TLP:WHITE

國家資安資訊分享與分析中心
(N-ISAC)
會員規章

國家資通安全研究院
中華民國111年12月

TLP:WHITE

修訂歷史紀錄表

項次	版次	日期	說明
1	V1.0	107/05/29	新編
2	V1.1	109/02/13	修訂內容: i. 每頁新增 TLP 標示。 ii. 修訂 3.4 停權、3.5 再申請、4.1 情資內容與 4.2 情資分享等級規範。 iii. 附件 1 一般會員說明增列區域聯防中心。 iv. 新增附件 3。
3	V1.2	109/06/03	修訂內容: i. 修訂 3.會員管理，以完備會員管理相關作業程序。 ii. 修訂附件 2 為 N-ISAC 會員管理作業程序，包含原有之申請作業程序，以及新增 4 項作業程序(資料異動、終止、停權、復權)。 iii. 修訂附件 3 情資分享等級規範，調整說明與新增範例。
4	V1.3	110/10/07	修訂內容: i. 修訂 2.會員，擴大技術會員之範圍，並更新其會員資格與責任項目。 ii. 修訂 4.1 情資內容與 4.2 情資分享等級規範，調整分享等級之說明 iii. 修訂附件 1 為會員說明列表。 iv. 修訂附件 3 情資分享等級規範自動轉發說明。
5	V1.4	111/08/27	修訂內容: 更新行政院資通安全處為數位發展部資通安全署。
6	V1.5	111/12/30	修訂內容:

			更新行政院國家資通安全會報技術服務中心為國家資通安全研究院

資料來源：國家資通安全研究院整理

1. 目的

本規章說明「國家資安資訊分享與分析中心」(National Information Sharing and Analysis Center,以下簡稱 N-ISAC)之會員要求與管理程序，以提升會員間聯繫與信任關係，俾利發揮資安情資分享與交流之效益。

2. 會員

2.1 會員類型

2.1.1 一般會員

係以負責管理特定範圍情資分享之政府機關、關鍵基礎設施(Critical Infrastructure, CI)領域主管機關及國家型電腦緊急應變團隊等。

●領域管理：管理國內特定範圍資安業務之機關或單位。

●應變聯防：協調處理國內特定範圍資安事件之單位。

●執法機關：偵蒐與處理國內網路犯罪事件之機關。

2.1.2 技術會員

係以可提供國內政府機關或 CI 資通安全服務或產品之業者，包含下列兩大類：

●監控服務

– 資通安全威脅偵測管理服務

– 端點偵測與應變服務

●技術支援

– 資通安全檢測服務

– 資通安全健診服務

– 資通安全防護服務或產品

➢防毒軟體

➢網路防火牆

➢電子郵件過濾

➢入侵偵測與防禦

➢應用程式防火牆

➢進階持續性威脅防禦

2.2 會員資格

2.2.1 一般會員

須負責管理國內特定範圍，有效掌握其資安防護現況，並能分享資安威脅預警、異常網路行為通知、事件案例分析及安全防護特徵等情資資訊，在必要時能協調執行緊急應變處理，以建立跨領域合作聯防機制。

2.2.2 技術會員

前述兩大類型業者，須能自主產製資安情資，並具備下列資格項目，由數位發展部資通安全署(以下簡稱數位部資安署)衡酌業務推動及整體運作所需，視情形主動邀請參加。

●監控服務

– 具備資安事件監控與分析能量。

– 具備惡意行為研究與偵測能量。

– 定期產製資安情資並配合法規要求落實提供監控情資。

●技術支援

– 對其服務或產品具備異常偵測與事件監控等防護能量。

– 對其服務缺失或產品漏洞具備及時處理與修補等防護能量。

– 能將漏洞資訊或惡意攻擊資訊轉化為資安情資並提供會員參考。

2.2.3 會員資格限制

N-ISAC 會員資格說明詳見附件 1，而大陸地區人民來台投資許可辦法第三條所定之投資人，以及經濟部投資審議委員會公告之陸資來台投資事業，不得成為 N-ISAC 會員。

