



## NetEyez バージョン 4.0 リリースノート

**2025-10-20**

**Version 4.0.2**

このリリースでは、既知の不具合を修正しました。また新機能も追加しました。

### アップグレードについて

リカバリメディアによるシステムリカバリを提供します。

### アップグレード適用可能モデル

- NTEZ-01GC-R2 (1GbE NetEyez Distributed モデル)
- NTEZ-10GM-R2 (1/10GbE NetEyez Distributed モデル)
- NTEZ-10GM-S-R (1/10GbE NetEyez Security Distributed モデル)
- NTEZ-10GM-S-P (1/10GbE NetEyez Security Portable モデル)

### 新機能

1. [セキュリティ] セキュリティ検知において、管理するアセットや、脅威のサブレッション機能を追加しました。これにより、大量の誤検出に埋もれることなく、お客様が本当に確認すべき脅威を効率的に把握できるようになりました。[#6003]
2. NetEyez の Linkage 機能を改善し、SYNESIS キャプチャセッションにおける解析性能を従来比で約 2 ～ 3 倍に向上しました。なお、SYNESIS 上のトレースファイル (PCAP) の解析性能は従来通りです。[#6701]

### Version 4.0.1 からの主な変更点

1. ICMP が通らない環境でも、指定した syslog サーバーへアラートを送信できるように改善しました。[#6692]
2. NetEyez の Linkage 機能を使って、SYNESIS のファイル名に 2 バイト文字を含むトレースファイルを解析できるように改善しました。[#6486]

3. [セキュリティ] 侵入検知処理において、参照するルールセットを「コミュニティルールセット (NetEyez デフォルト)」または「サブスクリバールールセット (お客様契約)」のいずれか一方のみ有効に変更しました。[#6585]
4. ログに出力内容を強化しました。[#6465]

### 修正した不具合

---

1. キャプチャ中の pcap ファイルをデコードすると、プロセス omni-decode がクラッシュする不具合を修正しました。[#6480]
2. セキュリティ機能で、[アラーム]>[セキュリティイベント]>[脅威] のエクスポート処理が 10 分を超えるとログイン画面に遷移し、データがエクスポートされない不具合を修正しました。[#6475]
3. ディスク空き容量が不足した場合に、キャプチャを正常に停止できない問題を修正しました。[#6546]
4. 解析ログファイルのサイズ取得処理において、2GB を超えるファイルサイズを正しく取得できず、同じログデータが繰り返し登録されて分析が完了しない不具合を修正しました。[#6865]
5. CVE-2025-10585 (Chromium V8 による型混同の脆弱性) への対策として、関連パッケージを最新版に更新しました。
6. CVE-2025-32462, CVE-2025-32463 (sudo によるローカル権限昇格の脆弱性) への対策として、関連パッケージを最新版に更新しました。

## システムリカバリ

---

リカバリメディアによるシステムリカバリを提供します。

## アップグレードについて

---

本リリースでは、OS が Ubuntu 24.04 にアップグレードされました。

既存のデータと設定、失われます。ただし、設定のエクスポート・インポート機能を使用することにより、構成情報を引き継ぐことは可能です。

## 新機能

---

1. OS を Ubuntu24.04 に更新しました。
2. NDPI を V4.8 に更新しました。
3. DPDK を V23.11.2 に更新しました。
4. Snort を V3.3.0.0 に更新しました。
5. TD-agent を V5.0.4 に更新しました。
6. マニュアルを充実しました。また配布ファイルも提供しました。[#6308]
7. 「メッセージセンター」機能を追加しました。ユーザー画面で表示した過去のエラーメッセージ最大 500 項目を確認できます。[#5779]
8. グローバル IP(カスタム IP のアセット)の解析機能を強化、IDS 解析の対象になりました。(セキュリティ)[#5834]

## Version 3.1.2 からの主な変更点

---

1. LLC ノードテーブルに ARP/RARP を登録より、ARP/RARP パケットの解析に対応しました。[#4870]
3. 「アナリスト」ユーザーが SYNESIS 連結機能を使用できるように変更しました。[#6336]
4. [設定]>[セキュリティ]>[パブリックアセット]を[カスタム IP のアセット]に変更しました。また新規登録/編集/有効設定変更後に、「適用」ボタンで適用するように変更しました。(セキュリティ)[#5728]

