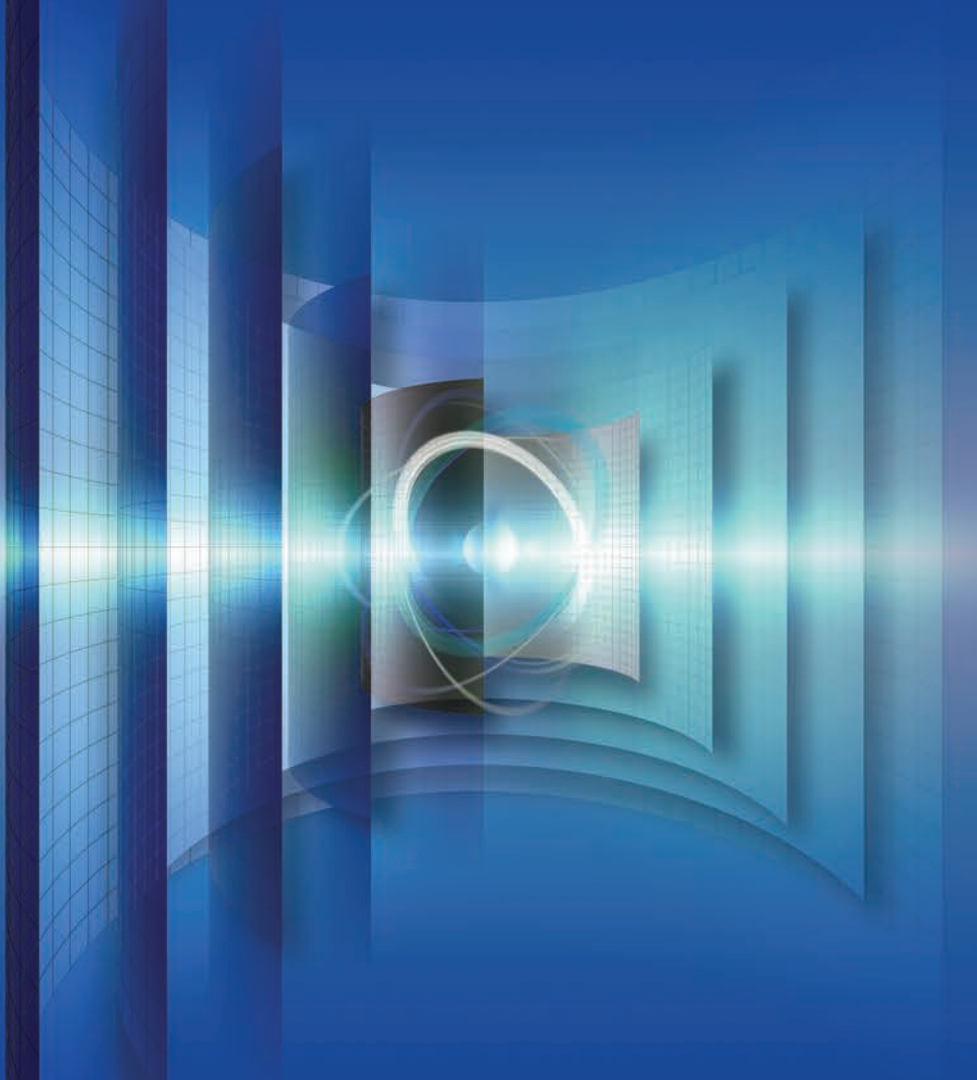
国际原子能机构《核安保丛书》第42-G号

实施导则

促进核安保的计算机安保



IAEA
国际原子能机构

国际原子能机构《核安保丛书》

国际原子能机构《核安保丛书》处理与防止和侦查涉及或针对核材料、其他放射性物质、相关设施或相关活动的犯罪行为或未经授权的故意行为并予以做出响应有关的核安保问题。这些出版物符合并补充国际核安保文书，例如《核材料实物保护公约》及其修订案、《制止核恐怖主义行为国际公约》、联合国安全理事会第 1373 号决议和第 1540 号决议以及《放射源安全和安保行为准则》。

国际原子能机构《核安保丛书》的类别

原子能机构《核安保丛书》出版物按以下类别发行：

- **核安保基本原则**详述国家核安保制度的目标和这种制度的基本要素。这些基本原则构成“核安保建议”的基础。
- **核安保建议**提出国家按照“核安保基本原则”为实现和保持有效的国家核安保制度应当采取的措施。
- **实施导则**就国家可以实施“核安保建议”中提出的措施的方法提供指导。因此，这些导则注重如何落实与广泛的核安保领域有关的建议。
- **技术导则**就具体技术主题提供指导，以补充“实施导则”中提供的指导。这些导则注重如何实施必要措施的细节。

起草和审查

《核安保丛书》出版物的编写和审查涉及原子能机构秘书处、成员国专家（协助秘书处起草这些出版物）以及审查和核准出版物草案的核安保导则委员会。适当时，在起草期间还举行不限人数的技术会议，为成员国和相关国际组织的专家提供机会审查和讨论文本草案。此外，为确保高水平的国际审查和达成高度国际共识，秘书处向所有成员国提交草案文本，以供进行 120 天的正式审查。

对于每份出版物，秘书处都要编写核安保导则委员会在编写和审查过程的相继阶段予以核准的以下内容：

- 说明预定新的或经修订的出版物的概要和工作计划、其预定用途、范围和目录；
- 提交成员国的出版物草案，以供在 120 天磋商期间发表意见；
- 考虑了成员国意见的最终出版物草案。

原子能机构《核安保丛书》出版物的起草和审查过程考虑到机密性，并且承认核安保与总体乃至具体的国家安保关切有着密不可分的联系。

一个基本的考虑因素是在这些出版物的技术内容上应当虑及相关的原子能机构安全标准和保障活动。特别是，在以上所述每个阶段由相关安全标准分委员会以及核安保导则委员会对涉及与安全有接口的领域的《核安保丛书》出版物（称作接口文件）进行审查。

促进核安保的计算机安保

国际原子能机构的成员国

阿富汗
阿尔巴尼亚
阿尔及利亚
安哥拉
安提瓜和巴布达
阿根廷
亚美尼亚
澳大利亚
奥地利
阿塞拜疆
巴哈马
巴林
孟加拉国
巴巴多斯
白俄罗斯
比利时
伯利兹
贝宁
多民族玻利维亚国
波斯尼亚和黑塞哥维那
博茨瓦纳
巴西
文莱达鲁萨兰国
保加利亚
布基纳法索
佛得角
布隆迪
柬埔寨
喀麦隆
加拿大
中非共和国
乍得
智利
中国
哥伦比亚
科摩罗
刚果
哥斯达黎加
科特迪瓦
克罗地亚
古巴
塞浦路斯
捷克共和国
刚果民主共和国
丹麦
吉布提
多米尼克
多米尼加共和国
厄瓜多尔
埃及
萨尔瓦多
厄立特里亚
爱沙尼亚
斯威士兰
埃塞俄比亚
斐济
芬兰
法国
加蓬
冈比亚
格鲁吉亚
德国
加纳
希腊
格林纳达
危地马拉
圭亚那
海地
教廷
洪都拉斯
匈牙利
冰岛
印度
印度尼西亚
伊朗伊斯兰共和国
伊拉克
爱尔兰
以色列
意大利
牙买加
日本
约旦
哈萨克斯坦
肯尼亚
大韩民国
科威特
吉尔吉斯斯坦
老挝人民民主共和国
拉脱维亚
黎巴嫩
莱索托
利比里亚
利比亚
列支敦士登
立陶宛
卢森堡
马达加斯加
马拉维
马来西亚
马里
马耳他
马绍尔群岛
毛里塔尼亚
毛里求斯
墨西哥
摩纳哥
蒙古
黑山
摩洛哥
莫桑比克
缅甸
纳米比亚
尼泊尔
荷兰
新西兰
尼加拉瓜
尼日尔
尼日利亚
北马其顿
挪威
阿曼
巴基斯坦
帕劳
巴拿马
巴布亚新几内亚
巴拉圭
秘鲁
菲律宾
波兰
葡萄牙
卡塔尔
摩尔多瓦共和国
罗马尼亚
俄罗斯联邦
卢旺达
圣基茨和尼维斯
圣卢西亚
圣文森特和格林纳丁斯
萨摩亚
圣马力诺
沙特阿拉伯
塞内加尔
塞尔维亚
塞舌尔
塞拉利昂
新加坡
斯洛伐克
斯洛文尼亚
南非
西班牙
斯里兰卡
苏丹
瑞典
瑞士
阿拉伯叙利亚共和国
塔吉克斯坦
泰国
多哥
汤加
特立尼达和多巴哥
突尼斯
土耳其
土库曼斯坦
乌干达
乌克兰
阿拉伯联合酋长国
大不列颠及北爱尔兰联合王国
坦桑尼亚联合共和国
美利坚合众国
乌拉圭
乌兹别克斯坦
瓦努阿图
委内瑞拉玻利瓦尔共和国
越南
也门
赞比亚
津巴布韦

国际原子能机构的《规约》于 1956 年 10 月 23 日经在纽约联合国总部举行的原子能机构《规约》会议核准，并于 1957 年 7 月 29 日生效。原子能机构总部设在维也纳，其主要目标是“加速和扩大原子能对全世界和平、健康及繁荣的贡献”。

国际原子能机构《核安保丛书》第 42-G 号

促进核安保的计算机安保

实 施 导 则

国 际 原 子 能 机 构

2023 年 • 维也纳

版 权 声 明

Marketing and Sales Unit
Publishing Section
International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 Vienna, Austria
传真：+43 1 26007 22529
电话：+43 1 2600 22417
电子信箱：sales.publications@iaea.org
https://www.iaea.org/zh/chu-ban-wu

国际原子能机构印制
2023 年 9 月 • 奥地利

促进核安保的计算机安保

国际原子能机构，奥地利，2023 年 9 月
STI/PUB/1918
ISBN 978-92-0-517122-7（简装书：碱性纸）
978-92-0-517222-4（pdf 格式）
ISSN 2790-7023

前　言

国际原子能机构《核安保丛书》就核安保各方面达成的国际共识提供指导，以支持各国积极履行其核安保责任。国际原子能机构开发并维护这些导则文件，作为其向成员国提供核安保相关国际支持与合作方面发挥核心作用的一部分。

国际原子能机构《核安保丛书》由机构与成员国专家合作，于2006年启动开发，之后不断更新。作为总干事，我承诺致力于确保国际原子能机构将持续维护和改进这套综合的、全面的、连贯更新的、用户友好的、适合用途的高质量核安保导则文件。在使用核科学和技术方面适当应用这些导则文件，确保提供高水平的核安保，使人们对核技术的持续应用保持必要的信心，从而造福所有人。

核安保是国家的责任。国际原子能机构《核安保丛书》是对核安保相关国际法律文书的补充，并成为帮助成员国履行其义务的重要参考。虽然核安保导则文件对成员国没有法律约束力，但它得到了广泛应用。它已成为绝大多数成员国不可或缺的参考文件，这些成员国已将这些核安保导则文件的相关建议纳入国家法规，以加强核电、研究堆和核燃料循环设施，以及核技术在医学、工业、农业和科学研究等领域应用中的核安保。

国际原子能机构《核安保丛书》提供的指导是以成员国的实践经验为基础，并通过达成国际共识产生的。核安保导则委员会的成员和其他专家的参与尤其重要，我对所有为这项工作贡献知识和专长的人们表示感谢。

国际原子能机构在帮助成员国开展评估活动和咨询服务时，也会使用《核安保丛书》中的相关导则文件。这有助于成员国应用这些导则文件，从而使有益经验和见解得以分享。上述评估活动和咨询服务过程中形成的反馈意见，以及在使用和应用核安保导则文件中对相关事件和经验的总结，在定期修订这些核安保导则文件时都会考虑借鉴。

我认为，国际原子能机构《核安保丛书》相关导则文件及其应用为确保核技术应用领域的高水平核安保作出了宝贵贡献。我鼓励所有成员国推广和应用这些导则文件，并与国际原子能机构合作，在现在和将来维护这些文件的质量。

编者按

国际原子能机构《核安保丛书》发布的导则对各国不具有约束力，但各国可利用这种导则协助其履行国际法律文书规定的义务以及在本国范围内履行其核安保责任。用“应当”表述的导则旨在提出国际良好实践和表示对各国有必要采取建议的措施或等效替代措施的国际共识。

安保相关术语按其所在出版物中或该出版物所支持的更高一级导则中的定义加以理解。在其他情况下，词语均按其通常理解的意义使用。

附录被视为出版物的一个不可分割的组成部分。附录中的资料具有与正文文本相同的地位。附件用于提供实例或补充资料或解释。附件不是主文本不可分割的组成部分。

虽已尽力保持本出版物中所载信息的准确性，但是国际原子能机构及其成员国对使用本出版物可能产生的后果均不承担任何责任。

使用某些国家或领土的特定名称并不意味着国际原子能机构作为出版者对这类国家或领土、其当局和机构或其边界划定的法律地位作出任何判断。

提及具体公司或产品的名称（不论表明注册与否）并不意味着国际原子能机构有意侵犯所有权，也不应被解释为国际原子能机构的认可或推介。

目 录

1. 引 言

背景

1.1. 基于计算机的系统在使用、存储和运输核材料及其他放射性物质的设施和活动 — 包括为其提供实物保护以及采取措施探测和应对脱离监管控制的材料 — 的安全可靠运行中发挥着至关重要的作用。因此，所有此类基于计算机的系统都需要受到保护，以防止针对其实施的犯罪行为或其他未经授权的行为。随着技术的进步，计算机系统在包括核安全和核安保在内的核设施运营中预计将发挥越来越重要的作用，其使用率亦将随之增加。

1.2. 《核安保基本法则》（Nuclear Security Fundamentals）[1]强调了信息安全（保）（包括计算机安保）在核安保制度中的重要性，并强调了有必要开展保障活动，识别并解决各种影响核设施运行能力的问题和要素，从而为核设施提供充分安全保证（包括计算机安保）。

1.3. 保证敏感信息的安全，是国家核安保制度的关键要素 3 的一个组成部分。参考文献[1]指出：“针对敏感信息保密性和敏感信息资产的保护工作，法律和监管框架及相关管理措施……构成了制定相关法规和要求的基础。”保证敏感信息和敏感信息资产的安全，意味着负责机构须保护这些信息和资产的保密性、完整性和可用性。《核材料实物保护公约》修订案[2]也将保护信息的保密性作为其基本原则。

1.4. 《核材料和核设施实物保护的核安保建议》（INFCIRC/225/Revision 5）[3]第 4.10 段指出：

> “用于实物保护、核安全和核材料衡算与控制的基于计算机的系统，应根据威胁评估或设计基准威胁受到保护，以防止其受到侵害（例如网络攻击、操纵或伪造）。”

1.5. 关于放射性物质和相关设施[4]以及脱离监管控制的核材料和其他放射性物质[5]的《核安保建议》还强调必须采取措施防止此类信息遭受未经授权的访问，保护此类信息，使其免受破坏。附件一中包括“建议”级指南，旨在对参考文献[3－5]中关于计算机安保的建议，在下一个修订版面世之前进行必要的补充。

1.6. 在使用基于计算机的系统处理、传输和存储数字形式的敏感信息时，需要在此类数字资产的整个生命周期中实施计算机安保措施，充分保护其保密性、完整性和可用性。计算机安保措施包括各类必要措施，旨在预防和探测网络攻击、对网络攻击做出响应以及在基于计算机的系统遭受网络攻击后使其恢复原状。

1.7. 核安保威胁已明确将网络攻击认定为一种为实施或协助实施恶意行为（既包括直接实施恶意行为，也包括与实体接触及内部人员作案等传统手段相结合的行为）而针对基于计算机的系统发起的攻击行为。此类行为可能导致核材料或其他放射性物质被擅自转移或遭到蓄意破坏，进而导致不可接受的放射性后果。网络攻击还可能被用于协助其他犯罪或未经授权的蓄意行为，例如将核材料或其他放射性物质运送至脱离监管控制之外的区域。

1.8. 因此，为了应对各种潜在的核安保威胁，核安保制度需要包括各种手段，应对那些掌握技术或者能够获取技术，能够对基于计算机的系统发动网络攻击的危险人物。此外，对于自己本身不具备这种技能、但能够诱使拥有此类技能的个人（例如通过雇佣或胁迫）向其提供协助的危险人物，核安保措施可以对其起到威慑作用。

1.9. 在处理核材料或其他放射性物质的设施中，亦或在这些材料的运输等相关活动中，维护计算机安保面临重大挑战，因为这方面的威胁十分巨大且始终都在快速发展之中。国家的核安保制度中许多基本要素都依赖于基于计算机的系统或受到基于计算机系统的支持，因此有效的计算机安保措施发挥着决定性的作用。

目标

1.10. 本出版物旨在指导如何开发和实施核安保措施的必要组成部分 — 计算机安保措施。

1.11. 本实施指南适用于政策制定者、主管部门、营运单位、托运人、承运人和其他负有核安保责任的人员。

范围

1.12. 本出版物中适用于与核安保有关的计算机安保及其与核安全的接口，以及与国家核安保制度中其他要素的接口，如核材料和核设施的实物保护、放射性物质和相关设施和活动的安保措施，并且适用于核安保事件的探测和响应事宜。本出版物还适用于基于计算机的系统，此类系统一旦遭到破坏，就可能会对核安保或核安全方面造成不利影响。

1.13. 本出版物系统阐述了与所有核安保领域相关的计算机安保，包括核材料和核设施安保、放射性材料及相关设施安保，以及脱离监管控制的核材料和其他放射性物质的安保。针对核设施安保的更详细的计算机安保指南，包括计算机安保措施和计算机安保风险管理技术实施的相关实例，可参阅国际原子能机构《核安保丛书》（Nuclear Security Series）第 33-T 号导则《核设施仪器仪表和控制系统的计算机安保》（Computer Security of Instrumentation and Control Systems at Nuclear Facilities）[6]和第 17-T 号导则《核设施的计算机安保技术》（Computer Security Techniques for Nuclear Facilities）[7]。

