私とデジタル・フォレンジック

東京電機大学
佐々木　良一
sasaki@im.dendai.ac.jp

目次

私のデジタル・フォレンジックとの出会い

1. 出会った時期：2002-3年ごろ
2. トリガー：弁護士の知り合いが多く、デジタル・フォレンジックやコンピュータ・フォレンジックという言葉を使っていた
3. 研究に着手した理由（2003-4年ぐらい）
   （1）今後、データは、大部分がデジタル化
   （2）今後、権利意識が増大し、民事訴訟が増加
   ＝＞　DFが重要にならないはずはない

初期の論文：上田　祐輔、佐々木　良一　他「データ喪失を想定したヒステリシス署名方式評価手法の提案」情報処理学会論文誌第45第8号pp1966-1976,（2004年8月）
（ログに対する署名方法に関するもの）

日本における デジタル・フォレンジックの歴史

1996年：電子的記録解析が警察庁情報管理課の管掌になる

2000年：警察庁情報通信局に技術対策課誕生

2003年：デジタル・フォレンジックを扱う会社UBIC（現FRONTEO）設立

2003年：警察政策学会のパネルでフォレンジックコンピューティングがテーマに

2003年：@policeにフォレンジックの解説（佐々木執筆）が掲載

2004年：デジタル・フォレンジック研究会発足

背景

1995年のオウム事件がトリガー

オウムのメンバーは情報処理技術に詳しい者が多く、公開鍵暗号等を用いファイルの防御に使用

=>電子的記録解析が警察庁情報管理課の管掌に

舟橋理事よりの情報

警察政策学会のパネル

1．日時：2003年6月20日
2．テーマ：「ネットワーク社会の安全
（フォレンジックコンピューティング）」
（於　警察政策学会5周年記念シンポジウム）
3．出席者：
コーディネーター：
佐々木　良一（東京電機大学）
パネリスト：
宮城　直樹（警察庁生活安全局）
内田　勝也（中央大学研究開発機構）
山崎　文明（グローバルセキュリティエキスパート）
尾崎　孝良（弁護士）

日本における
デジタル・フォレンジックの歴史

1996年：電子的記録解析が警察庁情報管理課の管掌になる

2000年：警察庁情報通信局に技術対策課誕生

2003年：デジタル・フォレンジックを扱う会社UBIC（現FRONTEO）設立

2003年：警察政策学会のパネルでフォレンジックコンピューティングがテーマに

2003年：@policeにフォレンジックの解説（佐々木執筆）が掲載

2004年：デジタル・フォレンジック研究会発足

@Policeの記事(2003年9月16日)

http://web.archive.org/web/20070410010543/http://www.cyberpolice.go.jp/column/index.html

海外の動向

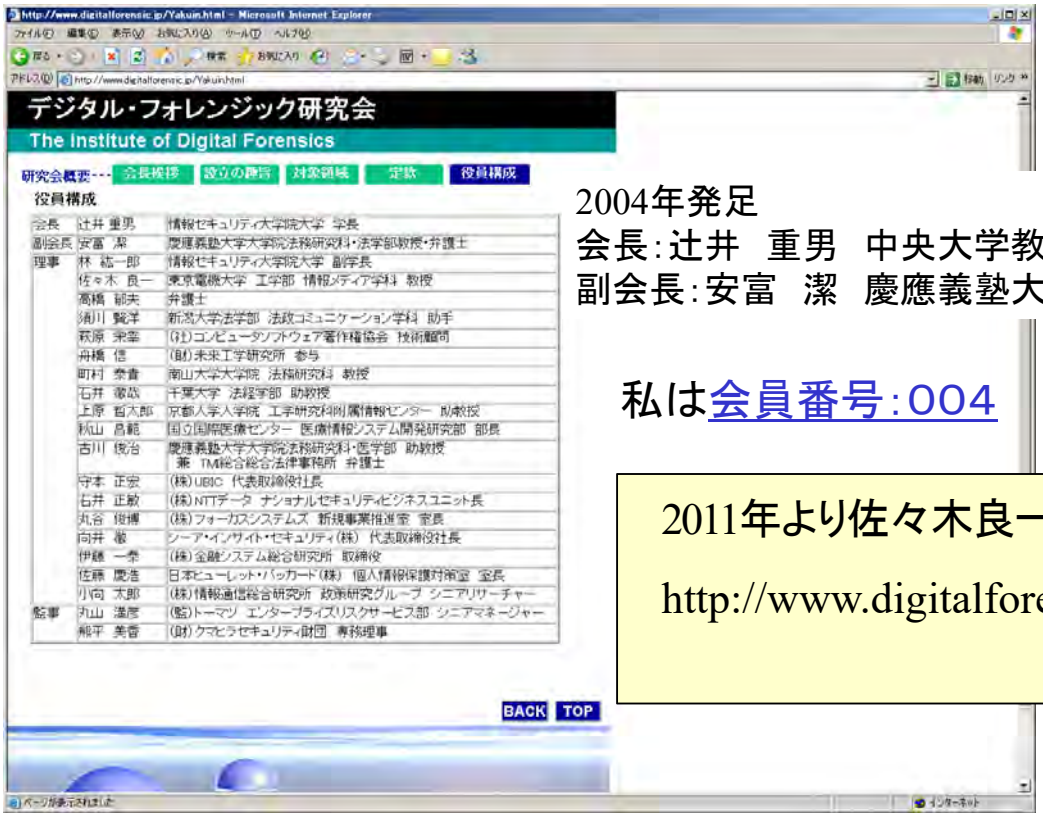
①1984 : 米国FBIにComputer Analysis and Response Team発足
②1985 : イギリスMetropolitan PoliceにComputer Crime Department 設置
③1986 : ハッカーMarkus Hess のCliff Stollによる追跡にDFを初めて使用（初歩的な技術）
④1989 : Michael WhiteがForensic Tool IMDUMPを作成。
1990年代になり高度な商用ツールEnCaseやFTKが誕生
⑤1992 : Computer Forensicsという言葉がCollier, P.A. and Spaul, B.J.によって初めて学術文献に登場
⑥2001 : DFに関する研究会議DFRWSの第一回会合を実施
⑦2002 : Scientific Working Group on Digital Evidence (SWGDE)が標準化のための文書"*Best practices for Computer Forensics*"（2005 ISO17025に）

http://en.wikipedia.org/wiki/Digital_forensics

発足後の事象

2004年 : デジタル･フォレンジック研究会発足
（同年第1回デジタル・フォレンジック・コミュニティ実施）
2005年 : 内閣官房セキュリティ技術戦略委員会報告書に11の重要技術の1つとしてデジタル･フォレンジックが取り上げられる
2006年 :「デジタル・フォレンジック事典」日科技連発刊
2008年 : 第4回Digital Forensic International Conferenceを日本で実施
2010年 :「実践的eディスカバリ」NTT出版発刊
2011年 : IDF講習会スタート
2012年 :「証拠保全ガイドライン第2版」公開
2013年 : 10周年記念行事

デジタル・フォレンジック研究会



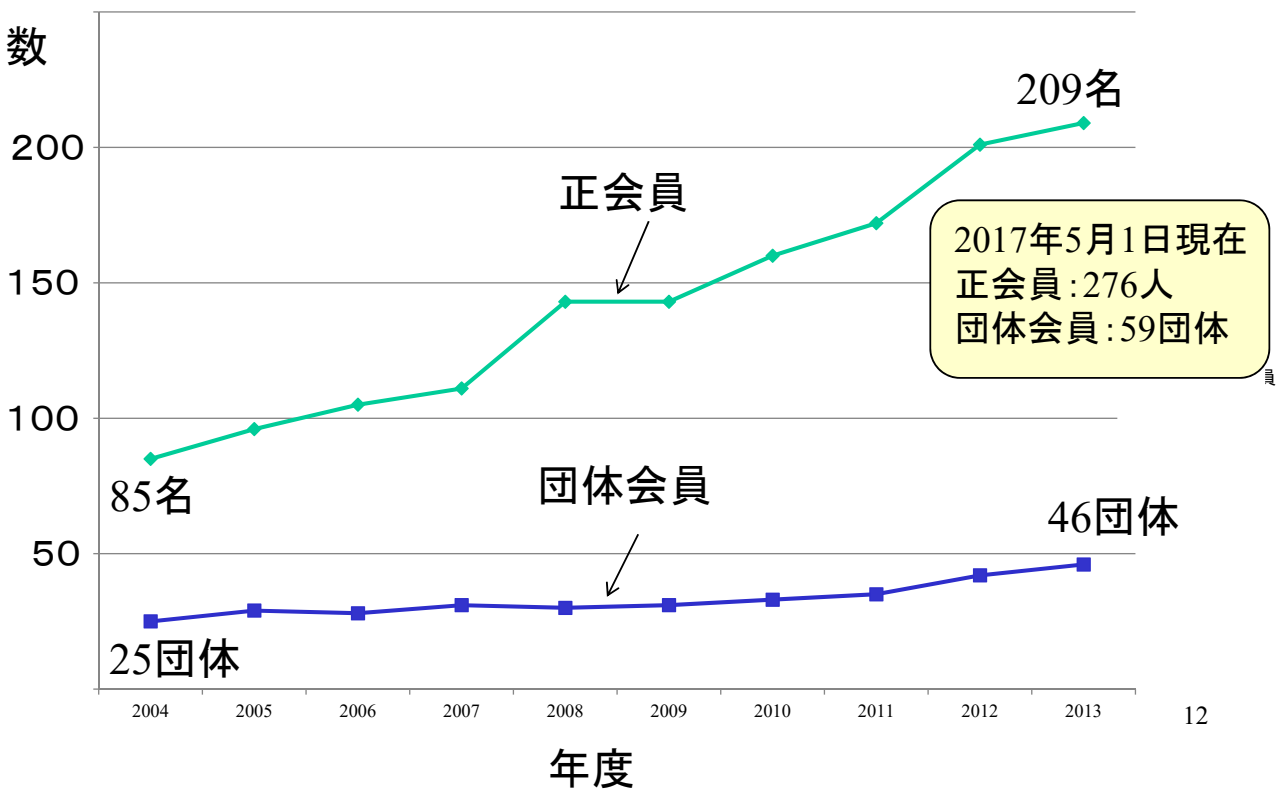
2004年発足
会長：辻井　重男　中央大学教授
副会長：安富　潔　慶應義塾大学教授

私は会員番号：004

2011年より佐々木良一が会長

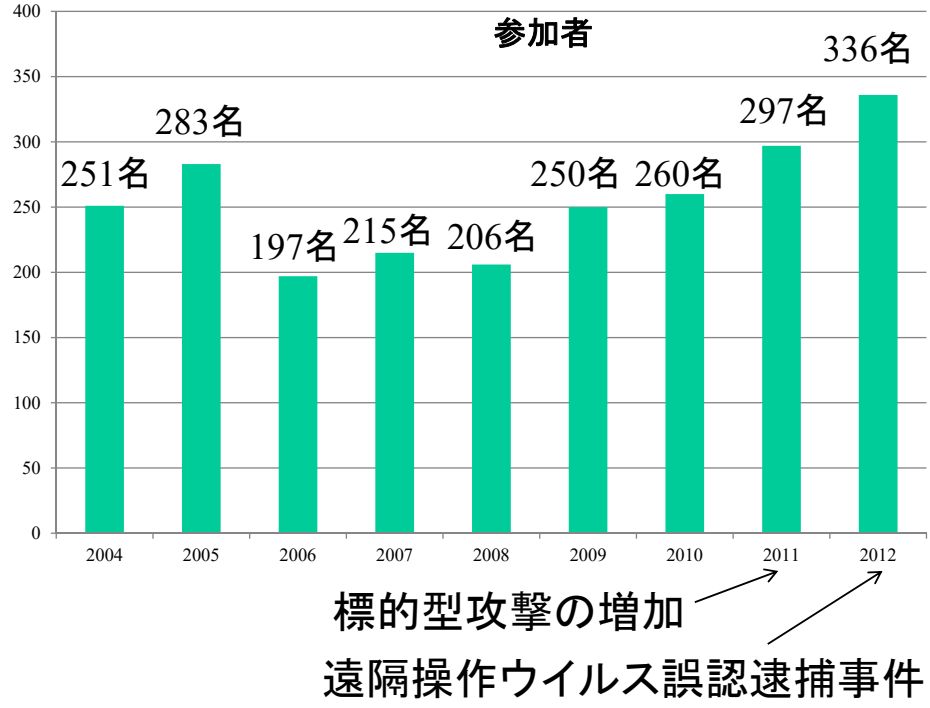
http://www.digitalforensic.jp/

会員の推移



2017年5月1日現在
正会員：276人
団体会員：59団体

デジタル・フォレンジック・コミュニティ参加者の推移



2013 328名
2014 343名
2015 334名
2016 332名

参加者

セキュリティ人材の不足

必要人員（34.7万人）

情報セキュリティ従事者（26.5万人）		不足 8．2 万人
従事者（技術力あり）（10.6万人）	従事者（技術力不足）（15.9万人）	

http://www.ipa.go.jp/files/000040646.pdf
2014年7月の報告書
（注）2012年の報告書では、2.2万人の不足
http://www.ipa.go.jp/security/fy23/reports/jinzai/

東京電機大学大学院における新たなセキュリティ教育

文科省「高度人材養成のための社会人学びなおし大学院プログラム」の1つで「国際化サイバーセキュリティ学特別コース」として認可。デジタル・フォレンジックは6つの科目の1つ。
対象は社会人20名、大学院生20名程度（実際は社会人も学生も30人以上）

