
【勉強会】 バイブコーディングの落とし穴

AI開発に潜むセキュリティリスクと今日からできる対策

2026年9月24日(木) 18:00-19:00

ハクビー株式会社

代表取締役 松永赳堯



目次

1. 自己紹介
2. システム開発のプロセス
3. 開発時における情報流出
4. 運用後のシステムにおける被害
5. 万が一、事故が起きたらどうなるか
6. 次回告知



1. 自己紹介

2. システム開発のプロセス

3. 開発時における情報流出

4. 運用後のシステムにおける被害

5. 万が一、事故が起きたらどうなるか

6. 次回告知

自己紹介



創業者の田中と松永

会社概要

商号 ハクビー株式会社
代表者 代表取締役 松永 昶亮
設立 2026年7月
事業内容 Webアプリの受託開発／情報セキュリティ
登記住所 静岡県浜松市中央区鍛冶町100番地の1
 ザザシティ浜松中央館 B1F
事務所 静岡県浜松市中央区舞阪町舞阪2701-9
 浜松市舞阪支所4階

自己紹介

大手ネットワーク機器メーカーでソフトウェアエンジニアとして、大規模なWebアプリケーション開発を経験後に独立。修士（工学）。犬が好き。



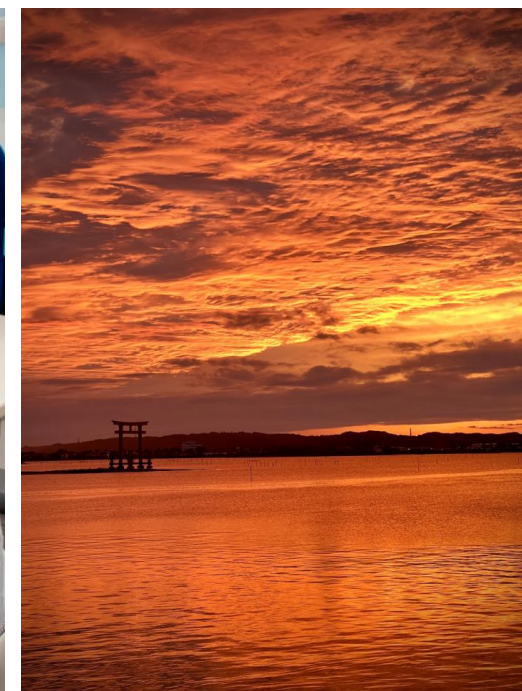
自己紹介



眺めがいいオフィス
(浜松市さまに感謝！)



