특수한 유형의
부가통신사업자(인터넷문자)
등록요건 및 등록서류 작성 요령

2026. 7.20.

과학기술정보통신부
중앙전파관리소

개정이력

순번	개정일	변경내용	발간부서	연락처
1	2023.9.5.	개정	중앙전파관리소 전파보호과	-
2	2026.7.20.	개정	중앙전파관리소 전파보호과	-

□ 개 요

특수한 유형의 부가통신사업자(인터넷 문자)를 경영하고자 하는 자는「전기통신사업법」제22조(부가통신사업의 신고 등) 및「전기통신사업법 시행령」 제29조(부가통신사업의 신고절차 등)에 따른 등록요건을 갖추어 중앙전파관리소에 등록신청을 해주셔야 합니다.

□ 특수한 유형의 부가통신사업자의 등록요건(시행령 제29조제9항, 별표3)>

<법 제2조제14호 나목에 해당하는 특수한 유형의 부가통신사업자(인터넷발송 문자)>

구분	등록 요건
가. 기술적 조치 실시 계획	1) 법 제84조의2제3항에 따른 이용자의 피해를 예방하기 위한 조치로서 다음 각 목의 기술적 조치를 할 것 가) 타인의 명의를 도용한 부정가입 방지 나) 문자메시지의 발신번호 등록·관리 다) 거짓으로 표시된 전화번호의 문자메시지 차단 라) 문자메시지 발송 및 재전송에 관한 통신이력을 1년 이상의 기간을 정하여 유지·보관 마) 문자메시지 발송 시 식별코드 삽입 바) 문자메시지 전달 과정에서 식별코드의 위·변조 방지 2)「정보통신망 이용촉진 및 정보보호 등에 관한 법률」제45조제1항에 따른 정보통신망의 안정성 및 정보의 신뢰성 확보를 위하여 다음 각 목의 보호조치를 할 것 가) 정보보호시스템의 설치·운영 나) 정보통신망 및 시스템의 취약점 점검 다) 접근통제 및 보안설정 관리 라) 로그기록 자료 유지 3)「정보통신망 이용촉진 및 정보보호 등에 관한 법률」제49조의2제1항에 따른 속이는 행위에 이용된 문자메시지 식별 및 차단 관련 기술적 조치를 할 것

나. 인 력 및 물적 시설	1) 부정가입 방지, 발신번호 등록·관리, 거짓으로 표시된 전화번호의 문자메시지 전달경로 확인·제공 및 이를 송신한 자의 해당 회선에 대한 전기통신역무 제공의 중지 등을 위해 대표자를 제외한 전담직원을 별도로 1명 이상 둘 것 2) 임원급 또는 부서장급 이상의 정보보호 최고책임자를 지정·공표할 것 3) 특수한 유형의 부가통신역무를 원활하게 제공하고, 법 제22조제2항제1호의2에 따른 기술적 조치 실시 계획을 이행하는 데 필요한 전기통신설비와 각종 부대장비를 갖출 것
다. 재무 건전성	납입자본금(개인인 경우는 영업용 자산평가액을 말한다) 1억원 이상
라. 사업 계획서	인원·시설 등 일반 현황, 사업개요, 사업추진방향, 매출방안, 향후 사업추진계획 등을 포함할 것
마. 이용자 보호 계획서	1) 다음의 내용을 포함하는 이용자 보호계획서를 작성할 것 가) 개인정보 보호를 위한 내부관리계획 나) 다음의 내용을 포함하는 서비스 약관 (1) 이용자 불만형태별 처리절차 및 처리기간 (2) 서비스제공이 불가능한 경우의 처리방안 (3) 거짓으로 표시된 전화번호를 송신한 자의 해당 회선에 대한 전기통신역무 제공의 중지를 위한 처리방안 (4) 부정가입 방지, 발신번호 등록·관리 등에 대한 사업자·이용자의 의무 및 그 밖의 기타 이용자 고지 사항 등 2) 그 밖에 과학기술정보통신부장관이 정하여 고시하는 이용자 보호기준에 적합한 것을 증명하는 서류를 제출할 것
바. 전송 자격 인증서	방송미디어통신위원회가 발급한 전송자격인증서를 제출할 것

1. 기술적조치 계획

1.1. 전기통신사업법」 제84조의2제3항에 따른 이용자의 피해를 예방하기 위한 다음 각목의 기술적 조치를 할 것

항목	타인의 명의를 도용한 부정가입을 방지하기 위한 기술적 조치
제출 서류	▸**증빙자료 ① : 타인의 명의를 도용한 부정가입을 방지하기 위한 기술적 조시 실시 계획서 및 본인확인을 위한 공인 인증업체와의 계약서 사본(별다른 양식없이 자율적으로 기재)** o 고객사 회원가입 시 본인인증 절차를 설명하고, 제출받는 서류는 무엇인지 명시할 것 - 계약시 업체확인(본인확인) 절차와 제출받는 서류목록(예 : 법인등기사항증명서, 사업자등록증, 인감, 통신서비스이용증명원, 신분증 등)을 기재 - "종이 신청서"인지 "온라인 폼(form)"으로 가입을 받는지 가입 방식 기재 : "종이 신청서"의 경우 신청서/계약서 양식(개인정보 수집·이용 및 위탁, 제공동의서 포함)을 첨부 - "온라인 폼(form)"의 가입방식일 경우 해당 홈페이지(URL포함) 캡쳐본을 첨부 ★ 대면계약(서류계약) 시 귀사와 고객사 간의 대면계약을 위한 신청서* 양식을 첨부할 것 * 대면계약을 위한 신청서란 휴대폰본인인증 외 일반전화(회사)의 명의일치 여부(본인인증)를 확인하기위해 대면(혹은 온라인)으로 문자계약을 위한 신청서를 받을 경우 이용하는 양식(온라인 폼(form))을 말하며 사본이나 캡쳐본 제출 예) 고객사의 담당자가 개인 명의 휴대폰으로 휴대폰본인인증 절차를 거쳐 회원가입 한 뒤 자사의 고객센터로 사업자등록증, 통신서비스이용증명원, 신분증, 재직증명서 등을 제출하면 확인 후 고객사의 대표번호를 등록한다. 예) 자사와 고객사가 대면 계약을 진행 → 계약 시 신분증, 재직증명서 등, 사업자등록증, 통신서비스이용증명원 제출 → 서류 확인을 마치면 자사 담당자가 회원 계정을 만들어회원에게 부여한다. ▶ **증빙자료 ② : 사업자의 서비스 화면에 인증 방법이 표시가 되어 있는 화면을 캡처한 자료 제출** o 관련증빙자료(홈페이지 캡처, 인증 관련 서비스 적용 화면 등)는 서비스 URL이 표시된 캡처만 유효 o 아이핀(I-PIN)은 한국인터넷진흥원 또는 한국인터넷진흥원에서 인정하는 사업자가 운영하는 아이핀 서비스만 해당 휴대폰 본인인증 캡쳐화면 

휴대폰 본인인증	I-PIN 인증
	

<table>
<tr><th>항목</th><th>문자메시지의 발신번호를 등록·관리하기 위한 기술적 조치</th></tr>
<tr><td rowspan="2">제출
서류</td><td>▶ 증빙자료 ③ : 문자메시지의 발신번호 등록·관리를 위한 기술적 조치 실시계획서
o 귀사의 발신번호 등록 절차와 방법을 명시할 것
예) o 통신서비스 이용증명원 서류 제출을 통한 발신번호 사전 등록 방법
- 통신서비스이용증명원 수령 -> (문자발송 서비스 이용) 계약서와 고객의 통신서비스이용증명원 상의 명의자 정보 일치 여부 확인 -> 일치하면 <u>담당자가 해당 발신번호로 직접 전화를 걸어 본인인지 여부를 확인</u> -> 발신번호 등록

o 회원가입 시 본인 인증한 명의와 발신번호 등록 시 인증한 명의자가 다를 경우 발신번호 명의자가 이용자에게 발신번호로 사용해도 된다는 승낙서(위임장) 등 추가 서류 인증을 통해 발신번호 등록을 진행</td></tr>
<tr><td>▶ 증빙자료 ④ : 문자메시지의 발신번호 등록·관리가 적용된 사업자의 서비스 화면을 캡처한 자료 제출
o 발신번호를 등록·관리하기 위한 기술적 조치 증빙자료(관리자 페이지 첨부필요)
- 관리자의 회원사 발신번호 등록화면(등록/심사중/거부 등)을 캡쳐하여 첨부할 것
- 발신번호로 ID, 이용자명, 발신일 등을 조회할 수 있도록 조치하고, 캡처 화면을 첨부할 것
- 발신번호 등록 인증 관련 서비스 적용 화면 캡처 시 사업자의 서비스 URL이 포함되어야 한다.
(예시) 발신번호 등록 방법화면
 

(해당 이미지는 AI를 활용하여 생성되었습니다.)
(예시) 발신번호 등록 관리화면(승인, 보류, 대기, 삭제 등)
 

(해당 이미지는 AI를 활용하여 생성되었습니다.)</td></tr>
</table>

▶ **증빙자료 ⑤ : 사전에 등록된 번호 이외의 발신번호를 사용하는 문자메시지 차단을 위한 기술적 조치 내용 및 적용된 화면을 캡처한 자료 제출**

(예시) 설명
ㅇ 등록(인증)된 번호로만 발신됨을 증명 - 문자 발송 서비스 화면에서 사전에 등록된 전화번호 외에 임의로 번호 수정/변경이 불가능함을 설명할 것(발신번호를 임의로 입력할 수 없고 등록된 번호를 선택하도록 하는 등) 예) 사전에 등록된 번호 이외의 발신번호를 사용하여 문자메시지를 발송하려는 경우 오류 팝업, 콤보박스 표출 등 기술적조치를 실시하고 있음을 설명할 것
(예시) 증빙화면(서비스 URL이 포함되도록 캡처)

항목	거짓으로 표시된 전화번호의 문자메시지 차단을 위한 기술적 조치

제출 서류

▶ 증빙자료 ⑥ : 거짓으로 표시된 발신번호의 문자메시지 차단을 위한 기술적 조치 실시계획서

(예시) 설명

○ 아래의 발신번호 규격에 맞지 않은 전화번호를 차단하는 번호 필터링 규칙을 적용하고 있다는 내용을 포함하여 거짓으로 표시된 전화번호로 문자발송을 한 회원 계정에 대한 문자발송 차단을 위한 조치 내용을 설명할 것

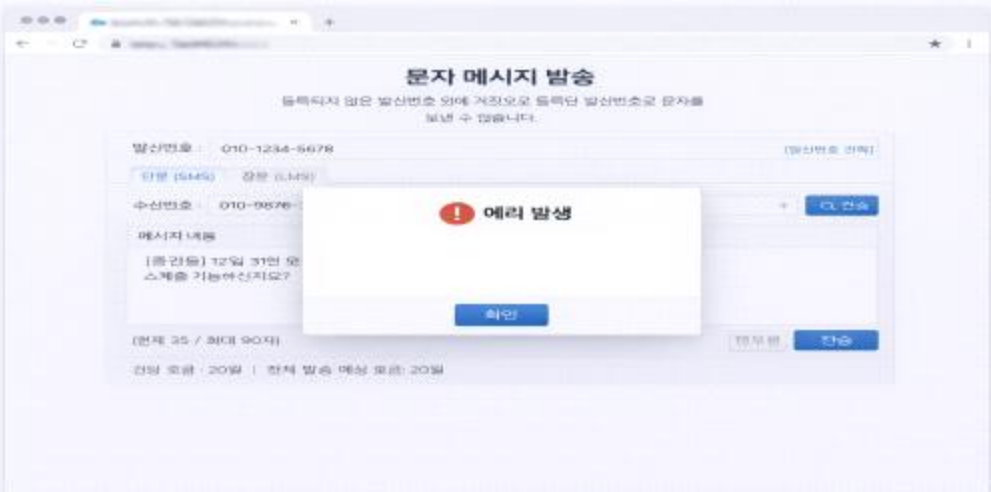
구 분	종 류
기본 원칙	- 발신번호의 전체 번호수가 8~11자리인 경우에만 문자메시지 발송
예외 사항	- 발신번호가 112, 1335 등 특수번호인 경우에는 해당 이용자(국가, 지자체, 공공기관 등)에 한해서만 문자메시지 발송 - 발신번호가 15YY, 16YY 등 대표번호 서비스인 경우에는 전체 번호 수가 8자리에 한해서만 문자메시지 발송 - 발신번호가 030, 050으로 시작하는 경우에는 전체 번호수가 12자리까지 한해서 문자메시지 발송 - 고시 제3조제1항 제6호에 따라 과기부장관이 승인한 전화번호

※ 참고: 과기정통부고시 제2022-7호(2022.3.2.) 거짓으로 표시된 전화번호로 인한 이용자의 피해 예방 등에 관한 고시

▶ 증빙자료 ⑦ : 거짓으로 표시된 발신번호의 문자메시지 차단을 위한 적용된 서비스 화면을 캡처한 자료 제출

(예시) 증빙화면(사업자의 서비스 URL이 포함되어야 함)

