TSC CAPITAL GROUP
The Bridge to the Asia Pacific Region

苗栗縣政府

苗栗縣政府109年資訊安全管理制度(ISMS)維運暨驗證服務案

課程名稱

資通系統防護需求分級原則與資通系統防護基準

實施日期：109年7月9日 2梯次

授課講師：德欣寰宇資安顧問 陳惠怡

- 現任：德欣寰宇 顧問部 資安顧問

相關證照：ISO 27001 LA、**ISO 29100 LA**、**BS 10012 (PIMS)**

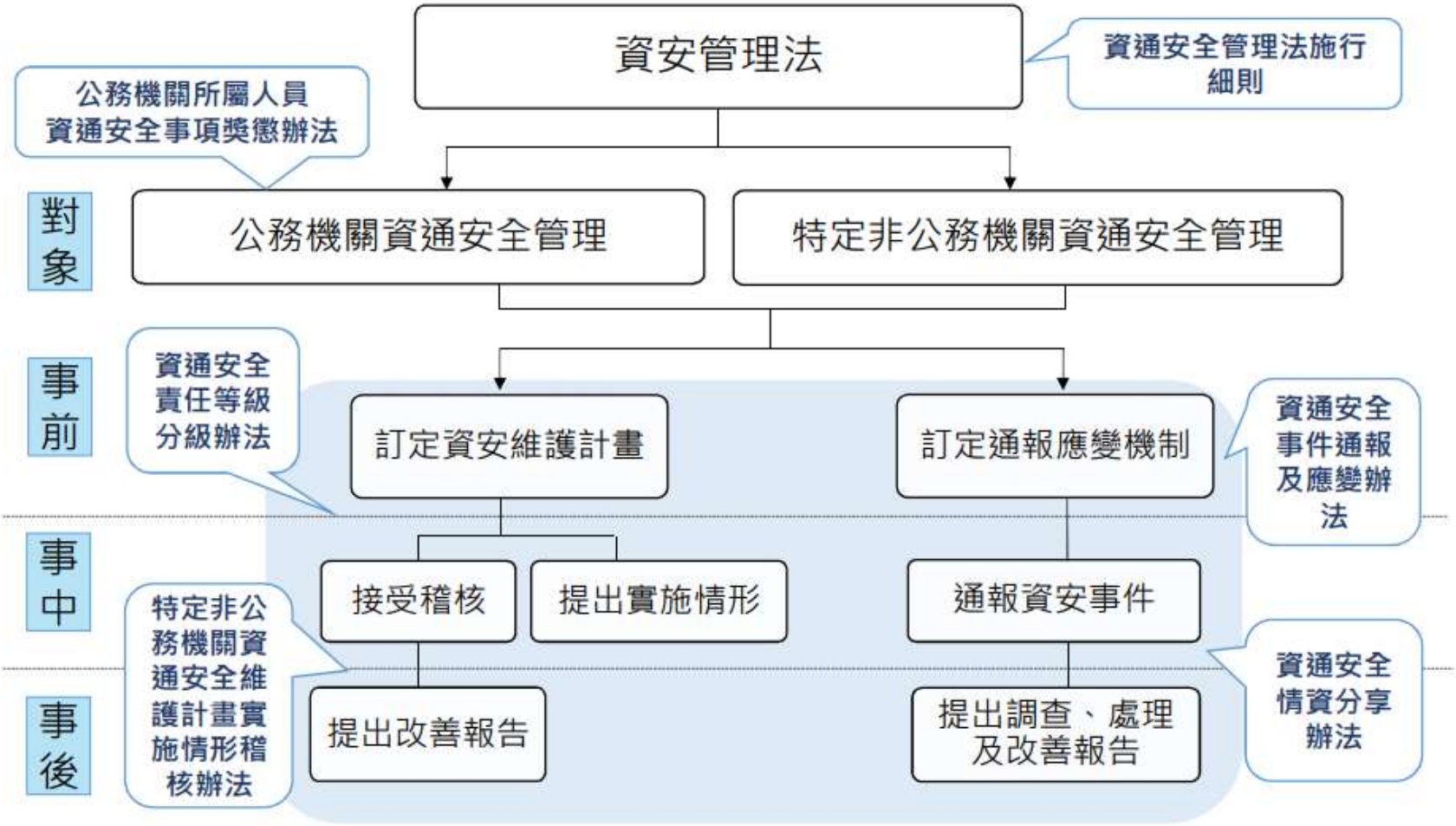
輔導經歷：

新竹縣政府、新竹市政府、苗栗縣政府、臺中市政府資訊中心、臺中市政府民政局、台灣自來水股份有限公司、臺灣港務股份有限公司、臺中市政府地政局、臺中市政府地方稅務局、臺中市政府警察局、國立台北藝術大學、財政部關務署臺中關、行政院原子能委員會核能研究所、衛福部食品藥物管理署

