NESS AI 엔진분석기반의 이메일 위협대응솔루션

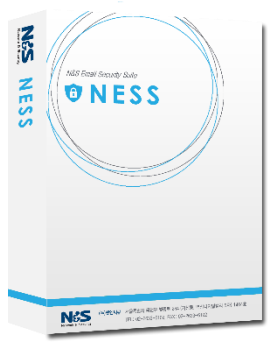
N&S Email Security Suite

2021년

㈜넷엔씨큐

목 차

1. 제안배경
2. 제품소개 – NESS 란?
3. NESS 엔진구성
4. NESS 주요기능
5. NESS 서비스 이미지
6. NESS 구성도
7. NESS 특장점
8. NESS 기능요약
9. 제품보증
10. LINE UP



❖ 본 문서는 2020년 9월 기준으로 작성하였습니다.
❖ 제안서상 서비스 이미지는 실제와 다를 수 있습니다. .

1. 제안배경

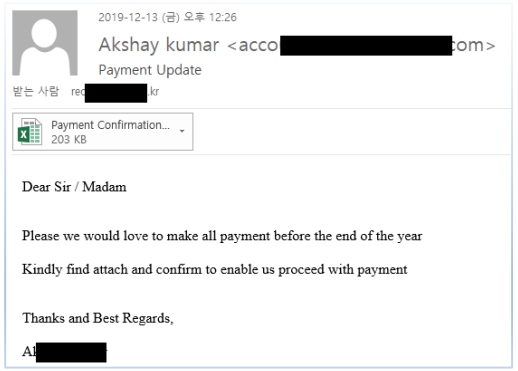
 # 최근 기존의 스팸메일 및 APT 솔루션으로 방어하지 못하는 신종 표적공격이 급증하고 있습니다.

 # 표적공격의 91% 이상이 이메일에서 시작되고 이메일의 94%가 악성코드-첨부파일을 가지고 있습니다.

※ 2018년 MS-ISAC 리서치 보고서

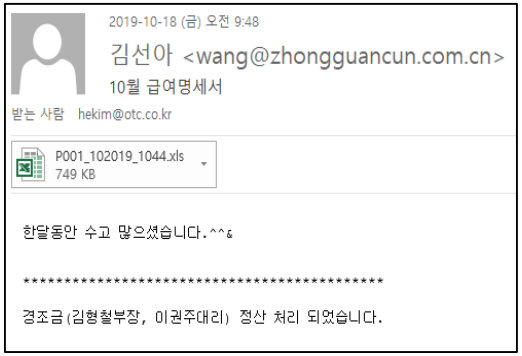
• • •

무역대금 사기메일



무역대금 지불과 관련된 사기 메일
첨부파일에 악성코드 포함

사회공학 이용 공격



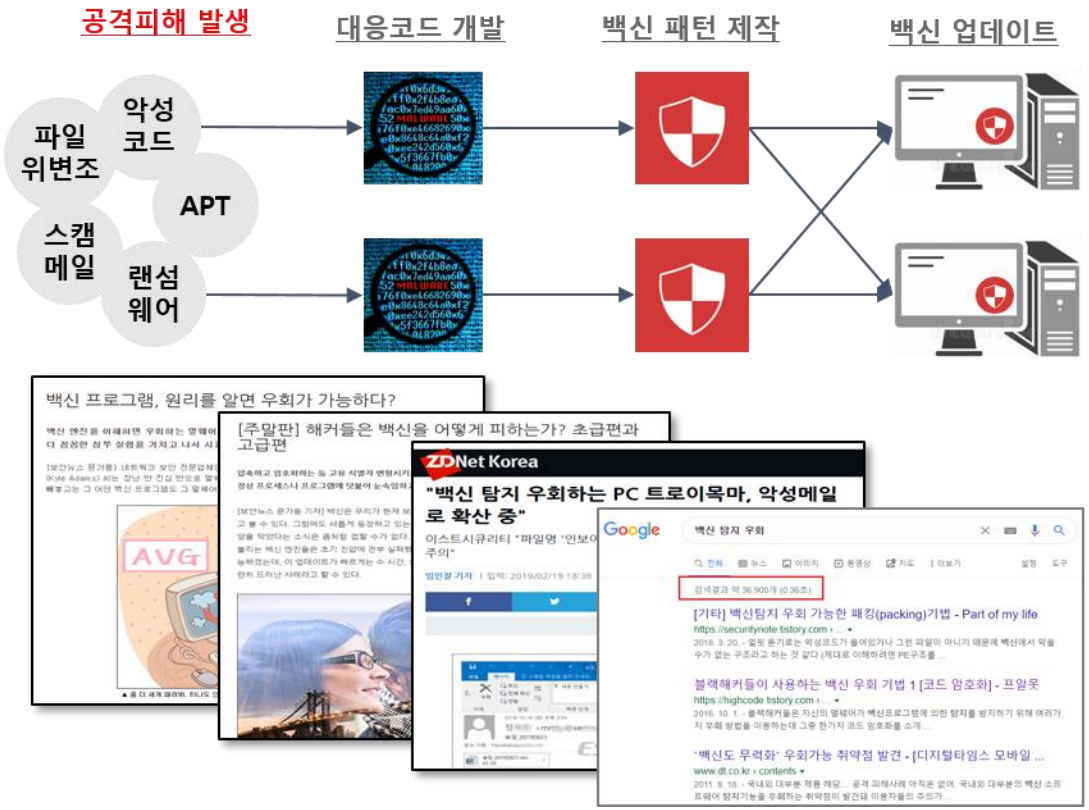
급여명세서를 위장한 메일
엑셀파일에는 악성코드가 포함되어 있음

정부기관 사칭메일

국세청을 위장한 악성 메일
첨부파일에 악성코드 포함

1. 제안배경

 # 기존 사후대응 방식의 필터 및 백신과 같은 보안 솔루션으로는 신•변종 악성코드 대응에 한계점을 보이고 있으므로 사후 대응 방식이 아닌 사전 대응 및 예방하는 형태로 변화가 필요 합니다.

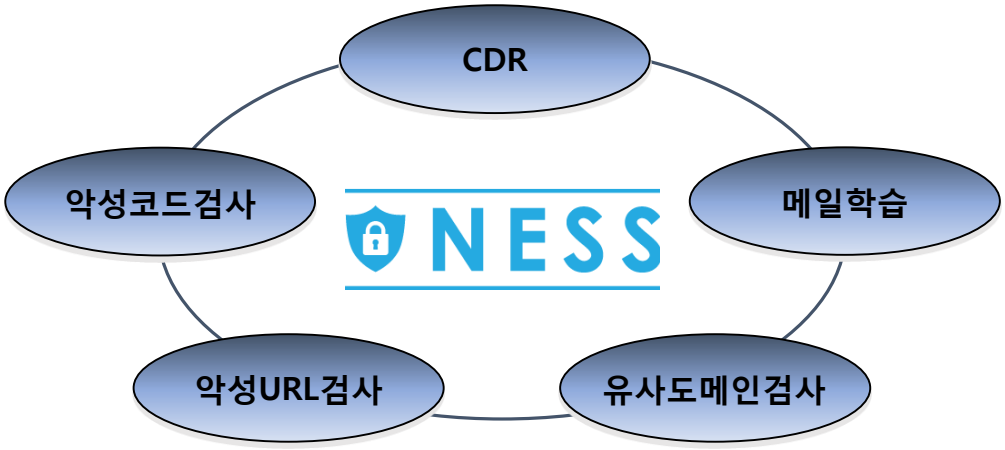


- 공격을 당하고 사후 대응이기에, 이미 발생한 피해 복구의 한계
- 대응 방안 마련시까지 추가 피해 발생
- 업데이트 된 공격이라도, 약간 변형하면(변종) 탐지하지 못함

