NIST網路安全框架2.0草案解讀

安全運營 (https://www.secrss.com/articles?tag=安全运营) · 綠盟科技研究通訊 (https://www.secrss.com/articles?author=绿盟科技研究通讯) · 2023-09-22

正式更名為“網路安全框架”，強調網路安全治理和供應鏈安全，並強調國際合作與參與。

一. 簡介

NIST的網路安全框架2.0（CSF2.0）草案的目的為產業、政府機構和其他組織提供指導，以降低網路安全風險。它提供了高階（摘要）的網路安全結果的分類，它可被任何組織使用，無論其規模、部門或成熟度如何。該框架並沒有規定應該如何實現這些結果，而是為實現這些結果提供指導。

此框架由三個部分組成：框架核心（Core）、實作層級（Tier）和設定檔（Profile）（註，ver1.0、ver1.1、ver2.0均為此三部分），如圖1所示。設定檔和層級是幫助組織將框架付諸實踐的工具，以在降低網路安全風險方面為行動設定優先順序。

圖1. 網路安全框架的三個主要部分

在製定網路安全框架的過程中，NIST遵循以下要求：

- 採用通用語言
- 適用於許多技術、生命週期階段、部門和用途
- 結果導向
- 基於風險
- 參考各種國際國內標準
- 活的文件（持續更新）
- 兼收並蓄，吸收多方面的觀點為，包括私部門、學術界、公部門等的

二，CSF2.0草案核心

框架核心（Core）提供了一組網路安全結果（按功能/任務、類別和子類別排列），如何實現這些結果的範例，以及關於如何實現這些結果的附加指南（資訊參考），如圖2所示。核心中的網路安全結果聲明反映了跨部門的活動，並且是技術中立的。這些活動不是必須執行的行動清單。為實現網路

安全結果所採取的具體行動將因組織和用例而異，負責這些行動的責任人也會不同。此外，核心中的功能（function）、類別和子類別的順序並不意味著它們應該被實現的順序或它們的相對重要性，其排序是為了交流中的一致性。

