

양자통신 환경 상에서의 가용성 침해 공격

한성대학교 IT융합공학부
권혁동 김현준 김경호 서화정

Contents

1. 보안의 3요소

2. 양자

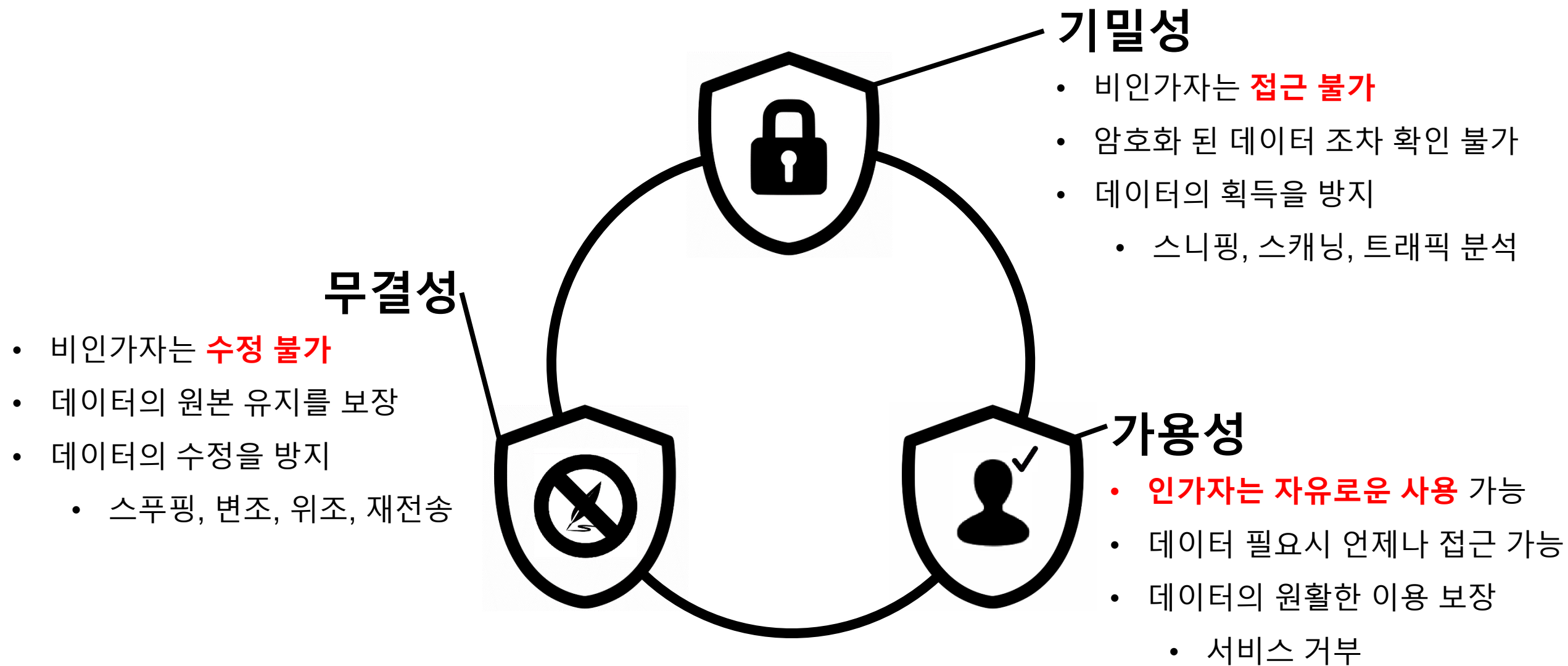
3. 양자통신

4. 스니핑 공격의 재분류

5. 결론

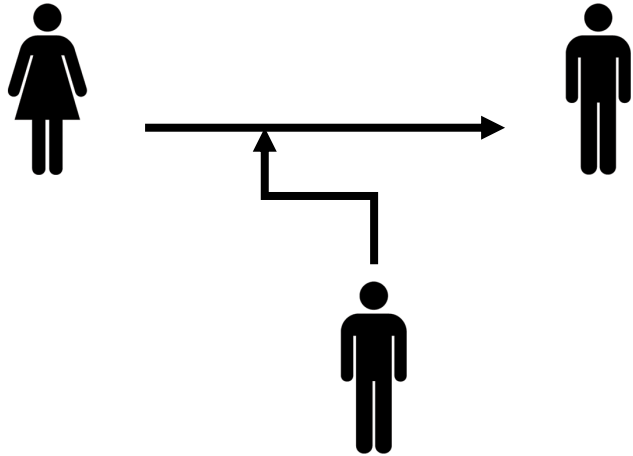


1. 보안의 3요소



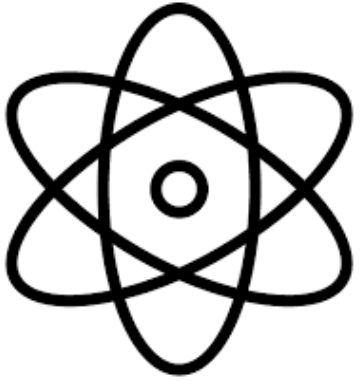
1. 보안의 3요소

스니핑(Sniffing)



- 네트워크 상에 흐르는 **패킷을 감청**하는 행위
- 인가되지 않은 **제 3자가** 데이터, 패킷에 **접근**
