OAtuh 인증



심준형대리
ndjun@cnthoth.com

CNThoth
IT Solution & Service

Agenda

I. OAuth란?

II. 기본용어

III. OAuth 사용 기업

IV. OAuth와 로그인의 차이

V. OAuth 인증 과정

VI. OAuth 2.0

VII. OAuth 구현 과정

VIII. OAuth로 인한 인터넷 서비스 변화

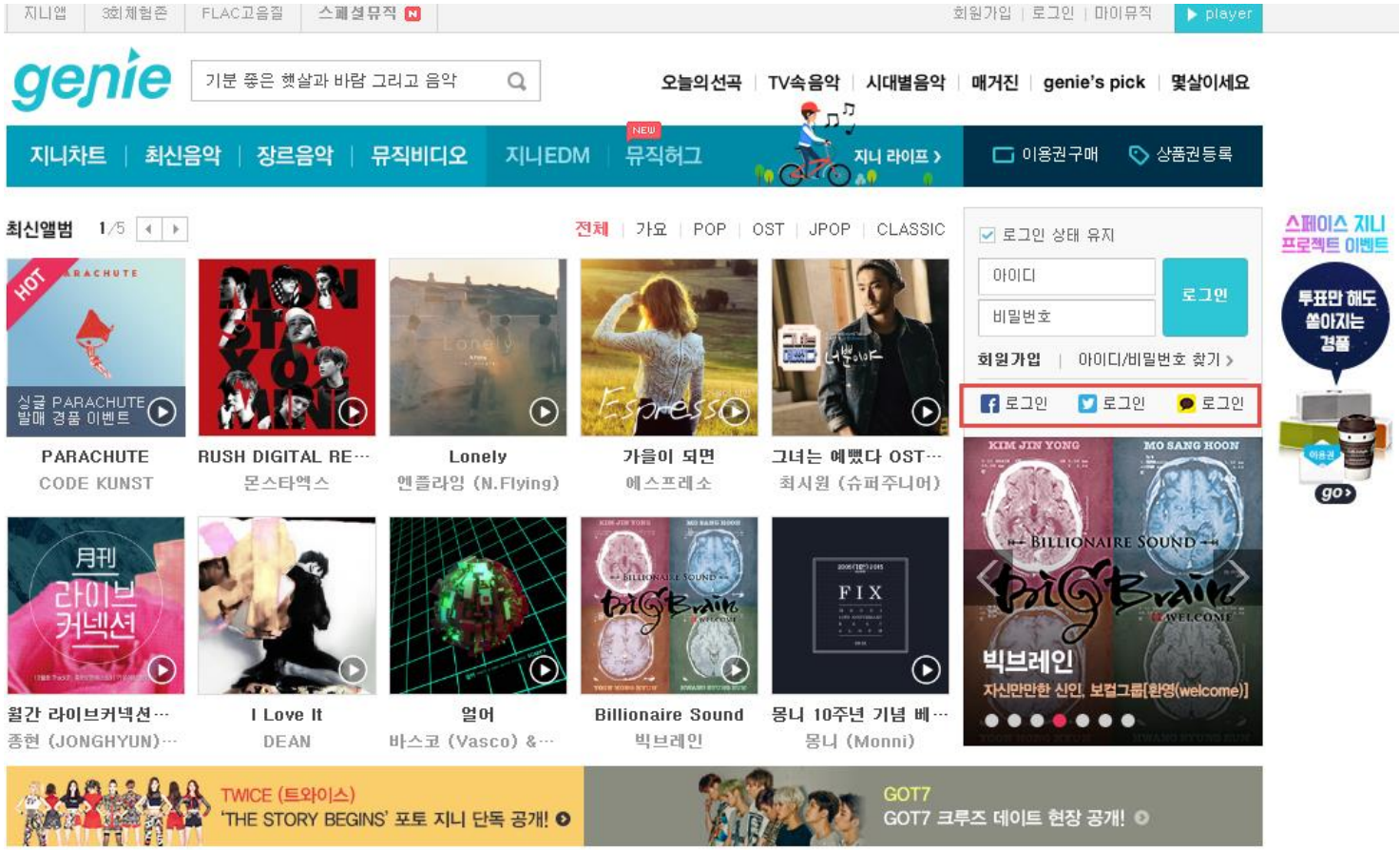


1. OAuth란?

❖ OAuth는 인증을 위한 Open Standard Protocol로, 사용자가 Facebook이나 트위터 같은 인터넷 서비스의 기능을 다른 애플리케이션(데스크톱, 웹, 모바일 등)에서도 사용할 수 있게 한 것