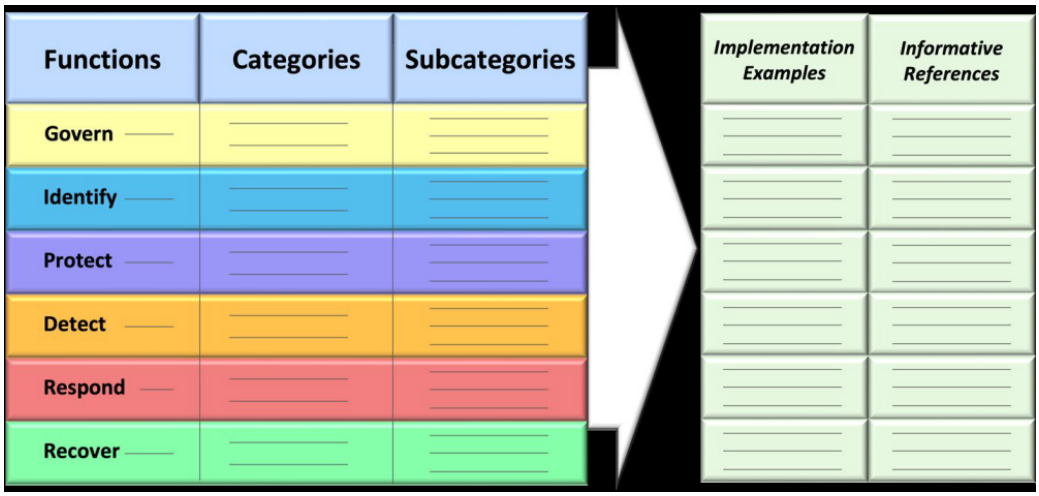

圖2. 網路安全框架核心

2.1 六大功能

CSF2.0草案核心包含有六大功能以及實施例和參考資訊。六大功能為：

治理（GV）-建立和監控組織的網路安全風險管理策略、期望和政策。

識別（ID）-幫助確定該組織當前的網路安全風險。

保護（PR）-使用安全措施來預防或降低網路安全風險。

檢測（DE）-查找和分析可能的網路安全攻擊和妥協。

回應（RS）-對偵測到的網路安全事件採取行動。

恢復（RC）-恢復受到網路安全事件影響的資產和操作。

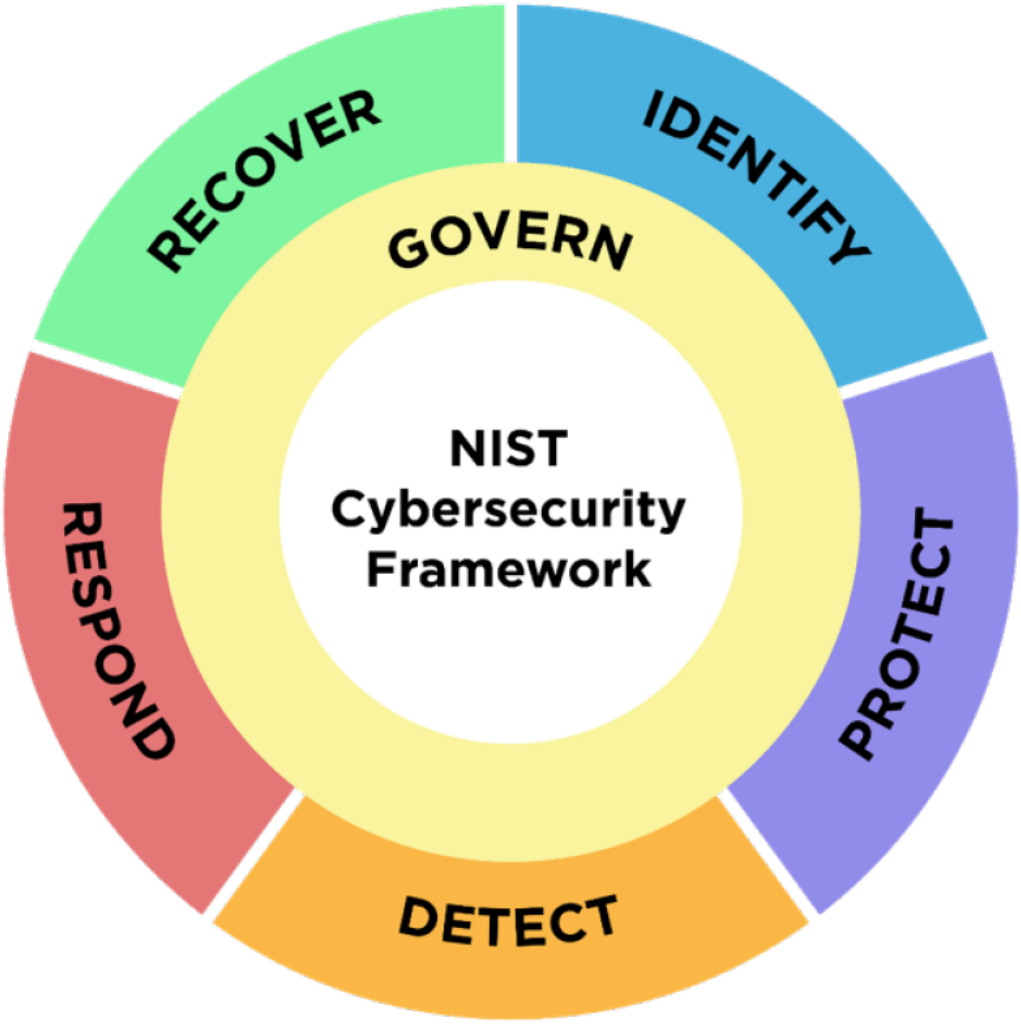

圖3. CFS2.0草案六大功能關係圖

「治理」處在中間的位置，它指示如何實現其他五項功能。要形成和維護一種應對動態網路安全風險的文化，這些功能必須同時實現。治理、識別、保護和偵測應是持續的，回應和復原行動則應隨時準備，並在網路安全事件發生時執行。

類別（Categories）是一個功能對相關網路安全結果群組的細分。子類別（Subcategories）進一步將一個類別劃分為技術活動和管理活動的具體結果。子類別不是完全詳盡的，但有助於實現每個類別的結果。

