

---

---

# 주식회사 솔라스트

## 정보 보안 대책 기준

### 목차

1장 소개.....	6
1.1 배경 .....	6
1.2 본서의 위치설정.....	6
1.3 본 설명서의 기재 방법 .....	6
1.4 용어의 정의.....	6
2장 조직적 관리 방법.....	8
2.1 정보 보안을 위한 정책군.....	8
2.2 정보 보안의 역할 및 책임 .....	8
2.3 직무의 분리.....	9
2.4 관리층의 책임 .....	9
2.5 관계 당국과의 연락 .....	10
2.6 전문 조직과의 연락 .....	10
2.7 위협 인텔리전스 .....	11
2.8 프로젝트 관리의 정보 보안 .....	11
2.9 정보 및 기타 관련 자산 목록 .....	11
2.10 정보 및 기타 관련 자산의 허용 이용	
2.11 자산 반환 .....	12
2.12 정보 분류 .....	13
2.13 정보의 라벨 첨부.....	13
2.14 정보 전송.....	14
2.15 액세스 제어 .....	15

---

2.16 식별 정보 관리 .....	16
2.17 인증 정보.....	16
2.18 액세스권 .....	17
2.19 조달 제품 서비스 및 위탁처의 정보 보안 대책의 평가와 관리	
2.20 정보 보안 요구 사항에 따른 외부 위탁 계약 .....	18
2.21 제품 서비스의 선정이나 조달에 있어서의 정보 보안의 관리.....	18
2.22 조달 제품 서비스 및 위탁처 서비스의 감시, 리뷰 및 변경 관리.....	19
2.23 클라우드 서비스 이용에 있어서의 정보 보안 .....	19
2.24 정보 보안 인시던트 관리 계획 수립 및 준비 .....	20
2.25 정보보안사건의 평가 및 결정.....	21
2.26 정보 보안 사고에 대한 대응 .....	22
2.27 정보보안 인시던트로부터의 학습.....	22
2.28 증거 수집	
2.29 사업의 중단·재해시의 정보 보안.....	22
2.30 사업 계속을 위한 ICT의 준비.....	23
2.31 법령, 규제 및 계약상의 요구사항.....	23
2.32 지적재산권 .....	23
2.33 기록 보호 .....	23
2.34 프라이버시 및 개인을 식별할 수 있는 정보(PII)의 보호	
2.35 정보 보안의 독립적인 검토 .....	23
2.36 정보보안을 위한 정책군, 규칙 및 표준의 준수 .....	24
2.37 조작 순서서 .....	24
3장 인적 관리책.....	25
3.1 전형 .....	25
3.2 고용 조건 .....	25
3.3 정보 보안 의식 향상, 교육 및 훈련 .....	25
3.4 징계 절차.....	26

---

---

3.5 고용의 종료 또는 변경 후의 책임.....	26
3.6 비밀유지계약 또는 수비의무계약	26
3.7 리모트 워크.....	26
3.8 정보 보안 사건 보고.....	27
4장 물리적 관리 방법.....	28
4.1 물리적 보안 경계.....	28
4.2 물리적 입퇴.....	29
4.3 사무실, 방 및 시설의 보안 .....	30
4.4 물리적 보안 모니터링 .....	30
4.5 물리적 및 환경적 위협으로부터의 보호 .....	30
4.6 보안을 유지해야 하는 영역에서의 작업 .....	30
4.7 클리어 데스크 클리어 스크린.....	31
4.8 장비 설치 및 보호 .....	31
4.9 구외에 있는 자산의 보안.....	31
4.10 저장 매체.....	32
4.11 자원 유틸리티 .....	32
4.12 케이블 배선의 보안.....	33
4.13 장치의 유지보수 .....	33
4.14 장치의 보안을 유지한 처분 또는 재사용.....	33
5장 기술적 관리방법.....	34
5.1 사용자 단말기.....	34
5.2 특권 액세스 권한 .....	35
5.3 정보에 대한 액세스 제한 .....	35
5.4 소스 코드 액세스 .....	35
5.5 보안을 유지한 인증.....	35
5.6 용량·능력 관리.....	36
5.7 맬웨어에 대한 보호.....	36

---

---

5.8 기술적 취약성 관리.....	37
5.9 구성 관리 .....	37
5.10 정보 삭제 .....	37
5.11 데이터 마스킹.....	37
5.12 데이터 누출 방지 .....	37
5.13 정보 백업 .....	37
5.14 정보처리시설·설비의 중복성.....	38
5.15 로그 취득.....	38
5.16 감시 활동.....	39
5.17 클럭 동기화 .....	39
5.18 특권적인 유틸리티 프로그램의 사용.....	39
5.19 운영 시스템에 소프트웨어 도입 .....	39
5.20 네트워크 보안 .....	39
5.21 네트워크 서비스 보안.....	39
5.22 네트워크 액세스 제어 .....	40
5.23 웹 필터링 .....	40
5.24 암호 사용 .....	40
5.25 보안을 고려한 개발 라이프사이클.....	40
5.26 애플리케이션 보안 요구 사항 .....	41
5.27 보안을 고려한 시스템 아키텍처 및 시스템 구축 원칙 .....	42
5.28 보안을 고려한 코딩 .....	42
5.29 개발 및 수용에 대한 보안 테스트 .....	42
5.30 외부 위탁에 의한 개발 .....	42
5.31 개발 환경, 테스트 환경 및 프로덕션 환경의 분리	
5.32 변경 관리.....	43
5.33 테스트용 정보.....	43
5.34 감사시 테스트 중 정보시스템 보호.....	43

---

【 개판 이력 】

판수	발행일	개정자	개정 내용·이유	개소
1.0.0	2024/4/1		초판	

1	소개	발행일	2024.04.01
적용 범위	전사·전 직원		

1장 소개

1.1 배경

본서는 주식회사 솔라스트의 정보보안경영시스템을 운용하기 위해 기술한 문서(이하 「본서」라고 적는다)이다.

또한, 의료 업무 (의료 정보를 취급하는 경우)는 본 문서에 기재된 대책 이외에 후생 노동성이 책정하는 「의료 정보 시스템 안전관리에 관한 가이드라인」의 최신판의 대책에 대응한다.

1.2 본서의 위치설정

이 문서는 문서 시스템의 상위 규정의 정보 보안 규정 (관리 측면)의 하위 문서에 해당합니다.

1.3 본서의 기재 방법

본서는 당사의 정보보안규정(관리측면)에서 정의되는 「조직적 관리책」 「인적관리책」 「물리적 관리책」 「기술적 관리책」의 순서로 기재하고, 각 관리책의 구체적인 대응 방법을 나타낸 것이다.

덧붙여 본서내에서 등장하는 【중요도 :고】가 기재된 대책은, 중요도 「고」를 취급하는 경우는 필수로 해, 그 이외의 경우는 임의로 한다.

1.4 용어의 정의

이 용어는 인용 된 표준의 용어를 따르지만 다음 정의를 추가합니다.

No.	용어	용어의 의미
1	ISMS	정보 보안 경영 시스템 (InformationSecurityManagementSystem) 약어.
2	정보 보안 인시던트	원하지 않거나 예기치 않은 단독 또는 일련의 정보 보안 사건으로 사업 운영을 위태롭게 할 확률과 정보 보안을 위협할 확률이 높은 것 [ISO/IECTR18044:2004]
3	위험	조직 활동의 목적으로부터 바람직하지 않은 방향※에 괴리할 가능성이 있는 것(※ :정의상 는 보다 바람직한 방향으로 괴리할 가능성도 포함한다) 실제로 조직의 목표 수행을 방해하는 이벤트 발생 가능성과 이벤트 발생시 피 손실 등으로 표현
4	정보 자산	조직에 가치가 있고 적절한 보호 (보안 조치)가 필요한 정보 및 시스템, 조직 구성원 등

5 위협	정보 보안 사고를 일으키는 직접적인 원인이 될 수 있는 것
6 취약성	정보 자산에 위협이 가해지면 정보 보안 사고가 발생하기 쉽습니다. 그렇다고 생각되는 약점
7 CISO	정보보안 총책임자(CISO), 보통 대표이사가 담당 CISO : ChiefInformationSecurityOfficer의 약자.
8 교육	각종 교육 · 훈련 · 사내외의 세미나 · 방재 훈련 · 기타
9 요원	조직의 지시에 따라 일하는 사람들
10 직원	직원, 촉탁, 파트, 아르바이트 등 회사와 직접 고용의 관계에있는 회사 업무 종사자의 총칭
11 직원	(각사의 정의로 한다)
12 계약 직원 13	(각사의 정의로 한다)
파견 직원	직원 이외의 회사 외부에서 파견되어 회사 업무에 종사하는 사람의 총칭
14 협력사 직원 직원 이외에	회사의 업무의 일부 또는 전부 종사하고 그 수행을 지원하는 회사 직원 의 총칭
15 공급자	자사의 정보 보안 경영 시스템에 서비스를 제공하는 모임 회사 및 위탁처의 총칭
16 공급망 N	공급자로부터의 위탁처(재위탁처)나 ICT 기기 부품의 조달처의 총칭
17 고객(제2자) 회사의 업무	서비스·상품 등을 제공하는 법인 또는 개인의 총칭
18 자산	조직에 가치가 있는 것. 회사가 지켜야 할 인적 자산, 물리적 자산, NW · 정보 시스템 자산, 정보 자산 모두
19 사용자 엔드포 인트 장비	네트워크에 연결된 종단 장비의 총칭 각종 서버 외에 사내에서 이용하는 PC류나 프린터, 사외에서 이용하는 휴대전 이야기, 스마트 폰, 태블릿 등이 해당
20 MDM 서비스 MDM은 (M	obile Device Management)의 약자입니다. 조직과 기업이 직원의 모바일 장치를 원격으로 관리하고 보안 정책 및 애플리케이션 배포, 데이터 보호, 디바이스 추적 등을 수행할 수 있습니다. 서비스
21 저장 매체	HD·FD·MO·CD·DVD, USB 메모리 등, 전자화 정보를 저장·유지할 수 있는 기기(파소 콘류는 제외)
22 내부 감사	정보 보안 경영 시스템에 대해 자체적으로 수행하는 감사
23 부문	회사부, 팀, 총칭
24 부문장 25	부문의 최고 책임자
이해관계자 고객, 사원, 이용자, 협력회사 사원, 파견사원, 감독관청, 업계단체, 주주, 빌딩	소유자, 노조, 주변 주민, NGO 등

2	조직 관리	발행일 2024.04.01
적용 범위	전사·전 직원	

## 2장 조직적 관리책

### 2.1 정보보안을 위한 정책군

경영자는 정보 보안 기본 방침을 정의한다.

