System Infrastructure Non-Functional Requirements Related Item List

April 2013

Information-Technology Promotion Agency, Japan
Software Engineering Center

[Usage conditions]

1. The copyright to this document is held by the Information-Technology Promotion Agency, Japan.

2. This document is protected by the Copyright Act of Japan and other international copyright protection conventions and treaties. Except for the exceptions listed in item 3, modification, public transmission, sale, publishing, translation, and adaptation of this document, in whole or in part, without the explicitly written permission of the Information-Technology Promotion Agency, Japan, is strictly prohibited, regardless of whether or not said actions are performed for purposes of profit.

3. The Information-Technology Promotion Agency, Japan grants users of this document to perform the two, and only two, actions mentioned below ((1) and (2)), provided that the following copyright notice is clearly indicated.
   Copyright notice: Copyright © 2010 IPA
   (1) Duplication of this document, in whole or in part.
   (2) Free redistribution of duplications of this document on the condition that the parties to which the duplication is redistributed are put under the same obligations as described on this page.

4. The Information-Technology Promotion Agency, Japan makes no guarantees of this document containing no infringements of the copyrights, patent rights, or other intellectual property rights, such as utility model rights, of third parties, nor does it assume any responsibility for possible errors contained herein. The Information-Technology Promotion Agency, Japan makes no guarantees that the content of this document will conform to the legal requirements for export, technology transfer, and other national laws and regulations of any country or region.

5. Other than the exceptions specified on this page, the Information-Technology Promotion Agency, Japan does not grant any rights nor any license relating to copyrights, patent rights, or other intellectual property rights, such as utility model rights, of the Information-Technology Promotion Agency, Japan or of third parties.

6. The Information-Technology Promotion Agency, Japan shall not be held in any way responsible for damages which may result from using this document in system development, the use of the developed systems, or the inability to use said systems.

7. Please contact the Information-Technology Promotion Agency, Japan's Software Engineering Center with inquiries regarding this document.

System Infrastructure Non-Functional Requirements Related Item List

• Item list explanatory notes

No.	Major category	Middle category	Minor category	Minor category description	Overlapping item	Important item	Metric	Level						Impact on operation costs	Notes
								0	1	2	3	4	5		
A.1.1.1	Availability	Continuity	Operation schedule	Information regarding system operating hours and operation outage.	X	X	Operating hours (normal)	Not specified	During business hours (9:00 to 17:00)	Outage only at night (9:00 to 21:00)	Possible outage for approximately 1 hour (9:00 to 8:00 the next day)	Possible outage for a brief period (9:00 to 8:55 the next day)	Uninterrupted 24 hours		[Overlapping Item] C.1.1.1. "Operating hours" indicates the possible level of system availability, and is an item which must be considered when deliberating about operability and maintainability related development costs and operation costs. As such, it is included in both "availability" and "operability and maintainability". [Metric] "Operating hours" refers to the time periods when the system is operational, including online and batch processing. [Level] The times in parentheses "()" are examples for each level. They are not to be used as level selection conditions. "Not specified" refers to a system not having specified service hours, and is envisioned essentially for cases where the system is shut down and started up as necessary by users (Ex: Backup systems prepared for failure recovery, development and validation systems, etc.) "During business hours" and "Outage only at night" are envisioned for general business usage, and the times provided as examples should be read as examples only, and modified as appropriate for systems with different operating hours. "Possible outage" refers to time periods where the system may possibly be shut down, not where it must be shut down. "Uninterrupted 24 hours" also includes cases where batch processes must be executed when the system is not involved in online business, and which therefore require that the system not be shut down.
A.1.1.2					X	X	Operating hours (specific days)	Not specified	During business hours (9:00 to 17:00)	Outage only at night (9:00 to 21:00)	Possible outage for approximately 1 hour (9:00 to 8:00 the next day)	Possible outage for a brief period (9:00 to 8:55 the next day)	Uninterrupted 24 hours		[Overlapping Item] C.1.1.2. "Operating hours" indicates the possible level of system availability, and is an item which must be considered when deliberating about operability and maintainability related development costs and operation costs. As such, it is included in both "availability" and "operability and maintainability". [Metric] "Specific days" refer to weekends, holidays, the end/start of months, and other days whose schedule is defined as differing from the normal operation schedule. If there are multiple specific days, their level values must be made consistent (Ex: "Monday to Friday is level 2, but Saturday and Sunday are level 0," "Normally, the level is 5, but the system is rebooted on the first of each month, so on that day, the level is 3"). In addition to user holidays, vendor holidays must also be recognized as specific days, and an operation and maintenance structure, etc. must be established accordingly.
A.1.1.3					X	X	Existence of planned system shutdown	Possible planned system shutdown (operation schedule can be changed)	Possible planned system shutdown (operation schedule cannot be changed)	No planned system shutdown				X	[Overlapping Item] C.2.1.1. "Existence of planned system shutdown" indicates the possible level of system availability, and is an item which must be considered when deliberating about operability and maintainability related development costs and operation costs. As such, it is included in both "availability" and "operability and maintainability". [Impact on Operation Costs] When there are planned system shutdown, operational costs may increase due to pre-shutdown backups and the preparation of procedures in accordance with the system configuration.

(a) (b) (c) (d) (e) (f) (g) (h) (i) (j) (k)

(a) No.	:	Sequential number indicating major category, middle category, minor category, or metric. Major categories are indicated with a letter (A to F), and each item number, from middle category to metric, is separated by a period.
(b) Major category	:	Broadest category for non-functional requirements systematically organized.
(c) Middle category	:	Category indicating which minor categories should be grouped to be considered as a single unit.
(d) Minor category	:	Item indicating a non-functional requirement for which a consensus should be reached between the user and vendor.
(e) Minor category description	:	Explanation of the contents of the minor category, and how it should be approached.
(f) Overlapping item	:	Item which is repeated in multiple major categories. The non-functional requirements grades assume that the parties involved in considering each major category, and the priority of their consideration, can be different. Some items are repeated in order to prevent them being overlooked.
(g) Important item	:	Item with significant impact on quality and cost when considering non-functional requirements. Items designated as important items are used in the structuring of the grade table.
(h) Metric	:	Indices used to quantitatively express minor categories. Depending on the system structure, one metric may require multiple consensus levels.
(i) Level	:	Value, from 0 to 6, corresponding to metric and indicating a value normally applicable for the item. The higher the level number, the harder the item is to implement, and generally the higher the development costs.
(j) Impact on operation costs	:	Metric indicating possibility of reducing operating costs by increasing development spending.
(k) Notes	:	Supplementary explanation for each metric. Provides information regarding items which could not be expressed within the item list structure.

System Infrastructure Non-Functional Requirements Related Item List

No.	Major category	Middle category	Minor category	Minor category description	Overlapping item	Important item	Metric	Level						Impact on operation costs	Notes
								0	1	2	3	4	5		
A.1.1.1	Availability	Continuity	Operation schedule	Information regarding system operating hours and operation outage.	X	X	Operating hours (normal)	Not specified	During business hours (9:00 to 17:00)	Outage only at night (9:00 to 21:00)	Possible outage for approximately 1 hour (9:00 to 8:00 the next day)	Possible outage for a brief period (9:00 to 8:55 the next day)	Uninterrupted 24 hours		[Overlapping Item] C.1.1.1. "Operating hours" indicates the possible level of system availability, and is an item which must be considered when deliberating about operability and maintainability related development costs and operation costs. As such, it is included in both "availability" and "operability and maintainability". [Metric] "Operating hours" refers to the time periods when the system is operational, including online and batch processing. [Level] The times in parentheses "()" are examples for each level. They are not to be used as level selection conditions. "Not specified" refers to a system not having specified service hours, and is envisioned essentially for cases where the system is shut down and started up as necessary by users (Ex: Backup systems prepared for failure recovery, development and validation systems, etc.) "During business hours" and "Outage only at night" are envisioned for general business usage, and the times provided as examples should be read as examples only, and modified as appropriate for systems with different operating hours. "Possible outage" refers to time periods where the system may possibly be shut down, not where it must be shut down. "Uninterrupted 24 hours" also includes cases where batch processes must be executed when the system is not involved in online business, and which therefore require that the system not be shut down.
A.1.1.2					X	X	Operating hours (specific days)	Not specified	During business hours (9:00 to 17:00)	Outage only at night (9:00 to 21:00)	Possible outage for approximately 1 hour (9:00 to 8:00 the next day)	Possible outage for a brief period (9:00 to 8:55 the next day)	Uninterrupted 24 hours		[Overlapping Item] C.1.1.2. "Operating hours" indicates the possible level of system availability, and is an item which must be considered when deliberating about operability and maintainability related development costs and operation costs. As such, it is included in both "availability" and "operability and maintainability". [Metric] "Specific days" refer to weekends, holidays, the end/start of months, and other days whose schedule is defined as differing from the normal operation schedule. If there are multiple specific days, their level values must be made consistent (Ex: "Monday to Friday is level 2, but Saturday and Sunday are level 0," "Normally, the level is 5, but the system is rebooted on the first of each month, so on that day, the level is 3"). In addition to user holidays, vendor holidays must also be recognized as specific days, and an operation and maintenance structure, etc. must be established accordingly.
A.1.1.3					X	X	Existence of planned system shutdown	Possible planned system shutdown (operation schedule can be changed)	Possible planned system shutdown (operation schedule cannot be changed)	No planned system shutdown				X	[Overlapping Item] C.2.1.1. "Existence of planned system shutdown" indicates the possible level of system availability, and is an item which must be considered when deliberating about operability and maintainability related development costs and operation costs. As such, it is included in both "availability" and "operability and maintainability". [Impact on Operation Costs] When there are planned system shutdown, operational costs may increase due to pre-shutdown backups and the preparation of procedures in accordance with the system configuration.
A.1.2.1			Business continuity	Business scope and conditions required to ensure availability		X	Affected business scope	Internal batch related businesses	Internal online businesses	All internal businesses	External batch related businesses	External online businesses	All businesses		[Metric] The "affected business scope" here refers to the scope which is used for uptime ratio calculation. [Level] "Internal" refers to closed (business) processing within the system. "External" refers to (business) processing which requires coordination with other systems.
A.1.2.2						X	Service switchover time	24 hours or longer	Less than 24 hours	Less than 2 hours	Less than 60 minutes	Less than 10 minutes	Less than 60 seconds	X	[Metric] "Service switchover time" refers to the amount of time necessary for a system which has suffered a possible failure (such as temporary business interruption due to hardware failures, etc.) to resume business by taking response measures (for example, performing server switchover in a clustered system). [Impact on Operation Costs] The longer the permitted interruption time, the ratio of manual response as recovery measures will be greater than automatic system response measure implementation, impacting operation costs.
A.1.2.3						X	Required level of business continuity	Business interruption is accepted when a system failure occurs	Business interruption is not accepted when a single failure occurs; processing is continued	Business is continued within service switchover time restrictions even in the event of double failures					[Metric] The "required level of business continuity" is the criteria indicating the extent to which business must be continued in the event of a failure. The equipment and components that make up systems have many single points of failure (SPOF), resulting in many risks of system outage. This requirement based on whether these SPOF are tolerated, or the extent to which continuity is ensured through redundancy measures, etc.
A.1.3.1			Recovery objective (When business outage occurs)	Objectives for what should be recovered, to which point, within how much time when a failure results in business outage.		X	Recovery point objective (RPO)	Recovery not necessary	Up until 5 business days prior to outage (Recovery from weekly backup)	Up until 1 business day prior to outage (Recovery from daily backup)	Up until the point at which failure occurred (Recovery from daily backup + archive)				[Metric] When an RLO specifies business recovery, applicable business data recovery is included in the scope, and business resumption consistency confirmation will be required separately. [Level 3] The "point at which failure occurred" refers to the point immediately after the last transaction which was processed just before the failure. Recovery to the point at which the failure occurred assumes that the transaction journal up to the point of failure is guaranteed. It also assumes that journals are archived, making it possible to restore the system to any desired point up to the point at which the failure occurred.

