更新日：2024年12月27日

◆ 本检查表介绍了由才望子信息技術 (上海) 有限公司提供的cybozu.com（中国）服务的安全对策。

已取得的信息安全管理体系(ISMS)认证如下：

ISO/IEC27001
认证注册范围：本公司所开发云端服务的运营基础架构系统设计、架构及维护
认证注册日： 2011年11月10日
认证注册编号：IS 577142
认证注册机关：BSI集团日本股份有限公司

ISO/IEC 27017
认证注册范围：作为才望云、cybozu.com、Garoon、Cybozu Office、Mailwise的云端服务提供商，用于系统运行与维护ISMS 云端安全管理系统
认证注册日： 2019年11月10日
认证注册编号：CLOUD 715091
认证注册机关：BSI集团日本股份有限公司

▼请参考以下内容
https://www.kintone.cn/service/security.aspx?cid=58

本检查表中的项目以经济产业省《云服务使用信息安全管理指南2013》为基础。
(https://www.meti.go.jp/policy/netsecurity/downloadfiles/cloudsec2013fy.pdf)，这是一个用日语书写的文件。 除此之外，本检查表对项目进行了适当增删并增加了对主客体的解释。

		要检查的事项	实施情况	言论
1	信息安全策略组			
	1	有一份文件建立了管理层批准的信息安全基本政策。 此外，还应向所有员工和云服务用户明确说明相关文件。	○	我们制定了经管理层批准的云服务相关的安全基本政策（https://www.cybozu.com/jp/terms/security.html） 以及员工应遵守的关于公司内部安全的规则和规范（信息安全规则等） 这些政策已作为公司规定，令所有员工周知，并在我们的公司网站上公开给使用云服务的用户们。 ▼ISMS基本政策 https://www.cybozu.com/jp/terms/security.html ※上面的网址是一个日本网站。
	2	建立信息安全基本方针的文件应定期审查，或者在与提供云服务相关的重大变化时进行审查。	○	我们已经建立了信息安全管理系统（以下称为"ISMS"），为了有效推进信息安全保护行动，我们制定了与云服务相关的安全基本政策，按其规定进行实施，审核和审查。 此外，管理层已经批准的云服务相关的安全基本政策在每年以及重大变化发生时，管理层会根据ISMS的规定，进行审查和再确认。
2	信息安全组织			
	1 内部組織			
	1	管理层应明确说明其对信息安全计划的责任和参与，并积极支持和支持组织内的安全。	○	本集团的内部控制基本政策明确了管理层、监事会成员和员工的行动指南，云服务相关的安全基本政策宣布了参与业务的管理人员和员工将持续推进信息安全对策。 ▼内部控制基本政策 https://cybozu.co.jp/company/internal-control/ ▼ISMS基本政策 https://www.cybozu.com/jp/terms/security.html 此外，我们在记录了ISMS的维护和操作方法的文件（以下简称"ISMS手册"）中明确了CISO（首席信息安全官）的责任和承诺。 此外，我们还建立了一个CISO（首席信息安全官）参与的，积极处理信息安全问题的跨部门会议机构，以努力提高组织内的信息安全水平。 ※上面的网址是一个日本网站。
	2	明确定义负责信息安全的人员及其角色。 此外，明确云服务信息安全联系点，对外公开。	○	ISMS手册规定，CISO（首席信息安全官）的职责和权力由董事长，人力资源部长和运营本部长全权负责。 此外，该手册明确记载了CISO的职责包括信息安全政策和目标的制定和审批，以及管理审查等。 关于云服务信息安全相关的联络窗口，我们建立了CSIRT（计算机安全事件应急响应小组），并在公司主页上公开了相关信息。 ▼CSIRT https://www.cybozu.com/jp/productsecurity/management/cysirt.html ※以上网址是日本官网。
	3	明确并记录信息安全措施、设备审批程序等。	○	在ISMS手册中，我们明确记载了信息安全对策（日常活动，应急响应，按角色划分的PDCA循环）。