5. ウィジェット「トップ N イベント分布」、「トップ N 悪意」で表示する件数を 25 件に変更しました。(セキュリティ)[#5751]
6. バックアップ時に指定する外部ディスクの保存先について、FAT32 ファイルシステムはサポート対象外としました。[#6307]
7. 日本語表記「脅威の傾向」を「脅威トレンド」に変更しました。(セキュリティ)[#5881]
8. セキュリティレポートにおいて、[全ウィジェットの時間範囲]設定を無効にし、常にチェック状態に変更しました。(セキュリティ)[#6344]
9. データ収集でのログ機能をオプション機能に変更しました。([データ収集]>[ログ]、セキュリティ) [#6342]  
※ログ機能：サードパーティーの製品からログ情報を取得します。NetEyez での脅威解析が可能になります。
10. Beat センサー機能をオプション機能に変更しました。([設定]>[セキュリティ]>[Beat センサー]、セキュリティ) [#6342]  
※Beat センサー機能：センサーNetEyez 機器のシステム状態および負荷状況を監視します。
11. SYNESIS 統合(Linkage)機能の仕様変更に伴い、SYNESIS 上のトレースファイルのデコードはサポート対象外となりました。[#6462]
12. IntSights 脅威インテリジェンスサービスを利用したセキュリティ検知機能の提供を終了しました。[#6473]

## 修正した不具合

---

1. 重複したファイル名でキャプチャすることはできますが、1つのみ解析できる不具合を、重複ファイル名を使用できないように修正しました。[#4651]
2. 「名前をつけて保存」や関連する Pcap ファイルダウンロード処理で作成した一時ファイルを削除されない不具合を修正しました。[#6349]
3. 解析> アプリケーション> ファイル監視にて、PDF または CSV ダウンロードで長いファイル名が表示不完全不具合を修正しました。[#5954]
4. サイズ大きい Pcap ファイルを解析時、リソース不足による検索・分析エンジンの停止を防ぐように修正しました。[#6346]

## 制限事項

---

1. 直近 5 分間を含む時間範囲を選択した場合、集計処理の影響により、表示されるデータに誤差が生じる可能性があります。[#5546]

2. リアルタイム監視において、監視停止直前の一部の解析結果が失われる可能性があります。[#6271]
3. 同一トラフィックを含んでも、リアルタイム監視、Pcap ファイル解析、SYNESIS キャプチャセッション解析で解析する結果は一致しない可能性があります。[#6358]
4. NetEyez で解析可能なトレースファイル (SYNESIS Next プロンプ上のファイルを含む) は、ファイル名に英数字、アンダースコア ( \_ )、およびダッシュ ( - ) のみが使用されている必要があります。
5. SYNESIS Next では、管理ポートのリンクスピードが 1G のみ動作検証済みです。
6. 設定のインポートおよびエクスポートでは、SYNESIS プロンプの設定はサポートされていません。
7. SYNESIS Next で一度に解析できる SYNESIS のキャプチャセッションデータは、最大 50GB までに制限されています。
8. SYNESIS Next は、NetEyez と SYNESIS のタイムゾーンが同じ場合にのみ正しく解析を行います。
9. 集計ステータスのオン・オフを切り替えると、ES に記録された統計と KPI が削除されます。
10. エージングにより過去の解析結果を消去した場合にも名前解決の結果は保持されます。
11. IP チェックサムエラーがあるパケットについての動作がリアルタイム監視とそれ以外 (pcap などの解析) で異なります。リアルタイム監視ではそのパケットについてはパケット数、バイト数を 0 としてカウントします。Pcap ファイルなどの解析では観察されたパケット数、バイト数をカウントします。
12. OS のアップグレードおよびデータベーススキーマ変更により、V3.1.2 以前のバージョンのデータは保持できません。
13. ナビゲーションメニューで検索モードに入ったら、サブメニューを閉じることができなくなります。
14. カテゴリをまたいだ重複チェックが行われないため、支店、VIP、サイト定義で IP アドレスやサブネットが重複していると、解析結果が不正確になる可能性があります。
15. 通常の検索は、現在リストテーブルに表示されているデータのみに対して実行されます。
  - 「IP グローバル検索」を有効にすると、データベース全体から IP アドレスを検索できます。ユーザー、アプリケーション、バイト数、パケット数のいずれの項目においても、ソートは常にデータベース全体に対して実行され、現在のリスト表示だけを対象にしているわけではありません。

- 一方で、グローバルではない通常のソートは、リストテーブルに表示されているデータのみに対して適用されます。