# 第肆章　研究分析

## 第一節　　訪談分析

藉由與技術人員所進行的訪談，資訊安全事故的掌控，主要可以分成四個構面，分別是組織、技術、程序以及人員。

組織的特質對於整個企業組織的環境影響很大，員工數、電腦數、分支數、產業別都是影響企業組織資訊安全的因子。員工數、電腦數以及分支數愈多的企業組織，其所建構的企業網路也會更爲複雜，因而增加控管的難度，導致遭遇資訊安全風險的可能性增大。不同的產業對於資訊系統的要求會有所不同，因此面臨資訊安全風險的可能性也大不相同。但是根據這些技術人員的經驗，企業組織的產業別對於資訊安全風險的影響並沒有顯著的差別，只要有網際網路，都會有發生中毒的可能性。根據技術人員以往的經驗，若改分成民營機構與公家機關，則會有顯著的差別。民營機構本身會比較謹慎地做規劃，而公家機關在這方面會比較馬虎。

技術在資訊安全架構中，提供主從式（Client-Server）架構的防毒安全，而在企業組織所使用的各項資訊安全系統產品的功能所得到的防護功能基本上都是大同小異的。就這方面而言，比較沒有什麼太大的問題。偶而可能會有產品問題的情況發生，這部分比較小，也比較容易解決。除非是因爲產品的功能故障導致無法偵測到病毒或是網路威脅，這部分的問題才會顯得比較嚴重。但這種情況發生的機率並不高。資訊安全在技術上有困難的原因是許多企業的各項應用程式通常是透過招標的方式，因此每個應用程式間的資料結構大不相同，使得在整合資訊安全技術及策略方面上，產生問題，不容易制訂一個統一的規格。因此在推動資訊安全防護政策時，無法快速的推動。

程序對於資訊安全是很重要的，一個組織若是沒有一套完整的資訊安全政策、放縱使用者任意不當使用電腦，如機器可以自由進出網際網路、收信並不受到約束等等，各種漏洞與弱點都會因此而產生，來源也會很複雜以至於無法掌

控，使得遭受到資訊安全風險的可能性無限提升。因此對於帳號密碼控管、軟體安裝政策、過濾惡意網站以及禁止資料夾分享等資訊安全政策，皆可降低資訊安全風險的可能性。不過資訊安全人員也必需考量終端使用者的需求，若是這個程式能夠提升終端使用者的生作生產力，資訊安全人員可以適度地放行，並且監控其使用狀況。企業組織資訊安全政策若採用統一集中式的管理，即使企業組織規模再大、分支數再多，亦可以有效地控管整個企業組織的資訊環境，將資訊安全風險的可能性降低。

人員是指專職資訊安全人員、終端電腦的使用者以及組織高層。在資訊安全人員的方面，雖然技術與程序可以提供許多有用的資訊給資訊安全人員，不過資訊安全人員必需透過這些大量的資訊，找出一個適當的應變之道。在所多企業組織中，資訊安全只是 MIS 人員眾多工作項目中的其中一項，因此不易掌控整個環境的資訊安全，甚至在發生資訊安全事故時，無法第一時間迅速處理，因而增加企業組織資訊安全的風險。除了靠培訓使得資訊安全人員擁有資訊安全這個領域的專業知識之外，經驗的累積對於資訊安全人員也是非常重要的。再多的訓練、再多的理論知識也無法取代長期累積下來的實戰經驗。一個經驗豐富的資訊安全人員，在遇到事件發生時，應該具備有能夠輕易地識別可疑的威脅的能力，並且能夠在短時間內快速地做出應變措施，盡量將企業組織所受到的損失降到最低。

終端使用者是直接使用終端電腦的使用者，因此終端使用者的使用習慣也是企業組織會不會因此受到網路威脅的主要原因之一。在很多的情況之下，人的行爲是無法強制限制的。有些部分當然可以直接透過資訊安全防護系統去控制與監管，不過有些部分是人的行爲的問題無法輕易地或有效地控制與監管。這些部分就必需透過資訊安全教育訓練來改善終端使用者的使用電腦的行爲與習慣。控制與監管嚴謹固然對企業組織的資訊安全有很大的幫忙，不過資訊安全人員也必需考量終端使用者的需求，若是這個程式能夠提升終端使用者的生作生產力，資訊安全人員可以適度地放行，並且監控其使用狀況。資訊安全人員必需在嚴謹控管與滿足終端使用者需求間，找到一個平衡點，才能爲企業組織帶來雙贏的局面。

組織高層對資訊安全重視的程度對於整個資訊安全影響很大。在部分組織

中，資訊安全人員的權力並不高，因而所做的資訊安全政策不被終端使用者所接受與配合，使得該組織的資訊安全政策只是白紙一堆，無法發揮實質的功用。部分組織因高層高度支持，並且由高層發公文與電子郵件要求終端使用者配合資訊安全策略的推動，使得網路威脅有明顯的減少。因此主要還是得看組織高層是否有意識到資訊安全的重要性與資訊安全策略執行的必要性，才能使得資訊安全政策推動地更快速、更有效率。

## 第二節　　調查樣本分析結果

### （一） 樣本基本資料分析處理

藉由問卷調查，以國內某知名防毒軟體公司的客戶爲樣本，發出 1910 份郵寄問卷與網路問卷邀請 E-mail 信，共回收 102 份有效問卷（網路問卷 61 份，郵寄問卷 41 份），回收率 5.3%。回收問卷中如果碰到有未作答的題目，會在分析該題時將其本份問卷剔除。

表8 客戶所屬產業分佈表

| 產業別 | 頻次 | 比例(%) |
|---|---|---|
| 金融業 | 10 | 9.8 |
| 製造業 | 23 | 22.5 |
| 電子資訊&通訊傳媒 | 11 | 10.8 |
| 政府機關 | 24 | 23.5 |
| 教育學術單位 | 16 | 15.7 |
| 貿易、百貨與零售商 | 9 | 8.8 |
| 其他 | 9 | 8.8 |

[資料來源：本研究整理]

以行業別來比較如表 8，根據之前與技術人員的訪談，產業別對於資訊安全的影響並沒有顯著的差異，若需要分群以做比較的話，則可以考慮以「公家機關」與「民營機構」分群來作比較。民營機構本身比較謹慎做規劃，所以在資訊安全方面並不敢馬虎；而相對於民營機構人員，擁有「鐵飯碗」的公家機關人員比較不會花心思在這方面上，因爲他們會覺得這不是他們的工作，或者覺得這部分是多餘的，得過且過，而不想去做。另外，在教育學術單位類別可分爲公立學校與

私立學校，不過體制上是大同小異的，所以亦可在分析比較上將私立學校一同與公立學校歸類進公家機關。

表9 機構員工數表

| | 頻次 | 比例(%) |
|---|---|---|
| 1-500 人 | 63 | 61.8 |
| 501-1000 人 | 14 | 13.7 |
| 1001-3000 人 | 16 | 15.7 |
| 3001 人以上 | 9 | 8.8 |

[資料來源：本研究整理]

表10 機構電腦數表

| | 頻次 | 比例(%) |
|---|---|---|
| 1-500 台 | 63 | 61.8 |
| 501-1000 台 | 14 | 13.7 |
| 1001-3000 台 | 16 | 15.7 |
| 3001 台以上 | 9 | 8.8 |

[資料來源：本研究整理]

在這次的問卷調查中，機構員工數的分佈表（如表 9），擁有 1-500 位員工的機構佔超過一半的比例（61.8%），而超過 3000 位員工的大機構只佔少數（8.8%）。相較於文獻中[20]，1-500 位員工的機構佔 34%，而超過 3000 位員工的大機構則佔約一半比例。因此本次問卷以小型機構爲主要樣本群。而各企業組織所擁有的電腦數（如表 10）的多寡與該企業組織所擁有的員工數有正相關，相關值爲 0.854，顯著水準頗高，其比例與企業組織中的員工數表相同。

表11 組織分散程度表

| | 頻次 | 比例(%) |
|---|---|---|
| 0-5 個 | 56 | 54.9 |
| 6-10 個 | 19 | 18.6 |
| 11 個以上 | 27 | 26.5 |

[資料來源：本研究整理]

如表 11 所示，約有稍超過一半（54.9%）的機構，其分散程度都在 5 個分支機構以下。所以分支程度高與低者約各佔半數。

表12 營利與非營利機構分佈表

| | 頻次 | 比例(%) |
|---|---|---|
| 非營利機構 | 36 | 39.1 |
| 營利機構 | 56 | 60.9 |

[資料來源：本研究整理]

