

<부분>

비공개처분취소 행정심판청구 답변서

2012. 03.



중앙선거관리위원회

(정보화담당관실)

2012. 3. 26

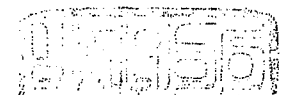
답 변 서

사 건 중앙행심 2012-15호 정보비공개결정취소등청구
청 구 인 명 광 복
피청구인 중앙선거관리위원회위원장

위 사건에 관하여 피청구인은 아래와 같이 답변합니다.

청구취지에 대한 답변

1. 주위적으로, 청구인의 청구를 각하한다.
 2. 예비적으로, 청구인의 청구를 기각한다.
- 라는 재결을 구합니다.



청구원인에 대한 답변

1. 이 사건 경위

가. 청구인은 2011. 12. 23. 피청구인에게 2011. 10. 26. 발생한 중앙선거관리위원회 홈페이지 대상 디도스 공격과 관련하여 선관위와 공급업체간 재발방지 및 원인규명을 위한 자료에 대해 정보공개 청구를 하였습니다.

나. 피청구인은 이에 대해 「공공기관의 정보공개에 관한 법률 (이하 '정보공개법'이라 한다) 및 「통신비밀보호법」에 따라 비공개를 결정하고 그 결정통지서를 2011. 12. 27. 청구인에게 통지하였습니다.

다. 이에 청구인은 2012. 1. 27. 피청구인이 비공개 결정한 것에 대하여 이의를 신청하였습니다.

라. 피청구인은 정보공개 대상이 되는 정보에 대해 공개여부를 결정하기 위하여 청구인의 주장대로 피청구인의 소유인 정보시스템에 대한 분석 자료인 LG엔시스의 분석보고서에 대해서는 공개를 결정하고, 피청구인이 임대한 회선에 대한 자료는 제3자의 정보에 해당하는 정보가 포함되어 있어 「정보공개법」 제11조(정보공개여부의 결정)제3항에 의거 정보제공자(KT, LG U+ 이하 "통신사")의 의견을 청취하고자 제18조제2항에 의거 청구인에게 연장사유를 통지하고 통신사의 의견을 청취하였습니다.

유심당인의

마. 청취결과 KT가 제공한 자료는 검찰조사 목적으로 제출된 자료이며, 네트워크 장비의 공인 IP주소와 네트워크 구성도 등 기업보안에 해당하는 자료 등이 다수 포함되어 있어 외부공개가 불가하다는 회신(2012. 2. 10.)이 있었으며, LG U+가 제공한 자료는 다른 고객의 IP자료에 대해서는 삭제한 후 공개가 가능하

다는 회신(2012. 2. 10.)이 있었습니다.

바. 따라서 피청구인은 통신사 의견의 일부를 인용하고, 통신사의 정보는 피청구인의 정보시스템에 연결되어 운영되었던 정보뿐만이 아닌 통신사의 영업 기밀에 해당되는 공인 IP주소 등이 포함되어 있어 「정보공개법」 제9조 제1항 제7호에 의거 비공개 하는 것이 마땅하여 비공개 결정을 하고, 2012. 3. 11. LG엔시스의 분석보고서만을 공개하는 것으로 하는 부분공개 결정사항을 청구인에게 통지하였습니다.

사. 청구인은 자료수령 후 피청구인의 '온라인 선거관리시스템을 공급한 업체들 간의 사태 재발 방지와 원인규명 논의자료에 관한 정보공개'를 요구하는 행정심판을 제기하였습니다.

2. 청구인의 '법률상 이익' 소멸



가. 청구인은 2012. 3. 2. 행정심판을 청구한 내용과 동일한 취지의 정보공개를 청구하였고(을 제1호증), 피청구인은 청구인이 공개를 요구한 정보에 대해 통신사로부터 제공받은 정보 중 로그기록에 대하여는 「정보공개법」 제9조 제1항 제2호에 따라 통신사의 영업비밀에 관한 자료는 「정보공개법」 제9조 제1항 제7호에 따라 비공개하고, 나머지 부분을 공개하는 결정을 하여 2012. 3. 12. 청구인에

게 통지하였습니다(을 제2호증).

나. 결국 피청구인이 청구인에 대하여 이 사건 정보를 이미 공개하였으므로, 청구인은 이 사건 정보 공개를 다들 법률상 이익이 없다고 할 것입니다.

다. 「행정심판법」 제13조 제1항은 “취소심판은 처분의 취소 또는 변경을 구할 법률상 이익이 있는 자가 청구할 수 있다”고 규정하고 있는바 청구인은 취소를 구할 법률상 이익이 없어 청구인 적격이 없다고 할 것입니다. 따라서 청구인의 청구는 청구인 적격이 없는 자가 제기한 것으로 부적법하여 각하되어야 할 것입니다.

3. 이 사건 처분의 적법성

설사 청구인의 청구가 적법하다 하더라도 피청구인의 처분은 다음과 같은 이유로 적법하다 할 것입니다.

가. 「정보공개법」 제9조의 비공개 사유의 존재

1) 비공개한 정보의 범위

2012. 3. 2. 정보공개한 부분을 제외한 나머지 부분은 청구인인 청구 당시 제외한 개인정보 사항을 제외하면, (ㄱ)로그기록 및 (ㄴ)기업의 영업상 비밀에 해당하는 자료에 해당합니다.

2) 비공개 사유

로그기록은 정보보호시스템 및 정보통신망 구성도와 관련된 자료로 「정보공개법」 제9조 제1항 제2호의 국가안전보장에 관한 사항으로서 공개될 경우 중대한 이익을 현저히 해할 우려가 있다고 인정되는 정보에 해당하며, 통신사의 IP 주소 등은 「정보공개법」 제9조 제1항 제2호의 법인의 경영·영업상 비밀에 관한 사항으로서 공개될 경우 법인 등의 정당한 이익을 현저히 해할 우려가 있다고 인정되는 정보에 해당하여 비공개대상정보에 해당한다 할 것입니다. 이와 관련하여 피청구인은 정보공개편람을 통해 비공개대상정보 세부기준을 마련하고 있는바, 이들 정보는 모두 정보공개편람 상의 비공개대상정보에 해당한다 할 것입니다(을 제3호증)

나. 처분 근거 법령의 추가·변경

피청구인이 청구인에게 이 사건 정보공개 통지 및 2012. 3. 12. 정보공개 통지 당시 처분 근거 법령을 정확하게 표시하지 않은 잘못은 있으나, 처분청이 처분 당시에 적시한 구체적 사실을 변경하지 아니하는 범위 내에서 단지 그 처분의 근거 법령만을 추가·변경하거나 당초의 처분사유를 구체적으로 표시하는 것에 불과한 경우에는 새로운 처분사유를 추가하거나 변경하는 것이라고 볼 수 없다는 판례(대법원 2008. 2. 28. 선고 2007두13791,13807)에 따르면 이 사건 정보공개 청구와 관련하여 처분의 근거 법령을 추가·변경하는 것은 처분사유를 추가하거나 변경하는 것이라 할 수 없고, 위법하지도 않다 할 것입니다.

