글로벌 ICT 표준 컨퍼런스 2022

Global ICT Standards Conference 2022

2022. 11.9.(수)~11.(금)
서울 양재 엘타워 오르체홀(5F)

ICT 표준특허 성공사례 발표

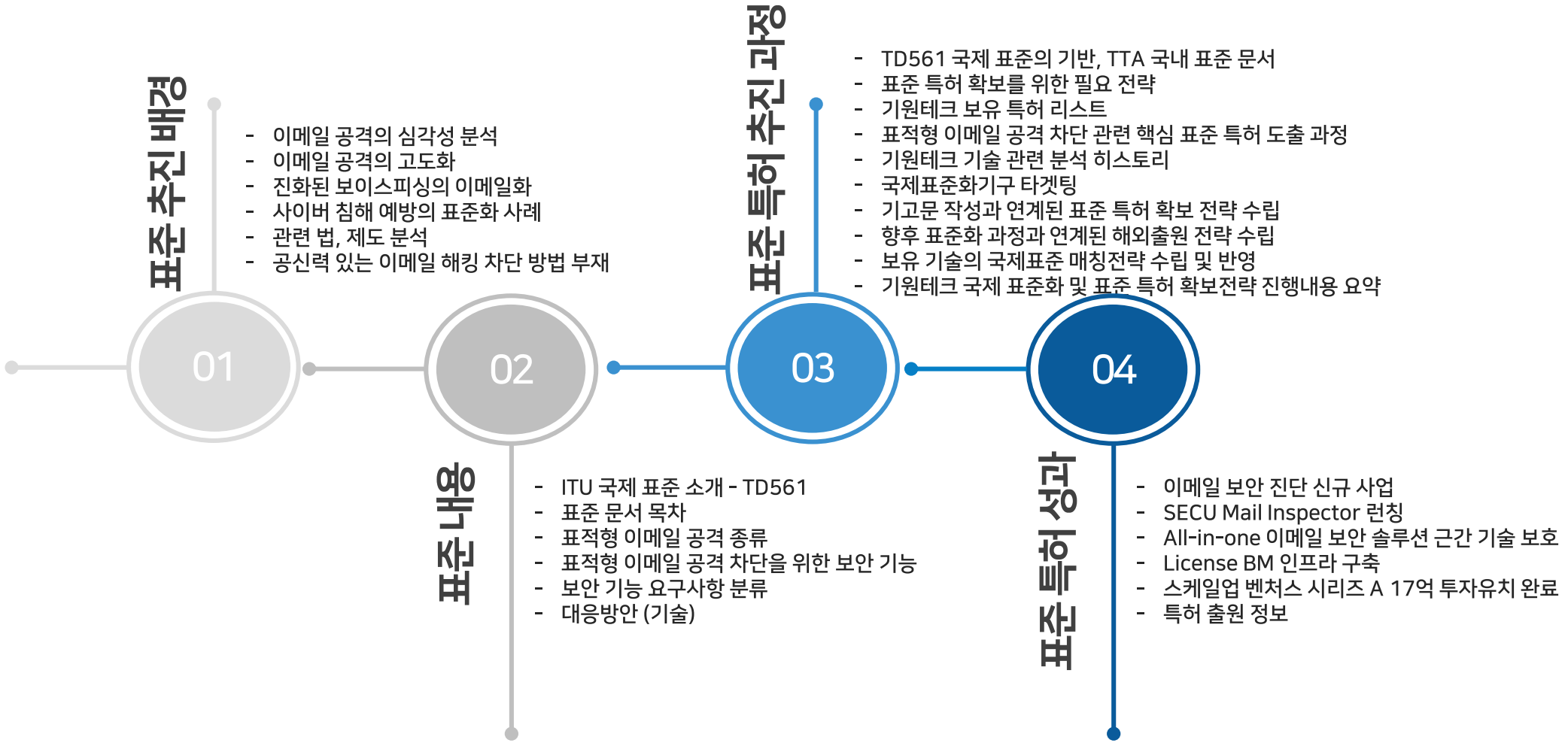
우수기술 보유기관 지원사례

이메일 보안 기술

김충한 팀장 ㈜기원테크

INDEX

목차


01
표준 추진 배경
- 이메일 공격의 심각성 분석
- 이메일 공격의 고도화
- 진화된 보이스피싱의 이메일화
- 사이버 침해 예방의 표준화 사례
- 관련 법, 제도 분석
- 공신력 있는 이메일 해킹 차단 방법 부재
02
표준 내용
- ITU 국제 표준 소개 - TD561
- 표준 문서 목차
- 표적형 이메일 공격 종류
- 표적형 이메일 공격 차단을 위한 보안 기능
- 보안 기능 요구사항 분류
- 대응방안 (기술)
03
표준 특허 추진 과정
- TD561 국제 표준의 기반, TTA 국내 표준 문서
- 표준 특허 확보를 위한 필요 전략
- 기원테크 보유 특허 리스트
- 표적형 이메일 공격 차단 관련 핵심 표준 특허 도출 과정
- 기원테크 기술 관련 분석 히스토리
- 국제표준화기구 타겟팅
- 기고문 작성과 연계된 표준 특허 확보 전략 수립
- 향후 표준화 과정과 연계된 해외출원 전략 수립
- 보유 기술의 국제표준 매칭전략 수립 및 반영
- 기원테크 국제 표준화 및 표준 특허 확보전략 진행내용 요약
04
표준 특허 성과
- 이메일 보안 진단 신규 사업
- SECU Mail Inspector 런칭
- All-in-one 이메일 보안 솔루션 근간 기술 보호
- License BM 인프라 구축
- 스케일업 벤처스 시리즈 A 17억 투자유치 완료
- 특허 출원 정보

표준 추진 배경

ICT Standards

- 이메일 공격의 심각성 분석
- 이메일 공격의 고도화
- 진화된 보이스 피싱의 이메일 화
- 사이버 침해 예방의 표준화 사례
- 관련 법, 제도 분석
- 공신력 있는 이메일 해킹 차단 방법 부재

이메일 공격의 심각성 분석

이메일을 이용한 예측할 수 없는 사이버 범죄 증가

해킹

"이 계좌로 송금하세요"…
이메일 해킹 무역사기 '또' 2020. 08. 24 뉴스1

피싱

"**피싱 URL**만 3만개 이상"…
코로나19 악성메일 공격 2020. 04. 14 뉴스핌

스팸

해외에서 온 **스팸메일** 큰 폭 늘었다
…대부분 중국발 2020. 03. 25 이뉴스투데이

악성코드

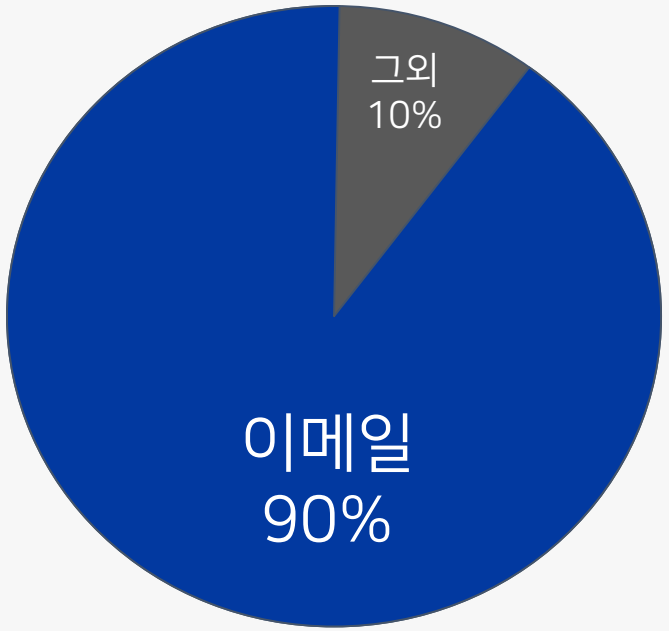
견적·구매 문의에다 대북관련 질의서까지… 요즘
메일은 **악성코드** '지뢰밭' 2021. 04. 12 보안뉴스

91%
사이버 공격 이메일에서 시작
출처 : KISA

90%
사이버 해킹과 데이터 유출 이메일에서 발생
출처 : Miimecast

89%
사이버 인프라 위협 이메일에서 탐지
출처 : Trendmicro

사이버 공격 수단 유형 비율



이메일 공격의 고도화

표적형 공격으로 고도화되고 있는 이메일 공격

신종 악성코드 공격

상반기 **표적형 랜섬웨어** 기승… 사이버공격 더욱 교묘해졌다

"업무 메일을 위장한 **정보유출형 악성코드** 유포" 2021. 07. 18 MoneyS

사회공학적 공격

국내 **기업·기관 타깃** '송장·인보이스' 악성메일 유포

"**송장을 사칭**한 이메일의 **헤더를 수정**해…" 2019. 02. 19 보안뉴스

이번엔 DHL 인보이스? **계정 탈취용** 악성 메일 또 유포

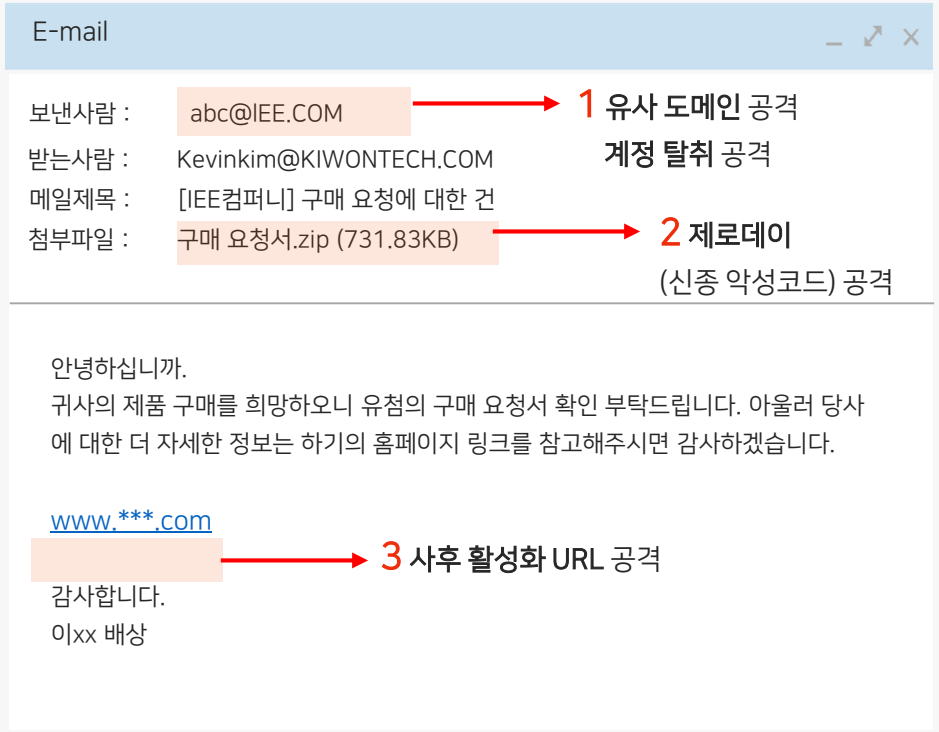
"html 파일을 클릭할 경우 받는 사람의 **메일 주소**를 기재하고, 해당 메일의 **패스워드 입력을 요구**…" 2021. 03. 16 보안뉴스

86%
표적형이메일 공격 비중
출처 : Fireeye

97%
표적형 이메일 공격에 취약한 사용자 비중
출처 : Proofpoint

표적형 공격 이메일이란?

