行政院及所屬各機關出國報告
（出國類別：考察）

考察網際網路資料中心之技術發展趨勢

出國人：中華電信公司資訊處處長錢世明
中華電信公司數據分公司公眾數據處科長尤能明
中華電信公司電信研究所研發服務室副研究員吳鴻煦

出國地區：香港

出國期間：民國 91 年 12 月 15 日-民國 91 年 12 月 18 日

報告日期：民國 92 年 7 月 18 日

系統識別號:C09105878
公務出國報告提要
頁數: 23　含附件: 否

報告名稱: 考察網際網路資料中心之技術發展趨勢

主辦機關: 中華電信股份有限公司
聯絡人／電話: 柯志勇／2344-4094
出國人員: 錢世明　中華電信股份有限公司　資訊處　處長
吳鴻煦　中華電信研究所　研發服務室　副研究員
尤能明　中華電信數據通信分公司　公眾數據處　科長

出國類別: 考察
出國地區: 香港
出國期間: 民國 91 年 12 月 15 日 -民國 91 年 12 月 18 日
報告日期: 民國 92 年 07 月 18 日
分類號/目: H6／電信　H6／電信
關鍵詞: SOC,資通安全,ISM,eTOM

內容摘要: 本次考察包括三個項目:(1)拜訪香港 HP 公司安全監控中心之規劃及運作機制、(2)拜訪香港政府資安實際落實機制、(3)拜訪香港 HP 公司 ISM 解決方案。 HP SOC 在 1999 年先於香港成立，主要由四位資深的安全顧問及一位經理組成。提供全球廠商的安全顧問服務及整合服務，主要有藉由攻擊的方法、技術的持續提昇及資訊安全的穿透測試及測試報告之提供。協助業者安全系統之先期防範及建構安全之防護體系。考察內容有 SOC 提供之服務、經營模式、建置方式及相關之軟硬體設備。香港政府成立資訊科技署(ITSD)專責資訊政策之制訂及落實、資訊安全預防及宣導，不只在政府機構、民營企業，甚至到各級學校、學生均達到良好的成效，值得我國政府機關的參考。HP ISM 在系統整合方面的技術及建構程序相當嚴謹，其相關經驗可供我們公司在系統軟體開發方面，可以利用模組化技術及共通整合介面的機制，建構快速安全的軟體發展生命週期環境，依據 eTOM 架構指引，可以檢視資訊科技對公司未來經營電子商務、內容服務及各種加值服務(總稱 xSP)是否完備，值得公司規劃資訊系統發展策略時之參考。

本文電子檔已上傳至出國報告資訊網

摘要

本次考察包括三個項目:(1)拜訪香港 HP 公司安全監控中心之規劃及運作機制、(2)拜訪香港政府資安實際落實機制、(3)拜訪香港 HP 公司 ISM 解決方案。 HP SOC 在 1999 年先於香港成立，主要由四位資深的安全顧問及一位經理組成。提供全球廠商的安全顧問服務及整合服務，主要有藉由攻擊的方法、技術的持續提昇及資訊安全的穿透測試及測試報告之提供。協助業者安全系統之先期防範及建構安全之防護體系。考察內容有 SOC 提供之服務、經營模式、建置方式及相關之軟硬體設備。香港政府成立資訊科技署(ITSD)專責資訊政策之制訂及落實、資訊安全預防及宣導，不只在政府機構、民營企業，甚至到各級學校、學生均達到良好的成效，值得我國政府機關的參考。HP ISM 在系統整合方面的技術及建構程序相當嚴謹，其相關經驗可供我們公司在系統軟體開發方面，可以利用模組化技術及共通整合介面的機制，建構快速安全的軟體發展生命週期環境，依據 eTOM 架構指引，可以檢視資訊科技對公司未來經營電子商務、內容服務及各種加值服務(總稱 xSP)是否完備，值得公司規劃資訊系統發展策略時之參考。

目次

1. 考察行程

91 年 12 月 15 日　去程
91 年 12 月 16 日　拜訪香港 HP 公司安全監控中心之規劃及運作機制
91 年 12 月 17 日　拜訪香港政府資安實際落實機制
91 年 12 月 18 日　拜訪香港 HP 公司 ISM 解決方案
91 年 12 月 18 日　回程

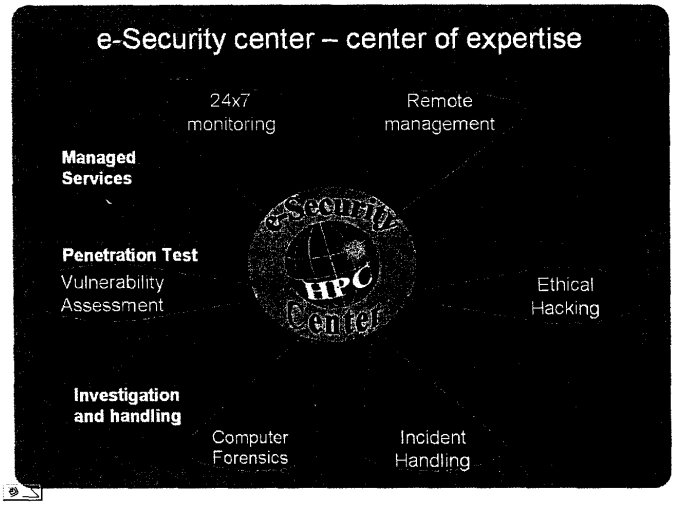
2. 考察內容

2.1 參訪 HP 公司安全監控中心(SOC)

