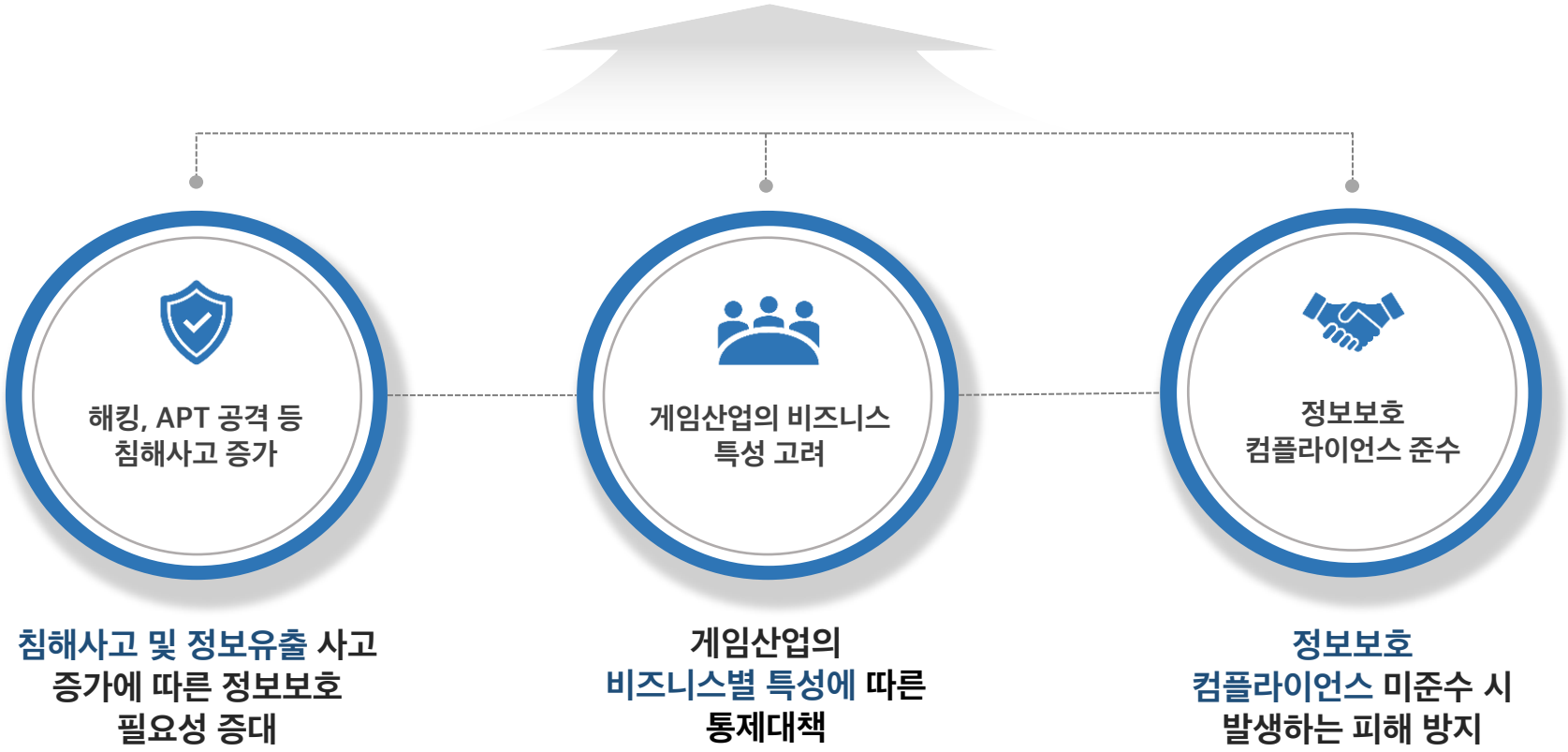
게임산업 서비스에 따른 정보보호 요구사항 도출

2022.12.15

목차

게임산업의 정보보호 컴플라이언스 및 인증을 고려한 정보보호 통제대책 수립

정보보호 통제대책 수립 및 가이드 도출



게임산업 분석 및 관련 컴플라이언스/리스크 식별하여 정보보호 요구사항 도출

게임산업 서비스 분류 및 환경 분석

게임제작업 (개발사)	게임배급업 (퍼블리셔)	게임제공업 (플랫폼)	IT자산			
			전자 정보	문서	S/W	인력
			H/W	시설	지원 설비	

컴플라이언스

법규 (정보통신망법 개인정보보호법 등)	지침 및 가이드	정보보호 인증 (ISMS, ISO27001 등)

정보보호 리스크 식별

위협	취약점	위험

정보보호 요구사항 도출 → 통합 및 분류 → 보안대책 수립

게임산업의 정의 및 분류

게임산업의 정의 (게인산업진흥법 제2조)

