



| ICT 중소기업 정보보호 | 종합컨설팅 결과보고서

세경하이테크

2021. 08. 25 (수)

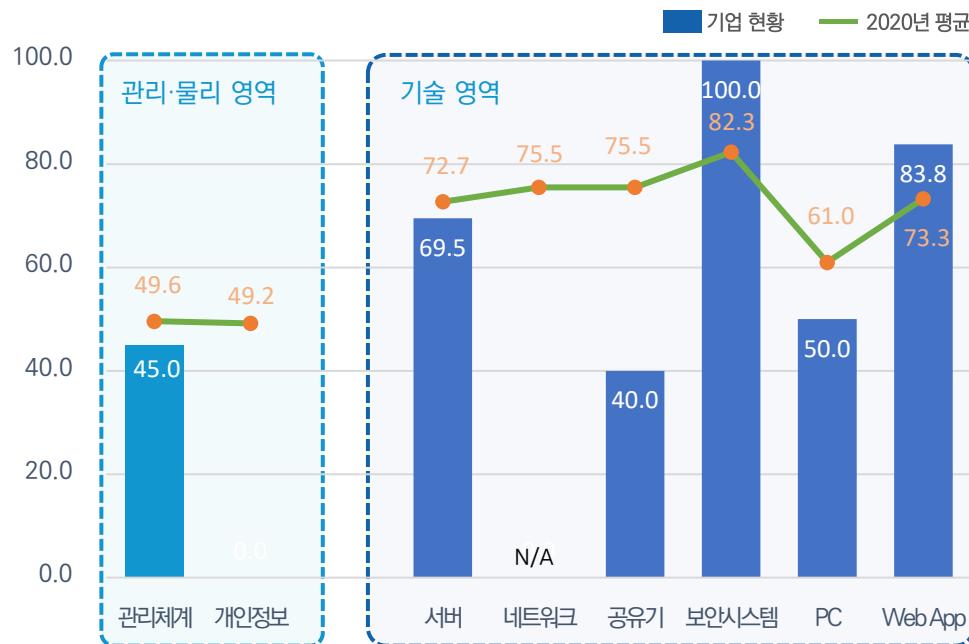


SEEDGEN Consortium

Keep IT simple. We've got you covered.

- 정보보호 컨설팅 수행결과 정보보호 수준 지수는 64.6%의 이행률을 보이고 있으며, 관리 및 기술영역에서 업무용 단말기기 등을 통한 기밀자료 유출 방지 대책이 마련 되어있지 않아 데이터 유출 방지(DLP) 제품군의 보안솔루션 도입을 추천 드립니다.
- 해당 수혜사는 중요 데이터(도면, 디자인 파일 등)를 개인 PC에 보관하고 PC의 공유폴더 기능을 이용해 파일을 공유하고 있어 적절한 권한 부여 등의 보안정책 관리가 이행되지 않아 데이터의 유출 및 체계적인 데이터 관리가 어려워 백업/복구 관리 시스템을 통한 체계적 정보 자산 관리가 필요합니다.

✓ 종합컨설팅 결과 [종합평균 : 64.6%]



✓ 추천 보안솔루션 및 기대효과

※ 솔루션 추천에 대한 세부사항은 23Page 참조

1 순위 : 데이터 유출 방지(DLP)

네트워크 DLP는 사용자의 고의 또는 실수, 외부 해킹, 멀웨어 등을 통해 네트워크를 이용한 정보유출을 컨텐츠 수준에서 차단. 단말 DLP는 사용자의 고의 또는 실수, 외부 해킹, 멀웨어 등을 통해 단말 호스트(PC, 서버, 모바일 등)에서의 정보유출을 차단. 각종 외부 인터페이스(USB, 외장하드, CD/DVD, 프린트, 블루투스 등)를 통해 유출되는 정보의 내용을 감시/차단

2 순위 : 백업/복구 관리 시스템

자료 손실을 예방하기 위해 자료를 미리 다른 곳에 임시로 보관해 두었다가 원래 상태로 복구해주는 관리 솔루션

✓ 주요 보안대책

	보안대책	위험등급
관리 · 물리 영역	▪ 정보보호 활동 식별 및 관리 시행	중
	▪ 공용 업무 환경에 대한 보안관리 시행	상
	▪ 사용자 PC를 통한 정보유출 차단대책 마련	상
	▪ 내부자료 유출방지 강화	중
	▪ 보조저장매체 관리 및 통제 강화	중
	▪ 백업 및 복구관리 시행	상
	보안대책	중요도
기술 영역	▪ 윈도우 서버의 원격터미널 접속 타임아웃 설정	상
	▪ 공유기 SSID 숨김 기능 설정	상
	▪ PC 화면보호기 대기 시간 및 암호 설정	상
	▪ 웹서버의 정보 누출 차단 설정	상

데이터 유출 방지(DLP) 제품군 도입

종합컨설팅 결과 내부 기밀자료 유출 방지 대책의 부재로 내부 정보 유출 가능성이 존재하여 DLP 제품군을 1순위로 추천하며, 해당 솔루션 도입 시 외부 해킹 및 내부 인력으로 부터의 주요 정보 유출 차단 효과가 있을 것으로 판단됩니다.



과학기술정보통신부



CONTENTS



현황 분석

- 수혜사의 정보보호 현장 컨설팅 상세 결과



대책 수립

- 정보보호 현장 컨설팅 결과의 취약한 부분에 대한 상세 대책

블임

사업 개요

진단항목

보안솔루션

I

현황 분석

1. 영역별 진단 현황
2. 관리·물리영역 진단 결과
3. 기술영역 진단 결과

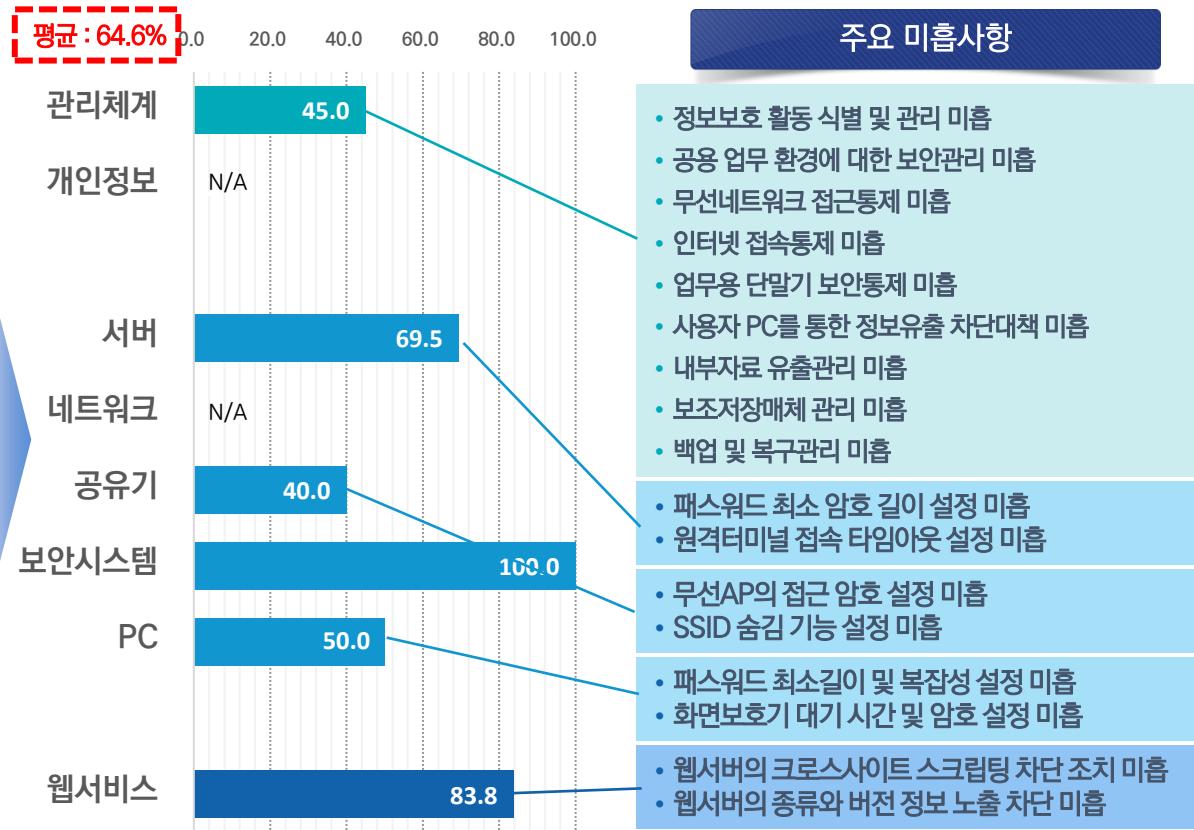
1. 영역별 진단 현황

1.1 진단 영역 및 주요 미흡사항

- 진단 영역 수행결과 정보보호 수준 지수는 64.6%의 이행률을 보이고 있으며, 특히 업무용 단말기에 대한 통제 정책이 수립되지 않아 비인가자의 접근 및 내부 중요정보 유출 등의 위험이 있어 내부 중요정보 유출에 대한 대책 수립이 필요하다고 판단됩니다.

진단 영역 및 주요 미흡사항

진단 영역			
분야	영역	점검여부	미 점검시 사유
관리	정보보호 관리체계	점검	
	개인정보 처리방침	미점검	• 개인정보의 처리가 존재하지 않음
기술	서버	점검	
	네트워크	미점검	• 공유기 점검으로 대체
	공유기	점검	
	보안시스템	점검	
	PC	점검	
웹 보안		점검	

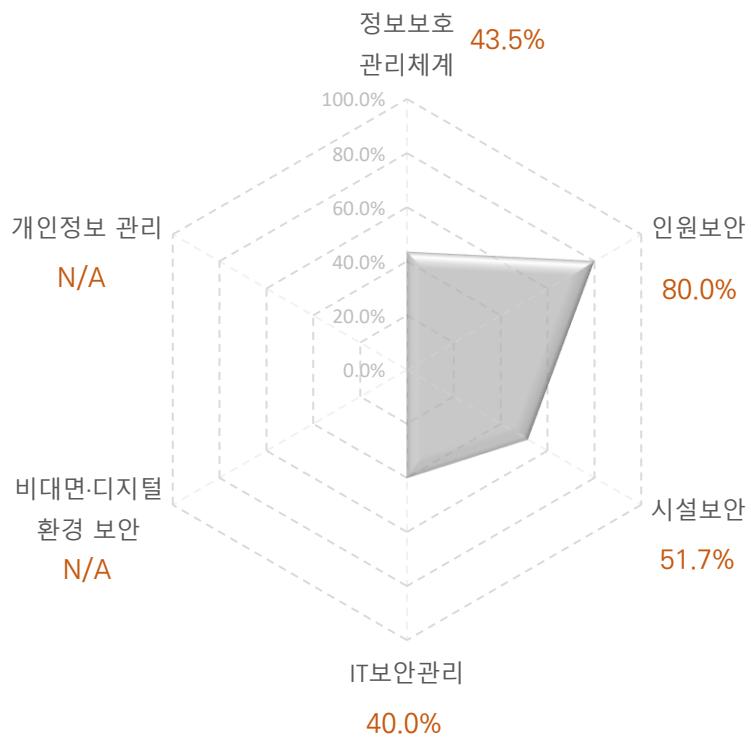


2. 관리·물리영역 진단 결과

2.1 정보보호 관리체계 보안 수준

- 정보보호 관리체계의 6개 영역별 점검 결과 보안율은 45.0%로 분석되었으며, 그 중 가장 취약한 영역인 IT보안관리의 업무용 단말기 및 보조저장매체 관리에 대한 우선적인 보안대책 수립이 필요합니다.

