TTA Standard

정보통신단체표준(영문표준) 제정일: 2018 년 xx 월 xx 일

클라우드 컴퓨팅의 모니터링 서비스에 대한 데이터 보안 요구사항

Data security requirements for the monitoring service of cloud computing

TTA 한국정보통신기술협회
Telecommunications Technology Association

표준초안 검토 위원회	**사이버보안 프로젝트그룹(PG503)**				
표준안 심의 위원회	**정보보호 기술위원회(TC5)**				
	성명	**소 속**	**직위**	**위원회 및 직위**	**표준번호**
표준(과제) 제안	김종현	한국전자통신연구원	책임연구원	사이버보안 프로젝트 그룹 위원	
표준 초안 작성자	김영수	한국전자통신연구원	책임연구원	사이버보안 프로젝트 그룹 위원	
	김종현	한국전자통신연구원	책임연구원	사이버보안 프로젝트 그룹 위원	
사무국 담당	박수정	TTA	책임연구원	-	

본 표준 발간 이전에 접수된 지식재산권 확약서 정보는 본 표준의 '부록(지식재산권 확약서 정보)'에 명시하고 있으며, 이후 접수된 지식재산권 확약서는 TTA 웹사이트에서 확인할 수 있습니다.
본 표준과 관련하여 접수된 확약서 외의 지식재산권이 존재할 수 있습니다.

발행인 : 한국정보통신기술협회 회장
발행처 : 한국정보통신기술협회
13591, 경기도 성남시 분당구 분당로 47
Tel : 031-724-0114, Fax : 031-724-0109
발행일 : 20xx.xx

서 문

1 표준의 목적

본 표준에서는 클라우드 컴퓨팅 환경에서의 모니터링 서비스와 연관된 데이터 보안 위협과 문제점을 분석하고, 데이터 범위/라이프사이클/획득/저장 등의 모니터링 서비스 데이터 보안 요구사항을 제시하고자 한다.

2 주요 내용 요약

이 표준은 클라우드 컴퓨팅의 모니터링 서비스에 대한 데이터 범위 및 라이프사이클과 모니터링 데이터 획득/저장 관련 보안 요구 사항 등을 포함한다. 모니터링 데이터 범위 요구사항은 클라우드 서비스 제공자(CSP, Cloud Service Provider)들이 클라우드 보안 및 최대 모니터링 범위 유지를 위해 제공해야 하는 필수 모니터링 범위를 포함한다. 모니터링 데이터 라이프사이클은 데이터의 생성/저장/사용/마이그레이션/표현/삭제/백업 등을 포함한다. 모니터링 데이터 획득은 모니터링 서비스로부터 데이터를 획득하는 기술 관련 보안 요구사항을 기술한다. 모니터링 데이터 저장은 CSP 차원의 모니터링 데이터 저장 시 보안 요구사항을 기술한다.

3 인용 표준과의 비교

3.1 인용 표준과의 관련성

본 표준은 인용표준(ITU-T X.1603, Data security requirements for the monitoring service of cloud computing)을 영문 그대로 수용한다.

3.2 인용 표준과 본 표준의 비교표

본 표준은 ITU-T X.1603 표준 전문을 인용하므로 비교표는 생략한다

Preface

1 Purpose

This standard analyses data security threats and challenges associated with the monitoring service in a cloud computing environment, and describes data security requirements of the monitoring service including data scope, data lifecycle, data acquisition and data storage.

2 Summary

This standard includes monitoring data scope requirements, monitoring data lifecycle, security requirements of monitoring data acquisition and security requirements of monitoring data storage. Monitoring data scope requirements include the necessary monitoring scope that cloud service providers(CSPs) should provide to maintain the cloud security and the biggest monitoring scope of CSPs. Monitoring data lifecycle includes data creation, data store, data use, data migrate, data present, data destroy and data backup. Monitoring acquisition determines the security requirements of the acquisition techniques of monitoring service. Monitoring data storage determines the security requirements for CSPs to store the monitoring data

3 Relationship to Reference Standards

This standard is fully equivalent to ITU-T X.1603 (Data security requirements for the monitoring service of cloud computing).

목 차

Recommendation ITU-T X.1603 (X.dsms)

Data security requirements for the monitoring service of cloud computing

Summary

Recommendation ITU-T X.1603 analyses data security requirements for the monitoring service of cloud computing which include monitoring data scope requirements, monitoring data lifecycle, security requirements of monitoring data acquisition and security requirements of monitoring data storage. Monitoring data scope requirements include the necessary monitoring scope that cloud service providers (CSPs) should provide to maintain the cloud security and the biggest monitoring scope of CSPs. Monitoring data lifecycle includes data creation, data store, data use, data migrate, data present, data destroy and data backup. Monitoring acquisition determines the security requirements of the acquisition techniques of monitoring service. Monitoring data storage determines the security requirements for CSPs to store the monitoring data.

Keywords

Cloud, data security, monitoring.

Recommendation ITU-T X.1603 (X.dsms)

Data security requirements for the monitoring service of cloud computing

1 Scope

This Recommendation describes the data security requirements for the monitoring service of cloud computing. The Recommendation analyses data security threats and challenges associated with the monitoring service in a cloud computing environment, and describes data security requirements of the monitoring service including data scope, data lifecycle, data acquisition and data storage. This Recommendation can be used by cloud service providers (CSPs) who provide monitoring services to cloud service customers (CSCs).

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 authentication [b-NIST-SP-800-53]: Verification of the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

3.1.2 capability [b-ISO/IEC 19440]: Quality of being able to perform a given activity.

3.1.3 cloud computing [b-ITU-T Y.3500**]**: Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on demand.

NOTE – Examples of resources include servers, operating systems, networks, software, applications, and storage equipment.

3.1.4 cloud service [b-ITU-T Y.3500**]**: One or more capabilities offered via cloud computing (3.1.3) invoked using a defined interface.

3.1.5 cloud service customer [b-ITU-T Y.3500**]**: Party (3.1.18) which is in a business relationship for the purpose of using cloud services (3.1.4).

NOTE – A business relationship does not necessarily imply financial agreements.

