

PNP4WEB

“ Perfect and Protected – for Web ”

웹 위.변조 방지 솔루션



C contents



1. PNP4WEB 제품 개요
 2. PNP4WEB 제품 구성
 3. PNP4WEB 특징 및 장점
 4. PNP4WEB 주요기능
 5. PNP4WEB 성능 및 안정성
 6. PNP4WEB 주요 구축사례
- 별첨. 회사소개



1. PNP4WEB 제품 개요 - 제안배경

금융기관 전자금융업무 컴플라이언스 보안요건 준수 필요

전자금융감독규정

제6절 전자금융업무

□ 제34조(전자금융거래 시 준수사항) 금융회사 또는 전자금융업자는 전자금융거래와 관련하여 다음 각 호의 사항을 준수하여야 한다.

1. 전화 등 거래수단 성격상 암호화가 불가능한 경우를 제외한 전자금융거래는 암호화 통신을 할 것(다만, 전용선을 사용하는 경우로서 제36조의 규정에 따라 자체 보안성심을 실시한 경우에는 그러하지 아니하다)
2. 전자금융사고를 예방하기 위하여 비대면 전자금융거래를 허용하지 않는 계좌 개설, 중요 거래정보에 대한 문자메시지 및 이메일(e-mail) 통지 등의 서비스를 이용자가 요청하는 경우, 동 서비스를 제공할 수 있도록 시스템을 갖출 것
3. 전자금융거래에 사용되는 접근매체를 발급받기 위해서는 반드시 실명확인 후 교부할 것.
4. 거래인증수단 채택시 안전성, 보안성, 이용편의성 등을 충분히 고려할 것
5. 금융회사 또는 전자금융업자는 전자금융거래에서 이용자에게 제공하거나 거래를 처리하기 위한 전자금융거래프로그램(거래전문포함)의 위·변조 여부 등 무결성을 검증할 수 있는 방법을 제공할 것

② 삭제

[전문개정 2016. 6. 30.]



제34조 5항

금융회사 또는 전자금융업자는 전자금융거래에서 이용자에게 제공하거나 거래를 처리하기 위한 전자금융거래프로그램(거래전문포함)의 위·변조 여부 등 무결성을 검증할 수 있는 방법을 제공할 것

금융보안적합성 시험대상 추가



금융보안연구원, 금융보안적합성 시험 대상에 '웹 위변조 대응기능' 추가

▲ 올한겨레 기자 | ⓒ 일력 2014.08.29 10:09 | 댓글 0

[아이티데일리] 금융보안연구원은 금융보안적합성 시험 서비스에 '웹 위변조 대응기능'을 신규 시험 대상으로 추가하고, 이달 말부터 해당 서비스를 회원사에 제공한다.

금융보안연구원은 올해 초 전자금융 보안위협에 대한 다각도의 분석을 원인으로 웹 위변조 공격을 주목하고 이에 대한 대응기능을 신규 시험 대상 프로그램으로 발생하는 웹페이지 위변조 위협을 체계적으로 정리하여 시험환경 구축 등 시험 준비를 최근 완료했다.



웹 위변조 대응 기능에 대한 금융보안적합성 시험은 웹페이지 접근 차단 및 변조 탐지 기능을 주된 대상으로 수행되며, 해당 서비스를 통해 금융회사는 웹 위변조 관련 보안취약점을 사전에 파악하고 전자금융 운영환경에서 발생 가능한 위협을 감소시킬 수 있을 것으로 기대된다.

인터넷진흥원 기술 권고사항

“인터넷 이용환경 개선을 위한 기술 안내서” 가이드라인

3.1 로그인 채널보호

나. Application Level Encryption 구성 웹 표준 환경에서 자바스크립트를 이용하여 Application Level의 Encryption을 구현하여 사용하는 것을 권장하고 있으며 Application Level Encryption의 가능한 구성은 다음과 같다.

공개키 암호 알고리즘 이용서버에서 공개키와 개인키 패어를 생성한 후 공개키를 클라이언트로 응답하고 클라이언트에서 데이터를 공개키로 암호화하여 서버로 전송한다. 서버에서 개인키로 복호화하여 로그인 데이터를 확인한다. ~ 대칭키 암호

알고리즘 이용서버와 클라이언트 간 동일한 키를 공유한 경우 클라이언트에서 데이터를 대칭키 암호화하여 서버 전송하고 서버에서 동일한 대칭키로 복호화하여

데이터를 확인한다.

Application Level Encryption 보안성 보장 조건

- 강력한 보안구성을 SSL/TLS Transport Layer 상에서 운용한다.

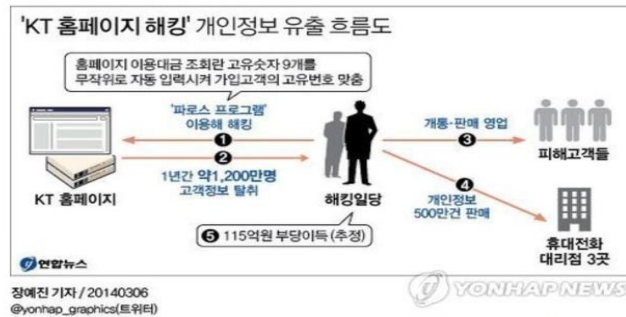
- Encryption/Decryption을 수행하는 자바스크립트에 대한 보호 대책을 적용한다.

1. PNP4WEB 제품 개요 - 제안배경

침해 사고 사례

취약점을 통한 정보유출

<실제 사례>



<사진출처: Google 나무위키 사전백과>

취약점을 통한 정보유출

이데일리

2021년 01월 29일 금요일
세상을 올바르게 세상을 바꾸기

三 Q IT·과학 모바일 방송통신 IT·인터넷 게임 과학일반

아이핀 무너뜨린 해킹, KT 해킹 때와 유사..시스템 '취약' 노출

'파라미터 위·변조', 전송정보 중간서 가로채 바꿔..1년전 K...

"정보 암호화·검증절차 등 미비" 지적..시스템 개편 목소리...

등록 2015-03-09 오전 12:01:17
수정 2015-03-09 오전 12:01:17

가 가

2월 28일부터 이달 2일까지 행정자치부가 관리하는 공공 아이핀(i-PIN) 시스템에서 75만 건의 아이핀이 부정 발급된 해킹 사고는 1년 전 [KT\(030200\)](#) 가입자 1200만명의 개인정보가 유출된 사고와 동일한 수법인 것으로 나타났다.

이는 내부 시스템의 전송 데이터들에 대한 암호화와 검증절차 등 보완대책이 미비해 발생한 것으로 분석된다.

지난해 유사한 보안사고를 겪고도 당국이 아이핀 시스템의 내부 보안조치에 허של했던 게 아니냐는 지적이 나온다.

8일 보안업계 등에 따르면, 이번 아이핀 해킹사고 수법인 '파라미터(매개변수 값) 위·변조'는 프록시 툴(proxy tool)을 이용해 클라이언트와 웹 서버를 오가는 각종 정보들을 중간에서 가로채 다른 정보로 바꾸는 기법이다. 이 수법은 해커가 내부 시스템의 취약점을 악용한 것으로, 악성코드 감염은 아니어서 백신 프로그램으로 치료할 수는 없다.

