# 作業系統安全

```

1.windows 的網路安全

1.1保護電腦

1.2瀏覽器的安全性

1.3垃圾郵件

2.使用者驗證

2.1使用者驗證方法

2.2.RADIUS

2.3Biometrics

3.授權

3.1保護資料避免未授權的檢視

3.2以使用權限來保護網站

3.3授權管理員

3.4授權管理員和管理工具比較

3.5以NTFS 權限保護檔案

3.6Active Diectory

3.7使用者帳戶

3.8服務系統管理帳戶及群組安全性

3.9群組原則功能

3.10 保護文件的簡單方法

3.11 Delegation

4.密碼原則

4.1密碼八不守則

4.2動態密碼

4.3密碼驗證系統

4.3.1可靠密碼的特性

4.3.2強式密碼

5.稽核

5.1稽核原則

5.2可稽核的事件類型

6.密碼學

6.1 不對稱密碼

6.2 對稱式密碼

6.3 Session Key

6.4 EFS

6.5 APPLocker

6.5TPM

6.6 Digital Signature

6.7 Private Key AND Public Key

7.惡意軟體

7.1電腦病毒

7.2防範電腦病毒

7.3防範IM病毒

7.4防範電腦病毒及間諜軟體

7.5Worms

7.6Trojans

7.7流氓軟體

7.8主動式攻擊

7.9Backdoor

8.windows 10全面的安全性

8.1虚擬化

8.2線上保護

8.3生物特徵辨識

8.4遺失裝置的資料保護

8.5裝置完整性

8.6加密處理

8.7信賴平台模組新功能

9.補充

9.1機密分級

9.2作業系統更新

9.3最小密碼長度

9.4憑證概觀

```

## 1.windows 的網路安全

### 1.1保護電腦

```

1,防火牆

2.防毒保護·

3.間諜軟體及其他惡意程式碼保護。

4.Windows Update Windows。

```

### 1.2瀏覽器的安全性

```

1, SmartScreen篩選工具可以協助保護您防範線上網路釣魚攻擊、詭計、詐騙或惡意的網站。

2.網域反白顯示,可讓您更輕松地查看您造訪之網站的實際網址。

這有助於防止使用不實網址欺騙您的假網站或網路釣魚網站。

您造訪的真實網域會在網址列中反白顯示。

3.管理附加元件可以讓您停用或允許網頁瀏覽器附加元件,並刪除不想要的Activex 控制項。

4.跨站台的指令碼處理(SS)篩選器,可協助防止可能嘗試竊取您個人及財務資訊之網路釣魚及詐騙網站的攻擊。

5.使用安全網站的128位元安全(SSL)連線，

可以讓Internet Explorer與銀行、線上商店、醫療網站或其他掌握機密客戶資訊的組織所執行的網站之間建立加密連線。

```

### 1.3垃圾郵件

```

1.垃圾郵件特徵

常見的垃圾郵件形式是訊息的「收件者:」或「副本:」欄位中沒有您的電子郵件地

址。有些垃圾郵件可能含有攻擊性語言或不當網站內容的連結。

2.垃圾郵件對策

(1).安裝垃圾郵件過濾/攔截軟體,如Norton 垃圾郵件過漉網

(2).如果您懷疑某封電子郵件是垃圾郵件,請勿回應,將它刪除即可

(3),考慮停用電子郵件的預覧窗格,並以純文字方式讀取電子郵件

(4).拒絕所有來自不在好友清單上之人員的即時通訊

(5),請勿按下即時通訊內的URL連結(除非是已知來源及預期的連結)

(6).將軟體及安全修正程式保持在最新狀態

```

## 2.使用者驗證

### 2.1使用者驗證方法

```

1.驗證

2.鎖定使用者帳戶

3.Smart cards

>使用Bitlocker

>使用PKINIT通訊協定的智慧卡網域登入

>文件和電子郵件簽屬

>與特定業務應用程式搭配使用

>隨插即用的增強支援

>透過WINDOWS UPDATA來發布

```

### 2.2.RADIUS

```

使用者服務是一個AAA協議，意思就是同時兼顧:

驗證(authentication)

授權(authorization)

帳戶管理(accounting)

三種服務的協議(protocol)。

