

證券商資安作業應辦 暨注意事項說明

證券商資安查核與輔導

資安查核重點

常見缺失說明

重要事項宣導



TAIWAN
STOCK EXCHANGE

證券商資安 查核與輔導

資安事件要怎麼防範

發生的可能性

• 公司沒有價值 = 不會發生？

影響的程度小

• 損害控管

110年政府機關重大資安事件通報

項次	通報時間	通報機關	事件說明	事件根因
1	110/1/25	教育體系	網站遭外部使用者不當存取方式，下載約1.3萬筆個人資料。	人為疏失
2	110/2/3	地方政府	廠商於活動網站發布抽獎資訊時，誤放連結使民眾資料外洩。	人為疏失
3	110/2/24	司法體系	資料庫服務中斷，超過可容忍中斷時間。	設備問題
4	110/3/26	教育體系	承辦人未將敏感資料進行遮罩即將包含個人資料上傳至網站。	人為疏失
5	110/3/26	教育體系	承辦人未將敏感資料進行遮罩即將包含個人資料上傳至網站。	人為疏失
6	110/4/16	教育體系	網站存在程式漏洞遭外部使用者不當利用，下載約650筆個人資料。	人為疏失
7	110/4/22	教育體系	來自國外異常連線以AP管理者帳號登入網頁，惟該職員休假中，疑似因弱密碼導致入侵。	人為疏失
8	110/5/10	中央機關	涉及CI維運系統服務中斷。	設備問題
9	110/6/4	教育體系	因線上報名程式漏洞導致部份個人資料外洩。	人為疏失
10	110/8/25	教育體系	線上表單權限設定不當導致學生填報資料外洩。	人為疏失
11	110/9/6	教育體系	線上表單權限設定不當導致填報資料外洩。	人為疏失

今年至今尚無入侵事件，多為人為疏失造成個人資料外洩，已要求加強個人資料的保護



年度資安例查

- 協助檢視整體資安防護及法規落實情形

選案查核

- 投資人檢舉、主管機關指示

專案查核

- 特定議題對市場之影響或檢視整體辦理情形

加強輔導查核

- 特定態樣強化輔導

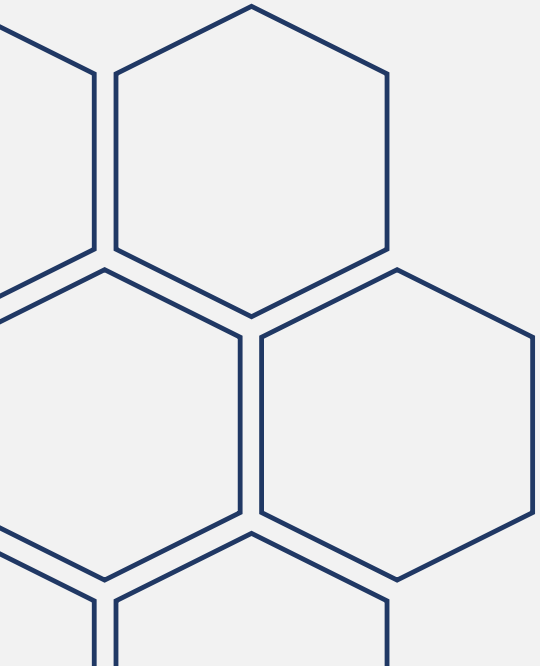
近兩年發生缺失本公司相關處置及違約金統計

處置內容	注意改善 併課違約金5萬元至43萬元不等
處置依據 (營業細則)	第135條第2項 第138條第2項

如重複發生相同缺失，本公司將依規辦理如下

重複發生	一	二	三	四
處置內容	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
處置依據 (營業細則)	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

