ICS 35.030
CCS L70

T/NJCESS

团　　体　　标　　准

T/NJCESS 002-2024

内生安全系统安全日志技术要求

Technical requirements for security logs in endogenous security systems

2024-12-26 发布　　2025-06-30 实施

南京市网络空间内生安全协会 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》的规定起草。

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专利的责任。

本文件由南京市网络空间内生安全协会提出并归口。

本文件起草单位：紫金山实验室、战略支援部队信息工程大学、南京市网络空间内生安全协会

本文件主要起草人：蒋笑笑、胡先君、卜佑军、陈韵、乔伟、张桥、蔡翰智、康艺霖、朱绪全、王涵

1 范围

本文件规定了基于动态异构冗余构建的内生安全系统安全日志的统一技术要求和规范，包括安全日志的通用记录要素、日志采集要求、日志存储要求，以及日志共享要求。

本文件适用于内生安全系统的产品以及其派生品等日志信息提供方与需求方之间进行事件信息的生成、共享和使用。内生安全系统的运维平台与安全威胁信息共享平台的建设与运营可参考使用。

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。

IETF RFC 2119 RFC 文档用于指出要求级别的关键词 (Key words for use in RFCs to Indicate Requirement Levels)

IETF RFC 5424 系统日志协议 (The Syslog Protocol)

IETF RFC 5234 增强型的用语规范 (Augmented BNF for Syntax Specifications: ABNF)

IETF RFC 4627 JSON 要求（The application/json Media Type for JavaScript Object Notation）

GB/T 7408 日期和时间 信息交换表示法

GM/T 0054 信息系统密码应用基本要求

YD/T 4223-2023 支持拟态防御功能设备的总体技术指南

3 术语和定义

IETF RFC 2119、IETF RFC 5424、IETF RFC 5234、IETF RFC 4627、GB/T 7408、GM/T 0054、YD/T 4223-2023 界定的以及下列术语和定义适用于本文件。

3.1

编码 encoding

每个编码声明都定义了如何使用特定语法将事件记录为构建成便于消费者解析的事件记录的过程。

3.2

解码 decoding

事件的消费者通过特定语法简单地解码的事件记录以获得原始事件信息的过程。

3.3

字段字典 fieldtypes dictionary

是应用于领域内的事件记录的字段和数据类型等信息的列表。

3.4

通用字段字典 common fieldtypes dictionary

定义了跨拟态设备和应用程序类型的字段字典。

3.5

最佳实践字段字典 specific fieldtypes dictionary

定义了单个业务形态内拟态设备和应用程序中使用的字段字典。

3.6

事件分类标签 event taxonomy label

由一组类别以及最能描述事件的每个类别的标签值组成。

3.7

事件分类标签词汇表 event taxonomy label table

是内生安全领域内事件分类标签的受控词汇表。

3.8

通用事件分类标签表 common event taxonomy label table

定义了跨拟态设备和应用程序类型的事件标签的受控词汇表。

3.9

最佳实践事件分类标签表 specific event taxonomy label table

定义了单个业务形态内拟态设备和应用程序中使用的事件标签的受控词汇表。

3.10

结构化数据 structured data

一种数据表示形式，按此种形式，由数据元素汇集而成的每一个记录的结构都是一致的并且可以使用关系模型予以有效描述。

3.11

3.12

多维动态重构 multi-dimension dynamic reconfigure

按照事先制定的重构重组方案从异构资源池中抽取构件元素生成功能等价的新执行体或编码架构的过程。

3.13

状态同步 state synchronization

清洗恢复后的执行体需要与在线执行体进行状态或场景再同步以维持与拟态裁决机制

的同步的过程。

4 缩略语

下列缩略语适用于本文件。

JSON：JavaScript 对象表示法（JavaScript Object Notation）

UTF-8：比特可变长度 Unicode 编码转换格式（8-bit Unicode Transformation Format8）

MTU：最大传输单元（Maximum Transmission Unit）

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

CPU：中央处理器（Central Processing Unit）

DHR：动态异构冗余（Dynamic heterogeneous redundancy）

5 概述

内生安全系统架构见图 1。输入/输出代理作为系统的左右边界功能，一方面需要将外部的输入激励按照调度策略导入相应的执行体或运行场景，另一方面将多个功能等价可重构执行体或运行场景输出矢量导入裁决器；功能等价执行体是功能等价结构不同的执行体，执行体可以是网络、平台、系统、部件或模块、构件等不同层面、不同粒度的设备或设施，也可以是软件实现对象、硬件实现对象、软硬结合实现对象、虚拟化实现对象；裁决器依据相对正确公理做出多数或少数、一样或不一样的判别；反馈控制器基于裁决器的反馈信息感知异常，生成多维动态重构的策略，并对功能等价执行体或运行场景进行重构。

本文件为内生安全系统提供一种统一的结构化安全日志事件记录方法，确保领域内内生安全系统产生的安全日志事件记录的一致性，从而提高事件信息共享的效率、互操作性。此外，本文件对内生安全系统安全日志采集、存储、共享作出要求。

