CASESCENARIO™ サンプル

対象業種：小売業
ゼロトラストDXソリューションの導入

αB Alpha Branding Corp.

CaseScenario™｜小売業

ゼロトラストDXソリューションの導入

目次

第1章　業界フィールドの設定 4

1-1. 業界の市場環境 4

1-2. 業界各社への経営的影響 4

第2章　想定企業のプロファイル 5

2-1. 企業概要 5

2-2. 業界における立ち位置 5

第3章　想定企業が直面している経営課題 7

3-1. 構造的な制約と課題の背景 7

3-2. 対応すべき経営課題の整理 7

経営課題1：事業継続性の確保 7

経営課題2：顧客信頼と説明責任の維持 8

経営課題3：運用品質とコストの両立 8

第4章　経営課題を現場レベルで見ると 9

4-1. 店舗・本社・物流・ECをまたぐアクセス経路の統制不足 9

4-2. 権限管理の複雑化（特権ID・委託先ID・兼務の増加） 9

4-3. 端末管理のばらつき（店舗POS・物流ハンディ・本社PC・BYODの混在） 10

4-4. クラウド利用・SaaS増加に対する可視化と制御の不足 11

4-5. 外部委託先・パートナー連携に伴うサプライチェーンリスク 11

第5章　ソリューションによる業務課題への対応 13

5-1. 本提案の対象範囲 13

5-2. 各業務課題への対応内容 13

状態変化1： アクセス経路が「説明可能な統制下」に置かれる状態へ 13

状態変化2： 権限が「付与根拠とライフサイクル」で管理される状態へ 14

状態変化3： 端末が「最小基準」で揃い、例外が追跡可能な状態へ 14

状態変化4： クラウド・SaaS利用が「設定と権限の棚卸し」で回る状態へ 14
状態変化5： 外部委託先接続が「統制と運用の分離」で管理される状態へ 15
第6章　経営課題への効果 16
6-1. 各経営課題への寄与 16
経営課題1：事業継続性の確保への寄与 16
経営課題2：顧客信頼と説明責任の維持への寄与 16
経営課題3：運用品質とコストの両立への寄与 16
6-2. この提案を経営アジェンダとして位置づける理由 17
APPENDIX 19
業務課題と紐づく経営課題の整理 19
1. 店舗・本社・物流・ECをまたぐアクセス経路の増加と統制不足 19
2. 権限管理の複雑化（特権ID・委託先ID・兼務の増加） 19
3. 端末管理のばらつき（店舗POS・物流ハンディ・本社PC・BYODの混在） 20
4. クラウド利用・SaaS増加に対する可視化と制御の不足 20
5. 外部委託先・パートナー連携に伴うサプライチェーンリスク 21
6. セキュリティポリシー運用の複雑さと標準化の遅れ 22

第1章　業界フィールドの設定

1-1. 業界の市場環境

小売・EC業界は、消費者行動のオンラインシフトとオムニチャネル化の進展により、事業運営の前提が構造的に変化しています。店舗販売だけで完結していた業務は、EC・物流・マーケティング・外部パートナーを跨いで動くことが常態となり、クラウド利用やリモートアクセス、外部連携が増えるほど、IT基盤は「売上を伸ばすための武器」であると同時に、「止まれば事業が止まる」インフラとしての性格を強めています。

同時に、外部環境の圧力も複合的に増しています。サイバー攻撃は高度化・継続化し、委託先やSaaS経由のサプライチェーン侵害が相次いでいます。個人情報保護法の強化、委託先管理の厳格化、ログ保全要求の引き上げなど、規制・監査の要求水準も上がり続けています。加えて、小売現場では人手不足と人員入れ替わりが進行しており、属人的な運用や拠点ごとのばらつきは、リスクと管理コストの両面で増幅要因となっています。

1-2. 業界各社への経営的影響

こうした環境変化は、業界各社の経営判断の比較軸そのものを書き換えつつあります。

第一に、事業継続性の観点です。店舗・物流・ECのいずれかで事故が起きれば業務停止と復旧負荷が連鎖しやすく、オムニチャネル体制であるほど影響範囲が広がります。セキュリティは「守りのIT投資」ではなく、事業継続を左右する経営インフラとして扱う必要性が高まっています。

第二に、顧客信頼と説明責任の観点です。顧客データを活用したマーケティングやパーソナライズ施策を継続する前提として、「誰が・どのデータに・どの条件でアクセスしたか」を説明できる状態が求められます。説明できないこと自体が、規制対応・取引先対応・顧客対応のすべてにおいて経営リスクとなります。

