Vol.2019-SPT-32 No.15
2019/3/7

ユーザのセキュリティパッチ適用行動を促す心理学アプローチの検討

寺田剛陽[†1]　稲葉緑[†2]

概要：人々にセキュリティ行動を促す積極的な取り組みが，政府や民間のセキュリティ調査機関によって盛んに行われているものの，セキュリティインシデントは依然として後を絶たない．2017 年 5 月以降に世界的に甚大な被害をもたらした Wanna Cryptor やその亜種も，Microsoft が事前に配布していた修正パッチを各自で適用していれば防げた攻撃であった．このことから，多くのユーザがセキュリティ行動に対して積極的ではないことは明確である．セキュリティ行動を阻む心理的要因は多様にある一方で近年，人々に何らかの社会的に望ましい行動を促すための知見や実践例が出てきている．本研究では，近年，社会的な問題の対策や施策にも応用されているナッジ(個人の選択の自由を尊重しつつ望ましい行動を促す手法や設計)に着目し，各社員の Windows 端末への月例セキュリティパッチ適用を促進する仕組みに活用した．検証の結果，統計上の顕著な効果は認められなかったものの，ナッジが奏功した可能性といくつかの改善点を得た．

Investigation of Prompting Users to Apply Security Patches by Using a Psychologic Approach

TAKEAKI TERADA[†1]　MIDORI INABA[†2]

Abstract: The positive activities to promote people doing security-conscious behavior have been performed by the government and information security agencies, however, there is no end to the security incidents. Wanna Cryptor and its subspecies, which caused enormous damage to companies and individuals in the world, would have been prevented if the patch program already provided by Microsoft before the crisis has been applied to their computers. This shows that many users aren't interested in security-conscious behavior. There are various psychological factors to prevent people from securing their computers for work. On the other hand, some knowledge and demonstration tests have been reported in recent years. This study adopted the "nudge" having been used for resolving social problems to the policy to promote employees applying monthly security patches to their PCs. Results of an experiment show that the policy exhibited the potential to promote applying patches although it didn't reach significant effect.

1. はじめに

企業は社員を含めたシステムのセキュリティ対策として，社員向けにセキュリティのコンプライアンスポリシーを設置し，企業のセキュリティ対策に資する行動（以下，「セキュリティ行動」と呼ぶ）を取るように求める．

しかし，セキュリティ行動を実施しない社員は多い[1]．企業が求めるセキュリティ行動を実施しないことはコンプライアンス違反である．企業から教育や説明を受けたにもかかわらずセキュリティ行動を実施しないのであれば，より深刻な状態であると言える．先行研究では，企業の社員における情報セキュリティ行動に対する態度が，その実施に大きく影響することが提案されている．セキュリティ行動に関するモデルによれば，セキュリティ行動への肯定的な感情を伴った態度がその実行を左右する[2]．しかし，このような肯定的態度をセキュリティ行動に対して持つことの難しさが多くの研究で指摘されている．この難しさの要因の一つに，セキュリティ行動以外の業務を優先させようとする心理があると考えられ，この解釈にゴールシステム仮説が使われることがある[3]．この仮説では，我々の様々な活動をヒエラルキー型に位置づける．最も高く位置付けられる活動のゴール（目標）を「プライマリゴール」と呼ぶ．我々はプライマリゴールを最も重視し，これに直接的に関連する作業や業務を優先する．問題なのは，我々が一度に費やすことができる労力や時間などのコストには上限がある．最も重要なプライマリゴールを到達するためにコストを全て投入できればよいが，プライマリゴールを到達するためには，このゴールを下支えする作業や業務を実施する必要がある．これらの下支えする作業にコストを投入すれば，プライマリゴールに投入できるコストは減る．このようなジレンマ状況において，我々は，下支えする作業や業務をプライマリゴールの達成を妨害するものとしてみなし，否定的な態度を持つとされる．一般的な社員にとっては，セキュリティ行動は，それ自体がプライマリゴールとなることはほとんどない．自身が担当する主業務がプライマリゴールであり，セキュリティ行動は，それを下支えする業務と位置付けられる．このような関係から，前述したとおり，社員は，セキュリティ行動をプライマリゴールとしての業務を妨害するものとして否定的な態度を持ちやすいことが示されている[4]．

社員が自身の主業務に対して意識を強く持つことは，企

†1 (株)富士通研究所
Fujitsu Laboratories Ltd.
†2 情報セキュリティ大学院大学
Institute of Information Security

