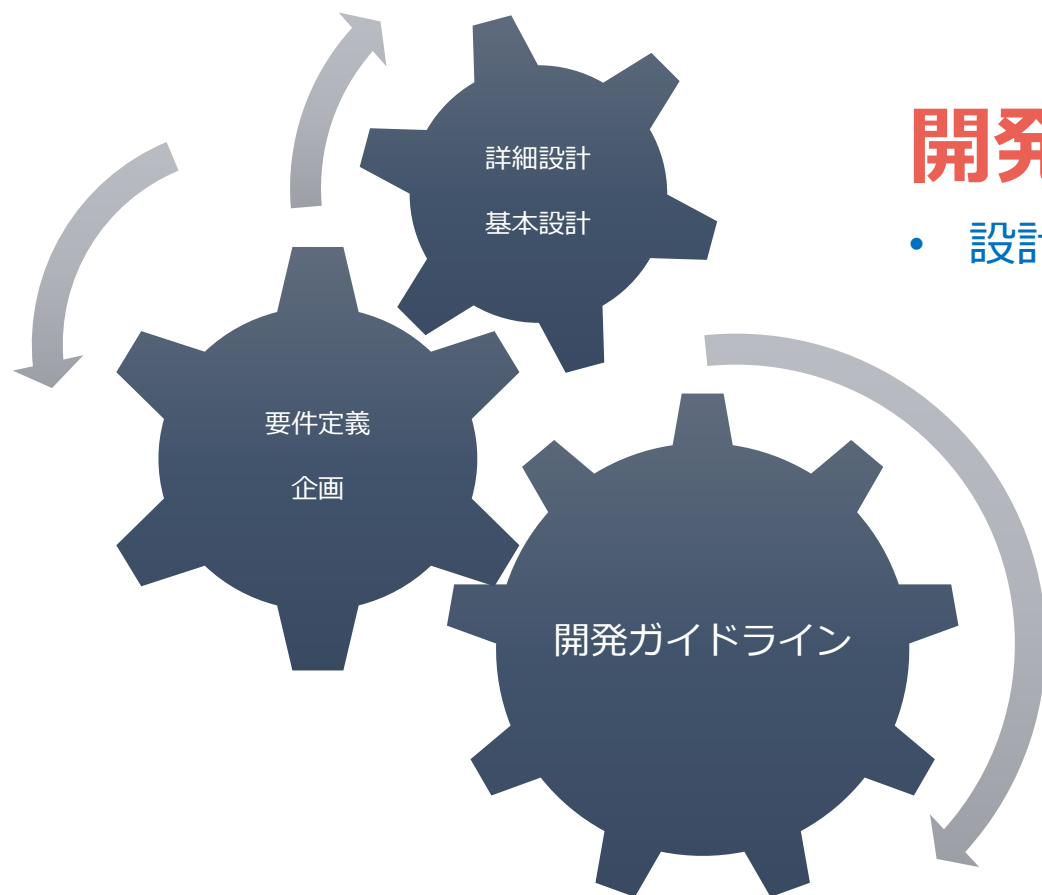


セキュア開発ガイドライン策定 サービス紹介

EGセキュアソリューションズ株式会社

セキュア開発ガイドライン策定サービス



開発ガイドラインとは？

- 設計の前に準備される開発全体の指針となる規約
- ガイドラインに基づき開発を進めることでセキュアなシステムを完成させることを目的とする
- 開発への普遍的かつ持続的に実施すべき内容が多く、他プロジェクトでの横断的な利用が可能

ポイント

1. 貴社ニーズに即した開発ガイドラインの策定

- ヒアリングにもとづく、現状に即したガイドライン。
- 使いやすく「逆引き」方式のガイドライン。
- SQLインジェクション、クロスサイト・スクリプティングのみならず、近年のセキュリティ動向に即した各種の脆弱性への対策が可能。

ガイドライン



2. 上記ガイドラインの遵守を確実にするためのチェックシートの策定

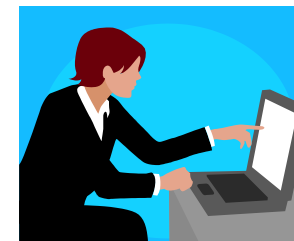
- 貴社向けにカスタマイズされ、セキュリティガイドラインに対応したチェックシートの作成。
- ソースコード検査、動作確認を組み合わせた効率的な検査方法。
- 開発委託先におけるチェック、貴社における受け入れ検査へ適用可能。

チェックシート



3. 同チェックシートの運用トレーニング、設計レビュー（オプション）

- 作成したチェックシートを運用するためのチェック体制が必要。
- 定着させるためのトレーニングをオンサイトで実施。
- ガイドラインに則した設計になっているのかレビューを実施。