- 백신을 우회하는 방법이 너무 많으며 공격코드도 일반화 되고 있음

2. NESS 란?

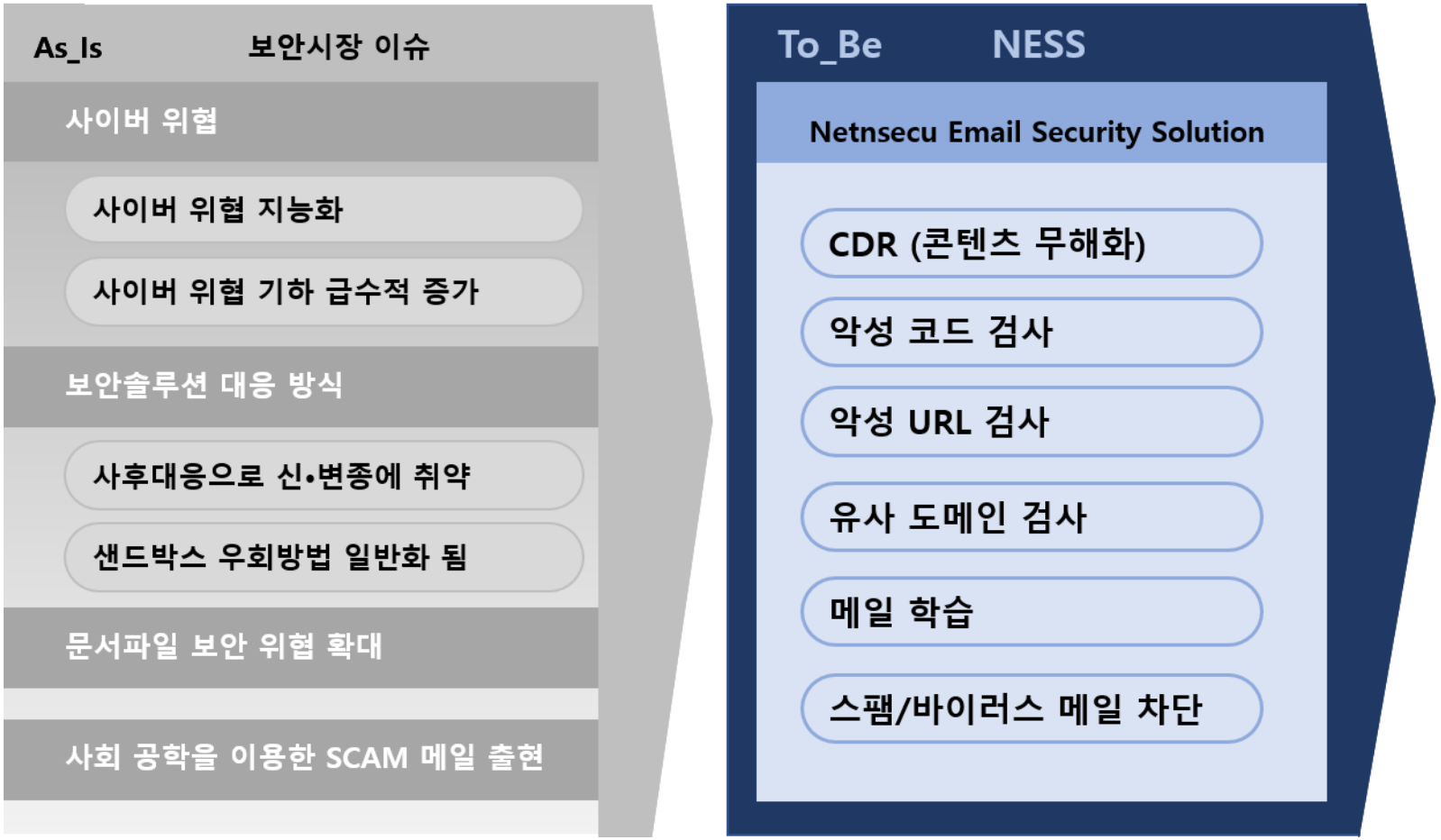
NESS (Netnsecu Email Security Solution)는 신·변종 악성코드나 위험한 콘텐츠를 가진 이메일 첨부 파일을 CDR(콘텐츠 살균 처리) 처리 엔진과 A.I.기반의 악성코드 DNA 탐지 기술로 신종 사기메일과 악성코드 공격 메일을 예방하는 "이메일 위협대응솔루션" 입니다.



CDR	악성코드검사	악성URL검사	유사도메인검사	메일학습
위험한 콘텐츠를 가진 문서일 경우 CDR 기능을 사용하여 문서를 무해화 합니다.	백신 엔진이 검출하지 못하는 신종 악성코드를 검출하여 치료합니다.	메일의 본문에 포함 URL에 대해서 악성 URL 여부를 검사합니다.	수신자를 속이기 위한 유사 도메인을 검출합니다.	사용자별 학습 DB를 구축하고 이를 바탕으로 스캠 메일을 분석합니다.

3. NESS 엔진구성

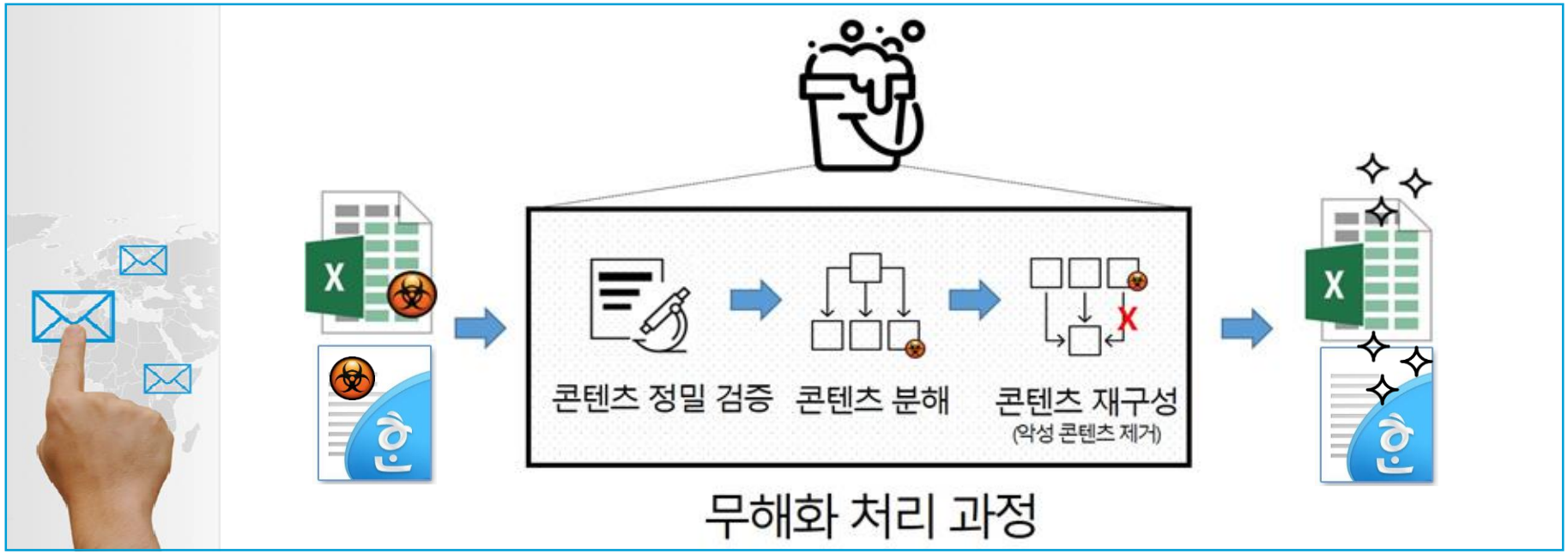
NESS는 샌드박스를 우회하는 악성코드를 차단하고, 위·변조 파일탐지 및 무결성 검사를 수행하며, 컨텐츠 무해화(CDR)를 통해서 사회공학을 이용한 사기성 스캠메일을 차단합니다.



