Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.28, NO.4, Aug. 2018 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2018.28.4.951

게임을 통한 정보보안인식 향상에 관한 연구: 개별 정보보안정책에 대한 인식변화를 중심으로

최 종 현†‡
고려대학교 정보보호대학원

A Study on Improvement of Information Security awareness through Game: Focusing on Changes in Awareness of Information Security Policies

Jong-hyun Choi†‡
Graduate School of Information Security, Korea University

요 약

조직의 정보보안을 강화하기 위해서는 정보보안설비에 대한 투자도 중요하지만 조직구성원들의 정보보안인식 역시 매우 중요하다. 이러한 정보보안인식을 높이기 위해서는 효과적인 교육이 필요하다. 하지만 대부분의 조직에서 활용하는 집체교육방식은 그다지 효과적이지 못하다. 기능성 게임을 이용한 교육 방식은 이에 대해 좋은 대안이 될 수 있다. 기능성 게임을 이용한 교육 방식은 이미 다양한 사례 및 연구를 통해 효과성이 입증되었고 많은 분야에서 활용되고 있다. 본 논문에서는 개별 정보보안정책 중요도에 대한 조직원들의 인식을 향상시키기 위하여 게임 프로그램을 설계 및 구현하였다. 조직원들을 대상으로 교육을 수행하였으며 교육 전 후 평가 데이터 분석을 통해 개별 정보보안정책 중요도에 대한 인식 변화 여부를 조사하였다.

ABSTRACT

In order to strengthen the information security of the organization, it is important to invest in the information security facility, but the information security awareness of the organization members is also very important. Effective education is needed to raise awareness of this information security. However, the method of collective education utilized by most organizations is not very effective. Educational methods using serious games can be a good alternative. Educational methods using serious games have already proved effective through various cases and researches and are used in many fields. In this paper, we design and implement a game program to improve the awareness of individual information security policy importance. The training was conducted for the members of the organization and the change of awareness about the importance of individual information security policy was examined through analysis of evaluation data before and after the training.

Keywords: Serious Game, Information security Awareness, Security Learning, Teaching Tool, Security policy

I. 서 론

해킹, 바이러스 등 사이버 공격이 발생하여 심각한 피해를 야기함에 따라 기업들은 앞 다투어 정보보안을 강화하고자 정보보안설비에 대한 투자를 늘렸다. 2017년 기준 정보보호 예산을 편성한 기업은 48.1%로 전년 대비 15.6% 증가하였고, IT예산 중 정보보호예산을 5% 이상 편성한 기업은 2.2%로 전

Received(05. 30. 2018), Modified(1st: 06. 28. 2018, 2nd: 07. 16. 2018), Accepted(07. 16. 2018)

† 주저자. rvd3737@naver.com
‡ 교신저자. rvd3737@naver.com(Corresponding author)

년대비 1.1% 증가하였다[1]. 하지만 정보보안을 강화하기 위해선 기술적으로 많은 투자 뿐 아니라 직원들이 정보보안에 대해 중요성을 인식하는 것이 무엇보다도 중요하다[2].

정보보안인식 강화를 위해서 공기업 및 공공기관들은 년1회 이상 정보보안교육을 의무적으로 수행한다. 하지만 교육방식 자체가 내·외부 강사를 초청해 임직원을 한자리에 모아놓고 하는 집체교육이 대부분이고, 교육 내용도 너무 딱딱한 절차에 관련된 설명이기 때문에 오히려 직원들에게 정보보안교육이 쓸모없다는 반감만을 주는 경우가 많았다[3]. 이는 기업 내부의 환경과 직원들의 선호를 반영한 다양한 교육방식에 대한 고찰이 부족하기 때문에 발생하는 현상으로 교육효과가 미비할 수 밖에 없다[4].

기능성 게임(serious game)을 통한 교육 방식은 대안이 될 수 있다. 기능성 게임이란 재미보단 특정한 내용을 교육시킬 목적으로 만들어 진 게임이며, 게임 요소 인 글, 그림, 비디오, 소리, 음악 등 다양한 요소들을 활용할 수 있다는 장점이 있다[5][6]. 선행 연구를 보면 비디오게임을 활용하여 청소년 당뇨병환자들이 인슐린 주사를 제 때에 투입할 수 있도록 환자들을 행동을 유발시킨 사례도 있었다[7]. 또한 대학에서 자동차 동작 원리를 학습하기 위해 시뮬레이션 게임을 통해 학생들을 교육하였고 그 결과 긍정적인 효과가 있다는 연구도 있다[8]. 이 밖에 기능성 게임을 통한 교육이 효과적이라는 주장을 입증하는 선행연구는 각 분야별로 쉽게 찾아 볼 수 있다. 하지만 게임을 통한 정보보안인식 교육에 관련된 연구는 부족한 실정이다.

본 논문에서는 정보보안 분야 중 개별 정보보안정책 중요도에 대한 조직원들의 인식 향상을 위하여 기능성 게임을 설계 및 구현하였다. 구현된 게임에 기능성 게임 요소가 어떤 식으로 반영되었는지 SGDA(Serious Game Design Assessment) 프레임워크를 통해 분석하였다. 그리고 정보보안인식 제고 프로그램으로 적합한지 여부를 따지기 위해 전문가 인터뷰를 수행하였다. 또한 A 공공기관 조직원들을 대상으로 시범적으로 교육을 실시하고 교육 전, 후 설문조사를 통해 개별 정보보안정책의 중요도에 대한 조직원들의 인식에 변화 여부를 조사하였다.

