出國報告（出國類別：參加國際會議）

出席「第十屆倫敦行動計畫(LAP；London Action Plan)」年度會議報告

服務機關：國家通訊傳播委員會

姓名職稱：吳簡任技正銘仁、陳專員俊瑋、林技士湛翔

派赴國家：日本東京

出國期間：2014 年 10 月 5 日至 10 月 10 日

報告日期：2014 年 12 月

摘要

本屆「倫敦行動計畫」年度會議於 10 月 7 日至 9 日為期 3 天在日本東京舉行，日方為加強臺日防制垃圾郵件國際合作，邀請我方於出席該年度會議前一日(10 月 6 日)共同召開「臺日防制垃圾郵件雙邊交流會議」，就臺日雙方有關垃圾郵件法案、防制系統技術與強化合作機制進行交流，並於會後受邀至位於東京巢鴨的「日本數據通信協會(JADAC；Japan Data Communications Association)」參訪，日本防制垃圾郵件諮詢中心主任西松薰親自解說並示範日方處理垃圾郵件之流程及步驟。

早期的網路環境單純，在當時並沒有「垃圾郵件」的概念，因此電子郵件的通訊協定 SMTP 缺乏必要的通訊認證機制，由於電子郵件成本低廉、快速、便捷的特性，很容易的被有心人士利用來大量濫發商業廣告，造成網路用戶權益受損，同時垃圾郵件廣告提供的商品或服務品質堪慮，通常誇大不實，容易造成消費權益受損而求償無門；由於網路科技的發達，各種創新應用不斷的推陳出新、蓬勃發展，現代人的生活早已離不開網際網路，網路成為商機無限的兵家必爭之地，由於商機所帶來的龐大利益，加上網路應用無孔不入的便利性，也成為駭客獲取不法利益的管道，駭客們利用電子郵件、垃圾簡訊等方式，誘騙網路用戶點選所提供的惡意連結，有可能連結到釣魚網站誘騙網路用戶提供個資，或藉機植入惡意軟體竊取敏感個資、癱瘓主機、進行社交工程詐騙、或綁架主機成為殭屍電腦，成為殭屍電腦的主機亦可被利用來大量濫發惡意郵件繼續擴散感染等，因此「垃圾郵件」和「垃圾簡訊」不再僅只傳統上帶來困擾的大量商業廣告，也成了惡意軟體散播的媒介，根據今年度(2014)趨勢科技的統計資料顯示，上半年相對於去年度，垃圾郵件成長了 60%，挾帶惡意軟體的垃圾郵件數量增加 22%，開啟帶有惡意內容的垃圾郵件對資訊安全造成嚴重威脅，防制垃圾郵件為資訊安全重要的一環，為宣示共同防制垃圾郵件及相關資訊安全威脅的合作的決心，本屆倫敦行動

計畫年度會議，與會各國代表聯合發表「東京宣言」，強調會員國共同合作減少垃圾郵件濫發的重要性，並鼓勵新成員加入倫敦行動計畫國際合作的行列。日本總務省提案建置「反垃圾郵件圖書館網頁」，以增進各會員國對於反垃圾郵件執法措施及先進技術之間的瞭解，獲得與會代表支持，並且均同意將適時提供支援，供各會員國交流參考，提升執法能量。

目錄

壹、 前言

為加強國際合作，宣示我防制垃圾郵件決心，以提升我國國際形象，國家通訊傳播委員會除努力爭取與他國洽簽雙邊、多邊防制垃圾郵件合作協議外，並積極參與國際防制垃圾郵件相關組織及活動，自 94 年 8 月 4 日以「臺灣」名義加入「倫敦行動計畫(LAP)」成為正式會員以來，逐年派員參與其年度會議，以蒐彙各國防制垃圾郵件之策略及經驗，同時尋求建立國際合作關係。日本方面鑒於垃圾郵件的活動屬於跨國性質，本質上並無國界之分，為有效防制垃圾郵件之泛濫，必須加強國際合作，因此邀請我方於出席該年度會議前一日(10 月 6 日)共同召開「臺日防制垃圾郵件雙邊交流會議」，就臺日雙方有關垃圾郵件法案、防制系統技術與強化合作機制進行交流；本次 103 年 10 月 7 日至 9 日於日本東京舉辦之「第十屆倫敦行動計畫」年度會議，已係我國加入該計畫後第 8 次參與之國際性工作會議，審酌垃圾郵件事實上屬於資訊安全中的一環，資訊安全相關的議題亦是本屆會議討論的重點，同時在法律層面上，已立法反垃圾郵件的國家將於會議中分享其執行經驗，本會特指派資源技術處吳銘仁簡任技正及法律事務處陳俊瑋專員、林湛翔技士出席會議。

本次會議主題以「垃圾行動簡訊(SMS Spam)」、「GSMA 對於手機垃圾簡訊濫發行為之因應」、「網路時代所面臨的執法挑戰」、「聯盟行銷對消費者的威脅」、「日本重要電信政策介紹」等為中心，會議之宗旨有促進國際合作、建立全球性夥伴關係、呼籲公協會及業者參與、提升公眾防堵資安事件意識、建立周全法規機制、加強資訊分享及追蹤技術之研發、共同致力於未來網路經濟之發展等項。鑒於會議討論事項相當廣泛，本報告僅就會議議程、議題內容、檢討心得與建議、附錄等擇要撰擬，期望對於相關業務之推動有所助益。

貳、 臺日防制垃圾郵件雙邊交流會議

一、 會議時間、地點

時間：103 年 10 月 6 日

地點：日本東京新宿京王廣場飯店(Keio Plaza Hotel)

二、 會議主旨

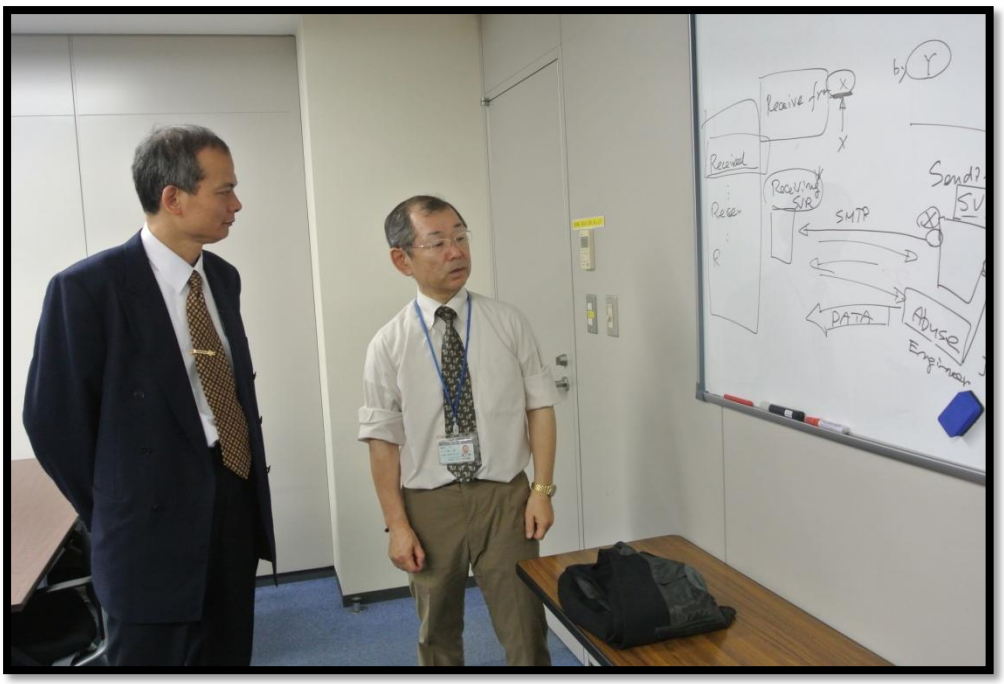
本次會議日方為加強臺日防制垃圾郵件國際合作，邀請我方共同召開，我方由本會資源技術處吳簡任技正銘仁代表致詞，就臺日雙方有關防制垃圾郵件法案、防制系統技術與強化合作機制進行交流。

三、 會議剪影

▲本會代表(吳簡任技正銘仁、陳專員俊瑋、林技士湛翔)與日方於雙邊交流會議後合影，日方代表為日本總務省課長補佐筒井邦宏(左一)、日本防制垃圾郵件諮詢中心主任西松薰(左二)、日本總務省企劃官藤波恒一(左三)。

▲本會代表於日本數據通信協會前合影。

▲本會吳簡任技正銘仁與日本防制垃圾郵件諮詢中心主任西松薰於協會前合影。



▲本會吳簡任技正銘仁與防制垃圾郵件諮詢中心主任西松薰討論情形。

▲日本數據通信協會參訪結束後，本會代表與日方代表合影，日方代表為協會所長西岡邦彥(左二)、防制垃圾郵件諮詢中心主任西松薰(右二)。

參、 第十屆倫敦行動計畫(London Action Plan)年度會議

一、 會議時間、地點及議程

時間：103 年 10 月 7 日至 10 月 9 日

地點：日本東京新宿京王廣場飯店

議程：詳附錄

二、 開幕式

本次會議係日本總務省(MIC；Ministry of Internal Affairs and Communications)所主辦，參與會議之會員包括美國、歐盟、加拿大、澳洲、紐西蘭、日本、南非、香港、新加坡、南韓、印度、我國及中國大陸等;倫敦行動計畫之目標在促進國際間垃圾郵件以及相關議題如網路詐欺、釣魚及散佈病毒之主管機關，共同合作及討論行動議題之機會。

開幕式由日本總務省總合通信基盤局局長(Director-General of the Telecommunications Bureau) Mabito Yoshida 致開幕辭，歡迎各國代表出席本屆日本東京主辦之「第十屆倫敦行動計畫」年度會議，藉由本年度會議的舉辦，持續加強國際合作，綜合各國執法、技術等層面的經驗進行交流分享，共同杜絕網路非法濫用以維護用戶資訊安全及權益，並於會議中發表東京聲明(Tokyo Statement)如下：

1. 繼續透過定期會議討論，在倫敦行動計畫的框架下，加強有關垃圾郵件防制和其他相關電子方面威脅之國際合作。
2. 為有效防制垃圾郵件，會員之間的合作十分重要，同時應鼓勵更多新成員加入倫敦行動計畫。
3. 成立「反垃圾郵件知識庫網頁(Anti-Spam library web pages)」，幫助加強各成員國執法人員之專業知識，並利用最佳的技術方式來防制

垃圾郵件。

三、 會議剪影

▲本會代表吳簡任技正銘仁(中)、陳專員俊瑋(右)、林技士湛翔(左)於會場前合影。

▲日本總務省總合通信基盤局局長吉田真人(Mabito Yoshida)致開幕

辭。

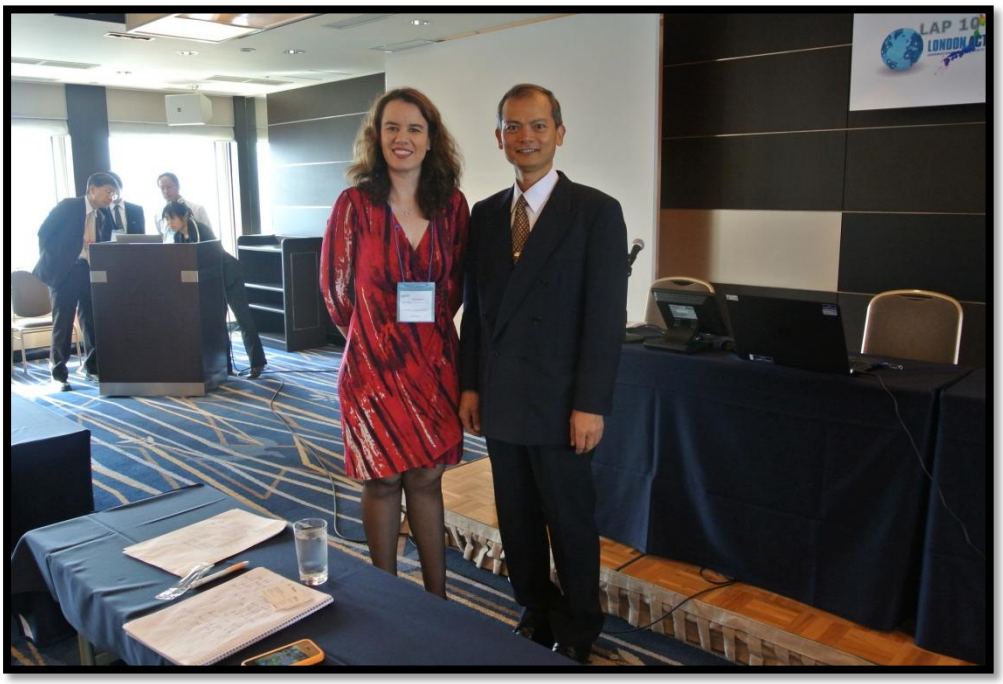
▲吳簡任技正銘仁代表本會向日本總務省總合通信基盤局局長吉田真人(Mabito Yoshida)致贈禮品。

▲會議期間各國經驗交流分享座談。

▲新加入成員(香港)之 Country Update，由香港通訊事務管理局辦公室李助理總監若愚擔任報告人。

▲會議期間互動討論情形。

▲會議中場休息期間，本會代表與中國大陸中國互聯網協會副秘書長石現升(右四)、工程師張鵬(右二)；香港通訊事務管理局助理總監李若愚(右三)等合影。



▲吳簡任技正銘仁與澳洲(ACMA,Australian Communications and Media Authority)代表 Julia Cornwell McKean 經理合影。

肆、 討論議題資料整理

一、 臺日防制垃圾郵件雙邊交流會議

本次「臺日防制垃圾郵件雙邊交流會議」討論題綱主要有如下 4 點：(1)臺灣防制垃圾郵件相關法案之立法情形；(2)日本垃圾郵件處理系統相關技術介紹；(3)臺灣垃圾郵件處理系統介紹；(4)強化合作機制經驗交流。本會代表訪日期間，為能深入瞭解日本垃圾郵件處理系統相關技術，吳銘仁簡任技正、陳俊瑋專員與林湛翔技士一行 3 人主動與日方代表西松薰主任洽詢，徵得所長西岡邦彥同意後，選定於 10 月 9 日倫敦行動計畫年度會議當日討論議程結束後，於晚間 5 點 30 分協同西松薰主任前往日本數據通訊協會(JADAC)垃圾郵件防制中心拜會西岡邦彥所長，並由西松薰主任為本會吳銘仁簡任技正、陳俊瑋專員與林湛翔技士進行日本垃圾郵件處理系統相關技術介紹並強化合作機制經驗交流；臺日通訊傳播相關資安議題討論如下(中英對照)：

(1) 請問日本針對通傳事業是否有特別訂定資安防護規範？有，如何規範？成效如何？ (First, Does Japan propose bill to regulate national information security regarding telecom sector? How are the regulations deployed? How do you think about your strengthening information security measures in this area?)

