大 仁 科 技 大 學
Tajen University

管 制 文 件 訂 修 廢 履 歷 表

文件編號	資訊-標準-05	文件名稱	外力入侵事件緊急應變作業標準書
使用部門	圖書資訊館	機密等級	普通

版次	頁數	文件修訂摘要	實施日期
A.0	4	初版	99/05/24

訂修廢者	單位主管	圖書資訊館館長

※管制文件不得擅自塗改及做記號並禁止影印。

1.外力入侵事件緊急應變程序

1.1 病毒及蠕蟲程式：

病毒及蠕蟲程式處理應變步驟如下：

1.1.1 第一步：通知相關人員

即刻通知系統管理人員或應用程式管理人員到場協助處理。

1.1.2 第二步：隔離系統

將遭受攻擊之系統迅速自網路移除，但在移除前，須先審慎考量相關修補程式或解藥程式是否可以安裝。在處理時必須要詳細紀錄下所有的步驟。在未確定蠕蟲或病毒完全被控制之前，不得將 Internet 的網路線重新接回。

1.1.3 第三步：辨識問題

緊急處理小組應在中毒主機列出可疑的病毒相關檔案或系統程序，並予以清除或隔離。在處理時必須要詳細紀錄下所有的步驟，以利日後分析。如無法辨識，緊急處理小組應聯繫防毒軟體廠商，提供解決的方法。

1.1.4 第四步：移除及預防病毒

將有問題的系統程序終止或移除，並利用廠商所提供的修補程式或解毒程式來移除病毒。所有系統，不論是否遭受攻擊，應同時進行掃毒及預防的工作。

1.1.5 第五步：恢復運作

在將系統恢復至正常運作狀態時，須逐步實施，並通知使用者恢復作業的進行。緊急處理組應要求各使用者或系統管理者密切注意系統復原狀況，發現任何異常，應立即停止所有復原程序進行查錯。若毫無任何升級或修補程式可用，則應利用事件發生前無瑕疵的系統備份來作恢復的工作或重新安裝系統。

1.1.6 第六步：後續檢討

當事件處理完畢，系統恢復至正常運作狀態後，緊急處理組應作後續的檢討，並評估或修改既有不合時宜的相關程序。所作成的報告在彙整之後可作為範例或教案分發給相關人員。

1.2 網路入侵：

發現或被入侵時，處理步驟如下：

1.2.1 第一步：斷線並通知相關人員

即刻予以斷線並通知系統管理者到場協助處理。

1.2.2 第二步：辨識問題

從系統事件紀錄檔及進行中的網路連線中找出攻擊的出處。相關網管人員協助嘗試找出入侵者 IP 位址。

1.2.3 第三步：控制問題

如果決定保持入侵者的連線以搜集證據，緊急處理小組應將營運停頓及資料外洩的風險納入考量。

1.2.4 第四步：移除問題

終止所有執行中的異常程序，並移除任何有心人士所留下的帳號、檔案或目錄。如果只有一個帳號為有心人士所使用，則此帳號的密碼須加以更改，如果是超過一個以上的帳號為有心人士所使用，則最好強迫所有使用者更改密碼。聯絡軟體廠商提供修補程式以修復系統的安全漏洞。

1.2.5 第五步：恢復運作

在將系統恢復至正常運作狀態時，須逐步實施，並通知使用者恢復作業的進行。緊急處理小組應要求各使用者或系統管理者密切注意系統復原狀況，發現任何異常，應立即停止所有復原程序進行查錯。

1.2.6 第六步：後續檢討

當事件處理完畢，系統恢復至正常運作狀態後，緊急處理小

組應作後續的檢討，並評估或修改既有不合時宜的相關程序。所作成的報告在彙整之後可作為範例或教案分發給相關人員。

1.3 人員進出管制：

若有未經授權進入的閒雜人等在管制區域(如資訊機房)中徘徊，平日該關閉的門窗無故開啟等，這些皆會對資安環境形成潛在的威脅。人員進出管制的處理步驟如下：

1.3.1 第一步：辨識問題

如有不明人士在管制區中徘徊而無陪同人員在場，發現者應要求對方提出識別證明及來訪的事由。

1.3.2 第二步：解決問題

若對方未能提出有效證明，發現者必須立即通報警衛或通知校安中心聯絡警察單位處理。不明人士進入的方式及時間必須調查清楚。

1.3.3 第三步：後續檢討

當事件處理完畢，緊急處理小組應作後續的檢討。檢視相關的人員出入紀錄，比對不明人士進入的方式及時間，並且利用此機會來評估或修改既有不合時宜的程序。

1.4 阻斷服務攻擊（DOS）:

阻斷服務攻擊的處理步驟如下：

1.4.1 第一步：辨識問題

從系統或 IPS 的事件紀錄辨識攻擊的形態、範圍、本質，辨識攻擊者所使用方法是利用應用程式、封包遞送過程，或者是通訊協定的安全漏洞。往連線上游找出被控制的阻塞點，或找出攻擊的源頭。

1.4.2 第二步：通知相關人員

即刻通知系統管理者或區網中心協助處理。

1.4.3 第三步：控制問題

緊急處理小組可立即修改防火牆或網管系統的 ACL(Access Control List) 來限制惡意封包的通過，或運用其他封包過濾工具來阻擋攻擊的進行。如果決定將自攻擊來源的連線強制中斷，緊急處理小組應將營運中斷的風險納入考量。

1.4.4 第四步：移除問題

移除不必要的服務埠或調整軟體參數以避免過多 session 同時啟動。聯絡軟體廠商提供修補程式以修復系統的安全漏洞。

1.4.5 第五步：恢復運作

在將連線恢復至正常運作狀態時，須逐步實施，並通知使用者恢復作業的進行。緊急處理小組應要求各使用者或系統管理者密切注意連線復原狀況，發現任何異常，應立即停止所有復原程序進行查錯。

1.4.6 第六步：後續檢討

當事件處理完畢，連線恢復至正常運作狀態後，緊急處理小組應作後續的檢討。