Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.29, NO.1, Feb. 2019 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2019.29.1.215

DISC 성격 유형과 사이버 보안 위협간의 상호 연관성에 관한 연구 : 스피어피싱 공격 사례를 중심으로

김 묵 정,† 이 상 진‡
고려대학교 정보보호대학원

A Study on the Interrelationship between DISC Personality Types and Cyber Security Threats : Focusing on the Spear Phishing Attacks

Mookjung Kim,† Sangjin Lee‡
Graduate School of Information Security, Korea University

요 약

최근의 사이버 공격 위협 트렌드는 기업 또는 개인의 중요 정보 자산을 탈취하기 위해 기술적으로 광범위하게 해킹을 시도하는 방법과, 인간의 심리학적 요인을 겨냥한 사회공학(social engineering) 해킹 기법이 복합적으로 활용되는 '지능형 지속 위협 공격(APT)' 이 주를 이루고 있다. APT 공격 기법 중 가장 보편적으로 활용되는 스피어피싱(spear phishing)은 약 90% 이상이 APT공격의 핵심 요소로 활용되며, 쉬우면서도 강력한 효과를 내는 해킹 기법으로 잘 알려져 있다. 사이버 보안 위협 방어를 위한 기존 선행 연구는 주로 기술적, 정책적 측면에 국한하여 접근하고 있다. 그러나 지능화된 해킹 공격에 맞서 선제적으로 대응하기 위해서는 사회공학 측면에서 기존과는 다른 관점의 연구가 필요하다. 본 논문은 스피어피싱 공격 사례를 중심으로 인간의 성격 유형(DISC)과 사이버 보안 위협간의 상호 연관성을 분석하고, 기존의 틀을 깨는 새로운 관점의 보안 위협 대응 방안에 대해 제안하고자 한다.

ABSTRACT

The recent trend of cyber attack threat is mainly APT (Advanced Persistent Threat) attack. This attack is a combination of hacking techniques to try to steal important information assets of a corporation or individual, and social engineering hacking techniques aimed at human psychological factors. Spear phishing attacks, one of the most commonly used APT hacking techniques, are known to be easy to use and powerful hacking techniques, with more than 90% of the attacks being a key component of APT hacking attacks. The existing research for cyber security threat defense is mainly focused on the technical and policy aspects. However, in order to preemptively respond to intelligent hacking attacks, it is necessary to study different aspects from the viewpoint of social engineering. In this study, we analyze the correlation between human personality type (DISC) and cyber security threats, focusing on spear phishing attacks, and present countermeasures against security threats from a new perspective breaking existing frameworks.

Keywords: Social engineering, APT, DISC, Security awareness cognitive, Spear phishing hacking cognitive

I. 서 론

2016년에 임직원 만명이 넘는 국내 굴지의 대기업에서 이메일 사기로 인해 수백억원의 회사 자금을 잘못 송금하는 사건이 발생하였다. 같은 해 국내 유명 온라인 쇼핑몰에서 약 2,500여만건의 개인 정보

Received(11. 12. 2018), Modified(12. 28. 2018), Accepted(01. 07. 2019)

† 주저자, mookdoris@korea.ac.kr
‡ 교신저자, sangjin@korea.ac.kr(Corresponding author)

가 대규모로 유출되어 수십억원의 과징금이 부과된 사건도 있었다. 이 두 사건의 공통점은 소위 '스피어피싱(spear phishing)'으로 불리는 해킹 기법에 의해 금전적 손해, 기업 이미지 실추 등 큰 피해를 입었다는 사실이다.

스피어피싱은 열대지방 어부들이 물고기 사냥을 할 때 특정 물고기를 정한 후 작살로 고기를 낚는 방식에서 유래된 보안 용어로, 가장 쉬우면서도 효과적인 해킹 공격 기법 중 하나이다. 스팸 메일(spam mail)과는 다르게 특정 타겟을 정해놓고 이메일(e-mail)을 활용하여 지속적이고 치밀하게 공격하기 때문에, 메일 발신인이 정상 사용자인지 해커인지 여부를 판단해내기란 여간 어려운 일이 아니다. 물론 전문 보안 솔루션을 활용하여 스피어피싱 공격을 기술적으로 분석하고 대응해 낼 수는 있다. 하지만 다양하게 수집된 정보를 활용하여 마치 정상 사용자인 것처럼 위장한 후 공격하는 스피어피싱의 특성상 근본적인 해결책이 될 수는 없다.

