様式 C-19

科学研究費補助金研究成果報告書

平成 21 年 3 月 31 日現在

研究種目：基盤研究(C)
研究期間：2006～2008
課題番号：１８５００００６３
研究課題名（和文）　感染経路特定によるワームの検知とディジタルフォレンジックスへの応用
研究課題名（英文）　Network Worm Detection by Identifying Infection Route and its Application to Digital Forensics.

研究代表者
重野　寛（SHIGENO HIROSHI）
慶應義塾大学・理工学部・准教授
研究者番号：30306881

研究成果の概要：

近年，ネットワークワームの脅威が増してきており，今後も強力な新型ワームの出現が予想されている．本研究では，脆弱ホストのアドレスリストを利用して感染先を発見するフラッシュワームを対象として，アノマリコネクションのツリーの検出を利用したワーム検知手法 ACTM と，その分散型の d-ACTM/VT を提案し，シミュレーションによって有効性を示した．さらに，自動アルゴリズムよる解析と視覚化システムを用いた人手による解析を併用するワーム感染経路の解析手法を提案し，ユーザ評価実験からその有効性を示した．

交付額

（金額単位：円）

	直接経費	間接経費	合　計
2006 年度	1,700,000	0	1,700,000
2007 年度	1,200,000	360,000	1,560,000
2008 年度	700,000	210,000	910,000
年度			
年度			
総　計	3,600,000	570,000	4,170,000

研究分野：　総合領域
科研費の分科・細目：　情報学・計算機システム・ネットワーク
キーワード：　情報ネットワーク，ディジタルフォレンジックス，ワーム検知，ロギング

１．研究開始当初の背景

情報化社会に必要不可欠なネットワークの安全を脅かす脅威として，ネットワークワームがある．これまでの比較的単純なワームに対して，今後，よりインテリジェントで強力なワームの出現が予想されており，その対策が求められている．

このようなワームとして，脆弱ホストのアドレスリストを利用して感染先ホストを発見するフラッシュワームの出現が想定されている．フラッシュワームは脆弱ホストのスキャンを行わず，ヒットリストを用いて感染活動を行う．このため，トラフィックの異常性を利用する従来の検知手法では検知が困難である．

加えて近年では，法的な解決に備えて，攻撃の電子的証拠（ログ）を集積したり，攻撃を解析したりする，いわゆる，ディジタルフォレンジックの重要性が認識されてきてい

る．ディジタルフォレンジックでは膨大なログを効率良く解析することや，わかりやすい解析結果の提示が必要になる．

本研究の全体構想は，フラッシュワームのような新型ワームの早期検知や，電子的な証拠であるログ解析による攻撃元やワームの影響の特定に取り組むことで，全体としてディジタルフォレンジックスの実現に寄与することである．

２．研究の目的

本研究課題の目的は以下の３点である．

(1) フラッシュワームの早期検知技術

ホスト数千台のイントラネットワークを対象としていて，非常に効率的な感染活動を行うフラッシュワームについて，感染活動の初期段階における検知技術の確立を目指す．

(2) 各種ログを関連付けるためのリンク技術

パケットログとシステムコールログの関連を推定し，これらの異なるログ間を有機的にリンクさせる技術を確立することを目的とし，精度の高いログの解析を目指す．

(3) ログから不正活動を抽出するための解析技術

大量のログに対して視覚化手法を用いることで効果的な解析を行い，不正活動の特定やその証拠を効率的に抽出するための技術の確立を目指す．

３．研究の方法

(1) 平成 18 年度は，フラッシュワームの早期検知技術の研究を進めた．文献調査等を通して，ネットワークワームの種類や特性，検知手法，評価方法と評価項目を整理した．フラッシュワームの中でも強力なワームをサイレントワームと定義し，モデル化を行った．サイレントワームの検知のために，アノマリコネクションのツリー構造を利用した検知アルゴリズム ACTM（Anomaly Connection Tree Method）を提案した．シミュレーションを実装し，ACTM の有効性を評価した．

(2) 平成 19 年度は，各種ログを関連付けるためのリンク技術の研究を進めた．文献調査等を通して，IDS の分散配置方法，各 IDS におけるローカルログの解析手法，IDS 間の情報のリンクによるワームの分散検知手法を検討した．前年度提案した ACTM 拡張し，ログのリンク付けを利用したワームの分散的検知手法 d-ACTM/VT (distributed ACTM with Virtual anomaly connection Tree detection)を提案した．シミュレーションを実装し，d-ACTM の有効性を評価した．

