

해외 입법 동향

중국, 국가 네트워크 안전사고 관리 방법 시행 (2025. 11. 1.)

○ 개요 및 추진배경

- 중국 국가인터넷정보판공실(国家互联网信息办公室)이 '25년 9월 15일 발표한 '국가 네트워크 안전사고 관리 방법(国家网络安全事件报告管理办法)*'이 시행 ('25.11.1.)

* 중국의 정책 문서 위계는 '헌법→법률(전국인민대표회의)→행정법규(국무원)→부처 규정→부처 규범성 문건' 순으로 구성되며, 방법은 부처의 규범성 문건에 해당 (출처 : 중국의 법령체계, 세계법제정보센터)

- 최근 중국 내 핵심정보기반시설과 대규모 개인정보 처리 기업을 대상으로 한 사이버 공격(알리페이, 웨이보, 디디추싱 등 중국 내 대규모 개인정보 유출사고)이 증가함에 따라 중국 정부는 고위험 사고 대응 체계를 강화
- 동 방법은 기존 법률에 산재되어 있는 사고보고 의무를 통합하여 구체적으로 명시하였으며, 특히 사고 등급을 4단계로 분류하여 사고 유형별 보고 주체, 기한, 보고 내용 등 사고보고 절차를 체계화

○ 주요내용

- **(목적)** 사이버보안 사고 보고 및 관리를 표준화하고, 사이버보안 사고로 인한 손실과 위해를 신속히 통제하며, 「네트워크안전법」, 「데이터안전법」, 「개인정보보호법」, 「핵심정보기반시설 안전보호 조례」 등 상위법 이행을 위하여 절차를 구체화(제1조)
- 중국 영토에서 네트워크를 구축, 운영 또는 네트워크를 통해 서비스를 제공하는 네트워크 운영자*는 동 방법에 따라 네트워크 안전사고**를 보고해야 함(제2조)
- **(네트워크 운영자)** 네트워크의 소유자, 관리자 및 네트워크 서비스 제공자
- **(네트워크 안전 사고)** 인위적 원인, 네트워크 공격, 네트워크의 취약점 또는 결함, 소프트웨어·하드웨어의 결함이나 장애, 불가항력 등의 요인으로 인해 네트워크·정보시스템·데이터·업무 응용에 손상을 주고, 그 결과 국가·사회·경제에 부정적인 영향을 끼치는 사고
- 국가인터넷정보부서는 전국의 네트워크 안전사고 보고 관리 업무를 총괄하고, 성(省)급 행정구역 인터넷 정보부처는 해당 행정구역 내 보고 관리 업무를 담당(제3조)
- 네트워크 운영자는 네트워크 안전사고를 발견하거나 알게 된 경우, '네트워크 안전사고 등급 분류 지침(网络安全事件分级指南)*'에 따라 분석·판단해야 하고 중대한 네트워크 안전사고 이상에 해당하는 경우의 보고 절차를 규정

* 동 방법은 네트워크 안전사고를 ▲특별 중대한 사고, ▲중대한 사고, ▲비교적 중대한 사고, ▲일반 사고 등 4단계로 분류하였고, 세부 내용은 하단의 붙임을 참고

〈 사고보고 주체 및 유형별 보고체계 〉

| 보고주체 | 주요내용 | | |
|---------------------|-----------------|--|---------------------------------|
| | 사고 유형 | 보고기관 | 보고 기한 |
| 핵심정보기반시설 관련 운영자 | • 전체 사고 | 보호업무부서(向保护工作部门) ·공안기관 | 1시간 이내 |
| | • 특별 중대한·중대한 사고 | 국가인터넷 보호업무부서 ▶ 정보부서· 국무원 공안부 | 30분 이내 (보호업무부서의 사고접수 후) |
| 중앙 및 국가기관 소속 운영자 | • 전체 사고 | 소속 부처 내 인터넷 정보 부서 | 2시간 이내 |
| | • 특별 중대한·중대한 사고 | 소속 부처 ▶ 국가인터넷 정보부서 | 1시간 이내 (소속 부처의 사고접수 후) |
| 일반 네트워크 운영자 | • 전체 사고 | 소재지 성급 인터넷 정보 부서 | 4시간 이내 |
| | • 특별 중대한·중대한 사고 | 성급 인터넷 정보 부서 ▶ 국가 인터넷 정보 부서 ·동급의 관련 부서 | 1시간 이내 (성급 인터넷정보부서의 사고 접수 후) |

