応することが可能になります。

CloudSPF が提示するセキュリティ対策の枠組みは、システム管理者に適切な指針を提供します。アラートを受け取り、ワークロードのマイクロセグメンテーションによってネットワークを隔離し、ワークロードの安全性をより高めることができます。さらに、ワークロードを信頼できるホストに移し変えるなど、総合的なアプローチが可能になります。また、この枠組みの中で、HyTrust CloudAdvisor は HyTrust CloudControl に指示を送り、バウンダリー管理のガバナンスを徹底させることができます。下図 5 は、CloudSPF が VMware の仮想データセンターにおいて施行可能なバウンダリー管理を表しています。

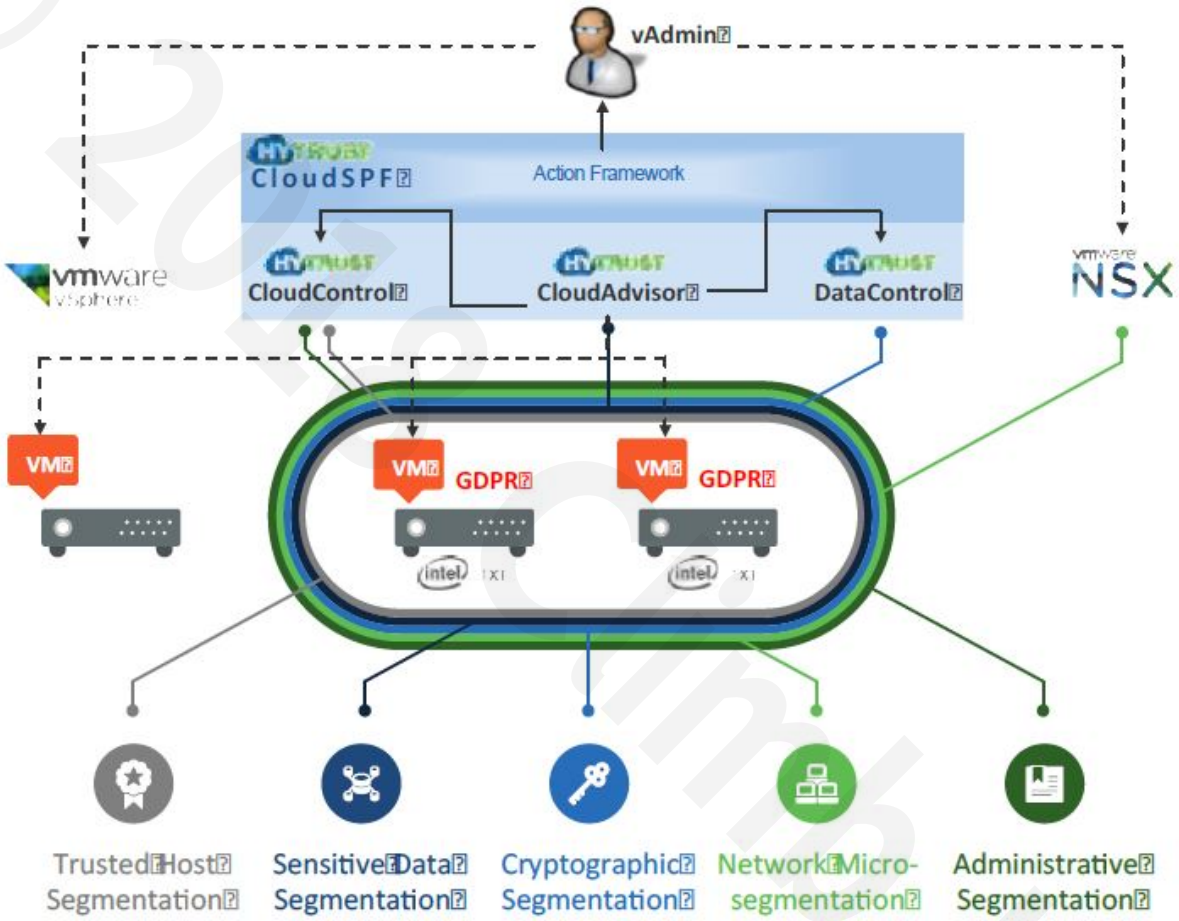

図 5. CloudSPF が実現する仮想データセンター内のバウンダリー運用

現行システムの処理・サービスにおける機密性、整合性、可用性、弾力性を確保するには、ソリューションの組み合わせが重要です。中でも、セキュリティ制御機能が果たす役割は幅広く、それを欠くと、脆弱性に付け込まれてインフラへの侵害を被る危険性があります。GDPR 規制対象のワークロードをサポートするインフラの場合、機密データの漏洩につながりかねません。

HyTrust のソリューションを GDPR の規定事項へ応用する上で、コールファイア社は以下の各条項への適用が可能であると判断しました。

第 5 条	個人データの処理に関する原則
第 6 条	データ保持／最小化および領域に関する処理の適法性
第 24 条	データ管理者（Controller）の責任
第 25 条	データ保護 by デザイン・データ保護 by デフォルト（設計・初期設定からデータ保護）
第 28 条	データ処理者（Processor）
第 30 条	処理アクティビティの記録
第 32 条	処理のセキュリティ
第 33 条	個人データ侵害の監督当局への通知
第 34 条	個人データ侵害のデータ主体への連絡

