6. 災害防救業務雲端之基礎服務規劃

6.1. 雲端規劃之方向與需求

本章節為災害防救業務雲端之資訊基礎服務規劃構面，依據防救災雲端架構圖之範疇，包含伺服主機架構、儲存設備、虛擬主機、主機代管、資源分配管理，以及支援各項服務之基礎建設，包含災難備援及備份機制、資料管理、網路架構、機房及環控設施等項目。

基於本案之規劃目標以及未來因應防救災業務之資訊基礎建設需求，本節重點將專注於整體資訊基礎建設服務進行分析，並說明未來整合發展所需要之技術。

圖 472、防救災雲端架構圖

6.1.1. 軟、硬體基礎建設整體架構

有關軟硬體架構規劃方向，分項說明如後：

6.1.1.1. 伺服器集中化與系統虛擬化

將伺服器硬體環境規劃成為 Computer Hardware Resources

Pool(簡稱 C.H.R.P.)，將既有伺服器硬體資源納入管理，共享硬體資源，提高伺服器硬體使用率。

伺服器集中化與系統虛擬化，需考量伺服器網路的頻寬需求，建議需支援 Giga 或 10G 的伺服器內網,核心交換器需支援 Giga 或 10G 介面。

6.1.1.2. 資料庫伺服主機架構

建議辦公室自動化系統、一般非主要應用系統的資料庫伺服器應納入虛擬化管理，以共享硬體資源，提高伺服器硬體使用率，並達成節能減碳，綠色環保之需求。

而防救災資料庫伺服器為了更進一步安全之考量則採單獨實體的建置方式，並透過 Cluster 叢集系統，提高系統的可靠度。

6.1.1.3. 儲存系統架構

將儲存環境集中化管理，導入 NAS(Network Attached Storage: 網路附加儲存)、SAN(Storage Area Network: 儲域網路)及 iSCSI(Internet SCSI)等儲存架構。

6.1.1.3.1. NAS (Network Attached Storage)儲存架構

NAS 和 SAN 等其他儲存技術,是為了滿足大型存放區和設備共用需求而產生。NAS 產品包括儲存部件(例如磁碟陣列)和內嵌系統軟體,它能夠支援多種應用協定(如 NFS、CIFS、FTP、HTTP 等),還能夠支援各種作業系統,如 Unix/Linux/Windows 等,而且在不同的網路環境中使用也無需對網路環境進行任何的修改。NAS 產品直接通過網路介面連接到網路上,簡單地配置 IP 位址後,就可以被網路上的使用者所共同使用，導入的複雜度低、相容性較高，NAS 尤其適宜於通過 LAN 傳輸儲存檔和共用檔。

NAS 儲存方式如下圖所示：

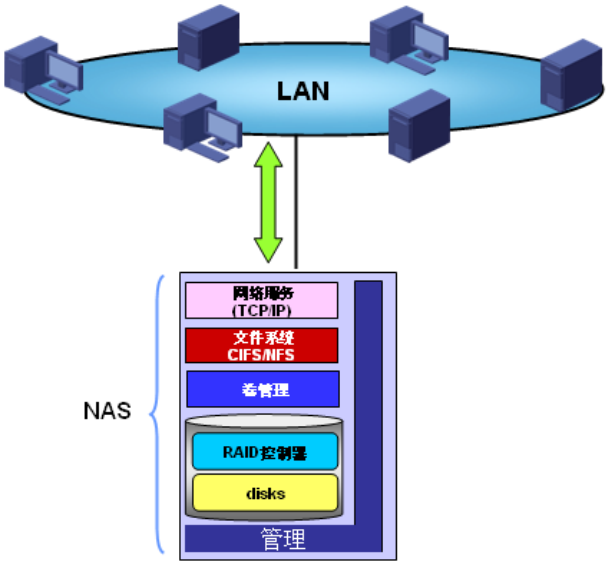

圖 473、NAS 儲存方式

6.1.1.3.2. SAN (Storage Area Netwrok)儲存架構

相對於 NAS，SAN 的優勢在於所有的資料處理都不是由伺服器完成的，SAN 是一種將存放裝置、連接設備和介面集成在一個高速網路中的技術，它本身就是一個儲存網路，承擔了資料儲存任務，SAN 網路與 LAN 業務網路相隔離，儲存資料流程不會佔用業務網路頻寬。SAN 儲存方式如下圖所示：

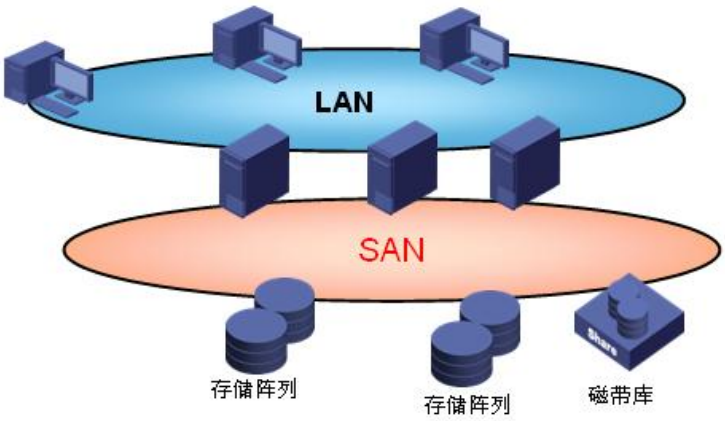

圖 474、SAN 儲存方式

在 SAN 網路中，所有的資料傳輸在高速、高頻寬的網路中進行，SAN 儲存實現的是直接對物理硬體的塊級儲存訪問，提高了儲存的性能和升級能力。

在過去以 FC 協定為主的 SAN 儲存系統建設中，人們逐漸發

現 FC 協議雖然基本解決了傳送速率和擴大容量的問題，卻難以完全承擔起儲存系統獨立化的重任。FC SAN 的互通性仍是實施過程中存在的主要問題。SAN 本身缺乏標準，尤其是在管理上更是如此。雖然光纖通道(Fibre Channel)技術標準的確存在，但各家廠商卻有不同的解釋，於是，互通性變成了問題。這就導致了 FC 相容性差、成本高昂、擴展能力差、異構化嚴重的問題。

6.1.1.3.3. iSCSI (Internet SCSI)儲存架構

在儲存技術裡，以 SAN 的名義獨立走上 IT 舞臺的同時，IP 和乙太網技術在網路領域突飛猛進，在同樣 1997-2005 的 8 年中，主流商用協定標準從 10M 發展到了 10G，整整提升了 1000 倍，行業的發展動力和技術標準的成熟性已無可爭辯。IP 技術已經成為整個 IT 行業中最成熟、最開放、發展最迅速、成本最低、管理最方便的資料通訊方式。在經歷了 FC SAN 發展的過渡性嘗試後，整個行業開始考慮將 FC 傳輸技術替代為更加成熟可靠、成本更低的 IP 技術，以適應廣域網路資料應用、大規模伺服器資料集中、海量資料儲存等應用對新一代儲存系統的要求，同時為“隨需應變”的 IT 新時代到來，奠定堅實的開放化標準基礎。2003 年，以 IBM 等公司共同發起的 iSCSI(Internet SCSI)協定，通過 IETF 組織的審議，公佈為 RFC 標準。iSCSI 協定實際就是將標準的 SCSI 儲存訪問指令，打包到 TCP/IP 中進行傳輸。

由於 iSCSI 協議將 SCSI 資料傳輸的基礎從封閉昂貴的 FC 協議轉移到 IP 之上，使儲存系統突破了長期困擾著儲存系統的相容性、成本和管理性桎梏，使儲存網格、廣域資料傳輸、大規模伺服器資料集中、遠端容災、高性能交換式儲存架構等儲存技術脫下昂貴的外衣，成為廣大行業客戶均能輕鬆獲得的最新儲存技術。

隨著 iSCSI 技術的完善，資料塊級的儲存應用將變得更為普遍，儲存資源的通用性、資料共用能力都將大大增強，並且更加易於管理。隨著 Giga 乙太網的普及以及 10G 乙太網路的成熟，IP

儲存必然會以其性價比、通用性、無地理限制等優勢發展，iSCSI 技術將聯合 SCSI、TCP/IP，共同開創網路儲存的新局面。

以下以一個表格總結幾種儲存模式的不同點：

表 107、FC & IP 儲存比較表

	FC 儲存	IP 儲存
協議類型	簡單二層通道協議。近似於權杖環。FC 是 90 年代乙太網尚未充分發展階段的歷史性技術	三層協議，標準化網路通訊協定
開放性	體系封閉僵硬，複雜昂貴，無管理，發展緩慢。技術近 10 年沒有更新。	標準化，高度開放，使用廣泛，成熟，成本低廉
體系結構	中低端採用仲裁環結構，容量越大，性能越低；高端交換結構採用共用記憶體方式。	中低端也採用先進的 Crossbar 交換結構，“高端貴族技術平民化”；容量越大，性能越高。
擴展性	擴展有限，擴展後性能降低	擴展無限
性能	1Gb/s、2Gb/s，2006 年已可達 4Gb/s，線速吞吐率可分別達到 100，200，400MB/s	100Mb/s、1Gb/s、2003 年 10G 開始規模商用，線速吞吐率分別達到 124MB/s，1240MB/s
互通性	歷史遺留存在嚴重的互通性問題，產品互聯性差，至今未建立管理標準。面臨業務擴展延伸、多儲存平臺整合等諸多問題。	與 IP、乙太網有優異的互通性，全球成熟標準，跨廠商互聯互通，管理方便、成本低廉
安全性	FC 技術協議簡單，沒有安全防禦手段，只能通過物理隔離手段保證資料安全	IP 技術中有完整的加密、認證技術，保證資料安全性，還可以通過 FW/IPS 等提高系統安全性
投資成本	較高初期投資成本和極高的後期維護管理成本	配套成本低，分步滾動投資，維護成本低
可管理性	專用獨立的 FC 網路管理，形成 FC 儲存孤島	第一網、第二網集中統一的 IP 管理，容易掌握
距離限制	距離局限在都會區網路範圍內(<30 公里)	無距離限制，距離可擴展到 IP 網路所及的範圍

6.1.1.3.4. Unified Storage 儲存設備

隨著企業資料儲存往簡化管理方向發展，企業也希望儲存設備能提供一個能統一所有協定於單一架構，不論 FCP、iSCSI、NFS、CIFS 都能在相同架構下直接提供服務，同時也不必受限於網路使用 FC 或 GbE。如果能達到此境界的儲存設備，一般稱之

為 Unified Storage。

其擁有的好處及特色如下:

- LUN 的透通移轉性:

對於某一主機使用 FCP 所連接使用的 LUN,可改用 iSCSI 來連接此LUN,完全不用將資料先備份出去,然後再還原回來，如此對於原有的 FCP 應用環境，可視需要隨時將傳輸協定轉乘 iSCSI，同時也可以為 10GbE 的環境做準備，如過原先使用 iSCSI 所連接的 LUN，若要轉換為 FCP，同樣的也不用搬動原有的資料。

- 單一平台的管理簡單化:

對於資料的備份與還原可以達到單一平台的管理介面簡單性，不需要透過不同的系統介面來管理，以降低高複雜度所帶來的管理成本與容易操作錯誤的危險。

- 儲存空間使用率的最佳化:

利用儲存系統內部的虛擬化功能，可隨時將空間剩餘很多的 Volume，立刻挪用給那些空間不足的 Volume，不但不用停機,也不會影響原有系統的運作,如此便不需要採購新的設備，增加空間使用的彈性並達到最佳化，以提高對於現有儲存空間的投資報酬率。

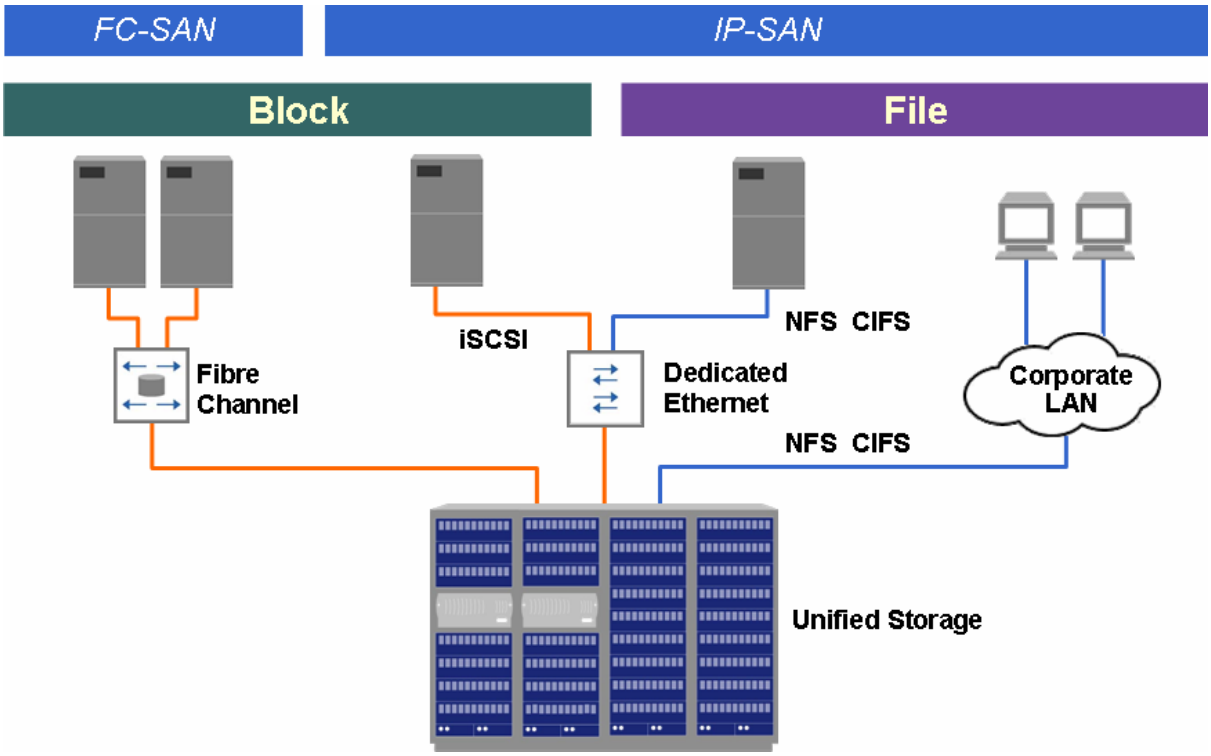

圖 475、Unified Storage 示意圖

6.1.1.4. 虛擬化軟體

虛擬化軟體須有分散式資源調度(Distributed Resource Scheduler，DRS)功能，可以持續不斷地監控虛擬化軟體主機群集中資源的利用率，並能夠根據需求在虛擬機中有效地分配其所需的資源。透過動態分配和平衡計算資源，虛擬化軟體 DRS 能夠整合伺服器，降低 IT 成本，增強靈活性；減少停機時間，保持服務系統的持續性和穩定性；減少需要運行伺服器的數量以及動態地切斷目前未需使用的伺服器的電源，提高了能源的利用率。另外虛擬化軟體須提供 High Availability (HA)之功能，為在虛擬機器內部執行的應用程式提供了容易使用、且符合成本效益的高可用性。如果伺服器發生故障，受影響的虛擬機器就會自動在其他伺服器上以備用處理資源重新啟動。由於防救災業務性質，我們建議虛擬化軟體需要有不停機便能新增虛擬資源(包括 CPU、Memory，虛擬硬碟)的功能，以備不時之需。

因此在購置虛擬化軟體時，建議需考量下列之功能:

- 支援將產業標準 PC Server (X86 架構) 上面的處理器、記憶體、儲存裝置及網路資源分割為多部虛擬機器，將數個獨立

的作業系統 (guest OS)，可同時執行於一部電腦硬體主機。

- 支援例如 IBM，HP，Dell，NEC 等各種品牌 PC 伺服器。
- 支援虛擬機器的作業系統(Guest OS) 含 Microsoft Windows 作業系統，例如：2008、2003、2000、Windows 7、Vista 等系統；及各廠牌 Linux 作業系統，例如：Red Hat、SUSE、Ubuntu 等系統。
- 需具備叢集檔案作業系統能力，將虛擬機器 (Guest OS) 置於高效能叢集檔案系統，該檔案系統能讓多個不同主機同時存取。
- 儲存設備可支援 SAN，iSCCI，與 NAS。
- 支援統一控管之圖形化界面。統一管理跨不同硬體主機上的虛擬機器。能提供具有互動功能的拓樸圖，以視覺方式呈現實體伺服器，虛擬機器，網路和儲存設備之間的關係。並監控實體伺服器及虛擬機器的可用性及使用率。
- 支援「虛擬主機線上移轉」，虛擬機器 (Guest OS) 能在不同硬體主機上移轉，並且服務與網路不中斷。
- 支援 HA (high availability)功能，提供虛擬機器(guest OS)在發生錯誤時進行切換。
- 提供虛擬機器在遭遇硬體錯誤時進行零停機切換。
- 提供虛擬機器之間動態資源與負載自動最佳化。
- 支援記憶體飄移功能，將閒置虛擬機器的記憶體以動態方式移轉給使用中的虛擬機器使用。讓閒置的虛擬機器使用自己的分頁空間(paging space)而將實體記憶體讓出給有需要的其它虛擬機器使用。
- 支援符合 SMI-S 相容的管理介面，可使用任何標準的 SMI-S 的感知儲存管理工具來監控虛擬儲存。
- 支援 CPU 資源優先順序功能，確保重要的虛擬機器能取得一定的 CPU 處理資源。
- 支援 Memory 資源優先順序功能，確保重要的虛擬機器能取

得一定的 Memory 處理資源。

- 支援網路流量調節功能，確保重要的虛擬機器能取得網路頻寬的優先存取權。
- 可支援 Microsoft MSCS 等虛擬機器內的叢集軟體。
- 需提供 Patch 管理工具，為虛擬機器與實體機器之作業系統自動進行 patch 管理，可以記錄比對及追蹤 patch 升級。
- 提供線上增加虛擬機 CPU 與記憶體功能
- 提供線上增加與移除網路設備與磁碟設備功能
- 支援第三方多重路徑存取功能 (3rd IO Multipathing)
- 支援第三方虛擬交換器功能 (3rd Distributed Switch)
- 提供網路分散交換器功能(vNetwork Distributed Switch)
- 提供 thing provisioning 功能，節省磁碟空間。
- 提供 host profiles 功能，以快速複製與部署所需的主機
- 提供備份至磁碟並進行重覆資料刪除功能(data recovery)

6.1.1.5. 整體架構建議

建議伺服器及儲存硬體架構規劃採集中式，成為 Computer Hardware Resources Pool，將伺服器硬體資源納入管理，共享硬體資源，並透過虛擬化軟體，動態管理集中化後的硬體資源，以提高伺服器硬體使用率，改善原有以系統為劃分的方式，資源分散，資料儲存分散，無法統一管理及做有效的資源分配，形成資源浪費。

硬體資源統一管理運用後，能達成幾項成效：

- 資源有效利用，大幅降低資源浪費。
- 推行綠色節能環保觀念，降低耗電量使用，降低碳排放量。
- 不影響原有管理模式，只將實體虛擬化，集中由資訊室人員作硬體控管。
- 提高工作效率，在硬體可容許的範圍內，可隨時提供系統需求，快速反應。
- 系統原地備援模式建置，提升系統可用率。
- 測試環境、驗證環境，建置與營運環境 100%相容，系統上

線部署容易，提高工作效率。

- 將硬體環境與系統需求做切割分離，除了特殊環境需求外，可以統一控管，不會浪費硬體採購費用。
- 儲存集中，備份資料只需考量儲域網路內既可完成。
- 資料統一儲存，提高資料安全性。
- 儲存需求統一控管，提高資源使用率。

整體虛擬化集中架構示意圖如下：

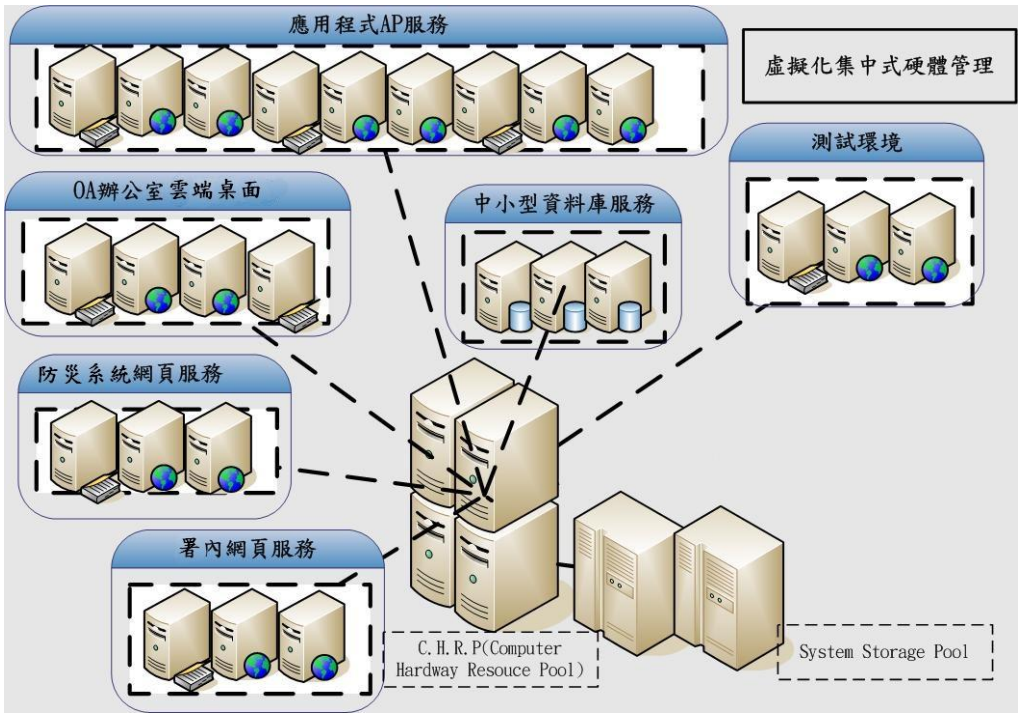

圖 476、虛擬化集中管理示意圖

6.1.2. 主機伺服器架構

6.1.2.1. 伺服器規劃及設計原則

目前在消防署伺服器數量眾多，各縣市災害應變中心皆有機房設施，無形中增加不少管理負擔，此外，伺服器使用多種硬體平台和作業系統,所需要的管理人員技術門檻很高,管理知識之傳承也較困難，未來雲端機房的伺服器應朝向以下的需求來規劃與設計：

- 採用伺服器實體集中與虛擬主機方式來減少伺服器硬體數量，並提高整體系統的可管理性，也較易進行資訊系統之變更管理，並簡化資訊系統管理工具之複雜性。

- 規劃採用虛擬化架構及技術能夠更動態地配置資訊資源，並且保留未來消防資訊系統集中之彈性，能有效提高伺服器與中介軟體之使用率。
- 整合業務應用系統,依防救災業務應用系統的業務型態規劃，儘量將業務型態較為類似的防救災業務應用系統擺設在同一個伺服器分割區內。

6.1.2.2. 伺服器虛擬化與實體整合規劃原則與方向

防救災伺服器虛擬化與實體整合規劃主要以 Unix 與 Windows 作業系統架構為主，其虛擬化與實體整合規劃的原則與方向說明如下：

- Unix 伺服器：

(1) 實體伺服器整合，使用邏輯分割技術。
(2) 支援動態邏輯分區，彈性資源調整，因應防汛期增加之負載。
(3) 使用新型伺服器，提昇整體防救災系統運作效能。
(4) 考量防救災業務的營運不中斷需求，於重要的業務應用伺服器，使用叢集(Cluster)的架構。
(5) 依網路分區規劃伺服器整合。

- Windows 伺服器：

(1) 實體伺服器整合，規劃使用 PC Server。
(2) 採用虛擬化技術，彈性資源調整，以因應防汛期增加之負載。
(3) 使用新型伺服器，提昇整體防救災系統運作效能。
(4) 考量防救災業務的營運不中斷需求，於重要的業務應用伺服器，使用負載平衡(Load-Balanced)的架構。
(5) 依網路分區規劃伺服器整合。

另外伺服器硬體或作業系統發生故障時，需為所有應用程式提供自動重新啟動功能，在短時間內便能完成啟動。伺服器虛擬化後須兼顧高效率化、安全性、擴充性、系統備援、彈性及易於管理之原則。

6.1.2.3. 伺服器管理規劃原則與方向

- 對於伺服器變更管理而言：

為便利進行資訊系統之變更與簡化資訊系統部署之複雜性，

規劃使用自動化軟體派送與安裝工具來進行應用軟體安裝以及系統重要更新的安裝。

- 對於伺服器備份管理而言：

  伺服器系統備份與資料備份應透過備份管理工具定期排程備份，並符合現行防救災的備份原則。

- 對於伺服器資源管理而言：

  為求能夠更動態地配置伺服器資源，便利與簡化伺服器系統管理，並且保留未來消防資訊系統集中之彈性，以及有效提高伺服器與中介軟體之使用率，規劃使用虛擬化軟體來進行伺服器虛擬分割作業、系統與硬體集中化的管理機制。

6.1.2.4. 效能要求

防救災雲端的伺服器數量規劃整體步驟將依據防救災資訊業務應用、以及虛擬化與實體整合規劃原則的實際需求，估算未來防救災資訊各相關硬體伺服器的負載容量與性能數值。

此外，考量業界眾多的伺服器系統並不是每一台皆具有或認證通過國際公認的性能標準，於規劃硬體設備時，我們亦將搭配業界伺服器系統的 RP 指標 (相對性能比較值)來作為依據與參考。

而整體未來防救災資訊雲端伺服器數量規劃原則如下：

- 首先設定期望的系統效能目標，然後重複運用設備廠商效能預估工具找出能滿足效能目標且符合成本效益之機容。
- 使用 TPC /SPEC benchmark 基準資料以轉換各廠牌伺服器規格。

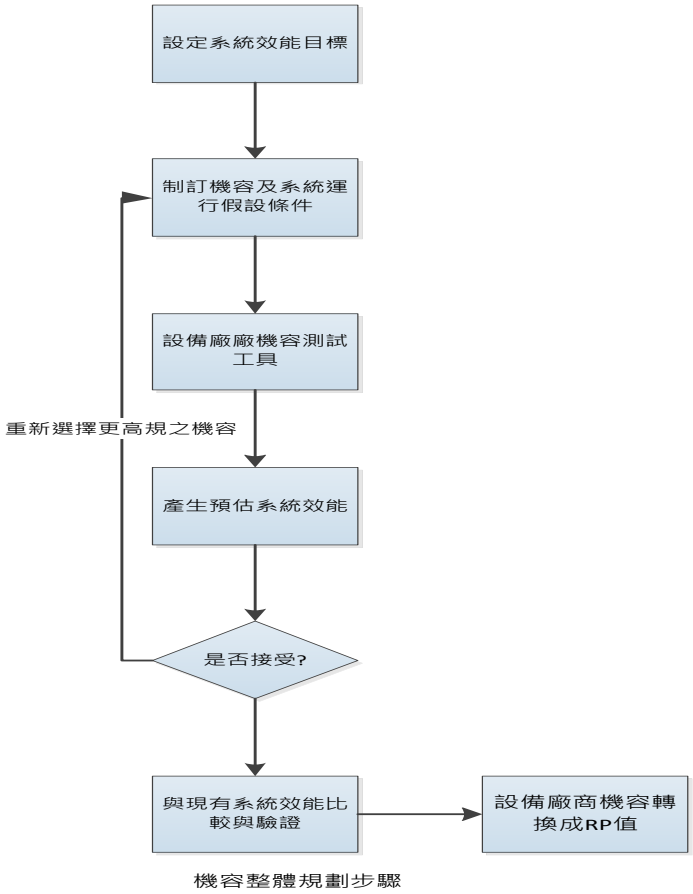

圖 477、機容整體規劃步驟

6.1.2.4.1. 設定系統效能目標

- 系統效能評估基礎：

  (1) 最多同時 2,400 使用者(以中央災害應變中心 200 人，22 個縣市災害應變中心同時開設，每個災害應變中心 100 人估計) 。

  (2) 每人平均每 60 秒提交一次需求。

  (3) 每次需求平均使用 3 個頁面(Frame)。

  (4) 每次頁面平均傳送 5 個物件(html、jpg、css、js…)

  (5) 每次需求平均 3 次 DB 交易。

- 設定系統效能目標：

  (1) 每個頁面平均回應時間小於 3 秒。

  (2) CPU 使用率小於 60%。

- 系統效能指標

  (1) Web

2400 (需求) / 60 (秒) = 40 (需求/秒)

(2) DB

2400(需求) * 3 (存取) / 60 (秒) = 120 (存取/秒)

6.1.2.4.2. 系統運行假設條件

- 應用程式平均使用 3 個頁面，頁面與頁面之使用者處理時間約 30 秒。
- DB 伺服器 85%之使用率在處理 Foreground 程序。
- 95%的交易必須滿足所設定之系統效能目標。

6.1.2.4.3. 試算入口網伺服器與應用伺服器規格與數量

根據 http:// www-304.ibm.com /partnerworld /wps /sizing /portal /sglist.jsp，網址提供之測試資料：

	PSAT file	PSAT file
Model/Feature:	x3250 M3-4251/22Y G1101 2260 2	x3250 M3-4251/22Y G1101 2260 2
Number of Systems:	1	1
xPerf:	67.50	67.50
Cores:	2	2
Sockets:	1 populated, 0 empty	1 populated, 0 empty
CPU Utilization:	3%	5%
Operating System:	Windows - Server 2003	Windows - Server 2003
Memory (MB):	352 of 16,384	363 of 16,384
Int. Disk Drives (arms):	3 of 8	3 of 8
Storage Capacity (GB):	156 of 1,196	229 of 1,196
Offering Family	IBM System x	IBM System x
Processor:	CELERON	CELERON
Processor Feature:	G1101	G1101
Clock Speed:	2260 MHz	2260 MHz

圖 478、Web 伺服器效能測試

對於 Web 應用，只需使用一般 PC Server (2 Core、4 GB RAM) 搭配虛擬化技術與負載平衡，可很容易的達到效能需求。

6.1.2.4.4. 試算資料庫伺服器數量

根據 http:// www-304.ibm.com /partnerworld /wps /sizing /portal /sglist.jsp，網址提供之測試資料：

	PSAT file	PSAT file
Model/Feature:	HS22-7870/A5Y E5603 1600 4-8	HS22-7870/A5Y E5603 1600 4-8
Number of Systems:	1	1
Cores:	4 cores of 4-8	4 cores of 4-8
Sockets:	1 populated, 1 empty	1 populated, 1 empty
CPU Utilization:	36%	38%
Operating System:	Windows - Server 2008	Windows - Server 2008
Memory (MB):	45,980 of 98,304	48,271 of 98,304
Int. Disk Drives (arms):	20 of 2(1)	20 of 2(1)
Storage Capacity (GB):	4,960 of 614(2)	5,207 of 614(3)
Offering Family	IBM System x	IBM System x
Processor:	Intel® Xeon	Intel® Xeon
Processor Feature:	E5603	E5603
Clock Speed:	1600 MHz	1600 MHz

