SCIS 2002 The 2002 Symposium on Cryptography and Information Security
Shirahama, Japan, Jan. 29 - Feb.1, 2002
The Institute of Electronics, Information and Communication Engineers

侵入検知及び内部攻撃者検知とヒューマンクリプト
Intrusion Detection and Extrusion Detection on HUMANCRYPT

山中 晋爾* 松浦 幹太* 今井 秀樹*
Shinji YAMANAKA Kanta MATSUURA Hideki IMAI

あらまし 現在、正当な接続権利を持たないユーザが、インターネットに接続されたネットワークや計算機などに対して、不正にアクセスする、という問題が増加している。不正アクセスは、機密情報の漏洩や、他の不正アクセスの踏み台にされる恐れがあり、被害を拡大する。これを防ぐためのひとつの手段として侵入検知(Intrusion Detection)技術があり、現在盛んに研究が行われている。 また、サービス拒否 (DoS)や分散サービス拒否(DDoS)を利用した攻撃は、あるネットワーク(もしくは、組織)内部にある計算機から、外部の計算機等への不正アクセスと見ることができる。これを検出することを内部攻撃者検知（Extrusion Detection）と呼ぶことにするが、このような検知技術に関する研究は十分に行われているとはいえない。組織に対する外部からの攻撃、及び組織の内部から外部に対する攻撃を検出することは、不正アクセスに対抗する手段として有効である。しかし同時に、ユーザのプライバシ情報を適切に保護することも重要である。侵入/内部攻撃者検知技術においては、通信路上や計算機上の様々な情報を利用するが、この情報にはユーザのプライバシ情報も含まれることになる。本論文では、ユーザが安心してネットワークシステムを利用できるように、ユーザのプライバシ情報の保護も含めて、ヒューマンクリプトを念頭においた議論を行う。

キーワード 侵入検知、内部攻撃者検知、ヒューマンクリプト、プライバシ保護

1 はじめに

インターネットに対して高速な接続が可能となり、ネットワークの利用が容易に行えるようになった今日、その利便性の向上に伴いネットワークや計算機の不正利用行為が年々増加している。表 1に警察庁による不正アクセス事犯の統計（平成 12 年および平成 13 年上半期）[1]を示す。

表 1 警察庁に報告のあった不正アクセス件数

	平成 13 年上半期	平成 12 年
認知件数	959	106
海外からのアクセス	418	25
国内からのアクセス	165	73
不明	376	8

これによると、平成 13 年上半期において不正アクセス禁止法に違反する行為として「警察が認知した件数」は 959 件である。もちろん、全ての不正アクセスが警察によって認知されているわけではないので、実際の不正アクセス数はこの限りではない。また、仮に Code Red のようなバックドアを作るタイプのコンピュータ・ウィルスやワームによる攻撃も不正アクセス行為に該当するとみなすと、現実に発生している日本国内における不正アクセス犯罪は 10 万件以上になる。

このような不正アクセスを防ぐためのひとつの手段として侵入検知技術がある。侵入検知技術では、ネットワークを流れるトラフィックや、守るべき計算機におけるアクティビティの変化といったものを元に、ネットワーク外部からの不正侵入や正当な権利を持たないものによる不正利用を検出する。侵入検知技術の研究は数多く行われており[2,3,4,5,6,7,8,9,10]、現在でも活発な議論が行われている。

これとは逆に、ネットワーク内部から外部に向かう攻撃も存在する。例えば、サービス拒否（DoS : Dinaial of Services）攻撃や分散サービス拒否（DDoS : Distributed DoS）攻撃は、あるネットワーク内部の計算機から外部の計算機等への不正アクセスと見ることができる。DoS は、攻撃を行っている計算機（それが真の攻撃者の計算機であるとは限らない）を特定し、攻撃を阻止することは比較的容易であるかもしれない。しかし DDoS は多数の計算機が攻撃に参加して、攻撃を受けている側においてその攻撃を完全に防ぐことは難しい。そこで、ネット

* 東京大学生産技術研究所 〒153-8505 東京都目黒区駒場 4-6-1.
University of Tokyo, Institute of Industrial Science, 4-6-1 Komaba Meguro-ku Tokyo 153-8505, Japan.
yamanaka@imailab.iis.u-tokyo.ac.jp, kanta@iis.u-tokyo.ac.jp, imai@iis.u-tokyo.ac.jp

