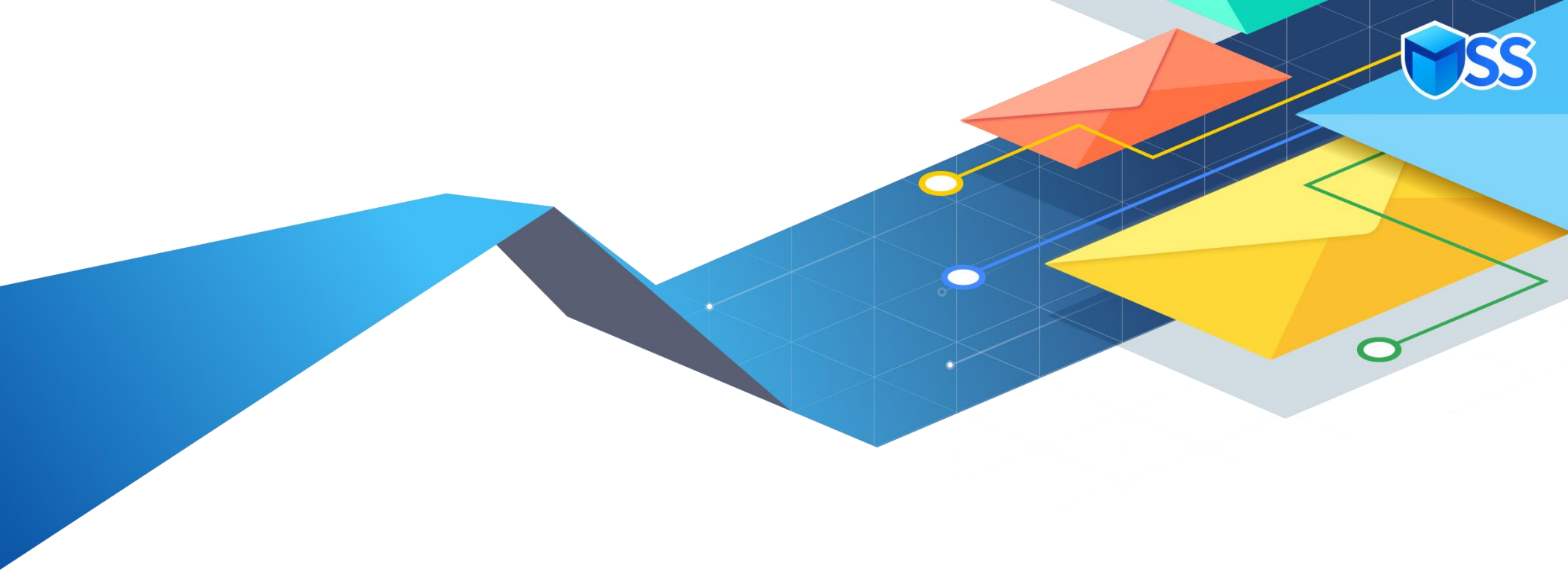
MSS
Mail Secure Server

MSS
ALL TIME PROTECTION

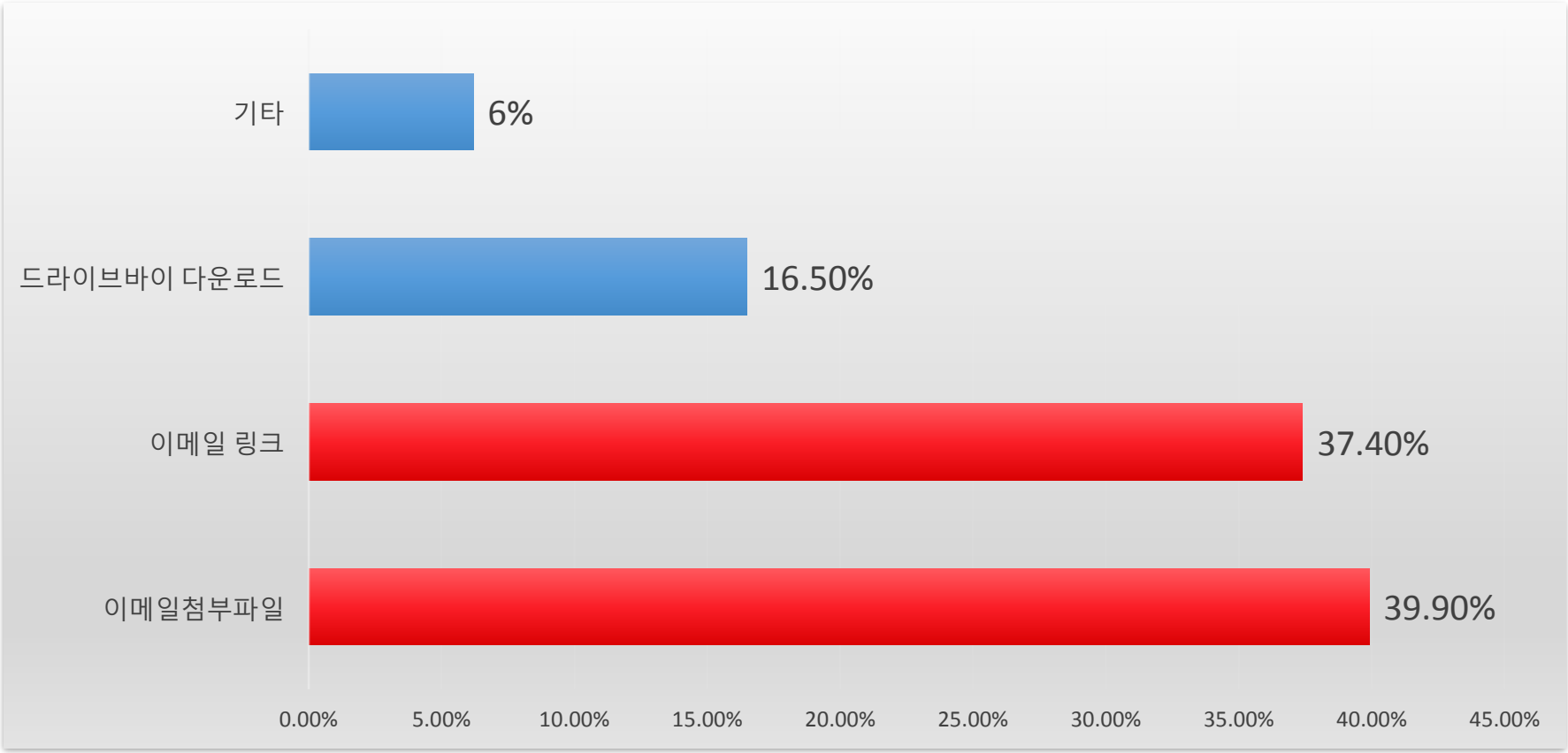
통합 메일 보안 및 메일 연계 솔루션

리투인 소프트웨어



1. 메일 보안 현황

사이버 공격 주요 경로(2018년)



대표적 메일 보안 사고 사례

2019년 지방에서 랜섬웨어 활개, 무역 거래 시 메일 내 계좌번호 해킹

2018년 12월 [단독]이번엔 국방위원 사칭… 해킹메일 무더기 유포 [출처:동아일보]

2018년 10월 [긴급]한국 정부 메일포함 1만7천여개 메일주소 / 비밀번호 유출

2018년 6월 암호화폐 해킹, 고전적인 e메일 악성코드 수법에 당했다. [출처:중앙일보]

2018년 6월

온라인 숙박 예약 업체 '여기OO' 개인정보 유출사고

웹 호스팅 업체 '나OO' 랜섬웨어 공격, 해커 비용 지불

2018년 5월

저렴한 몸값, 0.1 비트코인(당시 약 18만원) 요구하는 랜섬웨어

경찰서 사칭 '과태료 고지서' 메일 랜섬웨어 - eFINE을 사칭한 메일

2017년 4월

대선관련 해킹메일 - 당시 문OO 후보 캠프

인터넷 쇼핑몰 '인터OO' 고객정보 리스트 사칭한 랜섬웨어

웹포털 사이트 '네OO' 도메인 탈취(파밍), 금감원 사칭

금융악성 코드 드리덱스, 북한의심, 보안 프로그램의 탐지 무력화

메일을 통한 APT공격/해킹 증가

메일 본문
첨부 파일
외부 링크
실시간 통제 중요성 증가

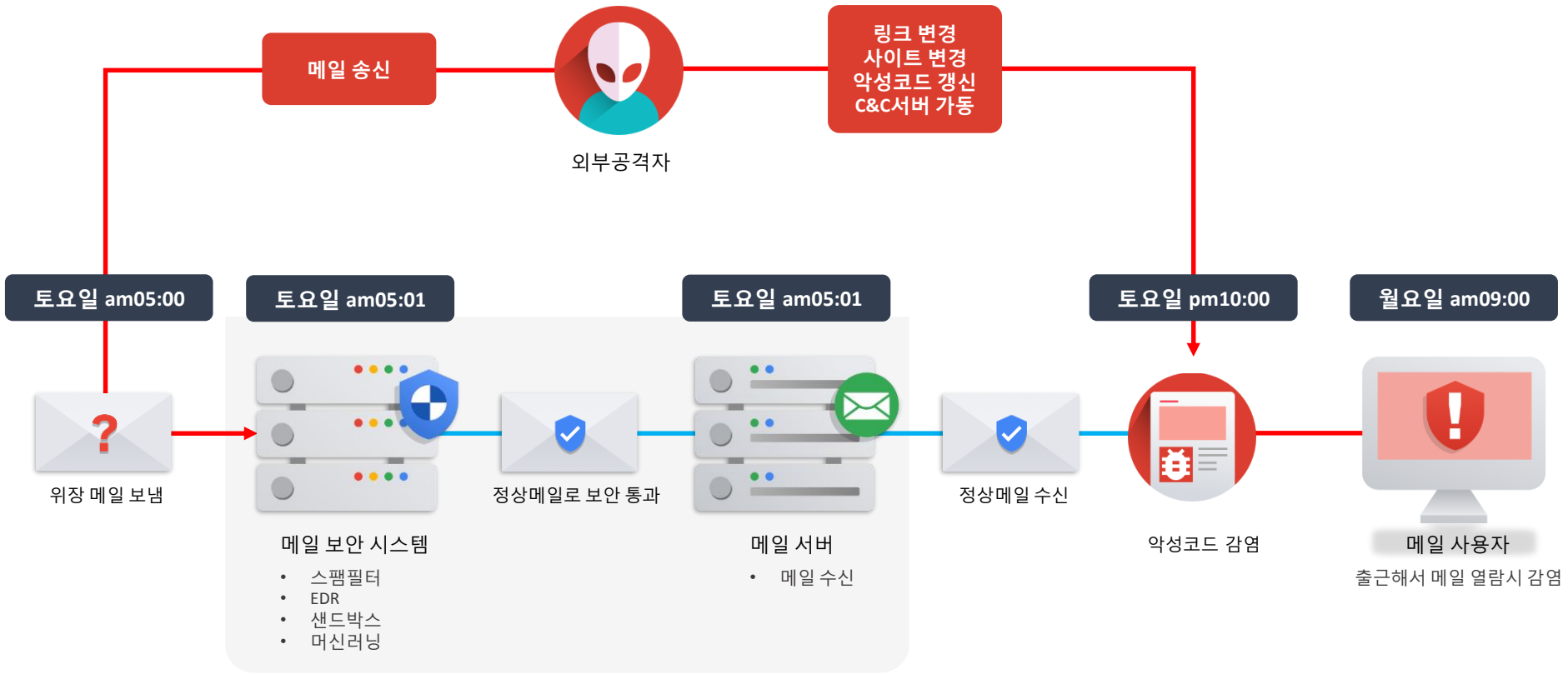
기존 메일 보안솔루션의 한계

메일 수신시에만 검사

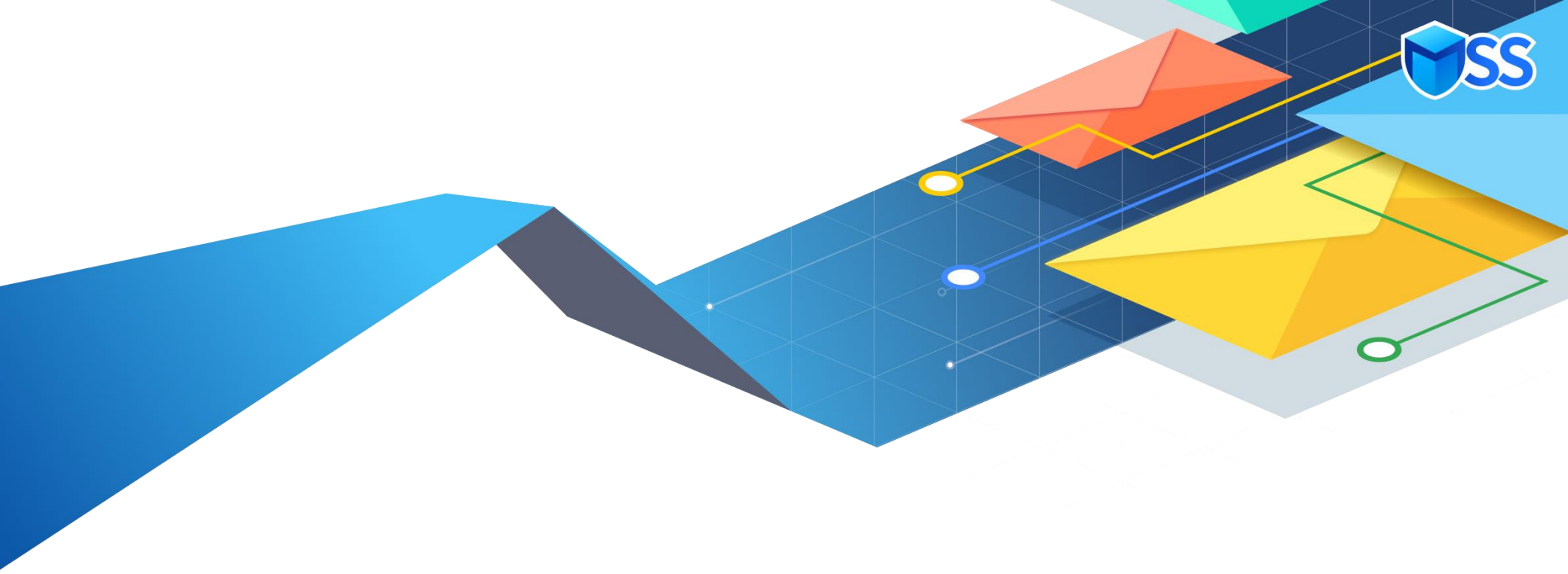
메일 수신이후에는 어떻게?
Zero Day, Unknown 공격은?

- 기존 메일 보안 솔루션은 메일 수신 시점에만 보안 검사를 실행하는 것이 가장 큰 한계이자 문제점 입니다.
- 수신 시점에만 보안검사를 하는 것 만으로 이메일을 신뢰하고 사용할 수 있을지 의문을 가질 수 밖에 없습니다.

지능화 되어 가는 공격기법



- 최근 해커들의 공격 방식은 다양한 메일 보안시스템의 허점을 이용하는 레벨까지 발전했습니다.
- 예를 들어 샌드박스 등의 가상환경이라고 인식되면 공격 행위를 진행하지 않는 변조 케이스가 발견되고 있습니다.
- 특히 수신 시점이 지나고 나서 메일에 포함된 컨텐츠를 공격하는 형태의 변종 기법 공격 패턴이 늘어나고 있습니다.



2. MSS 주요 특징

MSS 아키텍처 – International Airport

허브공항	MSS시스템
착륙	랜딩
도착 터미널	수신터미널
이륙	송신
입국	저장
화물	파일
보안	보안
관제탑	대시보드

- 모든 메일은 단순한 파일 배송시스템이 아닙니다, 메일은 저마다 다양한 의도를 가지고 출발하며, 도착합니다.
- 메일의 수신(착륙) – 보안 송신(갈아타기, 입국)으로 이어지는 경로를 구성할 수 있는 통합 메일 보안 플랫폼
- 메일 보안이란 메일의 화물검사(첨부파일) 뿐만 아니라 메일의 출발 의도, 도착지를 실시간으로 파악할 수 있어야 합니다.

MSS 위협메일 차단 솔루션

MSS는 메일과 관련된 모든 보안기능을 제공하는 통합 메일 보안 플랫폼 입니다.

01 All Time Protection

- 메일 클릭 시 실시간 보안검사
- 보안Proxy 서버, Web서버, 이미지 캐싱
- 외부링크, 첨부파일 클릭 시 마다 보안검사
- 관련 특허보유

02 스팸필터

- RBL(Internet-Based Real Time Blacklists)
- 스팸/스캠 메일 차단

03 안티바이러스

- ClamAV
- VirusChaser
- Kaspersky 지원
- 자체 검출 패턴

04 메일 분해 후 보안조치

- 메일을 분해하여 유해요소 제거 후 재조립
- 본문. 첨부파일, 이미지 등 MSS 서버 주소로 변환 후 단계별 보안조치
- 수신 메일의 이미지 캐싱 서버 기능 제공

05 CDR(파일무해화)

- 메일 첨부파일 전용 CDR
- HWP, MS오피스, PDF, 이미지 등 지원
- CDR 검출 / 위험 콘텐츠 제거 / 변환
- 첨부파일 내 알려진 피싱 링크 추적 삭제
- 본문, 첨부파일 유해요소 CDR 차단 기능
- 첨부파일 CDR 변환 기능

(변환파일 제공 - 옵션)

06 Sandbox

- 가상머신내 실행 후 행위탐지
- 첨부파일 이상 행위 탐지
- **옵션 제공**

07 메일 연계

- 망분리 환경에서 외부메일을 내부PC 원본형태로 볼 수 있는 유일한 솔루션
- 관련 특허 보유

08 대용량 첨부파일 다운로드

- 망 분리 환경에서 NAVER, Daum 등 포탈 사이트에서 첨부된 대용량 링크 파일을 업무 PC에서 다운로드 기능 제공

09 메일 서버 기능

- SSL TLS 기반의 POP3 메일 서버 기능 제공

10 자료전송 기능

- 메일을 통한 자료전송 기능 제공
- 대용량 파일의 경우 링크를 통한 수신기능 지원

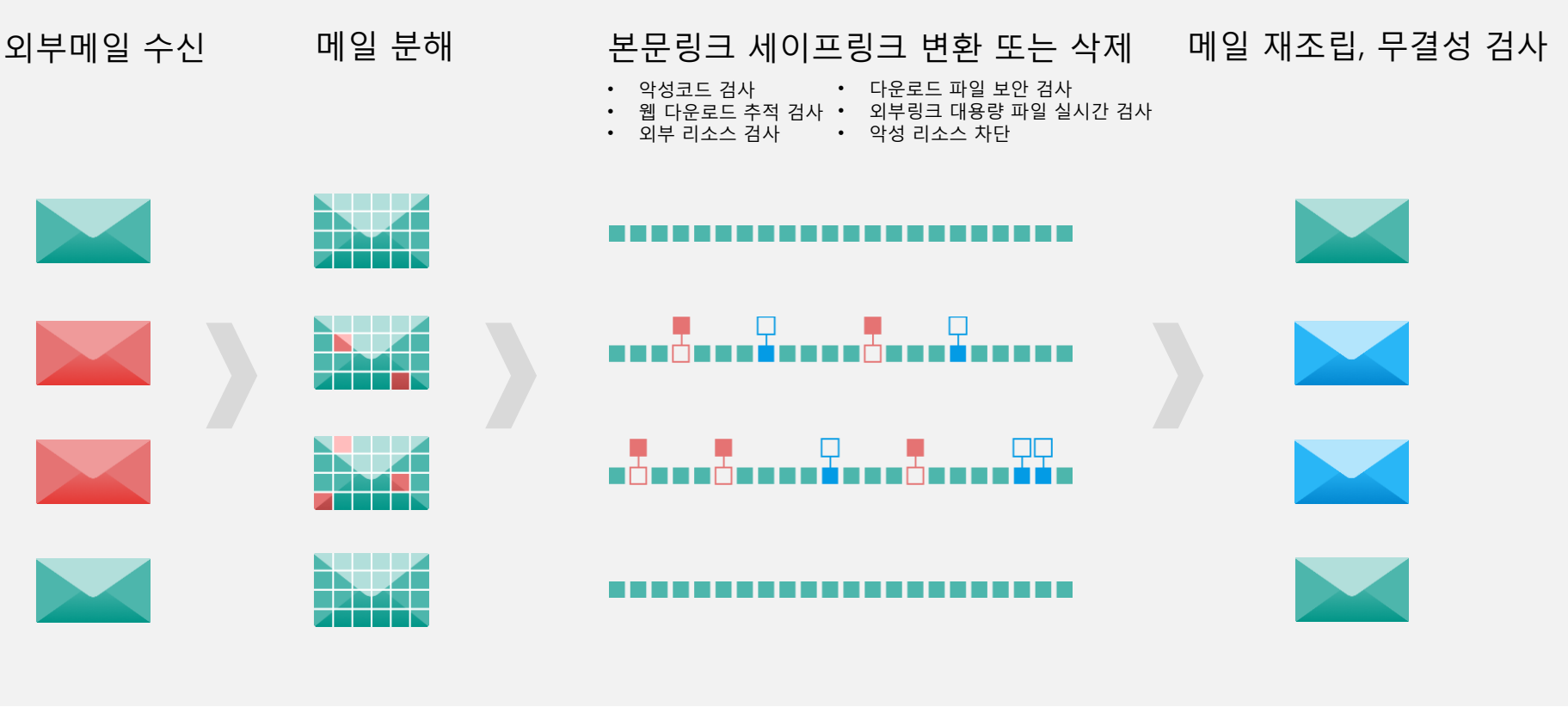
11 개인정보 필터

- 발송 메일 본문의 개인정보 및 첨부파일에 대한 개인정보 필터 기능 제공 (커스텀 패턴 추가 가능)