ⓒ 2019 Information Processing Society of Japan

業の成果を達成するという観点からすれば，社員として望ましい側面である．これを低下させる方向での対策を企業が取ることは難しい．一方，これらを下支えするセキュリティ行動を社員が実行しないことで，企業のシステムがリスクに冒されることを防ぐことが企業には求められる．そこで，社員のセキュリティ行動に対する否定的態度にかかわらず，社員が当該行動を実施するように働きかけることが重要であると考えられる．

本研究では，企業の社員の情報セキュリティを促進するにあたって効果的な働きかけについて検討する．この検討においては，セキュリティ上のリスクについて理解させる方法ではなく，リスク行動の抑制，および，対リスク行動あるいは低リスク行動の促進を目的とする方法として提唱された「ナッジ（Nudge）」に着目する．ナッジとは個人の選択の自由は尊重しつつも，望ましい選択や行動を促す手法や設計を指す[5].

また，研究対象とするセキュリティ行動は，「各社員が管理するパソコン端末への Microsoft Windows の月例セキュリティパッチ適用（以下，「パッチ適用行動」）」とする．2017 年 5 月以降に世界的に甚大な被害をもたらした Wanna Cryptor や PETYA，あるいはその亜種などのマルウェアによる企業の被害は，セキュリティパッチの適用というセキュリティインシデントを回避するための基本的な情報セキュリティ行動でさえも，社員に実施を徹底させることが難しいという現状を示すものであった．これらのマルウェアは Microsoft 製品に存在した脆弱性を攻撃するもので, Microsoft は 2017 年 3 月にこの脆弱性に対する修正プログラムを公開済みであった[6]．したがって，上述したマルウェアに感染した端末には，この修正プログラムが適用されていなかったと言える．日本の企業における深刻な感染例も報告された[7]．この事象の甚大な被害，および，パッチ適用行動と被害回避との明確な関係から，本研究ではパッチ適用行動を選んだ．

以上から本研究は，パッチ適用行動を促す効果の高いナッジについて明らかにすることを目的とする．この目的のため，企業における社員のパッチ適用行動を促進するナッジを実験的に導入し，その効果を評価する．

2. パッチ適用行動を促すナッジの検討

本章では，実験で検討するナッジについて具体的に考案する．はじめに，実験実施前の実験環境におけるパッチ適用行動に関する状況を紹介し，その心理的背景について推察する．

2.1 実験環境および実験前の状況

実験環境は，システム会社の中の一職場であった．この職場では，各社員がセキュリティパッチを自身の管理する端末に適用する．また，この職場の情報システム担当は，社員が管理する全ての端末を登録し，各端末にパッチが適用されたかについて，その時期も含めて把握することが可能である．このような環境において，社員がセキュリティパッチを端末に適用する流れは次のとおりである．

①セキュリティ担当が各社員に対し，月例セキュリティパッチを各端末に適用するようメールで依頼する．

②パッチ公開後の一定期間内にパッチが適用されない端末については，パッチ適用を催促するメールを社員およびその上司に送信する．

③催促メールが送信された 1 週間後にパッチが適用されていない場合は，その端末をネットワークから切断する．

このような方法によって，実験実施前は，この職場の社員の約半数が，セキュリティパッチ公開後 1 週間以内に自身が管理する全ての端末にパッチを適用していた. ただし，1 週間後のパッチ適用行動の進捗は徐々に緩やかになり，全端末に適用されるには至らないという状況であった．

社内の教育によって必要性や適用方法を認識しているはずの社員がパッチ適用行動を実施しない理由については，前章で述べたセキュリティ行動に対する否定的態度が考えられる．ただし，情報セキュリティ担当からのフォローアップがなされてもパッチ未適用者が当該行動を実施しないということは，その社員が出張などの物理的に実施出来る状況ではないか，あるいは，実施しないことを妥当であると考えている可能性が高い．本研究では後者の可能性について，2 つの要因を推測する．

第一に，このような社員は「他の社員も自分と同様にパッチ適用行動を実施していない」と認識している可能性がある. パッチ未適用によってインシデントが発生した場合，適用しなかった社員のコンプライアンス上の責任が問われる．しかし，その責任を負うのが自分一人ではないと考えると「責任の分散」が起こり[8]，パッチ適用行動に消極的になると考えられる．また，社員がパッチ適用行動に要する労力や時間をコストとみなしているのであれば，このコストを節約している社員と比較して自身が費やすことへの不公平感を抱いても不思議ではない[9]. 管理を担当する端末が増えるほどコストが増えることから, この不公平感は，複数端末を担当する社員ほど強く感じる可能性がある．