圖 479、資料庫主機 TPC-E 值

對於一般企業應用，使用一般 PC Server(4 Core、32 GB RAM)搭配 Microsoft SQL Server，可很容易的達到效能需求。

6.1.2.5. 規劃說明

■ 防救災雲端集中化應用系統架構說明：

防救災雲端應用系統集中化採用三層式的應用服務架構，亦即使用第一階層的入口網站與網頁伺服器來提供防救災使用者網頁的操作界面服務，並搭配第二階層的應用程式伺服器來處理使用者的應用操作邏輯，最後使用第三層次的資料庫伺服器來存放防救災系統的資料，考量系統的高可用性，第一階層的網頁伺服器與第二階層的應用程式伺服器設計採用負載平衡(Load-Balanced)的架構設計，第三階層是資料庫伺服器，未來防

救災雲端集中化應用系統架構規劃說明如下：

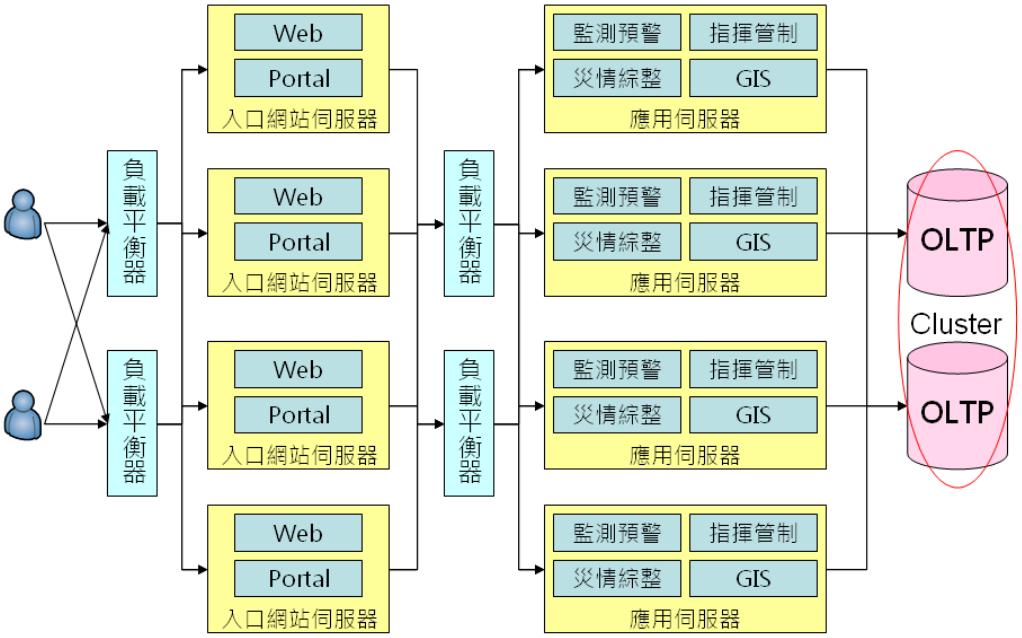

圖 480、大坪林中心防救災雲端集中化應用系統架構圖

■ 防救災雲端 OA 集中化應用系統架構說明：

防救災雲端 OA 集中化應用系統建議採用原兩層式的應用服務架構，亦即使用第一階層的應用伺服器來提供使用者網頁界面與應用操作邏輯，最後使用第二階層次的資料庫伺服器來存放 OA 的資料。考量系統的高可用性，第一階層的應用程式伺服器設計採用負載平衡(Load-Balanced)的架構設計，第二階層是資料庫伺服器，其中大坪林中心與兩個備援中心 OA 的資料庫規劃使用兩台資料庫伺服器來提供資料存取服務。未來防救災雲端 OA 集中化架構規劃說明如下：

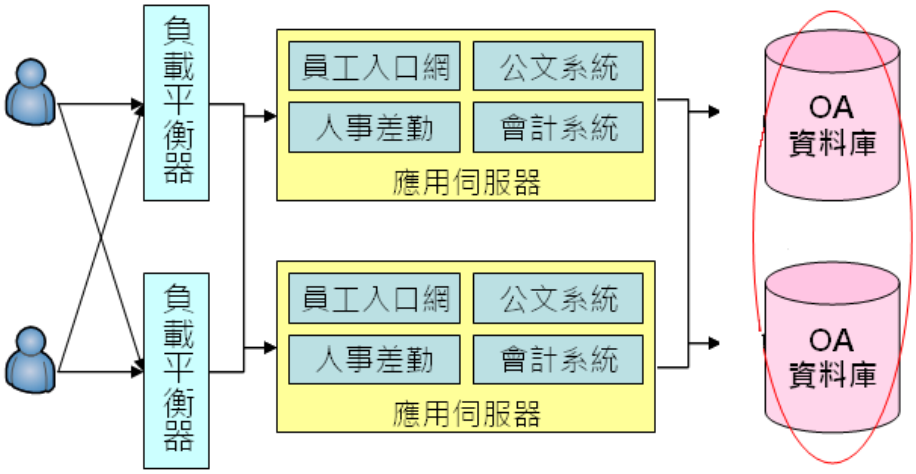

圖 481、大坪林中心防救災雲端 OA 應用系統集中化架構圖

■ 防救災雲端設備說明：

針對署內目前所做伺服器資料之收集，包括處理器使用率、記憶體使用率、網路及硬碟 I/O 封包等，並依照我們容機整體規劃步驟所設定容機系統效能目標，且參照國際第三方公正驗證單位(TPC-E，SPEC)的數據，作為未來評估導入主機虛擬化後，應採買伺服器隻數量及其所需效能等級之重要依據，以符合成本效益。將署內現有多品牌之主機統合為 PC Server 系列伺服器，於本案規劃為多台虛擬化伺服器主機，做為虛擬化移轉平台，並依據每部主機的應用特性進行記憶體與網路介面擴充昇級，除考量機房的主機管理外，更期望能將未來的機房建置為一個綠色節能環保的機房。在 IT 設備能源省電方面，建議透過虛擬化伺服器主機，以虛擬化軟體將現有實體主機整合為虛擬化環境。

除了辦公室應用系統、一般非主要應用系統的資料庫伺服器應納入虛擬化管理，以共享硬體資源，提高伺服器硬體使用率，並達成節能減碳，綠色環保之需求。

而防救災業務資料庫伺服器為了更進一步安全之考量則採單獨實體的建置方式，並透過叢集(Cluster)獲得更進一步的安全保障。

6.1.2.5.1. 虛擬主機

依 署系統運用系統分為 OA(消防)資訊系統及防救災業務資

訊系統，於虛擬化的管理建議，除了防救災業務資訊系統的資料庫伺服器及特殊的應用系統伺服器外,其餘皆將納入虛擬化管理。並建議虛擬化主機伺服器採用高可用性(HA)架構，測試主機及各縣市消防局的應用主機放置於備援虛擬化主機伺服器群內，以增加備援虛擬化主機伺服器群的可用性。

6.1.2.5.2. 實體主機

目前規劃防救災資訊系統資料庫伺服器，全國消防資訊系統資料庫、資料倉儲資料庫，採用叢集(Cluster)的實體主機，故共計六台，另外各地資訊中心各備有一台備份主機，兩台虛擬平台主控主機與雲端自動化管理主機採用實體主機。

6.1.3. 儲存設備

採用集中儲存方案，多個業務伺服器的資料要保存到集中存放裝置上，因此對設備的選型非常重要。可以參考以下點：

- 先進性

在儲存系統的設計過程中，充分依照國際上的規範、標準，儲存及備份設備採用標準的介面、規範和協定，借鑒國內外主流的網路儲存備份體系結構，使用國際上成熟的模式和最新的儲存及備份技術，以及業界領先的儲存產品，才能使網路儲存及備份系統的建設不斷地保持其技術與方案的先進性。

- 資料的安全性和系統的高可靠性

儲存系統負責完成對業務系統的業務連續性支援，對系統的可靠性有著很高的要求。作為該系統核心的儲存平臺的高可靠性則更是重中之重。儲存平臺的任何故障會造成巨大的影響。因此儲存平臺的資料安全性和系統高可靠性尤為重要。為了保證資料安全，除了建立可靠的資料儲存備份系統之外，建議採用國際上先進的設計方案和先進的軟、硬體產品。

- 系統的高性能

儲存系統要儲存大量的線上資料資訊，支援更多伺服器的線上業

務要求。由於總的資料量會很大，如何在這麼大資料量情況下滿足這麼多客戶機的併發訪問，整個儲存系統的性能也是一個非常關鍵的要求。而且網路容災備份系統也要支援不斷增加的資料流程量和儲存容量，以保證各種資訊的及時處理和可靠的完成，這要求網路儲存系統要具有足夠的容量，為了及時、迅速地傳送資料，網路存放裝置還必須具備高速處理能力，提供高速資料連結，保證系統高吞吐能力，滿足各種應用對數據傳送帶寬的需求，系統的性能應能很好的適應未來的擴充和擴展的需要。

- 系統的可擴展性/可擴充性

作為集中儲存的基本要求，儲存系統應能支援巨大的儲存容量，可以集中儲存不同平臺的企業資料，從而實現核心資料的集中儲存和集中管理。

隨著時間的推移、技術的發展以及環境的變化，業務系統的資料量會飛速增長，許多新業務系統會不斷產生，因此對儲存和容災備份系統的可擴展性有很高要求。需要充分考慮系統儲存備份容量空間的預留，同時隨著業務的發展，對儲存系統的可擴展性要求仍將非常迫切。這主要表現在對儲存和備份系統容量的平滑擴充以及對新的主機系統的平滑連接，以儘量減少對已有正常業務的影響。

- 靈活性和系統管理的簡單性

由於儲存及備份系統的資料量非常大，如何有效的管理大量的資料，包括資料備份/恢復，都對儲存系統的管理提出了巨大的挑戰。系統管理人員需要有高效的方法實現全面的儲存系統監控，包括即時資料性能監視、錯誤監測、錯誤狀態識別等等。另外作為集中的儲存平臺，由於前端需要連接的伺服器數量很多，如何在多個伺服器平臺之間對容量進行靈活的劃分和調度也是為儲存系統的管理提出了巨大的挑戰。

另外，儲存及備份方案除了要滿足當前應用系統的需要外，還要為未來的業務處理系統和資訊處理系統打下一個良好的基礎，必須考慮未來整個系統容災的現實需求，方案必須可以和已經建設的資訊基

礎架構完美結合，成為統一資訊基礎平臺。

- 價格合理性

建立儲存及備份系統的經濟性也是網路建設中的一個重要方面。經濟性需從兩個方面來考慮，首先是建立儲存、備份系統過程中的費用，同時還有系統建成後的維護費用和對投資的保護能力。因此在考慮使儲存、備份系統具有高性能的同時，還必須考慮投資的合理性，不能一味追求不切實際的先進性。在建設的過程中還需要考慮未來的升級能力和提供商的服務水準。

另外，儲存及備份方案除了要滿足當前應用系統的需要外，還要為未來的業務處理系統和資訊處理系統打下一個良好的基礎，必須考慮未來整個系統容災的現實需求，方案必須可以和已經建設的資訊基礎架構完美結合，成為統一資訊基礎平臺。

6.1.3.1. 二階式儲存架構

由上述諸多因素之考量結果，我們建議建置以 Storage 為核心的集中儲存架構需求，提供第一階及第二階儲存系統。將第一階磁碟陣列全量備份至第二階磁碟陣列，確保儲存系統之高可用性。而且為了不影響第一階儲存系統效能，建議儲存系統備份規劃以第二階儲存系統做為備份的原則。

提供第二階儲存系統做為第一階儲存系統之本地備援儲存系統，採用非同步模式 (Asynchronous)，將第一階儲存的系統資料(檔案系統及資料庫)抄寫一份至第二階儲存系統。透過資料複製軟體作業採用自動化機制進行，加強系統穩定度及減少人員操作負擔同時避免人為錯誤操作造成機制的異常，因此正常狀況下不需人員進行維運。因採用同步模式，故無資料遺失的疑慮，當第一階儲存系統完全無法使用時，主機連線快速切換至第二階儲存系統，無須切換至異地備援中心，日常本地端的備份也以第二階磁碟陣列為主，如此可不影響主系統端的效能，並可確保防救災資訊系統平台維運中心整體高可用性。

此外，所有規劃的儲存設備均需建立自動錯誤通報系統，若有異常狀態發生應立即產生錯誤通知，通知相關負責人員，進行進一步處

理，以保障異常狀況能在最短的時間內被排除。

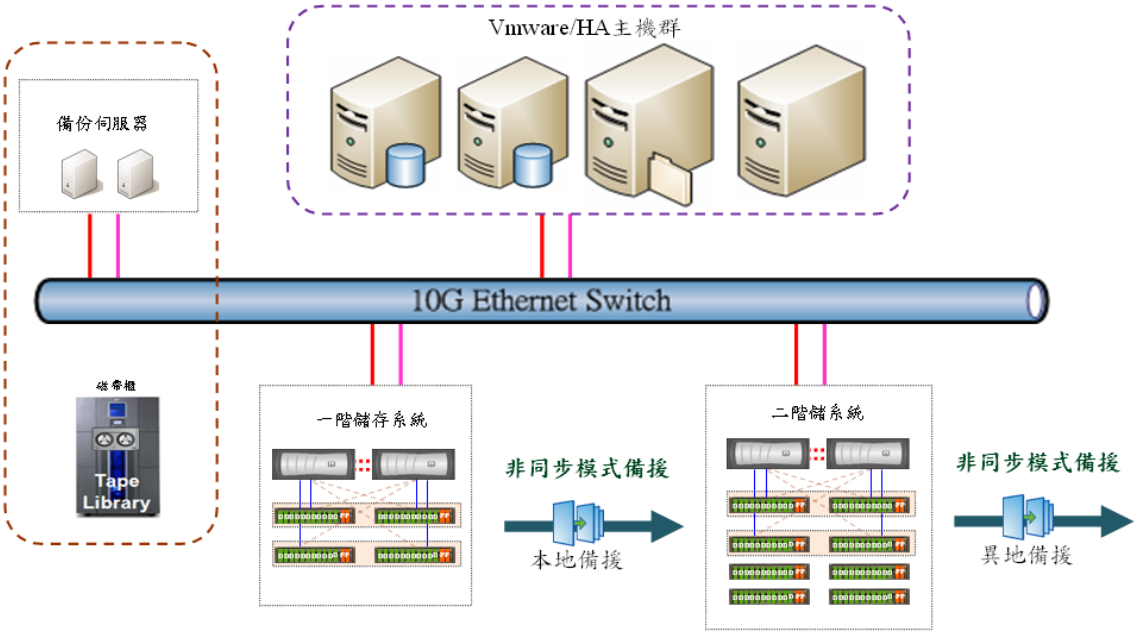

圖 482、二階式儲存架構圖

6.1.3.2. 儲存系統容量規劃

建議本案規劃之儲存系統建議採用 RAID 6 規劃可允許兩顆硬碟故障仍能提供服務，有效提昇資料安全性，並整合精簡配置(Thin Provisioning)與精簡刪除(Deduplication)功能，依實際系統所需容量進行配置並將重複資料刪除，提高儲存設備之使用效率。

透過 RAID 6 硬碟保護機制，可以確保儲存設備硬碟可以同時損壞兩顆硬碟，RAID 6 技術，可解決 RAID 重建期間，又發生另一顆硬碟故障的問題，也就是說可同時容許有兩顆硬碟故障且又能維持正常的運作，根據統計 RAID 6 的安全性比傳統的 RAID 4、RAID 5 高出 4000 倍。

雖然也有其他技術能同時容許兩顆硬碟故障(如 RAID0/1、RAID1/0)，但若仔細研究，這些技術都存有若干缺陷，如 RAID0/1、RAID1/0 要浪費多一倍的硬碟空間。

6.1.4. 虛擬主機

運用 VIRTUAL INFRASTRUCTURE 觀念，將伺服器硬體環境規劃成為 Computer Hardware Resources Pool(簡稱 C.H.R.P.)，新建系統都

在這個 Computer Hardware Resources Pool 中提供硬體資源需求，既有系統也應逐步導入 Computer Hardware Resources Pool，並可將既有伺服器硬體資源納入管理，共享硬體資源。

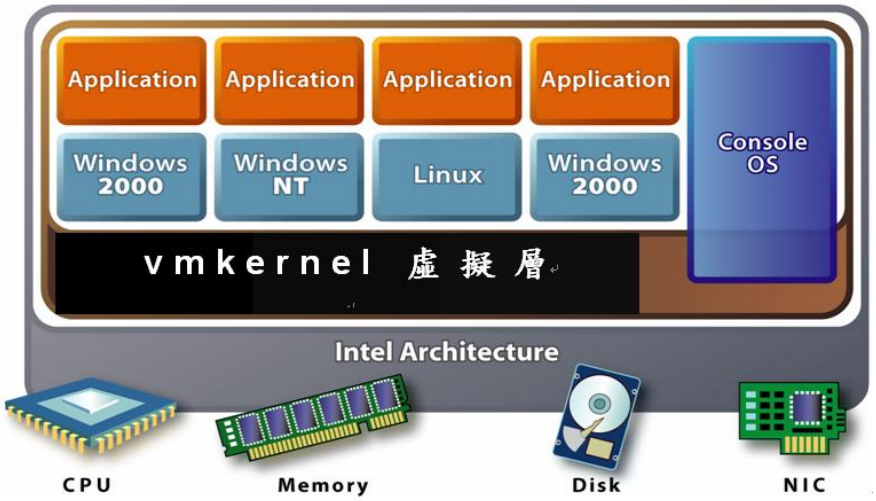

圖 483、虛擬化架構示意圖

6.1.5. 網路架構

6.1.5.1. 目標及需求概述

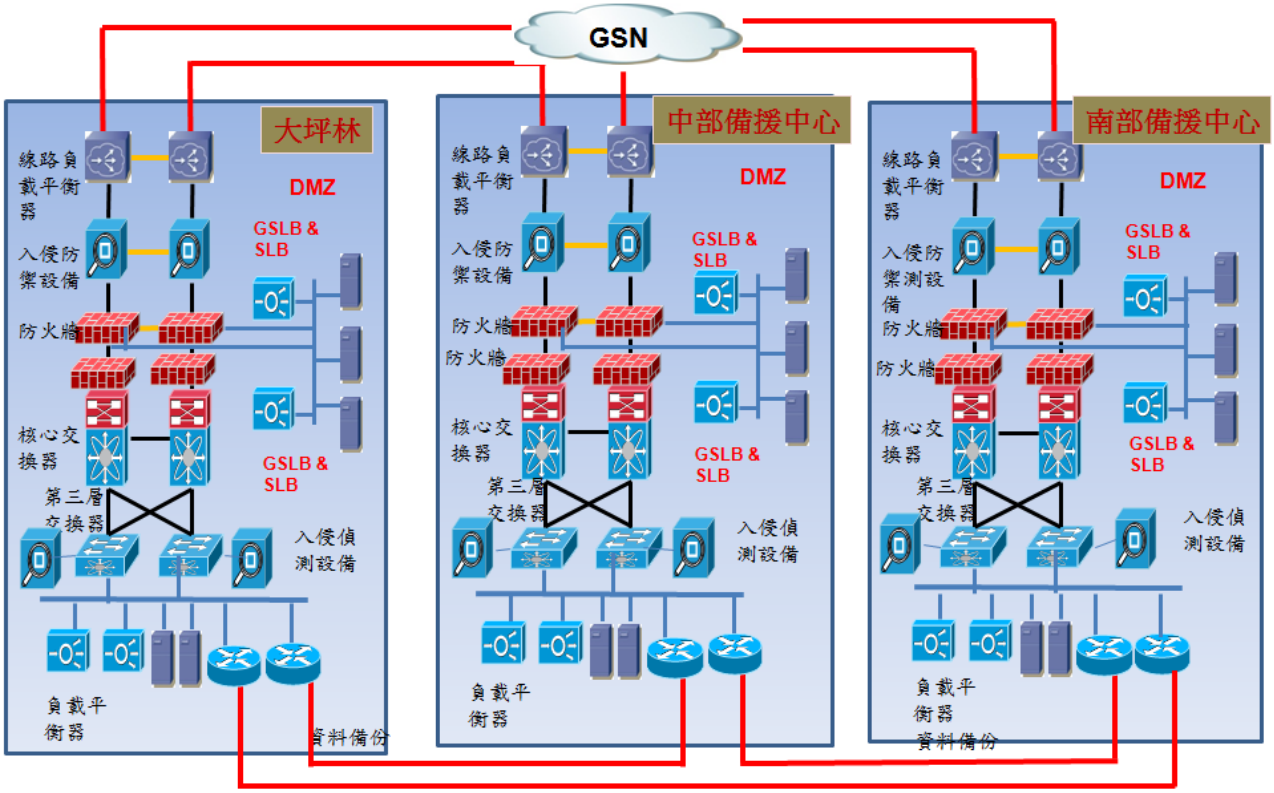

圖 484、整體網路架構示意圖

消防署防災雲端資料中心專案網路設備與架構設計目標為「可靠性(Reliability)」、「安全性(Security)」、「可擴充性(Scalability)」、「簡化管理(Simplicity)」與「效能提升暨彈性調整」。以下分別說明各個目標之需求與目的。

- 可靠性(Reliability)

對於雲端資料中心來說，可靠性是進行本專案網路設計的基本需求。可靠性是指一方面要保證導致網路不可用的設備故障時間極短，另一方面，還要保證網路能夠滿足遠端資料傳輸的需求，不會因性能下降而導致不可接受的回應時間。為達到可靠性的目標網路設計中要把先進的技術與現有的成熟技術結合起來，充分考慮到現狀和未來發展趨勢。可靠性網路設計中將採用高可靠性的網路產品和完備的網路備援機制來滿足可靠性的要求，對於不同層次的設備和線路進行不同級別的可靠性設計，使網路具有故障自癒的能力。本專案中的網路設備與設計網路架構能提供本專案可靠性與故障自癒能力。

- 安全性(Security)

憑藉核心網路區設備提供的廣泛安全特性，可在網路層保護重要資訊，防止未授權人員接入網路，確保私密性及維持不間斷運行。

為防止 DoS 攻擊和其他攻擊，可用 ACL 根據來源和目的地 MAC 位址、IP 位址或 TCP/UDP 埠進行區隔分組，從而嚴格管理網路的連線互通與接取。並提供 SSHv2 和 SNMPv3 功能可以對設備登入管理和網路管理資訊加密，保護網路管理封包避免遭干擾或竊聽。並提供 TACACS+或 RADIUS 支援能力，實現了核心網路設備的集中訪問控制，並限制未授權使用者改變設定配置。此外，可在網路設備上限制不同管理權限人員分配不同存取權限分級的能力。

- 可擴充性(Scalability)

業務的發展對網路的需求是不斷變化的，網路應用系統為了

滿足這些需求也會隨之變化。面對不斷變化的情況和需求，網路應當能夠作出快速和有效的反應。因此，網路必須具備良好的可擴展性，應支援核心業務系統的不斷擴展，適應未來業務的發展和變化。同時，網路結構應當能夠變化，具有靈活的伸縮能力，網路設備可以擴充和升級。

- 簡化管理(Simplicity)

隨著網路規模的不斷擴大和網路的不斷複雜，網路的維護量隨之增加。整個網路的可管理性變得尤其重要。因此網路系統應當具有統一的可管理性，不僅可達到對網路設備的管理，同時可掌握網路現況及網路設備及線路效能趨勢，以供網路未來成長規劃。

- 效能提升暨彈性調整

消防署的重要工作之一為防災與救災，本專案建置的系統在因應這樣的需求前提下，需提供最佳效能提升暨彈性調整功能，本專案採用的解決方案可以提供一個未來可擴充校能與彈性調整的架構，也就是未來擴充性與相容性，並建立一個開放式，遵循國際標準的網路系統。對於本專案網路、儲存設備、伺服主機等設備的網路連線均採用標準的網路協定 (如 IEEE 802.3ad LACP) 及介面電氣標準，這樣的產品與設計都將符合在台灣所應用的國際標準，為將來的擴充消除任何不必要的產品隔閡與障礙，並能確保未來效能的提升與彈性調整需求

6.1.5.2. 所採行之技術、方法及工具

本專案之雲端資料中心解決方案，隨時以最新、最專業的科技因應客戶需求與技術支援趨勢的變化，並針對消防署的不同需求提供協同運作(Collaboration)、數據中心 (Data Center)、安全 (Security)、行動 (Mobility)、網路系統 (Network Systems)、與商業視訊 (Business Video) 等六大類型解決方案，除了滿足消防署追求效率和經濟效益的目標，也同時兼顧未來升級的需求。

本專案建議之雲端資料中心系統解決方案，具備以下特色：

- 落實綠色機房、綠色 IT 與網路的解決方案。
- 雲端資料中心解決方案是消防署防災中心所有服務與應用的基礎，可與現有網路架構及軟體等結合成智慧型整合式網路，滿足未來的需求，包含：
  (1) 提供高可靠性(Reliability)的網路與各式相關設備
  (2) 網路與各式系統建置時優先考量網路安全性(Security)
  (3) 網路相關設備具備有優異的軟硬體擴充性(Scalability)
  (4) 提供網路相關設備的模組式擴展與整合性管理功能(Simplicity)
  (5) 提供網路相關設備的效能提升暨彈性調整能力

6.1.5.3. 未來整體架構

未來消防署主要資料中心網路架構示意圖如下：

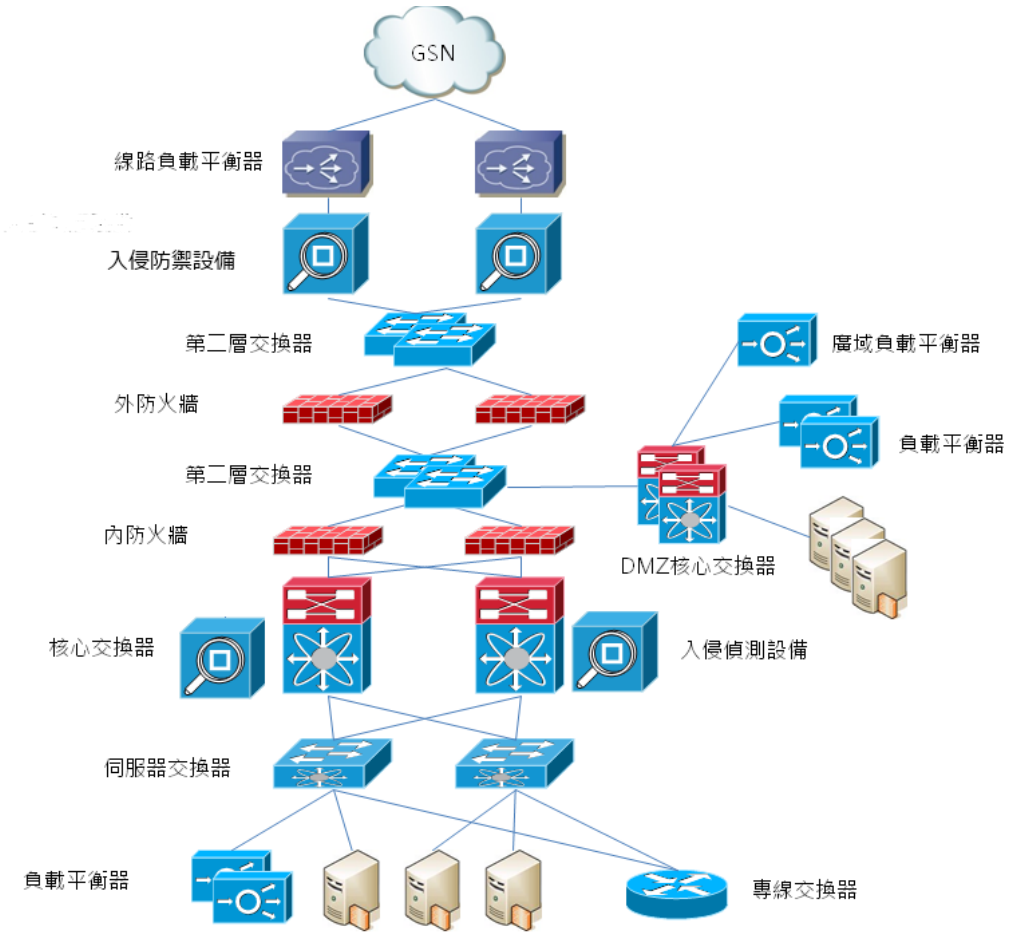

圖 485、未來消防署主要資料中心網路架構圖

消防署主要資料中心整體架構分成 4 區：Internet 線路區、DMZ 區、核心網路區、備份線路區。Internet 線路區為資料中心入口，使用雙線路確保資料中心對外服務不中斷。DMZ 區為消防署防災雲端資料中心防救災相關系統 Web Server 入口網。核心網路區包含核心網路設備、測試主機、管理主機、AP Server 及 DB Server。備份專線區為規劃主中心與異地備援中心資料同步線路。

- Internet 區規劃

對外線路及 VPN 線路，建議採用 GSN 所提供之線路服務，以降低線路成本，透過 GSN 連接消防署其他雲端資料中心、所屬各單位及 Internet。

一般民眾可透過 Internet 進入消防署防災雲端資料中心，並可依照民眾上網電腦所在地的網路 IP 資訊自動連接至最近的消防署防災雲端資料中心。

- DMZ 區規劃

DMZ 區為消防署防災雲端資料中心防救災相關系統 Web Server 入口網。Web Server 透過負載平衡器作負載平衡，可避免單一台 Web Server 故障，造成服務中斷之問題。Internet 使用者查詢防救災相關系統資料時，需透過 DMZ 區 Web Server 存取核心網路區之 AP Serve 及 DB Server，因應網路安全的考量，不允許一般使用者直接存取核心網路區。

- 核心網路區規劃

消防署防災雲端資料中心核心網路區包含叢集式架構之 AP Server 及 DB Server。相關系統 Web Server 在 DMZ 區。核心網路區因放置重要且具機密性的資料，因此不直接開放給使用者存取，必須透過 DMZ 區的 Web Server。 位於核心網路區的 AP Server 及 DB Server 同樣也利用負載平衡器作負載平衡，確保防救災服務不中斷。