12 메일 승인/반출

- 첨부파일이 있거나 개인정보가 포함된 내용 발송 시 승인을 통한 외부 발송 기능 제공

MSS 메일 위협요소 제거



- MSS는 메일을 분해/분석/재조립할 수 있는 특허기술을 국내 외 유일하게 보유한 솔루션 입니다.
- 1단계 처리 : MSS 서버 주소 치환 또는 링크 삭제 (첨부파일, 하이퍼링크, 이미지 등) / MSS 서버 설정정책 기준 필터링 / 악성코드 검사 / 파일 위 변조 검사 등

  (첨부파일의 압축파일에 암호가 설정된 경우 암호 추적 후 검사 기능 제공 – 모든 압축포맷 지원)
- 2단계 처리 : ALL TIME PROTECTION : URL 피싱 사이트 및 URL 추적 검사
- 3단계 처리 : CDR 파일 무해화 / 샌드박스 (첨부파일 이상행위 탐지)

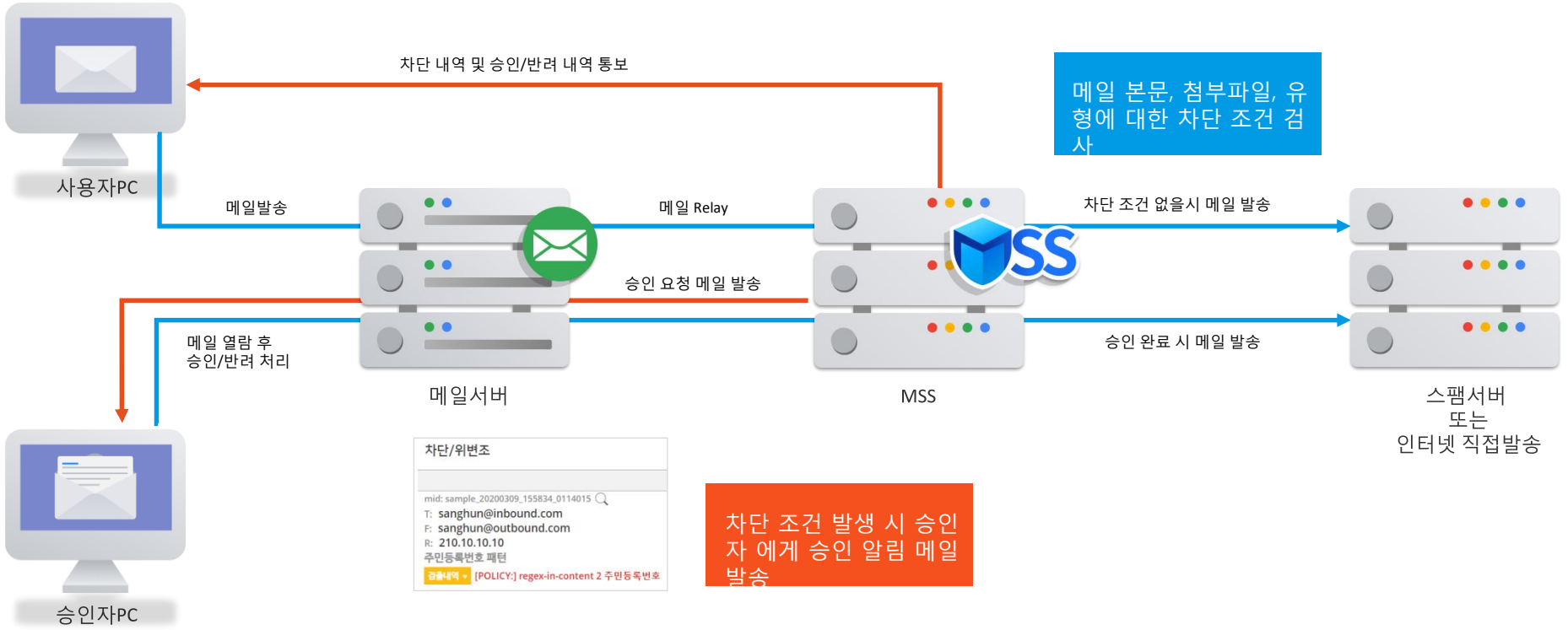
메일 분해·재조립

MSS는 메일을 분해, 유해요소를 완전히 제거 후 재조립 하여 안전한 메일을 제공합니다.

- 메일을 분해 및 보안처리 (분해 → 보안처리 → 재조립)하여, 안전한 메일을 사용자에게 제공.
  - 분　해 : 메일 헤더, 본문 분해 (텍스트 파일로 전환), 본문 내 이미지 파일, 첨부파일 분해
  - 재 조립 : 원본 메일의 내용 손실 없이 동일하게 재 조립
- 보안 처리
  - 메일 본문 텍스트 및 이미지 재 조립 : 외부 EML 태그 제거, 유해 태그 제거, 악성코드 및 취약점 공격 대응에 따른 보안 처리
- 외부 링크 / 이미지 / 첨부 파일 보안 검사 및 MSS 서버주소로 치환

개인정보 필터 및 다양한 조건의 발송 메일 차단 및 승인기능

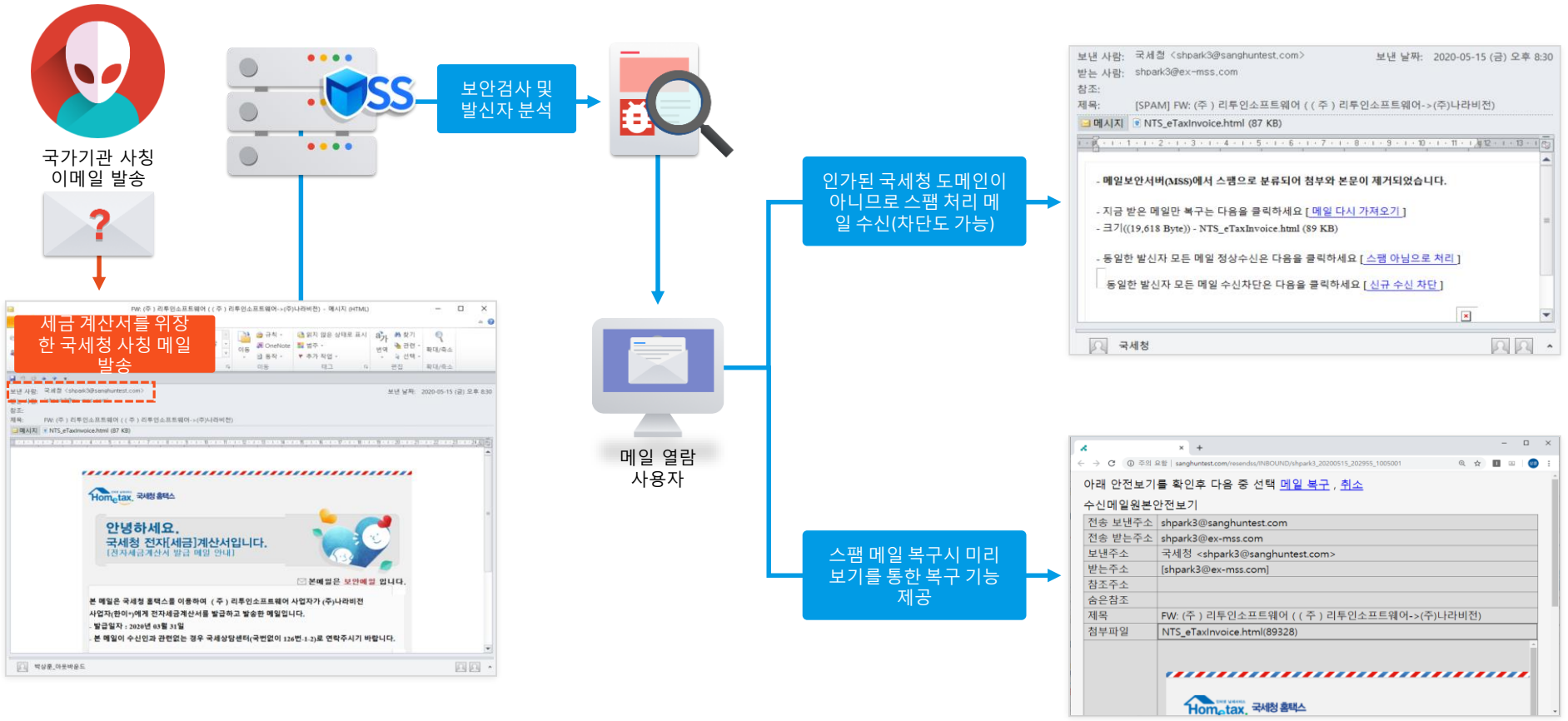
MSS는 발송되는 메일의 개인정보 필터 기능 및 메일 반출 승인 기능을 제공 합니다.



- 외부 발송 메일의 개인정보 탐지 및 차단 : 주민등록번호, 계좌번호, 카드 번호 등 주요 개인정보 및 고객사의 주요 커스텀 정보를 등록하여 메일 본문의 개인정보 및 주요정보의 외부 발송 차단 기능 지원 (첨부파일 : 텍스트, 오피스, 한글파일 등 주요 문서파일 지원) – 유형 및 임계치 설정 기능 제공
- 첨부파일 암호화 발송 : 외부로 발송되는 첨부파일을 압축 및 암호화하여 발송하는 기능 제공
- 그 외 발송하지 말아야 할 수신자 및 첨부파일 개수 등 패턴 등록을 통한 필터 및 차단 기능 제공
- 차단 조건 메일에 대한 별도의 승인 후 발송 기능 제공

메일 헤더 분석을 통한 사칭 메일 차단

MSS는 수신 메일의 헤더를 분석하여 국가기관 사칭 이메일을 차단합니다.

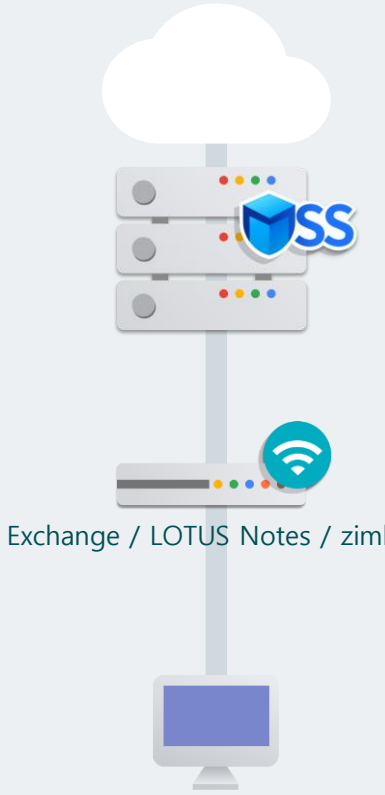


- 스팸 솔루션에서 제공 되는 RBL 리스트를 통한 메일 도메인 확인과 SPF, DKIM, DMARC 등의 일반적인 발신메일의 변조 유무 확인 기능을 포함하여 스팸 점수 설정,

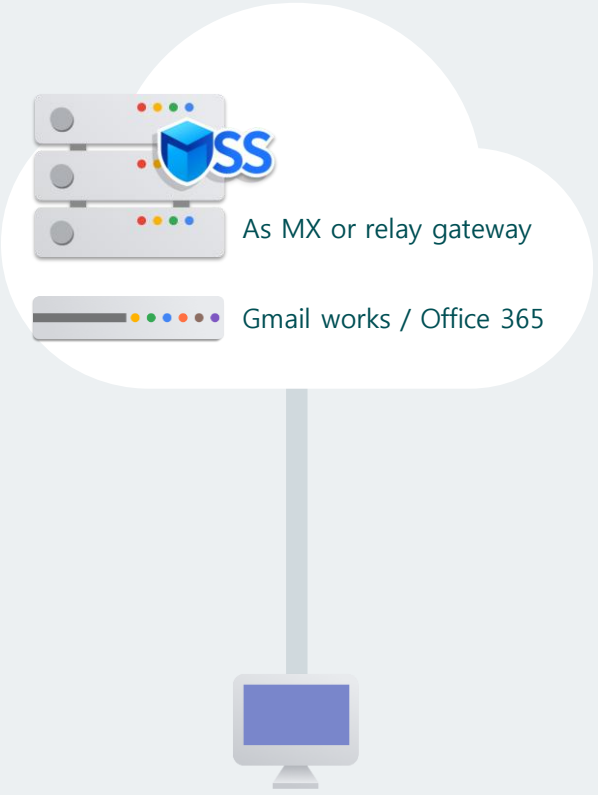
  스팸 경고 점수 설정, 스팸 메일 수신에 따른 다양한 복구 정책 (스팸 메일 수신 시 메일 차단, 본문 제거, 메일 미리 보기 후 복구) 기능을 제공합니다.
- Machine Learning 을 통한 자동 학습 및 수신 되는 메일의 헤더를 분석하여 발신자 위 변조, 국가 기관 사칭 이메일을 차단합니다.

MSS 구성 방안

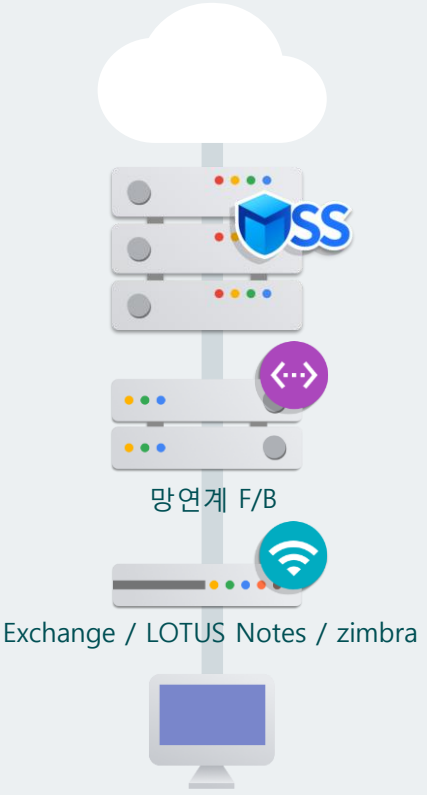
일반환경



클라우드 환경



망분리 환경



- MSS는 일반적인 메일 환경 / 망분리 환경 / 클라우드 환경 모두에 적용이 가능합니다.
- 현재 사용중인 메일 제품에 대한 호환성 및 가독성을 보장합니다.
- 엔드포인트 / PC / 모바일 운영서버 어디에도 추가로 설치되는 에이전트 등이 필요 없습니다.

시스템 다중화

DBMS 없는 자체적인 시스템 다중화 구성으로 인한 확장성을 보장합니다.

