動的ネットワーク構成による
サイバー攻撃対策支援手法の研究

長谷川 皓一

概要

近年，サイバー攻撃の手口が日々巧妙化しており，深刻な被害が伴った事例が相次いで発生している．我が国においては，2011 年に発生した大手重工メーカに対する攻撃や，2015 年に 125 万件の年金情報が流出した日本年金機構に対する攻撃などが広く世間の話題となった．このような深刻な被害を引き起こす巧妙な手口のサイバー攻撃の多くは，標的型サイバー攻撃と呼ばれる類のものである．従来行われてきたサイバー攻撃は，攻撃者が自身の技術誇示を目的に行うものなどが中心であり，不特定多数に対して単純な手口で行われ，その対策も比較的容易に行うことが可能であった．それに対し標的型サイバー攻撃は，先の例のように大手企業や国家機関などといった特定の攻撃対象を持ち，情報窃取などを目的に行われるものである．攻撃者の動機も機密情報の換金や脅迫などによる金銭を目当てとしたものであり，組織的な犯行の場合も多い．加えて，標的に関する事前調査活動を入念に行った上で，知り得た情報を元に攻撃対象に特化した手口や専用に設計したマルウェアを用いて攻撃が行われるなど，手口が非常に巧妙であり対策が難しい．このような攻撃対象専用のマルウェアは，ファイアウォールや侵入検知システムなどの既存のセキュリティ対策をすり抜けてしまう可能性が高い．そのため，従来から一般的に行われてきた，組織内部ネットワーク入口において外部からのマルウェア等の侵入を防止するためのセキュリティ対策ではマルウェアの侵入を完全に防止することは困難な状況である．

これに対し昨今では，新たな対策としてマルウェアがネットワーク内に侵入してしまった後に，実質的な被害を出さないための対策が重要視されている．そのうちの一つの対策手法として，ネットワーク内部分離設計がある．この対策手法では，組織内部のネットワークを複数セグメントに分割し，不必要な通信を行えない状態にする緻密なアクセス制御を施すものである．これにより，マルウェアが行う不正通信の抑制や，効率的なネットワークの監視，感染端末の効率的な切り離しなどが期待できる．しかしながら，ネットワーク内部分離設計はその構築や管理運用が困難であるという問題があり，一般的なエンタープライズネットワークに採用される例は少ない．

そこで本論文では，サイバー攻撃の対策支援手法の提案を目的とし，動的にネットワーク機器の設定を変更することで状況に応じた適切なネットワーク構成を構築する，動的

ネットワーク構成に着目する．動的ネットワーク構成のコンセプトのもとで，ネットワーク内部分離設計の構築支援手法，ネットワーク内通信の監視および不正通信解析の管理支援手法，インシデント対策支援手法の三つの提案を行う．これにより，インシデントが発生する以前より攻撃による影響を低減するためのネットワーク構築から，運用中のネットワークの効率的な監視および解析，またインシデント発生時における対策の適用まで，ネットワーク管理者の運用管理を包括的に支援することが可能となる．

一つ目のネットワーク内部分離設計構築手法として，ネットワーク内で運用されているディレクトリサービスの情報および観測したネットワーク内のトラフィックを用いて，ユーザのファイルへのアクセス権限を基準とした構築手法を提案する．ネットワーク内部分離設計の構築を行うためには，ネットワーク内の通信の必要性を判断するために何らかの基準が必要となるが，本論文では組織内のユーザのファイルへのアクセス権限とネットワーク上のトラフィックを用いることを検討した．一般にサーバには様々なファイルが保管されているが，各ファイルの用途や所有者などに応じてアクセス可能なユーザは限定されている．そこで，ネットワーク内の各端末において，端末を利用するユーザがアクセス権を有しないファイルを保管するサーバへの通信は必要ないと仮定し，アクセスを制限する候補とした．その上でトラフィックを収集し，アクセスを制限する候補の通信区間において，実際に通信が発生していないことを確認することで必要のない通信区間と判断した．アクセス権限の管理や設定は複雑なため，一般にはネットワーク内のディレクトリサービスサーバにより一元管理される場合が多い．ディレクトリサービスサーバよりこれらのアクセス権限情報を取得することにより，ネットワーク管理者の調査や入力などの手間をかけずアクセス制御の基準となる情報を取得可能とした．アクセス制限を動的ネットワーク構成によりネットワークに適用することで，容易に内部分離設計を構築可能とした．また，アクセス制限の追加や変更などを行う場合も，動的ネットワーク構成により容易に新たなネットワークを再構成可能である．ディレクトリサービスサーバとして Microsoft Windows Server 上の Active Directory を想定し，アクセス制御リストを自動的に生成するプロトタイプシステムを作成し，小規模のネットワークにおいて実験を行った．実験において，システムを利用して生成したアクセス制御リストと，被験者が手動で生成したアクセス制御リストを比較した．その結果，システムが生成したアクセス制御リストは冗長なアクセス制御が含まれておらず，また被験者が設定すべきと判断したアクセ

ス制御を概ね包含していた．また，システムが生成したアクセス制御リストを被験者が確認し，各アクセス制御の適用を許可するまでの時間と，被験者が手動でアクセス制御を生成する時間を比較した結果，システム利用時はより短い時間でアクセス制御リストを決定できることがわかった．以上により，提案手法の有効性を確認した．

二つ目のネットワーク内通信の監視および不正通信解析の管理手法では，構築したネットワーク内部分離設計の特性を利用し，効率的にネットワークの監視および疑わしい通信の解析を行う手法を提案する．組織内ネットワーク入口において，ネットワーク上のトラフィックを監視することによる不正な通信の検知はサイバー攻撃対策として一般的によく行われている．これを組織内ネットワークのトラフィック監視にも拡大し，標的型攻撃における初期侵入後の内部侵食などを検知する提案はされている．しかし，ネットワークの規模にもよるが組織内ネットワークの大量のトラフィックを一元的に監視するには多大なコストが必要である．また，不正通信の検知を行うシステムはその通知に必ず誤検知が伴うため，それらの処理もネットワーク管理者の作業を増やす大きな要因である．そこで，本論文では一度に監視対象とするトラフィックを一定のセグメントに限定し，対象セグメントを順次切り替えていく巡回監視を管理する手法を提案する．動的ネットワーク構成を用いることで，このような監視対象セグメントの異なるネットワークを繰り返し再構成可能であり，巡回監視が実現可能である．これにより，一度に監視を行うトラフィック量を低減させることが可能となり，監視コストの削減が期待できる．また，確実に不正な通信を検出するのみならず，不正な通信の疑いのあった事象を管理することで攻撃検知の支援が可能となる．不正な通信と疑われるものが検知された場合には，検知システムの特性や検知された不正の内容などに応じて監視頻度の増大，トラフィック解析を行うことで，さらなる証拠の取得や効率的な解析を支援することが可能となる．提案システムによる検出コストの低減と，監視を巡回的に行うことによる不正通信検出の遅延について，簡単なマルウェアモデルを用いて行った性能評価により，このトレードオフを定量的に評価し，有効性を確認した．

三つ目のインシデント対策支援手法では，インシデント発生時に状況に応じた対策設計候補を管理者に推薦する手法を提案する．インシデントが発生した際には，状況に応じて適切な対策を施す必要がある．しかし，ネットワーク内の端末の重要さや他の端末への感染拡大状態など，インシデントの状況に応じて適切な対策は異なる．本論文では，インシ

デントが発生した際に複数の対策ネットワーク設計候補を生成し，その内から管理者が選択した候補を適用するためにネットワーク内部分離構造の変更および新規アクセス制御の設定を行う．この際，管理者が容易に適切な候補を選択できるよう，生成された各対策候補の評価を行う．対策として端末の遮断等を行った場合には，その端末はマルウェアが行う不正な通信以外に通常の業務に関連する通信も行えなくなってしまう．これが重要な業務に携わる端末だった場合，対策によりマルウェアにより被害は阻止できても，業務活動が停止するという二次被害が発生してしまう．そこで評価基準は，対策としての有効性と対策を施した場合の業務活動への影響の双方を用いた．また，インシデントの状況によっては，情報漏洩等の深刻な被害を防ぐために，業務活動への影響よりも即座に通信を遮断するといったように，対策の有効性を優先すべき場合もある．提案する評価手法では，これらのプライオリティバランスを考慮して最終的な評価順位を決定し管理者に推薦することにより，適切な対策候補選択の支援が可能となる．動的ネットワーク構成では，対策候補が選択された後に迅速に対策をネットワークに適用可能であることに加え，対策の変更や，事態収束後のネットワークの復元なども容易に行うことが可能である．実際に小規模ネットワークにおいてインシデントの発生を想定した被験者実験を行い，提案手法の評価を行った．提案した評価手法を実装したプロトタイプシステムにより対策設計候補を推薦し選択する場合と，手動で対策を考案する場合のそれぞれの場合に要した時間を比較した結果，システムを利用した場合の方が所要時間が短いことがわかった．この結果から，提案手法の有効性を確認した．

目次

図目次

表目次

第 1 章

序論

近年，サイバー攻撃の手口が日々巧妙化しており，それに伴って深刻な被害が多数発生している．従来のサイバー攻撃と呼ばれるものは，攻撃の対象は不特定多数であり，またその動機も攻撃者の技術誇示や単なるいたずら目的などといったものであった．このような攻撃の場合，不特定多数に対して同一の単純な手口で行われるため，その対策も比較的容易に行うことが可能であった．それに対し，昨今は標的型サイバー攻撃と呼ばれる類の攻撃が横行している．標的型サイバー攻撃とは，特定の国家機関や大手企業などの標的に対して情報窃取や妨害行為を目的に行われる攻撃である．攻撃者の動機も金銭目的の場合が多く，組織的な手の込んだ犯行も多い．標的型サイバー攻撃では，標的ごとに異なる手口の攻撃が行われるためその対策の難しさが問題視されている．2015 年に 125 万件の年金情報が流出するという大きな被害が発生した日本年金機構への攻撃などを筆頭に，標的型サイバー攻撃による被害も多数報告されており [1]，標的型サイバー攻撃への対策が重要視されている．

標的型サイバー攻撃においては，事前に標的の企業等に対する入念な調査活動を行い，知り得た情報を用いて攻撃対象企業の構成員に対する標的型メールや，攻撃対象に合わせて専用に設計されたマルウェアの作成などが行われる．このようなマルウェアは個々が有する機能は少ないものが多いが，組織内部ネットワークにおいてマルウェア同士が通信網を生成し，C&C サーバ（Command and Control サーバ）との通信，攻撃者からの指令伝達，情報窃取など，異なる役割を持った複数のマルウェアが活動を行う．また，攻撃対象専用のマルウェアはネットワークに施されている既存のセキュリティ対策をすり抜けてしまう可能性が高い．つまり，従来から広く用いられてきたファイアウォールや IDS（Intrusion Detection System，侵入検知システム），IPS（Intrusion Prevention System，侵入防止システム）などの外部ネットワークと内部ネットワークとの境界において攻撃の

侵入を防ぐためのセキュリティ対策では，攻撃を完全に防ぐことは困難である．

標的型サイバー攻撃の対策は様々な手法が研究，議論されている．特に昨今では，外部からのマルウェアの侵入を防ぎきることが困難であるため，マルウェアに侵入されてしまった後に，実質的な被害を食い止めるための対策が重要視されている [2][3][4]．このような対策の内の一つに，ネットワーク内部分離設計が挙げられる．組織内部ネットワークを複数のセグメントに分割し，セグメント間や端末間において緻密なアクセス制御を行うことで，マルウェアが侵入したネットワーク内において行う感染拡大や情報摂取などの不正通信の抑制が期待できる．また，アクセス制御のログから，設定されたアクセス制御を違反して通信を試みた端末を洗い出し，調査することで，マルウェアの早期発見が期待できる．インシデントが発覚した際にも，感染端末や攻撃対象となったサーバの切り離しなどの対策が行い易くなる [5]．しかしながら，ネットワーク内部分離設計は構築が困難であるという問題点がある．ネットワーク内部分離設計を構築するためには，ネットワーク内においてどのような通信が必要であるかを細かく検討する必要がある．ネットワーク管理者のみで業務や人事に関するあらゆる情報を収集し，ネットワーク内における通信の必要性を検討することは難しい．また，ネットワーク内部分離設計を構築したとしても，その構成の複雑さから管理運用のコストも膨大となってしまう．そのため，一般的にはエンタープライズネットワークに採用される例は少ない．

そこで本論文では，サイバー攻撃の対策支援手法の提案を目的とし，動的にネットワーク機器の設定を変更することで状況に応じた適切なネットワーク構成を構築する，動的ネットワーク構成に着目する．動的ネットワーク構成のコンセプトのもとで，ネットワーク内部分離設計の構築支援手法，ネットワーク内通信の監視および不正通信解析の管理支援手法，インシデント対策支援手法の三つの提案を行う．一つ目のネットワーク内部分離設計構築支援手法では，すでにネットワーク内で運用されているディレクトリサービスの情報および観測したネットワーク内のトラフィックを用いて，ユーザのファイルへのアクセス権限を基準としたアクセス制御を生成する．これを動的ネットワーク構成を用いて適用することで，ネットワーク内部分離設計を構築し，アクセス制御の変更などの管理運用も容易に行うことが可能となる．これにより，ネットワーク内部分離設計の構築が困難であり，管理運用が複雑であるという問題点を解決する．二つ目のネットワーク内通信の監視および不正通信解析の管理支援手法では，構築したネットワーク内部分離設計の特性を

利用し，分割されているセグメントの中から順に対象を切り替えて通信の監視を行う巡回監視と，必要に応じて効率的に疑わしい通信の解析を行う．動的にネットワーク機器の設定を切り替え，監視対象の異なるネットワークを繰り返し再構成することで，効率的な巡回監視や不正通信の解析を可能とする．これによりネットワーク監視や解析のコスト低減を可能とする．三つ目のインシデント対策支援手法では，なんらかのインシデントが発生した状況下において，その対策としてマルウェアの侵食などの活動を抑えつつ，業務活動へ及ぼす影響を抑える形にネットワークを再構成するため，複数の対策設計の候補を生成し，それを評価することで管理者が適切な候補を選択し易いよう推薦する．動的ネットワーク構成を用いることで，選択された対策を即座にネットワークに反映可能であり，また対策の変更や事態収束後のネットワークの復元の容易に行える．これにより，効果的かつ業務継続性の高い対策を迅速に適用することが可能となる．以上の三つの支援手法を用いることにより，インシデントが発生する以前より攻撃による影響を低減するためのネットワーク構築から，運用中のネットワークの監視および解析，またインシデント発生時における対策の適用まで，ネットワーク管理者の運用管理を包括的に支援することが可能となる．

本論文の構成は以下の通りである．まず第 2 章において近年のサイバー攻撃の特徴やその手法について述べ，またサイバー攻撃への対策とその問題点について述べる．次に第 3 章では，本論文のサイバー攻撃へのアプローチである動的ネットワーク構成によるサイバー攻撃対策支援手法について述べる．第 4 章では，本論文が行うサイバー攻撃の対策支援の一つである，攻撃による不正通信の抑制および検知などが行い易いネットワーク構造であるネットワーク内部分離設計の構築支援手法を提案し，評価を行った．次に，構築した内部分離ネットワークにおいて，効率的にネットワーク内通信の監視や検知された疑わしい通信の解析を行うための，通信監視および解析の管理支援手法について第 5 章で述べる．第 6 章では，実際にネットワーク内においてインシデントが発生した際に，迅速に攻撃に対して効果的かつ業務活動への影響が少ない対策を行うための，インシデント対策支援手法について述べる．最後に，第 7 章でまとめる．

第 2 章

近年のサイバー攻撃

本章では，近年の巧妙化するサイバー攻撃の動向について，事例の分析を踏まえ紹介する．また，昨今の巧妙な手口の攻撃への対策の難しさと従来より用いられてきたセキュリティ対策の問題点について説明する．

2.1　サイバー攻撃の遷移

昨今では「サイバーセキュリティ」や「サイバー攻撃」などといったキーワードが広く一般的にも浸透するようになった．しかしながらサイバー攻撃の歴史は古く，世界初のコンピュータウイルスとも言われるパキスタンで開発された「Brain」が発見されたのは 1986 年である [6]．これは，違法コピーによって感染するコンピュータウィルスであり，著作権に関するメッセージを表示するという動作をするものであった．それ以降，種々のコンピュータウィルスが出現して来たが，多くの物は感染したコンピュータ上で何らかの副作用を生じさせ，また無差別な感染を行うものであった．この動作がコンピュータウィルスという名称の由来となっている．しかしながら，近年のサイバー攻撃では発覚を防ぐために感染対象を限定したり，コンピュータ内に潜んで間欠的な動作をするなど，名前の由来となった生物学上のウィルスのような動作をしない物も多用されている．そのため，近年ではコンピュータウィルスという名称に替わり，マルウェアという名称が主として用いられるようになってきてる．「マルウェア=malware」とは，「悪意がある=malicious」という言葉と，「ソフトウェア=software」という二つの言葉を組み合わせた言葉である．コンピュータウィルスおよびマルウェアは，その出現時より，サイバー攻撃において重要な地位を占める，悪意のあるソフトウェアである．

コンピュータの技術や性能が発達し，その使用目的も多種多様に変化してきた中で，サ

イバー攻撃もまたその目的や特徴が変化してきている．従来のサイバー攻撃は，愉快犯によるいたずら目的や攻撃者自身の技術誇示などの目的において，不特定多数を対象として行われていた．また，政府系や大手企業の Web サイトの改竄等のように政治的プロパガンダなどが目的の攻撃も存在した．このような攻撃のうちの多くは単純な手口で行われるものであり，その対策も比較的容易に行うことが可能であった．

それに対し近年では，ある特定の企業や国家機関などの攻撃対象に対して，機密情報や顧客情報等の窃取や妨害行為のためのデータやシステムの破壊行為を行う標的型サイバー攻撃と呼ばれるサイバー攻撃が増加している．このような攻撃は金銭を目的として商業的に行われており，犯行も組織的に行われるものが多い．そのため，その手口も多種多様で非常に巧妙なものであり対策が難しく，深刻な被害も多く発生している．独立行政法人情報処理推進機構（以降 IPA）では，このような攻撃を「新しいタイプの攻撃」,「高度標的型攻撃」などと呼んでいる．

2.2　標的型サイバー攻撃

標的型サイバー攻撃（以下，標的型攻撃）は様々な手口の攻撃が存在する．攻撃者は標的に関する事前の調査活動を行い，知り得た情報を用いて攻撃対象に合わせてカスタマイズされた攻撃が行われるため，全く同じ攻撃は存在しない．また，無差別な攻撃と比較して，多大な時間と手間をかけて攻撃を行うことも特徴的であり，念入りな調査活動により，利用中のセキュリティ対策機器およびソフトウェアなどの細かい情報を用いて，セキュリティ対策を回避する攻撃手法が検討される．また，標的型サイバー攻撃では他では手に入らない機密情報等を窃取することを目的とすることが多いため，一旦攻撃が失敗してもそこで攻撃は終わらず，手を変え品を変えしつこく攻撃を継続してくることもしばしば見られる．

2.2.1　標的型攻撃の手順

標的型攻撃の手口は多種多様ではあるが，攻撃の一連の過程は基本的には同一である [7]．本論文では，攻撃が行われる過程を以下の 5 段階に分類する．

1. 組織内部への侵入

2. 攻撃者との通信の確立
3. 組織内部でのマルウェア拡散
4. サーバ等の重要機器からの情報窃取
5. 外部への情報送出

以下，各段階の詳細と用いられる手口を説明する．

段階 1：組織内部への侵入

まず始めに，何らかの手法により組織内部の端末をマルウェアに感染させる段階である．組織への侵入が行われる方法は様々なものが存在する．以下は攻撃によく利用される代表的な 3 パターンを紹介する．

- 正規 Web サイト閲覧によるマルウェア感染

  Drive by Download 攻撃とも呼ばれる感染手段であり，組織内部の端末が攻撃者により改竄された状態の正規の Web サイトを閲覧することによりマルウェアに感染するパターンである．正規の Web サイトに対して攻撃者は SQL インジェクションを行うなど，なんらかの脆弱性を利用してあらかじめ Web サイトの改竄を行い，攻撃用サーバとして機能させてしまう．このような改竄が行われているサーバに対して標的となる特定の組織からアクセスを行うと，直接マルウェアのダウンロードが行われてしまう，もしくはマルウェアの配布を行うためのサーバにリダイレクトされてしまい，端末がマルウェアに感染する．近年では Web ブラウザやインターネット検索サイト，またアンチウイルスソフトウェアなどにより，ブラックリストに登録された不審なサイトに対するアクセスは警告を出すなどの取り組みが広まっている．しかしながら，改竄が行われるのはブラックリストに登録されにくい正規の Web サイトであるため，通常通りアクセスが可能であり，対策は非常に困難である．

  また標的型攻撃においては，改竄する Web サイトとして標的対象の端末が頻繁にアクセスを行う Web サイトを用いる水飲み場型攻撃と呼ばれる感染手段が利用される場合も多い．
- 標的型メール攻撃によるマルウェア感染

事前に調査した情報を用いて，受信者の関係者や取引先等を装い，送信元アドレスの偽装などを行った巧妙なメールを送りつける標的型メール攻撃がある．送付したメールからマルウェアの送り込みには，一般的にはメール本文に記載された URL をクリックすることによりマルウェアをダウンロードさせたり，脆弱性を狙った添付ファイルを実行させることによりマルウェアに感染させるといった手口が使用される．近年では標的型メール攻撃に対する社員教育を実施するなど，不審なメールを開封しないようにするための取り組みが行われている．しかしながら，電子メールは近年，業務上最もよく利用される連絡手段の一つであり，関係者や取引先を騙ったメールであれば業務上開かざるを得ないというのが現状である．特に，企業の人事，広報，苦情などの担当部署などといった，組織外部からのメールも数多く受け付ける部署にとっては，多少の不審さがあっても業務上開かざるを得ないことが多い．そのため，このような組織外部からのメールも数多く受け付ける部署は標的型メール攻撃において良く狙われることとなり，この手口によるマルウェア感染のリスクが非常に大きくなる．標的型攻撃においては，このような部署へのマルウェア感染を起点とし，組織内部へと攻撃を行い，侵食していく．

- 記憶媒体介在によるマルウェア感染

  様々な電子記憶媒体を用いたマルウェア感染も存在する．電子記憶媒体には SD カードや CD-ROM など様々な種類のものが利用されているが，中でも USB メモリはデータの受け渡しなどに最もよく利用される手段であり，これを狙った攻撃もよく行われる．この手段では，マルウェアが含まれた電子記憶媒体を端末に接続することによって，その端末はマルウェアに感染する．この方法では，ネットワークを介した感染とは異なり，インターネットから完全に分離され，独立している状態にあるスタンドアロンネットワークに対してもネットワーク内でマルウェア感染が拡がる危険性がある．また，スタンドアロン型のネットワークであれば一見すると情報漏洩の危険はないように思えるが，このような電子記憶媒体を用いたマルウェアの場合，収集したネットワーク内部の情報を電子記憶媒体に保存して持ち出すという手口もあり得るため，情報漏洩のリスクは存在する．

  記憶媒体介在マルウェア感染の例として，Stuxnet[8] が挙げられる．Stuxnet はインターネットから切り離されたイランの核施設に対する標的型攻撃に用いられたこ

とで有名であるが，これはまさにスタンドアロン型のネットワークを標的にした媒体介在マルウェアである．

段階 2：攻撃者との通信の確立

組織内の端末に感染したマルウェアは，C&C サーバと呼ばれる攻撃者側のサーバと通信を行うことで，自身の更新や指令のダウンロードなどを行う．また，外部からの遠隔操作を行うことが可能な RAT（Remote Administration Tool/Remote Access Trojan）などを使用した感染端末の直接操作により，攻撃者は感染端末のキータイプだけでなく，画面を覗き見することも可能となり，ソフトウェアキーボードなどの対策を講じても，認証情報を窃取できる．その結果，感染端末を踏み台とした社内への攻撃など，様々なリスクが増大する．

段階 3：組織内部でのマルウェア拡散

マルウェアが C&C サーバとの通信により攻撃者より司令を受け取るもしくは，マルウェアを介して攻撃者が遠隔操作を行うことにより，ネットワーク内で侵食活動を行う．この際，攻撃者が感染端末の操作を自由に行うことが可能となるローカルの管理権限の奪取の他に，組織内で利用される認証サーバを攻撃することでネットワーク全体の端末が操作可能となるシステム管理権限を狙う場合も多い．

一般的に，機密情報にアクセス可能な端末は組織内や外部との通信を制限されている場合が多い．しかしながら，マルウェア感染が拡大し，攻撃者が操作可能な端末が増えることによって，攻撃者が目的としている機密情報にアクセス可能な端末へと到達する通信経路の確立や，その端末の権限を奪われる可能性が高まり，情報漏洩の危険性が増加する．また，一部のマルウェアは発覚時に証拠隠滅のためにシステム破壊行動を取るものが存在するが，このマルウェアによるシステム破壊活動のリスクにおいても，マルウェアの浸透が深く進むほど，組織内部で破壊される可能性のある端末は増加するため，業務に与える影響は増加していく．

段階 4：サーバ等の重要機器からの情報窃取

一般的に，重要な情報が保存されているサーバについては，アクセスできる端末を限定するなどの措置が取られている．しかしながら，サーバへのアクセス権を持つ端末が限定されているような状況においても，アクセス権を持つ端末がマルウェアに感染し攻撃者により制御できる状態になってしまう場合，サーバから情報の窃取が可能となってしまう．さらに，ネットワーク管理者の端末が権限を取られれば，そのようなアクセス制限を解除されてしまうことも考えられる．これにより，重要な情報が保存されているサーバより個人情報などの組織内部の重要な機密情報が読み出され，攻撃者の手に渡ってしまう．

段階 5：外部への情報送出

最終的に，攻撃者は侵入した組織内ネットワークで獲得した情報を外部のサーバ等に送出する．通常，このような情報送出はインターネットを通してサーバ等に送信されるが，一般的には組織内部のホストが通常行う通信に紛れて行われるため，発見が非常に難しい．場合によっては暗号通信を利用されるため，発見はますます難しいものとなる．すべての段階が成功してしまうことにより，企業の重要な情報が窃取されてしまう．

2.2.2 標的型攻撃の事例

標的型攻撃の事例は数多く存在し，特に衆議院・参議院を狙った攻撃や JAXA に対する攻撃，国内大手重工メーカに対する攻撃など，広く世間の話題となったものも多い．なかでも，2015 年に発生した日本年金機構に対する攻撃では，125 万件の年金情報が流出するという深刻な被害が報告され話題となった．

大手重工メーカへの攻撃

2011 年，国内の大手重工メーカである三菱重工業に対して標的型攻撃が行われた [9]．IPA の分析レポート [10] によれば，この攻撃の侵入経路は標的型メールを開封したことであった．この標的型メール中には，正規に送られたメールを盗み取ってその内容や書式を模擬することで，約 10 時間後に標的型メールへと悪用され送付されたものもあり，非常に巧妙な手口であったことがわかる．マルウェアの感染が拡大し，組織内でマルウェア

に感染したサーバやコンピュータ端末は複数拠点で約 80 台にものぼったと報告されている．最終的に，ある拠点の事務所のサーバにマルウェアが窃取した情報を集約させ，そこから米国に置かれたサーバへと情報送出が行われた．これは，多くの端末が一つのサーバに集中して情報を送るより，一点からまとめて送信した方がマルウェア感染の発覚を遅らせる可能性があるためである．

日本年金機構への攻撃

2015 年 6 月，日本年金機構（以下，年金機構）より 125 万件の年金情報が流出したと発表され，大きな話題となった．内閣官房セキュリティセンター（以下，NISC）による調査報告 [11] によれば，この攻撃においては多数の巧妙な標的型メールが年金機構職員に対して送付され，職員が開封したことによりマルウェアに感染した．送付された標的型メールは 4 種類に分類されている．そのうち，最初のメールは外部に公開されているメールアドレスに対して送付されていたが，それ以降のものについては，何らかの方法で攻撃者が手に入れた，一般には非公開のメールアドレスに対して送付されたものも含まれていることからも，この攻撃が非常に巧妙な手口で行われたことが伺える．

NISC が厚生労働省ネットワークにおいて不審な通信を検知，通知したことから，年金機構では都度不審な通信を行った端末の LAN ケーブルを抜く対策が行われた．しかしながら，通信が遮断された後も攻撃は継続され，先述のように 4 度に渡り標的型メールが送られるという執拗な攻撃が行われた．その結果，最終的には 20 台以上の端末が攻撃者の操作可能な状態となり，125 万件の年金情報の流出という，甚大な被害を出してしまった．この攻撃においては，本来はネットワーク上では隔離されていたサーバに存在していた年金情報を，業務の利便性を優先してネットワーク上の端末に保存していたことも，被害の増大に拍車をかけた．