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

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



年度金融檢查重點

- 年度重點(本國銀行、壽險業)、系統參數檢查

機敏資料保護情形

- 端點防護

強化登入及憑證下載 驗證

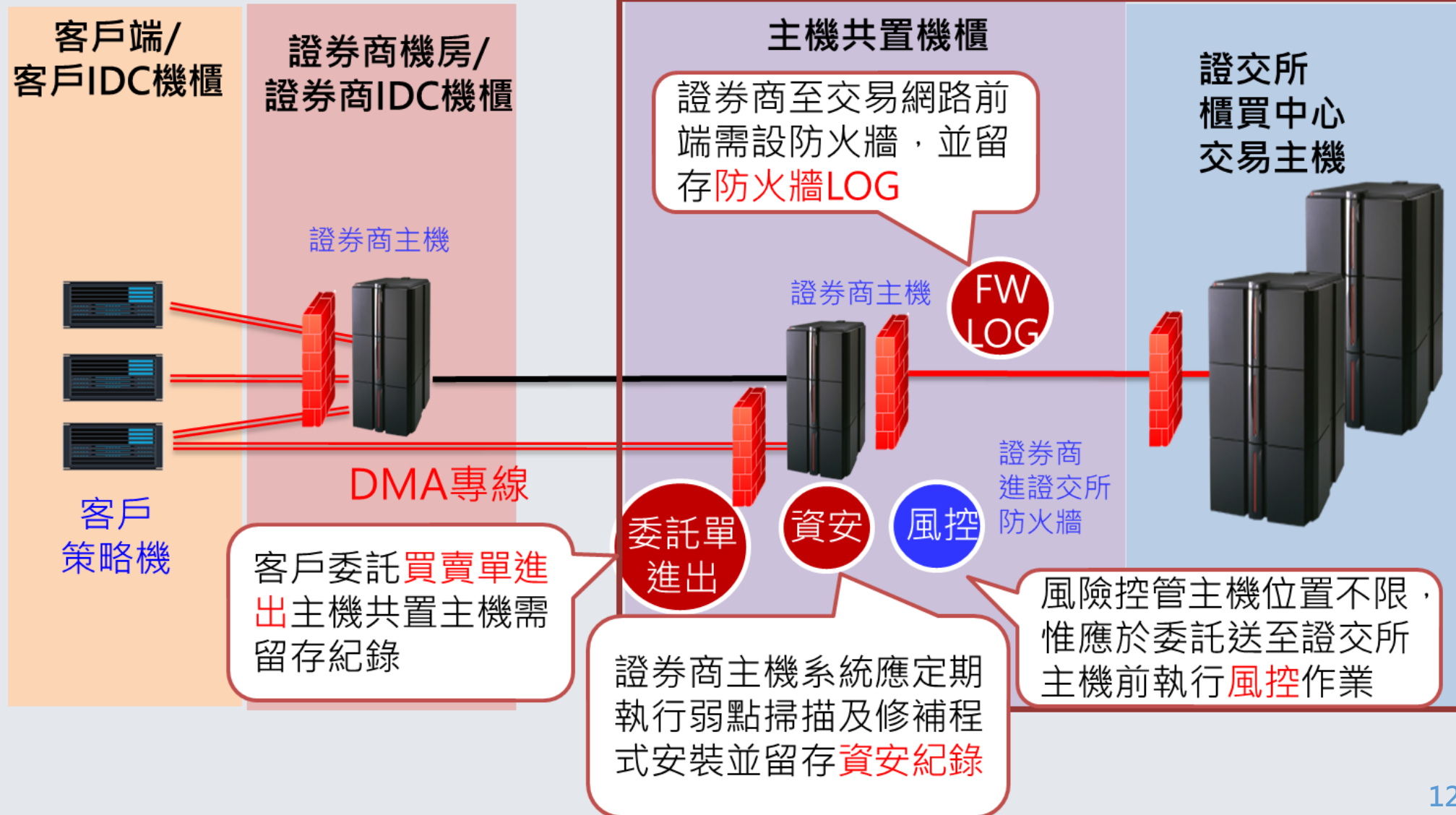
- 網路交易系統驗證完整性

駭客攻擊之防護

- 異常活動檢視、資料備份落實情形

資安查核重點

證券商就上述項目，應訂有內稽內控制度並留存稽核軌跡



資安防護
彙總



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

常見缺失說明

查核項目		查核缺失
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	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。
4	網路安全管理	網路下單未採多因子驗證方式。
5	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。

