生成AIとAIエージェントによるセキュリティ業務自動化について

株式会社エネコム
ITインテグレーション部　濱本　常義

2025.10.24

Copyright © enecom, Inc.

株式会社エネコム
情報システム事業本部　ITインテグレーション部　マネージャー
濱本常義

同社３０年勤務、５年間は研究開発部門に所属、社内LAN構築、社内ネットワークポリシー策定、CATVインターネット実験参加、社内セキュリティ監査業務に携わる。２０００年より、セキュリティ監査（ペネトレーションテスト含む）およびセキュリティコンサルティングなどの業務に従事、現在は上記に加えて標的型メール訓練、ログ監視、CSIRT運用業務に携わる

情報セキュリティポリシー策定、ポリシー教育実績
大手公共企業、大手メーカ、情報システムサービス会社、自治体
LASDEC 高度情報セキュリティ研修講師（2004年広島県、山口県、2005年愛媛県、2006年広島県、2007年広島、高松、鳥取）
経済産業省　学生22歳以下向けイベント、セキュリティキャンプ関係講師（2003～2025）
情報処理安全確保支援士向け講習会 講師（2017年～）
マイクロソフトから多数の人に影響をあたえられる個人に与える賞 MVP(Most Valuable Professional)をWindows-Securityの分野で12回受賞(2003～2014)

Copyright © enecom, Inc.

注意事項

　本講演は、新聞報道など公知の事実から事件を類推し、その対策を提言するものであるため、実際の事実関係とは異なる場合があります

　個人・組織のセキュリティ対策を多角的に検討する参考になれば幸いです

Copyright © enecom, Inc.

本日のアジェンダ

1. イントロダクション - "AI時代"のCSIRTに求められる変革
2. 事例に学ぶ【A Gr HD事案Qilinランサムウェアの脅威など】
3. CSIRT業務の生成AI活用事例 - 「AIエージェント」以前の即効性
4. AIエージェントによるCSIRT業務自動化 - Level 1 & 2
5. CSIRTの新たな選択肢 - AIエージェントで「自作する」Vibe Coding
6. "チャット開発"の限界を超える - AIオーケストレーション
7. 未来の働き方 - AI駆動開発(AI-DD)とセキュリティ担当者の進化
8. 乗り越えるべき課題 - AI駆動開発とVibe Codingの現実
9. まとめとQ&A

Copyright © enecom, Inc.

01

1. イントロダクション - "AI時代"のCSIRTに求められる変革

Copyright © enecom, Inc.

CSIRT業務の「理想」と「現実」

なぜ私たちはAIによる変革を目指すのか

理想
プロアクティブな脅威ハンティングと**インテリジェンス主導の防御**体制の確立

現実
終わらないアラート対応、増え続けるログの分析、そして巧妙化する攻撃への**後手後手の対応**

本講演のゴール
AIを「飛び道具」ではなく、業務に組み込まれた**信頼できる同僚**として活用する未来像を共有する

Copyright © enecom, Inc.

セキュリティ業務の進化段階

私たちは今、どのフェーズにいるのか

1. Phase 1: **手動運用** (属人化と疲弊)
2. Phase 2: **SOARによる自動化** (決められたことしかできない)
3. Phase 3: **生成AIによる効率化** (レポート作成、要約など「点」の支援)
4. Phase 4: **AIエージェントによる自律化** (調査・分析など「線」の自動化) ← **イマココ**
5. Phase 5: **AI駆動開発による業務再構築** (業務プロセス自体をAIと協創) ← **未来**

Copyright © enecom, Inc.

02

2. 事例に学ぶ対策案

Copyright © enecom, Inc.