정보보호 관리체계 보안 수준



□ 평균 보안수준 : 45.0%

※ 권고 보안수준 : 80%

□ 가장 취약한 영역 : IT보안관리

□ 가장 보안수준이 높은 영역 : 인원보안

주요 보안대책

보안대책 항목	소요 기간
정보보호 활동 식별 및 관리 시행	장기
공용 업무 환경에 대한 보안관리 시행	중기
무선네트워크 접근통제 강화	단기
업무용 단말기 보안통제 강화	단기
내부자료 유출방지 강화	단기
백업 및 복구관리 시행	중기

※ 영역별 상세 현황 및 조치방안은 별첨 '세경하이테크 - 관리체계 진단 결과 보고서_v1.0' 파일 참조

※ 주요 보안대책 수행 기간 : 단기(3개월), 중기(6개월), 장기(12개월)

2. 관리·물리영역 진단 결과

2.2 위험 분석 및 평가 결과

- 종합적인 위험 분석 결과, 전체 48개 위험 중에서 위험도가 하인 13개를 제외하고 중 16개, 상 19개로 도출되어 위험도가 상인 주요 미흡 사항부터 우선적인 조치가 필요합니다.

위험 분석 및 평가 결과



분포	주요 미흡 사항
상	<ul style="list-style-type: none"> 공용 업무 환경에 대한 보안관리 미흡 무선네트워크 접근통제 미흡 인터넷 접속통제 미흡 업무용 단말기 보안통제 미흡 사용자 PC를 통한 정보유출 차단대책 미흡 백업 및 복구관리 미흡
중	<ul style="list-style-type: none"> 내부자료 유출관리 미흡 보조저장매체 관리 미흡

※ 영역별 상세 현황 및 조치방안은 별첨 '세경하이테크 - 관리체계 진단 결과 보고서_v1.0' 파일 참조

평가기준

평가항목	점수	내용
항목 중요도	3	점검항목의 효과(1점), 시간(1개월 이내)(1점), 예산(1점)으로 평가한 점수가 3점에 해당
	2	점검항목의 효과(1점), 시간(1개월 이내)(1점), 예산(1점)으로 평가한 점수가 2점에 해당
	1	점검항목의 효과(1점), 시간(1개월 이내)(1점), 예산(1점)으로 평가한 점수가 1점에 해당
위험	3	법적준거성 평가 결과 벌칙이 벌금 이상의 경우
	2	법적준거성 평가 결과 벌칙이 과태료인 경우
	1	법적준거성 평가 결과 위협이 낮은 경우
취약성	1	평가 결과 '미이행'으로 'D' 선택 시
	0.7	평가 결과 '부분이행'으로 'C' 선택 시
	0.4	평가 결과 '부분이행'으로 'B' 선택 시
	0	평가 결과 '이행'으로 'A' 선택 시

위험도 산정

$$\text{위험등급} = \{\text{항목 중요도}\} \times \{\text{위험}\} \times \{\text{취약성}\}$$

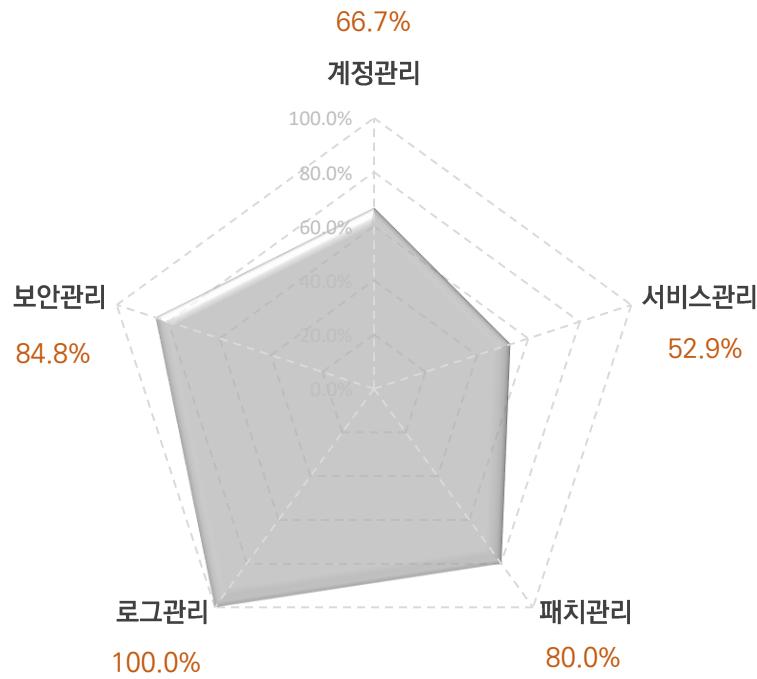
$$\text{상: } \text{위험등급} >= 4 \quad \text{중: } 4 > \text{위험등급} > 1 \quad \text{하: } 1 > \text{위험등급}$$

3. 기술영역 진단 결과

3.1 서버 취약점 진단 결과

- 서버 취약점 진단 결과 보안율은 69.5%로 분석되었으며, 그 중 가장 취약한 영역인 계정관리 및 서비스관리에 대해 관리자 그룹에 최소한의 사용자 포함, 공유 권한 및 사용자 그룹 설정 등에 대한 보안대책 적용이 우선적으로 필요하다고 판단됩니다.

공유기 보안 수준



□ 평균 보안수준 : 69.5%

※ 권고 보안수준 : 100%

□ 가장 취약한 영역 : 파일 및 디렉터리 관리

□ 가장 보안수준이 높은 영역 : 로그관리, 패치관리

주요 보안대책

보안대책 항목	보안 가이드라인	소요 기간
관리자 그룹에 최소한의 사용자 포함	9 Page	단기
패스워드 최소 암호 길이	15 Page	단기
공유 권한 및 사용자 그룹 설정	22 Page	단기
FTP 서비스 구동 점검	32 Page	단기
원격터미널 접속 타임아웃 설정	42 Page	단기

※ 주요 보안대책 수행 기간 : 단기(3개월), 중기(6개월), 장기(12개월)

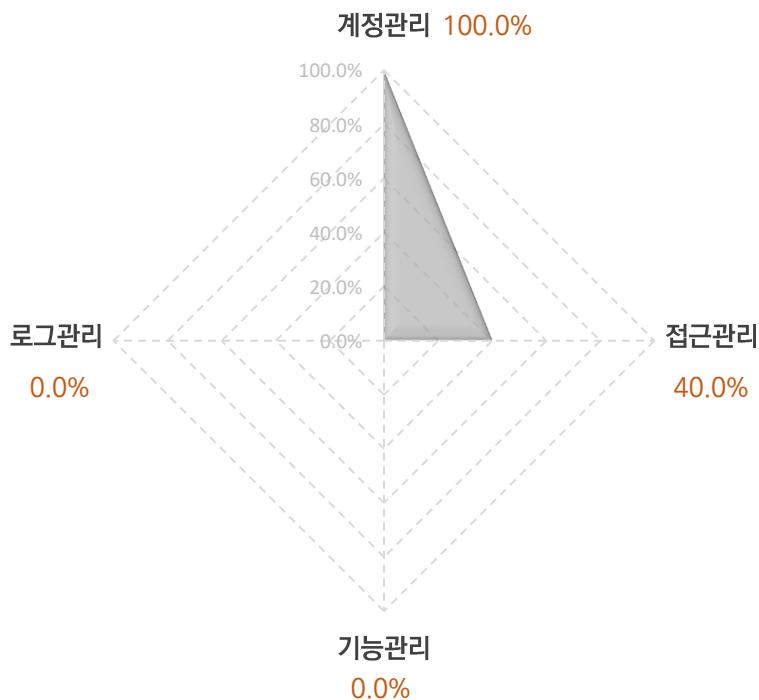
※ 영역별 상세 현황 및 조치방안은 별첨 '세경하이테크 - 공유기 취약점 진단 보고서_v1.0' 및 'KISA - 공유기 보안 가이드라인_v1.0' 파일 참조

3. 기술영역 진단 결과

3.2 공유기 취약점 진단결과

- 공유기 취약점 진단 결과 보안율은 40.0%로 분석되었으며, 그 중 가장 취약한 영역인 기능관리, 로그관리에 대해 최신 펌웨어 업데이트 시행 등의 보안대책 적용이 우선적으로 필요하다고 판단됩니다.