HP SOC 在 1999 年先於香港成立，主要由四位資深的安全顧問及一位經理組成。提供全球廠商的安全顧問服務及整合服務，主要有藉由攻擊的方法、技術的持續提昇及資訊安全的穿透測試及測試報告之提供。協助業者安全系統之先期防範及建構安全之防護體系。有鑑於安全業務的需求，HP 公司於 2001 年再於美國西雅圖成立另一個安全監控中心(SOC) 。

資通安全監控中心(SOC)是一個負責網路安全的監控中心，亦即有一組資安專家及時對企業或機構的網路環境進行安全監控及處理，有些企業亦可自行建置專屬的資安監控中心，負責監控該機構所屬的資訊安全環境。

SOC 提供的服務



包括

- 提供 7 天 24 小時全天候的用戶資訊安全系統與設備監控服務
- 執行定期網路安全掃瞄，達到全天候的安全監控與回應
- 遠端執行用戶防火牆、虛擬私有網路(VPN)、入侵偵測系統(IDS)、防

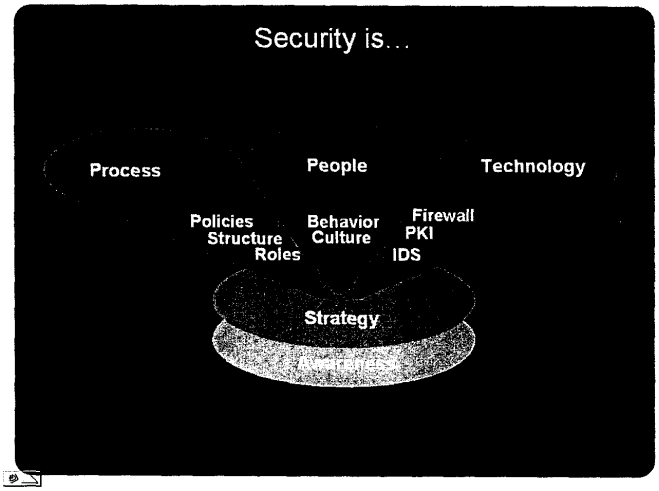
毒系統(Anti-Virus)等架設、設定及管理

- 弱點評估
- 事件分析
- 資料分析評估以及早發佈警訊
- 提供資訊環境安全改善建議
- 異常處理機制
- 調查異常原因及可能的發生方式
- 更提供及時到場之資安事件排除服務

HP 公司主要以提供資訊安全顧問服務，並非賣產品。除了提供顧問服務外，HP SOC 亦提供整合規劃的解決方案，包括各主要品牌的防火牆及路由器等設備之供應。因此，所提供之服務或相關技術或設備，並不會僅以 HP 公司之產品為主，包括其他廠商的解決方法或設備。

