Climb Inc.
Growing to Meet Your Needs

# HyTrust CloudAdvisor for Data

## 仮想環境で機密データの識別・分類・安全確保

2017 年 10 月

株式会社クライム

# 目　次

## HyTrust CloudAdvisor for Data の機能

- 仮想マシン（VM）に保存された機密データや取り扱い要注意の重要データを識別
- インストールとディプロイがすばやくできる仮想アプライアンス
- VMware vCenter および Veeam Backup & Replication をサポート
- ファイルの利用状況・内容・場所を緻密に分析し、データの的確な分類を実現
- データやユーザーのアクティビティを時系列を追って調査し、プロファイルを構築
- ファイルの内容を MIME タイプ、サイズ、場所、内容、休止状況、ファイルメタデータ、所有者にもとづいて分類
- クレジットカードデータ、社会保障番号（マイナンバーなど）、健康保険情報などを検知するルールをあらかじめ定義
- 特定キーワード、文字列、カスタムデータフォーマットを検知する特別ルールを独自に定義
- 仮想マシン（VM）を分析して、ユーザーアクティビティを時間ごとにファイルベースで識別
- ビヘイビアベースの検知機能（行動・振る舞いをもとに検証）で、不正または異常行動発生時にデータスナップショットを自動生成

## HyTrust CloudAdvisor for Data の効果

- 誰がデータにアクセスして、どのように使用しているのかを確認可能
- 機密データや重要データの検出・保護を自動化
- 各 VM ファイルの使用状況、内容、場所に関する詳細を取得
- データ検出ルールをビジネスのニーズに応じて自在に調整
- 稼働中か停止中にかかわらず、VM を分析
- 異常行動を検知することにより、不正アクティビティに対する防御を確立
- マルウェアや悪意あるユーザーアクティビティにより失われたファイルを即時に特定して復元
- 社内外のコンプライアンス事項をサポート

## 企業データ拡散のセキュリティリスクを軽減

企業や団体におけるデータ管理の重要さとそのリスク、特に機密データが不正利用された場合にその事業が被る潜在的な損害の大きさは周知の通りです。業務上欠かせない重要データが制御不能な状態で、各スタッフのラップトップやネットワークドライブはおろか、仮想環境やクラウドストレージなど、ほとんど無限とも言える広大な空間に瞬く間に

広がって行きます。そのような重要データには、顧客取引、クレジットカード、知的財産などの機密情報が含まれ、ストレージバックアップや社内連携用のデータシェア、ワークロード、仮想マシン（VM）クローンなど、様々な場所に分散しています。

## 重要データに積極アプローチ

データを分類するのは非常に困難な作業です。そこには、企業全体の IT エコシステムから機密データを洗い出し、所有者・責任者を特定して、業務上の重要度にもとづいてランク付けする、といった細かい作業がともなわれます。そのような難しい作業が従来、手作業による検索、さらにデータファイルの使用状況と所有者を割り出す推測に広く依存していました。しかし、今日、業界を代表する大手企業は、制御不能となったデータの識別に、より積極的なアプローチを採っています。データ分類時の妥協が及ぼす深刻な影響を、インテリジェントな自動化やアナリティクスにより回避し、処理を加速すると同時にコンプライアンスを強化しています。

## データ検出・分類を自動化

「このデータはどこに保管されているのか？」、「誰がデータを取り扱っているのか？」、「なぜ、そこに保管されているのか？」など、企業内の機密データに関する様々な質問に、HyTrust CloudAdvisor for Data が逐一答えを出します。HyTrust により、個人を特定する情報（PII：Personally Identifiable Information）を含め、業務上の重要データを見つけ出す施策をすばやく定義でき、ユーザーの不審な行動を検知し、情報漏えい、悪意あるユーザーアクセス、さらには、EU 一般データ保護規制（GDPR）などのコンプライアンス違反に対する防御が可能になります。

