

報道各位

2026年8月13日
株式会社インプレス

合法的なハッキング体験を提供！

『生成 AI ハッキング術 MCP を使った実践ガイド』発行

技術の泉シリーズ、8月の新刊

インプレスグループでIT・デザイン関連メディア事業を展開する株式会社インプレス(本社:東京都千代田区、代表取締役社長:高橋隆志)は、『生成 AI ハッキング術 MCP を使った実践ガイド』(著者:藤井 直行, 前田 尚志)をインプレス NextPublishing より発行いたします。

最新の知見を発信する『技術の泉シリーズ』は、「技術書典」や「技術書同人誌博覧会」をはじめとした各種即売会や、勉強会・LT 会などで頒布された技術同人誌を底本とした商業書籍を刊行し、技術同人誌の普及と発展に貢献することを目指します。

『生成 AI ハッキング術』

<https://nextpublishing.jp/isbn/9784295605010>



著者: 藤井 直行, 前田 尚志

小売希望価格: 電子書籍版 1,800 円(税別) / 印刷書籍版 2,000 円(税別)

電子書籍版フォーマット: EPUB3

印刷書籍版仕様: B5 / カラー / 本文 76 ページ

ISBN: 978-4-295-60501-0

発行: インプレス NextPublishing

<<発行主旨・内容紹介>>

本書は、生成 AI と Model Context Protocol (MCP) を活用し、合法的な練習環境でハッキング体験をたどる実践的なガイドです。安全な CTF 環境として自作の脆弱なサーバーを標的に据え、Hacking MCP サーバーを用いながら、日本語で LLM と対話するだけで進めるウォークスルーが段階的に示されます。あわせて、MCP クライアントと MCP サーバーがどのように連携し、外部サービスや対象環境へ必要な処理を橋渡しするのかという仕組みも、具体例を交えて解説されます。内容はハッキングや生成 AI に関心はあるものの、どこから入ればよいか分からない読者を想定し、できる限り平易に整理されています。また、MCP の利便性だけでなく、悪意のあるコードが仕込まれたサーバーを利用する危険性や、許可を得た環境または CTF のような合法的な場でのみ技術を用いるべきことにも触れています。

(インプレス NextPublishing は、株式会社インプレス R&D が開発したデジタルファースト型の出版モデルを承継し、幅広い出版企画を電子書籍 + オンデマンドによりスピーディで持続可能な形で実現しています。)

<<目次>>

はじめに

第 1 章 背景

第 2 章 MCP

第 3 章 本書で作成した MCP サーバーについて

第 4 章 「hacking-mcp」と Cursor を使って 30 分でハッキングする

第 5 章 本書で利用した MCP の概要と簡単な説明

第 6 章 野良 MCP + やられサーバー B の WalkThrough

第 7 章 あとがき

<<著者紹介>>

藤井 直行

1996 年生まれ。山口県出身。

徳山工業高等専門学校卒業後、大手企業を転々とし現在は外資系ビッグテックに所属。

サイバーセキュリティエンジニアとして、SOC 運用、ペネトレーションテスト、フォレンジック調査、内部不正調査、EDR / SIEM を用いた検知・対応に従事。防御と攻撃の双方の視点から、実践的なセキュリティ技術の研究に取り組んでいる。

主な取得資格は OSEP / OSWE / CRTE / RTO2 / C-ADPenX / eCTHP など。

著書に『Vulnerabilities in AI Generated Code ～ハッキングを通じて学ぶ実践的バイブコーディング手法～』など。

趣味は食べることだが、少食であることが悩み。

前田 尚志

1993 年生まれ。兵庫県出身。某メガベンチャー企業データサイエンティスト職として機械学習モデル開発、システム開発、ログデータ分析などを主に担当。最近では企画フェーズから担当する案件も増え、要求要件定義～開発__リリース・運用・エンハンス工程まで幅広く担当。著書に『Vulnerabilities in AI Generated Code ～ハッキングを通じて学ぶ実践的バイブコーディング手法～』など。趣味はドラマ、サウナ、ゲーム。

<<販売ストア>>

電子書籍:

Amazon Kindle ストア、楽天 kobo イーブックストア、Apple Books、紀伊國屋書店 Kinoppy、Google Play Store、honto 電子書籍ストア、Sony Reader Store、BookLive!、BOOK☆WALKER、BOOK TECH

印刷書籍:

Amazon.co.jp

※ 各ストアでの販売は準備が整いしだい開始されます。

※ 全国の一般書店からもご注文いただけます。

<<技術の泉シリーズについて>>

『技術の泉シリーズ』は、技術者の知見のアウトプットである技術同人誌を底本とした、2017 年創刊の技術書シリーズです。NextPublishing によるスピーディな編集制作とプリントオンデマンドによる 1 冊からの印刷製本により、技術の変化に追従しつつ返品や品切れのないサステナブルな出版モデルを特徴としています。本シリーズを通じて、エンジニアの“知の結晶”である技術同人誌の世界に、より多くの方が触れていただくきっかけとなることを目指しています。



【株式会社インプレス】 <https://www.impress.co.jp/>

シリーズ累計 8,000 万部突破のパソコン解説書「できる」シリーズ、デザイン・グラフィック関連の書籍ブランド「MdN」、「デジタルカメラマガジン」等の定期雑誌、IT 関連の専門メディアとして国内最大級のアクセスを誇るデジタル総合ニュースサービス「Impress Watch シリーズ」等のコンシューマ向けメディア、「IT Leaders」をはじめとする企業向け IT 関連メディアなどを総合的に展開・運営する事業会社です。IT・デザイン関連出版メディア事業、およびデジタルメディア&サービス事業を幅広く展開しています。

【インプレスグループ】 <https://www.impressholdings.com/>

株式会社インプレスホールディングス(本社: 東京都千代田区、代表取締役: 塚本由紀)を持株会社とするメディアグループ。「IT・デザイン」「音楽」「山岳・自然」「航空・鉄道」「モバイルサービス」「学術・理工学」を主要テーマに専門性の高いメディア&サービスおよびソリューション事業を展開しています。さらに、コンテンツビジネスのプラットフォーム開発・運営も手がけています。

【NextPublishing】

NextPublishing は、インプレス R&D が開発した電子出版プラットフォーム(またはメソッド)の名称です。電子書籍と印刷書籍の同時制作、プリント・オンデマンド(POD)による品切れ解消などの伝統的出版の課題を解決しています。これにより、伝統的出版では経済的に困難な多品種少部数の出版を可能にし、優秀な個人や組織が持つ多様な知の流通を目指しています。

【本件に関するお問合せ先】

株式会社インプレス : PubX 室

E-mail: np-info@impress.co.jp