(3) 平成 20 年度は，ログから不正活動を検出するための解析技術の研究を進めた．文献調査等を通して，ログの抽出や，視覚化に関する問題点，ディジタルフォレンジックの要件を整理した．ワームの感染経路にフォーカスを当て，通信ログの解析技術を用いて感染経路を特定する手法を提案した．プロトタイプシステムを実装し，ユーザ実験による評価を行った．

４．研究成果

(1) ACTM

ACTM の方式の概要

サイレントワームの検知のためにアノマリコネクションのツリー構造を利用した検知アルゴリズムを検討し，ACTM（Anomaly Connection Tree Method）を提案した．

サイレントワームを含めたネットワークワームの感染活動の特徴は，①通常は通信頻度が低いホスト間での通信が集中的に発生すること，②感染コネクションと感染ホストがツリー構造を形成することの二点である．そこで ACTM は，発生頻度が低い通信（Anomaly Connection, AC）を検出し，それらの組み合わせによって形成されるツリー構造であるアノマリコネクションツリー（AC ツリー）を検出することでワームの感染活動を検知する．

検知対象ネットワークの中の通信コネクションは，正規のネットワーク活動により発生する LC (Legitimate Connection)と，ワームの感染活動により発生する WC（Worm Connection）からなる．また，ACTM では，ある閾値を基準として発生頻度が高いコネクション を NC(Normal Connection)，発生頻度が低いコネクション を AC(Anomaly Connection）に分類する．

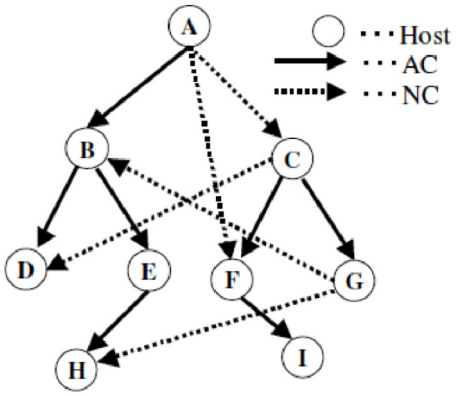

図１ AC ツリーの概念

図１に AC ツリーの概念を示す．ワームに感染していないホストのコネクション，すなわち，LC の宛先ホストは一般に一部ホストに集中するため，LC の多くは NC に分類される．一方，ワームは自身が感染したホスト

の通常の宛先ホストがどこに集中するかを考慮せずに感染活動を行うため，WC の多くは AC に分類される．ワームの感染活動によるコネクションである WC はツリー構造となるため，検出された複数の AC もツリー構造となることが期待できる．

ACTM では，あるサイズ以上の AC ツリーを検出すると，ワームの感染があると判断する．ここでサイズとは，そのツリーに含まれるホスト数である．LC が AC に分類される確率は，WC が AC に分類される確率よりも相対的に低い．したがって，ワームに感染した場合は，感染がない場合に比べて，大きなサイズの AC ツリーが検出される確率が高くなる．そこで ACTM は閾値を超えるサイズの AC ツリーが検出された場合，ワームがツリー中に存在すると判断する．

WC の一部が NC と判断される可能性があるため，WC のツリーは複数の AC ツリーに分断されて検出される可能性がある．ACTM では近傍に存在する複数の AC ツリーを集約することで Virtual AC ツリー（VAC ツリー）と呼ばれる仮想的な AC ツリーを検出し，このサイズが閾値を超えた場合もワームに感染していると判断する．

(2) d-ACTM/VT

ACTM をベースとして，分散型のワーム検出手法の d-ACTM/VT を提案した．d-ACTM/VT はネットワーク内に配置された複数の IDS が協調動作して，ACTM と同様の原理に基づきワーム検知機能を実行する．

図 2 に d-ACTM/VT の概要を示す．d-ACTM/VT では，各ホストを監視する一種の IDS である LACD（Local Anomaly Connection Detector）を導入する．LACD は監視対象ホストに関するローカルな通信ログを分析し，AC ツリーの一部である Local AC Tree（LAT）を検知する．さらに，LACD の間で LAT に関する情報を交換し，自身の情報と他の LACD から得られた情報をリンクして AC ツリーを分散的に検知する．

LACD は監視対象ホストに関するローカルな通信ログを分析し，そのホストに関する inbound コネクションや outbound コネクションを，比較的簡単なルールとその生成間隔をベースに LAT としてグループ化する．図 3 に LAT 検出の例を示す．この例では Host X に関するコネクションを LAT1, LAT2, LAT3 に分類している．