課程內容

1. 資通系統分級評估
2. 防護基準技術操作
3. 問題與討論

資通安全法整體架構



Source：行政院技術服務中心,"資通安全管理法簡介"

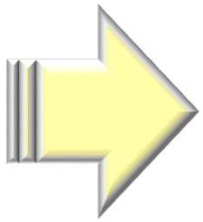
資通安全責任等級分級辦法

第11條

- 各機關自行或委外開發之資通系統應依附表九所定資通系統防護需求分級原則完成資通系統分級，並依附表十所定資通系統防護基準執行控制措施

資通安全責任等級分級辦法

資通系統防護需求分級



【高】等級防護措施

【中】等級防護措施

【普】等級防護措施

資通系統防護需求分級原則

附表九防護需求分級原則

防護需求等級依據該系統相關之機密性、完整性、可用性及法律遵循性四個構面中之最高者定之。

構面＼等級	普	中	高
機密性	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生有限之影響。	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生嚴重之影響。	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。

資通系統防護需求分級原則

附表九防護需求分級原則

構面 \ 等級	普	中	高
完整性	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生有限之影響。	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生嚴重之影響。	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響

資通系統防護需求分級原則

附表九防護需求分級原則

等級 / 構面	普	中	高
可用性	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生有限之影響	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生嚴重之影響	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響

資通系統防護需求分級原則

附表九防護需求分級原則

等級 / 構面	普	中	高
法律遵循性	其他資通系統設置或運作於法令有相關規範之情形。	如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統受影響而導致資通安全事件，或影響他人合法權益或機關執行業務之公正性及正當性，並使機關或其所屬人員受行政罰、懲戒或懲處。	如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統受影響而導致資通安全事件，或影響他人合法權益或機關執行業務之公正性及正當性，並使機關所屬人員負刑事責任。

課程內容

1. 資通系統分級評估
2. 防護基準
3. 問題與討論

資通系統防護需求分級原則

附表十 資通系統防護基準

構面	措施內容	控制措施
7	29	76

高	中	普
76	57	31

防護基準技術操作

行政院國家資通安全會報技術服務中心
National Center for Cyber Security Technology

https://www.nccst.nat.gov.tw/

防護基準技術操作

構面一、存取控制

防護基準技術操作

措施內容	系統防護需求分級		
	普	中	高
帳號管理	建立帳號管理機制，包含帳號之申請、開通、停用及刪除之程序	1.等級「普」之所有控制措施 2. 已逾期之臨時或緊急帳號應刪除或禁用 3.資通系統閒置帳號應禁用 4.定期審核資通系統帳號之建立、修改、啟用、禁用及刪除	1.等級「中」之所有控制措施 2.逾越機關所定預期閒置時間或可使用期限時，系統應自動將使用者登出 3.應依機關規定之情況及條件使用資通系統 4.監控資通系統帳號，如發現帳號違常使用時回報管理者

防護基準技術操作

帳號管理實作建議

- 控制措施(高)

  應依機關規定之情況及條件，使用資通系統。

- 說明

  –管理者介面通常可執行系統中較高權限的功能(例如權限與人員管理)，其相對風險較高，因此應盡可能不允許遠端存取，僅允許透過內部網路存取，以避免有心人士從外部嘗試攻擊之可能。若有必要允許外部遠端存取管理者介面，應限制特定存取來源IP，避免全面性開放存取。。

- 驗證方法

  –當使用者試圖遠端存取管理者介面時，取得來源IP資訊，驗證其合法性。

防護基準技術操作

JAVE實作範例

當使用者試圖遠端存取管理者介面時，取得來源 IP 資訊，驗證其合法性。

```
public static boolean isIpAllow(HttpServletRequest httpServletRequest) {
    String userIP = httpServletRequest.getRemoteAddr();//取得使用者 IP
    String allowedIP = Property.getString("all.ip.allow.reg");//取得允許列表
    //用正規表示式描述允許的 ip
    Pattern p = Pattern.compile(allowedIP);
    Matcher m = p.matcher(userIP);
    //ip 來源的檢查動作
    return m.matches( );
}
```

