ICS 35.030
CSS L80

中华人民共和国国家标准

GB/T XXXXX—XXXX

数据安全技术 数据接口安全风险监测方法

Data security technology — Data interface security risk monitoring methods

（征求意见稿）

本稿完成日期：2024-07-20

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分:标准化文件的结构和起草规则》的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本文件由全国网络安全标准化技术委员会（ SAC/TC260）提出并归口。

本文件起草单位：全知科技（杭州）有限责任公司、公安部第三研究所、中国电子技术标准研究院、国家信息中心、中国信息安全测评中心、中国网络安全审查技术与认证中心。

本文件主要起草人：（待补充）。

数据安全技术　数据接口安全风险监测方法

1　范围

本文件给出了数据接口安全风险监测的方法，包括方式、内容、流程等，明确了数据接口安全风险监测各阶段的监测要点。

本文件适用于指导各类组织开展的数据接口安全风险监测活动。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069-2022　信息安全技术　术语

GB/T 35273-2020　信息安全技术　个人信息安全规范

GB/T 39204-2022　信息安全技术　关键信息基础设施安全保护要求

3　术语和定义

GB/T 25069—2022界定的以及下列术语和定义适用于本文件。

3.1

数据接口 data interface

信息系统之间进行数据传输和交换的一种机制，它描述了一个由接口服务端和客户端共同遵守的合约，通常会约定数据的格式、通信协议、传输结构等。

3.2

监测需求方 monitoring stakeholders

具有监测需求的组织或实体。

3.3

风险源 risk source

可能导致危害数据的保密性、完整性、可用性和数据处理合理性等事件的威胁、脆弱性、问题、隐患等，也称“风险隐患”。

注:风险隐患，既包括安全威胁利用脆弱性可能导致数据安全事件的风险隐患，也包括数据处理活动不合理操作可能造成违法违规处理事件的风险隐患。

4　缩略语

下列缩略语适用于本文件。

Web API：网络应用程序接口（World Wide Web Application Programming Interface）

API：应用程序接口（Application Programming Interface）

HTTP：超文本传输协议（Hyper Text Transfer Protocol）
HTTPS：安全超文本传输协议（Hypertext Transfer Protocol over Secure Socket Layer）
JSON：JavaScript对象表示法（JavaScript Object Notation）
SSL：安全套接层协议（Secure Socket Layer）
TLS：安全传输层协议（Transport Layer Security）
SQL：结构化查询语句（Structured Query Language）

5 概述

5.1 数据接口

本文件所监测的数据接口是指跨网络区域、信息系统等环境，用于完成包含核心数据、重要数据及个人信息等数据传输交换的接口，常见的数据接口技术形态为Web API、文件下载接口等。关于数据接口常见场景、结构及技术形态参见附录A。

5.2 数据接口要素关系

数据接口安全风险监测涉及客户端、服务端、接口、交换数据、提供行为、调用行为等基本要素及其关系，要素关系如图1所示。

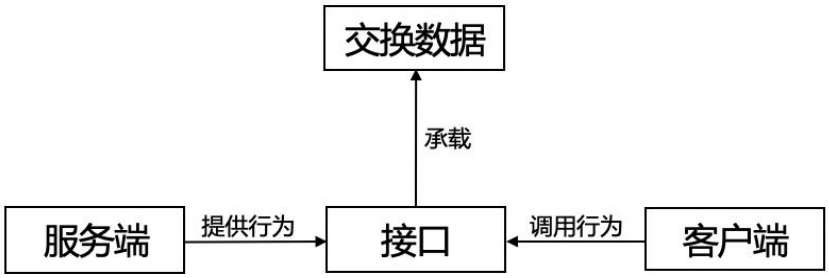

图1 数据接口要素及其关系

开展数据接口安全风险监测应充分考虑要素及其关系，确定要素可能引起的风险，各个要素关系说明如下：

a) 接口是核心要素，承载数据，完成服务端和客户端之间的数据交换；
b) 为满足数据交换的需求，服务端通过提供数据接口的方式对外开展数据服务；
c) 为完成数据交换，客户端触发调用行为，利用数据接口获取或提交数据。