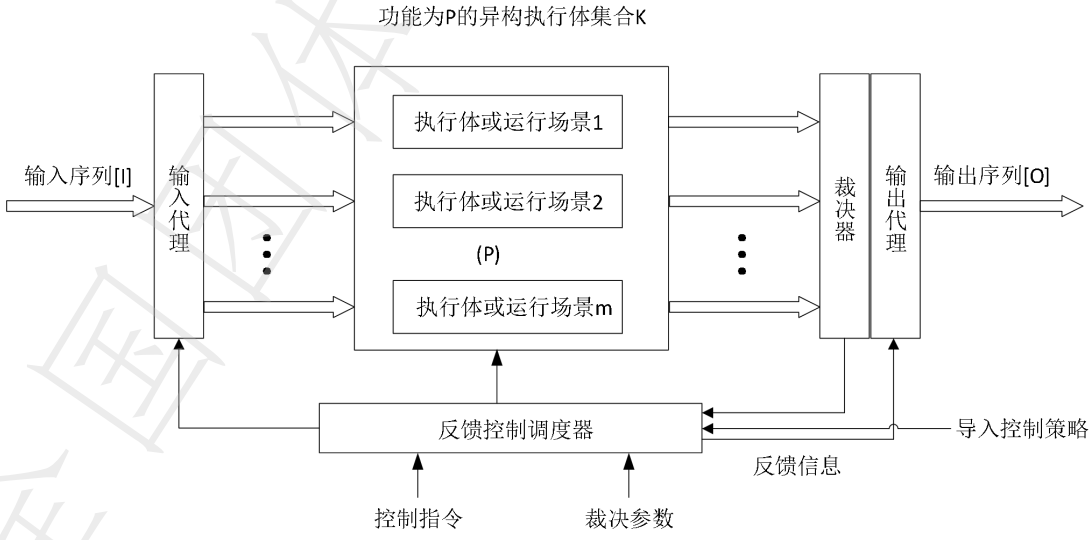

图 1 内生安全系统架构

6 内生安全系统安全日志记录要求

6.1 内生安全系统安全日志记录的组件

内生安全系统在运行过程会产生各类安全事件，本文件对内生安全系统安全日志事件在生命周期的每个步骤中定义了关键组件的规范：

a) 事件记录的信息维度应包括事件所属域、事件动作、作用对象、服务类型、事件结果、事件意义等 6 个信息维度，对领域内可观测的事件进行描述；
b) 应定义领域内通用字段字典，提供可用于记录、共享和分析事件的通用词汇和语法来解决领域内不同业务设备的供应商之间的对同一事件的表达术语不一致问题，以便写入日志数据的设备和应用程序可以使用统一的字段描述；
c) 应定义由一组类别以及最能描述事件的每个类别的标签值组成词汇表。利用统一的分类标签词汇表给领域内的事件打上事件分类标签信息，可实现跨不同拟态防御产品与拟态防御组织的事件类型得到一致的表达；
d) 应提供一种以定义明确、易于解析和解释的数据格式来表达事件的机制。

6.1.1 内生安全系统安全日志事件记录的字段字典

为了确保字段在领域内的许多产品中有用并真正标准化事件记录，字段字典中的所有字段及其属性都应符合以下要求：

a) 字段/字段应用域标识符（即对象和名称组件）应由美国信息互换标准代码字母数字和 _（下划线）字符组成；
b) 字段/字段应用域标识符不区分大小写，并且分层结构为零个或多个上下文对象和标识字段名称的组合；
c) 字段/字段应用域标识符总长度小于 255；
d) 通用字段字典中的字段必应足够常见以保证包含，不常见或不通用的字段不应包括在内；
e) 最佳实践字段字典应保证包含本业务形态内特有的字段，即使只有一个事件报告使用了该字段，该字段名称也将被概括，以允许未来的进入者使用该字段；
f) 最佳实践字段字典中不得出现与通用字段字典同名字段，如果某一业务形态内需要用同名不同义、同名同义不同类型的字段时，应在最佳实践字段中新增不同名字段；
g) 最佳实践字段字典中出现与通用字段字典同名同义同类型不同取值范围时，最佳实践字段字典中的字段取值范围应明确说明；
h) 字段字典头部应包含对象应用域、字段标识符、字段类型、字段描述、取值范围，除非本文件本身发生变化，否则这些头部字段不得更改；
i) 字段字典中的每个字段都应指定一个数据类型，该数据类型指定字段值的表示方式。如果没有类型限制，则应使用字符串类型。字段类型应是对本文件中有效数据类型的引用，不得使用此列表之外的数据类型。有效的数据类型是：字符串、比特、布尔、整数型、空值、时间戳、ipv4、ipv6、对象、文件、数组。

6.1.2 内生安全系统安全日志事件分类标签

事件分类标签表与字段字典中的字段在标识符方面要求保持一致，但有以下特有的约束规范：

a) 通用事件分类标签表应由中国网络空间内生安全技术与产业联盟维护，是领域内共性事件类型描述术语的词汇表；
b) 最佳实践事件分类标签表应由领域内不同组织创建，并提交给中国网络空间内生安