第二に，社員の上司が情報セキュリティ行動を評価していない可能性が挙げられる．実験環境の職場では，情報システム担当がパッチ適用行動を実施していない社員だけでなく，その上司に対してもフォローアップのメールを配信する．組織内で上司は部下に対してコンプライアンス項目を遵守するよう指導・監督する立場にある．企業におけるセキュリティのコンプライアンスについても，社員は自身との関係が弱い社員からの影響を受けにくいが，同僚や上司の行動には大きく左右されることが報告されている[1]. ここから，パッチ適用行動を実施していない社員は，自身の上司がその行動を評価していないとの認識を持っていると推察される．実際，パッチ適用未実施に対して上司から

ⓒ 2019 Information Processing Society of Japan

部下に対するマネジメント上の働きかけが行われていない可能性も十分に考えられる．

2.2 パッチ適用行動促進を目的としたナッジの考案

前節にて述べた実験前の状況を踏まえ，本節では，セキュリティパッチ公開後，実験環境にある社員が自身の管理する端末に対してパッチを適用することを促すナッジについて考案する．ナッジは次のように選定した．

１）ナッジ手法の選択

Thaler ら[10]らはナッジとして 5 種類の手法を提案している．今回の実験環境においては，セキュリティパッチの適用がコンプライアンス事項であると社員が認識しているとの前提がある．また，システム上，パッチ適用行動の実施には社員の能動的な判断が必要となる．以上を考慮し，実験で適用可能な手法として 5 種類の中から「動機付け」を選んだ．これは，ある動機によってユーザが社会的に望ましくない行動をとる場合，新たな情報や制度を追加的に提供することで別の動機を刺激し，ユーザが望ましい行動を選択する可能性を高めようとする手法である．

この「動機づけ」手法による情報提供の検討例が，家庭における電力の節約を目的として環境省が進めている「平成 29 年度低炭素型の行動変容を促す情報発信（ナッジ）による家庭等の自発的対策推進事業」である[11]．この事業の一環で，ある電力会社は一定の期間中毎月，無作為に抽出した世帯に対して「ご家庭の省エネルギーレポート」を送付した[12]．このレポートには，各世帯の前月の電力使用量，よく似た世帯との電力使用量の比較，省エネのヒントなどが記載され，ユーザはこれらの情報を受け取らない場合に比べ，電力を節約することが期待されている．

２）「動機付け」で使用する情報の選択

櫻井[13]は，動機付けを 5 種類に分類している．前節で推察した情報システム担当によるフォローアップがあるにもかかわらず社員がパッチ適用行動を実施しない要因に基づき，実験では「取り入れによる調整」の動機付けを刺激する情報を提供することとした．取り入れによる調整の動機づけとは，望ましくない行動の実施，あるいは，望ましい行動の未実施に対して羞恥心や不安を喚起するものである．また，本研究では，セキュリティパッチの未適用に対して羞恥心や不安を感じさせるため,「平均以上効果」や「同調行動」のメカニズムを応用した．平均以上効果とは，集団の中で自身が非常に優秀な成績や状態ではなくとも，平均並み，あるいは，平均よりも優秀であることへの志向性があり，そのために行動を起こすことを指す[14]．同調行動は，自身の見解や態度が他者と異なる場合に他者に自分を合わせようとする行動として現れる[8]．すなわち，他の社員がパッチ適用行動を実施していることを示すことで，未実施の社員がコンプライアンスの観点では「平均以下」の社員である状況にあり，その状況を脱しようとする気持ちを喚起しようとする情報を提供することとした．

さらに，この情報に関しては，2 点の工夫について検討することとした．1 点は，セキュリティパッチ適用行動に要するコストを揃えた比較を促すことである．先に述べたとおり，管理担当の端末が多いほどパッチ適用行動に要するコストは大きくなる．この点を無視して一律に適用行動を促した場合，複数端末を管理する社員の中に不公平感が生じ，情報の配信が逆効果となる可能性がある．そこで，提供する情報の 1 つは，管理端末台数が同等の社員とパッチ適用行動を比較するための情報とした．

もう 1 点は，パッチ適用行動を実施していない社員だけでなく，その上司にも羞恥心や不安を感じさせることである．すなわち，個々の社員を比較する情報ではなく，チームを比較する情報とする．自身の管理するチームのコンプライアンス遵守の状況が平均以下である場合，そのチームの長は，自身のマネジメント能力が他のチーム長の平均よりも下であると認識するかもしれない．このような平均以下の状況を回避しようと，チーム長は，部下の社員に対してパッチ適用行動を働きかけると期待される．また，社員も，自身が原因でチームが平均以下の状況となることを回避しようとパッチ適用行動を実施すると考えられる．

