論 文 内 容 の 要 旨

博士論文題目

Studies on Retrospective Identification of Link Layer Addresses
in Distributed Forensic Databases
(分散フォレンジックデータベースによるリンク層アドレスの
遡及的識別に関する研究)

氏 名　　金森　正高

(論文内容の要旨)

This dissertation presents an approach to assist an investigator with his/her incident analysis. In unexpected security incidents, one of the most important points is to ascertain whether or not a computer crime suspect is the culprit, and to avoid false charges. For this reason, various types of digital evidence are employed by an investigator to disclose a malicious user's activity. Accordingly, assurance of evidence is needed for an investigator to reach accurate conclusions. For this purpose, this research concerns two concepts: reliability and availability of evidence in the field of Computer and Network Forensics (CNF).

An investigator performs CNF procedures on the basis that the mapping between an IP address and a link-layer address is assigned correctly. This research, therefore, first introduces the Self-Confirming Engine (SCE) for the purpose of protecting address mapping tables in both Address Resolution Protocol (ARP) in IPv4 and Neighbor Discovery Protocol (ND) in IPv6. Both address resolution protocols are indispensable in the current Internet, because hosts communicate with each other by obtaining the pair of IP address and link-layer address. Consequently, even if a malicious user tries to compromise the tables, an investigator can perform CNF based on the trails of an attack because evidential information is recorded properly by address resolution procedures with the SCE. This method makes CNF that depends on various types of evidence both possible and reliable. The proposed system, moreover, is designed to be as simple as possible, because complexity makes general-purpose uptake/installation impractical in future digital devices.

Next, this dissertation presents an approach to making individual or obsolete evidence available, i.e., evidence linking. Even if an IP address or hostname is changed a long time after the occurrence of an incident, an information source accumulated by the SCE, called the TDB, is used to resurrect the links among traces recovered by the

investigator. Consequently, by applying the TDB, an investigator can retroactively identify whether or not an unauthorized access suspect is in fact the trespasser. From the difference of address mappings between a normal host and a third party, moreover, the user can prove that he/she is not the malicious host.

Finally, the importance of the two concepts is verified by implementation. An investigator can reduce the time required to analyze a security incident, and ensure that CNF works smoothly. Consequently, an investigator can indisputably determine guilt by applying this method. In this research, reliability and availability of evidence used as an information source are improved to resolve security incidents, and also trouble with a host or network. This research indicates that adequate preparation can enable users to cope with unexpected incidents.

氏名	金森 正高

（論文審査結果の要旨）

本論文は、ネットワーク内部における脅威に焦点を当てたものであり、第三者による情報の盗聴・改竄行為を回避し、セキュリティインシデント（以降、インシデント）発生後の調査が正当に行われるようにするため、事後対応に必要となる証拠の信頼性を確保し、時間経過に依存せず証拠が利用可能になるための提案を行い、その有効性を示したものである。本論文の主な成果は以下に要約される。

１．インターネットにて利用されているアドレス解決プロトコルである Address Resolution Protocol (ARP) / Neighbor Discovery Protocol (ND) とインシデントを調査するために必要な証拠となるシステム・アプリケーションログとの不可分な関係について指摘した。そして、情報漏洩により起因する甚大な損失を回避し、インシデントの正確な分析を達成し、そして冤罪の発生を防ぐためにもアドレス解決が重要な役割を担っており、内部犯からの脅威に対して対策を講じるべき最重要課題であることを示した。

２．アドレス解決の侵害により生じる情報の盗聴・改竄行為が可能な Man-in-the-Middle (MitM) 攻撃を回避するため、アドレスのマッピングに変更が生じた際に変更の正当性を確認する手法として Self-Confirming Engine (SCE) を両アドレス解決プロトコルにおいて提案し、実装、評価を行うことにより、その有効性を示した。また、提案システムとして新たなプロトコルを用いるのではなく、既存のプロトコルを利用することで ARP / ND への適応性を考慮し、汎用性を求めるためシンプルなアーキテクチャとした。

３．SCE を管理ネットワーク内のホストに導入し、アドレスのマッピング状況等の情報を蓄積することにより、インシデント発生時の当該ホストをリンク層アドレスから識別し、遡及的な事後調査を可能にしている。また、各ホストからの情報取得には Certification Authority (CA) を用いた Public Key Infrastructure (PKI) モデルのクライアント / サーバ認証を行うことにより、情報を受ける者と提供する者の真贋を確認している。これにより、提案システムは時間経過に依存しないインシデントの調査を可能にしたものであり、また本提案システムの利用者は情報保持者からの情報を基にアドレスやホスト名の利用実績を確認可能とするアプローチであることを示した。

以上のように、本論文はインシデント解明に必要な調査時間に囚われず、リンク層アドレスを基に証拠の利用価値を維持し、当該ホストの遡及的な識別を可能にする手法を提案、実装、評価したものであり、フォレンジックサイエンスの分野における研究として有益である。また、その有効性は学術上だけでなく、危機管理と法的措置が求められるネットワーク内部における不正行為対策を実現するための新しいアプローチとしても、その貢献度は大きいといえる。よって本論文は博士（工学）の学位論文としてふさわしいものと認める。