보안뉴스

전체기사

SECURITY

IT

SAFETY

Security World

#KT 해킹 #파로스 #파라미터 값 변조 #고객정보 유출

파로스 프록시 프로그램 이용해 파라미터 값 변조

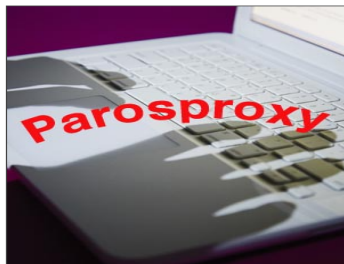
[보안뉴스 김태형] 6일 경찰 수사 발표로 밝혀진 KT 해킹 사건은 해커가 파로스라는 프로그램을 이용해 KT 홈페이지의 허점을 노린 것으로 파악되고 있다.

이번 KT 홈페이지 해킹에 사용된 해킹을 '파로스 프록시(Parosproxy)'는 인터넷 검색으로도 쉽게 찾을 수 있고 제작사 홈페이지에 접속해서 누구나 내려받을 수 있으며 자세한 사용방법은 쉽게 구할 수 있어 초보자나 중학생 정도면 사용할 수 있다.

이 프로그램은 원래 웹사이트의 취약점을 점검하고 분석하기 위해 만들어졌지만, 이를 역으로 이용하면 웹 해킹 도구로도 사용이 가능하다는 것.

이 파로스 프로그램은 클라이언트와 웹 서버 사이에 자리 잡고 있다가 오가는 각종 정보를 중간에서 가로채 볼 수 있는 기능을 갖고 있다. 이를 바탕으로 홈페이지 자체의 보안 홀이나 버그를 노리고 인터넷으로 나가는 패킷을 중간에서 가로채서 저장하고 있다가 변조하는 것이다.

이에 대해 보안전문기업 KTB솔루션 김태봉 대표는 "파로스는 프로그래밍은 웹상 서버와 웹브라우저에 접속할 때 파라미터 값을 조작해서 넣을 수 있다. 해커는 처음부터 KT 고객 1200만건의 정보를 빼낼 수는 없었을 것이다. 우선 해커는 자기 계정으로 KT 홈페이지에 로그인 했을 것"이라고 말했다.



1. PNP4WEB 제품 개요 - 제안배경

침해 사고 사례

이체금액 조작

발체 : 국내 인터넷뱅킹 계좌이체에 대한 MITB 취약점 분석
'P112' (제1권2호)

>2) 이체금액 조작 사례

가짜 계좌이체 화면을 겹치는데 성공한 악성프로그램은 이체금액폼에 이체가 가능 전액을 입력한 다. 이 과정은 이체가 가능 전액을 자동으로 입력해 주는 '전액' 버튼을 악용할 수 있다. '전액' 버튼은 팝업창을 통해 사용자에게 전액이체 여부를 확인한 이후에 금액이 입력되도록 되어있다. 하지만 이 동작은 스크립트 수준에서 구현된 것이기 때문에 함수 오버라이딩을 통해 사용자 확인과정 없이 전액이 입력되도록 이용할 수 있다.

<표 4> 이체가 가능 전액을 자동으로 입력하는 자바스크립트

```
var index =  
top.body.frm.WDRACTNO_15.selectedIndex;  
with (top.body.document) {  
    moneyFrmSum.ACTNO_15.value =  
        frm.WDRACTNO_15[index].value;  
    moneyFrmSum.action =  
        "/pib/bank/fndt/wpdep011_28i.jsp";  
    moneyFrmSum.target = "RECV_NAME";  
    top.body.XecureSubmit(moneyFrmSum);  
}
```

결제대금 조작

보안뉴스

전체기사

SECURITY

IT

SAFETY

Security World

Home > 전체기사

쇼핑몰 결제대금 어떻게 조작했나? 프록시 툴 악용한 해킹

좋아요 133개 | 입력: 2016-05-11 19:15

프록시 툴 사용해 파라미터 값 변조하면 결제금액 조작 가능

실제 상품가격과 결제 가격 비교하는 시스템으로 해킹 방지해야

2014년 KT 홈페이지 해킹사고 및 2015년 공공 아이핀 부정발급 사례와 유사

[보안뉴스 김태형] 최근 인터넷 쇼핑몰에서 5천만원 상당의 카메라와 렌즈 등을 구입한 후, 해킹프로그램을 이용해 결제금액을 1만 원대로 조작해 부당이익을 취한 20대 남성이 구속됐다.

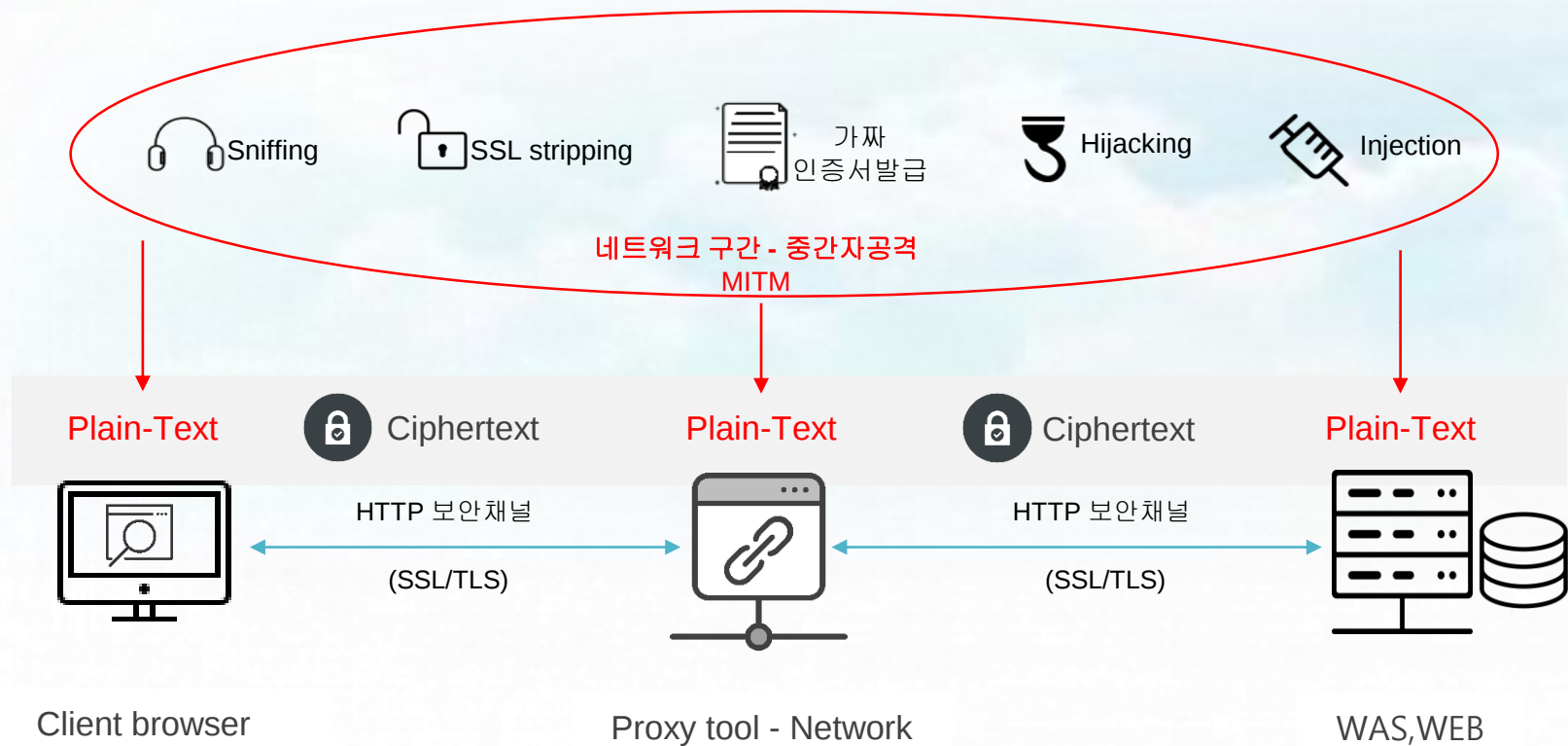
전체 물건값은 5천577만원이었지만, 이씨는 자신이 만든 해킹프로그램을 이용해 1만779원만 결제하고 물건을 챙겼다.

