사이버보안 관제센터 운영지침

ICT전략실 정보보호부

제정 2023.12.18. 지침 제413호

제1장 총 칙

제1조(목적) 이 지침은 「정보통신기반 보호법」, 「국가사이버안전관리규정」, 「국가정보보안기본지침」, 「보건복지부 정보보안 기본지침」, 「보건복지사이버안전센터 운영규정」, 건강보험심사평가원 「정보보안지침」에 따라 건강보험심사평가원의 사이버보안 관제센터 운영에 관한 사항을 규정함을 목적으로 한다.

제2조(명칭) 건강보험심사평가원(이하 “심사평가원”이라 한다)의 보안관제센터 명칭은 사이버보안 관제센터(이하 "센터"라 한다)라 하고, 영문명은 HSOC(HIRA Security Operations Center)라 한다.

제3조(다른법령과의 관계) 심사평가원의 “센터”에 대하여 다른 법령에 특별한 규정이 있는 경우를 제외하고는 이 지침에 따른다.

제4조(정의) ① 이 지침에서 사용하는 용어의 정의는 다음과 같다.

1. "정보통신기반시설"이라 함은 「정보통신기반 보호법」제2조제1호 따른 전자적 제어·관리시스템 및 정보통신망을 말한다.
2. "정보통신망"이라 함은「전기통신기본법」제2조제2호의 규정에 의한 전기통신설비를 활용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체제를 말한다.
3. "사이버공격"이라 함은 해킹·컴퓨터바이러스·논리폭탄·메일폭탄·서비스방해 등 전자적 수단에 의하여 정보통신망을 불법 침입·교란·마비·파괴하거나

정보를 절취・훼손하는 일체의 공격 행위를 말한다.

4. "사이버안전"이라 함은 사이버공격으로부터 정보통신망 및 정보자산을 보호함으로써 정보통신망과 정보의 기밀성・무결성・가용성 등 안전성을 유지하는 상태를 말한다.

5. "보안관제"라 함은 전자문서・전자기록물 또는 정보통신망을 대상으로 하는 사이버공격을 실시간 탐지・분석・대응하는 일련의 활동을 말한다.

6. "민간 클라우드컴퓨팅서비스"라 함은「전자정부법」 제54조의2 및 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제20조에 따라 클라우드컴퓨팅서비스 제공자의 클라우드컴퓨팅서비스를 말한다.

② 이 지침에서 사용하는 용어는 제1항에서 정하는 것을 제외하고는 「국가사이버안전관리규정」, 「국가정보보안기본지침」, 「보건복지부 정보보안 기본지침」, 「보건복지사이버안전센터 규정」, 심사평가원 「정보보안지침」 등 관계 법령 등이 정하는 바에 따른다.

제5조(관제목표) 보안관제의 목표는 심사평가원의 정보통신망에 대한 내·외부의 불법 침해 시도 등 사이버공격, 침해사고에 대해 실시간 탐지 및 침해 대응하여 피해의 발생 또는 확산을 방지하는데 있다.

제2장 보안관제체계

제6조(조직 및 업무) ① 센터는 심사평가원 정보보호업무 담당부서에서 운영하며, 센터장은 정보보호업무 담당부서의 장이 담당하고 센터 업무를 총괄한다.

② 센터에서 수행하는 업무는 다음 각 호와 같다.

1. 센터업무 기획·운영에 관한 사항
2. 센터 관련 지침·제도·매뉴얼·가이드의 제·개정
3. 사이버공격 실시간 관제·분석 및 예·경보 전파
4. 사이버침해사고 조사, 처리 및 복구조치 지원

5. 사이버공격 재발방지대책 수립을 위한 기술지원

6. 정보보안 취약점 및 침해요인의 대응 방안 관련 정보공유

7. 정보통신기반시설의 취약점 분석·평가, 보호 대책 수립 지원

8. 보안관제 결과의 작성 및 관리

9. 사이버공격 대응훈련 지원, 보안관제 탐지규칙 및 세부방안 기준의 작성

10. 그 밖에 센터장이 필요하다고 판단하는 업무

③ 원장은 센터의 책임 있는 수행 및 보안관리를 위하여 적정한 수의 정규직원을 상시 배치하여야 한다.

제7조(보안관제시스템 구축·운영) 센터장은 보안관제 업무를 효율적으로 수행하기 위하여 보안관제시스템을 구축·운영한다.

