サイバー攻撃の解析・検知に関する研究開発

～セキュリティ強化とＢＣＭのための自動ネットワーク構成技術の研究開発～

基本計画書

１．目　的

近年、標的型攻撃をはじめとしてサイバー攻撃の高度化・複雑化が進展し、既存の情報セキュリティ対策ではネットワークへの侵入、マルウェアの感染等の情報セキュリティ上の脅威を完全に防ぐことが困難となっている。

こうした状況においてサイバー攻撃の被害を最小化するには、攻撃を早期に検知し迅速に対処することが重要である。そのため、本研究開発においては、利用者の行動特性等に応じて不正な通信の痕跡を発見し、ネットワークへの侵入及びマルウェアの感染等のサイバー攻撃による被害の程度並びに被害に至った経緯を明らかにする技術、及び当該情報に基づきサイバー攻撃への動的な防御を実現する技術の研究開発を実施する。

２．政策的位置付け

「情報セキュリティ2012」（平成24年７月情報セキュリティ政策会議決定）では、「国や国の安全に関する重要な情報を扱う企業等に対する高度な脅威への対応強化」が基本方針として定められ、具体的な取組として、「我が国全体として対応能力を向上させるよう、サイバー攻撃に係る高度解析機能を整備するほか、データベースや分析環境の構築、高度な検知技術等の研究開発を推進する」とされている。

３．目　標

（１）　政策目標（アウトカム目標）

2011年以降、国や国の安全に関する重要な情報を扱う企業等に対する標的型攻撃が相次いで明らかになるなど、従前とは態様が異なる新たなサイバー攻撃の脅威が顕在化している。例えば、メールを利用した標的型攻撃では、攻撃対象となる利用者にあわせて時事情報等を組み込むなど、文面を巧妙化しメールを開封するよう仕向けるなど高度なソーシャルエンジニアリングの手法が用いられている。

そのため本研究開発で得られた成果を実用化することで、利用者の行動特性に応じて適切な対策を適用するとともに、被害が発生した場合においても被害の進行状況に応じて影響のない業務を継続可能とし、利用者に過剰な負荷・制限を強いるこ

となく安全に情報が活用できる社会の実現に貢献する。

（２） 研究開発目標（アウトプット目標）

標的型攻撃をはじめとする近年のサイバー攻撃は、巧妙な手口を駆使して執拗に繰り返されるため、既存の情報セキュリティ対策では対処することが困難である。

そのため、本研究開発では、利用者の行動特性及び環境特性の活用に着目することにより、組織内ネットワークにおける不正な通信等を検知する技術、サイバー攻撃の被害状況を把握する技術及びサイバー攻撃の影響を最小化し業務を継続するネットワーク制御技術を確立する。

４．研究開発内容

Ⅰ．利用者の行動特性に基づくサイバー攻撃検知技術の研究開発

本課題では、利用者の行動特性を収集・分析し、サイバー攻撃を早期に検知する技術の研究開発を実施する。

（１）利用者行動特性分析技術

① 概要

特定の利用者を標的とした標的型攻撃等のサイバー攻撃は、利用者個人のみならず組織全体にとって大きな脅威である。しかし、個々に見ると同一の組織内においても同種の標的型攻撃に対して、その被害に遭う者と遭わない者がいる。この違いの要因となる利用者の行動特性・プロファイルを明らかにすることにより、所属組織及び利用者個々人の行動特性を加味した柔軟な情報セキュリティ対策の基盤となる技術の研究開発を実施する。

② 技術課題

人の行動及び心理の隙を突く標的型攻撃への適切な対処には、アクセスコントロール等による一律的な対策ではなく、人間の行動特性を十分に考慮した対策が必要である。そのため、標的型攻撃の被害と相関のある行動特性の因子を明らかにするとともに、それらをプロファイルとしてモデル化し、形式的に表現・構築・共有・処理を実現する。

③ 到達目標

標的型攻撃を受けやすい（受けにくい）利用者個人の差異、所属部署及び取り扱う情報等の差異を考慮し、標的型攻撃の検知及び被害との相関、利用者個人の行動特性に係る複数の因子を抽出する技術を確立する。

