You Can’t Protect What You Can’t See

HTTPS를 통한 보안위협과 대처방안

SOMANSA

CONTENTS

I. HTTPS 위협

No Time Left to Hesitate

HTTPS는 전체 트래픽의 60-80% 차지

1. 웹 메 일: Gmail, NAVER, DAUM(2016년 10월 5일)
   Hotmail(Outlook), Yahoo 등 모든 상용웹메일

2. 웹 하 드: 구글드라이브, KT클라우드, 드롭박스,
   네이버클라우드(옵션) 등 주요 웹하드 서비스

3. SNS : FACEBOOK, Twitter등 주요 SNS서비스도 모두 HTTPS

4. 클라우드서비스 : 사용자 계정기반의 글로벌 서비스 모두 HTTPS

상용웹메일	웹하드/클라우드	SNS
Gmail NAVER Y! Outlook DAUM	Google Drive ucloud Dropbox	facebook twitter TALK [차단만 가능] LINE [차단만 가능]

SOMANSA

공공기관 인터넷 접속 통제 규정 준수

공공기관 HTTPS 접속 사이트 통제 필요성 강화

1. **2016 공공기관 상용웹메일 차단 규정**
   - (NAVER, DAUM, GOOGLE, OUTLOOK 웹메일) 등 주요한 상용웹메일 모두 HTTPS 통신 사용

2. **유해사이트 접근 통제 무력화 이슈**
   - HTTPS통신을 사용하는 도박사이트, 음란사이트, P2P사이트 증가
   - HTTPS통신을 사용하는 구글 번역사이트를 통해서 유해사이트 우회접속 빈번

3. **HTTPS 웹서비스를 통한 악성코드 유입 통제 이슈**
   - HTTPS 컨텐트에 대한 가시성 확보 필수

행정안전부

nis

정보통신 보안업무규정 준수

- ✓ **(33조) 상용웹메일 접속차단**
- ✓ **(34조) P2P와 웹하드/메신저 프로그램 설치제한**
- ✓ **(35조) 불법사이트 접속 및 프로그램 다운로드 금지**
- ✓ **(37조) 악성코드 유입방지**

SOMANSA

악성코드 배포 사이트 차단

HTTPS 웹사이트를 통한 악성코드 감염 증가(drive by download)

1. 웹 사이트를 악용한 공격 증가로 기업 내 보호책 마련이 시급함
2. 개인정보 유출이나 랜섬웨어 감염

총 악성코드 발생 추이

(2012) 1억 → (2015) 4억7천개

신종 악성코드 발생 추이

(2015년 1억4천 건, 2012년 대비 4배↑)

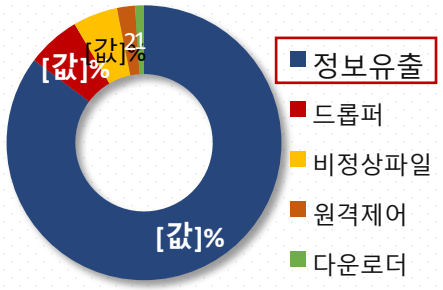
악성코드 경유지

① 엔터테인먼트, 여행·음식·숙박, 조합·협회, 부동산

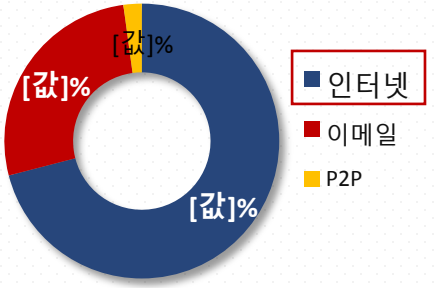
② 커뮤니티, 택배·교통, 언론, 웹호스팅, 취업 등

③ 웹하드, 병원·의료, 종교, 블로그, 포털, 교육 등

악성코드 목적 유형



랜섬웨어 감염경로



보안이 취약한 웹사이트 및 APP에 은닉하여 악성코드 침투	공격자의 주 목적은 정보유출 (81%)	웹사이트 방문이 주 감염경로

출처: AV-TEST, KISA (2016), 랜섬웨어침해대응센터(2015)

SOMANSA

SOMANSA

II. Web Security 기술 트랜드

유해사이트 차단

Web Security 진화 방향

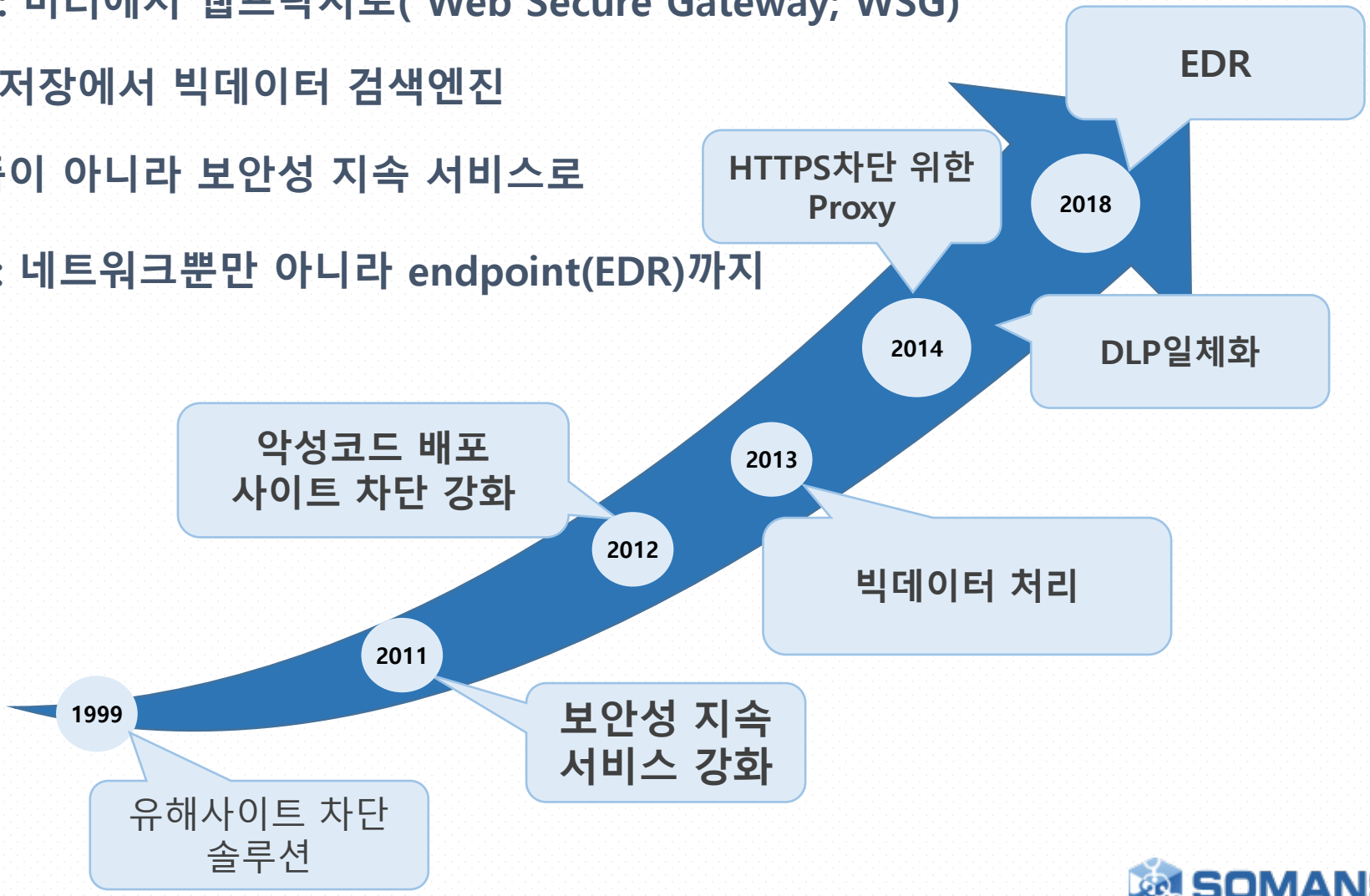
차단 대상 : 비업무 사이트 차단에서 악성코드 배포사이트 차단으로, 유출통제까지

