

## 内部監査・ネットワーク監視ソリューション

# TrueWitness

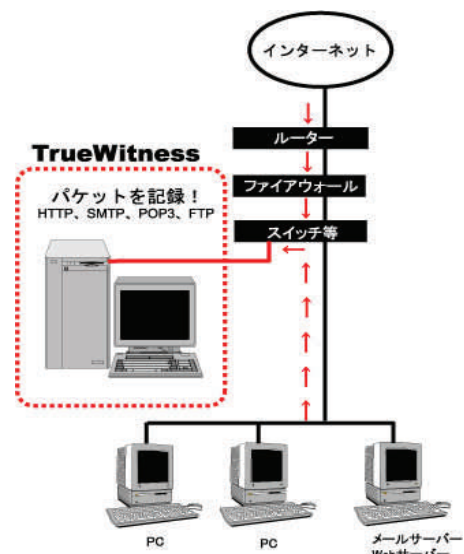
「TrueWitness」は、ネットワークを通るパケットを直接監視・記録するシステムです。ネットワークの私物化の防止、企業の機密情報の流失防止、電子メールでの取引証拠、不正アクセスの証拠、情報漏えいの痕跡、Webの閲覧、掲示板への書き込みなどをパケットレベルで記録・監視・解析することが出来ますので、ネットワーク犯罪の調査や内部犯罪の抑止などリスクマネジメントソリューションとして有効です。



モデル名	TrueWitness 1.7
ハードウェア形状	タワー型/ラックマウント型
メモリ	512MB~4GB (最大)
ハードディスク容量	500GB × 2~ (選択可能)
バックアップ装置	LTO (テープバックアップ装置)
ネットワークカード	NIC × 2
復元可能アプリケーション	HTTP、SMTP、POP3、FTP、その他全てのパケットをキャプチャ

### True Witnessの特徴

- ・ 電子メールでの取引証拠、不正アクセスの証拠、Webの閲覧、掲示板への書き込みなどをパケットレベルで記録・監視・解析。
- ・ 記録したいネットワークの手前に設置するだけで記録・監視を行うことができます。管理はWebブラウザから行うことができ、セキュリティの専門知識が無くても使用することができます。
- ・ Pingやポストスキャンに反応しません。そのため外部侵入者や内部員にも存在を気付かせずに調査解析を行うことができます。
- ・ メール利用閲覧機能/Web利用閲覧機能/FTP利用閲覧機能/侵入攻撃検知解析機能/メール、Web利用者別ランキング表示機能。



設置例

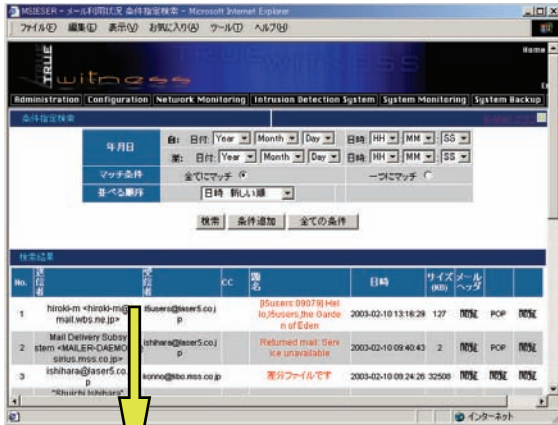
## TrueWitness

「TrueWitness」はインフィニートク株式会社の開発した製品です。株式会社CSPフロンティア研究所は販売代理店として扱っています。



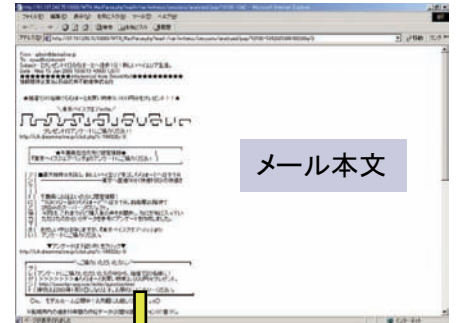
## TrueWitness使用方法 [メール]

- ◆ メールを使った情報漏洩や私用メールを「誰が」「何処に」「何を」「何時」送受信したかを簡単に検索することが出来ます。
- また、TrueWitnessの packets 解析機能により、その検索結果からメールの「本文」「添付ファイル」「ヘッダー情報」(CC、BCC、メール、サーバー等)を閲覧することが可能です。



### メール検索画面

特定のメールの件名をクリックするとメール内容が閲覧可能。



### メール本文



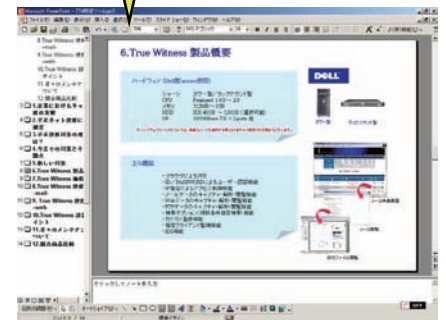
### ソースの閲覧

メールのヘッダー情報やソースもそのまま保存されています。メールの改竄履歴も確認することが可能。



### 添付ファイル閲覧

メールに添付されたデータの復元が可能。



## TrueWitness使用方法 [Web]

- ◆ Webでアクセスした履歴を全て保存することで、Webメールを使った情報漏洩や、掲示板などへの書き込み内容を全て閲覧することができます。また、一度に複数の条件を指定することができる高度検索機能により見つけた情報をすぐに検索することが可能です。

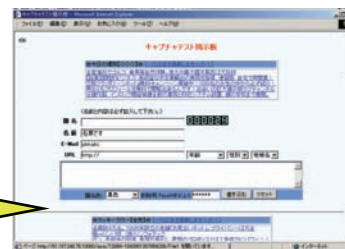
### Web利用解析画面

Webにアクセスしたクライアント、アクセス先、URL、日時などの表示。



### 利用Webの閲覧

Webページ閲覧可能。



### POSTデータの閲覧

掲示板などに書き込みを行った場合は「POST」という表示がされ、表示をクリックすると書き込み内容が閲覧可能。



株式会社CSPフロンティア研究所

〒151-0073 東京都渋谷区笹塚3-2-3 CSPテクノプラザ

TEL 03-5304-4521

FAX 03-5304-4522

Email: info@csp-frontier.jp