N&S
Network & Security

NESS

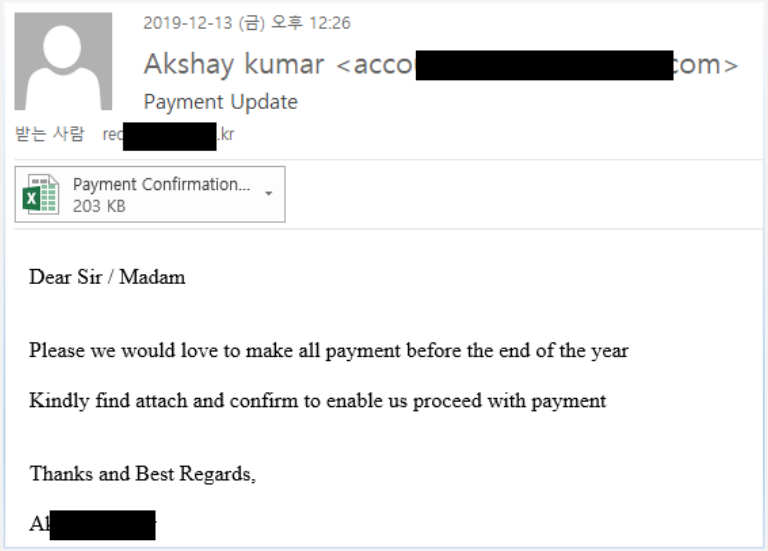
N&S Email Security Suite

2020년
㈜넷엔씨큐

스캠메일이란?

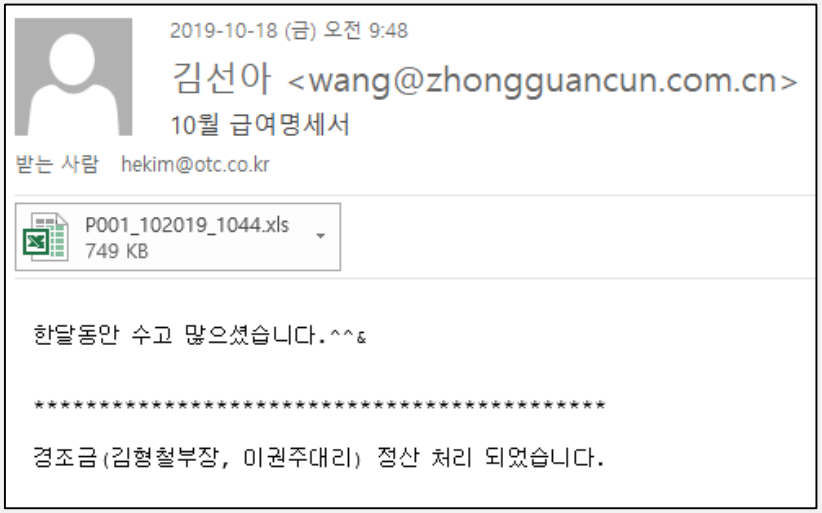
기존의 스팸 및 APT 솔루션으로 차단하지 못하는 신종 메일의 급증

- **무역대금 사기 메일**



- 무역대금 지불과 관련된 사기 메일

- **급여명세서 위장 (사회공학 이용)**



- 급여명세서를 위장한 메일
- 엑셀파일에는 악성코드가 포함되어 있음

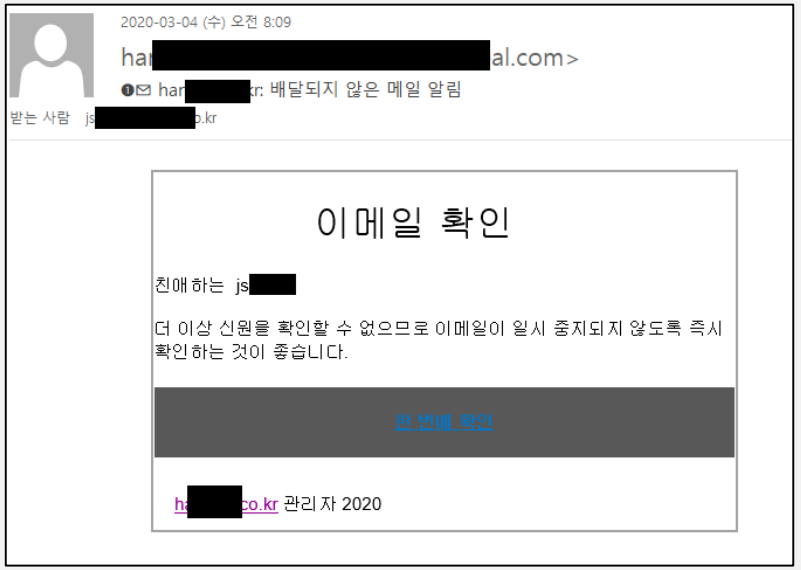
스캠메일이란?

기존의 스팸 및 APT 솔루션으로 차단하지 못하는 신종 메일의 급증

- **국세청 위장**

- 국세청을 위장한 악성 메일
- 첨부파일에 악성코드 포함

- **URL 클릭 시 악성첨부 다운로드**



- '한번에 확인' 링크를 클릭하면 악성파일 다운로드

CONTENTS

1. 제안 배경

이메일 보안 위협

2018년 MS-ISAC 리서치 보고서에 따르면...

표적 공격 중 91% 이상이
이메일에서 시작되고
이메일의 94%가 첨부파일을
가지고 있습니다.

...

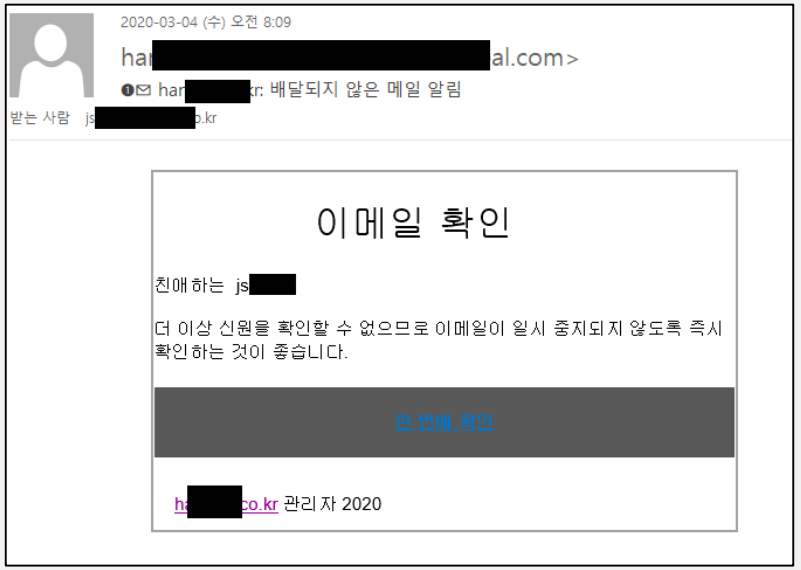
스캠메일이란?