정상데이터만 동기화

수신원본 / 외부리소스 / 정책생성시

해시키 인증기반 데이터 복제

이중화 이상의 성능 확장

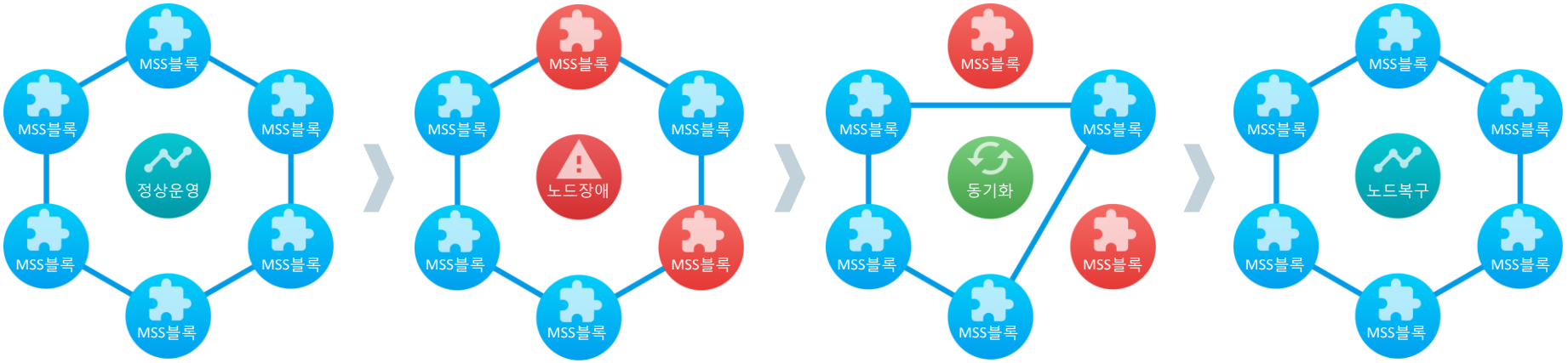
대규모 포털 메일과 동일 성능 제공

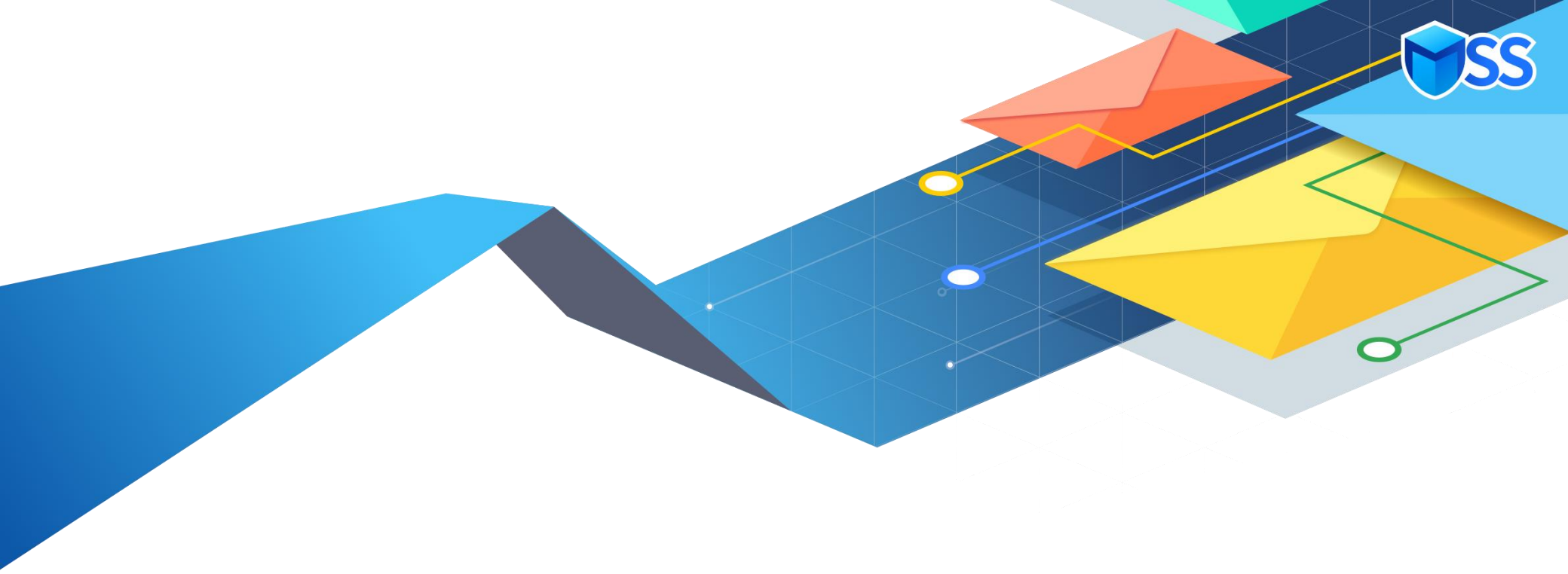
자체적인 로드밸런싱 제공

관리자 개입 최소화

장애 노드 자동 복구

복구 시 누락된 데이터만 동기화

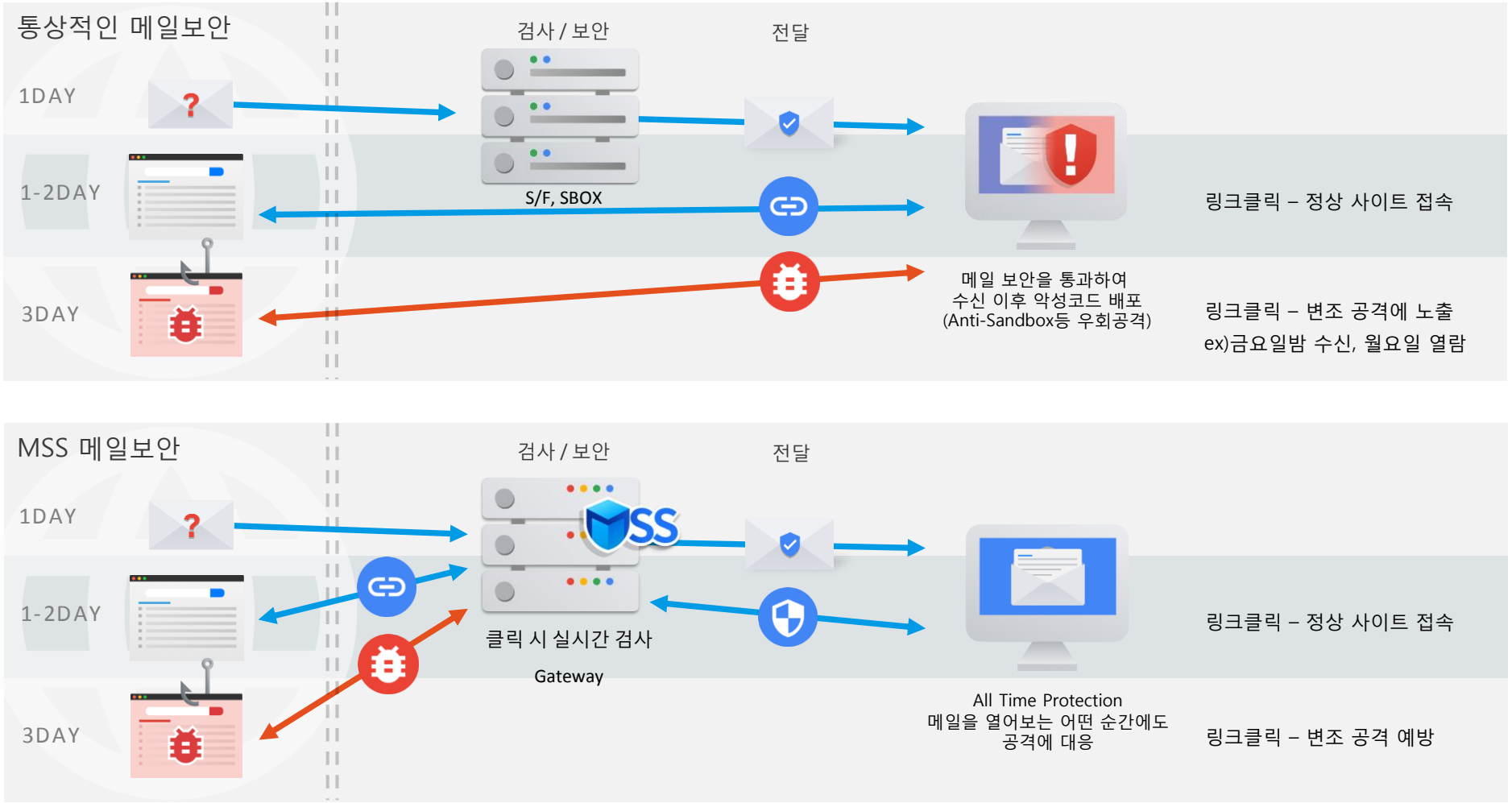




3. MSS ATP (All Time Protection)

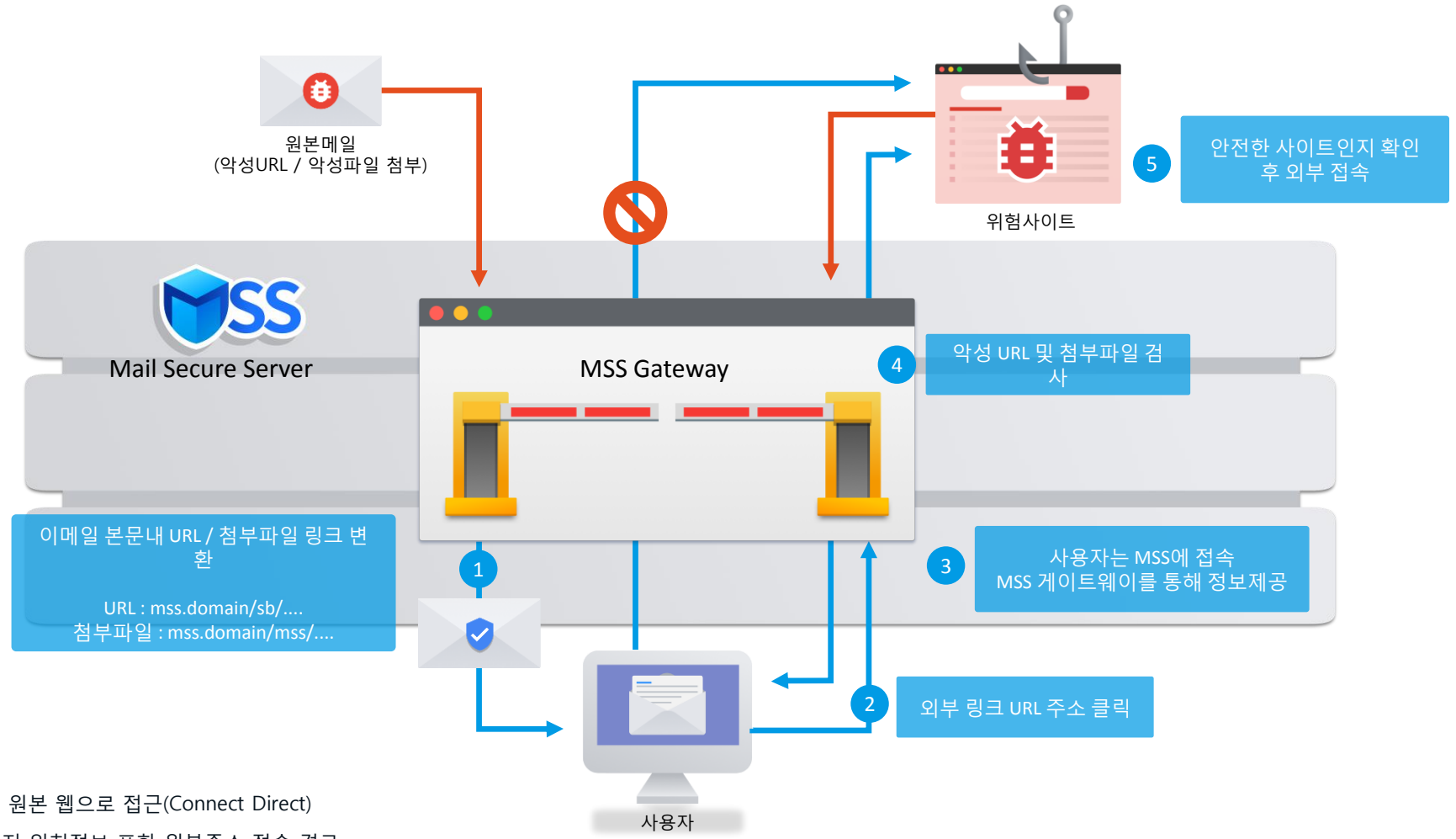
All Time Protection

MSS는 메일을 실시간(클릭할 때 마다) 검사하여 APT공격에 대응하는 유일한 솔루션 입니다.



외부링크 보안 검사 및 조치

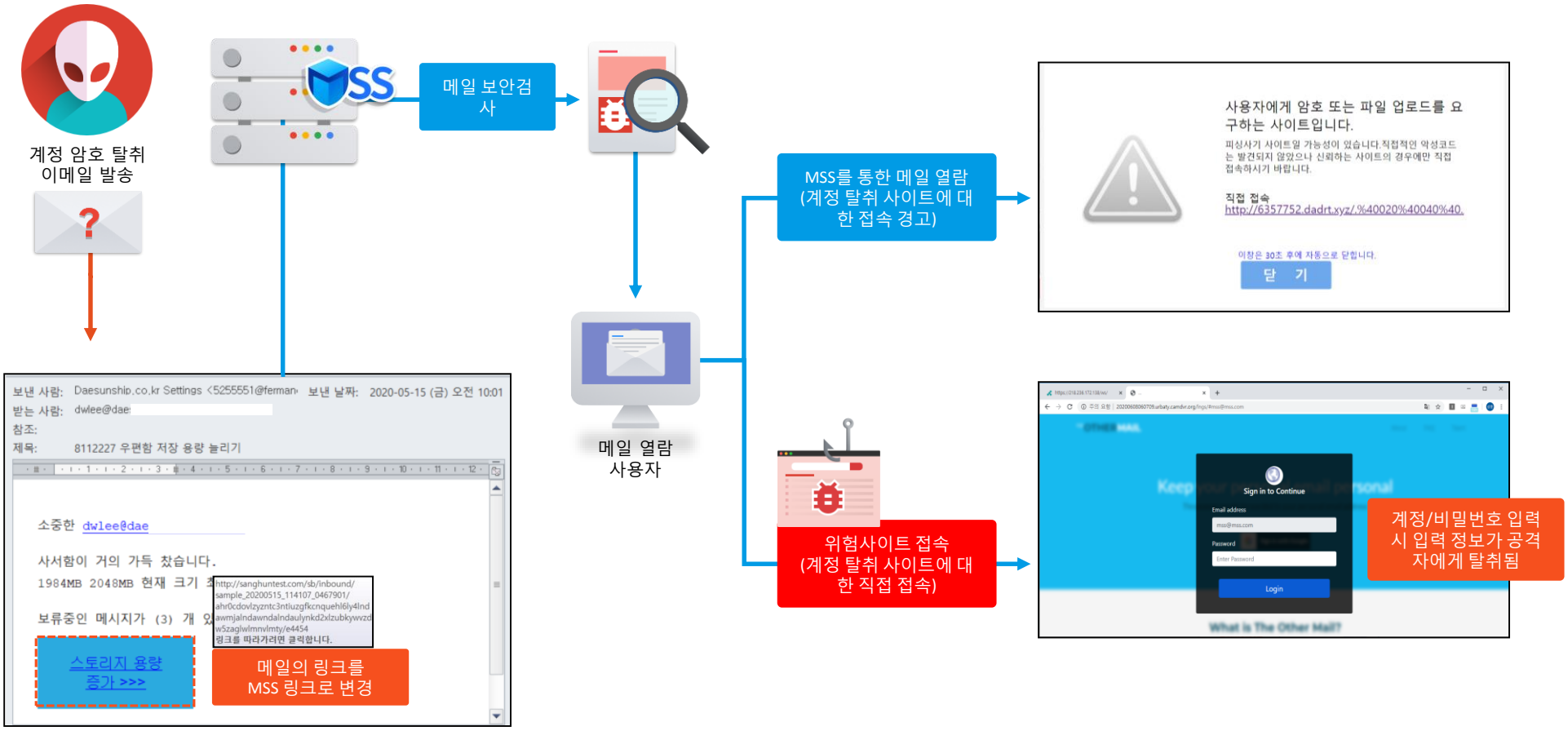
MSS는 외부링크 주소를 클릭 시 마다 보안검사를 하며, 궁극적인 안전장치로 MSS 주소로 변환합니다.



- Whitelist 원본 웹으로 접근(Connect Direct)
- 위험페이지 위치정보 포함 원본주소 접속 경고
- 안전한 페이지 위치정보 포함 원본주소 접속 경고
- Blacklist 웹 접속 차단

ATP를 이용한 계정/암호 요구 사칭 메일 차단

MSS는 메일에 첨부된 URL을 추적 검사 후 계정/암호 등을 요구하는 사칭 홈페이지로의 접속을 차단합니다.



- MSS는 메일에 포함된 URL을 실제 접속 후 접속 URL의 소스 코드를 파싱 하여 계정/ 암호 등을 요구하는 사칭사이트로의 접속과 재 연결 되는 페이지 등에서 악의적인 파일을

  다운로드 하는 행위 등을 차단합니다.
- 메일 수신 시점에 검사 또는 메일 열람 후 클릭 시에 재 검사를 수행하여 링크 변조 등을 통한 사칭 공격에 대한 접근을 차단합니다.

ATP를 통한 변조 공격 차단 유형

급증하는 해커들의 새로운 공격 유형을 MSS는 ATP를 통해 실시간 차단

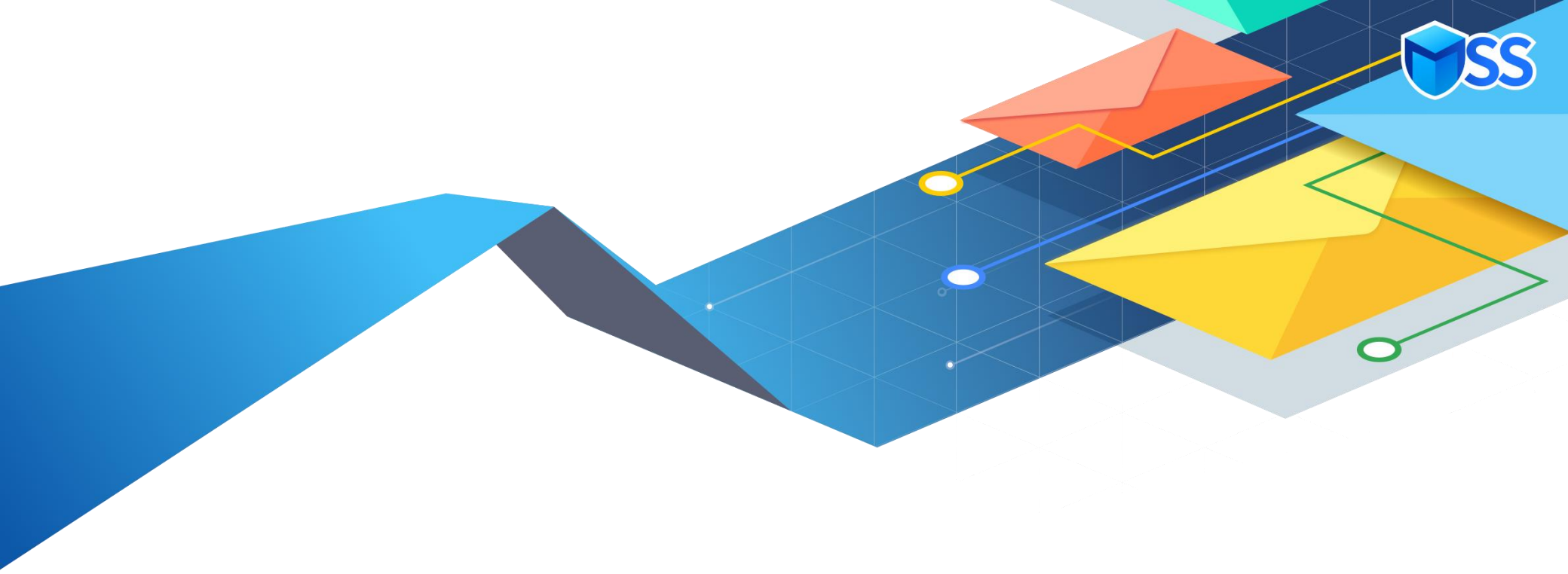
- ATP 기술을 통한 변종 공격 차단

- 시간차 등을 이용한 변종 공격 유형

공격유형	공격내용
404 ATTACK	최초 내용이 없는 링크로 메일 보내고 이후 공격자가 해킹할 때만 내용을 추가하여 공격하는 방식
500 ATTACK	최초 서버 연결오류 링크로 메일을 보내고 이후 공격자가 공격할 시 서버와 연결이 가능하도록 변경하여 공격하는 방식
DNS ATTACK	최초 IP가 없는 링크(도메인)으로 메일을 보내고 이후 공격할 때만 링크(도메인)을 변경하여 공격하는 방식
NORMAL CONTENS ATTACK	최초 일반적인 내용이 담긴 링크로 메일을 보내고 이후 공격 시점에 악성 컨텐츠로 변경하는 방식
REDIRECTION ATTACK	최초 정상적인 링크로 보내고 공격 시 악성페이지로 페이지를 연결하여 공격하는 방식
NO CONNCETION ATTACK	최초 연결되지 않는 링크로 메일을 보내고 이후 해당 링크에 연결이 되도록 구성하여 공격하는 방식
USER AGENT ATTACK	기존 보안 체계를 무력화 하도록 시스템 종류에 따라 다르게 동작하는 링크로 모바일 등과 같은 특정 단말기에서만 동작하는 방식

❖ 상기 7개의 공격 유형은 기존 보안 솔루션이 인지하지 못하는 공격유형 (이외 다수의 변종 공격 유형이 존재함)

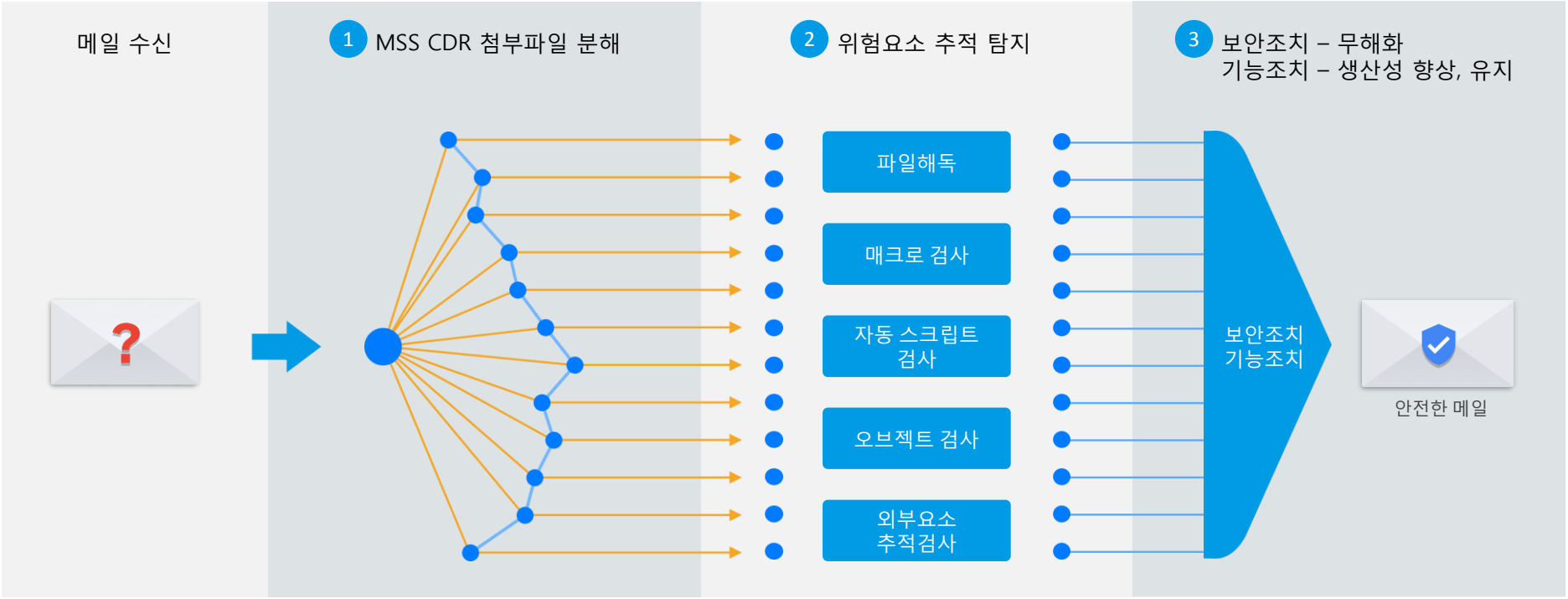
- ATP (All Time Protection)기술은 이미 알려진 해킹에 대해서 모두 대응하고 사용자가 메일의 연결된 링크나 첨부파일을 사용하는 모든 시간 동안 실시간으로 대응하기 때문에 시간차를 이용한 변종 공격 등을 미연에 방지할 수 있습니다.



4. MSS CDR & SANDBOX

MSS CDR 검출 차단 (무상 제공 기능)

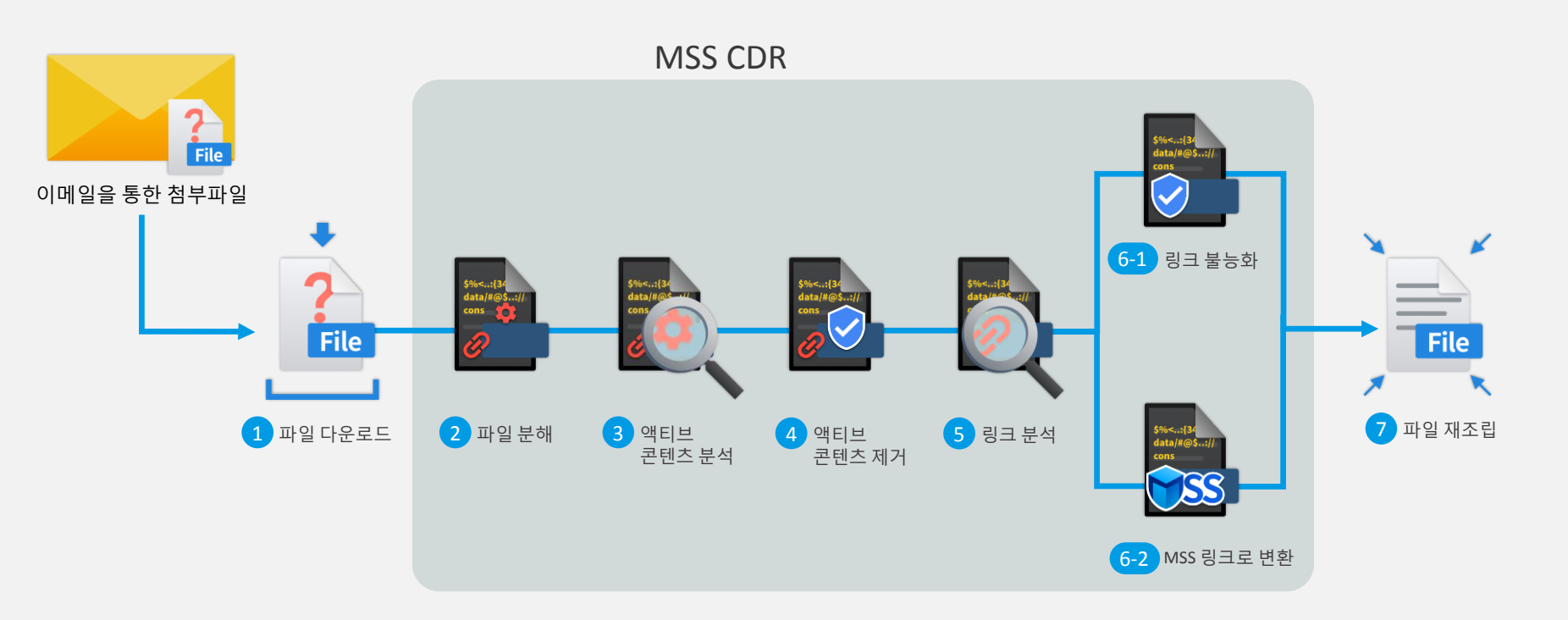
문서 해독을 통한 객체 검사 및 차단기능을 통해 위해 요소가 포함된 파일을 검출 및 차단 합니다.