다른 정책군을 정의한다.

액세스 제어 정책, 백업 정책

정보 보안 책임자는 정의된 정보 보안 기본 방침, 연도 목표 및 기타 방침군을,

정보보안위원회에서 승인을 받는다.

정보보안책임자는 종업원에게 정보보안기본방침, 연도목표 및 기타 방침군을 정보보안위원회로부터의 주지나 사내 홈페이지를 통해 인식하게 한다.

경영자 및 정보 보안 책임자는 정보 보안 기본 방침, 연도 목표 및 기타 정책 그룹을

정기적(연 1회 이상)에 재검토를 한다.

승인을 얻는다.

### 2.2 정보 보안의 역할 및 책임    경영자는 정보 보안

체제를 아래 표에 따라 할당하여 자산에 대한 보호 책임자 및 특정 업무 (자산의

관리, 사업계속)에 대한 실시책임자 및 각각의 책임범위를 정보보안제도에서 명확히 한다.



직책명	역할과 책임
정보 보안 책임자 (CISO)	정보 보안에 관한 책임자. 정보 보안 대책 등의 결정 권한을 가지는 것과 동시에, 전 책임을 진다.
정보 보안 부문 책임 사람	각 부서의 정보 보안 운영 관리 책임자. 보안 대책의 실시 등의 책임을 진다.
정보 시스템 부서 네트	사내의 정보 시스템에 필요한 정보 보안 대책의 검토·도입을 실시한다.
워크 관리자	사내의 네트워크에 필요한 정보 보안 대책의 검토·도입을 실시한다.
교육 책임자	정보 보안 대책을 추진하기 위해 직원에게 교육을 기획하고 실시한다. 한다.
사고 대응 책임자	사고의 영향을 판단하고 대응에 대해 의사 결정한다.
개인정보보호관리자	개인정보의 취급에 관하여 관련 법령을 준수할 책임을 진다.
감사 책임자	정보보안 대책이 제대로 시행되고 있는지 정보보안 관련 규정을 기준으로 검증 또는 평가하여 조언을 한다.
복구 책임자	자연 재해 및 사이버 공격을 포함한 정보 보안 사고가 발생합니다. 그 때, 사업계속계획에 따라 서비스나 시스템의 복구를 실시한다.

### 2.3 직무의 분리

부정행위를 쉽게 할 수 없도록 액세스권 등의 요구, 승인, 실시를 하는 담당을 분리한다.

시스템 운용을 안정적으로 운용하기 위해서, 시스템 운용 관리자와 시스템 운용 실시의 직무를 분리한다.

### 2.4 관리층의 책임

관리 계층은 정규직 및 계약 직원에게 정보 보안 정책, 정보 보안 목표 및 보안  
를 사내 홈페이지 등으로 공표·주지해, 준수를 지도한다.

## 2.5 관계 당국과의 연락

정보 보안 책임자 또는 정보 보안 부문 책임자는 보안 사건 · 사고의 경우 적절한

조치를 취할 수 있도록 아래 표에 나타내는 행정기관, 규제기관, 정보 서비스 제공자 및 통신업자와의 연락 체제

구축한다. 구체적인 연락처 등은 일람에 정리한다.

이름	연락 내용
내각부	인정 어린이 원업무 수탁에 의한, 행정상 필요한 보고
후생노동성	의료·개호 업무 및 보육원 업무 수탁에 의한, 행정상 필요한 보고
문부과학성 총	유치원 업무 수탁에 의한, 행정상 필요한 보고
무성	의료 업무 수탁에 의한 행정상 필요한 보고서
경제산업성 개	의료 업무 수탁에 의한 행정상 필요한 보고서
인정보보호위원회	개인 정보의 유출 등 개인 정보에 관한 사고의보고
경찰서	정보 보안 시설에의 침입 등, 정보 보안 사건 · 사고의 통보
소방서	정보 보안 시설이 화재나 요원의 부상·병 등의 구급 연락
전기 사업자	정보보안시설·설비에 전기공급에 관한 문의
전기 통신 사업자	네트워크 경로 등 통신 상황 문의
수도국	장비 냉각 설비에 대한 냉각수 공급에 관한 문의

## 2.6 전문 조직과의 연락

정보 보안 책임자 또는 정보 보안 부서 책임자는 필요에 따라 사내 또는 아래 표에 표시된 사외

정보 보안 전문가의 조언을 요구한다 조직 전체의 조정 방법은 정보 보안위원회를 이용한다.

조정하는 구체적인 연락처 등은 일람에 정리한다 (외부 커뮤니케이션 일람 등).

명칭	연락 내용
독립 행정법인 정보 처리 추진 기구(IPA)	기술적 내용을 포함한 정보 보안에 관한 상담 전반
일반 사단법 JPCER 코디 네이션 센터 (JPCERT/CC)	인터넷을 통해 발생하는 침입이나 서비스 방해 등의 사고 에 대해서, 일본 국내에 관한 인시던트 등의 보고 접수, 대응의 지원, 발생 상황의 파악, 수법의 분석, 재발 방지를 위한 대책의 검토나 조언
일반재단법인 일본정보경제 사회추진협회(JIPDEC)	개인정보의 유출 등 개인정보에 관한 인시던트의 보고, 개인정보보호 에 대한 좋은 사례 얻기
보안 벤더	시스템 취약성 및 바이러스 백신 소프트웨어 업데이트 정보 얻기 덴트 발생시의 포렌식 조사

---

## 2.7 위협인텔리전스

보안위원회와 같은 내부 조직으로부터 위협 정보를 수집한다.

정보보안책임자는 수집한 위협정보가 조직에 미치는 영향범위를 분석한다.

## 2.8 프로젝트 관리의 정보 보안    정보 보안 부문 책임자는 프로젝트 계획에서 고객의 정보 보안 요구 사항을 명확히

확실히 한다.

<고객으로부터의 정보 보안 요구사항 예>

– 기밀유지·수비의무의 정의나 연수 – 개인정보보

호법의 준수 – 지적재산권에 관한

합의

신규 시스템 또는 기존 시스템 개선에 관한 업무를 실시하는 경우, 시스템상의 보안 요구사항

항을 프로젝트 계획에서 명확히 한다. <시스템

상의 보안 요구사항 예>

– 기밀유지·수비의무의 정의나 연수 – 개인정보보

호법의 준수 – 지적재산권에 관한

합의

하는 제한 사항, 대책·순서 등 사양, 서비스 레벨 등

## 2.9 정보 및 기타 관련 자산의 목록    정보 보안 부문

책임자는 자산(공개된 정보를 제외한 인적 자산·물리적 자산·정보 자산)에 대해 인벤토리를 작성한다(“종업원 명부” “물품 관리부” 무) , 「문  
서 관리부」 , 「기록 관리부」 , 「고객 지급품 관리부」 「정보 자산 대장」등)

자산이 추가, 변경, 삭제된 경우 자산목록을 갱신한다.    자산목록대장에는  
정보·자산의 관리책임자(보유자)를 기재한다.

확실히 지정한다.

2.10 정보 및 기타 관련 자산의 허용되는 이용 정보에 수비  
구분을 표시함으로써 이용 범위를 명확히 한다

한다.

<이용 자격 (액세스 권한) 부여 기준> 종업원

이용자 NW 시스템			파견 사원 협력 회사 사원	고객
	직원 계약	직원		
본사, 사업소, 데이터세터 등 전사 공통 네트워크	모두		부분(필요에 따라)	부여하지 않음
특정 조직별 시스템 무 서비스	부분(필요에 따라)			부여하지 않음
고객에게 제공하는 시스템 무 서비스	부분(필요에 따라)			모두
상기 이외에 사외 워크 시스템	부여하지 않음 (정보 자산을 사외로 반출하지 않음)			부여하지 않음

건물, 집무실에서의 이용 범위를 정보 보안 구획도에 의해 명확하게 한다.

아니.

분류한 정보를 수비 구분에 따라 취급한다.

2.11 자산의 반환

변경/종료 시 반환 또는 폐기를 한다.

제3자가 반환 또는 폐기가 확실히 실시된 것을 확인하여 기록을 남긴다(정보자산 반환대장 등).

2.12 정보의 분류    아

래 표에 나타난 기밀성, 완전성, 가용성을 고려한 분류기준을 정한다.

<분류 기준 예>

	기밀성(C) 관점의 중요도	완전성(I) 관점의 중요도	가용성(A) 관점의 중요도
심각도: "높음"	정보 유출 등이 발생한 경우, 고객, 사회 및 사업에 중대한 그림자 울림이 미칠 우려가 있다.  예) 의료 업무 정보, 개인정보 보고, 영업 비밀, 기밀 정보.	변조 또는 파괴가 발생했습니다.  고객, 사회 및 사업에 심각한 영향을 미칠 수 있습니다.  한다.  예) 청구에 관련된 정보, 상품 업무 정보.	액세스 불가 또는 사용 실패한 상황이 발생하면 고객, 사회 및 비즈니스에 심각한 그림자 울림이 미칠 우려가 있다.  예) 1시간 이상의 액세스 또는 사용 불가 상태가 허용됨 불가능한 정보.
심각도: 「중」	정보 유출 등이 발생한 경우, 고객, 사회 및 사업에 영향을 미칠 수 있 습니다.  예) 회사 정보, 시설 정보 등 사외비정보.	변조 또는 파괴가 발생하면 고객, 사 회 및 사업 영향을 미칠 우려가 있다.  예) 경영 정보, 고객 정보.	액세스 불가 또는 사용 불가능한 상태가 발생하면, 고객, 사회 및 사업에 영향을 미칩니다. 우려가 있다.  예) 하루 이상 액세스 사용할 수없는 상태가 허용되지 않습니다. 없는 정보.
심각도: "낮음"	정보 유출 등이 발생한 경우 그러나 고객, 사회 및 사업에 그림자 히비키가 미칠 우려가 적다.  예)누설해도 영향이 적다 사내 정보.	변조 및 파괴가 발생하더라도 고객, 사 회 및 비즈니스에 영향을 미칠 위험 이 적습니다.  네.  예) 변조된 경우에도 영향 적은 사내 정보.	액세스 불가 또는 사용 불가능한 상황이 발생하더라도 고객, 사회 및 사업에 영향 이 미칠 우려가 적다.  예) 1 주 이상 액세스 사용 불가 상태가 허용 가능 아니 정보.

