經濟部電子資料遭竊事故處理作業程序

中華民國101年2月15日經資字第10104881030號函頒

壹、 目的：

經濟部（以下簡稱本部）為處理駭客入侵導致電子資料遭竊事故之作業程序標準化，以提升本類事故處理速度、保存事故相關資訊及強化本部資訊安全，特訂定本作業程序（以下簡稱本作業處理程序）。

貳、適用對象及時機：

一、適用對象：本部部次長室暨所屬幕僚單位（不含中部辦公室、中區聯合服務中心及南區聯合服務中心）。

二、適用時機：本部因駭客入侵導致電子資料遭竊時，依本作業處理程序辦理。

參、作業程序：

一、於本部資訊安全監控中心（以下簡稱監控中心）處理資訊安全事件且發現有資料遭竊跡象時，依下列程序處理：

（一）資安通報作業

依「經濟部資通安全事件緊急應變計畫暨作業處理程序」（附件一）陳報並於「國家資通安全通報應變網站」進行通報作業。

（二）事故處理作業

依設備類別（個人電腦或主機），進行以下處理作業。

1. 個人電腦

1.1 取得使用者電腦

將該部電腦取回資訊中心，以盡量保持其原始狀態之完整性，俾利後續調查處理作業。

1.2 電腦硬碟映像檔製作

取回之個人電腦硬碟由監控中心作業人員進行一對一(Bit-Stream)完全複製(一式三份)，一份作為事故調查用；一份作為歸還使用者備份資料用；另一份留存備用。

1.3 原始電腦硬碟封存

原始電腦硬碟以公文袋封存，標示後置於資訊中心機房防火保險櫃內（標示格式如附件二）。

1.4 電腦歸還使用者

將其中一份複製硬碟中的惡意程式清除後，安裝回使用者電腦，歸還使用者，並請使用者變更相關帳號之密碼。

1.5 電腦使用者備份資料

使用者將屬於個人的公私務資料部分進行備份作業。

1.6 電腦重新安裝

為確保使用者電腦環境之安全，俟電腦使用者備份作業完成後，再由資訊中心進行電腦重新安裝作業。

2. 主機

2.1 主機映像檔製作及封存

(1)如屬虛擬主機，則由監控中心作業人員直接複製該虛擬主機檔案二份。

(2)如屬實體主機，則由監控中心作業人員針對本機硬碟部分進行一對一（Bit-Stream）完全複製（一式二份）。

(3)複製品一份作為事故調查用；另一份封存備用。

2.2 清除惡意程式

清除主機上之惡意程式，以防駭客續以利用。

（三）事故調查作業

1. 監控中心針對複製品進行調查分析作業，檢查使用者電腦登入紀錄痕跡、系統機碼、文件開啟痕跡、USB 使用痕跡、上網痕跡、E-mail 痕跡、軟體使用痕跡、記憶體等項目，並進行發生時間、惡意程式、惡意網路連線關係、運用手法及運用系統漏洞等整體分析作業。

2. 於調查當時發現可立即進行之損害管控動作，資訊中心得先進行處理，如當下發現惡意程式連往之駭客中繼站位置，立即於安全設備上進行連線阻擋，或停用遭利用之帳號等，以降低損害。

（四）遭竊資料列表

疑似遭竊之資料檔由資訊中心進行檔名列表作業，以供資料所屬單位進行損害評估及管控之用。

（五）產出事故調查結果報告

監控中心進行事故調查暨處理作業後，產出「經濟部資通安全事故調查結果報告」(格式如附件三，不含「資料檔案檔名列表」部分)。

（六）資料整併及提供

1. 將前開之事故調查結果報告與檔名列表資料，合併成完整報告。
2. 將報告中之「資料檔案檔名列表」部分提供資料所屬單位進行損害評估及管控作業。

（七）損害評估管控及通報作業

1. 資料所屬單位針對遭竊資料進行損害評估及後續之損害管控作業。
2. 資料所屬單位須填具「經濟部遭竊電子資料機敏等級評估單」(附件四）回報資訊中心。
3. 如遭竊資料內含機敏資訊，資料所屬單位須向政風處通報。