네트워크 : 미러에서 웹프락시로(Web Secure Gateway; WSG)

검색 : DB 저장에서 빅데이터 검색엔진

지원 : 납품이 아니라 보안성 지속 서비스로

분석대상 : 네트워크뿐만 아니라 endpoint(EDR)까지



SOMANSA

Web Secure Gateway (Web Proxy) : 정교한 HTTPS 접속 차단

1. HTTP/HTTPs WebProxy

- WebProxy는 사용자 웹브라우져와 웹서비스사이에서 HTTPS암호화 통신을 중계하기에 주고받은 내용을 평문 확인 (visibility; 가시성)
- 사용자 브라우져와 WebProxy사이에 암호화 통신 중계 , WebProxy와 웹서비스사이에 암호화 통신을 중계
- WebProxy는 유해사이트 접속시 차단하며, 악성코드 배포 사이트 접속시 차단
- DLP일체형으로 개인정보 유출통제 기능 수행

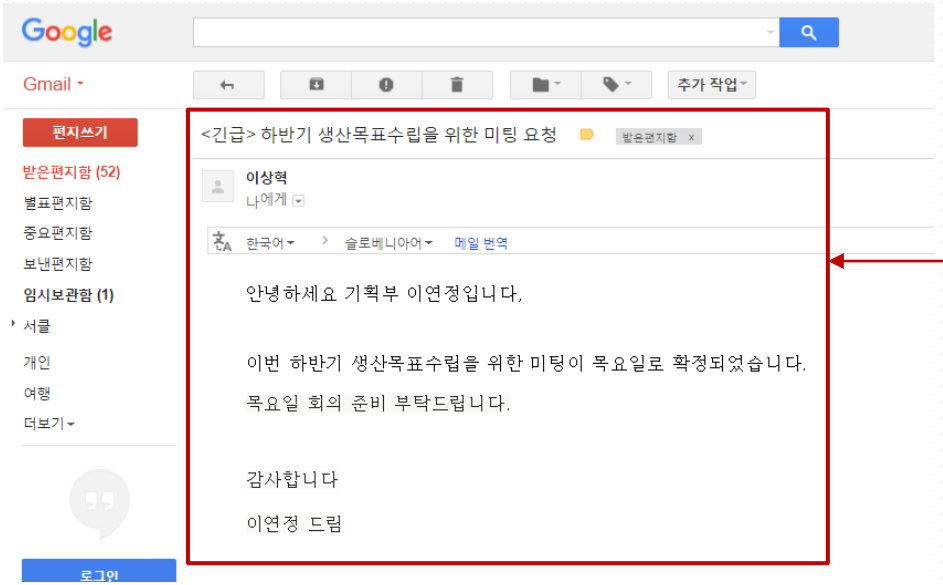
2. HTTPS의 페이지단위 통제, 상용웹메일 쓰기통제, SNS채널별 접속통제, HTTPS 우회접속 통제, 악성코드 배포 사이트 접속 통제 제공

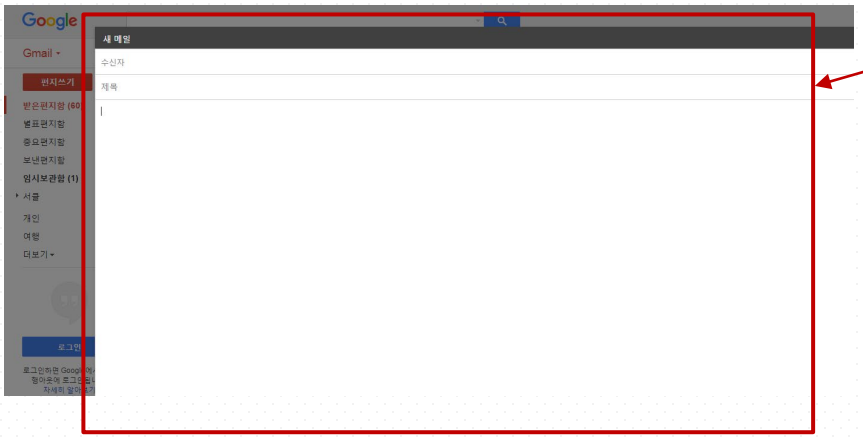
<HTTPS 통신 가시화 및 차단>

SOMANSA

상용웹메일 접속 차단

상용웹메일 자체를 원천적으로 통제
구글, DAUM, NAVER등 HTTPS를 사용하는 상용웹메일에 대해서 (특정 사용자에 대해서만)
읽기는 허용, 쓰기는 차단