SOC 主要的建置要點

資訊安全的構成要素：程序(Process)、人才(People)、技術(Technology)為三大主要的核心要素。



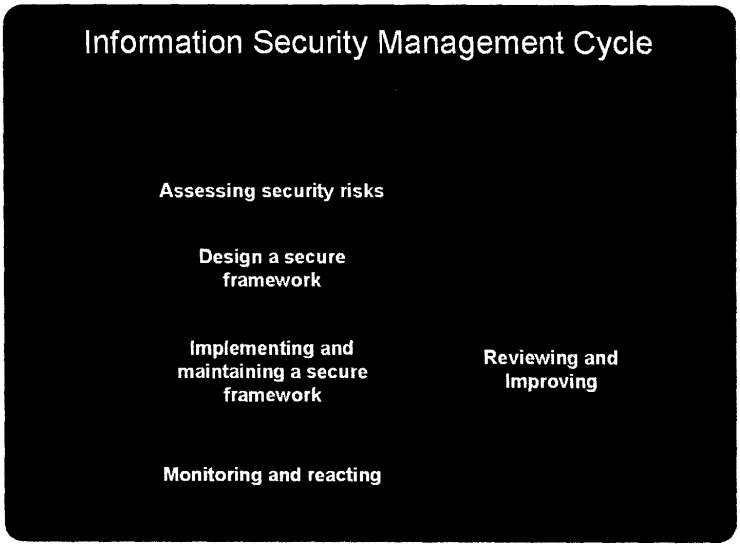
程序(Process)：

對於 SOC 之建立，主要的建置要求就是程序，各項的標準程序。依照 BS 7799/ISO 17799 制定之相關標準，建立標準程序，例如：

- 緊急應變程序
- 災害應變程序
- 異常處理程序
- 標準安全檢驗程序
- 安全等級評估程序

整個資訊安全程序的建立主要的就是資訊安全管理，包括：

- 各項安全的先期評估
- 設計一個安全的架構
- 落實及維運安全方案
- 監控及即時反應
- 定期重新檢討



事件處理機制應包括：

- 安全事件發生的處理程序
- 將事件發生的影響降至最低
- 嚐試找尋攻擊的地點防止類似的事件再發生

人才(People)：

對於資安之顧問服務及訓練落實，主要需要相當專精的資訊安全人才。HP SOC 的人員相當資深，具有相當廣泛的專業及安全知識。包括，作業系統(OS),應用系統或資料庫系統、網路及安全方面的技術。不但可以進行顧問服務亦可以直接上線進行技術提供，同時每個人可以隨時相互支援，並隨時針對最新的技術進行研究了解，建立一個相當良好的安全團隊。

技術(Technology)：

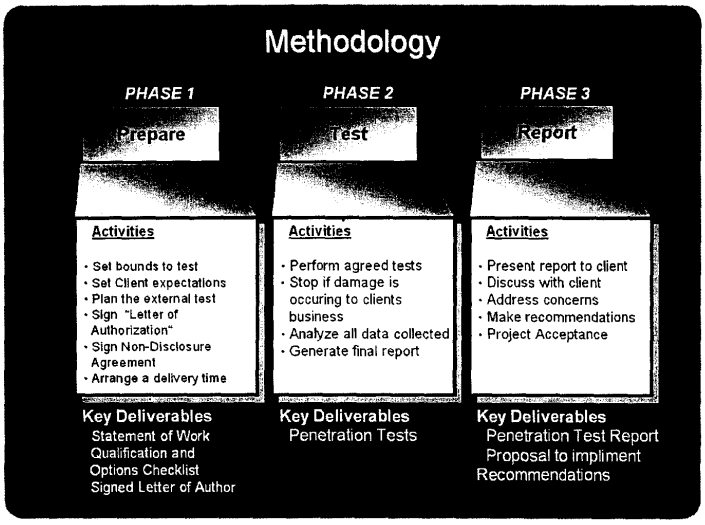
安全技術方面包括：

- 遠端異常處理
- 利用 IDS 或網管之 Agent 即時將各項可能之異常(Alert)回送至 SOC
- SOC 立即分析或研判可能的原因及提供即時之解決方案
- 安全滲透測試(Penetration Testing)

及各項必須之技術。

安全滲透測試(Penetration Testing)，主要分成三個階段

- 測試準備
- 進行測試
- 撰寫測試報告並轉交被測試的單位



HP SOC 小組自行開發弱點掃描報告自動產生系統，提供維運人員及相關主管不同等級的報告資訊。提供技術人員細部的報告，包括哪些弱點及如何改善之詳細問題；提供給主管的則是圖文並茂且易懂的統計整體報告，主管可以快速了解相關資安之現況及待解決的問題，具有相當實用性。

告知(Awareness)：

告知的方法就是訓練，安全訓練是一個非常重要的一個步驟。訓練的目的就是要讓從主管至全部的員工皆知道有哪些安全政策及如何落實或防制可能的入侵。

安全訓練需包括：

- 安全政策
- 安全程序
- 安全標準的訓練
- 新的資安技術
- 解釋哪些資安控制程序
- 如何進行資安控制程序控制或操作

一般企業委託資安監控中心服務主要是得到下列效益：

- 機構網路安全 24 小時有專人監控，安全有保障

- 提供並發揮事前之偵測與補強、事中之監控與警訊告知、事發之處理與回復、以及事終之鑑識與追蹤之功能
- 無須自行雇用各種領域的資安專家，節省人事成本

建置資安監控中心首要是確定服務對象，可以是對外提供服務，亦可是自行對企業內服務，同時要確定服務的對象數量及所有的設備數量，以決定營運規模。所要服務的項目就包含(1)監控：資安事件監控、事件關連性分析、資安問題分析，(2)管理：事件處理應變、資安設備之設定、協助制訂資安政策、提供統計分析報表。受 SOC 監控之機構則需配合(1)授權所需之監控服務範圍、(2)提供 SOC 所需之網路環境及設備資料、(3)裝置監控設備以將資料能傳送回 SOC 進行分析、(4)建置防火牆、入侵偵測系統等資安設備。

資安監控中心所需之設備則包含場地、硬體及軟體三部分：

場地：

- 365*24 小時人員值勤管理、警衛及攝錄影設備
- 通訊設備- 電話、網路、傳真
- 安全管制的實體空間
- 電腦機房、監控台
- 防地震、水災、火災等天災影響之考量
- 斷電、備援的處理
- 保護用戶資料之安全措施

硬體設備：

- 監控中心之控制台、銀幕、通信設備及網路環境
- 電腦、資料庫等資料儲存及處理設備
- 攝影機、冷氣、電源及防火等作業支援設備
- 資料收集系統

軟體設備：

- 惡意程式碼資料庫、弱點資料庫、駭客行為模式資料庫、受監控單位之環境資料庫、修補程式資料庫等資料庫
- 資料分析、研判及處理系統等分析工具
- 自動通報系統
- 事件管理及關連性分析系統
- 客戶報表系統