System Infrastructure Non-Functional Requirements Related Item List

No.	Major category	Middle category	Minor category	Minor category description	Overlapping item	Important item	Metric	Level 0	Level 1	Level 2	Level 3	Level 4	Level 5	Impact on operation costs	Notes
A.1.3.2						X	Recovery time objective (RTO)	1 business day or more	Within 1 business day	Within 12 hours	Within 6 hours	Within 2 hours			[Metric] The RTO recovery time differs from the recovery time of the service switchover time (A.1.2.2), indicating the duration time to recover when business continuity measures are not implemented (resulting in a business outage). When an RLO specifies business recovery, applicable business data recovery is included in the scope, and business resumption consistency confirmation will be required separately.
A.1.3.3						X	Recovery level objective (RLO)	System recovery	Specific businesses only	All businesses					[Metric] This level indicates what should be recovered when a failure results in business outage. [Level 0] System recovery includes not only hardware recovery, but data restoration as well. [Level 1] "Specific businesses" refers to, for example, business whose continuity is required as specified in A.1.2.1 "Affected business scope."
A.1.4.1			Recovery objective (In event of large-scale disaster)	This metric is the target recovery time in the event of a large-scale disaster. Large-scale disasters refer to damage caused by fires and natural hazards such as earthquakes, as well as man-made damage that are accidental or intentional, which cause extensive damage to the system, or make it difficult to recover the system because lifelines such as power are interrupted.		X	System resumption objective	Resumption not necessary	Resumption within several months	Resumption within 1 month	Resumption within 1 week	Resumption within 3 days	Resumption within 1 day		[Metric] For large-scale disasters, specific requirements such as RPO, RTO, and RLO are not defined; instead, a general resumption time is set as a system resumption objective. Regarding the recovery level objective (RLO), refer to "Recovery objective (When business outage occurs)".
A.1.5.1			Uptime ratio	Percentage of time that the system can provide the requested service under specified usage conditions. "Specified usage conditions" refers to the system's operation schedule and conditions under which business defined by the recovery objective are carried out. The uptime ratio is determined from the amount of time service is interrupted during the operating hours.		X	Uptime ratio	Less than 95%	95%	99%	99.9%	99.99%	99.999%		[Level] For 24/365 operation, annual business outage totals are shown below for each level. 95% ..... 18.3 days 99% ..... 87.6 hours 99.9% ..... 8.76 hours 99.99% ..... 52.6 minutes 99.999% ..... 5.26 minutes For a system which operates 8 hours a day, 5 days a week, the relationship between service switchover time and uptime ratio is as shown below. 1 hour per week ..... 97.5% 1 hour per month ..... 99.4% 1 hour per year 99.95%
A.2.1.1		Fault tolerance	Server	Requirements to maintain the requested service when a failure occurs on a server.			Redundancy (equipment)	Non-redundant design	Redundant design for specific servers	Redundant design for all servers					[Metric] Equipment and components in "Redundancy" indicate the units of redundancy. Equipment redundancy refers to providing multiple units of equipment; component redundancy refers to providing multiple components which make up a unit (disks, power supplies, fans, network cards, etc.). By applying virtualization technologies, multiple server functions can be aggregated in a single piece of hardware, resulting in a decreased amount of hardware necessary for redundancy. Either way, equipment redundancy must be considered in order to fulfill hardware business continuity requirements. [Level 1] "Redundant design for specific servers" refers to using different redundancy approaches for different types of servers which are used in a system (DB servers, AP servers, monitoring servers, etc.). When requirements are not for individual servers, but redundancy for business or functions, set levels based on the servers which is assumed will handle these business or functions.
A.2.1.2							Redundancy (components)	Non-redundant design	Redundant design for specific components only	Redundant design for all components					[Level 1] This assumes redundancy for the components which make up a server (internal disks, power supplies, fans, etc.) as needed (for example, mirroring of internal disks, dual network interface cards, etc.).
A.2.2.1			Terminal	Requirements to maintain the requested service when a failure occurs on a terminal.			Redundancy (equipment)	Non-redundant design	Installation of shared backup terminals	Installation of backup terminals for individual business and purposes					
A.2.2.2							Redundancy (components)	Non-redundant design	Redundant design for specific components only	Redundant design for all components					[Level 1] This assumes redundancy for the components which make up a terminal (internal disks, power supplies, fans, etc.) as needed (for example, RAID configuration of internal disks, etc.).
A.2.3.1			Networking equipment	Requirements to maintain the requested service when a failure occurs on equipment, such as routers or switches, which make up a network.			Redundancy (equipment)	Non-redundant design	Redundant design for specific equipment only	Redundant design for all equipment					[Level 1] "Specific equipment only" assumes switches, routers, and other network equipment which accommodate servers with redundancy provided.

System Infrastructure Non-Functional Requirements Related Item List

No.	Major category	Middle category	Minor category	Minor category description	Overlapping item	Important item	Metric	Level						Impact on operation costs	Notes
								0	1	2	3	4	5		
A.2.3.2							Redundancy (components)	Non-redundant design	Redundant design for specific components only	Redundant design for all components					[Level 1] This assumes redundancy for components which make up networking equipment, such as power supplies, CPUs, fans, etc., as needed.
A.2.4.1			Network	Requirements for improving network reliability.			Line redundancy	No redundancy	Partial redundancy	Full redundancy					[Metric] "Line redundancy" refers to providing multiple physical transmission routes (LAN cables, etc.) which make up a network, such that if a failure occurs on one transmission route, transmission is possible through an alternate transmission route. [Level 1] "Partial redundancy" assumes situations such as redundant design for backbone networks only, or segments which carry business data, etc.
A.2.4.2							Route redundancy	No redundancy	Partial redundancy	Full redundancy					[Metric] "Route redundancy" is the setting of multiple data flow sequences (sequences of routers being traversed) among segments which transmit or receive data within the network, such that if a segment experiences a failure, data can be rerouted to an alternate path, and transmission maintained. [Level 1] "Partial redundancy" assumes situations such as redundant design for backbone networks only, or segments which carry business data, etc.
A.2.4.3							Network segmentation	No segmentation	Segmentation for individual sub-systems	Segmentation by purpose					[Level 2] "Purpose" refers to administrative purposes such as monitoring and backups, as well as individual business purposes, such as online or batch processing. It assumes that segmentation is performed for individual sub-systems, and then further by individual purposes.
A.2.5.1			Storage	Requirements to maintain the requested service when a failure occurs on an external storage device, such as a disk array.			Redundancy (equipment)	Non-redundant design	Redundant design for specific equipment only	Redundant design for all equipment					[Metric] Includes NAS and iSCSI devices. However, as NAS and iSCSI are connected via LAN or other networks, NAS, iSCSI, and other similar connection environment fault tolerance measures are included in minor category A.2.4 "Network." [Level 1] "Specific equipment only" assumes that fault tolerance requirements will vary from device to device based on the importance of the data stored on the storage device.
A.2.5.2							Redundancy (components)	Non-redundant design	Redundant design for specific components only	Redundant design for all components					[Level 1] Assumes redundant design for storage device components other than disks (CPUs, power supplies, fans, interfaces, etc.) as needed.
A.2.5.3							Redundancy (disks)	Non-redundant design	Redundancy with RAID5	Redundancy with RAID1					[Level 2] Consider combining with RAID0 in order to satisfy performance requirements.
A.2.6.1			Data	Approach to data protection.	X		Backup method	No backups	Offline backups	Online backups	Offline backups + online backups				[Overlapping Item] C.1.2.7. Backup methods must be taken into consideration during backup operation design, and are an overlapping item shared with "Operability and maintainability." [Level] Offline backups refer to backups performed after shutting down systems (in whole or in part), while online backups refer to backups performed without shutting down systems.
A.2.6.2					X		Data recovery scope	Recovery not necessary	Recover necessary data only	Recover all system data					[Overlapping Item] C.1.2.1. This is an overlapping item, as it is necessary for availability from the perspective of to what degree to maintain data, and for operation from the perspective of up to what point data must be recovered. [Level 1] "Necessary data" refers to the data necessary to satisfy business continuity requirements.
A.2.6.3							Data integrity	No error detection	Error detection only	Error detection & retry	Data integrity guaranteed (Error detection & correction)				[Metric] Physical level guarantee that operations can be correctly carried out on data, that resulting quality levels are sufficient, and that changes to data can be detected, etc. [Level] Implementation includes detection by products and business applications.

System Infrastructure Non-Functional Requirements Related Item List

No.	Major category	Middle category	Minor category	Minor category description	Overlapping item	Important item	Metric	Level						Impact on operation costs	Notes
								0	1	2	3	4	5		
A.3.1.1		Disaster countermeasures	System	Requirements necessary to maintain business continuity in the event of a large-scale disaster such as an earthquake, flood, terrorist attack, fire, etc.			Recovery policy	No recovery	System rebuilding with limited configuration	System rebuilding with same configuration	System with limited configuration built at DR (Disaster Recovery) site	System with same configuration built at DR (Disaster Recovery) site			[Metric] This item specifies what and where replacement equipment is necessary in the event of a large-scale disaster. [Level] The "limited configuration" in levels 1 and 3 refer to system configurations necessary depending on recovery objectives (for example, omitting redundant configuration, etc.). The "same configuration" in levels 2 and 4 refer to the necessity for system configurations identical with the production environment in order to maintain the same service levels after recovery as were offered before. When the "system rebuilding" mentioned in levels 1 and 2 is selected, rebuilding after a disaster should not be thought of as the contract scope, but this item should be considered as a requirement regarding the system rebuilding policy, including using the facilities of the site affected by the disaster, as well as shared centers. On the other hand, the "built at DR site" of levels 3 and 4 includes the construction of recovery systems in specified DR sites.
A.3.2.1			Externally archived data	Requirements concerning archival of data and programs in sites separate from operation sites in preparation for the eventuality of damage due to a large-scale disaster such as an earthquake, flood, terrorist attack, fire, etc.			Level of storage decentralization	No external archival	1 location	1 location (Remote location)	2 locations (Remote locations)				
A.3.2.2							Archival method	Archival on media	Backup on separate storage within same site	Remote backup to DR site					
A.3.3.1			Ancillary facilities	Requirements for system ancillary facilities in response to disasters.			Disaster countermeasure scope	Countermeasures not implemented	Specific countermeasures implemented	All conceivable countermeasures implemented					[Metric] Some disaster countermeasure requirements are specified for ancillary facilities in "System environment and ecology" F.4.1.1 "Earthquake resistance intensity" and F.4.4.4 "Power loss countermeasures." [Level] The following are examples of envisioned disaster countermeasures. • Aseismic measures • Power loss countermeasures • Fire prevention measures • Electric leak countermeasures • Lightning countermeasures • Flooding countermeasures • Electric and magnetic field countermeasures
A.4.1.1		Recoverability	Recovery operations	This level covers work needed for recovery operations in the event of a failure resulting in a business outage.	X		Recovery operations	Recovery not necessary	Manual recovery without using recovery products	Recovery using recovery products	Recovery using recovery products + business applications				[Overlapping Item] C.3.1.1. Recovery operations are included in "Availability" and "Operability and maintainability" as well. In "Operability and maintainability," this is discussed from the perspective of effect on recovery objective operations, while "Availability" looks at the methods used to implement it. [Level] The use of in-house created tools is included in manual recovery. "Recovery products" refer to products for performing backups / recovery. When performing recovery using a recovery product, in some cases, the extent to which recovery is automated (automatic recovery function sufficiency rate, etc.) may be defined, but as the choice to use or not use recovery products results in significant differences, "Availability" level consideration is based on whether or not recovery products are used.
A.4.1.2					X		Alternative business operation scope	None	Alternative business operation required for some businesses	Alternative business operation required for all businesses					[Overlapping Item] C.3.1.2. Recovery operations are included in "Availability" and "Operability and maintainability" as well. In "Operability and maintainability," this is discussed from the perspective of effect on recovery objective operations, while "Availability" looks at the methods used to implement it. [Metric] "Alternative business operation" refers to methods of alternative business (operation by alternate equipment or manual operation) which can be used when a system failure makes recovery impossible.
A.4.2.1			Availability confirmation	Scope of confirmation of availability requirements.		X	Confirmation scope	Not performed, or up to simple failures	Failures which permit business to be continued	Some failures which result in business interruption	All failures which result in business interruption				[Level] Level 2 and 3 confirmation scopes include contents defined in level 1.
B.1.1.1	Performance and scalability	Business processing volume	Business volume during normal operation	Volume of business which have an effect on performance and scalability. Consensus is to be based on envisioned system operation. Instead of selecting a single value for each metric, intended system operation hours, seasonal factors, and the like must also be considered.	X	X	Number of users	Specific users only	Upper limit is fixed	Used by unspecified number of users					[Overlapping Item] F.2.1.1. The "number of users" is essential for deciding performance and scalability, as well as an item for specifying the system environment, so this item is included in both "Performance and scalability" and "System environment and ecology". [Level] Even if the numerical value for this prerequisite cannot be precisely determined, it is important that at least a tentative value, based on similar systems, etc., should be decided on.
B.1.1.2						X	Number of simultaneous users	Access limited to specified users only	Limited number of simultaneous users	Access by unspecified number of users					[Metric] The "number of simultaneous users" refers to the number of users who access the system at any given point.

System Infrastructure Non-Functional Requirements Related Item List

No.	Major category	Middle category	Minor category	Minor category description	Overlapping item	Important item	Metric	Level 0	Level 1	Level 2	Level 3	Level 4	Level 5	Impact on operation costs	Notes
B.1.1.3						X	Data volume	Total data volume is clear	Only primary data volume is clear						[Level 1] "Primary data volume" refers to the data that makes up the majority of the data stored by the system. For example, master tables and temporary storage of main transaction data. When only the volume of primary data has been determined, there is a risk of a need to add disks to handle data which has not been considered.
B.1.1.4						X	Number of online requests	Number of requests is clear for each process	Number of requests is clear for primary processes only						[Metric] The number of online requests is confirmed, clearly specifying the unit time involved. [Level 1] "Primary processes" refer to the online requests received by the system that make up the majority of received requests. For example, resident information system move-in / move-out processing, Internet shopping system transaction processing, etc. When only the number of requests for primary processes has been determined, there is a risk of insufficient server capabilities due to processes which have not been considered.
B.1.1.5						X	Number of batch processes	Number of processes is defined for individual processing units	Number of processes is defined for primary processes						[Metric] The number of batch processes shall be confirmed, clearly specifying the unit time involved. When defining requirements, an estimated number of primary processes (especially processes critical for the server) should have been decided on, and performance and scalability shall be considered based on this estimate. If this number has not been clearly specified when defining requirements, assumed values, including the degree to which they are decided, should be used. [Level 1] "Primary processes" refer to the batch processes which take up the majority of the system's processing time. For example, monthly aggregation processing of a personnel payroll processing system or billing system. When only the number of primary batch processes has been determined, there is a risk of insufficient server capabilities due to processes which have not been considered.
B.1.1.6							Number of business functions	Business functions are organized	A list of confirmed business functions has been created	There is a list of business functions, but have yet to be confirmed					[Metric] When defining requirements, even if there are differences in levels, a business function list should have be decided on, and performance and scalability shall be considered based on this. If this number has not been clearly specified when defining requirements, assumed values, including the degree to which they are decided, should be used.
B.1.2.1			Business volume expansion	Ratio, over the course of the system's lifecycle, from system operation inception to retirement, between the volume of business at the system's launch and its peak. Comparisons between start date average values and later steady state figures can also be used as needed.		X	Expansion rate of number of users	1-fold	1.2-fold	1.5-fold	2-fold	3-fold	10-fold or greater		[Level] The multiplication factor shown for each level is a rough estimate; consensus regarding specific figures is necessary.
B.1.2.2						X	Expansion rate of number of simultaneous users	1-fold	1.2-fold	1.5-fold	2-fold	3-fold	10-fold or greater		[Level] The multiplication factor shown for each level is a rough estimate; consensus regarding specific figures is necessary.
B.1.2.3						X	Expansion rate of data volume	1-fold	1.2-fold	1.5-fold	2-fold	3-fold	10-fold or greater		[Level] The multiplication factor shown for each level is a rough estimate; consensus regarding specific figures is necessary.
B.1.2.4						X	Expansion rate of number of online requests	1-fold	1.2-fold	1.5-fold	2-fold	3-fold	10-fold or greater		[Metric] The number of online requests shall be confirmed, clearly specifying the unit time involved. [Level] The multiplication factor shown for each level is a rough estimate; consensus regarding specific figures is necessary.
B.1.2.5						X	Expansion rate of number of batch processes	1-fold	1.2-fold	1.5-fold	2-fold	3-fold	10-fold or greater		[Metric] The number of batch processes shall be confirmed, clearly specifying the unit time involved. [Level] The multiplication factor shown for each level is a rough estimate; consensus regarding specific figures is necessary.
B.1.2.6							Expansion rate of number of business functions	1-fold	1.2-fold	1.5-fold	2-fold	3-fold	10-fold or greater		[Level] When evaluating the expansion rate of the number of business functions, it is advisable to indicate function granularity (estimated scale and service range of each function, etc.) with concrete numbers. The multiplication factor shown for each level is a rough estimate; consensus regarding specific figures is necessary.
B.1.3.1			Retention period	Period for which data used by the system infrastructure, such as OS or middleware logs, must be retained. Can be specified, as needed, for individual data types. When selecting data to be retained, the scope of the target data must also be defined.		X	Retention period	6 months	1 year	3 years	5 years	10 years or longer	Permanent retention		[Level] When there is multiple data that must be retained, and the retention periods vary, decision must be made for each type of data involved. [Level 0] Use 6 months when data retention period restrictions are short.
B.1.3.2							Scope	Online viewable scope	Includes archives						[Metric] Decide on a location to store the data to be retained. Data lookup may be difficult depending on where the data is stored. Consideration must also be paid to backup methods.