關於通訊傳播事業的資安防護，日本並未研訂專法規管。至於，各家電信公司對於資安防護議題則是依商業法規的有關規定予以處理。日本對於資安防護相關措施及各項具體作為，通常採行「由下而上」及「相助合作」方式辦理。目前由各家 ISP 業者所組成之 Telecom-ISAC Japan 協會，負責協調業界以自治方式進行資安防護管理。總務省(MIC)也與 Telecom-ISAC Japan 協會等建立密切合作關係共同維護確

保網路環境之安全。以日本網路惡意程式移除中心(Cyber Clean Center)計畫為例子，即是由總務省(MIC)與 Telecom-ISAC Japan 協會所共同執行完成之資安防護計畫。(Currently there is no "bill" proposed to regulate telecom sector for information security. Basically there is also no specific "act" regarding information security in telecom sector. The companies in telecom sector has their responsibility regarding information security as well based on the regular business law. In Japan the actions/measures for information security are usually conducted by "bottom-up" and "cooperative" approach. There is an association of ISPs called Telecom-ISAC Japan. They are basically an independent industrial association by themselves for themselves. We, MIC, is "collaborating closely" with them to secure Japanese network environment. The Cyber Clean Center is the project conducted by MIC and Telecom-ISAC Japan.)

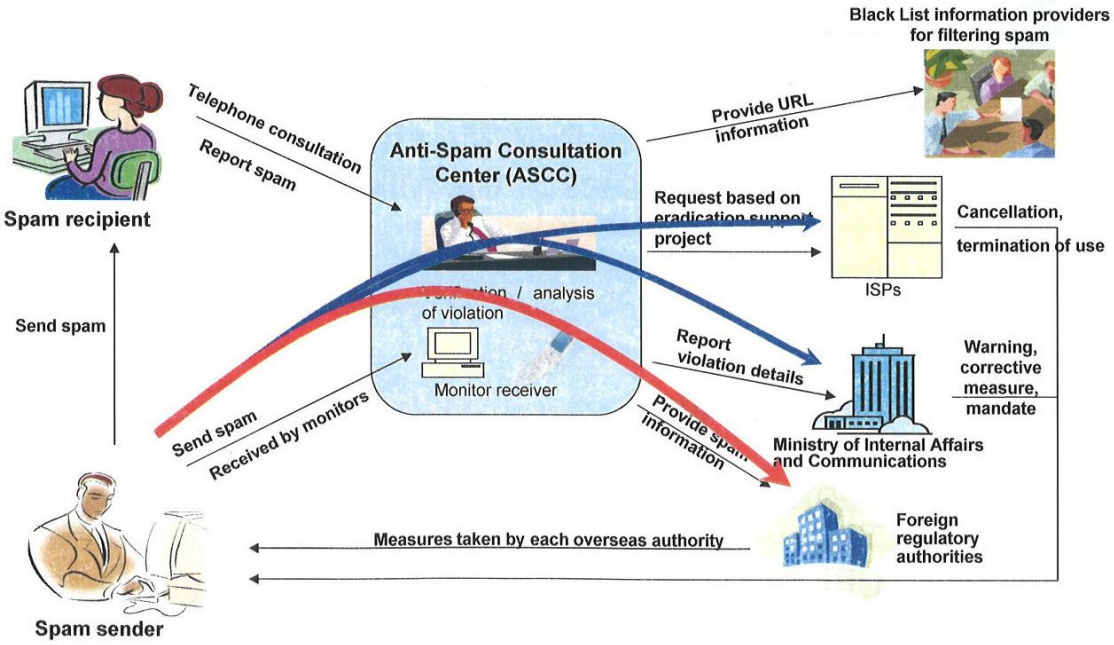
(2) 日本網路惡意程式移除中心(Cyber Clean Center)辦理經驗為何？是否有後續替代方案幫助消費者？(Next, As you know, TWCER/CC is running Cyber Clean Center project that is like Japan's C.C.C. project which was conducted from 2006 through March 2011. We would like to know more about Japan's advanced working experience in this area.)
正如同您所知，Telecom-ISAC Japan 協會所主導的日本網際網路惡意程式移除中心(Cyber Clean Center)計畫已經於 2011 年宣告終止。我們接著啟動 the ACTIVE project，該計畫如我於先前簡報所介紹是奠基於網際網路惡意程式移除中心(Cyber Clean Center)過往成就所啟動的新型計畫。the ACTIVE project 是項先進的惡意程式反制措施計畫，相關詳細內容請參閱附件資料供參考。

(3) 行動通訊網路資安問題已漸成重要課題，就日本 Botnet 防制、資安事件警訊分享等是否已包括行動通訊網路部分？行動通訊網路部分

是否有可能進行跨國資訊即時分享、交流？若有，則目前成果為何？若否，則有何考量？(Last, The information security of mobile communications has been a critical issue in Taiwan. Is the issue important in Japan? Do the actions of fighting botnet project include the sector of the mobile communications in Japan? Is it possible to establish an anti-botnet project information exchange channel or any kind of international collaborative information sharing, monitoring & analysis system in the realm of mobile communications between Taiwan and Japan? We are looking forward to collaborating with Japan.)

僅管我們充分認知行動通訊資安的重要，並已針對此一議題實施數個活動，期盼能喚起民眾強化自身資安維護之意識。但是，對於如何有效打擊包含行動通訊等在內的殭屍網路，目前仍無特定的行動或方法可以有效因應其諸多挑戰。我們針對 the ACTVIE project，也正討論是否擴大範圍，將行動電話手機等手持終端設備一併納入，不過，目前也僅處於討論中的階段。(We recognize that security of mobile communication and do several activities regarding awareness raising for this issue, but unfortunately there is no specific actions or approach for fighting bot-net include mobile communications. There is an discussion to expand the scope of the ACTVIE project to include mobile devices, but it's still discussion.)

日本防制垃圾郵件諮詢中心(ASCC；Anti-Spam Consultation Center)隸屬於一般財團法人日本數據通信協會(JADAC)，由日本總務省(MIC)授權專責處理垃圾郵件問題，並執行監控任務，其垃圾郵件來自於內部設立之誘捕(Honey- Pots)信箱和民眾檢舉，處理流程如下圖：



ASCC 提供相關網址訊息給垃圾郵件過濾服務供應商作為建立黑名單之參考依據，並分析垃圾郵件之來源 IP，若是 IP 源自日本國內，則透過電子郵件向其所屬網際網路服務供應商(ISP)發送確認信，確認 IP 是否正確屬於該 ISP，經確認無誤後即向上陳核總務省(MIC)，經總務省負責該管業務之三名長官簽章認定後，再透過電子郵件向所屬 ISP 進行舉報，由 ISP 對其濫發之用戶進行提醒、警告、停權等處置措施；若 IP 源自國外，則將垃圾郵件移送已建立合作機制的國家，由各合作國採取相關處置措施。

ASCC 並未自行開發系統處理大量之垃圾郵件，而是根據需求由採購的方式購入軟、硬體設備及維護，ASCC 之人員僅負責操作應用，參訪時 ASCC 主任西松薰親自介紹系統，並示範操作，其系統介面在網頁上運行，經由民眾檢舉或是來自誘捕信箱的垃圾郵件，程式分析處理後儲存在資料庫中，網頁介面有諸多選項設定，根據設定的條件，從資料

庫取出所需的資訊顯示在網頁上，並可將顯示的資訊存成 Excel 檔案，日方亦是透過此 Excel 檔案，以電子郵件附件的方式移案各合作國，舉例來說，將設定條件中的國家選項設為臺灣，並設定日期範圍，按下確認後在網頁介面上顯示來自臺灣的垃圾郵件標頭資訊，再按下按鍵將資訊生成 Excel 檔案儲存，再利用電子郵件附件的方式移送到本會，故本會接收到日本移案的電子郵件，需再利用程式讀取垃圾郵件標頭資訊之 Excel 檔案，重組還原成 eml 格式之後，通報其所屬的網際網路接取服務業者(ISP)。

為保護舉發人及延長誘捕信箱效期，將垃圾郵件通報所屬 ISP 之前，需將郵件標頭有關個資或其他所需隱匿的部份加以遮罩(Mask)，程式會檢查下列的項目內文將關鍵的部份進行遮罩處理：

- From
- Return-Path
- For
- To
- Message-ID
- Subject
- Text
- URL

以下為郵件標頭遮罩的範例：

```
From abh***e@nich**********al.co.in  Mon Jan 10 23:15:28 2011
Return-Path: <abh*****************al.co.in>
Received: by m.mserv.hi-ho.ne.jp (hiho-m601b) id p0ADxA5G032028; Mon, 10 Jan 2011 22:59:10 +0900
Received: from p674***********07.ap.so-net.ne.jp (p674***********07.ap.so-net.ne.jp [121.103.75.101])
      by mx.mserv.hi-ho.ne.jp (hiho-mi600) with ESMTP id p0ADx93t009867
      for <******@bz3.hi-ho.ne.jp>; Mon, 10 Jan 2011 22:59:10 +0900
Received: from [95.195.225.196] (account abh*****************al.co.in HELO aptj**************qz.su)
      by p674**********07.ap.so-net.ne.jp (CommuniGate Pro SMTP 5.2.3)
      with ESMTPA id 86******2 for ******@bz3.hi-ho.ne.jp; Mon, 10 Jan 2011 22:59:09 +0900
From: "Franklin@lbgjjeeafaf.{SPF_D1}" <Franklin@lbgjjeeafaf.{SPF_D1}>
To: <******@bz3.hi-ho.ne.jp>
Subject: Mon, 10 Jan 2011 22:59:09 +0900
Date: Mon, 10 Jan 2011 22:59:09 +0900
MIME-Version: 1.0
Content-Type: text/plain
      charset="iso-8859-2"
Content-Transfer-Encoding: 7bit
X-Mailer: payly 72
Message-ID: <803*******************03@lb*****afaf.{SPF_D1}>
Franklin Brock Mon, 10 Jan 2011 22:59:09 +0900Get 15% Disc1p1zfount On ALL Watku4zrm65ches Today!
Repzmk50jyolica Ro6t56lex mopqpygh4dels o12zswf the latest Baselwod6rld 2010 designs have just been launched
ok0c188n ofaelarur replica sites.These are the first run o4nfbwnr3f the 2010 mookzdels with inner Rof2lex
```

```
From ******** Tue May 31 09:30:50 2011
Return-Path: <********>
Received: from bbmts09sb.softbank.ne.jp (bbmts09sa.softbank.ne.jp [123.108.236.152]) by col2.antispam.go.jp
(8.13.8/8.13.8) with ESMTP id p4V0UnWk014811 for <********>; Tue, 31 May 2011 09:30:49 +0900
Received-SPF: Pass Received: from mx1.imx35.biz ([116.66.189.202]) by bbmts09sb.softbank.ne.jp with SMTP id
<20110531003049263.DUGJ.3755@bbmts09sb.softbank.ne.jp> for <********>; Tue, 31 May 2011 09:30:49
+0900
Received: from 216.179.212.38 ([216.179.212.38]) by 127.0.0.1 (The Phantom 1.5.0) with SMTP ID 9***4 for
<********>; Tue, 31 May 2011 09:30:23 +0900 (JST)
Received: from localhost (localhost.localdomain [127.0.0.1]) by I-ISI-w1.localdomain (Postfix) with ESMTP id
A9C4***00B for <********>; Tue, 31 May 2011 09:30:19 +0900 (JST)
Subject:最初会長は資産10億を部下に分配しようとしたのです。しかし私の部下は誰一人受け取るという人間はいませんでした。
From: love@psmixi.jp
To: ********@t.vodafone.ne.jp
MIME-Version: 1.0
Content-Type: text/plain; charset="shift_jis"
Message-Id: <2011053100301*****0109000B@I-ISI-w1.localdomain>
Date: Tue, 31 May 2011 09:30:19 +0900 (JST)
X-BMTA-TYPE-ISP: Content-Transfer-Encoding: 8bit
X-MIME-Autoconverted: from quoted-printable to 8bit by ******** id p4V0U*****4811
:
振込担当　鮎川さんからNew!メッセージ到着♪ [タイトル] 最初会長は資産10億を部下に分配しようとしたのです。しかし
私の部下は誰一人受け取るという人間はいませんでした。[続きはコチラ]　↓↓↓
http://xyu133.org/r/2/m/mailbox_data.php?mid=12*****7&x=b68c0a**********6289796983cb1d
 PASSIONメインページ↓
 http://xyu133.org/r/2/m/?x=b68c0a********6289796983cb1d
配信:PASSION 退会、利用停止、配信停止はコチラ info@psnx.net
```

