新光醫療財團法人
新光吳火獅紀念醫院
SHIN KONG WU HO-SU MEMORIAL HOSPITAL

新光吳火獅紀念醫院

資通安全風險評鑑程序書

－僅限本院同仁參閱－

新光醫療財團法人新光吳火獅紀念醫院

文 件 名 稱：資通安全風險評鑑程序書

文 件 編 號：ISMS-2-05

制 定 單 位：資訊部

制 定 日 期：114 年 05 月 26 日

修 訂 紀 錄			
修訂日期	修訂內容摘要	頁次	版本
98.09.01	初版		1.0
100.08.05	附錄 D 威脅發生次數應納入事件嚴重度等客觀評分		1.1
111.02.08	修訂風險值計算方式		1.2
112.04.17	依組織名稱、架構及職責修訂相關內容	全	1.3
114.05.26	因應 ISO27001:2022 轉版，相關內容改版		3.0

新光醫療財團法人新光吳火獅醫院

文件編號	ISMS-2-05	文件名稱	機密等級	版本	3.0
制訂單位	資訊部	資通安全風險評鑑程序書	內部使用	頁數	1/27

1 目的：

建立資通資產風險評鑑標準，以鑑別資通資產之弱點及威脅而導致之風險，並依據評鑑結果採取對策或控制措施，降低資通資產遭受損害的風險。

2 依據：

2.1 ISO 27001。

2.2 ISO 31000。

2.3 行政院國家資通安全會報頒訂之「資訊系統分類分級與鑑別機制參考手冊」。

2.4 ISMS-1-01_資通安全政策。

3 範圍：

3.1 資產風險評鑑：以驗證範圍內資訊資產為評鑑對象。

4 定義

4.1 權責

4.1.1 資通安全管理委員會

4.1.1.1 依據「風險評鑑報告」決定可接受風險等級。

4.1.1.2 審查「風險處理計畫」及確認執行成效。

4.1.1.3 決定風險評鑑之時機與範圍。

4.1.2 資通安全資安組

4.1.2.1 建立並維護系統化之風險評鑑方法。

4.1.2.2 監督風險評鑑之執行。

4.1.2.3 彙總「風險評鑑報告」，提報資通安全管理委員會。

4.1.2.4 彙總「風險處理計畫」，提報資通安全管理委員會。

4.1.3 資通資產管理者

4.1.3.1 執行風險評鑑作業。

4.1.3.2 擬訂「風險評鑑報告」。

4.1.3.3 擬訂「風險處理計畫」並執行。

4.1.3.4 管理與維護「資通資產清冊」。

4.2 風險（Risk）

威脅會利用資產的弱點造成資產的損失或損壞的潛在可能性。

4.3 威脅（Threat）

資通資產所面臨的事故，可能會對系統或組織及其資產造成傷害，威脅必須利用資產的弱點才能對資產造成傷害。

4.4 弱點（Vulnerability）

指單一或一系列會讓威脅有機可趁而造成資產損害的狀況。資產的脆弱點本身並不會造成傷害。

4.5 風險管理（Risk management）

以可接受的成本，對可能影響資訊資產的安全風險進行鑑別、控制及降低或排除的過程。包含風險評鑑與風險處理。

4.6 風險評鑑（Risk assessment）

對資通資產及資訊處理設施的威脅、衝擊及弱點及其發生可能性的評鑑。

4.7 風險處理（Risk treatment）

選擇與實施各項控制措施，以修正風險的過程。

4.8 資產價值（資產鑑價 C、I、A）

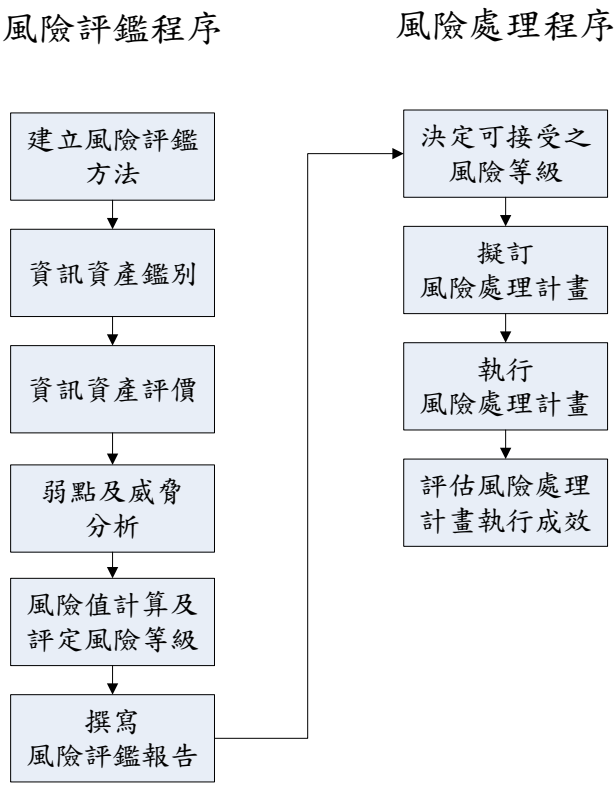
4.8.1 機密性（Confidentiality，簡稱 C）：確保只有經過授權的人才能存取資訊。

