# 智慧電網核心標準研討會

# 我國資通訊安全標準及應用概況

標準局資訊及通信國家標準技術委員會
資安標準分組召集人 蔡敦仁

103 年 6 月 26 日

# 愛沙尼亞事件

- 2007 年 4 月，愛沙尼亞拆除蘇聯紅軍銅像引發俄羅斯人的憤怒，接下來一個月愛沙尼亞全國電腦網路遭受激烈網路攻擊，癱瘓重要網路基礎設施，包括國會、總統府、總理辦公室、政府重要部會、中央銀行、幾家主要報社等的電腦網路，都受到阻斷服務攻擊而被迫關閉，讓愛沙尼亞處於網路圍城狀態
- 愛沙尼亞國防部長說：「情況已演變成攸關國家安全的大事，和重要港口遭敵人封鎖沒有兩樣。」

# 網路恐怖主義

- 指利用網路工具破壞重要的國家基礎設施 ( 如能源、交通或政府運營系統 )，以達成其脅迫政府或人民的目的
- 具有監控和資料擷取 (Supervisor Control And Data Acquisition) 功能的軟體稱之為 SCADA 軟體，為架構在電腦上的生產自動化及控制系統
- 此類軟體應用範圍很廣，包括電力系統、水利系統、石油、化工、製造業等重大民生系統
- 並非封閉系統，正遭受重大威脅
  - Mouse click could plunge city into darkness (CNN 報導 )
  - http://edition.cnn.com/2007/US/09/27/power.at.risk/index.html

# 便利性 vs 安全性

- 便利性和安全性經常是相反的
- 增加安全性經常會減低大家的便利性
- 但不安全的系統可能造成無法彌補的損失

# 何謂資訊安全？

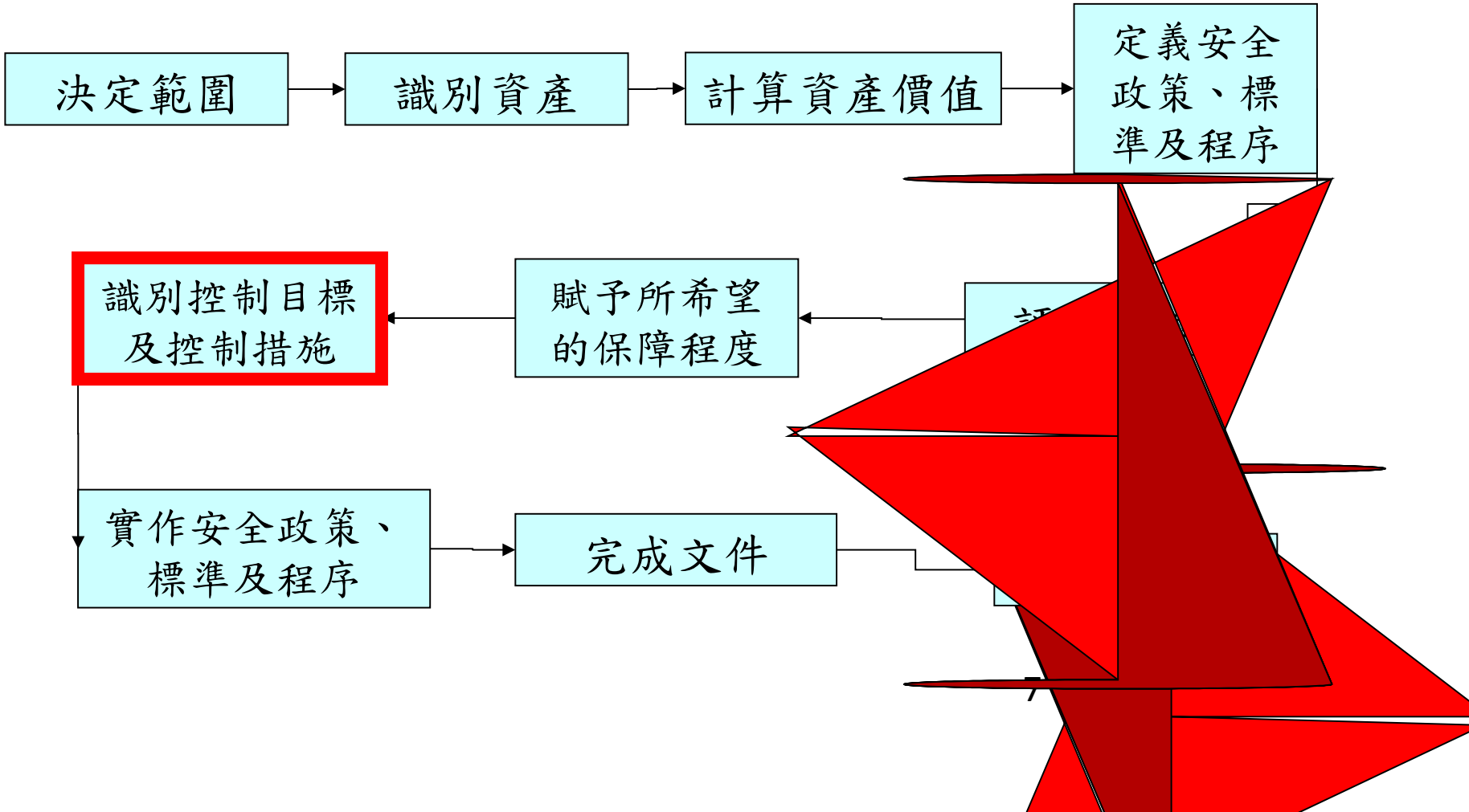
- 資訊存在的形式有許多種，可以列印或書寫於紙上表示、可以用電子方式儲存、可以用郵寄或是電子方式傳送、也可以用膠卷（片）展現或在交談中口述
- 資訊是一種資產，和其他重要的營運資產一樣，對組織營運是不可或缺的，因此需要妥善保護，此在日益互連的營運環境中特別重要
- **資訊安全**是使資訊不受各種廣泛的威脅之保護，以確保營運持續性、降低營運風險至最低、得到最豐厚的投資報酬率及最大商機
- **資訊安全**是資訊之機密性、完整性及可用性的保存；此外，亦能涉及如鑑別性、可歸責性、不可否認性及可靠度等性質