基本的に、セキュリティ境界保護メカニズムの適用は、クラウドインフラやアプリケーションプラットフォームを通じた個人データへのアクセスを最小限に抑え、データの露出を制限する上で、有効なコンセプトであると言えます。

下記の表は、GDPR におけるデータプライバシーの規制条項に対応する HyTrust CloudSPF の機能性を示しています。表中の CC は HyTrust CloudControl を、DC は HyTrust DataControl を、BC は Boundary Control（境界制御）を、CA は HyTrust CloudAdvisor を表します。ホストの堅牢化と安全性を確立する HyTrust CloudControl の機能性は、Intel TXT によるハードニングのサポートを前提としています。また、Boundary Control（境界制御）による地理的な境界設定に関しても、Intel TXT の機能との組み合わせによって論理的な識別と物理的なジオタグが適用されることを前提としています。さらに、HyTrust DataControl による暗号化では、効率性とセキュリティを高めるために、Intel プロセッサーにおいて Intel AES NI が活用されることを前提としています。

HyTrust サポート欄には、CloudSPF の既存の要素にはなく、追加の検討に値すると思われる機能や要件を「補足検討事項」として追記してあります。

EU 一般データ保護規則（GDPR） ― 2016/679				
条	条文見出し		項	HyTrust サポート
5	個人データの処理に関する原則	CC	5-1.(f)	権限のある管理者がその権限を越えて（許可なしに）VM を制御するのを防止し、管理者の行動を監査。GDPR の規定に沿った組織（企業）ポリシーにもとづいてホストを堅牢にし、セキュリティを強化。
		DC	5-1.(f)	データ保管上のリスクを最小限に抑える ― デクリプションをいつ、どこで行うかを制限。キー断裁による完全データ消去を必要なときすぐに実行可能。

