

국가 사이버보안 기본지침 시행

-망분리 일률규제 폐지·N2SF 도입과 민간사업자가 점검할 사항-

국가정보원은 2026년 5월 1일자로 종전 「국가 정보보안 기본지침」을 「국가 사이버보안 기본지침」(이하 “본 지침”)으로 명칭을 변경하고 일부개정하였습니다. 이번 개정의 핵심은 종전 제40조의 일률적 내부망·인터넷망 분리 조항을 삭제하고, 정보의 등급(기밀(C)·민감(S)·공개(O))과 도메인 구분에 기반한 국가 망 보안체계(N2SF)로 전환한 점입니다.

본 지침은 형식상 각급기관(공공기관)에 적용되나, 신설된 제4조 제3항에 따라 정보화사업 수주 용역업체, 정보시스템·정보보호시스템 개발·제조·공급업체, 클라우드컴퓨팅서비스 제공자, 전기통신사업자, 정보통신서비스 제공자도 국가정보원장의 자료제출 등 협조 요청에 정당한 사유가 없으면 응할 의무를 부담하게 되었습니다.

1. 적용 경로 및 주요 내용
2. 관련 쟁점
3. 시사점

1. 적용 경로 및 주요 내용

가. 적용 경로

본 지침은 「사이버안보 업무규정」 등 상위 법령에 근거한 국가정보원장의 행정규칙으로, 직접적 적용대상은 각급기관(제3조)이지만 다음과 같은 경로로 민간기업의 실무에 직접 영향을 미칩니다.

적용 경로	구체적 내용	근거 조문
직접 적용 (공공기관)	중앙행정기관·지방자치단체·공공기관·교육기관 등 각급기관의 사이버 보안업무 전반	제3조 (적용범위)

민간 협조의무 (신설)	① 정보화사업 수주 용역업체 ② 정보시스템·정보보호시스템 개발·제조·공급업체 ③ 클라우드컴퓨팅서비스 제공자 ④ 전기통신사업자 ⑤ 정보통신서비스 제공자 ※ 국가정보원장의 사실 조회·확인, 자료제출 등 요청에 정당한 사유 없다면 응하여야 함	제4조 제3항 (신설 2026.5.1.)
시장진입 요건	공공 부문에 클라우드컴퓨팅서비스를 제공하려는 민간 사업자는 「국가 클라우드 보안기준」 준수 및 클라우드컴퓨팅 도입 가능 목록 등재 필요	제24조의3, 제24조의4
간접 영향	망분리 솔루션·DLP·EDR·DRM·다중인증 등 보안제품 시장의 수요 구조 변화 (등급별 차등 통제로 전환)	제39조의2~5, 제76조 등

주의: 제4조 제3항의 협조의무는 신설된 조항이며, "정당한 사유"의 범위, 미협조 시 제재의 실효성, 그리고 영업비밀·고객정보 등과의 충돌 시 처리 방향에 대한 유권해석이나 후속 가이드라인은 현재까지 확인되지 않습니다. 자료제출 요청을 받은 기업은 사안별 법률 검토를 거쳐 대응 범위를 확정할 필요가 있습니다.

나. 주요 내용

(1) 망분리 일률규제 폐지와 N2SF(국가 망 보안체계) 신설

종전에는 모든 공공기관이 내부 업무망과 인터넷망을 물리적·논리적으로 분리하여야 한다는 일률적 의무가 규정되어 있었으나(舊 제40조), 이번 개정으로 동 조항은 삭제되었습니다. 대신 제3장 제1절(제39조의2~제39조의5)이 신설되어, 업무정보를 등급별로 분류하고 그에 상응하는 도메인·정보시스템·보안통제를 차등 적용하는 「국가 망 보안체계(N2SF, National network Security Framework)」가 도입되었습니다.

