SECaaS 집중 분석

정보보호연구실 조대인

중소제조업 보안 강화를 위한 SECaaS 활용 방안 연구 정리

[중앙대 대학원, 이송미]

클라우드 기본 개념 - 온디맨드 방식

- 인터넷 기반
- 아웃소싱
- 서비스 구독 모델

CAPEX - OPEX

CAPEX - 자본지출, 고정자산에 투자

OPEX - 운영비, 유지보수 비용

TCO - 총 소유 비용

결과적인 이점

- 자원을 필요할 때만 이용
- 솔루션 업데이트에 관심가질 필요 X
- 중소, 스타트업의 경우 사내 보안팀 운영하기 힘듬, 이를 해소

SECaaS의 서비스 제공 항목

1. IAM(identity and access management)
2. DLP
3. 웹보안
4. 이메일보안
5. 보안감사
6. 침입관리
7. SIEM(Security information and Event management)
8. 암호화
9. BC/DR (business Continuity and disaster recovery)
10. 네트워크검사
11. 취약점 검사
12. 지속적인 모니터링

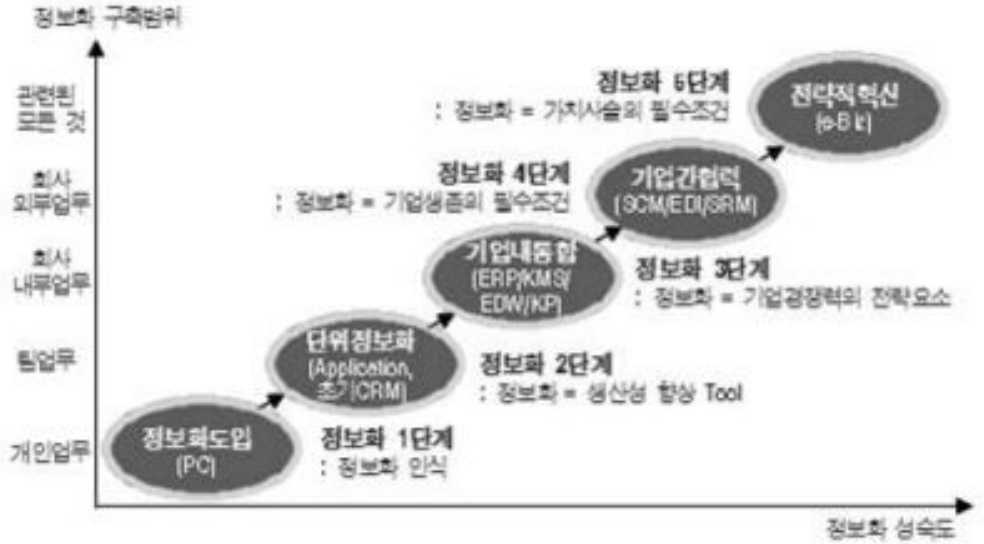
SECaaS를 제공하는 기업

펜타시큐리티

지란지교시큐리티

트렌드마이크로 등

정보화 구축 범위



[그림 9] 중소기업 정보화 발전 단계

SECaaS를 적용하는 방안

중소규모의 제조업, 도소매업, 지식서비스업 측면

-> 정보화 단계를 분석

(중소기업 정보화 수준 조사) => 이를 판단하는 지표

정보화 시스템 활용도

[표 7] 업무별 정보화 시스템 활용도 순위

산업별	업무(1순위)	업무(2, 3, 4순위)
제조	예산,결산,원가관리 회계처리 등 재무 프로세스	ERP(전사적 자원관리)
		GW(그룹웨어)
		홈페이지
건설		전자입찰 시스템
		전자결제 e-payment
		홈페이지
도소매		홈페이지
		전자결제 e-payment
		영업,마케팅,고객관리 프로세스
운수		창고 및 물류/운송관리 프로세스
		홈페이지
		전자결제 e-payment

정보화 시스템 활용도

운수	예산,결산,원가관리 회계처리 등 재무 프로세스	창고 및 물류/운송관리 프로세스
		홈페이지
		전자결제 e-payment
정보통신		홈페이지
		전자결제 e-payment
		영업,마케팅,고객관리 프로세스
지식서비스		홈페이지
		전자결제 e-payment
		인사관리
녹색/환경		전자결제 e-payment
		전자입찰 시스템
		창고 및 물류/운송관리 프로세스

보안 솔루션 적용 기준

[표 15] 보안 솔루션 맵 분류 기준(KISA, 2013)

