

# 국제보안인증 수용해도 '소스 공개'는 유효?

보안성 검토

CCRA

올해 우리나라의 CCRA 가입이 예상되면서 국내 보안 시장에 미칠 파장에 대해 관심이 쏠리고 있다. 글로벌 보안 업체들은 우리나라의 CCRA 가입에 따라 그간 외산 제품에 대해 진입 장벽이 높았던 국내 공공 시장에 진출할 수 있게 되고 더 나아가 공공 시장이 자유경쟁 체제로 바뀔 것으로 기대하고 있다. 그러나 국정원의 보안성 검토라는 장벽이 여전히 남아 있어 CCRA 가입을 무색케 할 수도 있다는 우려가 대두되고 있다. 게다가 KISA와 국정원이 CCRA EAL 인증 대상이 아닌 안티바이러스 제품에 대해서도 보안성 검토를 요구하고 있어 새해 벽두부터 보안 업계가 술렁이고 있다.

■ 유윤정 기자 yjyoo@bnimedia.com

**올** 해 상반기 내 우리나라가 CC 인증서 발행국(CCRA)이 될 확률이 높아짐에 따라 국산 보안 어플라이언스 제품으로 제한됐던 공공 시장의 입찰 기회가 외산 글로벌 보안 업체에게도 주어질지 귀추가 주목되고 있다.

국내 공공 시장은 외산 보안 업체들에게는 매우 제한적인 시장이었다. 심지어 외국 보안 업체들은 공공 시장을 '버린 시장'이라고도

얘기해 왔다. 공공 시장에 들어가기 위해서는 국정원의 K4인증, CC 인증 등을 받아야 하는데 이러한 인증을 받기 위해서는 소스 코드를 국정원에 제출해야 하기 때문.

이러한 소스 코드 제출 요구에 대해 외산 글로벌 업체들은 고유한 기술을 공개하는 것이

라며 "자사의 지적 재산권인 소스 코드 공개는 기술 진보를 내주는 것이나 다름없다"며 소스 코드 제출을 거부해 왔다.

하지만 우리나라가 올해 상반기 국제 공통 평가기준 상호인증협정(CCRA) 가입을 눈앞에 두고 지난해 말 마지막 관문인 실질 심사에 돌입하는 등 CCRA 가입에 박차를 가하고 있어 얘기는 달라질 것으로 전망되고 있다.

국정원 관계자는 "CCRA 가입 절차상 실질

## CCRA란

CCRA에 가입하면 각 국은 보안 제품 평가 인증 기준을 CC로 표준화하게 된다. CCRA의 경우 인증서를 발행하는 인증서 발행국(CAP), 인증서는 발행하지 않고 이를 인정하는 인증서 수용국(CCP)으로 이원화돼 있는데 우리나라는 인증서 발행국을 신청한 상태다.

인증서 발행국이 되면 국내에서 발행된 정보보호시스템 평가 인증서가 해외에서도 인정받을 수 있게 된다. 이에 따라 국산 보안 솔루션 업체들도 해외 인증을 별도로 받을 필요 없이 국내 인증만으로도 세계 기준을 만족시키게 되므로 국산 업체들의 해외 진출에 활로를 펼쳐줄 것으로 기대되고 있다.

반면, 상호 협정을 통해 외국에서 CC 인증을 받은 제품에 대해서도 국내에서 인정해야 함에 따라 글로벌 보안 업체들은 현재처럼 국내 고유의 보안 제품 평가 인증을 받을 필요가 없다. 따라서 글로벌 보안 솔루션 업체들은 그간 가로막혔던 국내 공공시장 진출이 이전보다 수월해질 것으로 전망된다.

심사가 끝나고 75일이 지난 후 가입국 전체 투표가 진행되는 일정을 감안하면 우리나라는 이르면 올해 3월께, 늦어도 상반기 안에 CAP가 될 것이다. 현재 국정원과 KISA는 실사의 원활한 진행을 위해 최선을 다하고 있다"고 강조했다.