조사 결과, 이씨는 인터넷 쇼핑몰에서 물건값을 결제할 때 결제대행사 서버로 전송되는 인증값을 미리 알아내 상품가격 정보를 임의로 조작하는 방법으로 사기 행각을 벌인 것으로 드러났다.

이렇게하면 885만원짜리 디지털 카메라를 구매한 뒤 전산 처리되는 가격정보를 '8850000'에서 '885'로 조작하는 수법을 썼다. 실제 가격의 1천~1만 분의 1에 해당하는 돈만 내고 고가의 물건을 가로챈 것이다.

1. PNP4WEB 제품 개요 - 제안배경

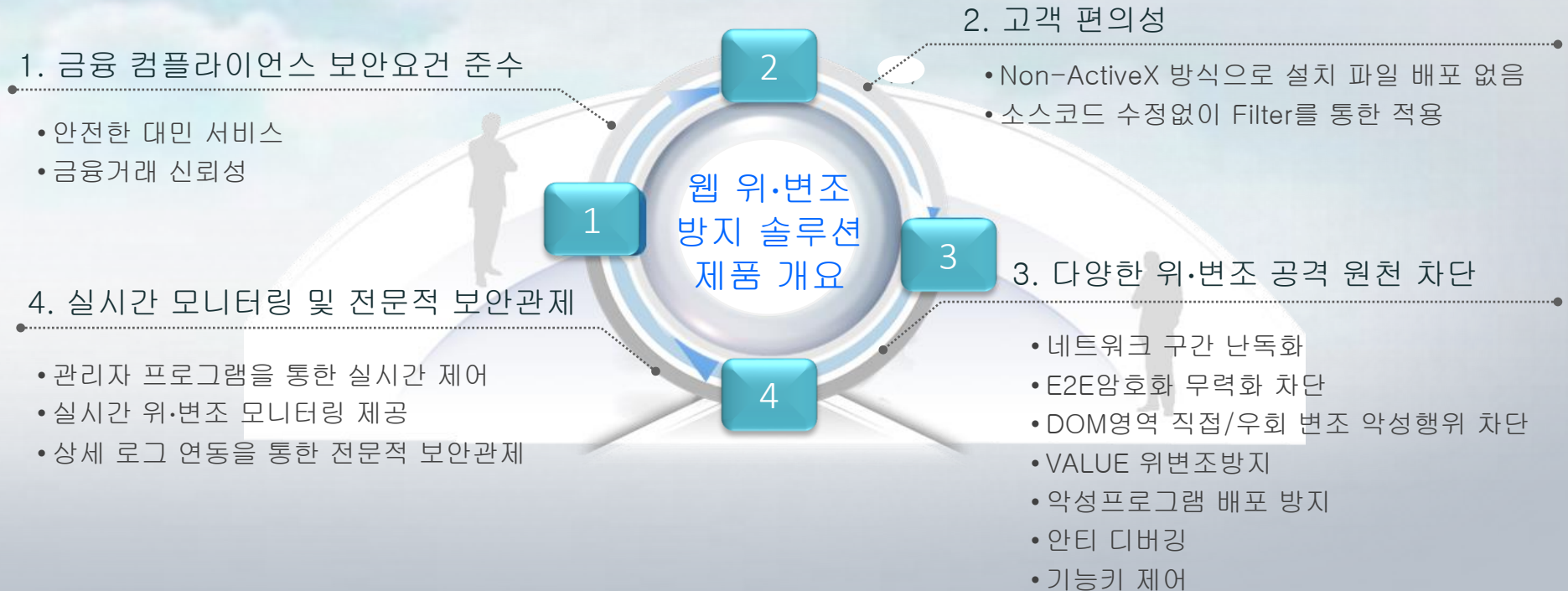
보안취약점을 통한 중간자 공격



네트워크 구간 데이터 무결성 보증 및 공격에 대한 대응방안 필요

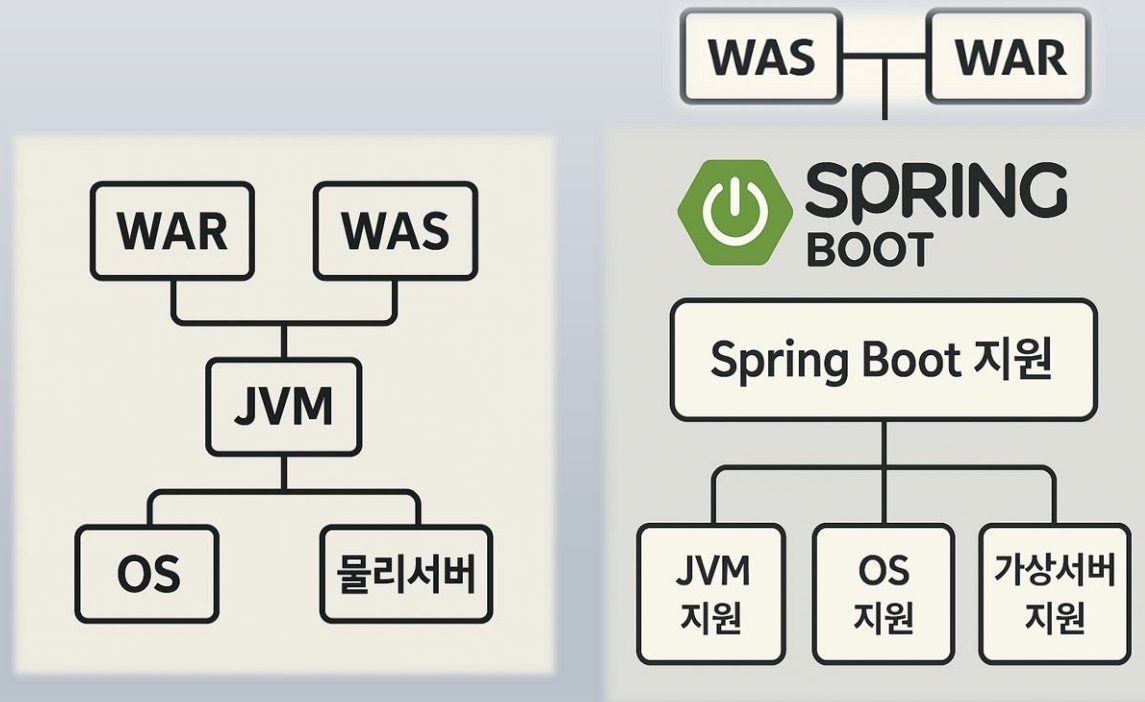
1. PNP4WEB 제품 개요 - 제품소개

웹 표준 준수 및 소스코드 수정 없는 None-Plugin 체계적용



1. PNP4WEB 제품 개요 - 제품소개

