https://doi.org/10.5392/JKCA.2021.21.01.426

IDC환경에서 공공부문 홈페이지 장애상황공지 시스템 구축방안

Implementaion Mechanism of Homepage Failure Notification System in Public Sector in IDC Environment

김용태, 조인준
배재대학교 사이버보안학과

Yong-Tae Kim(kytboy@nate.com), In-June Jo(injune@pcu.ac.kr)

요약

최근 들어 공공부문 정보화에 대한 투자가 기존보다 증가하는 추세이다. 초고속 인터넷과 스마트폰 보급이 일반화되었으며 그에 따라 공공부문 대국민에게 제공하는 정보시스템의 안정성은 무엇보다 중요한 관리요소가 되었다.

즉, 공공기관의 민원 처리와 증명서 발급, 은행의 금융 거래, 통관 업무, 개인 또는 기관의 전자상거래 등과 같은 업무가 대부분 온라인 처리로 이루어지고 있다. 그렇기 때문에 중요 민원 업무를 담당하고 있는 정보시스템에서 발생되는 장애를 어떻게 처리하느냐가 매우 중요한 쟁점으로 대두되고 있다. 즉, 짧은 시간이라도 정상적으로 동작하지 않는 장애의 경우 민원에게 재정상 큰 손해를 유발 등과 더불어 해당 업무처리 지연 시 다양한 문제가 발생할 수 있다. 이는 공공기관 신뢰도 하락과 민원 제기 등의 여러 가지 피해를 동반할 수 있다. 정보시스템 장애가 발생하는 이유들은 매우 다양하고 현실적으로 발생 시기를 예측하기 힘들다. 본 논문에서는 장애에 대응하는 여러 가지 방안 중에서 민원인 입장에서 홈페이지 장애 발생 시 민원인이 장애로 인한 혼란을 최소화할 수 있는 장애상황공지 시스템 구축방안을 제안하였다. 제안한 장애상황공지 시스템을 공공 IDC환경에 구축하여 활용 가능성을 보였다.

■ 중심어 : | 시스템 장애 | 장애 공지 | 장애 관제 | 홈페이지 장애 |

Abstract

Investment in public sector information services has been on the rise in recent years. The supply of high-speed Internet and smartphones has become more common, and the stability of the information system provided to the public in the public sector has become an important management factor.

In other words, tasks such as handling civil complaints and issuing certificates by public institutions, financial transactions by banks, customs clearance work, and e-commerce by individuals or institutions are mostly done online. Therefore, how to deal with obstacles arising from the information system, which is in charge of important civil service affairs, is becoming a very important issue. In other words, in the case of a disability that does not function normally even for a short period of time, various problems can occur when the work is delayed, as well as causing serious financial damage to the civil petitioner. This could be accompanied by a decline in public confidence and various other damages such as filing civil complaints. The reasons for the occurrence of information system failures are very diverse and realistically difficult to predict when. Among the various measures to cope with disability, this paper proposed a plan to establish a disability situation notification system that can minimize confusion caused by disability in the event of a homepage malfunction. The proposed disability situation notification system was established in the public IDC environment to show the possibility of utilization.

■ keyword : | System Fault | Fault Notice | Fault Control | Homepage Fault |

접수일자 : 2020년 09월 21일
수정일자 : 2020년 10월 12일
심사완료일 : 2020년 10월 12일
교신저자 : 김용태, e-mail : kytboy@nate.com

I. 서 론

최근 들어 공공부문 정보화에 대한 투자가 기존보다 증가하는 추세이다. 초고속 인터넷과 스마트폰 보급이 일반화되었으며 그에 따라 공공부문 대국민에게 제공하는 정보시스템의 안정성은 무엇보다 중요한 관리요소가 되었다. 일반적으로 장애란 “통제 가능한 요인들에 의한 정보시스템의 기능 저하, 오류, 고장”을 의미하며 재해(자연재해와 인적재해)와 같이 통제할 수 없는 장애, 발생원인 측면에서 기반구조장애(설비 장애, 운영장애) 또는 시스템장애 등은 통제할 수 있는 유형의 장애 등이 있다[1].