（八）陳報及資安通報結案作業

1. 遭竊資料如內含機敏資訊，資訊中心須依「經濟部資通安全事件緊急應變計畫暨作業處理程序」向本部資通安全處理小組召集人（資訊安全長）陳報。
2. 依前述程序於「國家資通安全通報應變網站」進行資訊作業面之結案作業。
3. 封存之硬碟併同完整報告以密件公文歸檔專用資料袋封存，標示後置於資訊中心機房防火保險櫃內。（標示格式如附件二）

（九）災害復原作業（主機）

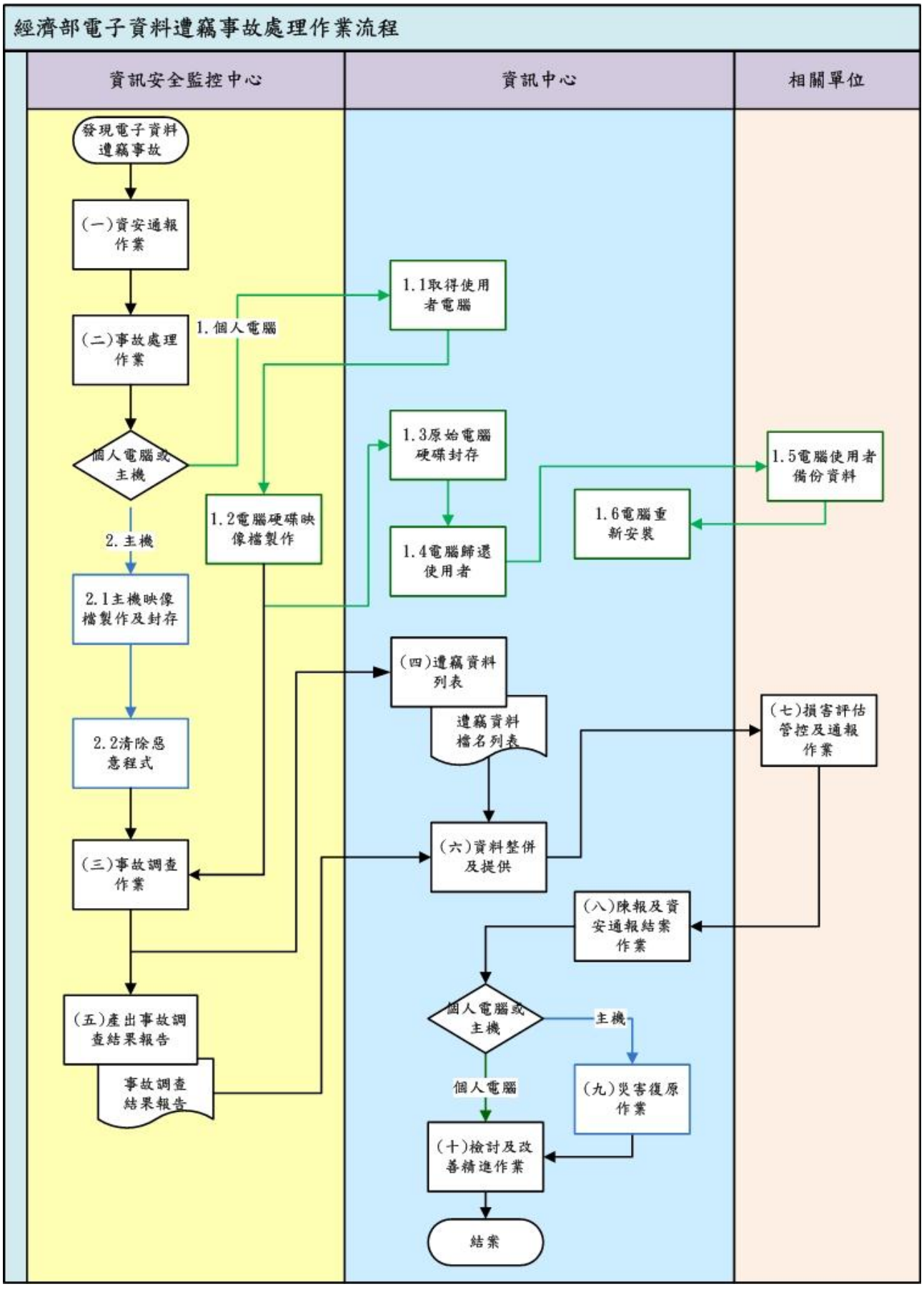
應變更該主機及系統相關使用之帳號及密碼，並依主機及系統復原程序進行災害復原作業。