WC のツリーの一部は，LACD では LAT として検出される．LACD は自身が検出した LAT のサイズがある一定値増加するたびに，その LAT の上位のホストを担当する LACD に，LAT に関する AC ツリーの情報を通知する．通知を受けた LACD は自身のもつ LAT と通知された LAT の組み合わせを AC ツリーの候補として検査し，サイズが閾値を超えたものに関しては，さらに上位のホストの LACD に通知する．このような動作を繰り返し，一定サイズ以上の AC ツリーが検出された場合にワームに感染していると判断する．

d-ACTM においても AC ツリーの分断が問題となる．そこで，AC ツリーのある閾値を超えた場合，NC の送信元となるホストの LACD に対しても AC ツリーの情報を送ることで，VAC ツリーを検出する．

図 4 に d-ACTM における AC ツリー検知を示す．図中，AC でリンクされる範囲は AC の上位に向かって LAT の情報を送ることを繰り返し，AC ツリーが検出されている．一部が NC により分断された AC ツリー，例え

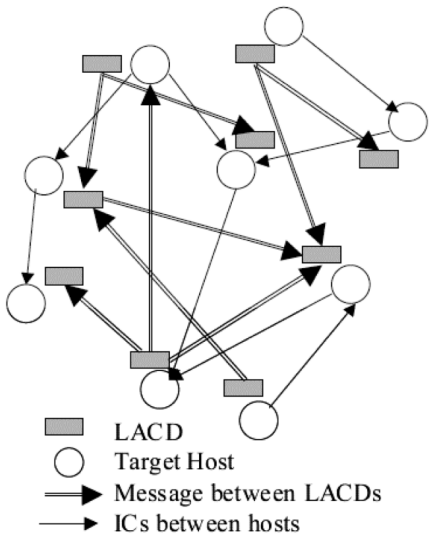

図 2 d-ACTM

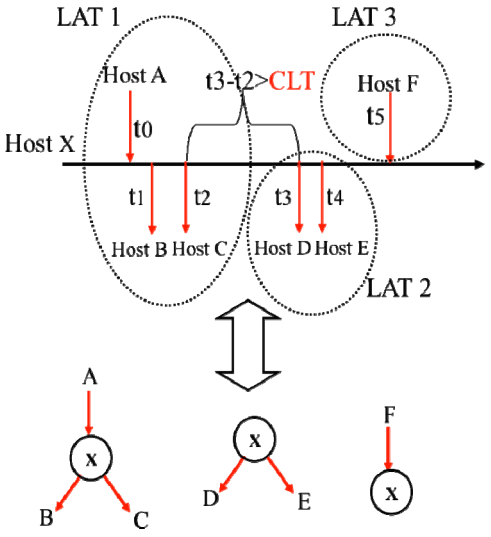

図 3 LAT の例

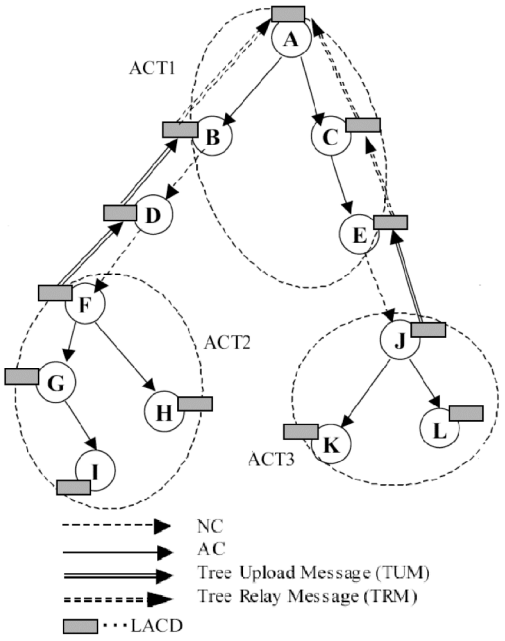

図 4 分断された AC ツリーの結合

ば, ACT1 と ACT2 については, 下位の ACT2 のサイズがある閾値を超えた際に NC に沿って上位の LACD に情報を通知され，VAC ツリーとして検出される.

(3) d-ACTM/VT の評価

d-ACTM/VT の，サイレントワーム検知に対する有効性を示すためにシミュレーションを用いて評価を行った．シミュレーションでは，ホスト数 500 台の組織ネットワークを想定し, 通常のコネクションの平均間隔は 10 時間単位（TU）とした．サイレントワームはヒットリストにより脆弱ホストを発見し，感染試行回数 2, 感染試行間隔は可変とした.

