

氏名（本籍）	畑島 隆（福岡県）
学位の種類	博士（工学）
学位記番号	乙第91号
学位授与の日付	令和5年3月22日
学位授与の要件	学位規則第4条第2項該当
学位論文題目	インターネット利用者の行動分析研究：Web ページ関心度，セキュリティ不 安全行動，セキュリティ疲れ
論文審査委員	(主査) 教授 谷本 茂明 (副査) 教授 岩下 基 教授 滝 聖子 准教授 矢吹 太朗 東京都市大学 教授 関 良明

学位論文の要旨

インターネット利用者の行動分析研究：Web ページ関心度，セキュリティ不 安全行動，セキュリティ疲れ

学術や軍事を目的としない情報流通プラットフォームやコミュニケーション手段としてのインターネットは 1990 年代後半から普及が始まり，2020 年代である現代では社会基盤として不可欠である。本研究は，インターネットを日常利用する人間の行動を 3 つの観点から研究したものである。3 つの観点とは，Web ページへの関心の現れとしての情報選択行動，私有端末を用いたりモートワークやテレワーク時について行われる従業員による不
安全行動，そして求められるセキュリティ対策行動に疲弊し正しく実施が出来なくなるセキュリティ疲労である。

最初に，Web ページへのアクセス行動に関する研究として検索サービス NTT DIRECTORY のログ分析を行い，インターネット利用者が Web サーバ上のどのページに関心を寄せているかを示す指標である関心度（TBI：Time-Based Interest）の算出方法を開発した。TBI の算出式はアクセスの発生による増加関数とアクセス間隔が空くことによる減衰比関数から構成される。減衰比関数を同一 Web ページへの最終アクセスからの経過時間による指数関数と演繹的に定義し，減衰比定数を特定イベントに関する検索頻度が時間経過によって減衰していく比率によって導出した。TBI の性質として，ページへのアクセス数と人気度の関係と同様の Zipf 分布となることを示した。また，TBI をはじめとしたアクセス傾向の分析表示システム CyberRanking を開発した。

次に，テレワークや私有モバイル端末の業務利用（BYOD：Bring Your Own Device）におけるセ

セキュリティ不安全行動(unsafe act)の研究を実施した。セキュリティ不安全行動とは、セキュリティ対策が求められているにもかかわらず、その対策行動から外れたインシデントの発生リスクを高める行為をしてしまうことである。本研究では2件の検討を実施した。まず、テレワーク時のセキュリティ不安全行動のうち悪意なくつい行ってしまいう情報漏洩を対象として、不安全行動をするテレワーカーの性格や行動に特徴があることを示した。次に、BYODに関する規約の整備状況、従業員の規約遵守状況、そしてBYOD実施による業務データの取扱状況の調査結果から、セキュリティ不安全行動がリスク補償行動(risk compensation)によって説明可能であることを示した。これらの結果から、前者の研究では、(1)確信的に敢行してしまう性向を抑止する施策が効果的、(2)テレワークに関する情報セキュリティ対策であっても、従業員が所属する職場についてセキュリティ環境を危険度の低い状態にする施策が有効、(3)情報セキュリティ対策の実施を促す施策に一定の効果があることは論を待たないが、本研究では有意な差は見られず、対策効果に個人差があることが示唆されるという3点の知見が得られた。後者の研究では、私有モバイル端末の業務利用が規約により許可されている従業員は、漏洩時のリスクが高い個人に関する情報のような機密度の高いデータでもテレワーク実施時に取り扱い、保存場所として自宅や端末内といった危険な場所も選択している傾向が見られた。この知見により、規約や環境の整備といった企業施策によってBYODを低リスク化する際には、BYOD実施者による高リスク行動によって全体のリスクレベルが補償されてしまうことに注意する必要があることを示した。

最後に、高度化し複雑化するばかりのセキュリティ対策に対してインターネット利用者が疲弊し、セキュリティ対策を実施させようとする施策の効果が上がらなくなる、セキュリティ疲れ(Security Fatigue)について研究した。この研究では、セキュリティ疲労度の測定尺度(SFS-13およびSFS-9)の開発、セキュリティ疲労度とセキュリティ対策実施度を組み合わせたセキュリティコンディションマトリクスの開発を行った。セキュリティ疲労度測定尺度は、一般的な燃え尽き症候群(バーンアウト)の測定手法の援用した質問紙調査によって開発した。具体的には、セキュリティ対策に疲弊したインターネット利用者が「セキュリティ疲れ状態」となり、この状態が進行することで情報セキュリティ対策を実施しなくなる「セキュリティバーンアウト状態」となるという仮説のもと開発を実施した。セキュリティ疲労度測定尺度の性質として、セキュリティ疲労度は低すぎても高すぎても良くなく、適度に緊張感がある中程度が理想状態であることを示した。また、セキュリティコンディションマトリクスを用いたリスクアセスメントによって、セキュリティ対策に対するインターネット利用者の理想状態は、セキュリティ対策に対して適度な緊張感を持っており、かつ、セキュリティ対策を実施している状態であることを明らかにした。そして、質問紙調査を実施し、調査対象者が理想状態にあるときにはその状態を維持し、それ以外の各状態であるときには理想状態に近づけるための対策を示した。更に、セキュリティコンディションマトリクスの拡張およびセキュリティ疲労度測定尺度の応用研究について示した。