以上から，パッチ適用行動を促すにあたって 2 点の工夫を加えた情報を作成した．この情報は実験において，メールで各社員および上司に送信する．具体的なメールの内容を次に示す．

あ）管理端末台数別にパッチ適用状況を知らせるメール

上述した 1 点目の工夫を加えた情報を提供するメールである（図 1）．メールには，管理端末台数別のパッチ適用率を示した．パッチ適用率は，管理端末台数別に社員数を割り出し，それを母数としたときの，パッチ適用行動を実施した社員数の割合である．

＝＝＝1月第1週集計（集計日：1月15日）＝＝＝
PC台数別 パッチ適用率（%）（適用済人数／全人数）
・1～2台： 49%（18名／37名）
・3～4台： 60%（15名／25名）
・5～11台：50%（4名／8名）

図 1　管理端末台数別パッチ適用率配信メール例

Figure 1　A sample of the email informing users of the rate of security patch applied PCs added up by the number of PCs users manage

い）チーム別のパッチ適用状況を示すメール（図 2）

各チームの社員数を母数とし，パッチ適用行動を実施した社員数の割合を表示する．

＝＝＝1月第1週集計（集計日：1月15日）＝＝＝
チーム別 パッチ適用率（%）（適用済人数／全人数）
・チームα： 43%（3名／7名）
・チームβ： 33%（3名／9名）
・チームγ： 50%（7名／14名）
・チームδ： 50%（9名／18名）
・チームε： 45%（5名／11名）
・チームζ： 45%（5名／11名）

図 2　チーム別パッチ適用率配信メール例

Figure 2　A sample of the email informing users of the rate of

ⓒ 2019 Information Processing Society of Japan

security patch applied PCs added up by project

3. 実験

実験では，従来のセキュリティパッチ適用を依頼するメールに追加して，前節で作成したナッジのメールを社員に配信した．このナッジが社員のパッチ適用行動を促進する効果を観測するために実験を実施する．ナッジの効果は，管理台数別の適用率を知らせるメール（図 1），チーム別の適用率を知らせるメール（図 2），および，および両方の配信した条件間で比較した．また，この効果は，社員が自身の管理する端末に対してパッチを適用するタイミング，適用作業終了の社員の割合，以上 2 指標で評価した．

3.1 方法

実験期間は 4 か月間であった．実験環境はシステム会社の，一職場であった．実験対象は，この職場の社員 77 名であった．この職場では担当する業務によって 6 つのチームが存在する．3 種類の配信メール（管理台数別のみ，チーム別のみ, 両方）の効果をなるべく客観的に検証するため，1 グループは異なる 2 チームの社員から構成される（グループ A には，あるチームの社員半数 A1 と，別のチームの社員の半数 A2 など）を割り当てた．また，対象者のうち 2 チームを兼務していた社員 3 名のパッチ適用データについては，両方のチームで使用した．このような設計でメール配信前後 2 か月間（それぞれ月例パッチ配信日を 2 回含む）での適用率の変化を比較した．

- グループ A（28 名）： 管理台数別のみの適用率
  - A1（9 名），A2（19 名）
- グループ B（24 名）： チーム別のみの適用率
  - B1（10 名），B2（14 名）
- グループ C（25 名）： 両方の適用率
  - C1（12 名），C2（13 名）

メール配信は, 毎週末に 1 回（金曜が 6 回, 木曜が 3 回），3 グループに同時配信した．週 1 回としたのは，文面上の催促はしていないとはいえ強制的な印象を与えないためである．配信にあたっては，社内の承認を経て，その旨をメール本文に含めることで本実験が正式な試行であることを社員に伝えた．

3.2 仮説

各チームについて，パッチ適用状況のメール配信の前後で，下記の効果が得られるという仮説を立てた．

- **仮説 1** ：パッチ適用率の最大値が更新される
- **仮説 2** ：パッチ適用率が一定割合（25%，50%，75%など）を超えるまでにかかる期間が短縮する
- **仮説 3** ：配信後 2 か月のパッチ適用率の平均値は，配信前 2 か月の平均値よりも向上する

4. 評価

図 3 に各チーム A1，A2，B1，B2，C1，C2 のパッチ適用率の時系列変化（4 か月間）を示す．横軸は適用率の集計回（毎週水曜と金曜とした．毎月第 2 水曜が日本での月