2.3　サイバー攻撃へのセキュリティ対策

2.3.1　従来対策とネットワーク構造

境界防御

従来から広く用いられてきたセキュリティ対策は，いわゆる境界防御と呼ばれるものが中心である．外部ネットワークであるインターネットと，組織内の端末が属する内部ネットワークにおいて，ファイアウォールやネットワーク型 IDS，IPS などを利用して不正な通信を検知，遮断する手法である．

ファイアウォールでは，インターネットとの境界においてあらかじめ設定された必要な通信のみを許可し，その他の通信を遮断する．しかしながら，2.2 節で述べたように標的型攻撃においては事前の調査活動により知り得た情報を用いて攻撃対象に特化した専用のマルウェアが使用されるため，組織内で通常行われる許可された通信に紛れて活動を行うものが送り込まれる．このような攻撃はファイアウォールで遮断することは困難である．

IDS などでは，ネットワーク上の通信の監視を行い，不正な通信を検知した場合にネットワーク管理者に警告を行う．IDS にはシグネチャ型という予め定義された攻撃の特徴との比較による検知を行うものと，通常通信の統計データをベースに外れ値に対して検知を行うアノマリ型の 2 種類が存在する．シグネチャ型のものでは，予め攻撃の特徴がわかっている必要があるため，ゼロデイ攻撃と呼ばれる未知の攻撃を検知することができない．それに対しアノマリ型のものは統計的に異常トラフィックを攻撃として検知するため，未知の攻撃に対しても効果を発揮する [12]．しかしながら，アノマリ検知によって発見された攻撃は既知のものか未知のものか，またどの程度のリスク要因が含まれているのかといったことがわからない．また，多くのアプリケーションで RFC 違反などの正しくない挙動を示すので，誤検知が多いといった問題点がある．

また，組織内ネットワークにおいてはエンドホストである各端末においてアンチウイルスソフトウェアを導入し，既知のマルウェアの駆除を行う．しかしながら，標的型攻撃で用いられる標的専用のマルウェアはアンチウイルスベンダーが検体を入手しづらいものや，未知の脆弱性を狙うゼロデイ攻撃も含まれているため，各端末でマルウェアを駆除することは困難である．実際に，これまで発生した標的型攻撃の事例では，アンチウイルス

ソフトウェアを適正に利用していたにもかかわらず，新種のマルウェアを検知出来ず事故が発生した．

ネットワーク構造

一般的に用いられる組織内ネットワークの構造を説明する．図 2.1 に示した例のよう

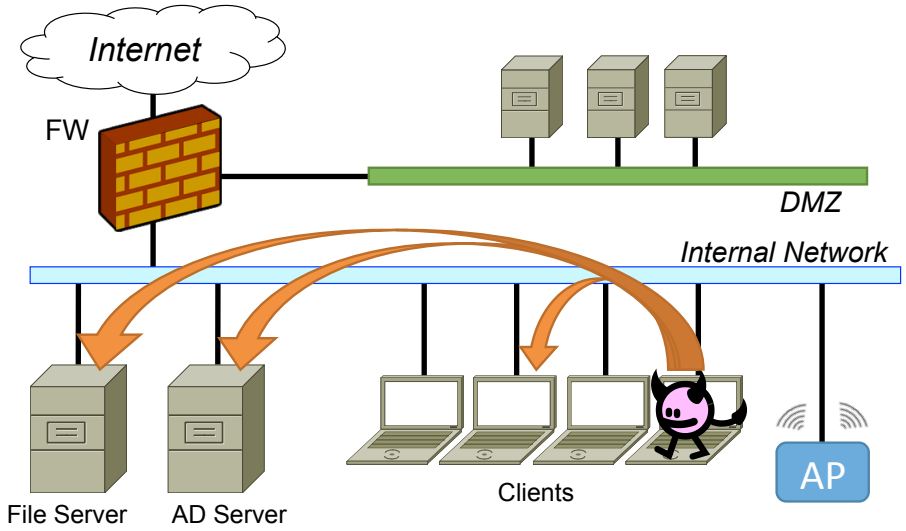

図 2.1　一般的な組織内ネットワーク構造

に，一般的な組織内ネットワークでは，いわゆるフラット構造なネットワークが採用される例が多い．フラット構造のネットワークとは，外部公開向けサーバ等が属する DMZ を除き，内部のネットワークでは全ての端末が同じセグメントに属するような構造を指す．つまり，重要な情報が保管されたファイルサーバや認証サーバ，一般ユーザが使用する端末から無線通信向けアクセスポイントなどまで，全てが同じセグメントに属し，自由に通信が行える状態である．これは，1 台の端末のマルウェア感染が発生した際，組織内に侵入したマルウェアは容易に他の端末と通信が行える状態であるため，感染拡大などの侵食活動や，標的情報の窃取などが行い易い状態である．また，インターネットとの境界に設置した IDS 等が一度マルウェアによる不正通信などを検知した場合においても，組織内ネットワークにおいては当該端末が他のすべての端末と通信可能な状態であるため，その他の端末の感染状況の調査が難しく，攻撃の全貌把握は困難となる．

これに対し，IEEE802.1Q などによる VLAN を導入し，組織内ネットワークを部署な

どを基準として複数のセグメントに大まかに分割して運用するケースも多く存在する．しかしながら，一般的には共有サーバや共有プリンタなどの使用の利便性を考慮し，全てのセグメント間のルーティングを行う設定となっているため，組織内部ネットワークの全ての端末が互いに通信可能である状態はフラット構造のネットワークと同様である．

このようなフラット構造のネットワークにおいては，一般的には前述の境界防御が行われるため，既存の対策をすり抜けたマルウェアにより被害を受けやすい状況となる．

2.3.2 新たな対策

前述のように，近年の巧妙な標的型攻撃に対しては，従来から行われてきた対策では効果が薄く，ネットワークの境界において組織内部ネットワークへのマルウェアの侵入を完全に防ぎきることは困難である．そこで昨今では，マルウェアが内部ネットワークに侵入してしまった後の対策が重要視されている [2][3][4]．侵入後のマルウェアの検知，不正通信の遮断などを適切に行うことで，マルウェアに侵入はされてしまうが，情報漏洩などといった実質的な被害は食い止めるという対策である．

米国国立標準技術研究所は具体的な対策手法の指針を示した文書を公開している [13]．このようなガイドライン等は様々なものが存在するが，人手によりガイドラインや対策指針に準拠した完璧なセキュリティ対策を構築することは困難であるが，これを自動化できる割合は少ない [14]．その為，セキュリティの実施や運用管理の補助等を容易に行うための研究が数多く存在する [15][16]．

第 3 章

動的ネットワーク構成によるサイバー攻撃対策支援

3.1　まえがき

第 2 章で述べたように，昨今のサイバー攻撃は非常に巧妙な手口で行われ，また対策も非常に困難な状況にある．そこで本論文では，ネットワーク管理者によるサイバー攻撃対策の支援手法の提案を目的とし，以下の 3 項目の支援手法を提案する．

- ネットワーク内部分離設計構築支援
- ネットワーク内の監視活動および不審な通信の解析支援
- インシデント発生時の対応支援

以上の項目の支援手法により，インシデントが発生する以前より攻撃による影響を低減するためのネットワーク構築から，運用中のネットワークの監視および解析，またインシデント発生時における事後対応までを含め，包括的にネットワーク管理者の補助を行い，より迅速かつ適切なサイバー攻撃対策を可能とする．

これを実現するために，本論文では，動的にネットワーク機器の設定を変更し，状況に応じて適切なネットワーク構成を構築する，動的ネットワーク構成を行う．平常時には，業務形態に応じて不必要な通信を遮断するアクセス制御をネットワークに対して構築することにより，サイバー攻撃の影響を受けづらいネットワークの構成が可能となる．また，ネットワーク内における監視対象や解析対象を状況に応じて変更してネットワークを構成することにより，効率的な監視および解析が可能となる．それに加え，インシデント発生時にはアクセス制御を変更しマルウェア感染端末や攻撃対象となったサーバ端末を切り離

したネットワークを構成することにより，ネットワークに対して適切なインシデント対応を施すことが可能となる．以下，本論文が提案する三つサイバー攻撃対策支援手法の全体構成について説明する．

3.2　想定環境

本論文が想定する組織内ネットワークを説明する．提案手法では，クライアントの台数が 100 台程度までの一般的な中規模ネットワークにおいて，一般的な運用形態としてすでに大まかにネットワークの分割が行われているが，アクセス制御等は行われていないネットワークを対象とする．また，ネットワークを構成しているネットワークスイッチ等の機器により，各 VLAN 間や端末間のアクセス制御を行うことが可能な状況を想定する．アクセス制御やネットワーク監視を行う際の端末の管理を行うために，全てのクライアント端末が静的に IP アドレスを割り当てられているものとする．IP アドレスを動的に割り当てる環境の場合にも，IEEE 802.1X 等の認証機構を用いることで本論文の提案システムを適用可能であるが，IP アドレスの割り当て管理や認証が行われる毎にアクセス制御をアップデートするといった仕組みが別途必要となる．

3.3　サイバー攻撃対策支援

本論文が提案する三つサイバー攻撃対策支援手法について，各項目の詳細を説明する．

3.3.1　ネットワーク内部分離設計構築支援

第 2 章でも述べたように，一般的な組織内ネットワークは内部の端末間で自由に通信が可能なフラット構造が主に用いられており，マルウェアの検知や攻撃の全貌把握，またインシデント時の対応が行いづらい状況である．マルウェア対策として有効なネットワーク構造にネットワーク内部分離設計がある．組織内ネットワークにおいて緻密なアクセス制御を行うネットワーク内部分離設計を実施した場合においては，分割されたサブネット間の通信制限によりマルウェアが行う不正通信の抑止や，通信制限に抵触した通信を出力したログにより，マルウェアが試みた通信を検知しやすくなる．それに加え，感染が発覚し

た端末の効果的な切り離し等，対策も取り易い．しかし，複雑な構造のネットワークはセキュリティ対策としての効果が高くても，その構築が非常に困難であるという問題点があり，一般的に用いられるケースは少ない．

そこで本論文では，組織内で運用されているディレクトリサービスの情報とネットワーク内のトラフィックを用いることで，ネットワーク管理者が容易にネットワーク内部分離設計が構築できる構築支援手法を提案する．これにより，ネットワーク内部分離設計の構築が困難であるという問題点を解決する．

3.3.2　ネットワーク内の監視活動および不審な通信の解析支援

組織内ネットワークの入口におけるトラフィックの監視は一般的にも行われている．しかしながら，組織内ネットワーク全てのトラフィックを同時に監視する活動は，ネットワークの規模によっては非常にコストがかかる．また，投入できるハードウェアリソース等の制約で，全てのトラフィックに対して同時に詳細な監視は行えない場合も多々ある．一方で，IDS 等を用いた監視において，サイバー攻撃の検出漏れが無いように厳格な検知ルールを適用すると，誤検知により大量の警告アラートが発生するという問題もある．そのため，厳密な検知ルールによって本物のサイバー攻撃に関連する通信が検知された場合においても，通常は発生したアラートを順に処理していくため，大量の誤検知情報に本当のサイバー攻撃に関する情報が埋もれて対応が遅れてしまう．また，不正通信を解析した結果として感染が疑われる端末が発見された場合においても，即座に通信を発した端末を遮断すべき場合，他の感染端末を調査した後に対策を行うべき場合など，状況に応じて異なる判断が必要となることが多々ある．

そこで本論文では，ある時点でのネットワークトラフィックの監視対象とするセグメントを限定し，一定時間ごとに動的に監視対象を切り替える巡回監視を行う．これにより，一度に監視する必要があるトラフィック量を減らすことが可能なため，監視コストの低減やマルウェア感染の疑いのある端末に対するより詳細な監視を行うことが可能となる．その上で，IDS 等が疑わしい通信に対して検知アラートを出力した場合に，検知を行った IDS 等の特性や検知内容，頻度に応じて，状況の緊急性を判断する．深刻な状況であると判断された場合に，検知の原因となった通信を発生させた端末に関連する通信を解析対象として解析システムへと転送するよう，ネットワーク機器の設定を変更する．以上によ

り，ネットワークトラフィックの効率的な監視を実現し，誤検知の処理や適切な状況判断の支援を行うことが可能となる．

3.3.3　インシデント発生時の対応支援

解析の結果，ネットワーク内の端末のマルウェア感染が発覚した場合，迅速なインシデント対応が求められる．この際，感染端末の切り離しや標的サーバのネットワークからの切り離しなどの対策を行う場合，切り離された標的サーバを利用する業務活動への影響が発生する．しかしながら，インシデント対応には迅速さが要求されるため，現状では，業務への影響を無視してインシデント対応を優先する形が一般的である．連携する業務活動への影響を考慮せずに対策を行った場合，情報漏洩等の被害は防げても業務の停止などの実質的な被害が発生してしまう．一方，業務活動への影響を考慮したインシデント対応を行った場合，複数の対策案に対して適用した場合に影響を受ける端末の洗い出しやその影響の内容の調査には膨大な作業量を必要とするため，人手で実施することは困難である．

そこで本論文では，感染端末の隔離からサーバセグメント全体の遮断などの複数の対策設計候補を生成し，各候補に対して業務への影響度を含めた評価を行った結果を数値として提示し，インシデント対応支援を行うシステムの実現に関する研究を実施した．対策設計候補として，感染が発覚した端末を起点として複数の異なる通信遮断範囲を適用したネットワーク設計を生成する．評価は，発生しているインシデントへの対策の有効性，対策が業務活動に与える影響，現在のインシデントの状況を考慮して行う．最終的には，評価結果を参考にネットワーク管理者が最適な対策設計を選択し，選択された設計をネットワークに反映する．これにより，ネットワーク管理者は業務活動への影響を考慮しつつ有効な対策を施すことが可能となり，迅速さと業務への影響を最小化したインシデント対応が可能となる．

3.4　動的ネットワーク構成によるサイバー攻撃対策支援システム

本論文では，3.3 節で述べた 3 項目のサイバー攻撃対策支援手法を実現するサイバー攻撃対策支援システムを提案する．

3.4.1　システム構成

図 3.1 に，提案システムの構成図を示す．提案システムは，本論文が対象とする 3 項目のネットワーク管理者支援機能のそれぞれを実現するための三つのサブシステムおよび，各サブシステムからの結果を受けて実際にネットワークの設定を行う一つのモジュール，ネットワーク構成情報等保管のための一つのデータベースから成る．

ネットワーク内部分離設計システム（Network Separation）

ネットワーク内部分離設計の構築支援を実現するサブシステムである．初期のネットワーク構築時や，構成変更，人事移動の際などにこの機能を使用し，内部分離ネットワークの構築を行う．ネットワーク内のディレクトリサービスサーバから得られる人事情報とファイルへのアクセス権限情報および，ネットワーク内で観測されるトラフィックを用いて自動的に ACL（Access Control List，アクセス制御リスト）を生成する．また，ACL の生成の際にネットワーク構成データベースに保存された現在の ACL，ネットワークセグメントの一覧と IP アドレス，およびネットワークに接続されるすべての端末の一覧と IP アドレスを取得，利用する．最終的に，管理者の承認を得た上で生成した ACL をネットワーク構成データベースに登録するとともに，ネットワーク設定モジュールへと出力する．このシステムの詳細は第 4 章で説明する．

監視・解析管理支援システム（Detection and Analysis）

ネットワークの効率的な監視，解析管理によりインシデントの検知・状況判断支援を実現するサブシステムである．各ネットワークセグメントに対して，セグメント内端末のマルウェア感染疑いのレベルを表す ISL（Infection Suspicious Level）を設定し，巡回監視や集中監視を実施する．ISL の低い平常時は監視対象の管理を行い，一定時間ごとに新たな監視対象をネットワーク設定モジュールへと出力する．また，ネットワーク内の侵入検知システム等からアラートを受け取り，各セグメントの ISL の変更を行う．複数のアラートや緊急度の高いアラートによって危険度が高くなれば，巡回監視の頻度向上などの監視の強化に移行し，最終的に ISL が最も高くなった状態では，ネットワークから監視対象に関するミラーパケットを受け取り解析を行う．各セグメントに対応する ISL の状態は

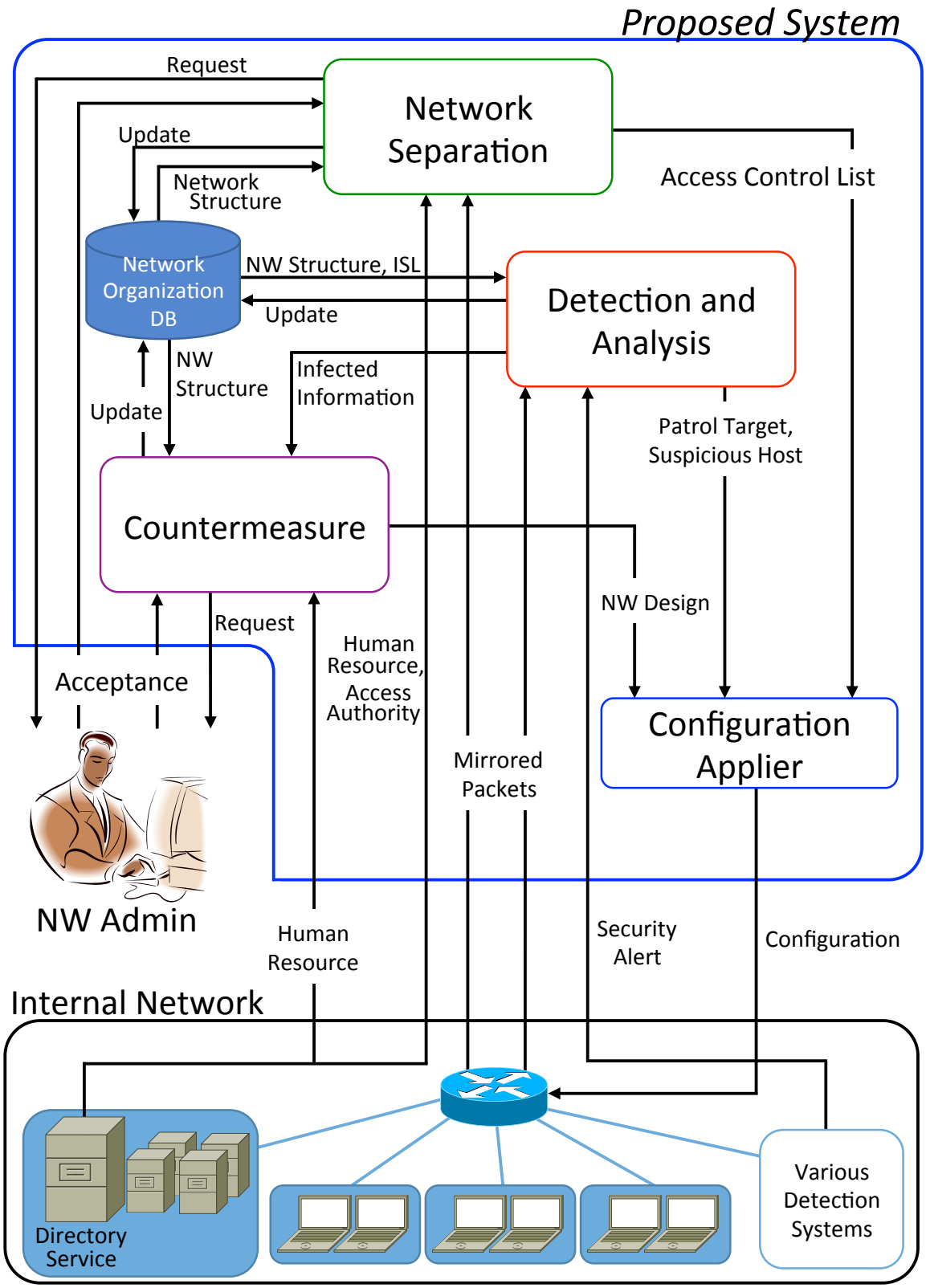

図 3.1　サイバー攻撃対策支援システム

ネットワーク構成データベースで管理し，アラートに応じてそれらを取得，更新する．また，感染が疑われる端末の一覧も同様にネットワーク構成データベースにて管理を行い，端末の解析を行う際には，この感染疑い端末の一覧を取得する．また，解析の結果に応じてネットワーク構成データベースを更新する．解析の結果からインシデントの状況判断を行い，インシデントの情報をインシデント対応支援システムへ出力する．このシステムの詳細は第 5 章で説明する．

インシデント対応支援システム（Countermeasure）

インシデント発生時に感染端末隔離等の対策設計適用支援を実現するためのサブシステムである．監視・解析支援システムから受け取った，感染端末情報や不審な通信状況などのインシデント情報と，ネットワーク構成データベースから取得するセグメントやネットワークに接続される機器の一覧および IP アドレス，各機器間の接続関係から成るネットワークの構成情報から，複数の対策設計候補を生成する．その上で，ネットワーク上のディレクトリサービスサーバから得られる人事情報などを基に各候補の評価を行う．評価結果を基にネットワーク管理者に適切な対策設計候補を推薦し，管理者が選択する対策設計候補を受け取ってネットワーク設定モジュールへと出力する．また，選択された設計の内容をネットワーク構成データベースに登録する．このシステムの詳細は第 6 章で説明する．

ネットワーク設定モジュール（Configuration Applier）

三つのサブシステムからのネットワーク設計や ACL などを受け取り，その内容をネットワークに反映させるためにネットワーク機器の設定を変更するためのモジュールである．設定を変更する対象機器として，ネットワークを構成するスイッチを想定している．

ネットワーク内の機器を自動的に設定する方法は様々なものが考えられる．例えば，従来から存在するネットワークの管理，設定プロトコルとして SNMP（Simple Network Management Protocol）[17] が存在する．SNMP はネットワーク機器からの設定情報の取得などによく用いられるが [18][19]，ネットワーク内の VLAN 管理を SNMP を用いて行っている手法も存在する [20].

SNMP は設定可能な項目が少ないことや，ネットワーク機器の機種依存などの問題が

あるが，今後の標準化によりこのような問題の解決が期待できるネットワーク機器設定プロトコルの NETCONF[21][22] なども存在する．

また昨今では，SDN（Software Defined Networking）と呼ばれるソフトウェアを用いたネットワーク制御の技術を利用した研究も盛んに行われている [23]．SDN 対応のスイッチでネットワークが構成されている場合には，それらの設定を変更する SDN コントローラとして本論文におけるネットワーク設定モジュールを実現することも可能である．

ネットワーク構成データベース（Network Organization DB）

ネットワーク構成情報等保管のためのデータベースである．ネットワークに接続された全てのクライアント端末とサーバ，ネットワーク機器の一覧と，それぞれの IP アドレスおよび MAC アドレスを保持する．クライアント端末については使用するユーザのアカウントも保持する．また，ネットワーク内のセグメントの一覧とネットワークアドレス，各端末間の接続関係，適用されているアクセス制御を保持する．それに加え，監視・解析管理支援システムが使用する ISL および，マルウェア感染の疑いがある端末の一覧もこのデータベースにおいて保持するものとする．

不正通信監視手法（Various Detection Systems）

本論文では，ネットワーク内通信監視の管理支援手法を提案するが，実際の通信の監視や解析は既存システムや提案されている手法を用いることを想定している．以下，本論文で想定するいくつかの監視手法を紹介する．

- 侵入検知システム

  2.3.1 節で述べたように，IDS は一般的に利用されるセキュリティ対策の一つである．Snort[24] などに代表される，パターンマッチングによる検知を行うシグネチャ型 IDS と，通信の振る舞いにより検知を行うアノマリ型 IDS の 2 種類がある．
- DNS クエリによる検知

  DNS クエリを用いた攻撃検知に関して，様々な研究が行われている [25][26][27]．DNS クエリを用いた検知手法の例として，図 3.2 に示すように，ブラックリストとして C&C サーバ等の悪意ある通信先の IP アドレスとホスト名のデータベースをあらかじめ用意する手法がある．検知を行うシステムは内部ネットワーク上の

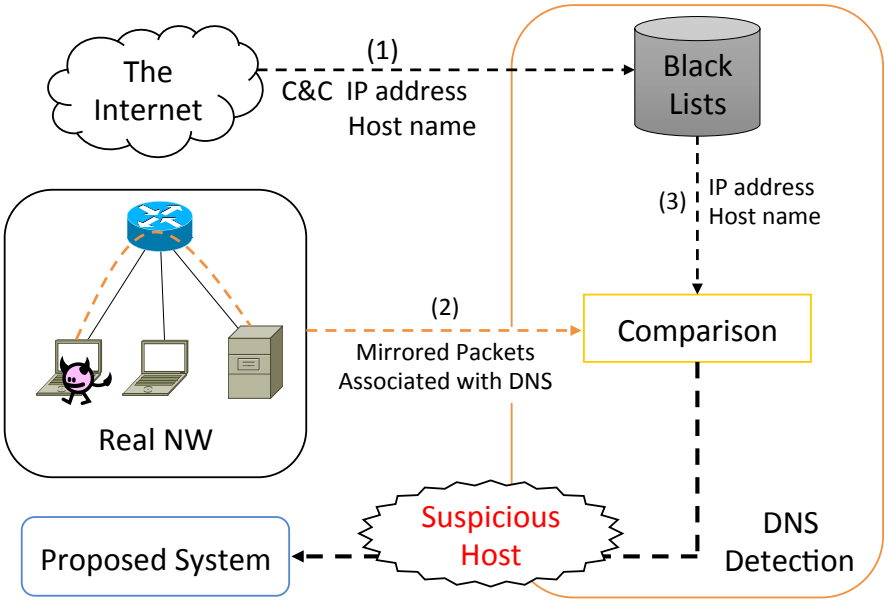

図 3.2　DNS 検知機構の例

DNS クエリに関連するパケットを収集し，それらの IP アドレスとホスト名をデータベース上のブラックリストと比較する．これにより，悪意ある通信先に接続を試みた感染端末を検知可能である．ただし，昨今の C&C サーバは正規のサーバを乗っ取って構築され，攻撃ごとに何台もの C&C サーバが用意される場合が多く，IP アドレスが短期間で変化してしまう可能性もある．そのため，ブラックリストの更新が困難であるという問題点が存在する．

- ネットワーク機器のログ

  ネットワークを構成するネットワーク機器のログは，ネットワークの故障検知 [28] やフォレンジック [29] など様々な活用がされており，重要な役割をはたしている．これを活用することにより不正侵入の検知に役立てるための研究も行われている [30][31]．また，IPA による「新しいタイプの攻撃」の対策に向けた設計・運用ガイド [2] においても，ファイアウォールのログから，ファイアウォールが遮断した通信を発生させた機器を特定するといった手法が紹介されている．本論文で構築するネットワーク内部分離設計が施された細かいアクセス制御が行われているネットワークにおいては，禁止された通信区間において活動を試みる端末を検知することが可能である．

3.4.2　ネットワーク管理者による承認手続き

提案システムでは，ネットワークの再構成を行う際には，必ずネットワーク管理者による承認手続きを経る設計としている．これは，機械的にネットワーク内にアクセス制御を追加することによって非常に重要な通信を遮断しないために，管理者に確認をさせた方が好ましいためである．また，インシデント対応には経営判断などシステム的には扱えない情報も影響するため，必ずしも一つの対策が適切であると定義することはできず，管理者による選択が必要と考えるためである．ただし，ネットワーク監視・解析管理支援システムにおける監視対象セグメントの切り替えスケジューリングなどの再構成では，ネットワーク内で行われている通信に対して直接影響を及ぼすような再構成を伴わないため，管理者の承認手続きを行わないこととした．

ネットワーク管理者に対してアクセス制御の内容やインシデントへの対策設計の内容を通知する手段は様々なものが考えられる．本論文において実装したシステムでは，第 4 章および第 6 章において詳細は後述するが，Web ブラウザを用いてアクセスするインターフェイスにおいて，アクセス制御一覧の文字列表示や，対策設計のイメージ図の表示などを行う簡易的なものである．本論文では，提案システムの検討段階においてネットワーク管理演習支援システム LiNeS[32] を用いて仮想ネットワーク環境をネットワーク管理者へ提示するモジュールの試作を行った．ネットワークの規模が大きくなった際の仮想端末の台数増大が問題とはなるが，システムによる変更後のネットワークの状態を仮想的にグラフィック表示可能であり，また各仮想端末の簡易的な操作により疎通確認なども行えるため，変更内容をネットワーク管理者により直感的に伝えるという点では有効な手段である．ユーザインターフェイスに関しては本論文の対象外であるが，上記の例のように様々な方法が考えられるため，検討の余地がある．

3.5　本章のまとめ

本論文では，サイバー攻撃の事前対策から事後対応までの包括的な対策支援を行う，動的ネットワーク構成によるサイバー攻撃対策支援システムを提案する．提案システムは，動的ネットワーク構成を用いることにより，攻撃の影響を受けづらいネットワークの構

