概 要

经济合作与发展组织信息系统与网络安全准则
发展安全文化

Overview

OECD GUIDELINES FOR THE SECURITY

OF INFORMATION SYSTEMS AND NETWORKS

TOWARDS A CULTURE OF SECURITY

概要系根据经济合作与发展组织出版物摘录翻译而来。

概要可从在线书店免费索取

(www.oecd.org/bookshop)

该概要为经济合作与发展组织非正式译稿

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

经济合作与发展组织

信息系统与网络安全准则

发展安全文化

前言

1992 年经合与发展组织首次制定信息系统安全准则以来，信息系统与网络的利用以及信息技术整体环境均发生了引人注目的变化。这些持续的变化带来了巨大进步，同时也要求开发、拥有、提供和管理信息系统与网络服务和利用的政府、企业、其它组织以及个人(“参与者”)更加重视安全问题。

功能越来越强大的个人电脑、日益趋同的技术和互联网的广泛应用已经取代了过去以封闭型为主的网络中规模不大的独立系统。目前，参与者之间的相互联接日益密切，而且联接是跨越国界的。另外，互联网支撑着诸如能源、运输和金融之类重要基础设施，同时对公司的经营方式、政府为公民和企业提供服务的方式以及公民个人通讯和交换信息方式产生重大影响。通讯与信息基础设施构成技术的性质与类型同样已发生了显著变化。基础设施接入设备的数量和性质也在成倍增加，扩大到包括固定、无线和移动设备，而且“不间断”式接入的比例越来越高。从而，经过交换的信息的性质、数量和敏感性均实质性扩大了。

由于相互联通日益增多，目前信息系统和网络呈现出越来越多种类的薄弱之处，同时暴露在数量种类越来越多的危险之下。因此，本准则适用于新的信息社会之内的所有参与者，同时提出了扩大对安全问题的认识和发展“安全文化”的必要性。

I. 发展安全文化

本准则是通过促进安全文化的发展，即在发展信息系统和网络过程中重视安全问题、在信息系统和网络之间的利用和相互作用过程中采用新的思维和行为方式，对不断变化的安全环境做出的迅速反应。该准则清楚表明了一个总是要事后才能想起网络和系统的安全设计与作用的时代已经结束。参与者已经变得越来越多地依赖于信息系

统、网络和相关服务，而所有这一切都必须可靠安全。只有一个能够适当考虑所有参与者的利益，以及系统、网络和相关服务的性质的方法才能保证有效的安全。

每一个参与者都是保证安全的重要角色。参与者应根据其职责，了解相关安全风险、预防性措施，并承担相应责任、采取措施提高信息系统与网络的安全性。

促进安全文化既需要领导角色，也需要广泛的参与。安全文化的发展应能够加深所有参与者对安全需求的理解，而且能够提高安全计划与管理的优先地位。各级政府、企业和所有参与者应关注安全问题并承担责任。准则生机条款奠定了在全社会发展安全文化的工作基础。这将使参与者能够在设计和利用所有信息系统与网络时考虑到安全因素。准则建议所有参与者将安全文化作为构思、分析、控制和操作信息系统与网络的一种思维方法加以接受并推广。

II. 目标

本准则的目标是：

- 将安全文化作为保护信息系统与网络的手段向所有参与者推广。
- 提高对信息系统与网络风险的认识；提高对可用于应对风险的作法、措施和程序的认识；提高对采纳和实施这些政策、作法、措施和程序的必要性的认识。
- 提高所有参与者对信息系统与网络以及对其提供与利用方式的信心。
- 建立一个通用的参考框架，协助参与者理解安全问题，并有助于在发展与落实连贯的信息系统与网络安全政策、做法、措施和程序过程中尊重伦理价值观。
- 在发展与落实安全政策、作法、措施与程序过程中，促进所有参与者之间的适当合作与信息共享。
- 促进介入制定和执行标准的所有参与者将安全作为一个重要目标来考虑。

III. 原则

下述九项补充原则应作为一个整体来理解。这些原则涉及到各个层面的参与者，包括政策与操作层面。根据本准则，参与者的责任因其职责而异。认识、教育、信息共享与培训会有助于更好地理解安全问题，有助于采取更好的作法，这将对所有参与

者带来帮助。为提高信息系统与网络安全而做出的努力应符合民主社会的价值观，尤其要尊重对信息开放与流动自由的需求以及对个人隐私的基本关注。[1]

1) 认识

所有参与者均应认识到信息系统与网络安全的需要、认识到他们可以为提高安全性可以做些什么。

认识到风险的存在和了解现有保障措施是保护信息系统与网络安全的起点。信息系统与网络可以受到来自内部和外部风险的影响。参与者应认识到安全失误会极大的损害其控制的系统与网络。他们也应认识到由于想到相互联通和相互依赖而对其它系统产生的潜在危害。参与者应了解其系统的配置与可采用的升级更新、系统在网络中的位置。参与者可以用来提高安全性的好做法，并了解其它参与者的需求。

