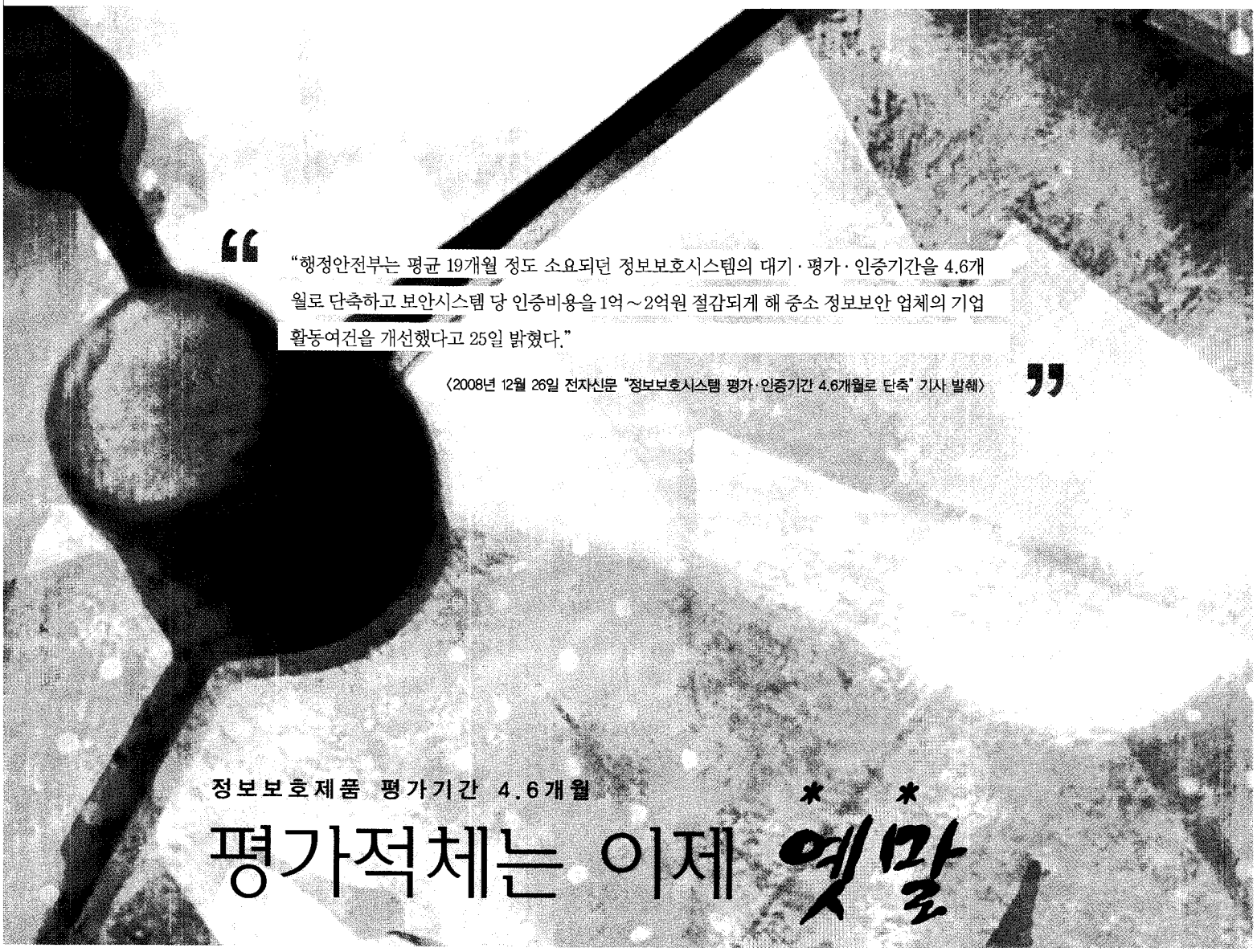


"행정안전부는 평균 19개월 정도 소요되던 정보보호시스템의 대기·평가·인증기간을 4.6개월로 단축하고 보안시스템 당 인증비용을 1억~2억원 절감되게 해 중소 정보보안 업체의 기업 활동여건을 개선했다고 25일 밝혔다."