제8조(센터의 운영) ① 원장은 사이버보안 관제업무의 수행을 위해 사이버공격에 대하여 24시간 탐지분석·대응할 수 있는 근무체계를 구축·운영하여야 한다.

② 사이버보안 관제업무를 수행하는 직원은 근무를 교대할 때에 근무 중에 발생한 주요 상황을 명확하게 인계인수하여 업무의 연속성을 유지하여야 한다.

③ 원장은 사이버보안 관제업무의 수행을 위해 필요한 경우 외부 전문 업체와 별도의 유지·보수 또는 관리에 관한 용역계약을 체결할 수 있다.

제9조(협력체계 및 비상연락망) ① 센터장은 침해사고 발생 시 신속한 대응 및 조치를 위하여 유관기관과의 침해사고 대응 협력체계를 구축·유지하여야 한다.

② 센터장은 사이버공격에 대한 신속한 탐지 및 대응을 위하여 국가사이버안보센터, 보건복지사이버안전센터 등 유관기관 및 외부 협력업체(유지보수 등)의 비상연락망을 현행화하여야 한다.

제3장 보안관제업무

제10조(공격 탐지) ① 센터장은 보안관제 업무수행을 위하여 보안관제시스템을 이용하여 사이버공격 관련 정보를 수집하여야 한다.

② 공격탐지 경로는 다음 각 호와 같다.

1. 센터 보안관제 및 수탁기관을 통한 공격 탐지
2. 국가사이버안보센터, 보건복지사이버안전센터 및 유관 기관으로부터의 통보
3. 언론 등 외부 수집

제11조(경보 발령) ① 센터장은 사이버공격에 대한 체계적인 대응 및 대비를 위하여 사이버공격의 파급영향, 피해규모 등을 고려하여 관심・주의・경계・심각 등 수준별 경보를 발령할 수 있다.

② 제1항에 따라 경보를 발령한 경우 이에 상응하는 수준별 조치를 취하여야 한다.

③ 센터장은 국가사이버안보센터 또는 보건복지사이버안전센터에서 사이버 경보가 발령된 경우 이에 대한 적절한 조치를 하여야 한다.

제12조(초동 조치) ① 센터장은 보안관제를 통해 사이버공격을 인지하면 즉시 피해 최소화 및 확산 방지를 위하여 심사평가원「정보보안지침」제131조제1항에 따른 초동 조치를 신속히 취하여야 한다.

② 센터장은 사이버공격으로 인한 피해 발생시 별지 제1호 서식에 따라 사고신고서를 보건복지사이버안전센터에 바로 보고하여야 한다.

제13조(사고보고 및 조사) ① 심사평가원「정보보안지침」제5조제5항에 따른 분임정보보안담당관(이하 “분임정보보안담당관”이라 한다)은 사이버공격으로 사고발생 또는 징후를 발견한 경우에 피해를 최소화하는 조치를 하고 그 사실을 지체 없이 센터장에게 보고하여야 한다.

② 센터장은 사이버공격으로 발생한 사고에 대하여 그 원인 분석을 위한 조사를 실시할 수 있다.

③ 분임정보보안담당관은 사고 원인이 규명될 때까지 피해 시스템에 대한 증거를

보전하고 임의로 관련 자료를 삭제하거나 포맷하여서는 아니 된다.

④ 센터장은 제2항에 따른 조사를 위해 분임정보보안담당관에게 다음 각 호에 해당하는 자료 제출을 별지 제3호 서식에 따라 요청할 수 있다.

1. 공격 주체 및 피해자를 식별하기 위한 IP 주소, 전자우편 주소, 정보통신서비스 이용자 계정 정보, 피해자의 성명 및 연락처

2. 사이버공격에 사용된 악성프로그램 및 공격 과정에서 생성·변경 또는 복제된 디지털정보

3. 공격 주체가 절취한 디지털정보

4. 공격 주체의 행위가 기록된 내역 또는 로그기록

5. 기타 센터장이 필요하다고 판단하는 자료

⑤ 제4항에 따른 자료 제출을 요청받은 분임정보보안담당관은 관계 법규에 저촉되지 않는 범위 내에서 별지 제4호 서식에 따라 해당 자료를 제출하여야 하며 센터장은 제출 받은 자료를 사이버공격에 대한 예방 및 대응과 관련한 목적으로만 사용하여야 한다.