PNP4WEB 설치 구조



지원 구조

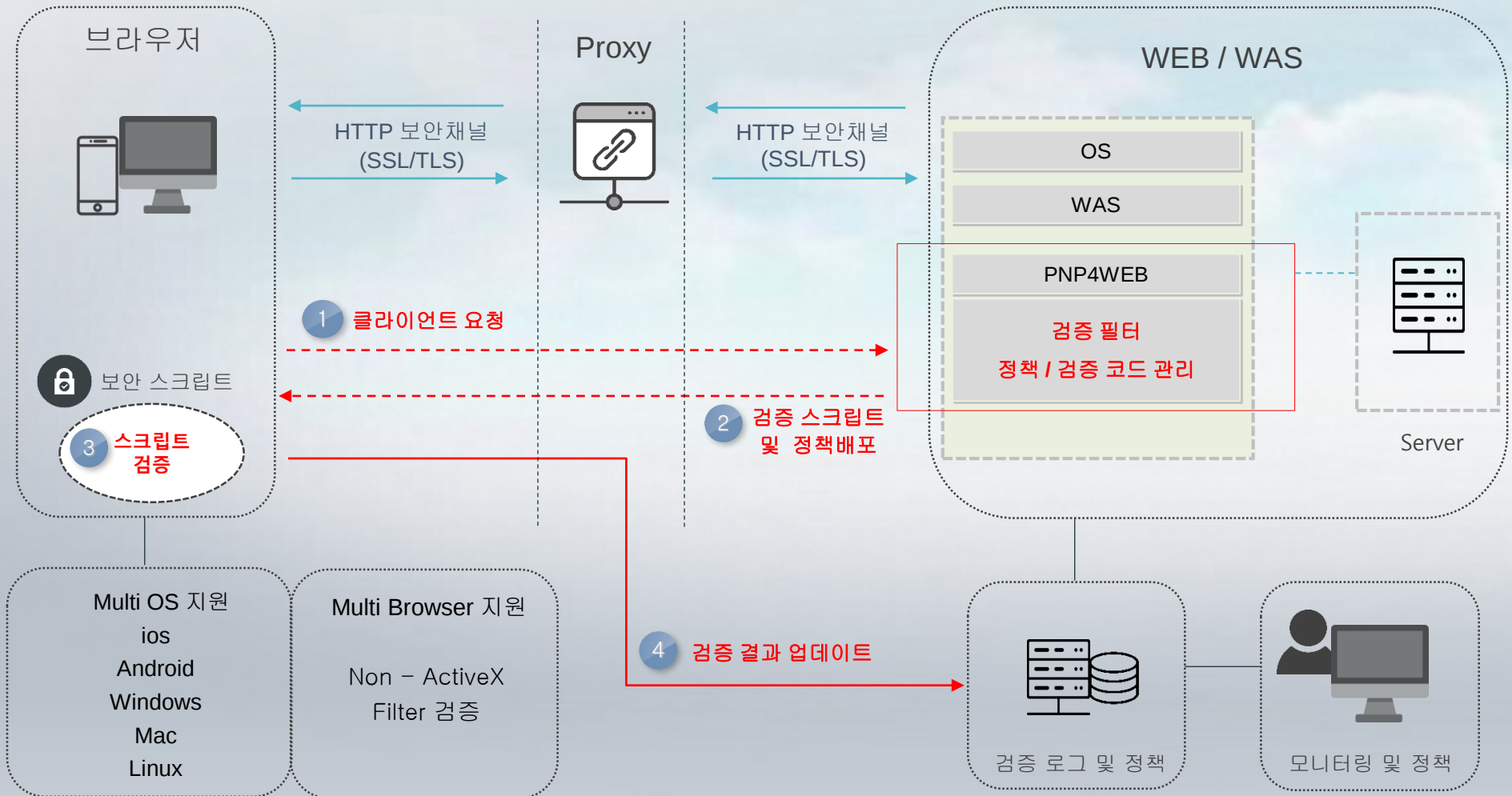
1. PNP4WEB 제품 개요 - 제품소개

PNP4WEB 3.0의 주요 기능표

PNP4WEB 3.0
웹.위변조 차단 지원 난독화 기반 기술 적용 (네트워크 구간 취약점 대응) - HTML 소스코드 , Ajax Request & Response - 웹 크롤링 방지
최신 프레임워크 지원 - vue, react 등 SPA 프레임워크 지원 - JAR + Spring Boot 지원 - 보안 적용 범위 확대
기존 설치환경을 유지하고 업그레이드 가능한 유연성 제공
- 개발자 도구 디버깅 방지 최신 개발자 도구 대응 - 크로미엄 엔진 지원 - 키보드, 마우스 제어
클라우드 환경 대응지원 - 컨테이너 기반 서비스 지원 - 고객사 환경 Auto Scaling 대응 - DevOps, 클라우드 환경 대응지원

