

공공부문 사이버보안 책임성 강화 방안

□ 공공부문 사이버보안 실태

- (기본 사이버보안 수칙 미준수) 공공부문 사이버 침해사고의 주된 원인은 상당수가 기본적 사이버보안 수칙 미준수

< 최근 공공부문 주요 사이버 침해사고 >

연번	시 기	사 고
1	'25.7월	온나라시스템 해킹 및 자료 유출
2	'25.11월	한마음혈액원 랜섬웨어 감염 및 자료 유출
3	'26.1월	강원대병원, 화순전남대병원 랜섬웨어 감염
4	'26.2월	국립외교원 교육시스템 개인정보 유출
5	'26.6월	'모두의창업' 합격자 비공개 정보 유출
6	'26.7월	정보통신기획평가원 개인정보 유출

- (기관장 징계 全無) 정보 유출사고 시 비정무직* 기관장이 직접 징계받은 경우는 없으며, 책임자·관리자 징계**로 이어지는 경우도 적음(1% 수준)***

* 「국가공무원법」 제3조1항에 따라 정무직 공무원의 경우 징계 대상이 아님

** 「공무원 징계령 시행규칙」 상 '비밀 엄수 의무 위반(해킹 등에 의한 비밀 침해, 개인정보 관리 소홀 등)'으로 징계 가능(최대 '파면'까지 가능)

*** '21년~'26.5월까지 약 247건의 정보 유출사고 발생 / 총 9건 징계처분 / 기관장 징계 無

< 공공부문 정보 유출사고 처분현황 >

■ 처분현황 ('21.1월~'26.5월, 해킹 등 사이버공격으로 인한 정보 유출사고)

- (개인정보위 개인정보 유출) 총 247건 조사처분 중 과징금 29건, 과태료 182건, 징계권고 19건(처분 6건)

■ 처분내용

- (과징금) 개인정보 유출사고에 대해 공공은 정액과징금(50억 상한)을 부과, 연평균 건당 과징금 매년 증가*
* ('21, '22년) 없음 → ('23년) 0.23억원/건 → ('24년) 2.39억원/건 → ('25년) 2.74억원/건 → ('26.1~5월) 4.11억원/건
- (징계) △ 개인정보 유출사고는 '23년 별도 징계기준 마련* 후 각 기관은 징계권고 이행 확대**, △ 내부 업무정보 유출사고는 해킹을 주요 원인으로 보기에 징계로 이어지는 경우는 적음
* 「개인정보 보호법 위반에 대한 징계권고 기준」 제정('22.12월), 「국가공무원 복무징계 관련 예규」 등에 반영('23.1월)
** 반영 전('21~'22년) : 징계권고 13건 중 이행 3건 / 반영 후('23~'26.5월) : 징계권고 6건 중 이행 3건

- **(기관 유인 부족)** 사이버보안 수칙 준수여부 등을 평가하는 ‘사이버보안 실태평가*’ 결과가 ‘정부업무평가’ 내 반영되는 비중이 낮아** 기관의 사이버보안 향상 노력을 유인하는 동기 부족
 - ’25년 ‘사이버보안 실태평가’ 결과 중앙부처·광역지자체 ‘우수’ 기관 全無
 - * 「사이버안보 업무규정」에 따라 국정원이 수행(’07년~, 매년) / 각 기관의 사이버보안 관리, 기술, 위기대응역량 등 3개 분야(100개 지표)의 수준을 점수로 종합 평가
 - ** △(중앙행정기관 ‘자체평가’) 6점/300점, △(지자체 ‘합동평가’) 3개/112개 지표, △(공기업·준정부기관 ‘공공기관 경영실적평가’) 0.6점/100점
 - 또한, ‘사이버보안 실태평가’ 대상도 평가가 가능한 전체 국가·공공 기관 (2,160개)* 중 실제 평가를 실시하는 기관은 150여개(7.1%)* 한정
 - * 「사이버안보 업무규정」에 따라 국정원은 중앙행정기관·지자체·공공기관 모두 평가 가능 중앙부처(49), 광역지자체(16), 공기업 및 준정부기관(88), 기타공공기관(254), 기초지자체(226), 지방공기업(423), 지방출자·출연기관(890), 시도교육청(16), 교육지원청(176), 과기분야정부출연연(22) 등 2,160개 기관
 - ** 중앙부처(49개), 광역지자체(16개), 준정부·공기업(88개) 등 153개 기관(’26년)
- **(전담조직·인력 부족)** 중앙행정기관(49개)에서 전담부서(과·팀)를 운영하는 기관은 22%(11개*)에 불과하며,
 - * 과 : 과기정통부·외교부·산업부·기후부·국토부·국세청 / 팀 : 교육부·행안부·복지부·병무청·기상청
- ’25년 ‘사이버보안 실태평가’ 결과 사이버보안 담당인력을 정보화업무 담당인력 대비 기준*을 지키지 못하는 기관이 24%(37개/152개)
 - * 정보화업무 담당인력 대비 사이버보안 인력 10% 이상 운영(「국가 사이버보안 기본지침」 제5조제3항)
- **(낮은 예산투자* 순위)** 기술지원이 어려워 보안에 취약한 노후 SW 교체도 기관 내 투자 우선순위가 낮아 예산 확보가 어려움
 - * 전문 컨설팅, 보안패치, 취약점 점검, 모의해킹, 보안장비·솔루션 도입 등 예산소요
- **(사기 저하)** 사이버보안 업무는 높은 전문성 요구, 사고 시 책임 부담, 무사고 등 성과 증명의 어려움* 등으로 기피되는 업무
 - * 사이버침해사고는 발생 후 상당기간이 지나 밝혀지는 경우도 많아 무사고 증명이 어려움

