LianLian Pay 连连

连连银通电子支付有限公司
信息安全白皮书

信息安全管理部

2019 年 7 月

V1.0

版权声明

本文档著作权归连连银通电子支付有限公司所有，未经连连银通电子支付有限公司事先书面许可，任何主体或个人不得以任何形式复制、修改、摘抄、翻译、传播全部或部分本文档内容。

商标声明

本文档所涉及的所有商标均为连连银通电子支付有限公司所有。

法律声明

由于监管政策变化、产品升级、技术调整或其他原因，本文档内容有可能变更。连连银通电子支付有限公司保留在没有任何通知或者提示下对本文档的内容进行修改的权利。

本文档未授予读者任何连连银通电子支付有限公司产品或服务的任何知识产权的法律权利。

前 言

连连银通电子支付有限公司（以下简称“连连支付”）成立于 2003 年，是一家持照的第三方支付机构。多年来，始终坚持：严格遵从监管要求、参照业界最佳实践、结合公司业务发展的实际需要，建立了一套目前正在有效运行并坚持持续改进的信息安全管理体系。

本白皮书就是这套信息安全管理体系的概要介绍，主要内容包括：

- 连连支付信息安全战略
- 连连支付信息安全风险管理框架
- 合规和隐私保护
- 安全责任与承诺
- 基础安全
- 安全运营管理

目 录

01

概述

1.1 连连支付信息安全战略

连连支付以数据安全保护为核心，以金融科技服务为依托，以法律法规、监管要求、业界标准遵从为基础，构建起纵深防御的信息安全保障体系，并将其作为连连支付信息安全发展战略。

“落实安全管控责任，规避与降低安全风险，保障业务安全运行，依法依规保护客户隐私”是连连支付信息安全管理方针；安全措施覆盖物理环境控制、访问控制、配置管理、应急响应、安全审计、持续监控、供应商等多个环节，提供多维度的安全防护；确保公司数据资产的保密性、完整性和可用性，保障业务安全与可持续发展。

- 落实安全管控责任

信息安全管理的关键要点在于：落实各项安全管控要求和技术措施；依据行业最佳实践和各项安全标准，不断完善自身的管理与机制；明确业务部门和 IT 部门的信息安全分工和岗位职责；将各项安全控制落到实处，做到有流程、有规范、有工具、有检查、有改进。

同时，通过一系列的标准认证以及定期的第三方安全评估和审计，确保持续向用户提供合规、安全、稳定的支付服务。

- 规避与降低安全风险

信息安全管理目标在于最大化降低安全风险，信息安全管理指导思想在于将信息安全事件损失控制到可接受的程度，树立预防为主、事前防范、事中监控和事后复核的管理思路。从底层架构到应用策略，从计算、网络、存储、数据库、应用、物理环境等领域，建立适应公司业务发展需要的信息安全控制能力。

- 保障业务安全运行

业务安全是信息安全保障的核心，始终围绕业务的要求，采取技术保障措施，确保在紧急情况下业务的连续稳定运行。

- 依法依规保护客户隐私

将保护客户隐私作为底线，在客户授权的前提下，基于业务的需要，依规收集、保存和使用客户隐私信息。同时，从制度上、技术上、员工及客户教育等多个角度，采取行之有效、系统化的手段，保护客户隐私信息的安全。

连连支付信息安全框架可参见图 1：

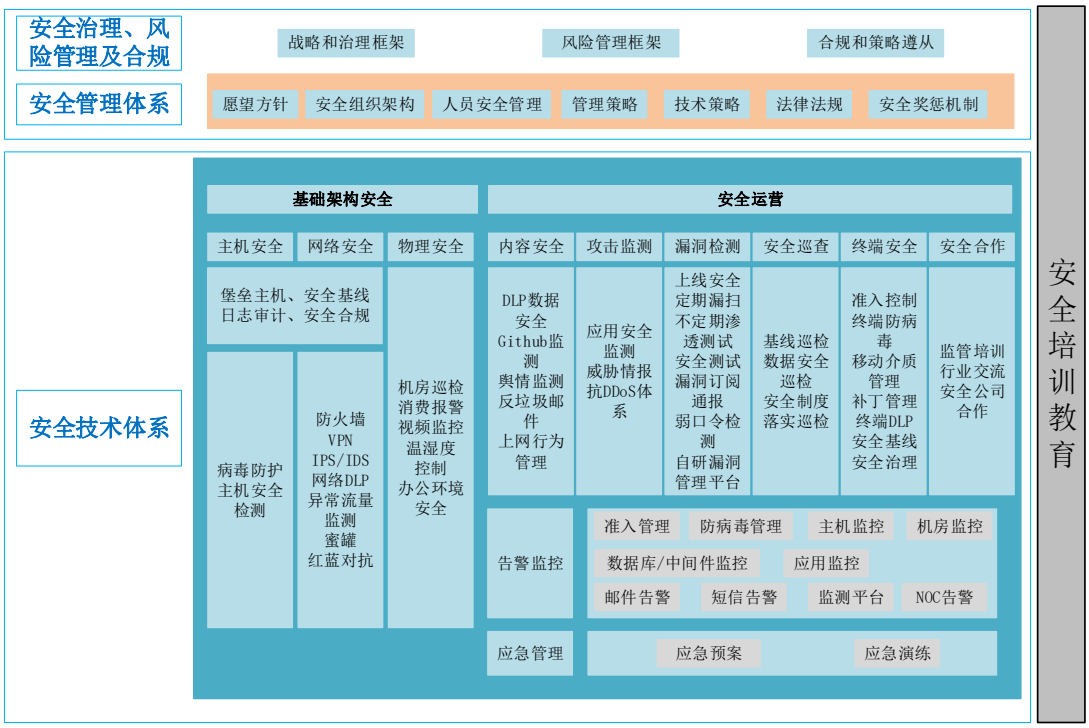

图 1：连连支付信息安全框架

1.2 连连支付风险管理框架

信息安全是企业业务安全开展的保护伞，包括：人员安全，如人员背景调查、保密协议等；物理安全，如机房物理环境、人员出入审核登记、环境视频监控等；信息系统安全，如信息系统基础架构安全、安全管理工具和安全管理制度等。

业界一致认为，不存在绝对的安全。有些风险可以避免，有些风险可以降低、转移，而有些则是只能接受。好的风险管理体系能帮助组织更好地了解风险，并且处理好风险。连连支付根据行业内最佳实践和行业标准，结合实际业务情况制定并实施风险管理架构。

同时，制订了《风险评估管理规定》，以规范信息安全风险识别、评估和风险处置的工作流程，及时发现并降低或规避风险。

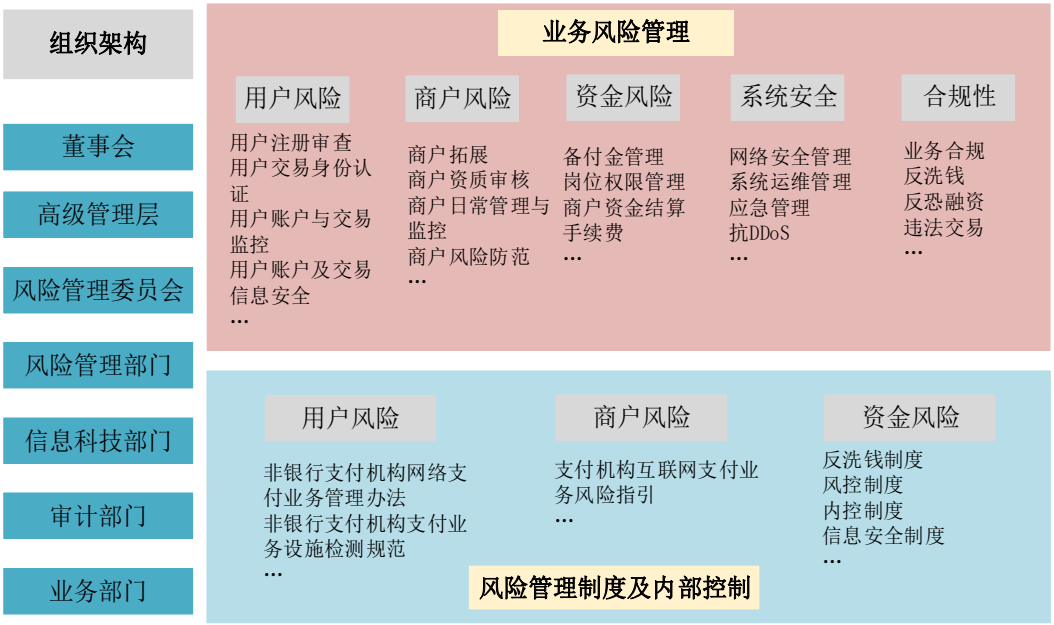

图 2：连连支付风险管理框架

02

合规和隐私保护

合规和客户隐私保护，是支付服务的基础保障。连连支付通过安全认证机构的审核以及业界权威组织或行业监管的测评，确保提供的支付服务安全、可靠；并从组织、流程、技术等多个方面有效落实安全策略及风险管控措施；持续地做好客户隐私保护和支付业务的安全保障。

