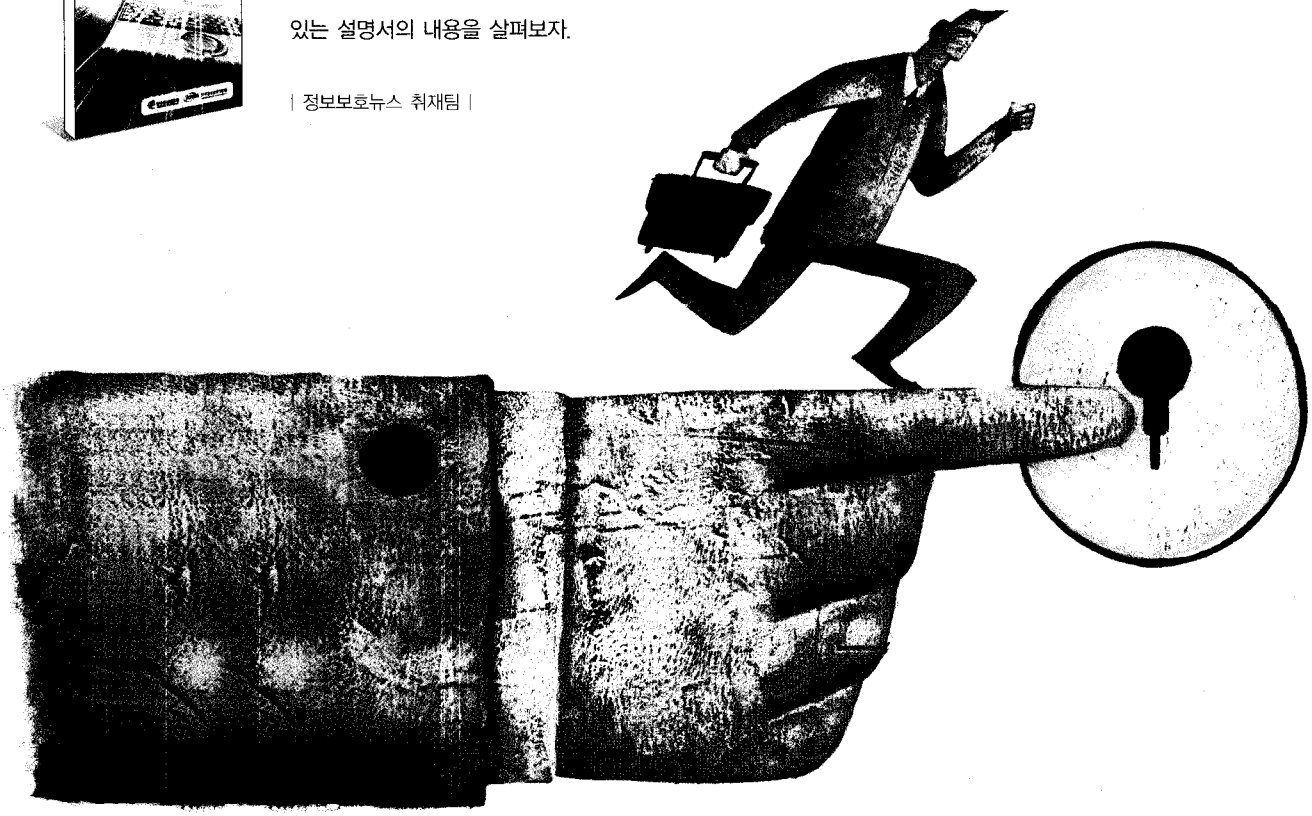
손에 잡히는 암.호.정.책

| 암 호 정 책 수 립 기 준 설 명 서 발 간 |

방통위와 KISA가 지난 12월 '암호정책 수립 기준설명서'를 발간했다. 약 30페이지로 구성된 이 설명서는 암호정책 기준, 세부기준에 대한 상세해설, 암호정책 모범사례 등을 수록, 기업 정보보호 담당자들이 필요 시 손쉽게 참고할 수 있도록 했다. 기업 정보자산을 보호하기 위한 암호정책의 기준을 제시하고 있는 설명서의 내용을 살펴보자.

| 정보보호뉴스 취재팀 |



각 기업과 기관이 보유한 주요 정보자산을 내외부의 위협으로부터 안전하게 보호하기 위해서는 적절한 암호제품 및 서비스 도입을 위한 암호정책을 수립해야 한다. 암호정책과 관련된 사항은 이미 기업 정보보호관리체계를 심사하는 ISMS 인증기준에서도 명시돼 대상기업의 암호정책수립 여부를 확인하는 등 암호정책의 중요성은 지속적으로 높아지고 있다.

