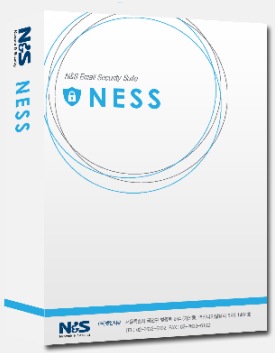
AI 분석기반의 이메일 위협대응솔루션

NESS

2022년

㈜넷엔씨큐

목차



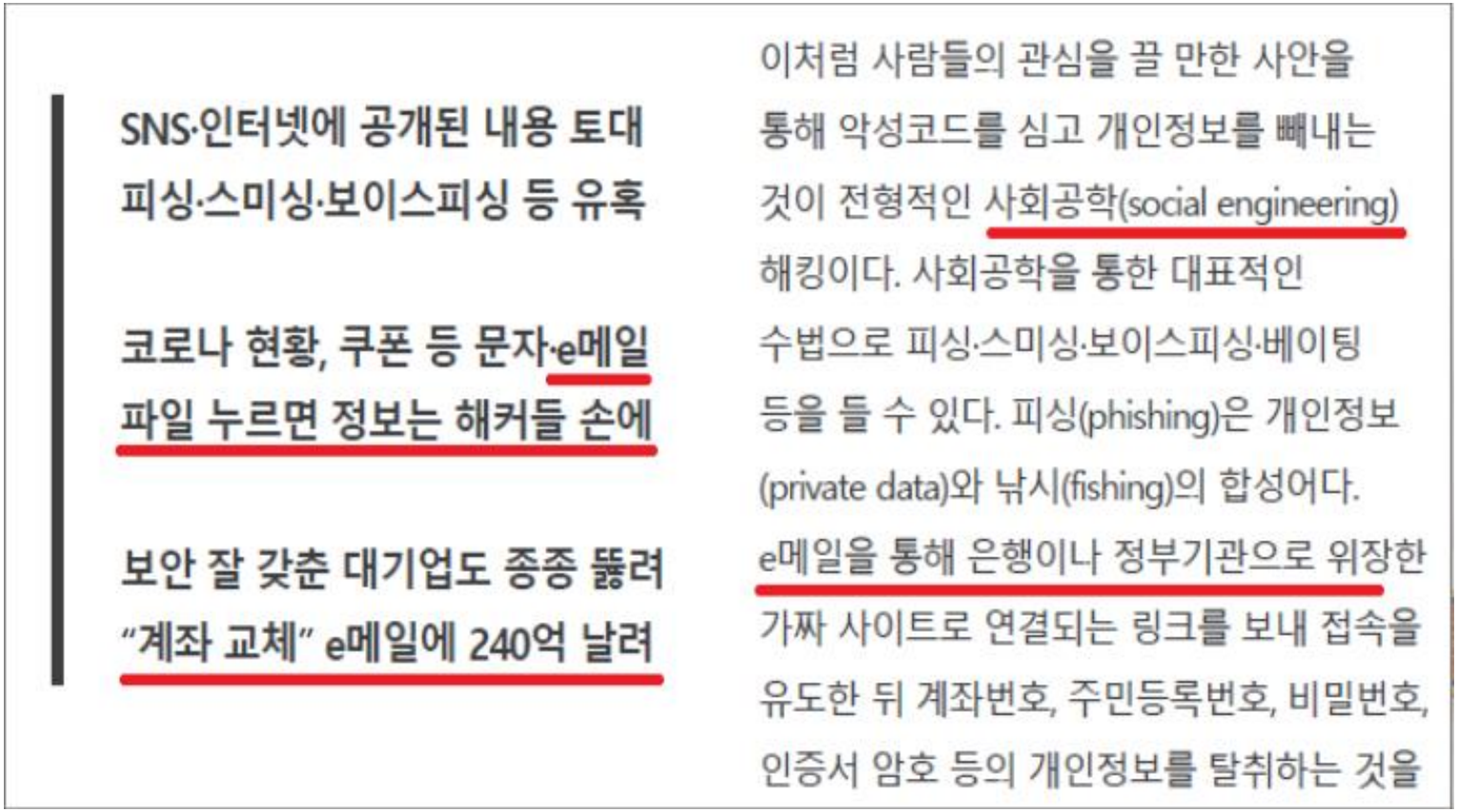
1. 제안배경

증가되는 이메일 보안위협

- 샌드박스를 우회하는 멀웨어
- 금전요구, 공공기관 사칭 스캠메일

신종 이메일 보안위협 증가

- 사회공학[1]을 이용한 사기메일 - 중앙일보 2020년 2월 22일 기사



SNS·인터넷에 공개된 내용 토대
피싱·스미싱·보이스피싱 등 유혹

코로나 현황, 쿠폰 등 문자·e메일
파일 누르면 정보는 해커들 손에

보안 잘 갖춘 대기업도 종종 뚫려
"계좌 교체" e메일에 240억 날려

이처럼 사람들의 관심을 끌 만한 사안을 통해 악성코드를 심고 개인정보를 빼내는 것이 전형적인 사회공학(social engineering) 해킹이다. 사회공학을 통한 대표적인 수법으로 피싱·스미싱·보이스피싱·베이팅 등을 들 수 있다. 피싱(phishing)은 개인정보(private data)와 낚시(fishing)의 합성어다. e메일을 통해 은행이나 정부기관으로 위장한 가짜 사이트로 연결되는 링크를 보내 접속을 유도한 뒤 계좌번호, 주민등록번호, 비밀번호, 인증서 암호 등의 개인정보를 탈취하는 것을

1) 사회공학: 고도의 기술과 장비를 통한 컴퓨터 해킹과는 달리 사람을 속여 정보를 빼돌리는 기법으로 인간의 기본적인 신뢰를 악용하는 것

신종 이메일 보안위협 증가 (계속)

- 문서 형태의 공격 증가 - 중앙일보 2020년 2월 22일 기사

김수키 해커그룹, HWP·DOC·EXE 복합 APT 공격 실시

doc 문서 포맷을 이용한 공격사례 분석

DOC 악성문서는 처음 실행 시 PROTECTED DOCUMENT 내용을 보여주면서, 마치 문서의 보안기능 때문에 본문이 안 보이는 것처럼 속인다. 그리고 '콘텐츠 사용' 버튼을 클릭해 악성 매크로 코드가 작동하도록 유인한다.

한편, 만약 이용자가 보안 경고를 무시하고, '콘텐츠 사용' 버튼을 클릭할 경우 악성코드가 실행된다. 그리고 정상적인 본문 내용을 보여주어 정상적인 문서로 오인하도록 만든다. 해당 문서의 만든이는 'Robot Karll'이란 사람으로 되어 있는데, 이 계정은 김수키 공격그룹이 사용한 다수의 침해사건에서 목격되고 있다.

- 샌드박스 보안장비를 우회하는 공격 증가 - 보안뉴스 2018년 7월 12일 기사

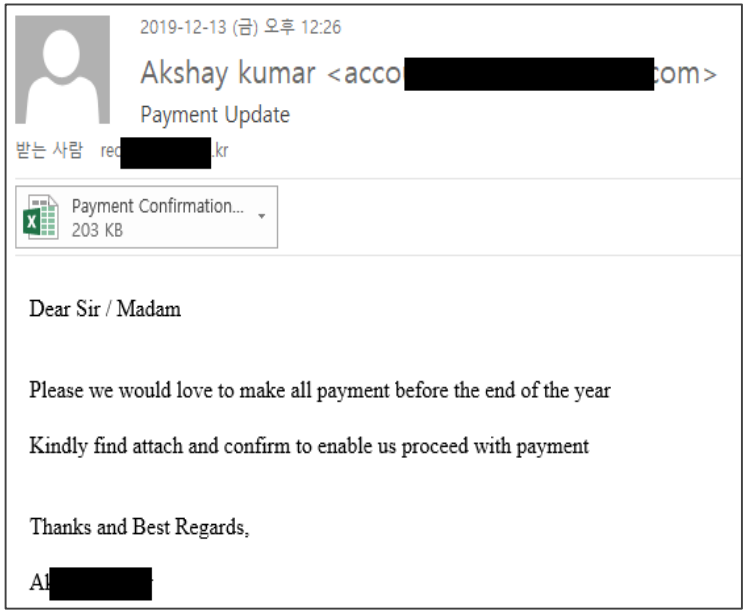
스펙터의 새 변종 등장! 원격 코드 실행과 샌드박스 우회

연구원들은 두 번째 스펙터 변종도 발견했다. 공격자가 Read/Write PTE 플래그를 우회할 수 있도록 해주는 것으로, 이를 성공적으로 익스플로잇 할 경우, 멀웨어가 보안용 샌드박스를 빠져나갈 수 있도록 해준다고 한다.