全技术与产业联盟审核、归档、发布；

c) 事件分类标签标识符应为有意义的标识符；
d) 某一个事件分类标签如果是数据类型字符串，其属性值的枚举应受到限制。
e) 各类别标签的属性值应指定至少一个可能的值；当一个维度存在多个类别标签值时通过分隔符‘,’进行分割；
f) 通用事件分类标签表中的类别标签应是领域内共性事件类别标签，不通用的类别不应包括在内。

6.1.3 内生安全系统安全日志事件记录数据组织格式

内生安全领域内事件记录的数据组织格式遵循扩展的巴科斯诺尔范式。

事件记录数据组织格式应为 mimic event express = HEADER SP ENTITY CRLF。HEADER 表示头域数据，ENTITY 表示实体数据。

HEADER 应使用字段字典中的字段，组成格式应为 HEADER = VERSION SP TIMESTAMP SP PRIVAL SP LOCATION SP LOGTYPE [SP MSGID SP MSGOFFSET]。应遵循一下规则：

a) 对于更改任何部分的任何新协议规范，VERSION 应递增；
b) TIMESTAMP 的格式应遵循 GB/T 7408 中定义的日期时间格式；
c) PRIVAL 取值“Emergency，Alert，Critical，Error，Warning，Notice，Info，Debug”，不区分大小写。具体内容参考事件记录的级别说明（事件记录的级别见附录 A）；
d) LOCATION 的数据格式应为 LOCATIONTYPE: LOCATIONVALUE; 例如：”process_id:100;thread_id:100“。具体内容参考 location 编码表（location 编码表见附录 A）；
e) LOGTYPE 应从下列类型中选择：desc、stat、visit、biz、dmf、sched、ids。具体含义参考日志类型说明（日志类型说明见附录 A）；
f) MSGID 应为可选字段，为递增序列；
g) MSGOFFSET 应在 MSGID 有值且消息分段情况下才有值，当前记录是最后一分段时此值为-1；

ENTITY 的组织格式应为 ENTITY =EVENT-STRUCTURED-EXP ，STRUCTURED-DATA，ADDITION-MSG。应遵循以下规则：

a) EVENT-STRUCTURED-EXP 应包含 6 个涵盖事件记录的结构化数据元素：事件所属域、事件动作、事件作用对象、服务类型、事件结果、事件意义；
b) EVENT-STRUCTURED-EXP 应通过 key-value 键值对的数据格式对事件记录的六个要素记录。Key 值应为事件记录的六个要素。Value 值应来自字段字典、事件分类标签词汇表中的字段或标签。如果 Value 为空值，则取值应为空值""，举例：event_domain:""。当某一 Value 值有多个取值时，此值应以列表形式组织[]，多个取值直接采用分隔符“,”；
c) STRUCTURED-DATA 应通过 key-value 键值对的数据格式对事件关键信息记录。Key 值应来自本文件的字段字典中的字段。Value 值应满足对应的 Key 值字段属性定义。当某一 Value 值有多个取值时，此值应以列表形式组织[]，多个取值直接采用分隔符“,”；
d) ADDITION-MSG 应提供一种利用非结构化的数据(NO-STRUCTURED-DATA)组织格式补充事件信息的机制,通过 key-value 键值对的数据格式对事件关键信息记录；
e) ADDITION-MSG 中使用的字符集应是 8 位字段中的 7 位 ASCII。

示　例　：　"event_domain":"mimic_multimode_ruling","event_action":"access", "event_object":"configure_table", "event_service":"multimode_ruling", "event_status":"success", "event_subject":"dmf_security_abnormal", "mimicrouter.msg_src":"config_multimode_ruling", "mimicrouter.exception_time": "2022-01-01 09:48:07", "addition_msg":"find error config!"\r\n。

6.2 内生安全系统安全领域内具体可观测事件最小集

内生安全系统安全领域内具体可观测事件最小集规范：

a) 事件自身属性字段字典应遵循事件自身属性字段字典说明（事件自身属性字段字典说明见附录 B）；

b) 输入代理可观测的事件最小集应包括内容激励信号、激励信号分发动作、激励信号适配动作、激励信号的合规控制、黑白名单过滤等主被动防御措施，输入代理事件分类标签通用词汇表最小集应遵循输入代理事件分类标签通用词汇表最小集说明（输入代理事件分类标签通用词汇表最小集说明见附录 B），输入代理字段字典应遵循输入代理字段字典说明（输入代理字段字典说明见附录 B）；

c) 输出代理可观测的事件最小集应包括内容：接收多模输出矢量、提取拟态保护的关注点信息、多模输出矢量预处理、输出预处理后的多模输出矢量。输出代理事件分类标签通用词汇表最小集应遵循输出代理事件分类标签通用词汇表最小集说明（输出代理事件分类标签通用词汇表最小集说明见附录 B）。输出代理字段字典应遵循输出代理字段字典说明（输出代理字段字典说明见附录 B）；