- 첨부파일 CDR 기술 : CDR 기술을 이용하여 파일 해독 및 매크로 검사, 외부 오브젝트 검사, 스크립트 자동 실행 검사 등을 이용한 위험요소 차단 기능 제공

MSS CDR 변환 (유상 옵션 기능)

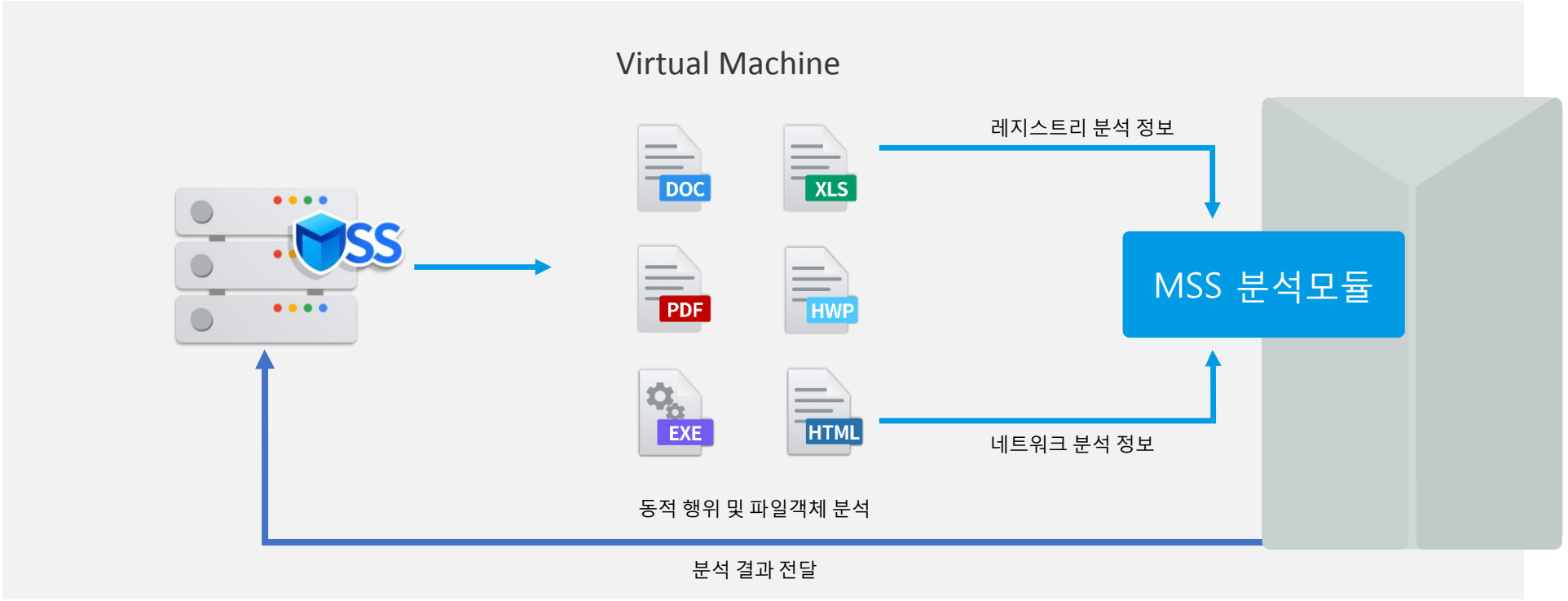
MSS CDR은 메일 첨부파일에 있는 메일을 분해하여 외부 객체를 삭제 후 재조립하며 메일에 있는 링크를 MSS 링크로 변환하여 첨부파일의 링크 접속 시 실시간 검사 기능을 제공합니다.



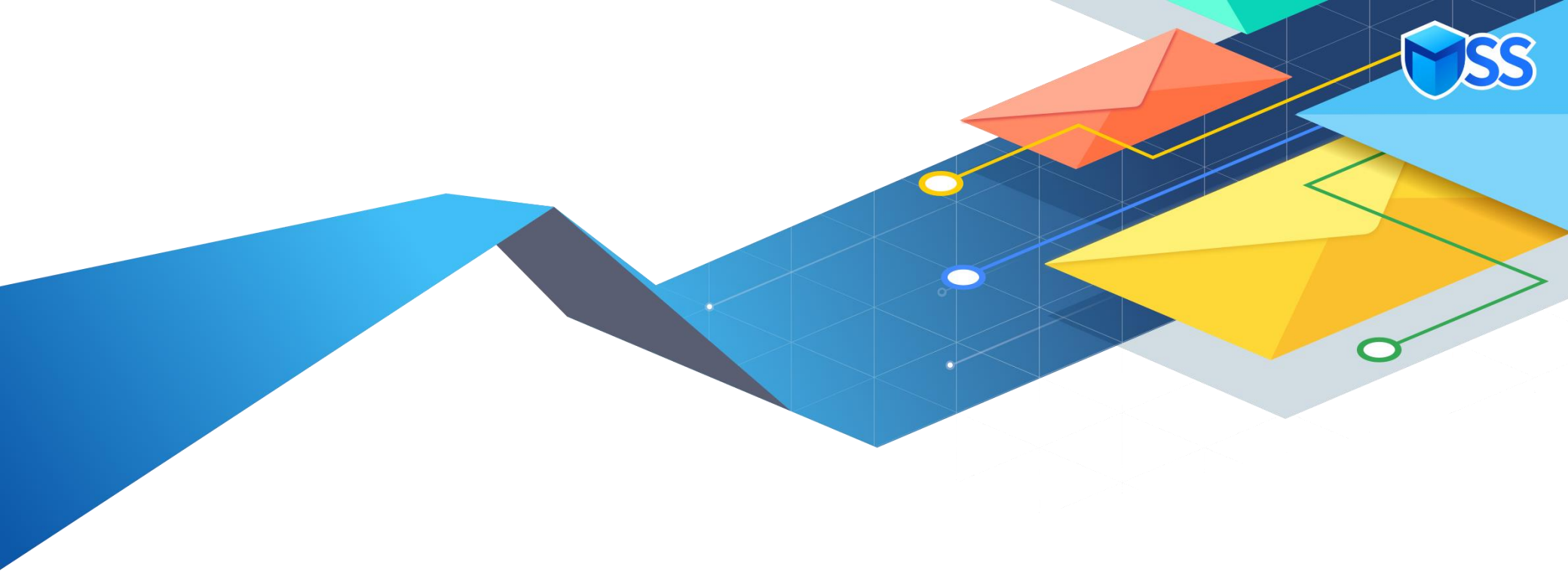
- MSS CDR 변환 기능 : 첨부파일의 링크를 MSS 링크로 변경하여 링크 접속 시 ATP 실시간 검사 기능 제공 (파일 재 조립 및 링크 변환 기능 – 유상 옵션)
- CDR 대상 파일 :오피스, PDF, HWP, HTML, 이미지 파일 등 약 20여가지 파일 CDR 기능 제공
- CDR 파일을 외부로 발송 시 MSS를 통한 링크 원복 (STEALTH) 기능 제공

MSS SANDBOX

SANDBOX를 통한 의심파일에 대한 분석 및 차단



- MSS SAND BOX
- CDR 검출을 통해 분석이 불가능한 파일에 대해서만 SANDBOX의 가상영역에서 해당 파일을 실행
- 실행되는 파일의 네트워크 통신 정보와 파일 객체 검사, 시스템 레지스트리 변경 정보를 추출
- MSS SAND BOX 를 통한 유해요소 차단 범위
- 네트워크 통신 정보에 대한 URL 추적 / 피싱 유무 확인 / 파일 객체의 연계 정보를 분석 후 악성일 경우 차단
- 악의적인 시스템 레지스트리 변경 건에 대한 차단
- MSS 서버 내 로컬 구성 및 SANDBOX를 별도의 하드웨어 분리 구성 가능



5. MSS ISMS 인증 패키지

MSS ISMS 메일보안 & 자료전송 패키지

MSS ISMS 패키지는 ISMS 인증 시 준수해야 할 망 분리 부분의 통제와 자료전송, 메일보안, 메일연계를 통한 망 분리 사용자의 업무 연속성을 보장할 수 있는 저비용 고효율 패키지 입니다.

01 스팸필터

- RBL(Internet-Based Real Time Blacklists)
- 스팸/스캠 메일 차단

02 안티바이러스

- ClamAV
- VirusChaser
- Kaspersky 지원
- 자체 검출 패턴

03 메일 분해 후 보안조치

- 메일을 분해하여 유해요소 제거 후 재조립
- 본문. 첨부파일, 이미지 등 MSS 서버 주소로 변환 후 단계별 보안조치

04 메일 박스 기능

- SSL TLS 기반의 POP3 메일 서버 기능 제공

05 메일 연계

- 망분리 환경에서 외부메일을 내부PC 원본형태로 볼 수 있는 유일한 솔루션
- 관련 특허 보유

06 대용량 첨부파일 다운로드

- 망분리 환경에서 NAVER, Daum등 포탈 사이트에서 첨부된 대용량 링크 파일을 업무 PC에서 다운로드 기능 제공

07 자료전송 기능

- 메일을 통한 자료전송 기능 제공
- 대용량 파일의 경우 링크를 통한 수신기능 지원

08 메일 승인/반출

- 첨부파일이 있거나 개인정보가 포함된 내용 발송 시 승인을 통한 외부 발송 기능 제공

09 개인정보 필터

- 발송 메일 본문의 개인정보 및 첨부파일에 대한 개인정보 필터 기능 제공 (커스텀 패턴 추가 가능)

- 수신되는 인터넷 메일의 보안 강화 및 망 분리 대상자의 업무 망 메일 서버 구축으로 업무 연속성 지속 (메일연계 기능을 통하여 유해요소를 제거한 상태로 원본과 동일한
  열람환경 제공 / SSL TLS 기반의 메일 서버 구성 및 메일 서버 간 암호화 프로토콜을 이용한 기능 구성 지원)
- 업무 망 메일 서버에서 인터넷 망 메일서버로 첨부 파일을 통하여 메일을 통한 자료전송 기능 제공 (대용량 파일의 경우 링크로 변환하여 수신 기능 제공)
- 메일 본문 / 첨부파일 DLP 검출 기능 및 승인을 통한 내부 정보 유출 통제 기능 제공

ISMS 인증 대상 범위

▪ 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령

☞ 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령

제49조(정보보호 관리체계 인증 대상자의 범위)

② 법 제47조제2항제3호에서 "대통령령으로 정하는 기준에 해당하는 자"란 다음 각 호의 어느 하나에 해당하는 자를 말한다.

1. 연간 매출액 또는 세입이 1,500억원 이상인 자로서 다음 각 목의 어느 하나에 해당하는 자
   가. 「의료법」 제3조의4에 따른 상급종합병원
   나. 직전연도 12월 31일 기준으로 재학생 수가 1만명 이상인 「고등교육법」 제2조에 따른 학교
2. 정보통신서비스 부문 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 100억원 이상인 자. 다만, 「전자금융거래법」 제2조제3호에 따른 금융회사는 제외한다.
3. 전년도 말 기준 직전 3개월간의 일일평균 이용자 수가 100만명 이상인 자. 다만, 「전자금융거래법」 제2조제3호에 따른 금융회사는 제외한다.

▪ ISMS 인증 의무 대상 기준

[표 2] 정보보호 관리체계 의무대상자 기준

구분	의무대상자 기준
ISP	「전기통신사업법」 제6조제1항에 따른 허가를 받은 자로서 서울특별시 및 모든 광역시에서 정보통신망서비스를 제공하는 자
IDC	정보통신망법 제46조에 따른 집적정보통신시설 사업자
다음의 조건 중 하나라도 해당하는 자	연간 매출액 또는 세입이 1,500억원 이상인 자 중에서 다음에 해당되는 경우 - 「의료법」 제3조의4에 따른 상급종합병원 - 직전연도 12월 31일 기준으로 재학생 수가 1만명 이상인 「고등교육법」 제2조에 따른 학교
	정보통신서비스 부문 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 100억원 이상인 자
	전년도 직전 3개월간 정보통신서비스 일일평균 이용자 수가 100만명 이상인 자

※ 정보통신망법 제47조제2항 및 시행령 제49조 참조

▪ 정보통신서비스 구분

구분	서비스 설명	정보통신서비스 부문 매출액 내역
신용카드 검색 (CCIS)서비스	인터넷으로 신용카드의 도난분실, 한도초과, 연체 등을 실시간으로 확인하는 서비스를 제공하는 사업자	카드조회수수료, 서비스 매출, 회원수익 매출, 부가수익 등
컴퓨터 예약 (CRS)서비스	인터넷을 통해 서비스나 상품에 대한 예약 서비스를 제공하는 사업자	상품 및 서비스 판매매출, 수수료, 회원 수익매출, 광고매출, 부가수익 등
전자문서교환 (EDI)서비스	인터넷을 통해 전자문서교환서비스를 제공하는 사업자	콘텐츠 판매매출, 수수료, 광고매출, 회원 수익매출, 부가수익 등
전자지불(PG)서비스	인터넷을 통해 지불중계역무를 제공하는 사업자	지불중계 수수료, 서비스 매출, 회원수익매출, 부가수익 등
인터넷 포털 서비스	인터넷 유,무선 포털 사이트를 제공하는 사업자	온라인 광고매출, 정보제공 수수료, 중계 수수료, 콘텐츠, 이용매출, 부가수익 등
인터넷 전자상거래	쇼핑몰 역무를 제공하는 사업자	판매 매출, 수수료, 광고매출, 부가수익 등
인터넷 방송	인터넷을 통해 신문기사나 방송프로그램을 제공하는 사업자	콘텐츠 판매매출, 수수료, 광고매출, 회원 수익매출, 부가수익 등
인터넷 게임	인터넷게임서비스를 제공하는 사업자	게임이용매출, 아이템 판매매출, 광고매출, 수수료, 무가수익 등
금융 관련 서비스	인터넷을 통한 금융업, 연금업, 보험관련 서비스업 등을 제공하는 사업자	인터넷 뱅킹·주식, 거래·선물, 거래 수수료, 인터넷 증권 중개, 홈트레이딩 등 기타 인터넷 금융 및 보험업 등
콘텐츠 제공 서비스	인터넷을 통한 교육서비스를 제공하는 사업자	콘텐츠, 이용매출, 수수료, 광고매출, 회원 수익매출, 부가수익 등
	인터넷을 통한 실시간 음악 감상 서비스를 제공하는 사업자	
	인터넷을 통한 기타 콘텐츠제공 서비스를 제공하는 사업자	
유선방송 서비스 (Cable-SO)	종합유선 방송서비스와 종합유선전송 서비스를 제공하는 사업자	방송중계서비스 매출을 제외한 초고속인터넷서비스 매출액 등
기타	인터넷을 통한 기타 정보통신서비스를 제공하는 사업자	

▪ 전년도 말 기준 직전 3개월간의 일일 평균 이용자 수 100만명 이상

- 일일평균 이용자 수는 일정 기간 동안의 정보통신서비스제공자의 홈페이지 방문자 수 등을 일평균으로 환산한 이용자 수를 말하며, 여러 가지 정보통신서비스를 제공할 경우에는 해당 서비스의 이용자 수를 모두 합하여 계산한다.
- 일일평균 이용자 수는 PV(Page View)를 말한다.
  - ※ PV(Page View) : 홈페이지에 들어온 접속자가 둘러 본 페이지 수
  - ※ PC, 스마트폰 등이 네트워크 운영을 위해 이용하는 DNS query, 기지국 등록 등의 접속은 제외
  - ※ 자체적 또는 공식적으로 이용자 수 확인이 어려운 경우, 민간 통계기관 등의 데이터 활용

- 4년제 대학 전년도 12월31일 기준 재학생 수가 1만명 이상인 대학교는 ISMS인증 의무 대상이며 정보통신서비스 부문의 콘텐츠 제공 서비스를 통한 매출액이 100억인
  사이버 대학교나 전문 대학교도 ISMS 인증 의무 대상이 될 수 있음.
- ISMS 인증 대상이 미 인증 시 최대 3000만원의 과태료가 부과됨

ISMS 인증 점검 항목에 따른 MSS 도입 효과

- ISMS 인증 : 접근통제 – 인터넷 접속

구분	통제 분야	NO	통제항목	통제목적	점검항목	설명
10.4	접근통제영역	10.4.6	인터넷 접속	인사정보, 영업비밀, 산업기밀, 개인정보 등 중요정보를 대량으로 취급·운영하는 주요직무자의 경우 인터넷 접속 또는 서비스(P2P, 웹메일, 웹하드, 메신저 등)를 제한하고 인터넷 접속은 침입차단시스템을 통해 통제하여야 한다. 필요시 침입탐지시스템 등을 통해 인터넷 접속내역을 모니터링하여야 한다.	다음과 같은 인터넷 접속에 대한 정책을 수립하고 있는가? - 인터넷 연결시 네트워크 구성 정책 - 이메일, 인터넷 사이트의 접속, 소프트웨어 다운로드 및 전송 등의 사용자 접속정책	ㅇ 인터넷 접속에 대한 보안정책을 수립하여야 한다. 보안정책에는 인터넷 연결 시의 네트워크 구성 정책, 사용자 접속정책을 포함하여야 한다.
					중요정보를 취급 · 운영하는 주요 직무자를 식별하여 인터넷 접속을 제한하고 있는가?	ㅇ 중요정보를 취급·운영하는 주요 직무자(개인정보취급자, 시스템관리자 등)의 경우 인터넷 접속 또는 서비스(P2P, 웹하드, 웹메일, 메신저 등)를 제한하는 등의 보호대책을 수립하고 이에 따라 이행하여야 한다. (인증기준 6.1.1 주요 직무자 지정 및 감독 참조) - 다만 일정규모 이상의 정보통신서비스제공자는 개인정보를 처리(다운로드, 파기, 접근권한 설정)하는 개인정보취급자 컴퓨터의 외부 인터넷 접속을 차단하여야 한다. ※ 참고 ※ - 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 제15조(개인정보의 보호조치) - 정보통신망 이용촉진 및 정보보호 등에 관한 법률 '개인정보의 기술적 · 관리적 보호조치 기준(고시)' 제4조(접근통제)
					내부 직원의 업무용 PC에서 유해사이트 등의 접속을 차단하고 있는가?	ㅇ 외부로부터의 악성코드 유입을 방지하기 위하여 내부 업무용 PC의 유해사이트(P2P, 웹하드 등) 접속에 대한 차단조치를 수행하여야 한다.
					내부 서버에서 외부 인터넷접속을 제한하고 있는가?	ㅇ 악성코드 유입, 리버스커넥션이 차단되도록 내부 서버(DB서버, 파일서버, 패치서버 등)에서 외부 인터넷 접속을 제한하여야 한다. 부득이하게 허용할 필요가 있는 경우 관련 위험분석을 통해 보호대책을 마련하고 정보보호책임자의 승인을 얻어야 한다.
					인터넷 PC와 내부 업무용 PC를 분리하고 있는 경우 PC간의 자료전송을 통제하고 있는가?	ㅇ 원칙적으로 인터넷망과 내부망 PC 간의 자료전송은 차단하여야 하며 필요한 경우 별도의 통제절차를 거쳐 전송하고 해당 로그를 주기적으로 검토하여야 한다.

- ISMS-P 인증 : 접근통제 – 인터넷 접속

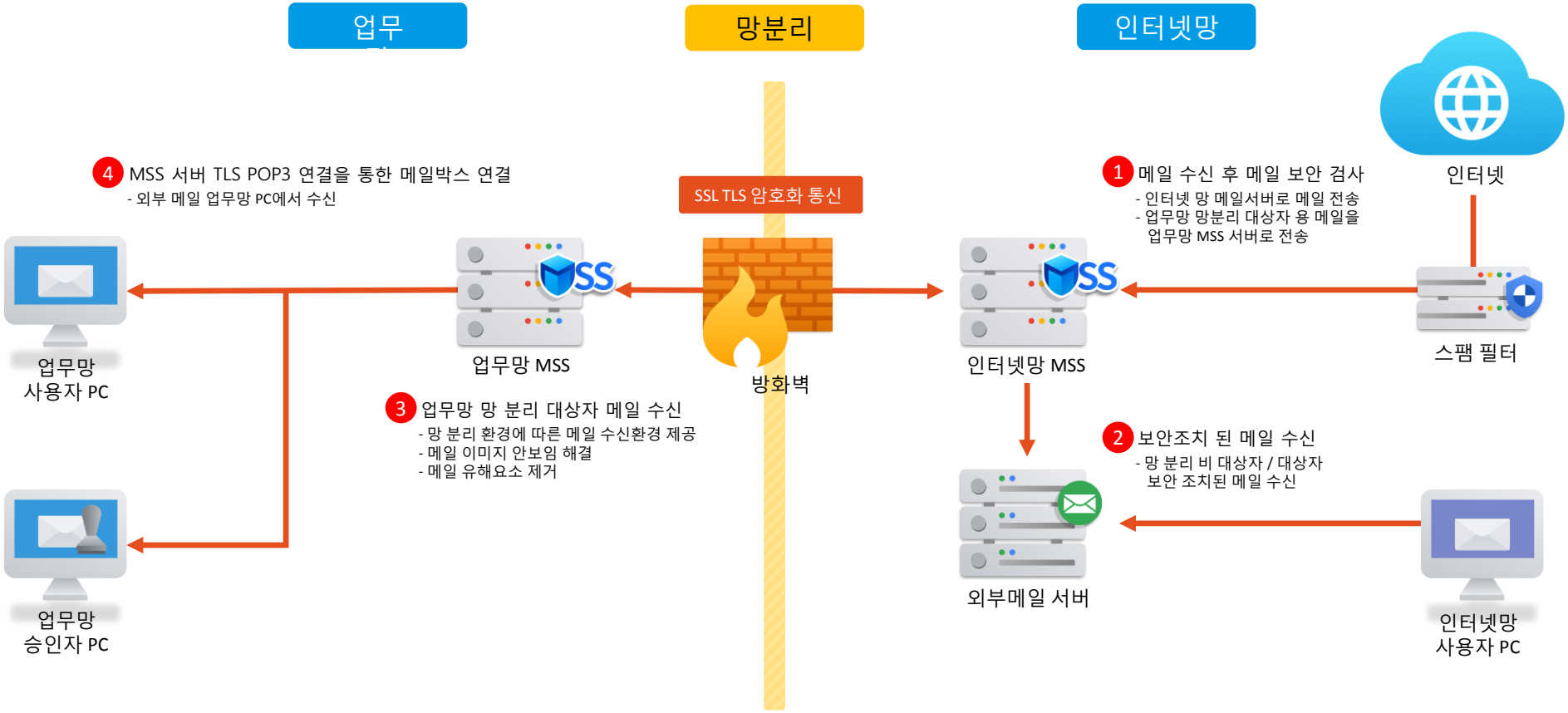
NO	분야	항목		상세내용	주요 확인사항
2.6	접근 통제	2.6.7	인터넷 접속통제	인터넷을 통한 정보 유출, 악성코드 감염, 내부망 침투 등을 예방하기 위하여 주요 정보시스템, 주요 직무 수행 및 개인정보 취급 단말기 등에 대한 인터넷 접속 또는 서비스(P2P, 웹하드, 메신저 등)를 제한하는 등 인터넷 접속 통제 정책을 수립·이행하여야 한다.	주요 직무 수행 및 개인정보 취급 단말기 등 업무용PC의 인터넷 접속에 대한 통제정책을 수립·이행하고 있는가?
					주요 정보시스템(DB서버 등)에서 불필요한 외부 인터넷 접속을 통제하고 있는가?
					관련 법령에 따라 인터넷 망분리 의무가 부과된 경우 망분리 대상자를 식별하여 안전한 방식으로 망 분리를 적용하고 있는가?

