ホワイトペーパー

複数拠点企業のサイバー保護における、分散管理と集中管理の比較

サイバーセキュリティとデータ保護の分散管理によって、企業のサイバーレジリエンスを高める方法

あらゆる規模の企業が、AI を利用したサイバー攻撃、ハードウェア障害、ソフトウェアの問題、人的エラーといった、さまざまな脅威からシステムのアップタイムとデータの完全性を維持するのに苦労しています。多くの企業が IT 運用とサイバーセキュリティ管理の集中管理化を選択していますが、リモート サイトの IT およびサイバーセキュリティスタッフに運用管理の一部を移管することで、サイバー レジリエンスを高められるケースもあります。

このホワイト ペーパーでは、リモートサイトや遠隔拠点に運用管理の一部を移管することで、企業が稼働率の向上、データ損失の効果的な防止、IT インフラストラクチャとデータの管理およびセキュリティ維持の費用を削減する方法について紹介します。本書では、このアプローチの長所と短所を比較検討し、企業がサイバーセキュリティと IT 運用管理を完全に集中化させることなく、コンプライアンスとガバナンスの目標を達成するための方法について紹介します。

多くの企業が分散を選択

米国企業のおよそ 4 分の 1 は、複数の拠点で事業を展開しています。欧州連合（EU）では拠点の数に基づいた企業レポートはとくにありませんが、複数の拠点を持つ傾向のある小売、接客、医療、金融サービスなどのセグメントが発展していることから、複数拠点を持つ企業が EU 経済でも重要な位置を占めていることがうかがえます。大企業ほど、地方オフィス、製造工場、倉庫および配送センターといった複数の拠点を持つことが多くなっています。

合併や買収を利用して自社のセクター内、他の業種および他の地域で事業を拡大しようとする企業も、集中管理化された IT およびサイバーセキュリティのスタッフから物理的に離れた拠点を多数持つことがよくあります。

分散化されたビジネスの例

小売業界は、高度に分散化されたビジネスの顕著な例となっています。典型的な小売業者は、世界および地域の本部、配送倉庫、および消費者向けの実店舗を展開しています。小売業界以外の多くのビジネスも、以下の例のように、地理的に分散した多くの店舗やオフィスを持つ小売企業と同様の構造となっています。

- 眼科、クリニック、歯科医院、薬局および動物病院などの医療サービス。
- 多数の支店を持つ、銀行、保険および金融サービス会社。

- 多数の配送センターとさらに多くのリテール配送とビジネスサービスの店舗を持つ、出荷/受け取り、宅配、運送会社。
- 場外馬券売り場、場外車券場、パチンコ店、および同様の施設を複数持つゲーム企業。
- ガソリンスタンドや電気自動車の充電施設が、コンビニエンスストアやクイックサービスレストランと組み合わされていることの多い、ロードサイドサービス。
- 企業はオペレーションの連携を前提に組織化されており、そのなかで中央のチームが会社全体の IT 運用、サイバーセキュリティおよびコンプライアンスを監督できます。ただし、個々の施設には独自の予算、スタッフの配備、およびビジネスユニットの IT インフラストラクチャを管理するための自治権があります。

IT とサイバーセキュリティの集中管理が課題になることも

高度に分散化されたビジネスでは、さまざまなテクノロジーベンダーのハードウェア、仮想化およびオペレーティングシステムとともに、さまざまテクノロジベンダーの在庫システムや POS システムなどのアプリケーションが混在していることがよくあります。技術インフラストラクチャとソフトウェアのリビジョンレベルの組み合わせが、拠点によっては大きく異なる場合もあります。

安定した運用テクノロジ環境を維持するために、レガシーのアプリケーション、カスタムビルドのソフトウェア、およびコンピューターを使い続けることが必要になっているために、企業全体で IT 標準化を推進することが困難になっており、IT 資産とサイバー セキュリティ ツールが増加することがあります。

中央に集中配備されたスタッフは、アプリケーションとデータを組織全体にわたって保護および管理し、セキュリティ施策を施すのに必要なすべてのツールに精通しなければならないこともあります。一方、アプリケーションは複雑さと多様性を増しており、それらを管理し、保護するためのツールも確実に増え続けています。