구분	종전 (As-Is, 2023.1.31)	개정 후 (To-Be, 2026.5.1.~)
망분리	내부망·인터넷망 물리적/논리적 분리 일률 의무 (구 제40조)	구 제40조 삭제 / 등급(C·S·O)별 도메인 구분 및 차등 보안통제로 전환 (제39조의2~5 신설)
정보 분류	비밀·대외비·일반 업무자료 위주의 비교적 단순한 구분	기밀등급(Classified, C) / 민감등급(Sensitive, S) / 공개등급(Open, O) 3등급 체계로 정비 (제2조)
클라우드	공공 부문의 민간 클라우드 활용에 일률적 제약	국가 클라우드 보안기준을 충족한 「클라우드 컴퓨팅 도입 가능 목록」 등재 서비스에 한해 도입·이용 허용 (제24조의3, 제24조의4)

보안 예산·인력	"확보를 위해 노력하여야 한다" 수준의 권고 규정	정보화업무 담당인력 대비 10% 이상, 정보화 예산 대비 15% 이상 운영 의무 (제5조 제3항)
다중인증 (MFA)	명시적 의무 부재 또는 권고 수준	원격근무자: 소유기반(OTP·SMS·모바일신분증)과 생체기반(지문·홍채) 등 서로 다른 방식 다중 적용 (제59조 제4항 제3호) / 정보시스템 관리자 권한 인증: 원칙적 다중인증 적용 (제76조 제4항 신설)
웹사이트 플러그인 설치	명시적 규정 없음	공공 웹사이트 구축·운영 시 이용자 단말의 플러그인 소프트웨어 설치 강제·유도 방식 최소화 (제54조 제6항 신설)
관제(EDR)	단말 위협탐지의 보안관제 연동에 대한 명시적 규정 미비	각 기관 도입 EDR을 보안관제체계와 연동하도록 규정 (제131조 제5항 제5호)

(2) 정보 등급 분류 체계 (제2조)

신설된 등급 체계는 단순한 분류표가 아니라 N2SF의 작동 단위입니다. 등급에 따라 처리 가능한 도메인·정보시스템·보안통제 수준이 달라지므로, 본 분류는 향후 공공조달 기획·솔루션 설계 단계에서 가장 먼저 결정해야 하는 변수입니다.

등급	대상 정보	도메인·시스템 구성
기밀등급 (C)	「보안업무규정」 제4조에 따른 비밀, 「보안업무규정 시행규칙」 제16조 제3항에 따른 대외비, 비밀의 주요 내용이 기술된 문장·문구	기밀등급 도메인: 기밀등급 이하의 정보 시스템·단말기를 두거나 기밀등급 이하의 업무정보를 처리하기 위해 각급기관이 직접 구축·운영하는 정보통신망 영역
민감등급 (S)	「공공기관의 정보공개에 관한 법률」 제9조 제1항 제5호~제8호에 따른 비공개 대상 정보 및 그 주요 내용이 기술된 문장·문구	민감등급 도메인: 민감등급 이하 정보의 처리 영역 (각급기관이 이용하는 외부 클라우드컴퓨팅 영역 포함)
공개등급 (O)	기밀·민감등급을 제외한 모든 업무정보 (공공데이터 포함), 관련 법령상 요건을 조치한 행정·민감정보	공개등급 도메인: 외부 인터넷·클라우드 컴퓨팅 영역 활용 가능 (상용 인터넷망 포함)

제39조의3 제1항 단서에 따라 「국가 망 보안체계 보안가이드라인」의 보안통제 항목을 준수하는 경우, 업무 정보 등급보다 낮은 등급의 정보시스템·도메인에서도 처리가 가능합니다. 즉 N2SF는 등급 간 절대적 차단이 아니라, 보안통제를 통해 가이드라인 충족을 조건으로 한 유연한 운용을 허용하는 구조입니다. 동 보안 가이드라인의 구체적 보안통제 항목은 '국가 망 보안체계 보안 가이드라인 1.0'를 통해 별도로 배포되었습니다.

