個人に合わせた巧妙な標的型メールの分析とその対策手法の研究

（課程博士・様式７）（Doctoral qualification by coursework,Form 7）

学 位 論 文 要 旨

Abstract of Doctoral Thesis

専　　攻：情報学専攻　　氏　名：西川弘毅

論文題目：個人に合わせた巧妙な標的型メールの分析とその対策手法の研究

論文要旨：

特定の企業・組織の機微情報や設備破壊による稼働防止，経済損失の発生を目的とする標的型攻撃はより深刻となっている．近年でも，日本国内の重要政府機関やインフラ企業が標的型攻撃の対象となり，機密情報や個人情報の漏洩など深刻な被害を受けており，対策が重要である．標的型攻撃では，標的に特化したメール（標的型メール）を利用して標的組織をマルウェアに感染させたのち，機密情報の窃取や，データの不正な暗号化によるシステム停止，といった攻撃者の目的を達成する活動を行う．その背景には，情報通信技術（ICT）の発展がある．マルウェアや不正な通信の検知技術，サーバの堅牢化など，サイバー攻撃防御技術の開発は進んでおり，攻撃者は，標的組織での目的を達成することが以前と比べて難しくなっている．そのため攻撃者は，セキュリティ上で最も弱い点(Weakest Link)である「人」を対象に攻撃を実施する．そして ICT の発展が，攻撃者が人に対する攻撃をより巧妙，かつ，より容易に行うことを可能としている．

攻撃は１点を突破すれば成功するのに対し,防御はすべての攻撃を防がなければならず,攻防はそもそも攻撃者有利の関係にある．その中でも「人」の価値観や振る舞いは非常に多様であり，その結果，人を対象とした攻撃も多岐に渡ることになる．このため，防御側がそのすべてに対応することは格段に難しく，標的型攻撃は攻高防低が特に顕著となる事案である．この課題に対し，現在の防御策は全ての人に対して一律の対策を実施するに留まっており，巧妙な攻撃を防ぎ切ることができていないという現状にある．本研究の最終目的は，今後，より深刻化していくことが予想される，人に対する脅威の可能性について明らかにし，人ごとに適した対策を取り入れていくことで，より効果的なセキュリティ対策を実現することである．その第一歩として，本論文では，攻撃者が標的を直接揺さぶることができるメールに着目して研究を行った．今後予想される標的型メールの脅威と対策を見据え，攻撃側が擬態精度あるいは心理操作効力の高いメールをどの程度作成することができるのかに関する検討と，その結果を防御側がどのように対策に活用していくことができるのかに関する検討を行った．

まず，擬態精度を高めたメールの脅威と対策を示した．具体的には，攻撃者は標的者の名前のみを手掛かりとして，インターネットに公開されている情報源から標的者に関する様々な情報を Open Source Intelligence（OSINT）ツールによって次々と取得し，これらの情報をメールに組み入れることによって，擬態精度が高いメールを標的者ごとに作成することが可能であることを示した．このような擬態精度を高める攻撃への対策として，攻撃者による OSINT の進行を状態遷移図によって定式化し，個々の攻撃段階（どこまでの情報が攻撃者に漏洩しているか）ごとに作成され得る標的型メール文面を整理した．各組織は，自らも OSINT を実行することによって攻撃者が自組織の情報をどこまで入手可能であるか確認し，本状態遷移図に照らし合わせることによって，自組織に届く可能性がある標的型メールの文面をあらかじめ把握することが可能となるため，それを踏まえたプロアクティブな対策選定に資することができる．

次に，心理操作効力を高めたメールの脅威と対策を示した．攻撃者は，AI ツールによって推定した標的者の特性に基づいて，その標的者に有効なチャルディーニの法則を推定することで，心理操作効力の高い標的型メールを標的者ごとに作成することができる．本研究では，100 人規模のアンケート調査を実施し，個人の性格因子とチャルディーニの法則の相関関係が，行動特性によって異なることを示した．これまで，種々の既存研究において説得のされやすさ（チャルディーニの法則に対する感受性）と性格因子との相関関係，あるいは，説得のされやすさ（詐欺師の説得を受け入れてしまいやすさ）と行動特性との相関関係がそれぞれ個別に調査されてきたのに対し，説得のされやすさ（チャルディーニの法則に対する感受性）を性格因子と行動特性のコンビネーションによって分析したことが，本研究の第一の貢献である．このような心理操作効力を高める攻撃への対策として，標的者が標的型メールを受けた際には，メールに含まれている説得のフレーズを通知することで標的者に注意を促すことが有効であると考えられる．本研究では，400 人規模のアンケート調査を実施し，効果的な注意喚起の方法（メール内のどの説得フレーズに対してアラートを提示すると，標的者は標的型メールへの不信感を高めるか）も，標的者の性格因子と行動特性の両者によって異なることを示した．

これまでの既存研究においては，標的型メールの脅威分析（攻撃側が擬態精度あるいは心理操作効力の高いメールをどの程度作成することができるのか）に主眼が置かれていた．これに対し本研究では，標的型メールへの対策（防御側が脅威分析の結果をどのように対策に活用していくことができるのか）にまで足を踏み込んだ．攻撃者による脅威をあらかじめ把握することで，標的者に応じた有効な対策を配備することができることを示したことが，本研究の第二の貢献である．本研究は，著者が知る限り，個々人の特性に応じてセキュリティシステムの防御方法を変える考えを具体化した初めての研究である．本研究が，Weakest Link である人に着目したサイバーセキュリティ防御研究の今後の足掛かりとなることを期待する．