- Interface ServletRequest

  http://docs.oracle.com/javaee/6/api/javax/servlet/ServletRequest.html

防護基準技術操作

措施內容	系統防護需求分級		
	普	中	高
最小權限	無要求	採用最小權限原則，僅允許使用者(或代表使用者行為的程序)依據機關任務和業務功能，完成指派任務所需之授權存取	
遠端存取	對於每一種允許之遠端存取類型，均應先取得授權，建立使用限制、組態需求、連線需求及文件化，使用者之權限檢查作業應於伺服器端完成	1.等級「普」之所有控制措施 2.應監控資通系統遠端連線 3.資通系統應實作加密機制 4.資通系統遠端存取之來源應為機關已預先定義及管理之存取控制點	

防護基準技術操作

遠端存取實作建議

- 控制措施(普)

  對於每一種允許之遠端存取類型，均應先取得授權，建立使用限制、組態需求、連線需求及文件化， 使用者之權限檢查作業應於伺服器端完成

- 說明

  –系統應包含具有一致全面性、位於伺服器端，強制適用於全系統的授權及存取控制機制(如使用Filter過濾器)， 避免被攻擊者繞過檢查機制

- 驗證方法

  – 以測試案例驗證，如停用瀏覽器JavaScript功能後，以一般使用者帳號登入，試圖存取他人或管理者頁面之功能，系統應拒絕存取

防護基準技術操作

- 實作範例
  - 利用Java Servlet Filter

web.xml

```
<filter>
  <filter-name>auth</filter-name> <filter-
  class>filter.AuthFilter</filter-class>
</filter> <filter-mapping>
  <filter-name>auth</filter-name> <url-
  pattern>/*</url-pattern>
</filter-mapping>
<filter>
```

所有頁面存取都要檢查授權

  - ASP.NET URL 授權

web.config

```
<configuration>
  <system.web>
    <authorization>
      <allow roles="admin"/>
      <deny users="*"/>
    </authorization>
  </system.web>
</configuration>
```

只允許admin角色存取，其他使用者拒絕存取

防護基準技術操作

– 採用過濾器(Filter)機制， 先檢查是否通過身分驗證，再檢查是否具有存取網頁或功能的權限

```
public class AccCtrlFilter implements Filter {
  public void doFilter(ServletRequest request, ServletResponse response,
      FilterChain chain) throws IOException, ServletException {
    HttpServletRequest req = (HttpServletRequest) request;
    HttpServletResponse res = (HttpServletResponse) response;
    HttpSession session = req.getSession();
    req.setCharacterEncoding("UTF-8");
    res.setCharacterEncoding("UTF-8");
    String user_id = (String) session.getAttribute("id");
    Map priv = (Map) session.getAttribute("priv");
    if (user_id == null || priv == null) {
      res.sendRedirect(req.getContextPath()+"/Login.jsp");
      return;
    }
    String uri = req.getRequestURI();
    if (priv.containsKey(uri)) {
      chain.doFilter(request, response);
    }else{
      res.sendRedirect(req.getContextPath()+"/Error.jsp");
      return;
    }
  }
```

不具權限則重導至錯誤訊息頁面

防護基準技術操作

構面二、稽核與可歸責性

防護基準技術操作

措施內容	系統防護需求分級		
	普	中	高
稽核事件	1.依規定時間週期及紀錄留存政策保留稽核紀錄 2.確保資通系統有稽核特定事件之功能，並決定應稽核之特定資通系統事件 3.應稽核資通系統管理者帳號所執行之各項功能	1.等級「普」之所有控制措施 2.應定期審查稽核事件	
稽核紀錄內容	資通系統產生之稽核紀錄應包含事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別等資訊，並採用單一日誌紀錄機制，確保輸出格式之一致性	1.等級「普」之所有控制措施 2.資通系統產生的稽核紀錄，應依需求納入額外的資訊	

防護基準技術操作

稽核事件實作建議(1/2)

- 控制措施(普)
  - 確保資通系統有稽核特定事件之功能，並決定應稽核之特定資通系統事件
- 說明
  - 留存日誌紀錄之目的如程式除錯、行為歸責、稽核取證及法規要求等
  - 稽核特定事件如身分驗證失敗、存取資源失敗、重要行為、重要資料異動，及功能錯誤等
- 驗證方法
  - 觸發特定事件以產生相關Log紀錄

防護基準技術操作

稽核事件實作建議(2/2)

- 控制措施(普)

  –應稽核資通系統管理者帳號所執行之各項功能

- 說明

  –稽核管理者行為，將有助於定期稽核系統行為及資安事件追查

- 驗證方法

  – 使用管理者帳號操作系統以產生相關Log紀錄

防護基準技術操作

稽核紀錄內容實作建議

- 控制措施(普)
  - 資通系統產生之稽核紀錄應包含事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別等資訊，並採用單一日誌紀錄機制，確保輸出格式之一致性
- 說明
  - ID紀錄不可為個資類型(如身分證號)
  - 採用單一的Log機制有助於事件追蹤
- 驗證方法
  - 檢視特定事件或管理者行為之Log紀錄，應包含關鍵資訊並具備一致格式