# 資訊安全之目標

- 資訊安全之目標為維護資訊之：
  - 機密性 (Confidentiality)：確定只有經授權的人才能存取資訊 => 防止未經授權的人存取資訊
  - 完整性 (Integrity)：保護資訊與處理方式的正確性與完整性 => 防止未經授權的人修改資訊
  - 可用性 (Availability)：確保經授權的使用者需要時可取得資訊及相關資源 => 防止無法取得資訊及資源

- 要達到資訊安全必須實施適當的控制措施，譬如訂定資訊安全政策、實務規範、程序、建立組織安全架構、保護硬體與網路、修改軟體…
  - 為了達成既定的安全目標，必須建立這些控制措施

# CNS 27001 之
# 資訊安全管理系統 (ISMS)



# 認證 VS 驗證

- **認證 (Accreditation)**：主管機關對某人或某機構給予正式認可，證明其有能力執行某特定工作之程序
  - 認證單位： TAF( 台灣 ) 、 CNAB( 大陸 ) 、 RAB( 美國 ) 、 DAR( 德國 ) 、 KAB( 韓國 ) 、 JAB( 日本 ) 等
  - 參加 IAF
- **驗證 (Certification)**：某一項產品、過程或服務能符合規定要求，由中立之第三者出具書面證明特定產品之程序
  - 驗證單位：經濟部標準局、 DNV 、 BSI 、 BVQI 、 SGS 等
- 通過 TAF 認證之 ISO 9001 驗證
- 27001 LA

# ISO 27001 by country (2011)

| Country | Number of certificates | % of total |
|---|---|---|
| Japan | 6914 | 39% |
| India | 1427 | 8% |
| United Kingdom | 1360 | 8% |
| China | 1219 | 7% |
| **Taiwan** | **791** | **5%** |
| Romania | 760 | 4% |
| Spain | 642 | 4% |
| Italy | 503 | 3% |
| Germany | 424 | 2% |
| United States | 313 | 2% |

# CNS 27000 系列標準

- 資訊安全管理系統 (information security management system, ISMS) 系列標準
  - ISO27k 系列標準 (ISO/IEC 27000 系列標準　)
  - 由 ISO 及 IEC ( International Electrotechnical Commission ) 共同制定
- 提供整體 ISMS 全景中，對資訊安全管理、風險、控制措施之最佳實務 (best practice) 標準
  - 類似品質保證之 ISO 9000 系列標準 及環境保護之 ISO 14000 系列標準

