2　トレーサブルネットワークの研究開発

2 Research and Development of Traceable Network

門林雄基
KADOBAYASHI Youki

要旨

今日のインターネットでは、セキュリティ上の問題が起きたときに、その根本原因を解明し、再発防止につなげるための措置が取られない場合が多く、セキュリティ対策の効率を低下させる一因となっている。本稿ではこの問題を解決するために三つのメカニズムが必要であることを指摘し、ネットワーク技術とセキュリティ技術の複合領域における取組の必要性について述べる。トレーサブルネットワークの研究開発において、アーキテクチャ、アルゴリズム、システム、ネットワークの 4 領域における研究手法を組み合わせ、複合問題の解決に取り組んでいる。本稿ではその取組の概要と、本特集における各論文との関連について述べる。

In today's Internet, necessary actions for root-cause analysis and recurrence prevention are ignored in most of the security incidents, resulting in the overall inefficiency of security countermeasures. In this paper, we argue that three mechanisms are necessary to address this problem. Then, we discuss the necessity of research efforts in the intersecting areas of networking technology and security technology. Our traceable network research group tackles these challenges by combining research disciplines of architecture, algorithm, system and networking research. This paper gives overview of our research efforts, along with connection to subsequent papers in this special issue.

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

1　まえがき

今日、インターネットは簡便な連絡網や情報交換ツールにとどまらず、商取引や娯楽など様々な目的に用いられている。商取引において信頼性や機密性が求められる一方で、娯楽目的では偽名や匿名でのメッセージがあふれている。インターネットはフラットなネットワークであるので、これらの様々なセキュリティ要件を持つコミュニケーションが渾然一体となり、意図しない相互作用を引き起こしている。言い換えれば、本人確認情報が付与された、セキュリティレベルの高い情報システムと、偽名や匿名による、セキュリティレベルの低い情報システムが並存しており、プログラムのバグや利用者の操作ミスなどの機会にセキュリティレベルの異なる情報システムに接点が生じ、望まれざる結果を招いている。

インターネットでは、利用者の知識不足や操作ミス、偽名や匿名でのやりとり、なくならないプログラムのバグ[1]-[3]などが複合的な原因となって、フラットなネットワークにおける発信者責任の回避、誤用や放任の結果として起きたことに対する説明責任の放棄が横行している。結果として、何か悪いことが起きたときにその根本原因が追求されないため、際限なく同じ問題が起きることになる。このことは、セキュリティ対策を非効率なものとしている一因でもある。

より安全なインターネットを作るためには、

三つのメカニズムが欠けていると考えられる。第一に、発信者の責任を問うメカニズムが挙げられる。今日のインターネットでは、問題のある通信を観測したときに、その発信源を探知することが非常に困難である。このため、当該通信と発信者の紐付けを行い、発信者の責任を問うことができない。

第二に、原因究明のためのメカニズムが挙げられる。これまでのインターネットでは、「どこで何が起きているか」を把握することすら困難であった。再発防止の観点からは、これに加えて、「なぜ、どのように事故が起きたか」を説明できることが必要不可欠であるが、これまでは原因究明のために要する時間が膨大であった。

第三に、対策技術を浸透させるための、インセンティブ・メカニズム[4]が挙げられる。これまで数多くの効果的なセキュリティ対策技術が開発・製品化されているが、インターネット全体でみればその導入規模は限定的である。これらの装置の多くは単体で動作するのみで、他の装置と連動して大きな相乗効果をもたらすものではない。また複数台で連動する製品であっても、他社製品との相互接続性がなく、連動できるのは自社製品に限られるなどの制約条件があるのが一般的である。その結果、セキュリティ対策製品を導入するためのインセンティブに乏しいのが現状である。

2 トレーサブルネットワーク

前節で述べた問題は、ネットワーク技術の特性とセキュリティ技術の特性の相互作用によって起こっていると考えられる。これまではネットワーク技術開発の視点からネットワークへの要件を整理し、セキュリティ技術開発の視点からセキュリティ要件を整理していたが、今日の多くの問題がネットワーク技術とセキュリティ技術の複合領域において起きているとすれば、従来とは異なるやり方で問題に取り組む必要がある。

トレーサブルネットワークグループでは、ネットワーク技術とセキュリティ技術のギャップを埋めることが重要であると考えており、ネットワーク技術開発の視点からのセキュリティ要件の整理及びセキュリティ技術開発の視点からのネットワーク要件の整理を行い、以下に述べるような課題を抽出した。

まずセキュリティ要件について述べる。従来、セキュリティ要件としてはOECDのガイドライン[5]で示された秘匿性、一貫性、可用性に加えて、ISO/IEC TR 13335[6]で示された真正性、責任追跡性、信頼性が一般的に用いられている。ネットワーク技術開発の視点からは、これらの特性に加えて、三つの特性が必要であると考えられる。