導入効果

1. セキュリティ対策の担当範囲が明確になり、あいまいさがなくなる。

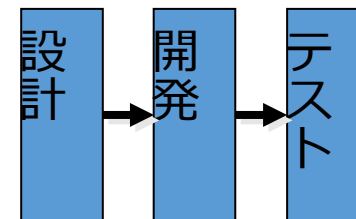


設計担当



プログラム担当

2. 各工程で脆弱性が入り込まないように、対策を実施することで、セキュリティレベルの向上が期待できる。



3. セキュリティチェックシートを用いることで、ガイドラインにもとづいたテストが出来、対策漏れ・テスト漏れをチェックできる。



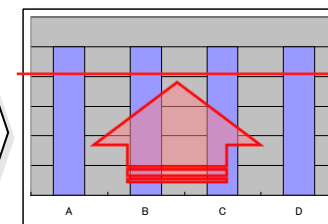
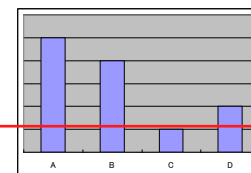
ガイドライン



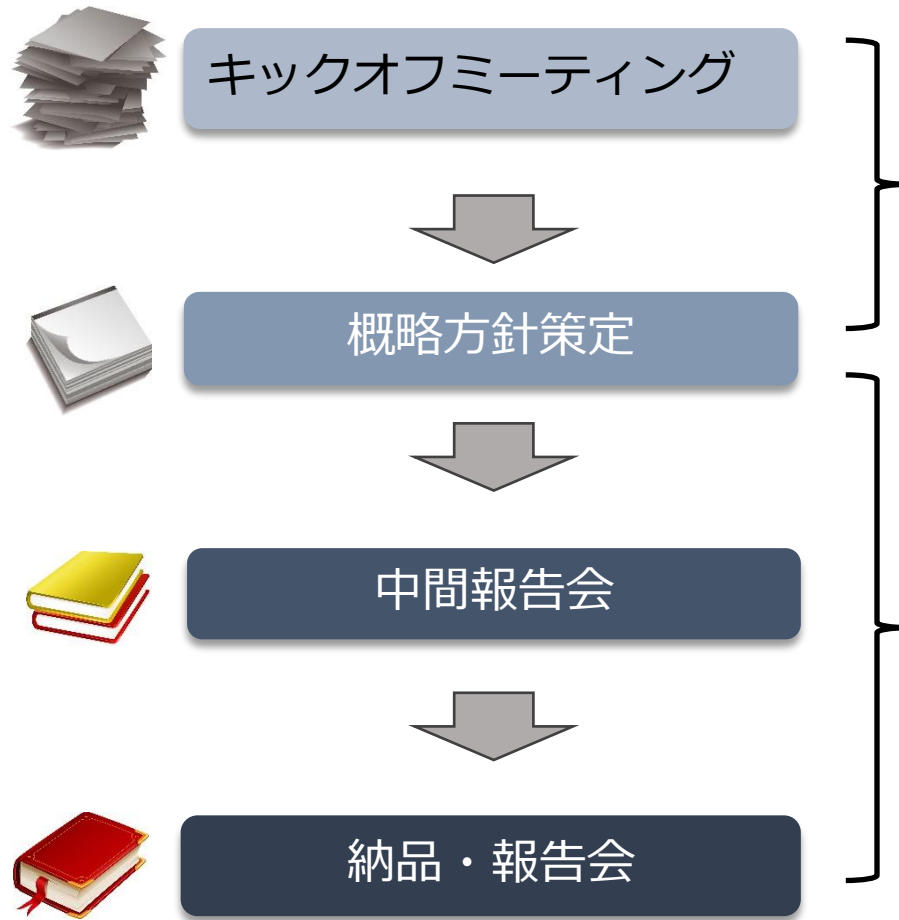
チェックシート

4. 担当者ごとのセキュリティ対策のばらつきが無くなり、セキュリティレベルの底上げが期待できる。

セキュリティレベル



導入ステップ



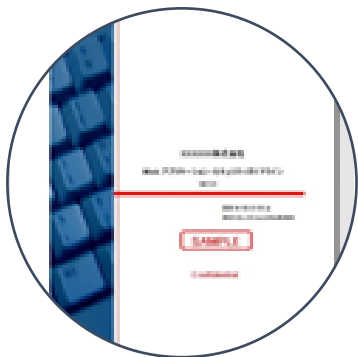
1. 貴社開発プロセスの現状ヒアリング

ギャップ分析
作成方針策定
メールなどでの確認作業
中間成果物作成

2. 中間報告会

カスタマイズされたガイドライン、
チェックシート制作
メールなどでの確認作業

特徴



「逆引き辞書」としての利用が可能

アプリケーションの機能別に作成するので、開発者が参照しやすい形態です

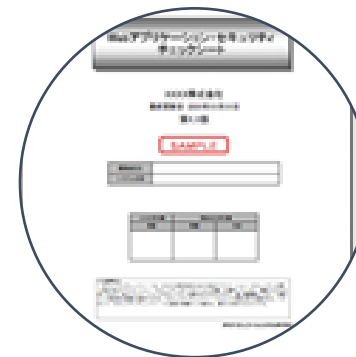
例：表示処理の留意点、SQL呼び出しの留意点...



