

フォレンジックサーバ TrueWitness



内部監査・情報漏洩に抑止効果を与えるネットワーク監視装置

「True Witness」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。電子メールでの証拠、不正アクセスの証拠、情報漏えいの痕跡、Webの閲覧、掲示板の書き込みなど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。また、ネットワークの私物化の抑止、企業の機密情報の流出抑止にも役立ちます。

TrueWitness 4つの特徴

1、パケットレベルで記録・監視・解析

電子メール、不正アクセス、Web、掲示板の書き込み、FTPなどをパケットレベルで記録・監視・解析。

2、被害情報の把握と調査

通信記録を残しておけば不正アクセスや情報漏えいが発生した時に「いつ・誰が・何を・どのようにして」といった被害状況を調査することが可能です。また、証拠として利用することにより、被害状況の把握、原因を突き止めることができるので、事故防止に役立ちます。

3、ステルス性

Pingやポートスキャンに反応しません。そのため外部侵入者や内部者さえ「True Witness」の設置に気付きません。

4、簡単導入

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。

フォレンジックサーバとは

フォレンジック (Forensic: 裁判、法廷) の意味する通り、個人情報流出事件などで、訴訟が提起された場合に備え証拠能力を有する通信記録 (証跡) を収集・管理するサーバ機器を指す用語です。

フォレンジックサーバの機能要件として概ね以下が必要とされます。

- 1、定常的・連続的に通信内容 (接続、通信タイプ、通信内容 / データ) を漏れなく記録すること。 1
- 2、採取した通信内容の記録から、個々の通信の解析が可能であること。 2
- 3、記録した通信履歴を検索し、問題となる通信が特定できること。

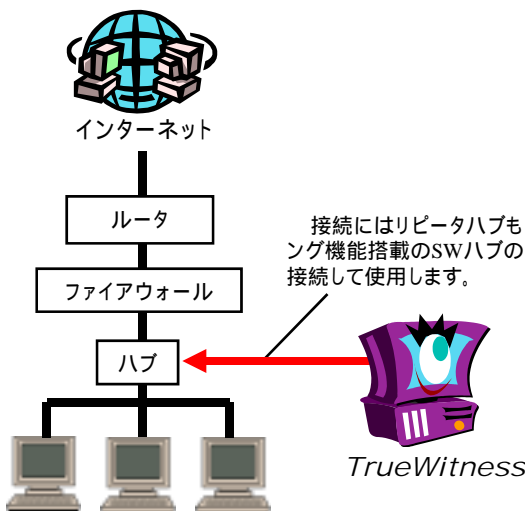
- 1 「TrueWitness」はスニッファ一型のパケット収集・記録機能を実現しており、データを取りこぼすことなく、殆ど完全にトラフィックを採取できます。
- 2 「TrueWitness」を用いて採取した通信記録を、管理PC (ブラウザによる遠隔管理・監視インターフェース) から、不正操作を特定するために解析・検索を行うことが可能です。



初期画面



検索・解析画面



設置環境によりTypeが
お選びいただけます。



タワー型



ラックマウント型

機能		
パスワード変更		
管理ホスト限定		
システムアラート警告メール送信		
一覧表示件数変更		
Web解析結果表示	最新リクエスト一覧	
	閲覧サイト別ランキング	
	利用クライアント別ランキング表示	
	条件指定検索 (年月日時間、クライアントIP、URL指定、サイト指定、サイズ別)	
メール解析結果表示	最新メール別一覧	
	メール送信者別ランキング表示	
	メール受信者別ランキング表示	
	条件指定検索 (年月日時間、件名指定、送信者指定、受信者指定、プロトコル別、サイズ別)	
FTP解析結果表示	最新リクエスト一覧	
	利用サーバ別ランキング表示	
	利用クライアント別ランキング表示	
	条件指定検索 (年月日時間、クライアントIP)	
解析可能プロトコル	http,smtp,pop3,ftp(暗号化されているものは除く)	
コンテンツカテゴリ作成機能		
ネットワーク接続履歴表示		
侵入攻撃検知解析機能		
システムリソースモニタ表示		
システムプロセス表示		
ポ-トスキャンログ表示		
製品仕様		
モデル名	TrueWitness1.5 Standard	TrueWitness1.5 Enterprise
形状	タワー型/ラック型	
筐体	NEC Express Server GT110a-s	
CPU	Intel PentiumR プロセッサー (E2160/1.80Ghz)	
メモリ	2GB	
HDD	SATA 1TB(1000GB)	
Ethernet	1000BASE-T/2nic	
オプション	DELL LTO Back up tape	
再現可能なアプリケーション	HTTP、SMTP、POP3、FTPは自動です。 (基本的に全てのパケットをキャプチャしていますのであらゆる通信分析が可能です)	
最高速度	1000BASE-T、100BASE-TX、及び10BASE-Tに対応	

上記のスペックは予告無く変更する場合があります。



営業部

アドバンスデザインテクノロジー株式会社 代理店

<http://www.adte.co.jp>

e-mail: adt_topsales@adte.co.jp

〒183-0056 東京都府中市寿町三ツ木1-1-3三ツ木寿町ビル10F

TEL:042-354-3460 FAX:042-354-3466