1.14. 本出版物参考了《核安保基本原则》[1]和《建议》[3－5]中关于信息安保的指导意见，但并未就该一般性主题提供详细指导意见。国际原子能机构《核安保丛书》第 23-G 号导则《核信息的安保》[8]就核信息安保以及敏感信息和敏感信息资产的识别和保护提供了指导。

结构

1.15. 在本节“概述”之后，第二节介绍了关键术语和概念。第三节阐述了国家在核安保制度中的计算机安保方面的角色和职责，第四节阐述了相关实体的角色和职责。第五节介绍了国家层面在核安保方面为制定计算机安保战略进行的活动，第六节介绍了与实施该战略有关的活动。第七节介绍了计算机安保计划（CSP[1] [1]）的要素和措施。第八节描述与维护计算机安保有关的活动。附录提供了与核安全接口问题相关的重要技术注意事项。

[1] 一些组织可能会将计算机安保项目称为计算机安保计划。

1.16. 附件一为国家核安保制度提供了关于计算机安保方面的建议性指南，这与本出版物中的实施导则保持了一致性。作为本出版物的支持性材料，附件二至附件四提供了可能的实施措施示例。附件二概述了网络威胁概况。附件三通过实例介绍了核安保制度中计算机安保责任的分配，附件四介绍了计算机安保能力框架。

2. 概念和背景

关键术语

2.1. 一个国家内的各种组织会创建、处理、管理和存储多种类型的信息。其中一些信息，如军事机密或公民的个人信息，可以视为足够敏感，需要予以特别保护。国家可以制定国家层面的信息安全（保）法律，对信息进行定义和分类，并就具体的保护要求做出规定，其中包括对数字形式的数据和相关计算机系统的保护要求。国家核安保制度内的信息也处于这类要求的保护范围之内，除了一般的保护需求外，核安保制度可能要求对其他附加的信息提供保护，或对某些类型的信息提供额外保护，之所以这样，是因为此类信息一旦被泄露，可能会助力敌手对某些设施或活动实施恶意行为，或助力其实施涉及核材料或其他放射性物质的其他犯罪行为或未经授权的蓄意行为。敏感信息是包括软件在内的任何一种形式的信息，未经授权对此类信息进行披露、修改、更改、破坏或造成此类信息无法使用，都可能会让核安保问题陷入危局[1]。图 1 描述了敏感信息资产、基于计算机的系统和敏感数字资产（SDA）的概念以及它们之间的关系。这些概念的定义详见下文。

2.2. 敏感信息资产指的是[1]用于存储、处理、控制或传输敏感信息的任何设备或组件。敏感信息可以是数字格式或任何其他格式的信息。

2.3. 基于计算机的系统是指用于创建、提供访问路径、处理、计算、交流或存储数字信息的技术，或实施、提供或控制此类信息相关服务的技术。此种系统可以包括台式计算机、笔记本电脑、平板电脑和其他个人计算机、智能手机、大型计算机、服务器、数字仪器仪表和控制设备、可编程逻辑控制器、打印机、网络设备以及嵌入式组件和设备。此种系统还可

以包括虚拟服务，例如云计算或虚拟机。此种系统可以作为单个组件存在，也可以作为数字资产的集合存在。

2.4. 在一国之内，基于计算机的系统可以实施多种功能。核安保制度中可能存在这样一类基于计算机的系统，可以提供有价值的商业和通信功能，但这种商业和通信与核安保无关，因此不在本出版物的指导范围内。

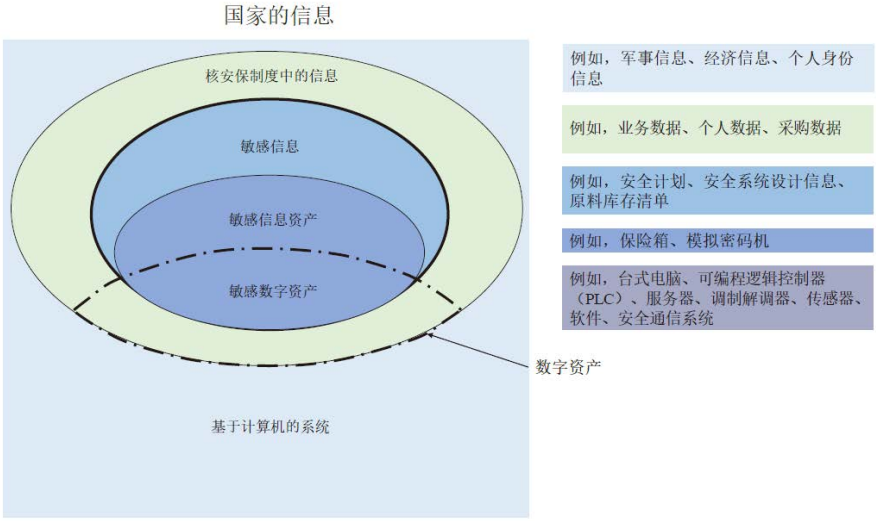


图 1. 国家和核安保制度中的信息和基于计算机的系统。

2.5. 敏感信息资产需要得到保护，防止其存储、处理、控制或传输的敏感信息遭到破坏或泄露。具体的保护方法会因相关资产类型和信息形式而异。参考文献[8]主要介绍如何对纸质书面信息和其他“硬拷贝”形式信息的保护问题。数字资产指的是与一国核安保制度相关或属于该国核安保制度范围内的基于计算机的系统（或其中的部分）。术语“敏感数字资产”（SDA）指的是那些作为基于计算机的系统（或其中的一部分）的敏感信息资产。敏感数字资产需要计算机安保措施为其提供保护。

2.6. 敏感数字资产可以为多种系统提供支持，这些系统可以执行核安全、核安保及核材料衡算与控制功能，或可以存储和处理与此类功能相关的敏感信息。敏感数字资产及其执行的基本功能可能容易受到网络攻击，并容易成为敌手的特定攻击目标。这种攻击及其对敏感数字资产的破坏可

能会对核安保和核安全产生不利影响。敏感数字资产遭到破坏可能会促成或导致诸多后果，例如：

(a) 蓄意破坏，进而导致不可接受的放射性后果，或者如果重要地区受到影响，则会导致严重的放射性后果；

(b) 核材料或其他放射性物质在未经授权的情况下遭到移动；

(c) 预防、探测和应对核安保事件的能力遭到削弱；

(d) 敏感资料遗失、更改或无法查阅。

2.7. 根据具体情况，我们需要将软件视为信息，或者视为基于计算机的系统的组成部分，或者两者兼而有之。例如，在软件的初始设计阶段，软件可能是某个处理算法的高级表达，因此我们最好将其视为信息。在其运行（即可执行）形式下，软件将构成其相关联的基于计算机的系统中的固有部分，没有该部分，系统将无法运行，并且大多数网络攻击都会利用该软件中的漏洞发动攻击。

2.8. 计算机安保是信息安保的一个特殊方面，会涉及保护基于计算机的系统，使其免受危害。计算机安保涉及所有的互联系统以及以这些系统为要素的网络。在本出版物中，我们将术语“信息技术安全”和“网络安全”视为计算机安保的同义词，因此未使用这两个术语。如参考文献[8]所述，计算机安保是信息安保的一个子集。信息安保和计算机安保通常有着相同的目标，并使用相同的方法和术语。

2.9. 鉴于计算机网络和信息流的互连性，亦需要采用计算机安保措施来保护敏感数字资产，以免有人利用其他数字资产和其他基于计算机的系统对其造成威胁。我们可采用分层方法，对安保措施进行分级，涵盖所有数字资产，为其提供纵深防御。

敏感数字资产的识别

2.10. 基于计算机的系统的所有者和/或设计者应使用系统化过程来确定由其数字资产所执行的核安保和核安全所需的功能，明确存在哪些敏感数字资产，并找出敏感数字资产受损时对核安保和核安全的潜在影响。通过进行这些操作，他们需要意识到这样一个问题，即如果一套基于计算机的系

统自身不包含敏感数字资产，在遭到破坏或感染了恶意软件 [2] 后，可能会影响到其他系统中的敏感数字资产。

2.11. 计算机安保旨在维护敏感数字资产内的敏感信息以及敏感数字资产本身的属性 — 保密性、完整性和可用性。敏感数字资产及其敏感信息有助于支持核安保制度相关功能的正确运行。根据敏感数字资产中敏感信息以及每项敏感数字资产执行的系统功能，我们应该考虑如何为其各项属性提供有针对性的保护。

2.12. 系统化过程的第一步应该是明确各项直接为核安保（例如实物保护、核材料衡算与控制以及敏感信息管理）和核安全的一个或多个方面提供支持的功能。进而明确与这些功能有关的基于计算机的系统和作为其组成部分的数字资产。

2.13. 然后，对此类系统内的数字资产遭受破坏的影响进行初步后果分析，确定哪些资产如果在网络攻击中遭到破坏，可能会影响所需的系统功能，对核安保产生不利影响。遭受破坏之后可能对系统产生不利影响的数字资产即为敏感数字资产。这一概念如图 2 所示。在进行本环节的初步分析时，不应考虑现有的计算机安保措施，只有这样才能确定如果数字资产遭到破坏，其“最坏的情况”会有什么影响。

2.14. 该过程还应包括评估支持系统或与核安保和核安全功能不直接相关的设备，明确针对这类系统或设备的网络攻击是否会直接或间接影响核安保和核安全的功能。任何可以临时连接到敏感数字资产的数字资产，也需要进行评估，以便确定其是否需要被归类为敏感数字资产。这方面的例子包括用于维护的计算机和数字测试设备。

2.15. 各种组织可以从许多不同的策略中做出选择，管理敏感数字资产。他们可以对敏感数字资产进行分组（例如，属于同一系统的敏感数字资产，或性质相似的敏感数字资产），并集中管理属于同一个组的所有敏感数字资产。因此，执行重要功能的基于计算机的系统可以视为一项单一的敏感数字资产，也可以视为由多个部分组成的一组敏感数字资产。对于那

[2] 恶意程序或恶意软件指的是故意被设计出来用于执行恶意行为的各种形式的计算机代码。可能包括辅助窃取敏感信息，损害基于计算机的系统的设计，或损害基于计算机的系统执行的功能。

些在遭受破坏后将导致相似的潜在后果的敏感数字资产而言，这种分组应有助于确保为其提供类似程度的保护。我们在确定了敏感数字资产，并根据其遭受破坏后将导致的潜在后果进行分类之后，就可以采用分级保护方法实施纵深防御了。

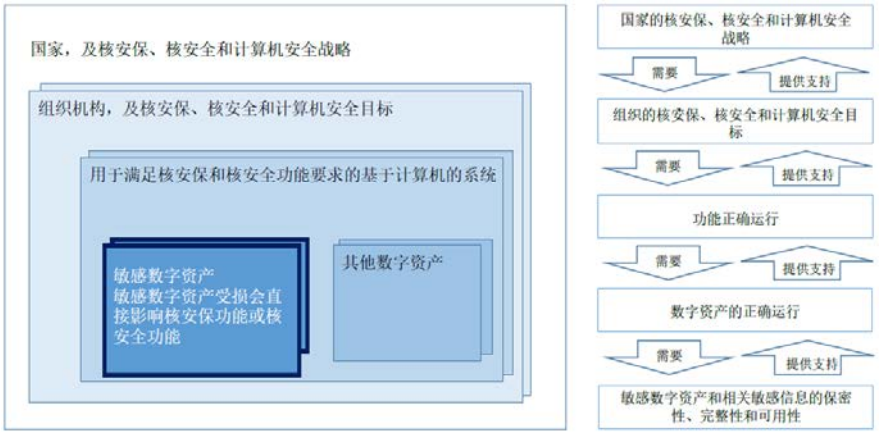


图 2. 组织内基于计算机的系统中的敏感数字资产概念图。

2.16. 每一项敏感数字资产在保密性、完整性和可用性等方面的要求，均应通过评估该项敏感数字资产对核安保和核安全的贡献，以及该项敏感数字资产在遭受网络攻击后因操作不当而导致的潜在后果的严重程度来确定。该项工作可能需要由主题专家根据相关原则和分析过程完成。

2.17. 在对基于计算机的系统进行评估以确定其是否为敏感数字资产（或包含敏感数字资产）之前，应将其视为“未指定”。出于谨慎起见，对于未指定的资产所采取的计算机安保措施通常应该非常严格，因为此时网络攻击对其的潜在影响尚属未知。有关人员应考虑是否有必要在核安保制度内禁止或限制使用此类资产。例如，核设施管理部门可能会禁止在设施内部使用属于工作人员的个人设备，如移动电话和平板电脑；第三方计算机与核设施的任何系统进行连接可能也会遭到禁止，直到其已经过详细评估。对敏感数字资产的构成、范围、边界和接口进行准确定义，对敏感数字资产对其他数字资产的依赖程度进行判断，这些都是创建安全设计的关键部分，需要在计算机安保和系统工程原则的指导下由专家进行判断。例如，通过修改整体系统设计在敏感数字资产和其他数字资产之间实现功能转移，就有可能简化敏感数字资产的定义并简化相关的计算机安保措施。

2.18. 如果使用来自虚拟服务和合同服务（如云计算）的敏感数字资产，应予特别谨慎，因为此类服务中包含不受数据所有者直接控制的元素。例如，如果某项敏感数字资产由基于云的应用程序或服务构成，其将依赖于云运营商控制下的软件和相关硬件（例如基于云的存储）。在这种情况下，在和供应商订立合同时，应就访问控制、可用性、数据隔离、数据销毁、通信接口、软件、硬件和行政程序等事项做出严格要求，以确保应用程序得到充分保护，防止未经授权的访问和操纵。将敏感数字资产的提供承包给另一个组织（即外包）的做法并不能免除程序所有者或操作人员对于敏感数字资产的保护责任。

2.19. 敏感数字资产可以包括信息技术系统和运行技术系统的组件。针对这些组件所采取的计算机安保措施将取决于系统的类型及其功能。但是，信息技术系统和运行技术系统之间往往存在接口，在针对个别系统设计计算机安保措施时，应考虑到此类接口的存在。

2.20. 近来，有一种通常被称为“生命周期模型”的流程被应用到系统中，确保敏感数字资产能够满足其特殊要求。生命周期模型描述了敏感数字资产的开发、运行、维护和消除活动，以及这些活动之间的关系。在敏感数字资产生命周期的所有阶段都需要考虑计算机安保。设施、功能、系统、组件、敏感数字资产和其他数字资产可能都有自己的生命周期，它们之间也存在相互作用。在设计基于计算机的系统（包括敏感数字资产）的生命周期时，可以使用一种面向仪器仪表和控制系统的观念性系统开发生命周期（notional system development life cycle）作为基础；注意，在使用这一概念时应当以设施的生命周期作为其背景。

网络攻击

2.21. “网络攻击”一词用于描述一种恶意行为，其目的是通过对防护性较弱的基于计算机的系统进行未经授权的访问 [3]（或在其内部进行操作），来窃取、更改、阻止访问或破坏特定目标。网络攻击危及敏感数字资产所包含的敏感信息或敏感数字资产本身的的保密性、完整性或可用性（或这些属性的组合），并可能被用于实施或协助实施针对相关设施或活

[3] 对其他属性的保护，如身份验证和不可否认性，包括在对保密性、完整性和可用性的保护中。

动的恶意行为，或针对核材料或其他放射性物质实施其他犯罪行为或未经授权的蓄意行为。与网络攻击密切相关的一个概念是无针对性攻击（non-targeted attack），例如，非定向恶意代码可能被无意中引入到基于计算机的系统和网络中。这种攻击也可能对核安保产生不利影响。

2.22. 网络攻击可以通过对信息或信息资产的直接实体访问，或通过电子访问、或两者的结合来实施，可以由敌手直接实施，也可以由知情或在不知情的情况下受到敌手影响的内部人员（或在其协助下）实施。一旦发现网络攻击，应将其视为计算机安保事件。

2.23. 由网络攻击引起的计算机安保事件可能导致进一步的计算机安保事件，并最终直接导致核安保事件，或者作为一系列恶意活动（其中可能包括其他网络攻击，或未经授权的实体访问或利用内部人员侵入，或多种混合攻击的组合攻击）的一部分间接导致核安保事件。

整个核安保领域中的计算机安保

2.24. 核安保制度涉及参考文献[3-5]中涵盖的三个领域，其中每一个领域的核安保目标都需要通过计算机安保措施提供支持。以下各节简要介绍了计算机安保措施在这些领域中的作用。

核材料和核设施

2.25. 核材料和核设施的实物保护依赖于安保措施来做到以下几点[3]：

(a) 防止擅自转移；
(b) 定位并找回丢失的核材料；
(c) 防止破坏；
(d) 减轻或尽量减少破坏的影响。

2.26. 核设施中基于计算机的系统可以为过程控制、核安全、核安保以及核材料衡算与控制功能提供支持。在这些功能中，每一项的运行都会涉及敏感数字资产，而敌手可以利用敏感数字资产的漏洞发起独立的攻击，或将之与实体攻击（例如混合攻击）结合使用。为了保护这些基于计算机的系统免受网络攻击，必须做好计算机安保方面的工作。

放射性物质及相关设施

2.27. 放射性物质的应用遍及全球，其用途十分广泛，其中还包括许多不涉及核材料的用途。此类行业的安全、安保和运营越来越多地需要来自基于计算机的系统的支持。运营机构需要采取安保措施，包括计算机安保措施，防止敌手未经授权接触或获取此类材料后实施恶意行为、防止其破坏此类材料和相关设施。

2.28. 法律和监管框架需要反映出这样一个事实，即国家放射源或放射性物质登记册通常包含某些需要予以保护的敏感信息。该领域需要实施计算机安保举措，以保护敏感信息和敏感信息资产（包括敏感数字资产）的保密性、完整性和可用性；例如，维护信息源登记册的保密性和完整性，以及保证事件响应所需数据的可用性。

脱离监管控制的核材料和其他放射性物质

2.29. 脱离监管控制的材料指的是这样一类核材料或其他放射性物质，其数量足够多，本应受到监管控制，但由于某些原因致使管制失灵，或从未存在过管制，从而导致这类物质未受到应有的监管和控制。脱离监管控制的核材料和其他放射性物质的安保是通过主管部门采取协调行动，履行其负责的预防、探测和应对核安保事件的职能来实现的。很多情况下，敏感数字资产构成了用于执行这些功能的系统中的一部分，为其提供所需支持。