2024年 インシデント事例（月別）

月	組織名	攻撃種別	被害内容
1月	北海道大学病院	パスワードリスト攻撃	不正アクセス被害。フィッシングメール3万件送付
2月	株式会社イズミ（ゆめタウン）	ランサムウェア	VPN機器経由で攻撃、全ネットワーク遮断、基幹システム停止、復旧に約3ヶ月、決算報告延期。特別損失前期10億円
2月	岡山県精神科医療センター	ランサムウェア	VPN機器経由で攻撃、仮想基盤、仮想用共有ストレージ、各サーバ、端末被害
2月	公益財団法人・埼玉県健康づくり事業団	ランサムウェア	X線画像読影システム停止、復旧に半年以上
3月	株式会社ほくやく・竹山ホールディングス	ランサムウェア	SIMカード付きのノートパソコンにRDP経由で感染。
4月	株式会社マリンネット	SQLインジェクション	Webサイトの脆弱性を突いた攻撃
5月	JR東日本	サイバー攻撃	モバイルSuica、えきねっとなどの交通系決済システム障害、約3時間で復旧
5月	積水ハウス	SQLインジェクション	会員サイト「Net オーナーズクラブ」から約57万人分の個人情報漏洩、運用終了10年以上の旧ページが攻撃経路
5月	株式会社イセトー	ランサムウェア	納税通知書作成業務委託先への攻撃、多数の自治体・金融機関への二次被害
6月	KADOKAWA（ニコニコ動画）	ランサムウェア（BlackSuit）	ニコニコ動画含む全サービス停止、出版物流システムも停止、復旧に1ヶ月以上、株価下落、約25万名の情報流出。特別損失36億円（後に23億円に修正）
6月	大手保険会社の業務委託先	ランサムウェア	約6万件の顧客情報漏洩の恐れ
7月	東京ガスエンジニアリングソリューションズ	不正アクセス	VPN機器を介して不正アクセス。取引先法人情報も漏洩二次被害が発生
12月	日本航空（JAL）	DDoS攻撃	手荷物預かりシステム障害、国内線60便・国際線11便で遅延（最大4時間超）、約4時間で復旧

Copyright © enecom, Inc.

2025年上期 インシデント事例（月別）

月	組織名	攻撃種別	被害内容
1月	複数の銀行	DDoS攻撃	年末年始にかけて複数の銀行が標的に
2月	株式会社保険見直し本舗	ランサムウェア	約170万件の情報漏洩の可能性、グループ会社への二次被害約130万件
2月	医療法人 DIC 宇都宮セントラルクリニック	ランサムウェア	約30万件の情報漏洩の可能性、健康保険組合への二次被害
4月	株式会社インターネットイニシアティブ	不正アクセス	メールサービスへの不正アクセス、当初20社が二次被害の可能性（後に15社は被害なしと判明）
4月	学校法人東海大学	ランサムウェア	パスワードリスト攻撃から不正侵入後にランサム攻撃
4月	オリオンシステム株式会社	ランサムウェア	情報サービス企業への攻撃
4月	エネクラウド株式会社	ランサム攻撃（新型）	データ暗号化ではなくファイル削除型の攻撃、Amazon S3のアクセスキー不正使用
4月～6月	複数の製造業への攻撃	ランサムウェア	製造業へのサプライチェーン攻撃
4月～5月	複数の運輸業への攻撃	ランサムウェア	運輸業へのサプライチェーン攻撃
5月	株式会社PR TIMES	不正アクセス	プレスリリース配信サービスへの攻撃、90万件以上の個人情報と1,182社分の未発表情報が漏洩、複数企業への二次被害
5月	株式会社ホスピタルサービス	ランサムウェア	卸・小売業への攻撃。不正アクセス後にランサム被害
5月	株式会社Core-S	ランサムウェア	福祉・介護業への攻撃。不正アクセス後にランサム被害
6月	株式会社はるやまホールディングス	ランサムウェア	製造業（アパレル）への攻撃。不正アクセス後にランサム被害
6月	損害保険ジャパン株式会社	不正アクセス	約1750万件以上の情報漏洩の可能性

Copyright © enecom, Inc.