工場の作業環境のような、セキュリティ要件が高い遠隔地は、エアギャップ化される可能性があるかもしれません。つまり、サイバー脅威への露出を最小限に抑えるために、企業ネットワークやパブリックインターネットから物理的に隔離されるかもしれません。その結果、中央のスタッフがリモート デスクトップ管理とその他のネットワークベースのツールを使用して、問題を診断および解決するためのアクセスが制限されるようになり、問題解決のために遠隔地への物理的な移動が必要になる可能性もあります。

砂漠の製油所、沖合の石油プラットフォーム、採掘施設、および陸上輸送ハブから遠く離れたその他の場所のような、アクセスが困難な場所では、これらの制約によりコストと時間を要する場合があります。

大規模かつ単一拠点の企業でデータ保護とセキュリティを管理すれば、地理的に離れている複数の拠点に分散している、同じ数のアプリケーションとエンドポイントを保護する場合よりも、複雑さは軽減され、時間もかかりません。バックアップデータが拠点ごとに隔離されていないと、1 つの拠点でバックアップからの復元を行った場合に、すべての拠点のパフォーマンスに悪影響が及ぶ可能性があります。

遠隔地では、広域ネットワークの接続性とネットワーク速度が地域によって大きく異なる場合があり、復旧時間が予測できなくなるだけでなく、復旧時間の基準を満たすまでに時間がかかりすぎる可能性があります。

リモート サイト管理では、IT スタッフがローカルのデータリポジトリとセキュリティ管理コンソールに個別に、繰り返しログインしなければならないことがあり、効率が悪くなるだけでなく、エラーが発生しやすくなり、処理が遅くなる可能性があります。従来のバックアップ、ディザスタリカバリおよびセキュリティためのツールの多くは、特定のアプリケーション環境に特化しているため、一般的なツールを組織全体で標準化するのが困難になっています。

その結果、IT 運用管理ツールとセキュリティツールが増え続け、費用がかさみ、サポートスタッフのオンボーディングとトレーニングのための費用も増えます。これは、IT とサイバーセキュリティスタッフの費用がずっと高止まりしている世界では、大きな問題となっています。

コンプライアンスを集中管理するのは困難

コンプライアンス要件も国によって大きく異なり、場合によっては州、省および自治体によっても異なります。たとえば、米国で事業を展開している企業は、連邦政、米国の複数の州、さらには個々の都市のプライバシー規制に従わなければならない場合があります。

データ主権のコンプライアンスも、大きな課題になりつつあります。これらの規制は、機密データを保存できる、あるいはネットワークを介して移動させることのできる、物理的な場所、データセンターおよびネットワークを制限するものとなっており、一部の国家政府が秘密裏に監視を行ってデータのプライバシーを侵害するかもしれないという前提に基づいています。広範囲に分散したビジネス全体でこれらの要件に従おうとすれば、管理が複雑になり、アプリケーションの性能に悪影響を与える可能性があります。

どのデバイスのどのデータを保護する必要があるのか、どの IT インフラストラクチャ要素がセキュリティと規制のさまざまな基準に適合していると認定されているのか、ならびにどの従業員がそのデータへのアクセスを許可されているのかを追跡し続けていると、混乱が生じ、組織によってコンプライアンスの費用に差異が生じるかもしれません。このような煩雑さが発生している一方で、ほとんどの企業では IT およびサイバーセキュリティのスタッフの予算が横ばいまたは縮小しているのに、管理および保護しなければならないデータの量が増え続けています。

規制当局は現在、重大な罰則を課して、コンプライアンスを強化しようとしています。たとえば、EU では、消費者データの保護に繰り返し失敗した企業に対して、定期的に年間収益の 2 ～ 4% の罰金を課しています。

これは、分散型の、複数拠点を持つ企業にとっては大きな問題になりかねません。たとえば、セキュアなアクセス管理、安全なアクセス制御、および一貫性のあるストレージなどの機能を備えたアプリケーションやストレージをホスティングしており、さらにコンプライアンス要件を満たしている、安全なサードパーティホスティングを見つけることが、ネットワーキングの潜在的な課題になり得るからです。

アクロニスは、複数拠点企業の管理とセキュリティの課題に取り組んでいます

Acronis Cyber Protect は、分散環境にデータ保護とセキュリティのソリューションを提供するという課題に、リモート管理、バックアップ、災害復旧および単一のプラットフォーム上でのセキュリティの統合によって対応いたします。個々のリモート拠点は、その拠点専用のコンソールから、現地スタッフが個別に構成および管理でき、コンソールはサイトにインストールすることも、クラウドでホストすることもできます。