이 논문의 구성은 다음과 같다. 2장에서 정보보호인식, 기능성게임을 통한 교육에 관련된 이론적 배경에 대해 살펴보고. 3장에서는 정보보안인식 교육 게임 설계 및 구현에 대해 기술한다. 4장에서는 개발된 게임을 전문가의 평가를 수행하여 정보보안인식 프로그램으로써 적합성 여부를 알아본다. 5장에서는 교육 수행을 통한 조직원들의 개별 정보보안 정책에 대한 중요도 인식 변화에 대해 조사한다. 마지막 6장에서는 결론 및 마무리한다.

II. 이론적 배경

2.1 정보보안인식

2.1.1 정보보안인식 정의

정보보안인식 정의에 대해 선행연구를 살펴보면 먼저 Bilal Khan 등[9]은 모든 구성원이 정보보안의 중요성 및 적정성 등 활동에 대한 책임에 대해 이해하는 것이라고 하였다. Staton 등[10]은 정보시스템 내의 정보유출과 관련하여 위험인식 및 그에 따라 행동하는 것이라고 하였다. Carrie 등[11]은 정보보안인식을 정보보안에 대해 중요성을 인식해서 알고 있는 것이라고 보았다. 이 논문에서는 Carrie 등[11]의 정의를 기반으로 정보보안인식 이란 조직 구성원들이 정보보안활동의 중요성 및 필요성에 대해 인지하는 것이라고 정의하겠다.

2.1.2 정보보안인식 중요성

정보보안 분야에서 조직의 구성원들이 사실상 가장 중요한 부분이다. 많은 정책결정자들이 가장 중요하게 여기는 부분은 사실 기술이 아닌 사람 부분이다[12]. 만약 기업들이 보안기술에 많은 비용을 사용한다 할지라도 정작 직원들의 정보보안의식이 결여되어 있으면 아무 소용이 없다[13]. 왜냐하면 보안시스템을 구축하여 사이버공격의 위험을 낮춘다고 한들 정작 이를 지켜야하는 직원들이 정보보안의 중요성을 인식하지 못한다면 그만큼 위험성은 가중될 수 있기 때문이다. 정보보안행동에 대해 개인이 자연스럽게 받아들이고 당연하게 여기는 단계가 되었을 때 비로소 실질적인 정보보안성 강화를 달성할 수 있다[14]. 그러므로 각종 교육 및 정보보안활동을 통해 직원들에게 정보보호절차에 대해 이유 및 배경 등을 이해시키고 그들의 태도를 변화시켜야 한다[14].

2.2 게임을 통한 교육

2.2.1 기능성 게임(serious game)

기능성 게임은 사회학자인 클라크 압트[5]가 그의 저서 기능성게임(serious game)에서 처음으로 언급하였으며 그는 기능성 게임을 사용자에게 놀이와 즐거움이 주 목적이 아닌 교육이 목적인 게임으로 정의하였다. 이는 일반 게임이 재미요소에 목적을 둔다면 기능성 게임은 게임적 요소를 충분히 활용하여 사람들에게 특정한 내용을 교육시킬 목적으로 주로 교육적 효과, 치료효과, 훈련효과 등을 갖는 게임을 말한다[16][17].

2.2.2 기능성 게임 디자인 평가 프레임워크

기능성 게임을 설계 및 구현함에 있어서 필요한 요소를 설명하기 위해 Konstantin 등[18]은 선행연구에서 기능성 게임 디자인 평가 프레임워크인 SGDA(Serious Game Design Assessment) 프레임워크를 제안하였다. SGDA 프레임워크는 그림 1과 같고 각 요소에 대해 요약하여 설명하면 다음과 같다.

- 목적(purpose) : 기능성 게임의 경우 플레이어에게 어떠한 영향을 줄 것인지에 대한 분명한 의도와 목적이 있어야 한다. 게임의 목적은 게임시스템 전체의 역동성과 일관성을 형성 하는 원동력이 된다.
- 컨텐츠(content/information) : 게임 내에서 플레이어에게 제공되는 정보는 사용자가 쉽게 접할 수 있어야 한다.
- 프레이밍(framing) : 플레이어 그룹에 대한 선정, 그리고 그들이 게임을 원활히 수행할 수 있는지 여부를 고려해야 한다.

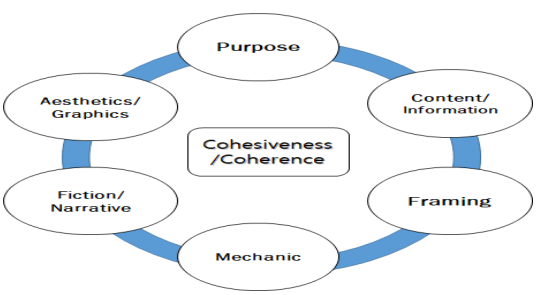

Fig. 1. SGDA Framework

- 게임기법(mechanic) : 게임기법은 플레이어와 게임 간 상호작용 할 수 있도록 만드는 방식으로 볼 수 있으며, 게임 내 규칙, 게임 내 목표, 보상, 장애물, 난이도, 승리조건 등이 이에 포함된다.
- 픽션(fiction/narrative) : 게임에 이야기적 측면이 필요하다. 이를 위해 창작된 시나리오, 스토리, 배경 등은 게임 목적과 관련 있어야 한다.
- 심미성(aesthetics/graphic): 게임 개발에 있어서 게임요소를 시청각적으로 표현하는 컴퓨터그래픽, 예술매체, 미적특징, 소리 등이 포함된다.
- 일관성(cohesiveness/coherence) : 각각의 게임요소가 게임의 목적과 잘 연관되어 있는지 고려되어야 한다.