다. 소결

청구인의 청구가 적법하다 하더라도, 피청구인이 비공개한 정보는 「정보공개법」 제9조의 비공개대상정보에 해당하므로 피청구인의 처분이 부적법하다는 청구인의 주장은 이유가 없습니다.

4. 결 론

청구인의 청구한 정보에 대하여 피청구인이 이미 공개를 하였으므로 청구인의 청구는 법률상 이익이 없는 자가 청구한 것으로 부적법합니다. 설사 청구인의 청구가 적법하다 하더라도 피청구인이 비공개한 정보는 「정보공개법」 제9조의 비공개대상정보에 해당하므로 피청구인의 처분은 적법하다 할 것입니다.

입 증 방 법

1. 을 제1호증(2012. 2. 29. 정보공개청구서)
2. 을 제2호증(2012. 3. 12. 정보공개결정통지서)
3. 을 제3호증(선거관리위원회 정보공개편람 45면~55면)



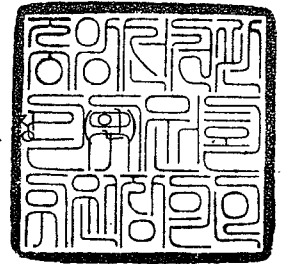
첨 부 서 류

1. 위 입증방법 각 2통

2. 답변서 부분 1통

2012. 3.

중앙선거관리위원회 위원장



중앙선거관리위원회사무처행정심판위원회 귀중



[첨부 1]

을 제1호증

정보공개청구서 1부



정보 공개 청구서

접수번호

2012-5155

접수일

2012년 02월 29일

성명(단체명 및 대표자 성명)
명광복
주소(소재지)
청구인 (110 - 043) 서울 종로구 통인동 132번지 5층
행정감시센터
전화번호
02-723-4251

주민등록(여권, 외국인등록)번호

710815-*****

사업자(법인, 단체)등록번호

전자우편주소

elle@pspd.org

노고에 수고가 많으십니다.
다음 각 사항을 정보공개청구합니다.

청구 내용

1. 중앙선거관리위원회에서 2011. 3월 제정 운영중인 메뉴얼 <분산서비스거부 공격 대응지침>문서 전문
2. 위 1 <분산서비스거부 공격 대응지침>중 언급되는<기술대응절차서>문서 전문
3. 협력업체 보고서 외에 회선/하드웨어/소프트웨어 협력 업체들이 선관위 인터넷 장애 사태 이후 제공한, 혹은 선관위 자체 조사로 파악한 유입트래픽 추이, 라우터 상태 및 접근기록 등 기초 데이터 일체(ip주소 등 블라인드처리 가능)

공개 형태 ☐ 열람, 시청 ☐ 사본, 출력물 ☒ 전자파일 ☐ 복제, 인화물
수령 방법 ☐ 직접방문 ☐ 우편 ☐ 팩스전송 ☒ 전자우편 ☐ 기타()

유법영인인

수수료 ☒ 감면 대상임

☐ 감면 대상 아님

감면 사유 선거관리위원회정보공개규칙 제17조제3항의 규정에 의하여 수수료 감면대상

「공공기관의정보공개에관한법률」 제10조제1항 및 「선거관리위원회정보공개규칙」 제4조에 따라 위와 같이 정보의 공개를 청구합니다.

2012년 02월 29일

청구인

명광복

(서명 또는 인)

(중앙선거관리위원회) 귀중

유의사항

수수료 감면 사유란 「선거관리위원회정보공개규칙」 제17조제3항의 규정에 의하여 수수료 감면 대상에 해당하는 경우에
기타하여, 감면 사유를 증명할 수 있는 서류를 첨부하시기 바랍니다.

[첨부 2]

을 제2호증

정보공개결정통지서 1부
정보공개자료 1부



“깨끗한 선거 대한민국의 얼굴입니다”



중앙선거관리위원회

수신자 명광복(elle@pspd.org/서울 종로구)

(경유)

제목 정보(공개) 결정 통지

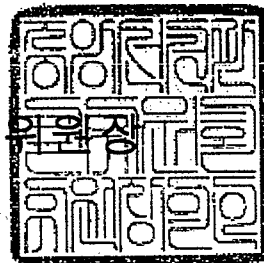
귀하의 정보공개 청구에 대한 결정 내용을 「공공기관의 정보공개에 관한 법률」 제13조제1항 및 제4항에 따라 붙임과 같이 결정 통지합니다.

붙임 1. 정보(공개) 결정 통지서 1부.

2. 유의사항 1부. 끝.



중앙선거관리위원회



★주무관

장병호

전산사무관

유훈옥

정보화담당관

전결 03/11
박혁진

협조자

시행 정보화담당관-891

(2012.03.11.) 접수

우 151-800 서울 관악구 남현동 1064-7 (2층 201호)

/ <http://nec.go.kr>

전화 (02)581-7616

/전송 (02)504-3454

/ hojang@nec.go.kr

/ 비공개(6)

[붙임1]

정보 ([]공개 []부분공개 []비공개) 결정 통지서

수신자 명광복 (110-043, 서울 종로구 통인동 132번지 5층 행정감시센터)

접수번호 2012-5155

접수일 2012년 02월 29일

청구 내용	1. 중앙선거관리위원회에서 2011. 3월 제정 운영중인 매뉴얼 <분산서비스거부 공격 대응지침> 문서 전문 2. 위 1 <분산서비스거부 공격 대응지침>중 언급되는 <기술대응절차서>문서 전문 3. 협력업체 보고서 외에 회선/하드웨어/소프트웨어 협력 업체들이 선관위 인터넷 장애 사태 이후 제공한, 혹은 선관위 자체 조사로 파악한 유입트래픽 추이, 라우터 상태 및 접근기록 등 기초 데이터 일체		
공개 내용	본 기관에서 직무상 보유·관리하고 있는 자료 중 귀하께서 요청하신 정보와 일치한 자료내역은 다음과 같습니다. - 분산서비스거부(DDoS)공격 대응지침 1부 - 협력업체 제공자료 2부 다만, 상기 청구내용 중 2번의 기술대응절차서는 문서 부존재(작성예정인 정보)로 공개 내용에서 제외함		
공개 일시	2012년 03월 12일	공개 장소	
공개 방법	☐ 열람·시청 ☐ 사본·출력물 ☒ 전자파일 ☐ 복제·인화물 ☐ 기타		
수령 방법	☐ 직접방문 ☐ 우편 ☐ 팩스전송 ☒ 정보통신망 ☐ 기타		
비공개(전부 또는 일부) 내용 및 사유	【비공개 정보】 해당사항없음		

귀하의 정보공개 청구에 대한 결정 내용을 「공공기관의 정보공개에 관한 법률」 제13조제1항 및 제4항에 따라 위와 같이 결정 통지합니다.

2012년 03월 11일



수신처: 중앙선거관리위원회 위원장

시행일자: 2011.11.01

보 기: 정보화담당관

재 목: 중앙선거관리위원회 홈페이지 접속장애 조치내역 송부

1. 관련

가. 정보화담당관-2344 ('11.9.29) 하반기 재보궐선거 관련 통신회선 증속 및 정보통신망 운영 협조요청

2. 귀 위원회의 무궁한 발전을 기원합니다.