各拠点のデータ保護計画とバックアップスケジュールはカスタマイズすることも、あるいは計画とスケジュールを標準化し、複数の拠点に展開することもできます。ローカルのすべてのリソースのデータ保護とセキュリティは、画面やアプリケーションを切り替えることなく、単一のコンソールから管理できます。

セキュリティおよびデータ保護のあらゆる機能は、各エンドポイントにインストールされた、単一のエージェントで管理されます。データ全体の暗号化とトランスポート層セキュリティ (TLS) による安全な転送により、転送中のデータが安全に保たれます。さらに、データ圧縮、重複除外および帯域幅調整が自動的に管理されて、トラフィックが妥当な接続速度に最適化されるとともに、実行中の操作への影響が最小限に抑制されます。

一方、本社の IT およびサイバーセキュリティスタッフは、図 1 に示すように、集中管理されたダッシュボードを通じて遠くの拠点を監視し、組織全体でのサイバーリスク、データ保護状態およびコンプライアンス状況を評価することができます。

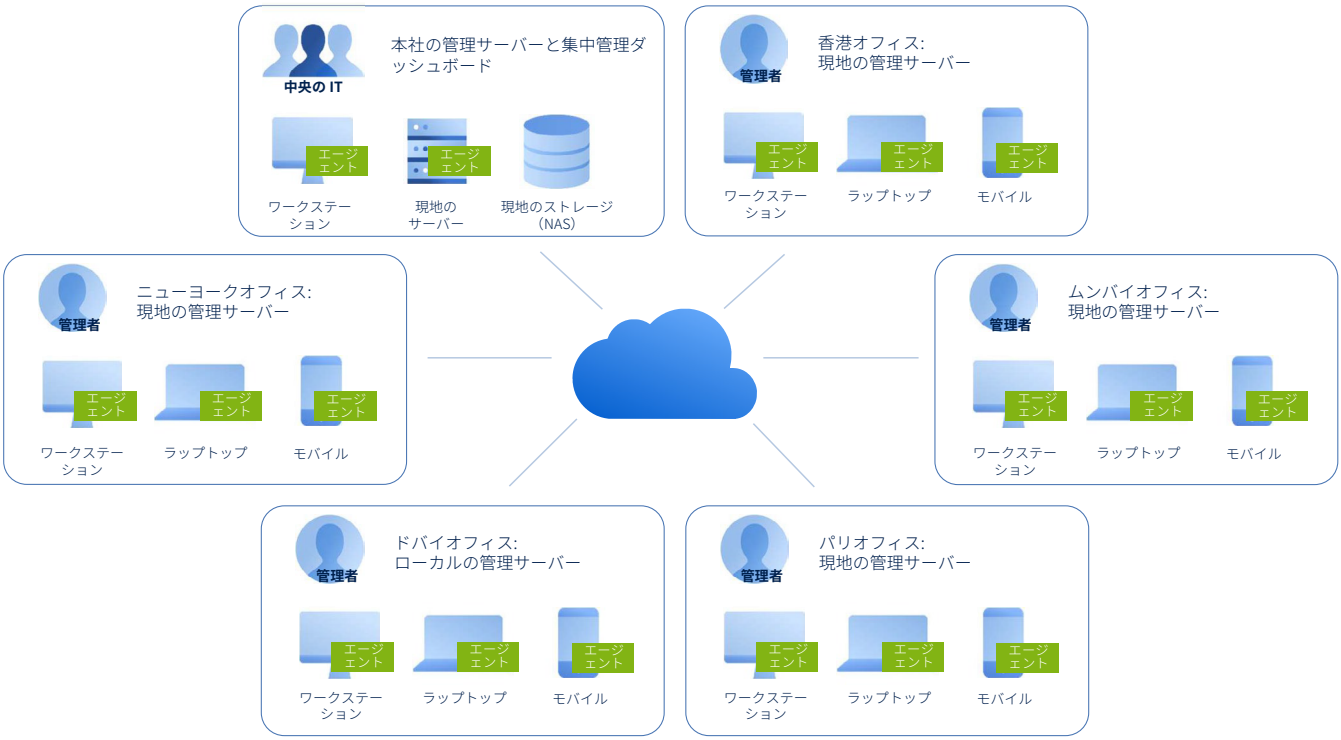

図 1.ローカル制御と集中監視による、サイバーセキュリティと IT 運用のマルチサイト管理

Acronis Cyber Protect の主な利点

- データストレージとセキュリティを拠点ごとに分離します。
- ハードウェア、ソフトウェアおよび仮想化に関連する、サイバーセキュリティの互換性の問題を軽減または解消します。
- データ主権の問題を解決し、規制コンプライアンスを促進します。
- 異なったネットワーク構成と接続に関連する問題を解消します。
- データ保護のために複数のホスティング環境が必要となる状況を、抑制または解消します。
- 物理的な拠点全体で、費用を一貫性があり、予測可能なものにします。
- 地理的に冗長なストレージを合理的に配置できます。
- 企業全体のサイバーリスク診断、データ保護状況およびコンプライアン状況を集中監視できるようになります。