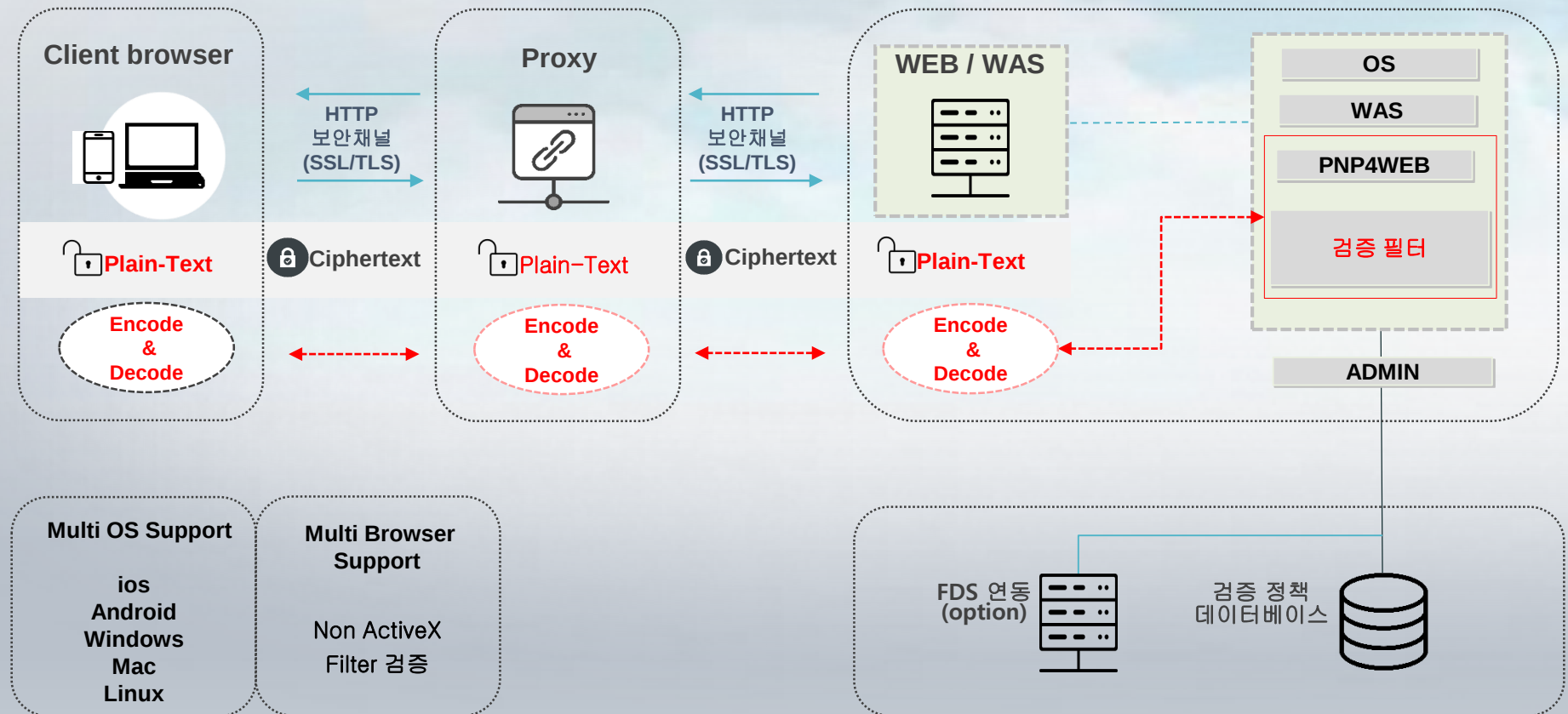
2. PNP4WEB 제품 구성 - 웹 위.변조방지

실시간 검증을 통한 강력한 보안환경 구성



2. PNP4WEB 제품 구성 - 네트워크 구간 난독화

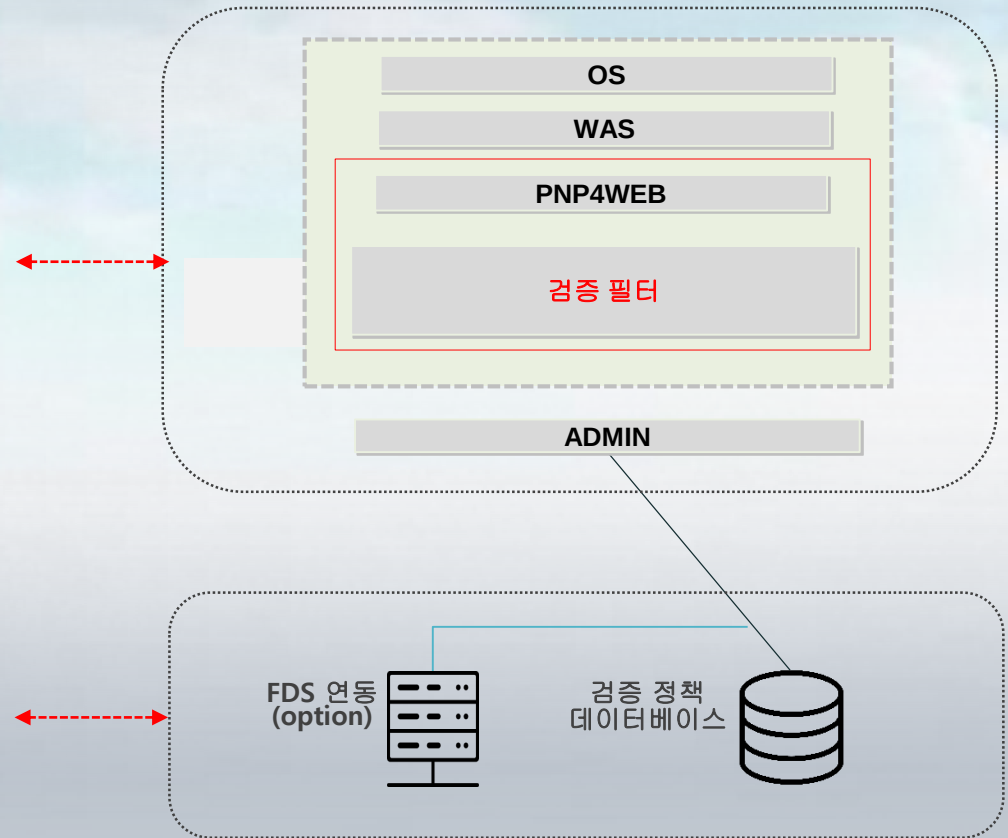
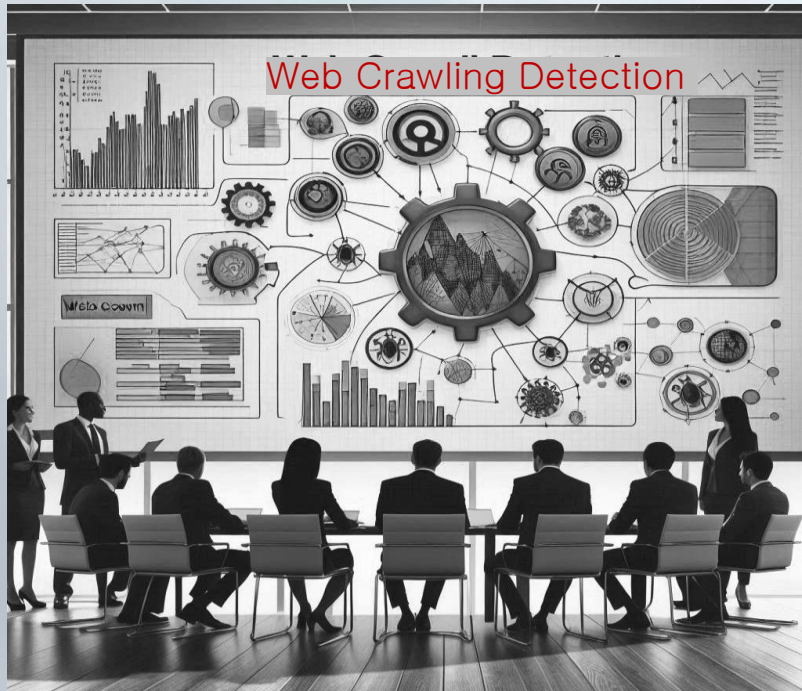
강력한 네트워크 구간 취약점 보완 - 구간 난독화



2. PNP4WEB 제품 구성 - 크롤링 방지

난독화를 통한 크롤링 방지

1. 난독화를 통한 웹 크롤링 방지
2. HTML 크롤링 원천차단
3. 대시보드를 통한 모니터링



2. PNP4WEB 제품 구성 - 지원환경

다양한 운영시스템 지원 및 Multi-OS / Multi-Browser 환경제공

WAS 서버	Filter 지원 WAS	• Unix, Linux, Windows • Servlet 2.3 이상 지원 WAS • JDK 1.5 이상
--------	---------------	---