**潜在的データリスクの発見・可視化・検索**

HyTrust CloudAdvisor for Data は、必要なデータを必要なときに発見します。キーワード検索、データ可視化、そして、データをさらに掘り下げるドリルダウンなどの機能により、IT 部門、特にセキュリティ担当者はファイルの内容やユーザーアクティビティを簡単に調べられ、分析・評価することができます。それにより、データ管理はもちろん、セキュリティやコンプライアンスを徹底することができます。

**データとユーザーアクティビティを時系列で確認**

HyTrust CloudAdvisor for Data は、個々の仮想マシン内に保管されたデータの内容を完全に可視化することにより、時間を追って、ユーザーアクティビティとファイル情報を関連付けることができます。600 種以上のファイルタイプに対応し、ユーザー定義のタグに対して、パターンに合致するデータの特定やキーワード索引によるデータ特定を可能にします。

### データの積極監視で機密データを保護

仮想マシン（VM）内の機密データや重要データが自動的に識別・監視され、アラートが発動されます。機密データを守るための堅実なルールを必要に応じて調整できるので、監査ログによって、すべてのファイルとユーザーアクティビティが維持管理され、コンプライアンスの証拠収集やフォレンジック分析が的確にサポートされます。

### 不正／過失アクティビティの検知

ユーザーファイルアクセスの追跡調査にビヘイビアベースの分析機能（ユーザーの行動・振る舞いを元に検証）が活用され、疑いのある、あるいは正常ではないアクティビティが IT セキュリティ担当者に通知されます。


図 1. HyTrust CloudAdvisor for Data は、仮想環境の重要・機密データの表示と分析、インテリジェンスを駆使した処理を提供

## 迅速な設定、簡単な管理

HyTrust CloudAdvisor for Data はディプロイ後ただちにその仮想アプライアンスが仮想環境内の VM をすべて洗い出し、一覧表示を可能にする機能を、VMware vCenter との連携により、あるいは Veeam バックアップイメージにおいて実現します。

VM を探し出すプロセスは、初期設定時に行われ、仮想環境に追加される、あるいは仮想環境から削除される VM を定期的に追跡調査します。その後、インベントリが規則的に更新されるので、IT 部門、特にセキュリティ担当者は

監視・分析すべき VM を時間を追って確認することができ、不正または過失アクティビティから保護することが可能になります。

## 緻密なデータ分析とタグ — 業務環境への影響ゼロ

HyTrust CloudAdvisor for Data は、その仮想アプライアンス内に保管された読み取り専用のスナップショットを用いて、VM 内のすべての対象ファイルのメタデータを効率的にインデックス付けします。それにより、運用中の VM 自体への影響が最小限に抑えられます。VM を分析する頻度は自由に変更することができ、分析のために VM を特別に起動する必要もありません。分析されたファイルデータは検索可能な情報として、ユーザーアクティビティからの相互参照が可能となり、利用状況のプロファイルが構築されます。

## ユーザーとファイルアクティビティの関連付けでセキュリティ強化

HyTrust CloudAdvisor for Data は、Microsoft Active Directory と密に連携して、VM 内に保存されたファイルに対するユーザーアクティビティを識別します。それにより、アクティビティの基準が構築され、ユーザーやシステムの異常行動を察知するための指針となります。HyTrust CloudAdvisor for Data 内で稼動する分析エンジンが極端なアクティビティを精査し、不正あるいは異常アクティビティが生じたら、自動的にアラートを発動するか、仮想マシンのスナップショットを生成し、自動的に適切な防御策を講じます。

## まとめ

HyTrust CloudAdvisor for Data は、取り扱い要注意の重要データや機密データなど、恣意的に仮想環境内で複製されたものも含め、その表示と分析はもちろん、インテリジェンスを駆使した処理機能を実現します。データの検索や詳しい分類、リスクの特定と軽減、コンプライアンス要件の遵守など、IT 担当者や、特にセキュリティ担当者が必要とする幅広い機能が、ディプロイ後ただちに利用可能となります。したがって、企業や団体における最重要データ資産が安全確実に保護されます。



**株式会社クライム** 〒103-0014 東京都中央区日本橋蛎殻町 1-36-7 TEL:03-3660-9336
Email : soft@climb.co.jp URL: www.climb.co.jp