Web 설정

주요웹메일읽기 | 통과 | **허용** | 차단

상용웹메일에서 메일 읽기가 가능

주요웹메일쓰기 | 통과 | 허용 | **차단**

상용웹메일에서
메일 쓰기 기능은 차단

SOMANSA

SNS 계정별 통제

FACEBOOK 등 HTTPS를 사용하는 SNS에 대해서 특정한 계정만을 차단하거나 허용

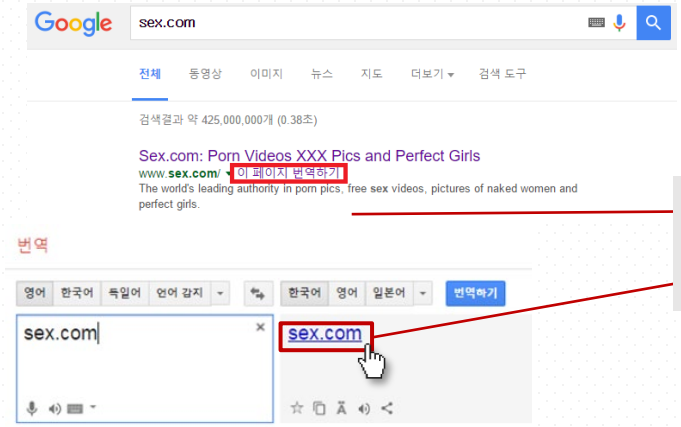
URL 호스트 추가로
도박 계정 접속 차단

패턴 추가로 해당(음란)
문자열이 포함된 URL 접속 차단

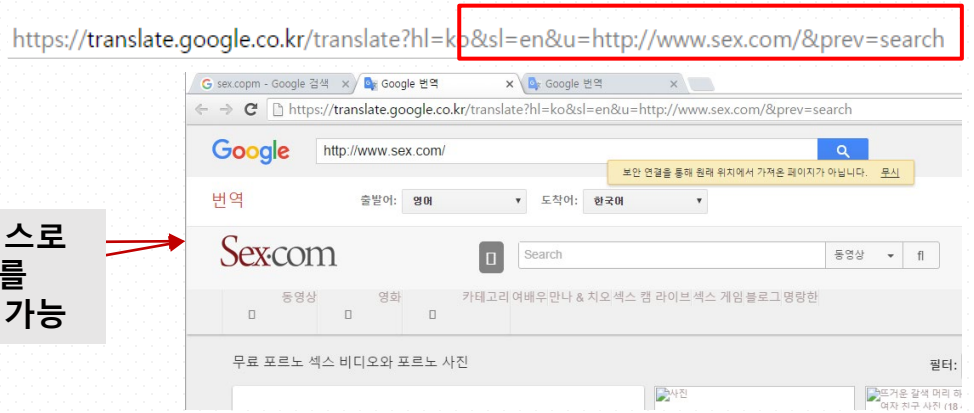
SOMANSA

구글 우회접속통제

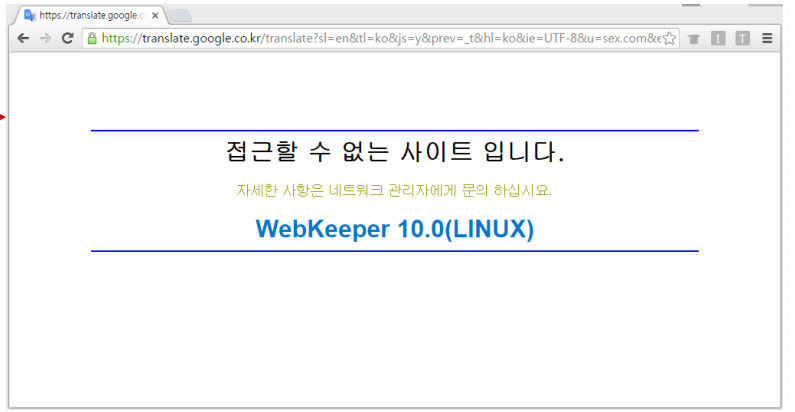
구글 번역 서비스를 프록시(Proxy) 서버로 이용하여 차단사이트를 우회 가능
WSG 프록시를 통해서 유해사이트에 우회접속 하는 것을 차단



구글 번역 서비스로
음란사이트를
쉽게 우회접속 가능



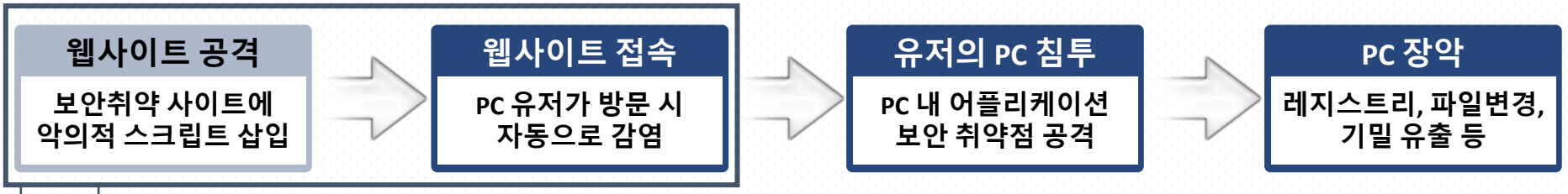
구글 번역 서비스를
이용해도
음란사이트
우회접속 불가



악성코드 배포사이트 차단

웹 접속만으로 악성코드가 배포되는 드라이브 바이 다운로드(Drive-By-Download)를 차단
연간 300만건이상 악성코드 배포사이트 DB를 갱신, 15분에 한번씩 업데이트

드라이브 바이 다운로드 공격 시나리오



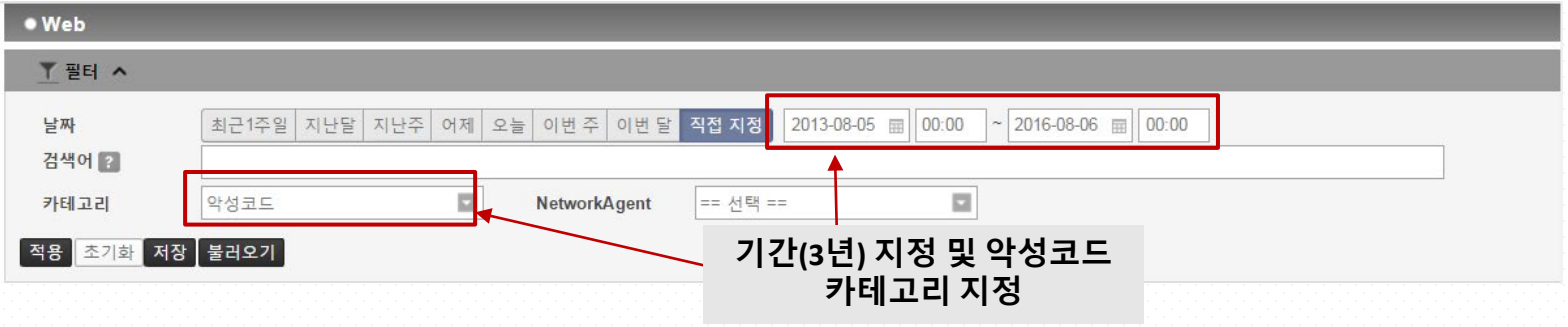
- 하루에 방문하는 수 많은 웹사이트 중 보안이 취약한 웹사이트 다수 존재
- 사용자의 행동과 무관하게 경고 없이 공격, 피해 확산 후 인지

- 악성코드 배포사이트 차단을 통해 드라이브 바이 다운로드 예방

빅데이터 검색: APT대처

3년치 인터넷 접속 내역을 3분이내 검색 (DB방식대비 100배속도 개선)

<3년치 악성코드 배포 사이트 접속 검색결과>



부서 이름	사용자 이름	대응 행동	카테고리	호스트	서브 URL	파일 개수	사용자 IP	서버 IP	발생 일시	정책
Intelli Agent 1팀	임태화	차단	악성코드	su5.ahnlab.com/	/onetouch_b/patch/e5/win	0	192.168.9.110	182.162.157.17	2016-06-07 13:02:10	Malicious code Site
Intelli Agent 1팀	임태화	차단	악성코드	su5.ahnlab.com/	/onetouch_b/patch/e5/win	0	192.168.9.110	182.162.157.146	2016-06-07 13:03:36	Malicious code Site
기술Y팀	윤창기	차단	악성코드	su5.ahnlab.com/	/onetouch_b/patch/e5/win	0				
기술Y팀	윤창기	차단	악성코드	su5.ahnlab.com/	/onetouch_b/patch/e5/win	0				
기술Y팀	윤창기	차단	악성코드	su5.ahnlab.com/	/onetouch_b/patch/e5/win	0				
기술Y팀	윤창기	차단	악성코드	su5.ahnlab.com/	/onetouch_b/patch/e5/win	0				
기술Y팀	윤창기	차단	악성코드	su5.ahnlab.com/	/onetouch_b/patch/e5/win	0	10.10.8.1	182.162.157.25	2016-06-16 17:06:04	Malicious code Site
기술Y팀	윤창기	차단	악성코드	su5.ahnlab.com/	/onetouch_b/patch/e5/win	0	10.10.8.1	182.162.157.147	2016-06-09 13:54:43	Malicious code Site
기술Y팀	윤창기	차단	악성코드	su5.ahnlab.com/	/onetouch_b/patch/e5/win	0	10.10.8.1	182.162.157.24	2016-06-13 17:45:31	Malicious code Site
기술Y팀	윤창기	차단	악성코드	su5.ahnlab.com/	/onetouch_b/patch/e5/win	0	10.10.8.1	182.162.157.149	2016-06-09 13:55:45	Malicious code Site
기술E팀	정상군	차단	악성코드	su5.ahnlab.com/	/onetouch_b/patch/e5/win	0	10.10.0.60	182.162.157.141	2016-06-03 13:26:26	Malicious code Site
기술E팀	정상군	차단	악성코드	su5.ahnlab.com/	/onetouch_b/patch/e5/win	0	10.10.0.60	182.162.157.19	2016-06-03 13:26:57	Malicious code Site
기술E팀	정상군	차단	악성코드	su5.ahnlab.com/	/onetouch_b/patch/e5/win	0	10.10.0.60	182.162.157.148	2016-06-03 13:27:07	Malicious code Site
기술I팀	박승훈	차단	악성코드	220.73.162.3/	/Download/WinCtrProc.ex	0	10.10.7.61	220.73.162.3	2016-06-10 12:00:29	Malicious code Site
기술I팀	박승훈	차단	악성코드	220.73.162.4/	/Download/WinCtrProc.ex	0	10.10.7.61	220.73.162.4	2016-06-10 12:02:13	Malicious code Site
기술I팀	박승훈	차단	악성코드	220.73.162.4/	/Download/WinCtrProc.ex	0	10.10.7.61	220.73.162.4	2016-06-10 12:10:30	Malicious code Site

