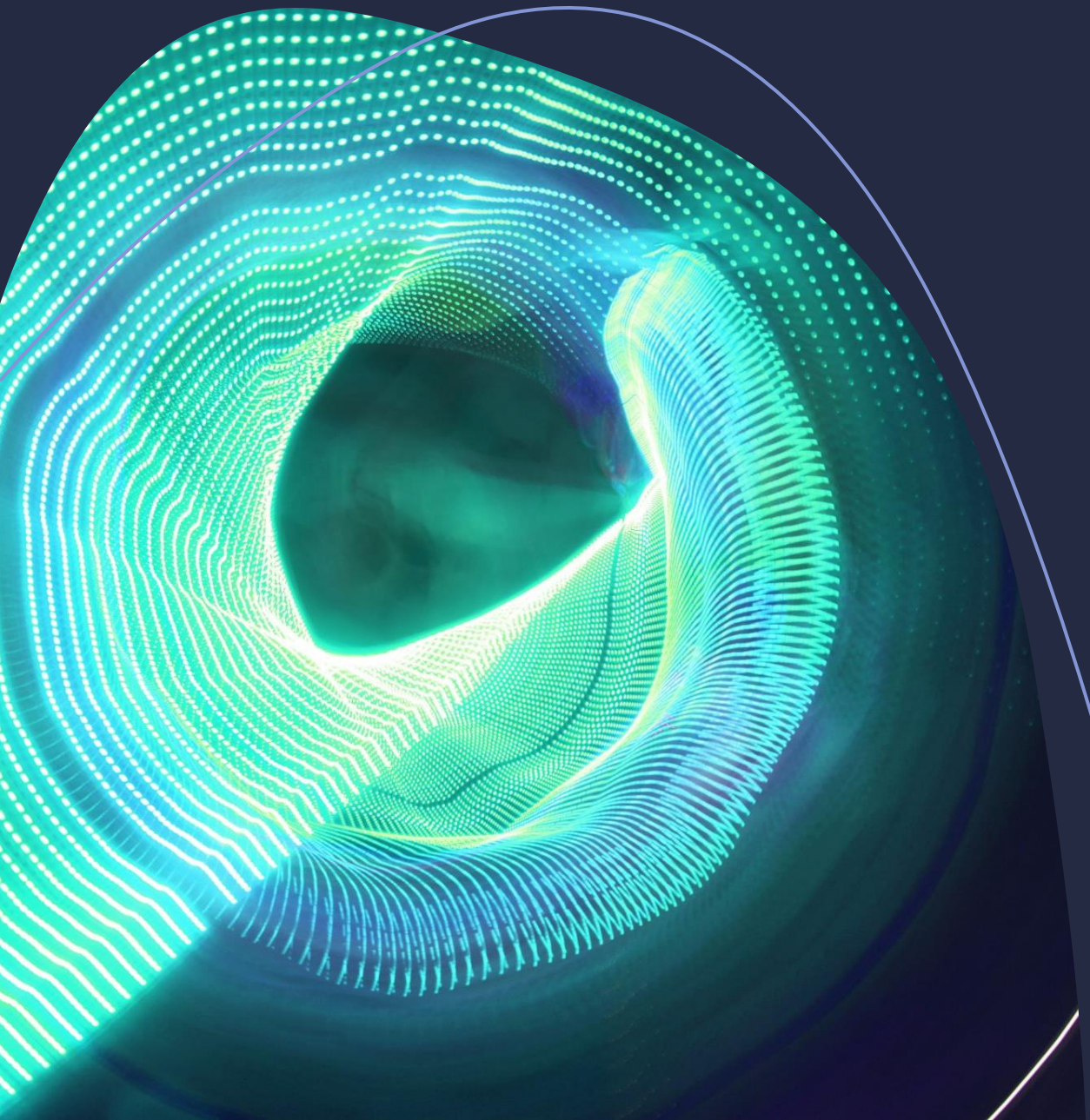


組織を守るためのASM

令和6年度.セキュリティ勉強会

第1章　ASMとは

Attack Surface Managementとは

組織の攻撃対象となりうる範囲を特定・評価・管理する取り組み。

- インターネット上に公開される自社資産の把握
- 潜在的な脆弱性の特定
- 攻撃可能な経路の理解と対策

これらを行うことでセキュリティの脅威から自社資産を守ります。

想定できる主な攻撃対象

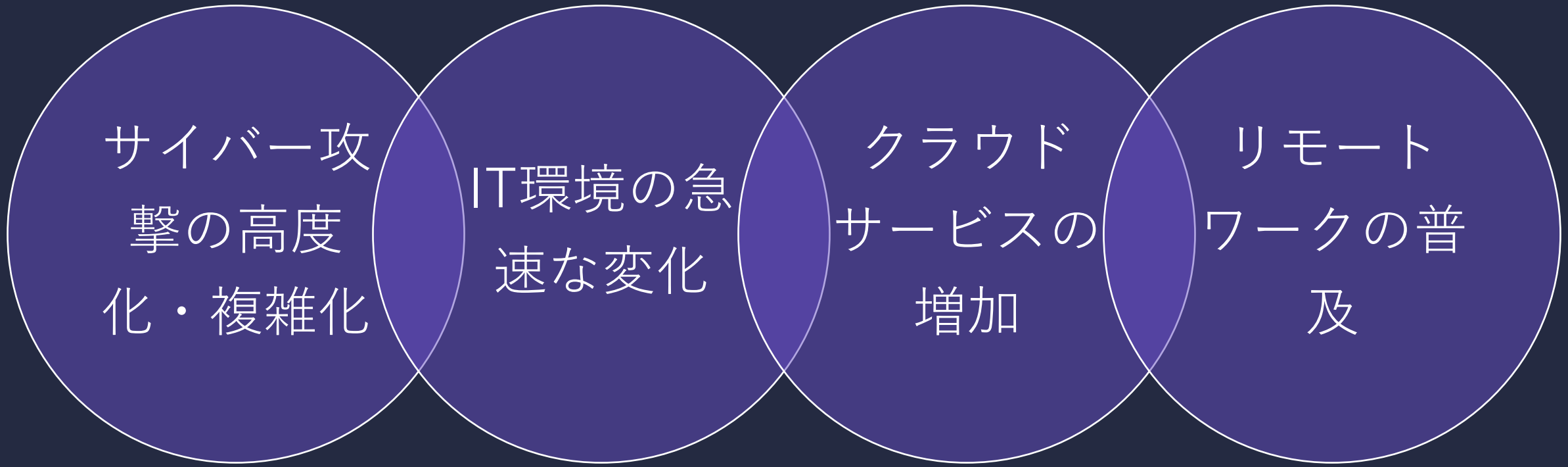
- Webサイト・サービス
- クラウドリソース
- メールシステム
- 社外向けサーバ
- リモートアクセス環境

このような外部との通信が発生するもの
が攻撃対象となりやすい。

ASMを怠ると…

思わぬ入り口からサイバー攻撃を受ける

