druva

ホワイトペーパー

Office 365:
データ保護の重要な課題

データ保護の不足機能をDruvaで補完

クラウドアプリケーションの問題を把握

クラウド独自の優位性によりSaaSアプリケーションの採用が急速に広まってきましたが、クラウドベースであろうがなかろうが、どの顧客に対してもすべてを提供できるサービスはないということに注意が重要です。たとえば、Office 365ではさまざまな機能が幅広い価格帯でパッケージとして提供されていますが、採用に際しては、このサービスが大企業の特定ニーズへの対応を主としていることを認識しなければなりません。Office 365には強力な中核機能がありますが、必ずしも企業向けのデータ可用性およびガバナンス要件の包括的ソリューションになるとは限りません。このため高いコンプライアンス体制を維持するためには、多くの企業でOffice 365のネイティブ機能を補完した強力なデータ保護ソリューションをクラウド上に構築する必要があります。

実際、ガートナーリサーチはOffice 365を導入した組織に対して、サードパーティーのサービスを使用してネイティブ機能の不足を補うことを強く推奨しています。これらサードパーティー機能には、訴訟ホールドの管理、eDiscovery、DLP、ランサムウェアからのリカバリ、高度な脅威防御、暗号化、事業継続性に関する不足を補う機能が含まれます。Office 365にもこれらの機能は多く含まれていますが、その基盤上ですべての組織にすべての機能を提供することはできず、いくつかの欠点があります。サードパーティーの専用サービスでは、それらをより適切に対処でき、多くの場合これら機能はMicrosoftよりも安価に利用できます。

サードパーティーによるデータ可用性およびガバナンス機能をOffice 365と連携させることが重要であり、機能や価格面でどの組織にも大きなメリットがもたらされますが、これにはいくつかの理由があります。

データ復旧

Microsoftなどの主要なオンラインサービスプロバイダは、世界中の企業や業務に不可欠なクラウドベースの情報ソリューションを提供しています。しかし、これら主要SaaSプロバイダは顧客データをバックアップやリカバリで保護しているでしょうか？なぜクラウド上に保管済みのデータをさらに保護したいのでしょう？クラウドプロバイダは、データへのアクセシビリティを確保し、自社と顧客をデータ損失から防ぐために実際にはさまざまなレベルのリカバリを提供しています。しかし、そのようなバックアップは顧客がすべてのデータを利用できるようにするためのものではありません。実際、クラウドソリューションはデータ復元を前提に設計されておらず、バックアップ機能を備えたクラウドプロバイダはかなりの料金を顧客に請求する場合があります。一般にほとんどのオンラインサービスでは、顧客が組織のデータ向けにバックアップとして使えるのは、一定期間後に自動的に削除される“ごみ箱”だけです。ごみ箱の削除が実行されると、そのデータは永遠に失われます。

実際のところ、データが偶発的または意図的に削除、変更、または壊れてしまったとき、それを取り戻すために管理者が行えることはほとんどないということです。

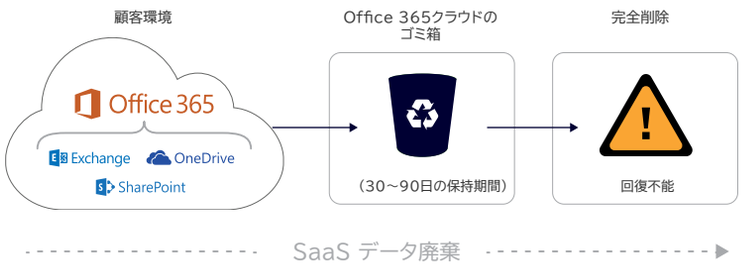
ファイル共有はデータ保護ではない

OneDrive for Businessのようなクラウドベースのファイル同期および共有ソリューションを使用していると、データがバックアップされているかのように保護されていると考えてしまいます。「OneDrive for Businessをすでに利用しています。OneDriveにファイルを保存すればそれで終わりでないのですか？」という質問が以前から寄せられます。端的に答えれば、これらの種類のオンラインサービスには重要かつ重大な違いがある、ということです。ファイル共有とデータ保護の技術には重複する機能がありますが、基本的にアプローチは異なります。次のことを理解する必要があります。

Microsoftのファイル同期および共有ソリューションであるOneDriveがバックアップではないことを理解することが重要です。ファイル共有は、ユーザーのコンテンツとリアルタイムなコラボレーション（共同作業）向けに構築されますが、ユーザーのエラー、データ破損、ランサムウェア被害に遭った場合のデータリカバリ目的には設計されていません。またアーカイブ目的や、全く新しいコンプライアンスやeDiscoveryの課題に対処するものでもありません。

「MicrosoftではOffice 365がうまくバックアップされないことを痛感するようになりました。Microsoftでリカバリできるだろうと考えていましたが、そうではありませんでした。Microsoftからは「サービスレベル契約に含まれていません」という回答でした。そのため、Office365データを保護するため、Microsoftで対処する必要があると考える、いくつかの問題を抱えたままでいます」

