KASPERSKY lab ENTERPRISE

伸縮性の高いハイブリッドクラウド用に設計されたボーダーレスのセキュリティ

Kaspersky Hybrid Cloud Security

www.kaspersky.com
#truecybersecurity

ハイブリッドクラウド環境用に設計されたボーダーレスのセキュリティ

データの流動性は高まるばかりです。データは、常に企業の IT の境界を越えてモバイルデバイス上を移動し、また、物理マシンに加えて仮想マシンでも処理されるようになっています。さらに、パブリッククラウドやマネージドインフラストラクチャにも取り込まれるようになったことで、オフプロミスとの間でデータの移動が飛躍的に増加しています。

伸縮性の高いクラウドサービスモデルを導入する企業が増えています。このクラウドモデルは、プライベートデータセンターのリソースがオンデマンドおよび必要に応じて瞬時に外部のクラウドへと拡張されるものです。このモデルの導入によって、極めて高い柔軟性、俊敏性、明確な経済的利益が得られます。インフラストラクチャへの先行投資は不要で、無駄もなく、必要なリソースの要求にも迅速に対応でき、管理業務も容易に行えます。

パブリッククラウドには、さらにもう 1 つのメリットがあります。それは事業継続性です。データセンターのサービス提供が中断してしまった場合や損害を被った場合に、問題が修復されるまで、オフプレミスのリソースによって運用を継続できます。パブリッククラウドのプロバイダーも、自社の事業継続性とサイバーセキュリティに多大な投資を行い、利用者のビジネスワークロードを安定して運用できるよう安全で継続性のあるクラウド環境を構築しています。しかしこれで安全というわけではありません。

クラウドを採用する上でのセキュリティの課題

- 物理、仮想、クラウドベースの各ワークロードを攻撃するマルウェアとランサムウェアの存在
- 予防型ではなく事後対応型セキュリティアプローチに起因したデータ侵害
- インフラストラクチャの複雑化による透明性の低下
- 管理やツールが散在していることによる管理上の課題
- 従来型のセキュリティソリューションによるシステムリソースの浪費
- 保護が不十分なプライベートデータセンターで保存されているデータ
- DoS 攻撃による事業継続性の中断やデータ交換の阻害

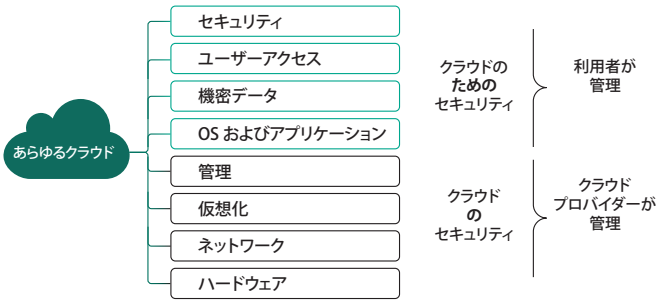
パブリッククラウドで保管されているデータは安全か

この質問に対する答えは期待しているものとは違うかもしれません。

現在のパブリッククラウドは、非常にセキュアな場所です。外部クラウドの内外で、常にホスト環境にデータが確実に格納されるよう、さらに漏えいの危険性がないようにするために、細心の注意が払われています。

しかし、データがセキュアに格納されているからといって、必ずしも安全であるとは限りません。データ漏えいは、セキュリティの一側面に過ぎません。たとえば、ランサムウェアによって感染したファイルが気づかれることなく、利用できない状態でファイルが保管され続けます。また、ビジネスにとって企業の情報資産であるデータは、人がデータにアクセスする限り、人為的なミス、また意図的に悪用される可能性があります。

