AS-1-3

ネットワークフォレンジックのためのホスト型のロギングについて

On Host-based Logging for Network Forensics

福田洋治[1] 溝渕昭二[2] 毛利公美[3] 白石善明[4] 野口亮司[5]
Youji Fukuta Shoji Mizobuchi Masami Mohri Yoshiaki Shiraishi Ryoji Noguchi

愛知教育大学[1] 近畿大学[2] 岐阜大学[3] 名古屋工業大学[4] 株式会社豊通シスコム[5]
Aichi University of Edu. Kinki University Gifu University Nagoya Institute of Tech. Toyotsu Syscom Corp.

1 はじめに

インシデントレスポンスや法的紛争・訴訟に対して，電磁的記録の証拠保全や調査，分析，電磁的記録の改竄・毀損等についての分析，情報収集等を行う手法・技術として，デジタルフォレンジックがある．その中で，我々は，ネットワークシステムの利用，動作の状況を記録して，ネットワーク障害や不正アクセス等の証拠保全，原因究明を行うためのネットワークフォレンジックシステム（NF システム）に注目している．

本稿では，個々の利用者のホストで通信パケットを記録し，ログを管理するホストに転送するホスト型 NF システムを想定して，ログの法的証明力を考慮し一連のロギングの機能の実現方法を検討する．

関連研究として，間形らにより，証拠性，安定性という 2 つの性質に基づき，訴訟の際に提出される電子データ（デジタル証拠）の法的証明力を高めるための要件が議論されている [4, 5]．第 2 節で我々の想定しているホスト型 NF システムについて述べて，第 3 節でホスト型 NF システムに関して間形らの要件を満足する機能の実現方法について検討する．

2 ホスト型 NF システム

ネットワーク障害や不正アクセス等の証拠保全，原因究明を目的とした，ネットワーク上を送受信される通信パケットの収集，保全を行う NF[1, 2, 3] のシステムについて考える．

通信のパケットを取得する既存の NF システムの形態には，図 1 のような，パケットを取得，記録するプローブを外部ネットワークの境界に設置するもの，ネットワークセグメントの境界に設置するものがある．しかしながら，組織内ネットワーク上のホストの全ての通信を把握するという観点では，全てのホスト間の通信のパケットを取得する仕組みの実現，パケットの取りこぼしへの対処が困難と考えられる．

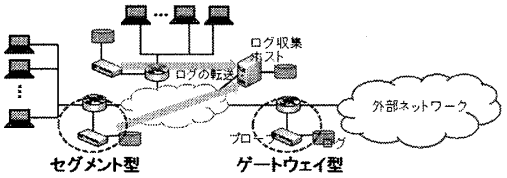

図 1 既存の NF システムの形態

そこで，ネットワークの経路上ではなく，図 2 のように，通信を行う末端のホストにプローブを配置して，パケットを収集，保全するホスト型の NF システムに我々は注目している．個々の利用者のホストで，ネットワークインターフェースを通過する通信パケットを取得，一時保存して，適時，ログを収集するホストに転送することで，ネットワーク上のホストの全ての通信パケットを取得することが可能と考えられる．

ホスト型 NF システムでは，図 3 のように，平時の通信パケットの取得，保全からインシデント発生時のログの提出までを，複数のフェーズに分けて考える．取得フェーズでは，ネットワークデバイスからパケットデータを取得し，そのデータを処理 1 フェーズの主体に送る．処理 1 フェーズでは，取得フェーズの主体からパケットデータを受けとり，それを加工し，ログデータとしてストレージに一時的に保存する．転送・収集フェーズでは，ストレージからログデータを読み出し，ログ収集ホストに転送，ログ収集ホストでそれを受け取り，処理 2 フェーズの主体に送る．処理 2 フェーズでは，収集フェーズの主体からログデータを受け取り，それを加工し，ストレージに保存する．提出フェーズでは，ストレージからログデータを読み出し，提出媒体に書き込み，提出する．