기존 불특정 다수를 향한 공격이 아닌 **개인이나 기업을 표적**으로 설정한 뒤 **특정 인물을 공격**하는 **지능적 이메일**



진화된 보이스 피싱의 이메일 화

악성코드 삽입 없이
사용자 사칭하여 정상 메일로 위장

유사 Email 계정 생성

알파벳 추가 , 삭제, 정렬, 글자변환, 서버변경

xxx@kiwon.com
▼
xxx@kion.com

표적 대상을 선정 후
맞춤형 이메일 공격 수행

사용자의
다양한 행동 유도

사이버 침해 예방의 표준화 사례

광범위하게 활용되는 표준화 기구 TTA & ITU, **국내·국제에서 영향력** 발휘

'사이버 위협 대응' ICT 표준화 현황

TTA

MTD 기술과 관련해서 능동적 네트워크 방어 서비스를 위한 기능 및 보안요구사항 표준이 제정
<TTAK.KO-12.능동적 네트워크 방어 서비스를 위한 기능 및 보안 요구사항> [2019]

악성코드의 감염 예방 가이드, Snort 기반의 침입탐지 규칙 요구사항, 악성코드 경유/유포지 정보 공유 및 악성코드 감염 시 대응 절차와 관련된 표준화 수행
<2019-1328, 다중 백신서비스 환경에서 STIX 기반의 악성코드 분석 정보 교환 포맷> [진행중 2021]

ITU

사이버보안 침해 데이터의 증거능력을 높이기 위해 수집 보존 도구에 대한 요구사항을 표준화 수행
<x.gcpie, Requirements for Collection and Preservation of Cyber Security Incident Evidence> [2020]

샌드박스 환경에서 악성코드 동적 분석을 위한 요구사항 및 가이드라인 표준 (X.rdmase) 개발을 진행하여 표준 제정 완료
<X.1218, Requirements and Guidelines for Dynamic Malware Analysis in a Sandbox Environment> [2020]

표준 상용화

출처: ICT 표준화전략맵 Ver.2021 종합보고서

▸ <한국> 국정원, 모든 **ICT 정보보호**제품에 대해 **보안기능** 시험결과서 발급 제도 시행 [2018]

▸ <한국> 과기정통부, **정보보호제품** 평가 인증 수행규정 개정 공표 [2017] & **정보보호시스템** 평가인증 지침 고시 [2017]

▸ <미국> 국토안보부의 사이버보안 및 통신부서 (DHS CS & C)의 한 부문으로 국가 사이버보안 및 통합 센터 (NCCIC) 내에서 새로운 사이버 위협에 대한 제어 시스템 환경의 방어를 위한 집중 운영 기능 제공 [2015]

▸ <일본> 내각관방, '**사이버보안 기본법**' 제정으로 사이버보안 정책 수립(2014), 기본법을 기반으로 '**사이버보안 전략** 2015' 발표 [2015]

▸ <EU> 유럽 연합 대응기구 ENISA, 빅데이터 **프라이버시 보호** 가이드라인 발표 [2015]

관련 법, 제도 분석

사이버 침해 예방을 위한 표준화 도입

과제번호	초안명	위원회	처리단계	처리일
2021-0677	SDN 기반의 네트워크 보안기능의 인터페이스(I2NSF) 프레임워크 - 제9부: 적용 정책 전달 인터페이스	PG503	초안작성중	2021-06-24
2021-0676	SDN 기반의 네트워크 보안 기능의 인터페이스(I2NSF) 프레임워크 - 제7부: 보안 정책 번역기의 구조 및 절차	PG503	초안작성중	2021-06-24
2021-0026	표적형 이메일 공격을 차단하기 위한 보안 아키텍처 및 요구사항	PG503	초안작성중	2021-06-24
2020-0710	인텔리전스 정보의 신뢰 및 자동화된 교환(TAXII) 버전 2.1	PG503	초안작성중	2021-05-13
2020-0498	모바일 기기 포렌식 지침	PG503	표준공고	2020-12-10
2020-0497	악성코드 통합진단명 생성절차 및 요구사항	PG503	표준공고	2021-06-30
2020-0496	SDN 기반의 네트워크 보안 기능의 인터페이스(I2NSF) 프레임워크 - 제8부: IBN-Blockchain 기반 네트워크 보안 관리 시스템	PG503	표준공고	2020-12-10

국내·국제 표준으로 제정

International Telecommunication Union

국제 ICT 표준화 기구 **ITU(국제전기통신연합)**

- 1865년 국제전신연합International Telegraph Union을 모체로 설립된 국제연합UN 산하 정보통신 관련 국제기구
- 현재 193개 국가가 회원국으로 참여
- 유무선 통신, 전파, 방송, 위성 주파수 등에 대한 규칙(Regulation)과 권고(Recommendation)의 개발과 국가 협력 역할을 수행

TTA 한국정보통신기술협회 Telecommunications Technology Association

우리나라 대표 ICT 표준화 기구 **TTA(한국정보통신기술협회)**

- 정보통신 산업과 기술진흥, 국민경제 발전을 목표로 방송통신발전기본법 제34조에 근거하여 1988년 설립된 비영리기관
- ICT 표준화 및 시험인증 업무를 수행하며, '정보통신표준화위원회'에서 통신망, 이동통신, 방송, 소프트웨어, 정보보호 등의 분야에 대한 TTA 표준 제정

공신력 있는 이메일 해킹 차단 방법 부재

송금 사기

news1 KOREA

"이 계좌로 송금하세요"… 이메일 해킹 무역사기 '또'

정보 유출

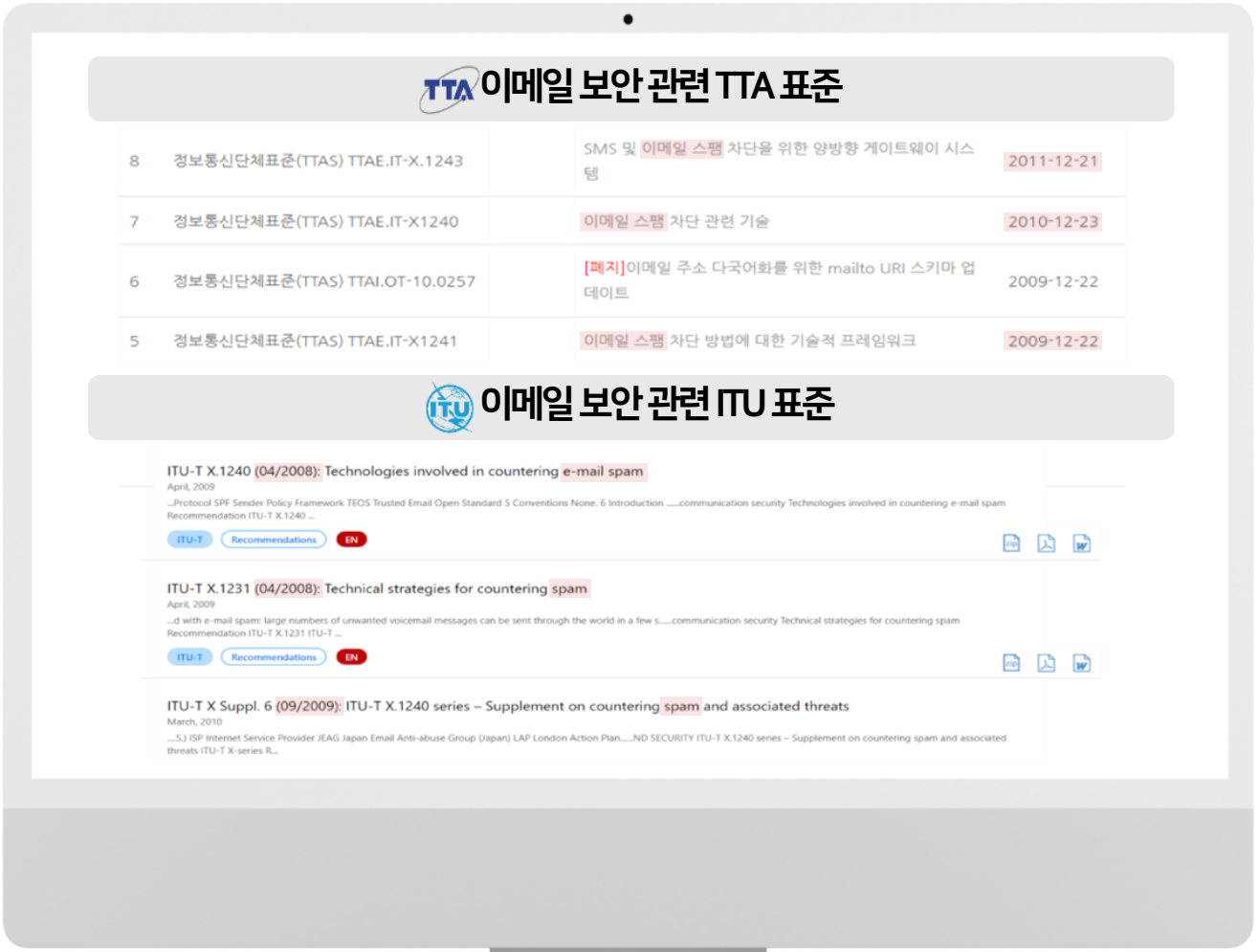
한국경제

전 세계 기업, 소비자 데이터 유출로 '몸살'

전산 마비

한국경제

독해진 디도스…포털·은행 공격 1년새 두 배



㈜기원테크 ITU 국제표준 TD561 관련 내용

ICT Standards

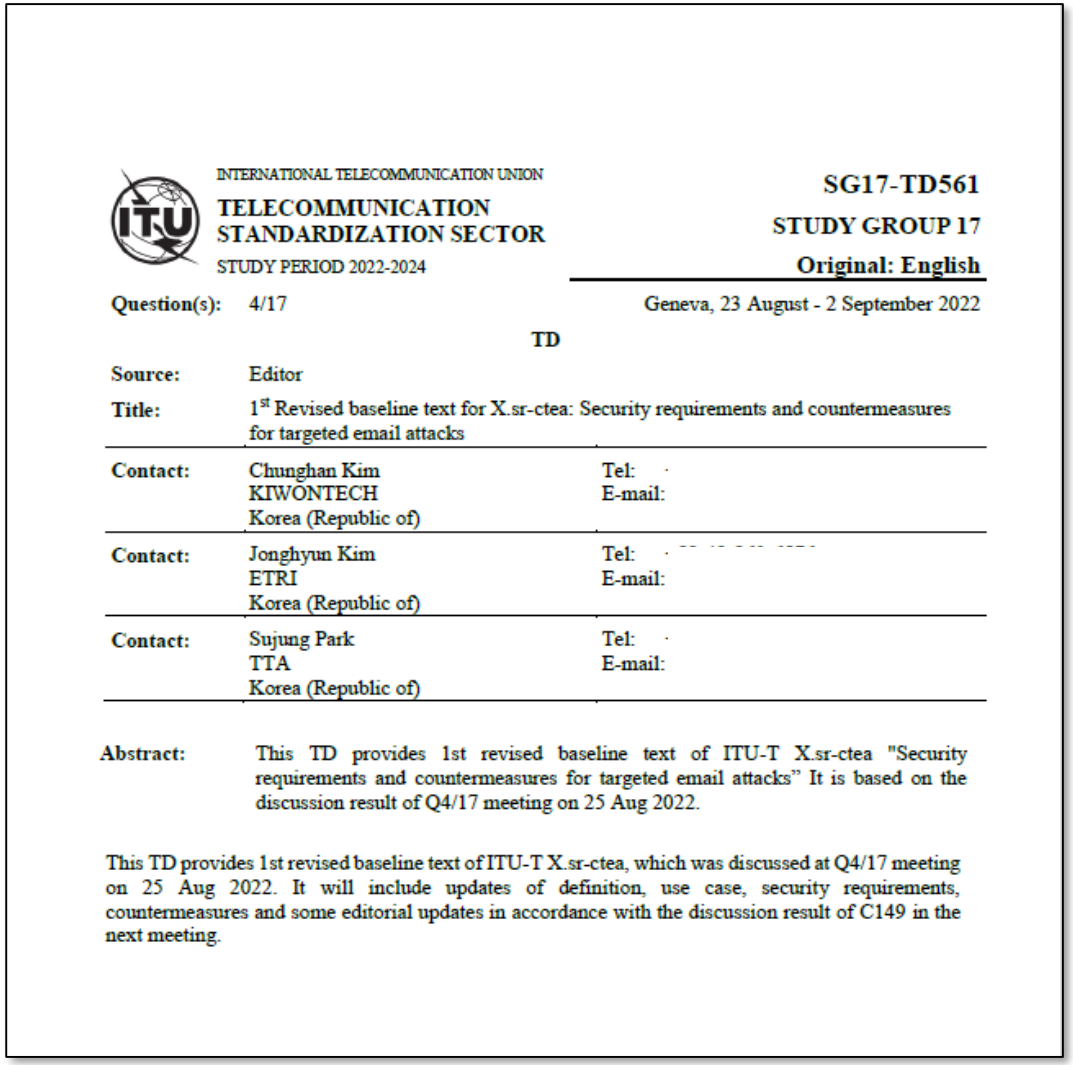
- ITU 국제 표준 소개 - TD561
- 표준 문서 목차
- 표적형 이메일 공격 종류
- 표적형 이메일 공격 차단을 위한 보안 기능
- 보안 기능 요구사항 분류
- 대응방안 (기술)

ITU 국제 표준 소개 - TD561

2022 ITU 2차 Geneva 회의를 통해 결정된 기원테크 TD561 문서

제목: “Security requirements and countermeasures for targeted email attacks”

