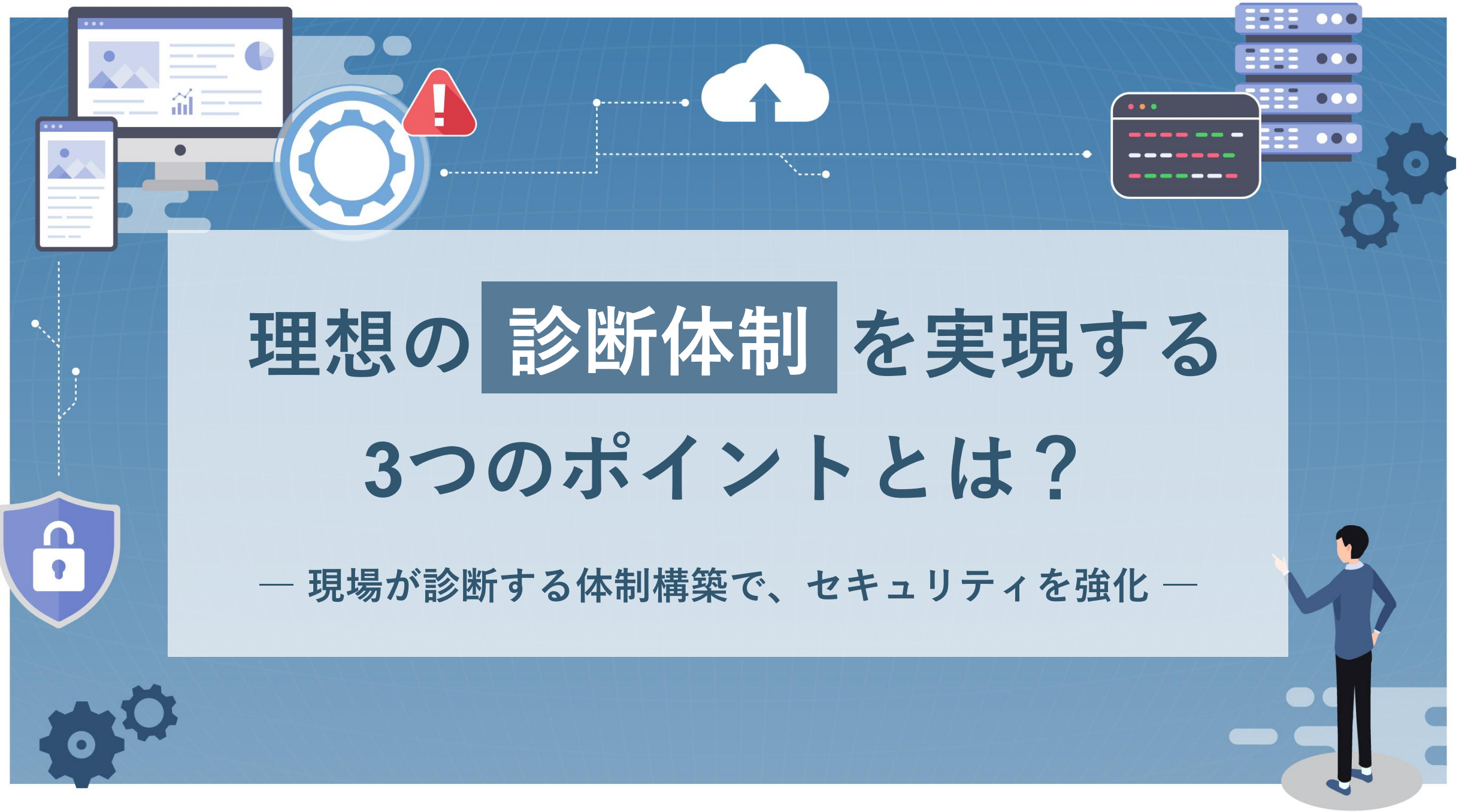
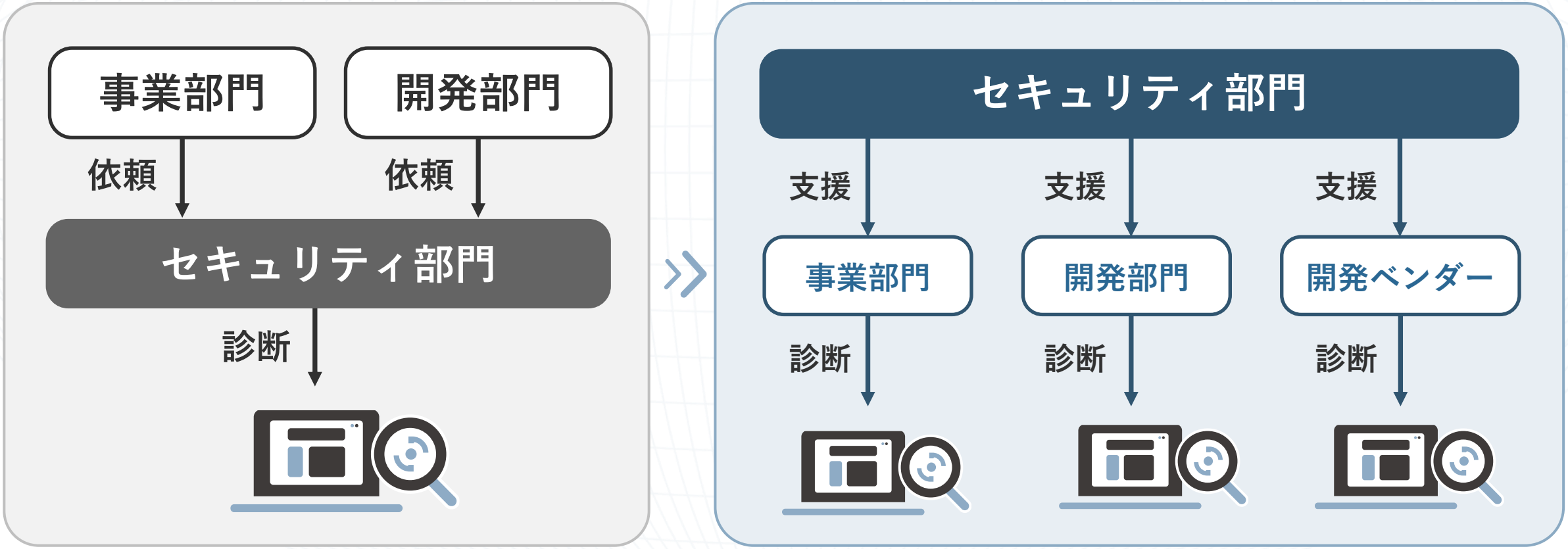