정보시스템 장애는 시스템 제공 용도에 따라 영향이 매우 심각할 수 있다. 제공 서비스가 대국민의 중요 업무를 담당하는 시스템(금융, 민원발급 등)이거나 개인정보를 관리하는 시스템인 경우 짧은 시간이라도 정상적으로 동작하지 않는다면 사용자의 재정상 손해 또는 업무수행에 차질이 발생한다. 제공 기관 입장에서는 신뢰도 하락과 불만민원 발생 등의 여러 가지 피해 발생할 수 있기 때문에 정상적인 서비스를 제공할 수 없는 경우 신속하게 향후 서비스 제공시간과 현 상황을 공지하여 사용자의 신뢰확보와 이용목적 차질을 최소화하는 것 또한 매우 중요하다.

정보시스템 장애가 발생하는 이유는 다양하며 현실적으로 발생 시기를 예측하기 힘들다. 장애가 발생하지 않는 시스템은 기대하기 어려우며 현실적인 대안은 최대한 신속하게 장애를 관제하고 시스템 담당자와 조치 가능자에게 즉시 상황을 전파하여 복구시간을 최소화하는 것이라고 할 수 있다[2].

본 논문에서는 이와 같은 연구목적을 달성하고자 대국민 서비스를 제공하는 인터넷 데이터 센터(IDC)환경에서 홈페이지 장애 발생 또는 정상적인 서비스 제공 불가 시 신속하게 홈페이지 상황을 사용자에게 공지하는 시스템 구축방안을 제안하였다.

II. 홈페이지 장애상황공지 시스템 구현

1. 장애상황공지 시스템 기본 구성방안

IDC(Internet Data Center)에서 외부 사용자가 특정 홈페이지로부터 정상적인 서비스를 받는 절차를 [그림 1]을 바탕으로 설명하면 다음과 같다. 홈페이지를 이용하려는 외부 사용자는 ISP(Internet Service Provider) 인터넷을 거쳐 IDC의 백본 스위치를 시작으로 방화벽과 보안 장비를 통과하여 홈페이지 서버에 접속하여 서비스를 제공 받는다. 최초 외부 유입 트래픽의 경로를 결정하는 네트워크 장비는 구성도 상단에 위치한 백본스위치이다.

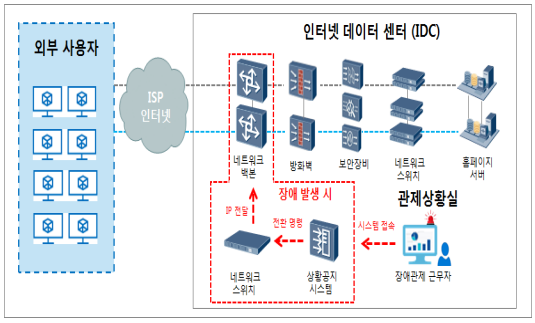

그림 1. 홈페이지 장애상황공지시스템 기본 구성도

본 논문에서 제안한 장애상황공지 시스템 기본 구성도는 [그림 1]의 점선 부분이다. 제안한 홈페이지 장애상황공지 시스템의 기본 동작 절차를 단계별로 살펴보면 다음과 같다. 첫째, 홈페이지 장애가 발생하면 장애의 종류에 따라 대응절차가 결정된다[3]. 둘째, 그 결정이 장애상황 공지로 결정되면 장애관제 근무자는 장애상황공지 시스템에 접속하여 해당 IP주소로 접근하는 트래픽에 대해 우회경로로 경로 전환을 수행한다. 즉, 해당 홈페이지 IP주소로 향하는 트래픽은 장애상황공지 시스템과 연결되어있는 네트워크 스위치로 동적 라우팅 IP주소로 전달된다. 이때, 백본 스위치와 라우팅 교환 알고리즘에 따라 정보가 동기화된다. 셋째, 동기화가 완료된 후에는 외부 사용자는 변경된 라우팅 정보에 따라 실제 목적지 홈페이지 서버가 아닌 장애상황 공지 시스템으로 트래픽이 우회 유입되어 장애상황공지 페이지의 내용을 확인할 수 있다. 다음 절들에서는 이러한 장애상황공지 시스템을 구체적으로 구현하기 위한 구성요소들을 설명하였다.

2. 장애상황공지 시스템 웹페이지 구성

홈페이지 장애상황공지 시스템의 개발환경은 [표 1]과 같다. 이와 더불어 네트워크 라우팅 테스트를 위해 Juniper L3 스위치를 사용하였다. 서버에서 라우팅 전환을 위해 Telnet 형식의 Perl 스크립트를 이용하여 L3 스위치에 전환 명령이 이루어지도록 하였다.