- 未落實資安通報可能造成資安聯防缺口(防範未然、防微杜漸、傷害管控)

金融資安聯防體系

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

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。

- 未定期審查並檢討久未使用之使用者權限
- 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。

 財團法人台灣網路資訊中心
TAIWAN NETWORK INFORMATION CENTER

域名服務 IP/ASN申請 網路統計 研討會 教育訓練 社會責任

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, 勒贖, 即時訊息, 國內外重要資安新聞, 國際瞭望



[← 回到上一頁](#)



- 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。



資料來源：資安人

- 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。



iThome 新聞 產品&技術 專題 AI Cloud DevOps 資安 研討會 社群 零信任資安講堂 搜尋

Windows重大漏洞ZeroLogon可讓駭客輕易掌控AD網域

位於Netlogon遠端協定的CVE-2020-1472漏洞，可讓未授權使用者取得管理員權限來控制整個網域。駭客一旦開採成功便能駭入並控制公司Active Directory網域，危及所有連網電腦。微軟在8月Patch Tuesday發布第一階段修補，預計明年第一季進行更完整的修補

文/ 林妍濤 | 2020-09-16 發表 讚 6.7 萬 按讚加入iThome粉絲團 讚 439 分享

[SecuraBV / CVE-2020-1472](#)

[Code](#) [Issues 1](#) [Pull requests](#) [Actions](#) [Projects](#) [Security](#)

ZeroLogon testing script

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 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%).

2021 iThome 鐵人館
鐵人webinar 鐵人遊樂場
各種 IT 技術學習資源
等你來體驗

合作夥伴 [arm](#) [永豐金控](#) [Shutterstock](#) [Microsoft](#) [台灣電](#)

iThome Security
說這專頁讚 1.4 萬 個讚

iThome Security
59 分鐘前

資安人員找尋並揭露漏洞的同時，很可能面臨被廠商以電腦詐欺或是著作權法進行提告的風險。其中

資料來源：iThome

重要事項 宣導

112、113年應完成項目

證券商分級 應辦事項	第一級(A級)證券商 實收資本額200億(含)以上	第二級(B級)證券商 實收資本額100億(含)~未達200億	第三級(C級)證券商 實收資本額40億(含)~未達100億	第四級(D級)證券商 實收資本額未達40億
國際標準通過驗證	V	V	V	-
資通安全專業證照	V	V	V	V
資通安全健診	V 每年辦理一次	V 每二年辦理一次	V 每二年辦理一次	-
資通安全威脅偵測(SIEM)管理機制	V	V	V	-
入侵偵測(IPS)及防禦機制	V	V	V	V
應用程式防火牆(WAF)	V	V	V	V
進階持續性威脅攻擊(APT)防禦措施	V	-	-	-

明年實施

資本額分級標準	資安單位暨人力編制
200億以上(1級)	應設資安專責單位，資安主管及至少 <u>3</u> 名資安人員
100億以上未達200億(2級)	資安主管及至少 <u>3</u> 名資安人員，但若已設專責單位，人員可維持 <u>2</u> 人
40億以上未達100億(3級)	資安主管及至少 <u>2</u> 名資安人員
未達40億(4級)	至少1名資安人員(維持)

資安事件通報

為確保資安通報之正確及有效性，資安事件通報應於初步通報後24小時內完成正式通報。



通報作業

竭誠為您服務

初步通報

知悉事件30分鐘內辦理

取消通報

釐清事件
確認誤報

正式通報

於查明事件
後儘速辦理

解除通報

事件處理
完成後

公司與資訊公司合作對外提供服務，應確實瞭解資訊公司具體業務內容，並就對外提供之服務有明確責任歸屬，且資訊公司如未經金管會許可及發給證券許可證照，不得涉及經營證券業務。



我是股神

模擬下單教學體驗營

第一階段活動日期
10/26 (三) 9:00 ~ 11/8 (二) 13:30

留言 按讚 分享

加入遊戲抽禮券，豐富獎項等你來拿！

簡報結束
敬請指導