理想の診断体制を実現する3つのポイントとは？

― 現場が診断する体制構築で、セキュリティを強化 ―

脆弱性診断の運用体制の「理想形」

大規模な組織では特に、セキュリティ部門で診断を集約している体制から、
事業部門・開発部門（もしくは開発ベンダー）が診断業務を行う体制に移行するのが理想的。



運用拡大のフェーズで、こんな課題はありませんか？

ユーザー数増加の課題

**アカウント管理が限界に。
利用者拡大に対応しきれない**

サブアカウントの有効／無効の
切替作業に時間を取られてしまう

権限付与の課題

**権限設定が粗く、
リスクを抱えたまま運用**

誰でもドメイン追加可能な状態が
潜在的なインシデント要因に

ログインの課題

**全社の認証統一に合わせ、
SSO対応が必須に**

複数ID管理から脱却し、
統制を強化する必要がある

課題解決のために検討したいこと

ユーザー数増加の課題

誰でも、いつでも、
好きなだけ診断できる体制へ

サブアカウントを追加

必要な全員にアカウントを発行。
手動での切替作業から解放される。

権限付与の課題

自由度と統制を両立する
柔軟な権限設計が可能に

カスタムロールを作成

ドメイン追加操作などの操作を制限し、
リスクを抑えつつ十分な権限を付与。

ログインの課題

全社ポリシーに沿った、
安全でシンプルなログインへ

SSO対応

社内ID基盤と連携可能。
パスワード管理を統一できる。

課題解決のために検討したいこと

サブアカウントを追加

- 多くの部署が関わっても、カスタムロール機能を活用することで、細かな権限設定ができる

カスタムロールを作成

- 「管理者」「編集者」「閲覧者」の3段階の基本ロールに加え、よりきめ細やかな権限設定が可能
- 各ユーザーが必要最小限の権限のみを持つことで、誤操作や不正アクセスのリスクを低減
- 開発ベンダーにもサブアカウントを払い出しやすい