5.3 风险监测方法框架

数据接口安全风险监测方法，由监测内容、监测方式和监测流程等部分组成。数据接口安全风险监测方法框架如图2所示。

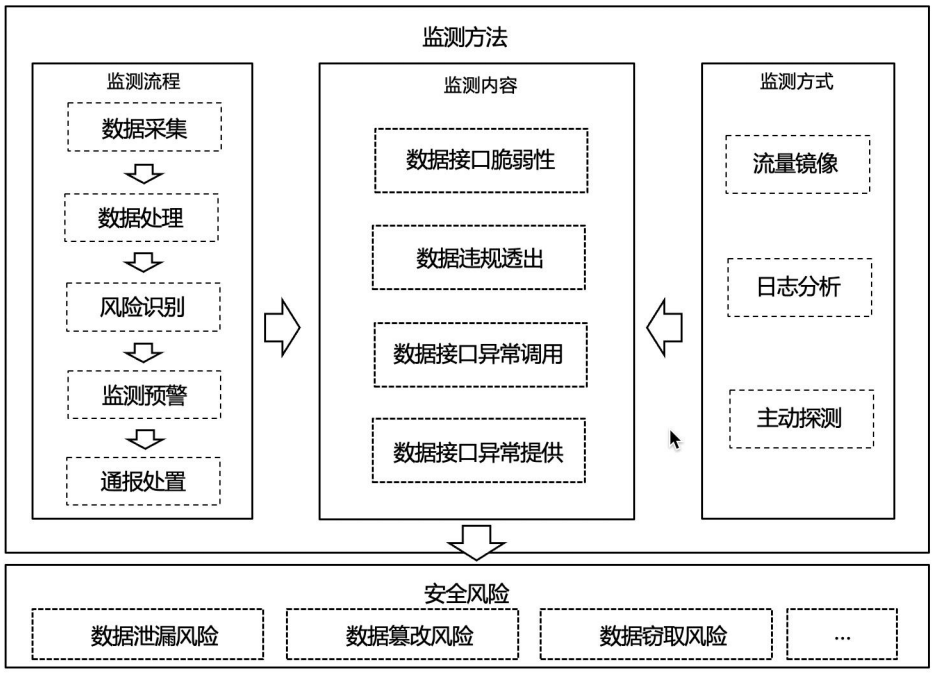

图 2 数据接口安全风险监测方法框架

5.4 监测过程控制

应采用适当的手段满足监测过程的安全性、合规性，包括但不限于：

a) 应对监测行为进行审计，记录监测运行、操作日志，且日志的存储时间不得低于 6 个月；
b) 应对监测过程产生的数据采取加密、完整性校验、访问控制、备份等保护措施，防止数据被非授权访问、泄露、丢失、篡改。对关键信息基础设施的相关数据接口进行安全风险监测，所产生的数据应按照 GB/T 39204 中 7.10 的要求予以保护；
c) 监测中需对网络流量进行特殊处理如流量解密，监测需求方应对监测方式是否符合数据安全和隐私保护相关的法律法规进行评估，并制定要求和策略；
d) 监测活动结束后，应对监测过程产生的数据采取加密、销毁等安全保护措施。

6 监测内容

本文件所指监测内容主要为数据接口脆弱性、数据违规透出、数据接口异常调用、数据接口异常提供等安全风险源。通过自动化或半自动化的手段发现上述风险源，并进一步分析可能引发的数据安全风险。关于常见的数据接口安全风险源类型参见附录B。

7 监测方式

7.1 流量镜像监测方式

流量镜像监测是将网络中的特定流量复制并传输到指定目的地以便于进行监测。具体监测方式可包括但不限于：

a) 网络设备流量镜像，通过在网络或安全设备（如交换机、路由器或防火墙）上设置镜像规则，让选定的流量被复制并重定向到监测设备或系统进行信息监测；

b) 客户端流量镜像，采用模拟请求的方式产生数据接口交互流量，并在数据接口调用客户端部署流量采集程序将相关流量发送至监测设备或系统；
c) 服务端流量镜像，在数据接口服务端部署流量监测程序，将数据接口产生的流量发送至监测设备或系统。