4.1 NESS 주요기능 – CDR

 # NESS는 메일의 첨부 파일에 대하여 보안취약점을 제거하는 최신 CDR 엔진을 제공합니다.

 # CDR (Content Disarm & Reconstruction) 엔진을 통해서 첨부 파일을 정밀하게 검증하고 분해, 재조립하여 파일의 무해화 처리를 제공합니다.



4.1 NESS 주요기능 – CDR (계속)

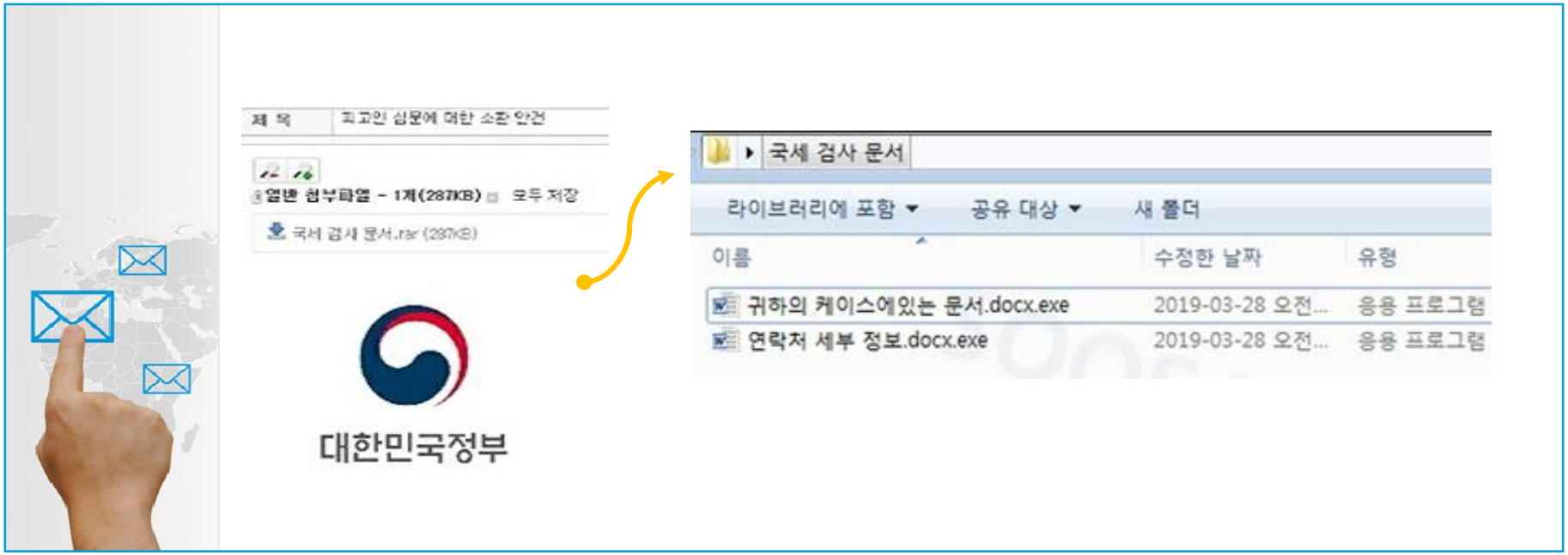
최근 CDR을 우회하기 위해 외산 제품이 지원하지 않는 egg, alz(알집) 압축을 사용한 공격이 증가

▷▶ 알집을 포함하여 zip, 7z, rar, cab, tar, gz, xz, bzip 등 다양한 압축 포멧 지원

다중 압축을 이용한 공격

▷▶ .hwp 파일을 zip으로 압축하고, 이를 다시 rar로 압축하기를 반복한 공격 방어

▷▶ 혼합 형태의 압축 및 다중 압축 파일도 처리 가능



4.1 NESS 주요기능 – CDR (계속)

 # NESS - CDR은 국내 최대, 이미지 파일 17종과 압축파일 10종 및 대용량 파일 무해화를 지원합니다.

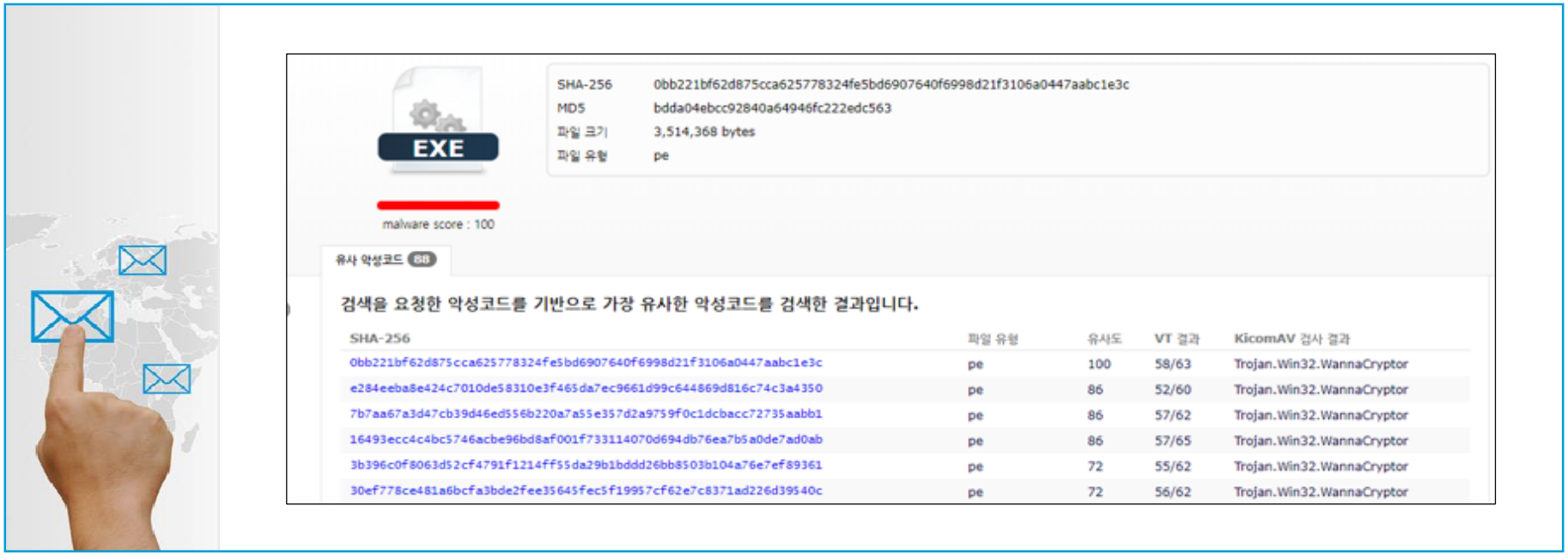
비교 항목		NESS	A사	B사	C사
백신 결합		O	-	O	O
문서 파일	HWP	O	O	O	O
	MS-Office	O	O	O	O
	매크로 처리	O	Δ	Δ	Δ
	PDF	O	O	O	O
	RTF	O	-	O	O
이미지 파일	BMP,JPEG,GIF 등	17종 지원	8종	6종	1종
검사 파일	사이즈 제한	무제한	X	X	X
압축 파일 (다중압축)	ZIP	O	-	O	-
	ALZ	O	-	-	-
	EGG	O	-	-	-
	기타(gz,tar,7z 등)	10종 지원	-	-	-
웹 파일	HTML	O	-	-	O