ワークから外部に向かうパケットを監査することで、DDoS に参加している（とみられる）計算機を特定し、何らかの対策をすることにより解決する方法が考えられる。このような検知技術に関する研究も大切であるが、残念ながらその研究が十分されているとはいえない。

このように、組織に対する外部からの攻撃と、組織内部から外部に向かう攻撃を検出することは、ネットワーク社会において不正アクセスに対抗する手段として有効である。しかし、これと同時にネットワーク利用者（ユーザ）のプライバシ情報を適切に保護することも重要である。侵入検知や内部攻撃者検知においては、ネットワーク上や計算機上における様々な情報を利用するが、この情報の中には、例えば送信元・送信先の IP アドレスや、計算機ログイン時のユーザ名のようなプライバシに関わる情報も少なくない。

そこで、本論文では侵入検知技術に関する調査を行い、その手法を内部攻撃者検知に利用した際に生じる問題点を示し、ヒューマンクリプトに則した考察を行う。

以下、第２章では侵入検知技術について、既存の技術や関連研究などを紹介し、第３章では内部攻撃者検知について述べる。また、第４章では、ユーザが安心してネットワークを利用しつつ、ユーザのプライバシ保護をどのように維持するかをヒューマンクリプトに基づいて考察し、第５章でまとめる。

2 侵入検知

ネットワーク外部からの不正アクセスは、機密情報の漏洩や破壊、Web ページの改ざん、他の不正アクセスの踏み台にされる、といった様々な問題をさらに引き起こす可能性があり、これをいかに防ぐかは、大変重要な課題である。

侵入検知技術とは、現実社会における監視カメラのようなものである。監視カメラは、リアルタイムでカメラの前を通過する人間を確認し、また後で必要となったときに記録を取り出してチェックすることができる。侵入検知技術は、ネットワークを流れるパケットや特定の計算機（ホスト）のアクティビティを監視して、ネットワークに対する不正アクセスや計算機資源の不正使用を検知するための技術である。

また本論文では、あるネットワーク内の計算機から同一ネットワーク内部の計算機資源に対して何らかの不正行為がなされたときに、これを検知することも侵入検知とよぶことにする。

2.1 侵入検知技術に関する関連研究

侵入検知技術に関する研究で最も古いもののひとつは、Denning によって行われた[2]。Denning は、侵入検知を行うシステムのモデルとして intrusion-detection expert system(IDES)を提案した。

最近では、pseudonymous を利用した研究がいくつか行われている。Sobirey らは、pseudonymous audit を用いて、プライバシ保護を目的とした侵入検知システムのプロトタイプを示している[11]。また、Lundin らは、pseudonymizer を利用した侵入検知システムを提案し、ユーザのプライバシと侵入検知分析の効率がトレードオフとなり、この問題を完全に解決する手法は無いと結論付けている[12]。

2.2 検査対象による分類

侵入検知技術は、侵入検知を行う対象によって分類するときは、ふつう下記の２つに分類される。

- ネットワーク型侵入検知システム
- ホスト型侵入検知システム

また、侵入検知システムの設置に関して図 1に示す。通常、ネットワーク型侵入検知システムは、（1）ファイアーウォールの外、（2）DMZ、（3）イントラネットのいずれか（もしくはその全てに）設置される。そして、ホスト型侵入検知システムは、DMZ にある Web サーバや、イントラネットにある重要なサーバに対して導入される。