7.2 日志监测方式

通过采集数据接口产生的日志信息进行分析，实现对数据接口安全风险的监测。具体监测方式可包括但不限于：

a) 日志埋点：按照监测信息字段需求，在数据接口的开发过程中设置特定程序或代码，在数据接口使用过程中可将相应日志发送到监测设备或系统；
b) 日志同步：通过跟保存有数据接口产生日志的相关设备、系统对接，将日志同步至监测设备或系统。

7.3 主动探测方式

通过主动扫描的方式发现数据接口清单，获取数据接口的请求和返回信息，该方式还需在不影响接口安全使用的前提下尽可能触发数据接口各种事件，以便获取更多有效的监测信息。具体监测方式可包括但不限于：

a) 人工模拟探测：通过人工模拟调用数据接口的方式，生成数据接口相关信息，操作过程需覆盖所有数据接口的请求方式；
b) 机器爬虫探测：基于机器爬虫，通过模拟真实的数据接口调用行为，自动访问数据接口的功能，从而获得数据接口的信息；
c) 访问接口文档：通过读取、访问描述数据接口相关功能、配置、状态等的文档获取监测信息，接口文档包括但不限于协议规范、开发者文档、配置文档、状态记录等。

8 监测流程

8.1 数据采集

数据采集主要指通过不同的监测方式，采集数据接口要素相关的基础信息。

a) 服务端相关信息，包括但不限于：
   1）IP 地址和端口号，如响应的目标 IP 地址和端口号；
   2）响应服务器信息，如服务器软件的名称和版本；
   3）TLS 证书信息，如证书域名、主机名、有效期；
   4）其他自定义响应头部或数据。
b) 客户端相关信息，包括但不限于：
   1）基于身份验证的凭证信息，如客户端用户名、令牌、口令；
   2）IP 地址和端口号，如请求的源 IP 地址和端口号；
   3）客户端代理信息，如应用程序或浏览器的类型和版本、操作系统信息、设备类型；
   4）位置信息，移动设备地理位置信息；
   5）其他自定义头部或数据字段。
c) 接口相关信息，包括但不限于：
   1）接口通信协议类型，如 HTTP、HTTPS、FTP、SFTP；
   2）接口标识符，用于访问或识别数据接口的资源标识符；

3）接口请求参数，如客户端接受类型、会话标识、请求数据类型、响应内容长度；
4）接口响应参数，如响应状态码、响应内容类型、响应内容长度、错误信息。

d) 交换数据信息，包括但不限于：
1）重要数据，一旦泄露可能直接影响国家安全、经济安全、社会稳定、公共健康和安全的数据；
2）核心数据，关系国家安全、国民经济命脉、重要民生、重大公共利益等数据；
3）个人信息，如个人基本资料、个人身份信息、个人生物识别信息。

e) 调用行为信息，包括但不限于：
1）操作行为类型，如创建、删除、更新、读取；
2）操作时间信息，如接口请求发起时间、服务响应时间、操作执行时间。

f) 其他数据，指未包含在上述的数据，包括但不限于：
1）网络通信统计信息，如会话数、总包数、丢错包率、总字节数、通信延迟、通信负载；
2）网络通信信息，如源 IP、源端口、目的 IP、目的端口。

8.2 数据处理

8.2.1 数据清洗

通过数据清洗解决收集的日志数据存在的空值、缺失值，数据大量冗余，错误数据，无效数据等问题，以便开展策略分析，包括但不限于：

a) 空值、缺失值清洗：通过手工填入、已有数据推导替代进行补齐；
b) 消除冗余数据：利用唯一性的字段或者特定的规则进行过滤消除；
c) 错误值检测处理：使用统计分析、规则库、约束条件等方式对错误值进行纠正。