공유기 보안 수준



□ 평균 보안수준 : 40.0%

※ 권고 보안수준 : 100%

□ 가장 취약한 영역 : **기능관리, 로그관리**

□ 가장 보안수준이 높은 영역 : **계정관리**

주요 보안대책

보안대책 항목	보안 가이드라인	소요 기간
공유기의 SSID 숨김 기능 설정	11 Page	단기
공유기의 접근 허용 단말 MAC 등록 및 필터링 적용	12 Page	단기
공유기의 최신 펌웨어 업데이트 실행	15 Page	단기
공유기의 로그 기능 실행	17 Page	단기

※ 주요 보안대책 수행 기간 : 단기(3개월), 중기(6개월), 장기(12개월)

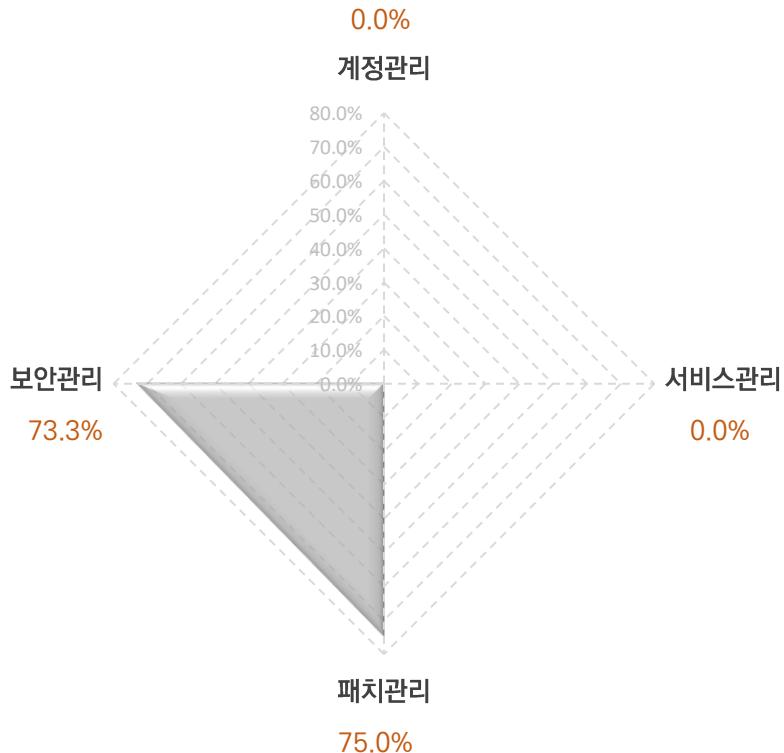
※ 영역별 상세 현황 및 조치방안은 별첨 '세경하이테크 - 공유기 취약점 진단 보고서_v1.0' 및 'KISA - 공유기 보안 가이드라인_v1.0' 파일 참조

3. 기술영역 진단 결과

3.3 PC 취약점 진단결과

- 총 3대의 PC 취약점 진단 결과 보안율은 평균 50.0%로 분석되었으며, 그 중 가장 취약한 영역인 계정관리, 서비스관리에 대해 패스워드 보안 설정, 공유 폴더 제거, 불필요한 서비스 제거 등의 보안대책 적용이 우선적으로 필요하다고 판단됩니다.

PC 보안 수준



□ 평균 보안수준 : 50.0%

※ 권고 보안수준 : 100%

□ 가장 취약한 영역 : 계정관리, 서비스관리

□ 가장 보안수준이 높은 영역 : 패치관리

주요 보안대책

보안대책 항목	보안 가이드라인	소요 기간
패스워드 최소 길이 8자리 이상으로 설정	1 Page	단기
기본 공유 폴더 제거 및 자동 공유 방지 설정	4 Page	단기
불필요한 서비스 제거	11 Page	단기
화면보호기 대기 시간 설정 및 PC 암호 설정	31 Page	단기

※ 주요 보안대책 수행 기간 : 단기(3개월), 중기(6개월), 장기(12개월)

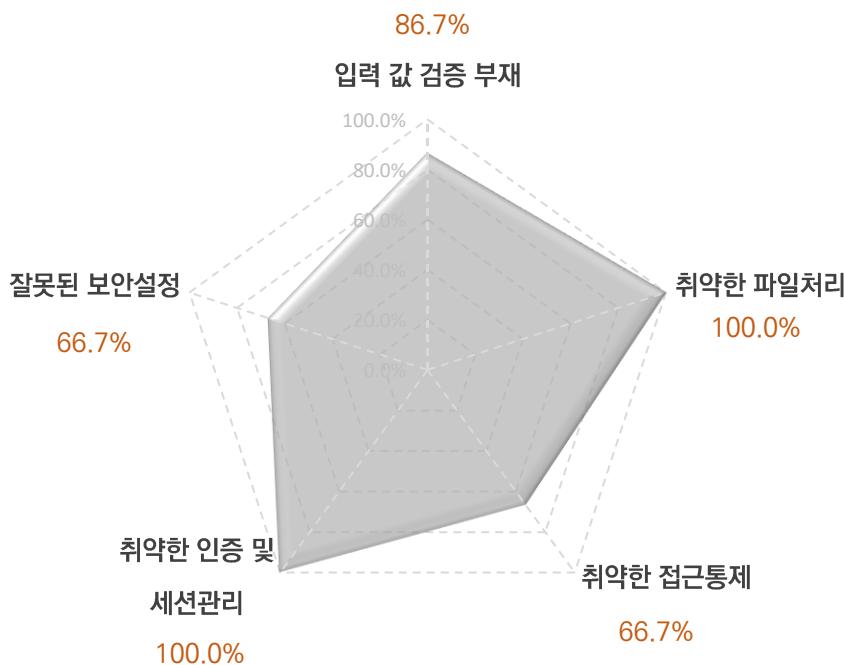
※ 영역별 상세 현황 및 조치방안은 별첨 '세경하이테크 - PC 취약점 진단 보고서_v1.0' 및 'KISA - PC 보안 가이드라인_v1.0' 파일 참조

3. 기술영역 진단 결과

3.4 웹 어플리케이션 취약점 진단결과 [1/3]

- 웹 어플리케이션에 대한 취약점 진단 결과 보안율은 83.8%로 분석되었으며, 그 중 잘못된 보안설정 영역의 데이터 평문 전송, 정보 누출 등에 대한 우선적인 보안대책 적용이 필요하다고 판단됩니다.

웹 어플리케이션 보안 수준



- 평균 보안수준 : 83.8% ※ 권고 보안수준 : 100%
- 가장 취약한 영역 : 취약한 접근통제, 잘못된 보안설정
- 가장 보안수준이 높은 영역 : 취약한 파일처리 등

주요 보안대책

주요 미흡 항목에 대한 보안대책	보안 가이드라인	소요 기간
[입력 값 검증 부재 : 크로스사이트 스크립팅] 해당 파라미터의 입력값에서 특수문자, 자바스크립트 코드를 필터링 적용	17 Page	중기
[취약한 접근 통제 : 관리자페이지 노출] 관리자 페이지의 위치를 이동시키고 인증 등의 접근통제 수행	41 Page	단기
[잘못된 보안설정 : 데이터 평문 전송] 중요한 정보를 전송할 때는 HTTPS등의 암호화를 사용하여 전송	57 Page	단기
[잘못된 보안설정 : 정보 누출] 웹서버의 설정에서 헤더에 웹서버의 정보가 노출될 수 있는 항목 제거	64 Page	단기

※ 주요 보안대책 수행 기간 : 단기(3개월), 중기(6개월), 장기(12개월)

※ 영역별 상세 현황 및 조치방안은 별첨 '세경하이테크 – 웹 어플리케이션 취약점 진단 보고서_v1.0' 및 'KISA – 웹 어플리케이션 보안 가이드라인_v1.0' 파일 참조

3. 기술영역 진단 결과

3.4 웹 어플리케이션 취약점 진단결과 [2/3]

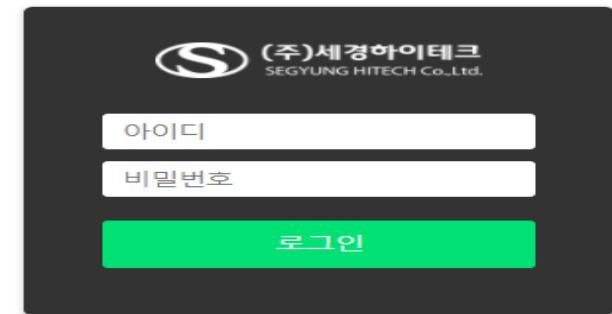
- 웹 어플리케이션에 대한 취약점 진단 결과 보안율은 83.8%로 분석되었으며, 그 중 잘못된 보안설정 영역의 데이터 평문 전송, 정보 누출 등에 대한 우선적인 보안대책 적용이 필요하다고 판단됩니다.

웹 어플리케이션 주요 취약점 현황

[크로스사이트 스크립팅]



[관리자페이지 노출]



현황 : find_val 파라미터에 자바스크립트 구문을 입력하면 해당 코드가 실행됨

현황 : /admin으로 이동하면 관리자 페이지가 인증 없이 노출됨

※ 영역별 상세 현황 및 조치방안은 별첨 '세경하이테크 – 웹 어플리케이션 취약점 진단 보고서_v1.0' 및 'KISA – 웹 어플리케이션 보안 가이드라인_v1.0' 파일 참조

3. 기술영역 진단 결과

3.4 웹 어플리케이션 취약점 진단결과 [3/3]

- 웹 어플리케이션에 대한 취약점 진단 결과 보안율은 83.8%로 분석되었으며, 그 중 잘못된 보안설정 영역의 데이터 평문 전송, 정보 누출 등에 대한 우선적인 보안대책 적용이 필요하다고 판단됩니다.

웹 어플리케이션 주요 취약점 현황

[데이터 평문 전송]

로그인 시 아이디와 패스워드가 평문으로 전송되어 아이디와 패스워드가 노출

Response Headers:

- Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
- Connection: Keep-Alive
- Content-Type: text/html; charset=UTF-8
- Date: Tue, 24 Aug 2021 23:50:25 GMT
- Expires: Thu, 19 Nov 1981 08:52:00 GMT
- Keep-Alive: timeout=15
- Pragma: no-cache
- Server: Apache/2.2.22 (Unix) mod_ssl/2.2.22 OpenSSL/1.0.2e-fips DAV/2 PHP/5.3.21
- Transfer-Encoding: chunked
- X-Powered-By: PHP/5.3.21

Request Headers:

- Host: 10.10.10.116
- User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4385.75 Safari/537.36
- Accept: */*
- Referer: http://10.10.10.116/login.php
- Content-Type: application/x-www-form-urlencoded
- Content-Length: 24
- Origin: http://10.10.10.116
- DNT: 1
- Sec-Fetch-Site: same-origin
- Sec-Fetch-Mode: navigate
- Sec-Fetch-Dest: document
- Sec-WebSocket-Version: 13
- Sec-WebSocket-Key: dGvBzqJLWZQHgk=
- Sec-WebSocket-Extensions: permessage-deflate; client_max_window_bits
- Upgrade: websocket
- TE:早急な応答を求める

[정보 누출]

▼ Response Headers

Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
 Connection: Keep-Alive
 Content-Type: text/html; charset=UTF-8
 Date: Tue, 24 Aug 2021 23:50:25 GMT
 Expires: Thu, 19 Nov 1981 08:52:00 GMT
 Keep-Alive: timeout=15
 Pragma: no-cache
 Server: Apache/2.2.22 (Unix) mod_ssl/2.2.22 OpenSSL/1.0.2e-fips DAV/2 PHP/5.3.21
 Transfer-Encoding: chunked
 X-Powered-By: PHP/5.3.21

▼ Request Headers

현황 : http 응답 메시지에 서버의 정보가 노출되어 있음

현황 : 로그인 시 아이디와 패스워드가 평문으로 전송되어 아이디와 패스워드가 노출

※ 영역별 상세 현황 및 조치방안은 별첨 '세경하이테크 – 웹 어플리케이션 취약점 진단 보고서_v1.0' 및 'KISA – 웹 어플리케이션 보안 가이드라인_v1.0' 파일 참조