第三に、運用品質とコストの観点です。拠点・部門・委託先ごとに運用ルールが分かれたまま統制を強めようとすると、例外対応が増殖し、IT管理部門の負荷が事業拡大以上に膨らみます。標準化と自動化を前提に置かなければ、統制強化は運用コストの肥大化として跳ね返ります。

業界各社に共通する経営的影響は、この3軸で整理できます。次章では、これらの業界共通の構造を、本提案が想定する企業に具体化して位置づけます。

第2章　想定企業のプロファイル

本章以降、想定企業としてアルファリテール株式会社（仮名、以下「アルファリテール」）を設定し、一貫してこの名称で記述します。

2-1. 企業概要

企業名	アルファリテール株式会社（仮名）
業種	小売・EC業界（総合小売業）
事業内容	実店舗運営、EC運営、物流・在庫管理、マーケティング
従業員数	約3,200名
拠点構成	国内500店舗／EC・物流拠点3カ所
売上規模	年間約2,500億円
主要取引先	大手消費財メーカー、食品メーカー、物流会社

アルファリテールは、食品・衣料・家電・日用品まで幅広い商品を扱う総合小売企業であり、自社ECと主要オンラインモールを組み合わせたオンライン販売、および店舗とECの在庫を統合管理するオムニチャネル運営を事業の中核に据えています。

2-2. 業界における立ち位置

アルファリテールは、消費財・食品メーカーおよび物流会社との取引基盤を持ち、店舗とデジタルチャネルを組み合わせた顧客体験の高度化を推進しています。EC比率の拡大に合わせて、オンラインとオフラインを横断したマーケティング施策や、AIを活用した需要予測・仕入れ調整を進め、リピーター獲得を中心に競争力を維持しています。

現在の経営上の最重点テーマは、オムニチャネル運営の高度化と顧客データ活用の継続的な拡張にあります。一方で、これらのテーマを支えるIT・データ活用範囲が広がるほど、事業運営の構造に起因する制約が顕在化しやすくなっています。

アルファリテールには、以下の構造的な制約が内在しています。

第一に、事業運営が「店舗・物流・EC・本社・外部パートナー」を跨ぐ横断構造になっている点です。500店舗、EC拠点3カ所、多数の外部委託先が同時並行で動くため、アクセス経路・権限・端末状態を全体で把握しにくく、拠点ごとの運用最適化が全社統制と両立しにくい構造になっています。

第二に、顧客データ活用と委託先連携が成長戦略の前提になっている点です。パーソナライズマーケティングやオムニチャネル在庫連携は、顧客データと委託先データを横断的に扱うことが前提となるため、データ保護と説明責任の水準が、そのまま成長施策の実行可能性を規定します。

第三に、小売業特有の低利益率構造と人員入れ替わりの激しさです。運用負荷の増大は利益率に直接跳ね返り、人員入れ替わりの多さはアクセス権限や端末運用の棚卸しを人手依存で回す限界を早めます。

これらの制約は、いずれも「現場の工夫や個別拠点の努力では吸収しきれない」水準に近づきつつあります。次章では、これらの構造的制約がどの経営課題として浮かび上がるかを整理します。

第3章　想定企業が直面している経営課題

3-1. 構造的な制約と課題の背景

アルファリテールでは、オムニチャネル運営と顧客データ活用の拡張に合わせ、扱うシステム・データ・接続先が拡大を続けています。一方で、アクセス管理・端末管理・クラウド利用の統制は、従来の境界防御とVPN中心の運用を拡張する形で積み上げられてきました。現場では拠点単位の工夫や例外運用で対処が進められていますが、外部連携とクラウド利用の増加ペースに対して、統制設計の追随が構造的に難しくなっています。

この状態が継続すると、情報セキュリティはIT部門の運用課題に留まり続け、経営としての優先順位が付きにくくなります。結果として、事業停止・顧客信頼毀損・監査対応失敗・運用コスト増大のいずれかが顕在化して初めて、経営論点として扱われることになります。現場の工夫が限界に達する前に、経営として比較・判断できる論点に組み替える必要があります。

3-2. 対応すべき経営課題の整理

アルファリテールが今期のアジェンダとして扱うべき経営課題は、以下の3点に集約されます。これらは、他の投資案件と並べて比較される際の経営判断の比較軸として機能します。