4.8.2 完整性（Integrity，簡稱 I）：保護資訊及其處理方法的準確性和完整性。

4.8.3 可用性（Availability，簡稱 A）：確保經過授權的用戶在需要時可以存取資訊並使用相關資訊資產。

5 作業內容

所謂風險管理即為包含「風險評鑑程序」及「風險處理程序」之資通資產風險控管程序，主要作業項目如下圖，並於以下各節說明。



5.1 風險評鑑程序

5.1.1 風險評鑑時機

風險評鑑作業應每年定期執行，並由資通安全資安組決定執行時機與範圍。除每年定期執行外，亦應於下列情形發生時，針對變動範圍內的作業程序與資通資產進行風險評鑑：

5.1.1.1 營運組織變更

5.1.1.2 作業流程重大改變

5.1.1.3 重要資通資產新增或變更

5.1.1.4 發生重大資訊安全事件

5.1.2 風險評鑑人員之要求

5.1.2.1 風險評鑑人員需由資通安全管理委員會主任委員，指派接受相關訓練者擔任。

5.1.2.2 風險評鑑人員應有效執行風險評鑑方法。

5.1.2.3 製作風險評鑑報告，並依照「ISMS-2-04-2_風險處理計畫表」之格式製作風險處理計畫。

5.1.2.4 風險評鑑人員之資格鑑定：風險評鑑報告及「ISMS-2-04-2_風險處理計畫

表」需於管審會議中審查，以鑑定人員風險評鑑能力及資格之適用。

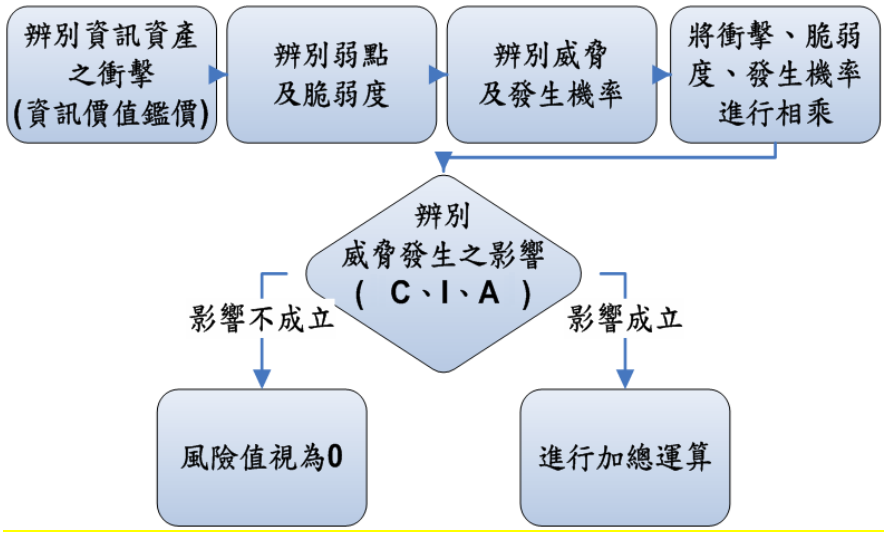
5.1.3 風險評鑑方法

5.1.3.1 風險評鑑因素

風險評鑑為計算資訊資產風險值之程序，用以決定風險處理之優先順序。資訊資產風險值是以其機密性、完整性、可用性等三項因子構成之資訊資產價值，以及所面臨之弱點脆弱度與威脅發生機率決定。

5.1.3.2 風險值計算流程

根據風險評鑑表格進行資訊資產評價，識別弱點之脆弱度、威脅之發生機率，將此三項評分進行相乘，即求出該資訊資產之風險值。



5.1.4 資訊資產鑑別

資通安全資安組依據「ISMS-2-05 資訊資產管理程序書」之作業說明，執行資訊資產鑑別作業，並建立「ISMS-2-04_資通安全風險評鑑程序書」。建立資訊資產清冊之作業方式詳見「ISMS-2-05_資通資產管理程序書」。

5.1.5 資訊資產評價

資訊資產管理者須針對各項資訊資產之機密性、完整性、可用性等三項資訊資產價值因子進行資訊資產評價。各因子評價標準詳見「附錄 A 資訊資產評價」。

5.1.6 弱點及威脅分析

5.1.6.1 資訊資產管理者須針對各項資訊資產之使用及管理現狀，識別資訊資產所面臨之內部弱點及外在威脅，並分析其脆弱度與發生機率。

5.1.6.2 資訊資產弱點之識別參考「附錄 B 資訊資產弱點、威脅與衝擊對應表」內之對應關係，列出各項資訊資產可能之弱點。

5.1.6.3 資訊資產威脅之識別應參考「附錄 B 資訊資產弱點、威脅與衝擊對應表」內之對應關係，列出各項資訊資產弱點所存在之可能威脅。

5.1.6.4 參考「附錄 B 資訊資產弱點、威脅與衝擊對應表」，鑑別各項威脅對資訊資產所造成之機密性、完整性、可用性之衝擊。

5.1.7 風險值計算

風險值因子	代號
資產價值之機密性	C
資產價值之完整性	I
資產價值之可用性	A
弱點脆弱度	VV
威脅發生機率	TR
資訊資產價值	AV

■資訊資產風險值(RV)＝資產價值(AV)x 弱點脆弱度(VV)x 威脅發生機率(TR)

5.1.8 撰寫風險評鑑報告

資通安全資安組依據風險評鑑結果撰寫「風險評鑑報告」，並分析資訊資產安全需求，提出可接受之風險等級建議，提報資通安全管理委員會審查及決定可接受之風險等級。

5.2 風險處理程序

5.2.1 可接受風險等級之決定

5.2.1.1 資通安全管理委員會應審查風險評鑑報告，並針對所提出之風險等級建議，決定可接受之風險等級。

5.2.1.2 可接受風險等級之決定因素：

5.2.1.2.1風險嚴重（衝擊）程度

5.2.1.2.2風險處理急迫性

5.2.1.2.3可分配之資源

5.2.1.3 為確保未遺漏需處理之資訊資產風險，除決定可接受風險等級外，亦應訂定風險處理之補償條件，於此補償條件中篩選需執行風險處理之資訊資產項目。

5.2.2 擬訂風險處理計畫

5.2.2.1 依風險評鑑結果及可接受風險等級之決議，由資通安全資安組針對需降低風險等級之資訊資產擬訂風險處理計畫，以期將風險降至可接受之程度。

5.2.2.2 風險處理計畫應依據「ISMS-2-04-2_風險處理計畫表」之格式撰寫。

5.2.2.3 風險處理計畫之風險處理措施，應根據 ISO27001 對各項資訊安全之要求目標，擬訂適當之處理措施及相關執行資源之資訊。

5.2.2.4 風險處理計畫應提報資通安全管理委員會審查後執行。

5.2.3 執行風險處理計畫

應依據風險處理計畫之風險處理項目、所需資源、預訂完成日期等規劃，執行各項風險控制措施，並將執行進度紀錄於「ISMS-2-04-2_風險處理計畫表」。

5.2.4 評估風險處理計畫執行成效

5.2.4.1 風險處理計畫於預訂完成日期結束後，須由資通安全資安組針對進行風險處理之資訊資產，依本說明書之風險評鑑程序實施風險重新評鑑，以確認風險處理計畫之執行能達到減緩風險，並將風險重新評鑑之結果提報資通安全管理委員會。

5.2.4.2 若經風險重新評鑑後，資訊資產之風險值未達預期效益，亦即仍處於不可接受之風險等級，資通安全資安組則需依本說明書之風險處理程序進行風險再處理作業或接受該項風險。

