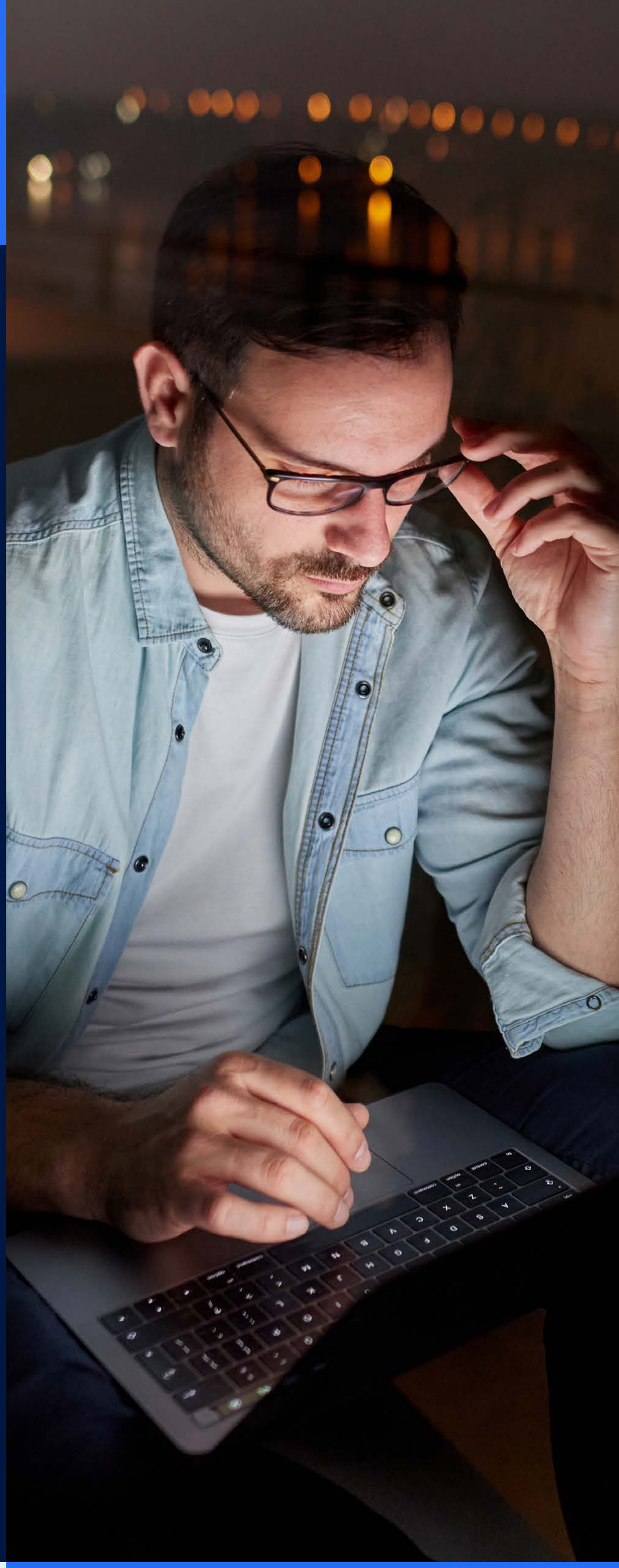
データセキュリティプログラムの構築

MICHAEL SCHNEIDER
Zscaler、ディレクター兼シニア
プリンシパル スペシャリスト アーキテクト



ホワイトペーパー

目次

はじめに

デジタル データの急激な増加は、組織に新たな機会をもたらす一方、重大な課題も突きつけています。個人情報、財務情報、ビジネス情報などの重要なデータを扱う立場として、データの紛失や不正アクセス、悪用を防ぐための包括的なデータ保護対策を実施することは組織の重要な責務です。

このデータ保護プログラムは、組織全体の情報資産を管理するための基盤となるフレームワークです。一般データ保護規則(GDPR)をはじめ、州および連邦のプライバシー法や関連する業界標準に準拠して設計されており、データの機密性、完全性、可用性を確保するための技術的、物理的、管理的な対策を網羅しています。

主な要素は以下のとおりです。

- **データの分類とインベントリー化：**機密性と規制上の義務に基づいて、データを特定、分類、追跡します。
- **アクセス制御：**機密情報へのアクセスや変更を許可された担当者のみに制限します。
- **リスク管理：**定期的なセキュリティ レビューとインシデント対応計画を通じて、脅威を評価し、軽減します。
- **トレーニングと意識向上：**データの取り扱いやセキュリティに関する責任とベスト プラクティスについて、従業員を教育します。
- **インシデント対応：**データ侵害やその他のセキュリティ イベントを迅速に検知し、対応および復旧を行うための体制を構築します。
- **継続的な改善：**進化するリスクとテクノロジーに対応するために、ポリシーを定期的に確認し、更新します。