2.13 정보의 라벨 지정    전자

데이터, 종이 매체 및 기록 매체는 중요도를 식별하고 전달할 수 있도록 관리하는 것이 좋습니다.

아하에 예를 나타낸다.

- 시스템 목록에서 보유한 정보의 중요도를 나타냅니다 - 전자 파일을 파일 서버 또는  
클라우드에 저장하는 경우 폴더 및 파일 이름에 중요도를 표시합니다.

표시 라벨을 붙이거나, 정보를 저장하고 있는 폴더의 일람을 액세스 용이한 장소에 나타낸다.

- 
- 종이 매체와 기록 매체는 보관 장소를 기재한 일람을 액세스 용이한 장소에 나타낸다.  
관 위치에 중요도를 나타내는 라벨을 붙입니다.

## 2.14 정보 전송

### <메일 이용사> 전자

메일을 송신할 때는 송신전에 반드시 수신처와 본문을 확인한다. 업무로 클라우드형 메일은 원칙적으로 이용금지로 한다.

#### 【중요도 “고”(기밀성)】

회사로부터 허가된 단말 이외에서 중요도 「고」의 메일이나 정보의 열람을 금지한다. 중요도 「고」의 정보 자산을 송신하는 경우는, 메일 본문에는 기재하지 않는다.

메일을 이용할 때 다음 사항은 금지한다.

- 업무에 지장을 줄 우려가 있는 사용. - 개인 이메일 서버  
에의 접속

### <물리적 매체의 수송사>

배송업체를 이용하여 기록매체를 배송하는 경우는 신뢰할 수 있고 물리적 손상으로부터 보호하기에 충분한 포장을 한다. 업자를 선정한다.

스스로 기록매체를 운반할 경우에는 물리적 손상으로부터 보호하기에 충분한 포장을 한다.

#### 【중요도 “고”(기밀성)】

종이매체의 개인정보를 동일한 건물 밖으로 배송하는 경우는 배송상황을 추적 가능하고 엄중하게 취급하는 방법으로 보내기.

전자 매체의 개인정보를 휴대용 기록 매체에 저장하고 동일한 건물 외부로 배송하는 경우 전자 파일을 암호화 하 또는 패스워드를 부여하여, 배송 상황이 추적 가능하고 엄중하게 취급되는 방법으로 송신한다.

### <FAX 이용시>

팩스 출력 용지를 방치하지 마십시오.

#### 【중요도 “고”(기밀성)】

팩스 송신 시에는 전화로 수신확인을 한다.

### <소셜 미디어 이용사>

---

종업원이 업무상 소셜미디어(TV나 신문 등의 미디어 포함)에 정보를 발신할 때에는 사전에 홍보·IR부에 그 취지를 통지하여 승낙을 얻어야 한다. 또한 그 때는 회사에 대해 말하는 것 및 자신의 발신의 영향도를 충분히 이해함과 동시에 그 최종적인 책임은 기업으로서 회사가 져야 한다.

하는 것을 인식한다.

직원은 업무상(공식 계정)으로 facebook, Instagram, YouTube, tiktok, X 등의 소셜 미디어

이어를 이용하는 경우, 아래에 내거는 사항을 이해해, 준수한다

- 공식 계정을 개설 할 때 "소셜 미디어 사용 매뉴얼"을 읽고 솔라 플로우  
보다 신청. 홍보과에 의한 최종 심사 후에 개설할 수 있는 것으로 한다
- 직무상 알게 된 비밀(회사 외부의 사람에게 공개되지 않은 정보)은 투고하지 않는다 - 회사의 종업원으로서 자각과 책임을 가지고 발신을 한다.

발신을 한다. 또한 정치적, 종교적인 발신도 하지 않는다.

- 발신한 정보가 장기간 공개될 것, 즉시 확산될 수 있음을 이해하고 발  
 믿는 정보의 내용을 조심스럽게 음미하다

종업원은 개인에서 소셜미디어를 이용하는 경우 원칙회사와 관련한 발신을 해서는 안 된다.

우발적으로 배달된 경우에는 그 사실을 지체없이 홍보·IR부에 보고한다.

#### <전자 서명>

법령으로 서명 또는 기명·날인이 의무화된 문서에서 기명·날인을 전자서명으로 대체하는 경우, 법령

에 준거한 조건을 만족하는 전자 서명을 실시한다.

법정 보존기간 등의 필요한 기간, 전자서명의 검증을 계속하여 할 수 있도록 필요에 따라 전자서명을 포함한 문서 전체에 타임스탬프를 부여한다.

를 채워 실시한다.

#### <기타>

공공의 장소(빌딩 공용부, 엘리베이터내 등)에서 업무에 관한 이야기를 하지 않는다.

공식 계약을 체결

누구나 사용할 수 있는 외부 서비스(예: 인스턴트 메시지, 소셜 네트워크, 파일 공유

또는 클라우드 스토리지)를 이용할 때는 사전에 상장과 정보시스템 부문의 승인을 얻는다.

#### 2.15 액세스 제어

정보 보안 책임자는 업무상 및 관련 법규상의 물리적·논리적 액세스 제어에 관한 요구사항을

정의하고 액세스 제어 규정을 수립한다.

<액세스 제어 규정에 기재하는 항목 예>

- 액세스 제어 정책

- 
- 사용자 계정 발급 및 관리 - 암호 설정 - 게스트 계정 발급 및 관리    네트워크 이용 규정을 정한다.

<네트워크 이용 규정에 기재하는 항목 예>

- 허가 절차 - 이용 제한 - 관리 시스템 - 관리 절차
- 트러블 발생시 대응

## 2.16 식별 정보 관리

- 전사 공통 네트워크 시스템 등 여러 사람이 이용하는 정보 시스템 및 서비스에 액세스하는 장소  
합은 관리자로부터 승인을 얻는다.
- 전사 공통 네트워크 시스템 등 여러 사람이 이용하는 정보 시스템 및 서비스에 액세스  
청·삭제·변경의 순서를 정한다.
- 전사 공통 네트워크 시스템 등 여러 사람이 이용하는 정보 시스템 및 서비스의 사용자 ID는  
고유한 것을 부여한다.

## 2.17 인증 정보

<시스템 이용자용>

- 시스템 이용 개시시에 설정된 초기 패스워드는, 신속하게 용이하게 추측할 수 없는 패스워드로 변경한다  
한다.

- 비밀번호는 10자 이상(영대문자, 영소문자, 숫자, 기호 중 3종류 이상이 혼재)의 패스프레이  
즈를 사용한다.

- 사용자가 비밀번호를 잊어버린 경우에는 이용자의 신분 증명이 이루어진 후에 초기 비밀번호를 발행한다. 개인 암호는 공유하지 않습니다.

<시스템 운용자용>

- 이용자에게 정기적인 비밀번호의 변경을 강제하지 않는다.



---

개인 계정을 다른 사람과 공유하는 것을 금지한다. 여러 사용자가 사용하는 계정 (공유 계정)은 개인을 식별 할 수없는 문제와 위험을 이해합니다. 에서 발행한다.

사용자 계정은 정보 보안 책임자의 승인에 따라 등록한다. 사용자 계정이 더 이상 필요하지 않은 경우, 정보 시스템 부서는 해당 계정을 삭제하거나 무효화합니다.

계정이 더 이상 필요하지 않은 날 다음날까지 실시합니다.

당사의 종업원 이외의 사람에게 계정을 발행하는 경우는, 부문장의 승인을 얻은 후에, 비밀 유지 계약을 체결한다.

## 2.18 액세스권

시스템 및 직무실이나 서고, 정보에 대한 액세스권의 제공 및 해제는 2.10에 기재된 이용 자격(엑세서리 권한)의 부여 기준에 따라 실시한다.

이용자의 액세스권을 정기적으로 검토하고 필요에 따라 변경한다. 사원, 계약 사원 등, 협력 회사 사원, 파견 사원의 고용 종료시, 계약 종료시 또는 합의의 종료시에 직무실, 사 - 방, 보안 방, 정보에 대한 불필요한 액세스 권한을 삭제하거나 변경합니다.

## 2.19 조달 제품 서비스 및 위탁처의 정보 보안 대책의 평가와 관리

사용한다.

청소업자나 보수업자(ICT 기기, 복사기, 자판기, 식재 등의 보수업자)가 물리적·논리적으로 조직의 엘리어나 자산에 액세스하는 경우 사전의 허가 및 액세스 기록을 취한다.

정보 보안 부문 책임자는 정보 자산을 취급하는 업무를 외부 조직에 위탁하는 경우에는 위탁처 사업자의 정보 보안 관리에 대해 「위탁처 정보 보안 대책 상황 확인 리스트」에 기재된 위탁처 사업자 평가 기준에 근거하여 평가한다.

위탁 개시 후에는 「위탁처 정보 보안 대책 상황 확인리스트」에 의해 위탁처 사업자의 정보 큐리티 대책의 실시 상황에 대해 정기적으로 평가할 기회를 마련한다.

### <위탁처 평가 방법>

- 위탁처 사업소에 방문하여 현장을 관찰한다. - 위탁처 사업자의 관리 책임자에게 인터뷰한다.

답해 달라고 한다.

---

## 2.20 정보 보안 요구 사항에 근거하는 외부 위탁 계약

하고 계약을 체결한다.

공급자의 서비스를 이용하는 경우에는 조직의 정보 보안 요구 사항을 충족하는 서비스를 선정하고 계약을 체결한다.