アサヒ Gr HD事案の衝撃

- 2025年9月、アサヒグループがランサムウェア「Qilin」の攻撃を受け、**受注・出荷システムが停止**
- これは単なるデータ暗号化ではなく、企業の基幹業務（ビジネスプロセス）そのものが標的とされた事件
- Qilinは、企業の**“心臓部”**である仮想基盤（ESXi, Nutanix）を直接狙う機能を保有（他事例）
- 一撃でビジネスの心臓部を停止させることが可能な、極めて危険な脅威

Copyright © enecom, Inc.

Qilinの巧妙な手口

CSIRTの"目・手・足"を奪う攻撃

復旧させない	検知させない
攻撃者は、復旧の手がかりとなるシャドウコピー（バックアップ）や**システムログを徹底的に削除**する	EDRなどのセキュリティ製品の検知を回避するため、**セーフモードで再起動**するなどの巧妙な手口を使う

Copyright © enecom, Inc.

Qilinの特徴：脅迫の"ビジネスモデル化"

- Qilinは「RaaS（Ransomware as a Service）」と呼ばれるサービス形態で提供
- 2025年4月からは、なんと**「法律の専門家に相談するサービス」**を提供開始
- 「弁護士が交渉を代行」し、被害企業が被る**訴訟リスクや評判低下**といった法的損害を評価
- これに基づき身代金支払いを迫る、極めて高度なビジネス戦術

Copyright © enecom, Inc.

03

3. CSIRT業務の生成AI活用事例

Copyright © enecom, Inc.

生成AI活用事例 (1/2)

ChatGPT/Gemini単体で実現できる工数削減

事例1：バイナリログの高速解析 (EDR対応)

ChatGPTなら**512MBのバイナリログを直接アップロードして解析可能**。AIが内部でStringsコマンドのように内容を調査し、インシデント概要や不審な挙動のタイムラインをレポート

(注) 情報漏洩の懸念があるので、本来、直接UPはNG、正式運用はOpenAI GPT-OSSなどを使ったローカル運用必須

事例2：ASM（Attack Surface Management）の簡易レポート生成

owasp amassやnslookupの結果をAIに**雑に**与えるだけで、AIが情報を整理・分類し、簡易的なASMレポート（公開資産の洗い出し）を生成可能。

(注)プロンプトを工夫しないとASMレポートのクオリティに揺らぎが発生

Copyright © enecom, Inc.

生成AI活用事例 (2/2)

日々のルーチンワークをAIで効率化

事例3：インシデント対応手順書の即時作成

VPN脆弱性（Ivanti等）発生時、AIに最新情報を調査させ、具体的な**Ivantiフォレンジック対応手順書**を作成。**内部ADへの横展開(Lateral Movement)調査**なども含めて作成可能

事例4：日次セキュリティニュースの収集と配信

RPAやn8nで自動収集した記事群をAIでサマリー化。最後は**人間がファクトチェックと編集**を行い、グループ企業全体に配信

Copyright © enecom, Inc.

04

4. AIエージェントによるCSIRT業務自動化 - Level 1 & 2

Copyright © enecom, Inc.

Level 1 & 2で活躍するツール

- **Difyとは？ (頭脳)**
- AIアプリケーション（頭脳）の構築ツール
- ノーコードで構築可能
- 社内マニュアルや過去のインシデント報告書を独自データ（RAG）として学習させ、**「CSIRT専用AIアシスタント」**を簡単に作れる

- **n8nとは？ (神経網)**
- ワークフロー（神経網）の自動化ツール
- 数百種類のツール（メール, Slack, VirusTotal等）をビジュアル的に連携
- メール受信やEDRアラートを**「トリガー」**として調査プロセスを起動できる

Copyright © enecom, Inc.

Difyとn8n：特徴と向き不向き

AIの「頭脳」と「神経網」をどう使い分けるか

項目	Dify	n8n
役割	AIアプリケーションの構築（頭脳）	ワークフローの自動化（神経網）
強み	・独自データ（RAG）の活用 ・対話型AIの簡単な作成	・豊富な連携先（数百種類） ・直感的なビジュアル連携
用途	**インテリジェンスが求められるタスク** （分析、報告書ドラフト、ナレッジ検索）	**プロセス連携が求められるタスク** （トリガー、API実行、ファイル操作、通知）

Copyright © enecom, Inc.