- 備份線路區規劃

規劃資料同步專用線路，使用專線路由器連接 FTTB 100Mb

乙太網路，分別為北、中、南三區消防署防災雲端資料中心資料同步專用。

異地備援中心的整體架構與主要資料中心相同，當主要資料中心發生異常時，服務系統會切換到異地備援中心，

異地備援中心網路整體架構示意圖如下：

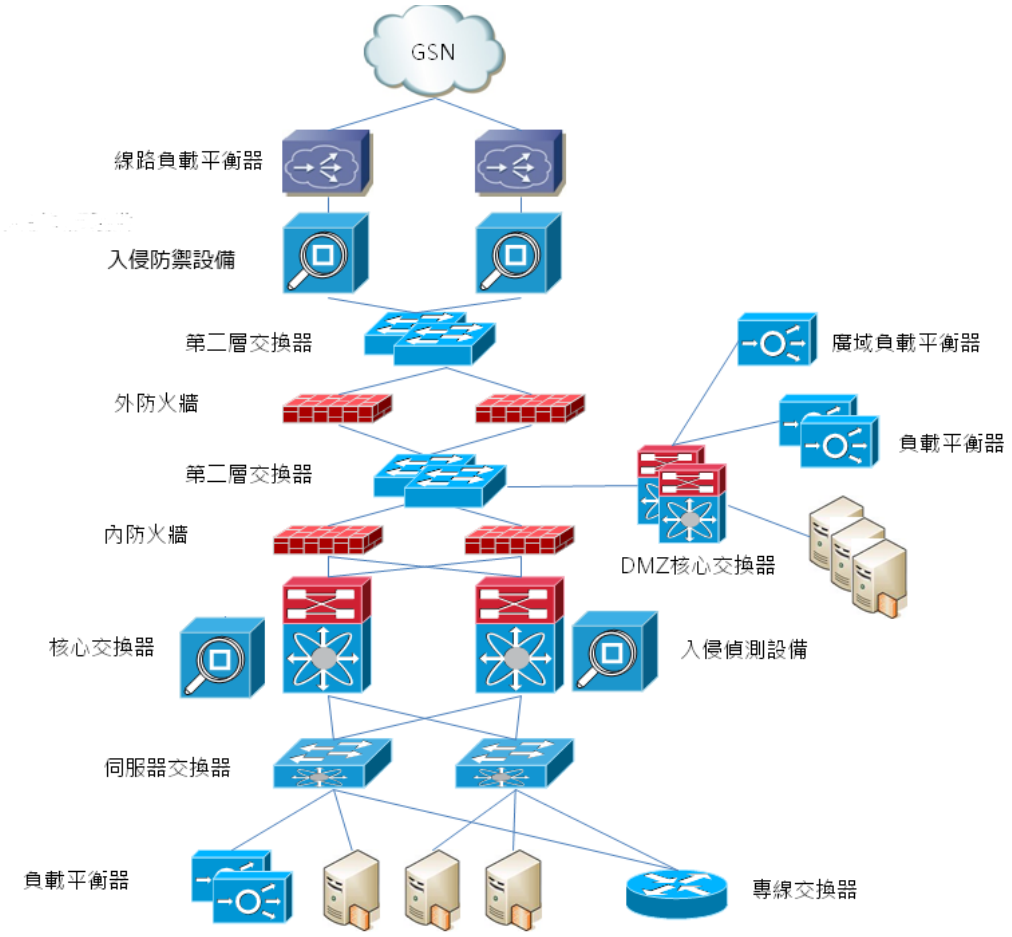

圖 486、異地備援中心網路整體架構示意圖

6.1.5.4. 整體架構

消防署防災雲端資料中心主中心與異地備援中心皆採用標準化的架構，如此設計將可大幅簡化管理工作的複雜度，管理流程、教育訓練的一致性，提升管理的效率。因為三中心的架構一致，在資料中心的備援切換工作也將能化繁為簡。

- Internet 區

消防署防災雲端資料中心所規劃的對外線路及 VPN 線路，建

議採用 GSN 所提供之線路服務，以降低線路成本與更有效率的政府機構間互相連線。

為落實存取控管及降低網路連線斷線造成服務中斷的風險、CE 及 PE 端設備故障等問題，建議建置二條 100Mb 乙太網路線路。二條 100Mb 乙太網路可同時提供服務並互為備援，故實際可使用頻寬為 200M，提升線路的使用率。

由於 Internet 規劃二條 Internet 線路，因此規劃建置線路負載平衡器監控 Internet 線路的可用性和性能，管理 Internet 線路的雙向流量，從而提供高度的容錯性和線路的優化。

消防署防災雲端資料中心所規劃的廣域附載平衡器提供北、中、南三個區域使用者取得最近、最快的服務，由於全球伺服器負載平衡可依據使用者 IP 網段選擇最近或回應最快的伺服器及避免發生問題的資料中心，令使用者能夠獲得最佳服務。任一資料中心發生問題時，其他資料中心可以立即且完全取代現有的功能，為資訊管理者能專心處理問題，不被煩人的電話浪費處理問題的時間，加速問題的解決。

- DMZ 區

DMZ 區為消防署防災系統 Web Server 入口網，建立多個 Web Server 並透過兩台伺服器應用負載平衡器作負載平衡，並可避免單一台 Web Server 或伺服器負載平衡故障，無法繼續提供服務之問題。

- 核心網路區

網路為應用系統最底層的通訊元件，當網路發生中斷時，主機與系統雖規劃高可用性架構，仍然會降低系統的可用率，嚴重時將會造成無法達成服務水準。為避免網路中斷造成系統無法使用，未來各消防署防災雲端資料中心核心網路架構的規劃原則如下：

◆ 避免單點失效

為避免單點失效發生，所有線路、重要網路連線設備及

VPN 皆設計備援機制。

◆ 易於管理

基於容易管理及簡化異地備援啟動作業，網路架構的規劃，將以系統存取觀點代替系統所在位置為考量,規劃未來北、中、南三區消防署防災雲端資料中心存取系統的網路架構一致，統一資料流路徑，使流量易於控制及監控。

◆ 高傳輸效能

備援網路採對稱式架構設計，流量經過備援網路之節點與頻寬與主要網路相同，線路備援兼具效能傳輸。

◆ 節能減碳原則

核心網路區主要網路具備虛擬化功能，防火牆及核心交換器皆可將實體設備模擬成多套的虛擬設備，將可降低機房使用空間,使用電力、冷卻系統、線路成本,達到節能減碳的目標。

規劃中也將各資料中心相互連接之點對點專線，連接至 GSN VPN，由於所有線路皆連至 GSN 機房，可減少各資料中心連線之設備數量，進而減少電力使用，可符合節能減碳潮流。

本專案網路架構上建議採取標準化，統一化與模組化之設計原則，以符合未來管理上的一致性與安全性。核心網路須按照安全等級劃分區域，建置防火牆與入侵偵測防禦系統(IPS&IDS)之防護機制。防火牆、入侵偵測防禦系統與資料中心核心交換器等設備皆採行具高度可用性之雙機備援機制(HA)。

消防署防災雲端資料中心為消防署重要資料與服務主機所在地，因此在建置此區塊網路時會以網路安全性、服務可靠性及存取效率做為設計該區塊之首要考量。 核心網路區規劃架構圖如下圖所示：

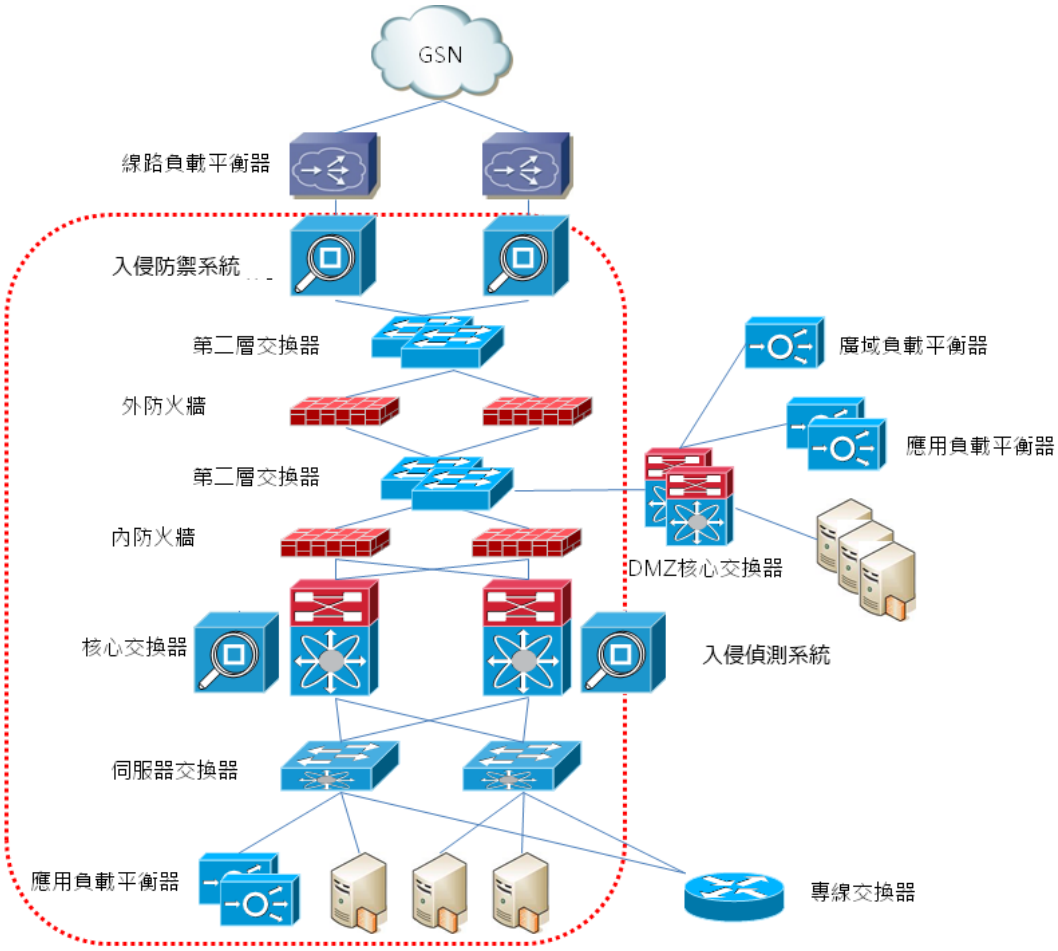

圖 487、核心網路規劃架構圖

消防署防災雲端資料中心之核心網路實體連線圖由上而下依序為入侵偵測防禦系統 、外防火牆、內防火牆、核心交換器、伺服器交換器及應用負載平衡器。

- 資料備份網路區

資料備份網路區為消防署防災系統非常重要的資料庫互相連線，提供資料庫間進行同步及備份，也是全球伺服器負載平衡(GSLB)的基礎，因每一個使用者皆需獲得最新且一致性的資料，使用者更新資料後也必需立即更新北、中、南三地的資料庫，另外北、中、南三地的資料庫於一定的時間必須進行資料全面同步，確認北、中、南三地的資料庫的已達到一致性與資料內容同步的比對。建議以 100Mb 乙太電路三條與北、中、南三地的資料庫互連形成環狀，使得資料庫的資料同步及傳送有不受干擾的頻寬與

備援電路。

6.1.5.5. 網路架構說明

以下針對網路架構設計作細部說明

6.1.5.5.1. Internet 入口規劃

- Internet 線路 load sharing & failover 說明

利用線路負載平衡器的 Dynamic DNS 功能供 DNS 名稱的解析，令使用者依據 DNS 名稱的解析的 IP 透過不同的 Internet 連線至伺服器，如此可提供 Internet 線路有效的運用且同時避免有問題的電路。兩條 100M 乙太電路可同時被使用，又可依其使用率去選擇較低者進行連線存取伺服器，避免網路擁塞。使電路獲得充分使用並降低營運成本。

6.1.5.5.2. DMZ 區

- Global Server Load balancing 說明

消防署防災雲端資料中心所規劃的廣域負載平衡器提供北、中、南三個區域使用者取得最近、最快的服務。優點如下:

(1) 確保應用服務可得性:

協助消防署建立一套穩固的災難備援與業務永續計畫，確保使用者永遠都能順利連接伺服器，不論該應用服務是否執行中。另外，能夠針對整個基礎建設進行詳細的健康檢查，將停機時間降至最低，在應用層上為每位用戶偵測應用服務的健康狀態，以改善用戶的使用經驗。

(2) 取得全球應用交付流量的控制:

每種應用服務與業務需求均各自不同，您可以自訂動態分散全球流量的政策，根據業務需求與應用的效能/可得性導引使用者至正確的網站主機。

(3) 增加應用服務效能:

不只是簡單將使用者流量導引至可以用的伺服器而已，廣域負載平衡器以動態判斷，讓消防署將使用者流量導引至最好用的伺服器。它使用各種不同的負載平衡演算法與

智慧型監控每一個特定應用服務與使用者，將根據消防署的業務政策與即時網路/使用者狀態如地理位置等資訊，導引使用者流量。同時，廣域負載平衡器提供應用服務協定持續連結功能，可消除破碎的連線階段與錯誤資料。

- 應用負載平衡器

DMZ 區為消防署防災系統 Web Server 入口網，建立多個 Web Server 並透過兩台應用負載平衡器作負載平衡，並可避免單一台 Web Server 或伺服器負載平衡故障，無法繼續提供服務之問題，多台 Web server 分散連線數量及提高處理，當單一 Web server 發生故障時，應用負載平衡器會偵測 Web server 服務狀態將會停止分配連線故障的 Web server，直到故障的 Web server 修復。優點如下:

(1) 為成長做好準備，避免任何停機時間:

規劃應用負載平衡器，即配至最先進的負載平衡與應用服務狀態監控功能。應用負載平衡器讓您能夠輕易增加實體或虛擬伺服器，當網路裝置或伺服器出現錯誤時，可將流量導引至其他設備。應用負載平衡器的高速效能確保您的網路架構保有成長空間。

(2) 加速應用服務達到數倍效能:

應用負載平衡器可減少網路流量，並將用戶端連線的瓶頸如 WAN、LAN 與網際網路延遲所造成的影響降至最低，為應用服務加速達到數倍效能，或是安裝廣域網路最佳化與 HTTP 加速等模組，增加您其他應用服務的效能。

(3) 保護應用服務與資料安全無虞:

從堅實的網路與協定分層安全性到應用服務攻擊過濾，應用負載平衡器可佈署安全服務套件，保護最重要的應用服務安全無虞。通訊協定、訊息與應用服務防火牆附加模組則能提供進階的安全保護。

(4) 減少伺服器、頻寬與管理成本:

先進的 TCP 連線管理、TCP 最佳化與伺服器卸載(offloading)功能，為現有的網路基礎建設進行最佳化，並提高使用率，將近可增加數倍的伺服器效能，減少頻寬費用。應用負載平衡器將安全、加速與高可得性功能整合在單一平臺中，幫助簡化系統管理工作。當僅需更少的伺服器、頻寬、電力與冷卻系統時，也節省了管理網路基礎建設的時間，有效降低營運費用。

- DMZ 核心交換器

DMZ 核心交換器用於連接 DMZ 區的應用負載平衡器、廣域負載平衡器及 Web Server。DMZ 區核心交換器是與核心網路區核心網路交換器同一實體交換器利用創新技術所模擬出的虛擬交換器。

DMZ 核心交換器是一個模組化資料中心級交換器,可提供高密度的 Gigabit 乙太網路連接傳統的伺服器，亦可提供高密度之 10Gb 網路介面連接新一代伺服器，適用於高度可擴展的 10GE 乙太網網路。

DMZ 核心交換器建立在一個成熟的作業系統上,借助不中斷的特性提供了即時系統升級，以及出色的可管理性和可維護性。它的創新設計專門用於支援點對點的資料中心連接，將 IP 的連接、存儲體的連接和伺服器的連接整合到單一乙太網路交換機上。

在傳統的 Data Center 網路中，通常配置二部核心交換器採用 Active-Standby 模式互相備援，但同時間只有一部核心交換器在運作，且同時因為 Layer 2 Spanning Tree 機制的收斂結果，將有一半的線路會無法使用。

在 DMZ 區網路中，規劃配置二部 DMZ 心交換器採用 Active-Active 模式互相備援，同時運用 DMZ 核心交換器提出的 Virtual Port Channel (vPC)的創新技術讓二部 DMZ 核心交換器成為一部具有 Active-Active 模式備援機制且能夠使用所

有頻寬的虛擬核心交換器，在簡單的設定及簡化的維運管理下，提供服務不中斷的新一代資料中心。

6.1.5.5.3. 核心網路區

消防署防災雲端資料中心之核心網路實體連線圖由上而下依序為防火牆、入侵偵測防禦系統、最後進到核心交換器及 Server 交換器。

- 防火牆 (Firewall)

防火牆設置的主要目的是以管制網路流量的方式，達到應用系統存取管控的目的。因此規劃核心網路架構時，在防火牆機制的設計上，任何來自資料中心外部流量，均為不可信任的來源，故建議防火牆設計採用二層設計，並採用不同廠牌，加強網路安全防禦。

設計二層防火牆的原因在於，各廠牌防火牆其設計上均有尚未發現的弱點，若僅採用單一防火牆，或採用同一廠牌，則當該廠牌防火牆的弱點遭攻破時，受管制保護的區域，即面臨嚴重的威脅。

而二層防火牆配置不同廠牌的防火牆，各層防火牆以相同廠牌防火牆採用 Active-Standby 模式互相備援，提供單一的管理者操作介面，防火牆之設定及 session 狀態會由 Active 防火牆自動同步至 Standby 防火牆。在簡單的設定及簡化的維運管理下，提供服務不中斷的新一代資料中心防護機制。

以防火牆作為消防署防災雲端資料中心的安全防護，防火牆提供了多種網路威脅防範的功能，可以在網路攻擊散布開來前就予以有效阻擋，並可以有效控制網路活動與應用程式的流量，並可以擴充提供彈性的 VPN 連線功能。這樣的一個多功能強大的網路安全設備，可以提供資料中心網路環境寬廣且深入的網路安全防護，同時也可以降低整體的建置、營運、維護成本，及減低網路安全設備運作的複雜度。

建議防火牆設備需專為資料中心所設計的高度擴充介面、

高速封包處理效能，更具備了虛擬化功能，一部實體防火牆多可模擬成多部虛擬防火牆，讓資料中心在未來擴充時具備更豐富的選擇與彈性。

另外建議防火牆設備需提供更有效果與效率的安全防護功能，同時也透過以下關鍵元件提供設備的投資保障：

- 經過市場驗證的安全與 VPN 功能:

除了全功能、高效能的防火牆外，另外可支援 IPS 入侵防禦、Anti-Virus 內容安全管理功能，以上這些網路安全功能，可以提供應用程式安全防護，使用者與應用程式存取控制，減緩蠕蟲與病毒的擴散，惡意程式防護，內容過濾及遠端使用者連線等多樣化應用。

- 可擴充服務基礎架構：

藉由防火牆的服務處理模組與安全策略框架的優勢，使用者可以依據每一個資料流特性給與特定的網路安全管理，並藉由高效率的流量處理能力提供各式網路服務獨立的策略管控與保護，提供了高度的網路安全管理策略彈性與擴充性，協助消防署在這瞬息萬變的資安威脅中得到應有的保護。

- 降低建置與營運成本：

本防火牆設備提供平台、設定、管理標準化功能，協助消防署在佈建大量設備時降低建置成本及後續的維運成本，預期將可大幅度降低管理人員之維護管理負擔。

- 入侵偵測系統

本專案規劃之入侵偵測安全平台完全符合消防署防災雲端資料中心對即時安全的需求，提供 Multi-Gigabit 的效能，以及整合式的企業級網路與系統安全防護能力。智能導向型安全性能協助消防署自動管理風險，並且符合法規遵循要求的目標，同時能強化運作效率與降低 IT 支出。

入侵偵測系統整合式的防護，可以廣泛保護消防署防災雲端資料中心資產、提供最大的可用性，使所需擔負的責任和安

全成本降到最小。高準確的防護技術則內含了可以阻擋大多數威脅與攻擊的防護能力：

- 零時差攻擊、網路攻擊與惡意軟體
- 動態式網路存取控制(Network Access Control)，阻擋未驗證或未符合安全規範的機器以降低威脅
- VoIP 的威脅與弱點
- 阻斷服務 (DoS)、分散式阻斷服務 (DDoS) 與 SYN flood 攻擊
- 加密式攻擊、蠕蟲、木馬程式與繞道攻擊
- 即時通訊與點對點應用程式
- 以通訊協定為基礎的動態速率限制
- 基礎架構的服務品質
- 整合式的智慧型網路與系統安全

建議本專案規劃之入侵偵測系統提供整合式的智慧型網路與系統安全能夠提供即時的安全保護，不僅能自動進行，還可以回應操作。並可以立刻從智慧型 IPS 取得關鍵主機、主要主機入侵與間諜軟體攻擊，以及準確的威脅與風險關聯性資訊。即時安全解決方案能協助進行即時安全的決策，讓消防署防災雲端資料中心可以

- 更快獲得保護：

  具備系統感知能力的終端防護中控平台整合、內建主機隔離功能，並且實施可調整速率限制

- 更快獲得信心

  透過按鍵即可獲得弱點掃描與管理的支援、內建主機隔離功能並且實施可調整速率限制

- 減緩部署更新與強制政策的急迫性

  有了堅強的弱點保護能力，您可以好整以暇地驗證與部署更新，保護系統不受風險的危害。

- 可實施速率限制

即時、可實施的速率限制功能能讓您簡單、有效地控制您的網路頻寬，同時 阻擋不需要與危險的應用程式

◆ 完整的威脅防護

主動保護端點與關鍵網路基礎架構的安全，阻擋已知威脅、零時差攻擊、DoS 與加密攻擊等，以及間諜軟體、VoIP 弱點、IM、傀儡程式、網路蠕蟲、惡意軟體、網路釣魚、木馬程式與 P2P 應用程式等的威脅

◆ 入侵偵測系統策略

透過入侵偵測系統策略，消防署防災雲端資料中心可以切實地對抗網路的安全威脅。以效果卓越的技術來提供特定攻擊與弱點所需的防護。

- 核心交換器

建議核心交換器是一個模組化資料中心級產品系列，適用於高度可擴展的 1GE 及 10GE 乙太網路，其交換核心的速度能擴展至 15Tbps 以上。它的設計旨在滿足大多數資料中心的需求，提供不中斷的系統運作和綠色節能的虛擬化服務。且核心交換器建立在一個成熟的作業系統上，借助不中斷的特性提供了即時系統升級，以及出色的可管理性和可維護性。

在傳統的核心網路中，通常配置二部核心交換器採用 Active-Standby 模式互相備援，但同一時間只有一部核心交換器在運作，且同時因為 Layer 2 Spanning Tree 機制的收斂結果，將有一半的線路會無法使用。

在核心網路區網路中，建議配置二部核心交換器採用 Active-Active 模式互相備援，同時運用 Virtual Port Channel (vPC) 的創新技術讓二部核心交換器成為一部具有 Active-Active 模式備援機制且能夠使用所有頻寬的虛擬核心交換器，在簡單的設定及簡化的維運管理下，提供服務不中斷的新一代資料中心。

在傳統的 Layer 2 網路中 Loop 是最重要的問題之一，許

多的協定或管理機制的提出就是為了要預防及解決 Loop 的發生，Spanning Tree Procotol 就是其中的代表。Spanning Tree Protocol 的基本原則是不管二部網路交換之間有多少條 Link，只有一條 Link 是 Active 的，如此才能避免 Loop 的發生。

也由於 Spanning Tree Protocol 的特性產生二個問題：

- 在 Layer 2 網路中至少有一半的線路頻寬是無法使用的。
- 當 Loop 的發生而使得 Spanning Tree 重新計算時，會造成整個資料中心網路暫時無法運作。

本建議方案是可以徹底解決 Layer 2 環境 Loop 的創新解決方案。核心交換器採用 vPC(virtual Port Channel)網路虛擬化技術，將二部實體核心交換器邏輯上視為一部具備高容量的交換器。

如下圖所示，SW1 及 SW2 使用虛擬化技術連接後，SW3、SW4 就邏輯上將 SW1 和 SW2 視為一部交換器，因此 SW3 或 SW4 與 SW1、SW2 連接的 UPlink 就可設定為 PortChannel，所以 Switch 之間的 Layer 2 環境將不會有 Loop 的存在，而 Uplink 的可使用頻寬也因為設定為 PortChannel 而加倍。

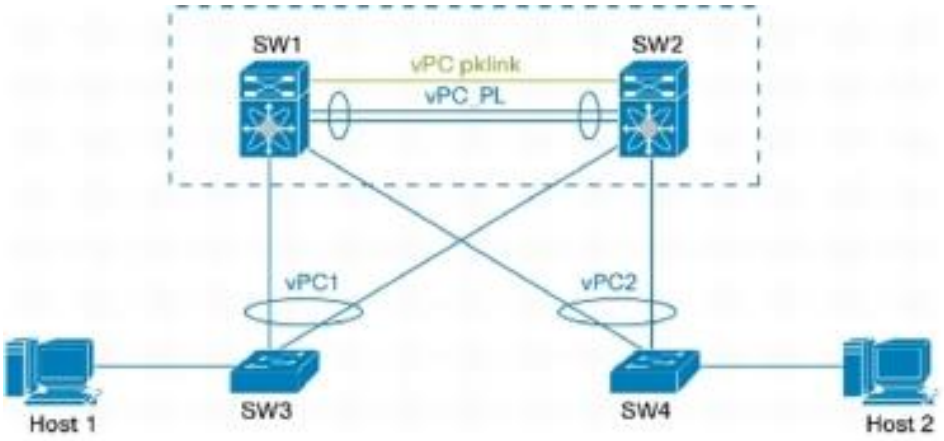

圖 488、Layer2 環境 Loop 創新解決方案示意圖

二部實體核心交換器虛擬化成為一部核心交換器提供消

防署防災雲端資料中心的重大效益如下：

- ◆ 提高資料中心網路平台的高可用性
- ◆ Loop Free 的 Layer 2 網路平台
- ◆ 所有頻寬可皆可善加利用
- ◆ 完善且快速的備援機制

- Server 交換器

建議資料中心之 Server Fram 規劃的 Server 交換器提供高密度 10GbE 與 Fiber Channel 接取介面，所有的 10GbE 接取介面更可以透過軟體升級方式，升級至 FCoE(Fiber Channel over Ethernet)介面，讓 Server Fram 可以保有未來擴展與應用的彈性。

除了高密度的 10GbE 與 Fiber Channel 接取介面需求外，還有大量的伺服主機是採用 1GbE 的接取介面，而高密度的 1GbE 可以透過 Server 交換器的外接擴充模組提供，外接擴充模組的管理控制介面是整合在 Server 交換器上，就外觀來看 Server 交換器及外接擴充模組是獨立的網路設備，但是實際上二者的互連整合提供使用者一個虛擬機箱管理擴充模式。

Server 交換器就像是機箱式交換器的管理控制模組；外接擴充模組如同機箱式交換器的網路介面擴充模組，透過這樣的虛擬機箱擴充模式可以提供高密度之 1GbE 接取介面給大量的伺服主機，同時透過 Server 交換器將提供給本專案儲存設備與伺服主機等網路接取設備高可用性、高頻寬之 Ethernet 與 Fiber Channel 接取介面。

- 應用負載平衡器

本專案規劃 AP Server 放置於核心網路區中心，由於核心網路區配置防火牆、入侵偵測防禦設備、及核心交換器等多重安全防護設備提供了多種網路威脅防範的功能，可以在網路攻擊散布開來前就予以有效阻擋，並可以有效控制網路活動與應用程式的流量。

一般使用者無法直接存取 AP Server，必須透過 Web Server 來存取。AP Server 也如同 DMZ 區的 Web Server 使用兩台應用負載平衡器作負載平衡，並可避免單一台 AP Server 或應用負載平衡器故障，無法繼續提供服務之問題，多台 AP server 分散連線數量及提高處理，當單一 AP server 發生故障時，應用負載平衡器會偵測 AP server 服務狀態將會停止分配連線故障的 AP server，直到故障的 AP server 修復。

使用應用負載平衡器的優點如下:

◆ 為成長做好準備，避免任何停機時間:

規劃應用負載平衡器，即配至最先進的負載平衡與應用服務狀態監控功能。應用負載平衡器讓您能夠輕易增加實體或虛擬伺服器，當網路裝置或伺服器出現錯誤時，可將流量導引至其他設備。應用負載平衡器的高速效能確保您的網路架構保有成長空間。

◆ 加速應用服務達到數倍效能:

應用負載平衡器可減少網路流量，並將用戶端連線的瓶頸如 WAN、LAN 與網際網路延遲所造成的影響降至最低，為應用服務加速達到數倍效能，或是安裝廣域網路最佳化與 HTTP 加速等模組，增加您其他應用服務的效能。

◆ 保護應用服務與資料安全無虞:

從堅實的網路與協定分層安全性到應用服務攻擊過濾，應用負載平衡器可佈署安全服務套件，保護最重要的應用服務安全無虞。通訊協定、訊息與應用服務防火牆附加模組則能提供進階的安全保護。

◆ 減少伺服器、頻寬與管理成本:

先進的 TCP 連線管理、TCP 最佳化與伺服器卸載(offloading)功能，為現有的網路基礎建設進行最佳化，並提高使用率，將近可增加數倍的伺服器效能，減少頻寬費用。應用負載平衡器將安全、加速與高可得性功能整合在

單一平臺中，幫助簡化系統管理工作。當僅需更少的伺服器、頻寬、電力與冷卻系統時，也節省了管理網路基礎建設的時間，有效降低營運費用。

6.1.5.5.4. 備份專用線路規劃

建議以 100M 電路三條與北、中、南三地的資料庫互連形成環狀，使得資料庫的資料同步及傳送有不受干擾的頻寬與備援電路。連線設備以北、中、南三地各配置兩個專線路由器，每個路由器需至少具有兩個 10/100/1000 ethernet 埠。一個 10/100/1000 ethernet 埠連線至 server farm 網路，與另一個路由器建立 VRRP (Virtual Router Redundancy Protocol) 或 HSRP(Hot Standby Routing Protocol)功能，提供 Server 或 Server farm 主幹交換器的閘道器備援功能，另外利用 VRRP 或 HSRP 功能可偵測 100M 電路及相鄰路由器狀態進行閘道器切換。另一個 10/100/1000 ethernet 埠連線至 100M 電路，與其他備援機房互連並建立動態路由，進行 IP 路由表交換並可偵測電路及動態路由交換功能是否正常，使得資料庫的資料同步及傳送獲得最佳及穩定的路徑。