築，ネットワーク内の効率的な監視および不正通信の解析，インシデント時の迅速な対策のそれぞれの問題点を解決し，ネットワーク管理者の支援を行うことによりこれらの 3 項目を容易に行うことを可能とするものである．次章以降，本論文において提案する 3 項目のネットワーク管理者支援手法に関して，サイバー攻撃対策支援システムのサブシステムとして各手法を実現する方法について述べる．

第 4 章

ネットワーク内部分離設計構築支援

4.1　まえがき

2.3.1 節でも述べたように，標的型サイバー攻撃の被害が深刻化する，もしくは対策が行い難い原因の一つとして，一般的に用いられる組織内ネットワークのフラット構造が挙げられる．この構造においては，組織内の全ての端末が互いに通信可能な状態にあるため，1 台の端末がマルウェアに感染してしまえば，マルウェアの侵食活動によりネットワーク内で感染被害が拡大していくことになる．加えて，ネットワーク内の全ての端末が容易にマルウェアに感染してしまう状態であり，またネットワーク内全体の膨大なトラフィックの中からマルウェアが活動を行った通信の形跡を見つけ出すことは困難な作業であるため，マルウェアの感染状況や攻撃の全貌把握を行うことが難しい．これに対して　本論文では，マルウェアによる不正通信抑制やその検知が比較的行い易く，標的型サイバー攻撃に対する有効な対策手法の一つである，組織内部ネットワークにおけるネットワーク内部分離設計に着目する．ネットワーク内部分離設計は効果的な手法の一つではあるが，構築が困難なために一般的な組織内ネットワークに用いられることは少ない．本章では，ネットワーク内部分離設計の構築の支援手法について述べ，ネットワーク内部分離設計の構築が困難という問題を解決する．

4.2　ネットワーク内部分離設計の概要と問題点

ネットワーク内部分離設計（以下，内部分離設計）とは，組織内部のネットワークを複数のセグメントに分割し，ネットワーク内の通信に対して緻密なアクセス制御を行う手法である．必要のない通信区間のアクセスをアクセス制御によって禁止しておくことにより，ネットワーク内でマルウェアが行う調査活動や感染拡大活動などの不正通信を抑制可

能となる．また，アクセス制御によって禁止された通信区間において組織内に侵入したマルウェアが通信を試みた場合，ネットワーク機器のログから遮断した通信の送信元 IP アドレス，宛先 IP アドレスなどを調査することでマルウェア検知の可能性が高まる．感染が発覚した場合には，特定の範囲の通信遮断など，感染端末の効率的な切り離しが可能となる [5]．

内部分離設計は，ネットワーク監視の観点からも有効な手段であると言える．組織内ネットワークの入口における不正通信の監視，遮断は一般的に行われる．一方で，一つのセグメントで構成されたネットワーク全体のトラフィックを常時監視するには，非常にコストがかかる．ネットワークの規模が大きくなるほどこのコストは増大するため，大規模なネットワークにおいては莫大なコストが必要となり現実的ではない．それに対し，内部分離設計が適用されたネットワークにおいては，ネットワークを複数のセグメントに分割してグループ化し，そのグループを周期的に切り替えて監視する巡回監視を適用することができる．これにより，監視対象となるトラフィック量が低減され，監視コストの削減が可能となる．また，前述のようにアクセス制御によって禁止された通信区間において通信を行おうとする端末を重点的に監視することで，マルウェアの検知も行い易くなる．

本来であれば，ネットワークの初期構築時から内部分離設計のようなセキュリティを意識した設計を行うべきである [33]．しかしながら，内部分離設計はその構築や管理が困難であるという問題点がある．内部分離設計を構築するためには，組織内ネットワークをどのような基準で分割するかを決定した上で，各セグメントごとにどのような通信が必要であるかを詳細に検討しなければならない．これを行うためには，ネットワーク構成のみならず，人事情報，各個人の業務内容，業務内容に応じて必要な通信内容等，組織内のあらゆる情報が必要となる．それに加え，組織における業務は時間とともに変化するので，初期設定のまま運用できるネットワークは稀であり，内部分離設計も常に最新の業務内容を意識した保守が必要となる．ネットワーク管理者のみでこれらの全ての情報を収集し，検討することは困難である．

また，ネットワークの分割とアクセス制御によりネットワークの構成が複雑となるため，ネットワーク機器の設定も複雑となり，ネットワーク構築時に設定ミスを引き起こす可能性もある．緻密なアクセス制御を行う内部分離設計においては，このような設定ミスにより事前の設計と異なるネットワークを構築してしまうことはネットワーク運用管理

に致命的な影響を与える可能性もある．例えば，業務上必要な通信区間を誤って制限してしまった場合には，必要な通信が行えなくなってしまう．また，冗長な ACL を作成してしまった場合には，ネットワーク機器の負荷が大きくなる可能性もある [34]．このような問題点から，内部分離設計は一般的な組織内ネットワークに導入されるケースは少ない．実際に運用されている例として，京都大学のキャンパスネットワークが挙げられるが，20000 ポート，4000VLAN という大規模な運用が行われており，ネットワーク管理者にとってその管理運用は大きな負担となっている [35]．

4.3 関連手法

VLAN の構築や管理に関しては様々な研究や製品が存在する．VLAN 構築の研究の一例として，トラフィック量に着目した VLAN 構築手法 [36] などがある．また，VLAN 管理の研究の一例として，複雑な構成の VLAN を管理する手法 [20]，セキュリティポリシの異なる複数の VLAN を用意し端末の接続先を切り替える手法 [37] など，様々な研究が行われている．VLAN を自動的に設計し実ネットワークへの構築が可能な製品の例として，VLAN .Config[38] などが挙げられる．

しかしながら，全ての VLAN 間における緻密なアクセス制限を自動的に構築することは既存の技術では難しい．文献 [36] において渡邊らは，トラフィックを用いて動的に VLAN を構成している．初期状態では全ての端末が同じデフォルト VLAN に属させた後に，マルチキャスト通信を行う端末は同じマルチキャストグループで一つの VLAN を構成し，ユニキャスト通信を行う端末はトラフィック量が一定の値を超えた端末同士で新たな VLAN を構成する仕組みである．トラフィック量の集計は一定時間ごとに行われ，トラフィック量が一定の値を下回った場合に VLAN を削除し端末をデフォルト VLAN に移動させるオペレーションなども行う．この手法では，通信量の多い端末同士を効率的にグルーピング可能であるが，トラフィック量が一定の値を超えない場合には，通信の必要性が高い端末同士であっても，デフォルト VLAN や別 VLAN に配置されてしまう可能性がある．そのため，マルウェア感染端末がデフォルト VLAN に属している状態で，少量のトラフィックのみを発生させ活動を行っている場合に，デフォルト VLAN に属す他の全ての端末が危険な状態となる．また，端末間のトラフィック量に応じて新たな VLAN を構成するこの手法の場合，別々の VLAN に配置された端末同士でも通信が発生する可

能性があり，全ての端末間の通信も把握する必要がある．つまり，VLAN 間ルーティングにより全ての VLAN 間で通信が行える状態でなければならない．これは，VLAN により内部分離が行われていても，他の VLAN の端末同士が通信可能な状態であるため，マルウェアが行う不正通信の防止は行えていない状態である．

内部分離設計を実現可能なネットワーク管理手法について，いくつかの提案が行われている．Nayak らは Resonance と呼ばれる組織内ネットワーク向けアクセス制御フレームワークを提案し，ジョージア工科大学で実運用を試みた [39]．これは，ネットワークに接続された端末は一旦未認証端末用 VLAN に入れ，認証された後に正規の接続先 VLAN に入れる動作を行うものである．通信の可否は lattice-base のアクセス制御をもととした動的ポリシーで制限される．また，接続された端末のリアルタイム監査を行い，端末に既存のセキュリティ上の問題が存在する場合には，端末を隔離 VLAN に隔離する機能も実現している．しかしながら，Resonance のアクセス制御では端末をどの VLAN に所属させるかという程度であり，端末を利用するユーザの属性やサーバ側から見たアクセス権限などは考慮されていない．

Gude らは NOX と呼ばれる大規模ネットワークを管理するためのネットワークオペレーティングシステムを提案している [40]．NOX では Python ライクなプログラミングモデルでユーザごとに異なる VLAN の割り当てやポートスキャン検知などが可能である．しかしながら，NOX はあくまでもプログラミングを可能とする基盤であり，アクセス制御のための ACL の投入などを行うためには新たに大規模なプログラミングを行う必要がある．

Cabuk らは Trusted Virtual Domain(TVD) 分割に基づくネットワーク分離設計，および，TVD 内外のセキュリティポリシの設定を可能とするフレームワークを提案している [41]．提案では，TVD 間の通信の可否を含めたフロー制御について，TVD 分離ポリシ，ネットワークポリシ，ストレージポリシ，端末に結び付けられたユーザなどの入力から TVD 間および TVD 内の仮想マシン間の ACL を生成し投入する．しかしながら，提案はデータセンタを指向した内容であるために設定内容が多く複雑であり，管理者にも高い技能を要求し，なおかつ，管理コストも高くなると考えられる．

橋本らは Openflow と認証基盤の連携によるアクセス制御手法を提案している [42]．提案では，ユーザの認証情報に応じて登録された正規のユーザのみをネットワーク内の Web

コンテンツへアクセス可能とする制御を行っている．しかしながら，ユーザの認証情報のみでは多数のファイルサーバが存在する環境におけるユーザごとに必要な通信の判断が困難であり，細かいアクセス制御の生成は難しいと考えられる．

4.4　ファイルアクセス権を用いた内部分離設計の構築

4.3 節で述べたように，ネットワークにおいて VLAN の構築は既存の手法や製品を用いて行うことが可能である．実際に，部署などを基準にして企業内ネットワークを大まかに分割して運用しているケースも多く存在する．しかしながら，内部分離設計では，分割されたセグメント間もしくは各端末間の適切なアクセス制御が重要であるため，既存の手法を用いて VLAN のみを構築した場合や一般的な運用形態では適切な内部分離設計が運用されているとは言い難い．また，ACL を正しく投入するためには包含関係や入力順を含めた ACL 入力などのプログラミング要素が含まれる点や細かいセキュリティポリシの入力など，高度な技術が要求される．そこで本論文では，ネットワーク内のユーザのファイルへのアクセス権限を用いてアクセス制御を自動的に生成しネットワーク機器に設定する動的ネットワーク構成により，内部分離設計が適用されたネットワークを構成する．これにより，管理者による細かい情報の入力や，機器の設定などの手間をかけず，容易に内部分離設計の構築を可能とする．また，内部分離設計の構築後において，ファイルアクセス権の追加や人事異動などによる ACL の変更が発生する場合にも，動的ネットワーク構成を用いることで，新たな内部分離設計を容易に適用することが可能である．

4.4.1　アクセス制御の構築基準

ネットワーク内でアクセス制御を行うためにはまずその基準を決定しなければならない．例えば，組織内の業務内容や各業務において必要な情報，ネットワーク内での情報の流れなどをネットワーク管理者が用意する．これらの情報を基準に不必要な通信区間を算出することが可能である．しかしながら，適切なアクセス制御を行うためには，前述したような組織内の情報を漏れなく用意する必要があり，その情報収集，入力は非常に手間のかかる作業となる．

そこで本論文では，アクセス制御のための基準としてユーザのファイルへのアクセス権

限を利用する．例として，図 4.1 の Server1 および Server2 を挙げる．Server1 には役職

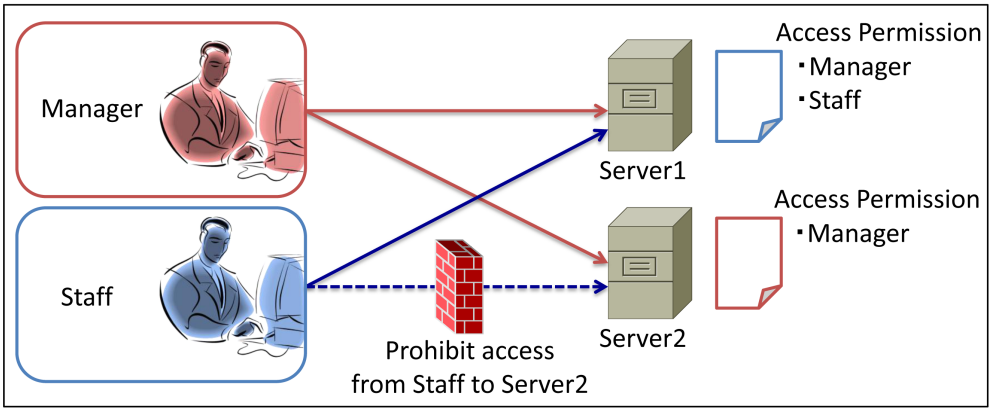

図 4.1　アクセス権限の例

が部長（Manager）の社員と従業員（Staff）の社員がアクセス可能なファイルが存在する．そのため，部長も従業員も Server1 に対しては通信可能でなければならない．それに対し，Server2 には部長がアクセス可能なファイルのみが存在する．この場合，Server2 に対しては部長のみが通信可能な状態であればよく，従業員からサーバ 2 に対する通信は必要ではない．よって，アクセス制御として従業員から Server2 に対するアクセスを禁止するというものとなる．

4.4.2　アクセス権限の取得とアクセス制御の生成

実際に運用中の組織内ネットワークにおいては，図 4.1 の例のように役職のみを基準にアクセス権限を設定するといった単純な場合のみならず，所属，業務内容，参加プロジェクトなどあらゆる内容に応じたアクセス権限が設定されるため，非常に複雑かつ多様となる．そのため，一つ一つのディレクトリごとに細かくアクセス権限を設定することは困難であり，一般的にネットワーク内に設置されたディレクトリサービスサーバを用いて一元的に管理・運用される場合が多い．そこで本論文では，ディレクトリサービスサーバからこれらのアクセス権限情報を取得することにより，ネットワーク管理者による情報入力等の手間をかけずアクセス制御の基準となる情報を利用することが可能となる．

4.5　内部分離設計生成手法

本論文では，内部分離設計を構築するため企業内ネットワークを VLAN により細かく細分化していき，各 VLAN 間のアクセス制御を行う手法を検討した．この手法では，ネットワーク内のディレクトリサービスサーバより取得する情報を基にネットワークを細かく分割した上で，分割されたネットワークにおけるネットワークトラフィックを用いて不必要な通信可能区間を判別し，アクセス制御の追加を行う．このようなネットワークの細分化，アクセス制御の追加を繰り返しネットワークに適用する動的ネットワーク構成を行うことにより，徐々にネットワークのセキュリティレベルを向上させることが可能となる．

4.5.1　内部分離設計生成手法の構成

内部分離設計生成手法の構成を図 4.2 に示す．内部分離設計生成手法は，3.4 節で述べたシステムのネットワーク設定モジュールおよびネットワーク構成データベース以外に，以下のモジュールおよびデータベースから成る．

- ネットワーク設計生成モジュール（Network Design Generation Module）
- 人事情報取得モジュール（Get-HRI Module）
- 抽出モジュール（Extraction Module）
- 人事情報データベース（Human Information DB）
- トラフィック統計データベース（Traffic DB）

ネットワーク設計生成モジュールは内部分離設計生成手法の主な機能となるネットワークセパレーティング，ネットワークリファインメント，ネットワークリコンストラクションの三つの機能を有する．それぞれ，ネットワーク内においてディレクトリサービスからのデータ取得および，ネットワーク機器からのトラフィック収集，機器設定を行う．

4.5.2　ネットワーク内のデータ取得

内部分離設計生成手法では，3.4 節で述べたシステムのネットワーク構成データベースからネットワークの構成情報を取得する．それに加え，人事情報データベースおよびトラ

フィック統計データベースにおいてネットワークから取得する人事情報およびトラフィック統計情報を保持する．

ネットワーク構成データベースからは，ネットワークアドレスの一覧，ユーザ端末の一覧と使用者アカウント，IP アドレス，サーバ端末の一覧と IP アドレス，アクセス制御の一覧を取得する．

人事情報データベースは，従業員に関する情報として各従業員の所属，役職，ユーザアカウントおよび，共有ファイルへのアクセスルールを保持する．これらの情報はディレク

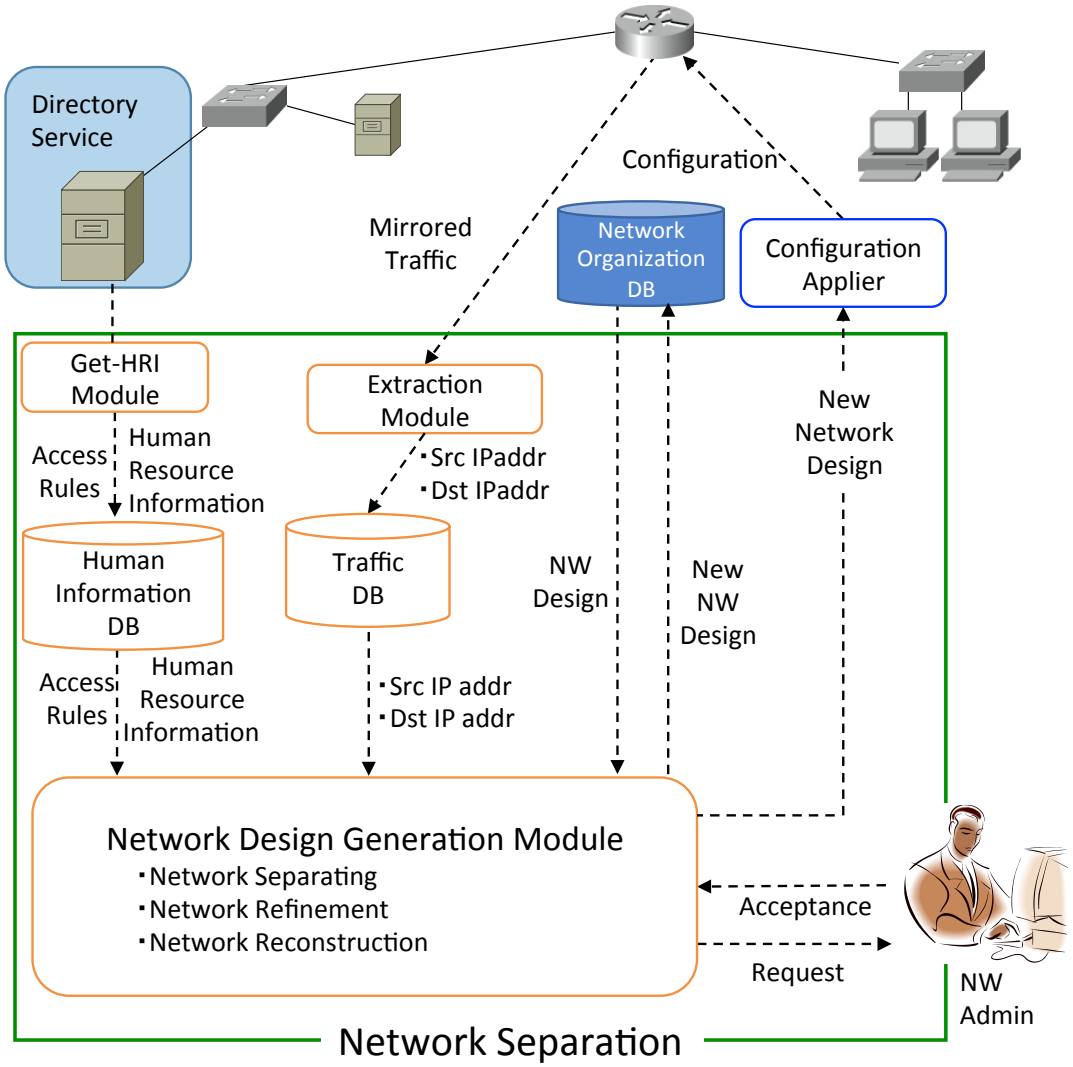

図 4.2　内部分離設計生成手法

トリサービスサーバにおいて管理されており，人事情報取得モジュールがディレクトリサービスサーバより取得する．アクセスルールに関しては，4.5.4 節にて後述する．

トラフィック統計データベースは，ネットワーク内の機器から取得したミラートラフィックから抽出モジュールが抽出した送信元 IP アドレス，宛先 IP アドレスをトラフィック統計情報として保持する．

4.5.3 ネットワークセパレーティング

この機能では，はじめにネットワークを部署ごとに大まかに分割し，分割されたネットワーク内で不必要な通信区間を特定しアクセス制御を行う．ネットワークセパレーティング処理を行うモジュールの構成を図 4.3 に示す．

部署によるネットワーク分割

ネットワーク分割コンポーネント（Network Separating）が人事情報データベースより，各ユーザのアカウントと所属を取得する．また，ネットワーク構成データベースより，現在のセグメントのネットワークアドレスの一覧，端末とその使用者アカウントの一覧を取得する．取得した情報から，部署ごとにセグメントを作成し，異なるネットワークアドレスを割り当てる．その後，各ユーザの使用端末について，各端末がどのセグメントに属するか決定し，IP アドレスを割り当てる．

それに加え，ネットワーク内のサーバ端末についてはサーバ用セグメントにまとめて配置する．ネットワーク構成データベースからサーバの一覧を取得し，それぞれにサーバセグメントの IP アドレスを割り当てる．

これらの変更内容についてネットワーク管理者に対して適用の可否の確認を行い，許可を受ける．その後，ネットワーク構成データベースが保持しているネットワークアドレスの一覧に作成した各部署のネットワークアドレスを追加する．また，各ユーザのアカウントと紐付けされた端末の所属先ネットワークおよび IP アドレスの情報を更新する．各サーバ端末についても，割り当てた IP アドレス情報を更新する．ネットワーク構成データベースの更新内容と同様の内容をネットワーク設定モジュールへと通知し，ネットワーク設定モジュールがネットワーク機器に反映させる．端末やサーバの IP アドレスについては，手動で切り替えを行うか，DHCP サーバなどを用いて MAC アドレスベースに IP

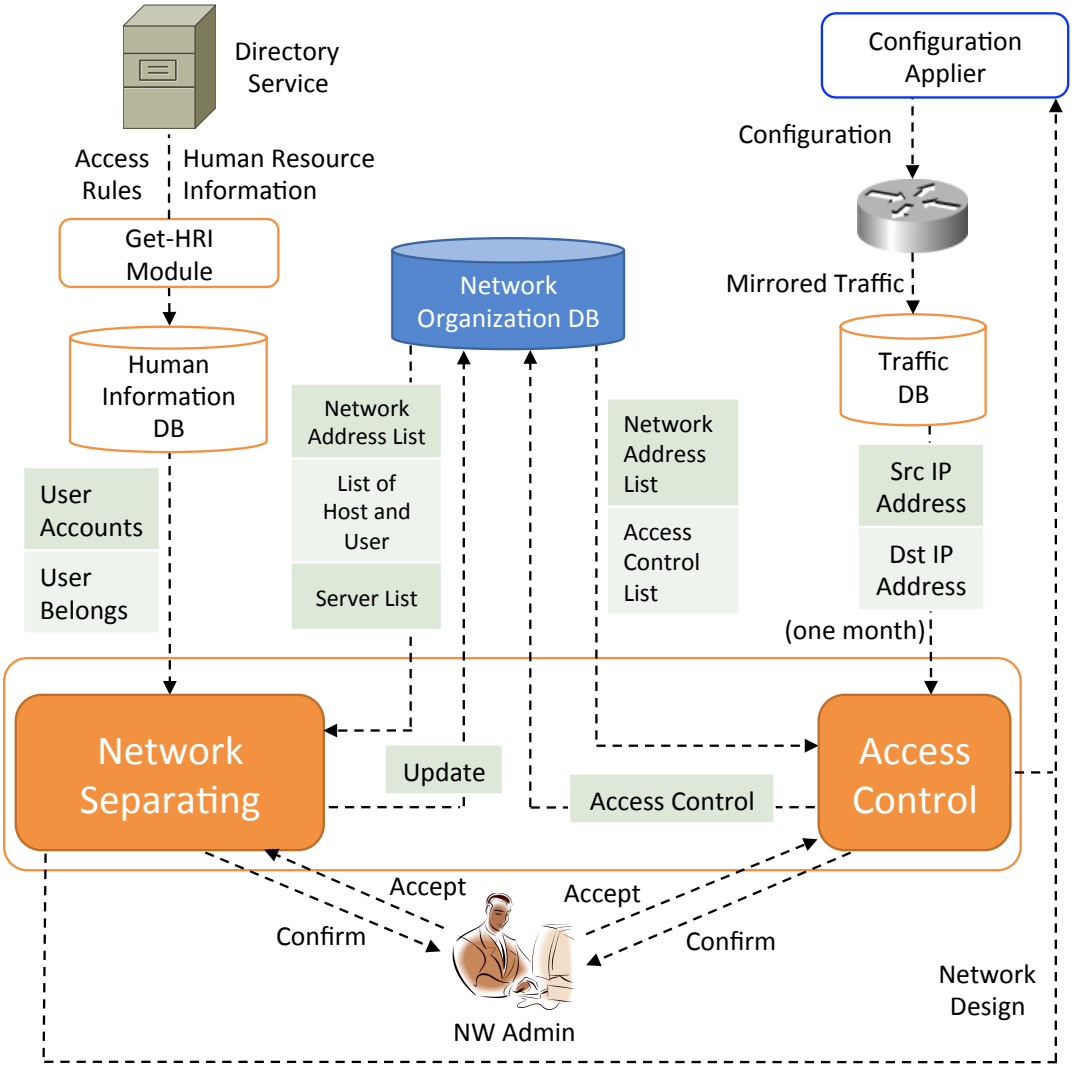

図 4.3　ネットワークセパレーティング

アドレスを更新する必要がある．ただし，後者の場合においては各端末の IP アドレスは即座に変更されないため，各端末上で割り当てられている IP アドレスの解放を行うなどの必要がある．

アクセス制御

分割されたネットワークにおけるトラフィックを収集し，それらを基にセグメント間の不必要な通信可能区間を特定し，アクセス制御を行う．アクセス制御コンポーネントがト

ラフィック統計データベースから，ネットワーク分割後 1 ヶ月等の一定の長期間の送信元 IP アドレス，宛先 IP アドレスを取得する．また，ネットワーク構成データベースからネットワークアドレスの一覧と，現在適用されているアクセス制御の一覧を取得する．取得した情報を用いて，同一セグメントの端末同士の通信，セグメント内でのブロードキャスト，外部ネットワークとの通信を排除し，セグメントを跨ぐ通信のみを抽出する．抽出した結果から，アクセスが許可されているにもかかわらずトラフィックが観測されない区間を特定し，不必要な通信可能区間の候補として管理者に通知する．管理者の許可を得た後，その区間の通信を遮断するアクセス制御をネットワーク構成データベースに登録すると共に，ネットワーク設定モジュールによりネットワーク装置に設定を投入する．

4.5.4 ネットワークリファインメント

ネットワークセパレーティングにより部署ごとのネットワーク分割およびアクセス制御を行った後，より細かくネットワーク分割を行い，アクセス制御を追加するのがネットワークリファインメントである．ネットワークリファインメントでは，以下に述べるネットワークの細分化とアクセス制御の追加を行う．この二つの工程を繰り返し行うことにより，ネットワークの内部分離を徐々に細かくしていくことが可能となる．これに伴い，ネットワークのセキュリティレベルを向上させることが可能となる．

アクセス権限によるネットワークの細分化

ネットワークをより細かく分割するため，人事情報データベースが保持するアクセスルールを利用する．Active Directory などのディレクトリサービスサーバでは，ダイナミックアクセス制御機能による共有フォルダなどのリソースへのアクセス制御が可能である．アクセス制御の適用方法は 2 段階で実施する．まず，ユーザの属性値（例えば，所属＝経理部，役職＝部長）に応じたアクセス権限（例えばフルコントロールアクセス可能）をアクセスルールとして定義する．その上で，リソースに対してディレクトリサービスサーバ上の適切なアクセスルールを選択する．前述の例のようなアクセスルールが選択されたリソースに対しては，経理部，部長という属性を持つユーザのみがフルコントロールアクセス可能となる．このアクセスルールはディレクトリサービスサーバが管理するため，これらを人事情報取得モジュールが取得し，人事情報データベースにおいて保持する．

内部分割を行ったネットワークに対し，さらにアクセスルールを用いて，ネットワークをより細かく分割する．1 回の分割につき一つのアクセスルールを使用し，分割を試みるセグメント内において属性値によりアクセスルールが適用されるユーザとされないユーザに分類されるかどうかを判定する．例えば先述の例のように，経理部という部署属性と部長という役職属性を使用したアクセスルールの場合，経理部のセグメント内においてこのルールが適用される部長属性を持つユーザと，ルールが適用されないそれ以外のユーザに分類できるはずである．このような場合に，この分類によってセグメントを分割する．

