行政院所屬各機關因公出國人員出國報告書

(出國類別：其他)

支付系統受到網路攻擊之復原方案暨金融市場基礎設施準則(PFMI)評估

服務機關：中央銀行

出國人職稱：一等專員

出國人姓名：吳桂華

出國地點：印度班加羅爾

出國期間：104.5.24-104.5.28

報告日期：104 年 8 月 20 日

目錄

壹、前言

一、研討會過程

本次參加 SEACEN 第 14 屆「新興經濟體支付及清算系統高階訓練課程-支付系統受到網路攻擊之復原方案」研討會，假印度班加羅爾舉行，由印度央行協辦，邀請來自國際清算銀行(BIS)、馬來西亞、泰國、韓國、香港及菲律賓等資深之資訊及支付系統人員擔任講師。

參與研討會之國家共計 12 國，除我國外，尚包括汶萊、柬埔寨、印度、印尼、韓國、寮國、馬來西亞、尼泊爾、菲律賓、斯里蘭卡及泰國，合計 35 名學員。

授課範圍主要集中在支付系統因應網路攻擊之相關措施及復原方案，以及金融市場基礎設施準則(Principles for Financial Market Infrastructures, PFMI)。詳細內容包括：網路安全(Cyber Security)與支付系統面對之資安議題、支付系統創新所帶來之風險、PFMI 概述及實施情況、網路安全之威脅及風險消弭措施、支付清算系統之網路安全管理以及如何抵禦網路攻擊、國家分享報告與小組案例討論與報告。

在研討會國家分享報告單元，SEACEN 於研討會第 3 天方選定 6 個國家進行簡報，依序包括：馬來西亞、臺灣、印尼、韓國、泰國及印度。國家分享報告部分主要重點如次：

(一) 六個國家簡報者均表示，央行營運之系統多屬封閉式網路系統，未曾受到網路攻擊影響。

(二) 惟馬來西亞表示，該國銀行等金融機構面對分散式癱瘓網路攻擊(DDoS)之威脅正提高。

(三) 韓國與會者表示，數家金融機構在 2013 年間遭受網路攻擊，導致銀行資訊系統失靈並洩漏數位認證等相關資訊，近 32,000 部電腦停止運作，自動提款機及銀行間連線系統亦中斷近 2 小時。

研討會最後一天進行小組案例討論與報告，與會者分成不同小組，每小組約 6 人，討論如何依據國際機構(如 BIS 等)發布之網路安全報告，研擬網路攻擊防禦方案並進行小組簡報。

本次研討會結束後，另隨同本局陳局長一端參加 SEACEN 局處長級會議開幕儀式，開幕式由印度央行副總裁 Mr. Khan 致詞，其認為網路攻擊威脅提高，歸納 7 個 S 作為網路安全(Cyber Security)之參考，包括：

1、 擬具整合性防禦策略(Strategy)
2、 強化網路系統監控措施(Surveillance)
3、 資訊分享(Share Information)：儘速將系統受網路攻擊之訊息通報相關單位及使用單位，俾利大家提早採取因應措施
4、 提高同仁對網路攻擊之憂患意識(Sensitization)
5、 進行網路攻擊模擬演練(Simulation)
6、 模擬演練得知系統何處存在脆弱性後，加強安全保護(Safeguard)措施
7、 從外部系統提供者到本身組織內部同仁，均應與時俱進強化相關網路安全技能(Skill)

二、 研究目的

近年來金融相關行業遭受之網路攻擊逐漸增加，一旦重要的支付及清算系統受到攻擊且無法即時復原運作時，將會使系統參與者與使用者對該系統失去信心，進而影響金融穩定。

本次參與第 14 屆「新興經濟體支付及清算系統進階訓練課程-支付系統受到網路攻擊之復原方案」研討會，旨在瞭解相關網路攻擊之型態及解決方案，俾利央行未來進行PFMI評估。研討會藉由與會者互動交流意見、進行國家分享報告及小組案例討論與報告等課程設計安排，使與會者獲益匪淺。

本報告後續章節安排如次，第貳章介紹研討會課程內容，其中包括網路攻擊及系統復原概述、BIS 提出之網路攻擊整合性復原方案以及對應之 PFMI 評估；在 PFMI 評估方面，除就評估注意事項、國際間辦理現況加以說明外，並摘述韓國央行之 BoK Wire+接受世界銀行及 IMF 工作小組進行 PFMI 評估之主要結論，以作為我國未來進行 PFMI 評估之參考；最後，第參章提出心得與建議。

貳、研討會內容重點

一、 網路攻擊及系統復原概述

金融相關系統遭受網路攻擊之情形逐漸頻繁、複雜，且攻擊面向更廣泛，依據 ENISA[1]統計，歐洲受到 15 種型態的網路攻擊，有 10 種型態的攻擊威脅增加、4 種型態攻擊趨勢下降、1 種持平(附錄 1)，整體而言，網路攻擊之威脅處於增加趨勢。

一般而言，網路攻擊者包括以下幾類：

(1) 駭客(Hacktivists)：侵入系統影響運作，純為滿足其成就感；

(2) 網路犯罪者(Cyber Criminals)：動機則是為獲取財務利益；

(3) 網路恐怖分子(Terrorists)：旨在造成政治及金融不穩定；

(4) 國家網路間諜(Nation State-Related Actors)：試圖竊取國家機敏資料。

近年來網路攻擊型態(附錄 2)快速演進，如傀儡網路(Botnet)[2]、社交工程(Social Engineering)[3]及進階持續性滲透攻擊(Advanced Persistent Threat, APT)等方式，造成不少損害案例(附錄 3)，例如：JPMorgan Chase 於 2014 年間遭受網路攻擊，造成 8,300 萬名客戶之姓名、地址、電話及郵件信箱被竊，主因該公司少部分電腦網路系統僅採用單層安全驗證系統(其他電腦系統與其他機構則均採雙層驗證機制)所致。

金融市場基礎設施(Financial Market Infrastructures, FMI)受到之攻擊點不僅只源自於 FMI 本身，亦可能從其他外部系統多個攻擊點進入，例如；相互連結之其他系統、系統使用其他系統供應商之商品(Vendor Products)、子工作站，以及機構內之惡意員工等。

---

[1] 歐洲網路及資訊安全聯盟組織(The European Union Agency for Network and Information Security, ENISA)致力於提供歐元區及會員國有關資訊安全之建言及建議。

[2] 受害電腦一旦被植入可遠端操控該電腦的惡意程式，即會像傀儡(或機器人)一般任人擺佈執行各種惡意行為，當一部電腦成為傀儡網路的一部分時，意味著 Botnet 操縱者可將募集到的龐大網路軍團當作機器人來遠端遙控，從事各種非法入侵並竊取資料。

[3] 社交工程惡意程式專門假冒其他軟體或隱藏在其他軟體之內，引誘使用者下載並安裝該軟體，藉此趁機安裝惡意軟體，進而導致機密資訊遭盜用竊取、損毀或外流。

有關網路攻擊與 PFMI 之關係，PFMI 準則 17 作業風險及準則 2 公司治理部分，均須就網路攻擊及資訊安全等措施進行評估。此外，準則 17 之主要考量 6 要求 FMIs 應能在受到網路攻擊後 2 小時內，恢復主要系統運作[4]，即使受到極端網路攻擊情況下，亦應能在日終前結束所有清算作業。

在網路攻擊與央行清算最終性部分，鑒於央行 RTGS 清算之款項一旦經移轉後，即具有不可撤銷性及無條件移轉之特色，即使因網路攻擊事件導致款項異常移轉，亦具有不可撤銷性，俾利維持金融交易事件之確定性及金融穩定。BIS 工作小組咸認，為維持央行清算之最終性，即使款項移轉之收入方無權擁有該款項(例如，網路攻擊使款項誤轉)，已執行之交易指令亦不得撤銷(Irrevocable)，而係應重新輸入另一個反向且金額相同的交易指令抵銷(Offset)先前因網路攻擊而未經正當授權之交易指令。

此外，許多國家已採用之風險管理及營運不中斷計畫係為防範實體(Physical)攻擊如地震及其他天然災害而設計，在防範網路攻擊時不但效果不佳，反倒可能會加重受害。

例如，自動即時備援系統(Automated Backup Systems)在受到如地震等實體災害攻擊時，透過自動備援可有效保存資料在異地系統，即使主系統因地震受損，異地系統亦能接續運作。但若系統受到網路攻擊，已被植入惡意程式並造成交易資料不正確，反會因即時自動備援而將惡意程式及錯誤資料立即傳播至備援系統，造成主系統及備援系統均受損。

