# イントラネット内のネットワークアクセス視覚化による集団監視システム

溜田英二

シーア・インサイト・セキュリティ株式会社

**概 要**

企業の情報資産の漏洩は、内部の不正行為に拠るところが大きく、それに対する防御としてのセキュリティ対策は数多く講じられてきた。しかしながら、その不正行為事体を抑制する対策といったものにはあまり目が向けられてきていない。そこで本論文では、不正を抑制する手法として、イントラネット内のネットワークアクセスを視覚化する手法を提案し、それに基づく集団監視システムを構築した。本システムを用いることにより、不正行為の抑制ばかりでなく、セキュリティに対する啓蒙効果といったものも享受できる。

# Group Monitoring System based on Visualization of Network Access over Intranet

Eiji Tameda

Seer Insight Security Inc.

**概 要**

This paper describes about a Visualization of Network Access over Intranet and Group Monitoring System based on it. Lost of information assets leakages on business were causede by inside dishonest. Therefor lots of defence systems have been working for security, but control systems of dishonest have not worked much. This Group Monitoring System controls it and brings a effect of enlightenment for security to us.

## 1 イントラネットにおける集団監視

IT 革命による高速な情報の流通及びボーダレス化が進展するなかで、ネットワークを経由して、外部の者が情報システムへ不正に侵入し、データを改ざん・窃取、あるいはシステムの破壊又は利用妨害を行うといったことが新しい脅威として社会的注目を浴びている。ただ、企業の情報資産の漏洩という観点から見ると、組織内部もしくは取引関係等、任意の第三者以外の者による情報の意図的な漏洩及び外部への不正なアクセス等が多数を占めているのが現状である。(図 1) このため、イントラネットにおいても一層のセキュリティ強化が求められるようになり、個人認証を例に挙げるなら、ユーザー ID およびパスワードの管理という基本的なものからから、ワンタイムパスワードの利用、指紋や声門、網膜等の識別といったよ

り手の込んだセキュリティ対策を施す方向に進んでいる。しかしながら、これも、正しく教育および運用されなければ意味がないし、まして、許可を受けた利用者/従業員による不正が第一位を占めるにいたっては、単一の方向性による対策だけでは不十分であり、さまざまなアプローチによるセキュリティ対策が必要となる。そこで出てくるのが、セキュリティポリシーの策定および教育そして運用管理という手法である。しかしながら、これを有効な手段とするためには、利用者や従業員がセキュリティポリシーを十分に理解することと、的確に運用するための労力の確保が条件となる。また、もう一つ考えなければいけないこともある。それは、コンピュータ＆ネットワークが浸透する以前の就業形態であれば、席を見渡すなりして人の行動を見れば、どのような資産に接触し、誰と連絡を取っているかは、大体把握できたのに対し、現在は各自がPC(ネットワークに接続されたパソコン)を使用して何にアクセスし、誰とコンタクトを取っているのかを把握することは非常に困難になっているということである。つまり、環境が不正をより行い易い状態へと遷移してきたにもかかわらず、これが放置されたままになっているということである。これでは、いくらセキュリティ対策を講じても不正の芽を摘むことはできない。そこで不正行為に対する抑止力という観点から見ると、「個々のPCのネットワークへのアクセス状況を見えるようにすればいいのでは」という発想が生まれてくる。方法としては、既存のコンピュータ＆ネットワークの監視ツールを導入し、システム管理者が監視するということが考えられるが、これは、少数の役員だけで全社員の行動を把握するようなもので、現実的ではない。また、監視する側といえども、不正を働く可能性はゼロではないことを考えると、従業員全員が監視できる仕組み、集団監視システムの構築が必要である。この、集団管理システムは「不正行為の抑止力」以外にも以下のような効果をもたらすと考えられるため、この点からも非常に有効な手段といえる。・セキュリティに対する認識を高めセキュリティポリシーを浸透させる啓蒙効果・ユーザー自身による監視や調査が可能となり、システム管理者の作業負担が軽減もちろんこれは、集団監視が的確に効率良く行われた場合であり、そのためには、ネットワークへのアクセス状況の的確な視覚化が重要となる。

## 2　ネットワークアクセスの視覚化

ネットワークへのアクセス状況を表示するアプリケーションは現時点でも数多く存在する。しかしながら、殆どが、限られた人数のシステム管理者用であって、集団監視という観点から見た場合、以下の部分が欠けている。1) 表示される内容が、学習なしでほぼ理解可能である (監視する側が一般ユーザーであるため) 2) 監視のためのシステム負荷が低い、もしくは分散可能である (監視者の数が多い) そこで以下の3つのフェーズでのシステムを考察する。