このような構造化されたアプローチを採用することで、法的な要件を満たすだけでなく、顧客、従業員、ビジネス パートナーのプライバシーを守り、信頼を築く姿勢を示すことができます。

本書は、データ保護プログラムの各側面について説明し、その効果的な実装と継続的な成功を確保するための役割と責任の概要を紹介します。また、多くの組織が従う一般的な構造の概要も示していますが、これは組織の規模、成熟度、規制環境に合わせて調整できます。

成功の鍵となる要素

データ セキュリティ プログラムの有効性と持続可能性を確保するには、単純な技術導入だけでなく、戦略的な視点と組織全体の連携も求められます。データ セキュリティ施策を成功に導き、長期的な成果を達成するためには、以下の重要な要素が不可欠です。

- **テクノロジーではなく、ビジネス目標から開始する**
- **部門横断的なサポートを早期に獲得する**
- **パイロット導入、監視、調整を行った後に、本格的に実施する**
- **保護と使いやすさを両立させる**
- **1回限りのプロジェクトではなく、継続的なプログラムとして扱う**

最初に重要なのは、プログラムをテクノロジーだけに依存するのではなく、ビジネス目標に基づいて設計することです。セキュリティ対策を組織の目標に合わせれば、データ保護が重要な業務や成長を妨げることなく、これを支援する役割を果たすようになります。また、早い段階で各部門の関係者の支持と協力を得ることで、統一された基盤が築かれ、部門間の連携が強化されます。このアプローチは、プロジェクトの推進力を高め、責任を共有する体制を作るうえで欠かせない要素となります。

実施においては、ソリューションのパイロット導入、監視、改善を行い、その後組織全体にポリシーを施行するという体系的な手法を採用します。このプロセスにより、課題を効果的に特定し、実践を最適化して最大限の効果を得ることができます。同時に、強力なセキュリティ対策と使いやすいプロセスも不可欠です。この2つを両立させることで、生産性を維持したまま機密情報を保護できます。

最後に、データ セキュリティを1回限りのプロジェクトではなく継続的なプログラムとして捉えることで、変化するリスク、ビジネスの優先順位、規制要件に継続的に適応できるようになります。これらの成功の要素を戦略に組み込むことで、回復性に優れた効果的かつ永続的なデータ セキュリティ プログラムの基盤を構築できます。

プログラムのフェーズ

目標と範囲の明確化

データ セキュリティ プログラムの主な目的を明確にします。不正アクセスの防止、データの完全性の維持、コンプライアンスの確保など、セキュリティ対策を通じて達成したい目標を明確にすることで、成功を測るベンチマークを設定し、適切な制御や対策を選択できるようになります。

次に、プログラムの適用範囲を設定し、対象とするデータの種類、システム、プロセス、事業部門を定義します。境界を明確にすることで、リソースを効果的に配分し、重要な資産を見落とすことなく、関連するすべての領域にセキュリティ対策を適用できるようになります。

目標と範囲の明確化は、データ セキュリティ プログラムの基盤を構築すると同時に、情報保護と組織全体の目標を支えるための戦略的なフレームワークを提供します。

タスク

- **ビジネス目標：**組織が達成したいことを明確にします(例：知的財産の保護、偶発的な漏洩の防止、GDPR/PCI/HIPAAへの準拠)。
- **適用範囲：**メール、エンドポイント、クラウド アプリのどれから始めるか、あるいはすべてを同時に進めるかを決定します。一般的には、プロキシ、メール、エンドポイント、クラウドといった単一のポイントから小規模にDLP導入を開始し、段階的に範囲を拡大していくアプローチが主流です。
- **リスク許容度：**経営幹部と協力し、データ移動の許容度と認められる例外を定義します。

ガバナンスおよび関係者との連携の構築

効果的なデータ セキュリティはテクノロジーだけでは実現しません。強力なガバナンス構造とすべての関係者間の積極的な連携が求められます。明確なガバナンス フレームワークを確立することで、役割、責任、意思決定プロセスを定義し、組織全体でセキュリティ ポリシーを一貫して適用できるようになります。