如表 12 所示，營利機構佔整個樣本的 60.9%

表13 防毒專職員工數表

| | 頻次 | 比例(%) |
|---|---|---|
| 沒有 | 17 | 16.7 |
| 1-5 位 | 81 | 79.4 |
| 6 位以上 | 3 | 2.9 |

[資料來源：本研究整理]

在表 13 中，79.4%的機構皆有 1-5 位的防毒專職員工，而 16.7%的機構並沒有安排防毒專職員工。根據之前的訪談，有些機構的 MIS 人員本身負責許多的業務，防毒工作只是他們工作項目的其中一項；回收樣本資料與訪談結果相符。

（二） 網路安全的基本資料

表14 機構業務仰賴網路程度

| | 頻次 | 比例(%) |
|---|---|---|
| 一點點 | 6 | 5.9 |
| 有點 | 19 | 16.7 |
| 非常多 | 79 | 77.5 |

[資料來源：本研究整理]

隨著網際網路的快速發展，企業所倚賴網路的業務也愈很愈多了。從表 14 可以得知企業的業務仰賴網際網路的程度是非常高的（77.5%）。從上下游的供應鏈管理到電子商務等，都是需要使用到網際網路的。

表15 內部使用者使用 Internet

| | 頻次 | 比例(%) |
|---|---|---|
| 可以 | 99 | 97.1 |
| 不可以 | 3 | 2.9 |

[資料來源：本研究整理]

表16 外部使用者使用網際網路

| | 頻次 | 比例(%) |
|---|---|---|
| 可以 | 68 | 66.7 |
| 不可以 | 34 | 33.3 |

[資料來源：本研究整理]

表 15 與表 16 分別爲各機構是否允許內部使用用（如員工）與外部使用者（如外來的廠商）在機構中使用網際網路的比例。大部分的機構允許員工使用網際網路，畢竟不少業務除了使用區域網路之外，還是需要使用網際網路的。而相較於內部使用者，允許外來廠商使用網際網路的比例明顯減少，以降低許多不必要的風險。

表17 外部電腦進入企業網路

| | 頻次 | 比例(%) |
|---|---|---|
| 可以 | 25 | 24.8 |
| 不可以 | 76 | 75.2 |

[資料來源：本研究整理]

表18 與外部做資訊交流

| | 頻次 | 比例(%) |
|---|---|---|
| 允許 | 61 | 60.4 |
| 不允許 | 40 | 39.6 |

[資料來源：本研究整理]

表 17 與表 18 分別爲機構是否允許外來的電腦連入機構內部的企業網與是否允許與外界的機構作資訊的交流。大部分的機構不允許外部電腦連進機構內部的企業網路使用資源，而少部分機構因工作需要，允許公司員工或合作廠商使用 VPN 等連線方式連進公司內部。相較於外部電腦進入機構內企業網路，各機構比較會允許與外界機構做資訊的交流。

（三） 弱點與防毒管理工具分析

表19 使用弱點管理工具

| | 頻次 | 比例(%) |
|---|---|---|
| 沒有使用 | 33 | 32.4 |
| 弱點掃描 | 38 | 37.3 |
| 入侵偵測系統 | 46 | 45.1 |
| 入侵保護系統 | 23 | 22.5 |
| 修補程式自動部署工具 | 41 | 40.2 |
| 其他 | 0 | 0 |

[資料來源：本研究整理]

表20 使用防毒管理工具

| | 頻次 | 比例(%) |
|---|---|---|
| 沒有使用 | 12 | 11.9 |
| FTP 閘道防毒 | 23 | 22.8 |
| HTTP 閘道防毒 | 39 | 38.6 |
| Email 閘道防毒 | 80 | 79.2 |
| 其他 | 8 | 7.9 |

[資料來源：本研究整理]

技術在資訊安全中，是個很重要的環節之一。在調查中，沒有使用弱點管理工具與防毒管理工具的比例分別爲 32.4%與 11.9%（如表 19 與表 20）。Email 伺服器是掌管電子郵件進出的中心，所以在 Email 閘道上設定爲第一個掃描病毒與廣告信的檢查點，理論上是可以降低病毒爆發的情況，因此 79.2%的機構皆有使用 Email 閘道防毒管理工具。

表21 防毒軟體安裝率

| | 頻次 | 比例(%) |
|---|---|---|
| 沒有追蹤 | 6 | 5.9 |
| 95%-100% | 79 | 77.5 |
| 90%-95% | 15 | 14.7 |
| 小於 90% | 2 | 2.0 |

[資料來源：本研究整理]

防毒軟體是電腦上防毒的最後一道防線。根據接受訪談的技術人員過去的經

驗，防毒軟體安裝率高的機構，即使中了病毒，也可以很快就被清除掉。雖然只是個治根的辦法，無法做到治本，但是至少可以降件病毒爆發的可能性。表 21 中，90%以上的機構的防毒軟體安裝率都在 90%以上。

表22 Desktop & Client 使用比例表

| | 頻次 | 比例(%) |
|---|---|---|
| 沒有使用 | 0 | 0 |
| OfficeScan | 48 | 100 |
| Anti-Spyware | 2 | 4.2 |
| PC-Cillin Internet Security | 6 | 12.5 |
| Home Network Security | 1 | 2.1 |

[資料來源：本研究整理]

表23 Outbreak Management 使用比例表

| | 頻次 | 比例(%) |
|---|---|---|
| 沒有使用 | 31 | 70.5 |
| Control Management | 13 | 29.5 |

[資料來源：本研究整理]

表24 Network Protection 使用比例表

| | 頻次 | 比例(%) |
|---|---|---|
| 沒有使用 | 41 | 91.1 |
| Network Virus Wall | 4 | 8.9 |

[資料來源：本研究整理]

表25 Email & Groupware 使用比例表

| | 頻次 | 比例(%) |
|---|---|---|
| 沒有使用 | 18 | 38.3 |
| ScanMail for Microsoft Exchange | 17 | 36.2 |
| ScanMail eManager | 6 | 12.8 |
| ScanMail for Lotus Domino | 8 | 17.0 |
| IM Security for Microsoft Office Live Communications Server | 0 | 0 |

[資料來源：本研究整理]

表26 Internet Gateway 使用比例表

| | 頻次 | 比例(%) |
|---|---|---|
| 沒有使用 | 27 | 58.7 |
| Spam Prevention Solution | 0 | 0 |
| InterScan Messaging Security Suite | 4 | 8.7 |
| InterScan Web Security Suite | 1 | 2.2 |
| URL Filtering | 0 | 0 |
| Java Applet | 0 | 0 |
| InterScan VirusWall | 11 | 23.9 |
| InterScan eManager | 0 | 0 |
| InterScan AppletTrap | 0 | 0 |
| InterScan WebProtect for ISA | 2 | 4.3 |

[資料來源：本研究整理]

表27 File Server & Storage 使用比例表

| | 頻次 | 比例(%) |
|---|---|---|
| 沒有使用 | 17 | 36.2 |
| ServerProtect for Microsoft Windows/Novell NetWare | 28 | 59.6 |
| ServerProtect for Network Appliance filers | 0 | 0 |
| ServerProtect for EMC Celerra | 0 | 0 |
| ServerProtect for Linux | 8 | 17.0 |
| PortalProtect for SharePoint | 0 | 0 |

[資料來源：本研究整理]

表28 Mobile Security 使用比例表

| | 頻次 | 比例(%) |
|---|---|---|
| 沒有使用 | 44 | 95.7 |
| TM Mobile Security | 2 | 4.3 |

[資料來源：本研究整理]

表 22 到表 28 爲樣本使用國內某知名防毒軟體公司的產品之頻次與比例。

表29 使用其他品牌的防毒軟體統計表

| | 頻次 | 比例(%) |
|---|---|---|
| 有 | 43 | 42.6 |
| 沒有 | 58 | 57.4 |

[資料來源：本研究整理]

表30 該防毒軟體安裝在網路上的哪個位置統計表

| | 頻次 | 比例(%) |
|---|---|---|
| Internet Gateway | 13 | 31.0 |
| Email/Groupware Server | 18 | 41.9 |
| LAN Server | 23 | 53.5 |
| Client PCs | 32 | 74.4 |

[資料來源：本研究整理]

有些機構因爲價格、功能或偏愛等原因，亦會同時使用其他廠商的防毒軟體。從表 29 可得知，有 42.6%的機構仍然有使用其他廠商的防毒軟體，並將之安裝在網路上的某些位置上。表 30 中顯示，安裝最多的，還是位於客戶端的電腦上。

（四） 回收樣本安全風險分群

表31 過去三年間，病毒爆發事件(平均一年幾件)

| 樣本數 | 最小值 | 最大值 | 平均數 | 標準差 |
|---|---|---|---|---|
| 97 | 0 | 10 | 2.16 | 1.944 |