표 1. 시스템 개발 환경

구 분	정 보
운영체제	CentOS (Linux) / WMWare
IP	192.168.80.10
WEB	Apache
Database	MySQL
개발 언어	PHP, Perl Script, Telnet
스위치	Juniper Switch (IP: 192.168.80.5)

2.1 장애상황공지 화면 작성

장애상황 공지내용을 작성하는 메뉴를 [그림 2]와 같이 구성하였다. 호스트, 홈페이지명, 화면 로고, 공지내용을 입력하여 신규 추가와 수정이 가능하도록 하였다.

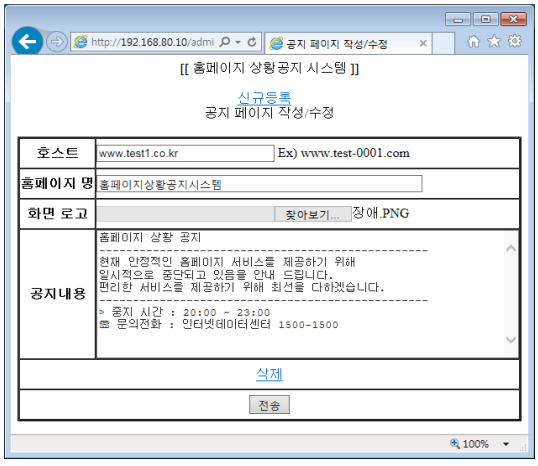

그림 2. 공지 화면 작성

2.2 장애상황공지 홈페이지 목록 관리

장애상황공지 홈페이지의 목록을 입력하여 관리 할 수 있도록 하였다. [그림 3]에서 본 바와 같이 라우팅 전환/해제, 공지 화면을 신규 등록, 수정, 삭제할 수 있도록 하였다.

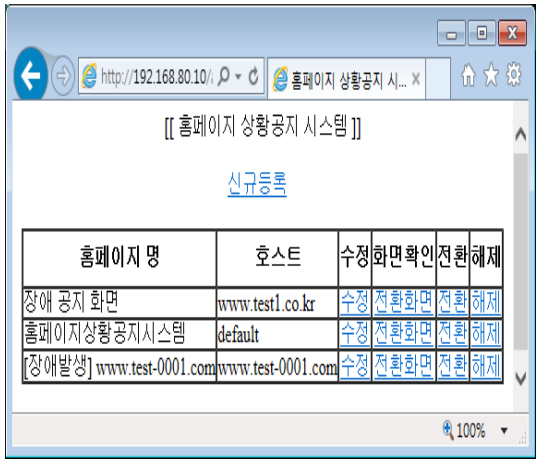

그림 3. 장애상황공지 홈페이지 목록 관리

2.3 장애상황공지 화면

장애 발생 홈페이지 접속 사용자에게 장애 상황을 공지하는 화면은 [그림 4]와 같이 구성하였다. 장애상황공지 홈페이지 목록정보를 조회할 수 있도록 하였다.