6.1.5.6. IP 規劃

消防署所屬各單位目前 IP 的配置以 10.0.0.0 網段，每一單未分配一個 B Class 的網段如下表所示：

表 116、目前消防署所屬單位 IP 分配表

單位名稱	IP 位址	單位名稱	IP 位址
消防署	10.1.0.0/16	台南市消防局	10.33.0.0/16
台北市消防局	10.3.0.0/16	台南縣消防局	10.35.0.0/16
高雄市消防局	10.5.0.0/16	高雄縣消防局	10.37.0.0/16
基隆市消防局	10.7.0.0/16	屏東縣消防局	10.39.0.0/16
台北縣消防局	10.9.0.0/16	台東縣消防局	10.41.0.0/16
桃園縣消防局	10.11.0.0/16	花蓮縣消防局	10.43.0.0/16
新竹市消防局	10.13.0.0/16	宜蘭縣消防局	10.45.0.0/16
新竹縣消防局	10.15.0.0/16	澎湖縣消防局	10.47.0.0/16

苗栗縣消防局	10.17.0.0/16	基隆港務消防隊	10.49.0.0/16
台中市消防局	10.19.0.0/16	台中港務消防隊	10.51.0.0/16
台中縣消防局	10.21.0.0/16	高雄港務消防隊	10.53.0.0/16
彰化縣消防局	10.23.0.0/16	花蓮港務消防隊	10.55.0.0/16
南投縣消防局	10.25.0.0/16	金門縣消防局	10.59.0.0/16
雲林縣消防局	10.27.0.0/16	連江縣消防局	10.61.0.0/16
嘉義市消防局	10.29.0.0/16	特種搜救隊	10.63.0.0/16
嘉義縣消防局	10.31.0.0/16		

本專案規劃之主中心及異地備援中心將依照 IP 配置原則，規劃北區資料中心網段為 10.65.0.0/16，中區資料中心網段為 10.67.0.0/16，南區資料中心網段為 10.69.0.0/16。目前 IP 網路主要是依照功能面來分區，透過 Firewall 來做區隔與保護，目前主要區分為 Web 區、測試區、主機代管、管理區、AP 區及 DB 區。

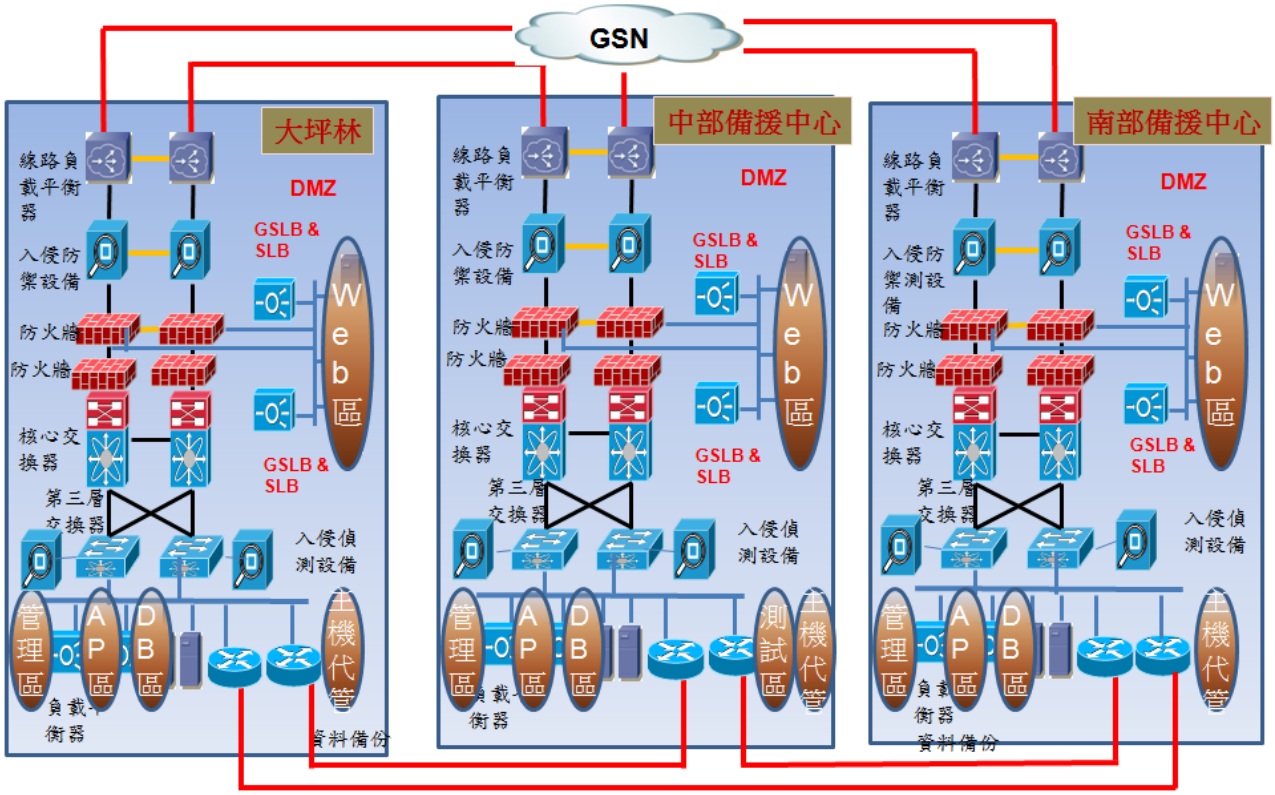

圖 489、IP 規劃示意圖

各區資料中心 IP 規劃如下所示：

表 117、北區資料中心 IP 規劃表

用途	IP 位址	說明

DMZ 區 Server	10.65.1.0/24 ~ 10.65.15.0/24	DMZ 區 Web Server 使用
核心網路區 Server	10.65.17.0/24 ~ 10.65.31.0/24	核心網路區內分測試區、管理區、AP Server 區、DB Server 區等使用
網路管理	10.65.253.0/24	網路設備管理用

表 118、中區資料中心 IP 規劃

用途	IP 位址	說明
DMZ 區 Server	10.67.1.0/24 ~ 10.67.15.0/24	DMZ 區 Web Server 使用
核心網路區 Server	10.67.17.0/24 ~ 10.67.31.0/24	核心網路區內分測試區、管理區、AP Server 區、DB Server 區等使用
網路管理	10.67.253.0/24	網路設備管理用

表 119、南區資料中心 IP 規劃

用途	IP 位址	說明
DMZ 區 Server	10.69.1.0/24 ~ 10.69.15.0/24	DMZ 區 Web Server 使用
核心網路區 Server	10.69.17.0/24 ~ 10.69.31.0/24	核心網路區內分測試區、管理區、AP Server 區、DB Server 區等使用
網路管理	10.69.253.0/24	網路設備管理用

6.1.6. 儲存雲

雲端應用必須能夠統一管理使用者的儲存空間，並且提供使用者檔案層次、可跨越終端裝置、跨越作業系統與跨越通訊協定界限的數位文件管理。必須發展雲端檔案庫系統，提供雲端應用的雲端檔案管理服務。雲端檔案庫系統設計，主要是同步機制與檔案傳輸協定虛擬化的充分運用，在桌面環境中安裝檔案同步代理程式(agent)，可將使用者個人儲存空間中的檔案，同步到集中的儲存區，並且提供 Web 使用介面，操作數位文件檔案所有複雜管理功能，包含新增、刪除、版本管理、分享等。使用者可用各種終端裝置，例如 PC、iPhone、iPad 或 Netbook，透過不同作業系統版本的同步代理程式(agent)與網路連結，達到無處不在自

行使用或分享使用數位檔案的方便性，堪稱雲端檔案總管服務。

儲存雲系統，包含以下幾個主要特色:

(1) 檔案管理 (File Management)

使用者可以存取物件，像是檔案或是資料夾，可以看到更多關於物件的資訊或是屬性的詮釋資料 (metadata)及任何新增的物件描述，例如，當使用者創造一個新的物件，他就是物件最後的修改者(modifier)。此外，一個使用者可以針對一個物件加入使用者的特別標籤(tags)，所有資訊皆可透過檔案搜尋及管理介面操作之。

(2) 儲存精簡自動配置 (Storage Thin Provisioning)

單一系統可以服務多個使用者，管理者可以動態的分配儲存空間給單一使用者，改良了傳統的儲存固定分享機制，假如使用者分配 2 GB 空間，其使用了 200 MB，則剩餘的 1.8 GB 空間可以重新分配給其他使用者使用。換言之、儲存空間分配給使用者並不是固定分配的，管理者可以更敏捷的調配與使用儲存空間。

(3) 版本控制 (Versioning)

使用者可以經常上傳新版本檔案到儲存雲上，在使用者的個人檔案夾中可以顯示完整的檔案歷史版本。有了歷史版本的追蹤，使用者可以查詢檔案版本(產生時間及檔案修改者)並且動態的回復舊版本，這個特色對於多使用者環境，協同合作編輯相同單一檔案或物件相當有幫助，在此環境下，儲存雲也提供檔案的 check-in 及 check-out 的版本控制機制 — 避免多人對同一檔案編輯的同時編輯。

(4) 分享機制 (Sharing)

在儲存雲中，檔案/物件分享機制支援兩個形式:

首先，呼叫 sharing by link 的機制，使用者分享檔案給其他使用者，被分享者可以在他們自己的目錄夾中看到被分享的檔案。假如其中一個使用者更新檔案或是修改檔案，其他使用者將會看到新修改

的版本，在這個模式下，真實的檔案只有一個，其他使用者看到的只是一個連接 (link)，這個特色對於協同合作開發環境相當有幫助。

第二，使用 sharing by copy 的機制，儲存雲可以 copy 檔案到其他被分享者的個人資料夾。在這個案例下，所有被分享的使用者可以產生他們自己的檔案版本在其他人的個人資料夾中，他們各自保有及維護被分享的檔案。假如使用者想要分享一個檔案，給其他不是儲存雲的使用者，使用者可以送出一個有下載連結的電子郵件給其他使用者，有了下載連接後，儲存雲的外部使用者可以更容易的按下滑鼠做下載檔案動作。

(5) 檔案搜尋 (Searching)

在儲存雲中，使用者可以透過檔案中的屬性搜尋檔案 (metadata，tags，and/or keywords)。使用者也可以使用關鍵字作全文搜尋。

(6) 客戶端代理人 (Client Agent)

Client agent 是一個客戶端代理人軟體，允許使用者存取遠端檔案在個人裝置上 (例如 Window、Mac OS、iOS、and Android)。特別的是 client agent 可以動態的同步客戶端的檔案及資料夾到儲存雲上。當網路不通的時候使用者可以在自己電腦上存取自己檔案 (例如，當使用者在飛行旅行時)。當使用者可以連線到儲存雲主機時，client agent 將自動同步本地端與遠端機器的差異處，所有的檔案存取行為就像使用個人電腦的檔案總管一般。這個特色也幫助網路操作不熟悉的使用者，可以在虛擬網路環境下達成共同協同合作。

6.1.7. 系統備份備援

在美國 911 恐怖攻擊後，雙子星大樓全毀，造成所有大樓內所有的企業資訊系統均癱瘓，重創企業的經營，因此如何提供系統備份備援之機制就越顯得重要。再加上近年來由於溫室效應造成全球氣候不穩定，風災、雨災頻繁，猶如電影”明天過後”的情節，歷歷在目。為維持企業的資訊系統正常運作，達到永續經營(Business Continuity)，系統備份備援

是必需要的。

為達成有效的系統備份備援必需有下列的規劃與考量：

- 實體的需求：

  在備援中心端置放備援的處理器、儲存設備及網路設備，主中心端在災難發生時，可立即切到備援中心端運轉。備援中心端必需離主中心端夠遠，避免與主中心端同時受災害。

- 軟體自動化備援的需求：

  利用叢集(Clustering)軟體提供主中、備援中心端應用層的高可靠度切換及資源的配置。

  - 必需監視主、備援中心端之健康狀況:

    必需通知備援中心端目前主中心端應用層之狀況並作適度的切換，如部份應用程式當掉時，可手動切換至備援中心端工作。

  - 一般性檔案資料的移動：

    需要即時的將主中心端之資料傳送到備援中心端、短距離的情況下可使用同步備份的執行方式，長距離的情況下則使用非同步備份的執行方式，以保持主、備援中心端間的資料同步。

6.1.7.1. 遠端異地備援

貴署系統運用分為防救災業務資訊系統、OA 資訊系統及消防資訊系統。防救災業務資訊系統資料庫遠端異地備援方案拓撲圖：

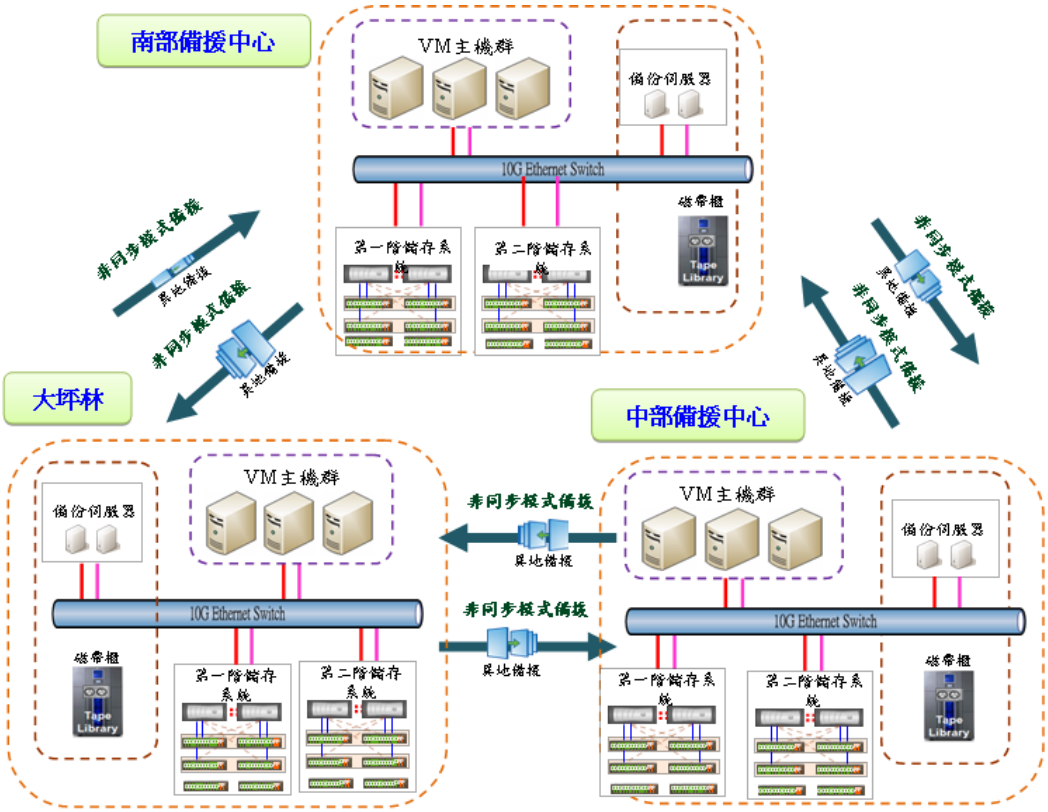

圖 490、資訊系統資料異地備援架構圖

中央災害應變中心涵蓋之異地備援系統切換範圍，各系統服務中斷之恢復時間(Recovery Time Objective，RTO) 必需小於 30 分鐘，而資料損失之時間點(Recovery Point Objective，RPO) 亦不可超過 60 分鐘。

防救災資料庫資料則透過資料庫複製軟體，保持三地(大坪林／中部備援中心／南部備援中心)資料庫同步，讓全台使用者能就近使用防救災資訊系統進行讀寫功能，促使三地(大坪林／中部備援中心／南部備援中心)防救災資訊系統達到全域負載平衡，建議資料庫複製軟體需符合下列功能:

- 提供直接擷取來源端資料庫中包括新增、修改、刪除等交易記錄(transaction log)，並且即時傳送確認(committed)的記錄至目的端。
- 資料複製架構，只需於來源端與目的端資料庫主機安裝複製程式，而無需另外的複製伺服器與 metadata 儲存庫，就可以達成複製功能。

- 擷取後的交易記錄以檔案型式存放於來源端與目的端，且獨立於雙方資料庫系統之外，同時此一交易記錄具有加密與壓縮機制。
- 提供多重資料來源端與目地端複製模型：包括一對一、一對多、多對一、多對、串聯(Cascading)、雙向(Bi-Direction)等複製模型。
- 在雙向、全主動(Active-Active)的複製模型中，提供碰撞偵測與解決方案
- 透過 TCP/IP 來傳遞交易記錄，並提供資料壓縮與加密能力，加速資料遞送。
- 支援多重資料庫擷取功能：包括 Oracle、DB2、SQL Server、Sybase ASE、Teradata、MySQL、Enscribe、SQL/MP、SQL.MX。
- 支援多重作業系統平台：包括 Windows 2000/2003/XP、 Linux、Sun Solaris、HP NonStop、HP-UX、HP TRU 64、HP OpenVMS、IBM AIX、IBM z/OS。

本案因三地(大坪林／中部備援中心／南部備援中心)距離較遠且資料並無立即同步需求，故建議 OA 及災防資訊系統檔案資料、資料庫及防救災資訊系統檔案資料採用非同步模式(A-synchronous)使用快照技術，並透過異地資料複製軟體將儲存系統內的系統資料抄寫一份至異地端儲存系統確保資料可靠度，資料複製作業採用自動化機制進行，加強系統穩定度及減少人員操作負擔同時避免人為錯誤操作造成機制的異常，因此正常狀況下不需人員進行維運，本案所提供之儲存設備亦可支援同步模式，甚至可支援因需求隨時做切換至非同步之功能，提供極佳之擴充性。

非同步式(Async)：非同步於執行時，其寫入之動作只需在主端儲存設備完成寫入即可，主端之主機就可執行下一個動作。而其副端通常較主端晚幾個 miliseconds 再寫入儲存設備。由於不同步，為了保證副端資料的完整性，需藉由記錄主端寫入的順序來保證副端寫入

的過程與主端一致。由於副端與主端無法完全同步，故災害發生時，副端儲存的資料不完整，由副端執行復原程序時，會有些許資料漏失。

建議異地資料複製軟體，可透過統一管理介面簡化異地備援管理，可以任意調整資料複製時間從零秒至數小時，無需重新傳輸資料，異地資料複製軟體應支援同步、非同步、半同步傳輸方式，其切換方式不需要重新傳輸資料，異地備援架構支援一對多、多對一、一對一等方式，透過網路壓縮技術，加快網路傳輸速度以降低 RPO 成本及網路頻寬成本。

6.1.7.2. 本地端虛擬化備份系統

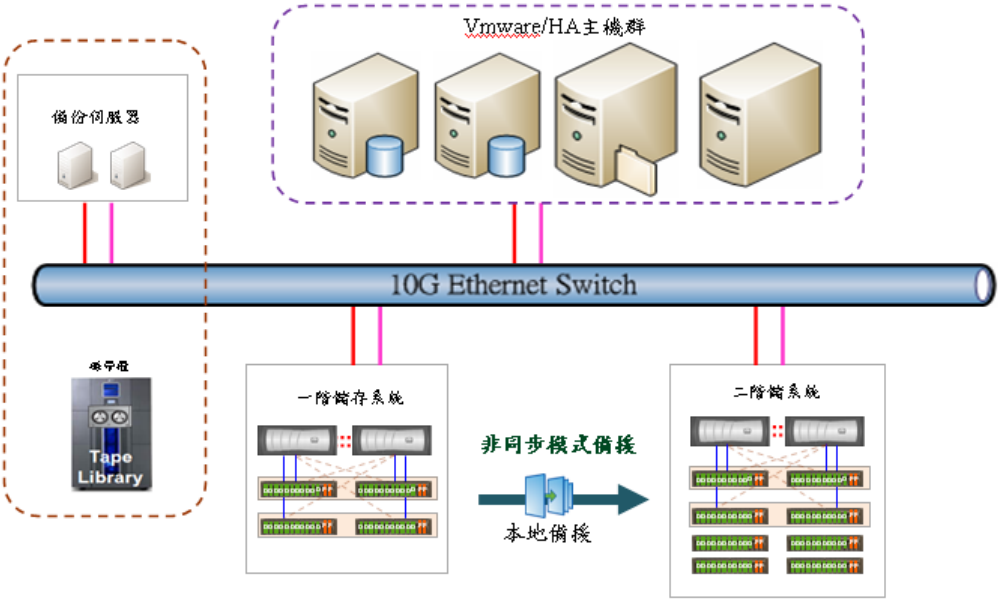

圖 491、本地端虛擬化備份系統圖

對資料進行備份是為了保證資料的一致性和完整性，消除系統使用者和操作者的後顧之憂。不同的應用環境要求不同的解決方案來適應，一般來說，一個完善的備份系統，需要滿足以下原則：

- 穩定性

備份產品的主要作用是為系統提供一個資料保護的方法，於是該產品本身的穩定性和可靠性就變成了最重要的一個方面。首先，備份軟體一定要與作業系統 100%的兼容，其次，當事故發生

時，能夠快速有效地恢復資料。

- 全面性

在複雜的計算機網路環境中，可能會包括了各種操作平台，並安裝了各種應用系統，選用的備份方式，要支援各種作業系統、資料庫和典型應用。

- 自動化

很多系統由於工作性質，對何時備份、用多長時間備份都有一定的限制。在非工作時間系統負荷較輕，適於備份。可是這會增加系統管理員的負擔，由於精力狀態等原因，還會給備份安全帶來潛在的隱患。因此，備份方案應能提供定時的自動備份，並利用自動磁帶櫃等技術進行自動更換磁帶。在自動備份過程中，還要有日誌記錄功能，並在出現異常情況時自動報警。

- 高性能

隨著業務的不斷發展，數據越來越多，更新越來越快，在休息時間來不及備份如此多的內容，在工作時間備份又會影響系統性能。這就要求在設計備份時，盡量考慮到提升資料備份的速度，利用多種技術加快對資料的備份。

- 維持業務系統的有效性

有時備份對業務系統的性能將會產生一定的影響。如何採取有效的技術手段避免備份對伺服器系統、資料庫系統、網路系統的影響，將是非常重要的。

- 操作簡單

資料備份應用於不同領域，進行數據備份的操作管理人員也處於不同的層次。這就需要一個直觀的、操作簡單的在任何作業系統平台下都統一的圖形化用戶界面，縮短作業員的學習時間，減輕作業員的工作壓力，使備份工作得以輕鬆地設定和完成。

- 實時性

部分關鍵性的業務是需要 24 小時不間斷營運的，在備份的時候，有一些檔案可能仍然處於打開的狀態。那麼在進行備份的時

候，要採取措施，實時地檢視檔案大小、進行事務跟蹤，以保證正確地備份系統中的所有檔案。

本案建議採購備份軟體、實體磁帶櫃進行資料備份，備份軟體軟體可以完整支援虛擬化軟體將資料備份至實體磁帶櫃。備份軟體可簡化備份管理人員備份工作，透過角色指定方式，定義每個管理人員管理權限，增加系統安全性。

6.1.7.3. 備份策略

必須根據實際需要配置備份策略，定義備份策略，涉及到以下內容:

在什麼時間(備份時間，如下午 6:00 後)、將什麼數據(備份內容，如主數據庫數據)、以什麼模式(備份模式，如全備份或增量備份)？

透過哪磁帶櫃(備份通道，如: 去是否放至磁帶)、備份到哪一個磁帶組(備份到達站)，在我們對每一組資料、資料庫都根據需要定義好備份策略後，系統就會自動的按照我們定義的時間、模式、將需要備份的數據備份到我們指定的磁帶櫃中，而備份的模式可以分為三種: 全備份、增量備份、累計增量備份。

- 全備份

  每次備份定義的所有數據，優點是恢復快，缺點是備份數據量大，數據多時可能做一次全備份需很長時間。

- 增量備份

  備份自上一次備份以來更新的所有數據，其優點是每次備份的數據量少，缺點是恢復時需要全備份及多份增量備份。

- 累計備份

  備份自上一次全備份以來更新的所有數據。

我們可以結合這三種模式，靈活應用。例如: 資料量少時，我們可以每次都用全備份備份數據，當資料復原時只需要指定一個資料來源即可，數據量大時，如果每天作全備份，效率會很低，我們可以結合全備份和增量備份模式，例如每星期作一次全備份(如星期天)，其它時間每天作一個增量備份(如:星期一到星期六)，資料復原時只要依

次恢復即可.(如: 上周日、星期一、星期二 ...直到出事前一天的資料。)，資料量特別大時，每星期作全備份對系統的壓力也會很大，這時我們可以結合全備份、累計增量備份、增量備份三種模式，提供相對效率高，恢復有快的備份方式，例如每個月作一次全備份(如每月初)，然後每星期日作一次累計增量備份，其它時間每天作一次增量備份，資料復原時先復原月初的全備份再恢復上周日的累計增量備份，在依次復原以後每一天的增量備份，如星期一、星期二 ...，直到損毀前一天的資料。 (最多恢復 8 份，相對的如果不採用累計增量備份模式，復原時最多可能需要 31 份，復原速度和複雜程度都會不理想) 。 對系統進行每日備份是必要的，可以更好的提升系統的安全性和可靠性.

6.1.7.3.1. 磁帶櫃備份流程:

日常備份操作由儲存系統提供的快照備份機制當作第一道資料安全保護機制自動完成，第一道資料安全保護機制透由備份軟體備份伺服器上製定備份策略備份至實體磁帶櫃上帶。這樣可以大大提升數據的備份效率，提升存儲設備的利用率。為提升備份質量、保證數據安全。

6.1.7.3.2. 備份策略建議:

對於計算機應用系統這樣的一個關鍵應用來說，製定一個良好的備份策略是至關重要的。備份工作的主要內容包括以下兩個方面：虛擬化主機、資料庫系統備份

- 虛擬化主機備份策略

為了在虛擬化主機上存放的應用軟體系統發生故障時，能夠迅速、有效的使系統得到恢復，日常備份儲存系統提供的快照備份機制當作第一道資料安全保護機制，每週或每月定期備份至實體磁帶櫃上帶。由於主機、應用軟體極少發生變動，所以它的備份策略也比較簡單。這些備份排程可以透過備份軟體的定時自動完成。

- 資料庫系統備份備份策略

日常備份儲存系統提供的快照備份機制當作第一道資料

安全保護機制，每日(增量備份)/週(全備份)經由備份軟體定期備份至實體磁帶櫃上，備份排程可以透過備份軟體的定時自動完成。

6.1.7.4. 災難備援方式

6.1.7.4.1. OA 及消防資訊系統

6.1.7.4.1.1. 大坪林

當大坪林儲存系統發生故障，由於以本規劃的範圍而言，在硬體設備比較有可能會發生的事件有：

- 儲存系統的 CPU 故障
- 儲存系統的 FAN 故障
- 儲存系統上的網路卡故障
- 儲存系統上的電源供應器故障
- 儲存系統上的線路故障
- 儲存系統上的硬碟故障
- 儲存系統上的儲存控制主機發生故障
- 儲存系統雙控制器發生故障

在軟體部份比較有可能會發生的事件有：

- 人為操作疏失，導致應用程式、或資料庫檔案發生損毀

針對以上的事件可能性分析，本規劃將以下列舉相對應的應變措施，以做為　貴署資訊單位相關人員的作業參考：

- 儲存系統的 CPU 故障

在本專案的架構當中規劃 Cluster 架構，當控制器上的 CPU 故障時另一個控制器接管。

由於儲存系統的產品內建了 I/O checksum 功能，所以在設備不是外力影響的情況下，若系統有異常的狀況持續發生時，將會由系統自動發送 e-mail 到原廠 Global Support Center 與　貴單位的系統人員(發送人員或單位可

再調整)，同時通透原廠 Global Support Center 之註冊聯絡人，透過 UPS 快遞公司將零件寄送到　貴單位，同時也會照會本專案之相關維護廠商，指派工程師到場置換零件。

◆ 儲存系統 FAN 故障

在本專案的架構當中規劃 Cluster 架構，當控制器上的 FAN 故障時另一個控制器接管。

由於儲存系統的產品內建了 I/O checksum 功能，所以在設備不是外力影響的情況下，若系統有異常的狀況持續發生時，將會由系統自動發送 e-mail 到原廠 Global Support Center 與　貴單位的系統人員(發送人員或單位可再調整)，同時通透原廠 Global Support Center 之註冊聯絡人，透過 UPS 快遞公司將零件寄送到　貴單位，同時也會照會本專案之相關維護廠商，指派工程師到場置換零件。

◆ 儲存系統上的網路 Port 故障

在本專案的架構當中規劃二個網路 Port 當作 Turnking，當控制器上的 Port 故障時另一個可以繼續提供 Service。

由於儲存系統的產品內建了 I/O checksum 功能，所以在設備不是外力影響的情況下，若系統有異常的狀況持續發生時，將會由系統自動發送 e-mail 到原廠 Global Support Center 與　貴單位的系統人員(發送人員或單位可再調整)，同時通透原廠 Global Support Center 之註冊聯絡人，透過 UPS 快遞公司將零件寄送到　貴單位，同時也會照會本專案之相關維護廠商，指派工程師到場置換零件。

◆ 儲存系統上的電源供應器故障

儲存系統每個機箱上都有二個電源供應器，當其中顆電源供應器有問題時，另一顆電源無應器可繼續提供運作。

由於儲存系統的產品內建了 I/O checksum 功能，所以在設備不是外力影響的情況下，若系統有異常的狀況持續

發生時，將會由系統自動發送 e-mail 到原廠 Global Support Center 與 貴單位的系統人員(發送人員或單位可再調整)，同時通透原廠 Global Support Center 之註冊聯絡人，透過 UPS 快遞公司將零件寄送到 貴單位，同時也會照會本專案之相關維護廠商，指派工程師到場置換零件。

◆ 儲存系統上的線路故障

儲存系統每個控制器到機箱及機箱到機箱上都有規劃二條路徑，當其中一條路徑有問題時，另一條路徑可以自動繼續提供服務。

由於儲存系統的產品內建了 I/O checksum 功能，所以在設備不是外力影響的情況下，若系統有異常的狀況持續發生時，將會由系統自動發送 e-mail 到原廠 Global Support Center 與 貴單位的系統人員(發送人員或單位可再調整)，同時通透原廠 Global Support Center 之註冊聯絡人，透過 UPS 快遞公司將零件寄送到 貴單位，同時也會照會本專案之相關維護廠商，指派工程師到場置換零件。

◆ 儲存系統的硬碟故障

因為儲存系統採用了 RAID 6 技術，可允許同時兩顆硬碟故障，或是先壞一顆，在 rebuild 過程再壞第二顆，仍不會發生問題。

由於儲存系統的產品內建了 I/O checksum 功能，所以在設備不是外力影響的情況下，若系統有異常的狀況持續發生時，將會由系統自動發送 e-mail 到原廠 Global Support Center 與 貴單位的系統人員(發送人員或單位可再調整)，同時通透原廠 Global Support Center 之註冊聯絡人，透過 UPS 快遞公司將零件寄送到 貴單位，同時也會照會本專案之相關維護廠商，指派工程師到場置換零件。