資安監控中心所需人員則可分成四個層次

諮詢服務人員：應具有基本的資安常識，負責客戶電話咨詢服務及簡易問題之排除

技術工程師：應具有網路及系統管理技能，並熟悉所使用的資安產品，負責監控、異常資料之分析研判、問題排除、與客戶聯繫之窗口

技術支援工程師：應具有進接網路及系統管理技能，並精通資安產品及其提供之服務，負責協助解決較困難之技術問題、異常資料之統計分析及研判、協助修正資安政策及流程、與廠商聯繫之協調

營運管理人員：應具有營運管理技能，負責整體營運管理

2.2 拜訪香港政府資訊科技署(ITSD)

ITSD(Information Technology Software Department) 共有一千多人隸屬於香港政府。對香港政府的 18 萬公務人員提供 IT 服務。本次拜訪的單位，其中有 10 人負責香港政府資安之實際落實工作。藉由拜訪以了解推行 SOC 之需求及可能的問題。有些工作由小組自行負責，其中相當的工作是委外給包括 HP 在內的公司，約有近 30 家委外公司。

資訊安全小組的工作範圍包括：

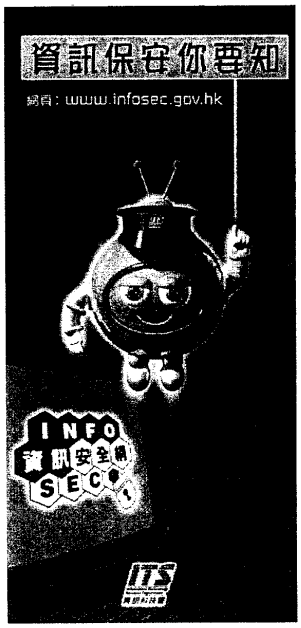
- 香港之資訊安全政策的制定
- 資訊安全政策的落實
- 弱點掃描
- 安全事件處理

- 資安資訊擷取
- 資安的訊息發佈，包括最新資安議題或軟體弱洞等
- 訓練外包
- call center
- 提供預防措施
- 提供顧問服務及解決方案

在資安觀念的宣導上強調無論對個人或企業來說，資訊形同一種資產。資訊保安乃指對這些資產加以保護，主要要求達到**機密性(Confidentiality)**－保護資訊免向未經授權人士披露、**完整性(Integrity)**－保護資訊免受未經授權人士更改、**可用性(Availability)**－讓資訊可供已獲授權人士在需要時取用、**不可否認性(Non-repudiation)**－提供原本的證據，使發件人不能否認曾發出信息，而收件人也不能否認曾收取信息、**認證(Authentication)**－用以辨識及證明嘗試發出信息或存取數據的用戶/一方身分之程序或方法等 **CIANA 的**目的。也強調資訊保安與我們息息相關，因為每個人很多時都會面對資訊保安的風險。

資安訓練除了香港政府所屬公務人員之外，還包括所有香港市民。例如製作【資訊保安你要知】，同時製作一些資訊安全小貼紙提供全香港市民資訊安全的相關訊息及法律資安常識。更不定時針對不同的族群包括中小企業、小朋友及家長/父母等舉辦資安研習會，藉以有效進行全民資安宣導。快速而有效的傳遞資訊保安的常識，使資訊安全政策可以快速落實。

資安小冊子



資安小貼紙

在提高民眾資訊安全教育上也提出了一套資訊安全自衛術：

(1) 提高本身的資訊保安意識

保護自己的資訊資產免受電腦相關罪行的攻擊，是我們每個人應負的責任。

要做的事	不要做的事
♦ 訊保安這個問題視之為你本身的責任。 ♦ 要留意有關的新聞，並學習最新的知識。 ♦ 要在有疑問時諮詢擁有相關知識的人士。 ♦ 要保存一份求助聯絡資料，例如軟件支援熱線、互聯網服務供應商服務熱線、具備技術知識而可即時提供協助的朋友或適當的組織等。	♦ 不要低估或忽視保安事故帶來的影響。有關影響可以十分嚴重，包括數據損失、個人資料外洩、耗費時間及影響他人等（例如：你的個人電腦一旦感染電腦病毒，或會把病毒進一步擴散。） ♦ 不要採取漠不關心的態度，即使你的電腦尚未遭黑客入侵或爆發電腦病毒。

(2) 處理帳戶及密碼指引

你處理撥號上網帳戶及密碼等個人數據的方式，是資訊保安的

前線工作。

要做的事	不要做的事
♦要選擇長度多於六個字的密碼，最好以隨機方式混有字母和數字。 ♦要定期更新密碼，以防密碼被黑客盜用。並要迅速更新預設的密碼和他人制定的密碼。 ♦要緊記在學校、圖書館或網吧等公眾地方離開或用完互聯網時登出系統。	♦不要洩露你的用戶號碼或密碼。 ♦不要與他人共用同一帳戶。 ♦不要使用個人資料作為你的密碼，例如姓名、 地址、生日等。 ♦不要在填寫以聯機方式遞交的表格時，填報你的用戶號碼或密碼。 ♦不要在瀏覽器內儲存密碼，又或隨便放置密碼，尤其不可放在電腦附近。 ♦不要使用舊密碼。