본 논문에서는 인간의 성격 유형 특성을 활용하여 사이버 보안 위협과의 상호 연관성에 대해 분석해보고, 점차 고도화되어가는 사이버 보안 위협에 어떻게 대처해 나가야 하는지에 대한 새로운 접근법을 제시하고자 한다.

II. 관련 연구

2.1 스피어피싱(spear phishing) 공격

스피어피싱은 '조직 내 특정 개인이나 그룹을 대상으로하는 고도의 타겟팅된 피싱'이라고 정의할 수 있다[1].

특정 대상을 타겟팅하여 공격하는 기법 중 가장 많은 비중을 차지하는 공격 형태가 이메일을 활용한 스피어피싱으로 2017년 기준 약 71.4%를 차지하고 있다. 스피어피싱은 공격 대상자를 속여 악성 첨부파일을 열게 하거나 C2/유포지 등 악성 링크로 접속하게끔 유도하는데, 조직 내 보안이 가장 취약한 '사람'을 대상으로 공격하는 것이기 때문에 방어가 대단히 어렵다. 따라서 스피어피싱 공격에 대응하기 위해서는 전문 보안 솔루션과 함께 스피어피싱의 위험성에 대한 교육이 반드시 병행되어야 하다[2].

스피어피싱의 특징은 공격 대상으로 선택된 특정 개인이나 그룹을 대상으로 한다는 점이다. 즉, 공격자는 악의적인 첨부 파일이나 링크를 포함하는 이메일을 사용자에게 보내어 시스템의 가장 약한 부분을 공격한다[3].

스피어피싱 공격을 실행하는 것은 광범위한 스팸메일을 보내는 것보다 훨씬 비용이 많이 들지만 성공가능성이 높으며 잠재적인 피해 규모도 더 크다[4].

스피어피싱이 스팸 메일과 구별되는 점은 1) 불특정 다수가 아닌 특정 기관 또는 기업을 노린다는 점(표적성), 2) 기밀 정보 유출, 시스템 파괴 등 구체적인 목표를 위한 악성코드를 이용한다는 점(심각성), 3) 정상적인 파일로 보이거나 의심하기 어려울 정도로 실제 메일처럼 보이게 한다는 점(정교함) 등을 들 수 있다. 해커는 스피어피싱과 같은 타겟팅된 공격을 위해서 페이스북(facebook), 트위터(twitter)와 같은 SNS(Social Network Services)를 비롯해 다양한 경로로부터 공격 대상에 대한 정보를 수집한다. 가령 공격 대상이 자주 방문하는 웹사이트나 취미, 소속 조직 등의 정보가 이에 해당된다. 짧게는 몇 개월, 길게는 1년 이상 장시간에 걸쳐 공격 대상에 대한 거의 모든 정보를 수집한다. 수집된 정보를 이용하여 공격 대상의 관심과 호기심을 자극하는 스피어피싱 이메일을 발송한다면 공격은 더욱 막기 어려워진다[5].

2.2 DISC 성격 유형 검사

미국 컬럼비아대학교 심리학과 교수인 William Mouston Marston 박사는 1928년, 자신의 저서 '인간의 감정(The Emotion of Normal People)'에서 환경에 대한 인간의 인식을 바탕으로 인간 행동을 이론화 하였다. 인간의 행동을 개인이 처한 환경에 대하여 우호적으로 지각하는지의 여부와 자신이 처한 환경에서 얼마나 많은 힘을 가지고 있는지의 인식 여부를 기준으로, 인간의 행동 유형을 4가지로 모형화 하였다. 주도형(Dominance), 사교형(Influence), 안정형(Steadiness), 신중형(Conscientiousness)이 바로 인간의 행동 유형을 유형화한 모델이다. Marston교수의 이론을 바탕으로 1972년 미국의 미네소타 주립대학 심리학과 교수인 John Geier는 성격에 대한 연구 결과를 토대로 Marston교수의 모델을 변경하였다. Geier 박사 연구팀과 미국 최대 산업 심리 진단 및 산업 교육 전문기관인 Carlson Learning Company는 독특한 강제 선택방식의 자가 진단도구인 PPS (Personal Profile System)를 간행하였다. 이 진단 도구 안