```

### 2.3Biometrics

```

Biometrics生物識別功能

愈來愈多的電腦(特別是可攜式電腦)包含内嵌的指紋辨識器。可用於識別和驗證Windows中的使用者。

```

## 3.授權

### 3.1保護資料避免未授權的檢視

```

目錄支援存取控制的方法有下列兩種:

1.提供儲存、分配、尋找和擷取存取控制清單(ACL)所需的儲存機制應用程式。

2.使用目錄定義物件以及用於授權應用程式和使用者存取特定網路資源的物件麗性。

```

### 3.2以使用權限來保護網站

```

1,網站使用權限不可用來替代NTFS使用權限。

而是與NTFS使用權限搭配使用,以加強網站內容的安全性。

2.可設定特定網站、目錄及檔案的網站存取使用權限。

與NTFS使用權限不同,網站使用權限會影響嘗試存取網站的所有人。

下列狀況適用於設定使用權限:

1.目錄或檔案的網站使用權限與NTFS權限衝突,則會套用較嚴格的設定。

2,停用權限會限制全部使用者。

例如:停用「讀取」權限,則無論使用者帳戶的NTFS 使用權限如何,所有使用者均無法瀏覽檔案。相反的,如果啟用該權限,所有的使用者皆可瀏覽該檔,除非 NTFS 使用權限禁止存取。

3,如果lS和NTS使用權限同時都有設定,則拒絕存取的設定會優先於授與存取。

```

### 3.3授權管理員

```

以角色為基礎的系統管理對兩種角色別有利

1.使用者授權角色

2.電腦設定角色

使用授權管理員你可使用下列兩種模式

1.程式開發人員模式

2.系統管理員模式

授權管理員新功能:

1.[授權管理員]存放區可以儲存在 Microsoft SQL Server 資料庫、Active Directory網域服務(AD DS)、Active Directory輕量型目録服務(AD LDS)或 XML 檔案中。

2.現在已能支援商務規則群組(也就是其成員資格是在執行階段由指令碼所決定的群組)。

3.支援自訂物件選取器,因此,應用程式系統管理員可以針對使用 AD LDS 或 SQL使用者帳戶的應用程式,使用授權管理貫。

4.LDAP 查詢並不只伺限於使用者物件。

5.如果稽核為使用中,則其他事件均會記錄於記錄檔中。

6.商務規則和授權規則的使用由登錄設定所控制。在Windows Server 2008 R2 及Windows Server2008中,預設值,規則是停用的。舊版Windows 中,預設會啟用規則。

```

### 3.4授權管理員和管理工具比較

```

1.存取控制清單

管理存取控制原則

2.委派控制精靈

自動設定多個權限，不提供追蹤與移除的方法

```

### 3.5以NTFS 權限保護檔案

```

設定NTFS使用權限時，請參考下列最佳做法:

1.指派使用權限給群組,。

2.避免變更物件上預設的使用權限項目,

3.切勿拒絕Everyone群組存取物件。

4.若物件有明確的「允許」使用權限項目,則繼承的「拒絕」使用權限不會防止存取物件。

5.「拒絕」使用權限只能使用在下列的特殊情況中:

・將具有「允許」使用權限群組的子集合排除在外。

・您指定「完全控制」給使用者或群組時,將某個特定的使用權限排除在外。

```

### 3.6Active Diectory

```

她處理了組織中的網路物件，使用者、群組、電腦、網域控制站、由建、設定黨、組織單元、樹系等等

Active Directory 網域的系統管理帳戶包括:

>Administrator帳戶,在網域第一個網域控制站安裝Active Directory 即建立。是網域權限最高的帳戶。

>新設在有系統管理特殊權限群組裡的帳戶,或直接指派系統管理特殊權限的帳戶。

Active Directory網域的系統管理群組會依安裝在網域的服務而有不同。用來管理Active Directory 的群組包括:

>[Builtin]容器自動建立的系統管理群組。

>[User]容器自動建立的系統管理群組。

>新建立在另一個有系統管理特殊權限群組裡的群組。

Active Directory 群組類型:

1.發布群組

2.安全性群組