- Microsoft Office 365のお客様より



企業向けバックアップソフトウェアは、すべてのユーザーのデータコピーをリカバリ用途に使用できるようソフトウェアが自動的に作成するという点で、ファイル同期および共有とは異なります。エンドポイントやクラウドアプリのデータは完全に保護され、デバイスの紛失や盗難に遭った場合、リモートワイプや位置情報追跡などの追加機能によってデバイスを追跡したり、企業データを遠隔から削除したりすることができます。さらに、ユーザーのシステムおよびアプリケーション設定をバックアップすることで、ユーザーが使い慣れた作業環境を維持しながら、新しいデバイスや入れ替え用のデバイスを迅速にセットアップすることができます。

さまざまなデータ損失の原因

主要なオンラインサービスプロバイダーですべてのデータが失われたり、完全に「サービス断」となる可能性は非常に低いですが、現実性が高く頻繁に起こりうるデータ損失の要因が以下のように数多くあります。

- **意図しない削除やユーザーエラー:** 特定のユーザーや組織が削除したデータが後から必要になることがよくあります。たとえば、解散したプロジェクトのデータを削除した後にそのプロジェクトの再開を知る場合があるでしょう。共同作業者がプロジェクトの共有データを意図せず削除してしまうこともあるかもしれません。また、ユーザーやサードパーティーのアプリケーションによって知らないうちにデータが上書きされたり、破損されたりすることもあります。
- **悪意ある操作:** 社員が解雇される疑いがあると思った場合や、上司や同僚に恨みを持った場合、退職する前にデータを削除することがよくあります。ハッカーもセキュリティシステムを乗り越えてデータを削除または破損させる犯人かもしれません。内部犯行であれ、外部犯行であれ、このような事例は現実に起きえます。
- **データ破損:** アプリケーションは絶えず更新される組織の重要な基幹業務データを大量に保持しています。データの上書きはよく起きる問題で、大量のデータが一括アップロードでアプリケーションにインポートされた場合や、連携するサードパーティーのアプリケーションを使用してSaaSアプリケーション内のデータを管理している場合に発生します。たとえば、プロジェクト管理アプリケーションがカレンダーのすべてのイベントを消去したり、受信トレイに不正形式の不要なメッセージを大量に詰め込んだりしたらどうなるでしょう？経費精算アプリが税務記録スプレッドシートにゴミデータを埋め込んだらどうなるでしょう？マーケティング分析ツールでCMSデータベースが破損し、慎重にコーディングしたすべてのWebデザインが破壊されたらどうなるでしょうか？
- **サービスプロバイダー:** クラウドサービスプロバイダーのデータ損失によるアカウントへのアクセス無効化は致命的であり、サービス利用が再開されるまで他に手はありません。利用中のファイル共有アプリケーションがオフラインとなり、問題が解決するまでレポート、プレゼンテーション、顧客への提出資料が利用できなくなったとします。組織にどの程度のコストがかかるでしょうか？

クラウド上のランサムウェア

数年前はランサムウェアについて誰からも尋ねられませんでした。今日ランサムウェアはありふれたものとなり、増加の一途をたどっています。SaaSアプリケーションも同じく危険にさらされていることをほとんどの組織は認識していませんが、ハッカーは絶えず新しい戦略を取り、かつて稀な形の侵入攻撃を成熟産業へと変えました。ランサムウェアの脅威は特定業界の少数の企業に限定されるものではなくなり、すべての組織や業界に影響を与えています。同時に、この脅威は物理デバイスに限定されたものではなくなり、クラウドアプリケーションのユーザーにとっても大きな懸念事項となっています。企業はこの新しく気味の悪い脅威について、またどうすれば攻撃への対応を十分に行えるかについて、何とか理解しようとしています。

ランサムウェアによる稼働停止は、中小企業では1時間あたり約8,500ドル（約94万円）の費用に相当します。米国では年間75億ドル（8,250億円）以上の損失につながります。犯罪者は大きな問題と考えずに運用し続けるため、これら犯罪行為は頻度や重大性が増すだけでなく、企業の日常的な脅威状況の一つにもなるでしょう。FBI（米国連邦捜査局）のインターネット犯罪苦情センターによると、2015年に約2,500件の苦情があり、損害額は1,600万ドル（約17億円）以上でした。実際に報告されるインシデントは全体の4分の1に満たないため、本当の被害額はさらに高いといえます。

ランサムウェアは
1100 億円
規模の産業となる勢い

druva

「2020年までに、企業データの50%以上は企業データセンター以外の場所に置かれるだろう。」

- Gartner、"Plan Your Data Exit Strategy Before You Sign a SaaS Contract"、2016年3月

何が危険なのか？

多くの組織では、クラウドが単にユーザー操作環境の拡張であることが理解されていません。クラウド上のデータにおける紛失や盗難、悪意ある攻撃の影響を受けやすさは他の場所と同じです。企業はクラウド上のデータを管理せざるを得ず、規則や規制を遵守しなければ莫大な罰金が科せられ、さらには信用の失墜にもつながります。

クラウドアプリケーションの成長によってもたらされるデータ保護およびガバナンスの問題に適切に対処するため、組織はデータ可用性、コンプライアンス、セキュリティに関する 3 つの新たな課題と検討事項を考慮する必要があります。