Table 1. DISC Personality features

Division	Personality features
D (Dominance)	direct, results-oriented, firm strong-willed, forceful
I (Influence)	outgoing, enthusiasitc, optimistic, high-spirited, lively
S (Steadiness)	even-tempered, patient, humble, actful, accommodating
C (Conscientiousness)	analytical, reserved, precise, private, systematic

에는 그래프, 행동의 강도, 15가지 전형적인 행동 유형에 관한 설명을 포함하고 있다. 인터뷰를 통하여 보완된 행동 유형의 세부사항들은 별도의 전형적인 행동 유형 해설지에 수록되었다. 현재는 Carlson Learning사를 Inscape Publishing사에서 인수하여 PPS에 대한 지속적인 연구 및 버전을 보완하고 있다. 한국에서는 한국 교육 컨설팅 연구소가 독점 계약하여 한국어판 PPS를 보급하고 있으며[6] DISC 유형별 성격 특징은 Table 1.과 같다[7].

III. 성격 유형에 따른 보안 수준 설문 조사

본 연구에서는 성격 유형별 집단군과 보안 인식, 스피어피싱 해킹과의 상호 연관성에 대하여 분석하고자 한다. 이를 위해 직장인 표본 집단군 100명을 추출하여 성격 유형 검사(DISC), 보안 인식 지각 정도, 스피어피싱 해킹 지각 정도 등 총 3가지 변인을 설정하였다. 직장인 표본 집단군은 IT, 제조, 금융, 교육 등 각기 다른 조직에 분포된 표본을 대상으로 선정하여 설문 조사하였다.

Table 2. Variable setting

Division	Variables
Independent variables	Personality type * D(Dominance), I(Influence). S(Steadiness), C(Conscientiousness)
Dependent variables	Security Awareness(S.A) cognitive * Classification : Technical/Policy/Social
	Spear phishing Hacking(S.H) cognitive * Classification : Internet/Fee/HR/Tax/ Personal/Culture/Finance

"성격 유형과 보안 인식 지각 정도, 스피어피싱 해킹 지각 정도 간에는 어느 정도의 상호 연관성이 있는가?" 라는 가설을 설정하고, Table 2.와 같이 변인을 설정하였다.

보안 인식 지각 정도 실험은 기술 이해도 측정을 위한 기술 측면과 정보 보안 규정 및 지침과 관련한 정책 측면, 보안 실천 행동과 관련한 사회 측면 등 총 3가지 영역으로 설문 조사를 세분화함으로써 보다 구체적이고 실질적인 활용 방안을 제시하고자 한다. 또한 다음과 같은 가설을 수립하였다.

가설 1. 성격 유형(DISC)에 따라 보안 인식(S.A)의 지각 정도에는 차이가 있을 것이다.
가설 1-1. 보안 인식 지각 정도(기술)는 성격 유형 집단 간에 차이가 있을 것이다.
가설 1-2. 보안 인식 지각 정도(정책)는 성격 유형 집단 간에 차이가 있을 것이다.
가설 1-3. 보안 인식 지각 정도(사회)는 성격 유형 집단 간에 차이가 있을 것이다.
a.주도형(D)은 보안 인식 수준이 낮을 것이다.
b.사교형(I)은 보안 인식 수준이 낮을 것이다.
c.안정형(S)은 보안 인식 수준이 높을 것이다.
d.신중형(C)은 보안 인식 수준이 높을 것이다.

즉, 주도형(D)과 사교형(I)은 말이나 행동에서 속도가 빠르고 외향적인 성향을 가지는 공통점을 가지므로 보안 인식 수준에 있어서도 비슷한 결과를 보일 것이다. 또한 안정형(S)과 신중형(C)은 말이나 행동에서 속도가 느리고 내향적인 성향을 가지는 공통점을 가지므로 보안 인식 수준에 있어서도 비슷한 결과를 보일 것이다.

가설 2. 성격 유형(DISC)에 따라 스피어피싱 해킹(S.H) 지각 정도에는 차이가 있을 것이다.
a.주도형(D)은 스피어피싱 피해를 입을 것이다.
b.사교형(I)은 스피어피싱 피해를 입을 것이다.
c.안정형(S)은 스피어피싱 피해를 입지 않을것이다.
d.신중형(C)은 스피어피싱 피해를 입지 않을것이다.