4.2 NESS 주요기능 – 악성코드 검사

최근 샌드박스를 우회하는 악성코드의 위협이 증가 하고 있습니다.

▷▶ NESS는 A.I. 기반의 미노스 엔진을 통해서 첨부파일을 이용한 신•변종 공격행위를 차단 합니다.

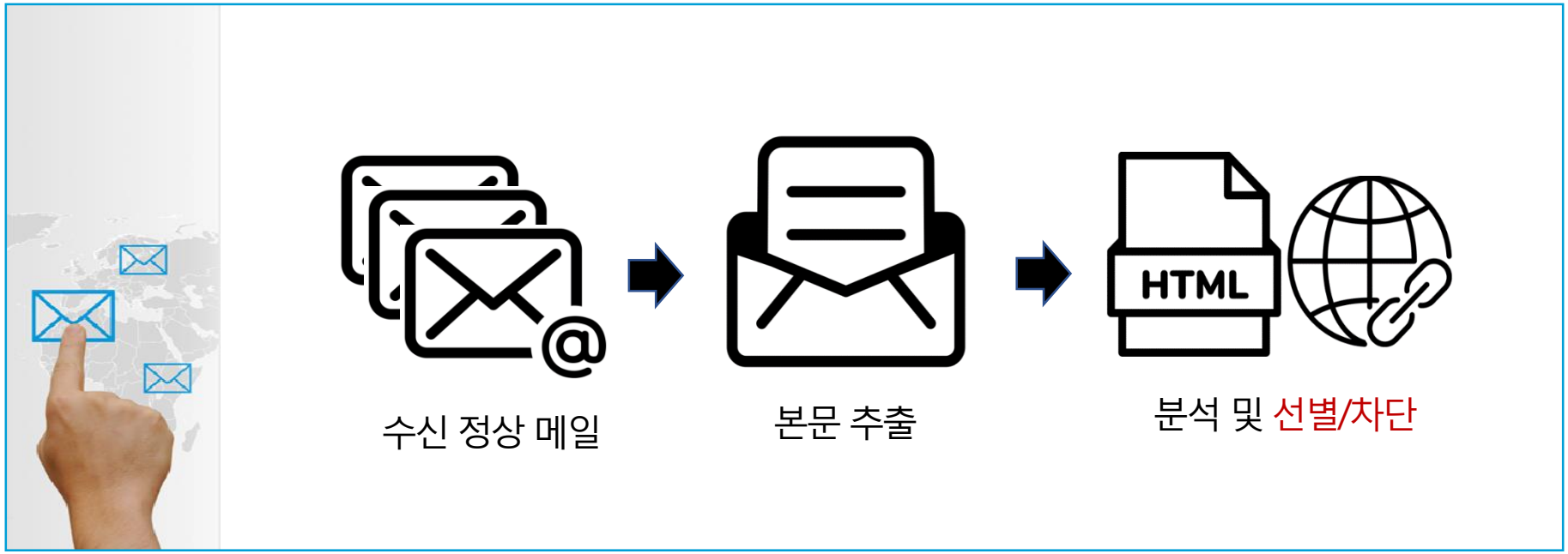
기존 업데이트 된 패턴을 기반으로 막는 악성코드를 차단하는 방식의 취약점을 개선하여
파일의 DNA 학습 데이타를 기반으로 첨부 파일의 DNA 분석 후 악성 유무를 판별 합니다.



4.3 NESS 주요기능 – 악성 URL 검사

 # 메일 본문을 분석하여 숨어 있는 악성행위를 차단 합니다.

- **NESS는 A.I. 기반의 미노스 엔진을 통해서 메일 본문의 위·변조 여부를 판단하고 악성 URL을 검출하여 악성행위를 사전에 차단 합니다.**
- **본문 소스 내 유해성 유무 검토는 물론 본문 내 URL 검출 후 페이지 및 링크파일에 대한 악성행위와 영향도를 분석하여 보다 철저한 보안 검사를 수행합니다.**