II

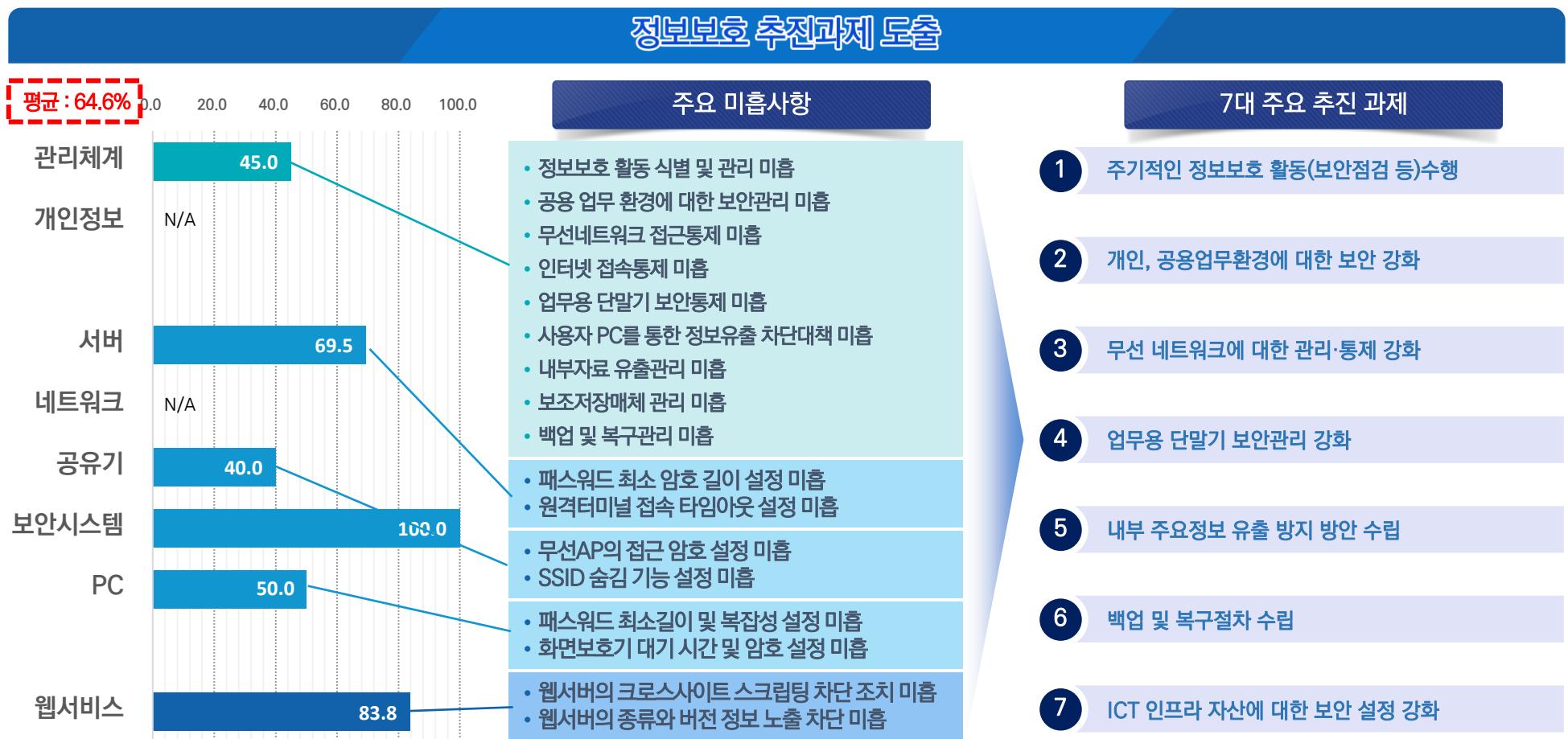
대책 수립

1. 추진과제 도출
2. 추진과제 세부사항
 - 주기적인 정보보호 활동(보안점검 등)수행
 - 개인, 공용업무환경에 대한 보안 강화
 - 무선 네트워크에 대한 관리·통제 강화
 - 업무용 단말기 보안관리 강화
 - 내부 주요정보 유출 방지 방안 수립
 - 백업 및 복구절차 수립
 - ICT 인프라 자산에 대한 보안 설정 강화
3. 보안솔루션 추천

1. 추진과제 도출

1.1 정보보호 추진과제 개요

- 관리적·물리적·기술적 취약점 분석 및 개인정보 취약점 진단결과에 대하여 원인을 분석하고, 이를 해결하기 위한 7대 주요 추진 과제를 도출하였습니다.



2. 추진과제 세부사항

2.1 주기적인 정보보호 활동(보안점검 등)수행

주요 작업 및 추진 일정

세부내용	<ul style="list-style-type: none"> ✓ 정보보호를 위해 주기적 또는 상시적으로 수행해야 하는 정보보호 활동을 식별하고 정기적으로 관리하여야 함 ✓ 정보보호 관리체계가 효과적으로 운영되는지를 점검하기 위한 보안점검을 수행하고 발견된 문제점을 경영진에게 보고하여야 함 ✓ 보안점검을 통해 식별된 관리체계 상의 문제점에 대한 근본 원인을 분석하여 개선조치 방안을 마련하여 이행하여야 함
주요 작업	<ol style="list-style-type: none"> 1. 정보보호 활동을 위한 정책 수립 및 식별 2. 정보보호 정책을 기반으로 한 연 1회 이상의 보안점검 실시 3. 보안점검을 통해 발견된 문제점에 대해 개선조치 이행
전제조건/제약사항	<ul style="list-style-type: none"> ✓ 정보보호 활동에 대한 임직원의 인식제고

AS-IS

- ✓ 정보보호를 위한 주기적·상시적 정보보호 활동을 식별 및 관리하고 있지 않음

TO-BE

- ✓ 정보보호 활동에 대한 정책 수립
- ✓ 연 1회 이상 보안점검 실시
- ✓ 보안점검 시 발견된 문제점에 대한 근본 원인 분석 및 개선조치 이행

구분	2021년						2022년					
	7월	8월	9월	10월	11월	12월	1월	2월	3월	4월	5월	6월
보안점검 실시						● →						
보안 미흡사항 개선							● →					

2. 추진과제 세부사항

2.2 개인, 공용업무환경에 대한 보안 강화

주요 작업 및 추진 일정

세부내용	<ul style="list-style-type: none"> ✓ 직원 PC에 암호설정 정책 마련 및 적용 ✓ 자리 이석시 화면보호기 잠금 기능 설정
주요 작업	<ol style="list-style-type: none"> 1. 직원 PC의 비밀번호 최소 자리수(8자리 이상) 설정 및 비밀번호 유효기간(90일) 설정 2. 직원 PC의 화면보호기(5분) 및 잠금기능 설정 3. 주요 문서 보관시 잠금장치가 있는 서랍등에 보관
전제조건/제약사항	<ul style="list-style-type: none"> ✓ 정보보호 교육 및 인식제고

AS-IS

- ✓ 각자 업무용 PC의 폴더 공유 기능을 활용해 파일을 공유하고 있음

TO-BE

- ✓ 정보보호 정책의 제정을 통해 개인 PC, 문서 등에 대한 보안대책 적용

구분	2021년						2022년					
	7월	8월	9월	10월	11월	12월	1월	2월	3월	4월	5월	6월
현황 파악				●	→							
정책 적용 및 시행					●	→						

2. 추진과제 세부사항

2.3 무선 네트워크에 대한 관리·통제 강화

주요 작업 및 추진 일정

세부내용	✓ 무선네트워크를 업무적으로 사용하는 경우 무선 AP 및 네트워크 구간 보안을 위해 인증, 송수신 데이터 암호화 등 보호대책을 마련하여 이행하여야 함
주요 작업	<ol style="list-style-type: none"> 1. 사내 보안정책에 무선랜 사용 금지 여부 체크 2. 인가된 무선기기만 접속할 수 있도록 설정 3. 주기적 검토를 통해 퇴직자, 비인가 사용기기 존재 여부 점검
전제조건/제약사항	✓ 무선 AP 사용에 대한 내부 정책 수립

AS-IS

- ✓ 회의실에 무선AP를 두고 비밀번호 설정이 되지 않은 상태로 내부망 접근이 가능 함

TO-BE

- ✓ 무선 AP 사용 가능 기기 등록 및 관리
- ✓ 무선 AP를 통한 송수신 데이터 암호화
- ✓ 단순 인터넷 접속을 위한 목적일 경우 내부망과 분리 진행

구분	2021년						2022년					
	7월	8월	9월	10월	11월	12월	1월	2월	3월	4월	5월	6월
현황 점검			●	→								
조치 시행				●	→							

2. 추진과제 세부사항

2.4 업무용 단말기 보안관리 강화

주요 작업 및 추진 일정

세부내용	<ul style="list-style-type: none"> ✓ PC, 모바일, 노트북 등 업무에 사용되는 단말기에 대하여 기기인증, 승인, 접근범위 설정, 기기 보안설정 등의 보안 통제 방안을 마련하여야 함 ✓ 서버, 네트워크시스템, 보안시스템, PC 등 자산별 특성 및 중요도에 따라 운영체제(OS)와 소프트웨어의 패치관리 절차 및 대책을 마련해야 함
주요 작업	<ol style="list-style-type: none"> 1. 업무에 사용되는 단말기의 보안 통제 방안 수립 2. ICT 자산(서버, 네트워크장비, 보안시스템, PC 등)의 운영체제와 소프트웨어에 최신 패치 적용
전제조건/제약사항	<ul style="list-style-type: none"> ✓ 임직원의 정보보호 인식제고 및 데이터 유출 방지(DLP) 솔루션 도입

	AS-IS						TO-BE					
	<ul style="list-style-type: none"> ✓ 사용자 PC 단말에 대한 별도의 관리 대책이 존재하지 않음 ✓ 외부·내부로부터의 기밀자료 유출 방지를 위한 대책을 마련하고 있지 않음 						<ul style="list-style-type: none"> ✓ 데이터 유출 방지 솔루션(DLP) 도입 ✓ 사내에서 허용된 단말기(PC, 모바일, 노트북 등)가 사용되도록 보안 통제 적용 ✓ ICT 자산의 운영체제 및 소프트웨어 최신 패치 적용 					

구분	2021년						2022년					
	7월	8월	9월	10월	11월	12월	1월	2월	3월	4월	5월	6월
정보보호 인식제고 및 보안솔루션 도입				●	→							
정책 수립 및 반영					●	→						

