



2023 年 11 月

2023 年 11 月にリリースされた、シスコのクラウドベースの機械学習によるグローバル脅威アラートに関するアップデートです。

- [追加の脅威検出 \(1 ページ\)](#)

追加の脅威検出

新しい脅威検出をポートフォリオに追加しました。

- 危機的状況主導型のサイバー脅威

また、既存の脅威検出のインジケータも更新しました。

危機的状況主導型のサイバー脅威

危機的状況に連動するサイバー活動は、パンデミック、戦争、自然災害などの世界的な危機によって引き起こされ、さまざまな攻撃者によって実行されます。1つのイベントに複数の攻撃者が関与している場合、その帰属が不明であったり混在していることはよくあります。これらのアクティビティには、通常、フィッシングキャンペーン (T1566)、正当な組織へのなりすまし (T1656)、信頼関係の悪用 (T1199)、および詐欺が含まれます。潜在的な成果には、情報戦に対する優位性の獲得、初期アクセスの獲得、サイバー攻撃の実施 (T1583)、および金銭的利益が含まれます。

お使いの環境で危機的状況主導型のサイバー脅威が検出されたかどうかを確認するには、[\[危機的状況主導型のサイバー脅威の詳細 \(Crisis-Driven Cyber Threat Detail\)\]](#) をクリックして、グローバル脅威アラートで詳細を表示します。

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。