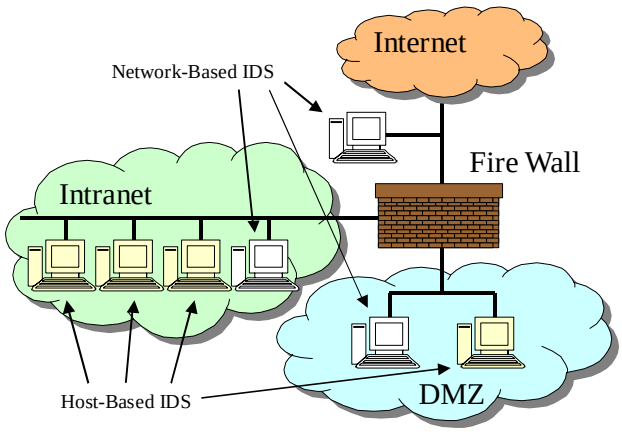

図 1　侵入検知システムの設置

以下では、ネットワーク型・ホスト型それぞれの侵入検知システムの特徴を説明する。

2.2.1 ネットワーク型侵入検知システム（N-IDS : Network-Based- Intrusion Detection System）

ネットワーク型侵入検知システムとは、侵入検知システムが接続するネットワークセグメントのトラフィックを監視するタイプの検知システムである。

このシステムが利用する情報は、監視を行うネットワ

ークを流れるパケット情報である。これは IP ヘッダに含まれるパケットの送信元や送信先の IP アドレスやポート番号といった情報で、時にはデータそのものを取得する。

ネットワーク型侵入検知システムの脆弱性としては、以下のようなものが挙げられる。

- 暗号化されたパケットの分析

  ネットワーク型侵入検知システムでは、パケット内のデータに基づいて分析を行うために、例えば端末間で暗号化されているような場合にはパケットを処理することができない。

- 高速なネットワーク/高負荷

  ネットワークを流れるパケットとシグネチャの比較や統計情報との比較をするときに、対象となるネットワークが高速であったり高負荷がかかったりしたときに、照合・分析処理が追いつかなくなることがありうる。

- 検知システムに対する(DoS 等による)攻撃

  検知システム自体に対して攻撃が行われることが考えられる。これは、検知システムがステルスモード（検知システムに IP アドレスを割り当てず、外部から見つからない状態で動作させること）で動作していても、わざと多量のパケットをセグメントに送り込まれた結果、検知システムがダウンしてしまうことがある。

- 挿入/回避攻撃

  侵入検知システムが、パケット分析の際にその整合性チェックや再構築処理を行わないこと利用した攻撃である。挿入攻撃では、検知システムがシグネチャとのマッチングに失敗するようなパケット(ターゲットのノードでは整合性チェックによって破棄されるような)を攻撃パケットに混在させる。そのようなケースでは、IDS はパケットがシグネチャパターンに合致しないため攻撃として判断しないが、エンドポイントでは、パケットの整合性チェックにより混在させられたゴミパケットが破棄され、最終的に攻撃用のデータが構築されてしまうといった仕組みである。回避攻撃はフラグメント化したパケットを利用し、検査システムでの検査をバイパスする手法である。

- 誤報

  リアルタイムで分析が行われるため、誤報をする可能性がある。

2.2.2 ホスト型侵入検知システム(H-IDS : Host-Based Intrusion Detection System)

ホスト型侵入検知システムは、ある単一の計算機（ホスト）上で動作して、同ホスト上における監査情報をチェックすることでホストの不正利用を発見する。例えば、インストールされた検知システムは、はじめに重要なシステムファイルの特徴（ファイルのハッシュ値等）を記録し、その後ファイルの状態を定期的に初期状態と比較し、問題を発見した場合には管理者に報告をする。

ほかに、ログイン・ログアウト情報やアプリケーションの稼動状況、コマンド履歴、レジストリ情報などを使用する場合もある。

また、当該ホストに到達するパケットの監視を行うものもある。これは、そのホスト専用のファイアーウォールのようなもので、何らかの疑わしいパケットを受信したときに管理者に報告する。ネットワーク型侵入検知システムでは対応が困難であった暗号化されたパケットに対しても、ホストにおいて再構築された後に検査を行うために攻撃の検出が可能となる。

2.3 検知方法による分類

一方、侵入を検知する方法により分類するときは、「既知攻撃検知モデル」と「異常使用検知モデル」の２つに分類するのが一般的である。

2.3.1 既知攻撃検知モデル

Signature-Based モデルとも呼ばれ、すでに知られている攻撃の手法（例えば、ポートスキャンやプログラムのセキュリティ上の弱点に対する攻撃）を知識（シグネチャ）として保持し、このシグネチャと照合することで不正アクセスを検知するモデルである（図 2)。ネットワーク型侵入検知システムでは広く用いられており、シグネチャを更新することにより様々な既知の攻撃からシステムを守ることができる。