- **常時オンのデータ可用性確保：** IT 部門長やエンドユーザーはどちらも、SLA（サービスレベルアグリーメント）の下に重要な企業情報は SaaS ベンダーによりバックアップされているため、SaaS データやクラウドデータの保護は必要ないと誤解しています。しかし SaaS ベンダーによる SLA は、例えばサービス断など SaaS プロバイダーの過失によるデータ損失のみが対象となることを多くの人は気づいていません。通常、意図しない削除や以降エラー、データ破損、悪意ある攻撃によって失われたデータは SLA の対象外です。SaaS ベンダーでは、30 日以上経過した削除済みデータのリカバリが行えない可能性があります。これは、サービスの標準仕様として 30 日後に削除済みデータを完全消去するためです。SaaS プロバイダーが顧客との作業をいとわずデータがまだ存在する場合でも、プロバイダーから高額な料金が請求され、クラウドバックアップソリューションの利用を推奨されることがあります。データが実際に復旧できる場合でも、復旧に際して数え切れないほどの時間の生産性が失われます。
- **訴訟ホールド義務の履行：** 今日、訴訟中に裁判所からデータ開示要求を受けて SaaS 基盤上に保存されたデータを提出できない場合、企業は非常に深刻な結果に直面することがあります。組織内の法務部門は、訴訟の弁護や高額な罰金を避けるために重大な影響を及ぼす可能性のあるユーザーデータに即座にアクセスする必要があります。多くの場合、このデータの一部または全部が Office 365 や Box のようなクラウドサービス上にあります。これらデータは訴訟の過程においてリカバリできなかったり、完全に保護されていない状態のためユーザーによる削除や誤操作を受ける可能性があったりします。

  訴訟開示の焦点は、訴訟に関連する情報を特定および分離するためにデータを取り出す手続きです。これを行うには、情報が適切にインデックス化され、検索機能が十分に柔軟であることが前提となります。さらに訴訟案件の早期評価査定（Early Case Assessment）では、リアルタイムに検索結果を確認し、その結果に基づいて検索を絞り込む機能が不可欠になります。

  収集や審査の段階で現在および過去のデータに適時かつ容易にアクセスできない場合、訴訟費用や訴訟結果に何億円もかかることがあります。法廷で正当化できる（ データの証拠隠滅がない ）方法で保全および授受しながらクラウドアプリケーションに保存されているデータを収集することが、組織や法務部門が効果的なソリューションで取り組む鍵となります。
- **クラウド上でのセキュリティとコンプライアンスへの取り組み：**情報セキュリティ（InfoSec）部門にとって最も懸念されるのは、機密性の高い重要データが漏えいするリスクです。Dimensional Research 社が実施した最近の調査によれば、95% 近くの企業がクラウド上に機密データを持っています。このデータを保護しなければコストは莫大なものになります。これは単に規制における罰金という形だけでなく、企業の風評に及ぼす影響と、その結果による著しい信用失墜によって測られます。

  頻繁にプライバシー保護法が改変される中で、規制環境は複雑さを増しています。欧州連合（EU）が採択した GDPR（ 一般データ保護規則 ）およびプライバシー・シールドでは、データ可視化に関して大半の組織が現在実施している以上のことが義務付けられます。SOX 法や HIPAA、新しいデータプライバシー規制により、企業はデータの取得、保管、保護方法を大きく変えるようになりました。

サードパーティーアプリの事例

Office 365 には、SaaS アプリケーション一式が含まれています。これらアプリケーションは、企業が生産性を上げて業務目標を達成するために日々活用されています。しかし、これら強力なツールは前述した重要な問題に対処するために必要とされる専用製品ではありません。エンドユーザーのデータ保護、データリカバリ、訴訟ホールドおよび電子情報開示、Office 365 アーカイブデータのサードパーティー管理の分野で問題に対処するよう行動をとった組織が増えています。

Office 365 には下記の機能がいくつも含まれていますが、プラットフォームはすべての組織に共通するものではありません。したがってサードパーティー製品が Microsoft よりもより適切な価格で対処できるという欠点が存在します。

