**一般狀況：關鍵基礎設施環境簡介**

* 資訊系統簡介

煉油廠有關的資訊系統有哪些？請簡述其功能及關聯性。

**例如** [煉油廠資訊系統包括管理資訊系統(Management Information System, MIS)及工業控制系統(Industrial Control System, ICS)兩大部份, 管理資訊系統管控行政系統各單位間之電腦及網路通訊, 受損時將影響煉油廠行政業務的正常運作。工業控制系統包括

\* 分散式控制系統(Distributed Control System,DCS),

\* 煉製程控資料收集系統(Process History Database, PHD),

\* 可程式邏輯控制系統(Programmable Logic Controller, PLC),及

\* 監控與資料蒐集系統(Supervisory Control and Data Acquisition, SCADA)。]

* OSMP(Offsite Software Management Package) 輸儲控制系統

提供OSMP系統簡介？系統組成與架構？

OSMP系統是否與網際網路(internet)實體隔離?

OSMP系統是否與中央控制室經由ICS控制網路（內部控制網路）相連接？

OSMP系統運作受到中央控制？OSMP系統是否回傳資訊給SCADA(中央監控及資料蒐集系統)？

OSMP系統的主機為一般個人電腦或特定作業系統之工業電腦？

* OSMP系統風險分析
  1. 設施重要性評估
  2. 核心功能簡述
  3. 設施受損時,對核心功能維持之影響
  4. 持續性評估

**特別狀況**

* 狀況概要

OSMP系統(Offsite Software Management Package)為煉廠輸儲控制系統，主要負責油品產出後的相關輸儲作業，經由OSMP系統運作可自動將各油品購透過管線輸送至儲槽。依據維修廠商建議，OSMP主機電腦需要進行升級，於升級作業中，主機交付時已有被植入惡意軟體，致使升級完畢重新開機時，造成系統軟體檔案被加密無法開啟，因此系統無法使用及影響油品自動輸儲機制。

整台主機汰換更新？

主機系統程式更新？補丁程式管理

主機升級後上線前是否執行病毒檢測程序？

* 事件時序
* 討論議題
  1. OSMP系統遭惡意程式攻擊,系統異常無法運作之緊急應變處置措施
  2. OSMP系統遭惡異程式攻擊,系統異常無法運作之緊急復原處置程序
  3. OSMP系統遭惡異程式攻擊,單位資安事件之處理程序
* 參演單位