

網站防護及應變處理說明

網站基本防護作業

請各單位自行查檢項目：

- 此檢查項目僅適用單位自行架設網站以及跟電算中心申請之虛擬主機，存放電算中心公務帳號空間中之網站不適用

主機：

○ 重新檢視防火牆相關設定是否合宜

檢視主機是否有開啟未使用的網路服務協定埠，沒有使用到的網路服務協定埠請關閉。

- 限定能存取該主機的 IP 連線。
- 例如：網站服務埠是 80、443，資料庫服務協定埠 3306(資料庫如果連到另一台主機)
- 限定只能存取該主機服務的 IP 連線(如 SSH 管理)

Linux:sudo ufw status verbose 或 iptables -L -n 可查看主機的防火牆規則

○ 檢視測試網站與帳號等已確實關閉或移除

定期的檢視是否有未建立或其他的帳號存在，若有請記得移除。

- 測試帳號只有相關管理者可以使用。
- 建議測試網站僅限特定 IP 才可以連線。

網頁主機：

cat /etc/passwd 可查閱整個系統的所有帳號

cat /etc/group 可查閱整個系統的所有群組

○ 確認內部使用網站未暴露於網際網路

設定特定範圍的 IP 能存取內部網站，可使用非特定範圍的 IP 連線，測試是否可以連到該網站。

- 例如：限定 140.115.*.* / 24 範圍的 IP 可以連，這樣的話可以使用手機的網路(非 wifi)測試連到該網站，若是連得到代表此設定是無效的。

如何設定 nginx 阻擋特定 ip / 網段存取，首先找到對應的 nginx configuration，

通常會在 /etc/nginx/sites-enabled/*.conf 或是預設的 /etc/nginx/nginx.conf

接著找到 server / location 區塊，加上 deny 語法

```

server {
    listen 443 ssl http2;
    server_name blog.camel2243.com
    # 阻擋特定 ip
    deny x.x.x.x
    ...
}
# 或者在指定的 location 區塊中
location / {
    # 阻擋 xxx.xxx.xx.0 ~ xxx.xxx.xx.255 的所有 ip
    deny xxx.xxx.xx.0/24;
    index index.php index.html index.htm;
    try_files $uri $uri/ /index.php?$args;
}
# 進階一點搭配 allow 的用法
server {
    listen 443 ssl http2;
    server_name blog.camel2243.com
    # 阻擋除了 ip 為 xxx.xxx.xx.235 以外的 xxx.xxx.xx.0 ~
    xxx.xxx.xx.255 網段
    allow xxx.xxx.xx.235;
    deny xxx.xxx.xx.0/24;
    ...
}

```

註:以上方式為舉例，請各單位自行依單位內網頁伺服器的套件搜尋設定方法。

若網頁遭置換緊急應變處理建議

○ 原因：

可能發生網頁被置換的原因是網站本身即存在漏洞，一旦被有心人士掌握，就可以在需要時隨他操弄。

萬一不幸發生網頁被置換的情況，在手忙腳亂當下，除了緊急將網站關閉，還能夠如何處理呢？

○ 緊急應變原則

參考行政院 111 年 8 月資安警戒專案相關會議指示，如發現所轄管系統網站內容遭竄改，應依下列原則辦理緊急應變：

- 將原網站立刻下架。（建議將原本 log 保存）
- 維護公告網頁：10 分鐘內發佈。
- 靜態資訊網頁：網站功能無安全疑慮的部分可先上架恢復服務，如純資訊公告、媒體播放等。
- 功能恢復：網站修復後請進行弱點掃描，確認無重大安全性弱點。
- 完成修復上架。

○ 網站放置於電算中心網頁空間(公務帳號)

- 網址為 <https://in.ncu.edu.tw/~ncuXXXXX>(公務帳號)

單位網站若原本放置於電算中心公務帳號網頁空間，當疑似因單位帳號遭竊導致網站內容被登入置換時，若無法立即將被置換網頁改回原狀，可採取以下做法：

- 密碼修改：請依照程序進行公務帳號密碼的修改。
- 置換通用版維護網頁：電算中心已事先設計通用版「網站維護中」訊息的網頁檔案，可先聯繫電算中心將單位網站首頁換成維護公告的網頁，且讓貴單位有時間將備份網頁檔還原到原網頁空間下。
- 導向備援網頁：若單位在另外的網頁空間已放置維護中訊息的網頁或重要訊息網頁，也可請聯絡電算中心將單位網站 URL 導向該備援網頁空間，以呈現單位客製化重要訊息，再請單位儘快修復網頁漏洞或將備份網頁檔還原到原網頁空間下。

