

# 大規模通信ネットワークにおける通信データの調査に威力を発揮！

2014年9月9日  
**新登場**



ネットワークフォレンジックサーバ

## NetEvidence® Enterprise

ネットエビデンス エンタープライズ

「NetEvidence Enterprise」は、ネットワーク上でやり取りされる外部との通信データを記録する「ネットワークフォレンジックサーバ」です。「どのような情報を」、「いつ」、「誰が」、「どこへ」、「どんな手段で漏えいさせたか」を素早く特定し、証拠として保全します。情報セキュリティ対策の強化に取り組むお客様において、大規模ネットワーク通信を可視化するための高性能なシステムをご提供いたします。

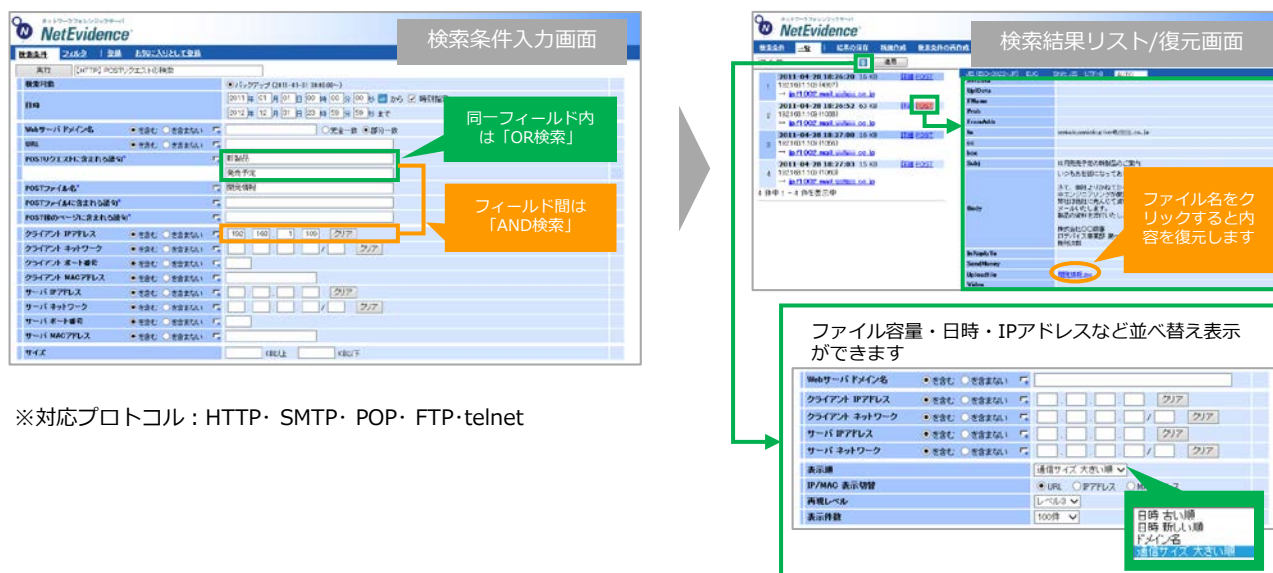
## 特長

- 1. 高い記録性能**  
ギガビット環境の高速ネットワークに対応しています。
- 2. 最適なシステム構成**  
ネットワークのトラフィック量や通信プロトコルに合わせたシステムを、自由に構成することができます。大流量の通信をリアルタイムで解析する構成や、通信パケットのみを記録する場合など、お客様のニーズに合わせた最適な構成を設計できます。
- 3. 高い拡張性**  
サーバの増設により記録や解析の処理性能を個別に強化できるため、導入後に通信量が増加した場合なども柔軟に対応できます。また、複数のNASを接続できるので、長期間に亘る膨大なデータも簡単に検索することができます。

## 検索画面イメージ

検索画面はどなたでも操作しやすいように、わかりやすく構成されています。

### ●POSTリクエスト検索画面例



The image shows two screenshots of the NetEvidence web interface. The left screenshot is titled '検索条件入力画面' (Search Condition Input Screen) and shows various search criteria fields. A green callout box points to a field with the text '同一フィールド内は「OR検索」' (Within the same field, it is 'OR search'). An orange callout box points to a field with the text 'フィールド間は「AND検索」' (Between fields, it is 'AND search').