 - 기밀성 침해 공격으로 분류
- 데이터의 의미 파악과는 상관 없이 공격으로 간주

2. 양자

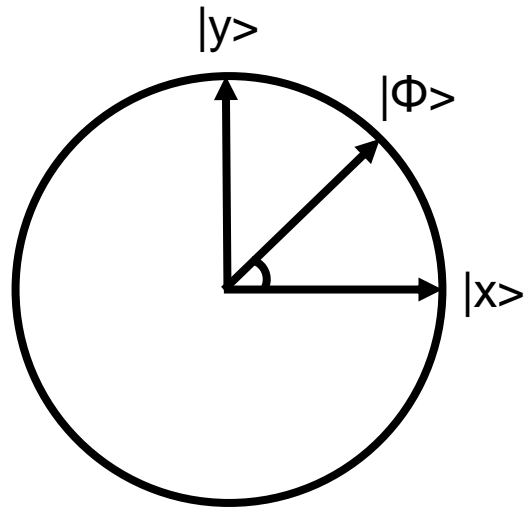


양자(Quantum)

- 막스 플랑크가 흑체 복사와 관련된 문제를 연구하던 도중 제시
- **에너지의 기초 단위**
- 양자 고유의 성질을 지님
 - 양자중첩(Quantum Superposition)
 - 양자얽힘(Quantum Entanglement)
 - 양자붕괴(Quantum Collapse)

2. 양자

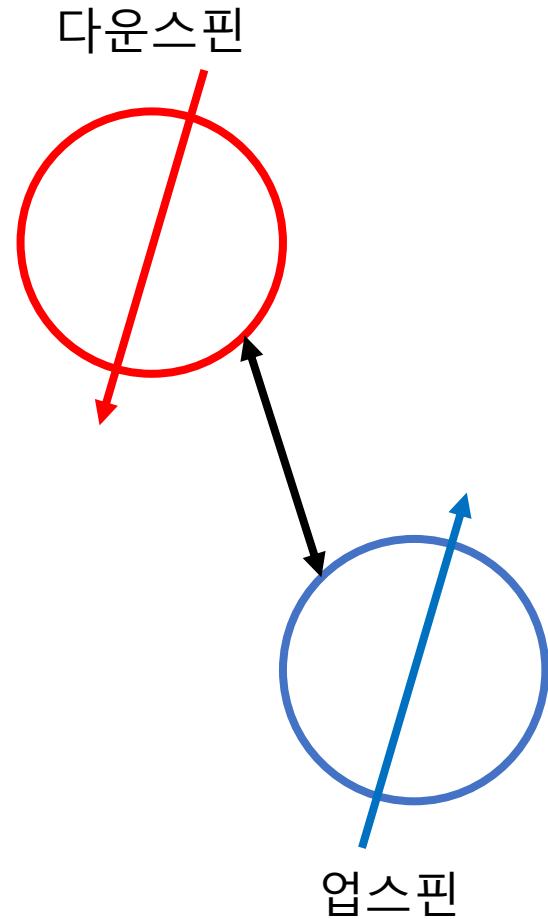
양자중첩(Quantum Superposition)



