분산서비스거부(DDOS)공격 대응지침

2011. 3. 23.

중앙선거관리위원회

개정이력 관리

개정번호	개정내용 요약	일 자	비 고
1.00	신규 제정	2011. 3. 23.	

차 례

분산서비스거부(DDoS)공격 대응지침

Ⅰ 총 칙

1. 목 적

본 지침은 「선거관리위원회 정보통신보안업무규정」(이하 '규정'이라 한다.) 제3장에 따라 분산서비스거부공격으로 인한 사이버침해사고를 예방하고 공격 발생 시 효과적 대응능력 확보 및 그 피해를 최소화하여 정보시스템 서비스가 중단없이 제공될 수 있도록 준거하여야 할 사항을 정함을 목적으로 한다.

2. 적용 범위

○ 본 지침은 다음의 자에 적용한다.

- 정보보호책임관 및 정보보호책임자(규정 제21조)
- 중앙(소속기관 포함) 및 시·도위원회 기반보호실무자
- 기타 선거관리위원회 홈페이지 등 정보시스템 서비스를 운영·지원하는 자

○ 기반보호실무자는 정보시스템 업무분야별로 정보보호담당, 보안장비담당, 네트워크담당, 서버담당, 홈페이지담당(이하 '담당실무자'라 한다)으로 구분한다.

3. 용어정의

○ "분산서비스거부공격"(이하 'DDoS[1]공격'이라 한다)이라 함은 인터넷 상에 분산되어 있는 다수의 악성코드 감염PC를 이용, 대량의 접속트래픽을 일시에 특정 사이트 또는 시스템에 전송하여 과부하를 유발시킴으로써 정상적인 정보시스템서비스를 할 수 없도록 하는 사이버공격을 말한다.

○ "악성코드"라 함은 PC나 서버에 침투하여 피해를 입히는 소프트웨어를 가리키며 컴퓨터바이러스, 웜, 트로이목마, 스파이웨어 등을 포함한다.

○ "좀비PC"(Zombie PC)라 함은 악성코드에 감염되어 PC이용자도 모르게 DDoS공격 등 사이버공격에 악용되는 일반 이용자 컴퓨터를 말한다.

○ "봇넷"(Botnet)이라 함은 사이버공격자들에 의해 제어되는 명령제어서버(Command & Control 서버)와 좀비PC들의 집합 또는 네트워크를 말한다.

---

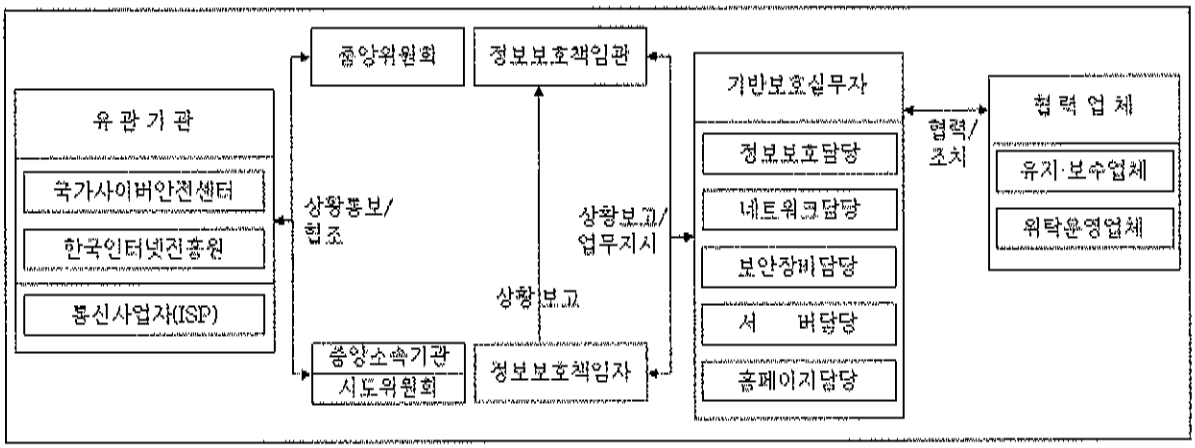
1) DDoS : Distributed Denial of Service

Ⅱ DDoS공격 대응체계

1. 대응조직

○ 정보보호책임관 및 정보보호책임자는 DDoS공격에 대한 예방활동과 공격 발생 시 신속하고 효과적인 대응을 위한 조직을 구성·운영하여야 한다.