「SaaS はオンプレミスソフトウェアの 3 倍の速度で成長している。」

- ボストンコンサルティンググループ

以下の表は効果的なサードパーティーのソリューションが、これらの重要なビジネス上の問題すべてを網羅して提供すべき重要な価値を明確に示しています。

Microsoft Office 365	サードパーティーが提供する利点
エンドユーザーの全データ保護	データがパソコン、スマートフォン、タブレット、クラウドアプリのどこにあるかにかかわらず、エンドユーザーデータを保護するサードパーティーのデータ保護サービスを導入することで、Office 365データ保護機能の2つの重大な欠点を補完できます。 ・ **限定的な機能:** Microsoftのサービスではバックアップ、リカバリ、アーカイブはOffice 365データのみに限定され、ラップトップやモバイルデバイスは対象外であるため、ユーザーが扱う電子データの全範囲が網羅されません。 ・ **高コスト:** エンドユーザーデータを保護するにはMicrosoftライセンスに追加費用が必要になりますが、エンドポイントやOffice 365以外の各クラウドアプリケーションに存在する情報は保護されません。
データ復旧の補完	Office 365とサードパーティーサービスを併用することでエンドユーザーや管理者は簡単かつ迅速にデータを回復でき、他のデバイスや元の場所へのダウンロードや復元が可能になります。これはOffice 365で提供されるリカバリサービスとは大きく異なります。 ・ Microsoftが顧客データを喪失した場合にのみ、SLAに準じてデータが復旧されます。 ・ 顧客がデータを喪失した場合のMicrosoftの復旧機能は限定的で、短期間(課金されたサービスによって30～90日)で復旧期限が切れます。その後顧客がデータを復旧することができなくなります。 ・ Microsoftはランサムウェア侵入の際にデータを回復することができません。この対処には時間インデックス付きスナップショット機能が必要であり、専用のバックアップサービスが必要です。
eDiscoveryやコンプライアンス向けの検索と絞り込み	Office 365環境をサードパーティーサービスで補完することで企業のコンプライアンスや規制、eDiscoveryの課題に対処できるようになり、時間、労力、コストが削減できます。 ・ インプレースのeDiscovery検索機能では検索結果がすぐに表示されません。そのため迅速なレビューや、大量データを関係するものへ絞り込む作業が難しくなります。さらに検索結果としてユーザーに関係ないものが見つかることで検索をすべてやり直し、貴重な時間が無駄になり、レビュープロセスが遅くなる場合もあります。 ・ Office 365ではすべてのファイルタイプでインデックスが作成されないため、Microsoft以外の全ファイルタイプを含む条件での検索ができません。
サードパーティーが管理するアーカイブ	データセンターのオフサイトレプリケーションと同じように、サービスプロバイダーが顧客アカウントへのアクセスを取り消した場合に備えて、クラウドアプリケーションの全データを別のクラウド環境に安全に保管します。

Druvaの適合性

Druva は、世界最大規模の組織におけるデータ損失やコンプライアンス違反からの Microsoft Office 365 の投資保護をサポートしています。Druva の業界をリードするソリューションは単一の管理画面を提供し、置き場所に関係なくデータが保護されます。

Druva は企業が自社防衛のためビジネスクリティカルな情報をアーカイブおよび開示するために欠かせないデータ保護機能を提供し、リスクにさらされる 4 つの重要分野においてセキュリティやコンプライアンスを損なわずに Office 365 のコア機能に付け加えることができます。

- エンドユーザーの全データ保護
- データ復旧
- データガバナンス
- サードパーティーが管理するアーカイブ

付加価値となる点

以下の表に、Office 365 と Druva inSync サービスに提供される機能比較を示します。

Microsoft Office 365	Druva insync
Office 365 Exchange: 削除されたアイテムは［削除済みアイテム］フォルダーに移動され、手動で削除されるか、保存ポリシーに基づいて自動的に削除される（デフォルトは30日間）まで保持されます。 ［削除済みアイテム］フォルダーから削除すると、アイテムは最低14日間［修復済みアイテム］フォルダーに残ります。	**Office 365 Exchange:** inSyncは、メール、カレンダー、連絡先を世代の上限なく無期限で保持します。 inSyncによってバックアップされたメールはどの時点のものでも復元できます。inSyncはユーザーのメールボックスに直接メールを復元する機能とともに、退職した従業員のメールを復旧するため別のユーザーに復元する機能も提供します。
Exchange Online のアーカイブ: Microsoftは、Exchange Online ArchivingをE3およびE5プランの機能として、または有償アドオンとして提供しています。これはメールボックスごとに設定が必要なメールのみのアーカイブ、カレンダー、連絡先、タスクのアーカイブは含みません。個々のメールは復元できますが、特定世代におけるメールボックスを復元する機能はありません。	**Exchange Online のアーカイブ:** inSyncは、ユーザーのExchange Online「インプレース」アーカイブメールボックスを世代上限なく無期限でバックアップすることもできます。inSyncでバックアップされたメールは、どの世代のものでも復元できます。inSyncはユーザーのメールボックスに直接メールを復元する機能とともに、退職した従業員のメールを復元する機能も提供します。
SharePoint OnlineとOneDrive for Business: 削除されたアイテムはまずサイトのごみ箱に送られ、90日後に自動的に消去されます。アイテムがごみ箱から自動または手動で消去されると、サイトコレクションのごみ箱に移動されます。これらアイテムはSharePointから完全に消去される前に、管理者が指定した日数だけ保持されます。	**SharePoint OnlineとOneDrive for Business:** inSyncには、OneDrive for Businessのバックアップを世代上限なく無期限に保持するオプションがあります。

法的証拠開示とコンプライアンスの要件

訴訟ホールド

情報、ガバナンス、法務の審査要件を満たそうとする場合、クラウドデータはエンドポイントまたはオンプレミス上に置かれたメールや CRM、ファイルサービスのデータと変わりありません。今日では SaaS プラットフォーム上に格納されたデータに関するレポート作成が行えないと、企業は窮地に立たされます。組織内の法務および人事部門は、調査に関する検索や係争中の訴訟を立証するためにユーザーデータにアクセスする必要があります。法的証拠となりうるデータが Office 365 などのクラウドサービス上に存在することは多く、アーカイブされていない場合もあります。データの収集や情報の審査のために現在および過去のデータに適時かつ容易にアクセスできないと、弁護士費用や訴訟の結果として何百万ドルもの負担が強いられることになります。

すべての組織とその法務部門は、法定で正当化できる（ 文書毀棄なしに ）レポート提出が行えるようクラウドアプリケーション上でデータの保全や提供、収集を行うことを検討すべきです。

