

【お知らせ】 Heuristic. HEUR/AGEN.* の大量検知について【解消】

2023年03月29日 19:00(更新)

2023年03月24日 21:00(発行)

弊社エンドポイントセキュリティ(EPP)において、3月22日リリースパターンファイルF-Secure Capricorn 2023-03-22_06以降、実行ファイル(exe)に対する大量の振る舞い検知(Heuristic. HEUR/AGEN.*)が発生しておりました。ウイルス研究ラボで当検知群の解析を実施し、過剰検知が確認されましたのでF-Secure Capricorn 2023-03-24_11パターンファイルでの修正を実施いたしました。この度はご不便をおかけいたしました事をお詫び申し上げます。製品デフォルト設定ではこれらのパターンファイル更新は自動的に行われますのでお客様側操作は特に不要となります。オフライン環境での御利用の場合、修正バージョン以降のパターンファイルを手動適用する必要があります。

経緯(日本時間)

2023年3月22日(水) 16:00 : F-Secure Capricorn 2023-03-22_06 をリリース

2023年3月23日(木) 10:00 : 誤検知報告増加を確認。検体ファイルの収集/解析を開始

2023年3月24日(金) 18:00 : 修正版パターンファイル 2023-03-24_06 をリリース

2023年3月25日(土) 01:00 : 再修正パターンファイル(ロールバック処理)Capricorn 2023-03-24_11 をリリース

これ以降、復旧確認のためCapricorn更新を一時停止

この間のEPPセキュリティはセキュリティクラウドとふるまい検知機能で担保

2023年3月29日(水) 01:00 : 完全復旧確認後、Capricorn 2023-03-29_01 をリリース

今回の事象の経緯は弊社サービスステータス確認ページでもご確認いただけます。

<https://www.withsecure.com/jp-ja/support/service-status-and-db-updates>

パターンファイルバージョン

<https://www.withsecure.com/jp-ja/support/service-status-and-db-updates>

不明な点がある場合は、弊社サポートセンターまでお問い合わせください。

お問合せフォーム

<https://www.withsecure.com/jp-ja/support/contact-support/email-support>