セキュリティ責任共有モデル

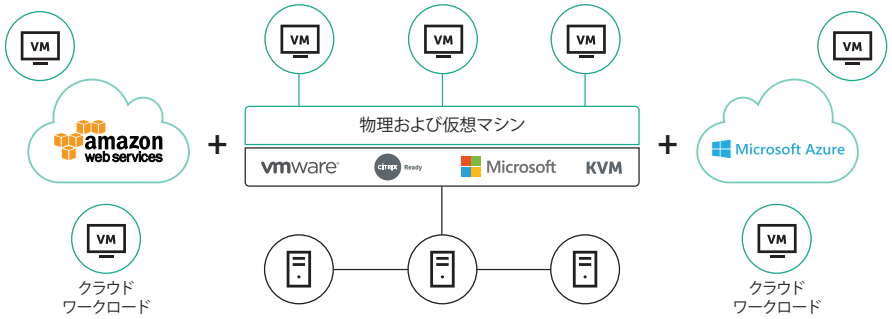


ホステッドクラウドサービスプロバイダーは、提供している環境のセキュリティについての責任を負いますが、各ワークロードの内部的なセキュリティについては、そのワークロードがどこにあろうとも、依然として利用者に責任があります。これは「セキュリティ責任共有」モデルとして知られています。このモデルは、利用者とサービスプロバイダーが、現在有効な関係および利用者のデータ資産のセキュリティについて、それぞれ別の側面の責任を担うというものです。

したがって、「パブリッククラウドで保管されているデータは安全か」に対する答えは、良くても「他の場所と同程度にセキュアである」というものになります。同様のセキュリティの懸念事項は、データがどこに移動しようが、そのすべてに適用されます。あらゆる時点でのデータの保存先を保護するだけでは、データを保護することはできません。この事実を認識することの重要性は高まっています。それは、ますます多くのビジネスクリティカルなデータが、管理された企業 IT 環境を越えて、より広い範囲を移動するようになっているためです。

データの周囲だけでなく、データ自体を保護する

すべてのデータパッケージを、どの時点においてもどこにあっても、移動中でも、内部から保護する必要があります。それが企業としての責任であり、この責任についてはアウトソーシングも委託もできません。



ワークフローを保護するにはワークフローのオーケストレーションが必要

ここで 1 つ目の質問です。データパッケージの一つひとつについて、どの時点でどこに存在するか、あるいはどこへ移動中か、またそのデータを操作しているのは誰か、正確に把握していますか？

アクセスのコントロールと監視は、現在直面しているセキュリティ問題の 1 つです。IT インフラストラクチャが大規模で複雑であればあるほど、効率性とシステムパフォーマンスを最適化するためのソリューションがより多く必要になり、ワークロード、あるいはアプリケーションでさえも、一つひとつを追跡することが難しくなります。データセンターのインフラストラクチャを拡張して外部のリソースを取り込む場合、この問題はさらに困難を極めます。オンプレミス、オフプレミスを問わず、アクセス中および処理中のデータとその方法を確実に特定できることが不可欠です。

ワークフローを保護するにはワークフローの堅牢化が必要

今起きていることを把握できていますか？ どのアプリケーションがどこで実行中ですか？ また、すべてのアプリケーションが想定どおりにふるまっていますか？ アプリケーションのぜい弱性は依然として、サイバー犯罪者に利用される、侵入や感染の主な手段となっています。このような侵入や感染を防ぐための多層のテクノロジーを配備することで、システムの堅牢化が実現されます。特定のアプリケーションの禁止や制限、組織内で実行中の全アプリケーションのふるまいの継続的監視、悪用からのぜい弱性の保護など、これらの重要な脅威防止/検知の管理と処理のすべてが、データ所有者の責任になります。

組織を保護するにはデータの保護が必要

実行中のデータを保護するためには、潜在的な攻撃や実際の攻撃をいつ、何から受けているかを検知できる必要があります。特定の企業を標的とした APT（Advanced Persistent Threat）から、隙があればつけ込むランサムウェアまで、あるいはデータの盗難や金融詐欺から偶然に起きる人為的ミスまで、データに対する脅威はあらゆる形式と規模で襲ってきます。さらに、サイバー犯罪が大きな利益を得られる高度な業界となった今、新しい攻撃手法が続々と開発され応用されています。

