セキュリティ YOROZU 相談

情報漏えいリスク診断（任意活用）のご案内

セキュリティ YOROZU 相談をご契約頂き、ありがとうございます。
社内における情報漏えいのリスクを簡易に診断するお客様任意利用のサービスをご案内致します。

【情報漏えいリスク診断の内容】

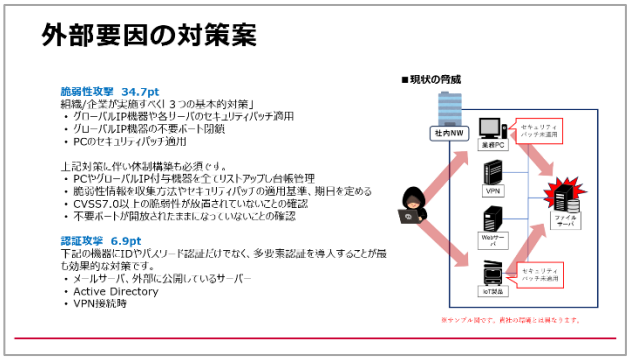
情報漏えいリスク診断は 11 の設問に回答することで、外的要因による情報漏えいのリスクと、内的要因による情報漏えいのリスクの両面から簡易に診断を行い、診断結果を「リスク度の総合評価」、「外的要因リスク度」「内的要因リスク度」を数値的に表し、要因に対する推奨対策をアドバイスとして纏めたレポートをご提示します。

診断レポートのサンプル


診断結果

情報漏えい発生リスク	66.8pt	リスクレベル	E

情報漏えい pt	リスクレベル	推奨事項
75~100	F	重大な被害が発生する可能性が極めて高く、早急な脆弱性の特定と対策が必須
60~74.9	E	重大な被害が発生する可能性が高く、早急な脆弱性の特定と対策が必要
40~59.9	D	重大な被害が いつ発生してもおかしくない、脆弱性の特定と見直し検討が必要
25~39.9	C	重大な被害が いつ発生してもおかしくない、脆弱性の特定と見直し検討が必要
10~24.9	B	危険度は低いが、将来的な危険性を認識するための脆弱性の特定を推奨
0~9.9	A	危険度は低い、現状問題が生じる可能性は低い。効果維持の継続が必要


外部要因の対策案

脆弱性攻撃 34.7pt
組織/企業が上級すべく 3 つの基本的対策」
・グローバルIP機器や各リーバのセキュリティパッチ適用
・グローバルIP機器の不要ポート閉鎖
・PCのセキュリティパッチ適用

上記対策し伴い体制構築も必須とり。
・PCやグローバルIP付与機器を全 (リストアップし台帳管理
・脆弱性情報を収集方法やセキュリティパッチの適用基準、期日を定める
・CVSS7.0以上の脆弱性が放置されていないことの確認
・不要ポートが開放されたままになっていないとの確認

認証攻撃 6.9pt
下記の機器にIDやパスワード認証だけでなく、多要素認証を導入することが最も効果的な対策です。
・メールサーバ、外部に公開しているサーバー
・Active Directory
・VPN接続時

■現状の構成

※サンプル値です。貴社の環境と比較なります。

【利用方法】

情報漏えいリスク診断を活用される場合、下記の URL にアクセスし、全 11 問の設問フォームより回答を入力して下さい。※最後に「送信」ボタンをクリックして下さい。

ヒアリングポータル URL はこちら：https://forms.office.com/r/KSV9cSM9d9

利用方法でご不明な点が有りましたら、ご遠慮なく「セキュリティ YOROZU 相談窓口」にお電話・Mail にてご連絡を頂くことで、診断用のヒアリングポータル URL をご連絡致します。

【診断書の送付について】

全 11 問の設問フォームより回答を入力頂いた後、診断結果としてレポートに取り纏めます。お客様へのレポート提供は、ご準備が整い次第（5営業日後を目安に）、お客様へ準備完了通知メールをお送りすると共に、メール本文に記載する URL から情報漏えいリスク診断レポートをダウンロードして頂きます。

セキュリティ YOROZU 相談