⑥ 센터장은 사이버공격으로 피해가 심각하다고 판단되는 경우에 국가사이버안보센터, 보건복지사이버안전센터등과 협의하여 합동조사팀을 구성·운영할 수 있다.

⑦ 민간 클라우드컴퓨팅서비스의 공공 전용 클라우드를 이용하는 부서의 장은 공공 전용 클라우드에서 사고가 발생한 경우 센터장과 합동으로 조사반을 구성하여 클라우드컴퓨팅서비스제공자에 대하여 계약의 범위 내에서 자료의 보전 및 제출 요구, 현장 조사 등 필요한 조치를 취하여야 한다.

제14조(사고처리 및 복구) ① 센터장은 발생한 사이버공격 사고에 대한 정밀분석을 실시하고 피해확산 방지 및 사고복구를 위해 필요한 조치를 취하여야 한다.

② 센터장은 사고발생 또는 징후를 발견하거나 제13조제1항에 따른 보고를 받은 경우에 분임정보보안담당관에게 제1항의 조치를 위한 협조를 요청할 수 있으며, 해당 분임정보보안담당관은 특별한 사유가 없는 한 지체 없이 이에 따라야 한다.

제15조(운영현황 보고) ① 센터장은 별지 제2호서식의 센터 운영현황을 작성하여 매년 1월 25일까지 보건복지사이버안전센터장을 거쳐 국가정보원장에게 제출하여야 한다.

② 센터장은 센터를 운영하면서 수집한 사이버공격 탐지·분석 등의 정보를 보건복지사이버안전센터장에게 매월 보고하여야 한다.

③ 센터장은 센터 운영현황에 변경이 발생한 경우「보건복지사이버안전센터 운영규정」제11조 제2항에 따라 그 변경사항을 발생일로부터 10일 이내에 보건복지사이버안전센터장에게 제출하여야 한다.

제4장 보안관리

제16조(시설보안) ① 원장은 센터를 제한구역으로 설정하여 관리하여야 하며, 접근권한이 없는 자에 대한 접근 통제 및 감시를 효율적으로 수행할 수 있도록 독립된 공간에 설치·운영하여야 한다.

② 원장은 보안관제 업무를 수행하기 위한 정보통신망을 별도로 구축·운영하여야 하며 다른 정보통신망(인터넷 포함)과 분리·운영하여야 한다.

③ 센터장은 센터 출입인가자의 범위를 설정하고 비인가자에 대한 접근 통제 대책을 마련하여야 한다.

④ 센터장은 외부로부터 시찰·견학 요청을 받은 경우에는 핵심시설에 대한 사진촬영을 제한하고 보안관제와 관련된 세부 정보의 제공을 금지하는 등 출입 인원에 대한 보안대책을 마련하여야 한다.

제17조(인원보안) ① 센터장은 외부 인력을 보안관제 업무에 활용하고자 하는 경우에는 다음 각 호의 보안대책을 수립·시행하여야 한다.

1. 계약서에 보안 주의사항과 위반 시 책임한계 명시
2. 비밀유지서약서 징구(별지 제5호 서식)
3. 보안관리 책임자 지정

4. 업무와 무관한 정보통신망 접속 금지 등 업무범위 명확화

5. 업무와 무관한 정보통신실 등 중요시설에 대한 출입 제한

6. 기타 필요하다고 인정되는 보안대책

② 센터장은 외부 인력에 대하여 매월 1회 이상 정기 또는 수시로 보안점검과 보안교육을 실시하여야 한다.

제18조(문서보안) ① 보안관제 업무를 수행하는 PC·서버 등 정보시스템에 대외비 또는 비밀을 보관·유통하여서는 아니 된다.

② 센터 내에 설치한 인터넷 접속이 가능한 PC·서버 등 정보시스템에 보안관제 업무와 관련된 문서를 보관·유통하여서는 아니 된다.

③ 누구든지 보안관제 업무와 관련된 세부적인 사항이 포함된 문서를 대외에 임의로 공개하거나 공개된 장소에 무단 방치하여서는 아니 된다.