① ワームの感染間隔と検知性能

図 5 に d-ACTM/VT によってワーム感染が検知された時点における感染ホスト数を示す．図より，ワームの感染試行間隔が平均コネクション間隔より短い場合，d-ACTM/VT はその監視対象ネットワークの総ホスト数 500 台の 10%に相当する 50 台のホストが感染する前にワームが検知できることが分かる．LAT 分割の閾値 CLT=10 のとき，感染間隔が短くなると検知性能は悪化する．これは AC ツリーが複数の小さな LAT の断片に分割されて検知されるためである．この点は複数の閾値を組み合わせることで改善できる. 図では二つの閾値 CLT=6, 10 を使った場合について示している.

② VAC ツリー検出の効果

図 6 に d-ACTM と d-ACTM/VT の二手法の性能の比較を示す．横軸の DAI(desirable false positive alert interval) は 各 LACD に許される false alert 間隔であり, 適切な false alert 率と検知率をバランスさせるために設定するパラメータである．図より，VAC ツリーの検出を行うことで, d-ACTM の性能を最大で 20%程度改善できることがわかる.

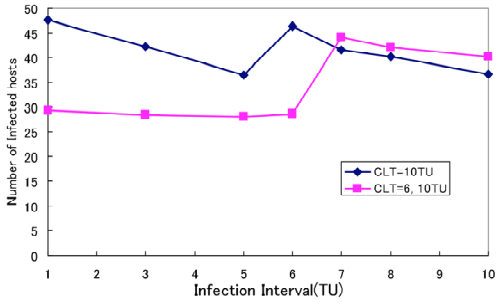

図 5 ワーム感染間隔の影響

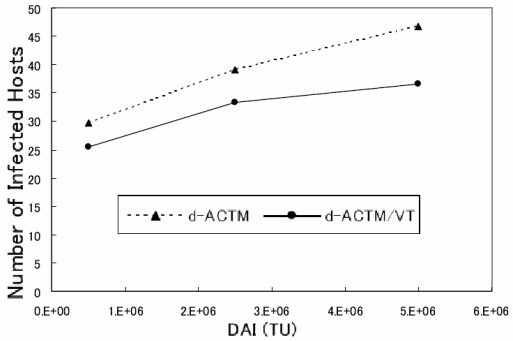

図 6 d-ACTM と d-ACTM/VT の比較

③性能評価のまとめ

ACTM および d-ACTM/VT の定性的な検討と，シミュレーションによる定量評価より，以下が分かった.

- ACTM と d-ACTM/VT は，ワームの感染のコネクションのツリー構造を検出することで，効果的にサイレントワームの検出することができる.
- ACTM に比較して，d-ACTM/VT は同程度以上の性能を有しつつ, 通信ログの監視, AC ツリーの検出処理等は分散化できるため，スケーラビリティに優れる.
- d-ACTM は，他のツリーベースのアプローチやチェーンベースのアプローチと比較しても性能の面で優位である.

以上より，非常に低速で検知が難しいサイレントの早期検知に対して，提案手法は有効であると言える.

(4) 通信ログ解析と感染経路の視覚化を用いたワーム感染経路の特定手法

ワーム感染経路の特定手法として，自動アルゴリズムよる解析と，視覚化システムを用いた人手による解析を組み合せて用いる解析手法を提案した.

① ワーム感染経路特定手法の概要

通信ログからワームの感染経路を特定する手順は以下の通りである．

ⅰ． 全てのコネクションを感染疑惑コネクションとする．
ⅱ． 自動アルゴリズムを用いて感染疑惑のないコネクションを検出し，削除する．
ⅲ． 視覚化システムを用いて，人手によって感染疑惑のないコネクションを検出し，削除する．
ⅳ． 視覚化システムを用い，解析結果をワーム感染経路として提示する．

② プロトタイプシステム

ホストがもつ内部アドレスリストを用いて感染活動を行うヒットリスト・ワームを対象として，本提案手法による解析システムのプロトタイプシステムを実装した．

自動検知アルゴリズムには「ダミーアドレスを用いたワームの自動検知手法」を用いた．この手法はあらかじめ用意されたダミーアドレスへのコネクションを検知することで，ワームの存在を検知する．さらに，ダミーアドレスへのコネクションの上位にログを遡って検査することで，感染疑惑のあるホストを特定し，ワームよる感染ツリーを推定する．自動化アルゴリズムよる解析は，false negative が十分に小さくなるように用いる．