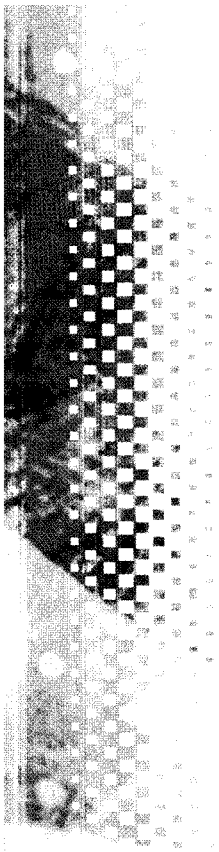
〈2008년 12월 26일 전자신문 "정보보호시스템 평가·인증기간 4.6개월로 단축" 기사 발췌〉

정보보호제품 평가기간 4.6개월

# 평가적체는 이제 옛말

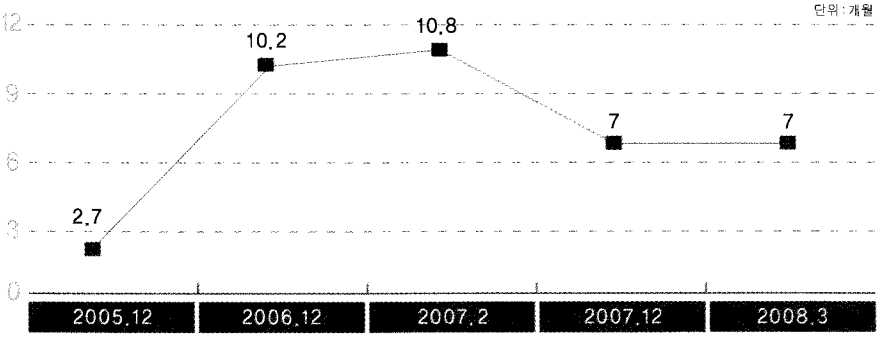
지난 2008년 12월말 정보보호 시스템에 대한 보안성 평가의 소요시간과 비용을 절감하기 위한 정책이 등장하면서 이에 대한 기사들이 등장했다. 보안성 평가과정에 있어 비용과 시간 절감은 정보보호 업계로서는 반가울 수밖에 없는 일. 그렇다면 실제 그 과정과 성과는 어떠했을까.

글 **오남호** | 평가기획팀 선임연구원 _ nhooh@kisa.or.kr



## 정보보호시스템 평가적체

2006년 공공기관에 납품되는 모든 정보보호시스템이 정보보호시스템 평가·인증(이하 CC평가·인증)을 받도록 의무화됨에 따라, CC평가·인증 수요가 급증해 평가적체가 발생하기 시작했다. 평가적체 현상이 발생하기 시작한 이후 이를 해소하기 위해 인증서 유효기간 폐지를 통한 재평가 수요축소(2007년), 국내용 평가제 및 복수 평가기관체제 도입(2008년) 등을 추진해 평가대기 기간의 상승 억제 노력이 이어졌다. 그러나 평가수요에 적기 대응하고 적체를 해소하기에는 다소 부족했다.



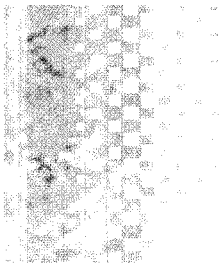

▲ 평가대기 기간 변동 추이(2008년 4월 이전)

평가적체 현상이 발생하는 원인으로는 CC평가를 수행할 수 있는 전문 평가인력 부족과 그로 인한 민간 평가기관의 평가반 확대 어려움, 평가기간이 긴 EAL4 위주의 평가수요, 평가 신청업체의 제출물 수준저하 등을 지적할 수 있다.

이와 같은 문제는 정보보호업체 제품검증에 소요되는 기간의 장기화로 경제적 부담이 가중되고 제품 경쟁력도 뒤떨어지게 되는 원인으로 이어졌으며, 여기에 정부/공공기관은 최신 정보보호기술이 적용된 시스템 도입이 적기에 이뤄지지 않아 빠르게 진화하는 사이버 공격에 효과적으로 대응하기 어렵게 되는 등 평가적체 현상으로 인한 부정적 여파가 적지 않았다.