❖ OAuth가 사용되기 전에는 인증방식의 표준이 없었기 때문에 기존의 기본인증인 아이디와 비밀번호를 사용

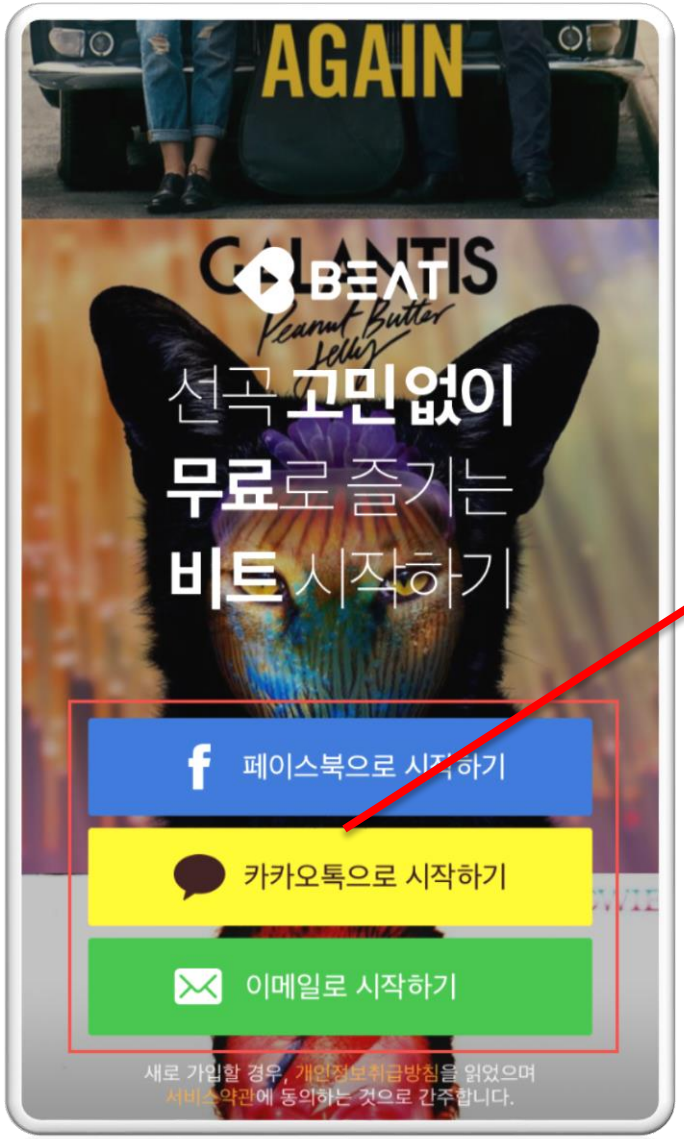
❖ Oauth는 3rd party(외부 서비스)를 위한 범용적인 인증 표준