- **표적형 이메일 공격**의 종류와 공격을 막기 위한 **보안 기능 요구 사항** 및 그에 따른 **대응방안**을 나열하고 있음



INTERNATIONAL TELECOMMUNICATION UNION
TELECOMMUNICATION STANDARDIZATION SECTOR
STUDY PERIOD 2022-2024

SG17-TD561
STUDY GROUP 17
Original: English

Question(s): 4/17 — Geneva, 23 August - 2 September 2022

TD

Source:	Editor	
Title:	1st Revised baseline text for X.sr-ctea: Security requirements and countermeasures for targeted email attacks	
Contact:	Chunghan Kim KIWONTECH Korea (Republic of)	Tel: E-mail:
Contact:	Jonghyun Kim ETRI Korea (Republic of)	Tel: E-mail:
Contact:	Sujung Park TTA Korea (Republic of)	Tel: E-mail:

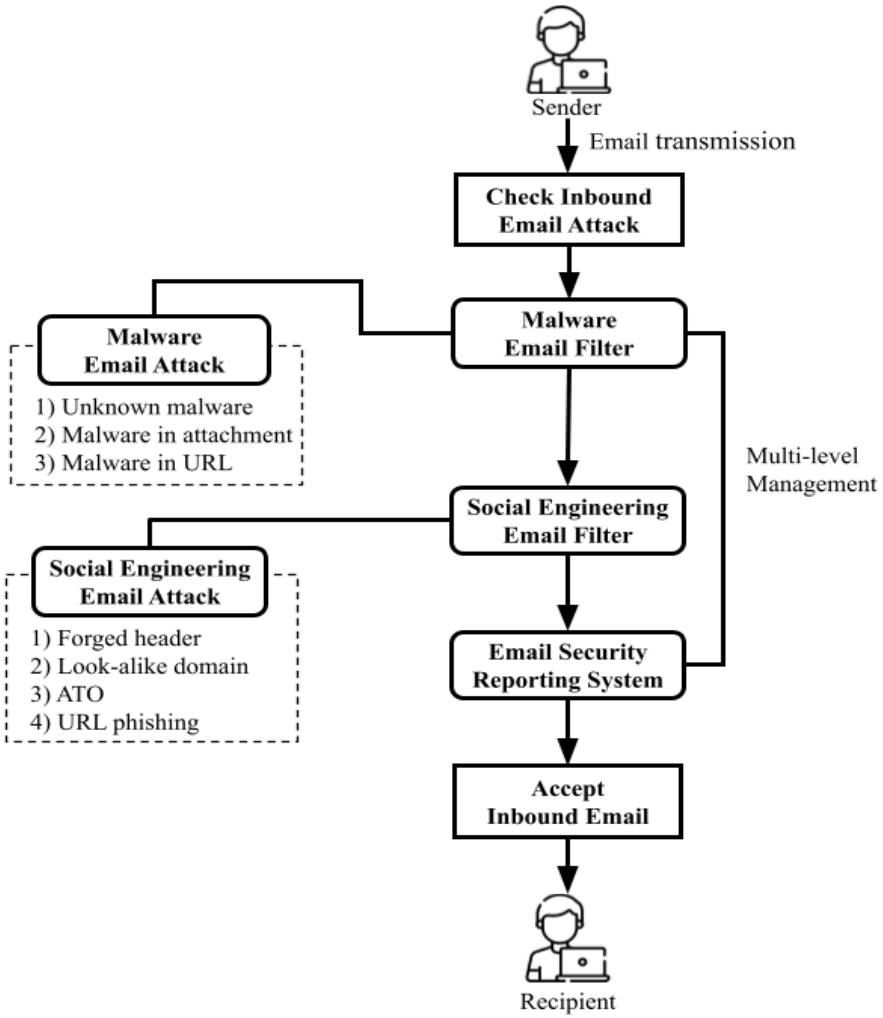
Abstract: This TD provides 1st revised baseline text of ITU-T X.sr-ctea "Security requirements and countermeasures for targeted email attacks" It is based on the discussion result of Q4/17 meeting on 25 Aug 2022.

This TD provides 1st revised baseline text of ITU-T X.sr-ctea, which was discussed at Q4/17 meeting on 25 Aug 2022. It will include updates of definition, use case, security requirements, countermeasures and some editorial updates in accordance with the discussion result of C149 in the next meeting.

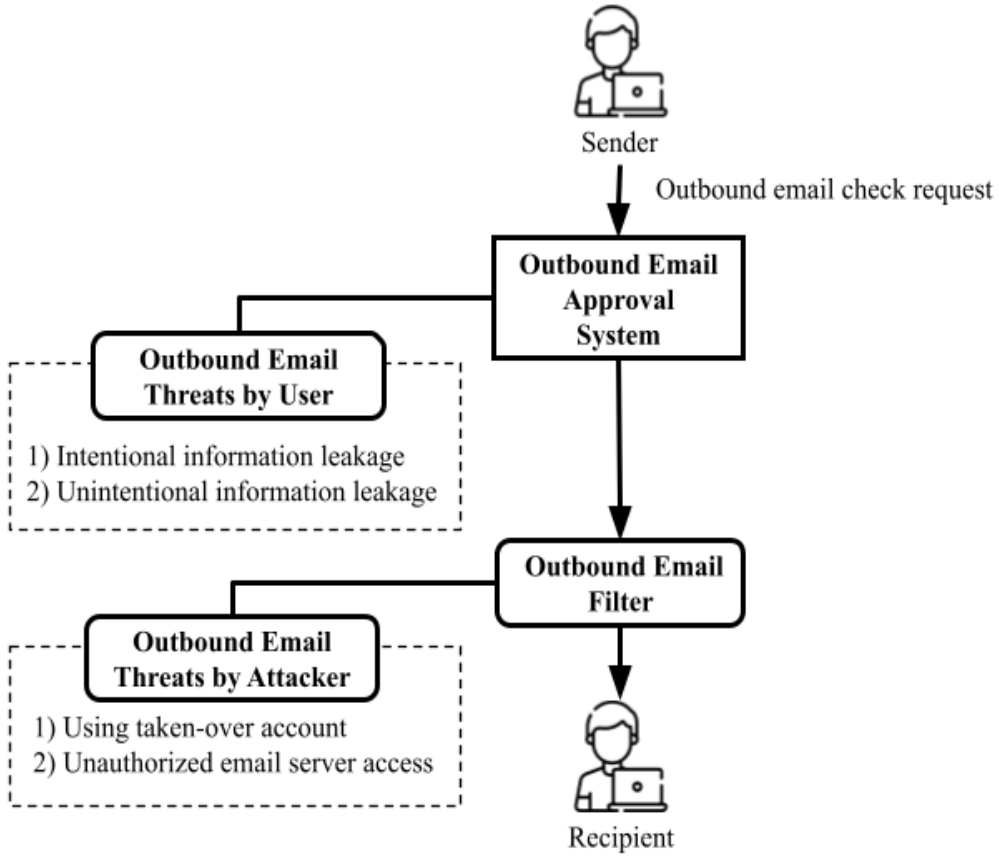
표준 문서 목차

Table of Contents

표적형 이메일 공격 종류



[수신 메일 공격과 보안 프로세스]



[발신 메일 공격과 보안 프로세스]

표적형 이메일 공격 차단을 위한 보안 기능

구분	No.	세부내용	기술중요도	기술특이성
스팸 메일 공격 대응 부문	1	관리자가 설정한 키워드를 포함하는 메일을 필터링할 수 있어야 한다.	필수	-
	2	등록되지 않은 IP의 릴레이 시도를 탐지 및 차단하는 기능이 제공되어야 한다.	필수	-
	3	수신된 이메일에 포함된 이미지도 탐지가 가능하여 스팸 메일로 분류할 수 있는 기능이 제공되어야 한다.	선택	이미지 탐지 방식 검토 필요
	4	기업 보안정책에 따라 선호도 반영 스팸 필터링을 통해 기업 정책 맞춤형 필터링과 그룹별 맞춤형 필터링 제공이 가능하여야 한다.	필수	맞춤형 필터링의 구체화에 따른 검토 필요
	5	IP/DNS 유효성 검사, 동일 IP 대량 메일 차단 필터링, 정규식 필터링 검사를 비롯하여 RBL, SURBL 필터링 등의 다중 필터링 체계를 운용하여야 한다. (RBL: Real-time Block List, SURBL: Spam URI Real-time Block List))	선택	다중 필터링 체계의 구체화에 따른 검토 필요

구분	No.	세부내용	기술중요도	기술특이성
악성 코드 공격 대응 부문	1	분류된 악성코드 의심 메일에 대하여 영구적으로 삭제가 가능하거나 사용자 요청 시 재전송하는 기능이 제공되어야 한다.	선택	-
	2	악성코드 공격에 대응하기 위하여 가상영역(virtual machine) 내에서 검사할 경우 다양한 파일 확장자에 대하여 검사가 가능하여야 한다.	필수	-
	3	제로데이 취약점을 이용하는 신종 악성코드 공격에 대응하기 위하여 행위 기반 검사를 시행하여 패턴에 등록되지 않은 신종 바이러스를 검출할 수 있어야 한다.	필수	행위 기반 검사 기술의 진보성 검토 필요
	4	URL에 악성코드 포함 여부 검사 시 다중으로 연결된 URL의 최종 URL까지 검사할 수 있어야 한다.	필수	-
	5	URL에 악성코드 포함 여부 검사 시 악성으로 의심되는 URL의 경우 사용자가 실수로 실행할 수 있는 경우를 방지할 수 있는 별도의 기능이 제공되어야 한다. (예 : URL의 하이퍼링크를 제거, URL을 별도의 문구로 표기, URL을 이미지로 변환 등)	필수	**실행 방지 기능** 구체화 시 검토 필요
	6	URL에 악성코드 포함 여부 검사 시, 사후 URL 활성 공격을 차단하기 위하여 사용자가 이메일에 수신된 URL을 실행할 때마다 안전 여부를 검사할 수 있어야 한다.	필수	-
	7	URL에 악성코드 포함 여부 검사 시 URL에 악성 요소가 있을 시 해당 URL이 분리되어 보안 웹 게이트웨이로 유도된 후 그곳에서 위험한 요소를 제거하여 안전한 웹 사이트 콘텐츠만 사용자에게 제공되는 기능이 있어야 한다.	선택	-

구분	No.	세부내용	기술중요도	기술특이성
사회공학적 공격 대응 부문	1	(헤더 위변조) 발신자의 메일이 SPF 등의 메일 통신 프로토콜을 준수하였는지 확인할 수 있어야 하며 이를 준수하지 않는 메일에 대하여 차단하거나 사용자에게 경고하는 기능이 있어야 한다.	**필수**	-
	2	(헤더 위변조) 정상발신자를 사칭하는 공격에 대응하기 위하여 발신자 주소, 도메인 및 IP 등 이메일 정보들에 대하여 국내외 평판을 모아 놓은 데이터를 활용하는 기능이 있어야 한다.	**선택**	-
	3	(헤더 위변조) 수신된 이메일에 대하여 '답장' 기능으로 회신 시 수신한 이메일 주소와 회신으로 수신할 이메일 주소가 다를 시 이를 차단 및 사용자에게 경고하는 기능이 있어야 한다.	**필수**	**위변조** 판별 기술의 검토 필요
	4	(유사 메일 주소) 정상발신자를 사칭하는 유사 메일 주소 공격에 대응하기 위하여 보안 관리자 및 사용자가 유사 메일 주소 공격이 시도될 수 있는 특정 메일 주소에 대하여 등록할 수 있는 기능이 있어야 한다.	**필수**	-
	5	(유사 메일 주소) 정상발신자를 사칭하는 유사 메일 주소 공격에 대응하기 위하여 이메일의 이력을 참조하여 사용자마다 이러한 공격을 차단할 수 있는 기능이 있어야 한다.	**필수**	**이메일** 이력 분석 기술의 검토 필요
	6	(계정 탈취) 정상발신자의 계정을 탈취한 후 해당 계정으로 시도되는 공격에 대응하기 위하여 보안 관리자 및 사용자가 특정 IP 및 국가를 등록할 수 있는 기능이 있어야 한다.	**필수**	-
	7	(계정 탈취) 정상발신자의 계정을 탈취한 후 해당 계정으로 시도되는 공격에 대응하기 위하여 사용자의 수신한 이메일의 이력을 참조하여 해당 유형의 공격을 차단할 수 있는 기능이 있어야 한다.	**필수**	**이메일** 이력 분석 기술의 검토 필요
	8	(계정 탈취) 정상발신자를 사칭한 모든 공격에 대하여 의심 징후가 발견될 시 메일을 열람 전 사용자에게 그 정보를 제공하는 기능이 있어야 한다.	**필수**	**의심 징후 탐지** 기술의 검토 필요
	9	(계정 탈취) 사용자 그룹별 별도 운영 정책 적용에 따라 차단 현황과 시스템 상황에 대한 모니터링 보고서는 사용자 설정에 따른 다양한 언어 선택이 가능해야 한다.	**선택**	-
	10	(계정 탈취) 해킹에 의한 악성 이메일 계정 복원을 방지하기 위하여 메일 계정 로그인 정보를 메일 서버와 연동 확인 가능해야 한다.	**선택**	-