経営課題1：事業継続性の確保

オムニチャネル運営を支える基盤として、店舗・物流・EC・本社・外部パートナーにまたがるアクセスを統制し、事業停止リスクを下げることが求められています。500店舗と3拠点のEC・物流、多数の委託先接続が同時並行で動く構造においては、いずれか一点での事故が横展開しやすく、復旧長期化が売上機会損失と取引先対応コストに直結します。

なぜ今期の重点課題か：オムニチャネル戦略の継続性が、IT基盤の統制成立を前提条件としている点にあります。事業の成長速度と統制の追随速度が乖離すると、成長そのものがリスクとして跳ね返ります。

比較軸としての位置づけ：他の投資案件と並べた際、「事業を止めない」という経営の最重要軸に直結する論点として優先順位が付きます。

経営課題2：顧客信頼と説明責任の維持

顧客データを活用した成長施策を継続するためには、データ保護と監査・規制対応を両立し、顧客信頼を毀損しない状態を維持することが必要です。パーソナライズマーケティングとオムニチャネル連携は、顧客データへのアクセスが「誰が・何のために・どの条件で行われたか」を説明できる状態を前提とします。説明できないこと自体が、個人情報保護法対応・委託先管理・取引先ガバナンスのすべてにおいてリスクとなります。

なぜ今期の重点課題か：データ活用の深化がすでに進行しており、説明責任の基盤整備を後回しにできる段階を過ぎている点にあります。事故が起きてから整えるのでは、事業上の信頼コストが回収不能になります。

比較軸としての位置づけ：「顧客信頼を毀損しないか」「規制・監査要求に耐えられるか」という軸で評価される論点であり、成長施策と並列で判断されます。

経営課題3：運用品質とコストの両立

拠点・人・委託先に依存した運用を減らし、権限・端末・クラウド利用・ログ管理を標準化・自動化することで、統制を強めながら運用負荷を抑えることが求められています。低利益率構造の小売事業においては、運用コストの肥大化は利益率に直接跳ね返ります。また、人員入れ替わりの激しさは、人手依存の棚卸し運用の持続性を制約します。

なぜ今期の重点課題か：統制強化と運用負荷抑制を同時に成立させない限り、どちらか一方を犠牲にする構造から抜け出せない点にあります。統制を緩めれば事業継続と信頼が毀損し、運用を拡張すれば利益率が毀損します。

比較軸としての位置づけ：「運用コストと統制品質を両立できるか」という財務・経営管理の軸で評価される論点であり、単独のIT投資ではなく経営インフラの整備として判断されます。

以上3つの経営課題は、いずれも現場の業務課題として日常的に現れています。次章では、これらが現場ではどのような業務課題として具体的に顕在化しているかを整理します。

第4章　経営課題を現場レベルで見ると

本章の目的は、第3章で整理した経営課題が、アルファリテールの現場ではどのような業務課題として日常的に現れているかを示すことです。症状の列挙ではなく、「なぜ現場の工夫で解消しにくいか」という構造要因と、「放置した場合に経営課題のどこに跳ね返るか」という放置リスクを併せて整理し、経営が判断できる論点として組み替えます。

4-1. 店舗・本社・物流・ECをまたぐアクセス経路の統制不足

紐づく経営課題：事業継続性の確保／顧客信頼と説明責任の維持

アルファリテールでは、店舗・本社・物流・ECに加え、多数の外部委託先がシステムに接続する構造となっており、アクセス経路が部門・拠点ごとに分散して広がっています。現場では「どの経路から誰がどのアプリケーションに入れるか」を全体で把握できておらず、業務上の必要に応じて個別に付与された接続経路や例外的な運用が積み重なり、全社統制の枠組みから外れた経路が常態化しています。

構造要因：これらのアクセス経路は、拠点・部門ごとに異なる時期・異なる要件で整備されてきたため、接続方式と運用ルールが当初から分かれています。さらに、境界防御とVPN中心の運用を拡張する形で統制が積み上げられてきたため、クラウド利用と外部連携が増えるほど追随が困難になります。これらは各拠点・部門内では合理的な対応として進化してきた仕組みであり、拠点単位の改善努力では解消できません。全社として「同じ定義で誰がどこから何にアクセスできるか」を把握する状態を作るには、拠点を越えた意思決定が必要になります。