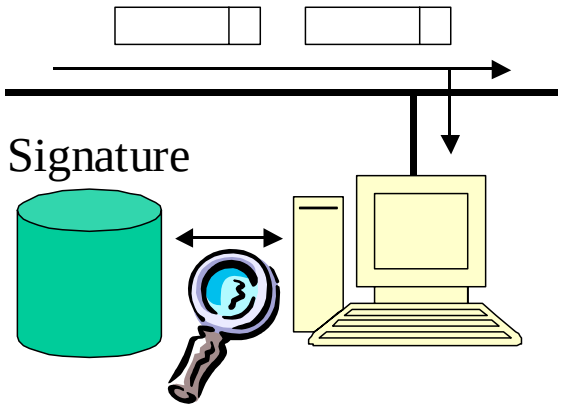

図 2　ネットワーク型-シグネチャ利用検知モデル

ただし、シグネチャの更新を必要とするために、未知の攻撃に即座に対応することは難しい。

2.3.2 異常使用検知モデル

不正アクセス・ユーザの行動に注目してその監視を行う手法である。まず、検査対象とするシステムやユーザの通常使用状態を一定期間採取し、これをプロファイルとして保存する。プロファイルにはユーザのログインした時間帯や利用するアプリケーションタイプ、またトラフィック量などが含まれる。そしてこのプロファイルをもとに、統計学的な処理を行い不審な活動に対して警告を出すモデルである。

システム環境の変更や、ネットワークやアプリケーションの利用形態が変化すると以前のプロファイル情報が無意味になるという問題や、システムに個別に導入する場合の導入コストや運用コストの問題がある。また、悪意の無いユーザが普段と異なる行動をしたときに起こる誤報の問題もある。しかし、既知攻撃検知モデルで検出できないような未知の、あるいは新種の攻撃を検出できる可能性もある。

3 内部攻撃者検知

本稿において内部攻撃者とは、ある組織に所属する計算機が組織外のネットワークや計算機に対して何らかの不正行為を行っている場合における、その計算機（及びその利用者）をさす。このときに、利用者が悪意を持って不正行為を行っているか、無意識のうちに（トロイの木馬プログラム等により）不正行為が行われているかは区別しない。そして内部攻撃者検知とは、このような不正行為を検知する技術をさす。

内部攻撃者検知のひとつの手段として、侵入検知の技術を利用することが考えられる。そこで、２章で述べた分類に従い内部攻撃者検知システム（EDS：Extrusion Detection System）を構成することを考える。

EDS の構成方法は以下の４通りである。

- ネットワーク型-既知攻撃検知モデル
- ネットワーク型-異常使用検知モデル
- ホスト型-既知攻撃検知モデル
- ホスト型-異常使用検知モデル

3.1 ネットワーク型内部攻撃者検知

はじめに、EDS をネットワーク型侵入検知システムベースで構成する（N-EDS）場合を考える。この場合に問題となるのは、検知システムの設置場所と収集するデータの種類である。N-EDS をイントラネットに設置する場合、検知システムはゲートウェイに向かうパケットを監視することになる。そして、既知攻撃検知モデルで用いられたようなシグネチャにマッチするような攻撃が外部に向けて行われていないか、また通常使用時のトラフィックと比較して、異常が無いかをチェックする。

N-EDS を DMZ に設置する場合は、DMZ 内にある Web サーバ等の挙動を監視することになる。この場合も、検知システムはゲートウェイに向かうパケットを検査する。

3.2 ホスト型内部攻撃者検知

つぎに、EDS をホスト型侵入検知システムベースで構成（H-EDS）する場合について考える。H-EDS の導入箇所としては DMZ に設置された Web サーバ等、イントラネット内の重要なサーバ、などが考えられる。

どちらの場合も、基本的にはホスト型侵入検知システムと連携を取ることが考えられる。すなわち、H-IADS が導入された計算機において何らかの外部への攻撃が検知された場合に、ホスト型侵入検知システムに対して当該計算機が侵入を受けたり、何らかのプログラムが仕掛けられていたりしていないかをチェックするよう依頼する、といった対応が考えられる。

3.3 既存の侵入検知手法の利用

既存の侵入検知の手法、例えば Lundin の用いた方法を、内部攻撃者検知システムに適用することが可能である。しかし、これにはユーザのプライバシを適切に守ることができない、という問題点がある。