보안 기능 요구사항 분류 - ①

구분	기능 코드	세부내용	기원테크 보유특허	경쟁사 보유특허	비고
스팸 메일 공격 대응 부문	1-1	관리자가 설정한 키워드를 포함하는 메일을 필터링할 수 있어야 한다.	⑤	O	상용 기능
	1-2	등록되지 않은 IP의 릴레이 시도를 탐지 및 차단하는 기능이 제공되어야 한다.	⑤	O	상용 기능
	1-3	수신된 이메일에 포함된 이미지도 탐지가 가능하여 스팸 메일로 분류할 수 있는 기능이 제공되어야 한다.	-	O	-
	1-4	기업 보안정책에 따라 선호도 반영 스팸 필터링을 통해 기업 정책 맞춤형 필터링과 그룹별 맞춤형 필터링 제공이 가능하여야 한다.	①	O	-
	1-5	IP/DNS 유효성 검사, 동일 IP 대량 메일 차단 필터링, 정규식 필터링 검사를 비롯하여 RBL, SURBL 필터링 등의 다중 필터링 체계를 운용하여야 한다. (RBL: Real-time Block List, SURBL: Spam URI Real-time Block List))	-	O	-
악성 코드 공격 대응 부문	2-1	분류된 악성코드 의심 메일에 대하여 영구적으로 삭제가 가능하거나 사용자 요청 시 재전송하는 기능이 제공되어야 한다.	-	-	부가 기능
	2-2	악성코드 공격에 대응하기 위하여 가상영역(virtual machine) 내에서 검사할 경우 다양한 파일 확장자에 대하여 검사가 가능하여야 한다.	①,③	O	-
	2-3	제로데이 취약점을 이용하는 신종 악성코드 공격에 대응하기 위하여 행위 기반 검사를 시행하여 패턴에 등록되지 않은 신종 바이러스를 검출할 수 있어야 한다.	⑥	-	-
	2-4	URL에 악성코드 포함 여부 검사 시 다중으로 연결된 URL의 최종 URL까지 검사할 수 있어야 한다.	⑥	O	-
	2-5	URL에 악성코드 포함 여부 검사 시 악성으로 의심되는 URL의 경우 사용자가 실수로 실행할 수 있는 경우를 방지할 수 있는 별도의 기능이 제공되어야 한다. (예 : URL의 하이퍼링크를 제거, URL을 별도의 문구로 표기, URL을 이미지로 변환 등)	⑤,⑥	O	-
	2-6	URL에 악성코드 포함 여부 검사 시, 사후 URL 활성 공격을 차단하기 위하여 사용자가 이메일에 수신된 URL을 실행할 때마다 안전 여부를 검사할 수 있어야 한다.	①,⑥	-	-
	2-7	URL에 악성코드 포함 여부 검사 시 URL에 악성 요소가 있을 시 해당 URL이 분리되어 보안 웹 게이트웨이로 유도된 후 그곳에서 위험한 요소를 제거하여 안전한 웹 사이트 콘텐츠만 사용자에게 제공되는 기능	⑥	O	-

보안 기능 요구사항 분류 - ②

구분	기능 코드	세부내용	기원테크 보유특허	경쟁사 보유특허	비고
사회 공학적 공격 대응 부문	3-1	(헤더 위변조) 발신자의 메일이 SPF 등의 메일 통신 프로토콜을 준수하였는지 확인할 수 있어야 하며 이를 준수하지 않는 메일에 대하여 차단하거나 사용자에게 경고하는 기능이 있어야 한다.	①, ③	O	-
	3-2	(헤더 위변조) 정상발신자를 사칭하는 공격에 대응하기 위하여 발신자 주소, 도메인 및 IP 등 이메일 정보들에 대하여 국내외 평판을 모아 놓은 데이터를 활용하는 기능이 있어야 한다.	①,③,⑤	O	-
	3-3	(헤더 위변조) 수신된 이메일에 대하여 '답장' 기능으로 회신 시 수신한 이메일 주소와 회신으로 수신할 이메일 주소가 다를 시 이를 차단 및 사용자에게 경고하는 기능이 있어야 한다.	③	-	-
	3-4	(유사 메일 주소) 정상발신자를 사칭하는 유사 메일 주소 공격에 대응하기 위하여 보안 관리자 및 사용자가 유사 메일 주소 공격이 시도될 수 있는 특정 메일 주소에 대하여 등록할 수 있는 기능이 있어야 한다.	②,③,⑤	O	-
	3-5	(유사 메일 주소) 정상발신자를 사칭하는 유사 메일 주소 공격에 대응하기 위하여 이메일의 이력을 참조하여 사용자마다 이러한 공격을 차단할 수 있는 기능이 있어야 한다.	①,②,⑤	O	-
	3-6	(계정 탈취) 정상발신자의 계정을 탈취한 후 해당 계정으로 시도되는 공격에 대응하기 위하여 보안 관리자 및 사용자가 특정 IP 및 국가를 등록할 수 있는 기능이 있어야 한다.	-	O	-
	3-7	(계정 탈취) 정상발신자의 계정을 탈취한 후 해당 계정으로 시도되는 공격에 대응하기 위하여 사용자의 수신한 이메일의 이력을 참조하여 해당 유형의 공격을 차단할 수 있는 기능이 있어야 한다.	②	O	-
	3-8	(계정 탈취) 정상발신자를 사칭한 모든 공격에 대하여 의심 징후가 발견될 시 메일을 열람 전 사용자에게 그 정보를 제공하는 기능이 있어야 한다.	③,⑤	-	-
	3-9	(계정 탈취) 사용자 그룹별 별도 운영 정책 적용에 따라 차단 현황과 시스템 상황에 대한 모니터링 보고서는 사용자 설정에 따른 다양한 언어 선택이 가능해야 한다.	-	-	부가 기능
	3-10	(계정 탈취) 해킹에 의한 악성 이메일 계정 복원을 방지하기 위하여 메일 계정 로그인 정보를 메일 서버와 연동 확인 가능해야 한다.	-	-	부가 기능

*범례(BC: Barracuda, FE: FireEye, GG:Google, MC: Mimecast, MS: Microsoft, TM: Trend Micro, PP: Proofpoint)

보안 기능 요구사항 분류 - ③

구분	기능 코드	세부내용	기원테크 보유특허	경쟁사 보유특허	비고
발신 관련 공격 대응 부문	4-1	웹 메일 접속 시 허용되지 않은 IP 및 국가로부터 접속이 차단되는 기능과 허용한 IP 및 국가에서만 접속이 가능하게 하는 기능이 있어야 한다.	-	O	접근 제어
	4-2	허용되지 않은 IP 및 국가로부터 메일 클라이언트에 접속이 차단되는 기능과 허용한 IP 및 국가에서만 메일 클라이언트에 접속이 가능하게 하는 기능이 있어야 한다.	-	O	접근 제어
	4-3	특정 조건 (키워드 및 메일주소)에 해당하는 발송 메일에 대해서는 별도의 승인 절차 및 차단하는 기능이 있어야 한다.	④,⑤	O	-
	4-4	특정 조건 (키워드 및 메일주소)에 해당하는 발송 메일에 대하여 첨부파일 및 메일을 암호화할 수 있는 기능이 있어야 한다.	⑧	O	-
	4-5	발송 메일에 대하여 스팸 또는 악성코드가 포함된 메일인지 검사할 수 있는 기능이 있어야 하며 이에 해당할 시 발송을 차단하는 기능이 있어야 한다.	⑤	O	-
	4-6	발송한 메일에 대하여 열람 위치와 열람 횟수를 확인할 수 있어야 한다.	-	-	보안메일 기능
	4-7	메일 발송 시 발송 전 대기 시간을 설정할 수 있어야 하며 오송신 시 대기 시간 내에 메일 회수 기능이 있어야 한다.	-	O	보안메일 기능
	4-8	계정별 메일 발송 횟수 제한이 가능해야 하며 제한 횟수를 초과한다면 도용된 계정으로 판단하여 메일 발송을 설정한 시간 내 자동으로 차단하는 기능이 있어야 한다.	-	-	부가 기능
공통보안기능	5-1	자체 또는 외부 데이터에 기반하여 스팸, 악성코드, 헤더 위변조, 유사 메일 주소, 계정 탈취 여부, 악성 주소로의 메일 발신 여부를 검사한다.	⑤	O	-
	5-2	스팸, 악성코드 공격, 헤더 위변조 공격, 유사 메일 주소 공격, 계정 탈취 공격 탐지, 악성 주소로의 메일 발신에 대한 탐지 및 차단 현황과 시스템 상황에 대한 모니터링 기능이 보안 관리자에게 제공되어야 하며 이에 대한 상세한(IP 기록 등) 보고서를 제공해야한다.	①	-	제조사특성
	5-3	오탐의 경우를 대비하여 관리자는 경우에 따라 차단한 이메일에 대하여 확인이 가능하여야 하며 (직접 열람 혹은 다운로드 등) 차단당한 계정의 복원 기능이 있어야 한다.	-	O	상용 기능

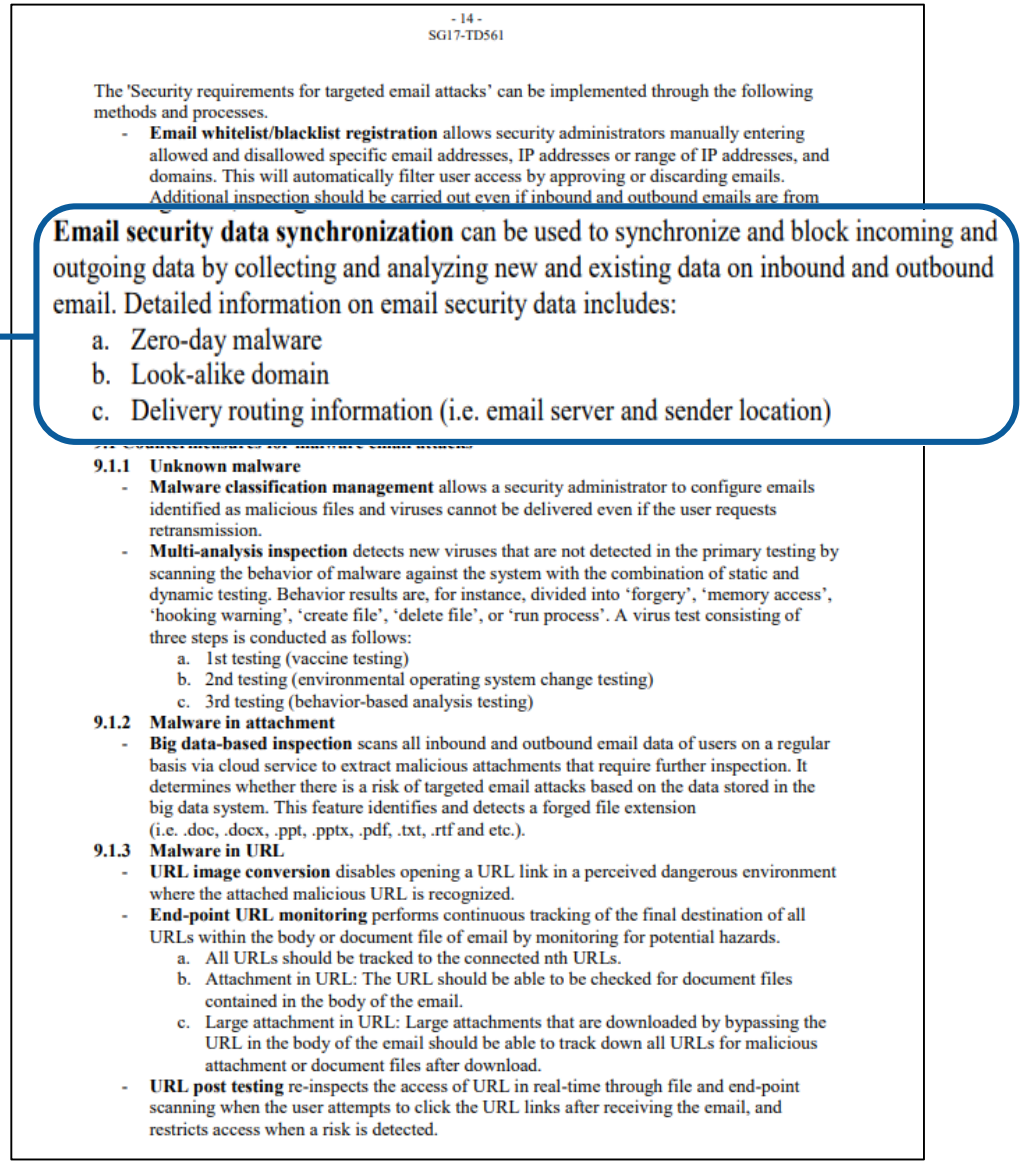
*범례(BC: Barracuda, FE: FireEye, GG:Google, MC: Mimecast, MS: Microsoft, TM: Trend Micro, PP: Proofpoint)

대응방안 (기술)

9. 표적형 이메일 공격에 대한 대응책

'표적형 이메일 공격에 대한 보안 요구 사항'은 다음과 같은 방법 및 과정을 통해 구현될 수 있다.