2. 관련 쟁점

가. 민간 클라우드의 공공 시장 진입 경로 정비

제24조의3은 각급기관이 도입·운영할 수 있는 클라우드컴퓨팅 서비스를 「클라우드컴퓨팅 도입 가능 목록」으로 명시화하였고, 제24조의4는 민간 클라우드컴퓨팅 서비스 이용 시 동 목록에 등재된 서비스만을 이용하도록 규정하였습니다. 또한 제41조는 자체 구축형 클라우드와 민간 클라우드 모두에 대해 「국가 클라우드 컴퓨팅 보안 가이드라인」상의 국가 클라우드 보안기준 준수를 요구합니다.

실무적으로 이는 민간 CSP(Cloud Service Provider)입장에서 ① 도입 가능 목록 등재 신청·심사 절차의 통과, ② 국가 클라우드 보안기준 충족, ③ 등재 후에도 제4조 제3항에 따른 자료제출 등 협조의무 부담의 3중 구조로 작동합니다. 등재 절차의 구체적 운영 기준과 통과는 향후 국가정보원이 공개하는 운영지침에 따라 결정됩니다. 전반적인 보안 지침은 국가사이버안보센터에서 발간한 '국가 클라우드 컴퓨팅 보안 가이드라인(2023.01)'등을 참고할 수 있습니다.

나. 협력업체 협조의무의 실질적 범위와 한계

제4조 제3항은 국가정보원장이 사이버보안 직무수행과 관련하여 사실의 조화·확인, 자료의 제출 등 협조 또는 지원을 요청할 수 있는 대상을 국가기관·관계 기관 외에 5개 유형의 민간 단체로 확장하였습니다. 이는 단순한 협력 권고가 아니라, "정당한 사유가 없으면 그 요청에 따라야 한다"는 의무 형식으로 규정되어 있습니다.

그러나 동 조항은 ① "정당한 사유"의 판단기준, ② 자료제출 범위(고객 개인정보·영업비밀·소스코드 등의 포함 여부), ③ 미협조 시 제재 수단의 직접적 근거를 명시하지 않습니다. 실무상으로는 「개인정보 보호법」상 정보주체의 권리, 「부정경쟁방지 및 영업비밀보호에 관한 법률」상 영업비밀 보호, 그리고 해외 고객·해외법인이 관련된 경우 외국법상 데이터 이전 제한과의 충돌 가능성이 있어, 사안별로 신중한 검토가 필요합니다.

다. 사용자 인증·관제 강화의 솔루션 시장 영향

제76조 제4항은 정보시스템 관리자 권한 인증에 다중인증을 원칙적으로 적용하도록 신설되었고, 제59조 제4항 제3호는 원격근무 시 소유기반 인증과 생체기반 인증 등 서로 다른 인증방식의 다중 적용을 의무화하였습니다. 또한 제131조 제5항 제5호는 EDR을 보안관제체계와 연동하도록, 제54조 제6항은 공공 웹사이트의 플러그인 강제·유도 방식을 최소화하도록 신설되었습니다.

이로 인해 ① 다중인증 솔루션·통합인증체계(SSO/IAM), ② EDR·XDR 및 보안관제 연동, ③ HTML5 기반 비-플러그인 본인인증·결재전자문서 솔루션의 공공 부문 수요가 구조적으로 확대될 가능성이 있습니다. 반면 종전 망분리 환경에 특화되었던 일부 솔루션 영역은 N2SF 전환에 따른 재정의가 필요할 수 있으며, 그 정도는 「국가 망 보안체계 보안가이드라인」의 구체적 통제항목에 따라 달라질 것입니다.

3. 시사점

이번 개정의 핵심은 단순한 제도 변경을 넘어 국가 사이버 보안의 패러다임이 획일적인 '차단'에서 데이터

중심의 '유연한 통제'로 완전히 전환되었다는 데 큰 의미가 있습니다. 특히 민간 기업에 부여된 협조 의무와 N2SF(국가 망 보안체계)의 도입은 공공 시장 진입을 위한 필수 요건이 단순한 제품 성능을 넘어 '거버넌스 준수 및 법률적 대응 역량'으로 확장되었음을 시사합니다. 이는 기업에 클라우드 기반의 유연한 업무 환경을 제공하는 기회가 되는 동시에, 영업비밀 보호와 공공 안보 협력 사이에서 정교한 균형점을 찾아야 하는 전략적 과제를 안겨줍니다. 따라서 각 기업은 하단의 점검 사항을 통해 자사의 비즈니스 모델이 변화된 규제 환경에서 가질 실무적 영향력과 법적 리스크를 선제적으로 파악해야 합니다.