防護基準技術操作

措施內容	系統防護需求分級		
	普	中	高
稽核儲存容量	依據稽核紀錄儲存需求，配置稽核紀錄所需之儲存容量		
稽核處理失效之回應	資通系統應在稽核處理失效時，應採取適當之行動		1.等級「中」及「普」之所有控制措施 2.機關規定需要即時通報之稽核失效事件發生時，資通系統應於機關規定之時效內，對特定人員提出警告

防護基準技術操作

稽核處理失效回應實作建議

- 控制措施(普)
  - –資通系統於稽核處理失效時，應採取適當之行動
- 說明
  - –當稽核處理失效時應有適當對應行動，如關閉系統、覆寫最舊的稽核紀錄或停止產生稽核紀錄等，並可即時通知系統管理員以進行異常排除)
- 驗證方法
  - –以測試案例驗證，如停用稽核資料庫讓稽核資料無法寫入，檢視系統是否正常運作或是通知機制是否生效

防護基準技術操作

措施內容	系統防護需求分級		
	普	中	高
時戳及校時	資通系統應使用系統內部時鐘產生稽核紀錄所需時戳，並可以對應到世界協調時間(UTC)或格林威治標準時間(GMT)	1.等級「普」之所有控制措施 2.系統內部時鐘應依機關規定之時間週期與基準時間源進行同步	
稽核資訊之保護	對稽核紀錄之存取管理僅限於有權限之使用者	1.等級「普」之所有控制措施 2.應運用雜湊或其他適當方式之完整性確保機制	1.等級「中」之所有控制措施 2.定期備份稽核紀錄到與原稽核系統不同之實體

防護基準技術操作

稽核資訊之保護實作建議

- 控制措施(普)
  - –對稽核紀錄之存取管理，僅限於有權限之使用者
- 說明
  - –應定時將日誌紀錄進行遠端備份，並將檔案設定存取權限限制，避免未經授權存取
- 實作方式
  - –儲存於本地端目錄內的日誌紀錄，可將目錄壓縮後傳送至其他主機進行異地備份。若是日誌紀錄存放於資料庫內，則可以將資料庫進行備份。而若是存放於syslog server，則應避免syslog訊息能從網路網路存取。

防護基準技術操作

構面三、營運持續計畫

防護基準技術操作

措施內容	系統防護需求分級		
	普	中	高
系統備份	1.訂定系統可容忍資料損失之時間要求 2.執行系統源碼與資料備份	1.等級「普」之所有控制措施。 2.應定期測試備份資訊以驗證備份媒體之可靠性及資訊之完整性	1.等級「中」之所有控制措施。 2.應將備份還原，做為營運持續計畫測試之一部分 3.應在與運作系統不同處之獨立設施或防火櫃中，儲存重要資通系統軟體與其他安全相關資訊之備份
系統備援	無要求	1.訂定資通系統從中斷後至重新恢復服務之可容忍時間要求 2.原服務中斷時，於可容忍時間內，由備援設備取代提供服務	

防護基準技術操作

構面四、識別與鑑別

防護基準技術操作

措施內容	系統防護需求分級		
	普	中	高
內部使用者之識別與鑑別	資通系統應具備唯一識別及鑑別機關使用者(或代表機關使用者行為之程序)之功能，禁止使用共用帳號		1.等級等級「中」及「普」之所有控制措施 2.對帳號之網路或本機存取採取多重認證技術
鑑別資訊回饋	資通系統應遮蔽鑑別過程中之資訊		
加密模組鑑別	無要求	資通系統如以密碼進行鑑別時，該密碼應加密或經雜湊處理後儲存	
非內部使用者之識別與鑑別	資通系統應識別及鑑別非機關使用者(或代表機關使用者行為的程序)		

防護基準技術操作

鑑別資訊回饋實作建議

- 控制措施(普)
  - –資通系統應遮蔽鑑別過程中之資訊。
- 說明
  - –應遮蔽在鑑別過程中之資訊(如密碼)，以防止未授權之使用者可能之窺探/使用
- 驗證方法
  - –使用者在輸入密碼欄位輸入密碼時，不顯示內容。