3. 위 관련 2011. 10.26일 실시한 하반기 재보궐선거 관련 중앙선거관리위원회 홈페이지 접속장애 발생건에 대한 조치내역을 아래와 같이 송부하오니 관련 업무에 참조하시기 바랍니다.

가. 장애내역 : 중앙선거관리위원회 홈페이지 접속장애

나. 발생일시 : 2011. 10.26 05:50 - 08:32

다. 발생원인

○ 중앙선거관리위원회 홈페이지 DDoS공격(1G)으로 접속불가

- DDoS공격 시간 : 2011. 10.26 05:50 ~ 11:20

○ 국내 250여개 IP에서 세션 및 대역폭 고갈 복합공격

라. 대응내역

○ 비정상트래픽 인지 후 공격자 IP차단

○ KT웹클린존 트래픽 우회 차단 후 홈페이지 정상(회복)

- KT 웹클린존 우회차단 (08:32)후 웹클린존에서 DDoS공격 차단하며 정상서비스 개시

○ 중앙선거관리위원회 회선 증설지원 (1G → 1회선, 155M → 2회선절체)

마. 홈페이지 접속불가원인 검토의견

○ 중앙선거관리위원회 총 대역폭 300Mbps 초과한 총 1G DDoS트래픽이 발생하여 퍼브넷 AR라우터에 병목현상 발생

○ AR라우터에서 1G트래픽이 비피킹되면서 중앙선거관리위원회로 300M 정도의 DDoS 트래픽이 지속적으로 발생되어 홈페이지 접속불가

바. 재발방지 대책(안)

○ 2012년 총선 및 대선관련 KT 웹클린존 도입검토 필요

○ 선관위 자체 DDoS 사이버 대응체계 구축 등 필요

붙임 : 1. 중앙선거관리위원회 홈페이지 접속장애 조치내역. 글.

주식회사케이티 Public고객본부



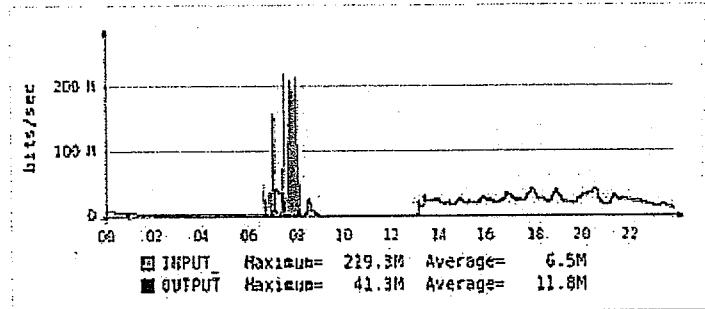
중앙선거관리위원회 (

속도 : 45.0 Mbps)

■ 장비정보

(at-0/1/0.0)

☐ 2011년 10월 26일 (수) 그래프



☐ 2011년 10월 26일 (Wed) 트리작표

시간	평균입력(bps)	입력비율(%)	평균출력(bps)	출력비율(%)
0 - 1	467,677	1.08	5,672,772	12.61
1 - 2	552,432	1.23	3,412,948	7.59
2 - 3	3,676	0.01	1,792,424	3.99
3 - 4	4,833	0.01	1,669,212	2.39
4 - 5	35,806	0.08	662,460	1.92
5 - 6	12,530	0.03	1,316,977	2.93
6 - 7	5,903,559	13.12	534,393	1.19
7 - 8	94,441,535	209.87	12,876,665	28.61
8 - 9	48,149,622	107.00	6,134,182	13.63
9 - 10	47	0.00	0	0.00
10 - 11	48	0.00	0	0.00
11 - 12	46	0.00	0	0.00
12 - 13	41	0.00	0	0.00
13 - 14	38,034	0.08	16,072,339	35.72
14 - 15	49,078	0.11	20,347,697	45.22
15 - 16	45,660	0.10	21,469,822	47.76
16 - 17	66,218	0.15	24,156,727	53.68
17 - 18	61,174	0.14	27,955,615	62.15
18 - 19	50,539	0.11	27,354,405	60.79
19 - 20	58,479	0.13	24,420,438	54.27
20 - 21	65,244	0.14	30,311,111	67.36
21 - 22	74,444	0.17	23,106,265	51.35
22 - 23	31,738	0.07	20,500,920	45.56
23 - 24	30,162	0.07	13,918,809	30.93
합 계	5,970,361	13.27	11,842,365	26.32

중앙선거관리위원회

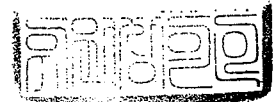
당사 DDos 탐지 시스템에서 탐지한 내역

ID	탐지시간	지속시간	공격대상	대상IP	타입	내용	원제 공격량		탐지량
							BP3	PP3	
000051	10-26 10:19:13	15분 0초	Others PUBNET/중앙 선거관리위원회	210.204.204.10	ICMP	39% (11.9 Kpps s/30.0 Kpps)	5.72M	11.92K	misuse
000055	10-26 08:51:13	12분 29초	Others PUBNET/중앙 선거관리위원 회/대전	210.204.204.10	ICMP	33% (10.0 Kpps s/30.0 Kpps)	4.0M	10K	misuse
000052	10-26 08:03:12	20분 0초	Others PUBNET/중앙 선거관리위원 회/대전	210.204.204.10	Bandwidth	93% (1.4 Gbps s/1.5 Gbps)	1.4G	39682K	misuse
000061	10-26 07:37:10	58분 2초	Others PUBNET/중앙 선거관리위원회	210.204.204.10	ICMP	145% (45.5 Kpps s/30.0 Kpps)	20.83M	495K	misuse
000066	10-26 07:37:10	58분 2초	Others PUBNET/중앙 선거관리위원회	210.204.204.10	UDP	104% (12.5 Kpps s/30.0 Kpps)	15.65M	182.83K	misuse
000005	10-26 07:04:11	14분 1초	Others PUBNET/중앙 선거관리위원회	210.204.204.10	UDP	259% (259.0 Kpps s/100.0 Kpps)	1.12G	259K	misuse
000007	10-26 07:04:11	14분 1초	Others PUBNET/중앙 선거관리위원회	210.204.204.10	ICMP	253% (76.0 Kpps s/30.0 Kpps)	36.43M	76K	misuse
000051	10-26 00:30:10	41분 2초	Others PUBNET/중앙 선거관리위원회	210.204.204.10	ICMP	123% (37.0 Kpps s/30.0 Kpps)	17.70M	37K	misuse
000058	10-26 05:52:11	57분 14초	Others PUBNET/중앙 선거관리위원회	210.204.204.10	ICMP	33% (10.2 Kpps s/30.0 Kpps)	4.68M	1017K	misuse
000470	10-26 00:59:13	12분 5초	Others PUBNET/중앙 선거관리위원회	210.204.204.10	ICMP	33% (10.0 Kpps s/30.0 Kpps)	4.3M	10K	misuse

※ DDos 발생 당시 DDos 탐지시스템에서 중앙선거관리위원회 IP로 공격이 감지된 자료임 (센플링에 의한 대략적인 수치임)

분산서비스거부(DDoS)공격 대응지침

2011. 3. 23.