二、 BIS 提出之網路攻擊整合性復原方案

BIS 成立工作小組研究各國對網路攻擊議題之看法，並於 2014 年 11 月發布相關報告，其中發現:(1)由於各個 FMI 相互連結及相互依賴，且網路攻擊的型態及動機愈趨多樣性及複雜度，使得網路攻擊變為 FMI 之首

[4] 並非要求系統受攻擊後 2 小時內全面恢復運作，而係指系統主要功能恢復運作，並能針對優先交易項目提供服務

要議題；(2)考量 PFMI 準則 17 建議，FMI 在受到網路攻擊 2 小時內須將主要系統復原運作之目標(2-hour Recovery Time Objective)，雖可能有其難度，但部分受訪者認為如採用整合性的解決方案則可望達成此目標；(3)FMI 間相互連結產生環環相扣甚至跨國資訊交換及分享之問題，爰 FMI 多支持主管機關提供誘因及動力，促使 FMI 間進行溝通及協調，俾有效解決網路攻擊問題。

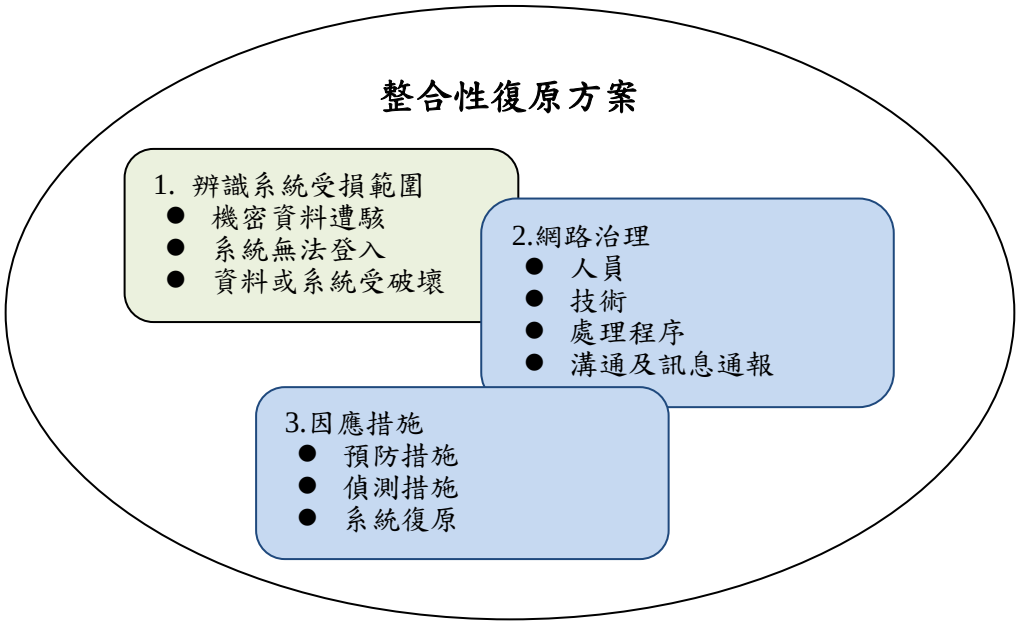
現今網路攻擊環伺的時代，企業必須瞭解到不可能完全消除遭受網路攻擊之風險，而須調整心態朝向建構出遭受網路攻擊後之復原措施及方案。爰 BIS 提出 FMI 系統因應網路攻擊之整合性復原方案，其中包括三大面向(圖 1)：

(一)辨識系統受損範圍(Scope)

(二)網路治理(Cyber Governance)

(三)因應措施(Range of Measures)

圖 1　網路攻擊之整合性復原方案



資料來源：BIS (2014), Cyber resilience in financial market infrastructures

(一) 辨識系統受損範圍(Scope)

須有相關技術及措施能辨識出系統受到攻擊的範圍,再採取因應方式。通常網路攻擊造成以下幾種受損情況：

1、機密資料遭駭(Confidentiality Breach)：FMIs 受網路攻擊，機敏資料被偷走。

2、系統無法登入(Availability Breach)：FMIs 受網路攻擊導致參加人及使用者無法登入使用。

3、資料或系統遭受破壞(Integrity Breach)：此情況影響最嚴重，將使系統運作之正確性及完整度受損。

下表顯示上述三種網路攻擊事件,損害之嚴重程度由情況 1 至情況 3 逐漸增加：

表 1　網路攻擊造成損害之嚴重程度

情況 1	情況 2	情況 3
機密資料遭駭	無法登入系統	資料或系統受到破壞
• 機密資料被駭 • 系統提供服務之功能未必受損 • 網路攻擊者可能會再進一步攻擊造成更大損害 • 不易得知被攻擊以採取因應措施 • 損害 FMI 信譽	• 被持續網路攻擊並導致系統癱瘓無法提供服務 (Distributed Denial-of-Service) • 影響 FMI 與參加者間的通信、影響 FMI 對其參加者的支援、影響 FMI 更新服務內容、影響 FMI 與交易對手的資訊交換 • 系統當機愈久，參加者及金融市場混亂的	• FMI 核心資料或系統因網路攻擊而損壞 • FMI 資訊系統之完整性已無法再被信賴 • 備援系統可能亦損壞 • 攻擊事件後，開始會以為系統運作正常，但必須儘速偵測問題俾決定是否應

	情況就愈惡化	停止系統提供服務，以便回復系統到未受攻擊前的可信賴狀態 • 須花時間偵測及分析問題 • 確認系統回到未受攻擊前的狀態，俾利重新啟動系統 • 可能產生全面性影響，因為參加者在作業系統中的部位被卡住無法移轉，亦無法信賴資料之正確性 • 由於無法相信參加人正確的持有部位，可能導致對金融市場的信心喪失 • 對其他 FMI 可能產生連鎖效應，包括參加者及其客戶造成流動性風險及信用風險

資料來源：BIS (2014), Cyber resilience in financial market infrastructures

(二) 網路治理(Cyber governance)

1. 人員(People)：從系統作業同仁至資深管理階層甚至到董事會，均應

參與並瞭解網路攻擊復原方案。網路攻擊不僅是系統運作議題，亦可能因外界對該系統喪失信心而演變為企業全面性的風險並涉及企業存續問題。資深管理階層如能介入網路攻擊整合性復原方案之建置，將更能引起組織內全體同仁之防範意識。

2. 技術(Technology)：網路攻擊者通常可辨識出系統的弱點，並繞過入侵偵測軟體進行攻擊，爰須有儘速恢復系統運作之完備技術。
3. 處理程序(Process)：應建立適當程序，包括監控系統作業、對網路攻擊之風險意識之認知、對各種突發情況之因應方式，以及系統關閉服務之時機及政策為何。
4. 溝通及訊息通報(Communication)：FMI 系統涉及參加者、系統服務廠商或外部系統販賣商，一旦受到攻擊，宜儘速通報利害關係單位，以避免其他單位亦被攻擊，導致損害層面擴大。然而部分 FMI 與國外系統相連結，如欲進行溝通及訊息分享時，往往面臨彼此信任等問題，主管機關如能介入協調 FMI 與國外相關單位進行資訊互享，將有利提升網路安全。

(三)因應措施(Range of Measures)

必要的資訊系統投資能阻卻並降低網路攻擊的程度，BIS 建議就預防(Prevention)、偵測(Detection)及復原(Recovery)等多個層面進行防禦控制措施(Layered Cyber Resilience Measures)，此三個層面的因應措施有相互強化(Mutually Reinforcing)的效果。以往對於網路攻擊著重在如何預防，惟近期普遍認為網路攻擊係難以完全避免，故轉為非常重視資訊系統復原能力之因應措施。

1. 預防措施：FMI 的系統必須具備偵測網路入侵之能力，尤其針對重要的系統。此外，機構內全體同仁亦須具備防止網路攻擊意識(Awareness)。相關措施包括：
   - 各階層同仁進行防駭資訊安全訓練。

- 建立多層級資訊系統及防火牆機制，以免單一系統受駭而直接影響到其他相關系統。至於網路應用程式介面，如桌上型電腦的電子郵件系統即具高度風險，宜與企業核心系統隔離。
- 使用防毒軟體以及網路服務分析工具，判斷網路攻擊者可能攻擊系統之脆弱點所在。
- 降低網路閘口(Gateway)數量、建立白名單軟體清單，只有經核准的軟體能安裝在電腦、定期更新修補程式、並且將核心的重要系統與其他系統隔離。
- 使用資安查核與網路滲透測試等資安事件管理(Security Information and Event Management, SIEM)工具，利用先進分析工具就模擬之攻擊情境加以演練，以確保系統符合資安標準。
- 採用 Identity and Access Management (IAM)工具，只開放有權限者才能進入系統之管控措施，並偵測及紀錄進入者之資訊，對於未經授權進入系統者應有警示措施。
- 使用 Virtual Machines 等技術軟體工具，在系統受到網路攻擊後，協助系統回復到未遭駭之前的安全狀態(Golden state 或 Golden Point)，以便有效移除被植入之惡意軟體，以免受到持續地攻擊。
- 安置加密防禦設備(Cryptographic Defenses)保護機敏資料。

