

證券商資安查核 重點暨案例分享

一、資安查核與輔導

二、資安查核重點

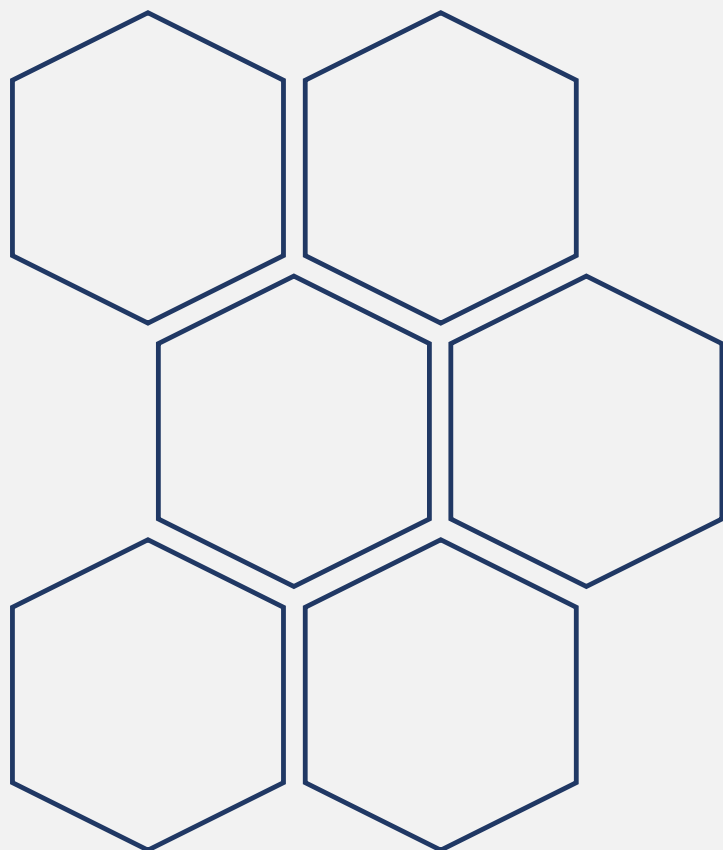
三、常見缺失說明

四、案例說明

五、未來展望



TAIWAN
STOCK EXCHANGE



資安查核與 輔導



TAIWAN
STOCK EXCHANGE

資安查核與輔導

資安法等六子法

強化資安

金融資安
行動方案
/資本市場藍圖

證券期貨業者
分級及其資安
防護標準

協助制定

新興科技管控參考指引

資通系統安全防护基準參考指引

供應鏈風險管理參考指引

網路安全防护基準參考指引

資訊作業韌性參考指引

日誌留存參考指引

資安事件應變處理參考指引

協助公會訂定
自律規範及參
考

內部控制制度標準規範
CC-10000~CC-22000

建立證券商資通安全檢查
機制

修訂法規並輔導業者

分級防護應辦事項

已於109年修訂至內控及建
立證券商資通安全檢查機制
(110、111、112三年實施)

查核

檢視法規遵循情形，
確保資安防護量能。

輔導

研議實務可行性規
範，協助業者落實
法規要求。

聯防

資安事件情資流通，
強化資安聯防。

中時新聞網

金管會領證券F4 打造韌性市場

陳柔蒨

2022年8月30日 週二 下午7:03



iThome 新聞 產品&技術 專題 AI Cloud DevOps 資安 研討會 社群 IT EX

AWS助您洞察未來資安核心價值 臺灣資安大會 高效資安術公開 全新系列【數位轉型】

編者的話

資安韌性已成企業組織永續發展的關鍵

無論我們防禦得多麼成功，都無法保證明天不會淪陷，因此，我們必須更重視企業組織永續發展的致勝關鍵：資安韌性，唯有韌性，得以決勝

文/ 李宗翰 | 2020-08-21 發表

資料來源：中時新聞網、iThome



年度資安查核
年度例查(約140項查核項目)



專案查核
多因子驗證導入情形，主機共置服務作業



選案查核
投資人檢舉案、主管機關指示事項



強化輔導
前一年度資安異常通報事項、前一年度漏未通報、缺失重複發生

資安缺失暨相關處置

<p>處置</p>	<p>1.注意改善 2.併課違約金5萬元至43萬元不等</p>
<p>依據</p>	<p>(營業細則)第135條第2項、 第138條第2項</p>

