抄録：　研究成果報告書

テーマ：

選択理論心理学のユーザブルセキュリティへの適用に関する調査研究

研究期間：　2020 年 11 月 01 日～2021 年 3 月 31 日

東京通信大学
情報マネジメント学部
角尾幸保・教授

2021 年 4 月 20 日

【2020 年度研究報告書・概要】

本報告は，選択理論心理学のユーザブルセキュリティへの適用に関する調査を進める目的をもって，2020 年 11 月より 2021 年 3 月まで実施した研究の報告書である．

本研究の本年度の計画は，以下の２点である．
（１）受動的防御としての対策の検討：
組織におけるセキュリティ更新プログラム適用の漏れを排除するために，選択理論を使って更新プログラム適用の行動を動機づけることができるかを調査すること
（２）能動的防御としての対策の検討：
防御行動となるメッセージの形成および発動が選択理論に基づいて実現可能なのかを検討すること

具体的には，以下の５項目①～⑤の活動を行った．

（１）に関しては，
委託元研究員殿がアンケート調査を実施することを前提として，
①データの収集・分析・評価の各段階で選択理論心理学を応用する方法論を構築するための技術討議を行った．
②想定するエンドユーザの動機づけで使用するメッセージの形式を協議した．
③行った調査研究の内容の一部を SCIS2021 で発表した．

（２）に関しては，
④昨年度までの研究成果の応用が可能かどうかを検討し SCIS2021 で発表した．
⑤能動的防御の手法を検討する準備として，２９０の項目について考察を行った．

上記（１）で，委託元研究員殿との作業を分離したのは，委託元研究員殿が行った調査実験の生データを外部に出さない情報の管理を重視したためである．
また，（２）⑤に関しては，能動的防御のために必要な技量や条件を検討する目的を持つため，選択理論心理学の概要を知っており，かつ，対人コミュニケーションの技量として選択理論心理学を使いこなせている者が検討を進める必要があった．

報告者　東京通信大学情報マネジメント学部教授　角尾幸保
報告日　2021 年 4 月 20 日

以上

【はじめに】

近年では，企業のサイバー攻撃への対処が必須となっており，脆弱性のある情報システムを放置すれば企業の存続にも影響を及ぼすといっても過言ではない．そして，情報を扱う企業においては，情報システムを構成する多数の情報機器から「脆弱性のある機器」をいかに排除するかが重要な課題となっている．

本年度の研究は，情報端末を扱う一個人が，組織の情報セキュリティのレベルを維持するためにできる行動は何か，という疑問から始まっている．

組織がサイバー攻撃を受ける際に攻撃の入り口となるのは，情報システムの中にある脆弱性を持つ PC や PC を扱う人間であることが多い．その入り口をふさぐ手段として決定的な物はなさそうである．現状では，例えば，組織の情報システム全体を一元管理しセキュリティソフトの維持管理・更新などを厳重に行うこと，および，それを行う組織内の人間に対する指示命令・規則の制定，倫理を含む教育などを厳重に行うこと，などが行われている．

残念なことに，入り口をふさぐ手段の実施は，実際に操作を行う人間が「絶対にやらない」と決意を固めてしまえば実施されないものである．機能のアップデートや修正のためのソフトウエアの更新作業をする際に「ダウンロードと再立ち上げに時間がかかる」と思った経験は多くの人が持っているに違いない．そのうちの何人かは，更新のために PC が使えなくなる時間に耐えられず，「更新よりも PC を使う通常の作業を優先する行動をとる」可能性が残ることになる．

我々は，この「更新よりも PC を使う通常の作業を優先する行動をとる」という状況を，「PC の更新作業」と「PC を使う通常の作業」の二つの行動を選択した状況と考え，さらに「動機により行動が選択される」のであれば『作業者の動機に影響を与えることができれば，「PC を使う通常の作業」よりも「PC の更新作業」を優先する行動を選択させること』が可能であると考えた．

