ホワイト ペーパー

事業分離やカーブアウトにおけるサイバー セキュリティの完全性の確保

はじめに

事業分離のプロセスにおいて、IT リーダーは売り手側 (RemainCo) の業務も、分離対象のエンティティー (SpinCo) の業務も中断することなく、安全に分離の準備を進めるという二重の責務を負っています。移行サービス契約 (TSA) の一環として、売り手側は SpinCo が事業を完全に独り立ちさせるまで、あるいは買い手側と完全な統合を達成するまで、必要な IT 支出をサポートすることに同意します。その際、RemainCo には、SpinCo と買い手側のユーザーのために、RemainCo の利用環境への安全なアクセス パスを作成しなければならないという、独特の課題が発生します。

売り手は通常、ビジネスを売りに出す数か月前から売却の準備を開始します。ビジネスの観点から鑑みた売却範囲が確定したら、売り手は SpinCo から引き継がれる技術資産や人材、RemainCo 内にとどまる技術資産や人材、それによって TSA が必要になるものなど、取引の境界を把握する必要があります。これは、IT 資産を保護して取引を確実に成功させるうえで不可欠な要素です。

取引上の境界が確定したら、売り手は SpinCo を独立した事業として運営するための単体の業務および資本支出を示すプロフォーマ財務諸表を作成します。そして最後に、売り手は SpinCo の従業員が安全にアクセスできるように、暫定的なアーキテクチャー アプローチに取り組むことになります。

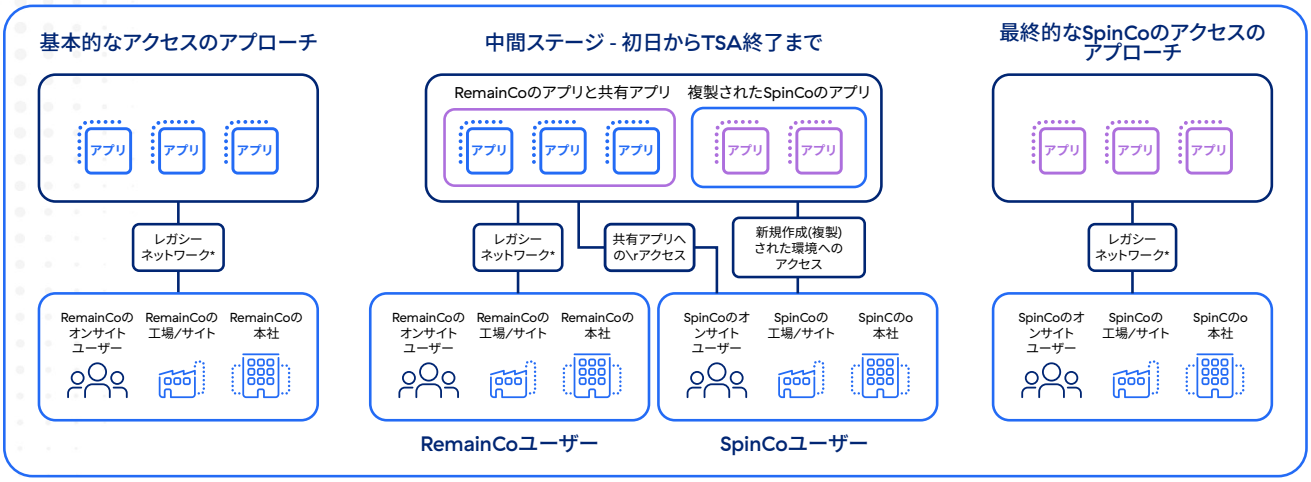
従来型のアプローチ

従来型のアプローチはネットワークベースの分離戦略を採用しており、TSA 期間中に売り手がアプリケーションへのアクセスを提供する方法には、次のような選択肢があります。

説明	潜在的な欠点
売り手の現在の環境内で SpinCo ユーザーに共有アクセスを付与する	セキュリティ態勢が不明なユーザーからアクセスされるため、侵害のリスクが非常に高い。
SpinCo 専用のアプリケーションを別の環境に移動し、現在の環境内で共有アプリケーションへのアクセスを提供するハイブリッド アプローチ	セキュリティ態勢が不明なユーザーからアクセスされるため、侵害のリスクが非常に高い。また、売り手が別の環境を分割して、トラフィックをセグメント化するため、かなりの先行作業が必要になる。
すべてのアプリケーションを別の環境に移行する (専用アプリケーションはそのまま移動でき、共有アプリケーションは SpinCo データのみを保持して複製可能)	このアプローチでは、新しい環境に移行する必要があるすべてのアプリケーションとデータを完全に理解する必要があるだけでなく、複数のワークストリーム (アプリケーション、データ、ホスティング、ネットワークなど) に依存するため、非常に複雑になる可能性がある。