d) 拟态裁决可观测的事件最小集应包括内容：执行裁决策略、裁决多模输出矢量、记录差模扰动、输出裁决状态信息。拟态裁决事件分类标签通用词汇表最小集应遵循拟态裁决事件分类标签通用词汇表最小集说明（拟态裁决事件分类标签通用词汇表最小集说明见附录 B）。拟态裁决字段字典应遵循拟态裁决字段字典说明（拟态裁决字段字典说明见附录 B）；

e) 负反馈控制器可观测的事件最小集应包括内容：接收调度策略、执行调度策略、清洗异常执行体、下线异常执行体、上线新执行体、同步执行体状态、通知输入代理、记录调度日志，负反馈控制器事件分类标签通用词汇表最小集应遵循负反馈控制器事件分类标签通用词汇表最小集说明（负反馈控制器事件分类标签通用词汇表最小集说明见附录 B），负反馈控制器字段字典应遵循负反馈控制器字段字典说明（负反馈控制器字段字典说明见附录 B）。

6.3 内生安全系统安全日志事件记录编码

字段字典映射规范：

a) 安全日志事件记录编码应使用可扩展标记语言和 JSON 等被广泛使用的编码；

b) 数值类型与布尔类型应直接映射到 JSON 数值和布尔类型，整数值应在 64 位整数内表示，范围为 [-(2^63), 2^63-1] 有符号或 [0, 2^64-1]无符号；浮点值应可以用 IEEE 754 64 位浮点格式表示；

c) 字段取值是多值时应映射到 JSON 数组；

d) 字段字典中的 object 类型应直接映射到 JSON 对象值类型；

a) 基本字符、字符串或其他非 JSON 支持的类型均应映射到 JSON 的字符串或对象值类型；

b) 整数、浮点数和布尔 字段类型应使用等效的内置 JSON 类型进行编码。对应于这些原生类型的值不应出现在引号字符中。

JSON 编码事件记录的规范约束：

a) JSON 编码的事件记录应完全符合 RFC 4627 规范；
b) 除了转义字符的要求 JSON 要求外，换行符和回车符在用作字段值时也应转义；
c) 所有 JSON 编码的事件记录应表示为有效的 UTF-8 编码的 Unicode 字符序列；
d) 具有多个值的 JSON 编码事件记录中的字段应使用本机 JSON 数组机制进行编码，具有单个值的字段应包装在 JSON 数组中；
e) JSON 对象结构应用于表示字段层次结构。也可以使用内联字段名称。

示例：

```
{
  "event_header": [
    "V.1.0.0",
    "2021-11-22T17:50:51,520+08:00",
    "INFO",
    "line_id:248",
    "stat",
    "0000",
    "0"
  ],
  "event_entity": {
    "event_domain": "mimic_multimode_ruling",
    "event_action": "multimode_ruling",
    "event_object": "configure_table",
    "event_service": "multimode_ruling",
    "event_status": "success",
    "event_subject": "dmf_security_abnormal",
    "mimicrouter.msg_src": "config_multimode_ruling",
    "addition_msg": "Reconnecting and resending!"
  }
}
```

6.4 内生安全系统安全日志文件形式信息载体的约束规范

文件作为日志的重要载体，约束规范主要包括事件记录在文件中的组织方式、日志文件的组织方式、日志文件目录的组织方式。

事件记录在文件中的组织方式：

a) 日志记录之间的分隔。每条日志记录之间应通过换行符\r\n 的方式进行分隔，界限划分清晰；
b) 日志记录的长度。本文件本身不对日志记录的大小限制；每条日志记录会被映射到指定的文件中，其大小由其所在的文件系统与其记录所有者决定；如果记录本身需要分多行存储应提供明确标识多行为同一事件记录，标识方法应显示提供给记录共享方；