단계	적용범위	설명
Step 1	소규모(15명이하), 비영리 기관	조직을 안전하게 운영하기 위한 최소한의 보안 솔루션
Step 2	중소기업	중소 규모의 조직에서 보안 체계를 효과적으로 갖추기 위한 보안 솔루션
Step 3	대기업	대규모 조직에서 효율적인 관리 및 통제를 하기 위한 보안 솔루션
Step 4	기밀정보를 다루는 주요 조직	주요 정부기관, 군사 등 고도의 보안 수준이 요구되는 조직을 위한 보안 솔루션

현대의 특이점

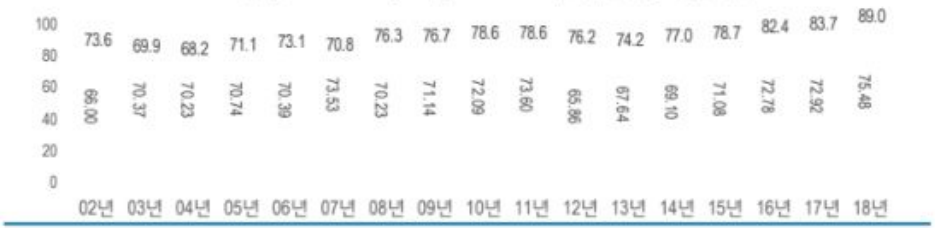
1) 정보화 수준

○ 2018년 중소기업 정보화 수준은 67.15점으로 대기업 대비 중소기업의 정보화 수준은 89.0%로 나타남

○ 지수가 개편된 2012년 이후 대기업과 중소기업의 정보화 수준은 꾸준히 증가하고 있으며, 대기업 대비 중소기업의 수준도 증가함

【그림 i-1】 정보화 수준 추이

(Base: 각 년도 전체, 단위: 점, %)



분야별로 다른 보안 항목

- 제조 생산: EndPoint, Network 보안 등이 필요
- IT 지식 활용: 웹보안, 취약점 검사 등이 필요
- 은행 및 회계: 암호화, 침입관리 등이 필요
- ...

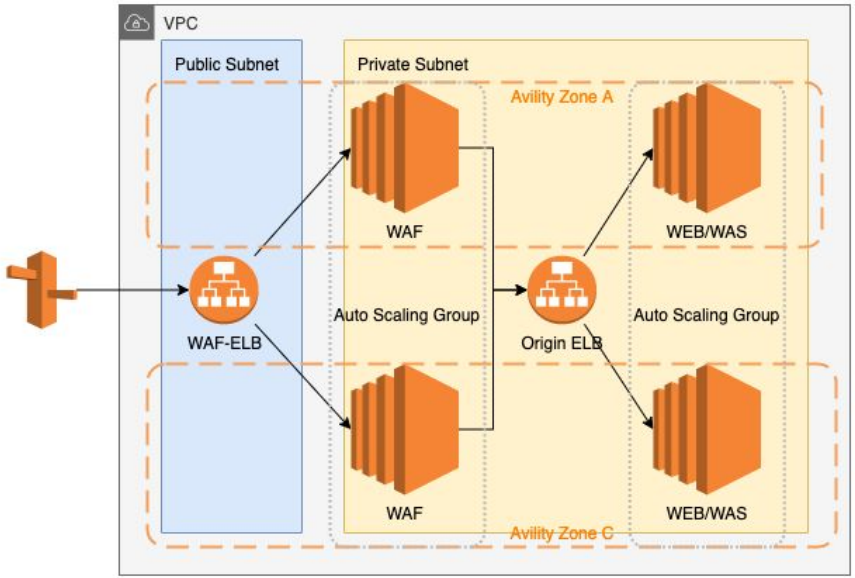
SECaaS 적용방안 - WAF(web aplication firewall)

VPC - Virtual Private Cloud

VPC 환경에서의 WAF는 IDC(Internet Data Center)에서의 WAF와 유사하게 구성

프록시의 형태로 방화벽 역할을 수행

SECaaS 적용방안 - WAF(web aplication firewall)



서비스형 WAF

- 머신 러닝을 이용한 솔루션이 이미 다수 존재
- 국내기업 중에는 펜타 시큐리티가 솔루션 서비스 중

-> 연구방향: 인공지능 다수 존재, 따라서 경량화, 또는 성능 향상 아이디어 제시

경량화?

- WAF 경량화에 대한 다양한 아이디어 존재
- 다중 레이어를 이용한 WAF 등

인공지능 VS 방법론

- 탐지까지 걸리는 시간, 오탐, 정탐, 미탐 여부
- 인공지능의 단점: 학습 데이터를 업데이트 하기 힘듬
- 방법론적인 접근법: 클라우드 환경에서 즉각적인 다중 레이어 생성 후 성능 측정

다른 항목들과의 결합

WAF + 이메일 보안

프록시방식 + DLP

보안감사 + 취약점 점검

...