신종 이메일 형태

무역대금 요구

무역대금을 요청하는 사기메일
송금을 요청하는 내용 있음
첨부파일이 포함되어 있는 형태
첨부가 없는 형태도 다수 있음



공공기관 사칭

국세청을 사칭한 메일
송신자나 본문의 내용을 보면 정상적으로 보이나 본인과 관계가 없는 메일

신종 이메일 형태 (계속)

- 샌드박스 우회 공격

공격시점을 1시간 이후 혹은 특정 시점으로 설정

1시간뒤에 실행 되는 멀웨어

탐지안됨

악성행위를 1시간 이후 실행하도록 함

가상환경(VM)을 인지하여 실행하지 않도록 함

가상환경에서 멀웨어가 실행되지 않도록 제작

탐지안됨

멀웨어가 가상환경에서는 실행되지 않음

기존 솔루션의 문제점과 해결방안

기존 솔루션	탐지 방법	문제점	해결방안
샌드박스	가상환경(VM) 에서 멀웨어를 실행하고 행위를 분석하여 차단	샌드박스를 우회하는 멀웨어 증가	• 샌드박스를 우회하는 멀웨어 차단 기술 필요 (신변종 멀웨어 차단 기술) • 탐지과정없이 보안취약점을 원천제거하는 기술 필요 (CDR 기술)
스팸차단	IP 기반, 키워드 기반, 패턴 기반으로 스팸메일을 차단	키워드, 패턴만으로는 사기성 스캠 메일 차단 어려움	• 송신자에 대한 신뢰도를 판단하고 유사도메인을 차단하는 기술 필요 (스캠 차단 기술)

해결방안의 제품화 !

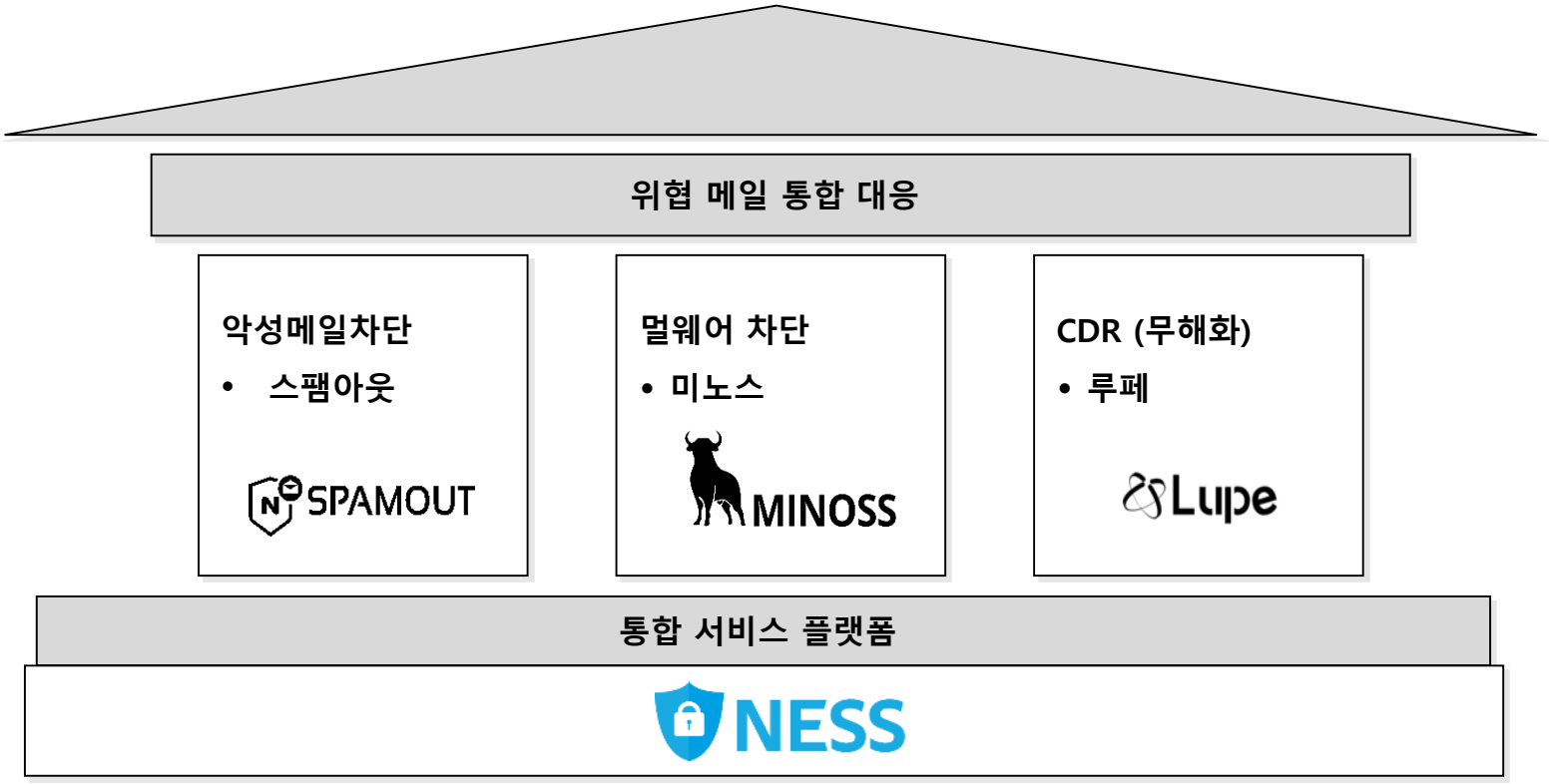
NESS

Netnsecu Email Security Suite

코드 DNA 유사도 분석 기반의 이메일 위협대응솔루션

- 샌드박스를 우회하는 멀웨어 차단
- 위·변조 탐지 및 무결성 검사, 그리고 컨텐츠 무해화(CDR)
- 사기성 스캠메일 차단
- & 악성메일 (스팸/ 바이러스/ 랜섬) 차단필터 기본 제공