2) 责任

所有参与者均对信息系统与网络的安全负有责任

参与者依赖于相互联接的本地和全球信息系统与网络，而且应认识到其对信息系统与网络安全所负有的责任，并承担与其角色相应适应的负责。参与者应定期审查自身的政策、做法、措施和程序并分析它们是否与其所处环境相适合。开发、设计和提供产品与服务的参与者应解决系统与网络的安全问题，并传播包括及时地升级更新在内的适用信息，这样用户可以更好的理解产品与服务的安全功能及其与安全相关的责任。

3) 反应

参与者应以及时和合作的方式采取行动，预防、查明安全事件并做出反应。

认识到信息系统与网络之间的相互联通性以及迅速并广泛传播的潜在破坏，参与者应以及时和合作的方式展开行动来处理安全事件。他们应当适当地分享有关危险与薄弱之处的信息，并实施可能迅速和有效合作预防、查明安全事件，并做出反应的程序。在允许的情况下，可能要发生跨国界信息共享与合作。

[1] 在安全准则之外，经合与发展组织还提出对世界信息界十分重要的其它准则的补充建议。这些建议涉及隐私权(1980 年经合与发展组织保护隐私权与个人数据跨国界流动管理准则)和密码(1997 年经合与发展组织密码政策准则)。本安全准则条款应与这些准则结合执行。)

4) 道德规范

参与者应尊重其他参与者的合法利益。

鉴于信息系统与网络已经普遍深入地存在于我们的社会，参与者必需认识到采取行动或无动于衷均会殃及他人。因此符合道德规范的行为是至关重要的，而且参与者应努力制定并采取最佳做法，并推广顾及安全需求并尊重其他人合法权益的行为。

5) 民主

信息系统与网络的安全必须与民主社会的核心价值观相容。

实现信息系统与网络安全的方式应当符合民主社会承认的价值观，包括交流思想与观念的自由、信息流动的自由、信息和通讯保密权力、个人信息的适当保护以及开放与透明度。

6) 风险评估

参与者应开展风险评估

风险评估可以发现存在的危险和容易受到破坏的薄弱之处。风险评估在包括内部和外部关键因素的充分广泛范围内进行，包括隐含安全影响的技术、物理和人为因素、政策及第三方服务。通过风险评估，能够确定可接受风险等级，有助于根据需要保护信息的性质与重要性选择适当的管理方法，控制信息系统与网络面临的潜在危害。由于信息系统之间的相互联通不断扩大，风险评估还应包括分析对其他方面或来自其它方面的潜在危害。

7) 安全设计与实施

参与者应将安全作为至关重要的成分纳入信息系统与网络

为实现最佳安全状况，需要妥善地设计、实施和协调系统与网络。这方面努力的一个主要，但非唯一的工作重点是设计并采用适当的防卫方法和解决方案，以避免或限制由已经明确的威胁和薄弱之处导致的潜在危害。技术和非技术防卫方法和解决方案都是必须的，而且应与各机构的系统与网络内信息的价值成比例。安全应是所有产品、服务、系统和网络的根本性内容，而且是系统设计与构架的必然组成部分。对于最终用户而言，安全措施的设计与落实大体上包括选择和设置其系统的产品与服务。

8) 安全管理

参与者应采取全面性安全管理方法

安全管理应以风险评估为基础，并积极地涉及到参与者活动的各个层面和参与者业务的所有方面。安全管理应包括对不断显现的威胁的前瞻性反应，应解决安全事件的预防、发现和应对、系统恢复、日常维护、审查和审计问题。应当协调和综合信息系统与网络安全的政策、作法、措施和程序，以建立连贯性的安全制度。安全管理的要求取决于介入水平、参与者的职责、牵扯到的风险和系统要求。