2.2 實施例和參考訊息

實施例和參考資訊是兩類額外的訊息，以幫助實現框架核心中的功能、類別和子類別。

參考資訊是告知組織實現功能、類別和子類別可參考的標準、指導方針、法規和其他資源。

有時，參考資訊比子類別更具體。

實施例則提供簡明的、行動步驟導向的概念性例子，以幫助實現子類別的結果。

實施例和參考資訊雖然也視作框架核心的組成部分，但以線上的方式提供，以便及時更新。

三．如何使用CSF

網路安全框架可以以多種不同的方式使用，它的使用將根據組織的獨特使命和風險而有所不同。透過了解利害關係人的期望、風險偏好和容忍度，組織可以優先考慮某些網路安全活動，以使他們能夠就網路安全支出和行動做出明智的決定。組織可以以不同的方式處理風險—包括減輕、轉移、避免或接受風險，組織也可以使用該框架監督第三方。

網路安全框架提供了一個靈活的、基於風險的實施方案，可與廣泛的網路安全風險管理流程一起使用，例如「國際標準化組織(ISO) 31000:2018」、「ISO/IEC 27005:2022」、「 SP800-37資訊系統和組織的風險管理架構: 安全和隱私的系統生命週期方法」以及「電力分行業網路安全風險管理流程(RMP)指南」等。

使用該框架的幾種方法：

- 建立和使用框架設定檔來理解、評估和溝通該組織的當前或目標網路安全態勢，並為實現目標網路安全姿態優先考慮結果。
- 評估該組織在網路安全成果方面的成就。
- 用層級來描述網路安全風險管理結果。
- 改善與內部和外部利害關係人的網路安全溝通。
- 管理整個供應鏈中的網路安全風險。

3.1 設定檔

依據框架核心內容中的結果來描述組織目前或目標網路安全姿態的機制稱為框架設定檔。創建和使用配置文件，目的是為了理解、評估、確定優先順序和溝通。

配置文件用於根據組織的任務目標、利益相關方期望、威脅環境、需求和主要實踐（特定部門或技術的實踐），來理解、評估、確定優先級，並定制部門中立和技術中立的核心結果（即功能、類別和子類別），如圖4所示。然後，組織可以優先考慮某些行動，以實現特定的結果，並將這些資訊傳達給內部和外部的利害關係人。

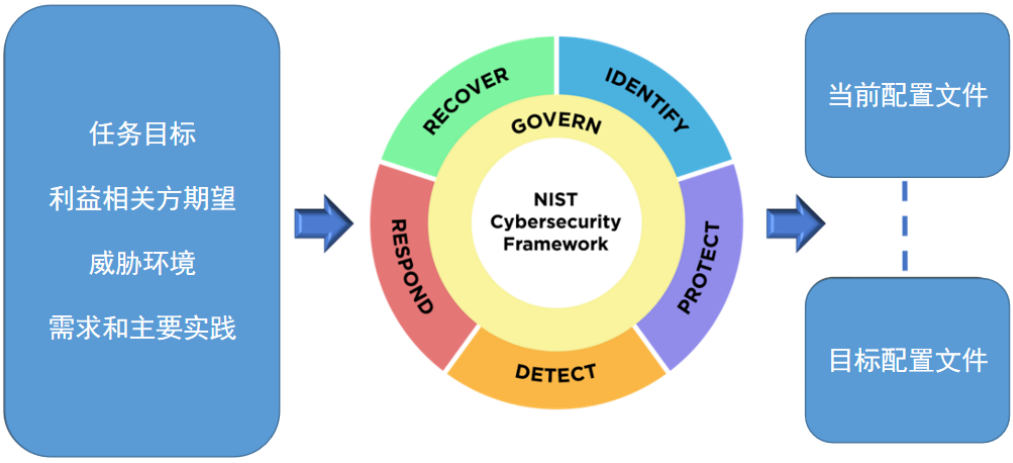

圖4. 設定檔

目前配置檔案涵蓋了組織目前實現（或試圖實現）的核心結果，並描述了每個結果如何實現的或實現到何種程度。

目標設定檔涵蓋了一個組織為實現其網路安全風險管理目標而從框架核心中選擇的需要優先考慮的預期結果。目標設定檔需考慮組織的網路安全姿態的預期變化，如新的要求、新技術的採用和網路安全威脅情報趨勢。

