|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | |  | |
| **證券期貨業**  **分散式阻斷服務防禦與應變作業程序**  **(V1.0)** | | | | |
|  | |  | |  |
|  | | | | |
|  | | | | |

**修訂歷史紀錄表**

|  |  |  |  |
| --- | --- | --- | --- |
| **項次** | **版次** | **修訂日期** | **說明** |
| 1 | V1.0 | 106/2/18 | 新編。 註：參照行政院國家資通安全會報105年11月18日修訂之「政府機關分散式阻斷服務防禦與應變作業程序(V2.0)」 |
| 2 |  |  |  |
| 3 |  |  |  |

**目次**

[壹、 前言 2](#_Toc475199401)

[一、 目的 2](#_Toc475199402)

[二、 適用對象 2](#_Toc475199403)

[三、 章節架構 2](#_Toc475199404)

[四、 使用建議 3](#_Toc475199405)

[貳、 DDoS防護機制及應變作業流程 4](#_Toc475199406)

[一、 DDoS防護機制 5](#_Toc475199407)

[二、 DDoS防禦與應變作業流程 6](#_Toc475199408)

[參、 業者因應DDoS之防護作為 8](#_Toc475199409)

[一、 事前準備 8](#_Toc475199410)

[(一) 維護系統及網管人員/廠商聯繫資訊 8](#_Toc475199411)

[(二) 調校系統/服務設定 8](#_Toc475199412)

[(三) 設置網路流量/系統資源監控機制 9](#_Toc475199413)

[(四) 啟用網路/防護設備DDoS防禦功能 9](#_Toc475199414)

[(五) 申請/建置流量清洗服務 12](#_Toc475199415)

[(六) 申請內容傳遞網路(Content Delivery Network, CDN)服務 12](#_Toc475199416)

[(七) 建置/申請雲端備援 13](#_Toc475199417)

[二、 事中應變 14](#_Toc475199418)

[(一) 攻擊事件通報 14](#_Toc475199419)

[(二) 攻擊事件分析 14](#_Toc475199420)

[(三) 啟用流量清洗服務 15](#_Toc475199421)

[(四) 啟用雲端備援 15](#_Toc475199422)

[三、 事後處置 16](#_Toc475199423)

[(一) 復原資訊設備運作 16](#_Toc475199424)

[(二) 持續監控網路流量 16](#_Toc475199425)

[(三) 記錄事件處理過程 16](#_Toc475199426)

[(四) 攻擊事件結報 16](#_Toc475199427)

[肆、 參考文獻 17](#_Toc475199428)

[伍、 附件 18](#_Toc475199429)

[附件1 事前準備階段查核清單 18](#_Toc475199430)

[附件2 系統及網管人員/廠商聯繫表 18](#_Toc475199431)

[附件3 服務主機防護設定 18](#_Toc475199432)

[附件4 網路流量及系統資源監控軟體(MRTG)安裝設定 18](#_Toc475199433)

[附件5 國內ISP流量清洗申請服務說明 18](#_Toc475199434)

[附件6 Cloudflare CDN服務申請與設定 18](#_Toc475199435)

[附件7 事中應變階段查核清單 18](#_Toc475199436)

[附件8 事後處置階段查核清單 18](#_Toc475199437)

**圖目次**

[圖1 DDoS多層次防護機制 5](#_Toc475199438)

[圖2 DDoS防禦與應變作業流程 7](#_Toc475199439)

[圖3 網路設備DDoS防護示意圖 9](#_Toc475199440)

[圖4 ADC運作示意圖 11](#_Toc475199441)

[圖5 CDN傳遞路徑示意圖 13](#_Toc475199442)

# 前言

## 目的

多家證券期貨業者於106年2月遭駭客集團以分散式阻斷服務攻擊（Distributed Denial-of-Service attack, DDoS）企圖癱瘓網站服務，進行勒贖事件，為能有效強化我國證券期貨市場DDoS防護能量，本程序書綜整應變防護機制，並供資訊人員進行相關資訊設備防護設定之參考，期望業者依內部設備與資源，發展 DDoS 攻擊之防禦與應變作業程序，當業者遭受DDoS攻擊時，資訊人員能參考適當的應變處置措施，儘速減緩DDoS攻擊影響，使資訊設備或服務能儘速恢復正常營運。

## 適用對象

本程序書所規劃之作業流程與相關工作建議事項，可適用於各證券期貨業者之一般主管、資安人員、資訊人員及資安聯絡人等。各證券期貨業者除依據各自發展的資訊安全管理制度(Information Security Management System, ISMS)處理DDoS攻擊事故之外，亦可參考本程序書所編撰的作業流程與相關工作建議進行處理。