- 이메일 보안 데이터 동기화를 통해 수/발신 이메일의 새 데이터와 기존 데이터를 수집하고 분석하여 수신 및 송신 데이터를 동기화하고 차단할 수 있다. 이메일 보안 데이터에 대한 자세한 내용은 다음과 같다.
    1.제로 데이
    2.유사 도메인
    3.발송 경로 정보(예: 메일 서버 및 보낸 사람 위치(발송지))



- 14 -
SG17-TD561

The 'Security requirements for targeted email attacks' can be implemented through the following methods and processes.

- **Email whitelist/blacklist registration** allows security administrators manually entering allowed and disallowed specific email addresses, IP addresses or range of IP addresses, and domains. This will automatically filter user access by approving or discarding emails. Additional inspection should be carried out even if inbound and outbound emails are from

Email security data synchronization can be used to synchronize and block incoming and outgoing data by collecting and analyzing new and existing data on inbound and outbound email. Detailed information on email security data includes:

a. Zero-day malware
b. Look-alike domain
c. Delivery routing information (i.e. email server and sender location)

9.1.1 Unknown malware

- **Malware classification management** allows a security administrator to configure emails identified as malicious files and viruses cannot be delivered even if the user requests retransmission.
- **Multi-analysis inspection** detects new viruses that are not detected in the primary testing by scanning the behavior of malware against the system with the combination of static and dynamic testing. Behavior results are, for instance, divided into 'forgery', 'memory access', 'hooking warning', 'create file', 'delete file', or 'run process'. A virus test consisting of three steps is conducted as follows:
    a. 1st testing (vaccine testing)
    b. 2nd testing (environmental operating system change testing)
    c. 3rd testing (behavior-based analysis testing)

9.1.2 Malware in attachment

- **Big data-based inspection** scans all inbound and outbound email data of users on a regular basis via cloud service to extract malicious attachments that require further inspection. It determines whether there is a risk of targeted email attacks based on the data stored in the big data system. This feature identifies and detects a forged file extension (i.e. .doc, .docx, .ppt, .pptx, .pdf, .txt, .rtf and etc.).

9.1.3 Malware in URL

- **URL image conversion** disables opening a URL link in a perceived dangerous environment where the attached malicious URL is recognized.
- **End-point URL monitoring** performs continuous tracking of the final destination of all URLs within the body or document file of email by monitoring for potential hazards.
    a. All URLs should be tracked to the connected nth URLs.
    b. Attachment in URL: The URL should be able to be checked for document files contained in the body of the email.
    c. Large attachment in URL: Large attachments that are downloaded by bypassing the URL in the body of the email should be able to track down all URLs for malicious attachment or document files after download.
- **URL post testing** re-inspects the access of URL in real-time through file and end-point scanning when the user attempts to click the URL links after receiving the email, and restricts access when a risk is detected.

대응방안 (기술)

9.4.2 비고의적 정보 유출

전송 시간 지연 및 발신 이메일 회신/삭제를 통해 사용자의 고의적인/비고의적인 정보 유출을 방지하려면 이메일 발송 시간과 전달 시간 사이에 **지연 시간을 설정**할 수 있어야한다. 지연 시간 동안 발송된 이메일은 전달 취소되어야 한다. 지연 시간 내에 **이메일을 취소할 수 있는 권한은** 관리자와 사용자에게 부여되며, 취소된 발신 메일은 발송할 수 없고 발송을 원할시 다시 작성해야 한다.

- **Email delivery restriction** allows to set the limit for the maximum number of emails that can be sent at once. To keep the email server's status and security of account by limiting the number of users can send per day and the number of recipients per email.

9.4.1 Intentional information leakage

- **Email encryption** protects sensitive information from being read by anyone other than the intended recipient by encrypting or disguising the contents of email and attachments.

Unintentional information leakage

Delay in sending time and retrieve/delete outbound email: To prevent intentional/unintentional leakage of information by the user, a delay time is recommended to be set between the sending time and the delivered time of the email, and the email sending during the delay time should be able to cancel. The right to cancel email within the delay time is granted to the administrator and user, and once cancelled outbound email cannot be sent, and email must be rewritten.

9.5.1 Using taken-over account

- **IP permission setting** allows a security administrator and an email user to register specific IP addresses and countries that are accessible by 'Security IP Registration' or 'Permitted Country Registration' for blocking email attacks by receiving emails from the permitted IP addresses and countries.

9.5.2 Unauthorized email server access

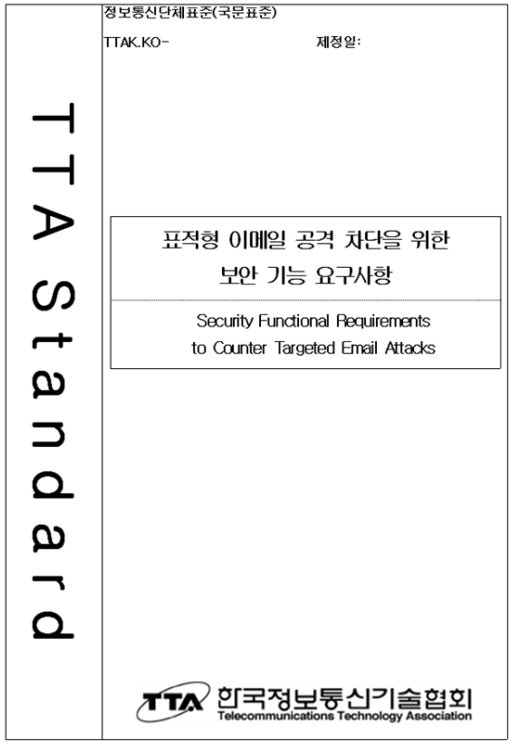
- **Email server/IP access control** allows administrators to control secure email links sent by restricting access to web mails or mail clients. Web mail can be blocked through registered IPs, and communication access based on client server protocol (POP3)/Mail Transfer Protocol (SMTP) is controlled to block mail client communication. You can send email from registered IP addresses and countries and provide logs of email server access restrictions such as IP addresses, dates, and so on.
- **Email server access log** allows to determine whether user's access is authorized or unauthorized with the following information:
  a. User identification,
  b. Encrypted email,
  c. User password,
  d. Device identification,
  e. Access IP,
  f. Access location,
  g. Access time,
  h. Communication protocol identification for the email engine.

표준 특허 추진 과정

ICT Standards

- TD561 국제 표준의 기반, TTA 국내 표준 문서
- 표준 특허 확보를 위한 필요 전략
- 기원테크 보유 특허 리스트
- 표적형 이메일 공격 차단 관련 핵심 표준 특허 도출 과정
- 기원테크 기술 관련 분석 히스토리
- 국제표준화기구 타겟팅
- 기고문 작성과 연계된 표준 특허 확보 전략 수립
- 향후 표준화 과정과 연계된 해외출원 전략 수립
- 보유 기술의 국제표준 매칭전략 수립 및 반영
- 기원테크 국제 표준화 및 표준 특허 확보전략 진행내용 요약

TD561 국제 표준의 기반, TTA 국내 표준 문서


정보통신단체표준(국문표준)

TTAK.KO-　　제정일:

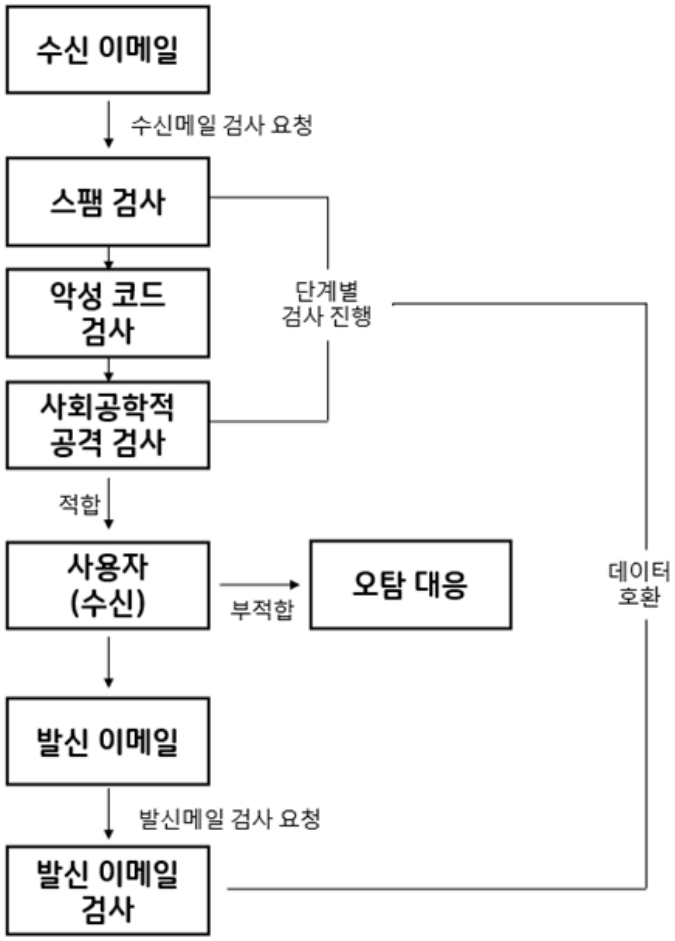
TTA Standard

표적형 이메일 공격 차단을 위한
보안 기능 요구사항

Security Functional Requirements
to Counter Targeted Email Attacks

TTA 한국정보통신기술협회
Telecommunications Technology Association

표준종류	정보통신단체표준(TTAS)		
표준번호	TTAK.KO-12.0379	구 표준번호	
제개정일	2021-12-08	총 페이지	26
한글 표준명	표적형 이메일 공격 차단을 위한 보안 기능 요구사항		
영문 표준명	Security Functional Requirements to Counter Targeted Email Attacks		
한글 내용요약	본 표준은 표적형 이메일 공격을 차단하기 위한 요구사항에 대한 최소한의 기준을 이메일 사용자 및 개발자들에게 제공한다. 또한 표적형 이메일의 정의부터 각 공격 유형별 대응방안도 제시한다.		
영문 내용요약	This standard provides email users and programmers with minimum criteria for their requirements to block targeted email attacks. It presents information from the definition of targeted email to the countermeasures for each type of attack.		



(그림 5-3) 표적형 이메일 공격 차단 개념도

표준 특허 확보를 위한 필요 전략

기원테크 보유 특허의 표준 매칭특허 발굴/창출:

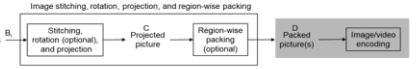
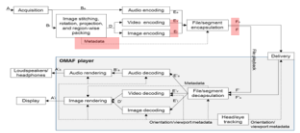
➔ TTA 확정 표준안(표적형 이메일 공격 차단을 위한 보안 기능 요구사항)을 기초로, 표적형 공격 위험의 보안 진단 솔루션의 국제 표준안 제안내용 대비 보유특허와의 상세비교분석