建立和使用設定檔的步驟如圖5所示。

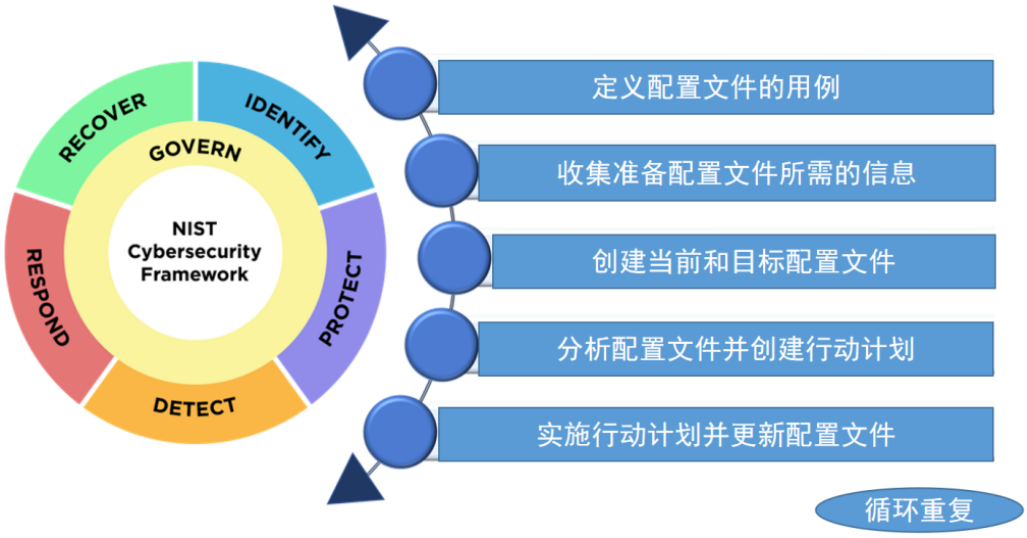

圖5. 建立和使用設定檔的步驟

3.2 層級

層級用於描述網路安全風險管理的結果。層級的選擇有助於為組織內就如何管理網路安全風險設定整體基調，並確定達到選定層所需的努力。層描述了組織的網路安全風險治理和管理結果的嚴謹性，並提供了組織如何看待網路安全風險以及管理這些風險的過程的上下文。

