F - ISAC

Financial Information Sharing and Analysis Center

建構金融資安聯防平台

金融資安資訊分享與分析中心
Financial Information Sharing and Analysis Center

F-ISAC 成立背景

行政院國家資通安全會報

國家層級

關鍵基礎設施
八大領域層級

關鍵基礎設施
領域提供者

關鍵資訊基礎設施安全管理組

基礎建設提供者

F-ISAC 成立宗旨

- 建構聯防體系
- 分享資安情資
- 強化金融業整體資訊安全

金融資安資訊分享與分析中心

建構安全的金融交易環境

- 強化資安基礎建設
- 提升金融機構資安應變及防護能量

- 增加金融機構與資安產業之互動
- 促進資安產業之發展

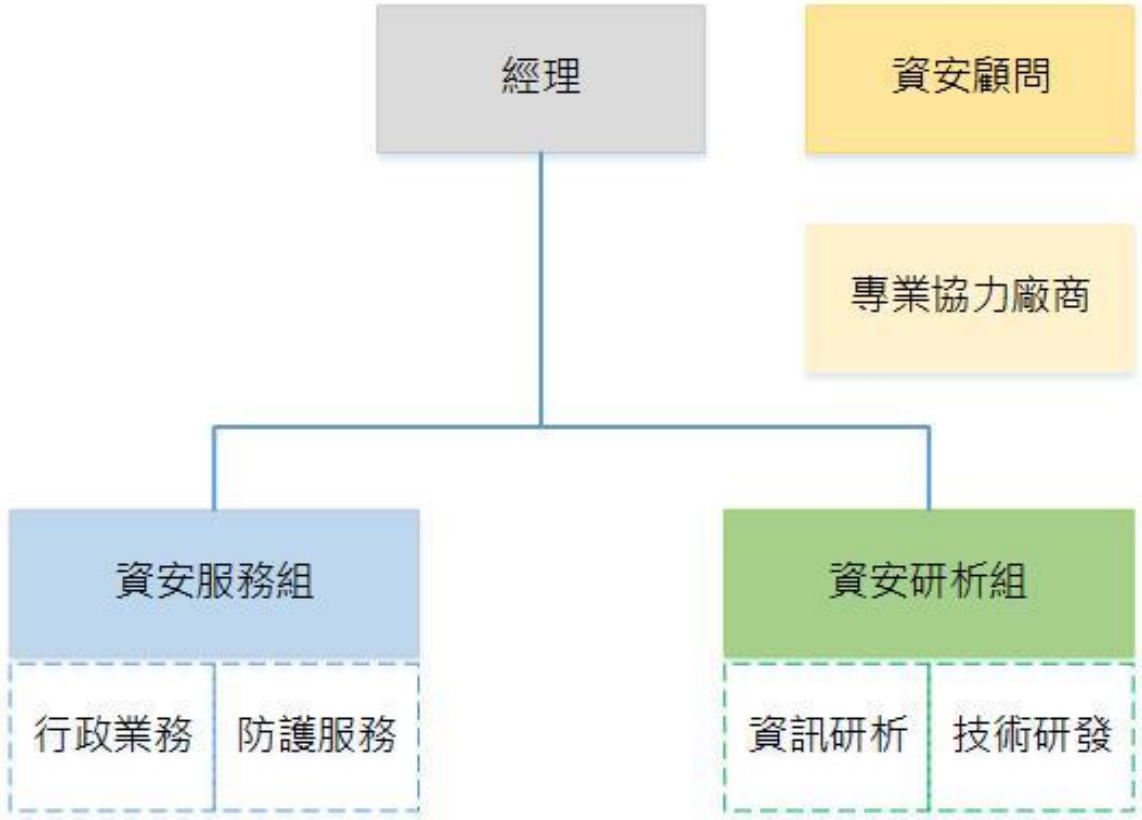
F-ISAC 運營角色

F-ISAC 運營角色


政府
高科技
醫療
國家資安資訊
分享與分析中心
(N-ISAC)
電信
交通
水源
電力
情資分享
金融資安資訊
分享與分析中心
情資分享
事件通報
銀行
保險
證券期貨
資安專業情資與技術支援
防護
監控
應變
堅強的資安防護