○ 거짓으로 표시된 전화번호로 문자발송을 한 회원 계정에 대한 문자발송 서비스 차단화면 캡처 (해당 회원 계정으로 등록된 전화번호로 문자메시지가 발송될 경우 차단 안내문, 에러메시지 등이 나오는 화면을 캡처)

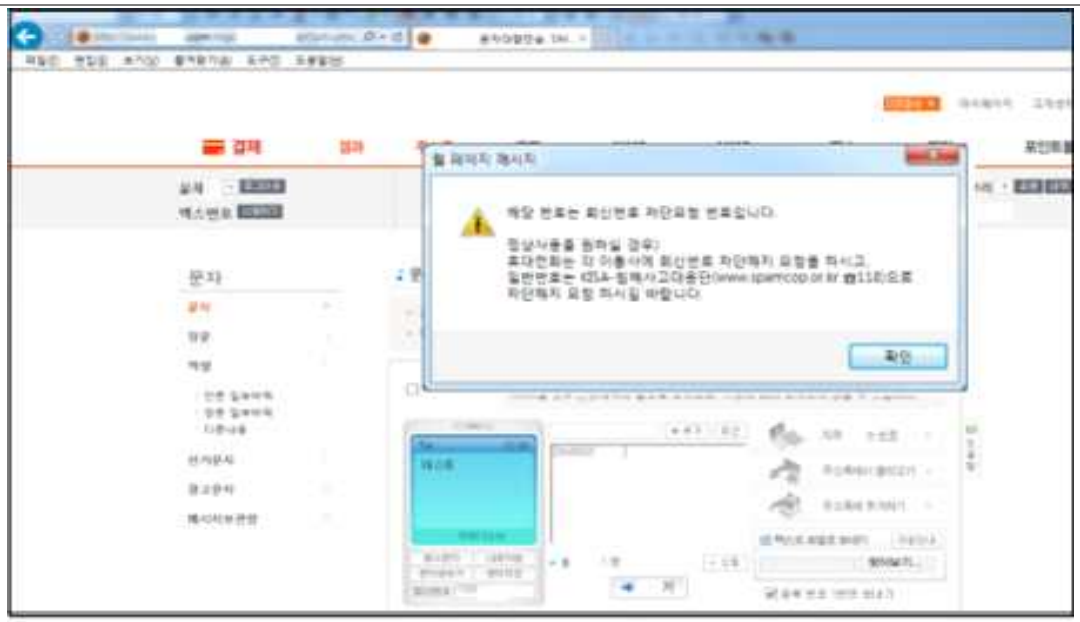


(해당 이미지는 AI를 활용하여 생성되었습니다.)

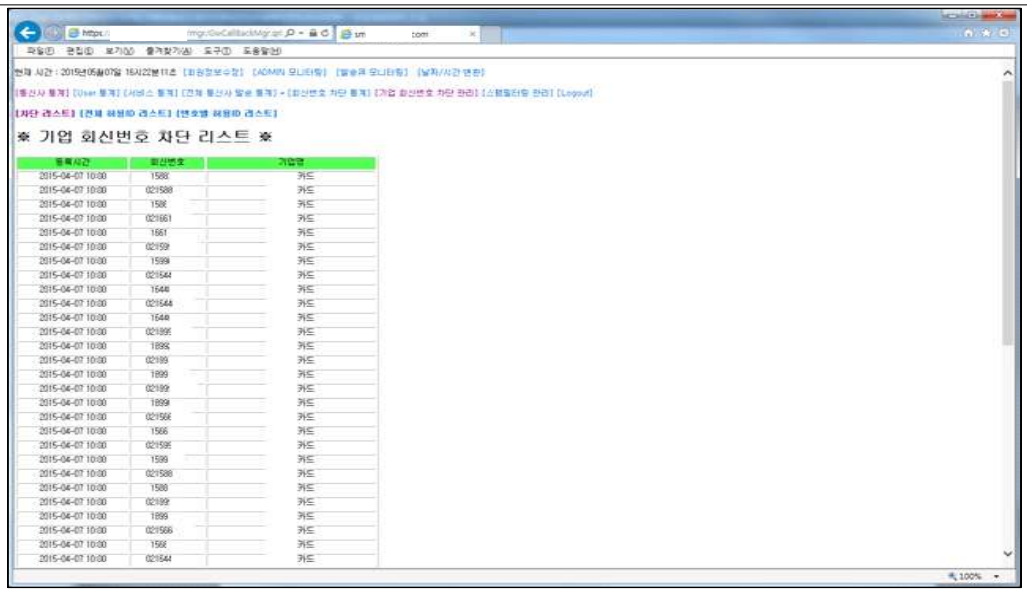
	▶ **증빙자료 ⑪ : 한국인터넷진흥원(KISA)의 사칭전화 신고 관리 시스템에 업체 및 담당자가 등록된 화면을 캡처한 서류 제출(사업자가 KISA에 등록하여야 함)** ㅇ '담당자 정보 목록' 메뉴에서의 사용중인 식별코드 정보까지 나오게 화면 캡쳐 ㅇ '소속 기관 담당자 목록' 메뉴의 정보가 특수부가통신사업 등록시 제출한 담당자와 동일하여야 함 ㅇ 등록된 담당자는 현행으로 관리(특수한 유형의 부가통신사업 변경등록 포함)하여야 하며, 전화번호 거짓표시 신고건 확인 및 답변을 위해 매일 1회 이상 접속 권고 (예시) 담당자 정보(사용중인 식별코드 정보 나오게)캡처화면  (예시) 소속기관 담당자 목록 
항목	**거짓으로 표시된 전화번호의 문자메시지 차단을 위한 기술적 조치 (문자중계사 추가 제출 증빙자료 8~10)**
제출 서류	**[문자중계사*인 경우만 제출] 증빙자료 ⑧** * 문자 중계사는 이통사와 직접 계약한 업체인 경우에 해당 ▶ **증빙자료 ⑧ : 문자중계사업자는 거짓으로 표시된 전화번호가 인터넷발송 문자메시지의 발신 번호로 사용된 경우 이를 차단하기 위한 기술적 조치가 적용된 화면을 캡처한 자료 제출** ㅇ 변작 등 거짓으로 표시된 발신번호 차단 관리 캡처 화면에는 사업자의 URL 또는 자사 시스템 여부가 표시(로고 등) 되어야 한다. ㅇ 변작 등 거짓으로 표시된 발신번호 차단 관리 화면이 없을 경우, 시스템에서 관리하고 있는 변작 등 거짓으로 표시된 발신번호 차단 목록(한국인터넷진흥원에서 제공)을 제출

(예시) 변작 등 발신번호 차단 적용 화면

변작된 발신번호를 사용할 경우 문자메시지 발송 차단이 적용된 화면



변작된 발신번호 사용에 대한 차단 화면은 사업자의 URL이 포함된 화면



[문자중계사인 경우만 작성] 증빙자료 ⑨, ⑩

▶ 증빙자료 ⑨ : 문자중계사업자는 변작번호 차단 결과 전송을 위한 기술개발 용역서 (계약서) 사본(직접 개발한 경우 관련 기술개발 규격서 등 관련 증빙자료)

별도 파일 제출필요

▶ 증빙자료 ⑩ : 문자중계사업자는 차단 결과 전송을 위하여 한국인터넷진흥원과 시스템 연동이 되어 있는 로그 자료 제출

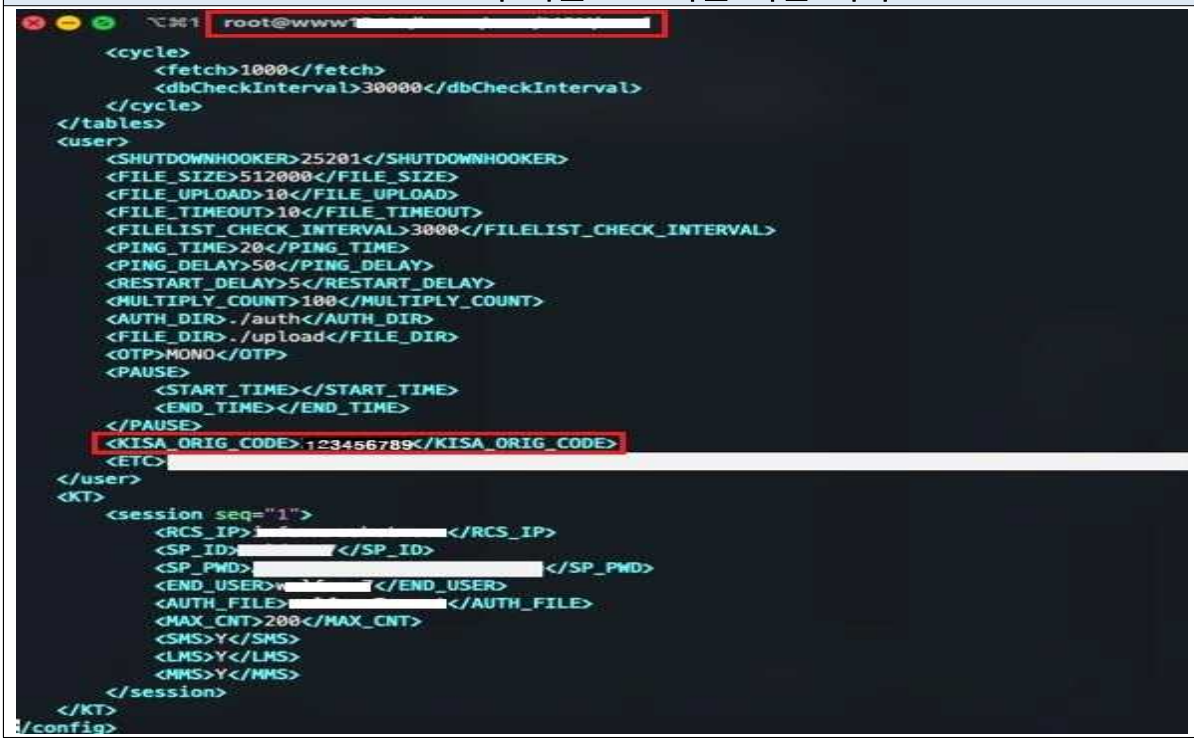
<table>
<tr><td>항목</td><td>문자메시지 발송 및 재전송에 관한 통신이력을 1년 이상의 기간을 정하여 유지·보관하기 위한 기술적 조치</td></tr>
<tr><td>제출 서류</td><td>
▶ 증빙자료 ⑫ : 문자메시지 발송 및 재전송에 대한 통신 이력을 1년 이상 보관 및 관리하기 위한 기술적조치 실시 계획서
<table>
<tr><td>(예시) 설명</td></tr>
<tr><td>ㅇ 귀사가 문자메시지 발송 및 재전송에 관한 통신이력을 보관하는 기간을 명시</td></tr>
</table>

▶ 증빙자료 ⑬ : 문자메시지 통신이력을 1년 이상 보관·관리하기 위한 조치
<table>
<tr><td>(예시) 증빙화면 (1년 이상 보관 여부)</td></tr>
<tr><td>ㅇ 통신이력 포함 항목 : 계정ID, 이름, 인적사항 등(증빙화면의 개인정보는 공백 처리)
ㅇ 문자발송 및 재전송에 관한 통신이력이 없는 경우(신규 등록)에도 통신이력의 조회가 가능함을 증빙하는 화면을 캡처(화면 캡처 시 URL이 포함되어야 한다.)
(예시 : 2025.01.01.~2026.01.01. 내역)
 

(해당 이미지는 AI를 활용하여 생성되었습니다.)</td></tr>
</table>
</td></tr>
</table>

항목	문자메시지 발송 시 식별코드 삽입
제출 서류	▶ **증빙자료 ⑭ : 인터넷 문자발송 장비(시스템) 내 식별코드 적용 화면 캡처** ※ 적용여부 확인을 위한 임시 식별코드(123456789)를 사용 ※ 임시 식별코드(123456789)는 인터넷 문자 발송 불가능(중계사 차단) ※ 화면 캡처 시, 사업자의 URL 또는 자사의 시스템 인지 여부가 표시(로고 등) 되어야 함

소스코드 내 식별코드 확인 화면 예시



문자발송 이력(로그) 내 식별코드 확인 화면 예시

<table>
<tr><td>항목</td><td>문자메시지 전달 과정에서 식별코드의 위·변조 방지</td></tr>
<tr><td>제출
서류</td><td>▶ 증빙자료 ⑮ : 문자사업자는 ‘인터넷 문자발송 현황’ 자료 제출(증빙자료 지정서식⑮)
<table><tr><td>문자사업자 인터넷 문자발송 현황</td></tr><tr><td>붙임1 서식</td></tr></table></td></tr>
</table>

1.2. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」제45조제1항에 따른 정보통신망의 안정성 및 정보의 신뢰성 확보를 위하여 다음 각 목의 보호조치를 할 것

항목	정보보호 기술적 조치
제출서류	▶ 증빙자료 ⑯ : 붙임4~21번까지 서식 등 포함 기술적 조치 계획서 제출

구 분			세 부 조 치 사 항
기술적 보호조치	네트워크 보안	정보보호시스템 설치.운영	▸ 외부망과 연계되는 구간에 침입차단시스템, 침입탐지시스템 등 네트워크의 안전성을 제고할 수 있는 정보보호시스템을 설치.운영
	정보통신설비 보안	취약점 점검	▸ 연 1회 이상 취약점 점검을 실시하고 발견된 취약점을 보완
		접근통제 및 보안설정 관리	▸ 인가된 자만 시스템에 접속할 수 있도록 설정하고, 인터넷 등을 통해 외부에서 접속할 경우 일회용 패스워드 사용 등 인가 절차를 강화 ▸ 불필요한 프로토콜 및 서비스 제거 등 보안설정
		로그 관리	▸ 최소 1개월 이상 로그기록 유지.관리(정보보호시스템은 3개월)

※ 1) 단순 문자 재판매사업자*는 '접근통제·보안설정'부문만 작성하시고, 나머지 정보보호 시스템설치.운영, 취약점점검, 로그관리 등은 '해당없음'으로 표기하고 그 부분을 담당하고 있는 사업자 또는 이용하고 있는 사업자와의 사실 및 관련 증빙(계약서, 시스템 연동·적용 화면 등)을 함께 기재·제출하여 주시기 바랍니다.