악성메일차단 + 멀웨어차단 + CDR



 # NESS는 특허받은 멀웨어차단 엔진 '미노스'와 컨텐츠무해화 CDR 엔진 '루페' 그리고 CC 인증의 스팸메일 차단 엔진 '스팸아웃' 을 통합 플랫폼으로 제공합니다.

2. 제품소개

S/W 구성

시스템 구성

미노스 기술

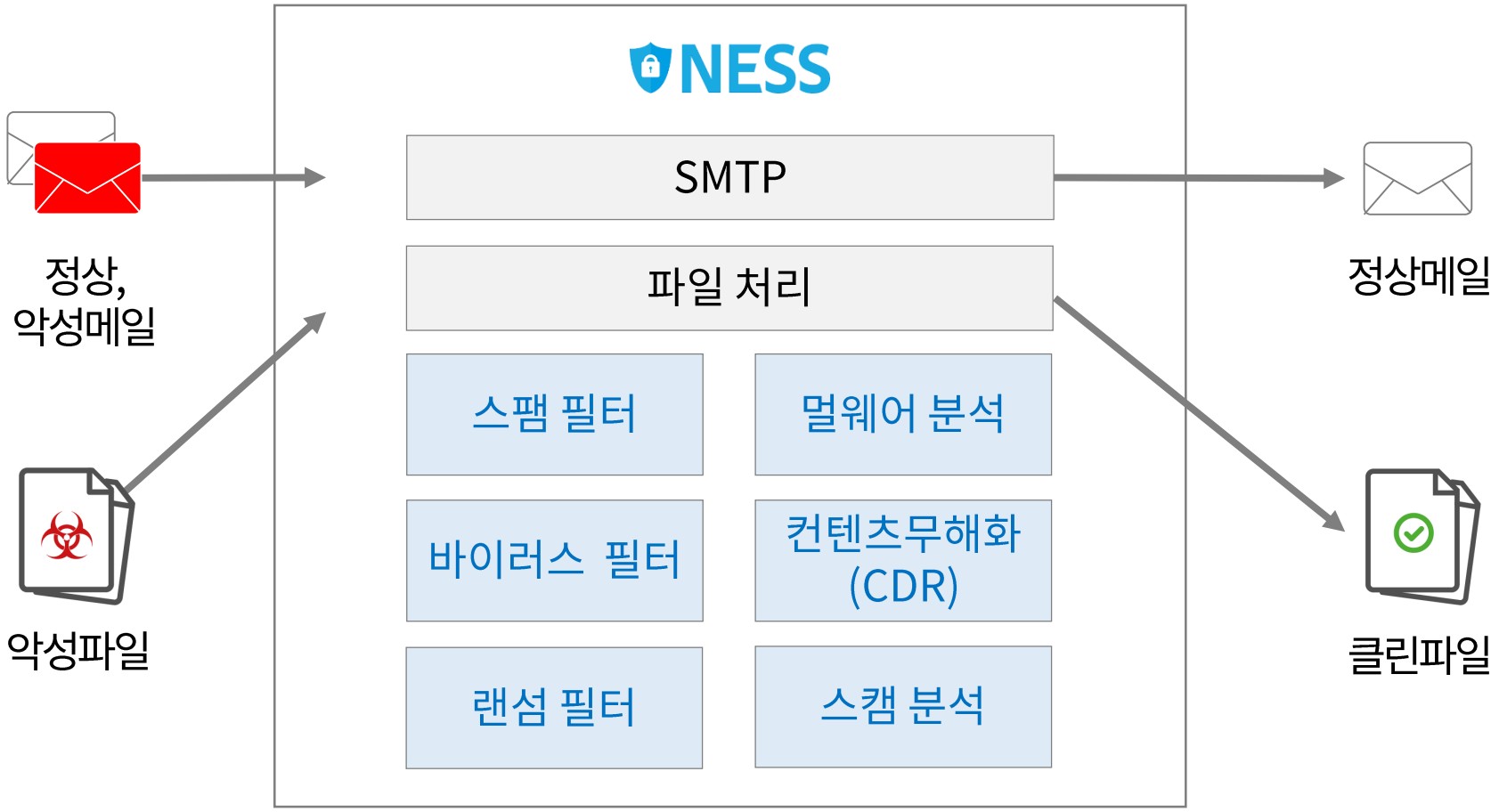
사기성 스캠메일 차단

보안위협을 원천 제거하는 CDR 엔진

스팸/바이러스 메일 차단

구축사례

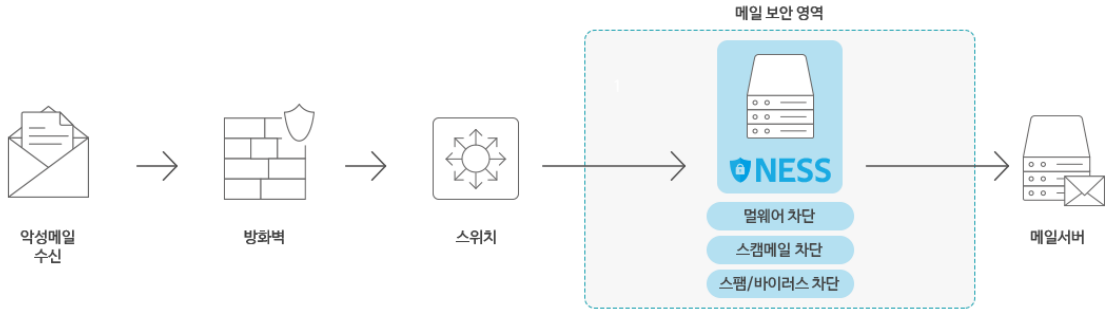
S/W 구성


NESS
SMTP
파일 처리
스팸 필터
멀웨어 분석
바이러스 필터
컨텐츠무해화 (CDR)
랜섬 필터
스캠 분석
정상, 악성메일
악성파일
정상메일
클린파일

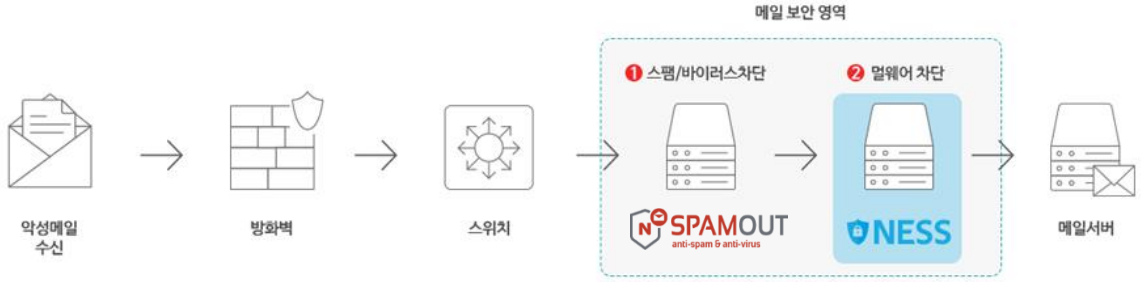
시스템 구성

스팸아웃과 융합하여 통합메일보안시스템 구성

스팸아웃 +NESS 일체형



스팸아웃 +NESS 분리형



- 고객 환경에 따른 맞춤형 구성 지원

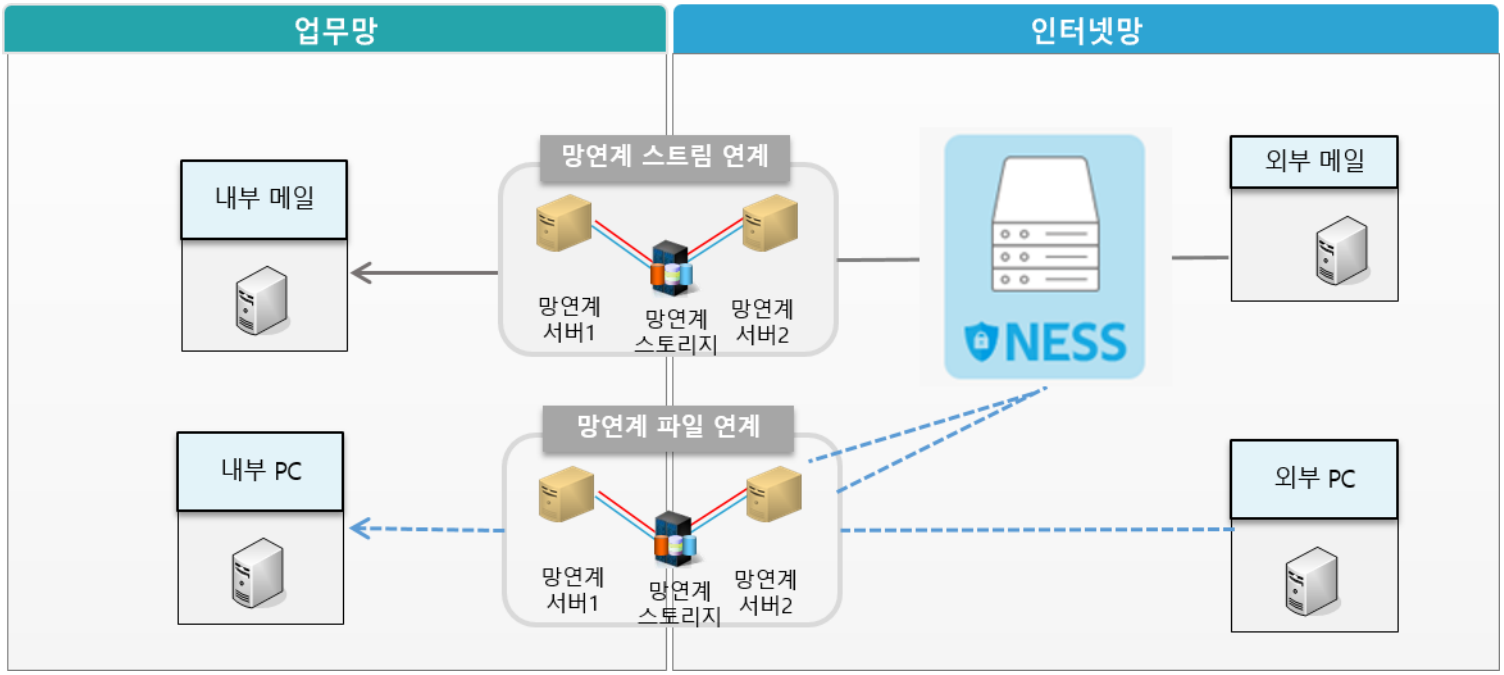
시스템 구성 (계속)

1차는 NESS, 2차는 APT에서 차단하는 구조

- 이중 구성 및 엔터프라이즈급 다중 구성 지원
- Microsoft AZURE, AWS, NAVER Cloud 등 Public 클라우드 에서 구성 지원
- Microsoft 365, Google Workspace 등 공유 이메일 서비스에서 구성 지원

시스템 구성 (계속)

망연계 솔루션 구성



- 망간 메일 전송 : 외부메일서버 → NESS → 망연계 → 내부메일서버
- 망간 자료 전송 : 외부망 PC → 망연계 → NESS → 망연계 → 내부망 PC