（1）サイバーセキュリティ基盤
（2）サイバーディフェンス実践演習
（3）セキュリティインテリジェンスと心理・倫理・法
（4）デジタル・フォレンジック
（5）情報セキュリティマネジメントとガバナンス
（6）セキュアシステム設計・開発

https://cysec.dendai.ac.jp/

講師陣

外部講師（他大学教師、社会人が多いのが特徴）
DF：上原、櫻庭、佐々木、白濱、野﨑、八槙

デジタル・フォレンジック①

重要性が高まっているが、従来、日本では行われてこなかった新分野の講義

（1）デジタル・フォレンジック入門（電大　佐々木）
（2）ハードディスクの構造、ファイルシステム（立命館　上原）
（3）フォレンジックのためのOS、Windows（立命館　上原）
（4）フォレンジック作業の基礎（FRONTEO　野崎）
（5）フォレンジック作業・データ保全（FRONTEO　野崎）
（6）フォレンジック作業・データ復元（トーマツ　白濱）
（7）フォレンジック作業・データ解析1（トーマツ　白濱）
（8）フォレンジック作業・データ解析2（FRONTEO　野崎）
（9）上記の演習（白濱、野崎）

デジタル・フォレンジック②

（10）ネットワークフォレンジック
　　（攻撃法、マルウェア、ログの取り方）（電大　八槇）
（11）上記の演習（電大　八槇）
（12）代表的な対象におけるDFの方法1　情報漏えい
　　（トーマツ白濱）
（13）代表的な対象におけるDFの方法2
　　不正会計、e-Discovery　（FRONTEO　野崎）
（14）法リテラシーと法廷対応（弁護士　櫻庭）
（15）デジタル・フォレンジックの今後の展開／学力考査と解説
　　（電大　佐々木）

2015年度の実績

- 2015年の受講者数は54名（社会人38名、学生16名）
- セキュリティの専門家が多い
- 民間企業のほか金融庁、防衛省、警察等からの参加者もいる
- アンケート結果によるとDFコースはもっとも組織だった講義になっているなどと評価は高い

2016年度の主な変更点

① モバイルフォレンジックの追加
② デジタル・フォレンジック入門とフォレンジック作業の基礎の一本化
③ 演習を2回から3回に増大
④ 代表的な対象におけるDFの方法が2回だったのを一本化
⑤ 2016年度も好評

デジタル・フォレンジックの教科書

佐々木　良一　編著
「デジタル･フォレンジックの基礎と実践」
電大出版、2017年3月

先端技術・ハイテクのベストセラーに

発売後
2週間程度

2017年4月26日現在8位

今後の方向

1. 東京電機大学での講義の継続
2. WEBサイトなどで専門企業などで行っている高度な教育とのリンクを図る
3. 他大学でのDF教育コース設立のサポート
4. 一般人向きのDF本の執筆

DFに関連する2つの事件

1. 遠隔操作ウイルス事件
2. 将棋ソフト不正使用事件

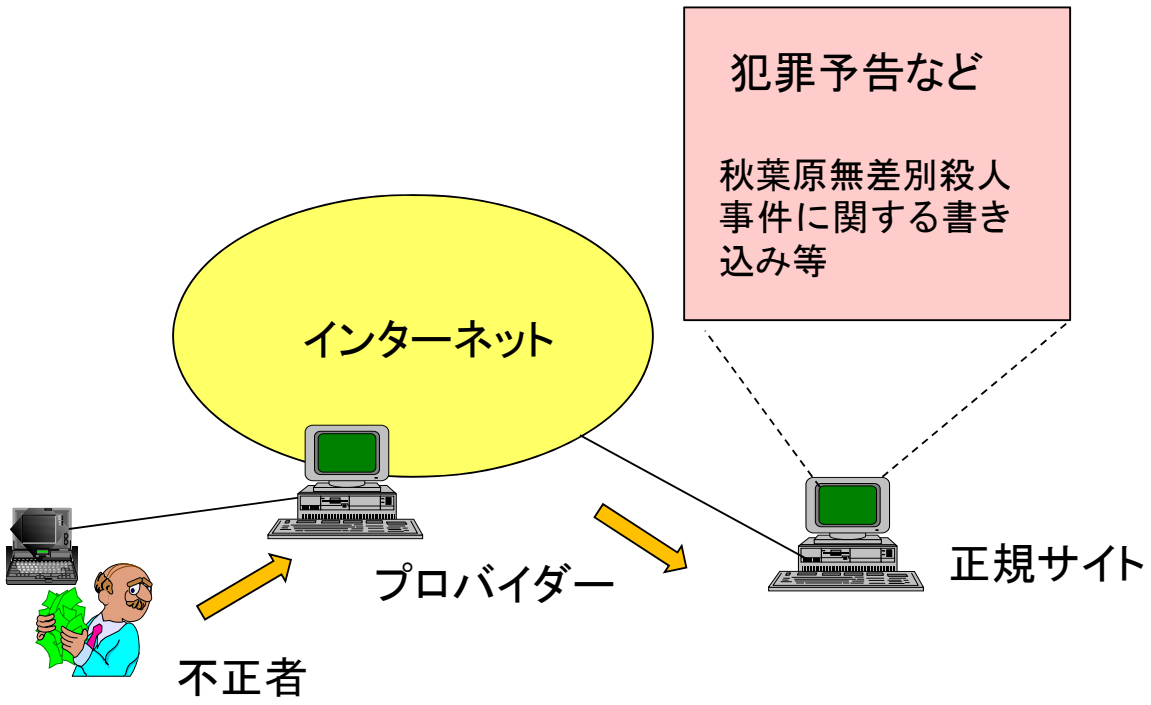
遠隔操作ウイルス事件の経緯（1）

（1）2012年「真犯人」が、インターネット掲示板を介して、少なくとも5人が所有するPCに対して不正な指令を与えて、所有者の認識しないところでPCを操り、少なくとも計13件の襲撃・殺害予告を行わせた。

（2）2012年10月9日：弁護士・落合洋司宛に真犯人から上記事件の犯行告白を主旨とするメールが送信される。

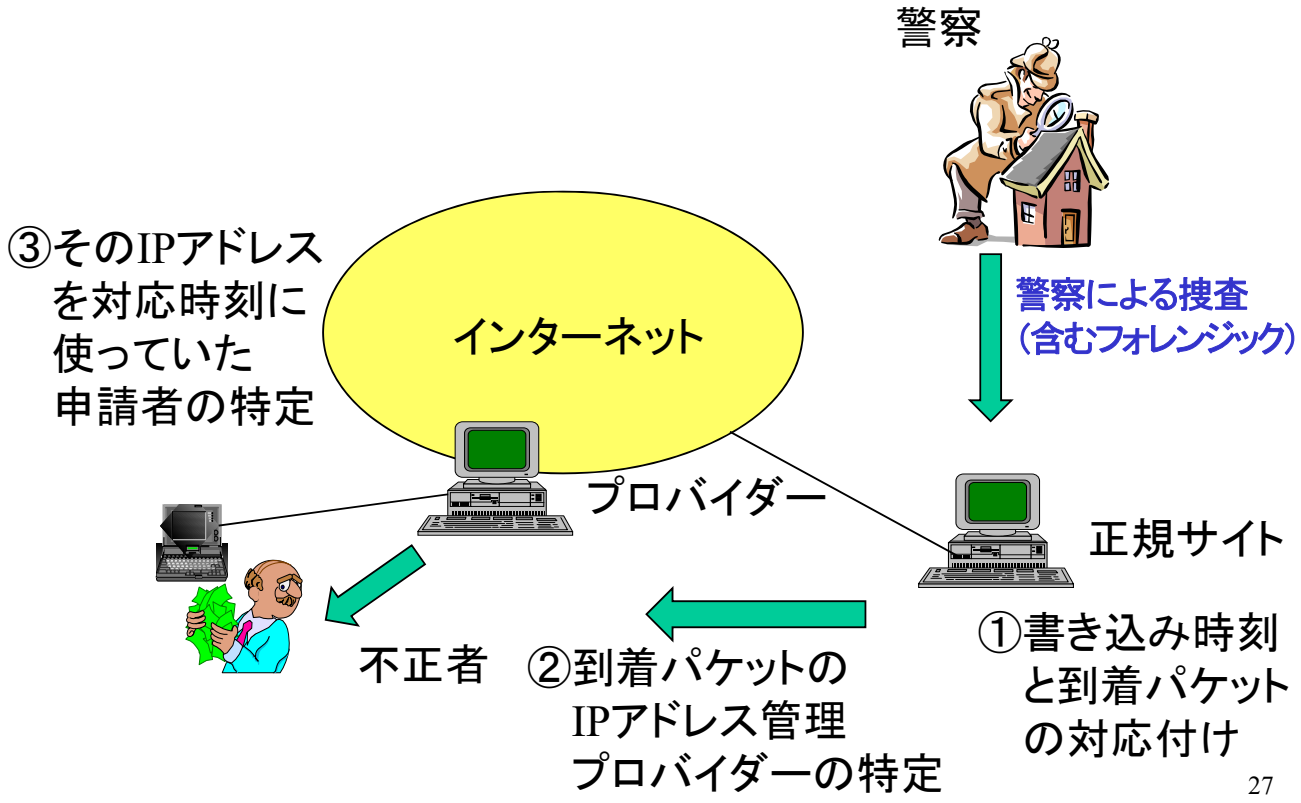
https://ja.wikipedia.org/wiki/%E3%83%91%E3%82%BD%E3%82%B3%E3%83%B3%E9%81%A0%E9%9A%94%E6%93%8D%E4%BD%9C%E4%BA%8B%E4%BB%B6

脅迫文書のWEBサイトへの書き込み



脅迫文書書き込み

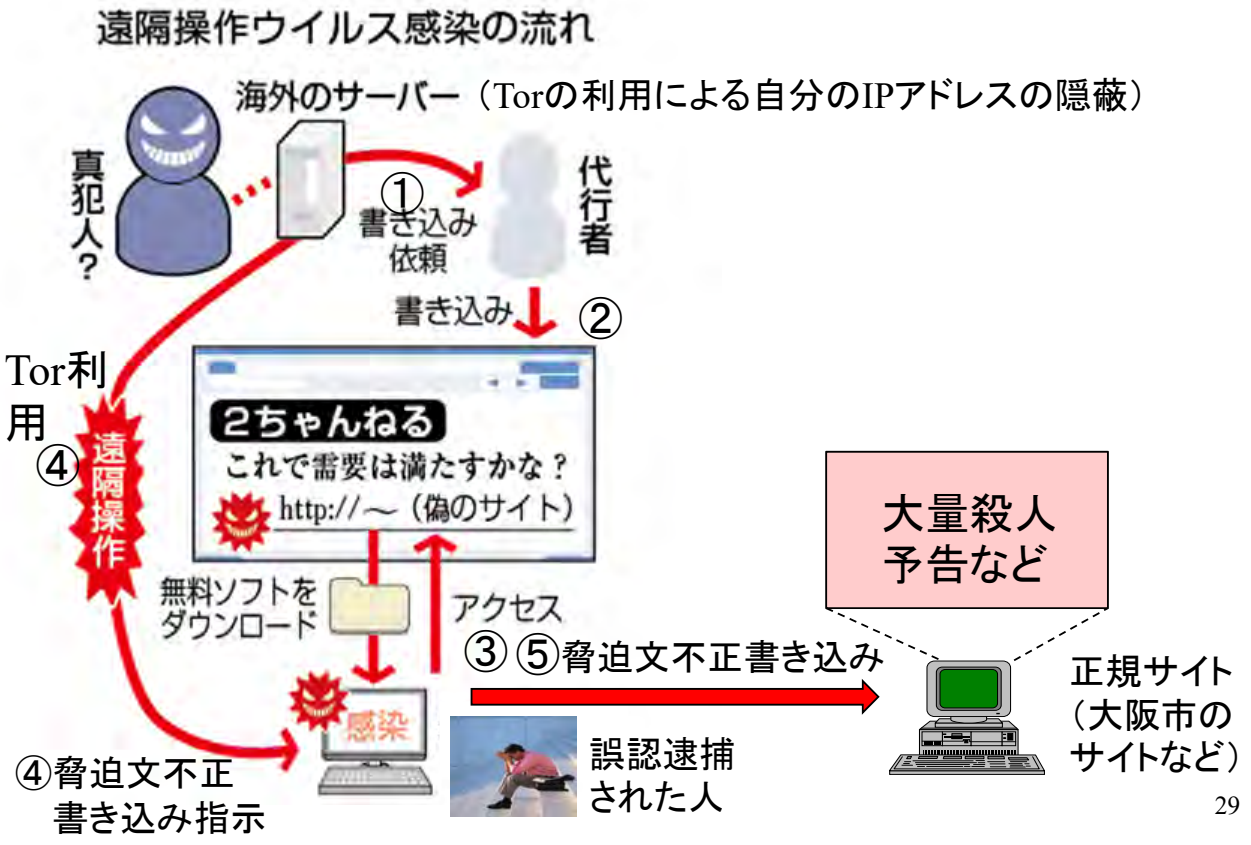
脅迫文書書き込み者の推定方法



誤認逮捕事件（2012年）

事件	逮捕と認否	刑事手続き	攻撃方法
東京の男子大学生（19）			
横浜市のサイトに小学校襲撃予告	神奈川県警が7月逮捕。当初否認	保護観察処分が確定	クロスサイトリクエストフォージェリ
大阪のアニメ演出家男性（43）			
大阪市のサイトに大量殺人予告	大阪府警が8月逮捕。否認	起訴後、釈放	遠隔操作
福岡の無職男性（28）			
幼稚園と有名子役に襲撃予告	警視庁が9月逮捕。供述が変遷	処分保留で釈放	遠隔操作
三重の無職男性（28）			
2ちゃんねるに伊勢神宮爆破予告	三重県警が9月逮捕。否認	処分保留で釈放	遠隔操作