放置リスク：侵害が発生した際に拠点・部門・委託先を横断して被害が広がり、復旧の長期化が業務停止の長期化に直結します。事業継続性の観点では店舗・EC・物流の停止が同時に発生する可能性があり、説明責任の観点では事故時の原因特定と対応説明が困難になります。

4-2. 権限管理の複雑化（特権ID・委託先ID・兼務の増加）

紐づく経営課題：顧客信頼と説明責任の維持／運用品質とコストの両立

アルファリテールでは、店舗運営・物流・ECの現場で兼務・応援・委託先入れ替わりが日常的に発生しており、その都度アクセス権限の付与・変更が必要になります。現場では業務継続を優先して例外的に権限を付与する判断が積み重なり、結果として「誰が・どの権限を・どの根拠で持っているの

か」を明確に説明できない状態が広がっています。特権IDが共有運用されているケースもあり、業務遂行上の必要性は理解されつつも、監査や事故対応の観点では追跡可能性が確保されていません。

構造要因：IDライフサイクル（付与・変更・停止）の運用が部門ごとに分断されており、棚卸しも人手依存で定期化しにくい構造があります。例外的に付与した権限の回収プロセスが組織横断で標準化されていないため、業務終了後の権限が残存しやすくなります。これらは各部門内では業務都合に応じた最適化として進化してきた運用であり、部門単位の改善努力では解消できません。全社としてIDライフサイクルを標準化するには、部門を越えた運用設計と統制基盤の統合が必要になります。

放置リスク：内部不正や誤操作のリスクが高まるだけでなく、監査対応において「誰がなぜアクセスできたか」を説明できない状態が恒常化します。顧客信頼の観点では、データへのアクセス説明責任を果たせない状態が成長施策の制約となり、運用品質の観点では棚卸しと例外処理の工数が継続的に増大します。

4-3. 端末管理のばらつき（店舗POS・物流ハンディ・本社PC・BYODの混在）

紐づく経営課題：事業継続性の確保／運用品質とコストの両立

アルファリテールで利用される端末は、店舗POS、物流ハンディ、本社PC、委託先端末、BYODなど用途が幅広く、OSや管理方法・更新ルールが統一されていません。現場では端末種別や設置環境の制約により、適切な管理水準が端末ごとに異なる状態が常態化しており、特に店舗端末は業務継続を優先して更新が後回しになりがちです。結果として、パッチ適用状況や端末状態（暗号化、セキュリティ設定、マルウェア対策）に拠点間・端末種別間でばらつきが生じています。

構造要因：端末調達と運用が拠点単位で最適化されてきた経緯があり、ライフサイクル管理が全社標準として確立していません。店舗業務の都合や物流現場の稼働制約により、全社一律の更新ルールを適用しにくい現実もあります。これらは各拠点・現場では業務継続を優先した合理的な判断として進化してきた運用であり、拠点単位の改善努力では統一できません。全社として端末状態の最小基準を揃えるには、拠点を越えた運用設計と適用範囲の合意が必要になります。

放置リスク：攻撃の入口になりやすい端末が残存し続け、端末起点の侵害が拠点を跨いで横展開するリスクが高まります。事業継続性の観点では店舗業務の停止と復旧負荷増大に直結し、運用品質の観点では端末更新・例外処理・事故対応の工数が継続的に発生します。

4-4. クラウド利用・SaaS増加に対する可視化と制御の不足

紐づく経営課題：顧客信頼と説明責任の維持／運用品質とコストの両立

アルファリテールでは、EC基盤・マーケティング・顧客分析・店舗運営などの領域で、業務スピードの要請に応えるため、部門ごとにクラウドサービスやSaaSの導入が進んでいます。現場では業務目的に応じた最適なサービスを選定・導入してきた一方で、全社視点ではどの部門がどのサービスを利用し、どのデータを扱っているかの全容が把握しにくい状態になっています。意図しない公開設定や不適切な権限付与が検知されにくく、事故が起きても原因特定に時間を要する構造です。

構造要因：導入主体が部門分散しているため、アクセス制御・権限設定・ログ取得の方式がサービスごとに分断されており、全社横断での棚卸しが回らない状態です。サービス追加のスピードに対し、設定監査・権限監査・ログ統合の運用整備が後追いになります。これらは各部門内では業務効率を優先した合理的な選択として進化してきた仕組みであり、部門単位の改善努力では統合できません。全社として「誰が何を設定変更できるか」「リスクの高い設定が放置されていないか」を把握する状態を作るには、部門を越えた制御面の統合が必要になります。

