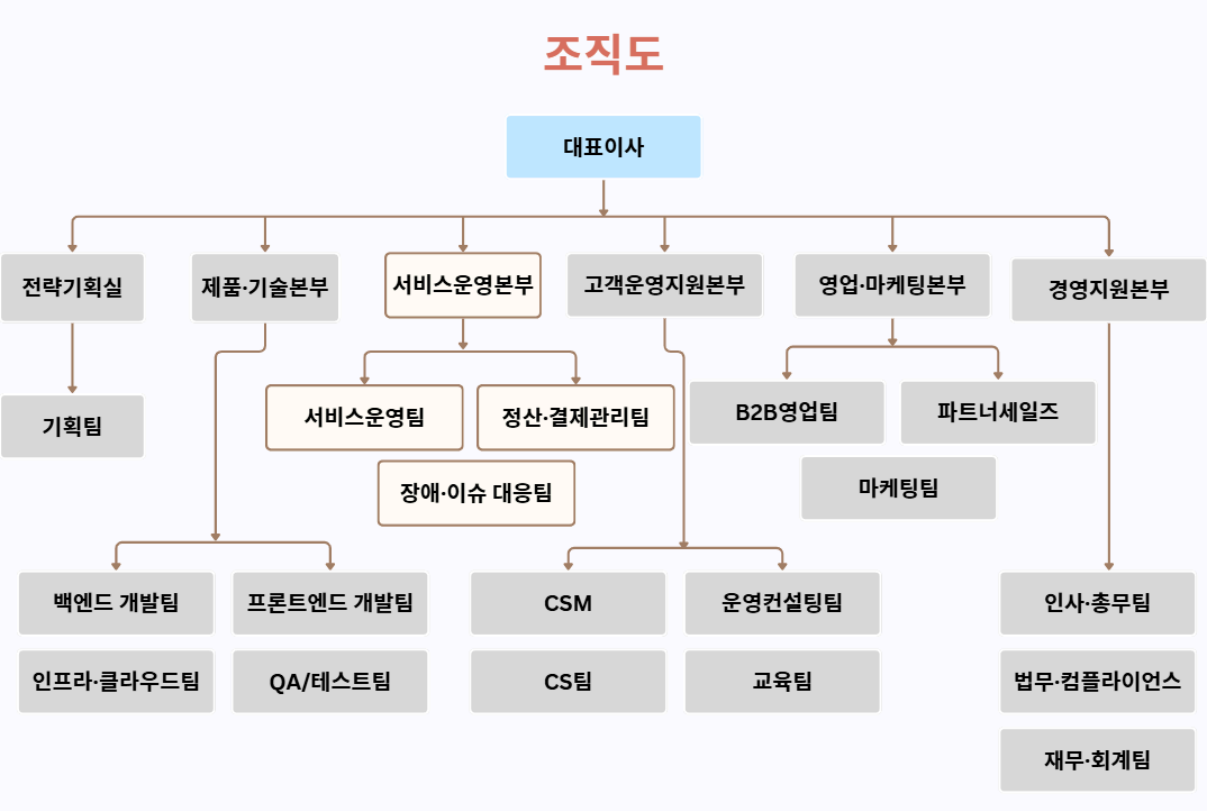
포트폴리오_최장현

1. 프로젝트 개요

본 프로젝트는 SaaS 서비스를 제공하는 이커머스 기업 푸드팡을 대상으로 정보보안 관리체계 현황을 진단하고 ISMS-P 기준에 부합하는 현실적인 정보보안 관리체계 개선 방안을 도출하기 위해 수행되었다

2. 회사 컨셉 및 환경

구분	내용
조직 규모	약 90명, 개발·운영 중심의 SaaS 기업
IT 환경	AWS 기반 클라우드, SaaS 서비스 운영
근무 환경	재택근무 및 BYOD 일부 허용
서비스 특성	회원·판매자·주문·결제 정보를 처리하는 이커머스 플랫폼
취급 정보	회원 개인정보, 판매자 사업자정보, 주문·결제·배송 정보



푸드팡은 빠른 서비스 확장을 목표로 **클라우드** 및 **SaaS** 환경을 도입하였으나, 재택근무 및 외부 협업 증가로 접근 통제와 개인정보 관리 범위가 지속적으로 확대되는 환경에 놓여 있다.