	4	准备和提供云服务用户接受云服务所需的材料。 此外，在服务开始前的协议，例如要提供的云服务SLA，应向正在考虑使用云服务的人员明确说明。	○	在本检查表中，我们记载了关于提供的云服务的安全措施并提供给我们的云服务的用户。 作为使用服务前的协议，在我司主页上，我们向云服务用户公布了我们的服务说明书。 ▼cybozu.com（中国） 服务说明书 https://www.kintone.cn/public/download/kintone_cn_service_CH20150828.pdf ▼cybozu.com（中国） 服务利用规范 https://www.kintone.cn/public/download/LI_kintone_CN_20220215.pdf
	5	明确云服务的支持台和投诉台，并向外部披露。	○	我们设立了以下的咨询窗口。 销售咨询电话 021-52392626 日文/中文皆可 接待时间: 工作日9:00-18:00 ▼官方网站 https://www.cybozu.cn/ ▼联系我们 https://formbridge.cn/public/form/show/90649ea024ca5a83e4107101d29ec300259e9aa05d92d4deb6bd5a47daf05b2d#/
3	人力资源安全			
	1 入职前			

	1	员工安全的角色和职责应根据信息安全基本方针确定和记录。 此外，向拟录用员工解释相关文件，并在明确同意本文件的情况下签订雇佣合同。	○	"无论何种雇佣形式，我们都在雇用合同和公司内部规定中制定了相关规定。 我们制定了管理层批准的云服务相关安全基本政策和员工应遵守的内部安全规则和条例（信息安全规则等）。 此外，对于雇佣的员工，我们都与其签订了雇佣合同，并确认其明确同意遵守雇佣规则和公司内部规则。 ▼ISMS基本政策 https://www.cybozu.com/jp/terms/security.html ※以上网址是日本官网。
	2 受雇期间			
	1	对全体员工进行教育和培训，提高员工的信息安全意识。	○	作为入职培训的一部分，对于新雇员工，从确定雇佣开始到试用期结束的六个月内，我们会进行合规培训，以及公司内部规则和规范的教学培训。如果出现违规情况，将针对当事人实施二次教学培训。 对于ISMS适用范围内的员工，作为 PDCA 循环的一部分，我们每年提供一次定期的教学培训。 并且，每当内部规则和规范发生变化时，我们会告知所有员工并令其了解这些变化。 除此之外，根据需要我们还会提供额外的有关安全，合规等方面的教学和培训。
	2	制定程序来应对违反安全漏洞的员工。	○	《信息安全规范》明确规定，做出以下违反安全行为的员工将受到公司雇佣规范规定的纪律处分。 - 故意引发安全事件/事故 - 在信息安全方面造成重大过失 - 屡次在信息安全方面造成过失
	3 终止或变更雇佣关系			
	1	在员工终止或变更雇佣关系时，明确信息资产、访问权限等的归还、删除或变更程序。	○	《信息安全规范》中明确规定了员工离职或离岗时的手续，具体如下。 - 离职时，删除或停用所有系统帐户 - 删除或停用访问权限和远程访问权限 - 从离职/离岗人员处回收公司提供的电脑、钥匙、卡片钥匙等
4	管理资产			
	1	澄清信息资产，编制和维护重要信息资产清单以及关于每个信息资产的允许使用的文件。 此外，指定一个负责管理信息资产的人员。	○	在信息资产台账中，每个资产都按名称、管理负责人、CIA TRIAD（信息安全三原则）的级别、允许使用范围、信息容器和保留期限进行分类和描述。 该台账根据ISMS的规定进行定期审查和更新。
	2	根据信息资产对组织的价值、法律要求、谨慎程度和处理重要性对信息资产进行分类。	○	
5	物理和环境安全			
	1	使用物理安全边界（例如，有人值守的接待处、卡控制的入口）来保护关键信息资产所在的区域。	○	对于信息资产所在的区域（安全区域是指工作区和限制进入的区域），我们使用安全卡来将其和自由进出的区域分隔开来。 对于重要信息资产所在的区域（限制进入的区域）我们使用安全卡控制和静脉身份验证进行物理分隔。