放置リスク：顧客データを扱うSaaSでの事故が顧客信頼の毀損に直結し、監査・規制対応の観点でも説明責任を果たせない状態が継続します。運用品質の観点では、サービスごとの個別対応が続く限り、統制コストが部門数・サービス数に比例して増大します。

4-5. 外部委託先・パートナー連携に伴うサプライチェーンリスク

紐づく経営課題：事業継続性の確保／顧客信頼と説明責任の維持

アルファリテールは、物流・コールセンター・運用保守・販促・決済など多数の外部委託先と常時接続しており、業務遂行上、委託先からの自社システムへのアクセスが日常的に発生しています。委託先側の運用変更や担当者入れ替わり、新規委託先の追加が継続的に発生する一方で、自社側のアクセス権限や接続方式の見直しが追随できず、委託先のセキュリティ状態を継続的に把握する仕組みも整っていません。委託先起点の事故が連鎖するリスクが高まっています。

構造要因：委託先ごとに接続要件・運用ルール・セキュリティ水準が異なり、契約・運用・IT部門が分断されているため、責任分界が曖昧なまま統制が進みにくい構造があります。委託先の入れ替わりや運用変更に対する追随プロセスが標準化されていないことも要因です。これらは個々の委託先との関係性の中では合理的に進化してきた運用であり、委託先単位の管理強化では解消できません。全社として「委託先ごとの権限と接続条件」を一貫して管理するには、契約・運用・技術を横断した責任

分界整理と統制基盤の整備が必要になります。

放置リスク：委託先起点の事故が自社の業務停止や顧客影響に直結します。事業継続性の観点では物流・供給網の停止が欠品やリードタイム悪化として顕在化し、説明責任の観点では委託先管理の透明性が問われる場面で十分な説明ができない状態となります。

以上の5つの業務課題は、いずれもアクセス・権限・端末・クラウド・委託先という統制対象の異なる側面から生じており、個別の対症療法では例外運用が増殖するだけで根本解決に至りにくい構造を持っています。次章では、これらの業務課題に対して、ゼロトラストDXソリューションの導入によって何がどう変わるのかを、状態変化として整理します。

第5章　ソリューションによる業務課題への対応

5-1. 本提案の対象範囲

本章で扱うのは、第4章で整理した5つの業務課題に対して、ゼロトラストDXソリューションが対応できる範囲です。アクセス統制、権限管理、端末管理、クラウド・SaaS利用統制、外部委託先接続の領域について、「統制の前提を同じ定義で揃え、運用として回り、事故時に説明できる」状態への変化に焦点を当てて整理します。

本提案の範囲外とする事項も明示します。具体的には、全社・全拠点・全端末・全SaaSを一律に対象化した要件確定、全社ネットワークの再設計、監査手順や規程類の最終確定、個別ベンダー選定や契約条件の確定は、本章の対象外とします。これらはSI営業と対象企業との対話の中で段階的に詰める事項です。

5-2. 各業務課題への対応内容

以下では状態変化として整理します。機能の詳細については別途の製品資料を参照してください。ここでは「現状の状態」と「ゼロトラストDXソリューション導入により実現される状態」を対比し、何がどう変わるかを示します。

状態変化1： アクセス経路が「説明可能な統制下」に置かれる状態へ

現状の状態：店舗・本社・物流・ECをまたぐアクセス経路が分散し、接続方式が拠点・部門ごとに乱立しています。「どこから誰が入れるか」を全体で把握できず、例外運用が積み重なっています。

ゼロトラストDXソリューション導入により、ZTNA（ゼロトラストネットワークアクセス）によるアプリケーション単位のアクセス制御、SSOによる統合認証、ユーザー・端末・アプリケーションの状態に基づく動的検証が、統一された制御面の上で運用されます。

実現される状態：VPN経由での広範な権限付与ではなく、アプリケーション単位で必要最小限の権限のみを付与する構造が成立します。重点領域において、誰がどこからどのアプリケーションにアクセスしたかが同じ定義で把握でき、例外運用の管理が追跡可能な形で回るようになります。

状態変化2： 権限が「付与根拠とライフサイクル」で管理される状態へ

現状の状態：兼務・応援・委託先入れ替わりに伴う例外権限が残存し、特権IDの共有運用が続いています。IDライフサイクルの運用が部門ごとに分断され、棚卸しが人手依存になっています。