6 實施與修訂

本程序書奉 資通安全委員會副主任委員核定後實施，修正時亦同。

7 輸出文件/紀錄

ISMS-2-04-1 資通資產清冊與風險評鑑

ISMS-2-04-2 風險處理計畫表

附錄A、資訊資產評價

A.1、評價標準

- 4-影響程度「極高」。
- 3-影響程度「高」。
- 2-影響程度「中」。
- 1-影響程度「低」。
- 0-不適用。

A.2、資訊資產評價標準定義

文件類資訊資產價值評分標準			
風險標準	**C (機密性)**	**I (完整性)**	**A (可用性)**
定義說明	著重於保護資產，確保只有獲得授權的人才能存取該資產	著重於確保資料的正確性及資產(作業)處理的完整性，以避免因運用錯誤的資料或因資產處理的不完全，而造成對組織的衝擊	確保資產提供使用者所需的服務，以達成預期之功能，主要為避免因災害而致使組織無法持續運作或提供服務之衝擊
(4)極高	■ 資產內資料屬於**密** ■ 資料內容若洩漏會**大多數客戶權益** ■ 組織**需立即採取補救措施** ■ 資訊、資料存取權限須經由**權責主管或代理人**核准同意者 ■ 可對應至文件分級或資訊資產分級之"**密**"等級	■ 資產內資料若不完整，將導致**全組織作業受創** ■ **影響大多數客戶權益**。 ■ 需立即通報**主管機關、警政單位或權責主管(代理人)**，並啟動應變機制	■ 作業**完全仰賴**資訊資產，且一旦資訊遺失或損毀時將**影響全組織**對外提供服務作業
(3)高	■ 資產內資料屬於**密** ■ 資料內容若洩漏會**影響組織聲譽及客戶權益** ■ 組織**需採取補救措施** ■ 資訊、資料存取權限須經由**權責主管或代理人**核准同意者 ■ 可對應至文件分級或資訊資產分級之"**密**"等級	■ 資產內資料若不完整，將導致**組織部分作業受影響** ■ 造成**少數客戶**權益受損 ■ 需通報**權責主管或代理人**，並採取補救措施	■ 作業**高度仰賴**資訊資產，且一旦資訊遺失或損毀時將**影響組織內跨部門**作業
(2)中	■ 資產內資料僅供**內部使用** ■ 資料內容若洩漏會對組織造成**有形或無形的損害**，此**損害**為組織**可承受之範圍** ■ 資訊、資料存取權限須經由**單位主管或代理人**核准同意 ■ 可對應至文件分級或資訊資產分級之"內部使用"	■ 資產內資料若不完整，將造成**部門作業受影響** ■ 造成**個人**權益受損 ■ 需通報**單位主管或代理人**，損害為組織**可承受之範圍**	■ 作業**仰賴**資訊資產，且一旦資訊遺失或損毀時將**影響部門作業**

文件類資訊資產價值評分標準			
風險標準	**C (機密性)**	**I (完整性)**	**A (可用性)**
(1) 低	■ 資產內為**一般性資料，但須遵守相關發佈流程** ■ 若流傳至組織以外，**不會**對組織**造成**任何有形或無形的**傷害**(註 1) ■ 資訊、資料存取權限只須經由**資產管理者或承辦人**同意者 ■ 可對應至文件分級或資訊資產分級之"**公開資訊**"等級	■ 資產內資料若不完整，將造成**少數或個別承辦人作業受影響** ■ 不對服務對象造成影響，最多是承辦人**重覆作業工作** ■ 不需通報，**資產管理者或承辦人**可自行處理	■ 作業**仰賴**資訊資產，且一旦資訊遺失或損毀時將**影響少數承辦人**作業
註 1：有形的傷害如：財務上的賠償、主管機關的懲處； 無形的傷害如：形象上的受損、組織內部員工士氣的低落。			

硬體類、建築與保護類及服務類資訊資產價值評分標準			
風險標準	**C (機密性)**	**I (完整性)**	**A (可用性)**
定義說明	著重於保護資產，確保只有獲得授權的人才能存取該資產	著重於確保資料的正確性及資產(作業)處理的完整性，以避免因運用錯誤的資料或因資產處理的不完全，而造成對組織的衝擊	確保資產提供使用者所需的服務，以達成預期之功能，主要為避免因災害而致使組織無法持續運作或提供服務之衝擊
(4) 極高	設備設定或內容若洩漏會影響組織重大權益 若遭有心人士所用將造成組織財務極大損失 組織需立即採取補救措施	設備或設定若不完整，將導致全組織作業受創 影響大多數使用者權益。 需立即通報主管機關、權責主管(代理人)，並啟動應變機制	■ 可忍受服務中斷時間：**12小時內** ■ 作業**完全仰賴**資訊資產，且一旦服務中斷時將**影響全組織**對外提供服務作業
(3) 高	設備設定或內容若洩漏會影響組織財務部分權益 若遭有心人士所用將造成財務損失 組織需採取補救措施	設備或設定若不完整，將導致組織部分作業受影響 造成少數使用者權益受損 需通報權責主管或代理人，並採取補救措施	■ 可忍受服務中斷時間：**12~24小時** ■ 作業**高度仰賴**資訊資產，且一旦服務中斷時將**影響組織內跨部門**作業
(2) 中	設備設定或內容若洩漏會對組織造成有形或無形的損害，此損害為組織可承受之範圍	設備或設定若不完整，將造成部門作業受影響 造成個人權益受損 需通報單位主管或代理人，損害為組織可承受之範圍	■ 可忍受服務中斷時間：**24~48小時** ■ 作業**仰賴**資訊資產，且一旦服務中斷時將**影響部門作業**
(1) 低	設備設定或內容若流傳至組織以外，不會對組織造成任何有形或無形的傷害(註 1)	設備或設定若不完整，將造成少數或個別承辦人作業受影響 不對服務對象造成影響，最多是承辦人重覆作業工作	■ 可忍受服務中斷時間：**48小時以上** ■ 作業**仰賴**資訊資產，且一旦服務中斷時將**影響少數承辦人**作業