중앙선거관리위원회

2010年10月10日 星期六

[illegible]

차 례

I. 총 칙	1
II. DDoS공격 대응체계	2
III. DDoS공격 예방활동	4
IV. DDoS공격 대응활동	5
V. 피해복구 및 사후조치	7
VI. 보 칙	9
[별지서식1] DDoS공격 대응 담당자 비상연락망	10
[별지서식2] DDoS공격 대응 정보시스템 구성장비목록	12
[별지서식3] DDoS공격 탐지지표	14
[별지서식4] DDoS공격 상황보고	15
[별첨] DDoS공격 징후발생 시 긴급대응요령	16

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

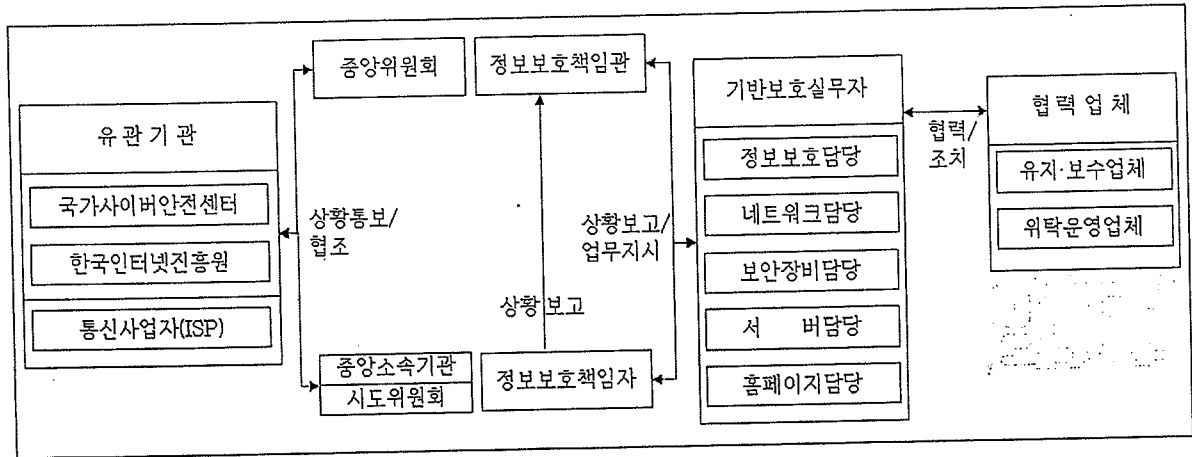
- "분산서비스거부공격"(이하 'DDoS'공격'이라 한다)이라 함은 인터넷 상에 분산되어 있는 다수의 악성코드 감염PC를 이용, 대량의 접속트래픽을 일시에 특정 사이트 또는 시스템에 전송하여 과부하를 유발시킴으로써 정상적인 정보시스템서비스를 할 수 없도록 하는 사이버공격을 말한다.
- "악성코드"라 함은 PC나 서버에 침투하여 피해를 입히는 소프트웨어를 가리키며 컴퓨터바이러스, 웜, 트로이목마, 스파이웨어 등을 포함한다.
- "좀비PC"(Zombie PC)라 함은 악성코드에 감염되어 PC이용자도 모르게 DDoS공격 등 사이버공격에 악용되는 일반 이용자 컴퓨터를 말한다.
- "봇넷"(Botnet)이라 함은 사이버공격자들에 의해 제어되는 명령제어서버(Command & Control 서버)와 좀비PC들의 집합 또는 네트워크를 말한다.

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(ISP²⁾) 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(IPS³⁾), 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 유해 사이트 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 Redirection⁴⁾ 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, DDoS공격탐지지도에 대한 상세 분석과 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.

<1단계> 피해복구 범위 결정	<2단계> 피해복구 우선순위 결정	<3단계> 피해복구	<4단계> 사후관리
---------------------	-----------------------	---------------	---------------

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 복구 형태에 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 DDoS공격 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 항목은 실정에 맞게 적절히 조정하여 작성)

□ 보안장비

구분 (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

구분 (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

구분 (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

DDoS공격 탐지지표

구 분	장비종류	탐지지표	항목	사용량		공격탐지 기준
				평상시	선거시	
네트 워크	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	
보안 정비	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

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	* DDoS 공격유형, 트래픽, 공격IP 주소 등 주요 공격지표 작성				
피해내용	* DDoS 공격으로 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
 - 평소 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

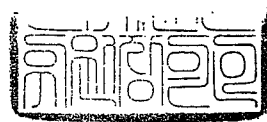
- 피해 발생 전 단계로 장비 설정 등 복구

○ 상황결과 보고 및 유관기관 통보

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

[첨부 3]

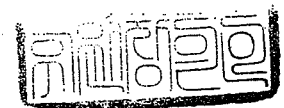
을 제3호증



선거관리위원회 정보공개편람 (45면 ~ 55면)

정 보 공 개 편 람

[제 9 조 비 공 개 대 상 정 보]



중앙선거관리위원회

라. 법 제8조

제8조 (정보목록의 작성·비치 등) ①공공기관은 당해기관이 보유·관리하는 정보에 대하여 국민이 쉽게 알 수 있도록 정보목록을 작성·비치하고, 그 목록을 정보통신망을 활용한 정보공개시스템 등을 통하여 공개하여야 한다. 다만, 정보목록중 제9조제1항의 규정에 의하여 공개하지 아니할 수 있는 정보가 포함되어 있는 경우에는 당해 부분을 비치 및 공개하지 아니할 수 있다.

②공공기관은 정보의 공개에 관한 사무를 신속하고 원활하게 수행하기 위하여 정보공개장소를 확보하고 공개에 필요한 시설을 갖추어야 한다.

③공공기관은 제1항 각 호의 범위 안에서 당해 공공기관의 업무의 성격을 고려하여 비공개대상정보의 범위에 관한 세부기준을 수립하고 이를 공개하여야 한다.

※ 우리 위원회 관련 사항

- 정보목록
- 문서등록접수 대장

◆ 정보목록 공개 관련

- 정보목록의 작성·비치 및 전자적 공개 규정은 원칙적으로 보유·관리하고 있는 모든 정보가 대상으로서 자체 생산 정보는 물론 타 기관으로부터 접수한 정보도 포함
- 정보목록 구성항목은 단위업무명칭, 정보의 생산일자, 등록번호, 담당부서, 담당자, 보존기간 및 공개여부이고, 목록 자체에 비공개 대상정보가 포함되어 있는 경우에는 제외됨
- 비공개 대상정보가 공개 가능 대상으로 잘못 구분되어 설정된 정보에 대하여 정보공개 청구가 접수되었을 경우 해당 정보목록의 공개여부와 관계없이 비공개대상 범위(정보공개법 제9조제1항 각호)에 해당된다면 비공개 결정이 가능함

비밀유지

[07. 8. 9. 행정안전부 질의응답]

마. 법 제9조

제9조 (비공개대상정보) ①공공기관이 보유·관리하는 정보는 공개대상이 된다. 다만, 다음 각호의 1에 해당하는 정보에 대하여는 이를 공개하지 아니할 수 있다.