2.1 安全合规

连连支付目前已获得的资质认证，包括：

- ISO9001：2015 质量管理体系认证（ISO9001:2015 Quality Management Systems ）；

  ISO9001 是在全世界范围内通用的关于质量管理和质量保证方面的系列标准，用于证实组织具有提供满足顾客要求和适用法规要求的产品的能力。通过认证，证明被检测方在各项管理系统整合上已达到了国际标准，表明企业能持续稳定地向顾客提供预期和满意的合格产品。

- ISO/IEC27001：2013 信息安全管理体系认证（ISO/IEC 27001:2013 Information

Security Management Systems）；

ISO27001 是信息安全领域的管理体系标准，是世界上应用最广泛与典型的信息安全管理标准，可有效保护信息资源,保护信息化进程健康、有序、可持续发展。通过认证，证明被检测方能保证和证明其所有的部门对信息安全的承诺。

- ISO/IEC 20000-1：2011 信息技术服务管理体系认证（ISO/IEC 20000-1:2011 Information Technology -- Service Management Systems）；

  ISO20000 即信息技术服务管理体系，是面向机构的 IT 服务管理标准，其目的在于提供建立、实施、运作、监控、评审、维护和改进 IT 服务管理体系(ITSM)的模型。通过认证，证明被检测方已建立了规范的服务流程，不断提供信息技术服务和运营效率，快速应对市场需求，提供客户满意度。

- PCI DSS：支付卡行业数据安全标准合规认证（Payment Card Industry (PCI) Data Security Standard (DSS)）；

  PCI DSS 全称是第三方支付行业(支付卡行业 PCI DSS)数据安全标准，致力于使国际上采用一致的数据安全措施，它对于所有涉及信用卡信息机构的安全方面作出标准的要求，全面保障交易安全。通过认证，证明被检测方对持卡人数据进行严格的保护，从安全管理、策略、过程、网络体系结构、软件设计等全方面对持卡人数据进行保护，确保交易安全。

- ADSS（UPDSS）：银联卡账户信息安全外部合规评估认证（Account Data Security Standard）；

  ADSS 是银联卡收单机构账户信息安全管理标准，由中国银联风险管理委员会审核通过，旨在加强银联卡收单网络账户信息安全管理，进一步明确和细化对收单业务各参与方账户信息安全管理要求，防范账户信息泄漏风险。通过认证，证明被检测方对于银行卡信息和持卡人资料的使用、存储的保护已经通过银联认可的防护标准，可有效防范账户信息泄漏风险。

- 中华人民共和国公安部“信息安全等级保护三级”（Classified Protection of Information System Security: Level Three）。

  信息安全等级保护，是对信息和信息载体按照重要性等级分级别进行保护的一种工作，主要验证信息系统是否满足相应安全保护等级，由公安部监制，由属地公安机关认可并颁发。通过认证，证明被检测方从技术措施、管理制度、以及员工安全意识教育水平已达到了公安部认可标准。

2.1.1 ISO9001 认证

质量管理体系认证证书

证书编号：19817QB067R0M
统一社会信用代码/组织机构代码：91330000751728692l

兹证明：

连连银通电子支付有限公司

质量管理体系符合：GB/T19001-2016 idt ISO9001:2015

证书覆盖范围：互联网支付、移动电话支付的相关服务及系统研发

注册地址：杭州市滨江区越达巷 79 号 1 号楼 11 楼
经营地址：杭州市滨江区越达巷 79 号 1 号楼 11 楼

首次发证日期：2017 年 02 月 28 日
本次换证日期：2019 年 03 月 05 日
证书有效日期：2020 年 02 月 27 日

中国认可
国际互认
管理体系
MANAGEMENT SYSTEM
CNAS C178-M

北京新纪源认证有限公司 证书专用章

签发：

本证书在国家规定的各行政许可、资质许可有效期内使用有效
获证组织必须定期接受监督审核并经审核合格后，方可使用证书有效性
证书有效性可通过新纪源网站www.x.jyrz.com查询或国家认监委网站www.cnca.gov.cn查询，也可通过扫描二维码查询

北京新纪源认证有限公司
地址：北京市朝阳区南湖东园122楼11层北区1201（邮编100102）

图 3：ISO9001 证书

2.1.2 ISO27001 认证

DNV·GL

管理体系认证证书

子证书号码:
264077CC1-2018-AIS-RGC-UKAS
主证书号码:
264077-2018-AIS-RGC-UKAS

首次签发日期:
2018 年 06 月 21 日

有效期限:
2018 年 06 月 21 日 - 2021 年 06 月 21 日

兹证明

连连银通电子支付有限公司

中国浙江省杭州市滨江区越达巷 79 号 1 号楼 10 楼&11 楼

信息安全管理体系符合:

ISO/IEC 27001:2013 标准

此证书对下列产品或服务范围有效:

信息安全管理体系包括第三方支付平台设计、开发和维护；上述服务的基础设施，同最新适用性声明保持一致（V2.0）

证书签发地点及日期:
上海, 2018 年 06月22日

UKAS MANAGEMENT SYSTEMS
0013

证书认可签发机构:
DNV GL – Business Assurance
中国上海市长宁区虹桥路1591号9号楼A座
邮编: 200336 电话: +86 21 32799000

Zhu Hai Ming
管理代表

未履行认证协议中规定条款会导致此证书失效
获得认可的单位: DNV GL Business Assurance UK Limited, 30 Stamford Street Vivo Building, 4th Floor, SE1 9LQ London, United Kingdom. TEL:+44(0) 207 357 6080. www.dnvgl.com

图 4：ISO27001 证书

2.1.3 ISO20000 认证

DNV·GL

管理体系认证证书

子证书号码:
264079CC1-2018-AQ-RGC-UKAS
主证书号码:
264079-2018-AQ-RGC-UKAS

首次签发日期:
2018 年 06 月 21 日

有效期限:
2018 年 06 月 21 日 - 2021 年 06 月 21 日

兹证明

连连银通电子支付有限公司

中国浙江省杭州市滨江区越达巷 79 号 1 号楼 10 楼&11 楼

信息技术服务管理体系符合:

ISO/IEC 20000-1:2011 标准

此证书对下列产品或服务范围有效:

信息安全管理体系包括第三方支付平台设计、开发和维护；上述服务的基础设施，同最新适用性声明保持一致（V2.0）

证书签发地点及日期:
上海, 2018年 06月22日

APMG International ISO/IEC 20000 CERTIFIED ORGANIZATION

UKAS MANAGEMENT SYSTEMS 0013

证书认可签发机构:
DNV GL – Business Assurance
中国上海市长宁区虹桥路1591号9号楼A座
邮编: 200336 电话: +86 21 32799000

Zhu Hai Ming
管理代表

未履行认证协议中规定各款会导致此证书失效
获得认可的单位: DNV GL Business Assurance UK Limited, 30 Stamford Street Vivo Building, 4th Floor, SE1 9LQ London, United Kingdom. TEL:+44(0) 207 357 6080. www.dnvgl.com

图 5：ISO20000 证书

2.1.4 PCI DSS 认证

the information security provider

Attestation of Compliance for PCI QSA Assessments

No.: atsec-2019-PCI-DSS-C-01293-02024

This is to certify that:

Lianlian Yintong Electronic Payment Co., Ltd.

Has been assessed and validated according to the following payment card industry standard:

Payment Card Industry (PCI) Data Security Standard (DSS) Requirements and Security Assessment Procedures

Version 3.2.1, May 2018

Service(s) assessed: Internet payment acquiring service

Office location: 11/F, Lianlian Tower A, 79 Yueda Lane, Hangzhou, Zhejiang Province, P.R.China

Data center location: No.10, Taiyangshan Road, Changkou Town, Fuyang District, Hangzhou, Zhejiang Province, P.R.China

Data center location: A2, Creative Industry, No.328, Xinghu Street, SIP Suzhou Industrial Park, Suzhou, Jiangsu Province, P.R.China

Assessment Scope:
Sensitive authentication data (CAV2/CVC2/CVV2/CVN2) and cardholder data (PAN, expiration and cardholder name) are securely transmitted over Internet with strong cryptographic HTTPS interface. Once internal payment processes are completed, cardholder data and sensitive data are transmitted to payment processors over leased lines. PANs, cardholder name and Expiration date are stored in the local database servers for reconciliation business purpose, and these stored cardholder data are protected via strong cryptography. Sensitive authentication data (CAV2/CVC2/CVV2/CVN2) are held in the VRAM and purged immediately after authorization. No sensitive authentication data are stored in the cardholder data environment.

Date of Issue: June 5, 2019
Date of Initial Compliance: April 27, 2015
Date of Expiry: April 26, 2020

ATSEC (BEIJING) INFORMATION TECHNOLOGY CO., LTD. 艾特赛克(北京)信息技术有限公司

LiuYan
PCI Laboratory Director

atsec (Beijing) Information Technology Co., Ltd

Tel: +86 10 53056681
Fax: +86 10 53056678
Email: info_cn@atsec.com
www.atsec.cn

The validity of this attestation can be verified through the above website.
Refer to Report on Compliance (ROC) for the compliance and assessment details.

