網路入侵事件作業程序

|  |  |
| --- | --- |
| ◎文件編號： | SO-09-005 |
| ◎文件版本： | V 2.2 |
| ◎發行日期： | 2017/04/10 |

文件修訂履歷

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 發行／修訂版次 | 發行／修訂  生效日期 | 發行與變更說明 | 發行／修訂人員 | 核准 人員 | 備註 |
| V1.0 | 2005/12/12 | 新版文件發行 | 余萬事 | 梁維誠 |  |
| V1.1 | 2006/12/12 | 1. 權責修定，技術研發處改為維護營運處主管及相關人員 2. 任務編組修定 | 李宏奎 | 郭美伶 |  |
| V1.2 | 2008/10/03 | 1. 處理程序修訂 2. 相關廠商聯絡電話更新 | 余萬事 | 梁維誠 |  |
| V1.3 | 2009/11/02 | 修訂第四章相關文件以SO-18-001\_事件管理辦法、SO-13-001\_問題管理辦法取代SO-09-001\_資訊安全事件通報暨處理作業辦法。 | 余萬事 | 梁維誠 |  |
| V1.4 | 2010/04/08 | 1. 修訂第三章第二節維運處人員職責說明。 2. 修訂第六章第三節，調整為由維運三科負責維護更新。 | 余萬事 | 梁維誠 |  |
| V1.5 | 2011/10/21 | 因應公司更名，修訂文件公司名稱。 | 余萬事 | 周宗亮 |  |
| V2.0 | 2011/11/18 | 因應公司文件核准層級，文件名稱配合變更。 | 余萬事 | 周宗亮 |  |
| V2.1 | 2014/3/20 | 增訂《SO-09-005-附件A\_網路入侵事件作業流程圖》 | 余萬事 | 丘建華 |  |
| V2.2 | 2017/04/10 | 修訂第五章名詞定義新增《SO-09-005-F01分散式阻斷服務攻擊(DDoS)之應變暨處理措施》 | 李柏慶 | 余萬事 |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

目 錄

[第一章 目的 4](#_Toc383088828)

[第二章 適用範圍 4](#_Toc383088829)

[第三章 職責分工 4](#_Toc383088830)

[第一節 維護營運處主管 4](#_Toc383088831)

[第二節 維運營運處人員 4](#_Toc383088832)

[第三節 相關系統管理員 4](#_Toc383088833)

[第四章 相關文件 4](#_Toc383088834)

[第五章 名詞定義 4](#_Toc383088835)

[第六章 作業內容 4](#_Toc383088836)

[第一節 任務編組 5](#_Toc383088837)

[第二節 處理程序 5](#_Toc383088838)

[第三節 相關廠商聯絡電話 7](#_Toc383088839)

[第七章 輸出文件/紀錄 7](#_Toc383088840)