## 章節架構

本程序書初步介紹相關的防禦設備與措施，提供業者在面對DDoS攻擊所可採取之系統化方法。

* 第壹章、前言：說明本程序書之目的、適用對象及章節架構。
* 第貳章、DDoS防護機制及應變作業程序：介紹DDoS攻擊之防護機制及相關應變作業程序。
* 第參章、業者因應DDoS之防護作為：提及面對DDoS攻擊可執行的應對策略，包含網路防護設備DDoS設定、雲端備援機制、申請/建置DDoS緩解設備、系統/服務設定調校與維護網路維護人員/廠商聯繫資訊。
* 第肆章、參考文獻：詳列本程序書所參考的文件或資料。
* 第伍章、附件：提供本程序書相關表單與設定操作說明。

## 使用建議

本程序書內容彙整DDoS防禦與應變相關作業，業者可詳閱並以本程序書為基礎，規劃符合業者所提供服務與需求之DDoS防禦與應變程序書。

# DDoS防護機制及應變作業流程

DDoS是利用分散於不同地方的資訊設備(多數為跨國之殭屍網路)進行多對一的攻擊，透過發送難以追查且大量的封包，癱瘓目標資訊設備，使之無法提供服務。DDoS攻擊之另外一種變形為反射式放大攻擊(Distributed Reflection Denial of Service, DRDoS)，是一種搭配偽造來源IP之封包與協定先天設計的漏洞或不當的服務主機設定之攻擊方式，近期攻擊手法多以效果較為顯著的DRDoS為主。

DDoS在網路攻擊中並不新穎，但因其極具破壞力而逐漸被頻繁利用，隨著攻擊技術的成熟與工具的開發，並配合運作殭屍網路作為攻擊來源，導致DDoS的攻擊在流量不斷攀升的同時，門檻也不斷地在下降。而攻擊手法也從以往的單一型態攻擊，轉而使用複雜度更高的混合型態，來瓦解既有的防護機制。

面對無完全防禦或阻擋措施的DDoS攻擊，除在事前作好防護準備作業，掌握近期常見攻擊手法，對相關資訊設備作好防護設定，並設計合宜的處置應變對策外，攻擊事件發生時，亦可透過分析/瞭解攻擊手法，針對攻擊特徵進行阻擋，達到減緩攻擊事件的目的。

## DDoS防護機制

如DDoS攻擊事件發生，業者除須具備應變能力外，亦須於事前對於常見DDoS攻擊手法具有防禦與備援機制，始能儘速減緩攻擊事件所造成的影響。透過檢視內部防護資源，依防護設備提供服務設定，建置多層次防護機制以增加DDoS之防護能量(詳見圖1)，例如：服務主機系統調校、防火牆DDoS防禦功能啟用及設置流量清洗等。然而攻擊流量若超過業者對外頻寬，導致系統/服務發生異常時，應協請網際網路服務提供者(Internet Service Provider, ISP)協助處理。

|  |
| --- |
|  |
| 行政院國家資通安全會報技術服務中心整理 |
| 1. DDoS多層次防護機制 |

## DDoS防禦與應變作業流程

參考美國國家標準與技術局(National Institute of Standards and Technology, NIST)所制定的資安事件應變程序生命週期(Incident Response Life Cycle)，規劃業者於面對DDoS攻擊之防禦與應變作業流程，業者可以此作業流程為基礎，發展業者之DDoS防禦與應變作業程序，以減緩攻擊事件對業者造成之衝擊。

DDoS防禦與應變作業流程(詳見圖2)分為「準備階段」、「偵測與分析階段」、「封鎖與根除階段」及「復原與事後處置階段」等4個階段，業者可依各階段工作項目作好DDoS防禦與應變作業：

* 準備階段

依業者現有資源進行系統/服務調校，並設置/申請相關防護設定與服務，以完備DDoS多層次防護機制。

* 偵測與分析階段

依準備階段所設置之安全防護設備進行網路監控，以即時發現攻擊事件，進行後續應變處置。

* 封鎖與根除階段

業者發現攻擊事件後，除應依「金融監督管理委員會證券期貨局所轄機關(構)資通安全通報作業要點」規範，進行資安事件通報外，依內部規劃之應變作業程序，緩解攻擊事件對業者造成的影響。攻擊流量超過業者對外頻寬，則應請ISP業者協助處理攻擊事件。