기존의 스팸 및 APT 솔루션으로 차단하지 못하는 신종 메일의 급증

- **국세청 위장**

- 국세청을 위장한 악성 메일
- 첨부파일에 악성코드 포함

- **URL 클릭 시 악성첨부 다운로드**

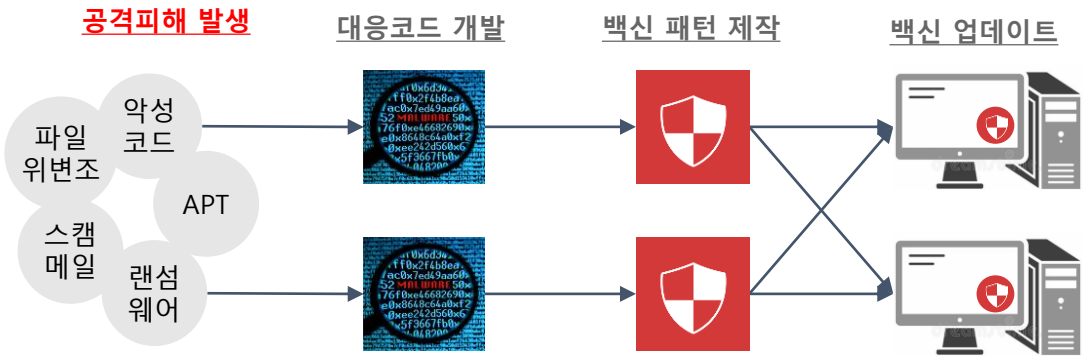


- '한번에 확인' 링크를 클릭하면 악성파일 다운로드

1. 제안 배경

보안 시장 이슈

기존 사후대응 체계인 백신 등의 보안 솔루션 대응 방식은 신•변종 악성코드 대응에 한계점을 보이고 있으므로 사후 대응 방식이 아닌 사전 대응 및 예방하는 형태로 변화 필요



- 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

1. 제안 배경

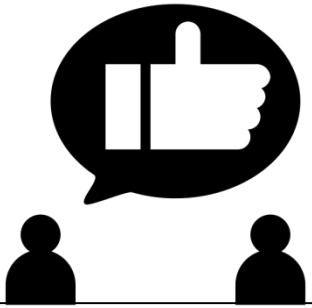
보안 시장 이슈

문서 파일 기반의 보안위협 확대 방어를 위해 파일 위•변종 및 무결성 검증을 위한
CDR 필요성 증대

글로벌 IT 자문기관 "가트너"에서는

악성코드 회피 기술이 발전함에 따라

CDR 사용을 권고하고 있습니다.



Gartner

"As malware sandbox evasion techniques improve, the use of content disarm and reconstruction (CDR) at the email gateway as a supplement or alternative to sandboxing will increase."

Gartner
Fighting Phishing: Optimize Your Defense

1. 제안 배경

As_Is 보안시장 이슈
사이버 위협
사이버 위협 지능화
사이버 위협 기하 급수적 증가
보안솔루션 대응 방식
사후대응으로 신•변종에 취약
우회방법 일반화 됨
문서파일 보안 위협 확대
사회 공학을 이용한 SCAM 메일 출현

To_Be 기술제안

다양한 기능 및 최신 보안체계

- CDR (콘텐츠 살균 처리)
- 악성 코드 검사
- 악성 URL 검사
- 유사 도메인 검사
- 메일 학습
- 스팸/바이러스 메일 차단

N&S Email Security Suite

NESS

기존의 스팸, APT 차단솔루션은 대응 불가

새로운 기법의 차단 제품이 필요합니다.

2. 제품소개

Overview

NESS : N&S Email Security Solution

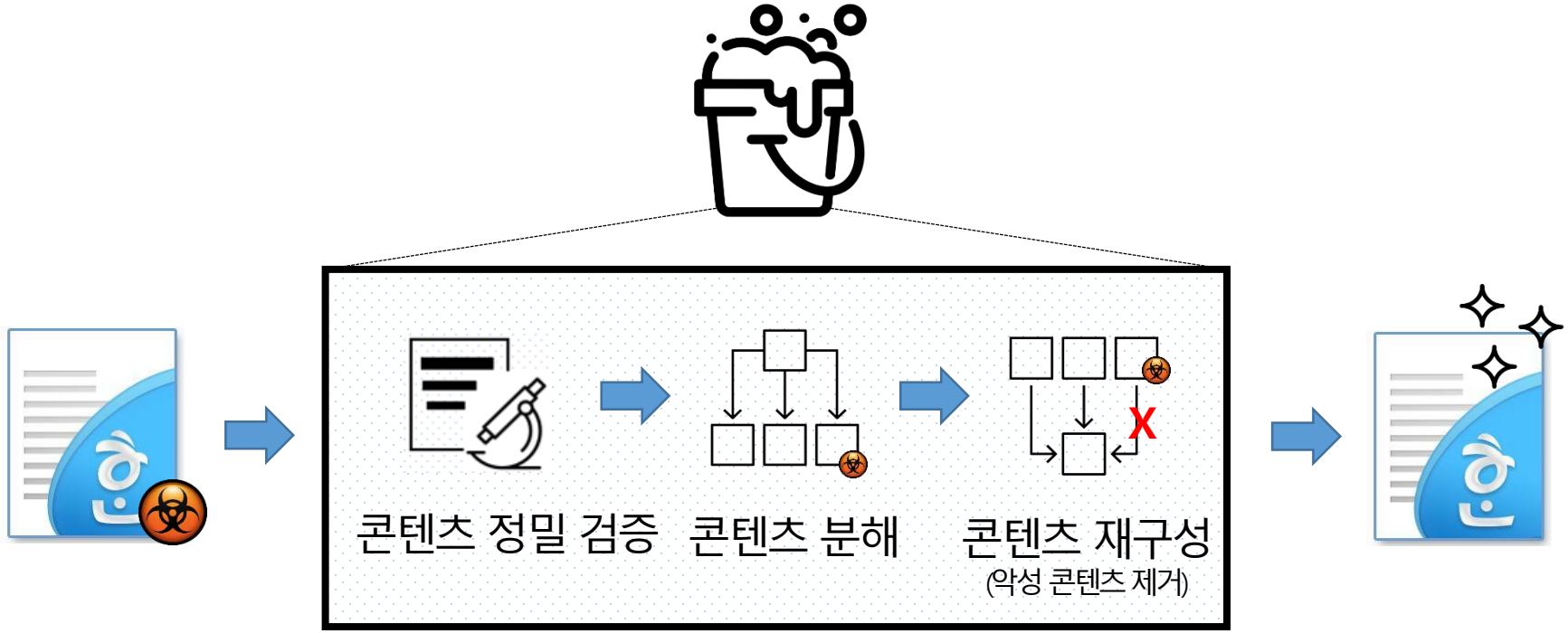
신종 문서형 악성코드이거나 위험한 콘텐츠를 가진 문서일 경우 무해화한 문서를
생성할 수 있는 **CDR(콘텐츠 살균 처리) 기능**을 기본으로
다양한 악성코드 제작자 및 스패머들이 발송한 이메일을 분석하고 학습하여
신종 사기메일/스팸메일/악성코드 관련 메일을 자동으로 판별해는
A.I. 기반의 스캠메일 차단 솔루션입니다.