オフィスのネットワークをつくる松永

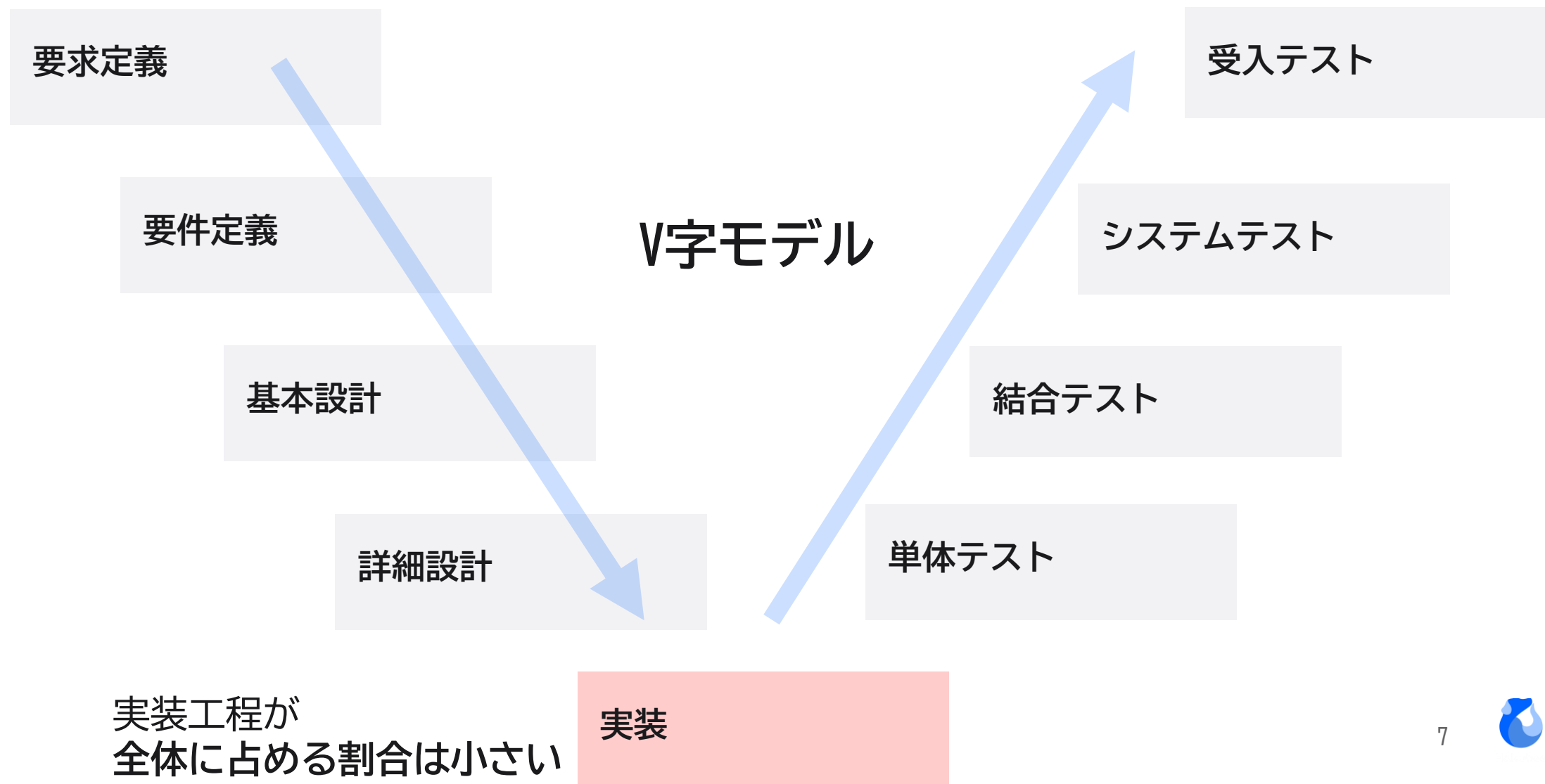


弁天島の夕焼け



1. 自己紹介
2. システム開発のプロセス
3. 開発時における情報流出
4. 運用後のシステムにおける被害
5. 万が一、事故が起きたらどうなるか
6. 次回告知

システムの開発プロセス



システムの開発プロセス



1. 自己紹介
2. システム開発のプロセス
3. 開発時における情報流出
4. 運用後のシステムにおける被害
5. 万が一、事故が起きたらどうなるか
6. 次回告知

設計時における情報流出

組織の外に漏らしてはいけない秘密をAIに入力してしまう

例

1. 企画段階で取得した個人情報
2. パートナー企業の秘密



設計時における情報流出

組織の外に漏らしてはいけない秘密をAIに入力してしまう

原因

1. AIが入力された情報をもとに検索エンジンを実行する
2. 検索エンジンにはログが残る

結果

1. 検索エンジンの運営者に情報が漏出する

被害

1. 検索エンジンの運営者が収集した情報を利用して、AIを学習させる



設計時における情報流出

組織の外に漏らしてはいけない秘密をAIに入力してしまう

対策

1. AIが検索エンジンを利用するときには、**ユーザーに確認を取る**ことを強制する

実例：Claude の チームプランを活用する → 個人の力量に頼らず、**組織で対策**する

組織の指示

これらのClaudeへの指示は、組織全体のすべての会話に適用され、ユーザーの個人設定よりも優先されます。コンプライアンスルール、データ処理、またはフォーマット標準の設定に適しています。変更が反映されるまで最大1時間かかる場合があります。

Web検索をするときに、顧客の情報を扱うときは固有名詞を一般化してください。例えば、顧客名、顧客の担当者名は検索ワードに含めないでください。また、Web検索をするときは、どのようなワードで検索するかを事前にユーザーに確認を求めてください。

実装時における情報流出

組織の外に漏らしてはいけない秘密をAIに入力してしまう

原因

1. AIがAPIキーを取得する
2. AIがAPIキーをコードに埋め込む
3. リポジトリマネージャー（例 GitHub）にAPIキーがコード一緒にpushされる

結果

1. リポジトリマネージャーにアクセスできる人やマシンにAPIキーが漏出する

被害

1. **APIキーが意図せず利用される** -> 金銭的な被害、秘匿したい情報の漏洩

用語

- API（Application Programming Interface）：アプリケーションが情報を取得するために利用する窓口
- リポジトリマネージャー：コードを保存するリポジトリを管理するサービス



開発時における情報流出

組織の外に漏らしてはいけない秘密をAIに入力してしまう

対策

1. AIにはクレデンシャルを渡さない、閲覧させない

```
{
  (省略)
  "permissions": {
    "allow": [],
    "deny": [
      "Read(**/.env)",
      "Read(**/.env.*)",
      "Read(**/secrets/**)",
      "Read(**/.ssh/**)",
      "Read(**/.aws/**)",
      "Read(**/config/credentials.json)",
      "Read(**/*.pem)",
      "Read(**/*.key)"
    ],
    "disableBypassPermissionsMode": "disable"
  },
  (省略)
}
```

