

強力な検証機能!

100%パケットキャプチャ&リアルタイム解析

添付ファイル内容  
検索可能

メール添付のファイルの内容もくまなく検索。圧縮ファイルにも対応しています。

ディスク上のデータは  
リアルタイムに  
検索可能

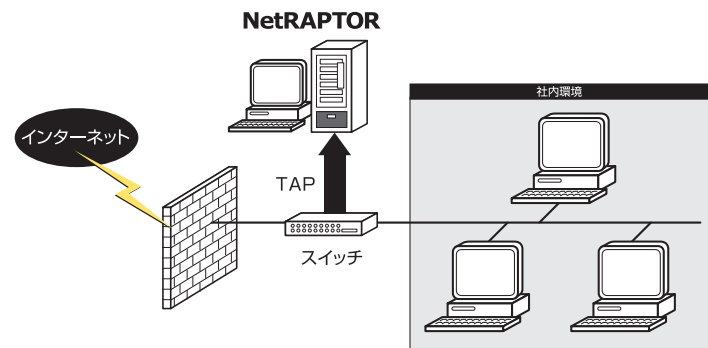
外部記憶装置の保存データは、リストア作業を行わず随時検索することができます。長期保存データも即検索可能。

テープ装置を  
サポート

1台構成で連続運転が可能。テープ装置の接続により、長期のデータ保存が可能です。

導入・運用上での利点

通信・ネットワーク運用への影響率0%



NetRAPTORは、TAP装置を経由して通信データを採取するため、既存のネットワークへの影響がなく、通信速度の低下や本製品障害発生時のネットワーク停止といった問題は起こりません。

- 導入作業の負荷が最小限
- 利用者の利便性を損なわない

運用中のサーバではテープ交換以外の操作が発生しません。

- 運用管理の負荷が最小限

機能一覧

簡易検索	フォームを用いて簡単に検索条件を設定することができます。
詳細検索	簡易検索フォームで設定した条件を自動的に論理演算式におこし、さらに詳細な条件に編集することができます。
条件リスト	簡易検索、詳細検索で設定した条件を保存可能。使用頻度の高い条件、複雑な条件、重要な条件を保存し、随時利用する事ができます。
検索結果一覧	検索結果一覧はCSV形式でのダウンロードが可能です。
アラート通知	設定したアラート条件に合致する通信をリアルタイムに管理者へ報告します。アラートには「警告」「注意」のレベル付けが可能です。
レポート	アラート履歴を日別、項目別に表示します。CSV形式でのダウンロードが可能です。
統計	HTTP(クライアント別、ホスト別、クライアント-ホスト別)、SMTP・POP(FROM別、TO/CC/BCC別、FROM-TO/CC/BCC別)の集計結果を表示します。CSV形式でのダウンロードが可能です。
閲覧ログ	NetRAPTORで行った検索の記録を表示します。検索者、検索条件、検索数、閲覧数、等確認する事が出来ます。CSV形式でのダウンロードが可能です。
ダンプデータ	採取したデータ(rawデータ)のダウンロードが可能です。SnifferやWireshark(Ethereal)へダウンロード可能です。

●記載内容は2010年9月1日現在のものです。 ●機能向上のため、予告なく仕様の一部を変更する場合があります。

開発元



トーテックアメニティ株式会社 eni事業推進室

■東京本社 TEL: 03-5436-2100  
〒141-0032 東京都品川区大崎1-11-1  
ゲートシティ大崎ウエストタワー21F

■大阪事業所 TEL: 06-6350-0850  
〒532-0003 大阪市淀川区宮原4-6-18 新大阪和幸ビル8F

URL: <http://www.netraptor.jp/>  
E-mail: [esales@totec.co.jp](mailto:esales@totec.co.jp)