图 6：PCI DSS 认证

2.1.5 ADSS（UPDSS）认证

证书编号 Certificate NO.: BCTC-UPDSS201901290001

银行卡检测中心
Bank Card Test Center

银联卡支付信息安全合规证书

CHINA UNIONPAY UPDSS CERTIFICATE

兹证明,连连银通电子支付有限公司的银通支付平台系统（V1.2）符合《银联卡支付信息安全管理标准》（银联风管委〔2018〕3号）要求。特发此证。（最终结果以合规评估报告为准）

This is to certify that Yintong Payment System V1.2 of Lianlian Yintong Electronic Payment Co., Ltd. has been assessed and approved as in compliance with the requirements of UnionPay Payment Data Security Management Standard (Risk Management Committee of China UnionPay (2018) No.3). (The Certificate is based on the report)

合规评估报告编号：SYDS18F1Q1TP　　评估完成日期：2019年1月23日
Report No.: SYDS18F1Q1TP　　Completion Date: 2019/1/23

证书签发地点及日期：北京 2019年1月29日
Issuing Address & Date: Beijing 2019/1/29

证书有效期：2020年1月28日
Expiry Date: 2020/1/28

评估机构：银行卡检测中心（UPDSS-I0001）
Approved by: Bank Card Test Center (UPDSS-I0001)

声明：本证书仅用于证明被评估单位在本次评估完成时符合 UPDSS 要求。合规评估报告详细记录了本次评估的结果。如被评估单位系统发生变更或升级造成变化，应根据 UPDSS 有关要求重新评估。

DISCLAIMER: THE CERTIFICATE SOLELY INDICATES THE COMPLIANCE STATUS OF THE ASSESSED ORGANIZATION WHEN THE ASSESSMENT IS COMPLETED. THE DETAILS OF THIS ASSESSMENT WERE RECORDED IN THE COMPLIANCE REPORT. THE ASSESSED ORGANIZATION SHALL BE ASSESSED AGAIN ACCORDING TO UPDSS REQUIREMENTS IF ANY CHANGES OCCUR ON ITS SYSTEM.

图 7：UPDSS 证书

2.1.6 信息安全等级保护三级认证


信息系统安全等级保护
备案证明

依据《信息安全等级保护管理办法》的有关规定，连连银通电子支付有限公司 单位的：

第 三 级 移动电话支付（远程支付） 系统予以备案。

证书编号： 330117-13054-00002

中华人民共和国公安部监制

备案公安机关公章

2019 年 03 月 06 日

图 8：信息系统安全等级保护三级证书

2.2 其他荣誉资质

2.2.1 全国信息安全标准化技术委员会成员单位

连连支付已加入全国信息安全标准技术委员会，参与信息安全国家标准化建设工作，参与编写和评审国家信息安全标准，是对连连支付信息安全能力的肯定，同时在参与标准化工作过程中，了解国家信息安全标准建设的方向，及时掌握标准相关内容要求，同时有效地落实标准要求。

图 9：全国信息安全标准技术委员会成员单位

2.2.2 浙江省计算机信息系统安全协会常务理事单位

浙江省计算机信息系统安全协会，是由浙江省公安厅主管，由从事信息网络安全领域研究、科研与教育人士、信息管理机关、信息服务部门和计算机信息安全产品生产、服务单位，计算机使用单位等自愿参加的具有独立法人的非营利性的行业自律社会团体。连连支付作为其常务理事单位， 积极宣传贯彻国家计算机信息系统安全管理的有关法律法规和政策，提高计算机使用单位和用户的安全防范意识和安全保护水平并协助政府的计算机安全管理部门制定地方性的有关规范。

图 10：浙江省计算机信息系统安全协会常务理事单位

2.2.3 浙江省网络空间安全协会理事单位

浙江省网络空间安全协会是由浙江省网信办主管，由关键信息基础设施网络运营者、网络安全企业级研究机构、高等院校、媒体机构和网络安全领域相关专家学者等共同发起成立。连连支付当选为首届理事单位，助力浙江省数字经济快速健康发展。

2.2.4 杭州市网络安全协会理事单位

杭州市网络安全协会性质是由杭州市内的从事信息网络安全领域研究、科研与教育人士、信息网络管理机关、信息服务部门和计算机信息网络安全专用产品生产、服务单位，业务主管部门是杭州市公安局；作为杭州市网络安全协会理事单位，连连支付积极参与开展计算机信息网络安全学术交流活动，研究和提供计算机信息网络安全技术、法律和管理措施，提高网络用户的安全意识；协助主管机关规范和加强计算机安全保护工作，促进社会信息化的健康发展。

2.2.5 国家信息安全漏洞共享平台（CNVD）

连连支付注重技术安全防控，持续投入信息系统安全漏洞研究工作，关注信息系统及国产软件的安全性。通过国家信息安全漏洞共享平台上报挖掘的漏洞信息，多次获得国家信息安全漏洞共享平台颁发的原创漏洞证书。

注：国家信息安全漏洞共享平台（China National Vulnerability Database，简称 CNVD）是由国家计算机网络应急技术处理协调中心（中文简称国家互联应急中心，英文简称 CNCERT）联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的国家网络安全漏洞库。

图 11：国家信息安全漏洞共享平台原创漏洞证明

2.3 隐私保护

连连支付采用基于业界高标准的安全防护措施确保用户隐私安全，包括建立合理的制度规范、安全技术来防止用户的个人信息遭到未经授权的访问、使用、修改，避免数据的损坏或丢失。保护用户对于个人信息访问、更正、删除以及撤回同意的权利，使用户拥有充分的个人信息自主权，同时保障其隐私和安全。

2.3.1 信息的采集

只以具体、明确、合法合规的目的收集个人信息，这些信息在与信息主体、所有者或提供者之间的协议中予以明确说明。用户授权同意后，连连支付才会采集业务所需的个人信息。采集原则：

- 根据最小需求和授权使用原则，连连支付仅收集能够满足业务开展所需的信息；

- 采用已告知的手段和方式向用户收集，不采取隐蔽手段收集用户信息；
- 采集用户信息前征得用户的明示同意；
- 与个人信息的收集和使用有关的所有过程和通告，以及对此类过程或任何所收集数据类型的任何变更，均须经过连连支付合规管理部、法务部、内部控制部、信息安全管理部等部门的审查和批准，确保信息采集的合法合规性。

2.3.2 隐私保护政策

连连支付风险管理部、法务部、信息安全管理部等多个部门组成法规解读小组，小组成员基于法律法规要求制定隐私保护政策，经小组评审后发布实施。

为确保隐私保护政策适用性，法规解读小组适时分析法律法规，定期组织差距分析，落实法规要求，审视隐私策略内容，组织评审更新。

03

安全责任

3.1 信息安全责任

连连支付致力于为客户提供安全稳定的支付服务，夯实安全责任，牢守安全底线：遵循法律法规、行业监管和内部管控要求；满足信息风险控制、数据安全和隐私保护要求；遵从组织的业务战略和安全战略；满足利益相关方需求。

3.2 信息安全承诺

连连支付坚持以公平和透明的方式提供产品和服务；在整个支付周期中实施真实性、公平性和不歧视文化的客户服务承诺。建立和实施相关制度；通过专门的资源、持续的监控、测试及监督；管理和减轻客户可能面临的安全风险，以保护客户的利益和权益。

04

基础安全

4.1 基础设施安全

连连支付业务基础设施依据行业最佳实践以及安全合规标准进行设计和管理，包括：机房、网络、硬件和支持这些资源的软件。

数据中心采用两地三中心的模式，达到应用级冗余及数据同步：关键数据实时同步、备份；通过专线连接合作机构，实现双线冗余；为用户提供高可用、安全、可信的基础设施。执行严格的数据中心巡检标准、设备准入标准以及人员进出管理标准，以保证整个支付业务基础设施的高可用性及安全性，提供不低于 99.99%的可用性保障。