3분 내에 악성코드 배포사이트 접속 로그 확인 가능

SOMANSA

미러방식 (SNI)과 프락시 방식 비교 : 유해 사이트 차단

항목	기존 솔루션 WebKeeper Mirror	WebKeeper SG
차단율	트래픽 폭주시 차단 불가	차단 100%
상용웹메일 읽기허용/ 쓰기만 차단	불가	완벽
구글 번역기 우회접속 차단	구글 번역기 기능 활용 불가	정교한 차단 구글의 언어 번역기능 활용은 허용하면서 번역기통해서 우회접속하것만 차단
FACEBOOK, TWITTER, 인스타그램 계정별 차단	불가능	특정 계정만 차단
FACEBOOK 등 SNS에 읽기는 허용, 자료 작성은 차단	불가능	가능
HTTP/HTTPS 접속기록 저장	HTTPS접속 기록 제한적	HTTPS까지 페이지단위 세부적인 접속로그 저장
HTTPS 응답값에 악성코드 의심되는 파일이 있을 경우	응답값 내용을 볼수없기에 대처불가	HTTPS 응답값 파일을 볼수있고 악성코드 의심시 분석가능

SOMANSA

III. WEB Security 소개

DLP 개인정보 유출통제

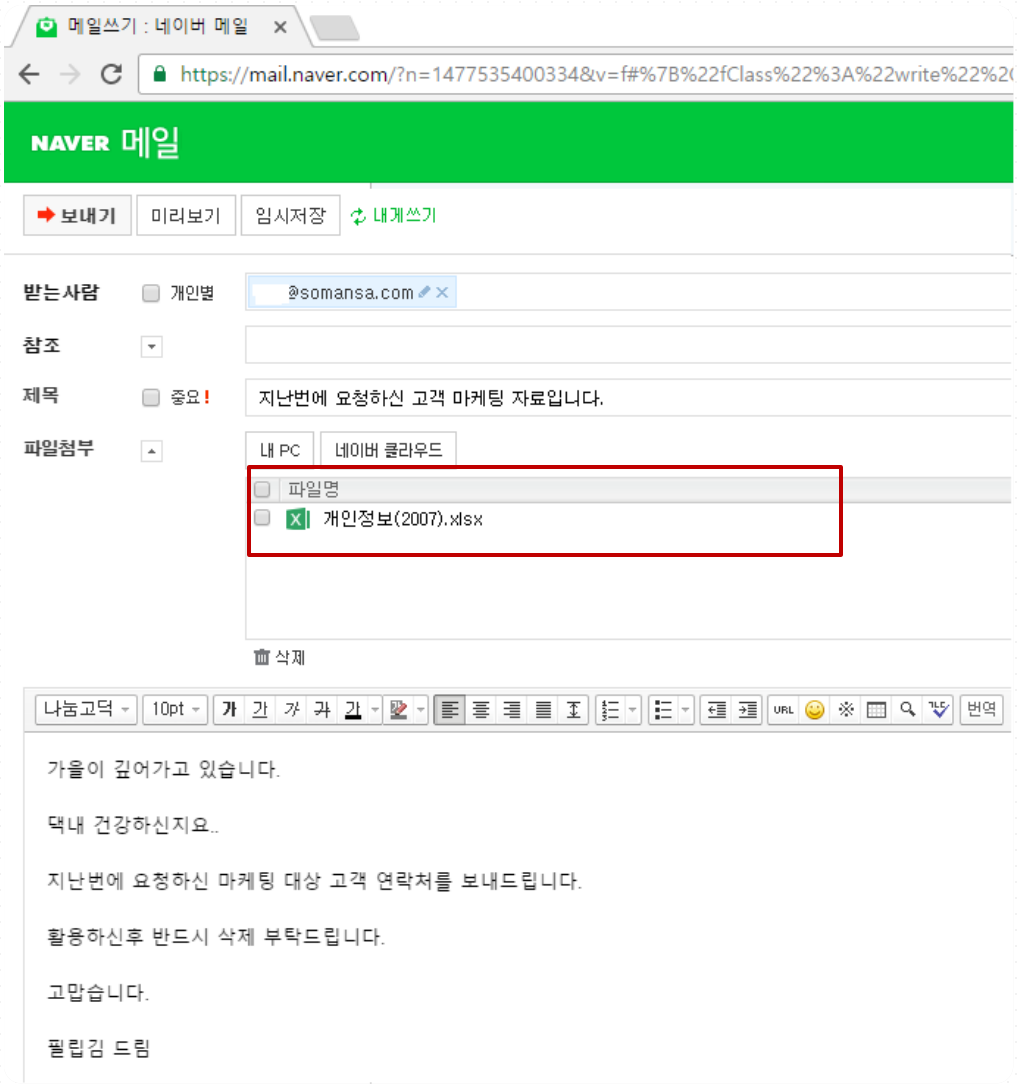
SOMANSA

HTTPS 개인정보 유출 통제 필요성

HTTPS : 개인정보유출을 위한 안전한 터널 보장, 네트워크 컨텐츠 보안장비 무력화

사전 통제불가, 로그 확보불가,
고객 주민번호 1000만건 G-mail로 친구에게 부주의하게 전송한다면

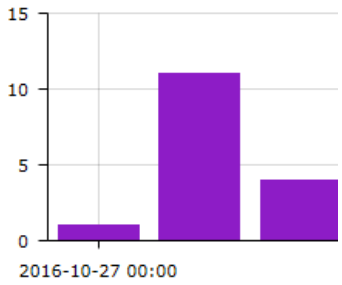
사례 : 네이버웹메일 통한 개인정보 유출통제



SOMANSA

사례 : 네이버메일

차트



내보내기 태그 입력

	부서 이름	사용자 이름	카테고
☐	CEO	김대환	웹메일
☐	예외그룹	오근문_예외	웹메일

제목	지난번에 요청하신 고객 마케팅 자료입니다.
보낸 사람	'@naver.com
받는 사람	@somansa.com
참조	
숨은 참조	

가을이 깊어가고 있습니다.

댁내 건강하신지요..

지난번에 요청하신 마케팅 대상 고객 연락처를 보내드립니다.

활용하신후 반드시 삭제 부탁드립니다.

고맙습니다.