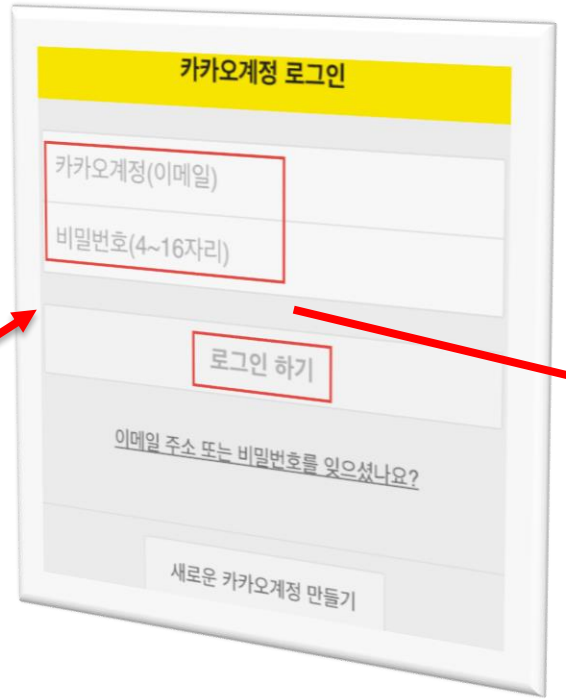


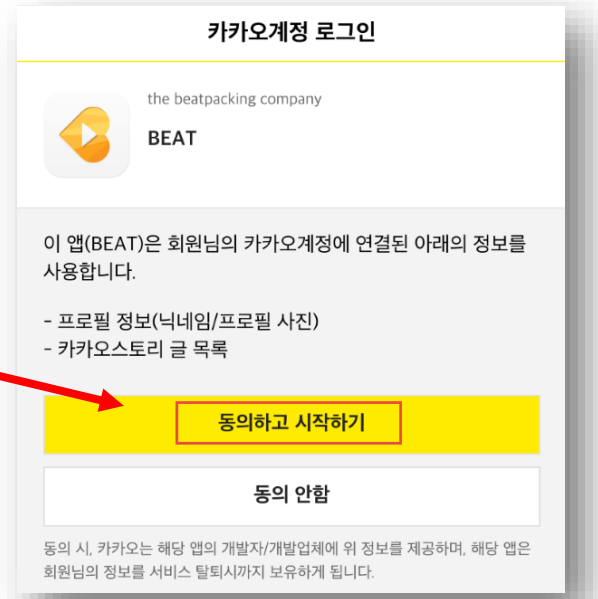


1. OAuth란?

❖ BEAT







1. OAuth란?

❖ 외부 사이트와 인증기반의 데이터를 연동할 때 ID, Password를 넘기는 방법은 매우 위험, 보안에 취약

ID, Password는 그 사용자의 모든 권한을 얻는 것이기 때문에 ID 도용 위험이 높음

❖ Oauth는 사용자 임시 인증을 위한 Token을 제공하는 방식을 사용 하는데

이 방법은 각 서비스마다 제 각각이어서 개발자들은 인증 연동을 각 서비스 별로 따로 해야 함

❖ 그러다 보니 표준적인 방법이 필요했고, 그 표준 방법이 OAuth



- 2007년 10월 : OAuth 1.0 발표
- 2008년 6월: OAuth 1.0a (1.0의 보안 문제를 해결한 수정 버전)
- 2010년 4월 : OAuth 1.0a가 IETF 표준으로 등록
  - RFC5849 – The OAuth 1.0 Protocol
- 2012년 3월: OAuth 2.0 draft 배포
- 2012년 10월: OAuth 2.0이 IETF 표준으로 등록
  - RFC6749 – The OAuth 2.0 Authorization Framework
  - RFC6750 – Bearer Token 사용

2. 기본 용어

❖ **Service Provider**
API를 제공하는 서비스
OAuth 인증을 지원하는 네이버등이 각 서비스들의 Provider에 해당

❖ **User**
서비스 Provider에 계정을 가지고 있는 서비스 사용자
통상적으로 네이버등의 계정을 가지고 있는 일반 사용자를 지칭

❖ **Consumer**
OAuth 인증을 사용하여 사용자 대신에 서비스 Provider에 접근을 하려고 하는 어플리케이션이나 웹 서비스를 지칭 함
네이버 API등을 사용하여 서비스에 접근하려고 하는 서드파티의 어플리케이션이나 웹 서비스를 말함

❖ **Service**
OAuth 인증을 통해 사용자 데이터 등을
제공하는 서비스를 뜻함



3. OAuth 사용 기업

인터넷 서비스 기업	OAuth 버전
Facebook	2.0
Foursquare	2.0
Google	2.0
Microsoft (Hotmail, Messenger, Xbox)	2.0
LinkedIn	2.0
Daum(티스토리	2.0
NHN (오픈API)	1.0a
Daum(요즘, 오픈API)	1.0a
MySpace	1.0a
Netflix	1.0a
트위터	1.0a
Vimeo	1.0a
Yahoo!	1.0a