신·변종 멀웨어를 차단하는 MINOSS 기술

MINOSS

사이버 위협 DNA를 수집하고 학습하여
보안사고를 사전예방하는 누리랩의 멀웨어 분석 플랫폼

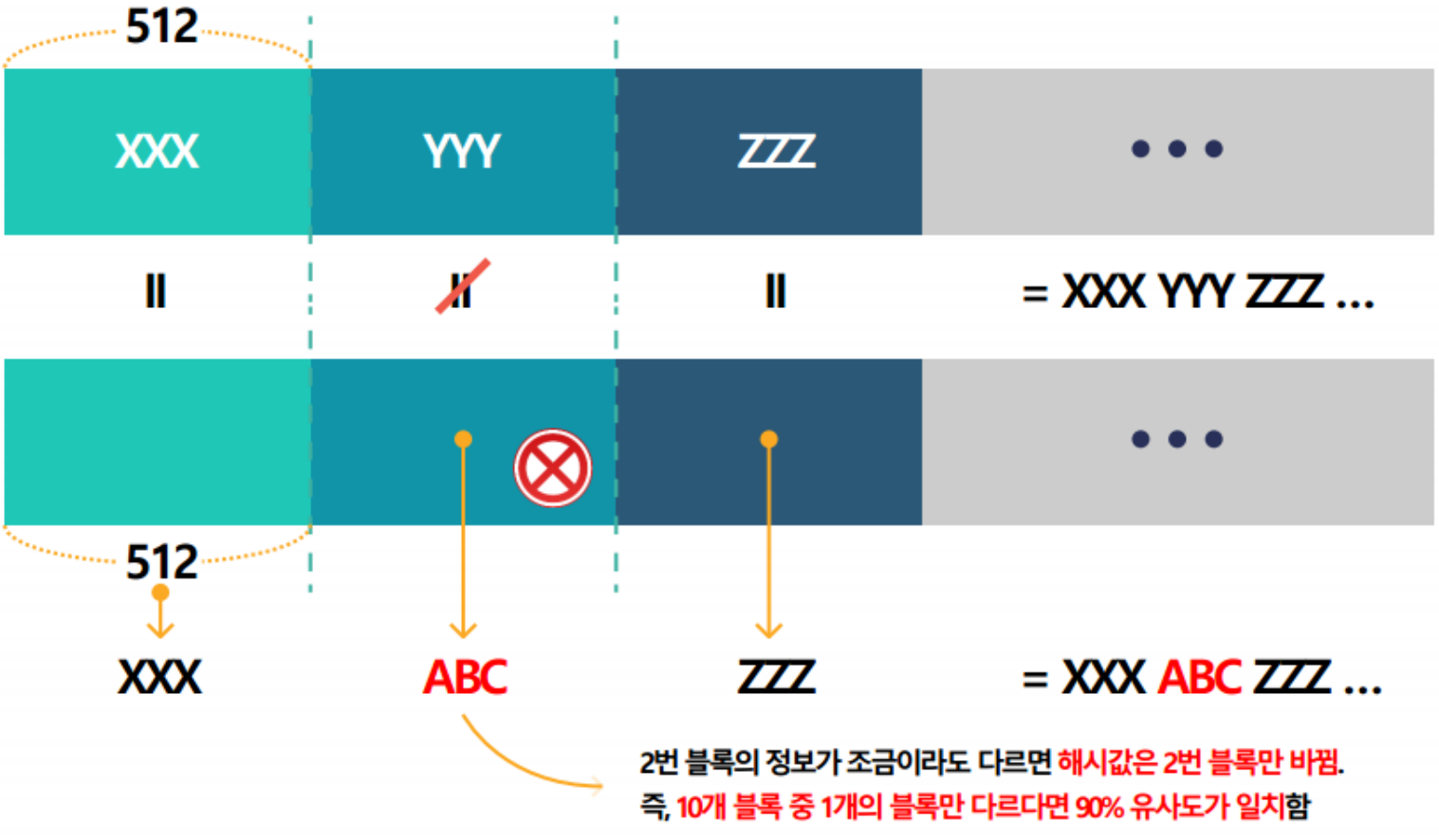
MINOSS 기술

1. 일일 50만건이상의 데이터를 수집
2. 데이터 분류 및 DB 구축
3. DB에서 빠르게 유사도를 찾아서 차단

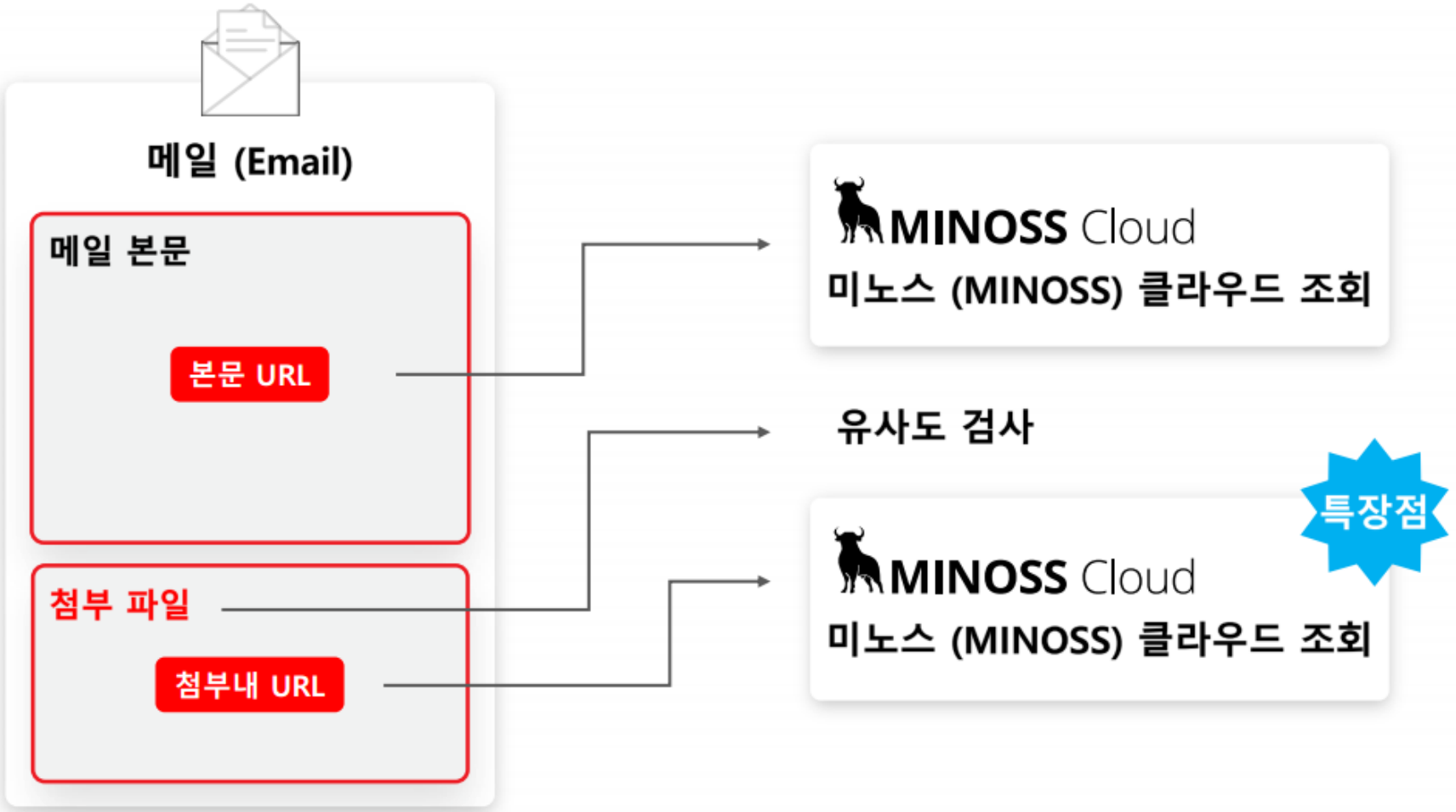
역 색인 구성방법, 역 색인을 이용한 유사 데이터 검색 방법 및 장치
[특허 제 10-2081867호]

유사도 분석 기술

- 대부분의 신·변종 악성코드는 과거 만들어진 소스코드를 살짝 수정하는 정도
- 코드의 유사도를 측정하면 신·변종 악성코드를 쉽게 판별할 수 있음