F-ISAC 組織構成

F-ISAC 組織構成



由主管機關、金融業公(協)會等代表組成，指導、協調F-ISAC業務推廣。

聘請產官學界熟悉金融產業資安專家，提供專案團隊相關法規、金融產業、資安技術等諮詢服務。

與資安專業廠商簽署服務契約或合作協議，依會員需求提供專業服務。

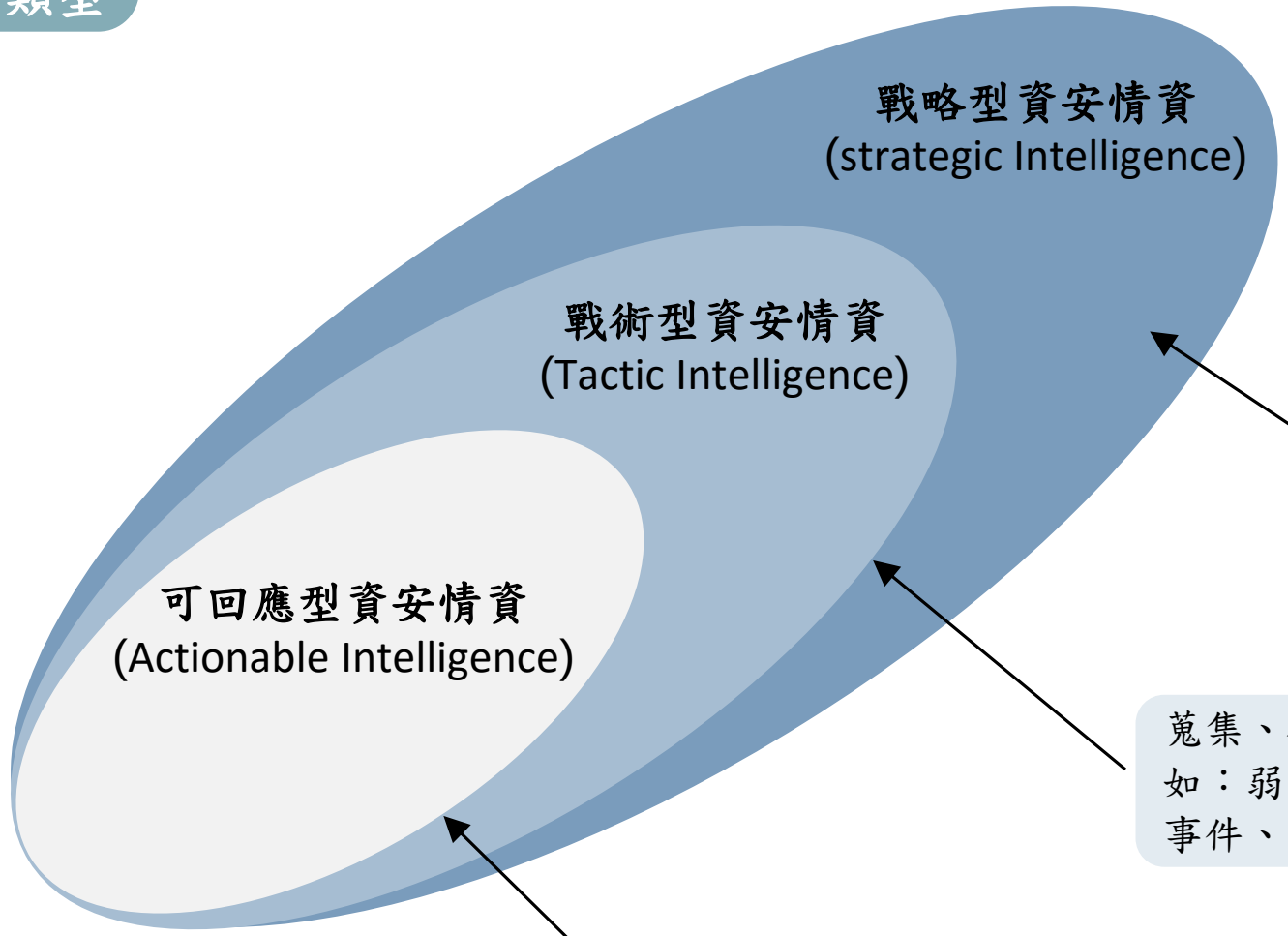
負責警訊分享、資安諮詢與評估、資安資訊分享、資安事件應變協助、系統維運、專案管理、教育訓練、研討會、國際交流、客服及行政管理。