3.1.6 cloud service partner [b-ITU-T Y.3500**]**: Party (3.1.18) which is engaged in support of, or auxiliary to, activities of either the cloud service provider (3.1.7) or the cloud service customer (3.1.5), or both.

3.1.7 cloud service provider [b-ITU-T Y.3500**]**: Party (3.1.18) which makes cloud services (3.1.4) available.

3.1.8 cloud service user [b-ITU-T Y.3500**]**: Natural person, or entity acting on their behalf, associated with a cloud service customer (3.1.5) that uses cloud services (3.1.4).

NOTE – Examples of such entities include devices and applications.

3.1.9 Communications as a Service (CaaS) [b-ITU-T Y.3500**]**: Cloud service category in which the capability provided to the cloud service customer (3.1.5) is real time interaction and collaboration.

NOTE – CaaS can provide both application capabilities type and platform capabilities type.

3.1.10 community cloud [b-ITU-T Y.3500**]**: Cloud deployment model where cloud services (3.1.4) exclusively support and are shared by a specific collection of cloud service customers (3.1.5) who have shared requirements and a relationship with one another, and where resources are controlled by at least one member of this collection.

3.1.11 hypervisor [b-NIST-SP-800-125]: The virtualization component that manages the guest OSs on a host and controls the flow of instructions between the guest OSs and the physical hardware.

3.1.12 Infrastructure as a Service (IaaS) [b-ITU-T Y.3500]: Cloud service category in which the cloud capabilities type provided to the cloud service customer (3.1.5) is an infrastructure capabilities type.

NOTE – The cloud service customer (3.1.5) does not manage or control the underlying physical and virtual resources, but does have control over operating systems, storage, and deployed applications that use the physical and virtual resources. The cloud service customer (3.1.5) may also have limited ability to control certain networking components (e.g., host firewalls).

3.1.13 monitor service [b-ITU-T Y.3502]: The monitor service activity monitors the delivered service quality with respect to service levels as defined in the service level agreement (SLA) between cloud service customer and cloud service provider.

3.1.14 multi-tenancy [b-ITU-T Y.3500]: Allocation of physical or virtual resources such that multiple tenants (3.1.27) and their computations and data are isolated from and inaccessible to one another.

3.1.15 Network as a Service (NaaS) [b-ITU-T Y.3500**]**: Cloud service category in which the capability provided to the cloud service customer (3.1.5) is transport connectivity and related network capabilities.

NOTE – NaaS can provide any of the three cloud capabilities types.

3.1.16 party [b- ISO/IEC 27729**]**: Natural person or legal person, whether or not incorporated, or a group of either.

3.1.17 personally identifiable information [b-ISO/IEC 29100]: Any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal.

3.1.18 Platform as a Service (PaaS) [b-ITU-T Y.3500]: Cloud service category in which the cloud capabilities type provided to the cloud service customer (3.1.5) is a platform capabilities type.

3.1.19 private cloud [b-ITU-T Y.3500**]**: Cloud deployment model where cloud services (3.1.4) are used exclusively by a single cloud service customer (3.1.5) and resources are controlled by that cloud service customer (3.1.5).

3.1.20 public cloud [b-ITU-T Y.3500]: Cloud deployment model where cloud services (3.1.4) are potentially available to any cloud service customer (3.1.5) and resources are controlled by the cloud service provider (3.1.7).

3.1.21 security domain [b-ITU-T X.810]: A set of elements, a security policy, a security authority and a set of security-relevant activities in which the set of elements are subject to the security policy for the specified activities, and the security policy is administered by the security authority for the security domain.

3.1.22 security incident [b-ITU-T E.409]: A security incident is any adverse event whereby some aspect of security could be threatened.

3.1.23 service level agreement (SLA) [b-ISO/IEC 20000-1]: A documented agreement between the service provider and customer that identifies services and service targets.

NOTE 1 – A service level agreement can also be established between the service provider and a supplier, an internal group or a customer acting as a supplier.

NOTE 2 – A service level agreement can be included in a contract or another type of documented agreement.

3.1.24 Software as a Service (SaaS) [b-ITU-T Y.3500]: Cloud service category in which the

cloud capabilities type provided to the cloud service customer (3.1.5) is an application capabilities type.

3.1.25 tenant [b-ITU-T Y.3500]: One or more cloud service users (3.1.8) sharing access to a set of physical and virtual resources.

3.1.26 threat [b-ISO/IEC 27000]: A potential cause of an unwanted incident, which may result in harm to a system or organization.

3.1.27 virtual machine (VM) [b-NIST-SP-800-145]: An efficient, isolated, logical duplicate of a real machine.

3.1.28 vulnerability [b-NIST-SP-800-30]: A weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 **necessary monitoring data**: Necessary monitoring data is used to maintain service level agreements (SLA). Necessary monitoring data could help cloud service provider (CSP) to keep cloud computing platforms security and stable. Necessary monitoring data could include, but is not limited to, management system monitoring data, physical resources monitoring data, network monitoring data and etc. Necessary monitoring data is mainly used by CSPs but could also be shared with cloud service customers (CSCs).

3.2.2 **monitoring data**: Monitoring data is the output of the cloud monitor service, which helps cloud service provider (CSP) and cloud service customers (CSC) manage cloud platforms and cloud resources.

3.2.3 **optional monitoring data**: Optional monitoring data is provided on the demand of cloud service customers (CSCs) and to provide cloud monitor service. Optional monitoring data could include, but is not limited to, virtual machine monitoring data, data storage service monitoring data, CSCs' application on cloud monitoring data and etc.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API Application Programming Interface

BCP Business Continuity Plan

CaaS Communications as a Service

CPU Central Processing Unit

CSC Cloud Service Customer

CSN Cloud Service Partner

CSP Cloud Service Provider

CSU Cloud Service User

DNS Domain Name System

IaaS Infrastructure as a Service

IAM Identity and Access Management

ICT Information and Communication Technology

IP Internet Protocol

IT Information Technology

NaaS Network as a Service

OS Operating System

PaaS Platform as a Service

PII Personally Identifiable Information

PKI Public Key Infrastructure

SaaS Software as a Service

SIM Subscriber Identity Module

SLA Service Level Agreement

VM Virtual Machine

5 Conventions

In this Recommendation:

The keywords "**is required to**" indicate a requirement which must be strictly followed and from which no deviation is permitted, if conformance to this Recommendation is to be claimed.