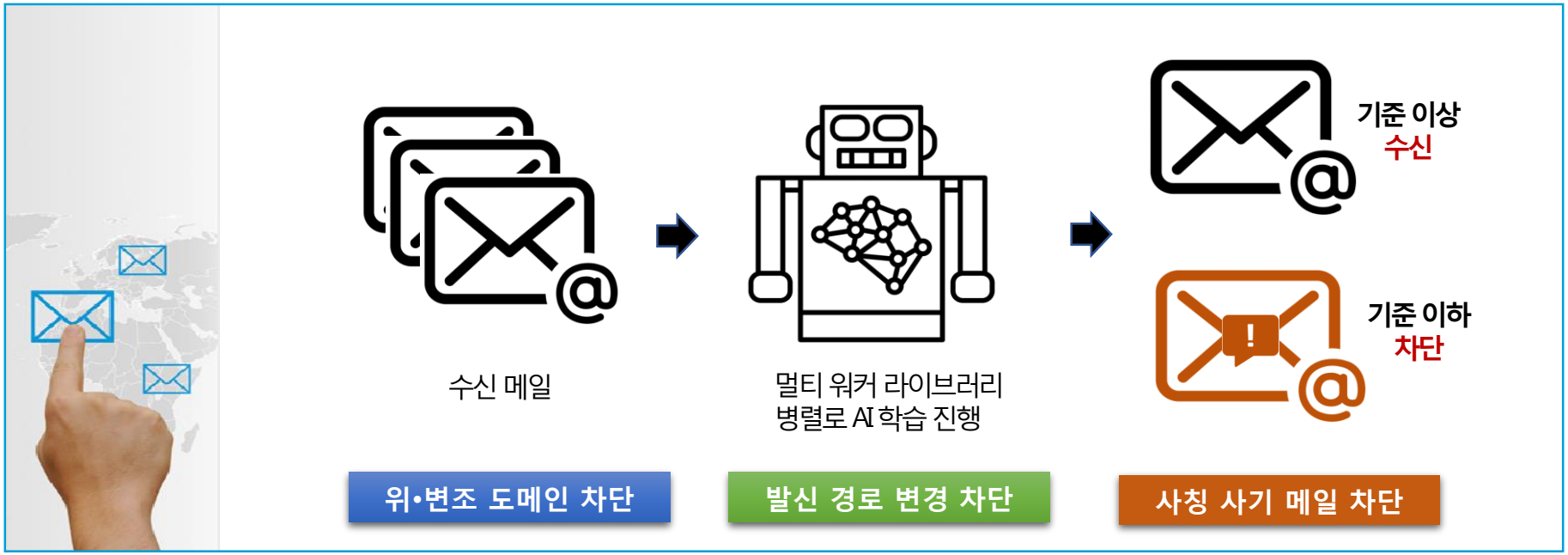
4.4 NESS 주요기능 – 유사 도메인 검사

수신된 메일 중 화이트리스트를 학습하고 이를 기반으로 발신자 신뢰성을 보장 합니다.

▷▶ NESS는 멀티 워커 라이브러리를 이용하여 병렬로 수신 메일에 대한 A.I. 학습 진행

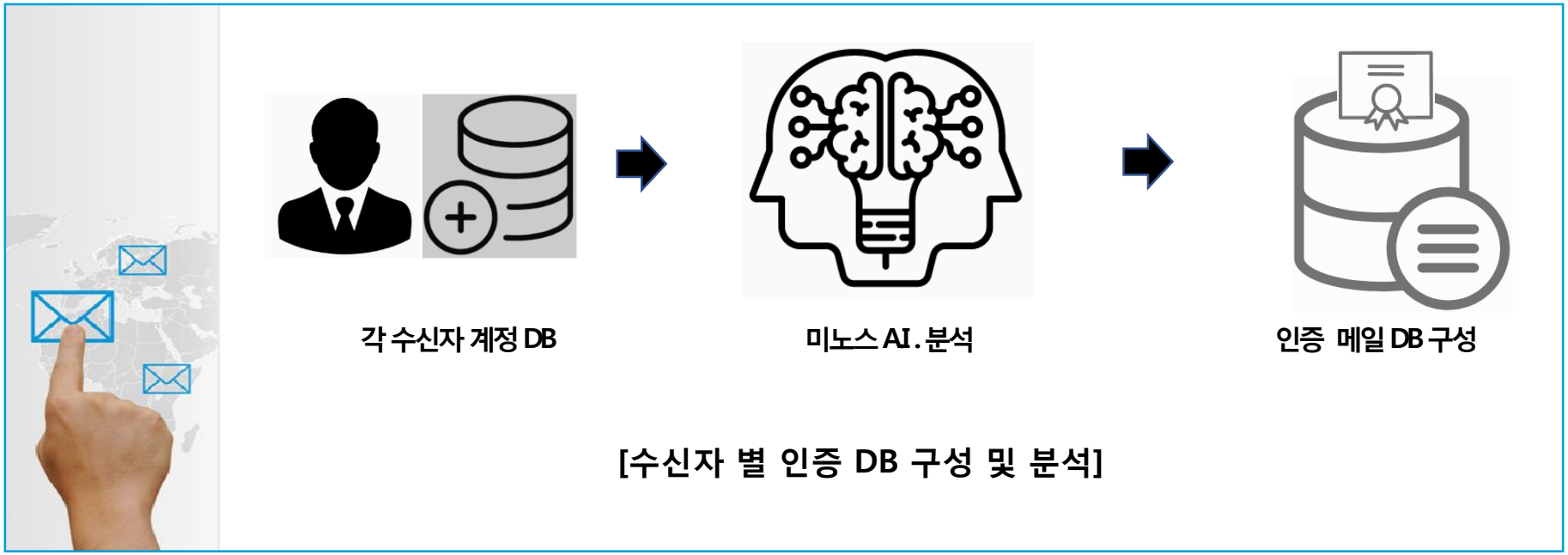
발신자 주소 위·변조 검사 및 추적, 유사 도메인 비교 검사를 통해서 각 메일 별 신뢰도를 수치화

▷▶ 기준점수 이하의 메일을 자동 차단하여 사칭 사기 메일 피해를 예방할 수 있습니다.



사회공학을 이용한 스캠(SCAM) 메일 차단

▷▶ 사회공학을 이용하여 사용자를 속이는 스캠(SCAM) 메일도 점점 늘어나고 있습니다.
NESS는 메일 수신자별로 수신 메일에 대한 학습 DB를 구축하고 이를 바탕으로 송신자의 유사도메인을 판별하여 사회공학을 이용한 스캠메일을 차단합니다.



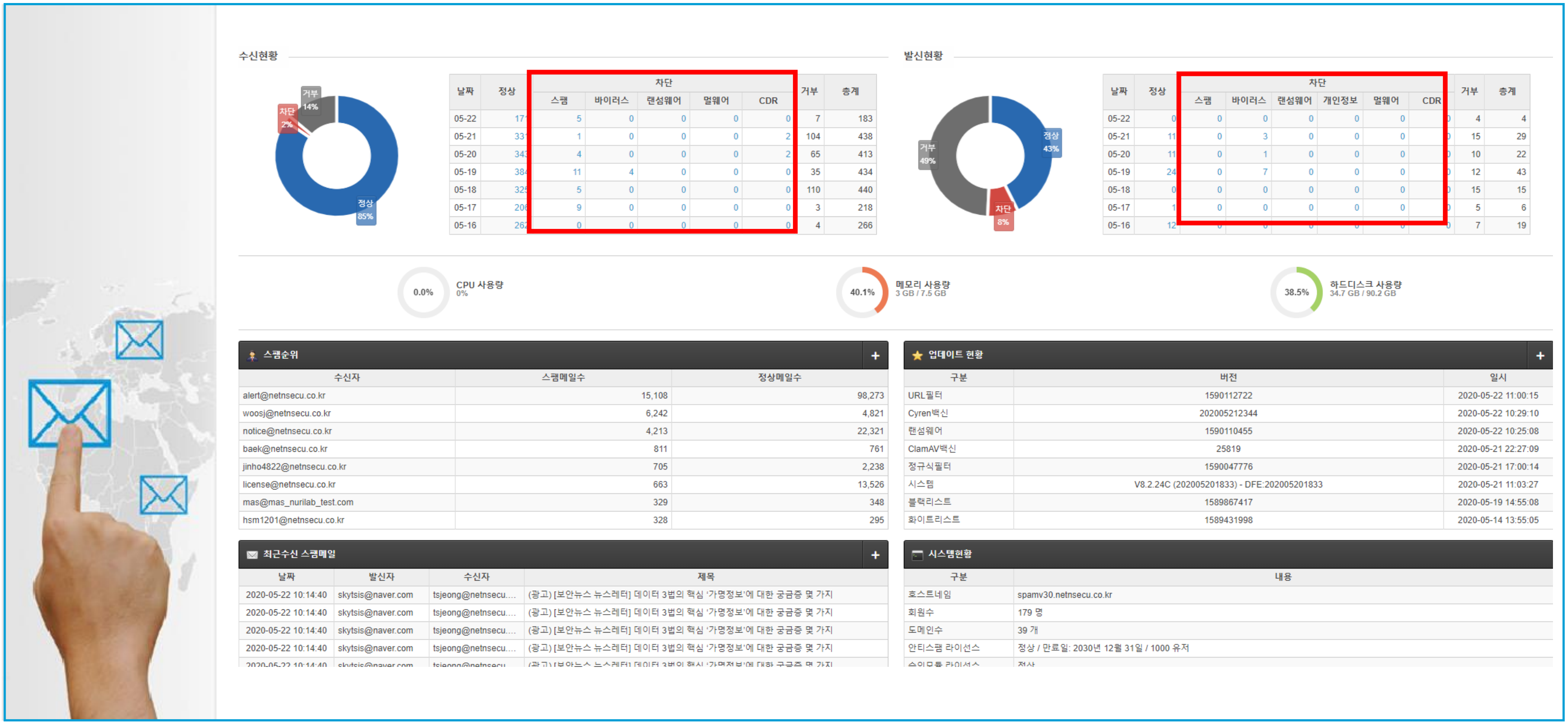
[수신자 별 인증 DB 구성 및 분석]