軟體類資訊資產價值評分標準

風險標準	C (機密性)	I (完整性)	A (可用性)
定義說明	著重於保護資產，確保只有獲得授權的人才能存取該資產	著重於確保資料的正確性及資產(作業)處理的完整性，以避免因運用錯誤的資料或因資產處理的不完全，而造成對組織的衝擊	確保資產提供使用者所需的服務，以達成預期之功能，主要為避免因災害而致使組織無法持續運作或提供服務之衝擊
(4) 極高	■ 軟體/程式邏輯若洩漏會**影響組織重大權益** ■ 若遭有心人士所用將**造成組織財務極大損失** ■ 組織**需立即採取補救措施**	■ 軟體若不完整，將導致**全組織作業受創** ■ **影響大多數使用者權益**。 ■ 需立即通報**主管機關、權責主管(代理人)**，並啟動應變機制	■ 可忍受服務中斷時間：**5 分鐘內** ■ 作業**完全仰賴**資訊資產，且一旦服務中斷時將**影響全組織**對外提供服務作業
(3) 高	■ 軟體/程式邏輯若洩漏會**影響組織財務部分權益** ■ 若遭有心人士所用將**造成財務損失** ■ 組織**需採取補救措施**	■ 軟體若不完整，將導致**組織部分作業受影響** ■ 造成**少數使用者**權益受損 ■ 需通報**權責主管或代理人**，並採取補救措施	■ 可忍受服務中斷時間：**5 分鐘以上 ~1 小時** ■ 作業**高度仰賴**資訊資產，且一旦服務中斷時將**影響組織內跨部門**作業
(2) 中	■ 軟體/程式邏輯若洩漏會對組織造成**有形或無形的損害，此損害**為組織**可承受之範圍**	■ 軟體若不完整，將造成**部門作業受影響** ■ 造成**個人**權益受損 ■ 需通報**單位主管或代理人**，損害為組織**可承受之範圍**	■ 可忍受服務中斷時間：**1 ~12 小時** ■ 作業**仰賴**資訊資產，且一旦服務中斷時將**影響部門作業**
(1) 低	■ 軟體/程式邏輯若流傳至組織以外，**不會**對組織**造成**任何有形或無形的**傷害**(註 1)	■ 軟體若不完整，將造成**少數或個別承辦人作業受影響** ■ 不對服務對象造成影響，最多是承辦人**重覆作業工作** ■ 不需通報，**資產管理者或承辦人**可自行處理	■ 可忍受服務中斷時間：**12 小時以上** ■ 作業**仰賴**資訊資產，且一旦服務中斷時將**影響少數承辦人**作業

註 1：有形的傷害如：財務上的賠償、主管機關的懲處；
無形的傷害如：形象上的受損、組織內部員工士氣的低落。

人員類資訊資產價值評分標準			
風險標準	**C (機密性)**	**I (完整性)**	**A (可用性)**
定義說明	著重於保護資產，確保只有獲得授權的人才能存取該資產	著重於確保資料的正確性及資產(作業)處理的完整性，以避免因運用錯誤的資料或因資產處理的不完全，而造成對組織的衝擊	確保資產提供使用者所需的服務，以達成預期之功能，主要為避免因災害而致使組織無法持續運作或提供服務之衝擊
(4) 極高	■ 人員所接觸之資料內容屬於**密** ■ 資料內容若洩漏會**影響大多數客戶權益**	■ 適任性極高 ■ 極高度符合工作執掌需求	■ 作業**完全仰賴**該員，且一旦該員無法作業時，將**影響全組織**對外提供服務作業
(3) 高	■ 人員所接觸之資料內容屬於**密** ■ 資料內容若洩漏會嚴重**影響組織聲譽及客戶權益**	■ 適任性高 ■ 高度符合工作職掌需求	■ 作業**高度仰賴**該員，且一旦該員無法作業時，將**影響組織內跨部門**作業
(2) 中	■ 人員所接觸之資料內容僅供**內部使用** ■ 資料內容若洩漏會對組織造成**有形或無形的損害**，此損害為組織**可承受**之範圍	■ 適任性中 ■ 符合工作職掌需求	■ 作業**仰賴**該員，且一旦該員無法作業時，將**影響部門**作業
(1) 低	■ 人員所接觸之資料為**一般性資料**，但須遵守相關發佈流程 ■ 若流傳至組織以外，不會對組織造成任何有形或無形的傷害(註 1)	■ 適任性低	■ 作業**仰賴**該員，且一旦該員無法作業時，將**影響少數承辦人**作業，但或許是可暫時人工作業、或可暫時替代
註 1：有形的傷害如：財務上的賠償、主管機關的懲處； 無形的傷害如：形象上的受損、組織內部員工士氣的低落。			

附錄B、資訊資產弱點、威脅與衝擊對應表

大類	小類	弱點	威脅	C	I	A
人員類	全類	人員短缺	人員短缺	0	0	1
		不足的安全訓練	操作人員的錯誤	0	0	1
		不當使用軟體及(或)硬體	操作人員的錯誤	0	0	1
			非法輸出/入軟體	1	1	1
		不當的招募程序	罷工	1	1	1
			偷竊	1	1	1
			惡意損毀	1	1	1
		缺乏安全的認知(awareness)	使用者錯誤	1	1	1
		缺乏文件(管理作業程序)	操作人員的錯誤	1	1	1

大類	小類	弱點	威脅	C	I	A
文件類	全類	未控制複製	偷竊	1	1	1
			未授權即使用媒體	1	1	1
		廢棄物處理疏於照管	偷竊	1	1	1
		缺乏安全的認知(awareness)	使用者錯誤	1	1	1
		不足的安全訓練	操作人員的錯誤	1	1	1
		缺乏有效的建構變更控制	操作人員的錯誤	1	1	1
		缺乏備援拷貝	火災	0	0	1
			水災土石流	0	0	1

大類	小類	弱點	威脅	C	I	A
服務類	全類	不足的安全訓練	操作者錯誤	1	1	1
		不當使用軟體及(或)硬體	操作者錯誤	1	1	1
		不當的招募程序	偷竊	1	0	0
			惡意損毀	0	1	1
		不當的服務維護回應	硬體故障	0	1	1
			電力供應故障	0	1	1
		缺乏安全的認知(awareness)	使用者錯誤	1	1	1

