**별첨6) JAVA Secure Coding Standard Guide**

|  |  |  |
| --- | --- | --- |
| **No** | **보안 코딩 표준** | **설명** |
| 1 | 입력 검증 및 데이터 세니타이즈(IDS) | 입력 데이터는 규범화와 정규와 수행 🡪 새니타이즈 수행 🡪 검증 수행 순서로 데이터의 신뢰도를 수행한 뒤 입력값이 상요되도록 프로그램을 작성한다. |
| 2 | 선언과 초기화(DCL) | 클래스를 선언하고 초기화 하여 사용하는 방법에 대한 정확하지 않은 코드도 취약점이 된다. |
| 3 | 표현식(EXP) | 수식에 대한 부정확한 이해와 잘못된 사용으로 인해 안전하지 않은 프로그램이 될 수 있다. |
| 4 | 수치형과 연산(NUM) | 수치형 데이터의 정확한 이해와 부적절한 연산은 안전하지 않은 프로그램을 작성할 수 있게 한다. |
| 5 | 객체지향(OBJ) | 오브젝트에 대한 접근 방식이나 객체의 생성과 소멸에 대한 정확한 이해가 없으면 안전하지 않은 프로그램을 작성할 수 있다. |
| 6 | 메서드(MET) | 각 메서드의 정확한 용도와 사용방법을 숙지하여 사용하지 않으면 취약한 프로그램을 작성할 수 있다. |
| 7 | 예외처리(ERR) | 시스템에서 발생된 예외에 대한 과도한 처리나, 무시, 부정확한 처리는 취약점을 가진 프로그램을 생산할 수 있다. |
| 8 | 가시성과 원시성(VNA) | 공유데이터를 사용해야 하는 경우 적절한 접근 방식 설정과 복합 연산에 대한 원자성을 보장할 수 있는 프로그램 작성 기법이 요구된다,. |
| 9 | 락(LCK) | 공유자원에 대한 동기화 설정시 락을 엳기, 사용, 반납에 대한 정확한 이해와 구현이 없다면 취약한 프로그램을 작성 할 수 있다. |
| 10 | 스레드API(THI) | 스레드의 라이프 사이클에 적절한 스레드 클래스의 메서드를 사용하는 방법을 숙지하지 않으면 안전하지 않은 프로그램을 작성할 수 있다. |
| 11 | 스레드 풀(TPS) | 스레드 풀을 사용하는 경우 안전하게 풀을 관리할 수 있는 메커니즘이 보장되어야 한다. |
| 12 | 그 밖의 스레드 안전(TSM) | 스레드 사용시 안전하게 메서드를 사용하는 메커니즘이 적용되지 않으면 프로그램이 취약할 수 있다. |
| 13 | 입출력(FIO) | 파일에 대한 입출력을 처리하기 위한 클래스나 메서드를 정확하게 이해하고 프로그램에 적용해야 안전한 프로그램을 작성할 수 있다. |
| 14 | 직렬화(SER) | 객체를 파일에 저장하거나 네트워크를 통한 전송을 위해 요구되는 직렬화를 처리하는 클래스와 메서드를 정확하게 이해하고 프로그램에 적용해야 한다. |
| 15 | 플랫폼 보안(SEC) | 자바 프로그램이 실행되는 플랫폼에 대한 보안정책을 이해하고 적용해야 한다. |
| 16 | 런타임 환경(ENV) | 자바 프로그램 실행시 사용되는 환경변수 사용이나 바이트 코드 검증 기능에 대해 정확하게 이해하고 활용해야 한다,. |
| 17 | 기타(MSC) | 잘 관리되는 메모리나 안전한 통신 채널을 사용하는 프로그램을 작성해야 한다. |

* 새니타이즈(Sanitize) : 입력 값이 시스템 또는 클라이언트에 악영향을 미칠 수 있다면, 그 값을 모두 무효화 시킨다.