협력 회사 사원, 경비원, 청소원, 보수업자가 정기적으로 서버 룸이나 보안 룸에 들어가는 경우, 보안요구사항을 명시한 계약을 체결한다.

협력 회사 직원이 보안 정책 및 절차를 위반한 경우 필요에 따라 협력 회사에 손해 배상을 요청한다.

위탁계약서에는 하기에 관한 사항을 명기한다.

- 당사의 정보자산 및 개인정보의 수비의무

항

- 정보 보안 대책의 실시 상황에 관한 감사의 방법과 그 권한 - 계약 내용이 준수되지 않는 경우의 조치 - 사고 발생시의 보고 방법

## 2.21 제품 서비스 선정 및 조달시 정보 보안 관리 정보 시스템 부서는 사

내 기반의 네트워크 시스템 운영에 대한 정보 보안 대책을 고려하여 제품 또는 서비스를 선택한다. 사내 기반 네트워크 시스템의 정보 보안 대책 및 관련 사양은 정보 보안 책임자가 승인합니다.

사내 기반의 네트워크 시스템에서 이용하는 서버 기기에 요구하는 정보 보안 요건은 정보 시스템

부서가 결정한다. 새롭게 서버 기기를 도입하는 경우에는 정보 보안 요건을 충족하는 제품을 선택하고 정보 시스템 부서의 허가를 얻어 도입한다.

사내기반의 네트워크시스템에서 이용하는 서버기기에 도입하는 소프트웨어는 정보시스템부문이 표준소프트웨어를 선정한다.

사내 기반 네트워크 시스템에서 사용하는 네트워크 장비에 필요한 정보 보안 요구 사항은

작업 관리자가 결정합니다. 새롭게 네트워크 장비를 도입하는 경우 정보 보안 요구 사항을 충족 제품을 선택하고 네트워크 관리자의 허가를 받아 배포합니다.

당사가 위탁하는 업무를 위탁처가 다른 조직 또는 개인에게 재위탁하는 경우에는 사전에 서면에 의한 보고를 위탁처 사업자에게 요구한다.

- 위탁처 사업자와 재위탁처 사업자와의 계약서안 사본(정보보안과 관련된 부분만) - 재위탁처 사업자 선정기준

- 
- 재위탁처 사업자가 정보 보안에 관한 적합성 평가 제도의 인증·인정을 취득하고 있는 경우에  
그 증서의 사본

위탁처 사업자와 계약할 때에는 재위탁에 관한 제한사항을 포함한다.

【중요도 “고”(기밀성)】

중요한 ICT 제품을 배포하고 교체할 때는 구성 관리를 철저히 하고 구성 요소에 대한 취약성 정보를 수집하고 필요한 경우 대책.

2.22 조달 제품 서비스나 위탁처 서비스의 감시, 리뷰 및 변경 관리 서비스 기간 중에 정기적 및 필요에 따라 업무 보고·기록 등을 취득하고

리티 레벨에 문제가 없는지 확인한다.

정기적 및 필요에 따라 내부 감사나 제3자 심사 등의 감사 결과를 확인한다. 이용하는 외부 서비스의 서비스 내용, 서비스 제공자의 보안 방침, 절차·대책 등이 변경되는 경우 변경 내용을 파악한다.

2.23 클라우드 서비스의 이용에 있어서의 정보 보안 업무 시스템으로서 클

라우드 서비스 등의 외부 서비스를 도입하는 경우는, 정보 시스템 부문이 서비스 프로바이더의 정보 보안 대책을 미리 평가한 후에 선정한다.

- 서비스 제공자가 공개하는 정보 보안 또는 개인 정보 보호에 대한 조치 정책  
이해하려는 정보 자산의 중요도에 비추어 적절하다.
- 서비스 사양에 포함 된 정보 보안 조치가 처리하려는 정보 자산의 중요성  
조명에 적합합니다.
- 정보 보안에 관한 적합성 평가 제도의 인증 및 인증을 취득하는 것이 바람직하다.

<적합성 평가 제도의 종류>

- 정보 보안 경영 시스템 적합성 평가 제도 (ISMS 클라우드 보안 인증) - 클라우드 정보 보안 감사 제도 - 프라이버시 마크 제도
- PCIDSS(신용카드 업계 보안기준) - 클라우드 서비스의 안전·신뢰성에 관한 정보 공개 인정 제도
- ISMAP 정부 정보 시스템을위한 보안 평가 시스템

2.24 정보 보안 사고 관리 계획 수립 및 준비    보안 사건 (보안 정책 위반, 사건, 사고, 중요한 시스템의 보안 문제)

처순(보고처 등의 역할 및 책임 포함)이 있고, 요원에게 사내 홈페이지 등을 통해 전달하고 있다.  
정보보안 인시던트가 발생한 경우에는 다음의 체제로 대응한다.

최고 책임자 정보 보안 책임자(CISO)	
대응 책임자 인시던트 대응 책임자 1차 대응자 발견	
자 또는 정보 시스템 부문	

사고 레벨 1 이상의 인시던트가 발생한 경우 발견자는 "긴급 연락처 목록"에 따라 대응자 또는 책임자에게 신속하게 보고하고 지시를 받는다.

2.25 정보보안 사건의 평가 및 결정    보고된 정보보안 사건이 정보보안 인시던트인지 여부를 결정하는 절차를 정한다.

<정보 보안 사고 레벨 정의>

일 고 레 벨	솔라스트 기준	보안 피해 상황	시스템 장애 상황	신고		
		무단 액세스, 바이러스 감염, 불법 메일 수신, 장치 분실, 정보 지출	인터넷 불통 · 시스템 이용 불가 예	집행 임원 원회	경영 회의	잡다 이 사 회
3	사회적 문제로 발전할 수 있는 가능성	정보 유출, 소실, 분실, 시스템 이용 불가로 사회에 대한 책임을 다할 필요가 특정 상황 대상 정보가 불특정 다수    개인 또는 타 기업이 금전적 피해 불이익을 겪다 많은 고객과 비즈니스 파트너에게 오랜 기간 동안 서비스를 제공하는 데 지장이 있습니다. <small>하다</small>	2일 이상 이용 불가(업무 영향이 있는 경우)	매주 보고	매월 보고 (위험 대책 업데이트)	매 4 분 기 보고
2	영향이 많은 관계자와 회사에 걸쳐	정보 유출·소실·분실이 있어, 전사에의 영향이 있는 상황 거의 모든 회사에서 비즈니스 연속성에 영향을 미칩니다. 직원, 일부 고객 및 비즈니스 파트너에게 영향을 미칩니다. 그러나 "연락 할 수 있는" "영향 정도"등으로 사회 영향을 제어 할 수 있는 상황				
1	영향은 일부 관계자 및 사업에 국한됩니다. <small>하다</small>	정보 유출, 소실, 분실을 수반하지 않음    사업에 제한적인 영향이 있음	당일 이내에 복구			
0	영향이 해당 사업에 제한 <small>하다</small>	사소한 사고	3시간 이내에 복구 부문 내에서	통보 (필요에 따라 시스템 관리 멘토부, 헬프 데스크에 연락		

인시던트를 다음과 같이 구분한다.

구분	사건·사고 상황
정보 유출 · 유출 정보 자산 도난, 유출, 분실	
변조, 소실, 파괴 정보 자산의 의도하지 않은 변조, 소실, 파괴	
서비스 중지 정보 자산이 필요할 때 사용할 수 없음	
바이러스 감염 악성 소프트웨어 감염	

2.26 정보 보안 사고에 대한 대응 정보 보안 사고 (보안 정책 위반, 사건 및 사고, 중요한 시스템 보안 리스크)가 발생하면 인시던트 대응 절차에 따라 처리한다.

2.27 정보 보안 사고로부터의 학습 정보 보안 사고 (보안 정책 위반, 사건, 사고, 중요한 시스템 보안 리스크) 재발 방지 및 피해 확대 방지를 위해 사건, 사고 및 중요한 시스템의 보안 문제 종류, 피해의 크기, 복구 비용 등을 명확히 하고 감시한다.  
교육 책임자는 정보 보안 인시던트에서 얻은 재발 방지책을 보안 교육 등으로 인원에 전달한다.

2.28 증거의 수집  
보안 사건 (보안 정책 위반, 사건, 사고, 중요한 시스템의 보안 문제) 감  
사증적(사건·사고의 경과를 추적할 수 있는 기록) 및 이와 유사한 증거를 수집해, 액세스 제어(시정) 장소에 보관한다.  
보안 사건(보안 방침 위반, 사건·사고, 중요 시스템의 보안 트러블)의 증거,  
삭제, 변조로부터 보호하고 소송과 관련된 작업을 실시하는 경우에는 증거의 복제를 사용한다.

2.29 사업의 중단·저해시의 정보 보안  
정보보안책임자는 중요한 업무의 식별 및 우선순위를 결정하고 이러한 업무가 중단됨으로써 사업에 미치는 영향을 고려한 정보보안 요구 사항을 다룬 사업계속계획을 수립  
정한다. <  
사업계속계획의 항목예>  
- 예상되는 정보 보안 사고 - 업무 내용  
  
- 자산  
- 사업 계속 방법 - 복구  
허용 시간 - 복구 책임  
자 및 관계 연락처

---

---

사업의 중단·저해 시에 정보 보안을 유지하기 위한 계획은 경영진의 승인을 얻는다.

에 따라 검토를 한다.

### 2.30 사업 연속성을위한 ICT 제공 정보 보

안 책임자는 사업 연속성 계획에서 업무 중단 등에 미치는 영향을 고려할 때

필요한 ICT 서비스의 중단 등에 의한 영향(가용성)을 분석, 평가한다.

정보 보안 책임자는 사업 지속 계획에서 ICT 서비스의 중단 등에 의한 영향의 분석 결과를 바탕으로

ICT 서비스에 관한 대응(예방/검지/복구 등)을 검토하고 결정한다.

정보보안책임자는 사업계속계획의 정기적인 시험·재검토에 있어서 필요에 따라 업무의 계속

에 필요한 ICT 서비스에 관한 시험, 재검토도 실시한다.