2.2.3 교육효과 메타분석

게임을 통한 교육에 관련 논문들을 메타 분석한 선행연구를 찾을 수 있었다. 랜들 등[19]은 게임을 통한 교육적 효과에 대해 연구한 68건의 논문을 분석하여 시뮬레이션과 전통적인 수업이 학생들의 실력 향상에 미치는 영향을 비교했다. 그 결과 56%는 게임과 전통 수업방식 사이에 차이를 보이지 않았고 32%는 게임을 선호했으며 5%는 전통 수업방식을 선호하였다. 보켈 등[20]은 교육 효과 관련 논문 32건을 분석하여 전통적인 수업방식 보다 상호작용 시뮬레이션이나 게임을 활용하면 학생들의 인지력이 높아졌다는 결과를 도출해 내었다. 시츠만 등[21]은 논문분석을 통해 시뮬레이션 게임을 활용할 때 학생들의 자신감이 20% 높아졌고 서술적 지식습득도 11% 높아졌고 절차적 지식 및 기억력도 전통적인 학습방식을 택한 학생들보다 게임화 교육을 통한 학생들이 뛰어나다는 결과를 도출하였다.

2.2.4 기능성 게임 사례

교육 사례를 살펴보면 S.J. BROWN 등[7]은 당뇨병에 걸린 아이들을 대상으로 정해진 시간에 인슐린을 주입해야 한다는 교육적 목적으로 게임을 개발하였고 게임을 수행한 그룹이 하지 않은 그룹보다 인슐린 미 주입에 의한 응급상황이 발생한 횟수가 적다는 결론을 도출했다.

이동혁 등[22]은 정보보호 에듀 게임을 만들어 초등학생들에게 정보보안개념을 쉽게 이해시키고 보안전문가 직업이 어떤 일을 하는지에 대해 간접적으로

체험할 수 있는 기회를 제공하였다.

글로벌 IT회사인 SAP는 로드워리어(roadwarrior)를 개발하여 영업사원들이 근무 중 발생할 수 있는 문제에 대해 비디오 및 객관식 질문을 사용하여 학습할 수 있게 하였고 그 결과 집체교육 방식보다 교육에 지출되는 비용을 현저히 낮추면서 높은 교육효과를 달성할 수 있었다[23].

III. 게임 설계 및 구현

3.1 게임 목표

조직원들이 부정적으로 인식하는 정보보안정책의 개념과 중요성에 대해 알기 쉽게 설명하고 이를 통해 개별 정보보안정책의 중요성에 대한 인식 제고를 목표로 한다. 정보보안부서 직원과의 인터뷰를 통해 직원들이 불신하는 보안정책으로 망분리, OTP(OneTimePad), 보안USB관리 정책을 선정하였다. 인터뷰에 따르면 보안정책을 반대하는 민원을 노동조합을 통해 제기하거나 관련 부서에 직접 항의 하는 등 부정적인 입장을 내비쳤다고 한다. 하지만 정작 보안정책의 중요성에 대해서는 적절히 인식하지 못하기 경우가 많았다. 그러므로 게임 플레이를 통해 개별 정보보안정책(망분리, OTP, 보안USB관리) 중요도에 대한 인식 향상을 목표로 한다.

3.2 게임시나리오

평소 정보보안정책에 매우 부정적인 인식을 가지고 있는 최대리는 보안 정책 예외 적용 여부를 두고 정보보안팀에 격렬히 항의하다 쓰러진다. 이 후 정신을 차려보니 사이버보안 월드로 차원 이동하게 되었고 이곳에서 보안용사가 되어 해킹맨과 싸운다.

3.3 게임 흐름 및 방식

3.3.1 게임 흐름

전반적인 게임 흐름은 그림 2와 같다. 게임 시작 시 메뉴화면이 나타나고 스타트 버튼을 누르면 프롤로그로 넘어간다. 프롤로그에서는 보안정책 예외 정책 적용 문제로 정보보안팀과 싸운 최대리가 사이버 보안세계로 워프하게 되고 이 곳에서 해킹맨의 공격을 막는다는 다짐을 하게 된다. 이 후 각각의 스테이지 별로 망분리, OTP, 보안USB 정책을 주제로 한 대화, 퀴즈, 그리고 정보보안개념을 활용한 슈팅게임을 진행하게 된다.

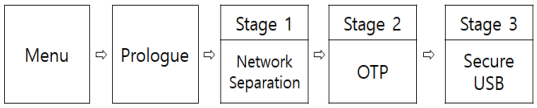

Fig. 2. Game Flow

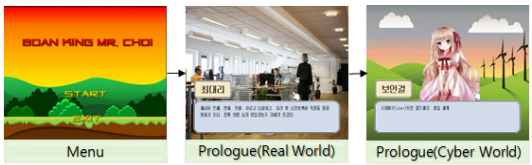

Fig. 3. Game Scenes 1

게임에 대한 이해를 돕기 위해 그림3(메뉴, 프롤로그 장면)을 첨부하였다.

3.3.2 스테이지 설명

스테이지는 총 3 스테이지로 구성되어 있고 각각의 흐름은 그림 4와 같다.

- 대화(dialogue) : 등장인물 간 스테이지 주제를 중심으로 대화를 담당하는 파트로써 사용자들에게 정보보안 정책의 도입 이유 및 중요도에 대해 설명한다.
- 문답(question) : 각각의 주제에 대한 개념을 질의하는 파트로 3가지 선택지가 주어지고 사용자는 마우스 클릭을 통해 답을 선택하게 된다. 만약 사

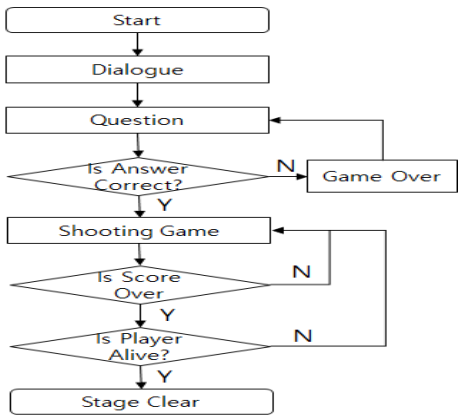

Fig. 4. Stage Flow

용자가 알맞은 정답을 고르지 않으면 게임오버 상태로 넘어가게 되고 다시 문답을 반복하게 된다.

