ekino.

セキュアSDLCチェックリスト

設計からデプロイメントまでのセキュリティレビューのフレームワーク

対象： CTO、エンジニアリングマネジャー、セキュリティ担当者

目標： セキュリティコントロールがSDLC全体に組み込まれるのを確認

フェーズ1：設計・計画

- [ ] **新機能・製品の脅威モデリングを完了**

  開発の前に潜在的な衝撃ベクター、信頼境界、センシティブデータフロー、そして不正使用のシナリオを特定する

- [ ] **潜在的な衝撃ベクターを記録**

  衝撃者によってAPI、UI、外部のインテグレーション、または特権アクセスポイントをどのように悪用する可能性があるかを文書化する

- [ ] **信頼境界を特定**

  セキュリティ暴露を把握するため、システム、サービス、ユーザ、そして外部の間におけるデータ移動を明確にする

- [ ] **セキュリティリスクを優先、オーナーに割り当てられ**

  重大度によってリスクを区別し、各リスクに対して低減を担当する責任者を明確に割り当てる

- [ ] **許可された開発ツールを定め**

  企業のセキュリティ要件に沿っている承認された開発、CI/CD、AI、コラボレーションのツールのリストを管理・維持する

ekino.

セキュアSDLCチェックリスト

設計からデプロイメントまでのセキュリティレビューのフレームワーク

対象： CTO、エンジニアリングマネジャー、セキュリティ担当者

目標： セキュリティコントロールがSDLC全体に組み込まれるのを確認

- [ ] **AIコーディングアシスタントを評価・承認**

  採用する前に、データプライバシー、コードの所有権、コンプライアンス、そしてセキュリティリスクをレビューする

- [ ] **データプライバシーの要件を文書化**

  センシティブデータ、顧客データ、規制対象データの収集、保存、処理、保持の方法を定義する

- [ ] **認証の要件を明確化**

  SSO、MFA、OAuth、またはパスワード基準といった認証メカニズムを**規定**する

- [ ] **認可要件を文書化**

  ユーザロール、アクセス権、特権境界を明確にする

- [ ] **暗号化の要件を特定**

  転送中データおよび静止中のデータの承認された暗号化方法を定める

ekino.

セキュアSDLCチェックリスト

設計からデプロイメントまでのセキュリティレビューのフレームワーク

対象： CTO、エンジニアリングマネジャー、セキュリティ担当者

目標： セキュリティコントロールがSDLC全体に組み込まれるのを確認

フェーズ2：開発

- [ ] **セキュアコーディング標準に関する開発者をトレーニング**

  エンジニアチームにセキュアコーディング手法と一般的な脆弱性の種類が理解するのを確認する

- [ ] **OWASP Top 10をレビュー**

  チームに最も一般的なウエブアプリケーションのセキュリティリスクおよび低減戦略が理解するのを確認する

- [ ] **必須のコードレビューを実施**

  全てのコードはproductionブランチに併合する前に独立したレビューを必要とする

- [ ] **人間でAIが生成したコードをレビュー**

  エンジニアはAI支援のコードのセキュリティ上の問題、論理エラー、コンプライアンスリスクをレビューしていることを確認する

- [ ] **CIパイプラインにSCAツールを統合**

  外部の依存関係に既存の脆弱性を自動的にスキャンする

ekino.

セキュアSDLCチェックリスト

設計からデプロイメントまでのセキュリティレビューのフレームワーク

対象： CTO、エンジニアリングマネジャー、セキュリティ担当者

目標： セキュリティコントロールがSDLC全体に組み込まれるのを確認

☐ 弱い依存関係を監視

ソフトウェアの依存関係に影響するセキュリティアップデートと脆弱性の開示を継続的に監視する

☐ 重要な依存関係のアップデートを優先

高リスクのライブラリとフレームワークをアップデートするSLAを定義する

ekino.

セキュアSDLCチェックリスト

設計からデプロイメントまでのセキュリティレビューのフレームワーク

対象： CTO、エンジニアリングマネジャー、セキュリティ担当者

目標： セキュリティコントロールがSDLC全体に組み込まれるのを確認

フェーズ3：テスト・検証

- [ ] **CIパイプラインにSASTを統合**

  デプロイメントの前にソースコードを自動的に分析し、脆弱性を発見する

- [ ] **テスト環境にDASTを実装**

  稼働中のアプリケーションに対する悪用可能な脆弱性を継続的にテストする

- [ ] **リリースプロセスにセキュリティスキャンを含め**

  セキュリティ検証は必須のリリース要件とする

- [ ] **高重大度の脆弱性によるデプロイメントを禁止**

  重要な脆弱性を修正しなかった場合、製品リリースを停止する

- [ ] **重要なシステムに対する侵入テストを完了**

  高リスクのアプリケーションとサービスに対して実際の衝撃をシミュレートする

- [ ] **認証メカニズムをテスト**

  ログインフロー、MFAコントロール、セッション管理、パスワードポリシーを確認する

ekino.

