



ネットワークフォレンジックサーバ

NetEvidence[®] Ax

ネットワークの通信を漏れなく記録

わかりやすい画面で簡単に検索

セキュリティ事故発生時に効果を発揮

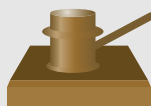
情報漏えい発生時にすばやく原因を特定できる
ネットワークフォレンジックサーバです。
内部関係者を牽制することで情報漏えいリスク
を軽減します。



企業に求められるリスクマネジメント

情報セキュリティ対策やコンプライアンスへの対応

- 個人情報保護法
- 内部統制報告書
- 新会社法など



インターネットに潜むさまざまなリスクへの対応

- ウイルス感染
- フィッシング詐欺
- スパイウェア など



『インターネット通信の記録と可視化』こそが最も有効な手段であると考えています。

インターネット通信が記録されていないと・・・

- 電子メールや掲示板への書き込みなど、どんな情報が社外に発信されているかわからない
- Proxyサーバなどのログだけでは、通信情報の内容はわからない

インターネット通信が記録されていれば・・・

- ネットワークからの情報漏えいなど、セキュリティインシデントが発生した際の原因が特定できる
- 記録していることを社内通知することで、インターネットの業務外利用を抑制できる

インターネット通信を記録するためには・・・

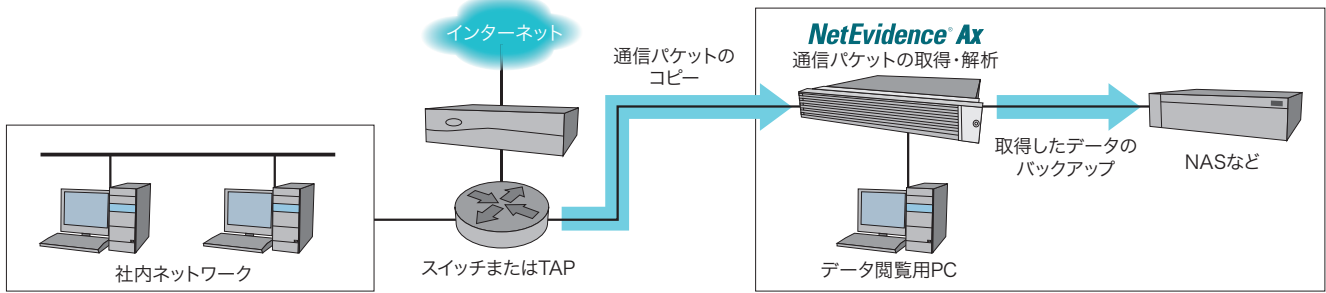
- 膨大なデータ量であるため、専用の機器が必要
- 通信パケットを直接記録するのが最も簡単で唯一の方法

ネットワークフォレンジックサーバNetEvidence Axを使うと

- 社内とインターネットの間でやり取りされるパケットをすべて記録します。
- 記録したパケットからメールや掲示板への書き込みなどの通信を復元します。
- 外部に発信されたデータを、任意のキーワードで検索できます。
- 取得したパケットを自動的にNASにバックアップします。
- バックアップしたNASのデータも検索できます。
- 定期的な検索(監査)を自動で行います。

NetEvidence Axシステム構成例

既存のネットワーク環境に接続するだけで、ネットワーク通信パケットを取得。記録したパケット、検索用データベースはNASなどのストレージにバックアップします。



インターネット通信の解析表示例

電子メールやWebの閲覧など、通信結果が一目瞭然。

登録検索条件一覧

タイトル	作成時刻	状態	操作
[SMTP] メールの検索			編集
[SMTP] メールの検索(送信元アドレスにoakisが含まれるメール)			編集
[HTTP] POSTリクエストの検索			編集
[HTTP] Webの検索(oakis)			編集
[HTTP] Webの検索(oakis表示したリスト)			編集
[SMTP] 昨日のメール一覧			
[SMTP] メールの検索			

検索条件のリスト
あらかじめ検索条件を登録できます。
よく使う条件はお気に入りとして設定します。

登録した検索条件を編集できます。

SMTP検索結果

検索結果からメールのタイトルをクリックするとメール本文を表示します。

添付ファイルも復元します。

Web(HTTP)検索結果

検索結果からURLをクリックすると閲覧したWeb画面を表示します。

検索条件編集

※対応プロトコル：HTTP・SMTP・POP・FTP・telnet