# 目的

為確保遭受網路入侵時，能有效通報並即時處理，爰擬訂此作業程序。

# 適用範圍

所有網路入侵事件皆適用此程序。

# 職責分工

## 維護營運處主管

負責網路入侵事件之處理，可授權或指定維運三科科主管，或資訊安全人員協助執行。

## 維運營運處人員

### 由維護營運處維運三科人員負責。

### 提供相關網路安控設備及系統之記錄，配合處理網路之設定與線路之介接。

### 發生疑似網路入侵事件時進行緊急處理並與相關廠商聯繫。

## 相關系統管理員

提供所管理之系統記錄。

# 相關文件

### SC-01-007\_通訊與作業管理

### BO-CM-007\_危機溝通程序

### SO-18-001\_事件管理程序

### SO-13-001\_問題管理程序

# 名詞定義

### 分散式阻斷服務攻擊(Distributed Denial of Service, DDoS)主要利用殭屍網路與系統弱點，發出大量合法或偽造之請求，占用大量網路及設備資源，以達到癱瘓攻擊目標網路及系統之目的。

# 作業內容

## 任務編組

主要由維護營運處維運三科負責。

## 處理程序

### 處理流程圖

辦識

抑制

追蹤

移除

復原

### 辦識階段

由維護營運處維運三科人員負責，判斷事件性質及預估事件處理時間。

#### 判斷事件是否為網路入侵事件：檢查所有徵兆，避免誤判。

#### 執行檢視入侵偵測系統事件記錄時，發現可疑侵入行為，應立即通知維護營運處維運三科科主管及處主管，由主管協助研判。

#### 在事件確認過程中，若因技術問題需要支援，則由維護營運處主管或相關廠商提供協助支援助。

#### 保存證據：記錄之保存，日誌之保存。

#### 通報流程：依《SO-18-001\_事件管理程序》、《SO-13-001\_問題管理程序》進行通報及處理，惟由於網路入侵除造成系統失效之外，可能造成資訊洩漏之狀況，因此若發現有資訊洩漏之可能時，經通報後應優先以A級事件進行處理，並依據《BO-CM-007\_危機溝通程序》進行必要之危機溝通程序。

#### 所有追蹤處理過程，需留下相關紀錄，以做為佐證依據。

### 抑制階段

由維護營運處維運三科科主管及處主管負責協助系統管理員，進行入侵事件抑制。

#### 立即由防火牆阻絕入侵者任何存取動作，防止災害繼續擴大。

#### 立即拔除受侵害主機之網路線使其與本部區域網路隔離，並關閉該系統之一切服務，待進一步釐清問題。

#### 避免使用有可能已被洩漏之帳號。

#### 將發生問題之系統、環境隔離出來。

#### 備份系統：將被破壞的系統備份，並保存備份。

#### 蒐集並分析取得之資訊：紀錄分析及建議、入侵者或資安事件來源是否持續動作。

#### 暫時關閉服務：斷線使存取失效、清查其它系統資料。

#### 持續和系統管理者交換意見。

### 移除階段

由維護營運處主管及相關部門系統管理員負責協助辦理。

#### 了解入侵事件之攻擊方式。

#### 移除入侵事件成因：人為破壞、病毒侵擾、惡意程式碼破壞、駭客入侵。

#### 弱點分析：若為系統問題，應進行系統之弱點分析。

#### 加強防護：檢查防火牆及系統紀錄，研判入侵管道及方式，並作主機安全漏洞修補，若發覺確有惡意攻擊行為或維護營運處主管無法研判應依循資訊安全事件通報暨處理程序進行通報及尋求支援。

### 復原階段

#### 立即通知主機供應商提供必要之回復協助，將完整的系統備份資料存回主機上，並測試其功能無誤後重新上線。

#### 確認系統屬於正常狀態。

#### 決定何時回復系統正常運作。

#### 持續監視系統運作。

### 追蹤階段

由資訊安全人員負責，並與相關人員討論是否修訂「資訊安全政策」。

#### 由系統管理員撰寫入侵事件報告。

#### 重新進行網路和系統的資產清查，並檢視是否有類似系統遭受波及。

#### 保存所有事件移除分析、處理紀錄，並與相關單位或人員進行事後檢討會議。

#### 對事件所造成衝擊，進行更嚴謹的風險分析，達成可執行之改進結論，將改善建議報告交給管理階層，執行管理階層許可後之改善動作。

#### 修訂安全防禦計畫、政策、程序，並進行使用者及管理者之教育訓練以防止遭受再次的資訊安全事件。

#### 結案時需將資料、報告整理完畢後歸檔，完成結案作業。

### 分散式阻斷服務攻擊(DDoS)相關應變措施詳見《SO-09-005-F01分散式阻斷服務攻擊(DDoS)之應變暨處理措施》

## 相關廠商聯絡電話

相關廠商聯絡資訊由維運三科廠商窗口人員負責維護更新。

# 輸出文件/紀錄

### SO-09-005-附件A\_網路入侵事件作業流程圖

### SO-09-005-F01分散式阻斷服務攻擊(DDoS)之應變暨處理措施