# 網路安全與管理簡介

```

1.網路安全

1.1安全威脅

1.2系統漏洞

1.3入侵手法

2.資訊安全

2.1資訊安全種類

2.2資訊安全防範

3.網路安全措施與管理

3.1系統管理者安全措施

3.2使用者安全措施

3.3環境安全措施

3.4網路安全管理

```

## 1.網路安全

### 1-1安全威脅

```

1.竊聽

2.偽裝

3.竄改

4.滲透

5.病毒

6.否認

7.癱瘓

```

### 1-2系統漏洞

```

1.網路漏洞:

瀏覽器或是系統程式的漏洞

2.設定漏洞

權限設定被忽略，造成連線漏洞。

3.標準漏洞

各家廠商不同標準，造成技術上的漏洞。

4.政策漏洞

安全防護措施不足所造成的安全性漏洞

```

### 1-3入侵

```

1.網路探查:

利用偵測城市偵測在進行入侵或攻擊

2.密碼入侵

利用密碼偵測程式碼竊取使用者密碼

3.癱瘓服務

傳送大量郵件、檔案造成癱瘓

4.網路竊取

藉封包解析解析傳送的資料訊息

5.身分偽裝

假借封包來源欺騙主機系統入侵主機

```

## 2.資訊安全

### 2-1資訊安全種類

```

1.實體安全

2.資料安全

3.程式安全

4.系統安全

```

### 2-2資訊安全防範

```

1.偶發事件防範

2.蓄意破壞防範

3.資料備份原則

4.密碼使用原原則

5.架設防火牆

6.資料加密解密

7.秘密通訊

8.憑證管理

```

## 3.網路安全措施與管理

### 3-1系統管理者安全措施

```

1.系統管理者應由主管人託付可以信賴的人。

2.需負責網路安全規範之訂定，執行網路管理之設定操作，確保資料安全。

3.負責規劃使用者帳號及製發帳號，提供授權之使用者使用。

4.開放業務有關人員可遠端登入內部系統服務，且嚴格身分辨識。

5.保留所有人員登入紀錄

6.未經使用者同意，不得新增、刪除、修改他人資料、亦不得變更稽核資料檔案

```

### 3-2使用者安全措施

```

1.只能在授權的範圍存取資料。

2.應遵守網路安全規定,了解權利及義務以及相關法規。

3禁止蓄意干擾或妨礙網路系統,造成系統癱瘓。

4.禁止任何方式竊取他人之帳號及密碼。

5,禁止使用任何工具或軟體竊聽網路通訊。

6,禁止使用未經授權的檔案或程式。

7.禁止偽造他人身份發送檔案或文件。

8,禁止發送垃圾郵件。

```

### 3-3環境安全措施

```

1,定期更新系統,使系統軟體處在最佳狀態。

2.修補系統與軟體的漏洞,減少駭客或病毒的入侵。

3. 加裝個人防火牆,保護電腦降低被攻擊或植入程式的機會。

4.定期更新防毒軟體的病毒碼。

5.垃圾郵件的過滤。

```

### 3-4網路安全管理

```

1.防火牆隔離架設

2.不斷電系統維護

3.備份系統的檢查

4.檔案傳輸加解密

5.系統管理者責任

6.遠端連線的控管

7.病毒碼更新維護

8.人員認知與訓練

9.網路位址的偽裝

10.電腦的門禁管制

```