ここから，人の動機づけにより情報システムのセキュリティレベルを向上させる方法が想起され，（標的と攻撃者が存在することから）情報端末を扱う一個人の動機づけと情報端末を狙った攻撃者の動機づけに対応する受動的防御と能動的防御の検討を行うこととなった．

【研究活動の実施状況】

（1）受動的防御としての対策の検討

受動的防御とは，標的自身の動作を平時と同程度に維持・継続する目的を達成するために，標的が攻撃された時に発動することを期待されている防御機能を，平時にあらかじめ準備することである（事前準備しておき，攻撃されたら発動する）．受動的防御では攻撃された時に「人手を介さずに自動的に防御機能が動作すること」への期待（即応性への期待）があり，一般的にはツールやアプリケーションを導入し，その機能や性能を継続的に更新していく作業が行われる．典型的には，個人が管理する PC にインストールされたウイルスチェックソフト，Windows などの OS のセキュリティ機能，ファイアウォールのパケットフィルタリング機能などが該当する．また，サイバー攻撃など攻撃手法が進化を続ける脅威に対しては，これら防御側の機能や性能の向上も継続的に行う必要がある．

今回我々は，身近な対象として「Windows Update」を取り上げ，組織におけるセキュリティ更新プログラム適用の漏れを排除するために，選択理論を使って更新プログラム適用の行動を動機づけることができるかを調査研究した．

（2）能動的防御としての対策の検討

能動的防御とは，次の攻撃を回避するまたは抑止する目的，あるいは，攻撃を継続させ情報を収集するまたは状況変化を待つ目的を達成するために，標的が攻撃されたと判断または攻撃される蓋然性が高いと判断した時に，攻撃者のメッセージ列に対する適応的な反応メッセージ列を作成し返信を行うことである （攻撃された時に効果的な反撃を行う）．能動的防御では「攻撃者からの情報を標的が判断し，標的がもつ目的に適した応答を返すこと」を期待しており，攻撃メッセージと防御メッセージが 1 対 1 に対応するような単純な刺激反応モデルでは実現が困難である．攻撃を検知する能力，標的の目的の達成に効果的で，かつ，攻撃に適応したメッセージを返信する能力，など，標的に高度な適応能力が求められるからである．典型的には，警察が捜査手法の一つとして行う「特殊詐欺に対する騙されたフリ作戦」などが該当する．特殊詐欺の事例を基に分析を行えば，「攻撃者が攻撃していることの判断」をする条件を決定したり，標的が攻撃を妨害するために作成すべき「攻撃者のメッセージ列に対する適応的な反応メッセージ列」の形式を決定したりすることが容易になると考えられる．

このような考えのもとで，能動的防御としての防御行動となるメッセージの形成および発動が選択理論に基づいて実現可能なのかを検討した．

【まとめと今後の課題】

本研究では，選択理論心理学のユーザブルセキュリティへの適用に関する調査を進める目的とした活動を行った．

具体的には，次の 2 項目の活動を行った．

（1）組織におけるセキュリティ更新プログラム適用の漏れを排除するために，選択理論を使って更新プログラム適用の行動を動機づけることができるかを調査した．
データの収集・分析・評価の各段階で選択理論心理学を応用する方法を検討し，アンケート調査を実施した．アンケート結果の分析及び活用によって，行動変容の動機づけに効果的なメッセージ形式を検討中である．また，先行論文を調査した成果を SCIS2021 で発表した．

（2）防御行動となるメッセージの形成および発動が選択理論に基づいて実現可能かを検討した．
昨年度までのリアリティセラピーのセキュリティ・マネジメント適用に関する研究成果が，本年度のユーザブルセキュリティへの適用研究に応用が可能かどうかを検討し SCIS2021 で発表した．また，標的から攻撃者に対して発動する能動的防御の手法を検討する準備として，２９０の項目について考察を行った．

今後の課題としては，能動的防御の実効性を上げるために，「標的の被誘導プロセスを分析する手法を確立すること」や「標的の被害を最小化するための汎用的なメッセージ形成と送出の方法論を確立すること」などが考えられる．

以上

【抄録作成： 2021 年 8 月 8 日】