게임물 또는 게임상품(게임물을 이용하여 경제적 부가가치를 창출하는 유·무형의 재화·서비스 및 그의 복합체)의 제작·유통·이용 제공 및 이에 관한 서비스와 관련된 산업

게임산업의 분류

분류	내용 (게임산업진흥법 제2조)
게임제작업	게임물을 기획하거나 복제하여 제작하는 영업
게임배급업	게임물을 수입하거나 그 저작권을 소유/관리 하면서 게임제공업을 하는 자 등에게 게임물을 공급하는 영업
게임제공업	공중이 게임물을 이용할 수 있도록 이를 제공하는 영업

게임산업의 가치사슬

개발사 → 퍼블리셔 → 플랫폼 → 소비자

주요 정보 자산 분류

전자정보

- 전자적 형태로 저장되는 데이터

예 데이터베이스, 데이터파일, 전자파일 등

문서

- 종이매체로 된 정보자산으로 업무에 사용 및 산출되는 문서나 기록물

예 규정 및 지침, 각종 대장, 계약서, 협약서 등

소프트웨어

- 사용 또는 자체 개발된 소프트카피나 하드카피로 보관중인 소프트웨어 자산

예 애플리케이션 S/W, 개발도구, 유틸리티 등

시설

- 시스템을 설치 및 운영하는 장소를 의미, 물리적 공간 및 각종 부대시설

예 전산실, 사무실, 방재실, 통신장비실 등

지원설비

- 전력공급, 환기시설, 방재 시설 등 정보시스템 운영을 지원하기 위한 설비

예 항온항습기, UPS, 공조 장비 등

인력

- 소유자, 사용자, 운영자, 개발자 등 시스템 운영 및 업무수행 중인 모든 인력

예 내부직원, 협력업체 등

하드웨어

- 네트워크 장비

예 라우터, 스위치 등

- 임직원 개인컴퓨터

예 노트북, 이동형 단말기 등

- 대내외 서비스 업무를 위해 사용되는 서버 자산

예 윈도우·유닉스 장비 등

참고 – LG CNS 분석 자료

게임산업 관련 컴플라이언스 및 분석 범위

법규

정보통신망법

- 정보통신망의 안전성 확보
- 침해사고 대응
- 정보보호 관리체계 인증 등

개인정보보호법

- 개인정보처리 제한
- 개인정보의 안전한 관리
- 정보주체의 권리 보장 등

게임산업진흥법

- 게임 과몰입 중독 예방 조치
  (14세 미만 이용자 법정대리인 동의 등)

부정경쟁방지 및 영업비밀법

- 영업비밀 침해 및 유출 예방 및 대응 등

저작권법

- 소프트웨어 불법 사용 제한 등

지침 및 가이드

정보보호조치에 관한 지침
정보통신망법 세칙

개인정보 보호조치 기준
개인정보보호법 세칙

정보보호 인증

ISMS-P
정보보호 및 개인정보보호
관리체계 국내 인증

ISO 27001
정보보호 관리체계
국제 인증

정보자산, 위협, 취약점, 위험 도출

*그룹핑한 일부 영역만 나타냄

자산	위협	취약점 구분
전자정보	**내부**	소프트웨어 취약점 (비인가 소프트웨어 사용, 삭용자 식별 인증 미흡 등)
문서	임직원의 실수	하드웨어 취약점 (보호설비 구축 및 운영 미흡 등)
소프트웨어	사익을 위한 정보유출 및 절도	네트워크 취약점 (부적절한 네트워크 관리, 암호화 미흡 등)
하드웨어	하드웨어 고장	내부직원 (보안인식 부족, 채용/퇴직 절차 미흡 등)
시설	권한남용	조직 (권한 관리/위험 식별 및 절차 미흡)
지원설비	**외부**	시설 (자연재해에 민감한 위치, 물리적 접근통제 미흡 등)
인력	협력업체의 실수	
	해커의 악의적인 공격	
	경쟁업체로의 정보유출	
	자연재해	