2. 偵測措施

FMI 若能儘速偵測到網路攻擊及得知受攻擊範圍，則可有效加快系統復原時間。惟若僅以自家電腦系統偵測網路及系統運作是否安全仍不足夠，另應與系統使用者或參加者協力偵測異常交易，例如，交易金額、交易對手及交易時間點如出現異常，系統外部使用者一旦發現異常須儘速通報。相關電腦偵測措施如次：

- 在系統中多個環節安置安全檢查點(Check Points)偵測不當使用者。
- 使用"Kill Chain"技術軟體工具，可追蹤侵入者的動靜，進而在系

統中每個連結處設置障礙，以提高駭客直接偷取資料之難度。

3. 系統復原

網路攻擊復原(Cyber Resilience)係指受到網路攻擊後，有能力確保系統持續運作，雖然作業能力可能退化(Degraded State)，但系統尚能就優先交易項目提供服務。系統網路若採用多層級(Layer)架構，則可先恢復特定層級系統的部分功能，同時間再修復其他受攻擊之層級。在系統復原過程，FMI 須考量到當日之系統作業時間是否須延長，甚或採人工作業方式。

協助系統回復到未遭駭之前的安全狀態的技術工具非常重要，目前已有技術可將交易及持有部位資料接近即時地儲存在系統以外地方，有利於辨識未遭受攻擊前，系統內正確的交易及部位資訊。接著，FMI 須有相關配套機制，例如，與獨立第三方、系統參與者或其客戶一起協力，將安全狀態重建後之各項交易資料重新輸入系統執行作業。

值得注意的是，許多國家採用之風險管理及營運不中斷計畫係為防範實體災害攻擊，如即時自動備援系統在受到地震等實體攻擊時，透過自動備援可有效保存資料在異地系統。但若系統受到網路攻擊，已被植入惡意程式並造成交易資料不正確，反會因即時自動備援而將惡意程式及錯誤交易立即傳播至備援系統，造成主系統及備援系統均受損。

近期有相關技術推出，認為可採用非近似之備援作業系統(Non-Similar Facility, NSF)，因 NSF 採用之備援作業系統與主系統不一樣，惡意程式無法由主系統直接傳染至備援系統。但也因為 NSF 作業系統與主機不同，所需投入之人力及成本高，且大多只備援重要的核心系統，因此帶來之效益仍待評估。

鑒於 FMI 之間已廣泛地相互連結及依存，網路攻擊復原的工作不再只與單一 FMI 有關，尚包括相連結之 FMI、重要網路與系統服務提供者、FMI 參與者。因此，整合且相互合作協調之網路安全方案及訊息分享益顯重要。爰 BIS 鼓勵各國主管機關更主動協助其 FMI 解決跨產業及跨國境溝通及資訊分享問題。

三、 金融市場基礎設施準則(PFMI)

鑒於金融市場基礎設施在降低系統性風險與促進金融穩定之重要性，國際清算銀行支付暨清算系統委員會與國際證券管理組織（CPSS[5]-IOSCO）重新檢視歷年發布之「重要支付系統之核心準則」、「證券清算系統建議準則」及「集中交易對手建議準則」，增列交易資料保管機構之相關準則，並納入強化風險控管與提升市場透明度等準則，於 2012 年發布 PFMI 報告書，將 PFMI 之評估適用於系統重要性之支付系統(SIPSs)、證券結算清算系統(SSSs)、證券集中保管(CSDs)、集中交易對手(CCPs)及交易資料保管機構(TRs)。其目的係為確保 FMIs 能提供金融市場穩定及效率之服務，俾利各國在 PFMI 之適用與監管作業上，能達到一致標準。

本次研討會之 BIS 講師除了針對網路攻擊與 PFMI 相關準則之評估進行說明外，亦介紹國際間 PFMI 評估之近況。以下章節擬介紹 PFMI 架構、國際間辦理現況，並舉韓國接受世界銀行及 IMF 評估之實例，俾利我國央行辦理評估作業時參考。

(一) 架構及概述

PFMI 包括 24 項準則及主管機關 5 項職責，其中準則 1 至 3 為整體架構；準則 4 至 7 為信用及流動性風險管理；準則 8 至 10 為清算；準則 11 及 12 屬證券集中保管機構及價值交換清算系統；準則 13 及 14 為違約管理；準則 15 至 17 屬一般營業及作業風險管理；準則 18 至 20 為系統參加者加入之相關條件；準則 21 及 22 有關效率；準則 23 及 24 與透明化相關。

[5] 2014 年 9 月更名為 Committee of Payment and Market Infrastructures (CPMI)

表 2　PFMI 24 項準則

準則	準則主要內容	準則分類
1	法規基礎	整體架構
2	治理機制	
3	全面性風險管理架構	
4	信用風險	信用及流動性風險管理
5	擔保品	
6	保證金	
7	流動性風險	
8	清算最終性	清算
9	款項清算	
10	實體交割	
11	證券集中保管機構	證券集中保管機構及價值交換清算系統
12	價值交換清算系統(消除本金風險)	
13	參加者違約之處理規範與作業程序	違約管理
14	CCP 參加者客戶部位之區隔與可移轉性	
15	一般營業風險	一般營業及作業風險管理
16	保管與投資風險	
17	作業風險	
18	加入與參加標準	系統參加者加入之相關條件
19	層級化參加機制	
20	金融市場基礎設施之連結	
21	效率與效能	效率
22	通訊作業程序與標準	
23	規約、重要作業程序及市場資料之揭露	透明化
24	TR 對市場資料之揭露	

資料來源：BIS (2012), PFMI

在主管機關 5 項職責方面，包括：(A)金融市場基礎設施之管理、監理及監管；(B)管理、監理及監管之權力與資源；(C)金融市場基礎設施相關政策之揭露；(D)金融市場基礎設施準則之適用；以及(E)與其他主管機關之合作。

表 3　FMI 主管機關 5 項職責

職責	主要內容
職責 A：金融市場基礎設施之管理、監理及監管	金融市場基礎設施應接受中央銀行、市場管理者或其他相關主管機關，適當且有效之管理、監理及監管
職責 B：管理、監理及監管之權力與資源	中央銀行、市場管理者及其他相關主管機關，應具備有效執行其管理、監理及監管金融市場基礎設施職責之權力與資源
職責 C： 金融市場基礎設施相關政策之揭露	中央銀行、市場管理者及其他相關主管機關應清楚定義與揭露其管理、監理及監管金融市場基礎設施之政策
職責 D：金融市場基礎設施準則之適用	中央銀行、市場管理者及其他相關主管機關應採用國際清算銀行支付暨清算系統委員會與國際證券管理組織之金融市場基礎設施準則，並一體適用
職責 E：與其他主管機關之合作	中央銀行、市場管理者及其他相關主管機關，應視情況進行國內與國際間之相互合作，以促進金融市場基礎設施之安全與效率

資料來源：BIS (2012), PFMI

(二)　評估注意事項

PFMI 評估範圍，包括具系統重要性支付系統(Systematically Important Payment System, SIPS)以及所有之證券集中保管機構(Central

Securities Depository, CSD)、證券清算系統(Securities Settlement System, SSS)、集中交易對手(Central Counterparty, CCP)、交易資料保管機構(Trade Repository, TR)，蓋因 PFMI 認為後四類機構均為系統重要性機構，若主管機關決定不將前揭機構列入評估，則須說明理由。至於支付系統(PS)則包括系統重要性與非系統重要性，主管機關可自行決定何者為系統重要性之支付系統並納入評估範圍。

進行 PFMI 評估時，PS 多為央行的支付系統，但由於央行有其特殊之組織架構、決策程序及治理方式，爰評估準則中有關準則 2 治理(央行政策制定及架構)、準則 3 之主要考量 4 有關經營不善退場計畫(resolution planning)、以及準則 7 有關持有流動資產部分，央行無須進行評估。

BIS 公布之 PFMI 雖已廣為各國主管機關及央行遵循，惟並不具法律拘束力，亦無意干涉或限制央行之政策決定權。因此，諸如在央行開立帳戶之對象、提供融通以及合格擔保品之相關政策均不在 PFMI 探討及評估範圍。