在郵件標頭資訊中，Received 標記記錄著郵件收發的網域名稱、IP 地址、信箱及時間等來源資訊，通常會有數個，其範圍由下往上看，在正常情況下，則愈往下愈接近來源，格式如下：

Received: from 送信端網域名稱與 IP 位址 **by** 接收端網域名稱與 IP 位址 **for** 接收端信箱 ； 時間

舉例：

Received: from msr10.hinet.net ([168.95.4.110]:60533) **by** seed.net.tw

with esmtp (Seednet 4.69:2) id 1UuwOE-000DH8-HG **for** marchfun@seed.net.tw**;** Fri, 05 Jul 2013 11:08:54 +0800

但在實際情況，Received 標記的順序未必是正確的，因目前我國尚未通過反垃圾郵件相關立法，因此本會分析程式會將垃圾郵件來源資訊根據時間加以重新排序，以找出濫發源 IP 所屬之 ISP，將完整資訊移送所屬 ISP 要求進行必要處置，而日本的做法是只依原有順序找出濫發源 IP 所屬之 ISP 即進入程序移送，因日本有立法制訂通過「特定電子郵件傳送標準化法」之反垃圾郵件法令，追查實際濫發源為法律上賦予 ISP 應負之責任，故主管機關僅需根據 IP 移送而不需前置處理；經追查即使個人用戶受到惡意軟體感染而濫發垃圾郵件，所屬 ISP 仍可對該用戶終止電子郵件服務，同時在時間部份也予以遮罩處理，以避免濫發者有機會根據時間資訊追溯誘捕信箱地址。

為有效防制垃圾郵件活動，除了受理並處理垃圾郵件案件外，在 ASCC 內部設有反垃圾郵件活動支援系統，其主要任務如下：

1. 垃圾郵件蒐集和垃圾郵件標頭資訊分析。
2. 遮罩來自於誘捕信箱的垃圾郵件標頭資訊後，回報給所屬 ISP。
3. 提供軟體插件(Plug-in)給主要檢舉者，以便於大量檢舉垃圾郵件。

反垃圾郵件活動支援系統目前仍然無法完全自動化，有下列項目需要經由人工確認或執行：

1. 違法事實之認定

   除了 ASCC 向 ISP 確認 IP 來源外，需經由總務省的長官再次確認後，才會判定該 IP 違法濫發垃圾郵件，移請所屬 ISP 處置，並根據「特定電子郵件傳送標準化法」裁罰。

2. 郵件標頭與內文遮罩

   要移請 ISP 處置或移送案件給合作國前，需自行點擊遮罩按鈕，方

能進行遮罩處理。

3. Whois 資料查詢

必須定期手動更新內部 Whois 資料庫，確保最新 IP 查詢資訊。

4. 選擇 ISP

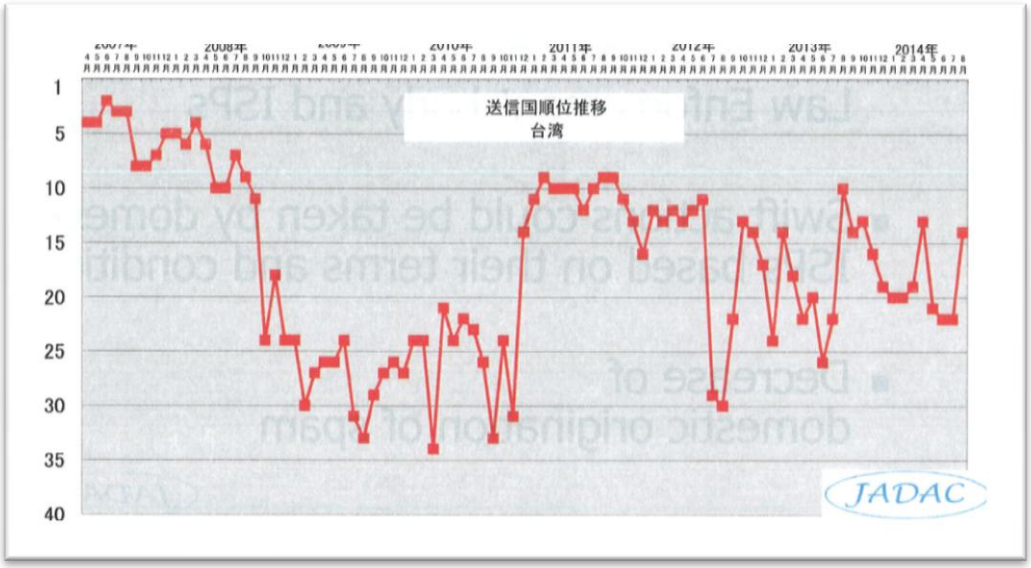
需自行點選所要移送的 ISP，系統無法自行判斷。

在日本，主管機關與民間 ISP 已經建立良好的合作關係，同時 ISP 可根據其服務條款對於違法濫發的行為迅速採取行動，大幅減少了源自國內的垃圾郵件，但目前大多數的垃圾郵件發送據點已轉移至國外，形成執法上的困難，因此日本非常積極拓展國際合作，以期有效嚇阻垃圾郵件的濫發行為。

傳統上電子郵件採用簡易郵件傳送通訊協定(SMTP；Simple Mail Transfer Protocol)，但此通訊協定制定於上世紀 80 年代，當時網路環境單純故未有垃圾郵件之概念，缺乏必要的身分認證機制，造成日後遭有心人士利用使得垃圾郵件氾濫且難以查緝，故衍生出了 SMTP 的擴充版本 SMTP-AUTH，AUTH 為 Authentication 的縮寫，在發送電子郵件之前必須提供帳號密碼進行身分驗證，確認後才能將郵件寄出，但即使增加了身分驗證機制，仍然無法制止遠端駭客操控殭屍網路做為跳板來大量濫發垃圾郵件，因此日本在國內採行 OP25B(Outbound Port 25 Blocking)的機制來收發電子郵件，由於使用者要寄送電子郵件，必須通過寄件人的 SMTP 伺服器，SMTP 伺服器的標準連接埠為 Port 25，OP25B 限制 Port 25 的使用，使用者只有透過自己線路的網際網路服務供應商(ISP)所提供的 SMTP 伺服器才能使用 Port 25 傳送郵件，而不允許非自身用戶使用 Port 25 發送郵件，若不同 ISP 業者的用戶要透過郵件伺服器發送郵件，則必須使用 Port 587 加上 SMTP-AUTH 協定，進行身分認證後才能寄送郵件，目的在於除了身分認證機制外，也防堵駭客利用殭屍電腦濫發垃

圾郵件。

日方提出來自我國 2007 年 4 月至 2014 年 8 月間垃圾郵件的數據統計圖如下：



▲臺灣向日本濫發垃圾郵件排名的歷年變化統計圖。

▲來自臺灣垃圾郵件所占百分比的歷年變化統計圖。

在 2007 年至 2008 年之間來自我國的垃圾郵件量偏高，一度排名前 5 名，垃圾郵件的佔比達到 10%至 12%之間，在 2008 年下旬之後開始大幅下降，我國的濫發排名都在 10 名之外，垃圾郵件佔比大部份都在 2%以下，日本總務省在 2008 年年初決定全面禁止垃圾郵件，並且向大量濫發垃圾郵件的企業下達改善命令，並於同年 4 月份，與我國建立防制

垃圾郵件的合作機制，數據上顯示已有顯著成效。

二、 倫敦行動計畫年度會議

為宣示共同防制垃圾郵件及相關資訊安全威脅合作的決心，本屆倫敦行動計畫年度會議，與會各國代表聯合發表「東京宣言」，其中文翻譯如下：

1. 我們是參加第 10 屆倫敦行動計畫(LAP 10 東京)的各國代表們，自 2014 年 10 月 7 日至 9 日在日本東京新宿京王廣場飯店舉行年度會議。
2. 我們再次確認將遵照倫敦行動計畫合作架構，定期召開會議共同研討防制垃圾郵件及相關電子資訊安全威脅的合作事宜。
3. 我們已充分認知到各成員國對於共同合作減少濫發垃圾郵件的重要性。此外我們也應該鼓勵新進成員加入倫敦行動計畫國際合作。
4. 我們針對日本總務省提案建置「反垃圾郵件圖書館網頁」，以增進各成員國防制垃圾郵件執法措施以及相關先進技術的瞭解，敬表歡迎，並且同意將適時提供支援。

我們(各國代表)謹在此承認此一宣言。

「東京宣言」英文及日文版本詳附錄。

議題一、日本重要電信政策介紹(Keynote address)專題演講。

主講人：總務省企劃官藤波恒一(Mr.Fujinami Koichi)

由介紹日本電信電話株式會社(Nippon Telegraph and Telephone Corporation；NTT)的歷史發展，論及日本電信產業及市場、智慧型手機隱私權保護及濫發商業電子郵件防制作為，因應時勢鬆綁法規並適度引進外資，促進消費者權益保障；介紹日本個人資料保護法，在日本不論是政府機關或是民間機構，只要有使用到個資的情形，

均受到個人資料保護法的規範，並且明確定義事業單位利用個人資料時應遵守之義務、資料的使用目的，與限制、取得、正確、安全、透明等該法之五項基本原則；而日本在 2012 年 8 月進行智慧手機隱私維權首次倡議(Smartphone Privacy Initiative I)，在 2013 年 9 月進行智慧手機隱私維權二次倡議(Smartphone Privacy Initiative II)。在最後介紹日本防制濫發商業電子郵件之作為，目前與日本建立合作管道的國家為臺灣、中國大陸、南韓、印度、巴西及越南等六國，其中雙向交換的國家為臺灣、南韓、巴西，單向交換的國家為中國大陸、印度、越南。

日本「特定電子郵件傳送標準化法」制定於 2002 年；分別於 2005 年與 2008 年進行兩次修正，2008 年第二次修正時變更原先立法採行的選擇退出(OPT-OUT)的機制，改採行(OPT-IN)機制，並進一步課予發信人資訊之開示義務，行政告誡與裁處流程如下：

(1) 由總務省寄發警告信給濫發商業電子郵件行為人。
(2) 若濫發人仍不遵守前揭警告信函，總務省將再發給措置命令(行政處分)。
(3) 若濫發人仍不確實遵守措置命令(行政處分)，濫發人依法將再受到主管機關進一步的裁罰(刑罰、行政罰)。

議題二、國際刑警組織百年創新介紹

國際刑警組織創立於西元 1914 年，成立至今適逢百年，為目前全球最大的跨國警察組織，會員共計 190 個國家，組織的目的在於藉由全球警察通力合作，讓國際犯罪無所遁形，共同創造安全生活環境；闡述新興的執法挑戰、複數管轄權調查程序(Multi-jurisdictional)

以及國際刑警組織全球創新中心(INTERPOL Global Complex for Innovation；IGCI)相關執法進程；IGCI 位於新加坡，在資訊發達的時代犯罪行為變得更具侵略性且難以捉摸，特別是在是在網路犯罪與兒童性剝削方面，全球化的時代，執法的複雜度與日俱增，遠超過傳統執法模式的想像，該中心積極研究新的領域並提供執法訓練，目的在使全球的警察都能使用最先進的技術工具，以應付犯罪份子所帶來日益嚴峻的挑戰。

議題三、會員國執法經驗交流活動

荷蘭垃圾郵件的主管機關為消費者保護暨市場管理局(Authority for Consumers & Markets；ACM)，其代表分享垃圾郵件防制發展趨勢的看法，與近十年的執法經驗、相關施政作為、垃圾郵件防制成功和失敗的經驗等；紐西蘭亦分享其執法經驗，以及網路安全對紐西蘭執法的挑戰；加拿大則分享濫發商業電子郵件、話費欺詐與各類型詐騙；綜合各國分享之結論，網路資訊的流通並非單一國家所能掌控，且各國並沒有相同的法律標準規範，且網路具有「匿蹤」的特性，容許用戶隱藏真實身分，此點特性雖促成網路應用蓬勃發展，但也使得身分難以確認，造成執法上的困難，且隨網路科技的發展,犯罪行為的手法日新月異,使得執法人員窮於應付，這也是當前網路時代所面臨的挑戰。

