

報道各位

2026年10月16日
株式会社インプレス

MCPセキュリティに特化した初の書籍

『MCP実践セキュリティ AIエージェント時代のModel Context Protocol安全運用ガイド』発行

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、『MCP実践セキュリティ AIエージェント時代のModel Context Protocol安全運用ガイド』(著者:井本 賢)をインプレス NextPublishingより発行いたします。

『MCP実践セキュリティ』

<https://nextpublishing.jp/isbn/9784295606024>



著者:井本 賢

小売希望価格:電子書籍版 1,400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／モノクロ／本文94ページ

ISBN:978-4-295-60602-4

発行:インプレス NextPublishing

<<発行主旨・内容紹介>>

世の中には「MCPは便利!」という記事はたくさんあります。しかし、本番導入で直面する現実的な問題(セキュリティ、コスト、ファイルの制約)を体系的にまとめた情報は、まだほとんどありませんでした。

MCPは2024年末に公開されてから約1年半で、Anthropic以外の主要LLMでも採用が広がり、freee、GitHub、Notion、Slackといった本番サービスが公式MCPサーバーを出すようになりました。「実験的プロトコル」から「本番環境に入り始めた標準」への跳躍が、わずかな期間で起きたことになります。

一方で、セキュリティの理解はそれに追いついていません。約40%のサーバーが認証なしで動き、大規模スキャンで100件超のゼロデイ脆弱性が見つかる現状(第6章)は、エコシステムの速度と成熟度の差を物語っています。今この本を出すのは、その差が広がりきる前に、本番でMCPを動かす人の手元に判断材料を届けるためです。

(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>>

第1部 MCPの全体像

第1章 MCPの全体像——LLMと外部ツールをつなぐプロトコル

第2章 MCPのアーキテクチャと通信仕様

第2部 実践——freeeで確定申告を自動化する

第3章 実践——freeeで確定申告を自動化

第4章 トークンコスト実測——接続しただけで課金される「家賃」

第5章 ファイルアップロード問題——7サービス検証

第3部 MCPのセキュリティ——攻撃面と認証

第6章 MCPの攻撃面とOWASP MCP Top 10

第7章 攻撃の実演——ツール経由でMCPはこう破られる

第8章 認証・認可——OAuth 2.1時代のMCPを安全につなぐ

第4部 本番運用——ワークアラウンドとガードレール

第9章 本番ワークアラウンド集

第10章 セキュリティ運用とガードレール——守りを仕組みに落とす

第5部 MCPのこれから

第11章 MCPの未来——何が固まり、何が残ри、今何を決めるか

<<著者紹介>>

井本 賢(いもと けん)

エンジニア歴8年。合同会社Propel-Lab代表社員。AI/LLMとWebRTC・リアルタイム通信を組み合わせたシステム設計を専門とする。Amazon Kindleで技術書4冊を出版(「実践Claude Code」「LLMO - AIに選ばれる最適化戦略」ほか)。Qiitaで技術記事23本を執筆し、累計41,000PV以上。Zenn Booksでは有料・無料合わせて5冊を公開中。

<<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

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。

【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