

令和 2 年 6 月 22 日現在

機関番号：52201
研究種目：基盤研究(C) (一般)
研究期間：2017～2019
課題番号：17K00504
研究課題名(和文) 仮想現実の体験で実現する情報セキュリティの脅威と安全を教育するeラーニングの開発

研究課題名(英文) Development of e-learning to educate cyber security safety realized by virtual reality

研究代表者
石原 学 (ISHIHARA, MANABU)
小山工業高等専門学校・電気電子創造工学科・教授

研究者番号：20211047
交付決定額(研究期間全体)：(直接経費) 3,500,000円

研究成果の概要(和文)：本研究は、情報セキュリティ教育に仮想現実の手法を取り入れ、ウイルスや攻撃を体験できるシステムを構築することで、通常は目に見えない情報の安全について理解させるシステムについて試作する。本システムは従来の可視化技術の先にある仮想現実を導入することで、情報セキュリティの理解を深める教育システムの構築を目指した。組織内に感染したPCからの異常通信によるネットワーク内の通信量の多さ等の変化を、水の流れを触るように体験できるシステムを構築した。

研究成果の学術的意義や社会的意義

セキュリティの1つであるウイルス対策ソフトウェア技術は、ネットワークを分析し、情報漏えいやウイルスソフトウェアを検出することができる。コンピュータは、検出されたウイルスをバックグラウンドで処理するように出来ている。今回、これらのウイルスによりネットワーク上でトラフィックの異常を感知することで、力覚に反応させて、セキュリティ技術の視覚化(可触化)を行う装置を試作した。これらは、セキュリティ上のウイルスが発生した場合の異常を体験するなど、初心者の教育にも対応できると考えている。

研究成果の概要(英文)：With recent developments in Virtual Reality technology, the VR industry is thriving and the availability of VR experience facilities and VR content is increasing. Currently, VR provides a virtual experience by acting on vision and audio. In this paper we experimented on determination criteria of the haptic force and constructed the system for experiment.
The cost has reduced and the diversification of VR equipment itself has already progressed since the appearance of VR technology; this technology is expected to become accessible to individuals worldwide in the future. The antivirus software is playing an important role in networking. It is interesting to combine antivirus software and haptic devices. Accordingly, we developed the system which analyze an IP address to cope with an attack to Web and can express the offensive ability from an opponent sensuously in haptic devices.

研究分野：仮想現実

キーワード：サイバーセキュリティ 仮想現実 教育工学 ネットワーク工学

様式 C - 19、F - 19 - 1、Z - 19 (共通)

1. 研究開始当初の背景

情報セキュリティの重要性は、十分に述べられているものの、現在の研究としては、ウイルス等への感染防止やウイルスの性質の知識の理解におかれている。また、システムとしても、最近の科研費の採択表題等においても、デジタル技術の観点から情報の安全性(暗号化を含む)の開発関係などが採択されている。情報セキュリティ教育においても、プラットフォームの開発やクラウドの仮想化技術を使用するシステムなどの研究が行われている。クラウドを含む情報セキュリティの可視化については、国立研究開発法人情報通信研究機構の NICTER において図 1 (NICTER の HP より) のような成果が得られ可視化としては大きな成果が得られているものの経費はたいへん高額であり、一般の普及や教育の利用については、まだほとんど行われていない。

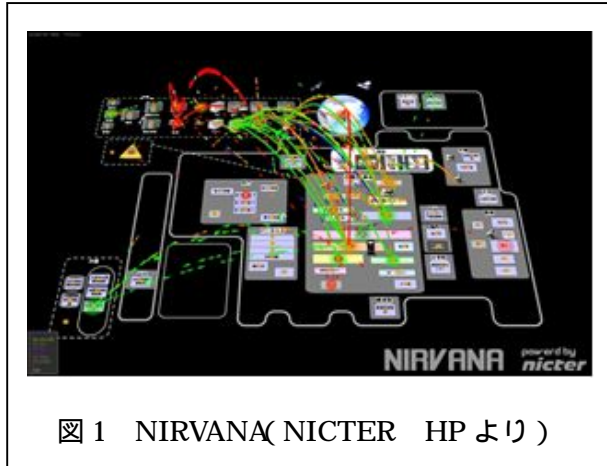


図 1 NIRVANA(NICTER HP より)

