



TAICS TS 5100-2-1

v0.9.0 (2017-09)

影像監控系統資安標準-網
路攝影機

TAICS TS 5101-2-1

v0.9.0 (2017-09)

影像監控系統資安測試規
範-網路攝影機

TAICS TC5 網路與資訊安全技術委員會/資策會 資安所

高傳凱 博士

2017/09/29



大綱

- 影像監控系統資安系列標準
- 影像監控系統家族
- 安全分級
- 標準框架
- 資安技術要求升級
 - 實體安全
 - 敏感資料儲存保護
 - 傳輸加密
 - 系統日誌檔警示機制
 - 隱私外洩防護
- IP CAM資安檢測制度推廣與落實規劃



影像監控系統資安系列標準

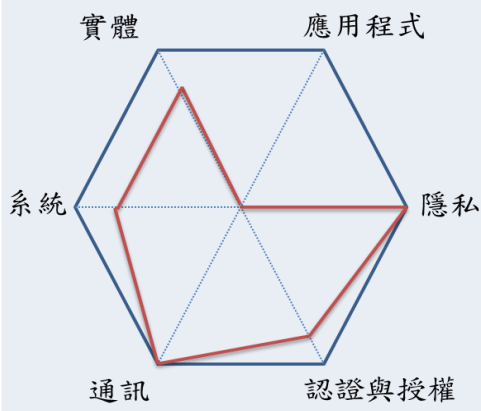
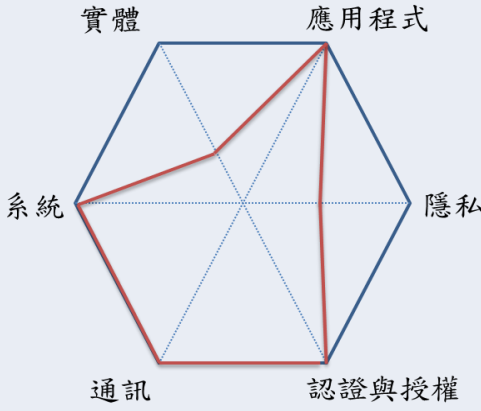
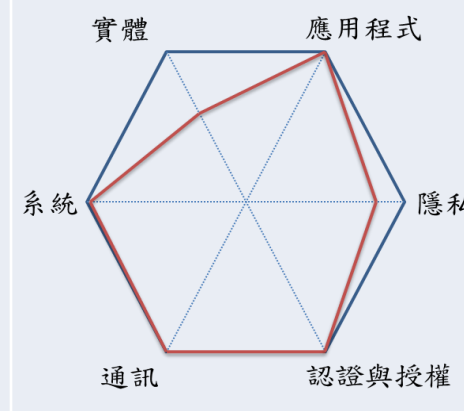
- TAICS TS 5100-1 影像監控系統資安標準 - 一般要求
- TAICS TS 5101-1 影像監控系統資安測試規範 - 一般要求

- TAICS TS 5100-2-1 影像監控系統資安標準 - 網路攝影機
- TAICS TS 5101-2-1 影像監控系統資安測試規範 - 網路攝影機

- TAICS TS 5100-2-2 影像監控系統資安標準 - 影像錄影機
- TAICS TS 5101-2-2 影像監控系統資安測試規範 - 影像錄影機

- TAICS TS 5100-2-3 影像監控系統資安標準 - 網路儲存設備
- TAICS TS 5101-2-3 影像監控系統資安測試規範 - 網路儲存設備

影像監控系統家族

差異	IP CAM	DVR/NVR	NAS
資安威脅	隱私(影像)外洩	DDoS傀儡機	勒索軟體
主功能	圖像採集	影像儲存	檔案存取
角色定位	終端	網路端	終端/雲端
資安面向	 <p>實體 應用程式 系統 隱私 認證與授權 通訊</p>	 <p>實體 應用程式 系統 隱私 認證與授權 通訊</p>	 <p>實體 應用程式 系統 隱私 認證與授權 通訊</p>

安全分級

表 1 安全要求等級總表

安全構面	安全要求分項	安全等級		
		1 級	2 級	3 級
實體安全	5.1.1. 出廠之實體埠必須具備安全管控。	5.1.1.1	5.1.1.2	
	5.1.2. 實體異常行為警示		5.1.2.1	
	5.1.3. 實體防護		5.1.3.1	5.1.3.2
	5.1.4. 安全啟動			5.1.4.1
系統安全	5.2.1. 作業系統安全	5.2.1.1	5.2.1.2	5.2.1.3
	5.2.2. 網路服務連接埠	5.2.2.1		
	5.2.3. 更新安全	5.2.3.1	5.2.3.2	
	5.2.4. 韌體程式安全	5.2.4.1	5.2.4.2	
	5.2.5. 敏感性資料儲存安全		5.2.5.1	
	5.2.6. 網頁管理介面安全	5.2.6.1		
	5.2.7. 操控程式之 API 安全	5.2.7.1		
	5.2.8. 系統日誌檔與警示			