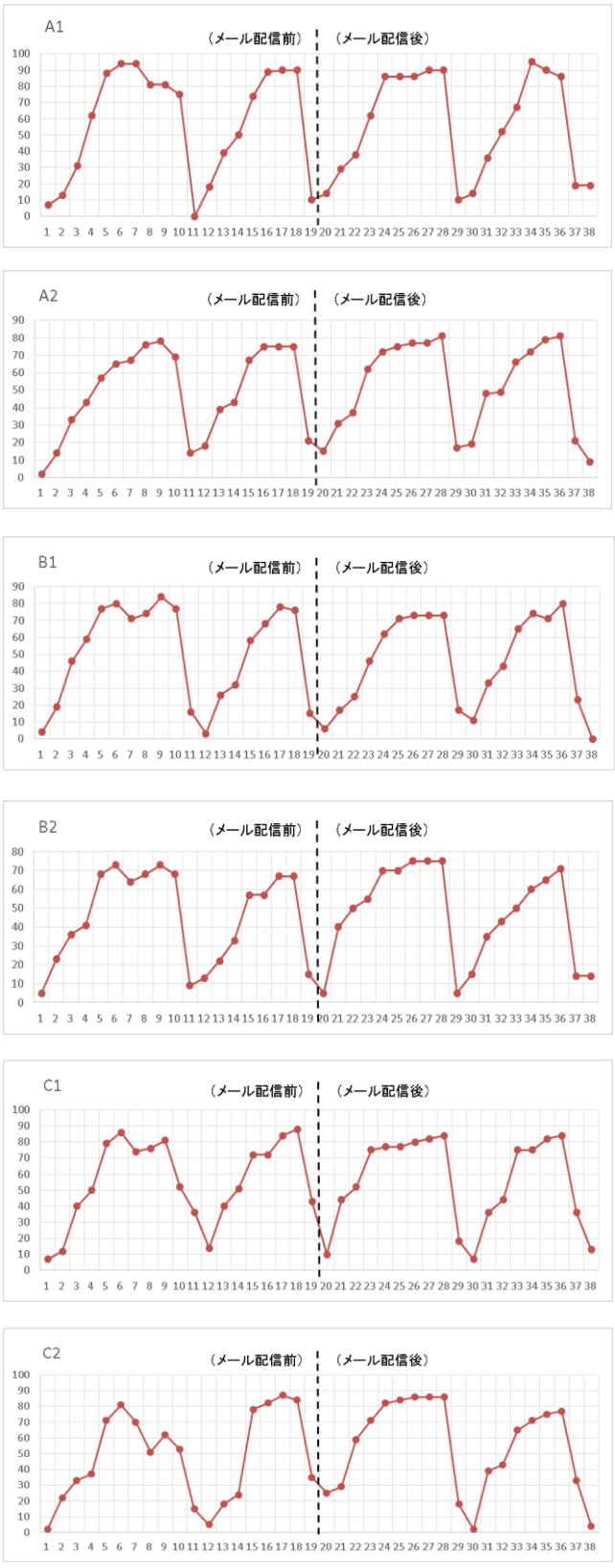

図 3 各チームのパッチ適用率の時系列変化

Figure 3 The time-series changes of the security patch applied rate by project

ⓒ 2019 Information Processing Society of Japan

例パッチ配信日)，縦軸がパッチ適用率を表している．どのグラフも山が４つあるが，２つ目の山（2 か月目）と 3 つ目の山（3 か月目）の境が初回のナッジメール配信日（集計 19 回目）である．実験期間における Microsoft の月例パッチ配信日は集計日のうち 1、11、19、29、37 回目の日であるが，配信直後のパッチ適用率はパッチ未適用の端末が増えるため 0 近くにリセットされる．

4.1 仮説１の検証

図 3 のグラフからもおよそ読み取れるが，データを参照したところ，どのチームにおいてもメール配信後のパッチ適用率の最大値が顕著に向上したとはいえなかった（仮説１は不成立）

4.2 仮説２の検証

図 3 のグラフから, パッチ適用率が一定割合（25%, 50%, 75%など）に達するまでの期間は，いくつかのチームにおいては, メール配信後のグラフの勾配(山の谷からピークに向けての区間)が配信前と比べて急になっていることから，短縮されているように見える．特にメール配信前後 1 か月（山の 2 つ目と 3 つ目）において比較的顕著に違いが見られる．表 1 はグラフの元データの一部であり，1 か月目の各チームのパッチ適用率の集計データ（単位は%）である．太字の数値は，各チームについて月例パッチ配信による適用率のリセットから初めて 25%，50%，75%を超えたことを表す．その他の月についても同様の集計データを作成している．