System Infrastructure Non-Functional Requirements Related Item List

No.	Major category	Middle category	Minor category	Minor category description	Overlapping item	Important item	Metric	Level						Impact on operation costs	Notes
								0	1	2	3	4	5		
B.2.1.1		Performance objective	Online response	Response required during online system utilization. Confirm what level of response is necessary based on the business to be handled by the system. Take into account of peak characteristics and operation during failure, and establish adherence rates for normal operation, peak times, and degraded operation. It is advisable to decide on specific numbers for specific functions and systems. (Ex: Web system search/update/viewing related, etc.)		X	Adherence rate of response during normal operation	No defined adherence rate	60%	80%	90%	95%	99% or greater		[Level] When there are specific targets and promised values, specify adherence rates for each process. The adherence rate shown for each level is a rough estimate; consensus must be reached regarding concrete response and adherence rate figures.
B.2.1.2						X	Adherence rate of response during peak times	No defined adherence rate	60%	80%	90%	95%	99% or greater		[Level] When there are specific targets and promised values, specify adherence rates for each process. The adherence rate shown for each level is a rough estimate; consensus must be reached regarding concrete response and adherence rate figures.
B.2.1.3							Adherence rate of response during degraded operation	No degraded operation	60%	80%	90%	95%	99% or greater		[Level] When there are specific targets and promised values, specify adherence rates for each process. The adherence rate shown for each level is a rough estimate; consensus must be reached regarding concrete response and adherence rate figures.
B.2.2.1			Batch response (turnaround time)	Response required during batch system utilization. Confirm what level of response (turnaround time) is necessary based on the business to be handled by the system. It is advisable to take into account peak characteristics and operation during failure, decide on adherence rates for normal operation, peak times, and degraded operation, and establish specific figures for individual functions and systems. (Ex: Daily processes / monthly processes / yearly processes, etc.)		X	Degree of response adherence during normal operation	No defined degree of adherence	Within specified time	Sufficient capacity is reserved to perform re-execution					[Level 1] The "specified time" does not include re-execution.
B.2.2.2						X	Degree of response adherence during peak times	No defined degree of adherence	Within specified time	Sufficient capacity is reserved to perform re-execution					[Level 1] The "specified time" does not include re-execution.
B.2.2.3							Degree of response adherence during degraded operation	No degraded operation	Within specified time	Sufficient capacity is reserved to perform re-execution					[Level 1] The "specified time" does not include re-execution.
B.2.3.1			Online throughput	Throughput required during online system utilization. Confirm what level of throughput is necessary based on the business to be handled by the system. It is advisable to take into account peak characteristics and operation during failure, decide on process margin rates for normal operation, peak times, and degraded operation, and establish specific figures for individual functions and systems. (Ex: Number of data entries / hour, number of Web pages accessed / min, TPS, etc.)			Process margin rate during normal operation	1-fold (No margin)	1.2-fold	1.5-fold	2-fold	3-fold	10-fold or greater		[Level] "Margin rate" refers to the transaction volume the system as a whole can process. For example, for level 3 (2-fold), the system is capable of processing twice the number of transactions. The multiplication factor shown for each level is a rough estimate; consensus regarding specific figures is necessary.
B.2.3.2							Process margin rate during peak times	1-fold (No margin)	1.2-fold	1.5-fold	2-fold	3-fold	10-fold or greater		[Level] "Margin rate" refers to the transaction volume the system as a whole can process. For example, for level 3 (2-fold), the system is capable of processing twice the number of transactions. The multiplication factor shown for each level is a rough estimate; consensus regarding specific figures is necessary.
B.2.3.3							Process margin rate during degraded operation	No degraded operation	Half the processing of normal operation is possible	The processing capability of the system is the same as for normal operation					
B.2.4.1			Batch throughput	Throughput required during batch system utilization. Confirm what level of throughput is necessary based on the business to be handled by the system. Take into account peak characteristics and operation during failure, and establish process margin rates for normal operation, peak times, and degraded operation. It is advisable to decide on specific numbers for specific functions and systems. (Ex: Personnel transfer information batch update processing, batch e-mail transmission processing, etc.)			Process margin rate during normal operation	1-fold (No margin)	1.2-fold	1.5-fold	2-fold	3-fold	10-fold or greater		[Level] The multiplication factor shown for each level is a rough estimate; consensus regarding specific figures is necessary.
B.2.4.2							Process margin rate during peak times	1-fold (No margin)	1.2-fold	1.5-fold	2-fold	3-fold	10-fold or greater		[Level] The multiplication factor shown for each level is a rough estimate; consensus regarding specific figures is necessary.
B.2.4.3							Process margin rate during degraded operation	No degraded operation	Half the processing of normal operation is possible	The processing capability of the system is the same as for normal operation					
B.2.5.1			Form printing capacity	Throughput required for form printing. Confirm what degree of form printing throughput is needed, considering when the printing is performed and the number of forms printed. Take into account peak characteristics and operation during failure, and establish margin rates for normal operation, peak times, and degraded operation. It is advisable to decide on specific numbers for specific functions and forms.			Printing margin rate during normal operation	1-fold (No margin)	1.2-fold	1.5-fold	2-fold	3-fold	10-fold or greater		[Level] The multiplication factor shown for each level is a rough estimate; consensus regarding specific figures is necessary.
B.2.5.2							Printing margin rate during peak times	1-fold (No margin)	1.2-fold	1.5-fold	2-fold	3-fold	10-fold or greater		[Level] The multiplication factor shown for each level is a rough estimate; consensus regarding specific figures is necessary.
B.2.5.3							Printing margin rate during degraded operation	No degraded operation	Half the printing of standard operation is possible	The printing capability of the system is the same as for normal operation					

System Infrastructure Non-Functional Requirements Related Item List

No.	Major category	Middle category	Minor category	Minor category description	Overlapping item	Important item	Metric	Level						Impact on operation costs	Notes
								0	1	2	3	4	5		
B.3.1.1		Resource scalability	CPU scalability	This item is used to confirm CPU scalability. It is based on CPU utilization and the number of open CPU slots when system operation starts. The lower the CPU utilization, the greater its scalability, but also the greater the CPU cost, and resulting waste. CPU addition capacity indicates scalability capacity by checking the presence and quantity of open slots.		X	CPU utilization	80% or greater	Between 50% and 80%	Between 20% and 50%	Less than 20%			X	[Metric] The "CPU utilization" indicates the ratio of CPU usage by running programs per unit time. Figures may vary greatly depending on what unit time is used, and the characteristics of the operating programs. [Level] The utilization ratio shown for each level is a rough estimate; consensus regarding specific figures is necessary. [Impact on Operation Costs] If the CPU utilization is high, measures such as deployment of additional equipment will be necessary for even minor increases of business volume.
B.3.1.2						X	CPU addition capacity	No addition capacity	1 open slot	2 open slots	3 open slots	4 or more open slots		X	[Level] Equipment with CPU addition capacity costs more than equipment with none. [Impact on Operation Costs] For equipment with no CPU addition capacity, additional equipment installation may become necessary.
B.3.2.1			Memory scalability	This item is used to confirm memory scalability. It is based on memory utilization and the number of open memory slots when system operation starts. The lower the memory utilization, the greater its scalability, but also the greater the memory cost, and resulting waste. Memory addition capacity indicates scalability capacity by checking the presence and quantity of open slots.		X	Memory utilization	80% or greater	Between 50% and 80%	Between 20% and 50%	Less than 20%			X	[Metric] "Memory utilization" indicates the ratio of memory usage by running programs per unit time. Figures may vary greatly depending on what unit time is used, and the characteristics of the operating programs. [Level] The utilization ratio shown for each level is a rough estimate; consensus regarding specific figures is necessary. [Impact on Operation Costs] If the memory utilization is high, measures such as deployment of additional equipment will be necessary for even minor increases in business volume.
B.3.2.2						X	Memory addition capacity	No addition capacity	1 open slot	2 open slots	3 open slots	4 or more open slots		X	[Level] Equipment with memory addition capacity costs more than equipment with none. [Impact on Operation Costs] For equipment with no memory addition capacity, additional equipment installation may become necessary.
B.3.3.1			Disk scalability	This item is used to confirm disk scalability. It is based on disk utilization and the number of disk expansion slots when system operation starts. The lower the disk utilization, the greater its scalability, but also the greater the disk cost, and resulting waste. Disk addition capacity indicates scalability capacity by checking the presence and quantity of open slots. Disks are more scalable than CPUs and memory, as external disks can be added when internal disk space becomes insufficient.			Disk utilization	80% or greater	Between 50% and 80%	Between 20% and 50%	Less than 20%			X	[Level] The utilization ratio shown for each level is a rough estimate; consensus regarding specific figures is necessary. [Impact on Operation Costs] When systems run out of disk space, simple addition file monitoring, etc., becomes necessary.
B.3.3.2							Disk addition capacity	No addition capacity	1 open slot	2 open slots	3 open slots	4 or more open slots		X	[Level] Equipment with disk addition capacity costs more than equipment with none. [Impact on Operation Costs] For equipment with no disk addition capacity, the addition of external disks may become necessary.
B.3.4.1			Network	This item relates to the scalability of the network environment used by the system. When using existing networking equipment, it is used to confirm existing network requirements. Please check "B.4.1 Existence of bandwidth guarantee functionality" regarding network bandwidth.			Networking equipment installation scope	None	Single floor LAN	Single site (building) LAN	Connections among multiple sites within the same company (LAN, WAN)	Connections with external sites			
B.3.5.1			Server processing capability enhancement	This item relates to server processing capability enhancement methods. Methods (scale up/scale out) for handling future business volume increases must be considered in advance. Methods must be selected in accordance with system characteristics. Scaling up is the increasing of processing capabilities by replacing servers with new servers with greater processing capabilities. Scaling out is the increasing of processing capabilities by adding more servers with equivalent processing capabilities.			Scale up	No scaling up	Some servers only	Multiple servers					[Level 1] Scaling up is envisioned for application servers in systems with a high ratio of update related processing, such as online transaction processing. [Level 2] This assumes, in addition to level 1, additional DB server scale up.
B.3.5.2							Scale out	No scaling out	Some servers only	Multiple servers					[Level 1] This is envisioned for systems with multiple front end units, such as Web servers and load balancers. [Level 2] This assumes, in addition to level 1, additional back end server scale out.
B.4.1.1		Performance quality assurance	Existence of bandwidth guarantee functionality	Whether or not to deploy functions for assuring network service quality, and, if so, to what degree. Indicates whether a schema is decided regarding transmission delay, packet loss, and bandwidth. Failure to guarantee bandwidths often results in poorer performance.			Bandwidth guarantee establishment	None	Set for individual protocols	Set for individual servers	Validation and guarantee provided for applications, end to end				