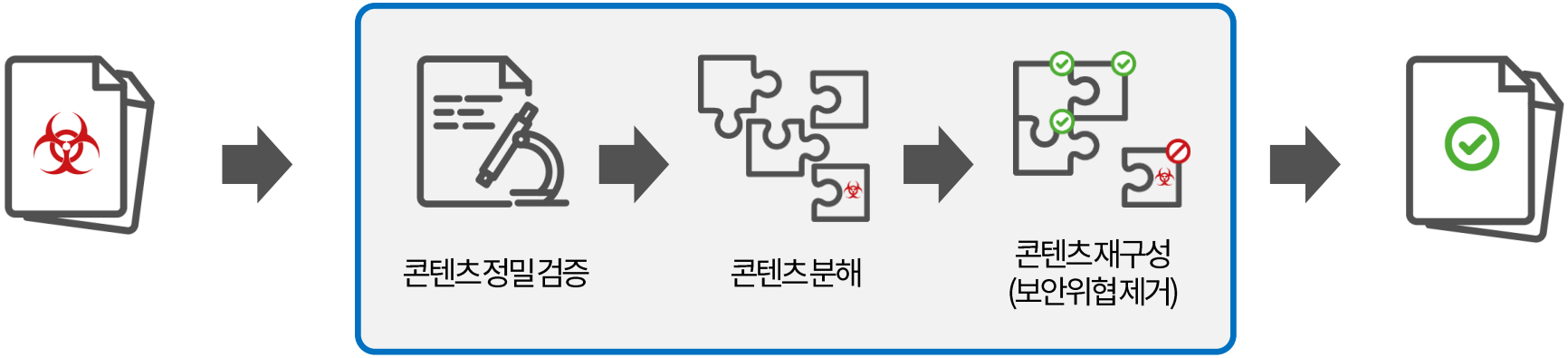


메일 본문 URL, 첨부, 첨부 내 URL 까지 탐지



잠재적 보안위협을 원천제거 하는 CDR 엔진

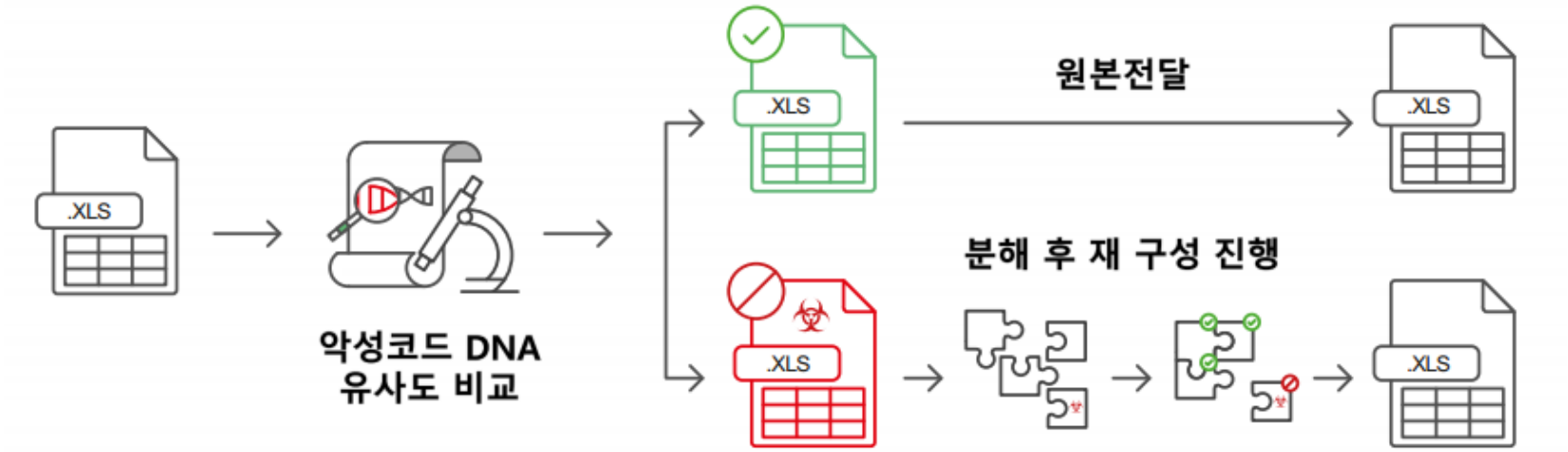
- CDR[1] 은 보안위협을 제거한 후 클린한 파일로 재조합하는 기술
- 탐지에 의존하지 않는 기술로 잠재적 보안위협을 원천제거
- 글로벌 IT 자문기관 '가트너'에서는 CDR 사용을 권고하고 있음



1) CDR : Contents Disarms and Reconstruction, 파일 무해화 및 재조합 기술

NESS CDR 엔진의 특징 1

- 외산 제품이 지원하지 않는 egg, alz(알집) 포멧도 지원
- 총 8종의 압축 포멧 지원 (zip, 7z, alz, egg, tar, bz2, gz, xz)
- 다중 압축 지원 (7z 파일을 zip 으로 압축한 경우)
- 엑셀 매크로 파일 → 악성코드 유사도 엔진으로 정상 or 악성 여부 판별



NESS CDR 엔진의 특징 2.

- **매크로 유사도 분석 기술로 원문의 완전성을 보장.**

- 복잡한 표도 완벽하게 재구성

  → 타사는 정상 콘텐츠를 추출하여 새롭게 파일을 구성하여 파일이 깨질 수 있음

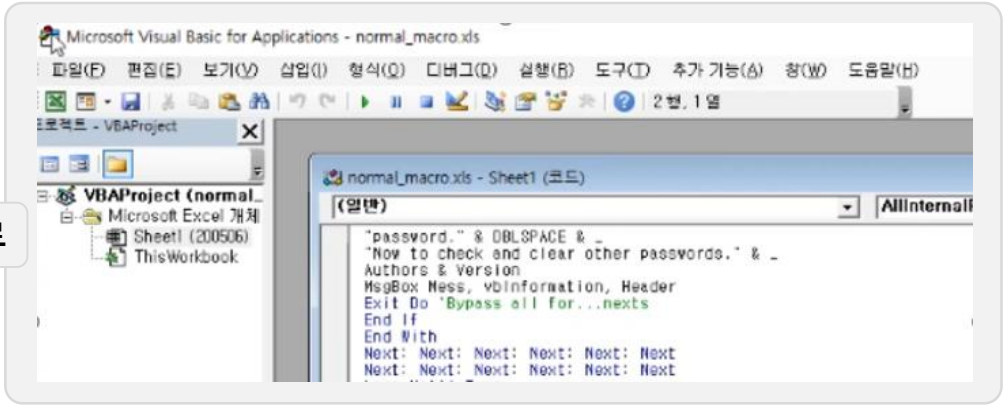
  → NESS는 악성 콘텐츠만 제거하여 원문의 완전성을 보장함.