위 가설 검증을 위해 아래와 같은 순서로 단계별 분석을 진행하였다.
[1단계] 성격 유형 검사
성격 유형 검사 설문지를 통해 피실험자를 대상으로 성격 유형을 파악한다.

〔2단계〕 보안 인식 지각 정도 실험

기술 측면, 정책 측면, 사회 측면 총 3개 요소별 보안 인식에 대한 지각 정도를 조사한다.

〔3단계〕 스피어피싱 해킹 지각 정도 실험

스피어피싱 이메일을 통해 인터넷, 연봉, 인사, 연말 정산, 개인, 문화, 금융 총 7개 영역별로 해킹에 대한 지각 정도를 조사한다.

〔4단계〕 통계 분석 및 결론 도출

실험 결과 데이터를 통해 성격 유형과 보안 인식 지각 정도, 스피어피싱 해킹 지각 정도 간에 어느 정도의 상호 연관성이 있는지 결론을 도출한다.

IV. 성격 유형에 따른 보안 수준 분석 결과

4.1 연구 표본 일반적 특성

연구 대상의 기초 통계 특성을 확인하기 위해 표본의 성별, 나이, 교육, 직급, 근속년수, 업종 등 일반적 특성에 대한 설문을 실시하였다.

Table 3. General characteristics of research subjects

Division		Number (N)	Ratio (%)
Gender	male	67	67
	female	33	33
Age	20s	31	31
	30s	43	43
	40s~	26	26
Education	high shool	4	4
	junior college	7	7
	university	81	81
	graduate school	8	8
Position	staff	26	26
	assistant manager	28	28
	manager	24	24
	senior manager~	22	22
Employment period	~1year	6	6
	1year ~ 3years	14	14
	3years ~ 5years	16	16
	5years~	64	64
Occupation	IT	58	58
	manufacturing	14	14
	finance	6	6
	education	8	8
	etc	14	14

4.2 성격 유형 검사 (DISC) 설문

본 설문에서는 미국 Carlson Learning Company가 개발하여 이미 신뢰도와 타당도가 공인된 DISC PPS 진단지를 곽유진[8]이 수정하여 사용한 진단 도구를 사용하였다[9].

Table 4.와 같이 주도형(D) 15%, 사교형(I) 24%, 안정형(S) 33%, 신중형(C) 28%의 통계 분석 결과를 보이고 있다.

Table 4. Personality type survey

Division	D	I	S	C	Sum
People (N)	15	24	33	28	100

4.3 보안 인식 지각 정도 설문지

보안 인식 지각 정도를 파악하기 위해 총 30개 문항의 설문을 조사하였다. 본 연구 설문지에 대한 타당도 검증을 위하여 탐색적 요인분석을 실시하였다. 모든 측정변수는 요인을 추출하기 위해 주성분분석을 사용하였고, 요인 적재치의 단순화를 위하여 직교회

Table 5. Security Awareness cognitive accuracy - factor analysis / reliability analysis

Division	Factor analysis				Reliability statistics	
	Social	Policy	Technical	Communnalities	Alpha if item deleted	Cronbach a
S.A#14	.951			.971	.981	
S.A#13	.943			.953	.983	
S.A#15	.936			.952	.983	0.987
S.A#12	.933			.956	.983	
S.A#19	.924			.923	.987	
S.A#22		.931		.894	.828	
S.A#30		.930		.911	.831	
S.A#28		.923		.884	.836	0.889
S.A#24		.647		.489	.911	
S.A#27		.599		.517	.904	
S.A#5			.906	.849	.707	
S.A#4			.897	.852	.704	0.811
S.A#6			.841	.727	.749	
S.A#7			.517	.494	.906	
Eigen-value	4.698	3.721	2.952			
% of Variance	33.555	26.577	21.089			

전방식(varimax)을 채택하였다. 본 연구에서의 문항 선택기준은 고유값은 1.0이상, 요인적재치는 0.40이상을 기준으로 하였다[10].

보안 인식 지각 정도는 3개의 하위요인으로 추출되었다. 추출된 요인은 기술 요인, 정책 요인, 사회 요인으로 명명하였다. 사회 요인 9개 문항 중 5개 문항(12,13,14,15,19), 정책 요인 10개 문항 중 5개 문항(22,24,27,28,30), 기술 요인 11개 문항 중 4개 문항(4,5,6,7)을 분석에 이용하였다. 총 30개 문항 중 16개 문항이 이론 구조에 맞지 않게 적재되어 제거하고, 최종적으로 14개 문항을 분석에 이용하였다.