System Infrastructure Non-Functional Requirements Related Item List

No.	Major category	Middle category	Minor category	Minor category description	Overlapping item	Important item	Metric	Level						Impact on operation costs	Notes
								0	1	2	3	4	5		
B.4.2.1			Performance testing	Frequency and scope of measurements to test whether performance of the built system is provided and maintained throughout its lifecycle.			Measurement frequency	No measurement performed	Measurement performed when system is built	Measurement can be performed as needed while system is operating	Measurement is performed throughout operation				
B.4.2.2							Confirmation scope	No confirmation performed	Confirmation that target values are satisfied for some functions	Confirmation that target values are satisfied for all functions					
B.4.3.1			Load spike handling	This refers to loads appearing within a short period of time that are far higher than loads experienced during normal operation. These are periods that exceed assumed business volume peaks. These are particularly prevalent on systems such as B2C systems in which the number of clients cannot be limited. As these often exceed system processing capabilities, sorry actions are often configured and used to handle load spikes.			Transaction protection	Transaction protection is not necessary	Function limiting number of simultaneous transactions	Function limiting number of simultaneous transactions, plus sorry action	Installation of separate sorry action server				
C.1.1.1	Operability and maintainability	Normal operation	Operating hours	Hours during which system operates. This refers to the hours during which the system is operated, performing online processing, batch processing, and the like, in order to provide services to users and system administrators.	X	X	Operating hours (normal)	Not specified	During business hours (9:00 to 17:00)	Outage only at night (9:00 to 21:00)	Possible outage for approximately 1 hour (9:00 to 8:00 the next day)	Possible outage for a brief period (9:00 to 8:55 the next day)	Uninterrupted 24 hours		[Overlapping Item] A.1.1.1. "Operating hours (normal)" are an overlapping item, as they also indicate the system's availability implementation level. [Metric] "Operating hours" refers to the time periods when the system is operational, including online and batch processing. [Level] The times in parentheses are examples for each level. They are not to be used as level selection conditions. "Not specified" refers to a system not having specified service hours, and is envisioned essentially for cases where the system is shut down and started up as necessary by users (Ex: Backup systems prepared for failure recovery, development and validation systems, etc.) "During business hours" and "Outage only at night" are envisioned for general business usage, and the times provided as examples should be read as examples only, and modified as appropriate for systems with different operating hours. "Possible outage" refers to time periods where the system may possibly be shut down, not where it must be shut down. "Uninterrupted 24 hours" also includes cases where batch processes must be executed when the system is not involved in online business, and which therefore require that the system not be shut down.
C.1.1.2					X	X	Operating hours (specific days)	Not specified	During business hours (9:00 to 17:00)	Outage only at night (9:00 to 21:00)	Possible outage for approximately 1 hour (9:00 to 8:00 the next day)	Possible outage for a brief period (9:00 to 8:55 the next day)	Uninterrupted 24 hours		[Overlapping Item] A.1.1.2. "Operating hours (specific days)" are an overlapping item, as they also indicate the system's availability implementation level. [Metric] "Specific days" refer to weekends, holidays, the end/start of months, and other days whose schedule is defined as differing from the normal operation schedule. If there are multiple specific days, their level values must be made consistent (Ex: "Monday to Friday is level 2, but Saturday and Sunday are level 0," "Normally, the level is 5, but the system is rebooted on the first of each month, so on that day, the level is 3"). In addition to user holidays, vendor holidays must also be recognized as specific days, and an operation and maintenance structure, etc. must be established accordingly.
C.1.2.1			Backups	Item regarding backups of data used by the system.	X		Data recovery scope	Recovery not necessary	Recover necessary data only	Recover all system data					[Overlapping Item] A.2.6.2. This is an overlapping item, as it is necessary for availability from the perspective of to what degree to maintain data, and for operation from the perspective of up to what point data must be recovered. [Metric] In order to recover a system after a failure, in addition to data backups, system backups of OS and application setting files, etc., may also be necessary. System backup methods and archival methods should be considered at the same time. [Level 1] "Necessary data" refers to the data necessary to satisfy business continuity requirements.
C.1.2.2						X	Possibility of using external data	Possible to use for recovery of all data	Possible to use for recovery of some data	Not possible to use external data					[Metric] "External data" refers to data stored on systems outside the scope of the relevant system (existing systems linked with the system being developed, etc.). Since the importance of system backup design decreases when system data can be recovered from external data, consideration priority and levels can be lowered.

System Infrastructure Non-Functional Requirements Related Item List

No.	Major category	Middle category	Minor category	Minor category description	Overlapping item	Important item	Metric	Level 0	Level 1	Level 2	Level 3	Level 4	Level 5	Impact on operation costs	Notes
C.1.2.3						X	Backup usage scope	No backups	Data loss prevention when failures occur	Recovery from user errors	Long term data storage (archival)				[Level 2] For recovery from user errors, systems have to be able to return processes which, from the system's perspective, have been performed correctly, to their previous state. As such, multiple generations of backups must be managed, and functions such as "Point in Time Recovery" may be necessary.
C.1.2.4						X	Backup automation scope	All steps performed manually	Some steps performed manually (tape replacement and backup initiation command entry)	One step performed manually (tape replacement only)	All steps performed automatically			X	[Metric] Backup operation includes the following steps: • Scheduled job startup • Selection of backup target • Selection of backup media (tape replacement) • File transfer When decentralized storage is performed by transporting media, tape replacement is not included here. [Impact on Operation Costs] Automation of backup operation requires hardware and software investments, resulting in increased deployment costs. However, as backup work does not need to be performed by users during operation, operation costs can be expected to decrease.
C.1.2.5						X	Backup interval	No backups	Random backups performed in situation such as system configuration changes, etc.	Monthly backups	Weekly backups	Daily backups	Synchronous backups		
C.1.2.6						X	Backup retention period	No backups retention	Less than 1 year	3 years	5 years	Fixed period of 10 years or longer	Permanently retained		[Metric] Unlike backup generation management, which is primarily performed from the viewpoint of availability, this item concerns backup data storage periods from the viewpoint of maintaining data integrity.
C.1.2.7					X		Backup method	No backups	Offline backups	Online backups	Offline backups + online backups				[Overlapping Item] A.2.6.1. Backup method includes consideration regarding whether or not system outage is necessary, and as such must take availability into consideration, making it an overlapping item. [Level] "Offline backups" refer to backups performed after shutting down systems (in whole or in part), while "online backups" refer to backups performed without system outages.
C.1.3.1			Operation monitoring	This item concerns monitoring of entire systems, as well as the hardware and software that make them up (including business applications). Security monitoring is not included within this item. It is considered separately in "E.7.1 Fraud monitoring."		X	Monitored information	No monitoring performed	Alive monitoring performed	Error monitoring performed	Error monitoring (including trace information) performed	Resource monitoring performed	Performance monitoring performed	X	[Metric] "Monitoring" refers to collecting information and, in accordance with the results, notifying appropriate parties. The objective of this item is the determination of what information should be issued as monitored information. Confirm where monitored information is sent to under "C.4.5.2 Existence of monitoring system." [Level] "Alive monitoring" refers to monitoring of whether the monitored object's status is online or offline. "Error monitoring" refers to monitoring of logs, etc. output by monitored objects to confirm whether errors have occurred. When "trace information" is included, the monitoring function also determines details such as in which module the error occurred. "Resource monitoring" refers to monitoring of logs output by monitored objects, and separately acquired performance information, and the usage of them to determine resource utilization conditions, such as CPU, memory, disk, and network bandwidth utilization. "Performance monitoring" refers to monitoring of logs output by monitored objects, and separately acquired performance information, and the usage of them to determine business application and disk I/O, network transfer and similar response times, and throughput. [Impact on Operation Costs] Error monitoring, resource monitoring, and performance monitoring make identification of fault points easier, and can assist in preventing faults from occurring, leading to lower operation costs involved in maintaining system quality.
C.1.3.2						X	Monitoring interval	No monitoring performed	Non-regular monitoring (manual monitoring)	Regular monitoring (daily intervals)	Regular monitoring (intervals of several hours)	Real-time monitoring (one minute intervals)	Real-time monitoring (one second intervals)		

System Infrastructure Non-Functional Requirements Related Item List

No.	Major category	Middle category	Minor category	Minor category description	Overlapping item	Important item	Metric	Level						Impact on operation costs	Notes
								0	1	2	3	4	5		
C.1.3.3							System level monitoring	No monitoring performed	Partial monitoring performed	Full monitoring performed					[Metric] "System level monitoring" refers to determining if a system is functioning as a system based on the results of confirming the states of individual servers, etc., which make up the system, including business applications. This includes backup monitoring and job monitoring, etc. [Level] When monitoring is performed, system level related monitoring information and monitoring intervals must be individually confirmed. It is assumed that monitoring will be performed of especially critical functions out of all the functions offered by the system.
C.1.3.4							Process level monitoring	No monitoring performed	Partial monitoring performed	Full monitoring performed					[Metric] "Process level monitoring" refers to determining if processes such as applications and middleware are functioning correctly. It assumes process information (alive state, CPU utilization, memory utilization, etc.) monitoring primarily via OS commands. [Level] When monitoring is performed, process level related monitoring information and monitoring intervals must be individually confirmed. The "partial monitoring" mentioned in level 1 assumes that monitoring will be performed of especially critical processes out of all the processes (applications and middleware) operating on the system.
C.1.3.5							Database level monitoring	No monitoring performed	Partial monitoring performed	Full monitoring performed					[Metric] "Database level monitoring" refers to confirming information provided by DBMS functions, and determining if they are functioning normally. It assumes monitoring of log output contents, parameter values, status information, disk usage ratios, etc. [Level] When monitoring is performed, database level related monitoring information and monitoring intervals must be individually confirmed. The "partial monitoring" mentioned in level 1 assumes that monitoring will be performed of especially critical databases out of all the databases operating on the system.
C.1.3.6							Storage level monitoring	No monitoring performed	Partial monitoring performed	Full monitoring performed					[Metric] "Storage level monitoring" refers to confirming the state of disk arrays and other external storage devices, and determining if they are functioning normally. It assumes monitoring of disk utilization ratios, etc., confirmed via OS commands, and log information, etc., output by firmware. [Level] When monitoring is performed, storage level related monitoring information and monitoring intervals must be individually confirmed. The "partial monitoring" mentioned in level 1 assumes that monitoring will be performed of especially critical storage devices out of all the storage devices connected to the system.
C.1.3.7							Server (node) level monitoring	No monitoring performed	Partial monitoring performed	Full monitoring performed					[Metric] "Server (node) level monitoring" refers to determining if the monitored server is functioning correctly at the OS level. This includes heartbeat monitoring, etc. [Level] When monitoring is performed, server (node) level related monitoring information and monitoring intervals must be individually confirmed. The "partial monitoring" mentioned in level 1 assumes that monitoring will be performed of especially critical servers out of all the servers (nodes) which make up the system.
C.1.3.8							Terminal/networking equipment level monitoring	No monitoring performed	Partial monitoring performed	Full monitoring performed					[Metric] "Terminal/networking equipment level monitoring" refers to confirming the state of client terminals, routers, and other networking equipment, and determining if they are functioning normally. It assumes both heartbeat monitoring and monitoring based on the information output by individual firmware, etc. [Level] When monitoring is performed, terminal/networking equipment level related monitoring information and monitoring intervals must be individually confirmed. The "partial monitoring" mentioned in level 1 assumes that monitoring will be performed of especially critical terminals/networking equipment out of all the terminals/networking equipment which make up the system.
C.1.3.9							Network/packet level monitoring	No monitoring performed	Partial monitoring performed	Full monitoring performed					[Metric] "Network/packet level monitoring" refers to confirming information contained in packets passing through the network, and determining if the network is functioning normally. It assumes monitoring of packet loss, network bandwidth utilization, and the like. [Level] When monitoring is performed, terminal/packet level related monitoring information and monitoring intervals must be individually confirmed. The "partial monitoring" mentioned in level 1 assumes that monitoring will be performed of especially critical network paths out of all the network paths which make up the system.

System Infrastructure Non-Functional Requirements Related Item List

No.	Major category	Middle category	Minor category	Minor category description	Overlapping item	Important item	Metric	Level						Impact on operation costs	Notes
								0	1	2	3	4	5		
C.1.4.1			Time synchronization	This item concerns time synchronization for the equipment that makes up the system.			Time synchronization scope	Time synchronization is not performed	Time synchronization is performed for servers only	Time synchronization is performed for both servers and client equipment	Time synchronization is performed throughout the system, including networking equipment	The entire system's time is synchronized with external standard time		X	[Level 4] When the entire system is synchronized with external standard time, system design must include what to do about internal system time synchronization when a failure occurs which affects the system's external connection. [Impact on Operation Costs] Because time synchronization ensures that the order of logs output by multiple server devices can be accurately determined, it can reduce the operation costs of fault investigation, auditing, etc.
C.2.1.1		Maintenance operation	Planned system shutdown	This item concerns planned service outages performed in order to carry out system maintenance operations, such as inspections, region expansion, defragmentation, master data maintenance, and the like.	X	X	Existence of planned system shutdown	Possible planned system shutdown (operation schedule can be changed)	Possible planned system shutdown (operation schedule cannot be changed)	No planned system shutdown				X	[Overlapping Item] A.1.1.3. "Existence of planned system shutdown" is an overlapping item, as it also indicates the system's availability implementation level. [Impact on Operation Costs] When there are planned system shutdown, operational costs may increase due to pre-shutdown backups and the preparation of procedures in accordance with the system configuration.
C.2.1.2							Advance announcement of planned system shutdown	No planned system shutdown performed	planned system shutdown are determined by annual plans	Notification 1 month in advance	Notification 1 week in advance	Notification 1 day in advance		X	[Impact on Operation Costs] When there are planned system shutdown, irregular handling, such as announcement to users and operation schedule changes, etc, may occur. The less time there is to carry these out, the more critical the need to carefully design system exception processing, resulting in higher deployment costs. However, due to this design work, exception processing operation itself will be simplified, resulting in expected lower operation costs.
C.2.2.1			Operation load reduction	This item relates to maintenance operation related work load reduction design.		X	Maintenance work automation scope	All maintenance work is performed manually	Some maintenance work is automated	All maintenance work is automated				X	[Metric] "Maintenance work" refers to the work performed in order to maintain and manage the system infrastructure together with maintenance operation, and is assumed to incorporate update work such as inspection work and patch application work, etc., region expansion, defragmentation, log rotation, and the like. It does not include fault handling or recovery operations. [Impact on Operation Costs] Automating system infrastructure maintenance operation work requires the installation of special operation management tools and a great deal of front end work. This will result in greater deployment costs, but, thanks to maintenance operation work performed by users becoming simpler, or even unnecessary, operation costs will fall.
C.2.2.2							Server software update work automation	Server software update file distribution functionality will not be provided	Server software update file distribution functionality will be provided, with distribution and updating performed manually	Server software update file distribution functionality will be provided, with distribution performed automatically and updating performed manually	Server software update file distribution functionality will be provided, with distribution and updating performed automatically			X	[Metric] Server software refers to server equipment OS and storage firmware, as well as middleware and applications which run on server equipment. [Impact on Operation Costs] Automating the distribution of update files to servers, and installation of those updates, requires the installation of special tools and a great deal of front end work. However, if server software update work is automated, this will decrease the amount of work which must be performed by users during system operation, resulting in reduced operating costs.
C.2.2.3							Terminal software update work automation	Terminal software update file distribution functionality will not be provided	Terminal software update file distribution functionality will be provided, with distribution and updating performed manually	Terminal software update file distribution functionality will be provided, with distribution performed automatically and updating performed manually	Terminal software update file distribution functionality will be provided, with distribution and updating performed automatically			X	[Metric] Terminal software refers to client terminal OS and networking equipment firmware, as well as applications which run on client terminals. [Impact on Operation Costs] Automating the distribution of update files to terminals, and installation of those updates, requires the installation of special tools and a great deal of front end work. However, if terminal software update work is automated, this will decrease the amount of work which must be performed by users during system operation, resulting in reduced operating costs.
C.2.3.1			Patch application policy	This item relates to patch information deployment and patch application policies.			Patch release information provision	Patch release information is provided by vendor when requested by users	Patch release information is regularly provided by vendor to users	Patch release information is provided in real-time (when patch is released) by vendor to users					
C.2.3.2							Patch application policy	Patches are not applied	Only recommended patches are applied	All patches are applied					[Metric] When the selected level varies depending on whether patches are individual patches or cumulative patches, consensus must be reached for each. Security patches are also considered in the "Security" item (E.4.3.2).