주요 기능	내 용
CDR (콘텐츠 살균 처리)	• 위험한 콘텐츠를 가진 문서일 경우 CDR 기능을 사용하여 문서를 무해화합니다.
악성코드 검사	• 백신 엔진이 검출하지 못하는 신종 악성코드를 검출하여 치료합니다.
악성 URL 검사	• 메일의 본문에 포함 URL에 대해서 악성 URL 여부를 검사합니다.
유사도메인 검사	• 수신자를 속이기 위한 유사도메인을 검출합니다.
메일 학습	• 사용자별 학습 DB를 구축하고 이를 바탕으로 스캠메일을 분석합니다.

주요 기능

CDR

CDR은 정확히 악성 콘텐츠를 제거하고 안전하게 콘텐츠를 재구성하는 것이 핵심
따라서 , 발생 되는 신•변종의 분석 작업 없이 **사전 방어가 가능**합니다.

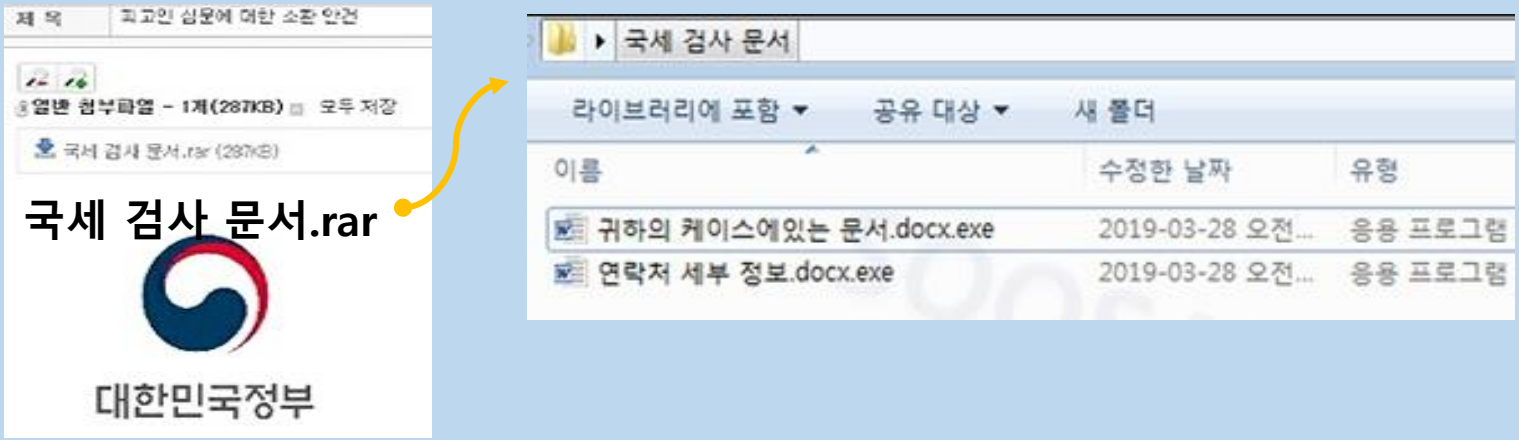


무해화 처리 과정

CDR

■ 기존 CDR 서비스의 한계점 해결

- 최근 CDR을 우회하기 위해 악성코드는 외산 제품이 지원하지 않는 egg, alz(알집) 압축을 사용
  - ✓ **알집을 포함**하여 zip, 7z, rar, cab, tar, gz, xz, bzip 등 **다양한 압축을 지원**
- 다중 압축을 이용한 공격
  - ✓ .hwp 파일을 zip으로 압축하고, 이를 다시 rar로 압축하기를 반복한다면 CDR 우회 시도
    - ➢ **어떤 혼합 형태**의 압축이든, **몇 단계로 다중 압축을 하더라도 처리 가능**