인시던트 대응 책임자는 상정하는 정보 보안 인시던트가 발생하여 사업이 중단되었을 때의 복구

책임자의 역할인식 및 관계자연락처에 대하여 유효하게 기능하는지 검증한다.

따라서 복구부터 사업 재개까지의 계획을 입안한다.

### 2.31 법령, 규제 및 계약상의 요구 사항 정보 보안

책임자는 조직의 정보 보안과 관련된 관련 법규 및 계약상의 요구 사항을 명시한다.

확실히 하고 조직으로서의 대처방법을 결정한다.

하나.

### 2.32 지적재산권

저작권, 의장권, 상표와 같은 지적 소유권이 있는 소프트웨어 제품 등을 사용하는 경우는 법령, 규칙

그리고 계약상의 요구 사항을 준수하기 위해 적절한 절차를 수행한다.

소프트웨어 제품을 사용하는 경우에는 사용권 계약서에 따라 이용한다.

### 2.33 기록 보호

종이 매체나 기록 매체의 기록은 열화, 손상, 분실, 파괴, 변조를 방지하기에 적합한 장소에 보호하고 보관한다.

한다.

전자매체의 기록은 삭제, 변조, 인가되지 않은 액세스를 방지하기 위해 액세스제어를 한다.

### 2.34 프라이버시 및 개인을 특정할 수 있는 정보(PII)의 보호

「개인 정보 사고 대응 매뉴얼」을 참조한다.

### 2.35 정보 보안의 독립적인 검토 정보 보안 기본 방침

및 연도 목표가 효과적으로 실시되고 있는 것을 내부 감사나 외부 감사로 확인

---

한다.

감사책임자는 정보보안관련규정의 실시상황에 대해 연 1회 점검을 실시하여 감사·점검결과를 정보보안위원회에 보고한다.

- 정보 보안 관련 규정이 효과적으로 구현되지 않은 경우 그 원인을 식별하고 개선 - 정보 보안 관련 규정에 명시된  
규칙이 조치로 불충분하거나 유효하지 않은 경우,

정보 보안 관련 규정 개정

- 정보 보안 관련 규정에 규정 된 규칙이 관련 법령 및 비즈니스 파트너의 정보 보안에 대해  
요구 사항을 충족하지 못하면 정보 보안 관련 규정 개정

2.36 정보 보안 정책, 규칙 및 표준 준수    보안 정책, 연도 목표 및 규정을 준수하

는지 확인하기 위해 정기적으로 절차 확인

다시 검토한다.

보안 방침, 연도 목표 및 규정류에 준거하고 있는지를 감사 등으로 정기적으로 확인한다.

## 2.37 조작 순서서

사내 시스템의 운영 절차서를 작성하여 필요한 사람이 이용할 수 있도록 한다.

한다.



3	인적 관리책	발행일 2024.04.01
적용 범위 모든	직원 (이사, 직원, 계약 직원, 파트 아르바이트 포함)	

3장 인적 관리책 3.1 전

형 신규 채

용, 중도 채용의 응모자가 제출한 이력서, 추천장 등의 내용이 정확한지 확인한다. 시큐리티상의 충분한 직능이나 자질에 대해서, 채용 후에도 계속적으로 확인한다. 정사원, 계약사원이 제출한 이력서, 추천장 등의 내용이 정확한지 확인한다. 또한 충분한 직능

또는 자질이 있는지 확인하십시오.

파견회사로부터 요원이 제공되는 경우에는 계약서에 요원의 전형에 대한 파견회사의 책임을 명기한다.

3.2 고용조건 정

직원을 고용할 때 정보보안에 관한 직원의 역할과 책임을 명기한 고용계약서(또는 서약서)에 동의하고 서명한다.

계약 직원을 고용 할 때 정보 보안에 관한 계약 직원의 역할과 책임을 명시한 각서에 동의하고 서명한다.

파견사원이 보안방침 및 절차를 위반한 경우에는 필요에 따라 파견회사에 손해배상을 청구한다.

고용시 정보 보안에 관한 협력 회사 직원의 역할과 책임, 협력 회사의 책임을 명기 한 계약서 (또한 서약서)를 협력회사와 교환한다.

업무상 알게 된 정보를 외부로 누설하지 않도록 사원 등을 고용할 때 기밀유지를 서약시킨다.

3.3 정보보안의 의식향상, 교육 및 훈련 교육책임자는 정사원, 계약

사원, 파견사원 등에 대하여 입사 시 반드시 보안연수를 실시한다. 마

정기적(연 1회 이상) 및 필요에 따라(이동·변경시) 보안교육을 실시한다.

고객 등 이해관계자가 상주하는 경우 등은 정기적 및 필요에 따라 보안교육을 실시한다.

- 정보보안 관련 규정의 설명(입사시, 취업시) - 최신 위협에 대한 주의 환기(수시) - 관련 법령의 이해(관련 법령의 공포·시행시) - 개인정보의 취급에 관한 유의사항

교육책임자는 아래에 제시된 추천자격의 취득에 의한 종업원의 정보보안에 대한 의식향상을 연도단위로 계획한다.

<정보 보안에 관한 추천 자격>

---

– IPA 정보 처리 기술자 시험 · 정보 처리 안전 확보 지원사 시험 – 정  
보 보안 경영 시험 – 시스템 감사 기술자 시험

### 3.4 징계절차 당사

의 정보보안방침 및 관련 규정을 준수한다. 위반시의 징계에 대해서는 취업규칙에 준한다.

### 3.5 일자리 종료 또는 변경 후의 책임

하자.

재직 중에 알게 된 당사의 영업 비밀 또는 업무 수행상 알 수 있는 기술적 기밀을 이용하여 경쟁적 또는 경쟁  
업적 행위를 해서는 안 된다.

### 3.6 비밀유지계약 또는 수비의무계약

요구사항을 명확하게 기재한다.

특정한 요구사항은 정기적(연 1회 이상) 및 필요에 따라 재검토한다.

### 3.7 리모트 워크

리모트 워크시의 인터넷 액세스는, 자택의 네트워크, 회사 제공의 SIM, 사급 스마트 데

바이스 테더링, 신뢰할 수 있는 기업 및 서비스 제공업체의 공중 Wi-Fi 사용.

리모트 워크를 하는 경우, 주거 환경을 공유하는 사람(가족, 친구 등)에 정보에 액세스 시키지 않는다 리모트 워크를 하는 경  
우, 공공 장소에 있어서의 제삼자로부터의 도둑질 방지를 위한 대책을 취한다.

경우에만.

원격 작업에서 물리 매체를 사용하는 경우 분실이나 도둑질을 방지하기 위해 적절한 보관 장소에 보관  
관하고, 파기는 사무소의 슈레더 등 읽을 수 없는 상태로 하는 것.

리모트 워크로 대여품이 있는 경우는 대출·반납 순서를 명확하게 한다 거래처

·렌탈 오피스·카페·호텔·패스트 푸드·편의점·공항·역·철도·버스 등

이동 중에 원격 작업을 수행 할 때는 다음 사항에 유의하십시오.

– 필요한 정보 이외는 꺼내지 않는다. – 기기나

서류는 눈이 닿는 범위에 두고 방치하지 않는다. 같은 매체를 버

리지 마십시오.

### 3.8 정보보안사건의 보고

의심이 발견되면 절차에 따라보고합니다.

보안의 약점이나 위협을 깨달았을 경우, 또는 그 의심이 있는 경우는 보고 순서에 따라 보고한다    인시던트 대응 책임자는 보고된 보안 사건·약점은 기록한다.

4	물리적 관리 방법	발행일	2024.04.01
적용 범위	모든 사업소		


4장 물리적 관리책  
4.1 물리적 보안 경계

조직의 정보와 자산이 있는 영역에는 보안 경계를 마련한다.

일반 구획 접수·응접	스페이스
이용자	종업원, 사외 관계자, 외부인이 출입 가능
자물쇠	최종 퇴실자에 의한 잠금
설치 가능 정보 장비 프로젝트	컴퓨터, 화이트 보드
제한 사항	사용하지 않을 때 정보 자산의 방치 금지
외부인 관리	직원의 허가를 받아 입실 가능
관리 기록	-
침입 탐지	-
방문객 이름표	요착용
화재 대책	화재 감지기, 소화기 설치

업무 구획	집무실 (개호 시설이나 보육 시설의 거실, 서류 관계가 보관되고 있는 사무소 등)
이용자	직원 이외의 입실은 직원의 허가 또는 에스코트가 필요
잠금	최종 퇴실자에 의한 자물쇠 및 경비 회사에의 통보 장치 작동
설치 가능 정보 기기 프로젝트	컴퓨터, 화이트 보드, PC, 복합기, 전화기, LAN 케이블 허브, 무선 LAN 중계기
제한사항	정보기기·설비의 무단조작금지·무단지출금지
외부인 관리 관	접수의 허가를 받아 입실 가능
리 기록	입퇴실을 소정 양식, 입퇴실 시스템에 기록
침입 감지	센서에 의한 경비 회사 통보
방문객 이름표	요착용
화재 대책	스프링클러, 소화기 설치

액세스 제한 파티션 서버 룸 / 보안 룸	
이용자	미리 허가받은 자
자물쇠	상시 잠금 및 경비 회사에 통보 장치 작동, 열쇠 관리 책임자
설치 가능 정보 기기 서버, 라우터 등의 네트워크 기기, 의료 정보 및 개인 정보를 취급하는 파손	콘
제한사항	정보기기·설비의 무단조작금지·무단지출금지 스마트 폰, USB 메모리, HDD, CD-R, 디지털 카메라 기타 정보 보보 매체의 무단 반입 금지
외부인 관리	보수·점검시 등에 사원의 에스코트 첨부로 입실 가능
관리 기록	입퇴실을 소정 형식으로 기록, 감시 카메라에 의한 기록
침입 탐지	센서에 의한 경비 회사 통보
방문객 이름표	요착용
화재 대책	불활성 가스계 소화 설비, 순수 베이스 소화기, 공조 설비

<p>액세스 제한 파티션</p> <p>(1) 일반 구획과는 인접시키지 않는다</p> <p>(2) 업무 구획과는 분리해, 항상 시정한다</p> <p>(3) 입퇴실의 이력 기록</p> <p>4) 사원은 항상 사원증을 착용</p> <p>(1) 일반 구획과는 분리해, 항상 시정한다</p> <p>(2) 사원은 항상 사원증을 착용</p> <p>(3) 사외의 자가 입실하기 위해서는, 사원이 동행한다</p>	<p>업무 구획 일반 구획</p>	<p>접수</p> 
<p>(1) 사원은 항상 사원증을 착용한다.</p> <p>(2) 방문자는 방문자 배치를 착용하거나 방문자 기록을 취한다</p>		

#### 4.2 물리적 입퇴

정직원, 계약사원은 사원증(입관증)을 보유한다.