ゼロトラストDXソリューション導入により、特権ID管理（PAM）による管理者アカウント制御、多要素認証（MFA）による本人性の担保、ユーザー属性と利用状況に応じた動的なアクセス制御が、全社横断のID基盤上で運用されます。

実現される状態：特権IDと委託先IDを含め、誰がどの権限をどの根拠で保持しているかが説明可能な状態になります。IDの付与・変更・停止のライフサイクルが運用として回り、棚卸しが人手依存から脱却する方向に進みます。

状態変化3： 端末が「最小基準」で揃い、例外が追跡可能な状態へ

現状の状態：店舗POS・物流ハンディ・本社PC・BYODの管理方法が分断され、パッチ適用や端末状態が統一されていません。店舗業務の都合で更新が後回しになる端末が残存しています。

ゼロトラストDXソリューション導入により、端末のセキュリティ状態の常時監視、不正挙動検知によるアクセス遮断、EDR/XDRとの連携による脅威対策が、端末種別を跨いで統合的に運用されます。

実現される状態：重点範囲の端末において、暗号化・更新・管理状態の最小基準が揃い、基準を満たさない端末からのアクセスが制御される状態が成立します。例外として運用せざるを得ない端末についても、例外として追跡・管理できる状態に置かれます。

状態変化4： クラウド・SaaS利用が「設定と権限の棚卸し」で回る状態へ

現状の状態：部門ごとに導入されたSaaSとクラウドで、アクセス制御・ログ・設定が分断され、不適切な公開設定や権限付与が検知されにくい状態です。

ゼロトラストDXソリューション導入により、CASBによるSaaSアプリの可視化と制御、CSPMによるクラウド設定監査と脆弱性検知、CWPPによるワークロード保護が、統合的な制御面の上で運用されます。

実現される状態：重点SaaSとクラウドで、誰が何を設定変更できるかが可視化され、リスクの高い設定が検知される状態になります。サービスごとの個別対応から、全社横断の棚卸しが回る運用への移行が進みます。

状態変化5： 外部委託先接続が「統制と運用の分離」で管理される状態へ

現状の状態：多数の外部委託先との接続点が増え、委託先側の運用変更に対してアクセス権限・端末・接続方式の追随が難しい状態です。契約・運用・ITが分断され、責任分界が曖昧です。

ゼロトラストDXソリューション導入により、接続場所・利用端末に応じたポリシー切替、リスクスコアに基づくアクセス制御、ポリシー変更の自動化と一元管理が、委託先接続に対しても統一的に適用されます。

実現される状態：主要委託先との接続について、委託先ごとの権限と接続条件が明示的に定義され、委託先側の変更にも運用として追随できる状態が整います。契約・運用・技術の責任分界整理の前提となる可視化が進みます。

以上の状態変化は、いずれも「統制の前提が同じ定義で揃う」「運用として回る」「事故時に説明できる」という共通の方向性に収束します。次章では、これらの状態変化が第3章の経営課題にどう寄与するかを整理します。

第6章　経営課題への効果

6-1. 各経営課題への寄与

本章では、第5章で示した状態変化が、第3章で整理した3つの経営課題それぞれにどう寄与しうるかを整理します。ここでは効果を断定せず、前提条件を明示したうえで「方向性」として記述します。外部環境（攻撃動向、委託先の入れ替わり、クラウド利用の拡大、規制動向）による効果のばらつきを織り込んで評価する必要があります。

経営課題1：事業継続性の確保への寄与

アクセス経路の統制、端末状態の最小基準化、委託先接続の可視化が進むと、侵害発生時の横展開が抑えられる方向に働きます。重点領域において、事故の影響範囲を局所化できる状態が整えば、業務停止リスクと復旧影響の低減が期待できます。また、初動対応の手順が「何が起きたか」を追跡できる前提の上に成立するため、復旧時間の短縮にもつながる可能性があります。ただし、実際の効果は、対象範囲の広がりと例外運用の管理成熟度に依存します。

経営課題2：顧客信頼と説明責任の維持への寄与

アクセス経路の統制、権限管理とクラウド利用統制が整い、アクセスとログの可視化が進むと、「誰がどのデータにどの条件でアクセスしたか」を説明できる状態に近づきます。顧客データを扱う領域で説明可能性が担保されるほど、個人情報保護法対応・監査対応・取引先対応における説明負荷が下がることが期待できます。委託先接続についても、権限と接続条件が明示的に定義されることで、委託先経由のアクセスに関する説明責任が対応範囲に含まれます。また、パーソナライズマーケティングやオムニチャネル連携といった成長施策の継続に必要な信頼基盤の強化にもつながる可能性があります。効果の実現は、ログ保全の範囲と定義、および監査観点との整合に依存します。