2. 추진과제 세부사항

2.5 내부 주요정보 유출 방지 방안 수립

주요 작업 및 추진 일정

세부내용	✓ 내부 기밀자료에 대해 외부 유출 및 내부 인력으로부터의 불법 복제 등을 방지하기 위한 관리 대책을 마련하여야 함
주요 작업	1. 내부 기밀자료 유출 방지를 위한 대책 마련 - 보안 솔루션(DLP, 문서중앙화 등) 도입 - 화면 캡쳐, 외부 이메일 및 메신저 등 차단 - 보조저장장치(USB 등) 사용 제한
전제조건/제약사항	✓ 보안솔루션 도입

AS-IS

- ✓ 중요 자료 유출 방지를 위한 대책이 마련되어 있지 않음

TO-BE

- ✓ 보안 솔루션(DLP, 문서중앙화 등) 운영을 통한 내부 기밀자료 보호
- ✓ 화면캡쳐, 보조저장장치 사용 제한 등을 통한 내부 통제 시행

구분	2021년						2022년					
	7월	8월	9월	10월	11월	12월	1월	2월	3월	4월	5월	6월
보안솔루션 도입 검토				●	→							
보안솔루션 도입 및 운영					●	→						

2. 추진과제 세부사항

2.6 백업 및 복구절차 수립

주요 작업 및 추진 일정

세부내용	✓ 백업 대상, 주기, 방법, 절차 등이 포함된 백업 및 복구 관련 대책을 마련하여 이행하여야 함
주요 작업	<ol style="list-style-type: none"> 1. 백업 및 복구 절차 수립 2. 백업 공간(백업/복구 솔루션, NAS, 스토리지 등) 확보 3. 주기적인 백업 및 복구 훈련 시행
전제조건/제약사항	✓ 백업 공간(백업/복구 솔루션, NAS, 스토리지 등) 확보

AS-IS

- ✓ 업무 시 생성되는 중요 데이터에 대한 백업 대책이 마련되어 있지 않음

TO-BE

- ✓ 백업 및 복구 절차 수립
- ✓ 백업 환경 구축을 위한 솔루션 도입(백업/복구 솔루션, NAS, 스토리지 등)
- ✓ 중요 정보(자료)에 대한 주기적인 백업 및 복구 훈련 시행

구분	2021년						2022년					
	7월	8월	9월	10월	11월	12월	1월	2월	3월	4월	5월	6월
솔루션 도입 검토				●	→							
백업 정책 수립 및 시행						●	→					

2. 추진과제 세부사항

2.7 ICT 인프라 자산에 대한 보안 설정 강화

주요 작업 및 추진 일정

세부내용	✓ ICT 인프라 자산(서버, 네트워크, 공유기, 보안시스템, PC)의 발견된 취약점에 대한 개선 대책 적용을 해야 함
주요 작업	<ol style="list-style-type: none"> 1. 취약점 점검 시 발견된 취약점 파악 및 보호대책 가이드 확인 2. ICT 인프라 자산 별 관리자(담당자)를 통한 취약점 개선 조치
전제조건/제약사항	✓ ICT 인프라 자산 별 취약점 개선 조치 가능한 인력 체크

AS-IS

- ✓ 서버, 공유기, PC 등 ICT인프라 자산의 취약점 점검 시 다수의 미흡사항이 발견됨

TO-BE

- ✓ ICT 인프라 자산에 대한 연 1회 이상의 취약점 점검 실시
- ✓ 발견된 취약점에 대한 개선 조치 시행

구분	2021년						2022년					
	7월	8월	9월	10월	11월	12월	1월	2월	3월	4월	5월	6월
취약점 파악				● →								
취약점 개선 조치					● →							

3. 보안솔루션 추천

3.1 주요 보안대책에 따른 보안솔루션 추천

- 컨설팅 결과 주요 보안대책 중 업무용 단말기기 등을 통한 기밀자료 유출 방지 대책이 마련 되어있지 않아 데이터 유출 방지(DLP) 제품군의 보안솔루션 도입을 추천 드립니다.

도출된 주요 보안대책에 따른 솔루션 추천

주요 보안대책

- 업무용 단말기 보안관리 강화
- 내부 주요정보 유출 방지 방안 수립
- 주요 데이터에 대한 백업 및 복구절차 수립

주요 보안대책 중 기업의 중요 데이터(도면, 디자인 파일 등)를 개인 PC에 보관하고 PC의 공유폴더 기능을 이용해 파일을 공유하고 있어 적절한 권한 부여 등의 보안정책 관리가 이행되지 않아 데이터의 유출 및 체계적인 데이터 관리가 어려워 백업/복구 관리 시스템을 통한 체계적 정보 자산 관리가 필요합니다.

✓ 최약영역별 추천 보안솔루션

컨설팅 결과 최약영역	추천 카테고리
내부자료 유출 대응 미흡	DLP, DRM 등
외부 공격 대응 미흡	침입차단, UTM 등
백업, 복구 미흡	백업복구 등
악성파일 차단 미흡	유해차단, 악성파일차단 등
기타	보안USB 등

솔루션
매핑

추천 솔루션

단계	추천 보안시스템	비고
1단계		
2단계		
3단계	데이터 유출 방지(DLP)	1 순위 추천
4단계	백업/복구 관리시스템	2 순위 추천
기타		

☞ 단계별 상세 정보는 붙임#3 '보안솔루션' 참조

기때효과

데이터 유출 방지(DLP) 제품군 도입

종합컨설팅 결과 내부 기밀자료 유출 방지 대책의 부재로 내부 정보 유출 가능성이 존재하여 DLP 제품군을 1순위로 추천하며, 해당 솔루션 도입 시 외부 해킹 및 내부 인력으로 부터의 주요 정보 유출 차단 효과가 있을 것으로 판단됩니다.



Thank you

Keep IT simple.
We've got you covered.

S E E D G E N

(우)08377 서울특별시 구로구 디지털로33길 28 우림e-biz센터 1차 701호
Woolim eBIZ Center 701, 28, Digital-ro 33-gil, Guro-gu, Seoul, Republic of Korea

<http://www.seedgen.kr>

#

불임

1. 사업 개요
2. 진단항목
3. 보안솔루션

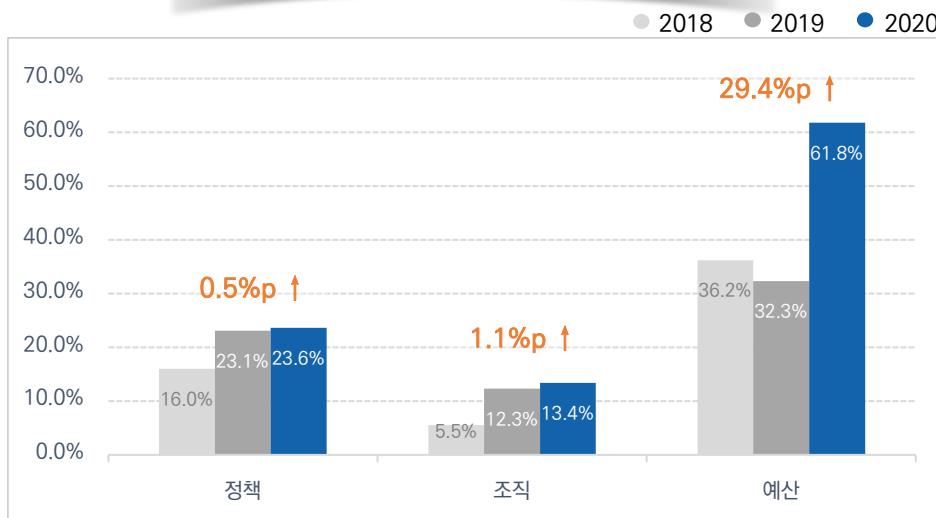
1. 사업 개요

1.1 배경 및 목적 [1/2]

- 중소기업은 정보보호를 위한 정책제정, 인력구성, 투자 여건 등이 부족하여 랜섬웨어 및 악성코드와 같은 피해가 매년 증가하고 있어 정보보호 강화를 위한 기업의 인식제고 및 투자가 필요한 상황입니다.

정보보호 환경과 침해사고 사례로 바라본 중소기업

3無로 인한 취약한 정보보호

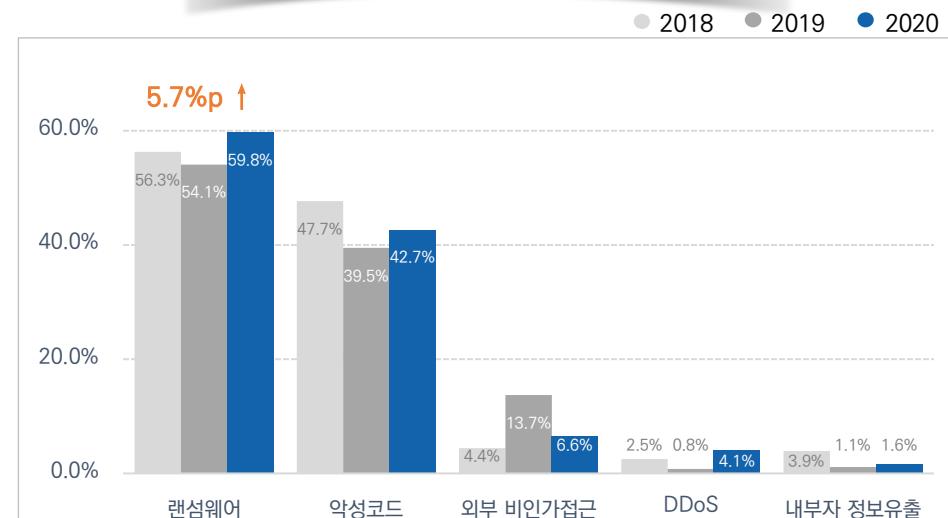


※ 출처 : 과기정통부 '2020년 정보보호 실태조사 보고서'

정책, 조직, 예산 등에 대한 투자 미흡

- 정보보호 정책, 조직을 보유한 기업은 각 **23.6%, 13.4%**로 매우 낮음
- 정보보호 예산(61.8%) 비중이 IT예산 중 **1% 미만인 기업은 49.4%**로 나타남

랜섬웨어, 악성코드 등의 보안 위협 노출



※ 출처 : 과기정통부 '2020년 정보보호 실태조사 보고서'