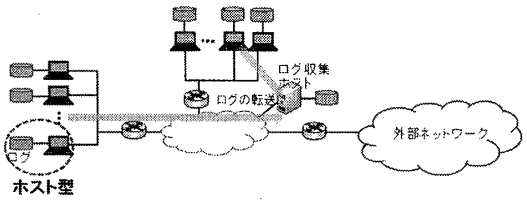

図 2 検討中の NF システムの形態（ホスト型ロギング）

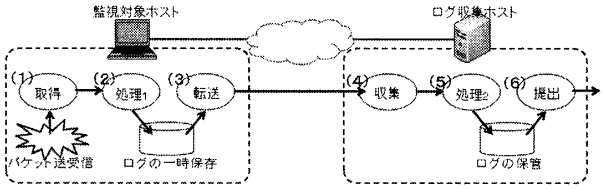

図 3 ホスト型 NF システムのフェーズ

3 ホスト型のロギングの実現

3.1 ログの法的証明力に関する要件

ホスト型 NF システムでは，利用者のホストで通信パケットをログとして取得，一時保持した後に，ログを管理するホストに転送，保管するまでの一連の過程で，ログの法的証明力を考慮した仕組みが必要と考えられる．

ログの法的証明力に関しては，間形らにより，証拠性，安定性という 2 つの性質に基づいて，訴訟の際に提出される電子データ（デジタル証拠）の法的証明力が議論されている [4, 5]．

要件 1 記録により必要な注意義務に従った運用実績を示すこと．

要件 2 故意過失の記録が含まれていないこと．

要件 3 記録の実在を証明できること．

要件 4 記録した主体が何かを証明できること．

要件 5 記録した日時を証明できること．

要件 6 記録の完全性を証明できること．

要件 7 記録の発生契機を証明できること．

要件 8 記録解釈の妥当性を証明できること．

要件 9 記録の正確性を証明できること．

要件 10 記録の網羅性を証明できること．

要件 11 記録保管の継続性を証明できること．

要件 12 記録の整合性があること．

要件 13 異常時の検出と対処が記録されていること.

要件 1,2 は証拠の内容が要証事実の裏づけになること（証拠性）に関する要件であり，要件 3〜13 は訴訟相手から証拠に対する反論を受けても再反論が可能で裁判官の心証に動揺を与えないこと（安定性）に関する要件と定義されている.

以降，システムによる支援が可能な安定性の要件について，特に要件 3〜7,9〜11 を満足するための，ホスト型ロギングの一連の機能の実現方法について検討する.

要件 8,12 に関しては，監視対象ホストが送受信するパケットデータを漏れなく記録することから，記録の解釈，他のログとの整合性は自明と考えられる．要件 13 に関しては，ネットワークシステムの障害時の検出，動作，対処の記録を残す仕組みを導入することが考えられ，今後，検討したい.

3.2 記録の発生契機，正確性，網羅性の要件の実現

記録の発生契機，正確性，網羅性の要件（要件 7,9,10）に関して，図 4 のような，記録を取得する機能のところで実現することを検討している.

取得部でアプリケーションと NIC の間でやり取りされる通信データをドライバのレベルで取得，ログとして記録する処理を行う間，ネットワークデバイスをロックして，ログの取りこぼしを防ぐ.

NDIS 層のフィルタドライバ (Windows を想定) により，必然的に通信データが取得できる構成にし，通信とその記録の生成が必ず同時に行われる仕組みにすることで，記録の発生契機（要件 7）の明確化と記録の網羅性（要件 10）の実現を考えている.

また，カーネルモードで動作するプログラムで機能を実装することにより，権限の無い利用者によるプログラムの不正操作を困難にし，プログラムのコード署名等と併せて，監視対象ホストにおける記録の正確性（要件 9）の実現を考えている.

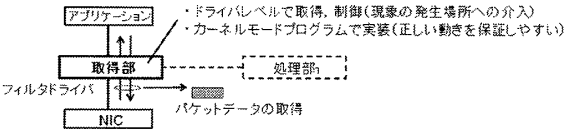

図 4 記録の取得機能

3.3 記録の実在，主体，日時，完全性の要件の実現

記録の実在，主体，日時，完全性の要件（要件 3,4,5,6）に関して，図 5 のような，記録の保全を行う機能のところで実現することを検討している.

