CMMC 모듈 4 번역본

주제 1: 정보 보호 (Protecting Information)

우리 국가의 적들은 항상 정보를 수집하려고 합니다. 처음에는 중요하지 않아 보이는 정보라도, 다른 정보들과 결합되면 위협이 될 수 있습니다. 예를 들어, PVC 스마트카드 200 개를 주문한 사실은 단순한 재고 보충일 수 있지만, 비정상적인 시기에 주문되면 적들이 부대에 변화가 있음을 추측할 수 있습니다. 이런 정보가 축적되면 공격 표적이 될 수 있기에, CMMC 모델은 이러한 정보 보호에 중점을 둡니다.

DoD 공급망은 다양한 정보를 주고받으며, 이러한 정보는 단독으로도 또는 결합해서도 적에게 가치가 있을 수 있습니다. 이 중 FCI(Federal Contract Information)는 가장 기본적인 수준의 정보이며, 보호가 요구됩니다.

CMMC 모델은 정보의 민감도에 따라 보호 수준을 구분합니다. 예컨대 스마트카드 주문은 낮은 민감도의 정보지만, 차세대 항공기의 착륙장치 사양은 훨씬 민감한 정보입니다. 따라서 후자는 더 높은 보호 수준이 필요합니다.

CMMC 레벨 1 은 연방조달규정(FAR)의 기존 요구사항과 일치하며, 대부분의 정부 계약에 포함되어 있습니다. 기존 계약자는 이미 이러한 요구사항을 충족한다고 자가 선언(self-attest)하고 있으며, 이 모듈에서는 FCI 여부를 식별하는 방법에 대해 다룹니다.

주제 2: 법적 의무 (Legal Obligations)

클라이언트 조직이 방산 공급망 어디에 있든, 정부의 민감 정보를 적절히 보호하는 것이 중요합니다. 향후 모듈에서 더 자세히 다루겠지만, 계약자는 계약 조건 중 민감 정보 보호 조항을 하청업체에도 적용되도록 해야 합니다. 이를 '흐름 다운(flow down)'이라고 하며, 매우 중요한 요소입니다.

계약자가 자신만의 시스템 보안뿐 아니라, 다른 협력업체에게 전달되는 정보의 보안도 보장해야 합니다.

미국 연방정부는 입법, 사법, 행정부의 세 부문으로 나뉘며, 각각 고유한 규칙과 절차를 가지고 있습니다. 이 중 행정부는 규모 면에서 가장 크며, 대부분의 연방 계약은 행정부 산하의 부처, 기관, 사무소 등에서 이루어집니다.

이를 표준화하기 위해 도입된 것이 바로 연방조달규정(FAR)입니다. FAR 는 대부분의 행정부 계약에서 사용되며, 계약 담당자는 이 규정에 따라 계약 조항을 삽입합니다.

FAR 52.204-21 조항은 계약자가 연방 계약 정보를 보호해야 한다고 명시하며, 최소한으로 따라야 할 15 가지 보안 요건이 포함되어 있습니다. 계약자는 계약서에 서명함으로써 이 요건을 충족한다고 스스로 인증하고 있으며, 이 요건이 계약서에 명시되지 않더라도 크리스천 독트린(Christian Doctrine)에 따라 계약에 포함될 수 있습니다.

계약 중 이 조항이 빠져 있다면, 법적으로 추가될 수 있으며, 계약자가 이를 위반하면 허위 청구 방지법(False Claims Act)에 따라 제재를 받을 수 있습니다. 이 법은 고의적으로 잘못된 청구를 한 자에 대해 정부가 소송을 제기할 수 있도록 하며, 손해액의 3 배 및 건당 벌금을 부과할 수 있습니다.

이러한 법적 환경은 내부 고발자(whistleblower)가 보안 위반을 신고하도록 장려하고 있으며, 실제로 Aerojet Rocketdyne 사건, Cisco 사례 등 여러 기업이 사이버 보안 위반으로 제재를 받았습니다.

최근 사이버 사기 대응 이니셔티브(Cyber Fraud Initiative)와 맞물려, 이러한 흐름은 CMMC 모델에 더욱 힘을 실어주는 중요한 요소입니다.

주제 3: 연방 계약 정보 (Federal Contract Information, FCI)

FCI(연방 계약 정보)는 공공 공개를 목적으로 하지 않고, 정부가 제품 또는 서비스를 개발하거나 제공받기 위해 계약하에 제공하거나 생성된 정보를 말합니다. FAR 52.204-21 에서 정의된 이 개념은 계약자가 반드시 보호해야 하는 기본 정보 범주입니다.

중요한 점은 FCI 는 물리적 제품이 아닌, 정보 또는 사양(specification)이라는 것입니다. 또한 정보가 공개용인지 아닌지를 판단할 때는 정보에 명확하게 '공개 가능' 표시가 없는 한, '공개 불가'로 간주해야 합니다.

정부가 제공한 정보든, 계약 하에 정부를 위해 생성된 정보든, 명시적으로 공개가 허용되지 않았다면 최소한 FCI 로 취급하고 보호해야 합니다.

예외는 거의 없습니다. 마케팅 자료처럼 외부 공개를 전제로 한 작업이라 하더라도, 정부의 명확한 허가가 없으면 해당 정보는 FCI 로 간주됩니다.

반면, 정부 계약 없이 자체 개발한 소프트웨어나 무기 사양 등은 FCI 가 아닙니다. 물론 다른 연방 규정의 적용을 받을 수 있지만, FCI 자체는 아닙니다.

결론적으로, 모든 정보가 어떤 법적 분류에 해당하는지 명확히 이해하고, 적절한 보호 조치를 취하는 것이 중요합니다.