(3) 使用軟件須知

許多電腦軟件均可作為資訊保安的工具。

要做的事	不要做的事
♦ 要使用抗電腦病毒軟件，並要經常更新。 ♦ 要先用抗電腦病毒軟件掃描磁碟、光碟及其他儲存媒體（尤其是來歷不明者），然後才開啟使用。 ♦ 要考慮採用防火牆等保安措施，以保護採用寬頻接駁互聯網的電腦。 ♦ 要在電腦內應用最新版本的軟件及修正檔案，以堵塞已知的保安弱點。 ♦ 要定期備份系統及數據，並且妥為保存。利用備份檔案復原流失的數據是最安全及有效的方法。 ♦ 要按照安裝指示來安裝電腦軟件。 ♦ 要按照許可證條款及協議來使用電腦軟件。	♦ 不要使用非法、不可信賴或令人生疑的來源的電腦軟件及程式。 ♦ 不要在未取得版權擁有人或特許持有人明確批准前下載電腦程式。

(4) 處理電子郵件須知

今時今日，電子郵件是與人通訊的普遍方式。它帶來了極大的

方便，但亦對你的電腦系統構成威脅。

要做的事	不要做的事
◆ 要先用抗電腦病毒軟件掃描所有電子郵件附件(尤其帶有 .exe、 .com 、 .doc 等副檔名者)，然後才開啟使用。 ◆ 要關掉互聯網電子郵件軟件所備有的自動處理電子郵件附件功能。 ◆ 要考慮使用電子郵件過濾軟件來控制濫發郵件。過濾軟件讓用戶可以設定一些簡單的過濾規條來隔絕或篩出濫發郵件。	◆ 不要開啟或轉寄來歷不明的電子郵件及電郵附件。 ◆ 不要發出電郵炸彈，也不要轉寄或答覆無意義的電子郵件或惡作劇電子郵件，因為這樣做可能會引來更大批該類郵件。

(5) 瀏覽網頁及線上購物須知

現在，你可足不出戶而盡握世界。由購物、銀行服務以至進修等各式各樣的事情，現在均可透過互聯網來進行。

要做的事	不要做的事
◆ 要在獲取網上商店服務前，檢閱其免責聲明條款，例如檢閱個人私隱聲明。 ◆ 要選擇著名或可靠的網上商店。 ◆ 要留意網站有關提供資料或購物的主要措施： - 就個人資料提供知情同意書 - 應用評價認證(例如：TRUSTe 或 WebTrust) ◆ ◆ 要在遞交個人資料及進行交易前，檢查電子商貿網站的安全性(例如：保密插口層(SSL)、保密超文本傳輸規約(https)、瀏覽器的鎖子圖示、證書簽發機關等) ◆ 要在電子交易上應用數碼證書。 ◆ 要考慮使用加密技術來保護敏感數	◆ 不要啟動電子郵件應用程式/瀏覽器中可啟動內容選項(例如：Active X 、Java、Javascript 、 cookie 程式)，以防受到惡性程式碼攻擊；除非與可靠的來源進行通訊，則屬例外。 ◆ 不要從令人生疑的來源下載數據。 ◆ 不要出於好奇而瀏覽不可信賴的網站。 ◆ 不要忘記檢閱網站的私隱政策，以確保你所提供的個人數據被適當地使用和保護。

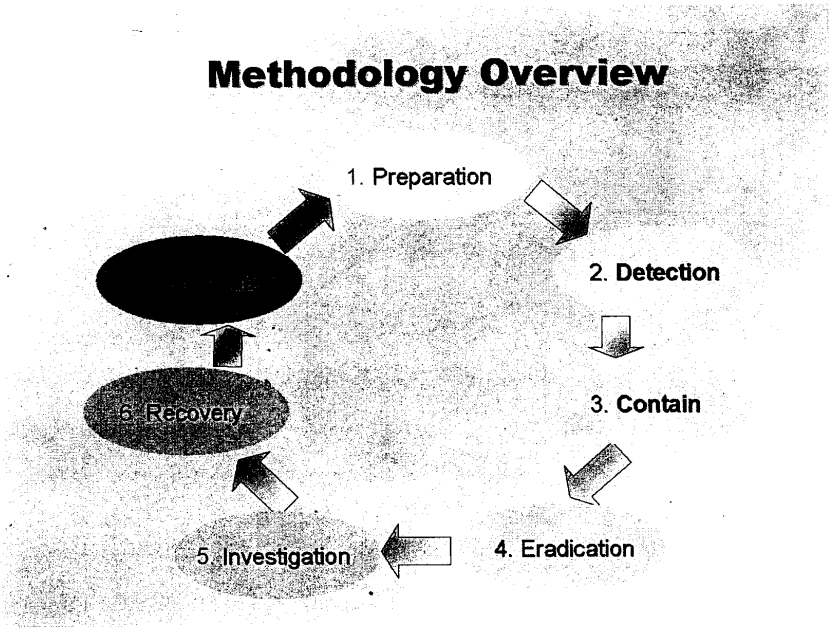
據，然後才透過公共網絡及互聯網進行傳送。 ◆ 要保留交易紀錄。大部分的電子商貿網站會在你點擊「傳送」鍵或「購買」鍵前，向你展示交易摘要。把它列印出來或存檔，日後有需要時以作參考。 ◆ 要避免遞交與搜集目的無關的任何數據。當被問及信用卡或銀行帳號等個人資料時要格外留神。 ◆ 要留意那些盛傳可疑或被標籤為「不良」網站的最新消息。	

