|  |  |
| --- | --- |
| **世界电信标准化全会（WTSA-20）****2022年3月1-9日****，日内瓦** |  |
|  |  |
|  |  |
| **全体会议** | 文件 37 (Add.8)-C |
|  | **2021年9月16日** |
|  | **原文：英文** |
|  |
| 亚太电信组织各成员国主管部门 |
| 第50号决议的拟议修改 |
|  |
|  |

|  |  |
| --- | --- |
| **摘要：** | 考虑到树立使用信息通信技术（ICT）的信心和提高安全性的重要性，建议修订世界电信标准化全会（WTSA）第50号决议，以进一步加强相关的标准化工作。主要修改包括加强ITU-T第17研究组在安全性方面的作用，其中包括第17研究组在ITU-T安全相关工作方面的协调职能、新议题和其他编辑性修改。 |
| **联系人：** | 亚太电信组织秘书长近藤正则（Masanori Kondo）先生 | 电话： +66 2 5730044传真： +66 2 5737479电子邮件：aptwtsa@apt.int |

引言

对当今的电信/信息通信技术基础设施而言，安全性正变得日益重要。因此，应在系统/网络/应用的整个生命周期中考虑安全性问题，否则将导致系统/网络/应用遍布需要大量修补工作的安全漏洞。

在系统/网络/应用的设计、开发和部署阶段，安全架构是一个重要的关键点，原因是它提供了统一的安全设计，解决了特定场景或环境中涉及的迫切需要和潜在风险，并规定了何时、何地以及如何定义/配置和实施安全策略。此外，安全架构的设计过程通常是可复制的。

本文件认识到安全性在ICT领域的重要性。

考虑到安全相关标准化活动有助于防止恶意网络活动造成的损害，安全相关工作应继续进行。此外，ITU-T研究组应研究已确定的新兴安全技术，其中包括自动驾驶安全、DLT、AI/ML相关安全、IMT 2020(5G) OTT和IMT 2030 (6G)安全以及智慧城市、智慧工厂、智慧健康、智慧能源、分布式身份管理和量子安全等新的ICT服务和应用。

应加强第17研究组在ITU-T中的协调职能，以提高ITU-T安全相关工作的知名度，这对第17研究组与ISO/IEC、JTC 1/SC 27、IETF、ETSI和3GPP等其他同行进行有效联络或合作以及吸引专家而言至关重要。在下一个研究期，应加强第17研究组在树立使用ICT的信心和提高安全性方面的作用。