5.1 NESS 서비스 이미지 – 대시보드

NESS

\# 수발신 메일 현황 및 스팸 순위 정보 제공

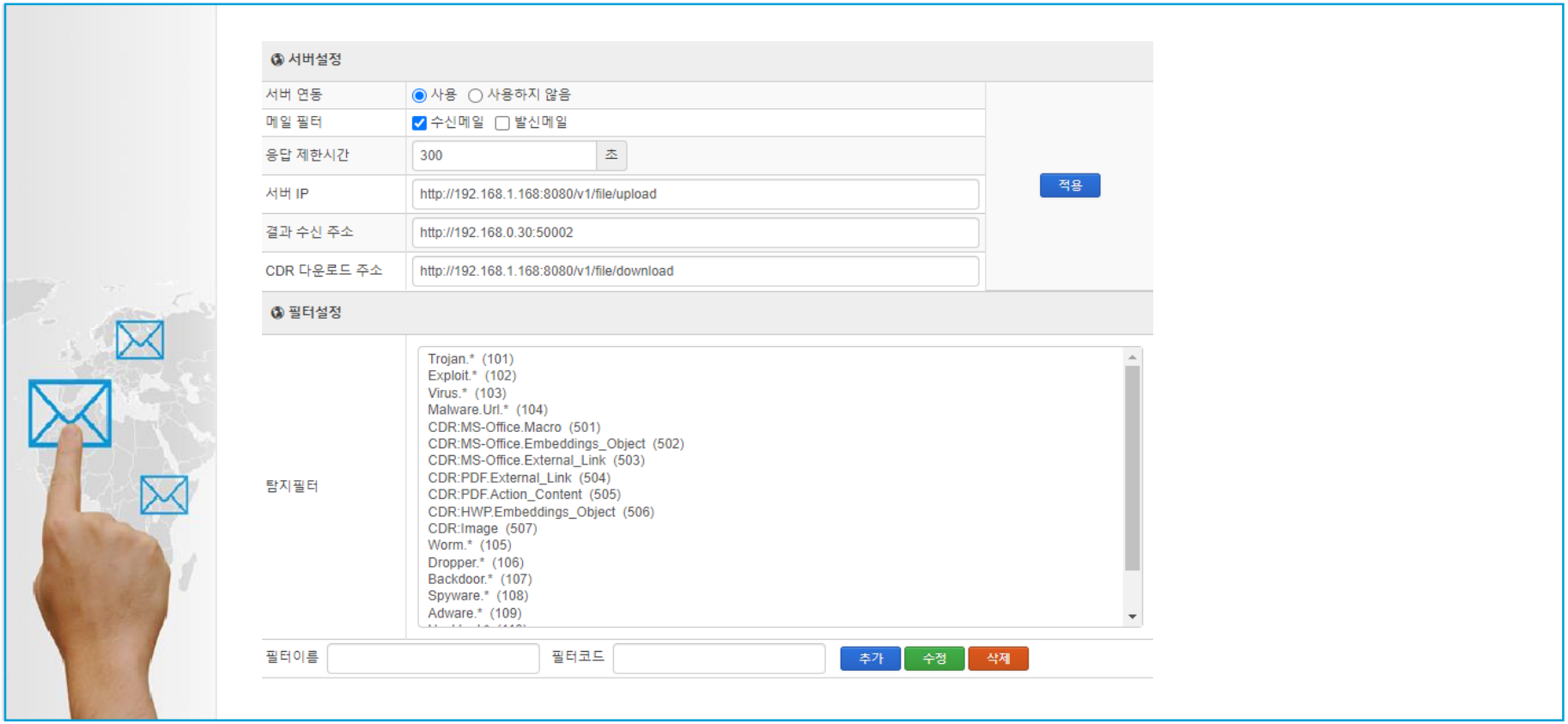
\# 스팸아웃 및 NESS 통합정보 제공



5.2 NESS 서비스 이미지 – 보안설정

멀웨어 필터 관리

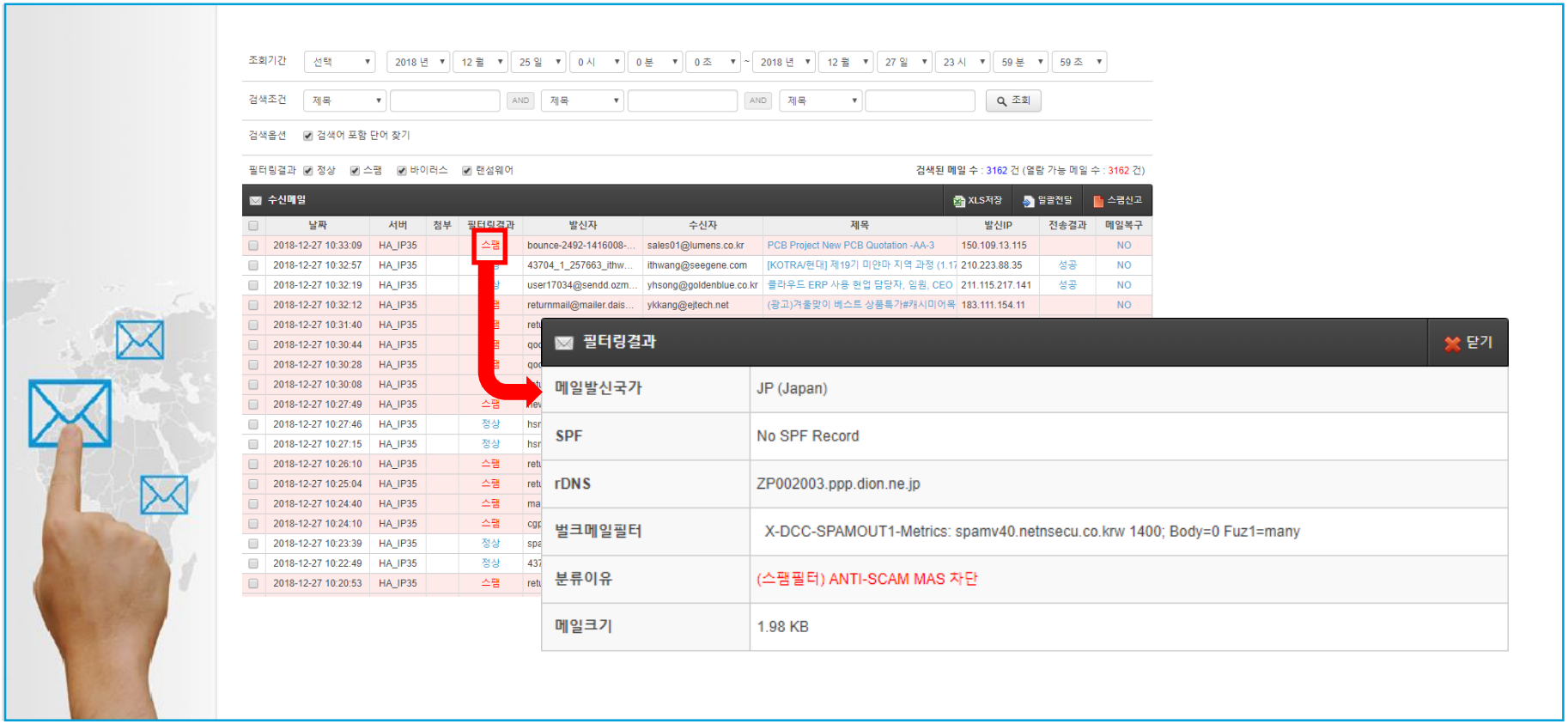
CDR 탐지 관리



5.3 NESS 서비스 이미지 – 탐지정보 제공

 # 메일리스트에서 탐지 정보(분류이유) 제공

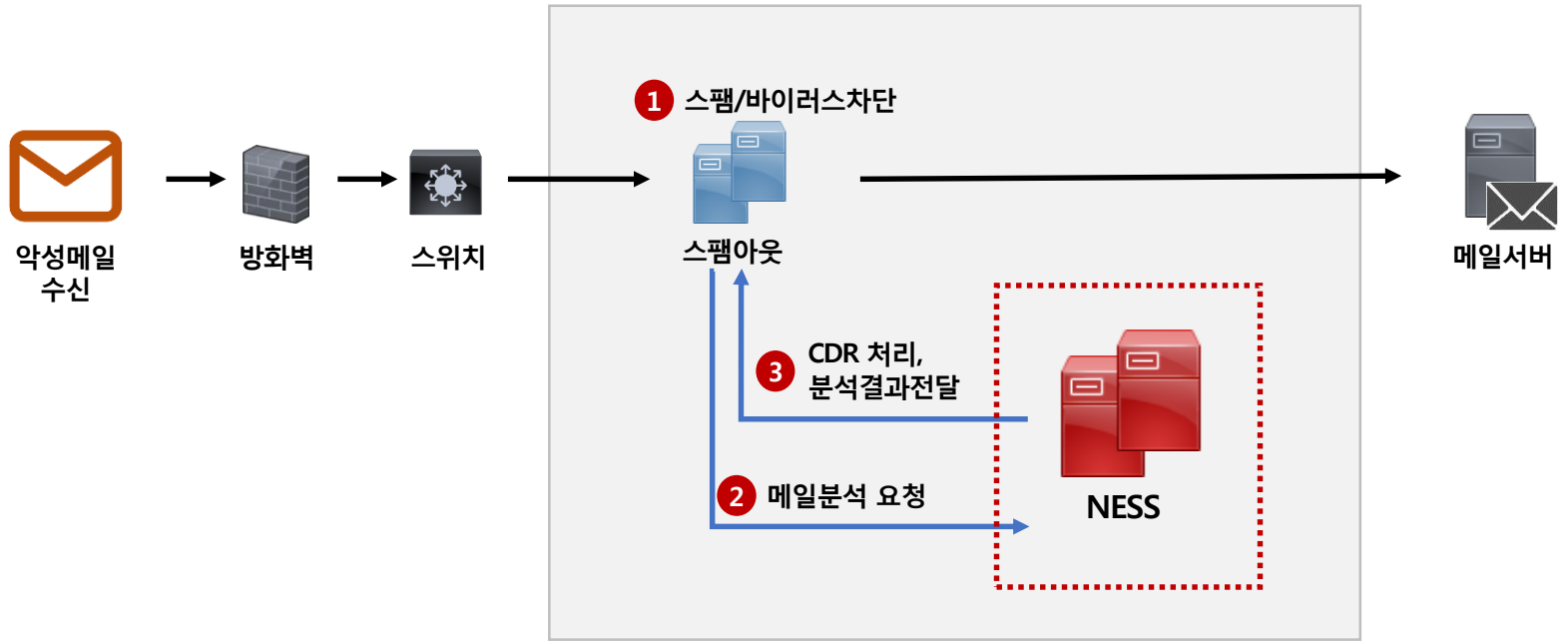
 # 다중 처리 결과에 대해서 치료한 항목을 모두 표시



6. NESS 서비스 구성

스팸아웃에서 처리한 메일을 NESS에서 한번 더 검사한 후 정상메일만 메일서버로 배달합니다.

보다 안정적인 메일 이용 고객을 위한 이중 구성 및 다중 처리 구성을 지원합니다.



7. NESS 특장점

구분	Anti-Virus	SandBox	NESS