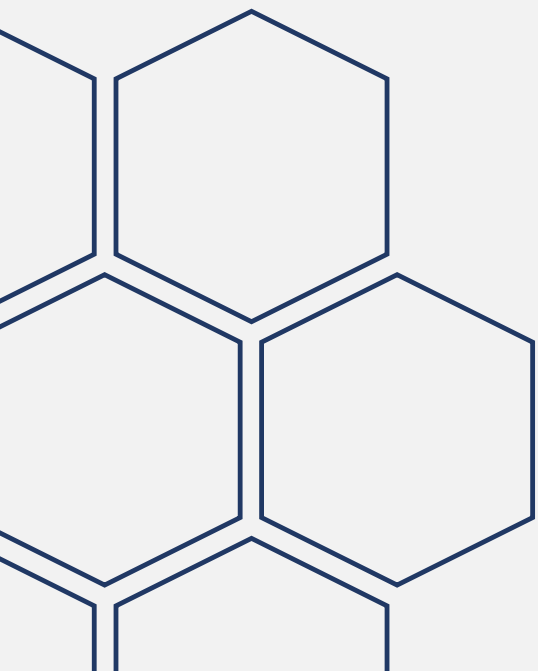
缺失重複發生，本公司得依營業細則處置如下

重複次數	一	二	三	四
處置	1.警告 2.併課新臺幣100萬元以下違約金	1.警告 2.併課新臺幣200萬元以下違約金	暫停3個月以下之買賣	暫停買賣
依據	1.第136條 2.第138條第2項	1.第136條 2.第138條第3項(半年內再次發生)	第139條	第142條第1項第5款