➔ 등록 특허에 대한 대한 Claim Chart 작성 지원

➔ 출원 중(Pending) 특허에 대한 대한 심층 분석 및 보정, 분할, OA 대응안 마련

No	국가	구분	발명의 명칭	출원번호	출원일	출원인	등록번호	등록일	분석 No.
1	KR	등록	지능형 및 학습형 메일 방화벽 장치	10-2015-0094764	2015.07.02	(주)기원테크	10-1814088	2017.12.26	①
2	KR	등록	사기성 메일의 위험도를 판단하는 방법 및 그를 위한 장치	10-2017-0082082	2017.06.28	(주)기원테크	10-1857969	2018.05.09	②
3	JP	등록	사기 메일의 위험도를 판단하는 방법 및 이를 위한 장치	2017-237201	2017.12.11	(주)기원테크	6483227	2019.02.22	N/A
4	KR	등록	인공지능 기반의 메일 관리 방법 및 장치	10-2019-7029159	2019.08.07	(주)기원테크	10-2247617	2021.04.27	③
5	KR	등록	메일 수신 및 발신 시스템	10-2014-0102511	2014.08.08	김충한	10-1696877	2017.01.10	④
6	KR	출원	업체 고객 기반의 영업처리장치	10-2020-0185480	2020.12.29	(주)기원테크	-	-	N/A
7	KR	출원	보안 레벨 기반의 계층적 아키텍처를 이용한 이메일 보안 서비스 제공 장치 및 그 동작 방법	10-2020-0180096	2020.12.21	(주)기원테크	-	-	⑤
8	PCT	출원	보안 레벨 기반의 계층적 아키텍처를 이용한 이메일 보안 서비스 제공 장치 및 그 동작 방법	PCT/KR2021/006395	2021.05.24	(주)기원테크	-	-	⑤
9	PCT	출원	메일 보안 기반의 제로데이 URL 공격 방어 서비스 제공 장치 및 그 동작 방법	PCT/KR2020/019256	2020.12.29	(주)기원테크	-	-	⑥
10	PCT	출원	전자 메일을 관리하는 방법 및 장치	PCT/KR2020/012181	2020.	(주)기원테크	-	-	⑦,⑧
11	PCT	출원	전자 메일 관리 방법 및 장치	PCT/KR2020/017248	2020.	(주)기원테크	-	-	⑦,⑧
12	PCT	출원	폴더 보호 기능을 제공하는 보안 장비 시스템의 구동 장치 및 그 동작 방법	PCT/KR2021/009940	2020.07.30	(주)기원테크	-	-	N/A
13	PCT	국제출원	인공지능 기반의 메일 관리 방법 및 장치	PCT/KR2019/009870	2019.08.07	(주)기원테크	-	-	N/A
14	US	개국출원	인공지능 기반의 메일 관리 방법 및 장치	16/499212	2019.09.27	(주)기원테크	-	-	N/A
15	SG	개국출원	인공지능 기반의 메일 관리 방법 및 장치	11201909530S	2019.10.11	(주)기원테크	-	-	N/A
16	JP	개국출원	인공지능 기반의 메일 관리 방법 및 장치	-	2019.10.15	(주)기원테크	-	-	N/A
17	VN	개국출원	인공지능 기반의 메일 관리 방법 및 장치	1-2019-05680	2019.10.15	(주)기원테크	-	-	N/A
18	MZ	개국출원	인공지능 기반의 메일 관리 방법 및 장치	PI2020005654	2020.10.28	(주)기원테크	-	-	N/A

[대상건 선정 검토작업]

Limitation	Relevant Portions of OMAF International Standard	Comments
상기 변환된 2차원 이미지를 부호화하는 단계; 및	**4.2.2** Stitching, rotation, projection, and region-wise packing … The image data on the unit sphere is further arranged onto a two-dimensional projected picture (C). The projected picture covers the entire sphere. Optionally, region-wise packing is then applied to map the projected picture onto a packed picture. If the region-wise packing is not applied, the packed picture is identical to the projected picture, and this picture is given as input to image/video encoding. Otherwise, projected regions are mapped onto a packed picture (D) by indicating the location, shape, and size of each packed region in the packed picture, and the packed picture (D) is given as input to **image/video encoding**. The packed picture may cover only a part of the entire sphere. … 	**Sections 4.2.2**에 따르면, 영역 기반 패킹(region-wise packing)이 수행된 "packed picture (D)"에 대해 ***image/video encoding***이 수행됨
상기 부호화된 2차원 이미지와 메타데이터를 전송하는 단계;를 포함하고,	**4.2 Overall architecture for omnidirectional media with projected video** **4.2.1 Overview**  …The **coded images, video**, and/or audio are then composed into a media file for file playback (F) or a sequence of an initialization segment and media segments for streaming (Fs), according to a particular media container file format. In this document, the media container file format is the ISO Base Media File Format specified in ISO/IEC 14496-12. The file encapsulator also includes **metadata** into the file or the segments, such as projection and region-wise packing information assisting in rendering the decoded packed pictures.	**Sections 4.2.1**에 따르면, *부호화된 이미지 또는 비디오 "coded images, video"*는 미디어 파일(F/F')에 포함되어 전송됨. 또한, 전송되는 미디어 파일(file or the segments)에는, 랜더링에 도움을 주는 projection and region-wise packing information 등과 같은 ***메타데이터(metadata)***를 포함함.

[Claim Chart 예시]

기원테크 보유 특허 리스트

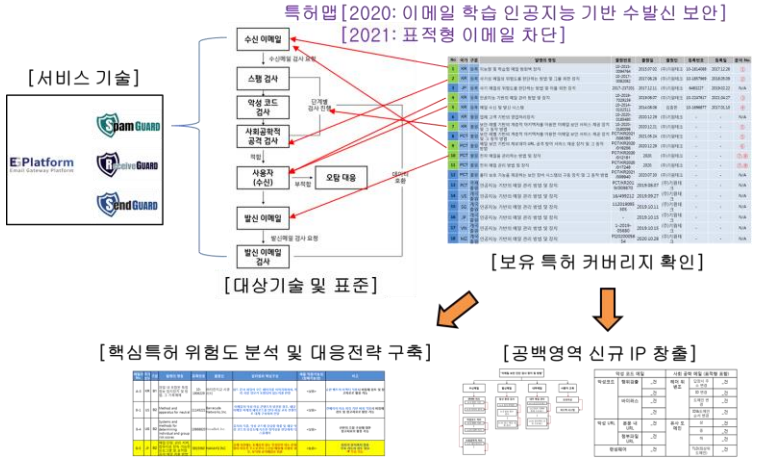
No	국가	구분	발명의 명칭	분석 No.
1	KR	등록	지능형 및 학습형 메일 방화벽 장치	①
2	KR	등록	사기성 메일의 위험도를 판단하는 방법 및 그를 위한 장치	②
3	JP	등록	사기 메일의 위험도를 판단하는 방법 및 이를 위한 장치	N/A
4	KR	등록	인공지능 기반의 메일 관리 방법 및 장치	③
5	KR	등록	메일 수신 및 발신 시스템	④
6	KR	출원	업체 고객 기반의 영업처리장치	N/A
7	KR	출원	보안 레벨 기반의 계층적 아키텍처를 이용한 이메일 보안 서비스 제공 장치 및 그 동작 방법	⑤
8	PCT	출원	보안 레벨 기반의 계층적 아키텍처를 이용한 이메일 보안 서비스 제공 장치 및 그 동작 방법	⑤
9	PCT	출원	메일 보안 기반의 제로데이 URL 공격 방어 서비스 제공 장치 및 그 동작 방법	⑥
10	PCT	출원	전자 메일을 관리하는 방법 및 장치	⑦,⑧
11	PCT	출원	전자 메일 관리 방법 및 장치	⑦,⑧
12	PCT	출원	폴더 보호 기능을 제공하는 보안 장비 시스템의 구동 장치 및 그 동작 방법	N/A
13	PCT	국제 출원	인공지능 기반의 메일 관리 방법 및 장치	N/A
14	US	개국 출원	인공지능 기반의 메일 관리 방법 및 장치	N/A
15	SG	개국 출원	인공지능 기반의 메일 관리 방법 및 장치	N/A
16	JP	개국 출원	인공지능 기반의 메일 관리 방법 및 장치	N/A
17	VN	개국 출원	인공지능 기반의 메일 관리 방법 및 장치	N/A
18	MZ	개국 출원	인공지능 기반의 메일 관리 방법 및 장치	N/A

표적형 이메일 공격 차단 관련 핵심 표준 특허 도출 과정

- **기원테크는** 국내 표준 '**표적형 이메일 공격 차단 보안 기능 요구사항**'을 기반으로, **표적형 공격 위험의 보안 진단 솔루션**을 제공하는 기술의 **국제 표준화 과정**을 진행하고 있음
- **사용자 맞춤형 이메일 보안 진단 검사 및 리포트**를 표준화하기 위하여는, **차단 기준, 통계 항목과, 진단 기준**의 유형별 표준화가 요구됨
- **국내 표준의 요소기술 대비 특허 동향 분석**과, 이를 기반으로 하는 **보안 진단 솔루션의 신규 표준기술 예측 및 표준특허 선점**을 위한 표준 특허 인큐베이팅 컨설팅 진행

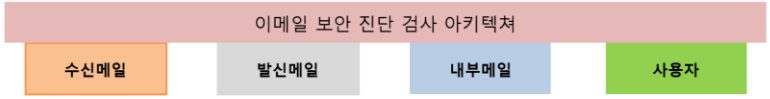
기원테크 기술 관련 분석 히스토리

[이메일 보안 플랫폼 관련 체계적 특허맵 수행]



[계층적 이메일 보안 진단 관련 특허전략 수립]

- 이메일 처리 대상별 단계적, 계층적 진단 검사 장치 및 방법을 통한 '통합'과 '표준화'



- 이메일을 통한 공격 유형에 따른 위험 대상을 분류 및 타겟팅하여, 단계적(Lv.[n]) 대응 기술 고도화

[표적형 이메일 공격 표준 특허 커버리지 분석]

◆ **(주)기원테크 보유 특허 커버리지 및 경쟁사의 보유 특허 분석 결과**

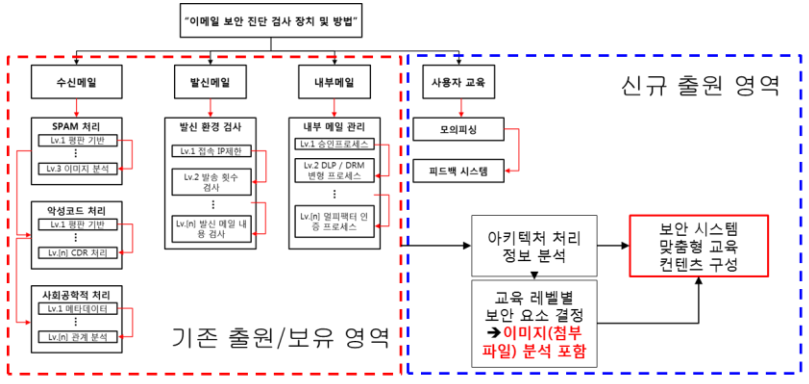
- 표적형 이메일 공격 차단을 위한 표준기술에 대하여 (주)기원테크의 보유 특허가 대응되는 커버리지를 분석함으로써 표준화 기술 기능 분류표에 따른 보유 또는 미보유 특허를 선별
- **표준화 기술 기능 분류표를 구축하여, 경쟁사 보유특허와의 대비 확인 수행**
- **기원테크 보유 특허는 없으나, 경쟁사의 특허는 존재하는 표준상의 위험 기술영역 확인**

구분	기능 코드	세부내용	기원테크 보유특허	경쟁사 보유특허
스팸 메일 공격 대응 부문	1-3	수신된 이메일에 포함된 이미지도 탐지가 가능하여 스팸 메일로 분류할 수 있는 기능이 제공되어야 한다.	-	○
	1-5	IP/DNS 유효성 검사, 동일 IP 대량 메일 차단 필터링, 정규식 필터링 검사를 비롯하여 RBL, SURBL 필터링 등의 다중 필터링 체계를 운용하여야 한다. (RBL: Real-time Block List, SURBL: Spam URI Real-time Block List))	-	○
발신 관련 공격 대응 부문	4-1	평 메일 접속 시 허용되지 않은 IP 및 국가로부터 접속이 차단되는 기능과 허용한 IP 및 국가에서만 접속이 가능하게 하는 기능이 있어야 한다.	-	○
	4-2	허용되지 않은 IP 및 국가로부터 메일 클라이언트에 접속이 차단되는 기능과 허용한 IP 및 국가에서만 메일 클라이언트에 접속이 가능하게 하는 기능이 있어야 한다.	-	○

요소 특허에 대응한 특허 분석 수행

- 경쟁사의 특허 기술요소 중 **이미지 탐지, IP 필터링**에 대한 분석을 통해 표준화 기술에서 요구되는 주요 기술의 권리범위를 확인하고 대응 전략을 검토
- 키워드 분석을 통해 **기술영역의 선점** 또는 **관련 기술의 회피설계**를 수행

[표적형 이메일 공격 관련 신규 특허 IPR&D]



➔핵심특허 및 주요특허들의 기술적 요소와, 기존 출원/보유기술을 유기적으로 결합시켜 대상 기술을 develop할 수 있으며, 이는 표준의 공백 영역을 커버 가능하면서도, **신규 IP 창출**을 위한 기술로서 활용가능