アクロニスのソリューションは画像とファイルがベースになっており、ビジネスや製造業で使用されている、ほとんどのコンピューティング環境と互換性のある、クロスプラットフォームエージェントを採用しています。アクロニスは、Microsoft 365 や Google Workspace などのクラウドベースの Eメールとコラボレーションプラットフォーム、ならびにオンサイトの Microsoft Exchange のようなオンプレミスベースのプラットフォームも保護します。

対応仮想化システム一覧

VMWare vSphere 4.1、5.0、5.1、5.5、6.0、6.5、6.7、7.0、8.0

Microsoft Hyper-V Server 2022、2019、2016、2012/2012 R2、2008/2008 R2

Citrix XenServer / Citrix Hypervisor 8.2 – 4.1.5

Linux KVM 8 – 7.6

Scale Computing HyperCore 8.8、8.9、9.0

Red Hat Enterprise Virtualization (RHEV) 3.6 – 2.2

Red Hat Virtualization (RHV) 4.0、4.1

Red Hat Virtualization (oVirt) 4.2、4.3、4.4

Virtuozzo 7.0.14 – 6.0.1.0

Virtuozzo Infrastructure Platform 3.5

Oracle Linux Virtualization Manager (Oracle LVM) 4.3

Nutanix Acropolis Hypervisor (AHV) 20160925x – 20180425x

Virtuozzo Hyper Server 7.5

Virtuozzo Hybrid Infrastructure 4.3 – 3.5

分散環境の場合のデータ主権とコンプライアンス

アクロニスは、世界中各所に拠点を持つ、グローバルで独立したデータ センター ネットワークを運営しており、分散型ビジネスがきわめて柔軟にデータストレージのセキュリティを維持しながら、データ保護性能を最適化し、データ主権のコンプライアンス規制に対応できるように支援しています。個々のリモート拠点では、拠点ごとにデータ保護とセキュリティを管理でき、コンプライアンスが必要なとき、および場所では、サーバー、エンドポイント、Eメール、コラボレーション データをさまざまな国で保管できます。

単一のプラットフォーム上の現地のコンソールでエンドポイント管理、データ保護およびサイバーセキュリティを統合することにより、IT 運用費用を約 60% 削減できるようになります。企業は、複数の IT およびサイバーセキュリティ ツールについてのスタッフのトレーニングとその維持に関連する諸経費、ならびにサードパーティの地理的要件に準拠したデータストレージと転送の費用を削減することで、さらなる節約が可能になります。

分散型および複数拠点のエンタープライズでは、セキュリティ、バックアップおよびディザスタリカバリのソリューションの導入と維持で独自の課題を抱えています。この例としては、複数の場所にまたがるソリューションの管理、ハードウェアソフトウェア テクノロジの無数の組み合わせを通じて提供されるサービスのナビゲートと維持、データプライバシーおよびデータ主権規制の順守、ならびにリソースと予算が制限された環境でのこれらのサービスの提供などがあります。国境を越える企業の場合、これらの課題はさらに大きくなります。

マルチサイト管理の利点

独立したエージェントを使った、遠隔拠点用のローカルコンソール

- それぞれの拠点、部門、事業単位、またはブランド向けの、オンプレミスまたはクラウドホストの単一のコンソール。
- 帯域幅の調整、データ圧縮および重複除外は常に増分的であり、オプションで物理ディスクの転送もできます。
- ソースのエージェントはデータ暗号化と TLS による安全な転送が施され、企業のネットワークを使用する必要はありません。

本社のダッシュボードが、リモートサイトのすべてのアクロニスのコンソールを集約監視

- リモート サイトのすべてのアクロニスのコンソールを集約的に、または個別に監視します。
- すべてのリモートデバイス、アラートおよびアクティビティが統合され、表示されます。
- リモートサイトのアクロニスのコンソール ウィジェットからデータをダウンロードします。
- 任意のリモートアクロニスのコンソール上の特定のデバイスを掘り下げることができます。