TAIWAN
STOCK EXCHANGE

資安查核重點





風險在哪裡？

外部威脅

- 駭客、天災...→防範未然

內部弱點

- 員工、門禁...→防微杜漸



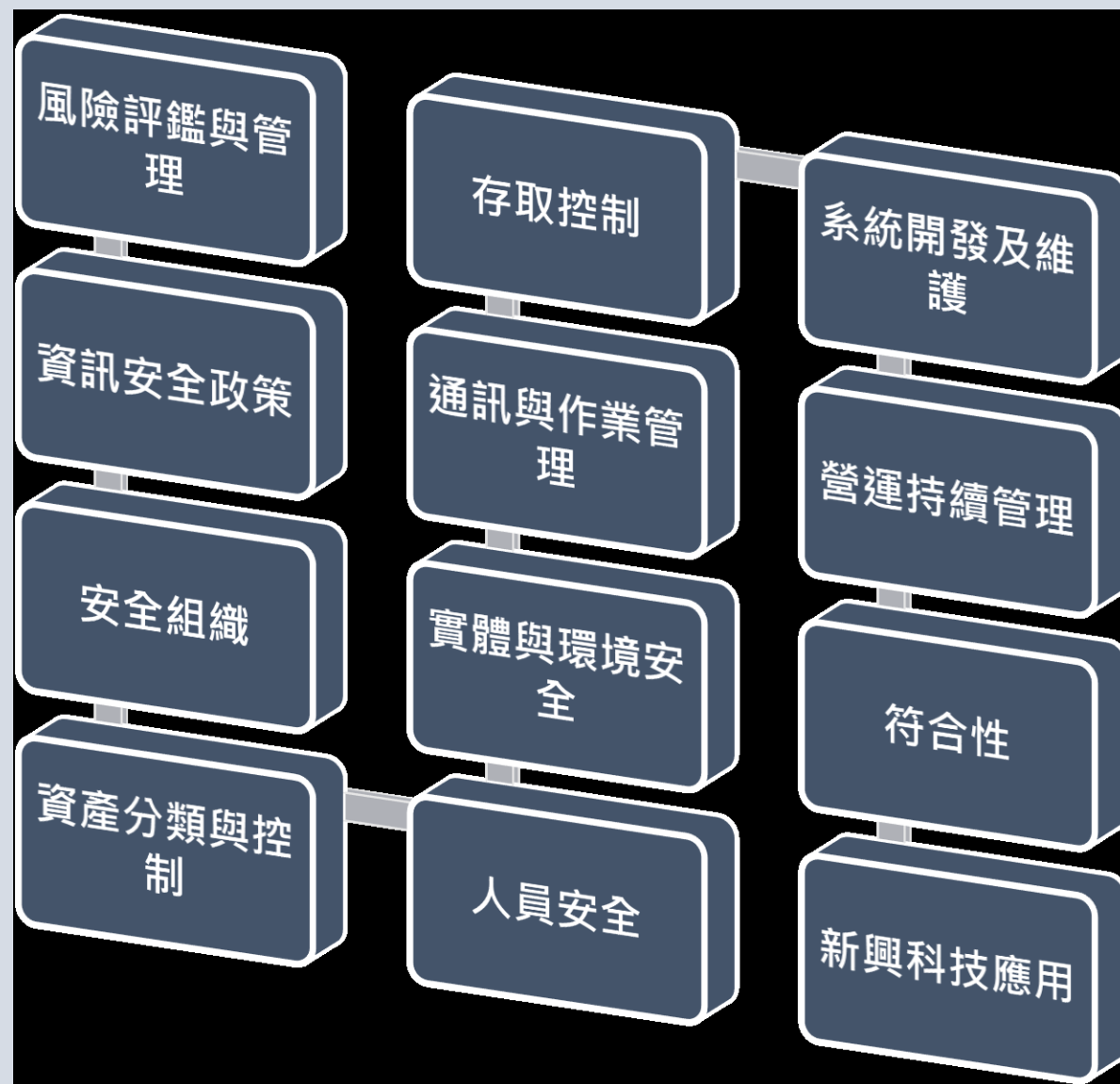




建立證券商資通安全檢查機制



- 辨識資安風險
- 訂定資安政策
- 配置組織資源
- 清查資訊資產
- 強化人員管理
- 監控環境設備
- 管理通訊作業
- 落實存取控制
- 控管開發維運
- 提升營運韌性
- 實作規範相符
- 納管新興科技



金融檢查重點

- 檢查局年度查核重點(本國銀行、壽險業)