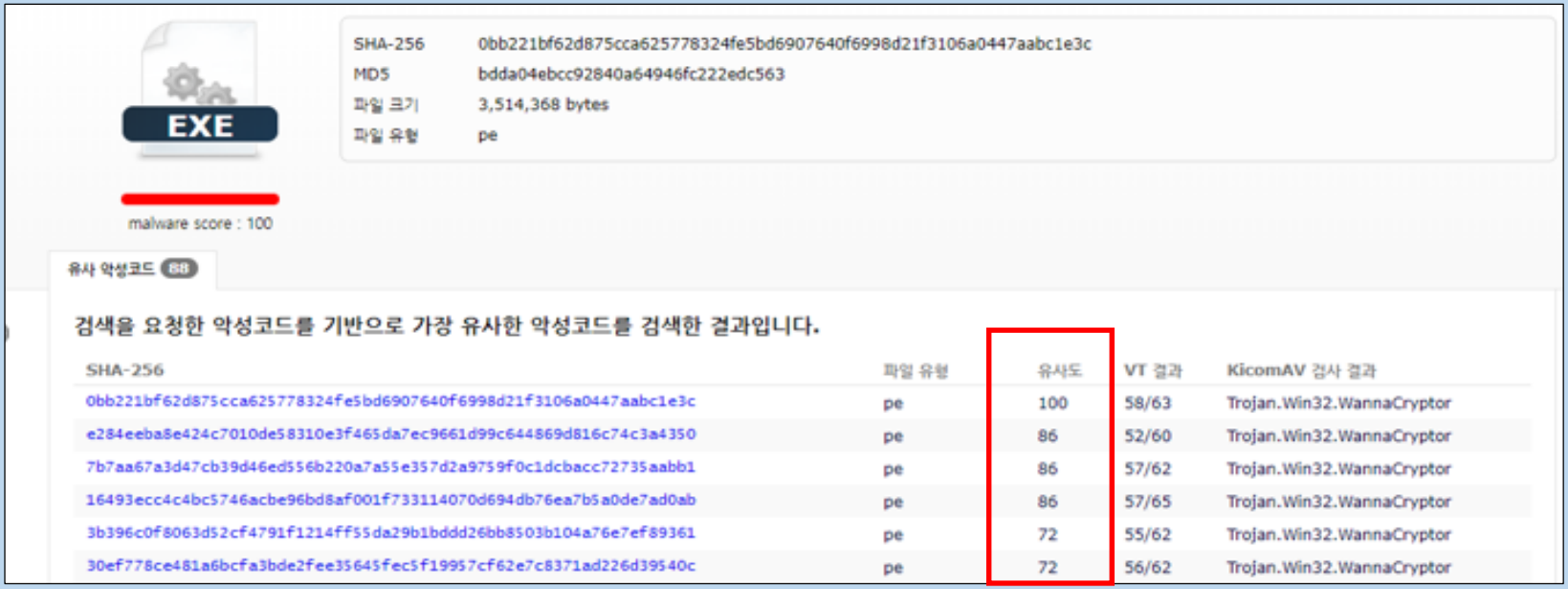


CDR 기능 비교

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

악성코드 검사

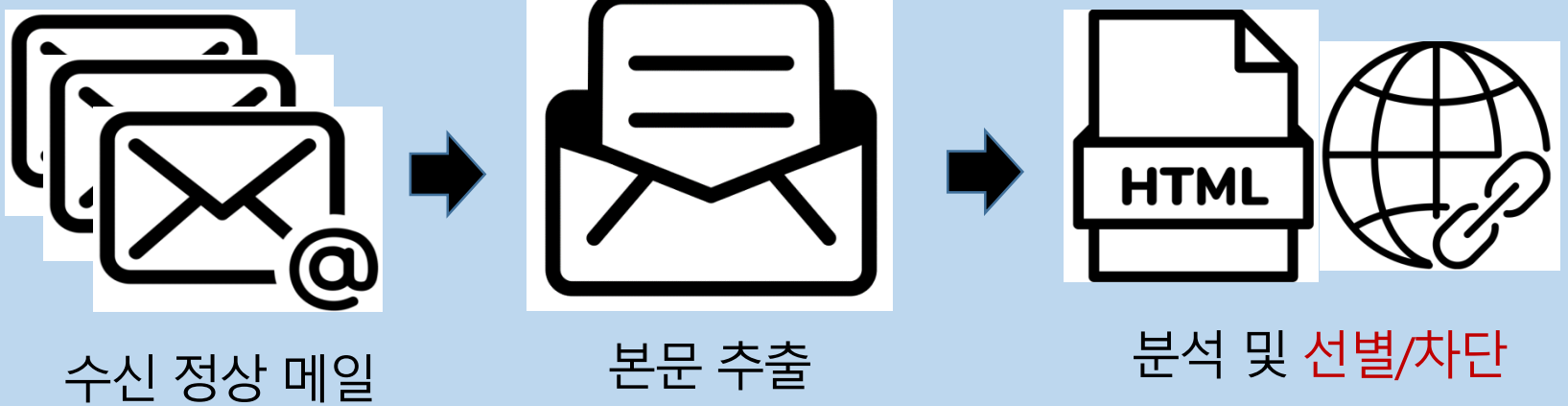
- 첨부파일을 이용한 신•변종 공격행위 차단
- 기존 업데이트 된 패턴을 기반으로 막는 방식의 우회 공격을 차단 할수 있는 파일 DNA 학습 데이타 기반으로 **첨부 파일의 DNA 분석 후 악성 유무를 판별**



SHA-256	파일 유형	유사도	VT 결과	KicomAV 검사 결과
0bb221bf62d875cca625778324fe5bd6907640f6998d21f3106a0447aabc1e3c	pe	100	58/63	Trojan.Win32.WannaCryptor
e284eeba8e424c7010de58310e3f465da7ec9661d99c644869d816c74c3a4350	pe	86	52/60	Trojan.Win32.WannaCryptor
7b7aa67a3d47cb39d46ed556b220a7a55e357d2a9759f0c1dcbacc72735aabb1	pe	86	57/62	Trojan.Win32.WannaCryptor
16493ecc4c4bc5746acbe96bd8af001f733114070d694db76ea7b5a0de7ad0ab	pe	86	57/65	Trojan.Win32.WannaCryptor
3b396c0f8063d52cf4791f1214ff55da29b1bddd26bb8503b104a76e7ef89361	pe	72	55/62	Trojan.Win32.WannaCryptor
30ef778ce481a6bcfa3bde2fee35645fec5f19957cf62e7c8371ad226d39540c	pe	72	56/62	Trojan.Win32.WannaCryptor

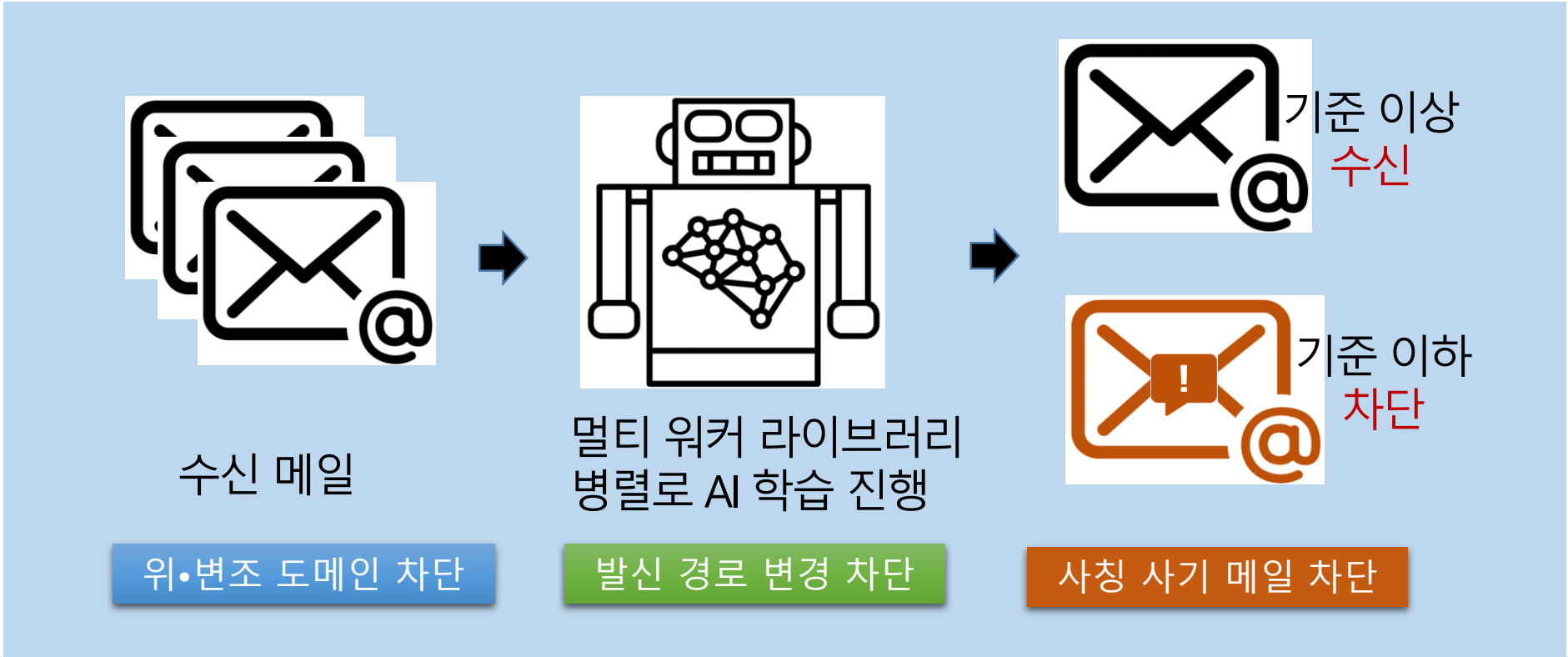
악성 URL 검사

- 메일 본문 분석 및 악성행위 차단
- 패턴 업데이트 방식의 신•변종 대응 문제 한계를 탈피한 악성코드 AI 분석 엔진
- 메일 본문 위·변조 여부 및 URL 검출 및 악성행위 사전 차단
- **본문 소스 내 유해성 유무 검토, 본문 내 URL 검출 후 페이지 및 링크파일에 대한 악성행위 분석**