방문객이 입실하는 경우 접수를 하여 일반 구획에서의 대응으로 한다.

보수 작업원(복사기, 자판기, 식물을 포함한다) 등이 집무실에 입실하는 경우에는 사원이 입회한다.

고객에 대한 입실 제한이나 정보 또는 자산에 대한 액세스 제어 정책을 명확히 한다

집무실에는 IC 카드로 입실을 허가하여 누구나 입실할 수 없게 한다.

집무실의 입실은 허가된 자만이 입실할 수 있다.

물품의 인도는 원칙적으로 일반 구획에서 실시한다.

【중요도 “고”(기밀성)】

---

서버 룸, 보안 룸에 입실 허가는 필요 최소한으로 한다 서버 룸, 시큐리티 룸의 입실 허가자를 정기적으로 재검토한다 서버 룸, 시큐리티 룸에는 IC 카드에 의해 입실을 허가해, 누구라도 입실을 할 수 없게

한다.

서버 룸, 시큐리티 룸의 입실은 허가된 사람만이 입실할 수 있다.

한다.

PC 등의 물품을 집무실, 서버 룸, 보안 룸에 반입받는 경우 직원

가 일을 하다

창고의 입실은 허가된 사람만 입실할 수 있다.

#### 4.3 사무실, 방 및 시설의 보안 집무실에서의 업무 내용이 옥

외에서 보이지 않도록 한다(예를 들면 블라인드를 내린다) 집무실이 무인이 될 때는 시정한다. 집무실이 무인이 될 때는 경보장치를 가동시킨다.

중요한 장비는 접근이 허용되지 않는 유지 보수 작업자 (복사기, 자판기, 식목 포함) 등 접근할 수 없는 장소에 설치한다.

#### 4.4 물리적 보안 모니터링

적절한 장소에 경비원을 배치한다.

##### 【중요도 “고”(기밀성)】

집무실이나 액세스 제한 구역의 입실을 육안 및 기록하기 위해 감시 카메라 등의 비디오 시스템 소개합니다.

감시 카메라나 경보장치는 정기적으로 시험을 한다

상용하는 모든 문이나 창으로부터의 침입에 대비하여 경보를 사용한다.

#### 4.5 물리적 및 환경적 위협으로부터의 보호 자연재

해 및 인적재해로 인한 피해를 받기 어려운 입지조건인 건물을 차용한다. 화재에 대비하여 화재 경보기 및 소화 시스템을 설치한다.

#### 4.6 보안을 유지해야 할 영역에서의 작업

##### 【중요도 “고”(기밀성)】

서버 룸이나 보안 룸에서는 협력 회사 직원만으로 작업하지 않는다.

---

---

서버 룸이나 시큐리티 룸에 입실하는 협력 회사 직원에게는, 지역의 이용에 관한 유의 사항을 준수한다.

서버 룸이나 시큐리티 룸의 입실 허가 책임자로부터 특별히 허가된 협력 회사 직원만이, 당 지역에 입실할 수 있다.

보수업체가 서버룸이나 시큐리티룸에 입실하는 경우는, 직원이 작업에 입회한다.

결정한다.

허가 없이 서버 룸이나 보안 룸을 카메라, 비디오 등으로 촬영하는 것은 금지한다 서버 룸이나 보안 룸에서 정보 처리 작업을 실시하고 있는 것이 옥외에서 보이지 않도록

한다(예를 들어, 블라인드를 내린다).

서버 룸이나 시큐리티 룸이 무인이 될 때는 잠그십시오.

곳에 설치하지 않는다.

#### 4.7 클리어 데스크 클리어 화면 로그인한 상태에

서 이탈할 때는 로그오프 하거나 화면 잠금을 한다. 로그오프 상태에서는 시스템 조작 화면은 비표시로 설정한다.

전원을 끕니다.

이석시나 귀가시에는 자료를 방치하지 않는다.

회의 등에서 사용한 화이트보드는 종료시 반드시 지운다.

#### 4.8 장비 설치 및 보호 장비가 설

치된 작업 영역에 대한 불필요한 접근은 최소화되어야 한다. PC류는 안정된 장소에 설치한

다. 낙하, 전도의 가능성이 있는 경우는 내진벨트 등

에 의해 PC를 고정한다. 설치 기기는 시정 관리나 감시 카메라의 설치 등 용이하게 반출이 되지 않는 궁리 등 대책이 되는 것.

【중요도 “고”(기밀성)】

중요한 네트워크 장비는 잠금 장치가 있는 랙에 보관한다.

#### 4.9 구외에 있는 자산의 보안

PC류, 스마트폰, 태블릿 단말기를 사외에서 이용하는 경우는 타인에게 들려다 보지 않도록 한다

한다.

PC류의 반출, 수락시의 순서를 책정해 실시한다.

---

---

PC류를 사외로 반출할 경우는 사전에 관리자의 승인을 얻는다.

#### 4.10 저장매체 PC

류를 반납 또는 반입할 경우에는 절차에 따라 문제가 없는지 확인한다. 기록매체의 수명보다 오래 보관할 필요가 있는 경우, 기록매체의 열화에 의한 정보의 소실을 피하기 위해서

기록 매체로 이동한다.

비공개 종이매체를 폐기할 경우는 비공개 종이매체는 재이용  
하지 않는다.

되지 않도록 파괴한다.

이동식 저장 매체의 포트(SD 카드, USB 등)는 필요에 따라 비활성화합니다.

트의 이용은, 보수 서포트 등 필요한 경우에만 한정해, 인증 기능이나 콜백 기능등을 구비하는 등,  
적절한 보안 조치를 취한다.

USB 메모리나 외장 HDD에 저장해야 하는 경우 회사 지정 저장 매체를 사용하여 파일을 암호화  
한다.

저장매체를 이용할 때는 다음을 준수한다.

- 회사가 지정한 USB 메모리는 직무상 필요한 처리에 대체 수단이 없는 경우에만 사용을 허가해야 한다.  
한다.
- 소속장 및 정보시스템부문의 관리자의 허가를 얻지 못한 외부기억매체를 사용하지 않는다.  
사용을 시도하지 마십시오.
- 보관 장소나 취급에는 세심한 주의를 기울여 대여를 받은 소속 부서에서 분실 또는 도난이 없도록  
적절히 관리해야 한다.
- 만일 회사가 대여한 USB 메모리를 도난하거나 분실했을 때는 신속하게 소속장  
그리고 정보 시스템 부서 담당자에게 연락한다.

부서 담당자에게 신고를 하는 것으로 한다. 또, USB 메모리의 이용의 필요가 없어진 경우는, 신속하게 정보 시스템 담당자에게 반환  
하는 것으로 한다.

#### 4.11 서포트 유틸리티 공조 설비

가 갖추어져 있어 정기적으로 보수·점검을 실시하고 있는 건물을 차용한다.



---

【중요도 “고”(가용성)】

일시적으로 정지할 수 없는 장치에 대해서는 전원의 이중화, 무정전 장치, 자가 발전 설비 등을 설치한다.

4.12 케이블 배선의 보안   케이블은 바닥 아

래에 배선하거나 케이블에 보호 커버를 한다.

【중요도 “고”(기밀성)(가용성)】

중요도가 높은 케이블은 대체 케이블을 준비한다.

서버는 잠긴 전용 랙에 수납한다.   LAN 케이블은 회선

도청 방지를 위해 배선을 노출하지 않는다.   무선 LAN에서 정보 착취 및

무단 액세스의 위험을 줄이기 위해 암호화를 사용하는 경우

안전한 암호화 방식을 이용하여 통신을 암호화한다.

4.13 장치의 보수   보

수요원이 집무실에 입실하는 경우에는 필요한 최소한의 액세스권을 부여하고, 또한 보수작업을 감시한다.

그렇지 않으면 제외).

저장매체를 내장한 장치를 수리에 내는 경우는 수비계약을 체결한 업자에게 의뢰한다.

【중요도 “고”(기밀성)(가용성)(완전성)】

지속적으로 기밀성, 가용성, 무결성을 유지할 필요가 있는 기기에 대해서는 하드웨어의 보수 계약을  
맺는다.

4.14 장치의 보안을 유지한 처분 또는 재이용

부서가 지정하는 톨을 사용하여 정보 단말 업무에서 이용한 데이터를 완전히 소거한다.

PC류를 폐기 또는 재이용할 때는 기록을 취득한다.

5	기술적 관리책	발행일	2024.04.01
적용 범위	정보자산 이용자 및 정보처리시설		

5장 기술적 관리책

5.1 이용자 단말

정보 시스템 부서에서 지정한 바이러스 백신 소프트웨어를 설치하고 정의 파일을 자동으로 업데이트합니다.  
설정으로 한다.

스토리지(하드디스크, SSD 등), 전자매체에 대하여 바이러스 체크를 한다.

- 기기 벤더의 공식적인 공개 장소(AppStore, GooglePlay 등) 이외에서 제공되는 것 - 의심스러운 벤더가 제공하는 것 - 정규 라이선스를 취득하지 않은 불법

OS나 어플리케이션 소프트웨어의 업데이트가 통지되면 신속하게 실시한다.

아니.

VPN 서비스를 이용하는 경우는 정보시스템 부문의 허가를 얻는다    VPN 서비스의 이  
용하는 경우는 다음을 모두 준수한다. - 리모트 접속으로 이용하는 정보 단  
말을 분실했을 경우는, 즉시 정보 시스템 부문에 연락해 지시에 따름

우.