実例：Claude Code が読み込むことができるファイルの範囲を制限する

Claude Code

管理された設定

組織全体の権限や許可ディレクトリなどを設定します。これはユーザーおよびプロジェクトの設定を上書きし、CLI、IDE、デスクトップアプリのClaude Codeに適用されます。 [詳細を見る](#)

管理



1. 自己紹介
2. システム開発のプロセス
3. 開発時における情報流出
4. 運用後のシステムにおける被害
5. 万が一、事故が起きたらどうなるか
6. 次回告知

人間が招いた設計の不備（仕様バグ）による情報流出

マッチングアプリにおける個人情報の漏洩

原因

1. データベースのアクセス制御に不備があった
-> 誰がどのデータにアクセスすべき/すべきでないか（認証・認可）の設計が甘かった

結果

1. ログインしなくても個人情報が閲覧できた

被害

1. メールアドレス、表示名、性別、年齢、大学／高校名、プロフィール画像が漏洩した

対策

1. 設計する力を身に着ける。AI任せにせずに、データベースの仕様を理解する。

ソフトウェアの脆弱性を利用した攻撃

サーバーが乗っ取られ、暗号通貨を採掘される

原因

1. アプリのフロントエンドを構成するためのモジュールに重大な脆弱性があった
-> 任意のコマンドが実行できる脆弱性（CVE-2025-55182 通称React2Shell）だった

結果

1. 攻撃者が暗号通貨を採掘するソフトウェアが実行され、CPUが利用された

被害

1. 電気代が増加した
-> ただし、他に悪影響がないかはログを確認する必要がある

対策

1. ソフトウェア部品表(SBOM)をつくり、日々脆弱性の報告を確認する

AIによるリスクの受容の強制

AIの作業を検証できないと、AIが持ち込んだリスクの受容を強制される

対策

1. 実装の効率が良くなった分、テストを強化してAIの作業を検証する



1. 自己紹介
2. システム開発のプロセス
3. 開発時における情報流出
4. 運用後のシステムにおける被害
5. 万が一、事故が起きたらどうなるか
6. 次回告知

経営者の責任が大きい

サイバー攻撃は防げない -> 天災と同じと考える

必要な対策をしていなかったことについて経営責任を問われる

事例

Webサイト改ざんによるフィッシング誘導 -> 顧客のクレカ情報が漏洩

- 金融・保険業
- 売上約4億円
- 従業員数50名、端末台数60台
- 営業担当が情シスを兼任
- 被害前に実施していた対策
 - ウィルス対策ソフト・UTMを導入
 - インシデント対応計画、データのバックアップ
 - セキュリティ予算の確保（売上比約0.375%、約150万円）

内容	金額（万円）
初期対応費用	約200
報告公表費用	約20
弁護士訴訟費用	約100
再発防止費用	約100
利益被害（一部顧客との取引停止）	約2,000

想定被害額 約2,420万円

20

（独）情報処理推進機構『中小企業のための実例で学ぶサイバーセキュリティリスク事例集』をもとに事例を作成

経営者が責任を果たした事例



説明する

補償する

資金が必要

サイバー保険に加入しておく



サイバー保険のすすめ

商工会議所会員向け 保険制度

[保険リスト](#)[お問合せ先（保険窓口検索）](#)[加入のメリット](#)[よくあるご質問](#)

商工会議所会員でない企業様はこちらをご覧ください

[会員になるには](#)

[HOME](#) > サイバー保険制度



サイバー保険制度

事業者のサイバーリスクに備える



1. 自己紹介
2. システム開発のプロセス
3. 開発時における情報流出
4. 運用後のシステムにおける被害
5. 万が一、事故が起きたらどうなるか
6. 次回告知

次回告知

経営者のための「5分でできる！情報セキュリティ自社診断」ライブ放送！

内容

1. 「5分でできる！情報セキュリティ自社診断」とは何か
2. (独) 情報処理推進機構が推進する「セキュリティ対策自己宣言」のご紹介
3. ハクビーが前回の自己診断からどれだけ改善したのかを確認

オンラインセミナー — 主催 ハクビー株式会社

経営者のための

「5分でできる！ 情報セキュリティ 自社診断」

ライブ放送！

25項目をその場で採点 自社の点数を全公開 SECURITY ACTION

こんな方へ 対策の必要性は感じているが、何から手をつければいいかわからない経営者の方

開催日時 10月15日 (木) 18:00-19:15 形式 Microsoft Teams

—— セキュリティ企業が、自社の弱点を点数ごと包み隠さず公開します

講師
松永 起亮
ハクビー株式会社
代表取締役

大手ネットワーク機器メーカーでソフトウェアエンジニアとして、大規模なWebアプリケーション開発を経験後に独立。現在はアプリ受託開発と情報セキュリティコンサルティングを手がける。修士 (工学)。

経営者のための「5分でできる！情報セキュリティ自社診断」ライブ放送！ - connpass 24





Hakubee