* 復原與事後處置階段

復原作業主要將因應攻擊事件所調整之資訊設備或網路設備相關設定復原，當確認DDoS攻擊已停止，即可評估恢復系統設定，或停用備援機制，以恢復系統業務正常運作。此外，應記錄事件處理過程，予以建檔管制，以利爾後備查使用，同時亦需針對DDoS攻擊事件所造成的影響進行評估，檢討網路安全措施或其他具體改善方案，必要時需修訂業者內部的應變計畫，以強化業者資通安全防護機制。

|  |
| --- |
|  |
| 1. DDoS防禦與應變作業流程 |

# 業者因應DDoS之防護作為

DDoS攻擊防禦與應變作業著重在事前準備作業，業者依內部網路架構與資源作好相關防護準備作業；攻擊事件發生時，即可透過事前準備的防護機制，採取應變措施以緩解攻擊事件對業者造成的影響；攻擊事件結束，需檢討各種軟硬體設備或資安防護設備不足之處，並提出建議改善方案，以提升業者整體資安防護能力。

## 事前準備

業者利用現有設備與資源，於事前規劃多層次防護架構，完成系統/服務之設定與申請，作好DDoS防禦準備，事前準備階段查核清單詳見附件1。

### 維護系統及網管人員/廠商聯繫資訊

除業者內部資訊人員聯繫資訊外，亦須維護相關系統及網管人員/廠商聯繫資訊，確保聯繫管道的暢通，當DDoS攻擊事件發生時，業者可快速依狀況聯絡所需之人員協助應處。「系統及網管人員/廠商聯繫表」詳見附件2。

### 調校系統/服務設定

服務主機應定期進行系統安全更新，避免遭駭客入侵利用外，同時可透過其他防護設備防止遭DDoS攻擊，針對其提供之服務進行安全防護設定，透過「連線數量」、「連線速率」、「通訊埠(Port)」及「主機防火牆」等限制/過濾流量方式，抵檔大量連線需求，以維持提供服務之主機的可用性，亦可避免遭利用造成主機本身成為或間接參與DDoS攻擊，而導致其網路頻寬耗損。附件3分別提供Apache(Linux Ubuntu 14.04)與IIS 7.5 (Windows Server 2008R2)網站服務主機、NTP服務主機及DNS服務主機之防護設定。

### 設置網路流量/系統資源監控機制

透過設置網路流量與系統資源監控流量監測等工具，即時監控網路及系統使用率外，亦可計算業者網路每日流量與使用量平均值，藉以定義網路流量與系統資源門檻值，確保業者能即時發現網路攻擊行為；另可定期檢視業者網路架構或狀態，並視情況進行調校，確實掌握業者網路流量與系統資源狀況。如業者內部無網路流量監測設備，可參考網路流量及系統資源監控軟體(Multi Router Traffic Grapher, MRTG)，MRTG軟體安裝設定方式詳見附件4。

### 啟用網路/防護設備DDoS防禦功能

一般的網路設備例如防火牆、交換器、路由器等，多有配置類似功能可協助防禦DDoS攻擊，以達到多層防護的效果(詳見圖3)。若業者發現開啟相關功能後造成系統效率不彰或使用者體驗不佳，可評估將此步驟移至「二、事中應變」執行。

|  |
| --- |
|  |
| 行政院國家資通安全會報技術服務中心整理 |
| 1. 網路設備DDoS防護示意圖 |

* 路由器(Router)

路由器與交換器功能雷同，以提供網路封包傳遞路徑為主，但仍可透過存取控制清單(Access Control List, ACL)減緩DDoS攻擊。

路由器多已提供入口過濾功能(Ingress Filtering)，然而此防護機制於提供大範圍網路服務的路由器設置時較有明顯成效，由於外部進入的封包來源IP不可能為內部位址，發現類此狀況表示封包可能已遭駭客竄改或偽造，即可針對此類型的封包加以過濾阻擋。目前國內部分ISP業者已於其網路設備啟用該功能，以禁止來源封包的IP為內部網路位址，防止IP造假之情形[4]。

* 入侵防禦系統(Intrusion Prevention System, IPS)

入侵防禦系統可針對具明顯特徵之攻擊進行阻擋，除可於遭DDoS攻擊時，依攻擊分析結果設置阻擋規則外，亦可將常見DDoS攻擊偵測特徵加入阻擋規則，以偵測/預防DDoS攻擊事件。

* 防火牆(Firewall)

防火牆可設定簡單規則來允許或阻擋特定通訊協定、Port及IP等，亦可阻擋攻擊來源，此外，於防火牆設置ACL，可緩解DDoS攻擊所造成的影響。目前大多數防火牆已配置DDoS防禦功能，可啟用相關的內建防禦功能，阻擋一般常見DDoS攻擊。