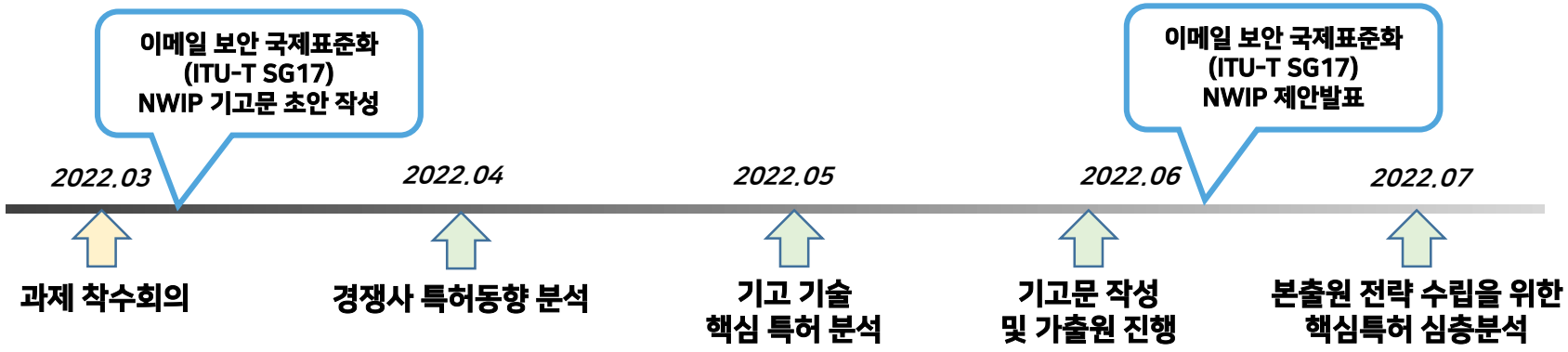
국제표준화기구 타겟팅

대상 표준화 기구: ITU-T SG17(Security)

보안구조 및 프레임워크, 정보보호 관리 기술, 사이버보안, 기술적인 방법에 의한 스팸 대응, 응용서비스 보안, 텔레바이오인식 기술, 아이덴티티 관리 및 메커니즘 등의 정보통신 언어 등 정보보호 분야 연구를 수행

SG17 WP		TITLE
WP 1	-	**Security strategy and coordination**
WP 2	-	**5G, IoT and ITS security**
WP 3	-	**Cybersecurity and management**
WP 4	-	**Service and application security**
WP 5	-	**Fundamental security technologies**
	Q1	Security standardization strategy and coordination
	Q2	Security architecture and network security
	Q3	Telecommunication information security management and security services
	Q4	**Cybersecurity and countering spam**
	Q6	Security for telecommunication services and Internet of Things (IoT)
	Q7	Secure application services
	Q8	Cloud computing and big data infrastructure security
	Q10	Identity management and telebiometrics architecture and mechanisms
	Q11	Generic technologies (such as Directory, PKI, formal languages, object identifiers) to support secure applications
	Q13	Intelligent transport system (ITS) security
	Q14	Distributed ledger technology (DLT) security
	Q15	Security for/by emerging technologies including quantum-based security

기고문 작성과 연계된 표준 특허 확보 전략 수립



» 표준 특허 확보를 위한 전략업무 진행

- ➔ NWIP 작성 및 제안발표가 임박한 시점을 감안하여, 기고문 작성에 참고가 될 수 있는 표준 관점에서의 경쟁사 선정
- ➔ 기술내용별 특허동향 분석과, 주요 경쟁사 보유 특허 분석을 우선적으로 수행
- ➔ 제안 예정인 표준기술 중 기업 고유의 차별화된 솔루션과 연관된 핵심 특허 분석을 진행
- ➔ 차별화된 솔루션들의 경우, 기고문 작성에 최대한 반영하여, 표준 특허 창출의 SEED로 활용

ITU-T T22-SG17-C-0021_MSW-E 최종 기고문

INTERNATIONAL TELECOMMUNICATION UNION
TELECOMMUNICATION STANDARDIZATION SECTOR
STUDY PERIOD 2022-2024

SG17-C021
STUDY GROUP 17
Original: English

Question(s): 4/17 — Virtual, 10-20 May 2022

CONTRIBUTION

Source: Korea (Republic of)

Title: Proposal for new work item: Security requirements and countermeasures for targeted email attacks

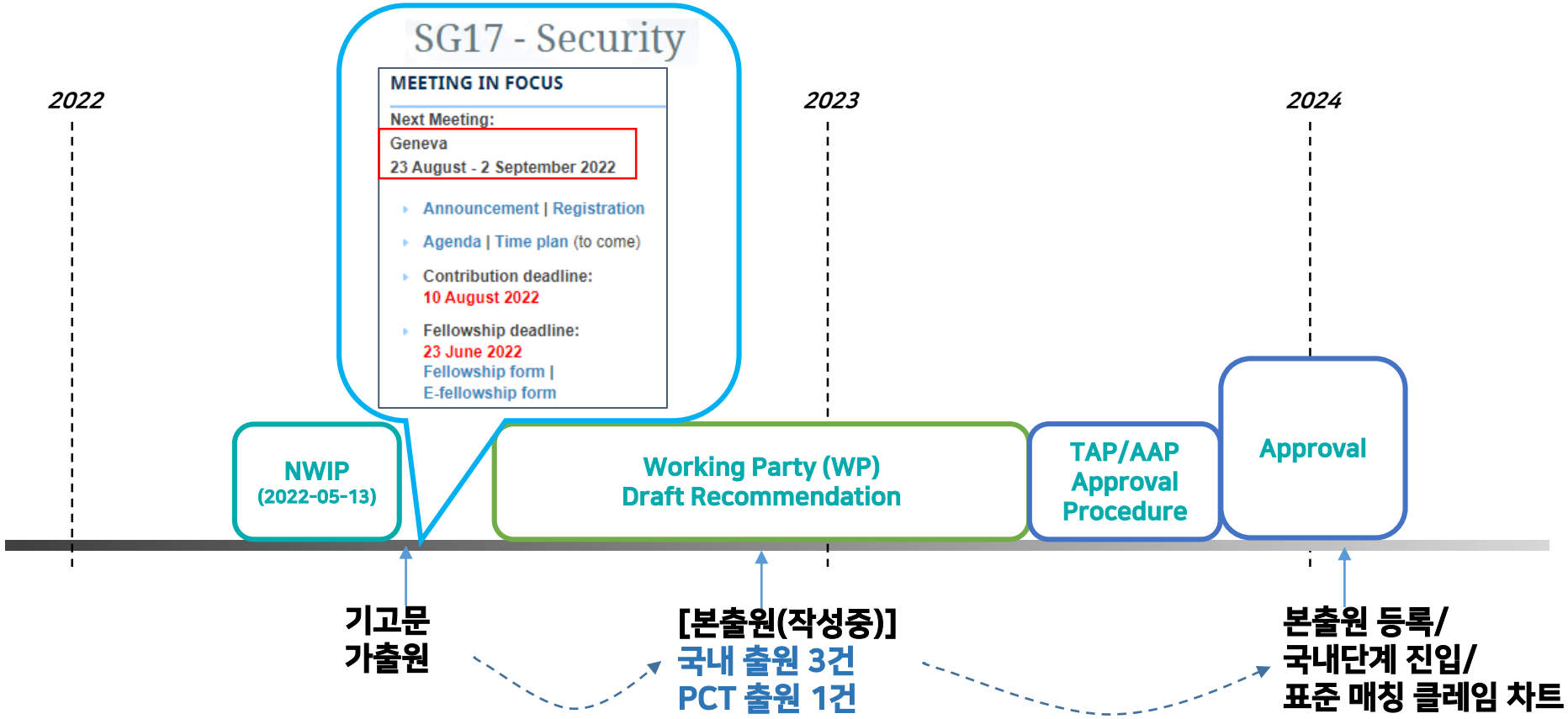
Contact: Chunghan Kim, KIWONTECH, Korea (Republic of) — Tel: +82-10-4183-5574, Fax: +82-2-6085-4330, E-mail: KevinKim@kiwontech.com

Contact: Jonghyun Kim, ETRI, Korea (Republic of) — E-mail: jhk@etri.re.kr

Contact: Sujung Park, TTA, Korea (Republic of) — Tel: +82-10-5110-5098, Fax: +82-31-724-0109, E-mail: sjpark@tta.or.kr

Abstract: This contribution proposes a new work item on "Security requirements to counter targeted email attacks" for consideration by Q4/17. It introduces the definitions of targeted email attacks, and security requirements and countermeasures to block targeted email attacks.

향후 표준화 과정과 연계된 해외출원 전략 수립



➔차기 기고문 준비와 연계하여, 표준화 아이템 창출 및 본출원 진행

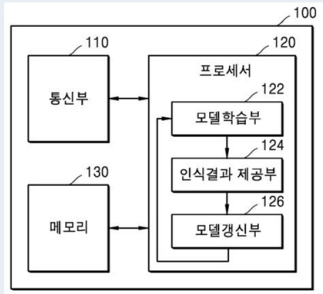
➔각 기고/발표 시점과 표준 진행화 정도를 고려하여, 기고/표준화 진행 내용에 대한 출원 및 권리화 예정

➔PCT 출원의 경우 진입 마감 2개월 전, WP Draft 최신버전을 참고한 Cliam 매칭검토 후 진입국가 결정

보유 기술의 국제표준 매칭전략 수립 및 반영

인공지능 기반의 메일 관리 방법 및 장치(The mail management method of the artificial intelligence base and apparatus thereof)			
국가	KR	문헌종류	B1
문헌번호	10-2247617 B1(2021.04.27)	출원번호	10-2019-7029159(2019.08.07)
출원인	(주)기원테크	패밀리	WO2021-025023A1, SG11201909530S
요약	본 개시의 일 실시예에 따라, 사용자 정보 및 사용자 계정 별로 수신된 악성 메일 정보를 획득하고, 사용자 정보 및 상기 악성 메일 정보를 기초로, 기 생성된 인공지능 모델에 사용자 계정 별로 수신된 악성 메일의 특성을 학습시키며, 특정 사용자의 계정을 상기 **학습된 인공지능 모델에 입력**하여, **특정 사용자가 수신할 수 있는 악성 메일의 유형에 관한 진단 정보를 제공**하는 인공지능 기반의 메일 관리 방법이 개시된다.		
대표청구항	사용자 정보 및 사용자 계정 별로 수신된 악성 메일 정보를 획득하는 단계; 상기 사용자 정보 및 상기 악성 메일 정보를 기초로, 기 생성된 인공지능 모델에 사용자 계정 별로 수신된 악성 메일의 특성을 **학습시키는 단계**; 및 특정 사용자의 계정을 상기 학습된 인공지능 모델에 입력하여, 상기 특정 사용자가 수신할 수 있는 악성 메일의 유형에 관한 진단 정보 - 상기 진단 정보는 **복수의 악성 메일의 유형을 수신할 수 있는 확률 또는 비율을 포함한 통계 정보**임 - 를 제공하는 단계를 포함하고, 상기 제공된 진단 정보에 따른 악성 메일의 유형과 사용자 계정에 실제 수신된 악성 메일의 유형을 비교하는 단계; 및 상기 비교 결과에 기초하여, 상기 인공지능 모델에 포함된 파라미터를 업데이트 하는 단계를 더 포함하는, 인공지능 기반의 메일 관리 방법.		

[대표도]



매칭 포인트

➔ **악성 메일의 유형**을 사회공학적 공격 유형(S-type) 에 매칭시킬 수 있음

➔ 메일 주소 사칭, 유사 도메인 공격의 유형(type)을 판단함에 있어서, **그 확률 또는 비율에 대한 통계 정보를 제공하고, 이를 이용한 인공지능 모델 학습**이 이루어지도록 하는 구성을 필수 또는 예시기술로서 제안할 수 있음

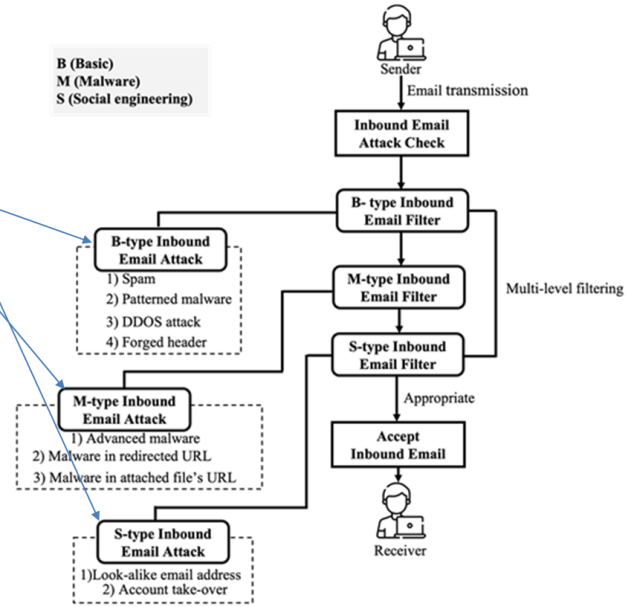
[보유 특허 매칭가능성 검토 기반 기고문 전략 수립]

[0117] 최상위 카테고리 중 하나인 상기 수신메일은 하위 계층으로 보안위협 유형이 구분될 수 있다. 세부적으로, 상기 보안위협 유형은 SPAM 처리, 악성코드 처리, 사회공학적 처리 등으로 구분될 수 있다.