		BC	5-1.(f)	機密データおよび VM のデクリプション可能領域（境界）を制限
		CA	5-1.(f)	非構造の機密データを識別し、その用途を追跡。保護を発動。非構造ファイルにおけるデータの不慮の露出を防止。
		補足検討事項		データ管理者／処理者のリスクを審査し、GDPR に則り、適切な技術的・組織的予防策を決定してリスクをなくす、あるいは減らす追加制御機能の必要性。
6	処理の適法性	DC	6-4.(e)	VM 全体、VM 上のディスク、パーティション、ファイルベースでファイル上の OS を暗号化する手段を提供。
		BC		HyTrust CloudControl から適用可能。HyTrust DataControl で暗号化された VM のデクリプション可能領域（境界）を制限。
		CA		継続的な処理の中でエンクリプションをサポート。形式化されていない非構造データでも個人データを識別でき、HyTrust DataControl に必要なエンクリプションを指示。
		補足検討事項		個人の承諾なしで、あるいは目的明確化の原則を超えての処理を検討するデータ管理者は、エンクリプションを継続的処理のリスク査定要素と見なす可能性あり。 データ管理者は、本来のデータ回収目的を超えた形でも処理の適法性を確保するために、データプライバシーのリスク軽減策として、データの匿名化などの他のオプションを検討する可能性あり。 第 6 条の主旨はレコードレベルでのデータプライバシー保護であり、典型的には、データプライバシーを機能として組み込んだアプリケーション設計によって達成される。
24	データ管理者（Controller）の責任	CC	24-1.	権限のある管理者に対するガバナンス、ホストインフラのハードニングなど、データ保護のためのセキュリティ策を提供。 ホストハードニング（セキュリティ強化）のため、技術的ポリシーの継続的な確認メカニズムを提供。
		DC	24-1.	GDPR 規制対象の保存データや OS イメージのエンクリプションにより、VM および VM ストレージのデータを保護。
		BC	24-1.	GDPR 規制対象の機密ワークロードが信頼性証明済みのホストでのみ稼動するよう制限。さらにデータのデクリプション可能領域（境界）を制限。それにより、ワークロードの実行とデータアクセスをサポート。
		CA	24-1.	ファイルの非構造データを積極的に検査し、機密データを含むファイルの存在や作成を確認、その使用法を監視して、以下のいずれかのデータセキュリティ策を発動。 • エンクリプションによりデータを隔離 • マイクロセグメンテーションにより VM を隔離

				• VM をトラステッド（安全確認済み）ホストに移行 • ACL（アクセス制御リスト）アプリケーションでファイルへのアクセスを遮断
		補足検討事項		データ管理者／処理者のリスクとプライバシー影響評価に関する発見にもとづいて、追加の技術的および組織的予防策を保証する可能性。
25	データ保護 by デザイン・データ保護 by デフォルト（設計・初期設定からデータ保護）	DC	25-1. 、25-2.	エンクリプションにより、GDPR 対象データへのアクセスを制限（アクセス可能領域・可能期間の設定）
		BC	25-1. 、25-2.	GDPR 対象データのデクリプション可能領域（ホスト、データセンター、地理的場所）を制約
		CA	25-1. 、25-2.	GDPR 対象データを含むファイルおよびファイルアクティビティを監視し、使用されていないファイルをデコミッション候補として識別。
		補足検討事項		「データ保護 by デザイン・by デフォルト」は、総括的な組織的ガバナンス設計への考慮事項。製品・サービスの新規設計または変更導入時に最初の段階からプライバシー・データ保護への考慮を要件とするもの。HyTrust による保護メカニズムは、組織的制御のいくつかの面に準拠する方策と見なし得る。また、防御の徹底戦略の一要素と見なし得る可能性あり。
28	データ処理者（Processor）	CC	28-1. 、28-3.(h)、r-81	システム管理者のアクティビティを制御（ロールベース）。仮想化ホストを堅牢化。コンプライアンスを示す監査証跡。
		DC	28-1. 、28-3.(g 、h)、r-81	共有インフラにおけるキーのマルチテナント分け、エンクリプションを提供。さらにキー裁断によるデータの削除を可能に。
		BC	28-1. 、28-3.(h)、r-81	GDPR 対象のワークロードを選別されたホストでのみ稼動させ、コンプライアンスを詳述するレコードを完備。
		CA	28-1. 、28-3.(h)、r-81	GDPR 対象データを含むファイルの用途を識別・記録。
		補足検討事項		HyTrust ソリューションは、その機能がデータ処理者のデータ管理者に対する責務遂行を可能にし、その一部をまかなう上で、GDPR 対象の環境に制御をもたらし得る。それは、より広範なプライバシー・セキュリティ規範の一部を成す。データ処理者からデータ管理者への報告義務のセキュリティ要件達成度を確認する上で便利な要素となり得るが、それ自体がすべての目標を満たすのに充分とは言い切れない。
30	処理アクティビティの記録	CC	30-2.(c)	ロールベースアクセス制御（RBAC）により、承認済みデータセンターのみへの移行を許可（監視）
		DC	30-1.(f) 、30-2.(c)	GDPR 対象データのエンクリプションによる保護、迅速な消去、それらを記録してコンプライアンスを実証。
		BC	30-2.(c)	GDPR 対象の機密ワークロードが稼動し得るホストのデクリプションを制限し、非承認ホストへのデータ露出を防止。
		CA	30-1.(c 、	GDPR 対象データを分類して、エンクリプション、ガバナンス、迅速な