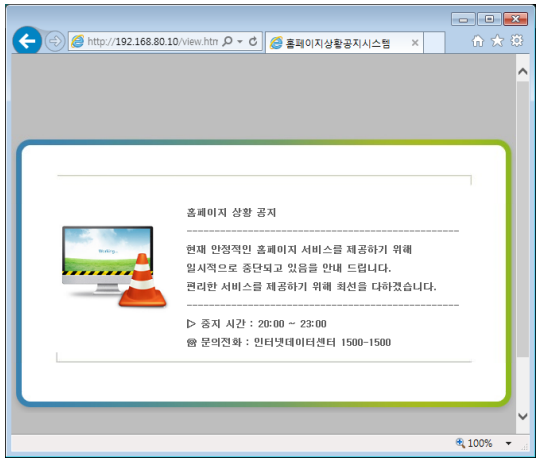

그림 4. 장애 상황 공지 화면

3. 주요 기능 구현

3.1 전환 대상 IP 정적 라우팅 설정

전환 대상 IP 정적 라우팅 설정 절차를 단계별로 설명하면 다음과 같다. 첫째, 장애상황공지 웹서버에 저장되어있는 호스트 정보를 DNS(Domain Name System) 서버에 질의하여 IP주소를 받아 온다. 둘째, 해당IP주소는 [그림 5]와 같이 스크립트의 '$STATIC_IP' 변수에 저장하고 이를 기반으로 공지 서버와 연결된 네트워크 스위치에서 실행된다[4]. 셋째, 스크립트 실행으로 네트워크 스위치는 라우팅 테이블에 정적 라우팅 대상으로 해당 IP주소를 추가한다. 넷째, 네트워크 스위치의 변경 정보를 연결된 백본 스위치와 동기화한다. 이후 해당 IP주소로 향하는 트래픽은 장애상황공지 서버로 우회된다.

```
# 네트워크 스위치 접속 정보
$unix_box = "192.168.80.5";
$username = "test01";
$password = "test01!@";

# 네트워크 스위치 접속
my $prmpt = '/.*)/i';
$telnet = new Net::Telnet (Timeout=>10, Prompt => $prmpt,
Errmode => 'die');
use Net::Telnet;
$telnet->open($unix_box);
$telnet->waitfor('/Login:/i');
$telnet->print($username);
$telnet->waitfor('/Password:/i');
$telnet->print($password);
$telnet->waitfor('/.*)/i');
$telnet->print("edit");
$telnet->waitfor('/.*#/i');

# 전환 대상 STATIC 라우팅 추가 및 적용
$telnet->print("set routing-options static route
$STATIC_IP[0]/32 next-hop 192.168.80.10");
$telnet->waitfor('/.*#/i');
$telnet->print("set policy-options policy-statement ind term 10
from route-filter $STATIC_IP[0]/32 exact");
$telnet->waitfor('/.*#/i');
$telnet->print("commit");
$telnet->waitfor('/.*#/i');
$telnet->print("exit");
$telnet->waitfor('/.*#/i');
$telnet->print("exit");
$telnet->close;
```

그림 5. 라우팅 IP 추가 스크립트

장애가 해결되어 해제 처리하는 소스코드는 [그림 6]과 같다. 즉, 해당 IP주소를 라우팅 테이블에서 삭제 시 실제 홈페이지 서버로 접속될 수 있도록 구현하였다.

```
-- 중략 --
# 전환 대상 STATIC 라우팅 삭제 및 적용
$telnet->print("delete routing-options static route
$STATIC_IP[0]/32 next-hop 192.168.80.10");
$telnet->waitfor('/.*#/i');
$telnet->print("delete policy-options policy-statement ind term
10 from route-filter $STATIC_IP[0]/32 exact");
$telnet->waitfor('/.*#/i');
$telnet->print("commit");
-- 이하 생략 --
```

그림 6. 라우팅 IP 삭제 스크립트

3.2 전환 트래픽 수신

공지 서버로 전환된 데이터 패킷의 실제 목적지는 장애가 발생한 홈페이지 서버이다. NIC(Network Interface Card)는 타 목적지 IP주소로 전달되는 데이터 패킷을 무시하도록 기본설정되어 있다. 전환된 데이터 패킷 수신을 위해 [그림 7]과 같이 'Promiscuous mode'를 적용하여 타 목적지 데이터 패킷을 수용할 수 있도록 설정하였다.

```
[/]# ifconfig eth0 promisc
[/]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:E7:CF:25
          inet addr:192.168.80.10  Bcast:192.168.80.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fee7:cf25/64 Scope:Link
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:2269 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2000 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:281038 (274.4 KiB)  TX bytes:269481 (263.1 KiB)
```

그림 7. Promiscuous mode 적용

3.3 전환 데이터 패킷 목적지 설정

전환 데이터 패킷의 처리 흐름은 [그림 8]과 같다. 'Promiscuous mode'를 적용하여 전환대상 데이터 패킷도 유입되도록 설정하였지만, 장애상황공지 서버는 실제 사용자가 요청한 목적지 홈페이지 서버가 아니다. 따라서

'HTTP Request'에 대한 '응답'이 불가하다.