보안 인식 지각 정도 설문지의 신뢰도는 3개의 하위요인별로 신뢰도 분석을 실시하였다. 크론바흐 알파(Cronbach α)값은 사회 요인은 0.987, 정책 요인은 0.889, 기술 요인은 0.811로 모두 높게 나타났다. 이를 통해 보안 인식 지각 정도 설문은 높은 신뢰도를 가지므로 본 실험에서 채택 가능하다[10].

4.4 스피어피싱 해킹 지각 정도 설문지

스피어피싱 해킹 지각 정도를 파악하기 위해 7개 문항의 설문을 조사하였다. 본 연구 설문지에 대한 타당도 검증을 위하여 탐색적 요인분석을 실시하였다. 모든 측정변수는 요인을 추출하기 위해 주성분분석을 사용하였고, 요인 적재치의 단순화를 위하여 직교회전방식(varimax)을 채택하였다.

스피어피싱 해킹 지각 정도는 7개 문항 중 총 6개 문항(2,3,4,5,6,7)을 분석에 이용하였다.

스피어피싱 해킹 지각 정도 설문지에 대한 신뢰도 분석 결과 크론바흐 알파값(Cronbach α)은 0.813으로 높게 나타났다. 이를 통해 스피어피싱 해킹 지각 정도 설문은 높은 신뢰도를 가지므로 본 실험에서 채택 가능하다[10].

Table 6. Spear phishing Hacking cognitive accuracy - factor analysis / reliability analysis

Division	Factor analysis		Reliability statistics	
	Spear plishing	Communalities	Alpha if item deleted	Cronbach a
S.H#4	.771	.594	.768	0.813
S.H#7	.739	.547	.781	
S.H#6	.725	.526	.784	
S.H#3	.711	.505	.785	
S.H#5	.700	.489	.790	
S.H#2	.676	.457	.794	
Eigen-value	3.118			
% of variance	51.975			

4.5 통계 분석 결과

분산 분석(ANOVA)을 통해 성격 유형(DISC)별 보안 인식 지각 정도와 스피어피싱 해킹 지각 정도에 대한 가설 검증을 실시하였다.

a.1 성격 유형에 따른 보안 인식 지각 정도 기술 요인 평균값(mean)을 보면, 주도형(D)/사교형(I)은 낮게, 안정형(S)/신중형(C)은 높게 나타났다.

b.1 성격 유형에 따른 보안 인식 지각 정도 정책 요인 평균값(mean)을 보면, 주도형(D)/사교형(I)은 낮게, 안정형(S)/신중형(C)은 높게 나타났다.

c.1 성격 유형에 따른 보안 인식 지각 정도 사회 요인 평균값(mean)을 보면, 주도형(D)/사교형(I)은 낮게, 안정형(S)/신중형(C)은 높게 나타났다.

d.1 성격 유형에 따른 스피어피싱 해킹 지각 정도 평균값(mean)을 보면, 주도형(D)/사교형(I)은 낮게, 안정형(S)/신중형(C)은 높게 나타났다.

따라서 성격 유형에 따라 보안 인식 지각 정도와 스피어피싱 해킹 지각 정도 간에는 차이가 있음을 알 수 있다. 즉 Fig.1.에서 보는바와 같이 주도형(D)/사교형(I)은 안정형(S)/신중형(C)에 비하여 보안인식 지각 정도와 스피어피싱 해킹 지각 정도 수준이 낮다는 것을 의미한다.

a.2/b.2/c.2/d.2 성격 유형에 따른 보안 인식 지각 정도 기술 요인(technical)/정책 요인(policy)/사회 요인(social), 스피어피싱 해킹 지각 정도 총 4가지 분석 결과의 유의확률(p-value)은 모두 0.000이다. 따라서 가설 1-1/1-2/1-3/2는 모두 채택되었다.

