项目描述

数据分类分级实践

促进以数据为中心的安全管理

Karen Scarfone
Scarfone Cybersecurity

Murugiah Souppaya
National Institute of Standards and Technology

2021年7月

data-nccoe@nist.gov

NIST National Institute of Standards and Technology U.S. Department of Commerce

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

国家网络安全卓越中心（NCCoE）是美国国家标准与技术研究所（NIST）的一个分部。它是一个协作中心，行业组织、政府机构和学术机构在此共同解决企业最紧迫的网络安全挑战。通过这种合作，NCCoE开发了模块化、适应性强的网络安全解决方案范例，展示了如何通过使用可购买的商用技术来应用标准和最佳实践。要了解有关NCCoE的更多信息，请访问https://www.nccoe.nist.gov/。有关NIST的更多信息，请访问https://www.nist.gov/。

本文件描述了一个与许多行业部门都相关的挑战。NCCoE网络安全专家将通过与包括网络安全解决方案供应商在内的利益共同体开展合作来应对这一挑战。由此产生的参考设计将详细说明一个可以被纳入多个部门的方法。

摘要

作为零信任方法的一部分，以数据为中心的安全管理旨在加强对信息（数据）的保护，无论数据位于何处或与谁共享。以数据为中心的安全管理必须依赖于组织了解他们拥有什么数据，其特征是什么，以及它需要满足什么样的安全和隐私保护要求，从而实现必要的保护。为了使以数据为中心的安全管理可以规模化实施，需要有标准化机制来传递数据特征和保护要求。本项目将研究这样一种基于定义和使用数据分类分级的方法。本项目的目标是为了开发与具体实现技术无关的推荐实践，用以定义数据分类分级和数据处理规则集，并向他人传递。本项目有助于数据分类分级和数据处理规则集的传递，将为现有网络安全和隐私风险管理过程提供信息，并可能找到改进的机会。它不会取代当前的风险管理实践、法律、法规或授权。本项目将产生一个免费的NIST网络安全实践指南。

关键字

以数据为中心的安全管理;数据分类分级;数据标签;数据保护;零信任体系结构;零信任安全

鸣谢

我们感谢来自摩根大通、微软、摩根士丹利、北约、NIST和Varonis的专家，他们在数据分类分级研讨会上发言，并为制定本项目说明做出了贡献。我们也感谢在公众评论期间花时间提供反馈的个人和组织。

免责声明

为了充分描述一个实验程序或概念，某些商业实体、设备、产品或材料可能在本文件中被标识。这种标识并不意味着NIST或NCCoE的推荐或认可，也不意味着相关实体、设备、产品或材料必定是最佳的。

目录

1 执行概要

目的

在任何业务中，取得成功的一个关键因素是能够切实高效地共享信息和协作，同时满足保护这些信息的安全和隐私要求。传统的以网络为中心的安全措施侧重于保护通信和信息系统，提供围绕用户、主机、应用程序、服务和终端具有多个复杂安全层的基于边界的安全防护。随着系统变得更加分散、移动、动态以及在不同环境和在归属不同的管理类型间进行共享，这种模式在保护信息方面越来越低效。

作为零信任方法[1]的一部分，以数据为中心的安全管理旨在加强对信息(数据)的保护，无论数据位于何处或与谁共享。以数据为中心的安全管理必须依赖于组织了解他们拥有什么数据，其特征是什么，以及它需要满足什么安全和隐私需求，以便实现必要的保护。为了使以数据为中心的安全管理可规模化实施，需要有标准化的跨系统和组织的数据特征和保护要求传递机制。这方面的理想方法是定义和使用数据分类分级，本项目将研究这种方法。

本文件定义了一个正在征集反馈的国家网络安全卓越中心（NCCoE）项目。本项目重点关注数据管理和保护背景中的数据分类分级，以支持业务用例。本项目的目标是为了说明并具体实现与技术无关的推荐实践，该推荐实践用于定义数据分类分级和数据处理规则集，并把定义内容与他人传递。各组织还能够使用推荐的实践，为其他安全管理目的编目和描述数据，例如为向后量子计算加密算法的过渡做准备和确定优先级。