• 슈팅게임(shooting game) : 사용자는 비행기를 조종하여 30초간 생존해야 하며 각 스테이지 목표 점수를 넘어야 미션클리어 된다. 적기를 알맞은 무기를 선택하여 공격하여야 파괴되고 점수를 올릴 수 있다. 게임에 대한 이해를 돕고자 그림 5에 대화, 게임오버, 문답 장면을 첨부하였다. 슈팅게임에 대한 상세한 설명은 다음 장에서 기술한다.

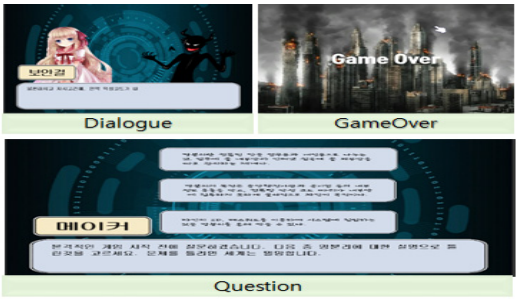

Fig. 5. Game Scenes 2

3.3.3 슈팅 게임

슈팅게임의 화면은 그림 6와 같이 구성된다.

① 목표점수 : 미션클리어를 위한 목표 점수, 스테이지에 따라 목표점수가 다르게 구성된다.

② 현재점수 : 현재 유저가 얻은 점수로 적기 한기를 없앨 때마다 100 점씩 얻는다.

③ 적 : 화면 위에서 아래로 내려오는 방식으로 한번에 5기씩 내려온다. 적은 3종류, 악성코드, 패스워드공격, 데이터무단반출이다. 알맞은 무기 또는 플레이어 기체와 충돌하면 파괴 된다.

④ 무기가이드 : 적기를 파괴하기 위해선 알맞은 무기를 선택하여 공격해야 한다.

- 망 : 망분리로 악성코드 적을 파괴 할 수 있다.
- 오 : OTP로 패스워드노출위험 적을 파괴 할 수 있다.
- U : 보안USB로 데이터무단반출 적을 파괴할 수 있다.

⑤ 조작 : 플레이어는 키보드 좌우키를 사용하여 기체를 움직일 수 있고, 무기의 경우 자동으로 발사되고 스페이스 바를 누르면 무기 변경이 가능하다.

⑥ 무기 : 발사된 무기의 경우 ④와 같이 무기이미지(망,O,U)가 플레이어 기체로 부터 일정시간 주기로 자동으로 생성된다. 그리고 생성된 위치 기준으로 화면 아래에서 위로 직선 이동한다. 적기와 충돌 시 적기는 파괴되고 한 기당 점수 100점을 얻는다.

⑦ 남은 시간 : 스테이지별 제한시간은 30초이고 남은 시간을 표현한다.

⑧ 플레이어 : 플레이어 기체의 경우 적기와 충돌하면 격추되므로 30초간 격추되지 않아야 한다.

⑨ 현재 무기 : 어떤 무기를 사용하는지 표현한다.

Fig. 6. Shooting Game Scene

적을 한기씩 격추 할 때 마다 100점씩 스코어를 얻을 수 있다. 30초간 스테이지별 목표점수를 넘기고 기체가 생존한다면 미션을 클리어 할 수 있다. 적과 충돌하여 격추 당하거나 30초간 목표점수를 얻지 못할 경우 게임 오버 되고 이 경우 다시하기가 가능하다. 그림 7과 같이 슈팅게임의 결과 장면을 구성하였다.

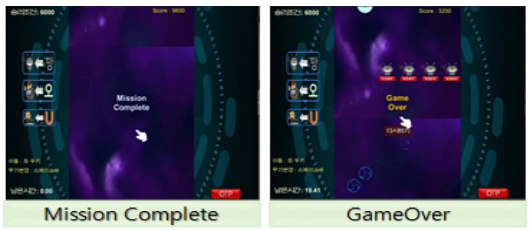

Fig. 7. Result Scenes

3.4 개발환경

표 1에서 보는 것과 같이 게임개발은 일반적인 보급형 PC에서 이루어졌다. 복잡하지 않은 구조이기 때문에 충분히 구현 가능했다.

Table 1. Development Environment

H W	CPU	Intel Pentium(R)2117U @1.8Ghz
	RAM	12GB
S W	O/S	Windows 10 64bit
	Tool	Unity
	Language	C#

3.5 기능성 게임 요소 분석

기능성 게임 필수적인 요소가 어떤 식으로 반영되어 있는지 설명하기 위해 2장에서 언급한 SGDA 프레임워크를 이용해서 분석하였다.