[資料來源：本研究整理]

表32 過去三年間，病毒爆發事，電腦一日 down 的比例

| 樣本數 | 最小值 | 最大值 | 平均數 | 標準差 |
|---|---|---|---|---|
| 98 | 0 | 80 | 11.3266 | 17.15990 |

[資料來源：本研究整理]

表33 最近三個月中，所偵測到的病毒數

| 樣本數 | 最小值 | 最大值 | 平均數 | 標準差 |
|---|---|---|---|---|
| 71 | 0 | 58078 | 5564.37 | 12845.994 |

[資料來源：本研究整理]

表34 最近三個月中，所偵測到的可能感染事件數

| 樣本數 | 最小值 | 最大值 | 平均數 | 標準差 |
|---|---|---|---|---|
| 61 | 0 | 57922 | 1659.72 | 7545.752 |

[資料來源：本研究整理]

本調查的應變數爲「過去三年間平均一年的病毒爆發事件」、「過去三年間病毒爆發時，平均一日電腦 down 的比例」、「最近三個月，平均一個月所偵測到的病毒數」與「最近三個月，平均一個月所偵測到的可能感染事件數」。表 31、32、33 與 34 分別列出其最大值、最小值、平均數與標準標。

在表 31 中，原本的平均值與標準差分別爲 4.44 與 18.562，有二間機構其病毒爆發事件爲 50 件與 180 件，因而拉高了平均。根據之前接受訪談的技術人員過去的經驗，平均一年 4-5 件已算是滿糟糕的情況了，而這兩間機構更遠超過於這個數字，因此在本調查的分析中，將這兩筆資料當作怪異值〈outlier〉，後續分析會將此 2 份樣本抽掉。抽掉這二筆資料後，其平均數與標準差分別爲 2.16 與 1.944。

表35 以病毒爆發事件數分群表

| 群組 | 病毒爆發事件數 | 樣本數 |
|---|---|---|
| 1 | 0-1 件 | 42 |
| 2 | 2 件 | 26 |
| 3 | 3 件 | 14 |
| 4 | 4 件以上 | 15 |

[資料來源：本研究整理]

表36 以病毒感染嚴重程度分群表

| 群組 | 病毒感染嚴重程度 | 樣本數 |
|---|---|---|
| 1 | 1%以下 | 26 |
| 2 | 2-3% | 20 |
| 3 | 4-10% | 30 |
| 4 | 10%以上 | 22 |

[資料來源：本研究整理]

根據病毒爆發的頻次與病毒感染嚴重程度的分配，分別將整個樣本分成四個群組使每群樣本數不要差別太大，利後續統計分析，分群結果如表 35 及表 36 所

示。

表37 以偵測到病毒數分群表

| 群組 | 偵測到病毒數 | 樣本數 |
|---|---|---|
| 1 | 0-15 隻 | 18 |
| 2 | 15-365 隻 | 18 |
| 3 | 365-1500 隻 | 18 |
| 4 | 1500 隻以上 | 17 |

[資料來源：本研究整理]

表38 以偵測到可能感染事件數分群表

| 群組 | 可能感染事件數 | 樣本數 |
|---|---|---|
| 1 | 0-4 件 | 15 |
| 2 | 4-24 件 | 16 |
| 3 | 24-350 件 | 15 |
| 4 | 350 件以上 | 15 |

[資料來源：本研究整理]

考量若一個機構規模愈大，則其相對的電腦數也會增加，所以偵測到病毒或是可能的感染事件數也應該會增多。因此在評量一個企業組織安全風險的強弱，宜以所偵測到的病毒數與可能感染事件數需除以電腦數，如此安全風評量較不會受樣本間的電腦數所影響。所以本統計分析中，將”1-500 台”設爲 1 單位，以下的偵測病毒數與偵測可能感染事件將除上單位台數。“1-500 台”單位爲 1；”501-1000 台”單位爲 3；”1001-3000 台”單位爲 5；”3001 台以上”單位爲 8。表 37 與表 38 爲將原先所偵測到的病毒數與可能感染事件數除以所對應的單位數後，依頻次分爲四個群組以做統計分析。

（五） 產業別與病毒感染交叉分析

表39 公家機關與民營機構病毒爆發頻次比較表

| | 樣本數 | 最小值 | 最大值 | 平均數 | 標準差 |
|---|---|---|---|---|---|
| 公家機關 | 33 | 0 | 10 | 1.89 | 1.919 |
| 民營機構 | 64 | 0 | 10 | 2.30 | 1.957 |

[資料來源：本研究整理]

表40 公家機關與民營機構病毒感染嚴重程度(%)比較表

| | 樣本數 | 最小值 | 最大值 | 平均數 | 標準差 |
|---|---|---|---|---|---|
| 公家機關 | 32 | 0 | 80 | 12.04 | 19.79 |
| 民營機構 | 64 | 0 | 80 | 11.24 | 16.05 |

[資料來源：本研究整理]

如果將政府機關與教育學術單位設定爲「公家機關」，其他產業設定爲「民營機構」，比較兩類之病毒爆發的頻次與病毒感染嚴重程度，結果如表 39 與表 40 所示。

## 第三節　影響資訊安全的關鍵因素分析

本研究共採兩種方法試圖找出影響資訊安全之較關鍵因素。第一種方法是以「病毒爆發數量」、「病毒爆發影響嚴重性」、「偵測病毒數」、「偵測到可能感染事件數」爲應變數，以「公司概況」及「防毒能力評估」各變項爲自變數進行單因子與多因子變異數分析。第二種方法是在回收樣本中以「病毒爆發數量」、「病毒爆發影響嚴重性」、「偵測病毒數」、「偵測到可能感染事件數」分群之四群爲自變數，以公司概況及防毒能力評估各變項爲應變數進行卡方分配檢定，結果詳述如下：

### （一） 單因子變異數分析

以企業特質與企業防毒能力評估個個問題項爲自變數〈Independent Variable〉〈類別資料〉，以平均病毒爆發事件 、感染嚴重程度、平均被偵測到之病毒數、及平均偵測感染數等四項爲應變數〈Dependent Variable〉〈數字資料〉，進行單因子變異數分析，比較各個問題中不同類之上述四項應變數是否有顯著差異〈分別以 $p<0.1$ 及 $p<0.05$ 爲標準〉如表 41。

表41 單因子變異數分析

| | | 病毒爆發事件數 F(p) | 病毒爆發影響嚴重程度 F(p) | 偵測病毒數 F(p) | 偵測到可能感染事件值 F(p) |
|---|---|---|---|---|---|
| 組織 | 員工數 | | 2.261(0.053) | 4.962(0.004) | 5.934(0.001) |
| | 電腦數 | | | 6.663(0.001) | 2.931(0.041) |
| 資訊安全政策 | 內部使用者使用 Internet | | 3.911(0.051) | | |
| | 隨時中斷辦公系統與關鍵系統間連線 | | | | 3.193(0.079) |
| | 統一資訊安全政策 | 4.518(0.036) | | | |
| | 統一安裝防毒軟體 | | | | 2.743(0.073) |
| | 監控防毒軟體安裝率 | | 4.859(0.030) | | |
| | 監控 Server 離線率 | 2.985 (0.087) | | | |
| | 監控防毒硬體裝置病毒碼過期比例 | 3.097(0.082) | | | |
| | 監控 AP Server 修補檔未更新比例 | | 4.999(0.028) | | |
| | Windows 客戶端修補檔未更新比例 | 2.454(0.068) | | | 2.982(0.039) |

表 41 單因子變異數分析(續)

| | | 病毒爆發事件數 F(p) | 病毒爆發影響嚴重程度 F(p) | 偵測病毒數 F(p) | 偵測到可能感染事件值 F(p) |
|---|---|---|---|---|---|
| 資訊安全政策 | Windows 伺服器端修補檔未更新比例 | 2.865(0.041) | | 5.662(0.002) | |
| | 後續動作改進修補檔部署 | | 5.037(0.027) | | |
| | 更新防毒元件 | | 4.801(0.031) | | |
| | 後續動作改進病毒碼更新 | | 13.999(0.000) | | |
| | 新增刪除帳號核對確認程序 | 6.992(0.010) | | | |
| | 密碼控管政策 | | | 4.915(0.030) | |
| | 軟體安裝政策 | 3.583(0.061) | | | |
| | 惡意網站過濾 | | 4.178(0.044) | | 3.347(0.072) |
| | 禁止分享資料夾 | | 3.614(0.060) | | 5.842(0.019) |
| 人員與訓練 | 舉辦資訊安全教育訓練 | | 7.494(0.007) | | |
| | 客制化教育訓練 | | | | 5.437(0.023) |
| | 社會工程教育訓練主題講座 | | 3.153(0.079) | | |
| | 發佈最新型態威脅警報 | | | 3.968(0.050) | |