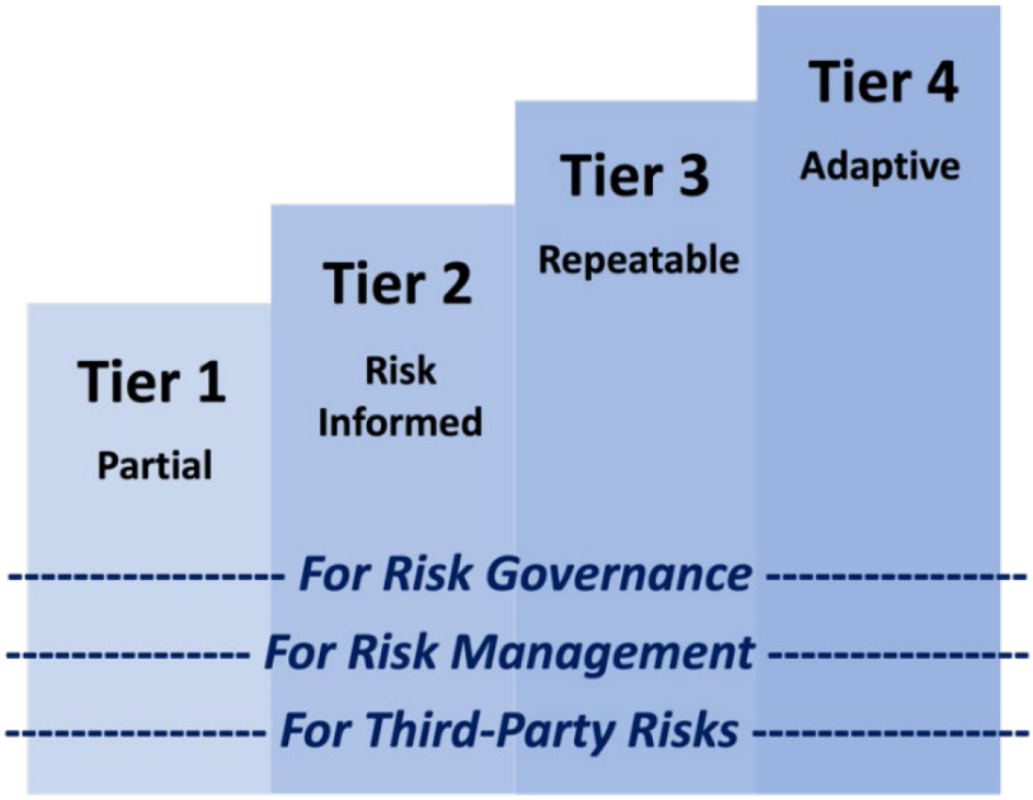

圖6. 框架中的層級

層級從部分的（層級1）到自適應的（層級4）共分4級，如圖6所示。它們反映了從非正式的、臨時的回應到敏捷的、風險已知的和不斷改進的方法的進展。

各層級詳細描述請參考[1]附錄B。這裡僅簡要說明其特徵如下：

層級1：部分的，組織對於風險管理與治理是臨時性的、不定期的，而對於其所用產品和服務的網路安全風險是不了解的。

層級2：了解風險的，風險管理實務得到了管理階層的批准，組織層級意識到網路安全風險的存在，也了解供應鏈中的網路安全風險，但沒有組織內部一致的應對風險的措施。

層級3：可重複的，組織的風險管理實務已正式批准，並以策略的形式表達出來。管理網路安全風險有一個全組織範圍的方法。管理供應鏈網路安全風險的全組織範圍的方法體現在組織的企業風險管理政策、流程和程序中。

層級4：自適應的，整個組織都有一種管理網路安全風險的方法，組織預算是基於對當前和預測的風險環境和風險承受能力的理解。組織根據以往和目前的網路安全活動，包括經驗教訓和預期指標，調整其網路安全做法。組織即時或準即時地了解與其提供和使用的產品和服務相關的網路安全風險，並有一個治理機構處理這些風險。

框架設定檔的建立或更新，可以考慮以層級描述作為指導。組織可能希望在其目前和目標設定檔中包含層級值（1到4）。例如，如果組織領導層已經確定組織應該處於第3層級（可重複的），那麼目前的配置檔案將反映出第3層級治理和管理特徵的實現。目標設定檔將反映出完全實現第3層級的描述所需的任何額外結果。

四．2.0版（草案）與1.1版（2018）的對比

CSF2.0（草案）在CSF1.1的基礎上進行了較大的調整。

4.1 正式更名為“網路安全框架”

文件標題直接更名為網路安全框架，而前面的兩個版本1.0和1.1，其官方名字都是以關鍵基礎設施為對象，「網路安全框架」只是通常的叫法。而在2.0版，取消了「關鍵基礎設施」這個限定詞，表示其重點已被修改為關注世界各地的組織，以反映該框架的廣泛適用性和國際應用。

4.2 強調網路安全治理

在ver2.0草案中，核心功能由原來的5個調整為六個。在ver1.1中，「治理」不是核心功能，只是核心功能「識別」中的一個類別。在ver2.0草案中，「治理」調整到與其他的幾個核心功能平級，體現了對治理的重要性認知。不僅如此，所有的其他功能，都與「治理」交叉。對比如圖7和圖3所示。NIST認為，在CSF 2.0中擴大治理的考量有許多好處。這項新的交叉功能將強調網路安全治理對於管理和降低網路安全風險至關重要，並促進網路安全活動與企業風險和法律要求的一致性。交叉治理功能也與人工智慧風險管理框架草案和隱私框架中的治理功能一致。在人工智慧風險管理框架草案中，AI風險管理的功能有治理、映射、測量和管理人工智慧風險，治理被設計為一個跨領域的功能，以告知並注入其他三個功能，如圖8所示。這些充分說明，在網路安全、人工智慧風險管理、隱私保護等方面，人們逐漸意識到治理的重要性。

圖7. CFS Ver1.1 概念圖[2]