连连支付数据中心架构可参见图 12：

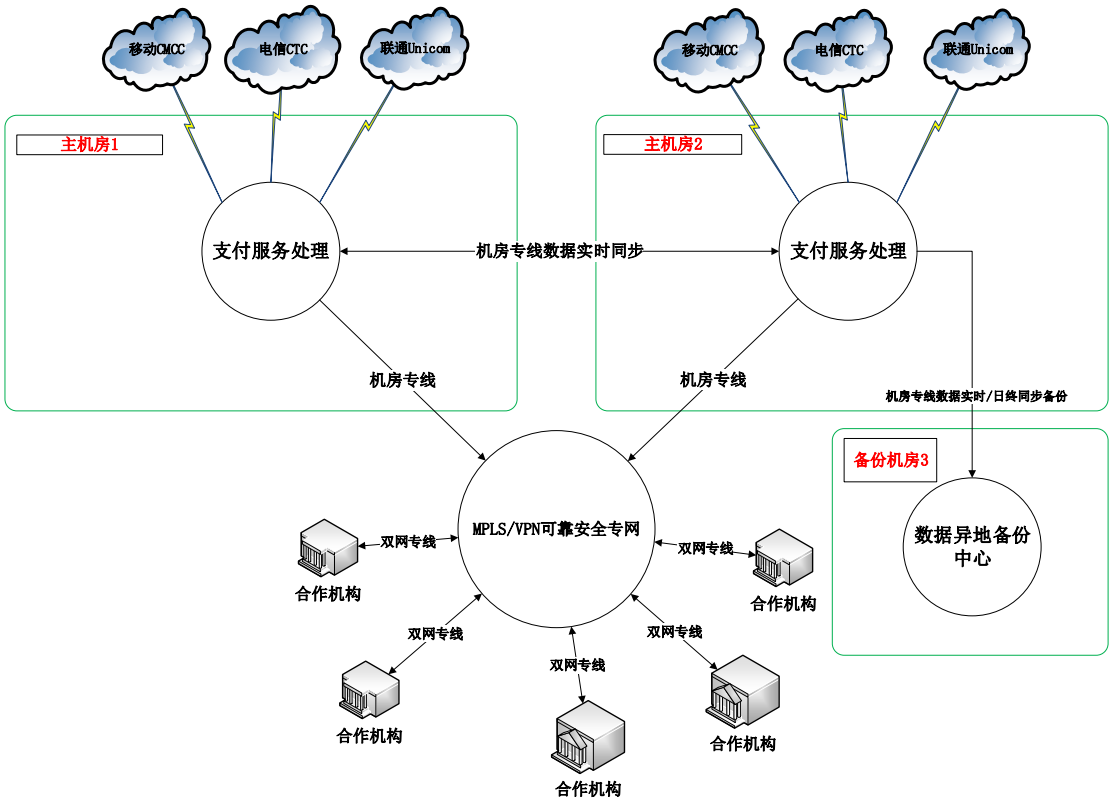

图 12：连连支付数据中心架构

4.2 物理环境安全

4.2.1 数据中心

连连支付的数据中心部署在国际 T4 等级（国际最高标准）和 T3+等级机房，比普通服务器机房具备更高的可用性和抗灾能力，达到银行级安全标准。

制定完善的物理环境安全防护策略、规程和措施，在数据中心里包含多级的安全保护措施，包括：

- 使用独立的双路高压供电和双路 UPS 电源，并配置柴油发电机，确保 99.99%以上的电力持续供应率；
- 采用先进的精密空调系统，保证机房的温度在 24 摄氏度正负 2 度，湿度在 50%RH 正负 10%RH，并对机房进行 7*24*365 的恒温恒湿环境监控；
- 配置了独特设计的专业消防系统，采用先进的烟感报警器和环保型气体灭火设备，保证在第一时间发现火灾隐患；
- 配备符合国家及行业标准的计算机安全防护系统，对整个网络和客户的主机进

行严密的保护；

- 采用实时摄像装置、远红外热源探器对所有机房区域进行全程、全方位的监控和录像；
- 配备多重门禁系统，采用计算机控制的电子感应锁及密码系统，自动识别进出人员身份，并且记录其进出时间；
- 建立了完整的人员访问控制安全矩阵，并配有专业运维团队进行 7*24 不间断机房巡视及门卫监控。

4.2.2 办公环境

为营造安全可控的办公环境，我们制定了办公场所安全管理规定，办公区出入口设立安保接待，对访客进出公司办公区进行管理。

4.3 系统&网络安全

连连支付具备可靠的网络安全架构及多层防护的安全方案：对生产网络与非生产网络进行物理隔离；同时提供可靠的网络基础结构以支持支付业务和服务连接需求；通过严格的审核机制以及上线流程来保证受信程序或端口的安全访问。

安全工程师每季度执行内部以及外部网络安全扫描测试以主动发现可能存在的网络隐患。同时采购安全服务，协助发现外部安全风险，如安全众测服务和渗透测试服务。

4.3.1 安全域划分

连连支付准照《非金融机构支付业务设施技术要求》规定，对网络进行区域划分，并对不同级别的安全域进行管控，各区域间划分单独 VLAN、同时部署防火墙进行访问控制和安全防护。

各安全域间互联时，基于网络维护成本及性能影响，采用合适的网络路由及网络设备访问控制策略，定期审阅和修改。根据网络设备用途或其使用者的工作内容分配适当的网络区域 IP，以便对网络使用的控制管理。

4.3.2 网络访问控制

网络区域间实施缺省拒绝的访问控制策略，只允许指定条件下的网络访问。所有的用户接入请求均通过严格配置的 NAT 策略实现，所有的维护请求均通过独立网络经由 DMZ 完成，对网络的出口处通过端口镜像的方式来甄别各种网络威胁。

4.3.3 Linux 操作系统安全基线

连连支付根据 Linux 操作系统的安全特性，参考《支付卡行业数据安全标准 V3.2》、《JR/T 0123.1-2018 非银行支付机构支付业务设施检测规范》、《JR/T 0071-2012 金融行业信息系统信息安全等级保护实施指引》、《JR/T 0072-2012 金融行业信息系统信息安全等级保护测评指南》、《JR/T 0073-2012 金融行业信息安全等级保护测评服务安全指引》等相关规范要求，制定《Linux 操作系统安全基线配置规范》，从身份鉴别、访问控制、安全审计、入侵防范、资源控制、防恶意代码等方面进行规范要求，用于指导安全例行工作、新系统入网安全检查等，确保公司的 Linux 系列操作系统安全。

4.3.4 Windows 操作系统安全基线

连连支付依据目前 Windows 操作系统的安全现状，参考《支付卡行业数据安全标准 V3.2》、《JR/T 0123.1-2018 非银行支付机构支付业务设施检测规范》、《JR/T 0071-2012 金融行业信息系统信息安全等级保护实施指引》、《JR/T 0072-2012 金融行业信息系统信息安全等级保护测评指南》、《JR/T 0073-2012 金融行业信息安全等级保护测评服务安全指引》等相关规范要求，制定《Windows 2008 操作系统安全基线配置规范》，从身份鉴别、访问控制、安全审计、入侵防范、资源控制、防恶意代码等方面进行规范要求，用于指导安全例行工作、新系统入网安全检查等，确保公司的 Windows 系列操作系统安全。

4.3.5 安全设备基线

连连支付参考《支付卡行业数据安全标准 V3.2》、《JR/T 0123.1-2018 非银行支付机构支付业务设施检测规范》、《JR/T 0071-2012 金融行业信息系统信息安全等级保护实施指引》、《JR/T 0072-2012 金融行业信息系统信息安全等级保护测评指南》、《JR/T 0073-2012 金融行业信息安全等级保护测评服务安全指引》等相关规范要求，制定《安全设备配置基线》，从身份鉴别、安全审计等方面进行规范要求，用于指导安全例行工作、新系统入网安全检查等，确保公司的设备安全。

4.3.6 DDos 防护

针对 DDoS 攻击，连连支付采用三层架构进行深度防御：第一层，采用电信云堤清洗方案进行近攻击源清洗，如在广东省发起的 DDoS 攻击，借助电信的广东清洗节点在当地进行清洗，其他省份同理；第二层，采用阿里云高防进行清洗；第三层，采用 IDC 机房本地硬件抗 DDoS 设备进行近目的清洗。

以上三层防御体系能够抵御各类基于网络层、传输层以及应用层的 DDoS 攻击，并通过安全运营后台实时掌握网络攻击趋势及防御状态。

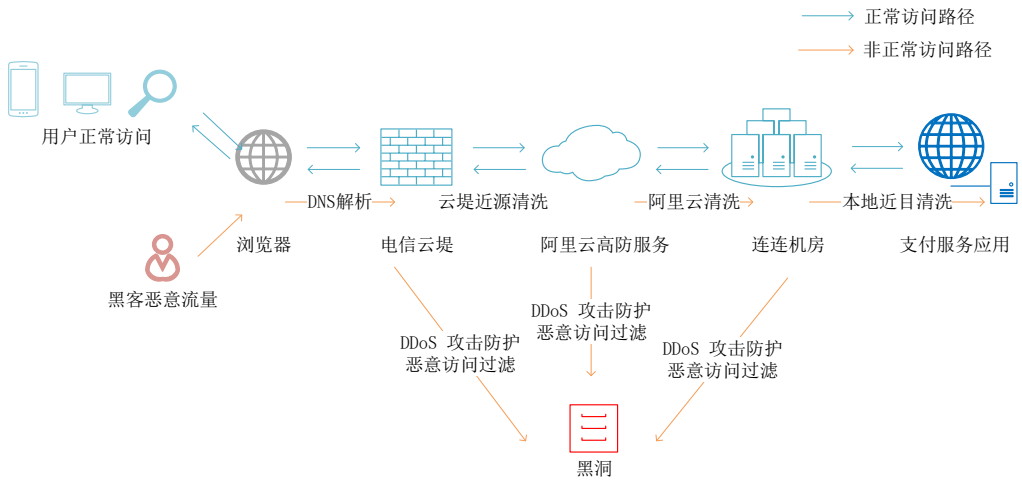

图 13：连连支付 DDos 防御体系

4.3.7 网络攻击防御

连连支付使用专业的安全工具、平台，对内外部网络端口进行监控，根据检测网络并发数，设置阈值，一旦超过预设阈值立即采取相关防护措施，包括但不限于封锁对应 IP 地址，加入黑名单等。同时对该异常行为进行分析判断，基于分析结果采取进一步的防护措施。