○ 조직도 및 업무흐름



2. 역할별 임무

가. 정보보호책임관

○ DDoS공격 발생 시 대응 총괄

○ 피해범위 및 상황보고서 작성, 규정 제39조제3항에 따라 보고

○ 국가사이버안전센터(NCSC)에 사고 통보 및 협조

○ DDoS공격 피해 복구방안 수립 및 수행

○ DDoS공격 대응 모의훈련 주관 및 예방정책 수립

○ 산하·소속기관 DDoS공격 대응 관련 업무지원

○ 홈페이지 접속불가 등 위기상황 발생 시 대외홍보대책 마련

나. 정보보호책임자

○ 소관 정보시스템 DDoS공격 발생 시 대응 주관

○ 피해범위 및 상황보고서 작성, 규정 제39조제3항에 따라 보고

○ 정보보호책임관 및 국가사이버안전센터(NCSC)에 사고 통보 및 협조

○ DDoS공격 피해 복구방안 수립 및 수행

○ DDoS공격 대응 모의훈련 수행

○ 홈페이지 접속불가 등 위기상황 발생 시 대외홍보대책 마련

다. 기반보호실무자

○ 정보보호담당

- 정보자산에 대한 보안점검 및 대응절차서 마련 등 보안강화방안 수립
- 이상징후 발생 시 모니터링 결과 등을 종합 분석하여 공격여부 인지
- 보안장비, 네트워크, 서버 및 홈페이지 담당실무자(이하 '장비별 담당실무자'라 한다)와 협조, 긴급조치 수행
- 공격내용 분석 및 피해범위 파악을 통한 현황 보고
- 대응조치 수행 총괄 및 통신사업자(ISP[2]) 협조
- DDoS공격 후 복구방안 수립 및 복구수행 실무 총괄

○ 보안장비, 네트워크, 서버 및 홈페이지담당

- 평시 장비 설정, 트래픽 모니터링 및 로그, 통계분석을 통한 최적화 수행
- 이상 징후 발생 시 정보보호 담당실무자에 통보
- 장비별 담당실무자 상호 간에 정보 공유
- 장비별 유지·보수업체 또는 위탁운영업체와 협력
- DDoS공격 인지 시 장비별 상태 확인 후 긴급조치 수행
- DDoS공격 대응절차에 따라 피해 최소화를 위한 대응 수행
- DDoS공격 후 장비별 복구방안 수립 협조 및 복구 수행

3. 비상연락망 유지

○ 정보보호책임관 및 정보보호책임자는 DDoS공격 발생 시 신속한 대응조치 수행을 위하여 비상연락망(별지서식1 참조)을 구성·유지하여야 한다.

○ 비상연락망에는 정보시스템 담당실무자, 유지·보수업체 및 위탁운영업체 담당자, 유관기관 등 필요한 연락처를 포함한다.

※ 별지서식 1 'DDoS공격 대응 담당자 비상연락망' 서식

4. 네트워크 및 장비현황 유지

○ 담당실무자는 DDoS공격에 대한 체계적 대응을 위하여 운영하는 보안장비, 네트워크장비, 서버장비, 홈페이지에 대한 규격 및 구성도 등 현황(별지서식2 참조)을 항상 최신의 상태로 유지하여야 한다.

※ 별지서식 2 'DDoS공격 대응 정보시스템 구성장비 목록' 서식

---

2) Internet Service Provider: 인터넷 접속에 필요한 장비와 통신회선을 갖추고 인터넷 접속서비스를 제공하는 사업자

○ 정보보호담당실무자는 DDoS공격에 대한 적절한 대응위치를 결정하고 신속한 대응활동을 위하여 네트워크 구성 요소들의 연동현황이 명확히 나타나는 구성도를 유지·관리하여야 한다.

Ⅲ DDoS공격 예방활동

정보보호책임관 및 정보보호책임자는 DDoS공격에 대비하기 위하여 수시로 시스템 운영상황을 점검하며, 다음과 같은 활동을 수행하여야 한다.