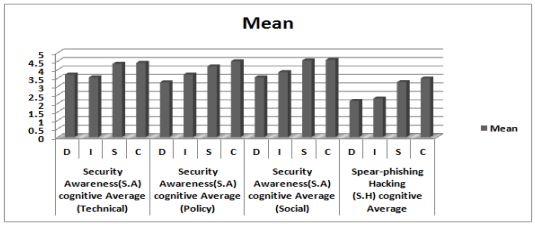

Fig. 1. Security Awareness based on the personality type

Table 7. Anova Result

Dependent variables	DISC	N	Mean		Std.Error	F-value	P-value	
a. Security Awareness(S.A) cognitive average (Technical)	D	15	a.1	**3.7000**	.53619	8.494	a.2	.000
	I	24		**3.5313**	.93342			
	S	33		**4.3333**	.53278			
	C	28		**4.3929**	.86984			
b. Security Awareness(S.A) cognitive average (Policy)	D	15	b.1	**3.2400**	1.16177	7.209	b.2	.000
	I	24		**3.7000**	.86678			
	S	33		**4.1758**	.98458			
	C	28		**4.4857**	.73722			
c. Security Awareness(S.A) cognitive average (Social)	D	15	c.1	**3.5333**	1.39318	10.192	c.2	.000
	I	24		**3.8417**	.64600			
	S	33		**4.5333**	.64356			
	C	28		**4.5714**	.38380			
d. Spear phishing Hacking (S.H) cognitive average	D	15	d.1	**2.1333**	.30342	56.023	d.2	.000
	I	24		**2.2847**	.45968			
	S	33		**3.2576**	.53860			
	C	28		**3.4702**	.29764			

좀 더 세부적인 결과 확인을 위해 다중 비교(multiple comparison)를 실시하였다. 성격 유형별로 보안 인식 지각 정도와 스피어피싱 해킹 지각 정도간에 어느 정도의 차이가 있는지에 대한 분석 결과는 Table 8.과 같다.

a3. 기술적(technical) 보안 인식 지각 정도에 있어서 성격 유형별로 어느 정도의 차이가 있는지 확인하였다. 분석 결과 주도형(D)-안정형(S), 주도형(D)-신중형(C), 사교형(I)-안정형(S), 사교형(I)-신중형(C) 간에 평균차(mean difference)가 큰 것으로 나타났다. 즉, 기술적 보안 인식 지각 정도 수준에 있어서 주도형(D)/사교형(I)은 안정형(S)/신중형(C)형에 비해 낮다는 것을 의미한다.

b3. 정책적(policy) 보안 인식 지각 정도에 있어서 성격 유형별로 어느 정도의 차이가 있는지 확인하였다. 분석 결과 주도형(D)-안정형(S), 주도형(D)-신중형(C), 사교형(I)-신중형(C)간에 평균차(mean difference)가 큰 것으로 나타났다. 즉, 정책적 보안인식 지각 정도 수준에 있어서 주도형(D)은 안정형(S)/신중형(C)에 비해 낮고, 사교형(I)은 신중형(C)에 비해 낮다는 것을 의미한다.

c3. 사회적(Social) 보안 인식 지각 정도에 있어서 성격 유형별로 어느 정도의 차이가 있는지 확인하였다. 분석 결과 사교형(I)-안정형(S), 사교형(I)-신중형(C)간에 평균차(mean difference)가 큰 것으로 나타났다. 즉, 사회적 보안 인식 지각 정도 수준에 있어서 사교형(I)은 안정형(S)/신중형(C)에 비해 낮다는 것을 의미한다.

d3. 스피어피싱 해킹 지각 정도에 있어서 성격 유형별로 어느 정도의 차이가 있는지 확인하였다. 분석 결과 주도형(D)-안정형(S), 주도형(D)-신중형(C), 사교형(I)-안정형(S), 사교형(I)-신중형(C)간에 평균차(mean difference)가 큰 것으로 나타났다. 즉, 스피어피싱 해킹 지각 정도 수준에 있어서 주도형(D)/사교형(I)은 안정형(S)/신중형(C)형에 비해 낮다는 것을 의미한다.