大類	小類	弱點	威脅	C	I	A
建築與保護類	一般辦公區域	不當的服務維護回應	水供應故障	0	0	1
			空調故障	0	0	1
			硬體故障	0	1	1
			電力供應故障	0	0	1
		未監督外來人員或清潔人員之工作	偷竊	1	1	1
		建築或房間不當或疏於使用實體進出管制	偷竊	1	1	1
			惡意損毀	1	1	1
			資源的不正確使用	1	1	1
		缺乏門禁管制	偷竊	1	1	1
		位處易有水患之地	水災土石流	0	1	1
	特殊辦公區域	位處易有水患之地	水災土石流	0	1	1
		不當的服務維護回應	水供應故障	0	0	1
			空調故障	0	0	1
			硬體故障	0	1	1
			電力供應故障	0	0	1
		未監督外來人員或清潔人員之工作	偷竊	1	1	1
		建築或房間不當或疏於使用實體進出管制	偷竊	1	1	1
			惡意損毀	1	1	1
			資源的不正確使用	1	1	1
		缺乏門禁管制	偷竊	1	1	1
	資訊機房、檔案室區域	位處易有水患之地	水災土石流	0	1	1
		不當的服務維護回應	水供應故障	0	0	1
			空調故障	0	0	1
			硬體故障	0	1	1
			電力供應故障	0	0	1
		未監督外來人員或清潔人員之工作	偷竊	1	1	1
		建築或房間不當或疏於使用實體進出管制	偷竊	1	1	1
			惡意損毀	1	1	1
			資源的不正確使用	1	1	1
		缺乏門禁管制	偷竊	1	1	1
		缺乏備援拷貝	水災土石流	0	1	1
			火災	0	1	1
			惡意損毀	0	1	1
		對溫度變化敏感	空調故障	0	0	1
			溫度與濕度超過限值	0	0	1

大類	小類	弱點	威脅	C	I	A
	倉庫(庫房)	不當的服務維護回應	水供應故障	0	0	1
			空調故障	0	0	1
			硬體故障	0	1	1
			電力供應故障	0	0	1
		未監督外來人員或清潔人員之工作	偷竊	1	1	1
		位處易有水患之地	水災土石流	0	1	1
		建築或房間不當或疏於使用實體進出管制	偷竊	1	1	1
			惡意損毀	1	1	1
			資源的不正確使用	1	1	1
	建築保護設施(火偵測、熱偵測、水偵測系統、滅火系統、溫濕度計)	位處易有水患之地	水災土石流	0	1	1
		不足的維護或安裝的錯誤	地震	0	0	1
			維護錯誤	0	1	1
			儲存媒體變質	0	1	1
		不當的服務維護回應	水供應故障	0	0	1
			空調故障	0	0	1
			硬體故障	0	1	1
			電力供應故障	0	0	1
		未監督外來人員或清潔人員之工作	偷竊	1	1	1
		建築或房間不當或疏於使用實體進出管制	偷竊	1	1	1
			惡意損毀	1	1	1
			資源的不正確使用	1	1	1
		缺乏監控(monitoring)機制	以非授權的方式使用軟體	1	0	1
			以非授權的方式使用網路設施	1	0	1
			非法使用軟體	1	1	1
			非法輸出/入軟體	1	0	1
			溫度與濕度超過限值	0	1	1
		對溫度變化敏感	空調故障	0	0	1
			溫度與濕度超過限值	0	0	1
		對電壓變化敏感	電壓不穩定	0	0	1

大類	小類	弱點	威脅	C	I	A
軟體類	OA 系統	缺乏備援拷貝	惡意軟體	1	1	1
		缺乏有效變更控制	操作人員的錯誤	0	1	1
			使用者的錯誤	0	0	1
		繁複的使用者介面	操作人員的錯誤	0	1	1
			使用者的錯誤	0	1	1
		不當的服務維護回應	空調故障	0	0	1
			電力供應故障/停水	0	0	1
			硬體故障	0	0	1
			軟體故障	0	1	1
		缺乏稽核軌跡	未經授權的使用	1	0	0
		缺乏識別及鑑別機制(如使用者鑑別)	假冒使用者身分	1	0	0
		缺乏發送端與接收端識別及鑑別機制	未經授權的使用	1	0	0
			偷竊	1	0	0
		離開工作站沒有登出(Logout)	未經授權的使用	1	0	0
		沒有或不足的軟體測試	軟體故障	0	1	1
		不良的通行碼(password)管理	假冒使用者身分	1	0	0
		通行碼以明碼傳送	未經授權的使用	1	0	0
		不明確或不完整的開發規格	軟體故障	0	1	1
		軟體的已知缺陷	非法輸出/入軟體	1	1	0
			惡意的軟體	0	1	1
			軟體故障	0	1	1
	資訊安全系統	缺乏備援拷貝	惡意軟體	1	1	1
		缺乏有效變更控制	操作人員的錯誤	0	1	1
			使用者的錯誤	0	0	1
		繁複的使用者介面	操作人員的錯誤	0	1	1
			使用者的錯誤	0	1	1
		不當的服務維護回應	空調故障	0	0	1
			電力供應故障/停水	0	0	1
			硬體故障	0	0	1
			軟體故障	0	1	1
		缺乏稽核軌跡	未經授權的使用	1	0	0
		缺乏有效的建構變更控制	使用者的錯誤	0	1	1
			操作人員的錯誤	0	1	1
			軟體故障	0	1	1
		缺乏識別及鑑別機制(如	假冒使用者身分	1	0	0

大類	小類	弱點	威脅	C	I	A
		使用者鑑別)				
		缺乏發送端與接收端識別及鑑別機制	未經授權的使用	1	0	0
			偷竊	1	0	0
		離開工作站沒有登出(Logout)	未經授權的使用	1	0	0
		沒有或不足的軟體測試	軟體故障	0	1	1
		不良的通行碼(password)管理	假冒使用者身分	1	0	0
		通行碼以明碼傳送	未經授權的使用	1	0	0
		不明確或不完整的開發規格	軟體故障	0	1	1
		軟體的已知缺陷	非法輸出/入軟體	1	1	0
			惡意的軟體	0	1	1
			軟體故障	0	1	1
	作業系統	缺乏稽核軌跡	未經授權的使用	1	0	0
		缺乏備援拷貝	惡意軟體	0	0	1
		缺乏有效的建構變更控制	操作人員的錯誤	1	1	1
			使用者的錯誤	0	1	1
			軟體故障	0	1	1
		缺乏識別及鑑別機制(如使用者鑑別)	假冒使用者身分	1	0	0
		離開工作站沒有登出(Logout)	未經授權的使用	1	0	0
		沒有或不足的軟體測試	軟體故障	0	1	1
		不良的通行碼(password)管理	未經授權的使用	1	0	0
			假冒使用者身分	1	0	0
		通行碼以明碼傳送	未經授權的使用	1	0	0
		軟體的已知缺陷	非法輸出/入軟體	1	1	0
			惡意軟體	1	1	0
			軟體故障	0	1	1
	應用系統	缺乏備援拷貝	惡意軟體	1	1	1
		缺乏有效變更控制	操作人員的錯誤	0	1	1
			使用者的錯誤	0	0	1
		繁複的使用者介面	操作人員的錯誤	0	1	1
			使用者的錯誤	0	1	1
		不當的服務維護回應	空調故障	0	0	1
			電力供應故障/停水	0	0	1
			硬體故障	0	0	1
			軟體故障	0	1	1