**국내 업체 "해외 진출 활로" 반응 엇갈려**

하지만 CCRA 가입에 따른 이러한 장밋빛 전망에도, 실제로 시장에 뛰고 있는 국산 보안 어플라이언스 업체와 외산 글로벌 보안 어플라이언스 업체의 반응은 각각 엇갈리고 있다.

정통부, 행자부, 외교부, 산림청, 전국지방경찰청, 경찰청, 전국시도교육청, 교육학술정보원(NEIS망) 등 200개의 공공기관 레퍼런스 사이트를 확보한 윈스테크넷은 "영향을 다소 받긴 하겠지만 지난해 하반기부터 국산 제품의 기능이 매우 향상됐기 때문에 공공 시장에서 글로벌 제품과 맞붙는다고 해도 국산 제품 공급이 크게 타격받지는 않을 것"이라고 강조했다.

외산 업체들 역시 아직은 국산 업체들에게 더 유리할 것이라는 입장이다. CCRA 가입이 국내 업체들의 해외 진출에 좋은 기회로 작용할 것이며, 어차피 국내 금융 및 공공 시장은 국정원의 보안성 검토에 의해 보호를 받기 때문에 국내 시장에서도 잃을 게 없다는 것이다.

탐레이어코리아 김경석 지사장은 "국산 업체들은 이미 국내 공공기관에 상당수 보안 장비들을 공급했다. 이미 기득권을 가진 입장에서 큰 타격은 없을 것으로 생각한다"고 전했다.

CCRA에서 포티게이트 전 제품에 대해 EAL4를 받은 포티넷코리아 역시 "CCRA 가입 후에도 외산 업체들이 국내 공공기관 시장에서 수월해지는 점은 없다. 국정원의 보안성 검토가 남아 있는 한, 아무리 좋은 취지라 할 지라도 외산 업체들에게는 진입 장벽으로 남을 것으로 생각한다"고 강조했다.

반면 해외 진출 확대에 대해서는 국내 업체들도 반신반의하고 있다. 시큐아이닷컴은 "CCRA 가입으로 국산 제품들의 해외 시장 진출에 긍정적인 영향을 펼칠 것으로 기대하고는 있지만 국내 보안 업체들 중에 얼마나 많은 업체들이 수출을 할 수 있을지 의문"이라고 잘라말했다. 국산업체들이 공공기관 프로젝트를 저가 수주하면서 출혈경쟁을 하고, 이로 인한 경쟁력 약화를 다시 공공 시장에 기대 해결 하려는 악순환의



탐레이어코리아 김경석 지사장은 "소스 코드 공개는 결국 칩 설계를 공개하라는 얘기라며, 이는 설계 기술을 100% 공개하는 것과 같으므로 인증받지 않은 모듈에 따른 부분별 공개도 어렵다"고 전했다.

고리가 선순환의 고리로 바뀌지 않는 이상 CCRA 가입은 시기 상조라는 입장을 보였다.

외산 보안 어플라이언스 업체들은 CCRA에 가입을 하더라도 공공 시장에 자사의 어플라이언스가 공급되기는 쉽지 않을 것으로 예상하고 있다. 우리나라가 CCRA에 가입을 하고 CCRA에서 EAL 인증을 받은 제품이라고 하더라도 국정원과 KISA가 내세우는 보안성 검토라는 또 하나의 장벽이 있기 때문.

라드웨어코리아 박진성 이사는 "CCRA 가입 명분도 좋고 타당성도 있지만 허울로 느껴진다"며 "CCRA에 가입된다고 하더라도 보안성 검토라는 또 다른 절차가 있기

**안티바이러스 업계 덮은 또다른 CC 인증 '먹구름'**

지난해 12월 9일 KISA는 안티바이러스 제품에 대해서도 보안성 검토 기준을 확대 적용한다고 백신 업체들을 소집해 발표했다. 국산 업체인 안철수연구소, 하우라 그리고 외산 업체인 시만텍과 트렌드마이크로 등 모두 CC 인증을 받아야 하는 것.