c) 不同日志记录应显示区分。日志记录应支持多线程，不同线程之间的日志信息写同一日志文件时不应产生冲突，日志信息应能被显示区分出来。

日志文件的组织方式：

a) 单个日志文件大小。本文件本身不对日志文件的大小限制，其大小由其所在的文件系统与其记录所有者决定；单个日志文件大小，推荐设置在 100MB~500MB 之间；
b) 日志文件分割规范要求：
   1) 以一定的周期生成日志文件，推荐以一个自然日为一个周期，便于分类归档。
   2) 当单个周期内日志量超过文件大小限制时，应按照单一文件配置大小分割。
   3) 当单个日志出现跨周期时，日志文件不应只以日志量大小进行分割，应创建新的日志文件；
c) 日志文件的命名组织方式规范要求：
   1) 以一定的周期生成日志文件，日志文件名称应追加日期标识“YYYYMMDD”，便于分类归档。例如：mimicrouter_dmf_20220101.log，其中，日期 20220101，应按照“YYYYMMDD”的格式进行统一；
   2) 单个周期内日志文件按照单一文件配置大小分割时，文件命名应按照文件编号顺序生成新文件，日志文件名应追加文件编号“XXXX”，其中 XXXX 代表四位数字编号，并以 0001 作为起始文件编号，例如：mimicrouter_dmf_20220101_0001.log，mimicrouter_dmf_20220101_0002.log；
   3) 当单个日志出现跨周期时，应重新创建一个以最新日志日期命名的文件，不应在前一个日期的日志日期文件中继续追加写入。例如：当前某个日志文件的日期为 20220101，日志文件大小为 1M(不需要按照大小分割)，但随后进入 20220102 的自然时间周期，那么后续记录，应重新创建一个日志日期为 20220102 的文件，不应在日志日期为 20220101 的已有文件中继续追加写入；
   4) 日志文件的命名组织方式，"设备类型_日志类型_日期.log"；
   5) 设备类型，mimic*，举例：mimicrouter；
   6) 日志类型，取自 4.4 事件记录头域数据组组织格式 LOGTYPE 字段；
   7) 日志类型不同语义（层次）的标识符之间以下划线 '_' 字符进行连接；
   8) 相同语义（层次）的标识符之间以 '-' 进行连接。

日志文件目录的组织方式：

a) 日志文件目录的组织方式，应能够直观反映出日志的组织方式，包括分类、索引以及层级等信息；
b) 日志文件目录的命名应取自 6.1.2 章节通用事件分类标签表和最佳实践事件分类标签表描述的标签元素；
c) 日志文件目录的命名禁止使用无法区分意义的纯数字、与拟态业务场景、拟态事件类型无关的命名方式。

7 内生安全系统安全日志采集要求

7.1 明确采集目标

明确采集目标应符合以下要求：

a) 应确定需要采集的拟态设备类型、型号及其网络位置和业务情况；
b) 应了解设备的功能和可能产生的日志类型，例如系统日志、攻击日志、错误日志等；
c) 应针对不同类型的日志，明确其重要性和优先级，以便在采集过程中重点关注。

7.2 选择采集工具

选择采集工具应符合以下要求：
a) 应选择业界类似业务场景的主流技术选型，具备成熟的社区，方便问题解决；
b) 应能够满足拟态设备日志数据与网络流量采集的需求，具备灵活的采集策略配置，有明确的指导文件；
c) 应对被采集设备的性能影响在要求范围内，轻量级，资源占用小；（资源占用与性能需要开发后予以评估给出详细报告）
d) 应具备灵活的对外接口，支持多种输出方式；
e) 采集器其代码应开源，开发语言与现有开发人员技术栈相符，便于二次开发；
f) 采集器应支持数据加密传输，同时保证传输可靠性；
g) 采集器应记录对日志数据的访问和操作日志，方便进行审计追溯；
h) 采集器应具备故障恢复能力、故障报警能力；
i) 应尽量选择拟态设备目前采用的日志采集器。

7.3 配置采集策略

配置采集策略应符合以下要求：
a) 应确定拟态设备中需要裁决日志的系统、应用或服务，如裁决模块、调度模块；
b) 应根据业务需求，采集所需数据，如系统运行的指标、运行状态和被攻击日志；
c) 应根据拟态设备应用或服务的特点，配置具体的日志采集规则，包括日志文件的路径、采集频率、过滤条件、采集的日志级别等。

7.4 日志采集安全

日志采集安全应符合以下要求：
a) 日志采集状态监控，确保采集工具正常运行，与拟态设备的连接保持稳定；
b) 日志采集过程不能影响拟态设备正常业务运行，避免因采集器的配置不当导致设备 CPU 使用率过高、内存泄露、占用大量磁盘等问题；
c) 适当限制日志采集器的访问权限，避免对设备上非授权文件的访问及操作；
d) 对敏感日志数据进行安全保护，采取加密、访问控制等措施，防止日志数据泄露或被篡改。

8 内生安全系统安全日志存储要求

8.1 日志存储保证可用性和可扩展性

日志存储的可用性和可扩展性应符合以下要求：
a) 日志的本地侧存储时，在业务形态允许条件下推荐采用备份存储、冗余存储等保证日志记录存储的可用性与可靠性的技术手段；

b) 日志在统一集中式日志平台存储时，在业务形态允许条件下推荐采用分布式拟态云存储等技术手段，提高系统的可靠性、可用性和存取效率，且易于扩展。

8.2 日志存储的时长

日志存储的时长应符合以下要求：

a) 日志存储时长应不少于六个月。

8.3 日志存储路径

日志存储的路径应符合以下要求：

a) 应支持根路径的可配置，支持路径场景迁移；
b) 应采用含有分类、索引等隐含的信息的命名方式、采用分层的目录组织结构。

8.4 日志存储安全

日志存储安全应符合以下要求：

a) 应分类分级，根据日志的级别限制访问；
b) 应基于日志数据的分类分级制定数据访问控制策略，形成敏感分级数据与用户角色的访问控制矩阵，为数据的安全合规使用提供支撑；
c) 应尽量减少敏感数据存储位置的数量并及时删除无关的数据，防止敏感日志数据泄露；
d) 应对相关人员进行日志数据安全的培训，明确日志数据的管理和使用流程；
e) 应对真实的隐私数据（业务面向的用户、组织本身等）进行改造并提供使用，从而降低隐私数据泄露的风险；
f) 应采用适合本组织（系统、设备）的存储策略控制来保护存储系统和基础设施以及存储在其中的日志数据，防止未经授权的泄露、修改或破坏，同时确保授权用户的可用性。

