千寻位置

精准位置服务安全白皮书

2018 年 12 月

V 1.0

目 录

1. 前言

千寻位置网络有限公司（以下简称：千寻位置）作为全球领先的精准位置服务公司，提供高达动态厘米级和静态毫米级的定位能力，是 IoT 时代的重要基础设施之一。公司基于北斗卫星系统（兼容 GPS、GLONASS、Galileo）基础定位数据，利用遍及全国的超过 2,200 个地基增强站及自主研发的定位算法，通过互联网技术进行大数据运算，为遍布全国的用户提供精准定位及延展服务。

为了帮助用户感知和理解千寻位置在精准位置服务上的努力，了解千寻位置精准位置服务全生命周期的安全建设和安全成果，让用户安全放心地使用精准位置服务，公司特编写《千寻位置精准位置服务安全白皮书》（以下简称：白皮书）。本白皮书系统地介绍了千寻位置精准位置服务的全生命周期的安全保障体系和技术实现过程。

1.1 术语定义

精准位置服务：通过建设强大的卫星导航定位基础设施，研发先进的精准位置算法，运用互联网播发服务能力，向 IoT 时代的各类应用终端提供米级、亚米级、厘米级甚至毫米级定位能力的位置服务。

全生命周期：精准位置服务解决方案中，从观测站获取原始数据到数据中心处理，从互联网播发再到终端数据解算完成位置服务的整个生命周期

IoT：Internet of Things，物联网，物物相连的互联网

AIoT：AI (artificial intelligence) and IoT，人工智能结合物联网

AES：Advanced Encryption Standard，高级加密标准，由于计算速度快，安全性更高，AES 已经成为主流对称加解密解决方案的首选算法

DDoS：Distributed Denial of Service，分布式拒绝服务攻击

ECS： Elastic Compute Service，是一种处理能力可弹性伸缩的计算服务器

ELK：Elasticsearch、Logstash、Kibana，大数据日志处理套件

GNSS：Global Navigation Satellite System，全球导航卫星系统

HTTPS：Hypertext Transfer Protocol Secure，超文本传输安全协议，是 HTTP 协议的安全实现

NTRIP：Networked Transport of RTCM via Internet Protocol，是在互联网上进行 RTCM 数据传输的协议

ODPS：Open Data Processing Service，开放数据处理服务

RSA：非对称加密算法，在公开密钥加密和电子商业中 RSA 被广泛使用

SDLC：Security Development Lifecycle，安全开发生命周期

SHA：Secure Hash Algorithm，安全杂凑算法

SLB：Server Load Balancer,对多台云服务器进行流量分发的负载均衡服务

SM4：国密分组密码标准

TLS：Transport Layer Security，传输层安全性协议

WAF：Web Application Firewall，Web 应用防火墙

VPC：Virtual Private Cloud，基于基础云平台构建的网络隔离环境

3DES：Triple Data Encryption Algorithm，三重数据加密算法（DES 块加密）的通称

1.2 精准位置服务的现实挑战

随着 IoT（物联网）时代的到来，人类社会各种生活场景对精准位置的需求越来越多。未来无数智能物联网设备都将是精准位置服务的使用者，它们将服务于人类生活的方方面面，如：智能穿戴、自动驾驶、精准农业、危房监测等。精准位置服务会像水、电、网络一

样成为我们生活中的重要基础设施。

与此同时，安全可靠对于精准位置服务而言，其重要性也变得不言而喻。精准位置服务一旦不可用或服务可用性下降，将直接影响成千上万的基础设施终端设备的正常运行，甚至导致生产事故，引发生命安全问题。除了安全，成功运营精准位置服务还面临其它方面的现实挑战，它要求企业：

- **法规层面，**拥有国家批准的测绘资质认证，合法开展测绘工作；
- **资源层面，**建设和维护遍布全国甚至全球的强大基础设施；
- **技术层面，**聚集尖端人才在核心算法上取得重大突破；
- **运营层面，**有能力将位置服务作为基础设施向公众提供；
- **业务层面，**严格执行行业标准规范，深入拓展业务场景；
- **安全层面，**保障服务连续高可用以及数据安全等。

1.3 千寻位置解决方案

精准位置服务的应用场景决定了用户对于服务安全性有极高的要求，千寻位置也一直致力于为用户提供稳定、可靠、安全的服务。公司在开展业务的同时，在多个层面开展工作，以应对精准位置服务所面临的现实挑战。

千寻位置在 2017 年获得**国家测绘地理信息局认证的甲级测绘资质**，标志着公司可以在中国境内开展“大地测量：卫星定位测量、全球导航卫星系统连续运行基准站网位置数据服务”，相关工作具备合法性。该认证为高精度位置服务的开展解除了法规层面的障碍，降低了开展精准位置服务的法律风险，为客户和合作伙伴解除了后顾之忧。

为将精准位置的服务质量提升到与国际同行同等的水平，甚至某些领域赶超国外同行，千寻位置从成立之初就在全球范围内搜寻 GNSS 导航领域的顶尖人才。2018 年 10 月在法兰