複数のツールを統合

単一のエージェントとコンソールによる管理

- バックアップとディザスタリカバリ。
- EDR（エンドポイントの検知と対応）による、Eメールとエンドポイントのセキュリティ。
- パッチ適用、インベントリ、リモート アシスタンス、スクリプト作成および監視。

ワークロードの保護

- サーバー、VM、クラウド VM およびワークステーション。
- デスクトップ、ラップトップおよびモバイルデバイス。
- Windows (2003/XP 以降)、Mac、Linux。
- Microsoft 365 および Google Workspace。

現地でのコンプライアンスの向上

- 50 を超えるグローバルデータセンター。
- 日本国内に 2 つのデータセンター。
- 企業保有のパスワードを使い、AES-265 によって、データのソースを暗号化。
- 暗号化されたデータは、SSL/TLS を使って送信。
- 不変ストレージ。
- 多要素認証。
- ロールベースのアクセス。

グローバルコンプライアンス認証。

ベンダーを使った場合のコストと煩わしさを軽減

アクロニスをベースにした統合により、複数のベンダーのツールを組み合わせた場合より、約 60% の費用削減が可能になります。

リソース制限の緩和

単一コンソールで、単一管理。

日常業務を支援する AI と機械学習 （ML）。

- デバイスの監視と自動修正。
- AI によるセキュリティインシデントの調査と修復。
- 自動バックアップと DR テスト。
- メンテナンスタスク用自動化スクリプトのライブラリ。

最後に

ほとんどの企業では、中央のスタッフが IT 運用とサイバーセキュリティの管理を行っていますが、IT 運用管理およびセキュリティ管理機能の一部を地方や遠隔地のチームに移管すれば、サイバーレジリエンスが向上できるようになる企業も現れるでしょう。

サイバー脅威、ならびにダウンタイムやデータ損失を招く、その他の原因に対する企業の防御、さらにインシデント発生時にデータとシステムを迅速に復旧する能力の管理を分散すれば、企業は、集中管理に比べて、より効果的にビジネスリスクを軽減できるようになります。

マルチサイトでローカル管理を行う企業は、サイバーセキュリティ、データ保護およびエンドポイント管理をネイティブ統合させるツールを備えた、地域およびリモートサイトのチームを持つ必要があります。地域レベルおよびリモートサイトレベルで使用されているコンソールを集中監視する能力を付け加えることにより、本社の IT チームとサイバーセキュリティチームは、IT ガバナンスとコンプライアンスについての自社の基準を適用させ、それが守られているかどうかを監査できるようになります。

IT 運用とサイバーセキュリティの中央での集中監視と分散管理をこのように組み合わせることにより、サポート対応の簡素化（とりわけ、エアギャップされた施設や非常に離れた場所にある施設の場合）、地域のセキュリティおよび IT 関連規制へのコンプライアンス強化、ならびに全体的なビジネスリスクの軽減が可能になります。

もっと詳しく知る

サイバーセキュリティと IT 運用管理では、集中監視型および分散制御型のトポロジのいずれが自社のビジネスに適しているかのを、アクロニスにご遠慮なくご相談いただけます。へのお問い合わせは、こちらから。

Acronis Cyber Protect の 30 日間無料トライアルのお申し込みは、こちらから。

アクロニスについて

アクロニスは、ネイティブに統合されたサイバーセキュリティ、データ保護およびエンドポイント管理をマネージド サービス プロバイダー（MSP）、中小企業 （SMB）およびエンタープライズの IT 部門に提供している、グローバル サイバープロテクション企業です。アクロニスのソリューションは効率性に優れており、最小限のダウンタイムで、最新のサイバー脅威を識別、防止および検出し、それらへの対応、その後の修復と回復によって、データの整合性とビジネスの継続性を維持するように設計されています。アクロニスは、多様かつ分散した IT 環境のニーズを満たす独自の機能を備えた、市場で最も包括的な MSP 向けセキュリティソリューションを提供しています。

2003 年にシンガポールで設立された、スイスの企業であるアクロニスは、全世界に 45 の拠点を有しています。Acronis Cyber Protect Cloud は、150 の国で 26 の言語で提供されており、20,000 を超えるサービスプロバイダーに使用され、750,000 を超える企業を保護しています。詳細は、www.acronis.com をご覧ください。

Acronis

詳細は、www.acronis.com をご覧ください。