[資料來源：本研究整理]

簡單敘述結果如下：

- 組織的基本資料顯示員工人數500人以下或500人以上病毒爆發影響的嚴重性差異顯著，病毒爆發時平均電腦無法提供每日例行運作分別爲8%及20%，而對偵測病毒數及偵測到可能感染事件值兩指標而言，雖然員工人數500至1000人這一群較1-500人這群可能員工人數平均只多一倍，可是偵測值卻差10倍之多，可見當企業規模大於500人時，病毒爆發事件的影響會比較嚴重。
  - **i.** 企業組織之員工數小於500人，其病毒爆發嚴重程度平均值爲8.0585%、標準差爲13.90579；企業組織之員工數介於501至1000人，其病毒爆發嚴重程度平均值爲19.7143%、標準差爲26.63262；企業組織之員工數介於1001至3000人，其病毒爆發嚴重程度平均值爲17.3125%、標準差爲18.01747；企業組織之員工數超過3000人，其病毒爆發嚴重程度平均值爲9.1875%、標準差爲10.87572。
  - **ii.** 企業組織員工數小於500人，其所偵測病毒數平均值爲1677.91隻、標準差爲3856.607；企業組織員工數介於501至1000人，其所偵測病毒數平均值爲12076.36隻、標準差爲20839.778；企業組織員工數介於1001至3000人，其所偵測病毒數平均值爲9068.00、標準差爲15095.605；企業組織員工數超過3000人，其所偵測病毒數平均值爲19896.50隻、標準差爲25574.630。
  - **iii.** 企業組織員工數小於500人，其所偵測到可能感染事件數平均值爲289.19件、標準差爲799.744；企業組織員工數介於501至1000人，其所偵測到可能感染事件數平均值爲2238.13件、標準差爲3577.104；企業組織員工數介於1001至3000人，其所偵測到可能感染事件數平均值爲980.33件、標準差爲2252.682；企業組織員工數超過3000人，其所偵測到可能感染事件數平均值爲15218.50件、標準差爲28488.655。
- 企業組織擁有之電腦台數顯示之結果與企業組織擁有之員工數類似，偵測病毒數及偵測到可能感染事件值兩指標而言，雖然電腦台數500至1000這一群較1-500這群可能台數平均只多一倍，可是偵測值卻差10倍之多。
  - **i.** 企業組織電腦數小於500台，其所偵測病毒數平均值爲1600.36隻、標準差爲3741.316；企業組織電腦數介於501至1000台，其所偵測病毒數平均值爲10092.08隻、標準差爲17330.627；企業組織電腦數介於1001至3000台，其所偵測病毒數平均值爲18470.00隻、標準差爲23407.016；企業組織電腦數超過3000台，其所偵測病毒數平均值爲7024.00隻、標準差爲4276.582。
  - **ii.** 企業組織電腦數小於500台，其所偵測到可能感染事件數平均值爲

289.50、標準差爲 774.770 件；企業組織電腦數介於 501 至 1000 台，其所偵測到可能感染事件數平均值爲 1904.36 件、標準差爲 3108.169；企業組織電腦數介於 1001 至 3000 台，其所偵測到可能感染事件數平均值爲 8527.00 件、標準差爲 20139.339；企業組織電腦數超過 3000 台，其所偵測到可能感染事件數平均值爲 249.50 件、標準差爲 348.604。

- 網路區隔方面，開放程度因爲不允許內部使用者使用 Internet 的樣本數太小〈只有 3 樣本〉，故本題結果可信度存疑，不予採用。但不能區隔辦公系統與關鍵任務系統間並隨時中斷兩者連線的組織有比較高的偵測到可能感染事件值。
- 有集中管理的資訊安全政策其組織病毒爆發事件只有沒有集中管理的資訊安全政策組織的五分之一。採用集中管理的資訊安全政策之企業組織，其病毒爆發事件數平均值爲 2.73 件、標準差爲 5.627；沒有採集中管理的資訊安全政策之企業組織，其病毒爆發事件數平均值爲 13.31 件、標準差爲 44.471。
- 有監控資訊安全相關資訊〈如監控防毒軟體安裝率、監控伺服器離線率、監控防毒硬體裝置病毒碼過期比例或監控 AP 伺服器修補檔未更新比例〉的組織其病毒爆發事件數或病毒爆發影響嚴重性都較未進行監控資訊安全相關資訊的組織低。
  i. 有進行監控防毒軟體安裝率的企業組織，其病毒爆發影響嚴重程度平均值爲 10.3697%、標準差爲 15.58977；沒有進行監控防毒軟體安裝率的企業組織，其病毒爆發影響嚴重程度平均值爲 26%、標準差爲 31.84337。
  ii. 有進行監控伺服器離線率的企業組織，其病毒爆發事件數平均值爲 2.73 件、標準差爲 5.768；沒有進行監控伺服器離線率的企業組織，其病毒爆發事件數平均值爲 10.41 件、標準差爲 37.939。
  iii. 有進行監控防毒硬體裝置病毒碼過期比例的企業組織，其病毒爆發事件數平均值爲 2.86 件、標準差爲 5.714；沒有進行監控防毒硬體裝置病毒碼過期比例的企業組織，其病毒爆發事件數平均值爲 11.11 件、標準差爲 40.920。
  iv. 有進行監控 AP 伺服器修補檔未更新比例的企業組織，其病毒爆發影響嚴重程度平均值爲 9.5865%、標準差爲 13.21467；沒有進行監控 AP 伺服器修補檔未更新比例的企業組織，其病毒爆發影響嚴重程度平均值爲 19.6176%、標準差爲 28.69970。
- 修補檔如果未及時更新的比例較高會造成組織其病毒爆發事件數顯著的高
  i. Windows 客戶端修補檔未更新比例介於 0%至 10%的企業組織，其病毒爆發事件數平均值爲 2.26 件、標準差爲 2.176；Windows 客戶

端修補檔未更新比例介於 11%至 20%的企業組織，其病毒爆發事件數平均值爲 4.19 件、標準差爲 10.595；Windows 客戶端修補檔未更新比例大於 20%的企業組織，其病毒爆發事件數平均值爲 18.27 件、標準差爲 53.705。

ii. Windows 伺服器端修補檔未更新比例介於 0%至 5%的企業組織，其病毒爆發事件數平均值爲 2.63 件、標準差爲 6.104；Windows 伺服器端修補檔未更新比例介於 6%至 10%的企業組織，其病毒爆發事件數平均值爲 20.30 件、標準差爲 56.135；Windows 伺服器端修補檔未更新比例超過 10%的企業組織，其病毒爆發事件數平均值爲 3.40 件、標準差爲 3.715。

- 如果修補檔更新比例過低會有後續修補動作的組織其病毒爆發影響嚴重程度較低。有做後續修補動作的企業組織，其病毒爆發影響嚴重程度平均值爲 10.4444%、標準差爲 14.46304；沒有做後續修補動作的企業組織，其病毒爆發影響嚴重程度平均值爲 19.6471%、標準差爲 25.73650。
- 會部署防毒元件更新及覺得更新不理想時會有後續補救措施的組織其病毒爆發影響嚴重性較低。會部署防毒元件更新的企業組織，其病毒爆發影響嚴重程度平均值爲 10. 3751%、標準差爲 15.58638；沒有部署防毒元件更新的企業組織，其病毒爆發影響嚴重程度平均值爲 25.9167%、標準差爲 31.92243。
- 會做後續動作來改進病毒碼更新的企業組織，其病毒爆發影響嚴重程度比不會做後續動作的企業組織來得低。有做後續動作來改進病毒碼更新的企業組織，其病毒爆發影響嚴重程度平均值爲 9.6375%、標準差爲 13.81559；沒有做後續動作來改進病毒碼更新的企業組織，其病毒爆發影響嚴重程度平均值爲 33.2857%、標準差爲 35.93844。
- 有一些有效的資訊安全管理政策，如新增刪除帳號核對確認程序、密碼控管政策、軟體安裝政策、惡意網站過濾、禁止分享資料夾均對安全風險結果有正面的影響。

i. 有做新增刪除帳號核對確認程序的企業組織，其病毒爆發事件數平均值爲 2.66 件、標準差爲 5.502；沒有做新增刪除帳號核對確認程序的企業組織，其病毒爆發事件數平均值爲 17.33 件、標準差爲 51.249。

ii. 有做密碼控管政策的企業組織，其所偵測病毒數平均值爲 3432.78 隻、標準差爲 7859.566；沒有做密碼控管政策的企業組織，其所偵測病毒數平均值爲 10639.57 隻、標準差爲 19693.156。

iii. 有做軟體安裝政策的企業組織，其病毒爆發事件數平均值爲 2.80 件、標準差爲 5.686；沒有做軟體安裝政策的企業組織，其病毒爆發事件數平均值爲 11.83 件、標準差爲 41.991。

iv. 有對惡意網站進行過濾的企業組織，其病毒爆發影響嚴重程度平均

值爲 7.0385%、標準差爲 10.59319；沒有對惡意網站進行過濾的企業組織，其病毒爆發影響嚴重程度平均值爲 14.1612%、標準差爲 19.96006。

v. 有進行禁止分享資料夾的企業組織，其病毒爆發影響嚴重程度平均值爲 2.1818%、標準差爲 2.17360；沒有進行禁止分享資料夾的企業組織，其病毒爆發影響嚴重程度平均值爲 12.4829%、標準差爲 17.86875。