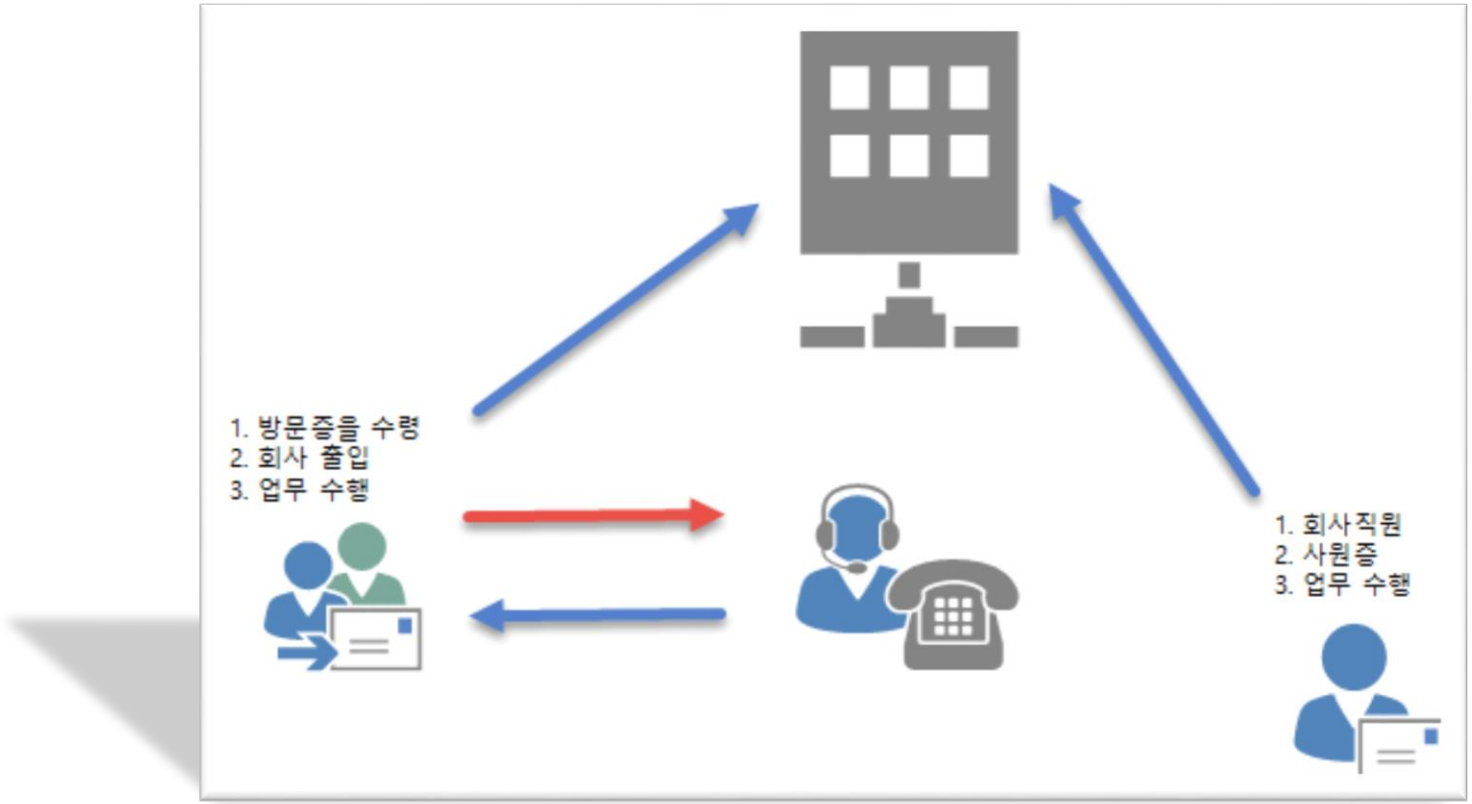
4. OAuth 와 로그인의 차이

❖ OAuth와 로그인 은 반드시 분리해서 이해해야 함.

