

주요금융업무 및 비주요금융업무의 식별에 따른 Infra, 개발 Process, 사내망 분리 운영 개선안 도출

Last updated by | Rex(정기주) | 2021년 2월 9일 at 오후 2:32 GMT+9

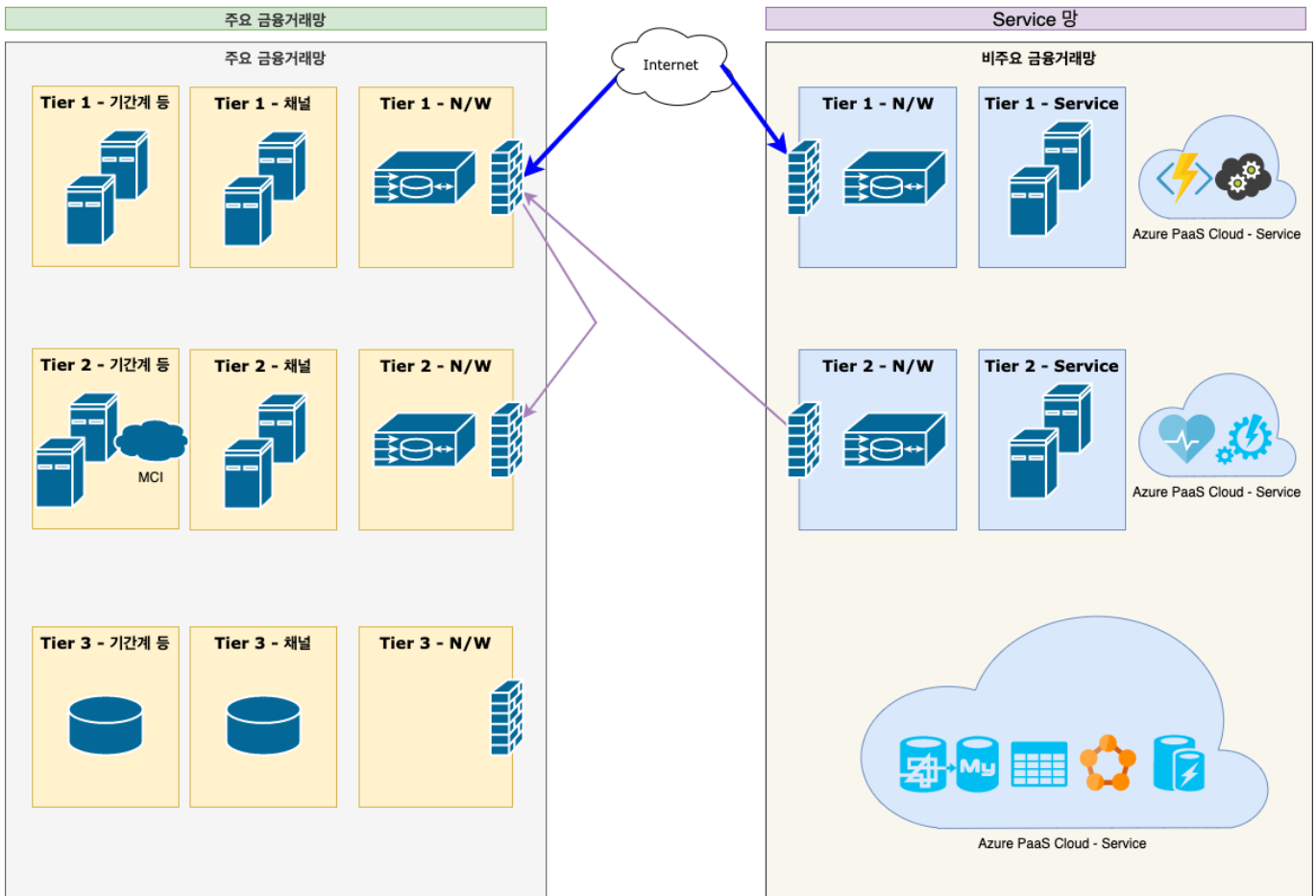
목표

- 주요금융업무를 명확히 식별하고, 비주요금융업무 와 구분하여 Infra / 개발 Process / 사내 업무 망을 분리 구축

캐롯의 주요 금융 업무의 식별

- 전자금융업무
 - 보험상품의 취급과 관련하여 발생하는 보험의 인수(引受), 보험료 수수 및 보험금 지급 등
- 미적용대상 검토 - 전자금융거래법의 적용범위
 - 법 제3조 및 시행령 제5조를 통해 결제중계시스템을 이용하는 전자금융거래는 미적용 가능.
 - 그 외 미적용 대상은 제외됨.
- 주요금융업과 일반 업무의 분리 근거
 - 전자금융감독규정 제12조(단말기 보호대책)의 3.에 따르면 그룹웨어 등은 주요 단말망과 분리해야함 -> 일반 업무와 주요 금융 업무의 분리를 명시
 - 3. 외부 반출, 인터넷 접속, 그룹웨어 접속의 금지 등 강화된 보호대책이 적용되는 중요단말기를 지정할 것
 - 제15조 1항 3에서 내부 업무용시스템의 외부통신망과 분리차단을 명시
 - 제29조(프로그램 통제)
 - 4. 변경 필요시 해당 프로그램을 개발 또는 테스트 시스템으로 복사 후 수정할 것
 - 금융분야 마이데이터 기술 가이드라인_의견조회용 의 Q&A 5.정보보호시설/보안의 Q3에 따르면 해당 업무에 대해서만 해당하는 것으로 협의의 업무 범위를 제시
 - Q3. 망분리의 범위는 어디까지인지?
 - 개인신용정보를 처리하는 서버, 서버에 접속하는 주요단말, 개인신용정보 관련 업무를 담당하는 담당자의 PC가 망분리 요건에 해당합니다.