# CNS 27000 系列標準關係

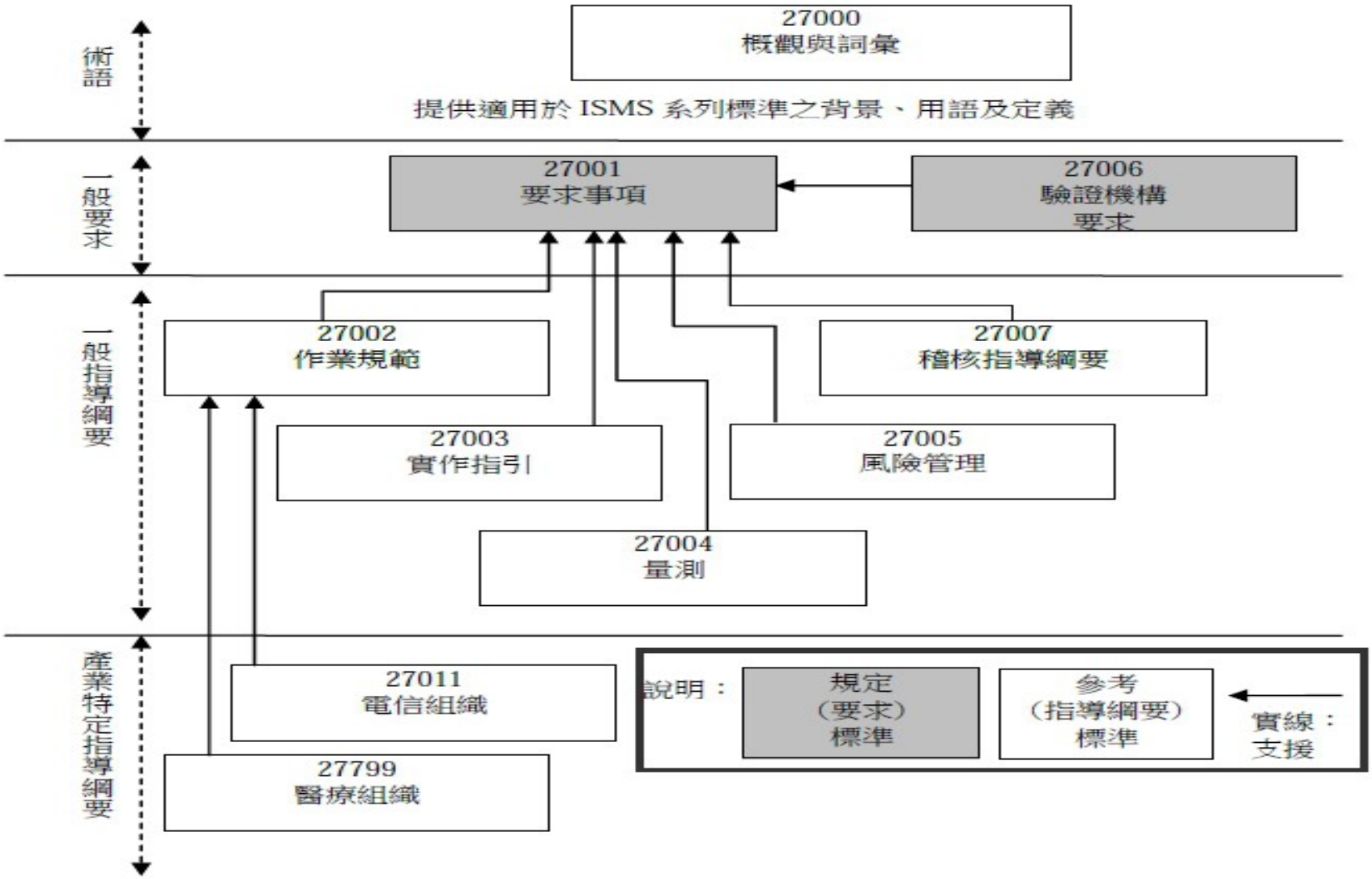



圖 1　ISMS 系列標準關係

# 27000 系列標準 (1)

CNS 27000 資訊技術－安全技術－資訊安全管理系統－概觀及詞彙

CNS 27001 資訊技術－安全技術－資訊安全管理系統－要求事項 (2013)

CNS 27002 資訊技術－安全技術－資訊安全管理之作業規範 ( 改版中 )

CNS 27003 資訊技術－安全技術－資訊安全管理系統實作指引

CNS 27004 資訊技術－安全技術－資訊安全管理－量測

CNS 27005 資訊技術－安全技術－資訊安全風險管理

CNS 27006 資訊技術－安全技術－提供資訊安全管理系統稽核與驗證機構之要求

ISO/IEC 27007 Guidelines for information security management systems auditing (focused on the management system)

ISO/IEC TR 27008 Guidance for auditors on ISMS controls (focused on the information security controls)

# 27000 系列標準 (2)

CNS 27010 資訊技術－安全技術－跨部門及跨組織通訊之資訊安全管理

ISO/IEC 27011 — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002

ISO/IEC 27013 — Guideline on the integrated implementation of ISO/IEC 20000-1 and ISO/IEC 27001

CNS 27014 資訊技術－安全技術－資訊安全治理

ISO/IEC TR 27015 — Information security management guidelines for financial services

ISO/IEC TR 27019— Information technology — Security techniques — Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy industry

CNS 29100 資訊技術一安全技術—隱私權框架

# 27000 系列標準 (3)

ISO/IEC 27031 Guidelines for information and communications technology readiness for business continuity