```

### 3.7使用者帳戶

```

1.標準

2.系統管理員

3.來賓

```

```

使用標準帳戶有助於讓您的電腦更安全。其他人在您登入電腦時，無法竄改電腦的設定及帳戶。

```

```

每個Active Directory 的安裝在每一個網域都有一個名為Administrator的帳戶。不可刪除或鎖定這個帳戶。

駭客企圖進系統時,通常會先嘗試取得Administrator帳戶密碼。因此請重新命名並消除任何顯示它是Administrator帳戶的文字。

建立一個沒有特別權限或使用者權限的誘餌使用者帳戶,命名為 Administrator並為這個Administrator 帳戶建立一個又長又複雑的空碼。

```

```

Guest允許没有帳戶的使用者,以來賓身分登入。這個帳戶預設停用。

```

### 3.8服務系統管理帳戶及群組安全性

```

在Active Directory建立一個受控制的組織單位(OU)樹狀子目錄·

OU是含有網域的容器,這些網域可包含其他OU、使用者、群組、電腦和其他物件。這些0U和子0U形成一個有網域的暦級結構,主要用於群組物件的管理。

建立包含所有服務系統管理員帳戶,及它們使用的系統管理工作站的樹狀子目錄,您就可憑用特定安全性和原則設定,達到最大的保護。

建立樹狀子目錄:

1,建立樹狀子目錄的OU結構。

2,設定樹状子目錄 OU的權限。

3,將服務系統管理員群組移到樹狀子目錄。

4,將服務系統管理員使用者帳戶移到樹狀子目錄。

5,將服務系統管理員工作站帳戶移到樹状子目錄。

6,在樹狀子目錄0U啟用稽核。

```

### 3.9群組原則功能

```

1,群組原則喜好設定定義了使用者可變更的預設設定,並針對對應的網路磁碟機、排程工作與其他非群組原則威知的Windows 元件進行集中式管理。

2.系統管理員可以要求使用者透過群組原則使用BitLocker To Go,對卸除式存

放裝置進行加密處理。

```

### 3.10 保護文件的簡單方法

```

1.銷毀影印資料

2.標示文件

3.使用密碼保護

4.安裝防火牆

5.把門鎖上

```

### 3.11 Delegation

```

授權分三種類型:

1.完全授權

2.部分授權

3.授權書授權

```

## 4.密碼原則

### 4.1密碼八不守則

```

1.不用個人基本賀料(如生日、身分證子號)

2.不用家人基本資料(如配偶、子女、男/女朋友)

3,不用個人電話號碼(如辦公室、家裡、手機)

4.不用個人名片所載資料(如eMail、公司統編)

5.不用個人銀行相關資料(如帳號、通提密碼)

6.不用個人生活相關資料(如車籍資料、醫療資料)

7.不用具規則性排列等容易被有心人士猜到的數字(如a111111)

8.不用一般性密碼(如會員密碼eMail密碼)

```

### 4.2動態密碼

```

1.一次性密碼(One Time Password,簡稱 OTP)·又稱動態密碼,是指只能使用一

次的密碼。

2一般的靜態密碼在安全性上容易因為木馬與鍵盤側錄程式等而被竊取,而只要花上相當程度的時間,也有可能被暴力破解。為了解決一般密碼容易遭到破解情況,因此開發出一次性密碼的解決方案。

3.每次使用時產生的密碼都不一樣,可以两補傅統「SL密碼」固定密碼的缺點,防

止駭客森得密碼後胡作非為。具有

(一)安全性高

(二)使用門檻低

(三)費用節省

(四)便利性高等優點

4.動態密碼係由晶片卡配合密碼產生器構成:即使密碼產生器並没有與電腦連線,但可以在核卡時就置入多樣化的個人Key值,每張卡片Key值皆不相同,再加上每

次使用時都賦予有不同的序號,兩者(i.e.Key值與使用序號)決定了密碼。所以

使用者每次使用的動態密碼也就不一樣。