Microsoft Office 365	Druva insync
訴訟ホールドに制限あり: メールボックスに複数の訴訟ホールドを適用できますが、1つのメールボックスに5つ以上適用すると訴訟ホールドが日付やキーワードで限定されていたとしてもメールボックス全体が保全されてしまいます。ユーザーがメッセージを削除すると、そのメッセージは隠しフォルダーに移動されます。夜間処理でこのフォルダーがクリーンアップされます。Office 365の訴訟ホールドは基本的に、このクリーンアッププロセスによる隠しフォルダーからのアイテム削除を除外するルールでしかありません。 1つの訴訟ホールドでは、10,000個のメールボックスまでしか適用できません。これ以上のメールボックスで行いたい場合、複数の訴訟ホールドを作成する必要があります。Microsoftの契約条件では訴訟ホールド対象となるユーザーの割合が制限されるため、法的に義務付けられているすべてのデータを保全することができないかもしれません。	**訴訟ホールドに制限なし:** メールボックスに無制限の訴訟ホールドを適用することができ、適切にルールを適用できます。 訴訟ホールドが適用できるメールボックスの数に制限はありません。

事件ごとの訴訟ホールド： 訴訟ホールドはメールボックスのグループに対して定義でき、オプションで日付またはコンテンツによって限定することもできます。	**事件ごとの訴訟ホールド：** 訴訟ホールドはメールボックスのグループに対して定義でき、オプションで日付またはコンテンツによって限定することもできます。

エクスポート

アーカイブソリューションの最終的な成果物は、他の訴訟データ審査システムに提供するデータや相手の弁護士に直接渡すデータです。エクスポートの性能と手順は、効果的なソリューションを判断する重要な要素です。

Microsoft Office 365	Druva insync
同時に1つのエクスポートのみ実行可能： エクスポートクライアントアプリケーションのインスタンスは、1台のマシン上で1つのみ実行できます。このため開示ユーザーは一度に1つのエクスポートジョブしか実行できません。 さらに夜間や週末の処理向けにエクスポートする検索ジョブをキューに複数入れることができず、処理時間が浪費されます。問題が発生した場合、顧客がエクスポートジョブを監視してサポートチケットを作成する必要があります。Microsoftはサービス機能としてエクスポートの監視を積極的に行いません。	**複数のジョブを同時に実行：** 処理向けにエクスポートジョブをキューに複数入れ、同時に複数のエクスポートジョブを実行できます。キューイングされたジョブは自動的に実行されるので、複数ジョブ間の処理時間が無駄になることはありません。 inSyncのサポート内容としてエクスポートジョブの進行状況監視が含まれるため、問題が発生した場合は迅速に対応できます。
エクスポートデータをサードパーティーに送れない： エクスポートされたデータはまずeDiscovery Centerからユーザーのローカルマシンにダウンロードし、その後法務サービスプロバイダにアップロードする必要があります。	**訴訟ホールドデータをeDiscoveryシステムに直接エクスポート可能：** inSyncでは、法務管理者が審査のため訴訟ホールドデータにアクセスできます。またエクスポート不要でサードパーティーのeDiscoveryプラットフォームに直接データを提供できます。簡単な手順で、審査とタグ付けの下流工程を開始できます。
開示ユーザーのデスクトップ上でエクスポートを実行： 検索結果のエクスポートにはクライアント側アプリが使用されます。そのためエクスポート実行中は、開示ユーザーのマシンリソースが占有されてしまいます。エクスポートが大量になると、処理時間が数時間かかることがあります。エクスポートが完了するまで、マシンをネットワークに接続したままにしておく必要があります。そのためユーザーはパソコンを持ち帰ることができません。ファイルはユーザーのローカルハードドライブに作成されるため、すべての検索データを保持するのに十分なディスク容量が必要になります。エクスポート速度は、開示ユーザーのマシンの速度に依存します。	**エクスポート不要：** サードパーティーのeDiscovery製品はinSyncのネイティブクラウド基盤に直接接続できるため、エクスポートは不要です。開示ユーザーのマシンも不要です。したがってユーザーのコンピュータリソースには依存しません。またローカルマシン上のデバイスとして訴訟ホールドを設定することで、データアクセスを簡単に行うことができます。エクスポート要求を明示的に行う場合、デバイスが利用可能か否かにより自動停止と再開が行われます。

検索と調査

訴訟開示の中心工程は、事件に関連する情報を特定または分離するためにデータをマイニングすることです。これを行うには、情報が適切にインデックス化され、検索機能の柔軟性が十分であることが前提となります。さらに、早期訴訟案件評価や調査作業中に検索結果から不要なものを除外する機能や結果をリアルタイムで表示する機能が重要になります。

Microsoft Office 365	Druva insync
限定的なファイル種別インデックス化： Office 365では、Officeドキュメント、PDFファイル、テキストドキュメントのインデックスが作成されます。他のドキュメント種別はインデックス化されないため、キーワード検索では関連するコンテンツが対象外となります。	**500種類以上のファイル種別インデックス化：** inSyncは、zipファイル内に格納されたアイテムを含む500以上のファイル種別のインデックスを作成します。 これにより、一般的ではないファイル形式であるという理由だけで関連する文書を対象外にすることはありません。