また、「サイバーセキュリティ戦略」(平成 25 年 6 月 10 日情報セキュリティ政策会議決定)で示された人材育成に係る課題として、情報セキュリティ人材の不足解消に向け、積極的な取組が必要とされているが、現在においても益々の質的不足や量的不足が示されている。その中で、**セキュリティのスキル向上のための実践的取組の実施・開発が提示されている。**

国立高専機構においても、情報セキュリティ人材育成として、カリキュラムの創設を含めて対応している。申請者においても、この人材育成プロジェクトの実践校責任者として運用を行っているところだが、当初指摘した、デ

ジタルデータを利用した演習方式に留まっている。その他の、拠点大学においても同様な傾向がみられる。

2. 研究の目的

本研究は、情報セキュリティ教育に仮想現実の手法を取り入れ、ウイルスや攻撃を体験できるシステムを構築することで、通常目に見えない情報の安全について理解させるシステムについて試作する。情報セキュリティ教育は一般的に、情報倫理教育との関係から、紙ベースやデジタルデータを利用して演習方式(パワーポイントや実験など)を通して理解させる教材が多い。仮想現実と連動させた体験型のシステムについての開発例は無いようである。本システムは従来の可視化技術の先にある仮想現実を導入することで、情報セキュリティの理解を深める教育システムの構築を目指し、教育システムへの導入を検討する。

3. 研究の方法

本研究では、ウイルスの危険性によって、人間が力覚としての感覚量として大きさから直感的な危険率の対応を測定する。これは、危険率などを色分けデータとして表現されていることからそれらとの対応についても考察する。トラフィック量を力覚の変化量に再現し、その対応を明らかにする。上記の 2 つの方法を利用して、危険率と情報データの流れを力覚データに変換する手法を開発する。これらを踏まえて、ウイルスチェックを行うシステムと力覚システムとの統合を図り、教育システムとしての構築を行う。

4. 研究成果

4.1 力の閾値測定実験

4.1.1 実験方法

まず始めに提示する力がどの程度の差であれば違いが認識できるのかを確認する。この差を基に提示する力を段階にわけトラフィック量と対応させる。アインシュタインとウェーバの報告によれば力覚に関するウェーバ比はおよそ 0.2 であるとされる。しかし Omni が提示する力は線形的なものではないためこのウェーバ比を用いることができない。そのため違いが認識できる差となる閾値を求める。なお本稿では 0.0 から 1.0 という値を使用している。これは Omni が提示できる最大提示力を 1.0、何も提示しない状態を 0.0 として表している。これをフォースレベルと呼ぶ。Omni の最大提示力は $3.0 \text{ (kg-m/s}^2\text{)} (3.0[\text{N}])$ であるため、フォースレベル 1.0 はおよそ $3.0[\text{N}]$ に当たる。

被験者に Omni のペン部分を持たせ、仮想空間上の左半分と右半分で異なる力の大きさを比較させた。片側は標準刺激、逆側は 4 種類の比較刺激と標準刺激の 5 種類からランダムなものが提示される。比較刺激は Omni 内の力覚提示用関数値 0.0~0.8, step0.2 で提示し、標準刺激は中央値である 0.4 で提示する。プログラムの実行画面を図 2 に示す。左右の力の大きさを比較して、「左の方が強い」、「同じくらい」、「右の方が強い」の 3 つから選択させる三件法を用いて回

答を得る．得られたデータは最尤法で処理を行った．

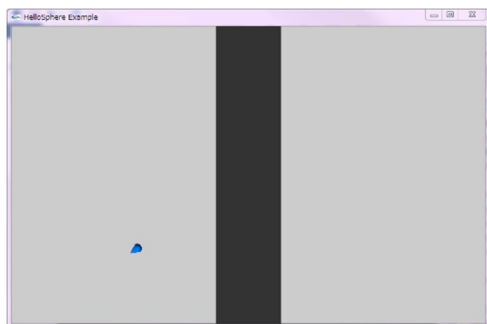


図 2 力の閾値測定実験画面

表 1 力の閾値測定実験結果

標準刺激値 a=0.4 step=0.2			
比較刺激 xi	a <	a ≈ xi	a > xi
	xi		
0.0	0	0	14
0.2	0	0	14
0.4	1	7	6
0.6	13	1	0
0.8	14	0	0