하지만 국제적 평가 기관인 CCRA에서도 안티바이러스 제품에 관해 EAL 인증을 요구하거나 수행한 적이 없어 CCRA에 가입이 된다고 하더라도 상호 협정의 이익을 받을 수 없다. 또한 안티바이러스 제품의 경우 검색 엔진이 생명이기 때문에 소스 코드를 공개하는 것은 말이 안 된다는 것이 국산 업체나 외산 업체의 동일한 주장이다.

안철수연구소의 조시행 상무는 "공공기관에 보안 장비를 납품하려면 CC 인증을 받아야 하는데, 국내 업체들로서도 CC 인증은 부담이다. 비용도 많이 들 뿐 아니라 인증 완료까지 소요되는 기간도 6-8개월 이상이다"며 "소스 코드를 국정원에 공개해야 할지는 심각하게 고려해야 할 사안"이라고 전했다.

국산 업체인 안철수연구소의 반응도 부정적인데 외산 업체들의 반응은 더욱 부정적일 수밖에 없다.

한국맥아피는 "안티바이러스 제품에 대해 CC 인증을 요구해 당혹스럽다. 세계 어떤 안티바이러스 제품도 CC 인증을 받은 사례가 없었다"며 "12월 9일에 KISA에서 안티바이러스에 관련해 설명회를 열었다. 일단 본사가 한국을 주요 전략 시장으로 여기고 있기 때문에 보안성 검토가 가능할 수도 있지만 PP의 구성, 등급 범위, 보안성 검토 방법론, 검토 가능 항목 등에 관련해 KISA나 국정원 쪽에서 명확한 가이드라인을 제시하지 않아서 어떻게 될지는 지켜봐야 할 것 같다"고 전했다.

시만텍도 안티바이러스 제품 중에 CC 인증을 받은 제품은 없으며 국제적으로 바이러스 제품의 경우 CC 인증을 받을 수가 없는데 CC 인증을 받으라고 요구하는 국내 공공기관을 이해할 수가 없다고 전했다. 시만텍 도영창 부장은 "소스는 회사의 기술력과 노하우가 결집돼 있는 것인데 공개하라는 것은 말도 안 된다"며 "국정원에서는 소스를 검토한 직원이 퇴사후에 동종 업계에서 일할수 없도록 한니까 안심하라고 얘기하지만 리스크가 크다고 생각한다"고 강조했다.