○ 單位自行架設網站

- 網址:https://xxx.ncu.edu.tw/等

1. 密碼修改:建議修改主機的密碼

- 若單位自行於系上架設網站，建議以下作法：

2. 事先準備另一台網站主機為備援網站，定期將網頁內容備份至此，當發生網站遭網頁置換事件或遭駭時，先將正式網站斷線後，把備份網站的 IP 位址改為正式網站的 IP 位址，讓備份網站上線。

- 爭取時間恢復正式網站被置換的內容，也檢查網站其他功能是否也有安全疑慮並予修復。

- 待網頁程式或主機修復後再換回正式網站主機。

3. 若無額外主機可供備援，可考慮在外部網頁空間放置靜態網頁/維護中公告網頁或將網站首頁導至電算中心通用版「網站維護中」網頁。

上述做法優缺點簡述如下：

作法（2）單位擁有網站自主控制權，可快速讓臨時網站上線，降低網頁被置換的衝擊；

作法（3）單位可使用外部免費網頁空間資源提供原網站重要資訊，但生效時間無法掌握；

○ 單位網站若建置於電算中心二代虛擬主機服務區

- 網站 IP 為:140.115.197.XXX

當發生虛擬主機遭入侵並置換網頁情況時，建議以下作法：

1. 密碼修改：建議修改主機的密碼

2. 準備外部備援網站：

- 單位可事先在外部網頁空間準備「網站維護中」的網頁或備援網站，需要時聯繫電算中心將單位網站虛擬主機 DNS 指向外部備援網站。
- 可先電話連絡修改 DNS 再補送申請單或寄 email 至 DNS 承辦人提供佐證，但因使用者端 DNS 查詢及網頁瀏覽器快取（cache）也需要時間更新，因此可能會花費較長且無法確定的時間讓臨時網站達到效果。
- 將網站修復後記得要再聯絡電算中心 DNS 承辦人改回已修復的網站 IP。

建議：

- ◆ 定期檢視網頁主機的作業系統、網站伺服器、及網頁應用程式、套件等版本更新與漏洞修補。

- ◆ 網站備援與定期(建議每日)備份重要資料等防護措施。
- ◆ 應定期檢視網路、系統有無異常狀況及進行網站弱點掃描。

結語

本文僅傳達當網頁遭置換時的緊急應變建議作法，追根究底還是應該強化網站的安全性，包含作業系統、網站伺服器、及網頁應用程式等版本更新與漏洞修補，定期進行網站弱點掃描也可提供修補改善建議，以防堵因伺服器本身問題導致遭入侵而引發的網頁置換，或甚至資料外洩、遭攻陷成為魁儡跳板機等更嚴重的資安事件。

- 通用版「網站維護中」網址：
<https://maintenance.ncu.edu.tw>

- 需修改單位 DN 的 IP 時，請洽電算中心服務櫃台
電話:57555、57566 轉 DNS 承辦人

以上 DNS 修改說明僅限校定 DNS 網站(xxx.ncu.edu.tw)，若系所自己的 DNS 底下的網站請逕洽單位的 DNS 承辦人(如:XXX.mgt.ncu.edu.tw 等)。

網站基本防護作業自我檢核表

檢核日期： 年 月 日

單位	網站 IP 及網址	備註	
項目	說明	是否確認	備註
重新檢視防火牆相關設定是否合宜 *註 1	檢視主機是否有開啟未使用的網路服務埠，沒有使用到的網路服務埠請關閉。 ● 例如：網站服務埠是 80、443，資料庫服務協定埠 3306(資料庫如果連到另一台主機)、SSH 預設 22，建議改掉。 ● 限定能存取該主機的 IP 連線。(如 SSH 管理)	☐ 未確認 ☐ 已確認	
檢視測試網站與帳號等已確實關閉或移除 *註 1	定期的檢視是否有未建立或其他的帳號存在，若有請記得移除。 ● 建議測試網站僅限特定 IP 才可以連線。 ● 測試帳號只有相關管理者可以使用。	☐ 未確認 ☐ 已確認	
確認內部使用網站未暴露於網際網路 *註 1	設定特定範圍的 IP 能存取內部網站，使用非特定範圍的 IP 連線，測試是否可以連到該網站。 ● 例如：限定 140.115.x.0/24 範圍的 IP 可以連，可以使用手機的行動網路(非 wifi) 測試連到該網站，若是連不到代表此設定是有效，若連得到代表此設定是無效的，需要重新設定限制規則。	☐ 未確認 ☐ 已確認	
單位內是否有準備緊急應變網頁或備用網站	例如： ● 【網頁維修中】公告頁面。 ● 備用網站	☐ 未確認 ☐ 已確認	

***註 1:** 此檢查方式僅適用單位自行架設網站、及放置於電算中心虛擬主機服務區