表 2 は，表 1 のようなデータをもとに，各チームの 4 か月間のパッチ適用率が月例パッチ配信によるリセットから初めて 25%，50%，75%を超えるまでの集計回数の一覧でである．ただしチームならびに月度によっては，月例パッチ配信日以降にその月度の適用率が最低値となった場合も存在したので（理由は不明だが，当社システムによる端末のパッチ適用状況データの収集に遅延があったのかもしれない)，その場合は配信日からではなく，その集計日からの集計回数を記述している．「未達」は 75%に達しなかったことを表す．表 2 から，メール配信前後 2 か月で集計回数の短縮がみられるのは 25%の C2, 75%の C1 のみであるこ

表 1 各チームの某月のパッチ適用率集計データ（単位は%．太字は 25%，50%，75%を初めて超えたことを示す）

Table 1　The patch applied rate by project in the first month before the informing mail. The unit of numbers is %, and the numbers in bold fonts represent that the rate exceeds 25%, 50%, and 75% for the first time in this month.

月	集計回	パッチ公開日	チーム					
			A1	A2	B1	B2	C1	C2
1か月目	1	○	7	2	4	5	7	2
	2		13	14	19	23	12	22
	3		**31**	**33**	**46**	**36**	**40**	**33**
	4		**62**	43	**59**	41	**50**	37
	5		**88**	**57**	**77**	**68**	**79**	**71**
	6		94	65	80	73	86	**81**
	7		94	67	71	64	74	70
	8		81	**76**	74	68	76	51
	9		81	78	84	73	81	62
	10		75	69	77	68	52	53
2か月目	11	○	0	14	16	9	36	15
	12		18	18	3	13	14	5

表 2　各チームのパッチ適用率が月例パッチによるリセットから 25%，50%，75%を超えるまでの集計回数（太字部分はメール配信後の集計回数が減ったチームを表す）

Table 2　The number of the calculating that the patch applied rate every month by project exceeds25%, 50%, and 75% for the first time after the reset to 0% by monthly patch release. The columns highlighted in bold fonts represent the number of the calculating decreased after the informing mail.

適用率	月	チーム					
		A1	A2	B1	B2	C1	C2
25%	1か月目	2	2	2	2	2	**2**
	2か月目	2	2	1	3	1	**3**
	3か月目	2	1	2	1	1	**1**
	4か月目	2	2	1	2	1	**1**
50%	1か月目	3	4	3	4	3	4
	2か月目	3	4	3	4	2	3
	3か月目	4	4	4	3	2	2
	4か月目	3	4	3	4	3	3
75%	1か月目	4	7	4	未達	**4**	5
	2か月目	5	5	5	未達	**5**	3
	3か月目	5	5	未達	6	**3**	4
	4か月目	5	6	6	未達	**3**	5

とから，パッチ適用状況メールがパッチ適用率のピークへの早期到達を促すとはいえない（仮説２は不成立）．

4.3 仮説３の検証

図 3 のグラフを眺めてみると，チームによってはメール配信前よりも配信後の方が期間を通じて高いパッチ適用率を維持しているように見える．これを検証するため，メール配信前後 2 か月間のパッチ適用率の平均値および中央値を調べた（表 3)．表 3 から平均値・中央値とも数値の増加があるのは 6 チーム中 4 チームである．そこで Wilcoxon の符号付き順位検定を用いて，メール配信がチーム全体を通じてパッチ適用率の平均値または中央値に影響があったかを調べた．結果，平均値では p=0.09（<0.1）となり 10%水準で有意であったが中央値では p=0.16 となり有意ではなかった．平均値と中央値どちらの結果に重点をおくべきか，実験期間における各チームのパッチ適用率の度数分布を参照したところ（図 4)，右寄りの分布で非対称であるた

ⓒ 2019 Information Processing Society of Japan

め中央値の検定結果を優先すべきと考える．ただし平均値の検定結果も，パッチ適用率自体の値域が[0,100]と狭いので一定の参考値にはなる．以上のことから，パッチ適用率（管理台数別ならびにプロジェクト別）の配信メールという“ナッジ”は，統計上の差は示さなかったものの，パッチ適用促進効果を持つ可能性がある．一方，仮説３としては不成立となる．

表 3　配信前後 2 か月間のパッチ適用率の平均値ならびに中央値（太字／斜字は 4 ポイント以上適用率が向上／低下を表す）

Table 3　The mean and median values of the patch applied rate by project before and after the informing mail. The numbers in bold fonts represents the difference by more than 4 points.