	2	记录用于管理对重要信息资产所在区域的访问的过程和管理方法，以便只有授权人员才能访问它们。	○	《信息安全规范》明确规定了重要信息资产所在的区域，并实施了安全卡控制，以确保只有授权人员才能访问它们。 访问范围（授予安全卡的访问权限）由每个部门的部门长根据以下标准确定。 - 业务的必要性 - 可靠性的观点 - 威慑性的观点
	3	安装服务器的数据中心必须具有抗震性。	○	抗震或免震结构符合1981年6月修订的《建筑标准法》的新抗震标准。
	4	检查数据中心的防雷保护。	○	防雷设备按照JIS标准安装，特高压接收变电站的避雷器作为防雷保护，PDU和PDF中的SPD作为对抗感应雷的措施。 感应雷电保护的电压保护等级为1.5kV。
	5	检查数据中心的洪水损坏对策。	○	已有应对海啸、风暴潮、洪水和强降雨的措施。 该数据中心符合FISC的设施标准，并在几乎所有领域都符合JDCC的数据中心设施标准的第4级。
	6	检查数据中心是否有静电。	○	在服务器区的地板上采取了防静电措施。 此外，服务器室的温度和湿度也得到控制，以防止静电的产生。
6	操作安全访问控制			
	1	记录和维护用于提供云服务的应用程序、操作系统、服务器和网络设备的操作和管理程序。	○	我们制作了应用程序、操作系统、服务器和网络设备的操作和管理手册。 每当操作程序发生变化或设备被添加或改变时，我们都会更新这些手册。 此外，我们也有公布cybozu.com服务的操作手册。 ▼ Cybozu产品 帮助 https://jp.cybozu.help/zh/
	2	管理对用于提供云服务的应用程序、操作系统、服务器和网络设备的更改。 此外，任何影响云服务用户的事情都应提前通知。	○	登录 cybozu.com 后，您将在首页上收到通知。 此外，我们会及时通过网站"通知（才望云快讯）"和电子邮件发布相关信息。 ▼通知（才望云快讯）（kintone） https://www.kintone.cn/service/maintain.aspx?cid=60 ▼ご利用中の方向け　お知らせ（Garoon） https://www.cybozu.cn/jp/support/
	3	明确指出可以使用云服务的操作系统和 Web 浏览器的类型和版本。 提前通知可用操作系统和浏览器中的任何更改。	○	我们在以下网页公布了操作环境的相关信息 ▼支持的浏览器 https://jp.cybozu.help/general/zh/user/webbrowser.html
	4	应定期收集用于提供云服务的应用程序、操作系统、服务器和网络设备中的技术漏洞信息，并进行适当修补。	○	除了每天收集漏洞信息外，我们还根据需要从供应商和安全组织（JPCERT等）接收信息，以确认影响范围。 我们还按照既定步骤安装补丁程序。
	5	监视和调整云服务资源的使用状态，并记录和维护基于使用情况预测设计的容量和性能等要求。	○	我们监控云服务的使用情况。 我们根据利用情况的变化制定扩展计划，并准备有关内容的文件。

6	对用于提供云服务的应用程序、操作系统、服务器和网络设备进行漏洞评估。 此外，应根据结果采取措施。	○	我们的相关部门会进行审查和测试。 另外，我们还接受由第三方进行的外部安全审计。 根据更新的内容，平台和应用程序都至少每年进行一次审计。 并且，我们会根据审计结果进行改善等相应措施。 ▼安全举措 https://www.kintone.cn/service-security.html
7	如果行动码的使用获得批准，最好有适当的偏好，以确保授权的行动码按照明确定义的安全策略运行。 还希望防止执行未经授权的行动码。	※	本公司创建和分发的移动端代码是根据本公司自己的安全政策开发和测试的。 我们服务中使用的一些移动端代码是由第三方创建的。 我们会对发布第三方创建的移动端代码进行管理，定期收集供应商发布的安全信息并适当更新。 cybozu.com上提供的部分服务为客户提供了加载JavaScript的功能。 为了帮助客户创建安全的 JavaScript 代码，我们在网站上发布了安全代码指南。 ▼ 安全代码指南 https://cybozudev.kf5.com/hc/kb/article/200180/