克福召开的 RTCM（国际海事无线电技术委员会）134 特别委员会（以下简称“SC-134”）工作会议正式决定，推选千寻位置首席科学家冯绍军担任**委员会第三工作组主席**，成为该委员会唯一一名来自中国的工作组负责人。为充分保障数以亿计终端的使用安全，进一步提升高精准定位服务在物联网时代的作用，冯绍军及其团队一直在研究让完好性技术帮助各类终端给出可信的定位结果，目前已取得多项成果。

目前千寻位置已经建立自身的算法人才体系，具有多个梯队的 GNSS 领域专家，为高精度位置服务的顺利开展奠定了算法研究的现实基础。2018 年，经过杨浦区、上海市和国家相关单位层层评审和审批，千寻位置成功获批设立**博士后科研工作站**，这是千寻引领北斗领域技术创新的重要“产学研”平台，也是千寻在导航和定位领域能力的真实体现。

基于超过 2，200 个北斗地基增强站组成的 **“全国一张网”**，千寻位置依托自主研发的星基增强、地基增强算法及互联网技术进行大数据运算，已逐步向用户提供**“星地一体”**的厘米级高精度定位服务。

作为精准位置服务的提供者和运营者，千寻位置从成立之初就已经将安全性纳入服务质量范畴。安全团队建设和安全工作开展几乎与公司业务同步启动。以下将重点阐述千寻位置精准位置服务安全保障的详细内容。

2. 精准位置服务安全保障

千寻位置精准位置服务的概略逻辑是：通过遍布全国各地的北斗地基增强系统基准站对北斗、GPS、 GLONASS、Galileo 等卫星进行观测，再经安全专网将原始观测数据回传至北斗数据中心。经过千寻核心算法对数据进行解算后，最终由播发服务将改正数据通过公有云基础设施向外播发，从而为用户提供服务。

各类定位终端（如：自动驾驶汽车、无人机、IoT 设备等）可以通过互联网模式下的 Open API（应用程序接口）、NTRIP 标准协议等向千寻位置发起精准位置服务请求；在无网络区域还可以通过接收千寻公司通过卫星播发的改正数据实现精准定位。

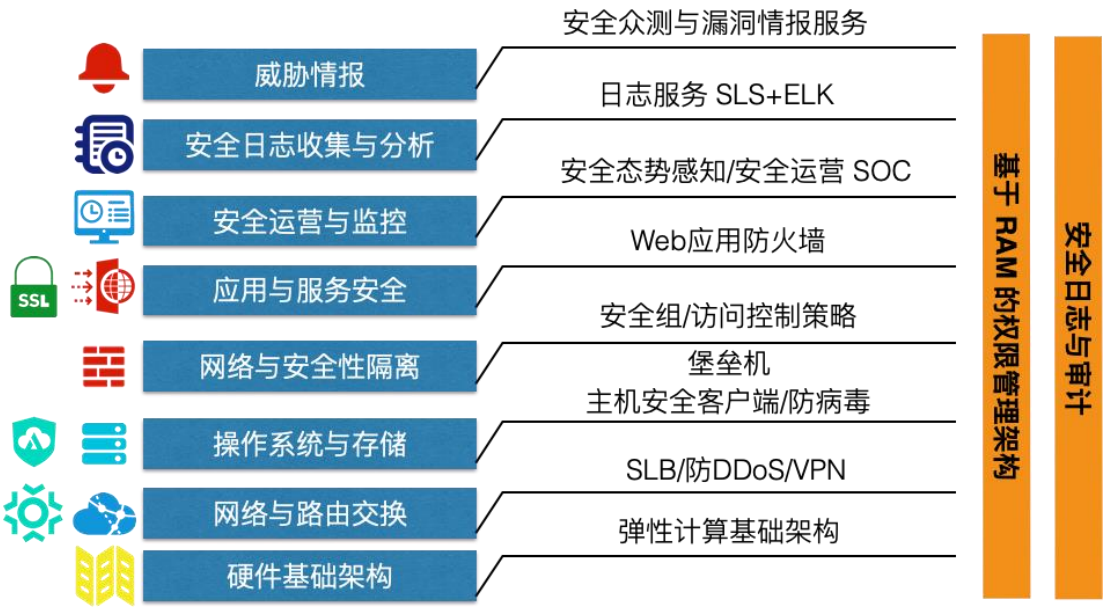
整个业务流程涉及到：基准站、专线网络、数据中心、核心算法、公有云、平台服务、网络通讯、运维监控、服务保障、终端算法与 SDK 和卫星通讯等复杂环节，其中任何一个环节出现风险，都有可能威胁整个精准位置服务的安全性。为此千寻位置在精准位置服务的全生命周期中融入安全，开展安全设计与防护体系建设，切实提升系统安全性和可靠性。

2.1 基础环境安全

云计算具有高可用、高扩展、高效率和高安全的特点，已经成为行业趋势。千寻位置也充分发挥了云计算的优势。公司通过全球领先的云计算平台——阿里云，向全球用户提供精准位置服务，为用户提供稳定可靠，安全的服务。基础平台经过近几年的发展，已经具有可靠的基础架构设计，强大的技术支持能力以及广大的用户基础。