System Infrastructure Non-Functional Requirements Related Item List

No.	Major category	Middle category	Minor category	Minor category description	Overlapping item	Important item	Metric	Level						Impact on operation costs	Notes
								0	1	2	3	4	5		
C.2.3.3							Patch application timing	Patches are not applied	Patches are applied when faults occur	Patches are applied during scheduled maintenance	Patches are applied when new patches are released				[Metric] When the selected level varies depending on whether patches are individual patches or cumulative patches, consensus must be reached for each. Security patches are also considered in the "Security" item (E.4.3.3).
C.2.3.4							Performance of patch validation	Patch validation is not implemented	Patch validation is only performed for recovery patches	Patch validation is performed for both recovery patches and security patches					
C.2.4.1			Maintenance during operation	Scope of components for which maintenance during operation can be performed without stopping the system.			Scope of hardware maintenance during operation	No maintenance during operation	Maintenance during operation for some hardware	Maintenance during operation for all hardware					[Metric] "Hardware maintenance during operation" refers to maintenance work which is performed without stopping the system, such as hardware replacement or firmware updating. [Level 1] "Some hardware" refers to cases where maintenance during operation is only possible for specific servers or storage devices.
C.2.4.2							Scope of software maintenance during operation	No maintenance during operation	Maintenance during operation for some software	Maintenance during operation for all software					[Metric] "Software maintenance during operation" refers to OS, middleware, and application patch application which is performed without stopping the system (ex: multiserver environment rolling upgrades, etc.). [Level 1] "Some software" refers to cases where maintenance during operation is only possible for specific software.
C.2.5.1			Scheduled maintenance frequency	Frequency of scheduled maintenance work on hardware or software as necessary for system maintenance.			Scheduled maintenance frequency	Scheduled maintenance not implemented	Once / year	Once / 6 months	Once / month	Once / week	Daily		
C.2.6.1			Preventive maintenance	Detection of potential system component and material faults, and taking of corrective action, such as replacement.			Preventive maintenance	No preventative maintenance	Handling of potential problems detected during scheduled maintenance	Detection of potential problems, and handling of said problems, at regular intervals (separate from scheduled maintenance)	Real-time detection and correction of potential problems				
C.3.1.1		Operation to ensure business continuity	Recovery operations	This level covers work needed for recovery operations in the event of a failure resulting in a business outage.	X		Recovery operations	Recovery not necessary	Manual recovery without using recovery products	Recovery using recovery products	Recovery using recovery products + business applications				[Overlapping Item] A.4.1.1. "Recovery operations" is essential for considering "Availability" recovery objectives (RTO/RPO), and as such is included in "Availability" and "Operability and maintainability." [Metric] User and vendor side organizational structure and authorities must be organized and prepared in accordance with selected levels. [Level] The use of in-house created tools is included in manual recovery. "Recovery products" refer to products for performing backups / recovery. When performing recovery using a recovery product, in some cases, the extent to which recovery is automated (automatic recovery function sufficiency rate, etc.) may be defined, but as the choice to use or not use recovery products results in significant differences, "Availability" level consideration is based on whether or not recovery products are used.
C.3.1.2					X		Alternative operation scope	None	Alternative operation required for some businesses	Alternative operation required for all businesses					[Overlapping Item] A.4.1.2. "Alternative operation scope" is essential for considering "Availability" recovery objectives (RTO/RPO), and as such is included in "Availability" and "Operability and maintainability." [Metric] "Alternative operation" refers to methods of alternative business (operation by alternate equipment or manual operation) which can be used when a system failure makes recovery impossible.
C.3.2.1			Fault recovery automation scope	This item relates to the scope of automation of fault recovery related operations.			Fault recovery automation scope	All fault recovery work is performed manually	Fault recovery work partly automated	Fault recovery work fully automated				X	[Level 1] "Fault recovery work partly automated" refers to cases where specific patterns (or positions) of fault recovery are automated. [Impact on Operation Costs] Automating fault recovery operations requires the creation of scripts for performing complex decisions based on individual fault patterns, making development costs correspondingly more expensive. On the other hand, recovery operations in the event of a fault are speeded, and the accompanying reduction in mistakes results in reduced operation costs.

System Infrastructure Non-Functional Requirements Related Item List

No.	Major category	Middle category	Minor category	Minor category description	Overlapping item	Important item	Metric	Level						Impact on operation costs	Notes
								0	1	2	3	4	5		
C.3.3.1			System fault detection handling	This item concerns vendor support when a system fault is detected.			Support hours	Support offered during vendor business hours (ex: 09:00 to 17:00)	Support offered during hours specified by user (ex: 18:00 to 24:00)	24 hour support					[Metric] Time period when maintenance staff provide support when system faults are detected.
C.3.3.2							On-site arrival time	No on-site dispatch	Maintenance staff arrive within days of fault detection	Maintenance staff arrive user business day after fault is detected	Maintenance staff arrive before start of next user business day after fault is detected	Maintenance staff arrive within hours of fault detection	Maintenance staff stationed on-site		[Metric] Time between when fault is detected and notification is provided to specified contact point, and when maintenance staff receive fault notification and arrive on-site.
C.3.3.3							Average SE on-site arrival time	No SE on-site dispatch	SE arrives within days of fault detection	SE arrives user business day after fault is detected	SE arrives before start of next user business day after fault is detected	SE arrives within hours of fault detection	SE stationed on-site		[Metric] Average time between system fault detection and SE on-site arrival.
C.3.4.1			Securing of replacement materials	Method of securing replacement materials for failed components.			Maintenance part securement level	Not secured	Based on maintenance contract, parts procurement vendor maintains maintenance parts for a specified number of years	Based on maintenance contract, maintenance vendor maintains maintenance parts for a specified number of years expressly for the system					[Metric] Maintenance part securement level for the system.
C.3.4.2							Availability of backup equipment	No backup equipment	Backups for some equipment	Backups for all equipment					
C.4.1.1		Operating environment	Establishment of development environment	This item relates to the environment that is deployed for the purposes of system development work by the user.		X	Presence of development environment	No system development environment established	Establish development environment limited to part of operating environment	Establish development environment identical to operating environment					[Metric] "Development environment" refers to a system of devices, separate from the production environment, that is expressly for development use. Development phase environments which will be used as production environments after the system is launched are not included in this item. [Level] Select level 0, "No system development environment established" for situations where a development environment is used during the development phase, but upon system launch, the environment is becomes the production environment.
C.4.2.1			Establishment of test environment	This item relates to the environment that is deployed for the purposes of system testing by the user.		X	Presence of test environment	No system test environment established	Establish together with system development environment	Establish dedicated test environment					[Metric] "Test environment" refers to a system of devices, separate from the production environment, that is expressly for testing. Test phase environments which will be used as production environments after the system is launched are not included in this item. [Level] Select level 0, "No system test environment established" for situations where a test environment is used during the test phase, but upon system launch, the environment is becomes the production environment.
C.4.3.1			Manual preparation level	Level of operation manual preparation		X	Manual preparation level	Standard manuals of each product are used	A normal operation system manual is provided	A normal operation system manual and maintenance operation system manual are provided	A manual customized in accordance with user system operation rules is provided			X	[Level] The normal operation manual contains explanations of standard system infrastructure operation (startup, shutdown, etc.) and functions. The maintenance operation manual contains explanations of system infrastructure maintenance work operations (part replacement, data recovery procedures, etc.) and functions. First-line support related contents (system switchover work, log acquisition procedure, etc.) related to failures are included in the normal operation manual. Information about recovering from backups is contained in the maintenance manual. [Impact on Operation Costs] The creation of manuals customized in accordance with user operation increases deployment costs, but speed up user reference during operation, resulting in reduced operation costs.

System Infrastructure Non-Functional Requirements Related Item List

No.	Major category	Middle category	Minor category	Minor category description	Overlapping item	Important item	Metric	Level						Impact on operation costs	Notes
								0	1	2	3	4	5		
C.4.4.1			Remote operation	This item defines whether or not it is possible to perform monitoring and operation via the network from an environment separated from the system installation environment.		X	Remote monitoring site	No remote monitoring performed	Remote monitoring performed via campus LAN	Remote monitoring performed from remote location				X	[Level] Monitored contents must be confirmed in the corresponding C.1.3.1 "Operation monitoring." [Impact on Operation Costs] Implementing remote monitoring requires special hardware and software deployment, resulting in higher deployment costs. However, with remote monitoring, there is no need for system administrators to physically go to where the servers are installed to check operations, resulting in lowered operation costs.
C.4.4.2						X	Remote operation scope	No remote operation performed	Only routine processes are performed from remote	Unspecified processes are performed from remote				X	[Metric] Consider the scope of operations which can be carried out from a remote monitoring site. [Level] Software to perform remote routine processes is inexpensive, while allowing unspecified remote operation results in the need to consider security and other additional aspects, so the level is higher for unspecified remote operation than routine processes. [Impact on Operation Costs] Implementing remote operation requires special hardware and software deployment, resulting in higher deployment costs. However, with remote operation, there is no need for system administrators to physically go to where the servers are installed to perform maintenance operations, resulting in lowered operation costs.
C.4.5.1			External system connection	This item relates to whether or not the system is connected to an external system which affects system operation.		X	Existence of external system connections	No connections with external systems	Connected to external systems inside the company	Connected to external systems outside the company					[Metric] If connecting to external connections, check their interfaces.
C.4.5.2							Existence of monitoring system	No monitoring system	Connected to existing monitoring system	Connected to new monitoring system					[Level 2] "Connected to new monitoring system" refers to situations where construction of a new monitoring functionality for the system is included in the requirements definition scope.
C.4.5.3							Existence of job management system	No job management system	Connected to existing job management system	Connected to new job management system					[Level 2] "Connected to new job management system" refers to situations where construction of a new job management functionality for the system is included in the requirement definition scope.
C.5.1.1		Support structure	Maintenance contract (hardware)	Scope of hardware requiring maintenance.		X	Maintenance contract (hardware) scope	No maintenance contract	Maintenance contract with each vendor for its own products (hardware) only	Multivendor support contract (some exceptions allowed)	Multivendor support contract (extending to all products which make up system)			X	[Level] "Maintenance contract with each vendor for its own products (hardware) only" refers to the establishment of support contracts with individual vendors who supply the products that make up the system, to provide support service for only said products. "Multivendor support contract" refers to the establishment of a support contract with a vendor who supplies support service for the entire system, and serves as a one-stop support contact for any issues affecting the system, which is made up of products produced by multiple vendors. [Impact on Operation Costs] Support contracts may appear to cause operating costs to rise, but as the costs involved in handling problems when they arise can be significant, support contracts may actually result in lower operating expenses.
C.5.2.1			Maintenance contract (software)	Scope of software requiring maintenance.		X	Maintenance contract (software) scope	No maintenance contract	Maintenance contract with each vendor for its own products (software) only	Multivendor support contract (some exceptions allowed)	Multivendor support contract (extending to all products which make up system)			X	[Level] "Maintenance contract with each vendor for its own products (software) only" refers to the establishment of support contracts with individual vendors who supply the products that make up the system, to provide support service for only said products. "Multivendor support contract" refers to the establishment of a support contract with a vendor who supplies support service for the entire system, and serves as a one-stop support contact for any issues affecting the system, which is made up of products produced by multiple vendors. [Impact on Operation Costs] Support contracts may appear to cause operating costs to rise, but as the costs involved in handling problems when they arise can be significant, support contracts may actually result in lower operating expenses.
C.5.3.1			Lifecycle period	The operation maintenance support period, and the actual system operation lifecycle period.		X	Lifecycle period	3 years	5 years	7 years	10 years or longer				[Metric] "Lifecycle period" here refers to the defined period until the next system renewal. When the lifecycle is longer than the available maintenance periods of the individual products, maintenance extension, upgrades to maintainable versions, etc., are required.
C.5.4.1			Division of maintenance work roles	This item relates to the division of vendor / user roles regarding maintenance operations, and the number of assigned personnel.			Division of maintenance work roles	Performed entirely by users	Performed partially by users	Performed entirely by vendor					
C.5.5.1			Division of first-line support roles	This item relates to the division of vendor / user roles regarding first-line support, first-line support time, and the number of assigned personnel.			Division of first-line support roles	Performed entirely by users	Performed partially by users	Performed entirely by vendor					