Table 8. Multiple comparison result

Dependent variables		(I) DISC	(J) DISC	Mean Difference(I-J)	P-value
a3. Security Awareness (S.A) cognitive average (Technical)	Dunnett T3	D	I	.16875	.977
			S	**-.63333**	**.004**
			C	**-.69286**	**.015**
		I	D	-.16875	.977
			S	**-.80208**	**.004**
			C	**-.86161**	**.008**
		S	**D**	**.63333**	**.004**
			I	**.80208**	**.004**
			C	-.05952	1.000
		C	**D**	**.69286**	**.015**
			I	**.86161**	**.008**
			S	.05952	1.000
b3. Security Awareness (S.A) cognitive	Scheffe	D	I	-.46000	.517
			S	**-.93576**	**.018**
			C	**-1.24571**	**.001**
		I	D	.46000	.517
			S	-.47576	.303

Dependent variables		(I) DISC	(J) DISC	Mean Difference(I-J)	P-value
average (Policy)			**C**	**-.78571**	**.030**
			D	**.93576**	**.018**
		S	I	.47576	.303
			C	-.30996	.637
			D	**1.24571**	**.001**
		C	**I**	**.78571**	**.030**
			S	.30996	.637
c3. Security Awareness (S.A) cognitive average (Social)	Dunnett T3		I	-.30833	.957
		D	S	-1.00000	.091
			C	-1.03810	.068
			D	.30833	.957
		I	**S**	**-.69167**	**.001**
			C	**-.72976**	**.000**
			D	1.00000	.091
		S	**I**	**.69167**	**.001**
			C	-.03810	1.000
			D	1.03810	.068
		C	**I**	**.72976**	**.000**
			S	.03810	1.000
d3. Spear phishing Hacking (S.H) cognitive average	Dunnett T3		I	-.15139	.765
		D	**S**	**-1.12424**	**.000**
			C	**-1.33690**	**.000**
			D	.15139	.765
		I	**S**	**-.97285**	**.000**
			C	**-1.18552**	**.000**
			D	**1.12424**	**.000**
		S	**I**	**.97285**	**.000**
			C	-.21266	.291
			D	**1.33690**	**.000**
		C	**I**	**1.18552**	**.000**
			S	.21266	.291

4.6 타당성 검증

위 분석 결과에 대한 타당성 검증을 위해 설문 대상자 중 간부급 관리자와 비관리자에 대한 통계 분석을 실시하였다.

Table 9.와 같이 간부급 관리자(administrator)를 분석한 결과, 안정형(S)/신중형(C) 집단 비율(약75%)이 주도형(D)/사교형(I) 집단 비율(약25%)에 비하여 높게 나타났다. 비관리자 중 안정형(S)/신중형(C) 집단 비율은 약 58% 이다. 간부급 관리자 중 안정형(S)/신중형(C) 집단 비율은 비관리자 안정형(S)/신중형(C) 집단 비율보다 약 17% 높은 것으로 나타났다.

즉, 간부급 관리자의 성격 유형이 안정형(S)/신중형(C) 집단에 속할 가능성이 높음을 분석 결과를 통해 확인할 수 있다.

Table 9. Validation of the person in charge

Division		D	I	S	C	Sum
Administrator	people	1	3	5	7	16
	%	6.3	18.8	**31.3**	**43.8**	100
Not administrator	people	14	21	28	21	84
	%	16.7	25.0	33.3	25.0	100

4.7 활용 방안

분석 결과로 도출된 바와 같이 성격 유형(DISC)에 따라 보안 인식 지각 정도, 스피어피싱 해킹 지각 정도에는 차이가 존재한다. 본 연구 결과를 통하여 아래와 같은 분야에 활용할 수 있다.

첫째, 기술적 측면에서 성격 유형별로 보다 강력한 보안 기술 적용이 가능하다. 해킹 공격에 취약한 성격 유형군(group)에 대해서는 좀 더 정밀하고 세밀하게 보안 기술을 적용할 수 있다. 예를 들어 방화벽을 통한 시스템 접근 제어시 주도형(D)/사교형(I) 집단은 안정형(S)/신중형(C) 집단에 비해 보다 강력한 방화벽 규칙(ruleset)을 적용함으로써 보안 위협을 감소시킬 수 있다.

둘째, 정책적 측면에서 기존의 획일적인 교육 시스템에서 벗어나 성격 유형별로 특화된 보안 교육 프로그램을 실시함으로써 투입되는 시간과 노력을 감소시킬 수 있다. 예를 들어, 연간 2회 보안 교육을 실시하는 기업의 경우 주도형(D)/사교형(I) 집단은 동일 수준으로 유지, 안정형(S)/신중형(C) 집단은 연간 1회로 교육 횟수를 조정함으로써 효과적으로 교육 시스템을 운영할 수 있다.