(1) 相互接続性：これまで数多くのシステムやアルゴリズムが開発されてきたが、これらは運用者とのインタラクションのみを前提としている。セキュリティ対策を効率化し、運用者の重荷を減らすためには、これらのシステムやアルゴリズムが相互に連携することが必要である。
(2) ドメイン分割：インターネットは複数の組織（ドメイン）から構成されているため、問題が発生したときに切り分けを行い、関係するドメインのみを含む連絡網を構成することが求められる。また、組織を超えてセキュリティ上の問題に対処する場合には、プライバシを確保することが特に必要となる。
(3) 規模拡張性：インターネットは帯域幅で集計すると毎年倍のペースで拡大している[7]ため、システムやアルゴリズムの実現にあたっては、このペースに追従可能な規模拡張性を有することが求められる。

次にネットワークへの要件について述べる。セキュリティ技術開発の視点からみると、以下の特性が求められると考えられる。

(1) 責任追跡性：ネットワーク上で観測された問題に対し、なぜ起きたのか、どのように起きたのかをさかのぼって説明できることが求められる。
(2) 可用性：特にアプリケーション層において、単一障害点を解消し、アクセス集中の影響を受けにくく、大規模な障害が起きないような高い可用性を有することが求められる。

我々の研究グループでは、ネットワーク技術とセキュリティ技術にこれらの特性をもたらすような研究開発に取り組んでいる。またこれら

に加えて、以下のようなエンジニアリングの側面からの目標設定を行っている。

1. 原因究明プロセスの効率化：これまで数日かかっていた原因究明作業を数時間、数十分へと短縮する。
2. 問題領域のカバレッジ：ネットワーク上で用いられる様々なアプリケーションを対象として、責任追跡性や可用性を向上させる方式やシステムを開発する。

3　トレーサブルネットワークの実現に向けて

これまでに述べた要件を満たすトレーサブルネットワークを実現するためには、理論だけ、あるいはシステム開発だけといった取組では不十分である。我々の研究グループでは、アーキテクチャ、アルゴリズム、システム、ネットワークの 4 領域において取組を進めており、これらの成果を組み合わせることによって初めて、さきに述べた要件を満たすことができると考えている。

トレーサブルネットワークの実現において、第一に重要なのがアーキテクチャである。トレーサブルネットワークのアーキテクチャを構成する要素としては、様々なアルゴリズムによる計算機及びネットワークの状態観測と抽象化、それらを入力として判断を行う並列推論エンジン及び判断の結果を受けて証拠保全や解析を行うシステムが挙げられる。現在、これらの要素を相互に接続し、系として動作させるためのメッセージバスの実現に取り組んでおり、今年度中に初回の結合実験を行い、アーキテクチャの有用性を検証する予定である。

なお、同一組織内ではヘッダのみならずペイロードの一部を用いて、システム間の連携を図ることができるが、組織を超えてシステムを連携させるためには、ヘッダやペイロード情報を開示せずに同一の事象に取り組む必要がある。このためプライバシ確保型の暗号プロトコルの実用化に取り組んでいる。具体的には、高速なプライバシ確保型の暗号プロトコルの設計、安全性の検証及びマルチコアプロセッサを活用した高速な実装である。その理論的取組の詳細については本特集の論文**3-1** を参照されたい。

アルゴリズム研究としては、高い精度で、かつ高速にネットワークや計算機内の異常を検知できる機械学習アルゴリズムの開発に取り組んでいる。機械学習を応用するためには、まずデータセットを拡充し、かつアルゴリズムの優劣を比較できる環境を整える必要があり、現在これらの点に注力して研究開発を行っている。

これらのアルゴリズムによる検知結果を入力として、並列推論エンジンによって各システムが駆動される。並列推論エンジンについては並行論理型プログラミング言語を応用することが可能であると考えており、このための処理系の開発を進めている。詳細については論文**6-1** を参照されたい。

システム研究としては、様々なアプリケーションを対象とした研究開発と、新たなシステムソフトウェア技術を応用した研究開発の両面において取組を行っている。まずアプリケーションについては、P2P 型のファイル交換ソフトウェアにおける責任追跡性の確保に取り組んでいる。P2P 型のファイル交換ソフトウェアは情報漏えいにおける拡散経路として用いられており、対策が急務である。このような取組の一端を論文**5-1** にて紹介している。

次に、新たなシステムソフトウェア技術としては、仮想マシン技術と分散ストレージ技術の応用に取り組んでいる。我々の研究グループでは、仮想マシンモニタを改良し、問題が起きたときに問題発生箇所を記録しておくことで責任追跡性を確保できると考えている[8]。また分散ストレージ技術については、ネットワークからの証拠保全に必要な I/O 性能を常に達成できるだけの規模拡張性を確保することが重要であり、このため、グリッドコンピューティング、クラスタファイルシステム、オーバーレイネットワーク[9] など異なる技術領域において開発されている分散ストレージ技術を比較検討し、その規模拡張性を明らかにしていく予定である。分散ストレージ技術については論文**6-2** にて詳述している。