The keywords "**is recommended**" indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

The keywords "**is prohibited from**" indicate a requirement which must be strictly followed and from which no deviation is permitted, if conformance to this Recommendation is to be claimed.

The keywords "**can optionally**" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option, and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

6 Overview

This Recommendation analyses data security requirements for the monitoring service of cloud

computing including monitoring data scope, monitoring data lifecycle， security threats and challenges, and monitoring data security requirements of cloud computing.

Monitoring data scope describes two types of cloud monitoring data: necessary and optional, and also explains the use cases. Monitoring data lifecycle, and the security threats and challenges, describe the content and security threats and challenges of cloud monitoring data collection, storage, use, migration, analysis, presentation, destruction and backup. Monitoring data security requirements describes the detailed requirements for each lifecycle stage of cloud monitoring data.

7 Scope of monitoring data for cloud computing

In a cloud computing environment, there are two types of monitoring data: necessary monitoring data and optional monitoring data. Necessary monitoring data is that which is used to maintain service level agreements (SLA). Necessary monitoring data can help the CSP run the cloud computing platform securely and stably. Necessary monitoring data may include, but is not limited to, management system monitoring data, physical resources monitoring data and network monitoring data. Necessary monitoring data is mainly used by CSPs but could also be shared with CSCs. Optional monitoring data is that which is provided as the request of the CSC to provide the monitoring service by the CSP. Optional monitoring data may include, but not be limited to, virtual machine monitoring data, data storage service monitoring data and the CSCs' data associated with the monitoring of their own application on cloud.

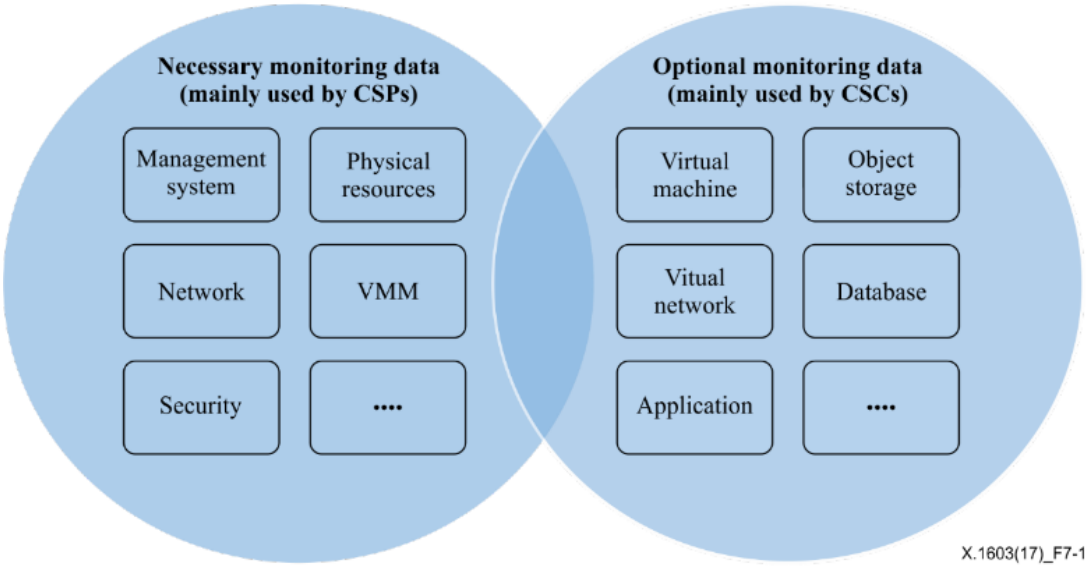


Figure 7-1 – Use cases of two types of monitoring data

Necessary monitoring data is mainly used by CSPs, but could also be used by CSCs. For example, monitoring data of cloud physical resources is mainly used by CSPs to maintain the stability of

the cloud platform, but could also be used by CSCs if the cloud related physical resources were provided to the customers as a service. Optional monitoring data is provided as the request of CSCs and also mainly used by CSCs. CSPs could also use optional monitoring data to maintain SLAs. For example, CSCs could require the CSCs' data associated with the monitoring of their own applications in the cloud. This data is provided by CSP, and used to better manage their applications in the cloud. For example, a CSP could use database as a service (DBaaS) monitoring data to maintain the security and stability of database resources and service in cloud.
The relationship of these two types of monitoring data is illustrated in Figure 7-1.

8 Monitoring data lifecycle in cloud computing

This clause describes the lifecycle of monitoring data in cloud computing and clarifies the main differences between it and lifecycle of other data in cloud computing.

8.1 Monitoring data collection

Monitoring data collection results from the acquisition of monitoring data and the transmission of that data to a storage server. Most monitoring data is created by the use of the cloud service by the CSC. Necessary monitoring data can also be created by other cloud services monitoring activities.

8.2 Monitoring data storage

After creating a monitoring data collection, cloud monitoring data can be stored in the CSC cloud resources locally, or in monitoring data storage servers of the CSP.

8.3 Monitoring data use

Monitoring data can be used to maintain the performance and security of the cloud platform and the cloud service by the CSP; it can also be used to maintain cloud resources performance and security by CSCs.

8.4 Monitoring data migration

When cloud resources are migrated, monitoring data can migrate along with the cloud resources.

8.5 Monitoring data analysis

Monitoring data can be analyzed by the CSP and CSC to understand the status of the cloud platform resources in order to better manage and secure them.

8.6 Monitoring data presentation

It is recommended that monitoring data be presentable in meaningful ways in order to be useful for better management of SLAs and cloud security. Since the volume of cloud monitoring data can be very large, is recommended that these data be summarized in a manageable and understandable way.

8.7 Monitoring data destruction

To maintain monitoring data security, the CSP is required to destroy monitoring data as CSCs demand. CSPs can optionally destroy monitoring data after an appropriate period of time after monitoring data creation.