이러한 환경에서는 보안 관리체계가 정립되지 않을 경우 단일 사고가 서비스 중단 또는 대규모 개인정보 침해로 직결될 가능성이 높다.

3. 문제 정의(Why)

현재상태(As-Is)

푸드팡은 기본적인 보안 정책과 일부 기술적 조치는 갖추고 있었지만, 실제 운영 관점에서 **누가 어떤 권한으로 개인정보에 접근하고 있는지**를 지속적으로 관리·점검하는 체계는 명확하지 않은 상태였다.

또한 재택근무 확산으로 외부에서 내부 시스템에 접근하는 경로가 다양해졌음에도, 이에 대한 접근 통제 기준과 승인 절차는 충분히 정립되어 있지 않았다.

문제점

기술적 보안 장비는 일부 적용되어 있었으나, 접근 기록 관리, 권한 승인·변경 이력 관리 등

관리적 통제가 운영 단계에서 제대로 작동하고 있는지 확인할 수 없는 구조였다.

클라우드와 재택근무 환경으로 서비스 구조는 빠르게 변화하고 있었지만, 보안 관리체계는 이러한 변화 속도를 따라가지 못하고 있었다.

잠재적 리스크

퇴사자 계정이 즉시 정리되지 않거나 업무 목적을 초과한 권한이 유지될 경우, 의도적인 행위뿐만 아니라 단순한 실수로도 개인정보가 외부로 유출될 가능성이 존재하였다.

또한 랜섬웨어 감염과 같은 침해 사고가 발생할 경우를 가정했을 때, 초기 대응 절차와 역할이 명확히 검증되지 않은 상태에서는 사고 인지와 대응이 지연되어 서비스 중단이 장기화될 수 있는 구조로 판단되었다.

백업 및 복구 체계 역시 절차는 일부 마련되어 있으나, 정기적인 복구 검증과 실효성 점검이 이루어지지 않는다면 사고 발생 시 정상적인 서비스 복구가 어려워 **업무 연속성 전반이 붕괴될 가능성**이 있었다.

4. 접근 방법 및 수행 범위(How)

이번 프로젝트는 개인정보 처리 흐름과 실제 운영 환경을 기준으로 위험을 식별하고, 이를 ISMS-P 요구사항에 따라 구조적으로 점검·개선하는 접근하였다.

우선 **개인정보 흐름도**를 기반으로 개인정보가 어디서 수집되고, 누가 접근하며, 어떤 시스템을 거쳐 처리되는지를 정리하여 시스템, 계정, 담당자 등 주요 정보자산을 식별하였다.

이후 자산·위협·취약점 관점의 위험 분석을 통해 현재 환경에서 현실적으로 발생 가능한 보안 사고 유형과 **주요 리스크**를 도출하였다.

도출된 위험 요소를 기준으로 ISMS-P 요구사항과의 **GAP 분석**을 수행하여 통제 미흡 영역과 개선이 필요한 항목을 식별하였으며, 사고 발생 가능성과 피해 확산 가능성을 고려해 개선 우선순위를 정리하였다.

마지막으로 GAP 분석 결과를 사고 시나리오와 연결하여, 실제 사고 발생 시 작동 가능한 사고 대응 체계와 이를 뒷받침하는 **보안 정책·지침·절차**를 ISMS-P 기준에 맞추어 수립하였다.

5. 정보자산 식별 & 위험분석

본 프로젝트에서는 ISMS-P 기준에 따라개인정보 흐름도 기반으로 정보자산을 식별하고, 자산·위협·취약점 관점의 위험 분석을 수행하였다.

먼저 회원, 판매자, 주문·결제 등 개인정보 처리 흐름을 기준으로 개인정보처리시스템, 관리자 계정, 업무 담당자, 외부 접속 환경 등 **개인정보에 직·간접적으로 영향을 미치는 핵심 정보자산을 식별**하였다.