1. 新加入之會員介紹

本屆新加入的會員為南非與香港：

(1) 南非由消費者保護委員會副主委(Ms. Thezi Mobuza,National Consumer Commission)代表出席與會，介紹南非消費者保護委

員會的機關執掌與功能，以及前瞻的施政規劃項目。

(2) 香港由通訊事務管理局(OFCA)助理總監李若愚介紹香港防制垃圾郵件的成果。

2. 日本總務省資安政策與相關施政作為

日本資安政策主要目的是為了建立安全且可靠的通訊環境，其概要如下：

(1) 網路

創造健全且可靠的網路、促進網路經營者間的資訊共享、ISP 業者防範對策的發展，促進電子簽章、認證、電子戳章已及密碼技術的使用。

(2) 個人

提升個人素質、警覺性並且教育網路使用者，參加 ACTIVE 計畫(Advanced Cyber Threats Response Initiative；進階數位威脅應對提案)來減少惡意軟體感染的影響。

(3) 技術

積極鼓勵研究和發展，進行研發計畫來發展安全對策來對抗新興的網路威脅，促進國家相關研發機構來從事研究工作。

(4) 國際

積極拓展國際合作，強化多邊及雙邊的夥伴關係，提升私營部門及研究機構的國際間合作，並標準化網路安全技術。

由惡意軟體所進行的惡意行為如 DDoS 攻擊等，已經十分普遍並影響到日本的商業活動，PRATICE 計畫(Proactive Response Against Cyberattacks Through International Collaborative Exchange；國際合作交換資訊積極應變以對抗網路之攻擊之專案) 屬於國際合作，由總務省和 ISP 業者網路安全協會(Telecom ISAC Japan/Telecom

Information Sharing and Analysis Center Japan)、研究機構(NICT/資訊通信研究機構)、和合作公司(KDDI 電信公司)等規劃，針對日益增長而且變得更有智慧網路攻擊者的趨向預測和快速回應之研發計畫，透過資料探勘，或是惡意軟體分析等方法學來掌握攻擊者的特徵，自 2011 年 8 月開始，透過研發及田野調查來掌握攻擊的特徵，並透過深度分析及經由國際合作交換資訊安全建構網路來快速應付攻擊；在個人電腦受到惡意軟體感染方面，例如不正常匯款的詐欺行為，經常以透過網路感染的惡意軟體形式出現，因此從 2013 年 11 月開始，與 ISP 業者合作，防堵惡意連結連線至散播惡意軟體網站；對於進階持續性滲透攻擊，易造成機密資訊洩漏，因此從 2013 年 9 月開始，透過分析進階持續性滲透攻擊的方式來了解現況，積極建立對於進階持續性滲透攻擊的防範模組，並且透過實際參與官方或私人機構主辦的攻擊演習活動來建構並提升防衛能力。

總務省在去年(2013 年)9 月 25 日在東京首次舉行官方與民間合作的網路攻擊演習活動 (CYber Defense Exercise with Recurrence；CYDER) ，目的在加強政府機關內網路管理者的能力，並讓大型企業能阻擋進階持續性滲透攻擊，透過反覆實施 CYDER 來獲得經驗，以發展成功有效的防衛模式，此為超過千人組織所構築的大規模虛擬網路，演練採用真實的進階持續性滲透攻擊，總共來自 33 個組織共有國家機關、公司行政部門、私人企業等共 293 人，以每組 3、4 人的方式分組參加演練。

在垃圾郵件方面，垃圾郵件占了日本 60%的總電子郵件流量，垃圾郵件屬跨國性質(日本超過 90%的垃圾郵件來自境外)，因此國際合作對打擊垃圾郵件具有重要性，目前日本積極與國際進行資訊分享，日本現在與臺灣、中國大陸、南韓、巴西、香港及越南分享關

於包含 IP 位址在內的垃圾郵件濫發者的資訊。

議題四、新興型態垃圾行動簡訊(SMS Spam)

垃圾行動簡訊(Short Message Service Spam；SMS spam)的分析數據中顯示，有 10%屬於色情內容，但最大宗屬於金融詐欺而非傳統商業性質廣告，約佔了 70%，攻擊的手法可分為釣魚、社交工程、費用詐騙等三類；金融詐欺相關的垃圾簡訊內容常利用免費贈品或優惠的方式吸引用戶點擊連結，要求如銀行帳戶、信用卡號碼等資訊，用戶的手機帳單很可能因此多出不必要的費用，而電信服務供應商通常只負責用戶簡訊的收發，而不在乎用戶增加多少費用，易造成消費權益受損求償無門，同時也有可能因此被植入惡意軟體，藉此收集敏感個資，再販售給營銷人員牟利，使用戶隱私受到侵犯；同時，惡意軟體存在手機的內部記憶體中，也會使用戶的手機效能降低，影響使用品質。垃圾行動簡訊的存在已經對美國消費用戶及電信服務供應商造成嚴重困擾，預付卡是常見的濫發源，具有價格低廉且不易追蹤的特性，少有電信服務供應商具備良好的防禦系統。

在美國濫發垃圾行動簡訊是違法的，除非發送者事先取得用戶同意，但是有下列兩項例外：

(5) 與用戶相關的消費行為確認，例如產品維修訊息、用戶訂購之產品詳細規格等。

(6) 非商業性質之簡訊，例如民意調查、募款訊息等。

美國聯邦貿易委員會(Federal Trade Commission；FTC)和美國聯邦通信委員會(Federal Communications Commission；FCC)均可接受電信

用戶申訴檢舉。

為防制垃圾行動簡訊，必須加強國際合作關係，建議國際間可簽訂合作備忘錄(MOU)以及相關保密協定(NDA)等，並藉由全球行動通訊系統協會(GSMA)建立的垃圾訊息舉報服務(Spam Reporting Service；SRS)機制，加強執法能量，共同打擊非法行為。

議題五、GSMA 對於手機垃圾簡訊濫發行為之因應

全球行動通訊系統協會(Global System for Mobile Communications Association；GSMA)成立於 1995 年，由全球電信業者、相關公司贊助所成立的協會。GSMA 建立的垃圾訊息舉報服務(SRS)針對行動用戶檢舉的簡訊威脅和濫用提供了一個全球相關數據的資料庫，驗證並分析問題的可能解決方案和需求，數據分析顯示垃圾簡訊的氾濫超乎預期，解決此問題不但能有效維護用戶的資訊安全，更能降低網路不必要的傳輸流量，不必要的濫用流量正佔用著寶貴的頻寬資源，SRS 的數據分析可讓全球電信服務供應商更清楚了解垃圾簡訊對自身網路的影響以及攻擊趨勢；手機簡訊濫用的問題是一個全球性、跨營運商的問題，GSMA 會協調並協同擬定計劃，以打擊垃圾簡訊，透過 GSMA 平台，電信服務供應商可快速、便利的對於垃圾簡訊之相關資訊進行交流，不需要追查出濫發來源即可採取適當行動，GSMA 的介入也有助於進行大規模垃圾簡訊報告服務，藉由網路公開詳細資訊，成為打擊有害垃圾簡訊的有效利器。更廣泛來說，GSMA 的主要目標之一是確保網路用戶可以信任 GSM 網路的安全性，共同維護消費者用戶對行動網路及設備環境的信心，並提升人性化服務的完整性。

議題六、加拿大最新濫發商業電子郵件防制與資安電子威脅立法

加拿大反垃圾郵件法已於 2014 年 7 月 1 日實施，執法單位分別是加拿大廣播電視暨通訊委員會(Canadian Radio-television and Telecommunications Commission；CRTC)、加拿大競爭局(Competition Bureau；CB)和加拿大隱私公署 (Office of the Privacy Commissioner of Canada；OPC)，加拿大垃圾郵件舉報中心(Spam Reporting Centre；SRC)由 CRTC 負責運作管理，受理未經同意發送的商業電子郵件或電子訊息、假冒或內容不實的商業電子訊息之檢舉，檢舉的資訊移送 CRTC、BC 及 OPC 等執法單位處理；CRTC 為加拿大反垃圾郵件法主要的執法單位，除了調查與進行反制措施外，並針對下列行為祭出行政罰：

(7) 違法發送商業電子訊息，即未取得民眾事先同意發送的商業電子訊息。

(8) 未經網路用戶同意，逕行改變傳輸數據內容，例如透過內部設定將不知情的用戶連結到他們不想造訪的網站。

(9) 未經用戶同意，逕行安裝軟體到用戶的電腦中，這些軟體很有可能是惡意程式或是病毒。

CB 為加拿大獨立的執法機關，目的在促進產業健全發展和維護消費者權益，CB 的角色在審查電子訊息是否涉及具有誤導或詐騙性質，包括偽造的發送人資訊或是容易造成誤導的標題資訊等；OPC 負責保護加拿大民眾的個人資料，法規允許 OPC 執法人員未經同意逕入電腦系統，以及未經授權收集 IP 位址清單之行為並加以處理之權限，並規管下列行為：

(1) 未經同意蒐集電子郵件 IP 位址。

(2) 利用非法行為收集個人資料。

濫發垃圾郵件違反規定者，主管機關為 CRTC，個人罰鍰加幣 100 萬，法人罰鍰加幣 1,000 萬；行政罰與私權訴訟並行，最高罰鍰金額為個人 100 萬，法人 1,000 萬；而商業性質的資訊中，有不實詐騙行為者，主管機關為 CB，若違反規定則個人第一次罰鍰加幣 75 萬，個人累犯罰鍰加幣 100 萬；法人第一次罰鍰加幣 1,000 萬，法人累犯罰鍰加幣 1,500 萬。

議題七、荷蘭 ACM 裁罰 Daisycon 案例以及對其網路行銷之規管作為

在荷蘭濫發商業電子郵件是違法的，在寄發電子郵件之前必須滿足下列需求：

(3) 必須事先徵得收信人之同意。

(4) 收件人必須看的到郵件來源，寄件人必須使用真實身分，不得使用匿名。

(5) 如果收件人不希望獲得後續更多資訊，必須有選擇退出之機制，且必須免費、容易操作。

Daisycon 為荷蘭一家藉由聯盟行銷(Affiliate Marketing)策略以 Lead Generation 和 CPC(Cost-Per-Click；點擊數付費)廣告業務為主的公司，Lead Generation 並沒有標準的中文名稱，目的是開發潛在的客戶，與一般的商業電子郵件不同，此為一種許可行銷，由用戶主動留下資料，由系統根據需求寄送相關電子郵件給用戶，讓用戶有機會變成客戶上門消費；CPC 廣告是聯盟會員根據網路用戶點擊商家廣告的次數來收取費用，亦即廣告主根據點擊次數的方式支付廣

告費給聯盟會員。荷蘭消費者暨市場管理局(ACM)收眾多到來自消費者的投訴，消費者投訴收到不請自來且無法取消的商業電子訊息並表示困擾，而且消費者表示事先並未同意接收，不知為何會收到此商業電子郵件，因此 ACM 對於 Daisycon 濫發超過 20 億筆商業電郵之網路行銷，核屬違法多層次傳銷(multilevel marketing)與誤導消費者(misleading consumer)之行為，依電信法規定裁罰 Daisycon 81 萬歐元，案經 Daisycon 向法院提出訴訟，初審法院判決維持 ACM 裁罰，案經 Daisycon 上訴二審，現交由二審法院審理中。

伍、 心得與建議

倫敦行動計畫是一個全球性的組織，其會員為各國專責資訊安全相關的政府機關或民間機構，除了在會議中分享垃圾郵件及資訊安全相關經驗，亦可以就各國報告的統計數據了解資訊安全問題的趨勢，同時取得資訊安全方面的最新知識與訊息，因網路通訊技術的迅速發展，資訊安全威脅的手法態樣也不斷翻新，國際間每年定期舉辦的會議實屬重要的交流管道，讓各資、通訊發達的國家可以迅速掌握新知，對打擊網路不法行為保持優勢，本會議是一個重要的國際交流平台，可以藉機了解各國處理資安問題的方式、法規機制，同時與會的各國代表也樂於分享，利用實際面談會議方式，交流不便於網路上公開之執法實務經驗，對於國際合作事務的推展來說，是一個良好互動的機會，除了直接面對互動交流外，亦可藉由交換名片或電子郵件的方式保持聯繫，回國後有利於業務的推展。

本次倫敦行動計畫由日本主辦，日本在防制垃圾郵件方面挹注了不少資源與研究人力，於 2008 年 12 月 1 日正式頒布施行「特定電子郵件標準化法」，從 2007 年開始，日本國內 ISP 業者陸續配合政策推行了 OP25B 的機制，使得源自於國內的垃圾郵件大幅下降，本會每週分析垃圾郵件的數據亦顯示來自日本的垃圾郵件數量大多只有個位數，甚至是零，相對於其他國家的垃圾郵件數量明顯偏低，可以顯見日本在國內防制垃圾郵件的成效，但來自國外的垃圾郵件問題仍然無法有效解決，因此日本非常積極拓展國際合作，根據統計，中國大陸目前是第二大垃圾郵件濫發國，因此亦是日本的合作國之一，中國大陸的對外合作窗口為中國互聯網協會。

