■ 헌법재판소 보안업무 규칙 [별표 2] <개정 2022. 4. 6.>

## 정보통신보안 규정 위반 사항(제39조의2 제1항 관련)

| 내용 | 세부내용 |
|---|---|
| 1. 적성국과의 통신 | 가. 적성국 인터넷망과의 메시지 또는 자료 송수신<br>나. 적성국의 국내외 인터넷 거점(경유지를 포함한다)과의 통신<br>다. 적성국의 국내외 인터넷 거점(경유지를 포함한다)에서 공직자 상용메일 불법 접속<br>라. 적성국의 인터넷 사회관계망서비스(SNS) 사용계정과의 메시지 또는 자료 송수신 |
| 2. 정보통신망을 통한 군사상 기밀의 누설 또는 유출 | 가. 군사전략, 작전계획 및 진행사항의 누설 또는 유출<br>나. 군 편제·임무·시설 및 그 밖의 부대현황의 누설 또는 유출<br>다. 병력(군·경·예비군) 현황 및 이동 상황의 누설 또는 유출<br>라. 경찰 및 특수기관의 장비(작전·정보·수사용) 현황과 집행사항의 누설 또는 유출<br>마. 특수기관·군사시설의 위치 및 이동상황의 누설 또는 유출<br>바. 군사장비의 구성·성능 및 발명개량 연구사항의 누설 또는 유출<br>사. 군사장비(군수품 등) 생산 및 공급사항의 누설 또는 유출<br>아. 그 밖에 국가방위에 영향을 초래하는 사항의 누설 또는 유출 |
| 3. 정보통신망을 통한 외교상 기밀의 누설 또는 절취 | 가. 국가 외교방침, 기본계획 및 재외공관에 발하는 훈령의 누설 또는 유출<br>나. 공개할 수 없는 외교조약 또는 협약의 누설 또는 유출<br>다. 특수임무를 수행하는 해외주재원의 활동(계획·지시·보고) 및 신원정보와 관련된 사항의 누설 또는 유출<br>라. 그 밖에 국가외교에 영향을 초래하는 사항의 누설 또는 유출 |
| 4. 정보통신망을 통한 국가정보 활동 관련 사항의 누설 또는 절취 | 가. 대공업무와 관련된 사항의 누설 또는 유출<br>나. 정보(첩보) 수집활동에 필요한 사항의 누설 또는 유출<br>다. 간첩 또는 대공용의자 발견과 수사활동의 누설 또는 유출<br>라. 정보 및 특수 수사기관의 기구 또는 임무기능 관련 사항의 누설 또는 유출<br>마. 국가원수 및 그 밖의 요인의 비공개행사의 누설 또는 유출<br>바. 불명선박의 발견 및 처리의 누설 또는 유출<br>사. 중요물자 수송활동의 누설 또는 유출<br>아. 테러·마약·밀수 및 국제범죄조직 관련 정보·수사활동의 누설 또는 유출<br>자. 적 또는 경쟁국에 유리한 과학기술 및 산업 관련 정보의 누설 또는 유출<br>차. 그 밖에 국가안보 및 공안유지에 불리한 영향을 초래하는 사항의 누설 또는 유출 |
| 5. 암호자재 관련 사항 | 가. 암호자재의 연구개발 및 제작에 필요한 사항 누설<br>나. 암호전문을 허위로 조립하여 송신 |

| | |
|---|---|
| | 다. 암호를 부정한 목적에 사용<br>라. 암호문과 암호화되지 아니한 평문의 혼용 및 이중사용<br>마. 암호문 작성시 동일 난수를 2회 이상 반복사용<br>바. 사용기간이 경과된 암호자재를 계속 사용<br>사. 암호문에 암호화되지 아니한 평문을 삽입하여 송신<br>아. 그 밖에 암호자재 보호체계를 손상시킬 우려가 있는 사항 누설 |
| 6. 전자정보 | 가. 주전산기(주요 서버 등)·대용량 전자기록(DB)의 손괴<br>나. 전자정보의 위조·변조·훼손 |
| 7. 정보통신망 및 정보통신시스템 관련 사항 | 가. 정보통신망에 대한 불법침입, 해킹·악성코드의 유포<br>나. 중요 정보시스템 및 정보통신실 파괴<br>다. 중요 정보시스템 기능 장애 및 정지 |
| 8. 비인가통신시설 및 통신제원 사용에 필요한 사항 | 가. 비인가된 유선·무선시설 또는 장비(소프트웨어를 포함한다)의 설치·운용<br>나. 비인가된 유선·무선시설 또는 장비(소프트웨어를 포함한다)와의 교신<br>다. 비인가된 호출부호 및 주파수 사용<br>라. 비인가된 전파형식 사용<br>마. 지정출력의 초과사용<br>바. 전파월경(電波越境) 방치 |
| 9. 허가목적 외의 방법으로 사용하는 경우 | 가. 허가목적 업무와 관련이 없는 통신<br>나. 군 통신망에서 군사업무와 관련이 없는 통신<br>다. 그 밖에 사회질서를 해치는 통신 |