- 업무에 관한 정보 자산의 보존을 금지한다.
- IPSec 등을 사용하여 통신 경로를 암호화합니다.

집무실이나 자택, 혹은 회사가 허가한 Wi-Fi 이외는 사용하지 않는다.

- 신뢰할 수 있는 통신 회선만을 이용한다 - 기기는 원  
칙적으로 근무시간만 가동시킨다.

한다.

데이터를 암호화하고 통신합니다.

---

이탈시에는 스크린 락하고, 작업 종료시에는 로그오프를 한다.

데이터를 완전히 지우거나 자기 파괴 또는 물리 파괴하여 복원할 수 없는 상태로 한다.

업무용 스마트 폰이나 휴대 전화를 이용할 때는 원격으로 관리하는 MDM 서비스 등에 가입하여 원격  
와이프, 리모트 락이 가능한 상태로 이용한다.

업무용 스마트 폰이나 휴대 전화는 방치하지 않고 참조 범위 밖의 사람에게 보이지 않도록 비밀번호 등으로  
한다.

PC류를 사외로 반출할 경우는, 수중에서 떼지 않는다.

## 5.2 특권적 액세스권

특권 사용자의 승인 절차를 명확히 하고 승인 기록을 남긴다. 특권유자의 할  
당은 동일인물에 집중함으로써 발생할 수 있는 부정행위 등을 고려하여 복수명으로 분산한다.

높은 빈도로 검토한다.

【중요도 “고”(기밀성)】

특권 사용자로 작업할 때마다 승인을 받는다.

## 5.3 정보에 대한 액세스 제한

이용자의 분류(사원, 계약 사원, 협력 회사 사원, 파견 회사 사원 등)에 따라 액세스권(리드권, 라  
이트권, 실행권 등)을 제어한다.

식별 정보, 장치, 위치, 응용 프로그램 등에 따라 액세스 권한을 부여합니다.

## 5.4 소스 코드에의 액세스

프로그램 소스 코드, 개발 도구, 프로그램 소스 라이브러리는 프로젝트 등으로 결정됩니다.

사람만 액세스할 수 있도록 제어합니다.

## 5.5 보안을 유지한 인증

로그온 절차에, 허가되어 있지 않은 이용자의 도움이 되는 메시지를 표시하지 않는다. 입력한 패스워드를  
평문으로 표시하지 않는다.

로그온에 성공 또는 실패한 로그를 기록한다.

---

IP에 의한 인증을 이용한다.

로그온 후 연결 시간을 제한합니다.

#### 5.6 용량·능력 관리

정보 시스템의 처리 능력 (CPU 및 메모리 사용률, HDD 사용량, 통신량 등)을 모니터링하고 앞으로 필요합니다.

처리 능력과 용량을 예측한다. 필요에 따라 CPU 사용률 및 저장 용량을 조정한다.

【중요도 “고”(가용성)】

처리 능력의 지표에 대해 설비 증강 등의 시스템 변경이 필요하다고 판단하는 기준의 값(임계값)을 설정한다.

매월 1회, CPU 사용률의 이용 상황 등을 감사해, 처리 능력이나 용량이 임계치를 넘지 않도록 조정한다. 조정해도, 임계치를 넘을 것 같은 상황의 경우는, 설비 증강도 포함한 대응을 실시한다.

인적자원의 증원이나 시설의 증가에 대해서도 필요에 따라서 검토하고 있다.

#### 5.7 맬웨어에 대한 보호

바이러스 백신 소프트웨어를 설치하고 정의 파일을 자동 업데이트하는 설정으로 한다. OS 및 소프트웨어를 업데이트합니다. 바이러스에 감염된 경우에는

절차에 따라 봉쇄·근절·복구한다. 바이러스에 감염되었거나 바이러스 감염의 우려가있는 경우 신속하게 사내 네트워크에서 분리

컴퓨터의 전원을 끄지 않고 정보 시스템 부서에 연락한다.

새로운 기기를 도입할 경우에는 사용 전에 바이러스 검사를 실시한다.

구매.

사외와 파일 공유 가능한 소프트웨어는 원칙적으로 사용하지 않는다. 사용하는 경우 정보 시스템 부서의 승인을 받아 사용한다.

【중요도 “고”(기밀성)】

중요한 시스템에서 사용하는 PC에서는 사외와 파일 공유 가능한 소프트웨어를 사용하지 않는다.

네트워크를 통해 입수하는 파일은 자동검출기능을 유효하게 하여 바이러스검출을 실시한다. 접속하는 경우, 정보 시스템 부서의 허가를 얻은 후, 해당 기기에 인스톨 되고 있는 바이러스 대책 소프트의 정의 파일을 최신판에 갱신해, 해당 기기의 풀 스캔을 실행해, 바이러스가 검지되지 않는다

확인한 다음 연결합니다.

바이러스에 감염되었거나 그 의심이 있는 경우의 대응방법에 대한 요원교육을 한다.

받은 경우 정보 시스템 부서에 보고하고 정보 시스템 부서는 사내에 주의를 촉구한다.

---

## 5.8 기술적 취약성 관리    사용

중인 정보 시스템의 기술적 취약성에 대한 정보를 얻고, 위험을 평가하고, 필요에 따라 대책을 취한다.

취약성을 식별하고 대책을 취한다. 취약성에 대한 대책의 유효성은 정보시스템 부문이 판단하고 승인한다.

(참고) IPA 정보 보안 취약성 대책

<https://www.ipa.go.jp/security/vuln/index.html>

취약성을 식별하고 패치 적용을 검증하기 위해 취약성 스캔 도구를 사용한다.

## 5.9 구성 관리

하드웨어, 소프트웨어, 서비스(클라우드 서비스 등) 및 네트워크에 관해서 도입했다

운영 시스템의 보안 설정이 올바르게 구성되어 있는지 확인하기 위해 운영 시스템을 점검하십시오.

정책, 벤더의 권장 사항 등을 고려한다.

## 5.10 정보 삭제

정보 시스템 및 장치에서 정보를 삭제하는 방법 (예 : 물리적 파괴, 자기 소거, 클라우드상의 정보 삭제 등)  
하고 실행합니다.

삭제 결과를 증거로 기록한다.

한다.

## 5.11 데이터 마스킹    필요

에 따라 개인정보나 요배려 개인정보는 마스킹이나 익명화·가명화하는 등의 대책을 강구한다.

## 5.12 데이터 유출 방지    조

직 내에 저장된 정보가 외부로 업로드되거나 이메일로 전송됨으로써 외부

정보가 유출될 가능성이 있는 경우에 검지, 방지하기 위한 대책을 강구한다. 또는 액세스 제어나 암호화  
저장을 수행한다.

## 5.13 정보 백업    백업 정책에 따라

백업을 얻는다.    백업에 이용한 기기의 취급은 다음의 모든 것에 따른다.

<보관 예>

CD/DVD, 외장 HDD, USB 메모리 등: 잠긴 캐비닛에 보관

NAS 서버: 잠금 장치가 있는 서버 랙에 저장

<폐기·재이용 예>

---

4.14(장치의 보안을 유지한 처분 또는 재사용)에 따른다.

클라우드 서비스를 이용하여 외부 서버에 백업을 저장하는 경우 다음 서비스 요구 사항을 확인하고 정보 시스템 부서의 허가를 얻어 도입한다.

<서비스 요건>

- 서비스 제공자의 서비스 이용 약관, 정보 보안 정책은 당사의 정보 보안 관련 규정 정도에 적합하다.
- 당사사업소가 있는 지역에서 발생하는 지진재해, 수해 등의 영향을 받지 않는 지역의 시설이다.

【중요도 : 「고」(가용성)】

매우 중요한 업무 정보 및 소프트웨어가 있는 경우 정기적으로 백업을 한다.

분리된 장소에 보관한다.

백업 파일을 정기적으로 검사합니다.

#### 5.14 정보처리시설·설비의 중복성

정보 처리 시스템은 그 중요성에 따라 중복 구성 또는 지역 분산을 수행한다.

【중요도 : 「고」(가용성)(완전성)】

지속적으로 가용성과 무결성을 유지해야 하는 장비 및 장비의 경우 하드웨어 또는 네트워크를 중복하거나 예비 하드웨어를 준비한다.

#### 5.15 로그 취득 사

용자 ID (특권 사용자도 포함), 로그인 및 로그 오프 일시, 시스템이나 데이터에 액세스를 시도하고 성공과 실패를 기록하고 중요도에 따라 필요한 기간 (예 : 1 년) 보관하십시오.

정보 보안 침해가 발생하지 않았는지, 시스템별로 정해진 간격으로 정기적으로 취득한 로그 분석합니다.

로그 기능의 설정은 허가된 사람만이 실시할 수 있도록 액세스 제어한다. 로그 정보는 허가된 사람만이 액세스할 수 있도록 제어한다.

시스템 부문에 보고한다.

【중요도 : 「고」(기밀성)】

다음 모두에 따라 게이트웨이에서 통신 로그를 얻고 저장합니다.

- 통신 로그의 보존 기간은 최소 1년으로 한다.

정보 시스템 부서는 통신 로그에 대해 다음의 모든 확인을 정기적으로 실시한다.

- 관리 외부의 인터넷 연결이 없는지 - 허가 없이 연결된 기기나 무선 LAN 기기가 없는지 - 의심스러운 통신이 없는지

---

#### 5.16 감시 활동

사내 시스템이나 네트워크의 비정상적인 트래픽이나 사외로부터의 의심스러운 액세스를 감지하고 경고하는 것  
세트를 마련한다.

#### 5.17 클럭 동기화

정보시스템에서 사용하는 서버나 PC는 컴퓨터내의 시계를 조직이 채용한 NTP에 맞춘다.  
오, 일부의 독립형 PC 등에 대해서는 제외한다.

#### 5.18 특권적인 유틸리티 프로그램의 사용 시스템 및 업무 프

로그래밍의 제어를 무효로 하는 시스템 유틸리티를 사용하는 경우, 사용한다

사람, 시간을 제한한다.

시스템 및 비즈니스 프로그램 제어를 비활성화하는 시스템 유틸리티를 사용할 때 사용 기록  
결립한다.