- 教育訓練對病毒爆發影響嚴重程度有正面的影響。有辦教育訓練的企業組織，其病毒爆發影響嚴重程度平均值爲 9.3736%、標準差爲 14.81625；沒有辦教育訓練的企業組織，其病毒爆發影響嚴重程度平均值爲 22.1333%、標準差爲 24.63118。

（二） 雙因子變異數分析

進一步以單因子變異數分析之後得到呈現顯著之問題項目，兩兩之間進行雙因子變異數分析，結果顯示 F 值及 P 值增強，代表如果組織同時滿足兩項關鍵影響因素，則對應變數之影響更大。

表42 二因子變異數分析

表 42-1 病毒爆發事件數 F(p)

表 42-1.1 公司概況與防毒能力二因子變異數分析

| 公司概況 / 防毒能力 | 統一資訊安全政策 |
|---|---|
| Windows 客戶端修補檔未更新比例 | 5.363(0.000) |
| Windows 伺服器端修補檔未更新比例 | 13.552(0.000) |
| 新增刪除帳號核對確認程序 | 9.271(0.000) |
| 軟體安裝政策 | 4.308(0.007) |

[資料來源：本研究整理]

- Windows 客戶端修補檔未更新比例與企業組織資訊安全政策是否有集中管理對於病毒爆發事件的影響。Windows 客戶端修補檔未更新比例高於 20%與企業組織資訊安全政策沒有集中管理時，會使得病毒爆發事件有明顯增加的趨勢。
- Windows 伺服器端修補檔未更新比例與企業組織資訊安全政策是否有集中

管理對於病毒爆發事件的影響。Windows 伺服器端修補檔未更新比例介於5%-10%間與企業組織資訊安全政策沒有集中管理時，會使得病毒爆發事件有明顯增加的趨勢。

- 企業組織資訊安全政策是否有集中管理與帳號管理對於病毒爆發事件的影響。企業組織資訊安全政策沒有集中管理與沒有進行帳號管理時，會使得病毒爆發事件有明顯增加的趨勢。
- 企業組織資訊安全政策是否有集中管理與軟體安裝政策對於病毒爆發事件的影響。企業組織資訊安全政策沒有集中管理與沒有正式的軟體安裝政策時，會使得病毒爆發事件有明顯增加的趨勢。

表 42-1.2 防毒能力與防毒能力二因子變異數分析

| 防毒能力 / 防毒能力 | Windows 客戶端修補未更新比例 |
|---|---|
| Windows 伺服器端修補檔未更新比例 | 2.770(0.003) |

[資料來源：本研究整理]

- Windows 客戶端修補檔未更新比例與 Windows 伺服器端修補檔未更新比例對於病毒爆發事件的影響。Windows 客戶端修補檔未更新比例高於 20%間與 Windows 伺服器端修補檔未更新比例介於 5%-10%時，會使得病毒爆發事件有明顯增加的趨勢。

表 42-2 病毒爆發影響嚴重程度 F(p)

表 42-2.1 公司概況與防毒能力二因子變異數分析

| 公司概況 / 防毒能力 | 員工數 |
|---|---|
| 監控防毒軟體安裝率 | 4.371(0.001) |
| 監控 AP Server 修補檔未更新比例 | 2.707(0.018) |
| 部署防毒元件 | 3.214(0.004) |
| 舉辦資訊安全教育訓練 | 5.673(0.000) |
| 社會工程教育訓練主題講座 | 3.883(0.002) |

[資料來源：本研究整理]

- 企業組織員工數與監控防毒軟體安裝率對於病毒感染程度的影響。員工數介於 501-1000 間與沒有監控防毒軟體安裝率時，會使得病毒感染程度有明顯增加的趨勢。
- 企業組織員工數與監控 AP 伺服器端修補檔未更新比例對於病毒感染程度的影響。員工數介於 501-1000 間與沒有監控 AP 伺服器端修補檔未更新比例時，會使得病毒感染程度有明顯增加的趨勢。
- 企業組織員工數與部署防毒元件對於病毒感染程度的影響。員工數介於 501-1000 間與終端使用者自行更新防毒元件且不追蹤結果時，會使得病毒感染程度有明顯增加的趨勢。
- 企業組織員工數與舉辦資訊安全教育訓練對於病毒感染程度的影響。員工數介於 501-1000 間與沒有舉辦資訊安全教育訓練時，會使得病毒感染程度有明顯增加的趨勢。
- 企業組織員工數與舉辦資訊安全教育訓練社會工程主題對於病毒感染程度的影響。員工數小於 500 與舉辦資訊安全教育訓練社會工程主題時，會使得病毒感染程度有明顯增加的趨勢。

表 42-2.2 防毒能力與防毒能力二因子變異數分析

| 防毒能力 / 防毒能力 | 監控防毒軟體安裝率 | 部署防毒元件 | 惡意網站過濾 | 社會工程教育訓練主題講座 |
|---|---|---|---|---|
| 監控 AP Server 修補檔未更新比例 | 2.441(0.069) | 5.311(0.002) | 4.173(0.008) | 5.736(0.001) |
| 社會工程教育訓練主題講座 | 5.238(0.007) | 6.723(0.000) | 3.665(0.015) | |
| 惡意網站過濾 | | 4.472(0.006) | | |
| 禁止分享資料夾 | | 3.962(0.022) | | |
| 舉辦資訊安全教育訓練 | 5.087(0.003) | | | 5.031(0.009) |

[資料來源：本研究整理]

- 監控防毒軟體安裝率與監控 AP 伺服器端修補檔未更新比例對於病毒感染程度的影響。沒有監控防毒軟體安裝率與沒有監控 AP 伺服器端修補檔未更新比例時，會使得病毒感染程度有明顯增加的趨勢。
- 監控防毒軟體安裝率與舉辦資訊安全教育訓練對於病毒感染程度的影響。沒有監控防毒軟體安裝率與沒有舉辦資訊安全教育訓練時，會使得病毒感染程度有明顯增加的趨勢。
- 監控防毒軟體安裝率與舉辦資訊安全教育訓練社會工程主題對於病毒感染

程度的影響。沒有監控防毒軟體安裝率與舉辦資訊安全教育訓練社會工程主題時，會使得病毒感染程度有明顯增加的趨勢。

- 監控 AP 伺服器端修補檔未更新比例與部署防毒元件對於病毒感染程度的影響。沒有監控 AP 伺服器端修補檔未更新比例與終端使用者自行更新防毒元件且不追蹤時，會使得病毒感染程度有明顯增加的趨勢。
- 監控 AP 伺服器端修補檔未更新比例與惡意網站過濾對於病毒感染程度的影響。沒有監控 AP 伺服器端修補檔未更新比例與沒有過慮惡意網站時，會使得病毒感染程度有明顯增加的趨勢。
- 監控 AP 伺服器端修補檔未更新比例與舉辦資訊安全教育訓練社會工程主題對於病毒感染程度的影響。沒有監控 AP 伺服器端修補檔未更新比例與舉辦資訊安全教育訓練社會工程主題時，會使得病毒感染程度有明顯增加的趨勢。
- 部署防毒元件與惡意網站的過濾對於病毒感染程度的影響。終端使用者自行更新防毒元件且不追蹤與沒有過濾惡意網站時，會使得病毒感染程度有明顯增加的趨勢。
- 部署防毒元件與禁止分享資料夾對於病毒感染程度的影響。終端使用者自行更新防毒元件且不追蹤與沒有禁止分享資料夾時，會使得病毒感染程度有明顯增加的趨勢。
- 部署防毒元件與舉辦資訊安全教育訓練社會工程主題對於病毒感染程度的影響。終端使用者自行更新防毒元件且不追蹤與舉辦資訊安全教育訓練社會工程主題時，會使得病毒感染程度有明顯增加的趨勢。
- 惡意網站過濾與舉辦資訊安全教育訓練社會工程主題對於病毒感染程度的影響。沒有過濾惡意網站與舉辦資訊安全教育訓練社會工程主題時，會使得病毒感染程度有明顯增加的趨勢。