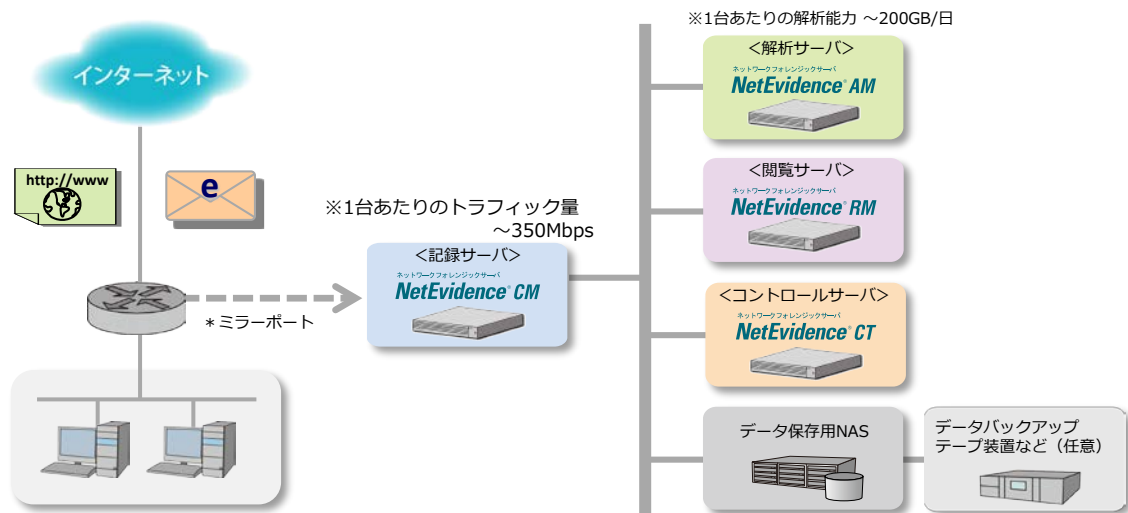
The right screenshot is titled '検索結果リスト/復元画面' (Search Results List/Recovery Screen) and shows a list of search results. An orange callout box points to a file name in the list with the text 'ファイル名をクリックすると内容を復元します' (Clicking the file name restores the content). Below this, a green callout box points to a filter section with the text 'ファイル容量・日時・IPアドレスなど並べ替え表示ができます' (Sorting and display by file size, date, IP address, etc. is possible).

※対応プロトコル : HTTP・SMTP・POP・FTP・telnet

## システム構成

下記4種類のサーバによって構成されます。


1. **NetEvidence CM <記録サーバ>**  
ネットワーク上の通信を記録し、パケットファイルをNASに保存するサーバです。  
1台のサーバで **[350Mbps]** のトラフィックまで対応可能であり、トラフィック量に応じて増設できます。
2. **NetEvidence AM <解析サーバ>**  
パケットの解析（通信の復元）を行うサーバです。  
1台のサーバで1日当たり **[200GB]** のパケットを解析でき、記録されるパケット量に応じて増設できます。
3. **NetEvidence RM <閲覧サーバ>**  
復元した通信の検索と閲覧を行うサーバです。
4. **NetEvidence CT <コントロールサーバ>**  
NASに保存されたパケットデータの解析を指示するサーバです。



### 「NetEvidence Enterprise」のここがすごい！

- ◆ **わかりやすい検索画面！**  
専門的な知識は必要なく、どなたでも直感的に操作できます。
- ◆ **自動バックアップ！**  
通信パケットの記録や解析を停止することなく、記録した通信パケットなどのデータを自動的にNASにバックアップします。
- ◆ **サーバへのリストア不要！**  
NASに保存されたデータは、NetEvidenceサーバにリストアすることなく直接検索できます。
- ◆ **外部メディアへのバックアップも簡単！**  
データはフォルダ単位で取り扱えるためテープなどの外部メディアにバックアップすることも可能です。
- ◆ **NASはCIFS/NFS対応！**  
データ保存用NASはお客様が自由に選択できます。（CIFS/NFS対応製品接続可）
- ◆ **柔軟なカスタマイズ対応！**  
お客様のご要望に応じたカスタマイズに対応しています。
- ◆ **安定稼働と万全なサポート体制！**  
ソフトウェア、ハードウェアとも国産製品で、安定した稼働実績が多数あります。万一の障害発生時にも全国対応の保守体制で、導入後も安心してお使いいただけます。

➡ **無料で検証機を貸し出ししております。お気軽にご相談ください。**

 株式会社 オーク情報システム

本店 〒131-0034 東京都墨田区堤通1-19-9 リバーサイド隅田セントラルタワー Tel.03-5247-3235  
大阪支店 〒550-0001 大阪府大阪市西区土佐堀1-4-11 金鳥土佐堀ビル7階 Tel.06-6441-2550  
E-Mail. NetEvidence@ml.oakis.co.jp URL. <http://www.netevidence.jp/>

N1414A1201