

次世代ファイアウォールのログを可視化し、不正通信端末をネットワークから遮断する syslog管理アプライアンス

LOG Adapter

ログアダプタープラス

そのログ、活用していますか？
保管するだけでは意味がありません。

アクセス状況の把握や情報漏洩対策、トラブルが発生した後の調査のために、システムを横断したログ管理を行います。



特徴 その1

ログを可視化するsyslog管理機能

システムを横断したログ管理で、ネットワーク利用者のアクセス状況を一元的に把握。異なるログを任意の項目（ユーザー ID など）により関連づけ。

横断ログの検索・集計・レポート (イベント管理機能)

No.	アクション	日時	ホスト	ユーザー	URL	IPアドレス	MACアドレス
1	ログイン	2018/5/10 08:57	Switch	user01			00:00:5E:00:53:01
2	アクセス	2018/05/10 14:05	ProxySrv	user01	https://www.hcnet.co.jp	192.0.2.10	00:00:5E:00:53:01
3	アップロード	2018/05/10 14:06	Firewall	user01	https://www.hcnet.co.jp/file/?id=xxxhcnetxxx	192.0.2.10	00:00:5E:00:53:01

管理者

- 不正アクセス把握
- トラブル発生後の調査分析
- 内部統制の対応

SNMPトラップ
メール通知
不正通信端末遮断

検索性の向上に、任意のログ定義が可能。
ログ送信機器に依存せず、検索・集計・レポート、イベント管理機能を利用可能

ユーザー定義ログテンプレート
認証ログテンプレート

データベース

検索
集計・レポート
イベント管理

登録性能5,000件/秒
大容量モデルで長期保存 ※1

複数システムのログを収容する性能。大容量モデルで長期間の保存に対応。*1
*1 受信するログのサイズによって保存できる期間は変動します。
ログエクスポート機能で保存期限が過ぎたログを外部サーバーに退避も可能。

特徴 その2

IPS/IDS・ネットワーク認証機器と連携し、不正通信端末をネットワークから自動遮断

検知ポリシーを定義し、不正アクセスや障害を通知。IPSなどの脅威検知製品と連携し、不正通信端末をネットワークから自動遮断。

通常への対応

管理者

資産台帳や装置コンソールで対象端末の調査・特定

利用者へ端末切り離し依頼

利用者

初動の遅れ!

連携ソリューション

管理者

LOG Adapter

次世代ファイアウォール

認証スイッチへ命令

自動で端末を特定し自動的に切り離し実行

効率化!

利用者

遮断