국내의 CC인증 현황

국산(국정원 통해 인증)			외산(CCRA 통해 인증)		
업체	인증제품	등급	업체	인증제품	등급
원스태크넷	PS V4.0 시리즈	EAL3+	시스코	DS 4200 시리즈	EAL2
아울림정보기술	사큐어웍스 PS월 1000 V4.0	EAL4		DSM2	EAL2+
	2000/3000 V4.0	EAL3+		시스코 사큐어 PFX 501, 506, 506E	EAL4
	사큐어웍스 V3.0	EAL3+		515, 525, 535, 1720, 1750, 2610	
	사큐어웍스@월 V3.0	EAL3+		2611, 2612, 2613, 2620, 2621	
	사큐어웍스@서버 V1.0	EAL3+		3620, 3640, 3660, 7120, 7140	
	사큐어웍스 V3.0 for SMOG	EAL3+		7204, 7206	
	사큐어웍스 1000/2000/3000 V4.0	EAL3+	포타넷	포타넷 전 시리즈	EAL 4+
퓨처시스템	사큐웨이스위트 6000 V3.0 +PS	EAL3+	맥아피	인트루질드 1200/2500/4000	EAL 3
	사큐웨이스위트 6000 V3.0	EAL3+	노키아	노키아 IP130, IP360, IP360	EAL 4
	사큐웨이스위트 2000 V2.0	EAL3+		IP260, IP266, IP360, IP365,	
사큐아이닷컴	NMG 50/100/200/500 V1.0	EAL3+		IP380, IP1220, IP1260, IP2250	
	NMG PS 2000 V1.3	EAL3+	리드웨어	AS 전 시리즈	EAL 2
LG엔시스	세이프존PS V3.0	EAL4			(EAL 3로 변경신청 중)
	세이프존PS V2.0	EAL3+	탐레이어	DS 밸런서 V2.2	EAL2
사큐브	사큐브 TOS 2.0	EAL3+	시만텍	시만텍 게이트웨이 사큐리티 400 시리즈 v2.1	EAL2
	사큐브 TOS V2.0 for HP-UX	EAL3+		시만텍 게이트웨이 사큐리티 5400 시리즈 v2.0	EAL4
	사큐브 TOS 2.0 for AX	EAL3+	트렌드마이크로	트렌드마이크로 인터스캔 바이퍼스월 352, 356	EAL 4
레드게이트	레드캐슬 v2.0	EAL3+			
	레드캐슬 v2.0 for HP-UX	EAL3+			
	레드캐슬 v2.0 for AX	EAL3+			
타렉스소프트	시스코 OS 솔라리스 9 V2.0	EAL3+			
넥스지	V-포스 1200 V1.0	EAL3+			
인프니스	솔라게이트 VPN-ng200 V1.0	EAL3+			

때에도 소스 코드 제출 요구가 없으며 현재까지 어느 CCRA 가입국에서도 적용하지 않고 있는 절차다. CCRA 가입이 된다면 한국에서도 타 가입국과 동일한 절차를 따라야 한다고 생각한다"고 전했다.

이같은 우려에 대해 국정원 관계자는 "CCRA 가입에 따라 CC 인증을 이증으로 받지 않도록 하기 위해 보안성 검토에 대한 지침을 수정중에 있으며 이 기준은 곧 공식적으로 발표될 예정"이라고 전했다. 또 "CCRA에서 EAL 인증을 받은 외산 보안 어플라이언스의 경우 여러 개의 모듈 중 안전하다고 인증을 받은 모듈에 관해서는 소스 코드를 제출하지 않아도 되며 인증을 받지 않은 모듈에 대해서만 소스 코드를 제출하는 방향으로 추진하고 있

때문에 별로 기대하지 않고 있다. 인증국만 신청하면 되는데 발행국까지 돼서 더욱 난항을 겪을 것으로 보인다"고 전했다.

“해결 열쇠”는 개정되는 보안성 검토 기준

국정원에서 아직 보안성 검토에 대한 기준을 확실히 정의하지 않은 상황이기 때문에 CCRA 가입 후 남겨진 보안성 검토의 정확함의 기준에 따라 시장 상황은 달라질 수 있을 것으로 업계는 예상하고 있다.

CCRA에 가입을 하고도 또 다시 국내에서 CC 인증을 받아야 한다면 외산 업체들은 두 번 인증을 받아야 하는 격이므로 CCRA 가입 자체에 의미가 없어진다. 외산 업체들은 "CCRA에 가입을 했고 CC 인증을 받았음에도 불구하고, 보안성 검토에서 또 한번 소스 코드를 제출해야 한다면 CCRA라는 기관이 '바보'가 아닌 이

상 국제적인 협약에 위배되는 것"이라며 국내에서 받은 CC 인증을 통해 해외로 진출하는 국산 업체들도 해외에서 소스 코드를 공개하고 또 한 번 인증을 받는 역차별의 경우가 발생할 수 있다고 우려했다.

한국쓰리콤의 강정민 과장은 "소스 코드를 봐야만 안심하겠다는 국정원의 입장을 이해하기 힘들다. 세계 어느 나라에서도 공공기관 전체에서 소스 코드 제출을 요구하지 않는다"며 "제품의 안정성을 판단하는 데 소스 코드가 유일한 잣대인 것은 아니다. 입장을 바꿔놓고 생각하면 국산 업체들이 해외 시장에서 똑같이 역차별 받을 수도 있다"고 전했다.