負責資安情資研判分析、攻擊手法及數據分析、協助資安演練規劃、資安防護規畫建議、資安規範評估與建議等。

F-ISAC 情資說明

金融資安資訊分享與分析中心
Financial Information Sharing and Analysis Center

F-ISAC 情資類型



透過長期觀察、研究金融資安事件與駭客行動，預估未來之資安威脅趨勢。

蒐集、研析最新威脅與攻擊手法如：弱點資訊、網頁攻擊、入侵事件、資安新聞等。

可立即進行比對、封鎖威脅之情資如：惡意中繼站IP、網域、檔案雜湊值（Hash）等。

F-ISAC情資流程

Threat Intelligence Process

1 蒐集

多元管道匯集情資

- 國內外公開/付費來源，如FIRST、NIST、ENISA等。
- CERTs
- ISACs
- SOCs
- 會員機構警訊分享

2 處理

關鍵情資處理分析

1. 衡量情資可信度
2. 廣泛蒐集相關訊息
3. 分析情資意涵
4. 評定情資重要性
5. 建議可行方案

3 發佈

重要情資訊息發佈

- 定期(週/月/半年)以email發送情資報告。
- 如遇緊急事件，即時以email或簡訊發送訊息。

4 回饋

會員機構需求回饋

- 依會員機構反應及需求，適時調整F-ISAC情資服務內容。

F-ISAC 防護對策

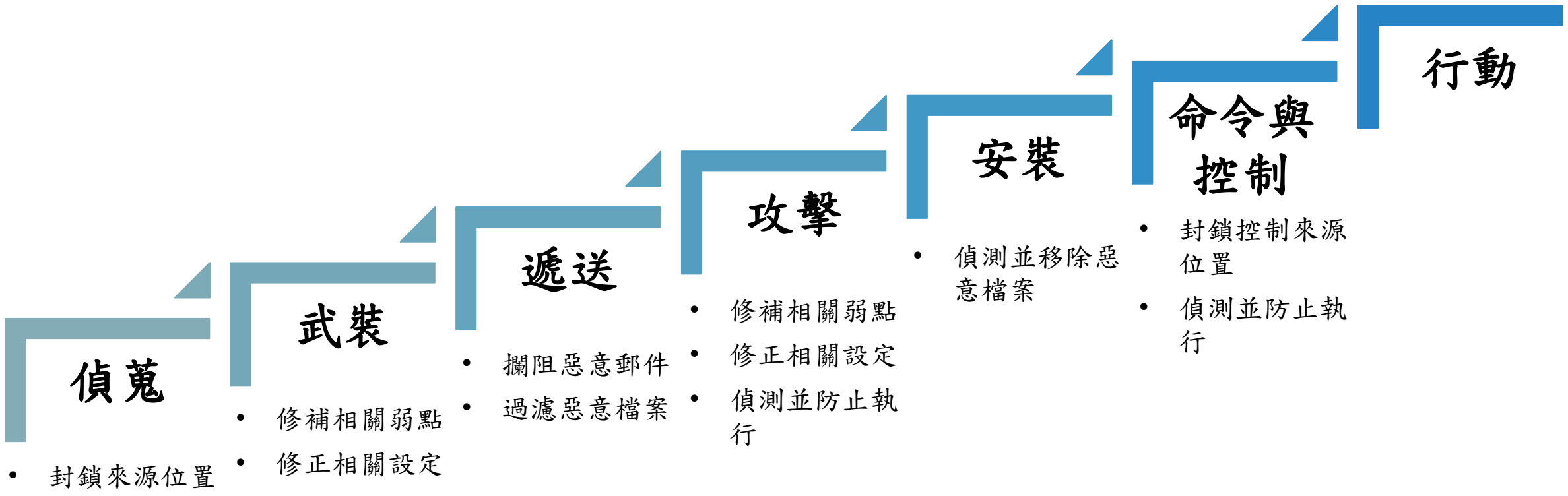
Prevention(預防)
會員可參考F-ISAC提供之資安威脅情資，預防潛在資安攻擊威脅。

Detection(偵測)
會員可依據情資報告之威脅特徵等資訊，以偵測、搜尋組織內部是否存在類似之資安攻擊威脅。

Response(應變)
會員依情資報告評估、研判、建立相關之應變計劃與程序，以有效、快速反應資安事故處理。

Mitigation(緩解)
會員可參考情資報告提供之處置作為，以減輕資安威脅造成之損害。

攻擊防禦之情資運用


偵蒐
封鎖來源位置
武裝
修補相關弱點
修正相關設定
遞送
攔阻惡意郵件
過濾惡意檔案
攻擊
修補相關弱點
修正相關設定
偵測並防止執行
安裝
偵測並移除惡意檔案
命令與控制
封鎖控制來源位置
偵測並防止執行
行動