9 内生安全系统安全日志共享要求

9.1 日志共享标准化

日志共享标准化应符合以下要求：

a) 应提供标准化的 API 接口，方便第三方工具和系统集成，实现日志数据的共享和交换。

9.2 日志共享安全

日志共享安全应符合以下要求：

a) 与外部合作伙伴（如安全厂商、监管机构等）共享日志数据，应遵守相关的隐私和法律要求。
b) 在共享日志数据时，应对敏感信息进行匿名化处理，保护用户隐私；
c) 应采用符合 GM/T 0054 等国家相关标准规定的密码技术，保证通信过程中数据的保密性和完整性。

附录 A

（规范性）
内生安全系统安全日志事件记录数据组织格式说明

A.1. 事件记录的级别说明

事件记录的级别说明见表 A.1。

A.1.事件记录的级别

code	定义	值
0	system is unusable	Emergency
1	action must be taken immediately	Alert
2	critical conditions	Critical
3	error conditions	Error
4	warning conditions	Warning
5	normal but significant condition	Notice
6	informational messages	Info
7	debug-level messages	Debug

A.2. location 编码表说明

location 编码表说明见表 A.1。

A.2. location 编码表

类型编码(code)	类型名（type）	类型定义(definition)	举例
1	process_id	进程标识：标识事件发生在哪个进程。	process_id:100
2	thread_id	线程标识：标识事件发生在哪个线程。	thread_id:100
3	function_name	函数标识：标识事件发生在哪个函数。	function_name:main
4	line_id	行号标识：标识事件发生在哪一行。	line_id:100
5	file_name	文件标识:标识事件发生在哪个代码文件	file_name:main.c

A.3. 日志类型说明

日志类型说明见表 A.3。

A.3.日志类型

Code	定义	值
1	系统启动、运行过程中记录的日志，表明系统的一些启动日志、启动参数等	desc
2	系统性能统计日志，应用会定时收集一些性能信息，便于查询应用当前状态	stat
3	外部请求相关的日志，定位该请求相关的所有日志	visit
4	业务数据相关日志，主要提供给数据统计使用	biz
5	差模扰动日志	dmf
6	执行体调度日志	sched

7	ids 日志	ids

附录 B

（规范性）
内生安全系统安全领域内具体可观测事件最小集说明

B. 1. 事件自身属性字段字典说明

事件自身属性字段字典说明见表 B.1。

表 B.1.事件自身属性字段字典

字段对象域（object_domain）	字段标识符（Field_identifier）	字段类型（Type）	字段描述(Description)	字段取值范围（Range）
event	host_name	string	事件主机的名字	1~255
	ipv4	ipv4	事件所在的主机 IPV4 地址	0.0.0.0/32
	ipv6	ipv6	事件所在的主机 IPV6 地址	::/128
	port	number	事件所在主机的应用端口号	0~65535
	app_name	string	事件所属应用名字	1~255
	pname	string	产生事件的进程的名字	1~255
	msg	string	事件描述信息	1~1024
	msgid	string	事件描述信息的身份标识	
	pid	string	产生事件的进程的身份标识	
	priv	string	事件级别	（参照表 3 事件记录的级别）
	tid	number	与产生事件相关的线程的身份标识	

B. 2. 输入代理事件分类标签通用词汇表最小集说明

输入代理事件分类标签通用词汇表见表 B.2。

B.2.输入代理事件分类标签通用词汇表最小集

事件类别	类别标签值	定义/描述
event_domain	mimic_interface	事件记录发生在拟态界上

	input_agent	事件记录发生在输入代理
event_action	distribute	事件的动作是分发激励信号
	adapte	事件的动作是处理激励信号以适配相应的执行体
	check	事件的动作是激励信号检查
	filter	事件的动作是激励信号过滤
event_object	excitation_signal	事件作用的目标对象，拟态界外输入的激励信号
event_service	input_distribution	事件涉及的操作类型是输入分发
	input_adpator	事件涉及的操做类型是输入适配
	input_compliancecheck	事件涉及的操作类型是输入信号的合规性检查
	input_filter	事件涉及的操作类型是对输入信号进行黑白名单过滤
event_status	fail	事件结果失败
	success	事件结果成功
	pass	事件结果通过
	block	事件结果阻断
event_subject	systemrunning_normal	正常系统运行事件记录
	systemrunning_abnormal	异常系统运行事件记录
	security_normal	主被动防御动作记录正常安全事件
	security_abnormal	主被动防御动作记录异常安全事件

