CMMC 모듈 5 번역본

이 모듈은 **두 개의 주제**로 구성되어 있으며, 이 모듈에서는

1. **상용 제품(COTS: Commercial Off-The-Shelf)** 및 서비스
2. **FCI 만 포함된 계약**
   에 대해 다룰 예정입니다.

주제 1: 상용 제품 및 서비스 (Commercial Off-The-Shelf Products and Services)

공구, 식료품, 소프트웨어, 차량 같은 **물품**부터 건설, 컨설팅, 엔지니어링 같은 **서비스**에 이르기까지, 국방부(DOD)는 다양한 제품과 서비스를 구매하고 있습니다.

일부는 DOD 맞춤형으로 제작되지만, **구매 물품의 상당수는 '상용 제품(COTS)'**이라고 불리는 범주에 속합니다.

COTS (Commercial Off-The-Shelf)는 일반 상업 시장에서 이미 판매되고 있는 제품 또는 서비스를 지칭하는 용어이며, 정부는 이 제품이나 서비스의 **단순 구매자 중 하나일 뿐**입니다.

즉, **COTS 제품 또는 서비스로 인정되기 위해서는**,
정부에 판매되는 버전이 상업용 버전과 **어떠한 수정 없이 동일해야** 합니다.
조금이라도 변경이 있다면 COTS 로 간주되지 않습니다.

이 점이 중요한 이유는, **국방부가 COTS 공급업체는 CMMC 인증을 받을 필요가 없다고 밝혔기 때문**입니다.

하지만 여기에는 **예외**가 있습니다.
일부 COTS 공급업체가 계약 과정에서 **FCI(Federal Contract Information)**를 받는 경우가 있기 때문입니다.
이 경우, 해당 업체는 CMMC 인증이 **필요할 가능성이 매우 높습니다**.

이 개념에 대해서는 이번 모듈에서 더 자세히 다루게 되며,
DOD 가 이 주제에 대해 추가적인 지침을 제공하는 경우, 그 내용을 반영하여 업데이트할 예정입니다.

주제 2: FCI 가 포함된 계약

앞서 논의했듯이, **연방정부는 일반적으로 제품을 생산하거나 서비스를 직접 제공하지 않고**,
계약을 통해 민간 계약자들로부터 물품과 서비스를 구매합니다.
국방부(DOD)도 마찬가지로, 계약 체결을 통해 제품 및 서비스를 확보합니다.

일반적으로 DOD 는 먼저 **요구사항과 기타 정보를 포함한 제안요청서(RFP)**를 공고하고, DOD 공급업체가 이에 대해 **제안서를 제출**합니다. 이 제안서가 채택되면 DOD 와 공급업체는 **계약을 체결**하게 됩니다.

계약 체결 시, **계약 조건, 제품 사양 및 기타 정보**를 주고받게 되며, 이 정보는 **연방 계약 정보(FCI)**로 간주될 수 있습니다.

DOD 는 대부분의 조달이 **CUI (Controlled Unclassified Information)**를 포함하지 않을 것이라고 예상합니다.
따라서 이번 시나리오에서는 계약에 **FCI 만 포함되어 있다고 가정**합니다.

CMMC 수준과 인증 요건

대부분의 CMMC 인증 희망 조직(OSC)은 **FCI 만 받기 때문에**,
DOD 는 이들이 **연 1 회의 CMMC 레벨 1 자기 평가와 고위 임원의 확인만으로 충분**하다고 기대합니다.

하지만 **일부 계약자들**, 특히 **주계약자(Prime Contractor)**는 CMMC **레벨 2 인증을 원하는 경우도 있습니다**.
이번 예시에서는 DOD 공급업체가 이미 **CMMC 레벨 2 인증을 보유**한 상황입니다.

하지만 설령 공급업체가 레벨 2 인증이 없더라도,
FCI 를 받는 이상 최소한 CMMC 레벨 1 요구사항은 반드시 충족해야 합니다.