2.30. 该领域需要实施计算机安保举措，例如保护敏感信息的保密性、探测系统的完整性、数据传输系统的保密性、完整性和可用性，以及支持响应措施（例如通信和核法证学）的可用性。

威胁、漏洞和计算机安保措施

威胁

2.31. 威胁是指有动机、有意图并且有能力实施恶意行为的个人或团体。任何实施或试图实施恶意行为的个人都是敌手。

2.32. 深入了解威胁以及可能的网络攻击所带来的风险，对于在核安保背景下开发有效的计算机安保措施至关重要。这包括了解核安保威胁在计划和实施网络攻击时可能具有的动机、怀有的意图、具备的能力和所使用的策略。附件二举例说明了可能利用网络攻击的核安保威胁的一般特征。

漏洞

2.33. 基于计算机的系统或网络中的漏洞属于系统的运行属性，它们使系统容易被利用或容易受到某些特定威胁。这种弱点可能是管理上的、实体上的或技术方面的。通过利用漏洞，敌手可能获得对敏感数字资产的访问或控制权。利用敏感数字资产漏洞所导致的后果可能微不足道，也可能十分严重，具体程度将取决于攻击行动在多大程度上影响敏感数字资产的运作和功能。

2.34. 基于计算机的系统配套的硬件和软件的复杂性不断增加，基于计算机的系统的数量及不同系统之间的互连性也在不断增加。这种复杂性使得人们难以对系统有全面了解，也难以完全掌握实施安全管理所需的专业知识。系统中漏洞的数量可能与其复杂性有关，因此应尽可能降低系统的复杂性，仅与其预期功能所需的程度一致即可。

2.35. 利用新发现的漏洞是许多网络攻击得手的基础。例如，“零日攻击”指的就是敌手探索利用防御者之前不知道的漏洞的情况。此外，新计算机技术的快速发展为漏洞性质的改变提供了机会，只有在这些新技术被采用并投入使用后，全新类型的漏洞才会显现出来。

2.36. 由于一些以计算机为基础的系统很复杂，其中可能存在隐藏的漏洞，现有的计算机安保措施可能不足以将风险降低到可接受的水平，因此无法将其用于某些特定的核安保和核安全应用当中。如果安保措施不能将风险降低到可接受的水平，则应考虑使用其他方法（例如，采用不同的设计或改变其用途）。

计算机安保的分级保护方法和纵深防御

2.37. 计算机安保措施可能是技术性、实体性或管理性的，或者是这些措施的组合。应采用风险评估方法，通过分级防御和纵深防御的组合来选择一组控制措施，以确保计算机安保。所采用的计算机安保措施应当是两个

方面的结合，其一为更高级别的指导或国家要求规定的某些措施，其二为运营机构通过自己的风险评估过程所确定的其他具体措施。

2.38. 计算机安保等级是一种分级保护法，用于表示不同的敏感数字资产需要不同程度的安保措施。分级保护方法中的每个级别都需要一套不同的保护措施来满足该级别的安全要求。敏感数字资产越关键，安全要求越高、执行须更严格。图 3 解释了这个概念。

2.39. 关于分级保护方法的实施，一个较实用的方法是将基于计算机的系统和相关的敏感数字资产划分为不同的计算机安保区域，并根据保护要求（即安全级别）为每个区域提供不同等级的计算机安保措施。然后，根据网络攻击对不同区域内的功能、系统和敏感数字资产的潜在影响，给该区域指定相应的计算机安保级别。

2.40. 如图 3 所示，使用计算机安保措施的等级是一种分级保护方法，需要人们首先确定网络攻击的潜在后果，然后有针对性地实施计算机安保措施。采用这种方法时可参考以下几点：

(a) 针对那些遭受损害后可能导致最严重后果，包括最重大核安保事件的敏感数字资产，应强制实施更高级别的保护要求。

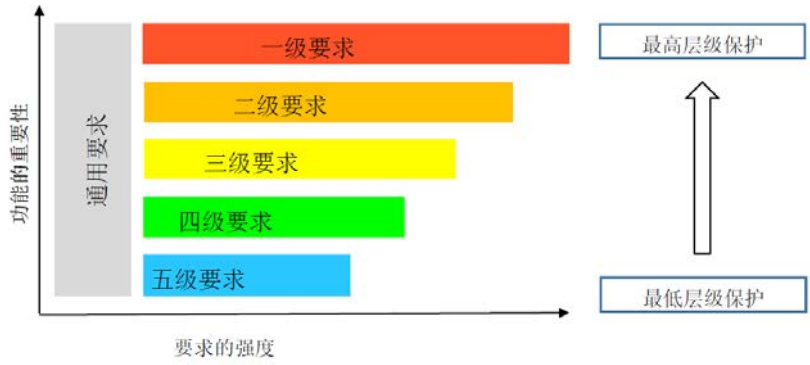


图 3. 通过计算机安保级别概念来理解分级保护法。

(b) 对于具有核安保相关功能但又没有被视为敏感数字资产的计算机系统，可实施较低等级的保护要求。

(c) 对于所有各个安保级别以及具有核安保相关功能的基于计算机的系统，可实施一般性要求，并可通过通用于其他领域的计算机系统的常见计算机安保措施来提供保护。

2.41. 对于未被视为敏感数字资产的基于计算机的系统，采取计算机安保措施也是必要的。鉴于计算机网络的互联互通和信息的流动性，有必要首先将基于计算机的系统分为不同的层次，然后再采用计算机安保分级法，从而提供纵深防御，对抗网络攻击。在上面的例子中，处于第四级和第五级这两个区域中的基于计算机的系统可能不会被归类为敏感数字资产，但仍须为这两个区域内的系统提供保护，这样可以为级别更高的区域内的敏感数字资产构建一个防护层，进一步降低其遭受入侵和破坏的风险。

2.42. 计算机安保的纵深防御意味着构建多个防御层来保证计算机安保，敌手要想使网络攻击得以进行并对敏感数字资产造成不利影响，需要攻破或规避所有这些层次的措施。通过适当的方式将彼此互补和重叠的计算机安保措施组合在一起，有助于提供纵深防御。不仅可以通过实施多层防御来构建纵深防御，还可以通过实施各种有助于预防、探测、防范、响应、减轻攻击影响并促进系统恢复的安保措施对其进行完善。例如，如果防范措施出现失败（例如，违反了禁止使用便携式存储介质的政策），或者如果保护机制被规避（例如，由于未能将一种新病毒识别为网络攻击），则仍会有机制来探测受影响的敏感数字资产中是否存在任何未经授权的更改并对此做出响应。

2.43. 有效的纵深防御还意味着，从分层式计算机安保体系的设计上来说，任何单一的层出现故障都不会导致其他层的失效或无效。例如，敌手利用常见的保护设备中的关键漏洞可能会绕过多个防御层，但如果将不同设备、配置或其他措施组合在一起构建起纵深防御，敌手的攻击则难以得手。计算机安保措施的多样性应遵循这样一个原则，即所提供的纵深防御和系统的复杂度之间需要取得平衡。

2.44. 纵深防御可能取决于一种由不同的计算机安保级别区域组成的系统设计，这些区域通常可以被表示为数个同心环。这种情况下的一般原则是，只有两个相邻的计算机安保区域之间才可以有直接连接。

2.45. 运营机构在安排工作人员在计算机安保方面的作用和责任时，应使其在彼此间具有互补性，并实现有效的职责分离，这样任何一位员工所犯的任何错误都能被另一员工注意到并予以纠正；这种方式也将有助于构建起有效的纵深防御。

2.46. 找出威胁和漏洞并评估其中的风险，为确定所需的安全措施提供了风险知情的基础。在这一背景下，风险是指核安保威胁者利用系统漏洞可能对敏感数字资产、并进而对核安保造成不利影响的可能性，因此风险是攻击发生的可能性及其后果严重程度的函数。在计算机安保的背景下，这些术语之间的关系可以解释如下，如图 4 所示：

(a) 核安保制度内基于计算机的系统，其所有者力求避免核安保事件，把有可能导致核安保事件的计算机安保风险降到最低。

(b) 核安保威胁者可能想要引发核安保事件，因而可能针对敏感数字资产发起攻击和/或破坏行动。

(c) 因此，核安保威胁者可能采取行动来利用系统漏洞，从而给敏感数字资产带来计算机安保风险；这类风险可能导致核安保事件。

(d) 基于计算机的系统的所有者采取计算机安保措施，以降低敏感数字资产面临的计算机安保风险。

(e) 所谓的风险知情方法，应包括在确定相称的计算机安保措施时考虑某些特定的计算机安保事件的可能性。有助于降低风险的举措包括消除威胁、采取计算机安保措施来降低遭受攻击的可能性并进而避免计算机安保事件，或者限制或减轻计算机安保事件影响的严重程度。

(f) 风险识别和相关的风险管理应当成为一个长期持续的过程，以应对风险因素可能有的变化。

核安保制度中的计算机安保责任

2.47. 核安保制度内，许多组织需要使用基于计算机的系统来履行诸如信息处理、核安保、核安全以及核材料衡算与控制等职能。

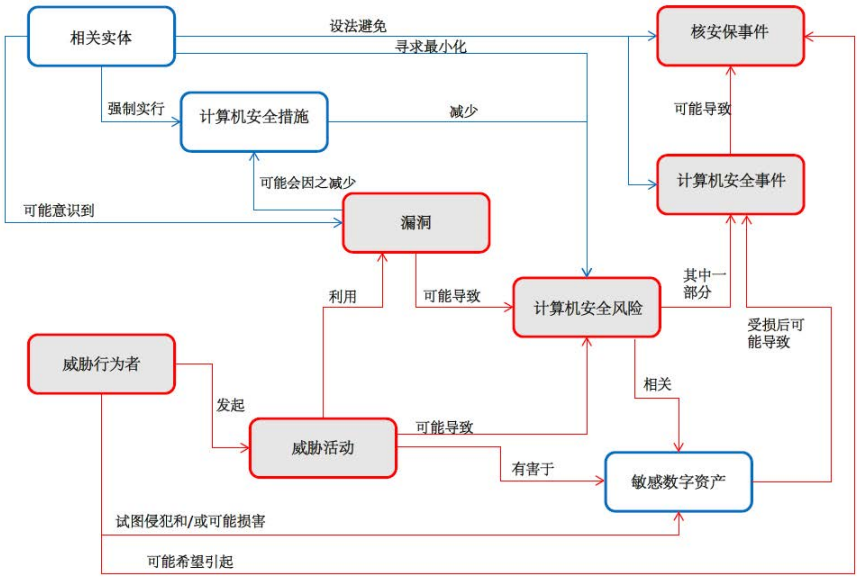


图 4. 计算机安保措施的风险知情方法（改编自 ISO/IEC 27005:2018）[9]。

2.48. 所有此类组织都有责任保护基于计算机的系统和相关敏感数字资产中的敏感信息。

2.49. 图 5 以可视化的方式呈现了核安保制度中可能承担计算机安保责任的各种组织，其中包括主管部门 [4] 和营运单位 [5]，在核安保制度中，两者按照国家相关法律法规均对计算机安保负有责任。

2.50. 国家可能会指定一个（或多个）计算机安保主管部门，该部门和负责核安保的主管部门可能并不相同。此外，除了核安保制度之外，其他国家法律法规可能也有主管部门需负责计算机安保的规定。

---

[4] 主管部门还包括警察、救援机构、边防警卫和国防部队，它们负责确保相关设施和活动的安全，并负责调查和应对各种涉及不受管制的核材料和其他放射性物质的事件。

[5] 本出版物中的“营运单位”一词是指核安保制度中获得许可的各相关实体，包括涉及核材料或其他放射性物质的设施和活动的经营者、托运人和承运人。

2.51. 销售商、承包商和供应商包括向主管部门和营运单位提供货物和服务的组织，但该类组织所承担的计算机安保方面的责任（例如保护敏感信息和相关敏感数字资产）可能并非来自国家法律和监管的要求，而是来自其与主管部门和营运单位的合同中的条款条件。

2.52. 第 3 节和第 4 节进一步解释了国家、主管部门和营运单位以及销售商、承包商和供应商在计算机安保方面的角色和责任。

计算机安保技能和能力

2.53. 有效且稳健的计算机安保有赖于有能力且值得信赖的员工、有效的管理，以及认真负责、经验丰富的领导者来实施、维护和维持。核安保制度内的每个组织都应根据其特定的作用和职责，培养并提高计算机安保方面的技能和能力，以确保计算机系统的安全。

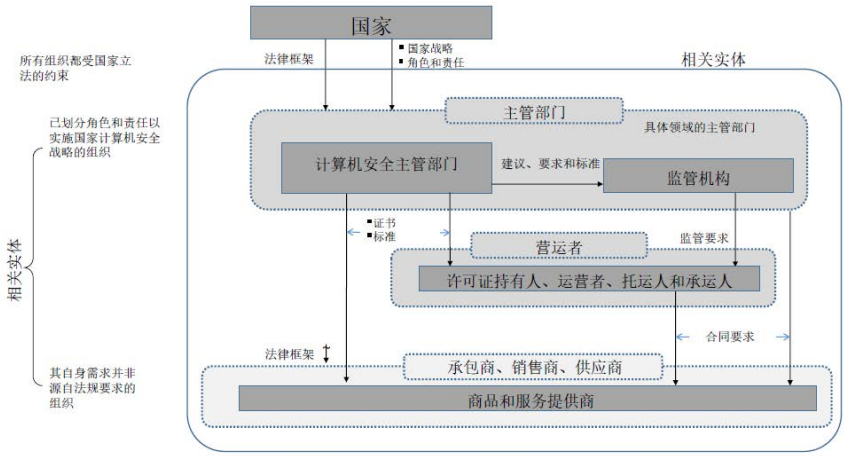


图 5. 在核安保制度中负有计算机安保责任的组织。

3. 国家的角色和责任

3.1. 国家应制定并维护国家计算机安保战略，作为其核安保制度的一部分（在本出版物的其余部分中称为“计算机安保战略”）。国家应指定一个主管机构，负责牵头制定该项战略。

法律和监管考虑

3.2. 国家应确保遵守适用于并符合核安保制度的法律和监管框架，保证计算机安保。国家应在其国家法律中纳入适当的计算机安保要求，确保核安保范围内的计算机安保能得到充分保障。

3.3. 国家法律应确保，按照核安保制度规定，对基于计算机的系统发动网络攻击会被定性为刑事犯罪。考虑到与网络攻击有关的某些犯罪和操作模式的独特性，保证计算机安保可能需要专项立法规定。

3.4. 对于针对敏感数字资产进行的、可能会危及核安保的犯罪或未经授权的蓄意行为，国家须确保予以制裁，并将此等制裁纳入到法律或监管框架内。

3.5. 国家可参考其他法律和国际法律文书（例如公约）中的例子，协助有关机构定义计算机安保及实施核安保制度中的规定。其他法律和国际法律文书可能包括：

(a) 关于计算机犯罪的法律；
(b) 关于恐怖主义的法律；
(c) 关于保护关键国家基础设施的法律；
(d) 强制执行信息披露的法律；
(e) 关于隐私和个人信息处理的法律；
(f) 关于网络犯罪的国际文书，如公约。

3.6. 国家应不断审查和更新其法律和监管框架，将针对新的和正在出现的网络威胁和漏洞的规定纳入其中。

3.7. 国家应指定计算机安保主管部门[6]，来负责监督和执行适用于核安保制度中计算机安保方面的法律法规（以下简称“计算机安保主管部门”）。

[6] 在不同情况下，国家可能会将计算机安保责任分配给不同的主管部门：例如，负责核设施计算机安保的主管部门和负责医疗实践或边境监测中的计算机安保的主管部门彼此独立，各司其职。

3.8. 国家所实施的计算机安保立法和监管框架可能并不限于核安保制度，一些法律和法规的范围可能会超出核安保制度。在这种情况下，计算机安保主管部门应确保该框架足以为核安保提供保障，否则，国家应根据核安保制度的实际需要，将相关法律法规补充到该框架中。

3.9. 国家应确保向主管部门提供足够的财政、人力和技术资源，使其能够履行职责，正确解释和履行其在国家核安保制度中与计算机安保有关的法律义务。

核安保制度中的计算机安保主管部门

3.10. 根据国家管理组织方式的不同，负责核安保制度中的计算机安保的主管部门可能是、也可能不是负责核安保的监管机构。同样，在一个国家之内，计算机安保方面的责任可能由多个机构共同承担，但在核安保领域，国家应指定一个具体的主管机构，来负责核安保制度中每个具体领域的计算机安保。例如，核电厂计算机安保的主管部门与边境监测行动中的计算机安保主管部门可能即为两个各自独立的部门。

3.11. 当核安保制度中存在多个计算机安保主管部门，或者计算机安保主管部门与负责核安保的主管部门不一致时，国家应建立并维护适当的协调机构或机制，以确保每个计算机安保方面的责任和问责都是清晰明确的，具体负责的主管部门不会出现混淆。

3.12. 国家应指定核安保制度中与计算机安保有关的所有主管部门 [7] 和营运单位，明确其各自的角色和责任，并确保每个此类组织都在核安保制度中负责计算机安保的主管部门的监督之下。

3.13. 国家应要求指定的主管部门和营运单位根据计算机安保战略制定和实施计算机安保计划。

3.14. 国家应为核安保制度中的所有相关实体界定和分配计算机安保责任。

---

[7] 相关主管部门应包括协调机构或机制、执法机构、海关和边境管制机构、情报和安全机构以及卫生和环境机构，具体设置视实际情况而定。

3.15. 附件三提供了一份核安保责任清单范例，可根据国家核安保制度及其敏感数字资产的性质从该类清单中推断出计算机安保相关任务。

3.16. 一些起支持作用的组织可能不在国家监管机构的管辖范围内，但在与实现核安保目标有关的计算机安保方面具有至关重要的作用。这些组织的责任和对其在计算机安保方面的要求可以通过合同协议来确定，如与销售商、承包商和供应商使用的合同。国家可以根据计算机安保战略，将基于计算机的系统在计算机安保方面的某些特定要求（如与设计、性能和员工培训有关的要求）分派给核安保制度中的销售商、承包商和供应商。