B. 3. 输入代理字段字典说明

输入代理字段字典说明见表 B.3。

B.3.输入代理字段字典

字段对象域（object_domain）	字段标识符（Field_identifier）	字段类型（Type）	字段描述(Description)	字段取值范围（Range）
input_agent	compliance_rules_file	file	合规规则文件	
	compliance_rules_list	object	合规规则列表	
	black_white_file	file	黑白名单规则文件	
	black_white_rules_list	object	黑白名单过滤规则列表	
	relation_feeo	object	关联的执行体信息	

B. 4. 输出代理事件分类标签通用词汇表最小集说明

输出代理事件分类标签通用词汇表最小集说明见表 B.4。

B.4.输出代理事件分类标签通用词汇表最小集

事件类别	类别标签值	定义/描述
event_domain	mimic_interface	事件记录发生在拟态界上
	output_agent	事件记录发生在输出代理
event_action	receive	事件的动作是接收异构执行体输出的结果

	send	事件的动作是发送输出矢量到拟态裁决
	extract	事件的动作是提取拟态保护的信息
	preprocess	事件的动作是对异构执行体输出是输出矢量预处理
event_object	output_vector	事件作用的目标对象，多异构执行体输出矢量
	buffer_queue	事件作用的目标对象，缓冲队列
event_service	output_vector_receive	事件涉及的操作类型是输出矢量的接收
	output_vector_send	事件涉及的操做类型是发送处理后的输出矢量到拟态裁决
	output_vector_preprocess	事件涉及的操作类型是输出矢量的预处理
	output_vector_extraction	事件涉及的操作类型是从原始输出矢量中提取拟态保护的信息
event_status	fail	事件结果失败
	success	事件结果成功
	full	事件结果缓冲队列满
	empty	事件结果缓冲队列空
event_subject	systemrunning_normal	正常系统运行事件记录
	systemrunning_abnormal	异常系统运行事件记录

B. 5. 输出代理字段字典说明

输出代理事件分类标签通用词汇表最小集说明见表 B.5。

B.5.输出代理字段字典

字段对象域（object_domain）	字段标识符（Field_identifier）	字段类型（Type）	字段描述 (Description)	字段取值范围（Range）
output_agent	buffer_queue	object	缓冲队列	
	output_vector	object	输出矢量	

B. 6. 拟态裁决事件分类标签通用词汇表最小集说明

拟态裁决事件分类标签通用词汇表最小集说明见表 B.6。

B.6.拟态裁决事件分类标签通用词汇表最小集

事件类别	类别标签值	定义/描述
event_domain	mimic_multimode_ruling	事件记录发生在拟态裁决
event_action	multimode_ruling	事件的动作是裁决输出
event_object	ruling_policy	事件作用的目标对象，裁决策略
	output_vector	事件作用的目标对象，输出矢量
	recorder	事件作用的目标对象，差模扰动事件记录
	file	事件作用的目标对象，差模扰动日志文件
	ruling_policy_set	事件作用的目标对象，裁决策略集
event_service	policy_execution	事件涉及的操做类型是裁决策略执

事件类别	类别标签值	定义/描述
		行
	dmf_logging	事件涉及的操作类型是差模扰动日志记录
	ruling_status_logging	事件涉及的操作类型是裁决状态信息日志记录
event_status	fail	事件结果失败
	success	事件结果成功
	simple	利用安全漏洞影响目标系统的难度“简单”
	complex	利用安全漏洞影响目标系统的难度“复杂”
	complete	利用安全漏洞对目标系统造成的损害程度“完全”
	part	利用安全漏洞对目标系统造成的损害程度“部分”
	slight	利用安全漏洞对目标系统造成的损害程度“轻微”
	none	利用安全漏洞对目标系统造成的损害程度“无”
	schedule	差模扰动造成执行体调度
	no_schedule	差模扰动未造成执行体调度
	different_mode_fault	造成差模扰动
	no_dmf	未造成差模扰动
event_subject	systemrunning_normal	正常系统运行事件记录
	systemrunning_abnormal	异常系统运行事件记录
	no_dmf_security_normal	无差模扰动正常安全事件记录
	dmf_single_executor_security_abnormal	差模扰动单执行体异常安全事件记录
	dmf_multi_executors_security_abnormal	差模扰动多执行体异常安全事件记录
	dmf_security_abnormal	差模扰动异常安全事件记录

B. 7. 拟态裁决字段字典说明

拟态裁决字段字典说明见表 B.7。

B.7.拟态裁决字段字典

字段对象域（object_domain）	字段标识符（Field_identifier）	字段类型（Type）	字段描述(Description)	字段取值范围（Range）
mimic_multimode_ruling	executor_info	object	执行体信息	[“1.1.1.1“,”2.2.2.2”]