- 목적(purpose) : 게임을 통해 플레이어가 각각의 정보보안정책(망분리,OTP,보안USB) 중요도 인식을 향상 시킨다.
- 컨텐츠(content/information) : 캐릭터 간 대화를 통해 각각의 정보보안정책 중요성에 관련된 내용을 전달하고 있기 때문에 플레이어는 자연스럽게 정책에 대한 정보를 접할 수 있다. 슈팅게임 진행 시 남은 시간, 조작법, 현재 스코어, 클리어 조건, 무기선택방식 등 게임 진행에 필요한 정보를 게임 화면에서 쉽게 접할 수 있다.
- 프레이밍(framing) : 게임을 플레이할 목표 그룹은 A 공공기관 20~30대 직원들을 대상으로 하였다. 비교적 젊은 세대이기 때문에 게임에 대한 거부감 적다고 여겨진다. 게임 조작은 스페이스바(무기변경), 좌우커서(이동), 정답선택(마우스 우클릭)로 간단하게 구성하였다.
- 게임기법(mechanic) :
  - 게임 목표와 규칙 : 각각의 스테이지를 클리어 하기 위해선 정보보안정책 관련된 퀴즈를 맞춰야하고, 슈팅게임 시 개별 승리조건을 달성해야 한다. 슈팅게임의 경우 좌우로 움직이는 기체를 조종하여 알맞은 무기로 악성코드를 파괴하면 점수를 얻을 수 있다. 또한 정해진 시간 내에 플레이어는 죽지 않고 목표점수 이상을 달성해야 한다.
  - 보상 : 각각의 스테이지를 클리어 할 수록 선택할 수 있는 무기가 하나씩 늘어난다.
  - 난이도 : 난이도 측면에서 퀴즈 파트는 각 정보보안정책에 대한 개념 질문과 답변으로 구성되어 있기 때문에 3개의 스테이지 모두 동일한 난이도로 볼 수 있다. 반면 슈팅게임의 경우는 남은 시간이 줄어들수록 적기체가 내려오는 속도가 빨라진다는 점, 스테이지가 올라갈수록 적들의 종류가 증가해서 무기를 변경해가며 플레이를 해야 한다는 점에서 난이도에 변화를 주었다.
- 픽션(fiction/narrative) : 사이버 월드로 워프한 주인공이 해킹맨 침공으로부터 지키는 이야기이다. 프롤로그 부분에서 보안팀직원과 정보보안정책 예외 적용 여부를 놓고 싸우는 모습을 표현함으로써 조직원들이 공감할 수 있도록 만들었다. 캐릭터 간 대화를 통해 개별 정보보안정책들이 왜 중요한지, 지키지 않을 시 본인에게 어떠한 피해가 발생할 수 있는지 설명한다.
- 심미적 요소(aesthetics/graphic) : 청각요소를 가미하기 위하여 효과음 및 배경음악을 삽입하였다. 화면 구성은 그림3, 그림6과 같이 되어있다. 심미성을 살리기 위해 고화질 이미지 배포사이트인 픽사베이(www.pixabay.com)에서 제공한 고화질 이미지를 활용하여 배경을 구성하였으며 유니티 상점에서 개발자 평가 점수가 높은 패키지를 선정하여 캐릭터 이미지로 활용하였다.
- 일관성(cohesiveness/coherence) : 게임의 목적에 관련된 정보보호를 주제로 이야기를 구성하였고 정보보안 개념정보를 쉽게 전달하기 위해 캐릭터 간 자연스런 대화를 활용했다. 또한 게임의 몰입을 위하여 심미적요소와 게임기법을 활용하였으며 단순한 조작을 통해 게임을 쉽게 즐길 수 있도록 제작하였다.

IV. 전문가 평가

4.1 평가목적 및 방식

구현된 게임이 정보보안인식제고 프로그램으로써 적합한지 평가하기 위하여 전문가 평가를 수행하였다. 전문가 집단은 표2와 같이 IT 및 정보보안 분야에서 경력이 최소 10년 이상인 사람들로 구성 되었다. 전문가들에게 미리 작성한 설문을 나눠주고 게임 시현 후 설문 항목을 중심으로 인터뷰를 진행하는 방식으로 평가를 진행하였다.

Table 2. Expert List

	Org	pos	care -er	Field
A	Univ	professor	10 years	Information Security Policy
B	Company	General Manager	20 years	Information Security, IT
C	Company	Manager	10 years	IT, Information Security education
D	Company	Manager	10 years	Information Security, IT

선행 연구에서 임채호[26]는 효율적인 정보보안인식 제고 프로그램에 필요한 7가지 요인에 대해 분석하였고 본 연구에서는 이를 참고하여 표 3과 같이 설문을 구성하였다

Table 3. Expert Question

	Elements	Question
1	Attention	Do you think it can attract the attention of the subjects?
2	Appeal	Do you think it can appeal to the audience?
3	Memorable	Was the conceptual description easy to remember?
4	Not Coercion	Is not it coercive?
5	Current	Is this what organization needs today?
6	Credible	Is the content reliable?
7	Continuing	Can it be done continuously?

4.2 평가 결과

전문가 의견을 종합하여 정리하면 다음과 같다.

- 주목하게(attention) : 게임을 통한 교육방식이 새롭다는 점, 대상에게 흥미를 줄 수 있는 게임요소를 활용했다는 점이 조직원들의 주목을 끌 수 있을 것 같다.
- 호소성(appeal) : 정보보안이 지켜지지 않을 시 본인이 어떠한 피해를 당할 수 있는지에 대해 캐릭터 간 대화를 통해 쉽게 설명하고 있다는 점에서 메시지를 잘 전달할 수 있을 것으로 판단된다.
- 기억하기 쉽도록(memorable) : 캐릭터 간 친근한 대화를 통해 보안정책에 대해 필요성에 대해 설명하는 점, 퀴즈를 통해 개념을 복습할 수 있다는 점, 정보보안 개념을 활용한 슈팅게임을 통해 반복적으로 학습할 수 있다는 점이 기억하기에 도움이 될 수 있다고 판단된다.
- 강압적이지 않게(not coercion) : 교육자체에 강압적인 부분은 없다고 판단된다.
- 현재의(current) : 최근 보안부서 직원과의 인터뷰를 통해 조직원들이 중요하다고 인식해야 하는 정보보안정책을 선별하여 주제로 정했다는 점에서 현재 실질적으로 필요한 주제를 선정하였다고 판단된다.
- 신뢰할 수 있는(credible) : 게임에서 전달하는 개념에 대한 오류가 없다고 판단된다.
- 지속적인(continuing): 언제든지 컴퓨터 환경에서 플레이 가능하다는 점, 게임자체가 단순하여 커스터마이징이 쉽다는 점에서 주제를 변경하여 활용할 수 있다는 점 등 지속적으로 활용가능하다고 판단된다.