なお、これらの具体的なシステムについては、まだ未発表であるため、大まか

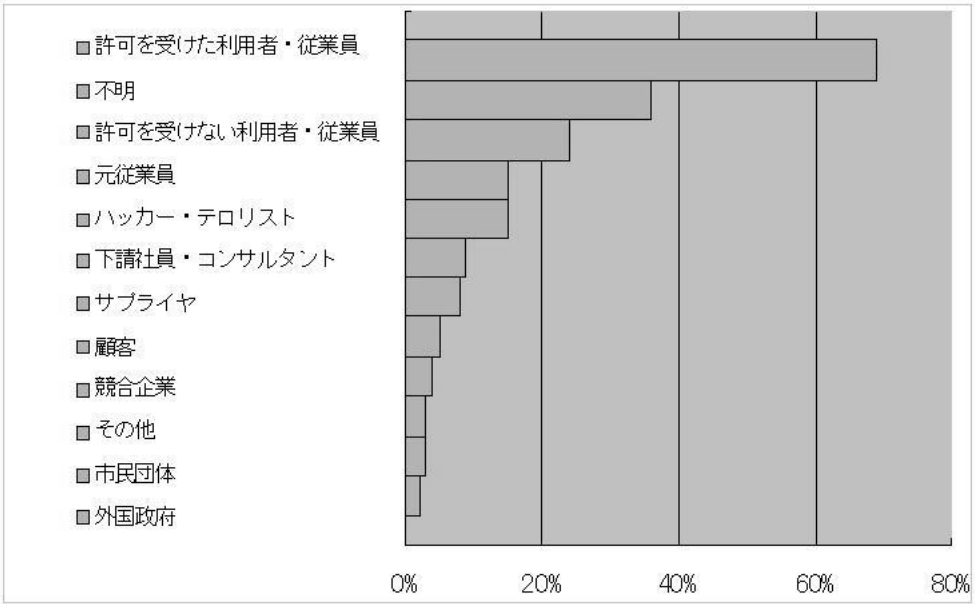


図 1: 米国におけるコンピュータ不正アクセスの実態 (最近 1 年間に発生した不正行為の犯人)[1]

な流れの考察になること、また、これらのフェーズを経て表示される内容の詳細に関しては、発表時のみの提示になることをお赦し頂きたい。

## 2.1 情報収集

まず、ネットワークへのアクセス状況を何らかの方法で収集する必要があるが、情報量の多さおよび稼動中のシステムへの影響度を最小限に抑えることから考えると、分析の難易度は高いが、LAN 上を流れるイーサネット・パケットを直接収集する方法を取る。なお、このイーサネット・パケットであるが、現在のイントラネットの環境を考えると、パケットを送出した側と受信した側を確実に捉えるためには、各ネットワークセグメント毎にパッケとを収集する仕組みを設ける必要がある (PC を特定するため MAC アドレスが必要)。また、収集したパケットは、パフォーマンスを考慮し、不要なパケットを除いた状態で次の解析フェーズに回す。

## 2.2 情報解析

イーサネット・パケットは大きく分けてヘッダー部分とデータに分けられるが、ヘッダーの中の、TCP ヘッダー部分にはポート番号が含まれ、これで何のアプリケーションのパケットかを大まかに判別することが可能である (例えば25 ならメール送信)。また、データ部分にはアプリケーションの固有情報 (例えばメールの宛先) が含まれており、これを抽出することでアプリケーションの利用状況が判明す

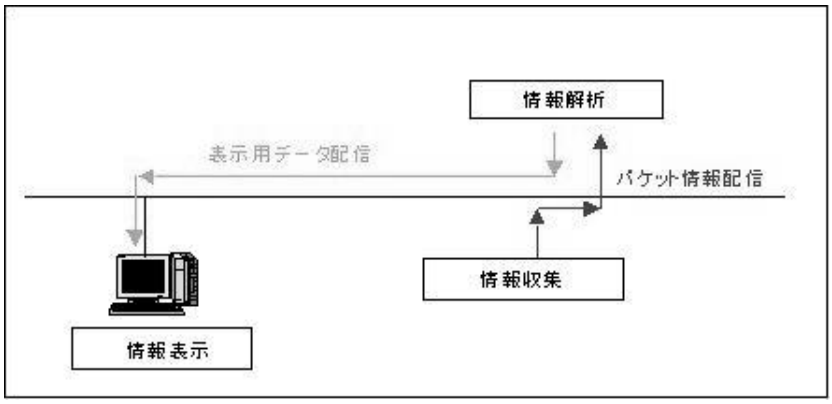


図 2: 視覚化フェーズの流れ

るので、それを各 PC 毎に分類し蓄積する。蓄積した情報は、一定時間毎に纏めて次の表示フェーズに回す。

### 2.3 情報表示

最も簡単な情報表示としては、収集/解析した情報を表やグラフを並べて表示することも考えられるが、「表示される内容が、学習なしでほぼ理解可能である」ということを考えると、監視する人間が周囲を見渡した時と同じような状況が画面上にも展開されるのが望ましいと考えられる。また、描画については、負荷分散を考えると PC 側で行うようにし、また、更新頻度についても監視側で調整できることが望ましい。

## 3 今後の課題

前述までの方法では取得、解析および判別できないが、セキュリティポリシーを補うという観点から見ると、以下の 3 点は、このシステムの監視対象として付加することが必要であると考えられる。1)PC 側で完結する作業 2) 暗号化された情報 3) ウィルスまず、1) であるが、これは PC 側に情報収集プログラムを入れる必要がある。ただ、PC 側に入れた場合、それを停止もしくは削除される可能性があるため、パケットの収集と組み合わせて監視する必要がある。2) に関しては、暗号の復号というのは、殆ど不可能 (可能な仕組みにすることは、セキュリティ的に問題がある) なので、ログ等を収集し解析する必要があるが、完全にアプリケーション毎の個別対応となりどれだけ共通化を図れるかが鍵となる。最後の 3) は、その殆どが単独では存在せず、他のアプリケーションのデータ等に寄生して存在することや種類の膨大さから、解析/判別方法もさることながら、いかに短時間に処理

するかが課題である。ここまで、イントラネット内のネットワークアクセス視覚化による集団監視システムの有効性および仕組みについて述べてきたが、もちろん、これさえあれば他のセキュリティ対策が不要になるというものではなく、あくまでそれらを補完するものであることを最後に付け加えておく。

## 参考文献

[1] **Information Week Price Waterhouse Coopers Global Information Security Survey** , *August 31,1998*