



# 福岡県警察からのお願い

令和6年4月 号外

## 「Global Protect」の深刻な脆弱性が公開

今回公開された脆弱性情報 (CVE-2024-3400)

**CVSS10.0(重大度最高レベル!)**



「Global Protect」は、Paloalto社の製品で稼働するPAN-OSにおいて、モバイル端末を含む通信機器からアクセスを可能にする機能です。

「CVE-2024-3400」は、同社のFW製品などで稼働する上記OSのGlobal Protect機能の脆弱性により、認証されていない第三者が管理者権限で任意のコードを実行できる可能性があります。

**対象のPAN-OSバージョン： Ver11.1 | 11.0 | 10.2**

JPCERT/CCでは、本脆弱性を悪用した攻撃による被害を確認していません。現在は限定的な被害であり、悪用する実証コードなどは未確認ですが、**今後本脆弱性を悪用する攻撃が広く行われる**可能性があります。

### Paloalto社 推奨事項

令和6年4月15日時点、本脆弱性を修正する対策バージョンは公開されていません。

※ 同社のHPに本脆弱性の緩和策について記載あり



### 対象機器における緩和策

(※詳細については、Paloalto社のHPを参照してください)

- デバイステレメトリ機能を一時的に無効にする。
- ライセンス契約ユーザーは
  - 脅威ID95187を有効にする。
  - GlobalProtectインターフェイスに脆弱性保護が適用されていることを確認する。

◆ 福岡県警察本部サイバー犯罪対策課では、最新のサイバー犯罪の手口や対策などを、X (旧Twitter) やHPに掲載していますので、ぜひご覧ください。

◆ 万一、被害に遭われた場合は、管轄警察署宛てご一報ください。

[X]



[HP]