위험				
악성코드 감염	가용성 침해	비인가 서비스 이용	비인가 네트워크 접근	정보유출

참고 - KISA 침해사고대응 가이드

정보보호 요구사항 식별

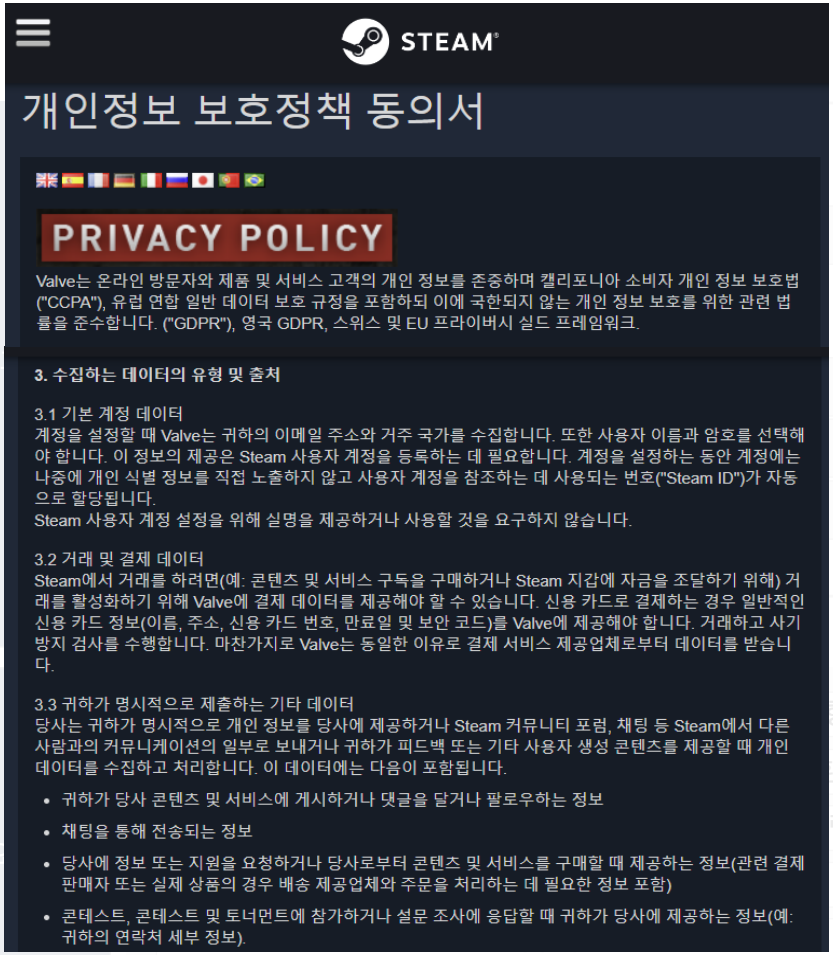
컴플라이언스 및 위험을 고려하여 11개의 영역에서 정보보호 요구사항 도출

정보보호 요구사항			
1. 관리과정	- 정책 수립 - 보안 점검/감사/위험 관리 등	7. 침해사고 대응	- 취약점 점검 및 조치 - 사고 대응 및 복구 등
2. 인적보안	- 보안서약서 징구 - 인식제고 및 교육훈련 등	8. 서비스 보안 관리	- 보안시스템 운영 - 암호화, 패치 관리 등
3. 외부자 보안	- 외부자 현황 관리 - 외부자 계약 및 계약 만료 시 보안 등	9. 서비스 운영 관리	- 백업 및 복구 관리 - 로그 및 접속 기록 관리 등
4. 물리보안	- 출입 통제 및 반출입 기기 통제 - 상황 감시, 업무 환경 보안 등	10. 개발보안	- 보안 요구사항 검토 - 소스 프로그램 관리 등
5. 인증권한 관리	- 사용자 식별 및 인증 - 접근권한 검토 및 관리	11. 개인정보보호	- 개인정보처리 제한 - 개인정보 주체 권리 보장 등
6. 접근 통제	- 네크워큰 접근 통제 - 정보 시스템 접근 통제		- 무선 네트워크 접근 통제 - 원격접근 통제 등

*그룹핑한 일부 영역만 나타냄

컴플라이언스 및 위험 고려하여 요구사항 도출

게임산업 서비스 흐름에 따른 요구사항



STEAM

개인정보 보호정책 동의서

PRIVACY POLICY

Valve는 온라인 방문자와 제품 및 서비스 고객의 개인 정보를 존중하며 캘리포니아 소비자 개인 정보 보호법("CCPA"), 유럽 연합 일반 데이터 보호 규정을 포함하되 이에 국한되지 않는 개인 정보 보호를 위한 관련 법률을 준수합니다. ("GDPR"), 영국 GDPR, 스위스 및 EU 프라이버시 실드 프레임워크.

