

ネットワークの監視カメラセット

高価だったネットワークフォレンジックを低価格で実現！

気づいたときに証拠なし。
そうなる前に対策を！

企業の状況とニーズ

標的型攻撃による感染、情報漏洩を
**100%防ぐことは現実的に
難しい→確実な証拠を残し
説明責任を果たす**

ネットワークの証拠

(誰が?いつ?どこで?何を?どのように?)

を残す必要→**ネットワーク
フォレンジックの重要性**
がますます高まっている

課題（一般的なフォレンジック機器）

コスト

導入費・維持費用が高い。機器のみで、数千万円(数10TB)。
長期間（1年以上）保存するには**膨大なコスト**がかかる。
冗長化すると2倍のコストがかかる。

取得率

バースト時、対象トラフィックの取りこぼしがある。
キャプチャ時に**取りこぼし（パケットロス）**は発生しないか？

安定稼働

システムを24時間365日**安定稼働**できる設計となっているか？

運用

大量に貯めたデータから、目的(調査・報告等)に応じて取り出すことができない。
SSLで暗号化されていてどのようなやり取りがあったか分からない。

構成

大容量データはRAID6上のシステムに保存すべきでは？

稼働率

分析機能は常に最新の状態にする必要があるが、更新時に**キャプチャ停止時間が発生**してしまう。

課題を解決します

- ・導入維持費が**安価**！
- ・安定稼働とネットワークフォレンジック本来の目的を実現。
- ・携帯やスマホ等で多いショートパケット(最も負荷の高い64byte)を連続キャプチャ可能。
- ・**安価に長期パケットデータの保存**を実現するソリューション。
- ・大量に貯めたデータから、目的に応じてデータを取得することができる**運用支援プログラム**を提供。

パケットの
確実な取得

大量データ
の保存

効率的
な分析

GIGA運用支援プログラム

<長期保存用プログラム>

- ・PCAPファイルの取得機能
- ・自動ローテーション機能
- ・HDD使用率アラート機能

<解析支援プログラム>

- ・PCAPのフィルタ機能
- ・PCAPのマージ機能
- ・PCAPからリジェネレーション機能

解析機能

- ・Web・メール・データベース
- ・IP電話・メッセージャー
- ・動画
- ・Webメール
- ・掲示板書き込み
- ・ファイルアップロード
- ・FTP
- ・Windowsファイル共有
- ・全文検索

POINT

LOGS

ヘッダー情報等の**限定的な情報**
LOGから分析ができること

- ✓ アクセスがあった事実
- ✓ ファイルが送信された事実

何時に誰からどこに送信されたかの**限定的な情報のみ判断可能**

PACKETS

通信全ての情報
ネットワークの完全な記録
パケットから分析ができること

- ✓ いつ誰からどこに送信されたかの証拠
(全通信の記録)

何時に誰からどこに送信されたかの**情報**

＋
アクセス記録と経緯の分析/添付ファイルの復元



03-5433-6602

株式会社 ギガ ネットワーク事業部 プロダクトソリューション統括グループ
〒154-0024 東京都世田谷区三軒茶屋2-11-26 コア第二ビル FAX.03-5433-6606

www.giga.core.co.jp

g-support@core.co.jp