「Claude Mythos」流出事案の分析：AIの進化とガバナンスの教訓

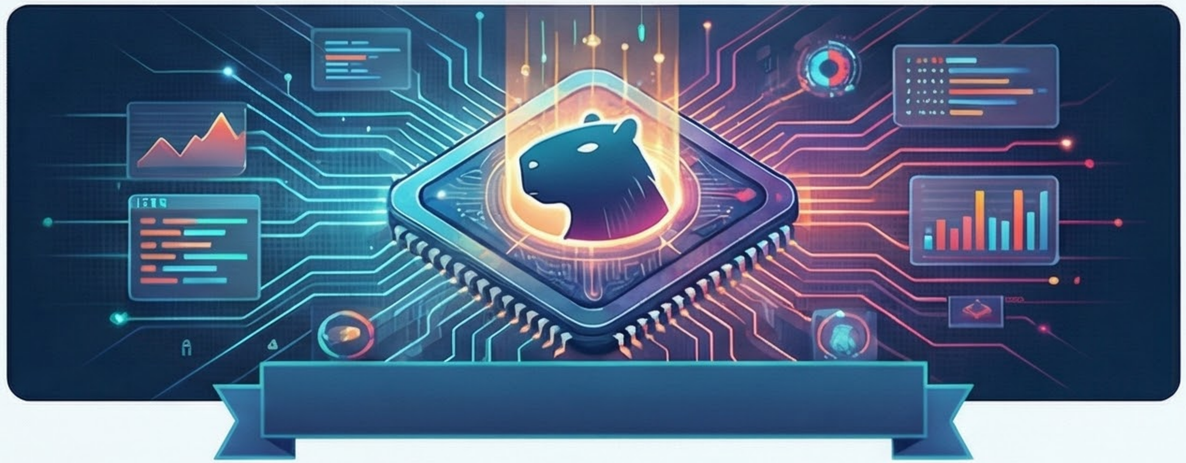
事案の概要と原因

外部CMSの設定ミスによる露出：
外部CMSツールの設定がデフォルトで「公開」になっていたことによる人的ミス。

約3,000件の未公開資産が流出：
報道機関の指摘まで、ブログ用の画像やドラフト資料が維でも閲覧可能だった。

コア資産（重み・顧客データ）は安全
流出したのは公開準備中の素材であり、モデルの重みや顧客データは含まれない。

次世代モデル「Mythos」の衝撃



現行Opusを凌駕する「Claude Mythos」：「Capybara」とも呼ばれ、現行モデルを大きく上回る知能と推論能力を持つ。

圧倒的なサイバー能力とリスク：
脆弱性悪用を加速させる懸念があり、防御側の先行アクセス提供が計画されている。

市場への波及とセキュリティ株の下落
AIによる攻撃優位への懸念から、CrowdStrike等の主要セキュリティ銘柄が下落。