기업 유형	핵심 질문	우선 점검 사항
민간 클라우드 사업자 (CSP)	"우리 서비스가 도입 가능 목록에 등재될 수 있는가? 등재 후 공공 매출 확대 여력은?"	국가 클라우드 보안기준 항목별 GAP 진단, C/SAP 등 기존 인증과의 연계, 등재 신청 일정 및 갱신·취소 사유 점검, 등재 후 협조의무 대응체계 마련
공공 SI·솔루션 사업자	"기존 망분리 기반 사업과 진행 중 RFP는 어떻게 영향을 받는가?"	진행 중 사업의 N2SF 적용 시점·범위 확인 (발주기관과 변경 협의), 향후 RFP 응대 표준의 등급 기반 재설계, 자체 솔루션 라인업의 등급별 보안통제 매핑
통신사·ISP·정보통신서비스 제공자	"제4조 제3항의 협조 요청 범위는 어디까지이며, 통신비밀·고객정보와 어떻게 조화시키는가?"	자료제출 요청 접수·검토·승인 프로세스 사규화, 통신비밀보호·개인정보보호와의 충돌 시 법률검토 절차, 거절 또는 일부 제출의 정당사유 판단기준 마련
보안제품·관제 사업자	"우리 솔루션이 등급별 N2SF 통제항목과 어떻게 매핑되는가?"	제품군별 보안가이드라인 적합성 분석, EDR·MFA·통합인증·DLP 등 신규 수요 라인업 강화, 망분리 의존 제품의 포지셔닝 재정의
해외법인·크로스보더 기업	"해외 본사·고객 데이터의 협조의무 대응이 외국법과 충돌하지 않는가?"	EU GDPR, 미국 CLOUD Act 데이터 이전 제한 등과의 충돌 가능성, 외국 정부의 자료요청과 한국 측 협조의무가 동시에 발생하는 시나리오의 사전 대응절차 수립

법무법인(유한) 화우 정보보호센터는 정보통신·정보보안 규제, 「개인정보 보호법」·「정보통신망법」·「전자정부법」 등 관련 법령 자문과 공공조달·클라우드·SI 사업 자문에 풍부한 경험을 보유하고 있습니다. 본 지침과 관련하여 화우는 ① 민간 클라우드 사업자의 「클라우드컴퓨팅 도입 가능 목록」 등재 전략 자문, ② 공공 SI·보안솔루션 사업자의 N2SF 전환 영향 분석 및 RFP 표준 재설계, ③ 통신사·ISP·정보통신서비스 제공자의 협조의무 대응체계 구축, ④ 자료제출 요청 사안별 법률검토(영업비밀·개인정보·외국법 충돌)에 이르기까지 통합적 자문을 제공하고 있습니다.

또한 공공조달 분쟁, 보안사고·침해사고 대응, 사이버보안 거버넌스 구축, 「국가정보원법」·「사이버안보 업무규정」 등 관련 법령 해석에 관한 자문 경험을 토대로, 고객사가 본 지침 시행에 따른 단기 대응뿐 아니라 중장기 사업전략 재설계까지 안정적으로 수행할 수 있도록 지원합니다.



Contacts

이근우

T. (+82) 2 6003 7558

센터장/파트너변호사 E. klee@yoonyang.com

정한근

T. (+82) 2 6003 7781

고문 E. hkjung@yoonyang.com

이수경

T. (+82) 2 6182 8132

파트너변호사 E. sgyi@yoonyang.com

이광욱

T. (+82) 2 6003 7535

파트너변호사 E. kwlee@yoonyang.com

정호선

T. (+82) 2 6182 8548

파트너변호사 E. junghs@yoonyang.com

지재원

T. (+82) 2 6003 7568

연구위원 E. jwji@yoonyang.com