此外，PFMI 評估時不包括設備服務機構(如 SWIFT)，因為該等國際機構已有高標準之監管措施[6]。

(三) 國際間辦理現況

BIS(CPMI)及 IOSCO 於 2012 年間共同發布 PFMI，IMF 之金融市場評估計畫(Financial Sector Assessment Program)小組及 World Bank 之資本市場小組(Capital Market Group)亦支持此項計畫，並接受會員國之申請協助進行公正之評估。整體評估流程如次：

1、會員國進行 PFMI 評估方式

(1) 國際組織派員協助評估：以韓國、新加坡及馬來西亞為例，World

[6] SWIFT 並非支付或清算系統，惟許多具系統重要性之支付系統均仰賴 SWIFT，爰 10 國集團(Group of Ten, G10)中央銀行自 1998 年起開始監管 SWIFT。SWIFT 總部位於比利時，爰以比利時央行為主要監管者，並協同 G10 其他央行成員進行監管(Oversight)。

Bank (Payment Systems Development Group)與 IMF (Financial Sector Assessment Program, FSAP)協助派員進行評估(含 24 項準則及 5 項主管機關職責)，通常評估報告會由 IMF 或 World Bank 公布於其網站。

(2) 會員國自行評估：並未向 World Bank 或 IMF 申請協助評估之國家則進行自評，但評估結果不一定對外公布。

(3) 評等結果分為已遵循、大致遵循、部分遵循、以及未遵循，如表 5 說明。

表 5　PFMI 評等結果分類

評等	內容
已遵循 (Observed)	所有被辨識出之落差及缺失，皆非關注議題，不重要且可控制，屬於 FMI 正常營運下可接受之範圍
大致遵循 (Broadly observed)	評估結果已辨識出一項或多項關注議題，FMI 應於指定期間內改善並追蹤
部分遵循 (Partly observed)	評估結果已辨識出一項或多項關注議題，若未立即改善可能變為嚴重議題。FMI 應優先處理這些關注議題。
未遵循 (Not observed)	評估結果已辨識出一項或多項關注議題，係屬情節重大，且應立即注意改善者。因此，FMI 應最優先處理這些關注議題
不適用 (Not applicable)	受評估 FMI 之類型，因特殊法規、制度、結構或其他特徵，使該項準則不適用

資料來源：BIS (2012), PFMI disclosure framework and assessment methodology

2、BIS-IOSCO 進行審視(Review)，分三階段進行

前揭各會員國之評估，其標準可能不一，為利 PFMI 的評估標準

具跨國一致性，2014 年間 BIS-IOSCO 成立工作小組(Task force)，洽詢其會員國是否願意參與其審視計畫，業經 28 個會員國及經濟體[7]回復加入該審視計畫，其中亞洲部分參與者，包括：中國大陸、香港、新加坡、日本、韓國、印尼、印度。整體的審視過程分成 3 階段(Level 1~Level 3)進行：

(1) 第 1 階段(Level 1)審視：係為確認會員國對五大受評系統(PS、CSD、SSS、CCP 及 TR)是否及時完成相關法令授權與政策修訂，俾據以要求 FMI 遵循 PFMI。

BIS 業於 2013 年首次發布第 1 階段審視報告，並於 2014 年更新，報告內容涵蓋 28 個會員國/經濟體之評等結果。其中，評等結果分為 1~4 個級距，1 表示草擬之法令或政策執行措施尚未公布，4 表示法令或政策執行措施已生效並實施，主管機關可據以要求 FMI 遵循 PFMI 相關準則，詳表 5。

表 5　第 1 階段審視結果評等分類

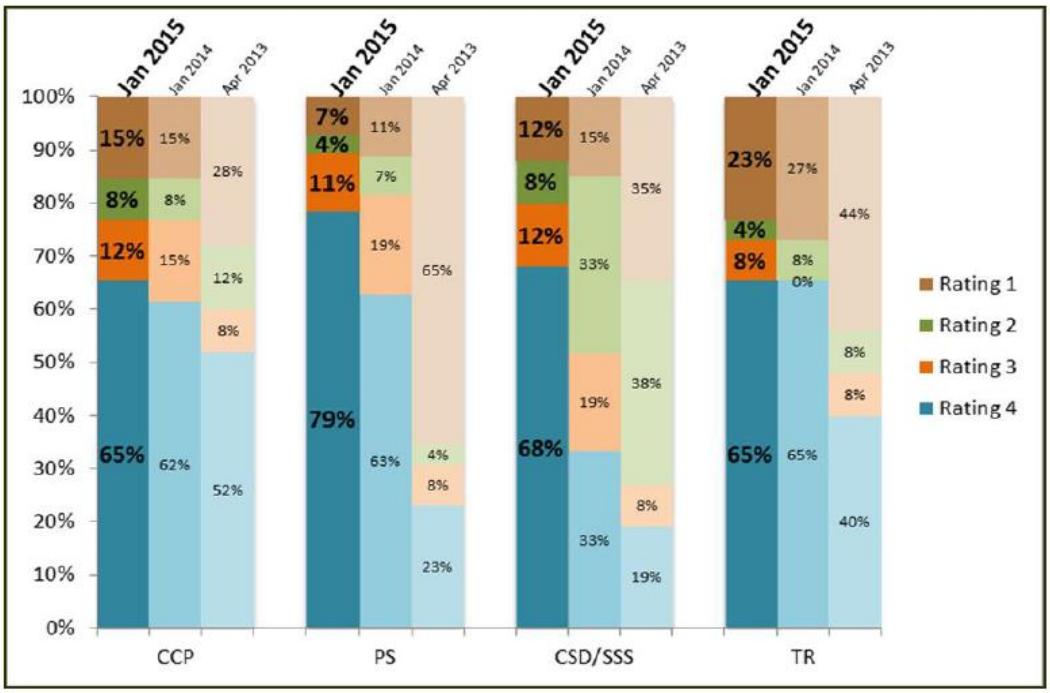
評等	內容
1	草擬之法令或政策執行措施尚未公布
2	草擬之法令或政策執行措施已公布，例如：草案已進入公告階段或考慮要修訂/新增法令
3	法令或政策執行措施已公布實施日期，但尚未生效
4	法令或政策執行措施已生效並實施。主管機關可據以要求 FMI 遵循 PFMI 相關準則
N.A	不適用(N.A)

資料來源：CPSS and Board of IOSCO (2014), “Implementation monitoring of PFMIs: First update to Level 1 assessment report”

[7] 參與之28個會員國及經濟體包括：阿根廷、澳洲、比利時、巴西、加拿大、智利、中國、歐元區、法國、德國、香港、印尼、印度、意大利、日本、韓國、墨西哥、紐西蘭、俄羅斯、沙烏地阿拉伯、新加坡、南非、西班牙、瑞典、瑞士、土耳其、英國及美國。

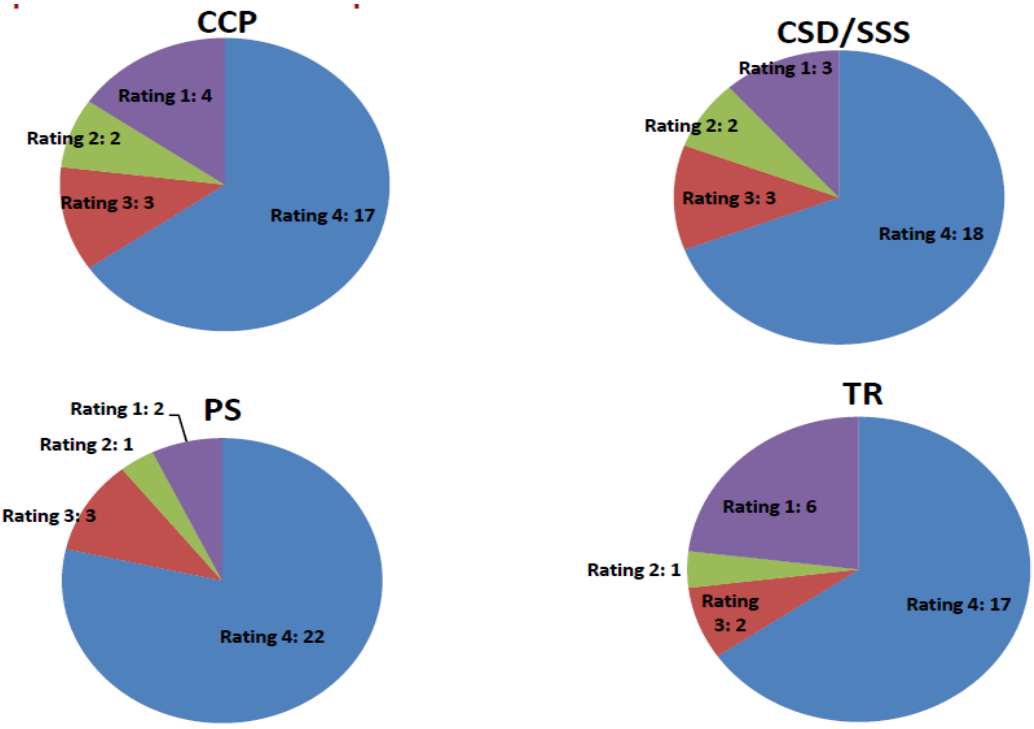
BIS 講師於研討會提供之資料顯示(詳圖 2 及圖 3)，以支付系統(PS)為例，截至 2015 年 1 月底，28 個經濟體/國家中，有 22 個評等為″4″ (比例達 79%)，3 個評等為″3″(比例達 11%)，合計評級″4″與″3″之比例高達 90%。整體而言，PS 在配合執行 PFMI 之法令修訂完備度較 CCP、CSD/SSS 與 TR 更高。