視覚化手法としては二種類の手法を採用し，感染経路をワームツリー形式で，ホストに関するコネクションをロググラフ形式でそれぞれ視覚化する．さらに，これらのグラフとインタラクションを行い，false positive コネクションを削除できるようにした．

図７にプロトタイプシステムの画面イメージを示す．上部にはワームツリーが表示されており，下部ではコネクションログが直接表示さている．それぞれをツリーウィンドウ，ログウィンドウと呼ぶ．

ツリーウィンドウでは感染疑惑ホストをノード，感染疑惑コネクションをエッジとするグラフの形で通信ログが表示される．コネクションを構成するノードの中で，左側が送信元ホスト，右側が宛先ホストを表す．横軸は時間軸を示し，宛先ホストの位置がコネクションの確立された時刻を表す．

図８にログウィンドウを示す．ログウィンドウでは，縦軸を各ホスト，横軸を時間軸として，すべてのコネクションログが表示される．コネクションは送信元ホストから宛先ホストへの矢印として表示される．

ログに対する操作はどちらのウィンドウでも可能であり，その操作結果は両方のウィンドウに反映される．したがって，解析者はこれらのウィンドウを交互に用いて解析を行うことができる．

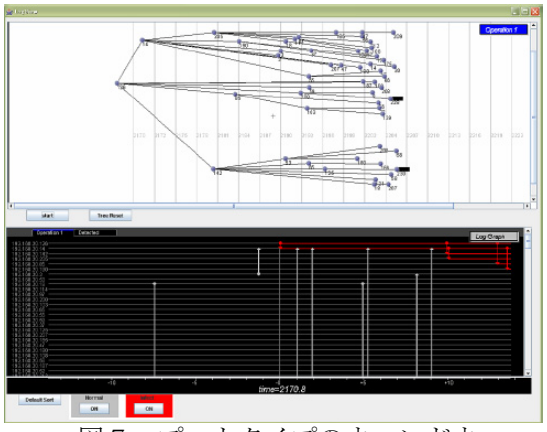

図７　プロトタイプのウィンドウ

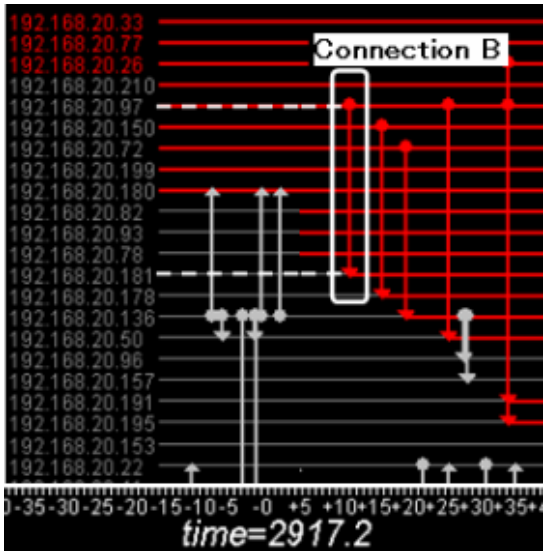

図８　ログウィンドウの拡大図

(5) 視覚化の有効性に関する評価

提案の視覚化手法がワームの経路特定に有効であることを示すために，プロトタイプシステムを用いてユーザ実験を行い，評価を行った．比較対象は視覚化ツールを用いる場合とログウィンドウのみを用いる場合である．本実験は情報工学を専攻する大学生、大学院生 18 人を対象に行った．評価実験に用いた通信ログは，DARPA の IDS 評価用のログから通常コネクションログを作成し，そこにシミュレーションによるワームのコネクションのログを混入したものを用いた．表１に使用したログセットの種類を示す．

表２に，解析作業後に未発見として残された false positive (FP)コネクション数を示す．

表１　ログセットの概要

ログセット	A	B	C
FP コネクション数	10	20	40
ワームコネクション数	50	40	20
感染疑惑コネクション数	60	60	60

表 2 作業後の平均 FP コネクション数

ログセット	A	B	C	平均
作業前	7.7	22.2	35.8	21.9
ログウィンドウ	4.3	9.8	22.1	12.1
ツリー& ログウィンドウ	1.7	0.6	3.2	1.8