2.1.1 定制化网络安全架构

基于公有云自身基础平台能力，千寻位置结合自身业务和基础平台的产品特性，建立了以下的网络安全架构：



安全架构体系的有效运作依赖于各个层级内的有效控制，以及层级之间的相互协作。如上图所述，千寻位置精准位置服务网络安全架构包含以下层级的安全控制：

硬件基础架构：弹性计算平台核心技术架构，自适应扩展。

网络与路由交换：基础平台专有网络，与其他租户隔离。

操作系统与存储：弹性计算主机安全防护，堡垒机授权管理，高可用数据库。

网络与安全性隔离：通过 VPC 进行安全域隔离，并通过安全组策略进行访问控制。

应用与服务安全：Web 应用防火墙防御 SQL Injection、Cross Site Script，CC 等攻击。

安全运营与监控：结合态势感知及自主开发的监控系统，发现攻击行为，挖掘潜在风险。

安全日志收集与分析：基础平台各类日志收集、处理、存储和分析。

威胁情报：通过第三方威胁情报服务和安全测试团队从外部视角发现企业安全漏洞，并快速开展修复和加固工作。

2.1.2 启用安全域实现安全隔离

网络安全的前提之一就是对网络进行合理的隔离和划分。专有网络 VPC（Virtual Private Cloud）是基于基础平台构建的一个隔离的网络环境，专有网络之间逻辑上彻底隔离，VPC 因此也就构成了云上的私有网络环境。

公司在基础平台上根据承载功能和安全级别的不同，通过 VPC 将网络划分出了**生产/预发布**，**开发/测试**，IT，**安全接入 DMZ** 等几大安全域。在不同的 VPC 安全域之间，根据业务访问需要以及安全级别的不同，制定了不同的路由策略以及严格的安全访问策略，生产环境与开发测试等环境是严格隔离的。VPC 内部根据业务属性启用不同的安全组，并设置严格的访问控制策略。

2.1.3 主动发现业务端口暴露风险

公司的各类应用服务，必须经过安全审核后，才能正式对外发布上线，端口对外开放更是严格管控。除现有的 VPC、安全组等访问控制规则外，公司信息安全部门还部署了外部端口扫描系统，及时扫描发现对外暴露的所有 IP 和端口，并将异常端口开放信息实时同步到钉钉办公系统，便于安全团队及时响应和处置。

2.1.4 防 DDoS 攻击

DDoS（分布式拒绝服务）攻击会对系统和业务的可用性产生重大影响，严重时可导致精准位置服务服务中断或数据质量下降。为此，公司部署了 DDoS 防御解决方案。该方案能够检测并防御各类基于网络层，传输层（包括 SYN Flood, UDP Flood, ICMP Flood 等）以及 HTTP/HTTPS 业务的应用层 DDoS 攻击。防 DDoS 攻击方案能自动检测、自动调度并触发

清洗功能，数秒钟内就可以完成攻击发现、流量牵引和流量清洗全部动作，保证了系统和业务的可用性。

所有的 DDoS 攻击事件，都会通过邮件、短信、电话和钉钉机器人接口，第一时间知会到安全团队。在日常运行过程中，安全团队也会通过自主开发的安全监控系统，实时监控 DDoS 高防服务的流量和连接数状况，为精准位置服务的高可用持续护航。

2.1.4 安全运维

2.1.4.1 运维账户安全

千寻位置启用了基础云平台的 RAM（Resource Access Management，用户身份管理与资源访问控制服务）功能。主账号由运维部门负责管控，同时通过创建 RAM 子账号授予给不同的部门用户。RAM 子账号在创建和授予时，需要由申请人，提交正式的申请流程，经主管和运维人员批准后，再由运维操作人员根据需要的权限，进行创建。

所有用户（包括基础云平台主账号以及 RAM 子账号）在使用账号登录运维控制台时，都要求启用多因素认证(MFA, Multi-Factor Authentication)，避免账号被黑客暴力破解及密码泄露导致的身份盗用。

对于应用程序通过 Access Key 访问基础云平台 API 接口的场景，千寻位置也进行了严格控制。应用程序只能通过对应 RAM 子账号的 Access key 进行访问，避免直接使用主账号的 Access key 进行操作，产生越权访问风险。

2.1.4.2 系统账户安全

对于系统账户，公司制定了一系列的安全制度和操作规范，避免使用弱口令作为密码，并要求用户定期更换密码。公司信息安全部也会通过服务端安全工具，检测系统是否存在弱口令。一旦出现弱口令，将及时跟进处理。

此外，公司还制定了主机安全管理规范，所有对生产环境主机的运维管理必须通过堡垒机进行操作；堡垒机权限需要用户通过 ITSM 系统申请，经部门主管和运维人员审批通过后，才会开放。公司信息安全部对堡垒机操作日志和系统账号行为日志进行收集并定期审计。

2.1.4.3 运维操作审计

千寻位置在日常运维过程中，开启了各类操作审计功能，所有基础云平台账号的操作，都进行了完整的日志记录和长期归档，归档时间至少一年。部分日志根据相关法规要求，则保留更长时间。千寻位置对上述各类日志进行收集，并统一发送到公司信息安全部门自主开发的安全系统，进行实时的监控分析，对典型的风险场景进行及时的告警。