お問合せ先

NetRAPTOR

情報セキュリティ監査アプライアンス

情報漏洩に対する調査と分析

ネットワーク・フォレンジック

情報漏洩とは、通信ネットワーク上で起こる「事故」のようなもの。  
そのような「事故」に遭遇し法的な解決が必要になった場合、証拠性を確保するためにはどうすればよいのでしょうか？

NetRAPTORはすべての通信データを採取して記録。  
万が一「事故」が発生したときにも証拠性を確保する上で必須となるデータを得ることが可能です。  
さらに、全通信データ採取・保存の方針を組織内に周知することで  
情報漏洩に対する抑止効果が生まれます。



企業法令遵守と企業価値向上を目指して

# NetRAPTOR

## 監査証跡確保！ ネットワーク・フォレンジック【ネットラプター】

「日本版SOX法」が施行され、いつ・誰がどの情報を扱ったのか管理・記録する事で企業としての責任を明確にしようとする「内部統制重視」の姿勢は今後ますます加速・浸透していくことが予想されます。

NetRAPTORは通信データの記録・保存をすることで、「情報を扱う」という行為に対する意識を新たにし、企業法令遵守の姿勢を育てることを基本とします。

同時に、いざというときには検証機能で追跡調査、企業責任を支援する情報セキュリティ監査ソリューションです。

### 1 保存

全ての通信データを採取、永続的に保存。  
非常時の証跡監査に。また自社で不正流出がないことの証拠として。

### 2 検証

通信内容を検索・再現し強力的に検証  
高速全文検索エンジン搭載。統計データによる自社傾向調査も。

### 3 報告

不正な通信をリアルタイムで報告  
報告条件を自在に設定可能。

通信に関する自社ポリシーを作成、日々状況を確認しながら検証結果に基づいてポリシーを更に最適化…  
長期的な運用でより強力な情報セキュリティ監査が実現します。

NetRAPTOR は導入負荷の少ない  
ネットワークキャプチャ型

- ❖ アプリケーションに依存しない
- ❖ 導入作業が容易
- ❖ 既存ネットワークに影響を与えない
- ❖ クライアントへの影響なし
- ❖ 運用管理が容易でTCOが安価

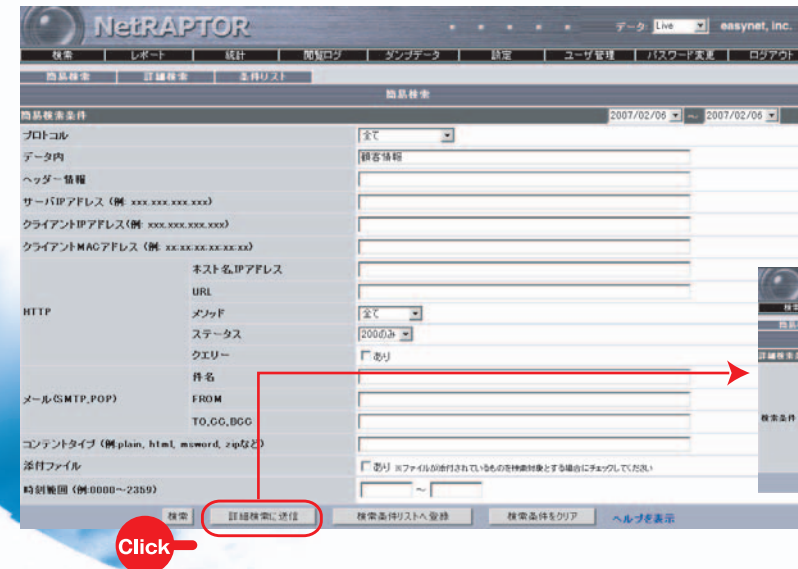
ネットワークキャプチャ型の弱点 “バケットロス”  
→ 該当箇所の再現ができない…

しかし! NetRAPTOR は  
ギガビットフルワイヤキャプチャ対応  
バケットロスがない!!  
→だから! 確実に証拠が残っている!!