- 정상적인 엑셀 매크로도 안전하게 재구성

  → 엑셀의 매크로는 CDR 처리 대상으로 타사 CDR은 정상 매크로를 삭제함

  → NESS는 악성 매크로 여부를 체크하여 악성 매크로가 아니면 CDR 처리를 하지 않음

NESS로 CDR 처리한 매크로



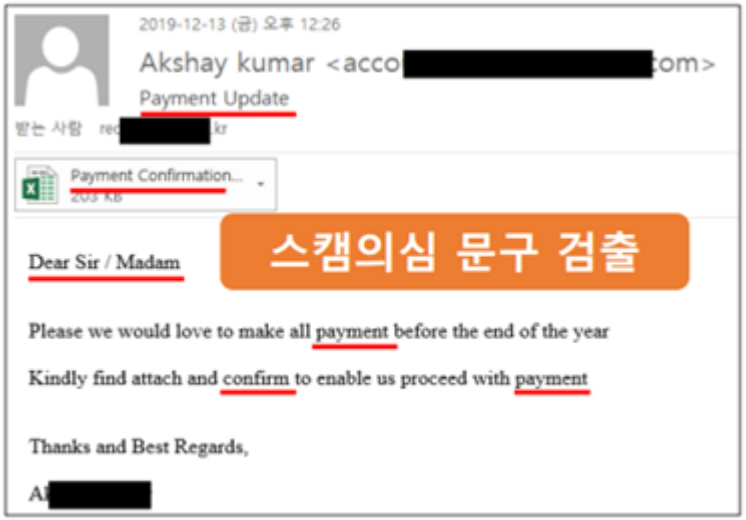
사기성 스캠메일 차단

① 계정별 메일이력 정보 구축

- 발신자, 수신자 간 1:1 매핑으로 학습 정보 구축
- 학습정보를 기반으로 유사도 검사를 수행하고 특정 퍼센트(%) 이하이면 차단 처리

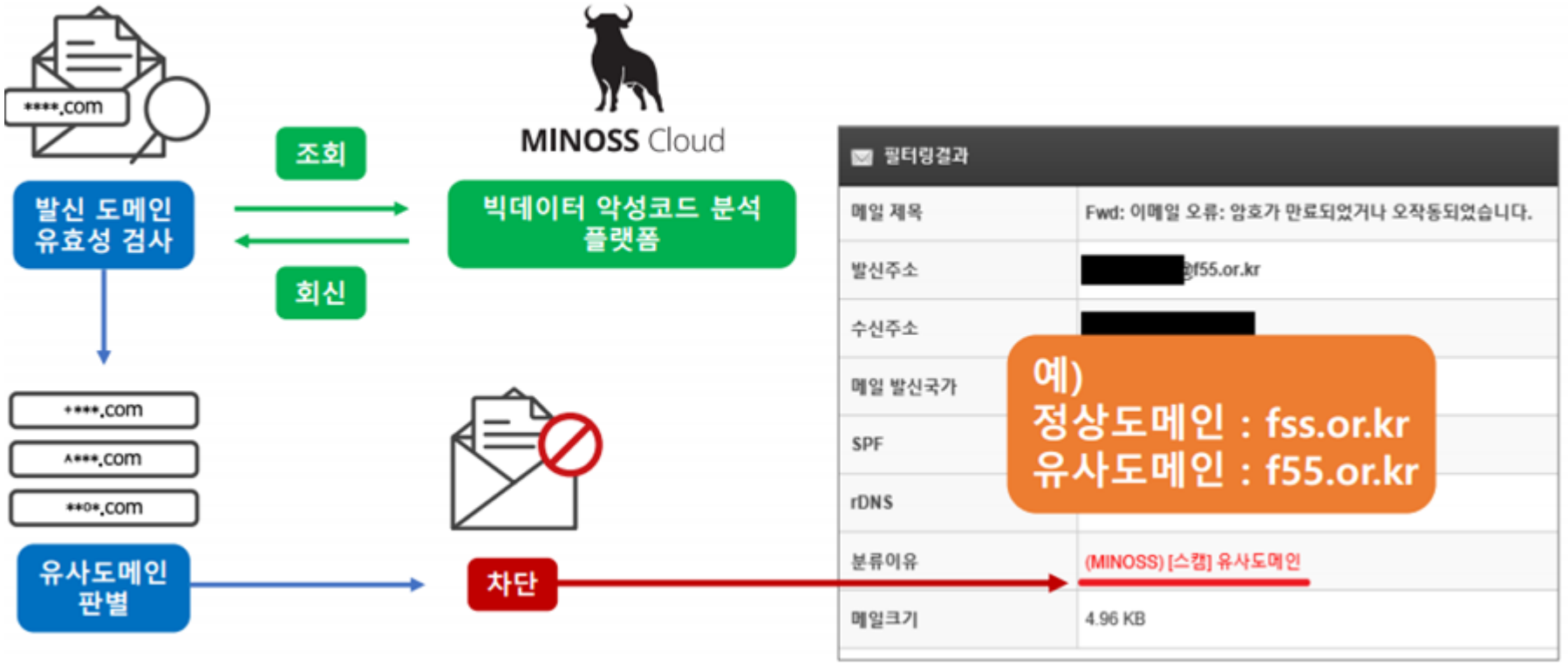
② 스캠의심 단어 검사

- 메일의 제목, 본문, 첨부파일의 형태를 검사하여 스캠의심 문구 검출



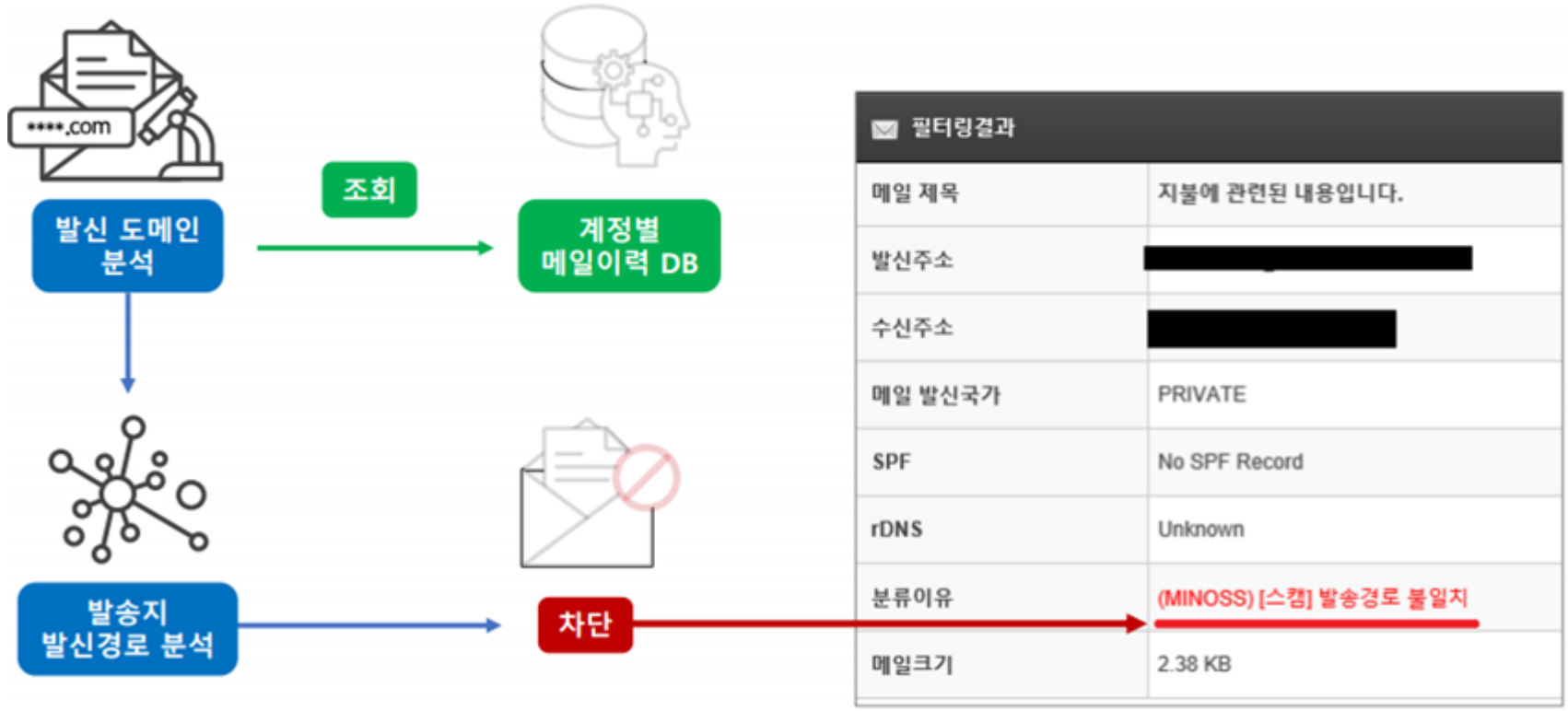
사기성 스캠메일 차단 (계속)

③ 유사도메인 차단



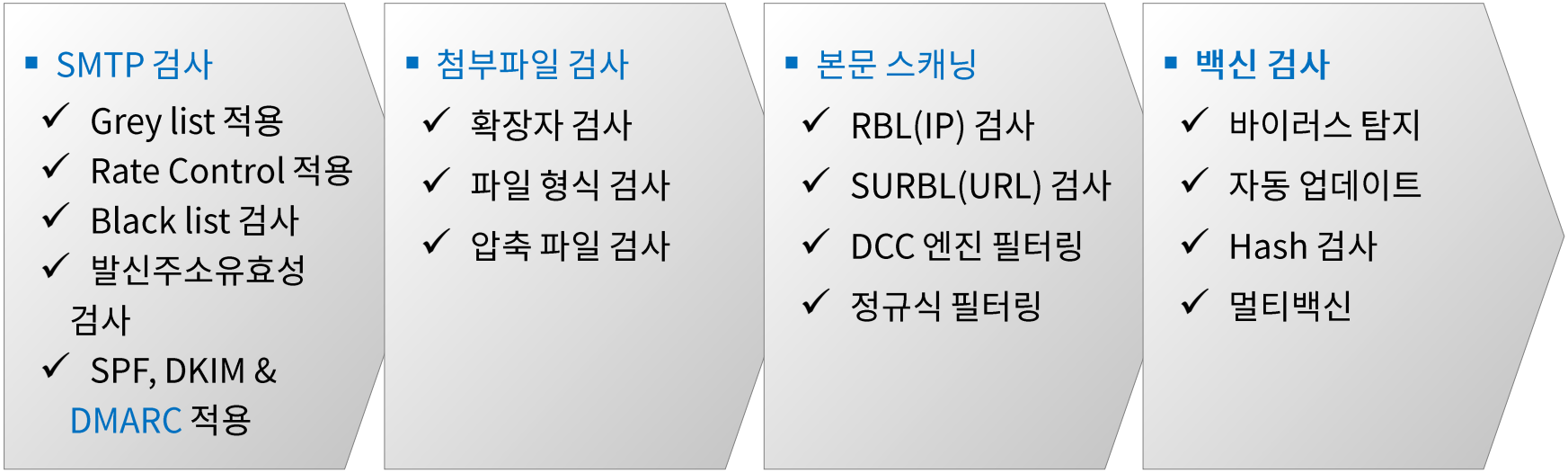
사기성 스캠메일 차단 (계속)

④ 발송 경로 불일치 차단



악성 메일(스팸/바이러스/랜섬) 차단

- 스팸메일을 4단계로 검사하고 차단
- 발신자 위변조를 탐지하는 DKIM , DMARC[1] 기능 제공
- 멀티 백신엔진 (Cyren, ClamAV, Kicom AV) 포함



1) DMARC : DMARC(Domain-based Message Authentication, Reporting and Conformance)는 이메일인증 프로토콜

구축사례

회사 개요	• S중공업, 1000명
시스템 구성	• 스팸차단서버 운영중, 메일서버도 자체운영
문제점	• 멀웨어 메일 다량 유입되어 업무상 불편함 가중 • 스팸차단서버에 고객지원 원할하지 않아 불만족 • 하드웨어 노후화로 인한 교체 필요
해결방안	• 기존 스팸차단서버 대신 NESS로 교체
성과	• 스팸 및 멀웨어 차단율 크게 증가 • 솔루션에 대한 만족도 높음 • 멀웨어로 인한 불편함을 느끼지 못함 • 솔루션에 대한 만족도 높음

구축사례

회사 개요	• A금융사, 2만명
시스템 구성	• 스팸차단서버 없음, 신규 도메인 생성
문제점	• 신규 도메인에 대해서 스팸차단서버가 없어 악성메일에 대한 피해가 우려됨
해결방안	• 스팸차단뿐만 아니라 멀웨어, 스캠차단기능까지 포함된 NESS 구매
성과	• 악성메일로 인한 스트레스 해소 • 메일서비스에 대한 신뢰도 향상 • 메일서비스 활용도 증가