サイバー攻撃を受けた際、原因究明が遅れて被害が拡大する



これらの理由から、昨今、ASMへの重要性が高まっている。

第2章　攻撃者から見た組織

攻撃者が収集する情報


不適切なアクセス制御
古いソフトウェアバージョン
ドメイン情報
• webサイト構成
• メールサーバ設定
• サブドメイン一覧
従業員情報
• メールアドレス
• 職務情報
• SNSアカウント
公開サービス
• クラウドストレージ
• 開発環境
• テスト環境
未把握の公開サーバ

第3章　シャドーITとリスク

シャドーITとは

情報システム部門の把握・管理外で利用されているIT資産やサービス

シャドーITの使用により、様々な問題が発生してしまう

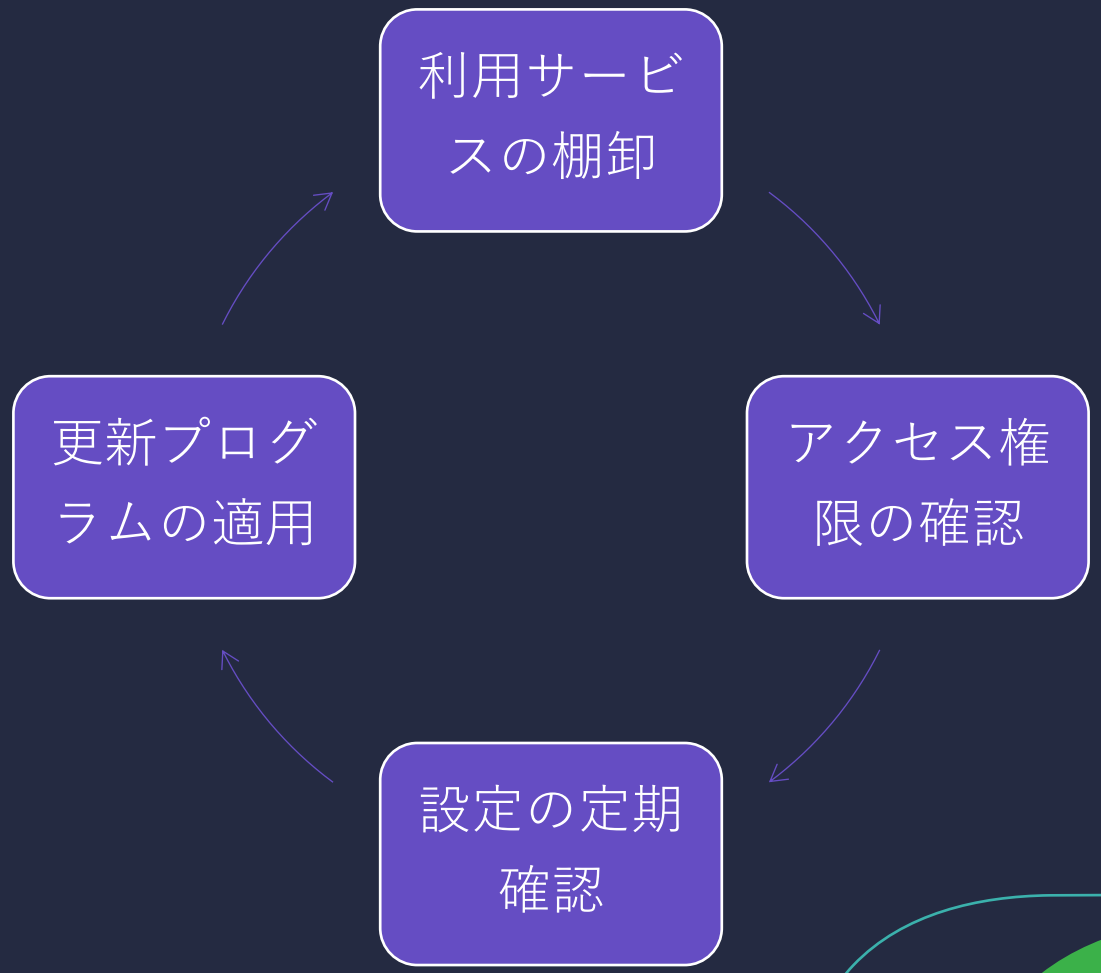
- 個人で契約したクラウドサービス
- 承認されていないアプリケーション
- 私用デバイスの使用
- 非公式なコラボレーションツール