由於日本國內實行 OP25B 機制，電子郵件的傳送均經過身分認證，沒有遠端駭客操控殭屍電腦濫發垃圾郵件的問題，因此在違法事實的認定上較為明確，執法單位行動也較無爭議，在今年(2014 年)9 月 5 日，日本一名 25 歲的男子町田俊樹因違法大量濫發垃圾郵件，無視日本總務省的警告而遭到

警視廳依法逮捕，成為日本國內首宗因濫發垃圾郵件遭到逮捕的先例；我國方面由於沒有強制實行有關電子郵件的認證機制，遠端駭客容易操控殭屍電腦大量濫發垃圾郵件，因此在當事人違法事實的認定上存在極大爭議，究竟是惡意濫發，或是無辜遭到惡意程式感染而不知情濫發？這也造成我國「濫發商業電子郵件管理條例」的立法瓶頸，即使立法通過頒布施行，爭議點仍然未解而窒礙難行，因此在制定反垃圾郵件相關法案前，事實認定的技術問題務必先行解決，但即使是日本，在實施前也存在人民秘密通訊自由、違反日本電氣通信事業法等爭議，日本的實務見解上則認定 OP25B 屬於「正當業務行為」而不違反相關法律規定，在我國是否適用類似的管制措施及解釋尚有待商榷，因此在防制垃圾郵件的議題上，建議先行凝聚全民共識，再據以建立適用於我國國情的認證管制措施，才能有效解決技術問題，技術問題解決，方能解決為法事實認定之爭議並順利完成立法，有效嚇阻國內濫發垃圾郵件的有心人士。

然而垃圾郵件的傳送是無國界的，源自國內的垃圾郵件僅一小部份，大部分的垃圾郵件均來自國外，因此要徹底防制垃圾郵件，惟有如同日本不斷加強並拓展國際合作，積極參與國際交流掌握趨勢，配合國內的有效防制措施，才能有效提升防堵垃圾郵件效率，本屆倫敦行動計畫年度會議，新加坡、香港、紐西蘭之代表均表示願意與我國建立合作關係，其中紐西蘭代表表達與我國簽署合作備忘錄的意願，對於拓展國際合作，總計目前合作國有美國、日本、南韓、巴西等，未來可能再洽商增加新加坡、紐西蘭；中國大陸為垃圾郵件的第二大濫發國，對於防制垃圾郵件合作上亦表達正面立場，但由於目前時機較為敏感，建議日後再尋求適當時機與大陸、香港建立合作管道；執法在移送垃圾郵件方面，我國是不同的國家採不同的檔案格式與傳送方式移送，例如移案南韓使用 FTP 及 eml 檔案格式、移案巴西使用 FTP 及 mbox 檔案格式、移案美國使用電子郵件及 msg 檔案格式、日本則是統一採 Excel

的格式以電子郵件附件方式移案，考量將來合作國日益增加，建議統一垃圾郵件的移案方式以及檔案格式，以縮短作業時間並提升分析、移案效率。除了國際合作之外，隨著行動通訊裝置的普及，在享受網路科技所帶來便捷服務的同時，網路用戶權益的保障除了加強認證機制與國際合作之外，配合宣導建立正確的資訊安全防護觀念，培養良好的網路使用習慣，方能將資訊安全的威脅降到最低，確保優質的網路使用環境。

陸、 附錄

一、 臺日防制垃圾郵件雙邊交流會議吳簡任技正銘仁致詞全文

Good evening Ladies and Gentlemen,

I'm Mr. Ming-Jen Wu, Resource and Technologies Department's Senior Technical Specialist of NCC.

I'm honoured to be with all representatives of the Japanese competent authorities and report the current status on combating Spam Emails in Taiwan. On behalf of NCC, I would like to say thank you for The Ministry of Internal Affairs and Communications (MIC) and Japan Data Communications Association (JADAC) to hold a JP/TW bilateral technical meeting here and share working experiences with each other today.

It is my pleasure to meet Mr. Fujinami Koichi, Director, Telecommunications Consumer Policy Division of MIC and Mr. Kaoru Nishimatsu, Director, Anti-Spam Consultation Center of JADAC and all our honoured guests to the opening of this meeting.

Now, I'd like to introduce my colleagues as you all will be seeing a lot of us in the next 4 days and we hope that we will have a chance to meet and chat with all of you:

Mr. Juin-Wei (Jeff) Chen, specialist of NCC's Legal Affairs Department , responsible for today's meeting power point presentation tasks and discussions about legal affairs.

Mr. Chan-Hsiang (Ken) Lin, associate Technical Specialist of NCC's Legal Affairs Department, is responsible for today's photography and discussions about technical affairs.

Last but not least, I want to express my heartfelt thanks and gratitude to Director Mr. Fujinami Koichi and Director Mr. Kaoru Nishimatsu, for all your efforts and supports, MIC and JADAC should be proud of the outstanding achievements of promoting anti-spam activities and international collaborations. In the mean time, We(NCC) are also grateful for the support of officials from MIC and staff members from JADAC.

Lastly, I would like to wish JP/TW Bilateral Meeting and LAP10 meeting every success. Thank you!

二、 臺日防制垃圾郵件雙邊交流會議簡報全文

Good evening Ladies and Gentlemen.

As the representative of Taiwan National Communications Commission, I am very honoured to be with all representatives and report the current status on combating Spam Emails in Taiwan. Please do not hesitate to make comments or share your feedback with me.

I've divided my presentation into four parts:

1. International cooperation on anti-spam work and strategies.
2. Status on Spam Emails and the Complaints Process.
3. Legislation Promotion on Spam Act in Taiwan (An overview of the (draft) of Abusing Commercial Electronic Mail Management Act in Taiwan).
4. Future Works

1. International cooperation on anti-spam work and strategies

In recent two years, NCC has setup an email trap called "honeypot" to gather spam emails, and it has come out that there are 90% spam come from overseas.

In this regard, NCC will urge more international cooperation on spam and will consider it as a core and primary mission in the future.

NCC has three spam emails sources. The first source is the spam information or data exchanged with collaboration countries; the second source is the spam reported by Taiwanese receivers; the third source is the spam captured by the Honey Pot system set up by NCC.

Every year, the amount of all the cases collected from other countries, top one is Brazil, and the second is South Korea. For those cases found in Taiwan, and transferred outside Taiwan, top one is the U.S., and the second

is South Korea.

To be brief, there are two different types of SPAM data sources are using to receive SPAM data files in Taiwan, international and domestic.

The international SPAM data sources are from SPAM cooperating countries of Taiwan as Japan, South Korea, Brazil and the U.S.

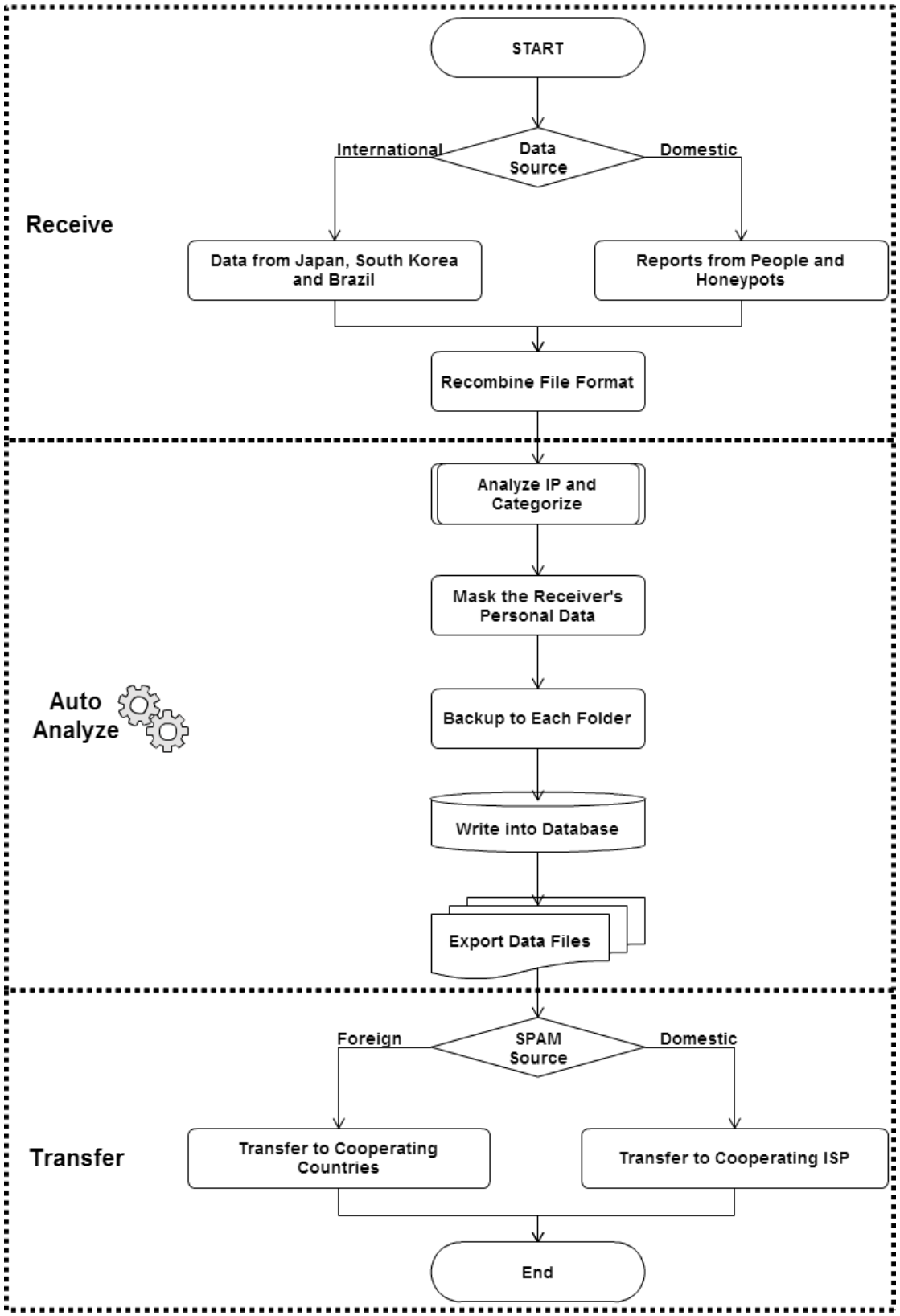
The cycle of receiving data files from Japan is once per week, the cycle of receiving data files from South Korea and Brazil and the U.S. are once per month.

All data files from cooperating countries of Taiwan are already checked by them and confirmed the IP of these SPAM are from Taiwan.

However, in order to let the data files can be easier to analyze, the data files will be recombine to same format no matter where it is from.

2. Status on Spam Emails and the Complaints Process

The SPAM system is complicated, but can be simplifies to three process blocks as receive, analyze and transfer. Below is the flow chart and its introduction.



International and Domestic SPAM System Workflow Chart of Taiwan.

2.1 Incoming international SPAM Data sources from Taiwan's Collaborative Partnerships

2.1.1 Japan

First, I want to introduce NCC'S latest statistics about SPAM data exchange from Japan transfer to Taiwan.

From the chart and graph, the numbers reach to its climax in 2013 is in November (before the Christmas day). In the figure, in 2014,we can find that the numbers are increasing gradually and reach its climax in April. I think maybe we could try to discover the reasons why the numbers of SPAM increase so drastically in April.

There are mainly three phases to deal with SPAM emails, that is receive, analyze and transfer.

Next, I want to introduce the brief workflow of Japan's SPAM data exchange with Taiwan. In the receive stage, the format of data files from Japan's Japan Data Communications Association (JADAC) is a kind of file named LHZ. Once the format of data files have been recombined and unified, the analyze process will then start. At first the process will analyze the email source IP of SPAM data by computer program and automatic categorize them by JADAC.

As to prevent from the leakage of personal data, the program will mask the receivers' personal data like email address and IP after analyze completed. Then the program will backup all original data files and masked data files by the categorize result. When backup is done, all information of SPAM as subtitle, source IP, data source and analyze result will be write into the database. Then the program will export several types of files by the using

of transfer process to Taiwan.

In the transfer stage, SPAM data transfer can finally classify to international and domestic too as receiving SPAM data. International transfer will transfer data files to SPAM cooperating countries of Taiwan.

2.1.2 South Korea

In the next slides, I want to introduce NCC'S latest statistics about SPAM data exchange from South Korea transfer to Taiwan.

From the chart and graph, the numbers reach to its climax in 2013 is in November (before the Christmas day). In the figure, in 2014, we can find that the numbers are increasing gradually and reach its climax in April. I think maybe we could try to discover the reasons why the numbers of SPAM increase so drastically in April.

There are mainly three phases to deal with SPAM emails, that is receive, analyze and transfer.

Next, I want to introduce the brief workflow of South Korea's SPAM data exchange with Taiwan. In the receive stage, The format of data files from South Korea's Korea Internet Security Agency(KISA) is a kind of file named EML. Once the format of data files have been recombined and unified, the analyze process will then start. At first the process will analyze the email source IP of SPAM data by computer program and automatic categorize them by KISA.