이후 식별된 정보자산을 대상으로 재택근무 및 BYOD 환경, 권한 부여 방식, 사고 대응 체계 등 **운영 환경에서 발생 가능한 위협 시나리오와 관리적 취약점을 중심으로 위험을 분석**하였다.

위험 분석 주요 결과

- 재택근무·BYOD 환경에서의 계정 관리 미흡
  → 계정 탈취 시 개인정보처리시스템 접근 가능성 증가
- 접근 권한 및 직무 분리 기준 미흡
  → 내부자 권한 오남용에 의한 개인정보 무단 열람 위험
- 랜섬웨어 감염 사고를 가정한 대응 및 복구 절차의 사전 검증 부재
  → DB 암호화 등 사고 발생 시 신속한 복구가 이루어지지 않아 서비스 중단이 장기화될 가능성

분석 결과, 개별 기술적 취약점보다 **접근 통제, 권한 관리, 사고 대응과 같은 관리적·절차적 통제 미흡이 사고 발생 가능성과 피해 확산에 더 큰 영향을 미치는 핵심 요인**으로 도출되었다.

해당 결과는 이후 ISMS-P GAP 분석의 기준 자료로 활용하여 개선이 필요한 통제 영역과 우선순위를 도출하는 근거로 삼았다.

6. ISMS-P GAP 분석

ISMS-P 기준에 따라 주요 보호조치 영역을 점검한 결과, 푸드팡의 보안 관리체계는 일부 기본적인 운영은 이루어지고 있으나, **접근 통제와 권한 관리 영역을 중심으로 구조적인 통제 미흡이 확인되었다.**

특히 인증(MFA), 접근통제, 권한관리 영역에서는 정책이나 인식은 존재하지만, 실제 운영 단계에서 이를 일관되게 적용·점검하는 체계가 부족한 상태였다.

이러한 미흡 사항은 개인정보처리시스템 및 중요 정보자산에 대한 **비인가 접근 또는 권한 오남용으로 직접 이어질 수 있는 핵심 통제 영역**으로 판단하였다.

최소 권한 원칙이 명확히 적용되지 않고, 강화된 인증 수단(MFA)이 도입되어 있지 않으며, 직무 분리 기준 또한 구체화되어 있지 않은 구조에서는 **단일 통제 실패만으로도 대규모 개인정보 침해 사고로 확산될 가능성**이 높다.

이에 따라 GAP 분석에서는 해당 영역을 기술적·관리적 보호조치 전반에 영향을 미치는 **최우선 개선 과제**로 분류하였다.

반면, 로그 관리, 백업·복구, 외부 인력 관리, 사고 대응 절차 영역은 기본적인 운영은 이루어지고 있으나, 절차의 명확성, 정기 점검, 훈련 및 검증 측면에서 보완이 필요한 상태로 확인되었다.

이들 영역은 침해 사고의 **예방보다는 탐지·대응·복구 단계와 밀접하게 연계된 통제 영역**으로, 핵심 접근 통제 영역 개선 이후 **단계적으로 개선해 나가는 것이 적절하다고 판단하였다.**

7. 보안 정책 & 수립 결과

이번 프로젝트를 통해 다음과 같은 정책서 및 절차서를 산출하였다.

- 정보보호 정책서

정보보호 정책서_251229_v0.03.docx

- 침해사고 대응 절차서

침해사고대응절차서_v0.01.docx

- 백업 및 업무 연속성 관리 절차서

백업_및_연속성관리_절차서_v0.01.docx

8. 사고 대응 컨설팅

위험 분석 개요

사고 대응 컨설팅은 앞선 위험 분석 및 ISMS-P GAP 분석 결과를 바탕으로, 푸드팡 환경에서 **실제 발생 가능성이 높고 서비스 중단으로 직결될 수 있는 사고 유형**을 중심으로 진행하였다.

재택근무 및 BYOD 환경, 내부 네트워크 중심의 시스템 구성, 사고 대응 및 복구 절차의 사전 검증 부재 등을 고려할 때, 단순 개인정보 유출보다 **랜섬웨어 감염으로 인한 핵심 시스템 가용성 침해 사고가 현실적인 주요 위협**으로 판단되었다.