- 네트워크 안전사고 보고 시 ①사고 관련 기관명·시스템 또는 시설 기본 상황, ②사고 발생 또는 발견 시간·장소·유형·등급·영향·조치 및 효과(랜섬웨어의 경우 몸값 요구 금액·방식·날짜 등 추가), ③사태 발전 추이 및 추가 위험성 ④사고 초기 원인 분석 의견, ⑤추적 조사 단서(공격자 정보·공격 경로·취약점 등), ⑥향후 대응 조치 및 지원 요청 사항 ⑦사고 현장 보호 상황 ⑧기타 사항 등 8가지 내용을 포함(제7조)

- 사고 처리 종료 후 30일 이내에 사고 발생 원인, 비상 대응 조치, 피해 상황, 책임 추궁, 개선 조치 상황 등을 종합적으로 분석·정리하여 사고 처리 종합 보고서를 원 보고채널을 통해 상급 기관에 제출(제8조)

- 네트워크 운영자가 동 방법에 따라 보고하지 않거나 사고를 지연·누락·허위 또는 은폐 보고하여 중대한 피해를 초래한 경우, 관련 법률 및 행정규정에 따라 관련 기관과 개인의 책임을 추궁(제10조)

※ 「네트워크 안전법」은 네트워크 운영자가 사고보고를 하지 않을 경우, 주무 부서가 시정을 명하고 경고를 하며, 네트워크 운영자가 시정을 거부하거나 네트워크 안전에 피해를 초래한 경우 1만 위안 이상 10만 위안 이하의 과태료를 부과하고 직접 책임이 있는 담당자에게 5천 위안 이상 5만 위안 이하의 과태료를 부과(제59조)

- 운영자가 적절한 방어 조치를 이미 취하고, 예비계획을 실행해 피해 등을 효과적으로 감소시켰으며, 적시 보고한 경우, 상황에 따라 책임을 완화하거나 추궁하지 않을 수 있음을 명시(제11조)

○ 전망 및 시사점

- 중국 정부는 급증하는 사이버 위협에 효과적으로 대응하고, 네트워크 안전사고 발생 시 신속한 보고 및 관리를 통해 국가 안보와 사회 질서, 경제적 손실을 최소화하기 위해 국가 네트워크 안전사고 관리 방법을 마련
- 동 방법은 네트워크 안전사고를 특별 중대한 사고, 중대한 사고, 비교적 중대한 사고, 일반 사고 등 4단계로 구분하여, 네트워크 운영자별 보고 기관과 기한을 명확히 하고, 보고해야 하는 세부 내용을 구체화
- 중국 내에서 사업을 운영하는 기업 및 공급망에 속한 기업들은 사고보고 의무 이행을 위한 내부 대응 체계를 점검하여, 법적 리스크를 관리할 필요