## 정보보호시스템 평가·인증체계 개선

이 같은 문제를 해결하기 위해 정책기관과 인증기관, KISA가 협력해 정보보호시스템 평가·인증체계를 개선하고, 정보보호시스템이 국가·공공기관에 납품되기까지 걸리는 기간을 크게 단축시키는 방안을 마련했다.



| 구 분 | 총 소요시간 | | 평가대기 | | 평가·인증 | | 적합성 검증 |
|---|---|---|---|---|---|---|---|
| 이 전(2008년 3월) | 19개월 | = | 7개월 | + | 8개월 | + | 4개월 |
| 1단계(2008년 9월) | 10개월 | = | 5개월 | + | 5개월 | + | 0개월 |
| 2단계(2009년 1월) | 6개월 | = | 2개월 | + | 4개월 | + | 0개월 |

▲ 정보보호시스템 평가·인증체계 개선 추진 목표(2008년 4월)

먼저, 전문 평가인력 부족으로 평가자 확보 및 평가반 확대가 어려웠던 점을 극복하기 위해 정부예산을 투입, KISA를 통해 계약직 평가인력을 양성하도록 했다. 양성된 평가인력은 단기적으로는 KISA 평가반 확대에 활용하고 장기적으로 전문 평가인력 부족으로 어려움을 겪던 민간 평가기관에 평가인력을 확보할 수 있는 길을 마련해 실질적인 복수 평가기관 체제 정립으로 이어졌다.

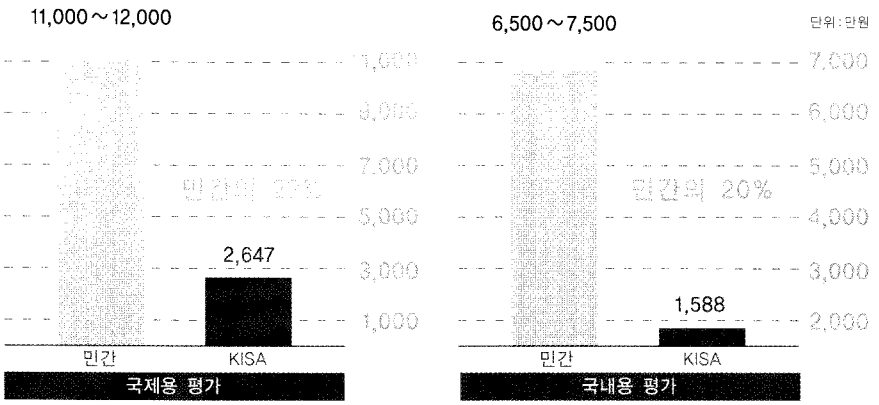
또한 기존 2인 1개반 1개 제품 평가원칙을 3인 2개반 2개 제품평가가 가능하도록 유연하게 조정하고 양성된 평가인력을 활용해 17개 반으로 운영하던 평가반을 2008년 12월까지 27개반으로 확대하기로 해 대기 중이던 제품의 조기 평가착수가 가능해졌다.

한편, 제품 평가적체가 발생된 원인 중에는 정보보호시스템 평가·인증 등급의 문제도 있었다. 공공기관의 요구사항, 업체들간의 경쟁 등으로 인해 제품 대부분은 EAL4로 거의 획일화돼 있었던 것이다. 이로 인해 평가기간은 장기화되고 EAL4 등급에서 요구하는 방대한 양의 제출물을 준비하는 업체의 부담은 증가할 수밖에 없었다. 정책기관과 인증기관은 정보보호시스템별 평가·인증 등급을 합리적으로 조정해 EAL2 이상 인증을 받은 제품도 공공기관 납품이 가능하도록 했으며, 보호프로파일 등급을 현실화해 평가 신청업체들이 EAL2~4까지 평가 신청할 수 있도록 유도했다. 즉, 과거처럼 평가기간이 긴 EAL4 평가·인증 등급을 굳이 획득하지 않아도 공공기관에 제품을 납품할 수 있는 길을 만들어놓는 것이다.