データ セキュリティ プログラムを効果的に監視するには、運営委員会の設置、責任者の指名、報告やエスカレーション経路の整備などの強力なガバナンス メカニズムが欠かせません。また、事業部門、技術部門、経営幹部、外部パートナーがプログラムの目的に沿って行動し、情報資産の保護における各自の役割を理解するために、関係者の継続的な関与も重要です。

責任の共有と透明性を重視する文化を育成することで、説明責任が強化され、情報に基づいた的確な意思決定が可能になり、データ セキュリティ対策の持続的な成功が促進されます。

タスク

- **運営委員会:** IT/セキュリティ、法務、コンプライアンス、人事、事業部門、データ所有者を含めて構成します。

- **役割と責任:**
  - **CISO/(情報)セキュリティ:** 全体を統括する責任者
  - **コンプライアンス/法務:** 規制要件への対応
  - **事業部門:** 重要なデータやワークフローの特定
  - **IT:** 統合とポリシー施行の実施

- **ポリシーと基準:** 自社のコンテキストでの「機密情報」の意味を定義します(PII、PHI、企業秘密、財務情報、ソース コードなど)。この定義をデータ分類ポリシーに明記し、全従業員が利用できる状態にしておくことで、データ セキュリティの意識を高め、曖昧さを排除できます。明確なガイドラインは、従業員が正しい意思決定を行う助けとなり、曖昧なポリシーやガイドラインによって責任が不明確になることを防止します。

データの検出と分類

効果的なデータ セキュリティ プログラムは、情報の全体像を明確に理解することから始まります。データの検出と分類は基本的な活動であり、組織が情報資産を機密性や価値に基づいて特定、分類、優先順位付けすることを可能にします。

組織全体のデータを体系的に検出することで、データがデータベース、ファイル システム、クラウド環境、従業員のデバイスのどこに保存されていても、どのようなデータが存在し、どこに保存され、業務のなかでどのように流れているかを可視化できます。

特定されたデータは、事前定義された重要度とリスク レベル(公開、内部、機密、規制対象など)に基づいて分類されます。この適切な分類により、必要なセキュリティ制御を適用すると同時に、コンプライアンス要件を満たし、機密情報を高いレベルで保護することが可能になります。

強力なデータの検出と分類の方法を確立することで、対象を絞ったリスク管理の基盤を築き、規制順守を強化し、データ セキュリティ プログラムの全体的な有効性をサポートできます。

タスク

- **データ マッピング：**機密情報の所在(エンドポイント、ファイル共有、クラウド ワークロード、SaaS、メール)を特定します。

- **分類：**前の手順で定義したポリシーと標準に従い、ラベル(公開、内部、機密、制限付き)を適用するか、データを特定の分類に移動します。

- **ツール：**Zscaler Endpoint DLPデータ スキャン、データ検出ダッシュボード、CASBスキャンなどの既存の検出ツールを活用し、あらかじめ構築されたDLP辞書/テンプレートを使用します。AIベースの分類は、データの特定を支援する優れたツールです。検出は必ずしも完全である必要はなく、特定の場所に機密情報が存在することを示す証拠があれば十分です。

- **優先順位付け：**まずは最も機密性が高く、リスクの高いデータ カテゴリーに焦点を当てます。良い例としては、PIIや財務、医療、法務情報などが挙げられます。

ポリシーの設計

データ セキュリティ プログラムを成功させるには、明確かつ包括的なポリシーを策定することが重要です。適切に設計されたポリシーは、従業員が取るべき行動やシステム要件を具体的に示し、組織全体で機密情報を一貫して保護するための指針と実践的なルールを提供します。

データの取り扱い、アクセス制御、インシデント対応、トレーニング、コンプライアンスなど、データ セキュリティの重要な側面すべてに対応するポリシーを策定する際には、慎重なアプローチが求められます。ポリシー設計の過程では、適用される法律や業界標準、組織の目標から導き出される要件を統合し、それらを実行可能かつ測定可能な指針として具体化する必要があります。

ポリシーの策定とレビューに主な関係者を関与させることで、ビジネス ニーズとの整合性を高め、責任を共有する意識を醸成できます。強力なデータ セキュリティ ポリシーは、不正行為に対する抑止力となるだけでなく、リスクに対応し、法律と倫理的義務を遂行するための重要なフレームワークとしても機能します。

効果的なポリシー設計を通じて、組織のミッションをサポートし、資産を保護し、顧客、パートナー、従業員との信頼を構築する安全な環境を構築します。

タスク

- **ユース ケース:**監視対象とするシナリオを定義します(例:組織外へのPIIの送信、GitHubへのソース コードのアップロード、USBへの大量のデータのコピー)。