	ナッジメール	チーム					
		A1	A2	B1	B2	C1	C2
平均値	前	70	58	62	54	64	57
	後	71	**65**	*58*	**60**	**69**	**68**
中央値	前	81	67	71	64	72	62
	後	**86**	**72**	68	62	**76**	**73**

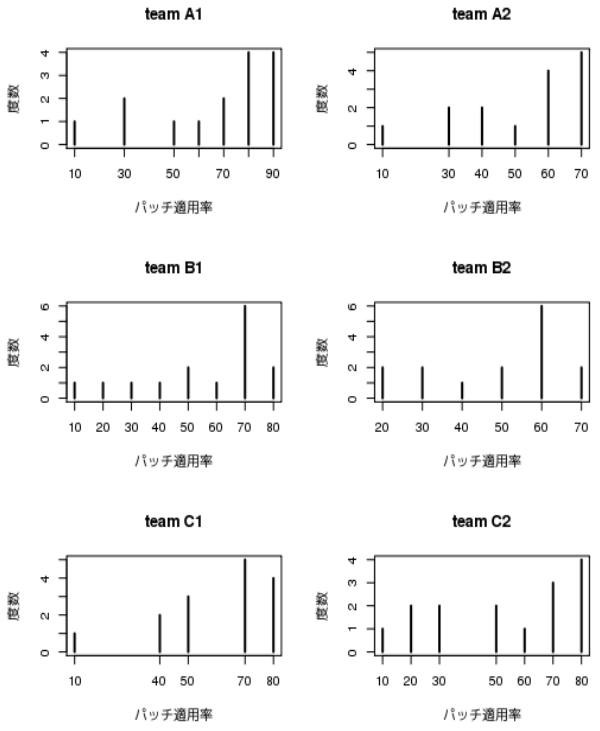

図 4　実験期間中のチーム別パッチ適用率の度数分布

Figure 4　The histograms of the patch applied rate by project in the experimental period.

5. 考察

以上の結果から，管理台数別，チーム別に他の社員のパッチ適用状況を定期的に通知するというナッジ（心理的刺激）に関する仮説１，２，３はいずれも不成立であった．ただし仮説３（パッチ適用促進効果）の検証で実施したデータ分析結果の一部は，ナッジが奏功した可能性を示した．一方で，今回のデータ分析の結果を今後のナッジ設計や実験要領に活かすため，改善点を考察する．

(1) チーム別提示の効果は小さかった可能性がある

表 3 が示すように，グループ B（チーム B1 と B2）は，配信前後での適用率のポイント向上が他のチームに比べて少ない（むしろ低下している）．このことからチーム別のパッチ適用率提示は適用促進に奏功しなかった可能性がある．グループ B の配信メールの内容はチーム別の適用状況のみであったことから，（グループ A，C も含めて）チームに対する各社員の帰属意識の希薄さに原因があると考える．

今回実験に協力いただいた職場の各チームは，実はより具体的な受託業務に基づくサブチームで構成されている．また，職場風土としても上意下達というより各社員の主体性が重視され，上司とも対等に議論するような職場であった．これら２つの背景から，チーム別の状況の提示は各社員に，パッチ適用についてチームへの貢献意識を刺激しなかった可能性が考えられる．したがってこのような職場においては，チーム別よりも居室別であるとか LAN のネットワークセグメント別で適用状況を示した方が，より貢献意識が高まるかもしれない．

(2) 動機づけの手段の強化

櫻井[13]の動機づけの 5 段階の分類には「1. 外的調整（金銭的インセンティブや賞罰などの提供）」，「2．取り入れによる調整（恥ずかしさや不安を刺激する）」，「3. 同一化／4. 統合による調整（対象者にとっての重要性や目標達成にパッチ適用行動がプラスになることを示す．2 つの動機は類似している為，区別されないこともある）」，「5．内的調整（行動そのものの魅力や楽しさをアピール）」がある．1. から 5. に進むにつれて対象者の裁量は広がるが，行動促進の効果は小さくなるとされる．

2.2 節の２）で述べたように，今回の実験ではパッチ適用行動を促す動機づけの手段として，「2．取り入れによる調整」を採用し，それを刺激する具体的手段として管理台数別やチーム別の適用状況の情報を社員に提供した．パッチ適用促進ナッジの強化策として他の分類に属する手段を追加することが考えられるが，1．と 3．によるパッチ適用促進は民間企業としては難しい．1. についてはパッチ適用促進に経営陣が理解を示して予算を割いてもらうことの難しさ，3. については社員各自の業務とパッチ適用の方向性の乖離があるためである．

残る 5．であるがパッチ適用にゲーム要素や承認要素を盛り込むことが考えられる．具体的には，各社員に対して管理台数別やプロジェクト別でパッチ適用が早く完了した人のランキングを提示したり（もちろん各社員には他の社員の順位は提示しない），上位の人を配信メールの中で月度ごとに提示するといったことが考えられる．今回の 2．の動機づけに 5．を加えることでより効果の高いパッチ適用