防火牆類型可分為狀態化(Stateful)與無狀態(Stateless)，狀態化防火牆會因設置的規則多寡影響防火牆檢查的速度，但可阻擋消耗系統資源類型的DDoS攻擊，因此業者可自行評估需求，採購適用之防火牆設備。

* 交換器(Switch)

交換器的功能為提供網路封包傳遞路徑，對於緩解DDoS攻擊的成效有限，但其提供的速率限制與ACL功能仍可減緩DDoS攻擊的影響。業者可視系統重要性，調整系統可使用之頻寬，確保當其他設備遭DDoS攻擊時，重要資訊設備仍可正常運作，同時亦可針對系統用途/功能，建立並設置其存取權限，避免遭消耗系統資源型態之攻擊。此外，部分交換器提供入口過濾功能(Ingress Filtering)，可過濾遭駭客所竄改或偽造之封包，阻擋部分DDoS攻擊來源。

* 網站應用程式防火牆(Web Application Firewall, WAF)

設置網站應用程式防火牆能辨識來自應用層服務的網路封包，以分析封包Header或驗證Cookie等方式，於到達受害資訊設備前，攔截非正常使用應用層服務之行為，亦可搭配負載平衡設備平均分攤網路流量，以維持資訊設備的正常運作。

* 應用程式遞送控制器(Application Delivery Controllers, ADC)

隨著網站安全防護的意識抬頭，一般伺服器處理日益複雜的加密憑證，可能會對其處理性能造成影響。藉由ADC的部署，可藉由目標伺服器的SSL流量卸載(SSL Offloading)功能，並搭配WAF或其他第三方資安設備對可疑連線進行阻擋，過濾完畢後，再將其重新加密並送至目標伺服器(詳見圖5)，期間目標伺服器不需要消耗資源，同時也可以減緩隱匿在加密安全連線中的攻擊行為[4][5][6]。

|  |
| --- |
|  |
| 行政院國家資通安全會報技術服務中心整理 |
| 1. ADC運作示意圖 |

### 申請/建置流量清洗服務

流量清洗(Cleaning Pipe)是一種由邊界閘道器協定(BGP)對路由進行廣播，將原本的攻擊流量導向流量清洗中心(Scrubbing Center)，藉由資安廠商自有的封包深度分析、連線特徵等技術來檢查、分析、過濾惡意封包之服務 。此時再把過濾後的流量導回原本對應的伺服器後，即便流量中仍有殘存的惡意攻擊封包，原本的防護設備應有足夠的能力來因應。

目前已有多家ISP與資安設備廠商提供流量清洗服務，業者可視網站流量需求採購所需服務項目，於事前提出申請，並支付月租費用，後續可視情況選購清洗流量。附件5以國內ISP業者為例，說明其服務費用、內容與申請流程。

### 申請內容傳遞網路(Content Delivery Network, CDN)服務

內容傳遞網路(CDN)目的是依照現有的網路架構，藉由內容分散式儲存、系統平衡負載、網路服務請求重導等功能，將網站的內容轉發至最接近用戶的網路節點，使用戶可就近取得服務的內容，解決單一服務主機因網路擁塞而造成服務效能不彰的狀況，進而在提高用戶訪問網站的回應速度、降低頻寬成本的同時，仍能維持服務品質。

當導入CDN服務的網頁伺服器主機遭受DDoS攻擊時，封包會導向最靠近攻擊者位址的服務主機，有助於稀釋攻擊封包流量。此外，透過CDN內部的DNS轉址與HTTP重導功能，可讓正常使用者轉接到負載較輕的其他服務主機，以維持網站服務的可用性。附件6以Cloudflare為例說明相關設定，該廠商目前提供免費無限制流量的CDN服務，惟僅限非子網域網站，且僅擷取靜態網頁(運作機制詳見圖6)。

|  |
| --- |
|  |
| 行政院國家資通安全會報技術服務中心整理 |
| 1. CDN傳遞路徑示意圖 |

### 建置/申請雲端備援

業者可評估透過雲端服務系統設置重要系統/服務之雲端備援機制，以確保攻擊事件發生時，重要系統/服務可持續對外提供服務。

惟採購雲端虛擬資源時，業者亦須規劃相關系統/服務資料庫同步方式，並確認雲端服務系統提供DDoS防禦機制。

## 事中應變

當DDoS攻擊事件發生時，除進行攻擊事件分析外，應以階段式方式逐一啟動防護機制，以維持系統/服務正常運作。事中應變階段查核清單詳見附件7。

### 攻擊事件通報

業者於發現攻擊事件後，應依「金融監督管理委員會證券期貨局所轄機關(構)資通安全通報作業要點」規範，至證券期貨市場資通安全通報系統(<https://sfevents.twse.com.tw>)執行通報作業，相關單位將視業者整體通報情況，進行後續處置。