주요 보안 위협에 노출

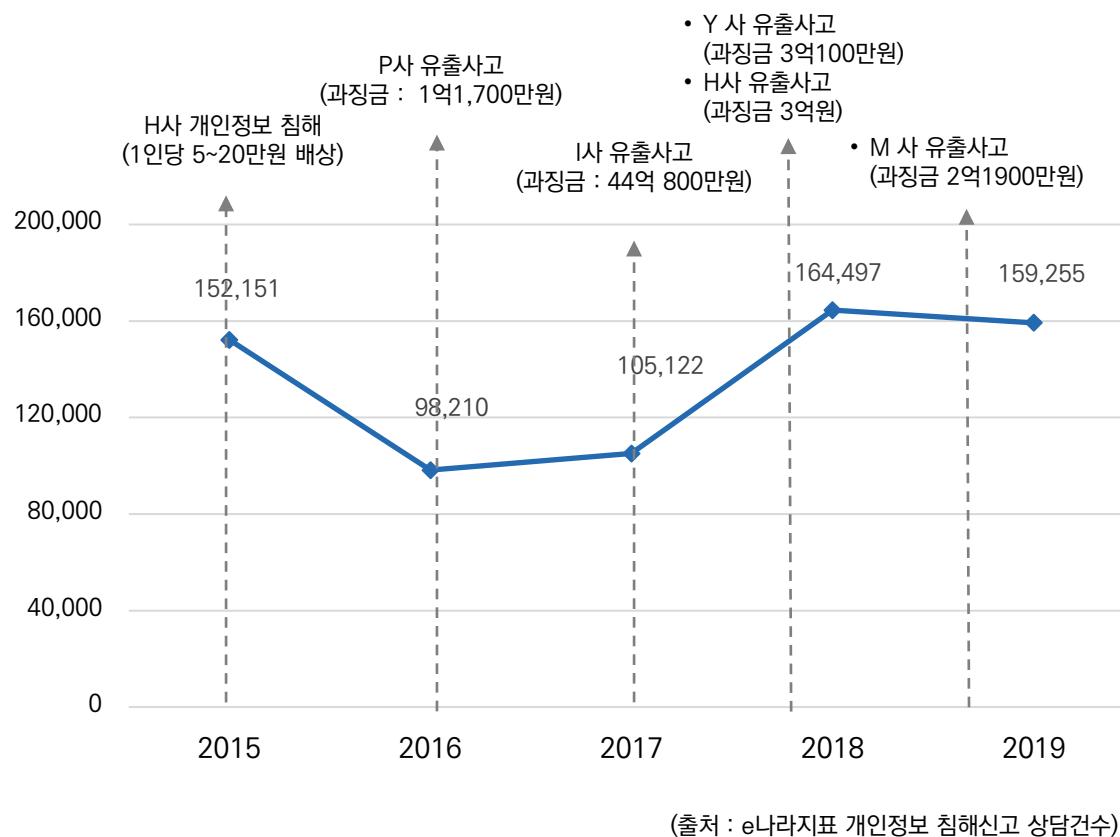
- 랜섬웨어 피해 비중이 가장 높음(**59.8%**)
- 전년도 대비 랜섬웨어의 피해사례는 **5.7%**가 상승

1. 사업 개요

1.1 배경 및 목적 [2/2]

- 지난 5년간 국내에서 지속적인 개인정보 유출 및 침해사고가 발생하고 있으며, 이에 따른 정부의 과징금 처벌 규정도 강화되고 있어 중소기업의 저조한 인식 수준을 높이고 선제적인 대응방안을 갖춰야합니다.

최근 5년 개인정보 침해 현황



(단위: 침해신고 상담건수)

구분	2015	2016	2017	2018	2019
개인정보 무단수집	2,442	2,568	1,876	2,764	3,237
개인정보 무단 이용 제공	3,585	3,141	3,881	6,457	6,055
주민번호 등 타인정보 도용	77,598	48,557	63,189	111,483	134,271
회원탈퇴 또는 정정 요구 불응	957	855	862	1,149	1,292
법 적용 불가 침해사례	60,480	38,239	30,972	37,156	8,745
기타	7,089	4,850	4,342	5,488	5,655
합계	152,151	98,210	105,122	164,497	159,255

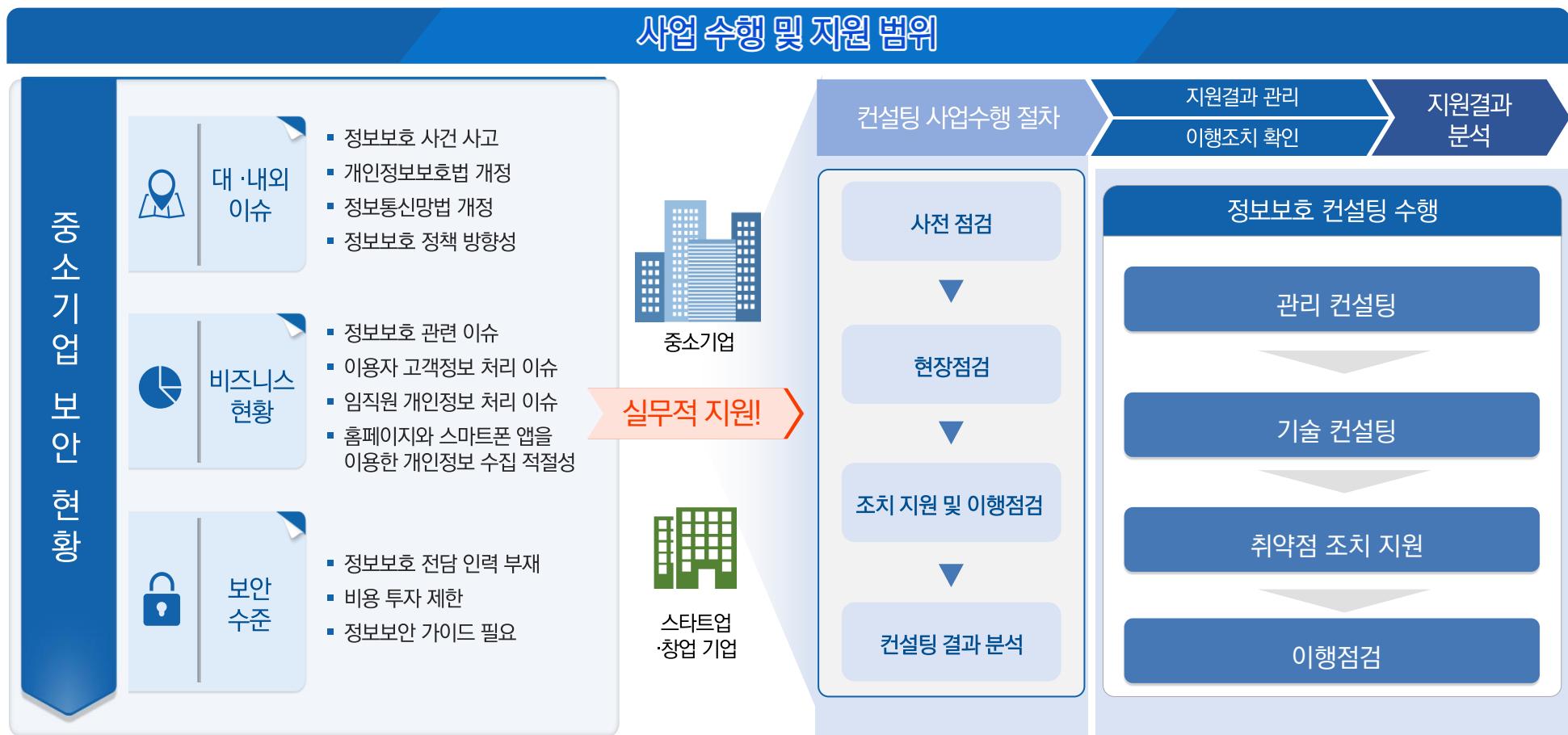
정보 유출 사고와 침해신고 현황

- 대규모 유출사고 지속 발생에 따른 과징금 강화 추세
- 소비자의 경우 유출사고 또는 침해사고 발생 시 상담보다 소송이라는 적극적 행동으로 이어짐
- 인식 수준이 다소 낮은 중소기업 대상 선제적 대응 필요

1. 사업 개요

1.2 사업 범위

- 정보보호 수준 향상을 위하여 중소기업과 관련한 대내·외 주요 이슈를 반영한 정책·지침 수립과 기술적·관리적 취약점 진단을 통해 위험분석·평가를 수행하여 현재의 위험을 낮추고, 자율적이고 자발적인 정보보호 수준관리를 위한 솔루션 선택을 가이드 합니다.



1. 사업 개요

1.3 수행 단계

- 컨설팅 수행은 사전 준비, 업종·규모별 현장 컨설팅 수행, 이행 조치 지원 단계로 진행되며 각 영역별 기업의 미흡 사항을 도출하여 개선 방안 제공 후 보완조치 및 이행 확인을 수행합니다.

수행 절차 세부 사항



1. 사업 개요

1.4 수행 절차 [1/4]

- 관리컨설팅 수행 절차는 관리체계 및 개인정보보호 영역으로 구분하여 진행하며 범위설정 후 이슈를 도출하여 개선방안을 가이드하고 교정 지원합니다.

관리체계 및 개인정보보호 영역

업무 기준 범위 설정

컨설팅 결과에 따른 이슈 도출

이슈 대응 및 개선 방안

적용 범위

인터뷰 및 현장실사

개선 대책 수립

관리 체계

- 기업 핵심 업무 프로세스를 관리, 물리, 기술영역으로 구분
- 내부 조직, 인력, 자산 운영, 출입 통제 등 대상 선정자산 식별

- 사전 개발 방법론 점검 항목 기준 업무 담당자별 인터뷰 진행
- 영역별 전문가 수행으로 기업의 관리 물리 영역 현황 파악

- 관리·물리 영역 개선 제언
- 방법론 점검 항목 기준 개선을 위한 문서 Templet 제공
- 방법론 항목 외 추가 이슈 대응

개인정보 보호

개인 정보보호 조직 구성, 자원(인력·비용) 관리 현황



개인 정보보호 정책 수립, 보안 프로세스 관리



생명주기 → 보호조치 → 침해대책

- 개인정보 수집 이용저장 파기의 흐름에 따른 분석
- 개인정보보호를 위한 기술적, 관리적, 물리적 보호조치 현황
- 개인정보 유출 등 침해사고 발생 시 대응 방안