これらの研究によってインターネット利用者の行動が測定可能となり、それぞれの行動の指標値や心理的な状態を知ることが出来る。これらの研究が有益なサービス開発や、よりよい利用環境を提供するための技術開発、より安心安全にインターネットを利用するための規約の整備の実

施が可能となることを期待する。

審査結果の要旨

インターネットへのアクセス機器として、スマートフォンやタブレット端末が急速に増えている。これらの世帯ベースでの普及率を例にとると、スマートフォンで 88.4%、タブレット型端末では 37.6%といずれも増加傾向にある(内閣府, 2022 年)。さらに、DX (Digital Transformation) の進展に伴い、ビジネス変革も進んでいる。このように、インターネット環境は、情報収集やコミュニケーション手段として広く一般社会に浸透しており、社会基盤として不可欠なものとなっている。本論文は、インターネット環境が 1990 年代後半から本格的に商用利用されてから社会基盤として広く浸透してきた現在に至る約 20 年間におけるインターネットを日常利用する人間の行動を対象にしている。具体的には、人間の行動データ分析によって、インターネット利用者にとって「より快適なサービス」、「よりセキュアな利用環境」を構築するための知見の提供を目的とした研究がなされており、これらの研究により、インターネット環境でのより利便性の高いサービス開発、より安心安全にインターネットを利用するための規約の整備などに寄与するものである。

本論文は、序論と結論を含む 5 部から構成されている。第 I 部で序論を述べ、本論文の背景と目的、構成について述べている。

第 II 部では、よりよいサービス提供をするための Web ページ関心度の可視化に関する研究が述べられている。具体的には、インターネット利用者の行動結果である Web ページへのアクセス状況、即ち、Web ページへの関心の集まり度合いを関心度(TBI : Time-Based Interest)として指標化した結果を提案している。1990 年代後半からインターネットの商用利用の進展に伴い、Web ページの関心度の指標として Page View(Web ページの閲覧回数)や Visit(Web ページの閲覧時間)などが開発された。しかし、これらの指標は、アクセスログのタイムスタンプが考慮されていないため、利用者がコンテンツにどの程度興味をもっているか判断するには不十分であった。本論文では、Web ページ検索サービス (NTT DIRECTORY) のログを用いた分析により、同一 Web ページへのアクセス間隔をパラメータとする Web ページ関心度 (TBI) の算出式を提案した。提案指標である TBI は、アクセス発生により増加し、アクセスされていない期間は指数関数的に減衰する性質を有している。提案指標である TBI の評価として、NTT DIRECTORY におけるサイト表示順の指標として実装され一般的に利用されるなど、その有用性を明らかにしている。

第 III 部では、安心安全なセキュリティ環境を構築・維持するために、テレワーク環境を対象に、利用者である従業員の行動の可視化によるセキュア化の方策を提案している。具体的な方策の検討に際し、従業員の業務行動におけるセキュリティ対策、特に、セキュリティ対策が求められているにもかかわらず、その対策行動から外れた行動をとるセキュリティ不安全行動を対象としている。最初に、テレワーク時の意図しない情報漏洩というセキュリティ不安全行動がテレワークカ

一の性格によって発生の仕方が異なるかについて、質問紙調査を用いて分析した結果、「確信的に敢行してしまう性向を抑止する施策が効果的」などの知見を得ている。次に、テレワークの規約とテレワーカーの業務実施状況の分析結果から、セキュリティ不安全行動がリスク補償行動として、「会社の規約を守る人は、セキュリティ事故のリスクを低く見積り、より機密度の高いデータを取り扱う傾向がある」などの知見を得ている。これらの行動は不安全行動の一種であり、情報セキュリティインシデントが発生した場合、情報セキュリティリスクがより高くなることが見込まれるため、このように新たな危険行動に対する対策の重要性を明らかにした。

第IV部では、セキュリティ疲れの測定尺度開発と、測定尺度の応用について提案されている。セキュリティ疲れは、2009年のFurnellらの研究「ユーザがセキュリティを維持するのが面倒になったりするしきい値が存在する」、2016年のStantonらの研究「情報セキュリティ疲れを起こした人は、鈍感になり、うんざりしている」などの研究がなされており、セキュリティ対策における疲れにより、セキュリティリスクが高まり、セキュリティ対策の効果が落ちることが懸念されている。しかし、これらの対策を具現化する際に必要となるセキュリティ疲れの指標などに関する検討は十分になされていない。本論文では、インターネット利用者として大学生から社会人までを対象に質問紙調査を行い、潜在ランク理論などに基づく分析により、セキュリティ疲れの測定尺度を開発している。具体的には、セキュリティ対策に疲弊したインターネット利用者が「セキュリティ疲れ状態」となり、この状態が進行することで情報セキュリティ対策を実施しなくなる状態を「セキュリティバーンアウト状態」と定義し、一般的な燃え尽き症候群(バーンアウト)の測定手法の援用によりセキュリティ疲労度測定尺度を新たに開発した。この結果、開発した測定尺度は、セキュリティ対策に対する意識を適度に有している中程度の尺度得点が理想的であることを明らかにした。この尺度により、セキュリティ疲労に対する状態が理想状態であれば維持させ、それ以外であればよりよい状態に移行させるための施策を実施させるなど、新たなセキュリティ対策の適用が期待できる。

第V部では、結論として、本論文で得られた成果を総括している。

本研究の成果は、審査付き論文6本(うち1本は研究速報)と国際会議論文1本として公表しており、公表も適切であると判断した。以上の研究成果により、本論文が博士(工学)の学位授与に十分値する内容であると判断した。