つまり、外部から内部への侵入を検知した場合には、それは悪意を持った侵入者であるとかなり高い確率で判断できる。しかし、内部から外部への攻撃を検知しようとするときには、ネットワーク管理者は比較的簡単に不正行為をした（と判断された）ユーザを特定することが可能である。この２つの条件の間には、プライバシ保護の観点から大きなギャップがあると考えられる。

すなわち、内部攻撃者検知においては侵入者検知と比べて、プライバシ保護に関してより多くの労力が必要となるし、より多くの労力を投入すべきである。

4 ヒューマンクリプトと検知技術

本章では、前述した侵入検知技術、および内部攻撃者検知技術と、ヒューマンクリプトとの関わりについて述べる。

ここでは、侵入検知技術や内部攻撃者検知技術により、ユーザが安心感を持ってネットワークシステムを利用できるようにすることを考える。

4.1 ヒューマンクリプトとは

ヒューマンクリプトとは、狭義には、人とコンピュータやネットワークとのかかわりの部分における暗号技術、広義には、このような部分における情報セキュリティ技術全般を言い、人とコンピュータネットワークを情報セキュリティの面から総合的に最適化するための技術である[13,14]。

そして、ヒューマンクリプトの要件として、

- 事前・事後を含みユーザに過重な負担をかけない
- 合理的なセキュリティレベルを達成している
- 人に安心感を与える

の３つがあるが、侵入検知技術や内部攻撃者検知技術がこのような要件を満たしていることが必要とされる。

4.2 侵入検知とヒューマンクリプトについて

まず、侵入検知技術が、前述のヒューマンクリプトの要件を満たしているかどうかを考察する。はじめに、ユーザに対する負担についてだが、基本的に侵入検知はユーザの目にふれない部分で行われる。このため、侵入検知システムの動作がネットワークやユーザの使用する計算機に対する負荷を増大させる事が無い限り、ユーザに過重な負担をかけることは考えにくい。

次に、侵入検知技術が合理的なセキュリティレベルを達成しているかどうかを考える。これは、守るべきネットワークや計算機への侵入が的確に検知されることが判断基準となる。当然のことながら、ネットワークの脆弱性は総合的に判断することが必要であり、システムでもっとも脆弱な部分のセキュリティレベルが、そのシステム全体の脆弱性を示すことは言うまでも無い。

最後に、人に安心感を与えているかどうかについて考える。ユーザは、侵入検知システムがきちんと動作していていることにより安心感を得る。もしくは、侵入検知システムがきちんと動作した結果、なにも問題が起きていないことに対して安心感を得る。そして、侵入検知システム等が動作していない自分が利用しているネットワークや計算機が、不正行為を簡単に行える状況であると知ったならば、ユーザは不安になる。その一方で、侵入検知システムに自分のプライベートな情報を採取・蓄積されていないことにより別の安心感を得る。つまり、自分のプライバシ情報が必要以上に採取・蓄積されることにより、やはりユーザは不安になる。

4.3 内部攻撃者検知とヒューマンクリプトについて

次に、内部攻撃者検知技術が、ヒューマンクリプトの要件を満たしているかどうかを考察する。ユーザに対する負担に関しては、侵入検知の場合と同様にシステムの動作がネットワークやユーザの使用する計算機に対する負荷を増大させる事が無い限り、ユーザに過重な負担をかけることは考えにくい。

合理的なセキュリティレベルに達しているかどうかについては、ネットワーク外部に対する攻撃を的確に検知できるかどうかによる。そのためには、セキュリティポリシーを適切に定め、必要な情報のみを採取・収集することが必要となる。

人に安心感を与えるかどうかについては、本人が意図しない状態でユーザの使用する計算機が外部への攻撃に参加していないことが確認できること。そして、内部攻撃者検知システムによって採取された情報が、プライバシを守る形で扱われていることを確認できることが重要となる。