→

- コンプライアンス違反
- データ漏洩
- 管理不能なアクセス経路
- セキュリティホール

第4章　実践的対策

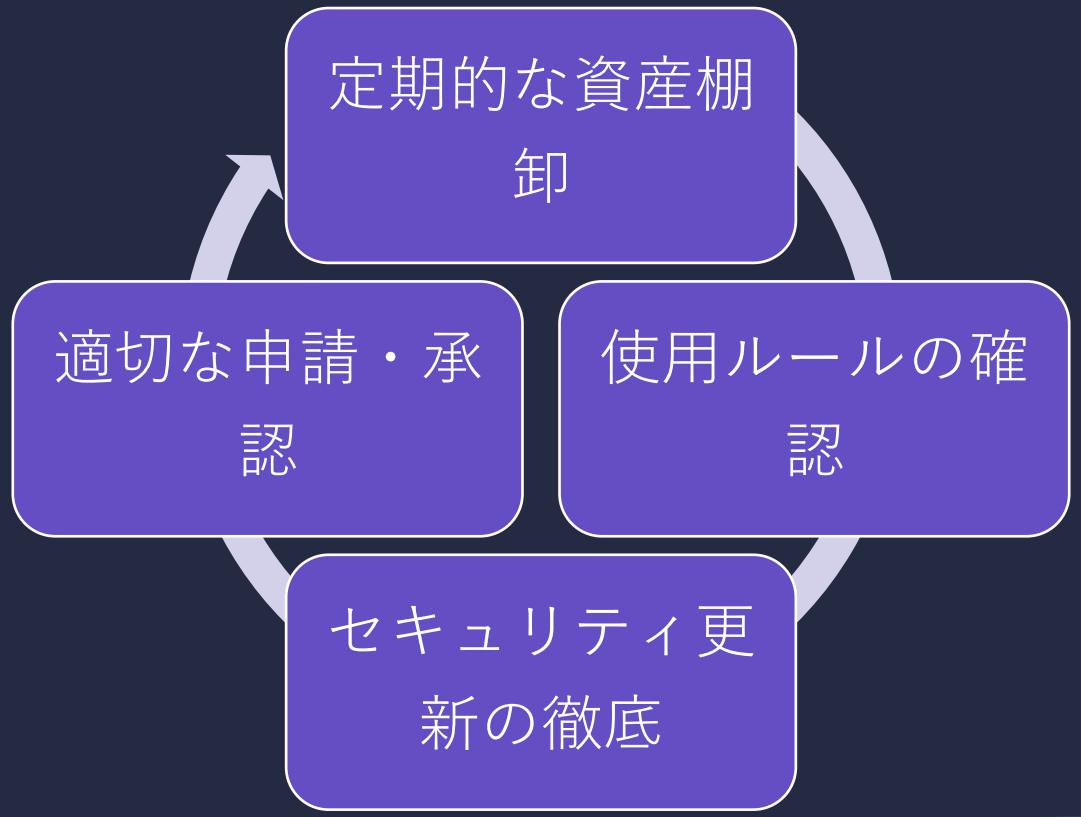
日常的な確認事項



報告すべき事項

- 新規サービス、デバイスの利用開始
- 設定変更
- 異常な動作
- 不審なアクセス

適切な管理を行うために



ディスカッション

ディスカッション

テーマ「私の考える公開資産」

- **グループディスカッション（10分）**
- **グループ発表（5分）**

3，4人組のグループで各部屋に分かれてディスカッションを行います。

テーマ「私の考える公開資産」

ディスカッションの流れ

自部門で把握している
公開資産の確認

参加者自身が考える
シャドーIT、公開資産
の情報交換

グループ発表

質疑応答

終わりに

ASMを適切に行い、

セキュリティの脅威から資産を守るためには、

皆様方全員の協力が必要です。

まずは自分が業務に使用するものの中にシャドーITが潜んでいないか、
確認してみてください。

最後に右のQRコードよりアンケートの回答をお願いします。