특히 랜섬웨어 사고는 단일 단말 감염으로 시작되더라도 내부 확산, 핵심 서버 암호화, 서비스 중단으로 빠르게 확대될 수 있어, 예방 통제 실패 시에도 탐지·대응·복구 통제가 유효하게 작동하는지 검증할 필요가 있다고 판단하였다.

위험도 산정 기준

위험도 평가는 자산의 중요도와 취약도·위협 수준을 조합하는 방식으로 산정하였다. 자산 중요도는 서비스 중단 여부, 개인정보 및 핵심 데이터의 가용성 영향을 기준으로 평가하였으며, DB 서버 및 백업 데이터와 같이 중단 시 전사적 서비스 장애로 이어질 수 있는 자산을 높은 중요도로 분류하였다.

취약도 및 위협 수준은 단말 보안 수준, 네트워크 분리 여부, 로그 및 모니터링 체계, 사고 대응 절차의 명확성 등을 기준으로 침해 발생 가능성과 피해 확산 가능성을 종합적으로 고려하였다.

위험도는 자산 중요도와 취약도를 곱하여 산정하였으며, 산정 결과는 GAP 분석 개선 우선순위 설정과 사고 시나리오 선정의 기준으로 활용하였다.

핵심 위험 Top 5

위험 분석 결과, 랜섬웨어 사고와 직접적으로 연관된 다음 위험 요소들이 핵심 위험(Top 5)으로 도출되었다.

1. 재택근무·BYOD 환경에서의 단말 보안 관리 미흡
2. 내부 네트워크 내 서버 및 시스템 간 접근 통제 미흡
3. 로그 수집 및 모니터링 체계 부재로 인한 사고 탐지 지연
4. 침해사고 발생 시 초기 대응 및 역할·절차의 불명확성
5. 백업·복구 체계의 실효성 검증 및 복구 훈련 부재

위험 처리 전략 판단

위험 분석 결과, 랜섬웨어 사고는 단일 보안 통제 실패로 발생하더라도 **탐지·대응·복구 단계의 통제가 미흡할 경우 서비스 중단이 장기화되는 구조적 위험**으로 확인되었다.

특히 DB 서버 및 서비스 운영 시스템은 가용성이 핵심인 자산으로, 랜섬웨어 감염 시 데이터 암호화로 인한 즉각적인 서비스 중단과 업무 마비로 이어질 가능성이 높다고 판단하였다.

이에 따라 랜섬웨어 관련 위험에 대해서는 위험 수용이 아닌 **위험 감소(Mitigation) 전략을 적용**하였으며, 단말 보안 강화, 네트워크 격리 절차 수립, 로그 기반 탐지 체계 강화, 침해사고 초기 대응 절차 정립, 백업·복구 검증 및 훈련을 우선 개선 과제로 도출하였다.

사고 시나리오 (랜섬웨어 감염)

내부 사용자의 업무용 단말이 악성 이메일 또는 외부 파일을 통해 랜섬웨어에 감염되고, 해당 단말을 경유하여 내부 네트워크로 악성코드가 확산되는 상황을 가정하였다.

초기 로그 모니터링 및 이상 행위 탐지가 이루어지지 않아 감염 사실을 즉시 인지하지 못하고, 그 결과 DB 서버의 데이터 파일이 암호화되어 서비스가 중단되는 사고로 확대되는 시나리오이다. 또한 사고 대응 절차와 백업·복구 체계가 사전에 충분히 검증되지 않은 경우, 서비스 복구가 지연되어 **업무 전반에 장기적인 영향을 미칠 가능성**이 존재한다고 판단하였다.

대응 범위

사고 시나리오에 대해, 랜섬웨어 감염 탐지부터 서비스 복구까지의 전 과정을 대응 범위로 설정하였다. 로그 및 모니터링을 통해 랜섬웨어 감염 및 이상 행위를 인지하고, 감염 단말 및 서버를 즉시 격리하여 추가 확산을 차단하도록 설계하였다.

이후 DB 서버 격리, 계정 차단, 사고 보고 절차를 통해 초기 대응을 수행하고, 백업 데이터를 활용한 서비스 복구를 진행한다. 사고 종료 후에는 원인 분석 결과를 바탕으로 단말 보안, 접근 통제, 사고 대응 절차 및 백업·복구 체계를 개선하여 재발 방지 대책을 수립하도록 대응 흐름을 정리하였다.