1. 시스템 증설 및 보안장비 도입

○ 홈페이지서비스 등 선거 시 급격히 증가하는 시스템 운영상황을 확인하여 서비스 중요도 및 의존도에 따라 단계별로 네트워크 회선 및 장비, 서버 등의 증설계획을 수립하고 전문인력 확보를 위한 방안을 마련한다.

○ DDoS대응장비, 침입방지장비(IPS[3]), 방화벽 등 보안장비의 도입과 운영, 재정비에 대한 계획을 수립·시행한다.

2. 시스템 최신상태 유지 및 악성코드 감염방지

○ 정보시스템 및 장비상태를 최신으로 유지하기 위한 관리대책을 마련하고, 유지·보수업체 및 위탁운영업체와의 협력을 통하여 보안패치 적용 및 시스템 재정비를 수행한다.

○ 악성코드 감염을 통한 좀비PC 및 봇넷의 확산을 방지하기 위하여 유해사이트 차단, 백신프로그램 설치 및 점검, 주기적 보안업데이트 적용 등에 대한 관리대책을 마련한다.

3. DDoS공격 대응 모의훈련 및 교육 실시

○ 유관기관 또는 유지·보수업체와의 협력을 통하여 모의 DDoS공격 대응훈련을 정기적으로 실시하고, 훈련결과를 분석하여 문제점 및 보완사항을 운영 시스템과 장비에 적용하기 위한 방안을 수립한다.

○ 담당실무자들이 최신의 DDoS공격 및 방어기술을 습득할 수 있는 교육에 참가할 수 있도록 한다.

3) IPS(Intrusion Prevention System) 네트워크 트래픽을 검사하여 악성코드나 유해트래픽 등 비정상적 공격 트래픽을 막아주는 보안장비

4. 유관기관과 협력체제 강화

○ 국가사이버안전센터, 통신사업자(ISP) 등 유관기관과 협력체제를 강화하여 공격 발생 시 효과적인 대응을 위한 방안을 마련한다.

Ⅳ DDoS공격 대응활동

1. DDoS공격 대응 개요

○ 담당실무자는 대응절차 및 요령을 숙지하고, 평시 운영장비 모니터링 중 이상 징후를 인지하는 경우에는 정보보호담당실무자에 통보하여 초동조치 등 DDoS공격에 적절히 대응할 수 있도록 하여야 한다.

○ 정보보호담당실무자는 DDoS공격 발생 시 신속한 대응조치를 위하여 담당실무자와 협조하여 운영장비에 맞는 기술대응절차서를 작성·구비하여야 하며, 항상 최신상태로 유지하여야 한다.

2. DDoS공격 대응절차

DDoS공격에 대한 대응절차는 다음과 같이 정의한다.

1단계(모니터링)	2단계(공격탐지)	3단계(초동조치)	4단계(상세분석)	5단계(차단조치)
• 네트워크 부하량 • 보안장비 차단 및 탐지 로그 • 보안장비 시스템 부하량 • 서버 자원사용량	• 네트워크 공격탐지 기준 초과 • 보안장비 공격탐지 기준 초과 • 서버 공격탐지기준 초과	• 정보보호책임관 통보 • ISP, 유지보수업체 협조 • 유관기관 통보 • 초동조치	• 장비 상태확인 및 정보 수집 • 공격기법, 사고원인분석 • 피해범위 파악 • 공격현황 보고서 작성 • 차단조치방안 수립	• 공격유형별 조치 • 네트워크 차단조치 설정 • 보안장비 차단조치 설정 • 서버 차단조치 설정

가. 1단계 : 모니터링

○ 담당실무자는 DDoS공격징후 인지를 위하여 운영장비의 부하량, 차단·탐지로그, 자원사용량 등을 지속적으로 모니터링하며, 평시 및 선거 시 장비 설정치와 임계치 설정에 필요한 기준자료를 관리하여야 한다.

○ 정보보호담당실무자는 장비별 담당실무자 및 유지·보수업체와 협의하여 평시 및 선거 시 확보한 기준자료를 반영한 DDoS공격탐지지표(별지서식3 참조)를 작성하고, 이를 DDoS공격 여부를 판단하는 데 활용한다.

○ 운영장비는 항상 최신 버전으로 유지될 수 있도록 보안패치 및 업데이트를 적용하며, 최신 공격기법에 대한 차단정책을 반영하여야 한다.