- ISMS 인증의 접근 통제 부문에 중요정보를 취급하는 사용자의 망 분리는 필수임.
- ISMS 인증 시 망 분리 대상자의 인터넷 접속에 대한 통제 및 내부 자료 유출 방지를 위한 보호 대책 마련이 필요함.
- MSS 도입을 통해 업무 망 메일 서버 구성 및 메일 연계 환경으로 망 분리 대상자의 업무 생산성 유지
- 내부에서 외부로 발송되는 자료의 개인정보 필터 및 승인 기능을 통하여 내부 자료 유출에 대한 통제 및 관리가 가능함
- 망 분리 시 필수적으로 사용되는 망간 자료전송 기능을 메일 서버를 통한 자료전송 기능을 통하여 업무 PC와 인터넷 PC 간 자료전송 기능을 대체하여 운영할 수 있음.

  (망간 자료전송 제품 운영에 대한 불편함 및 망간 자료전송 도입 비용을 하나의 MSS ISMS 패키지로 대체하여 사용할 수 있음)

MSS ISMS 메일보안과 자료전송 예시 구성도 #1

MSS ISMS 패키지 메일 수신 구성도



- 수신되는 인터넷 메일의 보안 강화 및 망 분리 대상자의 업무 망 메일 서버 구축으로 업무 연속성 지속
- 메일연계 기능을 통하여 유해요소를 제거한 상태로 원본과 동일한 열람환경 제공
- SSL TLS 기반의 메일 서버 구성 및 메일 서버 간 암호화 프로토콜을 이용한 기능 구성 지원
- 업무 망 MSS POP3 연결을 통한 메일 서버 기능 구성

망 분리 환경에서 원본메일 유지 (업무망 망 분리 대상자)

도입전 : 원본 이미지정보 읽지 못함

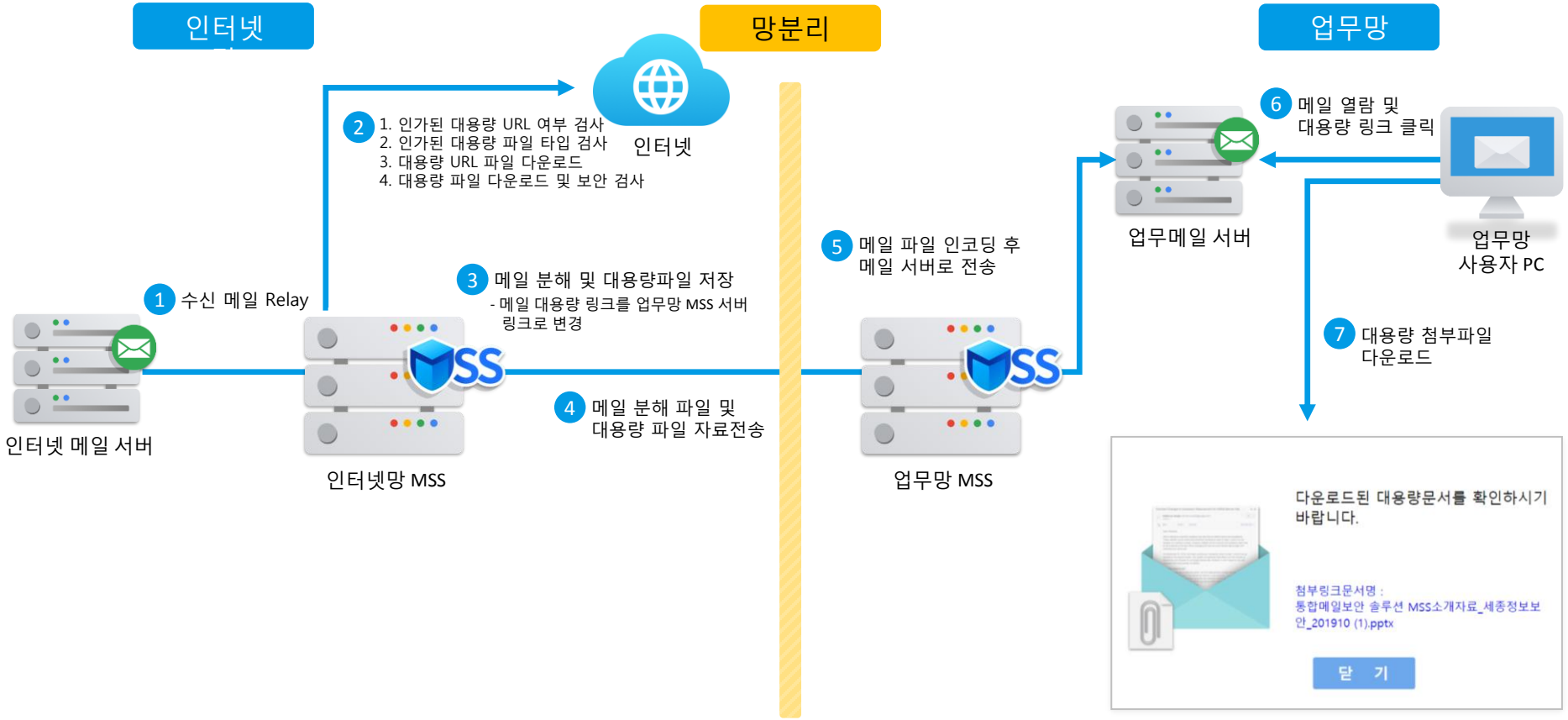
- 업무 연속성 불편
- 메일 회신 불편
- 장문 메일 본문 잘림
- 내용 복사x
- 빠른 업무대응x

도입후 : 원본 메일 유지로 불편함 해소

- 메일 사용 불편함 완벽 해소
- 메일 회신 편리
- 장문 메일 본문 유지
- 내용 복사 o
- 빠른 업무대응 o

대용량 첨부파일 다운로드

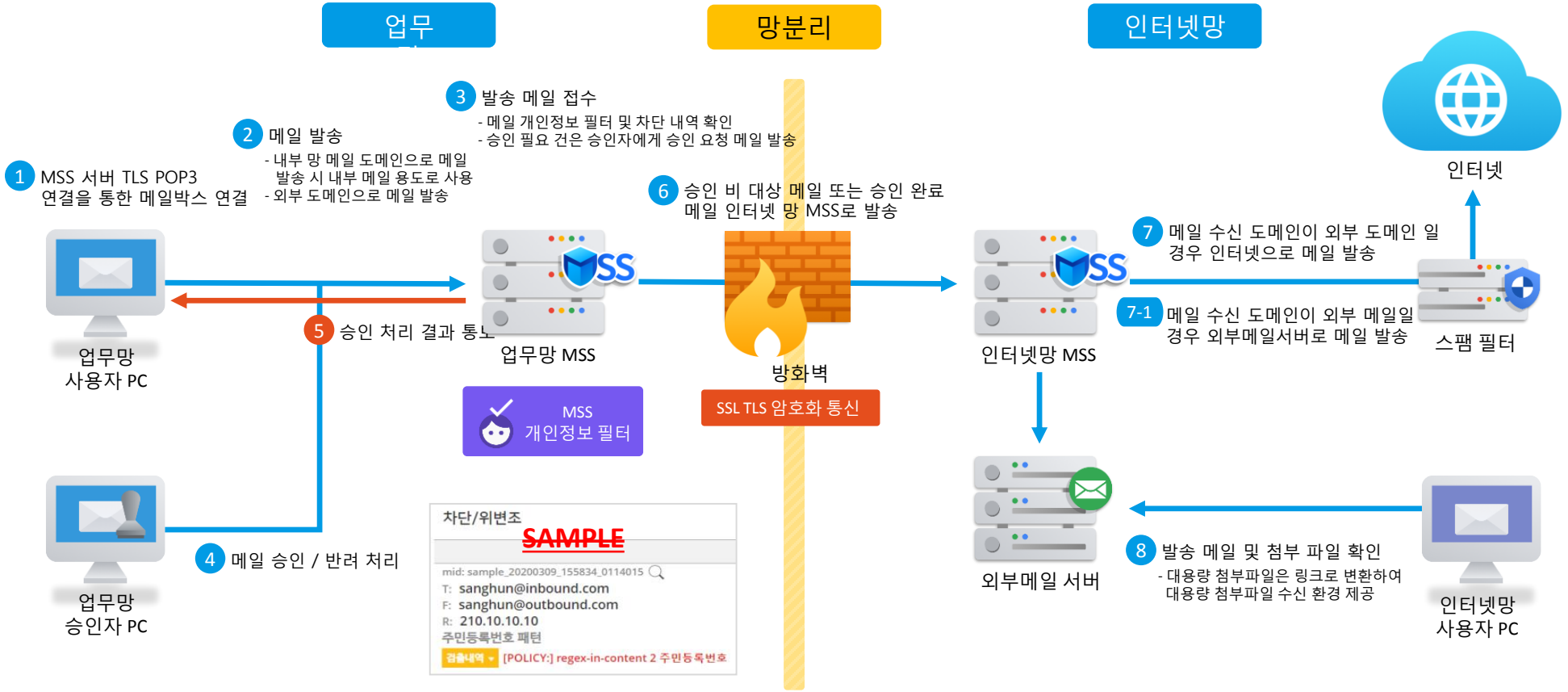
외부에서 수신되는 대용량 첨부파일을 다운로드 받아 업무망 PC에서의 수신 환경 제공



- 망 분리 환경에서 외부로부터 수신되는 대용량 첨부파일을 업무PC에서 다운로드 할 수 있는 기능 제공
- 관리자 설정에 따라 White List, Black List 형태의 대용량 URL 다운로드 설정 기능 제공
- 수신되는 파일 Format을 White List, Black List 방식으로 설정 기능 제공
  - 수신 파일이 압축파일의 경우 악성코드 검사, 파일 위 변조 검사, CDR 검사 등을 통해 안전한 대용량 첨부파일만 다운로드

MSS ISMS 메일보안과 자료전송 예시 구성도 #2

MSS ISMS 패키지 메일 발신 및 반출 구성도



- 메일 발신 시 내부 메일 서버 도메인으로 메일 발송을 통한 내부 전용 메일 서버 구성
- 외부로 메일 발신 시 MSS DLP를 통한 개인정보 필터 (본문, 첨부파일) 및 내부 정보 유출 통제 기능 제공 (승인이 필요한 내역에 대하여 **개인정보 유형, 개인정보 임계 값,**

  첨부파일 개수, 메일 유형 등을 관리자가 직접 지정할 수 있으며 별도의 커스텀 패턴 필터 기능도 제공)
- 외부 메일 서버 도메인으로 메일 발송을 통한 업무PC 와 인터넷 PC간 자료전송 기능 제공 (대용량 파일의 경우 첨부파일을 MSS 링크로 변환하여 수신)

MSS ISMS 패키지 주요 제공 기능 요약

스팸 및 사칭 메일 차단

- 글로벌 스팸 엔진을 통한 스팸 기능 및 MSS 자체 Machine Learning을 통한 스팸 메일 차단
- 공공기관 사칭 이메일 등에 대한 차단으로 불필요한 스팸 메일 및 사칭 이메일 차단

업무 망 메일 서버 구성

- 망 분리 대상자의 업무 효율성 증대 및 내부 자료 보안을 위한 망 분리 대상자용 내부 메일 서버 구성 기능 제공
- SSL TLS 암호화를 통한 ISMS 규격 준수

개인정보 필터 기능

- MSS DLP를 통한 외부 발송 메일의 개인정보 필터 기능제공 (메일 본문, 첨부 파일, 알려진 주요 개인정보 패턴 및 커스텀 패턴 추가 등록 기능 제공)

망간 자료전송 기능 제공

- MSS 서버 간 메일 전송을 통한 자료전송 기능 제공
- 내부로 반입되는 자료의 보안 강화
- 대용량 파일의 링크로 변환하여 수신 기능 제공

악성코드 검사 / 위 변조

- 메일 본문 및 첨부파일 안에 있는 URL요소까지 검사하여 보안추가 위험요소 차단
- 멀티 백신 및 제조사 패턴을 통한 보안 위해 요소 차단
- 매크로 및 오브젝트 등에 대한 구성요소 검사 후 차단

망 분리 환경 대상자 메일 연계

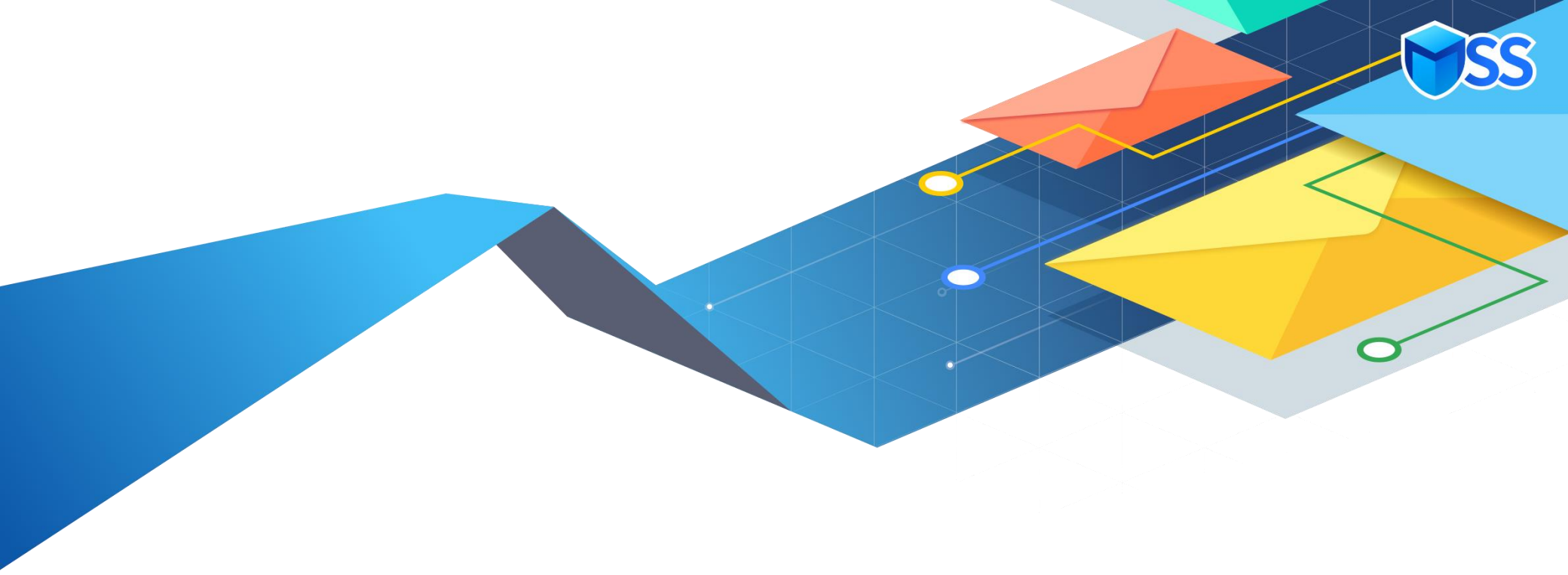
- 망 분리 환경에서 외부 메일을 내부로 연계하여 메일전달
  - 원본 메일 동일 형태 유지 (파일로 분해, 재 조립)
  - 유해 요소 제거 (외부 EML 태그 및 스크립트 등 제거)

메일 반출 / 승인

- 망 분리 대상자의 메일 반출 / 승인 기능을 통한 내부 자료유출 통제
- 첨부파일 유형, 개수 및 다양한 조건에 따른 승인 기능 제공

메일 보관 / 감사 기능 제공

- 내/ 외부로 수 발신 되는 모든 메일에 대한 내역을 로그로 보관
- 향후 감사 대비 및 사후 추적 용도로 사용할 수 있음 (메일 아카이빙 기능 제공)



6. 메일연계

MSS 메일연계 패키지

MSS 메일연계 패키지는 망 분리 환경에서 원본 메일과 동일함 열람 환경을 제공합니다.

01 메일 연계

- 망분리 환경에서 외부메일을 내부PC 원본형태로 볼 수 있는 유일한 솔루션
- 관련 특허 보유

02 안티바이러스

- ClamAV
- VirusChaser
- Kaspersky 지원
- 자체 검출 패턴

03 메일 분해 후 보안조치

- 메일을 분해하여 유해요소 제거 후 재조립
- 본문. 첨부파일, 이미지 등 MSS 서버 주소로 변환 후 단계별 보안조치

04 이미지 캐싱 서버

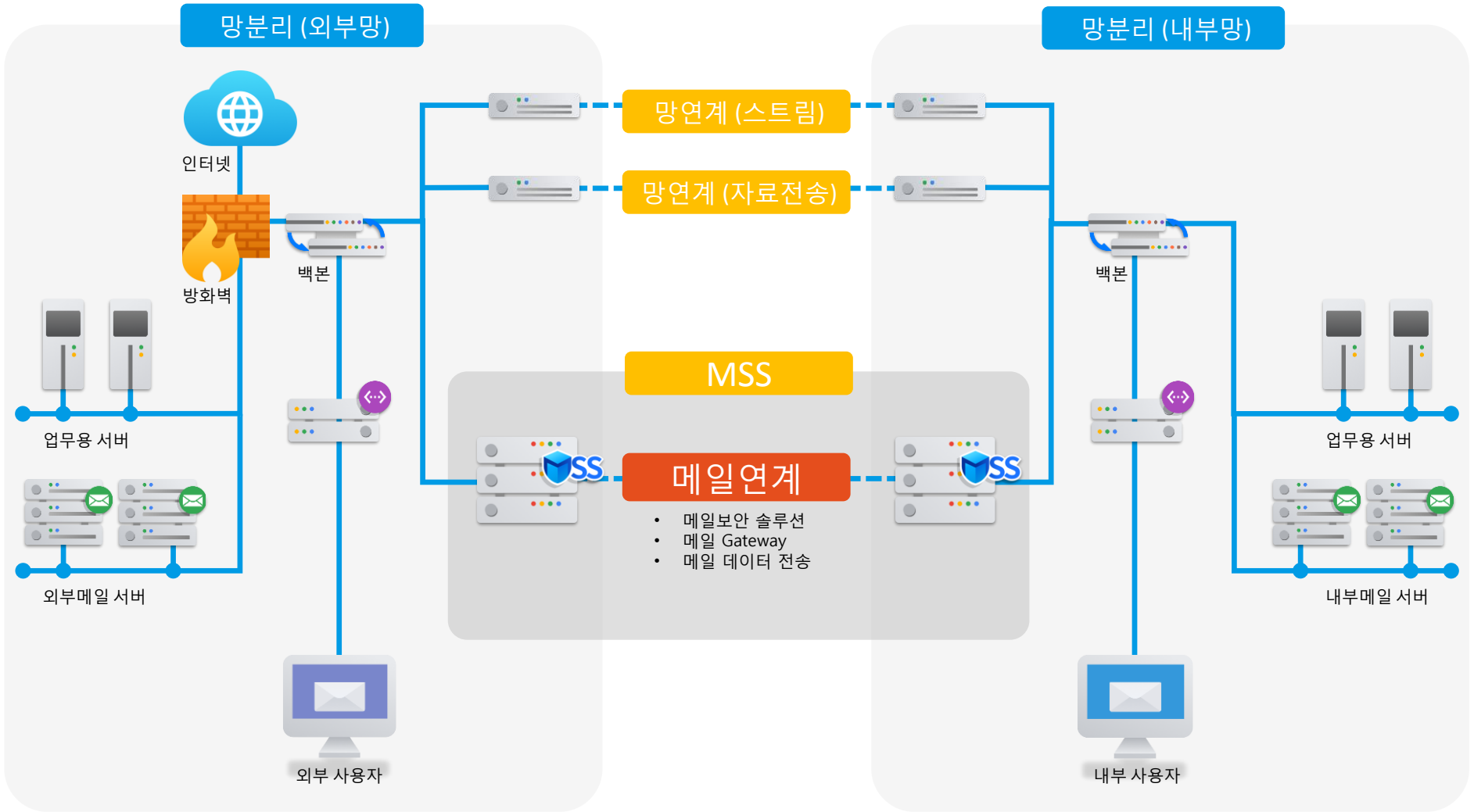
- 외부에서 수신 된 메일의 이미지를 내부에서 이미지 캐싱하여 메일 데이터 크기 증가 없이 원본과 동일한 수신환경 제공

05 다양한 메일 수신 정책

- 본문, 첨부파일 제거 or 첨부파일만 제거 하는 등의 다양한 수신 정책 구현
- 이슈 메일 등에 대한 사용자 복구 기능 및 메일 미리보기 (프리뷰)를 통한 원본메일 열람 후 복구 기능 제공

망분리 환경에서 MSS 구성도

MSS는 메일 수·발신에 대한 망분리 가이드 지원 및 메일연계 및 보안 강화



망 분리 환경에서 원본메일 유지 (업무망 망 분리 대상자)