8.8 Monitoring data backup

It is required to create monitoring data backups and restore data from backups.

9 Security threats and challenges for monitoring data of cloud computing

The security threats and challenges for cloud computing, clauses 7 and 8 respectively in [b-ITU-T X.1601], have provided the security threats and challenges for the CSC and CSP in cloud computing; cloud monitoring data also faces similar security threats and challenges that are defined in [b-ITU-T X.1601. Some of these security threats and challenges for cloud monitoring data include but are not limited to those shown below:

a) data loss and leakage;

b) insecure service access;

c) unauthorized administration access;

d) insider threats;

e) loss of trust;

f) loss of governance;

g) loss of confidentiality;

h) service unavailability;

i) misappropriation of intellectual property;

j) shared environment;

k) jurisdictional conflict;

l) bad migration and integration.

For each monitoring data lifecycle stage, cloud monitoring data face some particular security threats and challenges.

9.1 Security threats and challenges in monitoring data collection stage

a) data collection without authorization: A CSP or attackers may collect the CSC's monitoring data without permission or authorization.

b) acquisition interface vulnerability: Attackers may use a monitoring data acquisition interface vulnerability.

c) spoofing: Attackers could masquerade as the management system, or data storage server, of cloud monitoring service, and cause the loss of monitoring data.

d) tampering and intercepting: Attackers could use man-in-the-middle or other network attacks to

tamper with, or intercept monitoring data.

e) insecure service access: In the monitoring data collection stage, insecure access to the data collection interfaces could cause monitoring data loss.

f) unauthorized administration access: Unauthorized administration access to the CSP's monitoring data collection system, or the CSC's system could result in monitoring data loss. For example, attackers may use a system vulnerability to gain unauthorized administration access to the CSC's system and modify the monitoring collection destination IP address to that of the attacker's.

9.2 Security threats and challenges in monitoring data storage stage

a) data loss and leakage: As the cloud service environment is typically a multi-tenant one, loss or leakage of data is a serious threat to both the CSC and CSP. A lack of appropriate management of cryptographic information, such as encryption keys, authentication codes and access privilege, could lead to significant damages, such as data loss and unexpected leakage to the outside. For example, insufficient authentication, authorization, and audit controls; inconsistent use of encryption and/or authentication keys; operational failures; disposal problems; jurisdiction and political issues; data centre reliability; and disaster recovery, can be recognized as major threats.

b) service unavailability: A monitoring data storage server can be attacked by a denial of service (DoS) or distributed denial of service (DDoS) attack; in addition, the monitoring data storage hardware could fail and cause data loss or destruction.

9.3 Security threats and challenges in monitoring data use stage

a) data misuse: CSC monitoring data could be misused by the CSP. Monitoring data could be used by a CSP to maintain SLA and the operation of cloud computing platform and resources; however, CSC monitoring data could also be used for other purposes by the CSP without CSC permission.

b) insider threats: An employee of a CSP or CSC could misuse the CSC's monitoring data for other than intended purposes.

c) system vulnerability: Monitoring data could be lost during data usage due to system vulnerabilities.

d) eavesdropping: Monitoring data could be subject to eavesdropping by attackers.

9.4 Security threats and challenges in monitoring data migration stage

a) data misuse: Monitoring data could migrate between different physical locations. It is very important not to allow data to be misused as a result of monitoring data being transmitted to different locations.

b) spoofing: Attackers could masquerade as the management system or data storage server of a cloud monitoring service, and cause the loss or misuse of monitoring data.

c) tampering and intercepting: Attackers could use man-in-the-middle or other network attacks to tamper and intercepting monitoring data.

9.5 Security threats and challenges in monitoring data analysis stage

a) data misuse: CSC monitoring data could be misused by the CSP during data analysis.

b) system vulnerability: Monitoring data could be lost due to a data analysis system vulnerability.

c) DoS attack: A monitoring data analysis server could be attacked by DoS or DDoS attack.

9.6 Security threats and challenges in monitoring data presentation stage

a) data misuse: CSC monitoring data could be misused (or be presented without CSC permission) by the CSP during data presentation.

b) system vulnerability: Reporting and analysis data could be lost due to a data presentation system vulnerability.

c) misrepresentation: CSC monitoring data could be misrepresented during a data presentation.

9.7 Security threats and challenges in monitoring data destruction stage

a) spoofing: Attackers could masquerade as the management system of the cloud monitoring service and cause the loss of other monitoring data.

b) operating system vulnerability: Monitoring data could be lost during data usage due to a system vulnerability.

9.8 Security threats and challenges in monitoring data backup stage

a) operating system vulnerability: Monitoring data could be lost during the data backup and result in the inability to restore data due to a system vulnerability.

10 Security requirements for monitoring data of cloud computing

This clause identifies the data security requirements for the monitoring service of cloud computing.

10.1 Security requirements for monitoring data collection

The data security requirements for the monitoring data collection include the following:

a) optional monitoring data is required to be created only by CSC request;

b) it is recommended to provide notification to the CSC when necessary monitoring data is created;

c) it is recommended to notify the CSC of the scope of monitoring data;

d) it is required to maintain integrity and accuracy of monitoring data;

e) it is recommended to use standard data acquisition techniques;

f) it is recommended to provide access control methods to the interfaces of monitoring data acquisition such as white list, black list, etc.;

g) it is recommended to provide cryptographic methods to ensure the security of the monitoring data acquisition interface;
h) it is recommended to use standard network protocols between the cloud resources and monitoring data storage servers.

Table 10-1 provides a summary mapping of monitoring data collection security threats to security requirements

Table 10-1 – Monitoring data collection: security threats mapping to security requirements

Security threats	Security requirements
Data collection without authorization	a), b), c)
Acquisition interface vulnerabilities	d), e), f), g)
Spoofing	d), e), f), g), h)
Tampering and interception	h)
Insecure service access	b), d), e), f), g), h)
Unauthorized administrative access	d), e), f), g), h)

10.2 Security requirements for monitoring data storage

The data security requirements for the monitoring data storage include the following:
a) it is recommended that the CSP provide the appropriate access control methods to the monitoring data storage servers;
b) it is recommended that the CSP identify the maximum period of time for monitoring data retention;
c) it is recommended that the CSP provide appropriate encryption methods for monitoring data.