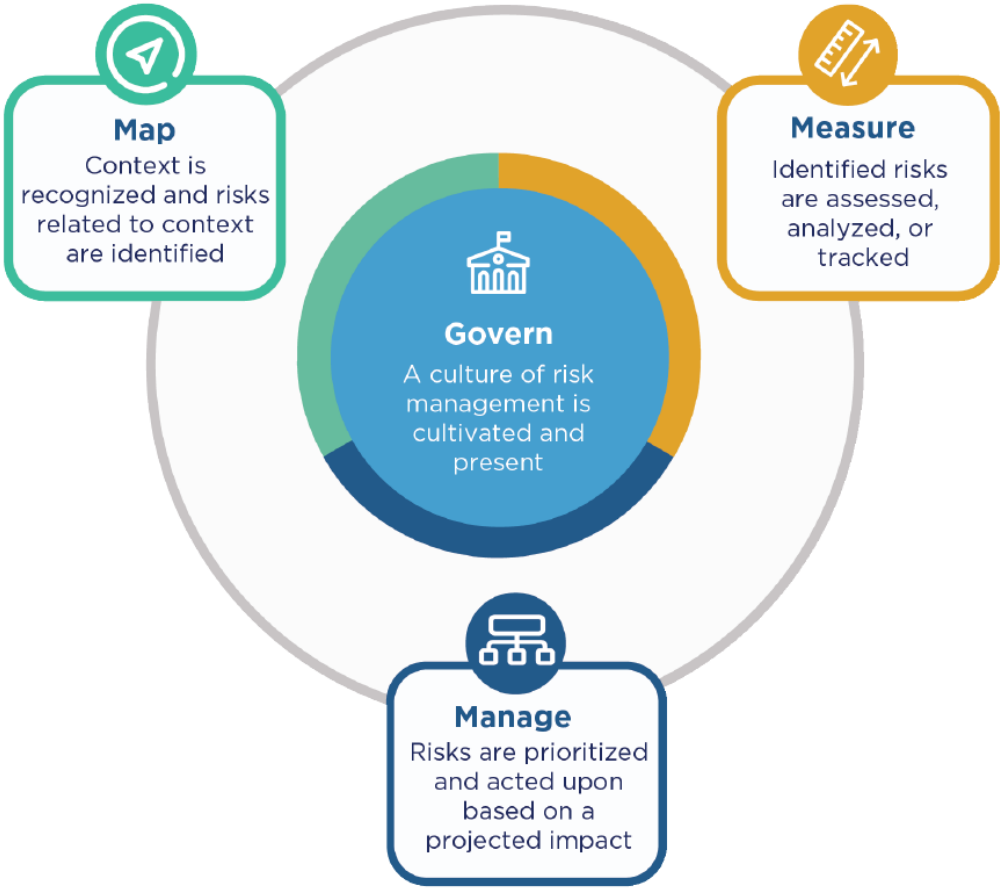

圖8. 人工智慧風險管理架構草案中的功能[3]

4.3 強調供應鏈安全

CSF Ver2.0 草案對供應鏈安全的關注有所增強。它提供了更多關於如何評估和管理供應鏈中的安全風險的指導。這反映了對供應鏈安全的日益重視，並提供了更具體的建議，以確保從供應商和合作夥伴那裡獲得的產品和服務的安全性。Ver1.1與Ver2.0核心功能與類別對比如圖9所示。

Function Unique Identifier	Function	Category
ID	Identify	Asset Management
		Business Environment
		Governance
		Risk Assessment
		Risk Management Strategy
		Supply Chain Risk Management
PR	Protect	Identity Management and Access Control
		Awareness and Training
		Data Security
		Information Protection Processes and Procedures
		Maintenance
		Protective Technology
DE	Detect	Anomalies and Events
		Security Continuous Monitoring
		Detection Processes
RS	Respond	Response Planning
		Communications
		Analysis
		Mitigation
		Improvements
RC	Recover	Recovery Planning
		Improvements
		Communications

(a) Ver1.1核心功能與類別

Function	Category
Govern (GV)	Organizational Context
	Risk Management Strategy
	Cybersecurity Supply Chain Risk Management
	Roles, Responsibilities, and Authorities
	Policies, Processes, and Procedures
	Oversight
Identify (ID)	Asset Management
	Risk Assessment
	Improvement
Protect (PR)	Identity Management, Authentication, and Access Control
	Awareness and Training
	Data Security
	Platform Security
	Technology Infrastructure Resilience
Detect (DE)	Continuous Monitoring
	Adverse Event Analysis
Respond (RS)	Incident Management
	Incident Analysis
	Incident Response Reporting and Communication
	Incident Mitigation
Recover (RC)	Incident Recovery Plan Execution
	Incident Recovery Communication

(b) Ver2.0核心功能與類別

圖9. 框架核心功能與類別

4.4 強調國際合作與參與

CSF的國際使用將提高網路安全工作的效率和效果。CSF1.1在其他國家製定的策略、政策和指導中經常被引用，CSF的早期版本，已有9種語言的翻譯版，包括：西班牙語、日語、葡萄牙語、 阿拉伯語、保加利亞語、波蘭語、印尼語、法語、烏克蘭語。NIST 也將在先前翻譯工作的基礎上，優先與組織合作開發CSF 2.0 的翻譯。NIST 鼓勵提交CSF 的國際翻譯、改編和其他資源。