遠隔操作ウイルス事件の概要



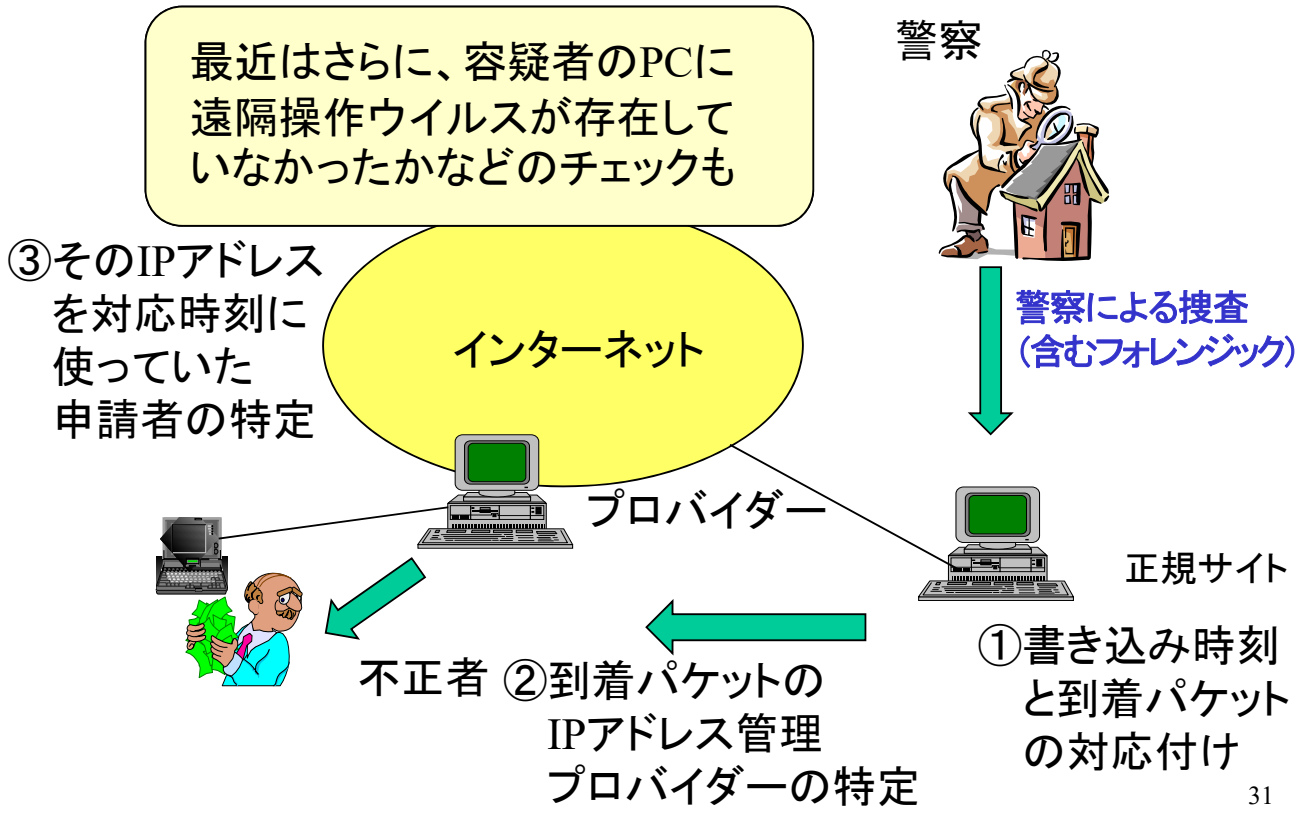
足あとを隠すための方法（Tor）

Tor（The Onion Router）は、TCP/IPにおける接続経路の匿名化を実現するための規格、及びそのリファレンス実装であるソフトウェアの名称。

Torは
①David Chaumが1981年に論文発表した匿名通信方式がMix-net（公開鍵ベース）をベースに
②米国Naval Research Laboratoryがインターネット上で実用的なパフォーマンスを得るためにハイブリッド化（公開鍵＋共通鍵）して実装したOnion（玉ねぎ）Routingを引きついで
③2004年以降米国EFFで実現したもの。（約3000のサーバ）

http://ja.wikipedia.org/wiki/Tor

脅迫文書書き込み者の推定方法



新展開

（1）犯人と思われる人物から2013年1月5日に江の島の地域猫にトロイの木馬ソフトiesys.exeが入っているピンクの首輪をつけたとの犯行声明

（2）防犯カメラの分析により、首輪をつけたと思われる動作をしている男を発見

（3）2013年2月10日に事件の真犯人と目される片山受刑者（当時30歳 ）が逮捕された。

遠隔操作ウイルス事件の経緯（2）

（4）東京地方裁判所で4回行われた勾留理由開示（2013年2月26日・3月21日・5月1日・5月28日）では、法廷で片山受刑者は無実を訴えた。

（5）2014年3月5日収容先の東京拘置所から約1年ぶりに保釈された。

（6）2014年3月13日に開かれた第3回公判で、検察側の証人として出廷したDFの専門家が証人台に

遠隔操作ウイルス片山裁判（1）

2014年3月13日に開かれた遠隔操作ウイルス事件の第3回公判で、検察側の証人として出廷した警察庁情報通信局情報技術解析課の岡田智明技官が証人台に立った。
岡田氏は被告の片山祐輔氏の元勤務先のパソコンに遠隔操作ウイルスの断片が見つかったことを解説した上で、片山氏以外の人間がこれをここに残すことは「非常に困難」との意見を開陳することで、弁護側の、片山氏のパソコンが何者かによって乗っ取られていたとする主張を否定した。

弁護側：真犯人が、片山被告を罪に陥れる目的で、外部から証拠を挿入と主張

http://www.videonews.com/marugeki-talk/675/

遠隔操作ウイルス片山裁判（２）

＜残っていたものに関するより詳しい情報＞

被告人が職場で使っていたPCのHDDイメージを解析した結果、ファイルスラック領域から「iesys.exe」など遠隔操作ウイルスのファイル名やファイルパス、ビルド用ファイルが見つかったほか、ウイルスの作成言語とされたC#の開発環境「Visual C# 2010 Express」について、4回にわたりインストールと削除が行われた履歴、ウイルスファイルが頻繁に変更された履歴などが残されていた。

http://itpro.nikkeibp.co.jp/article/NCD/20140522/558670/

遠隔操作ウイルス片山裁判（３）

＜その当時の私の認識＞

「Visual C# 2010 Expressを繰り返しインストール、削除するような作業を、遠隔操作の痕跡を完全に消し去りつつ、Windows OSに残された履歴の整合性を保ち、かつPCの利用者に気づかれないようGUIを隠蔽しながら行う、というのは非常に困難。」と認識。（検察側ならびに http://itpro.nikkeibp.co.jp/article/NCD/20140522/558670/ の記述にほぼおなじ。）

しかし、当時は真犯人が分からず、天才的な不正者ならひょっとするとできないとは言えないかも知れないとも思っていた

遠隔操作ウイルス事件の経緯（3）

（7）2014年5月20日に真犯人がいると言う偽装がばれ片山受刑者は身柄を拘束され、東京拘置所に再び収監された。

（8）2015年2月4日、東京地方裁判所は爆破予告メールで航空機を引き返させたハイジャック防止法違反も含め、威力業務妨害など10件の犯行を認定、懲役8年の実刑判決。

偽装がばれた経緯

（1）5月16日の公判中、報道関係者などに対し、真犯人を名乗る「小保方銃蔵」からの電子メールが送られてきた。これを以って男性Xも自身の無実が証明されたと訴えた。

（2）15日夕刻に男性Xが荒川河川敷に埋めているのを警視庁の特殊捜査班に所属する捜査員が目撃しており、
後に警察がこれを回収して調査したところ、公判中に発信されたメールの本文が発見され、またスマートフォンから男性Xと同じDNA型が検出された。

https://ja.wikipedia.org/wiki/%E3%83%91%E3%82%BD%E3%82%B3%E3%83%B3%E9%81%A0%E9%9A%94%E6%93%8D%E4%BD%9C%E4%BA%8B%E4%BB%B6

将棋ソフト不正使用疑惑事件と私

1．2016年10月11日、日本将棋連盟はスマートフォンなどによる将棋ソフト不正使用の疑いがあるとして、常務会において三浦九段に説明を求める。

2．10月12日に12月31日までの公式戦出場停止処分を決定。第29期竜王戦七番勝負に出場できなくなる。

3．10月27日、但木敬一を委員長とする第三者調査委員会の設置を決定。

Wikipediaを参照

将棋ソフト不正使用疑惑事件と私

4．12月26日、第三者委員会は、疑惑について処分の根拠とされていた電子機器を使用した形跡はなく、またソフトとの一致率はその性質上根拠とはなり得ず、不正行為に及んでいた証拠はないと発表。

5．2017年1月18日、谷川浩司が会長辞任。

Wikipediaを参照

フォレンジック調査

1．専門業者
　　FRONTEO
2．提出を受けた電子機器
・三浦棋士が契約名義であるスマートフォン1台
・三浦棋士の配偶者が契約名義であるスマートフォン1台
・三浦棋士が使用していたデスクトップパソコン2台、
　ノートパソコン2台
・三浦棋士の配偶者が使用していた
　デスクトップパソコン1台、ノートパソコン1台
・三浦棋士の母が使用していたタブレット1台

https://www.shogi.or.jp/news/investigative_report_1.pdf

FRONTEOによる調査結果の一部

	解析対象電子機器	将棋GUIアプリケーション	将棋ソフト	リモートデスクトップアプリケーション	本件4対局中の起動・使用状況
1	三浦棋士が使用していたスマートフォン（以下「本件スマートフォン」という。）	確認されず	確認されず	確認されず	本件4対局中の使用履歴は確認されず
2	三浦棋士の配偶者が使用していたスマートフォン	確認されず	確認されず	確認されず	本件4対局中に多数の使用履歴が存在するが、本件映像分析による対局映像の分析によれば、対局中の三浦棋士が電子機器を操作する様子等は確認されていないこと等をふまえれば、同棋士による使用とは判断されない

https://www.shogi.or.jp/news/investigative_report_1.pdf

毎日新聞2017年1月17日朝刊

三浦九段

対局中 使用履歴なし

ソフト不正疑惑 報告書概要公表

日本将棋連盟（谷川浩司会長）は16日、三浦弘行九段(42)の将棋ソフト不正使用疑惑について第三者調査委員会（但木敬一委員長）が「証拠は認められなかった」と結論づけた調査報告書の概要版を連盟の公式サイト（http://www.shogi.or.jp）で公開した。調査委は昨年12月、調査結果を記者会見で説明したが、報告書は公表していなかった。

公開されたのは報告書全文のうち約40％。調査の手法や結果データなどをまとめた「別紙」は、将棋連盟が「個人情報が含まれる」ことを理由に公表しなかった。

概要版によると、調査委は、三浦九段側から本人や妻、母が所有するスマートフォン2台、パソコン6台、タブレット1台の提出を受けた。データ解析会社に依頼し、将棋ソフトや遠隔操作ソフトの有無、疑惑を持たれた対局時間中の使用状況などを調べた結果、三浦九段のスマホにソフトがインストールされた痕跡や、対局時間の使用履歴は確認されなかった。パソコン3台には将棋ソフトがあったが、遠隔操作ソフトはなく、対局時間は「スリープ」や「シャットダウン」状態で起動していなかった。

妻のスマホやパソコンには対局時間に使用履歴があったが、対局映像などから「三浦九段による使用とは判断されない」とした。【山村英樹、最上聡、丸山進】

結論は妥当

電磁的記録の調査分析に詳しい佐々木良一・東京電機大教授（情報セキュリティー）の話 もしデータを消しても、おかしな部分は残り、全てを矛盾なく変えるのは難しい。結論は妥当と言える。問題は対象の機器を全て集められたかという点。デジタル鑑識の分野でも、完全に「黒」「白」を付けるのは難しいが、今回は家族のものも含め、通常考えられる範囲は集めたと言えるだろう。

①パソコンソフトにアクセスし、してないように偽装しても専門家が調べれば何らの証拠はかならず残る。
②本人以外のPCなどを広く調査の対象としている。

アクセスしていない可能性が強い

日本におけるDF関連論文の調査

- “Digital Forensics”、“デジタル・フォレンジック”でCiNiiを調査

CiNii is a searchable database service containing academic information on articles, books, etc in Japan.