また、数百名規模の行動特性・プロファイル共有システムを実現し、課題Ⅰ．～ Ⅲ．と連携して、サイバー攻撃の迅速な検知並びに所属部署及び利用者個々人の行動特性を加味した柔軟かつ高効率な情報セキュリティ対策を実現する基盤技

術を確立する。

（２） 利用者の行動特性分析に基づく不正な意図の検知技術及び通信の制御技術

① 概要

利用者の行動特性の分析によりプロファイリングされた情報と実際の利用者の行動について比較分析することにより、正常な通信と判別することが困難な不正な意図を持つ通信等を抽出し、踏み台とされた端末を特定する技術の研究開発を実施する。

また、課題Ⅲ．と連携して、検知した不正な通信及び踏み台とされた端末の情報を基に組織内のネットワーク全体の通信を制御し、サイバー攻撃による被害の封込め及び業務継続を可能とするネットワークの利用制限及び通信誘導技術の研究開発を実施する。

② 技術課題

近年、マルウェアは単純に感染を拡大するのではなく、感染した端末から一般的なツール及びプロトコルを用いて利用者の通信に紛れて目的のサーバ等にアクセスし情報窃取を行うなど、従来のマルウェア自体を解析する技術では検出が困難となっている。そのため、通信自体は正常にもかかわらずその意図が不正な通信を検知し、踏み台となる端末を特定する必要がある。

不正な通信の検知には、組織内ネットワークに多数のセンサをきめ細かく配置し、高速かつ高精度にデータを解析する必要がある。しかしその実現には、利用者の行動特性の分析によりプロファイリングされた情報と実際の利用者の行動との比較分析、類似の行動特性等を有する者との相関分析等を基に不正な通信等を迅速かつ効率的に検知する技術が必要となる。

また、マルウェアに感染した端末が検知された場合、現在は物理的にその端末の接続を切断するか、その直ぐ上流に位置するスイッチでその端末を切り離すことで対処することが一般的であるが、最新のマルウェアは組織内のネットワーク上に自らのネットワークを構成する。そのため、感染した端末のみならず感染が疑われる範囲を推定し、感染の範囲及びその影響度に応じた利用制限又は監視強化を実現する経路制御技術が必要となる。

③ 到達目標

利用者の行動特性の分析によりプロファイリングされた情報、実際の利用者の行動との比較分析、類似の行動特性等を有する者との相関分析等を基に、ネットワーク及びサーバの負荷を抑えつつ迅速にマルウェア感染を検知する技術を確立する。

また、マルウェア感染が検知された場合に、影響の範囲及び影響度に応じた利用制限、監視強化等を実現するため、リアルタイムに経路制御を行う技術を確立する。なお、本経路制御技術は、複数の拠点からＷＡＮ経由で通信を誘導可能とする。

Ⅱ．既存のログに依存しない利用者環境の特性を活用したサイバー攻撃の侵入経路及び進行状況を解析する技術の研究開発

マルウェアの感染経路及び被害範囲の特定に当たっては、ネットワークトラヒックのログの取得及び解析が有効であるが、ログの蓄積は膨大なコスト及び時間を要する。また、攻撃には未知のマルウェアが用いられる可能性があり、未知のマルウェアがどのような機能を有しどのような動作を行うのかが明らかでない状況においては、既存のログの取得及び解析のみではマルウェアへの感染有無及び感染経路を特定するための証跡として不十分である。

本課題では、既存のログ収集及び解析によらない、利用者環境の特性等を活用してのサイバー攻撃の有無、攻撃経路、攻撃による被害の状況を解析する技術の研究開発を実施する。

（1）利用者環境上の構成要素分析技術

① 概要

ネットワークで利用される機器の多様化が進展したことで、サイバー攻撃の対象が端末及びサーバ以外の機器（スマートフォン／タブレット、複合機、テレビ会議システム等）に拡大している。そのため、利用者組織のネットワーク上の機器を対象に、サイバー攻撃の有無、攻撃経路及び攻撃の進行状況を特定するために有用な状態を抽出／分析する技術の研究開発を実施する。