붙임

네트워크 안전사고 등급 분류 지침

| 구분 | 주요내용 |
|---|--|
| 특별 중대한 네트워크 안전사고 (特别重大网络安全事件) | <ul style="list-style-type: none"> • 다음 사항 중 하나에 해당하는 경우 특별 중대한 네트워크 안전사고로 분류 <ul style="list-style-type: none"> - 중요 네트워크 및 정보 시스템이 특히 심각한 시스템 손실을 입어 시스템이 광범위하게 마비되고 업무 처리 능력을 상실한 경우 - 핵심 데이터, 중요 데이터, 대량의 시민 개인정보가 유실되거나 도난, 변조, 위조되어 국가 안보와 사회 안정에 특히 심각한 위협을 초래한 경우 - 기타 국가 안보, 사회 질서, 경제 건설 및 공공 이익에 특별히 심각한 위협을 구성하거나 특별히 심각한 영향을 초래한 사고 • 일반적으로 다음 중 하나를 충족하는 경우 특별 중대한 네트워크 안전사고로 판단 가능 <ul style="list-style-type: none"> - 성(省)급 행정구역 이상의 당·정부 기관 포털 사이트 또는 중앙 주요 뉴스 사이트가 공격 또는 장애로 인해 24시간 이상 접속 불가 상태가 된 경우 - 핵심정보기반시설 전체가 6시간 이상 중단되거나 주요 기능이 24시간 이상 중단된 경우. - 한 개 이상의 성급 행정구역 인구 50% 이상 또는 1천만 명 이상의 용수·전력·가스·석유 공급, 난방, 교통 이동, 의료, 쇼핑 등 업무·생활에 영향을 미친 경우 - 핵심 데이터·중요 데이터 유출 또는 도난·변조·위조로 국가 안보와 사회 안정에 특히 심각한 위협을 초래한 경우 - 1억 명 이상의 시민 개인정보가 유출된 경우 - 성급 이상 당·정부 기관 포털 사이트, 중앙 주요 뉴스 사이트, 초대형 네트워크 플랫폼 등이 공격·변조되어 불법 유해 정보가 특대 범위(特大范围)*로 유포된 경우 <p>* (특대범위) ▲홈페이지에 게시되어 6시간 이상 지속되거나, 기타 페이지에 게시되어 24시간 이상 지속된 경우, ▲소셜 플랫폼을 통해 10만 회 이상 전파된 경우, ▲열람 또는 클릭 횟수가 100만 회 이상인 경우, ▲성급 이상 인터넷정보부서, 공안기관이 “특대 범위 전파”로 인정한 경우</p> <ul style="list-style-type: none"> - 1억 위안 이상의 직접적 경제적 손실을 초래한 경우 - 기타 국가 안보, 사회 질서, 경제 건설 및 공공 이익에 특히 심각한 위협을 가하거나 특히 심각한 영향을 초래한 네트워크 안전사고 |
| 중대한 네트워크 안전사고 (重大网络安全事件) | <ul style="list-style-type: none"> • 다음 사항 중 하나에 해당하며 특별 중대한 네트워크 안전사고에 해당하지 않는 경우, 중대한 네트워크 안전사고로 분류 <ul style="list-style-type: none"> - 중요 네트워크 및 정보 시스템이 심각한 시스템 손실을 입어 장시간 중단되거나 부분 마비되어 업무 처리 능력이 극히 저하된 경우. - 핵심 데이터, 중요 데이터, 대량의 시민 개인정보가 유실되거나 도난·변조·위조되어 국가 안보와 사회 안정에 심각한 위협을 초래한 경우. - 기타 국가 안보, 사회 질서, 경제 건설 및 공공 이익에 심각한 위협을 가하거나 중대한 영향을 초래하는 사고 • 일반적으로 다음 조건 중 하나를 충족하는 경우 중대한 네트워크 안전사고로 판단 가능 <ul style="list-style-type: none"> - 시(市)급 이상 당·정부 기관, 기업·기관 포털 웹사이트 및 성급 이상 주요 뉴스 사이트가 공격 또는 장애로 인해 6시간 이상 접속 불가 상태가 되는 경우 - 핵심정보기반시설 전체가 1시간 이상 중단되거나 주요 기능이 3시간 이상 중단되는 경우. - 한 개 이상의 시급 행정구역 인구 50% 이상 또는 100만 명 이상의 주민에게 수도, 전기, 가스, 석유, 난방, 교통, 의료, 쇼핑 등 업무 및 생활에 영향을 미친 경우 |