Level 1: ノーコード/ローコードで始める即効性のある自動化

- まずは、日々の運用で発生する「単純だが時間のかかる作業」を自動化
- ノーコード/ローコードで実現できるため、開発スキルがなくても着手可能
- **「小さな成功体験」**を積むことが、組織的なAI活用推進の鍵

Copyright © enecom, Inc.

Level 1: 実装案

n8n と OpenAI API で実現する自動化フロー

実装案1：不審メールの一次トリアージ	実装案2：EDRアラートの調査・レポート化	実装案3：Webサイトの簡易動的解析
[メール受信] → [n8n] (ヘッダー/本文抽出) → [OpenAI API] (危険度判定) → [n8n] (Slack, Sheetsへ記載)	[EDRアラート] → [n8n] (IoC抽出) → [VirusTotal API] (IoC調査) → [OpenAI API] (総合評価)→ [n8n] (Slackへ通知)	[TamasでURL依頼] → [n8n] (トリガー) → [外部Web診断サイト連携] (API実行) → [n8n] (結果を依頼者へ通知)→ [Teamsで受信]

Copyright © enecom, Inc.

Level 2: 専門的な調査・分析業務の高度な自動化

- Level 1の自動化に、より専門的なツールやAIの「判断力」を組み合わせる
- フィッシングサイトの詳細な挙動調査や、独自のASMツールの開発・運用
- Qilin事案のような**高度な脅威に対抗**するための自動化

Copyright © enecom, Inc.

Level 2: 実装案 (1/2)

高度な解析と自作ツールの開発

実装案1：Webサイトの本格的な動的解析

Codexとchrome-devtools-mcpを組み合わせ、サンドボックス環境でのブラウザ操作をAIに代行させ、**フィッシングサイト等の詳細な挙動**を安全に調査

実装案2：自作ASMツールの開発・運用

Claude Codeの強力な開発能力を活かし、Owasp Amass, nmap, Nessus等を統合管理する**独自の運用ツールを自作**する

Copyright © enecom, Inc.

Level 2: 実装案 (2/2)

フォレンジックとPC操作の自律化

実装案3：AIによるデジタルフォレンジック解析

Qilinによってログが消去された端末を想定し、Kali Linux上からマウント、Claude Codeを動作させ、**残された断片的なログから攻撃の全体像をAIが再構築**する試み

実装案4：究極の自動化：PC操作そのものを代行

「EDRアラートに基づき、端末をネットワーク隔離し、**フォレンジックツールを実行せよ**」といった人間の一連のPC操作を代行（スクリプト、RPA、 Google Gemini 2.5 Computer Use等）

Copyright © enecom, Inc.

（参考）Difyの真価はRAGとの組み合わせにあり

手法	要点	主な用途	Difyでの実現方法
1. Simple RAG	もっとも基本的なRAG構成。固定データベースから関連文書を検索して生成	FAQ・製品サポートなど定型的質問応答	ナレッジ機能 ＋ チャットボット
2. Simple RAG with Memory	過去の対話や履歴を保持し、継続的な文脈を扱う	カスタマーサポート、個別推薦	チャットボット（標準機能）
3. Branched RAG	複数のデータソースから、質問に最も適したソースだけを動的に選択	専門領域別情報検索（法務・医療等）	ワークフロー（LLM分類 ＋ IF/ELSE分岐）
4. HyDe (Hypothetical Document Embedding)	「理想的な回答文書」を仮想生成し、それをガイドに検索を行う	研究開発や創造的コンテンツ生成	ワークフロー（LLMで仮説生成 → 検索 → LLMで最終回答）
5. Adaptive RAG	質問の難易度に応じて検索方法を切り替える柔軟型	企業検索・社内ナledge活用	ワークフロー（検索 → LLMで自己評価 → IF/ELSE分岐）
6. Corrective RAG (CRAG)	検索結果を自己評価・採点し、必要に応じて再検索。高精度志向	法務・医療・金融など高信頼性領域	ワークフロー（検索 → LLMで評価 → IF/ELSEで再検索ループ）
7. Self-RAG	生成中に自律的に追加検索を行う。情報ギャップを補完	長文生成・探索型研究	エージェント（ツールとして検索機能を定義し、プロンプトで自律的思考を促す）
8. Agentic RAG	複数エージェントを起動し、メタエージェントが調整。複雑な意思決定を実現	自動リサーチ・マルチソース集約・意思決定支援	

Copyright © enecom, Inc.

