3　トレーサブルネットワーク技術

3　Traceable Network Technology

3-1　トレーサブルネットワーク技術の研究開発

3-1　Research and Development of Traceable Network Technology

門林雄基
KADOBAYASHI Youki

要旨

インターネットに代表される開放型のネットワークでは、ネットワークを構成するハードウェア・ソフトウェアの安全性向上とならんで、ネットワークにつながる計算機とその利用者を対象とした安全性向上についても考える必要がある。そのためにはネットワーク内の状況を把握する能力が必要不可欠であるが、ネットワークは規模拡大、広帯域化を続けており、目視などによる状況把握を補う技術開発が求められている。本稿では、大規模かつ高速なネットワークにおいて高精度かつ遡及可能な状況把握を可能とするトレーサブルネットワークの研究開発について概要を紹介する。

Open networks mandate improved security of connected devices and their users, as well as improved security in both hardware and software of networking nodes. Situation awareness is thus an essential capability, although scale and speed of networks keep continuing growth. It is thus imperative to develop technologies to complement labor-intensive monitoring of networks. This article describes the research and development of traceable networking technology that enables accurate and accountable situation awareness across large-scale, high-speed networks.

[キーワード]
ネットワークセキュリティ，トレーサブルネットワーク
Network security, Traceable network

1　はじめに

近年、インターネットに代表される開放型のネットワーク技術が世界的規模で普及した結果、近年のグローバルな経済的発展をもたらすと同時に、さまざまな緊張をもたらす事態にもなっている。開放型のネットワークでは、利用者数の増加によりネットワークそのものの価値が飛躍的に高まる一方で、価値観の対立や知識格差、経済格差など様々な問題をはらんだやりとりが常に発生しうる。そのような開放型のネットワークの在り方については批判もあろうが、いっぽうで知識格差、経済格差や価値観の対立を超えたコミュニケーション基盤は近年のグローバルな発展の原動力となっており、これを安全に使いこなす能力は大きな競争力の源泉である。

プロジェクト発足当時、このような開放型のネットワークを対象として安全性向上を考えた場合、そもそも我々は基本的な道具を有していないという状況であった。つまり、ネットワーク内において起きたことを観測する充分な手だてを持たず、また、このことから再発防止策を練ることも難しい状況であった。

1.1　ネットワークにおける状況把握の必要性

ネットワーク内でいま何が起きているのか、と

いう問いに答える取り組みとしてはネットワークの可視化や監視に関する先行研究を挙げることができる。可視化と監視は状況把握のためにきわめて有用な手段であり、前中期計画におけるセキュリティ高度化グループでも取り組みがなされてきた。これらの取り組みや実ネットワークにおける運用経験をふまえ、我々はプロジェクト発足当初、以下の4つの限界を認識し、これらに対する挑戦がつぎの研究の潮流をかたちづくるであろうと考えた。

1) 規模の限界：一定以上の規模のネットワークでは目視による状況把握が難しくなる。
2) 精度の限界：従来の単純なパターンマッチングや目視による検知では精度が著しく劣化する。
3) 速度の限界：ネットワークの高速化により目視による監視では追いつかなくなる。
4) 時間の限界：実時間で何が起きているのかを把握することが難しくなる。

これらの課題を一度に解決することは、グループ単独では困難であるが、同時に、このようなグランドチャレンジを設定し国内外の研究グループと連携する、またとない機会でもあった。

1.2 トレーサブルネットワーク

1.1 で述べた4つの限界は、裏を返せば、1つのグランドチャレンジに集約することができる。それは簡潔に表現すると「大規模かつ高速なネットワークにおける、高精度かつ遡及可能な状況把握」となる。これを実現可能なネットワークを我々はトレーサブルネットワークと呼び、研究目標として設定した。高速なネットワークとしては、100Gbpsのネットワークを想定した。これはプロジェクト終了時のバックボーン技術として想定される帯域幅であった。また高精度とは、誤検知率1%以下であることとした。これは従来の検知方式において誤検知率が10%程度であったことから、飛躍的改善を狙ったものである。