| 구분 | 주요내용 |
|--|--|
| | <ul style="list-style-type: none"> - 핵심 데이터 또는 중요 데이터가 유출되거나 도난, 변조, 위조되어 국가 안보와 사회 안정에 심각한 위협을 초래한 경우 - 1천만 명 이상의 시민 개인정보 유출 - 시급 이상 당정기관·기업·기관 포털 사이트, 성급 이상 주요 뉴스 사이트, 대형 이상 네트워크 플랫폼 등이 공격·변조되어 불법 유해 정보가 광범위*하게 유포된 경우 * (광범위) ▲홈페이지에 2시간 이상 노출되거나 기타 페이지에 12시간 이상 노출된 경우, ▲소셜 플랫폼을 통해 1만 회 이상 전파된 경우, ▲열람 또는 클릭 횟수가 10만 회 이상인 경우, ▲성급 이상 인터넷정보부서, 공간기관이 "대규모 전파"로 인정한 경우. - 2000만 위안 이상의 직접적 경제적 손실을 초래한 경우. - 기타 국가 안보, 사회 질서, 경제 건설 및 공공 이익에 심각한 위협을 가하거나 중대한 영향을 초래한 네트워크 안전사고 |
| <p>비교적 중대한 네트워크 안전사고 (较大网络安全事件)</p> | <ul style="list-style-type: none"> • 다음 사항 중 하나에 해당하며 중대한 네트워크 안전사고에 해당하지 않는 경우, 비교적 중대한 네트워크 안전사고로 분류 - 중요 네트워크 및 정보 시스템이 상당한 시스템 손실을 입어 시스템 중단을 초래하고, 시스템 효율에 현저한 영향을 미치며 업무 처리 능력이 저하된 경우 - 중요 데이터 또는 상당량의 시민 개인 정보가 분실·도난·변조·위조되어 국가 안보 및 사회 안정에 비교적 심각한 위협을 가한 경우 - 기타 국가 안보, 사회 질서, 경제 건설 및 공공 이익에 중대한 위협을 가하거나 심각한 영향을 초래하는 사고 • 일반적으로 다음 중 하나를 충족하는 경우 비교적 중대한 네트워크 안전사고로 판단 가능 - 시급 이상 당정 기관, 기업·기관 포털 웹사이트 또는 성급 이상 주요 뉴스 사이트가 공격·장애로 인해 2시간 이상 접속 불가 상태 - 핵심정보기반시설 전체가 10분 이상 중단되거나 주요 기능이 30분 이상 중단된 경우. - 한 개 이상의 시급 행정구역 인구 30% 이상 또는 10만 명 이상의 주민의 용수, 전력, 가스, 석유, 난방, 교통, 의료, 쇼핑 등 업무 및 생활에 영향을 미친 경우 - 중요 데이터 유출 또는 도난으로 국가 안보와 사회 안정에 중대한 위협을 초래한 경우. - 100만 명 이상의 시민 개인정보 유출. - 당·정부 기관, 기업·기관 포털 사이트, 주요 뉴스 사이트, 네트워크 플랫폼 등이 공격·변조되어 불법 유해 정보가 비교적 광범위*하게 유포된 경우 * (비교적 광범위) ▲홈페이지에 30분 이상 노출되거나, 기타 페이지에 2시간 이상 노출된 경우, ▲소셜 플랫폼을 통해 1000회 이상 전파된 경우, ▲열람 또는 클릭 횟수가 1만 회 이상인 경우, ▲성급 이상 인터넷정보부서, 공간기관이 "상당한 범위 전파"로 인정한 경우 - 500만 위안 이상의 직접적 경제적 손실을 초래한 경우 - 기타 국가 안보, 사회 질서, 경제 건설 및 공공 이익에 비교적 심각한 위협을 구성하거나 비교적 심각한 영향을 초래한 사고 |
| <p>일반 네트워크 안전사고 (一般网络安全事件)</p> | <ul style="list-style-type: none"> • 상기 사고 외에 국가 안보, 사회 질서, 경제 건설 및 공공 이익에 일정한 위협을 구성하거나 일정한 영향을 초래한 사고 |

Reference

- 中国网信网, 国家网络安全事件报告管理办法, 2025.9.15
- 中国网信网, 国家互联网信息办公室发布《国家网络安全事件报告管理办法》, 2025.9.15
- 金杜律师事务所, 唯见平安火入城《国家网络安全事件报告管理办法》解读及合规要点, 2025.9.19.
- 上海市锦天城律师事务所, 《国家网络安全事件报告管理办法》深度解读—构建制度化、规范化、精细化的国家网络安全事件报告体系, 2025.9.18.

인터넷·정보보호 법제 동향

(2025년 11월)

| 발 행 처 | 한국인터넷진흥원

(58324) 전라남도 나주시 진흥길 9 한국인터넷진흥원

Tel. 1433-25

| 기획·편집 | 법제연구팀

| 발간·배포 | www.kisa.or.kr

※ 본 자료의 내용은 한국인터넷진흥원의 공식 견해를 나타내는 것은 아닙니다.

※ 본 자료 내용의 무단 전재 및 상업적 이용을 금하며, 가공·인용할 때에는 반드시 출처를 밝혀 주시기 바랍니다.