제19조(비밀유지) ① 센터에 근무하는 자 또는 근무하였던 자는 업무수행 중 지득한 정보 및 자료 등을 센터운영 용도 이외에 다른 목적으로 사용하거나 외부에 임의로 공개·누설 또는 제공하여서는 아니 된다. 다만 다음 각 호의 경우에는 센터장의 승인을 거쳐 공개·사용할 수 있다.

1. 통계 및 학술 기타목적 등으로 특정기관 및 특정인이 나타나지 않도록 가공하여 사용할 경우

2. 관련 법령 및 지침 등에서 정한 규정에 따라 적법한 절차를 거쳐 정보를 제공하는 경우

② 제1항과 관련하여 센터에서 근무하는 자는 별지 제5호서식의 비밀유지서약서를 센터장에게 제출하여야 한다.

제5장 보 칙

제20조(위임규정) 센터의 효율적·체계적 운영 및 관리를 위하여 본 운영지침에 근

거한 세부 매뉴얼을 정할 수 있다.

부 칙<2023.12.18., 지침 제413호>

이 지침은 2024년 1월 1일부터 시행한다.

[별지 제1호서식]

사 고 신 고

<table>
<tr><th colspan="5">기 본 정 보</th></tr>
<tr><td>기 관 명</td><td colspan="2"></td><td>부 서</td><td></td></tr>
<tr><td>성 명</td><td colspan="2"></td><td>직 위</td><td></td></tr>
<tr><td>전자우편</td><td colspan="4"></td></tr>
<tr><td>연 락 처</td><td colspan="4">전화: H.P: FAX:</td></tr>
<tr><th colspan="5">사 고 내 용</th></tr>
<tr><td rowspan="2">사 고
일 시</td><td colspan="2">년 월 일</td><td rowspan="2">피 해
IP주소</td><td rowspan="2"></td></tr>
<tr><td colspan="2">시 분</td></tr>
<tr><td>피해
시스템
용도</td><td colspan="2">※ 뒷장의 시스템 분류 목록 입력</td><td>운영체제</td><td>□윈도우 □유닉스 □NW장비
상세버전정보:</td></tr>
<tr><td>사고유형</td><td colspan="2">※ 뒷장의 사고 유형 목록 입력</td><td>피해범위</td><td>○ 대
※ 피해시스템이 여러 대의 경우 피해숫자 기입</td></tr>
<tr><td>사고내용</td><td colspan="4"></td></tr>
<tr><th colspan="5">조 치 내 용</th></tr>
<tr><td>공격자
정보</td><td colspan="4"></td></tr>
<tr><td>피해현황</td><td colspan="4"></td></tr>
<tr><td>긴급조치
실시사항</td><td colspan="4"></td></tr>
<tr><td>관련
보안제품
운영현황</td><td colspan="4"></td></tr>
<tr><th colspan="5">그 밖에 사고 관련 내용을 구체적으로 서술</th></tr>
<tr><td colspan="5">없음</td></tr>
</table>

<시스템 분류 목록>

기호	시스템 분류	설 명
가	웹서버	기관의 홈페이지 운영 및 웹서비스를 제공하는 서버
나	전자우편 서버	전자우편 송수신을 위해 운영하는 서버
다	DB/업무서버	홈페이지 및 업무지원을 위한 데이터베이스 서버
라	개발/임시서버	개발 및 운영 테스트를 위하여 사용하는 임시 서버
마	통신전송장비	라우터, 스위치 등 통신전송장비 일체
바	보안장비	방화벽, IDS, VPN 및 백신서버 등 정보보안제품 일체
사	개인/업무PC	기관내 사용자의 PC
아	교육/임시PC	교육장 또는 공용 작업을 위해 여러 명이 사용하는 PC
자	기타	위의 시스템 용도에 없는 경우 서술식으로 기술

<사고 유형 목록>

기호	시스템 분류	설 명
A	경유지 악용	타기관의로부터 해킹시도 항의를 받았거나, 시스템 점검 중 해킹흔적 또는 해킹 툴이 설치되어 타 시스템에 접속한 기록이 발견되었을 경우
B	자료훼손 및 유출	내부 시스템의 자료가 변조가 되었거나, 대량의 데이터가 외부로 무단 송신된 흔적이 발견되었을 경우
C	단순침입 시도	지속적인 스캐닝 공격이 발생할 경우
D	웜바이러스 피해	기관내의 PC에서 웜바이러스가 발견되었을 경우
E	홈페이지 변조	기관의 홈페이지가 변조되었을 경우
F	홈페이지 접속 불가능	기관의 홈페이지 서버 또는 네트워크 이상으로 인해 홈페이지 접속이 불가능 할 경우
G	서비스거부공격 피해	불특정 다수의 IP로부터 접속시도 또는 대량 트래픽이 일시에 유입될 경우
H	시스템 파괴	내부 시스템의 자료가 삭제되어 사용이 불가능한 경우
I	기타	위의 사고유형에 포함되지 않을 경우 서술식으로 기술