8.2.2 关键信息提取和加工

对经过清洗规范化的基础信息进行多层次、多维度的演绎分析，逐层转化为关键信息，关键信息包括但不限于：

a) 服务端关键信息，包括但不限于：
1）域名信息，如域名所属业务、域名所属组织；
2）IP 信息，如 IP 所属网段、IP 所属部门、IP 所属业务。

b) 客户端关键信息，包括但不限于：
1）账号信息，如账号名称、所属部门、账号分布；
2）IP 信息，如 IP 所属地域、IP 所属网段。

c) 接口数据关键信息，包括但不限于：
1）认证和鉴权参数，如密钥、令牌、用户名和口令；
2）安全响应参数，如 CSP、XSS-Protection。

d) 交换数据关键信息，包括但不限于：
1）数据量，如数据条数、敏感数据条数等；
2）数据范围，如重要数据范围、核心数据范围、个人信息范围；
3）数据形态，如明文形态、脱敏形态、加密形态。

e) 调用行为关键信息，包括但不限于：
1）调用行为统计关键字段，如调用次数、调用频率、调用数据量、调用数据类型、调用成功或失败次数；

2）登陆行为统计关键字段，如尝试登录次数、尝试登录频率、登录失败次数和频率、失败的用户名/口令组合；

3）响应行为关键字段，如响应码分布、响应失败次数和频率、平均响应时间、平均延迟时间。

8.3 风险识别

8.3.1 概述

根据8.3.2、8.3.3、8.3.4给出的识别策略进行风险识别，并形成安全风险源清单，无法通过自动化手段识别的，应通过人工方式进行辅助判断或再次确认，关于数据接口常见风险源识别策略参见附录C。通过安全风险源清单，进一步分析可能引发的数据安全风险，常见的数据安全风险类型可参照附录D。

8.3.2 数据接口脆弱性

分析数据接口的输入输出参数、协议规范以及身份验证等基础信息和关键信息，利用统计比对、黑白名单等技术手段，发现脆弱性，常见的分析手段包括但不限于：

a) 建立接口参数异常特征库，对比接口参数数据进行检测和分析，以快速发现可能存在的安全隐患；

b) 建立接口透出数据集合清单，用于检测和分析传输内容数据，发现可能存在的过度或违规的数据传输；

c) 建立用于模拟接口调用的测试案例集，分析接口处理构造参数的响应结果，通过识别模拟行为产生的异常结果，发现接口存在的脆弱性。

8.3.3 数据违规透出

分析交换数据类型、数量等基础信息和关键信息，并结合实际的数据交换需求，发现数据违规透出，常见的分析手段包括但不限于：

a) 建立数据透出负面清单，发现所属清单内数据的违规透出；

b) 建立数据数量、类型透出阈值，监测数据过度透出。

8.3.4 数据接口异常调用、提供

利用人工智能、机器学习、模式学习和统计学等方法，围绕基础信息、关键信息进行自动化分析后归纳推理，形成正常行为特征，计算发现偏离正常行为特征的事件，识别异常调用、异常提供，常见的异常行为事件分析手段包括但不限于：

a) 建立接口调用特征库或调用行为基线，可通过对调用身份、接口行为等进行监测分析，发现异常的接口调用行为；

b) 建立客户端、服务端身份特征库，可通过对实际调用身份、提供身份等进行比对分析，发现异常的身份；

c) 建立接口列表清单集合，可通过对比授权开放接口清单，核查过度开放、超期开放接口。

8.4 监测预警

将风险识别结果进行展示，根据风险的影响对象、发生的可能性、影响程度等因素判断告警级别触发告警信息。告警具体内容包括但不限于：

a) 按照告警的触发原因进行分类，包括但不限于数据接口的认证缺陷、鉴权缺陷、违规透出、超期开放、违规开放;

b) 对告警形成可视报表进行展示，包括但不限于数据接口的状态、告警信息以及风险事件间的关联关系等;
c) 参照GB/T 20986-2023中5.2要求，确定相应风险的告警级别;
d) 告警方式包括但不限于短信、邮件、即时通信、站内信、系统间互联接口推送等。

8.5 通报处置

根据不同告警级别给出告警处置的建议，并启动相应的风险处置流程，数据接口安全风险处置措施参考示例见附录E。在监测过程中发现网络安全和数据安全事件的，应及时向监测需求方报告安全事件情况，并根据《国家网络安全事件应急预案》及相关规定处置。