* 예시: 자체 문자발송시스템이 없이 상위 사업자의 문자발송 API 및 솔루션을 사용하는 사업자

2) 통신망 구조 및 네트워크 구성도에 따라, 사업자의 위치에 따라 해당하지 않는 부문은 "해당없음"으로 표기하고, '해당 부문의 역할을 수행하는 사업자(예: ○○○사업자)와 그 사업자의 시스템을 활용·이용하고 있음' 이라고 기재하여 주시기 바랍니다.

사업자별 정보보호 기술적조치 제출서류에 대한 세부 문의는 한국정보통신진흥협회 정보통신시험인증본부 정보보호인증심사팀으로 연락주시기 바랍니다.

(☎ 02-580-0626)

구분	정보보호시스템 설치 · 운영
세부조치사항	▸ 외부망과 연계되는 구간에 침입차단시스템, 침입탐지시스템 등 네트워크의 안전성을 제고할 수 있는 정보보호시스템을 설치 · 운영
세부점검사항	① 외부망과 연계되는 모든 구간에 침입차단시스템(방화벽)이 설치·운영되고 있는가?
	② 웹서버 보호를 위한 정보보호시스템(웹방화벽 또는 웹쉘탐지)과 데이터베이스 보안솔루션(DB접근통제 또는 DB암호화)이 설치·운영되고 있는가?
	③ 침입차단시스템, 웹방화벽에는 적절한 정책이 반영되어 있는가?
	④ 정보보호시스템의 부하분산 방안을 수립하여 적용하고 있는가?
세부설명	【설 명】 ① 외부망과 연계되는 모든 구간에 침입차단시스템(방화벽)이 설치·운영되고 있는가? • 외부망과 연계되는 구간에 반드시 침입차단시스템(방화벽)을 설치하여야 한다. • 침입차단시스템(방화벽) 운영을 담당할 담당자를 지정하여야 한다. • 침입차단시스템(방화벽)의 보안정책 수립 등 관리를 위한 접근은 담당자로 제한하여야 한다. • 방화벽은 S/W방화벽 또는 H/W방화벽을 설치하여 운영할 수 있다. ※ 서버의 운영체제에서 제공하는 iptable을 이용한 접근통제는 허용되지 않음 ② 웹서버 및 데이터베이스 보호를 위한 정보보호시스템(웹방화벽 또는 웹쉘탐지, DB접근통제 또는 DB암호화)이 설치.운영되고 있는가? • 웹서버 및 데이터베이스 보호를 위한 정보보호시스템을 반드시 설치하여야 한다. • 정보보호시스템을 운영을 담당할 담당자를 지정하여야 한다. • 정보보호시스템에 대한 보안정책 수립 등 관리를 위한 접근은 담당자로 제한하여야 한다. • 웹방화벽은 S/W 웹방화벽 또는 H/W 웹방화벽을 설치하여 운영할 수 있다. • 웹서버가 제공하는 자체 웹방화벽(예: 아파치가 제공하는 ModSecurity 등)을 사용할 수 있다. • KISA에서 제공하는 무료 웹쉘탐지제품(휘슬(WHISTL))을 사용할 수 있다. ③ 침입차단시스템(방화벽), 웹방화벽, 웹쉘탐지, DB접근통제, DB암호화에 적절한 정책이 반영되어 있는가? • 침입차단시스템(방화벽), 웹방화벽, 웹쉘탐지, DB접근통제, DB암호화 운영 시 웹 하드 서비스에 적절한 보안정책을 적용하여야 한다. • 특히, 외부망(인터넷망)에서 내부망으로 접근하는 패킷에 대한 필터링 정책은 가능한 제한해야 한다. • 꼭 필요한 서비스나 프로토콜에 대해서만 허용하는 정책을 적용해야 한다.

	※ 출발지(any), 목적지(any), 서비스(all), 정책(allow)은 지양해야 함 • 외부에서의 접근 뿐 아니라 내부망과의 통신에 대한 정책도 수립하여야 한다. • 인터넷망에서 내부망으로의 접근은 모두 차단하여야 하며, 웹서버, 백업서버, 관리자의 접근만 허용하여야 한다. • 특히, 내부망으로 접근을 허용하는 정책의 경우 접근하는 IP, Port, 프로토콜, 접근시간 등에 기반하여 상세한 접근통제 정책을 적용하여야 한다. • 방화벽 등 정보보호제품 운영을 위탁하여 운영하는 경우 방화벽 정책 업데이트 관련 절차를 마련하고 관련 증적(업데이트 요청, 업데이트 확인 등)을 보관하여야 한다. ④ 정보보호시스템의 부하분산 방안을 수립하여 적용하고 있는가? • 주요회선의 소통량에 따라 과부하에 대비한 부하분산 방안을 수립하여 적용하여야 한다. • 부하분산 방안으로 로드밸런싱 및 이중구조의 사용 등이 적용될 수 있다. **【증빙자료】** • **침입차단시스템(방화벽), 웹방화벽, 웹쉘탐지, DB접근통제, DB암호화 등 정보보호시스템 목록 및 네트워크 구성도 (☞ [붙임 5] 네트워크 구성도, [붙임 18] 정보보호시스템 운영 현황 종합표 참조)** • **방화벽(웹방화벽) 정책(Rule Set) 증적 (☞ [붙임 6] 방화벽 정책, [붙임 7] WAF 정책 참조)** • **IPS/IDS 설치·운영 현황 (☞ [붙임 11] IPS/IDS 운영현황표 참조)** • **방화벽, 웹방화벽, 웹쉘탐지, DB접근통제, DB암호화 등의 업데이트 현황 (☞ [붙임 17] 부하분산 구성 현황표 참조)** **※ 특히, 웹방화벽 및 웹쉘탐지의 경우 최신 패턴에 대한 업데이트 이력**

구분	취약점 점검
세부 조치 사항	▸ 연 1회 이상 취약점 점검을 실시하고 발견된 취약점을 보완
세부 점검 사항	① 연 1회 이상 웹 어플리케이션, DBMS, 운영체제, 네트워크 장비 취약점 점검을 수행하고 있는가?
	② 취약점 점검 결과는 정보보호책임자에게 보고되고 있는가?
	③ 취약점 점검으로 파악된 취약점에 대한 적절한 조치 및 해결방안이 마련되어 적용되고 있는가?
	④ 취약점 점검 결과는 DB, 보고서 등의 형태로 기록·보관하고 있는가?
세부 설명	【설 명】 ① 연 1회 이상 웹 어플리케이션, DBMS, 운영체제, 네트워크 장비 취약점 점검을 수행하고 있는가? • 웹 어플리케이션(모바일 사이트 포함), DBMS, 운영체제, 네트워크 및 정보보호시스템, 관리용 PC 등 정보통신설비 목록 내 장비에 대하여 연 1회 이상 취약점 점검을 실시하고, 취약점 점검 시 발견한 취약점에 대해서 보완하여야 한다. ※ 웹 및 모바일 사이트에서 사용자 계정 정보 등 중요 정보가 암호화되어 전송되어야 한다. • 웹 어플리케이션에 대한 취약점은 KISA에서 제공하는 원격 웹 취약점 점검서비스를 활용하거나 자체적인 점검 또는 취약점 점검 전문기관(컨설팅 업체 등)을 활용하여 실시할 수 있다. • 웹 어플리케이션 취약성 점검 수행 시 OWASP의 10대 취약성, 국정원 8대 취약점 등을 참조하여 수행할 수 있다. • 자체적인 취약점 점검 수행 시 별첨으로 제공되는 “취약성 점검 항목 및 가이드”를 참고한다. • DBMS·운영체제·네트워크 장비에 대한 취약점 점검 범위는 "취약성 점검 항목 및 가이드"에 명시된 해당 점검항목을 포함하여야 한다. • 정보통신설비 또는 정보보호시스템을 위탁하여 운영하는 경우 위탁업체의 정기 점검 보고서, 취약점 점검 및 보완 결과 등으로 대체할 수 있다. ② 취약점 점검 결과는 정보보호책임자에게 보고되고 있는가? • ①항, ③항에서 실시한 취약점 점검에 대한 결과보고서, 보완조치 완료보고서는 보고서의 형태로 운영기관의 정보보호에 대한 책임이 있는 자(정보보호책임자 또는 정보보호관리자 등)에게 보고되어야 한다. • 보고서는 전자파일 또는 하드카피 형태의 보고서 형식이어야 한다.

	③ 취약점 점검으로 파악된 취약점에 대한 적절한 조치 및 해결방안이 마련되어 적용되고 있는가? • ①항의 취약점 점검에서 도출된 취약점을 보완/제거를 위한 계획을 수립하고 수립된 계획에 따라 보완조치를 수행해야 한다. • 보완조치 완료 후 해당 취약점이 보완/제거되었는지 점검하여야 한다. ④ 취약점 점검 결과는 DB, 보고서 등의 형태로 기록·보관하고 있는가? • 취약점 점검결과 보고서, 보완조치 완료보고서는 전자파일 형태로 보관 또는 하드카피 보고서 형태로 일정기간(2년) 이상 보관하여야 한다. 【참 고】 • 참고(https://www.crms.go.kr/lay1/S1T60C62/contents.do 하단) **【증빙자료】** • **정보통신설비 목록(서버, 네트워크 장비, 정보보호시스템, DB, 관리용 PC, 개발용 PC, 웹 어플리케이션 등) (☞ [붙임 4] 정보통신설비 목록 또는 [붙임 10] 정보통신설비(자산) 목록 대장-확장, [붙임 19] 네트워크 장비 관리자 IP 관리대장, [붙임 20] 네트워크 장비 주기적 점검기록 [위탁 관리용] 참조)** • **취약점 점검 결과보고서 (☞ [붙임 12] 취약점 점검 결과 보고서 참조)** • **취약점 보완조치 완료보고서 (☞ [붙임 13] 보안 패치 이력 관리대장 참조)** • **패치현황 및 보안패치 중단된 운영체제 교체 계획 수립 이행 현황** • **위탁업체의 취약점 정기점검 보고서(반기/년간) (☞ [붙임 21] 위탁업체 취약점 정기점검 보고서 양식 [반기/년간])** • **업데이트를 위한 유지보수 계약**

구분	접근통제 및 보안설정 관리
세부 조치 사항	▸ 인가된 자만 시스템에 접속할 수 있도록 설정하고, 인터넷 등을 통해 외부에서 접속할 경우 일회용 비밀번호 사용 등 인가 절차를 강화
세부 점검 사항	① 정보통신설비는 인가된 접속지로부터 인가된 사용자만 접속할 수 있도록 통제되고 있는가?
	② 인가된 사용자만 정보통신설비에 접속할 수 있는지 주기적으로 점검하고 있는가?
	③ 인터넷 등을 통해 외부에서 접속할 경우 안전한 채널(SSH, SSL 또는 VPN), 일회용 패스워드(OTP) 등을 사용하고 있는가?
	④ 정보통신설비에서 서비스를 제공하기 위해 반드시 필요한 프로토콜을 제외한 프로토콜 및 서비스는 중지하거나 제거하고 있는가?
세부 설명	【설 명】 ① 정보통신설비는 인가된 접속지로부터 인가된 사용자만 접속할 수 있도록 통제되고 있는가? • 정보통신설비에 대한 자산이 조사되고 관리 및 유지되어야 한다. • 정보통신설비는 인가된 사용자 접근만 가능하도록 통제하여야 한다. • 정보통신설비는 인가된 사용자만을 허용하기 위하여 계정/비밀번호를 반드시 설정하여야 한다. • 퇴사자, 보직이동 등으로 인가된 사용자의 변경이 발생한 경우 계정 삭제, 접근 IP 변경을 통하여 비인가된 사용자의 접근을 차단하여야 한다. • 유지보수 등을 위하여 물리적으로 시스템에 접근하여 콘솔로 연결하는 경우 반드시 관리자가 동행하여 유지보수 직원의 작업내역을 확인하여야 하며, 유지보수 등을 위한 별도의 계정을 발급하고 유지보수용 계정에 과도한 권한을 부여하지 않아야 한다. • 유지보수용 계정의 경우 평소에는 계정을 중지시키거나 삭제하여 사용하지 못하도록 하고, 필요시에 관리자의 허락 하에 사용할 수 있도록 한다. ② 인가된 사용자만 정보통신설비에 접속할 수 있는지 주기적으로 점검하고 있는가? • 비인가된 사용자의 접근을 확인하기 위하여 접근이력을 주기적(월1회)으로 검토하여야 한다. • 침입차단시스템의 로그를 기반으로 정보통신 접근이력을 검토하고, 운영체제가 제공하는 로그를 검토하여 비인가자의 접근이 시도되었는지 검토하여야 한다. ③ 외부망에서의 직접적인 접근은 원칙적으로 금지하며, 불가피하게 인터넷 등을 통해 외부에서 접속할 경우 안전한 채널(SSH, SSL 또는 VPN), 일회용 패스워드(OTP) 등을 사용하고 있는가? • 네트워크를 통해 접속하는 경우 VPN, SSH, SSL을 사용하여 안전한 통신채널을 확보하여야 한다. • 필요할 경우 추가적인 사용자 인증 수단으로 일회용 패스워드(OTP)를 사용할 수 있다.