表より，ツリーウィンドウとログウィンドウを併用することにより，FP コネクションの個数を作業前の 1 割程度にまで削減できている．作業前の FP コネクションが多くなると，ログウィンドウのみによる解析では，作業後の未検出 FP コネクションが増えているが，両方のウィンドウを用いた場合では，作業前の FP コネクションの個数によらず，大幅に FP コネクションを削減できている．

以上より，本提案手法は，作業前の FP コネクションが増加しても，FP コネクション大幅に削減可能であり，ワームの感染経路の特定に有効であると言える．

５．主な発表論文等

〔雑誌論文〕（計 3 件）

1. 稲場太郎，田原慎也，川口信隆，塩澤秀和，重野寛，岡田謙一，デジタルフォレンジックのためのワーム感染経路特定手法，情報処理学会論文誌，Vol.50,No.3,pp.1002-1011, 2009，査読有.
2. Nobutaka Kawaguchi, Hiroshi Shigeno, Kenichi Okada, ″d-ACTM/VT: A Distributed Virtual AC Tree Detection Method,″ IPSJ Journal, Vol.49, No.2, pp.1010-1021, 2008, 査読有.
3. 川口信隆，重野寛，上田真太郎，塩沢秀和，岡田謙一，サイレントワーム検知のためのアノマリコネクションツリーメソッド，情報処理学会論文誌，Vol.48, No.2, pp.614-624, 2007，査読有.

〔学会発表〕（計 9 件）

1. 稲場太郎，芝口誠仁，川口信隆，重野寛，岡田謙一，ディジタルフォレンジックのための視覚化によるワームの感染経路特定手法，情報処理学会 DICOMO2008 シンポジウム，2008 年 7 月 9 日，北海道札幌市.
2. Nobutaka Kawaguchi, Hiroshi Shigeno, Kenichi Okada, ″A Distributed Detection of Hitlist Worms,″ The IEEE 2008 International Conference on Communications, 2008 年 5 月 21 日, Beijing, China.
3. Taro Inaba, Nobutaka Kawaguchi, Sinya Tahara, Hiroshi Shigeno, Ken-ichi Okada, ″Early Containment of Worms Using Dummy Addresses and Connection Trace Back,″ The 13th International Conference on Parallel and Distributed Systems, 2007 年 12 月 6 日, Hsinchu, Taiwan.
4. Taro Inaba, Nobutaka Kawaguchi, Shinya Tahara, Hiroshi Shigeno, Kenichi Okada, ″Worm Containment with Dummy Addresses and Connection Trace Back,″ The 15th IPSJ Workshop On Multimedia Communication and Distributed Processing, pp.13-18, 2007 年 10 月 31 日，石川県加賀市.
5. Shinya Tahara, Nobutaka Kawaguchi, Taro Inaba, Hidekazu Shiozawa, Hiroshi Shigeno, Ken-ichi Okada, ″Cooperative Detection of Malicious Mobile Users using Network Activity History,″ DICOMO symposium, 2007 年 7 月 5 日，三重県鳥羽市.
6. Nobutaka Kawaguchi, Hiroshi Shigeno, Kenichi Okada, ″Detection of Silent Worms using Anomaly Connection Tree,″ In Proc. of The IEEE 21st International Conference on Advanced Information Networking and Applications, pp.412-419, 2007 年 5 月 21 日，Niagara Falls, Ontario, Canada.
7. Nobutaka Kawaguchi, Hiroshi Shigeno, Kenichi Okada, ″d-ACTM: Distributed Anomaly Connection Tree Method to detect Silent Worms,″ In Proc. of 26th IEEE International Performance, Computing and Communications Conference (Malware'07 Track), pp.510-517, 2007 年 4 月 13 日，New Orleans, Louisiana USA.
8. 重野寛，川口信隆，岡田謙一，″A Distributed Worm Detection Method based on ACTM,″ 情報処理学会研究報告 2007-DPS-130, pp201-206, 2007 年 3 月 1 日，福岡県福岡市.
9. 川口信隆，重野寛，岡田謙一，アノマリコネクションツリーを用いたサイレントワームの早期検知手法の提案，情報処理学会研究報告 2006-CSEC-33, pp31-36, 2006 年 5 月 12 日，茨城県つくば市.

〔その他〕

研究室ホームページ

http://www.mos.ics.keio.ac.jp/

６．研究組織

(1)研究代表者

重野　寛（SHIGENO HIROSHI）

慶應義塾大学・理工学部・准教授

研究者番号：30306881

(2)研究分担者

岡田　謙一（OKADA KENICHI）

慶應義塾大学・理工学部・教授

研究者番号：80118926

(3)連携研究者

該当なし