ネットワーク研究としては、問題の発生源となるような悪性プログラム（マルウェア）の挙動を隔離されたネットワークを用いて解析し、原

因と結果のデータベースを構築するための技術開発に取り組んでいる。このような再現ネットワークにおける隔離解析技術については論文**4-1**にて紹介する。

4 議論：より安全なインターネットは実現可能か

以上の節では、より安全なインターネットの実現に向けての一つの取組として、トレーサブルネットワークの研究活動の概要について述べてきた。しかしながら我々のグループでは、より安全な、ただ一つのインターネットが実現できるとは考えていない。冒頭にも述べたとおり、今日のインターネットでは、そもそも正反対のセキュリティ要件を持つ商取引と娯楽が、ただ一つのインフラストラクチャに多重化されており、このことが問題の根源であると言える。

プログラムのバグが根絶され、かつ利用者の操作ミスが全くなくならない限り[10]、安全なインターネットを実現するためには「高信頼インターネット」と「自由インターネット」を分ける必要があると考えられる。高信頼インターネットでは、利用者や計算機は認証され、アプリケーションはすべてセキュリティ対策が施されている。このようなインターネットは、機密性や完全性、責任追跡性などの基本的セキュリティ要件を必須とする電子商取引や電子政府にとってのビジネスプラットフォームとして用いられると考えられる。一方、自由インターネットでは、アプリケーションは任意のプロトコルを用いることができ、また利用者の識別方法についても制約がないため、研究者や開発者にとってのイノベーションプラットフォームとして用いられると考えられる。このような二分されたインターネットの下では、セキュリティ技術は高信頼インターネット向けに作られ、革新的なアプリケーションは自由インターネットの下で作られることになると考えられる。

一見、大胆な仮定のようにも思えるが、現実のインターネットでは二分された構造がいったんは作り上げられたことに注目すべきである。具体的には、企業などのファイアウォール内のネットワークと、それ以外のネットワークである。現実には二分された構造を作り上げることに対する社会的コンセンサスがなかったため、電子メールにおいてフラットなコミュニケーションを許容し続け、その結果としてメールでのウィルス感染などの事故が相次ぎ、二分法は瓦解することとなった。現在はエクストラネット、あるいは特定の迷惑メール対策技術を用いるユーザ企業のゆるやかな連合など、形を変えつつも二分されたインターネットへの試みが続けられている。

5 むすび

本稿では、より安全なインターネットを作るための三つのメカニズムについて述べ、ネットワーク技術とセキュリティ技術の複合領域で起きている問題に対処するためには、複合的な要件定義を行う必要があることを指摘した。トレーサブルネットワークにおける研究開発では、セキュリティ技術における相互接続性、ネットワーク技術における責任追跡性など具体的に五つの要件を設定し、様々な研究手法を組み合わせてその実現に取り組んでいる。本稿ではその取組の概要と、本特集における各論文との関連について述べた。トレーサブルネットワークのみで安全なインターネットを実現できるわけではないが、本特集をきっかけとして問題分析と研究戦略が共有され、さらに効果的な取組につながることを期待する。

参考文献

1 Ross Anderson, "Why Cryptosystems Fail", in Proceedings of the 1st ACM Conference on Computer and Communications, pp.215-227, Nov. 1993.

2 Justin E. Forrester and Barton P. Miller, "An Empirical Study of the Robustness of Windows NT Applications Using Random Testing", in Proceedings of the 4th USENIX Windows System Symposium, Aug. 2000.
3 Andy Chou, Junfeng Yang, Benjamin Chelf, Seth Hallem, and Dawson Engler, "An Empirical Study of Operating Systems Errors", ACM SIGOPS Operating Systems Review, Vol.35, No.5, pp.73-88, Dec. 2001.
4 Ross Anderson, "Why Information Security is Hard-An Economic Perspective", in Proceedings of 17th Annual Computer Security Applications Conference, pp.358-365, Dec. 2001.
5 Organization for Economic Cooperation and Development, "OECD Guidelines for the Security of Information Systems", 1992.
6 International Organization for Standardization, "Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management", ISO/IEC 13335-1, 2004.
7 Kerry G. Coffman and Andrew M. Odlyzko, "Growth of the Internet", in Optical Fiber Telecommunications Journal, Vol.ⅣB, pp.17-56, Jul. 2002.
8 Ruo Ando, Youki Kadobayashi, and Youichi Shinoda, "Incident-Driven Memory Snapshot for Full-Virtualized OS Using Interruptive Debugging Techniques", in Proceedings of the 2nd International Conference on Information Security and Assurance, Apr. 2008.
9 門林雄基，オーバーレイ・ネットワーク，コンピュータソフトウェア，日本ソフトウェア科学会，Vol.23，No.1，pp.15-23，2006年1月.
10 Ka-Ping Yee, "User Interaction Design for Secure Systems", in Proceedings of the 4th International Conference on Information and Communication Security, pp.278-290 , Dec. 2002.

門林雄基（かどばやしゆうき）
情報通信セキュリティ研究センター
レーサブルネットワークグループ客員
研究員　博士（工学）
ネットワークセキュリティ