アクセス制御の適用

ネットワークの細分化を行った後，細分化を行う以前の一つのセグメントに対して適用されていたアクセス制御をネットワーク構成データベースから取得し，同じアクセス制御を細分化されたそれぞれのセグメントに対して適用する．それに加え，ネットワークセパレーティングと同様に，1 ヶ月等の長期間のミラートラフィックから送信元/宛先 IP アドレスをトラフィック統計データベースに蓄積する．この情報を用いて，長期間通信が行われない区間を不必要な通信可能区間の候補として抽出し，管理者の判断によりアクセス制御を追加適用する．

ただし，アクセス制御について変更が行われない場合が存在する．例えば，前述の例のように経理部内で役職属性を用いるアクセスルールにより，部長属性を持つユーザとそれ以外のユーザを異なるセグメントに分割したとする．この場合，このアクセスルールを適用したリソースと，以前より経理部のユーザが利用していたリソースが経理部の一つのサーバ内に格納されている場合などは，分割された二つのセグメントは共にこの一つのサーバを利用するため，新たにアクセスを遮断する区間は存在しない．このような場合には，このネットワーク分割を解除する．

実行例

ネットワークリファインメントの実行例を図 4.4 に示す．営業部には 1 人の部長（Manager）と 2 人の従業員（Staff）が所属し，サーバセグメント内に営業部が使用するサーバが 2 台設置されている．この時，営業部サーバ A の共有フォルダには，所属が営業部のユーザにフルアクセスコントロールを許可するアクセスルールが設定されているも

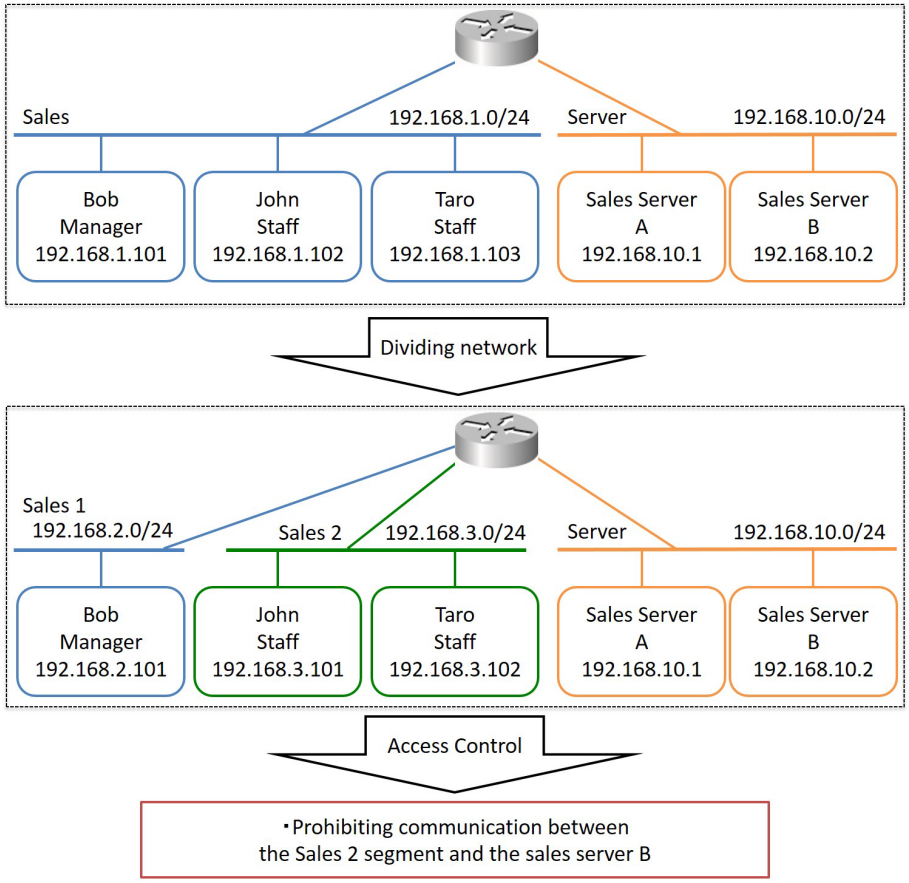

図 4.4　ネットワークリファインメントの実行例

のとする．また，営業部サーバ B の共有フォルダには，所属が営業部かつ役職が部長のユーザにフルアクセスコントロールを許可するアクセスルールが設定されているものとする．この場合，営業部サーバ A に適用されているアクセスルールは，営業部のユーザ全員に適用されるため，ネットワークリファインメントでは適用されない．営業部サーバ B に適用されているアクセスルールでは，役職に応じたアクセス権が与えられているため，営業部内でアクセス可能なユーザとそうでないユーザが存在することとなる．そこで，営業部セグメントを部長が属するセグメントと，それ以外が属するセグメントに細分化が行われる．

次に，細分化が行われたネットワークにおいて，ミラートラフィックの収集を長期間を行う．その結果，営業部 1 セグメントからは営業部サーバ A と営業部サーバ B のそれぞれに対してアクセスが存在するのに対して，営業部 2 セグメントからは営業部サーバ A

にのみアクセスが存在する．そこで，営業部 2 セグメントから営業部サーバ B への通信を不必要な通信可能区間の候補としてネットワーク管理者に確認し，許可を得た後にアクセス制御を追加する．

4.5.5　ネットワークリコンストラクション

人事異動や，社員の入社などによりネットワークの構成が変更された際には，ネットワークリコンストラクションを行う．ネットワーク管理者の変更通知を受け，現在の人事情報データベースに登録されているユーザアカウントとそれぞれの所属，役職を取得する．その後，人事情報取得モジュールを用いて，ディレクトリサービスサーバ上の情報の読み出しにより人事情報データベースを更新する．その上で再度人事情報データベースからユーザアカウントとそれぞれの所属，役職を取得し，変更箇所を特定する．以下のように新たに配置されたユーザの種別に応じた変更を行う．

- ユーザが他の部署より異動した場合

  引き継ぎ等のため，新たなユーザが以前に所属していた部署や使用していたサーバと通信を行う可能性がある．そのため，新たなセグメントを作成し，新たなユーザはこのセグメントに配置する．その上で，このセグメントへのアクセス制御として，移動先部署内で新たなユーザと同等の役職のユーザが所属するセグメントと同様のアクセス制御を設定し，さらにこのユーザが以前所属していたセグメントで許可されていた通信を可能とするようにアクセス制御を追加する．

  最終的には，移動先部署内の同等の役職のユーザが所属するセグメントに再配置し，新たに作成したセグメントは削除する必要がある．この基準としては，1 ヶ月後などの期間の設定，管理者による通知，トラフィックの分析により一定期間通信がない場合などが考えられる．

  また，ユーザが以前に所属していたセグメントについては，そのユーザが単独で分割されていた場合には当該セグメントを削除し，それ以外の場合には変更は行わない．
- 新入社員などの新規ユーザの場合

  新規のユーザの場合には，配置された部署内において存在するセグメントにユーザ

を配置する．配置するセグメントは，部署内において最も役職が低いユーザが属するセグメントとする．また，このセグメントのアクセス制御は変更しない．

4.5.6 問題点

内部分離設計生成手法により内部分離設計の構築が容易化した．一方，問題点として，過度なネットワーク細分化によって，ネットワーク管理がより複雑になってしまうという副作用が存在する．内部分離設計生成手法では，ネットワークリファインメント機能によって可能な限りネットワークを細分化していく．不慣れな管理者ではシステム側の提案を際限なく承認し，ネットワークが必要以上に細かく分割されてしまい，大量のセグメントが乱立する可能性が考えられる．例えば，極端な例としてネットワーク内の全ての端末が異なるセグメントに属するまで細分化されてしまった場合，全ての端末間の通信を細かく管理するために大量のアクセス制御が必要となってしまう．アクセス制御の種類があまりにも多すぎると，ネットワークを構成するルータやスイッチの負荷も大きくなってしまい，パケットのルータやスイッチの通過時間が延びることとなる [34]．また，ネットワークの細分化の際に必要な各端末の IP アドレスの変更も，管理運用を複雑化する要因となってしまう．

4.6 ディレクトリサービス情報とトラフィックデータによる ACL 自動生成システム

4.5 節で検討した内部分離設計生成手法の問題点を改善した手法として，ディレクトリサービス情報とトラフィックデータによる ACL 自動生成システムを提案する．提案する ACL 自動生成システムでは，内部分離設計生成手法と同様にディレクトリサービスサーバ上のアクセス権限情報および，ネットワーク上のトラフィックを利用して ACL を生成し，動的ネットワーク構成を用いてネットワークに適用する．この際，ACL 自動生成システムはネットワークの分割は行わず，既存のネットワークに対するアクセス制御の追加を行うため，4.5.4 節で述べたネットワークリファインメントを行わないため，ネットワークの細分化の問題を緩和できる．

4.6.1　アクセス制御の生成

4.5 節の内部分離設計生成手法においては，ディレクトリサービスから得られたアクセス権限情報をネットワーク細分化のために利用し，ネットワークトラフィックを分割されたネットワーク間のアクセス制御を生成するために用いていた．一方，ACL 自動生成システムにおいてはネットワークの細分化は行わず，アクセス権限情報をネットワークセグメント単位もしくは端末単位のアクセス制御の生成のために利用し，ネットワークトラフィックの実績とネットワーク管理者の判断により生成したアクセス制御を適用するか否かを決定する方式とした．

すべてのアクセス権限情報をディレクトリサービスサーバから取得し，ネットワーク内の各端末ごとに図 4.1 の例のように不必要な通信区間を算出し，アクセス禁止候補とする．アクセス禁止候補は，ネットワーク内のある端末の IP アドレスと，その端末が通信する必要のないサーバなどの端末の IP アドレスの組とする．この際，アクセス権限情報を基に生成されるアクセス禁止候補は，アクセス権限が設定されたファイルやディレクトリが保存されたサーバ端末等と，それらを使用するユーザ端末との間で不必要な通信区間を算出したもののみである．これに対し，異なるセグメント同士の通信を禁止するというアクセス制限をアクセス禁止候補に追加する．これは，異なる部署間でそれぞれのセグメントに属する端末等が直接通信を行うケースは一般的な組織内ネットワークでは少なく，あらかじめ分割されているセグメント間の通信は不必要と考えられるためである．

一般的に，ACL の表記は 2 種類の方法がある．一方は，基本的に全ての通信を禁止した上で，必要な通信区間の通信を許可を追加する．もう一方は，全ての通信を許可した上で，不必要な通信区間の通信を禁止するものである．ACL 自動生成システムはどちらの場合にも適用可能であるが，本論文では後者の場合について述べている．

4.6.2　アクセス制御の選定

4.6.1 節において，アクセス権限の有無により不必要な通信区間を算出し，アクセス禁止候補を生成した．しかしながら，企業内におけるコンピュータ端末の使用用途は非常に多様であり，サーバ内ディレクトリへのアクセス権限の有無だけで一概に通信が不必要で

あるとは言えない．例えば，企業内で運用されている独自アプリケーションなどが端末間の直接通信を必要とした場合，先述のアクセス禁止候補をそのまま適用してしまってはアプリケーションが使用不可となってしまう．

そこで，アクセス禁止候補のうちで真に不必要な候補を特定するため，内部分離設計生成手法と同様にネットワークトラフィックを利用する．まず，運用中の組織内ネットワークにおいて，一定時間トラフィックを収集する．収集したトラフィックから送信元 IP アドレスと宛先 IP アドレスを抽出し，通信が存在する区間はアクセス禁止候補から除外する．これにより，除外されなかったアクセス禁止候補を，端末がサーバ内ディレクトリへのアクセス権限を持たないかつ実際に通信が存在していない真に不必要な通信区間とする．最終的に，アクセス禁止候補をネットワーク管理者の承認を得た上で ACL としてネットワークに適用する．

4.6.3　システム構成

図 4.5 に ACL 自動生成システムの構成図を示す．ACL 自動生成システムは，五つのモ

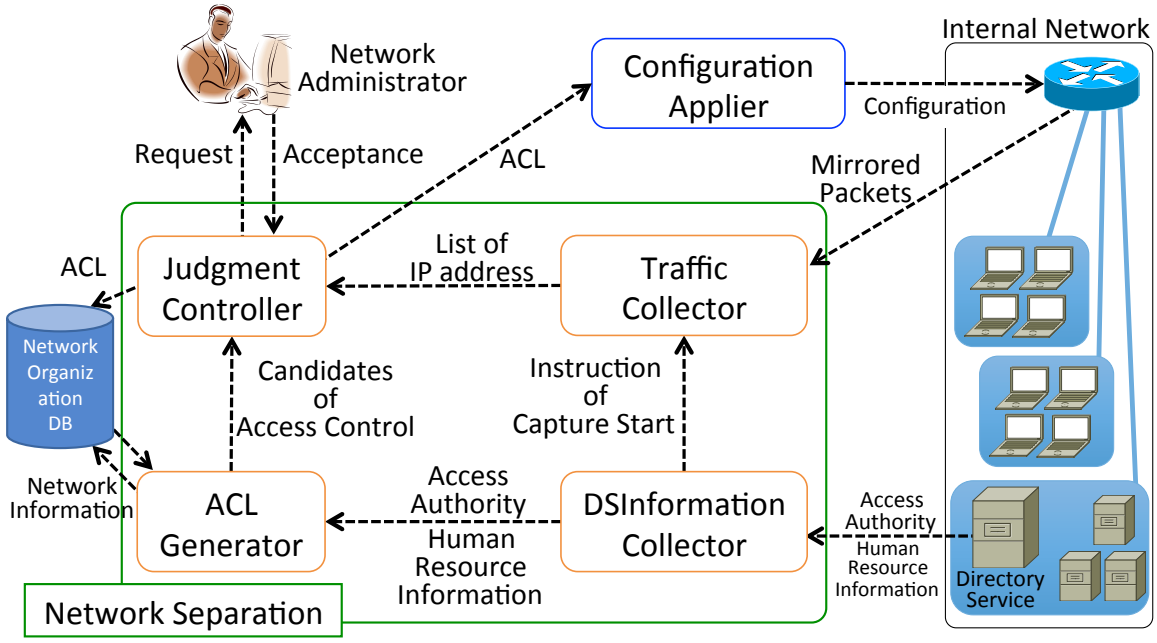

図 4.5　ACL 自動生成システム

ジュールと一つのデータベースから構成される．以下，各モジュールの詳細を述べる．

- DS 情報収集モジュール（DSInformation Collector）

  ACL 自動生成システムでは，まず初めに DS 情報収集モジュールがネットワーク内のディレクトリサービスサーバから，2 種類の情報を取得する．一つ目の情報は，組織の人事情報である．ACL 自動生成システムでは，人事情報に，各個人の名前，所属，役職，アカウント名，使用端末の IP アドレスが含まれていることを想定している．二つ目の情報は，ユーザのアクセス権限情報である．DS 情報収集モジュールは，収集したこれらの情報をアクセス制御生成モジュールに送信する．それとともに，トラフィック収集モジュールにネットワーク上のミラーパケットの収集開始の命令を送信する．

- アクセス制御生成モジュール（ACL Generator）

  このモジュールは 2 種類のアクセスを禁止する通信区間の候補を生成する．まず初めに，分割されたネットワークセグメント間のアクセス禁止候補を生成する．ネットワークの構成情報が保存されたデータベースから取得した各セグメントについて，全てのパターンのアクセス禁止候補を生成する．例えば，ネットワークに A，B，C の三つのセグメントが存在すると仮定する．この場合，システムは，A-B 間，A-C 間，B-C 間という 3 種類のアクセス禁止候補を生成する．

  次に，アクセス権限情報を基に端末単位のアクセス禁止候補を生成する．ACL 自動生成システムでは，ディレクトリサービスサーバから取得したアクセス権限情報を基に不必要な通信区間を決定する．例えば，あるサーバ内のディレクトリには，特定の端末のみがアクセス権限を有するとする．この場合，アクセス権限を有しない他のすべての端末はこのサーバとの通信が不必要とし，サーバとアクセス権限を有しない端末間の通信区間をアクセス禁止候補とする．

  最後に，2 種類のアクセス禁止候補を結合し，そのすべてを判断制御モジュールへ送信する．

- トラフィック収集モジュール（Traffic Collector）

  ネットワーク上のミラーパケットを一定時間収集するモジュールである．収集する時間は，“監視時間” として予め設定しておく．DS 情報収集モジュールから収集開始命令を受信した時点で収集を開始し，設定された監視時間まで収集を行う．その

後，収集したパケットから送信元 IP アドレスと宛先 IP アドレスを抽出し，それらを判断制御モジュールへ送信する．

- 判断制御モジュール（Judgment Controller）
  このモジュールは，トラフィック収集モジュールが収集したデータを用いて，アクセス制御生成モジュールが生成したアクセス禁止候補の正当性を判断する．アクセス禁止候補の通信区間のうち，実ネットワークにおいてトラフィックが存在する区間は通信必要区間と判断し候補から除外する．最後に，ネットワーク管理者にアクセス禁止候補を提示し，それらの実ネットワークへの適用の承認を得る．ネットワーク管理者の承認が得られた候補をデータベースに登録するとともに，ネットワーク自動設定モジュール（Configuration Applier）に送信する．

4.7 ACL 自動生成システムの実装

ACL 自動生成システムを実装し，評価用のプロトタイプシステムを作成した．このプロトタイプシステムは，ACL 自動生成システムの ACL 適用モジュールを除く各モジュールを Java（一部 Python および PHP）を用いて実装したものである．

4.7.1 想定環境

プロトタイプシステムでは，ディレクトリサービスとして一般的な企業で利用されている Microsoft Windows Server 2012 R2 上の Active Directory を想定した．Windows Server 2012 以降のバージョンにおける Active Directory には，各ユーザのディレクトリへのアクセスを集約的に管理するダイナミックアクセス制御機能が含まれている．このダイナミックアクセス制御機能に関する情報をアクセス権限情報として取得し，プロトタイプシステムを実現した．

4.7.2　各モジュールの実装

DS 情報収集モジュール

図 4.6 に示すように，あらかじめ ACL 自動生成システム内に共有フォルダを作成し，Windows Server が SMB を用いて共有フォルダに接続することとした．その上で，Windows Server 上に BAT ファイルを配置し，タスクスケジューラにより定期的にこの BAT ファイルを実行する．

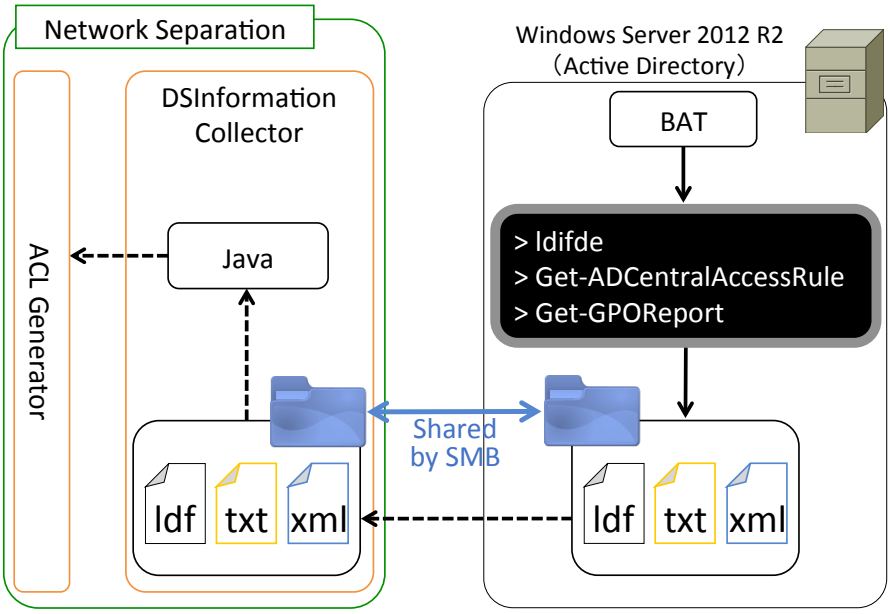

図 4.6　DS 情報収集モジュールの実装

Windows Server 上では，以下の Windows PowerShell コマンドを実行することによりディレクトリサービスの情報を取得する．

- ldifde

  登録されているユーザ情報を含んだ ldf ファイルを生成する．ユーザ情報には，ユーザの名前，所属，役職，アカウント名，IP アドレス (プロトタイプシステムではユーザの description 情報に記述した) が含まれる．
- Get-ADCentralAccessRule

  ファイルサーバ上のディレクトリへアクセス可能なユーザの条件が記述された集

約型アクセス規則を出力する．ただし，このコマンドは出力結果を保存できないため，Out-File コマンドを併用して出力結果をテキスト形式で保存している．

- Get-GPOReport
  Active Directory に保存された各集約型アクセス規則が，ネットワーク上のどのサーバに適用されているかの情報が含まれるグループポリシーを取得する．グループポリシーは xml ファイルとして保存可能である．

生成された 3 種類のファイルを，マウントされたネットワークドライブに配置することにより，ACL 自動生成システムにこれらのファイルを送信する．定期的に BAT ファイルを実行することで，ネットワークドライブ上には常に最新の情報が配置される．

DS 情報収集モジュールは，取得した 3 種類のファイルから必要な情報を抽出し，アクセス制御生成モジュールへと送信する．また，トラフィック収集モジュールを起動してトラフィックの収集を開始させる．

トラフィック収集モジュール

トラフィック収集モジュールは，ネットワーク上のコアスイッチのミラーポートに接続されたインターフェイスに対して tcpdump コマンドによりパケットを取得する．パケットの取得はあらかじめ設定された監視時間の長さだけ行われるが，ネットワークの規模や監視時間によっては収集するトラフィックの総量が大きくなり，その後の送信元 IP アドレスと宛先 IP アドレスの抽出処理に影響を及ぼしてしまう．この問題点については，収集する際に複数のデータに分割し，収集と並列して収集が完了したデータからの抽出作業を行うことにより解決した．プロトタイプシステムの実装では，監視時間を 30 分として，1 分単位の収集を 30 回行った．また，収集が終了した pcap ファイルから順に，送信元 IP アドレスと宛先 IP アドレスの抽出を行う．この抽出プログラムについては，Python と dpkt[43] を用いて実装した．30 個の pcap ファイルすべての収集，抽出が終了した後，判断制御モジュールに抽出結果を送信する．

判断制御モジュール

生成されたアクセス禁止候補と，実際のトラフィックから抽出された送信元 IP アドレスと宛先 IP アドレスの組を比較し，トラフィックが観測された区間はアクセス禁止候

補から除外する．最終的なアクセス禁止候補のリストを，PHP で作成した管理者用インターフェイスが読み込み，管理者の承認を得る．

4.7.3　実行例

図 4.7 は，ACL 自動生成システムが生成するアクセス制限候補の承認を行うための管理者用画面の例を示す．画面上に提示されるアクセス禁止候補の一覧をネットワーク管理

図 4.7　アクセス制御承認画面

者が確認し，実際にネットワークに適用してもよいと判断されるアクセス禁止候補には承認として Accept ボタンを選択する．同様に，ネットワークへの適用を否認する候補に対しては Reject ボタンを選択し，最終的に確定ボタンを押すことで実ネットワークに適用する ACL を決定する．

4.8　評価

ACL 自動生成システムの有効性を検証するため，実験用ネットワークを構築し，実装した ACL 自動生成システムと接続して内部分離設計を構築する被験者実験を行った．被験者は著者が所属する研究室において情報ネットワークに関連する研究を行っている大学

生および大学院生の計 5 名とした．

4.8.1　実験環境

本論文の実験では，総務部，経理部，営業部，運営管理部，開発部の 5 部署からなる，PC 端末を使用する社員が 25 名の企業を想定した．想定企業のネットワークの環境を図 4.8 に示す．ネットワークは部署ごとにセグメントに分割されており，25 台のクライアン

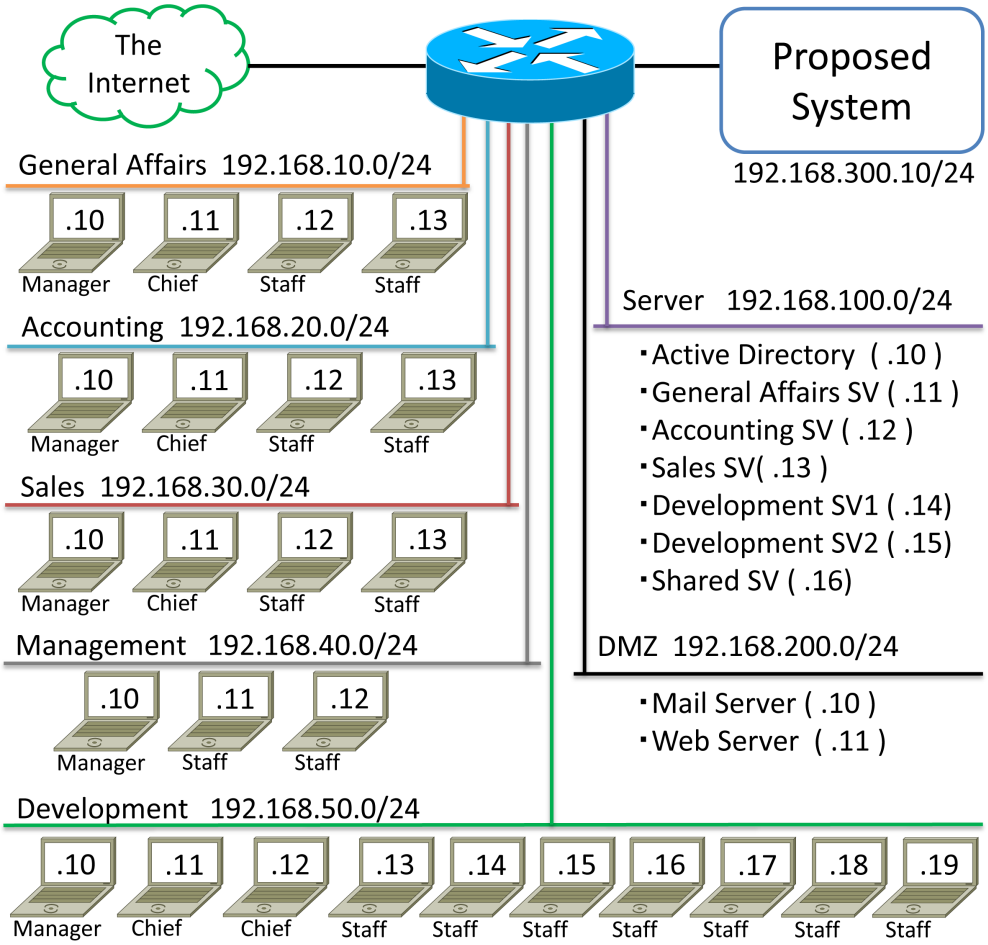

図 4.8　実験ネットワーク

ト端末はいずれかのセグメントに属している．また，全てのクライアント端末に対して管理のために静的に IP アドレスが割り当てられており，それぞれの利用者も固定されている．総務部，経理部，営業部は部長（Manager），課長（Chief）をそれぞれ 1 名，従業員

表 4.1　アクセス権限の一覧

		総務部サーバ	経理部サーバ	営業部サーバ	開発部サーバ 1	開発部サーバ 2	共有サーバ
総務部	部長	√	√				√
	課長	√	√				
	従業員	√					
経理部	部長		√				√
	課長		√				
	従業員		√				
営業部	部長		√	√		√	√
	課長		√	√		√	
	従業員			√		√	
管理部	部長		√				√
	従業員						
開発部	部長		√		√	√	√
	課長		√		√	√	
	従業員				√		

（Staff）を 2 名で構成されていることを想定している．また，運営管理部は 1 名の部長と 2 名の従業員，開発部は 1 名の部長，2 名の課長，7 名の従業員からそれぞれ構成される．

サーバ端末は，外部公開用のウェブサーバとメールサーバは DMZ セグメントに属し，その他のサーバはサーバセグメントに属している．25 名の全て社員の情報はサーバセグメント内の Active Directory に登録，管理されている．また，Active Directory のダイナミックアクセス制御機能により各ユーザの所属や役職に応じてサーバセグメントに属する各サーバ内のディレクトリに対するアクセス管理が行われている．表 4.1 は，各サーバに対するアクセス権限の一覧を示しており，表中の記号はアクセス可能であることを表す．

4.8.2 実験内容

実験準備

4.8.1 節で述べた環境において ACL 自動生成システムを実行するために，セグメントの一覧およびサーバの一覧をネットワーク構成情報として ACL 自動生成システムに登録した．また，これらの情報に加え，ネットワーク構成図，人事情報（すべての社員の名前，所属，役職，使用端末の IP アドレス），ディレクトリサービス情報（すべてのアクセス規則および適用されているサーバ）を被験者に提示する資料として用意した．