不同等級會有對應的特定安全要求

欲符合較高等級之安全要求，必須先滿足較低安全等級要求，

數字越大，安全等級越高

1級 -
 功能及操作為主，
 專注保護敏感資訊及個人資料

2級 -
 營運規劃上考量資安的重要性，
 準備付出額外的安全工程之意願

3級 -
 保護高價值資產對抗高風險
 須使用高階安全工程技術
 落實 Secure By Design



標準框架



實體安全確保

聚焦產品拆解、實體連接埠的管控及警示機制等

實體安全

- 實體安全管控
- 實體異常行為警示

•

系統安全確保

保證網路攝影機於作業系統、網路服務及韌體之安全性

系統安全

- 作業系統安全
- 韌體程式安全

•

傳輸機密性

敏感資料的傳輸加密，及通訊協定所引發的資安威脅

通訊安全

- 敏感性資料傳輸安全
- 通訊介面的安全設置
- 通訊協定安全

存取控制

認證機制的落實、認證強度要求及用戶授權之管控

身分認證與授權

- 認證機制安全
- 密碼認證安全
- 權限管控

隱私權

限制隱私資料的存取管控，影音資料的安全傳輸

隱私保護

- 隱私資料的存取保護
- 隱私資料的傳輸保護



資安技術要求升級

實體安全



編號	安全要求
5.1.1.1	(a) 實體埠預設不得被利用來存取產品之作業系統。(1級)
5.1.1.2	(a) 所有不使用的介面應移除，包括外接式儲存媒體使用的插槽、電路板上用於除錯或測試用途之介面，必須移除。(2級) (b) 外接實體埠的插拔操作須提供日誌記錄。(2級)
	實體入侵防護
5.1.2.1	(a) 產品於實體操作時，出現鏡頭被異物遮蔽、鏡頭遭調焦及鏡頭遭轉向之異常現象時，須提供警示機制。(2級) (b) 產品於實體操作時，出現實體設備遭受破壞，例如：斷電、斷訊狀況，須提供警示機制。(2級)
	實體異常警示
5.1.3.1	(a) 產品在實體上要有一定程度的防護，可能的做法：使用防盜螺絲增加拆解的困難。(2級)
5.1.3.2	(a) 晶片與功能編號不得存在於電路板。(3級) (b) 產品實體上不得存在未經由任何工具，即可輕易還原回預設密碼的設計。(3級)
5.1.4.1	(a) 確保產品於開機時，避免未經授權的韌體、驅動程式及作業系統的執行，一旦系統的完整性及可信度獲得保證，產品始得開機。(3級)
	安全啟動



資安技術要求升級

敏感資料儲存保護

編號	安全要求
5.2.5.2	(a) 敏感資料必須存放於產品的安全區域(Secure domain)中。(3級)

完整性 + 機密性

加解密金鑰

支援安全啟動

存取驗證資料

核心軟體演算法



資安技術要求升級 傳輸加密

編號	安全要求
5.3.1.2	(a) 確保 敏感資料 之網路 傳輸加密 演算法預設必須採用 AES-256 。(3級)
5.5.2.3	(a) 確保 隱私資料 之網路 傳輸加密 演算法預設必須採用 AES-256 。(3級)



國際大廠採用



資安技術要求升級

系統日誌檔與警示

編號	安全要求
5.2.8.1	<p>1 用以檢知異常狀態</p> <p>(a) 須具備安全事件日誌檔之顯示功能，記錄使用者的存取行為得以查核未授權或異常的登入操作。該日誌檔內須包括完整時間戳記、使用者身分及操作行為等，以供審計之用。(1級) 日誌檔完整性確保</p> <p>(b) 產品須對安全事件日誌檔進行權限控管，該紀錄檔不得允許未經授權的修改，防止被竄改的可能性。(1級)</p> <p>(c) 須要求產品之日誌檔留存時間，且須符合NIST SP 800-92[9]中high impact systems的日誌資料維護長度。日誌檔可用性確保</p>
5.2.8.2	<p>2 用以檢知異常狀態</p> <p>(a) 產品須提供當安全事件日誌檔無法儲存時之系統警示功能。警示功能設計如：E-Mail通知、訊息推播、蜂鳴器等。(2級)</p> <p>3 防止波及其它影像監控設備</p>

資安技術要求升級

隱私外洩

編號	安全要求
5.5.1.1	(a) 於每次產品發生新的 存取事件 時，產品必須主動發出警示。警示功能設計如：E- Mail通知、訊息推播、蜂鳴器等。(1級)