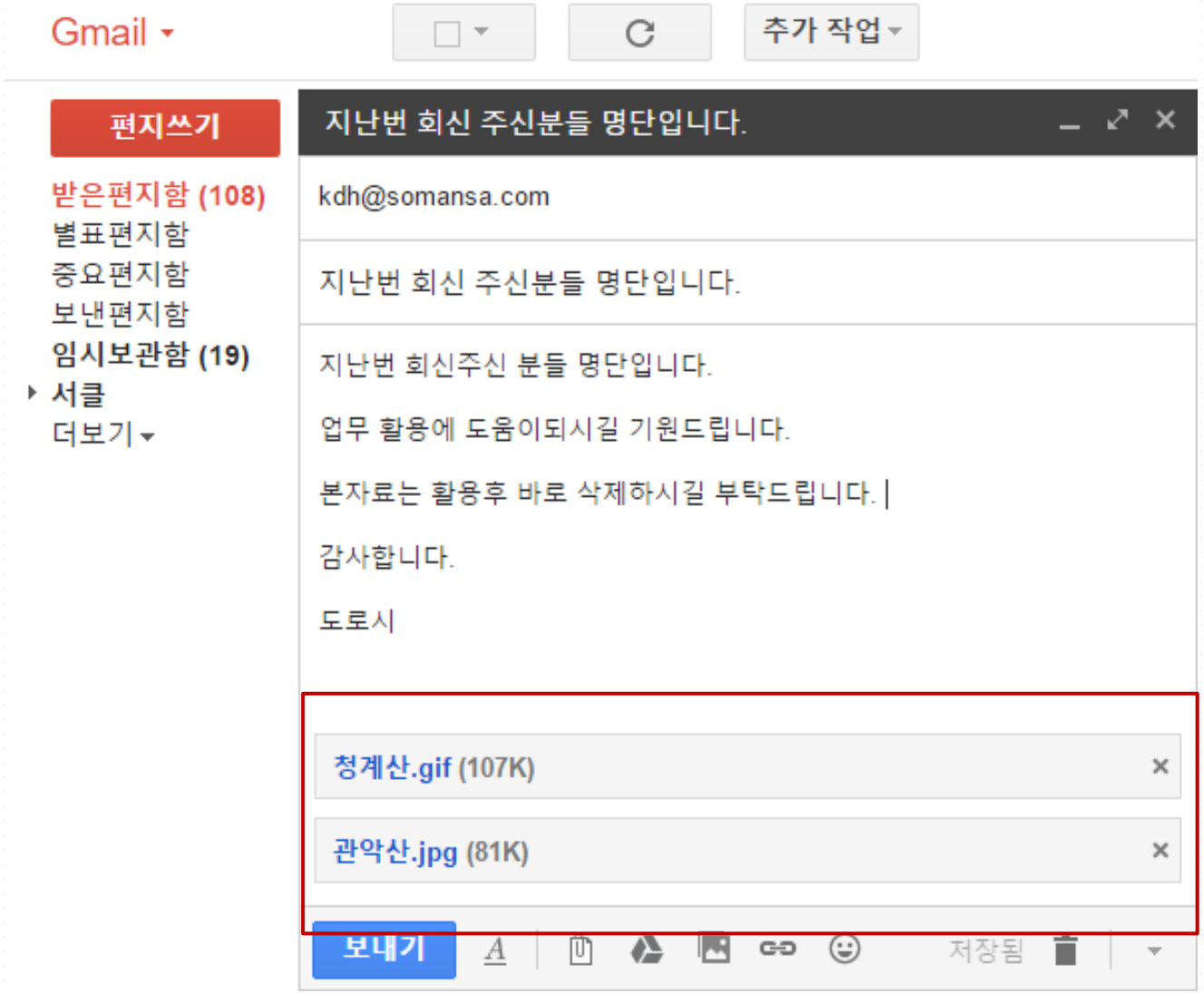
필립김 드림

패턴/파일/본문 정보

구분	패턴 개수	파일 크기(KB)	파일 전송 일시	파일 분석	개인 정보 분석	
본문	0					
개인정보(2007).xlsx	1,222	80	2016-10-27 11:38:59	파일 분석 성공	파일 분석 성공	
핸드폰 번호	19					
신용 카드 번호	300					
주민 등록 번호	300					
전화 번호	100					
IP 주소	100					
외국인 등록 번호	100					
계좌 번호	100					
E-Mail 주소	100					
운전 면허 번호	3					
여권 번호	100					
합계	1,222	80				

SOMANSA

사례 : G메일 개인정보 유출통제



SOMANSA

사례 : G메일

본문 내용

제목	지난번 회신 주신분들 명단입니다.
보낸 사람	10.10.7.104
받는 사람	"kdh@somansa.com" <kdh@somansa.com>
참조	
숨은 참조	

지난번 회신주신 분들 명단입니다.

업무 활용에 도움이되시길 기원드립니다.

본자료는 활용후 바로 삭제하시길 부탁드립니다.

감사합니다.

도로시

패턴/파일/본문 정보

구분	패턴 개수	파일 크기(KB)	파일 전송 일시	파일 분석	개인 정보 분석	
본문	0					
청계산.gif	-	106	2016-10-27 14:44:13	파일 분석 에러	파일 분석 전	
관악산.jpg	1,222	80	2016-10-27 14:44:13	파일 분석 성공	파일 분석 성공	
핸드폰 번호	19					
신용 카드 번호	300					
주민 등록 번호	300					
전화 번호	100					
IP 주소	100					
외국인 등록 번호	100					
계좌 번호	100					
E-Mail 주소	100					
운전 면허 번호	3					
여권 번호	100					
합계	1,222	187				

0091_청계산 (1).gif 0074_관악산 (1).jpg

SOMANSA

DLP일체형 장비 외산 대비 우위 : ICAP 연동 문제

외산 웹프락시는 DLP기능을 보유하고있지 않고, DLP서버와는 ICAP으로 연동
이때 큰 성능 부하가 발생하여, 실시간 성격을 가진 웹서비스의 속성상 현실적으로 운영 불가

항목	ICAP연동(Proxy+DLP 개별 운영방식)	프락시DLP 일체형
성능	ICAP의 부하가 30%이상	높음
장애분석	프락시와 DLP장비 분석해야하므로 복잡	한장비의 로그를 분석하면 되기에 단순
30M이상 대용량웹메일 개인정보 전송 사전 차단	ICAP의 부하때문에 대용량 첨부화일 분석시 네트워크 지연 발생때문에 처리 불가능 (10M이하 첨부화일만 허용)	대용량 첨부화일도 신속한 분석과 처리 가능
웹메일 재현 능력	웹메일 본문과 첨부화일이 별도의 POST로 전송될 경우에 DLP서버에서 두개의 POST를 하나의 웹메일로 재현이 불가능해질수있음.	웹메일 재현100%
서버 증설시 복잡도	프락시 서버와 DLP서버의 연관관계를 정리해서(N:N매칭) 증설 복잡	단순함