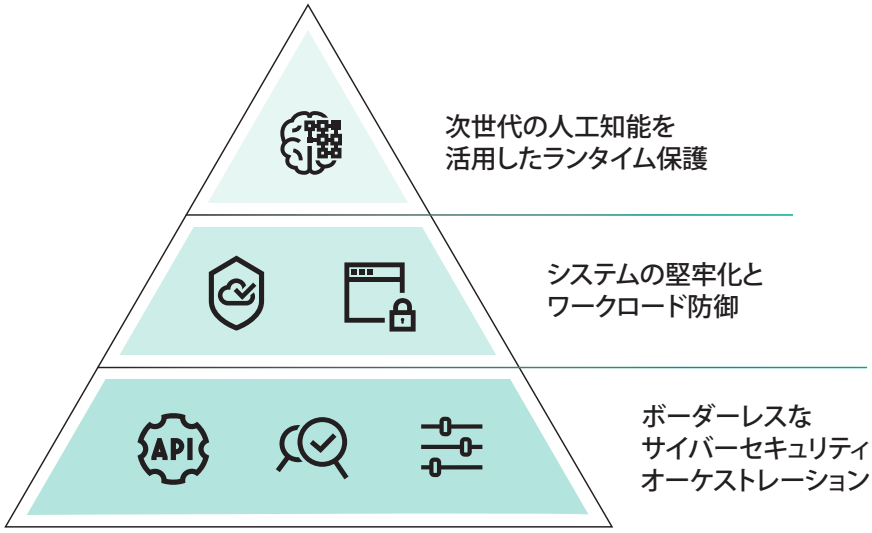
クラウド内のデータに当てはまることは、すべてのデータにも当てはまります。つまり、企業のセキュリティシステムが依存している脅威インテリジェンスの品質、およびそのアプリケーションの適時性と正確性が、継続的な保護の効果を決定付けるものとなっています。企業の IT セキュリティシステムは、潜在的な脅威がデータに到達して業務に影響を及ぼす前に、その脅威を特定し、ブロックし、対処できる必要があります。さらに、それを行う際には、システムパフォーマンスを損なわないこと、そして重要なこととして、「誤検知」を出さないことが求められます。誤検知を出すと、誤ったアラームによって業務が中断され、リソースが無駄に消費されることになります。

繰り返しますが、これらはすべてデータ所有者の責任です。現状、クラウドサービスプロバイダーができることはデータの保護だけで、それ以外はすべて利用者に委ねられています。

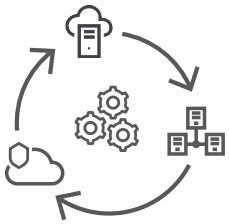
ハイブリッドクラウドデータセンターの保護に関して何を求めるべきか

端的に言えば、ワークロードを稼働させるための完結したセキュアな環境を提供する、外部のデータホスティングソフトウェアプロバイダーを頼ることはできます。しかし、データがどこにあっても、その一つ一つを監視し、管理し、保護するのは、データを所有するユーザーの責任となります。

Kaspersky Lab では、セキュリティの責任に関するこれら 3 つの側面を、「サイバーセキュリティのオーケストレーション」、「システムの堅牢化」、「ランタイム保護」と呼んでいます。以下に示す多くの相互に補完しながら連動するテクノロジーによって、これら 3 つのセキュリティ層のそれぞれを実現しています。



ハイブリッドクラウド環境を保護するためのソリューションを決定するときには、特に次のような要件を含めることを推奨します。



ボーダーレスのオーケストレーション

クラウド API：ネイティブ API 経由でのパブリッククラウド（AWS、Microsoft Azure など）との統合。これによりインフラストラクチャの探索、自動セキュリティエージェントのデプロイ、ポリシーベースの管理が可能になります。

アカウント管理：セキュリティ担当者と管理者に、サイバーセキュリティコンソールの特定領域にアクセスするために必要な権限を付与することで、クラウドベースのマシンを厳格に管理して、運用面での予防効果を向上させます。

ロールベースのアクセスコントロール：割り当てる運用上の役割に応じて、インフラストラクチャ担当チームとセキュリティ担当チームに、ハイブリッドクラウド環境のサイバーセキュリティ層に対する異なるレベルのアクセスとコントロールの権限を付与できるようにします。

システムの堅牢化

アプリケーションコントロールとホワイトリスト：いつ、どこで、どのアプリケーションを実行できるかを管理（または禁止）することで、攻撃対象領域を減らします（Kaspersky Lab は独自の「ホワイトリストラボ」を運営しており、このラボで顧客がどの時点においても安全に実行できるアプリケーションを明示しています。これによって、必要に応じて非常にセキュアな「デフォルト拒否」ポリシーを実装できるようにしています）。