提案

亚太电信组织（APT）各成员国主管部门提议修订本文件中关于网络安全的WTSA-16第50号决议。

MOD APT/37A8/1

第50号决议（2022年，日内瓦，修订版）

网络安全

（2004年，弗洛里亚诺波利斯；2008年，约翰内斯堡；2012年，迪拜；2016年，哈马马特；2022年，日内瓦）

世界电信标准化全会（2022年，日内瓦），

忆及

*a)* 全权代表大会第130号决议（2018年，迪拜，修订版）– 国际电联在树立使用信息通信技术（ICT）的信心和提高安全性方面的作用；

*b)* 全权代表大会第174号决议（2014年，釜山，修订版）– 国际电联在防范非法使用ICT的风险的国际公共政策问题上的作用；

*c)* 全权代表大会第179号决议（2018年，迪拜，修订版）– 国际电联在保护上网儿童方面的作用；

*d)* 全权代表大会第181号决议（2010年，瓜达拉哈拉）– 有关树立使用ICT的信心和提高安全性的定义和术语；

*e)* 有关建立打击非法滥用信息技术法律框架的联合国大会第55/63号和第56/121号决议；

*f)* 有关培育全球网络安全文化的联合国大会第57/239号决议；

*g)* 有关培育全球网络安全文化及保护重要信息基础设施的联合国大会第58/199号决议；

*h)* 有关从外层空间遥感地球原则的联合国大会第41/65号决议；

*i*) 关于全面审查信息社会世界高峰会议（WSIS））成果落实情况的大会高级别会议成果文件的联合国大会第70/125号决议；

*j)* 有关数字时代的隐私权的联大第71/199号决议；

*k)* 有关加强在网络安全（包括抵制和打击垃圾信息）领域合作机制的世界电信发展大会（WTDC）第45号决议（2014年，迪拜，修订版）；

*l)* 有关抵制和打击垃圾信息的本届全会第52号决议（2022年，日内瓦，修订版）；

*m)* 有关重点鼓励发展中国家1建立国家计算机事件响应组的第58号决议（2012年，迪拜，修订版）；

*n)* 国际电联是《信息社会突尼斯议程》WSIS C5行动方面（树立使用ICT的信心并提高安全性）的主要推进方；

*o)* WSIS成果中与网络安全相关的条款，

考虑到

*a)* 电信/ICT基础设施及其应用对于各种形式的社会和经济活动至关重要；

*b)* 传统的公共交换电话网（PSTN）由于其分层结构和内在的管理系统而具备一定程度的固有安全属性；

*c)* 如果在安全设计和管理方面没有足够当心，IP网络会减少用户构件和网络构件之间的分离；

*d)* 因此，如果融合的传统网络和IP网络的安全设计和管理未得到充分重视，这些网络将更易受到入侵；

*e)* 网络安全是一个跨领域问题，网络安全格局既复杂又分散，涉及国家、区域和全球层面负责确定、审查和回应与树立使用ICT的信心并提高其安全性和恶意网络活动相关的问题的许多不同利益攸关方；

*f)* 给电信/ICT系统用户带来显著且日益增多损失的愈演愈烈的网络安全问题，无一例外地给全世界所有发达国家和发展中国家敲响了警钟；

*g)* 以下事实：关键电信/ICT基础设施在全球层面的互连互通意味着，一国基础设施安全保障不充分会导致其它国家更易受害和面临更大风险，因此合作十分重要；

*h)* 网络威胁和恶意网络活动的数量和方法日益增多，保护网络和系统免受其害是一项具有挑战性的任务，与此同时我们也愈来愈多地依赖于互联网及其他网络获取服务和信息；

*i)* 标准可为物联网（IoT）和智慧城市与社区（SC&C）的安全和安全相关方面提供支持；

*j)* 为保护全球电信/ICT基础设施免受网络安全领域日益猖獗的威胁和挑战，需要协调国家、区域和国际层面的行动，以针对安全事件做好防范、准备、响应和恢复工作；

*k*) 国际电联按照WTDC（2014年，迪拜）通过的《迪拜行动计划》已经和正在开展的工作，其中包括国际电联电信标准化部门（ITU-T）第17研究组、国际电联电信发展部门（ITU-D）第2研究组已经和正在开展的工作以及ITU-D第1研究组第22/1-1号课题的最后报告；

*l)* ITU-T在其考虑到*j)*段的职责和能力范围内发挥作用，

进一步考虑到

*a)* ITU-T X.1205建议书提供了定义、技术描述和网络保护原则；

*b)* ITU-T X.805建议书为识别安全隐患提供了系统框架，ITU-T X.509建议书提供了公钥和属性证书框架，ITU-T X.1500建议书提供了网络安全信息交换（CYBEX）模型并探讨了可用来方便网络安全信息交流的技术；

*c)* ITU-T和国际标准化组织（ISO）/国际电工技术委员会（IEC）的信息技术联合技术委员会（JTC 1）万维网联盟（W3C）、结构化信息标准促进组织（OASIS）、快速在线身份认证联盟（FIDO）、互联网工程任务组和电子和电气工程师学会等若干集团和标准实体已出版了大量资料并正在针对该议题开展大量的工作，这一点需得到考虑；