나. 2단계 : 공격탐지

○ 담당실무자는 운영장비 모니터링 중 네트워크 트래픽, 보안장비 차단량, 서버 자원사용량, 통신세션수, 홈페이지 응답시간 등이 평소와 현저히 다르게 급격히 증가하는 등 DDoS공격으로 의심되는 상황이 발생하면, 즉시 정보보호담당실무자에게 통보하여야 한다.

○ 정보보호담당실무자는 장비별 담당실무자와 협의를 통해 DDoS공격 탐지지표 및 전체 상황을 분석·종합하여 공격탐지 여부를 결정하고 정보보호책임관 또는 정보보호책임자에게 보고하며, 초동조치를 수행한다.

○ DDoS공격으로 결정되지 않고 일시적인 사용량 증가 및 시스템 문제 또는 오탐으로 판명될 경우에는 모니터링 단계로 전환한다.

다. 3단계 : 초동조치

○ DDoS공격으로 판명되면, 정보보호담당실무자는 기술대응절차서에 따라 장비별 담당실무자로 하여금 피해규모를 최소화하기 위하여 공격IP주소 차단, 장비 임계치 조정 등 기본조치를 수행하도록 한다.

○ 정보보호담당실무자는 초동조치 수행 후, 국가사이버안전센터 및 통신사업자(ISP) 등 유관기관과 유지·보수업체 등에 통보하여 필요 시 다음과 같은 공격대응을 위한 협조를 요청하여야 한다.

- 유관기관에 파악된 공격사례를 신속히 전파하여 피해확산 방지조치
- 통신사업자에 공격IP주소 중 해외IP주소에 대한 차단요청 및 일시적 네트워크 대역폭 확대조치
- 유지·보수업체에 전문기술요원 파견 조치

○ 정보보호담당실무자는 DDoS공격에 의한 피해확산 여부를 지속적으로 모니터링하며, 피해발생 장비를 파악하고 공격유형을 식별하는 등 상세분석을 위한 정보를 수집하여야 한다.

라. 4단계 : 상세분석

○ 정보보호담당실무자는 장비별 담당실무자와 장비상태를 확인하고 수집된 공격 관련 정보를 분석하여 공격기법 식별 및 원인, 피해범위를 파악한다.

○ 정보보호담당실무자는 장비별 담당실무자와 DDoS공격탐지지표를 참조하여 장비 설정 변경 및 별도 대응조치 등 차단조치 방안을 수립하고, 다음의 내용이 포함된 공격분석보고서를 작성한다.

- DDoS공격 시 발생한 장비 로그 및 트래픽 분석결과
- DDoS공격 IP주소 및 트래픽 유발 IP주소 목록

마. 5단계 : 차단조치

○ 정보보호담당실무자는 수립된 차단조치 방안 및 기술대응절차서를 이용하여 장비별 담당실무자와 각 장비의 설정을 변경하고, URL Redirection[4] 등 사전 준비된 별도 대응조치와 함께 차단조치를 수행하여야 한다.

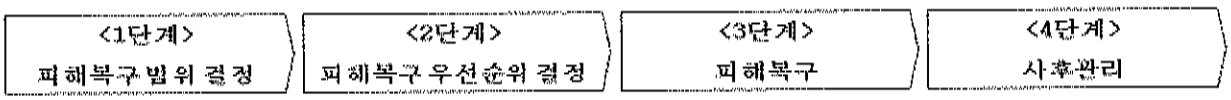
○ 정보보호담당실무자는 DDoS공격 차단조치 수행 후, 모니터링을 통해 공격차단 성공여부를 확인하여 공격이 진화되고 소강상태에 들었다고 판단되면, 유관기관에 통보하고 피해복구절차를 수행하여야 한다.

○ 정보보호담당실무자는 DDoS공격 차단조치 수행 후에도 공격이 완화되지 않을 경우 유관기관에 재협조 요청하고, DDoS공격탐지지표에 대한 상세분석과 차단조치를 반복적으로 수행하여야 한다.

○ 정보보호담당실무자는 DDoS공격에 대한 지속적 차단조치에도 불구하고 피해범위가 계속 확산되고 방어조치가 원활히 이루어지지 않는다고 판단되면, 정보보호책임관 및 정보보호책임자에게 보고하고 네트워크 케이블의 일시단절 및 서버 재부팅 등 강력한 대응조치를 수행할 수 있다.