이는 해당 업체가 자체 제품/서비스를 판매하든, 다른 업체의 제품/서비스를 재판매하든 **동일하게 적용됩니다**.

하도급업체(Subcontractor)와의 관계

대부분의 경우, **주계약자는 계약상 모든 구성요소나 서비스를 직접 제공하지 않고 여러 하청업체와 협력**하게 됩니다.

이번 예시에서는 **세 개의 하도급 업체**가 있습니다:

1. **Mako**: CMMC 레벨 2 인증 보유
2. **SmallCo**: 연 1 회 CMMC 레벨 1 자기 평가 및 고위 임원 확인서를 **SPRS**(Supplier Performance Risk System)에 제출
3. **Costco**: **CMMC 인증 없음**

- DOD 공급업체는 Mako 와 계약 조건 및 사양(FIC)을 공유할 수 있습니다.
  단, Mako 가 해당 정보를 **CMMC 인증된 환경 내에서 관리**한다는 조건이 계약에 명시되어야 합니다.
- SmallCo 의 경우도 마찬가지입니다.
  CMMC 레벨 1 자기 평가와 고위 임원 확인이 제출되어 있고, **CMMC 환경 내에서 정보가 관리된다면** FCI 공유가 가능합니다.
- **Costco 에는 FCI 를 제공할 수 없습니다.** 왜냐하면 인증이 없기 때문입니다.

Costco 의 참여 방식

하지만 그렇다고 Costco 가 **계약에서 완전히 제외되는 것은 아닙니다.**

예를 들어 Costco 가 **상용 볼트(COTS 부품)**를 제조하고, DOD 공급업체가 이를 구매하는 경우, 단순한 **발주서 발행**을 통해 구매는 가능합니다.
단, 이 과정에서 **어떠한 FCI 도 제공되어서는 안 됩니다.**

또 다른 예로, Costco 가 **안티바이러스 소프트웨어**를 판매한다고 가정해 봅시다.
이 경우 DOD 공급업체가 라이선스를 **직접 관리**하고, FCI 도 **자체적으로 보관/관리**해야 합니다.

즉, Costco 가 FCI 를 **전혀 수신하지 않도록 계약을 구성**한다면, Costco 는 CMMC 인증이 **필요 없습니다.**

이처럼, COTS 공급업체가 **FCI 를 받지 않도록 조치**하는 것은 **CMMC 인증을 피할 수 있는 방법**입니다.
그러나 이는 **주계약자와 COTS 공급업체 간의 명확한 계약**을 통해 이루어져야 합니다.

제안 제출 전 협력사 결정

DOD 공급업체는 일반적으로 제안서 제출 전부터 필요한 제품이나 서비스를 제공할 협력업체(Costco, SmallCo, Mako)를 이미 알고 있으며,
이들과 **데이터 처리 계약(Data Handling Agreement)**을 체결하고 **팀 구성 계약(Teaming Agreement)**의 일환으로 포함시킵니다.

또한 제안서에는 RFP 에 정의된 FCI 의 처리 및 주계약자와 하청업체 간의 **정보 공유 방식**이 명시되어야 합니다.

계약 수행 중에 하도급 업체를 교체하거나 새로 투입해야 하는 경우에도, **DOD 에 정보 공유 계획을 명확히 설명**할 준비가 되어 있어야 합니다.

요약

- COTS 공급업체는 **역할에 따라 CMMC 인증이 불필요할 수 있음**
- DOD 는 COTS 공급업체에게 CMMC 인증을 요구하지 않음 (단, **FCI 수신 시 예외**)
- **모든 참여 업체가 동일한 CMMC 수준을 요구받는 것은 아님**
- CMMC 레벨 1 또는 2 는 **받는 정보의 민감도**에 따라 결정됨
- **주계약자와 하도급 업체는 FCI 의 성격과 처리 방식을 명확히 정의해야 함**

다음 모듈은 Module 6: CMMC 도구 및 템플릿(CMMC Tools and Templates)입니다.