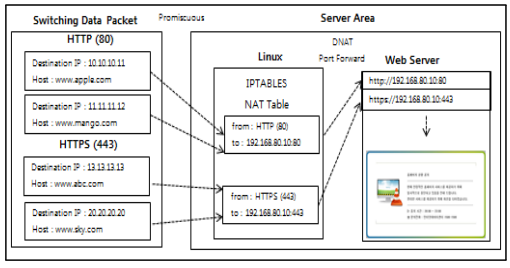

그림 8. 전환 트래픽 응답 처리 흐름도

공지 서버에 유입되는 'HTTP, HTTPS Request'에 대하여 '응답' 처리를 위해 [그림 9]와 같이 'iptables'의 DNAT(Destination network address translation)를 설정하여 목적지 포트 포워딩을 할 수 있도록 기능을 구현하였다[5][6].

```
[/]# iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT --to-destination 192.168.80.10:80
[/]# iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 443 -j DNAT --to-destination 192.168.80.10:443
[/]# iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination
DNAT       tcp  --  anywhere             anywhere            tcp dpt:http to:192.168.80.10:80
DNAT       tcp  --  anywhere             anywhere            tcp dpt:https to:192.168.80.10:443
```

그림 9. IPTABLES NAT 정책 설정

3.4 'HTTP Request' 메시지 'Host' 정보 식별

'HTTP Request'메시지 'Host' 식별처리는 [그림 10]과 같다.

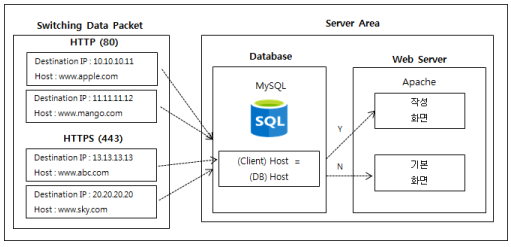

그림 10. HTTP Request 메시지 Host 정보 식별

[그림 11]과 같이 클라이언트의 'Host'정보를 '$http_host' 변수에 저장하여 '$query'의 SQL구문에 따라 얻어진 클라이언트의 'Host'와 장애상황공지 서버 DB에 데이터를 비교한다. 조회된 데이터가 존재 시 작성화면을 제공하고, 존재하지 않을 시 기본화면을 제공하도록 구현하였다.

3.5 클라이언트/서버 오류 상태코드 처리

장애상황공지 서버로 유입된 트래픽은 장애가 발생한 실제 홈페이지로 요청한 'HTTP Request'이다. 이와 같은 요구에 따라 발생되는 결과는 존재하지 않은 URL(Uniform Resource Locator) 접속(Not Found, 상태코드 404), 허용되지 않은 요청 메소드 사용(method not allowed, 상태코드 405), 그리고 서버 내부 처리 오류(Interval Server Error, 상태코드 500)

```
// 라우팅된 HTTP Request Header Host 저장
$http_host = explode(':',$_SERVER['HTTP_HOST']);

                        ---- 중략 ----

//호스트 정보 확인 쿼리
$query = " SELECT no,
                host,
                title,
                img,
                text
    FROM  (
                    // 호스트 정보 확인
                SELECT    '1'  AS no ,
                            host,
                            title,
                            img,
                            text
                 FROM    domain_list
                WHERE    host = '". $http_host ."'
                UNION
                    // 기본화면
                SELECT    '2'  AS no ,
                            host,
                            title,
                            img,
                            text
                FROM     domain_list
                WHERE    host = 'default')
          ) ;
                        ---- 이하 생략 ----
```

그림 11. HTTP Request 메시지 Host 식별 소스코드

등과 같다.

즉, 이들을 요약하면 클라이언트 요청 오류나 서버에서 처리 불가 오류이다.

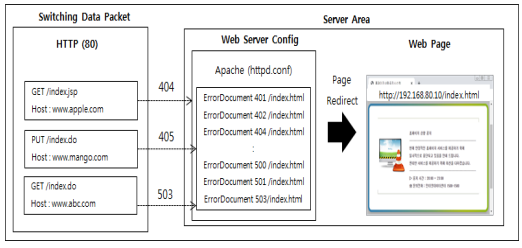

그림 12. HTTP 상태코드 별 내부 페이지 리다이렉트 설정

[그림 12]와 같이 장애상황공지 서버는 이러한 오류 상태코드와 관계없이 장애상황공지 화면을 제공하기 위해 웹서버(Apache일 경우)의 설정파일을 [그림 13]와 같이 'ErrorDocument' (사용자정의 오류응답)를 추가하였다[7].

```
ErrorDocument 400 /index.html
ErrorDocument 402 /index.html
ErrorDocument 403 /index.html
ErrorDocument 404 /index.html
ErrorDocument 405 /index.html
                : (중략)
ErrorDocument 500 /index.html
ErrorDocument 501 /index.html
ErrorDocument 502 /index.html
ErrorDocument 503 /index.html
ErrorDocument 504 /index.html
```

그림 13. 사용자 정의 웹서버 오류

Ⅲ. 실증 테스트

실증테스트 환경은 [그림 14]와 같으며 테스트 시나리오는 아래와 같이 4가지 경우를 대상으로 하였다.

