SHIN&KIM
법무법인(유) 세종

해킹 예방·대응력 강화를 위한 범부처 정보보호 종합대책 수립

2025.10.24

최근 전방위적인 해킹 사고로 국민들의 불안이 가중됨에 따라, 정부는 10월 22일(수) 대국민 보고(브리핑)를 통해 국가안보실이 중심이 된 과기정통부, 금융위원회, 개인정보보호위원회, 국가정보원, 행정안전부 관계부처 합동으로 「범부처 정보보호 종합대책」(이하 '종합대책')을 발표했습니다.

최근 분야를 막론하고 해킹 사고가 연이어 발생하고 있는데 정부는 이를 심각한 위기상황으로 인식하고 있으며, 이번 종합대책은 범정부 차원의 유기적인 대응체계를 즉시 가동하기 위한 것이라고 설명하였습니다.

종합대책의 주요 추진 방향 및 내용은 아래와 같습니다. 정부가 이번 종합대책은 현 사안의 시급성을 고려하여 즉시 실행에 옮길 수 있는 단기과제 위주로 제시하는 것이라고 부연한 만큼 관련 기업기관 등은 이에 차질 없이 대응할 수 있도록 사전에 철저한 준비를 하여야 할 것으로 보입니다.

1. 핵심 정보기술 체계(IT 시스템)에 대한 대대적 점검과 상시 취약점 탐지 체계 구축

- 발표 후 즉시 공공·금융·통신 등 국민 대다수가 이용하는 1,600여개* IT 시스템에 대해 대대적인 보안 취약점 점검 추진
  * 공공기관 기반시설 288개, 중앙·지방 행정기관 152개, 금융업 261개, 통신·온라인 플랫폼 ISMS 인증기업 949개 등
- ISMS, ISMS-P를 현장 심사 중심으로 전환, 중대한 결함 발생 시 인증 취소 등 실효성 제고

2. 소비자 중심의 사고 대응체계 구축 및 재발 방지 대책 실효성 강화

- 기업의 보안 해태로 인한 해킹 발생 시 소비자의 입증책임 부담 완화
- 개인정보 유출 사고로 인한 과징금 수입을 개인정보 보호에 활용할 수 있도록 기금 신설 검토
- 해킹 정황이 확인된 경우 기업 신고 없이도 현장 조사가 가능하도록 정부의 조사 권한 확대
- 보안 의무 위반에 대한 과태료·과징금 상향, 이행강제금 및 징벌적 과징금 도입

3-1. 정보보호 투자확대 유도 및 중소기업 지원 강화

- 정보보호 공시 의무 기업을 상장사 전체로 확대
- 정보보호 공시 결과를 토대로 보안 역량 수준을 등급화하여 공개하는 제도 도입
- CEO(최고경영책임자)의 보안 책임 원칙을 법령상 명문화
- CISO(보안최고책임자)의 권한 대폭 강화
- 자체적 보안 역량이 부족한 중소·영세기업 대상으로는 정보보호 지원센터 확대

3-2. 국제 변화에 부합하는 제도 마련 및 환경 조성
• 보안 소프트웨어 설치를 단계적으로 제한하는 대신 다중인증, 인공지능 기반 이상탐지체계 등의 활용을 통한 보안 강화 • 획일적인 물리적 망분리를 데이터 보안 중심으로 본격 전환 • 클라우드 보안 요건 개선
3-3. 보안산업 국가전략 산업화, 사이버안보 인력·기술 육성
• AI 에이전트 보안 플랫폼 등 차세대 보안 기업 집중 육성 • 화이트해커 양성 체계를 기업 수요에 따라 재설계, 정보보호특성화대학을 보안 인재 양성 거점으로 육성하는 등 기능 강화 • 양자내성암호 기술 개발 등 국가적 암호체계 전환 착수
4. 범국가적 사이버안보 협력 강화
• 범부처 위원회인 정보통신기반시설보호위원회(위원장: 국무조정실장)를 통해 주요정보통신기반시설 지정 확대 • 일괄(One-Stop) 신고체계 도입, 조사단별 투입시기 최적화, 상호 정보공유 강화 등 부처별로 파편화된 해킹 사고조사 과정을 체계화 • 국가사이버위기관리단(국가정보원 산하 민관군 합동 조직)과 정부 부처 간 사이버 위협 예방

배경훈 부총리 겸 과기정통부장관 역시 브리핑 과정에서 “과기정통부 등 관계부처는 이번 종합대책이 현장에서 제대로 작동될 때까지 실행 과정을 면밀히 살펴볼 것”이라고 예고하고, “정부는 인공지능 강국을 뒷받침하는 견고한 정보보호 체계 구축을 위해 총력을 기울이겠다”고 덧붙이는 등 정보보호 체계 전반에 대한 강력한 제도 개선 추진 의지를 재차 강조하였습니다.

관계부처는 이번 종합대책과는 별개로, 연내 종합대책의 중장기 과제를 망라하는 「국가 사이버안보 전략」을 수립할 계획인 것으로 확인됩니다.

시사점

- 이번 종합대책에서 가장 두드러지는 내용으로, CEO의 보안책임 법령상 명문화, CISO 및 CPO의 권한 강화, 정보보호 공시 제도 실효성 강화를 비롯해 해킹 사고 등 보안 리스크와 관련한 경영진의 책임이 강화되었다는 점에 주목할 필요가 있습니다.
- 이를 통해 정부는 해킹 사고의 예방 및 대응력 강화를 위해 기업 경영진이 직접 실질적인 행동에 나설 것을 요구하고 있는 것으로 보이며, 따라서 기업으로서는 내부통제 프로세스에 보안 리스크 항목을 반영하고 취약점 관리 체계를 마련하는 등 철저한 대비에 나서야 할 것으로 생각됩니다.
- 관련 기업은 보안의무 위반에 대한 징벌적 과징금 제도 도입, 해킹 사고로 인한 손해배상청구 시 소비자의 입증책임 완화와 관련하여 추후 개인정보 보호법 및 동법 시행령 등 관련 법령의 개정 방향을 지속적으로 모니터링하면서 기업의 책임범위 및 부담능력에 부합하는 합리적 제도가 도입될 수 있도록 대응할 필요가 있을 것입니다.

About Shin & Kim’s ICT Group

법무법인(유) 세종 ICT그룹은 ICT 분야에 차별화된 전문성과 인적 네트워크를 보유하고 있으며, 고객들로부터 최근 수년간 가장 높은 평가를 받고 있습니다. 방송과 통신, 개인정보, 인터넷 IT 분야에서 축적된 역량을 바탕으로 방송·통신·ICT 규제 동향 파악 및 대관, 법제개선·입법컨설팅, 규제영향력 분석과 기업의 전략 수립 등에 대한 종합적인 법률자문을 제공하고 있습니다. 특히 침해사고 대응 등과 관련하여

서도 다양한 업무경험과 전문성을 보유하고 있으므로, 보다 전문적인 내용이나 궁금하신 사항이 있으면 언제든지 연락 주시기 바랍니다.

관련구성원

강신욱
대표변호사

02-316-4059
sokang@shinkim.com

최광희
고문

02-316-4651
khchoi@shinkim.com

장준영
변호사

02-316-4985
jyojang@shinkim.com

안정호
변호사

02-316-2891
jhahn@shinkim.com

노진홍
변호사

02-316-1639
jhnoh@shinkim.com

윤호상
변호사

02-316-2584
hsyoon@shinkim.com

주해인
변호사

02-316-1825
hiju@shinkim.com

도지수
변호사

02-316-1930
jsdo@shinkim.com

Copyright SHIN & KIM LLC. All rights reserved.