情資發展趨勢

- 情資的使用範圍已逐漸擴大。
- 情資已與產品整合，提供預防性偵測或防禦。
- 情資的交換已有公開的標準。
- 使用者正參與情資的分享。

F-ISAC 服務規劃

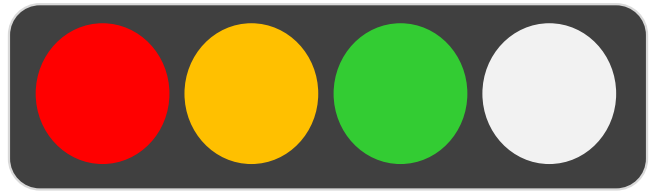
F-ISAC 服務規劃

金融資安資訊分享與分析中心
Financial Information Sharing and Analysis Center

警訊通報分享並非資安事件或事故之法定通報。

接收會員通知之資安發現或事件，經分析確認後依會員提供資訊之燈號(Traffic Light Protocol，TLP定義)進行後續之分享或告警，並視會員需要依相關作業程序協助會員處理。

以F-ISAC蒐集之資安情資為基礎，依威脅等級發布緊急資安訊息，並視需要追蹤後續處理情形。



TLP是信賴的處理原則

紅燈 TLP:RED

資訊僅限提供者指定之限定群組，通常透過口頭或面對面進行資訊交換。

黃燈 TLP:AMBER

接收者只可與自己組織的成員及需要了解這些資訊的廠商(進行必要之處理以防止傷害擴大)分享，但提供者仍可自由指定特定之資訊分享限制。

綠燈 TLP:GREEN

接收者可以與同屬單位或社群的人員或夥伴組織分享，但並非透過公開存取管道，且不可以在社群外散布。

白燈 TLP:WHITE

基於標準版權規則，此資訊可以無限制的散布。

蒐集國內外資安廠商、媒體、國際組織或會員提報之資安情資，分析其攻擊手法、潛在威脅或資安風險，提供以下服務：

- 定期提供會員資安威脅情資週報及月報。
- 不定期提供會員資安威脅情資報告。

資安威脅情資報告

- 資安威脅簡介
- 攻擊手法分析
- 威脅偵測與防護建議
- 弱點修補程序
- 相關參考資料

週報

- 彙整前一週資安威脅
- 惡意IP或URL資訊
- 惡意檔案或程式資訊
- 弱點、漏洞資訊

月報

- 當月資安威脅摘要
- 資安事件案例分析
- 重大資安新聞觀察
- 攻擊事件類型統計
- 攻擊來源分布統計
- DDoS攻擊流量統計
- 惡意軟體統計

半年報

- 前半年資安攻擊統計彙整
- 前半年重大資安事件回顧
- 後半年資安威脅趨勢預測

F-ISAC與「國家資安資訊分享與分析中心(N-ISAC)」等單位交換與分享資安情資。

F-ISAC與會員間分享與交流相關資安情資。

辦理資安研討會提升整體會員機構資安防護意識。

舉辦金融產業資安從業人員相關訓練課程。

參與國際資安相關交流活動。

金融資安資訊分享與分析中心
Financial Information Sharing and Analysis Center

依F-ISAC蒐集之資安情資為基礎，彙整資安漏洞資訊及相關修補程序或控制措施，提供會員資安諮詢服務。

依F-ISAC相關作業程序引介專業廠商或團體，提供會員資安諮詢與漏洞評估服務。

蒐集相關機構防護現況與需求。

依F-ISAC相關作業程序，就會員資安事件應變處理之需求，引介專業廠商或團體。

因應金融資安事件，研提資安防護及應變處理加強措施。

金融資安資訊分享與分析中心
Financial Information Sharing and Analysis Center

F-ISAC 入會事宜

F-ISAC 入會事宜

填寫申請書

會員參加/退出申請書

會員基本資料(異動)表

金融資安資訊分享與分析中心
會員參加/退出申請書

申請事項	☐ 加入會員 ☐ 退出會員			申請日期： 年 月 日	
基本資料					
業別	☐主管機關 ☐業管單位 ☐公(協)會 ☐銀行 ☐保險 ☐證券 ☐期貨 ☐投信 ☐投顧 ☐其他				
機構名稱	中文				
	英文				
證照號碼					
聯絡人					
同意聲明					
簽章	本機構申請成為金融資安資訊分享與分析中心之會員，並同意遵守其營運規章。				
審查結果		會員編號		參加日期	退出日期

