

## 注目を集める

脅威インテリジェンスを用いた次世代のサイバー攻撃防御ソリューション！

70以上の特許を有する「CleanINTERNETサービス」は、既知のサイバー攻撃のリアルタイムブロック&発生源の特定に加え、疑わしい通信の調査・報告まで提供することにより、**セキュリティ技術者を削減し、セキュリティ防御態勢を強化し、自動化によるセキュリティ運用負荷を大きく軽減します！**

株式会社ディックソリューション エンジニアリング

DICSE

## 株式会社ディックソリューションエンジニアリング様

## ●導入の背景

多くの取引先を持つディックソリューションエンジニアリング様にとって、ランサムウェアやエモテットなど最新のサイバー攻撃による情報漏えいや業務停止を防ぐ事は、経営上の最重要課題でしたが、それは技術面だけでなく、人的リソース面でも簡単に実施できる事ではありませんでした。

## ●導入の決め手

・従来の方法では不可能な、最新の脅威インテリジェンス(IoC:侵害の痕跡情報)を用いた自動化・リアルタイム防御

常にアップデートされる数十億の最新IoCを用いて、従来のソリューションではカバーしきれない脅威(未知の脅威を含む)に対し、リアルタイム対処。セキュリティ防御態勢の向上と自動化を同時に実現！

・疑わしい通信の調査&報告

防御要否の判定のために必要な調査はCentripetal社のセキュリティアナリストが行うので、お客様による調査作業は一切不要。

・運用は全てCentripetal社が実施

脅威インテリジェンスの更新、ルールの追加、疑わしい通信の調査&報告まで全てCentripetal社が行う為、運用負荷を大きく削減。

DICSE様が導入した  
"RuleGATE" 1100シリーズ



## 主な導入効果

業界で初めて、脅威インテリジェンスを用いたリアルタイム防御ソリューションを可能にした「CleanINTERNETサービス」の導入効果について、吉本正人氏(情通事業統括本部・課長)は以下の様に述べています。

## -----脅威の疑いのある通信の可視化-----

「当社から発生している全てのトラフィックのうち、既知のサイバー攻撃はブロックされますが、疑わしいトラフィックは危険度が高いものをCentripetal社のアナリストが調査し、その結果を週次レポートで受け取れるため、脅威の疑いのある通信を可視化できるようになり、導入効果を感じています」

## -----不正な通信の検出と遮断の判断の負担軽減-----

「運用部門ではCentripetal社から提供される週次レポートの内容から、ブロックルールへの追加要否の判断をするのみとなり、非常に運用が楽になりました」

## -----不正な通信発生源の特定と対処の迅速化-----

「当社ネットワークに接続しているパソコンは固定IPアドレスで割り当てているため、週次レポートに記載されている送信元IPアドレスおよび発生時刻の情報から不正な通信の発生源を利用者と紐づけて特定できるため、早期発見と対処が容易になり、運用面でとても役に立っています」

## -----パソコン以外のデバイスの通信を可視化-----

「ネットワークカメラなどパソコン以外のデバイスから発生したトラフィックについて、接続先の情報を元に意図した通信か否かの判断が容易に行えています」

## -----広告など業務との関係性の低い通信の特定と遮断による帯域への負荷の軽減-----

「脅威以外にも、業務と関係性の低いと考えられる通信もブロック対象として推奨してもらえするため、今まで気付かなかった不要なトラフィックを削減し、ネットワーク帯域の有効活用が可能となりました」

まずは1ヶ月間の無償トライアルで導入効果を御確認下さい！

"RuleGATE" Edge  
小型モデル

4.3cm(H) x21.6cm(W) x26cm(D)  
ラックマウントブラケット付き



クラウド環境対応の  
Cloud RuleGateも  
近日リリース予定

日本総代理店

コーネットソリューションズ株式会社

Cornet  
Solutions

(TEL) 03-5817-3655 (代)

www.cornet-solutions.co.jp