【붙임 1】 정보보호제품 성능평가 신규 제품군 후보 목록

구분	신규 제품군 후보 목록	설명
1	이메일 보안 솔루션	- 수신메일의 스팸 / 바이러스 / 악성메일 공격 차단 및 발송메일의 정보유출 차단 및 승인 보안을 통합한 E-mail 전용 보안 솔루션 - 스캠/스팸/악성메일과 메일 서버에 대한 공격에 효과적으로 대응할 수 있을 뿐 아니라 외부로 발송되는 메일에 대한 모니터링을 통해 기업의 중요 정보 유출을 차단할 수 있는 이메일 보안 솔루션
2	NAC (네트워크 접근 제어 시스템)	- 사용자의 기본적인 보안 상태와 다양한 사용자 보안 프로그램들의 상태 정보를 파악하여 사용자가 적절한 보안기능을 갖고 있는지를 점검하고 사용자가 보안 적절한 보안기능을 갖추지 못한 경우 자동격리하는 기능을 제공하는 제품
3	모바일 기반 VPN (모바일 VPN)	- 모바일 운영체제에서 사용하는 VPN - VPN은 Virtual Private Network의 약자로 두 개 이상의 물리적 네트워크(또는 장치) 사이의 인터넷/공용 네트워크를 통해 생성된 가상사설망
4	통합보안관제	- 보안장비, 업무서버・네트워크장비, APP 등 인프라 전체 데이터를 통합 관리하고 다양한 형태의 실시간 모니터링 및 통계 그래프, 상관관계 분석 기능을 통해 보안 위협 대응 및 장애 해결을 위한 솔루션
5	CDR(콘텐츠 무해화 솔루션)	- 사용자가 실행하는 모든 문서의 구조 분석을 통해 악성코드로 활용 가능한 액티브 콘텐츠 영역만을 탐지하여 제거(비활성화) 한 후 안전한 파일로 재조합하는 기능을 제공하는 제품
6	개인정보 비식별화 솔루션	- 개인정보 비식별 관련 각종 시행령 및 고시, 가이드라인 등이 완료됨에 따라, 비식별화가 필요한 개인정보가 포함된 개인정보 영역을 다양한 암호학적 방식을 통하여 사람의 육안으로 식별할 수 없도록 처리하는 시스템
7	통합계정관리시스템	- 계정 관리, 승인 서비스, 계정 배포 및 동기화 기능 등을 제공하여 기업의 계정관리 인프라를 효과적이고 효율적으로 운영할 수 있도록 기능을 제공하는 제품(EAM 및 SSO 시스템과 연계를 통해 안전한 인증 및 권한관리 서비스를 지원하는 기능도 제공함)
8	MFA(다중 인증 시스템)	- 두 가지 이상 인증 매커니즘에 성공적으로 제시한 이후에만 사용자에게 접근 권한이 주어지는 컴퓨터 접근 제어 기능을 제공하는 제품