### 攻擊事件分析

為能有效防禦DDoS攻擊，資訊人員應於攻擊事件發生時，蒐集並分析相關紀錄，以判斷DDoS攻擊類型，並依攻擊類型採取對應之防禦措施。

* 確認遭攻擊原因

攻擊者發動攻擊目的不同，其中涵蓋了政治立場、經濟利益或其他多樣化的意識形態，可透過網路平台相關管道，了解遭攻擊原因，勾勒攻擊事件全貌。

* 備份重要業務資料

由於在攻擊結束前，皆無法得知該次攻擊強度與攻擊持續時間，因此若遭受攻擊之設備存有重要業務資料時，建議即刻進行備份。

* 分析與阻擋攻擊來源IP

透過日誌保存機制蒐集相關攻擊紀錄，以分析攻擊來源IP，並透過網路防護設備(交換器、路由器、防火牆及IPS等)提供的存取控制功能進行初步的阻擋。

* 保留相關攻擊紀錄

保留相關日誌檔與側錄攻擊封包，可供日後資訊人員分析、判斷攻擊手法與特徵等，俾進一步提出相關防禦措施。

### 啟用流量清洗服務

如業者已購買流量清洗服務，可依相關流量清洗服務程序啟用服務，過濾大部分攻擊流量，以維持目標資訊設備正常運作。

### 啟用雲端備援

如業者已申請雲端虛擬資源，可啟用備援設備，並利用雲端系統的DDoS防禦機制，緩解攻擊流量，以維持系統/服務正常運作。

## 事後處置

事後處置階段大致可分為「復原作業」與「結案作業」等內容，當確認DDoS攻擊已停止，即可評估恢復系統設定，或停用備援機制，以恢復系統業務正常運作。此外，亦需記錄事件處理經過，檢討因DDoS攻擊事件所造成的影響進行評估，檢討網路安全措施或其他具體改善方案。事後處置階段查核清單詳見附件8。

### 復原資訊設備運作

資訊設備若於受到DDoS攻擊後已進行關機，抑或停止/限制提供部分網路服務(如變更部分設定檔)時，經過妥善處理後，應恢復其正常運作，若有啟用備援機制，建議一併進行運作，並持續觀察網路流量，確認DDoS攻擊已停止後，再行評估是否需停用備援機制。

### 持續監控網路流量

資訊人員均完成各項復原作業後，應持續監控網路流量，並觀察資訊設備運作情況，密切注意DDoS攻擊是否再度發生。

### 記錄事件處理過程

資訊人員需記錄整個事件發生過程與處理程序，包含攻擊原因及手法等資訊，同時記錄因應該次DDoS攻擊所採取之應變措施或解決方案，以及後續處理情形與追蹤事項，可提供未來發生類此事件時參考，有助於加速降低受DDoS攻擊後所造成的損害。

### 攻擊事件結報

攻擊事件結束後，業者應至證券期貨市場資通安全通報系統(<https://sfevents.twse.com.tw>)進行結案作業，提供事件處理過程與解決方案，以完成資安事件通報作業。

# 參考文獻

1. Mar 2016, Verisign DDoS Trends Report: Issue 4, 4th Quarter 2015. https://www.verisign.com/assets/report-ddos-trends-Q42015.pdf
2. June 2012, Response Rate Limiting in the Domain Name System (DNS RRL). Vernon Schryver and Paul Vixie. <http://www.redbarn.org/dns/ratelimits>
3. Aug 2012, Secure BIND Template. TEAM CYMRU. <http://www.cymru.com/Documents/secure-bind-template.html>
4. May 2000, Network Ingress Filtering:Defeating Denial of Service Attacks which employ IP Source Address Spoofing, The Internet Society. https://tools.ietf.org/html/bcp38
5. 2014年11月，從應用服務派送(ADC)確保持續的投資報酬率(ROI)。小枝逸人。http://www.runpc.com.tw/content/content.aspx?id=109840
6. Feb 2015, Using ADC's to Effectively Mitigate DDoS Attacks. http://www.informationweek.com/whitepaper/Security/Application-Security/mitigating-ddos-attacks-with-f5-technology-wp1360082510/118573?gset=yes

# 附件

1. 事前準備階段查核清單
2. 系統及網管人員/廠商聯繫表
3. 服務主機防護設定
4. 網路流量及系統資源監控軟體(MRTG)安裝設定
5. 國內ISP流量清洗申請服務說明
6. Cloudflare CDN服務申請與設定
7. 事中應變階段查核清單
8. 事後處置階段查核清單