```

### 4.3密碼驗證系統

#### 4.3.1可靠密碼的特性

```

1.長度至少有八個字元。

2,混合字母與數字(包含字母與數字兩者)。

3,至少有兩個字母、一個數字與一個特殊符號(像是標點符號或星號)。

4.不使用正式名稱、寵物名字或字典裡的字。

5.密碼的起頭與結尾不要用數字(除非是使用多位數字)。

6.如果可能,混合大小寫字母(有些系統會區分大小寫)。

7.看起來要沒有規律。

8,每六十天到九十天就要更換。

9.六個月内不能重複使用相同的密碼。

10.更換前后差異要很大。

```

#### 4.3.2強式密碼

```

1.長度至少為8個字元,愈長愈好

2,包括大小寫字母,以及數字和符號

3.經常變更

4.新的密碼和舊密碼不相似

```

## 5.稽核

### 5.1稽核原則

```

稽核原則(audit policy)定義了將事件寫在事件發生電腦的安全性記錄檔中。例如,

只要有人企圖登入,系統就將該事件寫在電腦的安全性記錄檔中。

1.建立稽核原則

追蹤事件的成功與否,例如下列各種嘗試:使用者的登入、特殊的使用者讀取特定

檔案、變更使用者帳戶或者群組成員關係,以及變更您的安全性設定。

2.消除或最小化非授權使用資源的危險性。

稽核功能上的改善讓專業人員得以使用群組原則,針對檔案與登錄存取設定更完整的稽核機制。

```

### 5.2可稽核的事件類型

```

1,存取檔案和資料夾

2.登入和登出

3,關閉和重新啟動一台執行Windows電脳

4.變更使用者帳戶和群組

5,企團變更基於Active Directory技術的目錄服務中之物件(只有在您執行電腦是

網域的一部分時會發生)

```

## 6.密碼學

```

密碼學(cryptography)是一門將資訊加密和解密的科學,

目的是不輕易的讓資訊内容被未經授權的人瞭解或修改。

密碼學可以應用在認證、不可否認、隱私、訊息完整、數位簸輩。

密碼(cipher)是密碼學的關鍵,好的密碼應該符合兩項規範:

首先,不使用金論應該難以將密文還原成明文

其次,密文所顯示的字母符號,出現的頻率應該相同。

若能符合這兩項規範,就不容易利用統計攻擊的方式找出密文的密碼對映模式。

```

### 6.1不對稱密碼

```

不對稱密碼使用了兩把不同的金論:公開金鑰與私密金鑰,這兩把金鑰也稱為金鑰對(key pair),

其中一把用來加密,另一把用來解密。

公開金鑰(publickey)領名思義是公開給大家使用,

而私密金鑰(private key)就只有擁有者能用,而且是由擁有者自行管理。

當傳送端要傳訊息給接收端,傳送端會以接收端的公開金鑰來加密訊息(接收端的公開金總是眾人皆能使用),然后將密文傳給接收端。

接收端收到後,就以其的私密金鑰來解密訊息;只有接收端擁有這把私密金鑰,因此也只有接收端能解讀訊息。

如果換成是接收端要傳訊息給傳送端,整個情況也跟著反過來。

```

### 6.2 對稱式密碼

```

對稱式密碼需要發送端和接收端共用加解密的金鑰資訊,

但這共用金鑰的簡單行為,卻會讓對稱式密碼的安全風險大於不對稱密碼,

因為共用金鑰就表示很多人都能知道這把金鑰的細節。

若通訊中的發送端和接收端相隔著賣體距離時,

要如何安全的在這兩端交換金鑰,就變得困難,因為相隔的賈體距離,會

增加兩端在交換金鑰時,為攔截或竊取金鑰而被入侵或攻擊的機會。

因為對稱式密碼只使用一把金鑰,

因此攻擊者就比較容易分辨出兩端所使用的金鑰。

共用同一把金舗其買也並非完全沒有優點,

例如:因為只用了一把金鑰,因此運算的速度會比不對稱密碼快。

```

### 6.3 Session Key

```

連線金鑰兼具對稱式密碼和不對稱密碼的優點。

連線金鑰(session key) 會使用定期更換、更新的金鑰對,

而且當發送端和接收端通訊之際,就會建立雙方的連線(session )

連線金鑰的作法是以對稱式密碼來傳送訊息,可更快的速度完成這部份的傳輸。

為了維持通訊的安全,就以不對稱密碼來傳送或更新對稱式密碼所共用的金鑰。

在通訊的時候,資料的加解密是由連線金鑰對完成,

而當通訊終止時,連線金鑰對也隨之終止