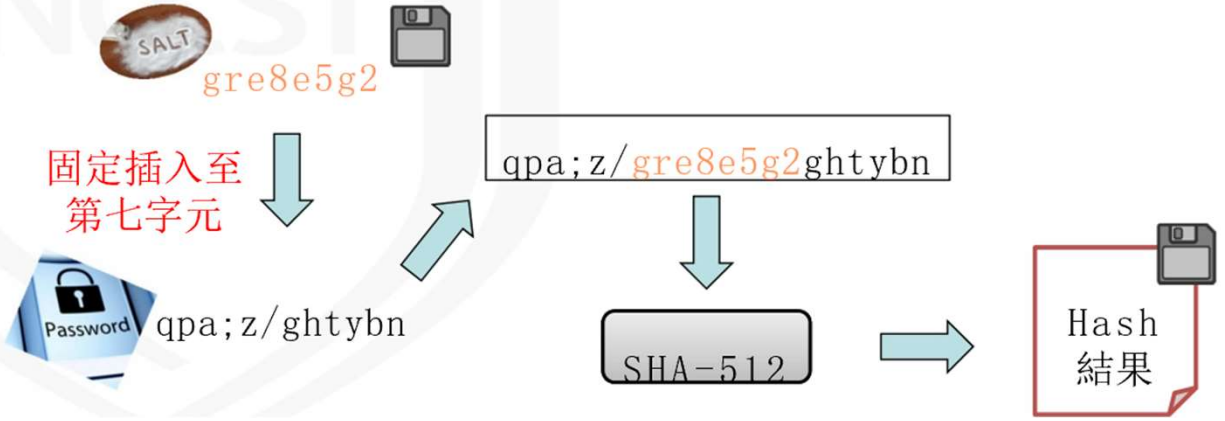
防護基準技術操作

加密模組鑑別實作建議

- 控制措施(中、高)
  - 資通系統如以密碼進行鑑別時，該密碼應加密或經雜湊處理後儲存。
- 說明
  - 避免駭客利用其他弱點取得資料庫或儲存媒體中的密碼
  - 明文密碼儲存或簡易的密碼hash皆不安全
- 驗證方法
  - 密碼添加亂數(Salt)進行雜湊函式(HASH Function)處理後，分別儲存亂數及雜湊後密碼

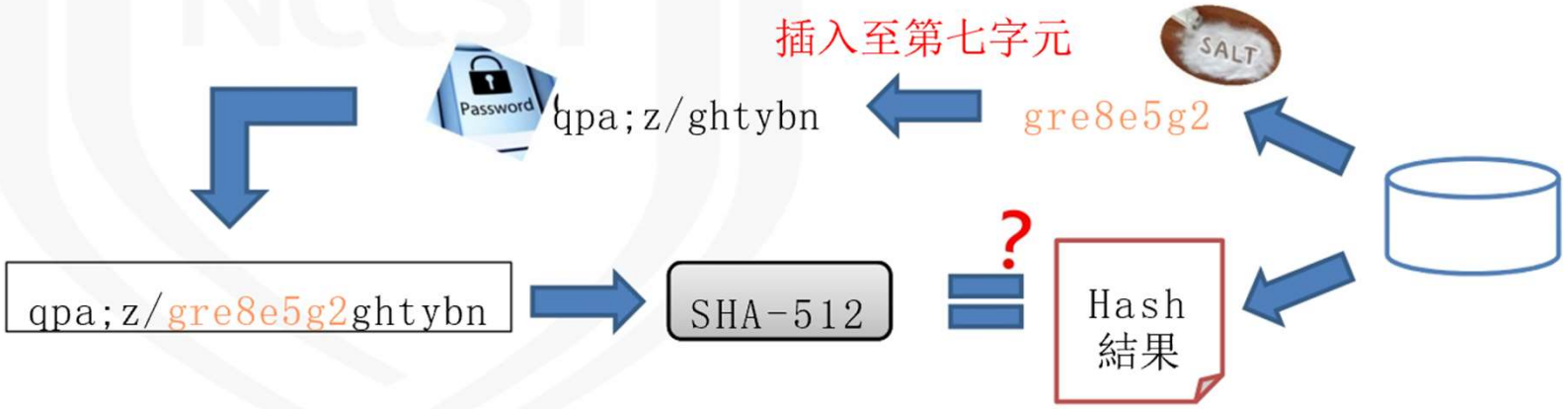
防護基準技術操作

- Password Hashing (Secure Salted)
  - 加鹽 (Salted)：
    - 初次設定
      1. 產生唯一且亂數的salt (EX: Java UUID)
      2. 將 salt 插入 password 的特定位置，產生新字串
      3. 使用雜湊演算法，例如SHA-512，對新字串進行Hash
      4. 分別儲存Salt 以及Hash結果



防護基準技術操作

- 比對密碼
  1. 取出salt 以及Hash結果
  2. 將salt 和使用者輸入的password 進行與初次設定相同的加鹽與Hash 動作
  3. 比對本次的Hash結果是否與取出之Hash結果相同