웹 기반 환경	웹 기반 자바 환경 지원	JAVA, Java Servlet, JSP
---------	---------------	-------------------------

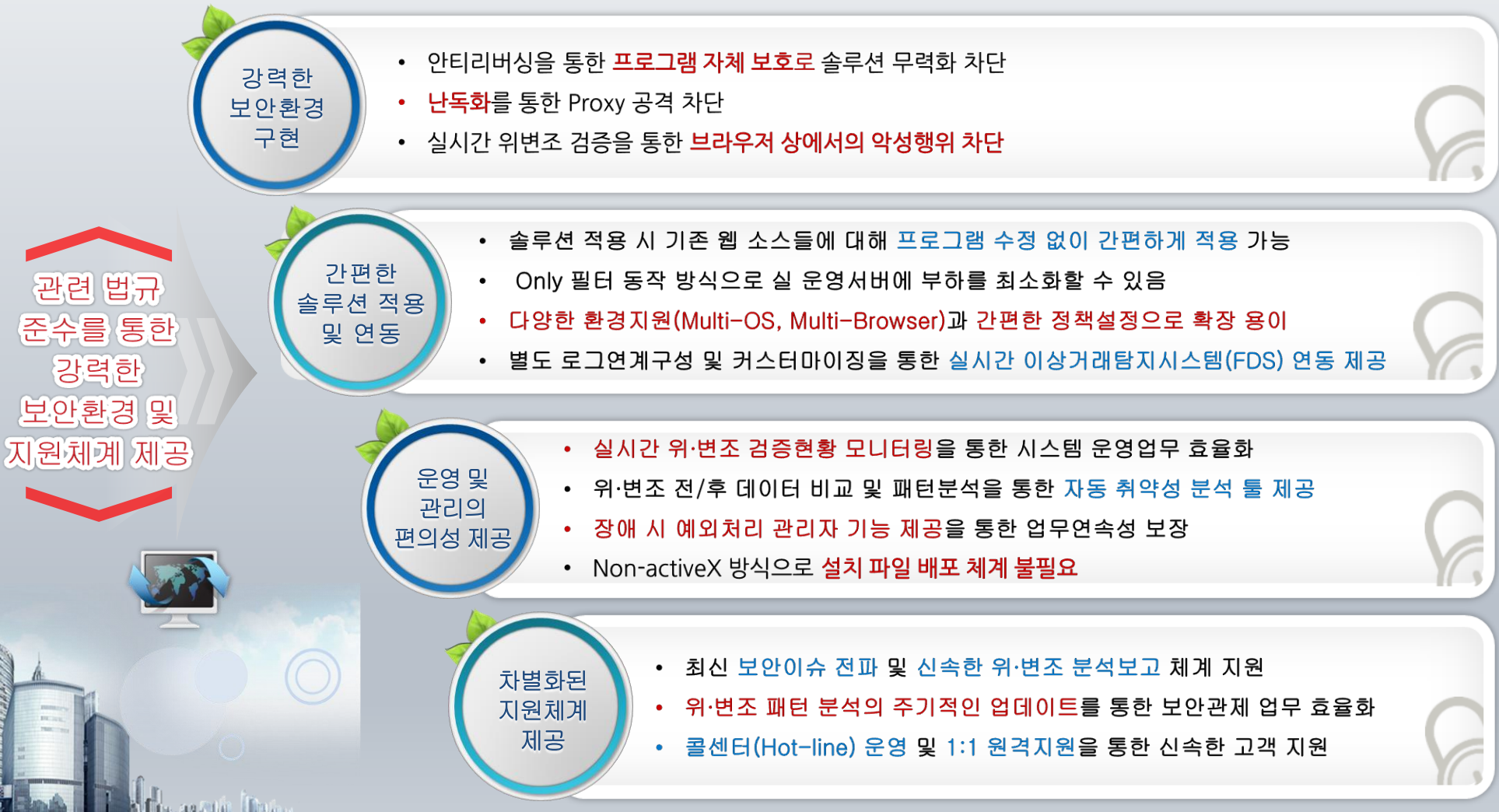
관리자 화면	DBMS	Oracle, MS-SQL, DB2, Sybase Informix 등
	관리자용 UI	웹 표준 지원 브라우저

클라이언트 지원 환경	
<u>웹 위변조 방지 적용 시</u>	<u>난독화 적용시</u>
IE 7.0 이상(32bit/64bit)	IE 11 이상
Firefox 3.6 이상	Firefox 78 이상
Opera 11.0 이상	Opera 50 이상
Safari 4.0 이상	Safari 11 이상
Google Chrome 10.0 이상	Chrome 72 이상

클라이언트 검증 Script	• Multi OS 지원
	Windows : XP ~ 10
	Mac : OSX, Yosemite 등
	Linux : Ubuntu, Fedora 등
	• Multi Browser 지원
	IE, Chrome , Firefox, Opera, Safari, Swing 브라우저 등
	• 가상화 환경 지원 : VDI,CBC 등
	• 모바일 웹 브라우저 지원 : iOS, Android 등

3. PNP4WEB 특징 및 장점

관련 법규 준수 및 강력한 보안환경 구성으로 안전한 전자금융서비스 보장



4. PNP4WEB 주요기능 1/2

주요 텍스트 위·변조 방지

- 웹 페이지 내 주요 텍스트 위·변조 시 탐지 및 차단
- 검증이력 및 위·변조 상세로그 제공

악성코드 배포 차단

- 비인가 Object 실행을 통한 악성코드 탐지 및 차단
- 비인가 ActiveX, Plug-In의 로딩을 사전에 차단

BHO, 툴바 접근의 위·변조 차단

- 외부 BHO 및 툴바를 통한 비인가 스크립트 차단
- Script 및 Object 변조를 통한 비정상적인 실행 방지

E2E 함수 무력화 및 우회접근 방지

- JS 및 Object Tag, Attribute 등 관련 스크립트 파일 보호
- 실행 함수(input tag enc=off) 무력화 시도 시 차단

