情報資産のセキュリティレベルを多角的に分析するためのレイヤを選択的に複合できる統合可視化手法

斎藤　雄一† 毛利　公美† 白石　善明‡ 福田　洋治†† 野口　亮司†††
岐阜大学† 名古屋工業大学‡ 愛知教育大学†† 株式会社豊通シスコム†††

1. はじめに

近年，クラウドコンピューティングが注目され，利用が進んでいる．組織内にあるIT資産情報や通信ログなど多くの情報は組織外にあるデータセンタにて一括して保存，管理されるようになった．これらの情報を利用してネットワーク管理業務やセキュリティ監査等を行う場合，セキュリティレベルを把握することが重要になる．しかし，膨大な情報の中から必要な情報を取捨選択し，それらを関連付けてセキュリティレベルの把握に繋がる情報として捉えなおすことは，経験豊富な技術者でさえ難しい作業である．

本研究では，このような現状を踏まえ，ネットワークに関する情報を概念ごとにレイヤ分けし，それを統合的に提示することで，多角的なセキュリティレベルの把握・分析を支援する新しい可視化手法を提案する．

2. 情報資産管理保護システム

現在，我々の研究グループで開発している情報資産管理保護システム[1][2][3]の全体構成図を図1に示す．このシステムでは，構成情報に基づく認証によって端末検証局から証明書が得られたホストのみがデータセンタのサービスを受けられる仕組みになっている．データセンタでは，インベントリの収集によるIT資産管理，ポリシに基づくアクセス制御，通信ログの収集・蓄積によるネットワークフォレンジック等のサービスを提供することを想定しており，各サービスに必要となる複数のデータベースを個別に保持している．

本研究では，これらのデータベースの情報を関連付けて組織内にある情報資産のセキュリティレベルを多角的に解析するための可視化手法を提案する．

3. セキュリティレベル分析における課題

3.1 蓄積情報の抽出と関連付けに関する課題

ネットワークのセキュリティレベルを把握するためには，IT資産情報や通信ログなど，複数の情報から必要な情報を抽出し，それを関連付けて意味のある情報として捉える必要がある．しかし，経験豊富な技術者でさえ，膨大な情報の中からどの情報を選び出して関連付ければ目的の情報が得られるかを判断するのは難しい．

また，既存のシステムでは，情報の関連付けがあらかじめ固定されており，ベンダーが想定した特定のセキュリティインシデントに関する情報等をいかに効率よく把握するかという点に特化されているものが多い．しかし，そのようなインシデントのみならず，未知のインシデントが発生する可能性もある．従って，蓄積情報の抽出と関連付けは柔軟性を持たせることが重要である．

3.2 ネットワークの全体像と個々の事象との関連性の把握に関する課題

セキュリティレベルの分析を行う際に，ある一部の事象を観測するだけでは，ネットワーク全体や個々のホストに生じた重大なセキュリティ上の問題を見落としてしまうことがある．ネットワーク全体のセキュリティレベルを多角的に分析するには，一部の事象がネットワーク全体にどのような影響を及ぼしているのか，他の複数の事象とどの様な関連性があるのかを把握することが重要である．

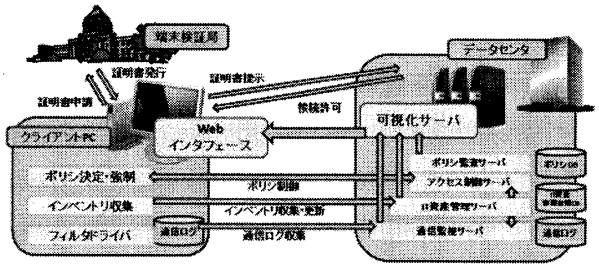

図1　情報資産管理保護システムの全体構成図

また，ネットワークに関する情報は，物理／論理ネットワーク構成図に記載されるような情報をはじめ，上位層のプロトコル情報やアプリケーションサーバの情報等，複数の概念で構成されており，一つの通信はそれらの関連付けによって表現できる．既存のシステムでは，個々の事象を提示する際に，概念の異なる情報を混在させたまま提示したり，特定の情報しか提示していないものが多い．これでは，セキュリティ事象の把握や問題の切り分けを難しくし，見落としにも繋ってしまう．セキュリティレベルの把握や分析を正確に行うためには，概念の異なる情報を明確に分けて捉えつつ，概念間の関連する情報を同時に把握できるようにする必要がある．