另外，系统日志分析也是连连支付网络攻击防御的一个重要手段，通过对系统日志的及时解析，做到异常行为提前预警防范，降低网络攻击风险。

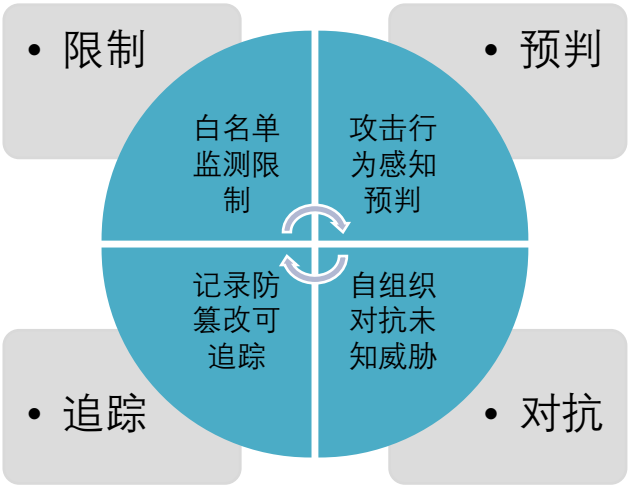

图 14：连连支付网络攻击防御体系

4.3.8 传输安全防护

连连支付使用 HTTPS 安全协议，建立了信息安全通道以保证数据传输的安全。使用行业标准传输层安全协议 SSL/TLS 加密，保护传入、传出以及在内部传输的数据。认证用户和服务器，确保数据发送到正确的客户机和服务器；加密数据以防止数据中途被窃取；维护数据的完整性，确保数据在传输过程中不被改变。

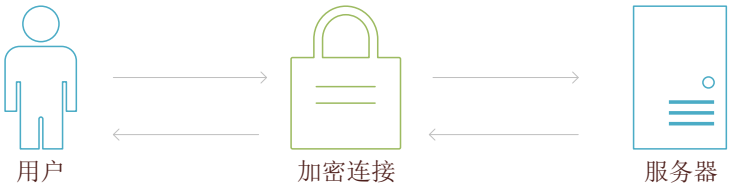

图 15：连连支付传输安全防护

4.3.9 交易报文安全

连连支付对所有交易信息加入签名机制，保障客户与连连支付之间消息来往的安全性。采用 RSA 和 SM2 加密方式算法实现，签名密钥（私钥）用于签名，验签密钥（公钥）用于验签。当接收方的期待串与签名原串一致时，校验成功；否则校验失败。在客户与连连支付的交易中，主要会使用到用户公私钥与连连支付公私钥两对公私钥对。

用户公私钥：用于用户向连连支付发送请求时的加签与验签。该公私钥由用户自己生成，其中，私钥用于对用户发往连连支付的数据签名，自己保存；公钥需要提交给连连支付，当收到您发来的数据时用该公钥验证签名。

连连支付公私钥：用于连连支付向用户发送通知或者响应时的加签与验签。

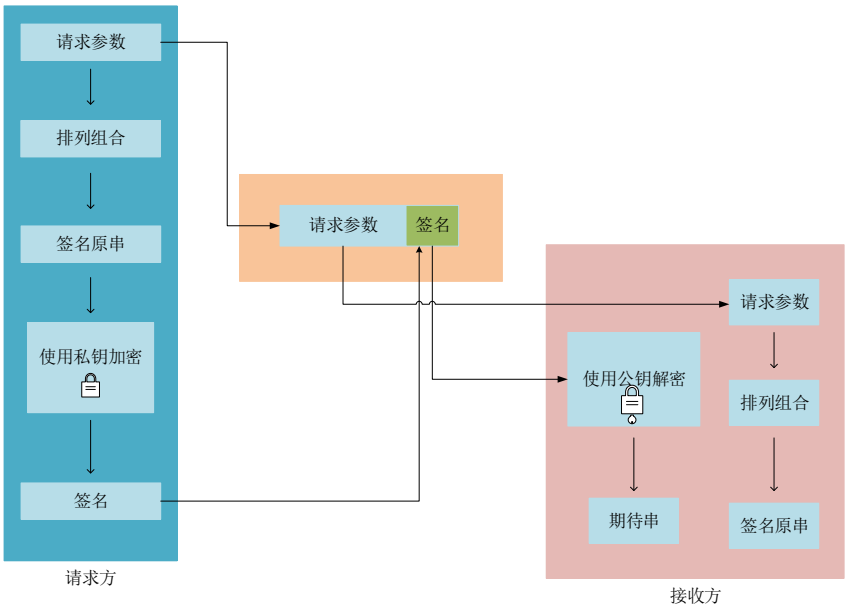

图 16：连连支付交易报文安全防护体系

4.3.10 安全蜜罐管理

主动防御是连连支付在网络攻击防御环节的一大特点，采用网络蜜罐系统，伪装存在安全缺陷的主机、网络服务或者信息形成蜜网，从而对攻击行为进行捕获和分析，了解其所使用的工具与方法，推测攻击意图和动机，进一步加强内部安全建设，增强主动安全防护能力。

4.4 应用安全

4.4.1 安全开发规范

为保障应用程序使用过程和结果的安全，连连支付制定了《系统获取、开发和维护管理办法》，确定严格的系统开发生命周期管理，从系统需求分析、设计、开发、测试、发布、运维到系统下线各个环节进行安全管理。

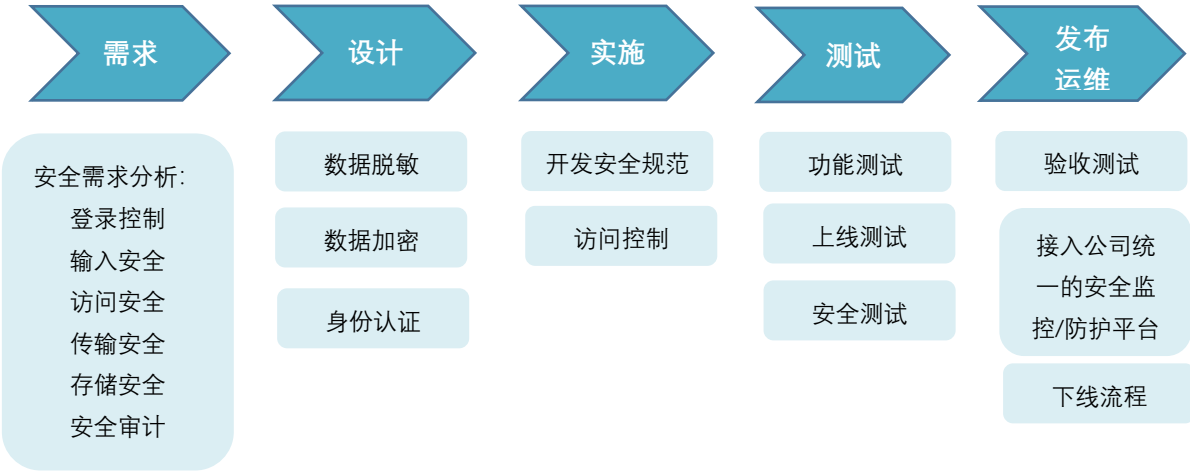

图 17：连连支付系统开发生命周期

4.4.2 应用安全扫描

为确保内部应用安全，除对内部应用开展上线前的安全测试、及时发现应用漏洞并确保修复外，连连支付还会不定期对应用安全进行扫描，对系统中不合适的设置或其它同安全规则抵触的对象进行检查，或通过执行一些脚本文件模拟对系统进行攻击的行为并记录系统的反应，尤其针对 SQL 注入、跨站攻击、信息泄露等漏洞风险进行扫描测试，以保证及时发现应用漏洞，降低黑客攻击风险。

4.4.3 纵深防御

连连支付建立了纵深防御体系，通过多层防御模式，从网络边界到网络端、服务器端以及数据库端均设置有相应的防御措施：

网络边界：部署防火墙、IPS、WAF 以及负载均衡等安全防护设备；

服务器端：统一部署主机 IDS、服务器防病毒软件等；

数据库端：数据库安全审计等。

图 18：连连支付 Web 防御体系

4.5 数据安全

连连支付信息安全核心工作是保护客户数据安全。我们遵循数据安全生命周期管理的标准，采取管理和技术结合的手段进行全面数据安全体系建设。依据数据安全生命周期，从数据采集、传输、处理、存储、展示、使用至销毁整个流程中，在身份认证、权限管理、访问控制、数据加密、数据隔离、传输安全、存储安全、数据销毁等方面，保障用户对其数据的隐私权、所有权和控制权不受侵犯，为用户提供最切实有效的数据保护。