本项目将着重于通过数据分类分级和标签来传递和保障数据保护要求。网络安全和隐私风险管理过程以及其他来源的数据保护要求超出了项目范围，强制执行数据保护要求的机制也是如此。本项目有助于数据分类分级和数据处理规则集的传递，将为现有风险管理过程提供信息，并可能找到改进的机会。它不会取代当前的风险管理实践、法律、法规或授权。

本项目将产生一份公开的NIST网络安全实践指南，该指南详细介绍了为应对此挑战而实施网络安全参考设计所需的实践步骤。

范围

本项目将采用分层和模块化的方法，以实现组织内部和跨组织边界的共享和协作。本项目将强调一条数据分类分级成熟度等级的演化路径，并被设计为可被任何组织级别（如部门、分部或组织）和任何地理位置内或跨地域采用。

本项目的第一阶段将定义与支持技术、服务、架构、操作环境等无关的解决方案方法。作为其中的一部分，将尝试一种简单的概念验证方法来实现该方法。概念验证将包括有限的数据发现、分析、分类分级和标签功能，以及表达每个用例场景中应如何处理带有特定标签的数据的

基础方法。为了支持此项目阶段，将根据现有实践和指南定义基本术语和概念，以提供讨论数据分类分级的通用语言。

本项目的后续阶段将建立在第一阶段的基础上，处理标准、技术、过程和推荐实践，以发现和执行数据分类分级、传递数据分类分级信息，从而对数据进行适当的保护和控制。这些信息将贯穿整个数据生命周期，跨设备和跨应用负载，跨多个经营场所、混合和云环境。后续阶段将主要集中于下列领域:

- 部署针对信息发现、分类分级、标签的附加解决方案，包括了安全持久性和与内容的绑定、互操作性、与信息生命周期相一致的生命周期管理的要求。
- 附加标签用于解决诸如来源和血缘、分类分级/敏感性、可释放性、与信息生命周期和共享相适应的策略定义和生命周期管理执行的适当机制等方面的问题。这将涵盖与隐私和安全有关的监管和业务策略。这些策略将由用例场景驱动。
- 按照现有网络安全和隐私风险管理框架的建议，确定适当的控制措施，以管理、监测、执行和证明符合所定义的分类分级，以便在整个信息生命周期内通过审计支持有效的、动态的安全和隐私风险管理。
- 用于申明和实施分类分级标签、数据处理规则集以及访问控制、权限管理和加密保护等相应控制措施的技术和工业标准。
- 针对最终用户意识教育和培训、应对不合规或网络安全事件、持续改进分类分级、数据处理规则集和控制的推荐实践。

假设/挑战

假设读者了解风险管理过程和基本的数据保护和零信任概念。

背景

数据分类分级和标签正成为更普遍的需求。在数字计算的早期，数据分类分级主要与武装部队和国防工业有关。诸如“绝密”这样的分类分级术语，虽然由于媒体的描述而为公众所熟知，但在特定政府机构和军事情景之外几乎完全不存在。

许多力量已经开始对所有组织施加压力，这些组织已经将数据分类分级和标签推到最前沿，并导致了建立用于所有数据的模型的紧迫感。如《加州消费者隐私法案》(CCPA)、《儿童在线隐私保护法案》(COPPA)、《公平信用报告法案》(FCRA)/《公平准确信用交易法案》(FACTA)、《家庭教育权利和隐私法案》(FERPA)、《通用数据保护条例》(GDPR)、《金融服务

现代化法案》(GLBA)、《健康保险携带和责任法案》(HIPAA)以及支付卡行业数据安全标准(PCI DSS) 等法规和标准强制要求包含特定类型信息的数据应采用特定的安全措施进行处理。随着新法规的出现和现有法规的修订，一个组织已拥有的大部分数据可能需要进行分类分级或差异化处理。