| 구 분 | 현 행 | 개 선 |
|---|---|---|
| 신청업체 제출서류<br>(3,900쪽 ➔ 2,000쪽) | **총 17종 제출**<br>* 보안목표명세서, 시험서<br>* 설명서 4종, 개발문서 5종<br>* 생명주기관련 4종, 취약성 관련 2종 등 | **총 10종 제출**<br>* 보안목표명세서, 시험서<br>* 설명서 4종, 개발문서 3종<br>* 생명주기관련 1종, 취약성 관련 1종 등 |
| 평가기간<br>(6개월 ➔ 2~4개월) | **EAL4(국내용)**<br>* 약 6개월 소요 | **EAL2~EAL4(국내용)**<br>* EAL2 : 약 2개월<br>* EAL3 : 약 3개월<br>* EAL4 : 약 4개월 |
| 평가항목<br>(88개 ➔ 48개) | * 형상관리 : 23항<br>* 배포 : 9항<br>* 일반적/인적/물리적/절차적 보안대책 : 56항 | * 형상관리 : 8항<br>* 배포 : 5항<br>* 일반적/인적/물리적/절차적 보안대책 : 35항 |
| 기능평가<br>(35개 ➔ 8~9개) | * 보안감사, 사용자데이터 보호, 식별 및 인증, 보안관리, TSF 보호 등 전체(약35개) 기능 평가 | * 제품별 8~9개 주요 보안기능 선택 평가<br>※ 예: IPS 경우, 접근통제 2개, I&A 2개, 감사 2개 및 보안관리 2개 |

▲ 평가기간 및 제출물 완화 세부내용

여기에 KISA 평가 수수료의 일부 현실화를 추진해 민간 평가기관의 수익성 개선 및 신규 수요 분산을 유도했다. 과거 KISA는 영세한 국내 정보보호업체의 지원을 위해 평가 수수료의 저가 정책을 유지했지만, 민간 평가기관과 비교해 지나치게 저렴한 수수료로 인해 평가신청 수요가 적절히 분산되지 못하고, KISA로 집중되는 등 평가적체의 한 요인으로 작용했다.




▲ KISA 수수료 정책 조정 전 민간 평가기관과의 수수료 비교(2008년 4월)

이 같은 문제를 해결하기 위해 KISA는 국제용 평가 수수료를 민간 평가기관과 동일한 수준으로 현실화하고, 국내용 평가 수수료는 중소기업의 경우 연 1건에 한해 50% 할인을 적용하고, 초과 시 민간 평가기관과 동일한 원가 수준으로 부과하도록 조정했다. 민간 평가기관 입장에서는 KISA의 평가 수수료가 일정부분 비슷하게 조정됨에 따라 평가신청 수요의 분산을 기대할 수 있게 됐다.

## 개선계획의 성과

정책기관과 인증기관, KISA를 포함한 평가기관은 앞서 설명한 정보보호시스템 평가·인증체계 개선 계획을 추진해 2008년 4월 기준으로 공공기관 납품까지 19개월 걸리던 기간을 4.6개월까지 단축해 2006년부터 지속된 정보보호시스템 평가 적체를 완전 해소했다.

장기간 문제가 됐던 평가 대기기간은 7개월에서 1개월 이내(2008년 12월 기준)로 6개월이 단축됐으며, 평가기간은 8개월에서 3.6개월(2008년 12월 기준)로 4.4개월 단축됐다. 또한 보안적합성 검증제도가 지난 2008년 4월 이후 先검증 後도입에서 '先도입 後검증'으로 변경되면서 4개월여의 적합성 검증기간이 단축되기도 했다.

| 구 분 | 총 소요시간 | | 평가대기 | | 평가·인증 | | 적합성 검증 |
|---|---|---|---|---|---|---|---|
| 2008년 3월 | 19개월 | = | 7개월 | + | 8개월 | + | 4개월 |
| 2008년 12월 | 4.6개월 | = | 2개월 | + | 3.6개월 | + | 0개월 |

▲ 정보보호시스템 평가·인증체계 개선 추진 성과(2008년 12월)

이로 인해 중소 정보보호업체는 제품 개발 후 판매까지 14개월이 단축되어 평가에 소요되는 경비를 대폭 경감할 수 있게 돼 어려운 국내외 경제상황에서 기업 경영수지 개선에 기여할 것으로 기대된다. 또한 정부/공공기관은 최신 정보보호기술이 접목된 정보보호시스템을 적기에 도입할 수 있게 됨에 따라 날로 증가하고 있는 각종 사이버 위협에 신속히 대응할 수 있게 됐고, 국가 정보보호수준도 향상될 것으로 기대하고 있다. S