填表說明：

1. **申請成為金融資安資訊分享與分析中心之會員，即已同意遵守本中心公告之營運規章。**
2. 證照號碼：營利事業單位請填寫營利事業統一編號，非營利事業單位請填寫扣繳單位統一編號或公務單位統一編號。
3. **辦理入會申請或會員資料異動時，請填寫「會員基本資料(異動)表」。**
4. 簽章欄請押蓋申請機構大小章。
5. 如果您對於會員申請有任何問題，歡迎來電洽詢(02)2655-7077，或 E-mail 至本中心客服信箱：service@fisac.tw。
6. 申請書正本請郵寄至台北市 11485 內湖區康寧路三段 81 號，「金融資安資訊分享與分析中心」收。

深紅經機內各欄請會員參照填表說明詳細填寫。

金融資安資訊分享與分析中心
會員基本資料(異動)表

填表日期	年 月 日							
基本資料								
業別	☐主管機關 ☐業管單位 ☐公(協)會 ☐銀行 ☐保險 ☐證券 ☐期貨 ☐投信 ☐投顧 ☐其他							
資料別	**異動前資料**				**異動後資料**			
名稱	中文							
	英文							
證照編號								
網址	http://				http://			
代表人								
地址								
電話								
傳真								
對外 IP 位置								
會員聯絡窗口								
人員別	**異動前資料**				**異動後資料**			
資安主管	姓名		職稱		姓名		職稱	
	電話		傳真		電話		傳真	
	電子信箱				電子信箱			
資安聯絡人(一)	姓名		職稱		姓名		職稱	
	電話		傳真		電話		傳真	
	電子信箱				電子信箱			
資安聯絡人(二)	姓名		職稱		姓名		職稱	
	電話		傳真		電話		傳真	
	電子信箱				電子信箱			
同意聲明								
簽章	(申請機構大小章)				(於會員聯絡窗口提供個人資料之人員，請閱讀第2頁之「金融資安資訊分享與分析中心個人資料保護聲明」，確認同意提供資料後分別於本欄簽名。)			
審查結果		會員編號			異動日期			

深紅經機內各欄請會員擇加填寫，填表說明請參閱背面。

營運規章

會員應遵守事項

會員及其所屬人員應妥善保管F-ISAC核發之帳號及密碼，避免遭盜用或外洩。

會員應確保自身網路之正常運作，F-ISAC不負因該網路相關問題致無法使用本中心服務之責。

會員如發現資安威脅，可循F-ISAC相關作業程序通報、登錄及回報後續處理情形。

會員應注意就其存取與使用F-ISAC平臺系統過程中，防免第三人可能利該平臺系統連結之相關渠道進行駭客攻擊、病毒植入、惡意程式或其他任何不法方式之行為而有侵害F-ISAC之虞。

營運規章

事故責任

F-ISAC不擔保所提供之服務符合會員之所有需求，且不擔保該服務可提供所有網路入侵、攻擊等惡意程式之資訊，亦不擔保服務內容得百分之百有效防堵或解決會員之資安問題。

F-ISAC不擔保或認證個別會員之資安防護狀態，會員自身之資安防護作業應自行負責。

營運規章

費用

自一0六年十二月一日起至一0七年十二月三十一日止免予收費。

F-ISAC得依相關作業程序引介專業廠商或團體提供會員資安服務，惟專業廠商或團體之相關服務費用須由會員自行負擔。

入會效益

取得國內外的金融資安情資，及時發現並因應類似之資安威脅，避免造成資安事故。

取得資安事故處理之協助，縮短異常回復之時間或減小事故之影響。

了解最新之資訊安全防禦技術及趨勢，維持組織內之資安防禦能量。

成為國內金融資安社群的一員，掌握國內金融資安之脈動。

歡迎加入 F-ISAC

F-ISAC會員服務資訊

電話：(02)2655-7077分機 9

傳真：(02)2655-7099

信箱：service@fisac.tw

網址：https://www.fisac.tw/

營運時間：每週一至週五上午9點至下午6點

金融資安資訊分享與分析中心
Financial Information Sharing and Analysis Center

金融資安資訊
分享與分析中心