```

#### 6.4EFS

```

檔案加密系統(EFS),可讓您將個別檔案及資料夾內全郎的資料加密。

EFS控制誰可以加密或修復這些資料。檔案加密後即使攻擊者能存取電腦資料的储存實體,也無法讀取使用者的資料。

若要使用EFS,全部的使用者必須擁有「加密檔案系統」憑證,允許擁有者使用

EFS 為資料加密和解密的數位文件。EFS使用者也必須擁有NTFS權限,才可以修改檔案。

EFS有兩種憑證

1.加密檔案系統憑證

2.檔案修復憑證

```

#### 6.5APPLocker

```

AppLocker提供簡單、強大的規則結構並引進發行者規則:

以應用程式數位簽章為基礎的規則。

發行者規則可以指定如應用程式版本的屬性,

以建立可在應用程式更新后使用的規則。

例如,建立「如果是由軟體發行者Adobe簽署的話,允許執行大於程式Acrobat Reader 9.0的所有版本」規則。

Applocker提供:

1,防止未授權的軟體在您的桌上型電腦環境下執行(如果該軟體不在允許清單中)

2,防止易受攻擊且未經授權的應用程式在您的電腦環境下執行

3,禁止使用者執行非必要性消耗網路頻寬或任何可能影響企業運算環境的應用程式

4.防止使用者執行使他們電腦環境不穩定且增加支援人員支援成本的應用程式

5.針對有效的桌面設定管理,提供更多選擇

6.允許使用者根據原則執行核准的應用程式和軟體更新,

同時保留只有具有系統管理認證的使用者可以安裝或執行應用程式和軟體更新的需求

7.協助確保桌上型電腦環境符合企業原則及業界法規

AppLocker:

1,根據衍生自数位簽章的檔案屬性定義規則。

2指派規則給安全性群組或個別使用者。

3,建立規則例外。

4.在強制執行原則之前,使用僅稽核模式部署原則並了解其影響。

5.匯入及匯出規則。

6.使用適用於 AppLocker 的Windows PowerShell Cmdlet,簡化 AppLocker 規則的建立及管理。

```

### 6.5TPM

```

何謂信賴平台模組?TPM是一種微晶片,

其設計用意在於提供基本的安全性相關功能

TPM通常是安裝在電腦的主機板上,並且使用硬體匯流排與其他系統通訊。

```

### 6.6 Digital Signature

```

Digital Signature 數位簽章,

讓訊息、檔案或其他數位編碼資訊的建立者將其身份識別連結到資訊的一種方法。

第三方的憑證管理機構(Certificate AuthorityㆍCA)通常能管理、使用数位憑證,

而且會將私密金鑰包入公開金錦·以保證安全通訊所用的数位簽章是有效的。

```

### 6.7 Private Key AND Public Key

```

Private Key

Private Key 私密金鑰,

與公開金鑰演算法搭配使用的密碼編譯識別碼配對秘密的那一半。

私密金鑰酒常是用來將對稱工作階段歳別碼、数位式簸器資料及使用相對公開金鑰加密的加密資料解密。

Public Key

Public Key公開金鑰

與公開金鑰演算法搭配使用的密碼編譯識別碼配對非秘密的那一半。

公開金鑰通常是在為工作階段識別碼加密、驗證數位簽章,或為可以使用相對私密金鑰加密的資料加密時使用。

```

## 7.惡意軟體

```

惡意軟體是一種惡意程式碼類別,

包括病毒、病蟲及特洛伊木馬程式。惡意軟體會利用熱門的通訊工具進行散佈,

包括透過電子郵件與即時通訊傳送病蟲、從網站丟下特洛伊木馬程式,

以及從點對點連線下載遭病毒感染的檔案,

惡意軟體也會刺探利用系統上存在的漏洞,進而無聲無息且輕松地入侵系統。

```

### 7.1電腦病毒

```

病毒可能會毀壞或刪除電腦上的資料,利用您的電子郵件程式自行散饰到其他電

腦,或者甚至會刪除您硬碟上的所有資料。

病毒可以很容易地透過電子郵件或立即訊息中的附件散饰,

病毒可能會偽裝成有趣的圖片、賀卡或音訊與視訊檔案等附件形式。