防護基準技術操作

措施內容	系統防護需求分級		
	普	中	高
身分驗證管理	1.使用預設密碼登入系統時，應於登入後要求立即變更 2.身分驗證相關資訊不以明文傳輸 3.具備帳戶鎖定機制，帳號登入進行身分驗證失敗達3次後，至少15分鐘內不允許該帳號繼續嘗試登入或使用機關自建之失敗驗證機制 4.基於密碼之鑑別資通系統應強制最低密碼複雜度；強制密碼最短及最長之效期限制 5.使用者更換密碼時，至少不可以與前三次使用過之密碼相同 6.第四點及第五點所定措施，對非內部使用者，可依機關自行規範辦理	1.等級等級「普」之所有控制措施 2.身分驗證機制應防範自動化程式之登入或密碼更換嘗試 3.密碼重設機制對使用者重新身分確認後，發送一次性及具有時效性符記	

防護基準技術操作

身分驗證管理實作建議(1/4)

- 控制措施(普)
  - 具備帳戶鎖定機制，帳號登入進行身分驗證失敗達3次後，至少15分鐘內不允許該帳號繼續嘗試登入或使用機關自建之失敗驗證機制
- 說明
  - 帳戶鎖定機制可延長駭客破解密碼所需花費的時間，避免駭客使用自動化工具進行攻擊
- 驗證方法
  - 以測試案例驗證，使用錯誤密碼嘗試登入3次後，在15分鐘內以正確的密碼嘗試登入，驗證無法登入成功即代表帳戶已鎖定

防護基準技術操作

身分驗證管理實作建議(2/4)

- 控制措施(普)
  - –基於密碼之鑑別資通系統應強制最低密碼複雜度
  - –強制密碼最短及最長之效期限制
- 說明
  - –規定密碼長度最小值與元素組成要求，目的在產生足夠數量之密碼組合，以延長破解所需時間
  - –依機關需求規定密碼效期，如最短效期1日，最長效期90日
- 驗證方法
  - –嘗試設定成弱強度密碼，系統應拒絕設定
  - –當變更密碼成功後，該密碼至少需使用1日後才能再次變更
  - –密碼使用超過90日後，必須再次變更密碼才能操作系統

防護基準技術操作

- 實作範例
  - .NET App_Start/IdentityConfig.cs

```
// 設定密碼的驗證邏輯
manager.PasswordValidator = new PasswordValidator
{
    RequiredLength = 12,
    RequireNonLetterOrDigit = false,
    RequireDigit = true,
    RequireLowercase = true,
    RequireUppercase = true,
};
```

密碼長度
特殊字元
數字
小寫字母
大寫字母

  - 使用正規表示式驗證密碼複雜度

    長度至少12，至少包含一個大寫，一個小寫，一個數字

    Java範例 ^.*(?=.{12,})(?=.*[a-z])(?=.*[A-Z])(?=.*[0-9]).*$

長度大於12
(?=.{12,})
至少包含一個英文小寫
(?=.*[a-z])
至少包含一個英文大寫
(?=.*[A-Z])

至少包含一個數字
(?=.*[0-9])
至少包含一個特殊字元
(?=.*[!@#$%A&*()\-_=+[\]\{}I;I:'",./<>?-·])

防護基準技術操作

身分驗證管理實作建議(3/4)

- 控制措施(中、高)
  - –身分驗證機制應防範自動化程式之登入或密碼更換嘗試
- 說明
  - –全自動區分電腦和人類的圖靈測試(Completely Automated Public Turing test to tell Computers and Humans Apart, CAPTCHA)，俗稱驗證碼
- 驗證方法
  - –輸入錯誤或空白驗證碼，系統應拒絕登入

防護基準技術操作

–使用免費的reCAPTCHA widget

```
<html>
  <head>
    <title>reCAPTCHA demo: Explicit render after an onload callback</title>
    <script type="text/javascript">
      var onloadCallback = function() {
        grecaptcha.render('html_element', {
          'sitekey' : 'your_site_key'
        });
      };
    </script>
  </head>
  <body>
    <form action="?" method="POST">
      <div id="html_element"></div>
      <br>
      <input type="submit" value="Submit">
    </form>
    <script src="https://www.google.com/recaptcha/api.js?onload=onloadCallback&render=explicit"
        async defer>
    </script>
  </body>
</html>
```

防護基準技術操作

身分驗證管理實作建議(4/4)

- 控制措施(中、高)
  - –密碼重設機制對使用者重新身分確認後，發送一次性及具有時效性符記
- 說明
  - –系統產生具有時效性之URL連結，發送至該信箱
  - –使用者登入信箱並點選該URL連結後，即可使用重設密碼功能頁面
- 驗證方法
  - –點選忘記密碼，檢視是否收到Email，並於時效內進行密碼重設