前述したように、このアプローチには数か月にわたる事前計画が必要であり、企業は分離プロセスが始まる前の段階から、ハードウェアやネットワーク インフラストラクチャー コンポーネントのサプライチェーン問題を考慮して、安全な仲介ネットワークを設定するといった保守的なスケジュールを組むことになります。さらに、RemainCo のネットワークは SpinCo ユーザーに公開されているため、水平移動や情報漏洩のリスクも発生します。

従来型のアプローチ：エンティティー間アクセス用の中間ネットワークを備える複製された SpinCo ネットワーク



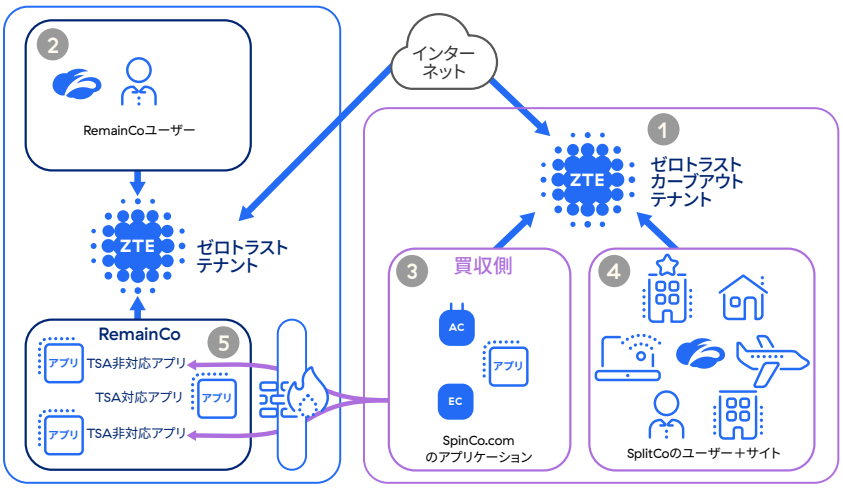
*従来型のアプローチでは、MPLS、ファイアウォール、ロード バランサーなどを利用

例えば、ある大手小売業者は先日 2 つの事業体に分割されましたが、2 年間の TSA 期間中はアプリケーション、インフラストラクチャー、ネットワークを共有していました。事業分離を確実に成功させるには、個別の IT 環境を作成したうえで、アプリケーションを複製して複雑なネットワークを簡素化する必要があります。これは、IT リーダーやビジネス リーダーの双方にとって難しい課題であり、案件の価値を高めるうえでリスクとなる可能性があります。

Zscaler のクラウド プラットフォームに支えられた最新アプローチ

Zscaler のクラウドベースのゼロトラスト プラットフォームは、従来型のネットワーク セグメンテーションやハードウェア主導の接続アプローチを排除します。このプラットフォームは、Zscaler のクラウドによって施行されるアクセス ポリシーを定義することで、ユーザー レベル、アプリケーション レベルでのセグメンテーションを実現します。通常、事業分離においては、共有環境で共有アプリケーションへの接続を可能にするために、テナントが立ち上げられます。そこからポリシーや影響を受けるユーザーを定義し、アクセス権を付与します。

Zscaler のアプローチ：カーブアウト テナントを介した SpinCo へのゼロトラスト アクセス



1. SplitCo ZTE のテナント、IDP、ドメインを確立
2. ユーザー、アプリ、ポリシーを定義するための環境を作成
3. SplitCo のユーザーを SplitCo ZTE にリダイレクト
4. SplitCo ZTE に SplitCo のアプリを割り当て
5. 残された TSA 対象アプリの制御を確立