2.1.5 主机安全

2.1.5.1 安全基线

公司制定了 ECS（弹性计算主机）操作系统安全基线，内容包括账户安全、身份认证、最小服务、最小授权、日志审计、时钟同步等，并根据使用环境的不同，对操作系统镜像进行不同程度的安全配置加固，确保新 ECS 主机在创建时即满足相应的安全基线要求。

2.1.5.2 漏洞管理

所有线上 ECS 均部署主机安全客户端，实现操作系统、程序组件，应用中间件等软件产品的实时漏洞检测，一旦发现当前环境下存在产品漏洞或不安全的配置，即发出漏洞告警，同时提供详情描述和修复建议。

通过在企业内部部署业界知名商业漏洞扫描产品，定期对开发测试环境执行完整策略的漏洞扫描，输出漏洞扫描报告和统计分析报表。

公司信息安全部根据漏洞检测告警及扫描报告，依照《漏洞及补丁管理办法》要求，评估漏洞风险，制定修复计划，并联合运维及相关技术部门，落实漏洞修复和加固，实现漏洞管理闭环。

2.1.5.3 威胁检测

运维过程中使用堡垒机，对服务器权限做严格管控并对人员操作进行全面审计。ECS 上部署的主机安全客户端能够对攻击威胁进行实时检测，识别出包括异常登录，进程异常，异常网络连接，敏感文件篡改，可疑文件，网站后门，恶意进程等潜在威胁行为。上述安全事件信息都已接入内部安全监控系统，系统会在威胁发生的第一时间通知到安全人员，提升应急处置效率。

2.1.6 应用安全

通过部署 WAF（Web 应用防火墙），千寻位置对包括官方网站、API 服务、技术论坛等在内的主要对外 Web 应用进行了防护，将云计算大数据统计分析及安全防护能力相结合，实现对 SQL 注入、XSS 跨站脚本、常见Web 服务器插件漏洞、木马上传、暴力破解、越权访问

等 OWASP TOP10 常见风险的有效识别，拦截海量恶意探测请求，保障千寻 Web 应用的安全性与可用性。

2.3 产品与服务安全

2.3.1 实名认证

千寻位置官方网站对外提供服务过程中，严格执行国家测绘管理规定，对所有使用高精度位置服务的人员进行实名认证和用途登记。只有经过认证的企业或个人才能使用高精度位置服务。

用户在申请使用千寻位置网络服务时，必须向千寻位置提供中国地区有效、真实、正确及完整的个人或企业资料。针对企业用户，公司要求认证企业必须上传企业相关的详情信息，包括企业名称、联系方式、使用用途和营业执照等。千寻位置将按法律法规之要求对上述资料进行实名认证并将不定期审核。

2.3.2 服务鉴权

用户在千寻位置官网注册并购买服务后，可以创建自己名下的服务实例。每一个实例都是单独的服务空间，包括关联的设备数、服务周期、计费方法等。服务账号之间相互隔离，互不影响。

网站登录过程中，采用账户、密码、短信验证码和图形验证码等多重安全机制保障用户账号安全。用户购买服务后，名下各类终端设备或应用系统可以通过千寻位置颁发的 APPKEY 和 APPSECRET 与千寻服务端进行通讯，服务端会对 APPKEY 与用户账号映射关系进行校验和权限判断，非授权用户禁止使用精准位置服务。

2.3.3 通讯安全

为保障客户端与千寻服务端通讯安全，公司提供基于 NTRIP 协议标准数据格式的播发服务，也提供基于千寻位置开放时空协议的通讯方式（支持更多安全参数设置）。位置服务标准 API 同样支持加密方式与服务端通讯，HTTPS、TLS 、AES、RSA 、SHA 等技术在整个解决方案中被广泛使用。

2.3.4 密钥安全

用户购买的服务实例对应的 APPKEY 和 APPSECRET 是 API 通讯的重要安全参数，RTK 服务账号对应的服务密码同样也是终端设备与服务端通讯的重要认证凭据。除了客户需要保护好这些凭据外，作为平台，千寻位置对用户的敏感信息都做了加密处理，降低信息泄露风险。存储密钥和密码的数据库有增量每日备份、和定期全量备份，确保安全可用。

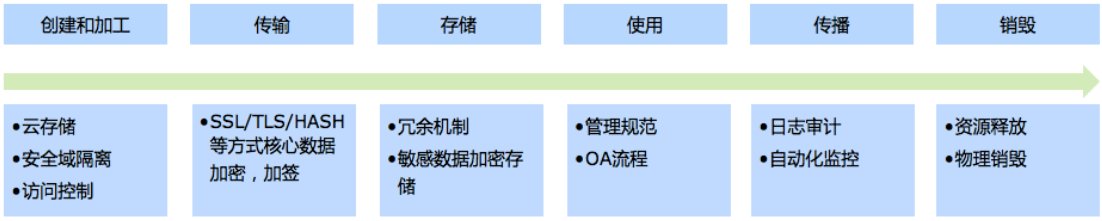
2.3.5 隐私安全

公司在提供高精度位置服务的同时，会严格履行作为位置服务提供商的安全保护义务。公司仅利用收集的信息为用户提供有价值的产品和服务，开发符合隐私权标准和隐私权惯例的产品。相关产品研发、测试和运营遵循业界安全最佳实践，使用先进的技术架构和安全加密措施保障用户服务和数据安全。