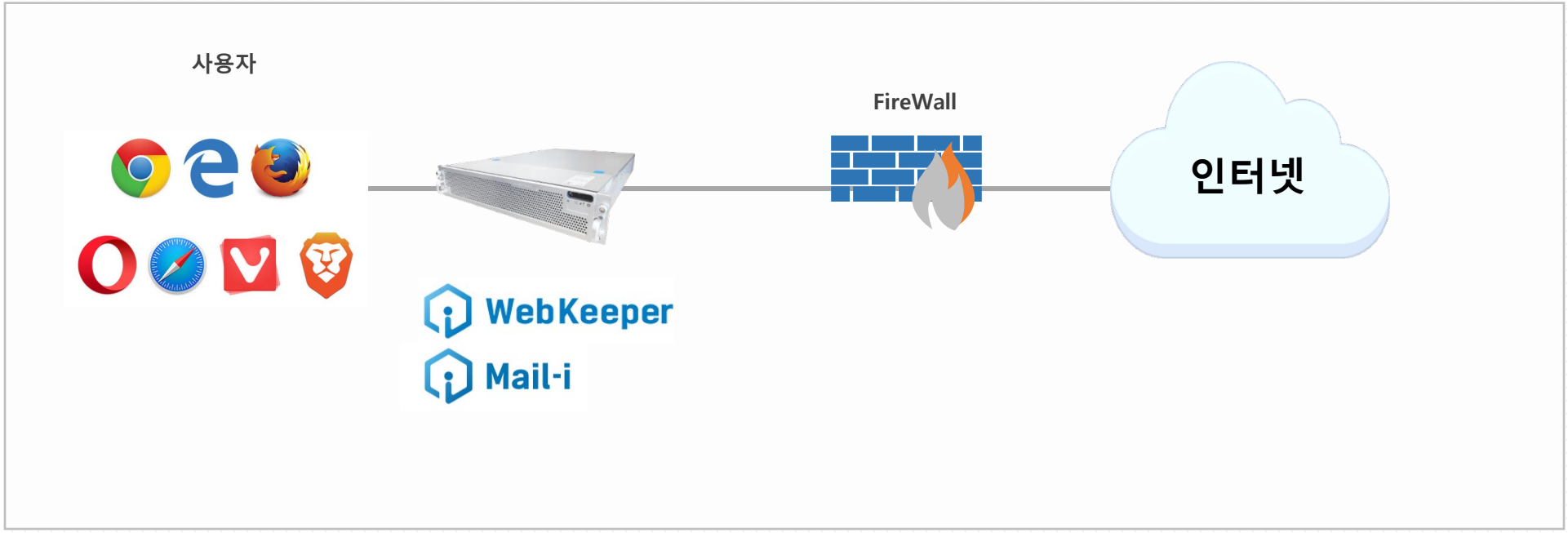
Ⅳ. 네트워크 구성

WSG+DLP

네트워크 구성 : 투명 프락시 (transparent proxy) 방식

명시적 프락시와 투명 프락시 모두 지원. 대부분 투명 프락시 방식

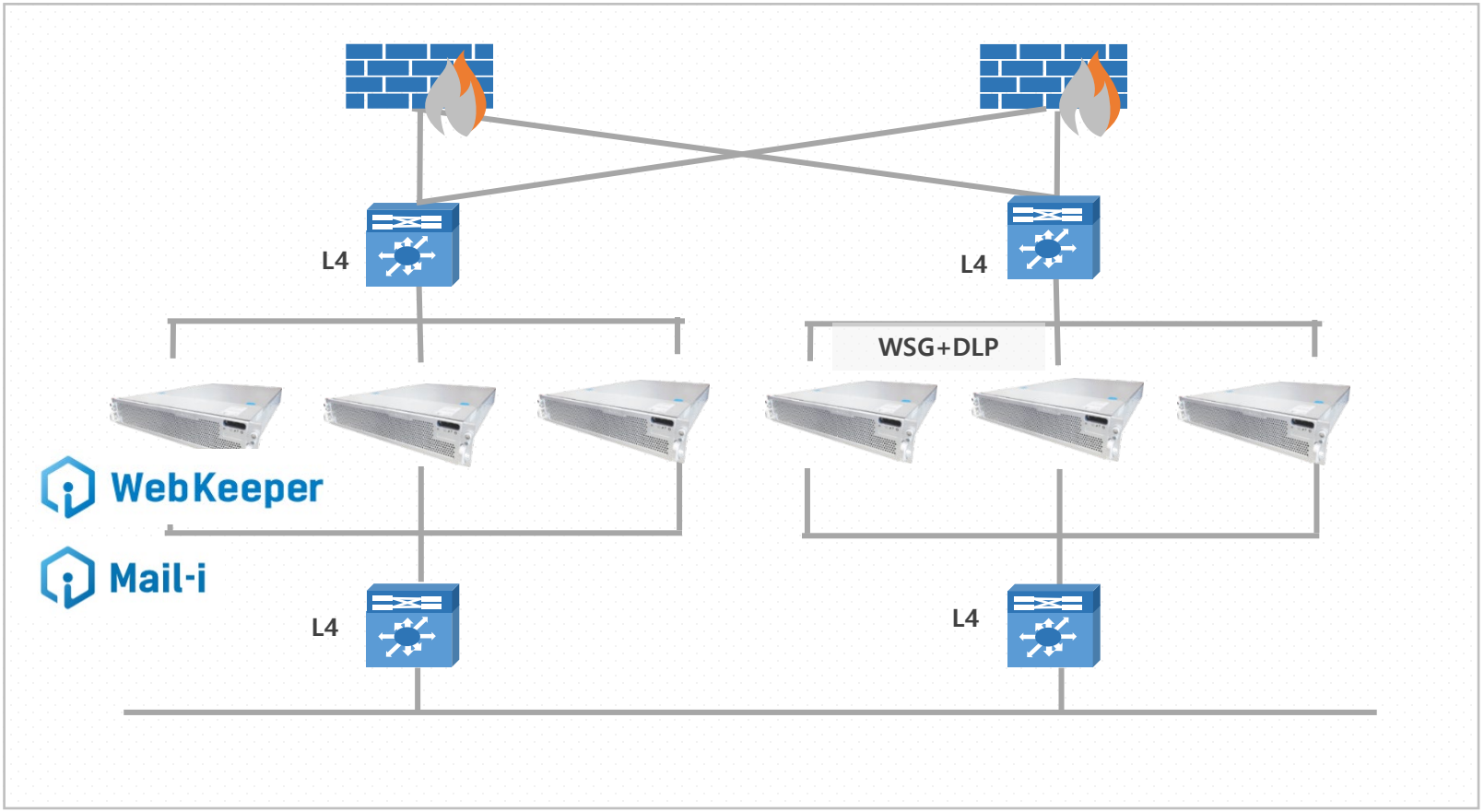
1G 라인 하나당 in-line형태의 WSG(유해사이트차단 + DLP) 구성, FOD 내장형



SOMANSA

네트워크 구성

L4를 활용하여 고가용성, 로드밸런싱 구성 사례 (1G, 10G)