V. 시범 수행 및 평가

5.1 목적 및 방식

구현된 게임이 실제 정보보안정책(망분리, OTP, 보안USB)에 대한 조직원들의 인식에 어떠한 영향을 미쳤는지 알아보기 위해 A 공기업 조직원 25명을 대상으로 교육을 시범 수행하였다. 조사대상은 표 4와 같이 구성되어 있다. 개별 정보보안정책(망분리, OTP, 보안USB) 별 중요도 인식 정도를 측정하기 위해서 동일한 설문을 게임 전, 후에 수행하였다.

Table 4. Person list

	Field	Num
1	Human Resource	5
2	Construct	3
3	Accounting	4
4	Budget	4
5	Legal	4
6	Labor	5
Sum		25

5.2 설문구성

본 설문은 백민정 등[25]이 회사원 150명을 대상으로 정보보안인식을 측정하기 위하여 활용했던 선행연구의 설문을 본 논문 주제에 맞게 수정하여 표 5와 같이 구성하였다. 설문 항목은 각각 중요성, 준수여부, 필요성, 개념이해로 구성되었다. 선행 연구의 경우 조직원들의 일반적인 정보보안에 대한 인식 정도를 측정하였지만 본 논문에서는 일반적인 정보보안 인식이 아닌 특정 정보보안정책(망분리, OTP, 보안USB)에 대한 인식 변화를 조사하는 것이 목적이기 때문에 측정대상을 망분리, OTP, 보안USB로 수정하여 설문을 구성하였다. 각 문항에 대한 답변은 리커트(Likert)척도를 활용하였으며 1.전혀 아니다. 2.아니다. 3. 보통이다. 4.그렇다. 5.매우 그렇다 로 구성 되어 있다.

Table 5. Question List

		Question	Cron alpha
Network Seperation	N1	Do you think the network separation policy is important?	0.814
	N2	Do you think you should keep your network separation policy?	
	N3	Do you think you need a network seperation policy?	
	N4	Are you familiar with the concept of network separation?	
OTP	O1	Do you think OTP policy is important?	0.908
	O2	Do you think you should keep OTP policy?	
	O3	Do you think you need an OTP policy?	
	O4	Are you familiar with OTP concept?	
Secure USB	U1	Do you think a secure USB policy is important?	0.922
	U2	Do you think you should obey the security USB policy?	
	U3	Do you think you need a secure USB policy?	
	U4	Are you familiar with the security USB concept?	

5.3 결과 분석

5.3.1 문항별 분석

각각의 설문조사 문항을 기준으로 평균값을 계산하였다. 이 값을 바탕으로 대응표준 T검증 방식을 활용하여 문항별 인식 변화 정도를 관찰했다. 측정결과는 표6과 그림8과 같다.

망분리의 경우 그림 8과 같이 교육 수행 전 후 측정된 값의 차이가 크지 않았다. 또한 문항별 p값이 (N1=0.294 N2=1, N3 = 0.405 N4 = 0.77) 0.05보다 크기 때문에 조직원들의 인식이 향상되었다고 할 수 없다. OTP의 경우 O1(3 → 3.92) O2(3.08 → 4.12) O3(3.08 → 4.28), O4(3.2 → 4.36)로 문항별 평균점수가 높아졌다. 보안USB의 경우도 마찬가지로 U1(2.52 → 4.12),

Table 6. Result of Evaluation 1

Policy	Q	Pre	Post	Diff	P
Network Seperation	N1	2.8	2.64	-0.16	0.294
	N2	2.72	2.72	0	1
	N3	2.8	2.96	0.16	0.405
	N4	2.88	2.92	0.04	0.77
OTP	O1	3	3.92	0.92	0
	O2	3.08	4.12	1.04	0
	O3	3.08	4.28	1.2	0
	O4	3.2	4.36	1.16	0
Secure USB	U1	2.52	4.12	1.6	0
	U2	2.76	4.08	1.32	0
	U3	2.56	4	1.44	0
	U4	2.88	4.2	1.32	0

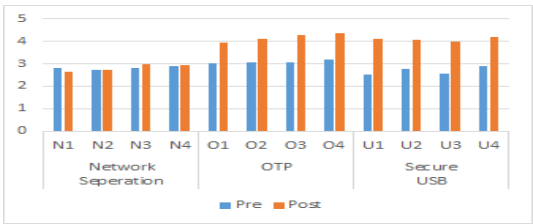

Fig. 8. Result Graph 1

U2(2.76 → 4.58), U3(2.56 → 4), U4(2.88 → 4.2)로 문항별 평균점수가 높아졌다. OTP와 보안USB의 경우 p값에 대해서도 0.05보다 작기 때문에 보안정책에 대한 중요도 인식이 향상되었다고 판단할 수 있다.

5.3.2 정책별 분석

각각의 정보보안정책(망분리,OTP,보안USB)에 대한 4 질의항목에 응답 값을 개개인 별 전체 평균값을 계산하였다. 개개인 별 평균값을 바탕으로 대응표본 T검정방식을 활용하여 게임 전 후에 정보보호 정책에 대한 조직원들의 인식 변화를 확인해보았다.