DF関連研究記事数の推移

Year	Number of Articles
2006	4
2007	6
2008	11
2009	13
2010	2
2011	7
2012	4
2013	11
2014	7
2015	12
Total	78

合計: 78

平均: ~8

海外誌に含まれるものは除く

主要な研究の位置づけ

応用

理論

②DFガイドシステム

⑤ NWフォレンジック

④ 証拠保全方式

③ LIFT システム

⑥DFとプライバシー

① ログの署名方式

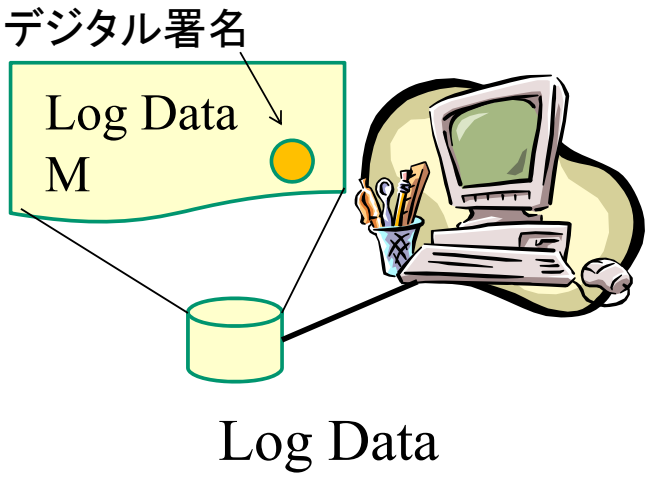
（⑦その他）

要素的 ⟷ システム的

LIFT: Live and Intelligent Network Forensic Technologies

背景

- 証拠確保のためにログの収集と署名が必要に。

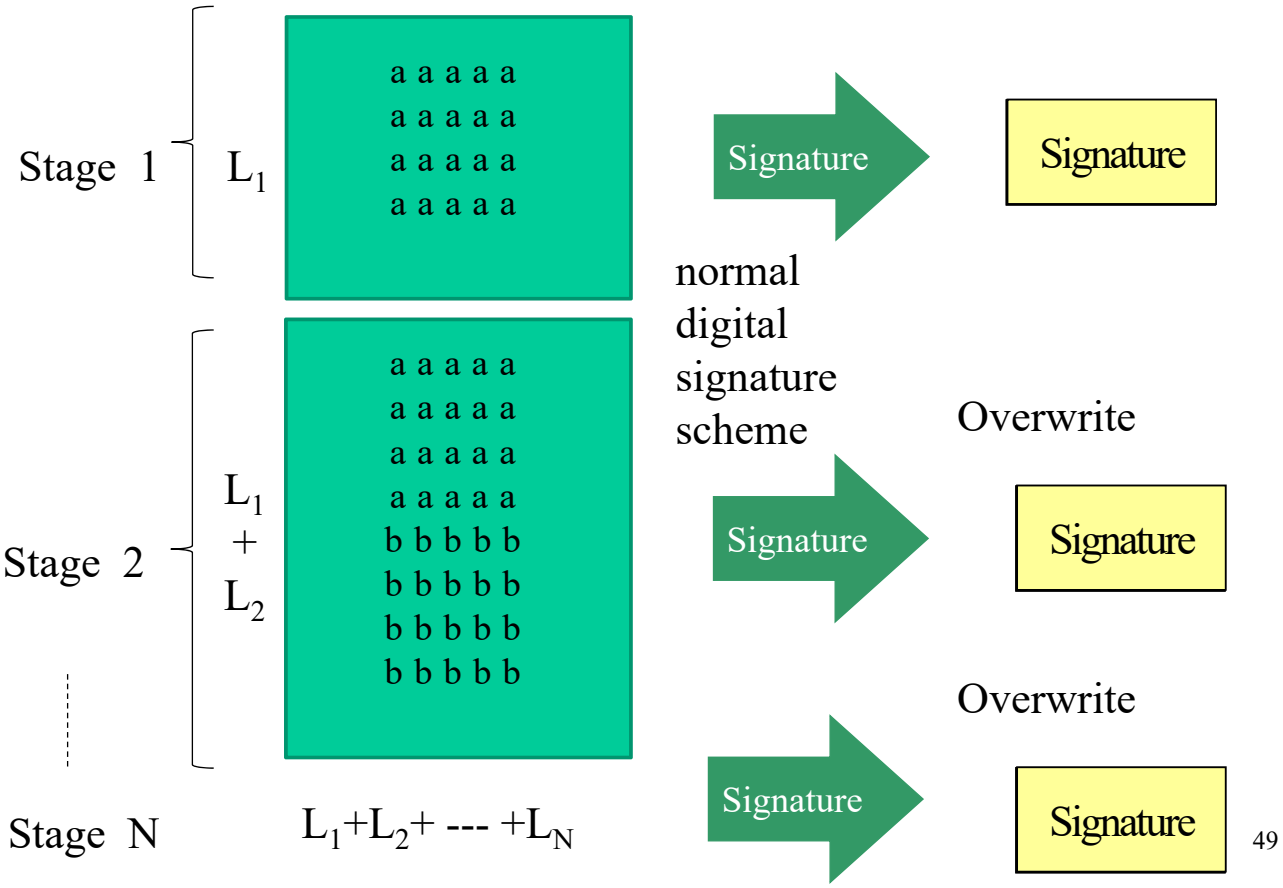


Sig = S(h(M))
where
Sig: デジタル署名
h:ハッシュ関数
S:秘密鍵を用い公開鍵暗号方式を適用

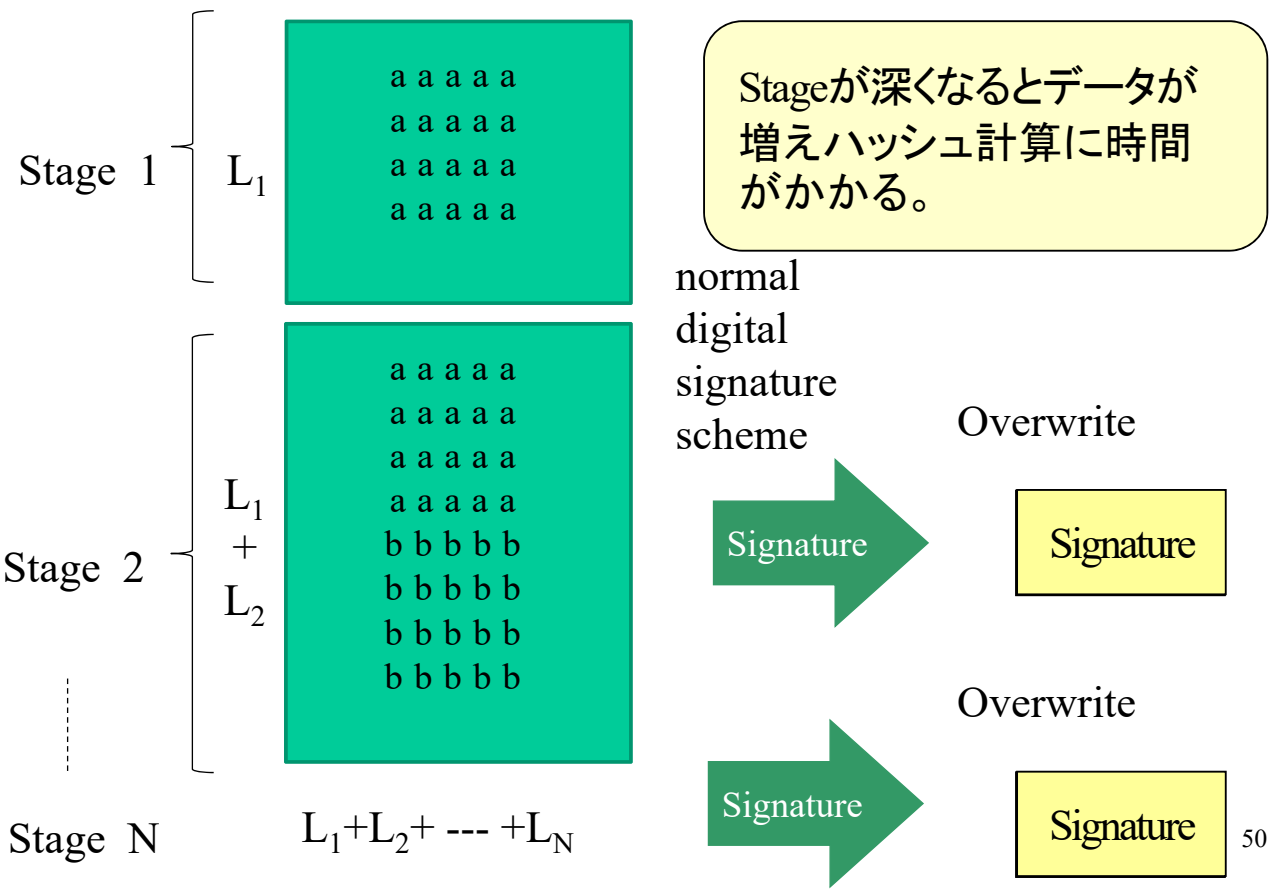
ログへの署名の基本方式

- ログデータは間欠的に出てくるのでそのたびに署名が必要
- しかし、間欠的に出てきた元のログデータと署名を同時に消去すると検知不可能

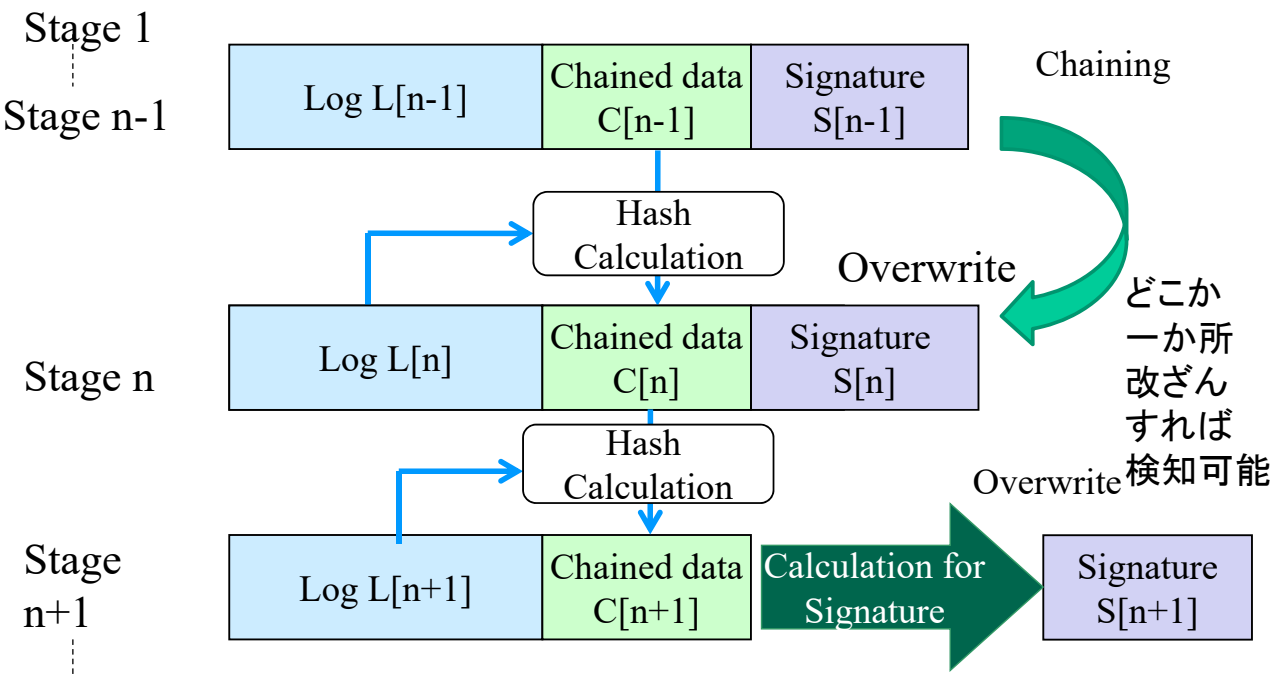
単一署名方式



単一署名方式

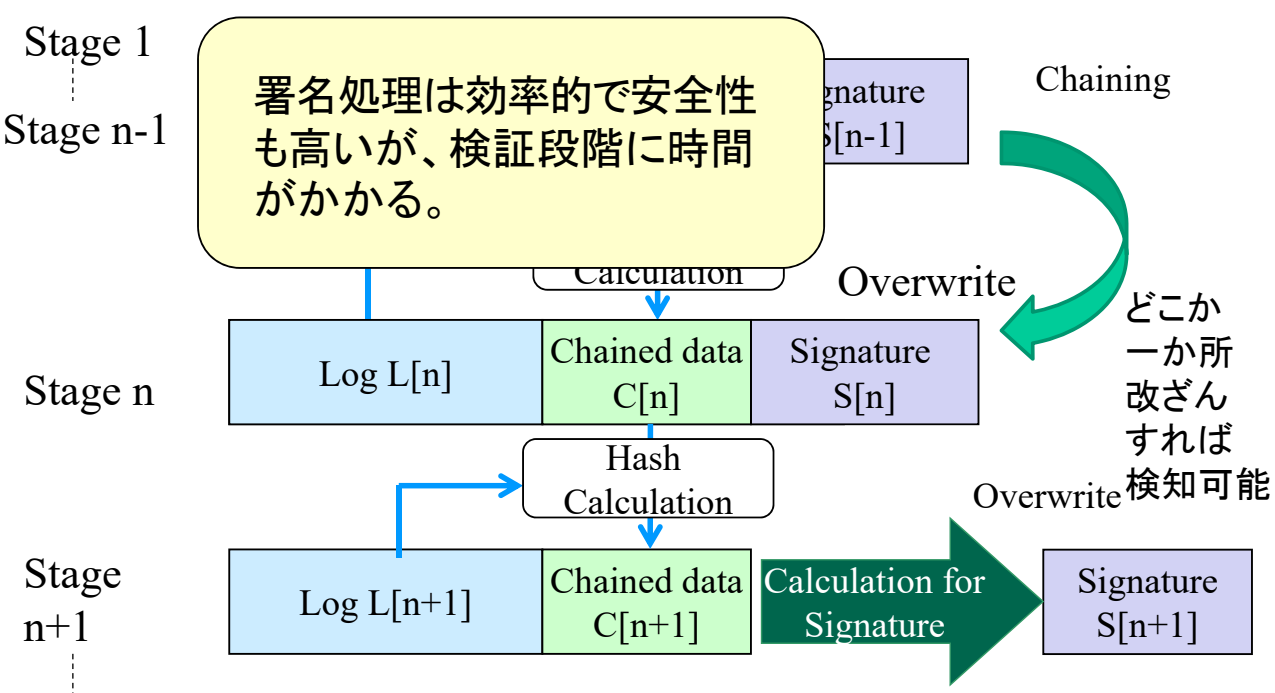


ヒステリシス署名方式



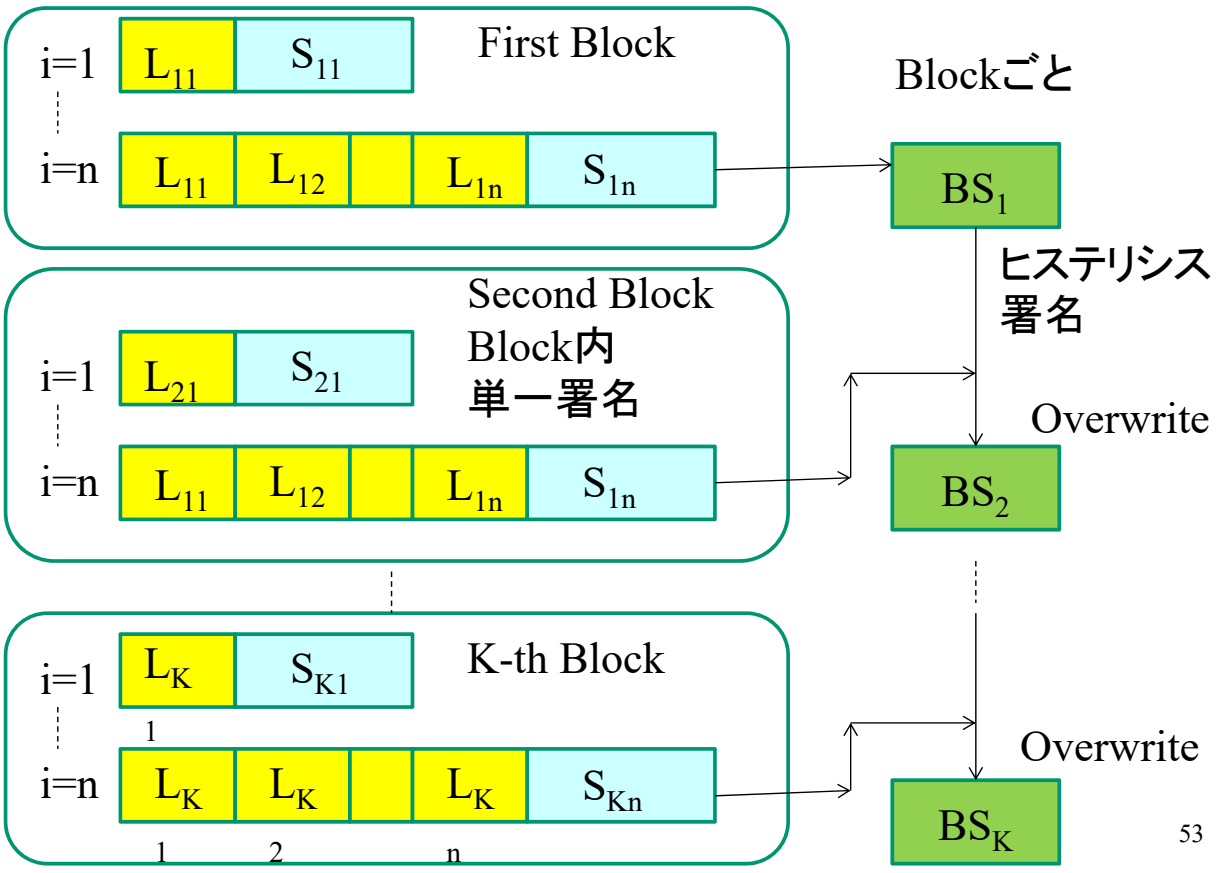
ブロックチェーンの一種。2000年ごろ開発。
岩村充、宮崎邦彦、松本勉、佐々木良一、松木武「電子署名におけるアリバイ証明問題と経時証明問題　ヒステリシス署名と電子古文書の概念」bit, Nov.2000, Vol32,No.11

ヒステリシス署名方式



ブロックチェーンの一種。2000年ごろ開発。
岩村充、宮崎邦彦、松本勉、佐々木良一、松木武「電子署名におけるアリバイ証明問題と経時証明問題　ヒステリシス署名と電子古文書の概念」bit, Nov.2000, Vol32,No.11

ハイブリッド署名方式（提案方式）



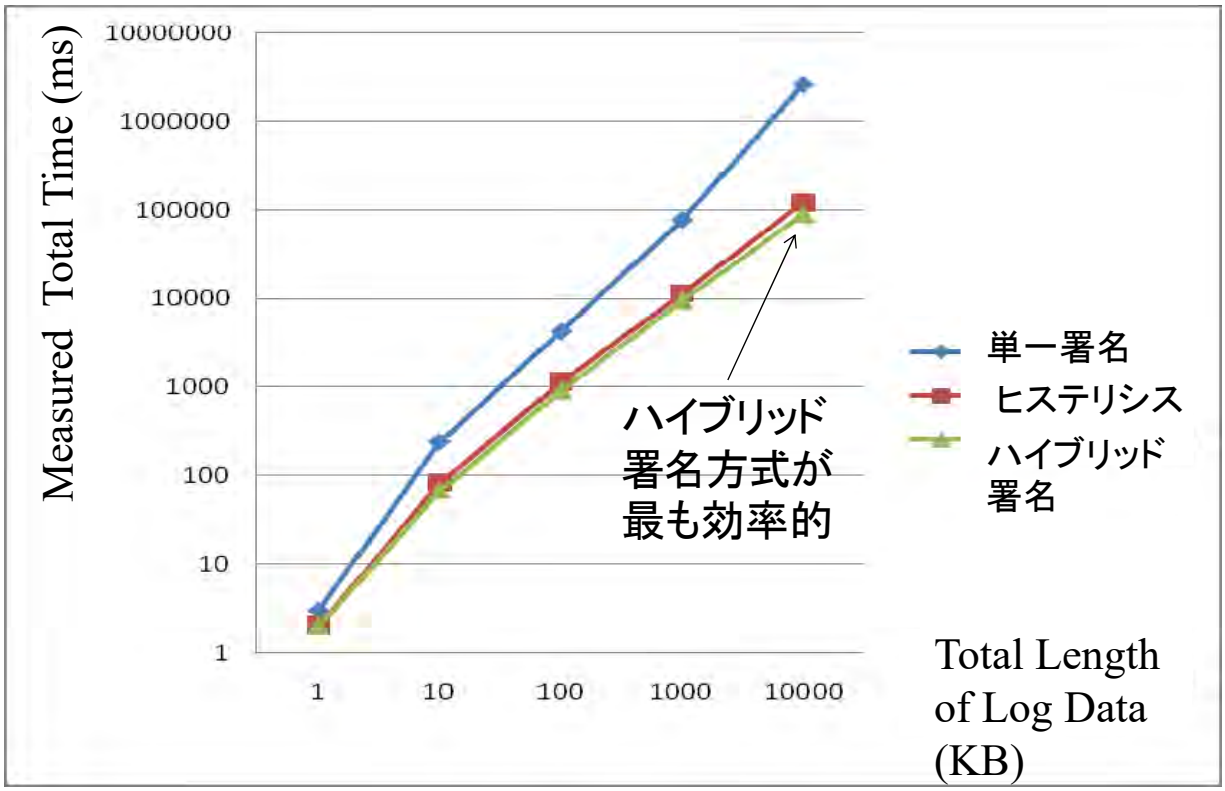
実験環境

(1) CPU: Intel Core i5
(2) OS: Windows 7 Enterprise 64-bit
(3) RAM: 2 [GB]
(4) SSD: 120 [GB]
(5) Development language of the computer program for the experiment: C#

Parameter values

1	K: Number of blocks	200
2	n: Number of log data in each block	5
3	L: Length of each log data	1 KB
4	N: Number of log data	1000
5	L*N	1 MB

トータル演算時間の測定結果



関連論文

1] 上田、佐々木他「データ喪失を想定したヒストリシス署名方式評価手法の提案」情報処理学会論文誌第45第8号 pp1966-1976,2004

12] 小林、佐々木「証拠性保全のための安全で効率的なログ署名方式の提案と評価」日本セキュリティマネジメント学会誌28巻第2号2014年9月pp11-21