한국맥아피의 이해영 부장도 "CCRA 가입국인 미국, 일본 등에서도 CC 인증을 받은 제품에 대해서는 별도의 소스 코드 제출을 요구하지 않는다. 미국의 국방부, CIA, NSA에 납품할

다"고 설명했다.

여기에 대해 외산 업체들의 반응은 엇갈린다. 일정 부분의 소스 코드 제출도 어렵다는 업체와, 그나마 다행이며 외산 업체에게 유리하게 작용할 것이라는 업체도 있다.

포타넷코리아는 "외산 업체 입장에서 대단히 반가운 일이다. 이런 방식대로라면 모듈에 대해서만 소스 코드를 공개, 인정받으면 되고, 공정한 시장 경쟁을 유도할 수 있어 외산 업체에게는 좋은 기회로 작용할 것으로 예상된다"며 "그러나 모듈과 기능의 범주를 확실히 구분하는 작업이 선행돼야 한다"고 지적했다.

하지만 탐레이어와 같은 업체들은 대부분의 보안 장비가 ASIC 기반의 하드웨어로 디자인돼 있으므로 소스 코드 공개는 결국 칩 설계를 공개하라는 얘기라며, 이는 설계 기술을 100% 공개하는 것과 같으므로 부분별 공개도 어렵

다는 입장이다.

또 국정원 보안성 검토 지침의 타당성 여부 이전에, 국정원 CC에 대한 원천적인 문제 제기도 이어지고 있다. 국정원 CC가 금융, 공공 등 정부 관련 기관의 좋은 보안 장비를 도입하자 는 취지라고 하지만 근본적으로 보호 무역주 의의 일환으로 만들어진 제도이기 때문에 어 떤 형태로든 글로벌 업체들에게는 부담이 된다는 것이 해당 업계의 중론이다.

한 관계자는 "국정원의 보안성 검토 제도가 기존보다 많이 악화된다고 해도 완전히 없어 지지 않는 한, 시장의 공정 거래를 저해하는 요 인으로 남을 것"이라고 전했다.

**"제품으로 평가 받는 것이 상호 이득"**

업계는 국정원과 KISA가 가입의사를 밝힌

후부터 7년 이상을 표류해 온 CCRA 가입을 더 이상 미룰 수는 없다고 강조하고 있다. 또한 보 안성 검토가 남아 있긴 하지만 CCRA 가입으로 인해 공공 시장의 폐쇄적 제한성은 조금 풀릴 것으로 기대된다. CCRA의 발행국 및 인증국까 지 된 이상 우리나라도 더 이상 글로벌 기준을 따라가지 않을 수는 없기 때문이다.

글로벌 업체들은 한국의 기업 고객들이 최 고의 제품을 선택할 수 있는 기회를 주는 것이 올바른 정책이며, 이에 따라 국내 솔루션 업체 가 성장할 수 있는 터전이 마련될 것이라고 주 장한다. K4까지 거슬러 올라가서 지금까지 국 산 업체들을 10년이나 보호해 왔는데, 현재 살 아남은 곳이 몇 군데나 되라는 것.

포티넷코리아 이종열 부장은 "국내 보안 시 장 규모가 작고, 정보 유출 가능성 때문에 정부

가 외산 제품 사용에 민감하게 반응하고 있으 나 국산 업체에 대한 보호는 이제 어느 정도 이 뤄졌다고 본다. 또 현실적으로 정보 유출은 사 람에 의해서 이뤄지며, 시스템에 의한 정보 유 출은 매우 제한적이다"고 강조했다.