用户实名认证信息在数据库中以加密方式存储，基于公司公司数据安全规范，对数据脱敏、匿名化有严格的管理要求和执行标准。敏感数据只有在脱敏或匿名化处置后，才能用于公司内部以故障诊断和性能改善为目的的调试和分析。

2.4 数据安全

公司制定了《数据安全规范》，明确数据生命周期中创建、加工、传输、存储、使用、传播和销毁等各个环节的管理原则，并在各环节都单独制定了相应管理要求和技术保障手段。



2.4.1 数据创建

按照数据的不同类别和重要程度，千寻位置制定了企业内部《数据安全规范》，将数据资产分为客户、业务、公司三个类别，以及 G1（可公开）、G2（内部）、G3（秘密）、G4（机密）四个级别。数据分类分级在数据产生之前已经确定。针对不同类别和级别的数据，公司依据《数据安全规范》分别从数据存储与传输，身份认证，访问控制，安全监控与审计，数据提取，数据开放与披露等方面采取不同的管控措施。

2.4.2 数据传输

针对测绘行业的严格安全要求，所有基准站观测数据通过安全专网传输到数据中心。对个别无法使用专线的特殊观测站，采用 4G 网卡和支持国密算法的 VPN 传输观测数据。

位置服务网站和服务接口 API 支持 TLS 加密的 HTTPS 方式安全接入统一应用网关，保障网络通讯安全。关键数据交互支持通过认证、签名、加密等措施进行严格校验，全面保障数据机密性、完整性、可用性和不可否认性。

2.4.3 数据存储

千寻位置使用 MySQL、MongoDB、ODPS、Redis 等数据存储解决方案处理各类业务数据。所有数据存储采用冗余机制，并定期执行快照和备份管理，防止数据误删除或遭遇病毒入侵删除。

同时，根据不同等级的数据分类，公司采用了不同的安全控制措施。敏感数据一律采用加密存储，并严格控制数据访问权限。企业内部在用的加密算法包括： 3DES、AES、SM4、RSA、SHA 等，并且密钥长度满足安全保护要求。

除此之外，千寻位置团队也在与云厂商共同探索更安全便捷的加密存储方式，例如部分数据库系统的全库加密技术。

2.4.4 数据使用

基站精密坐标和原始观测数据在内部受严格管控，除核心位置算法和质量监测外，其他系统一律使用经过加偏改正过的脱敏数据。

服务端应用层面，所有内部应用必须接入单点登录和中央授权系统，访问主体必须根据权限、角色和风险级别按需申请，并详细说明访问内容、访问理由等相关信息。未经授权用户禁止访问内部系统。

2.4.5 数据传播与销毁

针对核心数据的提取、使用等业务需求场景，公司内部还设置了核心数据使用申请审批流程，严格执行数据操作规范。数据使用完成后，还必须遵循安全规范及时销毁。通过设立和执行严格的数据安全规范，使用安全可靠的工具支持，千寻能够保障核心数据在生命周期

内的安全。

2.4.6 数据安全审计

除了完善的单点登录、中央授权等安全机制外，公司业务系统都启用了严格的操作审计功能。授权用户在后台的操作行为可以被审计记录，一旦发现异常行为及时告警，确保违规操作有迹可循。

为保护企业内部敏感信息，公司在所有办公客户端部署了防数据泄露产品。当有针对敏感文件的违规操作后，系统能够触发后台告警机制，通知安全人员及时处理。

对于公司的代码资产，内部代码托管系统 Gitlab 实行了基于项目和用户的权限分割和最小授权，确保开发者只能访问自己参与的项目，且所有的操作行为会被日志记录，输出到自建的 ELK（Elasticsearch, Logstash, Kibana）日志管理系统。

综上所述，公司正是从管理和技术，内部和外部等不同的角度，确保了核心数据资产的不外流，最终保障公司的数据安全和核心竞争力。

2.5 业务连续性

自动驾驶、无人机、精准车联等场景对高精度位置有极高的依赖，因此服务必须持续可用。为了保障千寻业务能够 7x24 小时不间断向万物互联的定位终端提供精准位置服务，位置服务的高可用是首当其冲要考虑的问题。

2.5.1 灾备与冗余

如上所述，千寻位置在基于云平台高可用的基础设施上，根据自身业务需要，规划并实施了千寻位置网络安全架构。为了进一步确保公有云环境下基础架构的安全，继千寻位置华

北数据中心提供稳定精准位置服务的基础上，公司华东数据中心即将投入使用。公司在浙江德清还部署了安全机房，用于在极端情况下保障公司业务高可用。两地三中心的运维基础架构，是精准位置服务高可用的重要保障。

网络接入层面，防 DDoS 解决方案支持电信、联通和 BGP 网络三线接入，单个接入点出现故障，不会导致服务瘫痪。应用交付层面，内外部双层负载均衡，可以保障应用交付的平滑切换。技术架构设计层面，千寻位置 SpaceX 框架支持集群水平扩容，可应对各种极端业务增长场景。