また，実験環境において ACL 自動生成システムを実行し，アクセス禁止候補の生成を行った．この際，トラフィック収集モジュールの監視時間は 30 分間として設定を行い，ネットワーク内で行われるすべての通信を収集するために，この 30 分間中に 25 台のすべてのクライアント端末において必要な通信を行った．必要な通信とは，各クライアント端末の使用者がアクセス権限を有する各サーバ内のファイルへのアクセス，メールの送受信，DMZ 内 Web サーバへの Web アクセス，およびインターネットへの Web アクセスである．ただし実際の運用においては，実験のように設定した短期間のうちにすべての通信が収集できるという理想的な状況であるとは限らず，すべての通信を収集するためにはより長期間の監視時間が必要であると考えられる．

被験者に説明するネットワークの条件として，サーバセグメントと DMZ 間は基本的に通信は発生しないが，今後 Active Directory とメールサーバがアカウントの連携を行う可能性があるという状況を説明した．また，全てのクライアント端末は，DMZ 内のメールサーバとの通信が必須であり，DMZ 内の外部向け Web サーバとの通信も行うことを説明した．

被験者実験

下記の手順により被験者による実験を行った．

手順 1　被験者に対してネットワーク内部分離設計に関する説明を行う．

手順 2　被験者は提示された資料を基に，実験用ネットワークにおけるアクセス制御を設計する．ただし，アクセス制御を決定する基準は ACL 自動生成システムと同様，

表 4.2　アクセス制御設計の所要時間

	システム非利用時	システム利用時
被験者 1	35 min	5 min
被験者 2	48 min	14 min
被験者 3	26 min	11 min
被験者 4	27 min	16 min
被験者 5	22 min	16 min

各ユーザのアクセス権限を用いるものとする．

手順 3　後日，手順 2 と同様の資料を提示し，ACL 自動生成システムのアクセス制御承認画面（図 4.7）を操作し，ACL 自動生成システムが生成したアクセス禁止候補の承認，非承認の判断を行うことで，再度アクセス制御を設計する．

手順 4　被験者が手動で設計した ACL と，ACL 自動生成システムを用いて設計した ACL の比較を行う．また，それぞれの ACL の設計に要した時間の比較を行う．

ただし，学習効果を考慮して半数の被験者は手順 2 と手順 3 の順序を入れ替えて実験を行った．

4.8.3　実験結果

所要時間

被験者が ACL 自動生成システムを利用しない場合と利用した場合のそれぞれにおいて，アクセス制御の設計に要した時間の一覧を表 4.2 に示す．ただし，被験者 4 および被験者 5 は，実験の手順 2 と手順 3 を入れ替えて実験を行った．表 4.2 の結果から，すべての被験者においてシステム利用時にアクセス制御の設計時間の大幅な減少が認められた．よって，システムを用いることによってアクセス制御の設計時間が短縮できることがわかった．

アクセス制御の数

各被験者が生成したアクセス制御について，冗長なアクセス制御と，改善可能なアクセス制御の数を調べた．冗長なアクセス制御とは，複数のアクセス制御が一つの通信区間に対して設定されている箇所を指す．例えば，192.168.20.0/24 と 192.168.100.11 間のセグメントとしてのアクセス制御と，192.168.20.10 と 192.168.100.11 間の端末単位のアクセス制御が存在する場合などである．また，改善可能なアクセス制御とは，複数のアクセス制御を一つのアクセス制御で代替可能な箇所を指す．例えば，経理部のセグメントに属する全ての端末（192.168.20.10-13）と 192.168.100.11 の間の四つのアクセス制御の場合，これらをまとめて 192.168.20.0/24 と 192.168.100.11 の間のセグメントとしてのアクセス制御で代替可能である．このような代替したアクセス制御の場合，経理部のセグメント内のホストが存在しない IP アドレスについても，192.168.100.11 との通信を禁止することを実現可能である．

ACL 自動生成システムは，冗長なアクセス制御および改善可能なアクセス制御を生成しなかった．また，手動による設計の場合，冗長なアクセス制御を生成した被験者はいなかった．3 名の被験者は改善可能なアクセス制御も生成しなかった．しかしながら，被験者 4 と被験者 5 の 2 名はアクセス制御をまとめるといったことは行っておらず，それぞれ 19 箇所，15 箇所の改善可能なアクセス制御が存在した．

アクセス制御の内容

ACL 自動生成システム，被験者共に同じ基準を用いてアクセス制御を設計しているため，それぞれが生成したものは概ね同様の内容となった．

- 各部署セグメント間の通信
  ACL 自動生成システム，被験者共に，各部署セグメント間の通信を適切に禁止した．
- 各部署セグメントとサーバセグメント間の通信
  アクセス権限情報を基に，アクセスの必要がない通信区間のアクセスを禁止する．つまり，表 4.1 中の空欄部のアクセスを禁止する．ACL 自動生成システムは，表 4.1 中の空欄部全てのアクセスを禁止していた．それに対し，被験者が設計したア

クセス制御では，5 箇所の空欄部において 1 名もしくは 2 名の被験者がアクセスを禁止していなかった．また，1 名の被験者はアクセスが存在する区間 7 箇所に対して，アクセス制限を行っていた．実験終了後に確認したところ，これらは被験者の意図したものではなく，見落としによるものであった．そのため，全ての被験者は ACL 自動生成システムが提示したこれらの区間に対するアクセス制限候補の適用を全て承認している．

- 各部署セグメントと DMZ 間の通信

  ACL 自動生成システム，被験者ともに各部署セグメントから DMZ に対する通信は禁止されていなかった．

- サーバセグメントと DMZ 間の通信

  現在は通信が行われておらず，今後行う可能性がある区間が存在するため，被験者により判断が別れる結果となった．まず，ACL 自動生成システムは通信が発生していない区間のため，サーバセグメントと DMZ 間の通信を禁止する候補を提示した．それに対し，被験者 1 は ACL 自動生成システムを利用した場合の実験においてこの候補の適用を否認した．また，被験者 1 が手動で生成した ACL では，Active Directory を除く 6 台のサーバと DMZ 間の通信を禁止していた．この結果は，被験者 1 が今後通信の可能性がある区間を遮断しないことを優先したためであった．

  被験者 5 も同様に ACL 自動生成システムを利用した場合の実験においてこの候補の適用を否認した．また，被験者 5 は手動で生成した ACL においては，サーバセグメントと DMZ 間に関する通信は一切禁止していなかった．これは，被験者 5 が今後通信の可能性がある区間を優先したためであったが，被験者 1 に比べて通信の必要がない区間を考慮していないためであった．

  一方，残りの被験者 3 名は ACL 自動生成システムの候補を承認し，手動で生成した ACL においても通信を遮断していた．これはそれぞれ，現在は通信が行われていない区間であるため，通信の必要がないと判断したためであった．

4.9 考察

実験の結果から，ACL 自動生成システムが提示したアクセス禁止候補は，ほぼ被験者が設計したものと同等であり，被験者が意図するアクセス制御をほぼ網羅したと言える．また，同等の内容でありながら一部の被験者と比べてアクセス制御の数を改善可能であった．しかしながら，DMZ，サーバセグメント間の通信など，一部被験者の意図するアクセス制御を提示できていない区間があった．この区間については，被験者の意図するアクセス制御は ACL 自動生成システムでは生成することが不可能であるため，システムが提示する以外にも任意でアクセス制御を追加できるような仕組みも必要であることがわかった．

システム利用時，非利用時の所要時間の結果から，被験者により個人差が生じるが，システムを利用する場合には一概に所要時間が減少しているため，ACL 自動生成システムはネットワーク管理者の判断に大いに役立っていることがわかる．実験はクライアント端末が 25 台の環境で行ったが，実際に運用されている企業ネットワークはさらに大きな規模の場合が多い．端末の台数が多いほどアクセス制御の数も多くなると考えられる．手動でアクセス制御を設計する場合，アクセス制御の数に応じて生成の所要時間も大きくなっていくため，システムが候補を提示する場合の所要時間との差はより大きくなると考えられる．

また，実験手順を入れ替え，ACL 自動生成システムを利用する実験を先に実施した被験者については，システム利用時の所要時間が他の被験者に比べ長時間ではあったが，システム非利用時との差は最も少ない結果となった．この結果から，ACL 自動生成システムを利用することにより，学習効果が得られ，以後の設計作業に要する時間を短縮可能であると期待できる．以上より，ACL 自動生成システムは内部分離設計の構築に対して有効な手法である．

本論文の実験は，ネットワーク内で使用される全ての経路の通信を収集するという ACL 自動生成システムの仕組みに対し，4.8.2 節で述べたように使用される全ての経路の通信が収集できる理想的な条件の元で行った．実際の運用においては収集時間が短ければ全ての通信を収集できず，一方で収集時間が長ければ不必要な収集データ量が増大してしまう．そのため，運用する環境に応じて適切な監視時間は変動すると考えられ，環境に応じ

て適切な時間を設定する必要がある．それに加え，頻度が少ない通信（例えば，週に 1 度のファイルアクセスなど）が存在する場合には，この通信を収集するために収集時間およびデータ量の増大を引き起こしてしまうため，システムが収集する通信に加え手動で必要な通信を追加する仕組みも導入すべきである．

また，ACL 自動生成システムにおけるトラフィックの収集は，ネットワーク上の端末がマルウェア感染等の状態に陥っておらず，ネットワーク内において正常な通信しか存在しないという前提で行っている．そのため，ACL 自動生成システムの運用前にすでにマルウェアに感染した端末が存在し，不正な通信が行われている状態でトラフィックを収集してしまった場合には，そのような不正通信に対するアクセスの制限は行うことができない．しかしながら，標的型攻撃のように侵入したネットワーク内で侵食を繰り返し状況が刻一刻と変化するものに対しては，システム使用時点での不正通信は見落とすこととなるが，システムによりアクセスを制限した経路においてそれ以降に発生する不正通信の抑制や検知が可能となるため，攻撃自体の検知や実被害の防止という観点から有効な手段であると考えられる．

4.10　本章のまとめ

この章では，標的型攻撃に対する有効な対策手法である内部分離設計に着目し，その構築が困難であるという問題点を解決するためにディレクトリサービス情報とネットワークトラフィックを用いた ACL 自動生成システムを提案した．提案システムにより，ネットワーク管理者が容易に内部分離設計を構築することを可能とした．実験用ネットワークにおける評価実験を行った結果，各被験者ともにシステムの利用により内部分離設計の設計時間が減少するという結果が得られ，ACL 自動生成システムの有効性が示された．

ACL 自動生成システムが提示したアクセス禁止候補の内容において，提示した候補が不十分な点がごく一部生じた．これに対し，提示された候補以外でもネットワーク管理者がアクセス禁止候補を追加可能とすることで解決可能である．

ACL 自動生成システムでは，システムの実行時に一定時間トラフィックの収集を行い，内部分離設計を行った．この仕組みは，トラフィックの収集を定期的に行い，ACL の内容やネットワークの構成と比較することで，ネットワーク内の端末の死活監視などの管理運用技術としても利用できる可能性がある．

第 5 章

ネットワーク内の監視活動および不審な通信の解析支援

5.1　まえがき

第 4 章では，マルウェアによる不正通信の抑制や効率的な検知を行うためのネットワーク内部分離設計の構築支援手法について述べた．ネットワーク内部分離設計の利点の一つとして，ネットワーク内の不正通信の監視や検知が効率的に行えるというものがある．これは，一般的なフラット構造ネットワークにおいてはネットワーク内の全トラフィックを一元的に監視する必要があるのに対し，適切な分離およびアクセス制御が行われている状態では監視対象セグメントを限定して切り替えることで監視対象トラフィックの削減を行えるためである．

本章では，構築した内部分離ネットワークの特性を利用し，効率的にネットワークの監視，および不正通信の解析を行うための管理支援手法について述べる．これは，動的ネットワーク構成を用いることで，監視を行う対象が異なるネットワーク構成を切り替えて適用することによる，監視対象セグメントの切り替えを基本とする手法である．提案手法では，各ネットワークセグメントに対して，セグメント内端末のマルウェア感染疑いのレベルを表す ISL（Infection Suspicious Level）を設定する．ISL の状況に応じて，巡回監視や集中監視を実施することで，監視コストの低減が可能となる．また，ISL の状況に応じて通信の解析を行うためのネットワーク構成に切り替えることにより，検知された不正通信の効率的な解析を行うことが可能となる．

5.2　ネットワーク監視・不正通信解析の問題点

5.2.1　ネットワークの監視コスト

組織内ネットワークの入口における監視は一般的に行われる活動である．一方で，ネットワークの内部も含めた全体のトラフィック監視については，監視対象となるトラフィックが膨大な量となり，非常にコストがかかる．これは，組織内ネットワークの監視には入口における監視よりも一桁以上大きなトラフィックに対応しなくてはならないことによる機器コスト，および，トラフィック量に応じて増大するアラートを処理する人的コストの双方の点から問題となる．

機器コストの問題点については，一般的に監視に用いられる手法は様々なものが存在するが，それぞれにメリットとデメリットが存在するため，適切に組み合わせて利用が望ましい点がコストの問題に拍車をかける．従来からの監視手法として，ファイアウォールやシグニチャをベースとしたネットワーク型 IDS などがあるが，これらはあらかじめ登録されたシグニチャにマッチしたものを検知する．そのため，既知のマルウェアの検知には有効であるが，標的組織専用に設計され組織内の通常通信に紛れて行われる巧妙な標的型マルウェアなど，未知の検知は困難である．昨今では，それまで通信が行われていなかった区間において突然通信が頻繁に行われるようになった等，正常時の通信パターンとは異なる通信が行われた場合に異常として検知するアノマリ型の IDS の研究も盛んに行われている [12]．それぞれの手法で検知を行い易いマルウェアが異なるため，これらの手法は組み合わせて利用することが効果的である．しかし，いずれの手法においても，誤検知の問題もある．日々発生する大量のアラートの中から，ごく一部の重要な情報を見つけ出すことは困難な作業である．

5.2.2　不正通信の解析コストと遅延

監視対象のトラフィックからなんらかの異常が検知され，アラートが発生した場合には，その原因となった異常通信を行った端末のマルウェア感染を疑い，解析を行う必要がある．このような解析を実施できる人材のコストは高いため，組織内ネットワークの監視によって増加するアラートに追従するための人材増強は厳しい．近年のセキュリティ人材

不足は，この人材コストの問題にさらに拍車をかけるものとなる．また，疑わしい通信を一つ一つ解析していくには膨大な時間が必要であり，また通常は検知された順に解析を行うため，重要なアラートの解析が遅れインシデントへの対応が遅れてしまう可能性もある．

5.3 ネットワーク監視・不正通信解析の管理とインシデント状況判断

本論文では，効率的にネットワークの監視を行うことが可能なネットワーク巡回監視を適用し，監視方法および，セキュリティアラートが発生した際の巡回監視の管理を行うことにより，前節で述べた問題点を解決する．また，これを行うことによりインシデントの深刻度合いの状況判断を行い，状況に応じた適切な対策を施すための支援が可能となる．

5.3.1 ネットワーク巡回監視

4.2 節で述べたように，第 4 章で構築したネットワーク内部分離設計が適用されたネットワークにおいては，分割されたセグメントをグループ化し，そのグループを周期的に切り替えて監視する巡回監視が適用可能であり，効率的にネットワークの監視を行うことが可能である．巡回監視を適用することで，監視対象となるトラフィック量を低減可能であるため，監視コストの問題を解決する．本論文では，監視対象セグメントのトラフィックのミラーリングを行い，ミラートラフィックを検知システムへと転送する．動的ネットワーク構成により，ミラーリングを行う監視対象セグメントが異なるネットワークへと動的に切り替えを行うことにより，巡回監視を実現する．

5.3.2 異常トラフィックの解析

なんらかのセキュリティアラートが発生した場合，マルウェアの感染によるものか，誤検知であるのかを解析する必要がある．マルウェアの解析手法は様々なものがある．一般的には，マルウェアの解析では異常通信を行った端末内の疑わしいファイルの解析が通常行われるが，一般的にファイル解析は時間がかかるものである．本論文が対象とするよう

なエンタープライズネットワークは規模が大きく，日々大量のアラートが発生するため，可能な限り迅速に異常通信の判定を行う必要がある．そこで本論文は，ファイルの解析ではなくトラフィックを解析することでマルウェア解析を実現する．例えば図 5.1 のように，SDN 機器の設定を変更し，監視対象となる端末に関するすべての通信を，サンドボックスなどの組織内部ネットワークを模した安全な解析環境へ転送する．解析環境で

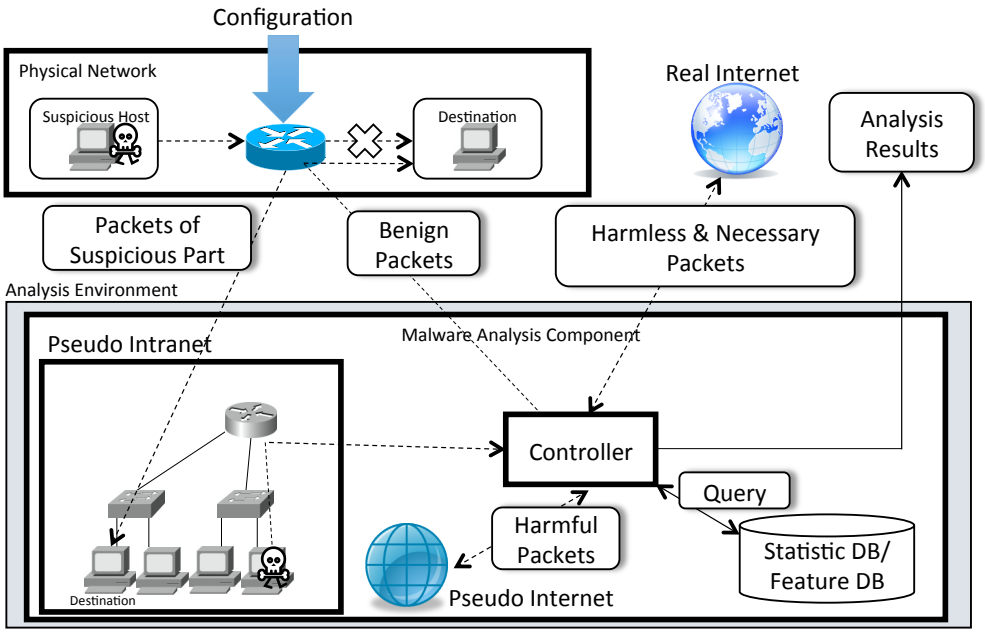

図 5.1　トラフィックの解析手法

は，外部への攻撃などの危険な通信は擬似的なインターネットで処理し，C&C サーバから司令を受け取るなどの無害かつ解析に必要な通信のみを外部と接続する．これによりトラフィックを安全に解析することが可能となる．細かい解析手法については本論文の対象外とするが，既存の手法 [44] などを用いて行うことが可能である．本論文では，動的ネットワーク構成により，図 5.1 の例のようなトラフィック解析を実現可する．

5.4　ネットワーク監視と不正通信解析の管理

巡回監視とネットワークトラフィックの解析により，効率的にネットワーク監視と不正通信解析が可能であるが，本論文においてはこれらをさらに細かく管理運用することで，

組織内ネットワーク監視におけるコストの問題を解決する．また，多量の誤検知により真に解析が必要なアラートが埋もれてしまうもしくは対応が遅くなってしまうという問題を解決するために，巡回監視の際の監視時間を動的に切り替えた上で，マルウェアの感染可能性が高い端末の解析を優先して行う仕組みを提案する．

5.4.1 ISL（Infection Suspicious Level）

まず初めに，マルウェアの感染疑いの度合いを 4 段階に分類する ISL（Infection Suspicious Level）を定義する．ネットワーク内の全てのセグメントごとにセグメント内の端末がマルウェアに感染している疑いの度合いとして ISL の 4 段階のうちのいずれかを割り当てる．レベル 1 からレベル 4 で表される 4 つの段階は，値が大きくなるほどより感染疑いの度合いが高く，深刻な状況であることを示す．ISL の段階に応じて巡回監視の頻度や時間，トラフィック解析を行うか否かを動的に切り替えることにより，深刻なアラートを優先して対処することを可能とする．

ISL はインシデントの状況判断を行うためにも使用する．インシデントが発覚した際には，特に標的型攻撃において攻撃の進行状況に応じて適切な対策は異なるため，ネットワーク管理者は対策の選択に頭を悩ませることになる．第 2 章で述べたように標的型攻撃におけるマルウェアは異なる機能をもつ多数のマルウェアが組織内ネットワークに侵入し，マルウェア同士が通信網を形成する．ある端末の感染が発覚した場合に即座にその端末の通信を止めるような対策を取ってしまうとマルウェア同士で通信が行えなくなるために，攻撃者が検知されたことを把握してしまう．これにより，その他の未検知の状態のマルウェアや攻撃の痕跡の隠蔽活動を行い，検知が出来ない状態で攻撃が進行するもしくは攻撃の全貌把握や証拠の確保が難しくなってしまう．そのため，攻撃が比較的早期の段階であれば即座に対策を取らず感染端末の洗い出しを行った後にすべての感染端末をまとめて対策を行うことが求められる．このように，インシデント対応は状況判断と適切な対策が必要であるが，ISL を用いることで，トラフィックの解析結果等を管理し，状況に応じて適切な対策を行うことが可能となる．以下，ISL の各段階の詳細を説明する．

レベル 1-監視（Monitoring）

正常な状態を表す段階である．初期の状態では，すべてのセグメントに対してこのレベルの ISL が割り当てられる．この段階では，通常の巡回監視を行い，ネットワークのミラートラフィックを検知システムに転送する．巡回監視の監視対象は監視に用いるシステムの処理能力に応じて決定する．例えば，2 並列に 2 つのセグメントを監視する場合や，3 並列に 3 セグメントを監視する場合などである．このような並列度合いで，あらかじめ設定した監視時間として，10 分間隔などで監視対象の切り替えを行っていく．

レベル 2-重点監視（Intensive Monitoring）

セキュリティアラートの発生など，端末のマルウェア感染が疑われるセグメントが発生した場合には，そのセグメントの ISL をこのレベル 2 へと変更する．この段階では，重点監視として対象セグメントの巡回監視を強化する．監視システムの処理能力が比較的高い場合には，並列して監視する対象の一つをレベル 2 となったセグメントに固定し，残りの監視対象を巡回的に切り替えて監視を行う．

レベル 3-解析（Analysis）

セキュリティアラートの頻度や内容に応じて，マルウェア感染が強く疑われる端末が存在する場合には，その端末が属するセグメントの ISL をこの段階へ変更する．この段階では，レベル 2 の重点監視に加えて，解析段階として 5.3.2 節で述べたように感染が疑われる端末に関する全ての通信を解析システムへと転送する．解析により，疑わしい端末がマルウェアに感染しているか否かを判断する．

レベル 4-対策（Countermeasure）

マルウェアの感染が発覚し，この段階に遷移したセグメントに対しては，レベル 2 の重点監視，レベル 3 の解析に加えて感染端末の切り離し等の対策を施す．対策が有効に機能したことを確認するために，レベル 4 の状態の間は対策を施した後も重点監視と解析は継続する．

5.4.2　ISL の段階遷移

図 5.2 に，ISL の各段階とその遷移を示す．

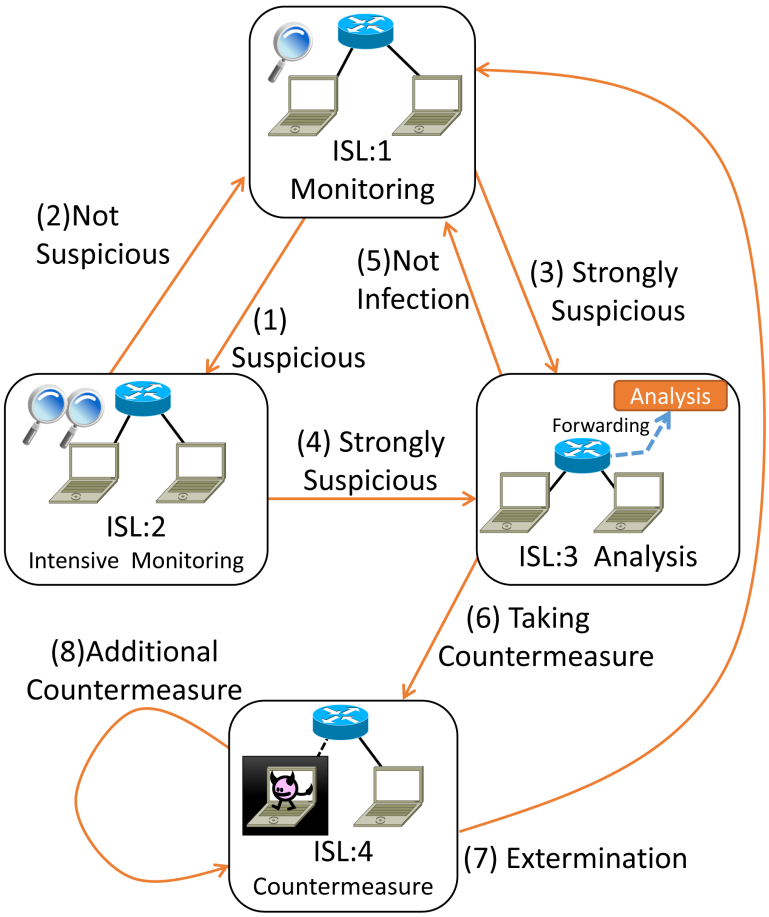

図 5.2　ISL 段階の遷移

初期状態では全てのセグメントの ISL はレベル 1 である．この状態で，巡回監視中に何らかの検知システムによるセキュリティアラートが発生した場合，これをトリガとして ISL をレベル 2 へと変更する（図 5.2 (1)）．

ISL がレベル 2 の状態における巡回監視において，一定期間追加のアラートが発生しない等，マルウェア感染の疑いが弱まった場合には ISL をレベル 1 へと変更する（図 5.2 (2)）．

ISL がレベル 1 の状態で，ブラックリストに登録された C&C サーバとの通信が検知された等，マルウェア感染の疑いが非常に強い場合には ISL のレベルを 1 から直接レベル 3 へと遷移させる（図 5.2 (3)）．同様に，ISL レベル 2 の状態の重点監視の結果，疑わしい端末からその他のアラートがいくつも発生するなどといったように感染の疑いが強まった場合には，レベル 2 からレベル 3 へと遷移する（図 5.2 (4)）．

ISL がレベル 3 の状態において，トラフィックの解析の結果から疑わしい端末がマルウェアに感染していないと判断された場合，ISL はレベル 1 へと遷移する（図 5.2 (5)）．それに対し，セグメント内の端末のマルウェア感染が発覚した場合には，ISL はレベル 4 へと遷移する（図 5.2 (6)）．ただし，攻撃の状況によって，即座に対策を施すべきか否かは異なる [45]．例えば，攻撃が初期の状態で対策を施してしまった場合には，攻撃者はマルウェアが検知されたことを気づいてしまい，攻撃手順の変更やシステムの破壊活動を行う可能性もある．そのため，状況によっては即座に ISL を遷移させず，レベル 3 の状態で感染端末の洗い出しを行った後，レベル 4 へと遷移させる．

ISL レベル 4 において，インシデントに対する対策を行った後，重点監視とトラフィック解析を継続する．これにより，施した対策が有効に機能しているか否かを判断し，その結果に応じて次の ISL の遷移先レベルを決定する．対策の結果，疑わしい活動は観測されなくなり，インシデントによる脅威から脱したと判断された場合には，ISL をレベル 1 の平常状態へと遷移させる（図 5.2 (7)）．それに対し，依然として疑わしい活動が検知されるような場合には，ISL はレベル 4 を維持し，再度異なる対策を行う（図 5.2 (8)）．

5.5　監視・解析管理支援システム

3.4 節のサイバー攻撃対策支援システムを実現するためのサブシステムとして，ネットワーク監視と不正通信解析の管理手法を用いた監視・解析管理支援システムを提案する．

5.5.1　システム構成

図 5.3 に監視・解析管理支援システムの構成図を示す．監視・解析管理支援システムは，ISL 管理モジュール（ISL Manage），巡回監視モジュール（Patrol），解析モジュール（Analysis）の三つのモジュールと 4.6.3 節で利用したものと同一のネットワーク構成