◆ 儲存系統上的儲存控制主機發生故障

在本規劃的架構當中，是由兩部儲存系統互作叢集備

援，所以若其中一部儲存系統控制主機發生故障時，另一部儲存系統控制主機將會馬上接手，不會造成作業停擺。

若因為不正常斷電造成儲存系統停機，則可在供電後 10 分鐘以內完成開機。

由於儲存系統的產品內建了 I/O checksum 功能，所以在設備不是外力影響的情況下，若系統有異常的狀況持續發生時，將會由系統自動發送 e-mail 到原廠 Global Support Center 與 貴單位的系統人員(發送人員或單位可再調整)，同時通透原廠 Global Support Center 之註冊聯絡人，透過 UPS 快遞公司將零件寄送到 貴單位，同時也會照會本專案之相關維護廠商，指派工程師到場置換零件。

◆ 儲存系統儲存雙控制器發生故障

在本規劃的架構當中，透過異地備援復製軟體，將大坪林的系統資料抄寫一份至中部備援中心及南部備援中心儲存系統內。

災難發生時，即可快速將備援中心儲存系統設為可讀寫模式，便能取代大坪林儲存系統。

由於儲存系統的產品內建了 I/O checksum 功能，所以在設備不是外力影響的情況下，若系統有異常的狀況持續發生時，將會由系統自動發送 e-mail 到原廠 Global Support Center 與 貴單位的系統人員(發送人員或單位可再調整)，同時通透原廠 Global Support Center 之註冊聯絡人，透過 UPS 快遞公司將零件寄送到 貴單位，同時也會照會本專案之相關維護廠商，指派工程師到場置換零件。

6.1.7.4.1.2. 在軟體部份

人為操作疏失，導致應用程式、或資料庫檔案發生損毀，在這種情況發生時，將判定為資料檔案損毀，此時將可透過儲存設備的快速回復技術機制將資料檔案由 Snapshot 快照備份

資料回復到最近的時間點，再繼續作業。

6.1.7.4.1.3. 大坪林災難啟動方式說明

災難發生時，手動將中部或南部備援中心第二階儲存系統設為可讀寫模式(儲存設備切換時間約為 10 分鐘(不含資料回復時間) ，便能取代主大坪林儲存系統立即提供服務。

- 透過儲存設備自動災難備援機制，即可輕鬆達成災難備援、備份等工作

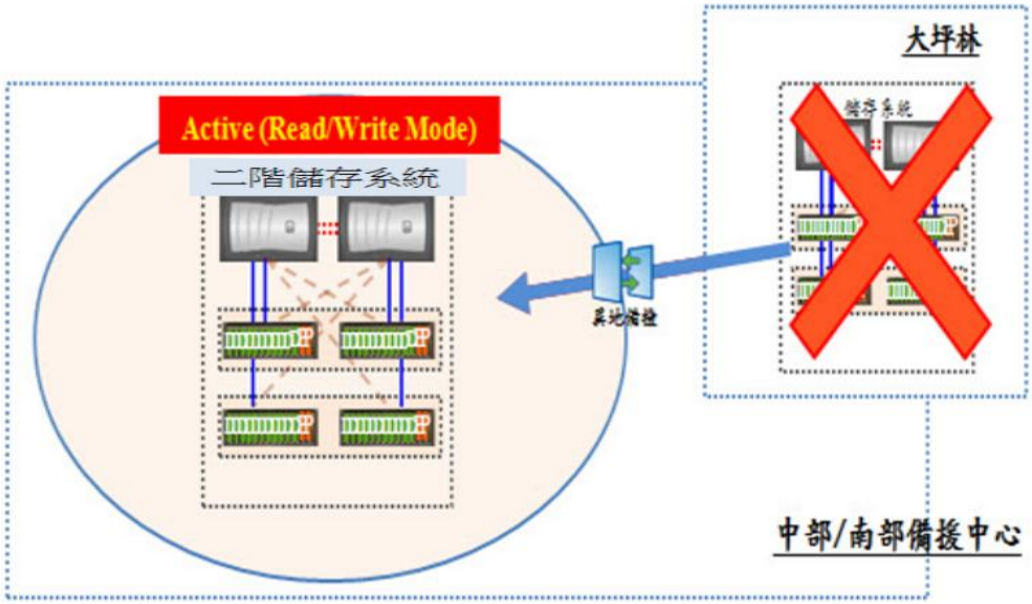

圖 492、大坪林災難啟動方式示意圖一

- 將備援期間 DB & File 異動或新增之資料更新回第一階儲存系統
- 將一階儲存系統切換為可讀寫模式，立即提供服務
- 重新將主第一階儲存系統資料傳送至第二階儲存系統儲存系統

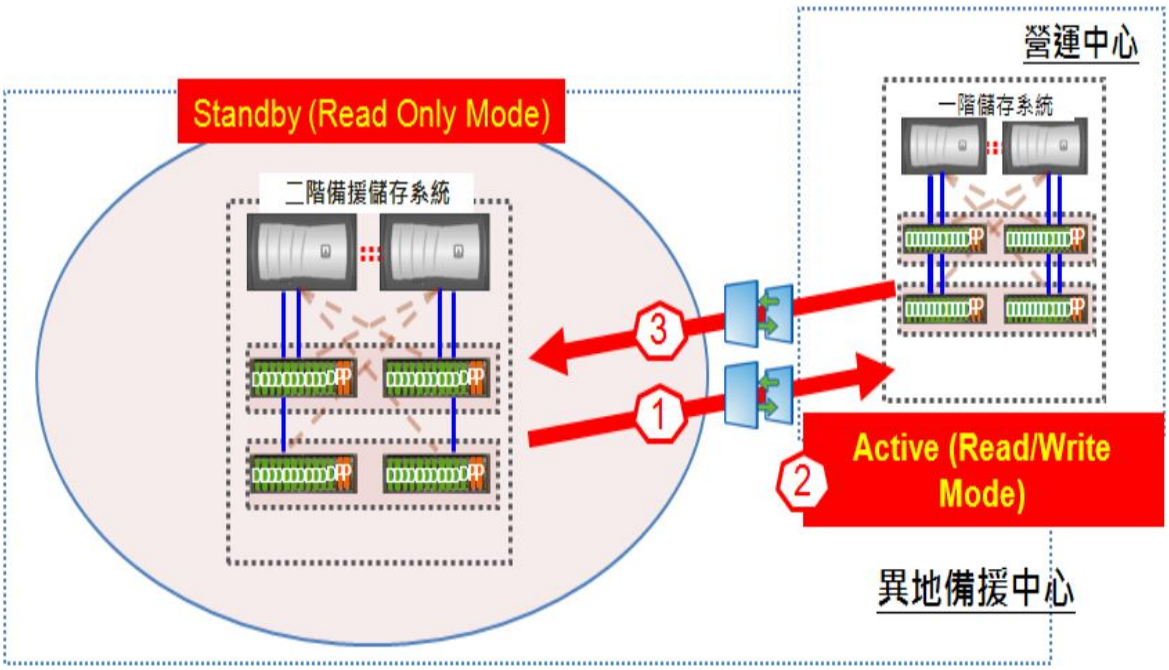

圖 493、大坪林災難啟動方式示意圖二

6.1.7.4.1.4. 中部備援中心及南部

備援中心的災難備援機制如同大坪林的方式進行。

6.1.7.4.2. 防救災業務資訊系統

當災難發生時，防救災業務資訊系統檔案資料會如同"OA 及消防資訊系"災難備援機制一般，進行災難復原的工作，但防救災業務資訊系統的資料庫，則會透過資料庫同步複製軟體，進行災難復原的工作。

下面將就資料庫同步複製軟體於日常作業，網路斷線後復原機制，機房毀損後復原機制等狀況，做其運作上的說明:

6.1.7.4.2.1. 日常作業。

1，大坪林 - 將異動資料，主動推送到另兩地資料庫的"目的端"。

2，南備 - 將異動資料，主動推送到另兩地資料庫的"目的端"。

3，中備 - 將異動資料，主動推送到另兩地資料庫的"目的端"。

4，5，6，- 各資料庫，收到另外兩地資料庫的異動資料，依據所制定的規則，主動將異動資料 Delivery 到資料庫中。

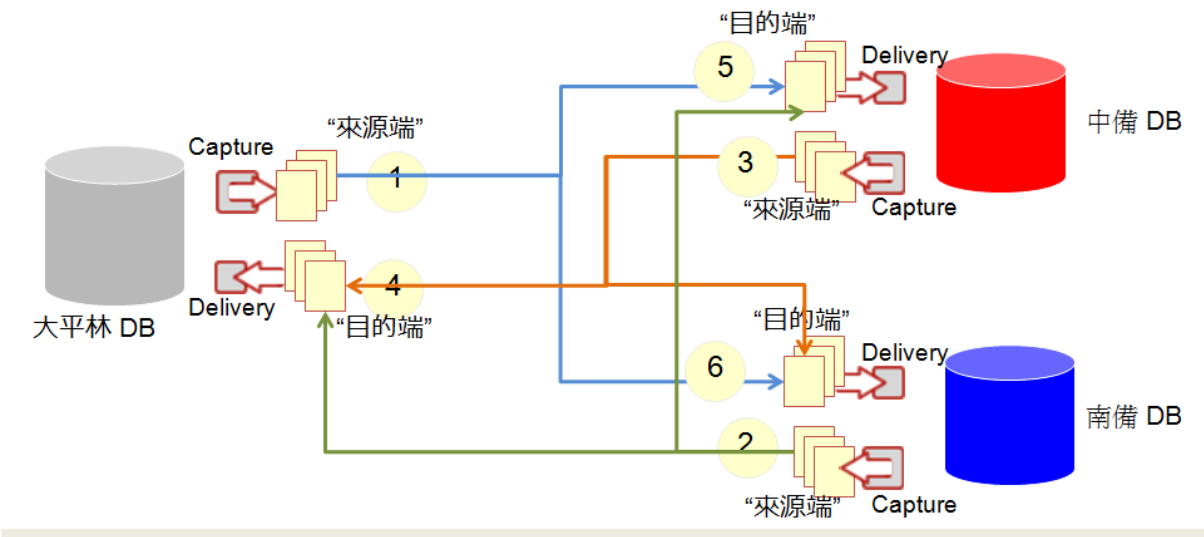

圖 494、資料庫同步複製軟體日常作業示意圖

6.1.7.4.2.2. 網路斷線復原機制。

圖中標示的 scn 為 sequence number 的簡寫。

- 中備/南備 DB 的 Target File 將紀錄到與大坪林 DB 最後的同步資料為 scn: x。
- 中備 DB 的 Source File 將紀錄到，送出給大坪林 DB 的最後一筆同步成功的資料為 scn: y。
- 南備 DB 的 Source File 將紀錄到，送出給大坪林 DB 的最後一筆同步成功的資料為 scn: z。

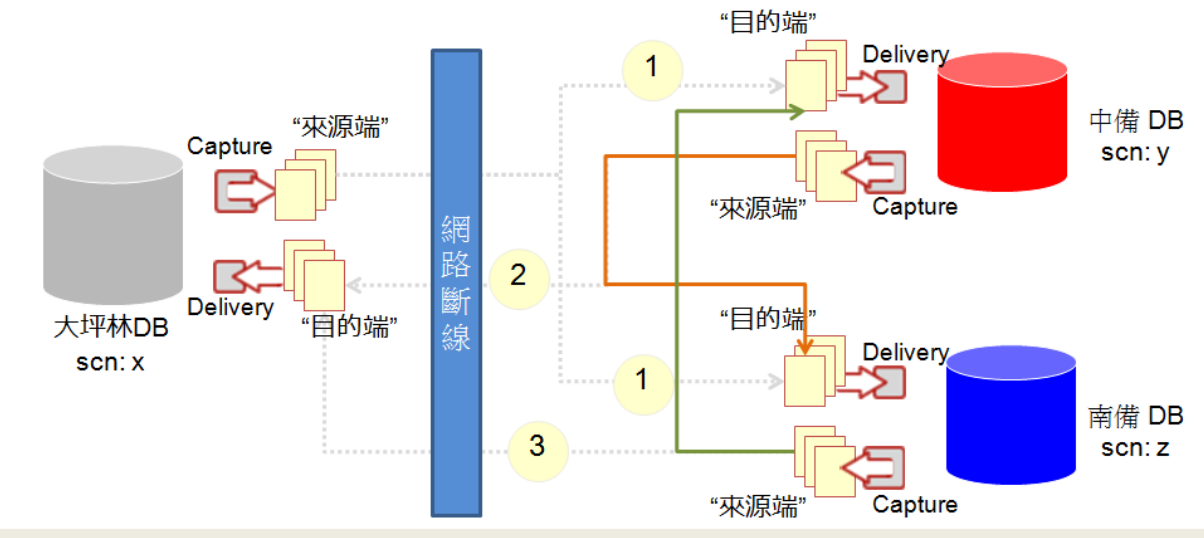

圖 495、網路斷線復原機制(一)示意圖

- 中備/南備 DB 的 Target File 將紀錄到與大坪林 DB 最後的同步資料為 scn: x。
- 中備 DB 的 Source File 將紀錄到，送出給大坪林 DB 的最後一筆同步成功的資料為 scn: y。
- 南備 DB 的 Source File 將紀錄到，送出給大坪林 DB 的最後一筆同步成功的資料為 scn: z。

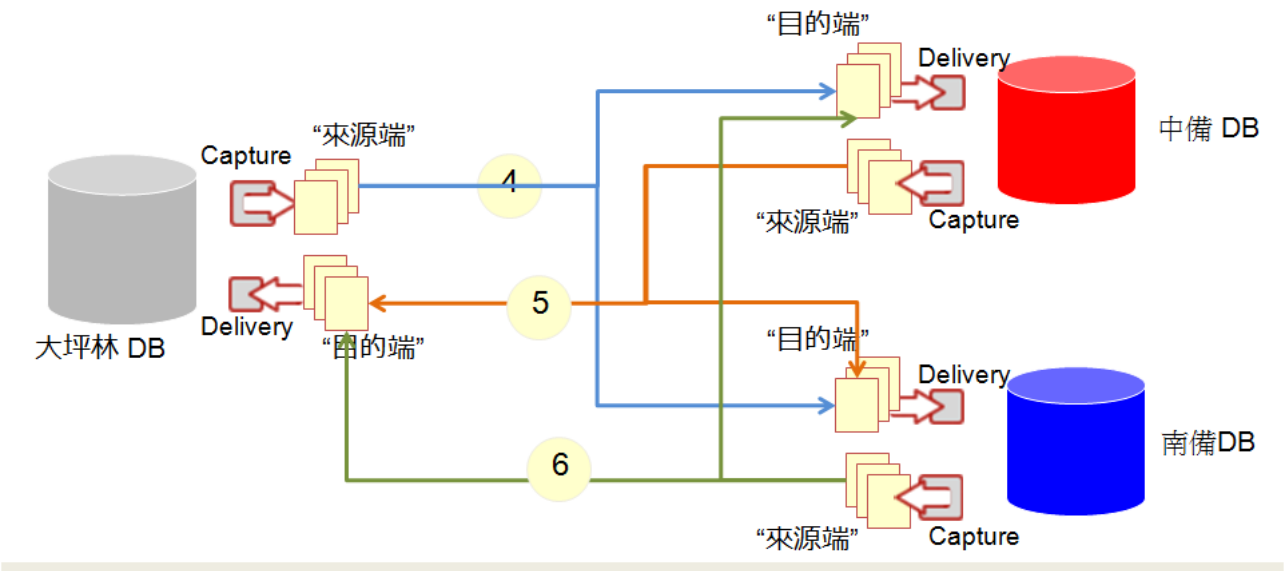

圖 496、網路斷線復原機制(二)示意圖

6.1.7.4.2.3. 機房毀損復原機制。

圖中標示的 scn 為 sequence number 的簡寫。

- 大坪林機房毀損後，中備/南備 DB 的 Target File 將即時更新同步紀錄到接近大坪林 DB 毀損前的資料。
- 中備 DB 的 Source File 將持續更新異動資料到南備 DB。
- 南備 DB 的 Source File 將持續更新異動資料到中備 DB。

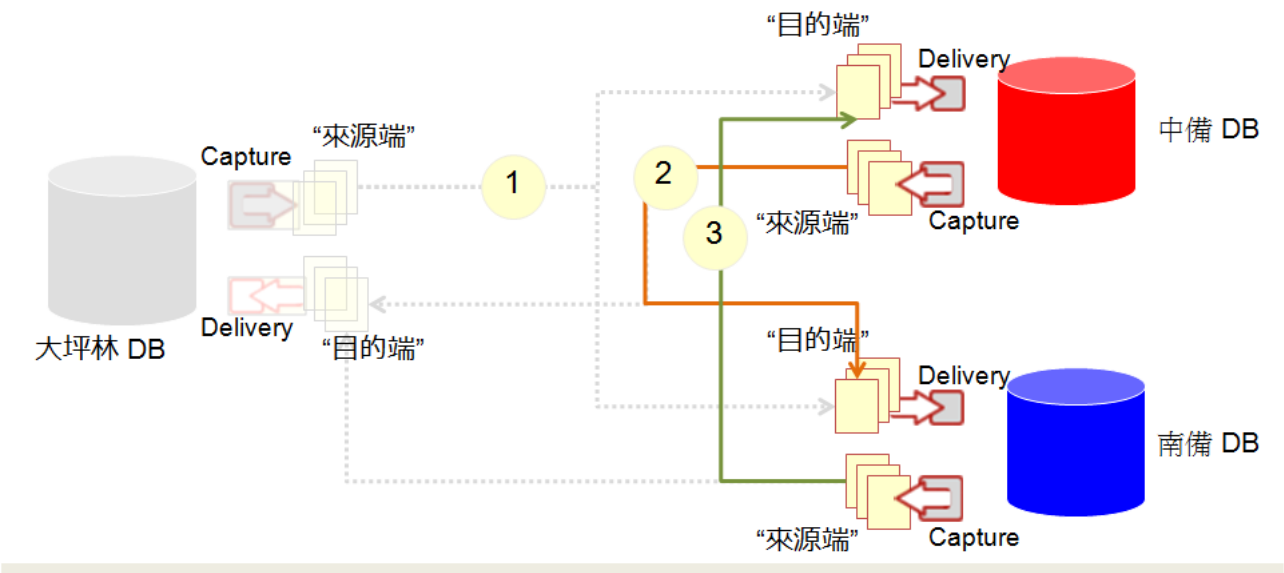

圖 497、機房毀損復原機制(一)示意圖

◆ 由南備(或中備) Clone 一套資料到重建後的大坪林 DB。其最後異動資料將是中備 DB scn:y/南備 DB scn: z。

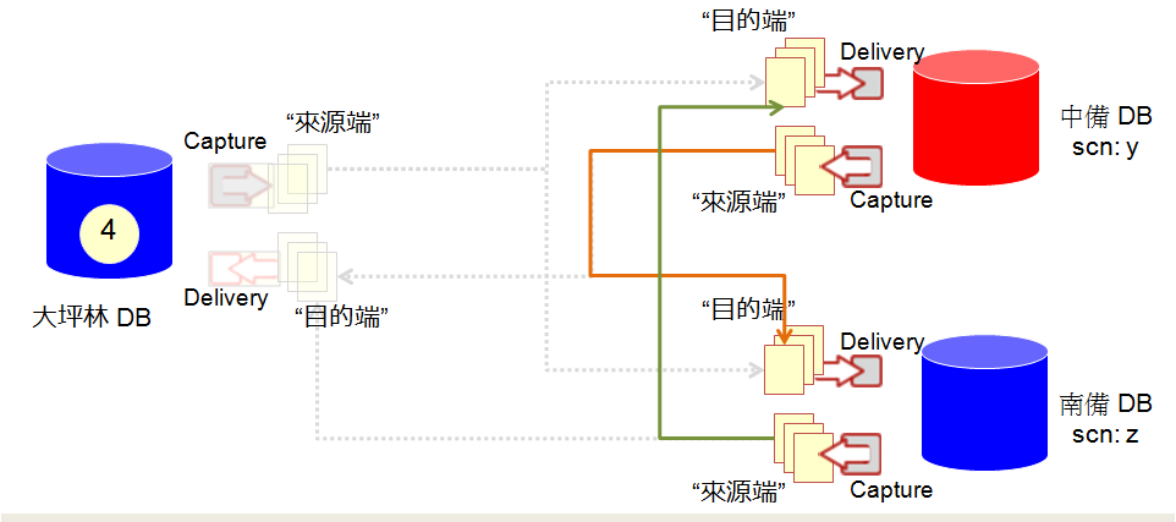

圖 498、機房毀損復原機制(二)示意圖

◆ 重新啟動大坪林 DB 的 Capture 功能和 Delivery 功能，Delivery 分別設定中備 DB 由 scn:y 之後開始同步；南備 DB 由 scn:z 之後開始同步。

◆ 大坪林 DB 恢復上線後，新的異動資料會開始同步到中備/南備兩組 DB。

◆ Delivery 功能，會由中備 DB 同步 scn:y 之後的異動，直

到兩地資料同步。

◆ Delivery 功能，會由南備 DB 同步 scn:z 之後的異動，直到兩地資料同步。

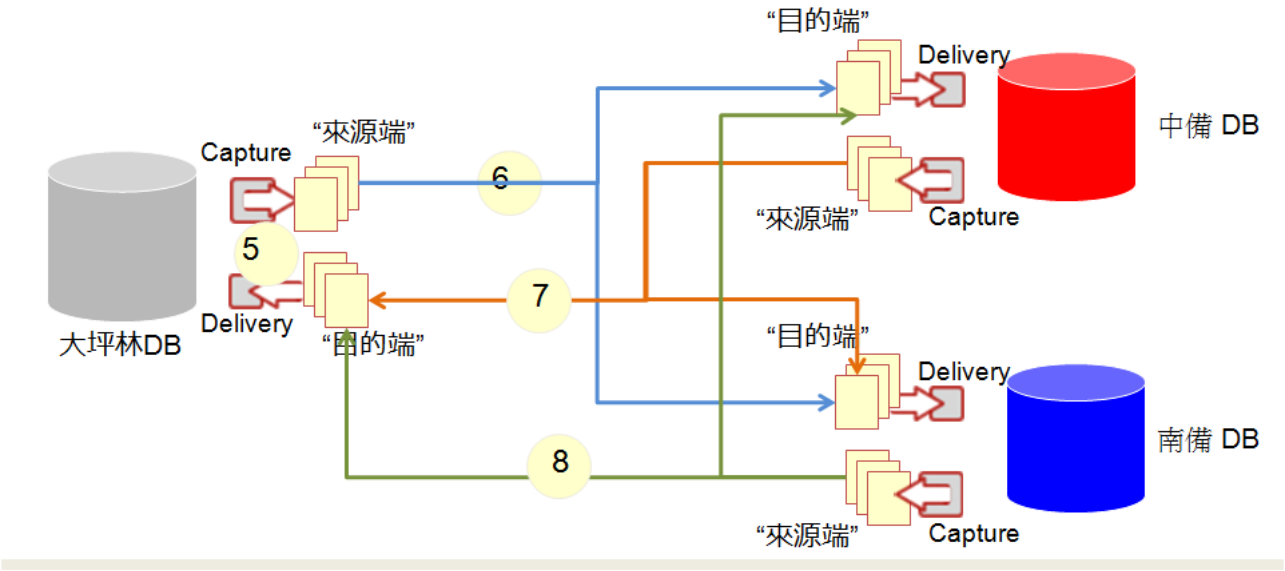

圖 499、機房毀損復原機制(三)示意圖

6.2. 雲端基礎建設之軟、硬體設備需求

6.2.1. 防救災雲端伺服器設備

根據之前對各功能與設備的需求分析，統計設備數量如下：

6.2.1.1. 大坪林中心伺服器清單如下表:

表 120、大坪林中心伺服器清單

名稱	區域	數量	Core	RAM (G)	磁碟 (GB)	形式	備註
民眾入口網主機	DMZ	2	2	4	250	虛擬	
防救災入口網主機	DMZ	2	2	4	500	虛擬	
防災數位學習主機	DMZ	2	2	4	1000	虛擬	
整合通訊主機	DMZ	2	2	4	250	虛擬	
防救災應用主機	防救災	8	4	8	250	虛擬	
GIS 主機	防救災	2	4	8	500	虛擬	
資料倉儲分析主機	防救災	2	2	4	250	虛擬	
企業匯流排主機	防救災	2	2	4	250	虛擬	
資料交換主機	防救災	2	2	4	250	虛擬	
整合通訊主機	防救災	4	2	4	250	虛擬	
雲端檔案系統主機	防救災	2	2	4	1000	虛擬	
決策支援主機	防救災	2	2	4	250	虛擬	
圖資倉儲主機	防救災	2	2	8	1000	虛擬	
氣象局主機	防救災	2	2	4	500	虛擬	
全國消防應用主機	消防	4	2	4	250	虛擬	
辦公室自動化主機	OA	30	2	2	250	虛擬	公務統計系統 會計系統 GBA 公文管理系統 公文電子交換系統 人事系統 差勤系統 線上投票系統 財產系統 國有財產查詢系統 簡報新聞儲存系統
Exchange Mail 主機	OA	4	2	4	1000	虛擬	
防救災資料庫主機	DB	2	8	32	1000	實體	
全國消防資料庫主機	DB	2	4	16	500	實體	
資料倉儲資料庫主機	DB	2	4	8	3000	實體	
備份主機	管理	1	2	4	250	實體	
虛擬主控台	管理	2	2	4	250	實體	
雲端自動化主機	管理	1	2	2	250	實體	
目錄主機	管理	4	2	4	500	虛擬	
安控主機	管理	4	2	4	250	虛擬	含憑證管理

DNS 主機	管理	2	2	4	250	虛擬	
網管主機	管理	2	2	4	250	虛擬	
NOC 主機	管理	1	2	4	250	虛擬	
SOC 主機	管理	1	2	2	250	虛擬	
異地備援控制主機	管理	1	2	2	250	虛擬	
防毒主機	管理	1	2	2	250	虛擬	
伺服器監控主機	管理	1	2	2	250	虛擬	
系統管理主機	管理	1	2	2	250	虛擬	
系統效能監測主機	管理	1	2	4	250	虛擬	
原始碼資安掃描主機	管理	1	2	4	250	虛擬	
港消消防主機	代管	1	2	2	250	虛擬	
縣市消防主機	代管	30	2	4	250	虛擬	10 縣市各 3 部
測試主機	測試	8	2	8	250	虛擬	
實體小計 ：		11	42	128	10250		
虛擬小計 ：		130	284	530	42500		
合計 ：		141	326	658	52750		

6.2.1.2. 中部備援中心伺服器清單如下表:

表 121、中部備援中心伺服器清單

名稱	區域	數量	CPU Core	RAM (G)	磁碟 (GB)	形式	備註
民眾入口網主機	DMZ	2	2	4	250	虛擬	
防救災入口網主機	DMZ	2	2	4	500	虛擬	
防災數位學習主機	DMZ	2	2	4	1000	虛擬	
整合通訊主機	DMZ	2	2	4	250	虛擬	
防救災應用主機	防救災	4	4	8	250	虛擬	
GIS 主機	防救災	2	2	8	500	虛擬	
資料倉儲分析主機	防救災	2	2	4	250	虛擬	
企業匯流排主機	防救災	2	2	4	250	虛擬	
資料交換主機	防救災	2	2	4	250	虛擬	
整合通訊主機	防救災	4	2	4	250	虛擬	
雲端檔案系統主機	防救災	2	2	4	1000	虛擬	
決策支援主機	防救災	2	2	4	250	虛擬	
圖資倉儲主機	防救災	2	2	8	1000	虛擬	
氣象局主機	防救災	2	2	4	500	虛擬	
全國消防應用主機	消防	4	2	4	250	虛擬	

辦公室自動化主機	OA	30	2	2	250	虛擬	公務統計系統 會計系統 GBA 公文管理系統 公文電子交換系統 人事系統 差勤系統 線上投票系統 財產系統 國有財產查詢系統 簡報新聞儲存系統
Exchange Mail 主機	OA	4	2	4	1000	虛擬	
防救災資料庫主機	DB	2	4	32	1000	實體	
全國消防資料庫主機	DB	2	4	16	500	實體	
資料倉儲資料庫主機	DB	1	2	8	3000	實體	
備份主機	管理	1	2	4	250	實體	
虛擬主控台	管理	2	2	4	250	實體	
雲端自動化主機	管理	1	2	2	250	實體	
目錄主機	管理	2	2	4	500	虛擬	
安控主機	管理	2	2	4	250	虛擬	含憑證管理
DNS 主機	管理	2	2	4	250	虛擬	
網管主機	管理	2	2	4	250	虛擬	
NOC 主機	管理	1	2	4	250	虛擬	
SOC 主機	管理	1	2	2	250	虛擬	
異地備援控制主機	管理	1	2	2	250	虛擬	
防毒主機	管理	1	2	2	250	虛擬	
系統管理主機	管理	1	2	2	250	虛擬	
系統效能監測主機	管理	0	0	0	0	虛擬	
原始碼資安掃描主機	管理	0	0	0	0	虛擬	
港消消防主機	代管	1	2	2	250	虛擬	
縣市消防主機	代管	30	2	4	250	虛擬	10 縣市各 3 部
測試主機	測試	0	0	0	0	虛擬	
實體小計 ：		11	42	128	10250		
虛擬小計 ：		114	244	418	38000		
合計 ：		125	286	546	48250		

6.2.1.3. 南部備援中心伺服器清單如下表:

表 122、南部備援中心伺服器清單

名稱	區域	數量	Core	RAM (G)	磁碟 (GB)	形式	備註
民眾入口網主機	DMZ	0	2	4	250	虛擬	
防救災入口網主機	DMZ	2	2	4	500	虛擬	
防災數位學習主機	DMZ	0	2	4	1000	虛擬	
整合通訊主機	DMZ	0	2	4	250	虛擬	
防救災應用主機	防救災	4	4	8	250	虛擬	
GIS 主機	防救災	2	4	8	500	虛擬	
資料倉儲分析主機	防救災	0	2	4	250	虛擬	
企業匯流排主機	防救災	2	4	4	250	虛擬	
資料交換主機	防救災	2	2	4	250	虛擬	
整合通訊主機	防救災	0	2	4	250	虛擬	
雲端檔案系統主機	防救災	0	2	4	1000	虛擬	
決策支援主機	防救災	0	2	4	250	虛擬	
圖資倉儲主機	防救災	0	2	8	1000	虛擬	
氣象局主機	防救災	2	2	4	500	虛擬	
全國消防應用主機	消防	0	2	4	250	虛擬	
辦公室自動化主機	OA	0	2	2	250	虛擬	
Exchange Mail 主機	OA	0	2	4	1000	虛擬	
防救災資料庫主機	DB	2	8	32	1000	實體	
全國消防資料庫主機	DB	0	4	16	500	實體	
資料倉儲資料庫主機	DB	0	4	8	3000	實體	
備份主機	管理	1	2	4	250	實體	
虛擬主控台	管理	2	2	4	250	實體	
雲端自動化主機	管理	1	2	2	250	虛擬	
目錄主機	管理	2	2	4	500	虛擬	
安控主機	管理	2	2	4	250	虛擬	含憑證管理
DNS 主機	管理	2	2	4	250	虛擬	
網管主機	管理	2	2	4	250	虛擬	
NOC 主機	管理	0	2	4	250	虛擬	
SOC 主機	管理	0	2	2	250	虛擬	
異地備援控制主機	管理	1	2	2	250	虛擬	
防毒主機	管理	1	2	2	250	虛擬	
系統管理主機	管理	1	2	2	250	虛擬	
系統效能監測主機	管理	0	2	2	250	虛擬	
原始碼資安掃描主機	管理	0	2	2	250	虛擬	
港消消防主機	代管	0	2	2	250	虛擬	