2.5.2 应急响应机制

千寻位置为保障公司重要业务系统持续有效运行，建立了长效业务连续性管理机制，从业务影响分析和风险评估、业务连续性计划、应急预案、应急演练、持续改进五个环节，建立业务连续性管理机制，并随着公司业务发展和技术架构更新持续优化。

公司内部根据风险评估结果，对基础云平台实例故障、核心业务数据库故障、DDoS 攻击、IT 服务中断等中高级别风险制定相应的应急预案，由相关团队人员组成应急小组，定期执行应急演练，根据演练结果或实际应急响应情况，适时优化和改进应急预案。

在业务服务和系统运行监控方面，公司建立了 7*24 小时的监控机制，并配备专门的业务监控室和大屏展示系统。根据业务和系统类型，公司制定了事件分级标准，监控团队持续关注公司核心网络、系统、应用及业务服务的健康状况，确保在业务影响事件发生时，监控团队及系统能够在第一时间，通过钉钉，电话等渠道向关联团队或个人即时反馈异常信息，依据应急机制及时排障和恢复，将可能的影响降到最低，确保业务服务稳定。

2.6 安全运营

2.6.1 反入侵

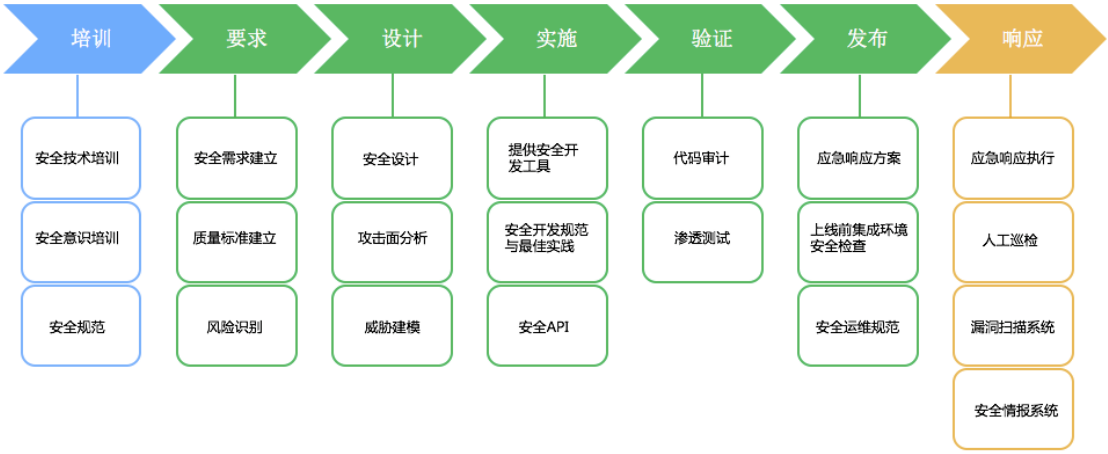
公司各类系统、平台每天都产生海量的日志数据，包括终端安全日志、防病毒日志、网络安全日志、系统运行及入侵检测日志、态势感知告警、WAF 防护日志、Web 服务日志以及网络流量、基线检查等信息。基于这些日志，千寻位置通过安全监控分析平台实现异常行为数据的自动识别、分析和关联，精准有效感知业务系统可能存在的风险隐患。结合办公网异常流量分析检测，实现云上、云下一体化安全联动配置，保障业务系统的安全性和可用性。

2.6.2 安全自动化

为加快安全事件处理效率，降低风险事件可能带来的潜在影响，公司信息安全部自主开发和部署了一系列安全监控分析工具，能从汇总的海量日志及监控信息中，根据自定义告警模板和规则引擎，分析出亟需关注的安全事件，并将事件告警信息通过钉钉机器人接口进行通知。安全自动化工具间的有效配合极大地降低了事件误报率，提高了事件处置效率和质量。

2.7 安全开发生命周期管理

公司在对外产品和服务平台的开发过程引入安全开发生命周期管理（SDLC），借鉴行业内的最佳实践并结合千寻自身的项目管理流程，从安全培训、需求评审、产品设计、编码实现、安全测试、发布维护等关键节点，将安全措施贯彻落实，保障代码安全规范。



此外，公司信息安全部定期为开发测试人员开展安全开发专项培训，提高开发人员的安全开发意识。开发人员在开发过程中，遵循《OWASP 安全编码规范快速参考指南》，同时公司参考业内最佳安全开发实践，制定了适用于公司自身的《快速安全编码指南》；并通过商业版静态代码检测工具、动态代码扫描工具、安全测试工具在编码、测试、验收阶段提升代码质量，保障最终产品和服务的高可靠。

除了内部人员的测试和评估外，公司还启用了第三方安全众测服务，定期对重要系统如公司官网进行安全检测。检测过程中，“白帽黑客”以攻击者视角，能更全面的发现系统存在的安全漏洞。安全团队会根据安全众测的结果，和开发团队一起推动漏洞的修复加固。针对精准位置服务相关的 SDK 和 APP，公司定制了专项移动端安全解决方案，进行漏洞检测和安全加固，确保应用交付的质量。正是这样全流程，多方位的安全介入，确保了产品开发和项目实施中的全生命周期安全管理。

