Solutions

¥400,000
税別・1回

ActiveDirectory脆弱性診断サービス

お客様のADは今、安全ですか？ ― 中小企業のセキュリティを本格診断

こんなお悩みはありませんか？

01 管理が属人化
AD担当者が少なく設定ミスが長期放置されている

02 リスクが見えない
過剰権限・休眠アカウントの実態を数値で把握できていない

03 リスクの実態が不明
設定不備がどのくらい存在するか把握できていない

04 ISMS・Pマーク対応で苦労
証跡・ログ整備に時間とコストがかかっている

サービスの特長

● スコアで見えるリスク評価
ADを4カテゴリ100点満点でスコアリング。リスクの大きさを数値・グラフで経営層にも説明できる

● 診断専用ライセンス使用
診断専用ツールによる安全・合法なサービス提供。安心してご依頼いただけます

● 最短1週間で納品
ヒアリング～診断～レポート提出まで約5～7営業日。迅速な課題把握を支援します

● 経営層に伝わるレポート
リスクスコア・成熟度・改善提言を整理。技術者以外にも伝わる構成で作成します

● 改善提言まで一貫対応
発見で終わらず「30日以内」「90日以内」の優先度別アクションプランを提示します

● 明確な定額料金
¥400,000（税別）の追加費用なし。見積もり・相談は無料でお気軽にどうぞ

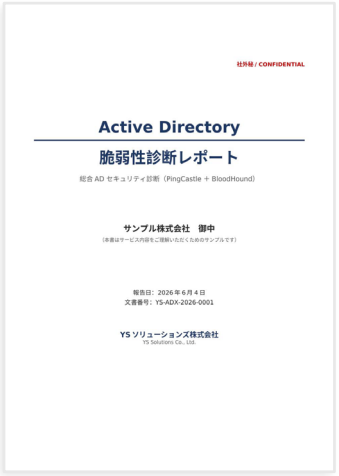
他社サービスとの比較

比較項目	YS診断サービス	大手IT セキュリティ	一般SIer AD診断
ADリスクスコア（100点）	**あり**	独自指標	なし
料金（スポット）	**¥400,000**	¥500,000～	要見積
納品期間	**5～7営業日**	2～4週間	1～2ヶ月
改善提言（優先度付）	**あり**	あり	指摘のみ
無料相談・見積	**あり**	なし	なし

診断の流れ：
① ヒアリング（1～2日） → ② 診断実施（2～3日） → ③ レポート作成（2～3日） → ④ 報告・改善提案（1日）

ActiveDirectory脆弱性診断サービス

スコアで見えるリスク、具体的な改善提言まで。経営層にも伝わる診断レポートをお届けします。


社外秘 / CONFIDENTIAL

Active Directory

脆弱性診断レポート

総合 AD セキュリティ診断（PingCastle ＋ BloodHound）

サンプル株式会社　御中

（本書はサービス内容をご理解いただくためのサンプルです）

報告日：2026 年 6 月 4 日

文書番号：YS-ADX-2026-0001

YS ソリューションズ株式会社

YS Solutions Co., Ltd.

表紙


AD 脆弱性診断レポート（サンプル） | 社外秘

1. エグゼクティブサマリー

1.1 総括

サンプル株式会社の Active Directory（以下 AD）環境を診断した結果、ドメイン全体の管理者権限（Domain Admins）が、一般利用者の権限から比較的容易に奪取され得る状態にあることを確認しました。総合リスクスコアは 70 ／ 100（低いほど安全）、成熟度レベルは 5 段階中 2 と評価され、早急な是正を要する重大なリスクが 3 件、重要なリスクが 5 件存在します。

特に、特権アカウントへ到達する具体的な攻撃経路が複数確認されており、万一いずれかの一般アカウントが侵害された場合、攻撃者は数ステップで AD 全体を掌握し得ます。これはランサムウェア被害や情報漏えいに直結する深刻な状態です。

総合リスクスコア	成熟度レベル	重大度別件数
70 / 100（低いほど安全）	2 / 5（5 が最良）	C:3 H:5 M:4 L:6

1.2 主要な発見事項

- 【重大】サービスアカウントが Kerberoasting に対して脆弱で、かつ Domain Admins に所属。1 アカウントの侵害で AD 全体が掌握され得る。
- 【重大】事前認証が無効なアカウントが 3 件存在し、AS-REP Roasting によりオフラインでパスワード解読が可能。
- 【重大】krbtgt アカウントのパスワードが長期間（5 年以上）未更新で、Golden Ticket 攻撃の潜在リスクがある。
- 【重要】Domain Admins のメンバーが 15 名と過剰で、最小権限の原則から逸脱している。
- 【重要】LAPS が未導入で、複数端末のローカル管理者パスワードが共通化している疑いがある。