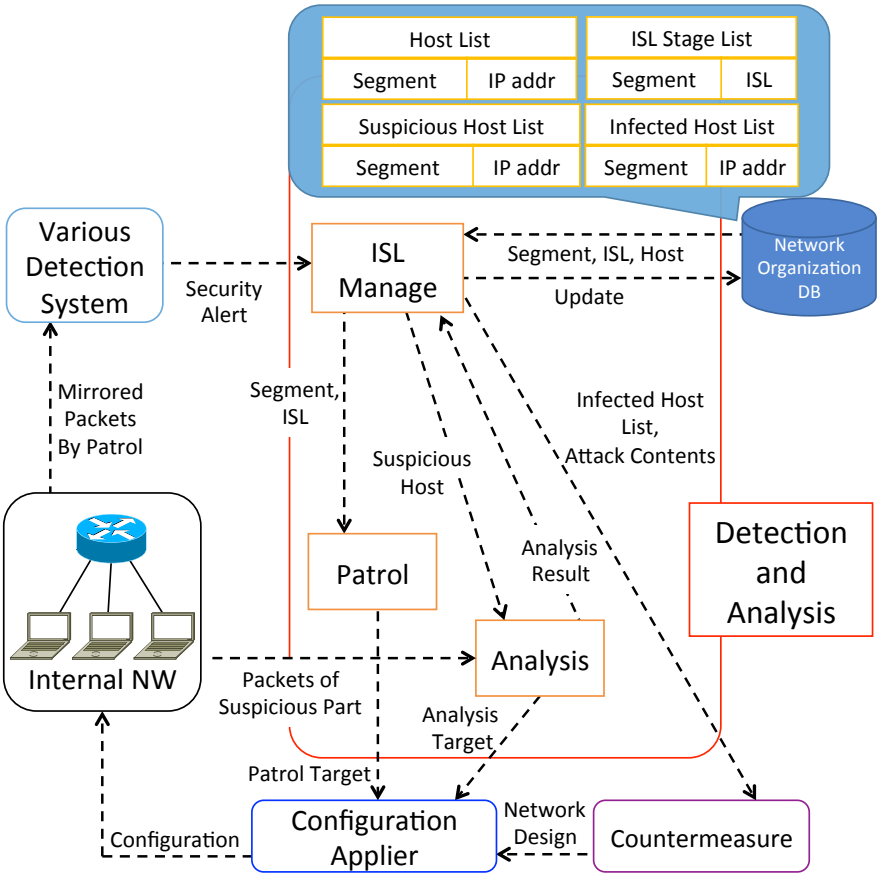

図 5.3　監視・解析管理支援システム

データベースからなる．

監視・解析管理支援システムでは，ISL のレベル遷移のためのトリガとしてセキュリティアラートを利用するが，5.2.1 節で述べたように検知率を向上させるために，複数の異なる検知システムを組み合わせて利用する．以下，各モジュールの詳細について説明する．

5.5.2　ISL 管理モジュール（ISL Manage）

ISL 管理モジュールでは，各セグメントの ISL の状態を二つのトリガを用いて遷移させる．一つ目は，ネットワーク内の検知システムから通知されるセキュリティアラートである．二つ目のトリガは，解析モジュールから出力されるマルウェア感染が強く疑われる端

末に関する解析結果である．

ISL 管理モジュールは，疑わしい通信を行った端末の IP アドレスを含んだセキュリティアラートを受け取った際，データベースの情報を用いて当該端末が属するセグメントのネットワークアドレスを特定し，そのセグメントの現在の ISL を確認する．現在の ISL がレベル 1 だった場合，ISL 管理モジュールはアラートを生成した検知システムの種類やアラートの内容などに応じて ISL をレベル 2 またはレベル 3 へと遷移させる（図 5.2 (1) または (3)）．また，ISL 管理モジュールは疑わしい端末の IP アドレス，その端末が属するセグメントのネットワークアドレス，その端末に関連するセキュリティアラートの数，最初にその端末に関するアラートが発生した時刻をデータベースに登録する．発生したアラートが実際の攻撃によるものであれば，重点監視によってさらなる証拠を取得できる可能性がある．そこで，監視システムが疑わしい端末に関する新たなアラートを通知した場合に，ISL 管理モジュールは当該セグメントの ISL をレベル 3 へと遷移させる（図 5.2 (4)）．しかしながら，最初のアラートが通知されてから一定期間が経過しても一切追加のアラートが発生しない場合などには，ISL 管理モジュールは ISL をレベル 1 へと引き戻す（図 5.2 (2)）．

ISL がレベル 3 の際に解析モジュールの行った不正通信の解析結果を受け取った際にも，ISL 管理モジュールは ISL を変更する．解析の結果，ISL がレベル 3 となっているセグメント内において感染が疑われる端末が一切ないとわかった場合，ISL 管理モジュールは当該セグメントの ISL をレベル 1 へと変更する（図 5.2 (5)）．それに対し，疑わしい端末がマルウェアに感染していると判定された場合には，当該端末をデータベース上の感染端末リストへと登録する．以降，解析システムが通知した，現在行われている攻撃の状況に応じて異なる対応を行う．C&C サーバとの通信など，攻撃が比較的初期の段階であれば，ISL 管理モジュールは ISL をレベル 3 の状態で維持し，重点監視と通信解析を継続することによって発見した感染端末以外の端末の調査を行い，感染拡大が発生していないか確認する．その後，セグメント内の全ての疑わしい端末の解析が終了したのち，ISL 管理モジュールは ISL をレベル 4 へとアップデートし，対策を行う（図 5.2 (6)）．標的型攻撃における情報送出段階にあるなど，攻撃が深刻な状況にある場合には，ISL 管理モジュールは即座に ISL をレベル 4 へと変更し，感染端末のネットワークからの隔離などの対策を施行する．ISL がレベル 4 の状態において，対策が適切に作用した場合には新たなアラー

トが発生する可能性は低い．しかしながら，近年の洗練された攻撃では，予備の感染端末を同一ネットワークに潜ませておき，遠隔操作中の感染端末が利用不可能となった場合に動作を開始する場合がある．そこで，重点監視と通信解析をアラートの発生がなくなるまで継続し，最終的に ISL をレベル 1 へと変更する（図 5.2 (7)）．対策の効果が薄く，引き続き異なるアラートが多く発生する場合には，ISL 管理モジュールは継続中の重点監視および通信解析の結果から得られた情報により最新の状態にアップデートされた感染端末リストを再度対策モジュールへと通知し，対策を行う（図 5.2 (8)）．

5.5.3 巡回監視モジュール（Patrol）

巡回監視モジュールは，監視対象となるネットワークセグメントの管理，切り替えを行うためのモジュールである．図 5.4 に示すように，巡回監視モジュールは監視リスト（Patrol List）として監視対象セグメントの一覧を保持する．また，巡回監視モジュールにはネットワーク内のセグメントの一覧と，一度につき 10 分間などといった監視時間をあらかじめ設定しておく．このとき，監視システムがいくつのセグメントを監視可能であるかの処理能力を考慮するものとする．

ISL 管理モジュールはネットワーク内のセグメントの ISL が変更された際，当該セグメントのネットワークアドレスおよび新たな ISL のレベルを巡回監視モジュールへと出力する．その後，巡回監視モジュールは監視リストを更新し監視対象を変更する．最後に，変更された監視リストを基に監視対象セグメントのネットワークアドレスを 3.4 節のネットワーク設定モジュールに転送することで，巡回監視のためのミラーを行っているネットワーク機器の設定を変更する．

図 5.4 は巡回監視モジュールの動作例を，ISL のレベル遷移の際の ISL 管理モジュールの動作も含めて示している．まず初めに，ネットワーク内の検知システムがマルウェア感染の疑われる端末を検知し，疑わしい端末の IP アドレスを含んだセキュリティアラートが ISL 管理モジュールへと通知される（図 5.4 (1)）．次に，ISL 管理モジュールはデータベースへ問い合わせを行い，疑わしい端末（IP アドレス：192.168.3.10）が属するセグメントのネットワークアドレス（192.168.3.0）と，そのセグメントの現在の ISL の状態（レベル：1）を取得する（図 5.4 (2)）．ISL 管理モジュールは ISL をレベル 2 へと変更する（図 5.4 (3)）とともに，疑わしいセグメントのネットワークアドレス（192.168.3.0）およ

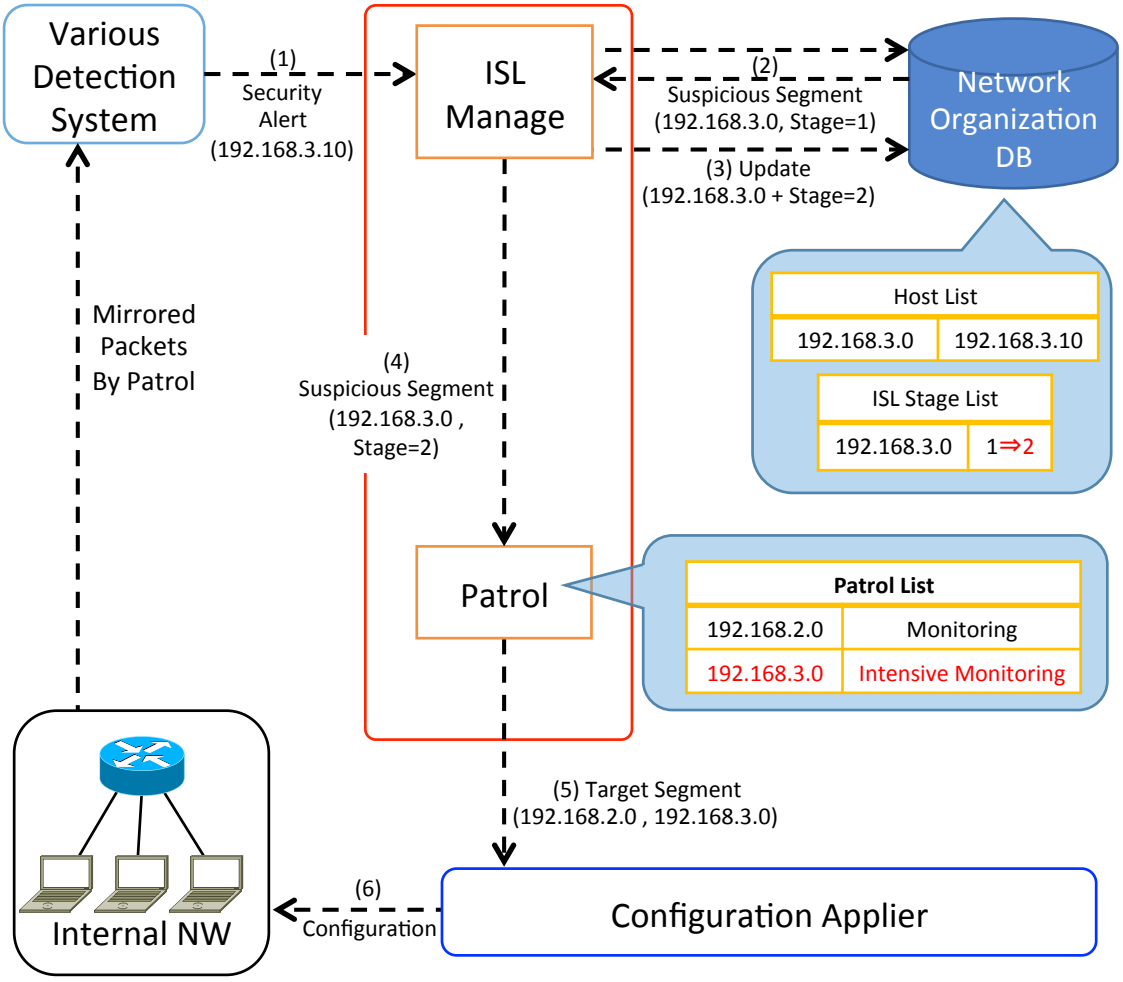

図 5.4　巡回監視モジュールの動作例

びそのセグメントの新たな ISL の状態（レベル 2）を巡回監視モジュールへと通知する（図 5.4 (4)）．この動作例では，監視システムが二つのセグメントを並列して監視可能であり，平常時の監視時間を 10 分間に設定していると仮定している．巡回監視モジュールは平常時は設定された監視時間である 10 分ごとに監視リストを更新し監視対象を切り替えるが，ISL 管理モジュールからの入力があった場合にも監視リストを更新する．この場合は，IP アドレスが 192.168.3.0 のセグメントが重点監視の対象となり，監視システムが行う 2 並列の監視のうち一つはこのセグメントの監視を行い，残りの監視対象セグメントの巡回監視をもう 1 並列の監視において巡回的に切り替えて実施する．最終的に，ネット

ワーク設定モジュールに新たな監視対象の情報を送信し（図 5.4 (5)），その内容がネットワークに適用される（図 5.4 (6)）．

5.5.4　解析モジュール（Analysis）

ISL がレベル 3 へと変更されたセグメントが発生した場合，ISL 管理モジュールは感染が疑われる端末の IP アドレスを解析モジュールへと転送する．その後，解析モジュールは感染が疑われる端末に関する通信の解析を行う．

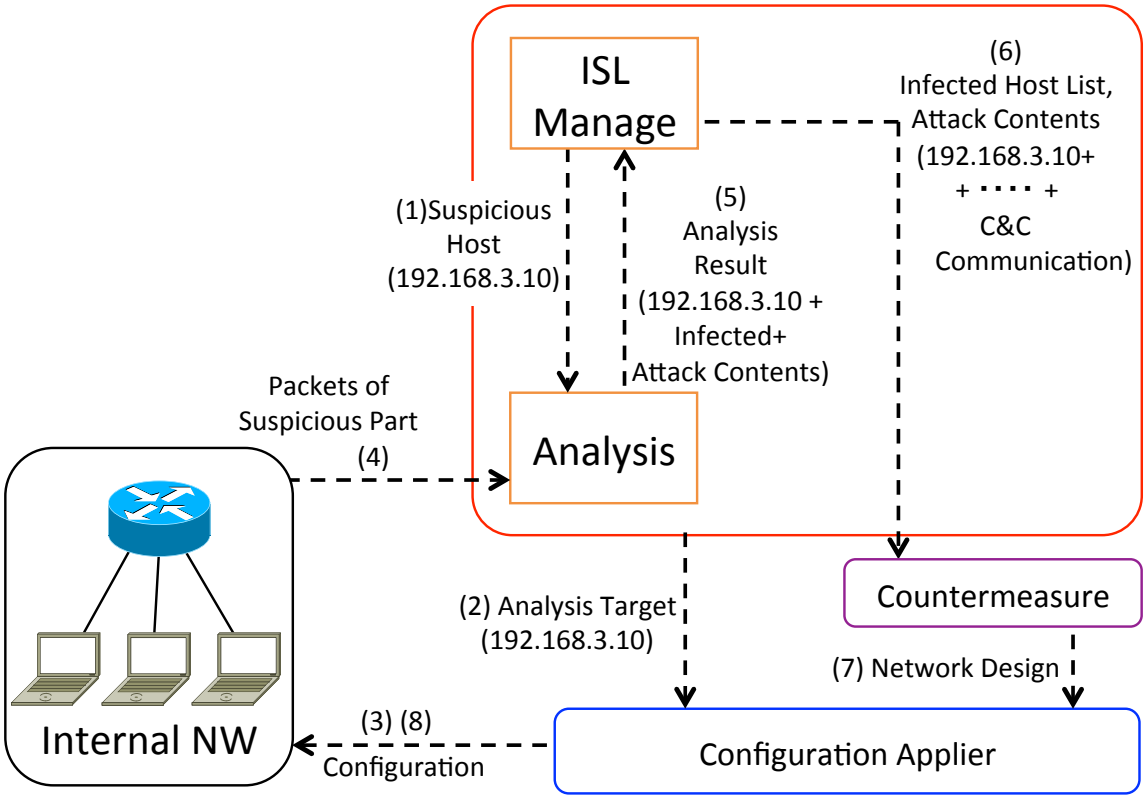

図 5.5　解析モジュールの動作例

図 5.1 が示す例のように，ISL 管理モジュールは感染が強く疑われる端末の IP アドレス（192.168.3.10）を，ISL の状態をアップデートした後に解析モジュールへと通知する（図 5.1 (1)）．解析モジュールは，解析対象となった IP アドレスをネットワーク設定モジュールへと通知し（図 5.1 (2)），ネットワーク設定モジュールがネットワーク機器の設定を変更することで，解析対象となった端末に関する全ての通信（送信先 IP アドレスも

しくは送信元 IP アドレスが解析対象端末となる全ての通信）の転送を行う（図 5.1 (3)）．解析対象端末に関する全ての通信が解析モジュールへと転送され（図 5.1 (4)），解析モジュールでは 5.3.2 節で述べた解析環境，手法を用いて通信の解析を実行する．解析終了後に解析モジュールは解析結果を ISL 管理モジュールへと通知する（図 5.1 (5)）．

通知された解析結果に応じて，対策が必要な場合には ISL 管理モジュールは感染端末の IP アドレスと行われている攻撃の内容をインシデント対応支援システムへと転送し（図 5.1 (6)），最終的に攻撃への対策がネットワークへと適用される（図 5.1 (7)，(8)）．

5.6 性能評価

本節では，提案システムの性能評価を行う．提案システムでは，巡回による監視コスト削減が可能である一方で，インシデントの見逃し確率が上がるための検出遅延が発生し，コストと遅延がトレードオフの関係にある．従来方式では，見逃し確率は低いが高コストの非巡回方式しか想定されていなかったことに対して，本提案では，使用者のニーズに合わせてトレードオフを調整可能である．

実際に，どの程度のトレードオフとなるかを，簡単な例で評価する．実験環境として，4.8.1 節で述べた実験環境（図 4.8 参照）を想定する．4.8.1 節で用いた実験環境の構成では，ネットワーク内に総務部，経理部，営業部，運営管理部，開発部の 5 部署に加え，サーバセグメントと DMZ セグメントが存在する．この環境において監視対象は，最初の 5 部署とサーバセグメント，すなわち DMZ を除く 6 セグメントのみである．この 6 部署におけるインシデントの発生を想定し，提案システムを適用することによる監視コストとインシデントへの対応開始時間について定量的に評価する．

5.6.1 監視コストの低減

この環境において，DMZ を除く 6 セグメントの監視を行う場合を想定し，まず，提案システムを用いることにより低減可能なネットワークの監視コストを検証する．実験環境において，提案手法を用いずに全てのセグメントを常時監視するために必要な機器コストを比較基準とし，1 とする．また，全てのセグメントにおいて単位時間あたりの通信の流量が同じであると仮定する．ここで，提案システムを用いて監視を行う際に，一度に並列

で監視を行うセグメントの数を並列監視数 $n(1 \leq n \leq 6)$ とする．並列監視数 n が最大値（この場合 6）を取る場合，全てのセグメントを並列に監視できる．従って，$n = 6$ の場合の機器コストは，提案手法を導入しない場合における機器コストと同等の 1 となる．それに対し，n の値を 1 から 5 とする場合，n の値が小さいほど一度に監視するセグメントの数は少なくなり，導入する機器コストは低減可能である．つまり，$n/6$ の機器コストで監視を行うことが可能となる．

5.6.2 インシデント対応の開始時間

次に，提案システムを用いた場合の，インシデントへの対応開始までに要する時間を検証する．インシデントの発生モデルとして，以下の条件を想定する．

- 営業部セグメントの 1 台の端末（192.168.30.12）がマルウェアに感染した．
- マルウェアは，60 分間に 1 回，ランダム時間に C&C サーバ等の名前解決を行う．
- 名前解決を行うドメインはブラックリストに登録されており，3 章の図 3.2 で示した検知システムにより検知が可能である．

ここで，検知やアラートの発生に要する時間は含めず，マルウェアが通信を行った際にアラートが発生した時点以降の所要時間を対象として検証を行う．提案システムが一度に監視を行う監視時間は 10 分間とし，常に同じ順に監視対象を切り替えると想定する．また，提案システムにおける ISL の変更や解析開始までの遅延時間も 0 とする．これらの時間は，インシデント発生時間に比較して極めて小さいため無視できうるためである．

このモデルにおいて，提案システムを用いない場合には，全てのセグメントを常時監視しており，マルウェアの通信を即座に検知し，アラートを出力することが可能である．つまり，提案システムを用いない場合，インシデント対応を開始する時刻は最初にマルウェアが行った通信に対してアラートが発生した時刻となる．

これに対し，提案システムを用いる場合のインシデント対応開始時刻の遅延を評価する．提案システムにおいては，インシデント対応開始時刻は，ISL がレベル 3 となり，解析が開始される時点に相当するため，この時刻までの所要時間を評価する．名前解決に関する検知の場合，マルウェア感染の危険性が高いと判断されるため，提案システムにお

いてはアラートに対して，ISL のレベルを即座に 1 から 3 へと変更し，解析を開始する．従って，提案システムにおいても，マルウェアが行う名前解決を検知でき，アラートが発生した時刻がインシデント対応開始時刻となる．

提案システムでは，並列監視数 n を最大（$n = 6$）として常時全てのセグメントの監視を行う場合，最初にマルウェアが通信を発生させた時刻に検知が可能であり，インシデント対応開始時刻は提案システムを用いない場合と同等である．しかしながら，並列監視数 n が 1 から 5 で巡回監視を行う際には，感染端末が発生した営業部セグメントの監視を行っていない時間帯にマルウェアが名前解決を行う場合に検知が行えず，何回か見逃す可能性がある．見逃しが発生する場合には，マルウェアが行う何回目かの通信を検知できるまでの時間がインシデント対応開始時刻の遅延となる．そこで，見逃す可能性を考慮し，検知するまでに要する時間の期待値を分単位で求める．マルウェアは 60 分間に 1 回の頻度で名前解決を行うため，60 分単位で検知できる確率を離散的に求めることにより，検知するまでに要する時間の期待値を求めた．

まず，並列監視数 n に応じて，60 分間のうちで一つのセグメントを監視できる時間 $Time(n)$ を求める．

$$Time(n) = \left(\frac{60}{\text{セグメント数}} \right) n \tag{5.1}$$

想定するモデルでは監視を行うセグメント数は 6 であるため，$Time(n) = 10n$ となる．$Time(n)$ を用いて，以下の式により検知するまでに要する時間の期待値を求めた．

$$\text{期待値 } E(n) = \sum_{h=0}^{\infty} 60h \left(\frac{Time(n)}{60} \right) \left(1 - \frac{Time(n)}{60} \right)^{h} \tag{5.2}$$

表 5.1 に，並列監視数 n と検知するまでに要する時間の期待値を示す．コスト減に従って，検知するまでに要する時間の期待値も増えているが，より低コストで幅広く検知することが重要であるという状況もあるため，このトレードオフを考慮して，最適なシステム（パラメータ n）を選択すればよい．

5.6.3 考察

前述の評価においては，数値例として，ある特定のマルウェア（インシデント）のモデルを想定した．ここでは，マルウェアの特性が変化すると，提案システムのトレードオフ

表 5.1　並列監視数 n と検知に要する時間の期待値

n	検知に要する時間期待値
1	300 分
2	120 分
3	60 分
4	30 分
5	12 分
6	0 分

（特に検知に要する時間）がどのように変化するかについて議論する．

マルウェアの通信特性については，次のように考える．今回の想定では，ある端末に感染したマルウェアが 60 分間中で 1 回の名前解決を行っている．これに対し，名前解決を行う時間間隔が今回の想定より短い場合には，提案システムを用いた際の検知に要する時間の期待値も小さくなるが，長い場合，検知に要する時間の期待値は長くなってしまう．

一方，実際の標的型攻撃で用いられるマルウェアの感染特性と巡回監視による検出の可能性については次のように考える．標的型攻撃のマルウェアは目的とする情報を窃取するためにネットワーク内で感染を拡大させ，機密情報を保持しているサーバにアクセス可能な端末への感染を目指す．今回は，ネットワーク内感染は起こっていないと仮定しているが，巡回監視を行うセグメント内において，マルウェアに感染し悪性の通信を発生させる端末の台数が今回の想定より多くなる場合には，検知時間の期待値はより短くなることが予想できる．従って，用意する監視機器の数は単純に表 5.1 の数字と機器コストから決定する以外に，感染拡大ステージにおける発見を感染拡大ステージにおける発見を許容することによってより機器数を削減するというトレードオフも選択することができると考える．

5.7　本章のまとめ

この章では，効率的なネットワークの監視および不正通信の解析を行うための管理支援システムについて述べた．検知率を向上させるために，複数の検知システムを組み合わせ

て利用し，それによる弊害である誤検知問題を解決した．監視・解析管理支援システムでは，セグメント内の端末のマルウェア感染可能性を表すための指標である ISL（Infection Suspicious Level）を定義し，ISL の状態に基づいて適切な巡回監視や検知された不正通信の解析を行った．提案システムは，本章で定義した ISL コンセプトを用いることにより，意味のないアラートなどの誤検知を除外して対応が行え，ネットワーク管理者が手動で解析を行うべきアラートの低減が可能である．また，従来手法では選択できなかった，検出コストと検出遅延というトレードオフの選択を実現することができ，簡単なマルウェアモデルを用いて行った性能評価により，このトレードオフを定量的に評価し，有効性を確認した．

第 6 章

インシデント発生時の対応支援

6.1　まえがき

第 5 章では，ネットワーク内部分離設計の特性を利用した効率的な監視，不正通信解析管理の支援手法を提案した．これにより，発生しているインシデントの現在の状況を判断し，状況に応じた適切なタイミングや適切な対象に対して対策を施すことが可能になった．そこで，第 5 章の不正通信解析で得られた結果を基にインシデントへの対策を行うことが必要となる．しかしながら，対策により通信遮断などを行った場合には業務上必要な通信も遮断される可能性もあるため，インシデントによる被害は食い止められたとしても業務活動に大きな影響を与えてしまう可能性がある．本章では，インシデントの状況判断が行われた状況において，複数の対策設計を用意し，対策設計のインシデントに対する有効性および業務活動に及ぼす影響の二つの基準を用いて行った評価により，適切な対策設計をネットワーク管理者に推薦する対策支援手法について述べる．提案手法により，ネットワーク管理者が状況に適した効果的かつ業務への影響の少ない対策設計の選択するための支援が可能である．また，動的ネットワーク構成により選択された対策を適用したネットワークを再構成することにより，インシデントへの対策を容易に行うことが可能となる．

6.2　対策による業務への影響と適切な候補の推薦

第 5 章で述べたように，インシデントが発覚した際には，迅速に状況判断を行い適切な対策を施すことが求められる．何らかの対策を行う場合，既存のフラットなネットワーク構造においては，考えうる対策数が非常に多くなるために，実質的に対策を行うこと自体が困難であるが，第 3 章で述べたような適切なネットワーク内部分離設計が行われたネッ

トワークにおいては，分割された複数のセグメントのうち，ある部署のセグメントを停止する，もしくはアクセス制御を変更し感染端末を切り離すなどのように，様々なパターンの対策を検討することが可能である．

しかしながら，インシデント対策のためのアクセス制御はマルウェアが行う通信の遮断のみならず，業務活動において必要な通信さえも遮断してしまう可能性がある．例えば，2.2.2 節で述べた日本年金機構の情報漏洩事件の事例も含め，感染が疑われる端末の通信を遮断する迅速かつ確実な手段として，LAN ケーブルを抜くといった物理的な対策がしばしば行われる．このような対策の場合，マルウェアが行う不正通信を迅速かつ確実に遮断できる一方で，その他のあらゆる正常通信も行えなくなってしまう．極端な例としては，社内ネットワークの全接続を遮断することでネットワーク内の端末の感染状況がわからずとも全ての不正通信の遮断と感染拡大の防止が可能であり，情報漏洩を防止することが可能である．組織内で扱われている情報の重要度や機密度が非常に高い，もしくはすでに情報漏洩が発生しているといった深刻な状況など，場合によっては必要な手段ではあるが，感染の有無に関わらずネットワーク内の全ての端末が通信を行えず業務活動に多大な影響を与えてしまうため，現実的な対策とは言い難い．インシデントへの対策は，単純に被害を食い止めることだけを行うのではなく，このような業務活動への影響を踏まえた上で最適な対策を検討する必要がある．しかし，実際に検討中の対策により業務にどのような影響を与えるのかを把握するためには，感染端末の使用者や使用状況を調査などが必要である．例えばクライアントの数が 10 台程度の小規模オフィス等であれば，このような調査は比較的短時間で行うことが可能であると考えられるが，本論文が対象としているクライアント数が 100 台程度の規模であれば，調査時間は著しく増大すると考えられる．

一般に，組織内においてどのようなセキュリティ対策を導入すべきかといった議論は様々な検討がなされており，経済的な面も考慮した手法 [46] や，要員数や開発期間などといったプロジェクトの特性を考慮した手法 [47] など様々な手法が存在する．また，ペネトレーションテスト [48] と呼ばれるセキュリティ診断により導入しているセキュリティ対策の有効性の議論などもしばしば行われる．一方で，インシデントが発生した際の対策に関しては，迅速さが優先されるため，その対策による業務上のリスクなどに関しては議論されることは少ない．