縣市消防主機	代管	0	2	4	250	虛擬	11 縣市各 3 部
測試主機	測試	0	2	8	250	虛擬	
實體小計 ：		7	26	80	3250		
虛擬小計 ：		25	66	118	8250		
合計 ：		32	92	198	11500		

6.2.2. 防救災雲端實體伺服器數量

除了防救災資訊系統、全國消防資訊系統、一般非主要應用系統的資料庫伺服器應納入虛擬化管理，以共享硬體資源，提高伺服器硬體使用率，並達成節能減碳，綠色環保之需求。

而防救災資料庫伺服器為了更進一步安全之考量則採單獨實體的建置方式，並透過 Cluster 叢集獲得更進一步的安全保障。

6.2.2.1. 虛擬主機伺服器數量

系統運用系統分為 OA(消防)資訊系統及防救災業務資訊系統，於虛擬化的管理建議，除了防救災業務資訊系統的資料庫伺服器及特殊的系統伺服器外，其餘皆將納入虛擬化管理。

(1) 建議虛擬化採 1:10 的比例進行設備數量規劃，計算結果如下；

表 123、大坪林實體主機虛擬化數量試算

項目	台數	CPU Core	RAM
大坪林實體主機預估	149	306	568
1:10 比例虛擬化	15	31	57

以此原則計算中部備援中心與南部備援中心的虛擬主機數量:

表 124、三中心實體主機虛擬化數量試算

項目	大坪林中心	中部備援中心	南部備援中心
實體主機預估	149	139	85
1:10 比例虛擬化	15	14	9

(2) 需求成長預估

預估每年以 10%的比例成長，預留 4 年的成長空間：

15 x 10% x 4 (年) = 6

15 + 6 = 21

以此原則計算中部備援中心與南部備援中心的虛擬主機數量:

表 125、虛擬主機預留成長數量試算

項目	大坪林中心	中部備援中心	南部備援中心
1:10 比例虛擬化	15	14	9
預留 4 年成長	21	20	13

(3) 備援需求預估

大坪林中心提供 2 倍的數量供同地備援與異地備援使用，中部備援中心與南部備援中心因為需要備援大坪林中心，故須提供與大坪林中心相同之數量，數量調整如下：

表 126、虛擬主機預留成長數量試算

項目	大坪林中心	中部備援中心	南部備援中心
Production 虛擬主機	21	20	13
備援虛擬主機	21	21	21
合計	42	41	34

- 虛擬主機伺服器規格數量建議

表 127、虛擬主機伺服器規格表

規格
CPU：提供 4 顆以上 Intel Xeon eight-Core 2.26GHz 以上處理器，CPU 具 18MB 以上 Level 3 快取(cache)記憶體；提供 CPU 散熱裝置。 系統記憶體：提供 96GB 以上 DDR3 以上記憶體，可擴充至 1024GB 以上。 擴充槽(slot)：需提供 7(含)以上之 PCI-E 插槽。 I/O 界面： ◇ 序列埠×1 以上。 USB 2.0×4 埠以上。 提供 KVM(鍵盤、顯示器、滑鼠)連結介面。 硬碟及控制介面：

SAS(Serial Attached SCSI)磁碟陣列控制器，支援 RAID0、1、5、10(RAID 0+1)，支援主機本身安裝 Hot-Swap Bay 4 個以上。 提供 10000RPM(含)以上，SAS 146GB(含)以上，熱抽換式硬碟 2 顆(含)以上，最大支援 12 顆(含)以上。 光碟機：8 倍速(含)以上 DVD-ROM 唯讀式光碟機一台(含)以上。 內建顯示介面，解析度 1024x768 像素以上。 網路介面：10/100/1000 Mbps Ethernet 網路介面 12 個以上，10/100/1000 Mbps 傳輸速度自動切換，最高可支援 30 個(含)以上虛擬網路介面或實體網路介面。 電源及散熱管理： 提供 2 個以上原廠可熱抽換式電源供應器。 提供 2 個以上系統散熱風扇；具備散熱管理、支援損壞警示功能。 原廠機架型主機(提供上機架套件)。 系統管理： 具自我診斷燈號顯示功能，可顯示硬體狀況。 提供該主機原廠伺服器管理軟體。 可透過網路做遠端控制及監督；提供 WEB Based 管理功能或提供 GUI 圖形遠端管理介面。 支援中央處理器、記憶體、硬碟等損壞警示功能。 提供系統管理功能操作手冊。 須通過 BSMI、FCC、UL、CE 等安規之電磁(EMC)檢驗標準。 伺服器搭配系統運作，提供最新中文版 MS Windows Server 或企業版 Linux Server 作業系統授權，須整合於本署現行更新機制並更新至最新 patch(以驗收日期為基準)。

6.2.2.2. 實體主機伺服器數量

目前規劃防救災業務資訊系統的資料庫主機有防救災資訊系統資料庫主機、防救災地理圖資倉儲資料庫主機、資料倉儲資料庫主機。另外各地資訊中心各有一台備份主機，兩台虛擬平台中控主機。

- 資料庫主機規格數量建議

表 128、資料庫主機伺服器規格表

規格
CPU：提供 2 顆以上 Intel Xeon quad-Core 2.4GHz 以上處理器，未來可再擴充二顆處理器，CPU 具 12MB 以上 Level 3 快取(cache)記憶體；提供 CPU 散熱裝置。 系統記憶體：提供 16GB 以上 DDR3 以上記憶體，可擴充至 192GB 以上。 擴充槽(slot)：需提供 2(含)以上之 PCI-E 插槽。 I/O 界面 序列埠×1 以上。

USB 2.0×4 埠以上。 提供 KVM(鍵盤、顯示器、滑鼠)連結介面。 硬碟及控制介面 SAS(Serial Attached SCSI)磁碟陣列控制器，支援 RAID0、1、5、10(RAID 0+1)，支援主機本身安裝 Hot-Swap Bay 4 個以上。 提供 10000RPM(含)以上，SAS 146GB(含)以上，熱抽換式硬碟 2 顆(含)以上，最大支援 8 顆(含)以上。 光碟機：8 倍速(含)以上 DVD-ROM 唯讀式光碟機一台(含)以上。 內建顯示介面，解析度 1024x768 像素以上。 網路介面：10/100/1000 Mbps Ethernet 網路介面 2 個以上，10/100/1000 Mbps 傳輸速度自動切換。 電源及散熱管理 提供 2 個以上原廠可熱抽換式電源供應器。 提供 2 個以上系統散熱風扇；具備散熱管理、支援損壞警示功能。 原廠機架型主機(提供上機架套件)。 系統管理 具自我診斷燈號顯示功能，可顯示硬體狀況。 提供該主機原廠伺服器管理軟體。 可透過網路做遠端控制及監督；提供 WEB Based 管理功能或提供 GUI 圖形遠端管理介面。 支援中央處理器、記憶體、硬碟等損壞警示功能。 提供系統管理功能操作手冊。 須通過 BSMI、FCC、UL、CE 等安規之電磁(EMC)檢驗標準。 伺服器搭配系統運作，提供最新中文版 MS Windows Server 或企業版 Linux Server 作業系統授權，須整合於本署現行更新機制並更新至最新 patch(以驗收日期為基準)。

- 備份主機伺服器規格數量建議

表 129、備份主機伺服器規格表

規格
CPU：提供 2 顆以上 Intel Xeon quad-Core 2.4GHz 以上處理器，CPU 具 12MB 以上 Level 3 快取(cache)記憶體；提供 CPU 散熱裝置。 系統記憶體：提供 4GB 以上 DDR3 以上記憶體，可擴充至 192GB 以上。 擴充槽(slot)：預留 2 個以上 PCI-E 插槽。 I/O 界面： 序列埠×1 以上。 USB 2.0×4 埠以上。 提供 KVM(鍵盤、顯示器、滑鼠)連結介面。 硬碟及控制介面 SAS(Serial Attached SCSI)磁碟陣列控制器，支援 RAID0、1、5、10(RAID 0+1)，支援主

機本身安裝 Hot-Swap Bay 4 個以上。 提供 10000RPM(含)以上，SAS 146GB(含)以上，熱抽換式硬碟 2 顆(含)以上，最大支援 8 顆(含)以上。 光碟機：8 倍速(含)以上 DVD-ROM 唯讀式光碟機一台(含)以上。 內建顯示介面，解析度 1024x768 像素以上。 網路介面：10/100/1000 Mbps Ethernet 網路介面 2 個以上，10/100/1000 Mbps 傳輸速度自動切換。 每台主機需提供 1 埠(含)以上 8Gbps 光纖通道埠介面卡(HBA Card)兩片 電源及散熱管理 提供 2 個以上原廠可熱抽換式電源供應器。 提供 2 個以上系統散熱風扇；具備散熱管理、支援損壞警示功能。 原廠機架型主機(提供上機架套件)。 系統管理 具自我診斷燈號顯示功能，可顯示硬體狀況。 提供該主機原廠伺服器管理軟體。 可透過網路做遠端控制及監督；提供 WEB Based 管理功能或提供 GUI 圖形遠端管理介面。 支援中央處理器、記憶體、硬碟等損壞警示功能。 提供系統管理功能操作手冊。 須通過 BSMI、FCC、UL、CE 等安規之電磁(EMC)檢驗標準。 伺服器搭配系統運作，提供最新中文版 MS Windows Server 或企業版 Linux Server 作業系統授權，須整合於本署現行更新機制並更新至最新 patch(以驗收日期為基準)。

- 虛擬平台中控主機伺服器規格數量建議

表 130、虛擬平台中控主機伺服器規格表

規格
CPU：提供 2 顆以上 Intel Xeon quad-Core 2.4GHz 以上處理器，CPU 具 12MB 以上 Level 3 快取(cache)記憶體；提供 CPU 散熱裝置。 系統記憶體：提供 4GB 以上 DDR3 以上記憶體，可擴充至 192GB 以上。 擴充槽(slot)：預留 2 個以上 PCI-E 插槽。 I/O 界面 序列埠×1 以上。 USB 2.0×4 埠以上。 提供 KVM(鍵盤、顯示器、滑鼠)連結介面。 硬碟及控制介面： SAS(Serial Attached SCSI)磁碟陣列控制器，支援 RAID0、1、5、10(RAID 0+1)，支援主機本身安裝 Hot-Swap Bay 4 個以上。 提供 10000RPM(含)以上，SAS 146GB(含)以上，熱抽換式硬碟 2 顆(含)以上，最大支援 8 顆(含)以上。

光碟機：8 倍速(含)以上 DVD-ROM 唯讀式光碟機一台(含)以上。
內建顯示介面，解析度 1024x768 像素以上。
網路介面：10/100/1000 Mbps Ethernet 網路介面 2 個以上，10/100/1000 Mbps 傳輸速度自動切換。
電源及散熱管理
提供 2 個以上原廠可熱抽換式電源供應器。
提供 2 個以上系統散熱風扇；具備散熱管理、支援損壞警示功能。
原廠機架型主機(提供上機架套件)。
系統管理
具自我診斷燈號顯示功能，可顯示硬體狀況。
提供該主機原廠伺服器管理軟體。
可透過網路做遠端控制及監督；提供 WEB Based 管理功能或提供 GUI 圖形遠端管理介面。
支援中央處理器、記憶體、硬碟等損壞警示功能。
提供系統管理功能操作手冊。
須通過 BSMI、FCC、UL、CE 等安規之電磁(EMC)檢驗標準。
伺服器搭配系統運作，提供最新中文版 MS Windows Server 或企業版 Linux Server 作業系統授權，須整合於本署現行更新機制並更新至最新 patch(以驗收日期為基準)。

6.2.3. 防救災雲端儲存設備數量與容量

(1) 基本儲存需求

根據各地儲存需求規劃，基本儲存空間需求如下：

表 131、各中心儲存數量表

項目	大坪林中心	中部備援中心	南部備援中心
實體磁碟空間預估	57,250 GB	54,750 GB	29750 GB
建議採購	60 TB	60 TB	30 TB

(2) 成長預估

預估每年 10% 資料量增加，以大坪林中心資料計算：

60 x 10% x 4 = 24 (TB)

60 + 24 = 84 (TB)

採購 85 TB，可滿足 5 年成長需求。各中心儲存空間修正如下：

表 132、各中心儲存空間預留 5 年成長數量表

項目	大坪林中心	中部備援中心	南部備援中心

建議採購	60 TB	60 TB	30 TB
預留 5 年成長	85 TB	85 TB	42 TB

(3) 功能需求

磁碟陣列進行備份或異地備援需採用 SnapShot 技術，對資料進行快照，採用 SnapShot 快照需多預留 20%的空間，採用 SnapShot 技術後，磁碟陣列空間修正如下：

表 133、各中心儲存空間預留 SnapShot 數量表

項目	大坪林中心	中部備援中心	南部備援中心
建議採購	85 TB	85 TB	42 TB
預留 SnapShot 20%	102 TB	102 TB	50.4 TB

(4) 備援需求

為避免單一磁碟陣列損毀，需建立備援磁碟陣列進行同地備援，可在主磁碟陣列損毀時快速接手。備援磁碟陣列除了進行同步備援外，亦提供異地資料備援，因此須提供兩倍空間，一部份為同地備援，需提供 1：1 空間，。另一部份為提供異地備援用。備援磁碟陣列規劃空間如下：

表 134、各中心儲存空間預留 SnapShot 數量表

項目	大坪林中心	中部備援中心	南部備援中心
主磁碟陣列建議空間	102 TB	102 TB	50.4 TB
備援磁碟陣列建議空間	204 TB	204 TB	101 TB

6.2.3.1. 大坪林中心儲存設備數量與容量

表 135、大坪林中心儲存設備數量表

儲存設備名稱	容量 (每部)
主磁碟陣列	102 TB 可用空間
備援磁碟陣列	204 TB 可用空間
磁帶櫃	最少須提供具 24 個(含)以上之磁帶槽位(slot)，即非壓縮 36TB(含)以上的磁帶儲存容量

註：(*)異地備援中部、南部備援中心資料

6.2.3.2. 中部備援中心儲存設備數量與容量

表 136、中部備援中心儲存設備數量表

儲存設備名稱	容量 (每部)
主磁碟陣列	102 TB 可用空間
備援磁碟陣列	204 TB 可用空間
磁帶櫃	最少須提供具 24 個(含)以上之磁帶槽位(slot)，即非壓縮 36TB(含)以上的磁帶儲存容量

註：(*)異地備援大坪林、南部備援中心資料

6.2.3.3. 南部備援中心儲存設備數量與容量

表 137、南部備援中心儲存設備數量表

儲存設備名稱	容量 (每部)
主磁碟陣列	50.4 TB 可用空間
備援磁碟陣列	101 TB 可用空間
磁帶櫃	最少須提供具 24 個(含)以上之磁帶槽位(slot)，即非壓縮 36TB(含)以上的磁帶儲存容量

註：(*)異地備援大坪林、中部備援中心

6.2.3.4. 磁帶櫃規格建議

表 138、磁帶櫃規格數量表

規格
具備擴充性，LCD 介面操作控制介面板模組無須置於最頂層。 支持 LTO5、LTO4、LTO3 磁帶機。 最少須提供具 35 個(含)以上之磁帶槽位(slot)，並可擴充至 40 個(含)以上磁帶槽位(slot)，需提供 2 個(含)以上 LTO5 磁帶讀寫頭(Tape Drive)，所有磁帶槽需隸屬於同一磁帶庫所控管。 具備進階的擴充性，19”機架尺寸可隨需求應變容量的成長調整。 提供端對端主動路徑與光纖準備就續檢查，光纖通道阜容錯移轉以及磁帶機效能最佳化功能。 所提供之 LTO5 (含)以上之磁帶機，其速率未壓縮之情況下需可達 140MB/sec 之規格。 磁帶櫃提供之擴充能力須在同一機械臂控制介面之下，即同一機械臂須可存取到所有的磁帶與磁帶機，並提供自動換帶功能的機械手臂(Robotics)。 單卷磁帶容量未壓縮可達容量 1.5TB(含)以上。 傳輸速度：未壓縮可達速度 140MB/Sec(含)以上。 支援作業系統 UNIX、Linux、Windows 等作業平臺。 提供 4GB 或 8GB 光纖通道控制介面。 提供內建的遠端監控軟體與內建的 SNMP 能力，並可支援經由乙太網路的系統遠端事件通知與報告能力。 提供磁帶輸出輸入埠，供磁帶進出作業。磁帶輸入埠/輸出埠至少 4 埠(含)以上。 配置有彩色觸控面版，且系統支援雙電源模組設計可以執行熱插拔(Hot-Swappable)操作。維修或更換電源模組時，並不會影響系統的正常運作。 提供磁帶讀寫頭(Tape Drive)對外的連接介面是 FC 介面。 磁帶讀寫頭(Tape Drive)可執行熱插拔操作，於不斷電的狀態下進行維修工作。 具備特定的清潔磁帶槽位，可經由磁帶櫃本身或備份軟體啟動自我清潔功能。 須支援 Web-Based、SNMP、SMI-S 之管理方式。 提供本機 LCD 介面操作控制介面板及機架相關配件，可讓遠端使用者執行磁帶櫃組態設定、診斷控制及顯示磁帶櫃、磁帶、插槽、系統設定、掛載、I/O、容量及偵錯等狀態，並內建光學條碼閱讀機，以有效管理磁帶。 須提供遠端管理軟體、可設定、監控系統資源及效能且本系統可藉由電腦中的 WEB Browser 執行遠端操控。 提供遠端管理功能 (Remote Management)，可透過瀏覽器界面，進行磁帶櫃的監視、控制、更改設定。 提供磁帶機效能報告、及時及有效益的管理磁帶機的使用實際效能。 磁帶櫃無需外置配置硬件就可以提供及時以及歷史的使用情況及偵錯報告，包括磁帶機讀寫了多少数據，以及加載磁帶的情況等。並且可以跟踪所有磁帶之使用警報歷史、提供完

整性分析及保護寶貴歷史數據。 磁帶櫃無需外置配置硬件，支持瀏覽器界面遠端管理和控制(Remote Management)，進行磁帶櫃的分區(partitioning)，監視、控制、更改設定及支持遠端通知和報警，可以將详细的日誌和分析診斷結果通過 email 發送到系統管理员或者客戶技術服務中心。 要求磁帶櫃中的磁帶讀寫頭(Tape Drive)可執行熱插拔操作，於不斷電的狀態下進行維修工作。

6.2.3.5. 儲存系統規格建議

表 139、儲存系統規格表

規格
每座儲系統需提供 260 顆(含)以上 600GB 15，000 轉之光纖硬碟(Fibre Channel Disk)或 SAS Disk(Serial Attached SCSI)。並支援更換控制機組在不搬動硬碟資料的情況下可擴充達 1100 顆以上硬碟。 儲存控制器支援線上不停機擴充硬碟,所使用之裝置均須具備援容錯及線上抽換(Hot Swap)功能，避免單一元件故障造成停機或資料毀損。 在任一磁碟群組(RAID Group)中，同時任二顆硬碟發生故障時仍可繼續提供服務。 提供 64GB(含)以上記憶體，原機可擴充快取記憶體 512GB(含)以上。 快取記憶體須具備映射保護功能(Cache Mirror)，以保障所寫入的資料不會因快取記憶體故障等因素而造成遺失，遇停電或外部電源故障時，須保護快取記憶體內資料 48 小時(含)以上。 需提供或內建虛擬供應技術軟體(Thin/Virtual Provisioning)及去除重複資料技術軟體，以提升儲存資源的利用率。 內建資料快照及 LUN 完整複製功能，可快速複製資料，快照功能可隨時提供多份複製，且複製後之檔案內容應可在不同之伺服器中獨立存取使用。 儲存設備須能針對前端應用系統的工作負荷狀況分派儲存資源，確保重要的應用系統能有最佳的效能。 須提供在數秒內瞬間還原整個檔案系統(不限容量大小)至任一快照時間點的備份資料功能 提供 Web 或 GUI 管理介面，作為磁碟陣列維護管理及組態設定用，並具主動監督和發生軟硬體錯誤訊息時，以 Email 通知功能 可擴充支援遠端儲存複製功能，可同時支援同步與非同步模式 磁碟陣列系統可支援 Windows，AIX，HP-UX，Solaris，Linux 及 VMware 等多種平台。

6.2.4. 防救災雲端網路設備

6.2.4.1. 大坪林中心

表 140、大坪林中心網路設備清單

項次	設備名稱	數量	目 的
1	線路負載平衡器	2	提供線路備援機制
2	入侵防禦系統	2	主動防禦網路攻擊事件
3	外防火牆	2	提高資料中心之安全性
4	內防火牆	2	內網防火牆，和外網防火牆屬異質防火牆
5	DMZ 區核心交換器	2	DMZ 區 Core Switch
6	核心交換器	2	Core Switch
7	應用負載平衡器	4	提供 Server 負載平衡用
8	廣域負載平衡器	2	提供資料中心負載平衡用
9	專線路由器	2	資料同步用
10	光纖交換器	2	連接磁帶櫃備份之用
11	第二層交換器	6	設備之間連接用

6.2.4.2. 中部備援中心

表 141、中部備援中心網路設備清單

項次	設備名稱	數量	目 的
1	線路負載平衡器	2	提供線路備援機制
2	入侵防禦系統	2	主動防禦網路攻擊事件
3	外防火牆	2	提高資料中心之安全性
4	內防火牆	2	內網防火牆，和外網防火牆屬異質防火牆
5	DMZ 區核心交換器	2	DMZ 區 Core Switch
6	核心交換器	2	Core Switch
7	應用負載平衡器	4	提供 Server 負載平衡用
8	廣域負載平衡器	2	提供資料中心負載平衡用
9	專線路由器	2	資料同步用
10	光纖交換器	2	連接磁帶櫃備份之用
11	第二層交換器	6	設備之間連接用

6.2.4.3.

6.2.4.4. 南部備援中心

表 142、南部備援中心網路設備清單

項次	設備名稱	數量	目 的
1	線路負載平衡器	2	提供線路備援機制
2	入侵防禦系統	2	主動防禦網路攻擊事件
3	外防火牆	2	提高資料中心之安全性
4	內防火牆	2	內網防火牆，和外網防火牆屬異質防火牆
5	DMZ 區核心交換器	2	DMZ 區 Core Switch
6	核心交換器	2	Core Switch
7	應用負載平衡器	4	提供 Server 負載平衡用
8	廣域負載平衡器	2	提供資料中心負載平衡用
9	專線路由器	2	資料同步用
10	光纖交換器	2	連接磁帶櫃備份之用
11	第二層交換器	6	設備之間連接用

6.2.4.5. 網路規格建議

- 線路負載平衡器

表 143、線路負載平衡器規格表

規格
提供 6 個 10/100/1000 Base-TX 介面及 2 個 1000 Base-SX/LX 介面。 提供 1Gbps Throughput 處理能力，支援原機升級至 4 Gbps Throughput 處理能力。 具備支援可達 40 條不同 ISP 線路數。 設備須採用非 Windows/Unix 系列的高安全性之嵌入式即時作業系統(Embedded Real-Time OS)。 支援 10/100/1000Mbps Copper 管理介面，為獨立運作模組，執行管理不影響運作效能。 須支援網路位址轉換功能(NAT)，其中包含靜態通訊埠 NAT、動態多對一 NAT、靜態一對一 NAT，並至少提供 8，000 個 NAT IP 位址之需求。 提供 Router 與 Bridge 功能，支援靜態路由與動態路由 RIP v1/v2、OSPF、VRRP 雙機備援。 路由表須能支援達 30，000 筆。 本設備須支援不同 ISP 線路之上傳(Inbound)及下載(Outbound)多線路負載分配管理功能。 本設備可以針對客戶需求，依照 Source IP、Destination IP、TCP/UDP 應用埠 Service Port，及 HTTP 內容來指定特定線路，並針對線路群組套用不同的負載平衡及備援政策。 本設備須提供下列負載分配模式: 循環模式(Cyclic)。 依線路最少流量者優先分配模式(Least Traffic)。

依線路最少使用者優先分配模式(Least User)。 依線路最快回應時間優先分配(Response Time)。 用戶端至服務端最快時間優先分配(Latency)。 用戶端至服務端最短路徑優先分配(Hop count)。 用戶端至服務端最快時間與最短路徑優先分配(Hop AND Latency)。 依線路之權重分配(Weight)。 依線路之使用成本分配(Cost)。 需提供 Web-based 或是 GUI-based 設備控管軟體，可進行設備之管理、設定及報表功能。 網管設備與所有設備間須提供加密方式連線管理，須可限制管理者由特定之任意實體介面進入控管。 本設備須支援下列管理介面方式與通訊協定： HTTP。 HTTPS。 TELNET。 SSH。 SNMP v3。 Console。 SNMP MIB RADIUS。 SYSLOG。 EMAIL Alert。 符合標準 19 吋機架式規格或可安裝於 19 吋機櫃。

- 入侵防禦系統

表 144、入侵防禦系統規格表

規格
獨立主機須採硬體式設備(Hardware Appliance)架構，並使用嵌入式或專屬作業系統，本身須具備 2Gbps(含)以上處理效能。 具以旁接方式安裝(避免影響網路效能或增加封包延遲)，或提供 in-line 模式雙機備援設計(避免網路單點故障) 例如支援 HSRP 或是 EtherChannel。 須提供 6 個(含)以上自動偵測(Auto-Sensing)10／100／1000 乙太網路連接埠。 具當偵測攻擊行為時，透過 Agent 可即時自動方式隔離單一異常行為來源 IP 位址，使其無法與其他(包括同 VLAN 內)任何主機連線，而不影響其他主機之功能。 可有效阻擋嘗試入侵設備並加以記錄，且支援各種作業系統偵測，並可阻斷異常流量。 須具能夠阻隔以下網路攻擊類型之功能： 拒絕服務(DoS)攻擊，例如：Smurf、Ping of death、Ping sweep、Ping flood、Port sweep、TCP flood 和分散式拒絕服務(DdoS)。 病毒和蠕蟲，例如 Welchia、Slammer、Blaster 和 MyDoom。

變形病毒、混合攻擊(Blended attacks)和未知威脅(Day-Zero Threats)。 須具提供即時告警系統，可直接顯示問題源之資訊，並支援 EMAIL，SNMP，SYSLOG 等方式通知。 可顯示攻擊來源及目的 IP 位址(含 Spoofed IP)、數量及 TCP/UDP 埠號之功能。 須支援 IPv6 網路協定。 具使用者可檢視、更改原廠提供之攻擊行為或特徵資料庫，及自定攻擊行為或特徵資料庫。 設備須可支援集中控管機制。 須具即時警報系統，可透過 E-mail 或 SNMP 等 Alert 方式通知管理者，並須顯示攻擊方式等資訊。 須提供 Web 或 Java 圖形化管理及報表系統。 可分別依據攻擊來源或目的表列並排序之功能。 特徵資料庫(Signature Database)須能透過網路更新。 具備備援電源供應器。 須符合標準 19 吋機架式規格或可安裝於 19 吋機櫃。

- 外防火牆

表 145、外防火牆規格表

規格
獨立主機須採硬體式設備(Hardware Appliance)架構，並使用嵌入式或專屬作業系統(無硬碟)。 須提供 8 個(含)以上自動偵測(Auto-Sensing)10／100／1000 乙太網路連接埠。 Concurrent Sessions 須達 750，000 個(含)以上、New Sessions 每秒須達 25，000 個(含)以上及整體處理效能 Throughput 須達 4Gbps(含)以上。 須具備 IPSec 及 SSL VPN 功能，加密演算法支援 3DES(Data Encryption Standard)及 AES(Advanced Encryption Standard)，且 VPN 處理效能 Throughput 須達 1Gbps(含)以上。 須提供位址轉換(Address Translation)功能： 靜態(一對一)或動態(多對一)之 IP 網路位址轉換(Network Address Translation，NAT)功能，可隱藏真實 IP 位址。 TCP 埠位址轉換(Port Address Translation，PAT)功能。 須具備 URL Block 及 Java Applet、ActiveX 過濾的功能。 支援虛擬防火牆系統(Virtual System)或虛擬路由器(Virtual Router)功能。 須具備網頁式或 Java 管理設定介面。 針對特定過濾之封包，須提供接受(Accept 或 Permit)，禁止(Reject 或 Deny)功能。 支援 H.323、SIP 等 VoIP 以及多媒體視訊會議專用通訊協定。 須具備使用者認證功能(User Authentication)，可內建使用者或支援外部 RADIUS 及 TACACS+，以分散使用者的管理，增強安全性提供進出網路之認證 須具備記錄管理(Syslog/Event logs)和警訊(alarm)，可提供使用者登出入防火牆及任何設定

變更(含防火牆政策)記錄，另可透過本機或經由中央管理軟體提供 E-mail notify 功能。 須支援 IPv6 網路協定。 支援網路設備 HA(High Availability)備援功能，使單機發生故障無法運作時，備援設備可接續網路運作。 獨立主機機箱本身須提供 2 顆(含)以上之電源供應器，具備熱抽取式備援功能。 無授權使用人數限制。 須符合標準 19 吋機架式規格或可安裝於 19 吋機櫃。