ⓒ 2019 Information Processing Society of Japan

効果が期待できる．

(3) パッチ適用率がある程度高くなってから配信する

今回，パッチ適用率の値に関わらず毎週配信を実施したが，適用率が低いうちは社員に「他の社員もパッチを適用していないので，自分もまだしなくてよい」と考えさせていた可能性がある．このような問題を軽減するためには，はじめに，どの程度の割合のパッチ適用率が社員のパッチ適用を促進するのか調べ，促進効果が確認される適用率の閾値に到達したところでメールを配信し始める工夫が考えられる．

6. まとめ

本研究の目的は，心理学の観点から，ユーザのセキュリティ行動のメカニズム，および，それを促進する仕組みについての案を示すことである．はじめに，ユーザのセキュリティ行動に関する心理的要因について説明した．モデルとして，セキュリティに関する理解，肯定的態度，主体性がセキュリティ行動への積極性に寄与しているとされる．ただし，それぞれをユーザが持つためには数々の心理的な困難があることを示した．次に，セキュリティ行動を促す対策に関する知見や実践例を紹介した．従来のセキュリティ教育の効果は頑健に確認されていない．そのため，望ましい選択や行動を促す手法の一つとして，近年，社会的な問題の対策や施策にも応用されているナッジに着目し，セキュリティ行動を促進する仕組みに援用することとした．

対象とするセキュリティ行動は，各社員が管理するパソコン端末への Windows の月例セキュリティパッチ適用とした．企業で現在行われているパッチ適用促進策の問題点を考察し，この考察に基づいて他者のセキュリティパッチ適用状況をメールで知らせるナッジを提案し検証を行った．結果，統計上の顕著な効果は認められなかったものの，ナッジが奏功した可能性といくつかの改善点を得た．

参考文献

[1] Blythe, J.M., Coventry, J., & Little, L. (2015) Unpacking security policy compliance: The motivators and barriers of employees' security behaviors. Proceedings of Symposium On Usable Privacy and Security, 103-122.
[2] Ng, B. & Rahim, M. (2005) A Socio-Behavioral Study of Home Computer Users' Intention to Practice Security. Proceedings of the 9th Pacific Asia Conference on Information Systems.
[3] Junger, M., Montoya, L., & Overink, F-J. (2017) Priming and warnings are not effective to prevent social engineering attacks. Computers in Human Behavior 66 75-87.
[4] West, R. (2008) The psychology of security. Communications of the ACM, 51(4), 34-40.
[5] Thaler, R.H. & Sunstein, C.R. (2009) Nudge: Improving Decisions About Health, Wealth, and Happiness. Penguin Books.
[6] IPA（2017）：世界中で感染が拡大中のランサムウェアに悪用されている Microsoft 製品の脆弱性対策について. Retrieved from https://www.ipa.go.jp/security/ciadr/vul/20170514-ransomware.html（アクセス日 2019 年 1 月 26 日）
[7] 日立製作所セキュリティ事業統括本部（2018）社会インフラを守る日立のセキュリティ．はいたっく, 2-4.
[8] 今井芳昭（1996）影響力を解剖する．福村出版.
[9] Beautement, A., Sasse, M. & Wonham, M. (2009) The compliance budget: managing security behaviour in organisations. Proceedings of the 2008 workshop on New security paradigms, 47-58.
[10] Thaler, R.H., Sunstein, C.R., & Balz, J.P.（2010）Choice Architecture. Available at SSRN: https://ssrn.com/abstract=1583509 or http://dx.doi.org/10.2139/ssrn.1583509（アクセス日 2019 年 1 月 26 日）
[11] 環境省 (2017) 日本版ナッジ・ユニットを発足します！～平成 29 年度低炭素型の行動変容を促す情報発信（ナッジ）による家庭等の自発的対策推進事業の採択案件について～. 報道発表資料. http://www.env.go.jp/press/103926.html（アクセス日 2019 年 1 月 26 日）
[12] 東北電力（2017）環境省ナッジ事業への参画に伴う省エネレポート等の送付について．https://www.tohoku-epco.co.jp/information/1196020_821.html（アクセス日 2019 年 1 月 26 日）
[13] 櫻井茂男（2009）自ら学ぶ意欲の心理学ーキャリア発達の視点を加えて． 有斐閣.
[14] Alicke, M. D., Klotz, M. L., Breitenbecher, D. L., Yurak, T. J., & Vredenburg, D. S. (1995) Personal contact, individuation, and the better-than-average effect. Journal of Personality and Social Psychology, 68(5), 804-825.

ⓒ 2019 Information Processing Society of Japan