3. 安全生态

千寻位置提供的北斗精准时空服务不仅将面向数十亿自然人，更将面向未来数百亿甚至上千亿智能终端和无人系统，将成为 AIoT 时代的新基础设施。随着 2020 年北斗卫星增强系统形成全球服务能力，北斗高精度定位服务应用也将走向全球，千寻位置将与合作伙伴一起，推动基于北斗卫星导航系统的产业生态在全球范围内变得更加繁荣，充满活力。

3.1 业界交流

千寻位置作为一家深度融合应用互联网大数据运算的精准位置服务公司，充分重视互联网行业的资源整合，积极与行业内各家公司展开互动与交流，使公司的安全管理理念，安全服务能力以及安全防护水平，能够在安全技术迭代较快，新安全风险不断出现的情况下，与时俱进，不断提高，满足公司业务长期发展的需要。

公司与阿里云建立了深度合作和长效沟通机制。在提高自身安全防护能力和安全工作效率的同时，千寻位置作为云计算深度用户，依托并充分发挥了基础云平台产品特别是云安全产品的特性。

服务方式上，基础云平台为千寻位置提供 7*24 小时的紧急响应支持。千寻位置运维保障部、信息安全部与云平台安全产品团队建立了月度沟通机制，对平台安全产品和服务的持续优化交换彼此意见，定期复核安全事件，共同提升千寻位置服务在基础平台上的安全防护能力。

自千寻位置信息安全部成立以来，通过与基础云平台建立的长效沟通反馈机制，为平台安全及时反馈了众多改进需求、建议、产品缺陷（Bug），促进了整个云生态安全的发展。

3.2 产品生态

公司鼓励用户基于千寻位置 Open API 或产品 SDK 进行集成和开发，以便与用户实际应用场景无缝结合，享受更高品质的精准位置服务。千寻位置提供的 Open API 以及 SDK，从业务逻辑、鉴权保护、敏感信息屏蔽以及代码质量等方面，充分考虑整个业务应用过程中的安全性，构建精准位置服务的安全生态闭环。

公司提供的 Open API 及 SDK 在开发过程中，遵循 SDLC 的理念，在需求、设计、编码、验证和发布等各个阶段，都充分考虑其安全因素；同时产品充分考虑到用户场景的多样性和可变性，用户在使用的过程中，可以方便而安全的进行集成。

对于 SDK 需要与客户硬件深度集成的场景，公司开发人员和安全人员会与客户深度沟通交流，明确业务交互过程，识别潜在风险，并基于对双方的核心数据同时进行保护的原则，设计合理的实现方式，确保安全交付。

未来千寻位置还将提供面向物联网设备的更为便捷又安全的 OSS 协议（开放时空协议），助力万物互联的技术发展。

4. 安全合规与标准化

4.1 积极落实政策合规及体系建设

ISO/IEC 27001 信息安全管理体系是世界应用最广泛的信息安全管理标准。2017 年，千寻位置通过 ISO27001 国际体系认证；同步通过的认证还包括 ISO9000（质量体系）和 ISO20000（IT 服务管理体系）。

信息安全等级保护是由公安部监制，由属地公安机关认可并颁发的国家级信息系统安全等级认证。2018 年公司官方网站和 OA 系统通过安全测评，获得公安部上海网络安全总队颁发的信息系统安全等级保护备案证明。

公司按照《中华人民共和国网络安全法》、《中华人民共和国测绘法》、《测绘地理信息质量管理办法》等国家相关法律法规要求，同时结合 ISO27001、信息安全等级保护等国内外安全体系标准和规范，建立了覆盖信息安全方针、组织及人员安全、访问控制、通讯安全、系统安全、信息系统开发、信息安全事件管理、业务连续性管理和合规审计等 14 个控制域的安全管理体系。每个控制域建立了三级文档架构和可配置的度量体系，基本实现安全流程线上化，过程数据指标化，运营度量平台化，将安全落到实处，确保为广大用户提供高质、高效、安全可靠的产品和服务。

4.2 通过内控审计规避各类风险

信息安全管理体系的建设和运营是一个持续优化的过程。公司建立了定期内部审计机制，对安全管理工作的合理性、安全控制措施的有效性开展定量和定性结合的风险评估和安全审计。内部审计覆盖公司所有部门，并将信息安全策略要求全面推行，及时发现可能存在的安全风险，持续改进安全体系现状，以确保随着业务的发展和技术的演进，安全服务和安

全防护能力也能不断提升。

4.3 践行行业标准保障产品质量

作为 IoT 时代的重要基础设施，精准位置服务可以在不同行业、不同场景中得到有效应用，发挥其巨大价值。千寻位置致力于为客户提供优质、安全的产品和服务，充分考虑到典型的行业应用场景对安全的需求，在产品设计和研发中，始终坚持最高的标准和最优的产品实践。

千寻位置从产品需求导出，到设计研发和交付用户，全流程遵循行业内极其严苛的流程规范和技术标准。以车企合作为例，为了向车企行业提供安全可靠的精准位置服务，千寻位置主动在企业内部推动 ASPICE（Automotive Software Process Improvement and Capacity Determination， 是车载软件开发的过程标准，用于欧洲整车厂对供应商进行严格的软件过程评估，使软件产品和过程标准化。）高标准软件研发管理流程的落地执行。