- 內防火牆

表 146、內防火牆規格表

規格
內防火牆須採用與外防火牆不同廠牌。 獨立主機須採硬體式設備(Hardware Appliance)架構，並使用嵌入式或專屬作業系統。 須提供 4 個(含)以上自動偵測 10／100／1000 乙太網路連接埠，及 2 個(含)以上 10GbE 網路介面。 Concurrent Sessions 須達 750，000 個(含)以上、New Sessions 每秒須達 50，000 個(含)以上及整體處理效能須達 4Gbps(含)以上。 須具備 IPSec 及 SSL VPN 功能，加密演算法支援 3DES 及 AES，且 VPN 處理效能須達 1Gbps(含)以上。 須具備入侵偵測功能，同時處理效能可達 2Gbps(含)以上。 須提供位址轉換功能： 靜態(一對一)或動態(多對一)之 IP 網路位址轉換 NAT 功能，可隱藏真實 IP 位址。 TCP 埠位址轉換 PAT 功能。 須具備 URL Block、Java Applet 及 ActiveX 過濾的功能。 支援虛擬防火牆系統或虛擬路由器。 須具備網頁式或 Java 管理設定介面。 須可針對來源位址、目的位址及網路服務功能定義交叉混合過濾規則。 針對特定過濾之封包，須提供接受及禁止功能。 支援 H.323、SIP 等 VoIP 以及多媒體視訊會議專用通訊協定。 須具備使用者認證功能(User Authentication)，可內建使用者或支援外部 RADIUS 或 TACACS+，以分散使用者的管理，增強安全性提供進出網路之認證。 須具備記錄管理(Syslog/Event logs)和警訊(Alarm)，可提供使用者登出入防火牆及任何設定變更(含防火牆政策)記錄，另可透過本機或經由集中監控管理系統提供 E-mail Notify 功能。 須支援 IPv6 網路協定。 須具備 Stateful 功能。 須具備韌體更新系統及組態異動功能。 獨立主機機箱本身須提供 2 顆(含)以上之電源供應器，具備熱抽取式備援功能。 無授權使用人數限制。

- DMZ 核心交換器

為配合資料中心各區域的不同需求，本案之核心交換器可根據需求將此設備劃分成 (1) 核心交換器 (2) DMZ 核心交換器等多種交換器之功能，每個劃分出的虛擬交換器均擁有其獨立及專用的軟硬體資源，可將介面 (Interface)，介面卡板 (Interface Card)，路由數目 (Routing Entry)， ACL 數目 (Access Control List)，VLAN 數目 (VLAN Number) 及網路流量管理數目 (Netflow Entry) 等依據需求來做分配，並可經過角色存取控制 (Role Based Access Control) 達成個別管理的目的。

表 147、DMZ 核心交換器規格表

規格
提供至少 8 個使用者介面插槽，每個介面插槽可提供 46 Gbps 至 230 Gbps 的傳輸能力。 系統整體的交換能力最高可擴充 3.68 Tbps 系統可支援至少 128 個 10 GbE 介面 Port 及每個介面插槽至少 60 Mpps 的處理能力。 提供至少 2 個控制引擎模組，具有線上不中斷的備援功能。 每個控制引擎上有獨立的連接管理處理器 (Connectivity Management Processor)，提供遠程 (Remote Light-out) 的管理功能，包括遠程啟動控制引擎等功能，或額外提供終端伺服器以達遠端管理功能。 每一個傳輸引擎 (Forwarding Engine) ASIC 設計，提供 60 Mpps 的二層交換及 MAC 學習能力. 提供 60 Mpps 的 IPv4 處理能力或 30 Mpps 的 IPv6 的處理能力。 支援三個 AC 電源供應器，可提供 N + 1 備援。 支援熱插拔功能 (Online Insertion and Removing) 。 具備二套系統風扇可以互為備援。 劃分後的虛擬化設備容量，可依據需求至多支援到 128 個 10 Gigabit 以太網路介面或 380 個 1 Gigabit 以太網路介面或至多可以支援 60 個線速 10 Gigabit 以太網路介面。 劃分後的各虛擬化設備皆可支援二層 (Layer2) 及三層 (Layer3) 的交換能力。 須通過國際電檢安規認證如 UL、CSA、IEC、FCC Class A 等。

- 核心交換器

表 148、核心交換器規格表

規格
提供至少 8 個使用者介面插槽，每個介面插槽可提供 46 Gbps 至 230 Gbps 的傳輸能

力。 系統整體的交換能力最高可擴充 3.68 Tbps 系統可支援至少 128 個 10 GbE 介面 Port 及每個介面插槽至少 60 Mpps 的處理能力。 提供至少 2 個控制引擎模組，具有線上不中斷的備援功能。 每個控制引擎上有獨立的連接管理處理器 (Connectivity Management Processor)，提供遠程 (Remote Light-out) 的管理功能，包括遠程啟動控制引擎等功能，或額外提供終端伺服器以達遠端管理功能。 每一個傳輸引擎 (Forwarding Engine) ASIC 設計，提供 60 Mpps 的二層交換及 MAC 學習能力. 提供 60 Mpps 的 IPv4 處理能力或 30 Mpps 的 IPv6 的處理能力。 支援三個 AC 電源供應器，可提供 N + 1 備援。 支援熱插拔功能 (Online Insertion and Removing) 。 具備二套系統風扇可以互為備援。 劃分後的虛擬化設備容量，可依據需求至多支援到 128 個 10 Gigabit 乙太網路介面或 380 個 1 Gigabit 乙太網路介面或至多可以支援 60 個線速 10 Gigabit 乙太網路介面。 劃分後的各虛擬化設備皆可支援二層 (Layer2) 及三層 (Layer3) 的交換能力。 本機須通過國際電檢安規認證如 UL、CSA、IEC、FCC Class A 等。

- 光纖交換器

表 149、光纖交換器規格表

規格
提供每台埠數為 12 個(含)以上光纖通道埠以及相關之短波小型可拔插式(Small Form Pluggable，SFP)光學收發器，最大可擴充至 24 個(含)以上光纖通道埠。 支援 Class 2、Class 3、Class F 等光纖通道服務水準及安規認證合格。 提供之光纖埠皆支援 2/4/8 Gbps(含)以上之速率自動偵測，視連接設備自動變更為 2Gbps、4Gbps、或 8Gbps 功能。 具熱插拔之功能。 具備擴充連接埠功能，可透過任一通道插槽與其他交換器進行連接。 可從乙太網路介面(RJ45)或序列埠進行維護。 提供指令列及 GUI 圖形介面管理功能。 具備即時效能監控功能，可透過 GUI 圖形介面或 CLI 指令介面即時觀測交換器流量狀況。 具備 SNMP 管理協定，提供事件記錄、故障警示等功能。 具備開機自我檢測功能。 主機燈號需可顯示通道模組工作狀態及其他交換器硬體環境狀態。 輸入電源：需支援 110V 或 200-240V。

- 專線路由器

表 150、專線路由器規格表

規格
獨立主機本身提供 3 個個(含)以上 10/100/1000 之自動偵測之乙太區域網路介面。 具備 512MB(含)以上記憶體，並且記憶體須可擴充至 1GB(含)以上。 具備 256MB(含)以上快閃記憶體，支援 2GB(含)以上。 路由封包轉送率須可達 250Kpps(含)以上，且同時路由傳輸效能須可達 120Mbps(含)以上。 具備 Layer3 靜態路由設定，及動態路由通訊協定。動態路由通訊協定須支援 RIP v2.0、OSPF、BGP 等。 具備 Multicast Control 功能。 具備 NAT 位址轉換功能。 具備 PAP 或 CHAP 或 RADIUS(Remote Authentication Dial-In User Service)或 TACACS+ 或 ACLs 使用者認證功能。 支援主動發出監控封包及訊息(ICMP、TCP、UDP 及 HTTP)，以監控遠端設備或線路之服務品質(Delay、Jitter、Connectivity 及 Packet loss)。 提供 Console、Command-line 介面或 Web Browser 介面等網路管理功能。 須支援 IPv6 網路協定。

- 第二層交換器

表 151、第二層交換器規格表

規格
單一機體具備 48 個 MDI/MDIX 10/100/1000 Base-TX Ports 單一機體具備 160 Gbps 之 交換容量 (switching fabric capacity)、整體封包傳送效能 (Packet Forwarding Rate) 最高可達 71，400，000pps；每埠可以線速(wirespeed) 1，488，100pps 傳送封包。 提供 port based 及 protocol based 虛擬網路(VLAN) 。 支援虛擬網路數(VLANs)可達 256 個，可支援 16，000 Mac Address。 支援多重(最多 8 個)802.1d Spanning Tree group，充分享有網路設計彈性。 支援 Jumbo frames (封包最大長度 9，216 bytes) 。 支援 IEEE802.3 10BASE-T Ethernet。 支援 IEEE802.3ab。 支援 IEEE802.3u 100BASE-TX Fast Ethernet。 支援 IEEE802.3z 1000base-X Ethernet。 支援 IEEE802.3x Flow Control。 支援 IEEE802.1p Priority Queues with 8 QOS queues。 支援 IEEE802.1Q。 支援 IEEE802.3ad Link Aggregation， 具備 ARP Spoofing，DHCP Snooping/Spoofing 功能。 具備 Syslog 功能，並可將 log 傳送至 Syslog Server 。

支援 WEB-based 管理，管理者可透過網路瀏覽器用 HTTP 及 HTTPS 兩種方式對設備進行管理。 標準 19 吋機架 Standard 19-inch rack-mount width。

- 應用負載平衡器

表 152、應用負載平衡器規格表

規格
本設備具備 4 個(含)10/100/1000 Base-T 自動偵測(Auto-sensing)超高速乙太網路埠高速乙太網路埠及 2 個(含)SPF slot。 本設備須具備 4GB RAM (含)。 本設備須具備 1 個(含) 10/100 Base-Tx 管理介面 與 RS-232 管理介面 須符合 IEEE802.1Q 標準並支援 802.3ad(Port aggregate) 須能提供 Virtual LAN 4094 個以上。 具備 Spanning Tree (IEEE802.1d)能力 including STP MSTP，RSTP 資料處理能力 L4 TCP session Setup Rate，須 60，000 session(含)/秒以上。 L7 TCP session Setup Rate，須 40，000 session(含)/秒以上。 位址辨識能力：須能提供 MAC 位址 2048 (含)個以上。 支援支援 Layer7 的內容操控 (包含插入/移除/修改第 7 層的內容) 本設備須具備以下多種負載平衡模式： ◇Round Robin(輪流) ◇Ratio 或 Weight(權重) ◇Least Connections(最少連結) ◇Fastest 或 Response Time(最快回應時間) 本設備須支援連線堅持(Persistence)技術 ◇Cookie persistence ◇Source address affinity persistence ◇SSL persistence 本設備須具備下列健康狀態檢查功能： ◇Layer 3 checking：ping(ICMP) ◇Layer 4 checking：port service ◇Layer 7 checking：延伸內容檢查(Extended Content Verification) ◇Layer 7 checking：延伸應用程式檢查(Extended Application Verification) 本設備須支援雙機備援模式，至少提供二種(含)以上備援連線方式，包括：Hardware Failover、Network Failover。 本設備須可支援 IPV6 gateway 功能 本設備須支援下列認證方式 ◇RADIUS ◇TACACS+

- 廣域負載平衡器

表 153、廣域負載平衡器規格表

規格
本設備具備 4 個(含)10/100/1000 Base-T 自動偵測(Auto-sensing)超高速乙太網路埠及 2 個(含)SPF 擴充介面。 本設備須具備 4GB RAM (含)。 本設備須具備 1 個(含) 10/100 Base-Tx 管理介面 與 RS-232 管理介面 須符合 IEEE802.1Q 標準並支援 802.3ad(Port aggregate)須能提供 Virtual LAN 4094 個以上。 硬體整體效能 1Gbps(含)以上 須符合 IEEE802.1Q 標準並支援 802.3ad(Port aggregate) 需內建或支援 BIND DNS v9 或同等品 支援標準 DNS SOA，A，Cname，MX record，DNSSec。 具備加密安全網頁管理 DNS 介面：如 HTTPS。 自動控制全區 DNS 記錄更新檔案無需重啟 DNS 服務 支援每秒至少 80，000 筆 DNS 查詢 針對一個 DNS A Record 可以依據負載平衡演算法回應最佳的 IP Address。 支援 SIP、Oracle、POP3、SMTP、HTTP、FTP 等應用程式檢查機制決定 DNS 回應結果。 可整合後端負載平衡伺服器的檢查機制做為廣域負載平衡條件。 DNS 演算機制除了主要演算法之外還支援次要演算法及備援演算法。 至少支援下列負載平衡演算法 ◇Round Robin ◇Ratio ◇Global Availability ◇Topology ◇Real Server 的系統狀態 ◇Server 或 L4 device Completion Rate ◇Server 或 network interface Packet Rate ◇Virtual Server 系統狀況及上述監控條件做複合負載平衡 ◇依據 Topology，自定地區，國家及 LDNS IP 地址作出自定負載平衡演算法 支援 SSH 及 HTTPS 管理 支援 IP v6 及 IP v6 DNS 服務 須為標準 19”機架式尺寸。

6.3. 機房及環控需求規劃

6.3.1. 機房空間配置規劃

為符合本專案因各方面之需求，在機房施工與佈建上，亦需根據實際環境需求，及有關機房監控機制、電力配置、冷氣空調等等考量進去，以利後續能有完整之維運。

本專案之機房需求，需配合消防署機房之環境，擬整合現有資訊設備及相關網路、作業環境等需求，並需完整規劃相關主機房空間規劃、通訊纜架、環境監控、空調系統、不斷電力工程等做適當之設計調整，以確保系統正常運作，不致因為任何因素而導致停頓，影響相關資訊業務之推展。

6.3.1.1. 一般規定

1. 內外阻隔：機房與公共區域應規劃分開。
2. 機房建議設計為單獨出入口，當與其他部門共用出入口時，應避免人流、物流的交叉。
3. 管道規劃與設計，不論是電路、水路、油路與電信網路應儘量具備兩套以上的管道，一套提供營運服務使用外，另外一套則是提供備援。
4. 主機房內通道與設備間的距離應符合下列規定：
    - 兩相對機櫃正面之間的距離不應小於 1.2m；機房建築的入口至主機房應設通道，通道淨寬不應小於 1.5m。
    - 機櫃側面(或不用面)距牆不應小於 0.5m，當需要維修測試時，則距牆不應小於 1.2m；
    - 走道淨寬不應小於 1.2m。
5. 在施工時應保證現場、材料和設備的清潔。隱蔽工程(如地板下、吊頂上、假牆、夾層內)在封口前必須先除塵、清潔處理，暗處表

層應能保持長期不起塵、不起皮和不龜裂。

6. 機房所有管線穿牆處的裁口必須做防塵處理，然後對縫隙必須用密封材料填堵。在裱糊、粘接貼面及進行其他塗複施工時，其環境條件應符合材料說明書的規定。裝修材料應選擇無毒、無刺激性的材料，儘量選擇難燃、阻燃材料，否則應盡可能塗防火塗料。

7. 對於集中荷重區(如變壓器、UPS，電池，發電機等)之至放區域，應考量樓板承載進行結構補強或防振之工程。

6.3.1.2. 機房空間配置注意事項

1. 依據現場實際環境，設置適當的隔熱設施與相關工程。

2. 針對機房出入口，須以安全性、出入管制便利性、設備進出便利性為設計參考依據。

3. 機房控制室出入口之位置亦須留意，避免因監視器或相關硬體設施，而造成不便。

4. 機房內不應配置操作人員辦公區與儲藏區。

5. 規劃時須留意高架地板線槽，以及地板下線槽關係空調設計(如:下吹式、直吹式等等)。

6. 電力線路與資通線路部分，建議隔離佈建，以避免電力或線路受到干擾，而一切規劃依據實際環境而定。

7. 於規劃地板線槽佈線時，建議須搭配機櫃位置，且應考量加強冷熱通道設置，以及考量空調出風冷熱通道問題。

8. 在空調冷卻水管線佈建規劃方面，建議規劃管線備援線路設計，而一切規劃依據實際環境而定。

9. 環控設施部分，建議考量將溫度、濕度、漏水、空調、消防、市電、發電機、UPS 等等，皆考量在環控範圍之內，以確保機房之整體環控效果。

6.3.1.3. 吊頂

1. 電腦機房吊頂板表面應平整，不得起塵、變色和腐蝕;其邊緣應整齊、無翹曲，封邊處理後不得脫膠;填充頂棚的保溫、隔音材料應平整、乾燥，並做包縫處理。
2. 按設計及安裝位置嚴格放線。吊頂及馬道應堅固、平直，並有可靠的防銹塗覆。金屬連接件、鉚固件除鏽後，應塗兩遍防銹漆。
3. 吊頂上的燈具、各種風口、火災探測器底座及滅火噴嘴等應定準位置，整齊劃一，並與龍骨和吊頂緊密配合安裝。從表面看應佈局合理、美觀、不顯凌亂。
4. 固定式吊頂的頂板應與龍骨垂直安裝。雙層頂板的接縫不得落在同一根龍骨上。
5. 用自攻螺釘固定吊頂板，不得損壞板面。
6. 活動式頂板的安裝必須牢固、下表面平整、接縫緊密平直、靠牆、柱處按實際尺寸裁板鑲補。根據頂板材質作相應的封邊處理。
7. 提供機房內所需之足夠照明，並須提供 600 Lux 以上之照度，須附照度表。

6.3.1.4. 隔斷牆

1. 無框玻璃隔斷，應採用槽鋼、全鋼結構框架。牆面玻璃厚度不小於 10mm，門玻璃厚度不小於 12mm。表面不銹鋼厚度應保證壓延成型後平如鏡面，無不平的視覺效果。
2. 石膏板、吸音板等隔斷牆的沿地、沿頂及沿牆龍骨建築圍護結構內表面之間應襯墊彈性密封材料後固定。當設計無明確規定時固定點間距不宜大於 800mm。
3. 有耐火極限要求的隔斷牆豎龍骨的長度應比隔斷牆的實際高度短 30mm，上、下分別形成 15mm 膨脹縫，其間用難燃彈性材料填實。

全鋼防火大玻璃隔斷，鋼管架刷防火漆，玻璃厚度不小於 12mm，無氣泡。

4. 安裝隔斷牆板時，板邊與建築牆面間隙應用嵌縫材料可靠密封。
5. 有耐火極限要求的隔斷牆板應與豎龍骨平等鋪設，不得與沿地、沿頂龍骨固定。
6. 隔斷牆兩面牆板接縫不得在同一根龍骨上，每面的雙層牆板接縫亦不得在同一根龍骨上。
7. 安裝在隔斷牆上的設備和電氣裝置固定在龍骨上。牆板不得受力。
8. 隔斷牆上需安裝門窗時，門框、窗框應固定在龍骨上，並按設計要求對其縫隙進行密封。

6.3.1.5. 鋁合金門窗和隔斷

1. 鋁合金門框、窗框、隔斷牆的規格型號應符合設計要求，安裝應牢固、平整，其間隙用非腐蝕性材料密封。當設計無明確規定時隔斷牆沿牆立柱固定點間距不宜大於 800mm。
2. 門扇、窗扇應平整、接縫嚴密、安裝牢固、開閉自如、推拉靈活。
3. 施工過程中對鋁合金門窗及隔斷牆的裝飾面應採取保護措施。
4. 安裝玻璃的槽口應清潔，下槽口應補墊軟性材料。玻璃與扣條之間按設計要求填塞彈性密封材料，應牢固嚴密。

6.3.1.6. 高架地板

1. 高架地板下的地面和四壁裝飾，可採用水泥砂漿抹灰。地面材料應平整、耐磨。當高架地板下的空間為靜壓箱時，四壁及地面均應選用不起塵、不易積灰、易於清潔的飾面材料，不得起皮和龜裂。
2. 主機房和基本工作間的內門、觀察窗、管線穿牆等的接縫處，均應採取密封措施。

3. 當主機房和基本工作間設有外窗時，宜採用雙層金屬密閉窗，並避免陽光的直射。當採用鋁合金窗時，可採用單層密閉窗，但玻璃應為中空玻璃。

4. 當主機房內設有用水設備時，應採取有效的防止給排水漫溢和滲漏的措施。

5. 當房間內有強烈震動的設備時，設備及其通往主機房的管道，應採取隔震措施。

6. 現場切割的地板，周邊應光滑、無毛刺，並按原產品的技術要求作相應處理。

7. 高架地板施作高度應按實際需要確定，但至少達 35cm 以上(理想高度在 18-24 英寸(46-61cm)之間)。

8. 機房區域採用的高架地板可由鋼、鋁或其他阻燃性材料製成(如鋁合金 500 型)。

9. 高架地板下須建置保溫層，防止下一樓層之結露滴水。

10. 高架地板下接地銅網採用 3.5mm 裸銅線，應符合電力，電信施工接地規範及 IEEE 標準電力接地電信接地邏輯(設備)接地。

11. 採蜂巢板製作安裝，蜂巢板出風率至少達 16%

12. 高架地板週邊做 V 型斜支撐

13. 高架地板下應安裝地網

6.3.2. 電力系統規劃

6.3.2.1. 電源分類：

1. 市電：由電源分電盤分別送至空調、照明配電箱和維修插座配電箱，再分路送至燈具及牆面插座。

2. UPS：由電源分電盤引至牆面配電箱，分路送到高架地板下插座，

再經插座分接電腦電源處。

3. 柴油發電機組：是作為特別重要負荷的應急電源，正常情況下的運行方式為，柴油發電機組始終處於準備發動狀態，當市電均中斷時，機組應立即啟動，並具備帶 100%負荷的能力。市電恢復時，機組應能自動退出運行並延時停機，恢復市電供電。機組與電力系統間應有防止並列運行的連鎖裝置。柴油發電機組的容量應按照用電負荷的分類來確定，因為有的負荷需要很大的啟動功率，如空調電動機，應考量機組容量，以避免產生過大的啟動電壓降，一般根據上述用電負荷總功率的 2.5 倍來計算。

4. 機房系統供配電系統應考慮設備未來擴充、升級等可能性，應預留備用容量。

6.3.2.2. 電力系統設計原則

1. 電力系統提供雙迴路不中斷電源供應系統給所有機櫃，並對空調系統和其他用電設備單獨供電，以避免空調系統啟停對重要用電設備的干擾。且每迴路中之不中斷電源供應系統單體於最大負載時為 n+1 並聯供電，可供應全載 20 分鐘以上；並設置發電機組備用電力，二十四小時以上之油槽及戶外加油管路等，以供穩定且乾淨的電力需求。燃油供應可考慮與供油之廠商簽訂供油合同，提供一小時可送達燃油服務。

2. 機房宜由專用電力變壓器供電。機房內其他電力負荷不得由電腦主機電源和不間斷電源系統供電。主機房內宜設置專用動力配電箱。

3. 電力線槽以配置於高架地板下方為原則，機房高架地板下的低壓配電線路宜採用銅芯遮罩導線或銅芯遮罩電纜，電源線應盡可能遠離電子設備信號線並避免並排敷設。當不能避免時，應採取相應的技術措施。高架地板下敷設的電纜一般採用金屬線槽保護。電纜線配置於線槽內需整齊收容。

4. 主機房內應分別設置一定數量的維修和測試用電源插座，兩者應有

明顯區別標誌。測試用電源插座應由電腦主機電源系統供電。其他房間內應適當設置維修用電源插座。

5. 相關配置迴路銜接電力線槽須採用管接，與插座間採 PVC 被覆金屬軟管。

6. 電力管線需穿越各樓層或隔間牆時其相關銑孔需進行防火填塞。

7. 盤面設計應設置數位式集合式電表，且主要盤體須加設燈具照明。

8. 電力設計需考慮功率因數改善。單相負荷應均勻地分配在三相線路上，並應使三相負荷不平衡度小於 20%。

9. 配電箱、櫃應有短路、過載保護，其緊急斷電按鈕與火災報警連鎖。

6.3.2.3. 電力系統設計注意事項

整體電力工程需完整考量包含：不斷電系統、空調、照明、配電盤及機櫃電源等等。

1. 在規劃電源迴路時，須考量到 UPS 備援電力問題，及動力管線工程問題。

2. 設計規劃需考量未來擴充性及維運便利性。

3. 得標商未來須提出設計架構與方式，且須能支援機房內所有機器設備之用電。

4. 電力設計需能支援環境監控系統，以便監測運作、跳脫狀態，可從環境監控系統得知用電狀況，包含電壓、電流、不斷電系統及市電運作是否正常，若發生異常可由環境監控系統通知操作人員。

5. 環控系統需在該迴路用量 80%時，由環控系統發出警告。

6. 設置數位式集合電表，裝置於相關配電盤體或 PDU 盤上，且需可監視每一機櫃用電迴路之用電量。

7. 本專案電力纜線以配置於高架地板下方為原則，並須單獨配置於金

屬線槽內整齊收容。

6.3.2.4. 電力設計內容

1. 不斷電系統。

(1) 本專案需至少須提供 2 台以上 120KVA 不斷電主機(UPS)。

(2) 須為 on-line 型式，並考慮未來擴充性及可同時維護性。

(3) UPS 提供相關電腦設備及主機房部分緊急照明電力。

(4) 須提供 120KVA 負載滿載時能維持 10 分鐘以上供電能力。

(5) 新增 UPS 須與現有發電機連接，並預留銜接後續擴建新增電力系統。

(6) 輸入電壓三相四線 380VAC±10% 60HZ、電壓可調範圍±5%、總諧波失真低於 5%、功率因素 0.9 以上，整體效率 92%以上，並聯功能：單機需內含並聯介面卡及另提供原 UPS 之並聯介面卡各一套，可依現場需求擴充並聯運作，提供 N＋1 擴充電力。可透過網路監控使用及整合到環控系統工程使用。

(7) 提供指示狀態模擬圖,LED 或 LCD 面版需能顯示電壓、電流、頻率、電池電壓、故障顯示。

(8) 當不斷電系統需要維修時，可讓系統均能自市電與負載完全切離，其切換方式採先投入後切離方式。

(9) 提供相關通訊介面，例 RS232、AS400、RS485，供環控系統整合。

(10) UPS 設備、開關箱及電池箱，均應加裝壓克力牌標示名稱及注意事項。

(11) 電池須為免維護式全新品，電池應為免保養電池或鉛鈣免加水電池或密閉式免維護。

(12) 所有電池均須安置於固定式電池箱內，且須加裝開關保護。

(13) UPS 及電池組(架)須考慮安運空間與維護動線。重量需符合安裝位置條件，必要時須經專業技師計算或補強後方可施作。

(14) 電池組(架)如需安裝於機房內，須考慮電池組(架)充放電釋出氣體，增設專屬抽風裝置。

2. 配電盤工程：

(1) 需依插座電力負載及空調電力設備負載需求，提出適當可行之負載分配。

(2) 配線及結線方式需依電工法規等相關之規定施作，並應由有執照之電工承辦。

(3) 所有配電箱內應標示各迴路用途或佈線迴路，箱外並以壓克力名牌標示。

(4) 專用分電盤提供各電腦設備使用之獨立控制/保護開關迴路。

(5) 提供預留迴路及容量。

(6) 需配合 CCTV、門禁監控、環境監控及消防設備等設置必要之 UPS 電源。

(7) 每一組出線口之插座,若有 110V 或 220V 或其他電壓規格，需標示清楚，並標示相對之 UPS 及配電盤之位置。

(8) 須有一緊急開關置於操作室，可切斷電源系統。

(9) 配合電盤設計，機櫃需設計每個機櫃雙迴路電源 220V 及 110V(設計量為 20%)。

(10) 電機技師簽證(不含相關事業送審)。

6.3.3. 空調系統規劃

1. 主機房和基本工作間空調系統的氣流組織，應根據設備對空調的要求、設備本身的冷卻方式、設備佈置密度、設備發熱量以及房間溫濕度、室內風速、防塵、消音等要求，並結合建築條件綜合考慮。

2. 在空調系統方面，空調和製冷設備宜選用高效、低雜訊、低震動的設備，並有自動復歸之功能。若選擇獨立式電腦恆溫恆溼下吹式水冷空調主機，採下送風上回風方式，以保證空氣的流通性，建構模式應採用 N+1 之設計理念，冷卻水塔亦同，並具備用儲水槽及屋外加水管

路。

3. 機房的風管及其它管道的保溫和消聲材料及其粘結劑，應選用非燃燒材料或難燃燒材料。冷表面需作隔氣保溫處理。採用活動地板下送風方式時，樓板應採取保溫措施。

4. 主機房內的設備需要用水時,其給排水幹管應暗鋪,引入支管宜暗裝。管道穿過主機房牆壁和樓板處，應設置套管，管道與套管之間應採取可靠的密封措施。

5. 水冷式空調系統主機下方應設置 Epoxy 止水墩,以防滲漏水漫入機房其它地區，並加裝自動排水系統，於滲漏水時可自動排出。

6. 一般伺服器之機架，設計容量每機架散熱 5KW，若使用刀鋒等高散熱設備，設計容量每機架散熱 10～15KW。

7. 空調系統需有備援電力系統提供市電停電下，電力之持續供應。

8. 機房溫度需保持在 20±2°C；相對濕度保持在 45%~65%。

9. 空調製冷設備的製冷能力，應留有 15%-20%的餘量。

10. 與主機房無關的給排水管道不得穿過主機房。

11. 冷卻水塔擺放位置、管路走法選定及協調管委會。

12. 依現況新增下吹式恆溫恆濕空調機，空調機應有備援之設計考量。

13. 電腦機房空調系統建置，需考量到整體散熱的能力及冷熱通道之建立。建立熱通道隔離機制，以減少冷熱混風提高冷房效能，設計時須同時考量機房內之恆溫控制，以確保設備之安全性。

14. UPS 室或電池室應設有排風系統，設置獨立空調設備。

15. 預留氣冷式冰水主機作為備援系統的擴充性。

16. 冷氣須有自動切換功能、自動平衡功能。

17. 需有漏水偵測系統。

18. 本案之規劃設備，主要伺服器為 36 部，以每部機櫃安裝 8 部 4U 伺服器計算，需 5 個伺服器機櫃。依
冷氣使用之噸數(USRT)與電力 WATTS 換算公式為
1 BTU/hr = 1 WATTS*3.413
1 USRT = 12，000 BTU/hr
以每部伺服器滿載時發熱 2KW 計算，計約 72KW；非滿載時平均發熱 1.1KW 計算，計約 39.6KW。

6.3.4. 環控系統規劃

資訊機房為資訊設備運轉的重要地點，如何建置適合資訊設備運轉的環境及確保環境穩定運轉，機房建置中的五大系統，電力、空調、消防、安全及環控是相互依賴，任何一個機電的問題，都會導致上述系統的異常，而引發更大的災害。透過各項系統連動功能，可以控管機房內部各項子系統運作情形，亦可透過遠端連線了解機房運作狀況，若發生異常狀況時，可透過告警子系統提供警告，立即得知機房變化情況，做最快速的反應措施，同時可以記錄機房運作情況，紀錄各項設備運轉情況，作為機房運轉調整之依據。各區域資料中心之資訊機房皆採行 7*24hr 運轉模式，如何使各值班人員或機房維運人員簡單方便的了解機房運作狀態，以預防資訊機房系統的故障，為機房環控系統之最終目的。

6.3.4.1. 環境監控系統軟體

1. 全中文化視窗操作環境，所有畫面一律採用中文顯示。
2. 具 Web 操作介面，可遠端監視機房各項設備狀態及強制啟動待控設備。
3. 內建多種界面驅動程式，包含 RS-232/RS-485、FieldBus、DeviceNet、CanBus 及 ProfiBUS，可直接連接多類裝置。
4. 內建工業標準 OPC Client 功能，可與多類 OPC Server 直接連