	④ 정보통신설비에서 서비스를 제공하기 위해 반드시 필요한 프로토콜을 제외한 프로토콜 및 서비스는 중지하거나 제거하고 있는가? • 각 서버(웹서버, DB서버, 백업서버, 어플리케이션 서버)는 각 용도를 제외한 서비스 및 프로토콜을 제거하거나 해당 서비스를 중지시켜야 한다. **【증빙자료】** • **정보통신설비 목록 (☞ [붙임 10] 정보통신설비(자산) 목록 대장-확장 참조)** • **계정/비밀번호 관리대장 (☞ [붙임 9] 계정·비밀번호 관리대장 참조)** • **서버별(웹서버, DB서버, 백업서버, 웹 어플리케이션 서버 등) 서비스 포트 현황 (☞ [붙임 8] 서버별 서비스 포트 현황표 참조)** • **접근권한(사용자) 관리대장 (☞ [붙임 14] 접근권한 관리대장 참조)** • **정보보호시스템 정기점검 보고서**

구분	로그 관리
세부 조치 사항	▸ 최소 1개월 이상 로그기록 유지.관리(정보보호시스템은 3개월)
세부 점검 사항	① 정보통신설비의 침입시도 및 이상징후 등에 대해 분석하고 능동적으로 대응하기 위해 기록 관리되어야 할 중요 로그가 식별되어 있는가?
	② 정보통신설비의 식별된 중요 로그는 1개월 이상 보존.관리되고 있는가?
	③ 정보보호시스템의 로그는 3개월 이상 기록·관리되고 있는가?
세부 설명	**【설 명】** ① 정보통신설비의 침입시도 및 이상징후 등에 대해 분석하고 능동적으로 대응하기 위해 기록 관리되어야 할 중요 로그가 식별되어 있는가? • 웹 어플리케이션, 정보보호시스템, DB, 운영체제에서 침입시도 및 이상징후를 의미하는 로그가 생성되어 기록될 수 있도록 식별하여야 한다. • 각 시스템에서 생성되어야 하는 로그를 분류하기 위한 기준을 마련해야 한다. • 웹 어플리케이션에서 생성되어야 하는 로그의 예는 허용되지 않은 페이지 접근 시도, 소스코드 다운로드 시도, Brute Force Attack 등에 대한 로그를 생성할 수 있어야 한다. • 정보보호시스템에서 생성되어야 하는 로그의 예는 우회접근, 보안정책 우회, 관리자 권한 획득 시도 등에 대한 로그를 생성할 수 있어야 한다. • DB에서 생성되어야 하는 로그의 예는 대량 데이터 다운로드, 비인가자의 접근 시도, 관리자 권한 획득 시도 등에 대한 로그를 생성할 수 있어야 한다. • 운영체제에서 생성되어야 하는 로그의 예는 로그인 기록, 서버접속 기록, su 로그, 사용자의 명령어 및 작업내용에 대한 로그를 생성할 수 있어야 한다. • 각 시스템에서 생성된 로그는 관리자가 해석하기에 적합해야 한다. ※ 로그는 접근 시도자(계정정보, IP정보, Port정보, 시간정보 등)의 정보가 포함되어야 한다. • 관리자는 주기적인 로그 분석을 통하여 침입시도 및 데이터 유출 등을 확인하고, 수행의 결과를 기록해야 한다. ② 정보통신설비의 식별된 중요 로그는 1개월 이상 보존.관리되고 있는가? • 웹 어플리케이션, DB, 네트워크 장비에서 생성된 로그는 최소한 1개월 이상 보존하여야 한다. ③ 정보보호시스템의 로그는 3개월 이상 기록·관리되고 있는가? • 침입차단시스템(방화벽), 웹방화벽, 웹쉘탐지, DB접근통제, DB암호화 등의 정보보호시스템에서 생성된 로그는 최소한 3개월 이상 보존하여야 한다. **【증빙자료】** • **로그분석 수행 결과 기록** • **식별된 중요로그 목록** • **로그분류를 위한 기준 또는 지침** • **로그 보존 화면 증적(1개월 또는 3개월)** • **로그 관리 현황표 (☞ [붙임 15] 로그 관리 현황표 참조)** • **백업 현황 및 복구 관리대장 (☞ [붙임 16] 백업 현황 및 복구 관리대장 참조)**

1.3. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」제49조의2제1항에 따른 속이는 행위에 이용된 문자메시지 식별 및 차단 관련 기술적 조치를 할 것

항목	악성문자 사전차단체계 기술적 조치
제출 서류	▶ 증빙서류 ⑰ : 붙임2 '악성문자 사전차단체계(X-ray) 관련 가이드라인' 참고하여 관련 서류 제출

2. 인력 및 물적시설

2.1. 전담인력

항목	부정가입 방지, 발신번호 등록・관리, 거짓으로 표시된 전화번호의 문자메시지 전달 경로 확인・제공 및 이를 송신한 자의 해당 회선에 대한 전기통신역무 제공의 중지 등을 위해 대표자를 제외한 전담직원을 별도로 1명 이상 둘 것
제출 서류	**발신번호 변작방지 등 전담인력 지정** **▶증빙자료 ⑱ : 발신번호 변작방지 담당자 명부 1부** - 전담인력은 해당 사업자의 직원임을 입증할 수 있는 공적기관*의 자료 첨부 *고용보험, 건강보험, 소득세 납부사실증명서 등

2.2. 정보보호최고책임자 지정·공포

항목	임원급 또는 부서장급 이상의 정보보호 최고책임자를 지정・공표할 것
제출 서류	**정보보호 최고책임자 지정·공표** **▶증빙자료 ⑲ : 정보보호 최고책임자를 지정하고 공표하였음을 증명할 수 있는 서류(품의문서 및 홈페이지 캡처화면 등) 각 1부**

2.3. 물적시설

항목	전기통신설비와 각종 부대장비 구비 여부 확인
제출 서류	**▶증빙자료 ⑳ : 사업용 주요 설비 내역, 설치 장소 및 통신망 구성도, 문자발송 체계* 설명 자료, 사업자 홈페이지 화면 및 문자서비스 화면**을 캡처한 서류(컬러)를 제출(증빙자료 지정서식 ⑳)** - 클라우드 서비스 이용중인 사업자의 경우 이용계약서 첨부 * 문자발송 체계는 통신망 구성요소인 발신자, 해당 사업자, 상위 사업자(중계 또는 재판매 사업자), 이동통신사, 수신자 등의 역할과 문자발송 방법 등이 포함되어야 함 ** 사업자 홈페이지 및 문자서비스 화면은 사업자의 URL이 포함되어야 함 특수한 유형의 부가통신사업 물적시설 **붙임3 서식**

3. 재무건전성

항목	납입자본금(개인인 경우는 영업용 자산평가액을 말한다) 1억원 이상
제출서류	▶증빙자료 ㉑ : 법인등기사항증명서, 개인인 경우 영업용 자산 평가액(영업용자산명세서 및 그 증빙서류, 은행에서 발급한 예금잔고증명서, 사업용 사무실 임대계약서 ※ 영업용 자산평가액은 영업과 관련된 자산으로, 개인 거주용 주택매매계약서, 개인용 주식 잔고 등 영업과 상관없는 자산은 인정 불가

4. 사업계획서

항목	인원·시설 등 일반 현황, 사업개요, 사업추진방향, 매출방안, 향후 사업추진계획 등을 포함할 것
제출 서류	▶증빙자료 ㉒ : 전기통신사업법 제22조제2항제5호 및 같은 법 시행령 제29조제8항에 따른 사업계획서 제출

5. 이용자보호계획서

<table>
<tr><th>항목</th><th>이용자보호계획서</th></tr>
<tr><td>제출 서류</td><td>
▶증빙자료 ㉓ : 전기통신사업법 제22조제2항제5호 및 같은 법 시행령 제29조제8항에 따른 이용자보호 계획서 제출(아래 사항이 포함되어야 함)
<table>
<tr><th>이용자보호 계획 내용</th></tr>
<tr><td>· 개인정보보호를 위한 내부관리계획 수립
- 개인정보 관리책임자의 지정, 개인정보취급자의 교육에 관한 사항, 개인정보에 대한 불법적인 접근을 차단하기 위한 조치, 개인정보가 안전하게 저장 전송될 수 있는 조치(보안서버 설치 등) 등이 포함되어 있는가?</td></tr>
<tr><td>· 서비스 약관 제정
- 이용자 불만형태별 처리절차 및 처리기간이 명시
- 서비스 제공이 불가능한 경우의 처리방안이 명시
- 거짓으로 표시된 전화번호를 송신한 자의 해당 회선에 대한 전기통신역무 제공의 중지를 위한 처리방안 명시
- 발신번호 등록·관리, 부정가입 방지 등에 대한 사업자·이용자의 의무 및 기타 이용자 고지 사항 명시 등</td></tr>
</table>
</td></tr>
</table>

6. 전송자격인증서

항목	전송자격인증서
제출 서류	▶증빙자료 ㉔ : 전기통신사업법 제22조의11 및 같은 법 시행령 제30조의11에 따라 방송미디어통신위원회가 발급한 전송자격인증서 사본 제출

붙임1 인터넷 문자 발송 현황 자료 양식 [지정서식 15]

신청인	상호	(필수입력)	대표자 성명	(필수입력)
	사업자등록번호	(필수입력)	법인등록번호	(선택입력)
	주소	(필수입력)		
	담당자 성명	(필수입력)	담당자 전화번호	(필수입력)
	담당자 이메일	(필수입력)		

운영방식

o 아래 제시된 사항 중, 해당 되는 운영 방식에 체크(중복체크 가능)

□ 이용자 대상 인터넷 문자 발송 서비스 제공 목적으로 웹사이트 개설 및 운영

□ 사설문자발송장비 고객 또는 하위연동 문자재판매사 대상으로 API 연동기능 제공

□ 기타*: _____

* 인터넷 문자발송 서비스가 아닌 다른 서비스를 제공하는 웹사이트를 운영하면서, 필요시 문자 발송 기능을 일부 제공하는 경우 등

사이트 주소

o 이용자 대상 인터넷 문자 발송 서비스를 제공하는 웹사이트 주소 기입

※ 사이트가 여러 개인 경우 모두 기입 할 것

- www._____

망 연동 사업자

o 상위 연동 사업자

상호	사업자등록번호	담당자		
		이름	연락처	이메일

o 하위 연동 사업자

상호	사업자등록번호	담당자		
		이름	연락처	이메일

전기통신사업법 시행령 제29조제9항 별표3 제2호의 기술적 조치를 확인하기 위한 증빙서류로 위와 같이 인터넷 문자 발송 현황 자료를 제출하며, 해당 내용이 사실과 다름없음을 확인합니다.

추후 변동사항 발생 시 요청된 방식에 따라 수정사항을 제출할 것이며, 미 제출된 사항으로 인해 발생하는 모든 불이익은 본 사업자의 책임으로 함을 확인합니다.

