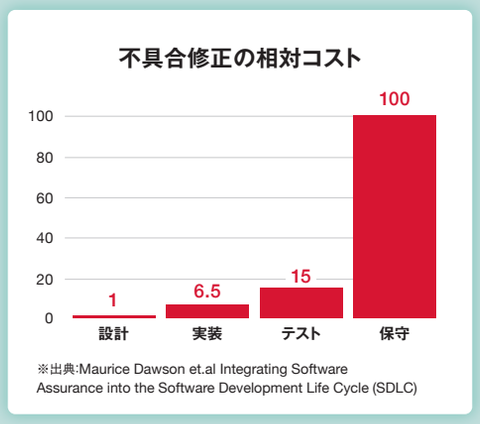
その常識、変えてみせる。
SHIFT

これからのソフトウェアセキュリティは、
上流工程から手を打つ。

セキュア・バイ・デザイン支援サービス

ソフトウェアの設計上の問題点が保守段階で見つかった場合、
設計段階で発見するのに比べておよそ100倍のコストがかかるといわれています。
セキュリティ上安全なソフトウェアを開発するためには、**上流工程の設計段階からセキュリティを考慮し（Shift Left）**、ソフトウェア開発工程における設計段階からセキュリティ対策を行う**「セキュア・バイ・デザイン」**の考え方が重要です。
SHIFTでは、要件定義と基本設計のフェーズにおいてセキュア・バイ・デザインの実践をご支援。 製品ローンチ後にセキュリティ設計上の問題点が発覚して**手戻りが生じるリスクを低減**できISMSなど多くの標準やガイドラインで求められている**セキュアな開発体制の構築が可能**となります。



※出典:Maurice Dawson et.al Integrating Software Assurance into the Software Development Life Cycle (SDLC)

Shift Left

要件定義
- **セキュリティ要件の策定**
- 外部利用サービスのセキュリティ上の安全性確認
- データマッピング

基本設計／詳細設計
- セキュリティアーキテクチャー設計
- **脅威モデリング**
- セキュリティ詳細設計

実装

テスト／リリース

保守／運用

上流工程施策のうち、要件定義書アセスメントと脅威モデリングを中心にご支援いたします。

2つのアプローチで相互補完しながら、設計上の問題点を洗い出し。

ベースラインアプローチ

包括的な基準（ベースライン）に基づいて
セキュリティ要件の充足性を網羅的にチェック

［要件定義書アセスメント］

お客様が作成した要件定義書について、
独自のセキュア設計チェックシートに基づき
内容の充足性を確認します。

要件定義書

レビュー

機能要件
機密性・完全性を
確保するための要件

非機能要件
可用性を確保するための要件

法令要件
サイバーセキュリティ
関連法令の遵守要件

調達要件
サプライチェーン
セキュリティに関する要件

相互補完

リスクベースアプローチ

脅威シナリオに対するリスク評価により
設計上の弱点を特定し、対策の優先度を絞り込む

［脅威モデリング］

**脅威モデリングの標準的な手法である
STRIDE／DREAD法**を用いて
攻撃手口を洗い出し、リスク評価を行います。

STEP 1	守るべき資産と脅威エージェントの識別
STEP 2	データフローの可視化
STEP 3	脅威の洗い出し（STRIDE）
STEP 4	脅威に基づく攻撃シナリオの抽出
STEP 5	攻撃シナリオに関するリスク評価（DREAD）

支援実績

実施時期		お客様
2022年	5月	大手精密機器メーカー
	10月	大手印刷会社
	11月	大手部品メーカー
	11月	大手広告会社
	12月	大手不動産販売会社
2023年	3月	大手ゲームメーカー
	5月	大手事務機器メーカー
	5月	小売業者
	7月	ソフトウェアメーカー
	9月	大手銀行

実施時期		お客様
2023年	12月	損保会社
2024年	3月	大手ゲームメーカー
	4月	大手証券会社
	5月	大手証券会社
	5月	銀行系ソフトウェアメーカー
	10月	小売業者
	10月	銀行
	11月	銀行
	11月	大手映像制作会社
		and more...

セキュア・バイ・デザインの実践について、お気軽にお問い合わせください。

その常識、変えてみせる。
SHIFT

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/