Zscaler Deception

# CSAのMythosへの対応：90日以内にデセプションを展開

概要

**250人以上のCISOが**デセプション機能の構築を含む、**11の優先アクションに署名しました。**

## Mythosとは？

Mythosは、Anthropicが開発したAIモデルで、主要なオペレーティング システムやブラウザーにおける数千もの重大な脆弱性を自律的に発見し、人間の介入なしに稼働可能なエクスプロイトを生成する能力を備えています。社内ラボ テストでは、MythosはFirefox上で181個の稼働可能なエクスプロイトを生成しましたが、Claude Opus 4.6が成功したのはわずか2回でした。業界では、Mythosによって攻撃者の能力が大幅に向上し、脆弱性発見に必要なコストとスキル レベルが大幅に低下すると考えられています。

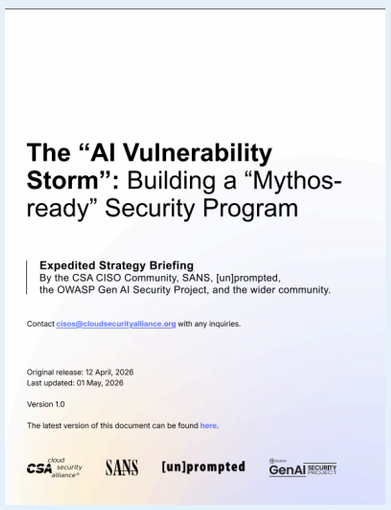
## CSAの対応

Mythosが発表されてから5日後、Cloud Security Allianceは緊急戦略ブリーフィングを発表しました。これは、元CISA長官、元NSAサイバーセキュリティ局長、Google、Netflix、Wells Fargoなどの企業のCISOを含むリーダーたちの貢献によりまとめられたものです。ブリーフィングでは、「インシデントの検出と対応の速度不足」が「CRITICAL」な能力ギャップであると指摘されています。その理由は、機械速度の攻撃に対して人間の速度で検出と対応を行うことのリスクです。

## 11の優先アクションの中でデセプションが必須となっている理由

CSAの優先アクションの9項目では、既知の攻撃ツールやCVEの使用ではなく、攻撃者の行動に基づいて検出を行う機能を展開することを求めています。方法の転換は構造的な違いです。定義上、シグネチャーベースの検出では、新しい脆弱性が検出データベースに存在しないため、新たなエクスプロイトに対応できないのです。攻撃者がPowerShell、標準API、有効な資格情報などの正当なツールを使用するときは、行動検出も失敗します。ー従業員の通常の行動と区別できないからです。

デセプションはどちらにも依存しません。そのため、何かが触れたとデコイが報告した瞬間に、そのアラートは必然的に確実なものとなります。調査やトリアージは一切必要なく、誤検知もありません。デコイによるアラートには曖昧性がまったくないため、デセプションは、運用上健全に、封じ込めを自動化できる唯一のツールです。MythosレベルのAI悪用型攻撃の速度で、ホストの隔離、資格情報の取り消し、IPのブロックを行います。




Cloud Security Allianceは、企業がMythosを悪用した攻撃に備えられるよう、米CISA、NSA、およびホワイトハウスの元サイバー政策責任者らをはじめとする、250名以上のCISOとセキュリティ リーダーを招集しました。

**その結果、**Mythosに対応できるセキュリティ プログラムのための**11の優先アクションをまとめた、**緊急戦略ブリーフィングが作成されました。

### 9：デセプション能力を構築する

今後90日以内の実装義務化を伴う「HIGH」リスクの分類。

「デセプションは攻撃ツールや脆弱性に依存せず、*TTP*に基づいて攻撃と攻撃者を特定します。」



+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com/jp

Zero Trust Everywhere