년 월 일

사업자명 (서명·직인)

붙임2 악성문자 사전차단체계(X-ray) 관련 가이드라인

전기통신사업법 시행령 개정에 따른 '악성문자 사전차단체계' 운영(안)

- (전제조건) 제도시행 초기임을 고려해 [별표 3]의 '속이는 행위에 이용된 문자메시지 식별 및 차단 관련 기술적 조치'는 **기 확인된 악성URL에 대해 탐지·차단**하는 것에 한정
  ※ 향후 이 범위는 신규 URL/앱에 대한 분석·차단까지 확대 될수 있음
- (용어)
  - **KISA 악성URL정보** : 악성URL로 판별된 KISA보유 데이터베이스로서 API를 활용해 제공
  - **KISA 악성문자 사전차단 체계** : KISA가 특수부가통신사업자로부터 의뢰 받은 URL의 악성URL 여부에 대해 확인 후 회신하는 체계
  - **Black List 기반 악성문자 사전차단 체계** : 속이는 행위로 판단되어 'KISA 악성URL정보' 및 자체 수집한 악성URL정보를 추가 활용하여 발신을 차단하는 체계
  - **White List 기반 문자 발송** : 특수부가통신사업자가 문자메시지 내 포함된 내 URL을 확인·검증 후 안전하다고 판단하여 발송하는 체계

□ 악성문자 사전차단 체계 도입 · 운영 방안

○ (적용 예외) 문자메시지 內 URL이 포함되지 않는 문자만 발송하는 경우 기술적 조치* 완료 후 확약서**로 갈음 가능

* 예시) 문자발송 프로그램·시스템에 문자메시지 內 URL포함 여부 확인 및 포함시 발송을 중단하고 관리자에 알리는 기능 포함

** URL포함 문자를 발송을 차단하는 기술적 조치를 완료(기능정의서 포함)하였으며, URL포함 문자 발송시 기 해당 사항(기술적 조치 미비)이 법 위반에 해당한다고 확약하는 공문 등

< Black List 기반 악성문자 사전차단체계 운영 방안 요약 >

유형	설명	발급서류(안)
1	· 전문 솔루션사를 활용하여 특수부가사업자가 자체 구축	솔루션사 도입확인서
2	· 특수부가사업자 자체 개발 및 운영 ※ KISA 악성 URL 블랙리스트 정보 사용 필수	KISA 악성URL 연동 확인서
기타	· KISA의 '악성문자 사전차단 체계'와 연동	KISA 도입확인서

○ (유형1) 전문 솔루션사를 활용하여 특수부가통신사업자가 자체개발 및 운영

- (대상) 외부 솔루션사와 연계하여, 자체적인 차단체계 운영이 가능한 사업자

- (비용/기간) 솔루션 사업자별 상이

- (운영방식) 악성URL 정보를 보유한 전문 솔루션사*와 계약 등을 통한 차단체계 운영

  * KISA 악성URL정보 연동 필수

- (조건) 별도 조건 없음.

  ※ 전문 솔루션사를 통해 차단 URL 및 건수 KISA 제공

- **(고려사항) 이용약관에 문자 내 포함된 URL에 대해 전문 솔루션사를 통해 검증될수 있으며, 그 결과가 KISA에 제공된다는 내용 포함 필요**

- (확인서류) 솔루션사 차단체계 도입 완료 확인서 발급

- (검증방법) 자격요건 검증 시 'KISA 악성URL정보' 중 10개 이내 URL을 무작위로 추출하여 시범 발송(중앙전파관리소 등)

- (기타) 불가피한 경우* 특수부가통신사업자의 판단하에 악성URL 여부를 자체 판단하여 발송가능

  * 예시) 사전 확인 시 수신자의 권익을 현저히 침해하는 경우, 실시간성이 요하는 경우, 동일·유사 URL(내용)을 지속·반복적으로 발송하는 경우 등

  ※ 단, URL포함 문자 발송 차단 기술적 조치를 완료하여야 하며, 발송일자, 수신자, 발송URL 등이 포함된 'White list 기반 문자 발송' 대장을 유지하여야 함

○ (유형2) 특수부가통신사업자가 자체개발 및 운영

- (대상) 자체적으로 차단 체계를 도입하여, 운영가능한 사업자
  ※ 필요시 제3자를 통한 서비스 연동 가능

- (비용/기간) 사업자별 상이

※ KISA 악성URL정보 반영을 위한 연동 비용 무상 / 1년(자격요건 검증 후 연장)

- (운영방식) 악성URL 데이터베이스*를 자체적으로 구축하여 차단체계 운영
  * KISA 악성URL정보 반영 필수

- (조건) KISA 악성URL 정보 연동을 위해서는 보안조치*가 완료되어 있어야 하며, 보안이 취약하거나 법 위반 이력이 있는 사업자 등은 연동 제한
  * DB와 인터넷연결 차단, DB암호화, 백신, 비인가 접속 차단 등의 보안 조치
  ** 예시) 최근 3년간 해킹·개인정보 유·노출 등 사고가 발생했거나, 직전년도 스팸 신고 다량발생 상위 50대 사업자에 1회라도 포함되었을 경우 등

- (신청방식) x-ray@kisa.or.kr 을 통해 악성URL 정보 제공 요청

- **(고려사항) 이용약관 내 문자내 포함된 URL에 대해 분석될수 있고, 차단 정보에 대해 KISA에 제공된다는 내용 포함 필요**

- (확인서류) KISA의 악성URL 정보 제공을 위한 API연동 확인서

※ 차단체계 적용이 완료되었다는 의미는 아님

- (검증방법) 자격요건 검증 시 'KISA 악성URL정보' 중 10개 이내 URL을 무작위로 추출하여 시범 발송(중앙전파관리소 등)

- (기타) 불가피한 경우* 특수부가통신사업자의 판단하에 악성URL 여부를 자체 판단하여 발송가능
  * 예시) 사전 확인 시 수신자의 권익을 현저히 침해하는 경우, 실시간성이 요하는 경우, 동일·유사 URL(내용)을 지속·반복적으로 발송하는 경우 등

※ 단, URL포함 문자 발송 차단 기술적 조치를 완료하여야 하며, 발송일자, 수신자, 발송URL 등이 포함된 'White list 기반 문자 발송' 대장을 유지하여야 함

[참고 : 영세사업자]

○ 한국인터넷진흥원(KISA)를 통해 악성문자 사전차단 체계 연동 지원(최대 2년)

- (대상) 영세사업자
- (비용/기간) 무상 / 1년(1회 연장가능하며, 최장 2년간 이용 가능)

※ 종료일로부터 60일(휴일포함) 前 연장 신청(신청 서류는 별도 안내)하여야 하며, 자격요건 검증 후 연장 여부 결정

- (운영방식) 특수부가통신사업자-KISA 시스템 間 API 연동 후 문자 內 포함된 URL을 API를 통해 KISA에 질의 후 KISA의 악성여부 판단결과에 따라 발송 여부를 결정하는 체계
- (조건) 부가가치세법상 간이과세자*인 사업자만 허용, 사회적 물의**를 일으킨 사업자 제외, 일 최대 100건 검증 가능(이후 차단)

* 전년도 매출액 기준 1.04억원, 신규기업의 경우 자본금 1.04억 미만

** 예시) 최근 3년간 해킹·개인정보 유·노출 등 사고가 발생했거나, 직전년도 스팸신고 다량발생 상위 50대 사업자(spam.kisa.or.kr 기준)에 1회라도 포함되었을 경우 등

※ KISA가 수용가능 한계 도달시 연동이 거부될 수 있음

- (신청방식) x-ray@kisa.or.kr 을 통해 신청 시 안내되는 서류를 작성하여 이메일로 제출
- (고려사항) 특수부가통신사업자는 이용약관 내 문자내 포함된 URL이 KISA에 제공되어 악성여부를 판별한다는 내용 포함 필수
- (확인서류) KISA 차단체계 도입 완료 확인서 발급
- (검증방법) 자격요건 검증 시 'KISA 악성URL정보' 중 10개 이내 URL을 무작위로 추출하여 시범 발송(중앙전파관리소)
- (기타) 불가피한 경우* 특수부가통신사업자의 판단하에 악성URL 여부를 자체 판단하여 발송가능

* 예시) 사전 확인 시 수신자의 권익을 현저히 침해하는 경우, 실시간성이 요하는 경우, 동일·유사 URL(내용)을 지속·반복적으로 발송하는 경우 등

※ 단, URL포함 문자 발송 차단 기술적 조치를 완료하여야 하며, 발송일자, 수신자, 발송URL 등이 포함된 'White list 기반 문자 발송' 대장을 유지하여야 함

붙임3 문자발송 특수부가통신사업 물적시설 (지정서식 20)

① 전기통신설비와 각종 부대장비 내역

사업용 주요 설비 내역	
설치장소	

② 통신망 구성도 및 문자발송 체계

통신망 구성도	
문자발송 체계 (문자발송 방법 등)	

③ 증빙사진(홈페이지 화면, 문자 서비스 화면)

사업자 홈페이지 화면	
문자 서비스 화면(문자 작성 화면 등)	

「전기통신사업법」 제22조제2항과 같은 법 시행령 제29조제9항에 따라 위와 같이 자료를 제출합니다.

년 월 일

제출인 (서명 또는 인)

작 성 방 법

1. 클라우드 서버를 사용하는 경우 설치장소는 클라우드 서버 설치장소를 기재하십시오.
2. 통신망 구성도는 발신자, 해당 사업자, 상위 사업자(중계 또는 재판매 사업자), 이동통신사, 수신자 등이 표시된 구성도를 기재하십시오.
   - 증빙자료로 상위 사업자와의 계약서 또는 신청서 제출 필요
3. 문자발송체계는 통신망 구성요소(발신자, 해당 사업자, 상위 사업자(중계 또는 재판매 사업자), 이동통신사, 수신자 등)의 역할, 문자발송 방법 등을 기재하십시오.
4. 사업자 홈페이지 및 문자 서비스 화면은 사업자의 URL이 포함되어야 합니다.

붙임4 정보통신설비 목록 (샘플)

정보통신설비 목록

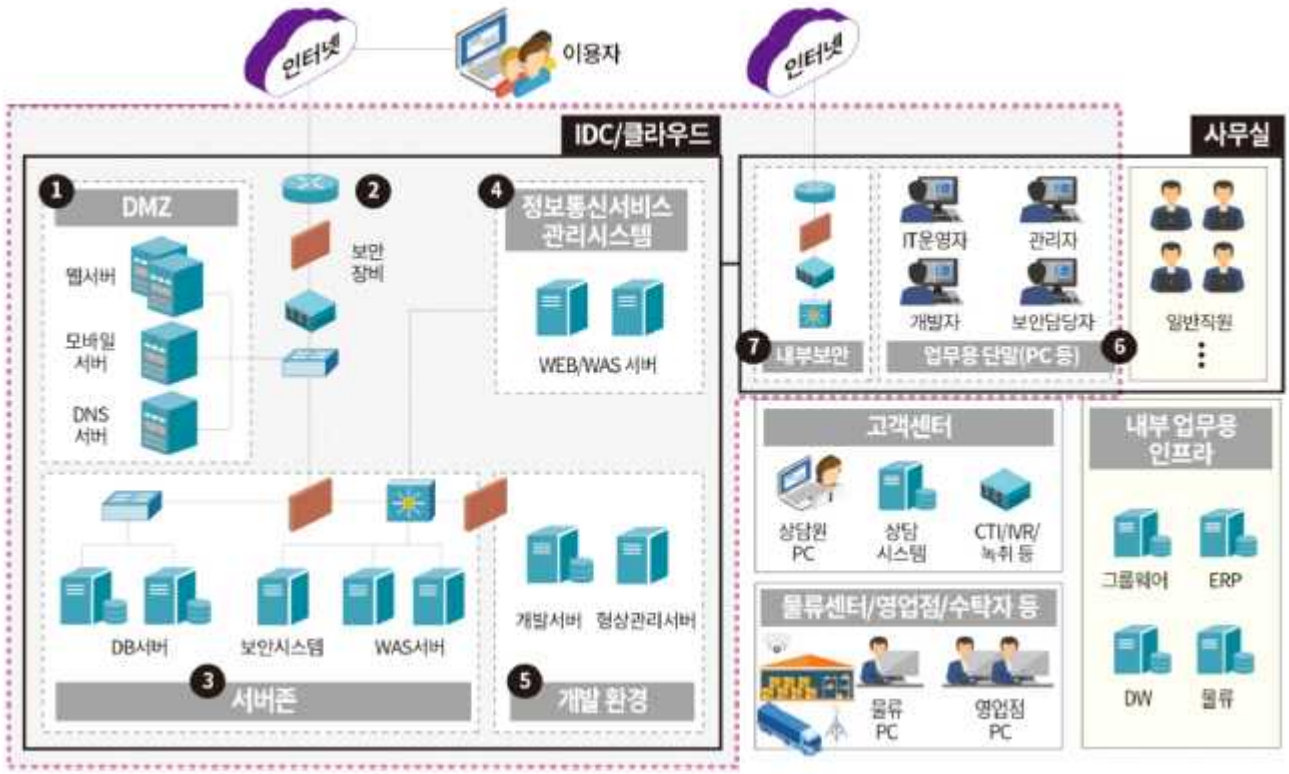
■ 업체명: _____, 서비스명: _____

NO	유형	자산 명칭	자산 번호	시리얼 번호 (또는 라이센스)	제품명 및 버전	운영체제(OS)	설치 장소	관리자	도입년월	중요도 (상·중·하)

※ 유형 예시 : 서버, 네트워크 장비, 정보보호시스템(방화벽, 웹방화벽, 웹쉘탐지, DB접근통제, DB암호화 등), DB, 관리용PC, 개발용PC, 웹 어플리케이션 등

※ 중요도 예시 : 비밀성, 무결성, 가용성에 근거한 자산 중요도를 상·중·하 등급으로 산정

붙임5 네트워크 구성도 (샘플)



※ 대외서비스를 수행하는 DMZ 영역(❶) 인터넷 연결 구간(❷), 내부 서버 영역(❸), 관리서버 영역(❹), 개발환경 영역(❺), 업무용 사용자 영역(❻), 내부 보안솔루션 영역(❼ 등 내부 네트워크를 접근통제 관점에서 영역영 별로 도식화 하여 표시

붙임6 방화벽(Firewall) 정책 Rule Set 현황표 (샘플)

※ 침입차단시스템(방화벽)에 설정된 정책 목록을 아래 양식에 맞게 작성하여 제출하시기 바랍니다.