表 42-3 偵測病毒數 F(p)

表 42-3.1 公司概況與公司概況二因子變異數分析

| 公司概況 / 公司概況 | 員工數 |
|---|---|
| 電腦數 | 4.739(0.000) |

[資料來源：本研究整理]

- 企業組織員工數與企業組織電腦數對於病毒偵測數的影響。企業組織員工數大於 3000 與企業組織電腦數介於 1001-3000 間時，會使得病毒偵測數有明顯增加的趨勢。

表 42-3.2 公司概況與防毒能力二因子變異數分析

| 公司概況 / 防毒能力 | 員工數 | 電腦數 |
|---|---|---|
| 密碼控管政策 | 7.672(0.000) | 5.910(0.000) |

[資料來源：本研究整理]

- 企業組織員工數與密碼控管政策對於病毒偵測數的影響。企業組織員工數大於 3000 與沒有密碼控管政策時，會使得所偵測病毒數有明顯增加的趨勢。
- 企業組織電腦數與密碼控管政策對於病毒偵測數的影響。企業組織電腦數介於 1001-3000 與沒有密碼控管政策時，會使得所偵測病毒數有明顯增加的趨勢。

表 42-3.3 防毒能力與防毒能力二因子變異數分析

| 防毒能力 / 防毒能力 | Windows 伺服器端修補檔未更新比例 | 密碼控管政策 |
|---|---|---|
| 密碼控管政策 | 6.345(0.000) | |
| 發佈最新型態威脅警報 | 3.184(0.009) | 3.723(0.015) |

[資料來源：本研究整理]

- Windows 伺服器端修補檔未更新比例與密碼控管政策對於病毒偵測數的影響。Windows 伺服器端修補檔未更新比例大於 10%與沒有密碼控管政策時，會使得病毒偵測數有明顯增加的趨勢。
- Windows 伺服器端修補檔未更新比例與發佈最新型態威脅警報對於病毒偵測數的影響。Windows 伺服器端修補檔未更新比例大於 10%與有發佈最新型態威脅警報時，會使得病毒偵測數有明顯增加的趨勢。
- 密碼控管政策與發佈最新型態威脅警報對於病毒偵測數的影響。有密碼控管政策與有發佈最新型態威脅警報時，會使得病毒偵測數有明顯增加的趨勢。

表 42-4 偵測感染事件數 F(p)

表 42-4.1 公司概況與公司概況二因子變異數分析

| 公司概況 / 公司概況 | 員工數 |
|---|---|
| 電腦數 | 136.228(0.000) |

[資料來源：本研究整理]

- 企業組織員工數與企業組織電腦數對於可能感染事件偵測數的影響。企業組織員工數大於 3000 與企業組織電腦數介於 1001-3000 間時，會使得可能感染事件偵測數有明顯增加的趨勢。

表 42-4.2 公司概況與防毒能力二因子變異數分析

| 公司概況 / 防毒能力 | 員工數 | 電腦數 |
|---|---|---|
| Windows 客戶端修補檔未更新比例 | 3.557(0.001) | |
| 隨時中斷辦公系統與關鍵系統間連線 | 7.636(0.000) | 7.800(0.000) |
| 統一安裝防毒軟體 | 128.489(0.000) | 5.773(0.000) |
| 客制化教育訓練 | 6.427(0.000) | 7.443(0.000) |
| 惡意網路過濾 | | 5.749(0.000) |

[資料來源：本研究整理]

- 企業組織員工數與 Windows 客戶端修補檔未更新比例對於可能感染事件偵測數的影響。企業組織員工數大於 3000 與 Windows 客戶端修補檔未更新比例大於 20%時，會使得可能感染事件偵測數有明顯增加的趨勢。
- 企業組織員工數與中斷辦公系統和關鍵任務系統間連線對於可能感染事件偵測數的影響。企業組織員工數大於 3000 與無法中斷辦公系統和關鍵任務系統間連線時，會使得可能感染事件偵測數有明顯增加的趨勢。
- 企業組織員工數與安裝客戶端防毒軟體方式對於可能感染事件偵測數的影響。企業組織員工數大於 3000 與終端使用者自行安裝防毒軟體時，會使得可能感染事件偵測數有明顯增加的趨勢。
- 企業組織員工數與舉辦客制化資訊安全教育訓練對於可能感染事件偵測數的影響。企業組織員工數大於 3000 與舉辦客制化資訊安全教育訓練時，會使得可能感染事件偵測數有明顯增加的趨勢。
- 企業組織電腦數與中斷辦公系統和關鍵任務系統間連線對於可能感染事件偵測數的影響。企業組織電腦數介於 1000-3000 間與無法中斷辦公系統和關鍵任務系統間連線時，會使得可能感染事件偵測數有明顯增加的趨勢。
- 企業組織電腦數與安裝客戶端防毒軟體方式對於可能感染事件偵測數的影響。企業組織電腦數介於 1000-3000 間與終端使用者自行安裝防毒軟體時，會使得可能感染事件偵測數有明顯增加的趨勢。
- 企業組織電腦數與惡意網站的過濾對於可能感染事件偵測數的影響。企業組織電腦數介於 1000-3000 間與過濾惡意網站時，會使得可能感染事件偵測數有明顯增加的趨勢。
- 企業組織電腦數與舉辦客制化資訊安全教育訓練對於可能感染事件偵測數的影響。企業組織電腦數介於 1000-3000 間與舉辦客制化資訊安全教育訓練時，會使得可能感染事件偵測數有明顯增加的趨勢。

表 42-4.2 防毒能力與防毒能力二因子變異數分析

| 防毒能力 / 防毒能力 | 統一安裝防毒軟體 | 惡意網站過濾 | 客制化教育訓練 |
|---|---|---|---|
| Windows 客戶端修補檔未更新比例 | 100.709(0.000) | | |
| 隨時中斷辦公系統與關鍵系統間連線 | 2.932(0.020) | 4.326(0.008) | 4.821(0.005) |
| 統一安裝防毒軟體 | | 193.887(0.000) | 8.775(0.000) |
| 惡意網站過濾 | | | 3.676(0.017) |

[資料來源：本研究整理]

- Windows 客戶端修補檔未更新比例與安裝客戶端防毒軟體方式對於可能感染事件偵測數的影響。Windows 客戶端修補檔未更新比例大於 20%與終端使用者自行安裝防毒軟體時，會使得可能感染事件偵測數有明顯增加的趨勢。
- 中斷辦公系統和關鍵任務系統間連線與安裝客戶端防毒軟體方式對於可能感染事件偵測數的影響。無法中斷辦公系統和關鍵任務系統間連線與終端使用者自行安裝防毒軟體時，會使得可能感染事件偵測數有明顯增加的趨勢。
- 中斷辦公系統和關鍵任務系統間連線與惡意網站的過濾對於可能感染事件偵測數的影響。無法中斷辦公系統和關鍵任務系統間連線與過濾惡意網站時，會使得可能感染事件偵測數有明顯增加的趨勢。
- 中斷辦公系統和關鍵任務系統間連線與舉辦客制化資訊安全教育訓練對於可能感染事件偵測數的影響。無法中斷辦公系統和關鍵任務系統間連線與舉辦客制化資訊安全教育訓練時，會使得可能感染事件偵測數有明顯增加的趨勢。
- 安裝客戶端防毒軟體方式與惡意網站的過濾對於可能感染事件偵測數的影響。終端使用者自行安裝防毒軟體與過濾惡意網站時，會使得可能感染事件偵測數有明顯增加的趨勢。
- 安裝客戶端防毒軟體方式與舉辦客制化資訊安全教育訓練對於可能感染事件偵測數的影響。終端使用者自行安裝防毒軟體與舉辦客制化資訊安全教育訓練時，會使得可能感染事件偵測數有明顯增加的趨勢。
- 惡意網站的過濾與舉辦客制化資訊安全教育訓練對於可能感染事件偵測數的影響。過濾惡意網站與舉辦客制化資訊安全教育訓練時，會使得可能感染事件偵測數有明顯增加的趨勢。

（三） 卡方分配檢定

回收樣本根據「病毒爆發事件數」、「病毒爆發影響嚴重性」、「偵測病毒數」及「偵測感染事件」分別將樣本分成四個群組，爲了了解分群之可能在安全風險上是否有差異性，本研究僅對第一個群組（最好的情況）與第四個群組（最差的情況）做比較，其中企業組織及技術架構不同之群組在安全風險上有影著差異者如表 43，分述如下：