1.3 ビジネスインパクト

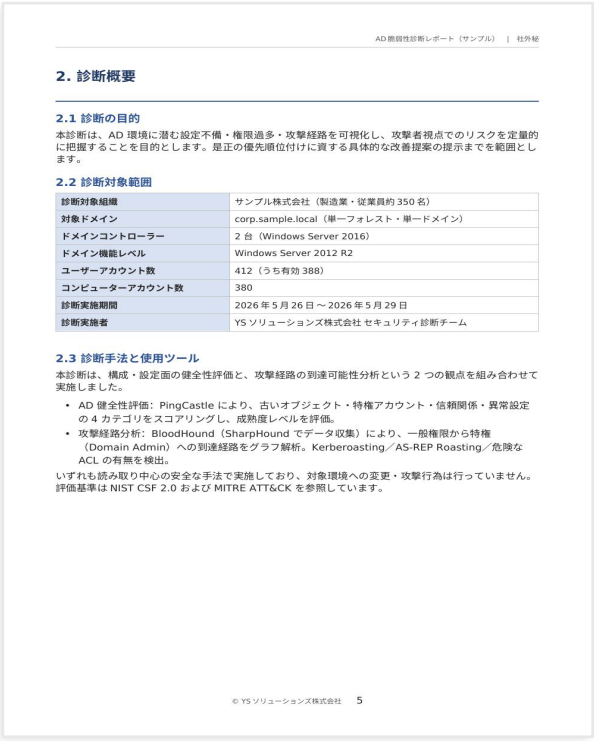
AD は全社の認証基盤であり、ここを奪取されることは「全システムへの不正アクセス」「業務停止を伴うランサムウェア感染」「個人情報・機密情報の大量漏えい」に直結します。本診断で確認された経路は、いずれも特別なゼロデイ攻撃を必要とせず、既知の手法のみで成立する点が特徴です。是正は技術的に十分実行可能であり、優先度の高い項目から順次対応することでリスクを大きく低減できます。

1.4 推奨される最優先アクション（30 日以内）

1. Domain Admins 所属のサービスアカウントを専用の権限分離アカウントへ移行し、SPN を見直す。
2. 事前認証無効アカウントの設定を是正し、サービスアカウントのパスワードを長く複雑なもの（25 文字以上）へ変更する。
3. krbtgt パスワードを 2 回ローテーションし、Domain Admins メンバーを必要最小限へ削減する。

© YS ソリューションズ株式会社　4

エグゼクティブサマリー（スコア・主要発見事項）


AD 脆弱性診断レポート（サンプル） | 社外秘

2. 診断概要

2.1 診断の目的

本診断は、AD 環境に潜む設定不備・権限過多・攻撃経路を可視化し、攻撃者視点でのリスクを定量的に把握することを目的とします。是正の優先順位付けに資する具体的な改善提案の提示までを範囲とします。

2.2 診断対象範囲

診断対象組織	サンプル株式会社（製造業・従業員約 350 名）
対象ドメイン	corp.sample.local（単一フォレスト・単一ドメイン）
ドメインコントローラー	2 台（Windows Server 2016）
ドメイン機能レベル	Windows Server 2012 R2
ユーザーアカウント数	412（うち有効 388）
コンピューターアカウント数	380
診断実施期間	2026 年 5 月 26 日～2026 年 5 月 29 日
診断実施者	YS ソリューションズ株式会社 セキュリティ診断チーム

2.3 診断手法と使用ツール

本診断は、構成・設定面の健全性評価と、攻撃経路の到達可能性分析という 2 つの観点を組み合わせて実施しました。

- AD 健全性評価：PingCastle により、古いオブジェクト・特権アカウント・信頼関係・異常設定の 4 カテゴリをスコアリングし、成熟度レベルを評価。
- 攻撃経路分析：BloodHound（SharpHound でデータ収集）により、一般権限から特権（Domain Admin）への到達経路をグラフ解析。Kerberoasting／AS-REP Roasting／危険な ACL の有無を検出。

いずれも読み取り中心の安全な手法で実施しており、対象環境への変更・攻撃行為は行っていません。評価基準は NIST CSF 2.0 および MITRE ATT&CK を参照しています。

© YS ソリューションズ株式会社　5

診断概要・診断専用ツールスコア表

主な検出項目

特権アカウント	Domain Admins過剰・サービスアカウントのKerberoasting脆弱性	**Kerberos設定**	AS-REP Roasting・krbtgt長期未更新・Golden Ticket攻撃リスク
成熟度レベル評価	5段階の成熟度でAD管理体制を評価。経営層向け説明資料として活用可	**パスワードポリシー**	最小文字数・ロックアウト設定不備・LAPS未導入の検出
休眠・不要OBJ	90日以上未ログイン・退職者アカウント・未使用コンピューター	**GPO・信頼関係**	グループポリシーの矛盾・危険なACL設定・外部信頼の有無

納品物

1. **エグゼクティブサマリー**
   経営層向けにリスクスコア・成熟度レベルを提示
2. **重大リスク一覧**
   Critical～Lowに分類・MITRE ATT&CKマッピング
3. **スコア表**
   4カテゴリ別スコアと検出項目の詳細一覧
4. **優先度別改善提言**
   30日以内・90日以内・中長期アクションプラン

Solutions

YSソリューションズ株式会社

〒102-0074
東京都千代田区九段南1-5-6 りそな九段ビル5F KSフロア
TEL：03-6403-7459　　info@ys-solutions.jp
https://www.ys-solutions.jp/