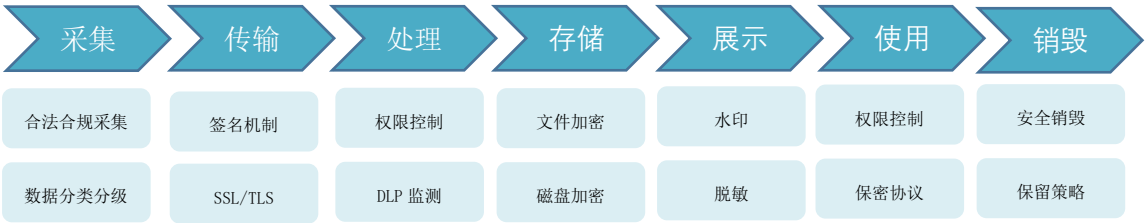

图 19：数据生命周期安全管理

4.5.1 数据分类分级

连连支付将信息资产按资产类型及等级进行分类分级。信息所有者是信息资产最终的

责任部门，保管其管理范围内的所有信息资产，对于每一类信息资产，信息所有者必须根据其重要性程度确定它的安全保护和使用措施，并且指定信息管理者来执行这些安全措施。

4.5.2 数据使用授权

连连支付为用户和企业数据提供访问控制保障。所有权限的设置、审批和授权需考虑不同资产级别，以及政府部门和监管部门对于相应信息资产的安全保护规定，符合以下访问控制基本原则：

- 最小权限：用户应只拥有完成某项工作所需的最小访问权限，用户权限应与工作职责紧密关联并及时更新；
- 按需审批：在授予用户访问权限时，应根据用户的工作职责实际需求进行授权，避免用户访问权限过大的情况出现；
- 职责分离：一个用户不能同时承担多个存在职责冲突的角色，以防止获得过大权限，重要访问过程的请求方、授权方、管理方应实现职责分离；
- 默认拒绝：未经明确授权的用户，系统应默认采用禁止访问原则；
- 身份唯一：所有用户必须在系统中建立唯一的账号，只供自己使用，不得将其账号共享给其他人员使用。

并对数据的使用和对外提供也均进行严格的控制，包括：禁止违规传输和未授权使用敏感信息；对于需要对外提供的信息需经严格的审批流程；对于涉及用户隐私或机密数据的使用，包括对第三方应用的访问，实施权限多次校验及加密存储的策略，同时需经过企业或用户可感知的授权；对于所依赖的第三方服务，当存在数据访问合作时，均需签订相关保密条例。

4.5.3 数据安全审计

连连支付对数据安全进行实时监测，监测范围覆盖所有重要数据活动，实现对用户访问行为的主动控制，及时发现、预警并采取相应的响应流程，阻断可能的泄密行为。

对日志进行统一收集管理审计，配备告警机制，保留所有行为日志，如登录失败、权限升级、计划变更、非法访问、敏感数据访问等，做到所有用户操作有迹可循。并及时对日志开展审计，及时分析确保所有行为的合规性。

4.5.4 数据销毁管理

在满足法律法规以及监管要求前提下，当用户提出合理请求或数据存储时间超出其授

权的保存期限时，连连支付会执行数据清除。

连连支付所有的存储介质维修前，均确保清除其中的敏感数据，对于生产环境的存储介质维修，出机房前进行消磁处理。

05

安全运营管理

5.1 人员安全

5.1.1 背景调查

为了确保所有应聘者信息的真实可靠性，减少聘用风险，连连支付在招聘中对候选人进行筛选、面试、资料核实和背景调查。内容包括其工作经历、诚信、犯罪记录等信息，并对以上信息进行存档。

同时根据岗位特殊性以及具体特点，采用不同方式（如外部供应商）进行背景调查。当背景调查出现与应聘信息不符、有犯罪记录、有劳动仲裁记录、曾有重大违纪的情况则背景调查不通过。

5.1.2 聘用条款和条件

新进员工均需签订劳动合同，且合同中明确规定员工需承担的信息安全责任，并在员工到岗时明确告知；根据岗位情况和人员情况，与新进员工签订独立的保密协议，并明确

所有员工的安全角色和职责应包括以下要求：

- 遵守并执行公司信息安全管理制度；
- 保护公司信息资产免受未授权访问、泄露、修改、销毁或干扰；
- 报告安全事件或潜在事件或其他安全风险事件。

5.1.3 安全培训

连连支付建立完善的信息安全培训体系和年度培训计划，要求每一位新入职员工在入职当周参加信息安全入职培训并完成信息安全入职测试。

在任职期间，连连支付信息安全团队将针对不同岗位人员开展具有针对性的安全培训，并不间断进行多形式多维度的信息安全意识宣贯，连连信息安全培训体系和计划详情可参见图 20 和图 21：

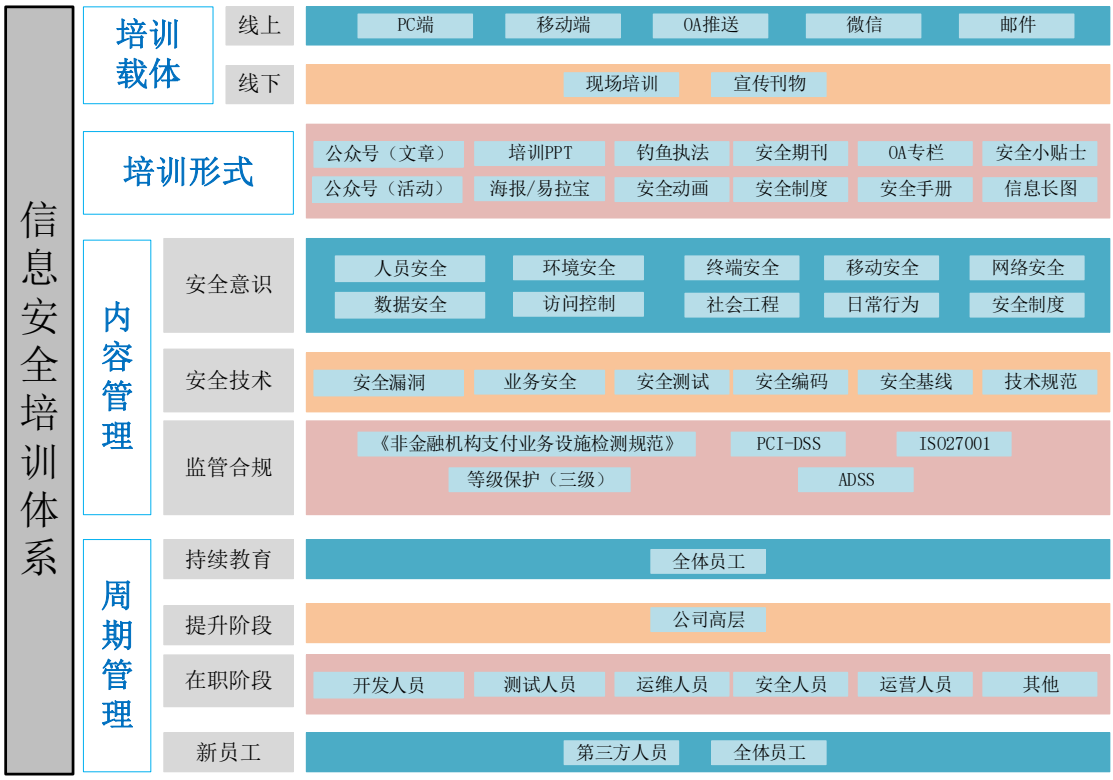

图 20：连连支付信息安全培训体系

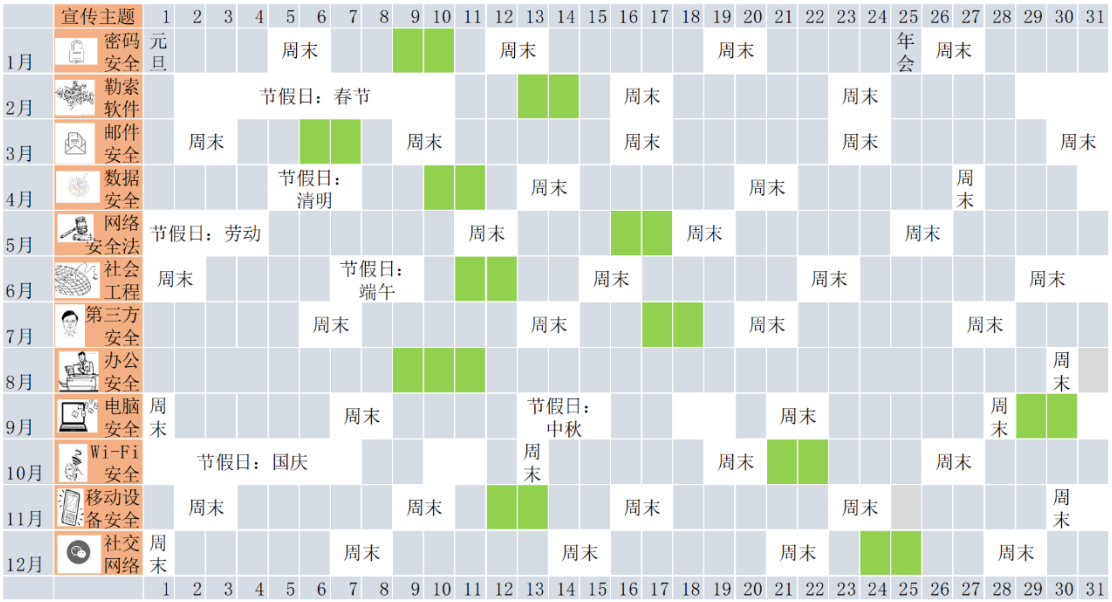

图 21：连连支付信息安全年度培训计划

5.1.4 安全奖惩

连连支付制定了严格的信息安全奖惩管理办法，使所有员工知悉信息安全的重要性并严格履行其信息安全义务，做到有规可依，违规必罚。

连连支付的信息安全红线行为主要包括：

1. 泄露公司技术信息、商业信息、客户信息及内部员工信息；
2. 恶意篡改、删除业务数据或系统参数；
3. 攻击、破坏计算机信息系统；
4. 其他网络违法犯罪行为。