与其他领域的接口

3.17. 国家应确保计算机安保与其他领域之间的接口的有效运行。这可能要求国家采取超出计算机安保范围的行动（例如，对其他领域提出要求）。

3.18. 国家应确保计算机安保战略能够明确界定计算机安保与所有其他相关领域之间的接口，以便各主管部门和营运单位了解其自身在这些接口方面的角色和责任。

核安全

3.19. 核安保和核安全有着共同的目标，即保护人员、财产、社会和环境的安全。安保措施和安全措施必须以一种综合的方式来设计和实施，以便两个领域能够形成协同作用，同时确保安保措施不会影响安全，安全措施也不会影响安保。

3.20. 计算机安保在核安保和核安全之间的接口中发挥着重要作用，特别是考虑到核设施的所有运行操作上均越来越依赖基于计算机的系统。

3.21. 国家在制定计算机安保规定时，应将核安全和核安保相关规定考虑在内，在实施过程中须确保不同规定之间的连贯性和一致性。

3.22. 任何依赖于计算机系统或由计算机系统支持的核安全功能，其正常运行都将取决于相关信息（包括软件）的完整性和可用性，必要时还取决于其保密性。因此，计算机安保应作为核安全机制内基于计算机的系统的

生命周期过程中一个组成部分来实施，以确保能够同时考虑到计算机安保和核安全两个方面的需求。

3.23. 数字资产的安全类别和相关联的计算机安保等级之间应保持一致和合理的关系，以确保被划分为某一特定安全类别的数字资产拥有适当的计算机安保保护措施，但安全类别和计算机安保等级之间不一定存在简单的对等关系。此外，从安全角度来看，尽管一些数字资产未进行正式安全分类，但其对于系统安全非常重要，因此属于敏感数字资产。计算机安保级别的确定将取决于系统的功能以及系统和组织具体拥有哪些特定数字资产。这需要适当的技能和能力，并基于协商原则来做出判断。

3.24. 计算机安保措施的实施不应对核安全功能的性能、有效性、可靠性或运行产生不利影响。

3.25. 附录进一步介绍了国家在处理与核安全的接口时需考虑的问题。

实物保护

3.26. 实物保护系统，例如各种提供实体访问控制、安保监控和探测以及报警和响应功能的系统，通常依赖于基于计算机的系统。恶意破坏这些基于计算机的系统（即破坏其中信息的保密性、完整性和/或可用性）可能会损害实物保护系统的功能，并可能有助于各种试图擅自转移材料或进行蓄意破坏的实体行为。对于用于提供实物保护功能或系统的基于计算机的系统，计算机安保应作为其生命周期流程的一个组成部分来实施。

3.27. 实物保护系统（如实体访问控制）在保证计算机安保方面可能发挥重要作用，因此应考虑将其用于保护基于计算机的系统。

3.28. 有些国家可能将计算机安保视为实物保护的一部分，如参考文献[3]中所定义的那样，但本出版物将计算机安保作为一个与实物保护截然不同的独立主题，以阐明和强调两者的区别。实物保护界面的性质将取决于每个国家的情况。

3.29. 计算机安保措施的实施不应对实物保护系统功能的性能、有效性、可靠性或运行产生不利影响。

信息技术和运行技术职能

3.30. 信息技术系统和运行技术系统（包括工业控制、仪器仪表和控制系统）的管理和安保责任通常由组织内的不同部门承担。这些部门之间的有效对接和协作对于整体安保至关重要。以往的网络攻击曾涉及使用信息技术系统，将其作为侦察资源和攻击运行技术的手段。

3.31. 负责信息技术系统的人员和负责运行技术的人员在程序、词汇表和风险评估方面可能存在差异。而对于避免误解，同时避免实施计算机安保措施的过程中出现不一致的情况，两者之间的有效合作至关重要。

情报机构

3.32. 国家应确保情报机构能够提供适当的支持，协助有关部门对国家面临的威胁做出及时、准确的评估，其中包括网络攻击对核安保制度造成的威胁。应制定相应的协议和程序，支持向核安保制度内的相关实体酌情传递有关网络威胁的信息，充分保证计算机安保，应对不断变化的威胁。

3.33. 国家应确保情报机构能够熟知计算机安保在核安保制度中的作用，包括能够熟知其中可能存在的敏感数字资产的类型及其意义。

响应机构

3.34. 国家应确保所有主管部门和营运单位都建立起核安保体系并采取相应措施，以便发现对核安保有实际影响或潜在影响的计算机安保事件并对其进行评估，并将此类事件通知有关主管部门，以便采取适当的应对行动。

3.35. 突发事件应对计划中应包括应对网络攻击和混合攻击的规定。

国际援助与合作（包括信息交流）

3.36. 鼓励各国在适当情况下相互合作并与国际组织合作，以确保敏感数字资产和相关敏感信息的安全，并查明网络攻击的威胁来源，特别是威胁破坏核材料或核设施（例如，根据经修订的《核材料实物保护公约》第 5 条第 3 款的定义[2]）的可靠信息。及时分享和分析有关漏洞、威胁和计算

机安保事件的信息有助于建立互信，并强化计算机安保保障。此类信息的保密性应得到适当保护。

3.37. 国家应建立安全和受控的信息共享机制，以协调应对针对国家核安保制度的网络攻击。鼓励各国开展国际合作和援助项目，以更有效地调查网络攻击和对违者展开司法程序。

3.38. 鼓励各国定期开展咨询或评估活动，以评估其计算机安保战略和计算机安保计划及其在国家核安保制度中的实施情况。

4. 主管部门和营运单位的角色和责任

4.1. 在核安保制度中，计算机安保对于主管部门和营运单位来说是一个交叉问题。所有这类组织在保护敏感数字资产方面都负有一定责任。

4.2. 主管部门和营运单位既是敏感信息的产生者，也是敏感信息的用户，敏感信息的处理、存储或整合往往经由两者控制下的敏感数字资产进行。主管部门和营运单位应实施计算机安保措施，保护此类敏感数字资产和相关敏感信息。

4.3. 主管部门和营运单位应详细了解其所拥有的敏感数字资产，根据这类资产在受损后对核保安和核安全的潜在影响来对其进行定性，并通过计算机安保计划来明确各项敏感数字资产所需的计算机安保措施的级别。

4.4. 主管部门和营运单位应实施计算机安保措施，以保护敏感数字资产及其所含敏感信息的保密性、完整性和可用性。例如，计算机安保措施应具有以下特点：

(a) 计算机安保措施在设计上，应该能够防止人员、程序或设备在未经授权的情况下访问敏感数字资产（按照分级保护方法）。
(b) 计算机安保措施应确保不会将恶意代码或数据引入敏感数字资产。
(c) 计算机安保措施应将其整合进供应链管理措施当中。

4.5. 主管部门和营运单位应采用正式的程序，确保人员经查确实称职和值得信任，才可以得到授权，从事与计算机安保有关的活动。

4.6. 主管部门和营运单位应仅在特殊情况下，并且只有在采取了强有力的补偿性安保措施用以预防或探测未经授权的行为时，才可允许可信性尚未确定的人员从事该类活动。

4.7. 主管部门和营运单位应评估和管理核安保与核安全[4]之间与计算机安保相关的接口，以确保安保措施和安全措施不会相互产生不利影响，并尽可能使其能够相互支持。

4.8. 各主管部门和营运单位均须制定计算机安保计划，用以说明其将如何按照国家及其计算机安保主管机构的要求，为计算机安保提供足够的保障。如果不同的组织共享或依赖于彼此的敏感数字资产，那么所有共享的责任或依赖性均应反映在各自的计算机安保计划中。

4.9. 主管部门和营运单位应定期评估其计算机安保措施，以确保其符合监管要求。在设定评估之间的间隔期时，应将面临的威胁所可能引发的任何变化或影响风险的其他因素考虑在内。评估活动可酌情包括审计、审查、性能测试和演习。当基于计算机的系统经过修改之后，主管部门和营运单位也应进行自我评估，探讨修改是否会引入新的漏洞和/或产生新的敏感数字资产。

与销售商、承包商和供应商合作

4.10. 主管部门和营运单位在和销售商、承包商和供货商签订合同时，应通过相关合同条款要求销售商、承包商和供货商实施与其角色相称的计算机安保措施。合同要求对计算机安保措施应予明确规定，确保任何一方的活动都不会提供可用于向另一方发起网络攻击的途径，并确保双方的敏感信息得到适当保护。

4.11. 主管部门和营运单位及其销售商、承包商和供应商应维护相关协议和程序，及时交流沟通计算机安保事件方面的信息。

计算机安保主管部门

4.12. 计算机安保主管部门应基于风险知情的分级保护方法，明确适合各主管部门或营运单位的计算机安保要求、标准和建议。

4.13. 计算机安保主管部门应确保此类要求能够反映出相关主管部门或营运单位的战略、具体的运行要求和安保要求以及其所展示的技能和能力。

4.14. 计算机安保主管部门应基于风险知情的方法[1]，使用分级保护方法和纵深防御法为计算机安保提供充足的保障。

4.15. 各主管部门应确保其所负责的敏感数字资产整个生命周期内的所有操作（如设计、实施、维护和最终处置）都得到恰当的控制、监测和记录。

4.16. 各主管部门应通过定期评估来验证对其计算机安保规定的持续遵守情况，并确保在必要时采取纠正措施。

4.17. 计算机安保主管部门可根据其对风险的评估，制定出具体的计算机安保措施，方便各主管部门或营运单位进行实施（即合规性方法）。或者，计算机安保主管部门可以制定基于性能的计算机安保要求，这样主管部门或营运单位可以使用风险知情的方法来确定相应的计算机安保措施。计算机安保主管部门还可以将这两种方法进行组合使用。

4.18. 究竟选择合规性方法还是基于性能的方法（或两者的适当组合），其标准将取决于国家的立法框架和组织结构，以及其他几个方面的因素，例如：

(a) 营运单位理解达到目标性能所需的能力，以及设计、实施和评价有效核安保体系的能力；
(b) 受此规定管辖的设施和营运单位的数量和种类，以及合规性要求会在多大程度上限制营运单位制定适当措施的灵活性；
(c) 作为防止或防范目标的恶意行为，其潜在后果及其严重程度[10]。

合规性方法

4.19. 在合规性方法中，计算机安保主管部门根据实际需要来制定具体的计算机安保措施，满足其确立的计算机安保目标。

4.20. 合规性方法自有其优势，对计算机安保主管部门和各具体领域的主管部门或营运单位来说，该方法实施简单，无需共享敏感信息，并且便于检查和评估。在威胁程度较低、潜在后果较轻微的情况下，使用合规性方

法可能特别合适。在无法进行详细的威胁评估，或建立“设计基准威胁”（design basis threat，DBT）不可行的情况下，合规性方法也可能更合适。

4.21. 另一方面，合规性方法在处理具体情况时可能缺乏灵活性。此外，采用这种方法，具体领域的主管部门无须确保所实施的计算机安保措施是否充分；应对风险的主要责任归属于计算机安保主管部门，因为该机构对于应对网络攻击威胁所需的计算机安保措施均做出了明确规定。具体领域的主管部门或营运单位只负责实施既定的计算机安保措施。

基于性能的方法

4.22. 在基于性能的方法中，计算机安保主管部门定义计算机安保目标，并要求具体领域的主管部门或营运单位设计并实施能够满足既定目标的计算机安保措施，从而在防止网络攻击和提供应急响应方面达到一定的有效性水平。

4.23. 在基于性能的方法中，各具体领域主管部门或营运单位可以根据本部门实际需要灵活提出所需的计算机安保措施组合。他们将根据威胁评估或设计基准威胁来测试这些安保措施的充分性，以确保基于性能的措施满足安保目标。基于性能的方法的优点在于，这种方法承认不同组织及其运行环境有可能不同，因此将多种不同的计算机安保措施按照实际需求进行搭配组合，可以有效保证计算机安保。

4.24. 基于性能的方法不仅依赖于计算机安保主管部门，还要求具体领域的主管部门或营运单位在计算机安保方面具备足够的技能和能力，以明确自身需求并相应地实施计算机安保措施。基于性能的方法可能需要国家向各个具体领域的主管部门和营运单位提供与威胁评估或设计基准威胁有关的敏感信息。

组合式方法

4.25. 组合式方法包括来自上述两种方法（即合规性方法和基于性能的方法）的元素。有许多方式可应用这种组合式方法，其中包括如下两种情况：

(a) 对于潜在影响很大或非常大的情况，国家可能要求采用基于性能的方法，而潜在影响很小或非常小时则可采用合规性方法；

(b) 国家可以强制推行一套合规性要求，要求各有关部门在处理计算机安保的某些特定方面（例如保护敏感信息）时必须遵守，同时补充一些具体的计算机安保措施，以解决使用基于性能的方法时发现的所有其他问题。

4.26. 组合式方法的主要优点在于其具备一定的灵活性。而组合式方法的局限性与基于性能的方法和合规性方法的局限性也是一致的，并且取决于具体的实施情况。不过，一套实施良好的组合式方法有助于在两种方法之间达到一定的平衡，并在一定程度上改善它们的限制性。

监督管理机构

4.27. 核安保监管机构[8]应负责制定与计算机安保措施有关的监管要求，以保护敏感数字资产和相关敏感信息。监管机构应运用法规，确保相关实体遵守监督管理要求，履行其计算机安保责任。

4.28. 监管机构应确保其法规具有足够的灵活性，以适应基于计算机的系统、网络攻击和计算机安保措施不断变化的性质和环境。

4.29. 建议监管机构针对其所制定的计算机安保法规发布一份指南，以协助相关实体更好地遵守法规规定。监管机构应定期审查该指南，以确保其能够妥善处理网络威胁并实现法规的目标。

4.30. 监管机构应确保计算机安保是评估程序、许可程序或任何其他涉及向被许可人授权的程序中的一部分。

4.31. 监管机构应确保所有营运单位都有计算机安保计划，明确其计算机安保措施。

---

[8] 一个国家可能有多个监管机构，每个机构负责不同情况下的核安保事务；例如，负责核设施核安保的监管机构和负责使用放射源的工业核安保的监管机构可能是两个完全独立的机构。在本出版物中，“监管机构”一词是指在特定的上下文中负有监管责任的任何此类机构。核安保监管机构也可能是计算机安保的主管部门，在这种情况下，前一小节中的指南也适用于本节内容。

4.32. 监管机构应通过定期检查来验证被监管对象对与计算机安保有关的监管要求和许可条件的持续遵守情况，并可在必要时使用强制措施，确保被监管对象及时采取纠正行动。

5. 制定计算机安保战略

核安保制度的计算机安保战略

5.1. 计算机安保战略 [9] 为与国家核安保制度有关的计算机安保设定高等级的目标，反映在用于落实该战略的较低层级的文件当中。该战略必须是可实施的、可实现的和可审计的。

5.2. 计算机安保战略应包括以下内容：

(a) 如何进行威胁评估，包括识别可能的网络攻击情景；
(b) 如何确定计算机安保目标；
(c) 如何明确规定所需的计算机安保方面的技能和能力水平；
(d) 为所有主管部门和营运单位（可能还包括销售商、承包商和供应商）划定计算机安保的角色和责任；
(e) 在存在能力缺口的地方，确定和设立新的机构，或调整现有机构在计算机安保方面的角色；
(f) 主管部门和营运单位负责实施、整合和协调计算机安保活动的办法；
(g) 在核安保制度中用于维持计算机安保能力的措施。

5.3. 第 5—8 节针对上述内容提供了进一步的指导，应将其记录在该项战略中。

5.4. 本节介绍了国家及其计算机安保主管部门在制定战略时应开展的筹备活动，包括以下内容：

(a) 开展威胁评估；

[9] 国家可选择将一些敏感信息列入计算机安保战略的附录，以便更有效地限制这些资料的传播。

(b) 评估针对敏感数字资产的网络攻击对核安保造成的影响；

(c) 确定使用合规性方法或基于性能的方法，亦或者两者相结合的方法来管理计算机安保问题；

(d) 针对计算机安保方面的技能和能力制定一个框架；

(e) 实施（整合和协调）主管部门和营运单位的计算机安保活动。

核安全制度面临的网络威胁评估

5.5. 国家应掌握其核安保制度所面临威胁的最新情况，及时进行威胁评估[1,5]。这些信息可用于制定国家威胁声明或设计基准威胁（DBT）。

5.6. 国家的威胁评估和/或设计基准威胁应包括使用网络攻击的潜在敌手，同时也包括此类攻击中可能使用的内部人员，以及混合型攻击。

5.7. 网络攻击使得敌手能够从目标场址之外，甚至从目标场址的国家所管辖范围之外的地点发起恶意行为。因此，国家在评估时应考虑到国际威胁因素。

5.8. 国家应确保能够定期更新与网络攻击有关的威胁评估（网络威胁评估）。威胁评估的审查频率应反映出技术快速发展的特性、基于计算机的系统的进步、新发现的漏洞以及潜在网络攻击和相应的计算机安保方法不断变化的属性。

5.9. 当与网络攻击有关的威胁评估出现变更时，国家应确保及时、安全地将变更信息传达给相关主管部门和营运单位。

5.10. 国家应采取一切合理措施将网络威胁不断变化的性质纳入考虑范围，并鼓励采用能够预见或迅速适应这种变化、从而始终保持有效的计算机安保措施。

5.11. 除国家情报机构外，其他主管部门、营运单位、销售商、承包商和供应商均可能拥有可以用于威胁评估的信息。

5.12. 国家可制定信息共享协议，实现威胁信息（包括各组织之间的直接通信）的安全共享。

5.13. 我们不能期望主管部门和营运单位能够防范和应对所有级别的威胁。当威胁超过一定级别时，应由国家作出响应，向主管部门或营运单位（图 6）提供支持。对于使用设计基准威胁的主管部门和营运单位，这种情况通常被称为“超出设计基准威胁范围的事件”。

5.14. 国家应确保计算机安保的威胁评估和/或设计基准威胁能够为后续的风险评估提供足够的细节，这将有助于确保国家核安保制度中的计算机安保措施实施的充分性和有效性。