大類	小類	弱點	威脅	C	I	A
		缺乏稽核軌跡	未經授權的使用	1	0	0
		缺乏有效的建構變更控制	使用者的錯誤	0	1	1
			操作人員的錯誤	0	1	1
			軟體故障	0	1	1
		缺乏識別及鑑別機制(如使用者鑑別)	假冒使用者身分	1	0	0
		缺乏發送端與接收端識別及鑑別機制	未經授權的使用	1	0	0
			偷竊	1	0	0
		離開工作站沒有登出(Logout)	未經授權的使用	1	0	0
		沒有或不足的軟體測試	軟體故障	0	1	1
		不良的通行碼(password)管理	假冒使用者身分	1	0	0
		通行碼以明碼傳送	未經授權的使用	1	0	0
		不明確或不完整的開發規格	軟體故障	0	1	1
		軟體的已知缺陷	非法輸出/入軟體	1	1	0
			惡意的軟體	0	1	1
			軟體故障	0	1	1

大類	小類	弱點	威脅	C	I	A
硬體類	個人電腦	不當使用軟體及(或)硬體	資源的不正確使用	1	0	1
			儲存媒體變質	0	1	1
		未保護的儲存空間	偷竊	1	0	1
			惡意損毀	1	0	1
			溫度與濕度超過限值	0	1	1
			儲存媒體變質	0	1	1
		存取控制的錯誤配置	未授權即使用媒體	1	0	1
			資源的不正確使用	1	0	1
		缺乏正確使用通訊媒體與傳訊的政策	未授權即使用媒體	1	0	1
			偷竊	1	0	1
			惡意損毀	1	0	1
			資源的不正確使用	1	0	1
		缺乏監控(monitoring)機制	未授權即使用媒體	1	0	1
			偷竊	1	0	1
			溫度與濕度超過限值	0	1	1
			資源的不正確使用	1	0	1
			儲存媒體變質	0	1	1
		缺乏稽核軌跡	未授權即使用媒體	1	0	1
			資源的不正確使用	1	0	1
		對電磁輻射敏感	硬體故障	0	0	1
			電磁輻射	0	0	1
			靜電	0	0	1
			儲存媒體變質	0	1	1
		對電壓變化敏感	硬體故障	0	0	1
			電壓不穩定	0	0	1
			儲存媒體變質	0	1	1
		對濕度灰塵及塵土敏感	灰塵	0	0	1
			空調故障	0	0	1
			硬體故障	0	0	1
			儲存媒體變質	0	1	1
	可攜式個人電腦	不足的維護或儲存媒體錯誤的安裝	硬體故障	1	0	1
			維護錯誤	0	0	1
		不當使用軟體及(或)硬體	硬體故障	0	0	1
			資源的不正確使用	1	0	1
		不當的服務維護回應	硬體故障	0	0	1
		未控制通訊線路	由非授權人員存取網路	1	0	1
			流量分析	1	0	1
			訊息轉接(rerouting)	1	0	1

大類	小類	弱點	威脅	C	I	A
			資源的不正確使用	1	0	1
		存取控制的錯誤配置	偷竊	1	0	1
			惡意損毀	1	0	1
			資源的不正確使用	1	0	1
		缺乏有效的建構變更控制	硬體故障	0	0	1
			維護錯誤	0	0	1
			操作人員的錯誤	0	0	1
		缺乏監控(monitoring)機制	偷竊	1	0	1
			惡意損毀	1	0	1
			硬體故障	0	0	1
			溫度與濕度超過限值	0	0	1
			操作人員的錯誤	0	0	1
		對電壓變化敏感	硬體故障	0	0	1
			電壓不穩定	0	0	1
		廢棄物處理疏於照管	偷竊	1	0	1
			資源的不正確使用	1	0	1
		撥接線路	由非授權人員存取網路	1	0	1
			資源的不正確使用	1	0	1
		儲存媒體未加以適當清除即丟棄或再利用	偷竊	1	0	1
			資源的不正確使用	1	0	1
	伺服器(對內&對外)、託管設備	不足的維護或儲存媒體錯誤的安裝	硬體故障	0	0	1
			維護錯誤	0	0	1
		不當使用軟體及(或)硬體	硬體故障	0	0	1
			資源的不正確使用	1	0	1
		不當的服務維護回應	硬體故障	0	0	1
		存取控制的錯誤配置	偷竊	1	0	1
			惡意損毀	1	0	1
			資源的不正確使用	1	0	1
		缺乏有效的建構變更控制	硬體故障	0	0	1
			維護錯誤	0	0	1
			操作人員的錯誤	0	0	1
		缺乏監控(monitoring)機制	偷竊	1	0	1
			惡意損毀	1	0	1
			硬體故障	0	0	1
			溫度與濕度超過限值	0	0	1
			操作人員的錯誤	0	0	1
		單點失效(Single point of failure)	通訊服務故障	0	0	1
			通訊纜線損壞	0	0	1