05

5. CSIRTの新たな選択肢 - AIエージェントで「自作する」Vibe Coding

Copyright © enecom, Inc.

CSIRTの"開発"ジレンマ

- CSIRT業務には「ちょっとしたツール」で劇的に効率化できる業務が山積み
- しかし現実は… 日々のインシデント対応に追われ、メンバーに**ツールを開発する時間的余裕が全くない**
- このジレンマが、CSIRTの生産性向上を阻害する大きな要因となっている

Copyright © enecom, Inc.

新たな解決策：「Vibe Coding」 (AI駆動開発)

- AIコーディングエージェント（CLIツール）の登場により、"開発"の概念が変化
- AIに自然言語で指示するだけで、コードを**生成・修正・デバッグ**してくれる開発スタイル
- これにより、「数日、数週間、数か月かかっていたツール開発」が「数十分」に短縮
- 業務多忙なCSIRTメンバーでも、**必要なツールを自作できる時代**に突入

Copyright © enecom, Inc.

CSIRTのための「AIコーディングエージェント」3選

ターミナルで使える強力なAIエージェントの比較

ツール	Codex CLI (OpenAI)	Gemini CLI (Google)	Claude Code (Anthropic)
品質 (SWE-bench)	69.1%(o3)	63.8%	**72.7% (業界トップ)**
コンテキスト	200K	**100万トークン (最大)**	200K
CSIRT的強み	シンプル・高速	Web検索・PDF/画像解析	高品質・高セキュリティ

Copyright © enecom, Inc.

【CSIRT業務別】AIエージェント使い分けガイド

Case 1: ログ抽出スクリプト

「至急、このログからIPを抽出するスクリプトが欲しい」
推奨: **Codex CLI**（シンプルで保守性の高いコードを素早く出力）

Case 2: 脆弱性レポート調査

「最新の脆弱性レポート(PDF)を読み込ませ、Web検索で関連情報を調査させたい」
推奨: **Gemini CLI**（100万トークン + マルチモーダル + Google検索）

Case 3: 自動化ツールの開発

「インシデント対応を自動化する、信頼性の高いツールを開発したい」
推奨: **Claude Code**（業界トップの品質とレビュー能力）

Copyright © enecom, Inc.

"Vibe Coding"の効率化：AIエージェント同士の「協業」

課題	解決策：AI同士の協業 (agents.md)
• Codexは「速い」が品質が不安 • Claude Codeは「高品質」だがレートリミット（使用制限）が厳しい	• 基本は**レートリミットのないCodex**で高速に開発 • 「ここぞ」という重要な局面（セキュリティレビュー等）だけ、**CodexからClaude Codeを呼び出す** • Claude Codeの使用制限を温存しつつ、両者の長所を活かせる

Copyright © enecom, Inc.

06

6. "チャット開発"の限界を超える - AIオーケストレーションと仕様駆動開発

Copyright © enecom, Inc.

第5章の課題：「AIとのチャット」の限界

- CLIツールを単体で使うと「指示 → 生成 → 人間がレビュー → 修正指示 → …」という、**"チャット開発"の往復**になりがち

- これでは、AIの能力を最大限に引き出しているとは言えない

- 人間は「タスクを実行するプレイヤー」から、「AIエージェントを指揮するプロジェクトマネージャー」へと役割を変える必要がある

Copyright © enecom, Inc.