ASPICE 是行业公认的严格的开发过程标准，为切实落地 ASPICE 相关要求，企业必须从各方面严格执行标准要求，建立并遵循企业内部流程（从产品需求到开发、设计、实现交付和作废），使用恰当的工具保障执行效率，如：需求管理统一通过系统维护，代码编写遵从 MISRA C 的标准规范，代码安全质量使用经过认证的安全工具进行静态和动态扫描，统一管理代码中使用的各类开源或免费代码组件等。

不仅如此，为保障精准位置服务全生命周期的产品功能安全，千寻位置还通过一系列质量检测和过程实践，积极满足 **IEC61508、ISO26262 等电子及汽车行业严苛标准对安全的要求**。IEC61508 是功能安全行业的总体标准，旨在提供各类机制和措施将系统性失效和随机性失效降到标准可接受的 SIL 等级内。ISO26262 电子及汽车行业的功能安全共识标准，也是最为严苛的功能安全标准之一，涵盖了整个产品设计的各个方面，包括系统设计、软件设

计、硬件设计等，并贯穿于整个产品的生命周期，从产品概念阶段一直到产品报废。

ASPICE、IEC6150 和 ISO2626 等标准规范的落地，需要企业持续运营和不断改进。千寻位置已经并将持续投入大量人力、财力等资源，用于改进内部研发流程，提升产品质量，保障产品安全，包括：建立制度规范、改进内部流程、促进研发质量、培训人员技能、问题跟踪反馈、持续改进优化等等。

5. 安全文化

信息安全是一个系统性工程，需要公司战略层面的支持，以及全体员工的集体参与。千寻位置在日常的运营管理过程中，充分遵循了这一原则。

5.1 安全组织

公司成立之初就充分认识到信息安全在公司长期业务发展中的战略地位以及对业务发展的支撑作用，设立了独立的信息安全部门，信息安全部门负责人直接向公司 CEO 汇报。同时，公司组建了信息安全管理小组，信息安全工作小组，信息安全内审小组等组织，确保信息安全从公司战略层面能够全局统筹，安全政策能够有效逐级传递，并最终将各项安全措施贯彻实施。

为了在数据资产管理、数据安全、数据治理、数据架构、数据需求满足等方面开展长效工作，除上述小组之外，公司还成立了专门的数据工作小组，确保数据能安全高效地支撑公司业务发展。

5.2 人员安全

千寻位置重视员工对企业发展的影响和贡献，充分认识到人员安全在整体信息安全以及公司战略层面的重要性，在招聘、入职、培训、离职等流程，采取多种方式，确保所有成功入职的候选人品行端正，具备良好的职业道德和素养，符合千寻位置的价值观，满足整体信息安全要求和业务发展的战略需要。

新员工入职须签订保密协议，学习员工守则，阅读新人入职安全手册，观看商业行为准则视频，参加信息安全知识培训，并且通过数据安全考试。

在日常的工作过程中，公司通过《数据安全规范》、《信息安全奖惩管理制度》、《员工信

息安全手册》等规范员工的行为，并定期开展信息安全培训；对研发、测试部门，单独开展专项安全培训，确保所有员工都能充分理解和应用安全防护技术，遵循公司的信息安全政策。

员工离职环节，公司通过完善的离职管理流程，回收员工的信息资产，并对离职员工所拥有的账号权限进行关闭；对于关键岗位，视情况签署竞业协议并开展离职重点审计。

5.3 社会责任

随着万物互联时代的到来，物联网行业正呈现出爆发式增长态势，根据工信部的数据，到 2020 年，全球的 IoT 终端连接数预计将达到约 500 亿，并且该数字将在未来持续增长；这些 IoT 终端要更好地服务于人类的生产生活 ，就需要精准的时空信息。

千寻位置以卫星定位为基础，融合各类定位技术，针对特定的应用场景，不同的应用终端，推出与实际场景相结合的解决方案，向各类终端和应用系统提供精准位置服务；分享对位置相关的海量数据接入、存储、融合和开放的能力，为企业和开发者的集成开发、应用推广提供一站式的服务支撑；让精准位置服务成为连接、激活和驱动 IoT 生态发展的重要基础设施，这正是千寻位置的产品初衷和社会责任。

此外，千寻位置还承担着国家北斗地基增强系统“全国一张网”的安全建设运营，国家北斗相关产业的技术实践和应用推广的重大使命。这使得确保精准位置服务的可靠和安全，成为社会责任的重要内涵。

6. 总结

千寻位置网络有限公司在“控制企业安全风险，保护企业信息安全； 切实保障位置服务高可用；促进企业战略和业务目标的实现”的信息安全总体方针指引下，从人员、技术、管理、流程等多个方面全面推进信息安全政策的落地，履行监管合规义务，同时积极探索新技术，推进安全自动化、智能化，实现安全防护能力高效输出。

在当前日趋复杂的互联网环境下，技术迭代周期愈发短暂，新型攻击手段层出不穷，我们每时每刻都在面临各类安全威胁。为保障精准位置服务的持续高可用，捍卫未来时空基础设施安全，千寻人恪尽职守，时刻待命。

千寻位置，助力人类触摸无所不在的精准时空。