これに対し本論文では，インシデント発生時に効果的かつ業務への影響の少ない対策設

計をネットワーク管理者に推薦する手法を提案する．提案手法では，第 4 章で構築した，部門，部局等に応じてネットワークが分離されており，細かいアクセス制御を行うことが可能なクライアント数が 100 台程度の規模のネットワークを想定する．その上で，インシデントが発生した際に対策として制限する通信の範囲が異なる複数のネットワーク設計（以下，対策設計候補と呼ぶ）を用意し，発生しているインシデントの状況に応じて各対策設計候補の対策としての有効性および業務活動へ与える影響を評価し，総合的に評価の高いものをネットワーク管理者に推薦する．これにより，ネットワーク管理者は迅速かつ容易に適切なインシデントへの対応を判断することが可能となる．また，通常のインシデント対応においては，ネットワーク管理者が対策を選定した後，ネットワーク機器の等の設定変更を行う必要があるが，複雑なネットワーク構成においては機器の設定も難しくなり，対応に時間を要する．本論文では，ネットワーク機器のアクセス制御設定を変更し，ネットワーク管理者が選択した対策設計候補を適用したネットワークを動的に構成する．これにより，迅速に対策設計候補の適用が可能となるとともに，対策の変更やインシデント収束後の復旧も容易に行うことが可能である．

6.3　対策設計候補の評価

提案手法では，対策設計候補に対して二つ評価基準を用いた評価を行う．一つ目に，対策設計のインシデントに対する有効性を求める．二つ目に，対策設計が業務活動に及ぼす影響を求める．さらに，攻撃の進行状況に応じてこれら二つの評価基準に対するプライオリティバランスを考慮した上で，総合的な評価を行う．

6.3.1　対策設計のインシデントに対する有効性評価

まずはじめに，発生しているインシデントに対して各対策設計候補の有効性を評価する．本論文では，対策の有効性を算出するために，マルウェアに感染した端末が発生させる有害な通信を対策により遮断可能か否かを指標として用いる．そこで，まず初めに二つのパラメータを設定する．一つ目に，ネットワーク内の端末がマルウェアに感染している可能性を表すパラメータを α とする．二つ目に，ネットワーク内においてマルウェアが行う通信の有害性を表すパラメータを β とする．

【感染可能性：α】

はじめに，組織ネットワーク内に属する全ての端末について，マルウェアに感染している可能性を算出する．しかしながら，第 2 章でも述べたように標的型攻撃は標的専用の手法で行われ同じ攻撃が存在しない上，ネットワーク内の各端末に対するアクセス制御の状況によってマルウェアの通信の行い易さ，感染のし易さが異なるため，組織内の各端末の感染可能性を定式化することは困難である．そこで本論文では，感染が発覚した端末を起点として，その他の端末に関しては感染端末との通信を行う際に中継するネットワーク機器および，セキュリティ装置の数を用いて擬似的に算出する．これは，ネットワーク内部分離設計によるセグメント間のアクセス制御やファイアウォール等による不正通信の遮断が行われるため，中継する機器の数が多いほど不正通信を遮断できる可能性が高まり，マルウェアの感染可能性が低下するためである．

まず，端末のマルウェア感染可能性を α とし，感染が発覚した端末の α を α_0 と定義する．その上で，ネットワーク内の各部署 VLAN，サーバセグメント，DMZ セグメントのそれぞれについて，各セグメントに属している端末の α を計算する．ここでは，中継する機器の数を Via とし，以下の式により感染可能性 α を求める．

$$\alpha = \begin{cases} \alpha_0 & (InfectedHost) \\ \alpha_0 \times \frac{1}{2^{Via+1}} & (Otherwise) \end{cases} \tag{6.1}$$

本論文では中継する機器の数のみを用いて α を求める計算を行ったが，各中継機器に適用されているアクセス制御を考慮し，感染ホストから上記分類の各ホストまでのホップ数等を計算に加味することで，より実際の攻撃に近い値を求められる可能性もある．

【通信の有害性：β】

ネットワーク内の各セグメント間の通信に対して，その通信によってマルウェアによる悪影響があるか否かについて，後述する表のようにパラメータ β $(0 \leq \beta \leq 1)$ をそれぞれに設定する．ここでは，一切影響がないと考えられる通信に対して $\beta = 0$ を，またマルウェアによる悪影響が懸念され，遮断することが好ましい通信に対して 0 以外の値を β に対して設定する．ただし，攻撃の侵入段階を表す緊急性 E に応じて β の値は変化する．侵入段階とは，インシデントの状況判断の結果，マルウェアによる悪意ある通信が第 2 章で述べた攻撃の過程のどの段階にあてはまるかを示す．緊急性 E は，最も初期の場合の内部への侵入の場合を 1，最終段階である情報送出の場合を 5 として 1 から 5 の値を設定

する．よって，本論文では以下のように β を設定する．

- E=1: 組織内部への侵入
  この段階では，標的型メール攻撃など，様々な手法を用いて組織内部にマルウェアが侵入する．提案手法はマルウェアに侵入された後の対策にフォーカスしているため，この段階は考慮しない．
- E=2: 攻撃者との通信
  マルウェアは攻撃者の C&C サーバ等と通信を行うことにより，攻撃者からの指令や新たなマルウェアをダウンロードする．この段階では，感染ホストとその通信先 (C&C サーバ等) に対して最も高い β の値を設定する．また，C&C サーバは複数バックアップが存在する場合があるため，感染ホストとインターネットとの通信に対して低い β を設定する．
- E=3: 組織内部でのマルウェア拡散
  組織内部へ侵入したマルウェアは，組織内部で侵食を行っていく．この段階では，マルウェアは組織内の他の端末に対する自身のコピーの配布や，組織内部の認証サーバ等への侵入，ファイルサーバへの必要な認証情報の調査等が行われる．そのため，感染ホストからすべてのホスト，サーバに対する通信に対して高い β の値を設定する．このようなマルウェアの侵食は情報窃取のためのアクセス権の奪取やマルウェア間の伝令網の構築が目的であるため，組織内部を中心に行われる．そのため，DMZ の端末に関しては組織内部の端末に比べて情報偵察やマルウェアの侵食の可能性が低いため，低い β の値を設定する．
- E=4: サーバ等の重要機器からの情報窃取
  この段階では，マルウェアは重要な情報が保管されたサーバ等に対して侵入し，機密情報の窃取等が行われる．そのため，感染ホストと情報が保管されたサーバ間の通信により影響が発生する．よって，この通信に対して最も高い β の値を設定する．
- E=5: 外部への情報送出
  マルウェアは窃取した機密情報等を外部の攻撃者側に送出する．そのため，感染ホストと情報の送出先との通信によって影響が発生する．よって，この区間に最も高い β の値を設定する．また，機密情報がすでにマルウェアに窃取されているため，

情報流出を防ぐために感染ホストからインターネットおよびDMZへの通信についても同様に最も高い β の値を設定する．

対策の有効性

マルウェア感染可能性 α および通信の有害性 β を用いて，対策設計候補の有効性 P_{Effect} を求める．はじめに，ネットワーク内の各通信に対して重み $Weight$ を設定する．β に0以外の値が設定されている場合，その通信はマルウェアによるなんらかの影響があると考えられる．このような通信に対しては，送信元ホストの α と β の積とする．

$$Weight = \alpha \times \beta \quad (\beta > 0) \tag{6.2}$$

さらに，$\beta > 0$ の場合の $Weight$ の和を $W_{Positive}$ として求める．

$$W_{Positive} = \sum_{\beta>0} Weight \tag{6.3}$$

また，$\beta = 0$ となる通信区間の数を N_{Zero} とし，以下の式により Weight を均等に与える．

$$Weight = \frac{W_{Positive}}{N_{Zero}} \quad (\beta = 0) \tag{6.4}$$

これらの Weight を元に，各設計候補の有効性を求める．この際，マルウェアにより影響があると考えられる通信が遮断できているか否かの判定を行い，設計のスコアを決定する．また，これに加え影響のない通信は可能な限り継続させるべきであるため，これも判定基準に加え，以下の式により有効性 P_{Effect} を算出する．

$$P_{Effect} = \sum_{\beta>0 \ \&\ blocked \ or \ \beta=0 \ \&\ non-blocked} Weight \tag{6.5}$$

6.3.2 対策設計が業務活動に及ぼす影響評価

次に，各対策設計候補をネットワークに適用した際に，業務活動に与える影響を評価する．ここでは，対策設計候補が業務活動に与える影響の度合いを影響度 P_{Impact} と定義する．一般的には，企業内のユーザはその役職に応じて情報へのアクセス権限が与えられる．また，より役職が高い人間ほど責務や業務上の判断権限等も多く，通信が遮断された場合に業務に与える影響も大きい．そこで本論文では，企業内ユーザの役職を用いて影響

度計算を行う．影響度計算のために企業内の各役職に対して重要度を設定する．重要度は高位の役職ほど大きな値をとり，非負の値とする[*1]．ここで，ある部署 i における役職を表す $Role_i$ について，その重要度を返す関数を GI と定義する．影響度は，部署に属する人間の役職の重要度の和とし，各役職ごとの人数は考慮しない．これは，一般的に，低位の役職ほど人数が増えるため，影響度に役職ごとの人数を反映すると，重要度よりも人数の方が影響度の算出に大きく作用する悪影響が想定されるためである．以上より，以下の式により影響度 P_{Impact} を求める．

$$P_{Impact} = \sum_{i} CI \times GI(Role_i) \tag{6.6}$$

ここで，係数 CI はサーバと通信ができないなどといった通信の状態に応じて変化するものとする．

6.3.3 対策設計の総合評価

行われている攻撃の種類や侵攻状態に応じて，最適な対策は変化する．例えば，攻撃が初期の段階であれば，不必要な通信遮断を無意味に数多く行うのではなく，最低限の通信遮断によって可能な限りの業務継続を目指すべきである．また，攻撃によって情報漏洩が行われようとしてる，もしくはすでに行われているなど，最終的な段階まで進行している場合には，業務継続よりも情報漏洩の防止を優先すべきである．

このように，セキュリティと可用性はマルウェアの侵攻状態に応じて優先度が変化する．そこで，侵攻が進んでいる，つまり緊急性 E の値が大きいほど業務への影響の割合を小さくすべきであるため，業務影響度 P_{Impact} を $1/E$ 倍し，以下の式により総合的な結果を判定する．

$$P_{Total} = P_{Effect} - \frac{1}{E} \times P_{Impact} \tag{6.7}$$

[*1] 業務を妨害する役職がないことを仮定している．

6.4　対策設計推薦システム

提案手法を用いて，インシデント発生時において複数の対策設計候補を生成し，管理者に候補を推薦するための対策設計推薦システムを作成した．

6.4.1　システム構成

図 6.1 に対策設計推薦システムの構成を示す．以下，システムの流れを説明する．

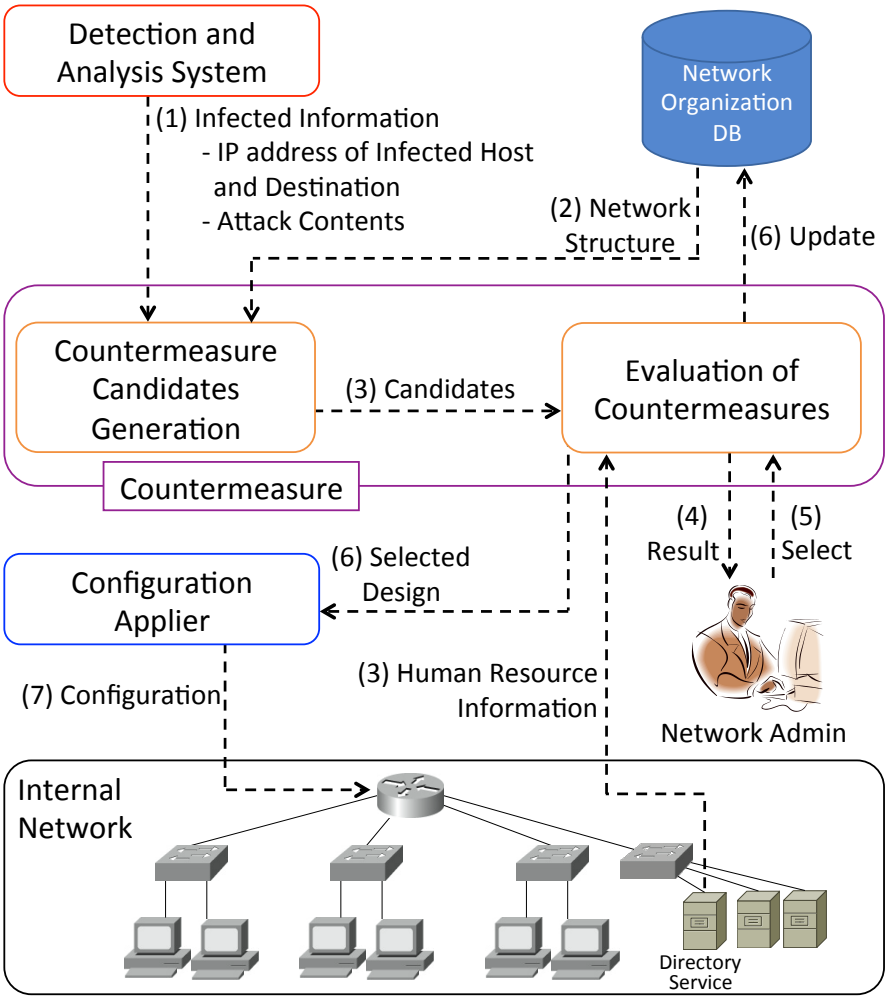

図 6.1　対策設計推薦システム

1. 第 5 章で述べた監視・解析管理支援システムの ISL Manage モジュールがインシデントの状況判断を行い，対策が必要な状況であると判断した場合に感染情報を通知する．感染情報には，感染ホストの IP アドレス，マルウェアによる悪意ある通信の宛先 IP アドレス，およびマルウェアの侵入段階が含まれる．対策設計推薦システムでは，対策候補自動生成モジュール（Countermeasure Candidates Generation）がこの通知を受け取る．
2. 対策候補自動生成モジュールは受け取った感染情報に加え，3.4 節で述べたシステムのネットワーク構成データベースより，ネットワーク情報として組織内部ネットワークに属するサーバ，クライアント，ネットワーク機器，およびそれぞれの IP アドレス，VLAN およびネットワークアドレス，各端末間の L3 接続関係を取得する．これらの情報により，複数の対策設計候補を作成する．
3. 作成された対策候補は設計候補評価モジュール（Evaluation of Countermeasures）が受け取り，ネットワーク情報および，従業員情報として各端末を扱う従業員やその所属，役職をディレクトリサービスサーバから取得し，各候補の評価を行う．
4. 評価結果はネットワーク管理者へと通知される．
5. ネットワーク管理者は状況に応じて最も適切な候補を選択する．
6. 設計候補評価モジュールは選択された対策候補の情報をネットワーク構成データベースに登録し，選択された対策候補をネットワーク自動設定モジュール（Configuration Applier）へと入力することで，最終的に物理ネットワークに対して設計を反映させる．

6.4.2 対策設計の自動生成機能

第 5 章で述べた監視・解析管理支援システムが出力する感染情報と，ネットワーク構成データベースより取得したネットワーク情報を用いて，対策候補自動生成モジュールでは新たなアクセス制御を行った 9 パターンの設計を対策設計として生成する．本来はシステムが生成する 9 パターン以外にも様々な設計が考えられる．しかしながら，迅速な対応が求められている状況にもかかわらず，大量の候補を提示することによりネットワーク管理者は複雑な判断が求められ判断が困難となってしまう．また，それら全てを網羅した場合

には計算量が膨大となってしまい，対策候補をネットワーク管理者に提示するまでに長時間の計算が必要となるため，提案システムが想定しているような初動の緊急対応には適さない．そのため，提案システムは以下に示す 9 パターンを対策設計候補として生成する．

1. 「感染端末」と「悪意ある通信の宛先」を遮断
   感染端末と悪意ある通信の宛先の間の通信のみを遮断することにより，検知された悪意ある活動は抑止可能であり，業務への影響も最小限となる．ただし，検知された感染端末以外は悪意ある通信の宛先との通信が継続しているため，マルウェアが侵食していた場合は被害が出る可能性がある．
2. 「感染端末」と「悪意ある通信の宛先の VLAN」を遮断
   感染端末と，悪意ある通信の宛先と同じ VLAN に属するすべての機器との通信を遮断するため，通信先の端末のみならず関連する端末の安全性も高められる．しかし，感染端末は悪意ある通信の宛先の VLAN に関連する業務に大きな影響を受ける．
3. 「感染端末」と「すべての端末」を遮断
   感染端末を完全に切り離してしまう設計である．感染端末に関する業務への影響が非常に大きい．
4. 「感染端末 VLAN」と「悪意ある通信の宛先」を遮断
   感染端末が所属する VLAN 内の端末は感染端末と直接通信可能であり，マルウェアに感染している危険性が高い．そのため VLAN 全体からの通信を遮断することで悪意ある通信の宛先端末の安全性を高めることが可能である．
5. 「感染端末 VLAN」と「悪意ある通信の宛先の VLAN」を遮断
   関連する VLAN 同士の通信を制限する．これにより安全性は高いが，感染端末が属する VLAN は悪意ある通信の宛先の VLAN に関する業務に大きな影響を受ける．
6. 「感染端末 VLAN」と「すべての端末」を遮断
   感染端末が属する VLAN 全体を切り離す設計である．これにより，感染の危険性が高い端末を切り離せるが，VLAN 全体が業務への影響を受ける．
7. 「すべての端末」と「悪意ある通信の宛先」を遮断
   標的を隔離するパターンである．悪意ある通信の宛先の端末の保護は可能である

が，これに関連する業務に対してネットワーク全体で影響を及ぼす．

8.「すべての端末」と「悪意ある通信の宛先の VLAN」を遮断
悪意ある通信の宛先とその VLAN に属するすべての端末を隔離する．これにより，悪意ある通信の宛先に関連する他の端末の安全性も高まるが，業務に与える影響は大きくなる．

9.「すべての端末」と「インターネット」を遮断
外部へ情報を送出しないために最も安全な設計であるが，外部と通信する必要があるあらゆる業務に影響を与える．

6.4.3　対策設計候補の評価

インシデントの対策のために 9 個の設計候補が生成される．これらの各対策設計候補について，6.3 節で述べた提案手法を用いて評価を行う．これにより，各候補の評価結果を用いて順位付けを行い，上位の候補を管理者に推薦する．

6.5　対策設計推薦システムの実装

対策設計推薦システムにおける対策候補自動生成モジュールおよび，設計候補評価モジュールの実装を Java を用いて行った．図 6.2 は実装したシステムの構成図を示す．Java プログラムにより実装された対策候補自動生成機能および対策候補評価機能がサーバ上で実行され，評価結果および感染情報が出力される．この結果を用いて，Apache サーバ上の PHP により出力画面が生成される．ユーザは Web ブラウザを介して出力結果を確認可能である．また，出力結果のうちの対策設計候補の詳細については，クライアントの Web ブラウザ上で JavaApplet を用いて出力される．

実装した二つのモジュールと，企業において開発されたネットワーク自動設定システム [49][50] を用いて，小規模の実験用ネットワークにおいてインシデントを想定した検証実験を行った．図 6.3 に，実験を行ったネットワーク環境を示す．

この環境では，二つのクライアント向けセグメントに 4 台の端末が属し，それぞれの使用者として 2 名の従業員，1 名の課長，1 名の部長を配置している．また，サーバセグメントに 4 台のサーバとしてデータベースサーバ，ファイルサーバ，ActiveDirectory サー

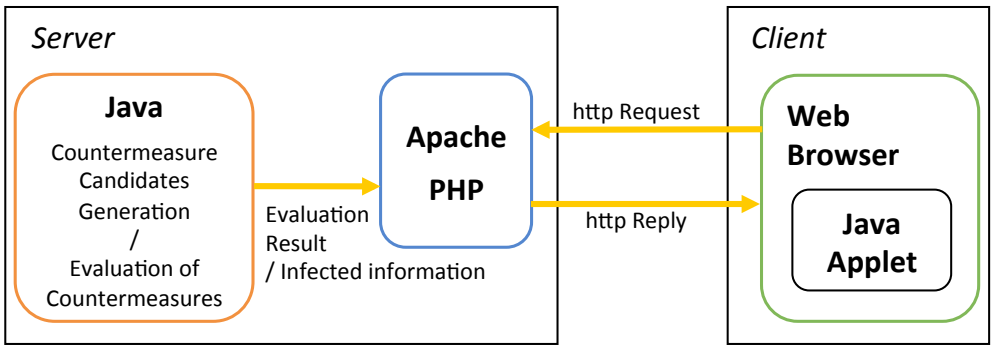

図 6.2　実装構成図

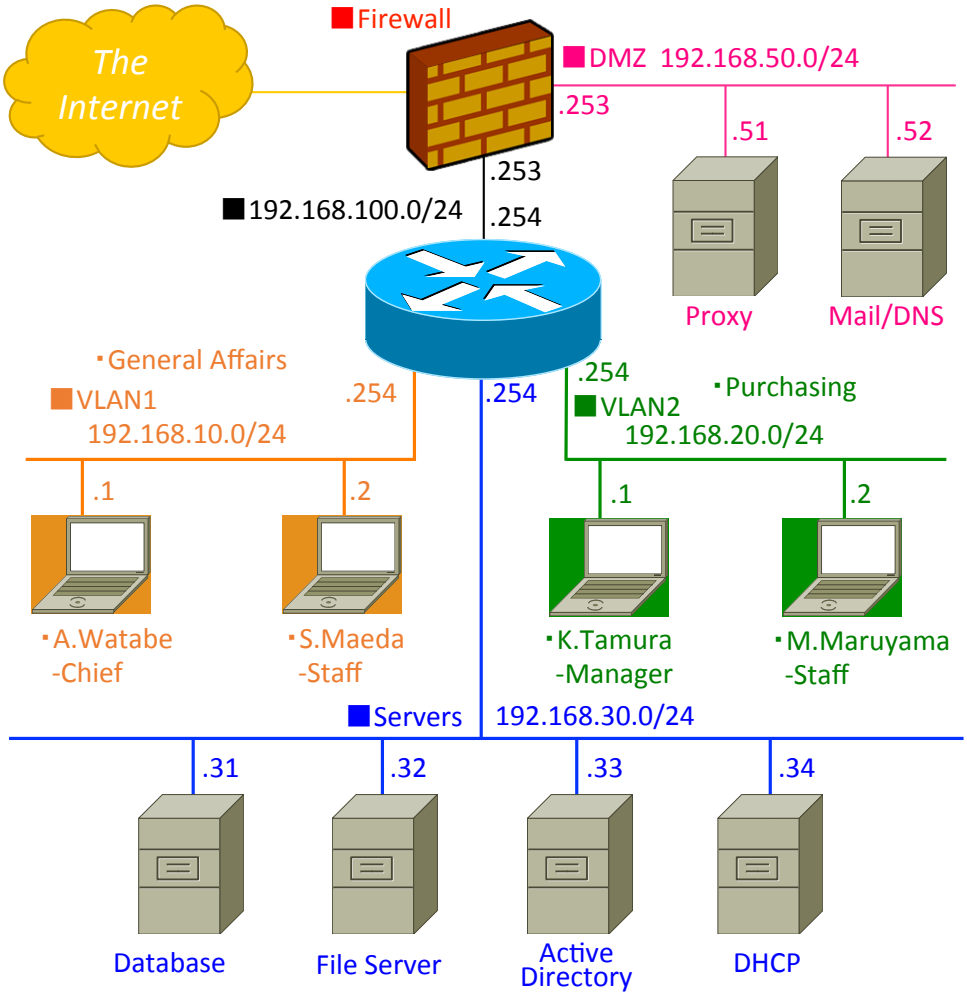

図 6.3　実験環境

表 6.1　情報窃取段階の β

Source \ Destination	標的サーバ	インターネット	DMZ	サーバ VLAN	その他 VLAN	感染端末 VLAN	感染端末
感染端末	1	0	0	0	0	0	N/A
感染端末 VLAN	0	0	0	0	0	0	0
その他 VLAN	0	0	0	0	0	0	0
サーバ	N/A	0	0	N/A	0	0	0
DMZ	0	0	0	0	0	0	0

バ，DHCP サーバを配置し，DMZ セグメントに 2 台のサーバとしてプロキシサーバおよびメール・DNS サーバを配置している．

実装したシステムにおけるパラメータの設定として，$\alpha_0 = 1$，マルウェアによるサーバからの情報窃取段階の β を表 6.1 に示す通り，それぞれ設定した．表 6.1 は，マルウェアが目的の情報が保存された重要サーバから機密情報を窃取している段階であるため，他のサーバや端末等への攻撃等はないと仮定し，感染端末から標的サーバへ対する通信にのみ，最大値を与える設定としている．また，組織内の各使用者の役職とその重要度を表 6.2，CI の値を表 6.3 に示す．

表 6.2　役職とその重要度

使用者	役職	t	重要度
前田幸子	従業員	0	1
丸山麻衣	従業員	0	1
渡部亮	課長	1	2
田村賢一	部長	2	3

組織内の役職の重要度は，1 人あたりの部下の平均人数とし，以下の式 (6.8) を用いて設定した．ここでは，役職を表す変数を t とし，N_t は組織内において役職が t である社員の総人数を表す．

$$\text{役職 t の重要度} = \frac{\sum_{i=0}^{t-1} N_i}{N_t} \tag{6.8}$$

表 6.3　係数 CI

通信の状態	値
他の全てと通信不可	1
インターネット又はサーバと通信不可	0.5
その他	0

ただし，最も低い役職 $t = 0$ の場合，その役職の重要度は 1 とする．これにより，本論文の実験環境においては，最も低い役職である従業員の重要度が 1，課長が 2，部長が 3 となる．

係数 CI は，一つの部署がインターネット，DMZ，内部サーバセグメントなど通信する必要があるネットワークセグメント数に対し，通信が行えなくなるセグメント数の割合で算出する．本論文の実験では，DMZ と内部サーバセグメントが実際には一つのサーバセグメントで構成されている悪条件を想定した．この条件下で，ある部署がインターネットとサーバセグメントの両方との通信を遮断された場合は $2/2 = 1$，いずれか一方が遮断された場合は $1/2 = 0.5$，遮断がない場合は $0/2 = 0$ となる．

6.6　評価

6.5 節で例示した組織と組織内ネットワークおいてインシデントの発生を想定し，想定した状況をマルウェア解析結果としてインシデント対応支援システムに通知する条件のもとで，検証実験を実施した．以下，実験について述べる．

6.6.1　検証実験

実験 1

実装した提案システムと実験用ネットワーク環境を用いて，以下の場合を想定した実験を行った．

- IP アドレスが 192.168.10.2 の端末がマルウェアに感染した
- 感染した端末は，IP アドレスが 192.168.30.32 のファイルサーバに悪意ある通信をしている
- 悪意ある通信の内容 (侵入段階) は，サーバからの情報窃取である

実際にインシデント対応支援システムを実行し，Web ブラウザを用いて結果を確認すると，まず始めに図 6.4 に示す画面が表示される．ここでは，感染端末の情報，通信先の

図 6.4　システム実行例

情報，侵入段階，および対策設計の候補を提示する．この際，9 パターンの対策設計候補のうち，評価結果の上位 4 候補を提示している．各候補を選択すると，リンク先画面にお

いて候補を確認可能である．図 6.5 にリンク先画面上に表示される JavaApplet の画面の一例を示す．

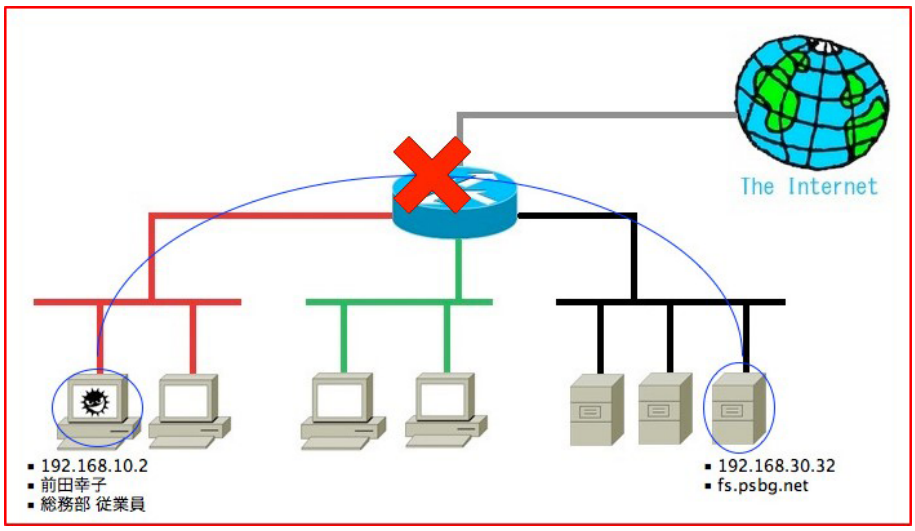

図 6.5　対策設計候補 1

以下，実行結果として出力された候補を説明する．

- 候補 1(自動生成パターン 1)