経営課題3：運用品質とコストの両立への寄与

IDライフサイクル運用の標準化、端末管理の最小基準化、クラウド設定の棚卸し運用、ポリシー適用の自動化が進むと、拠点・人・委託先ごとの個別対応が減る方向に働きます。統制を強化しながらも運用負荷の肥大化を抑える構造に移行できれば、IT管理部門の人手依存が軽減され、人員入れ替わ

りへの耐性が高まることが期待できます。ただし、効果の実現は、標準化の範囲設定と例外運用の管理方針に依存するため、重点領域からの段階的な整備が前提となります。

6-2. この提案を経営アジェンダとして位置づける理由

ここまで整理してきた業務課題は、いずれも「現場の運用工夫で一時的にはしのげる」性質のものです。しかし、オムニチャネル運営の拡張、顧客データ活用の深化、外部委託先連携の拡大、クラウド利用の進展という変化が同時進行する中で、現場対応の積み上げで対処し続ける運用は、事業継続・顧客信頼・運用品質の3軸を同時に満たすことが構造的に難しくなっています。

業務課題を放置した場合、経営への跳ね返りは次のように現れます。アクセス・権限・端末の統制不備は、店舗・物流・ECの業務停止として顕在化し、売上機会損失と取引先対応コストに直結します。クラウド利用と委託先連携の統制不備は、顧客データ事故時の説明責任を果たせない状態として顕在化し、顧客信頼の毀損と規制対応コストの増大に跳ね返ります。運用の人手依存は、IT管理部門の負荷肥大化として利益率を継続的に圧迫します。これらは独立した問題ではなく、共通する構造要因（拠点・部門・委託先をまたいだ統制の分断と運用の属人化）から生じているため、個別対処では根本的な解消に至りません。

したがって、ゼロトラストDXソリューションの導入は、特定業務の効率化ではなく、事業継続・顧客信頼・運用品質を同時に満たすための経営インフラへの投資として位置づけられます。問うべきは「導入するかどうか」ではなく、「経営課題をいつ・どのような段取りで前進させるか」です。これに対して、他の投資案件と比較可能な形で検討テーブルに載せることが、次の論点になります。

APPENDIX

APPENDIX

業務課題と紐づく経営課題の整理

対象業界：小売・EC業界（総合小売業）
対象製品：ゼロトラストDXソリューション
想定企業：アルファリテール株式会社（仮名）

---

1. 店舗・本社・物流・ECをまたぐアクセス経路の増加と統制不足

業務課題

店舗端末、本社システム、物流システム、EC基盤、外部委託先を跨いでアクセス経路が広がり、「どこから誰が入れるか」を全体で把握できない状態です。

- 店舗端末、本社システム、物流システム、EC基盤、外部委託先など、アクセス経路が多岐にわたり、全体で把握できていない
- 拠点・部門ごとに接続方式や運用ルールが分かれ、例外運用が積み重なって統制が形骸化している
- 境界防御やVPN中心の構成のままクラウド利用が増え、統制設計が追いつかなくなっている

経営課題

- 経営管理：オムニチャネル運営を支える基盤の統制が崩れると、事業停止リスクと全社ガバナンスに直結するため
- 店舗運営：店舗オペレーションの継続性が、アクセス経路の不備による事故で遮断される恐れがあるため
- EC・デジタルチャネル：オムニチャネル連携はアクセス統制の成立を前提とするため、統制不備はデジタルチャネル戦略の土台を揺るがすため

---

2. 権限管理の複雑化（特権ID・委託先ID・兼務の増加）

業務課題

兼務・応援・委託先入れ替わりに伴う例外権限が残存し、特権IDの共有運用やIDライフサイクルの分断が継続しています。

- 例外的に付与した権限が業務終了後に回収されず残存している
- 特権IDが共有運用され、誰がいつ何のために使ったかを追跡できていない
- IDライフサイクル（付与・変更・停止）の運用が部門ごとに分断され、棚卸しが人手依存で定期化できていない