処理部 1 で TPM[7] と連携して取得されたパケットデータに日時，カウンタ値等を付加，それに対してヒステリシス署名 [6] を計算，付加して，ログデータとしてストレージに保存する．ただし，事前に，監視対象ホストは TPM をセットアップし，公開鍵，秘密鍵を用意，デジタル署名を検証するホストとの間で，公開鍵証明書，公開鍵を共有しておく.

TPM の署名機能，保護メモリ機能を利用して，個々のホストで，ログデータに対してデジタル署名を作成，付加することで，記録の実在，主体の証明（要件 3,4），記録の完全性（要件 6）を実現することを考えている.

また，TPM のカウンタ機能，NTP 等のホストの時計同期機能を併用することで，パケットデータの取得された時刻情報をログデータに含めて，記録の日時の証明（要件 5）を実現することを考えている.

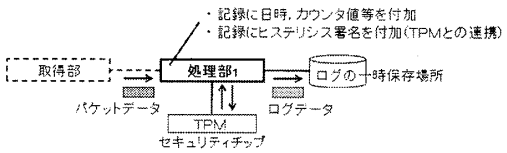

図 5 記録の保全処理機能

3.4 記録保管の継続性の要件の実現

記録保管の継続性の要件（要件 11）に関して，図 6 のような，記録の転送の機能のところで実現することを検討している.

監視対象ホストの転送部で，ストレージの記憶容量をオーバする前に，ログ収集ホストにログ転送要求を出し，適切にスケジューリングした上で，ログ収集ホストの収集部へログデータを転送する.

監視対象ホストのストレージの記憶容量，ログ収集ホストの負荷の問題で，ログ転送が困難な場合はネットワークデバイスをロックしてログ生成を停止させることで，監視対象ホストの記録保管の継続性（要件 11）を実現することを考えている.

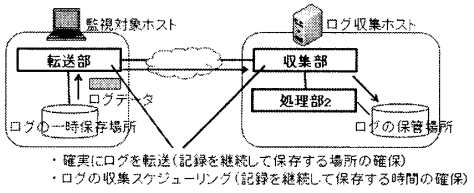

図 6 記録の転送機能

4 おわりに

本稿では，個々のホストで通信パケットをログとして取得し不定期にログを収集するホストに転送するホスト型 NF システムを想定して，間形らによって示されたログの法的証明力を高める要件を満たすロギングの機能の実現方法を検討した.

今後の課題として，検討中のロギングの機能の詳細を定義，実装すること，監視対象ホストにおけるロギングの動作の速度評価，シミュレータによる監視対象ホストとログ収集ホストの間のログ転送方式の検討，評価が挙げられる.

参考文献

[1] P.Branch, A.Pavlicic, and G.Armitage, "Using MAC Address in the Lawful Interception of IP Traffic," paper presented at the Australian Telecommunications Networks and Applications Conference 2004.

[2] A.Rojas, and P.Branch, "Lawful Interception based on Sniffers in Next Generation Network," paper presented at the Australian Telecommunications Networks and Applications Conference 2004.

[3] E.Casey, "Network traffic as a source of evidence: Tool strengths, weaknesses, and future needs," Digital Investigation, vol.1, no.1, pp.28-43, 2004.

[4] 間形文彦，高橋克巳，金井敦，"デジタル証拠の法的証明力を高めるための要件に関する一考察，" 電子情報通信学会 SCIS2008 予稿集，4E1-6，2008 年 1 月.

[5] 川西英明，加藤弘一，間形文彦，勅使河原可海，西垣正勝，佐々木良一，"デジタル・フォレンジック対策選定のための法的証明力を高める要件の関係性に関する検討，" 情報処理学会 DICOMO2008 予稿集，pp.580–586，2008 年 7 月.

[6] 洲崎誠一，松本勉，"電子署名アリバイ実現機構－ヒステリシス署名と履歴交差，" 情報処理学会論文誌，Vol.43, No.8，pp.2381–2393，2002 年.

[7] TCG，Trusted Platform Module(TPM), *https://www.trustedcomputinggroup.org/groups/tpm/*