Zscaler が先日支援を行った大手産業コングロマリットでは、分離された事業体向けに別のテナントが作成され、ポリシー構成を使用して共有アプリケーションへのアクセスが制限されていました。最終的に、分離された事業のすべてのユーザーが新しいテナントに移行されました。このような事業分離の際、Zscaler は専用環境と共有環境の両方にアクセスするあらゆる場所の異なるペルソナを持ったユーザーをサポートします。

事業分離時に Zscaler がサポートする一般的なユース ケース

1. **カスタム アプリケーションへのアクセス：** Zscaler Private Access (ZPA) を活用して、オンプレミスのデータ センターまたはパブリック クラウドでホストされているカスタム アプリケーションへのアクセスを保護します。Zscaler は、共有および専用アプリケーションをホストする売り手の環境と、SpinCo の環境およびその専用アプリケーションの双方へのアクセスを保護する機能を提供します。これらはすべて、クラウド構成ベースのアプローチを通じて、リモート ユーザーとオフィス ユーザーの両方に迅速に実現できます。追加のハードウェアは一切必要ありません。

2. **インターネット トラフィックの保護：** Zscaler Internet Access (ZIA) が SaaS アプリケーションやインターネット Web サイトへのアクセスを保護します。さらに、ボタンをクリックするだけで高度な脅威対策機能を有効にして、移行期間中のサイバー攻撃や侵害のリスクから売り手を保護します。

3. **アプリケーションの検出：** Zscaler はすべての展開が完了すると、SpinCo ユーザーが使用するアプリケーションを検出します。これにより、IT 部門は使用頻度が最も高いアプリケーションとその使用パターンを把握できるようになるため、TSA 期間中の分離の必要性を判断するのに役立ちます。

4. **パフォーマンスの監視：** Zscaler Digital Experience (ZDX) は、Zscaler ZTE 管理ポータルで一元化された画面を提供します。この管理ポータルを通じて、売り手と SpinCo 双方のヘルプデスクがネットワークの停止やパフォーマンスの問題を細かく監視できるため、IT 運用の負担が軽減されます。また、ZDX は 2 つの環境間で必要なテレメトリー データを提供することで、サポート チケットの処理や問題の所有者の特定といった困難なプロセスから売り手と SpinCo 双方のヘルプデスクを解放します。

Zscaler のアプローチのメリット

 **価値実現までの時間**	• アプリケーションのインベントリーを速やかに確定 • ユーザーとアプリケーション間の接続を数週間で実現 • TSA の期間を短縮
 **簡素化**	• 初日の準備のためのクリティカル パスから IT を除去 • 100% クラウドベースのアプローチを接続に活用 • ゼロトラスト ソリューションでアクセス パスとインターネット トラフィックを保護
 **財務**	• 一時的および経常的な分離コストを削減 • TSA コストや座礁資産 / 技術的負債を削減 • 移転可能な Zscaler プラットフォームで IT の立ち上げコストを削減
 **完全性**	• 情報漏洩のリスクを最小化 • 内部脅威や第三者による不正アクセスを削減 • 監査可能な制御を有効にして初日の必要事項に対応

まとめ

従業員が生産性を発揮できるように、適切なタイミングで安全なアクセスを提供する ── 事業分離の際にこれを実現しようとすると、多くの混乱や課題が生じるため、IT の分割は難航する場合が少なくありません。さらに、従来のアプローチでは 2 つのネットワーク間が露出することで、サイバー リスクが発生しやすくなります。Zscaler は、大企業レベルの分離に取り組む場合だけでなく、小規模な資産を売却する場合でも、取引範囲に含まれる主要なアプリケーションにユーザーが安全にアクセスできるようにする過程で、極めて重要な役割を担います。Zscaler は分離プロセスを簡素化しながら、サイバー リスクを大幅に軽減します。

zscaler™ | Experience your world, secured.™

Zscaler について

Zscaler (NASDAQ: ZS) は、より効率的で、俊敏性や回復性に優れたセキュアなデジタル トランスフォーメーションを加速しています。Zscaler Zero Trust Exchange は、ユーザー、デバイス、アプリケーションをどこからでも安全に接続させることで、数多くのお客様をサイバー攻撃や情報漏洩から保護しています。世界 150 拠点以上のデータ センターに分散された SSE ベースの Zero Trust Exchange は、世界最大のインライン型クラウド セキュリティ プラットフォームです。詳細は、**zscaler.jp** をご覧いただくか、Twitter で **@zscaler** をフォローしてください。

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.jp