수행 역할

이번 컨설팅에서는 위험 분석 및 ISMS-P GAP 분석 결과를 기반으로 랜섬웨어 사고 시나리오를 설계하고, 해당 시나리오를 통해 기존 보안 통제의 실효성을 점검하였다.

또한 사고 탐지, 초기 대응, 확산 방지, 복구 단계별로 드러난 통제 미흡 사항을 정리하여 로그 관리, 사고 대응 절차, 백업·업무 연속성 관리 측면의 개선 과제를 도출하였으며, **실제 사고 발생 시 조직이 대응 가능한 수준의 사고 대응 체계로 고도화하는 방향을 제시하였다.**

9. 본인 기여도

프로젝트 초기 단계부터 서비스 환경을 기준으로 개인정보 처리 흐름과 핵심 정보자산 구조를 분석하여, 이후 위험 분석 및 ISMS-P GAP 분석의 기준이 되는 기초 자료 도출에 참여하였다.

정책·지침·절차 수립 단계에서는 사고 대응과 업무 연속성 관점에서 내용을 검토하였으며,

침해사고 대응 절차서와 백업 및 복구 절차서를 직접 작성하여 사고 발생 시 대응 흐름과 복구 절차가 문서로 명확히 정리되도록 구성하였다.

특히 백업 주기, 백업 대상 자산, 복구 절차, 복구 검증 항목을 중심으로

사고 발생 후 서비스가 어떻게 복구되는지 한 흐름으로 이해할 수 있도록 정리하였다.

위험 분석 및 사고 대응 컨설팅 영역에서는 위험분석 보고서를 팀원과 공동으로 작성하였으며, 그중 랜섬웨어 사고 시나리오를 직접 설계하였다.

내부 사용자 단말 감염을 시작으로 내부 네트워크 확산, DB 서버 암호화, 서비스 중단으로 이어지는 사고 흐름을 설정하고,

백업·복구 체계가 미흡할 경우 서비스 중단이 장기화될 수 있는 구조적 위험을 중심으로 분석하였다.

이를 통해 위험 분석 결과, ISMS-P GAP 분석, 사고 대응 절차, 백업·복구 절차가 각각 분리되지 않고

사고 발생 → 대응 → 복구 → 재발 방지 로 이어지는 하나의 흐름으로 정리되도록 기여하였다.

10. 결론 및 느낀점

이번 프로젝트를 통해 정보보안 관리체계는 단순히 보안 솔루션을 적용하거나 문서를 만드는 것이 아니라, 실제 서비스 환경과 운영 방식에 맞게 설계되어야 의미가 있다는 점을 배울 수 있었다.

ISMS-P 기준을 바탕으로 개인정보 흐름 분석, 위험 분석, GAP 분석을 수행하면서, 각 통제가 단독으로 존재하는 것이 아니라 서로 연결되어 하나의 보안 흐름을 만든다는 점을 이해하게 되었다.

특히 통제가 미흡한 부분이 사고 발생 시 어떤 단계에서 문제로 이어질 수 있는지를 사고 시나리오를 통해 구체적으로 확인할 수 있었다.

랜섬웨어 사고 시나리오와 백업·복구 절차를 정리하는 과정에서는, 사고 자체보다도 사고 이후 대응과 복구 준비가 얼마나 중요한지를 체감하였다.

또한 백업이 마련되어 있더라도, 절차와 역할이 명확하게 정리되어 있어야 사고 발생 시 효과적으로 활용될 수 있다는 점을 이해하게 되었다.

이번 프로젝트를 통해 정보보안 업무는 단순한 점검이나 규정 확인이 아니라, 사고를 미리 가정하고 운영 관점에서 위험을 줄이는 역할이라는 인식을 갖게 되었다.

앞으로는 실무 경험을 통해 보안 정책과 기술에 대한 이해를 더 넓히고, 조직과 서비스 환경에 맞는 보안 체계를 고민할 수 있는 보안 인력으로 성장하고자 한다.