圖 2　第 1 階段各類評等結果-比例



資料來源：SEACEN 研討會資料

圖 3　第 1 階段各類評等結果-數量



資料來源：SEACEN 研討會資料

(2) 第 2 階段(Level 2)審視：評估會員國法令架構及政策內容是否與 PFMI 一致。BIS 已於 2015 年 2 月公布美國、日本及歐元區對集中交易對手(CCP)及資料保管機構(TR)之審視報告。預計第 2 波會針對澳洲、香港及新加坡進行審視並公布結果報告。

第 2 階段之評等級距包括：一致、大致一致、部分一致與不一致，詳細內容參見表 6。

表 6　第 2 階段審視結果分評等分類

評等	內容
一致 (Consistent)	法令架構與 PFMI 準則一致，評估結果認為無落差或僅有少數不具實質影響的小落差存在
大致一致	法令架構與 PFMI 準則大致一致，評估結果

(Broadly Consistent)	認為僅有少數些微影響的落差存在
部分一致 (Partly Consistent)	法令架構與 PFMI 準則部分一致，評估結果認為有明顯影響一致性的落差存在
不一致 (Not Consistent)	法令架構與 PFMI 準則不一致，評估結果認為有重大影響一致性的落差存在
不適用 (Not Applicable)	該項準則不適用

資料來源：CPMI (2015), "Implementation monitoring of PFMIs: Level 2 assessment report for central counterparties and trade repositories-United States"

(3) 第 3 階段(Level 3)審視：係為評估不同國家/經濟體間之會員實施 PFMI 之結果是否具一致性，目前尚無相關報告公布。BIS 預計 2015 年底方啟動此部分審視，且以主題方式(Theme Based Approach)進行評估，例如針對 PFMI 準則中，涉及信用風險、流動性風險、以及壓力測試模型等主題進行跨國/跨經濟體之一致性評估。

(四) 韓國央行支付系統(BoK Wire+)之評估案例

韓國BoK Wire+以及韓國證券交易所(KRX)，係由IMF與World Bank於2013年7月間協助進行PFMI評估，並由IMF於2014年10月發布評估報告。謹就BoK Wire+評估報告中涉及PFMI評估之法規架構、系統特色及主要評估結果說明如次：

1. 法規架構

(1) 韓國央行法

涉及支付清算之主要規定在第 81 條，其中揭露央行維持支付清算系統之安全及效率應採行之措施，說明如次：

a. 為維持支付清算系統之安全及效率，BoK 得決定其營運系統

須採行之措施。

b. 對於非 BoK 營運之支付清算系統，BoK 必要時得要求該營運者或其主管機關採行必要措施，例如要求改善作業相關法規等。

c. 為利整體支付清算系統之順暢運作，BoK 得要求支付清算營運機構提供支付清算相關之資料，且渠等機構應予遵循。

d. BoK 得要求其支付系統之參加機構提供相關資料。

(2) BoK 訂定之「支付清算系統營運及管理辦法」(簡稱本辦法)

BoK 依據韓國央行法訂定本辦法(Regulation on the Operation and Management of the Payment and Settlement Systems, ROMPSS)，並於 2012 年間配合 PFMI 之發布進行修訂，期以更符合國際準則慣例之要求。

本辦法揭露清算最終性及不可撤銷性；另外，亦規定 BoK 對支付清算系統之監管措施及範圍，並界定具系統重要性支付清算系統，說明如次：

a. 第 7 條(僅間接提及清算最終性)，規定支付清算系統營運機構如欲申請與 Bok Wire+連結執行最終清算，BoK 應評估該機構在支付清算方面之安全性及效率性。

b. 第 10 條第 3 項(支付指令不可撤銷及其例外)，規定 BoK Wire+參加人或與其連結之支付清算系統，在送出支付指令且 BoK 亦已收到後，該指令不得撤銷；惟該指令若處於佇列(帳戶資金不足支付)狀態，則可撤銷。

c. 第 33 條有關 BoK 之監管職責，包括以下 5 款：

(a) BoK 得界定何種支付清算系統須被其監管(Oversight)

(b) 蒐集並分析與支付相關之資訊

(c) 評估 BoK 監管之支付清算系統的安全及效率性

(d) 就 BoK 監管之支付清算系統要求進行改善

(e) 其他緊急之措施

d. 第 35 條第 2 項定義具系統重要性支付清算系統(Systemically Important Payment and Settlement System, SIPSs)，包括 BoK Wire+以及下列經 BoK Wire+進行款項清算之系統：

(a) 由韓國金融通訊及清算機構(Korea Financial Telecommunications and Clearings Institute)營運之支票清算系統、銀行間匯款系統，以及電子銀行系統

(b) 韓國集保公司(Korea Securities Depository)營運之機構投資者債券清算系統(Institutional Settlement System of Bonds)

(c) 韓國證交所及集保公司營運之 KOSPI 及 KOSDAQ 市場清算系統

(d) 韓國交易所之衍生性商品市場清算系統

(e) 持續連結清算(Continuous Linked Settlement, CLS)銀行營運之清算系統

e. 第 37 條(納入 PFMI)，BoK 應採用 PFMI 作為評估標準，就支付清算系統進行安全及效率性之評估

(3) IMF 與 World Bank 對 BoK Wire+在法規架構面之評估建議

a. 參酌前揭韓國相關法令，可知其央行法第 81 條提及央行應維持支付清算系統之安全及效率性之職責；

b. 至於清算最終性及不可撤銷性則揭露在「支付清算系統營運及管理辦法」第 7 條及第 10 條第 3 項，值得注意的是，有關清算最終性在法規上的呈現，僅隱約提及尚欠明確。

c. 爰 IMF 及 World Bank 之評估報告[8]認為，可再將清算最終性

[8] 原報告第 19 頁第 28 段

的文字更明確地揭露在相關規定內。

2. BoK Wire+重要特色

(1) BoK Wire+自 2005 年起規劃更新其 RTGS 作業系統，並於 2009 年正式上線，採混合式(Hybrid) RTGS 作業，另增加雙邊及多邊互抵之清算機制，以節省參加者之日間流動性。

(2) 銀行、保險公司、證券交易商、中介商、政府代理機構、CLS 銀行等，可在 BoK Wire+開立帳戶。

(3) 參加者在 BoK Wire+須開立兩種帳戶，分別為交易帳戶(Current account)及清算用存款帳戶(Deposit account for settlement)，交易帳戶透過 RTGS 系統，清算有關 BoK 貸款、政府債券交易、CLS 與零售交易之款項；至於存款帳戶則透過混合(Hybrid)系統，清算一般資金移轉、銀行間短期拆借，以及證券交易端之款項。

表 7　韓國 BoK Wire+混合式 RTGS 帳戶

清算系統(帳戶)	處理之交易	清算機制
RTGS (Current account)	CLS 資金撥轉 ● 指定時點淨額清算(DNS) ● 政府債券發行及償還 ● BoK 貸款 ● 系統參與者下午 5:30 後償還日間透支款項	RTGS
Hybrid (Deposit account for settlement)	● 一般資金移轉(含第三方資金移轉) ● 銀行間短期拆借 ● 證券交易款項端清算(含 BoK 附買回交易)	RTGS，雙邊及多邊互抵機制

資料來源：IMF (2014), “Republic of Korea Financial Sector Assessment

Program”

(4) BoK 提供日間透支及日間 Repo 交易之融通機制，降低參加者流動性需求。

(5) 參與者資金不足之排序等候機制：RTGS 對支付指令採先到先處理(First in, first out)原則；在混合系統中，參加者可變更其支付指令之優先順序。

(6) BoK 的擔保品管理系統連結至韓國證券集保公司(KSD)，公債由 KSD 保管，BoK 在接受高品質債券作為融通之擔保品時，會就擔保品進行市價評估並採用折價率(Hair cut)。