			f) 、 30-2.(c)	消去を促進。そのような保護処理の記録を保持。
32	処理のセキュリティ	CC	32-1.(b 、 d)	ロールベースアクセス制御をポリシーとしてデフォルトで実装。その効果を測るハードニングスキャンを継続的に実行。
		DC	32-1.(a 、 b)	GDPR 対象の保存データのエンクリプションによる機密性確認ポリシーをデフォルトで実装。
		BC	r-77、r-78	非承認ホストへのワークロードの配置・実行と GDPR 対象データのデクリプションを阻止。
		CA	32-1.(a 、 b、d)	GDPR 対象データをエンクリプション向けに積極的にスキャンしてセキュリティ策の有効性を定期的にテストし、必要な保護を発動。
		補足検討事項		HyTrust ソリューションはコンプライアンスを徹底するための制御の枠組みの一部を成し得る。企業・団体には、技術的・組織的予防策を含むより広範なセキュリティ制御の枠組みを用いた包括的セキュリティプランが必要。偽名化に関し、エンクリプションは非承認公開リスクをある程度軽減し、データが復号化キーなしで露出された場合のセキュリティ侵害通知をサポート可能。32-1.(a)における偽名化は、個人データを扱うビジネスアプリケーションの機能、およびプログラミング的手段による不正アクセスの防止により特定される。
33	個人データ侵害の監督当局への通知	DC	33-1.	データが暗号化されている場合、データ侵害の監督当局への通知は不要。ただし、企業・団体は、データ侵害において、暗号化キーが被害を受けていないことを証明する必要あり。
		CA	33-1.	GDPR 対象のデータを積極的にスキャンし、保存データを暗号化することにより、多くのデータ侵害リスクを軽減。
34	個人データ侵害のデータ主体への連絡	DC	34-3.(a)	当該データが暗号化されている場合、データ侵害のデータ主体への通知は不要。
		CC	34-3.(a)、 r-87	データ侵害発生時、当該データの特徴を特定し、露出した可能性のある GDPR 対象データの範囲を確定。
		補足検討事項		企業・団体は、HyTrust のエンクリプションでは保護し切れない方法でデータが露出された場合における他の違反通知の必要性も考慮すべき。

表 1. CloudSPF 概要と GDPR への適用性

CC＝HyTrust CloudControl、DC＝HyTrust DataControl、BC＝Boundary Control、CA＝HyTrust CloudAdvisor

まとめ

UE 一般データ保護規則（GDPR）の発効により、EU 在住者データのセキュリティとプライバシーを保護する適切な技術的および組織的方策を講じることが義務付けられました。それを実証できない企業・団体は、欧州のデータ

保護監督機関から甚大な罰則を受けることになります。GDPR は、データ主体（対象となる個人）の管轄区域を考慮したソリューションを、企業・団体が設計すべきである点を強調しています。そのような設計には、同時に、現代の企業ニーズを満たす柔軟性も求められます。HyTrust CloudControl、HyTrust DataControl、HyTrust CloudAdvisor の三本柱から成るソリューション CloudSPF は、仮想データセンターにコンプライアンスポリシーの的確な施行を実践し、より広範なバウンダリー（境界）保護を適用することにより、アプリケーションとデータの安全確保を促進するのに有益であると言えます。企業・団体のプライバシー影響評価に応じて CloudSPF の制御機能を活用すれば、その技術的戦略によって、欧州在住者のプライバシーへの影響が最小限に抑えられるはずです。

〒103-0014 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　FAX: 03-3660-9337

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