各个组织正在同时应对存储数据量的快速增长和保护和控制这些数据要求的快速增加，其中包括更长时间的数据保存期。这将导致可预见的更大的资本性支出和管理支出。沟通传递数据分类分级结果和数据处理规则集的能力可提高资源支出和分配的效率，因为所使用的控制措施可以与指定的数据分类分级相符合。此外，在满足安全、隐私和监管合规要求的同时，还需要打破数据孤岛，实现跨组织边界的数据共享，以支持业务目标。这种需求可能因部门而异。

现有的NIST关于数据分类分级和标签的标准和指南，如联邦信息处理标准（FIPS）199[2]和NIST特别出版物（SP）800-60[3]，解决了联邦政府的特定要求，但没有解决联邦机构和其他组织所要遵守的其他诸多要求。

一般来说，妨碍有效使用数据分类分级方法的重大挑战包括以下几点：

- 政府和军队之外现存的数据分类分级标准的局限性，意味着大多数组织没有使用与其合作伙伴和供应商一致的分类分级。组织与其他组织间执行难以计数的与数据分类分级和保护相关的业务，而行业标准的缺失削弱了组织强制执行数据处理要求的能力。

- 缺乏对分类器的共同定义和理解，会导致信息的分类分级和标签不一致。依赖最终用户识别和分类分级由他们创建和接收的数据尤易出错且不完整。

- 数据无处不在：在设备上（如笔记本电脑、台式机、移动设备），在经营场所内和外包环境中运行的应用程序中，以及在云中。数据的这种分布式特性导致建立和维护数据清单的过程变得复杂。

- 数据分类分级和数据处理需求经常在数据生命周期中发生变化，例如，数据的机密性先被保护，然后此数据被公开发布。另一个例子是数据被保护和保留一段时间，然后被销毁以防止再被访问。由于量子计算技术对受当前公钥算法保护的数据构成了威胁，随着量子计算技术的进步，这一问题变得更加复杂。

- 本项目旨在应对这些挑战，并使任何规模和复杂程度的组织都能启动和维护一个解决方案，以定义和传递数据分类分级、标签、数据处理规则集。本项目还旨在

为FIPS 199、NIST SP 800-60和其他NIST出版物的未来更新提供信息。

2 场景

我们在项目第一阶段考虑的用例场景如下：

场景1：金融领域

此场景涉及到一个大型的受监管的金融部门组织，根据法规和法律要求，该组织必须保护其客户的个人电话号码不被未经授权的访问和更改。该组织还将其客户信息提供给某些商业伙伴（例如，在合同中共享数据），并要求这些伙伴代表该组织保护电话号码。这些合作伙伴分布在多个司法管辖区。

场景2：政府领域

此场景涉及来自几个国家的政府机构、国际组织和非政府组织的联盟，它们需要相互协作并分享信息。支持的用例包括撰写和编辑报告，召开网络会议，作为一个团体讨论工作并相互分享材料，交换电子邮件和聊天信息，以及在自动系统之间发送特定的应用数据。不同合作伙伴之间的信任程度会有很大的不同，在联盟中有几个独立的管理机构。

场景3：制造业领域

此场景涉及一家小型制造公司。该制造商拥有只能让特定雇员、承包商和商业伙伴能够接触到的商业秘密，。

场景4：技术领域

此场景涉及一家小型技术公司，该公司正在放弃其办公室租赁，过渡到100%的随时随地办公。随着公司的过渡，它也将采用零信任架构原则。这个场景的焦点是一个特定产品源代码的完整性。该代码存储在公司基于云的代码库中。

场景5：医疗保健领域

此场景涉及到小型医疗机构，它需要根据患者的授权或法律法规要求与其他医疗机构共享受保护的健康信息（PHI）。该医疗机构还需要确保在规定的时间期限内保留所有的PHI，并且一旦不再需要保留了就将其销毁。