V 피해복구 및 사후조치

정보보호책임관 및 정보보호책임자는 DDoS공격이 진화되면 네트워크 등 정보시스템서비스의 정상화를 위하여 다음과 같이 피해복구절차를 수행하고, 사고 재발 방지대책을 수립하여야 한다.



1. 피해복구 범위결정

○ 정보보호담당실무자는 DDoS공격에 의한 장비별 피해현황을 종합 분석하여 피해수준을 산정하고 피해복구범위를 결정하여야 한다.

○ 피해복구범위는 장비별 담당실무자와 협의하되, 복구형태에 따라 다음과 같이 구분하여 결정한다.

4) DDoS공격 대응 기술적 조치 중 하나로 공격대상 목적지 URL을 재지정한 다른 목적지로 수정하여 정상 접속을 유도하는 방어기법.

- 단순데이터 복구 : 피해사고가 발생한 시스템의 데이터만 손상된 경우
- 소프트웨어 복구 : 피해사고가 발생한 시스템의 프로그램 및 운영체제에 대한 단순오류가 발생한 경우
- 시스템 재설치 : 피해사고가 발생한 시스템의 운영체제에 복구가 불가능한 심각한 오류가 발생한 경우
- 하드웨어 교체 : 피해사고가 발생한 시스템의 하드웨어 손실이 발생한 경우

2. 피해복구 우선순위 결정

○ 정보보호담당실무자는 피해복구범위와 우선순위를 결정하는 경우 정보시스템서비스에 영향이 없도록 서버 등 장비 운영상황을 확인하여야 한다.

○ 피해복구범위가 정해지면, 복구수행이 정보시스템서비스에 미치는 영향을 충분히 검토한 후, 다음 사항을 고려하여 복구우선순위를 결정하여야 한다.

- 서버 등 운영 장비의 중요도
- 즉시조치 또는 중장기적 계획에 따라 수행할 복구내용

3. 피해복구

○ 장비별 담당실무자는 서버 등 장비가 정상적으로 운영될 수 있도록 복구형태에 따라 다음과 같이 복구를 수행한다.

- 단순데이터 복구 : DB서버 등 데이터 처리가 주된 장비의 데이터 손실 및 훼손이 발생한 경우, 백업데이터를 이용하여 복구 수행
- 소프트웨어 복구 : 웹서버 등 응용프로그램의 비정상 동작 시 프로그램 재설치, 최신 보안패치 적용 및 복구프로그램으로 정상 복원 수행
- 시스템 재설치 : 시스템 자체 오류 발생 시 운영체제 및 응용프로그램 재설치, 데이터 복원 등 전체 시스템 재설치 복구
- 하드웨어 교체 : 소프트웨어적 복구 수행 후에도 장비가 정상적으로 동작하지 않을 경우에는 하드웨어 장비 또는 부품 교체 복구

○ 정보보호담당실무자는 피해복구가 완료된 후, 전반적인 정보시스템서비스의 정상동작 여부를 최종 점검하여야 한다.

4. 사후관리

○ 장비별 담당실무자는 피해복구 수행 후 일정기간 동안 운영장비에 대한 정상동작 여부를 충분히 모니터링하여야 한다.

○ 장비별 담당실무자는 사고에 대비하여 평시 운영장비 환경설정값 백업, 데이터 및 응용프로그램 백업, 운영체제 등 시스템소프트웨어CD 등의 상태를 주기적으로 점검하여야 한다.

○ 정보보호담당실무자는 피해복구내용 및 보안강화방안 등에 대한 보고서를 작성하고, 장비 설정치와 임계치 설정에 필요한 기준자료를 재검토하여 DDoS공격탐지지표를 정비하여야 한다.

Ⅵ 보 칙

1. DDoS공격 대응보고

○ DDoS공격에 대한 조치가 종료된 후, 정보보호책임관 또는 정보보호책임자는 규정 제39조제3항에 따라 최종상황보고(별지서식4 참조)를 하여야 한다.