接。

5. 支援多種網路通訊協定，包含 TCP/IP、UDP、DDE、ActiveX、SNMP、XML、.NET。

6. 支援多種圖檔格式，包含 BMP、JPEG、PNG、GIF、WMF、DWG。

7. 提供所有監測設備之即時、歷史資料查詢及列印功能，操作人員可選擇列表或圖型(趨勢圖或統計長條圖)顯示列印。

8. 監測設備須可自行設定上、下限警戒值，並可自訂各項警訊告警優先權順序，並依順序發出警訊。

9. 提供操作人員新增、修改、查詢及刪除告警訊息傳送之 Email 位址(需無組數限制)，並可做 Email 群組編輯(可依據警報事件之嚴重性等級，設定不同之之 Email 位址) 。

10. 警訊發生時，應於配置圖位置以動態圖形及不同顏色方式指出警報點之位置與內容，並發出告警語音提醒操作人員即時處理。

11. 可由操作人員設定各項警訊告警優先權順序；警訊發生時，系統根據警訊優先權順序播放告警語音及決定警訊撥號先後順序。

12. 警訊發生或復歸時，現場監控電腦自動啟動 E-mail、簡訊系統、信差服務，傳送告警訊息至預設之各台電腦 (訊息內容須包含警訊類型、發生或復歸時間及警報值)。

13. 警訊發生時，顯示裝置立刻在監測區域配置圖位置以動態圖形及不同顏色方式明確指出警報點之位置與內容，並發出告警語音提醒操作人員即時處理。

14. 警訊發生或復歸時，現場監控電腦自動啟動簡訊及 Email 系統，傳送警訊訊息至預設之行動電話或 Email 位址，簡訊內容須包含警訊類型、發生或復歸時間及警報數值。

15. 警訊發生或復歸時，現場監控電腦自動啟動語音撥號系統，透過預

設之緊急聯絡電話，播放警訊相關之告警語音，語音內容須能清楚敘述警訊類型及警報數值。

16. 警訊發生或復歸時時，現場監控電腦自動發送 SNMP TRAP，傳送告警訊息至預設之 TRAP Receiver，訊息內容須包含警訊類型、發生或復歸時間及警報數值。

6.3.4.2. 電力系統監控：

電力系統係為機房運作能否之主要關鍵，對於資訊機房所需之不斷電系統及空調系統，皆須提供穩定的電力供電系統。

電力各項系統運作若能充分的掌握狀態，可以避免電力系統的故障跳脫，如若能掌控電力系統各幹線迴路用電品質狀態，在事故發生前作預警性的警告，電力系統迴路發生故障時，若能立即得知故障地點斷路器，即可立即將故障排除，確保系統供電穩定，以上功能皆可透過環境控制系統提醒值班人員做緊急狀態的處理，避免電力系統潰決。

本專案在規劃所需之供電需求同時，所需注意電力監控之功能，所需注意事項包含：

1. 電力狀態偵測：

監測市電供電品質(含電壓、電流、功率、頻率、功因)及提供上、下限警戒監視。

2. 不斷電系統偵測：

需提供 UPS 電力系統，及緊急供電系統橋接(新增 UPS 含線路)，監測 UPS 系統供電品質(含輸出入電壓、輸出入電流、輸出功率、輸出頻率、電池電壓、負載%比)、輸出電壓、電流及負載上、下限警戒、運轉狀況、電池低電位警示、市電供電、電池供電監視。

3. 發電機電力狀態偵測：

發電機運轉狀況、供電品質(含電壓、電流、功率、頻率)、油位監視、溢漏監視、啟動電池狀態監視、發電機遠端啟動、停止控制。而發電機擺放位置，則需於得標後，依實際環境及與協調管委會共同討論。

6.3.4.3. 空調系統監控功能

空調系統最主要的工作是將機房內部的熱散出，保持機房內部工作溫度，避免資訊設備發生過熱。監控之功能含：

1. 監視及控制機房冷氣機運轉/停止狀態。
2. 冷氣輪替切換自動排程交替運轉、異常時自動切換、室溫過高時自動啟動備援空調。
3. 電子設備機房內有空調系統或供暖系統，必要時在空調機四周、水管沿線等處，鋪設液漏水偵測系統 sensor。
4. 漏水位置顯示。與自動排水系統聯動，自動偵測水位啟動排水馬達，進行漏水之排放。
5. 遠端電腦可經由 Web 界面強制啟動空調箱。

6.3.4.4. 消防系統監控功能

1. 消防主機正常、異常監視。
2. 消防一次感知、火警警報監視。

6.3.4.5. 環境偵測：

機房溫/濕度監測與記錄，提供上、下限警戒監視。

6.3.4.6. 門禁系統監控功能：

門禁系統各門禁控制器啟閉狀態監視(開啟過久需發出警報)及控制。

6.3.5. 監視系統規劃

1. 機房中有大量的伺服器及機櫃、機架。由於這些機櫃及機架一般比較

高，所以監控的死角比較多，因此在電視監控布點時主要考慮各個出入口，每一排機櫃之間安裝攝像機。如果在各出入口的空間比較大，可考慮採用帶變焦的攝像機。

2. 一般情況下，定焦攝像機在光照度變化大的場所應選用自動光圈鏡頭並配置防護罩，在光照穩定光源充足的地方，用固定光圈鏡頭可降低成本。

3. 圖像信號應保持 24 小時錄影,錄影保存 3 個月,7*24 小時集中監視。錄影方式可採用硬碟錄影，也可採用傳統的錄影系統。閉路電視控制系統最好有視頻動態報警功能。同時如果具有視頻遠端傳輸功能，可通過 Internet 或區域網路將監視信號傳輸到遠端，增加監控之方便性。

4. 在安裝閉路電視的同時，也可考慮在重要的機房媒體存放區安裝防盜報警系統以增加防範機制

5. 輔以閉路監視系統，提供彩色 CCD 於重要出入之地點，主機房內重要設備，並進行 24 小時之監視錄影作為整體監視管理。

6. 監控範圍為本專案之北區主要營運中心機房。

7. 監視器要有夜視功能。

8. 須有動態錄影存檔功能。

9. 監控儲存量最少 3 個月以上。

6.3.6. 消防系統規劃

1. 機房圍護結構的構造和材料應滿足保溫、隔熱、防火等要求，耐火等級應符合現行國家標準(耐火一級)，並儘量採用綠建材以符合環保之要求。

2. 機房與其他建築物合建時，應單獨設防火分區。

3. 機房的安全出口，不應少於兩個，並宜設於機房的兩端。門應向疏散

方向開啟，走廊、樓梯間應暢通並有明顯的疏散指示標誌。主機房出口應設置向疏散方向開啟且能自動關閉的門。並應保證在任何情況下都能從機房內打開。

4. 機房應設置疏散照明和安全出口標誌燈

5. 為確保機房為密閉空間，自動滅火系統噴發藥劑可達滅火之功能，需進行氣密測試。

6. 需設立排風系統，以確保藥劑噴發後人員進入之安全。

7. 報警系統和自動滅火系統應與空調、通風系統連動。空調系統所採用的電加熱器，應設置無風斷電保護。

8. 設置固定滅火系統及火災探測器的機房，其吊頂的上、下及活動地板下，均應設置探測器和噴嘴。探測器應採用感煙、感溫兩種探測器的組合。

9. 機房內存放記錄介質應採用金屬櫃或其他能防火的容器。

10. 可採用極早期偵煙監控警報系統(VESDA)及 FM-200、FE-13 等氣體式滅火系統(需符合 NFPA 2001 – 為無污染自動滅火系統，系統及氣體經中華民國內政部消防署認證許可使用)，並備有手提式二氧化碳(CO2)滅火鋼瓶，以備不時之需。

11. 消防控制中心包括智慧火災報警控制主機，用於集中報警及控制。消防控制中心週邊聲光報警系統及控制包括光電感煙探測器、感溫探測器、組合控制器和氣瓶等。上述設備位於現場和端子箱內(需符合中華民國內政部消防署各類場所消防設備設置標準)。

12. 消防技師簽證(不含相關事業送審)。

13. 滅火氣體(藥劑)：採用 FM200 滅火藥劑。

14. 消防系統完成後必須要作功能之測試。

15. 消防有誤報取消功能。

16. 需設極早期火災預警系統(VESDA)。

17. 消防警報需接至大樓系統。

18. 消防啟動時需有空調停機、門禁開啟之功能。

19. 需設消防排氣系統。

20. UPS 室各需設置 1 具 10 磅(含)以上環保型手提滅火器(環保藥劑)。

21. 使用防火填縫劑於隔間縫隙或貫穿結構的縫隙，做為防火填塞膠。

22. 發生火災時，空調主機必須經由環境設備控制主機關閉，避免擴大火災災害。

23. 在系統設備方面，本系統須為一完整全自動滅火系統，即包括所有必須之電氣及機械設備安裝。為顧及全系統完整發揮效能及穩定之品質採用之全套同一廠牌設備，其主機設備和各項設備及其配件之安裝、測試須有內政部消防署認同，並再經消防署發函認證許可。

6.3.7. 門禁系統規劃

門禁管理系統的主要目的是保證重要區域設備和資料的安全，便於人員的合理流動,對進入這些重要區域的人員實行各種方式的門禁管理，以便限制人員隨意進出。

1. 卡片最好採用現在流行的感應式卡片。

2. 門禁卡出入系統首先應具有許可權設置的功能，即每張卡可進出的時間、可進出哪道門，不同的卡片持有者應有不同的許可權。

3. 每次有效的進入都應存檔或統計。

4. 應有完善的密碼系統，即對系統的更改，不同的操作者應有不同的許可權。

5. 電鎖應採用安全可靠的產品，有電閉鎖或無電閉鎖根據用戶要求可

調。

6. 緊急情況下或電鎖出現故障的情況下應有應急鑰匙可將門打開。

7. 門禁系統最好採用電腦控制系統。

8. 全套系統應有備用電源。

9. 整合樓層之門禁系統，並具有報表管理軟體及視窗操作環境之安全管理功能。

10. 系統所使用的軟、硬設備必須具有高效率，以及高穩定性之特色。

11. 須提供緊急逃生開關。

6.3.8. 機房現況與建議

依據以上機房建置之規劃需求，參照各機房現況、規劃文件以及系統建置文件，提出各機房相關建議如下：

6.3.8.1. 大坪林機房

依據「消防署設備虛擬化建置案」之機房環境改善需求，工作計畫書以及大坪林機房現況，提出以下基礎設施建議事項：

機房對外落地窗實體隔熱設施

機房面向北新路之玻璃落地窗外牆，建議整體加強隔熱設施，阻絕外部熱源進入，以降低外部溫度變化對內部溫度的影響，解決外部高溫加上陽光直射造成的空調效率不足之狀況，提升空調設施之冷卻效率，節省空調電力之耗用。

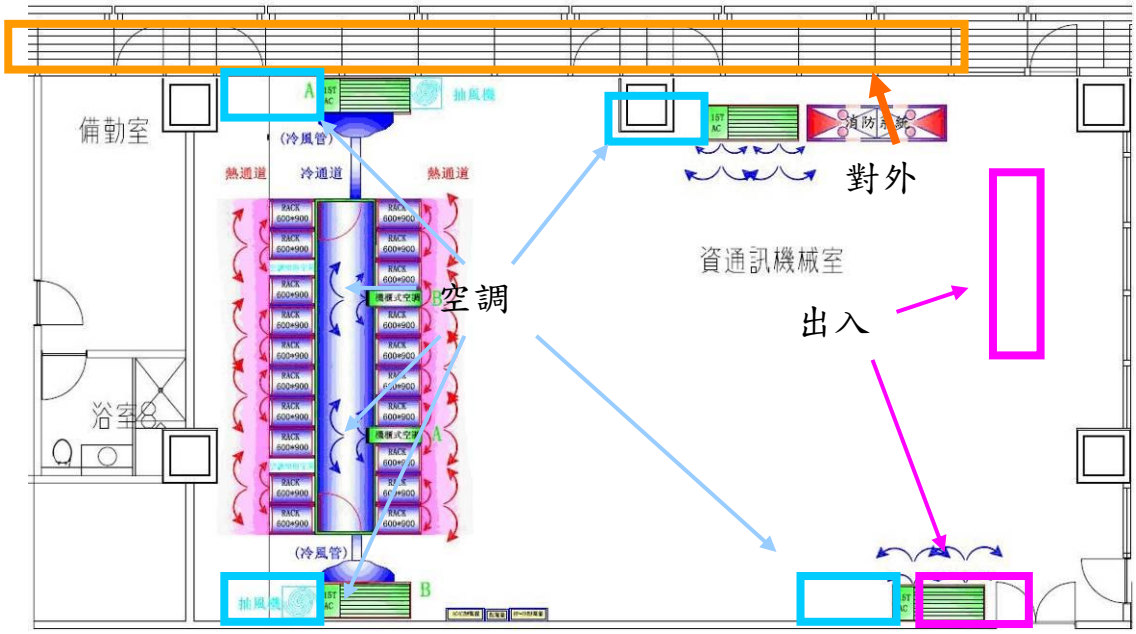

圖 500、大坪林機房空間配置圖

1. 電力線路與資通訊線路管道布署調整

目前電力線路與資通訊線路均布署於高架地板下之線槽，建議規劃將電力線路與資通訊線路隔離布署，或將輕鋼架天花板移除，於機櫃上方配置高架資通訊線路配線管路，以減低資通訊線路與電力線路之干擾。

2. 空調冰水管備援管路布署

目前空調冰水管皆以明管單路布署，考慮空調水管維修及備援需求，建議規劃備援管路，以便管路故障維修時，還能由備援管路支援空調系統之正常運作。

3. 空調系統備援電力布署

目前空調系統並未納入備援發電機之電力供應範圍，應規劃施工將空調系統電力接入備援發電機之供電，避免停電時機房仍因空調系統無法運轉而須停止運作。

4. 空調系統停水備援方案

目前空調系統配置專用戶外冷卻水塔，以及室內空調箱，若

停水時，冷卻水塔即無法運作。建議建置氣冷式空調設備，以因應停水時之機房空調備援需求。

5. 規劃所需空調能力

依據雲端系統規劃，大坪林機房至少需 22 部伺服器，預估散熱需求為 23.2kw~44kw。現況資訊主機空調能力為 71kw，日後增加設備需注意空調能力上限。

6. 全域負載平衡 GSLB 機制布署

配合三個區域資訊中心之網路架構及備援機制，建置 Global Server Load Blance 全域負載平衡設備，以達成服務之高可用性以及不中斷，以及三個區域中心之同時服務全國三個區域之規劃。

6.3.8.2. 竹山機房

依據中部備援中心建置案-資通訊影像系統需求說明書，以及服務建議書、施工計畫書之內容，提出以下基礎設施配置建議事項：

1. 機房對外之隔熱設施設置

竹山機房內側有面向西南方之對外窗，機房門外之走道有面向東北方對外窗，分別會於下午及上午受到日照之影響，需設置適當隔熱設施，以避免影響空調系統之效能。另機房位於建築物頂樓，其屋頂之隔熱工程應須能有效隔絕來自屋頂之日照熱源。

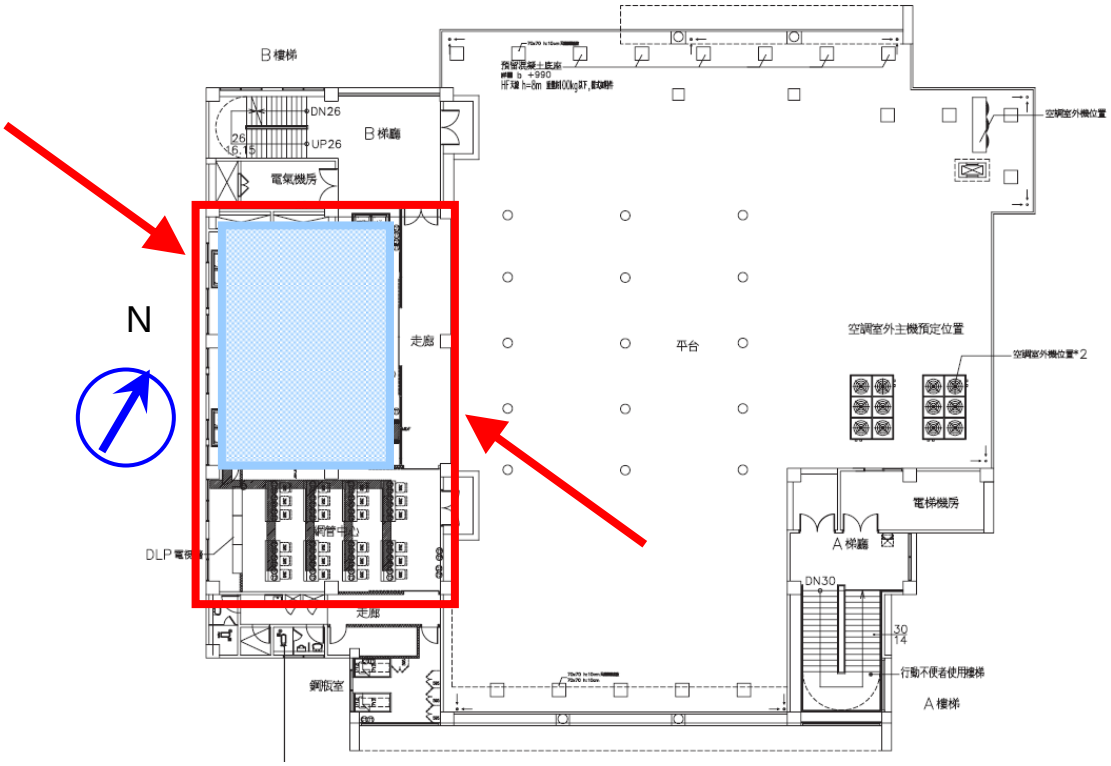

圖 501、中部備援中心三樓平面圖

2. 空間設計

機房出入口設計有二處，應考慮安全性、出入管制便利性、設備進出便利性，來設置機房營運時之出入口。

圖面上機房與控制室之間的出入口在電視牆後方，建議設置於較方便進出機房之位置，人員進出機房由控制室進行管制。

機房內不建議配置操作人員辦公區與儲藏區，設計上有配置通訊協調中心人員座位，建議另覓座位或是進行隔間，以維機房安全性，以及空調冷房效率。

3. 佈線設計

規劃書繪製有機房內高架地板線槽，高架地板下線槽之配置關係空調設計(下吹式空調箱、直吹式空調箱)，應搭配空調系統之設計規劃，進行線槽之布置。電力線路與資通訊線路，建議隔離佈設(地板線槽佈電力線，架空線槽佈網路通訊線)。

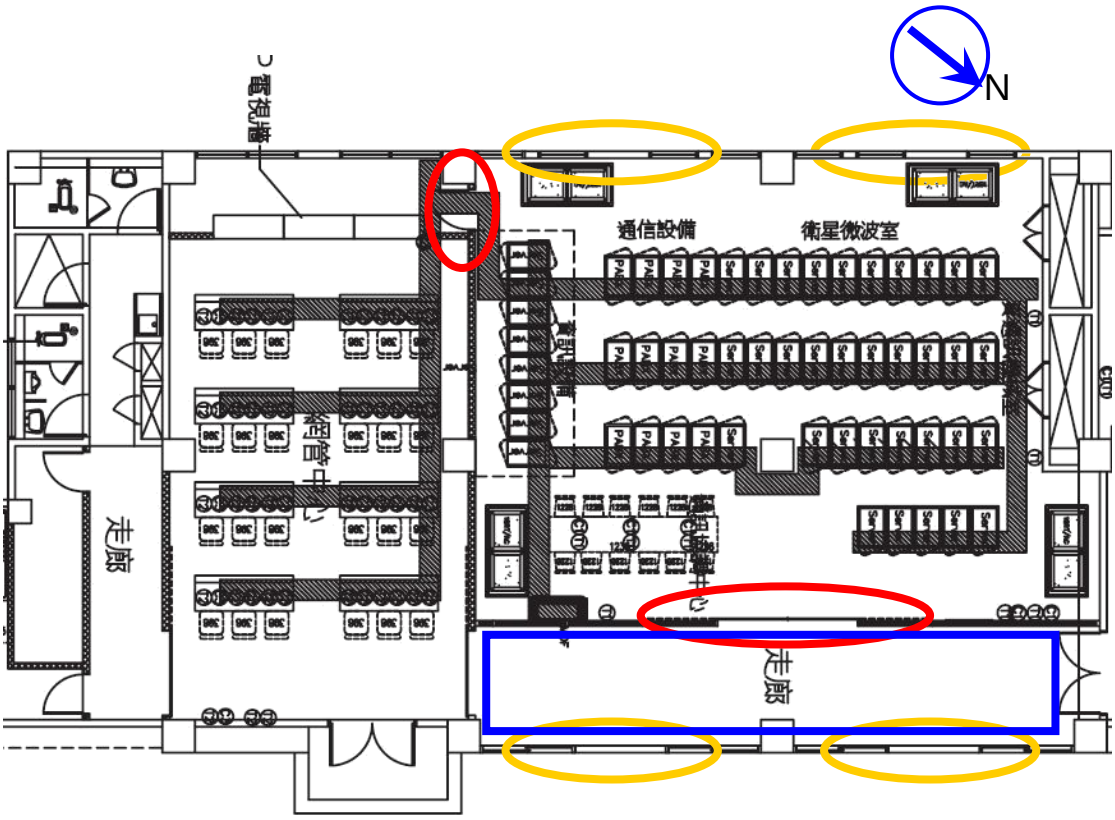

圖 502、竹山機房空間配置圖

4. 冷熱通道配置

目前規劃平面圖之配置為 53 座機箱，建議將機櫃、空調出風口、地板線槽佈線三者相互搭配，形成冷熱通道設置。

5. 規劃所需空調能力

依據雲端系統規劃，竹山機房至少需 18 部伺服器，預估散熱需求為 19.8kw~36kw，規劃空調能力為 200kw x 2。屆時尚需注意空調系統是否能支持其他如通信系統之建置設備散熱需求。

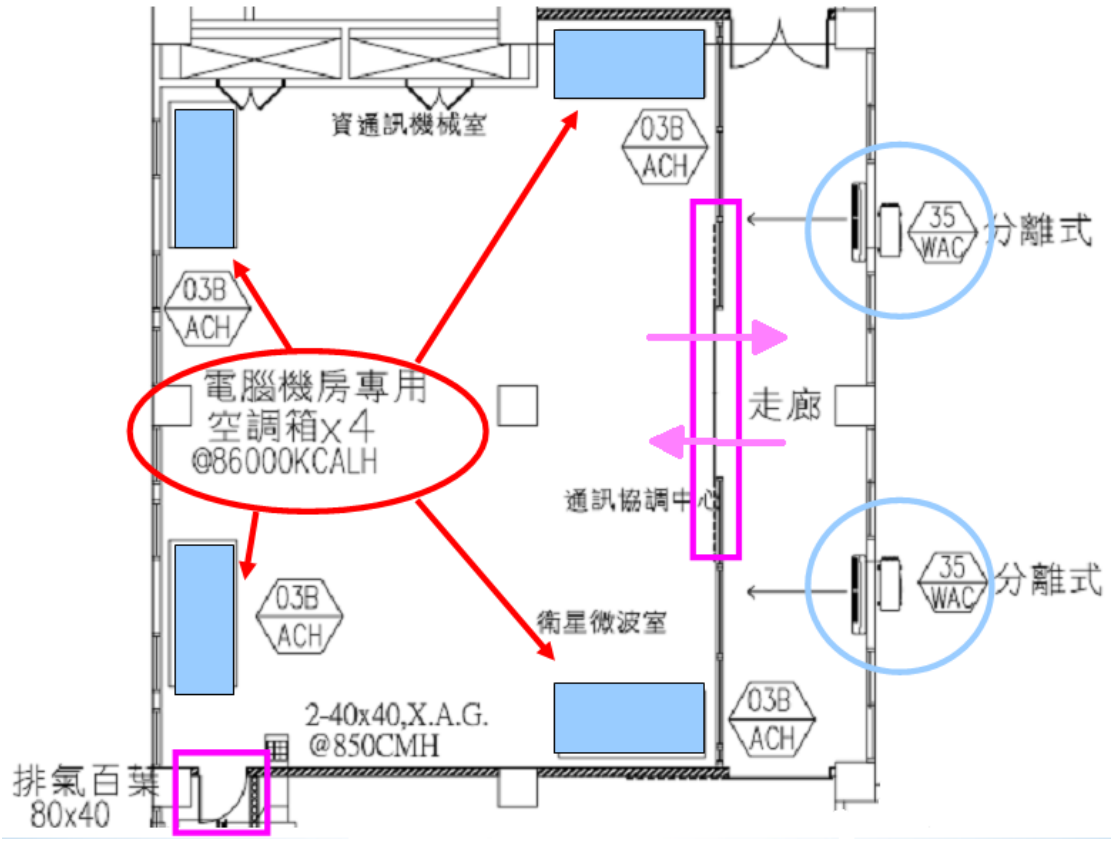

圖 503、竹山機房空調配置圖

5. 空調冷卻水管線佈設

此部分屬於機電部分，建議須注意管線備援線路之設計，以減少管線施工停機之時間。

6. 環控設施監控項目

環控設施列於資通訊服務施工計畫書內，監控機房之溫度、濕度、空調、消防、UPS、市電、發電機等狀態與設施。後續建置時，需確認監測點位置及監測數量是否足夠。

7. 電力設施

依據系統需求書第四章佈線工程及 UPS 之內容，UPS 共設置 160KVA UPS 4 台，系統正常運轉時可提供中部備援中心總容量 480KVA 之負載使用，UPS 採並聯複置(redundant)設置，系統架構採(3+1)方式設置。

需注意 UPS 之容量是否可以保證供應竹山機房之用電需求，

避免其他設施用電需求過大，影響機房於停電時之用電狀況。

8. 監視設備

應確認施工佈設位置圖是否符合監控無死角之需求。

6.3.8.3. 高雄機房

基於以下南部備援中心建置案規劃文件：南部備援中心合建共構新建工程-資通訊影像系統建置系統需求規格說明書(2011/03/25)，南部備援中心機房設備系統說明 (2011/04/18)，提出以下注意之事項：

1. 電氣規劃

資通訊機房相關用電容量之估算依據，應依據機房之進駐設備用電需求，並預留擴充容量。

資通訊機房應有獨立之電力迴路，避免受到其他區域用電之影響，且獨立用電迴路規劃，以及備援用電規劃，均需涵蓋空調冷卻系統。

2. UPS 不斷電系統

UPS 系統之規劃於 9F 蓄電池室設置三部 160KVA (2+1) ，以及確認規劃規格是否能足應需求？

3. 空調系統

整棟大樓使用水冷式冰水機之規格 200USRT 二部，及備援用氣冷式冰水機 100USRT 二部，資通訊設備及機房並無獨立之空調設備，應注意如何確保資通訊機房之空調需求，不受其他區域負載之影響。

空調機規劃為下吹式 N+1 備援配置，可考慮 2N+1 輪吹配置，且空調地板蜂巢板出風口應搭配機櫃成冷熱通道配置。

4. 規劃所需空調能力

依據雲端系統規劃，高雄機房至少需 16 部伺服器，預估散熱

需求為 17.6kw~32kw。屆時尚需注意機房之空調系統是否能支持建置設備之散熱需求。

5. 機房佈置

機房規劃二個出入口，建議設置單一出入口，以便出入口門禁及人員、設備動線規劃。

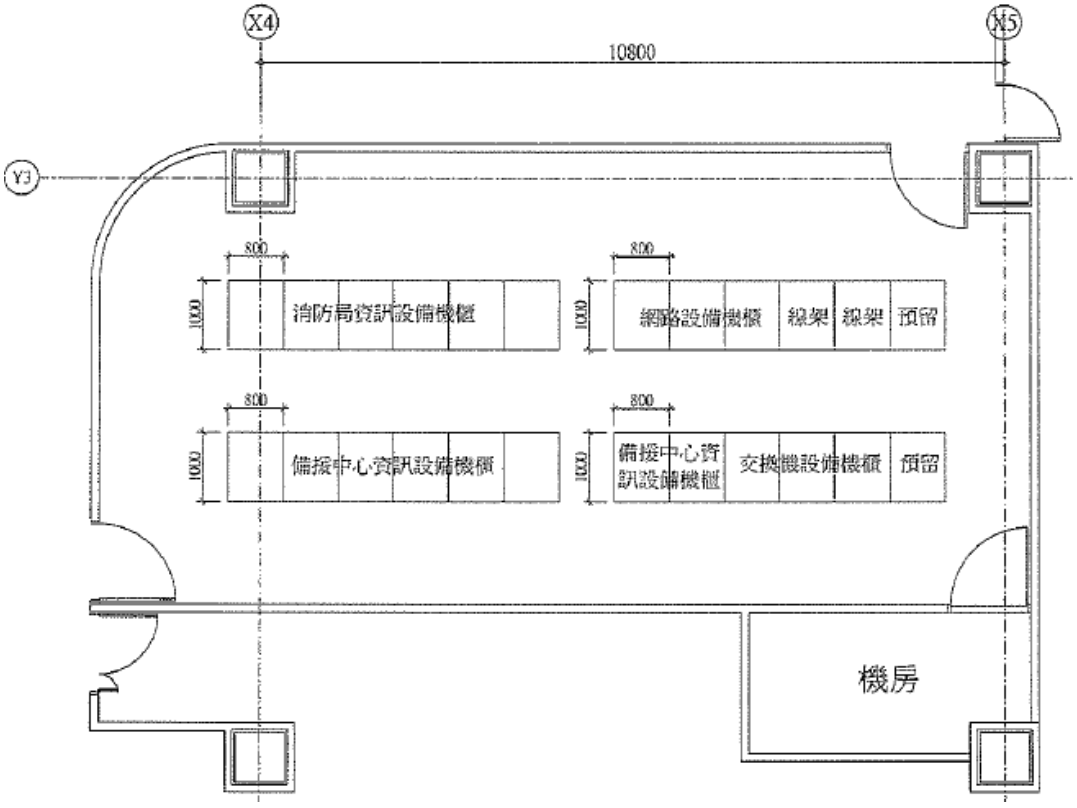

圖 504、高雄機房空間配置圖

6. 機房電力、資通訊布線

電力、資通訊建議隔離配置，採用高架配線盤布置資訊配線，以便利維修查線，且避免電力線之干擾。

高架地板下布置電力配線，且高架地板下布線需配合下吹式空調之出風口配置。

7. 環境監控

機房環控設施監控項目如：溫度、濕度、漏水、消防、空調、UPS、市電皆有規劃，需注意監測點之細部規劃位置及數量。

8. 雲端規劃案之配合

建置時須整合中部備援中心之全域負載平衡 GSLB 機制布署。