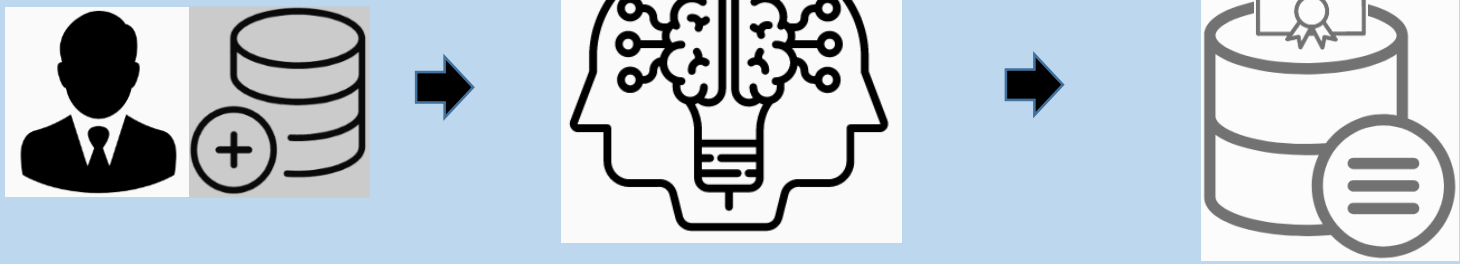
유사 도메인 검사

- 수신된 메일 중 화이트리스트를 학습하고 이를 기반으로 발신자 신뢰성을 보장
- **발신자 주소 위·변조 검사 및 추적, 유사 도메인 비교 검사, 각 메일 별 신뢰도를 수치화**



메일 학습

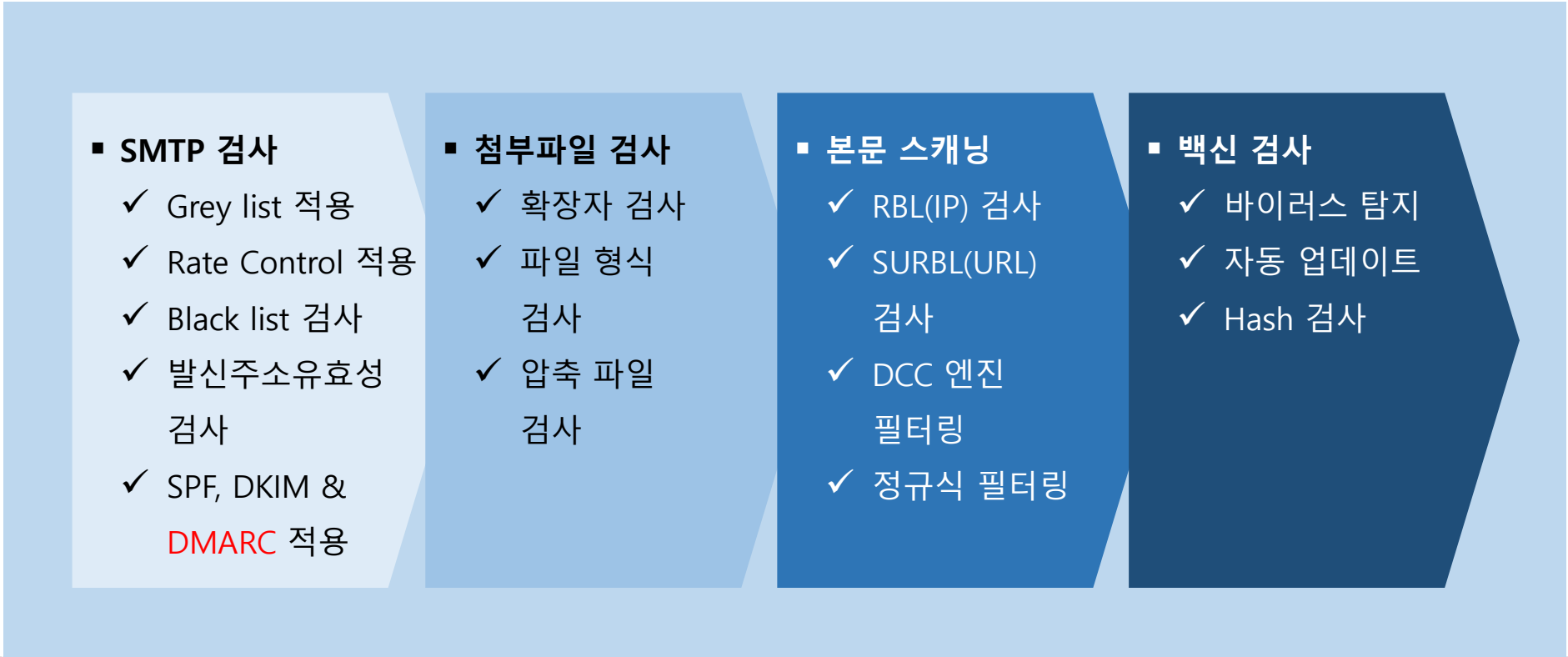
- **내부 계정별 메일의 데이타베이스 구축 후 AI 분석 진행**
- 시스템 구축 시점에서 일정 기간 동안 수신자 별 DB를 구성 후 AI 분석 후 인증된 DB 구성 완료 후 비 정상 메일에 대한 차단 진행



[수신자 별 인증 DB 구성 및 분석]

스팸/바이러스 메일 차단 기능

스팸 메일은 물론 각종 정크메일과 바이러스 메일까지 **4단계의 스캐닝**을 통해 불필요한 메일 및 메일에 포함된 유해 컨텐츠를 차단하고 **메일 서버를 보호**



발송 메일 통제

메일은 피싱 및 스캠 메일에 의한 Email 비밀번호 탈취 등의 보안사고를 예방하고
각종 Compliance에 효과적으로 대비하기 위해서 **보안성 강화 프로그램을 제공**

- **발송메일 통제**
  - ✓정해진 메일계정 외에는 아웃룩을 통해 메일을 발송할 수 없도록 제한
  - ✓메일 발송량 제한 기능
  - ✓발신자 인증 매칭 검사
- **SMTP 보안 차단**
  - ✓일정횟수 이상 인증 실패 시 해당 IP 차단, phishing(피싱) 메일 차단
  - ✓취약한 메일 계정 차단
  - ✓사용자 인증(AUTH) 국가 제한