[별지 제2호서식]

보안관제센터 운영현황

보안관제센터 개요				
개소		* 개소일자	위치	
규모		* 상황실 면적 등	예산	* 구축예산 및 운영예산
조직 현황				
개요		* 조직구성, 인원 및 임무, 근무형태 등		
1	부서		센터장	
	직급		성명	
	이메일		연락처	전화: HP:
2	부서		직급/직책	
	담당분야		성명	
	이메일		연락처	전화: HP:
3	:	* 센터장과 탐지・분석・대응 등 분야별 대표자만 기입		
외부인력 현황				
업체명			대표이사	
인원수			근무형태	
계약기간			수행업무	
지침・매뉴얼 현황				
지침			기준	
매뉴얼			기타	
보안관제시스템 현황				
시스템명		* 주요 기능	시스템명	
시스템명			시스템명	
시스템명			시스템명	

보안장비 현황			
F/W	* 제품명 및 사용대수	IDS/IPS	
ESM		WEB F/W	
라우터		그 밖의 장비	예) NMS 1대 * 네트워크 구성도 사본 제출

보안관제 연동기관 현황
* 대상기관 수, 기관명, 대상목표(인터넷 또는 내부망, 홈페이지 등)

연동기관 IP할당 현황					
1	연동기관		IP 관리자	성 명	
	공인IP			연락처	전화: HP:
	사설IP			이메일	
2					
3					
4					
5					
6					

국가사이버안전센터 탐지규칙 재배포 현황			
기관명	배포방법	기관명	배포방법

[별지 제3호서식]

사 고 조 치 요 청

요청일자			관련부서		
사고 의심 시스템 정보					
시스템명			시스템 IP		
시스템 분류	가	※ 뒷장의 시스템 분류 목록 입력	사고 유형	A	※ 뒷장의 시스템 분류 목록 입력
피해범위	0 대		기타사항		
초동 조치 담당자 정보					
소속					
직위			성명		
초동 조치 내용					
발생일시			탐지일시		
조치완료일시			탐지장비		
공격자IP			공격방법		
탐지내역					
분석내역					
조치내역	-				
조치 요청 내용					
요청목적	☐ 사고예방 ☐ 사고조사 ☐ 사고대응 ☐ 후속조치				
요청내용					
조치기한	0 일				

<시스템 분류 목록>

기호	시스템 분류	설 명
가	웹서버	기관의 홈페이지 운영 및 웹서비스를 제공하는 서버
나	전자우편 서버	전자우편 송수신을 위해 운영하는 서버
다	DB/업무서버	홈페이지 및 업무지원을 위한 데이터베이스 서버
라	개발/임시서버	개발 및 운영 테스트를 위하여 사용하는 임시 서버
마	통신전송장비	라우터, 스위치 등 통신전송장비 일체
바	보안장비	방화벽, IDS, VPN 및 백신서버 등 정보보안제품 일체
사	개인/업무PC	기관내 사용자의 PC
아	교육/임시PC	교육장 또는 공용 작업을 위해 여러 명이 사용하는 PC
자	기타	위의 시스템 용도에 없는 경우 서술식으로 기술

<사고 유형 목록>

기호	시스템 분류	설 명
A	경유지 악용	타기관의로부터 해킹시도 항의를 받았거나, 시스템 점검 중 해킹흔적 또는 해킹 툴이 설치되어 타 시스템에 접속한 기록이 발견되었을 경우
B	자료훼손 및 유출	내부 시스템의 자료가 변조가 되었거나, 대량의 데이터가 외부로 무단 송신된 흔적이 발견되었을 경우
C	단순침입 시도	지속적인 스캐닝 공격이 발생할 경우
D	웜바이러스 피해	기관내의 PC에서 웜바이러스가 발견되었을 경우
E	홈페이지 변조	기관의 홈페이지가 변조되었을 경우
F	홈페이지 접속 불가능	기관의 홈페이지 서버 또는 네트워크 이상으로 인해 홈페이지 접속이 불가능 할 경우
G	서비스거부공격 피해	불특정 다수의 IP로부터 접속시도 또는 대량 트래픽이 일시에 유입될 경우
H	시스템 파괴	내부 시스템의 자료가 삭제되어 사용이 불가능한 경우
I	기타	위의 사고유형에 포함되지 않을 경우 서술식으로 기술