13] Naoki Kobayashi, Ryoichi Sasaki,「Proposal and evaluation of an evidence preservation method for use in a common number system」nternational Journal of Electronic Commerce Studies vol.6,no.1,pp51-68, 2015

ネットワーク・フォレンジックとは

ネットワーク・フォレンジックとは、「セキュリティ上の攻撃や問題を発生させるインシデントの発生源を発見するために、ネットワーク上のイベントをキャプチャ、記録、分析すること」である。

Marcus J. Ranum
セキュリティ・システムの設計や開発の専門家として世界的に有名。プロキシー型ファイアウォールの発明者として、1980年代に最初の商用ファイアウォールを提供。

背景

- サイバー攻撃がますます激烈化・巧妙化
- 不正通信の原因を確認することが不可欠に

研究の目的（その1）

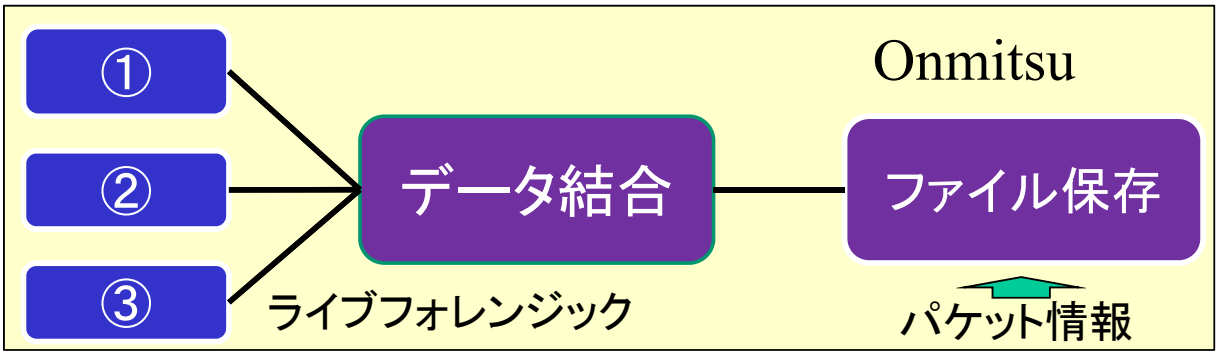
```
62.113.232.164      54 49446 > http [ACK] Seq=231 Ack=154 Win=131328 Len=0
62.113.232.164      54 49446 > http [FIN, ACK] Seq=231 Ack=154 Win=131328 Len=0
192.168.137.69      54 http > 49446 [FIN, ACK] Seq=154 Ack=231 Win=15680 Len=0
```

不正な通信とPCの中で動いている
プロセスの関連を知りたい　＝＞
これを可能とするロガープログラム
Onmitsuを開発

Onmitsuにおけるライブフォレンジック

パケット情報と、PC内のプロセスの動きを関連付けて記録することにより、不正パケットが発信された原因などを明確化するツール

- Windows Filtering Platform - ①
- PsSetCreateProcessNotifyRoutineEx - ②
- PsSetLoadImageNotifyRoutine - ③



三村聡志、佐々木良一「プロセス情報と関連づけたパケットを利用した不正通信原因推定手法の提案」情報処理学会DICOMO2014

Onmitsuによるログ収集例

TYPE	PID	PARENT	CMDLINE	SRCPORT	DSTIP	DSTPORT
PROCESS_LAUNCH	1832	1848	C:¥Users¥TESTUSER¥Desktop¥SHARE¥invoice_928649039284232_9482934d88.pdf.exe			
PROCESS_LAUNCH	2068	1832	C:¥Users¥TESTUSER¥AppData¥Local¥Temp¥zdttuqbg.exe			
PROCESS_LAUNCH	1896	2068	C:¥Users¥TESTUSER¥AppData¥Local¥Temp¥zdttuqbg.exe			
PROCESS_LAUNCH	2716	752	C:¥Program Files¥Internet Explorer¥iexplore.exe -Embedding			
NETWORKV4	2716			49446	62.113.232.164	80
NETWORKV4	2716			49447	62.113.232.164	80
PROCESS_QUIT	2716					
NETWORKV4	1896			49450	178.250.245.198	80