System Infrastructure Non-Functional Requirements Related Item List

No.	Major category	Middle category	Minor category	Minor category description	Overlapping item	Important item	Metric	Level						Impact on operation costs	Notes
								0	1	2	3	4	5		
C.5.6.1			Support personnel	This item relates to the number of personnel that make up the support structure, support time, and skill levels.			Number of vendor side stationed assigned personnel	None stationed	1 person	Multiple people					
C.5.6.2							Vendor side support time slots	No support	During vendor business hours (09:00 to 17:00)	Support available except at night (09:00 - 21:00)	Support not offered for approximately 1 hour per day due to handover (09:00 - 08:00 the next day)	24 hour support			
C.5.6.3							Vendor side support personnel required skill level	Not specified	Able to operate equipment under direction of an expert	Able to understand the system configuration, and acquire and check logs	Well-versed in system operation and maintenance procedures, and capable of performing hardware and software maintenance	Involved in system development and/or construction, and is well-versed in business requirements and user situation			
C.5.6.4							Escalation handling	Not specified	On-call standby	Hub standby	On-site standby				[Metric] Confirm the expert personnel standby system at escalation point for ISV / IHV products which require escalation in the event of a failure.
C.5.7.1			Deployment support	Whether or not there is special support for system deployment, and, if so, for how long.			Deployment support period for system test operation	None	Same day only	1 week or less	1 month or less	1 month or more			
C.5.7.2							Deployment support period for system entering production operation	None	Same day only	1 week or less	1 month or less	1 month or more			
C.5.8.1			Operation training	This item relates to the implementation of operation training.			Division of roles for operation training implementation	Not performed	Performed entirely by users	Performed partially by users	Performed entirely by vendor				
C.5.8.2							Operation training scope	Not performed	Normal operation training performed	Normal operation training and maintenance operation training performed	Normal operation, maintenance operation, and failure recovery operation training performed				[Level] "Normal operation" refers to normal system infrastructure operation (startup, shutdown, etc.). "Maintenance operation" refers to system infrastructure maintenance work operations (part replacement, data recovery procedures, etc.).
C.5.8.3							Implementation frequency of operation training	Not performed	Only at system launch period	Held regularly					
C.5.9.1			Regular reporting meetings	Whether or not regular reporting meetings are held to report on maintenance.			Implementation frequency of regular reporting meetings	None	Once / year	Once / 6 months	Once / 3 months	Once / month	Once / week or more		[Metric] Non-regular reporting meetings that are held when failures occur are not included in this metric.
C.5.9.2							Report content level	None	Failure reporting only	Failure reporting and operation condition reporting	Failure reporting, operation condition reporting, and improvement proposals				

System Infrastructure Non-Functional Requirements Related Item List

No.	Major category	Middle category	Minor category	Minor category description	Overlapping item	Important item	Metric	Level						Impact on operation costs	Notes
								0	1	2	3	4	5		
C.6.1.1		Other operation management policies	Internal control support	This item relates to whether or not to perform internal control support for IT operation process.		X	Existence of Internal control support implementation	Internal control support is not specified	Internal control support is performed in accordance with existing company regulations.	New regulations are established, and internal control support is performed in accordance with them.					[Metric] This item confirms whether internal control support will be performed. After confirming whether or not internal control support will be performed, clarify specific support methods (whether control would be carried out during operation, or by implementing functions in the system, etc.).
C.6.2.1			Service desk	This item relates to whether or not there will be a service desk function which serves as a single point for user contact.		X	Presence of service desk	Service desk establishment not specified	Existing service desk will be used	New service desk will be established					[Metric] This item confirms whether or not a service desk will be established for communications between users and the vendor. After confirming whether or not a service desk function will be provided, clarify specific implementation methods.
C.6.3.1			Incident management	This item relates to whether or not rapid recovery processes are implemented for incidents which result in business outages.			Incident management implementation	Incident management not specified	Incident management will be performed in accordance with existing incident management process	New incident management process will be established					[Metric] This item confirms whether or not incidents which occur within the system are managed. After confirming whether or not incident management will be performed, clarify specific implementation methods.
C.6.4.1			Problem management	This item relates to whether or not incident root cause will be tracked down, and, when possible, processes will be carried out to eliminate said root causes.			Problem management implementation	Problem management not specified	Problem management will be performed in accordance with existing problem management process	New problem management process will be established					[Metric] This item confirms whether or not problem management will be carried out to identify the root causes of incidents. After confirming whether or not problem management will be performed, clarify specific implementation methods.
C.6.5.1			Configuration management	This item relates to whether processes will be carried out to appropriately manage IT environment configuration, such as hardware and software.			Configuration management implementation	Configuration management not specified	Configuration management will be performed in accordance with existing configuration management process	New configuration management process will be established					[Metric] This item confirms whether or not configuration management will be performed to manage to make sure released hardware and software is configured appropriately within the user environment. After confirming whether or not configuration management will be performed, clarify specific implementation methods.
C.6.6.1			Change management	This item relates to whether processes will be carried out to efficiently manage IT environment changes.			Change management implementation	Change management not specified	Change management will be performed in accordance with existing change management process	New change management process will be established					[Metric] This item confirms whether or not change management will be performed to manage system environment changes such as hardware replacement, software patch application, version upgrades, and parameter changes. After confirming whether or not change management will be performed, clarify specific implementation methods.
C.6.7.1			Release management	This item relates to whether or not release management will be performed for software, hardware, and IT service deployment.			Release management implementation	Release management not specified	Release management will be performed in accordance with existing release management process	New release management process will be established					[Metric] This item confirms whether or not release management will be implemented to manage whether authorized changes are correctly made to the system environment. After confirming whether or not release management will be performed, clarify specific implementation methods.
D.1.1.1	Migratability	Migration period	Migration schedule	The system migration period from migration work planning to the start of operation, dates/times for system outages, whether or not parallel operation will be performed. (Including rollback time for exceptional circumstance, pre-migration backup work, etc.)		X	System migration period	No system migration	Less than 3 months	Less than 6 months	Less than 1 year	Less than 2 years	2 years or longer		
D.1.1.2						X	Days/times when system outages are possible	No limitations (System can be shut down for as long as needed)	5 days or more	Less than 5 days	1 day (Using scheduled system outage day)	During low usage times (night, etc.)	System outage for system migration is not allowed		[Metric] For some systems, it may not be possible to secure continuous days or time slots for system outage. (For example, 1 full day, followed by a day where the system can only be shut down at night, followed by a scheduled system outage day, when the system can be shut down for a full day.) When this is the case, confirm both days and time slots available for system outage. [Level] Level 0 indicates that the system can be shut down for as long as needed for migration, regardless of system limitations. Levels 1 and over indicate the days/times when system outages are possible, given system outage (business, etc.) related limitations. The higher the level, the greater the effect of system limitations on migration plans, such as days/times when the system can be shut down for migration.
D.1.1.3						X	Existence of parallel operation	None	Yes						[Level 1] When parallel operation is used, specify the period, location, etc. F.4.2.3 and F.4.4.3 are related items.
D.2.1.1		Migration scheme	System deployment scheme	To what degree multi-step deployment schemes are used in system migration and new deployments.		X	Number of steps for site deployment	No regulations, as there is only 1 site	Simultaneous deployment	Less than 5 steps	Less than 10 steps	Less than 20 steps	20 steps or more		[Level] Depending on site deployment risks, the difficulty may be reversed, with simultaneous deployment being the most difficult. Consider deployment risks of the system for each site and determine the number of steps for site migration.

System Infrastructure Non-Functional Requirements Related Item List

No.	Major category	Middle category	Minor category	Minor category description	Overlapping item	Important item	Metric	Level						Impact on operation costs	Notes
								0	1	2	3	4	5		
D.2.1.2						X	Number of steps for business deployment	No regulations, as there is only 1 business	Simultaneous deployment for all businesses	Less than 4 steps	Less than 6 steps	Less than 10 steps	10 steps or more		[Level] Depending on business deployment risks, the difficulty may be reversed, with simultaneous deployment being the most difficult. Consider deployment risks of the system for each business and determine the number of steps for business deployment.
D.3.1.1		Migration scope (equipment)	Equipment to be replaced	Which equipment used in the system before migration will be replaced with new equipment in the new system.		X	Equipment / device migration contents	Nothing in migration scope	Hardware replacement of equipment / devices in migration scope	Hardware, OS, and middleware replacement of equipment / devices in migration scope	Total system replacement of equipment / devices in migration scope	Total system replacement and integration of equipment / devices in migration scope			[Level] Reach consensus for each piece of equipment when there are multiple pieces of equipment within the migration scope, and migration contents vary for each.
D.4.1.1		Migration scope (data)	Migration data volume	The amount of business data which must be migrated (including programs) from the old system.		X	Migration data volume	Nothing in migration scope	Less than 1TB	Less than 1PB	1PB or more				
D.4.1.2						X	Migration data format	Nothing in migration scope	Same format as migration destination	Different format than migration destination					[Metric] "Data format" refers to data format patterns which must be considered during new system migration, such as application dependant formats, table formats, and character codes. [Level] When there are multiple migration data format patterns, perform data format confirmation for each.
D.4.2.1			Migration media	The volume of media to be migrated, and the number of media types needed for migration.			Volume of migration media	Nothing in migration scope	Less than 10 (Less than 1TB)	Less than 1000 (Less than 1PB)	1000 or more (1PB or more)				
D.4.2.2							Number of migration data media types	Nothing in migration scope	1 type	2 types	3 types	4 types	5 types or more		[Metric] The total number of types of media which must be used during migration (ex: tapes, disks, paper forms, etc.). Data transfer via network connection shall also be included as a media type.
D.4.3.1			Converted objects (DB, etc.)	Volume of data to undergo conversion, and difficulty of data conversion tool(s) (number of conversion rules).			Volume of data to be converted	No data to be converted	Less than 1TB	Less than 1PB	1PB or more				
D.4.3.2							Difficulty of migration tool(s) (number of conversion rules)	Migration tool(s) unnecessary or Support offered by existing migration tool(s)	Migration tool(s) with less than 10 conversion rules	Migration tool(s) with less than 50 conversion rules	Migration tool(s) with less than 100 conversion rules	Migration tool(s) with 100 or more conversion rules			
D.5.1.1		Migration plans	Migration work division	Division of migration work.			Division of migration work between user and vendor	Performed entirely by user	Performed by user and vendor together	Performed entirely by vendor					[Metric] Final migration result should be confirmed by the user, regardless of the selected level. It is advisable to conclude security arrangements between the user and vendor regarding the handling of user data. Please check "F.1.1.1 System construction restrictions" for specific contents. [Level 1] When performing migration work together, the division of operations by the user and vendor must be specified. This is especially true for data to be migrated, as specifications must be established regarding the division of duties involved in old system migration scope data investigation, selection and conversion of migration data, entry of data into the production system, data confirmation, and the like.
D.5.2.1			Rehearsal	Migration rehearsal (including rehearsal of handling failures during migration).			Rehearsal scope	No rehearsal	Main problem-free migration cases only	All problem-free migration cases	Problem-free migration cases + abnormal cases requiring rollback to pre-migration state	Problem-free migration cases + abnormal cases requiring recovery from system failure			
D.5.2.2							Rehearsal environment	No rehearsal	Production data is usable	Production data is not usable					[Level] Security risks, etc. such as information leakage due to using production data shall be determined in "F.1.1.1 System construction restrictions." This item is limited to the rehearsal environment.
D.5.2.3							Number of rehearsals	No rehearsal	1 time	2 times	3 times	4 times	5 times or more		
D.5.2.4							Joint rehearsal with external entities	None	Yes (No external connection specification changes)	Yes (With external connection specification changes)					[Metric] When connection specifications for external systems are changed, support may be offered in the new system for both old and new connection specifications in order to reduce system migration risks. When this is the case, a joint rehearsal with external entities must be scheduled to confirm both connection specifications. [Level] When joint rehearsals with external entities are performed, the external system with which the rehearsal are performed as well as the scope of the rehearsals, environment, and number of rehearsals must be specified.