```

### 7.2防範電腦病毒

```

1,使用網際網路防火牆。

2,造訪 Microsoft Update 並開啟自動更新。

3.訂閱產業標準級防毒軟體,例如Windows Live OneCare,

並隨時將其保持在最新狀態。

4.絕不開啟陌生人寄來的電子郵件附件。

5,除非您確切瞭解附件內容,否則應避免開啟認識的人寄來的電子郵件附件。

寄件者可能不知道附件夾帶病毒。

```

### 7.3防範IM病毒

```

1小心IM中的連结和檔案

2更新您的Windows 軟體

3確定您使用的是最新版的1M軟贈

4使用防毒軟體:並保持更新

5使用反間業功能軟體·並保持更新

```

### 7.4防範電腦病毒及間諜軟體

```

1.自動更新 Windows

2.下載最新的反間諜軟體以及防毒更新程式,然后立刻掃描您的霍腦。

3.使用防火牆

4.開啟收到的權案及電子郵件附件之前·先掃描

5.使用垃圾郵件篩選功能

6. 安装並執行程式·有助於偵測並移除間謀軟體。

```

### 7.5Worms

```

蠕蟲無需與使用者互動,即可從一台電腦複製到另一台。

跟電腦病毒不同的是,蠕蟲可自動複製。

舉例來說,蠕蟲自我複製,並將複製出來的蠕蟲寄給您電子郵件通訊錄中的每一個

人,接著再陸續寄給這些人電子郵件通訊錄中所有的人。

防止感染蠕蟲的方法,就是開啟電子郵件時要謹慎小心。

朋友寄來的電子郵件有附件,最安全的方法就是連繫朋友,

問他們是否傳送了該附件。收到不認識的人的郵件,最安全的方法是將其刪除。

```

### 7.6Trojans

```

特洛伊木馬是有用軟體的電腦程式,但它卻會危害您的安全性造成許多的損害。最近的特洛伊木馬程式的形式為一封電子郵件

,其宣稱為Microsoft安全性更新的附件檔,

之後化身為病毒並嘗試停用防毒軟體和防火牆軟體。

當人們被引誘開敗程式時,特洛伊木馬程式即會散布開來。

為了更完善地保護使用者,Microsoft通常是送過電子郵件寄出安全性公告,但絕不會包含附件檔。

```

### 7.7流氓軟體

```

微軟安全應變中心(Microsoft Security Response Center, MSRC) 發現越來越大量的流氓軟禮在網路上流盛,造成使用者損失。

流氓軟體是一種介於正常軟體與惡意程式/病毒中間的程式,

近期大量流行於網路上的流氓軟體外觀上大多偽装成防毒、反間諜軟體,

誘騙使用者信賴安裝,甚至進一步透過其介面進行線上採。

實際上往往内含相當多的惡意行為，

輕則持續性彈出质告視窗,嚴重如側錄鍵照敲擊，遠端惡意程序下載、開啟後門允許駭客從遠端入侵,綁架瀏覧器存取固定頁面等實質危害。

```

### 7.8主動式攻擊

```

主動式攻擊可分為四類

1.偽裝.

2.修改訊息內容

3.重送

4.阻絕服務

```

### 7.9Backdoor

```

後門程式通常指 不明遠端人士未經系統管理員之允許，且利用不正當的手法進入電腦中，

且可能會偷走個資、機密資訊等、甚至隨心所欲操縱電腦。

```

## 8.windows 10全面的安全性

### 8.1虚擬化

```

藉由Windows10虚擬化技術。採取Hypervisor技術提供的虚擬化安全性(VBS)之

後,

可以將一些最具敏感性的Windows程序,移至安全的執行環境以避免遭到竄改,

即使發生Windows核心全面獾须的情況,也不必擔心。

在Windows 10中,VBS 可提供如裝置防護和機密防護等功能,

以有效防護惡意程式、駭客工具和漏洞。