PID 2716

PID 1896

```
62.113.232.164      54 49446 > http [ACK] Seq=231 Ack=154 Win=131328 Len=0
62.113.232.164      54 49446 > http [FIN, ACK] Seq=231 Ack=154 Win=131328 Len=0
192.168.137.69      54 http > 49446 [FIN, ACK] Seq=154 Ack=231 Win=15680 Len=0
62.113.232.164      54 49446 > http [ACK] Seq=232 Ack=155 Win=131328 Len=0
62.113.232.164      54 49447 > http [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
192.168.137.255     92 Name query NB WPAD<00>
192.168.137.69      54 http > 49446 [ACK] Seq=155 Ack=232 Win=15680 Len=0
64.4.11.42         363 GET / HTTP/1.1
192.168.137.69     714 HTTP/1.1 302 Found  (text/html)
64.4.11.42          54 49437 > http [ACK] Seq=1255 Ack=41924 Win=65280 Len=0
178.250.245.198     66 49450 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SA
192.168.137.69      66 http > 49450 [SYN, ACK] Seq=0 Ack=1 Win=12600 Len=0 MSS=12
178.250.245.198     54 49450 > http [ACK] Seq=1 Ack=1 Win=132096 Len=0
178.250.245.198    779 GET /V7MqD64K7VJOOHWZvlU7oe4s%2feLsgFA%2foi1kOacN4S0tN1RtS
192.168.137.69      54 http > 49450 [ACK] Seq=1 Ack=726 Win=14080 Len=0
192.168.137.69     207 HTTP/1.1 503 Service Unavailable  (text/html)
```

Onmitsuによるログ収集例

TYPE	PID	PARENT	CM
PROCESS_LAUNCH	1832	1848	C
PROCESS_LAUNCH	2068	1832	C
PROCESS_LAUNCH	1896	2068	C
PROCESS_LAUNCH	2716	752	C
NETWORKV4	2716		
NETWORKV4	2716		
PROCESS_QUIT	2716		
NETWORKV4	1896		

マルウエアが立ち上がったり、テンポラリーファイル内の他のプログラムを活性化するのを知ることができる。

また、インターネットエクスプローラの立ち上げ後マルウエアが通信をスタートするのを知ることができる。

PID 2716

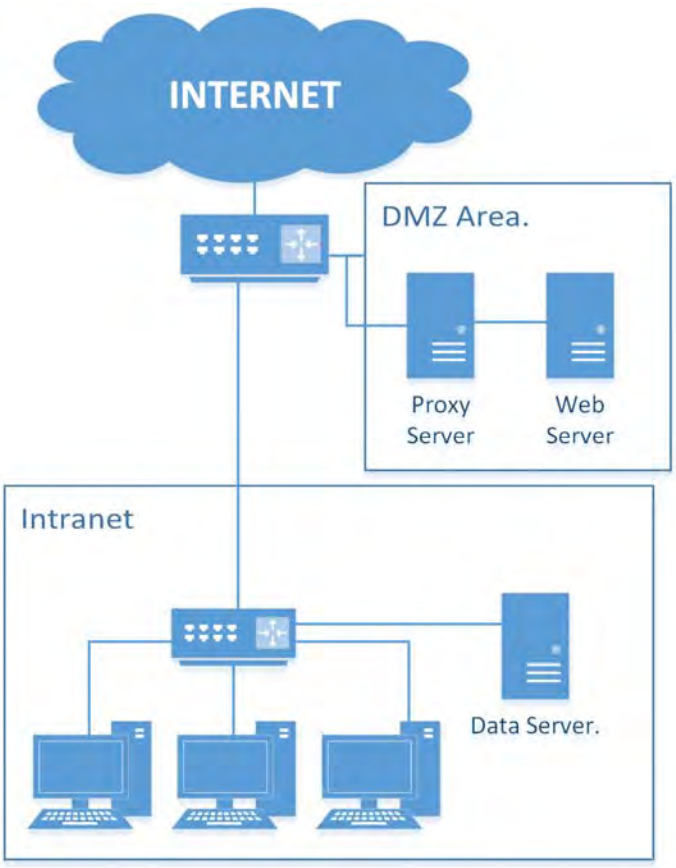
PID 1896

```
62.113.232.164
62.113.232.164
192.168.137.69
62.113.232.164
62.113.232.164
192.168.137.255
192.168.137.69      54 http > 49446 [ACK] Seq=155 [illegible]=232 Win=15680 Len=0
64.4.11.42         363 GET / HTTP/1.1
192.168.137.69
64.4.11.42
178.250.245.198
192.168.137.69
178.250.245.198
178.250.245.198
192.168.137.69      54 http > 49450 [ACK] Seq=1 Ack=726 Win=14080 Len=0
192.168.137.69     207 HTTP/1.1 503 Service Unavailable  (text/html)
```

Onmitsuによるログは有用

63

ネットワークを用いた実験環境



Microsoft Windows Vista or later is required for the client PC as for the OS version.

64

実験結果 ①

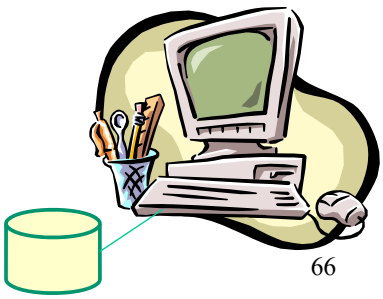
- ログファイルサイズ
  - Onmitsu試験利用時間: 3 hours.
  - ファイルサイズ: 10,868,492 (10.36 MB)
    "zip" による圧縮後 : 755,732 bytes (738.01 KB / 6.95%)
  - 1年間の推定データ量.
    - 2,205,651,767 bytes (2.05 GB)

➡ 最近のPCは1TB程度の容量があるので許容範囲と判断

実験結果 ②

- Onmitsu を導入することによる処理負荷の増大は1%程度

➡ 負荷の増大は無視できる



現在の状況

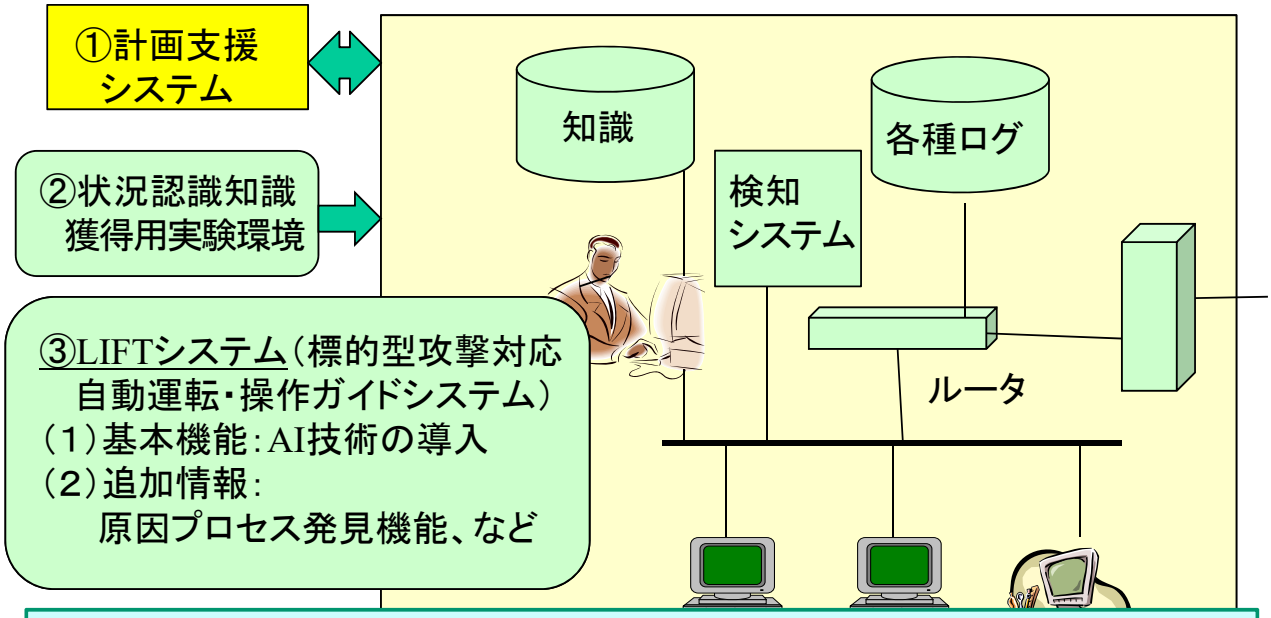
1. Onmitsu は企業に移管されCapLoggerとして製品化
2. LAN上の複数のPC内のOnmitsuを用い、マルウエア感染源の推定する方法を確立
3. 現在、LAN内の感染範囲の推定法を確立中

関連論文

16] 三村聡志、佐々木「プロセス情報と関連づけた通信情報保全手法の提案」情報処理学会論文誌, Vol.57,No.9,pp1944-1953,2016

17] 佐藤、佐々木他「マルウエアによるネットワーク内の挙動を利用した標的型攻撃における感染経路検知ツールの開発と評価」情報処理学会論文誌, Vol.58,No.2,pp1-9,2017

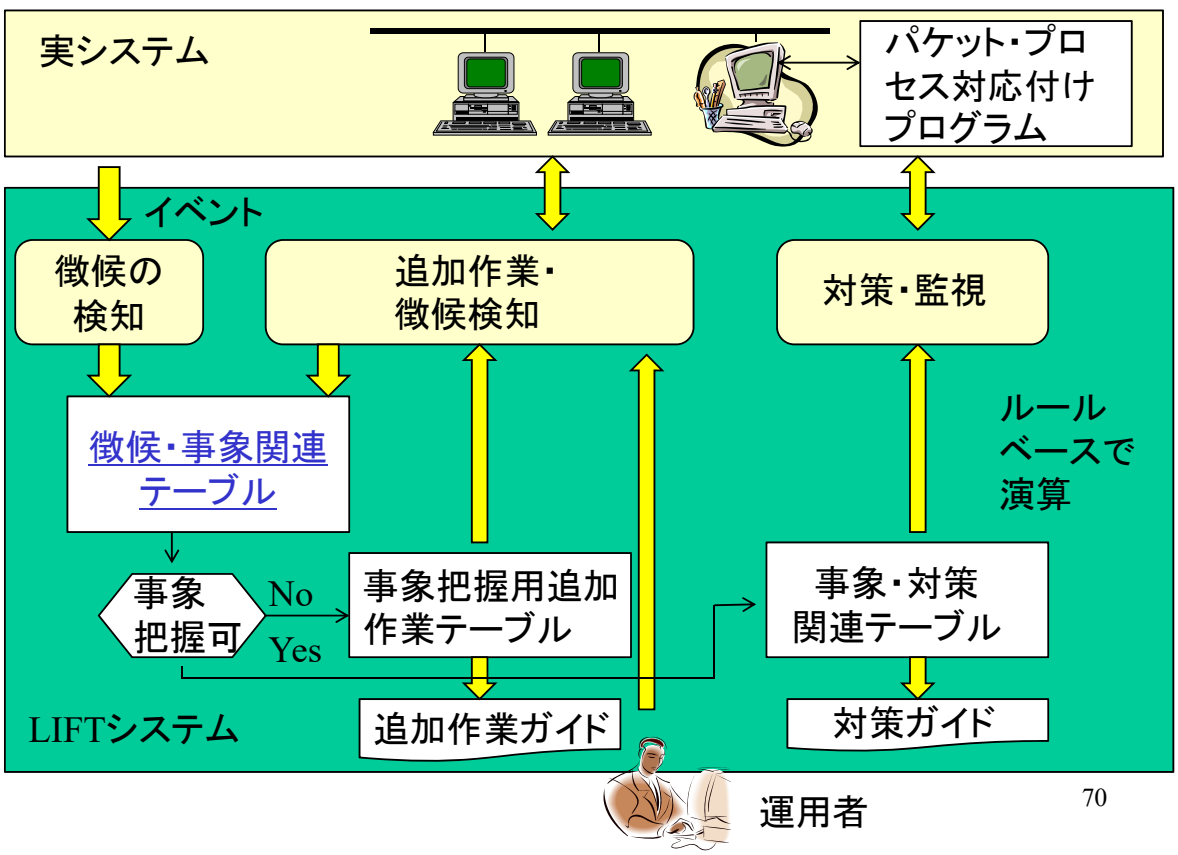
LIFTプロジェクトの概要



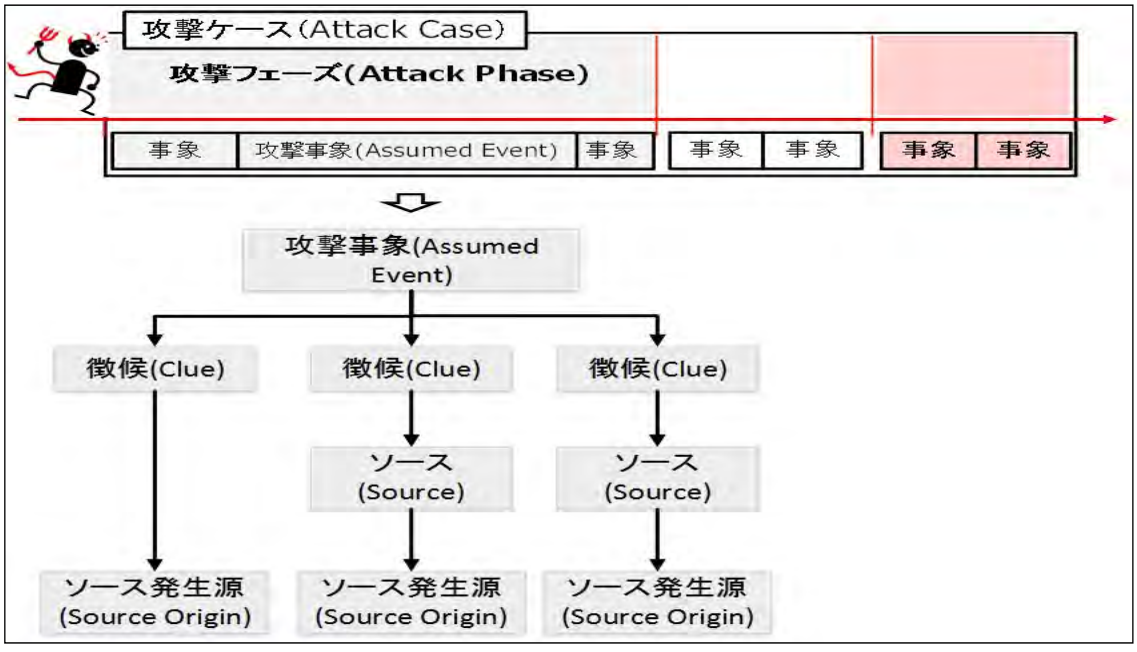
③LIFTシステム（標的型攻撃対応
自動運転・操作ガイドシステム）
（1）基本機能：AI技術の導入
（2）追加情報：
原因プロセス発見機能、など