五. NIST網路安全框架的歷程

在2013年2月的美國總統令13636“提升關鍵基礎設施網路安全”下，NIST於2013年7月發布“提升關鍵基礎設施網路安全框架：初始版”，並於2014年2月發布正式版（ CSF 1.0 ）。NIST於2018 年對該文件進行了修訂更新，發布CSF 1.1。美國網路安全框架的發展歷程如圖10所示。

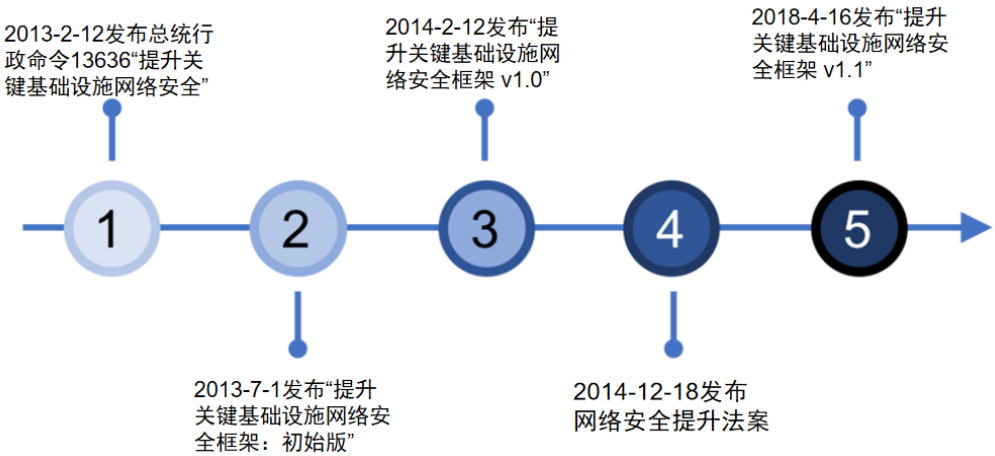

圖10. 網路安全框架的發展歷程

2022年2月22日，NIST發布「關於評估和改善網路安全資源的資訊請求：網路安全框架與網路安全供應鏈風險管理」[4]，進而開啟了框架的修訂之旅。此後，2022年8月，NIST組織了第一次研討會，2023年2月，組織第二次研討會，2023年8月發布2.0版草案。如圖11為CSF2.0的時間軸，NIST預計2023年9月舉辦第三場研討會，CSF2.0正式版預計2024年早期發表。

圖11. CFS2.0時間線

六. 小結

隨著技術的發展以及全球網路安全態勢的變化，NIST適時地對網路安全框架進行了更新，使其更符合網路安全保障的需要。同時，NIST將其網路安全框架推廣到國際應用，一方面彰顯其網路安全大國地位，另一方面也進一步增強了其網路安全領域的國際影響力。

參考文獻

1. The NIST Cybersecurity Framework 2.0, Initial Public Draft, August 8, 2023

2. Amy Mahn,Cherilyn Pascoe, It's a Journey…Where is NIST Headed with the Cybersecurity Framework,RSAC2023

3. NIST, Artificial Intelligence Risk Management Framework (AI RMF 1.0),January 2023

4. https://www.govinfo.gov/content/pkg/FR-2022-02-22/pdf/2022-03642.pdf

內容編輯：創新研究院李德全

責任編輯：創新研究院董炳佑

安全營運 (https://www.secrss.com/articles?tag=安全运营)

相關資訊

安全存取服務邊緣(SASE) 產業發展現況及未來發展趨勢
(https://www.secrss.com/articles/62092)

安全營運 (https://www.secrss.com/articles?tag=安全运营) · 資訊安全與通訊保密雜誌社
(https://www.secrss.com/articles?author=信息安全与通信保密杂志社) · 2023-12-22

網路安全制度的內在關係 (https://www.secrss.com/articles/62046)

安全營運 (https://www.secrss.com/articles?tag=安全运营) · 關鍵資訊基礎設施安全保護聯盟 (https://www.secrss.com/articles?author=关键信息基础设施安全保护联盟) · 2023-12-22

評論（0）

登入後才能發表評論，請先登入/ 註冊 (https://www.secrss.com/login)