CMMC 교육 모듈 2 한글 번역

모듈 구성

이 모듈은 총 5 개의 주제로 구성되어 있습니다.

1. 국방 공급망과 DOD 의 안전
2. 정보 보호의 중요성
3. CMMC 와 그 모델
4. CMMC 모델 구조 및 레벨
5. CMMC 적용 사례와 시나리오

첫 번째 주제: 국방 공급망 (DSC, Defense Supply Chain)

많은 사람들이 미국 국방부(DOD)의 공급망에 대해 이야기할 때, 주로 국방 산업 기반(DIB, Defense Industrial Base)에 초점을 맞춥니다.

DIB 는 다음을 가능하게 하는 산업 복합체를 의미합니다:

- 연구 및 개발
- 설계
- 생산
- 납품
- 군사 무기 및 소프트웨어 시스템 유지보수

DIB 는 전 세계 수많은 기업이 포함된 산업 복합체이며, 군수 제품 및 서비스의 전 범위를 포함합니다. 이는 미국 국내뿐만 아니라 해외 기업들도 포함되며, 200 개 이상의 DIB 기업과 하청업체들이 이에 포함됩니다.

예를 들어 전투기 하나를 제작하려면 헬멧, 조종석, 센서 등 수천 개의 부품이 필요하며, 각 부품은 다른 업체가 제작하는 경우가 많습니다.

따라서 공급망의 각 단계(tier)는 자신에게 맡겨진 정보를 보호하기 위한 적절한 보안 수칙을 반드시 갖추어야 합니다.

국방 공급망의 범위 확대

국방 공급망(DSC)은 DIB 보다 훨씬 광범위합니다.

단순히 무기 시스템이나 소프트웨어만이 아니라, 다음과 같은 다양한 요소들이 DSC 에 포함됩니다:

- 사람 (직원, 계약자)
- 시설
- 식자재 공급업체
- 청소 용역
- 건설 및 토목 작업자
- 사무기기 및 통신 장비 공급업체

이처럼 복잡한 공급망은 DOD 에 다양한 위험 요소를 안겨줍니다.
예: 비즈니스 이메일 침해, 섬 타기(Island Hopping), 공급망 교란 및 변조

사례 (2019 년, 월스트리트 저널):
미국 전력망을 공격하려던 적대 세력은 전력망 자체가 아닌, 하위 계약업체에 피싱 메일을 보내 침입 기반을 마련한 뒤 상위 공급망 업체로 확장했습니다.

두 번째 주제: 정보 보호의 중요성

국방 공급망(DSC)에 속한 모든 조직은 민감한 정보를 처리, 저장, 전송하는 데 책임이 있습니다.
이에 따라 DOD 는 전체 DSC 의 보안을 강화하기 위해 노력하고 있습니다.

적대 세력은 DOD 관련 데이터의 기밀성, 가용성, 무결성을 노리고 있으며, 그 침투 경로로

국방 공급망을 활용합니다.

처음에는 무해해 보일 수 있는 정보 — 계약 금액, DOD 담당자 이름 등 도 퍼즐 조각처럼 모여 DOD 의 활동을 명확히 파악할 수 있게 합니다.

DOD 와 DSC 는 다양한 민감 정보를 주고받습니다:
- FCI (Federal Contract Information): 정부 계약에 포함된 비공개 정보
- CUI (Controlled Unclassified Information): 법/정책에 따라 보호가 요구되는 정보
- CTI (Controlled Technical Information): 군사/우주 관련 기술정보
- CDI (Covered Defense Information): 계약 중 생성된 민감 정보

이러한 정보는 분류되지 않았더라도 반드시 보호되어야 합니다.

사례:
2016 년 악성 사이버 활동으로 미국 경제에 약 570 억 ~ 1,090 억 달러 손실
2017 년 글로벌 사이버 범죄 비용은 약 6,000 억 달러

사이버보안은 이제 DOD 계약의 비용, 일정, 성능을 지탱하는 기반 요소로 간주됩니다. 따라서 CMMC 프로그램은 모든 조직이 최소한의 보안 기준을 갖추도록 돕습니다.

세 번째 주제: CMMC 란 무엇인가

CMMC(사이버보안 성숙도 모델 인증)는 기존의 자가 인증 방식 대신, 제 3 자의 검토를 도입한 시스템입니다.

CMMC 레벨 2 에서는 계약 전에 제 3 자가 보안 프로그램을 검토하고, 성과 기간 중에도 정기적으로 확인합니다. 이는 계약자에게만 책임이 전가되지 않도록 하며, 문제를 더 빠르게 발견하고 수정할 수 있도록 돕습니다.

레벨 1 에서는 여전히 자가 인증 방식이지만, 원한다면 제 3 자 검토를 요청할 수도 있습니다.

CMMC 는 업계의 확장성과 민첩성을 활용해 DOD 가 목표를 달성하도록 설계되었습니다.