4.1.2 実験結果

18 歳から 21 歳の 14 人の被験者から表 1 の結果を得た．表における a は標準刺激を，xi は比較刺激を表している．表 1 を最尤法で処理したものを図 3 に，得られたパラメータを表 2 に示す．

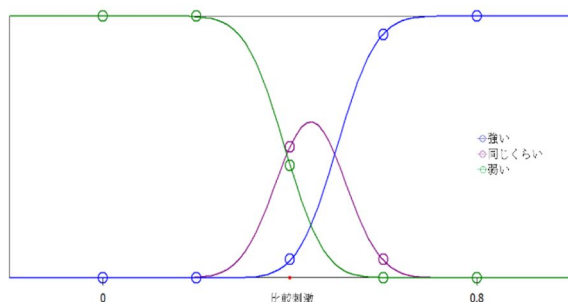


図 3 力の閾値実験解析結果

表 2 力の閾値実験のパラメータ

平均 μ	分散	判断基準 c	弁別閾 $Z_{0.75}$	上弁別閾 $\mu + Z_{0.75}$	下弁別閾 $\mu - Z_{0.75}$
0.44	0.067	0.056	0.045	0.485	0.395

表 2 のパラメータ値は μ を平均， を分散， c を判断基準， $Z_{0.75}$ を正規分布における累積確立が 0.75 となる正規偏差を表す．また， $\mu + Z_{0.75}$ は上弁別閾， $\mu - Z_{0.75}$ は下弁別閾を表す．図 3 は提示した比較刺激を横軸として，確率分布（判断の比率）を縦軸としてグラフ化したものである．各点は実験で得られたデータ値を表している．またこれらのデータから得られたパラメータ値による判断確率を曲線で表している．

表 1 から標準刺激同士を比較した場合以外では，ほとんどの被験者が正しく違いを理解していることが分かる．また，表 2 の判断基準 c は c=0.056 の値なので，step0.2 の間隔を有していれば十分に与える刺激の差を認識できる．これより作成するシステムでは提示する力をフォースレベル 0.2 ごとに段階わけし，トラフィック量と関連付けることでトラフィック量の差を認識できるようになる．

4.2 試作システム設計

作成したシステムは IP パケットの解析とトラフィック量に応じた反力を提示する．試作システム動作画面を図 4 に示す．中心は試作システムを制御するパーソナルコンピュータを表す．中心から放射状に伸びる線はネットワークのイメージである．この線の付近に IP アドレスが表示されている．青い三角錐はポインタでありユーザはこれを自由に移動させる．図 4 では試作システムが自動的にパケットキャプチャを行っている．

ユーザのポインタが線に触れていて，かつ Omni のボタンが押下されたときユーザはトラフィック量を力として感じることができる．線の色は感情的意味を考慮し，温度のようにトラフィック量に応じて変化する．また，ホップ数が 30 以上のものを異常なパケットとして線を赤く表示させている．

提示する力は始め 1 分毎に変化するようにした．しかしながら実際に使用してみた結果更新が遅く，使用感が悪いと感じたため 10 秒毎に変化させるようにした．トラフィック量と線の色，フォースレベルとの関係は表 3 の通りである．この評価式は 5 日間トラフィック量を観測した

結果から求めている。

次の段階として図 5 に示すようにトラフィック量を日と時間の二次元平面上に表す。図中の色は表 3 と同じようにトラフィック量に応じて変化している。

表 3 評価式と色，フォースレベルの関係

評価式の値	色	フォースレベル
~10	青	0.0
11~20	薄い青	0.2
21~30	緑	0.4
31~40	黄	0.6
41~50	橙	0.8
50~	赤	1.0
hop 数 30~	赤	1.0