同时在连连支付《纪律制度》中将信息安全行为划分为三类，针对不同类别的违规行文，根据情节严重情况，给予开除、记过和警告等处分。

5.2 漏洞管理

为了规范公司内部信息系统安全漏洞（包括操作系统、网络设备和应用系统）的评估及管理，降低信息系统安全风险，连连支付遵循以下四个原则：分级原则、及时性原则、安全风险最小化原则、保密性原则，根据漏洞的利用难易程度以及对业务的影响情况对漏洞风险分级和评估，并针对不同级别的漏洞制定不同的漏洞修复时效性要求。

基于此，连连支付信息系统安全漏洞生命周期管理主要分 4 个阶段：

1） 漏洞的发现：

- 对公司的应用系统、操作系统和网络设备进行安全测试，及时发现信息系统存在的安全漏洞；
- 建立和维护公开的漏洞收集渠道，漏洞的来源应同时包括公司内部、厂商及第三方安全组织；并在规定时间内验证自行发现或收集到的漏洞是否真实存在；依据内部风险定级原则，确定漏洞的风险等级，出具相应的解决建议。

2） 漏洞的验证：

- 利用漏洞对信息系统的保密性、完整性和可用性造成破坏的过程。

3） 补丁的测试：

- 从官方渠道获取补丁或者新的版本，并经过严格测试。

4） 漏洞的修复：

- 通过补丁、升级版本或配置策略等方法对漏洞进行修补的过程，使该漏洞无法被利用。

5.3 应急与灾备

一旦支付业务设施因为突发灾难造成关键业务数据丢失或信息系统故障，将严重影响公司业务的正常运营，甚至威胁到金融秩序稳定。

连连支付所提供的支付服务，能够应对业务连续性风险，具有快速反应的能力，得益于制定了以下保障措施。

5.3.1 应急与灾备技术

采用两地三中心的运营模式，数据库实时双向同步，应用级灾备数据中心，保证数据一致性。核心业务及数据服务均实现冗余或主备部署，部署在分布于不同地域，相互间通过多家运营商实现多链路链接的多机房；数据库采用热备、冷备相结合，实时同步到不同物理机，以准实时的方式同步到异地机房，保障业务连续性。

连连支付利用数据库相关的复制技术生成多个副本来实现容灾；针对文件类型的数据，利用其自身的复制技术，采取生成多个副本并定期转储至异地机房的方式，实现容灾。

5.3.2 业务连续性管理

连连支付建立了《业务连续性管理制度》以及完备的应急响应和灾难恢复流程，应对业务中断事件，快速恢复被中断业务，维护公众信心，确保公司正常运营秩序。

根据业务紧急性和敏感性进行业务影响分析，识别业务部门对中断的最大可忍耐时间，确定恢复的优先级以及所需要的最少人力资源。根据业务中断的最大可忍耐时间确定系统恢复目标时间（RTO），即业务中断后必须对业务进行恢复的最早时间点，同时确定恢复点目标（RPO），即可接受的数据恢复时间点，制定业务连续性计划并定期复核与演练，确保计划的实时有效性和可行性。

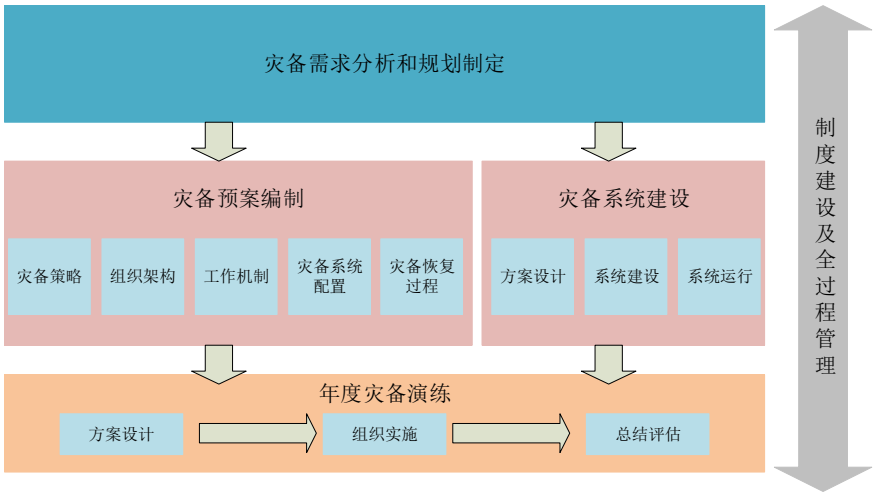

图 22：业务连续性管理体系

5.3.3 NOC 7x24 小时监测

NOC 网络监控中心进行 7x24 的监控，实现基于网络层、服务器硬件层、操作系统层、应用服务层、业务层的监控。当出现故障时，报警系统会根据故障类型及故障级别，通过短信、邮件、即时通讯软件、电话等方式，将故障报警发给指定的对应负责人。

5.3.4 威胁情报管理

为了更进一步确保连连支付以及相关客户数据的安全性，了解数据流向以及对外公开情况，连连支付通过舆情监测、Github 监控等技术了解相关行业内外动态，及时了解其在线信息资产和安全状况， 以及其所在行业的威胁环境，对企业的进一步的安全决策和防范措施提供帮助。

5.3.5 网络红蓝对抗

为了不断提升连连支付内部人员技术能力以及进一步确保内部网络架构的安全性，连连支付安全团队成员积极参加业界组织的权威网络攻防对抗大赛，不断学习行业新技术，加强行业内交流，提升个人技术能力。

同时，连连支付内部也不定期进行网络模拟攻防对抗演习，加强内部网络安全保障，检验安全措施有效性。

5.4 反欺诈管理

连连支付自主研发的反欺诈系统，其在海量数据的基础上，构建一个结合复杂网络的多维度数据、国密算法的加密方式，利用递归神经网络、随机森林等人工智能技术，建设 AI 风控模型，预测、评估已知、未知金融风险的大数据风控系统。

流程主要包括四个步骤：数据采集与处理、数据建模、用户全息画像系统和风险监测分析。在商户交易的支付、反洗钱、风险控制、经营分析、账户认证等产品中进行应用，可多渠道、多维度智能判定风险事件，全方位降低用户及商户面临的交易风险。

业务应用架构主要包含 4 大模块：风险数据平台、风险识别平台、风险策略平台、风险运营平台。

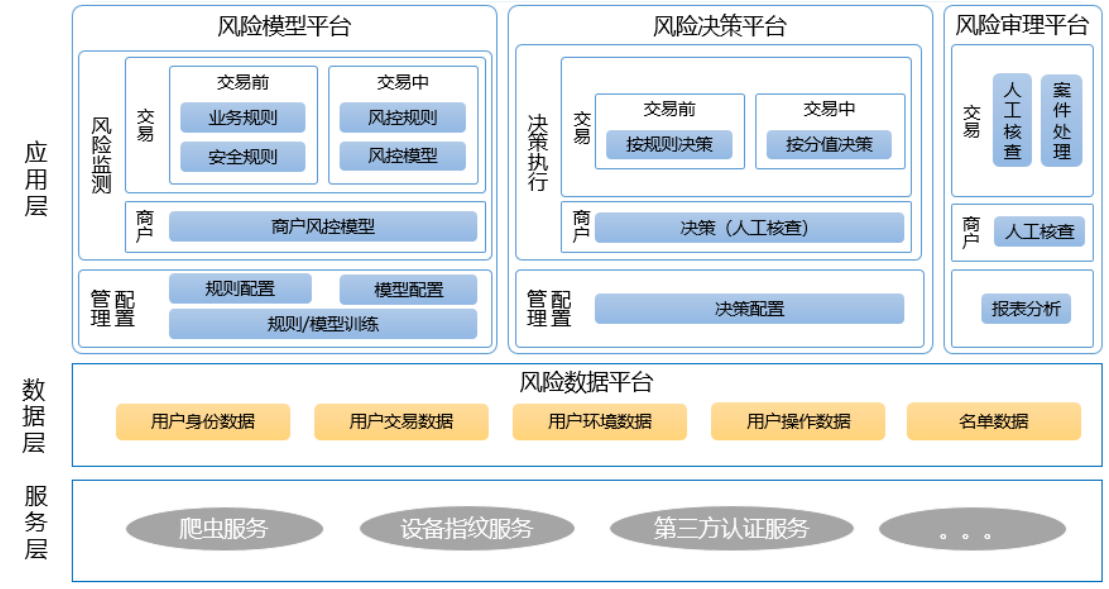

图 23：反欺诈系统业务应用架构

5.5 反洗钱管理

连连支付构建了包括产品洗钱风险评估、客户身份识别、名单筛查、客户身份信息及交易记录保存、客户洗钱风险评估、交易监测与报告、后续控制措施等阶段的洗钱风险核心防御体系，涵盖了组织架构的搭建、内控制度的建设、配套系统的完善、培训宣传活动的开展、整改措施的追踪、考核问责的实施等方方面面，最大程度降低洗钱风险。