5.15. 对于为应对敌手针对各具体领域主管部门、营运单位及其销售商、承包商和供应商发起的网络攻击所需的标准、流程和资源，国家应通过计算机安保主管部门予以确定。其中应包括与响应组织的安全通信协议。

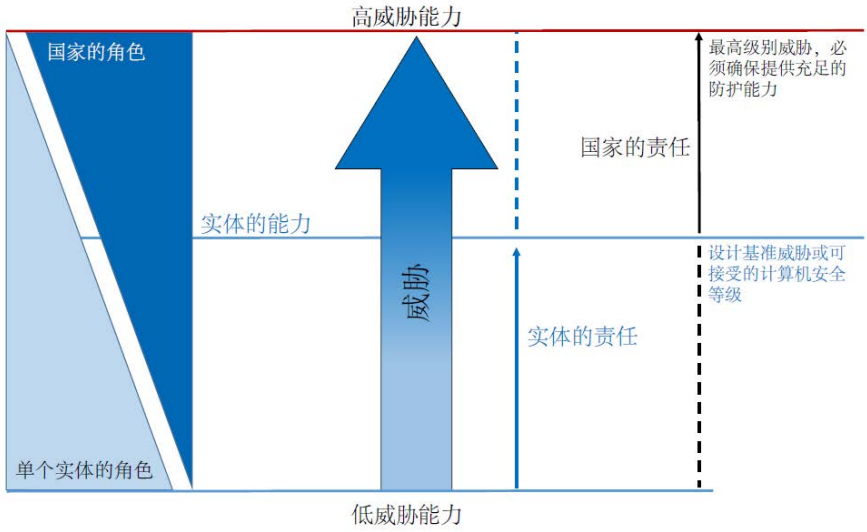


图 6. 抵御威胁的角色和责任。

指定一个主管部门进行网络威胁评估

5.16. 国家应确保定期和及时地对网络攻击威胁进行评估。国家应指定一个具备网络威胁识别和评估专业知识和技能的主管部门来承担这一职责。网络威胁评估主管部门可能不同于计算机安保主管部门。

5.17. 在履行其职能时，负责网络威胁评估的主管部门应与国家认定的、在网络威胁评估中发挥作用和承担责任并在正式的网络威胁评估过程中具备所需技能和能力的所有主管部门和营运单位进行协商和合作。主管部门应领导协调和综合与此有关的进程，以评估网络攻击的威胁。

5.18. 负责网络威胁评估的主管部门应负责确保网络威胁评估为后续风险评估提供足够多的细节信息，这些信息将用于设计适当且有效的计算机安保措施，便于在整个国家核安保制度中推广实施。

对敏感数字资产操作不当造成的影响进行评估

5.19. 计算机安保主管部门应为每个具体领域的主管部门和营运单位确定网络攻击潜在后果的严重程度，要求其通过有效的计算机安保措施来防止此类攻击的发生。

5.20. 对后果严重性的评估应基于敏感数字资产的固有特征和属性。无论网络攻击发生的可能性多大，无论其属于何种类型，主管部门和营运单位均须考虑其潜在后果的严重程度。

5.21. 图 7 显示了参考文献[3－5]涵盖的核安保领域中不同类型核安保事件对应的影响等级。计算机安保主管部门应确定后果的严重程度，并评估相关计算机安保措施是否足以确保预防或减轻这些后果。

5.22. 计算机安保主管部门可与其他具体领域的主管部门合作，确定后果严重程度的每一等级所需的保护等级。

5.23. 为确保计算机安保，各主管机构、营运单位、销售商、承包商和供应商必须具备一系列技能和能力水平，来充分发挥其作用和承担其职责。在需要根据判断作出决定和采取行动时，必然需要其提高自身的能力水平。有效的计算机安保措施包括在所需技能和能力水平方面向各主管部门、营运单位、销售商、承包商和供应商提出要求，并确保这些措施得到恰当的维护和应用。

5.24. 计算机安保主管部门应建立计算机安保所需技能和能力水平的框架。附件四提供了一个框架范例。

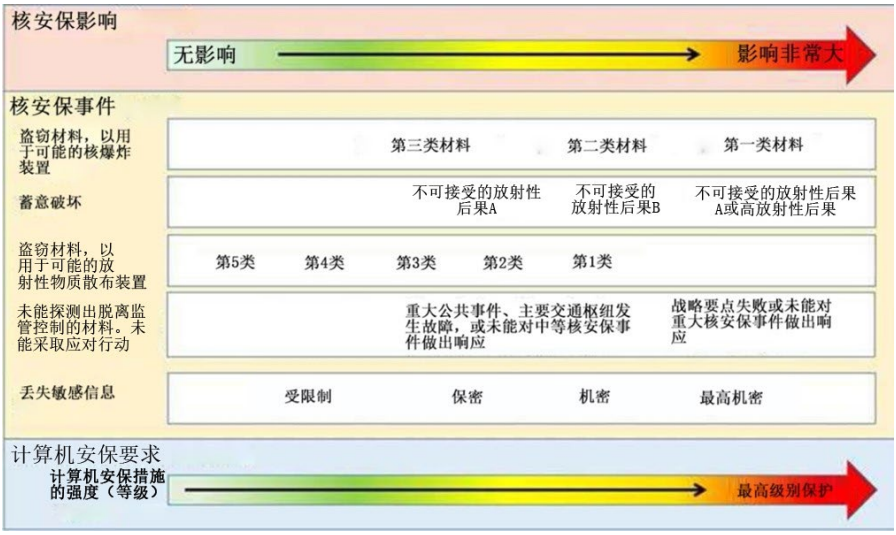


图 7. 不同类型核安保事件后果的不同严重程度（影响的等级具有独立性，不同事件所造成影响的严重程度应进行单独评估）。HRC — 高放射性后果，NED — 核爆炸装置，RDD — 放射性物质散布装置，URC — 不可接受的放射性后果。

5.25. 该框架应确保各个主管部门、营运单位、销售商、承包商和供应商所需的计算机安保技能和能力水平适合于其履行各自的计算机安保责任。更多关于定义角色、发展和维护组织内能力以及组织和个人能力建设的指南，可参阅国际原子能机构《核安保丛书》的其他出版物[3,11]。

用于确定计算机安保措施的风险评估方法

5.26. 计算机安保措施的应用应基于风险知情的方法。计算机安保主管部门应定义一种风险评估方法或一系列方法，使得具体负责的组织可据此进行下列工作：

(a) 确定每个基于计算机的系统是否为核安保制度提供相关功能；

(b) 确定每项数字资产是否是敏感数字资产

(c) 进行计算机安保风险分析，以确定该敏感数字资产或其他数字资产所需的计算机安保措施的强度，如图 3 所示。

5.27. 该方法应考虑以下因素：

(a) 所有相关的法律或法规；
(b) 敏感数字资产功能的重要性，包括保护敏感数字资产及其敏感信息的保密性、完整性和可用性对于核安保和核安全的重要性（即其安全分类）；
(c) 评估该敏感数字资产遭受网络攻击的后果；
(d) 敏感数字资产的运行环境；
(e) 根据国家威胁评估或设计基准威胁或威胁声明，识别并评估与主管部门和营运单位及其销售商、承包商和供应商以及与敏感数字资产相关的威胁；
(f) 敏感数字资产对于核安保威胁的吸引力；
(g) 敏感数字资产的内在弱点。

5.28. 计算机安保主管部门可根据敏感数字资产受损的潜在影响来修改风险评估的结果，特别是需要考虑敏感数字资产受损是否会导致以下情况：

(a) 敏感数字资产的功能变得不确定；
(b) 敏感数字资产出现意外的行为或行动；
(c) 敏感数字资产出现故障；
(d) 敏感数字资产按预期运行（即具有容错能力）。

5.29. 风险评估应综合考虑安保工作的所有方面，以应对混合型攻击，这种攻击可以将实物保护（包括人员，尤其是内部人员）和计算机安保网络攻击结合在一起。因此，从事风险评估的人员应能够接触到所有相关岗位的人员，例如与实物保护、用于核安保和核安全的计算机安保等工作相关的人员。

6. 实施计算机安保战略

6.1. 本节介绍了计算机安保主管部门在向各具体领域的主管部门或营运单位分配计算机安保角色和责任这一工作中的职责。

6.2. 这些角色和责任应记录在战略文件或支持文件中。

6.3. 计算机安保主管部门可以以制定标准、通过监管机构制定监管要求或通过和销售商、承包商或供应商签订合同的形式来确立要求，并可提供指导性文件，说明应何如满足这些要求。

计算机安保责任的分配

6.4. 计算机安保主管部门应确保所有运行敏感数字资产的具体领域主管部门和营运单位对其运行的敏感数字资产的计算机安保负有主要责任，此外，如果其所运行的其他数字资产受损后会对核安保或核安全产生不利影响，他们也将对此类数字资产负有主要责任。

6.5. 计算机安保主管部门应确保敏感数字资产生命周期中所涉及的所有相关主管部门、营运单位、销售商、承包商和供应商都被赋予适当的责任，负责其所运行的敏感数字资产的计算机安保。

6.6. 计算机安保主管部门应确保国家、具体领域的主管部门和营运单位之间适当分担责任，以确保最具威胁性的核安保威胁带来的风险被控制在可接受的水平。

6.7. 计算机安保主管机关应确保各具体领域主管部门和营运单位在探测和应对任何计算机安保事件的整个过程中负责规划并解决计算机安保问题。

主管部门与营运单位之间的关系

6.8. 对于核安保制度内的主管部门和营运单位以及核安保制度外的主管部门和营运单位之间的计算机安保责任，计算机安保主管部门应对其协调工作做出规定。例如，在核安保制度之外可能有负责计算机安保的国家机构，这就需要与核安保制度内的机构进行协调。

6.9. 在适用的情况下，计算机安保主管部门应在具体领域的主管部门和营运单位与在第 3.11 小节所述的协调机构或机制之间建立明确的沟通渠道。

6.10. 计算机安保主管部门应确保在具体领域的主管部门和营运单位之间建立合作、协调、信息交换机制，并在适当情况下对两者的计算机安保活动进行整合。

6.11. 在向具体领域的主管部门和营运单位分配计算机安保责任时，计算机安保主管部门应在相互竞争的两种需求 — 即纵深防御需求和高效利用国家核安保制度现有资源的需求之间取得平衡，同时将以下因素纳入考虑范围：

(a) 独立性有助于实现纵深防御，因为独立的设计和操作选择，不太可能允许共因故障或共模故障出现。独立性包括在职能上和财政上既独立于受监管的组织又独立于负责处理核材料或其他放射性物质利用的任何其他机构。计算机安保主管部门应确保具体领域的主管部门和营运单位有足够的技能和能力，用以支持其在计算机安保决策方面的独立性。

(b) 分享能力有助于提高资源利用的效率和效力。例如，在计算机安保取证这一专门领域，由于很少需要这种能力，某一具体领域的主管部门和营运单位可能会依赖另一具体领域的主管部门。在这种情况下，有关实体之间的协议应就响应时间做出具体规定，以便在有需求时及时得到所需支持。计算机安保主管部门应做出适当安排，以确保当具体领域的主管部门和营运单位需要其他主管部门提供支持时，对方能够及时有效地提供支持。

6.12. 具体领域的主管部门和营运单位两者之间既需要彼此独立又相互依赖，在考虑独立和依赖之间的平衡时，计算机安保主管部门应考虑防范和应对混合型攻击所需的资源，这可能涉及将计算机安保措施与可能由其他主管部门提供的其他核安保措施（例如实物保护响应力量）结合起来。

6.13. 在分配职责、明确技能和能力水平时，可以观察是否需要建立新的组织或对现有组织做出调整。

计算机安保技能和能力

6.14. 计算机安保主管部门应要求具体领域的主管部门和营运单位对其计算机安保目标进行分析，并就其组织所需的能力制作一份综合性的清单。

计算机安保主管部门可以选择自己进行这种分析，特别是如果具体领域的主管部门和营运单位主要采用由计算机安保主管部门规定的计算机安保措施。

6.15. 计算机安保主管部门应要求具体领域的主管部门和营运单位证明其具备必要的技能和适当的能力水平，以履行赋予其的计算机安保责任。附件三描述了一种较典型的面向主管部门的责任分配情况，附件四提供了一个技能和能力水平框架范例。

6.16. 计算机安保主管部门应要求具体领域的主管部门和营运单位证明，所有负责计算机安保的人员都是值得信赖的，接受过适当的培训，在其工作职责中具备足够的技能和能力，并对网络攻击的威胁有足够的认识。

6.17. 计算机安保主管部门应要求具体领域的主管部门和营运单位实施继续实施培训计划，以发展和保持履行其计算机安保责任所必需的能力。

6.18. 计算机安保主管部门应鼓励具体领域的主管部门和营运单位评估其自身在与其职责相关的技能方面的能力水平，为其技能的进一步发展和改进做好准备。

6.19. 计算机安保主管部门应开展保证活动，以此评估和确保具体领域的主管部门和营运单位在计算机安保方面的培训和技能。计算机安保主管部门应要求各具体领域的主管部门和营运单位证明其对于其在计算机安保方面的技能和能力水平的保持与其计算机安保责任相称。

计算机安保事件的应对

6.20. 计算机安保主管部门应要求具体领域的主管部门和营运单位制定、实施并演练计算机安保计划，以便更好地预防、探测和应对计算机安保事件。

6.21. 计算机安保主管部门应就如何识别可能构成计算机安保事件的事件向具体领域的主管部门和营运单位提供指导。计算机安保事件也可能是核安保事件，例如窃取敏感信息或破坏核安保或核安全功能。此外，网络攻击可能构成混合攻击的一部分。成功探测到不易察觉的或隐蔽的网络攻击有助于对潜在敌手的意图做出预判。

6.22. 计算机安保主管部门应确保具体领域的主管部门、营运单位和相关响应组织具有适当的响应能力来处理计算机安保事件，并且确保由这些组织来确定按照其计算机安保计划，将在何种情况下来激活这些能力。

6.23. 计算机安保主管部门应制定规定，要求发生计算机安保事件时须及时将其报告给核安全监管机构和/或其他具体领域的主管部门。

6.24. 计算机安保主管部门应确保具有较先进能力（例如，计算机安保取证能力）的具体领域的主管部门或营运单位，对所有涉及敏感数字资产的计算机安保事件进行技术特性描述。

演练

6.25. 计算机安保主管部门应确保在核安保演习中加入计算机安保方面的内容，以评估国家应对计算机安保事件（包括混合攻击）的能力。

6.26. 计算机安保主管部门应确保具体领域的主管部门和营运单位能够定期进行计算机安保演习，在对参与者进行培训的同时验证其计算机安保计划，包括突发事件应对计划。在适当情况下，计算机安保演习应与其他核安保演习相结合，并应定期与应急演习联合进行。

保证活动

6.27. 计算机安保主管机构应开展保证活动，以确保计算机安保相关措施和活动能够在国家核安保制度中得到有效实施，并验证正在实施的计算机安保措施所提供的保护水平与威胁评估和由国家确定的可接受风险相一致。

6.28. 计算机安保主管部门应向国家提供正式的和定期的保证，确保所有具体领域的主管部门和营运单位都具有足够的计算机安保相关技能和能力。

零部件和服务的安保认证

6.29. 具体领域的主管部门、营运单位及其各自的销售商、承包商和供应商需要确保所采购的设备、零部件和服务已采用适当的计算机安保措施，以防止引入漏洞，包括直接引入恶意软件或网络攻击途径。

6.30. 具体领域的主管部门和营运单位应确保负责为其提供敏感数字资产的销售商、承包商和供应商已实施相关的计算机安保要求（例如安全软件开发），以最大限度地减少敏感数字资产的漏洞，并防止敌手利用供应链，使其成为网络攻击的途径。具体可以通过审查销售商、承包商和供应商采用的方法、流程和设备，实现上述目的。

6.31. 计算机安保主管部门可为具体领域的主管部门、营运单位、销售商、承包商和供应商指定相关国家或国际标准，供其在敏感数字资产和相关服务的采购规范中使用。此类标准应适用于敏感数字资产生命周期的所有阶段。

6.32. 计算机安保主管部门可指定一个认证机构，对负责设计、提供和支持敏感数字资产的销售商、承包商和供应商进行审查，确保其已按照标准遵循计算机安保实践方面的规定。

6.33. 鼓励各具体领域的主管部门和营运单位酌情检查销售商、承包商和供应商进行的进一步的保证活动，例如工厂验收测试和计算机安保检查和/或审计（根据合同规定）。

国际合作与援助

6.34. 计算机安保主管部门应确保与其他国家对应的主管部门和国际机构建立必要的关系，以便在有所需求时能够有效利用国际合作与援助，此举有助于为与核安保制度有关的计算机安保提供更坚实的保障。计算机安保主管部门应根据所有相关组织的责任、能力和技能来考虑建立此类关系。

7. 开发计算机安保计划

7.1. 本节描述了推荐各相关组织使用的计算机安保计划组件和措施。图 8 展示了计算机安保计划框架的范例，包括其中的支持文档和附属文档。

7.2. 各具体领域的主管部门和营运单位所采用的计算机安保计划通过组织角色、承担的责任和采用的程序等形式，定义了该组织在实施计算机安保战略的过程中所扮演的角色。计算机安保计划还规定了具体领域的主管部门和营运单位实现计算机安保目标所使用的方法，以及该类组织将如何实施由监管机构和计算机安保主管部门通过相关法律、法规、标准和指南所规定的计算机安保措施。

7.3. 计算机安保主管部门应确保各具体领域的主管部门和营运单位按照本节的规定来制定和维护其计算机安保计划。计算机安保计划应建立在总体安保计划的框架范围内，并从属于各组织的管理系统。

7.4. 计算机安保主管部门应确保将计算机安保被视为核安保文化的重要组成部分，应要求各具体领域的主管部门和营运单位的高级管理层做出明确承诺，以实现计算机安保的持续改进。