4. セキュリティ分析のための可視化モデル

4.1 可視化モデルに対する要件

前節の議論から，情報資産のセキュリティレベルを多角的に分析するための要件は次のようにまとめられる．

要件1.　情報の関連付けが柔軟に行えること
要件2.　ネットワーク全体の状態と個々の事象間の関連性を把握できること
要件3.　情報を概念ごとにまとめたレイヤとして表現し，レイヤ間の関連性を把握できること

以下では，これらの要件を満たす，新たな可視化モデルを提案する．

4.2 レイヤ選択型統合可視化モデル(提案モデル)

提案モデルは，情報を概念ごとにまとめたレイヤを任意に選択し，それらを統合して可視化する手法である．図2に提案モデルの概念図を示す．

提案モデルではロケーション，物理NW，論理NW，アプリケーションサービスごとにレイヤを分け，可視化を行う．ロケーションレイヤは，ネットワークに属する機器の設置場所や管理者などの情報を提示するレイヤであり，このレイヤの機器設置場所情報は後述する他のレイヤ上の機器表示位置に反映される．物理NW／論理NWレイヤは，一般にネットワーク運用管理の際に用いられる物理ネットワーク構成図，及び論理ネットワーク構成図に相当し，それぞれの構成図に記載する情報を提示するレイヤである．アプリケーションサービスレイヤは，このモデルを適用するシステムが有する複数のサーバ(通信ログサーバやポリシ監査サーバ等)の情報を可視化するためのレイヤであり，各サーバの情報ごとに一つのレイヤが割り当てられる．各レイヤは，分析内容に応じて可視化ビュー内で差し替えて表示することができる．

A Visualization Method by Selecting and Stacking Information Layers for Multidirectional Analysis of Security Level for Network Resource.
† Yuichi Saito and Masami Mohri・Gifu University
‡ Yoshiaki Shiraishi・Nagoya Institute of Technology
†† Youji Fukuta・Aichi University of Education
††† Ryoji Noguchi・Toyotsu Syscom Corp.

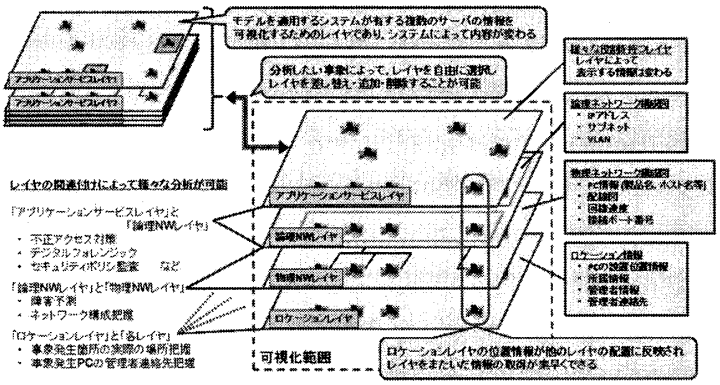

図２　提案モデルの概念図

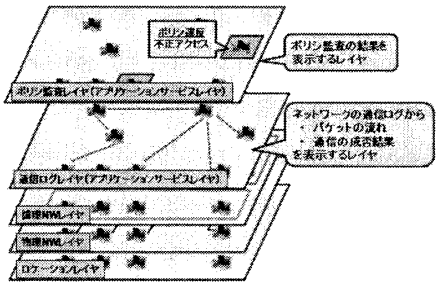

図３　アプリケーションサービスレイヤにポリシ監査レイヤと通信ログレイヤを適用した場合の例

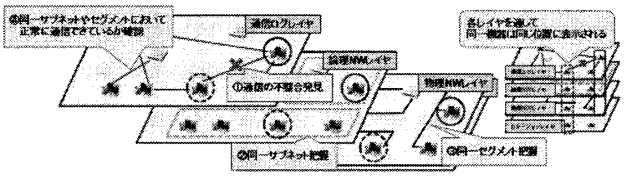

図４　全体を捉えつつ複数のレイヤを参照して事象を分析

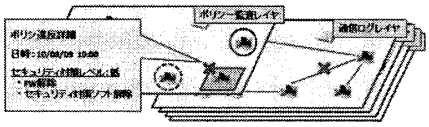

図５　レイヤを差し替えて違う視点から分析

このモデルの特徴は，ビュー内に各レイヤを同時に表示することによって，レイヤごとに個々の情報を把握しながら，レイヤ間の関連性も捉えやすくしている点にある．各レイヤ内の機器の表示位置はロケーションレイヤの機器設置場所情報が反映されている．このため，ある機器について，レイヤをまたがって情報を取得する場合は，各レイヤで同じ位置に表示されている機器の情報を参照すればよい．この表示手法によって，例えばアプリケーションサービスレイヤで通信ログを参照し，それと物理 NW／論理 NW レイヤの情報を関連付けて，不正アクセスや通信障害履歴の把握等，多角的な分析が可能になる．また，通常の物理／論理ネットワーク構成図では把握できなかった機器の位置情報や，物理構成図の膨大な情報なども一つの画面内で参照できるようになっている．