개선 대책 수립

- 개인정보처리방침 개정 지원
- 개인정보관리계획 수립 지원
- 개인정보 수집 동의 서식 개편
- 위·수탁 및 제3자제공에 대한 가이드 제공

※ 상세 점검 항목은 붙임# '진단항목' 참조

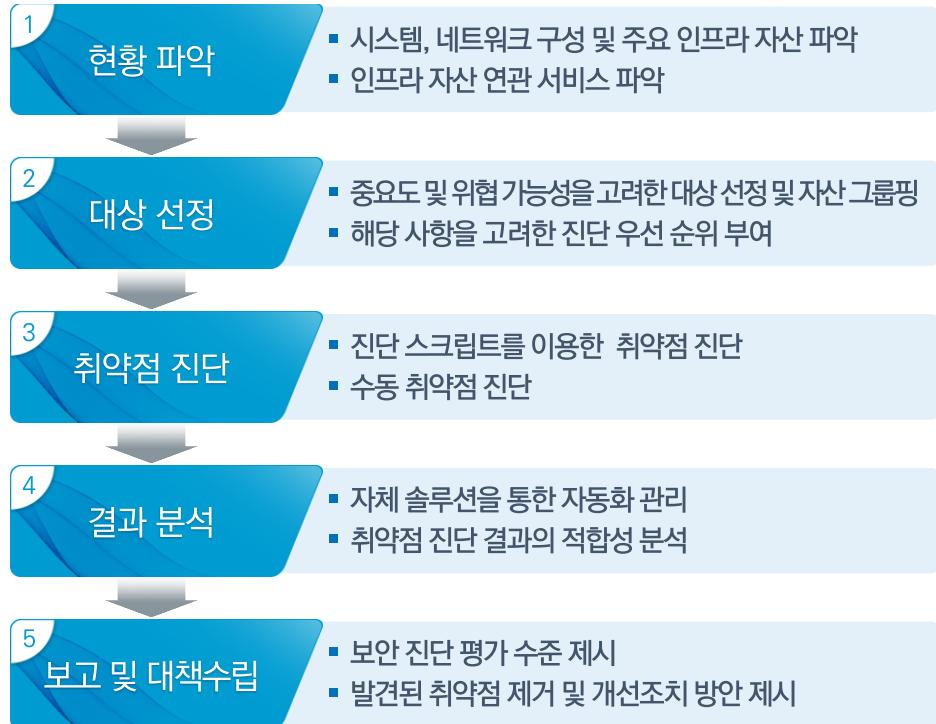
1. 사업 개요

1.4 수행 절차 [2/4]

- 기술컨설팅 수행 절차는 인프라 진단 및 웹 어플리케이션 취약점 진단 영역으로 구분하여 진행하며 현황 파악 후 진단을 통해 이슈를 도출하여 대책수립을 제시합니다.

인프라 진단 및 웹 어플리케이션 취약점 진단 영역

인프라 진단 절차



웹 어플리케이션 취약점 진단 절차



※ 상세 점검 항목은 불임# '진단항목' 참조

1. 사업 개요

1.4 수행 절차 [3/4]

- 발견된 문제점에 대한 상세 보완 가이드를 제공하여 현업 담당자들이 정확히 조치할 수 있도록 지원하며 추가 이슈 발생 시, 해당 업체에 대한 지속적인 관리를 수행합니다.

취약점 조치 지원

취약점 조치 지원방안

- 발견된 문제점을 개선하기 위한 가이드와 기업의 보안활동에 도움이 되는 자료(양식, 템플릿 등) 제공
- 제공된 조치 가이드 내용이 해당 업체의 현황에 맞지 않는 경우 해당 업체 현황에 부합하는 대체 방안 제시
- 컨설팅 종료 후 개선 사항에 대한 지속적인 관리를 수행하여 개선 조치 지원

◆ 수혜사 요청 사항

가이드라인 설명 요구

- 조치 관련 담당자가 가이드 및 개선 사항에 대한 내용을 이해하지 못하여 추가 설명 및 수정을 요구하는 경우

가이드라인 적용 불가

- 중소기업의 특성 및 현황상 가이드 내용 적용에 제한이 있어 조치가 불가능한 경우

추가 이슈 대응

- 컨설팅 범위 외 추가 이슈에 대한 문의
- 컨설팅 종료 후 보안 관련 추가 이슈에 대한 문의

◆ 수행사 조치 지원 방안

가이드 추가 상세 설명 제공

- ✓ 가이드 및 개선 사항을 조치 담당자 요구사항에 맞춰 이해할 수 있도록 업데이트하여 제공



기업 현황에 맞는 대안 제시

- ✓ 해당 문제점에 대한 대체 조치 방안 검토 및 제공



원격 시스템 및 메일을 통한 관리

- ✓ 지원이 가능한 범위 내에서 최대한 지원
- ✓ 컨설팅 종료 후 메일 및 유선을 통하여 보안 이슈에 대해 지속적인 관리 수행



1. 사업 개요

1.4 수행 절차 [4/4]

- 발견된 모든 취약점의 이행조치가 완료될 수 있도록 발견된 취약점에 대한 조치를 지원하며 절차에 따라 일정 협의 후 이행점검을 진행합니다.



2. 진단항목

2.1 관리체계 및 개인정보보호 영역

No	관리체계 진단항목	항목 수
1	정보보호 관리체계	관리체계 기반 마련 및 운영
		위험관리
		관리체계 점검 및 개선
2	인원보안	인적 보안
		외부자 보안
3	시설보안	물리보안
		업무환경 보안
4	IT보안관리	인증 및 권한관리
		접근통제
		시스템 보안관리 및 암호화
		업무용 단말기기/보조저장매체관리
		악성코드 및 패치관리
		정보시스템 개발보안
5	보안사고관리	침해사고 예방 및 대응체계 구축
		재해복구
6	개인정보관리	개인정보보호 관리체계 운영
		개인정보의 기술적 보호조치
		개인정보 처리 시 보호조치
		정보주체 권리보호
총계		64

No	개인정보 처리방침 진단항목	항목 수
1	개인정보 처리방침 수립 및 공개 여부	1
2	개인정보의 처리 목적	1
3	개인정보의 처리 및 보유 기간	3
4	개인정보의 제3자 제공에 관한 사항	2
5	개인정보처리의 위탁에 관한 사항	3
6	정보주체와 법정대리인의 권리. 의무 및 행사방법	2
7	처리하는 개인정보 항목	3
8	개인정보 파기애에 관한 사항	3
9	개인정보의 안전성 확보조치에 관한 사항	1
10	개인정보 자동 수집 장치의 설치. 운영 및 그 거부에 관한 사항	3
11	개인정보 보호책임자에 관한 사항	2
12	개인정보처리방침 변경에 관한 사항	1
13	개인정보 열람청구를 접수. 처리하는 부서	1
14	권익침해 구제방법	1
총계		27

2. 진단항목

2.2 인프라 진단 및 웹 어플리케이션 취약점 진단 영역 [1/2]

Unix/Linux 서버 진단 체크리스트

영역	항목
1. 계정관리	root 계정 원격 접속 제한 패스워드 복잡성 설정 패스워드 파일 보호 root 이외의 UID '0' 금지 패스워드 최소 길이 설정 불필요한 계정 제거 관리자 그룹에 최소한의 계정 포함 Session Timeout 설정
	root 훔, 패스 디렉터리 권한 및 패스 설정 /etc/passwd 파일 소유자 및 권한 설정 /etc/shadow 파일 소유자 및 권한 설정 /etc/hosts 파일 소유자 및 권한 설정 /etc/syslog.conf 파일 소유자 및 권한 설정 /etc/services 파일 소유자 및 권한 설정 접속 IP 및 포트 제한 UMASK 설정 관리
	finger 서비스 비활성화 Anonymous FTP 비활성화 r 계열 서비스 비활성화 cron 파일 소유자 및 권한 설정 NFS 서비스 비활성화 NFS 접근 통제 automountd 제거 RPC 서비스 확인 tftp, talk 서비스 비활성화 ssh 원격접속 허용 ftpusers 파일 설정 SNMP 서비스 구동 점검 SNMP 서비스 커뮤니티스트링의 복잡성 설정 FTP 서비스 확인 Ftpusers 파일 소유자 및 권한 설정 로그온 시 경고 메시지 제공
	최신 보안패치 및 벤더 권고사항 적용
	정책에 따른 시스템 로깅 설정
4. 패치관리	
5. 로그관리	

Windows 서버 진단 체크리스트

영역	항목
1. 계정관리	Administrator 계정 이름 바꾸기 Guest 계정 상태 불필요한 계정 제거 해독 가능한 암호화를 사용하여 암호 저장 해제 관리자 그룹에 최소한의 사용자 포함 Everyone 사용 권한을 익명 사용자에게 적용 해제 패스워드 복잡성 설정 패스워드 최소 암호 길이 마지막 사용자 이름 표시 안함 로컬 로그온 허용
	공유 권한 및 사용자 그룹 설정 하드디스크 기본 공유 제거 불필요한 서비스 제거 NetBIOS 바인딩 서비스 구동 점검
	FTP 서비스 구동 점검 FTP 디렉토리 접근권한 설정 최신 서비스팩 적용 SNMP 서비스 구동 점검 SNMP 서비스 커뮤니티스트링의 복잡성 설정 원격터미널 접속 타임아웃 설정
	최신 HOT FIX 적용 백신 프로그램 업데이트 정책에 따른 시스템 로깅 설정
	원격으로 액세스 할 수 있는 레지스트리 경로 이벤트 로그 관리 설정
	백신 프로그램 설치 화면보호기 설정 로그온하지 않고 시스템 종료 허용 해제 원격 시스템에서 강제로 시스템 종료 Autologon 기능 제어 이동식 미디어 포맷 및 꺼내기 허용
	사용자가 프린터 드라이버를 설치할 수 없게 함 경고 메시지 설정
5. 보안관리	

네트워크 장비 진단 체크리스트

영역	항목
1. 계정관리	패스워드 설정 암호화된 패스워드 사용 VTY 접근(ACL) 설정 Session Timeout 설정 VTY 접속 시 안전한 프로토콜 사용 로그온 시 경고 메시지 설정
	최신 보안 패치 및 벤더 권고사항 적용
	로깅 버퍼 크기 설정 정책에 따른 로깅 설정
	NTP 서버 연동 원격 로그서버 사용 timestamp 로그 설정
	SNMP 서비스 확인 SNMP community string 복잡성 설정 SNMP ACL 설정 SNMP 커뮤니티 권한 설정 Spoofing 방지 필터링 적용 또는 보안장비 사용 DDoS 공격 방어 설정 또는 DDoS 장비 사용
	TCP keepalive 서비스 설정 Finger 서비스 차단 웹 서비스 차단 TCP/UDP small 서비스 차단 CDP 서비스 차단 Directed-broadcast 차단 Source 라우팅 차단 Proxy ARP 차단 ICMP unreachable, Redirect 차단 identd 서비스 차단 pad 차단 mask-reply 차단
4. 로그관리	
5. 기능관리	

2. 진단항목

2.2 인프라 진단 및 웹 어플리케이션 취약점 진단 영역 [2/2]

보안시스템 진단 체크리스트

영역	항목
1. 계정관리	보안시스템 Default 계정 정보 변경
	보안시스템 계정 관리
2. 접근관리	보안시스템 원격 관리 접근 통제
	보안시스템 보안 접속
	Session timeout 설정
3. 패치관리	벤더에서 제공하는 최신 업데이트 적용
4. 로그관리	보안장비 로그 설정
	보안장비 로그 보관
	보안장비 정책 백업 설정
	원격 로그 서버 사용
5. 기능관리	NTP 서버 연동
	정책 관리
	NAT 설정
	DMZ 설정
	이상징후 탐지 모니터링 설정
	장비 사용량 검토
	SNMP 서비스 확인
	SNMP community string 복잡성 설정