3. 제품의 특장점

특장점

타 제품과의 비교

인증과 특허

특장점

항목	내용
멀웨어 차단	• 샌드박스를 우회하는 멀웨어 차단 • 악성첨부뿐만 아니라 악성URL 도 차단 • 샌드박스 대비 2배 빠른 속도 (적은 하드웨어 자원 필요)
컨텐츠 무해화 (CDR)	• 외산 제품이 지원하지 않는 알집(alz, egg) 도 재조합 • 다중압축도 탐지하고 무해화 및 재조합 • 매크로 유사도 분석 기술로 원문의 안전성 보장
스캠메일 차단	• 스캠의심과 스캠차단 2단계로 구분하여 대응 • 스캠의심메일에 대해서 수신자가 컨트롤할 수 있도록 함
스팸/바이러스 차단	• 8개의 RBL 사이트 지원 • DCC 엔진 필터링 (전 세계 메일의 체크섬을 계산하여 스팸으로 판단하는 필터, 아시아 국가 중 최초 연동 및 시그너처 서버 운영)

타 제품과의 비교

	 멀웨어 차단 방식	 하드웨어 사양	 스캠의심 처리 및 스캠차단	 CDR 엔진 포함	 다양한 압축파일 지원 및 다중압축 파일 CDR처리
NESS	코드 DNA 유사도 분석	저사양	O	O	O
A사 제품	샌드박스	고사양	△ 차단만 가능	X	X
B사 제품	△ 샌드박스 옵션	고사양	△ 차단만 가능	△ 옵션	X
C사 제품	정적분석	저사양	X	X	X

인증과 특허

SpamOUT V9.0

Lupe V1.0

MINOSS V2.0

SpamOUT V9.0

4. 제품 UI

대시보드

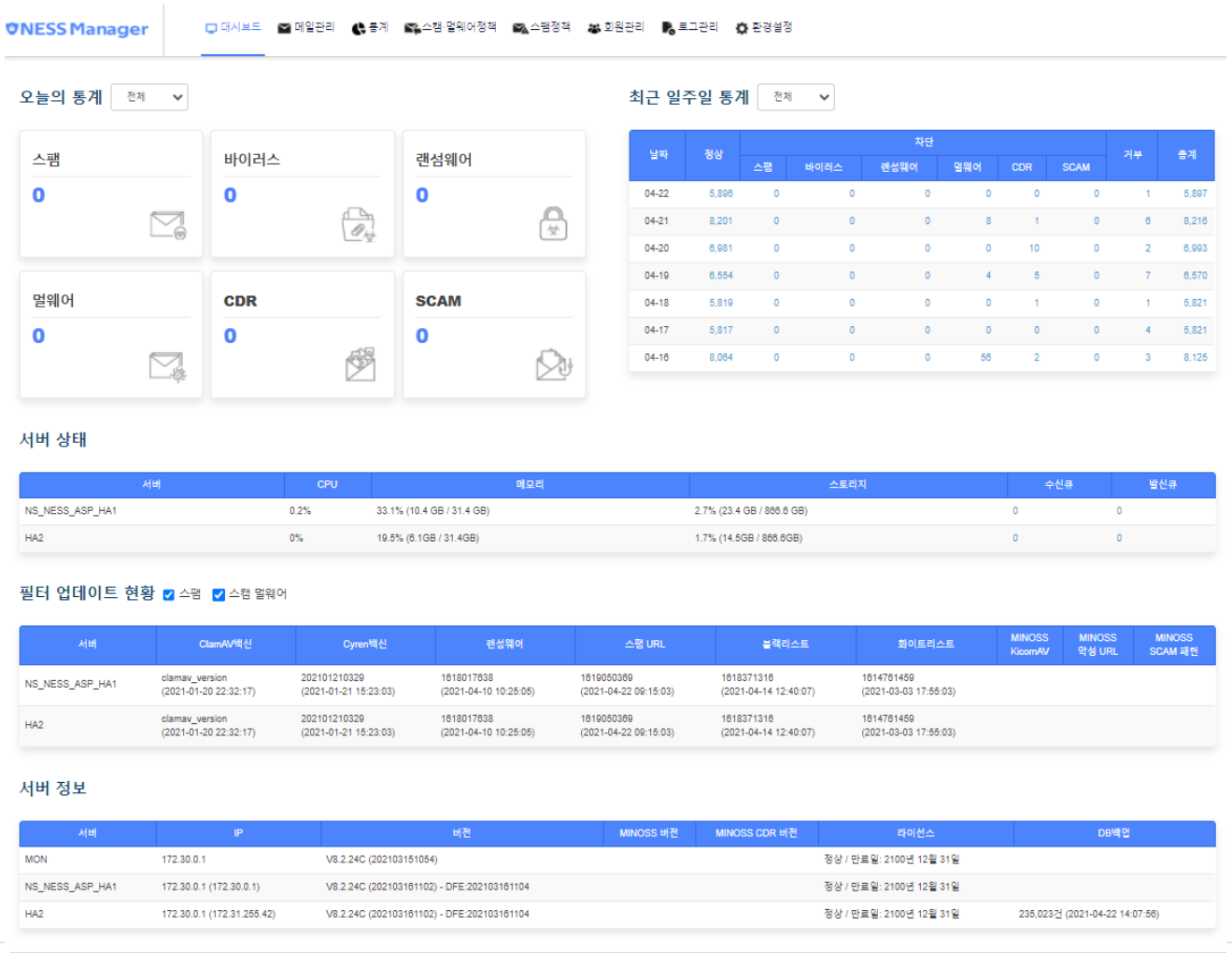
메일 관리에서 차단항목별 구분

탐지필터 항목별 ON/OFF 설정기능 제공

차단 통계

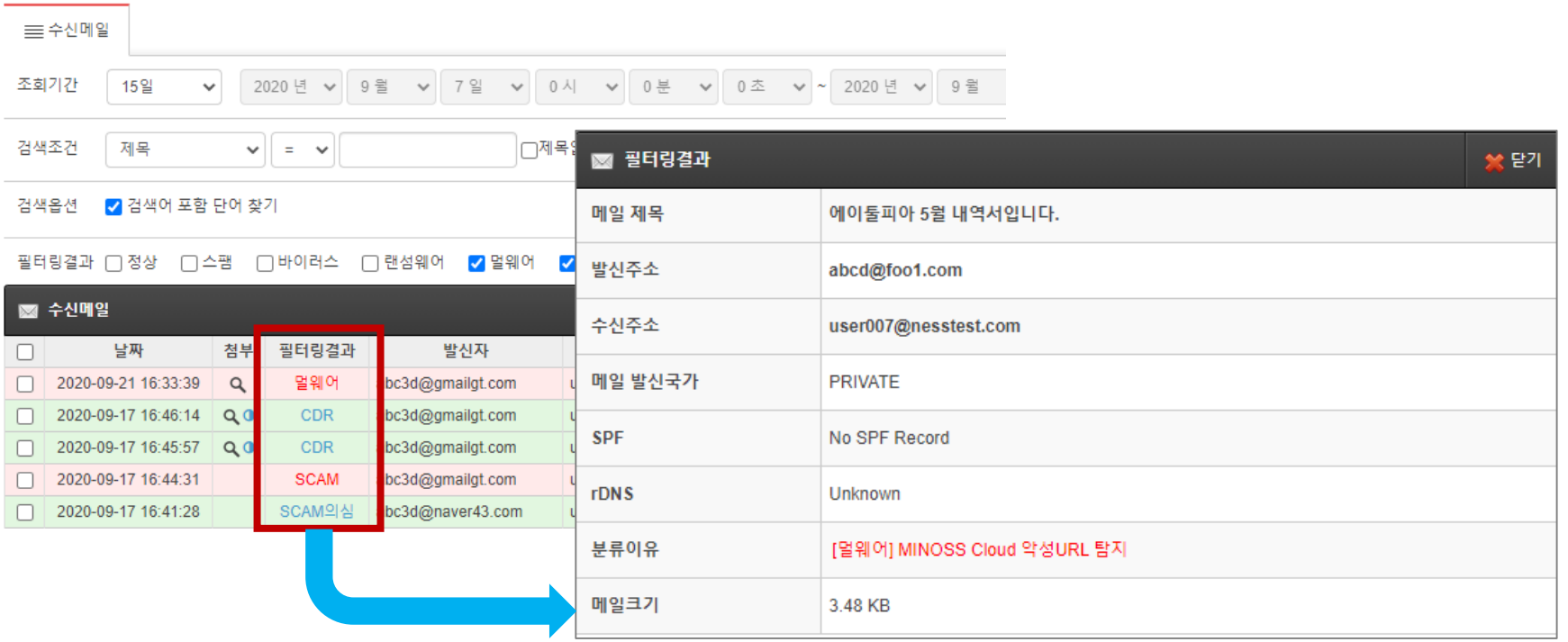
대시보드

- 수·발신, 스팸메일 수신, 업데이트, 최근수신 메일, 시스템 현황 정보 제공



메일 관리에서 차단항목별 구분

- 메일에 대해 멀웨어, CDR, SCAM, SCAM의심으로 구분하여 표시
- 필터링결과 클릭 시 '분류이유' 표시
- SCAM의심으로 처리된 메일은 수신자에게 알림메일 발송