機敏資料作業

- 端點防護資料外洩

登入及憑證下載

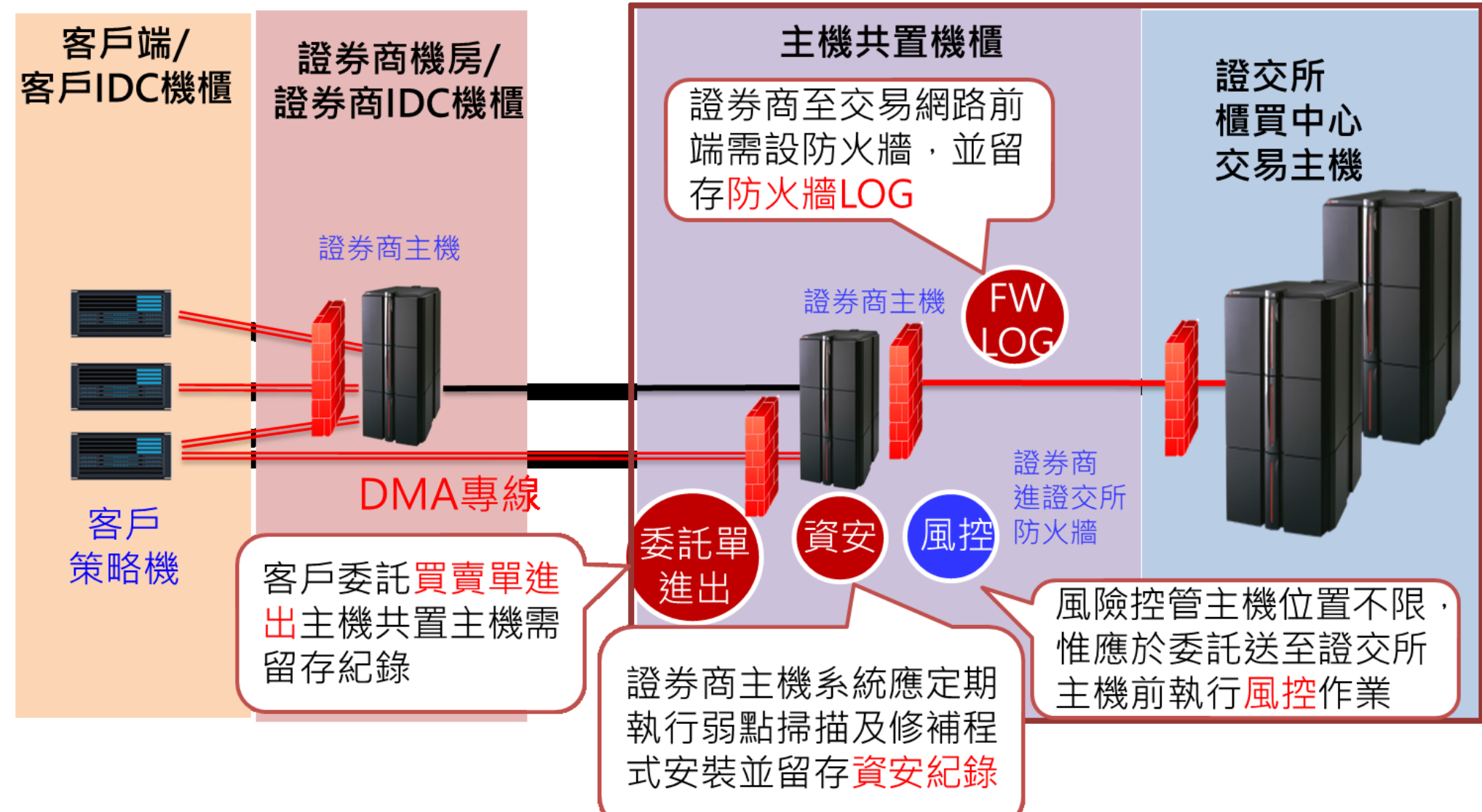
- 網路交易系統驗證完整性

駭客攻擊防護

- 異常活動檢視、資料備份落實情形

證券商就上述項目，應訂有內稽內控制度並留存稽核軌跡

主機共置服務





查核總結
會議



資安組織與人力配置

網路與系統防護

程式變更管理

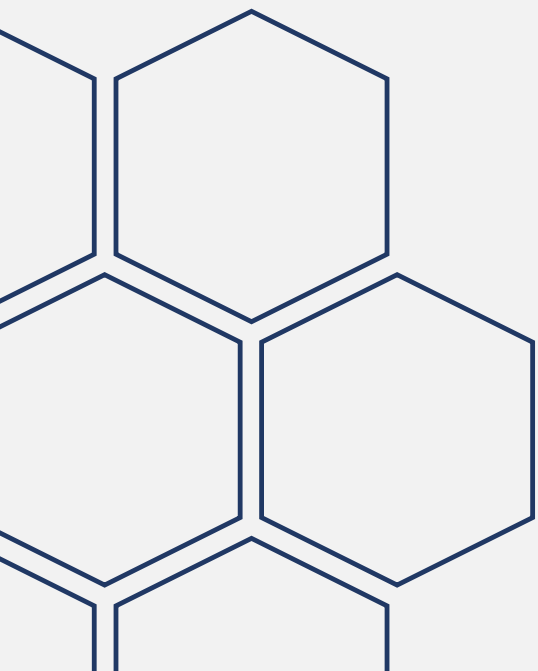
持續營運量能

機敏資料防護



TAIWAN
STOCK EXCHANGE

常見缺失說明



類別	缺失
1 營運持續	未依主管機關「證券期貨市場資通安全事件通報應變作業注意事項」規定，向主管機關辦理資通安全事件通報。
2 存取控制	未定期審查並檢討久未使用之使用者權限。
3 存取控制	資通安全存取控制之密碼管理作業，尚未能全面使用優質密碼設定，或未能定期3個月以內更新相關使用者之密碼。
4 網路安全管理	網路下單未採多因子驗證方式。
5 網路安全管理	未定期或適時修補網路運作環境之安全漏洞。

1. 未落實資安通報 形成資安聯防缺口

金融資安聯防體系

事前防患未然

F-ISAC彙整分析全球資安事件情資，發布駭客威脅預警，並培育資安專業人員，讓金融業者得以事先防範。

事中防微杜漸

F-SOC關聯分析金融業者回傳之事件資訊，探究潛在之可疑行為與攻擊風險，結合情資分享平台強化聯防監控體系。

事後降低傷害

F-CERT協同資安廠商提供應變處理服務，協助金融業者進行損害控制，期能降低損害，儘早恢復金融服務。

2. 未定期審查並檢討久未使用之使用者權限
3. 資通安全存取控制之密碼管理作業，尚未能全面使用優質密碼設定，或未能定期3個月以內更新相關使用者之密碼。

已故員工也可能存在 資訊安全風險

2021/03/09 作者：國際瞭望

分類：社群, 資安

Tags：cyber hygiene, 勒索病毒, 勒索, 即時訊息, 國內外重要資安新聞, 國際瞭望



[< 回到上一頁](#)



4. 網路下單未採多因子
驗證方式、重複使用
知識因子進行驗證。



5. 未依規定期評估網路系統安全、未依評估結果進行弱點修復。



The screenshot shows a news article on the iThome website. The article title is "Windows重大漏洞ZeroLogon可讓駭客輕易掌控AD網域". The text describes a CVE-2020-1472 vulnerability in Netlogon that allows unauthorized users to gain administrative control of an Active Directory network. It mentions that Microsoft released a patch on Patch Tuesday in August, with a first-stage fix expected in the first quarter of the following year.