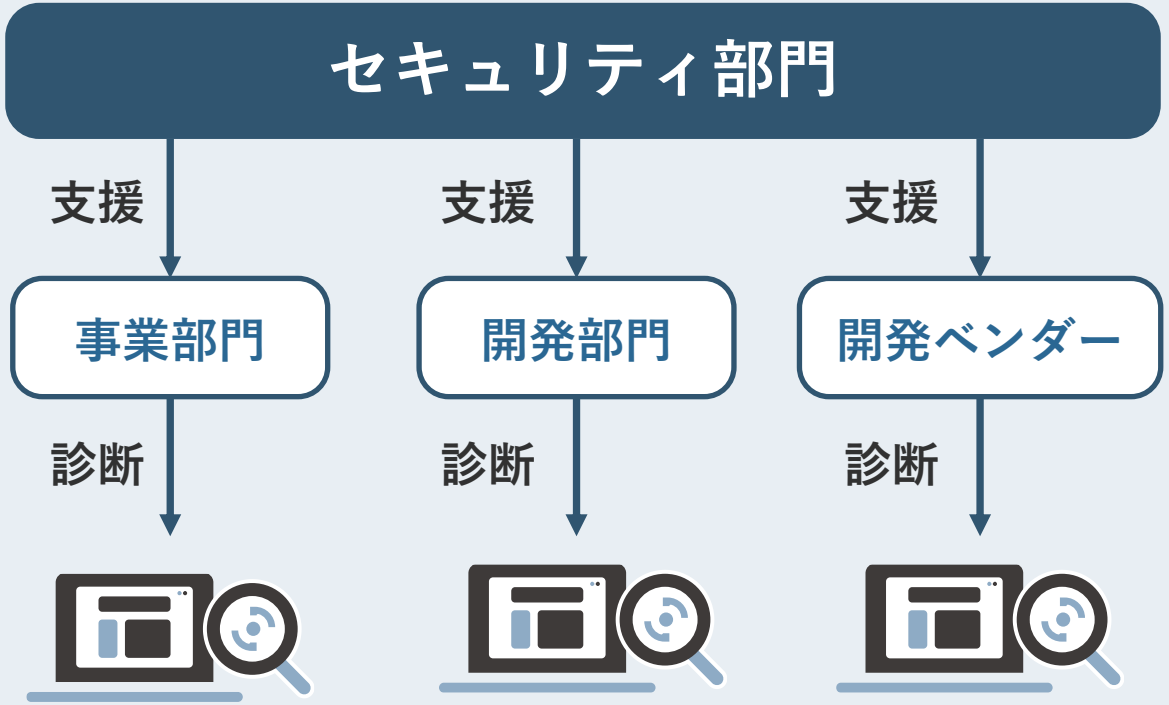
SSO対応

- パスワードの使い回しや忘れによる脆弱性を低減
- Google等のセキュアなログインの仕組みを使える
- 退職者のアカウント削除漏れなど、アカウント管理におけるセキュリティリスクを低減
- 強固なパスワードポリシーを容易に適用できる

事業部門・開発部門で診断する体制への移行で、セキュリティ品質が向上

セキュリティ部門は診断業務や間接作業から解放され、
戦略やガバナンス強化に集中できる。

事業部門・
開発部門は
手戻りや作業負荷を
なくし
スピードと品質を
両立できる。



開発ベンダーに
対しては
自社のセキュリティ
基準に沿った
診断が依頼できる。

診断体制を移行した企業の成功事例

金融系A社

セキュリティ部門

支援

品質管理部門

診断

メーカーB社

セキュリティ部門

支援

開発ベンダー

納品前に
AeyeScanで診断

- ドメイン追加はセキュリティ部門が行い、診断を行う部門・ベンダーは指定されたドメインだけ診断
- 「巡回実行」「スキャン実行」の権限のみを付与したカスタムロールを作成し、割り当て

まとめ

診断業務を事業部門・開発部門が実施する体制に移行することで、
持続可能な診断とセキュリティ品質向上が実現します。

体制移行の進め方や、新体制での診断の運用法についても
弊社カスタマーサクセス担当者がご相談を承ります。

ご興味がございましたら、ぜひ弊社担当までお声がけください！

※弊社担当へのメールでなくとも、ご都合の良い手段でご連絡いただけますと幸いです

セキュリティに、確かな答えを。