이미지 위·변조 방지

- DOM 영역 이미지 파일 및 속성(alt, src 등) 보호
- 검증이력 및 위·변조 상세로그 제공

주소 창 Javascript Abusing 차단

- JavaScript Abusing을 통한 주요 함수 무력화 차단
- 검증이력 및 위·변조 상세로그 제공

Over-Layer 공격 차단

- 주요 입력 필드의 Over-lapping 공격 시 원천 차단
- 주요 입력 필드의 Over-Layer 공격 시 원천 차단

Link 변조 피싱사이트 유도 방지

- 비인가 스크립트 실행을 통한 피싱사이트 차단
- URL로의 Link 변조 및 비정상적인 실행 사전 차단

4. PNP4WEB 주요기능 2/2

입력필드 속성 및 HTML 보호

- DOM 영역 이미지 파일 및 속성(alt, src 등) 보호

안티 디버깅

- 브라우저 별 맞춤전략으로 개발자도구 디버깅 방지
- 검증 이력 및 위·변조 상세로그 제공

Javascript 전역함수 보호

- Javascript 전역함수 위·변조 시 탐지 및 차단
- 무력화 방지 및 비정상 실행을 사전에 차단



Script 및 Object Tag 보호

- Script Tag 및 Object Tag 위·변조 시 탐지 및 차단
- 스크립트 value 및 attribute 변조 시 탐지 및 차단



사용자 입력 제한

- 키보드 이벤트 인터셉트를 통해 기능키 제어
- 마우스 이벤트 인터셉트를 통해 마우스 우클릭 제어



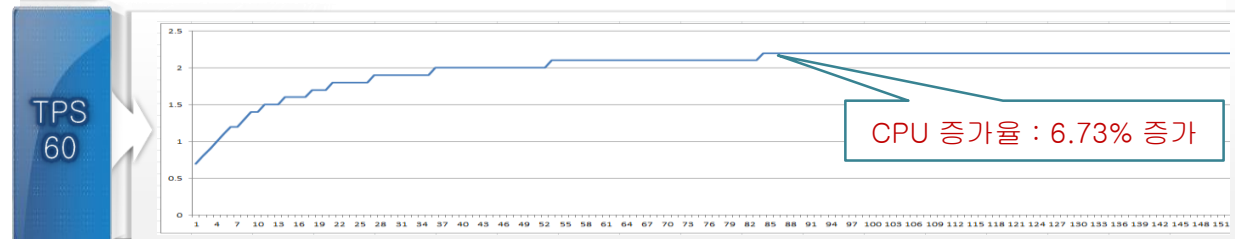
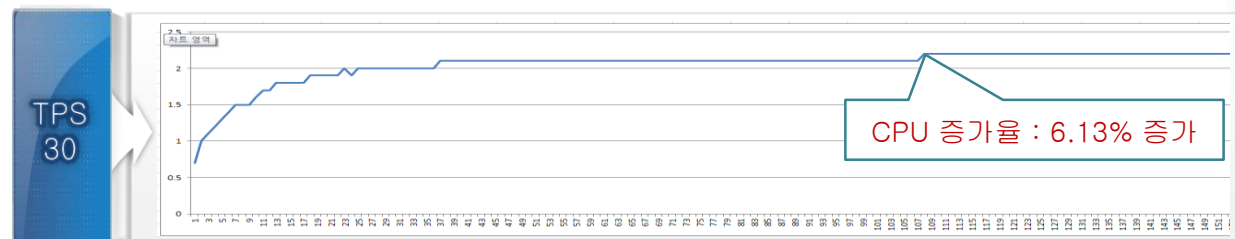
네트워크 구간 난독화

- url 패턴 등록을 통한 난독화
- Ajax Request 난독화 지원
- Ajax Response 난독화 지원
- HTML 소스코드 지원

5. PNP4WEB 성능 및 안전성 - 시스템 성능

솔루션 동작 시 시스템 성능 최소화 및 페이지 로딩 시간 최소화 보장

웹 위·변조 방지 솔루션 적용 전/후 성능 비교



▶ 테스트 환경

- 총 5개 페이지에 대해 로드런너(LoadRunner) Tset Tool을 이용하여 테스트 실시
- 부하발생에 따른 CPU 증가량 측정(부하 증가에 따른 CPU 증가율이 비례하지 않음)

응답 시간 비교

- 솔루션 적용전 : 총 hit수 = 377579, 처리량 = 약 269 TPS, **평균응답시간 = 약 38 ms**
- 솔루션 적용후 : 총 hit수 = 340539, 처리량 = 약 233 TPS, **평균응답시간 = 약 47 ms**

▶ 테스트 환경

- 제안 솔루션 적용 전후의 응답시간을 MS Stress Test Tool을 이용해 테스트
- Client 동시 부하 발생 thread 수 20 기준, 총 hit수, 처리량, 평균응답시간을 조사

특징 및 기대효과

- 필터로만 동작하여 리소스 점유 최소화
- 평균 CPU 증가율 **6.13%** (TPS 30) / **6.73%** (TPS 60)로 운영환경 성능 최소화 보장
- 웹 위·변조 방지 솔루션 적용 전/후 페이지 요청시

평균응답시간

차이로 빠른



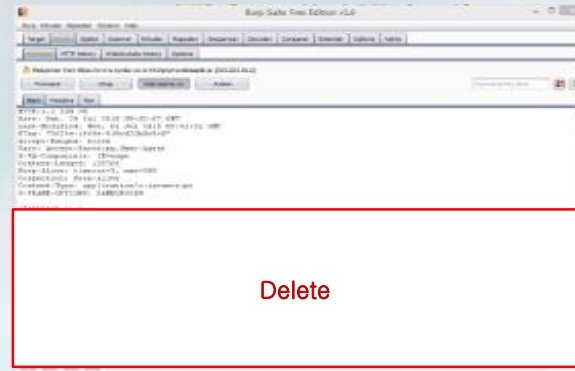
5. PNP4WEB 성능 및 안전성 - 프로그램 자체보호

자체보호 API 적용을 통한 솔루션 무력화 원천 차단

Self-Protect 적용



자체 보호기능 API 적용



Delete

검증 스크립트 무력화



차단 페이지 이동/화면 로딩 차단

주요특징

- 자체 보호기능 적용으로
검증스크립트가 로드되지
않으면 서비스 차단 적용
- 검증스크립트 변조를
통한 우회 접근 시
차단페이지로 이동/화면
로딩 차단

5. PNP4WEB 성능 및 안전성 - 업무연속성 보장

다양한 예외처리 기능 제공을 통한 신속한 장애대응

정책관리

정책관리

그룹: 그룹 선택, 호스트명/URL: jsweb01, 검증정책명: 정책, 정책: 정책

그룹	서버명	URL(호스트명)	검증정책명	정책명	등록일자
기본	jsweb01/asp.asp	/jsweb01/asp.asp	정책	정책	2014/05/29 10:02:58
기본	jsweb01/asp.asp	/jsweb01/asp.asp	정책	정책	2014/05/29 10:02:58
기본	jsweb01/asp.asp	/jsweb01/asp.asp	정책	정책	2014/05/29 10:02:58
기본	jsweb01/asp.asp	/jsweb01/asp.asp	정책	정책	2014/05/29 10:02:58
기본	jsweb01/asp.asp	/jsweb01/asp.asp	정책	정책	2014/05/29 10:02:58
기본	jsweb01/asp.asp	/jsweb01/asp.asp	정책	정책	2014/05/29 10:02:58
기본	jsweb01/asp.asp	/jsweb01/asp.asp	정책	정책	2014/05/29 10:02:58
기본	jsweb01/asp.asp	/jsweb01/asp.asp	정책	정책	2014/05/29 10:02:58
기본	jsweb01/asp.asp	/jsweb01/asp.asp	정책	정책	2014/05/29 10:02:58
기본	jsweb01/asp.asp	/jsweb01/asp.asp	정책	정책	2014/05/29 10:02:58