以上のことから提案モデルでは，レイヤの差し替えによる柔軟な情報の関連付け(要件 1)や，ネットワークの全体像を捉えつつ個々の機器に対する詳細な情報の把握(要件 2)が可能となり，さらに，レイヤをまたいでの関連付けを容易に行うことができる(要件 3)ため，前述の要件を全て満たしている．

5. 提案モデルを使ったセキュリティレベル分析の例

我々の研究グループで開発している情報資産管理保護システム[1][2][3]では，データセンタのサービスとして IT 資産管理サーバやポリシ監査サーバ，通信監視サーバ等を用意している．このシステムに提案モデルを適用する場合には，ポリシ監査サーバと通信監視サーバを，それぞれポリシ監査レイヤと通信ログレイヤというアプリケーションサービスレイヤとして追加することができる(図３参照)．これらのレイヤを差し替えることによって，ポリシ違反や，不正通信などの事象を物理 NW／論理 NW レイヤと関連付けて把握できるようになる．

以下では，上記のシステムで整合性が取れない通信が行われた(送信側／受信側の通信ログが不一致)場合を例に挙げて，提案する可視化モデルを使ってセキュリティレベルを分析する様子を説明する．

5.1 全体を捉えつつ複数のレイヤを参照して事象を分析

図４は，アプリケーションサービスレイヤとして追加された通信ログレイヤにおいて，整合性のとれない通信が行われた 2 台の PC が観測された様子を表している．この事象が発生するケースとしては，いくつかのことが考えられるが，その原因を特定するために複数のレイヤ情報を使って分析を行う．

まず，通信障害を仮定して分析を行う場合は，該当箇所だけではなく，ネットワーク全体での現象を捉える必要がある．対象となる 2 台の PC の表示位置から，同一セグメント／サブネットに属する機器を物理 NW／論理 NW レイヤを使って把握し，通信ログレイヤでそれらの機器の通信状態を調べる(要件 1，2，及び 3 の実現)．同一セグメント／サブネットの機器でも整合性のとれない通信が行われていた場合は，何らかの原因による通信障害が原因であったと判断できる．一方，正常に通信が行われている場合は，別の原因を仮定して分析する必要がある．

5.2 アプリケーションサービスレイヤを追加して別の視点から分析

先の分析で通信障害ではないと推測された場合は，他のアプリケーションサービスレイヤを追加し，別の視点から分析する．ここでは，ポリシ監査レイヤを追加し，整合性の取れていない通信の原因を分析する．例えば，図５のようにポリシ監査レイヤ上で，対象となる 2 台の PC 以外にポリシ違反を示す強調表示と，その詳細情報が「セキュリティ対策レベル：低 (FW 解除，セキュリティ対策ソフト解除)」となっている PC が確認された場合は，マルウェア感染等によるなりすまし(詐称パケットの送信)が考えられるため，該当 PC の稼働期間と他の整合性がとれない通信との関連性を調査する．このように，レイヤを追加してネットワーク内のセキュリティ事象を捉えることで多角的な分析が可能になる．

6. おわりに

本研究では，情報資産のセキュリティレベルを多角的に解析するための可視化に対する要件を①情報の関連付けを柔軟に行えること，②ネットワーク全体を捉えつつ個々の事象間の関連性を把握できること，③情報を概念ごとにレイヤで分け，そのレイヤ間の関連性の把握も容易にできることとしてまとめ，それらを満たす可視化モデルを提案した．また，提案した可視化モデルを具体的なネットワークサービスシステムに適用し，有用性を確認した．

参考文献

[1] 脇田知彦，白石善明，毛利公美，福田洋治，野口亮司，“サーバサイドのネットワークを保護するための TPM を用いた接続資格保障基盤”，情報処理学会第 72 回全国大会講演論文集，2010 年(掲載予定)．

[2] 佐々木啓，白石善明，毛利公美，福田洋治，野口亮司，“エンドポイントでポリシー強制を行うアクセス制御フレームワーク”，情報処理学会第 72 回全国大会講演論文集，2010 年(掲載予定)．

[3] 大谷佳輝，毛利公美，白石善明，福田洋治，野口亮司，“ポリシー強制ポイントをエンドホストで実現するための通信制御機構”，情報処理学会第 72 回全国大会講演論文集，2010 年(掲載予定)．