SOMANSA

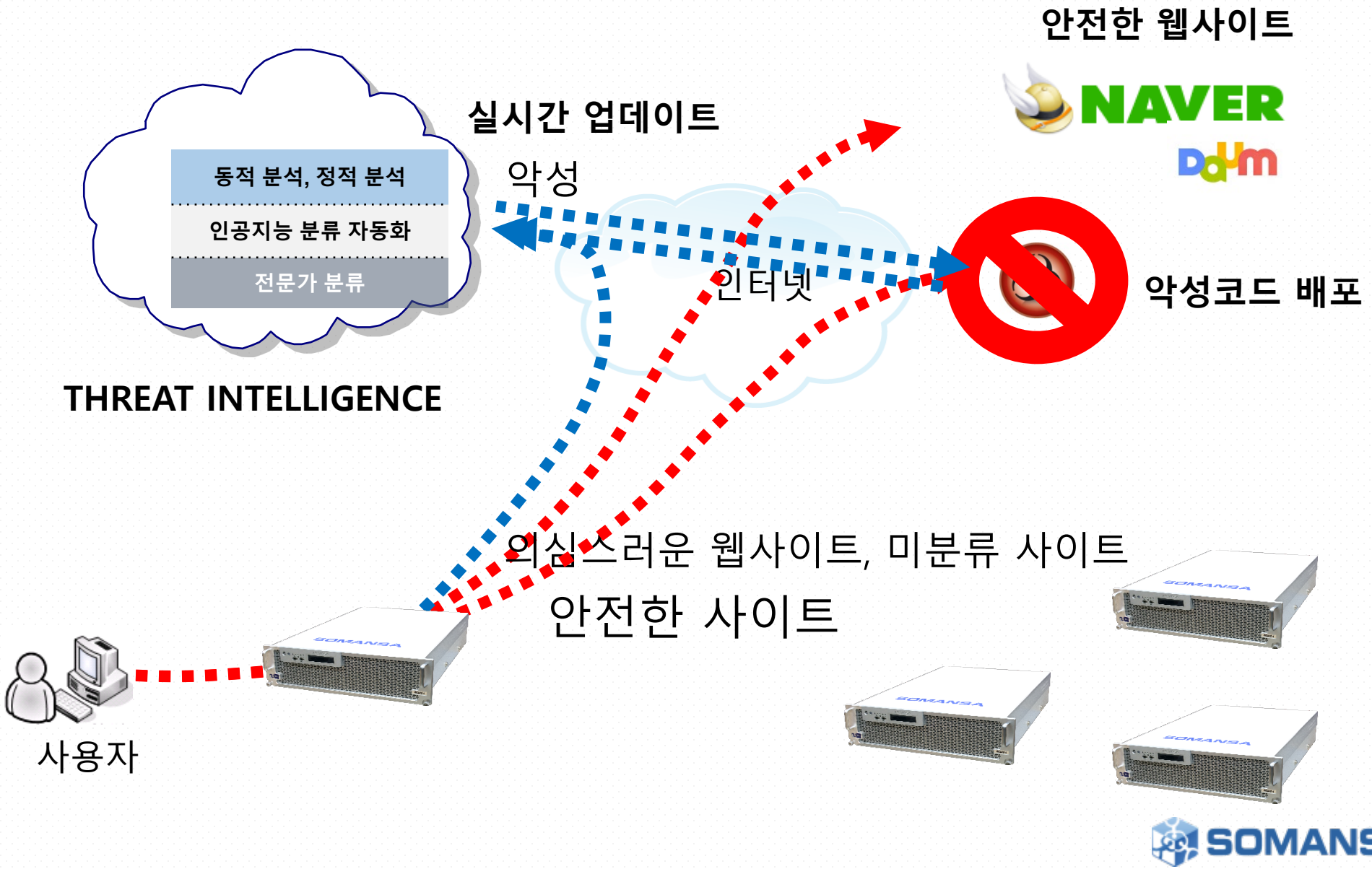
네트워크 구성 : 타솔루션 연동

HTTPS 가시성 제공
타 솔루션과 연동 (APT, IPS, NetForensics, DLP, 유해사이트 차단 etc)

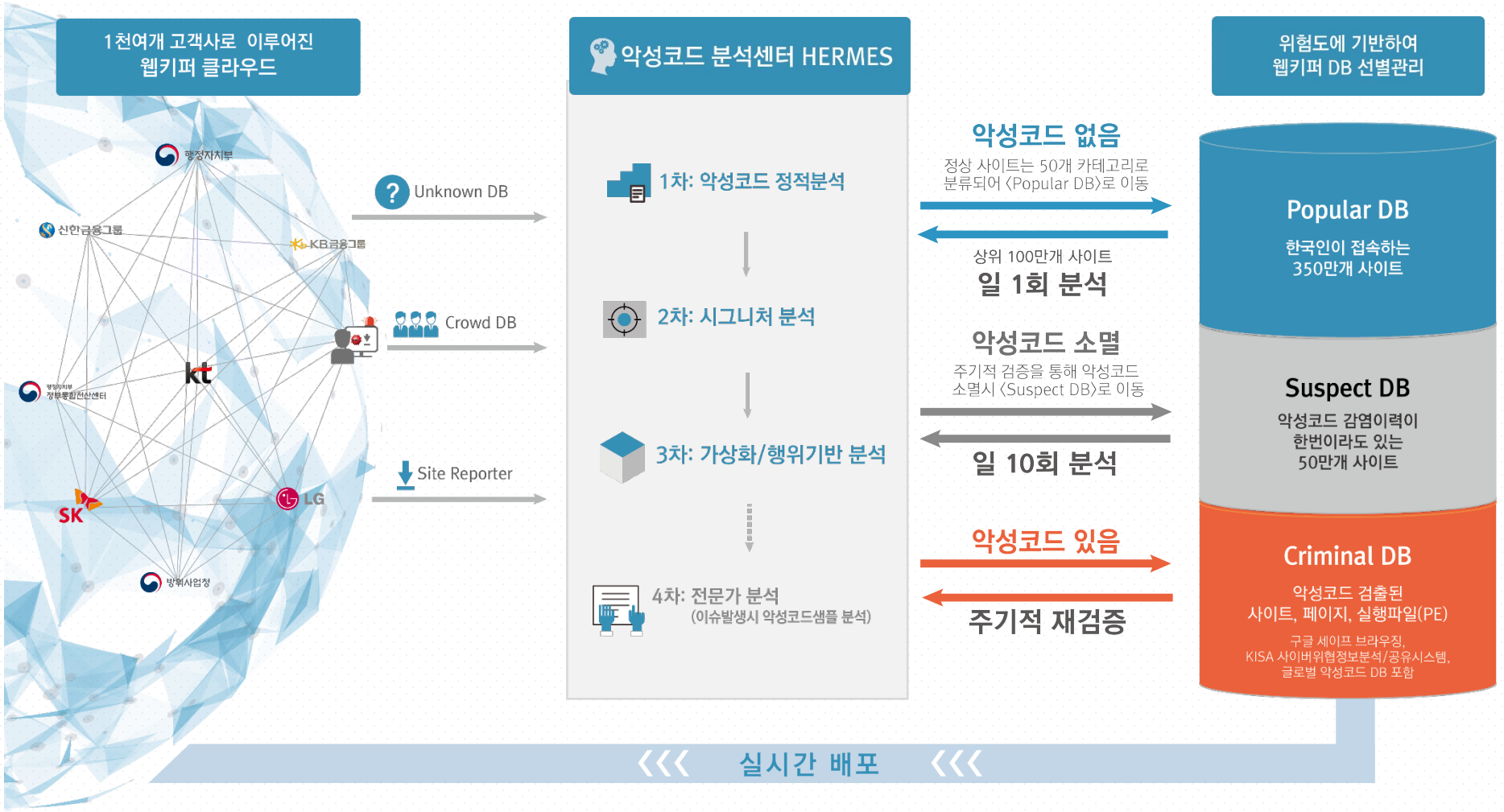
Ⅴ. 보안성 지속 서비스

유해사이트와 악성코드 배포사이트 DB 업데이트 체계

웹키퍼 클라우드를 통한 악성코드 수집 및 분석



악성코드 배포 사이트 분석 체계



SOMANSA

[11/17] 악성코드 데일리카톡
63,947(+) 85,322(-)

#세이프브라우징
www-verylife-co-kr, 생활정보사이트, 생활_가정
www-smrobotics-co-kr, TOPHORSE-탑홀스, 여행_레저
www-namgo-co-kr, 부산리조트, 이미지_광고서버
www-proavgood-co-kr, 성음사운드, 전자상거래_경매
www-monsterfx-co-kr, 몬스터코리아, 전자상거래_경매
www-reinassemall-co-kr, 라이네쎄 쇼핑몰, 전자상거래_경매
www-bronce-co-kr, 반도레포츠, 전자상거래_경매
www-yypc-co-kr, 영풍정밀, 컴퓨터_소프트웨어_서비스
www-itqa-co-kr, 국제기술품질인증원, 학교_학술_교육_연구기관