$$|\Phi\rangle = \alpha |x\rangle + \beta |y\rangle$$

- 양자를 **측정**하기 **전**까지는 어떤 **값**을 가지는지 **알 수 없음**
 - 스칼라 곱을 갖춘 2차원 공간 상의 벡터
 - 기저벡터 요소: $|x\rangle$, $|y\rangle$
 - $|\alpha|^2 + |\beta|^2 = 1$ (α , β 는 복소수)
 - 측정 시 $|\alpha|^2$ 확률로 $|x\rangle$, $|\beta|^2$ 확률로 $|y\rangle$ 획득
- 원자 수준의 대상에만 적용

2. 양자

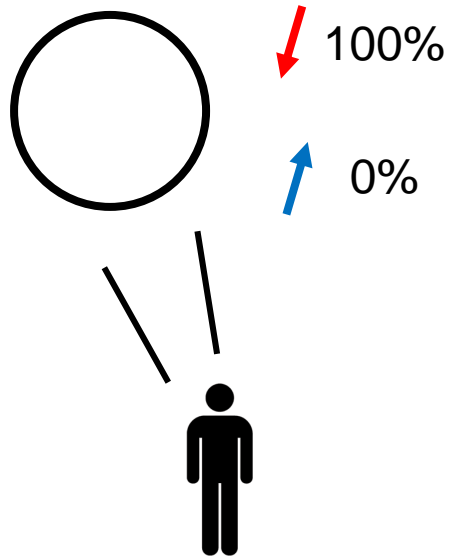


양자얽힘(Quantum Entanglement)

- 측정하기 전 까지 상태를 알 수 없는 입자의 쌍이 존재
- 이때 **입자 하나를 측정**하는 순간 해당 입자의 상태가 결정
- 동시에 그 입자와 얽힌 **다른 입자의 상태까지 결정**
- 정보가 순식간에 전달되는 것과 같이 보임
 - 국소성의 원리 위배: 멀리 떨어진 두 물체는 서로 영향을 줄 수 없음

2. 양자

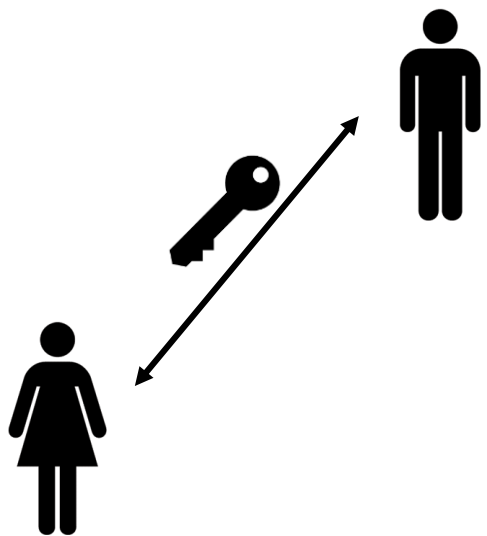
양자붕괴(Quantum Collapse)



- 파동함수의 붕괴
- 확률이 매끄러운 형태를 가지다 **관측하는 순간 확률이 확정**
 - 관측한 지점에서 무한대, 그 외의 지점에서 0
 - 디랙-델타 함수, 확률을 계산할 때는 함수를 제공하고 적분
- 관측 지점에서 100% 확률, 그 외의 지점에서 0% 확률이 됨

