各機關基於風險導向之弱點處置期限評估指引

115 年 11 月 6 日訂定

一、依據與目的

依資通安全責任等級分級辦法應辦事項，各機關辦理資通安全弱點管理，應於知悉資通安全弱點時，適時修補或採行緩解措施。又因應 AI 快速發展導致自動化攻擊與弱點武器化加速之趨勢，為協助各機關落實資通安全弱點管理，採取基於風險導向之弱點處置策略，有效確保機關整體資通安全，特訂定本指引。

二、適用對象

（一）依資通安全管理法第 3 條第 5 款、第 6 款規定之公務機關、特定非公務機關。

（二）特定非公務機關之中央目的事業主管機關就弱點處置期限認有另為規定之必要者，得自行訂定弱點處置期限，依其規定辦理。

三、名詞定義

本指引所稱弱點處置，包含執行安全性更新、關閉有弱點的服務或功能、停用資訊資產、進行網路隔離，或其他為降低風險至機關可接受程度所採行的各項弱點緩解或補償性控制措施。

四、弱點處置期限評估指標及評估流程

各機關應依下列評估指標判斷各項資訊資產弱點處置期限：

（一）資訊資產曝露於公眾網路情形：指該資訊資產得由未經授權或不被信任之實體，透過網際網路等公眾網路直接存取者。

（二）弱點已知被利用：指該弱點已由美國網路安全暨基礎設施安全局（Cybersecurity and Infrastructure Security Agency, CISA）列入所維護的「已知被利用之弱點（Known Exploited Vulnerabilities, KEV）清單」。

（三）弱點能否被自動化利用：指攻擊者能否穩定地以自動化方式完成網路狙殺鏈（Cyber Kill Chain）的偵察（Reconnaissance）、武器化

（Weaponization）、傳遞（Delivery）及利用（Exploitation）等階段。

（四）弱點遭利用後對資訊資產之技術影響程度：指弱點遭利用後，對機關資訊資產所造成的影響，包括完全控制及部分控制。

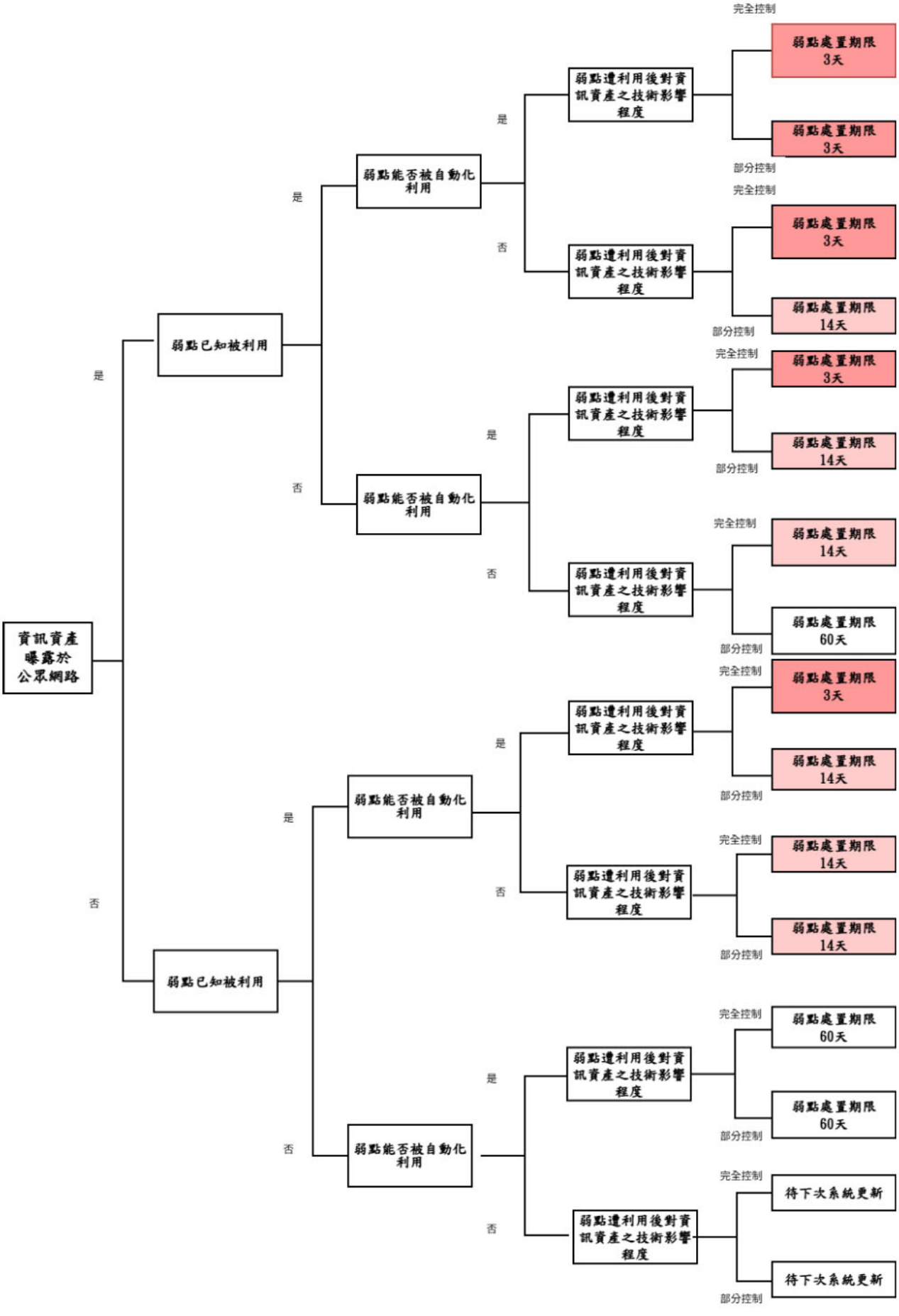
1. 完全控制（Total impact）：指攻擊者可取得遭駭資訊資產的完全控制權，或該資訊資產之全部資訊可被完全揭露。