Table 10-2 provides a summary mapping of monitoring data storage security threats to security requirements.

Table 10-2 – Monitoring data storage: security threats mapping to security requirements

Security threats	Security requirements
Data loss and leakage	a), b), c)
Service unavailability	a), c)

10.3 Security requirements for monitoring data use

The data security requirements for the monitoring data use include the following:

a) it is required that the CSP clearly identify how the monitoring data is going to be used to the CSC;

b) it is recommended that the CSP provide a formal monitoring data use declaration to the CSC, such as that illustrated in Figure 10-1.

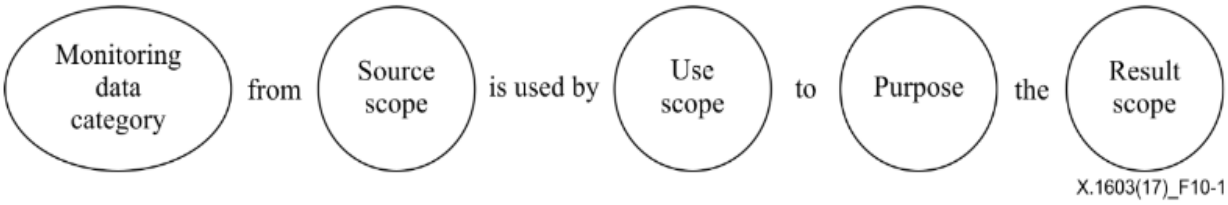


Figure 10-1 – Recommended monitoring data use declaration

c) it is required that the CSP provide notification and obtain CSC permission prior to the use of monitoring data for other than intended purpose;

d) it is required that the CSP support logging and auditing of monitoring data usage.

Table 10-3 provides a summary mapping of monitoring data use security threats to security requirements.

Table 10-3 – Monitoring data use: security threats mapping to security requirements

Security threats	Security requirements
Data misuse	a), b), c), d)
Insider threats	a), b), c), d)
System vulnerabilities	d)
Eavesdropping	d)

10.4 Security requirements for monitoring data migration

The data security requirements for the monitoring data migration include the following:

a) it is recommended that the CSP provide notification to the CSC of monitoring data migration;

b) it is required that the CSP ensure secure transmission during monitoring data migration;

c) it is required that the CSP support logging and auditing of monitoring data migration operations.

Table 10-4 provides a summary mapping of monitoring data migration security threats to security requirements.

Table 10-4 – Monitoring data migration: security threats mapping to security requirements

Security threats	Security requirements
Data misuse	a), c)
Spoofing	b), c)
Tampering and intercepting	b), c)

10.5 Security requirements for monitoring data analysis

The data security requirements for the monitoring data analysis include the following:

a) it is required that the CSP provide notification regarding the purpose of monitoring data analysis to the CSC;

b) it is required that the CSP implement defenses against the vulnerabilities of monitoring data analysis system, for example the CSP should prevent data loss and leakage in the monitoring data analysis system;

Table 10-5 provides a summary mapping of monitoring data analysis security threats to security requirements.

Table 10-5 – Monitoring data analysis: security threats mapping to security requirements

Security threats	Security requirements
Data misuse	a)
System vulnerability	b)
Dos attack	b)

10.6 Security requirements for monitoring data presentation

The data security requirements for the monitoring data presentation include the following:

a) it is required that the CSP maintain the integrity and accuracy of presented monitoring data;

b) it is required that the CSP implement authentication methods to protect access the monitoring data presentation;

c) it is required that the CSP support defenses against the vulnerabilities of the monitoring data presentation system, for example the CSP could use penetration testing methods to prevent vulnerabilities of the monitoring data presentation system.

Table 10-6 provides a summary mapping of monitoring data presentation security threats to security requirements.

Table 10-6 – Monitoring data presentation: security threats mapping to security requirements

Security threats	Security requirements
Data misuse	a), b)
System vulnerability	b), c)
misrepresentation	a), b), c)

10.7 Security requirements for monitoring data destruction

The data security requirements for the monitoring data destruction include the following:

a) it is required that the CSP provide appropriate destruction methods for monitoring data;

b) it is required that the CSP prevent the unintended destruction of monitoring data;

c) it is required that the CSP prevent the incomplete destruction of monitoring data;

d) it is required that the CSP erase any CSC specific keys for encrypted data;

e) it is required that the CSP destroy copies of monitoring data;

f) it is required that the CSP provide notification of monitoring data destruction to the CSC.

Table 10-7 provides a summary mapping of monitoring data destruction security threats to security requirements.

Table 10-7 – Monitoring data destruction: security threats mapping to security requirements

Security threats	Security requirements
Spoofing	a), b), c), d), e), f)
Operating system vulnerability	b), c), d), e), f)

10.8 Security requirements for monitoring data backup

The data security requirements for the monitoring data backup include the following:

a) it is required that the CSP provide backup methods to prevent monitoring data loss;

b) it is required that the CSP maintain the integrity and accuracy of restored monitoring data;

c) it is required that the CSP support logging and auditing of monitoring data restoration.

Table 10-8 provides a summary mapping of monitoring data backup security threats to security requirements.

Table 10-8 – Monitoring data backup: security threats mapping to security requirements

Security threats	Security requirements
Operating system vulnerability	a), b), c)

Bibliography

[b-ITU-T E.409] Recommendation ITU-T E.409 (2004), *Incident organization and security incident handling: Guidelines for telecommunication organizations*.

[b-ITU-T X.810] Recommendation ITU-T X.810 (1995), *Information technology – Open System Interconnection – Security frameworks for open system: Overview*.

[b-ITU-T X.1601] Recommendation ITU-T X.1601 (2015), *Security framework for cloud computing*.

[b-ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014), *Information technology – Cloud computing – Overview and vocabulary*.

[b-ITU-T Y.3502] Recommendation ITU-T Y.3502 (2014), *Information technology – Cloud computing – Reference architecture*.