メールボックスベースのインデックス構造: Exchangeではメールボックスごとにインデックスが管理されます。これはエンドユーザーがメールボックス内を検索するには最適なモデルですが、複数メールボックスを検索する場合にパフォーマンス上の問題が生じます。また、Exchangeのインデックス作成はバックグラウンドプロセスで「ベストエフォート型」のモデルであるため、メールボックスに存在するすべてのアイテムが常にインデックスに登録されるわけではありません。データ保護要件によりますが、あるユーザーがメッセージコピーを削除したが他のメールボックスには存在する場合、当該ユーザーのメールボックスのみを検索すると、保持している関連アイテムが見つからないことがあります。	**リポジトリ全体のインデックス構造:** inSyncでは、アーカイブ全体で統一されたインデックス構造が保持されます。アーカイブ内には各メッセージのインスタンスコピーが1つだけ存在し、各メッセージが属するメールボックスに関するメタデータが含まれます。これにより、複数メールボックス間またはリポジトリ全体にまたがる検索がほぼリアルタイムで可能になります。inSyncではコンテンツがアーカイブに追加される前にインデックスが生成されます。これによりアーカイブ内の全アイテムが検索できるようになります。
バッチ検索: Office 365はメールボックスごとのインデックス化を行うため、リアルタイムで検索を実行できません。その代わりに管理者が検索ジョブを作成して完了したら通知を受け取るようにします。結果を「証拠開示用メールボックス」にコピーする(検索結果が証拠開示用メールボックスの制限である50 GB以内である場合)か、PSTファイルに直接エクスポートジョブを作成することができます。この方式はメールボックス全体を抽出するには有効ですが、調査や検索の絞り込みには向きません。結果的に、処理するデータが増えるにつれ、証拠開示下流工程のコストが高くなる場合もあります。	**リアルタイム検索:** inSyncのリアルタイム検索機能により、簡単に検索結果に目を通して絞り込みが行えるようになります。これは何が起こっていたかを把握しようとする調査活動において重要なだけでなく、サードパーティーのツールやベンダーにエクスポートされるデータ範囲を絞り込んで法的証拠開示のその後の工程を減らすこともできます。
メールボックス数により検索時間が増加: Office 365ではメールボックス単位で検索が実行されます。そのため検索するメールボックス数が多くなるとバッチ検索完了までの時間が長くなります。また検索完了まで結果のプレビューやエクスポート操作開始が行えないため、完了後すぐに次の作業を開始しないと証拠開示の主要工程で膨大な時間が失われます。	**アーカイブ全体を検索可能:** デフォルトでは、アーカイブ全体で証拠開示検索が実行されます。これにより情報識別工程でアーカイブを使用することで、事件のカストディアンになる可能性のある人物を特定することができます。
訴訟ホールド内で検索できない: Office 365の訴訟ホールドは単にデータ破棄を防止するよう設計されています。特定データの論理コンテナを表すものではありません。そのため検索に訴訟ホールド対象となるデータは含まれているものの、事件の識別工程が済んだ情報を対象とする検索操作に絞り込むことはできません。	**アーカイブ全体を検索可能:** デフォルトでは、アーカイブ全体で証拠開示検索が実行されます。これにより情報識別工程でアーカイブを使用することで、事件のカストディアンになる可能性のある人物を特定することができます。

データの整合性

法的証拠開示に役立てるには、データは証拠となりえる必要があります。元のメッセージのメタデータをすべて保持する必要があります。さらにデータ管理に関する工程においてデータの喪失や破損がないようにしなければなりません。

Microsoft Office 365	Druva insync
ベストエフォート型のデータ損失管理: Office 365は第一にコミュニケーションとコラボレーションの業務要件を満たすために設計されています。そのためデータは高可用性確保のためデータセンター間でほぼリアルタイムで複製されます。スナップショット作成やバックアップは実行されません。このアプローチの欠点は、データ破損も複製されてしまうことで、ロールバックもできません。法的証拠開示に関して、これは訴訟ホールド対象であってもメッセージが失われる可能性があることを意味します。	**データ損失なしの設計:** inSyncクラウドはオブジェクトストレージサービスを使用することで99.99999%の信頼性が保証され、inSyncのデバイスデータバックアップに適したデータ復元性が提供されます。inSyncではデータとメタデータの通信が分離されます。inSyncクラウドでは、データとメタデータは指定されたリージョン内の3つのデータセンターに複製されます。inSyncクラウドではバックアップサーバーとしてステートレスなコンピュートノードが実行されます。バックアップサーバーがステートレスなため、inSyncではサービスに影響を与えずにコンピュートノードの障害対応を実現できます。

データレジデンシーが保証できない： MicrosoftはOffice　365の顧客データをユーザーの場所によって複数の異なる国に保管しています。これはユーザーの近くにデータを置くことでOffice　365のパフォーマンスを向上させるために行われますが、Microsoftは予告なしに顧客データを移動することができます。20,000人以上のユーザーがあれば専用環境で導入できますが、ほとんどの顧客では実現不可能です。	**リージョン別、オンデマンドのオブジェクトストレージ：** Druvaでは顧客が選択可能なリージョンを30以上提供されており、ユーザーは地域ごとのプライバシー規制の変化に対処し、データレジデンシー法や各種規制の要件を満たすことができます。
独立したデータストアがない： Office　365（または他のクラウドプロバイダー）はデータソースが1つしかないという隠れた問題があります。データ検証目的専用の保管領域がない場合、データの破損や削除によって重要な業務記録の唯一の「真実」が削除される可能性があります。独立したアーカイブ/データストアにこれらの記録専用の保管元を持つことが包括的な情報ガバナンスのベストプラクティスです。	**独立したデータストア：** ベンダーとの関係悪化や、ベンダーが提供するシステムが何らかの形で利用できなくなった場合に備え、顧客はinSyncを二次データソースとして利用できます。