결과는 표 7, 그림 9와 같다. OTP정책(3.09→ 4.17)과 보안USB정책(2.68→ 4.1) 중요도에 대한 인식은 높아졌다. 하지만 망분리 정책의 경우 값의 유의성을 판단하는 p값이 0.93으로(>0.05) 중요도 인식이 향상되었다고 볼 수 없다. 원인을 파악하기 위해 교육에 참가한 직원 중 5명을 선정하여 개별 인터뷰를 진행하였다. 인터뷰 내용을 요약하면 다음과 같다.

- 망분리 정책은 OTP정책 및 보안 USB정책과 달리 하루에 사용되는 빈도수가 훨씬 많기 때문에 체감 상 직원들이 받는 스트레스가 크다.
- 망분리 정책의 필요성, 중요성에 대해서는 이성적으로 받아들일 수 있지만 너무 시스템 자체가 불편해서 감정적으로 도저히 동의할 수 없다.
- 교육으로 인식을 바꾸기 보단 망분리 정책 및 시스템을 사용자 가용성을 고려하여 수정하는 것이 필요하다.

Table 7. Result of Evaluation 2

Policy		Ave	Stdev	Dif	T	P
Network Seperation	pre	2.8	0.43	0.01	-0.8	0.93
	post	2.81	0.54			
OTP	pre	3.09	0.82	1.08	-6.2	0
	post	4.17	0.36			
Secure USB	pre	2.68	0.37	1.42	-12.5	0
	post	4.1	0.41			

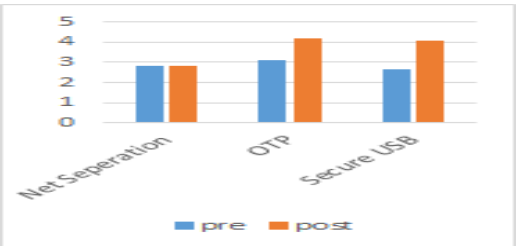

Fig. 9. Result Graph 2

개별 인터뷰를 통해 망분리 정책의 경우 유독 사용량이 많고 불편하다는 점 때문에 조직원들의 반감이 컸음을 알 수 있었다. 또한 1회 게임 수행을 통해 조직원들의 인식 변화를 발생시키기에는 역부족이라고 판단된다.

정보보안 인식 교육의 경우 인식변화를 발생시키기 위해서는 지속적으로 수행하는 것이 중요하다[24]. 그러나 본 연구에서는 한번 밖에 수행하지 않았다. 따라서 향후 지속적인 활동이 필요하다고 볼 수 있다. 정보보안 강화를 위하여 정보보안정책을 만들 때 반드시 조직원들과의 충분한 소통을 통해 의견을 반영하는 것이 중요한데 이는 실질적으로 정책을 지켜야 하는 조직원들 입장에서는 부담이 될 수 있기 때문이다[26]. 조직원들의 의견이 반영되지 않은 경우 즉 권위적인 접근방식으로 정책을 만들고 일방적으로 적용한 경우 조직원들은 보안정책을 업무상 부담만 가중시키는 현명하지 않은 것이라고 치부하고 그 결과 정보보안 정책에 대한 반감만 높아지게 되고 중요도에 대한 인식은 낮아질 수밖에 없다. 따라서 조직원들의 의견을 반영하여 정책 및 시스템 수정이 필요할 것이라고 판단된다.

VI. 결론 및 한계

기업의 정보보안을 강화하기 위해서는 정보보안 설비투자 뿐 아니라 직원들의 정보보안인식도 높아져야 한다. 이를 위해 회사나 조직에서는 정보보안인식 교육을 실시하지만 획일적인 집체교육 방식으로는 그 효과를 기대하기 어려웠다. 기능성 게임은 이에 대한 대안이 될 수 있으며 효과성은 각종 연구 자료나 사례를 통해 접할 수 있다. 본 연구에서는 개별 정보보안정책 중요도에 대한 인식 향상을 목표로 기능성 게임을 설계 및 구현하였다. 구현된 게임에 기능성 게임요소가 어떤 식으로 반영되었는지 SGDA 프레임워크를 통해 분석하였고 정보보안인식 제고 프로그

램 적합성 여부를 판단하기 위해서 전문가평가(4명)를 진행하였다. 그리고 A 공기업 직원 25명을 대상으로 개별 정보보안정책(망분리,OTP,보안USB)에 대한 인식에 변화를 조사하기 위해 시범 교육을 수행하였다.

교육 수행 전 후 설문 조사 데이터 분석 결과 3가지 보안정책 주제 중 2가지 정책(OTP,보안USB)에서 게임을 통해 중요도 인식이 향상됨을 보였다. 하지만 실제 수행한 인원(25명)이 적기 때문에 양적인 측면에서 정확한 측정이 이루어졌다고는 보기 어렵다. 또한 본 연구는 3가지 정보보안정책 중요도에 대한 인식 향상을 목표로 하기 때문에 이를 개개인의 일반적인 정보보안 인식 변화로 보기 어렵다. 그리고 인식교육의 경우 지속적으로 수행함을 원칙으로 하는데 1회 수행한 점은 지속성 측면에서 부족함을 보인다. 그러나 기능성 게임을 통해 정보보안정책에 대한 인식교육을 수행했다는 점, 수행 후 두 보안정책에 대해 조직원들의 중요도 인식 향상이 있었다는 점에서는 의의가 있다고 여겨진다.

향후, 다양한 정보보안정책 및 활동을 주제로 게임을 확장하여 구성하고자 한다. 그리고 많은 조직원들에게 지속적인 교육을 통해 지속성면에서의 부족한 점을 보충하고자한다. 또한 기존에 진행 중인 집체교육이나 이러닝 등 비교를 통해 게임을 통한 교육의 효과성을 분석하는 연구를 수행하겠다.