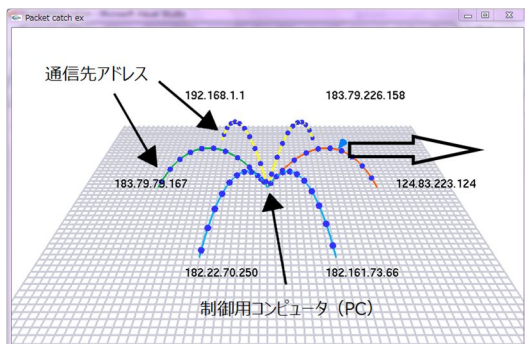


図 4 試作システム動作画面

ネットワークにおけるマルウェアの振る舞いに注目することでマルウェアを分類する方法を提案する。この振る舞いは反力としてユーザに提示されている。日と時間の二次元を利用するアルゴリズムに変更することで、直近のトラフィック量と比較することで異常な振る舞いを検出できる。

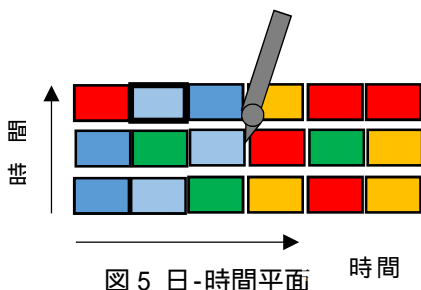


図 5 日-時間平面

4.3 試作システムの改良

4.3.1 改良とその問題点

提案した手法を実装したシステムの動作画面を図 6 に示す。中心が制御用コンピュータの位置を示す。各ブロックは一定時間のトラフィック量を表している。青い円錐はユーザが使用するポインタである。IP アドレスはブロックの終端付近に表示される。

改良したシステムの特徴として、一定時間のトラフィック量をまとめてブロック状にすることで、前後の時間と比較することが可能となった。更にこのブロックを日ごとに積むことで昨日の同じ時間、一昨日の同じ時間とも比較することが可能となる。

このようにして線からブロックへと力覚を提示する物体を変化させた。しかしブロックに触れた瞬間に力を提示すると、その力によってブロックから離れてしまい連続的に力を提示するにはユーザの鎌度が必要だった。そのためブロックの表面付近では提示する力を弱く、中心では大きくすることによってブロック表面で力を受けた際にブロックから離れさせる力を調整する。この変化部が最も利用しやすい割合を求める必要がある。

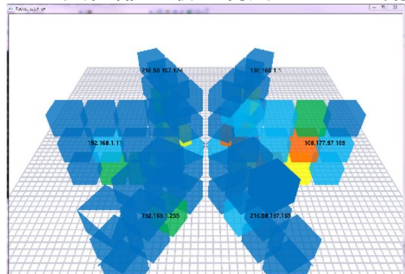


図 6 改良システム動作画面

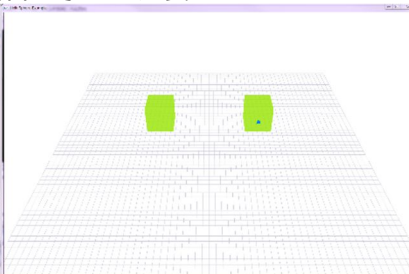


図 7 変化部測定プログラム実行画面

4.3.2 変化部の割合閾値測定

被験者に Omni のスタイラス部分を持たせ、仮想空間上にある二つのブロックに触れさせ変化部の割合を比較した。実験中のプログラム実行画面を図 7 に示す。片側のブロックには標準刺激、逆側には 4 種類の比較刺激と標準刺激の 5 種類からランダムなものが提示される。ブロック

の表面から提示する力が上限に達するまでの部分を変化部として、その割合を 1/4, 1/3, 1/2, 2/3, 3/4 としてそれぞれを比較する。1/2 を標準刺激としてそれ以外を比較刺激とする。図 8 にブロックと変化部の関係を示す。まず比較対象の違いが認識できているかを確認する。左右の変化具合を比較して、「左の方が変化が急」、「右の方が変化が急」の 2 つから選択させ二件法を用いて回答を得る。被験者は 10 代の男性 3 人で各 5 回施行した。