② 技術課題

サイバー攻撃の有無及び進行状況を特定するに当たっては、現状、機器上のＯＳ及びソフトウェアが出力するログ（ＯＳの起動及び停止の履歴、ソフトウェアの実行履歴等）のみによっているが、状態（自動起動設定、サービス／プロセスの稼働状況、通信状態等）も含めた解析を行うことが有効であると考えられる。そのため、組織内ネットワーク上の各機器において、どのような状態を取得することで、サイバー攻撃に関するどのような事象を特定できるのかを定義し、組織内ネットワーク上の機器から実際に状態を抽出して解析する技術が必要となる。

また、攻撃経路及び攻撃の進行状況を特定するため、組織内ネットワーク上の機器の構成を正確に把握する識別技術が必要となる。

③ 到達目標

サイバー攻撃の有無、攻撃経路及び攻撃の進行状況を特定するため、必要な状態を特定して既存ログとの有効性を比較するとともに、必要なデータを抽出する技術を確立する。

また、各対象機器から必要なデータを最小限の頻度で抽出する技術及び組織内ネットワーク上に存在する機器を把握する識別技術を確立する。

さらに、課題Ⅱ.（2）の実施状況を踏まえ、検知精度の向上に必要な状態を追加・

変更して抽出する技術を確立する。

そして、これらの技術を基にマルウェア感染の有無を特定し、マルウェア感染の要因を根絶する技術を確立する。

以上の技術について、一般的な組織のネットワーク構成を踏まえ、本技術を大規模組織に適用した際のフィージビリティを、５つ以上のブロードキャストドメインを持つネットワーク上で検証する。

（２）利用者環境上の状態を用いたサイバー攻撃の有無、攻撃経路及び進行状況の特定技術

① 概要

端末がマルウェアに感染した場合においても、マルウェア感染後の比較的短時間、あるいは攻撃の初期段階で検知することができれば、機密情報の窃取、組織内の特定システムの停止等の被害の甚大化を防ぐことができると考えられる。

そのため、課題Ⅱ.（１）の結果を分析し、迅速かつ確実に組織内ネットワーク上の機器に対するサイバー攻撃の有無、攻撃経路の特定及び攻撃の進行状況を特定する技術の研究開発を実施する。また、同一の組織内ネットワークの機器において同様の攻撃の有無を特定し、攻撃の原因を根絶する技術の研究開発を実施する。

② 技術課題

大規模な情報漏えい等の被害を未然に防ぐためには、利用者環境の状態監視のタイミングを一定のリアルタイム性を確保した上で実施し、サイバー攻撃の有無等を特定する技術が必要である。

また、組織内ネットワーク上の１台の機器にマルウェア感染等の攻撃を確認した場合、同様の攻撃経路にて他の機器がマルウェアに感染していないか、感染機器からアクセス可能な組織内ネットワーク上の他の機器に感染が及んでいないかを確認する必要がある。そのため、１台の機器上で攻撃を確認し攻撃経路等を特定できた場合、当該情報を活用して組織内ネットワーク上の他の機器で同様の攻撃が発生していないか、攻撃が発生している場合はその進行状況を分析する技術が必要である。

さらに、早急に攻撃を受けた状態から回復し、同様の攻撃経路から攻撃が繰り返される可能性を踏まえて感染原因を特定し根治しなければならない。そのため、抽出した情報及び分析結果を基に、攻撃を受けた組織ネットワーク上の機器を一括で回復する技術及び攻撃経路を根絶するための技術が必要となる。

③ 到達目標

課題Ⅱ.（１）の技術により抽出した状態を利用者環境の特性を踏まえて分析する技術、及びマルウェア感染が疑われる機器の活動を過去に遡り把握する技術を確立する。また、実際にマルウェア感染が疑われる機器の活動、抽出した情報、分析結果等を１箇所に集約して時系列で表示することにより、組織内ネットワーク上の端末、サーバ等の他の機器に同様のマルウェア感染が発生していないかを一括で特定

可能な技術を確立する。

最終的には、課題Ⅱ.（１）の開発と連携し、本技術を大規模組織に適用した際の有効性を確認するために、100台以上の機器で検証する。

Ⅲ. サイバー攻撃の封込めと業務継続を可能とする組織内ネットワーク制御技術の研究開発

本課題では、サイバー攻撃の影響を極小化するため、アクセス制限及び監視を強化しつつ、攻撃対象とならないネットワークでの業務を継続させるネットワーク制御技術の研究開発を実施する。