2. 部分控制(Partial impact)：指攻擊者僅可有限度地控制遭駭資訊資產，或該資訊資產之部分資訊被有限度地揭露。

進行弱點處置期限評估時，應考量評估指標形成的風險，以鑑定為類型1~16，據以對應弱點處置期限。各類型要件請見表一，評估流程請見圖一。但數位發展部資通安全署或國家資通安全研究院就特定弱點因整體性風險另指定處置期限者，從其規定。

表一：弱點處置期限評估表

評估指標/類型	評估指標				弱點處置期限
	1. 資訊資產曝露於公眾網路情形	2. 弱點已知被利用	3. 弱點能否被自動化利用	4. 弱點遭利用後對資訊資產之技術影響程度	
1	是	是	是	完全控制	3 天
2	是	是	是	部分控制	3 天
3	是	是	否	完全控制	3 天
4	是	是	否	部分控制	14 天
5	是	否	是	完全控制	3 天
6	是	否	是	部分控制	14 天
7	是	否	否	完全控制	14 天
8	是	否	否	部分控制	60 天
9	否	是	是	完全控制	3 天
10	否	是	是	部分控制	14 天
11	否	是	否	完全控制	14 天
12	否	是	否	部分控制	14 天
13	否	否	是	完全控制	60 天
14	否	否	是	部分控制	60 天
15	否	否	否	完全控制	待下次系統更新
16	否	否	否	部分控制	待下次系統更新



圖一：弱點處置期限評估流程圖

五、弱點處置期限評估結果處理

（一）弱點處置期限，係以知悉日起算並以日曆天計之。

（二）各機關應訂定弱點處置之內部評估程序，其中弱點處置期限原則應依表一、圖一所示流程定之；惟例外時，機關得依下列個案情形衡酌營運衝擊，經資訊（安）主管核准後自訂處置期限，並留存紀錄備查。

1.考量機關系統維運環境差異，因業務需求且有其他適當資安防護措施者，或經風險評估該弱點對機關影響程度有限。

2.評估程序中，如無前揭評估指標可供依循。

（三）針對表一評估類型 1、2、3、9，各機關應先評估受影響範圍，保存與檢視相關日誌紀錄，並監控不尋常或未經授權之活動，確認該弱點是否已遭利用。

（四）弱點處置期限應進行動態調整，依表一、圖一評估事實與條件異動情形重新評估，以展延或縮短處置期限。

（五）弱點經評估歸類於同一處置期限，各機關得依其弱點遭利用後對資訊資產之技術影響程度、弱點嚴重程度指標（Common Vulnerability Scoring System, CVSS）分數、漏洞利用預測評分系統（Exploit Prediction Scoring System, EPSS）分數或其他弱點評估指標進行處置優先排序。

六、弱點緩解或補償性控制措施建議

弱點無法立即修補或及時處置時，機關應依弱點內容、資訊資產特性及環境，評估採取下列或其他為降低風險至機關可接受程度所採行的各項弱點緩解或補償性控制措施。

（一）停用資訊資產：將受影響或無法修補之系統或設備進行淘汰、停用或報廢。

（二）移除易受攻擊的軟體：針對產生弱點之特定非核心軟體或元件，執行解除安裝或完全移除。

（三）劃分網段：透過切分實體或虛擬網段，將具有弱點之資訊資產限縮在特定且受嚴格控管的安全網段內，防範橫向移動攻擊。

（四）進行網路隔離：完全切斷或嚴格限制受影響資訊資產與內部網路、外部或公眾網路的實體及邏輯連線。

（五）強化存取控制：導入零信任架構，至少經身分鑑別、設備鑑別機制確認後，方得存取指定之資訊資產。

（六）建置代理伺服器過濾防護：架設專屬代理伺服器作為存取中介，實施流量監控，用以過濾、阻擋或清洗針對受影響資訊資產之異常連線與攻擊特徵。

（七）實施虛擬修補（Virtual Patching）：透過應用程式防火牆、入侵防禦系統（Intrusion Prevention System, IPS）等資安防護措施或設備，偵測並阻擋符合已知弱點利用特徵的攻擊行為。

七、其他事項

各機關應配合本指引說明，納入機關資訊安全管理系統（Information Security Management System, ISMS）相關程序規範辦理。