## 検索機能

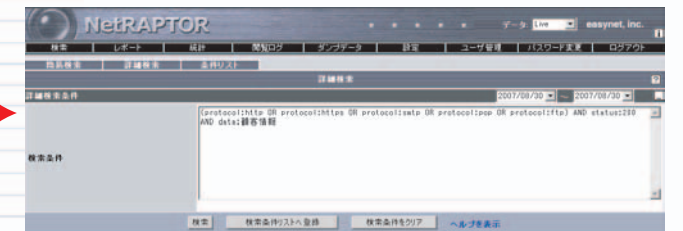
採取した通信データを検索します。

検索フォーム…「顧客情報」というキーワードで検索する場合



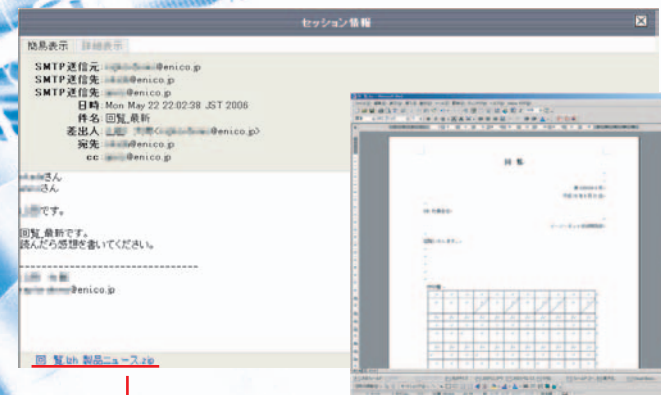
【簡易検索】  
プロトコル:全て  
データ内:「顧客情報」を設定。

【詳細検索】  
簡易検索で設定した条件を自動的に論理演算式におこします。ここでさらに詳細な条件に編集することも可能。

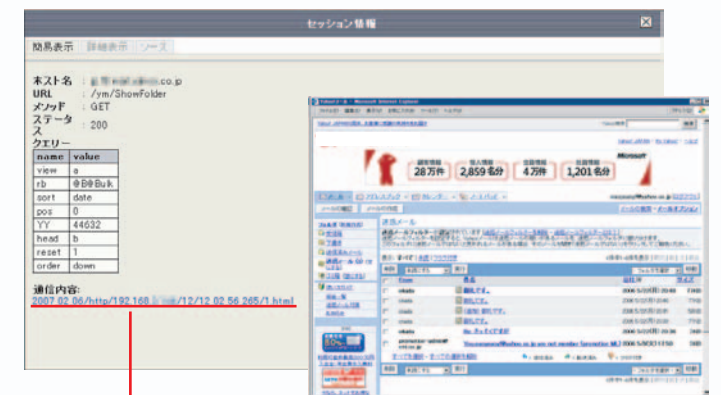


検索結果…検索結果一覧、セッション情報（簡易/詳細）、およびweb閲覧画面、メール添付ファイル等、表示可能。

【セッション情報（簡易）】  
●メールデータの場合  
セッション情報およびメール本文を表示。



●webデータの場合  
セッション情報を表示。



## アラート機能

不正な通信を管理者に報告します。

条件リスト… 簡易検索、詳細検索で利用した条件を保存、アラート条件を指定します。

アラート通知…アラート条件に合致する通信をリアルタイムに管理者へ通知します。

レポート…アラート履歴を画面から確認することができます。

警告 注意のレベル設定可能。( X は条件をアラート利用せず保存。)

アラート条件	登録者	名前	コメント	対象アナライザ	メール送信先	
なし	初期管理者	1-1 メール(添付ファイル付)		全アナライザ	初期管理者	検索 詳細
警告	初期管理者	1-2 へのアクセス	2006/5/1より実施	全アナライザ	登録者	検索 詳細
注意	初期管理者	1-3 HTTPS通信		全アナライザ	初期管理者	検索 詳細

自社開発の **高速全文検索エンジン標準搭載**  
**検索が速い！ 目的の情報へすばやく到達**