Technical Solution
テクニカル ソリューション

パケットキャプチャデータを活用し外部からのアクセスを自動集計・見える化

インターネットを利用中に，「時々通信が遅くなる」もしくは「つながらなくなる」などの故障申告があります．原因の１つとして，外部からの不正アクセスにより，回線に余分な負荷がかかっている場合があります．このような状況を把握するためには，パケット解析が有効となりますが高度な IP スキルが必要となります．NTT 東日本技術協力センタでは，パケットを簡易にキャプチャする装置を活用し，簡単な PC 操作で不正アクセスによるセキュリティリスクを見える化するツールを開発しました．

開発の背景

故障修理の現場では，電話やPCが使用できなくなるなどのさまざまな故障申告に対応しています．その中で，フレッツ光などでインターネットをご利用中のお客さまから，「時々通信が遅くなる」「つながらなくなる」といった故障申告を受けることがあります．これらの事象の一要因として，悪意のあるユーザからのサイバー攻撃（多量のパケットを送りつけるなど）により，回線に負荷がかかり，インターネットなどの通信に支障をきたす場合があります．それらサイバー攻撃からPCを守るために通常のセキュリティ対策としては，セキュリティソフトを用います．しかし，それらのソフトは，既知のセキュリティリスクからPCを守ることはできますが，未知の攻撃などの状況を明示し，セキュリティリスクを示すことができませんでした．

これら悪意あるユーザからの不正アクセスによる回線の負荷増加などの脅威を明示するためには，IP区間に流れている全パケットから不正アクセスとなり得るパケットを抽出し通信内容を解析することが有効となります.そのためにはWiresharkなどのソフトウェアを用いて，高度なIPスキル保有者が解析を行う必要があり，解析自体にも時間を要していました．これら状況をかんがみ，より簡単に，より早く不正アクセスの脅威を明らかにするために，簡単なPC操作で不正アクセスによるセキュリティリスクを見える化するツール「不正アクセスカウンタ」の開発を行いました．

表１　トイキャプの諸元

項　目	仕　様
容量	約25 GByte
寸法	130×95×28 mm
重量	220 g
Ethernet 規格	1000BASE-T（ミラーリングにてキャプチャ）
キャプチャ性能	最大100 Mbit/s（パケットサイズに依存）

パケットキャプチャの簡易化

パケットデータを用いて不正アクセスによるリスクを明らかにするには，まずIPパケットをキャプチャする必要があります．パケットキャプチャを専用に行う装置も販売されていますが，値段が高価であったり，操作が複雑であったりと，すべての現地対応者が作業するには障壁がありました．これらの課題を解決するためには，技術協力センタで仕様検討した簡易パケットキャプチャ装置「トイキャプ*」が活用できます[(1)]．トイキャプの諸元を**表１**に示します．トイキャプは小型・軽量で廉価なパケットキャプチャ装置であり，電源ケーブルとLANケーブルをトイキャプに接続するだけで自動的にパケットキャプチャを開始します．操作が簡単なので短時間でパケットキャプチャの準備ができ，かつ小型であるため現地対応者が携行しやすいので，パケットキャプチャが可能な機会を逃すことなく設置することができます．

「不正アクセスカウンタ」の機能と特徴

「不正アクセスカウンタ」では，トイキャプを用いて

＊ トイキャプ：グリーン株式会社とNTT東日本技術協力センタ　ネットインタフェース技術担当で共同制作した小型軽量の簡易パケットキャプチャ装置．

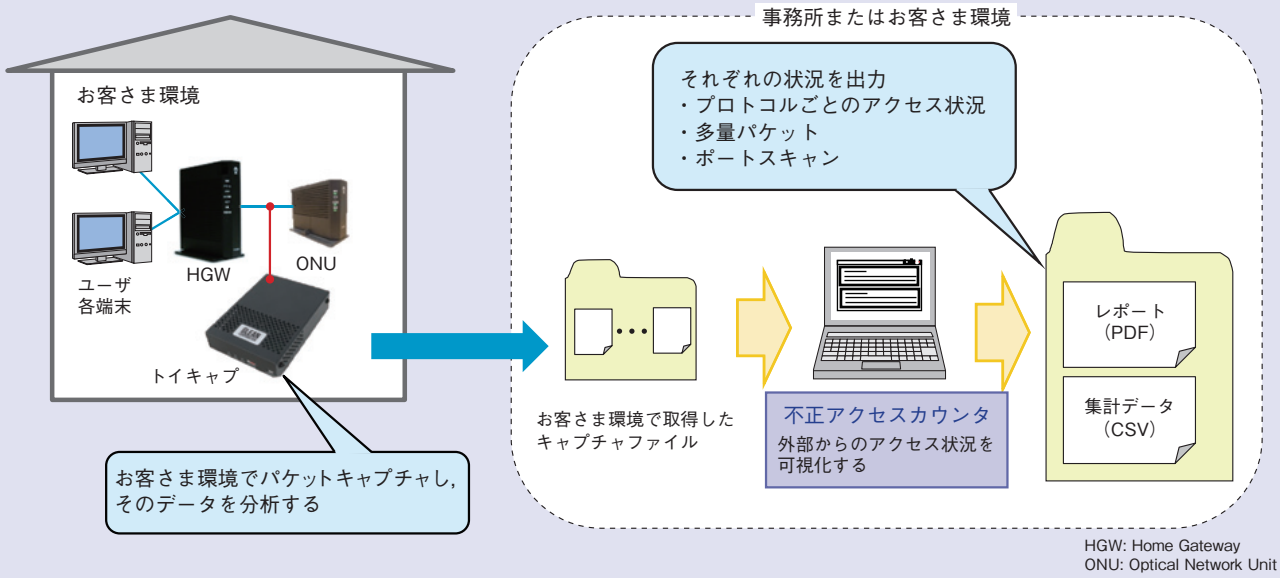

図　不正アクセスカウンタの使用イメージ

お客さま宅内でキャプチャしたIPパケットを読み込ませることによって，外部からのアクセスをカウントし，結果をCSVファイルの集計データとPDFファイルのレポートとして出力することができます．「不正アクセスカウンタ」の使用イメージを**図**に示します．「不正アクセスカウンタ」は，解析したいパケット群が格納されているディレクトリを指定するだけの簡単なPC操作で使用できます．