ぜい弱性の保護：ぜい弱性攻撃ブロック、ぜい弱性評価、自動パッチ管理（Kaspersky Security for Hybrid Clouds に含まれている機能です）など、ユーザーが利用している広く一般に利用されているアプリケーションに潜むぜい弱性経由でのシステムへの侵入を防ぐ技術です。

ランタイム保護

ランサムウェア対策：メール、Web のマルウェア対策を含む、ランサムウェアの侵入・感染を防止する機能。Kaspersky Hybrid Cloud Security には、「自動ロールバック」も組み込まれているため、破損したファイルはすべて自動的に以前の暗号化されていない状態に戻ります。

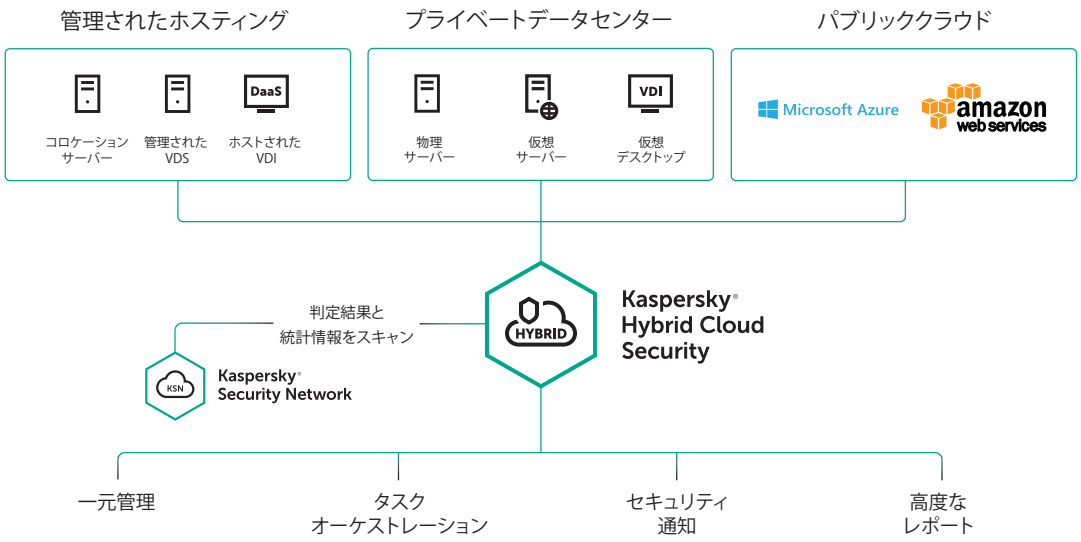
高度な脅威インテリジェンス：高品質のリアルタイム脅威インテリジェンスにアクセスして、システムとデータ保護メカニズムに適用できる機能。

中でも脅威インテリジェンスは最も重要な機能です。このインテリジェンスは、人工的なインテリジェンス、すなわち、ソフトウェアやふるまいの異常を特定して、これまでに遭遇したことのない脅威を認識し特定するシステムの能力を指しています。このインテリジェンスは、機械学習とふるまい分析を含む技術の組み合わせ、クラウドベースのインテリジェンスデータベースの活用、およびエキスパートによる分析により実現します。

この未知の脅威を特定し、その脅威から防御する能力は、データセキュリティの確固たる基礎となるものです。当社が「HuMachine®（ヒューマシン）インテリジェンス」と呼ぶ、専門家と専門システムが融合して対処するレベルのセキュリティでなければ、他のセキュリティ技術をいくつ適用したとしても、データは将来の攻撃に対してぜい弱な状態になります。Kaspersky Lab のソリューションは、このマシンインテリジェンス（当社は 10 年にわたって機械学習を当社の技術に組み込んでいます）と当社の最高レベルの専門知識の組み合わせを基に構築されています。そのため、現在だけでなく将来の脅威をも検知し、特定し、ブロックすることができます。

必要な保護機能を実装し洗練されたクラウドセキュリティ

Kaspersky Lab の Hybrid Cloud Security ソリューションは、上記のすべての機能の他、多数の機能も備えることで、適応型のセキュリティ環境を提供し、最も高度な脅威からハイブリッドクラウド全体を保護します。