- **粒度:**業務の中断を回避するために、監視のみのポリシー(ブロックなし)から始めるか、ユーザーがアクティビティーを続行するかどうかを選択できるオプションを実装します。これにより、ユーザーを暗黙のうちに教育することにもなり、重要なステップとなります。

- **例外処理:**オーバーライドと承認のための明確なプロセスを定義します。

- **法律/プライバシーのレビュー:**現地の労働法に準拠していることを確認します(特に従業員の監視に関するEUの規定)。

テクノロジーの選定と統合

データ セキュリティ プログラムの成功は、整備されたポリシーや手順、そしてテクノロジーの戦略的な使用によって支えられています。常に進化する脅威から機密情報を保護するには、適切な技術的ソリューションの選定と統合が重要です。

組織に最適なテクノロジーを見つけるには、既存のインフラを評価し、データの機密性とリスクに基づいて要件を決定し、セキュリティ目標と業務の両方に適合するソリューションを選択する必要があります。

統合も同様に重要です。導入するツールやシステムは、既存のワークフローとシームレスに連携し、効率性を確保するとともに、業務の中断を最小限に抑える必要があります。相互運用性を強化し、主要なセキュリティ制御を自動化することで、迅速なインシデント対応と確実なデータ保護が可能となります。

タスク

- **要件の収集:**既存のスタック(メール ゲートウェイ、プロキシ、エンドポイント、M365、GCP/Azure/AWS、CASB、SIEM/SOAR)との統合または拡張を行います。

- **評価:**エンドポイント、ネットワーク、クラウド ネイティブ、ハイブリッドのDLP保護から選択します。Zscalerはこれらすべての場面でデータを保護できます。

- **統合:**Zscaler Workflow Automationを活用し、SIEMによるログ記録やチケット管理システムの統合、インシデント対応の自動化を計画します。

パイロット導入と段階的な展開

パイロット導入と段階的な展開を組み合わせたアプローチにより、新しいセキュリティ対策を徐々に導入できます。まず特定の領域やグループを対象に始め、最終的には組織全体へと展開することで、データ セキュリティ プログラムの効果を高めつつ、業務への影響を最小限に抑えられます。

パイロット導入から始めて、実際の環境でプロセス、テクノロジー、ポリシーをテストし、フィードバックを収集し、課題を特定して改善を行います。初期の結果を注意深く監視し、早期導入ユーザーから学ぶことで、戦略を洗練させ、予期せぬ問題に対処し、関係者の信頼を構築できます。

次に、段階的な展開を開始してデータ セキュリティ プログラムを計画的に拡張し、各事業部門が移行期間中に適切なサポートとトレーニングを受けられるようにします。この慎重なアプローチにより、リスクの軽減、ユーザーの受容性の向上、日常業務の維持、そして全体的なセキュリティ態勢の強化が可能になります。

タスク

- **パイロット グループ:** 代表的なデータ フローを持つ、管理された小規模の事業部門を選択します。
- **監視のみのモード:** データを収集し、ポリシーを調整し、誤検知を最小限に抑えます。
- **フィードバック ループ:** エンド ユーザーと協力し、実際のワークフローを理解します。
- **段階的な拡張:** 追加の部門やデータの種類、チャネルを段階的に展開します。

インシデント対応とワークフロー

セキュリティ インシデントを管理するための堅牢なアプローチがなければ、データ セキュリティ プログラムは完成しません。迅速かつ効果的なインシデント対応は、データ侵害、サイバー攻撃、組織の資産や関係者の信頼を脅かす可能性のあるその他のセキュリティ イベントの影響を最小限に抑えるために不可欠です。

セキュリティ インシデントの検出、報告、分析、解決のための明確なワークフローと手順を策定することが重要です。定義された役割、エスカレーション経路、コミュニケーション チャネルを確立することで、技術部門、法務部門、事業部門間のスムーズな調整と迅速な対応を実現できます。包括的なインシデント対応計画は、定められた期間内に侵害を報告するという規制要件の順守にも役立ちます。

定期的なテスト、トレーニング、インシデント後のレビューを通じて、インシデント対応プロセスを継続的に改善することで、準備の強化、復旧時間の短縮、将来のインシデント発生防止が可能になります。構造化されたワークフローをデータ セキュリティ プログラムに組み込むことで、組織の回復力を強化し、機密情報の保護と事業継続性の維持への取り組みを示すことができます。