  図 6.5 で示した候補である．感染端末と通信先サーバの通信を制限する設計である．これにより，マルウェアによる情報窃取を阻止することが可能である．ただし，検知された感染端末以外に，このマルウェアと同様に情報窃取の役割を持つマルウェアが感染した端末が存在する場合，情報窃取が継続される可能性がある．この設計では，感染端末は通信先サーバが必要な業務に対して影響が及ぶ．
- 候補 2(自動生成パターン 2)

  感染端末とサーバセグメントの通信を制限する設計である．感染端末はサーバセグメントに属するすべての端末と通信不可となる．これにより，今回検知された悪意ある通信の宛先であるファイルサーバ以外のサーバも保護される．ただし，感染端末は ActiveDirectory との通信が不可能となり，使用者には大きな影響が出る．感染端末以外の端末は業務継続が可能であり，影響は少ない．
- 候補 3(自動生成パターン 4)

  感染端末が属する VLAN1 のすべての端末と，通信先サーバとの通信を制限する設

計である．感染端末以外の端末を利用した情報窃取も抑止できるため，安全性の高い設計と考えられる．ただし，感染端末が属する VLAN 内のすべての端末において通信先サーバが必要な業務に対して影響が及ぶため，感染端末のみの場合と比べて業務への影響は大きくなる．

- 候補 4(自動生成パターン 5)
  感染端末が属する VLAN1 のすべての端末と，サーバセグメントの通信を制限する設計である．候補 3 に比べ，ファイルサーバ以外のサーバも保護されるため，より安全性が高い設計となる．ただし，VLAN1 のすべての端末が ActiveDirectory と通信不可となるため，業務に対する影響は非常に大きくなる．

実験 2

実験 1 と同様の環境において，想定する感染端末を 192.168.20.2 に変更し，再度実験を行った．その結果，候補 1 から候補 3 までは実験 1 と同様の結果が得られ，候補 4 のみ異なる結果が得られた．

- 候補 4(自動生成パターン 3)
  感染端末を切り離し，他の全ての端末との通信を制限する設計である．感染端末に感染したマルウェアによる，他の端末への活動を完全に遮断することが可能である．ただし，感染端末は通信を必要とする業務が一切行えなくなる．

考察

実験 1 と実験 2 の結果より，各候補は感染端末のマルウェアによる情報窃取を確実に抑止しつつ，検知された以外のマルウェアの脅威も考慮した設計である．また，業務への影響を小さく留めることが考慮された推薦の順位となっていることがわかる．特に，実験 1 と実験 2 において候補 4 の設計が異なった点について考察すると，実験 1 の候補 4 では VLAN1 に属するすべての端末がすべてのサーバと通信不可となっている．この場合，感染端末以外に影響を受ける端末の使用者の役職は課長である．しかしながら，実験 2 において同じ設計を行った場合，感染端末以外に影響を受ける端末の使用者の役職は部長であ

るため，実験 1 に比べ業務への影響が大きくなると考えられる．表 6.4 は，実験 1 と実験 2 における対策設計候補パターン 1 からパターン 5 の P_{Total} の結果を表している．なお，パターン 6 からパターン 9 は上位 4 候補以内には入らなかったため割愛する．実験 1 ではパターン 5 が候補 4 となっているが，実験 2 ではパターン 5 の業務への影響が大きく，P_{Total} の数値が減少してしまうため，パターン 3 が候補 4 となり，実験 1 と実験 2 ではパターン 3 とパターン 5 の順位が入れ替わっていることがわかる．よって，実験 2 の結果ではより業務への影響が少ない感染端末の切り離しが推薦されている．

表 6.4　実験結果 (P_{Total})

	実験 1	実験 2
パターン 1	1.83	1.83
パターン 2	1.77	1.77
パターン 3	1.27	1.27
パターン 4	1.47	1.30
パターン 5	1.34	1.17

6.6.2　被験者実験

実験 1，実験 2 と同様の環境において実際にインシデントの発生を想定し，システムを用いて提示された対策候補の中から適切なものを選択するまでの判断時間と，システムを用いずに手作業で感染端末の切り離し等の対策を立案，決定するまでの判断時間をそれぞれ計測した．ただし，どのような対策を講じるかは被験者の主観により異なるため，決定したネットワークの差異については評価の対象とせず，対策を決定するまでの経過時間を比較した．

被験者

提案システムはネットワークの管理を行っているネットワーク管理者が使用することを想定しているため，被験者は著者が所属する研究室内でネットワークに関連した研究を行っており，ネットワークに関する一定の知識を有する大学院生 5 名とした．

実験方法

以下の方法により，システムを利用する場合と利用しない場合の判断時間をそれぞれ 5 回ずつ計測した．

- システムを利用する場合
  インシデントが発生し，マルウェア解析が終了した状況を想定し，対策候補自動生成モジュールに感染情報を通知した時点を計測開始とする．システムは対策候補の生成，各候補の評価を行った上，被験者に通知する．被験者は通知された各候補を確認し，適切だと判断した候補を選択した時点で計測終了とする．
- システムを利用しない場合
  システムを利用する場合と同様に，マルウェア解析が終了した状況を想定し，感染情報を被験者に通知した時点を計測開始とする．被験者はあらかじめネットワーク構成を知らされているが，端末の使用者等の情報は知らされない．被験者は知らされていない情報で判断に必要な情報があれば，その項目を質問できることとした．被験者が適切だと考える対策を決定し，それを宣言した時点で計測終了とする．

計測結果および考察

実際に判断時間を計測した結果を表 6.5 に示す．なお，結果は 5 名の被験者がそれぞれ 5 回の実験を行ったすべての平均時間，5 名の中での最短時間と最長時間を示す．

表 6.5　実験結果 (対策決定に要する時間)

	システム利用	手動
平均時間	1 分 27 秒 5	2 分 5 秒 5
最短時間	0 分 30 秒 7	0 分 22 秒 4
最長時間	2 分 58 秒 3	8 分 1 秒 6

まず，システムを利用する場合とそうでない場合とで平均時間を比較すると，システムを利用する場合の方が短時間で判断が行われている．しかしながら，システムを利用しない場合は最高値と最低値の差からもわかるように，被験者によって判断時間が大きく異な

り，一概にシステムを利用した方が短時間で判断可能であったわけではない．それに対し，システムを利用した場合には全実験を通して比較的安定して短時間で判断が行えていた．

実験で用いたネットワークは小規模のものであり，実験結果からも手動での対策設計は容易であると言える．一方，対象とするネットワークの規模が大きくなれば，提案システム，手動のいずれも対策の設計にかかる時間は増加する．

例えば，10 個の部署セグメントに平均 10 台ずつの端末が接続された規模のネットワークで考察する．実験と同様に，部署間の通信は平常時も遮断されており，部署セグメントからはインターネットとサーバの 2 セグメントにしか通信できない環境であれば，通信状況を把握し，対策を検討せねばならないセグメント間の数は 5 倍となる．実験に比べ，1 セグメントの端末数が増加しているが，セグメントあたりで対策決定までの所要時間は変化しないと仮定すれば，全体の対策決定までにかかる時間も 5 倍の 7 分 17 秒 (システム利用)，10 分 27 秒 (手動) となり，その差が広がる結果となる．さらに，手動では状況把握と対策候補の立案までも手作業を求めるが，提案手法ではこれらの作業を自動化するので，所要時間の差はさらに拡大すると考えられる．

また，本論文の実験では対策を決定するまでの判断時間のみを計測したが，実際には提案システムは自動的にネットワーク機器の設定を行うのに対し，手動の場合には設定に必要な時間を加わるため，システムの利用の有無による対策に必要な時間はさらに差が生じると考えられる．

以上より，提案システムは迅速なインシデントへの対応に大きく貢献できるものであると考えられる．

6.7　本章のまとめ

この章では，インシデントが発生した際に，業務への影響と対策の有効性を考慮し，状況に応じた対策候補をネットワーク管理者に推薦するインシデント対策支援手法について述べた．提案システムにより，業務への影響を最小限に留めつつ，より迅速かつ効率的にインシデントに対して適切な対応を行うことが可能となる．実験用ネットワークにおける評価実験の結果，提案システムを用いることにより短時間でインシデント対応の判断が行えるという結果が得られ，インシデント対策支援システムの有効性が示された．

第 7 章

結論

本論文では，状況に応じてネットワークを動的に構成することにより，昨今の巧妙化するサイバー攻撃への対策支援を可能とする研究について述べた．本研究の技術により，ネットワーク管理者によるサイバー攻撃への対策が容易に行えるようになり，昨今の対策が難しい巧妙化するサイバー攻撃による情報漏洩等の被害を防止する一助となる．

第 2 章では，サイバー攻撃の遷移や昨今の深刻な状況について述べた．昨今では標的型サイバー攻撃と呼ばれるように，特定の攻撃対象から情報窃取などを行うため深刻な情報漏洩被害などが発生する．広く世間の話題となった事例をいくつか紹介したが，そのどれもが非常に巧妙な手口で行われており，従来のセキュリティ対策だけでは被害を防止することは難しい状況にある．また，この章では従来のセキュリティ対策や，現在の一般的な組織内ネットワークの構造について，それらの問題点を議論した．

第 3 章では，本論文における提案手法である動的ネットワーク構成によるサイバー攻撃支援手法について述べた．この手法では，組織内部のネットワークを動的に再構成することで，攻撃による被害低減を目指したネットワークの構築およびその監視や解析，また攻撃への対策を支援するためのものである．本手法を用いることにより，一般的に採用されるネットワーク構造とは異なる，攻撃への対策が行い易いネットワークを容易に構築可能となる．また，ネットワークの監視や不正通信の解析の管理を行うことで，効率的にこれらの運用が行えるように支援することが可能である．加えて，インシデントが発覚した際にも，感染端末の切り離し等の設計を迅速に適用可能となり，サイバー攻撃による被害低減が期待できる．

第 4 章では，サイバー攻撃への対策が行ない易いネットワーク構造であるネットワーク内部分離設計の構築支援手法について述べた．組織内部のネットワークを複数のセグメントに分割し，不必要な通信を遮断するアクセス制御を行うこの手法は，その構築が困難で

あるという問題があった．本論文では，ネットワーク内のディレクトリサービスよりユーザのファイルへのアクセス権限を取得することで，ネットワーク内部分離設計を容易に構築出来ることを可能にした．提案手法を用いて小規模ネットワークにおいて行った実験では，被験者が手動で構築する場合に比べて短期間でネットワークを設計可能であることを確認した．また，被験者が生成したネットワーク設計には冗長なアクセス制御などが含まれていたが，システムを用いた場合には不必要なアクセス制御を生成することがないため，より適切なネットワーク設計を適用できることを確認した．

第 5 章では，ネットワーク内の通信監視および，不正通信の解析を効率的に行うための管理支援手法について述べた．通常のネットワーク監視は監視対象トラフィックが膨大でコストも大きいため，提案手法では監視対象を順次切り替える巡回監視を適用し，監視対象や時間を細かく管理することでコスト低減および効率的な不正通信の検知を可能とした．また，検知した不正通信を逐一解析することなく，感染の疑いが強いものを順次解析することにより，不正通信が誤検知に紛れて対応が遅れることがなく，深刻な被害を防ぐことも期待できる．

第 6 章では，ネットワーク内で発生したインシデントに対する対策設計の適用するため，複数の対策設計候補を生成し，状況に応じて適したものを推薦する対策支援について述べた．従来はセキュリティ対策を行うことによる業務活動に対して生じるリスクや被害は考慮されてこなかったが，提案手法は業務活動への影響を評価の際に加味することによって，インシデントへの適切な対応を行いつつ，業務活動への影響も可能な限り生じないインシデント対応が行えることを可能とした．また，被験者を交えて行った評価実験においても，対策設計の選択，決定時間が提案手法を用いることで低減可能な結果が得られたため，より迅速な対応が期待できる．

本論文で述べた手法では，社会問題となっている近年の高度化するサイバー攻撃にフォーカスし，ネットワーク管理者によるサイバー攻撃への対策の負担を軽減することが可能である．本手法では，インシデント発生前のネットワーク構成から，インシデント発生時の対策によるネットワーク再構成までを含めて，包括的なセキュリティ対策支援を行うことで，サイバー攻撃による被害低減が期待できる．本手法はネットワーク管理者の支援を目的とした研究であるため，使用する不正通信検知システムや，解析システムは様々な手法が利用可能であり，セキュリティ対策としての多層防御をより一層強化することが

可能である．

本研究の将来的な発展として，提案システムに擬似的な攻撃を入力してサイバー攻撃対策演習に用いることによる，実際にインシデントの対応を行うネットワーク管理者の育成や，運用のための仕組みづくりが挙げられる．セキュリティ人材の不足は以前より危惧されている問題である．本手法においては，評価実験により被験者の学習効果が期待できることもわかったため，これを活用した仕組みづくりにより，より的確な判断を行えるセキュリティ人材育成の一助となることも期待される．また，ネットワークの規模によっては末端までの管理が不十分となることや，ネットワーク管理者が本当に通信制限を行って良いのか等の判断が難しくなるため，部局ごとのセキュリティ対応者の選定など，提案手法を用いる場合も含め体制作りを的確に行うことがセキュリティ的により強固なネットワークを構築していくことに繋がると考えられる．

謝辞

本博士論文の主査として多数の貴重なご意見を頂きました名古屋大学情報基盤センターの村瀬勉教授に深く感謝致します．

本研究を行うにあたり，修士課程時代からこれまで様々なご指導，ご助言を頂き，また本博士論文の副査をお引き受け頂きました国立情報学研究所の高倉弘喜教授に心より深く感謝致します．

本研究を行うにあたり，英語論文の添削など様々なご指導を頂き，また本博士論文の副査をお引き受け頂きました名古屋大学情報基盤センターの嶋田創准教授に深く感謝致します．

本研究を行うにあたり，日常の研究活動において様々なご意見を頂きました名古屋大学情報基盤センターの山口由紀子助教に深く感謝致します．

ご多忙中にもかかわらず，本博士論文の副査をお引き受け頂き，貴重なご意見を頂きました名古屋大学大学院情報科学研究科の高田広章教授に感謝いたします．

本研究を行うにあたり様々な貴重なご意見を頂きました東京電機大学情報環境学部の八槇博史教授に深く感謝いたします．また，本研究の基盤となる知識を身につける機会となりました，修士課程時代に参加したインターンシップにおいて様々なご指導，ご助言をいただきました新麗様をはじめ株式会社 IIJ イノベーションインスティテュート技術研究所の皆様，長崎県立大学情報セキュリティ学科の加藤雅彦教授に感謝致します．

学部生時代に研究室に所属させて頂き，論文の添削や博士課程進学へのご助言などの様々なご指導，修士課程進学後もご助言，ご協力を頂きました名古屋工業大学大学院工学研究科の高橋直久教授，片山善章教授，立岩佑一郎助教に感謝致します．

修士課程時代に，先輩として研究活動について様々なご助言を頂きました東京農工大学工学研究院の北川直哉助教，また日常の研究活動においてともに議論し研鑽した同期の皆様に感謝致します．

学会出張や実験機材購入の手続きなど様々なご協力をいただきました，前技術補佐員の森山さくら様，事務補佐員の坂口潤子様に感謝いたします．また，評価実験の協力など多くの支援を頂きました村瀬・嶋田研究室の皆様に感謝いたします．

最後に，本研究を行うにあたり長い間支えて頂いた家族の皆様に感謝致します．

発表論文リスト

（1）主論文に関連する論文

- 学術雑誌論文（査読付き）
  - 長谷川皓一，山口由紀子，嶋田創，高倉弘喜，
    “ディレクトリサービス情報とトラフィックデータによる自動 ACL 生成システム，”
    電子情報通信学会論文誌，Vol.J100-D，No.3，pp.353-364，2017.
  - 長谷川皓一，山口由紀子，嶋田創，高倉弘喜，
    “標的型攻撃に対するインシデント対応支援システム，”
    情報処理学会論文誌，Vol.57，No.3，pp.836-848，2016.
- 国際会議発表論文（査読付き）
  - Hirokazu Hasegawa，Yukiko Yamaguchi，Hajime Shimada，Hiroki Takakura，
    “An Automated ACL Generation System for Secure Internal Network，”
    The 6th IEEE International Workshop on Network Technologies for Security, Administration and Protection (NETSAP2016)，
    10.1109/COMPSAC.2016.54，pp.559-564，2016.
  - Hirokazu Hasegawa，Yukiko Yamaguchi，Hajime Shimada，Hiroki Takakura，
    “An Incident Response Support System Based on Seriousness of Infection，”
    The 30th International Conference on Information Networking (ICOIN2016)，
    10.1109/ICOIN.2016.7427090，pp.69-74，2016.
  - Hirokazu Hasegawa，Yukiko Yamaguchi，Hajime Shimada，Hiroki Takakura，

“A Countermeasure Recommendation System against Targeted Attacks with Preserving Continuity of Internal Networks，”
The 38th IEEE Annual International Computers，Software and Applications Conference (COMPSAC2014)，
10.1109/COMPSAC.2014.63，pp.400-405，2014.

- 国内研究会等発表論文（査読なし）
  - 長谷川皓一，山口由紀子，嶋田創，高倉弘喜，
    “ディレクトリサービス情報とネットワークトラフィックを用いた内部分離ネットワーク構築手法，”
    コンピュータセキュリティシンポジウム 2015 論文集，3E3-3，pp.1221-1228，2015.
  - Hirokazu Hasegawa，Yukiko Yamaguchi，Hajime Shimada，Hiroki Takakura，
    “Proposal of a Network Control System to Detect, Analyze and Mitigate Targeted Cyber Attacks，”
    電子情報通信学会技術報告，Vol.113，No.240，IA2013-26，pp.1-6，2013.
  - 長谷川皓一，山口由紀子，八槇博史，立岩佑一郎，新麗，加藤雅彦，高倉弘喜，
    “ネットワーク内部分離設計のための自動評価機能および自動設定機能の実装，”
    情報処理学会第 75 回全国大会講演論文集，3Z-6，pp.545-546，2013.
  - 長谷川皓一，新麗，加藤雅彦，山口由紀子，八槇博史，高倉弘喜，
    “組織内部攻撃に対するリスク緩和のためのネットワーク設計支援システムの提案，”
    電子情報通信学会技術報告，Vol.112，No.315，ICSS2012-51，pp.37-42，2012.

（2）その他の論文

- 国内研究会等発表論文（査読なし）

– 淵上智史，長谷川皓一，山口由紀子，嶋田創，高倉弘喜，
“マルウェア感染拡大抑止に向けたネットワーク型動的解析システム，”
電子情報通信学会技術報告, Vol.115, No.482, IA2015-105, pp.221-226, 2016.

– 長谷川皓一，立岩佑一郎，片山善章，高橋直久，
“LAN 接続機器の配置図管理補助システムの実現について，”
情報処理学会第 74 回全国大会講演論文集，4X-8，pp.329-330，2012.

参考文献

[1] 独立行政法人情報処理推進機構，情報セキュリティ白書 2015，独立行政法人情報処理推進機構，2015.

[2] 独立行政法人情報処理推進機構，“「新しいタイプの攻撃」の対策に向けた設計・運用ガイド 改定第 2 版”．https://www.ipa.go.jp/files/000017308.pdf

[3] 独立行政法人情報処理推進機構，“「標的型メール攻撃」対策 に向けたシステム設計ガイド”．https://www.ipa.go.jp/files/000033897.pdf

[4] 独立行政法人情報処理推進機構，“「高度標的型攻撃」対策に向けたシステム設計ガイド”．https://www.ipa.go.jp/files/000046236.pdf

[5] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, “Computer security incident handling guide,” NIST Special Publication 800-61 Revision 2, 2012.

[6] MaAfee ウイルス情報，“Brain”．http://www.mcafee.com/japan/security/virB.asp?v=Brain

[7] 株式会社ラック サイバーグリッド研究所，“Cyber GRID View vol.1 日本における標的型サイバー攻撃の事故実態調査レポート”．http://www.lac.co.jp/security/report/2014/12/16_cgview_01.html

[8] 独立行政法人情報処理推進機構，“『新しいタイプの攻撃』に関するレポート”．http://www.ipa.go.jp/files/000009366.pdf

[9] 内閣サイバーセキュリティセンター，“三菱重工業等に対するサイバー攻撃事案について（経緯等）”．http://www.nisc.go.jp/conference/seisaku/dai27/pdf/27shiryou1.pdf

[10] 独立行政法人情報処理推進機構，“標的型サイバー攻撃の事例分析と対策レポート”．https://www.ipa.go.jp/files/000024536.pdf

[11] 内閣サイバーセキュリティセンター，“日本年金機構における個人情報流出事案に関する原因究明調査結果”．http://www.nisc.go.jp/active/kihon/pdf/incident_report.pdf

[12] M. Sato, H. Yamaki, and H. Takakura, “Unknown attacks detection using feature extraction from anomaly-based ids alerts,” Applications and the Internet (SAINT), 2012 IEEE/IPSJ 12th International Symposium onIEEE, pp.273–277 2012.

[13] JOINT TASK FORCE TRANSFORMATION INITIATIVE, “Security and privacy controls for federal information systems and organizations,” NIST Special Publication 800-53 Revision 4, 2013.

[14] R. Montesino and S. Fenz, “Information security automation: how far can we go?,” Availability, Reliability and Security (ARES), 2011 Sixth International Conference onIEEE, pp.280–285 2011.

[15] R. Martin, et al., “Making security measurable and manageable,” Military Communications Conference, 2008. MILCOM 2008. IEEEIEEE, pp.1–9 2008.

[16] I. Priescu and S. Nicolăescu, “Managing security monitoring in enterprise networks,” 2008.

[17] J. Case, M. Fedor, M. Schoffstall, and C. Davin, “A Simple Network Management Protocol (SNMP)”. https://tools.ietf.org/html/rfc1157

[18] 兒玉清幸，釜崎正吾，吉田和幸，“ネットワーク構成情報表示システムのための自動配置アルゴリズムの評価,” 情報処理学会マルチメディア, 分散, 協調とモバイル (DICOMO2007) 論文集，pp.1754–1761，2007.

[19] 大浦　昇，河野　優，釜崎正吾，吉田和幸，“VLAN を考慮した Layer2 ネットワーク構成情報推測アルゴリズムについて,” 情報処理学会マルチメディア, 分散, 協調とモバイル (DICOMO2006) 論文集，pp.629–632，2006.

[20] 宮本貴朗，田村武志，鈴木亮司，平岡大樹，松尾英普，泉正夫，福永邦雄他，“大規模ネットワークにおける VLAN 管理システム,” 情報処理学会論文誌，vol.41，no.12，pp.3234–3244，2000.

[21] 新　麗，“NETCONF の現状と今後,” 電子情報通信学会技術研究報告. IA, インターネットアーキテクチャ，vol.108，no.120，pp.49–54，July 2008.

[22] 新　麗，“次世代ネットワーク機器管理プロトコル NETCONF とその応用,” 情報処理，vol.50，no.12，pp.1199–1205，2009.

[23] 山崎康広，大和純一，宮本善則，後藤英昭，曽根秀昭，“OpenFlow による Campus VLAN システム，” 電子情報通信学会技術研究報告. CQ, コミュニケーションクオリティ，vol.111，no.132，pp.43–48，2011.

[24] “Snort”. https://www.snort.org

[25] E. Stalmans and B. Irwin, “A framework for dns based detection and mitigation of malware infections on a network,” Information Security South Africa (ISSA), pp.1–8, 2011.

[26] A. Schonewille and D.-J. vanHelmond, “The domain name service as an ids,” Research Project for the Master System-and Network Engineering at the University of Amsterdam, pp.1–24, 2006.

[27] A.M. Manasrah, A. Hasan, O.A. Abouabdalla, and S. Ramadass, “Detecting botnet activities based on abnormal dns traffic,” International Journal of Computer Science and Information Security, IJCSIS, vol.6, no.1, pp.97–104, 2009.

[28] 木村達明，竹下恵，豊野剛，横田将裕，西松研，森達哉，“Syslog+sns 分析によるネットワーク故障検知・原因分析技術，” NTT 技術ジャーナル，pp.20–24，2013.

[29] 佐々木良一，上原哲太郎，松本隆，“標的型攻撃に対するネットワークフォレンジック対策の現状と今後の展望，” コンピュータセキュリティシンポジウム 2013 論文集，vol.2013，no.4，pp.155–162，2013.

[30] 江端真行，小池英樹，“不正侵入調査を目的とした複数ログの時系列視覚化システム)，” 情報処理学会論文誌，vol.47，no.4，pp.1099–1107，April 2006.

[31] 大谷尚通，北野美紗，重田真義他，“企業内ネットワークの通信ログを用いたサイバー攻撃検知システム，” コンピュータセキュリティシンポジウム 2013 論文集，vol.2013，no.4，pp.287–294，2013.

[32] 立岩佑一郎，安田孝美，横井茂樹，“仮想環境ソフトウェアに基づく linux ネットワークトラブルシューティング実習環境提供システムの開発，” 情報処理学会研究報告コンピュータと教育 (CE)，vol.2007，no.123，pp.37–44，2007.

[33] 八津川直伸，石野貴子，“重大な脅威に対するセキュリティ設計手法の考察，” ユニシス技報，vol.28，no.3，pp.351–375，2008.

[34] D. Samociuk, B. Adamczyk, and A. Chydzinski, “Impact of router security and

address translation mechanisms on the transmission delay," Proceedings of the 7th International Conference on Evolving Internet (INTERNET 2015), pp.38–42, 2015.

[35] 高倉弘喜，江原康生，宮崎修一，沢田篤史，中村素典，岡部寿男，"安全なギガビットネットワークシステム kuins-iii の構成とセキュリティ対策，" 電子情報通信学会論文誌 B，vol.86，no.8，pp.1494–1501，2003.

[36] 渡邊利晃，北崎基久，井手口哲夫，村田嘉利他，"トラフィック解析によるダイナミック vlan 構成法の提案とシミュレーションによる評価，" 情報処理学会論文誌，vol.46，no.9，pp.2196–2204，2005.

[37] 久長　穣，北上悟史，渡邊孝博，棚田嘉博，井上裕二，"複数 vlan の動的切り替えネットワークの構築について，" 情報処理学会研究報告. DSM, [分散システム/インターネット運用技術]，vol.2001，no.80，pp.39–44，2001.

[38] 株式会社イイガ，"Vlan .config". http://www.iiga.jp/solution/config/vlan.html

[39] A.K. Nayak, A. Reimers, N. Feamster, and R. Clark, "Resonance: dynamic access control for enterprise networks," Proceedings of the 1st ACM workshop on Research on enterprise networkingACM, pp.11–18 2009.

[40] N. Gude, T. Koponen, J. Pettit, B. Pfaff, M. Casado, N. McKeown, and S. Shenker, "Nox: towards an operating system for networks," ACM SIGCOMM Computer Communication Review, vol.38, no.3, pp.105–110, 2008.

[41] S. Cabuk, C.I. Dalton, H. Ramasamy, and M. Schunter, "Towards automated provisioning of secure virtualized networks," Proceedings of the 14th ACM conference on Computer and communications securityACM, pp.235–245 2007.

[42] 橋本直樹，園生遥，牛込翔平，菊田宏，永園弘，廣津登志夫，新村正明他，"Openflow による認証基盤と連携したネットワークアクセス制御の実現，" 研究報告インターネットと運用技術 (IOT)，vol.2014，no.24，pp.1–6，2014.

[43] "dpkt". https://dpkt.readthedocs.io/en/latest/

[44] S. Hirono, Y. Yamaguchi, H. Shimada, and H. Takakura, "Development of a secure traffic analysis system to trace malicious activities on internal networks," Computer Software and Applications Conference (COMPSAC), 2014 IEEE 38th

AnnualIEEE, pp.305–310 2014.

[45] J.T. Luttgens，M. Pepe, and K. Mandia, インシデントレスポンス 第 3 版，日経 BP 社，April 2016.

[46] 武田圭史，“情報セキュリティ対策の経済合理性評価，” コンピュータセキュリティシンポジウム 2016 論文集，vol.2016，no.2，pp.249–254，2016.

[47] 呉洋，小崎真寛，岡田謙一他，“プロジェクトの特性を考慮した最適なセキュリティ対策選定手法，” 情報処理学会論文誌，vol.54，no.1，pp.309–317，2013.

[48] P. Kim, サイバーセキュリティテスト完全ガイド Kali Linux によるペネトレーションテスト ，マイナビ出版，Aug. 2016.

[49] 株式会社インターネットイニシアティブ，“ネットワーク接続手段の集中管理システム及び方法,” 特開 2004-193988.

[50] 株式会社インターネットイニシアティブ，“ネットワーク接続機器の自動生成機構,” 特開 2009-104648.