②, ③ 생략

1) 제1호 ⇒ 법령상 비밀·비공개 정보

다른 법률 또는 법률이 위임한 명령(국회규칙·대법원규칙·헌법재판소규칙·중앙선거관리위원회규칙·대통령령 및 조례에 한한다)에 의하여 비밀 또는 비공개 사항으로 규정된 정보

※ 우리위원회 관련 사항

- 선거비용 보전상황
- 선거사무관계자 수당, 실비 등 지급명세서

◆ 법률이 위임한 명령의 의미

- ‘법률이 위임한 명령’은 조문에 “국회규칙·대법원규칙·헌법재판소규칙·중앙선거관리위원회규칙·대통령령 및 조례에 한한다”고 명시되어 있기 때문에 법규명령 중 총리령과 부령은 해당이 되지 않으며, 대통령령은 위임명령을 의미하므로 집행명령은 해당되지 않음
- ‘법률이 위임한 명령’이란 법률의 위임규정에 의하여 제정된 대통령령, 총리령, 부령 전부를 의미한다기보다는 정보의 공개에 관하여 법률의 구체적인 위임아래 제정된 법규명령(위임명령)만을 의미함

[’07. 10. 10. 행정안전부 질의응답]

2) 제3호 ⇒ 국민의 생명·신체·재산 관련 정보



공개될 경우 국민의 생명·신체 및 재산의 보호에 현저한 지장을 초래할 우려가 있다고 인정되는 정보

◆ 비공개대상정보 해당 여부

- 제3호의 규정에 의한 비공개 유형으로는 수사관계 조희사항, 건축물 등의 경비위탁내용, 방재·방법에 방해가 되는 정보, 범죄행위·위법행위·부정행위 등의 통보자·참고인(또는 피의자 명단), 인감업무·주민등록 관리에 관한 사항으로서 공개될 경우 위·변조, 범죄목적 사용 등으로 인하여 공공의 이익을 해할 우려가 있는 정보임
- “계약서류”는 공개가 원칙임. 다만, 정보공개법 제9조 제1항 제6호, 제7호의 저촉여부를 검토하여 이를 가리고 부분공개함

[’07. 7. 12. 행정안전부 질의응답]

3) 제4호 ⇒ 재판·수사 등 관련 정보

진행중인 재판에 관련된 정보와 범죄의 예방, 수사, 공소의 제기 및 유지, 형의 집행, 교정, 보안처분에 관한 사항으로서 공개될 경우 그 직무수행을 현저히 곤란하게 하거나 형사피고인의 공정한 재판을 받을 권리를 침해한다고 인정할 만한 상당한 이유가 있는 정보

※ 우리 위원회 관련 사항

- 문답서, 확인서, 소명자료 등
- 선거법위반행위 처리현황, 조치현황

◆ 피고발인이 제출한 소명자료 공개 여부

- 현행법상 청구자가 청구취지를 밝힐 것을 공공기관이 강요할 수 없다 할지라도 공개여부에 대한 비교·형량에 필요한 '정보의 사용목적(청구취지)'을 밝히지 않는다면 비교·형량시 공개로 인한 청구자의 이익을 당해 공공기관으로서는 알 수가 없으므로 공개로 인해 침해되는 다른 이익에 더 주안점을 둘 수밖에 없음을 청구자에게 주지시킬 필요가 있음
- 고소장 및 고소인 진술조서, 피고소인 진술조서 및 당사자간 제출된 증거자료 등에 대한 내용에는 고소인과 피고소인의 진술내용 등만 기재되어 있으므로 법 제9조제1항제4호에 해당한다고 볼 수 없으나, 검찰에 기소하지 않고 내사 종결된 사건으로 고소인의 재고소가 가능한 경우 범죄수사의 진행상황, 수사의 방향, 수사의 방법 등의 내용이 포함되어 있는 수사보고서·내사결과보고서·내사중간보고서 등 '기타 수사보고 등 일체'의 경우처럼 정보가 공개되는 경우 수사와 관련된 직무의 수행이 현저히 곤란해진다고 인정할 만한 상당한 이유가 있는 경우에 한하여 법 제9조제1항 제4호에 해당되어 비공개 할 수 있을 것임
- 공직선거법 위반 피고발인이 소명자료로 제출한 증빙서류 등은 당해 피고발인의 사생활의 비밀 또는 자유를 침해할 우려가 있다고 인정되는 정보에 해당될 수 있을 것이며, 해당 정보가 공개되기 위해서는 정보공개법 제9조제1항제6호 단서조항 각목에 해당되어야 하나, 고발인 신분인 청구인의 청구취지가 단서조항 각목에 해당되지 않으므로 비공개의 실익이 크다고 할 것임

['08. 3. 27. 행정안전부 질의응답]

◆ 수사관 출장내역 및 출장복명서 공개 여부

청구인이 공개를 요구하는 수사관의 출장내역은 범죄정보의 출처 등 정보수집 기법, 내사방법, 수사기관 상호간의 연락체계, 현장 활동의 내역 등이 수록된 수사기관 내부문서이고, 출장복명서 등 관련 기록에 수록된 정보원의 인적사항은 사생활의 비밀에 직결되는 것이므로, 위 정보가 청구인을 통해 외부로 함부로 유출되는 경우 범죄수사를 위한 직무수행에 현저한 지장이 초래되고, 정보원의 사생활의 비밀을 침해할 우려가 있으므로 비공개 대상에 해당됨

[서울고검행정심판위원회 2005-8]

4) 제5호 ⇒ 감사·감독·계약·의사결정과정 등 관련 정보

감사·감독·검사·시험·규제·입찰계약·기술개발·인사관리·의사결정과정 또는 내부검토 과정에 있는 사항 등으로서 공개될 경우 업무의 공정한 수행이나 연구·개발에 현저한 지장을 초래한다고 인정할 만한 상당한 이유가 있는 정보

※ 우리 위원회 관련 사항

- (예비)후보자 홍보물, 인쇄물 계약현황
- 의안대장, 회의록 등

◆ 예비후보자 홍보물 공개 여부

- '예비후보자홍보물'은 선거구안의 세대수의 100분의 10에 해당하는 수 이내에 서 예비후보자 자신의 사진, 성명, 전화번호, 학력, 경력, 그 밖에 홍보에 필요한 사항을 게재한 인쇄물을 작성하여 관할 선거관리위원회로부터 발송대상, 매수 등을 확인받은 후 우편발송하는 사안이므로 해당 정보가 공개될 경우 당해 예비후보자의 사생활의 비밀 또는 자유를 침해할 우려가 있다고 인정되기 어렵다고 할 것이고,



- '선거관리업무'로서 공개될 경우 업무의 공정한 수행에 현저한 지장을 초래한다고 인정할 만한 상당한 이유가 있는지 여부는 청구자가 상호 경쟁관계에 있는 다른 예비후보자로서 인쇄물이 선거권자인 각 세대에 발송되기 이전에 공개함으로써 인해 당해 예비후보자의 학력, 경력 등에 대한 시시비비에 휘말려 업무의 공정한 수행에 현저한 지장을 받을지 유무를 구체적인 상황에 따라 개별적으로 판단하여야 할 것이나, 법 제9조제1항제5호를 들어 비공개할 경우 한시적인 비공개로서 그 공개시점(홍보물 발송시점)을 미리 청구인에 알려주어야 할 것임

