Cookie和session由于实现手段不同，因此也各有优缺点和各自的应用场景：

1. 应用场景

Cookie的典型应用场景是Remember Me服务，即用户的账户信息通过cookie的形式保存在客户端，当用户再次请求匹配的URL的时候，账户信息会被传送到服务端，交由相应的程序完成自动登录等功能。当然也可以保存一些客户端信息，比如页面布局以及搜索历史等等。

Session的典型应用场景是用户登录某网站之后，将其登录信息放入session，在以后的每次请求中查询相应的登录信息以确保该用户合法。当然还是有购物车等等经典场景；

2. 安全性

cookie将信息保存在客户端，如果不进行加密的话，无疑会暴露一些隐私信息，安全性很差，一般情况下敏感信息是经过加密后存储在cookie中，但很容易就会被窃取。而session只会将信息存储在服务端，如果存储在文件或数据库中，也有被窃取的可能，只是可能性比cookie小了太多。

Session安全性方面比较突出的是存在会话劫持的问题，这是一种安全威胁，这在下文会进行更详细的说明。总体来讲，session的安全性要高于cookie；

3. 性能

Cookie存储在客户端，消耗的是客户端的I/O和内存，而session存储在服务端，消耗的是服务端的资源。但是session对服务器造成的压力比较集中，而cookie很好地分散了资源消耗，就这点来说，cookie是要优于session的；

4. 时效性

Cookie可以通过设置有效期使其较长时间内存在于客户端，而session一般只有比较短的有效期（用户主动销毁session或关闭浏览器后引发超时）；

5. 其他

Cookie的处理在开发中没有session方便。而且cookie在客户端是有数量和大小的限制的，而session的大小却只以硬件为限制，能存储的数据无疑大了太多。

http://www.cnblogs.com/chenchenluo/p/4197181.html