8	定期备份和检查云服务用户信息、软件和软件设置。	○	对于数据备份，除了实时复制外，我们会每日取得增量备份数据。 备份数据每日会被复制并存储在日本东部和西部的两个备份服务器上。 如果东日本的数据中心完全瘫痪，恢复工作将由西日本的备份中心处理。 然而，西日本的数据中心并不作为整个服务的热备份保护，而只是对客户环境进行备份。 ▼ 基础设施运营 https://www.cybozu.com/jp/infrastructure/#infrastructure 我们还每天检查备份期间是否有错误输出到日志中。 除了预定的维护实施日，每天都会进行恢复测试，在日常操作中也会检查，以确保能够正常恢复。 ※以上网址是日本官网。
9	监控用于提供云服务的应用程序、操作系统、服务器和网络设备的运行。 如果检测到服务暂停，请通知用户。	○	该服务的运行状态受到监控。 您可以在cybozu.com运行状态网站上查看服务的状态 ▼ cybozu.com 可用性状态 https://status.cybozu.cn/status/ 如果发现服务中断，我们将通过我们的新闻网站通知您。 ▼通知（才望云快讯）（kintone） https://www.kintone.cn/service/maintain.aspx?cid=60 ▼ご利用中の方向け　お知らせ（Garoon） https://www.cybozu.cn/jp/support/
10	监视用于提供云服务的应用程序、操作系统、服务器和网络设备的故障。 如果检测到故障，请通知用户。	○	设备的运行状态被监控。 如果出现故障，我们会在登录后的首页和通知网站上通知您。 根据影响的程度，也会发送电子邮件。 ▼来自cybozu的通知(故障信息) https://cs.cybozu.co.jp/maintenance/ ■通知时间 原则上，故障通知的目标时间（首次报告到注册的电子邮件地址）为检测到故障后的一小时内。 *根据故障类型不同，情况不限于此。
11	记录操作系统人员的工作。	○	系统操作人员的所有工作都有记录。操作日志以不可更改的格式保存，并保留五年。 按照变更管理的要求，工作的开展要经过负责人的批准，并在两人小组的相互检查下进行。
12	获取记录异常处理和安全事件的审核日志。 此外，还会定期检查相关日志中的警报，以防止篡改和未经授权的访问。	○	每天都会获得审计日志的相关日志警报。 相关的日志被保护起来，防止被篡改。
13	明确指示记录在云服务上获取的用户活动、异常处理和安全事件的审核日志。 此外，还应明确审计日志的保留期限、提供方式和提供时间。	○	应用程序审计日志的存储期限、存储格式和查看可由用户的管理员账户进行管理。 关于我们服务的访问日志，我们会根据法律法规和指导原则进行存储。 *除了审计日志外，我们不提供任何其他日志
14	将用于提供云服务的应用程序、操作系统、服务器和网络设备与准确的时间源同步。	○	NTP（ntp.nict.jp）用于与精确的时间源（如操作系统和网络设备）同步时间。
15	对云基础设施系统的访问应由每个人的唯一标识符以及安全友好的登录过程和身份验证技术控制。 您还应该记录您的访问控制策略。	○	根据我们的规定，系统账户为每个人分配一个独特的标识符。 系统访问是通过VPN网络进行的，这可以防止未经授权的人访问和登录系统。 另外，我们的制度中有规范账户和加密政策。
16	准备添加、删除和更改对云基础架构系统的访问权限的过程。 限制和管理权限的分配和使用。	○	关于添加、删除或更改系统的访问权限的方法已被记录在操作手册中。 对于特别权限，只有负责cybozu.com系统的运营和管理的人员才可以拥有该权限。
17	管理系统操作员使用的密码并使其质量良好。	○	密码按照《信息安全规范》和《信息系统操作手册》进行管理。
18	云服务提供商最好呈现与云服务使用管理相关的信息的类型和内容，以便云用户制定有关网络服务使用的政策。	○	使用cybozu.com服务的登陆方法和访问限制设置在我们的网站上有明确的说明。 ▼ 数据安全 https://www.kintone.cn/service/security.aspx?cid=58
19	在提供的云服务中提供访问控制功能。	○	除了基本认证（免费）和IP地址限制（免费）之外，还可以配置使用客户证书的额外认证（收费）和使用安全确认码的双因素认证。 ▼ 数据安全 https://www.kintone.cn/service/security.aspx?cid=58