セキュアで伸縮性のあるクラウド環境を利用するために
ハイブリッド環境はビジネスによって大きく変わります。変わり続ける運用環境の進化と規模拡大に合わせて、セキュリティを迅速に適応させる必要があります。

- 端から端までを網羅する高品質の保護のために、クラウド環境全体にわたって可視性を強化
- 人とマシンが併せ持つ力を活用して、高度なサイバー脅威を検知し、それに対応
- 複数のコントロールによって、クラウド上のワークロード、システム、ネットワーク、データを保護

１つの製品であらゆるクラウドを保護
大規模なハイブリッドクラウド環境向け次世代型サイバーセキュリティを実現するように設計されたソリューションです。

- 物理サーバー、仮想サーバー、VDI、ストレージ、さらにプライベートクラウド内のデータチャネルにも対応する、実績のあるセキュリティ
- パブリッククラウド（AWS、Azure など）のワークロードに対応する高度なセキュリティ管理
- サイバーリスクを最小限に抑えることで、エンタープライズ用の継続的なサービスレベル目標（SLO）を達成

シームレスなセキュリティエクスペリエンス
IT およびセキュリティの透明性と横断的な統合により、既知の脅威、未知の脅威、最新の脅威に対する防御力が向上します。

- クラウドのコア技術とセキュリティ層をネイティブ API によって統合
- セキュリティの自動プロビジョニングによって、セキュリティのレベルを損なうことのないクラウド移行が可能
- あらゆるクラウドに対応するシームレスなエンタープライズレベルのセキュリティオーケストレーション

Hybrid Cloud Security ソリューションに実装されている先進的な機能によって、インフラストラクチャ層とセキュリティ層が統合され相互に運用されます。それぞれの強みを組み合わせて安全で効率的な環境を作り出し、プライベートクラウドとパブリッククラウド間でのワークロードのボーダーレスな移行が可能になります。その結果、継続的で、弾力性と透明性があり、管理が容易なセキュリティが実現し、ビジネスニーズに合わせたハイブリッド環境を構築できるようになります。

まとめ

外部で運営されているクラウド型ホスティングサービスを活用することはビジネス的に多くのメリットを享受でき、組織のデータを安全に保存し処理できるセキュアな環境を構築できます。しかし、ワークパッケージのセキュリティは、データ所有者の責任として残っています。当社は、お客様がデータ、プロセス、アプリケーションをいつでも完全に可視化して管理できるようにし、HuMachine® ベースの高度な脅威インテリジェンスをデータ保護に適用することで、ハイブリッドクラウドデータセンターのあらゆる側面でセキュリティを確保できるようにしています。

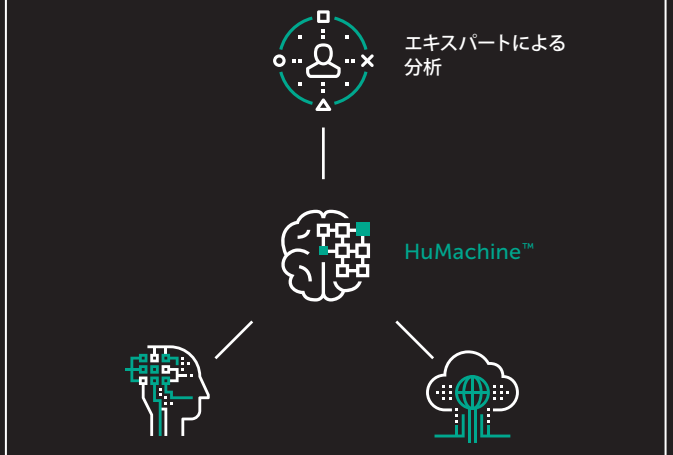
株式会社カスペルスキー

企業向けサイバーセキュリティ：www.kaspersky.co.jp/enterprise/
サイバー脅威に関する最新情報：www.securelist.com
IT セキュリティに関する最新情報：blog.kaspersky.co.jp
ご購入相談窓口：jp-sales@kaspersky.com

#truecybersecurity
#HuMachine

www.kaspersky.co.jp

© 2018 Kaspersky Lab. All rights reserved.
Kaspersky およびカスペルスキーは Kaspersky Lab の登録商標です。
その他記載された製品名などは、各社の商標もしくは登録商標です。
なお、本文では、®は記載していません。



PMM-1025-201808