[b-ISO/IEC 19440] ISO/IEC 19440 (2007), *Enterprise integration – Constructs for enterprise modelling*.

[b-ISO/IEC 19944] ISO/IEC 19944 (2016), *Information technology – Cloud services and devices: data flow, data categories and data use*.

[b-ISO/IEC 20000-1] ISO/IEC 20000-1 (2011), *Information technology –Service management – Part1: Service management system requirements.*

[b-ISO/IEC 27000] ISO/IEC 27000 (2016), *Information technology –Security techniques – Information security management systems – Overview and vocabulary*.

[b-ISO/IEC 27729] ISO/IEC 27729 (2012), *Information and documentation – International standard name identifier (ISNI).*

[b-ISO/IEC 29100] ISO/IEC 29100 (2011), *Information technology –Security techniques – Privacy framework.*

[b-NIST-SP-800-30] NIST Special Publication 800-30 (2012), *Guide for Conducting Risk Assessments.*

[b-NIST-SP-800-53] NIST Special Publication 800-53 Rev.3 (2009), *Recommended Security Controls for Federal Information Systems and Organizations.*

[b-NIST-SP-800-125] NIST Special Publication 800-125 (2011), *Guide to Security for Full Virtualization Technologies.*

[b-NIST-SP-800-145] NIST Special Publication 800-145 (2011), The NIST Definition of Cloud Computing.

부 록 Ⅰ-1

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

지식재산권 확약서 정보

Ⅰ-1.1 지식재산권 확약서(1)

- 해당 사항 없음.

Ⅰ-1.2 지식재산권 확약서(2)

- 해당 사항 없음.

※ 상기 기재된 지식재산권 확약서 이외에도 본 표준이 발간된 후 접수된 확약서가 있을 수 있으니, TTA 웹사이트에서 확인하시기 바랍니다.

부 록 Ⅰ-2

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

시험인증 관련 사항

Ⅰ-2.1 시험인증 대상 여부

- 해당 사항 없음.

Ⅰ-2.2 시험표준 제정 현황

- 해당 사항 없음.

부 록 Ⅰ-3

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

본 표준의 연계(family) 표준

- 해당 사항 없음.

부 록 Ⅰ-4

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

참고 문헌

[1] Recommendation ITU-T E.409 (2004), Incident organization and security incident handling: Guidelines for telecommunication organizations.

[2] Recommendation ITU-T X.810 (1995), Information technology - Open System Interconnection - Security frameworks for open system: Overview.

[3] Recommendation ITU-T X.1601 (2015), Security framework for cloud computing.

[4] Recommendation ITU-T Y.3500 (2014), Information technology - Cloud computing - Overview and vocabulary.

[5] Recommendation ITU-T Y.3502 (2014), Information technology - Cloud computing - Reference architecture.

[6] ISO/IEC 19440 (2007), Enterprise integration - Constructs for enterprise modelling.

[7] ISO/IEC 19944 (2016), Information technology - Cloud services and devices: data flow, data categories and data use.

[8] ISO/IEC 20000-1 (2011), Information technology -Service management - Part1: Service management system requirements.

[9] ISO/IEC 27000 (2016), Information technology -Security techniques - Information security management systems - Overview and vocabulary.

[10] ISO/IEC 27729 (2012), Information and documentation - International standard name identifier (ISNI).

[11] ISO/IEC 29100 (2011), Information technology -Security techniques -Privacy framework.

[12] NIST Special Publication 800-30 (2012), Guide for Conducting Risk Assessments.

[13] NIST Special Publication 800-53 Rev.3 (2009), Recommended Security Controls for Federal Information Systems and Organizations.

[14] NIST Special Publication 800-125 (2011), Guide to Security for Full Virtualization Technologies.

[15] NIST Special Publication 800-145 (2011), The NIST Definition of Cloud Computing.

부 록 Ⅰ-5

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

영문표준 해설서

Ⅰ-5.1 표준의 범위

본 표준은 클라우드 컴퓨팅에서의 모니터링 서비스에 대한 데이터 보안 요구사항을 기술하는 문서이다. 클라우드 컴퓨팅 환경에서의 모니터링 서비스와 연관된 데이터 보안 위협과 문제점을 분석하고, 데이터 범위/라이프사이클/획득/저장 등의 모니터링 서비스 데이터 보안 요구사항을 기술하고 있는 본 표준은 모니터링 서비스를 클라우드 서비스 고객(CSC, Cloud Service Customer)들에게 제공하는 클라우드 서비스 제공자(CSP, Cloud Service Provider)들이 사용할 수 있다.

Ⅰ-5.2 참조 표준

해당 사항 없음

Ⅰ-5.3 용어 정의

본 표준에서 사용되는 용어를 정의한다.

Ⅰ-5.4 약어

본 표준에서 사용되는 약어를 정의한다.

Ⅰ-5.5 규약

본 표준에서 사용되는 문구 규약를 정의한다.

Ⅰ-5.6 개요

본 표준은 클라우드 컴퓨팅의 모니터링 서비스에 대한 데이터 범위 및 라이프사이클과 모니터링 데이터 획득/저장 관련 보안 요구 사항 등을 포함한다. 모니터링 데이터 범위 요구사항은 클라우드 서비스 제공자(CSP, Cloud Service Provider)들이 클라우드 보안 및 최대 모니터링 범위 유지를 위해 제공해야 하는 필수 모니터링 범위를

포함한다. 모니터링 데이터 라이프 사이클은 데이터의 생성/저장/사용/마이그레이션/표현/삭제/백업 등을 포함한다. 모니터링 데이터 획득은 모니터링 서비스로부터 데이터를 획득하는 기술 관련 보안 요구사항을 기술한다.

Ⅰ-5.7 모니터링 데이터의 범위

클라우드 컴퓨팅 환경에서의 모니터링 데이터는, CSP가 주로 사용하는 필수 데이터와 CSC가 요청하고 CSP가 제공하는 옵션 데이터로 구분된다. SLA 유지에 주로 사용되는 필수 데이터는 CSP로 하여금 클라우드 컴퓨팅 플랫폼을 견고하고 안정적으로 운영할 수 있도록 하는 것으로, 리소스/네트워크/시스템 모니터링 데이터 등이 해당되는 반면, 가상머신 및 데이터 스토리지 서비스 모니터링 데이터와 클라우드 상의 CSC별 애플리케이션 모니터링 데이터 등은 옵션 데이터에 해당된다.