（十）檢討及改善精進作業

檢討遭入侵原因後，進行後續改善精進作業。

二、封存之證物，於資安通報結案作業完成日二年後銷毀，調查結果報告循公文程序歸檔。

肆、經濟部電子資料遭竊事故處理作業流程如附圖。


經濟部電子資料遭竊事故處理作業流程
資訊安全監控中心
資訊中心
相關單位
發現電子資料遭竊事故
(一)資安通報作業
(二)事故處理作業
個人電腦或主機
1.個人電腦
2.主機
1.1取得使用者電腦
1.2電腦硬碟映像檔製作
1.3原始電腦硬碟封存
1.4電腦歸還使用者
1.5電腦使用者備份資料
1.6電腦重新安裝
2.1主機映像檔製作及封存
2.2清除惡意程式
(三)事故調查作業
(四)遭竊資料列表
遭竊資料檔名列表
(五)產出事故調查結果報告
事故調查結果報告
(六)資料整併及提供
(七)損害評估管控及通報作業
(八)陳報及資安通報結案作業
個人電腦或主機
主機
個人電腦
(九)災害復原作業
(十)檢討及改善精進作業
結案

附件二

經濟部電子資料遭竊事故證物/調查結果報告封存封

事故編號	（同「經濟部資通安全事故調查結果報告」）
封存內容及數量	
封存日期	年　　月　　日
設備使用者	**單位：** **姓名：**
封存人員	
資安通報單 ID	（國家資通安全通報應變作業發配之編號）
資安通報結案日期	年　　月　　日
※封存內容於通報結案作業完成日 2 年後銷毀	

附件三　　**經濟部資通安全事故調查結果報告**

事故說明	
事故編號	(MOEA-AIR-西元年-流水號3碼，流水號每年由001開始累計，AIR：Accident investigation report)
事故發現日期	年　　月　　日　　時　　分
作業人員	
事故描述	
通報單ID	（國家資通安全通報應變作業發配之編號，無則免填）
通報作業日期	通報日期：　　年　　月　　日 通報結案日期：　　年　　月　　日
設備及證物(硬碟)資訊	
設備IP	
設備使用者	
設備Patch狀態	
防毒軟體版本	
證物廠牌	（未保留證物則不需要）
證物型號	（未保留證物則不需要）
證物容量	（未保留證物則不需要）
證物外觀	（證物照片，未保留證物則不需要）
調查暨處理過程描述	
使用工具	調查時使用之軟硬體工具
檢查項目	使用者登入紀錄痕跡、系統機碼分析、文件開啟痕跡、USB使用痕跡、上網痕跡、E-mail痕跡、WebMail痕跡、IM聊天痕跡、軟體使用痕跡、記憶體分析、關鍵字搜尋等
發現狀況說明	遭植入惡意程式、有被打包資料殘留等
疑有資料遭竊	□是　□否
事故原因及手法分析	發生時間分布圖、惡意網路連線關係圖、運用手法及運用系統漏洞等

經濟部資通安全事故調查結果報告

處理作業說明	停用網路服務、清除惡意程式等
惡意程式或工具分析	
檔名	
存在路徑	
建立日期	
修改日期	
存取日期	
擁有者	
檔案大小(Bytes)	
MD5	
防毒軟體掃描結果	
行為描述	
檢討及建議事項	

資料檔案檔名列表

序號	檔名	檔案大小(Bytes)	建立日期	修改日期	擁有者

附件四

經濟部遭竊電子資料機敏等級評估單

※以下由「資訊中心」填列	
事故編號	
事故發現時間	年　　月　　日
※以下由「資料所屬單位」填列	
填列日期	年　　月　　日
遭竊資料 最高機敏等級	□絕對機密等級公務資料（4級） □極機密等級公務資料（4級） □機密等級公務資料（4級） □密等級公務資料（3級） □敏感等級公務資料（3級） □非屬密級以上或敏感之核心業務資料（2級） □非核心業務資料（1級）
是否已通報政風處	□是　□否
填報人員： 填報人員主管： 填報單位主管：	
本評估單請於資料送達後2日內回擲資訊中心	