附录 A
（资料性）
数据接口常见场景、结构、技术形态说明

A.1 跨网络区域的数据接口

指的是在不同网络之间进行数据交换和通信的接口，包括互联网、企业内部网络中或其它网络环境。跨网络区域的数据接口如图A.1所示。

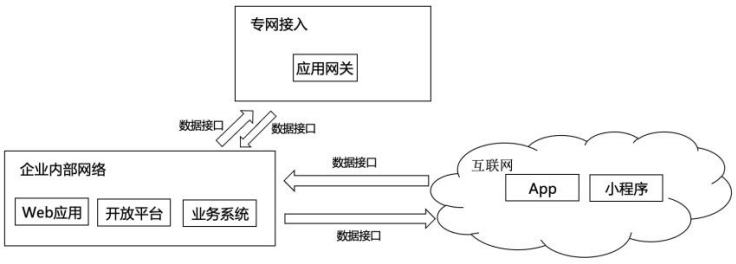

图 A.1 跨网络区域的数据接口示例

A.2 跨信息系统的数据接口

指的是在不同系统之间进行数据交换和通信的接口。跨信息系统的数据接口如图A.2所示。

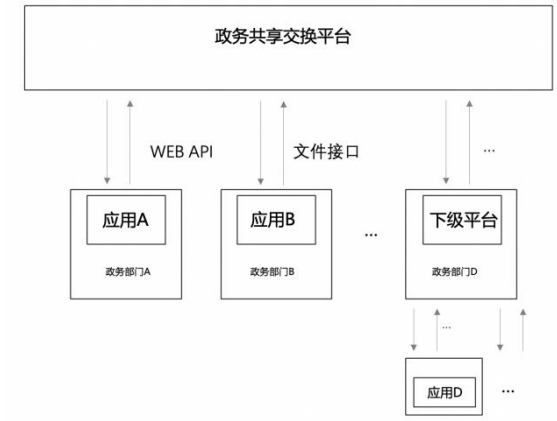

图 A.2 跨信息系统的数据接口示例

A.3 数据接口的结构

数据接口的结构一般由接口地址、请求方式、支持格式、请求参数、返回参数等内容构成。数据接口的常见结构参考如下：

a) 接口地址：http://xxx/xxx/.../xxx/xx.do；
b) 请求方式：GET/POST；
c) 支持格式：JSON；
d) 请求参数，表 A.3.1 提供了一种请求参数的示例；

表 A.3.1 请求参数的示例

名称	类型	说明
app_id	Int	商户号，支付服务商分配给用户的唯一标识。
out_trade_no	string	订单号，商户网站生成的唯一订单标识
total_amoun	float	支付金额，订单总金额

cust_name	string	用户姓名
cust_pho	string	用户手机号

e) 返回参数，表 A.3.2 提供了一种返回参数的示例。

表 A.3.2 返回参数的示例

名称	类型	说明
trade_status	string	支付状态，交易状态
rade_no	string	支付流水号，支付服务商交易号，唯一标识一笔交易
out_trade_no	string	订单号，商户网站生成的唯一订单标识
total_amount	float	支付金额，实际支付的金额

A.4 数据接口的技术形态

数据接口的常见技术形态包括Web API、文件下载接口等，常见的参考示例如下：

a) Web API 的数据接口包括：RESTful API、SOAP API、GraphQL API；

b) 文件下载接口包括：HTTP 文件下载接口、FTP 接口、SFTP 接口。

附录 B
（资料性）
常见风险源类型示例

B.1 数据接口脆弱性

B.1.1 接口鉴别缺陷

数据接口的鉴别机制缺陷，常见的风险源如：

a) 数据接口鉴别存在弱口令：未对访问数据接口的账号口令强度做校验，存在弱口令；
b) 数据接口缺乏身份校验机制：数据接口未通过动/静态口令、短信码、公私钥、数字证书、令牌等方式对用户身份进行鉴别；
c) 数据接口鉴别方式简单重复：各数据接口使用统一的账号、口令等简单的鉴别方式或者接口鉴权令牌管理不当；
d) 数据接口可被越权访问和操作：可通过修改或遍历数据接口的请求参数实现数据越权访问操作。