■ 업체명: 서비스명: 작성일:

순번	정책명	출발지IP	목적지IP	포트	프로토콜	허용/차단	설명	등록일	최종검토일
※ 출발지/목적지IP가'관리단말'인 경우 해당IP 목록을 별도 명시 권고 | 차단 규칙(Default Deny)은 반드시 최하단에 위치									
1	외부→웹서버HTTP	Any (0.0.0.0/0)	192.168.1.10	TCP/80	TCP	허용	외부 사용자 웹 접근	2024-01-10	2025-01-10
2	외부→웹서버HTTPS	Any (0.0.0.0/0)	192.168.1.10	TCP/443	TCP	허용	외부 사용자 HTTPS 접근	2024-01-10	2025-01-10
3	웹서버→WAS	192.168.1.10	192.168.2.10~11	TCP/8080	TCP	허용	WEB→WAS 내부 통신	2024-01-10	2025-01-10
4	WAS→DB	192.168.2.10~11	192.168.3.10~11	TCP/3306	TCP	허용	WAS→DB 쿼리 통신	2024-01-10	2025-01-10
5	관리단말→서버SSH	192.168.5.10	192.168.2.0/24	TCP/22	TCP	허용	관리자SSH 접속(허가IP 한정)	2024-01-10	2025-01-10
6	관리단말→DB	192.168.5.10	192.168.3.10~11	TCP/3306	TCP	허용	DBA 직접 접속(제한적)	2024-01-10	2025-01-10
7	서버→백업서버	192.168.2.0/24	192.168.4.10	TCP/873	TCP	허용	rsync 백업 통신	2024-01-10	2025-01-10
8	기타 외부→내부	Any	Any	Any	Any	차단	비인가 트래픽 전체 차단 (Default Deny)	2024-01-10	2025-01-10

붙임7 웹방화벽(WAF) 정책 Rule Set 현황표 (샘플)

※ 웹방화벽에 적용 중인 정책 목록을 작성하고, 가능한 경우WAF 관리 콘솔 캡처 화면을 함께 첨부하시기 바랍니다.

■ 업체명: WAF 제품명/버전: 작성일:

순번	규칙명	규칙 유형	탐지 패턴/조건	동작	우선순위	적용URL	비고
※ 동작: 허용/차단/모니터링 중 선택 | 우선순위 숫자가 낮을수록 먼저 적용 | WAF 제품별 실제 설정 화면 캡처 첨부 권고							
1	SQL Injection 차단	공격 탐지	SQL 예약어 패턴 (SELECT, UNION, DROP 등)	차단	1	전체URL	OWASP Top10
2	XSS 차단	공격 탐지	<script>, on* 이벤트, javascript: 패턴	차단	2	전체URL	
3	파일 업로드 제한	파일 업로드	.php/.jsp/.asp 확장자 업로드 차단	차단	3	/upload/*	웹쉘 업로드 방지
4	디렉토리 트래버설	경로 탐색	../ 패턴 포함 요청 차단	차단	4	전체URL	
5	비정상HTTP 메서드	프로토콜 위반	PUT, DELETE, TRACE 메서드 차단	차단	5	전체URL	관리 기능 제외
6	IP 기반 차단	접근 통제	블랙리스트IP 요청 차단	차단	6	전체URL	주기적 업데이트
7	비정상 요청 크기	DoS 방어	요청Body > 10MB 차단	차단	7	전체URL	
8	로그인 무차별 대입	인증 공격	동일IP 로그인 실패5회 이상 시 차단	차단	8	/login/*	5분간 잠금
9	화이트리스트 허용	접근 허용	관리자IP 대역 (192.168.5.0/24) 허용	허용	0	/admin/*	

붙임8 서버별 서비스 포트 현황표 (샘플)

※ 웹서버, WAS서버, DB서버, 백업서버 등 모든 서버의 서비스 포트를 빠짐없이 기재하시기 바랍니다.

■ 업체명: 작성일:

순번	서버명	서버 유형	IP 주소	포트	프로토콜	소프트웨어/버전	용도/설명	사용여부
※ 현재 사용 중인 포트만 기재 | 불필요 포트는 비활성화 후'미사용'으로 표기 | 서버별netstat/ss 명령 결과 캡처 첨부 권고								
1	WEB-01	웹서버	192.168.1.10	TCP/80	HTTP	Apache 2.4	외부 웹서비스(HTTP)	운영중
2	WEB-01	웹서버	192.168.1.10	TCP/443	HTTPS	Apache 2.4	외부 웹서비스(HTTPS)	운영중
3	WEB-01	웹서버	192.168.1.10	TCP/22	SSH	OpenSSH 8.9	관리자 원격 접속	운영중
4	WAS-01	WAS서버	192.168.2.10	TCP/8080	HTTP	Tomcat 9.0	웹→WAS 내부 통신	운영중
5	WAS-01	WAS서버	192.168.2.10	TCP/22	SSH	OpenSSH 8.9	관리자 원격 접속	운영중
6	WAS-02	WAS서버	192.168.2.11	TCP/8080	HTTP	Tomcat 9.0	웹→WAS 내부 통신	운영중
7	DB-01	DB서버	192.168.3.10	TCP/3306	MySQL	MySQL 8.0	WAS→DB 쿼리 통신	운영중
8	DB-01	DB서버	192.168.3.10	TCP/22	SSH	OpenSSH 8.9	DBA 원격 접속	운영중
9	DB-02	DB서버(슬레이브)	192.168.3.11	TCP/3306	MySQL	MySQL 8.0	DB 복제 (Replication)	운영중
10	BAK-01	백업서버	192.168.4.10	TCP/873	rsync	rsync 3.2	서버→백업 데이터 전송	운영중
11	BAK-01	백업서버	192.168.4.10	TCP/22	SSH	OpenSSH 8.9	관리자 접속	운영중

붙임9 계정 · 비밀번호 관리대장 (샘플)

※ 서버, DB, 네트워크 장비, 정보보호시스템 등 모든 시스템의 계정을 기재하시기 바랍니다.

※ 비밀번호 원문은 기재하지 않으며, 최종 변경일 및 변경 주기 준수 여부만 확인합니다.

■ 업체명: 작성일:

순번	서버/시스템명	계정ID	계정 유형	부서/담당자	생성일	최종PW 변경일	사용여부	비고
※ 비밀번호 자체는 기재하지 않음 | 비밀번호 변경 주기: 90일 이내 권고 | 미사용 계정은 즉시 삭제/잠금 처리								
1	WEB-01 (Linux)	root	시스템 관리자	인프라팀/홍길동	2023-03-01	2025-01-15	사용중	직접 로그인 불가 (sudo 전환)
2	WEB-01 (Linux)	webadmin	일반 관리자	인프라팀/홍길동	2023-03-01	2025-01-15	사용중	웹 서비스 전용 계정
3	WAS-01 (Linux)	root	시스템 관리자	인프라팀/이순신	2023-03-01	2025-01-15	사용중	직접 로그인 불가
4	WAS-01 (Linux)	wasadmin	일반 관리자	인프라팀/이순신	2023-03-01	2025-01-15	사용중	Tomcat 구동 계정
5	DB-01 (MySQL)	root	DB 관리자	DBA팀/강감찬	2023-03-01	2025-02-01	사용중	외부 접속 비허용
6	DB-01 (MySQL)	smsapp	애플리케이션 계정	DBA팀/강감찬	2023-03-01	2025-02-01	사용중	WAS 연동 전용 계정
7	DB-01 (MySQL)	dbauser	DBA 계정	DBA팀/강감찬	2023-03-01	2025-02-01	사용중	운영DBA 전용
8	BAK-01 (Linux)	bakadmin	백업 관리자	인프라팀/이순신	2023-03-01	2025-01-15	사용중	
9	FW-01 (방화벽)	admin	방화벽 관리자	보안팀/유관순	2023-03-01	2025-01-10	사용중	2FA 적용
10	WAF-01 (웹방화벽)	wafadmin	WAF 관리자	보안팀/유관순	2023-03-01	2025-01-10	사용중	

붙임10 정보통신설비(자산) 목록 대장 - 확장 (샘플)

※ 문자발송 서비스에 관련된 모든 정보통신설비를 빠짐없이 기재하시기 바랍니다.

■ 업체명: 서비스명: 작성일:

순번	설비명	유형	세부유형	모델명	OS/버전	IP 주소	설치 위치	중요도	운영상태
※ 유형: 서버, 네트워크 장비, 정보보호시스템, DB 서버, 관리용PC, 개발용PC, 웹 어플리케이션 등 | 중요도: 상/중/하									
1	WEB-01	서버	웹서버	Dell R740	CentOS 8.5	192.168.1.10	DMZ	상	운영중
2	WAS-01	서버	WAS서버	Dell R740	CentOS 8.5	192.168.2.10	내부망	상	운영중
3	WAS-02	서버	WAS서버	Dell R740	CentOS 8.5	192.168.2.11	내부망	상	운영중
4	DB-01	DB 서버	DB서버 (Master)	HP DL380	CentOS 8.5	192.168.3.10	내부망	상	운영중
5	DB-02	DB 서버	DB서버 (Slave)	HP DL380	CentOS 8.5	192.168.3.11	내부망	상	운영중
6	BAK-01	서버	백업서버	Dell R540	Ubuntu 22.04	192.168.4.10	내부망	상	운영중
7	FW-01	네트워크 장비	방화벽	Piolink TiFRONT	TiFRONT v3.2	192.168.0.1	외부연결	상	운영중
8	FW-02	네트워크 장비	내부방화벽	Juniper SRX300	Junos 21.4	192.168.2.1	DMZ-내부 경계	상	운영중
9	WAF-01	정보보호시스템	웹방화벽	WAPPLES v5.0	WAPPLES OS	192.168.1.5	DMZ	상	운영중
10	IPS-01	정보보호시스템	IPS	시큐아이 MFI	MFI v4.1	192.168.0.2	외부연결	상	운영중
11	MGMT-PC-01	관리용PC	관리단말	삼성 데스크톱	Windows 11	192.168.5.10	관리망	중	운영중

붙임11 IPS/IDS 운영현황표 (샘플)

※ 침입차단(IPS) 및 침입탐지(IDS) 시스템의 설치·운영 현황을 기재하시기 바랍니다.

■ 업체명: 작성일:

▶ IPS/IDS 장비 현황

순번	장비명	유형	설치 위치	IP 주소	OS/버전	운영 모드	유지보수업체	도입일	정책 업데이트일
※ 운영모드: 인라인(Inline)-직접 차단, 미러링(Mirroring)-탐지만 | 정책 업데이트 주기: 최소 월1회 권고									
1	IPS-01	IPS	외부→DMZ 경계	192.168.0.2	MFI v4.1	인라인 (Inline)	시큐아이	2023-03-01	2025-02-20
2	IDS-01	IDS	DMZ 내부망 경계	192.168.1.3	SnortIDS v3.1	미러링 (Mirroring)	자체관리	2023-03-01	2025-01-30

▶ 월별 탐지/차단 통계(예시)

집계 기간	탐지 건수(IPS)	차단 건수(IPS)	탐지 건수(IDS)	탐지 공격 유형
2026.01.01.~ 2026.01.31	1,234건	987건	456건	SQL Injection, Port Scan, Brute Force

붙임12 취약점 점검 결과 보고서 (샘플)

※ 취약점 점검은 연1회 이상 수행해야 하며, 점검 결과 및 조치 이력을 본 양식에 기록하여 보관하시기 바랍니다.