この大目標に対し、我々は情報科学の最新の研究成果を総動員してアプローチを模索することからはじめた。

2 トレーサブルネットワーク研究への取り組み

トレーサブルネットワークを実現するためには、運用者によるログや可視化システムの目視だけではもはや不十分である。このため認識機能の大部分をコンピュータで代替して、運用者の負荷を下げる必要がある。

従来、ネットワークセキュリティの現場において運用者の負荷となっているのは誤検知を切り分ける作業であった。検知精度を上げ、誤検知を減らす事でそのような負荷を減らす事ができ、ネットワークの規模拡大により効率的に対処していくことができる。しかしながら検知精度向上への取り組みとしては、従来、セキュリティ専門家が既存の機械学習アルゴリズムを適用しているものが多く、機械学習の専門家による対象領域の理解と対象領域にあわせたアルゴリズムの最適化にはほとんど取り組まれていない状況であった。

またインターネットに代表される大規模なネットワークは、単一事業者だけに閉じるものではない。このような環境では通信の秘密などの法的要請から、他の事業者に詳細情報を開示することなく問題の対処にあたることが求められる。言い換えれば、プライバシの確保と問題への対処能力を両立することが求められている。

その一方で、ネットワーク上でのアプリケーションの重要性がますます大きくなり、迷惑メールをはじめとしてアプリケーションで起きた問題についても状況把握し、対処する能力が求められている。つまり、ネットワークの中枢から、アプリケーションへとカバレッジの向上を求められていると言える。

これらの考察から、当グループではトレーサブルネットワーク実現へむけての多面的な取り組みを行った。目標達成のためには、アルゴリズム、システム、プロトコルなど多方面にわたる取り組みが必要であった。以下ではそれらの取り組みを「事案対応の効率化」「カバレッジの向上」「解析能力の向上」および「プライバシの確保」という4つの柱で整理して紹介する。

2.1 事案対応の効率化

前述したように高い検知精度は対応業務の効率

化に直結するため、より高い精度を有する検知アルゴリズムの開発が望まれていた。しかしながらプロジェクト発足当時、機械学習アルゴリズムではネットワークセキュリティにおけるパターン認識問題の性質を十分に考慮できていたわけではなかった。それらは以下の4点にまとめることができる。

1) クラス偏差：クラス間の頻度分布に著しい偏りがある。
2) 多クラス：正常／異常といった2値分類問題ではなく、3つ以上のクラスへの分類問題を考える必要がある。
3) インクリメンタル：パケットなど続々と到着するデータを対象として認識を行う必要がある。
4) オンライン：実時間で分類・認識を行う必要がある。

これらの性質を有し、かつ精度の高い機械学習アルゴリズムを開発するためニュージーランド・オークランド工科大学と共同研究を行い、サポートベクタマシンの多クラスへの拡張、GPU（Graphics Processing Unit）を用いた高速実装などに取り組んだ。この結果、従来のCPUによる処理と比べて50倍という高速化を達成することができ、また迷惑メールの検知などいくつかの用途において誤検知率1%以下を達成することができた。

さらに、検知した問題を正確かつ迅速に隣接業務や隣接するネットワークに伝えるためには命名規則や採番規則、メッセージ形式などを標準化する必要がある。これらについてもプロジェクト3年目よりITU-Tでの標準化に取り組んだ結果、X.1500勧告シリーズ（サイバーセキュリティ情報交換技法CYBEX）として国際的な取り組みに発展した。X.1500勧告シリーズは、サイバーセキュリティ情報の識別、構造化、検証、交換などのそれぞれの機能を提供するモジュール性の高い勧告案から構成され、それらを組み合わせることでサイバーセキュリティ情報交換が実現される。CYBEXをセキュリティ機器およびセキュリティ対策組織が採用することで、命名規則や採番規則、メッセージ形式などが標準化され、検知した問題や対応状況の詳細を隣接業務や隣接するネットワークにより効率的に伝えることができるようになると期待される。