タスク

- **トリアージ プロセス：**アラートを調査する担当者と対応のスピードを定義します。
- **エスカレーション経路：**法務、人事、コンプライアンス部門が関与すべきタイミングを定義します。
- **ユーザー教育：**アクションを単にブロックするのではなく、そのリスクをユーザーに通知し、教育します。
- **自動化：**可能な場合は、SOARと統合して反復的なタスクを効率化します。

ユーザーの意識向上とトレーニング

組織のデータ保護の最前線に立つのは、従業員自身です。そのため、効果的なユーザーの意識向上とトレーニングは、データ セキュリティ プログラムの成功に欠かせません。この取り組みによって、従業員は情報資産を保護するための役割と責任をより深く理解できるようになります。

セキュリティ意識の高い文化を構築するには、継続的な教育と関与が必要です。カスタマイズされたトレーニング セッション、定期的なコミュニケーション、実用的なリソースを提供することで、ユーザーはフィッシング、ソーシャル エンジニアリング、データの不適切な取り扱いなどの潜在的な脅威を正しく認識し、適切に対応するためのベスト プラクティスを習得できます。

一貫したユーザーの意識向上とトレーニングにより、ヒューマン エラーの可能性を低減し、規制要件への準拠をサポートし、全体的なデータ保護戦略を強化できます。その結果、セキュリティが全員の責任となり、組織のデータが適切に保護され続ける環境が実現します。

タスク

- **保護の文化：**DLPを「従業員の監視」ではなく「企業と顧客の保護」として捉えます。
- **マイクロトレーニング：**機密情報を誤って送信しようとした場合に何が起こるかをユーザーに示します。
- **フィードバック チャネル：**従業員が誤検知を報告したり、安全な例外を申請したりできるようにします。

指標と継続的な改善

真に効果的なデータ セキュリティ プログラムは静的なものではなく、新たな脅威とビジネス要件に対応し、規制順守を維持するために継続的に進化します。セキュリティ対策のパフォーマンスを測定し、継続的な改善の文化を育むことは、長期にわたって強力なデータ保護を維持するために不可欠です。

重要な指標を追跡および記録し、セキュリティ制御、ポリシー、プロセスの有効性を評価することが求められます。インシデント対応時間、ユーザー トレーニングの参加率、コンプライアンス監査の結果などの重要業績評価指標は、強みとなる領域と改善が必要な領域を把握するための貴重な洞察を提供します。

継続的に改善を進めるには、定期的なレビューやフィードバック、変化への柔軟な対応が必要です。セキュリティ インシデントから得られた教訓、脅威環境の変化、テクノロジーの進歩はすべてプログラムの更新に役立ちます。測定と改善を行うための構造化されたアプローチを導入すれば、データ セキュリティ対策をより予防的かつ効果的なものにし、組織の戦略目標と一致させることができます。

タスク

- **KPI:**インシデント数、誤検知率、対応時間、ユーザー例外数を指標にします。
- **リスク削減の追跡:**機密情報の移動がどの程度防止されているかを経営陣に示します。
- **ポリシーの改善:**実際のビジネス ワークフローに基づいて継続的に改善します。
- **監査準備:**コンプライアンス監査用のログ、レポート、指標を維持します。

長期的な成熟

強力なデータ セキュリティを実現して維持することは、1回限りのプロジェクトではなく継続的な取り組みです。長期的な成熟こそが、テクノロジー、規制環境、ビジネス目標の変化にかかわらず、機密情報を継続的に保護する最善の方法です。

セキュリティ機能を定期的に評価し、業界標準と比較し、過去の経験から得られた教訓を統合することで、プログラムの有効性を継続的に強化し、徐々に進化する成熟した適応型のセキュリティ態勢を構築できます。

長期的な成熟に重点を置くには、基礎的な制御を維持しながら、高度なテクノロジーへの投資、従業員の関与の促進、セキュリティ戦略と組織全体の目標との整合を進めることが必要です。包括的な計画、戦略的なリソース配分、継続的な改善の取り組みを通じて、データ セキュリティ プログラムが回復力と関連性を維持し、将来の課題にも対応できるようにします。

タスク

- **事後対応**(「データ漏洩の阻止」)から事前対応(「安全なワークフローの設計」)に移行します。
- **ゼロトラスト**やデータ セキュリティ ポスチャー管理(DSPM)と統合します。
- **適用範囲を拡大**し、サプライ チェーン、請負業者、サードパーティーのSaaSまで対象とします。
- **分類**とポリシーの適用をAI/MLを活用して自動化し、手動による調整を削減します。