As to prevent from the leakage of personal data, the program will mask the receivers' personal data like email address and IP after analyze completed. Then the program will backup all original data files and masked data files by the categorize result. When backup is done, all information of SPAM as

subtitle, source IP, data source and analyze result will be write into the database.

In the transfer stage, the program will generate EML files for Taiwan(NCC) and Taiwan can use the FTP Client easily to download exchange files in the FTP SERVER.

In the transfer stage, SPAM data transfer can finally classify to international and domestic too as receiving SPAM data. International transfer will transfer data files to SPAM cooperating countries of Taiwan.

2.1.3 Brazil

In this slides, I want to introduce NCC'S latest statistics about SPAM data exchange from Brazil transfer to Taiwan.

From the chart and graph, the numbers reach to its climax from may to august in 2014. If we compared to the numbers involved and numbers spam in the figure, we can clearly find that the numbers are increasing so drastically and reach its climax . I think there must be many spammers use dynamic IP to send spam emails from may to august, maybe we could try to discover the reasons beneath the numbers.

There are mainly three phases to deal with SPAM emails, that is receive, analyze and transfer.

Next, I want to introduce the brief workflow of Brazil 's SPAM data exchange with Taiwan. In the receive stage, the format of data files from Brazil's Brazilian National Computer Emergency Response Team (CERT.br) is a kind of file named MBOX and it will be converted into TGZ files. Once the format of data files have been recombined and unified, the analyze process will then start. At first the process will analyze the email source IP of SPAM

data by computer program and automatic categorize them by CERT.br.

As to prevent from the leakage of personal data, the program will mask the receivers' personal data like email address and IP after analyze completed. Then the program will backup all original data files and masked data files by the categorize result. When backup is done, all information of SPAM as subtitle, source IP, data source and analyze result will be write into the database. Then the program will export files by the using of transfer process to Taiwan.

In the transfer stage, SPAM data transfer can finally classify to international and domestic too as receiving SPAM data. International transfer will transfer data files to SPAM cooperating countries of Taiwan.

2.1.4 International Cooperation on anti-spam work

According to NCC'S latest statistics, about 97% of reported spam emails were from overseas but only a small number of government agencies work with us to exchange of spam information, thus NCC is eager to take this opportunity to invite more countries to establish cooperation with us on the anti-spam issue.

NCC selected a random sample of spam emails to survey the main spam sources. In this figure, the average of this data, the top 3 sources of spam sent to Taiwan in 2014 are the US, China and Singapore. As for the United States the spam amount has been decreasing, but the spam amount has been growing in China.

NCC has also developed relationships of spam data exchange with Anti-Spam Consultation Center (ASCC) of Japan Data Communications Association (JADAC), Korea Internet Security Agency (KISA), Brazilian

National Computer Emergency Response Team (CERT.br), and Federal Trade Commission (FTC). Such spam data exchanges with the U.S. and Brazil are one-way, while data exchanges with Japan and South Korea are mutual.

2.2 SPAM Data originating from Taiwan to its Collaborative Partnerships

2.2.1 Japan

In this slides, I want to introduce NCC'S latest statistics about SPAM data exchange from Taiwan transfer to Japan.

From the chart and graph, the numbers reach to its climax in 2013 is in June(it is just the time that school children's summer vacation is around the corner).In the figure, in 2014,we can find that the numbers are increasing gradually from June and reach its climax in August. I think maybe we can conclude that summer vacation could be the reasons why the numbers of SPAM increase so drastically in 2013 and 2014.

Next, I want to introduce the brief workflow of Japan's SPAM data exchange from Taiwan transfer to Japan. In the first stage, The format of data files from Taiwan's National Communications Commission(NCC) is a kind of TXT file . Once the format of data files have been recombined and unified, the analyze process will then start. At first the process will analyze the email source IP of SPAM data by computer program and automatic categorize them by NCC.

As to prevent from the leakage of personal data, the program will mask the receivers' personal data like email address and IP after analyze completed. Then the program will backup all original data files and masked data files by the categorize result. When backup is done, all information of SPAM as

subtitle, source IP, data source and analyze result will be write into the database. Then the program will export several types of files by the using of transfer process to JADAC.

In the transfer stage, SPAM data transfer can finally classify to international and domestic too as receiving SPAM data. International transfer will transfer data files to SPAM cooperating countries of Taiwan.

2.2.2 South Korea

In the next slides, I want to introduce NCC'S latest statistics about SPAM data exchange from Taiwan transfer to South Korea.

In the figure, we can find that the numbers are increasing rapidly and rise to its climax in July 2014 . I think maybe we could try to discover the reasons why the numbers of SPAM increase so drastically in April.

Next, I want to introduce the brief workflow of South Korea's SPAM data exchange from Taiwan transfer to South Korea. In the first stage,The format of data files from Taiwan's National Communications Commission(NCC) is a kind of TXT file . Once the format of data files have been recombined and unified, the analyze process will then start. At first the process will analyze the email source IP of SPAM data by computer program and automatic categorize them by NCC.

As to prevent from the leakage of personal data, the program will mask the receivers' personal data like email address and IP after analyze completed. Then the program will backup all original data files and masked data files by the categorize result. When backup is done, all information of SPAM as subtitle, source IP, data source and analyze result will be write into the database.

In the transfer stage, the program will generate EML files for South Korea (KISA) and Taiwan can use the FTP Client easily to upload exchange files to South Korea in the FTP SERVER.

In the transfer stage, SPAM data transfer can finally classify to international and domestic too as receiving SPAM data. International transfer will transfer data files to SPAM cooperating countries of Taiwan.

2.2.3 U.S.A

In the next slides, I want to introduce NCC'S latest statistics about SPAM data exchange from Taiwan transfer to the U.S.

In the figure, in 2014, we can find that the numbers are increasing gradually from May and reach its climax in August. I think maybe we can conclude that summer vacation could also be the reasons why the numbers of SPAM increase so drastically in 2014.

Next, I want to introduce the brief workflow of SPAM data exchange from Taiwan transfer to the U.S . In the first stage, The format of data files from Taiwan's National Communications Commission(NCC) is a kind of original EML file .

As to prevent from the leakage of personal data, the program will mask the receivers' personal data like email address and IP after analyze completed. Then the program will backup all original data files and masked data files by the categorize result. When backup is done, all information of SPAM as subtitle, source IP, data source and analyze result will be write into the database.

In the transfer stage, SPAM data transfer can finally classify to international and domestic too as receiving SPAM data. International transfer will

transfer data files to (Federal Trade Commission，FTC),one of the SPAM data exchange cooperating countries of Taiwan.

2.2.4. SPAM Data captured by the Honey Pot system set up by NCC

The domestic SPAM data sources are from reports of people and honey pots in Taiwan. In order to meet the needs of people, the cycle of receiving data files from domestic sources is once per week. The data files received from domestic sources are includes not only domestic SPAM (email source IP from Taiwan) but also international SPAM (email source IP from foreign). However, in order to let the data files can be easier to analyze, the data files will be recombine to same format no matter where it is from.

Upon receipt, those emails will be analyzed by our NCC mail system to check if its IP address is located in the countries that have cooperation activities with us. As those spam emails whose IP address is located in collaboration countries will be exchanged to that country. One very important thing to consider is the latest implementation of Taiwan Personal Information Protection Law, the personal information of the Taiwanese reporter should not be disclosed, so we will try to mask out the reporter's personal information before the exchanged spam data is sent out to collaboration countries. If the source of spam is inside Taiwan, as Spam Act has not been passed, we usually request the IASP – Internet Access Service Provider, to help confirm the IP, find the spammers and give them a warning or even forbid them to use the internet for a certain period of time.

Among the three kinds of sources, the current spam NCC deal with the most are from the international exchanges, in this way, we have seen a

certain decrease in the spam sent from Taiwan. However, this does little help to decease the total spam amount received in Taiwan. To better reduce the quantity of spam, we are now planning to set up more Honey Pot systems and increase the data exchanged with collaboration countries in the hope to combat the cross-border spam more effectively.

To sum up, nowadays in relation to combat SPAM emails in Taiwan, there is still no law to specify or clarify the rule of sending commercial e-mail, which means no appropriate regulation applicable to regulate sending email.

As the main measure to handle SPAM issues, the competent authorities have taken steps on cooperating with private institutions.

When providing e-mail services, the IASPs have been requested to specify the agreement between the subscribers and the IASPs, which rules that under the circumstances the subscribers send email repeatedly and those repeated emails are confirmed as SPAM, the IASP may take the necessary enforcement procedures, such as suspend port25 for a period of time to avoid causing further interference or damage.

Therefore in the present time, if the user has received a spam email, the receiver could provide the original spam email to NCC or the IASPs and file a complaint.

Then NCC or the IASPs would request the ISPs who offer the sender email service to confirm the communication records by matching the originating IP of the mail header and according to the service agreement which between the IASP and the sender to take measures to combat spam emails.

3. An overview of the (draft) of Abusing Commercial Electronic Mail

Management Act in Taiwan

Due to the increasing development of ecommerce and the ubiquity of the internet, email has become a primary means of communication in business, as well as marketing goods or services. In comparison to other traditional marketing tools, email has the advantages of convenience, low cost, and easily distributed in large volumes at high speeds across countries.

However, as a marketing tool it has been increasingly abused; consequently, recipients must spend a considerable amount of time in dealing with mass commercial emails (spam), which not only wastes time, but also impedes legitimate communications. It also leads to network congestion as it exhausts system service resources because of the extremely high number of unsolicited commercial email. Moreover, email service providers expend great efforts in dealing with the situation. In addition to hindering the communication services, it has seriously affected usage.

Moreover, based on the anonymity of the net, if the sender does not reveal their true identity, the recipients have no means to reject such email, which can lead to being continually bombarded with such emails; it also makes it very challenging to claim for compensation.

Thus, commercial email abuse has damaged the recipient's interests, as well as the service providers' network facilities and services. In order to protect consumers and providers and enhance the security of the net, the United States, Australia, Japan, Korea, Singapore, Hong Kong, and China among others are actively developing laws to regulate such behavior. For instance, the EU requires member states to pass relevant directives on privacy and electronic communications to contain criteria on commercial email. Some countries, such as Germany, France, Italy, have already passed relevant legislation. As such, it can be said that controlling commercial email abuse has become a regulatory trend.

In order to enhance the IT infrastructure in Taiwan, facilitate efficiency online, minimize harassment from commercial email abuse, and enhance network security and efficiency, the government of Taiwan has referred to the latest laws in the US, Japan, the EU, among others as benchmarks to examine the characteristics of commercial email abuse. Subsequently, the draft of the Abusing Commercial Electronic Mail Management Act has been drawn up encompassing five aspects: action prior to sending, condition of legally sending email, options for legal action, the rights and obligations of service providers, and a supporting mechanism. The main points of the Draft are as follows:

I. A sender must abide by the following regulations when sending commercial email: (Draft 4)

- If the recipient does not reply to the initial mail, it should be deemed as refusal to receive further email correspondence.
- The initial email must include a free reply function.
- Commercial email must be marked in the subject line with the wording - “Commercial”, “Advertisement” or other words that can identify it as commercial email.
- Commercial email must provide accurate header information.

II. The following actions of senders are forbidden:

- Sending follow up commercial emails without the prior consent of recipients.
- Sending commercial email despite being aware of the recipient expressing disapproval of receiving commercial mail.
- Sending commercial email despite being aware of false or misleading statement in the subject line.
- Sending commercial email despite being aware of a false header in the commercial email.
- Sending commercial email that uses a dictionary attack or other

similar methods as publicly announced by the competent authority. (Draft 5)

III. The competent authority may order ESPs or IAPs to take necessary measures to prevent commercial email abuse. By providing justifiable grounds, ESPs and IAPs may refuse to transmit or receive the sender's email; they will also be required to provide an appeal mechanism for disputes arising from senders using a dictionary attack or other methods as publicly announced by the competent authority. (Draft 6)

IV. A recipient may claim for compensation against a sender that violates Article 4 or Article 5. In view of the damages that are difficult to ascertain, the total amount of compensation determined under the preceding two paragraphs is calculated by not less than TWD500 and no more than TWD2000 per person per commercial email, with the exception of recipients proving damages exceed the pro forma amount aforementioned. (Draft 7)

V. The advertiser or advertising agent that is aware or may have been aware that the sender is abusing commercial email, or a party that compiles or sells email addresses without the recipients' approval, or a party that supplies computer programs that can abuse commercial email should be held jointly liable for prosecution and compensation damages. (Draft 8)

VI. Having been empowered by not less than 20 persons and also having been permitted by the competent authority, a foundation may bring litigation of compensation of damages on its behalf, and may request ESPs, IAPs, advertisers or advertising agents to provide data on the sender. (Draft 9)

VII. Qualification of class action, the procedure to bring litigation of class action, etc is specified. (Draft 9 to 15)

VIII. ESPs or IAPs that fail to take necessary measures to prevent

commercial email abuse or refuse to provide data without justifiable grounds or provides false information, shall be imposed with a fine by the competent authority; an advertiser or advertising agent that refuses to provide without justifiable grounds or provides false information shall also be imposed with a fine by the competent authority. (Draft 16, 17)

IX. A party that violates Paragraph 5 of Article 9 shall be imposed with a fine by the competent authority. If the violation is of a serious nature, the competent authority may annul the status of litigation. (Draft 18)

4. Future Works

In order to attack spammers and promote international cooperation on anti-spam work and strategies effectively, here are actions we've adopted:

4.1 Short-term:

(1) Establish information exchange channel.