セキュアSDLCチェックリスト

設計からデプロイメントまでのセキュリティレビューのフレームワーク

対象： CTO、エンジニアリングマネジャー、セキュリティ担当者

目標： セキュリティコントロールがSDLC全体に組み込まれるのを確認

☐ 認可ロジックを確認

ユーザは承認された許可かぎりのリソースと行動しかアクセスできないのを確認する

☐ セキュリティ承認を取得

リリースの前にセキュリティの関係者により正式な承認を必要とする

ekino.

セキュアSDLCチェックリスト

設計からデプロイメントまでのセキュリティレビューのフレームワーク

対象： CTO、エンジニアリングマネジャー、セキュリティ担当者

目標： セキュリティコントロールがSDLC全体に組み込まれるのを確認

フェーズ4：デプロイメント・運用

- [ ] **パイプラインのアクセスを限定**

  最小権限の原則に基づき、認可された担当者へのCI/CDパイプラインのアクセスを制限する

- [ ] **秘密を安全に管理**

  承認されたシークレット管理プラットフォームに資格情報、鍵、トークンを保管する

- [ ] **構築アーティファクトを確認**

  デプロイパッケージの整合性、信頼性、トレーサビリティを検証する

- [ ] **プロダクションアクセスに対するMFAを実施**

  本番システムへのすべての特権アクセスに対してMFAを必要とする

- [ ] **最小特権モデルを実現**

  業務機能の実行に必要な最小限の権限のみを付与する

ekino.

セキュアSDLCチェックリスト

設計からデプロイメントまでのセキュリティレビューのフレームワーク

対象： CTO、エンジニアリングマネジャー、セキュリティ担当者

目標： セキュリティコントロールがSDLC全体に組み込まれるのを確認

- [ ] **インフラ強化を完了**

  不要なサービスを無効にし、未使用のポートを閉じ、安全な構成を適用する

- [ ] **セキュリティロギングを有効化**

  アプリケーション、インフラストラクチャ、アイデンティティシステム全体でセキュリティ関連のイベントを収集する

- [ ] **重要なイベントを監視**

  不審なアクティビティとセキュリティインシデントに対するアラートと監視体制を確立する

- [ ] **インシデント対応連絡を記録**

  最新のエスカレーションパスとインシデント対応の責任体制を維持する

ekino.

セキュアSDLCチェックリスト

設計からデプロイメントまでのセキュリティレビューのフレームワーク

対象： CTO、エンジニアリングマネジャー、セキュリティ担当者

目標： セキュリティコントロールがSDLC全体に組み込まれるのを確認

リリース前の最終検証

- [ ] **重大な脆弱性が残存しない**

  すべての重大な発見が修正、あるいはリスクガバナンスを通じて正式に受容されたことを確認する

- [ ] **セキュリティレビューを完了**

  アーキテクチャ、コード、インフラストラクチャ、構成の最終的なセキュリティ評価を実施する

- [ ] **ペネトレーションテストを承認**

  結果がレビューされ、修正活動が完了したことを確認する

- [ ] **監視が稼働中**

  ログ、アラート、ダッシュボード、そして対応ワークフローが正しく機能していることを確認する

- [ ] **ロールバック計画を文書化**

  運用上またはセキュリティ上の問題が発生した場合、リリースを安全に元に戻す方法を定義する

- [ ] **ビジネスオーナーの承認を取得**

  ビジネスのステークホルダーが、運用上のリスクおよび残存セキュリティリスクを受容することを確認する

- [ ] **セキュリティオーナーの承認を取得**

ekino.

セキュアSDLCチェックリスト

設計からデプロイメントまでのセキュリティレビューのフレームワーク

対象： CTO、エンジニアリングマネジャー、セキュリティ担当者

目標： セキュリティコントロールがSDLC全体に組み込まれるのを確認

迅速評価

Scoring

Status	点
完了	1
未了	0

合計点： ___ / 48

結果	セキュリティの準備
0 - 24	高リスク
25 - 36	基盤
37 - 44	管理
45 - 48	成熟