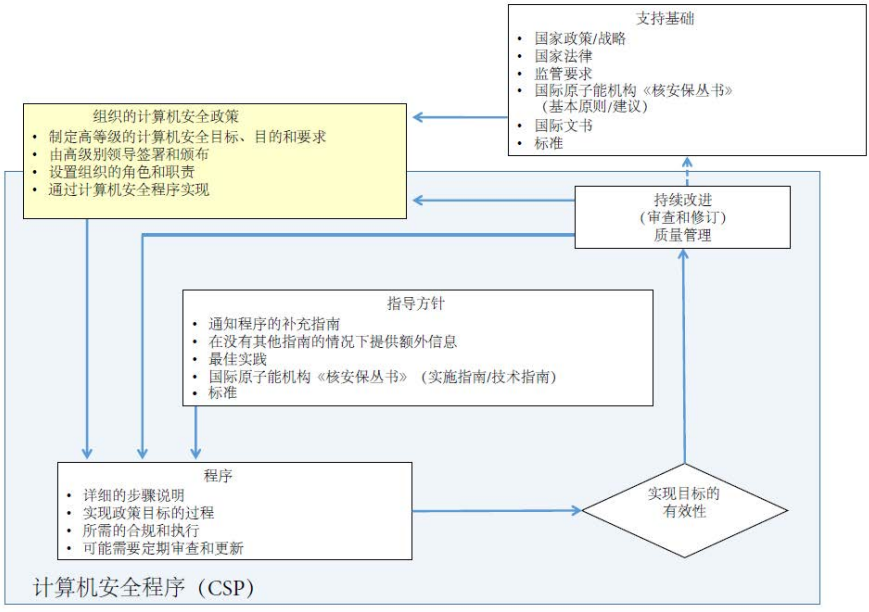


图 8. 典型的计算机安保计划概览。

计算机安保计划的内容

7.5. 计算机安保计划应从易受攻击性、保护措施、后果分析和缓解措施等方面来描述组织的计算机安保情况，从而正确识别网络攻击引起的风险，并将风险保持在可接受水平，同时推动系统恢复到安全运行状态。

7.6. 计算机安保计划至少应包括以下内容：

(a) 组织机构和职责方面：

(i) 组织结构图；
(ii) 负责人员和报告责任；
(iii) 处罚和纠正行动；
(iv) 定期审查和批准程序；
(v) 与其他计划的接口。

(b) 数字资产管理：

(i) 基于计算机的系统的完整清单；
(ii) 基于计算机的系统应用的完整清单；
(iii) 数据流和网络图，包括与外部基于计算机的系统的所有连接；
(iv) 配置管理（硬件、固件、软件应用、设备状态和相关配置）；
(v) 数字资产的分类和敏感数字资产的识别，包括重要性分类（根据不同资产对核安保、核安全和核材料衡算与控制功能的不同贡献）。

(c) 风险、脆弱性和合规性评估：

(i) 审查和重新评估计算机安保计划的周期；
(ii) 自我评估（包括主动和被动测试程序）；
(iii) 定期及反应性风险重新评估及相关方法；
(iv) 审计程序以及对缺陷的跟踪和纠正；
(v) 审查对法律的遵守情况和监管合规情况。

(d) 系统安保设计：

(i) 基本结构和设计原则；
(ii) 基本安全保设计方法（例如安保级别和区域）；
(iii) 对销售商、承包商和供应商的计算机安保要求的规范化；
(iv) 全生命周期安全。

(e) 运行安保计划：

(i) 访问权限控制；
(ii) 数据安全；
(iii) 通信安全；
(iv) 平台和应用安全（例如，加固、补丁管理、恶意软件保护）；
(v) 系统监测（包括日志管理）；
(vi) 计算机安保维护；
(vii) 事故处理；
(viii) 业务连续性和灾后恢复；
(ix) 系统备份。

(f) 人员管理:

(i) 可信度检查（人员背景审查）；
(ii) 提高认识层次和培训；
(iii) 人员资格；
(iv) 终止雇用或人员调动。

7.7. 计算机安保计划应当是组织管理体系的一个完整的、协调的部分。可以将计算机安保计划分为多个拥有不同安全分类级别的部分，以促进计划的有效使用，并与“知所必须”（need to know）原则和保密要求保持一致。

7.8. 应定期审查和更新计算机安保计划，以反映核安保制度内外的相关新知识，包括以下内容：

(a) 可用于网络攻击或防范网络攻击的新技术；

(b) 网络威胁的新特点，包括关于战术、技术和程序的已知变化；

(c) 新型计算机安保事件或核安保事件。

7.9. 计算机安保计划应包括关于定期演习的规定，以培训参与者并对计算机安保计划（包括突发事件应对计划）进行验证。在适当的情况下，应将此类演习与其他安全演习相结合，并应定期与紧急演习联合进行。

组织层面风险评估

7.10. 根据具体领域的主管部门或营运单位的能力以及网络攻击对其负责的敏感数字资产的潜在不利影响，计算机安保计划可以提供一种风险评估方法，供组织基于本地威胁环境对其基于计算机的系统进行本地风险评估。

7.11. 本地风险评估的目的是：

(a) 识别并了解风险以及造成此种风险的因素；

(b) 作为识别基于计算机的系统和敏感数字资产的基础；

(c) 设定基线，以支持对敏感数字资产和其他数字资产的变化、对计算机安保的威胁和潜在影响以及由此对核安保的影响进行分析；

(d) 协助验证更高层次的要求。

7.12. 一个组织可以在组织层面和系统层面上进行风险评估。

7.13. 此类风险评估应以国家威胁声明和/或设计基准威胁为基础，并考虑其他可用的网络威胁信息来源，为评估过程提供信息。

7.14. 风险评估过程应包括这样一项 — 考虑每个基于计算机的系统遭受的破坏和/或错误操作对核安保或核安全造成的不利后果，以此作为识别敏感数字资产的基础。

7.15. 如果风险评估的结果与计算机安保主管部门的假设有重大偏差，则具体领域的主管部门或营运单位应及时解决该问题。例如，这种偏差可能是由本地威胁环境或所用设备发生变化并引入了新的漏洞所引起的。

7.16. 风险评估应涵盖核安保的所有方面，包括例如实物保护和内部威胁防护以及计算机安保，以便评估混合攻击的风险。因此，在进行风险评估时，应该听取各相关领域专家的意见。

计算机安保措施

7.17. 计算机安保计划需要包括旨在提供预防、探测、延迟、响应和缓解等功能的计算机安保措施，并须确保非恶意行为不会导致计算机安保性降低（从而加剧对网络攻击的易感性）。

7.18. 具体来说，计算机安保措施可分为以下三种类型：

(a) 技术控制措施：用于防范、探测、缓解和恢复针对敏感数字资产的入侵或其他恶意行为的硬件和/或软件解决方案。在评价不同类型措施的有效性时，应考虑到技术控制措施的优点，特别是该种措施可提供连续的和自动的保护行动。

(b) 实体控制措施：用于保护敏感数字资产免受实体损坏和未经授权的实体接触的实体屏障。实体控制措施包括警卫和障碍，如锁、栅栏、大门、实体包装、篡改指示装置和隔离室。

(c) 行政控制措施：旨在通过控制人员行动和行为来保护敏感数字资产的政策、程序和做法。行政控制措施包括运行措施和管理措施，通常为指令性的，其内容具体规定了内部员工和第三方人员应该做什么和不应该做什么；此外还包括影响力措施，如推动建设强有力的安全文化。

确定计算机安保措施的分级保护方法

7.19. 计算机安保计划中的计算机安保措施应基于分级保护方法，即根据网络攻击潜在影响的大小采取相称的应用安保措施。分级保护方法的应用方式之一是将核安保中基于计算机的系统划分为多个区域，每个区域均采用分级式计算机安保措施。分级式计算机安保措施的一种常见应用方法是划分计算机安保的不同级别（见第 2.41－2.46 段）。

7.20. 计算机安保计划中应包含一个文件化方法，如第 2 节所述，如果计算机安保主管部门提出要求，可使用该方法来确定各项数字资产（包括敏

感数字资产）的计算机安保级别。例如，一些具体领域的主管部门或营运单位可能根据要求，无法自行确定基于计算机的系统、数字资产和敏感数字资产对安保级别的要求，而是要实施合规性计算机安保措施。

7.21. 计算机安保主管部门应批准用于审定计算机安保等级的方法。

计算机安保措施的设计

7.22. 计算机安保计划应尽最大可能推动将计算机安保措施纳入基于计算机的系统的设计当中。如果计算机安保措施能够作为系统最初设计的一部分而不是事后添加到系统中，之后的实施通常会更容易，也更有效。

7.23. 在设计基于计算机的系统时，应将核安保要求和核安全要求考虑在内。

计算机安保措施的纵深防御

7.24. 纵深防御概念对于核安保至关重要。计算机安保计划应阐明如何将纵深防御应用于计算机安保措施当中。纵深防御可以通过不同的方式实现，包括以下几种：

(a) 采用多样化且独立的计算机安保措施，并要求各项措施在设计、运行和维护方面具有独立性。其优势在于，例如，可以确保单一的计算机安保漏洞不会被敌手利用，进而使其能够系统地深入绕过多层防御。

(b) 将有权优先使用敏感数字资产的人员或团队的职责分开。这应包括考虑将计算机安保措施的设计、实施和管理方面的职责与设施或活动的运作分开。

销售商、承包商和供应商的管理

7.25. 具体领域的主管部门或营运单位可能通过销售商、承包商或供应商来提供商品或服务，而在此过程中，销售商、承包商或供应商会不可避免地访问敏感信息和敏感数字资产。在这种情况下，相关法律协议，如许可证或涉及商品或服务供应的合同，应包括部分条款，用以提出与计算机安保有关的适当要求。

7.26. 在起草此类许可证或合同时，具体领域的主管部门或营运单位应考虑纳入一些条款，用以说明销售商、承包商和供应商可能拥有关于其产品或服务的独家和专有信息（例如，关于在原始合同完成后可能出现的网络攻击漏洞），以及他们可能需要与具体领域的主管部门或营运单位分享这些信息。

7.27. 具体领域的主管部门或营运单位应在其计算机安保计划中阐明对销售商、承包商和供应商的具体的计算机安保要求，可以包括与现场和场外工作相关的要求。

7.28. 具体领域的主管部门或营运单位应确保销售商、承包商和供应商在开发和交付其所提供的产品和服务的过程中实施计算机安保措施。

7.29. 具体领域的主管部门或营运单位可以在合同安排中规定对计算机安保的具体要求，其中可包括以下内容：

(a) 不披露敏感信息和其他特定信息；
(b) 针对敏感信息的保护要求，包括保留或销毁此类信息的要求；
(c) 对进入基于计算机的系统的权限限制和在基于计算机的系统上进行活动的限制；
(d) 违禁的活动；
(e) 对不按规定遵守计算机安保要求的处罚；
(f) 对远程访问的限制；
(g) 对按照合同交付的服务和产品的测试要求。

7.30. 具体领域的主管部门或营运单位可考虑要求销售商、承包商和供应商提供证明，证明其按照合同规定遵守了计算机安保要求。

7.31. 具体领域的主管部门或营运单位应要求销售商、承包商和供应商及时报告计算机安保事件，包括识别出可能影响核安保的潜在威胁和漏洞。报告的义务和规程应作为合同的一部分。

7.32. 使用销售商、承包商和供应商可能会导致风险的转移或分担。这种风险转移或分担也可能需要经过核安保监管机构或计算机安保主管部门的批准。但是，包括计算机安保在内的核安保责任不能转移给销售商、承包商和供应商。

8. 维护计算机安保

8.1. 本节描述了与维护计算机安保有关的要素和措施。这些要素和措施应该以文件形式记录在计算机安保计划中。

8.2. 具体领域的主管部门或营运单位应根据需要实施人力资源发展计划，以确保相关人员保持履行其指定的计算机安保责任所需的技能和能力。

8.3. 具体领域的主管部门或营运单位应制定程序，着力于从成功经验中提炼最佳做法，从失败案例中总结经验教训[1]，特别是计算机安保事件方面的经验教训，在可能的情况下，还可借鉴其他国家的具体领域主管部门或营运单位、其他相关行业及同等组织的经验教训。

8.4. 具体领域的主管部门或营运单位应将计算机安保纳入其可持续性计划，并提供充足的资源予以支持。对于敏感数字资产和其他数字资产的开发、实施、维护、停止运行或注销，可持续性计划应涵盖其所需技能和能力水平的各个相关方面。

安保文化

8.5. 发展、培养和维护一种强有力的核安保文化，是核安保制度的重要组成部分[1]。在计算机安保中，人员和过程通常是确保基于计算机的系统安全的关键因素，而人为错误是计算机安保事件的最大促成因素之一。核安保文化应支持员工识别和报告基于计算机的系统或使用系统的人员的异常行为，支持员工报告可能对计算机安保产生不利影响的人为错误。

8.6. 计算机安保应通过高级管理层的明确承诺以及通过意识提升和培训项目，作为核安保文化的重要组成部分加以推广。计算机安保计划中应包括旨在加强核安保文化的活动。

8.7. 作为有效核安保文化的一部分，所有组织都应确保其员工和承包商充分了解其对于计算机安保的责任以及这些责任的重要性，涉及核安保和核安全的部门尤其如此。员工和承包商应接受与其角色和职责相称的计算机安保教育和培训。

培训

8.8. 具体领域的主管部门和营运单位应为所有员工和承包商制定计算机安保培训计划，该计划应以开发和保持其员工和承包商所需的技能和能力为目的，反映其计算机安保战略的内容。

8.9. 培训计划应包括旨在提升意识、培养能力和技能的活动。

8.10. 计算机安保意识提升培训的主题应包括：

(a) 了解网络威胁的类型和相关攻击技术；
(b) 抵御社会工程学攻击的相关意识及指南；
(c) 识别和应对网络攻击；
(d) 计算机安保的个体责任和对失职行为的处罚；
(e) 网络攻击对核安保和核安全的潜在影响；
(f) 计算机安保的良好做法；
(g) 便携式设备和可移动媒体的使用；
(h) 社交媒体的使用；
(i) 网络威胁或风险的级别或性质的变化。

8.11. 负责核系统的维护、操作和工程技术的人员应了解针对仪器仪表和控制功能发起的网络攻击给核安保和核安全带来的风险。

8.12. 负责实物保护系统的维护、操作和工程技术的人员应了解网络攻击对实物保护系统功能的潜在影响。

8.13. 如安保规则和程序发生变更，应尽快将相关信息传达给所有相关员工和承包商。

8.14. 负责计算机安保相关工作（包括管理和技术两个方面）的员工和承包商，例如，信息技术支持人员、仪器和控制人员、安保系统管理员、技术设备维护人员，应根据其具体的工作职能接受相应的专业技能培训。

8.15. 培训计划中应提出对销售商、承包商和供货商的现场及场外工作培训要求。

8.16. 高级管理层应定期接受关于网络威胁和风险管理的培训，并定期听取相关简报，提高网络威胁和风险管理意识。

8.17. 考虑到计算机安保的动态性质，具体领域的主管部门和营运单位应经常性审查和更新其培训计划，以涵盖网络威胁和网络攻击技术可能出现的变化。

8.18. 具体领域的主管部门和营运单位应就培训计划划分具体责任，并提供足够的资源以支持和维持培训计划的顺利开展。

8.19. 已完成培训计划的员工和承包商，其正式培训的记录应予以妥善保存。

8.20. 信息安全（保）和计算机安保的相关培训和意识提升活动，通常是结合在一起的。附件三的参考文献[8]提供了一个信息安全（保）意识计划的范例，该计划可进行调整以纳入计算机安保。

突发事件应对计划和响应

8.21. 计算机安保计划应记录下各种用于探测、响应和减轻计算机安保事件后果的计算机安保措施。

8.22. 计算机安保计划中应包括适当的分析和响应措施，用以描述计算机安保事件的原因、直接影响和潜在影响。这些元素可能不是显而易见的，但需要尽快进行确定。

8.23. 在对计算机安保事件进行分析时，应当考虑这样一种可能性，即该事件可能是未来规模更大的攻击的前兆或侦察活动。

8.24. 计算机安保计划中应包括用以应对网络攻击的突发事件应对计划。这些计划应该考虑到内部攻击和混合型攻击等可能性。突发事件应对计划应逐一列出各种类型的计算机安保事件以及应对这些事件所需的应对措施。

8.25. 当计算机安保事件同时也是核安保事件时，应启动相关的突发事件应对计划。计算机安保计划和相关突发事件应对计划中应具体规定在核安

保受到危害时应予立即采取的行动（在这种情况下，也可启动应急预案，但该问题超出了本出版物的范围）。

8.26. 计算机安保计划中应规定额外资源的参与准则，以及这些资源在应对计算机安保事件时所扮演的角色。

8.27. 对计算机安保事件的分析可能需要组建跨部门小组，以更全面地分析事件对核安全和保安的影响。

计算机安保保证活动

8.28. 具体领域的主管部门和营运单位应确保其管理系统（包括供应链）中包含有效的安保手段，确保能够满足计算机安保要求。

8.29. 具体领域的主管部门和营运单位（其工作仅涉及到实施监管机构或计算机安保主管部门规定的计算机安保措施的人员除外）应向计算机安保主管部门保证，其向计算机安保领域分配的资源是充足的，与威胁评估中确定的威胁级别相称。

8.30. 具体领域的主管部门和营运单位在核实核安保要求的合规情况的检查或评估活动中，应确保包括对计算机安保措施的评估。

附 录

核设施计算机安保的核安全接口注意事项

A.1. 对于一些使用、依赖基于计算机的系统（或由其提供支持）的设施，其核心安全系统遭到网络攻击时，可能会危及此类设施的核安全或损害其可用性。这种攻击可能导致设施的核心安全系统出现故障或错误操作，但如果该系统处于运行状态或预期的故障状态，则不会出现此种情况。

A.2. 恶意行为可能仅影响单一系统（或物项），也可能导致多个系统（或物项）出现不良行为。在设计设施时，应不会导致多层次纵深防御的失效或使确保恶意行为无法绕过此种防御。

A.3. 计算机安保旨在降低敌手通过网络攻击实施破坏行为的可能性，确保设施的安全、安保或可用性不受此类行为的影响。如参考文献[12]所述，计算机安保有助于保障纵深防御体系各个层级正常运行，因此各个层级的功能、系统和设备都需要实施计算机安保措施。