对于每个场景，我们将做以下工作：

1. 记录一个概念性的架构，该架构
    a. 显示直接参与或受数据分类分级活动影响的人员、系统、应用程序和服务以及终端用户设备。这些将体现此场景的代表性，而不是综合性。
    b. 标志数据生命周期活动，如数据创建/捕获、处理、存储、传输/传送/共享、保留和销毁。这些活动对于场景来说将是有代表性的，而不是全面的。
    c. 在一个数据分布在许多地方的应用程序中、被许多设备处理并由不同的用户随时随地访问的世界中，强调数据分类分级是如何在减轻对数据保护的担忧上发挥基础作用，例如数据泄漏。
    d. 不一定包括强制执行数据或系统保护安全控制的实施。情景和架构的目的

是探索数据分类分级和表达这些分类分级的具体挑战，而不是针对特定组织如何将表达的分类分级转化为实施的安全控制。

2. 定义将应用于场景中特定数据集的数据分类分级。分类分级必须考虑适用的规章、法律和组织政策。
3. 创建一个数据处理规则集，以根据数据分类分级为场景中的数据指定强制要求。该数据处理规则集必须与数据分类分级完全兼容，并包括强制数据保护要求、安全数据共享要求、数据保留要求等。
4. 在NCCoE实验室和云环境中实现概念架构。
5. 在实施中，将必要的信息(数据分类分级、数据处理规则集等)传递给已部署环境中必要的个人、系统和组织。

3 高级结构

组件列表

高级架构将包括但不限于以下组件:

- **终端**
  - **客户端设备：**各种PC（台式机或笔记本电脑）和移动设备将参与数据的创建、存储、传输、保留和销毁，以及以数据为中心的安全管理。一些客户端设备将由组织管理，一些将由组织的员工使用，而另一些将由其他组织的人使用。
  - **客户端设备应用程序：**客户端设备将拥有用于数据生命周期活动的商用现货（COTS）应用程序，如文字处理软件和电子邮件客户端软件。
  - **附加设备：**可被利用的附加设备的例子是联网的打印机和物联网（IoT）设备。
- **网络/基础设施设备** - 该架构将包括提供网络功能和网络流量限制所需的设备，如防火墙、路由器或交换机，以及管理这些设备的软件。
- **服务和应用** - 该架构将包括几种类型的服务和应用，它们参与一个或多个场景的数据生命周期活动。以下是可能的服务和应用类型的例子：
  - **企业服务/应用：**电子邮件、协作、文件共享、网络会议、文件/数据备份、代码库、内容管理系统。
  - **数据服务/应用：**数据处理、数据分析、人工智能/机器学习服务。
  - **商业服务/应用：**各种系统对系统和人对系统的业务应用，包括商用现货

COTS和自定义编写的，包括那些产生和/或消费数据的应用。

- **数据分类分级解决方案** - 该架构将包括用于履行数据分类分级职责的几种类型的组件，如数据发现、梳理、分析、分类分级和标签。

所需的安全能力

本项目旨在利用可获得的商用技术，开发一个符合以下特点的参考设计和实现：

- 所有的数据都被发现并进行分析，以确定其应该如何被分类分级。
- 所有数据分类分级和数据处理规则集的创建、修改和删除都只限于经授权的人员，所有行动都有记录和可审计，所有通信都受到保护。
- 对于所有的数据分类分级和数据处理规则集，都有一个机制来验证策略或规则集的完整性。
- 数据分类分级标签或标识被分配给所有数据。
- 对于分配给数据的所有数据分类分级标签或标识，都有一个机制来验证标签或标识的完整性。

