その常識、変えてみせる。
SHIFT

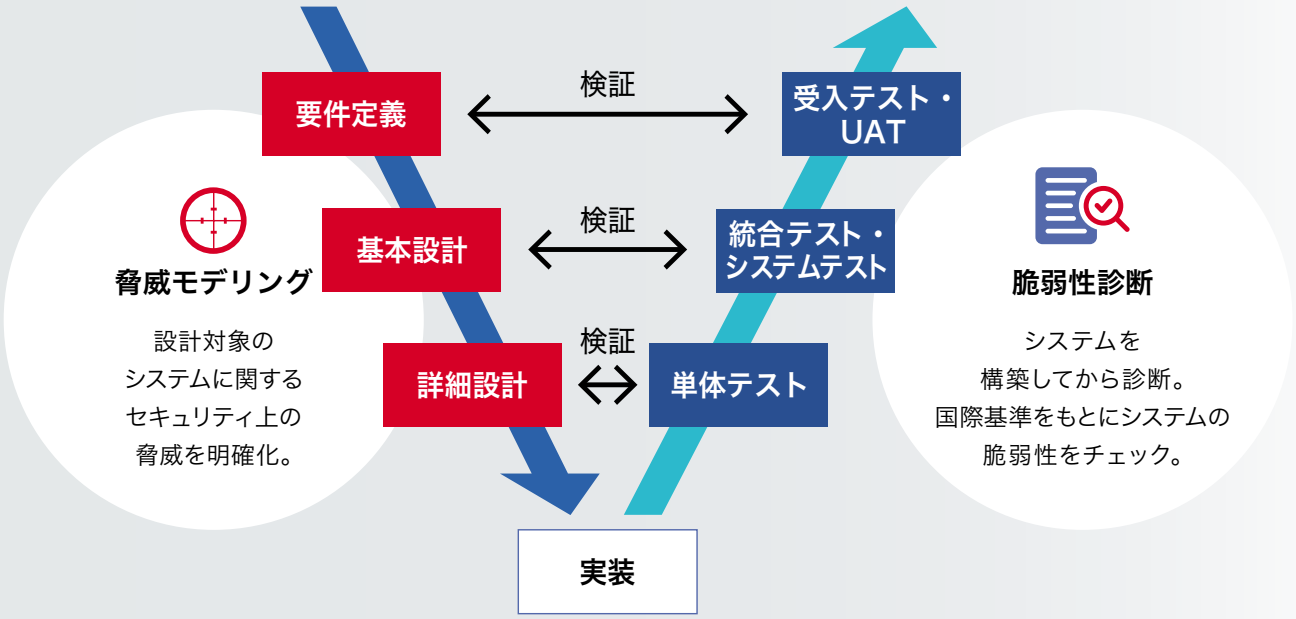
脅威モデリングサービス

敵（てき）を知る。先手を打つ。

- なりすまし
- データの改ざん
- 否認
- 情報漏えい
- サービス妨害
- 権限昇格

脅威モデリングは、**攻撃者の目線**でシステムアーキテクチャーや機能仕様上の弱点を洗い出し、セキュリティリスクを特定するセキュリティ診断手法です。**設計段階**からセキュリティを意識して予防することで、運用時点での対策よりも**低コストで安全性の高い開発**が可能に。「サイバー攻撃対策にどこまでコストをかけていいかわからない」「脆弱性診断だけでいいのか不安がある」そんなお客様に最適です。

脆弱性診断との違い



SHIFTの脅威モデリングの特長

1 攻撃意図と アタックサーフェスを 明確化

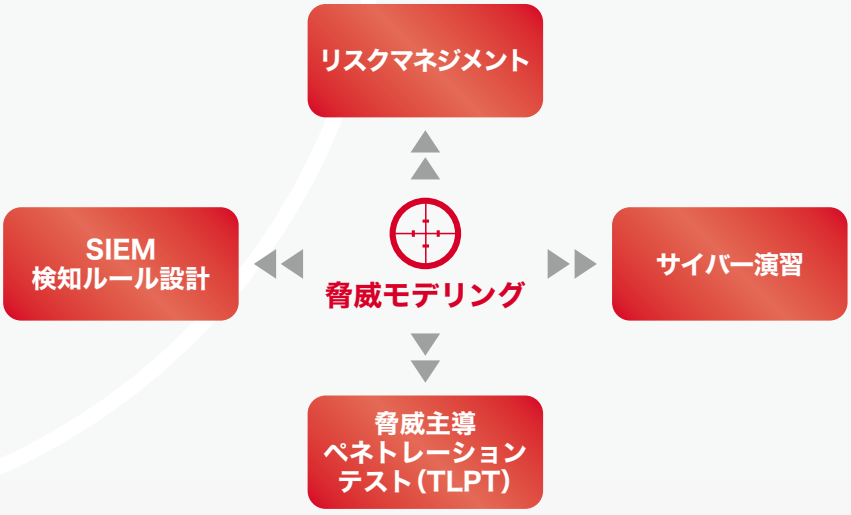
攻撃者の攻撃意図を明確にするとともに、データフロー図（DFD）により攻撃の突破口となるアタックサーフェスを明確にします。

2 攻撃手法ライブラリや 最新の攻撃手法をもとに 攻撃シナリオを抽出

米国 MITRE による攻撃手法のナレッジベース（CAPEC、ATT&CK）や最新の攻撃手口に基づいて攻撃シナリオを抽出します。

3 脅威モデリングの 実施結果を、 さまざまな セキュリティ施策に活用

脅威モデリングで抽出された攻撃シナリオやリスク分析の結果は、さまざまなセキュリティ対策に活用することができます。



導入実績（一例）

実施時期	お客様	評価対象システム
2022年 5月	大手精密機器メーカー	PoSシステム
2022年 10月	大手印刷会社	カード発行サービス
2022年 11月	大手部品メーカー	ソフトウェア開発基盤システム
2022年 11月	大手広告会社	社内情報システム
2022年12月	大手不動産販売会社	不動産売買サービス
2023年 3月	大手ゲームメーカー	ゲームサービス
2023年 5月	大手事務機器メーカー	社内情報システム

実施時期	お客様	評価対象システム
2023年 5月	小売業業者	販売ポータルサイト
2023年 7月	ソフトウェアメーカー	大規模イベントサイト
2023年 9月	大手銀行	社内システム
2023年12月	損保会社	保険契約システム
2024年 3月	大手ゲームメーカー	全社システム
2024年 5月	大手証券会社	SASE環境
2024年 5月	システム開発ベンダー	デジタルバンキングシステム

その常識、変えてみせる。
SHIFT

お気軽にお問い合わせください
0120-142-117（ひんしつ いいな）
IP電話など、フリーダイヤルをご利用できない場合は、市外局番の電話番号におかけください。
TEL.03-6809-2979
（電話受付時間／平日9:00～18:00）
marketing@shiftinc.jp
https://service.shiftinc.jp/contact/