위협 대응 방식	● 알려진 위협은 탐지하지만 알려지지 않은 위협이나 제로데이 위협은 탐지 불가 - 시그니처 기반 솔루션인 Anti-Virus는 새로운 악성코드에 대한 대응에 한계가 존재	● 샌드박스를 우회하는 기술은 다양함 - 일부 유형의 악성코드는 탐지를 회피하고, 샌드박스에서 휴면 상태를 유지하며 프로덕션 환경에서 한 번만 실행되도록 설계됨	● **NESS**는 알려진 위협 뿐만 아니라 알려지지 않은 신·변종 위협 차단에 효과적임 ● CDR은 탐지에 의존하지 않으며, 제로데이 위협을 포함하여 문서 내 숨겨진 악성 위협을 제거하고 안전한 문서 사용을 보장함
처리속도	● 시스템 작동이 느려질 수 있음 - 패턴(DB) 업데이트 및 실시간 감시와 같은 백그라운드 프로세스 등은 시스템에 영향을 미칠 수 있음	● 동적분석을 위한 처리 시간이 길어져 병목 현상 발생 - 파일에 대한 동적 분석 과정에서 병목 현상이 발생 할 수 있어, 메일 수신 지연 현상이 발생됨	● **NESS**는 유사도 분석(특허) 기술을 적용하여 수초 내 가장 유사한 악성코드 탐지가 가능함 ● CDR은 악성 위협만을 제거함으로 악성 콘텐츠가 없으면 1초 내로 파일 무해화 진행