根據 HK CERT 2001 年之統計 ：

- 總計有 1387 份資安事件報告被提出
- 估計造成約 1.5M HK$ 之財物損失
- 有較往年更多的本地攻擊事件發生

依執行面而言,針對資訊安全的確保建議可以 7 個 PHASE 的方法來處理,即 1.Preparation 2.Detection 3.Contain 4.Eradication 5.Investigation 6.Recovery 7.Follow-up , 如下圖所示 ：

Methodology overview



事件發生後 SOC 在各階段之處理模式：

1). Call to response => 2 hrs upon receive the call.

2). On-side support => 2 hrs upon request

3). Preliminary Investigation Report

=> Next day after the security incident

4). Recovery Analysis => Depend

5). Follow-up Monitorning => Negotiable

6). Detail Investigation Report => Depend

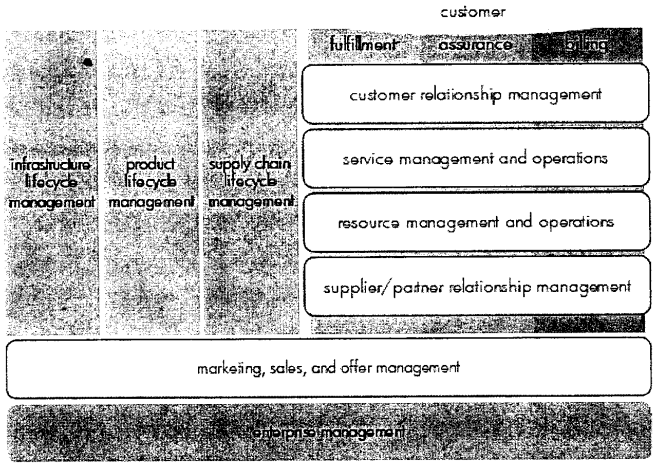
ITSD 建立 SOC 的主要成功因素

- 政府高層的支持
- 技術及經驗分享
  - 事件的處理及經驗累積
  - 技術的更新
- 資安的訓練
- 定期的檢討資安政策、標準及程序

- 公務人員守則+資訊安全準則 => 組織定位明確作業執行確實 =>員工確實遵守

2.3 HP ISM 解決方案

HP 的 ISM(Integrated Services Management)解決方案包含軟體、硬體及服務，使服務提供者(Service Providers)可以很容易地在它提供服務的所有服務元件上，來監控及管理整個服務的生命週期。ISM 基本上是植基於電信管理論壇(TMF, TeleManagement Forum)所發展的 eTOM 架構指引。eTOM 定義一個確認及組織一個服務提供者(Service Provider, 通訊或數據服務提供者，包括加值服務的提供者，例如 application hosting, unified messaging 等，通常可稱為 xSP，包括 CSP, ISP, Asp, MSP 等)重要的企業流程的架構，可以由下圖表示。



這個架構包括四大部分-兩個功能性流程群組及兩個端對端流程群組：

- 端對端客戶作業群組
  - 服務提供(service fulfillment 也稱 service delivery):將客戶訂單轉成可提供服務的流程，包括訂單處理、供應及啟用運作等過程。
  - 服務確保(service assurance):確保對客戶提供具有等級及品質的服務，假如要提供一個有保證的服務等級合約(service level agreement)，這個流程是一個關鍵。

- 服務帳務(service billing):對客戶所獲得的服務收集帳務資料，並計算費用及產生帳單的過程，HP 把它延伸稱為 service usage。

■ 功能性作業流程

- 客戶關係管理(CRM):提供可以管理客戶關係的功能，包括客戶之獲得、增加及維護等。包含對客戶以 people-based 的(櫃臺、call center、直銷等)及 web-based 的支援。
- 服務管理及作業：處理所提供給客戶產品及服務的計畫、發展及管理。
- 資源管理及作業：管理提供客戶服務所需要的基礎建設，根據企業的特性，可包括網路、電腦系統、應用及其他設備及資源。
- 供應商及企業伙伴關係管理：執行與供應商或其他服務提供者間合約的過程，包含必要的供應、帳務、障礙處理及其他流程的系統介接等。