[별지 제4호서식]

사 고 조 치 결 과

발생일시	※ 조치 요청서 참조		**탐지일시**	※ 조치 요청서 참조	
조치분류	☐ 사고예방 ☐ 사고조사 ☐ 사고대응 ☐ 후속조치				
시스템 정보					
시스템명	※ 조치부서 확인 후 기입		**시스템 IP**		
사용용도					
시스템 분류	가	※ 뒷장의 시스템 분류 목록 입력	**사고유형**	A	※ 뒷장의 사고 유형 목록 입력
서비스장애	☐ 있음 ☐ 없음		**피해범위**	0 대 ※ 추가 피해여부 확인 후 기입	
조치 담당자 정보					
조치부서					
직위			**성명**		
조치 내용					
조치일시	※ 조치부서 조치일시				
조치기한	0 일		**조치소요기간**	0 일	
조치기한 초과사유	※ 해당 시 작성				
피해내용	※ 해당 시 작성				
조치결과 (예정사항 포함)					

<시스템 분류 목록>

기호	시스템 분류	설 명
가	웹서버	기관의 홈페이지 운영 및 웹서비스를 제공하는 서버
나	전자우편 서버	전자우편 송수신을 위해 운영하는 서버
다	DB/업무서버	홈페이지 및 업무지원을 위한 데이터베이스 서버
라	개발/임시서버	개발 및 운영 테스트를 위하여 사용하는 임시 서버
마	통신전송장비	라우터, 스위치 등 통신전송장비 일체
바	보안장비	방화벽, IDS, VPN 및 백신서버 등 정보보안제품 일체
사	개인/업무PC	기관내 사용자의 PC
아	교육/임시PC	교육장 또는 공용 작업을 위해 여러 명이 사용하는 PC
자	기타	위의 시스템 용도에 없는 경우 서술식으로 기술

<사고 유형 목록>

기호	시스템 분류	설 명
A	경유지 악용	타기관의로부터 해킹시도 항의를 받았거나, 시스템 점검 중 해킹흔적 또는 해킹 툴이 설치되어 타 시스템에 접속한 기록이 발견되었을 경우
B	자료훼손 및 유출	내부 시스템의 자료가 변조가 되었거나, 대량의 데이터가 외부로 무단 송신된 흔적이 발견되었을 경우
C	단순침입 시도	지속적인 스캐닝 공격이 발생할 경우
D	웜바이러스 피해	기관내의 PC에서 웜바이러스가 발견되었을 경우
E	홈페이지 변조	기관의 홈페이지가 변조되었을 경우
F	홈페이지 접속 불가능	기관의 홈페이지 서버 또는 네트워크 이상으로 인해 홈페이지 접속이 불가능 할 경우
G	서비스거부공격 피해	불특정 다수의 IP로부터 접속시도 또는 대량 트래픽이 일시에 유입될 경우
H	시스템 파괴	내부 시스템의 자료가 삭제되어 사용이 불가능한 경우
I	기타	위의 사고유형에 포함되지 않을 경우 서술식으로 기술

[별지 제5호서식]

비밀유지 서약서

기 관 명	부 서 명
직 위	성 명
생년월일	주 소

상기 본인은 건강보험심사평가원 「사이버보안 관제센터 운영지침」 제19조제2항에 따라 사이버보안 관제센터에 근무하는 동안에 지득한 비밀 및 중요 사항에 대해 근무기간은 물론이고 퇴직 후에도 제3자에게 공개하거나 누설하지 아니하며 이를 위반 시 민·형사상의 모든 책임을 다할 것임을 엄숙히 서약합니다.

년 월 일

성 명 : (서명 또는 인)

사이버보안관제센터장 귀하

210㎜×297㎜[백상지(80g/㎡) 또는 중질지(80g/㎡)]