Infra

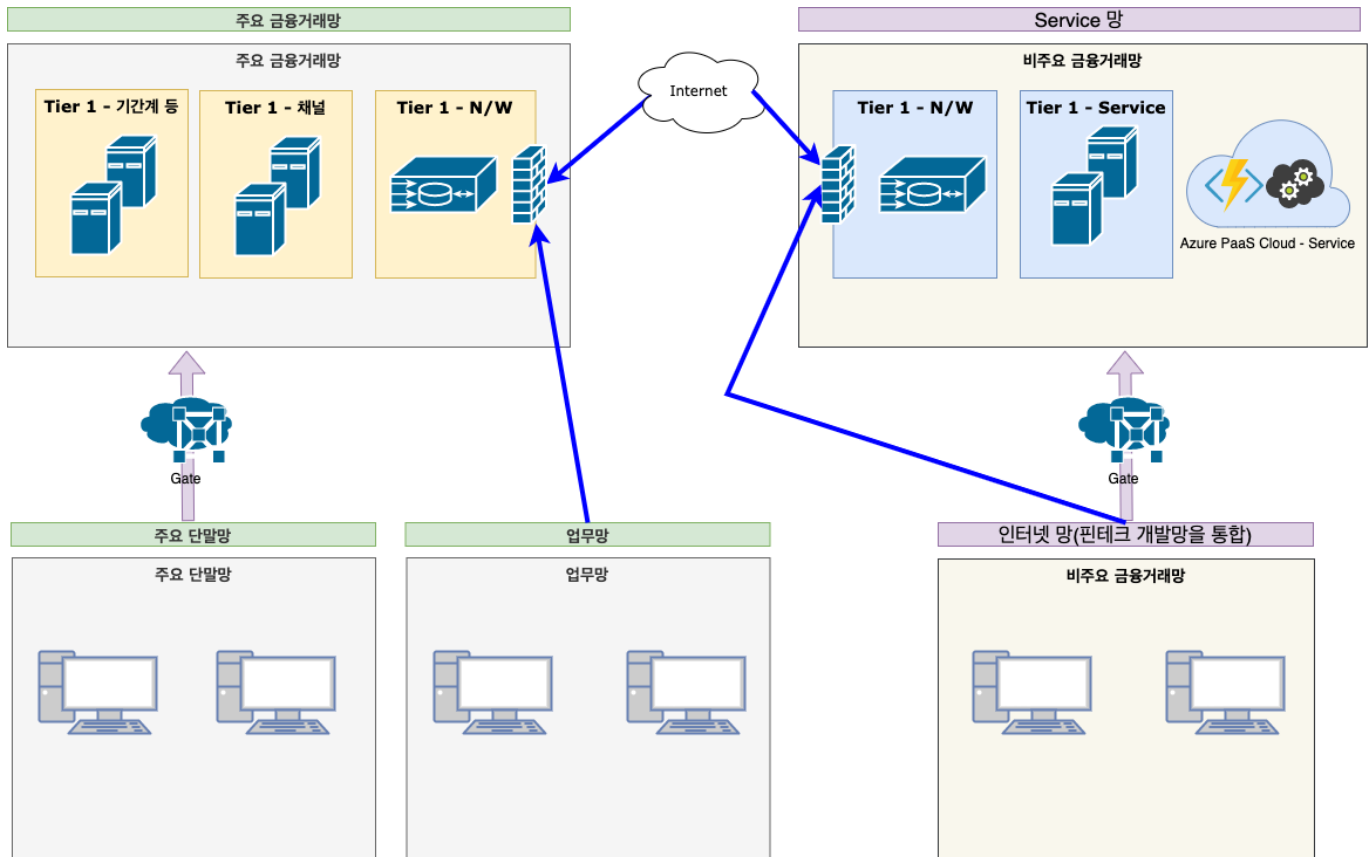


- 주요금융거래망의 경우 보험의 인수(引受), 보험료 수수 및 보험금 지급 등의 업무에 해당되는 경우가 대상이며,
- 그 외의 업무는 비주요금융거래업무 - 서비스망에 인프라를 구성한다.
- 주요금융거래망의 경우 전자금융감독규정에 명시된 규정을 준수하나,
- 서비스망의 경우 개인정보보호법령 및 사내 정보보호규정 을 준수하되, IT 인프라 구성을 자유도를 부여한다.

개발 Process

- 주요금융업무의 경우 전자금융거래법 및 전자금융감독규정에 명시된 요청 / 변경 / 배포 등의 내역을 엄격히 관리하되,
- 비주요금융업무의 경우 요청 / 변경 / 배포 등에 대한 내용을 Jira / Jenkins 등의 도구를 통해 관리한다.
 - 두 경우의 가장 큰 차이는 내용에 대한 감사 기능의 포함 여부임.

사내 업무망



- 주요 단말망의 경우 주요금융거래망의 서버 접속만 허용
- 업무망의 경우 주요금융거래망의 내부 시스템을 접속하는 업무에 한해 운용한다.
 - 일반적인 사내 업무의 경우 인터넷망으로 이전.
- 현행의 인터넷망과 핀테크개발망을 하나로 통합
 - 비주요 금융거래업무에서 소요되는 내부 전산 자원은 서비스망에 두고 인터넷망에서의 접속을 허용한다.