経営課題

- 経営管理：ガバナンス・内部統制の観点から、アクセス権限の説明責任を果たせない状態は監査・規制対応上の重大な弱点になるため
- 人材管理：異動・離職・委託先入れ替わりへの対応が人手依存となり、IT管理部門の負荷と人材確保の課題に跳ね返るため
- 財務：内部不正や誤操作による損失リスクが、低利益率構造の小売事業に追加的な損失を与える恐れがあるため

---

3. 端末管理のばらつき（店舗POS・物流ハンディ・本社PC・BYODの混在）

業務課題

店舗POS、物流ハンディ、本社PC、委託先端末、BYODなど用途が幅広く、OSや管理方法・更新ルールが統一されていません。

- 端末種別ごとにOS・セキュリティ設定・パッチ適用状況が統一されていない
- 端末調達と運用が拠点単位で最適化されており、ライフサイクル管理が不徹底
- 店舗業務の都合で更新が後回しになり、攻撃の入口になりやすい端末が残存している

経営課題

- 店舗運営：端末起点の事故が現場オペレーションを直接停止させ、業務の標準化・作業負担軽減の方向性と矛盾するため
- 経営管理：システム障害による業務中断が、事業継続の観点で重大な経営リスクとなるため
- 人材管理：セキュリティ事故対応の負荷が現場スタッフと管理部門に集中し、教育負担・離職リスクを高めるため

---

4. クラウド利用・SaaS増加に対する可視化と制御の不足

業務課題

EC基盤・マーケティング・顧客分析・店舗運営などで部門ごとにクラウド・SaaS導入が進み、アクセス制御・ログ・設定が分断されています。

- 部門ごとにSaaS導入が進み、アクセス制御・権限設定・ログ取得の方式が分断されている
- 意図しない公開設定や不適切な権限付与が検知されにくく、事故の入口になりやすい
- サービスごとの棚卸しが回らず、事故時の原因特定と説明責任を果たしにくい状態

経営課題

- 販売促進・マーケティング：顧客データ活用を前提とした施策は、データ保護と監査対応の成立なしには継続困難なため
- EC・デジタルチャネル：ECサイトと顧客データを扱う領域のセキュリティ担保は、オムニチャネル戦略の前提条件となるため
- 経営管理：個人情報保護法・委託先管理・内部統制の観点から、クラウド利用統制はガバナンス論点に直結するため

---

5. 外部委託先・パートナー連携に伴うサプライチェーンリスク

業務課題

物流・コールセンター・運用保守・販促・決済など多数の委託先との接続点が増え、委託先起点の侵害が連鎖するリスクが高まっています。

- 委託先が増えるほど接続点も増え、侵害の連鎖リスクが上がる
- 委託先側の運用変更や担当入れ替わりに対し、アクセス権限・端末・接続方式の追随ができていない
- 契約・運用・ITが分断され、委託先のセキュリティ状態を継続的に把握する仕組みが弱い

経営課題

- 物流・供給：委託先起点の事故が物流・供給網の停止に直結し、リードタイム短縮・欠品防止の基盤を揺るがすため
- 経営管理：取引先ガバナンスの透明性確保は、監査・規制対応上の重要論点となるため
- 財務：委託先起点のインシデントによる仕入・供給混乱は、原価・仕入コスト増大として業績に跳ね返るため

---

6. セキュリティポリシー運用の複雑さと標準化の遅れ

業務課題

店舗・本社・在宅勤務・委託先など多様な働き方でポリシー管理が煩雑化し、手動運用で抜け漏れが発生しやすい状態です。

- 多様な働き方でポリシー管理が煩雑化し、手動運用で抜け漏れが発生しやすい
- 拠点・部門ごとに運用差があり、標準化を進めると現場反発が起きやすい構造
- 例外処理が人手対応となり、IT管理部門の運用負荷が継続的に増大している

経営課題

- 人材管理：IT管理部門の運用負荷肥大化が人材確保・定着の障害となるため
- 店舗運営：ポリシー運用の煩雑さが店舗業務の標準化・効率化の足かせになるため
- 経営管理：オムニチャネル戦略と働き方改革の土台としてセキュリティ統制の一元化が不可欠なため

※ 本論点「6. セキュリティポリシー運用の複雑さと標準化の遅れ」は課題1～5に共通する構造要因（拠点・部門・委託先ごとの運用差、手動運用の抜け漏れ、例外処理の増殖）として各業務課題に内包されています。そのため、本文第4章では独立した業務課題としては立てず、各業務課題の構造要因の中に織り込んで扱っています。

BRANDING

ALPHA BRANDING Corp.