[’08. 3. 11. 행정안전부 질의응답]

◆ 의정보심의위원회 회의록 공개 여부

각종 심의회 및 위원회의 회의록 공개 여부는 그 심의회 및 위원회의 법적 설치근거, 업무의 성격 등 사안에 따라 공개 여부를 결정할 수 있다고 판단할 수 있으나, 위원회 회의록이 정보공개법 제9조제1항제5호에 의한 비공개 대상정보에 해당된다는 구체적 사유를 당해 공공기관이 입증할 수 없다면 공개로 인한 청구자의 이익이 비공개로 인한 당해 심의회 업무의 공정한 수행 이익보다 크다고 할 수 있으므로 발언자 내용을 가린 형태로 부분공개 하여야 할 것임

[’07. 11. 1. 행정안전부 질의응답]

◆ 전체 공무원의 인사기록 내용의 정보공개 가능 여부

- “전체공무원(시장과 일용직 포함)의 직급별로 초임발령일자, 초임직급, 몇급 공채인지, 공채인지 또는 특채인지 여부, 각 부서별 직원의 근무이력”에 대한 공개 여부를 판단하여 볼 때 “초임발령일자, 초임직급, 몇급 공채인지, 공채인지 또는 특채인지 여부”는 공개로 인하여 개별 공무원의 사생활의 비밀 또는 자유를 침해할 우려가 있다고 보기 어려우므로 공개가 가능할 것으로 사료되며, 다만 “각 부서별 직원의 근무이력”의 정보는 개별 공무원의 초임 발령부터 현 재직기간까지의 전체 근무이력을 의미하는 것으로 사료되는 바, 이는 공무원 개인의 근무이력으로서 비공개가 가능함
- 정보공개 청구자가 특정 재직공무원 또는 퇴직공무원의 재임기간 전체에 대한 근무 경력에 대한 정보를 공개 요청하였다면 당해 공무원의 성명과 주민등록번호, 주소의 개인정보와 경력사항인 근무기간별 직급과 직위, 근무부서, 근무년한, 최종직위(직급), 퇴직이유, 상벌사항(포상 및 징계), 직위해제 등의 인사기록 사항들을 포함하고 있어 이를 공개할 경우 개인의 사생활의 비밀 또는 자유를 침해할 우려가 상당할 것이므로 비공개가 가능하나, 다만, 재직 또는 퇴직공무원의 재임기간 중 특정기간 및 부서에 대한 근무사실이 있는지 여부는 그 사실여부의 공개로 인하여 당해 퇴직자의 사생활의 비밀 또는 자유를 침해할 우려가 크다고 볼 수 없기 때문에 공개가 가능함
- 일용직 등 비정규직 직원의 정보공개와 관련하여 비정규직은 경력직 및 특수경력 공무원에 해당되지 않으며, 일용인부임 근로계약서 등 별도 계약을 통해 단기간의 근로조건을 부여하는 사안이니 만큼 청구인의 청구내용에 해당되지

않기 때문에 “정보공개법 제2조 및 제3조의 규정에 의한 정보(자료)의 부존재에 따른 비공개” 결정을 하시기 바라며, 청구인이 이의신청 등을 통해 구체적으로 일용직 근로자의 성명, 계약일자, 계약기간, 근무부서 등의 청구내용으로 변경하면 이는 일용직 당사자의 사생활의 비밀 또는 자유를 침해할 우려가 있는 개인정보로서 정보공개법 제9조제1항제6호에 의해 비공개가 가능함

[07. 9. 12. 행정안전부 질의응답]

◆ 각 회의록 등에 기재된 발언내용에 대한 해당 발언자의 인적사항 공개 여부

심사위원회의 회의록 및 의결서 중 발언내용 이외에 해당 발언자의 인적사항까지 공개된다면 위원이나 출석자는 회의록 등의 공개에 대한 부담으로 인한 심리적 압박 때문에 심사위원회의 심의절차에서 자유로운 의사교환을 할 수 없고, 심지어 당사자나 외부의 의사에 영합하는 발언을 하거나 침묵으로 일관할 우려마저 있으므로 이러한 사태를 막아 위원들이 심의에 집중하도록 함으로써 심의의 충실화와 내실화를 도모하기 위하여서는 회의록 및 의결서의 발언내용 이외에 해당 발언자의 인적사항까지 외부에 공개되어서는 아니 된다고 할 것임

[서울행정법원 2005구합 34794]

5) 제6호 ⇒ 이름·주민등록번호 등 개인정보

당해 정보에 포함되어 있는 이름·주민등록번호 등 개인에 관한 사항으로서 공개될 경우 개인의 사생활의 비밀 또는 자유를 침해할 우려가 있다고 인정되는 정보. 다만, 다음에 열거한 개인에 관한 정보는 제외한다.

- 가. 법령이 정하는 바에 따라 열람할 수 있는 정보
- 나. 공공기관이 공표를 목적으로 작성하거나 취득한 정보로서 개인의 사생활의 비밀과 자유를 부당하게 침해하지 않는 정보
- 다. 공공기관이 작성하거나 취득한 정보로서 공개하는 것이 공익 또는 개인의 권리구제를 위하여 필요하다고 인정되는 정보
- 라. 직무를 수행한 공무원의 성명·직위
- 마. 공개하는 것이 공익을 위하여 필요한 경우로써 법령에 의하여 국가 또는 지방자치단체가 업무의 일부를 위탁 또는 위촉한 개인의 성명·직업



※ 우리 위원회 관련 사항

- 선거관리위원회 위원·직원 성명, 연락처, 주소 등
- (예비)후보자 사무실 주소·연락처 등
- 투개표 참관인 명단, 선거인명부 등
- 소속공무원 공무상 해외여행 경비

◆ 본인이 제출한 무소속후보자 추천장의 공개 여부

- 당해 후보자가 선거종료 후 후보자추천장 사본에 대해 정보공개 청구한 경우, 비록 청구인 본인이 제출한 정보라고 하더라도 이를 취득하여 보유·관리하고 있는 공공기관의 입장에서는 청구인 본인 자신의 개인정보가 아닌 후보자를 추천한 개별 개인의 개인정보이기 때문에 정보주체(개별 후보자 추천인)의 동의나 법 제9조제1항제6호의 단서조항 각목에 해당되지 않는다면 비공개가 가능할 것이나, 최종적인 정보공개여부 결정은 대상 정보가 법 제9조 제1항 각호의 규정에 해당된다는 논리로 무조건 비공개하는 것이 아니라 공개로 인한 청구자의 이익과 비공개로 보호되는 제반이익을 비교·형량하여 결정하여야 함
- 다른 후보자가 후보자추천장에 대해 정보공개 청구한 경우 그 공개여부는 타인의 개인정보로서 공개할 경우 개인의 사생활의 비밀 또는 자유를 침해할 우려가 있다고 인정되고, 그 청구취지 또한 법 제9조제1항제6호 단서조항 각목에 해당되기 어렵기 때문에 비공개 하여야 할 것임