System Infrastructure Non-Functional Requirements Related Item List

No.	Major category	Middle category	Minor category	Minor category description	Overlapping item	Important item	Metric	Level						Impact on operation costs	Notes
								0	1	2	3	4	5		
D.5.3.1			Problem handling	Contents of support structure, support plans, etc., for problems occur during migration.			Existence of problem handling specifications	Not specified	Only support structure specified	Support structure and support plan specified					[Level] When problem handling specifications are in place, confirm the specification contents of the support structure and support plan.
E.1.1.1	Security	Prerequisites / restrictions	Information security related compliance	This item is for confirming whether or not there are information security related organizational policies, rules, laws, guidelines, etc., which must be observed by users. In the event that there are rules, etc to be observed, measures must be considered to ensure that there are no conflicts with said regulations, etc. Ex) • Information security policy • Act Concerning the Prohibition of Unauthorized Computer Access • Personal Information Protection Law • Electronic Signature Law • Provider Responsibility Law • Act on Regulation of Transmission of Specified Electronic Mail • Sarbanes-Oxley Act • Basic Law for Building an Advanced Info-Communications Network • ISO/IEC27000 series • Standards for Information Security Measures for the Central Government Computer Systems • FISMA • FISC • PCI DSS • PrivacyMark System • TRUSTe Etc. (* The above examples are mainly Japanese laws, systems, etc.)		X	Existence of applicable company regulations, rules, laws, guidelines, etc.	None	Yes					[Metric] Regulations, laws, guidelines, etc., must be confirmed, and decide security related non-functional requirement item levels in accordance with them.
E.2.1.1		Security risk analysis	Security risk analysis	This item confirms the policy regarding the scope of system threat identification and impact analysis for the developed system. In order to establish an appropriate scope, it is necessary to identify assets, confirm data lifecycles, etc. The scope of countermeasures for identified threats must also be considered.		X	Risk analysis scope	No analysis	Scope which includes highly important assets, and external connection related areas	Development scope					[Level 1] "External connection related areas" refer to external connections to the Internet, connections to media, etc., used for carrying information and data outside the system, and areas which handle data transactions with external systems. The same meaning is used for all levels.
E.3.1.1		Security diagnostics	Security diagnostics	This item is used to confirm whether or not specialized security testing and inspection will be performed for the system and individual documents (design documentation, environment definition documents, implemented software source code, etc.)		X	Existence of network diagnostics implementation	None	Yes						[Metric] "Network diagnostics" refer to diagnosis, in a broad sense, of the system. Network diagnostics include visual confirmation of settings, as well as diagnoses of vulnerabilities by performing simulated attacks (penetration testing).
E.3.1.2						X	Existence of Web site diagnostics implementation	None	Yes						[Metric] "Web site diagnostics" refers to security diagnostics of Web servers and Web applications performed on Web sites.
E.3.1.3							Existence of database diagnostics implementation	None	Yes						[Metric] "Database diagnostics" refers to security diagnostics performed on database systems.
E.4.1.1		Security risk management	Security risk review	This item is for confirming the scope of identifying newly discovered threats affecting the system after starting the operation, as well as analysis of their impact. This includes investigation etc. of security holes, vulnerabilities, and new threats.			Security risk review frequency	None	Performed when security related events occur (as needed)	Performed when security related events occur (as needed) + Performed regularly					[Level] "Performed when security related events occur" refers to when information security related incidents, such as virus infection, unauthorized access, DoS attacks, information leaks, and the like occur.
E.4.1.2							Security risk review scope	No analysis	Scope which includes highly important assets, and external connection related areas	Entire system					

System Infrastructure Non-Functional Requirements Related Item List

No.	Major category	Middle category	Minor category	Minor category description	Overlapping item	Important item	Metric	Level						Impact on operation costs	Notes
								0	1	2	3	4	5		
E.4.2.1			Security risk countermeasure review	This item is for confirming the policy regarding countermeasures against threats discovered after starting the operation. When considering this item, clarify the support scope for identified threats.			Risk support scope after starting the operation	No support	Support for highly important assets, and external connection related areas	Support for all identified threats					
E.4.2.2							Risk countermeasure policy	None	Yes						[Level 1] If there is a risk countermeasure policy, the type of measures which will be implemented must be confirmed.
E.4.3.1			Security patch application	This item is for confirming the scope, policies, and timing for applying security patches to counter system vulnerabilities, etc. These security patches include antivirus pattern files, etc. The scope of security patch application must be confirmed for each OS, middleware products, etc., and when considering security patch application, the effect on the entire system must be verified, and whether or not to apply the patch must be determined. It is advisable to clearly define effect verification, etc., in the maintenance contract.			Security patch application scope	Security patches are not applied	Scope which includes highly important assets, and external connection related areas	Entire system				
E.4.3.2							Security patch application policy	Security patches are not applied	Only highly critical security patches are applied	All security patches are applied					
E.4.3.3							Security patch application timing	Security patches are not applied	Applied together with recovery patches	Applied during scheduled maintenance	Applied when patches are issued				
E.5.1.1		Access / usage restrictions	Authentication function	This item confirms whether or not agent (user and equipment, etc.) authentication is performed in order to use assets, and, if so, to what degree. The effectiveness of deterrence can be raised by performing authentication multiple times. Authentication methods include ID/password authentication and IC card authentication, etc.		X	Authentication of agents with administrative rights	Not performed	1 time	Authentication performed multiple times	Authentication performed multiple times using different authentication methods				[Metric] "Agents with administrative rights" refers to system administrators and business and operation administrators.
E.5.1.2							Authentication of agents without administrative rights	Not performed	1 time	Authentication performed multiple times	Authentication performed multiple times using different authentication methods				
E.5.2.1			Usage restrictions	This item is for confirming whether or not software or hardware access controls are placed on the usage, etc. of assets by authenticated agents (users and equipment). Ex) Door and storage cabinet locks, USB, CD-RW, keyboard, and other input/output device restrictions, command execution restrictions, etc.		X	Operation restrictions placed by system measures	None	Only minimum necessary amount of program execution, command operation, and file access is permitted						[Metric] Refers to software measures such as software installation restrictions, usage restrictions, etc.
E.5.2.2							Operation limitations placed by physical measures	None	Only minimum amount of hardware usage and operation allowed						[Metric] This refers to physical measures, such as access management for server rooms via security gates, etc., locks for data storage locations, servers, etc., and restrictions on input/output devices such as USB memory or CD-RWs.
E.5.3.1			Management method	This item relates to the establishment of rules concerning the addition, updating, deletion, etc., of information necessary for authentication (ex: unique agent identification information such as IDs/passwords, fingerprints, retinal scans, and vein patterns).			Management rule establishment	Not performed	Performed						
E.6.1.1		Data confidentiality	Data encryption	This item is for confirming whether or not encryption of confidential data is performed when transmitting or storing data.		X	Transmitted data encryption	None	Only authentication information is encrypted	Important information is encrypted					[Level 1] "Only authentication information is encrypted" means that, regardless of whether the system is handling critical information, only authentication information, such as passwords, etc., is encrypted.
E.6.1.2						X	Encryption of stored data	None	Only authentication information is encrypted	Important information is encrypted					[Level 1] "Only authentication information is encrypted" means that, regardless of whether the system is handling critical information, only authentication information, such as passwords, etc., is encrypted.

System Infrastructure Non-Functional Requirements Related Item List

No.	Major category	Middle category	Minor category	Minor category description	Overlapping item	Important item	Metric	Level						Impact on operation costs	Notes
								0	1	2	3	4	5		
E.6.1.3							Key management	None	Software based key management	Tamperproof device based key management					[Level] "Software based key management" refers to the use of software settings, etc., to restrict access to private key data. "Tamperproof device based key management" refers to the use of IC cards or other physical measures in order to provide management through dedicated devices with improved attack resistance. This makes it possible to perform even more thorough management of threats such as key data tampering or leakage.
E.7.1.1		Fraud tracking / monitoring	Fraud monitoring	This item is for confirming the scope of fraudulent activity monitoring, the volume of stored monitoring records, and the length for which said monitoring records are retained. The types of logs which should be acquired must be decided based on the specific system and service. When logs are taken, together with fraud monitoring targets, the scope of logs which are checked for fraud must also be defined.		X	Log acquisition	Not performed	Performed						[Metric] Acquired logs refer to logs such as the following, used to detect fraudulent activities. • Login / logout history (success / failure) • Operation logs Etc.
E.7.1.2						X	Log retention period	6 months	1 year	3 years	5 years	10 years or longer	Permanent retention		
E.7.1.3						X	Fraud monitoring scope (equipment)	None	Scope which includes highly important assets, and external connection related areas	Entire system					[Metric] The "fraud monitoring scope (equipment)" metric is used to confirm the scope of logs which are to be acquired in order to perform fraudulent access monitoring, etc., for servers, storage devices, etc.
E.7.1.4						X	Fraud monitoring scope (network)	None	Scope which includes highly important assets, and external connection related areas	Entire system					[Metric] The "fraud monitoring scope (network)" metric is used to confirm the scope of logs which are to be acquired in order to monitor unauthorized packets, etc., on the network.
E.7.1.5						X	Fraud monitoring scope (intruders / unauthorized operations, etc.)	None	Scope which includes highly important assets, and external connection related areas	Entire system					[Metric] The "fraud monitoring scope (intruders / unauthorized operations). etc." metric is used to confirm the scope of monitoring consisting of monitoring cameras installed to monitor for intruders, etc.
E.7.1.6							Confirmation interval	None	Performed when security related events are recognized (as needed)	Performed when security related events are recognized (as needed) + Performed regularly	On-going confirmation				[Level] "Security related events" refer to when critical threats are detected, or when there is a possibility that an incident has occurred due to service malfunctions, etc. "On-going confirmation" refers to constant monitoring for unauthorized access, and the ability to take immediate response measures. The implementation of automatic detection systems, and systems where e-mail notifications, etc., are automatically sent in the event that fraudulent or unauthorized actions are detected, are included in "Performed when security related events occur (as needed)."
E.7.2.1			Data validation	This item is for confirming whether a digital signature system is implemented in order to make it possible to certify that data has been correctly processed and stored, and to detect data tampering.			Digital signature usage	None	Yes						
E.7.2.2							Confirmation interval	None	Performed when security related events are recognized (as needed)	Performed when security related events are recognized (as needed) + Performed regularly	On-going confirmation				
E.8.1.1		Network measures	Network control	This item is for confirming whether transmission control is implemented in order to block unauthorized transmissions.		X	Transmission control	None	Yes						[Level 1] When implementing transmission control, firewall deployment, etc., must also be considered.
E.8.2.1			Fraud detection	This item is for confirming the scope of network based fraud tracking / monitoring detection of fraudulent activities or transmissions within the system.		X	Fraudulent transmission detection scope	None	Scope which includes highly important assets, and external connection related areas	Entire system					[Metric] Depending on the defined detection scope, the deployment of IDS, etc., must also be considered.
E.8.3.1			Denial of service (DoS) attack avoidance	This item is for confirming whether countermeasures are enacted against congestion caused by attacks on the network.		X	Network congestion countermeasures	None	Yes						

System Infrastructure Non-Functional Requirements Related Item List

No.	Major category	Middle category	Minor category	Minor category description	Overlapping item	Important item	Metric	Level						Impact on operation costs	Notes
								0	1	2	3	4	5		
E.9.1.1		Malware countermeasures	Malware countermeasures	This item is for confirming the implementation scope of measures to prevent malware (viruses, worms, bots, etc.) from infecting the system, and the timing of malware checking. When countermeasures are implemented, virus pattern file update methods and timing must also be considered, and virus patterns must be kept up to date.		X	Malware countermeasure implementation scope	None	Scope which includes highly important assets, and external connection related areas	Entire system					
E.9.1.2							Real-time scanning implementation	Not performed	Performed						[Level 1] Real-time scanning is performed, for example, at the occasions listed below. When implementing real-time scanning, the timing must be considered. • When copying data to the file server • When receiving data from the mail server • Before performing input/output processing to files Etc.
E.9.1.3							Regular full scan check timing	None	Non-regularly (Full scanning performed when possible)	1 time/month	1 time/week	1 time/day			
E.10.1.1		Web measures	Web implementation measures	This item is for confirming whether measures related to Web application-specific threats or vulnerabilities are implemented		X	Measure enhancement through secure coding, Web server configuration, etc.	None	Measure enhancement						[Metric] The number of Web system attacks is increasing, and when constructing a Web system, measures such as secure coding and Web server configuration must be considered. When implemented, consideration must also be given to specialist review and source code diagnostics as well as tool-based checking in order to evaluate their effectiveness.
E.10.1.2						X	WAF implementation	None	Yes						[Metric] WAF stands for Web Application Firewall.
F.1.1.1	System environment and ecology	System restrictions / prerequisites	System construction restrictions	This item relates to whether or not there are applicable restrictions when constructing the system, such as company regulations, laws, local governmental ordinances, etc. Ex) • Financial Instruments and Exchange Act • ISO/IEC27000 series • Standards for Information Security Measures for the Central Government Computer Systems • FISC • PrivacyMark System • Construction location restrictions Etc. (* The above examples are mainly Japanese laws, systems, etc.)		X	System construction restrictions	No restrictions	Possible restrictions (only critical restrictions apply)	Possible restrictions (all restrictions apply)					[Metric] During system development, sometimes it is necessary to handle confidential information, personal information, etc. In order to minimize the risk of their leakage, projects must prepare a development environment which implements risk reduction measures such as restricting personnel that can use the information/data, controlling room access, encrypting information/data, etc. Other restrictions may also apply, such as situations where the planned operation site cannot be used for system construction, and it is necessary to construct the system in a staging environment at a different site and transporting it to the planned operation site, or situations where system construction can only be performed at the planned operation site.
F.1.2.1			Operating restrictions	This item relates to whether or not there are applicable restrictions when the system is in live operation, such as company regulations, laws, local governmental ordinances, etc. Ex) • Financial Instruments and Exchange Act • ISO/IEC27000 series • Standards for Information Security Measures for the Central Government Computer Systems • FISC • PrivacyMark System • Possibility of remote operation Etc. (* The above examples are mainly Japanese laws, systems, etc.)		X	Operating restrictions	No restrictions	Possible restrictions (only critical restrictions apply)	Possible restrictions (all restrictions apply)					
F.2.1.1		System characteristics	Number of users	The number of system users (end users).	X	X	Number of users	Specific users only	Upper limit is specified	Usable by unspecified number of users					[Overlapping Item] B.1.1.1. The "number of users" is essential for deciding performance and scalability, and is an item that defines the system environment as well, so this item is included in both "Performance and scalability" and "System environment and ecology". [Level] Even if the numerical value for this prerequisite cannot be precisely determined, it is important that at least a tentative value, based on similar systems, etc., should be decided on.