「不正アクセスカウンタ」は，読み込ませたすべてのパケットの中で外部からの接続要求パケット（TCP SYNなど）を抽出してカウントします．外部からのアクセスかどうかを判別する方法は，パケット送信元装置MAC（Media Access Control）アドレスのベンダコードを抽出して，そのベンダコードが宅内装置のMACアドレスベンダコードと一致するかどうかを判別し，一致しないパケットを外部からのパケットとして認識する仕組みとなっています．外部からのアクセスと認識されたパケットは，不正アクセスとなり得るリモートシェル接続やファイルサーバへの接続などのサービスごとにカウントされます．サービス種別の判別は，通信に使用するプロトコルおよびポート番号に基づいて実施されます．「不正アクセスカウンタ」の検出項目一覧を**表2**に示します．各検出項目のうち，代表的な項目のセキュリティリスクについて記載します．

⑴　リモートシェル

LAN内端末にログイン可能で，遠隔操作されてしまうおそれがあります．その結果，踏み台とされて，他のシステムなどへのサイバー攻撃に利用されるおそれがあります．

⑵　Windows共有サービスおよびファイルサーバ

LAN内端末のフォルダ内部が閲覧され，保存しているファイルを抜き取られてしまうおそれがあります．

⑶　短時間多量パケット

DoS（Denial of Service）攻撃を受けている可能性があり，多量のパケットを受信してしまうことで，通信容量や処理能力が飽和状態となり端末などが応答できなく

表2　不正アクセスカウンタの検出項目

検出項目	検出内容	検出条件
リモートシェル	機器への遠隔ログイン・操作を行うtelnetやsshで使用するポートへのアクセス	TCP SYNの宛先ポート番号が22，23のもの
ping	機器の死活監視などで使うpingのリクエスト	ICMPのTypeが8（echo request）のもの
DNS	HPを見る際などにURLとIPアドレスの解決を行うDNSで使用するポートへのアクセス	UDPの宛先ポート番号が53でQR，OPECODEが共に0（通常のクエリ）のもの
電子メール	電子メールの送信・受信で使うSMTP・IMAPで使用するポートへのアクセス	TCP SYNの宛先ポート番号が25，143のもの
Webサーバ	ブラウザでHPを見る際などに使われるhttpやhttpsで使用するポートへのアクセス	TCP SYNの宛先ポート番号が80，443のもの
Windows共有サービス	Windows端末どうしのフォルダ共有やネットワーク管理で使うSMBやNBNSで使用するポートへのアクセス	TCP SYNの宛先ポート番号が139，445のもの UDPの宛先ポート番号が137，138のもの
ファイルサーバ	FTPサーバとのファイルのやり取りで使うFTPで使用するポートへのアクセス	TCP SYNの宛先ポート番号が21のもの
IP電話	IP電話の呼制御で使用するSIPのうち通常使わないOPTION，MESSEGEパケット	UDPの宛先ポートが5060でmethodsがOPTIONS，MESSAGEのもの
ネットワーク設定サービス	IPアドレス取得などで使うDHCPで使用するポートへのアクセス	UDPの宛先ポートが67でメッセージタイプがDISCOVER，REQUESTのもの
接続要求	TCPで通信しようとしてくるアクセス	TCP SYNパケット
短時間多量パケット	1秒間に多量のパケットが送られてくる（DoS攻撃イメージ）状況	同一IPアドレス，ポートに対するパケット数が1秒間に10を超えたもの
ポートスキャン	短時間に発生した多数ポートへのアクセス（ポートスキャン）	同一IPアドレスから1秒間に10以上のポートへパケットが送られてきたもの

なるおそれがあります．

⑷　ポートスキャン

さまざまなサービスのポートへ接続要求を行うパケットを送信し，アクセスを許可しているポートがないかどうかを探索する行為で，外部の悪意あるユーザから，脆弱性などがないかを調査されている可能性があります．

他の項目についても，Webページ閲覧やメール送受信など一般的な利用では，外部からの接続要求が発生しないサービスです．

今後の展開

トイキャプを用いてキャプチャしたパケットを「不正アクセスカウンタ」で解析することにより，不正アクセスによるセキュリティリスクの見える化を，短時間かつスキルレスで実現することができます．今後は，現地対応者が「不正アクセスカウンタ」を用いて，お客さまにとって安心・安全が実現できるセキュリティサービスを提案するなどの利用シーンを検討していきます．さらに，故障修理においてパケット解析を行っているノウハウを活かし，パケット解析を自動で行う新たなツールなども開発していきます．

■参考文献

⑴　テクニカルソリューション：“廉価版キャプチャ装置によるパケットキャプチャの新たな活用方法の模索，” NTT技術ジャーナル，Vol.29，No.1，pp.50-51，2017.

◆問い合わせ先

NTT東日本
ネットワーク事業推進本部　サービス運営部
技術協力センタ　ネットインタフェース技術担当
TEL　03-5480-3702
E-mail　nif-ngn-ml@east.ntt.co.jp