*d)* 在电子商务业务数据整个寿命期管理参考架构方面正在开展工作的重要性，

认识到

*a)* 责成电信标准化局（TSB）主任强化现有ITU-T各研究组内部工作的全权代表大会第130号决议（2018年，迪拜，修订版）的执行段落；

*b)* 2014年世界电信发展大会批准了提交《国际电联2016-2019年战略规划》的输入意见，对五项部门目标表示赞同，其中包括部门目标3 – 提高使用电信/信息通信技术的信心和安全性，并加强ICT应用和服务的部署，以及相关联成果3.1：树立使用ICT和服务的信心及安全性，在其执行框架内包括网络安全计划和ITU-D第3/2号课题；

*c)* 国际电联全球网络安全议程（GCA）促进旨在为增强ICT使用信心并提高安全性而寻找解决方案、制定战略的国际合作；

*d)* 各国，尤其是发展中国家，在树立使用ICT的信心和提高安全性方面所面对的挑战，

进一步认识到

*a)* 诸如网络钓鱼、网址嫁接、诈骗/入侵、分布式服务拒绝、网页涂改、非授权进入等网络安全事件或网络犯罪不断出现并带来严重后果；

*b)* 使用僵尸网络是传播僵尸恶意软件和进行网络犯罪的手段；

*c)* 恶意网络活动的来源有时难以确定；

*d)* 一些恶意网络活动是由连接到电信网络的系统和设备在没有充分认证的情况下造成的；

*e)* 通过引入分布式账本技术等新兴技术，可以减少未经授权访问ICT系统的情况，此类技术允许各类智能设备仅在经过验证程序后才能访问网络；

*f)* 注意到软件和硬件所面对的重大网络安全威胁可能需要及时进行缺陷管理和及时进行软硬件更新；

*g)* 确保数据安全是网络安全的核心组成部分，因为数据往往是恶意网络活动的目标；

*h)* 网络安全是树立使用电信/ICT的信心和提高其安全性的一项因素；

*i)* 安全性在系统/网络/应用/数据的整个生命周期中占据重要地位；

*j)* 公共安全架构十分重要，可被视作各种系统/网络/应用/数据的安全架构的基础，

注意到

*a)* ITU-T安全和身份管理问题的牵头研究组第17研究组及其它标准化机构（包括全球标准协作（GSC）组）在制定电信/ICT安全标准和建议书方面所开展的积极活动和各方对此的关注；

*b)* 有必要在尽量大的范围内协调国家、区域和国际战略，避免重复工作并优化资源的使用；

*c)* 各国政府、私营部门、民间团体、技术社团和学术界在各自职责范围内为树立使用信息通信技术的信心并提高安全性协作而付出的巨大努力与写作精神，

做出决议

1 根据ITU-T的能力和专业特长，继续在部门内部高度重视此项工作，包括促进各国政府和其它利益攸关方在国家和国际层面就树立使用ICT的信心和提高安全性达成共识；

2 所有ITU-T研究组均将继续依据第2号决议（2022年，日内瓦，修订版）规定的职责范围，评估现有的和不断演进的新建议书的设计稳健性以及被恶意行为方利用的可能，同时考虑到由全球电信/ICT基础设施支持的新服务和新应用（如包括但不局限于基于电信/ ICT网络的云计算、分布式账本技术、量子安全和物联网）；

3 ITU-T继续在其职责和能力范围内提高人们对于加强和防范信息和通信系统受到网络威胁和恶意网络活动影响的必要性的认识，并继续促进适当的国际和区域性组织之间的合作，以便加强信息和电信网络安全领域技术信息的交流；

4 ITU-T应与ITU-D密切合作，特别是围绕第3/2号课题 – 保障信息和通信网络的安全：培育网络安全文化的最佳做法；

5 ITU‑T继续为制定和完善有关树立使用电信/ICT的信心和提高安全性的术语和定义（包括术语“网络安全”）开展工作；

6 应促进建立全球、一致且可相互操作的进程，用于共享事件响应相关信息；

7 ITU-T各研究组继续与活跃在该领域的标准组织及其它机构联络；

8 在ITU-T标准制定整个进程中均需考虑安全问题；

9 制定测试和认证ICT系统安全性的规范和标准，以树立用户信心，并协助建立试验台和测试实验室，在发展中国家尤应如此；

10 应开发和维护安全、可信和适应力强的电信/ICT网络和服务，以增强对使用ICT的信心，

责成第17研究组

1 推进关于网络安全的研究，其中包括全球电信/ICT基础设施支持的新服务和新兴应用的安全；

2 支持电信标准化局主任维护“ICT安全标准路线图”，该路线图应包括推进安全相关标准化工作的工作项目，并作为安全领导小组的任务与ITU-R和ITU-D相关小组进行交流；