「安全なWebアプリケーションの作り方」との整合性

「安全なWebアプリケーションの作り方」に準拠したガイドライン、チェックシートを作成いたします

「安全な...」を参照することにより、ガイドラインとチェックシートを薄く、読みやすく作成できます



ガイドラインと対になるチェックシートの提供

ガイドラインの準拠度を測るチェックシートにより、納品物の品質チェックに利用できます

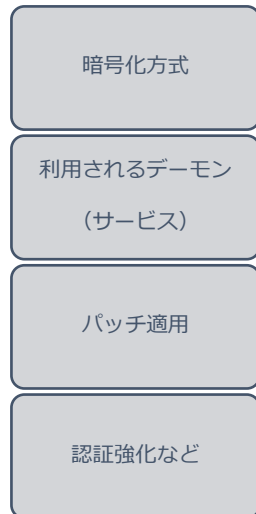
注) 自己申告なので脆弱性診断の代用になるものではありません

スコープ

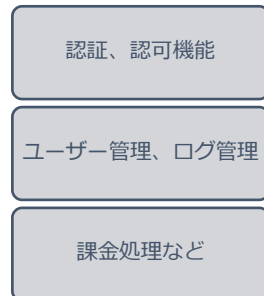
- 開発ガイドラインの適用範囲の例を示します。
- お客様の開発環境により柔軟なカスタマイズが可能です。



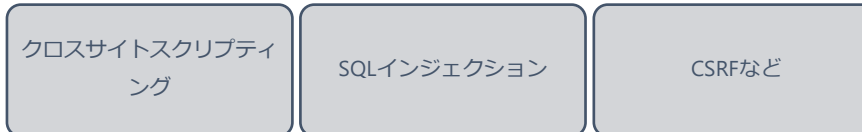
サーバーに関するガイドライン



ウェブアプリケーションのセキュリティ機能のガイドライン



ウェブアプリケーションの脆弱性対処に関するガイドライン



費用、スケジュールの例

プロジェクト名	期間	訪問回数	納品物	料金
A社 開発ガイドライン策定	2カ月	4回 1)お打合せ 2)キックオフミーティング 3)中間報告会 4)報告会	・ガイドライン ・チェックリスト	150万円～
B社 開発ガイドライン見直し	2カ月	4回 1)お打合せ 2)ガイドラインの精査 チェックリストの精査 3)ガイドライン適用状況の調査 4)報告会	・レビュー報告書	80万円～
C社 協力会社開発ガイドライン策定	3カ月	4回 1)お打合せ 2)開発依頼状況のヒアリング 3)報告会 4)開発会社説明会	・ガイドライン ・チェックリスト ・検査基準書	200万円～