共同開発プロジェクト （リーダ佐々木、上原先生、高倉先生、八槙先生、
柿崎先生、日立他） 期間：2013年9月ー2018年3月（第一期）
現状での主な成果：①方式確立 ②原因プロセス発見ソフト開発

LIFTシステムの運用イメージ



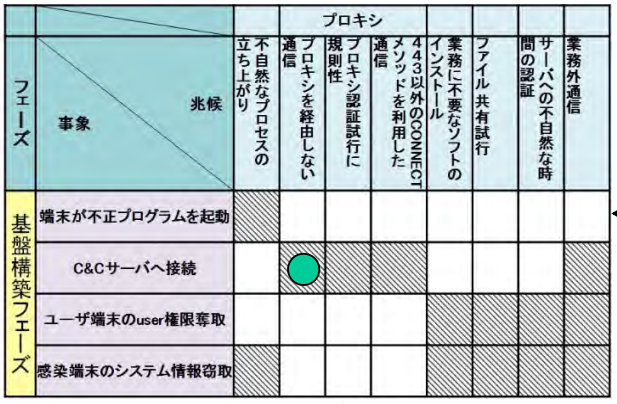
攻撃における各種名称の階層構造



徴候・事象関連テーブルと確信度

	攻撃事象 \ 徴候	不自然なプロセスの立ち上がり	プロキシ		長時間のセッション	業務に不要なコマンド
			プロキシを経由しない通信	443以外のCONECTメソッドを利用した通信		
基盤構築フェーズ	端末が不正プログラムを起動	0.3				
	C&Cサーバへ接続		0.6	0.6	0.4	
	必要な機能のダウンロード	0.4	0.4		0.3	
	端末の情報入手	0.5			0.2	0.4

事象把握用追加作業の例



徴候：プロキシーを経由しない通信

事象シーケンス

事象候補：不正C&Cサーバへの接続

②端末が不正プログラムを起動しているかどうかの確認

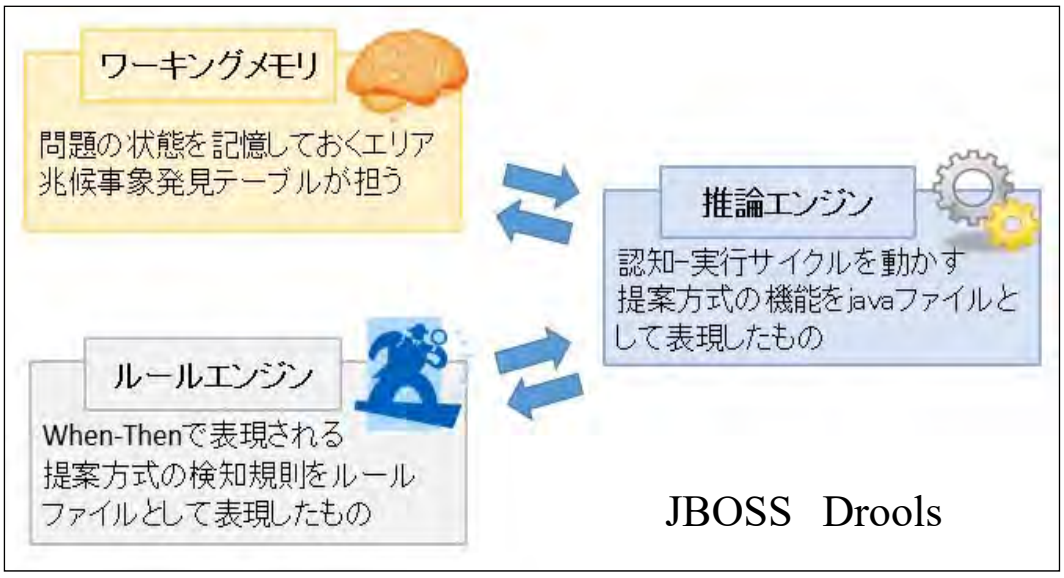
①確信度向上のための徴候チェック

追加作業候補：候補PCの把握
候補PCのパケットと対応プロセスの関連付け
（パケット・プロセス対応付けプログラムの利用）
親プロセスが不正プログラムであることの発見

事象・対策関連テーブル

フェーズ	事象＼対応	ルータで該当端末Pの遮断	ルータで該当ポートの遮断	ルータで該当通信ドメインの遮断	該当端末のインバウンド通信の遮断	該当端末のアウトバウンド通信の遮断	該当ネットワーク遮断	該当端末が所属するネットワークの隔離	ネットワーク全体の遮断	該当端末の隔離
基盤構築フェーズ	端末が不正プログラムを実行	有効でない	有効でない	有効でない	有効でない	有効でない	有効でない	有効でない	有効でない	有効
	C&Cサーバへ接続	有効	有効	有効	有効	有効	有効	有効	有効	有効
	ユーザ端末のuser権限奪取	有効でない	有効でない	有効でない	有効	有効	有効	有効でない	有効でない	有効
	感染端末のシステム情報窃取	有効でない	有効でない	有効でない	有効でない	有効でない	有効でない	有効でない	有効でない	有効

ルールベースプログラムの構成



ルールベースプログラムの例

JBOSS Droolsを用いた簡単なプログラムを作成

```
rule "Support"↓
        agenda-group "Aggregation"↓
    when↓
      sign : Sign ()      event : Event ()↓
      support : Support (signId == sign.getID() && eventId == event.getID() &&
effective != true)↓
      Detected (signId == sign.getID())↓
      sourceSupport : SourceSupport(signId == sign.getID() && collectFlag == tru
e)↓
    then↓
      support.setEffective (true);↓
      update (support);↓
      System.out.println ("※Rule Support fired.");↓
      System.out.println ("Assumed Event" + event.getID() + "(" + event.getDescr
iption () + ") is supported by detected Clue " + sign.getID() + "(" ↓
      + sign.getDescription() +  ") with score(確信度) = " + support.getScore();
↓
end↓
```

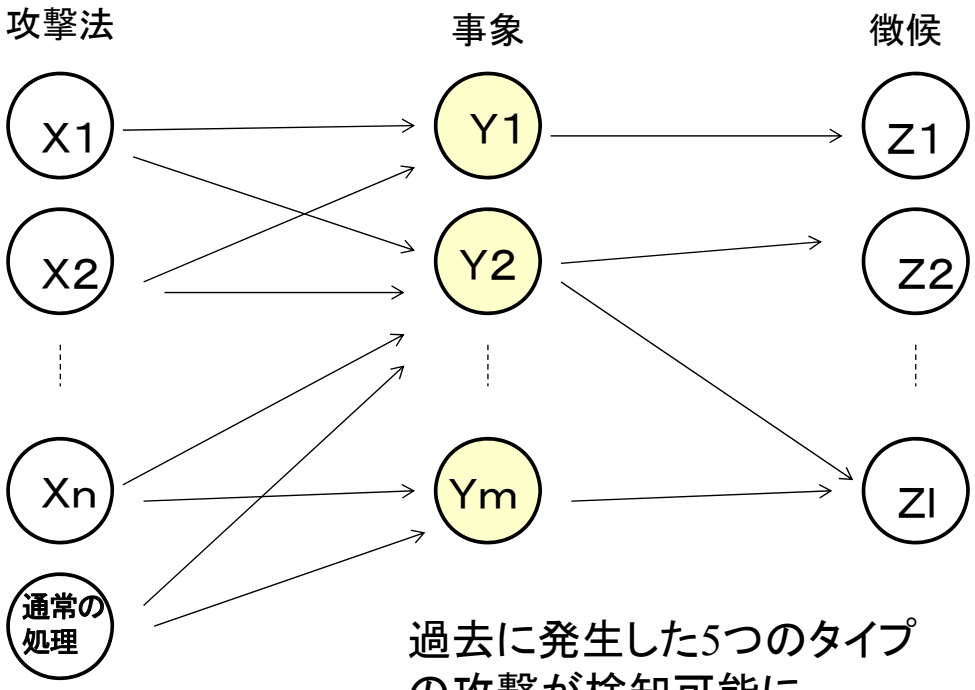
開発プログラム実行画面

```
1 Clue:308(プロキシを経由しない通信)がDetectされました↓
2 Assumed Event:305(C&Cサーバへの通信)の可能性があります↓
3 ↓
4 ※Rule NotSupport fired.↓
5 Mini Clue: 308(プロキシを経由しない通信) のソース 201(Router_log)は取られていま
6 せん↓
7 Mini Clue: 308 のソース 201の取得をONにします↓
8 ↓
9 ※Rule Support fired.↓
10 Assumed Event305(C&Cサーバへの通信) is supported by detected Clue 308(プロキシを
11 経由しない通信) with score(確信度) = 5↓
12 Certainty for Assumed Event305  is 5↓
13 ↓
14 ※Rule Calculate Certainty fired.↓
15 =====↓
16 Most likely event is Assumed Event(C&Cサーバへの通信) with certainty(確信度) = 5↓
17 =====↓
```

基本的適用可能性を確認

LIFTのGUI

ベイジアンネットワーク利用による事象推定方式の提案



過去に発生した5つのタイプの攻撃が検知可能に

Super-LIFTシステム開発の構想

- 既存の攻撃であれば、LIFTシステムをブラッシュアップすることで、自動運転やガイドが可能な見通しに。
- しかし、新しい攻撃に対応できず、セキュリティ技術者は常に後追いの対応しかできなかった。
- 限界を打ち破り、プロアクティブな対策が行えるようにしたい。