도입전 : 원본 이미지정보 읽지 못함

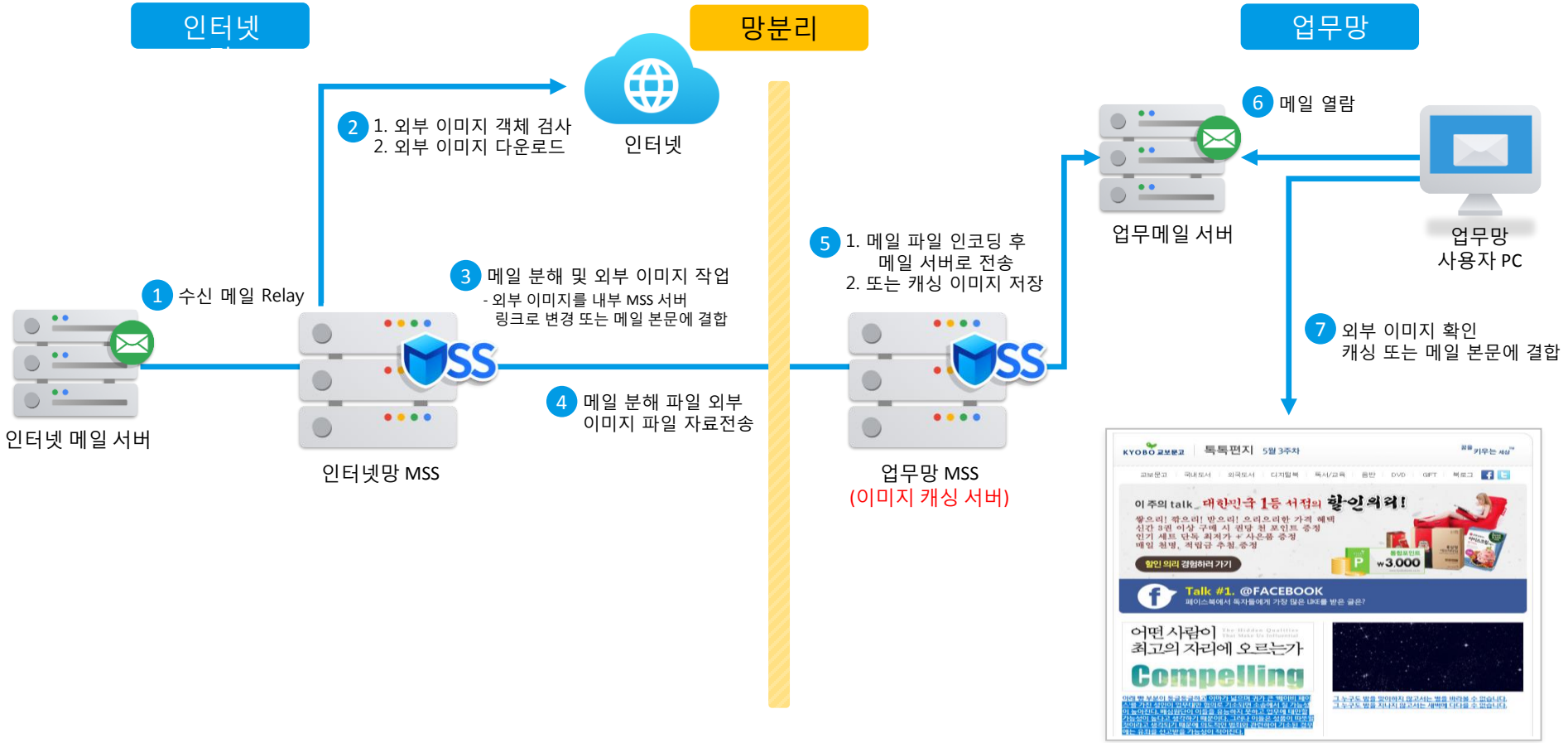
- 업무 연속성 불편
- 메일 회신 불편
- 장문 메일 본문 잘림
- 내용 복사x
- 빠른 업무대응x

도입후 : 원본 메일 유지로 불편함 해소

- 메일 사용 불편함 완벽 해소
- 메일 회신 편리
- 장문 메일 본문 유지
- 내용 복사 o
- 빠른 업무대응 o

외부 이미지 캐싱 기능

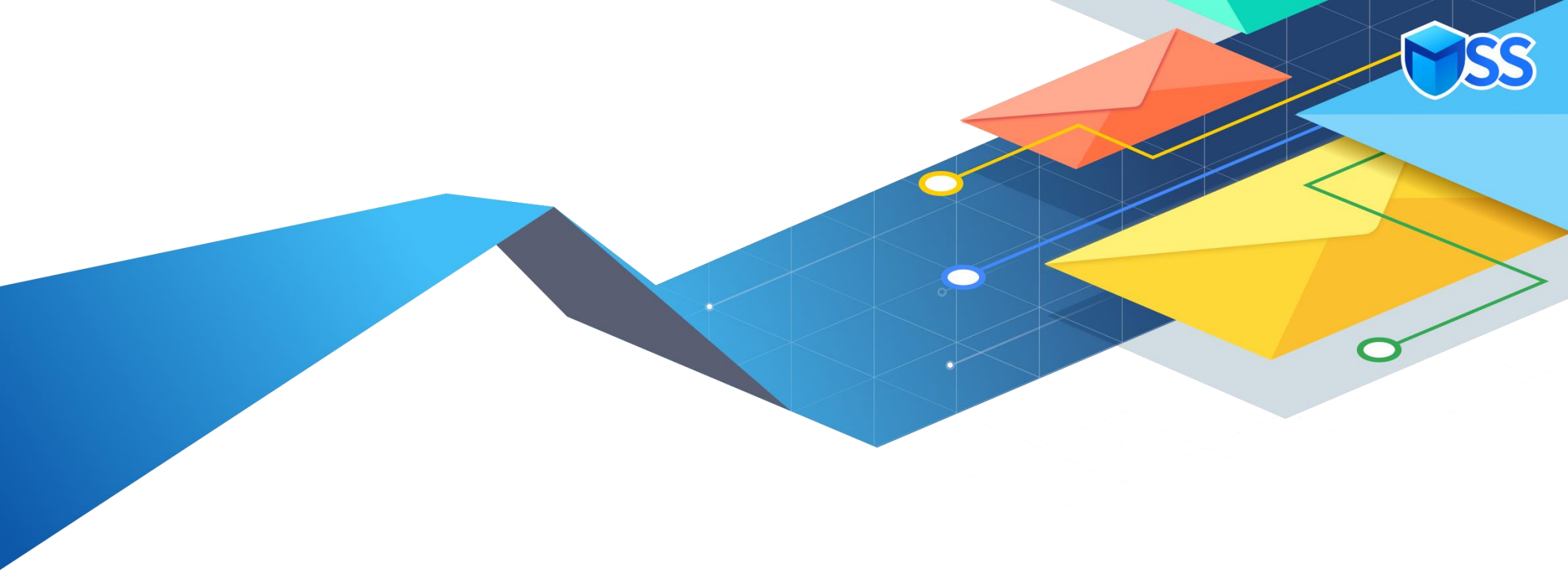
외부에서 수신되는 이미지를 메일 본문에 결합 또는 내부에서 이미지 캐싱 서버 역할 지원



- 망 분리 환경에서 외부로부터 수신되는 메일의 외부 링크 이미지 등을 업무 망 에서 열람할 수 있는 환경 제공
- 외부 이미지를 메일 본문에 결합하여 가독성 보장 (메일 사이즈가 증가될 수 있음)
- 또는 메일 외부 링크 이미지를 업무망 MSS 서버에서 캐싱하여 가독성 보장 (메일 사이즈 증가가 없음)

메일 연계 방식에 대한 금융감독원 답변서

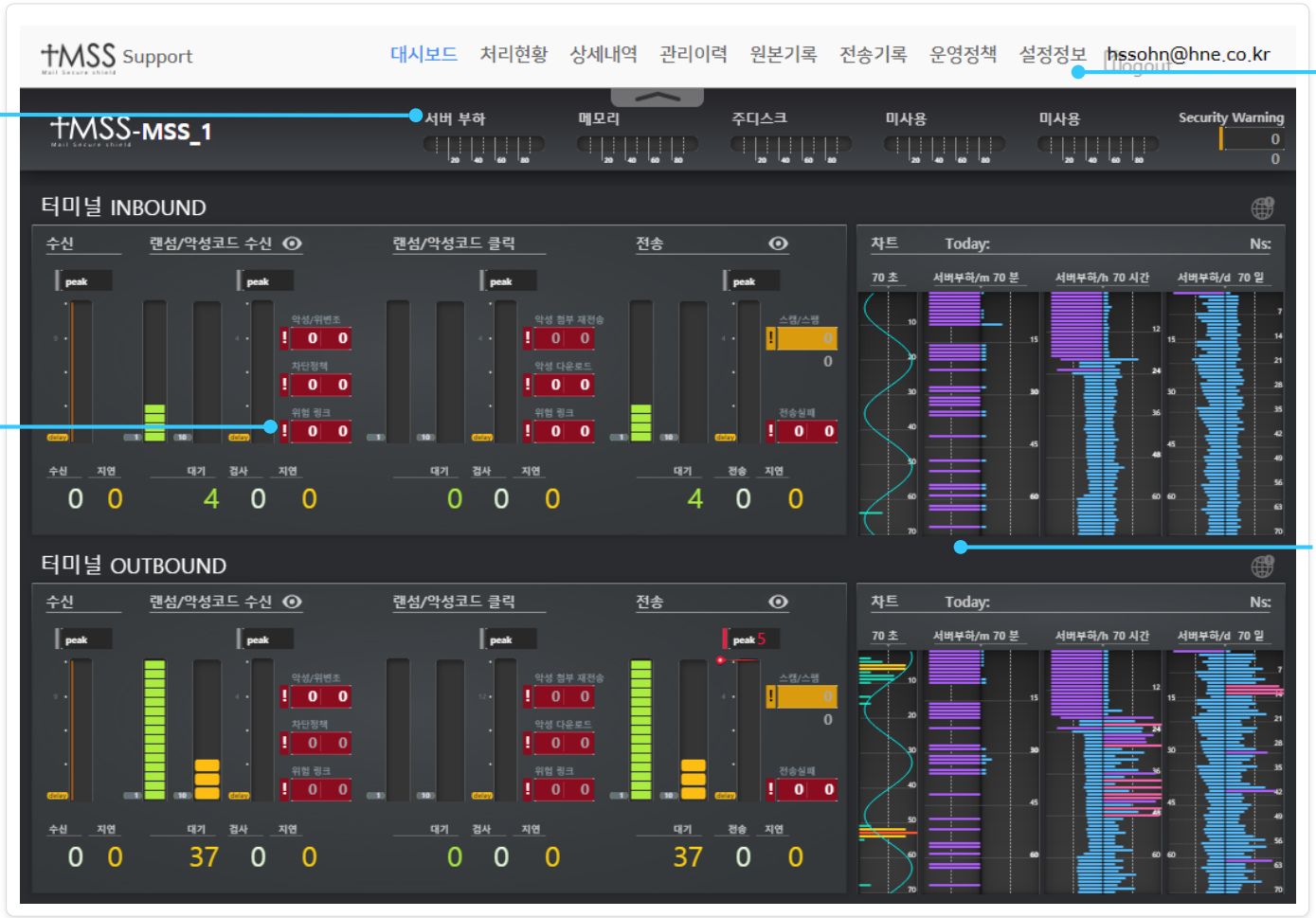
제목	외부메일 내부망 전송시 대체 정보보호 통제 방식에 대한 문의
회신일	2019-11-26
요청대상 행위	외부로부터 전송 받은 전자메일을 내부 업무망 메일서버로 전송할 때, 망연계 시스템을 통해 본문의 스크립트와 악성코드를 제거하고 재조립하여 전송하는 것이 망분리 관련 규정에 위배되는지 여부
판단	**요청대상 행위는 망분리 규정을 위반하지 않은 것으로 보입니다.**
판단이유	금융회사는 정보처리시스템 및 정보통신망을 해킹 등 전자적 침해행위로부터 방지하기 위해 내부통신망과 연결된 내부 업무용시스템을 외부통신망과 분리·차단 및 접속금지의 조치를 하여야 하고, 업무상 필요에 의한 내부망과 외부망 간 자료 교환을 위해 보조기억장치 또는 망간 자료전송시스템 등을 이용할 수 있습니다. 따라서 망간 자료전송시스템을 이용하여 인터넷망에서 수신된 이메일을 파일 형태로 변환하여 내부망으로 전송하는 것은 가능하며, 다만, 자료전송 과정에서 침해행위에 대비하기 위해 악성코드 검사, 본문 Text 또는 이미지 변환*, 첨부파일 필터링** 등 적절한 통제 절차를 적용해야 합니다. * 외부 링크, eml Tag, 스크립트 등 제거 ** 문서파일 및 이미지파일 외 첨부파일은 내부통신망 전송 전 제거



7. MSS 관리자 & 사용자 UI

MSS 대시보드

대시보드를 통한 메일의 실시간 처리 현황 및 시스템 자원 사용률 모니터링 기능

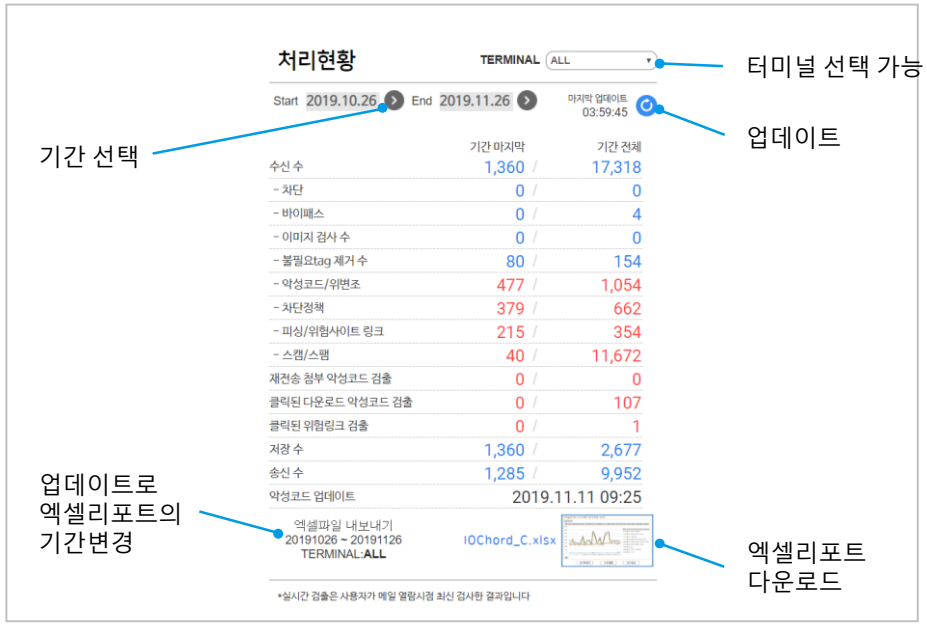


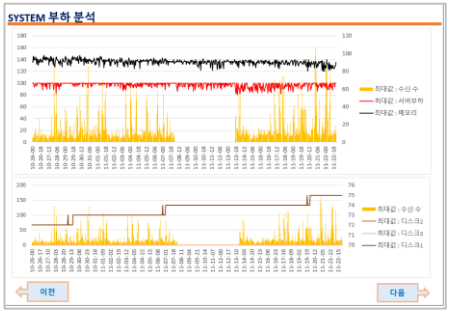
- 대시보드를 통해 메일의 실시간 처리 정보 및 감염 내역을 직관적으로 확인할 수 있습니다. 또한 터미널 별로 메일 수신 Que / 악성코드 검사 Que / ATP 검사 Que / 메일 발송 Que 를 논리적으로 조정할 수 있습니다.

MSS 대시보드 시연 동영상

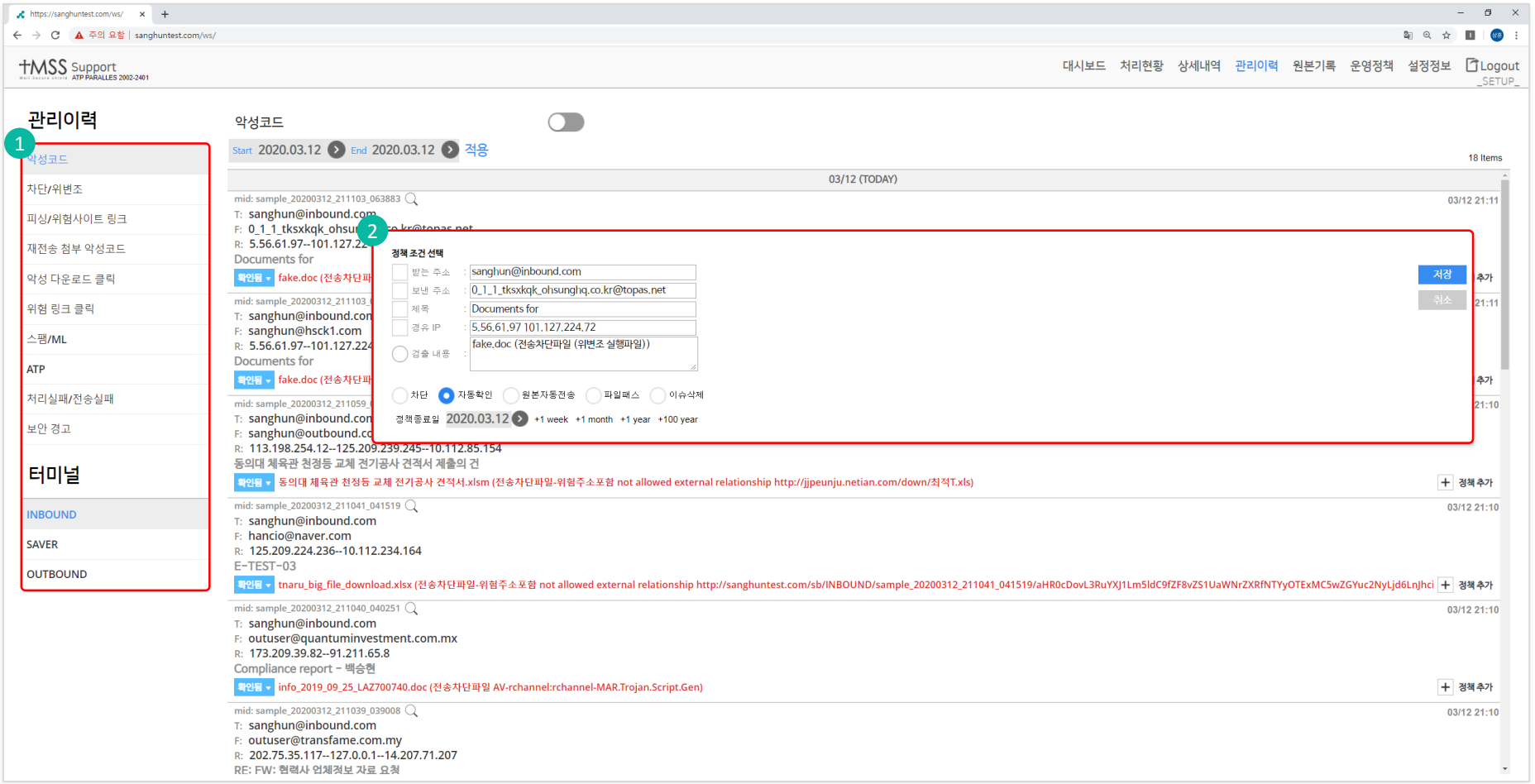
MSS 레포팅 기능

각종 현황 및 감사 대비 다양한 레포팅 기능 제공





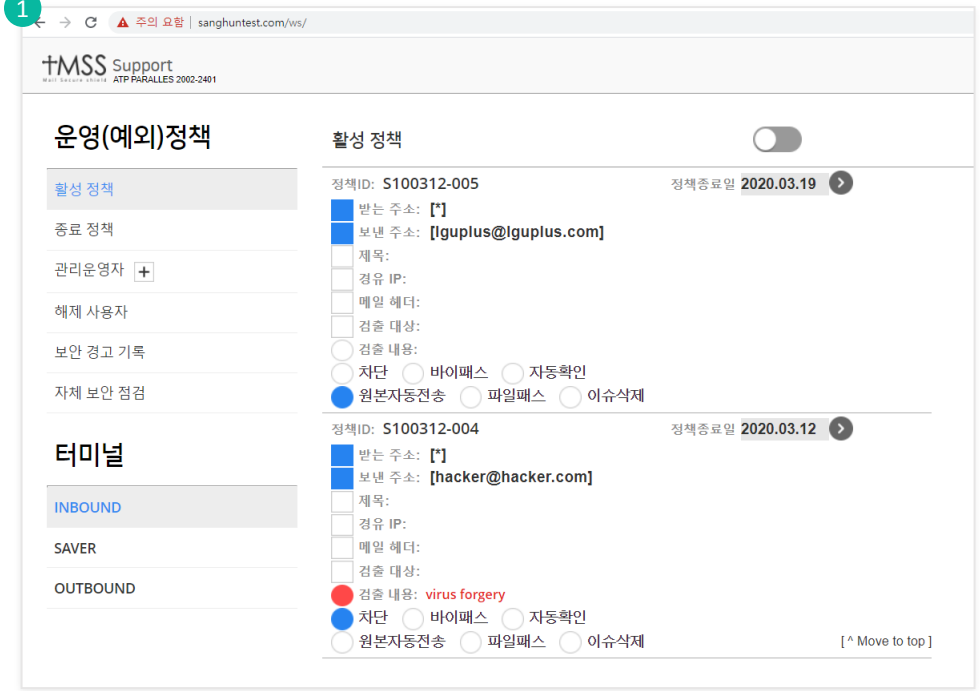
MSS 관리페이지 – 관리 이력



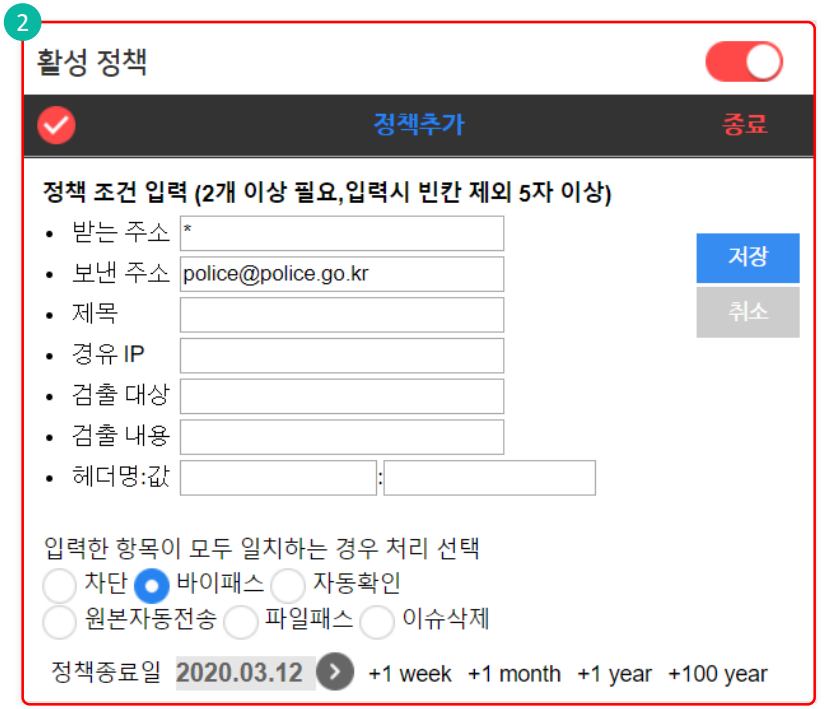
- 1 관리 이력을 통해 유형별 검출 내역을 확인할 수 있습니다.
- 검출 내역 확인 후 2 + 정책 추가 를. 이용하여 동일 이력에 대한 차단 / 원본 자동 전송 / 이슈 삭제 등을 관리자가 직접 설정할 수 있습니다.