2.3 會員責任

2.3.1 一般會員

●分享資安情資或資安事件訊息。

●針對業務轄管範圍(或 CI 領域)，提出資安防護執行報告。

●於 N-ISAC 會員會議中分享資安防護案例或專題報告。

●應定期提供並更新所管理之 IP 位址範圍，以及資安事件統計資訊。

●針對接收國家資通安全研究院提供之中繼站黑名單，每月應回饋其阻擋統計資訊。

2.3.2 技術會員

●監控服務

– 分享資安情資或資安事件訊息。

– 協助會員分析資安事件或惡意程式。

– 於 N-ISAC 會議中分享資安威脅趨勢或資安防護技術等議題。

– 針對接收國家資通安全研究院提供之中繼站黑名單，每月應回饋其阻

擋統計資訊。

– 定期分享資安威脅清單。

●技術支援

– 分享資安情資與資安事件訊息。

– 協助會員分析資安事件或惡意程式。

– 於 N-ISAC 會議中分享資安威脅趨勢或資安防護技術議題。

– 針對接收國家資通安全研究院提供之中繼站黑名單，每月應回饋其阻擋統計資訊。

– 定期分享與自身服務或產品相關資安情資，供其他會員做為資安防護參考。

3. 會員管理

3.1 申請

N-ISAC 會員申請需經過國家資通安全研究院預審與數位部資安署審核，俟數位部資安署審核通過後，由國家資通安全研究院公告會員名稱與代碼於 N-ISAC 平台，申請作業程序詳見附件 2。

3.2 資料異動

N-ISAC 會員資料如有異動，應主動向國家資通安全研究院提出異動申請，以確保聯繫管道與情資交流作業暢通，資料異動作業程序詳見附件 2。

3.3 終止

N-ISAC 會員如無法符合 N-ISAC 會員資格或無法履行會員責任時，應主動向國家資通安全研究院提出終止申請，由國家資通安全研究院提報數位

部資安署核定後，終止其會員身分，並由國家資通安全研究院公告會員名稱與代碼於 N-ISAC 平台，終止作業程序詳見附件 2。

3.4 停權

N-ISAC 會員如違反 N-ISAC 會員規章所要求之事項，且經查證屬實，由數位部資安署召開審查會議，視情節輕重予以停權其會員身分 3 個月至 1 年，停權期間自通知公文之發布日期起算，停權後由國家資通安全研究院公告會員名稱與代碼於 N-ISAC 平台，停權作業程序詳見附件 2。

3.5 復權

停權會員須俟停權期限屆滿方可提出復權申請，應提交改善報告與檢附佐證資料，由數位部資安署召開審查會議，同意復權後由國家資通安全研究院公告會員名稱與代碼於 N-ISAC 平台，若停權期限屆滿後 6 個月未提出復權申請者，視同放棄復權資格，其會員身分將逕行終止，復權作業程序詳見附件 2。

4. 情資交流

4.1 情資內容

N-ISAC 會員應提供真實之情資內容，並依據 4.2 情資分享等級規範確實標示分享等級，情資內容如為特定對象之資安事件通知，則應檢附佐證紀錄以利後續應變處置。

4.2 情資分享等級規範

N-ISAC 採用 Traffic Light Protocol (TLP)情資分享等級規範(附件 3)，N-ISAC 會員透過 N-ISAC 取得之情資內容(包含會議資料)，應遵循 TLP 妥善使用與保護，避免不當之資訊揭露。

4.3 智慧財產權

N-ISAC 之所有情資內容，以及所使用之系統或程式，包括但不限於文字、著作、圖片、照片、影像、插圖、檔案、網站架構、網頁設計等文件、資料或資訊，均由數位部資安署、國家資通安全研究院或其他權利人依法擁有其智慧財產權，受中華民國法律保障，包括但不限於商標權、專利權、著作權、營業秘密等。除另有約定外，任何人不得逕自修改、重製、改作、散布、發行、公開發表、進行還原工程、解編、反向組譯或藉以產生衍生商品或商業服務，如有違反應自行負擔法律責任與相關損害賠償。

5. 其他

N-ISAC 會員不得利用 N-ISAC 平台進行商業行為，其他未盡之事項，將依資通安全管理法相關規範與作業程序辦理，如有任何疑義請向國家資通安全研究院(nisac@nics.nat.gov.tw)反映。

6. 會員規章之公告及修訂

N-ISAC 會員規章由數位部資安署核定後實施，並公布於 N-ISAC 平台與國家資通安全研究院網站，同時以電子郵件通知 N-ISAC 會員，修訂時亦同。