Attack Surface Management Service

ASMレポーティングサービス

機密情報を盗まれないように
定期的なチェックが必要です

その課題、可視化から始めませんか？

公開 IT 資産把握

テスト用の公開環境の放置
（停止忘れ）、旧サーバの廃止漏れ

問題・脆弱性把握

アプリケーションの設定不備、
セキュリティパッチの適用漏れ

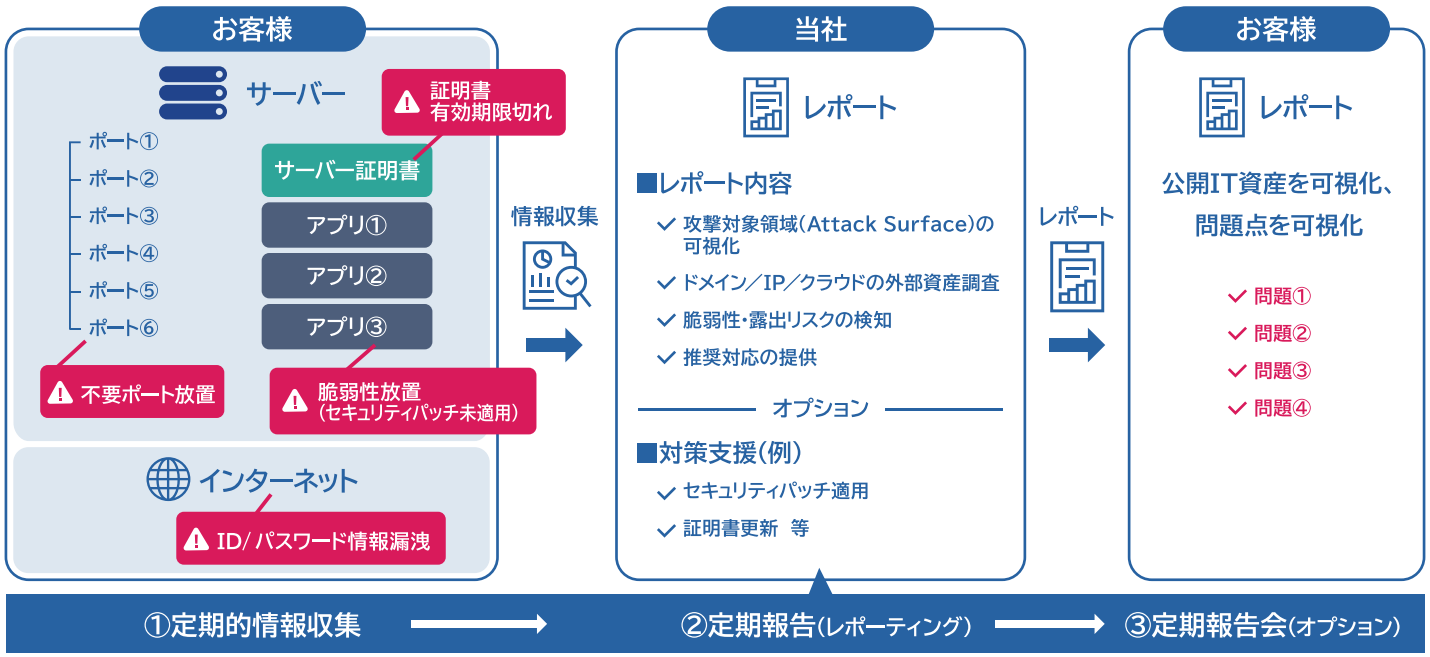
個人情報漏洩の把握

ダークウェブ等への認証情報の流出
（本人も気づかないケースあり）

昨今、企業の情報システムを取り巻く環境の変化により、近年のインシデントは「想定外の公開資産」から発生するケースが増えています。
特に、最も攻撃されやすいポイントである「自社で把握できていない IT 資産」へのセキュリティ対策が重要です。
当社の ASM レポーティングサービスでは、貴社の課題を可視化し、適切な対策をご提案いたします。

ASMレポーティングサービスとは

ASM（アタックサーフェスマネジメント）とは、サイバー攻撃の対象となり得る領域（Attack Surface）を把握・管理（Management）する取り組みです。
組織の外部（インターネット）に公開されている IT 資産を洗い出し、攻撃者と同じ視点でリスクを特定します。
従来のセキュリティ対策ではカバーしきれなかった「認識されていない資産」や「管理外のシステム」も含めて可視化し、レポーティングを行います。
これにより、攻撃を受ける前にリスクを発見し、迅速な対策が可能になります。



納品物（レポートサンプル）

毎月、サマリーレポート、アタックサーフェイス詳細レポート、情報漏洩（ID/ パスワード）レポートを提出します。

こちらはサンプルとなります

※サービスの詳細および提供価格については、当社までお問い合わせ下さい

株式会社クエスト
本社：東京都港区芝浦 3-1-1 msb Tamachi 田町ステーションタワー N 14F
TEL：050-3785-3977
Mail：market@quest.co.jp
URL：https://www.quest.co.jp/security/

お問い合わせはこちら