- 在電腦數方面，電腦數少的企業組織比電腦數多的企業組織所偵測到的病毒數較少。
- 仰賴網路程度較多的企業組織會比較重視資訊安全這方面，因此其病毒爆發事件數會比較少。資訊安全人員可以得知病毒的種類，即可快速找到解決方案以降低病毒爆發的嚴重性。
- 使用某公司產品的「Email & Groupware」產品的企業組織在病毒爆發事件數上，有顯著的幫助。而使用「File Server & Storage」的企業組織在於偵測感染事件上，會偵測比較少的可能感染事件數。
- 若有使用防毒管理工具的企業組織在病毒爆發事件數上，會比沒有使用防毒管理工具的企業組織少。
- 若禁止外部使用者使用組織內部的網際網路，會降低偵測到可能感染的事件數。

表43 公司概況

| 應變項 / 公司概況 | 病毒爆發事件數 $X^2(p)$ | 病毒爆發影響嚴重性 $X^2(p)$ | 偵測病毒數 $X^2(p)$ | 偵測感染事件 $X^2(p)$ |
|---|---|---|---|---|
| 電腦數 | | | 5.619(0.060) | |
| 仰賴網路程度 | 5.04(0.08) | | | |
| 專職資訊安全人員 | | | 4.88(0.087) | 5.299(0.071) |
| 知道病毒種類 | 2.78(0.095) | | | |
| 使用 PC-Cillin Internet Security | 5.881(0.015) | | | |
| 使用 Email & Groupware | 3.082(0.079) | | | |
| 使用 ScanMail eManager | 2.723(0.099) | | | |

表 43 公司概況(續)

| 應變項 / 公司概況 | 病毒爆發事件數 $X^2$(p) | 病毒爆發影響嚴重性 $X^2$(p) | 偵測病毒數 $X^2$(p) | 偵測感染事件 $X^2$(p) |
|---|---|---|---|---|
| 使用 ScanMail for Lotus Domino | | | | 2.744(0.098) |
| 使用 File Server & Storage | | | | 6.429(0.011) |
| 使用 ServerProtect for Microsoft Windows/Novell NetWare | | | | 6.429(0.011) |
| 使用防毒管理工具 | 3.215(0.073) | | | |
| 使用 Email 閘道防毒 | | | | 2.727(0.099) |
| 外部使用者使用 Internet | | | | 3.968(0.046) |

[資料來源：本研究整理]

在防毒能力偵測上，不同之兩分群在安全風險上有顯著差異者，如表 44 所示，分述如下：

- 客戶端病毒碼、伺服器端病毒碼與防毒硬體裝置病毒碼過期比例較低的企業組織在於偵測到可能感染事件數上，會比過期比例高的企業組織的感染事件數來得少。由監控機制所搜集到的資訊會透過監控系統自動分析並且轉換成一些報表的企業組織，取得的資訊是比較有詳細說明的，因此在病毒爆發事件數上也會比較少。
- 如果能夠有效地控管使用者在網路的使用狀況的話，不管是病毒爆發事件數、病毒爆發影響嚴重程度、偵測病毒數與偵測感染的事件數上，都會有顯著的幫助。
- 資訊安全政策與教育訓練對於一個企業組織是非常重要的，不過往往因爲資訊部門權力不夠或是缺乏這方面的人才，因此無法順利或有效地推動。推動資訊安全政策與教育訓練並且強制性的企業組織，在於病毒爆發影響嚴重程度會比較容易掌控。

表44 防毒能力

| 應變項 / 防毒能力 | 病毒爆發事件數 $X^2$(p) | 病毒爆發影響嚴重性 $X^2$(p) | 偵測病毒數 $X^2$(p) | 偵測感染事件 $X^2$(p) |
|---|---|---|---|---|
| 客戶端病毒碼過期比例 | | | | 6.429(0.040) |
| 伺服器端病毒碼過期比例 | | | | 4.705(0.095) |
| 防毒硬體裝置病毒碼過期比例 | | | | 7.019(0.030) |
| 監控 Windows 伺服器端修補檔未更新比例 | | | 2.951(0.086) | |
| AP 伺服器修補檔未更新比例 | | | | 6.086(0.048) |
| 使用由監控機制所搜集到的資訊 | 7.693(0.021) | | | |
| 透過電腦名稱追蹤電腦實體位置 | | | | 3.333(0.068) |
| 辦公系統與關鍵系統使用不同網段 | | | 4.794(0.091) | |
| 隨時中斷辦公系統與關鍵系統間連線 | | | | 5.19(0.075) |
| 知道有無弱點在機構電腦中 | 7.577(0.023) | | | |
| 安裝防毒軟體方式 | | | | 5.4(0.067) |
| 增刪帳號核對確認程序 | | | 5.362(0.069) | |
| 軟體安裝政策 | | | 3.099(0.078) | 3.333(0.068) |
| 控管使用者的網路使用情況 | 4.81(0.028) | 2.797(0.094) | 2.913(0.088) | 2.727(0.099) |

表 44 防毒能力(續)

| 應變項 / 防毒能力 | 病毒爆發事件數 $X^2$(p) | 病毒爆發影響嚴重性 $X^2$(p) | 偵測病毒數 $X^2$(p) | 偵測感染事件 $X^2$(p) |
|---|---|---|---|---|
| 惡意網站過濾 | | 4.481(0.034) | | 3.394(0.065) |
| 即時通訊軟體過濾 | | 5.483(0.019) | | 6.136(0.013) |
| 串流式媒體過濾 | | | | 3.333(0.068) |
| P2P 軟體過濾 | 6.959(0.031) | | 3.747(0.053) | |
| 禁止分享資料夾 | | 5.802(0.016) | | |
| 禁止使用即時通訊軟體 | | 3.692(0.055) | | |
| 病毒爆發反應程序 | 5.201(0.074) | | | |
| 辨識病毒爆發與發毒感染的管道與原因 | | | | 4.816(0.090) |
| 資訊安全政策強制執行程度 | | 2.711(0.100) | | |
| 資訊安全教育訓練 | | 4.288(0.038) | | |
| 線上教育訓練課程 | | 5.389(0.020) | | |
| 通知使用者最新型態威脅 | | | 3.367(0.067) | 7.6(0.022) |

[資料來源：本研究整理]

## 第四節　　樣本類型探勘

本研究選擇以統計集群分析〈Cluster Analysis〉法來探索回收樣本以資訊安全角度來看是否有不同類型。進行 2 類集群分析探索：

- 以前述影響中毒之關鍵因素分析中所找出之關鍵因素進行 K means〈假設 K=4，分爲 4 群 〉 分析，然後將分群結果與本調查的應變數「過去三年間

平均一年的病毒爆發事件」、「過去三年間病毒爆發時，平均一日電腦 down 的比例」、「最近三個月，平均一個月所偵測到的病毒數」與「最近三個月，平均一個月所偵測到的可能感染事件數」比較。

- 試圖以不同之變數群〈如組織基本資料、網路安全基本資料、某公司產品使用情形、防毒能力評估變相等〉進行層次分群分析法（Hierarchical Cluster Analysis），試圖找出不同之樣本類型。

結果敘述如下：

透過卡方分配檢定對群組 1-4 做分析與僅對群組 1 和 4 做分析的結果做比較，選取出使得這兩個分析中的產生顯著差異的變異數。其變異數爲「機構電腦數」、「有無使用 File Server & Storage」、「有無使用 Server Protect for Microsoft Windows/Novell NetWare」、「客戶端電腦病毒碼過期比例」、「伺服器端電腦病毒碼過期比例」、「防毒硬體裝置病毒碼過期比例」、「監控 Windows 伺服器端修檔未更新比例」、「如何使用監控機制所搜集到的資訊」、「客戶端防毒軟體安裝移除方式」、「是否有軟體安裝政策」、「是否控管使用者網路使用狀況」、「惡意網站的過濾」、「即時通訊軟體的過濾」、「禁止分享資料夾」、「是否有做資訊安全教育訓練」與「是否有發佈最新型態威脅的警報」。透過以上幾個變異變，使用 K-Means Cluster 將整個樣本分成 4 個 Cluster，如表 45 所示。

表45 使用 K-Means Cluster 分成 4 個群組

| | Cluster | | | |
|---|---|---|---|---|
| | 1 | 2 | 3 | 4 |
| 如何使用由監控機制所搜集到的資訊 | 1 | 1 | 3 | 1 |
| 沒有控管使用者的網路使用狀況 | 0 | 0 | 0 | 0 |
| 禁止分享資料 | 0 | 0 | 0 | 0 |
| 資訊安全教育訓練 | 1 | 1 | 1 | 1 |