From the incoming international spam sources mentioned above, most spam came from US., Singapore ,China, UK and so forth. We're working on contacting the relative official managements to look for cooperation. Developing close working relationship with Service Providers to provide new spam reporting tools.

(2) Continuing to promote international cooperation on anti-spam work and strategies.

(3) Proceeding legislation to establish a standard of judgment.

4.2 Mid-term:

(1) Sign up bilateral MoU.

(2) Arrange visits.

(3) Steering consecutive official conferences.

4.3 Long-term:

(1)Coordinate industry cooperation.

(2)It would be best to proceed as soon as the anti-spam act has been passed.

(3)The Government could intermediate the cooperation of industry on Anti-Spam.

In order to build up Spam information exchange channel to each country, we are always pleased to participate in international conferences, such as London Action Plan, to establish mutual collaboration channel and get more experience on the topic of regulating Spam.

Draft of Abusing Commercial Electronic Mail Management Act

Article 1 (Purpose)

The Abusing Commercial Electronic Mail Management Act (hereinafter referred to as "this Act") is specifically enacted for the purposes of maintaining the convenience use of the Internet, minimizing harassment resulted from abusing commercial electronic mail, and enhancing the security and efficiency of the Internet environment.

Article 2 (Definitions)

(1) The terms adopted herein are defined as follows:

(a) “Commercial electronic mail (hereinafter referred to as "commercial E-mail")” means any E-mail was transmitted thru the Internet for the purpose of promoting products or commercial services, except those on existing transaction or relationship.

(b) “Electronic mail address (hereinafter referred to as "E-mail address")” means the identifiers of the E-mail server and the E-mail subscriber account.

(c) “Header information” means the source, routing information, destination, originating date, and any other information attached to an E-mail, by which the

Email sender can be accurately identified.

(d) “Electronic mail service provider (hereinafter referred to as "ESP")” means one that provides the service for conveying, transmission or reception of E-mail by installing E-mail server.

(e) “Internet access service provider (hereinafter referred to as "IAP")” means an enterprise that provides subscribers to access the internet by wire, wireless or any other manner.

(f) “Sender” means a juridical person, group or individual who initiates commercial E-mail.

(g) “Recipient” means a juridical person, group or individual who make use of the E-mail address to receive commercial E-mail

(h) “Abusing commercial E-mail” means the behavior of the sender violates Article 4 or Article 5.

(i) “Dictionary attack” means the indifferent sending of Email, of which the address was generated by using software or program that combining alphabetic letters, signs, or numbers at random.

(2) The term “those based on existing transaction or relationship” referred in subparagraph (a) of the preceding paragraph means the information in an E-mail comply with one of the followings:

(a) To make necessary contact with a commercial transaction that the recipient previously agreed to enter into with the sender;

(b) To provide warranty, recall, recycle or security information with respect to products or services required by the recipient;

(c) To inform the recipient of significant transactional information, including the term of transaction, any change in the recipient’s rights or liability, or the execution status concerning an ongoing contract;

(d) To deliver products or services, as well as any update or upgrade, in accordance with the conditions of a transaction that the recipient has previously agreed to enter into with the sender.

Article 3 (Competent Authority)

The competent authority in this Act is the National Communications Commission (NCC).

Article 4 (Condition of lawful sending E-mail)

(1) A sender must abide by the following regulations to send the commercial E-mail:

(a) The Initiative E-mail must include a free-charged reply function or contact method for the recipients to opt in of receiving similar commercial E-mail from the same sender, and must note that if the recipient doesn't reply email, it should be deemed as refusal to receive further Email.

(b) The further E-mail that the recipients opt in of receiving must provide free-charged reply function or contact method for opting out of receiving similar commercial E-mail from the same sender;

(c) The commercial E-mail must mark with the additional wording - "Commercial", "Advertisement" or other identifiers publicly announced by the competent authority–enough to identify the commercial E-mail in the subject line;

(d) The commercial E-mail must provide the accurate header information;

(e) The commercial E-mail must contain the sender's and principal's name or title, and valid office, business place or domicile thereof.

(f) The commercial E-mail sending contract between the recipient and the sender against the provisions of the preceding paragraph is void.

Article 5 (Forbidden behavior)

The following actions of senders are forbidden:

(a) Still sending the following commercial E-mail without the recipients' consent after first commercial E-mail had been initiated;

(b) Still sending the commercial E-mail if the sender knew, or might know the recipients had expressed the rejection on receiving the commercial E-mail;

(c) Still sending the commercial E-mail if the sender knew, or might know the subject of the commercial E-mail had false or misleading statement;

(d) Still sending the commercial E-mail if the sender knew, or might know the commercial E-mail has false header;

(e) For the purpose of sending commercial E-mail that makes use of dictionary attack or other sending methods publicly announced by the competent authority.

Article 6 (The power of the competent authority and the right of service providers)

(1) The competent authority may order ESPs or IAPs to take necessary measures to prevent abusing commercial E-mail.

(2) The necessary measure in preceding paragraph shall be publicly announced by the competent authority.

(3) With the doubt of obstacle of against service providing and justifiable grounds, ESPs and IAPs may reject to transmit or receive the sender's E-mail and must provide appeal mechanism for disputes resolution under the condition that the sender made use of dictionary attack or other measure publicly announced by the competent authority.

(4) Within 14 days after rejecting the transmission and receiving of the specific sender's E-mail, the service provider mentioned in the preceding paragraph must submit the communication record to the competent authority and preserve the record in the specific period. The range, format, preservation period and other enforcement of the communication record shall be ruled by the competent authority.

Article 7 (The compensation of damages of tort)

(1) A sender who violates Article 4 or Article 5 and therefore prejudices the recipients is bound to compensate for the damages.

(1) A recipient may claim a reasonable compensation in money even if such damage is not a purely pecuniary loss.

(2) The total amount of compensation determined under the preceding two paragraphs is calculated by not less than NT$500 but no more than NT$2000 per person per commercial E-mail, except the recipients could prove the damages exceed the pro forma amount of compensation above.

(3) If multiple recipients are damages suffered derived from the same cause, the total amount of compensation of damages will not exceed NT$20,000,000. Provided that the interest obtained from the same cause exceeding NT$20,000,000 toward the sender, the total amount of compensation of damage should be under the interests acquired.

(4) The claim of the paragraph (2) shall not be transferred or inherited, except it has been promised by contract or has been filed litigation.

(5) The claim for compensation of damages of the paragraph (1) and (2) is extinguished by prescription, if not exercised within 2 years from the date when the damages and the person bound to compensate became known to the damaged person. The same rule is applied if 5 years have elapsed from the date when the act was committed.

Article 8 (Joint and several obligation)

(1) The advertiser or advertising agent, who knew, or might know the sender who violates Article 4 or Article 5, should be charged with the sender with joint liability for the compensation of damages.

(2) The person who gathers or sells E-mail address without the recipients' consent to provide the sender to abuse commercial E-mail should be charged with the sender with joint liability for the compensation of damages.

(3) The person who deliver, transmit, distribute or by using other gratuitous or non-gratuitous methods to supply computer program with the following function to provide the sender to abuse commercial E-mail should be charged with the sender with joint liability for the compensation of damages:

(a) The implementation of dictionary attack;

(b) Address-harvesting without the recipients' consent;

(c) To Send E-mail with the fraud header

(d) Other type of function publicly announced by the competent authority according to technology development.

Article 9 (Class action and information providing)

(1) Having been empowered by not less than 20 persons who were damaged by the same cause led to the event of violation of Article 4 or Article 5 and also having been permitted by the competent authority, a foundation may bring litigation of compensation of damages on its behalf. A party may withdraw the empowerment to bring litigation prior to termination of oral-arguments and must provide notice to the court.

(2) After the litigation being brought in accordance with the provision of the preceding paragraph by the foundation, the court may, on motion or on its own initiative, publish a notice to inform other persons suffering damages due to same cause to empower it to bring litigation in specific period, it may expand the claims asserted for

judgment prior to termination of oral-argument session in the court of first instance.

(3) The empowerment to bring litigation in accordance with the preceding two paragraphs must be granted in document.

(4) For the purpose of validation of defendant's identification, the foundation who had been empowered by damaged party and was permitted by the competent authority may request ESPs, IAPs, advertisers or advertising agents for following information; the requested party may not reject without justifiable grounds:

(a) Name or title of sender;

(b) Valid office, business place, domicile or contact method of sender;

(c) E-mail address of sender;

(d) Internet Protocol which send the E-mail;

(e) Sending time of E-mail;

(f) The pattern or technology type of conveying;

(g) Other information for the identification of the sender designated by the competent authority.

(5) The foundation obtained information in accordance with the preceding paragraph must only used for the litigation in this article.

(6) The ordinance of enforcement, including methods of requesting information by the foundation, and procedures, standards of application fee, period of data retention, designation of provided information and other compliance matters of ESPs, IAPs, advertisers or advertising agents, shall be ruled by the competent authority.

(7) The Time Limit of the claim for compensation of damages of each party in accordance with the paragraph (1) and (2) must be calculated separately.

(8) The relevant portion proceeding of the litigation stopped automatically after the party's empowerment to bring litigation has been withdrawn in accordance with the paragraph (1); the party must move for the assumption of litigation, or the court may, on its own initiative, order the party to assume the litigation.

(9) After the litigation has been brought by the foundation in accordance with this article, the event that a portion of the party withdraw their empowerment which bring the litigation to result in the number of the party less than 20 persons doesn't affect that the remaining portions of the litigation proceed.

(10) If the foundation brings litigation in accordance with this Act, the court fees for the

portion of the claim exceeding NT$600,000 shall be waived temporarily.

Article 10 (The qualification of class action institution)

(1) The foundation in this Act must abide by the following conditions; its bylaw and execution plan of class action must be verified and publicly announced by the competent authority:

(a) The foundation established as a juridical person has total registered assets of NT$10,000,000;

(b) The foundation has been established for more than 3 years after the official approval.

(2) The foundation in this Act must appoint lawyers to litigate on its behalf.

(3) The regulation to the foundation in accordance to paragraph (1) , including methods and procedures of verification, standards of qualification, status of litigation of revocation or annulment, supervision and other relevant matters, shall be ruled by the competent authority.

Article 11 (Regime of publishing inform)

(1) As the litigation proceeds in accordance with Article 9, the court may, with the consent of the foundation, publish a notice to the effect that other persons with damages due to the same cause may join the litigation by filing a pleading within a designated period of time specifying: the transaction or occurrence giving rise to such claim, the evidence, and the demand for judgment for the relief sought.

(2) Other persons with damages due to the same cause may also move the court to publish the notice provided in the preceding paragraph.

(3) A written copy or photocopy of the joiner’s pleading must be served upon all parties to the action.

(4) The publication period of the notice provided for in the paragraph (1) of this article and the Article 9 paragraph (2) must be not less than twenty days and must be disclosed on the court's bulletin board, information network and other appropriate places. Considering its necessary, the court may publish the same notice in official gazettes, newspapers, or other similar means of communication. The expenses for such publication must be advanced by the national treasury.

Article 12 (The limitation of litigation action of class action institution)

(1) The foundation shall have power to perform all procedural acts of the litigation empowered by the party, but the party may restrict its power to make waivers, withdraw, or enter into a settlement.

(2) The effect of a restriction set by one member of the party does not extend to other members.

(3) Any restriction as referred to paragraph (1) must be set out in document as prescribed in the Article 9 paragraph (3) or submitted to the court in pleadings.

Article 13 (Appeal right of the party)

(1) If a party objects to the judgment in a litigation brought pursuant to Article 9 paragraph (1), the party can withdraw the empowerment to bring a litigation and duly institute an appeal under the law before the expiration of the period for appeal by the foundation.

(2) After receiving a judgment’s exemplification, the foundation must immediately notify the party of the outcome, and within 3 days must provide written notice of whether it intends to prefer an appeal.

Article 14 (Necessary fee and rewards of litigation)

(1) The foundation must distribute compensation it receives in litigation to the parties who empowered it to initiate the litigation after deducting the expenses required in those procedures, and may collect necessary fee in advance.

(2) The regulation of necessary fee related to items, collection and other relevant matters shall be ruled by the competent authority.

(3) The foundation must not claim rewards from the party in the litigation referred to Article 9 paragraph (1).

Article 15 (Exclusive jurisdiction of class action)

(1) As to the litigation of compensation concerning damages in this Act, exclusive jurisdiction resides in the district court for the place where the sender’s office, business place and domicile is located.