20	云提供商希望管理分配给每个云用户的计算资源，以便其他云用户和未经授权的用户无法访问它们，并确保虚拟环境的隔离，而不管物理配置或迁移如何。 如果没有网络或接口分离，云运营商最好考虑应用层通信的端到端加密。 云提供商最好对云环境中的信息安全性进行评估，以确定后门访问云用户信息和软件的可能性。	○	cybozu.com服务是一个多租户架构。 数据库和网络是分离的，访问受到限制，关于注册数据，除了利用该数据的用户以外，其他的用户都无法访问该数据。 详细的分离机制披露如下。 ▼ cybozu.com 的多租户配置中的逻辑分离 https://www.cybozu.com/jp/support/data/cybozucom_multi_tenant.pdf ※上面的网址是一个日本网站。

	21	提供在提供的云服务中注册和删除用户 ID 的功能。	○	我们提供了注册和删除用户ID的功能。
	22	提供用于分配、限制使用和管理所提供的云服务的权限的功能。	○	我们提供了管理权限分配的功能。
	23	提供在提供的云服务中启用密码管理的功能。 它还能够确保密码良好。	○	我们提供了设置密码的到期日期、字符数、复杂度等功能。
	24	列出并明确标明所提供的云服务提供的信息安全措施和功能。	○	我们在网站上公布了提供的安全措施和功能 ▼管理员帮助 https://jp.cybozu.help/general/zh/id/0202.html ▼用户管理和认证 https://www.cybozu.com/jp/account/ ※上面的网址是一个日本网站。
	25	当使用中断时间超过一定时间时，应阻止暂停使用的会话。 此外，对于高风险业务软件，请使用连接时间限制。	○	您可以设置session的有效期。 默认值为 24 小时。 ▼cybozu.com 帮助>与登录相关的安全性设置的初始值 https://jp.cybozu.help/general/zh/id/02052.html
	26	正确管理和控制对网络的访问，以保护其免受威胁并维护网络的安全性。	○	为了维护网络安全，我们对网络配置进行管理，对网络设备实施监控。 除此之外，我们对访问控制进行了记录、管理和实施。
	27	限制和管理网络管理员权限的分配和使用。 此外，网络管理员还应通过具有安全意识的登录过程和身份验证技术来控制访问。	○	只有cybozu.com的系统运营管理人员才被授权为网络管理员。 访问是通过VPN网络进行的，并且访问受到控制，未经授权的人无法访问或登录。 在我们的公司规定中，我们规范了帐户和加密政策。
	28	引入设备（防火墙等）以防止从外部和内部进行未经授权的访问。 并仅提供对您授权使用的服务的访问权限。	○	我们设置了防火墙。 只有我们的服务需要使用的端口处于打开状态，其他端口全部处于限制访问的状态。
	29	根据云服务的连接方法提供身份验证方法。 对于考虑使用云服务的用户，应明确指出根据连接到云服务的方法的身份验证方法。	○	我们的网站上公布了所提供的云服务中的安全措施和功能。 ▼数据安全 https://www.kintone.cn/service/security.aspx?cid=58
	30	云服务合同终止时，数据将被删除。 如果是这样，请确认何时以及在多大程度上将其删除。	○	如终止对cybozu.com服务的订购，输入数据、用户信息和审计日志将在订购终止的次日起30天内被删除。 备份数据将在各种数据删除后约两周内被完全删除。 但是，如果是签约的复数个服务中的一部分被取消，只有被取消的服务的输入数据会被删除。 *用于加密存储数据的加密密钥不是为每份合同产生的，即使在合同终止后的30天内也不会被删除。 系统操作人员对加密密钥的使用与客户数据一样受到限制，所有的工作都有记录，因此不会出现未经授权使用密钥的情况。
	31	确保使用云服务的网络路径已加密。 云服务使用的信息在系统上加密。	○	所有传输数据和存储数据都是加密的。 *我们不提供用户自定义加密方式或是用户独自对自己的存储数据进行加密的功能。 此外，加密密钥的管理是我们公司的责任，我们不提供用户自行生成、存储或销毁加密密钥的功能。
7	供应商关系			