字段对象域（object_domain）	字段标识符（Field_identifier）	字段类型（Type）	字段描述(Description)	字段取值范围（Range）
	executor_count	number	在线执行体数量	“3~MAX_LONG（其中，MAX_LONG 代表能表示最大的 Long 整数）
	executor_running_duration	number	执行体运行时长	0~MAX_LONG
	dmf_executor_count	number	发生差模扰动的执行体数量	0~executor_count
	dmf_log	object	差模扰动日志数据结构，裁决作用对象	
	dmf_count	number	差模扰动次数	0~MAX_LONG
	ruling_policy	object	裁决策略	
	algorithm	string	多模裁决算法	“majority_multimode_ruling“: (择多裁决), “weight_multimode_ruling“: (权重裁决), “random_multimode_ruling“: (随机裁决)
	level	string	多模裁决层次/粒度	“executor_level“: (执行体层次), “component_level“: (组件层次), “payload_level“: (载荷层次), ”byte_level”: (字节层次), ”bit_level”: (比特层次)
	conclusion	string	多模裁决结论	“completely_same“: (完全相同), “majority_same“ : (多数相同), “minority_same“: (少数相同), “completely_different”: (完全不同)
	syslog	object	syslog 日	

字段对象域（object_domain）	字段标识符（Field_identifier）	字段类型（Type）	字段描述(Description)	字段取值范围（Range）
			志数据结构	
	exploiting_difficulty	string	利用安全漏洞影响目标系统的难度	"simple" | "complex"
	damage_potential	string	利用安全漏洞对目标系统造成的损害程度	"complete"|"part"|"slight"|"none"
	output_status	object	输出到负反馈控制器的状态信息	
	output_response	object	裁决后输出给目标用户的响应消息	
	output_schedule_policy	object	输出到负反馈控制器的策略信息	

B. 8. 负反馈控制器事件分类标签通用词汇表最小集说明

负反馈控制器事件分类标签通用词汇表最小集说明见表 B.8。

B.8.负反馈控制器事件分类标签通用词汇表最小集

事件类别	类别标签值	定义/描述
event_domain	feedback_control_function	事件记录发生在负反馈控制器
event_action	schedule	事件的动作是调度异构执行体
	receive	事件的动作是接收调度策略
	logging	事件的动作是日志记录
	clear	事件的动作是清洗异常执行体
	recover	事件的动作是恢复异常执行体状态
	synchronize	事件的动作是同步新执行体状态
	offline	事件的动作是下线异常执行体
	online	事件的动作是上线新执行体
	notify	事件的动作是通知输入代理当前执行体

事件类别	类别标签值	定义/描述
		集发生变化
event_object	schedule_policy	事件作用的目标对象，调度策略
	executor	事件作用的目标对象，执行体
	recorder	事件作用的目标对象，调度事件记录
	file	事件作用的目标对象，调度日志文件
	schedule_policy_set	事件作用的目标对象，裁决策略集
event_service	schedule_executor	事件涉及的操作类型是异常执行体调度
	policy_execution	事件涉及的操做类型是调度策略执行
	schedule_logging	事件涉及的操作类型是调度日志记录
	executor_clear	事件涉及的操作类型是执行体清洗
	executor_recover	事件涉及的操作类型是执行体恢复
	executor_offline	事件涉及的操作类型是执行体下线
	excutor_online	事件涉及的操作类型是执行体上线
	msg_notify	事件涉及的操作类型是消息通知
event_status	fail	事件结果失败
	success	事件结果成功
	disconnect	链接异构执行体池失败
	no_response	通知消息无响应
	no_schedule	未执行异构执行体调度
event_subject	systemrunning_normal	正常系统运行事件记录
	systemrunning_abnormal	异常系统运行事件记录
	executor_schedule_abnormal	执行体调度异常事件记录
	executor_schedule_normal	执行体调度正常事件记录
	executor_recover_abnormal	执行体恢复异常事件记录
	executor_clear_abnormal	执行体清洗异常事件记录
	executor_synchronization_abnormal	执行体状态同步异常事件记录

B. 9. 负反馈控制器字段字典说明

负反馈控制器字段字典说明见表 B.9。

B.9.负反馈控制器字段字典

字段对象域（object_domain）	字段标识符（Field_identifier）	字段类型（Type）	字段描述(Description)	字段取值范围（Range）
feedback_control_function	recorder.schedule	object	差模扰动日志数据结构	
	recorder.syslog	object	syslog 日志数据结构	
	executor	object	执行体信息	
	schedule_policy	object	调度策略	
	schedule_count	number	调度次数	0~MAX_LONG

字段对象域（object_domain）	字段标识符（Field_identifier）	字段类型（Type）	字段描述(Description)	字段取值范围（Range）
	executor_count	number	在线执行体数量	3~max_long
	online_executor_count	number	本次调度上线的执行体数量	0~executor_count
	online_executor_list	array	本次调度上线的执行体 IP 列表	
	offline_executor__count	number	下线的执行体数量	
	offline_executor_list	array	下线的执行体 IP 列表	
	notification_msg	object	通知消息数据结构	
	recover_data	object	恢复的状态信息数据结构	
	clear_data	object	清洗的信息数据结构	
	syn_data	object	同步的状态信息数据结构	
	recover_count	number	执行体状态恢复次数	
	clear_count	number	执行体清洗的次数	
	recover_executor_count	number	恢复的执行体数量	
	clear_executor_count	number	清洗的执行体数量	