SMTP 인증IP 목록

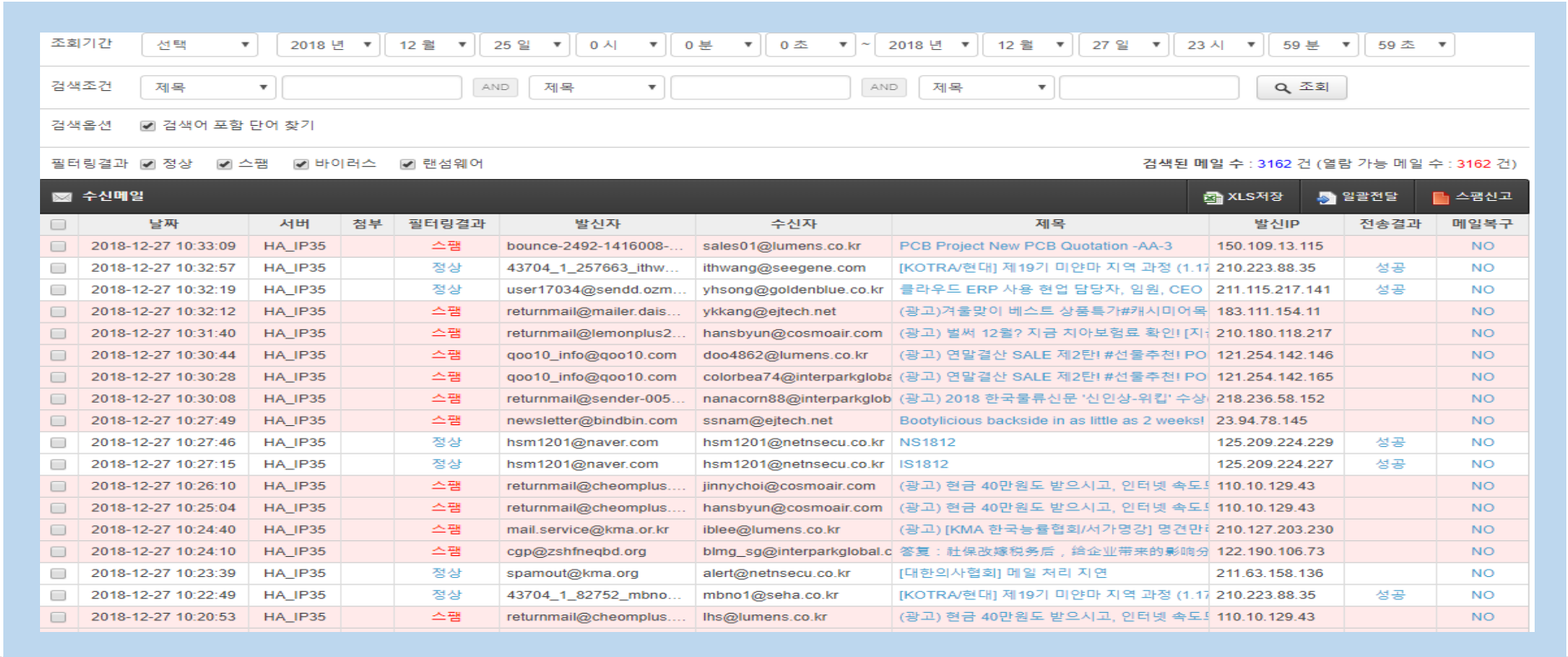
IP	최초탐지시간	최근탐지시간	차단만료시간	인증실패횟수	인증차단횟수	등록타입	정책	발신국
191.53.58.208	2019-07-13 06:21:51	2019-07-16 09:37:23	2019-07-16 10:37:23	3	0	자동	탐지	BR
117.95.19.31	2019-07-16 08:55:53	2019-07-16 08:56:46	2019-07-16 09:56:46	3	7	자동	탐지	CN
191.53.197.186	2019-07-10 19:40:46	2019-07-16 06:19:53	2019-07-16 07:19:53	3	0	자동	탐지	BR
170.150.48.148	2019-07-12 21:20:37	2019-07-16 03:15:46	2019-07-16 04:15:46	3	0	자동	탐지	BR
177.129.206.188	2019-07-09 04:29:51	2019-07-16 01:14:45	2019-07-16 02:14:45	3	0	자동	탐지	BR
168.228.148.253	2019-07-06 18:30:39	2019-07-15 23:55:50	2019-07-16 00:55:50	3	0	자동	탐지	BR
189.91.6.177	2019-07-08 06:36:21	2019-07-15 22:06:24	2019-07-15 23:06:24	3	0	자동	탐지	BR
81.169.168.25	2019-07-15 19:20:46	2019-07-15 21:44:41	2019-07-15 22:44:41	3	0	자동	탐지	DE
205.252.237.195	2019-07-15 08:07:41	2019-07-15 08:07:52	2019-07-15 09:07:52	3	0	자동	탐지	US

관리자 화면_대시 보드

- 수발신 메일 현황 및 스팸 순위 정보 제공
- 필터 및 백신 업데이트 현황 보기

관리자 화면_메일 관리

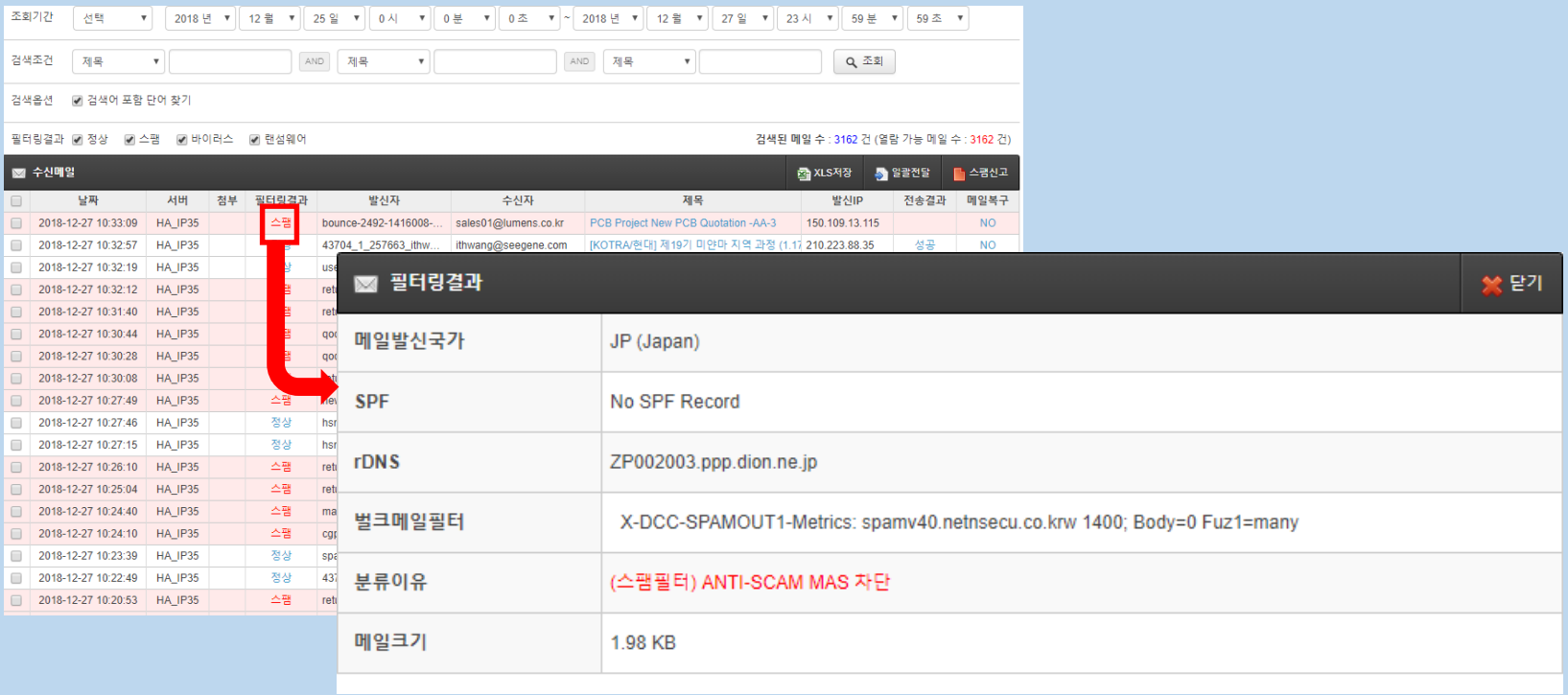
- 수신, 발신 메일 분리 및 거부 메일 분류
- 스팸 메일에 대한 직관적인 표시