A.4. 计算机安保中的“安全-安保”接口包括若干对核安保和核安全非常重要的元素。其中包括制度（体系）、程序和人员。核安全措施通常也为核安保提供有价值的功能（反之亦然），在制定计算机安保措施时应考虑利用好这种互补功能。

A.5. 安全措施也可能具有安保效益；比如有这样一种特定功能 — 在接收到的数据被输入安全功能之前，该功能可自动检查数据的有效性、真实性和完整性。在对该功能进行维护或修改时，如果工作人员不了解其多功能性（相互依赖性），可能出现误操作，进而影响系统的安全或安保能力。因此，这些特定功能所执行的安全和安保功能都应该在系统和组件文档中予以描述。

A.6. 安全策略也可能对安保产生不利影响（反之亦然）。例如，安全设计通常涉及将功能分散至不同的项目或系统，以便在发生故障时隔离其影响，也涉及提供冗余的和多样化的系统，以便单一故障不会危及重要功能。这种策略可能会导致系统中与安全相关的项目数量过多，从而增加系

统的复杂性，并可能增加网络攻击的潜在目标的数量。因此，在识别和解决任何冲突时，安保和安全两方面的措施都必须予以考虑。

A.7. 要想确保某项特定的计算机安保措施的充分和完整，需要从安保性和安全性两个方面予以保障，因此设计此类措施时需要用到这两个领域的专业知识。计算机安保措施包括技术措施、实体措施和管理措施，而且所有这些措施都需要协同工作。这种方法可能涉及，比如，某些安全功能（例如，收集审计记录、生成安全警报）需要由能够监控仪器仪表和控制系统但又不能影响其性能的系统来实现，或者只有在仪器仪表和控制系统离线时才实施主动安全扫描。这种办法可能允许有例外情况，但需要根据具体情况分析和论证。

A.8. 一项设施所面临的风险既可能是由安全事件也可能是由安保事件引发，但无论哪一种，设施对风险的可接受程度都可以是相同的。做到这一点的常用方法可以总结如下：

(a) 安全和安保都采用纵深防御的概念（即使用多层保护措施）。
(b) 设法防止发生引发性事件，及早发现任何异常情况，出现异常情况时迅速做出反应，避免事态升级。
(c) 在初始设计时即纳入缓解措施，以防前面的步骤失败。
(d) 制定广泛的突发事件应对计划，以应对预防、探测和缓解失败的情况。

A.9. 计算机安保与安保之间的关系需要有效的协调，例如在资产分类和管理中将安保和安全事务纳入考虑范围。这可能会因计算机系统对软件和网络的依赖日益增加而变得复杂，再考虑到软件和网络的发展日新月异，这意味着计算机安保措施的设计和运作也需要不断变化。如果安全分析依赖于对未来确定性行为的准确预测，这就提出了一个挑战。由于计算机安保措施的有效性存在不确定性，安全分析也随之变得更加复杂，这意味着安全分析可能无法准确预测未来系统会以何种行为应对引发性事件（例如，当成为网络攻击的目标时）。

A.10. 将计算机安保措施应用于现有系统，很可能需要对现有的安全分析进行审查。一般来说，与单独的或独立的安全措施相比，综合性计算机安保措施有可能限制或改变某些对安全至关重要的系统的行为。

参考文献

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Objective and Essential Elements of a State's Nuclear Security Regime, IAEA Nuclear Security Series No. 20, IAEA, Vienna (2013).

[2] Convention on the Physical Protection of Nuclear Material, INFCIRC/274/Rev.1, IAEA, Vienna (1980); Amendment to the Convention on the Physical Protection of Nuclear Material, INFCIRC/274/Rev.1/Mod.1, IAEA, Vienna (2016).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 13, IAEA, Vienna (2011).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Radioactive Material and Associated Facilities, IAEA Nuclear Security Series No. 14, IAEA, Vienna (2011).

[5] EUROPEAN POLICE OFFICE, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL CIVIL AVIATION ORGANIZATION, INTERNATIONAL CRIMINAL POLICE ORGANIZATION–INTERPOL, UNITED NATIONS INTERREGIONAL CRIME AND JUSTICE RESEARCH INSTITUTE, UNITED NATIONS OFFICE ON DRUGS AND CRIME, WORLD CUSTOMS ORGANIZATION, Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control, IAEA Nuclear Security Series No. 15, IAEA, Vienna (2011).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security of Instrumentation and Control Systems at Nuclear Facilities, IAEA Nuclear Security Series No. 33-T, IAEA, Vienna (2018).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security Techniques for Nuclear Facilities, IAEA Nuclear Security Series No. 17-T (Rev. 1), IAEA, Vienna (in preparation).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Nuclear Information, IAEA Nuclear Security Series No. 23-G, IAEA, Vienna (2015).

[9] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, Information Technology — Security Techniques — Information Security Risk Management, ISO/IEC 27005:208, ISO, Geneva (2018).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, National Nuclear Security Threat Assessment, Design Basis Threats and Representative Threat Statements, IAEA Nuclear Security Series No. 10-G (Rev. 1), IAEA, Vienna (2021).

[11] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Culture, IAEA Nuclear Security Series No. 7, IAEA, Vienna (2008).

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. SSR-2/1 (Rev. 1), IAEA, Vienna (2016).

附 件 一

国家核安保制度中计算机安保的“建议”级指南

I–1. 本附件中的“国家核安保制度中计算机安保的要素”由来自 20 多个成员国的专家制定，作为对国际原子能机构《核安保丛书》[I–1 至 I–3]“建议”系列出版物的补充，并就国家核安保制度中计算机安保的设计、实施和维持提供“建议”级指南。各国可选择将该案文视为“建议”级的导则。本出版物正文中的实施导则与本附件中的“建议”级导则在内容上具有一致性。

背景

I–2. 国际原子能机构《核安保丛书》的“建议”级出版物[I–1 至 I–3]的目的是就如何制定或加强、实施及维护有效的国家核安保制度，从而为核材料和核设施、其他放射性物质和相关设施以及脱离监管控制的核材料和其他放射性物质提供安全保障，向各国及其主管部门提供指导。

I–3. “建议”级出版物介绍了各成员国在落实《核安保基本法则》[I–4]时应采用的最佳实践。这些基本原则确立了国家对于敏感信息和敏感信息资产免受核安保威胁的责任。

I–4. 核安保威胁可能会以敏感信息或敏感信息资产为攻击目标，使核安保或核安全系统功能无法正常运行。攻击活动可能是单独的破坏行为，也可能是针对设施发起的混合攻击的一部分（其中可能包括网络攻击和实体攻击的元素），或者针对某个组织，以获得对某些材料的访问权限。因此，计算机安保是国家核安保制度的固有内容，也是实现核安保目标的必要条件。

I–5. 敏感数字资产是指属于基于计算机的系统的敏感信息资产，这类资产若遭受损害，可能会对核安保造成不利影响。因此，需要通过计算机安保措施对敏感数字资产加以保护。

I–6. 计算机安保措施旨在维护敏感数字资产中的敏感信息以及敏感数字资产本身的保密性、完整性和可用性。

I–7. 在用于保护敏感数字资产的计算机安保措施方面，现有的“建议”级出版物所提供的指导在内容上有所欠缺。

目标

I–8. 本附件针对在实施《核安保基本法则》[I–4]各项基本要素的过程中涉及计算机安保的方面提供了指南，“建议”[I–1 至 I–3]未过多论及这方面的内容。本导则无意以任何方式对现有的建议做出修改。

I–9. 本附件旨在供各国、主管部门、营运单位[1]、供应商、销售商、承包商、核安保专业人员和核安全专业人员使用。

范围

I–10. 本导则在核安保的计算机安保方面适用。

I–11. 本导则涉及计算机安保的一般方面，适用于核安保的所有领域，包括核材料和核设施的安保[I–1]、放射性物质和相关设施的安保[I–2]以及脱离监管控制的核材料和其他放射性物质的安保[I–3]。应用本导则时应使用分级保护方法。

国家核安保制度中计算机安保的各项要素

国家责任

I–12. 国家应制定面向核安保领域的计算机安保战略[2]，为核安保制度的正常运行提供支持。

---

[1] 就此而言，“营运单位”系指许可证持有者、供应商和承运商。

[2] 这一战略可能具体针对核安保制度，也可能更具普遍性，如适用于关键基础设施保护的战略。就此而言，一些国家可能使用“政策”这一术语。

计算机安保责任的分配

I–13. 国家应指定并授权主管部门制定和实施与核安保有关的计算机安保法律和监管框架，为核安保制度提供法律和监管支持。计算机安保主管部门可能不同于核安保其他方面的主管部门。

I–14. 国家应确保计算机安保的职能、作用均已进行明确阐述，相关规定均已制定，核安保领域的各主管部门之间及部门内部能够就此进行密切协调。

法律和监管框架

I–15. 国家应确保法律和监管框架下的核安保要求涵盖未经授权行为方面的内容，以预防、探测和应对可能针对基于计算机的系统实施的未经授权行为，以免对核安保造成不利影响。国家在开发威胁评估时应以这些核安保要求为基础。

I–16. 国家应在其法律和监管框架内建立视察和执法程序，以核实对计算机安保要求的合规情况。

I–17. 国家应确保其法律和监管框架中涵盖制裁方面的内容，用于制裁对可能对核安保产生不利影响的、基于计算机的系统的未经授权行为。

主管部门

I–18. 主管部门应确保营运单位根据国家核安保要求，制定和实施计算机安保政策和相关的计算机安保方案。

I–19. 主管部门应确保评估程序、许可程序或其他授权程序均包含计算机安保相关内容。

I–20. 主管部门应定期视察并在必要时采取强制措施，核实营运单位是否持续遵守计算机安保要求，确保其采取纠正措施。

营运单位的责任

I–21. 营运单位应明确哪些资产属于敏感数字资产，并根据该类资产受损后对核安保的潜在后果对其进行定性。

I–22. 营运单位应明确适当的计算机安保措施[3]，并确保此类措施得到充分实施；营运单位应按照分级保护方法和纵深防御的概念，在敏感数字资产的整个生命周期内（尽最大可能）保护其免受危害。

I–23. 营运单位应将计算机安保作为敏感数字资产的设计原则和使用原则，包括防止（人员、流程或设备)未经授权的访问和恶意软件。

I–24. 营运单位应对计算机安保措施进行评估和管理，使其不会对实物保护、核安全、核材料衡算与控制活动产生不利影响。

I–25. 营运单位应开展保证活动，以验证自身的计算机安保措施是否符合计算机安保相关要求。

I–26. 营运单位应确保将计算机安保措施整合到其核供应链管理安排中，最大限度地减少基于计算机的系统中的漏洞，并防止供应链被敌手用作实施网络攻击的途径。

I–27. 包括主管部门在内的国家机构在保护由其负责的敏感数字资产时，应遵循第 I–21 至 I–26 段中的建议。

国际合作与援助

I–28. 国际合作与援助应包括与核安保有关的计算机安保事宜。

威胁的识别与评估

I–29. 国家的威胁评估[4]（以及设计基准威胁，如适用）应将潜在敌手利用计算机的能力（包括可能的内部活动和混合型攻击）纳入考虑范围。国家应对威胁评估进行审查和更新，以反映网络威胁可能出现的变化，并就此问题及时进行沟通。

I–30. 当针对网络攻击的设计基准威胁或威胁评估与针对实体攻击的设计基准威胁或威胁评估被分开时，国家应确保以协调的方式开展威胁评估（以及设计基础威胁，如适用）。

---

[3] 安保措施可包括物理、技术和行政控制措施。

[4] 这可能被称作“国家威胁评估”。

安全和安保接口

I–31. 安全与安保之间的接口，包括计算机安保，应以一种相辅相成的方式加以管理，以确保两者不会相互产生不利影响，并尽可能使其能够相互支持。

维护计算机安保

I–32. 在各具体领域的主管部门和营运单位的管理系统内，应以综合和协调的方式处理计算机安保问题。

I–33. 计算机安保应得到加强，使其成为核安保文化的一个重要组成部分。

I–34. 计算机安保应成为具体领域的主管部门和营运单位可持续性方案的一部分，并得到充足的资源支持。

对计算机安保事件的规划、准备和响应

I–35. 国家应确保具体领域的主管部门、营运单位和其他相关方已制定突发事件应对计划并具备所需能力，能够有效应对可能对核安保产生不利影响的计算机安保事件。

I–36. 国家应确保具体领域的主管部门、营运单位和其他相关方定期就响应计划开展演练，以评估和验证其计划中计算机安保方面的内容。

I–37. 国家的核安保制度应包括及时向主管部门报告计算机安保事件的要求。

附件一 参考资料

[I–1] 国际原子能机构，《核材料和核设施实物保护的核安保建议》（INFCIRC/225/Revision 5），国际原子能机构《核安保丛书》第 13 号，国际原子能机构，维也纳（2011）。

[I–2] 国际原子能机构，《关于放射性物质和相关设施的核安保建议》，国际原子能机构《核安保丛书》第 14 号，国际原子能机构，维也纳（2011）。

[I-3] 欧洲警察局、国际原子能机构、国际民用航空组织、国际刑警组织、联合国区域间犯罪和司法研究所、联合国毒品和犯罪问题办公室、世界海关组织，《关于脱离监管控制的核材料和其他放射性物质的核安保建议》，国际原子能机构《核安保丛书》第 15 号，国际原子能机构，维也纳（2011 年）。

[I-4] 国际原子能机构，《国家核安保制度的目标和基本要素》，国际原子能机构《核安保丛书》第 20 号，国际原子能机构，维也纳（2013）。

附 件 二

网络威胁概况

II–1. 了解网络威胁对于制定和实施保护措施非常重要。网络威胁不同于核材料和其他放射性物质及其相关设施和运行可能面对的实体威胁。网络威胁不受位置远近、攻击者数量或目标设施边界的限制。通过了解网络威胁的特征以及可能的攻击场景所获得的见解有助于制定预防和响应措施。敌手及其工具、战术和目标均为动态要素，在评估当前威胁时需要保持谨慎和勤勉的态度。

II–2. 主要的趋势包括以下各项[II–1，II–2]：

(a) 有能力实施网络攻击的敌手越来越多；
(b) 越来越多的个人或团体将网络犯罪作为一种服务来提供，帮助此前缺乏必要技能的敌手降低其犯罪的门槛；
(c) 用于网络攻击的技术越来越复杂，使得检测和应对这些技术日益困难；
(d) 越来越多地在网络攻击中使用社会工程手段，包括“鱼叉式网络钓鱼”和“水坑式攻击”技术；
(e) 敌手日益注重发现和利用工业控制系统中的漏洞；
(f) 勒索软件泛滥；
(g) 保护供应链免受网络攻击变得日益困难。

II–3. 网络威胁评估主管部门、计算机安保主管部门和参与威胁评估过程的营运单位，必须至少考虑下一节中描述的每一个已识别的内部和外部威胁的属性和特征。由于识别攻击者较为困难以及攻击多采用匿名的方式，人们很难对网络威胁进行描述。但是，建立威胁概况文件可能会有所帮助。

网络威胁的属性和特征

II–4. 以下网络威胁的属性和特征可能有助于编写威胁概况文件：

(a) 动机：政治、经济、意识形态或个人。

(b) 意图：破坏放射性物质或放射性设施，盗窃放射性物质或核材料，引发公众恐慌和社会混乱，煽动政治不稳定，造成大规模伤亡，窃取敏感信息。

(c) 相关技能（能力）：应用于计算机和自动控制系统中直接为实体攻击、情报收集、基于计算机的攻击和集资活动提供技术支持的技能。

(d) 知识：目标、场地平面图和程序、安保措施、安全措施和辐射防护程序、操作、核材料或其他放射性物质的潜在使用。

(e) 经费：来源、数额和可获得性。

(f) 战术：使用秘密行动、欺骗或武力。

网络威胁的基本描述

II–5. 威胁可以按多种方式进行分类。下面的类别仅作为示例之用（某些类别可能会有重叠）。

II–6. 内部威胁：内部威胁是最具挑战性、最难以防范的攻击方式之一。“内部人员”是指有权接触相关设施或相关活动或敏感信息或敏感信息资产的个人，他们可能独立实施或协助敌手实施涉及或针对核材料、其他放射性物质、相关设施或相关活动的犯罪行为或故意的未经授权行为，或国家确定的对核安保产生不利影响的其他行为[II–3]。内部人员是受信任的、接受过内部系统培训的人员，他们可能出于不同的动机和原因，以一种具有破坏性的、恶意的方式利用这种访问权限和对于系统的了解。内部人员的具体行动理由千差万别，其身份包括从心怀不满的员工到秘密特工不一而足。不知情的内部人员属于特例。不知情的内部人员是指没有意图和动机实施恶意行为的内部人员，他们属于在不知情的情况下被敌手利用[II–3]。

II–7. 极端主义：极端主义是指在政治或社会表达上超越常规（即超越公认行为的激进主义）的群体。极端分子可能单独行动，也可能与持有相似想法的其他个人松散地合作，对指定的目标发动网络攻击。这样的集体可能并不受一个中心人物的严格控制，其运作方式也可能并不遵循特定的参与规则。

II–8. 娱乐性黑客：娱乐性黑客包括个人或团体，他们的动机是追求名声或恶名，而不是为了造成破坏或追求金钱利益。娱乐性黑客的危害可能是非定向性的（即核设施并非其特定目标）；目标所遭受的损害可能是由于其所在的环境遭到破坏。例如，由于对便携式设备和可移动介质的不安全管理，导致核设施的控制系统感染了一种常见病毒。

II–9. 有组织犯罪：有组织犯罪已经发展出针对多个行业的非常复杂的、有针对性的网络攻击。其目的是获得金钱利益，其所获受益可能直接来自盗窃钱财，也可能间接来自出售窃取的数据，或出售有关其他威胁的信息。

II–10.民族国家：民族国家通常代表着一种非常强大且持久的威胁。此类攻击的动机和目标通常仅限于收集信息，并且其行为通常受到结构化交战规则的约束。

II–11.恐怖分子：过去被认为是由恐怖分子发动的网络攻击采用的手段往往较为简单，如对意识形态敌人进行“电子邮件轰炸”、拒绝服务攻击或破坏网站，但在今天，恐怖分子可能正在获得越来越多的技术能力来进行基于网络的攻击。这种技术能力可能来自目标内部的专家或受雇黑客[I-4]。恐怖分子可能会以核电站等关键基础设施为目标并试图采取破坏行动，但他们的重点也可能是获取核材料和其他放射性物质。

