

## 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。

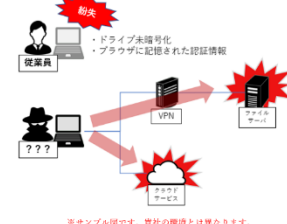
### 【情報漏えいリスク診断の内容】

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			docomo business
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要	
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、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	

内部要因の対策案		docomo business
<b>機器紛失 20.6pt</b> 機密情報が保存されている記憶媒体(PC、USB等)の紛失を想定した対策を推奨します。 ストレージメディアの保護策として暗号化設定(HDD暗号化、ドライブの暗号化、フォルダ暗号化等)が有効です。 さらにPCには、起動時にパスワード入力求め、入力失敗上限回数(ロックアウト機能)を設定が有効です。	<b>■機器紛失の現状の脅威</b> 	
<b>故意(内部犯行) 8.4pt</b> 1人の担当者が2つ以上の職務を重複して持つことで不正の機会が発生してしまいます。例えば、アクセス権の要求に対し、自己承認が認められている、または正しく承認されるプロセスがない場合、本来必要のないアクセス権が付与され、不正な閲覧や持ち出しが発生する可能性があります。 「アクセス権の要求・承認・実装」や「アクセス制御と監視」等の職務を分離することが重要です。		

※サンプル図です。貴社の環境とは異なります。

### 【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/kaAjvwNu2R>

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。