■ 支援流程

- 行銷及推廣管理：提供服務行銷及推廣策略之需要，支援市場研究、通路及供應鍊管理、產品提供發展、及促銷活動，這個流程將驅動由 ISM 管理的服務，ISM 也將提供資訊給這個流程。
- 企業管理應用：這個流程與一般企業經營所需要的觀點一致，對服務提供者並無差異。包括企業計畫、財務管理、人力資源管理、公共關係及法制管理等，對 ISM 提供業務支援。

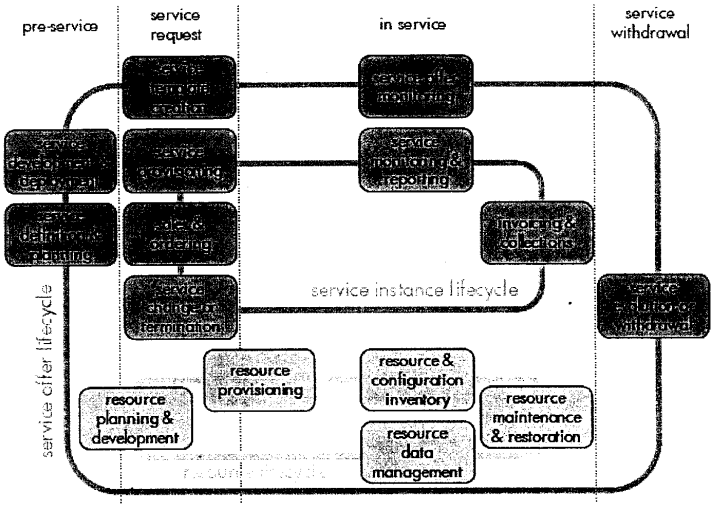
■ 端對端生命週期管理流程

- 產品生命週期管理：有關於產品的定義、計畫及實現，從這個流程可以瞭解產品的營收特性及客戶滿意度，以進一步計畫及設計新產品或更新產品。
- 基礎建設生命週期管理：對於提供服務及支援流程等基礎建設的定義、計畫及實現。
- 供應鍊生命週期管理：在現今互連的世界，大部分的服務提供者可能都是其他服務提供者的客戶及供應商，由此流程可以規劃供應鍊策略、發展供應商及伙伴關係、評估及追蹤績效。

ISM 主要著重在作業流程，關注橫跨在功能流程及端對端流程間的生

命週期，有三個主要的生命週期

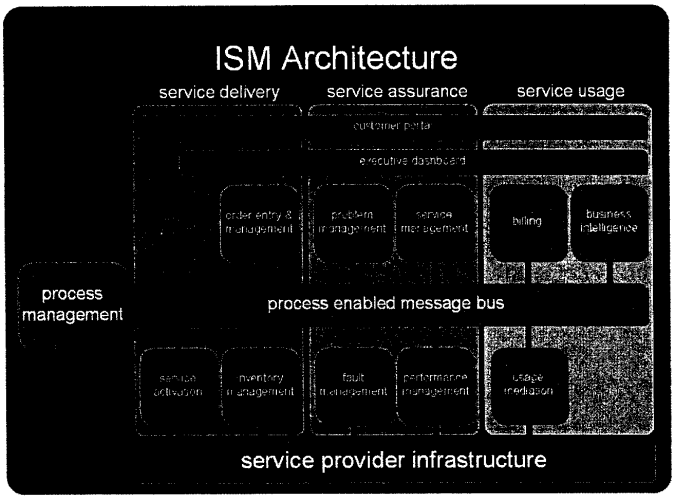
- 服務提供生命週期(service offer lifecycle)
- 服務專案生命週期(service instance lifecycle)
- 資源生命週期(resource lifecycle)



- 服務提供生命週期：這個生命週期包含不同服務產品的引進、修正及退出，接近 eTOM 的產品管理生命週期。由於新產品一般相對的引進頻率較低，因此這個生命週期相對的轉移的也較慢，許多程序需要人工步驟，程序包含：服務的定義及計畫、服務的發展及部署、產品的組合及產品的改良或退出。
- 服務專案生命週期：這個生命週期是針對個別的客戶或服務，處理變化較快的服務增加、改變、及減少，一般來說需要較多的系統整合、較少的人工介入。程序包括：銷售及訂單、服務供應、服務監控及報告、帳單及收集、服務改變及終止。
- 資源生命週期:提供服務基礎建設的構建及運作，需要支援前面兩個生命週期。有兩種型態的工作項目與資源有關，一個是類似故障維修之非計畫型的，另一種則是對新服務所部署的基礎建設、因應客戶需求增加的服務容量、或定期維修等計畫型的工作。程序包括：資源計畫及發展、資源供應、資源及架構庫存、資源維護及儲