4.4 考察

いずれにしても、システム管理者に悪意があれば、ユーザのプライバシを守ることは困難である。Lundin は仮名（pseudonym）を用いたログを利用した手法を提案している。この場合、たとえ管理者に悪意がなくても、一度警告へ対応する際に目にした 実名⇔仮名の関係が管理者の記憶に残っていて、以後ログファイルを見ただけでその特定ユーザの行動がわかってしまうことは防ぎたい。例えば、その都度 実名⇔仮名 を割り当てしなおすことも考えられるが、あきらかに非効率的である。また、同報告書では user1、user2、･･･という仮名のつけ方を採用しているが、これは明らかに記憶に残りやすいので問題である。これを、一見乱数（ランダムな文字列）にみえるものにするだけでも、ヒューマンクリプトとしては好ましい。

仮名を用いるという事は、ある種の暗号化を意味する。このときパケットの一部のみを暗号化することになるので、暗号化されていないデータから暗号化された部分を推測される可能性も残されている。

また、管理者の管理行動を（改ざんされないような方法で）確実に記録することができれば、管理者がユーザの行動を追跡することを抑止することができると考えられ、さらにユーザに安心感を与えることができる。

5 まとめ

本論文では、侵入検知に関する最近の研究状況および問題点を報告し、内部攻撃者検知について述べた。また、これらの検知技術がヒューマンクリプトの要件を満たすかどうかを考察した。今後は pseudonym や改ざん不可

能な記録手法を利用して、ユーザのプライバシ保護を考慮した、侵入検知・内部攻撃者検知システムを提案し、またその実装を行いたい。

参考文献

[1] http://www.npa.go.jp/hightech/fusei_ac6/hassei1308.htm

[2] Dorothy E. Denning, “An Intrusion-Detection Model”, IEEE Transactions on Software Engineering, vol. SE-13, no. 2, February 1987, pp.222-232

[3] Liepins G. E. and Vaccaro H. S. “Anomaly detection purpose and framework”. In Proceedings of the 12th National Computer Security Conference, pp.495-504, Oct. 1989.

[4] Carettoni F., Castano S., Martella G. and Samaratti P. RETISS: “A Real Time Security System for Threat Detection using Fuzzy Logic”, In Proceedings of the 25th Annual IEEE International Carnahan Conference on Security Technology, pp.161-167, Oct. 1991.

[5] Hochberg J., Jackson K., Stallings C., McClary J., DuBois D. and Ford, J. NADIR: “An automated system for detecting network intrusions and misuse”. Computers and Security 12(1993)3, May, pp. 253-248.

[6] Winkler J. R. and Landry L. C. “Intrusion and anomaly detection”, ISOA update. In Proceedings of the 15th National Computer Security Conference, pages 272-281, Oct. 1992.

[7] Sandeep Kumar and Eugene H. Spafford. “A pattern matching model for misuse intrusion detection”. In Proceedings of the 17th National Computer Security Conference, pages 11-21, October 1994.

[8] Staniford-Chen S., Cheung S., Crawford R., Dilger M., Frank J., Hoagland J., Levitt K., Wee C., Yip R., Zerkle D. “GrIDS - A Graph Based Intrusion Detection System for Large Networks” In Proceedings of the 19th National Information Systems Security Conference, pages 361-370, Oct. 1996.

[9] U. Lindqvist and P. Porras. eXpert-BSM: “A host-based intrusion detection solution for Sun Solaris”, In Proc. of the 17 th Annual Computer Security Applications Conference, Dec. 2001.

[10] D. Curry and H. Debar, “Intrusion detection message exchange format data model and extensible markup language (xml) document type definition”, Internet Draft, draft-ietf-idwg-idmef-xml-03.txt, February 2001.

[11] Michael Sobirey, Simone Fischer-Hübner, and Kai Rannenberg, “Pseudonymous Audit for Privacy Enhanced Intrusion Detection”, IFIP/SEC '97, pp.151-163, Copenhagen, Denmark, May 1997.

[12] Emile Lundin and Erland Jonsson, “Privacy vs Intrusion Detection Analysis”, In Proceedings of the Second International Workshop on the Recent Advances in Intrusion Detection - RAID'99, West Lafayette, Indiana, USA, September 7-9 1999.

[13] 今井秀樹, “暗号のおはなし”, 日本規格協会（1993-03）

[14] 今井秀樹, 古原和邦, 渡邊曜大, “ヒューマンクリプトとは”, 電子情報通信学会技術研究報告 ISEC2000-17, pp.57-64 （2000-05）