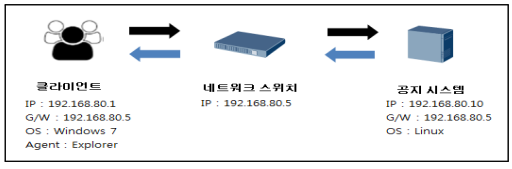

그림 14. 실증 테스트 구성도

첫째, 장애상황공지 웹서버에서 대상 'Host'로 전환 시 해당 IP주소로 전달되도록 네트워크 스위치에서 정적 라우팅 확인, 둘째, 외부에서 http/https 접속 시 정상 공지 화면 제공 여부, 셋째, 클라이언트 오류 발생 시 정상 페이지 제공 여부, 넷째, 실 서버 구축 시 최대 동시 접속자 수를 확인하기 위해 트래픽 테스트를 진행하였다.

1. 전환 대상 IP주소 라우팅 추가

장애상황공지 웹서버의 공지화면 관리메뉴에서 홈페이지01(IP주소 : 192.168.80.100), 홈페이지02(IP주소 :192.168.80.200) 라는 두개의 홈페이지를 등록하여 [그림 15]과 같이 전환대상으로 하였다.

[[홈페이지 상황공지 시스템]]

신규등록

홈페이지 명	호스트	수정	화면확인	전환	해제
홈페이지 01	192.168.80.100	수정	전환화면	전환	해제
홈페이지 02	192.168.80.200	수정	전환화면	전환	해제

그림 15. 전환 대상 추가

테스트 결과 [그림 16]와 같이 전환을 수행한 두개의 IP주소를 연결된 스위치에 정적 라우팅 대상으로 추가되었다. 그 결과 목적지인 공지 서버(IP주소 :192.168.80.10)로 트래픽 유입됨을 확인하였다. 해제 시 라우팅 테이블에서 해당 정보가 삭제되었음을 확인하였다.

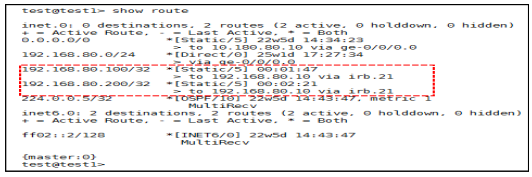

그림 16. 스위치 라우팅 테이블 정적 IP추가

2. 전환 후 상황공지화면 제공

클라이언트의 'hosts 파일'을 변경하여 [그림 17]과 같이 2개의 테스트 호스트로 접근 시 장애상황공지 서버로 접속되도록 설정하였다.

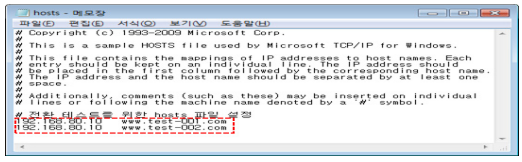

그림 17. 클라이언트 hosts 설정

장애상황공지 웹서버에서는 [그림 18]과 같이 장애와 작업 공지화면을 호스트별로 작성하여 식별 여부를 확인하였다.

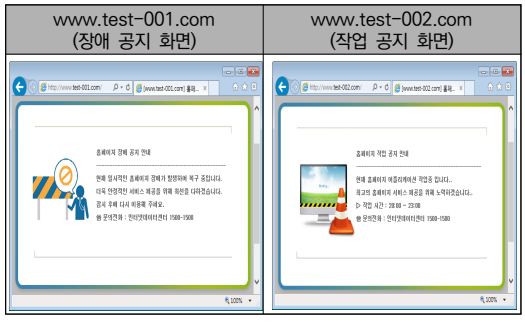

그림 18. 장애/작업 공지 화면

테스트 결과 'http://' 접속 시 데이터 패킷은 [그림 19]와 같이 평문전송으로 'HTTP Request'의 'Header host '값을 확인하여 작성한 공지화면이 정상적으로(상태코드 200)제공되었다. 그러나 'https://' 접속 시 해당 호스트의 기관 인증서가 공지 서버에 존재하지 않아 암호화된 데이터 패킷의 정보를 확인할 수 없어 기본페이지가 제공되었음을 확인하였다.