□ 공공부문 사이버보안 책임성 강화 방안

① (기관장 우선 책임) 정보 유출사고 발생 시 사이버보안 규정 위반에 대한 징계기준을 상향*

* 「공무원 징계령 시행규칙」 개정, 관련 비위에 대한 최소 징계양정 상향 검토

- 감독자(고위직) 문책 대상 위규로 위중한 정보 유출사고 명문화*(~11월) 인사처

* 「공무원 징계령 시행규칙」에 위중한 정보 유출사고의 경우 관련 감독자에게 엄중 책임을 묻는 사항 신설(현재 금품수수, 직무태만에 따른 국민권익침해·재정손실 시 감독자 엄중 책임 규정)

② (기본 사이버보안 수칙 준수 책임) 명확한 징계조치를 위해 현재 단순 분류*된 사이버보안 관련 위규사항을 세분화·구체화한 사이버보안 위규 처리기준**을 마련하여 「국가공무원 복무·징계 관련 예규」에 반영(~12월) 인사처·국정원

* 현행 「국가공무원 복무·징계 관련 예규」의 「XVI. 「보안업무규정」 등 보안법령 관련 비위행위자 처리 지침」에 위반 행위 관련 단순 예시만 나열

** (안) 서비스 개통 전 보안 검토, 보안장비(방화벽 등) 관리 부실 등 기본적 정보보호 수칙 위반, 반복적 규정·수칙 위반, 발견된 보안 문제점 장기간 미조치 등 명시적 징계기준

③ (기관책임 평가체계) 현 ‘사이버보안 실태평가’에 정보 유출사고 시 감점, 사고 신속조치 등 신규지표를 도입하여 실효성 보강 국정원

- ‘중앙행정기관 특정평가(정부혁신)’에 중대 정보 유출사고 발생 시 평가점수 감점 조정사항 추가(‘특정평가 세부지침’ 개정사항, ’27년~) 국조실·행안부·국정원

- ‘지방공기업 경영평가’에 사이버보안 평가지표 신설(‘지방공기업 경영평가 편람’ 개정사항, ’28년도(’27년 실적) 평가~) 행안부·국정원

④ (실태평가 확대) 중앙부처·광역지자체와 협력하여 ‘사이버보안 실태평가’ 대상을 공공부문 모든 기관으로 확대*하고, 평가체계 구축 추진 국정원·중앙부처·지자체

* 평가대상 : (현재) 153개 기관 → (’27년) 기타공공기관(276)·지방공기업(423)·시도 교육청(16) 추가, 868개 기관 → (’28년~) 전체 2,160개 기관

⑤ **(담당자 인센티브)** 중요직무 선정기준에 정보보호 업무 포함* 및 정보보호 업무수당 신설 검토 국정원·개인정보위·인사처·기획처

* 기관에서 중요직무 담당자로 선정시 4~5급 월 15만원, 6급이하 월 10만원 상당의 중요직무급 지급(「공무원보수 등의 업무지침」 개정사항)

- 성과평가(승진) 시 가점 부여*로 정보보호 업무 담당자 우대(~12월) 인사처

* 기관이 승진후보자 명부 작성 시 고려하는 '가점평정 기준표(예시)'에 '정보보호 업무' 포함 (「공무원 성과평가 등에 관한 지침」 개정사항)

⑥ **(전담조직 설치)** 사이버보안 인력을 보강*(~12월)하고 행안부, 중장기적으로 중앙행정기관·광역지자체에 전담조직**을 설치('27년~) 행안부·지자체 하여 기관 내 및 소속·산하기관 사이버보안에 대한 상시적·전문적 지원 강화

* 중앙행정기관 사이버보안 인력 : 완료(개인정보보호 포함 100명 보강, 8.28.), 지방자치단체 사이버보안 인력 : 추진 중(~12월)

** 정보보호 전문성 확보를 위해 민간 정보보호 전문가를 장으로 과·팀 등 구성·운영

⑦ **(안정적 예산확보)** 정보시스템 특성에 따라 정보보호 활동에 필요한 기본적인 소요사항*을 발굴·정리(~10월)하고 국정원, 안정적인 사이버보안 예산 투자 유도 방안을 기획처 등 관계 부처 논의

* (안) 모의해킹 등 정기적 취약점 점검 및 긴급조치, 보안지원 종료된 노후 SW 교체 또는 유료 보안지원 서비스 이용, 민간 클라우드서비스 이용 시 보안 서비스 구독 등