（１）管理ポリシーに基づく自動ネットワーク構成技術

① 概要

組織の論理的な構成要件を示した管理ポリシー及びネットワーク機器の接続状態を基に安全性の高いネットワーク設計を行い、複数の設計候補から利便性及び安全性に基づいてネットワークを自動的に構成する技術の研究開発を実施する。

② 技術課題

サイバー攻撃への耐性を高めるためには、仮想化ネットワーク技術、ＳＤＮ（Software Defined Network）技術等を活用し、組織の論理的な構成を反映したきめ細やかなアクセス制御が求められる。しかし、組織構成の変更、部屋の移動等、時間経過に伴い論理構成とネットワークの物理構成に不一致が生じること、その都度、論理構成を修正することなどを考慮すると、過度に細かいアクセス制御は組織ネットワーク運用の負荷を大幅に増大させることになる。

そこで、組織の論理的な構成要件（部門間のアクセス可否、優先度に基づいた保護すべき機器の配置等）を示した管理ポリシー及びネットワーク機器の接続状態を基に安全性の高いネットワーク設計を行い、複数の設計候補について利便性と安全性の評価を行う技術が必要となる。

また、利用者の行動特性を解析することにより論理構成と実際の運用状態の不一致を検知し、ポリシー違反によるサイバー攻撃の可能性又は論理構成の変更によるネットワーク設計変更の必要性をネットワーク管理者に通知する技術が必要となる。

③ 到達目標

管理ポリシーを表現するための記述法、当該ポリシーに基づいた論理ネットワークの構築及びネットワーク間のアクセス制御技術を確立する。また、設計された複数の候補について、組織外ネットワークとのアクセス性及びサイバー攻撃のリスクを自動的に評価する仕組みを確立する。

（２）緊急時における自動ネットワーク構成変更技術

① 概要

サイバー攻撃を検知した際に、マルウェア等の感染が疑われる端末及びこれを収容するネットワークから、組織内ネットワークへのアクセス制限を強化すると同時に、攻撃対象とならないネットワークから組織内ネットワークへのアクセス性を維持する技術の研究開発を実施する。

② 技術課題

サイバー攻撃を検知した場合、既に被害が発生しているネットワークを特定し組織内のネットワークから速やかに切り離す必要がある。一方、現時点で被害が発生しているネットワークは単なる中継点であり、真の攻撃目標は別であることも推定される。また、サイバー攻撃の可能性があることのみをもって、組織ネットワークを全て停止することは、組織の業務に甚大な影響を及ぼす。

そこで既に被害が発生しているネットワークに対するアクセス制限、隔離及び攻撃対象と推定されるネットワークの保護、更にそれ以外のネットワークでの業務継続を支援するため、ネットワーク間の管理ポリシーを変更し、それに基づくアクセス制御を評価する技術が必要となる。

また、マルウェア駆除等の対策が完了したネットワークに対し、順次、アクセス制限及び隔離を解除する技術、マルウェアの完全駆除が確認できない端末及びネットワークが残存する場合、暫定的な運用継続を行う技術も必要となる。

③ 到達目標

標的型攻撃を検知し、被害が発生していると推定されるネットワークに対するアクセス制限及び組織ネットワークからの切離しを実行するとともに、今後の攻撃対象と推定されるネットワークの保護及び対象外となったネットワークでの業務を継続させるネットワーク構成技術を確立する。

（3）動的管理ポリシー生成技術

① 概要

マルウェアに感染した端末が存在するネットワークから組織内ネットワークへの通信の中で、無害と判断されたものを許可することで業務継続を支援する技術、サイバー攻撃への対処が完了後に、業務に影響を及ぼさない範囲において、より安全なネットワーク構成を提案する技術を確立する。

② 技術課題

サイバー攻撃の被害の拡大を防ぐために、当該ネットワークから組織内ネットワークへのアクセスを完全に遮断することは、組織全体の業務継続が不可能になるおそれがある。また、サイバー攻撃への対処が完了した後、管理ポリシーの見直しにより業務に影響を及ぼさない範囲内でより強固なものを提案し、同時にこれを実現するためのネットワーク構成を提案する必要がある。