[’08. 2. 25. 행정안전부 질의응답]

◆ 특정공무원의 여비, 시간외수당, 맞춤형복지비용 집행내역의 공개 범위

- “시간외 근무수당 집행내역과 초과근무내역서”는 원시적으로 공공기관이 “공표”를 목적으로 작성하거나 취득한 정보라고 볼 수는 없으나, 그 공개로 인하여 실현되는 청구인의 알권리와 공익적 측면을 배제할 수 없고, 또한 직원 개개인을 식별할 수 있는 요소가 배제된 ‘시간외근무수당지급 총 시간’과 ‘시간외근무수당 총액수’에 관한 정보는 공개한다 하더라도 개인의 사생활의 비밀과 자유가 침해될 소지가 없음
- “여비 집행내역과 관내 출장명령서 사본”의 공개 여부와 관련하여, 여비지출에 관계된 회계문서로서 여비 수령자의 주민등록번호, 개인별 계좌번호 등이 명시되어 있으면 이를 가린 형태로 부분공개 하여야 할 것임. 여비는 출장명령에 의한 공적수행의 대가로 일비, 교통비, 숙박비, 식비 등이 지급되는 것으로서 이를 개별 공무원의 소득원의 정보로 해석하기에는 무리가 있을 것이므로 공개하여야 할 것이고, 여비지출의 증빙서류인 근무상황부 중 출장명령부는 정보공개법 제9조 제1항 제6호의 단서조항 ‘라목’에 해당되어 공개하여야 할 것이나, 그 출장내용에 관련된 업무가 의사결정중이거나 내부검토과정 에 있는 사안으로서 이를 공개할 경우 당해 업무수행의 공정한 수행에 현저

한 지장을 초래할 우려가 있다면 동법 제14조의 규정에 의거 이를 가린 형태로 부분공개 하여야 할 것임

- “맞춤형복지비 집행 및 수령 내역”의 공개 여부와 관련, 이는 비록 그 복지항목과 단가가 공개되어 있다 하더라도 그 구성항목의 산출근거가 당해 공무원의 근무년수와 배우자 등 부양가족수이고, 그 집행내역도 개별 공무원이 복지비 지출가능 항목의 범위내에서 자율적으로 지출하는 항목이므로 해당 정보가 개별 공무원의 소득원의 정보라고 보기는 어려울 지라도 사생활의 비밀 또는 자유를 침해할 우려가 크다고 판단되므로 법 제9조제1항제6호의 규정에 의거 비공개 해야 할 것임

[’08. 1. 14. 행정안전부 질의응답]

◆ 업무추진비 사용내역 등 공개여부

“지방의회의원 국외여비, 의정운영공통업무추진비 사용내역 및 증빙자료”는 예산 지출에 관계된 회계문서로서 국외여비 수령자의 주민등록번호, 개인별 계좌번호 등이 명시되어 있으면 이를 가린 형태로 부분공개 하여야 할 것이고, 업무추진비 지출 증빙자료에 특정인의 개인정보라든지 금융계좌번호 등 비공개 정보가 있으면 이를 가린 형태로 정보공개법 제14조의 규정에 의거 부분공개 하여야 할 것임

[’07. 10. 18. 행정안전부 질의응답]

◆ 회계지출 서류에 첨부된 세금계산서 등의 공개 여부



회계지출 서류 중 세금계산서에 기록되어 있는 법인·단체 또는 영업소를 경영하는 개인의 상호, 단체명, 영업소명, 사업자등록번호, 대표자, 사업장 소재지, 업종 등에 관한 정보는 법인·단체 또는 개인의 경영·영업상의 비밀에 관한 사항으로서 공개될 경우 법인 등의 정당한 이익을 해할 우려가 있다고 인정되는 정보로 보기 어렵고, 또한 개인의 사생활의 비밀 또는 자유를 침해할 소지도 적기 때문에 공개대상 정보임. 다만, 관련 회계 지출 내역에 법인 등이 거래하는 금융기관의 계좌번호나 상품 제조방법, 생산기술 또는 영업상의 정보, 경영방침, 경리·인사 등 업체의 내부관리 사항 등 영업상의 비밀에 관한 사항으로 법인 등의 이름·사업자등록번호와 결합하여 공개될 경우 해당 법인 등의 영업상의 이익 및 지위가 위협받을 우려가 있을 경우에는 “공개될 경우 정당한 이익을 현저히 해할 우려가 있다고 인정되는 정보”에 해당되어 비공개가 가능할 것임

[’07. 10. 18. 행정안전부 질의응답]

◆ 퇴직공무원의 징계사실 및 사유에 대한 공개 여부

- 퇴직공무원이 교육감선거 출마 후보자로서 시민단체에서 후보자의 도덕성 확인 등 공익적 감시활동 차원에서 “재직 중 징계 받은 사실 및 징계사유”에 대하여 정보 공개 요청을 하였을 경우, 청구취지가 법 제9조 제1항 제6호 단서조항 ‘다목’에 해당된다고 보기 어렵고, 오히려 해당 정보가 공개됨으로 인하여 후보자간 선의의 경쟁이 아닌 상대방을 비방하고 헐뜯는 정보로 악용될 수 있는 점을 고려하여 보면 비공개에 의하여 보호되는 후보자 개인의 사생활의 보호 등의 이익이 공개에 의하여 보호되는 공익(유권자의 알권리)보다 크다고 할 것이므로 비공개 결정 처분이 타당함

- 정보공개법 제9조 제1항 제6호와 관련된 대법원 판례 중 “개인의 사생활에 관련된 정보라도 언제나 비공개 되는 것이 아니고, 공개될 경우 개인의 사생활의 비밀 또는 자유를 침해하는 것은 물론 침해할 우려가 있는 정보만이 비공개 대상임.(대법원 1997.5.23, 선고 96누2438판결)”이라는 판례 내용은 제 6호의 단서조항인 ‘가목~마목’의 입법취지와도 일치되는 내용이며, 단서조항인 각 목별 조문해석을 하면 다음과 같음

예외적일일

- 첫째, ‘가목’인 “법령이 정하는 바에 따라 열람할 수 있는 정보”의 단서조항은 다른 법률에서 정보공개와 관련하여 열람의 방법이 별도로 규정되어 있는 경우에는 해당 법률의 입법취지를 최대한 살리고 정보공개법과의 상호충돌을 피하기 위함으로 정보공개법의 적용에 앞서 해당 개별법의 특별한 규정을 우선 적용하여야 한다는 의미인 정보공개법 제4조에 열람의 특별한 규정이 있는 정보에 대하여 사본·복제물로 공개형태를 달리하여 정보공개 청구하였을 경우, 해당 정보에 성명, 주소 등 개인정보가 포함되어 있는 정보공개법 제9조제1항제6호에 해당되는 비공개 대상 정보라도 ‘가목’의 “법령이 정하는 바에 따라 열람할 수 있는 정보”는 예외적으로 공개가 가능한 정보이므로 이는 사본·복제물 형태로도 공개하여야 한다는 조항임
- 둘째, ‘나목’인 “공공기관이 공표를 목적으로 작성하거나 취득한 정보로서 개인의 사생활의 비밀과 자유를 부당하게 침해하지 않는 정보”의 단서조항은 심의회 등 위원명부, 수상자명단 등 공공기관의 작성 및 취득 목적이 공표대상 정보로서 이의 공개로 인하여 개인의 사생활의 비밀과 자유를 부당하게 침해하지 않는 정보가 해당됨