■ 업체명: 서비스명: 작성일:

▶ 점검 개요

점검 수행일	2025년O월OO일~ O월OO일	점검 기관	○○○ (자체/ 외부위탁)
점검 대상	WEB-01, WAS-01~02, DB-01~02, FW-01, WAF-01	점검 도구	NESSUS, OpenVAS, KISA 취약점 점검 도구
총 취약점 수	상: 2건/ 중: 5건/ 하: 8건	조치 완료	상: 2건/ 중: 3건/ 하: 6건

▶ 취약점 목록 및 조치 현황

순번	대상 서버	취약점 유형	취약점 내용	위험도	현재 상태	조치 방법	조치 예정일	조치상태
※ 위험도: 상(즉시 조치)/중(1개월 내)/하(분기 내) | 조치상태: 완료/조치중/해당없음								
1	WEB-01	OS 취약점	OpenSSL 1.1.1 버전 사용 (CVE-2023-0286)	상	OpenSSL 3.0 업그레이드 필요	OpenSSL 3.0으로 패치 적용	2025-01-20	완료
2	WEB-01	설정 오류	불필요한 서비스 포트(TCP/8443) 오픈	중	포트 비활성화 필요	방화벽 차단 및 서비스 중지	2025-01-21	완료
3	WAS-01	취약 설정	Tomcat 관리자 페이지 외부 노출	상	/manager 경로 외부 차단 필요	IP 기반 접근 제한 설정	2025-01-22	완료
4	DB-01	계정 관리	테스트 계정 (testuser) 잔존	중	불필요 계정 삭제 필요	testuser 계정 삭제 완료	2025-01-23	완료
5	DB-01	암호화	특정 컬럼 평문 저장(고객 연락처)	중	DB 암호화 적용 필요	AES-256 암호화 적용 예정	2025-03-31	조치중
6	FW-01	정책 관리	미사용 방화벽 규칙23개 잔존	하	미사용 정책 정리 필요	분기별 정기 점검 후 정리	2025-02-28	조치중

붙임13 보안 패치 이력 관리대장 (샘플)

※ OS, 미들웨어, DBMS, 네트워크 장비 등 모든 시스템의 보안 패치 적용 이력을 기록하시기 바랍니다.

※ KISA(한국인터넷진흥원) 보안공지(https://www.kisa.or.kr) 정기 확인을 권고합니다.

■ 업체명: 작성일:

순번	대상 서버	현재 버전	패치 내용	위험도	CVE/패치 사유	적용일	담당자	상태
※ 위험도'상' 패치: 발표 후72시간 내 적용 권고 | '중' 패치: 1개월 내 | '하' 패치: 분기 내 | KISA 보안공지 참조 권고								
1	WEB-01	OpenSSL 1.1.1	OpenSSL 3.0.8 업그레이드	상	CVE-2023-0286 (X.509 인증서 파싱 취약점)	2025-01-20	홍길동	완료
2	WAS-01~02	Apache Tomcat 9.0.70	Tomcat 9.0.85 업그레이드	중	CVE-2024-21733 (HTTP 요청 스머글링)	2025-01-25	이순신	완료
3	DB-01~02	MySQL 8.0.31	MySQL 8.0.36 업그레이드	중	CVE-2024-20977 (권한 상승 취약점)	2025-02-05	강감찬	완료
4	전체 서버	Linux Kernel	보안 업데이트 패치 적용	중	KISA 월별 보안 업데이트 권고	2025-02-10	홍길동	완료
5	FW-01	TiFRONT v3.1	TiFRONT v3.2 펌웨어 업그레이드	하	제조사 정기 보안 패치	2025-02-15	유관순	완료
6	WAF-01	WAPPLES v4.9	WAPPLES v5.0 업그레이드	하	신규 공격 패턴 DB 업데이트	2025-02-20	유관순	완료

붙임14 접근권한(사용자) 관리대장 (샘플)

※ 서버, DB, 네트워크 장비 등에 접근 권한을 가진 모든 내부 사용자 및 외부 위탁업체 인원을 기재하시기 바랍니다.

■ 업체명: 작성일:

순번	성명	소속/부서	직책	계정ID	접근 대상 시스템	권한 수준	부여일	만료일	최종 접속일
※ 퇴직/부서이동/업무변경 시 즉시 권한 변경/삭제 | 외부위탁업체 계정은 계약 기간 내로 만료일 설정 필수 | 분기별 접근권한 검토 권고									
1	홍길동	인프라팀	팀장	infra_hong	WEB-01, WAS-01~02, BAK-01	관리자(sudo)	2023-03-01	-	2025-03-10
2	이순신	인프라팀	팀원	infra_lee	WAS-01~02	일반 사용자	2023-05-01	-	2025-03-08
3	강감찬	DBA팀	팀장	dba_kang	DB-01~02	DBA(전체 권한)	2023-03-01	-	2025-03-09
4	유관순	보안팀	팀원	sec_yoo	FW-01, WAF-01, IPS-01	보안 관리자	2023-06-01	-	2025-03-07
5	김개발	개발팀	팀원	dev_kim	WAS-01(개발 환경)	읽기 전용	2024-01-10	2025-06-30	2025-02-28
6	외주운영(주)A사	외부위탁	운영요원	vendor_a01	WEB-01 (SSH)	제한적 관리자	2024-03-01	2025-02-28	2025-02-20

붙임15 로그 관리 현황표 (샘플)

※ 모든 정보통신설비의 로그 종류, 저장 위치, 보관 기간, 정기 점검 주기를 기재하시기 바랍니다.

■ 업체명: 작성일:

순번	시스템명	로그 유형	로그 파일명	저장 위치	보관 기간	점검 주기	담당자	비고
※ 로그 보관 기간: 최소6개월 이상 권고(전기통신사업법 준거) | 로그 무결성 보장을 위해 외부SIEM 또는 별도 로그 서버 활용 권고								
1	WEB-01	접근 로그	Apache access.log	/var/log/ apache2/	6개월	월1회	홍길동	자동 로테이션
2	WEB-01	오류 로그	Apache error.log	/var/log/ apache2/	6개월	주1회	홍길동	
3	WAS-01~02	애플리케이션 로그	Tomcat catalina.out	/opt/tomcat/logs/	6개월	주1회	이순신	
4	DB-01~02	쿼리 감사 로그	MySQL general_log	/var/log/ mysql/	1년	월1회	강감찬	DB접근통제 시스템 연동
5	DB-01~02	에러 로그	MySQL error.log	/var/log/ mysql/	1년	주1회	강감찬	
6	FW-01	방화벽 정책 로그	TiFRONT syslog	SIEM 서버 (192.168.6.10)	1년	월1회	유관순	외부syslog 서버 전송
7	WAF-01	WAF 탐지/차단 로그	WAPPLES audit.log	SIEM 서버 (192.168.6.10)	1년	주1회	유관순	
8	IPS-01	IPS 탐지/차단 로그	MFI event.log	SIEM 서버 (192.168.6.10)	1년	주1회	유관순	
9	OS 전체	시스템 인증 로그	/var/log/auth.log	/var/log/ 및SIEM	6개월	월1회	홍길동	SSH 로그인 포함

붙임16 백업 현황 및 복구 관리대장 (샘플)

※ 백업 대상, 주기, 저장 위치, 복구 테스트 이력을 체계적으로 관리하시기 바랍니다.

■ 업체명: 작성일:

순번	대상 서버	백업 대상 데이터	백업 유형	백업 주기	저장 위치	최근 백업일	복구 테스트일	복구 소요 시간
※ 백업본은 원본 서버와 물리적으로 분리된 장소에 보관 권고 | 최소 분기1회 복구 테스트 수행 권고								
1	DB-01~02	MySQL DB 전체(가입자/발송 데이터)	전체백업	매일02:00	BAK-01 (/backup/db/) + 외부 NAS	2025-03-10	2025-02-28	4시간(복구 테스트 완료)
2	DB-01~02	MySQL DB 바이너리 로그	증분백업	1시간마다	BAK-01 (/backup/binlog/)	2025-03-10	2025-02-28	
3	WEB-01	웹 소스코드 및 설정파일	전체백업	매주 일요일03:00	BAK-01 (/backup/web/)	2025-03-09	2025-01-31	30분
4	WAS-01~02	WAS 설정파일 및 배포 파일	전체백업	배포 시+ 주1회	BAK-01 (/backup/was/)	2025-03-08	2025-01-31	
5	FW-01, WAF-01	방화벽/WAF 설정파일	전체백업	정책 변경 시+ 월1회	관리망 파일 서버	2025-03-01	2025-01-15	
6	전체 서버	OS 시스템 이미지	전체백업 (스냅샷)	분기1회	외부 스토리지(오프사이트)	2025-01-01	2025-01-15	1일(복구 테스트 완료)

붙임17 부하분산(Load Balancing) 구성 현황표 (샘플)

※ L4/L7 스위치 또는 소프트웨어 방식의 부하분산 장비 구성 현황을 기재하시기 바랍니다.

■ 업체명: 작성일:

순번	장비명	VIP 주소	서비스 포트	분산 방식	대상 서버 목록	상태 점검 방법	제품명	도입일
※ 분산 방식: Round Robin / Least Connection / IP Hash / Active-Standby 등 | 상태 점검(Health Check) 설정 필수								
1	LB-WEB-01	192.168.0.10	TCP/80,443	Round Robin	WEB-01(192.168.1.10)	HTTP 상태코드 확인(GET /health)	파이오링크 AX	2023-03-01
2	LB-WAS-01	192.168.1.100	TCP/8080	Least Connection	WAS-01(192.168.2.10) WAS-02(192.168.2.11)	TCP 포트 응답 확인	파이오링크 AX	2023-03-01
3	LB-DB-01	192.168.2.100	TCP/3306	Active-Standby	DB-01(Master) DB-02(Slave)	MySQL ping 쿼리	자체 구현 (HAProxy)	2023-03-01

붙임18 정보보호시스템 운영 현황 종합표 (샘플)

※ 방화벽, 웹방화벽, IPS, IDS, DB접근통제, DB암호화, 웹쉘탐지 등 운영 중인 모든 정보보호시스템을 기재하시기 바랍니다.

■ 업체명: 작성일:

순번	시스템명	유형	제조사/제품명	버전	설치 위치	담당자	도입일	유지보수 만료일	운영 상태
※ 유지보수 만료 전 갱신 또는 대체 계획 수립 필요 | 운영상태: 정상/점검중/장애/미운영 중 선택									
1	FW-01	방화벽 (Firewall)	파이오링크 TiFRONT	v3.2	외부-DMZ 경계	유관순 (보안팀)	2023-03-01	2026-02-28	정상
2	FW-02	방화벽 (Firewall)	Juniper SRX300	Junos 21.4	DMZ-내부망 경계	유관순 (보안팀)	2023-03-01	2026-02-28	정상
3	WAF-01	웹방화벽 (WAF)	PENTA WAPPLES	v5.0	DMZ 웹서버 앞단	유관순 (보안팀)	2023-03-01	2026-02-28	정상
4	IPS-01	침입방지 시스템 (IPS)	시큐아이 MFI-1200	v4.1	외부-DMZ 경계	유관순 (보안팀)	2023-03-01	2026-02-28	정상
5	IDS-01	침입탐지 시스템 (IDS)	Snort 기반 자체구축	v3.1	DMZ 내부	홍길동 (인프라팀)	2023-06-01	-	정상
6	DAM-01	DB접근통제	신시웨이 PETRA	v4.2	DB서버 앞단	강감찬 (DBA팀)	2023-03-01	2026-02-28	정상
7	DBE-01	DB암호화	이글로벌시스템즈D-ARES	v3.5	DB-01~02 적용	강감찬 (DBA팀)	2023-03-01	2026-02-28	정상
8	WSC-01	웹쉘탐지	웹쉘어택WAS 연동	v2.0	WAS-01~02	이순신 (인프라팀)	2023-06-01	2025-12-31	정상

붙임19 네트워크 장비 관리자 IP 관리대장 (샘플)

※ 네트워크 장비(방화벽, 스위치, 라우터, IPS 등)에 접속 가능한 관리자 IP를 관리하는 대장입니다.
※ 관리자 접속은 지정된 IP에서만 허용하며, 미인가 IP에서의 접근은 차단되어야 합니다.