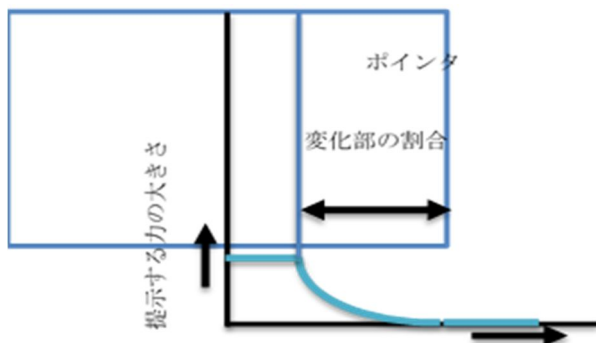


図 8 ブロックと変化部の関係

4.3.3 変化部の割合閾値測定結果

表 4 に測定結果を示す。表では回答数を記している。これを最尤法で処理したものを図 9 に示す。横軸は刺激の強さ、縦軸は正答確率を表す。4.2 節と同じように表における a は標準刺激を、 x_i は比較刺激を表している。

表 4 変化部の割合閾値測定結果

標準刺激 $a=1/2$		
比較刺激 x_i	$x_i > a$	$x_i < a$
1/4	3	12
1/3	0	15
1/2	5	10
2/3	12	3
3/4	12	3

標準刺激は 1/2 であり主観的等価点 (PSE) は 0.55 であった。これよりわずかに標準刺激と PSE の間に誤差があることが分かる。また、PSE と同等の刺激と判断される範囲は 0.41 から 0.69 であった。従ってこれらの値より差が大きければ同等の刺激でないと判断される。

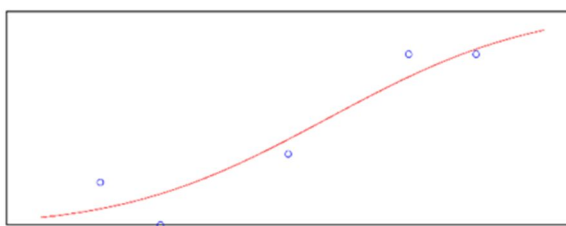


図 9 変化部の割合閾値解析結果

4.4 まとめ

本システムで通信量や悪質なパケットを、Omni を通して使用者に直感的に示すことができた。また改良したシステムでは、日時で通信を比較することで、人間の感覚を用いたホワイトリスト方式のフィルタリングソフトとして利用できるのではないかと考えている。これにより一般的なパソコン使用者がセキュリティ技術の必要性や重要性、信頼度などを知り、インターネットに対する自衛の方法を探る一助となることを期待する。

5. 主な発表論文等

〔雑誌論文〕 計3件（うち査読付論文 3件 / うち国際共著 0件 / うちオープンアクセス 0件）

1. 著者名 Manabu Ishihara, Taiki Kanayama	4. 巻 10916
2. 論文標題 Visualization of Network Security Data by Haptic.	5. 発行年 2018年
3. 雑誌名 Lecture Notes in Computer Science	6. 最初と最後の頁 1-10
掲載論文のDOI（デジタルオブジェクト識別子） https://doi.org/10.1007/978-3-319-91467-1_7	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 -

1. 著者名 Manabu Ishihara	4. 巻 ISSN: 2378-8143
2. 論文標題 How to reflect pen pressure with a haptic device	5. 発行年 2018年
3. 雑誌名 2018 IEEE 7th Global Conference on Consumer Electronics (GCCE)	6. 最初と最後の頁 1-2
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/GCCE.2018.8574767	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 -

1. 著者名 Manabu Ishihara	4. 巻 CFP20T07-ART
2. 論文標題 Modeling Sharpening a Pencil in Virtual Reality	5. 発行年 2020年
3. 雑誌名 Proceedings of 2020 IEEE 2nd Global Conference on Life Sciences and Technologies (LifeTech)	6. 最初と最後の頁 345-346
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 -

〔学会発表〕 計2件（うち招待講演 0件 / うち国際学会 0件）

1. 発表者名 石原学, 和氣哲郎
2. 発表標題 データ量を直感で感じるインタフェースの試作
3. 学会等名 電子情報通信学会大会講演論文集(CD-ROM) 2018 ROMBUNNO.A 13 2
4. 発表年 2018年

1. 発表者名 金山泰樹, 石原 学
2. 発表標題 力覚装置を使用したセキュリティデータの可視化
3. 学会等名 電子情報通信学会研究会HCGシンポジウム2017
4. 発表年 2017年

〔図書〕 計0件

〔産業財産権〕

〔その他〕

-

6. 研究組織

	氏名 (ローマ字氏名) (研究者番号)	所属研究機関・部局・職 (機関番号)	備考
--	---------------------------	-----------------------	----