7. NESS 특장점 (계속)

구분	Anti-Virus	SandBox	NESS
유지보수 및 비용	● 잦은 패턴 업데이트 및 유지 관리 필요 - Anti-Virus가 탑재된 시스템에는 자체 업데이트 및 유지관리를 위해 비용과 시간이 필요	● 복잡하고 광범위한 유지 관리 및 리소스 필요 ● HW 구축 비용이 비쌈 - 수만건~수십만건의 동적분석 수행을 위한 IT 자원의 비용이 많이 소요됨	● 스팸아웃 연동, 통합관리 가능 ● 샌드박스 운영을 위한 고가의 HW장비가 불필요함
정책 요구사항	● 정상 파일이 차단될 수 있으며, 신·변종 악성 파일을 사용자가 실행할 수 있음 - 정상 파일을 차단하는 오탐의 위험성을 내포하고 있고, 탐지 못하는 악성파일 실행으로 보안 위험성 증가	● 복잡한 보안 정책 및 장비 운영 중 상시적으로 담당자의 개입이 필요함 - 샌드박스 분석 결과에 대한 지속적인 모니터링이 필요	● 정책 적용 후 A.I 분석 엔진에 의한 자동화 운영으로 담당자 개입을 최소화 할 수 있음 ● CDR은 조직으로 유입되는 모든 문서 파일을 대상으로 하므로 어려운 정책 결정은 없음

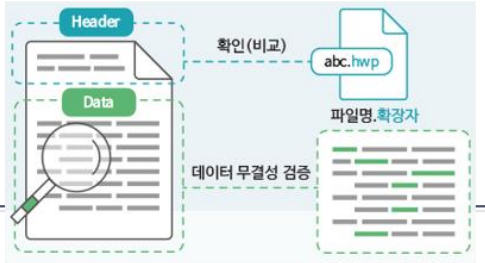
8. NESS 기능요약

AI 기술로 악성코드 차단

- 샌드박스를 우회하는 악성코드들이 점점 늘어나는 경향을 보이고 있습니다. NESS는 유사도 분석을 통하여 악성코드의 DNA를 탐지하고 차단합니다.
- 20년 2월 유사도검색 특허등록

파일의 위·변조 탐지, 무결성 검증

- 파일의 위·변조를 탐지하고 무결성을 검사하는 엔진이 포함되어 있습니다.

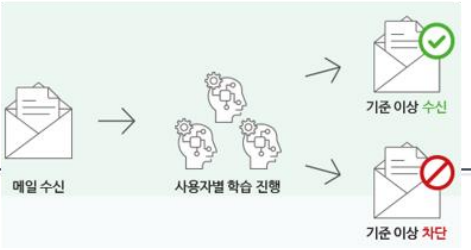


문서를 재조합하는 CDR 기술

- 글로벌 IT 자문기관 '가트너' 에서는 악성코드 회피 기술이 발전함에 따라 CDR 사용을 권고하고 있습니다. NESS 는 보안취약점을 제거하고 클린한 파일로 생성하는 CDR 엔진이 포함되어 있습니다.

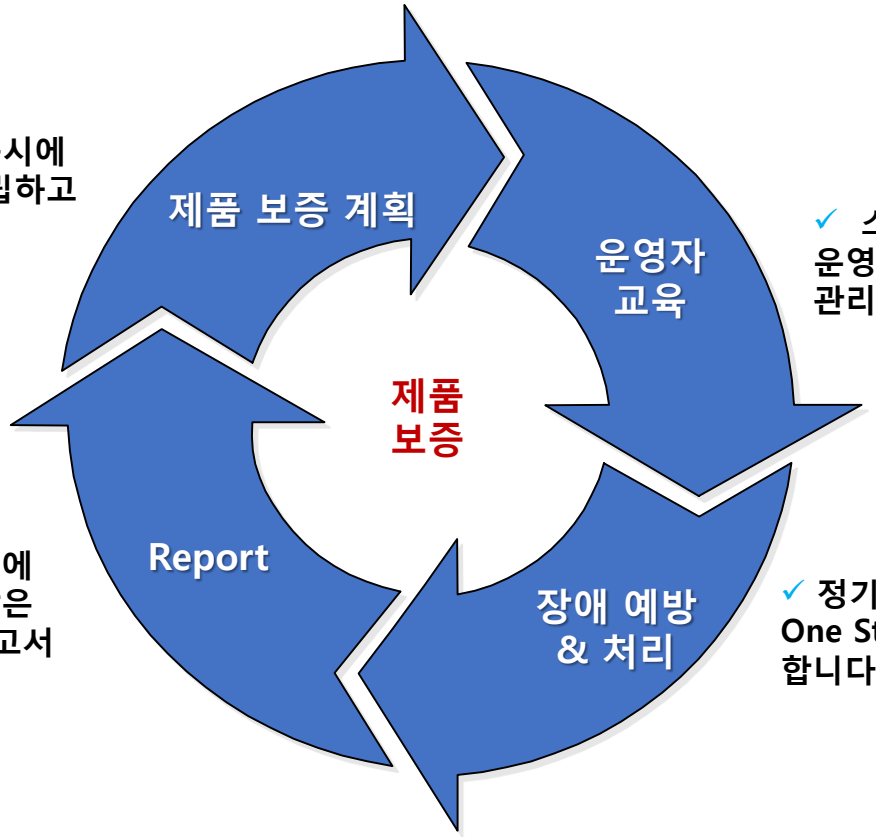
사회공학을 이용한 스캠메일 차단

- 사회공학을 이용하여 사용자를 속이는 SCAM메일도 점점 늘어나고 있습니다. NESS는 사용자별 학습 DB를 구축하고 이를 바탕으로 송신자의 유사도 메인을 판별하여 스캠메일을 차단합니다.



NESS 도입효과를 극대화 시킬 수 있도록, 실질적인 운영방안을 제시해 드리며,
유사 시에는 "365지원센터"에서 One Stop Customer Care Service를 제공합니다.

✓ 솔루션 설치공급과 동시에 제품 보증 계획을 수립하고 보증서를 제공합니다.



✓ 스팸아웃 전문가 그룹을 통한 운영 know-how 중심의 맞춤형 관리·운영자 교육을 실시합니다.

✓ 모든 지원 활동 후에는 각 상황에 알맞은 다양한 형식의 보고서를 제공합니다.

✓ 정기점검을 통한 장애 예방 및 유사시 One Stop Customer Care Service를 제공합니다.

10. NESS line up

NESS는 Cloud 및 전용 어플라이언스 타입으로 공급합니다.

구분		Line up (단위, 명)									
Cloud		10 사용자 부터 (10명 단위)									
구축형	SMB	~50	~100	~200	~300	~400	~500	~600	~700	~800	~900
	ENT	1000	2000	3000	4000	5000	6000	7000	8000	9000	10000

※ 구축형은 고객사 사정에 따라서 SW만 구매할 수 있으며,
기업용 가상화 서버 및 AWS, MS Azure Cloud에서도 구축할 수 있습니다.

✓ "NESS" 와 함께 도입하면 좋은 솔루션은 ?

① Arch5 : 메일 아카이브 솔루션, 실시간 메일 백업 및 압축 저장, 보관메일 검색 및 복원

② CHECKOUT : 승인메일 솔루션, 발신메일 모니터링 및 부서장 승인

NESS

감사합니다.

제품 문의 : 한진호 대표

010-2225-4822, jinho4822@netnsecu.co.kr

백재훈 이사

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