날짜	서버	첨부	필터링결과	발신자	수신자	제목	발신IP	전송결과	메일복구
2018-12-27 10:33:09	HA_IP35		스팸	bounce-2492-1416008-...	sales01@lumens.co.kr	PCB Project New PCB Quotation -AA-3	150.109.13.115		NO
2018-12-27 10:32:57	HA_IP35		정상	43704_1_257663_ithw...	ithwang@seegene.com	[KOTRA/현대] 제19기 미얀마 지역 과정 (1.17	210.223.88.35	성공	NO
2018-12-27 10:32:19	HA_IP35		정상	user17034@sendd.ozm...	yhsong@goldenblue.co.kr	클라우드 ERP 사용 현업 담당자, 임원, CEO	211.115.217.141	성공	NO
2018-12-27 10:32:12	HA_IP35		스팸	returnmail@mailer.dais...	ykkang@ejtech.net	(광고)겨울맞이 베스트 상품특가#캐시미어목	183.111.154.11		NO
2018-12-27 10:31:40	HA_IP35		스팸	returnmail@lemonplus2...	hansbyun@cosmoair.com	(광고) 벌써 12월? 지금 치아보험료 확인! [지	210.180.118.217		NO
2018-12-27 10:30:44	HA_IP35		스팸	qoo10_info@qoo10.com	doo4862@lumens.co.kr	(광고) 연말결산 SALE 제2탄! #선물추천! PO	121.254.142.146		NO
2018-12-27 10:30:28	HA_IP35		스팸	qoo10_info@qoo10.com	colorbea74@interparkgloba	(광고) 연말결산 SALE 제2탄! #선물추천! PO	121.254.142.165		NO
2018-12-27 10:30:08	HA_IP35		스팸	returnmail@sender-005...	nanacorn88@interparkglob	(광고) 2018 한국물류신문 '신인상-워킵' 수상	218.236.58.152		NO
2018-12-27 10:27:49	HA_IP35		스팸	newsletter@bindbin.com	ssnam@ejtech.net	Bootylicious backside in as little as 2 weeks!	23.94.78.145		NO
2018-12-27 10:27:46	HA_IP35		정상	hsm1201@naver.com	hsm1201@netnsecu.co.kr	NS1812	125.209.224.229	성공	NO
2018-12-27 10:27:15	HA_IP35		정상	hsm1201@naver.com	hsm1201@netnsecu.co.kr	IS1812	125.209.224.227	성공	NO
2018-12-27 10:26:10	HA_IP35		스팸	returnmail@cheomplus....	jinnychoi@cosmoair.com	(광고) 현금 40만원도 받으시고, 인터넷 속도도	110.10.129.43		NO
2018-12-27 10:25:04	HA_IP35		스팸	returnmail@cheomplus....	hansbyun@cosmoair.com	(광고) 현금 40만원도 받으시고, 인터넷 속도도	110.10.129.43		NO
2018-12-27 10:24:40	HA_IP35		스팸	mail.service@kma.or.kr	iblee@lumens.co.kr	(광고) [KMA 한국능률협회/서가명강] 명견만리	210.127.203.230		NO
2018-12-27 10:24:10	HA_IP35		스팸	cgp@zshfneqbd.org	blmg_sg@interparkglobal.c	答复：社保改嫁税务后，给企业带来的影响分	122.190.106.73		NO
2018-12-27 10:23:39	HA_IP35		정상	spamout@kma.org	alert@netnsecu.co.kr	[대한의사협회] 메일 처리 지연	211.63.158.136		NO
2018-12-27 10:22:49	HA_IP35		정상	43704_1_82752_mbno...	mbno1@seha.co.kr	[KOTRA/현대] 제19기 미얀마 지역 과정 (1.17	210.223.88.35	성공	NO
2018-12-27 10:20:53	HA_IP35		스팸	returnmail@cheomplus....	lhs@lumens.co.kr	(광고) 현금 40만원도 받으시고, 인터넷 속도도	110.10.129.43		NO