 - 기존 핀테크개발망과 같이 비주요금융거래업무 - 서비스 개발, 운영, 배포에 필요한 망 연결은 게이트웨이 서버를 통해 서비스망 서버에 직접 연결을 허용한다,
 - 주요금융거래업무라 하더라도 아래에 따라 접속 허용 가능
 - 제2조의2 (망분리 적용 예외) 1항
 - 2. 규정 제12조의 보안대책을 적용한 단말기에서 전용회선과 동등한 보안수준을 갖춘 통신망을 이용하여 외부망으로부터 내부 업무용시스템으로 원격접속 하는 경우
 - 제2조의2 (망분리 적용 예외) 2항

- - 2. 업무상 외부통신망과 연결이 불가피한 다음의 정보처리시스템(다만, 필요한 서비스번호(port)에 한하여 연결할 수 있다)
 - 가. 전자금융업무의 처리를 위하여 특정 외부기관과 데이터를 송수신하는 정보처리시스템
 - 나. DMZ구간 내 정보처리시스템과 실시간으로 데이터를 송수신하는 내부통신망의 정보처리시스템
- - 3. 규정 제23조의 비상대책에 따라 원격 접속이 필요한 경우
 - 3항 제1항 및 제2항의 규정은 금융회사 또는 전자금융업자가 자체 위험성 평가를 실시한 후 <별표 7>에서 정한 망분리 대체 정보보호통제를 적용하고 정보보호위원회가 승인한 경우에 한하여 적용한다.

• 법령 링크

- [전자금융거래법](#)
- [전자금융거래법 시행령](#)
- [전자금융감독규정](#)
- [전자금융감독규정시행세칙](#)