Ⅰ-5.8 클라우드 컴퓨팅 환경에서의 모니터링 데이터 라이프사이클

클라우드 컴퓨팅 환경에서 사용되는 모니터링 데이터의 라이프사이클을 표로 정리하면 다음과 같다.

모니터링 데이터 라이프사이클	설명
Data Collection	모니터링 데이터를 획득하고 스토리지 서버에 전송할 때까지의 데이터를 의미
Data Storage	수집된 모니터링 데이터는 CSC 클라우드 리소스에 로컬하게 저장되거나 CSP 스토리지 서버에 저장
Data Use	모니터링 데이터는 클라우드 플랫폼과 CSP가 제공하는 클라우드 서비스 성능 및 안전성 유지를 위해 사용
Data Migration	클라우드 리소스가 마이그레이션되면, 모니터링 데이터도 마이그레이션된다.
Data Analysis	양질의 서비스 및 보안성 강화를 목적으로, 클라우드 플랫폼 리소스 상태를 파악하기 위해 모니터링 데이터를 분석
Data Presentation	모니터링 데이터가 의미있는 형태로 표현되면, 양질의 SLA 및 효율적 클라우드 보안 관리가 가능해짐
Data Destruction	모니터링 데이터의 안전성 강화를 위해, CSC의 요구가 있거나 데이터 생성 후 지속 시간이 경과하면 모니터링 데이터를 폐기
Data Backup	모니터링 데이터를 백업하고 필요 시 데이터를 복구할 수 있도록 하는 것이 요구됨

Ⅰ-5.9 클라우드 컴퓨팅 모니터링 데이터에 대한 보안 위협과 문제점

클라우드 모니터링 데이터의 보안 위협과 문제점은 데이터 손실(loss)과 누출(leakage), 안전하지 않은 서비스 접속, 비인가 관리자 접속, 내부자 위협, 신뢰 상실, 거버넌스 상실, 기밀성(confidentiality) 상실, 서비스 불가용성(unavailability), 지적 재산 유용(misappropriation), 공유 환경, 법적 분쟁, 마이그레이션/통합 오류 등으로 요약할 수 있다.

모니터링 데이터 보안 위협	설명
Data collection without authorization	허락이나 권한 없이 CSC의 모니터링 데이터를 수집
Acquisition interface vulnerability	모니터링 데이터 획득 인터페이스 취약성을 이용한 공격
Spoofing	클라우드 모니터링 서비스 관리 시스템이나 데이터 스토리지 서버로 가장하여 모니터링 데이터 공격
Tampering/Intercepting	Man-in-the-middle 공격이나 다른 네트워크 공격을 통해 모니터링 데이터 도청/가로채기
Insecure service access	데이터 수집 인터페이스에 대한 안전하지 않은 접속은 모니터링 데이터 손실을 가져올 수 있음
Unauthorized administration access	CSP 모니터링 데이터 수집 시스템이나 CSC 시스템에 대한 비인가 관리자 접속은 모니터링 데이터 손실을 가져올 수 있음
Data loss and leakage	클라우드 서비스는 멀티 테넌트 환경에서 제공되므로, 데이터 손실이나 누출은 CSC나 CSP 모두에게 매우 심각한 위협이 될 수 있음. 충분하지 않은 인증/허가/감사 제어, 부적합한 암호/인증키 사용, 동작 오류, 폐기 처분 문제, 사법적/정치적 이슈, 데이터 센터 신뢰도, 재해 복구 등이 원인이 될 수 있음
Service unavailability	DoS/DDoS 공격을 받거나 또는 모니터링 데이터 스토리지 하드웨어 고장으로 인하여 데이터 손실이 발생할 수 있음
Data misuse	CSP는 CSC에게 허가를 득하지 않고 CSC 모니터링 데이터를 원래 목적이 아닌 다른 목적으로 사용할 가능성이 있음
Insider threats	CSP/CSC 직원이 CSC의 모니터링 데이터를 다른 의도로 사용할 수 있음
System vulnerability	시스템의 취약성으로 인해 사용중인 모니터링 데이터가 손실될 수 있음
eavesdropping	모니터링 데이터는 공격자로 하여금 도청의 대상이 될 수 있음
DoS attack	모니터링 데이터 서버들은 서비스 거부 공격이나 분산 서비스 거부 공격에 취약할 수 있음
misrepresentation	CSC 모니터링 데이터가 왜곡되게 표현될 수 있음
Operating system vulnerability	시스템 취약성으로 인해 다양한 경우에 모니터링 데이터 손실이 발생할 수 있음

Ⅰ-5.10 클라우드 컴퓨팅 모니터링 데이터에 대한 보안 요구사항

클라우드 모니터링 데이터의 보안 요구사항을 앞서 설명한 보안 위협 및 문제점과 매핑될 수 있도록 구분하여 기술한다.

Ⅰ-5.10.1 모니터링 데이터 수집 단계에서의 보안 요구사항

a) 옵션 모니터링 데이터는 CSC 요청에 의해서만 생성되도록 하는 것이 요구된다.
b) 필수 모니터링 데이터가 생성되면 이를 CSC에게 통지하는 기능을 제공하는 것을 권고한다.
c) CSC에게 모니터링 데이터의 범위를 알려주는 것을 권고한다.
d) 모니터링 데이터 무결성 및 정확성을 유지하도록 하는 것이 요구된다.
e) 표준 데이터 획득 기술을 사용하는 것을 권고한다.
f) 모니터링 데이터 획득 인터페이스에 화이트리스트나 블랙리스트 같은 접근 제어 방법을 제공하는 것을 권고한다.
g) 모니터링 데이터 획득 인터페이스 보안성 강화를 위해 암호학적 방법을 제공하는 것을 권고한다.
h) 클라우드 리소스와 모니터링 데이터 저장 서버 간에 표준 네트워크 프로토콜을 사용하는 것을 권고한다.