表 45 使用 K-Means Cluster 分成 4 個群組(續)

| | Cluster | | | |
|---|---|---|---|---|
| | 1 | 2 | 3 | 4 |
| 追蹤Windows伺服器端的修補檔未更新的比例 | 1 | 1 | 1 | 1 |
| 軟體安裝政策 | 2 | 2 | 2 | 2 |
| File Server & Storage | 0 | 0 | 0 | 1 |
| ServerProtect for Microsoft Windows/Novell NetWare | 1 | 1 | 1 | 0 |
| 追蹤客戶端電腦的病毒碼過期的比例 | 2 | 1 | 2 | 2 |
| 追蹤伺服器端電腦病毒碼過期的比例 | 2 | 1 | 2 | 2 |
| 追蹤防毒硬體裝置的病毒碼過期的比例 | 2 | 1 | 2 | 2 |
| 安裝或移除客戶端防毒軟體的方式 | 3 | 3 | 3 | 1 |
| 惡意網站的過濾 | 0 | 1 | 1 | 0 |
| 即時通訊軟體的過濾 | 0 | 0 | 0 | 1 |
| 向使用者發布最新型態威脅的警報 | 1 | 3 | 3 | 3 |
| 電腦數 | 1 | 2 | 2 | 3 |

[資料來源：本研究整理]

這四個集群的分佈並沒有驗證之前所假設的四個群組的分佈。以「病毒爆發事件數」來看，四個集群（如表 46）的平均病毒爆發事件數落在 1.9 與 2.47 件之

間，也就是落在之前所預期的群組 2 與群組 3 內。而在「病毒感染嚴重程度」來看，四個集群的平均嚴重程度落在 9.33%與 15.09%之間，也就是落在之前所預期的群組 3 與群組 4 內。雖然試圖將四群分別命名，但因爲「病毒爆發事件數」及「病毒感染嚴重程度」差異並不是很顯著，因此只能說這樣的分群有一些辨別力，但可能分辨力不是太強。

表46 K-Means Cluster

| | | 病毒爆發頻次 | 病毒感染嚴重程度 |
|---|---|---|---|
| K-Means Cluster1 | 樣本數 | 24 | 24 |
| | 平均值 | 1.90 | 11.0417 |
| | 標準差 | 2.116 | 19.94008 |
| K-Means Cluster2 | 樣本數 | 25 | 25 |
| | 平均值 | 2.00 | 12.1400 |
| | 標準差 | 1.658 | 16.54635 |
| K-Means Cluster3 | 樣本數 | 31 | 30 |
| | 平均值 | 2.32 | 9.3333 |
| | 標準差 | 1.990 | 13.27776 |
| K-Means Cluster4 | 樣本數 | 17 | 17 |
| | 平均值 | 2.47 | 15.0882 |
| | 標準差 | 2.095 | 21.19569 |

[資料來源：本研究整理]

希望能夠從資料中找出分群，因此首先試圖透過「某公司產品使用情形」來進行層次分群（Hierarchical Cluster），以求能夠在這些資料中，找出分群的可能性（如果係數遞增量有鉅增時，代表可能是一個合適的分群數目）。而層次分級的結果如表 47 所示，並無法如預期一樣，從「某公司產品使用情形」的各項變數中，找出合適的分群。〈註：由 5 群降至 4 群時，雖然係數遞增量有鉅增的情況，但考慮分成 5 群後，各群樣本太少，不太容易找出差異或是差異不見得有代表性，因此並沒有繼續再做後續分析〉

表47 第一次層次分群係數增量表

| 分析組 | | |
|---|---|---|
| 集群數 i | 凝聚係數 | 係數遞增量 i-(i+1) |
| 10 | 4 | 0.00% |
| 9 | 4 | 0.00% |
| 8 | 4.5 | 12.50% |
| 7 | 4.663 | 3.62% |
| 6 | 4.833 | 3.65% |
| 5 | 4.925 | 1.90% |
| 4 | 5.606 | 13.83% |
| 3 | 6.189 | 10.40% |
| 2 | 6.5 | 5.03% |
| 1 | 6.942 | 6.80% |

[資料來源：本研究整理]

之後再嘗試從「某公司產品使用情形」、「弱點管理工具使用情況」與「防毒管理工具使用情況」等變數來進行層次分群分析。結果如表 48 所示，也無法從這些變數中，求出分群。

表48 第二次層次分群係數增量表

| 分析組 | | |
|---|---|---|
| 集群數 i | 凝聚係數 | 係數遞增量 i-(i+1) |
| 10 | 6.843 | 5.28% |
| 9 | 7 | 2.29% |
| 8 | 7 | 0.00% |
| 7 | 7.667 | 9.53% |
| 6 | 7.7 | 0.43% |
| 5 | 8.222 | 6.78% |
| 4 | 9 | 9.46% |
| 3 | 9.216 | 2.40% |
| 2 | 9.65 | 4.71% |
| 1 | 10.183 | 5.52% |

[資料來源：本研究整理]

最後，透過「防毒能力評估」中的變數進行層次分群分析。結果如表 49 所示，有顯著的成長，因此可以將試圖透過「防毒能力評估」中的變數將整個樣本分成二個集群。

表49 第三次層次分群係數增量表

| 分析組 | | |
|---|---|---|
| 集群數 i | 凝聚係數 | 係數遞增量 i-(i+1) |
| 10 | 20 | 11.11% |
| 9 | 20.25 | 1.25% |
| 8 | 20.333 | 0.41% |
| 7 | 21.08 | 3.67% |
| 6 | 21.662 | 2.76% |
| 5 | 23 | 6.18% |
| 4 | 23.426 | 1.85% |
| 3 | 24.135 | 3.03% |
| 2 | 25.253 | 4.63% |
| 1 | 34.207 | 35.46% |

[資料來源：本研究整理]

這兩個集群的「病毒爆發事件數」與「病毒感染嚴重程度」的比較如表 50 所示，而集群 1 的樣本在於「防毒能力評估」方面都比集群 2 的高，不過從分群的比較如表 51 中，不管是「病毒爆發事件數」或是「病毒感染嚴重程度」的平均值，集群 1 皆高於集群 2，所以這個分群不合理。

表50 驗證集群

| | 集群 | |
|---|---|---|
| | 集群 1 | 集群 2 |
| 追蹤伺服器的離線率 | 2 | 2 |
| 追蹤客戶端電腦的病毒碼過期的比例 | 2 | 2 |
| 追蹤伺服器端電腦的病毒碼過期的比例 | 2 | 2 |
| 追蹤防毒硬體裝置的病毒碼過期的比例 | 2 | 2 |
| 追蹤Windows客戶端的修補檔未更新的比例 | 2 | 2 |
| 追蹤Windows伺服器端的修補檔未更新的比例 | 2 | 2 |
| 追蹤伺服器端的修補檔未更新的比例 | 2 | 2 |
| 機構防毒監控與偵測能力 | 2 | 2 |

表 50 驗證集群(續)

| | 集群 | |
|---|---|---|
| | 集群 1 | 集群 2 |
| 如何使用由監控機制所搜集到的資訊 | 2 | 1 |
| 透過電腦名稱來追蹤電腦的實體位置 | 3 | 2 |
| 使用不同的網路區段 | 2 | 1 |
| 隨時中斷辦公系統與關鍵任務系統間的網路連線 | 2 | 2 |
| 知道目前有無任何弱點 | 2 | 1 |
| 部署安全修補檔 | 2 | 2 |
| 後續動作來改進修補檔的部署 | 2 | 1 |
| 安裝或移除客戶端防毒軟體的方式 | 3 | 2 |
| 部署防毒的元件 | 3 | 2 |
| 後續動作來改進病毒碼的更新 | 2 | 2 |
| 帳號核對確認程序 | 3 | 2 |
| 密碼控管政策 | 2 | 1 |
| 軟體安裝政策 | 2 | 1 |

[資料來源：本研究整理]

【註】數字小者表選項較前，因此情況沒有數字大者好。

表51 驗證集群：集群 1 與集群 2 比較

| | | 病毒爆發事件數 | 病毒感染嚴重程度 |
|---|---|---|---|
| 集群 1 | 樣本數 | 70 | 69 |
| | 平均值 | 2.34 | 11.5580 |
| | 標準差 | 2.111 | 17.25832 |
| 集群 2 | 樣本數 | 27 | 27 |
| | 平均值 | 1.7 | 11.3889 |
| | 標準差 | 1.353 | 17.69090 |

[資料來源：本研究整理]