2.2 カバレッジの向上

プロジェクト発足当初、アプリケーションにおいて状況把握を困難にする要因として最も懸念されたのがファイル共有アプリケーションと仮想マシンであった。このため、これらを対象とした観測技術の研究開発に取り組んだ。仮想マシンはオペレーティングシステム技術の一種と捉えることもできるが、ネットワークから見るとあらゆるアプリケーションを実行可能なアプリケーションコンテナとして捉えることもできる。このため仮想マシンをハイパーバイザ（仮想マシン実行環境）から観測可能とするためのハイパーバイザの機能拡張に取り組み、仮想マシンの挙動観測技術を開発した。またファイル共有アプリケーションにおける最も大きな脅威として情報漏洩が挙げられるが、情報漏洩による情報の拡散範囲を観測するシステムの構築に取り組み、複数のアプリケーションを対象として可測性を確保することに成功した。

実際にこれらの要素技術をインターネットで用いる際には、あとで述べるプライバシ確保のための技術と組み合わせて用いることが求められる。

2.3 解析能力の向上

ネットワーク内で遡及して状況把握を行うためには、高い精度で問題の兆候を捉えておくことはもちろん重要であるが、それに加えて、兆候とその後の状況変化を関連づけることができなければならない。そのためには兆候を解析する能力が必要となる。

兆候となるのは、たとえば一見データのように見える文字列である。しかしながら特定のシステムに与えられるとこれがプログラムとして解釈され、システムの停止や情報漏洩につながってしまうというものである。これを攻撃ベクタと呼ぶ。

システムの停止などの明らかな障害は容易に観測可能であるが、それを引き起こした真の原因がどのデータ系列であるのか、といったことを探るためには小規模なシステムを再現し、候補となるデータ系列を与えてみなければならない。

このようなことから、まず構内網やインターネット・バックボーンを再現可能な再現ネットワーク技術の研究開発に取り組み、これを礎として

小規模攻撃再現システムを構築した。再現ネットワーク技術を用いることで、ネットワーク設計に基づいて構内網やインターネット・バックボーンを一定の規模で再現し、その中で問題となるシステムを動作させることができる。この技術をもとに一定の隔離を行い、攻撃ベクタの投入、遠隔操作・遠隔観測のための機能を付与したものが小規模攻撃再現システムである。実際にこのシステムを用いて大学研究機関が遠隔地から攻撃ベクタを投入し、解析を行うことが可能であった。

2.4 プライバシの確保

これまでに述べてきたような高い観測・検知・解析能力は、インターネットのような一般利用者向けのネットワークにおいて誤用されるとプライバシを損なう恐れがある。このためプライバシの確保とこれらの能力の両立についても研究に取り組んできた。

そのような取り組みとして、まず秘匿計算プロトコルを挙げることができる。これは暗号化したまま（つまり内容を見ずに）乗算や加算などの演算ができる準同型暗号の性質をつかって、2者間でお互いに内容を明かさずに照合処理などができるというものである。具体的には2者が同じ事象を観測したかどうかを、互いに観測内容を明かさずに知る事ができる秘匿共通集合計算という問題に注目し、この問題の計算量を飛躍的に短縮することに成功した。この問題は遡及可能性とプライバシ確保を両立するために必ず解かなければならない問題である。

また、このような秘匿計算プロトコルは、問題発生箇所を特定するために用いることができる。これにより複数事業者により構成される開放型ネットワークにおいても、他の事業者に詳細情報を開示することなく、かつ協調して問題の対処にあたることができる。

3 トレーサブルネットワーク研究の展開

トレーサブルネットワークを構成するための要素技術については十分な研究開発を行うことができたと考えるが、実地へのシステム投入は一部にとどまっていることから、実際にグランドチャレンジを達成したと言い切れる状況にはまだない。

しかしながらプロジェクト5年間の成果として110本を上回る論文を発表しており、また再利用可能な形でソフトウェアのソースコード等を残していることから、平成23年度から始まった新たな中期計画や今後立ち上がる実証実験において成果を活用し、トレーサブルネットワークが目指した性質を実現することは可能であると考える。

新たな中期計画では、従来プロジェクト単体での取り組みであった事案対応の効率化、プライバシの確保などのテーマが研究所全体での取り組みに活かされている。また、いささか逆説的ではあるが、本プロジェクトの成果を可視化による状況把握に活かすことも可能であると考えられる。