이에 따라 다양한 업계 대표들이 모여 **CMMC 인증기관(CMMC-AB)**을 설립했고, 그 주요 임무는 다음과 같습니다:

1. 10 만 개 이상의 DSC 조직을 인증
2. 인증을 위한 교육, 승인, 평가 생태계 구축

CMMC-AB 는 독립적인 제 3 자 평가 기관(C3PAO)을 지정하고,
인증 심사를 수행할 수 있는 인증 평가자를 양성합니다.

중소기업도 모든 레벨에서 인증을 감당할 수 있도록 **비용 효율적인 구조**로 설계되어 있으며, 대부분의 조직은 CMMC 레벨 1 자가 평가만 요구받게 됩니다.

이 레벨에서는 17 개의 기본 보안 실무만 적용되며, 이는 기존 FAR 52.204-21 에서 요구하는 기준과 거의 같습니다.

CMMC 모델 버전 2 의 기반은 **NIST SP 800-171**로, 이는 CUI 보호를 위한 보안 요구사항이 담긴 표준입니다.

CMMC 는 세 개의 수준(Level)을 통해 FCI 및 CUI 를 점진적으로 보호할 수 있게 합니다.
레벨이 올라갈수록 보안 성숙도가 높아지고, 위험에 따라 실무도 강화됩니다.

CMMC 인증은 계약 수준에 맞는 보안이 이루어지고 있음을 보장하며, 레벨 2 부터는 고급 보안 조치를 시행해야 합니다.

CMMC 요건은 **버전 2.0 규칙 제정 이후** 점진적으로 계약에 도입될 예정입니다.

네 번째 주제: CMMC 모델 구조

CMMC 는 기존의 보안 기준 위에 보안 실무를 추가해 일관된 사이버보안 기준선을 제공합니다.

구성 요소는 다음과 같습니다:
- FCI 용 FAR 기준: 15 개 기본 제어
- CUI 용 NIST SP 800-171: 110 개 요구사항
- 추가로 NIST SP 800-172 에서 일부 고급 요구사항도 반영 예정

모델은 14 개 보안 영역(Domain)으로 구성되어 있으며, 보안 실무는 3 단계 레벨에 따라 나뉘고 점진적으로 강화됩니다.

예: 시스템 접근을 사용자 권한에 따라 제한하는 실무는 특정 레벨과 도메인에 배정됨

- **레벨 1:** 6 개 도메인, 17 개 실무 (기초적 보호)
- **레벨 2:** 14 개 도메인, 110 개 실무 (CUI 보호)
- **레벨 3:** 고급 보호 (세부사항은 아직 결정 중)

레벨 2 와 3 에서 받은 인증은 **3 년간 유효**합니다. 단, 보안 실무가 변경되면 재평가가 필요할 수 있습니다.

조직의 환경 또는 특정 구역(enclave)이 인증되면, 그 인증 환경 내에서 여러 계약의 정보를 처리할 수 있습니다.

적용 사례: Bob's Machine Shop

Bob's Machine Shop 은 다양한 고객에게 맞춤형 부품을 제작하며, DOD 도 그 중 하나입니다.

1. **Widget 1 계약 제안:**
   - FCI 만 포함됨 → CMMC 레벨 1 필요
   - 자가 평가 완료 → 계약 수주

2. **Widget 2 계약 제안:**
   - 여전히 FCI 만 포함됨 → 연례 자가 평가로 대응 가능

3. **Widget 3 계약 제안:**
  - FCI 및 CUI 모두 포함됨 → 최소 CMMC 레벨 2 필요
  - 제안서를 제출함과 동시에 레벨 2 인증 절차 시작
  - 인증 완료 후 계약 수주

이처럼 인증은 계약 단위가 아닌 조직 환경 또는 특정 구역 단위로 수행될 수 있으며, 각 인증은 여러 계약에 활용될 수 있습니다.

CMMC 의 발전 및 향후 방향

2017 년 말까지, 모든 국방 계약자는 NIST SP 800-171 을 구현하여 CDI 보호를 위한 충분한 보안을 제공해야 했습니다.

하지만 여전히 문제가 남아 있었고, 이에 따라 2019 년 초 DOD 는 CMMC 프로그램을 시작했습니다.

- **2020 년 1 월:** CMMC 버전 1.0 공개
- **2020 년 3 월:** DOD 와 CMMC-AB 간 MOU 체결, 유일한 인증기관으로 인정
- **2021 년:** 내부 리뷰 및 정책 개선 작업
- **2021 년 11 월:** CMMC 버전 2.0 발표
  - 목표: 정보 보호, 사이버 회복력, 중소기업 지원, 신뢰 구축

현재 DOD 는 9~24 개월의 규칙 제정 기간을 거쳐 CMMC 를 계약에 본격 도입할 예정입니다.

이 과정에서 인증을 자발적으로 도입하는 업체에 대한 인센티브도 제공됩니다.

결론적으로, CMMC 는 조직이 보안 요건을 충족했는지를 평가하고, 적절한 레벨에서 CUI 를 안전하게 다룰 수 있도록 돕는 제도입니다.