大類	小類	弱點	威脅	C	I	A
			硬體故障	0	0	1
		對電壓變化敏感	硬體故障	0	0	1
			電壓不穩定	0	0	1
		廢棄物處理疏於照管	偷竊	1	0	1
			資源的不正確使用	1	0	1
		儲存媒體未加以適當清除即丟棄或再利用	偷竊	1	0	1
			資源的不正確使用	1	0	1
	其他硬體、儲存設備	不足的維護或儲存媒體錯誤的安裝	硬體故障	0	0	1
			維護錯誤	0	0	1
		不當使用軟體及(或)硬體	硬體故障	0	0	1
			資源的不正確使用	1	0	1
		不當的服務維護回應	硬體故障	0	0	1
		存取控制的錯誤配置	未授權即使用媒體	1	0	1
			非法輸出/入軟體	1	0	0
			偷竊	1	0	1
			惡意損毀	1	0	1
			資源的不正確使用	1	0	1
		缺乏有效的建構變更控制	硬體故障	0	0	1
			維護錯誤	0	0	1
			操作人員的錯誤	0	0	1
		缺乏監控(monitoring)機制	偷竊	1	0	1
			惡意損毀	1	0	1
			硬體故障	0	0	1
			溫度與濕度超過限值	0	0	1
			操作人員的錯誤	0	0	1
		對電壓變化敏感	硬體故障	0	0	1
			電壓不穩定	0	0	1
		廢棄物處理疏於照管	偷竊	1	0	1
			資源的不正確使用	1	0	1
	網路設備	不良的佈線	通訊服務故障	0	0	1
			通訊纜線損壞	0	0	1
			傳輸錯誤	0	0	1
			滲透通訊	1	0	1
			維護錯誤	0	0	1
			操作人員的錯誤	0	0	1
		不良的通行碼(password)管理	由非授權的人員使用軟體	1	0	1
			假冒使用者身分	1	0	1
		不足的維護或儲存媒體錯誤的	通訊服務故障	0	0	1

大類	小類	弱點	威脅	C	I	A
		安裝	硬體故障	0	0	1
			網路組件故障	0	0	1
			維護錯誤	0	0	1
		不當使用軟體及(或)硬體	通訊服務故障	0	0	1
			硬體故障	0	0	1
			資源的不正確使用	1	0	1
			網路組件故障	0	0	1
		不當的服務維護回應	通訊服務故障	0	0	1
			硬體故障	0	0	1
			網路組件故障	0	0	1
		不當的網路管理 (路由彈回 resilience of routing)	流量超載	0	0	1
			通訊服務故障	0	0	1
		未保護公眾網路連線	由非授權人員存取網路	1	0	1
			資源的不正確使用	1	0	1
		未保護敏感性資訊流	流量分析	1	0	1
			訊息被重組或轉送	1	1	1
		未保護通行碼資料表	由非授權的人員使用軟體	1	0	1
			假冒使用者身分	1	0	1
		未控制通訊線路	流量分析	1	0	1
			訊息轉接(rerouting)	1	0	1
			通訊纜線損壞	0	0	1
		存取控制的錯誤配置	惡意損毀	1	0	1
			資源的不正確使用	1	0	1
		缺乏有效的建構變更控制	硬體故障	0	0	1
			網路組件故障	0	0	1
			維護錯誤	0	0	1
			操作人員的錯誤	0	0	1
		缺乏發送端與接收端識別及鑑別機制	由非授權人員存取網路	1	0	1
			訊息被重組或轉送	1	1	1
			訊息轉接(rerouting)	1	0	1
		缺乏監控(monitoring)機制	惡意損毀	1	0	1
			硬體故障	0	0	1
			溫度與濕度超過限值	0	0	1
			操作人員的錯誤	0	0	1
		缺乏稽核軌跡	以非授權的方式使用網路設施	1	0	1
			由非授權人員存取網路	1	0	1
			惡意損毀	1	0	1

大類	小類	弱點	威脅	C	I	A
		缺乏識別及鑑別機制(如使用者鑑別	由非授權的人員使用軟體	1	0	1
			假冒使用者身分	1	0	1
		軟體的已知缺陷	由非授權的人員使用軟體	1	0	1
			軟體故障	0	0	1
			惡意軟體	1	0	1
		通行碼以明碼傳送	由非授權的人員使用軟體	1	0	1
			假冒使用者身分	1	0	1
		單點失效(Single point of failure)	通訊服務故障	0	0	1
			硬體故障	0	0	1
			網路組件故障	0	0	1
		對電壓變化敏感	硬體故障	0	0	1
			電壓不穩定	0	0	1
		繁複的使用者介面	操作人員的錯誤	0	0	1
	通訊設備	不良的佈線	通訊服務故障	0	0	1
			通訊纜線損壞	0	0	1
			傳輸錯誤	0	0	1
			滲透通訊	1	0	1
			維護錯誤	0	0	1
			操作人員的錯誤	0	0	1
			竊聽	1	0	0
		不良的通行碼(password)管理	假冒使用者身分	1	0	1
			資源的不正確使用	1	0	1
		不足的維護或儲存媒體錯誤的安裝	通訊服務故障	0	0	1
			硬體故障	0	0	1
			維護錯誤	0	0	1
		不當使用軟體及(或)硬體	通訊服務故障	0	0	1
			硬體故障	0	0	1
			資源的不正確使用	1	0	1
		不當的服務維護回應	通訊服務故障	0	0	1
			硬體故障	0	0	1
		未保護公眾網路連線	資源的不正確使用	1	0	1
			竊聽	1	0	0
		未保護敏感性資訊流	竊聽	1	0	0
		未控制通訊線路	通訊纜線損壞	0	0	1
			竊聽	1	0	0
		存取控制的錯誤配置	惡意損毀	1	0	1
			資源的不正確使用	1	0	1
		缺乏有效的建構變更控制	通訊服務故障	0	0	1

大類	小類	弱點	威脅	C	I	A
			硬體故障	0	0	1
			維護錯誤	0	0	1
			操作人員的錯誤	0	0	1
		缺乏發送及接收訊息的證據	否認服務交易或收送訊息	1	1	1
		缺乏發送端與接收端識別及鑑別機制	否認服務交易或收送訊息	1	1	1
			資源的不正確使用	1	0	1
		缺乏監控(monitoring)機制	惡意損毀	1	0	1
			硬體故障	0	0	1
			資源的不正確使用	1	0	1
		缺乏稽核軌跡	惡意損毀	1	0	1
			資源的不正確使用	1	0	1
		缺乏識別及鑑別機制(如使用者鑑別	否認服務交易或收送訊息	1	1	1
			假冒使用者身分	1	0	1
		單點失效(Single point of failure)	通訊服務故障	0	0	1
			硬體故障	0	0	1
		對電壓變化敏感	硬體故障	0	0	1
			電壓不穩定	0	0	1
		撥接線路	資源的不正確使用	1	0	1
		繁複的使用者介面	使用者錯誤	0	0	1
	有資料的可攜式儲存媒體	不良的通行碼(password)管理	未授權即使用媒體	1	0	1
		不足的維護或儲存媒體錯誤的安裝	硬體故障	0	0	1
			儲存媒體變質	0	1	1
		不當使用軟體及(或)硬體	非法使用軟體	1	0	1
			非法輸出/入軟體	1	0	0
			資源的不正確使用	1	0	1
			儲存媒體變質	0	1	1
		未保護的儲存空間	偷竊	1	0	1
			惡意損毀	1	0	1
			溫度與濕度超過限值	0	0	1
			儲存媒體變質	0	1	1
		未控制複製	偷竊	1	0	1
			資源的不正確使用	1	0	1
		存取控制的錯誤配置	未授權即使用媒體	1	0	1
			非法使用軟體	1	0	1
			非法輸出/入軟體	1	0	0
			資源的不正確使用	1	0	1
		缺乏正確使用通訊媒體與傳訊的政策	未授權即使用媒體	1	0	1
			偷竊	1	0	1