4 相关标准和指南

以下资源和参考资料提供了更多的信息，可以用来开发这个解决方案：

- National Institute of Standards and Technology (NIST), Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, April 2018 https://doi.org/10.6028/NIST.CSWP.04162018
- NIST Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004 https://doi.org/10.6028/NIST.FIPS.199
- NIST Internal Report (IR) 8112, Attribute Metadata: A Proposed Schema for Evaluating Federated Attributes, January 2018 https://doi.org/10.6028/NIST.IR.8112
- NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0, January 2020 https://doi.org/10.6028/NIST.CSWP.01162020
- NIST Special Publication (SP) 800-53 Rev. 5, Security and Privacy Controls for Information

Systems and Organizations, September 2020
https://doi.org/10.6028/NIST.SP.800-53r5

- NIST SP 800-60 Vol. 1 Rev. 1, Guide for Mapping Types of Information and Information Systems to Security Categories, August 2008
https://doi.org/10.6028/NIST.SP.800-60v1r1
- NIST SP 800-154 (Draft), Guide to Data-Centric System Threat Modeling, March 2016 https://csrc.nist.gov/CSRC/media/Publications/sp/800-154/draft/documents/sp800_154_draft.pdf
- NIST SP 800-171 Rev. 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, February 2020
https://doi.org/10.6028/NIST.SP.800-171r2
- NIST SP 800-207, Zero Trust Architecture, August 2020
https://doi.org/10.6028/NIST.SP.800-207

附录A 参考文献

[1] National Institute of Standards and Technology (NIST), NIST Special Publication (SP) 800-207, Zero Trust Architecture, August 2020
https://doi.org/10.6028/NIST.SP.800-207

[2] National Institute of Standards and Technology (NIST), NIST Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004
https://doi.org/10.6028/NIST.FIPS.199

[3] National Institute of Standards and Technology (NIST), NIST Special Publication (SP) 800-60 Vol. 1 Rev. 1, Guide for Mapping Types of Information and Information Systems to Security Categories, August 2008
https://doi.org/10.6028/NIST.SP.800-60v1r1

附录B 缩略语

CCPA	California Consumer Privacy Act 加州消费者隐私法案
COPPA	Children's Online Privacy Protection Act 儿童在线隐私保护法案
COTS	Commercial-Off-the-Shelf 商用现货
FACTA	Fair and Accurate Credit Transactions Act 公平和准确的信贷交易法
FCRA	Fair Credit Reporting Act 公平信用报告法
FERPA	Family Educational Rights and Privacy Act 家庭教育权利和隐私权法案
FIPS	Federal Information Processing Standard 联邦信息处理标准
GDPR	General Data Protection Regulation 通用数据保护条例
GLBA	Gramm Leach Bliley Act 格拉姆-里奇-布莱利法案，也称为：金融服务现代化法案
HIPAA	Health Information Portability and Accountability Act 健康保险携带和责任法案
IoT	Internet of Things 物联网
IR	Internal Report 内部报告
NCCoE	National Cybersecurity Center of Excellence 国家网络安全卓越中心
NIST	National Institute of Standards and Technology 国家标准和技术研究院
PC	Personal Computer 个人电脑
PCI DSS	Payment Card Industry Data Security Standard 支付卡行业数据安全标准
PHI	Protected Health Information 受保护的健康信息
SP	Special Publication 特别出版物

翻译说明

翻译声明：

原文来自NIST公开网站，翻译为公益性质，仅供信息安全产业相关研究人员、管理人员参考，如有错漏敬请指正。

内容提要：

随着全球经济形式的转变及数字化转型的发展，数据生产要素已经成为未来数字时代的最重要资源，如何保护数据安全也将是未来一段时间内讨论的重点。本次翻译的目的旨在跟踪国际数据安全保护的发展动态，共同探讨、研究数据安全的基本理论及方法。本文是美国国家网络安全卓越中心（NCCoE）正在开展的研究项目说明，重点讨论了“以数据为中心的安全管理”的背景、特征及主要关注点，可供相关研究人员参考、借鉴。天融信多年来持续关注数据安全的最新进展，未来将陆续发布相关翻译文献及研究报告，敬请关注。