셋째, 사회적 측면에서 기업 내 직무 배치 시 본 연구 결과를 참고 자료로써 활용 가능하다. 예를 들어 보안 사고가 발생할 경우 영향도가 비교적 큰 주요 부서(연구소, 재무/회계, 인사, 보안) 또는 앞서 타당성 검증을 통해 확인한 관리자 발령 등 인사 제도 운영에 있어 그 효용 가치가 클 것으로 보인다.

V. 결 론

사이버 보안 위협 및 사고 발생의 원인은 결국 공격자(attacker)와 피해자(victim), 즉 인간이다.

이 점에 착안하여 설문을 활용한 통계 분석을 통해 심리학에서 말하는 성격 유형(DISC)과 사이버 보안 위협간에는 밀접한 상호 연관성이 있음을 확인하였다.

보안 강화를 위해 기존 선행 연구에서 다루고 있는 접근 방법에서 더 나아가, 사회공학 측면에서 새로운 접근법이 필요하다는 점에서 시사하는 바가 크다. 성격 유형과 보안 위협간 연관성을 바탕으로 기업내 인사 시스템을 구체적으로 프로세스(process)화한다면 좀 더 가시적인 효과를 기대할 수 있을 것이다. 즉, 신규 인력 채용 시 성격 유형 검사를 실시하고 해당 데이터를 참고 자료로 활용한다면 보다 실질적이고 구체적인 보안 강화 활동을 수행할 수 있다.

성격 유형별로 보안 기술을 차등 적용하고 특화된 보안 교육을 실시하며, 주요 직무 배치 시 인사 정보로 활용하는 등 다양한 방면에서 적용 가능하다. 본 연구 결과를 통해 보안 위협에 대한 새로운 접근 방향을 제시함으로써 사이버 보안 위협 대응에 큰 도움이 될 것으로 기대한다.

References

[1] TrendLabsSM APT Research Team, "Spear-phishing email: Most favored APT attack bait," Trend Micro, Sep. 2012

[2] Gillian Cleary, "ISTR (Internet Security Threat Report)," volume 23, Symantec, March. 2018

[3] Aron Laszka, Yevgeniy Vorobeychik, and Xenofon Koutsoukos, "Optimal personalized filtering against spear-phishing attacks," Twenty-Ninth AAAI Conference on Artificial Intelligence, pp. 958-964, Jan. 2015

[4] Mengchen Zhao, Bo An, and Christopher Kiekintveld, "Optimizing personalized email filtering thresholds to mitigate sequential spear phishing attacks," Thirtieth AAAI Conference on Artificial Intelligence, pp. 658-664, Feb. 2016

[5] Kwon chi-jung, "Target attack, starting at the end of the spear phishing window," AhnLab, Jan. 2014

[6] Oh Dong-seop, "Relationship between DiSC behavior types and organizational effectiveness," MA, Korea University, Jan. 2009

[7] Alex Bradley, "Workplace profile DiSC profile," John Wiley & Sons, Feb. 2016

[8] Kwak Yu-jin, "The effects of supervisor-subordinate DiSC behavioral tendencies on subordinates's organizational commitment and job satisfaction," MA, Sookmyung Women's University, Dec. 2011

[9] Kim Do-yeon, "A study on job satisfaction depending on salesman's DiSC behavior types," MA, Hanyang University, Feb. 2016

[10] Song Ji-joon, Statistical analysis method for spss/amos, 21cbook, Jun. 2017

〈저자소개〉

김 묵 정 (Mookjung Kim) 정회원
2010년 2월: 경희대학교 전자정보대학 전자공학과 졸업
2014년 3월~현재: 고려대학교 정보보호대학원 정보보호학과 석사과정
2010년 2월~현재: 삼성SDS 보안사업담당 보안서비스팀 시니어 엔지니어
〈관심분야〉 디지털 포렌식, 네트워크 보안, Threat Intelligence

이 상 진 (Sangjin Lee) 종신회원
1989년 10월~1999년 2월: ETRI 선임 연구원
1999년 3월~2001년 8월: 고려대학교 자연과학대학 조교수
2001년 9월~현재: 고려대학교 정보보호대학원 교수
2008년 3월~현재: 고려대학교 디지털포렌식연구센터 센터장
2017년 3월~현재: 고려대학교 정보보호대학원 원장
〈관심분야〉 디지털 포렌식, 심층암호, 해쉬 함수