DLPプログラムのロードマップ(0～18か月)

フェーズ1:基盤構築(0～6か月目)

目標:目標と範囲を定義し、ガバナンス体制を構築し、基盤を整備する。

- **経営層の支援とガバナンス体制の確立**
- **ポリシーのフレームワークの策定**
- **データの検出と分類**
- **ポリシーの設計**
- **テクノロジーの選定と統合**

成果物

- **DLPガバナンス憲章**
- **データ分類標準**
- **ベンダー/ツールの選定に関する決定**

フェーズ2:パイロット導入とテスト(6～9か月目)

目標:テクノロジーを検証し、ポリシーを調整し、誤検知を最小限に抑える。

- **パイロット導入**
- **ポリシーの展開(監視のみ)**
- **インシデント対応とワークフロー**

成果物

- **パイロット導入レポート**
- **初期インシデント対応マニュアル**
- **ポリシー調整ガイド**

フェーズ3:段階的な展開(9〜18か月目)

目標:範囲を拡大し、ポリシーを慎重に施行する。

- **段階的な展開を通じた範囲の拡大**
- **選択的な施行の開始**
- **ユーザーの意識向上とトレーニング**
- **指標と継続的な改善**

成果物

- **全社規模のユーザー トレーニング**
- **経営陣向けの指標ダッシュボード**
- **重要なワークフローにおけるポリシーの施行**

フェーズ4:全社への展開と最適化(13〜18か月目)

目標:幅広い範囲をカバーし、文化に浸透させて、プログラムを最適化する。

- **全面的な展開**
  - » すべての事業部門と地域にDLPを展開します。
  - » 統合を拡張します(SIEM、SOAR、UEBA)。
- **高度なポリシー**
  - » コンテキスト ポリシー(場所ベース、リスク スコアリング、内部脅威インジケーター)を適用します。
  - » 可能な場合はMLを活用して分類を自動化します。
- **インシデント対応の拡張**
  - » トリアージとエスカレーションのためのSOCマニュアルを作成します。
  - » 一般的な修復アクション(隔離や暗号化)を自動化します。
- **長期的な成熟**

成果物

- **組織全体のDLPカバレッジ**
- **自動対応ワークフロー**
- **経営層向けのKPIレポート**

このロードマップを通じて、組織はその場しのぎのモニタリング体制から脱却し、十分に整備されたガバナンス、効果的なポリシーの施行、そして最適化が進んだエンタープライズDLPプログラムを構築できます。加えて、リスク管理やコンプライアンスとの完全な融合を図ることができます。

ロードマップ

フェーズ	月	目標	主要な取り組み	成果物
フェーズ1: 基盤構築	0〜6	目標と範囲を定義し、ガバナンス体制を構築し、基盤を整備する	• 経営層の支援とガバナンス体制の確立 • ポリシーのフレームワークの策定、データの検出と分類 • ポリシーの設計 • テクノロジーの選定と統合	• DLPガバナンス憲章 • データ分類標準 • ベンダー/ツールの選定に関する決定
フェーズ2: パイロット導入とテスト	6〜9	テクノロジーを検証し、ポリシーを調整し、誤検知を最小限に抑える	• パイロット導入 • ポリシーの展開(監視のみ) • インシデント対応とワークフロー	• パイロット導入レポート • 初期インシデント対応マニュアル • ポリシー調整ガイド
フェーズ3: 段階的な展開	9〜18	範囲を拡大し、ポリシーを慎重に施行する	• 段階的な展開を通じた範囲の拡大 • 選択的な施行の開始 • ユーザーの意識向上とトレーニング • 指標と継続的な改善	• 全社規模のユーザートレーニング • 経営陣向けの指標ダッシュボード • 重要なワークフローにおけるポリシーの施行
フェーズ4: 全社への展開と最適化	13〜18	幅広い範囲をカバーし、文化に浸透させて、プログラムを最適化する	• すべての事業部門と地域へのDLPの全面的な展開 • 統合の拡張(SIEM、SOAR、UEBA) • 高度なポリシー(コンテキスト、MLを活用した自動化) • インシデント対応の拡張(SOCマニュアル、自動化) • 長期的な成熟	• 組織全体のDLPカバレッジ • 自動対応ワークフロー • 経営層向けのKPIレポート

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™プラットフォームは、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.com/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.com/jp**

zscaler™

Zero Trust Everywhere