B.1.2 接口注入缺陷

利用数据接口输入参数校验缺失或薄弱，常见的风险源如：

a) 数据接口可被 SQL 注入：通过在数据接口的请求参数中修改指定的 SQL 命令或语句,执行数据访问、修改、导出或删除等操作；
b) 数据接口可被代码命令注入：通过在数据接口的请求参数中修改指定的操作命令，执行数据访问、修改、导出或删除等操作。

B.1.3 数据接口传输缺陷

利用数据接口传输数据的安全机制缺陷，常见的风险源如：

a) 数据接口未采用加密传输通道：数据接口未采用加密传输协议进行数据传输；
b) 数据接口传输敏感信息未加密：在传输过程中对敏感信息未进行加密；
c) 数据接口采用不安全的协议或算法:数据接口使用不安全的传输协议或弱加密算法可能导致数据的保密性和完整性受到威胁。

B.2 数据违规透出

利用数据接口返回的信息超出业务所需，如过度透出口令、凭证、错误日志、敏感数据等，常见的风险源如：

a) 敏感配置信息暴露风险：数据接口返回内容包含 API 密钥、用户口令、系统配置、系统文件、系统路径、系统错误等信息；
b) 数据接口返回脱敏数据时包含未脱敏或脱敏不规范的数据:未采用恰当的数据脱敏方式对敏感数据进行脱敏处理，导致可完整或者部分还原脱敏前的敏感信息；
c) 数据接口返回数据时未遵循最小化原则：超出数据接口服务协议的数据被返回或展示，导致调用方超范围获取大量数据。

B.3 数据接口异常调用

调用方对数据接口非法使用、异常使用、滥用行为，常见的风险源如：

a) 调用方滥用接口：调用方未按照合同约定的范围调用数据接口，或私自缓存、转发数据；
b) 调用方机器爬虫：通过自动化程序对数据接口进行频繁访问、操作，非法获取数据或导致数据接口无法正常使用。

B.4 数据接口异常提供

提供方违反法律、行政法规等有关规定开放了数据接口行为，常见的风险源如：

a) 超期开放：数据接口在超出服务周期后未及时关闭，调用方仍可继续调用数据；

b） 违规开放的特权后门：开发人员私自保留了数据接口的特权调用方式，从而可能越权对数据进行访问和操作；

c） 未经审核的开放：管理人员未经审核或配置不当导致内部的数据接口被公开。

附录 C
（资料性）
常见风险源识别策略示例

C.1 数据接口脆弱性识别策略

C.1.1 接口鉴别缺陷识别策略

针对数据接口缺乏身份校验机制的识别策略：分析数据接口的身份鉴别机制，若未识别到动/静态口令登录、访问凭证等身份鉴别机制，则生成鉴别机制缺失的数据接口的安全风险告警；

针对数据接口鉴别存在弱口令的识别策略：如数据接口采用口令登录认证，可对口令强度进行监测，若存在连续数字、字母、简单的英文单词、用户名等容易被猜测或暴力攻击等组合，则生成关于数据接口存在弱口令的安全风险告警；

针对数据接口可被未经授权访问的识别策略：结合数据接口的鉴别脆弱性，从登录频次、登录失败次数、登录账号数量、登录的IP等维度，对数据接口的身份鉴别方式进行持续的监测和分析，若登录频次、登录失败次数、登录账号数量、登录的IP等信息与预设的、常规的状态不一致，则生成数据接口鉴别风险相关的威胁行为的安全风险告警；

针对数据接口可被越权访问和操作的识别策略：识别数据接口请求参数可遍历、存在高级权限功能的数据接口，若数据接口存在绕过安全控制机制，可以进行不受限制的操作，则生成数据接口存在水平越权（同级用户之间的越权访问，使用同级用户的资源）或者垂直越权（通过低级权限跨越到高级权限，使用高级权限的资源）的安全风险告警。