이와 달리, 일부 기업들은 자사의 암호정책 수립과정에서 안전하지 않은 암호기술을 도입함으로써 주요 정보자산의 노출위협이 발생하는 등 암호정책의 적절성 및 실효성에 대한 문제가 지속적으로 제기돼 왔다. 이번에 발간된 '암호정책 수립 기준설명서'는 정보보호관리체계 관련 제도 및 표준 요구사항에 적합한 상세 암호정책 수립기준을 제공하고 있다는 점에서 의미를 갖고 있다.

No	통제목적	통제내용	점검항목	설 명
9.1	암호정책	암호사용에 대한 정책을 수립하여야 한다.	문서화된 암호정책이 있는가?	적절히 승인된 문서화된 암호정책(지침)이 존재하여야 한다.
			암호정책에는 다음 사항을 포함하고 있는가? • 암호를 사용해야 하는 경우 • 경우에 따른 암호화 방법 또는 필요한 신뢰정도 • 안전한 암호 프로그램의 배포관리 • 전자서명, 부인봉쇄, 서비스의 신뢰정도	암호정책에는 어떤 경우에 암호화 방법을 사용할 것인지를 명시하고 각각의 경우, 필요한 암호화의 방법과 수준(강도)을 명시하여야 한다. 채택할 수 있는 암호화 방법에는 다음과 같은 것들이 있다. • 비밀성을 위한 암호화 • 전자서명 • 부인봉쇄 서비스의 사용
9.2	암호사용	암호정책에 따른 암호사용 시 적절한 알고리즘의 유형, 신뢰성 및 키 길이를 결정하여야 한다.	암호정책에 따라 암호화가 필요한 경우, 적절한 알고리즘과 키 길이를 결정하여 사용하고 있는가?	암호정책에서 확인한 대로 직원들이 각 경우에 대하여 적절한 알고리즘과 적절한 키 길이로 암호화하고 있는지 확인한다.
			암호정책에는 전자서명 또는 부인봉쇄 서비스 시 암호화의 적용에 대한 내용을 포함하고 있고, 이에 따라 이행하고 있는가?	전자서명이나 부인봉쇄 서비스를 제공하는 서비스 제공자의 신뢰성을 확인한다. 암호저액에서 확인한 대로 직원들이 각 경우에 대하여 적절한 알고리즘과 적절한 키 길이로 암호화하고 있는지 확인한다.
9.3	키 관리	암호 키에 대한 관리지침, 절차 및 방법을 마련하고 필요시 복구방안을 마련하여야 한다.	암호 키에 대한 관리지침과 절차 및 방법이 마련되어 있고, 이에 따라 관리되고 있는가?	키를 안전하게 관리하고 복구하기 위한 지침, 절차, 방법이 마련되어야 한다.

정보보호관리체계 인증에서의 암호통제 항목 예시

"가상의 기업을 통해 구체적인 사례 소개"

총 3개의 Part로 구성된 해설서의 가장 핵심적인 부분은 암호정책 수립 기준 및 해설 부분. 총칙 및 책임사항, 암호관리, 키 관리, 문서 및 기록 등 4개 항목으로 구성된 암호정책 수립 기준에서는 총 17개 세부기준을 명시하고 있으며, 국내외 정보보호관리체계 관련 제도 및 표준에서 공통적으로 요구하는 항목을 소개하고 있다. 항목 기준뿐만 아니라, 각 기준의 필요성을 비롯해 암호정책 수립을 위한 국내외 권고 암호알고리즘, 안전한 패스워드 기준 등을 구체적 예시를 통해 소개했다는 점도 이번 해설서의 특징이다. 이와 함께 기업 및 기관이 실제 암호정책을 수립하는 과정에서 도움을 받을 수 있도록 가상의 기업을 설정해 암호정책 수립기준을 소개함으로 일반적인 해설서가 갖고 있는 딱딱함 대신, 보다 현실적인 내용으로 구성됐다는 점이 눈에 띈다.

한편, 이번에 출간된 해설서는 보안 컨설팅, 안전진단 및 정보보호관리체계 인증 업체 및 인증 심사원 등에게 배포됐으며, 'KISA 홈페이지 → 정보보호관리체계 인증 → 자료실'에서 PDF 형태로 다운로드 받을 수 있다.

이번 해설서 발간에 대해 KISA 관계자는 "이번에 발간된 암호정책 수립기준 설명서와 함께, '암호이용가이드라인', '패스워드 선택 및 이용가이드' 등을 함께 참고한다면 기업은 더욱 강력한 암호정책을 수립 적용할 수 있을 것"이라고 설명했다. S