	1	从涉及外部组织的业务流程中识别信息资产的风险，并实施适当的对策。	○	客户在cybozu.com上的录入数据，无论其内容如何，我们都尽全力谨慎管理，除另有规定外，未经客户书面同意，不得为服务以外的任何目的而使用或复制，或向任何第三方提供，披露或泄露。 我们不会使用、披露或泄露这些信息。 对于经由本公司，在外部组织使用此类信息的情况，我们将按照本公司的规定选择和签约。 在签订合同时，我们会签订一份包括安全要求在内的正式协议。 ▼ 服务利用规范 14. 录入数据的处理　25. 委托 https://www.kintone.cn/public/download/LI_kintone_CN_20220215.pdf cybozu.com 使用一个外部数据中心的主机托管服务。 在此也会根据上述服务利用规范和条件签订正式合同。
8	信息安全事件和信息安全事件			
	1	所有员工都应记录并报告他们在系统或服务中发现或怀疑的任何安全漏洞。	○	《信息安全规范》规定了安全事件的定义和此类事件的报告，以及使用的服务疑似病毒感染或信息泄露时的报告和沟通方式以及响应程序。
	2	建立责任制和程序体系，对信息安全事件做出迅速、有效、果断的响应。	○	《信息安全规范》规定了应对信息安全事件的报告和沟通方法以及响应程序。 我们建立了CSIRT（计算机安全事件应急响应小组）来应对与云服务相关的信息安全事件。 管理层在ISMS手册中确立了CSIRT的责任制度。 我们在公司网站上公布了信息安全事件的响应程序。 CSIRT明确记录了运营体制和活动流程，ISMS 手册明确指出，信息安全事件（包括系统故障、机密泄漏、损坏和其他人为错误）将通过适当的通信渠道尽快报告并横贯整个组织中进行管理。 ▼CSIRT https://www.cybozu.com/jp/productsecurity/management/cysirt.html ※上面的网址是一个日本网站。
	3	编制信息安全事件报告，并定期向云用户披露。	○	我们建立了一个 CSIRT（计算机安全事件应急响应小组） 来联络、服务窗口人员，事务对应人员，和其他相关方。 每当发现漏洞时，都会通过公共机构（JPCERT），以下本公司网页向云用户清楚地公布信息。 cybozu.com 和每项服务的维护、更新和事件信息，可在"cybozu.com 公告列表"中找到。 ▼通知（才望云快讯）（kintone） https://www.kintone.cn/service/maintain.aspx?cid=60 ▼ご利用中の方向け　お知らせ（Garoon） https://www.cybozu.cn/jp/support/
9	业务连续性管理中的信息安全方面			

	1	确定可能导致业务流程中断的事件，以及中断的可能性和影响以及中断对信息安全的后果。	○	我们在BCP（营运持续计划）中进行营运持续的风险和业务影响分析。 根据每个业务流程的中断概率和可接受的恢复时间确定优先次序，并制定BCP和BCP的程序手册，以便能够在规定的水平和时间内进行恢复。
	2	云服务提供商希望使提供云服务的系统冗余，并向正在考虑使用云服务的人员明确指示云服务冗余的状态。	○	所有服务器、网络、存储和数据都经过冗余处理。
	3	应定期测试和更新业务连续性计划。	○	我们制定了BCP（营运持续计划），并定期对其进行测试和审查。
	4	用于提供云服务的设备应采取措施在发生停电或停电时确保电力安全。	○	所有用于提供云服务的设备都安装在数据中心，确保在停电或断电的情况下有电力供应。
	5	安装用于提供云服务的设备的客房应当配备火灾探测和通知系统和灭火设备。	○	所有用于提供云服务的设备都位于数据中心，数据中心配备了火灾探测和通知系统以及灭火设备。
10	順守			
	1	明确定义、记录和维护相关法律、法规和合同要求，以及组织满足这些要求的方法。 此外，应保护重要记录不丢失、销毁和伪造，并应妥善管理。	○	可能对ISMS内容产生影响的变更（例如法律法规的变更），我们会反应，更新到ISMS里。 在ISMS中创建和使用的文件和记录要每个文件逐一指定管理者、批准者和保留期来进行适当管理。