시스템 및 비즈니스 프로그램 제어를 비활성화하는 불필요한 유틸리티 소프트웨어는 제거  
토르한다.

#### 5.19 운영 시스템에 소프트웨어 도입

시스템의 유지관리를 실시하는 경우, 운용 프로그램의 갱신은 임명된 담당자에 의해 실시한다.

관리한다.

#### 5.20 네트워크 보안

각 네트워크 (사내 기간 네트워크, 인터넷 연결 세그먼트, 엑스트라 넷 연결 세그먼트  
, 애플리케이션 서비스 세그먼트, OA 네트워크, 개발 네트워크, 부서 기간 네트워크 등)의 경계와 관리 책임의 위치를 명확히 한다.

네트워크 관리자는 네트워크에 흐르는 정보의 보호 및 네트워크 기반(라우터, 방화벽, 게이트웨이 등)을 보호(라우터 등의 올바른 설정 포  
함)하기 위한 대책을 강구한다.

네트워크 운영 절차에 따라 네트워크를 운영합니다.

#### 5.21 네트워크 서비스 보안 네트워크 서비스 제공자 (전

사 네트워크 관리자, 자체 네트워크 관리자)는 네트워크 이점

사용자에게 서비스의 보안 특성을 명확하게 설명하고 사용자와 합의한다.

WAN 및 인터넷 서비스의 경우 SLA 및 보고서를 수령하고 문제가 있는지 정기적으로 확인하고 합의했습니다.

SLA와 같은 네트워크 서비스인지 여부를 모니터링합니다 (LAN의 경우 네트워크 트래픽 등  
를 정기적으로 확인한다.

---

## 5.22 네트워크 액세스 제어

사내 네트워크(독자 네트워크를 포함)와 사외 네트워크를 분리하여 액세스 제어를 한다.

불필요 · 불법 액세스가 발생하지 않도록 액세스 제어한다.

## 5.23 웹 필터링 정보 유출로 이

어지는 사이트나 업무상 불필요하다고 생각되는 사이트에 대한 액세스를 금지한다. 정보 유출로 이어지는 사이트나 업무상 불필요하다고 생각되는 사이트에 대한 액세스를 막기 위한 기술적 구조를 구축한다.

액세스가 금지된 사이트에 업무상 액세스할 필요가 있는 경우는, 예외 신청 순서에 따른 대응을 행  
우.

정보시스템부문은 바이러스 등의 악의가 있는 소프트웨어에 감염될 우려가 있다고 인정되는 유해 웹사이트는 사내주지 또는 웹필터링 소프트웨어를 사용하여 직원의 열람을 제한한다.

종업원은, 업무로 웹 열람을 실시하는 경우는 이하의 모두에 주의한다.

– 공서양속에 반하는 사이트에의 액세스를 금지한다 – 의심스러운 사이

트에의 액세스 및 사용 메일 주소 등록을 금지한다. 신뢰할 수있는 사이트에서 서명 된 모바일 코드를 다운로드하지 않는 한 모바일 코

드(클라이언트 PC측에서 동작하는 프로그램)를 실행하지 않는다.

## 5.24 암호의 이용

암호화 기술을 이용하는 규칙을 정한다.

전송되는 정보를 보호하기 위해 암호화 기술을 사용하는 등.

암호화 키를 사용하는 경우에는 키 생성, 공개 키 인증서 얻기 방법, 키 배포 방법, 키 변경 및 업데이트, 파기 방법  
법과 같은 절차를 만듭니다.

암호의 이용에 있어서는, 디지털청·총무성·경제산업성의 암호 기술 검토회 및 관련 위원회(CRYPTREC)  
권장하는 암호화 기술을 사용합니다.

## 5.25 보안을 고려한 개발 라이프사이클

시스템 및 소프트웨어 개발의 보안을 고려한 규칙을 확립하고 실시한다.

템 부문의 승인을 얻는다.

① 대상 업무의 범위 정의 ② 하

드웨어, 소프트웨어, 네트워크 기능 검토 ③ 필요한 성능 검토



- 
- 
- ④ 정보 보안 요건 정의 ⑤ 백업/장애 복  
구 요건 정의 ⑥ 정보 시스템 운용 요건 정의 ⑦  
운용 체제 ⑧ 이행 계획 입안

5.26 애플리케이션 보안 요구 사항 애플리케이션을 개발 또  
는 취득하는 경우 애플리케이션에서 거래하는 정보의 기밀성, 무결성 및  
진실성을 보장하기 위해 정보를 암호화합니다.  
응용 프로그램을 개발할 때 설계 단계에서 보안 요구 사항을 고려한다.

하기 위해 정보를 암호화합니다.  
거래 서비스를 제공하는 응용 프로그램의 경우 전자 인증서로 거래 상대방의 본인 확인  
인정한다. 전자인감은 해당되지 않는다.  
통신경로를 암호화한다.  
"정 가이드라인"에 따라 대응한다.  
온라인 거래 정보를 암호화한다. 전자 서명  
을 사용하여 온라인 거래 정보의 정당성을 보장한다.

을 얻는다.

#### <인터넷 뱅킹·전자 결제>

- 인터넷 뱅킹을 이용할 때, 자신이 설정한 북마크와 은행이 제공하는 전  
응용 프로그램 소프트웨어를 사용합니다.
- 전자결제를 이용할 때에는 SSL/TLS에 의한 통신 암호화를 채용하고 있는 사이트를 이용한다.

로의 유도일 수 있으므로 액세스하지 않는다.

【중요도 : 「고」(기밀성)】

중요한 시스템에서 사용하는 PC에서 인터넷 뱅킹·전자 결제를 실시하지 않는다.

#### <온라인 스토리지>

- 중요도 : "고"정보 자산을 보존하는 경우, 정보 시스템 부서의 허가를 얻는다. - 메일 주소의 등록이 필요  
한 경우는 사용 메일 주소를 등록한다.

---

## 5.27 보안을 고려한 시스템 아키텍처 및 시스템 구축의 원칙    시스템의 보안이 침해되기 어려운 구조 및 방어하는 기능을 고려한다.

<예> 압

호화 기능, 전자 서명 등

제로·트러스트 원칙 등의 보안을 배려한 시스템 구축을 실시한다.

## 5.28 보안을 고려한 코딩    보안을 고려한 프로그래밍 방법을 사용한다. (보안 코딩)

한다.

## 5.29 개발 및 수용에 있어서의 보안 테스트    신규 시스템을 개발하거나 기존 시스템을 개수한 경우는, 보안 시험(취약성 진단,

소스 코드 검토 등)를 실시한다.

【중요도 : 「고」(기밀성)】

중요한 시스템을 신규 개발 또는 개조할 경우, 침투 테스트를 실시한다.

새로운 정보시스템, 개판 및 변경판을 수락할 경우에는 수락기준을 명확히 하고 기준을 만족하고 있다.

수락하기 전에 검사한다.

## 5.30 외부 위탁에 의한 개발

소프트웨어 개발을 외부 위탁하는 경우에는 보안 요구 사항을 충족하는지 확인한다.

한다.

외부 위탁한 작업의 제공이 합의 사항을 충족하고 있는지를 (개발 기간 중의 회의나 보고에서) 지속적으로 감시하고 검토합니다.

소프트웨어 개발을 외부 위탁하는 경우는 소스 코드의 품질, 작업의 질 및 정확도 등을 고려한다.

정보 시스템에 알려진 취약점이 존재하지 않는 상태에서 운영한다.

- 개발시에 사용한 소프트웨어에 대한 취약성이 공표된 경우에는 신속하게 그 영향이 현재화하지 않기 위한 대책을 강구한다.

- 개발 시 사용한 소프트웨어 및 하드웨어 제조업체가 제공하는 지원 종료가 예정됨

그렇다면, 다른 소프트웨어나 하드웨어를 이용한 재구성 또는 해당 정보 시스템의 이용 정지를 검토하여 정보 시스템 부서의 승인을 얻는다.

## 5.31 개발 환경, 테스트 환경 및 프로덕션 환경의 분리

큐리티 환경을 확립하고 개발한다.

---

개발·시험 환경과 프로덕션 환경은 논리적 또는 물리적으로 분리한다. 개발에서 운영 단계로 마이그레이션하는 경우 마이그레이션 절차를 만듭니다. 정보시스템의 개발 및 개수를 하는 환경은 운용환경과는 분리한다. 새롭게 정보시스템의 개발을 실시한 경우나, 정보시스템의 개수를 실시한 경우는, 해당 정보시스템의 운용을 개시하기 전에, 필요한 정보시큐리티 대책이 강구되고 있는지를 확인해, 정보시스템 부문의 승인을 얻는다.

### 5.32 변경 관리

소프트웨어, 문서, 프로그램 등은 프로젝트 등에서 정한 구성 관리 순서에 따라 변경을 관리합니다.

【중요도 : 「고」(가용성)】

중요한 업무용 소프트웨어의 OS를 변경하는 경우 운영중인 시스템에 장애가 발생하지 않도록 시도  
시험 환경에서 확인한다.

패키지 소프트웨어는 원칙적으로 변경하지 않는다. 정보 시스템의 하드웨어 또는 소프트웨어를 변경할 때는 다음의 모든 단계를 거쳐 실시한다.

한다. 각 단계가 완료되면 정보 시스템 부서의 승인을 얻습니다.

① 현행 시스템의 문제·과제의 파악

### 5.33 테스트용 정보

개인정보를 포함한 운용데이터는 시험에 사용하지 않는다.

그렇다면 개인 정보의 사용, 보관, 반환 등의 취급 절차를 확인하고 그 절차를 따릅니다.

개인정보를 포함한 운용 데이터를 시험에 사용하는 경우는 시험 완료 후 삭제한다.

### 5.34 감사에서 테스트 중 정보 시스템 보호

정보시스템의 감사를 실시하는 경우는 업무가 중단되는 리스크를 최소한으로 억제하도록 신중하게 계획을 세워,  
관계자의 합의를 얻고 나서 실시한다.

정보 시스템에 액세스하여 감사를 수행하는 경우 운영 시스템에 부정적인 영향을 미치지 않도록 신중하게 계획을 세우고 관계자의 합의를 얻고 나서 실시한다.