[0118] 수신메일의 보안위협 검사를 위해 SPAM 처리 부문 내 레벨 1(Lv.1)은 평판 기반으로의 스팸메일 여부를 검사할 수 있다. 이 후, 평판 기반의 스팸메일 검사에서 발견된 문제점이 없는 경우 레벨 2(Lv.2)은 사용자 지정 키워드에 근거하여 필터링을 통한 스팸메일 여부를 검사할 수 있다.

[0119] 레벨 2의 수행이 완료된 후, 다음 단계인 레벨 3(Lv.3)은 이미지 기반의 내용 분석을 통한 스팸메일 여부를 검사할 수 있다. 이와 같이, 메일보안 서비스 아키텍처는 SPAM 처리 유형 내에서의 특정 스팸필터링 프로세스를 통해 레벨별 검증을 수행하고, 상기 검증이 완료될 시 다음 레벨로 이행될 수 있도록 한다. 그리고 상기 메일보안 서비스 아키텍처는 SPAM 처리를 통한 메일의 스팸여부 검사를 완료한 후, 메일 내 악성코드 포함 여부를 판별하는 악성코드 처리 단계로 이행될 수 있다.

➔ **단계적 매칭에 따른 표준 매칭 가능성 존재**
➔ **레벨=타입에 대응**



[출원 중인 특허의 매칭 보정 진행➔등록완료]

기원테크 국제 표준화 및 표준 특허 확보전략 진행내용 요약

(1) 표준 관점에서의 보유 특허 분석 및 진단
➔ TTA 확정 표준안 대비 표준 매칭가능성 검토 기반
➔ 보유 특허에 기초한 특허 포트폴리오 전략, PCT 국내단계 진입 타임라인 수립

(2) 표준 특허 기술 동향 분석
➔ 표준화 아이템 기반 검색 테크트리를 설정
➔ 표준 기술요소에 따라 연도별, 기술별, 주요 특허별 종합적 특허기반 기술동향 분석 수행

(3) 표준 특허 경쟁사 분석
➔ 표준화 과정에서의 경쟁사로서 인지되는 특허기반의 경쟁사 확인
➔ 표준 특허 관점에서의 경쟁사 보유 특허 및 출원동향, 매칭가능성 검토

(4) 국제 표준화 DRAFT를 위한 선행특허조사분석
➔ DRAFT에 부가될 신규 요소를 중심으로 하는 선행특허조사 및 침해/등록 위험성 분석
➔ 특허성이 높은 요소를 기반으로 하는 Spec 기재사항, 우선순위 선정

(5) 기고문 분석 및 작성
➔ 유사 분야 관련 제안된 기고문/표준문서의 수집, 조사, 기술분석자료 검토
➔ 선행 특허 및 기고문을 고려한 DRAFT 수행

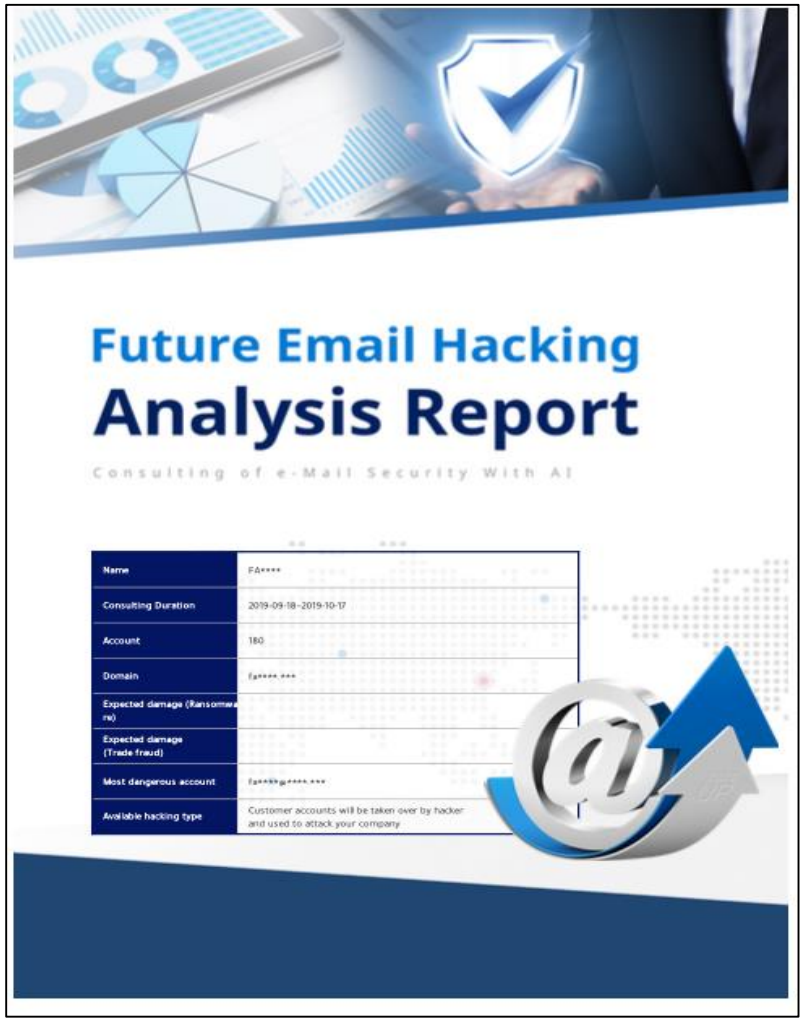
(6) 신규 특허 출원 아이템 도출 및 명세서 작성
➔ 국제표준화 제안서 내용 및 신규 아이템의 특허성 검토하여 출원아이템 도출, 명세서 작성

표준 특허 성과

ICT Standards

- 이메일 보안 진단 신규 사업 런칭
- All-in-one 이메일 보안 솔루션 근간 기술 보호
- License BM 인프라 구축
- 17억 투자유치 완료
- 특허 출원 정보

이메일 보안 진단 신규 사업 런칭



All-in-one 이메일 보안 솔루션 근간 기술 보호

국내 유일 이메일 보안 전 구간 자체 개발 기술 보유

기술에 대한 표준 특허 개발로 인해 경쟁사의 침해여지 차단

스팸메일 보안구간	메일APT 보안구간	메일서비스 구간	발신메일 보안구간
광고성 스팸메일, 대량메일 공격 차단	바이러스/URL 및 위·변조 메일 차단	사용자가 수신된 메일을 확인하고, 메일을 발신하는 구간	발신메일 필터링 및 모니터링
SpamGUARD	**ReceiveGUARD**	**SECUMAIL**	**SendGUARD**
학습형 스팸 필터링	APT 사기메일 차단	자체 개발 메일 엔진	기업정보 유출방지 수/발신 데이터 동기화 솔루션

License BM 인프라 구축

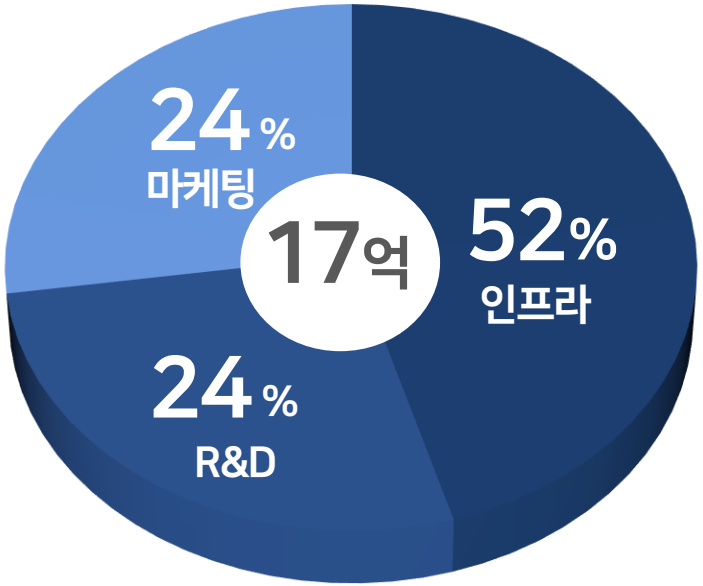
EG-CLOUD Price Policy

(Price : USD $)

Service Model	Minimum Number of Accounts	Size(number of people) of the Enterprise	Customer Price per Account (monthly)
EG 3 Package	3	3 or more to 10 or less	USD 2
EG 5 Package	5	Over 10 or more to 15 or less	USD 1.7
EG 10 Package	10	Over 15 or more to 25 or less	USD 1.5
EG 15 Package	15	Over 25 or more to 35 or less	USD 1.2
EG 20 Package	20	Over 35 or more to 50 or less	USD 1
EG 30 Package	30	Over 50 or more to 70 or less	USD 0.8
EG 40 Package	40	Over 70 or more to 100 or less	USD 0.7
EG 80 Package	80	Over 100 or more to 200 or less	USD 0.5

※ The minimum number of accounts should comply when proceeding with a contract

스케일업 벤처스 시리즈 A 17억 투자유치 완료



이메일 보안 진단 검사 장비 구매 및 운영 인프라 확대를 위한 서버 구매 50(대)

9억

30(대) 메일서버 보유 기업 사내 구축형 진단 활용
20(대) 자사 데이터센터에 CLOUD 서비스로 활용

이메일 보안 진단 솔루션 고도화

4억

정보유출 유형 위험 진단 / 금융사기 유형 위험 진단 / 전산마비 유형 위험 진단
V3, 알약의 이메일 버전 소프트웨어 개발

이메일 보안 진단 검사 홍보 및 마케팅을 위한 국내외 영업비용

4억

표준 이메일 보안기술 정보, 보안진단 프로모션을 위한 유튜브 등 온라인 마케팅
이메일 보안 진단 검사 결과를 활용할 영업 인력 확보
보안학회, 전시회 등 오프라인 마케팅

특허 출원 정보

		구	발명의 명칭	출원번호	출원일	출원인	등록번호	등록일	
14	KR	등록	보안 레벨 기반의 계층적 아키텍처를 이용한 이메일 보안 서비스 제공 장치 및 그 동작 방법	10-2020-0180096	20				39)
15	PCT	출원	보안 레벨 기반의 계층적 아키텍처를 이용한 이메일 보안 서비스 제공 장치 및 그 동작 방법	PCT/KR2021/006395	20				102-
16	PCT	출원	메일 보안 기반의 제로데이 URL 공격 방어 서비스 제공 장치 및 그 동작 방법	PCT/KR2020/019256	20				137-
17	KR	출원	메일 보안 기반의 제로데이 URL 공격 방어 서비스 제공 장치 및 그 동작 방법	10-2021-7025415	20				002)
18	PCT	출원	폴더 보호 기능을 제공하는 보안 장비 시스템의 구동 장치 및 그 동작 방법	PCT/KR2021/009940	20				106-
19	KR	출원	폴더 보호 기능을 제공하는 보안 장비 시스템의 구동 장치 및 그 동작 방법	10-2021-7025416	20				003)
20	PCT	국제출원	인공지능 기반의 메일 관리 방법 및 장치	PCT/KR2019/009870	20				
21	US	개국출원	인공지능 기반의 메일 관리 방법 및 장치	16/499212	20				
22	SG	개국출원	인공지능 기반의 메일 관리 방법 및 장치	11201909530S	20				
23	JP	등록	인공지능 기반의 메일 관리 방법 및 장치	2019-556265	20				
24	VN	개국출원	인공지능 기반의 메일 관리 방법 및 장치	1-2019-05680	20				
25	MZ	개국출원	인공지능 기반의 메일 관리 방법 및 장치	PI2020005654	20				
26	KR	출원	내부망 분리 보안 네트워크에서의 내부망 대용량 파일 첨부 메일을 외부 네트워크로 안전하게 전송하기 위한 메일 변환 처리 장치 및 그 동작 방법	10-2022-0052826	20				92)
27	KR	출원	내부망 분리 보안 네트워크에서의 내부망 대용량 파일 첨부 메일을 외부 네트워크로 안전하게 전송하기 위한 메일 복원 처리 장치 및 그 동작 방법	10-2022-0052827	20				93)
28	KR	출원	이메일 통신 프로토콜 기반 접속 관리 및 차단 기능을 제공하는 메일 접속 보안 시스템의 메일 보안 처리 장치 및 그 동작 방법	10-2022-0091025	20				80)
29	KR	출원	표적형 이메일 공격 차단을 위한 보안 시스템	10-2022-0097174	20				34)
30	KR	출원	보안 레벨 기반의 계층적 아키텍처를 이용한 이메일 보안 서비스 제공 장치 및 그 동작 방법	10-2022-0128975	20				D1)

Thank you

김충한 팀장, ㈜기원테크
Kevinkim@kiwontech.com