大類	小類	弱點	威脅	C	I	A
			惡意損毀	1	0	1
			資源的不正確使用	1	0	1
		缺乏有效的變更控制	使用者錯誤	0	0	1
			操作人員的錯誤	0	0	1
		缺乏定期替換計畫(schemes)	硬體故障	0	0	1
			儲存媒體變質	0	1	1
		缺乏備援拷貝	水災土石流	0	0	1
			火災	0	0	1
			偷竊	1	0	1
			惡意損毀	1	0	1
			儲存媒體變質	0	1	1
		缺乏發送及接收訊息的證據	否認服務交易或收送訊息	1	1	1
			儲存媒體變質	0	1	1
		缺乏監控(monitoring)機制	未授權即使用媒體	1	0	1
			非法使用軟體	1	0	1
			非法輸出/入軟體	1	0	0
			偷竊	1	0	1
			溫度與濕度超過限值	0	0	1
			資源的不正確使用	1	0	1
			儲存媒體變質	0	1	1
		缺乏稽核軌跡	未授權即使用媒體	1	0	1
			資源的不正確使用	1	0	1
		對電磁輻射敏感	硬體故障	0	0	1
			電磁輻射	0	0	1
			靜電	0	0	1
			儲存媒體變質	0	1	1
		對電壓變化敏感	硬體故障	0	0	1
			電壓不穩定	0	0	1
			儲存媒體變質	0	1	1
		對濕度灰塵及塵土敏感	灰塵	0	1	1
			空調故障	0	0	1
			硬體故障	0	0	1
			儲存媒體變質	0	1	1
		廢棄物處理疏於照管	偷竊	1	0	1
			資源的不正確使用	1	0	1
		儲存媒體未加以適當清除即丟棄或再利用	未授權即使用媒體	1	0	1
			偷竊	1	0	1
			資源的不正確使用	1	0	1

大類	小類	弱點	威脅	C	I	A
	沒有資料的可攜式儲存媒體	不當使用軟體及(或)硬體	資源的不正確使用	1	0	1
			儲存媒體變質	0	1	1
		未保護的儲存空間	偷竊	1	0	1
			惡意損毀	1	0	1
			溫度與濕度超過限值	0	1	1
			儲存媒體變質	0	1	1
		存取控制的錯誤配置	未授權即使用媒體	1	0	1
			資源的不正確使用	1	0	1
		缺乏正確使用通訊媒體與傳訊的政策	未授權即使用媒體	1	0	1
			偷竊	1	0	1
			惡意損毀	1	0	1
			資源的不正確使用	1	0	1
		缺乏監控(monitoring)機制	未授權即使用媒體	1	0	1
			偷竊	1	0	1
			溫度與濕度超過限值	0	1	1
			資源的不正確使用	1	0	1
			儲存媒體變質	0	1	1
		缺乏稽核軌跡	未授權即使用媒體	1	0	1
			資源的不正確使用	1	0	1
		對電磁輻射敏感	硬體故障	0	0	1
			電磁輻射	0	0	1
			靜電	0	0	1
			儲存媒體變質	0	1	1
		對電壓變化敏感	硬體故障	0	0	1
			電壓不穩定	0	0	1
			儲存媒體變質	0	1	1
		對濕度灰塵及塵土敏感	灰塵	0	0	1
			空調故障	0	0	1
			硬體故障	0	0	1
			儲存媒體變質	0	1	1
	電腦保護設施	不足的維護或儲存媒體錯誤的安裝	硬體故障	0	0	1
			維護錯誤	0	0	1
		不當的服務維護回應	硬體故障	0	0	1
		存取控制的錯誤配置	惡意損毀	1	0	1
			資源的不正確使用	1	0	1
		位處易有水患之地	水災土石流	0	0	1
		缺乏有效的建構變更控制	硬體故障	0	0	1
			維護錯誤	0	0	1

大類	小類	弱點	威脅	C	I	A
			操作人員的錯誤	0	0	1
		缺乏定期替換計畫(schemes)	硬體故障	0	0	1
			儲存媒體變質	0	1	1
		缺乏監控(monitoring)機制	惡意損毀	1	0	1
			硬體故障	0	0	1
			溫度與濕度超過限值	0	0	1
			操作人員的錯誤	0	0	1
		單點失效(Single point of failure)	硬體故障	0	0	1
			電力供應故障	0	0	1
			電壓不穩定	0	0	1
		對電壓變化敏感	硬體故障	0	0	1
			電壓不穩定	0	0	1

附錄C、資訊資產弱點脆弱度評分

評分標準：必須評估脆弱點的嚴重程度，亦即容易被威脅所利用的程度。

- 4-弱點無受到適當控制且無初步計畫與認知。
- 3-弱點無受到適當控制且無初步計畫但具有認知。
- 2-弱點無受到適當控制但已有初步計畫。
- 1-弱點已受到適當控制。
- 0-不適用。

附錄D、資訊資產威脅發生機率評分

判斷該威脅對資訊資產造成營運衝擊的可能性並納入影響嚴重度等客觀評分。

- 4-發生可能性極高：每月至少發生兩次(MAX：∞次/年；MIN：24 次/年)
- 3-發生可能性高：每月發生一次以上(MAX：23 次/年；MIN：12 次/年)
- 2-發生可能性中度：每季發生一次以上(MAX：11 次/年；MIN：4 次/年)
- 1-發生可能性低或無：每年發生三次以下(MAX：3 次/年；MIN：0 次/年)
- 0-不適用