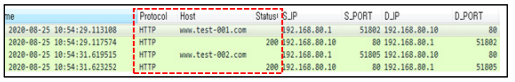

그림 19. http 접속 시 요청 데이터 패킷 확인결과

3. 사용자 정의 응답 설정

사용자 정의 응답 설정 전 웹서버에 존재하지 않는 "http://192.168.80.10/main.do"로 접속 시 "존재하지 않는 URL 접속(상태코드 404)" 오류가 발생하였으나, 설정 후 결과는 "http://192.168.80.10/index.html"로 페이지 재 전환이 되어 정상적으로 공지 화면이 제공되었다. 결과는 [그림 20]과 같다.

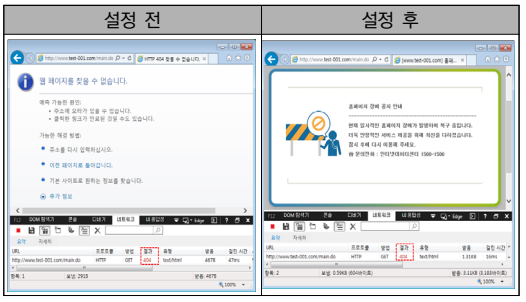

그림 20. 사용자 정의 응답 설정 결과

4. 서버 수용량 테스트

실 서버 구축 시 최대 동시 접속자 수를 확인하고자 [그림 21]과 같은 환경에서 테스트를 진행하였으며 사용자 1명이 접속 시 공지화면을 구성하는 6개 객체를 호출하였다.

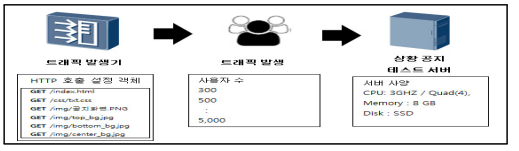

그림 21. 트래픽 수용량 테스트 구성

트래픽 발생기에 공지 서버를 연결하여 단일/다중 호스트로 전환 시 수용량을 확인하였으며 그 결과는 [표 2]와 같다.

표 2. 서버 응답률 통계

접속자	접속 성공률			평균	HTTP 응답 처리	동시 접속자
	1 페이지	3 페이지	5 페이지			
300	100%	99%	99%	99.3%	2,085	348
500	99%	98%	98%	98.3%	3,441	574
1,000	50%	53%	58%	53.7%	3,759	627
1,500	28%	27%	28%	27.7%	2,909	485
2,000	18%	22%	22%	20.7%	2,898	483
3,000	14%	14%	12%	13.3%	2,793	466
5,000	7%	9%	7%	7.7%	2,695	449
평 균					**2,940**	**490**

테스트 결과 1초 평균 490명이 동시 접속 가능했다. 클라이언트 요청을 처리하지 못하는 경우 CPU 사용률이 90%이상 사용되었고, 웹서버 요청 처리를 하는 httpd 프로세스가 '큐(Queue)'에서 처리를 기다리는 상태로 누적되어 있었다. 장애상황공지 페이지 접속 시 응답 대기 상태가 확인되었다. 장애 발생으로 다수 홈페이지를 전환 시 공지 서버의 자원 사용율과 유입 트래픽을 확인하여 사용자 세션을 제한할 필요성이 확인되었다.

Ⅳ. 기대 효과

IDC환경에서 공공부문 홈페이지 장애상황공지 시스템 도입 시 기대 효과는 첫째, 사용자 불만 민원이 감소될 것이다. 갑작스러운 장애 발생으로 아무런 공지 없이 서비스 이용에 문제가 발생하면 해당 기관으로 불만 민원이 발생할 수 있다. 시스템도입으로 장애 인지 시 신속하게 상황을 공지하여 불만민원을 최소화할 수 있을 것이다. 둘째, 제공기관의 신뢰도확보이다. 중요업무를 담당하고 있는 정보시스템이 상황공지 없이 장시간

장애로 언론 미디어에 공개 발표되어 제공 기관의 신뢰도가 하락하는 사례가 종종 발생하고 있다. 시스템을 이용하여 사용자에게 안내문과 예상 복구시간을 공지한다면 제공기관의 이미지 실추를 줄일 수 있을 것이다. 셋째, 홈페이지 작업의 경우에도 활용될 수 있다. 어플리케이션 소스 변경 및 오프라인 서버점검 등의 상황으로 서비스가 중단될 경우 사전에 제공문구와 중단시간을 관제상황실과 협의하여 전환/해제를 함으로써 사용자에게 작업으로 인한 중지안내공지를 할 수 있다.