(2) Provided that the sender is a natural person, and he has no domicile in the R.O.C., or his place of domicile is unknown, then the sender's place of residence in the R.O.C.

shall be deemed to be the sender's place of domicile. While the sender has no place of residence in the R.O.C. or his place of residence is unknown, his last domicile in the R.O.C. shall be deemed to be the sender's place of domicile. If the sender has no last place of domicile, exclusive jurisdiction resides in the district court for the place where the central government is located.

(3) Provided that the sender is a juridical person or a group, and he doesn't have main office place and main business place, or his main office place and main business place are all unknown, exclusive jurisdiction resides in the district court for the place where the central government is located.

Article 16 (The punishment of failure to take necessary measures)

ESP or IAP fails to take necessary measures of Article 6 paragraph (1) as ordered by the competent authority, shall be imposed with a fine of not less than NT$30,000 but no more than NT$300,000 if it failed to take after an order within a prescribed period of time and may result in consecutive fines in each case until full compliance.

Article 17 (The punishment of failure to provide information without justifiable grounds)

ESP, IAP, advertiser or advertising agent is requested to provide sender's personal information by the foundation in accordance with Article 9 paragraph (4) but refuses to provide without justifiable grounds or provides false information, shall be imposed with a fine of not less than NT$30,000 but no more than NT$300,000 if it failed to comply after a order by the competent authority to provide within a prescribed period of time and may result in consecutive fines in each case until full compliance.

Article 18 (The punishment of abusive using personal information)

The foundation which violates Article 9 paragraph (5) shall be impose with a fine of not less than NT$30,000 but no more than NT$300,000, together with an order to improve within a prescribed period by the competent authority. Failure to improve within a prescribed period may result in consecutive fines and annulment of status of litigation if the violation is serious.

Article 19 (The authority of international cooperation)

For the execution affairs ruled in this Act, the competent authority may exchange resources, tracing methods and other relevant information of E-mail with related international organizations.

Article 20 (The procedure of announcement)

The public announcement determined under this Act must be published on official gazettes, except paragraph (4) of Article 11.

Article 21 (The authority of ordinance of enforcement)

The enforcement rules for this Act shall be prescribed by the competent authority.

Article 22 (Effective date)

This Act will come into effect after 6-months promulgation.

Note：This Act is made in Chinese which shall prevail in case of any discrepancy between the English translation and the Chinese original.

三、 日本 the ACTIVE project 惡意程式反制措施

ACTIVE（Advanced Cyber Threats response InitiatiVE） 1

Summary

- "ACTIVE(Advanced Cyber Threats response InitiatiVE)" is a project of providing comprehensive countermeasures against malware by collaborating with ISPs, anti virus vendors, and so on.
- Aiming at preventing malware infection and cleansing malware, ACTIVE will alert Internet users who don't recognize malware infection.

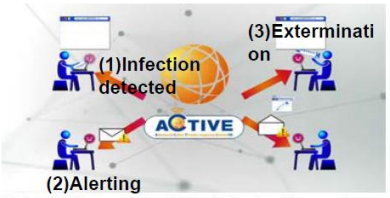
(i)Approach for preventing malware infection

(1)Listing information on malignancy websites.

(2)Alerting users when they are accessing malignancy websites.

(3)Alerting administrator of malignancy websites.

(ii)Approach for malware extermination



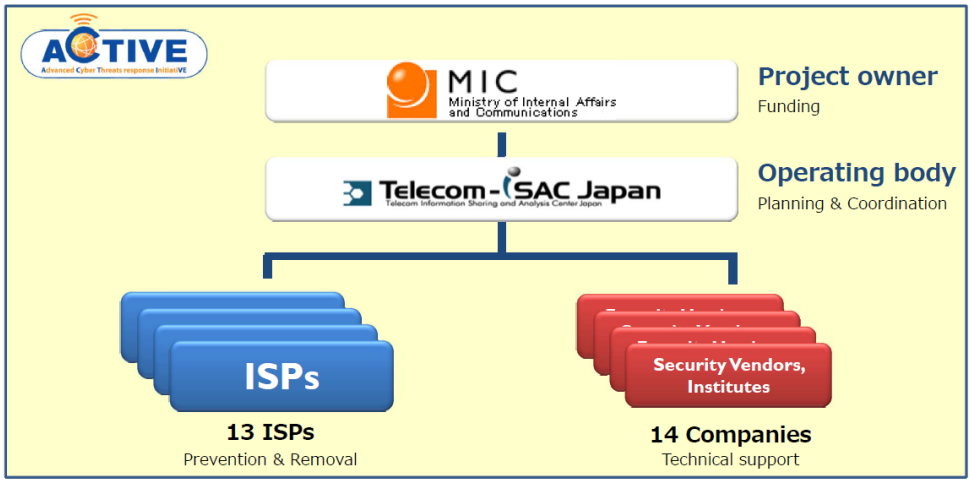
(1)Identifying user's PCs infected by malware.

(2) Sending an alert email to the users to make them aware of current infected condition.

(3)Exterminating malware by complying with instructions in the email.

Team structure of ACTIVE 2

- Ministry of Internal Affairs and Communications (MIC) is the project owner.
- Telecom-ISAC Japan has been operating ACTIVE among participants (planning and coordinating).
- ISPs, Security vendors and Institutes are collaboratively working with ACTIVE.



Current status of ACTIVE

- ACTIVE was launched on 1st November, 2013 supported by MIC.
- Major ISPs and security experts join ACTIVE.
- Activities
  - ACTIVE listed 18,700 URLs of malware embedded websites to ISPs. (2014 March)
  - ACTIVE issued 6,560 warnings to malicious website access users. (2013 November – 2014 March)
  - ACTIVE requested removal of malware to 740 users. (2013 November – 2014 March)

四、「東京宣言」英、日文版

◆ 英文版：

8th October, 2014

10th London Action Plan annual conference (LAP 10 Tokyo)

Tokyo Statement

1. **We**, the participants of the 10th annual London Action Plan conference (LAP 10 Tokyo), met on 7-9 October 2014, in Tokyo, Japan.

2. **We reaffirmed** to continue the discussion through periodic meetings, under the framework of LAP, in order to enhance the cooperative activities pertaining to spam and related electronic threats.

3. **We recognized** the importance of cooperation among members to reduce spam. In addition we **confirmed** that we should encourage new members to join LAP.

4. **We welcomed** the proposal from the Ministry of Internal Affairs and Communications, Japan, for the establishment of 'Anti-Spam library webpages' to enhance the mutual understanding of each member jurisdiction's law enforcement and cutting edge technological approaches to counter spam and **consented** to support their formations.

◆ 日文版：

2014 年 10 月 8 日

ロンドン・アクション・プラン第 10 回定期会合（LAP 10 Tokyo）

東京宣言
（仮訳）

１．我々、ロンドン・アクション・プラン第 10 回定期会合（LAP 10 Tokyo）参加者は、2014 年 10 月 7 日から 9 日まで、日本国東京で会合を行った。

２．我々は、迷惑メールに関する取組み及び関連する電子的脅威についての協力活動を促進するため、LAP の枠組みの下での定期的な会合を通じ、議論を継続していくことを再確認した。

３．我々は、迷惑メールの削減に向けた構成員間の協力の重要性を認識した。加えて、我々は、LAP に新たな構成員が参加するよう奨励すべきであることを確認した。

４．我々は、各構成員の法執行及び迷惑メールに対処するための最先端の技術的取組みについて相互理解を促進するため、日本国総務省から提案のあった“Anti-Spam Library ウェブページ“設置の提案を歓迎し、その構築に協力することに同意した。

五、 第十屆倫敦行動計畫年度會議議程

Day One – October 7

	Subject	Contents	Moderator/Panelist
8:00 – 9:00	Registration		
9:00 – 9:05	Welcome from LAP Secretariat	Welcome, and practical information for the conference.	LAP Secretariat
9:05-9:10	Opening Remarks from the Director General		Mr. Mabito YOSHIDA, Director General, Telecommunications Business Department, MIC Japan
9:10 – 9:30	Keynote address	Telecommunications Policy in Japan	Mr. Koichi FUJINAMI, Director, Consumer Policy Division, MIC Japan
9:30 – 9:45	Group Photo		
9:45 – 10:30	Interpol's Global Complex for Innovation	Interpol's New Cyber Initiative in Singapore	Steve Honiss, Project Manager, Cyber Innovation and Outreach
10:30 – 10:45	Tea Break		
10:45 – 11:45	Enforcement and Update Panel	Reports from members on recent enforcement and other activities	Moderator: Betsy Broder FTC (USA); Lynne Perrault CRTC (CA); Toni Demetriou Dept of Internal Affairs (NZ); Evert Jan Hummelen ACM (NL)
11:30 – 11:45	New Member Update	Report from Hong Kong	Mr. Tony Li, Assistant Director (Support), Office of Communications Authority (OFCA)

11:45 – 12:15	The Japanese Approach to Cyber Security	Japan's Approach Cyber Security; Combatting botnets, malware and other threats	Mr. Kunihiro TSUTSUI, Deputy Director, ICT Security Office, MIC, Japan
12:15 – 1:45	Lunch	Following lunch, we invite you to visit the exhibit on Japan's Smartphone Privacy Initiative	
1:45 – 3:00	SMS Spam	SMS Spam is widespread in some countries, but is virtually nonexistent in other nations. This panel will explore the different experiences and focus on best practices.	Moderator: Toni Demetriou, Dept. of Internal Affairs, NZ; Sandy Gomo, GSMA; Alan Ranger, Cloudmark; Peter Merrigan, DIA, NZ; Patricia Hsue, FTC Max Choo, KISA
3:00 – 3:30	The Japanese Approach to Combatting Spam: Public/Private Collaboration	The activities of the Anti-Spam Mail Promotion Council (ASPC)	Mr. Shuji Sakuraba, Deputy Chairperson, ASPC (Senior Engineer, Internet Initiative Japan, Inc.
3:30 – 3:45	Tea Break		
3:45 – 5:15	Fighting Botnets and Malware: New Challenges, New Tools	Analysis of botnets, and lessons from successful technology and enforcement programs	Moderator: Julia Cornwell-McKean, ACMA (AU); Ken Katayama, Microsoft; Masayoshi Someya, TrendMicro
6:00	Welcome Party	For all LAP members	MIC Japan (host)

LAP 10

Day Two – October 8

	Topic	Content	Moderator/Panelists
9:00 – 9:45	Canada's Anti-Spam Law	Reflections on Three Months of Enforcement and Visions for the Future	Lynne Perrault, CRTC Noel Lachance, Office of the Privacy Commissioner, Canada
9:45 – 11:00	Affiliate Marketing	Roundtable discussion of the threats to consumers caused by affiliate marketing: Various responses	Facilitators Julia Cornell-McKean, ACMA Evert Jan Hummelen, ACM
11:00 – 11:15	Tea Break		
11:15 – 12:30	Initiatives with Developing Economies	Anti-spam initiatives in developing economies: Opportunities for LAP mentoring	Moderator: Betsy Broder, FTC Discussants: Karen Mulberry, ISOC Marco Obiso, ITU
12:30 – 1:45	Working Lunch: Choose your topic	Asia Pacific Regional Activities; Mentoring with ISOC; Training for LAP members	
1:45 – 3:00	LAP Value Proposition	Consideration of a LAP Anti-Spam Index; Review of Existing Value Proposition	LAP Secretariat/MIC
3:00 – 3:15	Tea Break		
3:15 – 4:30	LAP Strategic Plan	Roundtable Discussion of Work Plan: Outreach & Mentoring with developing economies; enforcement initiatives; training program	LAP Secretariat/MIC
4:30 – 5:00	Closing Remarks for Plenary Session	Final Remarks and "See you in Ireland, June 9-11!"	LAP Secretariat/MIC

Do Not Call Network – 9 October 2014
Tokyo, Japan

8:30 Registration

9:00 - Welcome Remarks and Overview

9:15 – 10:30
Home Energy Improvements and DNC Violations
As many countries offer incentives for adoption of energy saving measures, many countries have seen dramatic increases in telemarketing campaigns promoting insulation, energy efficient windows and other home improvements. The DNC network will consider how best to approach these violations.
Facilitator: Julia Cornwell-McKean - ACMA

10:30 – 11:00
Memorandum of Understanding
To continue our efforts to enhance information sharing and coordination among LAP DNC members, we will continue our discussion of forging a multilateral MOU.
Facilitator: Julia Cornwell-McKean - ACMA

11:00 – 11:15 – Break

11:15 – 12:30
Caller ID Spoofing and Automated Calls
As the M³AAWG Voice Telephony Abuse group pursues technological solutions to CLI spoofing, LAP members continue to support the initiative with enforcement, information sharing, and development of a model honey pot. We will discuss the value of honeypots and future enforcement initiatives.
Facilitator: Lynne Perrrault - CRTC

12:30 – 1:30 Lunch

1:30 – 3:00
Affiliate Marketing
List brokers, list assemblers, and other third parties harvest and provide lists of consumers for marketing and other campaigns. Many LAP members have already targeted many of these companies for DNC and fraud violations. We will consider possible joint initiatives to address this threat.
Facilitator: Betsy Broder - FTC

3:00 – 5:00 – Planning for other LAP DNC Activities
A roundtable discussion of future initiatives and improvements, including proposals from LAP Montreal.