



# セキュリティアセスメント

業務や開発プロセスに潜む脆弱性を洗い出し、想定される脅威を特定します。  
脅威分析の結果を踏まえ、課題やセキュリティ対策をアドバイスします。



既存／新規事業のセキュリティ脅威を知る



システムや組織に損害をあたえる「脅威」を把握できていますか？

- サイバー攻撃による脅威  
盗聴、改ざん、不正アクセス、盗難、ウイルス感染など
- ミスやリテラシー不足による脅威  
システムのバグ、メール誤送信、誤ったファイルの削除など



「セキュリティアセスメント」で解決！

- 脅威分析の結果をセキュリティ強化に活かしたい
- 脅威分析の時間を確保できない
- 自社にとって特にリスクの高い脅威が知りたい

Service Menu

ドキュメント精査

業務／開発プロセス可視化

- ドキュメント精査や従業員へのヒアリングをもとに、想定される脅威を特定
- リスク評価によるランク付けでクリティカルな課題を浮き彫りに

特長



「システム」「人」  
「プロセス」の脅威を  
総合評価



対処の優先度が  
一目でわかる



ヒアリングに  
基づく  
現実的な改善策

Service Flow

サービスの流れ

01

現状把握



脆弱性診断等によるシステムの現状調査や、業務マニュアルや設計書の精査を通じて、検査対象の全体像を把握します

02

ヒアリング



現状把握の結果をもとに、実担当者にヒアリングを行い、システムや組織の実態を明らかにします

03

アセスメント



1～2の結果をふまえ、組織や業務に潜む脆弱性と脅威を洗い出します

04

リスク評価／  
改善策の提案



脆弱性や脅威をもとにリスクを評価し、改善策をご提案します