防護基準技術操作

- 實作範例

```
public class GenToken extends HttpServlet {
    protected void doGet(HttpServletRequest request,
            HttpServletResponse response)
            throws ServletException, IOException {
        doPost(request, response);
    }
    protected void doPost(HttpServletRequest request,
            HttpServletResponse response)
            throws ServletException, IOException {
        String account = request.getParameter("account");
        String email = request.getParameter("email");

        try {
            String token = UUID.randomUUID().toString();
            Timestamp t = new Timestamp(System.currentTimeMillis());

            if( userIsExist(account, email) ){
                setToken(account, email, token, t);
                //請記得改為Eamil方式寄送連結
                PrintWriter out = response.getWriter();
                out.println("<a href='CheckToken?token=" +
                    token + "'>reset link</a>");
            }
        } catch (Exception e) {
            e.printStackTrace();
        }
    }
```

產生亂數token

確認帳號存在，則將密碼重設功能之連結寄送至原留存信箱

防護基準技術操作

構面五、系統與服務獲得

防護基準技術操作

措施內容	系統防護需求分級		
	普	中	高
系統發展生命週期需求階段	針對系統安全需求(含機密性、可用性、完整性)，以檢核表方式進行確認		
系統發展生命週期設計階段	無要求	1.根據系統功能與要求，識別可能影響系統之威脅，進行風險分析與評估 2.將風險評估結果回饋需求階段的檢核項目，並提出安全需求修正	
系統發展生命週期開發階段	1.應針對安全需求實作必要控制措施 2.應注意避免軟體常見漏洞及實作必要控制措施 3.發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細之錯誤訊息		1.等級「中」及「普」之所有控制措施 2.執行「源碼掃描」安全檢測 3.具備系統嚴重錯誤之通知機制

防護基準技術操作

系統發展生命週期開發階段實作建議(1/2)

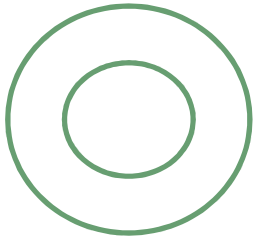
- 控制措施(普)
  - –應注意避免軟體常見漏洞及實作必要控制措施
- 說明
  - –常見漏洞如OWASP Top 10:2017
- 驗證方法
  - –弱點掃描
  - –滲透測試

防護基準技術操作

系統發展生命週期開發階段實作建議(2/2)

- 控制措施(中)
  - –發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細之錯誤訊息
- 說明
  - –避免駭客根據錯誤訊息刺探系統資訊或弱點
  - –可於伺服器設定檔設定特定錯誤頁面
- 驗證方法
  - –嘗試產生錯誤操作，檢視頁面所呈現之訊息，如存取不存在的網址、輸入錯誤數值等

防護基準技術操作



防護基準技術操作

措施內容	系統防護需求分級		
	普	中	高
系統發展生命週期測試階段	執行「弱點掃描」安全檢測		1.等級「中」及「普」之所有控制措施 2.執行「滲透測試」安全檢測
系統發展生命週期部署與維運階段	1.於部署環境中應針對相關資通安全威脅，進行更新與修補，並關閉不必要服務及埠口 2.資通系統相關軟體，不使用預設密碼	1.等級「普」之所有控制措施 2.於系統發展生命週期之維運階段，須注意版本控制與變更管理	

防護基準技術操作

措施內容	系統防護需求分級		
	普	中	高
系統發展生命週期委外階段	資通系統開發如委外辦理，應將系統發展生命週期各階段依等級將安全需求（含機密性、可用性、完整性）納入委外契約		
獲得程序	無要求	開發、測試以及正式作業環境應為區隔	
系統文件	應儲存與管理系統發展生命週期之相關文件		

防護基準技術操作

構面六、系統與通訊保護

防護基準技術操作

措施內容	系統防護需求分級		
	普	中	高
傳輸之機密性與完整性	無要求	無要求	1.資通系統應採用加密機制，以防止未授權之資訊揭露或偵測資訊之變更但傳輸過程中有替代之實體保護措施者，不在此限 2.使用公開、國際機構驗證且未遭破解的演算法 3.支援演算法的最大長度金鑰 4.加密金鑰或憑證週期性更換 5.伺服器端之金鑰保管應製定管理規則及實施應有之安全防護措施
資料儲存之安全	無要求	無要求	靜置資訊及相關具保護需求之機密資訊應加密儲存