解決策：AIオーケストレーションツール

複数のAIエージェントを管理・指揮する

解決策①：Vibe Kanban	解決策②：cc-sdd (国産・仕様駆動開発ツール)
AIエージェントによる開発を「カンバン方式」で管理・オーケストレーション。「実装が速いタスクはCodexに」、「高品質なレビューはClaude Codeに」といった**采配が可能**	AIにタスクを丸投げすると、望んだものと違う成果物が出来上がるリスクがある。国産ツールcc-sddは、「仕様書」でAIに「何を作ってほしいのか」を明確に伝え、**手戻りを防ぐ**

Copyright © enecom, Inc.

【CSIRT業務の未来図】AIオーケストレーション実践例

シナリオ: 新種のマルウェアアラート発生

PM (人間)	Orchestrator (Vibe Kanban)	Agents (AI)
[To Do] 「アラート調査」カードを作成 →	[In Progress] エージェントA (Gemini)へ指示 →	A: アラート情報(PDF)とIoCをWeb検索
	[In Progress] エージェントB (Codex)へ指示 →	B: 社内ログ検索スクリプトを生成・実行
	[Review] 人間へレビュー依頼 →	C: 調査結果に基づき、Jiraチケットと経営層向け報告書ドラフトを作成
	[Done] エージェントC (Claude)へ指示	

Copyright © enecom, Inc.

07

7. 未来の働き方 - AI駆動開発(AI-DD)とセキュリティ担当者の進化

Copyright © enecom, Inc.

Vibe CodingからAI駆動開発 (AI-DD) へ

AIと共に開発プロセス全体を進化させる

1. **Vibe Coding** (AIによるコード生成支援)
2. **AI駆動開発 (AI-DD)** (AIが開発の主体となる)
3. **仕様駆動開発 (SDD)** (「何を作るか」を人間が定義)
4. **AI-DLC** (AI-Development Life Cycle) (AIを中心とした開発サイクルの確立)

Copyright © enecom, Inc.

セキュリティ担当者の新たな役割

- 単純なオペレーションはAIエージェントが担う
- セキュリティ担当者は、そのAIエージェントを**「開発」する役割**へとシフト
- ローカルAIモデル（Ollama等）を活用し、機密情報を外部に出さずにAIを「調教」するスキルが重要に
- AIエージェントに「武器」を与える（例：Codex + mcp）発想が求められる

Copyright © enecom, Inc.

AIと共に働く上での必須リテラシー

AIの生成物を「監査」する能力

プロンプトエンジニアリング
AIに意図した通りの高品質なアウトプットを出させる技術（例：**まじん式プロンプトv3**）

AI生成物のレビュー能力
『【Python】生成AIがこのコード書いたら気をつけろ！』のような知見に基づき、AIが生成したコードに**脆弱性が含まれていないか**を厳しく監査する必要性

監査の重要性
AIが生成した防御コードや分析スクリプトが、**Qilinのような攻撃者に見破られる脆弱性**を含んでいないか、人間の専門家が監査する責任を持つ

Copyright © enecom, Inc.

【参考】MCP (Model Context Protocol) とは何か？

AIエージェントが外部ツールと対話するための「共通言語」であり「通信規約」

なぜAIエージェントにMCPが必要か？

従来のAIはチャットボックス内で閉じていたが、MCPはAIに**「手足」や「感覚器」**を与えるインターフェース (例: chrome-devtools-mcp → ブラウザ操作 / Jira連携 → チケット読解)

本講演の事例との関連

第4章のCodex + chrome-devtools-mcpや、第5章のClaude CodeのJira/GitHubネイティブ統合は、まさにこの**MCP（または類する規格）**によって支えられている

未来の展望 (Vibe Kanbanとの連携)

第6章のVibe KanbanによるオーケストレーションはMCPによって更に強力化。メタエージェントがタスクを分解し、**MCPを通じて専門エージェントに自律的に指示**を出す未来を想定

Copyright © enecom, Inc.