Windows PC 진단 체크리스트

영역	항목
1. 계정관리	패스워드 정책이 해당 기관의 보안 정책에 적합하게 설정
2. 서비스관리	공유 폴더 제거 항목의 불필요한 서비스 제거
3. 패치관리	HOT FIX 등 최신 보안패치 적용 최신 서비스팩 적용
4. 보안관리	바이러스 백신 프로그램 설치 및 주기적 업데이트 바이러스 백신 프로그램에서 제공하는 실시간 감시기능 활성화 OS에서 제공하는 침입차단 기능 활성화 화면보호기 대기 시간 설정 및 재시작 시 암호 보호 설정 CD, DVD, USB 메모리 등과 같은 미디어의 자동실행 방지 등 이동식 미디어에 대한 보안대책 수립

공유기 진단 체크리스트

영역	항목
1. 계정관리	관리자 계정 초기 설정값 변경 패스워드 복잡성 설정
2. 접근관리	무선 AP 접근 암호 변경 인증 및 암호화 방식 설정 SSID 변경
3. 기능관리	SSID 숨김 기능 설정 MAC 필터링 사용 WPS 비활성화
4. 로그관리	최신 펌웨어 업데이트 실행 로그 기능 실행

웹 어플리케이션 취약점 진단 체크리스트

영역	항목
1. 입력 값 검증 부재	SQL 인젝션 SSI 인젝션 XPath 인젝션 LDAP 인젝션 버퍼 오버플로우 포맷스트링 운영체제 명령 실행 크로스사이트 스크립팅 크로스사이트 리퀘스트 변조
2. 취약한 파일처리	파일 업로드 파일 다운로드 악성콘텐츠 자동화 공격 프로세스검증 누락 관리자페이지 노출 위치 공개
3. 취약한 접근통제	불충분한 인증 불충분한 인가 세션 예측 세션 고정 불충분한 세션 만료 취약한 패스워드 복구
4. 취약한 인증 및 세션관리	쿠키 변조 데이터평문 전송 디렉터리 인젝싱 정보 누출 약한문자열 강도 경로 추적
5. 잘못된 보안설정	

3. 보안솔루션

3.1 단계별 보안솔루션 메뉴판 구성

- 솔루션 1단계와 2단계는 레이어 단계로 기본적인 보안솔루션에 해당하며, 3단계인 정보유출방지 보안, 4단계인 암호·인증 보안 단계를 통해 기업보안의 고도화를 구축해 나갈 수 있습니다.

보안솔루션 메뉴판 및 주요기능



단계	솔루션 주요기능
1단계	미 승인 사용자의 네트워크 접근 차단 및 방지
2단계	파일이나 폴더, 시스템 등에 미 승인 사용자의 접근 차단 및 방지
3단계	데이터나 기밀정보 등에 대한 유출 차단 및 방지
4단계	암호/인증을 통해 데이터와 사용자 정보를 안전하게 관리 발생할 수 있는 각종 보안 위협 감소
기타	향상된 보안을 위해 필요한 기술

3. 보안솔루션

3.2 보안솔루션 분류

분류	No	솔루션 유형	설명
네트워크 보안	1	웹방화벽	네트워크 방화벽과 달리 OWASP(Open Web Application Security Project) Top10, 국가정보원의 8대 웹 취약점, 웹페이지 위·변조 등 다양한 형태의 웹 기반 해킹 및 유해 트래픽을 실시간 감시하여 탐지하고 차단하는 웹 애플리케이션 보안 솔루션
	2	방화벽 (네트워크 방화벽, UTM, NGFW 등 포함)	시스템의 보안을 위해 네트워크 상에서 외부에서 내부로, 내부에서 외부로의 불법적인 접근은 차단하는 보안 솔루션
	3	침입방지시스템(IPS)/DDoS 차단 시스템	IPS는 네트워크 패킷을 분석하여 공격 시그니처(Signature)를 찾아내 제어함으로써 비정상적인 트래픽을 중단시키는 보안 솔루션으로, 수동적인 방어 개념의 방화벽이나 침입탐지시스템(IDS)과 달리 침입 경고 이전에 공격을 중단시키는 능력을 개념의 솔루션. 해당 서버의 비정상적인 행동에 따른 정보 유출을 자동으로 탐지하여 차단 조치를 취함으로써 인가자의 비정상 행위를 통제 가능
	4	가상사설망(VPN)	DDoS 차단 시스템은 대량의 트래픽을 전송해 시스템을 마비시키는 DDoS(Distributed Denial of Service, 분산서비스거부) 공격 전용의 차단 솔루션으로, 대량으로 유입되는 트래픽을 신속하게 분석해 유해트래픽 여부를 판단해 걸려 줌으로써 보호대상 네트워크의 가용성과 안정성을 높여주며, 해당 서비스의 연속성을 보장하는 데 중요한 역할을 함
	5	네트워크 접근제어(NAC)	인터넷망 또는 공중망을 사용하여 둘 이상의 네트워크를 안전하게 연결하기 위하여 가상의 터널을 만들어 암호화된 데이터를 전송할 수 있도록 만든 네트워크로 공중망 상에서 구축되는 논리적인 전용망
	6	무선 네트워크 보안	네트워크에 접근하는 접속단말의 보안성을 강제화할 수 있는 보안 인프라로, 허가되지 않거나 웜·바이러스 등 악성코드에 감염된 PC 또는 노트북, 모바일 단말기 등이 회사 네트워크에 접속되는 것을 원천적으로 차단해 시스템 전체를 보호하는 보안 솔루션
시스템(단말) 보안	7	악성코드/랜섬웨어 대응	바이러스(virus), 웜(worm), 트로이목마(trojan horse), 스파이웨어(spyware)와 같은 독립적인 실행파일(악성코드)이나 스크립트, 컨텐츠 등 다양한 형태로 제작되는 멀웨어를 통해 발생할 수 있는 위협으로부터 시스템을 보호하기 위한 백신을 포함하는 보안솔루션과 사용자 PC의 자료를 인질로 몸값을 요구하는 악성코드인 랜섬웨어(ransomware)로부터 데이터를 보호하고 복구하는 기능이 포함된 보안솔루션
	8	스팸차단 솔루션(이메일 보안)	스팸전송자로 알려진 특정 이메일주소, 메일서버IP, URL, 제목과 내용, 대량전송 여부 등을 통해 스팸내용 및 불건전사이트 등을 검사하고 인식하여 차단하는 보안 솔루션
	9	지능형 지속공격(APT) 대응	APT공격에 대응하기 위한 보안 시스템. APT대응 솔루션은 PC에이전트, 서버 소프트웨어, 어플라이언스 또는 그 조합으로 운영(APT : 의도가 분명한 악의적인 경제적 또는 정치적인 동기를 가지고 있고, 특정 기업이나 국가, 공공을 타겟으로 실행되는 은밀하고 지속적인 컴퓨터 공격 행위를 의미)
	10	엔드포인트 탐지 및 대응(EDR)	패턴화돼 이미 알려져 있는 악성코드를 잡아내는 백신과 달리 신종 악성코드나 기존 바이러스가 변종돼 백신이 잡아낼 수 없는 악성코드까지 인지하고 이를 차단하는 보안 솔루션. 기존 백신이 A위협, B위협을 각각 모니터링한다면, EDR은 통합적으로 이를 탐지하고 관리할 수 있는 역할까지 하게 돼 보안 사각지대를 줄일 수 있다는 장점이 있음
정보유출 방지	11	DB보안/DB암호	DB보안(접근통제)은 데이터베이스 및 데이터베이스 내에 저장된 데이터를 인가되지 않은 변경, 파괴, 노출 및 비밀관성을 발생시키는 사건으로부터 보호하는 보안 솔루션. DB암호는 데이터의 실제 내용을 허가받지 않은 사람이 볼 수 있도록 은폐하기 위해 데이터를 암호화하는 보안 솔루션
	12	보안USB	사용자식별, 지정데이터 암·복호화, 지정된 자료의 임의복제 방지, 분실 시 데이터 보호를 위한 삭제 등의 기능을 지원하는 보안 컨트롤러가 있는 휴대용 메모리 스틱으로 보안 컨트롤러는 H/W, S/W로 구성될 수 있음
	13	디지털저작권관리(DRM)	웹을 통해 유통되는 각종 디지털 콘텐츠의 안전 분배와 불법 복제 방지를 위한 보안 솔루션. 파일 교환 프로그램을 통해 전파되는 상업적 자료의 온라인 불법 복제로부터 디지털 콘텐츠를 보호하기 위한 것으로, 관련 법령이나 위반자 단속만으로는 예방이 어렵기 때문에 사후 단속 보다는 사전에 문제점을 파악해 첫 단계에서 내용 복제가 불가하도록 함
	14	데이터 유출 방지(DLP) (네트워크 DLP, 단말 DLP 등)	네트워크 DLP는 사용자의 고의 또는 실수, 외부 해킹, 멀웨어 등을 통해 네트워크를 이용한 정보유출을 컨텐츠 수준에서 차단. 단말 DLP는 사용자의 고의 또는 실수, 외부 해킹, 멀웨어 등을 통해 단말 호스트(PC, 서버, 모바일 등)에서의 정보유출을 차단. 각종 외부 인터페이스(USB, 외장하드, CD/DVD, 프린트, 블루투스 등)를 통해 유출되는 정보의 내용을 감시하고, 필요에 따라 차단
암호/인증	15	공개키기반구조(PKI)/차세대 인증(FIDO, DID, IDoT 등)	실체의 식별자와 공개키를 포함하는 정보로서 공개키 정보는 한 실체에 대한 데이터와 이 실체를 위한 공개키로 제한되며, 인증기관, 실제, 공개키 또는 관련된 알고리즘에 관한 다른 정적인 정보일 수 있음. 공개키 암호 기반기술의 집합체로써, 보안 서비스에서 핵심적으로 필요한 비밀성, 무결성, 인증, 부인방지 기능 및 접근제어 기능을 제공하는 Application 계층의 데이터 보안 기술
보안관리	16	취약점 분석 시스템	악성코드 민감도, 안전하지 않은 소프트웨어 설정, 열린 포트 등 컴퓨터 시스템의 알려진 취약점들을 분석하기 위해 사용되는 솔루션
보안관리	17	백업/복구 관리 시스템	자료 손실을 예방하기 위해 자료를 미리 다른 곳에 임시로 보관해 두었다가 원래 상태로 복구해주는 관리 솔루션
기타	18		기타