#악성코드공유서비스
wan-58-com-ejzql-cn
yz-msjy100-com

#악성코드검색엔진
static-109-145-130-94-clients-your-server-de
105-158-87-135

#고객신고
sevialeon-com/documents/document/invoice-html
ucplus-fr/have-php?
www-chothuemaitet-vn
myp0nysite-ru
www-bringscorp-ru

2017년 누적 (44주차)

지난 1주일 누적 (2017.10.30~11.03)

17,033,990 악성코드 배포사이트 — 259,239 (차단 133,522 / 차단해제 125,717)

수집출처	추가 사이트(예)
세이프 브라우징	www.aplusenglish.co.kr
	www.camhouse.co.kr
	www.hyodotour.co.kr
	www.hidisk.com
고객신고	find.bobbyj.tk/PHP/index.php?action
	sprecic.net/Recent-money-transfer-details
악성코드 검색엔진	45.216.238.47
	78.164.141.217.dynamic.ttnet.com.tr
악성코드 공유서비스	07111cgac8t.desksaw.world
	4q1b.miamz.com
웹키퍼클라우드	176.223.112.66/updatefile/primepc/1.6/PrimePC.exe
	176.223.112.108/Download/DtsMainProc.exe

2,023 암호화웹 (HTTPS)사이트 — 48

카테고리	추가 사이트(예)		비고
〈음란물〉	chunjaa 외 19개	https://www.chunjaa.net/	신규
	johnnybet	https://www.johnnybet.com/	신규

SOMANSA

외산제품 대비 DB 품질

외산 유해사이트 차단 솔루션은
국내 대표적인 음란사이트, P2P(토렌트), 도박사이트
검색엔진 상위 100대 사이트중 30%를 미분류하는것으로 분석

항목	외산제품	WebKeeper
평판 사이트(랭키, 알렉사 외)처리율	랭키 상위 10% 미분류	높음
검색엔진 상위 사이트 처리율	도박사이트 30% 미분류 한글 키워드 검색 음란사이트 40% 미분류	높음
구글 세이프 브라우징 DB	업데이트 주기가 늦음. 참조하지 않는것으로 보임	처리
국내 악성코드 DB업데이트속도	한국 솔루션보다 업데이트가 늦을 때가 있음	빠른 처리
글로벌 악성코드 DB업데이트	빠름	글로벌 악성코드 DB 라이선스 받아 대응

VI. 법인 소개

SOMANSA

소만사 (SOMANSA)

Global Leader in Data Security

인원	210분	기술인력 120
업력	**22년**	**1997년 창업**
매출	300억	2018
신용등급	**A0**	**무차입 경영**
고객사	Secure GateWay 핵심 100곳	1000개 고객사 600 유지관리 고객
수상/인증	Gartner	**아시아 유일** **DLP분야 가트너 등재**

And Web Security

SOMANSA

글로벌 개인정보보호/DLP 리더 소만사

Gartner

- IT 리서치 최고 권위
- Enterprise(통합) DLP 부분 Magic Quadrant 2년연속 등재
- 아시아 유일, 세계 Top 10 제품(전세계 100+개 제품 중)

FORRESTER

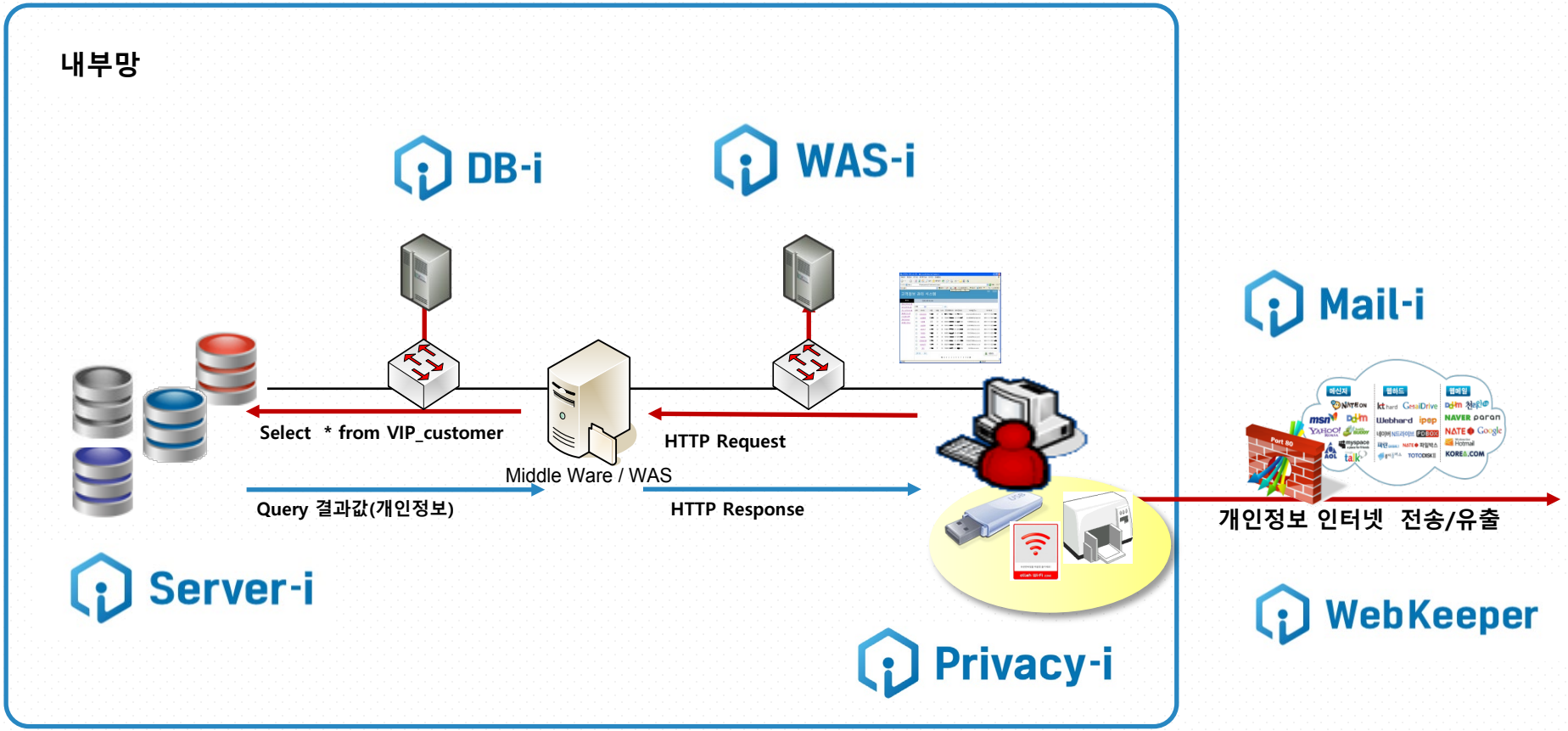
- DLP 부분 Vender Landscape 등재
- 아시아 유일

SC MAGAZINE FOR IT SECURITY PROFESSIONALS

- 보안분야 최고 잡지
- Endpoint DLP 부분 제품 평가 ★★★★½

SOMANSA

You Can't Protect your data
When you don't know where it is



참고 : 망분리, DB암호화, 바이러스/APT, 인증인프라 외 도입 또한 필요

Secure Gateway 도입 국내 핵심 고객사

우리은행 KB

HYUNDAI HEAVY INDUSTRIES CO.,LTD. Hyundai Card 삼성카드 SAMSUNG

LG Chem SK innovation HYUNDAI MOBIS kt

산업통상자원부 보건복지부 문화체육관광부

NPS 국민연금 National Pension Service

You Can’t Protect What You Can’t See

And No time to Lose

Thank you