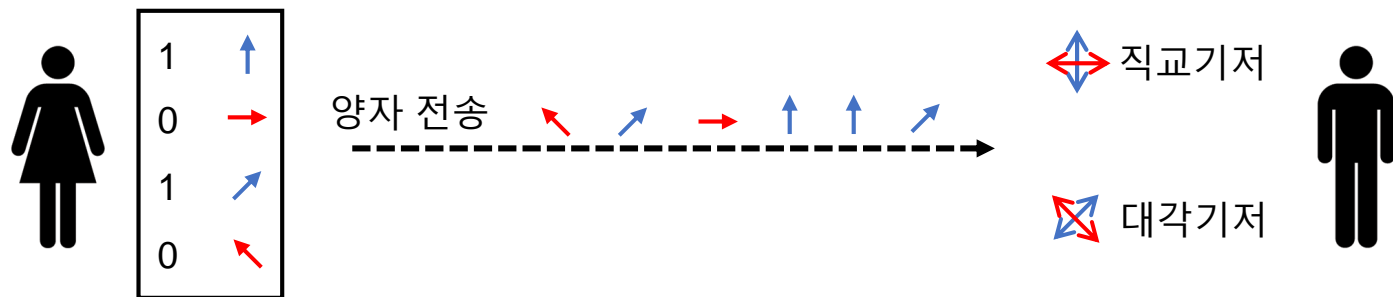
3. 양자통신

























BB84 프로토콜



- 1984년 찰스 H. 베넷과 질 브라사드가 제안
- 송신자와 수신자간 OTP(One Time Pad)를 생성
- 양자 **키 분배 프로토콜**
- 양자채널과 고전채널을 복합적으로 사용

3. 양자통신



전송 양자								
전송 비트	0	1	0	1	1	1	0	1
수신 양자								
측정 비트	1	1	0	1	1	1	0	0
측정 기저 교환								
동일 기저 확인		○		○		○	○	
도출된 시프트 키		1		1		1	0	

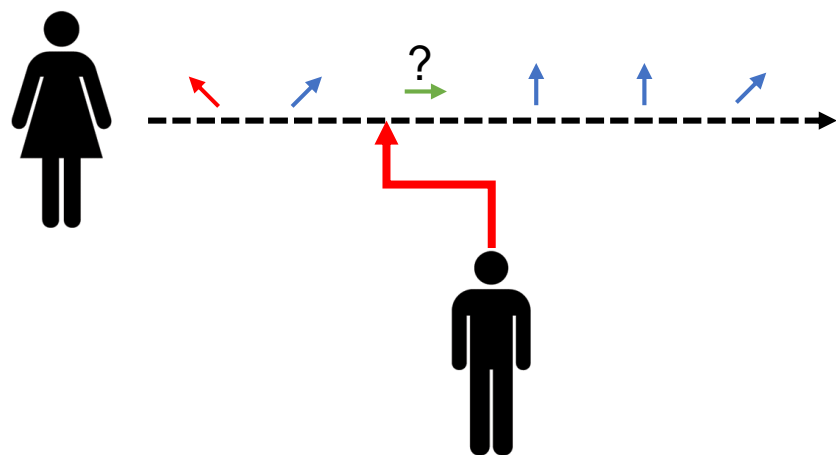
1. 양자에 값을 인코딩하여 전송
2. 수신자는 임의의 기저로 측정
3. 서로 사용한 기저 정보를 교환
4. 동일 기저에 대한 값을 남김
5. 4의 값을 시프트 키(shifted key)로 사용