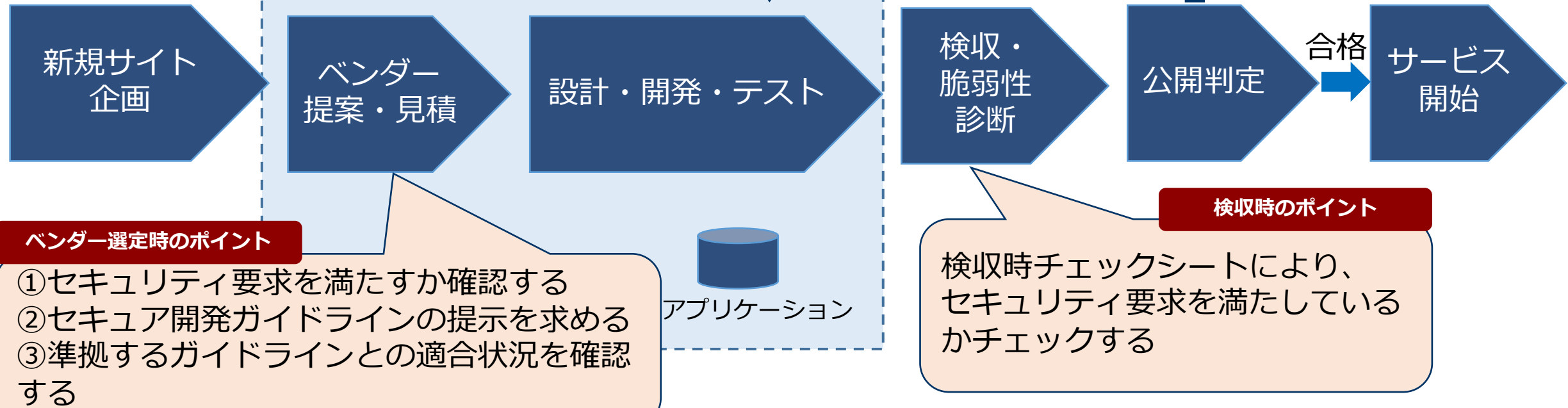
※費用はお打合せの回数やカスタマイズ内容、開発言語等により変わります。

参考：セキュアなシステム開発プロセス

企画時のポイント

- ① サービスレベルの脅威分析の結果をもとにセキュリティ要求を決める
- ② 準拠するガイドラインを決める
- ③ ①②をもとに、検収時チェックシートを作成する

ベンダー側作業



参考：リスクアセスメント方法

(1) ベースラインアプローチ

既存の標準や基準をもとにベースライン（自組織の対策基準）を策定し、チェックしていく方法。簡単にできる方法であるが、選択する標準や基準によっては求める対策のレベルが高すぎたり、低すぎたりする場合がある

(2) 非形式的アプローチ

コンサルタント又は組織や担当者の経験、判断によりリスクアセスメントを行う。
短時間に実施することが可能であるが、属人的な判断に偏る恐れがある。

(3) 詳細リスク分析

詳細なリスクアセスメントを実施。情報資産に対し「資産価値」「脅威」「脆弱性」「セキュリティ要件」を識別し、リスクを評価していく。

厳密なリスク評価が行えるものの多大な工数や費用がかかる

(4) 組合せアプローチ

複数のアプローチの併用。よく用いられるのは、(1)ベースラインアプローチと(3)詳細リスク分析の組合せ。ベースラインアプローチと詳細リスク分析の両方のメリットが享受できる。

IPA 「情報セキュリティマネジメントとPDCAサイクル」より引用
https://www.ipa.go.jp/security/manager/protect/pdca/risk_ass.html

会社概要

名 称	EGセキュアソリューションズ株式会社
本 社	〒105-0001 東京都港区虎ノ門1-2-8 虎ノ門琴平タワー 8F
設 立	2008年4月2日
代 表	齊藤 和男
株 主	イー・ガーディアン株式会社 (東証プライム/証券コード：6050) 100%
事業内容	1. 情報セキュリティ、情報システムに関する監査、コンサルティング 2. 情報セキュリティに関する調査、研究、執筆 3. 情報セキュリティ関連の教育及びコンテンツ制作 4. セキュリティ製品の開発、販売、サポート



IS575950 / ISO27001:2013

情報セキュリティサービス基準適合（脆弱性診断）

2020年9月23日登録

<https://www.ipa.go.jp/files/000067318.pdf>



020-0012-20

取締役CTOプロフィール

徳丸 浩（とくまる ひろし）



略 歴

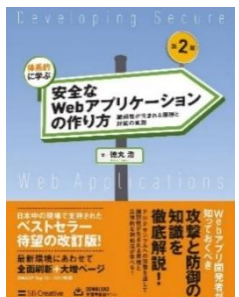
1985年京セラ株式会社に入社後、ソフトウェアの開発、企画に従事。1999年に携帯電話向け認証課金基盤の方式設計を担当したことをきっかけにWebアプリケーションのセキュリティに興味を持つ。2004年同分野を事業化。

2008年独立、Webアプリケーションセキュリティを専門分野とするHASHコンサルティング株式会社（現EGセキュアソリューションズ株式会社）を設立。

2015年イー・ガーディアングループに参画。2019年よりイー・ガーディアン子会社のグレスアベイル株式会社取締役を兼任。2021年取締役CTO就任。

京セラコミュニケーションシステム株式会社技術顧問
独立行政法人情報処理推進機構（IPA）非常勤研究員
技術士（情報工学部門）

著 書



実 績 等

相次ぎ発生する預貯金の不正引き出しについて、テレビ東京ワールドビジネスサテライト等メディアでの解説や東洋経済、産経新聞他、ITmedia等IT系メディアの取材実績多数。
その他、セキュリティイベントでの基調講演やゲスト講演も多数。

著書『体系的に学ぶ 安全なWebアプリケーションの作り方 第2版』を教材、出題範囲とする民間試験「ウェブ・セキュリティ基礎試験」（徳丸基礎試験）が2019年より開始。

本サービスに関するお問合せ・お見積のご依頼

- 公式サイト <https://www.eg-secure.co.jp/contact/>
- メール contact@eg-secure.co.jp
- 電話 **03-6257-3927** (9:00～18:00/月～金)