※ 별지서식 4 'DDoS공격 상황보고' 서식

2. DDoS공격 대응 관련 작성자료의 현행화 및 보안관리

○ 정보보호담당실무자는 DDoS공격 대응장비 등 주요 장비에 대한 DDoS 공격 기술대응절차서를 작성하고, 본 지침 별지서식의 비상연락망, 구성 장비목록, 공격탐지지표 등과 함께 상시 현행화 관리하여야 한다.

○ 담당실무자는 DDoS공격 대응과 관련하여 작성한 기술대응절차서 등 각종 자료가 외부에 유출되지 않도록 대외비에 준하여 관리하여야 한다.

3. 위탁운영업체에 대한 보칙

○ 위원회 홈페이지 등 정보시스템서비스를 위탁운영하는 경우에 DDoS공격 등 사이버공격에 대한 대응은 위탁운영업체의 자체규정에 따른다. 다만, 자체규정이 불비한 경우에는 본 지침을 준용하도록 한다.

○ 정보보호책임자는 위원회 정보시스템서비스의 위탁운영계약 시 DDoS공격 등 사이버공격에 대한 대책을 명시하도록 지도한다.

○ 정보보호책임자는 위탁운영하는 홈페이지 등 정보시스템서비스에 대한 DDoS공격 등 사이버공격으로 피해가 발생한 경우에는 정보보호책임관에게 통보하여야 한다.

【별지서식 1】

DDoS공격 대응 담당자 비상연락망

(※ 해당사항만 기재 작성)

□ ○○선거관리위원회

직책	부서명	성명	직위(급)	연락수단	연락처
정보보호책임관 (정보보호책임자)				전 화	
				핸드폰	
				이메일	
정보보호담당 실무자				전 화	
				핸드폰	
				이메일	
보안장비담당 실무자				전 화	
				핸드폰	
				이메일	
네트워크담당 실무자				전 화	
				핸드폰	
				이메일	
서버담당 실무자				전 화	
				핸드폰	
				이메일	
홈페이지담당 실무자				전 화	
				핸드폰	
				이메일	

□ 유지 · 보수업체/위탁운영업체

구 분	업체명	성명	직위(급)	연락수단	연락처
총괄책임자				전 화	
				핸드폰	
				이메일	
보안장비담당				전 화	
				핸드폰	
				이메일	
네트워크담당				전 화	
				핸드폰	
				이메일	
서버담당				전 화	
				핸드폰	
				이메일	
홈페이지담당				전 화	
				핸드폰	
				이메일	

□ 유관기관 및 통신사업자

(※ 유관기관은 수정·작성하지 않음)

구 분	기관명	성명	직위(급)	연락수단	연락처
유관기관	국가사이버안전센터	-	-	전 화	국번없이 111
				이메일	info@ncsc.go.kr
				홈페이지	www.ncsc.go.kr
	한국인터넷진흥원 인터넷침해대응센터	-	-	전 화	02-118
				이메일	cert@krcert.or.kr
				홈페이지	www.krcert.or.kr
	경찰청 사이버테러대응센터	-	-	전 화	02-3939-112
				이메일	cyber112@npa.go.kr
				홈페이지	www.ctrc.go.kr
통신사업자 (ISP)				전 화	
				핸드폰	
				이메일	
				전 화	
				핸드폰	
				이메일	

【별지서식 2】

DDoS공격 대응 정보시스템 구성장비 목록

(※ 서식 구분 및 함목은 실정에 맞게 적절히 조정하여 작성)

□ 보안장비

구 분 (설치년도)	규격 및 성능	수량	IP주소	관리콘솔
DDoS 대응장비 (년)	-제조사 및 모델: -동시세션: -CPU : -Mem: -HDD: -NIC :			-제조사(설치년도): -모델명: -IP주소:
침입방지 (IPS) (년)	-제조사 및 모델: -동시세션: -CPU : -Mem: -HDD: -NIC :			-제조사(설치년도): -모델명: -IP주소:
방화벽 (Firewall) (년)	-제조사 및 모델: -동시세션: -CPU : -Mem: -HDD: -NIC :			-제조사(설치년도): -모델명: -IP주소:
침입탐지 (IDS) (년)	-제조사 및 모델: -동시세션: -CPU : -Mem: -HDD: -NIC :			-제조사(설치년도): -모델명: -IP주소:
웹방화벽 (년)	-제조사 및 모델: -동시세션: -CPU : -Mem: -HDD: -NIC :			-제조사(설치년도): -모델명: -IP주소:

□ 네트워크장비

구 분 (설치년도)	규격 및 성능	포트수	수량	IP주소
라우터 (　　년)	-제조사 및 모델: -처리성능: -CPU : -Mem:			
L4스위치 (　　년)	-제조사 및 모델: -처리성능: -CPU : -Mem:			
L3/L2스위치 (　　년)	-제조사 및 모델: -처리성능: -CPU : -Mem:			

□ 서버장비

구 분 (설치년도)	규격 및 성능	호스트명	IP주소	시스템용도
웹서버 (　　년)	-제조사 및 모델: -운영체제: -CPU : -HDD: -Mem: -NIC :			
WAS서버 (　　년)	-제조사 및 모델: -운영체제: -CPU : -HDD: -Mem: -NIC :			
DB서버 (　　년)	-제조사 및 모델: -운영체제: -CPU : -HDD: -Mem: -NIC :			
스토리지 (　　년)	-제조사 및 모델: -HDD: -저장용량 :			

□ 홈페이지

홈페이지명	홈페이지 주소(URL)	서비스 웹서버명	서비스 IP주소

【별지서식 3】

DDoS공격 탐지지표

구 분	장비종류	탐지지표	항목	사용량		공격탐지 기준
				평상시	선거시	
네트워크	라우터·스위치	트래픽 사용량	평균	Mbps	Mbps	사용량 급격히 증가
			최고	Mbps	Mbps	
		CPU 사용량	평균	%	%	사용량 급격히 증가
			최고	%	%	
		메모리 사용량	평균	%	%	사용량 급격히 증가
			최고	%	%	
		패킷 수	평균	pps	pps	패킷 수 급격히 증가
			최고	pps	pps	
보안정비	DDoS 대응장비	차단 트래픽량	평균	Mbps	Mbps	차단량 급격히 증가
			최고	Mbps	Mbps	
		IP주소별 연결요청 수	임계치	SYN패킷 /sec	SYN패킷 /sec	임계치 초과
		IP주소별 세션수	임계치	세션/sec	세션/sec	임계치 초과
		IP주소별 패킷수	임계치	패킷/sec	패킷/sec	임계치 초과
	IPS	차단 트래픽량	평균	Mbps	Mbps	차단량 급격히 증가
			최고	Mbps	Mbps	
		CPU 사용량	평균	%	%	사용량 급격히 증가
			최고	%	%	
		세션 수	평균	세션/sec	세션/sec	세션 수 급격히 증가
			최고	세션/sec	세션/sec	
	방화벽	CPU 사용량	평균	%	%	사용량 급격히 증가
			최고	%	%	
		메모리 사용량	평균	%	%	사용량 급격히 증가
			최고	%	%	
		세션 수	평균	세션/sec	세션/sec	세션 수 급격히 증가
			최고	세션/sec	세션/sec	
서버	웹서버, DB서버	트래픽 사용량	평균	Mbps	Mbps	사용량 급격히 증가
			최고	Mbps	Mbps	
		CPU 사용량	평균	%	%	사용량 급격히 증가
			최고	%	%	
		세션 수	평균	세션/sec	세션/sec	세션 수 급격히 증가
			최고	세션/sec	세션/sec	
		응답시간	평균	msec	msec	응답시간 급격히 증가
			최고	msec	msec	

※ 선거시 사용량은 전국선거와 재·보궐선거로 구분하여 작성

【별지서식 4】

DDoS공격 상황보고

기 관 정 보						
위원회명				부 서		
성 명				직위(급)		
연 락 처	전 화		핸드폰		팩스	
	이메일					
사 고 내 용						
발생일시	년 월 일 시 분부터 월 일 시 분까지					
사고원인	* DDoS공격유형, 트래픽, 공격IP주소 등 주요 공격지표 작성					
피해내용	* DDoS공격으로 인한 피해내용 및 피해시스템 수량 작성					
조 치 내 용						
조치경과	* 시간대별 주요조치사항 요약 작성					
조치사항	* 자체긴급조치 및 피해복구, 유관기관 협조사항 등 요약 작성					
조치결과	* 사고대응 조치 후 상황 요약 작성					
조 치 자	* 대응조치 참여인력(위원회, 유지·보수업체, 유관기관 포함) 현황 작성					
기 타 사 항						
재발방지 대 책	* 상황종료 후 공격대응 관련 미비점, 보완사항 등 개선대책 기술					
특이사항						