System Infrastructure Non-Functional Requirements Related Item List

No.	Major category	Middle category	Minor category	Minor category description	Overlapping item	Important item	Metric	Level						Impact on operation costs	Notes
								0	1	2	3	4	5		
F.2.2.1			Number of clients	The number of clients used by the system, which must be managed.		X	Number of clients	Specified clients only	Upper limit is specified	Usable by unspecified number of clients					
F.2.3.1			Number of sites	The number of sites in which the system is in operation.		X	Number of sites	Single site	Multiple sites						[Level 1] Specify the exact number when consensus has been reached regarding the number of sites.
F.2.4.1			Geographical spread	The geographical range over which the system operates.		X	Geographical spread	Inside site	Within 1 city	Within 1 prefectural area	Within 1 region	Domestic	International		[Level] When the selected level is 5, consideration must also be given to multi-language support, etc. Even for domestic systems, if the geographical reach of the system is expansive, network, logistical, and support handling will also be necessary.
F.2.5.1			Specification of specific products	This item is for confirming if users have specified the use of open source products, third-party products (ISV/IHV, etc.). Confirmation is from the perspective of whether the selection has an impact on the difficulty of providing support.		X	Use of specific products	No products specified	Some products specified	Products that are difficult to support are specified					
F.2.6.1			System utilization scope	Range of groups to which system users belong.			System utilization scope	Within division only	Within company only	External (BtoB)	External (BtoC)				
F.2.7.1			Multi-language support	Languages which must be used in system construction, or which must be offered by services. Consider the number of languages which must be supported, and accessibility to people skilled in each language.			Number of languages	Only handles numbers, etc.	1	2	5	10	100		[Level] In addition to the number of languages, the difficulty of the languages must also be considered. Consideration must also be given to currency units, etc. [Level 0] "Only handles numbers, etc." assumes systems designed to interface with machines, not to offer presentation functions for people. For example, gateway systems.
F.3.1.1		Conformity standards	Product safety standards	This item is for confirming whether product safety standards such as UL60950 are required to be held by products used in the system.		X	Standard certification	Standard certification not necessary	UL60950 equivalent certification acquired						
F.3.2.1			Environmental protection	This item is for confirming whether specified toxic substance usage restriction related standards such as those set out in the RoHS directive are required to be held by products used in the system.		X	Standard certification	Standard certification not necessary	RoHS directive equivalent certification acquired						
F.3.3.1			Electromagnetic interference	This item is for confirming whether standards governing equipment maintaining an electromagnetic emission level equal to or below a specific level, such as VCCI, are required to be held by products used in the system.			Standard certification	Standard certification not necessary	VCCI Class A acquired	VCCI Class B acquired					
F.4.1.1		Conditions of equipment installation environment	Earthquake resistance / seismic isolation	Specifies the effective maximum earthquake intensity which the system environment must be able to withstand. If measures such as building vibration damping are used to, for example, decrease the effective seismic intensity of an earthquake from 7 or greater outside the building to a maximum inside intensity of 4, then set the level for seismic intensity to 4. If it is acceptable for service to be discontinued at or above a given seismic intensity, set the level for that given seismic intensity.		X	Earthquake resistance intensity	Countermeasures not necessary	Seismic intensity 4 equivalent (50 Gal)	Seismic intensity 5-lower equivalent (100 Gal)	Seismic intensity 6-lower equivalent (250 Gal)	Seismic intensity 6-upper equivalent (500 Gal)	Seismic intensity 7 equivalent (1000 Gal)		[Metric] For buildings containing system environments which have the same degree of vibration inside as out, the effective seismic intensity of the system environment can be expected to be roughly equivalent to the external seismic intensity. As such, the level can be selected based on the exterior seismic intensity. When seismic isolation facilities, etc., guarantee a reduced maximum seismic intensity for the system environment, that seismic intensity can be considered as the effective seismic intensity, and level assignment can be based on it (users may specifically request a higher level assignment). In the event that an earthquake of a certain intensity or greater would result in there being no system users in environments where they could use the system, and as such system continuity becomes unnecessary, the level may be set based on that seismic intensity. In any case, it is unreasonable to set the standard higher than the earthquake resistance intensity of the building itself. [Level 0] The risk of service outage due to earthquakes must be accepted.
F.4.2.1			Space	This item relates to how much floor space (WxD) and height is necessary. Consideration must also be given to maintenance operation space. Whether or not space for parallel operation of new and old system can be secured for system migration must also be confirmed. If possible, it must be confirmed in advance.		X	Installation space restrictions (machine room)	No space related restrictions	Design using floor-standing equipment	Design using rack-mount equipment					[Metric] Confirm specific floor space and height. Also note the shape of the space, and any variations in load-bearing by location.
F.4.2.2						X	Installation space restrictions (installation in office space)	No space related restrictions	Dedicated space can be set aside for system	System must be installed in space also used by people					[Metric] Confirm specific floor space and height. Also note the shape of the space, and any variations in load-bearing by location. [Level] Consider installation space restrictions as already defined prerequisites, and set levels based on the difficulty of installing the system given those requirements. Please note that this is not the difficulty involved in securing the space itself.

System Infrastructure Non-Functional Requirements Related Item List

No.	Major category	Middle category	Minor category	Minor category description	Overlapping item	Important item	Metric	Level						Impact on operation costs	Notes
								0	1	2	3	4	5		
F.4.2.3							Parallel operation space (migration)	A dedicated space can be secured	A shared space can be secured	No space can be secured					[Metric] During system construction, if the space in which will be used for production system operation is not available, consideration must also be given to space in which to construct the system, and the transportation of the constructed system. Specific floor space and height must also be verified. Also note the shape of the space, and any variations in load-bearing by location. [Level 2] When parallel operation is performed, consider related measures separately. D.1.1.3 and F.4.4.3 are related items.
F.4.2.4							Installation space expansion capacity	There is sufficient expansion capacity	There are some limitations (which can be handled with existing products)	There are limitations (which require customization or construction work)					[Metric] "Installation space expansion capacity" refers not only to direct floor placement, but also rack restrictions, floor load, etc.
F.4.3.1			Weight	This item is for confirming whether system design must take building floor load limit into account. When the floor load limit is low, there is a high likelihood that special measures will need to be taken in relation to installation.			Floor load limit	2,000Kg/m^2 or more	1,200Kg/m^2	800Kg/m^2	500Kg/m^2	300Kg/m^2	200Kg/m^2	X	[Level] Set level based on floor's load capacity. The greater the floor's load capacity, the lesser restrictions on system installation. [Impact on Operation Costs] When the floor load limit is high, high-density installation may be possible, resulting in the need to perform maintenance work at high rack positions.
F.4.3.2							Installation measures	Not necessary	Installation of load distribution materials (metal plates, etc.)	Limit weight per rack, and distribute system across racks	Perform installation design, taking into consideration specific conditions of installation environment (beam locations, etc.)				
F.4.4.1			Compatibility with electric facilities	This item relates to the compatibility of the system with the electrical conditions of the installation site provided by the user (power supply voltage / current / frequency / phase / number of power lines / power protection / scale of required construction work, etc.). Installation location air conditioning must also be evaluated. The possibility of parallel operation during migration must also be considered. If possible, it must be confirmed in advance.			Compatibility with supplied electric power	No restrictions of note with current facilities	Electrical work is necessary, but it can be handled through secondary work, such as power distribution board improvement	Electrical work is necessary, but both primary and secondary electrical work are possible	Electrical work is not possible, and power capacity is slightly low for system scale	Power is completely insufficient, and installation location must be reconsidered			
F.4.4.2							Power capacity restrictions	No restrictions (needed power capacity can be secured)	Some limitations (which can be handled with existing products)	Some limitations (which will require customization, construction, etc.)					
F.4.4.3							Parallel operation power (migration)	Needed power can be completely available	Needed power is partially available	It is difficult to secure sufficient power					[Level 2] When parallel operation is necessary for migration, consider related measures separately. D.1.1.3 and F.4.2.3 are related items.
F.4.4.4							Power loss countermeasures	None	Short interruptions (approx 10ms)	10 minutes	1 hour	1 day	1 week		[Level 1] Consider power stabilization measures, such as UPS or CVCF use.
F.4.4.5							Prospective installation location voltage fluctuation	+/-10% or less	Over +/-10%						[Level 1] When equipment operation conditions are exceeded, power stabilization measures, such as UPS or CVCF use, will be necessary.
F.4.4.6							Prospective installation location frequency fluctuation	+/-2% or less	Over +/-2%						[Level 1] When equipment operation conditions are exceeded, power stabilization measures, such as UPS or CVCF use, will be necessary.
F.4.4.7							Grounding	Grounding not necessary	Grounding necessary	Exclusive grounding necessary					

System Infrastructure Non-Functional Requirements Related Item List

No.	Major category	Middle category	Minor category	Minor category description	Overlapping item	Important item	Metric	Level						Impact on operation costs	Notes
								0	1	2	3	4	5		
F.4.5.1			Temperature (range)	Environmental temperate range conditions of system. Depending on the surrounding environment, special measures may be required for normal system operation.			Temperature (range)	Countermeasures not necessary	16 degrees C to 32 degrees C (operating conditions for many tape devices)	5 degrees C to 35 degrees C (operating conditions for many types of equipment)	0 degrees C to 40 degrees C	0 degrees C to 60 degrees C	-30 degrees C to 80 degrees C		[Metric] Also consider maintaining temperature gradient of approximately 10 deg C/h or less. For level 2 and above environments, separate consideration must be given to the temperature range during system downtime. [Level] Set the level based on the surrounding environmental temperate range when equipment is operating. For example, for an environment whose ambient temperature range varies between 0 to 20 degrees C, choose the lowest matching level, level 3.
F.4.6.1			Humidity (range)	Environmental humidity range conditions of system. Depending on the surrounding environment, special measures may be required for normal system operation.			Humidity (range)	Countermeasures not necessary	45% to 55%	20% to 80%	0% to 85%	The only condition is that there be no condensation			[Level] Set the level based on the surrounding environmental temperate range when equipment is operating. For example, for an environment whose ambient humidity range varies between 20% to 50%, choose the lowest matching level, level 2.
F.4.7.1			Air conditioning capacity	Air conditioning with sufficient cooling capacity for system operation, and, if there are specific hotspots, cooling air supply which takes them into consideration.			Air conditioning capacity	Sufficient available capacity	Targeted measures are necessary for hotspots, etc.	Insufficient capacity, measures are required					[Metric] Countermeasures etc. against refuse, hazardous gas, and others must also be considered as necessary.
F.4.7.2							Air conditioning facility restrictions	No restrictions (Sufficient air conditioning can be secured)	Some limitations (which can be handled with existing products)	Some limitations (which will require customization, construction,					
F.5.1.1		Environmental management	Measures to reduce environmental load	This item concerns measures which reduce the environmental load of the system, such as the purchasing of environmentally preferable purchasing law compliant products or the use of materials and supplies with minimal environmental load. Reduction of waste materials throughout the system lifecycle must also be considered, such as the use of materials which do not need to be disposed of during system expansion, but can be merely replaced or added to. Also, the longer the lifecycle of a unit, the less waste it can be considered to create.			Degree of compliance with environmentally preferable purchasing law	Does not need to be addressed	Some Law on Promoting Green Purchasing standard conformant products used	Only Law on Promoting Green Purchasing standard conformant products used					
F.5.1.2							Expandability of the existing equipment	None	2-fold	4-fold	10-fold	30-fold	100-fold or greater		[Metric] This refers to the ability to expand existing equipment merely by adding to it, without disposing of existing equipment (cases where contractually only addition occurs but in reality equipment is entirely replaced and the previous equipment disposed of is not covered by this). Consideration must also be paid to the energy used during production, and the amount of waste. [Level] Generally, a scale up approach is primarily used when expanding a system to a size several times larger than its initial configuration, after which a scale out approach is used.
F.5.1.3							Equipment lifecycle period	3 years	5 years	7 years	10 years or longer			X	[Metric] "Lifecycle" here refers to the defined period before hardware replacement. It is generally advisable to use equipment for long periods of time, but if used for an excessively long time, the system may not be able to reap the benefits of performance improvements and advances in energy savings. [Impact on Operation Costs] Using equipment with short lifecycles results in frequent updates, and increased operation costs.
F.5.2.1			Energy consumption efficiency	Normally, this is the amount of work per unit of energy, determined by defining the system's work volume by the amount of energy consumed. However, as there are no universal definitions of work volumes, it is difficult to directly calculate efficiency. Also, there are frequently no comparable systems performing the same work, making comparison difficult. As such, with regards to energy consumption efficiency, a slightly different perspective is used, with levels based on whether users issue targets or not. For systems based on power energy, energy consumption is roughly equivalent to heat generation. When data center energy efficiency is looked at instead of system work volume, indices such as PUE (Power Usage Effectiveness) and DPPE (Datacenter Performance Per Energy) are also used.			Energy consumption targets	No targets	Targets provided	Targets provided, as well as requirements for further reductions				X	[Level 0] Reconfirmation of compatibility with power supply facilities is required. [Level 2] Indicates that in addition to achieving level 1 targets, there are additional, stricter standard option demands. [Impact on Operation Costs] When consensus is reached for a low level, additional measures may need to be taken after the system goes into operation and a new legislation, etc., is passed.

System Infrastructure Non-Functional Requirements Related Item List

No.	Major category	Middle category	Minor category	Minor category description	Overlapping item	Important item	Metric	Level						Impact on operation costs	Notes
								0	1	2	3	4	5		
F.5.3.1			Amount of CO_2 emissions	The amount of CO_2 emissions resulting from the system over the course of its lifecycle. Assignment of levels directly based on CO_2 emissions is difficult, so a slightly different perspective is used, with levels based on whether users issue targets or not.			CO_2 emission targets	No targets necessary	Targets provided	Targets provided, as well as requirements for further reductions				X	[Metric] CO_2 emission levels during system operation are generally linked to the amount of power consumed. This, plus the amount of CO_2 emissions resulting from equipment and device manufacturing and disposal, makes up the system's total lifecycle emissions. [Level 0] If no targets are required, reconfirmation of compatibility with CSR, etc., is required. [Level 2] Indicates that in addition to achieving level 1 targets, there are additional, stricter standard option demands. [Impact on Operation Costs] When consensus is reached for a low level, additional measures may need to be taken after the system goes into operation and a new legislation, etc., is passed.
F.5.4.1			Low noise	This item relates to the amount of noise generated by the system. Requirements tend to be particularly high when the system is installed in an office environment. When installed in data centers, as well, noise over a certain level is a problem from a work environment perspective.			Noise value	Countermeasures not necessary	87dB (tolerance limit value taking into consideration use of protective hearing equipment as defined by the British RoSPA noise standard) or less	85dB (2nd action level according to the British RoSPA noise standard) or less	80dB (1st action level according to the British RoSPA noise standard) or less	40dB (library level) or less	35dB (bedroom level) or less	X	[Impact on Operation Costs] If consensus is reached for a low level, reconfirmation of compatibility with the work environment, etc., is required.

Total	6	34	116	92	236