페이지 / 웹 파일별 검증대상
예외처리 적용

정책관리

사용자ID/단말IP별 검증대상관리

사용자ID: 사용자ID, 단말IP: 단말IP, 검증정책명: 정책, 정책: 정책

사용자ID	검증정책명	서버명	정책명	등록일자
jsweb01/asp.asp	정책	jsweb01/asp.asp	정책	2014/05/29 10:02:58
jsweb01/asp.asp	정책	jsweb01/asp.asp	정책	2014/05/29 10:02:58
jsweb01/asp.asp	정책	jsweb01/asp.asp	정책	2014/05/29 10:02:58
jsweb01/asp.asp	정책	jsweb01/asp.asp	정책	2014/05/29 10:02:58
jsweb01/asp.asp	정책	jsweb01/asp.asp	정책	2014/05/29 10:02:58
jsweb01/asp.asp	정책	jsweb01/asp.asp	정책	2014/05/29 10:02:58
jsweb01/asp.asp	정책	jsweb01/asp.asp	정책	2014/05/29 10:02:58
jsweb01/asp.asp	정책	jsweb01/asp.asp	정책	2014/05/29 10:02:58
jsweb01/asp.asp	정책	jsweb01/asp.asp	정책	2014/05/29 10:02:58
jsweb01/asp.asp	정책	jsweb01/asp.asp	정책	2014/05/29 10:02:58

사용자ID / 단말IP별 검증대상
예외처리 적용

정책관리

개별 서버 환경설정

서버명: jsweb01/asp.asp, 검증정책명: 정책, 정책: 정책

서버명	검증정책명	정책명	정책	정책	정책	정책	정책	정책	정책
jsweb01/asp.asp	정책	정책	정책	정책	정책	정책	정책	정책	정책
jsweb01/asp.asp	정책	정책	정책	정책	정책	정책	정책	정책	정책
jsweb01/asp.asp	정책	정책	정책	정책	정책	정책	정책	정책	정책
jsweb01/asp.asp	정책	정책	정책	정책	정책	정책	정책	정책	정책
jsweb01/asp.asp	정책	정책	정책	정책	정책	정책	정책	정책	정책
jsweb01/asp.asp	정책	정책	정책	정책	정책	정책	정책	정책	정책
jsweb01/asp.asp	정책	정책	정책	정책	정책	정책	정책	정책	정책
jsweb01/asp.asp	정책	정책	정책	정책	정책	정책	정책	정책	정책
jsweb01/asp.asp	정책	정책	정책	정책	정책	정책	정책	정책	정책
jsweb01/asp.asp	정책	정책	정책	정책	정책	정책	정책	정책	정책

서버 / 인스턴스별 검증대상
예외처리 적용

주요
특징

- 페이지 오류 발생 시 특정 URL 예외처리 적용 가능
- 서버 부하 및 시스템 장애 발생 시 서버별 예외처리 기능 제공
- 사용자 장애 발생 시 사용자ID 및 단말 IP 예외처리 적용을 통해 서비스 연속성 보장

5. PNP4WEB 성능 및 안전성 – 신뢰성 제공

소프트웨어 품질인증을 통한 제품의 신뢰성 제공



나라장터종합쇼핑몰



주요 특징

- GS 인증으로 신뢰성 제공
- GS 인증 제품명 – PNP4WEB 웹 위.변조방지 솔루션
- 품질인증 = GS 1등급, 나라장터 3자 단가 공급제품으로 등록

6. PNP4WEB 주요 구축사례

다수의 대형기관 웹 서비스에 웹페이지 위·변조 방지 솔루션 구축

IBK 기업은행  (2012.07~2012.10)	KB 국민은행  (2016.09~2018.7)	신협중앙회  (2014.04~2014.07)	하나은행  (2014.09~2014.12)	교보생명  (2015.03~2015.05)
적용업무 인터넷뱅킹(WEB) 서비스	적용업무 인터넷뱅킹(WEB) 서비스 1,2,3 센터 구축	적용업무 인터넷뱅킹(WEB) 서비스	적용업무 인터넷뱅킹(WEB) 서비스	적용업무 보험계약(WEB) 서비스
씨티은행  (2015.04~2015.06)	IBK연금보험  (2015.09~12)	저축은행중앙회  (2017.02~07)	대구은행  (2013.12~2014.02)	한국교직원공제회  (2017.12~2018.12)
적용업무 인터넷뱅킹(WEB) 서비스	적용업무 인터넷뱅킹(WEB) 서비스	적용업무 인터넷뱅킹(WEB) 서비스	적용업무 인터넷뱅킹(WEB) 서비스	적용업무 모바일 홈페이지 서비스

6. PNP4WEB 주요 구축사례

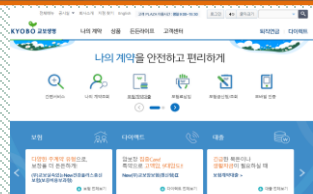
다수의 대형기관 웹 서비스에 웹페이지 위·변조 방지 솔루션 구축

KB 국민은행  (2018.09 구축완료)	IBK 기업은행  (2018.12 구축완료)	SC 제일은행  (2019.05 구축완료)	IBK 기업은행  (2020.02 구축완료)	KB 국민은행  (2019.03~ 구축중)
적용업무	적용업무	적용업무	적용업무	적용업무
인터넷뱅킹(WEB) 서비스 제 3 센터 구축	모바일 웹(WEB)	모바일 웹(WEB)	외환 페이고스 사업	The K 프로젝트(2년) 비대면 채널개편

신용회복위원회  (2019.11 구축완료)	한국교직원공제회  (2019.11 구축완료)	한국환경공단  (2020.06 구축완료)	KB 국민은행  (2020.10 구축완료)	우리금융캐피탈  (2020.10 ~)
적용업무	적용업무	적용업무	적용업무	적용업무
페이퍼리스사업	PC웹 홈페이지 서비스	외환사업부 모바일 웹(WEB)	모바일브랜치	PC & 모바일웹 (WEB)

6. PNP4WEB 주요 구축사례

다수의 대형기관 웹 서비스에 웹페이지 위·변조 방지 솔루션 구축

한화생명  (2020.11 ~)	IBK 기업은행  (2020.12 ~)	IBK 기업은행  (2021.3 ~)	신용정보원  (2021.05 ~)	한국교직원공제회  (2021.7 ~)
적용업무	적용업무	적용업무	적용업무	적용업무
보험코어 구축사업	OPEN API 구축사업	마이데이터 구축사업	마이데이터 종합포털 및 중계플랫폼 구축사업	모바일보험 전자청약 시스템
수출입은행  (2021.08 ~)	교보생명  (2022.01 ~)	한국투자캐피탈  (2022.06 ~)	신협중앙회  (2023.04~2023.07)	신협중앙회  (2023.08~2023.12)
적용업무	적용업무	적용업무	적용업무	적용업무
대고객 디지털 플랫폼 구축 프로젝트	홈페이지&모바일 통합 리뉴얼 구축 사업	리테일 구축사업	기업 전자금융 채널구축사업	라이프온 구축사업

6. PNP4WEB 주요 구축사례

다수의 대형기관 웹 서비스에 웹페이지 위·변조 방지 솔루션 구축

한국환경공단



(2023.12 ~ 2024.04)

적용업무

무공해차 대민서비스
WEB WAS 증설사업

한국교직원공제회



(2024.09 ~ 2025.01)

적용업무

보험청약
DR시스템 구축사업

한국환경공단



(2024.07 ~ 2024.12)

적용업무

대민서비스
DR시스템 구축사업

지능정보사회진흥원



(2025.01 ~)

적용업무

정부 디지털감
서비스구현 사업