学位報告 4

報告番号	※甲　　第　　号

主　論　文　の　要　旨

論文題目	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
氏　　名	長谷川　皓一

論 文 内 容 の 要 旨

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．

学位関係