9) 再评估

参与者应审查和再评估信息系统与网络安全，并对安全政策、作法、措施和程序做出适当调整。

新的而且变化的危险和薄弱环节在不断地被发现。参与者应持续地审查、再评估并完善与安全有关的各个方面，以应付变化之中的风险。

理事会关于信息系统与网络安全准则的建议

发展安全文化

理事会

注意到 1960 年 12 月 14 日通过的经济合作与发展组织公约，特别是其中第 1 条 b)款、c)款和第 5 条 b)款；

注意到 1980 年 9 月 23 日理事会关于保护隐私权与个人数据跨国际流动管理公约[C(80)58(Final)]的建议；

注意到经合与发展组织成员国政府于 1985 年 4 月 11 日通过的跨国界数据流动宣言[Annex to C(85)139]；

注意到 1997 年 3 月 27 日理事会关于密码政策准则的建议[C(97)62/FINAL]；

注意到 1998 年 12 月 7-9 日关于在全球网络中保护隐私权的部长会议宣言[Annex C(98)177/FINAL]；

注意到 1998 年 12 月 7-9 日关于电子商务验证的部长会议宣言[Annex C(98)177/FINAL]；

认识到对于政府、企业、其它组织和个人用户而言，信息系统与网络的用途和价值日益扩大；

认识到信息系统与网络日益扩大的重要作用和国民经济、国际贸易的稳定与效率日益依赖于信息系统与网络，以及社会、文化和政治生活要求投入特别的努力保护信息系统与网络，并增强对信息系统与网络的信心；

认识到信息系统与网络及其在世界性扩展始终伴随着新的和不断扩大的风险；

认识到由信息系统与网络存储、传输的数据与信息面临着来自未经授权闯入、利用、盗用、改动、传输恶意代码、拒绝服务或破坏等不同形式的威胁，并且需要得到适当保护；

认识到必须提高对信息系统与网络面临风险的认识，必须提高对风险应对政策、作法、措施和程序的认识，而且必须鼓励将适当的作法发展安全文化的关键步骤；

认识到必须审查当前的政策、作法、措施和程序，以保证它们能够应对信息系统与网络所受威胁引起的不断变化的挑战；

认识到在借助安全文化提高信息系统与网络安全性的过程中存在着共同利益。安全文化有利于为应对安全故障对国家经济、国际贸易和参与者在社会、文化和政治生活方面的潜在危害所带来的挑战而进行的国际协调与合作；

并进一步认识到本建议附件中陈述的信息系统与网络安全准则：发展安全文化属于自愿性，而且不触及国家主权；

认识到，本准则无意指出存在任何一种适用于任何特殊情况的安全解决方案或某种政策、做法、措施和程序，准则提供的是一个原则框架，目的是促进更好地理解参与者如何受益并为安全文化发展做出贡献。

向开发、拥有、提供、管理、服务和利用信息系统与网络的政府、企业，其它组织与个人用户推荐信息系统与网络安全准则：发展安全文化；

建议成员国：

制定新的，或修订已有政策、作法、措施和程序，通过接受和推广准则中陈述的安全文化，反映并考虑信息系统与网络安全准则：发展安全文化；

为执行准则条款，在国内和国际水平开展磋商、协调和合作；

向公共和私营部门全面传播本准则，包括政府机关、企业，其它组织和个人用户，以推广安全文化，并鼓励有关各方承担责任并采取必要步骤以适合其职责的方式执行本准则条款；

以及时并适当的方式向非成员国家散发本准则；

每 5 年对准则进行一次审核，以促进信息系统与网络安全相关事宜的国际合作；

指示经合与发展组织信息、计算机与通讯政策委员会促进本准则的实施。

本建议取代 1992 年 11 月 26 日理事会关于信息系统安全的准则[C(92)188/FINAL]。

信息系统与网络安全准则起草过程

安全准则于 1992 年首次起草完成，并于 1997 年进行了审核。目前的审核于 2001 年开始。由信息安全与隐私权工作组（WPISP）遵照信息、计算机和通讯政策委员会的要求进行审核。受 9.11 悲剧的影响，审核进程在加快了。

信息安全与隐私权工作组内一个专家组负责起草准则。专家组分别于 2001 年 12 月 10-11 日、2002 年 2 月 12-13 日和 2002 年 3 月 4 日和 6 日在华盛顿特区、悉尼和巴黎召开了会议。信息安全与隐私权工作组分别于 2002 年 3 月 5-6 日、4 月 22-23 日和 6 月 25-26 日在巴黎召开了会议。

目前版本的经合与发展组织信息系统与网络安全准则：发展安全文化是作为经合与发展组织理事会的建议于 2002 年 7 月 25 在 1027 届理事会会议上批准的。

出版物英文原文目录(不包括附件、插文、表格和图)

信息与网络安全准则：
安全文化 7
前言 7
I. 发展安全文化 8
II. 目标 8
III. 原则 9
理事会建议 13
大事记 16

本概要根据下述文件的摘要翻译：

OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security

Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information : vers une culture de la sécurité

经济合作与发展组织出版物在巴黎中心有售
地址：2, rue André-Pascal, 75775 Paris Cedex 16, FRANCE
也可通过互联网购买：www.oecd.org/bookshop

免费索取本概要，请浏览：
www.oecd.org/bookshop

本概要由公共事务与交流司版权与翻译处制作。

电子邮件：rights@oecd.org
传真：+33 1 45 24 13 91