Druvaによるファイルの同期と共有へのアプローチ

- ファイルの同期と共有は対話型であり、ユーザーは同期するファイルやフォルダーの選択、コピー、移動を行います。一方バックアップはユーザーの目に見えず全体的に行われます。
- ファイルの同期と共有では、複数デバイス間でファイルが同期されたときにあるファイルバージョンが削除や破損された場合、すべてのデバイスが影響を受けます。一方バックアップは、あるファイルバージョンが喪失、削除、破損した場合に備えて冗長を生成するよう設計されています。
- ファイルの同期と共有では、所有ファイルの一部を他のデバイスやユーザーに利用させることができます。すべてのファイルを確実にバックアップして安全に保持することで、必要なときにファイルへのアクセスや復元が可能になります。

Microsoft Office 365	Druva insync
自動化がない： OneDriveは、ユーザーが「同期フォルダー」に置いたファイルのみを保存するため、エンドユーザーのトレーニングが必要となり、取り込まれるデータ範囲も著しく制限されます。開いているファイルは閉じるまで同期されず、データは危険にさらされたままになります。OneDriveの同期と共有は自動化された導入やレポート機能が欠けているため、IT部門による手動管理が必要です。	**エンドユーザーの操作不要：** inSyncは、.pstファイルを含むすべてのデータを継続的に保護します。オプションでユーザー操作不要のファイル除外が可能で、既存ファイルのアクセスと復元性が常に確保されます。
ファイルのサイズと同期に制限がある： OneDriveのファイルごとに10GBのアップロードサイズ制限があり、保存できるアイテム数も制限されています。ビジネスライブラリは20,000ファイル、サイトライブラリは5,000件が上限です。OneDriveはファイル数の多いディレクトリをサポートしておらず、パスのサイズは250文字に制限されているため、使い勝手が限定的です。	**制限なし：** inSyncでは最大ファイルサイズや、バックアップできる最大のファイル数やバージョンに制限がありません。管理者はinSyncを設定して自社環境向けに制限を設けられますが、デフォルト状態のinSyncにはこれら制限はありません。
ロックされたファイルをサポートしない： OneDriveは、Adobe　PDFビューアやOutlookなど他のアプリケーションによって開かれているファイルはバックアップしません。	**ロックされたファイルをサポート：** inSyncではWindowsボリュームシャドウサービス（VSS）を使用することで開いているファイルもバックアップできます。LinuxやMacではWindowsのような強制ロックが行われないので、そのようなファイルもバックアップ可能です。
帯域管理がない： OneDriveには重複排除やリソース制限（帯域とCPU）がないため、特にWANや低品質ネットワークを使うユーザーにとっては、エンドユーザーの使用感が悪くなるリスクが上がります。	**ネットワークパフォーマンスを向上：** inSyncのWAN最適化、リソース制限（帯域とCPU）、自動再開機能により、バックアップやリストアは無停止で、エンドユーザーにとって効率的に行われます。

サポートされていないファイルタイプがある： OneDriveでは、.exe、.msi、.dllのようなSharePoint Onlineでブロックされているファイル種別のファイルをユーザーがアップロードすることはできません。またブロックされるファイル種別は固定されており、変更することはできません。	**すべてが含まれる：** inSyncは、.pstファイルを含むすべてのデータを継続的に保護します。オプションでファイル除外が可能です。
OSサポートが限定される： OneDriveでは現在、Linuxがサポートされていません。	**複数OSをサポート：** inSyncでは現在、Windows、Mac、Linuxをサポートしています。Druvaは適用と実現が可能であればOS間で機能（OS移行、メールのバックアップ、除外ポリシー）の同等性を保つよう努めています。
エンタープライズクラスのサポート： Office　365のサポートは、営業時間内のみ利用可能で、重大度が「高」であっても「重大」ではないイベントに対しては応答時間目標が規定されていません。	**エンタープライズクラスのサポート：** Druvaのカスタマーサクセスチームによりエンタープライズクラスのサポートが24時間365日提供されます。
データのアーカイブとコンプライアンスが限定される： ユーザーの退職によりプロファイルが削除された場合、管理者が当該ユーザーのデータにアクセスしてダウンロードできる期限は14日間しかありません。当該ユーザーが所有していたドキュメントは14日間の期限後に完全削除されます。	**完全なデータのアーカイブとコンプライアンス：** inSyncを使うと、企業はユーザー退職後も当該ユーザーのデータを無期限に管理できます。退職ユーザーを保全状態とすることで、そのユーザーのデータは削除されずに残るとともに、新規ユーザー用にライセンスを再割り当てすることができます。
不完全な訴訟ホールド： Office 365は、Exchange、OneDrive / SharePointのコンテンツに対してのみインプレースのeDiscoveryおよび訴訟ホールド機能を提供するため、エンドユーザーのデバイスや他のクラウドサービス上の情報は無視されます。	**エンドポイントとクラウドにまたがる訴訟ホールドとeDiscovery：** inSyncでは、バックアップされているすべてのサービス（エンドポイントとクラウド）に対して訴訟ホールドおよびeDiscoveryがサポートされます。inSyncでは、別のストレージリポジトリにデータのリストアや移動を行う必要なしにインプレースの訴訟ホールドが提供されます。inSyncの訴訟ホールドおよびeDiscovery機能は一から開発され、eDiscoveryベンダー（たとえばRecommind, AccessData, Guidance社）向けに設定不要のHTTPSコネクターが提供され、データの収集、分析、処理に利用できます。eDiscovery連携ではリストアを行う必要はありません。カスタムコネクタを使用して即座にeDiscoveryツール内の情報にアクセスできます。
プライバシー： OneDriveの暗号化キーモデルでは、キーがクラウド上に保存されるだけです。このモデルでは、Microsoftが召喚、裁判所命令、データに関する捜査令状を受けた場合など、データのプライバシーが保証されません。	**デジタルエンベロープ暗号化と認証：** inSyncのキー管理は、銀行の貸金庫システムをモデルにしており、両当事者がそれぞれキーを保持します。暗号化はデジタルエンベロープ暗号化の概念に基づいています。この暗号化の仕組みにより、顧客のキーは保存されず、ユーザーのアクティブセッション以外からはアクセスできなくなります。またDruvaが令状、召喚、裁判所命令を受けた場合であっても顧客データを提出することはできません。