* 1,2단계: 양자채널

* 3,4단계: 고전채널

3. 양자통신

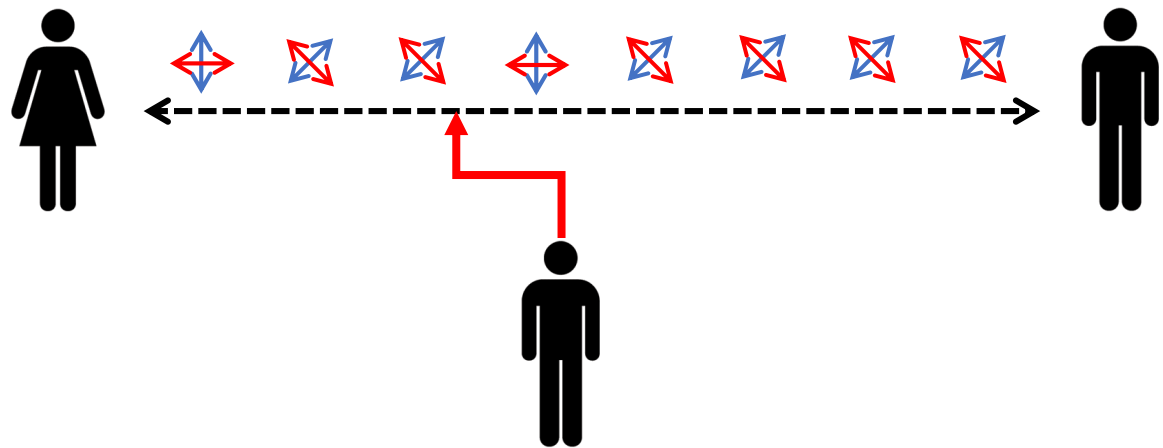
양자통신의 보호 기법



- **양자붕괴** 현상을 응용함
- 송수신 측은 양자 비트 에러율을 점검
 - Quantum Bit Error Ratio, QBER
- QBER가 급격히 상승할 경우 공격 상황으로 판단
- 공격자는 고전채널, 양자채널 선택이 가능

4. 스니핑 공격의 재분류

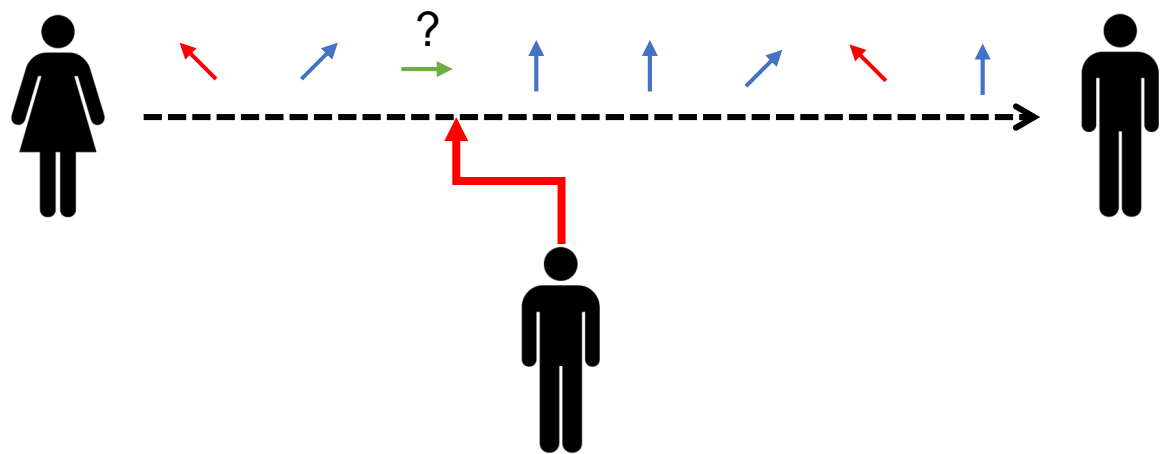
고전채널 공격 시



- 고전채널 상에서는 기저 정보를 교환
- 기저 정보는 측정 값과는 무관한 정보
- **의미 있는 값을 확보하기 어려움**

4. 스니핑 공격의 재분류

양자채널 공격 시



- 송신자가 수신자에 양자 정보를 전송
- 공격자가 측정하는 순간 양자붕괴 발생
- 원 데이터의 의미는 손실
- 채널을 감시하는 것으로 원활한 통신 방해
- 무결성 침해 -> 가용성 침해 공격으로 둔갑

5. 결론



- 가용성 침해 공격은 일반 사용자에게 가장 와닿는 공격
- 통신 상태가 원활하지 않을 경우 서비스 제공자가 책임
- 양자통신이 활성화 된 상황은 아니지만 **대응책 설립**이 중요
 - 채널 자체의 관측을 피할 수 있는 회피 기법
 - 공격 발생 시 우회 할 수 있는 대처 기법 등
- 추후에 발생할 수 있는 피해를 줄이거나 방지

Q & A