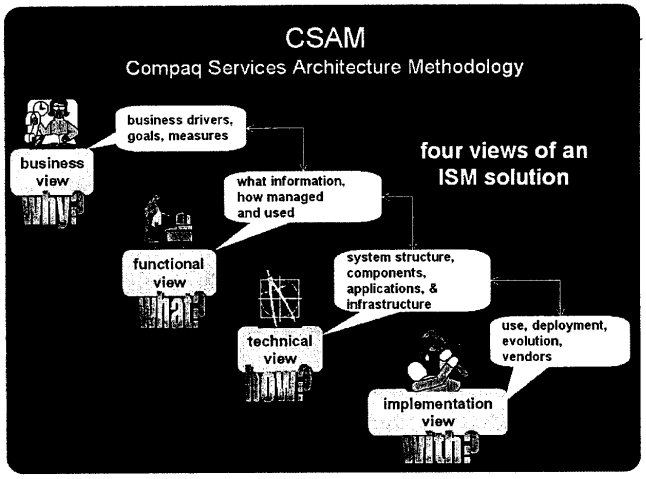
存、資源運用。

整合服務管理架構，並不是一個產品，而是一個軟體架構。HP 公司再開發或建構軟體系統時，就依照此架構建構軟體系統。藉由模組化及系統化的架構，可以快速開發完成，並可以藉由標準的機制達到共同的管理機制，例如：服務等級(Service Level Agreement, SLA)的提供。經由訊息巴士(message bus)的介接方式，系統與系統之介接介面非常單純。利用訊息巴士統一介面，可以管控 SLA 之 QoS，而非僅僅是網路層的品質保證。



在軟體開發的程序上有四個階段或步驟：

- 商業面(business view)
- 功能面(functional view)
- 技術面(technical view)
- 實作面(implementation view)



經由各階段的考量後，依照整合服務管理架構可以整合或開發一個可用的軟體系統。實作的系統可以保有相當程度的標準及共通性。最重要的是軟體系統品質可以符合使用者的需求。

3. 考察心得

對於此次赴香港考察網際網路資料中心之技術發展趨勢、服務應用及經營模式，主要的心得包括：

- 由於網路應用的蓬勃發展，資安監控中心的服務將成為一個新興業務，國家資通安全會報技術服務中心也以在數位台灣(e-Taiwan)計畫中的「建置安全的資訊通信環境」子計畫內提出「規劃與建置資通安全營運中心」的工作項目，將為政府機關提供 SOC 的監控服務，本公司在這方面的發展將可由三個觀點來考量，(1)建置委外服務的 SOC，以增取廣大的委外服務商機，尤其是針對未來的電子化政府、電子商務發展，並結合本公司自行發展的資通安全技術、PKI 技術等應用。(2)公司經營的電信網路或 HiNet 網際網路建置網路安全監控的 SOC，以提供安全可靠的網路服務品質。(3)公司內部的企業支援系統(BSS)及營運支援系統(OSS)建立資通安全 SOC，以維護公司資訊資產的安全，並提供安全的營運支援環境，本公司內的 SOC 應增加資訊應用、資訊擷取、系統監控、系統運作紀錄監控及資料使用記錄集中監控等服務項目，以建立全面的資通安全防護。在技術方面，其中的各項惡意程式碼資料庫、弱點資料庫、駭客行為模式資料庫、修補程式資料庫等，必須具有專業且長期經營建置的，非屬本公司現有的核心業務，應可尋求與資訊服務提供者，如 HP、Trend 公司 SOC 等之技術及顧問合作及聯盟。
- 資訊處正在積極規劃，並請電信研究所發展資訊資源管理系統(IrMas)，功能上將涵蓋資源管理、弱點偵測及自動告警、安全通報、安全知識庫、病毒防治管理、軟體修補程式監測、終端維修管理、軟體派送、IP 管理等，除可達成資源有效運用、資訊安全監控告警、終端使用效率等目標外，未來也可作為本公司之資訊產品，並整合到 SOC 運用。
- 為建立完整的資訊安全稽核，未來本公司應積極建立一個從資訊系統建設計畫、預算編列、系統發展、上線申請、安全檢查、上線及後續安全稽核等過程的申請、審核、驗證程序，以避免資訊系統的

重複開發、並確立共同的發展標準及安全機制。各項資訊系統也應完成安全程序(SOP) 及備援計畫的擬定。

- 在組織方面應確立專責的資訊安全人力，全力負責資安政策的落實，使本公司的資訊網路及系統可以更安全。
- 香港政府成立資訊科技署(ITSD)專責資訊政策之制訂及落實、資訊安全預防及宣導，不只在政府機構、民營企業，甚至到各級學校、學生均達到良好的成效，值得我國政府機關的參考，在相關資訊安全的宣導方式，如資安小冊子、資安小貼紙、資訊安全自衛術等作法，都能具體落實到所有的民眾，這部分的作法值得政府及公司在推廣全員資安防護觀念時之參考。
- HP ISM 在系統整合方面的技術及建構程序相當嚴謹，其相關經驗可供我們公司在系統軟體開發方面，可以利用模組化技術及共通整合介面的機制，建構快速安全的軟體發展生命週期環境，依據 eTOM 架構指引，可以檢視資訊科技對公司未來經營電子商務、內容服務及各種加值服務(總稱 xSP)是否完備，值得公司規劃資訊系統發展策略時之參考。