	2	云提供商被定义为云业务运营的地区（国家、州等）、数据中心所在的地区（国家、州等），以及 云提供商最好清楚地说明他们适用的法律、法规和合同要求。	○	cybozu.com（中国）的服务是在东日本的数据中心运作，而备份数据则储存在西日本的数据中心。 公司网站上公布的服务利用规范规定了适用的法律和管辖权。 ▼服务利用规范 26. 准据法·诉讼管辖 https://www.cybozu.cn/jp/pdf/support/index/cybozu_ch_20220215.pdf
	3	云提供商最好通知云用户许可云用户使用其知识产权的范围和限制。	○	我们网站上发布的服务利用规范规定了知识产权的许可范围。 ▼服务利用规范 21. 知识产权等 https://www.cybozu.cn/jp/pdf/support/index/cybozu_ch_20220215.pdf
	4	禁止将信息处理设施用于未经授权的目的。	○	《信息安全规范》规定了谁被允许进入物理边界和其他边界，并限制未经授权的人进入。 还规定了确定访问授权的政策。
	5	确保个人数据和个人信息根据相关法律、法规以及合同条款的要求（如适用）受到保护。	○	根据我们网站上发布的服务利用规范及个人信息保护方针进行处理。 ▼服务利用规范 https://www.cybozu.cn/jp/pdf/support/index/cybozu_ch_20220215.pdf ▼个人信息保护方针 https://www.kintone.cn/service/privacy.aspx?cid=59
	6	云提供商应定期进行独立审查和评估（例如，内部和外部审计，认证，漏洞，渗透测试等），以确保其组织遵守信息安全基本政策和适用的法律要求。 此外，云提供商不会响应云用户的个人审计请求，而是根据与云用户的协议， 最好提供独立审查和评价的结果。	○	我们通过公司内部相关部门进行审查和测试。 我们还由第三方组织进行外部安全审计。 平台和应用程序都实施1次/年以上，并根据更新内容实施。 漏洞审核结果可在公司网站上找到。 ▼ 数据安全 https://www.kintone.cn/service/security.aspx?cid=58 此外，如果您自行请求漏洞验证，我们将提供验证环境。 有关详细信息，请参阅下面的网站。 https://cybozu.co.jp/products/bug-bounty/ ※上面的网址是一个日本网站。
11	その他			
	1	记录媒体（文档、记录媒体）的适当存储和管理。 此外，在处理信息时，请安全处理，以便无法恢复记录的信息。 此外，重复使用时，请采取措施，以免导致机密信息泄露。	○	《信息安全规范》规定了记录介质上的信息处理方法（存储和销毁），并妥善处理。
	2	将重要的信息资产存储在安全的地方，不要将它们放在办公桌上（Clear Desk）。 另外，锁定信息终端的屏幕，以便在您离开座位时不会窃听信息。	○	《信息安全规范》规定并实施干净办公桌（重要的信息资产在工作日结束后保存在上锁的柜子和抽屉里）和屏幕锁等措施，防止第三方在离开办公桌时轻易操作和查看信息。
	3	防止员工计算机上的病毒。 此外，应定期收集有关技术漏洞的信息，并应适当应用补丁。	○	《信息安全规范》规定并遵守有关客户端PC的用户合规事项（病毒对策等）。 对于有关技术漏洞的信息，我们收集有关针对病毒、间谍软件、技术漏洞等的对策的信息并进行告知。
	4	终止提供本服务时，应提前通知用户。	○	服务的取消通知应至少在预定的取消日期前三个月通过本公司发出。 ▼服务利用规范 17. 取消服务https://www.cybozu.cn/jp/pdf/support/index/cybozu_ch_20220215.pdf
	5	在提供服务时必须明确职责分工和责任范围。	○	关于cybozu.com 提供的每项服务的责任分界点，请参考以下内容 ▼cybozu.com 责任分界点 https://www.cybozu.com/jp/support/data/cybozucom_boundary.pdf ※上面的网址是一个日本网站。
	6	提供了标记信息的功能。	○	有关每项服务功能的详细信息，请参阅手册。 ▼kintone 帮助 https://jp.cybozu.help/k/zh/ ▼cybozu.com 帮助 https://jp.cybozu.help/general/zh/
	7	提供了有关 IPv6 支持的信息。	※	不支持 IPv6。