■ 업체명 : 작성일 : 최종 검토일 :

순번	장비명	장비 유형	장비 IP	허가된 관리자 IP	관리 포트	관리 계정 ID	담당자	관리 방식
※ 허가된 관리자 IP 이외의 접속 시도는 방화벽/ACL에서 차단되어야 함 | 관리 계정은 공용 계정 사용 금지, 개인별 계정 발급 권고								
1	FW-01 (외부방화벽)	방화벽 (Firewall)	192.168.0.1	192.168.5.10 (관리자PC)	TCP/443 (HTTPS)	admin	유관순 (보안팀)	H/W 웹UI 접속
2	FW-02 (내부방화벽)	방화벽 (Firewall)	192.168.2.1	192.168.5.10 (관리자PC)	TCP/443 (HTTPS)	admin	유관순 (보안팀)	H/W 웹UI 접속
3	WAF-01 (웹방화벽)	웹방화벽 (WAF)	192.168.1.5	192.168.5.10 (관리자PC)	TCP/8443 (HTTPS)	wafadmin	유관순 (보안팀)	관리콘솔 접속
4	IPS-01	IPS	192.168.0.2	192.168.5.10 (관리자PC)	TCP/22 (SSH)	ipsadmin	유관순 (보안팀)	SSH 접속
5	SW-CORE-01 (코어스위치)	L3 스위치	192.168.0.10	192.168.5.10 (관리자PC)	TCP/22 (SSH)	admin	홍길동 (인프라팀)	SSH 접속
6	SW-DMZ-01 (DMZ스위치)	L2 스위치	192.168.1.1	192.168.5.10 (관리자PC)	TCP/22 (SSH)	admin	홍길동 (인프라팀)	SSH 접속
7	LB-WEB-01 (L4스위치)	부하분산 장비	192.168.0.10	192.168.5.10 (관리자PC)	TCP/8080 (HTTP)	lbadmin	홍길동 (인프라팀)	관리콘솔 접속

▶ 관리자 비인가 접속 시도 현황 (월별 모니터링)

점검 월	대상 장비	비인가 접속 시도 횟수	출발지 IP	접속 시도 계정	조치 내용	담당자 확인
※ 침입차단시스템 로그 및 각 장비 인증 로그 기반으로 월 1회 이상 점검 수행 | 비인가 접속 시도 발생 시 즉시 차단 조치						
2025년 1월	FW-01	3회	203.xxx.xxx.xx (해외IP)	admin (브루트포스 의심)	IP 차단 조치 완료	유관순
2025년 2월	-	0회	-	-	이상 없음	유관순
2025년 3월	-	0회	-	-	이상 없음	유관순

붙임20 네트워크 장비 주기적 점검기록 [위탁 관리용] (샘플)

※ 네트워크 장비를 위탁하여 운영하는 경우, 위탁업체가 수행하는 주기적 점검 결과를 아래 양식에 기록하여 제출하시기 바랍니다.
※ 점검 주기: 월 1회 이상 권고 | 점검 결과는 발주처(수검자) 담당자가 반드시 확인·서명하여야 합니다.

▶ 점검 개요

위탁업체명	(주)○○정보기술	계약 기간	2024.01.01 ~ 2025.12.31
점검 기간	2025년 1월 1일 ~ 1월 31일	점검 담당자 (위탁업체)	홍길동 (010-xxxx-xxxx)
점검 대상 장비	방화벽(FW-01, FW-02), WAF-01, IPS-01, 스위치(SW-CORE-01, SW-DMZ-01)	확인자 (발주처)	이순신 (인프라팀장)

▶ 점검 항목 및 결과

순번	점검 대상 장비	점검 항목	점검 내용	점검 결과	조치 내용	확인
*※ 점검 결과: 정상 / 이상(즉시 조치) / 이상(조치계획 수립) / 해당없음	확인란: 발주처 담당자 서명 또는 날인*					
1	FW-01 FW-02	**정책 유효성 확인**	미사용 방화벽 규칙 존재 여부 점검 - 최근 90일간 미사용 정책 현황 확인 - 불필요 정책 정리 여부 확인	**정상**	미사용 규칙 3개 삭제 조치	☐
2	FW-01 FW-02	**로그 분석**	방화벽 로그 이상징후 분석 - 차단 이벤트 급증 여부 확인 - 비인가 접속 시도 현황 확인	**정상**	이상 없음	☐
3	FW-01 FW-02	**펌웨어/버전 확인**	현재 운영 중인 펌웨어 버전 확인 - 제조사 최신 보안 패치 적용 여부 - 취약점 공지 해당 여부	**정상**	최신 버전 운영 중 (v3.2)	☐
4	WAF-01	**탐지 패턴 업데이트**	웹방화벽 탐지 패턴 최신화 여부 - 신규 공격 패턴 DB 업데이트 확인 - 패턴 업데이트 일자 확인	**정상**	2025.01.15 패턴 업데이트 완료	☐
5	WAF-01	**탐지 이벤트 분석**	WAF 탐지/차단 이벤트 분석 - 정탐/오탐 비율 분석 - 신규 공격 패턴 식별	**정상**	SQL Injection 시도 87건 차단 (정탐)	☐
6	IPS-01	**시그니처 업데이트**	IPS 시그니처 최신화 여부 - 신규 취약점 시그니처 적용 확인 - 오탐 발생 시그니처 튜닝	**정상**	2025.01.20 시그니처 업데이트 완료	☐
7	IPS-01	**탐지/차단 현황 분석**	IPS 이벤트 로그 분석 - 공격 유형별 탐지 현황 - 주요 출발지 IP 분석	**정상**	Port Scan 23건, Brute Force 12건 차단	☐
8	SW-CORE-01 SW-DMZ-01	**포트 상태 점검**	스위치 포트 사용 현황 점검 - 미사용 포트 shutdown 여부 - 불필요 VLAN 제거 여부	**정상**	미사용 포트 8개 shutdown 유지	☐
9	SW-CORE-01 SW-DMZ-01	**접근제어 목록(ACL) 점검**	스위치 ACL 적용 현황 확인 - 허가된 IP 대역 외 접근 차단 여부 - Management VLAN 격리 여부	**정상**	이상 없음	☐
10	전체 장비	**관리자 계정 점검**	관리자 계정 현황 점검 - 기본 패스워드 사용 여부 - 미사용 계정 존재 여부 - 패스워드 변경 이력 확인	**정상**	기본 패스워드 미사용 확인, 계정 이상 없음	☐
11	전체 장비	**백업 및 설정 보존**	장비 설정파일 백업 현황 확인 - 월간 설정 백업 수행 여부 - 백업본 무결성 확인	**정상**	2025.01.28 설정 백업 완료 (관리망 서버 보관)	☐

▶ 점검 종합 의견

종합 의견	금월 점검 결과, 네트워크 장비 전반에 걸쳐 특별한 이상징후는 발견되지 않았습니다. 단, 방화벽 미사용 규칙 3개를 정리하였으며, WAF 및 IPS 시그니처는 최신 상태로 유지되고 있습니다. 향후 분기 내 방화벽 정책 전체 재검토를 수행할 예정입니다.
주요 조치 사항	① 방화벽 미사용 규칙 3개 삭제 (FW-01) ② WAF 탐지 패턴 업데이트 완료 (2025.01.15) ③ IPS 시그니처 업데이트 완료 (2025.01.20)
차기 점검 예정일	2025년 2월 28일

작성자 (위탁업체)	검토자 (위탁업체)	확인자 (발주처 담당)	승인자 (발주처 책임자)
홍길동 / 010-xxxx-xxxx (서명) ___년 ___월 ___일	김점검 (팀장) (서명) ___년 ___월 ___일	이순신 (인프라팀장) (서명) ___년 ___월 ___일	박책임 (CISO) (서명) ___년 ___월 ___일

붙임21 위탁업체 취약점 정기점검 보고서 양식 [반기/년간] (샘플)

※ 정보통신설비를 위탁하여 운영하는 경우, 위탁업체로부터 이 양식에 준하는 반기 또는 연간 취약점 점검 보고서를 제출받아야 합니다.
※ 위탁업체 자체 보고서 양식 사용 시에도 아래 항목들이 모두 포함되어야 합니다.

▶ 보고서 기본 정보

보고서 제목	문자발송시스템 정보통신설비 취약점 정기점검 결과 보고서 (2025년 상반기)		
위탁업체명	(주)○○정보기술	**제출일**	2025년 7월 15일
발주처(수검자)	○○문자발송(주)	**계약번호**	계약-2024-001호
점검 기간	2025년 1월 1일 ~ 2025년 6월 30일 (6개월)	**점검 주기**	반기 1회 (연간 2회 수행)
점검 범위	웹서버(WEB-01), WAS서버(WAS-01~02), DB서버(DB-01~02), 방화벽(FW-01~02), WAF-01, IPS-01, 백업서버(BAK-01), 관리용PC(MGMT-01)		
점검 방법	자동화 도구(Nessus, OpenVAS) + 수동 점검 병행	**점검 기준**	KISA 주요 정보통신기반시설 취약점 점검 기준, OWASP Top 10

▶ 취약점 점검 결과 요약

구분	점검 대상	발견 취약점 (위험도 상)	발견 취약점 (위험도 중)	발견 취약점 (위험도 하)	조치 완료	잔여 취약점 (조치 계획 수립)
웹 어플리케이션	WEB-01, WAS-01~02	1	3	4	7	1
운영체제(OS)	WEB-01, WAS-01~02, DB-01~02, BAK-01	0	2	6	8	0
DBMS	DB-01~02	0	1	2	3	0
네트워크 장비 / 보안장비	FW-01~02, WAF-01, IPS-01	0	0	3	3	0
관리용 PC	MGMT-01	0	1	1	1	1
합 계	**전체 8개 대상**	**1**	**7**	**16**	**22**	**2**

▶ 주요 취약점 상세 목록

순번	점검 분야	대상 서버	취약점 내용	위험도	CVSS 점수	조치 방법	조치 기한	조치 상태	조치자
※ CVSS(Common Vulnerability Scoring System) 점수: 0~10 (7.0 이상: 상, 4.0~6.9: 중, 4.0 미만: 하)									
1	웹 어플리케이션	WAS-01	XSS 취약점 (비밀번호 찾기 페이지 입력값 미검증)	**중**	6.1	입력값 필터링 강화 (XSS 방지 라이브러리 적용)	2025-08-15	**완료**	이순신
2	웹 어플리케이션	WAS-01	세션 관리 취약점 (세션 만료 시간 미설정)	**중**	5.3	세션 만료시간 30분으로 설정	2025-08-15	**완료**	이순신
3	웹 어플리케이션	WAS-01~02	불필요한 HTTP 메서드 허용 (PUT, DELETE)	**하**	3.7	WAF 정책 및 서버 설정에서 불필요 메서드 차단	2025-08-31	**완료**	이순신
4	웹 어플리케이션	WEB-01	디렉토리 리스팅 노출	**상**	7.5	아파치 설정 변경 (Options -Indexes)	2025-07-31	**완료**	홍길동

순번	점검 분야	대상 서버	취약점 내용	위험도	CVSS 점수	조치 방법	조치 기한	조치 상태	조치자
5	OS	WAS-01~02	OpenSSH 구버전 사용 (CVE-2024-6387)	**중**	5.1	OpenSSH 최신 버전(9.8p1) 업그레이드	2025-08-31	**완료**	홍길동
6	OS	DB-01~02	불필요한 서비스 활성화 (rpcbind)	**하**	3.5	rpcbind 서비스 비활성화	2025-09-30	**완료**	강감찬
7	DBMS	DB-01	MySQL 감사 로그 미설정	**중**	4.3	MySQL general_log 및 audit_log 플러그인 활성화	2025-08-31	**완료**	강감찬
8	관리용 PC	MGMT-01	백신 정의 파일 구버전 (30일 이상 미업데이트)	**중**	5.0	백신 업데이트 자동화 정책 적용	2025-09-30	**조치 중 (계획 수립)**	홍길동

▶ 조치 완료 현황 요약

총 발견 취약점	조치 완료(상)	조치 완료(중)	조치 완료(하)	잔여 취약점	잔여 취약점 조치 완료 예정일
24건	**1건 (100%)**	**6건 (86%)**	**15건 (94%)**	**2건**	2025년 9월 30일

▶ 종합 의견 및 권고사항

종합 의견	2025년 상반기 취약점 점검 결과, 총 24건의 취약점이 발견되었으며 그 중 22건(91.7%)에 대한 조치가 완료되었습니다. • 위험도 '상' 취약점 1건(디렉토리 리스팅 노출)에 대해서는 점검 후 즉시 조치 완료하였습니다. • 위험도 '중' 취약점 7건 중 6건 조치 완료, 잔여 1건(MGMT-01 백신 업데이트)은 2025.9.30까지 조치 예정입니다. • 위험도 '하' 취약점 16건 중 15건 조치 완료, 잔여 1건도 2025.9.30까지 조치 예정입니다. ★ **권고사항:** ① 관리용 PC 백신 자동 업데이트 정책 강화 ② 분기 1회 WAF 정책 재검토 수행 권고 ③ MySQL 감사 로그 정기적 검토 체계 수립 권고

▶ 확인 서명

작성자 (위탁업체)	검토자 (위탁업체)	확인자 (발주처 담당)	승인자 (발주처 책임자)
홍길동 / 010-xxxx-xxxx (서명) ___년 ___월 ___일	김점검 (팀장) (서명) ___년 ___월 ___일	이순신 (인프라팀장) (서명) ___년 ___월 ___일	박책임 (CISO) (서명) ___년 ___월 ___일