【参考】【究極】まじん式プロンプトv3　とは

Google GeminiとGASによるスライド自動生成Webアプリ

- **概要**: Google GeminiとGASを連携させ、Googleスライドを自動生成する**専用Webアプリ**

- **Point 1 (アクセス性)**: 無料版Geminiでも動作し**APIキー不要**。セキュリティが厳しい企業でも導入しやすいモデル

- **Point 2 (高度な自動化)**: 28種のパターン（フローチャート等）や画像挿入に対応。インシデント報告書や勉強会資料など**定型業務を劇的に高速化**

- **Point 3 (システム化)**: 「Gem」（カスタム指示）と「Webアプリ」を組合せ、**AIを中核に据えた業務自動化システム**を構築した好例

リンク　【究極】まじん式プロンプトv3｜まじん

Copyright © enecom, Inc.

08

8. 乗り越えるべき課題 - AI駆動開発とVibe Codingの現実

Copyright © enecom, Inc.

AI駆動開発の現実的な課題

1. スキルの退化と依存性の増加

AIに任せすぎることで、プログラミングの基礎力（構文、アルゴリズム、デバッグ能力）が低下する懸念

2. AIの出力に対する評価と責任

AIが生成したコードの**セキュリティ脆弱性や論理的欠陥**をレビューし、品質を確保する人間の高度な評価スキルが不可欠

3. 新たに求められるスキル（プロンプトと構想力）

AIに意図を伝える「プロンプト能力」と、ビジネス課題に対し「AIをどう活用すべきか」を構想する力が必要

4. 法的・倫理的リスクへの対応

著作権の問題や、機密情報漏洩のリスクについて、担当者が正しく理解し対応できるリテラシー教育が必須

Copyright © enecom, Inc.

課題を乗り越えるためのヒント

「プロンプト（指示）」と「レビュー（評価）」の質を高める参考資料

1. 「プロンプト能力不足」への対策

AIへの指示は「仕様書」と捉えることが重要。**Claude Codeのドキュメント実例**や、**プロンプト設計術（役割付与、具体化）**が参考になります。

【参考】【Claude Code】マネできる！個人開発するときに最初に用意したドキュメント24種と機能要件書を全公開 #生成AI - Qiita

2. 「AIの出力評価と責任」への対策

AIのコードを鵜呑みにせず、人間のレビューが不可欠。**Pythonの危険コードチェックリスト**や、**コードレビュー用プロンプト設計法**を活用し、脆弱性を見抜きます。

【Python】生成AIがこのコード書いたら気をつけろ！ - 事故らないためのチェックリスト #初心者 - Qiita

Copyright © onecom, Inc.
©2025 Google Inc.

09

9. まとめ

Copyright © enecom, Inc.

本日のキーメッセージ

AIはCSIRTの「アシスタント」である

脅威の現実

Qilinのような攻撃者は、「技術（仮想基盤攻撃）」と「ビジネス（法務サービス）」の両面で我々の**事業継続性**を脅かしている

対抗策の進化

もはや手動対応では追いつけない。Dify/n8nによる自動化、Vibe Codingによるツール自作、そしてVibe Kanbanによる**オーケストレーション**が新たな戦い方

AIは「アシスタント」である

AIエージェントとAI駆動開発は、CSIRT担当者を単純作業から解放し、高度化する脅威と対等に渡り合うための**必須スキル**となる

Copyright © enecom, Inc.

なぜ今AIか？ - "100倍"の可能性 (OpenAI "GDPval"調査)

AIが専門的な知識労働のコストを劇的に下げる

タスク速度	タスクコスト	品質 (vs 人間)
100倍	**100倍安価**	**47.6%**
(理論値)	(理論値)	同等以上 (Claude Opus 4.1)

https://openai.com/ja-JP/index/gdpval/

Copyright © enecom, Inc.

現実的な活用法と本講演の結論

> AIが人間に取って代わるのではなく、AIを「アシスタント」として補助的に使うことで、CSIRTの生産性と経済的価値を飛躍的に高められる

— 本講演の結論

Copyright © enecom, Inc.

ご清聴ありがとうございました

エネコムでは、CSIRTメンバーを募集しております

Copyright © enecom, Inc.