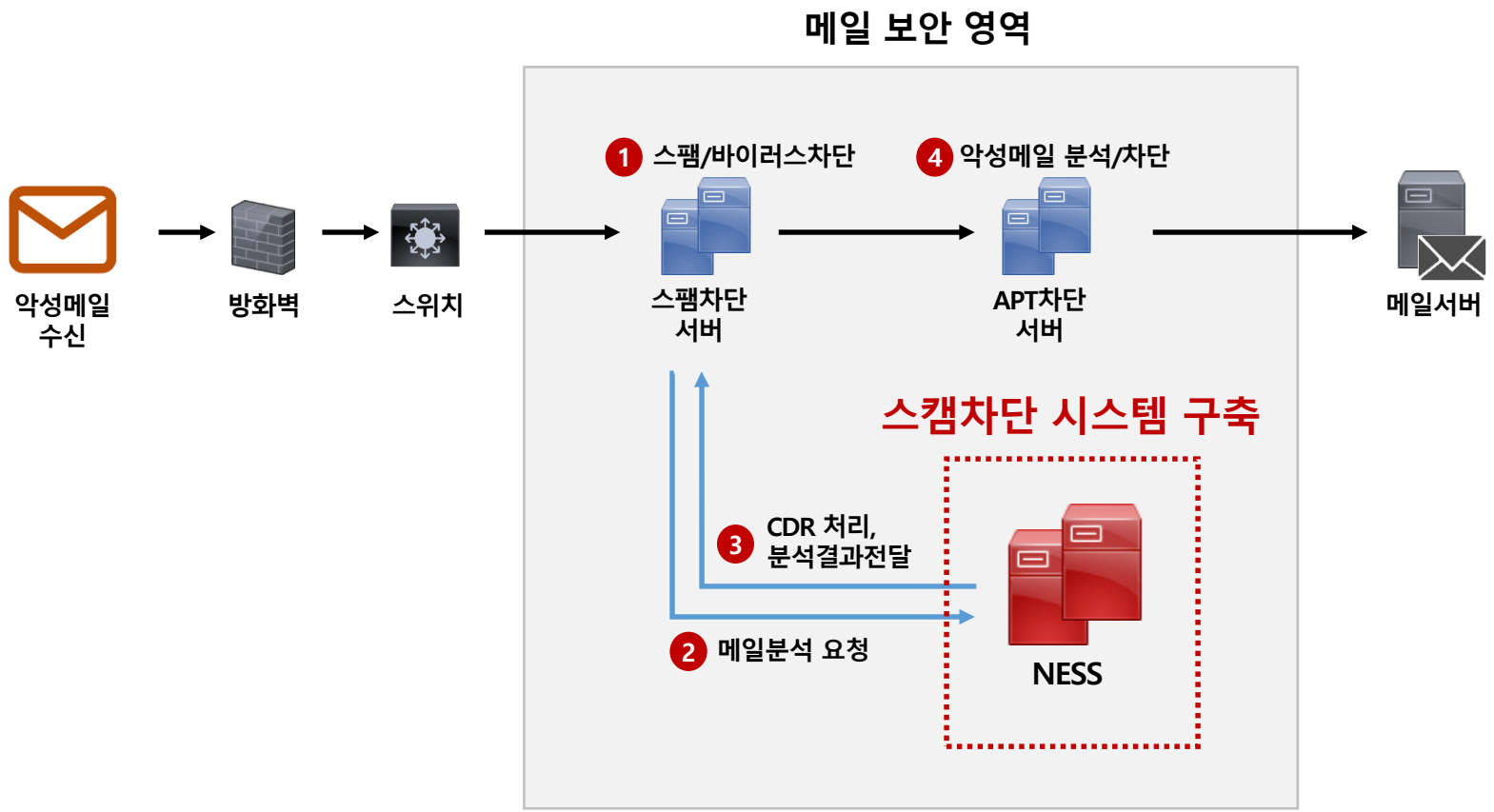
관리자 화면_악성코드 탐지

- 메일리스트에서 필터링 결과(분류이유) 제공



3. Service Flow

구축 후 시스템 구성도



4. 특장점(vs. Anti-Virus & 동적분석)

구분	Anti-Virus	SandBox	NESS
위협에 대한 보호수준	● 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 피하고, 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.
레이턴시	● 시스템 작동이 느려질 수 있음 - 패턴(DB) 업데이트 및 실시간 감시와 같은 백그라운드 프로세스 등은 시스템에 영향을 미칠 수 있음.	● 동적분석을 위한 파일 처리 시간이 길어져 병목 현상 발생으로 효율성이 저하됨. - 모든 파일에 대한 동적 분석을 위해 병목 현상이 발생 할 수 있어, 이로인한 온라인 프로세스가 느려짐.	● **NESS**는 유사도 분석(특허) 기술로 수초 내 가장 유사한 악성코드 탐지가 가능함. ● CDR은 악성 위협만을 제거함으로 악성 콘텐츠가 없으면 1초 내로 파일 무해화 진행.

4. 특장점(vs. Anti-Virus & 동적분석)

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 원활하게 유지 하기 위한 IT 자원의 비용이 많이 소요됨.	● 시스템 연동 방식으로 중앙 집중 관리 가능 ● 동적분석 기반의 REST API 및 JAVA(JNI) 연동(필요시 Appliance 최소화)
정책 요구사항	● 정상 파일이 차단될 수 있으며, 신·변종 악성 파일을 사용자가 열 수 있음 - 정상 파일을 차단하는 오진의 위험성을 내포하고 있고, 탐지 못하는 악성파일 실행으로 업무 생산성이 저하됨.	● 복잡한 보안 정책과 어려운 결정을 수반 - 파일의 악의적인 행위의 등급을 판단하는 정책을 지속적으로 결정해야 하지만, 많은 위협이 이런 정책을 우회함으로 책임이 전가될 수 있음.	● CDR 프로세스에 의해 정화된 문서 파일은 완전한 기능을 유지하여 항상 안전함. ● CDR은 조직으로 유입되는 모든 문서 파일을 대상으로 하므로 어려운 정책 결정은 없음.

5. 도입 효과

알수없는 수 많은
악성코드 위협에
대한 효율적인 대응

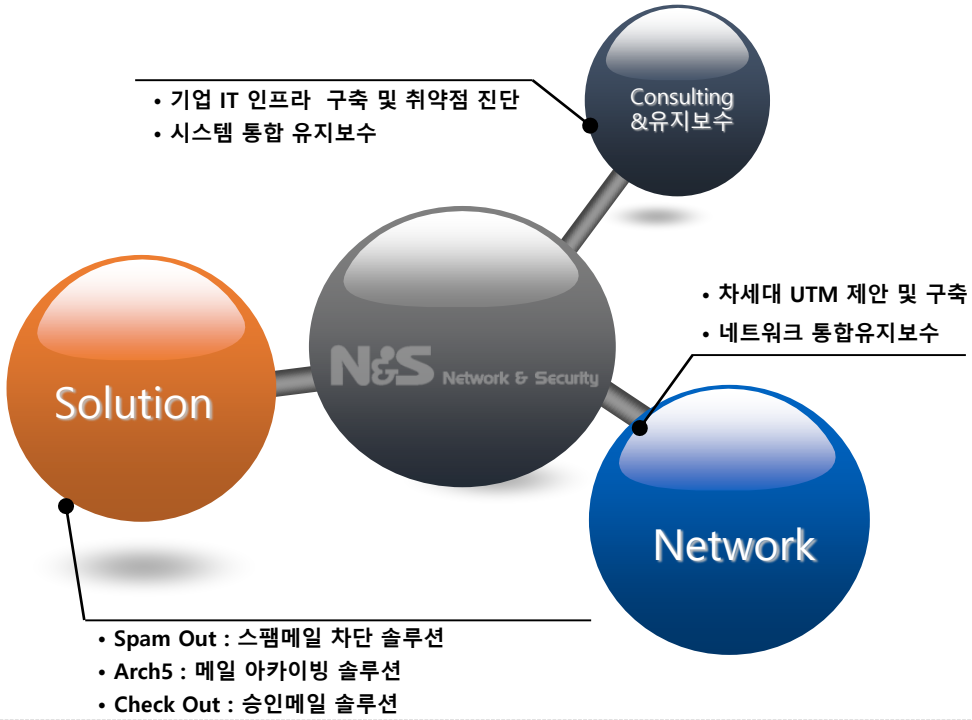
한번만 성공하면 되는
공격자의 **신•변종 악성코드**
공격의 효과적인 대응

악성코드 탐지·분석·대응 까지의
시간에 발생하는
피해를 최소화

5. 회사 소개

 # 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



✓ 일반 현황

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, 1110호 (가산동, 벽산디지털밸리5차)		
전 화 번 호	전화 : 02-2633-6102 FAX : 02-2633-6192		
홈 페 이 지	http://www.spamout.co.kr		

NESS

감사합니다.

제품 문의

백재훈 이사

010-9755-6372,

baek@netnsecu.co.kr