MSS 관리페이지 – 운영 정책

1



2



- 1 별도의 수 발신 메일 예외 (활성) 정책을 확인할 수 있습니다.
- 터미널 별 설정이 가능하며 관리자가 직접 내역 기재 및 날짜를 지정하여 종료 날짜를 지정할 수 있습니다.
- 2 정책 추가 시 받는 주소, 보낸 주소, 메일 제목, 경유 IP, 검출 대상, 검출 내용, 특정 헤더 등을 관리자가 지정하여 원하는 날짜 까지 예외 정책을 운영할 수 있습니다.
- 별도로 메일 수 발신자 및 첨부파일 패턴, 도메인 유형, IP 유형, 메일 제목 등을 CSV 파일 형태로 WHITE LIST, BLACK LIST를 설정 하는 기능을 제공합니다.

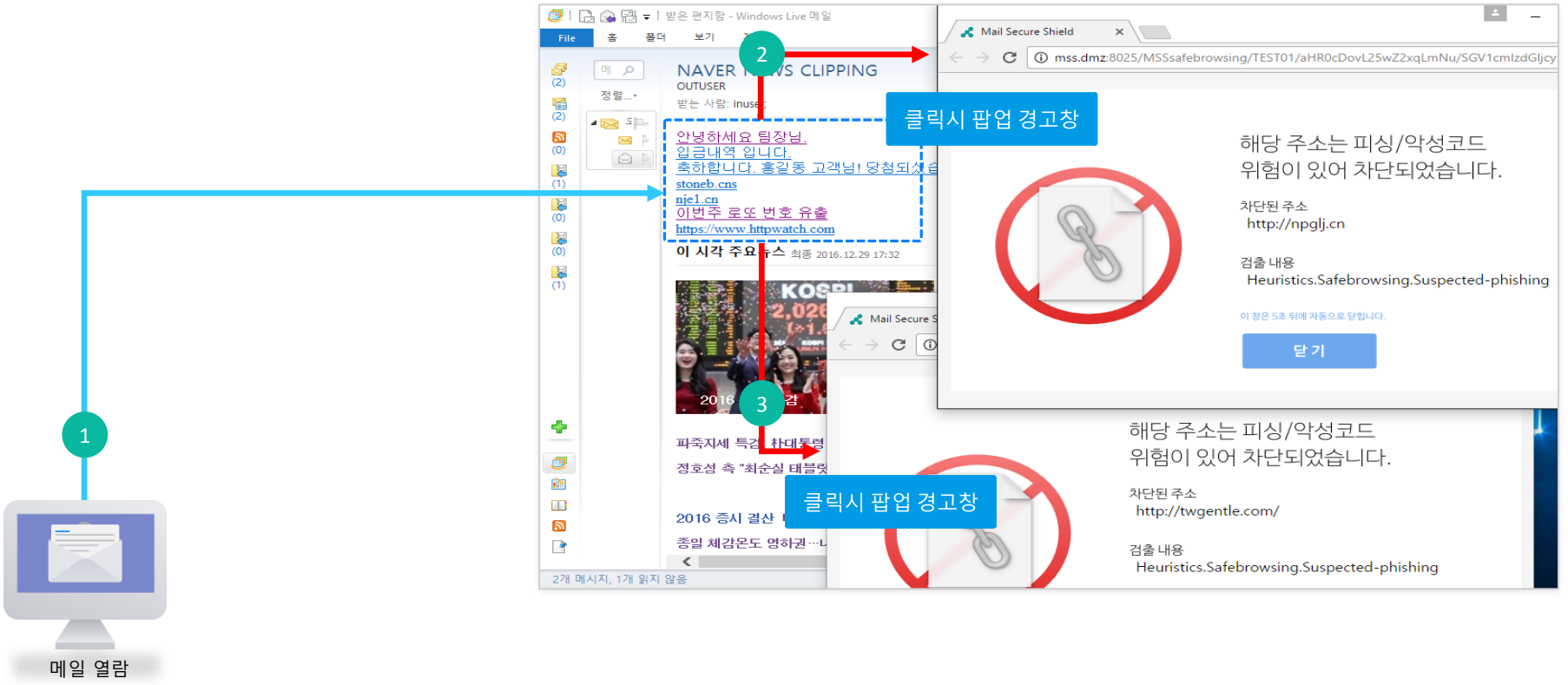
MSS 사용자 메일 수신 시 링크 변경 (safe href)

- 사용자 메일에 포함된 링크가 MSS 도메인 링크로 변경됩니다. (화이트리스트 도메인 또는 주소 제외)
- 메일 본문에 있는 텍스트 링크와 이미지 등에 포함된 링크가 모두 MSS 링크로 변경되어 사용자가 해당 링크 접속 시 MSS 를 통해 보안검사 후 통과된 링크만 접속됩니다.

MSS 사용자 첨부파일 재전송 기능

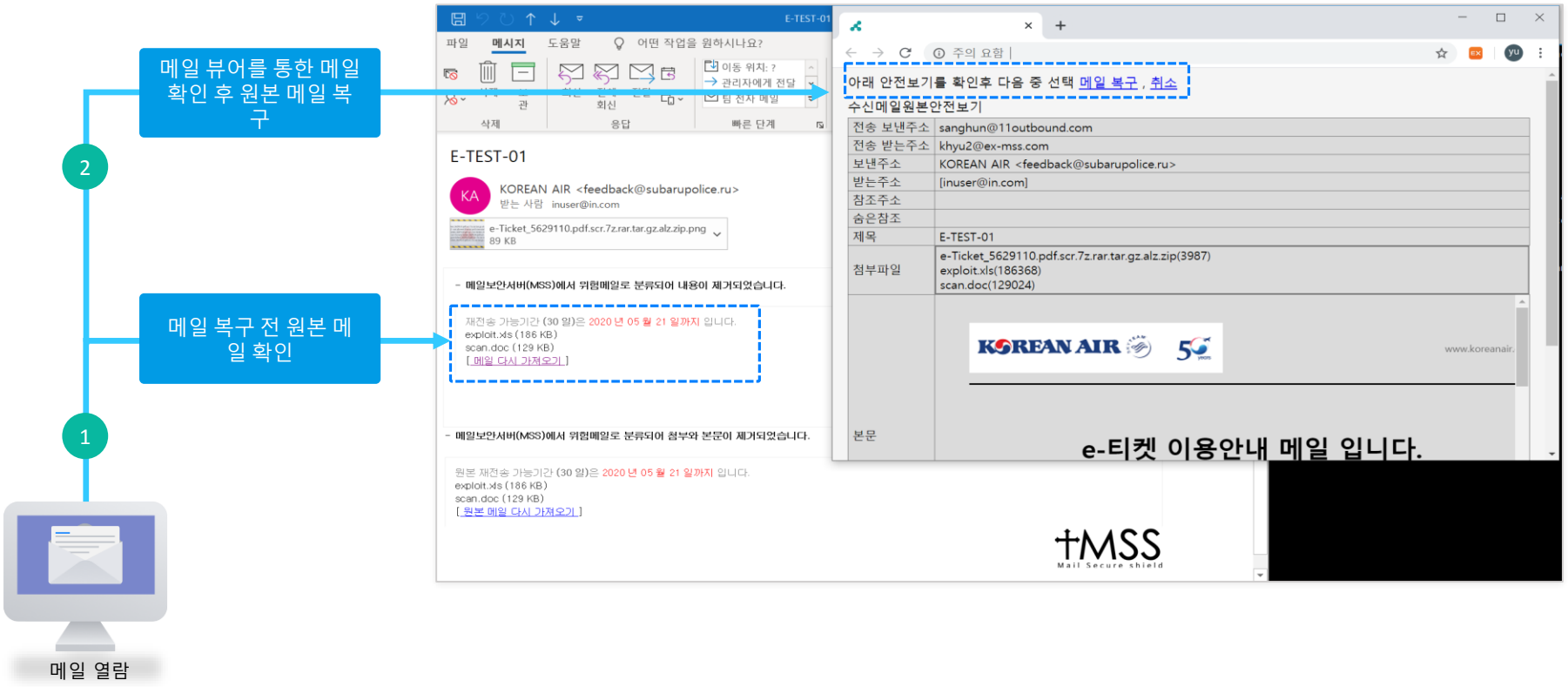
- 사용자에게 메일 수신 시 첨부파일을 제거 후 사용자 요청에 따라 첨부파일이 포함된 메일을 수신하는 "재 수신" 기능 제공
- 악성코드나 차단된 내역에 대해서만 재 전송 기능을 사용하거나 모든 첨부파일을 제거 등, 다양한 재 수신 옵션 기능 제공

MSS 사용자 UI – 실시간 링크 검사



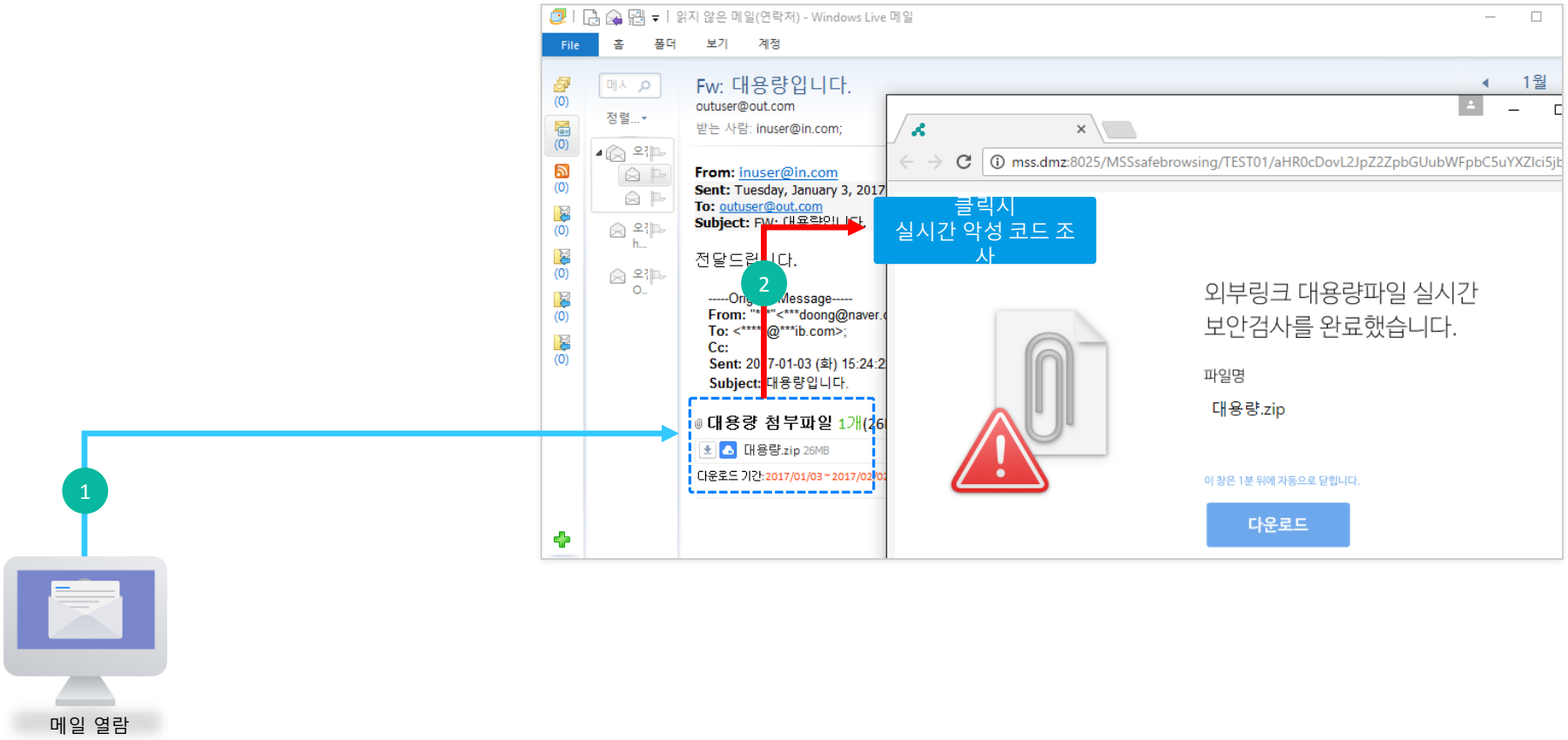
- 사용자가 메일 본문에 있는 링크를 클릭할 때 마다 실시간 검사를 수행하며 링크에 문제가 없을 경우 원래 접속주소로 재 연결 합니다.
- 사용자가 접속하는 사이트의 URL을 검사하여 피싱사이트 이거나 악의적인 컨텐츠 또는 악성코드 파일이 있을 경우 접속을 차단합니다.

MSS 사용자 메일 복구 또는 재전송 시 메일 미리보기 기능



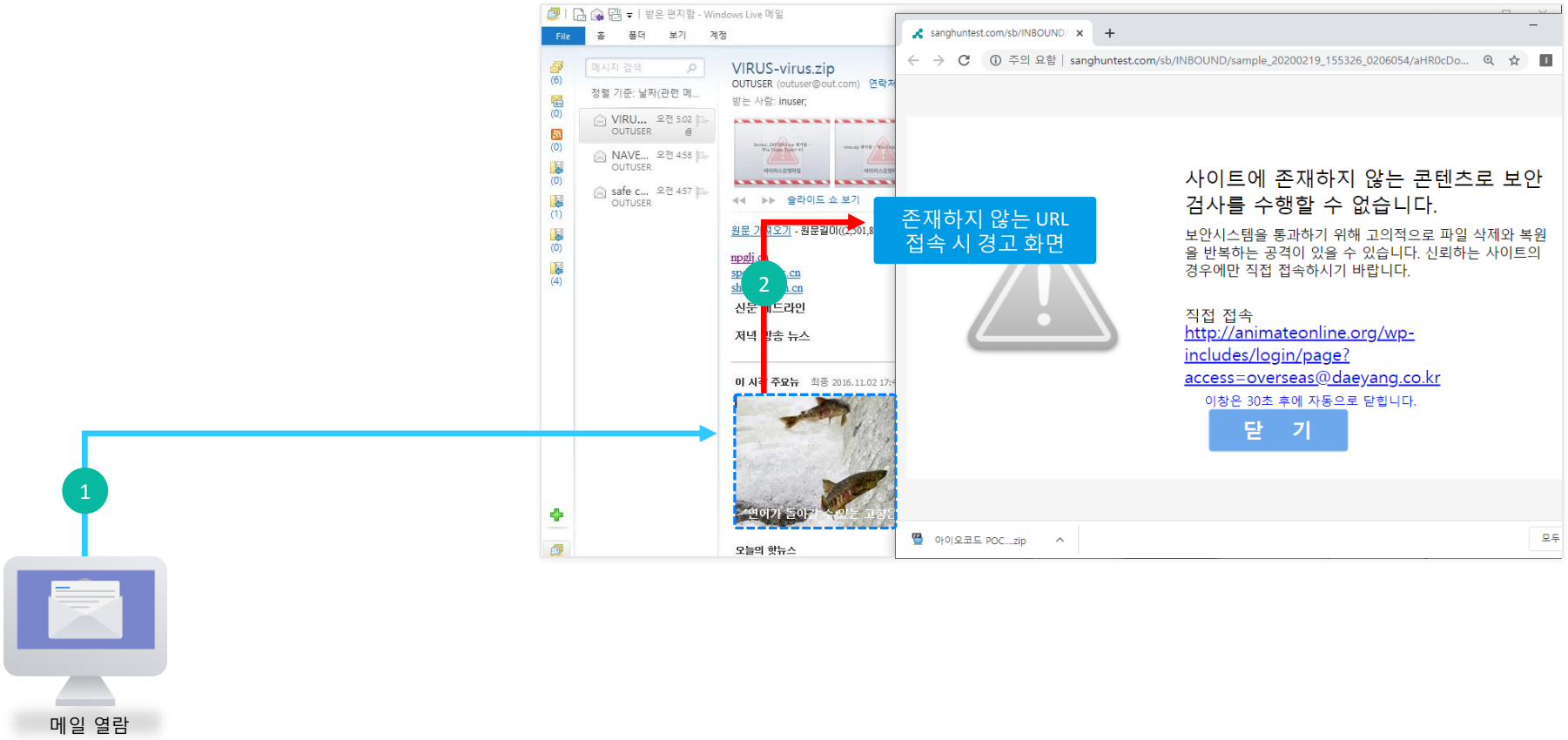
- 사용자에게 메일 수신 시 첨부파일을 제거 후 사용자 요청에 따라 첨부파일이 포함된 메일을 수신하는 "재 수신" 기능 제공
- 스팸 차단 내역에 대해 사용자에게 복구 권한 할당 시 메일 뷰어를 통한 원본 메일 확인 후 스팸 메일 복구 기능 제공
- 악성코드나 차단된 내역에 대해서만 메일 뷰어를 통한 원본 메일 확인 후 메일 복구 기능 제공 (관리자 옵션에 따른 설정)

MSS 사용자 UI – 대용량 외부링크 실시간 검사



- 대용량 외부 링크 파일에 대해서 실시간으로 보안 검사를 실시합니다. (망 분리 환경도 지원)
- 대용량 파일을 다운로드는 다운로드 할 접속 URL과 첨부파일 포맷을 WHITE LIST 또는 BLACK LIST로 관리자가 지정하여 반입 여부를 결정할 수 있습니다.

MSS 사용자 UI – 존재하지 않는 URL로 접속 시 화면 (ATP 대응)



- 메일 링크에 있는 URL의 컨텐츠가 존재 하지 않을 시 사용자에게 경고 알림 메시지를 띄웁니다. (MSS ATP에서의 제공 기능-링크 실시간 보안 검사)
- 일반적으로 해커들이 보안시스템을 통과하기 위해 해당 URL의 웹 서버를 주기적으로 ON / OFF 하여 수신 시점에 검사를 통과 하여 공격하는 방식으로 많이 사용 됩니다.

MSS 사용자 UI – 스팸 차단 리포트

스팸 차단 리포트 발송 기능

이 메시지가 표시되는 방식에 문제가 있으면 여기를 클릭하여 웹 브라우저에서 메시지를 확인하십시오.

보낸 사람: MSS server <noreply@info.mss>
보낸 날짜: 2020-02-12 (수) 오후 4:00
받는 사람: sanghun@inbound.com
참조:
제목: [메일보안] 스팸/차단 리포트 (02월 12일 16시)

스팸 리포트 메일 입니다.
읽기를 원하시는 메일은 제목 왼쪽의 '복구' 버튼을 누르세요.

요약 정보

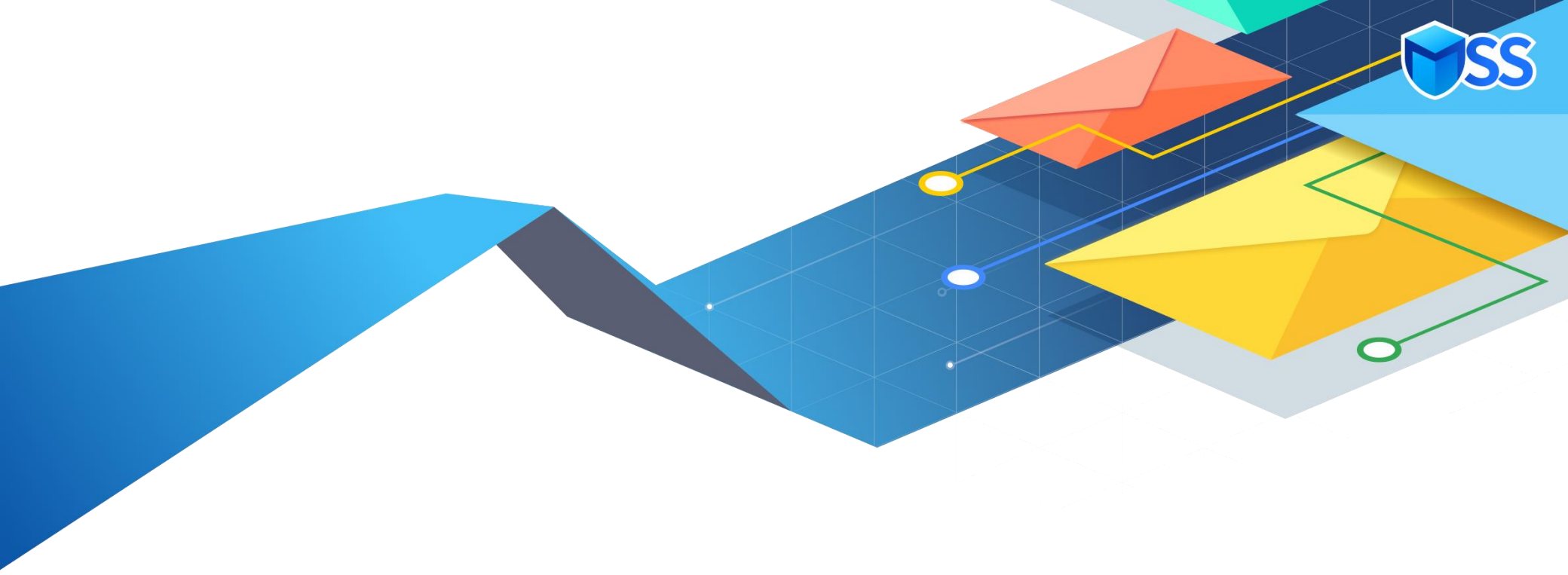
리포팅 대상 시간	2020년 02월 10일 18시 00분 01초 ~ 2020년 02월 10일 19시 00분 00초
작성 시간	2020년 02월 10일 19시 00분 08초
사용자 계정	sanghun@inbound.com

구분	스팸	바이러스	위변조차단	위험링크	합계
수신메일	1	4	1	1	7

수신된 스팸/차단 메일 목록

번호	시간	구분	제목	발신자	필터링 정보
1	18시 55분	위험파일	[복구]tttt	sanghun@outbound.com	hangul.hwp (전송차단파일-위험주소포함 전송차단...
2	18시 44분	스팸	[복구]바이낸스	sanghun@outbound.com	전송차단파일 (위변조 실행파일) https://ftp....
3	18시 41분	위험링크	[복구]URL BLACK에 URL PATTERN에 NAVER ...	sanghun@outbound.com	전송차단파일 (파일검사 불가) http://bigfil...
4	18시 37분	위험파일	[복구]	sanghun@outbound.com	GT 64비트깔기 (1).zip (전송차단파일 (위변조...
5	18시 22분	위변조	[복구]이슈파일	sanghun@outbound.com	fake.doc (전송차단파일 (위변조 실행파일))
6	18시 06분	위험파일	[복구]TEST	sanghun@outbound.com	ipscan-win64-3.5.5.no password...
7	18시 1분	위험파일	[복구]동연 검출메일	sanghun@outbound.com	검출메일.zip (전송차단파일 AV-CLAM-Do...

