**3장 통합 구현**

056 통합 구현

- 사용자의 요구사항에 맞춰 송,수신 모듈과 중계 모듈 간의 연계를 구현하는 것

통합 구현의 구성 요소

송신 시스템과 모듈 / 수신 시스템과 모듈 / 중계 시스템 / 연계 데이터 / 네트워크

연계 요구사항 분석

- 통합 구현을 위해 사용자 요구사항을 분석하여 연계데이터를 식별 및 표준화하여 연계 데이터를 정의하는 것

분석 절차

1. 하드웨어 및 소프트웨어 구성, 네트워크 현황 확인

2. 테이블 정의서, 코드 정의서 등의 문서 확인

3. 체크리스트 작성

4. 관련 문서 공유 및 인터뷰, 설문조사 실시

5. 요구사항 정의서 작성

연계 데이터 식별 및 표준화 절차

연계 범위 및 항목 정의 -> 연계 코드 변환 및 매핑 -> 연계 데이터 식별자와 변경 구분 추가

-> 연계 데이터 표현 방법 정의 -> 연계 정의서 및 명세서 작성

057 연계 메커니즘

- 데이터 생성 및 전송을 담당하는 송신 시스템과 데이터 수신 및 운영 DB 반영을 담당하는 수신 시스템으로 구성됨

연게 방식 – 직접 연계 방식 / 간점 연계 방식

송신 시스템 및 송신 모듈

연계 데이터 생성 및 추출 -> 코드 매핑 및 데이터 변환 -> 인터페이스 테이블 또는 파일 생성 -> 연계 서버 또는 송신 어댑터 -> (수신 시스템 및 수신 모듈) -> 연계 서버 또는 수신 어댑터 -> 인터페이스 테이블 또는 파일 생성 -> 코드 매핑 및 데이터 변환 -> 운영 DB에 연계 데이터 반영

연계 메커니즘의 구성

연계 데이터 생성 및 추출 / 코드 매핑 및 데이터 변환 / 인터페이스 테이블 또는 파일 생성 / 로그 기록 / 연계 서버 또는 송수신 어댑터 / 전송 / 운영 DB에 연계 데이터 반영

058 연계 장애 및 오류처리 구현

연계 매커니즘 구간별 장애 및 오류 모니터링 현황

- 연계 메커니즘에서 오류 발생시점, 오류 로그 기록 장소, 오류 로그 기록 주체는 송수신 시스템, 연계 서버 구간으로 구분됨

장애 및 오류 유형과 처리 방안

- 장애 및 오류 유형의 분류

-> 송수신 시스템의 연계 프로그램 오류

-> 연계 서버의 오류

-> 연계 데이터의 오류

장애 및 오류의 정의와 설계

- 장애 및 오류 관리 대상 / 관리 대상의 장애 및 오류 코드와 메시지 / 장애 및 오류 코드와 메시지 관리 방식 / 장애 및 오류 기록 방식

059 연계 데이터 보안 적용

연계 데이터 보안 – 송신 시스템에서 수신 시스템으로 전송되는 연계 데이터는 보안에 취약할 수 있으므로 데이터의 중요성을 고려하여 보안을 적용해야 함

전송 구간 보안 – 전송되는 데이터나 패킷을 쉽게 가로챌 수 없도록 암호화 기능이 포함된 프로토콜을 사용

데이터 보안 – 송신 시스템에서 연계 데이터를 추출할 때와 수신 시스템에서 데이터를 운영 DB에 반영할 때 데이터를 암호화, 복호화 하는 것이다.

송신 시스템

1. DB에서 연계 데이터 추출

2. 보안 적용 대상 컬럼을 암호화

3. 연계 데이터를 인터페이스 테이블 또는 파일에 등록 및 송신

수신 시스템

1. 수신된 데이터 중 암호화된 컬럼을 복호화

2. 운영 DB에 반영

암호화 복호화 적용 절차

암호화 적용 대상, 암호화 알고리즘, 암호화 키 선정 -> 암호화 적용 대상 컬럼의 데이터 길이 변경 -> 암호화 알고리즘 라이브러리 확보 및 설치 -> 연계 응용 프로그램에서 암호화, 복호화 처리 수행