* 모니터링 데이터 수집에 관한 보안 위협과 보안 요구사항의 상호 매핑은 원문 표 10-1을 참조한다.

Ⅰ-5.10.2 모니터링 데이터 저장 단계에서의 보안 요구사항

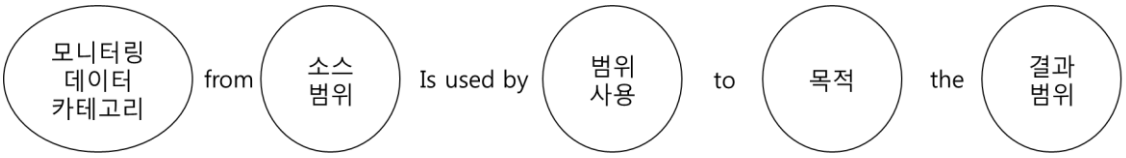
a) CSP는 모니터링 데이터 저장 서버에게 정확한 접근 제어 방법을 제공하는 것을 권고한다.
b) CSP는 모니터링 데이터 최대 보유 기간을 정하는 것을 권고한다.
c) CSP는 모니터링 데이터에 대한 정확한 암호화 방법을 제공하는 것을 권고한다.

* 모니터링 데이터 저장에 관한 보안 위협과 보안 요구사항의 상호 매핑은 원문 표 10-2를 참조한다.

I -5.10.3 모니터링 데이터 사용 단계에서의 보안 요구사항

a) CSP는 모니터링 데이터가 CSC에게 어떻게 사용되는지 명확하게 정의하는 것이 요구된다.

b) CSP는 다음 그림과 같이 정규 형태의 모니터링 데이터 사용 관계도를 CSC에게 제공하는 것을 권고한다.



X.1603(17)_F10-1

c) CSP는 고유 용도가 아닌 다른 목적으로 모니터링 데이터를 사용할 경우, 사용 전에 CSC의 허락을 득하고 이를 통보하는 기능을 제공하는 것이 요구된다.

d) CSP는 모니터링 데이터 사용에 대한 로깅과 감사 기능 지원을 제공하는 것이 요구된다.

* 모니터링 데이터 사용에 관한 보안 위협과 보안 요구사항의 상호 매핑은 원문 표 10-3을 참조한다.

I -5.10.4 모니터링 데이터 마이그레이션 단계에서의 보안 요구사항

a) CSP는 모니터링 데이터 마이그레이션 여부를 CSC에게 통보하는 기능을 제공하는 것을 권고한다.

b) CSP는 모니터링 데이터 마이그레이션 동안 안전한 전송을 보장하는 것이 요구된다.

c) CSP는 모니터링 데이터 마이그레이션 동작에 대한 로깅과 감사 기능 지원을 제공하는 것이 요구된다.

* 모니터링 데이터 마이그레이션에 관한 보안 위협과 보안 요구사항의 상호 매핑은 원문 표 10-4를 참조한다.

I -5.10.5 모니터링 데이터 분석 단계에서의 보안 요구사항

d) CSP는 모니터링 데이터 분석 목적에 대하여 CSC에게 통보하는 기능을 제공하는 것이 요구된다.

a) CSP는 모니터링 데이터 분석 시스템 취약성에 대한 방어 기능을 제공하는 것이 요구된다. 예를 들면, CSP는 모니터링 데이터 분석 시스템 상의 데이터 손실 및 누출을 방지할 수 있어야 한다.

* 모니터링 데이터 분석에 관한 보안 위협과 보안 요구사항의 상호 매핑은 원문 표 10-5를 참조한다.

Ⅰ-5.10.6 모니터링 데이터 표현 단계에서의 보안 요구사항

a) CSP는 표현되는 모니터링 데이터에 대한 무결성 및 정확성을 유지하는 것이 요구된다.
b) CSP는 모니터링 데이터 표현 시스템에 대한 접근을 제어할 인증 방법을 제공하는 것이 요구된다.
c) CSP는 모니터링 데이터 표현 시스템 취약성에 대한 방어 기능을 제공하는 것이 요구된다. 예를 들면, CSP는 모니터링 데이터 표현 시스템 취약성을 막기 위해 침투 테스팅 방법을 사용할 수 있다.

* 모니터링 데이터 표현에 관한 보안 위협과 보안 요구사항의 상호 매핑은 원문 표 10-6을 참조한다.

Ⅰ-5.10.7 모니터링 데이터 폐기 단계에서의 보안 요구사항

a) CSP는 모니터링 데이터에 대한 정확한 폐기 방법을 제공하는 것이 요구된다.
b) CSP는 의도되지 않은 모니터링 데이터 폐기를 막도록 하는 것이 요구된다.
c) CSP는 완전하지 않은 모니터링 데이터 폐기를 막도록 하는 것이 요구된다.
d) CSP는 CSC의 특정 암호화키들을 삭제할 수 있도록 하는 것이 요구된다.
e) CSP는 모니터링 데이터 복사본을 폐기하는 것이 요구된다.
f) CSP는 CSC에게 모니터링 데이터 폐기 여부를 통보하는 것이 요구된다.

* 모니터링 데이터 폐기에 관한 보안 위협과 보안 요구사항의 상호 매핑은 원문 표 10-7을 참조한다.

Ⅰ-5.10.8 모니터링 데이터 백업 단계에서의 보안 요구사항

a) CSP는 모니터링 데이터 손실을 막기 위해 백업 방법을 제공하는 것이 요구된다

b) CSP는 복구된 모니터링 데이터의 무결성과 정확성을 유지하는 것이 요구된다.

c) CSP는 모니터링 데이터 복구에 대한 로깅 및 감사 기능을 제공하는 것이 요구된다.

* 모니터링 데이터 백업에 관한 보안 위협과 보안 요구사항의 상호 매핑은 원문 표 10-8을 참조한다.

부 록 Ⅰ-6

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

표준의 이력

판수	채택일	표준번호	내용	담당 위원회
제1판			-	사이버보안 (PG503)