3.1 研究目標の共有

本プロジェクトでは、常勤のメンバーによる研究だけに頼るのではなく、彼らが所属する研究コミュニティにおいて我々の課題設定を共有することをひとつの目標として取り組みを進めてきた。

その結果、機械学習の分野においては国際会議ICONIPにおいてDMC（Data Mining for Cybersecurity）コンペティションを設置することができ、機械学習分野において音声認識や画像認識とならんでサイバーセキュリティ分野のパターン認識に取り組んでもらう素地をつくることができた。

またサイバーセキュリティ標準としてX.1500（CYBEX）において組織間の情報交換に取り組むための枠組みをつくることができた。CYBEXはセキュリティ技術をネットワーク化するという大きな技術的方向性を示唆しており、標準化によって、国内外の研究機関やセキュリティサービス事業者においてこの方向性を共有することができた。

3.2 教育への成果展開

解析能力を向上させるための取り組みとして、マルウェア対策研究人材育成ワークショップへの再現データセット提供、奈良先端大・北陸先端大・京都大・大阪大の4大学が中心となったセキュリティ専門家育成カリキュラムIT-KEYSへの再現環境提供を行ってきた。マルウェア対策研究人材育成ワークショップへの取り組みにおいては、サイバークリーンセンター・情報処理学会が

中心となって作成したMWSデータセットをもとに、小規模攻撃再現環境の技術を応用して作成した再現データセットを提供し、再現環境をもたない大学等の若手研究者達がさまざまなデータ解析方式を開発・発展させる素地をつくることができた。またIT-KEYSでは平成20年度より毎年20名を超える大学院生を対象として、セキュリティ専門家育成の一環として小規模攻撃再現環境を提供した。これにより、企業ネットワーク等で起こりうるさまざまなセキュリティ上の問題について、問題発生のメカニズムおよび観測手法について実ネットワークに近い環境のもとで学び、対策について考える他に類をみない体験演習環境を構成することができた。

3.3　事業者への波及効果

特に情報漏洩に関する状況把握の技術、プライバシ確保と解析能力を両立する技術については小規模な実証研究などを通じてセキュリティサービス事業者からも高い評価を得ている。その一方で、研究機関が作成したソフトウェアが事業者において直ちにサービス展開できるものでないこともまた明らかである。

またX.1500勧告シリーズにおいてセキュリティ技術のネットワーク化に関する方向性が示されたことで、セキュリティサービス事業者におけるサービス構築のありかたも大きく変わってくる可能性がある。

これらについてはプロジェクト終了後も引き続きフォローアップ作業をつづけている。

4　おわりに

開放型のネットワークを対象として安全性向上を考えた場合、規模、精度、速度、時間の4つの限界に対して挑戦を行っていかなければならない。本稿ではその具体的取り組みとして、大規模かつ高速なネットワークにおいて高精度かつ遡及可能な状況把握を可能とするトレーサブルネットワークの研究開発について概要を紹介した。本プロジェクトの成果は研究コミュニティへの展開、教育カリキュラムへの応用、標準化などさまざまな方法で展開しており、セキュリティサービス事業者やネットワークサービス事業者への波及効果も今後期待される。

ネットワークセキュリティに関する研究はまだ道半ばである。これはセキュリティ技術のネットワーク化、ネットワーク技術のセキュリティ強化という2面性をもったアプローチが必要とされる融合領域であるが、これら2つの技術を同時に理解している研究者は依然として少ないため、プロジェクト研究という形で共同して問題にあたることが引き続き求められている。

謝辞

本プロジェクトでの研究に真摯に取り組んでいただいた研究グループメンバー各位、ならびに研究遂行の機会を与えていただいた関係者各位に感謝します。

（平成23年6月15日 採録）

門林雄基（かどばやし ゆうき）
ネットワークセキュリティ研究所
専攻研究員／
奈良先端科学技術大学院大学
情報科学研究科准教授　工学博士
IPトレースバック、サイバーセキュリティ