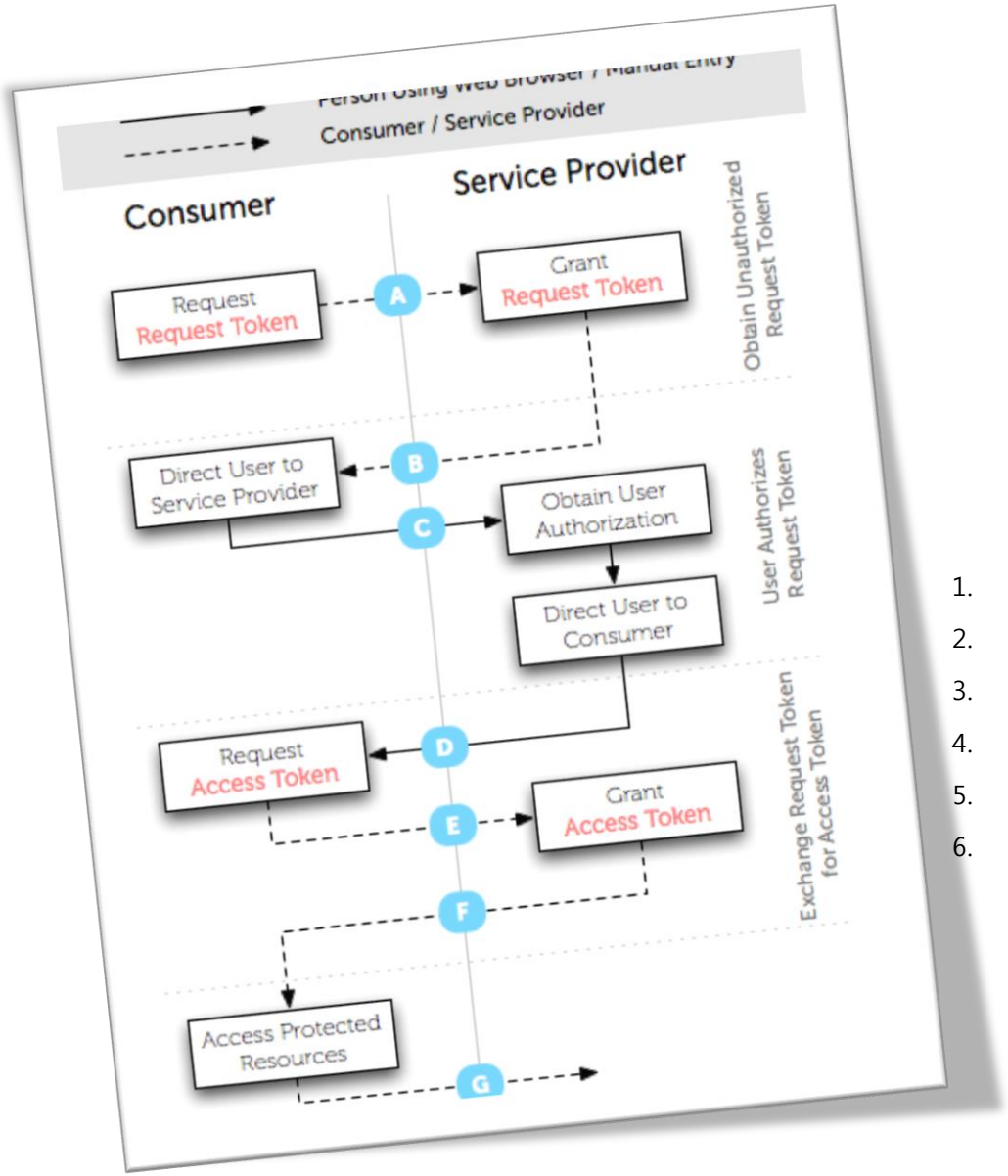
❖ 일상 생활을 예로 들어 OAuth와 로그인의 차이

- 사원증 을 이용해 출입할 수 있는 회사가 있고, 외부 손님이 그 회사에 방문할 일이 있을 때

회사 사원이 건물에 출입하는 것이 로그인 이라면 OAuth는 방문증 을 수령한 후 회사에 출입하는 것에 비유 할수 있다.