3 发起安全联合协调活动（安全JCA），并在国际电联和其他标准制定组织（SDO）的所有相关研究组和焦点组之间协调安全标准化活动；

4 与ITU-T所有其他研究组密切协作，制定一项行动计划，以评定ITU-T在应对安全漏洞方面的现有、演进中和新的建议书，并且继续定期向电信标准化顾问组（TSAG）提供有关电信/ICT安全的报告；

5 为信息系统/网络/应用/数据生命周期的每个阶段定义一套总体/通用的安全能力，以便从第一天起就能实现系统/网络/应用/数据的内在安全性（可通过设计来获得的安全能力和特征）；

6 设计具有安全功能组件的通用安全架构，这些组件可被视为各种系统/网络/应用/数据的安全架构设计的基础，以提高安全相关建议书的质量，

责成电信标准化局主任

1 在有关“ICT安全标准路线图”和ITU-D所开展的网络安全相关努力的基础上，在其它相关组织的帮助下，尽可能全面地清点国家、区域和国际性举措及活动并继续加以完善和更新，以便在世界范围内促进此重要领域战略和工作方法的统一，其中包括出台网络安全领域的通用方法；

2 如同全权代表大会第130号决议（2018年，迪拜，修订版）所规定的，就树立使用ICT的信心和提高安全性向提交国际电联理事会的年度报告提供文稿；

3 向国际电联理事会汇报“ICT安全标准路线图”活动所取得的进展；

4 继续承认在安全标准领域具有经验和特长的其他组织发挥的作用并酌情与这些组织开展协调；

5 通过与国际电联其它部门协作并与相关利益攸关方合作，继续实施并跟进有关树立使用ICT的信心和提高安全性的相关WSIS活动，从而分享有关国家、区域和国际以及全球有关网络安全的非歧视性举措的信息；

6 与秘书长提出的《全球网络安全议程》（GCA）及其它全球或区域性网络安全项目开展适当合作，酌情与各区域性和国际网络安全相关组织和举措发展良好关系和伙伴关系，并请所有成员国，特别是发展中国家参加这些活动，同时与这些不同活动进行协调与合作；

7 支持电信发展局主任协助成员国在发展中国家之间建立适当的框架，以便在重大事件发生时做出快速响应，并提出行动计划，加大保护力度，同时酌情顾及各种机制和伙伴关系；

8 支持相关ITU-T研究组开展与增强并树立使用ICT的信心和安全性相关的活动；

9 与电信发展局主任协作，通过组织培训项目、论坛、讲习班、研讨会等，向所有利益攸关方传播与网络安全有关的信息，其中包括政策制定机构、监管机构、运营商和其他利益攸关方，特别是来自发展中国家的利益攸关方，以提高认识并确定需求，

请各成员国，部门成员、部门准成员和相关学术成员

1 在考虑到全权代表大会第130号决议（2018年，迪拜，修订版）的情况下，通过密切协同加强区域和国际合作，从而增强使用ICT的信心并提高安全性，以便缓解网络风险和网络威胁；

2 开展合作并积极参与本决议的实施工作和相关行动，其中包括审查和更新其网络安全架构和协议设计；

3 参加相关ITU-T研究组的活动，制定网络安全标准和导则，以通过数据保护和安全机制树立使用ICT的信心并提高安全性；

4 利用相关ITU-T建议书及增补；

5 作为网络安全做法的一部分，制定网络风险管理机制，以挽回恶意网络活动（如网络保险）造成的各类损失和损害。

\_\_\_\_\_\_\_\_\_\_\_\_\_\_