有效防護

Insecam Project

攻擊簡介

Insecam計畫，公布包括會議、賣場、旅遊景點通通入境，直播的網站分類除美、韓、中有數千鏡頭外，台灣也在其中。這些畫面並非「駭」來的，皆是因未設定或未更改預設密碼，才會在網上流出



2015年台灣台中

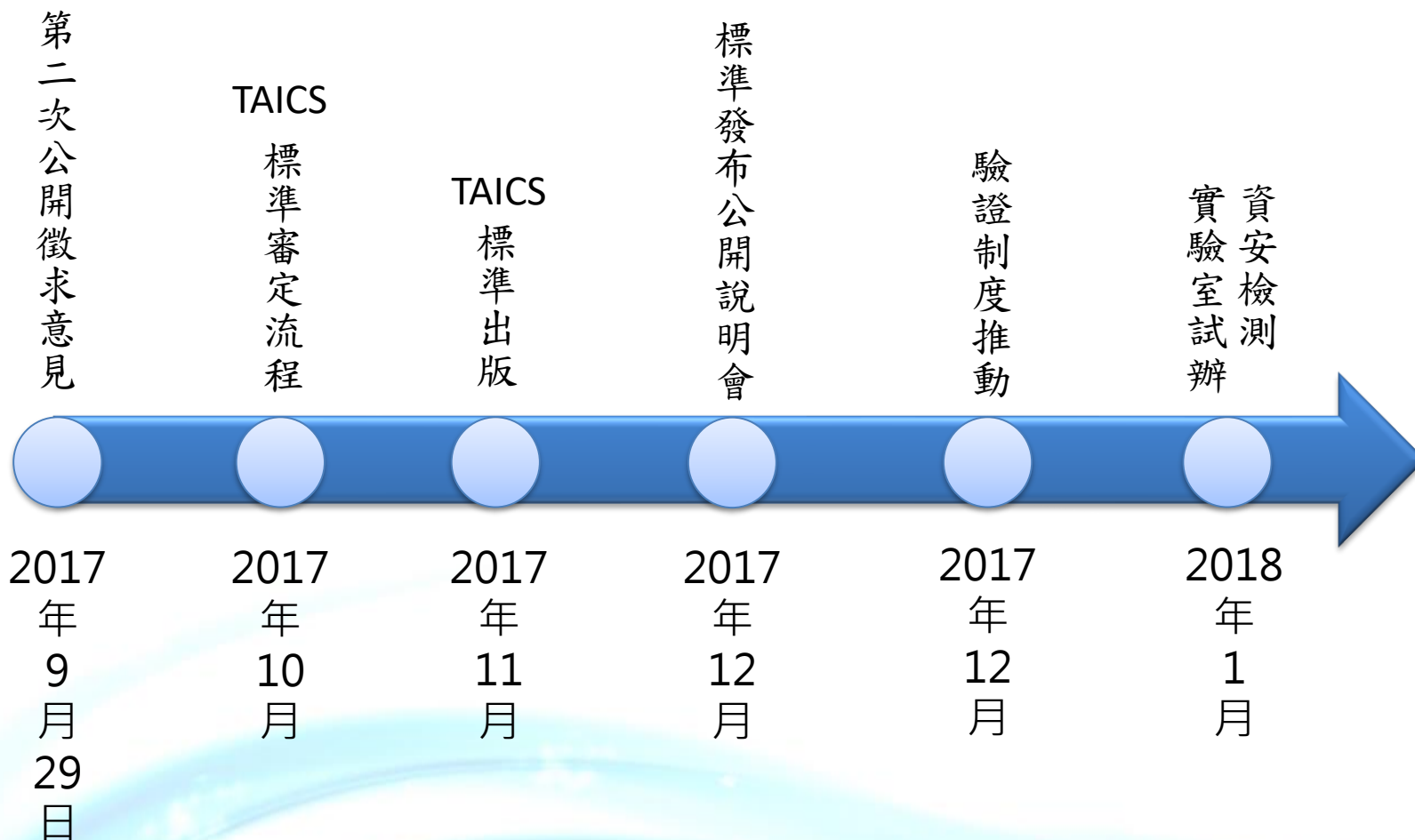
攻擊簡介

吳女準備洗澡只穿內衣褲，攝影機出現怪聲還會自動轉動，手機登入後竟發現機器登入人數是2人，當時螢幕的畫面停留在被害者的下半身，閃躲鏡頭時機器竟然跟著轉，研判產品可能留有後門。





IP CAM資安檢測制度推廣與落實





台灣資通產業標準協會

Taiwan Association of Information and Communication Standards