- 셋째, '다목'인 "공공기관이 작성하거나 취득한 정보로서 공개하는 것이 공익 또는 개인의 권리구제를 위하여 필요하다고 인정되는 정보"의 단서조항에서 공개하는 것이 '공익 또는 개인의 권리구제를 위하여 필요하다고 인정되는 정보'에 해당하는지 여부는 비공개에 의하여 보호되는 개인의 사생활 보호 등의 이익과 공개에 의하여 보호되는 공익 및 개인구제(사익)를 비교·형량(교량) 하여 그 구체적 사안에 따라 신중히 판단하여야 함. 이것은 비교형량원칙이 적용되는 사안으로서 정보공개담당자에게 우월적 지위와 재량이 주어졌지만 정보공개법이 공개가 원칙이고, 그 우월적 지위와 재량의 발휘조건은 공개에 의하여 보호되는 공익과 개인구제의 이익에 더 중점을 두어야 할 것임. 예외적인 공개사항 중 '다목'의 의미는 신체장애자 상담원 명부처럼 공개하는 것이 공익상 필요한 정보이거나 민사소송을 통한 확정판결 후 또는 가압류, 가등기 등 법원의 허가를 얻은 후 채권자가 채무자에 대한 채권확보를 위해 필요한 채무자의 재산상황에 관한 정보와 같이 개인의 권리구제를 위하여 필요한 정보는 예외적으로 공개하는 것임
- 넷째, '라목'인 "직무를 수행한 공무원의 성명과 직위"의 단서조항은 청구자가 청구한 정보에 해당되는 직무를 수행한 공무원의 성명과 직위는 의무적으로 공개하여야 한다는 의미로서 여기서 중요한 것은 '공무원'의 범주임. "당해 직무를 수행한 공무원의 성명·직위"에서 공무원의 범주에는 국가공무원법 및 지방공무원법상의 공무원뿐만 아니라 정보공개법 제2조 제3호 및 동법시행령 제2조의 정보공개 대상기관 중 공공기관의 임직원도 포함되는 개념임
- 다섯째, '마목'인 "공개하는 것이 공익을 위하여 필요한 경우로서 법령에 의하여 국가 또는 지방자치단체가 업무의 일부를 위탁 또는 위촉한 개인의 성명과 직업"의 단서조항은 예외적인 공개사항 중 '라목'과 같이 '마목'은 공익적 성격의 개인정보로서 직무를 수행한 공무원의 성명·직위, 업무의 일부를 위탁 또는 위촉받은 개인의 성명·직업을 공개하도록 하여 정부업무수행의 투명성을 강화하고자 '04. 1. 29 전문개정시 신설한 조문임. 따라서 '공무수탁사인'처럼 법령에 의하여 국가 또는 지방자치단체가 업무의 일부를 위탁 또는 위촉한 개인의 성명과 직업은 공개하여야 하며, 그 공개조건인 '공익을 위하여 필요한 경우'에 해당하는지 여부는 비공개에 의하여 보호되는 개인의 사생활 보호 등의 이익과 공개에 의하여 보호되는 공익 및 개인구제(사익)를 비교·형량(교량) 하여 그 구체적 사안에 따라 개별적으로 신중히 판단하여야 할 것임

[07. 11. 16. 행정안전부 질의응답]

6) 제7호 ⇒ 법인의 경영·영업비밀 관련 정보

법인·단체 또는 개인(이하 "법인등"이라 한다)의 경영·영업상 비밀에 관한 사항으로서 공개될 경우 법인 등의 정당한 이익을 현저히 해할 우려가 있다고 인정되는 정보. 다만, 다음에 열거한 정보를 제외한다.

가. 사업활동에 의하여 발생하는 위해로부터 사람의 생명·신체 또는 건강을 보호하기 위하여 공개할 필요가 있는 정보

나. 위법·부당한 사업활동으로부터 국민의 재산 또는 생활을 보호하기 위하여 공개할 필요가 있는 정보

◆ 법인에게 지원된 보조금 지원현황 공개 여부

- 제7호에서 "법인"이라 함은 "법인성을 갖춘" 주식회사 등의 영리법인과 공익법인·종교법인 등의 비영리법인, 그리고 특수법인을 포함한 개념이며, 학교법인·종교법인과 같은 비영리 법인도 제7호의 "법인"에 포함이 됨을 고려할 때 경영·영업상의 비밀은 반드시 "경제적 가치"를 가질 필요는 없고 비공개성의 필요성·상당성이 인정되는 한 "비경제적 가치"도 당연히 포함됨
- 제7호의 비공개 유형의 대표적인 사례를 들면, ①계약체결에 이르는 과정 또는 결과에 관한 문서로서 공개할 경우 설계·시공의 노하우 등이 공개되어 설계·시공자에게 불리한 경우, ②최저임금적용제외인가신청서, 차량의 세부 제원, 세부도면 또는 부품의 규격 및 하중분포별 분담하중의 산출방법 등이 포함된 형식승인신청서 등, ③국가보조금 지원을 받는 민간단체 또는 정부가 허가한 비영리 사단법인 관련 사항 중 그 단체의 자금·인사 등 내부관리 에 관한 정보, ④각종 용역수행과 관련한 제안업체(개인·단체·법인 등)에 대한 기술수행능력 평가 결과 등이 있음

[’07. 10. 31. 행정안전부 질의응답]

바. 법 제11조

제11조 (정보공개여부의 결정) ①공공기관은 제10조의 규정에 의하여 정보공개의 청구가 있는 때에는 청구를 받은 날부터 10일 이내에 공개여부를 결정하여야 한다.

②공공기관은 부득이한 사유로 제1항에 규정된 기간 이내에 공개여부를 결정할 수 없는 때에는 그 기간의 만료일 다음 날부터 기산하여 10일 이내의 범위에서 공개여부 결정기간을 연장할 수 있다. 이 경우 공공기관은 연장된 사실과 연장사유를 청구인에게 지체없이 문서로 통지하여야 한다.

③공공기관은 공개청구된 공개대상정보의 전부 또는 일부가 제3자와 관련이 있다고 인정되는 때에는 그 사실을 제3자에게 지체없이 통지하여야 하며, 필요한 경우에는 그의 의견을 청취할 수 있다.

④공공기관은 다른 공공기관이 보유·관리하는 정보의 공개청구를 받은 때에는 지체없이 이를 소관기관으로 이송하여야 하며, 이송을 한 공공기관은 지체없이 소관기관 및 이송사유 등을 명시하여 청구인에게 문서로 통지하여야 한다.

⑤정보공개를 청구한 날부터 20일 이내에 공공기관이 공개여부를 결정하지 아니한 때에는 비공개의 결정이 있는 것으로 본다.