References

[1] Ministry of Science and ICT, "Results of the survey on the status of information security in 2017", http://www.msit.go.kr/web/msipContents/contentsView.do?cateId=mssw311&artId=1372723, 2018.05.20

[2] Amitava Dutta and Kevin Mccrohan "Management's role in information security in a cyber economy," California Management Review, vol. 45, no. 1, pp. 67-87, Oct. 2002.

[3] Boannews, "Is not it a good time to s pend your company's security training time?", http://www.boannews.com/media/view.asp?idx=50323, 2018.05.22

[4] Karina Korpela, "Improving cyber security awareness and training programs with data analytics," Information Security Journal: A Global Perspective, vol. 24, no. 1-3, pp. 72-77, Jun. 2015.

[5] Clark C. Abt, Serious Games, Viking Press, NewYork, pp. 5-6, 1970.

[6] Jesse Schell, The art of game design, ELSEVIER, Oxford, pp. 96, 2008.

[7] S.J. Brown, D.A. Lieberman, B.A. Gemeny, Y.C. Fan, D.M. Wilson and D.J. Pasta "Educational video games for juvenile diabetes: result of a controlled trial," Medical informatics, vol. 22, no. 1, pp. 77-89, Jan. 1997.

[8] B.D. Coller and D.J. Shernoff, "Video game-based education in mechanical engineering: a look at student engagement," International Journal of Engineering Education, vol. 25, no. 2, pp. 308-317, Jan. 2009.

[9] [9] Bilal Khan, Khaled S. Alghathbar, Syed Irfan Nabi and Muhammad Khurram Khan, "Effectiveness of information security awareness method based on psychological theories," African Journal of Business Management, vol. 5, no. 26, pp. 10862-10868, Oct. 2011.

[10] Jeffrey M. Stanton, Kathryn R. Stam, Paul Mastrangelo and Jefferey Jolton, "An analysis of end user security behaviors," Computers and Security, vol. 24, no. 2, pp. 124-133. Mar. 2005.

[11] Carrie Mccoy and Rebecca T.F., "You are the key to security: establishing a successful security awareness program," SIGUCCS '04 Proceedings of the 32nd annual ACM SIGUCCS conference on User service, pp. 346-349, Oct. 2004.

[12] Mete Eminagaoglu, Erdem Ucar and Saban Eren, "The positive outcomes of information security awareness train-

ing in company - a case study," Information Security Technical Report, vol. 14, no. 4, pp. 223-229, Nov. 2010.
[13] Basie Von Solms, "Information security - a multidimensional discipline," computers & security, vol. 20, no. 6, pp. 504-508, Sep. 2001.
[14] P.S. Dowland, S.M. Furnell, H.M. Illingworth and P.L. Leynolds, "Computer crime and abuse: a survey of public attitudes and awareness," Computers and Security, vol. 18, no. 8, pp. 715-726, 1999.
[15] Chang-gyu Oh and Jong-gi Kim, "Development of a framework for effective information protection education and training," Korea Institute Of Information Security And Cryptology, 13(2), pp. 59-69, April. 2003.
[16] Karl M. Kapp, The gamification of learning and instruction: game-based methods and education, Wiley, Newjersey, pp. 49, 2012.
[17] Kil-sang Yoo, In-woo Kim, Je-hyuk Youn, Dong-jae Lee and Won-hyung Lee "A design of functional game contents and analysis of power spectrum," Journal of The Korean Society for Computer Game, 4(6), pp. 25-31, Jun. 2005.
[18] Konstantin Mitgutsch and Narda Alvarado, "Purposeful by design?:a serious game design assessment framework," FDG '12 Proceedings of the International Conference on the Foundations of Digital Games, pp. 121-128, Jun. 2012.
[19] Randel J.M., Morris B.A., Wetzel C.D. and Whitehill B.V., "The effectiveness of games for educational purposes: a review of recent research," Simulation & Gaming, vol. 23, no. 3, pp. 261-276, Sep. 1992.
[20] D.S. Vogel, J. Cannon Bouwes, C.A. Bowers, K. Muse and M. Wright, "Computer gaming and interative simulations for learning: a meta-analysis," Journal of Educational Computing Research, vol. 34, no. 4, pp. 229-243, April. 2006.
[21] Sitzmann. T, "A meta-analytic examination of the instructional effectiveness of computerbased simulation games," Personnel Psychology, vol. 64, no. 2, pp. 489- 528, May. 2011.
[22] Dong-hyeok Lee and Nam-je Park, "Teaching book and tools of elementary network security learning using gamification mechanism," Journal of the Korea Institute of Information Security & Cryptology, 26(3), pp 787-797, Jun. 2016.
[23] Gamified UK, "Gamification Examples and Case Studies", https://www.gamified.uk/2013/07/29/gamification-in-the-wild-examples-and-case-studies/, 2018.04.05.
[24] Chae-ho Lim, "Effective information protection awareness improvement plan," Journal of Information Security, 16(2), pp 30-36, April. 2006.
[25] Min-jung Baek and Seyung-hee Son, "A study on the effect of Information security awareness and behavior on the information security performance in small and medium sized organization," Asia Pacific Journal of Small Business, 33(2), pp. 113-132, Jun. 2011.
[26] Anne Adams and Martina Angela Sasse, "Users are not the enemy," COMMUNICATIONS OF THE ACM, vol. 42, no. 12, pp. 40-46, Dec. 1999.

〈저자소개〉

최 종 현 (Jong-hyun Choi) 정회원
2013년 2월: 고려대학교 컴퓨터통신공학부 졸업
2017년 3월~현재: 고려대학교 정보보호학과 석사과정
〈관심분야〉 정보보호, 정보보안인식, 정보보안교육