CNS 27032 資訊技術－安全技術－網際安全指導綱要 ( 起草中 )

ISO/IEC 27033 Network security (parts 1-5 published, part 6 DRAFT)

ISO/IEC 27034 Guideline for application security (part 1 published, rest in DRAFT(2~8))

ISO/IEC 27035 Security incident management

ISO/IEC 27036:2013 Information security for supplier relationships (parts 1 & 3 published, remainder in draft)

ISO/IEC 27037 Guidelines for identification, collection and/or acquisition and preservation of digital evidence

ISO/IEC 27038:2014 Information technology — Security techniques — Specification for digital redaction

ISO 27799 Information security management in health using ISO/IEC 27002

# 準備中之 27K 標準

ISO/IEC TR 27023 Information technology — Security techniques — Mapping the Revised Editions of ISO/IEC 27001 and ISO/IEC 27002 (draft)

ISO/IEC 27017 Code of practice for information security controls based on ISO/IEC 27002 for cloud services (DRAFT)

ISO/IEC 27018 Code of practice for PII protection in public clouds acting as PII processors (DRAFT)

ISO/IEC 27039 Intrusion detection and protection systems(IIDPS) (FINAL DRAFT)

ISO/IEC 27040 Storage security (FINAL DRAFT)

ISO/IEC 27041 Assurance for digital evidence investigation methods

ISO/IEC 27042 Guidelines for the analysis and interpretation of digital evidence (DRAFT)

ISO/IEC 27043 Digital evidence investigation principles and processes (FINAL DRAFT)

ISO/IEC 27044 Guidelines for security information and event management (SIEM) (DRAFT)

ISO/IEC 27050 Electronic discovery (DRAFT)

參考 **http://www.iso27001security.com/**

| CNS | 名稱 | ISO | 制修訂現況 |
|---|---|---|---|
| 27000 | 資訊技術－安全技術－資訊安全管理系統－概觀及詞彙 | ISO/IEC 27000 | 102 年 1 月公布制定 |
| 27001 | 資訊技術－安全技術－資訊安全管理系統－要求事項 | ISO/IEC 27001 | 95 年 6 月公布制定<br>96 年 10 月公布修訂<br>103 年 4 月年公布修訂 |
| 27002 | 資訊技術－安全技術－資訊安全管理之作業規範 | ISO/IEC 27002 | 96 年 10 月公布修訂 |
| 27003 | 資訊技術－安全技術－資訊安全管理系統實作指引 | ISO/IEC 27003 | 102 年 4 月公布制定 |
| 27004 | 資訊技術－安全技術－資訊安全管理－量測 | ISO/IEC 27004 | 102 年 1 月公布制定 |
| 27005 | 資訊技術－安全技術－資訊安全風險管理 | ISO/IEC 27005 | 99 年 2 月公布制定<br>102 年 10 月公布修訂 |
| 27006 | 資訊技術－安全技術－提供資訊安全管理系統稽核與驗證機構之要求 | ISO/IEC 27006 | 99 年 2 月公布制定 |
| 27010 | 資訊技術－安全技術－跨部門及跨組織通訊之資訊安全管理 | ISO/IEC 27010:2012 | 102 年 12 月公布制定 |
| 27014 | 資訊技術－安全技術－資訊安全治理 | ISO/IEC 27014 | 102 月公布制定 |
| 27032 | 資訊技術－安全技術－網際安全指導綱要 | ISO/IEC 27032 | 草案審議中 |

27000 系列國家標準，配合 ISO/IEC 國際標準版本之更新，適時進行調和

# 個人資料保護

**CNS 29100** 資訊技術—安全技術—隱私權框架

# CNS 15408 共同準則 (Common Criteria)

- 目標
  - 提供評鑑安全產品之方法
  - 提供如何建立更安全產品之指引
  - EAL 1~7
- CNS 15408-1：資訊技術安全評估準則—第 1 部：簡介及一般模型 ( 待改版 )
- CNS 15408-2: 資訊技術安全評估準則—第 2 部：安全功能需求 ( 待改版 )
- CNS 15408-3：資訊技術安全評估準則—第 3 部：安全保證需

# EAL 1 ~ 7

- EAL1 — functionally tested
- EAL2 — structurally tested
- EAL3 — methodically tested, checked
- EAL4 — designed, tested, reviewed
- EAL5 — semiformally designed, tested
- EAL6 — “ verified, designed, tested
- EAL7 — formally ….

# 對共同準則之要求

- EAL4 最常見
  - 美國政府對所採購產品之最低要求
- EAL7 要求正式證明
  - 很少見產品通過 EAL7
- 誰負責執行評估？
  - 認證過之實驗室
  - 很貴

# 謝　謝