이들의 주장은 지금껏 국내 업체들이 나라 가 보호해 주는 시장에서 땅 짚고 헤엄치기식 으로 사업해 왔기 때문에 치열한 기술 개발 투 자나 노력이 없었고, 안일한 자세로 현상 유지 만 해온 까닭에 기술 개발 중심의 외산 업체에 밀려날 수밖에 없었다는 것이다. 이로 인해 국 산 보안 솔루션의 기술력이 글로벌 제품보다 뒤쳐지는 악순환으로 이어졌다는 것.

시스코코리아 장성현 차장은 "우산 속에 가 려지면서 너무 많은 보안 업체들이 난무했고 기술 개발보다는 출혈 경쟁이 많이 이뤄졌다. 당장은 CCRA 가입으로 국산 업체들이 피해 를 받겠지만 향후에는 좋은 영향을 미치게 될 것으로 기대하며 가치 있고 기술력 있는 국산 업체들만이 살아남을 수 있을 것"이라고 강조 했다.

더 이상 국내 시장만으로는 사업 확장과 기 술 발전이 힘들어 글로벌 무대로의 진출을 과 제로 안고 있는 현재, 우리나라의 CCRA 가입 은 국내 업체들에게는 본격적인 국제 무대 진 출의 교두보가 될 수 있다.

한 예로, 삼성전자의 경우 네트워크 장비 제 조 판매 사업에 뛰어들었지만 국내 시장만 대 상으로 했기에 수익성에 문제가 있어 사업을 결국 접은 바 있다. 이는 글로벌 시대에 기업의 수익성 창출은 규모의 경제에 따르지 않을 수 밖에 없다는 사실을 보여준다.

전세계 보안 솔루션 업체의 3분의 1이 국내 에 포진해 있다는 미야냥을 벗어나기 위해선, 공공 시장에서 국산 업체들끼리 출혈 경쟁, 저 가 수주로 인한 악순환의 고리를 끊고 당당히 글로벌 기업과의 경쟁에서 맞설 힘을 길러야 할 것이라는 데 업계는 한 목소리를 내고 있 다. e

*Interview* 라드웨어 박진성 이사

**"비용 · 인력 · 시간 모든 면에서 CC인증 부담"**

CCRA 가입 후 외산 업체에게도 공공 시장으로의 진출 활로가 펼쳐질 것으 로 기대하나.

국정원과 KISA에서는 국산 업 체들을 얼마나 보호할 수 있을지 에 대해서만 관심이 있는 것 같다. 때문에 CCRA에 가입한다고 하더 라도 국정원은 국산 업체를 보호 하기 위한 또 다른 방법을 취할 것이다. 보안성 검토가 그 방법 중 하나일 것이다. 또 공공시장 에 들어가기 위해서는 EAL3 플러스를 받아야 한다. 이것이 함정이다. CCRA에는 3 플러스 라는 등급은 없다. 그렇다면 EAL 4를 받아야 만 공공기관에 들어갈 수 있다는 얘기다. EAL4를 받기 위해서는 원천소스를 모두 제출 해야만 받을 수 있는데, 이렇게 희생하면서까 지 CC인증을 받아야 하는지 의문이 든다.



국정원 CC인증에 대해 어떤 문제가 있 다고 생각하는가.

보호 무역 주의가 많이 산재해 있 다고 생각한다. 공공기관에 납품하 기 위해 본사에서 소스코드 제출까 지 겨우 허가를 받았다. 하지만 실 질적으로 인증을 받으려고 하니 버 전이 바뀔 때마다 새로 받아야 하는 문제, 6개월에서 1년 이상의 시간낭비, 인력 소모 등 CC 인증을 받기 위해 너무 많은 부담 을 감수해야 했다. 국정원의 CC인증을 받기 위해 몇 천만원이나 드는 비용은 가장 나중 문 제였다.

차라리 공공 시장 진입보다는 금융권과 같은 다른 산업에 힘을 쏟는 것이 더 낫다고 생각했 다. 보안 장비가 아닌 L7스위치는 충청권 지자체와 언론재단 등에 많이 들어가 있어 공공 시 장에서는 L7스위치로 선전할 계획이다. <유>