V. 결 론

대국민에게 공공부문 홈페이지 서비스하는 데이터센터의 시스템 장애는 현실적으로 예측하기 힘들며 명확한 장애 예방법은 존재하지 않는다.

홈페이지 서비스를 위해 네트워크/서버 장비를 위탁운영하는 데이터센터, 소스코드 개발/관리하는 외부개발조직, IT장비를 제조/납품하는 공급업체로 나누어져 있어 장애 발생 시 실시간 대응이 어렵다.

본 논문에서는 IDC환경에서의 홈페이지 장애 또는 정상 서비스 제공 불가 시 사용자에게 실시간으로 상황을 공지하는 시스템 구성안을 제시하였다.

이를 통해 불가피하게 서비스를 제공할 수 없는 경우 즉시 상황을 공지하여 현재 상황과 서비스 제공 예상시간을 공지를 통하여 사용자의 이용과 업무수행에 있어 차질을 최소화할 수 있을 것이라 기대한다.

향후 실증테스트에서 도출된 보완사항으로 각 기관별 HTTPS 인증서를 관리하는 시스템과의 연계, 장애상황공지 서버의 자원사용률이 모니터링되어 접속 제어를 할 수 있는 기능이 추가 연구되어야 할 것이며, 웹해킹/서비스거부(DDoS) 공격에 대한 방어가 가능한 네트워크 영역에 시스템 구성이 되어야 할 것이다.

참 고 문 헌

[1] 국무조정실, 정보시스템 장애 관리지침, 국무조정실, 11-13, 2005.

[2] 전은희, *정부기관 정보시스템의 장애관리를 통한 장애 발생유형 및 최소화 방안에 관한 연구*, 강원대학교, 국내석사학위논문, pp.9-11, 2009.

[3] 재난위기종합상황실, 재난위기종합상황실 운영규정, 행정안전부, 6-10, 2012.

[4] http://www.perl.or.kr/tipsinaction

[5] https://ko.wikipedia.org/wiki/Iptables

[6] http://web.mit.edu/rhel-doc/

[7] https://httpd.apache.org/docs/2.4/ko/

[8] 오영택, 조인준, “인공지능 기술기반의 통합보안관제 서비스모델 개발방안,” 한국콘텐츠학회논문지, Vol.19, No.1, pp.108-116, 2019.

[9] 박영수, 이병엽, “일회용 세션을 활용한 인증정보 기반의 사용자 인증 방안,” 한국콘텐츠학회논문지, Vol.19, No.7, pp.421-426. 2019.

저 자 소 개

김 용 태(Yong-Tae Kim) 준회원

- 2008년 2월 : 우송공업대학 컴퓨터프로그래밍 전문학사
- 2017년 2월 : 국가평생교육진흥원 컴퓨터공학 학사
- 2019년 3월 ~ 현재 : 배재대학교 사이버보안학과 석사과정
- 2014년 1월 ~ 현재 : 이글루시큐리티(보안관제)

〈관심분야〉 : 장애관제, 보안관제, S/W 개발

조 인 준(In-June Jo) 정회원

- 1982년 2월 : 전남대학교 계산통계학과 학사
- 1985년 2월 : 전남대학교 전자계산학과 석사
- 1999년 2월 : 아주대학교 컴퓨터공학과 박사
- 1983년 ~ 1993년 : 한국전자통신연구원 선임연구원
- 1991년 ~ 현재 : 컴퓨터시스템응용기술사
- 2006년 ~ 현재 : 정보시스템수석감리원
- 1994년 ~ 현재 : 배재대학교 사이버보안학과 교수

〈관심분야〉 : 정보보호, 컴퓨터네트워크보안, 컴퓨터시스템응용, 정보시스템감리