탐지필터 항목별 ON/OFF 설정기능 제공

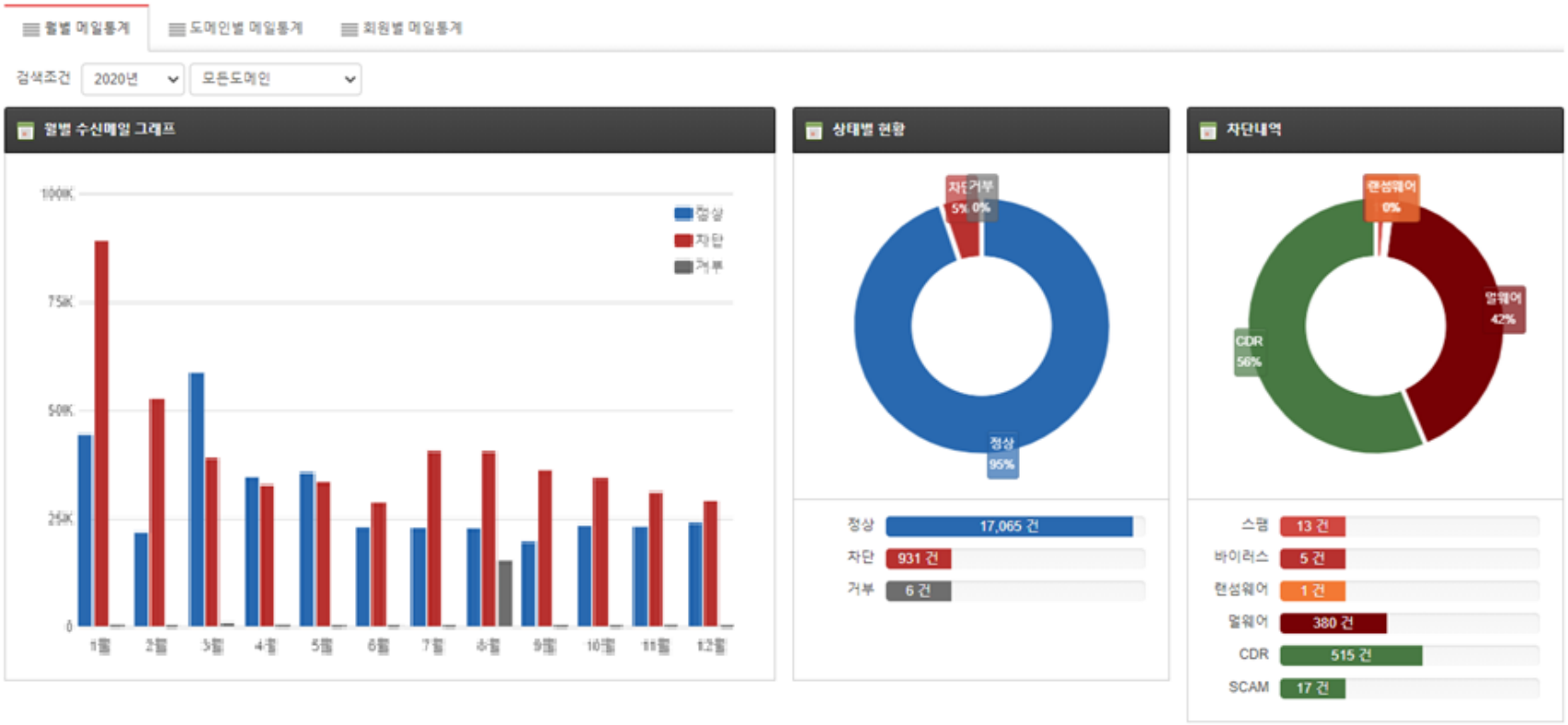
- 멀웨어, CDR 이름과 코드 매칭 설정
- 웹에서 표시되는 필터이름 편집 기능 제공

탐지필터 | 필터추가 | 삭제

등록시간	설정자	필터이름	필터코드	사용	수정
2020-09-18 17:24:57	admin	[스캠] 유사도메인 차단	301	사용중	
2020-09-18 17:24:50	admin	[스캠] 발송경로 불일치	901	사용중	
2020-09-18 17:24:31	admin	[스캠의심]	801	사용중	
2020-09-18 17:24:11	admin	[무해화] HWP 외부객체 삭제	556	사용중	
2020-09-18 17:24:01	admin	[무해화] PDF 액티브 콘텐츠 삭제	555	사용중	
2020-09-18 17:23:50	admin	[무해화] PDF URL링크 삭제	554	사용중	
2020-09-18 17:23:37	admin	[무해화] MS오피스 URL링크 삭제	553	사용중	
2020-09-18 17:23:26	admin	[무해화] MS오피스 외부객체 삭제	552	사용중	
2020-09-18 17:23:11	admin	[무해화] MS오피스 매크로 삭제	551	사용중	
2020-06-08 09:16:58	system	[멀웨어] MINOSS Cloud 악성URL 탐지	104	사용중	
2020-06-08 09:16:58	system	[멀웨어] 유사도 검사 악성코드 탐지	101	사용중	
2020-06-08 09:16:58	system	[멀웨어] MINOSS Cloud 악성코드 탐지	102	사용중	
2020-06-08 09:16:58	system	[멀웨어] Kicom AV 악성코드 탐지	103	사용중	
2020-06-08 09:16:58	system	[무해화] MS오피스 매크로 탐지	501	사용중	
2020-06-08 09:16:58	system	[무해화] MS오피스 외부객체 탐지	502	사용중	
2020-06-08 09:16:58	system	[무해화] MS오피스 URL링크 탐지	503	사용중	
2020-06-08 09:16:58	system	[무해화] PDF URL링크 탐지	504	사용중	
2020-06-08 09:16:58	system	[무해화] PDF 액티브 콘텐츠 탐지	505	사용중	
2020-06-08 09:16:58	system	[무해화] HWP 외부객체 탐지	506	사용중	

차단 통계

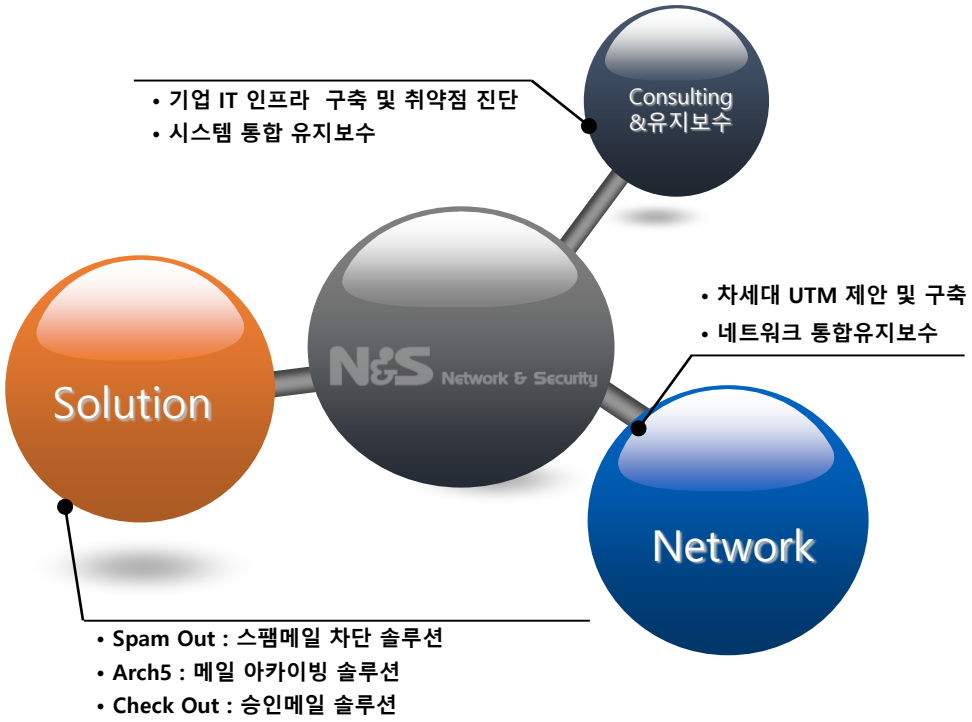
- 월별 , 도메인, 회원별 메일 통계
- 상태별, 차단내역별 표시



넷엔씨큐…

 # 넷엔씨큐는 기업메일 보안 및 네트워크 보안 분야에서 최고 수준의 전문가 집단으로 기업 IT 인프라의 안정적 운영 및 운용효율 극대화를 위하여 고객의 경영환경에 가장 적합한 정보보안 솔루션 및 서비스를 제공하고 있습니다.

✓ **주요사업 영역 및 제품 소개**



✓ **일반현황**

회 사 명	㈜넷엔씨큐	**대표자**	한진호
설 립 년 도	2007년 1월 2일		
사 업 분 야	기업 IT 인프라 및 보안 컨설팅 보안 소프트웨어 개발 및 공급 네트워크 통합유지보수		
사 업 자 등 록 번 호	107-86-85828		
주 소	서울시 금천구 벚꽃로 244, 1404호 (가산동, 벽산디지털밸리5차)		
전 화 번 호	전화 : 02-2633-6102 FAX : 02-2633-6192		
홈 페 이 지	http://www.netnsecu.co.kr http://www.spamout.co.kr		

감사합니다.

제품 문의 : 백재훈 이사

010-9755-6372, baek@netnsecu.co.kr