最適プランの選択

Microsoft Office 365 では、あらゆる組織のニーズを最大限に満たすためさまざまなプランを利用できますが、サービスと価格はプランによって大幅に異なります。

サービスファミリー: Enterprise		Office 365 E1	Office 365 E3	Office 365 E5
対象顧客	ユーザー当たり月額※1	￥870	￥2,180	￥3,810
	最大ユーザー数	無制限	無制限	無制限
Officeアプリ	Office Online	●	●	●
	フル機能のOfficeアプリ		●	●
	タブレットとスマートフォン		●	●
標準サービス	法人メール機能、カレンダー、連絡先	◒ ユーザーあたり 50 GBのメールボックス	● 無制限のメールボックス	● 無制限のメールボックス
	HDビデオ会議	●	●	●
	チームサイト	●	●	●
拡張サービス	Office 365 Docsのセルフサービスのビジネスインテリジェンス		●	●
	Office365ドキュメントのインプレース保持と訴訟ホールド		●	●
	Advanced eDiscoveryによるOffice 365ドキュメントのサードパーティー審査アプリへのエクスポート機能			●
	未知のマルウェアおよびウイルスからの保護			●
	分析ツール			●

※1: 2018年2月現在。年間契約時の月額相当金額。
出典) https://products.office.com/ja-jp/business/compare-more-office-365-for-business-plans

Office 365 E3+inSyncによるデータ保護と復旧

E1, E3, E5 の大きな価格差を考えると、安価な E3 プランを選択してデータガバナンスと可用性をサードパーティーのアプリケーションで補完するのが、データ保護とガバナンスの適切な組み合わせを探している企業にとって適切です。

主な機能	Office 365 E1	Office 365 E3	Office 365 E5	Druva inSync + E3
コスト				
ユーザー当たり月額※1	￥870	￥2,180	￥3,810	お問い合わせください
可用性				
Office 365ドキュメントのバックアップとリカバリ	◒ 限定的	◒ 限定的	◒ 限定的	●
サードパーティー製クラウドアプリのバックアップとリカバリ				● Office 365, Box, G Suite, Salesforce
デバイス更改用のシステムおよびアプリケーション設定のバックアップ				●
スマートフォンとタブレットのデータバックアップ				●

主な機能	Office 365 E1	Office 365 E3	Office 365 E5	Druva inSync + E3
データガバナンス				
Office 365向け クラウドベースアーカイブ	● 50 GB のメールボックス	●	●	●
Office 365向け 全ユーザー対象の横断検索	●	●	●	●
エンドポイントとクラウドアプリの 全ユーザー対象の横断検索				●
Office 365向け全ユーザー対象の インプレース訴訟対応と インプレース訴訟ホールド				●
エンドポイントとクラウドアプリの 全ユーザー対象のインプレース訴訟 対応とインプレース訴訟ホールド		●	●	●
サードパーティー製審査アプリへの 訴訟ホールドデータのエクスポート			◒ Office 365文書のみ	●
Advanced eDiscovery （高度な電子情報開示）			◒ Office 365文書のみ	●
エンドポイントとクラウドアプリの プロアクティブコンプライアンス				●

※1: 2018年2月現在。年間契約時の月額相当金額。
出典）https://products.office.com/ja-jp/business/compare-more-office-365-for-business-plans

Office 365 サービスの重大な欠点を補完する方法の詳細については
https://jp.druva.com/products/insync/cloud-application-backup/
を参照してください。また、無償トライアルをお試しください。

Druva合同会社
〒100-0004 東京都千代田区大手町1-9-2
大手町フィナンシャルシティ グランキューブ 3F
E-mail: japan-sales@druva.com
URL: jp.druva.com