攻击特征

II–12.了解攻击特征对于建立威慑、预防、探测、缓解和响应措施也很重要。接下来的内容描述了几种类型的攻击（这些类别并不相互排斥）。

非定向攻击

II–13.上述许多威胁都可能针对特定的核安保目标进行攻击。然而，他们也可能发起非定向攻击，例如，非定向恶意代码可能被无意中引入基于计算机的系统和网络，从而对核安保造成不利影响。这方面的一个例子是，由于对移动媒介的安全管理不到位，导致核设施的控制系统感染了常见的病毒。

持续攻击

II–14.网络攻击可能会追求一击必杀的效果，也可能会针对某个设施或组织发起长期持续的攻击。对于持续攻击，其初始动作可能是破坏基于计算机的系统，然后是漫长的信息收集活动。其结果可能是一个有影响的事件，或者可能只是为了为未来的活动建立存在感。

混合攻击

II–15.混合攻击是一种协同行为，其中包括了与实体行为相关联的网络攻击。例如，实体访问控制系统可能会被网络攻击破坏，从而允许未经授权的个人获得实体进入权限。

威胁概况表

II–16.表 II–1 和 II–2 呈现了一组可能的攻击者概况。表 II–1 主要针对内部威胁（另请参见参考文献[II–3]），而表 II–2 则针对可能的外部威胁。通过这种方式，攻击者的一般类型与其资源、攻击的时间跨度、可能使用的工具和攻击者的动机被汇总在同一个表格内，得到集中展示。本表格仅供参考，对于现实中的攻击，必须根据实际情况对照来看。

表 II–1. 内部威胁

威胁	资源（技能、知识、渠道、资金）	时间	战术	动机	意图
秘密特工	为“社会工程”提供协助，某种级别的系统访问权限，可用的系统文档和专业知识	视情况而定，但通常不能在正常工作职能之外投入太多时间	现有的访问权限，了解编程和系统架构，可能了解现有密码； 可能插入专门制作的后门和/或木马； 可能的外部专家支持，可能由外部人员提供指导	政治、金融、意识形态	窃取商业信息、技术秘密、个人信息 蓄意破坏

表 II–1. 内部威胁（续）

威胁	资源（技能、知识、渠道、资金）	时间	战术	动机	意图
遭受胁迫的内部人员	某种级别的系统访问权限 可用的系统文档和专业知识	视情况而定，但通常不能在正常工作职能之外投入太多时间	现有的访问权限，了解编程和系统架构，可能了解现有密码，可能插入专门制作的后门和/或木马 可能的外部专家支持，由外部人员提供指导	个人	窃取商业信息、技术秘密、个人信息 蓄意破坏
不知情的内部人员	与正常工作职能有关的系统访问		无意中为敌手提供了内部访问权限	不涉及动机	

表 II–1. 内部威胁（续）

威胁	资源（技能、知识、渠道、资金）	时间	战术	动机	意图
心怀不满的员工/系统用户（多种类型）					
目前在职-非技术类计算机用户	中等/丰富的资源 某种级别的系统访问权限 某些特定业务和操作系统的系统文档和专业知识	视情况而定，但通常不能投入很长时间（可能并不适用于所有情况）	现有的访问权限，了解编程和系统架构，可能了解现有密码，能够插入“kiddie”工具或脚本（如果他们具备相关计算机技能，可能会更复杂）	个人、财务	报复、破坏、制造混乱、窃取商业信息 让雇主或其他雇员难堪，降低公众形象或信心
目前在职-技术类计算机用户，管理员，开发人员等。	高级别的计算机访问和权限 可能的远程访问	很多时间		个人、财务	

表 II–1. 内部威胁（续）

威胁	资源（技能、知识、渠道、资金）	时间	战术	动机	意图
目前签约-第三方	可能与当前所提供支持相关联的本地或远程访问	视情况而定	对包含受损组件的供应链元素的渗透。通过移动媒介或远程连接渗透	个人、财务	
心怀不满的员工/用户（已离职）	如果未与更大的团队合作，可用资源有限。可能仍然拥有系统文档。可能使用此前的非托管访问权限。可能与设施员工有联系	视情况而定，取决于相关的人群	可能了解现有的密码。可能使用此前的非托管访问权限 可能还在职时就创建了系统后门 “社会工程”	个人	报复、破坏、制造混乱、窃取商业信息、让雇主/其他员工难堪 降低公众形象或信心

表 II–2. 外部威胁

威胁	资源（技能、知识、渠道、资金）	时间	战术	动机	意图
非定向攻击	掌握多种技能	视情况而定	没有特定的目标，通常依赖于正常的信息技术流程和漏洞，包括社会工程	个人 — 乐趣、地位	名气，媒体关注度 寻找机会目标
极端分子	掌握多种技能，但总体上有限，除公共信息之外，对系统的了解很少	对时间可能比较敏感，因为活动可能多集中在当前或最近的事件	个人或小规模黑客活动，将工具分发给更大的群体	追求政治效果	媒体关注度，制造公共尴尬事件
娱乐性黑客	掌握多种技能，但总体上有限，除公共信息之外，对系统的了解很少	很多时间，不是很有耐心	通常可用的脚本和工具，可能具备一定的工具开发能力	个人 — 乐趣、地位	寻找机会目标和“低挂果实”

表 II–2. 外部威胁（续）

威胁	资源（技能、知识、渠道、资金）	时间	战术	动机	意图
有组织犯罪	丰富的资源 拥有可资利用的专业知识和技能	视情况而定，但大多为短期	脚本，自制工具 可能会雇佣“黑客雇工” 可能雇用前任/现任员工 “社会工程”	勒索 敲诈勒索（经济利益） 利用对财务和业务的担忧心理 售卖信息（技术、商业或个人信息）	盗窃材料 盗窃敏感信息 出售信息或访问权限
民族国家	强大的资源和专业知识 情报收集活动 可能的系统培训/操作经验 训练有素的专家团队	视情况而定，但能够支持持续攻击	复杂的工具 可能雇佣前任/现任员工“社会工程”	搜集政治情报，为以后的行动建立接入点	技术盗窃 为未来的攻击进行事先侦察，蓄意破坏

表 II–2. 外部威胁（续）

威胁	资源（技能、知识、渠道、资金）	时间	战术	动机	意图
恐怖分子	掌握多种技能 可能有系统培训/操作经验，可能有秘密特工渗透，可能有充足的资金 技能不断拓展	很多时间，非常有耐心	脚本，自制工具 可能雇佣黑客 可能雇用前任/现任员工 “社会工程”	情报收集 为未来的行动建立访问点 制造混乱 报复 影响公众舆论（制造恐惧）	支持混合攻击 为未来的行动进行事先侦察，蓄意破坏 盗窃材料

附件二　参考资料

[II–1]　澳大利亚网络安全中心，《ACSC2015 威胁报告》（ACSC 2015 Threat Report）（2015），www.cyber.gov.au/sites/default/files/2020-04/ACSC_Threat_Report_2015.pdf

[II–2]　佐治亚理工学院，《2016 年新兴网络威胁报告》（Emerging Cyber Threats Report 2016）（2015），https://iisp.gatech.edu/sites/default/files/documents/threats_report_2016.pdf

[II–3]　国际原子能机构，《防范内部威胁的预防和保护措施》，国际原子能机构《核安保丛书》第 8-G 号（Rev.1），国际原子能机构，维也纳（2020）。

[II–4]　国会研究服务部，《恐怖分子对互联网的使用：网络空间的信息行动》（Terrorist Use of the Internet: Information Operations in Cyberspace）（2011），www.hsdl.org/?view&did=8233

附 件 三

计算机安保职责的分配

III–1. 表 III–1 描述了典型的主管部门责任分配。建议根据各项典型核安保责任来制定一份相对应的典型计算机安保责任表。

表 III–1. 核安保制度中典型的计算机安保责任

实体类型	核安保责任
监管机构	建立对放射性物质、相关设施和相关活动的监管控制制度，由授权人员承担核安保的主要责任； 建立基于安保的分类系统； 建立并维护国家放射性物质登记册，参与国家威胁评估； 制定并应用设计基准威胁，代表性威胁声明或其他定义的威胁，以达到安保监管的目的； 实施授权（许可）流程，包括对安全系统和安全管理措施进行评审和评估； 建立法规要求（包括信息保护要求）并提供安保指导原则，管理安全-安保接口； 开展安保视察； 对不合规行为采取强制措施； 参与区域和国际数据库及其他合作活动； 鼓励和促进强有力的核保安文化；参与核安保事件的规划、准备和应对，包括参与演习；管理放射性物质进出口的授权和控制程序； 将特定的或增加的威胁的相关信息告知营运单位； （在授权过程中）审查和评估安保体系的设计。

表 III–1. 核安保制度中典型的计算机安保责任（续）

实体类型	核安保责任
执法部门	对恶意行为（未经授权的访问、擅自转移、蓄意破坏）做出响应以促使其中断；
	参与核安保事件的规划、准备和应对，包括参与演习；参与国家威胁评估；
	识别特定的或增加的威胁；
	进行背景调查，以验证可信度；
	探测和调查核安保事件。
海关和边境管制	参与国家威胁评定；
	识别特定的或增加的威胁；
	控制和发现进出口方面的违规行为；
	就国家放射性物质库存与管理机构沟通。
情报和安保机构	直接的国家威胁评定；
	识别特定的或增加的威胁。
国家应急响应机构	协调核安保事件的规划、准备和应对
民防卫生和环境部门	参与核安保事件的规划、准备和应对
司法部和检察机关	对恶意行为的肇事者实施制裁
外交部	参与区域合作和国际合作

附 件 四

计算机安保技能和能力水平框架范例

IV–1. 在确保组织和个人有能力且持续有能力履行其计算机安保角色和职责方面，建立技能和能力水平的框架起着关键作用。

IV–2. 本附件仅旨在介绍什么是技能和能力水平框架，无意为制定这样一个框架提供充分的指导。

IV–3. 对于每个组织或个人，该框架将有助于明确其所需的计算机安保特定领域的技能。此类领域的列表可参考如下范例：

(1) 管理（生产能力、战略、危机管理、治理、组织）；
(2) 事件应对（计算机取证、网络防御）；
(3) 法律和监管框架（刑法、条例）；
(4) 信息安全（保）和管理（密码术、加密、存储）；
(5) 采购（合同、供应链）；
(6) 保证活动（测试、认证、配置管理）；
(7) 计算机安保架构；
(8) 国际协调和援助。

另外，国际标准 ISO 27002 [IV–1]（适用于信息安全（保）管理系统）和 IEC 63096 [IV–2]（适用于核电站的 ISO 27002）提供了可用于技能领域的控制区域列表。

IV–4. 该框架基于对网络攻击的威胁评估、对用于核安保制度的基于计算机的系统的性质的了解以及对此类基于计算机的系统的脆弱性的了解，确定了各技能范围内所需的具体的计算机安保技能和知识。

IV–5. 组织和个人在计算机安保能力方面的成熟度各不相同。该框架对每项能力的能力等级进行了分类，使用了至少三个不同级别的等级。这为分级方法的实施提供了依据。这种从最低成熟度到最高成熟度的分类示例如下：

(a) 初级（新手）：表现出自动的、基于规则的行为，这种行为受到许多约束并且不灵活。

(b) 中级（从业者）：有意识地在既定政策范围内实现长期目标和计划。

(c) 高级（专家）：能够直观地了解情况，能够立即将关注重点放在关键方面。

IV–6. 需要更高级别的能力，以更有效地防范高强度威胁或防止高放射性后果。例如，负责储存、运输或使用第一类或第二类核材料，或操作设施或开展有可能产生高度放射性后果的活动的主管部门和营运单位，会被视为正在管理非常高或高放射性后果。

IV–7. 该框架确保负责设计计算机安保措施的组织和个人表现出较高等级的相关能力。

IV–8. 一些组织需要自身具备这些能力，而另一些组织则依赖其他组织的协助。

IV–9. 该框架详细规定了主管部门或营运单位或第三方可能被允许实施的典型活动。例如，在与计算机安保有关的国家威胁评估活动中，具备高等级必要能力的主管部门或营运单位可能能够发挥主导作用。而具备初级能力的主管部门或营运单位在此类威胁评估活动中可能只能起到辅助作用。表 IV–1 展示了这一点。

表 IV-1. 根据能力水平对活动进行分类

活动类型	基础利益相关者	中级利益相关者（对基础利益相关者的补充）	高级利益相关者（对中级利益相关者的补充）
关于威胁环境知识的活动	对威胁行为有基本意识（例如“网络钓鱼”攻击）	了解计算机安保威胁对自身环境的影响	持续主动地监控不断演变的计算机安保威胁
关于威胁评估和创建场景的活动	在需要时发挥贡献者作用（例如，提供工作场所实际情况的实际细节）	在国家威胁评估中发挥参与作用。在潜在影响为中、低或非常低的情况下，创建特定场地的场景，以详细说明威胁评估	在国家威胁评估活动中发挥主导作用；创建潜在影响非常高或很高的特定场地的场景；评估来自中级利益相关者的场景

附件四　参考文献

[IV–1] 国际标准化组织，信息技术 — 安保技术 — 信息安保控制实施规程（Code of Practice for Information Security Controls），ISO/IEC 27002:2013，ISO，日内瓦（2013）。

[IV–2] 国际电工委员会，核电厂 — 仪表、控制和电力系统 — 安保控制，IEC 63096:2020，IEC，日内瓦（2020）。

术　语

混合型攻击。协同使用网络攻击和实体攻击的恶意行为。

基于计算机的系统。一类技术，能够创建、处理、计算、传递或存储数字信息或提供对其的访问路径，或执行、提供或控制涉及此类信息的服务。

ⓘ 基于计算机的系统可能是实体的，也可能是虚拟的。这些系统可能包括：台式机、笔记本电脑、平板电脑和其他个人电脑、智能手机、大型计算机、服务器、虚拟计算机、软件应用程序、数据库、可移动介质、数字仪器仪表和控制设备、可编程逻辑控制器、打印机、网络设备以及嵌入式组件和设备。

计算机安保。信息安保的一个特殊方面，涉及保护基于计算机的系统免受危害。

计算机安保事件。实际或潜在地危及基于计算机的系统（包括其中的信息）的保密性、完整性或可用性的事件，或构成或有风险即将构成违反安保政策的事件。

计算机安保等级。为满足与核安保、核安全、核材料衡算与控制和/或敏感信息管理有关的功能的需求，计算机安保所需达到的等级。

计算机安保措施。旨在预防、探测或延迟、响应及减轻恶意行为或其他可能危及计算机安保的行为所造成的后果的措施。

计算机安保计划（CSP）。计算机安保战略的实施方案，定义了各相关组织的角色、职责和程序。该程序规定并详细说明了实现计算机安保这一目标所需的措施和手段，是整体安保计划的一部分（或与之相关）。

计算机安保区域。一组具有共同物理和/或逻辑边界的系统（必要时可使用附加标准进行安排），它们被赋予同一个计算机安保级别，以简化计算机安保措施的管理、通信和应用。

网络攻击。一种恶意行为，旨在通过对易受攻击的基于计算机的系统进行未经授权的访问（或在其中进行操作）来窃取、更改、阻止访问或破坏指定目标。

信息安保。对信息的保密性、完整性和可用性的维护。

敏感数字资产（SDA）。可被归类为（或从属于）基于计算机系统的敏感信息资产。

敏感信息。可能是包括软件在内的任何一种形式的信息，在未经授权的情况下对此类信息进行披露、修改、更改、破坏或无法使用此类信息可能会危及核安保。

敏感信息资产。用于存储、处理、控制或传输敏感信息的任何设备或部件。例如，敏感信息资产包括控制系统、网络、信息系统以及任何其他类型的电子或实体介质。

IAEA
国 际 原 子 能 机 构

No. 26

当 地 订 购

国际原子能机构的定价出版物可从下列来源或当地主要书商处购买。
未定价出版物应直接向国际原子能机构发订单。联系方式见本列表末尾。

北美

Bernan / Rowman & Littlefield
15250 NBN Way, Blue Ridge Summit, PA 17214, USA
电话：+1 800 462 6420 • 传真：+1 800 338 4550
电子信箱：orders@rowman.com • 网址：www.rowman.com/bernan

世界其他地区

请联系您当地的首选供应商或我们的主要经销商：

Eurospan Group
Gray's Inn House
127 Clerkenwell Road
London EC1R 5DB
United Kingdom

交易订单和查询：
电话：+44 (0) 176 760 4972 • 传真：+44 (0) 176 760 1640
电子信箱：eurospan@turpin-distribution.com

单个订单：
www.eurospanbookstore.com/iaea

欲了解更多信息：
电话：+44 (0) 207 240 0856 • 传真：+44 (0) 207 379 0609
电子信箱：info@eurospangroup.com • 网址：www.eurospangroup.com

定价和未定价出版物的订单均可直接发送至：

Marketing and Sales Unit
International Atomic Energy Agency
Vienna International Centre, PO Box 100, 1400 Vienna, Austria
电话：+43 1 2600 22529 或 22530 • 传真：+43 1 26007 22529
电子信箱：sales.publications@iaea.org • 网址：https://www.iaea.org/zh/chu-ban-wu

本出版物为作为核安保关键组成部分的计算机安全的开发和实施提供了指南。本出版物适用于核安保的计算机安全方面及其与核安全以及与一国核安保制度其他要素 — 包括核材料和核设施、放射性物质和相关设施以及脱离监管控制的核材料和其他放射性物质的安全 — 的接口。本出版物的范围包括：基于计算机的系统，该类系统若遭到破坏可能会对核安保或核安全产生不利影响；国家和有关实体在核安保制度中所承担的计算机安全方面的角色和责任；国家在制定和实施核安保计算机安全战略方面的活动；计算机安全程序的各项要素；以及与维护作为核安全制度的一部分的计算机安全有关的活动。

国际原子能机构
维也纳