C.1.2 数据接口注入缺陷识别策略

针对数据接口可被SQL注入的识别策略：分析数据接口的请求返回内容，若请求中包含特定的SQL代码、特殊的SQL字符或返回内容中包含SQL语法错误的错误消息等特征，则生成关于数据接口存在SQL注入的安全风险告警；

针对数据接口可被代码注入的识别策略：分析数据接口的请求返回内容，若请求中包含特殊的命令字符、异常的系统命令或外部命令，返回包异常响应时长等特征，则生成关于数据接口存在代码注入的安全风险告警。

C.1.3 数据接口传输缺陷识别策略

针对数据接口采用不安全的协议或算法的识别策略：通过分析数据接口的请求内容和返回内容，若数据接口的安全协议或算法与预期的足够强度和安全性保护效果不一致，则生成数据接口未采用敏感数据加密传输、未采用安全的加密协议或算法的安全风险告警；

针对数据接口重放攻击的识别策略：对数据接口的请求进行匹配分析，若监测数据接口的访问日志或者对数据接口进行抓包分析，检查存在重复的、大量相同的请求或者请求包，则生成发现数据接口的重放攻击行为的安全风险告警。

C.2 数据违规透出识别策略

针对数据接口返回内容存在敏感数据的识别策略：分析数据接口返回的敏感数据类型、范围等内容，若返回内容与业务所需的内容不一致，则生成敏感数据被暴露的安全风险告警；

针对数据接口返回脱敏数据时包含未脱敏数据的识别策略：分析数据接口返回的数据明文和密文的状态等内容，若数据接口返回脱敏数据与预设的脱敏效果不匹配，则生成脱敏内容可还原敏感信息的安全风险告警；

针对数据接口返回数据时未遵循最小化原则的识别策略：分析数据接口返回的数据类型、数量等内容，若返回数据的类型和数量与约定的、预设的不一致，则生成过度数据透出的安全风险告警。

C.3 数据接口异常调用识别策略

针对调用方滥用数据接口的识别策略：以调用方为维度，对数据接口的调用频次、时间、数量等行为进行监测分析，若数据接口的使用情况与正常的业务调用行为不匹配，则生成异常数据接口调用行为的安全风险告警；

针对机器爬虫遍历数据接口的识别策略：对数据接口的调用行为进行监测分析，若请求频率、相应速度、请求时间、大量请求来自同一IP地址或者同一时间段内有大量频繁的接口访问行为等与正常用户的访问行为、使用习惯进行对比不一致，则生成数据接口被机器爬虫遍历的安全风险告警。

C.4 数据接口异常提供识别策略

针对异常开放特权接口或违规留存后门接口的识别策略：对数据接口的请求方式、鉴权参数、返回内容等进行分析，若存在某些接口具有特殊权限和功能未经授权或未经审计就对外开放，则生成存在特权接口或者后门接口的安全风险告警；

针对数据接口超期开放或违规公开数据接口的识别策略：如果监测手段梳理的数据接口清单和组织审核备案的数据接口清单进行对比发现不一致，则生成未经审核错误公开的数据接口的安全风险告警。

附录 D
（资料性）
常见风险类型示例

本附录给出了常见的数据接口相关的数据安全风险类别，如表D.1所示。

表 D.1 典型数据接口引发的数据安全风险类别示例

序号	风险类别	描述
1	数据泄漏风险	由于数据接口被爬取、攻击等威胁行为，且数据接口存在弱口令、身份校验等鉴别机制缺陷，导致数据接口的数据泄漏、恶意窃取等影响数据保密性的风险。
2	数据篡改风险	由于数据接口被sql注入、代码命令注入等缺陷或者缺乏安全控制措施、人员有意或无意操作等，可能导致数据接口被篡改影响数据完整的风险。
3	数据滥用风险	由于数据接口缺乏授权访问控制、权限管控等有效的安全管控措施、人员有意或无意操作等，导致数据接口被未授权或超出授权范围使用的风险。
4	数据传输窃取	由于攻击者利用数据接口未采用加密传输通道等安全机制缺陷或者缺乏安全控制措施、人员有意或无意操作等，影响数据的保密性和完整性的风险。
5	数据伪造风险	由于攻击者通过伪造数据接口的请求或参数来欺骗数据接口等威胁行为或者缺乏安全控制措施、人员有意或无意操作等，影响数据的保密性的风险。
6	数据破坏风险	由于数据接口被潜入恶意代码、设备故障、自然灾害等安全威胁或者缺乏安全控制措施、人员有意或无意操作等，导致数据接口被破坏、毁损等影响数据的保密性、可用性的风险。
7	数据丢失风险	由于数据接口的传输链路过载、软硬件故障等问题或者缺乏安全控制措施、人员有意或无意操作等，导致数据接口性能下降、数据丢失等安全风险。