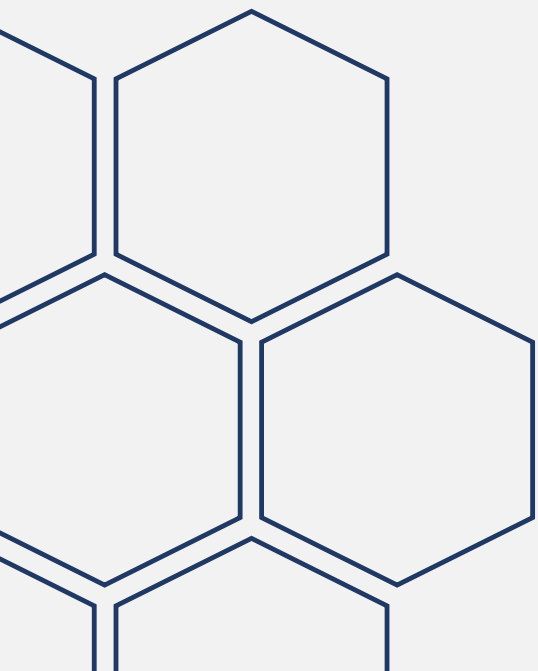
Below the article is a GitHub repository for "SecuraBV / CVE-2020-1472". The repository title is "ZeroLogon testing script". The description states: "A Python script that uses the Impacket library to test vulnerability for the ZeroLogon exploit (CVE-2020-1472). It attempts to perform the Netlogon authentication bypass. The script will immediately terminate when successful performing the bypass, and not perform any Netlogon operations. If the target domain controller is patched, the script will give up after sending 2000 pairs of RPC calls and conclude the target is not vulnerable (with a false chance of 0.04%)."

On the right side of the screenshot, there is a promotional banner for "2021 iThome 鐵人館" (Iron Man Pavilion) featuring a webinar and learning resources. Below that is a social media-style notification for "iThome Security" with 1.4 million followers, mentioning a security alert about a vulnerability.



TAIWAN
STOCK EXCHANGE

案例說明



- 110年11月○○證券察覺到部份客戶之海外複委託下單，出現購買港股「深藍科技控股」之異常案件，隨即清查客戶相關交易帳戶。
- 主因是APP下單之憑證申請僅使用「出生年月日」或「弱密碼」，遭到駭客破解下載憑證並偽冒下單。

7家證券期貨商遭「撞庫攻擊」 金管會祭3大措施

2021/12/15 07:40



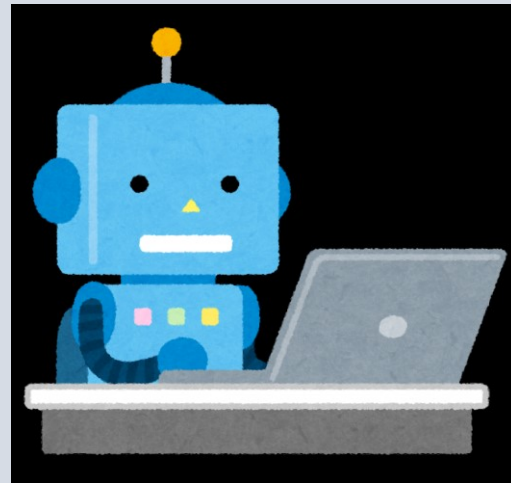
針對駭客以密碼「撞庫攻擊」，金管會表示，已責成證交所與期交所督導國內證券期貨商進行3大強化措施，以保護投資人權益。(資料照)

圖片來源：自由時報

透過各種管道
取得投資人帳
號等資訊



透過腳本執行
撞庫攻擊，確
認可用帳號



盜用帳號透過
APP申請交易
憑證



複委託偽冒下
單





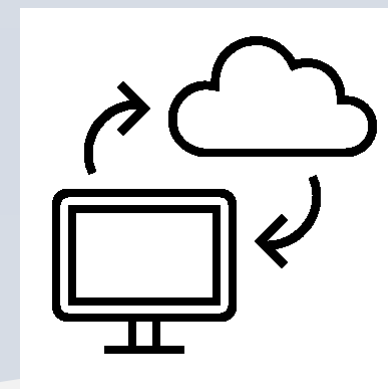
TAIWAN
STOCK EXCHANGE

未來展望

機密不外洩

資料不錯誤

服務不中斷



期待證券商資安落實C.I.A.，達成「零容忍」目標。



TAIWAN
STOCK EXCHANGE

簡報結束
敬請指導