5. OAuth 인증 과정



회사 방문 과정과 OAuth 인증 과정

	회사 방문 과정	OAuth 인증 과정
1.	**방문자 A** 가 안내 데스크에서 업무적인 목적으로 **고객사B**를 만나러 왔다고 말한다.	Request Token의 요청과 발급
2.	안내 데스크에서는 **고객사B**에게 **방문자A**가 방문했다고 연락한다.	사용자 인증 페이지 호출
3.	**고객사B**가 안내 데스크로 찾아와 **방문자A**의 신원을 확인해 준다.	사용자 로그인 완료
4.	**고객사B**는 업무 목적과 인적 사항을 안내 데스크에서 기록한다.	사용자의 권한 요청 및 수락
5.	안내 데스크에서 **방문자A** 에게 방문증을 발급해 준다.	Access Token 발급
6.	**고객사B**와 **방문자A**는 정해진 장소로 이동해 업무를 진행한다.	Access Token을 이용해 서비스 정보 요청

6. OAuth 2.0

❖ OAuth 1.0은 웹 애플리케이션이 아닌 애플리케이션에서는 사용하기 곤란하다는 단점
❖ 절차가 복잡하여 OAuth 구현 라이브러리를 제작하기 어려움
❖ 복잡한 절차 때문에 Service Provider에게도 연산 부담이 발생

❖ OAuth 2.0 은 이러한 단점을 개선

- 웹 애플리케이션이 아닌 애플리케이션 지원 강화
- 암호화가 필요 없으며, HTTPS를 사용, HMAC을 사용하지 않음
- Signature 단순화 정렬과 URL 인코딩이 필요 없음
- **Access Token 갱신 - OAuth1.0에서 Access Token을 받으면 Access Token 을 계속 사용 가능**
  일례로 트위터 의 경우 Access Token을 만료시키지 않음
- **OAuth 2.0 에서는 보안 강화를 위해 Access Token의 Life-time을 지정할 수 있음**
- 이외에도 OAuth 2.0에서 사용하는 용어 체계는 OAuth 1.0과는 전혀 다르나 같은 목적의 프로토콜

구분	OAuth 1.0	OAuth 2.0
지원 범위	웹 애플리케이션에 초점	다양한 애플리케이션 지원
요청방식	토큰 요청 시 암호화된 서명 사용	서명 없이 HTTPS로 요청 가능
토큰 유효기간	**Access Token 의 유효기간 없음**	**Access Token의 유효기간 설정 가능**

❖ 참고자료

- http://www.joinc.co.kr/modules/moniwiki/wiki.php/man/12/oAuth2/Google

2.6 인증 UI 프로세스

Google OAuth를 이용한 인증 프로세스를 그려보자. 대략 다음과 같을 것이다.



1. 대부분의 서비스들이 비슷한 유형의 로그인 인터페이스를 제공할 거다. 한쪽 구석에 서비스가 지원하는 인증수단 목록들이 있고, 다른 한쪽 구석에 서비스 회원가입을 위한 인터페이스가 있다.
2. "Sign in with Google" 을 클릭하면, 두 개의 흐름으로 분기된다.
    1. 구글 로그인을 하지 않았을 경우, Google sign in 페이지로 리다이렉트 한다.
    2. 이미 구글 로그인을 했다면, "서비스 허가" 페이지로 리다이렉트 된다.
3. 서비스 허가 페이지로 넘어간다. 유저는 서비스를 위해서 인증정보와 함께, (이메일이나 프로파일 혹은 유저의 동영상 등)자원의 사용을 허가할지를 판단한다.
4. 사용을 허락하면, 다시 mytest 사이트로 리다이렉트 된다. 이때 인증과 허가가 끝났다는 정보를 담고 있는 토큰을 함께 넘기는데, mytest는 이 토큰을 이용해서 구글로 부터 인증된 유저인지 확인하고, 원하는 정보를 가져올 수 있다.

8. OAuth 로 인한 인터넷 서비스의 변화

OAuth는 요즘의 인터넷 생태계의 주요 요소로 자리매김하고 있으며,

신생 업체들은 고유의 인증 방식을 사용하기 보다는 Facebook이나 트위터 의 인증을 이용

개발 비용과 운영 비용을 줄이는 효과도 있지만 Facebook이나 트위터 를 통해 서비스를 홍보하는 효과

Service Provider 입장에서는 핵심 기능을 더욱 공고히 하는 효과

표준 인증 방법 하나가 인터넷 업계에 변화를 주고 있다.



감사합니다

씨앤토트
IT Solution & Service