(7) BoK Wire+在不同時段已採取差異化收費方式，可有效使清算作業在不同時間點順暢進行。然而，在下午 4 點以後時段，因韓國證交所(KRX)、銀行拆借及 Repo 款項清算指令陸續進入 BoK Wire+，仍造成清算作業過度集中在該段時間。

3. PFMI評估結果

BoK Wire+受評結果，準則5為大致遵循、準則23為部分遵循外(詳表8)，其餘皆為已遵循。

表8　BoK Wire+評等結果彙總表

評等等級	準則
已遵循	1,2,3,4,7,8,9,12,13,15,16,17,18,19,21,22
大致遵循	5
部分遵循	23
未遵循	
不適用	6,10,11,14,20及24

資料來源：IMF (2014), “Republic of Korea Financial Sector Assessment Program”

4. 謹分別就對大致遵循之準則5，以及部分遵循之準則23，說明其詳細評估如次：

(1) 遵循準則之詳細評估-準則5

遵循準則之詳細評估

準則 5：擔保品

金融市場基礎設施為管理本身及其參加者的信用曝險所接受之擔保品，應具備較低之信用風險、流動性風險及市場風險。金融市場基礎設施亦應妥適訂定及採行保守的擔保品折價率與集中度限制

主要考量 1： FMI（例行地）接受作為擔保品之資產，一般應僅限於具備低信用風險、流動性風險及市場風險者	● 在十足擔保基礎下，BoK 提供日間流動性融通予 BoK Wire+參加者 ● BoK 接受銀行與非銀行參加者提供之政府債券(KTB)以及 BoK 發行之金融穩定債券(MSB)作為擔保品 ● BoK 特殊情況下可依據韓國央行法第 65 條規定，提供緊急融通予銀行，銀行提供之任何資產均可暫時充作擔保品；惟此情況實際上未發生過 ● 錯向(Wrong-way)風險[9]不存在，因為 BoK 只接受 KTB 及 MSB 等高品質債券作為擔保品
主要考量 2： FMI 應建立審慎的評價實務，並訂定一套經常被檢測，且考量市場遭受壓力情況時之擔保品折價率	● BoK 每日營業開始進行擔保品評價，並依據到期日之長短決定其折價率如下表所示 期限 | 低於 1 年 | 低於 3 年 | 低於 5 年 | 超過 5 年 比率(%) | 98 (98) | 97 (96) | 96 (95) | 95 (94) 債券價格波動率(%) | 1.60 | 1.71 | 1.68 | 2.02 註：1. 括弧數字為零息債券

[9] 係指對交易對手之信用曝險因為交易對手之信用品質惡化，導致曝險金額提高之反向變動關係。

	2. 計算自 2007 年 9 月至 2008 年 9 月之債券指數標準差 ● 折價率之決定係依據 Regulation on BoK's Loan (ROBL)第 1~3 點及 Regulation on Operation and Management of Payment and Settlement Systems(ROMPSS)第 58 之 5 點辦理 ● 折價率每 6 個月決定一次，但缺乏折價率之壓力測試、擔保品充裕性以及順景氣循環分析等細節
主要考量 3： FMI 應在實務可行及審慎的原則下，建立穩定與保守的擔保品折價率，且經檢驗涵蓋市場遭受壓力期間，以降低順景氣循環調整的需要	● BoK 依據所持債券所涉風險及市場壓力情況(順景氣循環調整的需要)，每 6 個月設定一次折價率。考量市場情況變動，必要時可增加折價率調整之頻率
主要考量 4： FMI 應避免集中持有特定資產，因集中持有將嚴重損及快速變現資產的能力，且會產生嚴重負面價格效果	● BoK 並未對其持有之特定資產有風險集中度之限制，蓋因 BoK 持有之擔保品均為高品質債券且可快速變現，尚不致於受到嚴重的價格減損，爰無須對所持之擔保品設定風險集中度
主要考量 5： FMI 如接受跨境擔保	● 不適用，BoK 不接受跨境擔保品

品，應降低動用該等擔保品之相關風險，並確保可及時動用	
主要考量 6： FMI 應採用經妥善設計，且具備營運彈性之擔保品管理系統	● 擔保品管理系統設計 BoK 使用韓國集保公司(KSD)之 Safe+系統進行擔保品管理。KSD 之 Safe+包括韓國政府債券之保管，並與 BoK Wire+相互連結，俾利 BoK 提供日間融通予銀行及非銀行參加者。Safe+系統亦提供 BoK 得以處分其持有擔保品之功能 ● 營運彈性 Safe+系統於 2011 年取代原有之 Safe 系統，它提供更快速、先進的處理效能，並改善使用者介面
準則 5 主要結論	● BoK Wire+的合格有價證券擔保品，僅限於低信用風險、流動性風險及市場風險之債券，且對擔保品市價評估及折價。擔保品系統與 BoK Wire+連結，且折價率係依據 WROMPSS 及 WROBL 辦理，每 6 個月決定一次折價率。 ● 尚無折價率之壓力測試、擔保品充裕性以及順景氣循環分析之細節；此外，對於市價評估及折價率之決定及計算過程，未每年進行獨立的有效性驗證評估
準則 5 之評估	● 大致遵循

建議與評論	● 有必要對折價率之檢視頻率增加，其中包括對評價及折價率計算方法每年進行有效性驗證評估，以便於在市況不利時，BoK 仍可得到充分的保護

資料來源：IMF (2014), “Republic of Korea Financial Sector Assessment Program”

(2) 遵循準則之詳細評估-準則23

遵循準則之詳細評估

準則 23：規約、重要作業程序及市場資料之揭露

金融市場基礎設施應有清楚與周延的規約及作業程序，並應提供充分資訊，使參加者正確瞭解參加金融市場基礎設施所遭受的風險、費用及其他重要成本。所有相關的規約與重要作業程序，均應公開揭露。

主要考量 1： FMI 應採用清楚與周延的規約及作業程序，並對參加者充分揭露。相關規約與重要作業程序也應公開揭露	● 規約及作業程序 ROMPSS 及其子規定明訂 BoK Wire+架構、運作方式及作業程序 ● 揭露 相關公布之規定中已明訂緊急狀況下應採之必要措施，例如 BoK Wire+營運時間延長、參加單位應採程序與營運不中斷計畫
主要考量 2： FMI 應揭露系統設計及作業之詳細說明，以及 FMI 與其參加者的權利及義	● 參加單位的權利、義務及風險管理程序均規定在 ROMPSS 及其子規定中。此外，BoK Wire+的系統設計架構亦揭露在提供給各參加單位之操作手冊及使用說明中

務，使參加者可以評估其因參加 FMI 所遭受的風險	
主要考量 3： FMI 應提供所有必要及適當的文件與訓練，俾有助於參加者瞭解其規約與作業程序，以及因參加 FMI 所面臨的風險	● 為利參加單位瞭解 BoK Wire+，BoK 提供參加單位相關規定、操作手冊及使用說明，並在例行性的會議場合提供說明。此外，BoK 亦會在非例行性的參加單位諮詢委員會中，提供相關資訊；如有更重要之資訊，例如重建 BoK Wire+系統，則會對所有參加單位召開說明會
主要考量 4： FMI 應公開揭露其提供個別服務的收費水準，以及任何可利用之折扣政策。FMI 對於計費的服務，應提供清楚之說明，以供參加者比較	● 依據相關規定及重大政策變動前之預告規範，為確保收費制度之透明化，BoK 在設定 BoK Wire+之收費水準前，須廣徵意見，並且與參加單位諮詢委員會討論擬收取之費用 ● 在設定收費水準前，BoK 應就收費水準、架構對參加單位進行調查，並召開說明會向參加單位收集廣泛意見。BoK 設定收費水準時應考量調查及說明會之結論
主要考量 5： 金融市場基礎設施應定期完成，並公開揭露其對 CPSS-IOSCO FMI 揭露架構的回應。FMI 至少也應揭露交	● 有關對 CPSS-IOSCO 揭露架構的回應方面，相關規定及程序均個別揭露在 BoK 網站，對 Bok Wire+之評估亦包括在「支付清算系統年報」，且對外公布 ● BoK 計畫採用 CPSS-IOSCO 於 2012 年 12 月發布之揭露架構 ● 有關 BoK Wire+相關統計，包括月交易金

易筆數及交易金額等基本資料	額及數量等，均揭露在 BoK 網站；此外，「支付清算系統年報」亦包括 BoK Wire+ 相關統計數據之分析
準則 23 主要結論	● 為利參加單位瞭解 BoK Wire+，BoK 於其網站揭露 ROMPSS 及其子規定，並提供參加單位操作手冊及使用說明 ● BoK 計畫採用 CPSS-IOSCO 於 2012 年 12 月發布之揭露架構
準則 23 之評估	● 部分遵循
建議與評論	● 為利相關人士及參加單位瞭解 BoK Wire+，BoK 計畫採用 CPSS-IOSCO 於 2012 年 12 月發布之揭露架構 ● BoK 就其公布之資訊，除以韓文揭露外，亦應以金融市場慣用之語言(英文)揭露