防護基準技術操作

傳輸之機密性與完整性實作建議

- 控制措施(高)
  - –使用公開、國際機構驗證且未遭破解之演算法
  - – 支援演算法最大長度金鑰
- 說明
  - –採用加密傳輸保護機敏資訊
  - –避免採用不安全的協定如SSL及TLS1.0版本
  - –避免採用已被破解的演算法如SHA-1
- 驗證方法
  - –可使用nmap工具，測試站台的加密協定及演算法

防護基準技術操作

nmap --script ssl-cert,ssl-enum-ciphers -p 埠號 站台位址

```
C:\Users\wisely>nmap --script ssl-cert,ssl-enum-ciphers -p 443 www.[redacted].gov.tw

Starting Nmap 7.50 ( https://nmap.org ) at 2017-06-14 16:41 ¥×¥_?D·CRE?!
Nmap scan report for [redacted]
Host is up (0.032s latency).
PORT    STATE SERVICE
443/tcp open  https
| ssl-cert: Subject: commonName=www.[redacted].gov.tw/organizationName=\xE8\xAI\x8C\x
| Subject Alternative Name: DNS:www[redacted].gov.tw
| Issuer: organizationName=[redacted]countryName=TW
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2016-12-28T05:52:16
| Not valid after:  2019-12-28T05:52:16
| MD5:   9ef4 9519 f3b2 b742 1360 3117 4a68 8c08
|_SHA-1: 4c84 cd73 7276 f7ce 599c 5f2c fa30 a56d 65aa 503f
| ssl-enum-ciphers:
|   TLSv1.0:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|     compressors:
|       NULL
|     cipher preference: server
|   TLSv1.1:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|     compressors:
|       NULL
|     cipher preference: server
|_  least strength: A
```

檢測結果顯示，站台仍有使用安全性不足之TLS1.0協定

防護基準技術操作

- 實作範例
  - 調整伺服器設定檔，指定傳輸加密協定及演算法
  - Apache Tomcat設定檔範例：

```
<Connector
protocol="org.apache.coyote.http11.Http11NioProtocol"
port="443" maxThreads="200“
scheme="https" secure="true" SSLEnabled="true"
keystoreFile="%HOME%/.keystore" keystorePass="changeit"
sslProtocol="TLSv1.2" sslEnabledProtocols="TLSv1.1,TLSv1.2"
clientAuth="false“
ciphers=“TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,
        TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,
        TLS_RSA_WITH_AES_256_CBC_SHA,
        TLS_RSA_WITH_AES_128_CBC_SHA”/>
```

指定加密協定

指定演算法

防護基準技術操作

資料儲存之安全實作建議

- 控制措施(高)

  –靜置資訊及相關具保護需求之機密資訊應加密儲存

- 說明

  –靜置資訊指資訊位於資訊系統特定元件，如儲存設備上之狀態。與系統相關需要保護的資訊，例如：資訊系統組態設定。

- 驗證方法

  –參數設定或系統設定存放處，限制存取或進行適當保護

防護基準技術操作

構面七、系統與資訊完整性

防護基準技術操作

措施內容	系統防護需求分級		
	普	中	高
漏洞修復	系統之漏洞修復應測試有效性及潛在影響，並定期更新	1.等級「普」之所有控制措施。 2.定期確認資通系統相關漏洞修復之狀態	
資通系統監控	發現資通系統有被入侵跡象時，應通報機關特定人員	1.等級「普」之所有控制措施 2.監控資通系統，以偵測攻擊和未授權之連線，並識別資通系統之未授權使用	1.等級「中」之所有控制措施 2.資通系統應採用自動化工具監控進出之通信流量，並於發現不尋常或未授權之活動時針對該事件進行分析

防護基準技術操作

措施內容	系統防護需求分級		
	普	中	高
軟體及資訊完整性	無要求	1.使用完整性驗證工具，以偵測未授權變更特定軟體及資訊 2.使用者輸入資料合法性檢查應置放於應用系統伺服器端 3.發現違反完整性時，資通系統應實施機關指定之安全保護措施	1.等級「中」之所有控制措施 2.應定期執行軟體和資訊完整性檢查

防護基準技術操作

軟體及資訊完整性實作建議

- 控制措施(中)
  - –使用者輸入資料合法性檢查應置放於應用系統伺服器端
- 說明
  - –於伺服器端以正規表示式(Regular Expression)方式，檢查使用者輸入資料合法性。
- 驗證方法
  - –對於使用者輸入欄位資料，採用正規表示式進行檢查，僅允許輸入特定白名單內容，檢查其邏輯規則是否合法

課程內容

1. 資通系統分級評估
2. 防護基準技術操作
3. 問題與討論