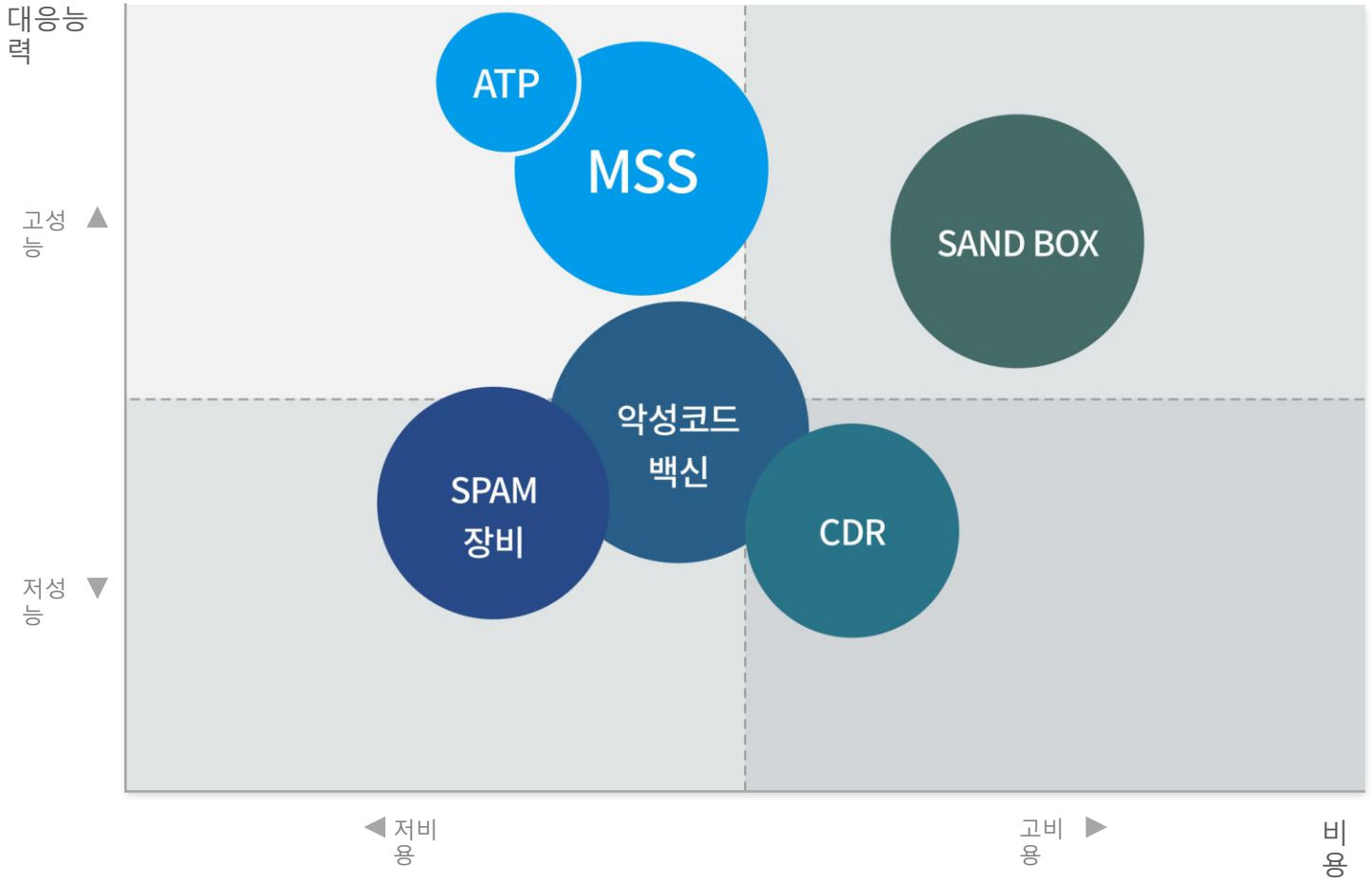
- 사용자의 업무 편의성을 위해 관리자 설정에 따라 스팸 / 악성 / 차단내역 위험 링크에 감염된 메일 현황을 사용자에게 발송할 수 있습니다.
- 발송 시간을 지정할 수 있으며 감염 유형에 따라 사용자에게 복구할 수 있는 옵션을 제공합니다.



8. 경쟁제품 비교

경쟁제품 비교

MSS는 성능과 가격을 한번에 잡을 수 있는 획기적인 차세대 메일 보안 제품입니다.



주요 메일 보안 솔루션과 기능 비교

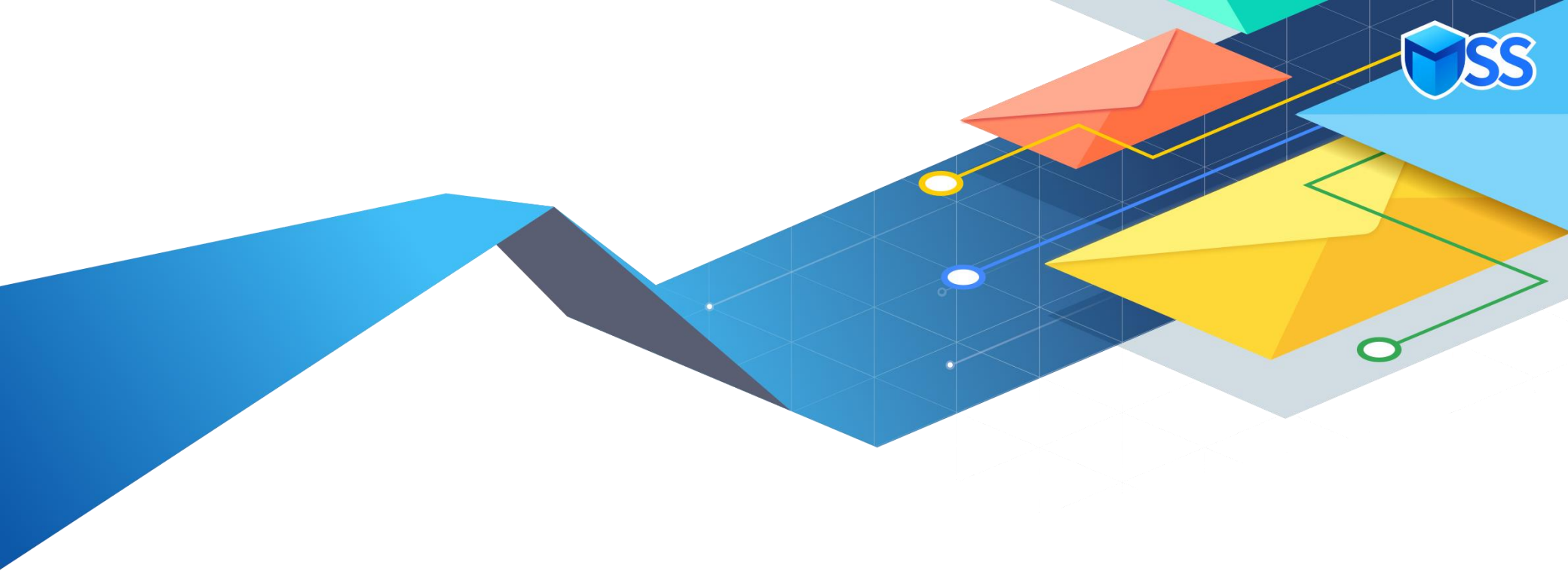
구분	MSS	TREND*	SYMAN*	FIRE*
국가	대한민국	미국	미국	미국
제품명	MSS	Email Security	Email Security.cloud	EX
설치방식	SW	SW	Cloud	어플라이언스
분류	**ALL TIME 메일보호 (등록특허5건)**	**메일수신시 백신기반**	**메일수신시 백신기반**	**ZERO-DAY대응 메일수신시 샌드박스**
PC 메일 환경	열람시 보호	수신 완료 후 연동 없음	수신 완료 후 연동 없음	수신 완료 후 연동 없음
모바일 메일 환경	열람시 보호	수신 완료 후 연동 없음	수신 완료 후 연동 없음	수신 완료 후 연동 없음
사용백신	오픈소스/ 상용백신 제조사 자체 패턴	자체 백신	자체 백신	자체 백신
메일관제	**실시간 대시보드**	**조회지원**	**조회지원**	**조회지원**
웹설정관리	지원	지원	지원	지원
메일 다중 분기	지원	미지원	미지원	미지원
이벤트기반 정책설정	지원	미지원	미지원	미지원
본문 무해화	지원	미지원	미지원	미지원
첨부문서 무해화(CDR)	**지원**	**미지원**	**미지원**	**미지원**
인터넷 이미지 처리	**지원(등록특허)**	**미지원**	**미지원**	**미지원**
파일다운로드링크	추적검사	미지원	미지원	미지원
메일 필터 (개인정보 검출)	**본문,첨부파일 개인정보 필터 기능 제공**	**미지원**	**미지원**	**미지원**
메일 박스 기능 제공	지원	미지원	미지원	미지원
메일 승인 반출 기능	제공	미지원	미지원	미지원
출시일	2017	2004	1982	2010

메일연계 솔루션 기능 비교

구분		MSS	(주)휴네시온	(주)소프트위드솔루션
보안 기능	메일연계 백신	Clamav, Kaspersky, 자체패턴	바이러스체이서	바이러스체이서
	스팸 검사 기능	Spam Assassin	없음	없음
	본문 링크 제거	지원	미흡 (메일 본문을 이미지 변환하여 링크가 삭제됨)	지원
	본문 악용 요소 제거	클릭 이벤트, Iframe, 스크립트 동영상, 하이퍼링크 등	미흡	스크립트, 하이퍼링크, Iframe 제거
	본문 및 첨부파일 제거 후 링크 첨부	지원	수신 완료 후 연동 없음	지원
	암호 설정된 압축 파일 검사 기능	암호가 알려진 암호 또는 메일 본문에 존재 시 검사 기능 제공	자체 백신	자체 백신
	개인정보 필터 기능	자체 개인정보 필터 기능 제공 (메일 본문, 첨부파일)	미지원	미지원
	인터넷 이미지 처리	지원(등록특허) : 메일 본문 결합 및 내부 이미지 캐싱 서버 기능 제공	미흡	메일 본문 결합만 가능
	대용량 링크 첨부 다운로드 기능	지원 (다운로드 받을 URL 및 포맷을 White List, Black List로 지정)	미흡	미흡
	CDR 기능	MSS CDR을 통한 기능 지원 (별도 유상 제품)	미지원	미지원
	SANDBOX 기능	MSS SANDBOX를 통한 기능 지원 (별도 유상 제품)	미지원	미지원
	메일 링크 실시간 검사	MSS ATP를 통한 기능 지원 (별도 유상 제품)	미지원	미지원
사용자 편의 기능	본문 이미지 삽입 기능	지원	미지원	지원
	제목 및 본문 편집 기능	지원	미지원	미흡
	Agent 필요 유무	불필요	필요	불필요
	수신자, 발신자 리스트 확인	지원	미흡	지원
	첨부파일 재전송 기능	지원	미흡	지원
	그룹 계정 분기 기능	지원 : 그룹 계정에 속한 사용자 계정 별로 별도의 링크 생성	미흡	미흡

메일연계 솔루션 기능 비교 (계속)

구분		MSS	(주)휴네시온	(주)소프트위드솔루션
메일 전송 기능	다중 전송 기능	지원	미지원	미지원
	시간(요일, 시간)별 전송 컨트롤 기능	지원	미지원	미지원
	메일 발신 시 SFP 레코드 조회 후 인터넷으로 메일 직접 발송	지원	미지원	미지원
	파일 변환 저장 기능	지원	지원	미지원
	대략 메일 처리 성능	우수	미흡	보통
관리기능	실시간 통합 대시보드	지원 (실시간 모니터링 대시보드 제공)	미지원	미흡
	실시간 자원 사용량 모니터링 기능	지원	미지원	미지원
	다중 정책 설정 기능	지원	미지원	지원
	정책 분기 설정 기준	도메인, 계정, 발신서버 IP, 제목, 메일 헤더 등	미지원	미지원
	수신 메일 조회 기능	지원	미지원	미지원
	실시간 메일 처리 위치 확인 기능	지원	미지원	미지원
	실시간 예외 정책 추가 기능	지원	미지원	미지원
	실시간 처리 메일 정책 이동 기능	지원	미지원	미지원
	메일 처리 성능 튜닝	지원 (수신, 검사, 전송 큐를 논리적 변경 지원)	미지원	미흡



9. MSS 전체 기능 요약

MSS 주요 기능 요약 (1/2)

All Time Protection

- 시간이 지난 뒤 변조되어 위협이 되는 이슈에 대해서도 실시간 검사를 통해 보안이 가능함.
  (피싱 사이트, 웹다운로드 추적 악성 / 위·변조 검사)

악성링크 보안

- 링크가 연결되어 있는 주소는 MSS가 미리 악성코드 검사
- 본문 및 첨부파일에 있는 URL까지 검사, 추가 위험성 사전 차단
- 악성링크는 차단 및 사용자에게 경고 메시지

랜섬웨어 차단

- 기존 메일 보안 솔루션 취약점 보안
- 메일의 안전한 본문만 재조립하여, 안전성 100% 확보
- 첨부파일은 링크로 제공하고, 외부링크는 미리보기 및 URL 주소를 알려줘 악성사이트 여부를 사전에 인지

바이러스 / 위변조 검사

- 첨부파일에서 악성코드가 검출되면 검출 정보를 이미지로 제공하여 필요한 메일의 미 수신 상황으로 인한 불필요한 시간 낭비를 방지

유사도메인 비교 / 검사

- 기존 도메인과 유사성 비교 분석
- 위험계정일 경우 비교분석 후 경고

스팸 / 스캠 검사

- 확인되지 않은 발신자 차단
- 수신메일의 스팸 / 스캠 유무 확인 및 재수신 기능 (Spam Assassin)

대용량 파일 실시간 검사

- 본문 외부링크 대용량 파일을 클릭시 마다 실시간 악성 코드 검사

위 / 변조 파일분석, 무결성 검사

- ppt, DOC, XLS, HWP, PDF등 오피스파일 및 자주 사용하는 문서 파일로 위장한 악성코드와 바이러스 검출
- 다운로드 전송시점 백신 재검사
- 다운로드 전송시점 메일파일원본 무결성 확인

MSS 주요 기능 요약 (2/2)

발송된 경로 추적

- 수신 메일 별 발송된 경로 정보 제공
- 국가별, IP정보 등 제공

다중화 구현

- 이중화 및 다중화를 지원하여 시스템의 높은 가용성과 안정성을 확보

발신 메일 보안 검사

- 메일발송 시 수신 메일과 동일한 과정으로 보안검사 (바이러스, 피싱, 악성코드 등)를 거친 뒤 발송됨.

리포트 기능

- MSS에서는 데일리 리포트 기능을 제공합니다.
- XLS 확장자로 파일 다운로드 제공
- 메일 관리 기능 : 수신 내역 조회, 메일 차단 내역 등 제공

피싱 유무 검사

- 메일 본문 링크의 피싱 유무 검사
- 첨부파일안의 피싱 유무 검사(텍스트,오피스,PDF)

메일흐름 실시간 정보 제공

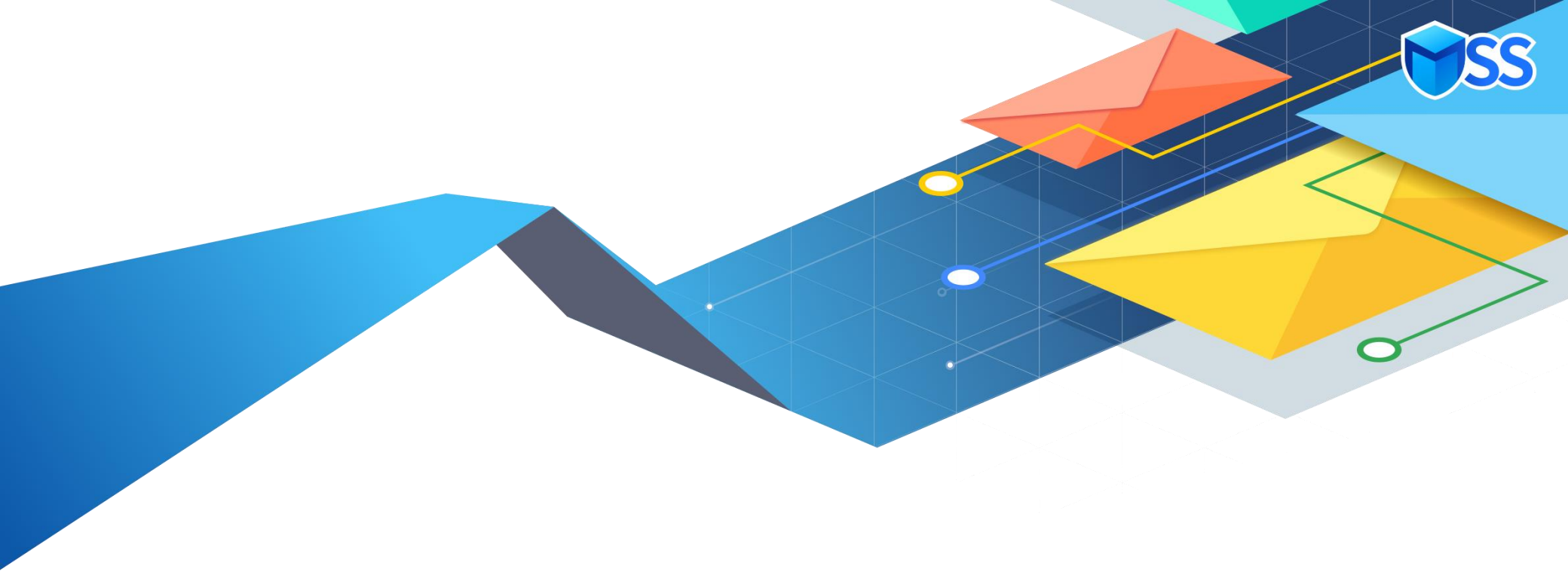
- 실시간 대시보드를 통한 메일 보안 상황 실시간 관리
- 실시간 시스템 사용량 모니터링으로 효율적 자원관리

망분리환경 메일 연계

- 망분리 환경에서 외부 메일을 내부로 연계하여 메일전달
  - 원본 메일 동일 형태 유지 (파일로 분해, 재조립)
  - 메일 이미지 형식
  - PDF 문서 형식

서버취약점 평가표 제공

- 법적 규제 준수에 부합하는 기술적취약 분석 및 평가
- 자동화 된 보안 평가표 제공



10. 구축사례 & 특허

MSS 주요 구축 사례

금융

- 참! 좋은 은행 IBK기업은행
- Cigna 라이나생명
- 한화손해보험
- 현대차투자증권

제조

- DK 동국산업
- CTR 센트랄
- OHSUNG ELECTRONICES CO.,LTD.
- DAE SUN
- DAEYANG ELECTRIC CO.,LTD.
- CHEIL ELECTRIC

공공

- APCC APEC CLIMATE CENTER

대학교

- 경남대학교 KYUNGNAM UNIVERSITY
- 동의대학교 DONG-EUI UNIVERSITY

MSS 특허정보

특허 10-1847381

1. 이미지캐싱 특허

특허 10-1885156

2. 망분리 환경에서 원본 메일 수신 특

특허 10-1934516

3. 세이프링크 특허

특허 10-1989509

4. 메일분석 특허

특허 10-1959534

5. 메일 열람시 마다 보안검사 특허

특허 10-2164338

6. 발송자 사칭 방지를 위한 특허

등록번호 10-1847381 : 전자메일 제공 시스템 및 그 방법

등록번호 10-1885156 : 원본상태의 전자메일 제공시스템 및 그 방법

등록번호 10-1934516 : 메일열람 시 보안을 위한 전자메일처리시스템

등록번호 10-1989509 : 전자메일 가공 시스템 및 방법

등록번호 10-1959534 : 전자메일 보안 시스템 및 그 방법

등록번호 10-2164338 : 발송자 사칭을 방지하기 위한 전자메일 보안 시스템 및 그 방법