資料來源：IMF (2014), “Republic of Korea Financial Sector Assessment Program”

5. 對BoK Wire+之建議

在建議處理事項優先順序表方面，係就各項評估準則之結果有落差或須改進者，進行彙整、摘陳並提出建議如下表：

對BoK Wire+之建議處理事項優先順序表

準則	關注議題與落差	建議行動	處理時程及優先順序
5	擔保品折價率每半年決定一次，有關折價率充足性測試與	擔保品折價率之檢視頻率應提高，以因應市場情勢之變化。另亦無	短期、中等優先順序

	壓力測試，尚不完備	折價率壓力測試、擔保品充裕性以及順景氣循環分析之細節	
7	參加人的支付指令若在佇列排序中，可以取消或撤銷；但只有在事前取得資金收取方之同意時，方能取消或撤銷	宜修訂相關規定，以實際反映在何種情況下，支付指令可以取消或撤銷	中期、中等優先順序
7	結算過度集中在接近BoK Wire+關帳前之時段	BoK已考量進行差別取價之衝擊分析，俾更深入瞭解支付流量分佈，以避免支付指令過度集中在特定時段	短期、 中等優先順序
8	BoK Wire+具清算最終性之陳述，在相關規定之陳述仍不明顯	建議修訂「ROMPSS」規定，明確加入最終性及不可撤銷性之文字	中期、 中等優先順序
3, 17	BoK Wire+的營運不中斷計畫(BCP)，包括12種情境因應措施，針對KRX、KSD及零售支付清算系統(KFTC)，無法個別(system-by-system)運作時，分析可能對BoK Wire+的影響	建議再增加同時有一個以上之系統無法運作之情境分析，俾更完整	短期、 高優先順序

23	為利相關人員瞭解，BoK將依據CPSS-IOSCO於2012年底期間發布之揭露架構報告對外公布	宜採用CPSS-IOSCO發布之揭露架構，並對外公布	短期、中等優先順序
23	除揭露韓文資訊外，BoK應將相關資訊以金融市場常用之語言揭露	所有資訊除以韓文揭露外，亦應以英文揭露於BoK網站	短期、中等優先順序

資料來源：IMF (2014), “Republic of Korea Financial Sector Assessment Program”

(五) 我國央行辦理評估之規劃

為促進國內支付系統之健全發展，我國央行擬依據BIS「金融市場基礎設施準則（PFMI）」辦理國內重要支付系統之評估作業，經訂定評估執行計畫及時程如次：

1. 評估範圍：

(1) 央行營運系統：業務局同資系統及國庫局中央登錄債券系統。

(2) 央行主管系統：包括財金公司之跨行通匯、ATM 及外幣結算系統，以及票交所之票據交換結算系統。

2. 成立央行評估小組：

由本局邀集外匯局、國庫局、金檢處、資訊處及法務室組成評估小組，小組成員任務分配如次：

(1) 業務局：

a. 辦理央行同資系統之自評及審查。

b. 審查財金公司跨行通匯系統與ATM系統自評報告。

c. 審查票交所票據交換結算系統自評報告。

(2) 國庫局：辦理央行中央登錄債券系統之自評及審查。

(3) 外匯局：審查財金公司外幣結算系統自評報告。

(4) 金檢處：針對各單位自評報告提供審查意見。

(5) 資訊處：針對各單位自評報告提供審查意見。

(6) 法務室：針對各單位自評報告提供審查意見。

3. 評估步驟：

本次先就國內重要支付及清算系統遵循PFMI 24項準則情形進行評估，評估步驟如下：

(1) 先由自評單位依據 PFMI 揭露架構及評估方法辦理自評，並撰寫自評報告送央行審查。

(2) 再由央行「評估小組」就自評報告內容進行審查，對於未能符合準則要求者，提出建議改善措施，並督促自評單位落實執行。

4. 推動時程：

(1) 2015 年 6 月初邀集相關單位召開說明會並交付本局所翻譯之 PFMI 評估問項予自評單位。

(2) 預計2015年9月底業務局同資系統、國庫局中央登錄債券系統、財金公司(跨行通匯、ATM 與外幣結算系統)及票據交換結算系統完成自評，並將自評報告送交央行。

(3) 央行評估小組進行審查，必要時函請自評單位進行修改，並於 2015 年下半年「促進支付系統健全運作座談會」(預計 12 月)討論前揭審查結果。

參、心得與建議

一、心得

(一)網路攻擊者可分為四大類，各有其不同動機

1、駭客(Hacktivists)：侵入系統影響運作，純為滿足其成就感。

2、網路犯罪者(Cyber criminals)：動機為獲取財務利益。

3、網路恐怖分子(Terrorists)：意圖造成政治及金融不穩定。

4、國家網路間諜(Nation state-related actors)：試圖竊取他國機敏資料。

(二)BIS 建議 FMI 對於網路攻擊應採整合性之復原方案

BIS 於 2014 年底發表因應網路攻擊報告，建議 FMI 應採行包含以下 3 個面向之整合性復原方案：

1、**辨識系統受損範圍**：須有相關技術及措施能辨識系統受到攻擊的範圍。

2、**網路治理**：建立因應網路攻擊之治理方式，包括人員訓練、強化電腦防禦技術、建立處理程序，以及訊息通報等措施。

3、 **採取一系統因應措施-包含預防、偵測及復原措施**

(1) 預防措施(Prevention)：FMI 的系統必須具備偵測網路入侵之能力，尤其針對重要的系統。

(2) 偵測措施(Detection)：FMI 若能儘速偵測到網路攻擊及得知受攻擊範圍，則可有效加快系統復原時間；另應與系統參加者協力偵測異常交易，一旦系統參加者發現異常情況，須儘速通報。

(3) 系統復原(Resilience)：系統網路若採用多層級架構，則可先

恢復特定層級系統的部分功能，同時間再修復其他受攻擊之層級。

(三)善用先進技術降低網路攻擊造成之傷害

目前已有技術可將交易及持有部位資料接近即時地儲存在系統以外地方，有利於辨識未遭受網路攻擊前之正確交易及部位資訊。FMI 接著須有相關配套機制，例如，在系統回復到未遭駭之前的安全狀態後，與系統參加者一起將遭受網路攻擊後之各項交易資料重新輸入系統，以完成清算作業。

(四)網路攻擊防禦科技雖持續演進，但仍有其限制

傳統的即時備援系統，在受到地震等實體攻擊時，透過自動備援機制可有效保存資料在異地備援系統；惟若受網路攻擊時，主系統已被植入惡意程式造成交易資料不正確，透過即時備援，反會將惡意程式及錯誤交易立即傳到備援系統，使二個系統均受損。

近期有專家提出非近似之備援作業系統(Non-Similar Facility, NSF)，因 NSF 採用之備援作業系統環境與主系統不一樣，惡意程式無法由主系統傳染到備援系統；但也因 NSF 備援作業系統與主系統不同，新增之人力及投資成本甚高，成本與效益之取捨仍待進一步評估。

(五)不能因網路攻擊而破壞央行清算最終性之原則

央行 RTGS 款項一旦經過清算後即具最終性而不可撤銷，BIS 工作小組認為，即使因網路攻擊事件導致款項錯誤移轉亦不可撤銷，而應再重新輸入另一個反向且金額相同的交易指令，抵銷先前因網路攻擊而未經正當授權之交易指令，俾維持金融交易之穩定。

二、 建議

(一)PFMI 評估應納入網路攻擊因素，並宜公布精簡版評估結果

1、 鑒於網路攻擊之潛在威脅增加，本次 PFMI 各自評單位(含票交所及財金公司)，宜將網路攻擊部分納入評估。

2、 PFMI 揭露架構要求自評單位應揭露精簡版之評估資訊,鑒於該等資訊尚不涉及受評單位是否遵循各準則之細節，爰自評單位似宜對外揭露。

(二)央行同資系統營運不中斷作業亦宜納入網路攻擊因素

為利同資系統營運中斷後之復原運作，儘速將前述離線交易補登至系統，央行業務局已規劃透過適當介面，將人工登帳交易資料整批上載至系統並執行入檔，以節省後續正常作業之銜接處理時間。