```

### 8.2線上保護

```

SmartScreen篩選工具内建在Windows 、 Microsoft Edge 和 Internet Explorer 瀏覺器中的線上保護,保護免於恐意網站和下載威脅。

Windows電腦、手機和Xbox都使用這個隨時保持最新狀態的功能,當在線上時提供全年無休的頂級保讓,

不受網路釣魚和惡意程式碼威脅。

```

#### 8.3生物特徵辨識

```

Windows 10 具體進行革新

並提供 Microsoft Passport 和 Windows Hello 等功能。

這些企業級技術可提供與智慧卡類似的強大多因素驗證功能,且在指紋、臉部及虹膜生物特徴辨識技術的運用方面更具有彈性。

```

### 8.4遺失裝置的資料保護

```

Windows使用內建加密,將資料亂碼化,維護資料安全,藉以保護裝置。

如果裝置遺失或遭竊,資料變得更加安全,免於未經授權的存取:加密金鑰可讓使用者照常登入Windows 和使用檔案。

```

### 8.5裝置完整性

```

為抵擋惡意程式和駭客的攻擊,必須能夠維持硬體的完整性以及作業系統的開機程序。

在Windows8出現之前,的確是一項艱鉅的挑戰。

開機和 Rootkit 惡意程式會在系統展開任何防禦之前就侵入裝置,使得這些防禦措施無法順利運作。

Windows8認證或新型的裝置包含一種稱為「UEI安全開機」的新硬體元件,

無論是開機或關機狀態都能維持系統韌體和作業系統的完整性。

```

### 8.6加密處理

```

真實世界中無法完全杜絕安全性漏洞的發生,為了保護如加密金鑰和使用者身分識别等高敏感性資料,

需要一個能協助提供最高等級安全保證的硬體。

Windows使用受信任的平台模組(TPM)中的標準技術來產生這類資訊

,在與作業系統隔離的硬體式環境中執行作業。

```

### 8.7信賴平台模組新功能

```

1.金鑰儲存提供者(KSP)和 svcrypt支援橢圓曲線加密法(ECC)。

裝置健康情況證明

2.Microsoft Passport 支援

3.Device Guard 支援

4.Credential Guard 支援

```

## 9.補充

### 9.1機密分級

```

1. 不分類

2. 機密

3. 秘密

4. 最高機密

```

### 9.2作業系統更新

```

作業系統更新包含的新軟體可協助您的電腦保持在最新狀態。

更新的範例包括 ServicePack、版本升級、安全性更新、驅動程式,或其他類型的更新。

重要與高優先順序更新對於電腦的安全性和可靠性而言很重要。

它們提供最新的保護以抵抗惡意線上活動。

您必須更新所有程式,包括Windows 、 Internet Explorer Microsoft Office 以及其他程式等等。

請造訪Microsoft Update以掃描電腦並檢視更新清單,然后決定是否要下載與安裝更新。

```

### 9.3最小密碼長度

```

這項安全性設定決定使用者帳戶密碼可包含的最少字元數。

您可以設定介於1和14個字元之間的值,

或設定字元數為0,如此便不需要密碼。

預設值:

在網域控制站上為7。

在獨立伺服器上為0。

附註

1.預設成員電腦會遵循其網域控制站的設定。

2.藉由開啟適當的原則並展開主控台樹狀目錄,可以設定此安全性設定,

```

### 9.4憑證概觀

```

公開金鑰憑證(通常簡稱為憑證),它會將公開金鑰連結到有相應私密金鑰的使用者、裝置或服務的識別身分。

大部分常用的憑證是以 x.509v3憑證標準為基準。

憑證可用於多種功能,

如網頁使用者驗證、網頁伺服器驗證、安全電子郵件(使用安全多功能網際網路郵件擴充(S/MME))、

網際網路通訊協定安全性(IPSec)、傳輸階層安全性(TLS)及代碼簽署(code signing)。

各憑證授權單位(CA)間也可相互發行憑證,以建立憑證階層。

通常憑證包含下列資訊:

1.主體的公開金鑰值。

2,主體識別元資訊(如名稱及電子郵件位址)。

3,有效期間(憑證有效的時間長度)。

4.發行者識別元資訊。

5,使用發行者的數位簽章可驗證主體公開金鑰及主體識別元資訊之間連結的有效性。

```