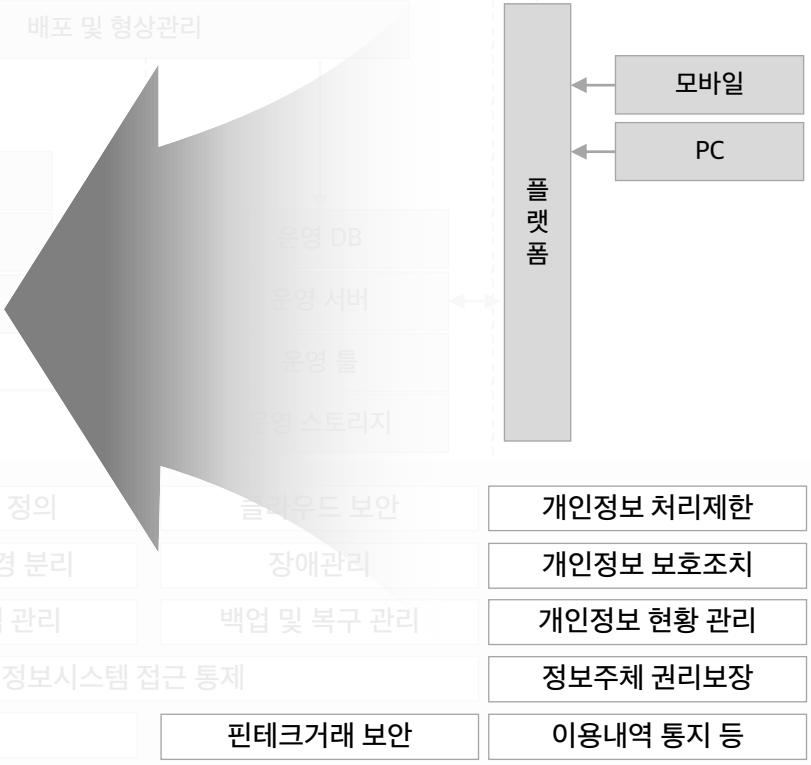
3. 수집하는 데이터의 유형 및 출처

3.1 기본 계정 데이터
계정을 설정할 때 Valve는 귀하의 이메일 주소와 거주 국가를 수집합니다. 또한 사용자 이름과 암호를 선택해야 합니다. 이 정보의 제공은 Steam 사용자 계정을 등록하는 데 필요합니다. 계정을 설정하는 동안 계정에는 나중에 개인 식별 정보를 직접 노출하지 않고 사용자 계정을 참조하는 데 사용되는 번호("Steam ID")가 자동으로 할당됩니다.
Steam 사용자 계정 설정을 위해 실명을 제공하거나 사용할 것을 요구하지 않습니다.

3.2 거래 및 결제 데이터
Steam에서 거래를 하려면(예: 콘텐츠 및 서비스 구독을 구매하거나 Steam 지갑에 자금을 조달하기 위해) 거래를 활성화하기 위해 Valve에 결제 데이터를 제공해야 할 수 있습니다. 신용 카드로 결제하는 경우 일반적인 신용 카드 정보(이름, 주소, 신용 카드 번호, 만료일 및 보안 코드)를 Valve에 제공해야 합니다. 거래하고 사기 방지 검사를 수행합니다. 마찬가지로 Valve는 동일한 이유로 결제 서비스 제공업체로부터 데이터를 받습니다.

3.3 귀하가 명시적으로 제출하는 기타 데이터
당사는 귀하가 명시적으로 개인 정보를 당사에 제공하거나 Steam 커뮤니티 포럼, 채팅 등 Steam에서 다른 사람과의 커뮤니케이션의 일부로 보내거나 귀하가 피드백 또는 기타 사용자 생성 콘텐츠를 제공할 때 개인 데이터를 수집하고 처리합니다. 이 데이터에는 다음이 포함됩니다.

- 귀하가 당사 콘텐츠 및 서비스에 게시하거나 댓글을 달거나 팔로우하는 정보
- 채팅을 통해 전송되는 정보
- 당사에 정보 또는 지원을 요청하거나 당사로부터 콘텐츠 및 서비스를 구매할 때 제공하는 정보(관련 결제 판매자 또는 실제 상품의 경우 배송 제공업체와 주문을 처리하는 데 필요한 정보 포함)
- 콘테스트, 콘테스트 및 토너먼트에 참가하거나 설문 조사에 응답할 때 귀하가 당사에 제공하는 정보(예: 귀하의 연락처 세부 정보).



*출처-Steam 홈페이지

결론 및 시사점

결론 및 고려사항

- 정보보호 컴플라이언스 및 리스크를 고려하여 총 11개의 영역에서 84개의 통제항목 도출
- 게임산업 통합적인 관점에서의 보안 대책 수립 및 운영 가능

시사점

- 정보보호와 개인정보보호의 차이 이해

구분	정보보호(정통망법)	개인정보보호(개보법)
접근권한 부여 기록 보관	최소 5년	최소 3년
접속 기록 점검 주기	월 1회 이상	반기별 1회 이상
비밀번호 변경 주기	반기별 1회	분기별 1회
개인정보 강화 기준	SSL/응용 프로그램	암호화

감사합니다.

2022.12.15