そのため、サイバー攻撃が継続している間、利用者の行動特性と合致しかつ無害と判断されたアクセスが当該ネットワークから組織内ネットワークへ向うことを許

可することで、安全性を確保しつつ業務継続を支援する技術が必要となる。また、サイバー攻撃への対処が完了した後、業務に影響を及ぼさない範囲内で新たな管理ポリシー強化の複数候補をネットワーク管理者に提示する技術も必要となる。

③ 到達目標

サイバー攻撃に関係せずかつ管理ポリシーに照らし合わせて、業務継続に不可欠と判断される通信を特定する技術を確立する。さらに、サイバー攻撃への対処完了後に、サイバー攻撃の侵入経路となった通信、被害拡大の要因となった通信及び業務継続に不可欠であった通信を明らかにし、新たな管理ポリシーの候補とこれを適用する際に必要となるネットワーク構成の組を複数生成し、可視化して提案する技術を確立する。

５．研究開発期間

平成25年度からの５年以内

６．その他　特記事項

（１） 提案及び研究開発にあたっての留意点

① 提案に当たっては、基本計画書に記されているアウトプット目標に対する達成度を評価することが可能な評価項目を設定し、各評価項目に対して可能な限り数値目標を定めるとともに、目標を達成するための研究方法、実用的な成果を導出するための共同研究体制又は研究協力体制、及び達成度を客観的に評価するための実証実験の方法について、具体的に提案書に記載すること。

② 本研究開発成果を確実に展開し、アウトカム目標を達成するため、事業化目標年度、事業化に至るまでの実効的な取組計画（標準化活動、体制、資金等）についても具体的に提案書に記載すること。

③ 複数機関による共同研究を提案する際には、研究開発全体を整合的かつ一体的に行えるよう参加機関の役割分担を明確にし、研究開発期間を通じて継続的に連携するための方法について具体的に提案書に記載すること。

④ 研究開発の実施に当たっては、関連する要素技術間の調整、成果の取りまとめ方等、研究開発全体の方針について幅広い観点から助言を頂くとともに、実際の研究開発の進め方について適宜指導を頂くため、学識経験者、有識者等を含んだ研究開発運営委員会等を開催するなど、外部の学識経験者、有識者等を参画させること。

⑤ サイバー攻撃の手法は日々高度化・巧妙化する傾向にあり、こうした情勢の変化に遅滞なく対処していく必要があることから、本研究開発については、可能な限りスケジュールの前倒しによる実現を目指すとともに、検討課題の追加・変更等についても適宜計画を見直すことなどにより柔軟に対応すること。

⑥ 本研究開発は総務省施策の一環として取り組むものであることから、総務省が受託者に対して指示する、研究開発に関する情報及び研究開発成果の開示、関係研究開発プロジェクトとのミーティングへの出席、シンポジウム等での研究発表、共同実証実験への参加等に可能な限り応じること。

（２） 人材の確保及び育成への配慮

① 研究開発によって十分な成果が創出されるためには、優れた人材の確保が必要である。このため、本研究開発の実施に際し、人事、施設、予算等のあらゆる面で、優れた人材が確保される環境整備に関して具体的に提案書に記載すること。

② 若手の人材育成の観点から行う部外研究員受入れ、招へい制度、インターンシップ制度等による人員の活用を推奨する。これらの取組予定の有無及び計画について提案書に記載すること。

（３） 研究開発成果の情報発信

① 本研究開発で確立した技術の普及啓発活動を実施するとともに、その活動計画及び方策については具体的に提案書に記載すること。

② 研究開発成果については、原則として、総務省としてインターネット等により発信を行うとともに、マスコミを通じた研究開発成果の発表、講演会での発表等により、広く一般国民へ研究開発成果を分かりやすく伝える予定であることから、当該提案書には、研究成果に関する分かりやすい説明資料、図表等の素材、英訳文書等を作成し、研究成果報告書の一部として報告する旨の活動が含まれていること。さらに、総務省が別途指定する成果発表会等の場において研究開発の進捗状況、成果について説明等を行う旨を提案書に記載すること。

③ 本研究開発終了後に成果を論文発表、プレス発表、製品化、ウェブサイト掲載等を行う際には「本技術は、総務省の『サイバー攻撃の解析・検知に関する研究開発』による委託を受けて実施した研究開発による成果である。」という内容の注記を発表資料等に都度付すこととする旨を提案書に記載すること。