【별첨】

DDoS공격 징후발생 시 긴급대응요령

1단계 DDoS공격 징후탐지

○ 서비스 응답시간 급증
- 평시 응답시간에 비해 급증하거나 증가 추세인 경우

○ BPS(Bits per second), PPS(Packets per second) 값 급증
- 라우터 및 스위치 장비 모니터링
- 평균 트래픽과 비교하여 BPS, PPS가 급증한 경우

○ 유입 BPS, PPS 임계치 초과
- 서버에서 처리할 수 있는 대역폭 이상의 트래픽 유입
- DDoS대응장비, IPS에서 임계치 초과 경고

○ 트래픽 모니터링 결과 차단 트래픽량 급증
- DDoS대응장비, IPS에서 모니터링

○ 동시 세션 개수의 변화
- DDoS대응장비, IPS, 웹서버 대상 실시간 모니터링

○ 웹서버 로그 모니터링
- 특정 페이지에 대한 요청 급증 및 CPU/Memory 사용률 급증

2단계 초동조치

○ 긴급 대응반 가동
- 비상연락망을 통해 상황을 전파하고 각 장비 담당자 대응 시작

○ 유관기관 및 유지·보수업체 통보 및 협조
- 유지·보수업체에 통보하고 협조 요청
- 국가사이버안전센터 및 통신사업자(ISP) 등 유관기관에 상황 통보

○ 네트워크장비 조치
- 해외 IP주소 및 스푸핑된 IP주소 Null 라우팅 처리
- 공격 의심 IP주소 및 네트워크 주소 접근차단 조치(ACL 이용)

○ 보안장비 조치
- 트래픽 차단 임계치를 낮추고 상태 모니터링
  ※ 네트워크 트래픽 bps/pps, 연결된 TCP pps/session, 소스 IP주소별 Syn패킷 개수, HTTP요청 개수
- DDoS대응장비 및 IPS 등에 최신 차단정책 적용

○ 서버장비 조치

- 자원사용 임계치를 조정하고 상태 모니터링
- 미연결 상태 허용 임계치는 상향 조정

※ TcpMaxHalfOpen(Windows), tcp_conn_req_max_q0(Solaris) 등

- 연결 유지 및 SYN+ACK 패킷 재전송 간격 등은 하향 조정

※ KeepAliveTime(Windows), tcp_rexmit_interval_max(Solaris) 등

3단계 분석 및 차단조치

○ 장비상태 확인 및 공격유형 분석

- 웹서버 등 정상 동작 확인
- 공격 IP주소, 공격기법 및 패턴 추출

○ 피해 완화대책 가동

- URL Redirection 등 사전 준비된 피해 완화대책 가동
- ISP와 협조하여 IP주소 차단, 대역폭 증설 등 수행

○ 공격이 지속되거나 심화될 경우 장비별 임계치 강화

- 네트워크장비에서 IP주소 차단조치(분석결과 반영)
- 보안장비 임계치 설정 강화 및 분석결과 탐지정책 적용

※ 네트워크 트래픽 bps/pps, 연결된 TCP pps/session, 소스 IP주소별 Syn패킷 개수, HTTP요청 개수

- 서버 자원 관련 임계치 강화

※ TcpMaxHalfOpen(Windows), tcp_conn_req_max_q0(Solaris) 등

※ KeepAliveTime(Windows), tcp_rexmit_interval_max(Solaris) 등

4단계 복구 및 정상화

○ DDoS공격 트래픽이 지속될 경우

- DDoS대응반 지속 가동
- 장비 임계치 설정을 유지하고 피해 완화대책 지속 가동

○ DDoS공격 트래픽이 미탐지 또는 극소량으로 감소될 경우

- 장비 임계치 설정 단계적으로 완화

○ 피해장비 복구 수행

- 피해 발생 전 단계로 장비 설정 등 복구

○ 상황결과 보고 및 유관기관 통보

- 대응조치 완료 후 DDoS공격 상황결과보고서 작성·보고
- 국가사이버안전센터 등 유관기관 상황종료 통보