9	AP(Access Point)	- 유·무선 연동 브리지 기능을 수행하는 외부 IT실체로서, 무선랜 인증 서버와 무선랜 인증 클라이언트간 인증 관련 메시지를 중계하고 무선랜 접근통제 정책에 근거하여 무선랜 단말의 네트워크 사용을 통제하는 장치
10	인터넷 전화 방화벽	- 인터넷전화망으로 유입되는 인터넷전화 트래픽 제어 및 비정상 메시지에 대한 탐지·차단 기능과 스팸, SIP/RTP Flooding 공격 탐지·차단 기능을 통해 인터넷전화와 연관된 각종 공격으로 부터 인터넷 전화망을 보호하는 제품
11	WIPS(무선침입방지시스템)	- 무선랜 표준을 사용하는 모든 무선랜 단말의 송수신 트래픽을 실시간으로 관찰하여 Rogue AP, 정책위반 AP, Ad-Hoc 접속 등과 같은 무선위협을 탐지하고 차단함으로써 외부 사용자의 침입을 방지하고 무선랜 단말을 사용하는 내부 사용자의 비 인가된 정보유출 등을 방지하는 제품
12	망간 자료전송(망분리) 제품	- 망간 자료전송제품은 서로 다른 영역(보안영역과 非보안영역 등)간 사용자 PC 자료 및 서버 스트림을 보안 정책에 따라 안전하게 전송해주는 시스템
13	NDR(네트워크 위협 탐지 및 대응)	- NDR(Network Detection and Response)은 네트워크 트래픽을 분석하여 악성 활동이나 보안 위협을 탐지하고 대응하는 제품
14	랜섬웨어 대응 제품	- 랜섬웨어 대응 제품은 사용자의 데이터(시스템파일, 문서, 이미지, 동영상 등)을 암호화하고 복구를 위한 금전을 요구하는 악성 코드등의 랜섬웨어를 탐지하고 대응하는 제품
15	DRM(디지털 저작권 관리)	- DRM(Digital Rights Management)은 디지털 콘텐츠의 무단 복제, 배포, 위조 등을 방지하여 저작권자의 권리를 보호하고, 합법적인 사용만을 허용하는 시스템
16	통합접근관리(EAM)	- EAM(Enterprise Access Management)은 사용자 인증, 권한 부여, 접근 제어, 감사 로그 관리 등의 기능을 통해 조직 내 사용자들의 시스템 접근을 통합적으로 관리하여 자산을 보호하는 제품
17	서버접근통제	- 서버접근통제는 보호하고자 하는 서버의 중요자원(파일, 디렉토리, 프로세스 등)에 대한 접근을 정해진 규칙에 따라 허용하거나 거부하여 조직 내부의 주요 자원을 인가되지 않은 접근으로부터 보호하는 제품
18	SOAR	- SOAR(Security Orchestration, Automation, and Response)은 보안 팀이 침해 사고를 신속하게 탐지, 조사 및 대응할 수 있도록 지원하며, 반복적인 보안 작업을 자동화하여 인력 부담을 줄이고 보안 대응 시간을 단축하기 위하여 보안 도구 및 프로세스를 통합하고 자동화하여 보안 위협에 대한 대응을 효율적으로 관리하는 시스템.

【붙임 2】 정보보호제품 신속확인 제품군/제품유형 분류

구분	제품군	제품 유형
1	침입차단	1.1 침입차단시스템(FW)
		1.2 웹 방화벽
		1.3 DDoS 대응 장비
		1.4 인터넷전화 보안
		*** 침입차단제품군에 속한 신기술·신종 제품**
2	침입방지	2.1 침입방지 시스템(IPS.IDS)
		2.2 무선침입방지제품(WIPS)
		*** 침입방지제품군에 속한 신기술.신종 제품**
3	구간보안	3.1 가상사설망(VPN)
		3.2 네트워크 접근통제제품(NAC)
		3.3 무선랜 인증제품
		*** 구간보안제품군에 속한 신기술.신종 제품**
4	전송자료보안	4.1 스팸메일차단시스템
		*** 전송자료보안제품군에 속한 신기술.신종 제품**
5	보안관리	5.1 통합보안관리제품(EMS.통합로그관리등)
		5.2 소스코드 보안약점 분석도구
		5.3 패치관리시스템
		5.4 데이터베이스 접근통제제품
		*** 보안관리제품군에 속한 신기술.신종 제품**
6	가상화	*** 가상화제품군에 속한 신기술.신종 제품**
7	엔드포인트 보안	7.1 안티바이러스제품(Windows용)
		7.2 스마트폰 보안관리제품(MDM.EMM 등)
		7.3 운영체제(서버) 접근통제제품
		*** 엔드포인트보안제품군에 속한 신기술·신종 제품**

※ 각 제품군의 **파란색 글자(*)** 신기술·신종 제품에 해당하는 제품만 신속확인 가능