惟考量網路攻擊及威脅逐漸升高，同資系統營運不中斷作業部分，除考量傳統實體災害造成之因素外，亦宜納入網路攻擊因素。

(三)建請國內重要結算機構參考 BIS(2014)「金融市場基礎設施網路攻擊復原」報告，俾強化因應能力

近年網路攻擊威脅逐漸增加，以韓國為例，2013 年間數家金融機構遭受網路攻擊,導致銀行資訊系統失靈並洩漏數位認證等相關資訊,且自動提款機及銀行間連線系統亦中斷近 2 小時。

BIS 於 2014 年底發布「金融市場基礎設施網路攻擊復原」報告，提出相關建議，包括對網路攻擊之偵測技術、復原措施，以及備援機制(例如 NSF)等,國內重要支付系統營運者(例如財金公司及票交所)似可參考該報告建議，強化對網路攻擊之因應能力。

附錄 1 ENISA 統計之網路攻擊趨勢

Top Threats	Current Trends	Top 10 Threat Trends in Emerging Areas						
		Cyber-Physical Systems and CIP	Mobile Computing	Cloud Compu-ting	Trust Infrastr.	Big Data	Internet of Things	Netw. Virtuali-sation
1. Malicious code: Worms/Trojans	↑	↑	↑	↑	↑		↑	↑
2. Web-based attacks	↑	↑	↑	↑	→		↑	
3. Web application attacks /Injection attacks	↑	↑	↑	↑	↑		↑	↑
4. Botnets	↓		↑	↑				
5. Denial of service	↑	↑		→	→		↑	↑
6. Spam	↓	↑						
7. Phishing	↑		↑		↑	↑	↑	↑
8. Exploit kits	↓		↑		↑		↑	
9. Data breaches	↑			↑		↑		↑
10. Physical damage/theft /loss	↑	↑	↑		↑	↑	↑	↑
11. Insider threat	→	↑		↑		↑	↑	↑
12. Information leakage	↑	↑	↑	↑	↑	↑	↑	↑
13. Identity theft/fraud	↑	↑	↑	↑	↑	↑	↑	↑
14. Cyber espionage	↑	↑		↑	↑	↑		↑
15. Ransomware/ Rogueware/ Scareware	↓		↑					

Legend: Trends: ↓ Declining, → Stable, ↑ Increasing

附錄 2 重要之網路攻擊型態

網路攻擊名稱	內容
Botnet (傀儡網路)	傀儡網路另一個說法是殭屍網路或機器人網路，當受害電腦一旦被植入可遠端操控該電腦的惡意程式，即會像傀儡(或機器人)一般任人擺佈執行各種惡意行為，當一部電腦成為 Botnet 的一部分時，意味著 Bot 操縱者可將募集到的龐大網路軍團當作機器人來遠端遙控，從事各種非法入侵，竊取資料。瀏覽網頁者易在無法察覺的情況下，連線到殭屍網路背景植入間諜軟體等載惡意程式，並成為殭屍網路的一員，繼續壯大殭屍網路軍團
Social Engineering (社交工程)	社交工程惡意程式專門假冒其他軟體或隱藏在其他軟體之內，引誘使用者下載並安裝該軟體，藉此趁機安裝惡意軟體，進而導致機密資訊遭盜用竊取、損毀或外流
malicious code (惡意程式碼)	如病毒、病蟲、邏輯炸彈和特洛伊木馬之類的程式，它們會暗中插入程式來破壞資料、執行破壞性或介入式程式，或者以其他方式危害受害者電腦資料的安全性或完整性
denial-of-service attack (癱瘓服務攻擊)	假借向網站詢求資訊服務之名，傾入大量偽假的詢求資訊，使網站伺服器因疲於處理大舉進站的資訊量而當機，從而阻斷其他使用者接受網站服務管道的行徑。它有別於駭客入侵，因未闖入網站電腦安全系統，但卻可使網站功能癱瘓
Advanced Persistent Threat (進階持續性滲透攻擊)	進階持續性滲透攻擊通常包括以下幾個步驟進行持續性且常時間的攻擊： • 【鎖定特定目標】針對特定政府或企業，長期間進行有計劃性、組織性竊取情資行為，可能持續

	幾天，幾週，幾個月，甚至更長的時間 • 【假冒信件】針對被鎖定對象寄送幾可亂真的社交工程惡意郵件，如冒充長官的來信，取得在電腦植入惡意程式的第一個機會 • 【低調且緩慢】為了進行長期潛伏，惡意程式入侵後，具有自我隱藏能力避免被偵測，伺機竊取管理者帳號、密碼 • 【客製化惡意元件】攻擊者除了使用現成的惡意程式外亦使用客製化的惡意元件 • 【安裝遠端控制工具】攻擊者建立一個類似殭屍網路/傀儡網路 Botnet 的遠端控制架構攻擊者會定期傳送有潛在價值文件的副本給命令和控制伺服器審查。 • 【傳送情資】將過濾後的敏感機密資料，利用加密方式外傳

附錄 3 近年金融業受到之重要網路攻擊案例

案例 1：

美國 Nasdaq 於 2010 年間發現電腦系統遭駭並植入惡意軟體，該惡意程式監控並搜集上櫃公司董事會之機密文件及董事會紀錄，在 2010 年被發現前，Nasdaq 無法得知該程式已被植入多久時間。

案例 2：

芝加哥商品交易所(CME)於 2013 年 11 月間發布，其負責處理 OTC 能源及金屬交易合約之CME ClearPort 平台於該年7月間遭網路攻擊，有2,000多家使用該平台之公司，共計約 7,000 多組密碼被駭。

案例 3：

韓國數家金融機構在 2013 年間遭受網路攻擊，導致銀行 IT 系統失靈並洩漏數位認證等相關資訊，近 32,000 部電腦停止運作，自動提款機及銀行間之連線作業系統亦中斷近 2 小時。

案例 4：

Operation High Roller 屬創新金融詐騙技術，在 2012 年成功攻擊位在歐洲、美國及拉丁美洲金融業，目標鎖定在信用合作社、全球及區域型銀行之大金額商業存款戶、高資產個人帳戶，估計自銀行帳戶偷偷轉走約 7,800 萬至 25 億美元。

案例 5：

Red October Cyber Attack 在 2013 年間，成功地自全球許多大使館、核能研究中心及石油公司等單位偷走加密過之機密資訊，甚至包括電腦已刪除之資料

案例 6：

JPMorgan Chase 於 2014 間遭網路攻擊，並造成 8,300 萬名客戶之姓名、地址、電話及郵件信箱被竊。系統被駭受損(Compromised)主因該公司某部分電腦網路系統僅採用單層安全驗證系統(其他金融機構多採雙層驗證機制)。

參考資料

一、 中文部分

1. 中央銀行業務局編譯(民國 104 年)，「金融市場基礎設施準則」
2. 中央銀行業務局編譯(民國 104 年)，「金融市場基礎設施準則之揭露架構及評估方法(Principles for financial market infrastructures: Disclosure framework and Assessment methodology)」
3. 黃昱程(民國 103 年) ，「BIS 支付與市場基礎設施委員會舉辦之 CPMI 準則及其實施，以及零售支付發展」出國報告
4. 張國興(民國 103 年)，「遵循金融市場基礎設施準則以增進金融穩定與有效監管：評鑑方法及交易資訊揭露」出國報告
5. 陳啟超(民國 104 年)，「參加 SEACEN 舉辦之「第 2 屆支付及清算系統監管」訓練課程出國報告」出國報告

二、 英文部分

1. BIS (2014), Committee on Payments and Market Infrastructures, “Cyber resilience in financial market infrastructures”
2. BIS (2012), “Principles for financial market infrastructures”
3. Bank of Korea (2012), “Bank of Korea Act”
4. Bank of Korea (2012), Monetary Policy Committee, “Regulation on the Operation and Management of the Payment and Settlement System”
5. CPMI (2015), “Implementation monitoring of PFMIs: Level 2 assessment report for central counterparties and trade repositories-United States”
6. CPSS and Board of IOSCO (2014), “Implementation monitoring of PFMIs: First update to Level 1 assessment report”
7. CPSS and Board of IOSCO (2012), “Principles for financial market infrastructures: Disclosure framework and Assessment methodology”

8. IMF (2014), “Republic of Korea Financial Sector Assessment Program-Detailed Assessment of Compliance of the CPSS-IOSCO Principles for Financial Market Infrastructures-BoK Wire+ and KRX CCP”
9. IMF (2013), “Detailed Assessment of Observance-Assessment of Observance of the CPSS-IOSCO principles for financial market infrastructures”
10. National Institute of Standards and Technology (2014) “Framework for Improving Critical Infrastructure Cybersecurity”
11. SEACEN(2015), Seminar materials: “Resilience of Payment System to Cyber Crime”, 14th SEACEN Advanced Course on Payment and Settlement Systems for Emerging Economies