Super-LIFT研究の背景

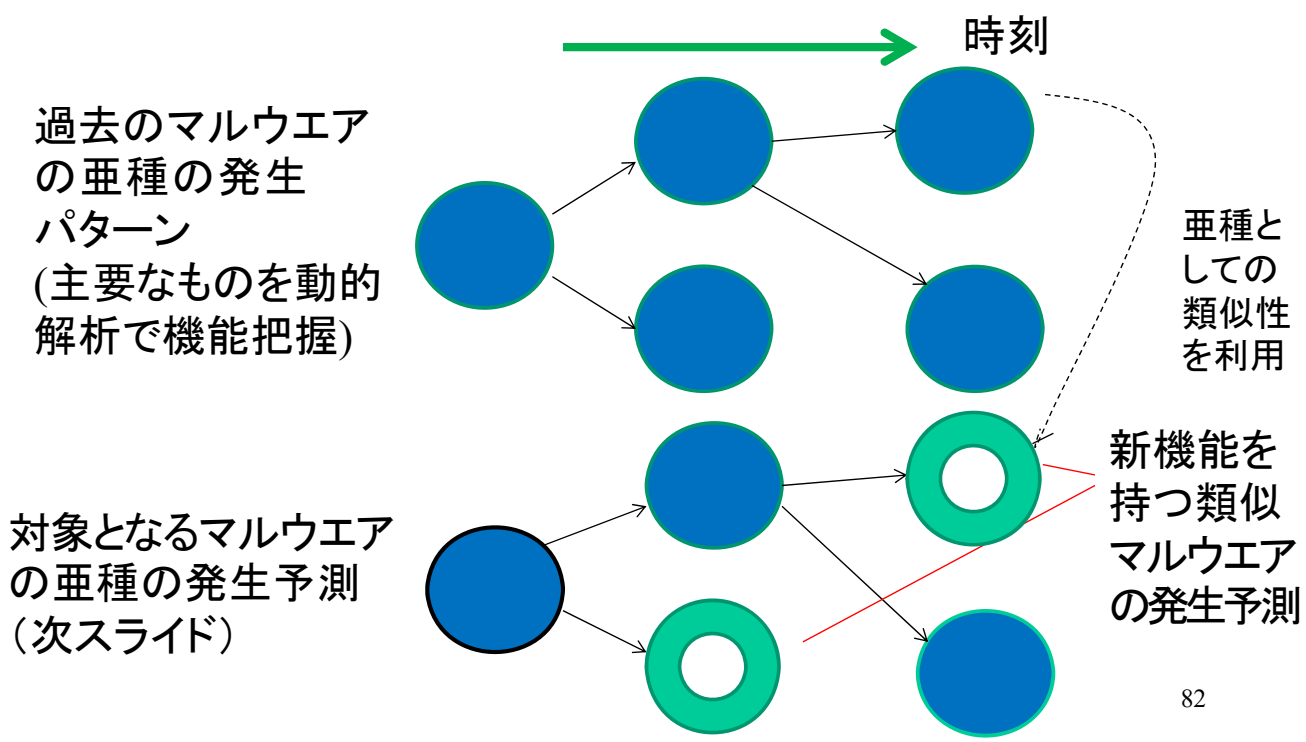
セキュリティ対策は、被害を受けてから、対策を始める後追い型研究だった

AIを高度に利用し、人間の能力を超える対応を可能に

AIを高度利用し、Beyond the Attackers技術を実現し、Proactiveな対策を可能にする研究の実施

新機能を持つ類似マルウエアの予測法（1）

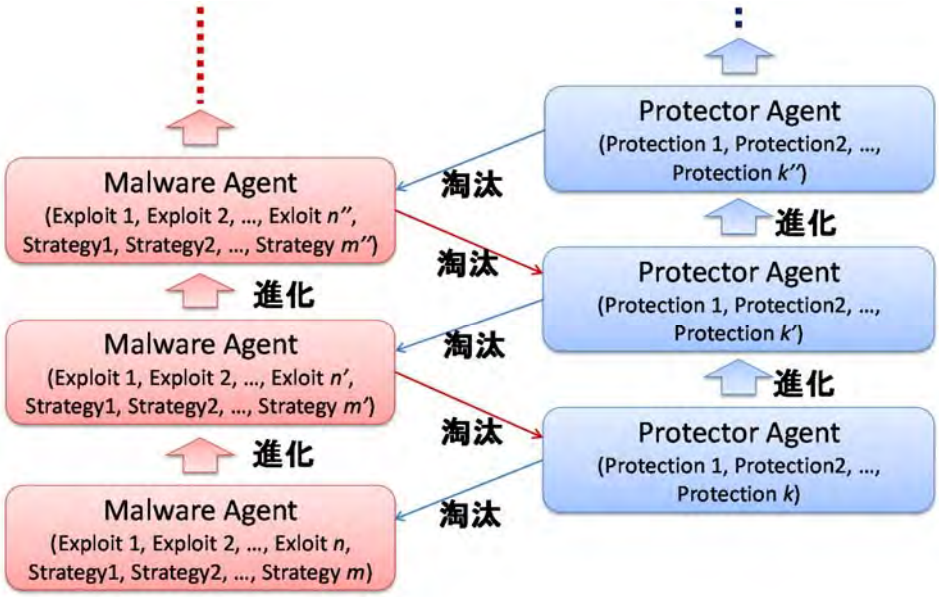
パターンマッチングによる出現の予測法



新機能を持つ類似マルウエアの予測法（2）

共進化モデルに基づく新しいマルウェアの予測

基本的考え方：どちらか一方が単独で進化するのではなく、
互いへの対応の中で高度化していく



進化のプロセスについてはGAを利用予定

Development of intellectual network forensic system LIFT against targeted attacks

Kazuki Hashimoto,Hiroyuki Hiruma, Takashi Matsumoto, Kosetus Kayama, Yoshio Kaikizaki, Hiroshi Yamaki, Ryoichi Sasaki
Tokyo Denki University
5 Senju Asahi-cho, Adachi-ku, Tokyo, JAPAN
hashimoto@isl.im.dendai.ac.jp,
hiruma@isl.im.dendai.ac.jp,
sasaki@im.dendai.ac.jp

Tetsutaro Uehara

Ritsumeikan University
1 Nojihigashi, Kusatsu, Shiga, JAPAN
Uehara@cs.ritsumei.ac.jp

***Abstract*—Recently, the number of targeted attacks to specific organizations, such as companies or governments, has been increasing. Although such organizations are required to conduct to protect against the attack or mitigate the effect of the targeted attack, it is very difficult to perform the proper operation without the assistance of a support system. Therefore, the authors developed the Live and Intelligent Network Forensic Technologies (LIFT) system to guide the proper operation and/or conduct an automatic operation using artificial intelligence. The LIFT system collects the logs from servers, PCs, and communication equipment such as routers and detects abnormal signs from the collected logs. Next, the**

to perform the proper operation without the assistance of a support system.

The Security Information and Event Management (SIEM) system has been attracting attention as a support system against targeted attacks [3]. The SIEM system gives real-time security threat detection capabilities to the log management system. Because it performs network forensics in real time, SIEM can be called a live network forensics system. Network forensics secures the evidence of saved collections for an analysis of a log in real time.

However, it is difficult to protect against an attack or

Cybersec 2015 held in Indonesia

デジタル・フォレンジックに関する新しい動き(1)

1．ディスクの変化へのDFの対応
　SSDの普及

2．ディスクフォレンジック以外のフォレンジックの重要化
（1）ネットワークフォレンジック
（2）メモリーフォレンジック（ライブフォレンジック）
（3）クラウドフォレンジック
（4）スマートフォンフォレンジック、SCADAフォレンジックなど

デジタル・フォレンジックに関する新しい動き(2)

3．E-Discoveryにおける新しい動き
（1）関連ファイルの抽出のための機械学習の導入
（2）抽出や処理のための日本語情報処理の高度化

4．新しい応用分野
　デジタル遺品対応

5．デジタル・フォレンジックはますます重要に。会員の方々のいろいろな分野での活躍を期待。

デジタル遺品とは

遺品とは、個人が残した現金や有価証券など、資産価値がはっきりとわかるもの以外の物品のことをいう
Ex. 家具やコレクションなど

- デジタル遺品とは、デジタルで遺された情報のこと
  Ex. PCやスマートフォン上に残っているデータ
  インターネットバンキングやSNSのアカウントなどの情報

デジタル遺品の問題点

- 実際のトラブル例（FXの場合）

FX会社「すみません、『FXトレード』ですが、ご主人のことで、実はご主人が
１５００万円の損失を出していらっしゃいまして」
奥さん　「１５００万？！どういうことですか？」
夫の死後、相場が大きく動き、為替レートが大暴落、１５００万円の損失となってしまった。
奥さん　「だから、夫は、半年前に亡くなってるんですって・・・」
FX会社「そう言われましても、こちらには取引キャンセルの通知がきていないので、
取引は続いているんです」

※夫のPCから浮気写真がでてきた…といったことも起こっている

※（出典）荻原栄幸 “「デジタル遺品」が危ない” ポプラ社 2015-10-01

デジタル遺品の問題点

- 実際のトラブル例（FXの場合）

FX会社「すみません、『FXトレード』ですが、ご主人のことで、実はご主人が１５００万円の損失を出していらっしゃいまして」

奥さん　「１５００万？！どういうことですか？」

夫の死後、相場が大きく動き、為替レートが大暴落、１５００万円の損失となってしまった。

奥さん　「だから、夫は、半年前に亡くなってるんですって・・・」

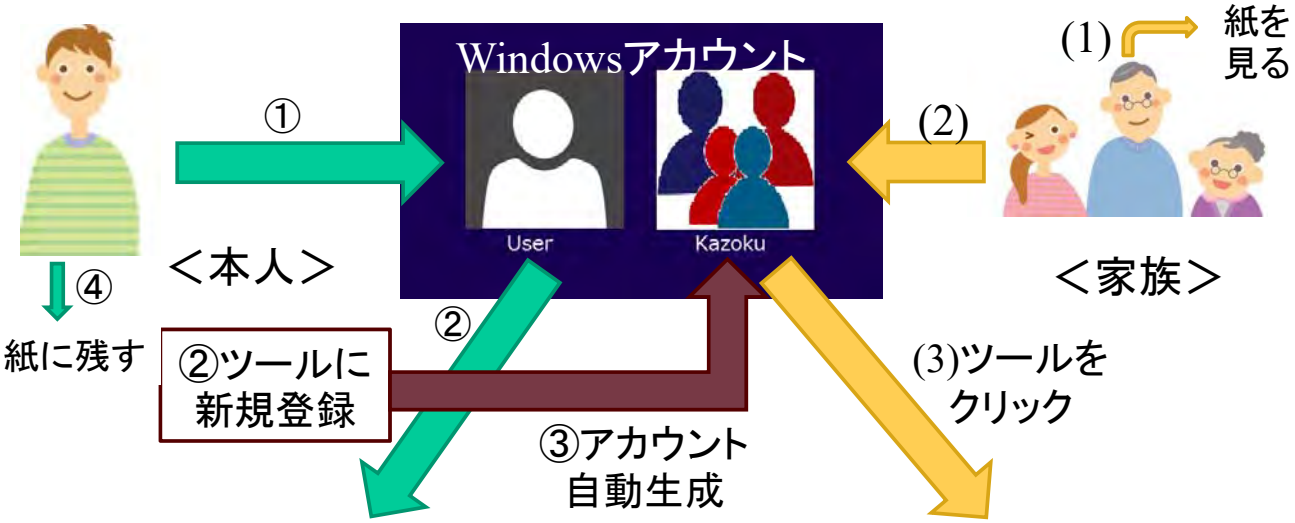
FX会社「そう言われましても、こちらには取引キャンセルの通知がきていないので、取引は続いているんです」

※夫のPCから浮気写真がでてきた..

※（出典）荻原栄幸 “「デジタル遺品」

残すべきなものが残されず、知られなくてよいことが知られてしまうという問題が発生。

支援ツールの開発



主要な研究の位置づけ

応用

理論

②DFガイドシステム

⑤ NWフォレンジック

④ 証拠保全方式

③ LIFT システム

⑥DFとプライバシー

① ログの署名方式

（⑦その他）

要素的 ⟷ システム的

LIFT: Live and Intelligent Network Forensic Technologies

主要な論文（1）

1] 上田、佐々木他「データ喪失を想定したヒストリシス署名方式評価手法の提案」情報処理学会論文誌第45第8号pp1966-1976,2004 ①

2] 佐々木他「デジタル･フォレンジックの体系化の試みと必要技術の提案」日本セキュリティ･マネジメント学会20巻第2号、pp49-61、2006 ⑦

3] 芦野、佐々木「セキュリティデバイスとヒステリシス署名を用いたデジタルフォレンジックシステムの提案と評価」情報処理学会論文誌、49巻2号, pp. 999-1009、2008 ④

4] 高塚、佐々木他「開示情報の墨塗りと証拠性確保を両立させるe-Discoveryシステムの提案」情報処理学会論文誌第49号第９号pp3191-3198、2008 ⑥

5] Jigang Liu,Uehara,Sasaki「Development of digital forensics practice and research in Japan」Wireless Communications And Mobile Computing(Wiley InterScience)www.interscience.wiley.com、2010 ⑦

主要な論文（2）

6] 藤田、芦野、上原、佐々木「不正プログラムの起動制御機能を持つDFシステムの提案と評価」情報処理学会論文誌VOL.51,No.9、pp1507-1519、2010 ④

7] 長谷部、上原、佐々木「複数組織にまたがる疫学調査におけるプライバシー確保のための大容量タンパー装置HiGATEの適用方式の開発」日本セキュリティマネジメント学会誌VOL.25,No.3、pp24-34,2012 ⑥

8] 土方、佐々木他「デジタル・フォレンジクスを考慮した個人情報漏洩対策に関する合意形成のための多重リスクコミュニケータの適用」日本セキュリティマネジメント学会誌26巻第1号2012年5月pp3-14,2012 ⑦

9] Shuhui Hou, Siuming Yiu, Uehara, Sasaki et al,「A Privacy-Preserving Approach for Collecting Evidence in Forensic Investigation」InternationalJournal of Cyber-Security and Digital Forensics (IJCSDF) (Vol.2,No.1pp70-78）2013 ⑥

主要な論文（3）

10] Shuhui Hou,Sasaki, Uehara, Siuming Yiu「Double Encryption for Data Authenticity and Integrity in Privacy-preserving Cofidential Forensic Investigation」Journal of Wireless Mobile Networks, Ubiquitous Computing and Dependable Application Vol.4 NO. pp104-113,2013 ⑥

11] Takashi Shitamichi, Sasaki,「Technology of Federated Identity and Secure Loggings in Cloud Computing Environment」International Journal of Electronic Commerce Studies Vol.5, No.1, pp. 39-62, 2014 doi: 10.7903/ijecs.1157,2014 ④

12] 小林、佐々木「証拠性保全のための安全で効率的なログ署名方式の提案と評価」日本セキュリティマネジメント学会誌28巻第2号2014年9月 pp11-21 ①

13] Naoki Kobayashi, Ryoichi Sasaki,「Proposal and evaluation of an evidence preservation method for use in a common number system」nternational Journal of Electronic Commerce Studies vol.6,no.1,pp51-68, 2015 ①

主要な論文（4）

14] Takashi Shitamichi, Ryoichi Sasaki「A Proposal and Evaluation of User Centric Trusted Log Archival Architecture」International Journal of Cyber-Security and Digital Forensics (IJCSDF) 4(3): 442-452(ISSN: 2305-0012),2015 ④

15] 天野貴通、上原、佐々木「デジタル・フォレンジックのためのガイドライン総合支援システムの提案と開発」情報処理学会論文誌, Vol.56,No.9,pp1889-1899,2015 ②

16] 三村聡志, 佐々木「プロセス情報と関連づけた通信情報保全手法の提案」情報処理学会論文誌, Vol.57,No.9,pp1944-1953,2016 ⑤

17] 佐藤、佐々木他「マルウエアによるネットワーク内の挙動を利用した標的型攻撃における感染経路検知ツールの開発と評価」情報処理学会論文誌, Vol.58,No.2,pp1-9,2017 ⑤