附录 E
（资料性）
风险处置措施参考示例

本附录给出了常见的触发风险的风险源的处置措施，如表E.1所示。

表 E.1 典型风险源处置措施示例

触发风险的风险源类型	风险场景	风险规避、控制等处置措施建议
数据接口认证和鉴权相关缺陷	弱口令	采用动/静态口令、短信验证码、公私钥等多因素鉴别策略避免暴力破解。
	数据接口未鉴权	采用动/静态口令、短信验证码、公私钥等多因素鉴别策略。
	数据接口鉴别方式简单重复	采用动/静态口令、短信验证码、公私钥等多因素鉴别策略。
	越权访问	中断或停止相关的越权访问，禁用或修复受到越权影响的数据接口，以阻止未经授权的访问。
数据接口注入缺陷	数据接口可被SQL注入	使用验证输入、使用参数化查询、最小权限原则、Web应用程序防火墙等安全措施。
	数据接口可被代码命令注入	禁用或修复该数据接口，对用户输入获取的数据进行严格的输入验证和过滤。
数据接口传输缺陷	未加密传输导致数据泄漏	使用TLS/SSL技术进行加密、签名，或者脱敏、匿名化处理等，或者通过建立数据访问的持续监测策略，评估敏感数据的暴露面，计算数据使用画像来统计数据流向和发现异常数据访问风险。
	传输敏感信息未加密	在数据传输前进行适当的脱敏处理，以减轻敏感信息泄漏的风险。脱敏后的数据更难以被滥用。
	采用不安全的协议或算法	使用安全协议，如TLS/SSL，确保数据在传输过程中进行加密，防止中间人攻击和数据截获。
数据接口异常暴露	数据类型过度暴露	实施数据最小化原则，只共享业务所需的最基本信息。
	数据接口返回脱敏数据时包含未脱敏的数据	定期检查脱敏策略的有效性，特别是针对新增或修改的数据字段，以确保其仍然符合脱敏规则。
	数据接口返回大量敏感信息	根据业务实际情况，针对待脱敏数据采取合适的脱敏规则或减少敏感信息的返回量。
数据接口异常调用	滥用接口	实施全面的审计和监控机制，定期审查数据接口的使用情况，及时发现异常行为并采取措施。
	机器爬虫抓取数据	在不同的业务热度下，主体的历史基线可能存在偏差，可以通过主体的分类进行横向的对比，发现异常的数据访问风险。
数据接口异常提供	超期开放数据接口	为每个数据接口设定有效期限，确保接口在规定的时间后自动关闭或需要重新授权。
	违规公开数据接口	下线未经审核开放的接口或加强相关的访问控制措施，降低数据泄漏滥用风险。

	未经允许泄漏数据	确定泄漏的源头，有必要时关闭漏洞、禁用受影响的系统或服务。

参 考 文 献

[1] GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求
[2] GB/T 35273—2020 信息安全技术 个人信息安全规范
[3] GB/T 35274—2023 信息安全技术 大数据服务安全能力要求
[4] GB/T 37988—2019 信息安全技术 数据安全能力成熟度模型
[5] GB/T 39477—2020 信息安全技术 政务信息共享 数据安全技术要求
[6] GB/T xxxxx—xxxx 信息安全技术 数据安全风险评估方法（征求意见稿）
[7] GB/T xxxxx—xxxx 信息安全技术 数据分类分级规则要求
[8] 国家网络安全事件应急预案