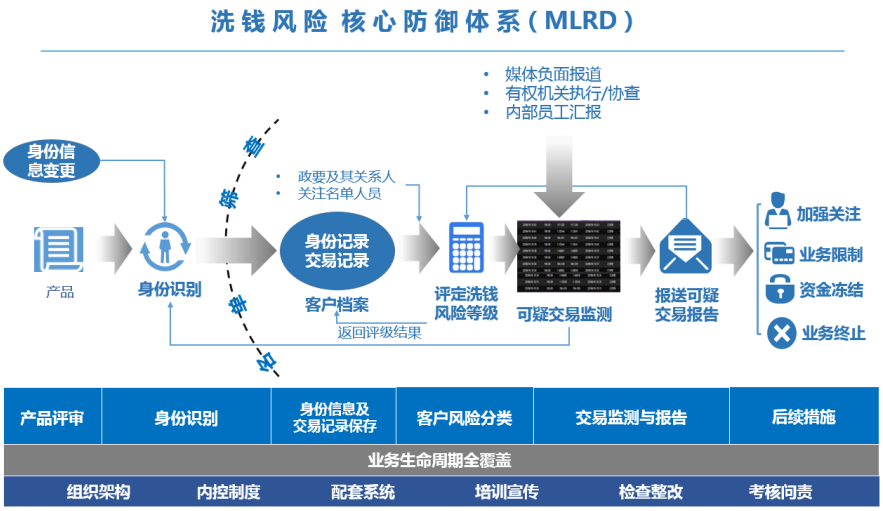

图 24：洗钱风险核心防御体系

同时基于该洗钱风险防御体系，自主研发配套的反洗钱系统。其基于数据与算法驱动的大数据平台，应用机器学习等相关智能算法，形成了数据+专家交互的工作模式，智能模型提升交易监控的性能，大数据分析助力可疑交易报告。

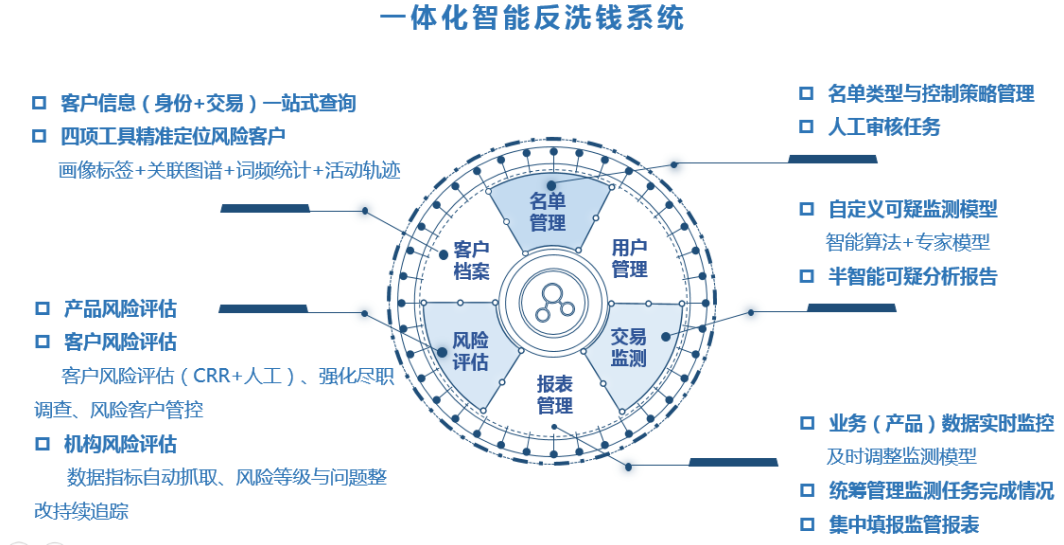

图 25：反洗钱系统

5.6 业务合规管理

连连支付致力于建立能够满足监管合规需要、推进合规文化的业务合规管理框架：董事会、高级管理人员和合规与法务部负责建立、支持和监督合规计划；合规与法务部根据合规计划的要求为事业部制定制度和流程；事业部以此为依据进一步制定与自身特定业务活动相适应的合规控制措施。

同时合规与法务部对事业部执行制度和流程的情况进行定期的合规监控和合规测试，以确保其遵守合规制度和流程，按照设计要求开展运营，并且及时更新以适应法律法规和监管要求和流程本身的变化。

同时，通过合规风险评估、合规监控、合规测试、业务自测、客户投诉或询问、内部审计以及监管监察等多种方式迅速识别、报告以及更正合规问题（特别是可能影响消费者的问题），确保业务合规。

连连支付的业务合规管理采用三线防范的工作机制：

- 一线防范：事业部有责任对于其产品、业务及流程建立起相关合规控制措施，并保证控制措施持续有效地进行。上述合规控制措施包括多种方式，业务自测是其中重要的一种；
- 二线防范：合规与法务部通过合规监控、合规测试及其他方式对于一线防御工作的有效性进行管理；
- 三线防范：审计部对于上述一线、二线合规工作的执行质量和有效性进行独立的内部审查。

06

结束语

本白皮书旨在全面、客观反映连连支付在信息安全及安全保障领域的相关工作内容和进展，分享连连支付的研究成果和实践经验，是对现阶段信息安全工作及其他保障工作的总结汇报，也是连连支付的自律声明，同时呼吁社会各界共同关注互联网金融行业信息安全的政策研究、技术投入和标准建设，为产业的健康、安全、有序发展夯实基础。

连连支付深知信息安全建设不是一蹴而就的，需要持续不断地投入和建设，同时信息安全工作是一个系统工程，需要公司决策层、领导层、执行层的通力配合。从安全制度建设和安全技术层面着手，同步加强信息安全意识的教育和培训，增强自我保护意识，采取综合的防范措施，不断改进和完善安全管理机制。坚持强化安全防范意识，采取全面、可行的安全防护措施，把安全风险降到最低程度。

在今后的工作中，连连支付将持续坚持合规发展、安全经营的理念，切实保障用户的权益，打造全方位的安全体系，连通世界、服务全球。

附录 1：规范性参考文件

规范性参考文件（包括但不限于）：

- 法律法规：

[1] 《中华人民共和国网络安全法》

[2] 《中华人民共和国消费者权益保护法》

- 国家标准：

[3] GB/T 22239-2008 信息安全技术 网络安全等级保护基本要求（Information security technology—Baseline for classified protection of information system security）

[4] GB/T 35273-2017 信息安全技术 个人信息安全规范（Information security technology—Personal information security specification）

- 国际标准：

[5] ISO/IEC 20000:2011 1 信息技术 服务管理体系规范（Information technology-service management）

[6] ISO/IEC 27001：2013 信息技术 信息安全管理体系（Information technology-security techniques-Information security management systems）

[7] ISO/IEC 27002：2013 信息技术 安全技术 信息安全控制实用规则（Information technology-Security techniques-Code of practice for information security controls）

[8] ISO 22301：2012 社会安全 业务连续性管理体系（Societal security-Business continuity management systems-Requirements）

[9] 支付卡行业数据安全标准(PCI DSS) V3.2（Payment Card Industry DataSecurity Standard）

- 行业标准和规范：

[10] JR/T 0071-2012 金融行业信息系统信息安全等级保护实施指引

[11] JR/T 0123.1-2018 非银行支付机构支付业务设施检测规范

[12] 中国人民银行令〔2010〕2 号 《非金融机构支付服务管理办法》

[13] 银发〔2011〕17 号 《关于银行业金融机构做好个人金融信息保护工作的通知》

[14] 中国人民银行公告〔2011〕第 14 号 《非金融机构支付服务业务系统检测认证管理规定》

[15] 中支协技标发[2016]2 号《非银行支付机构信息科技风险管理指引》

[16] 杭银发〔2016〕143 号《中国人民银行关于进一步加强银行卡风险管理的通知》

[17] 银发〔2016〕 290 号《中国金融移动支付支付标记化技术规范》

[18] 银反洗发〔2018〕19 号关于印发《法人金融机构洗钱和恐怖融资风险管理指引（试行）》的通知

[19] 杭银办〔2018〕83 号《中国人民银行杭州中心支行办公室关于进一步加强金融城域网安全管理的通知》

[20] 银办法〔2018〕146 号《中国人民银行办公厅关于开展支付安全风险专项排查工作的通知》

[21] 银发〔2019〕85 号《中国人民银行关于进一步加强支付结算管理防范电信网络新型违法犯罪有关事项的通知》

编委会介绍

本文档由连连支付信息安全管理部发起，统筹规划和发布，最终解释归口。

本文档批准人：林颜双。

本文档参与起草人（按姓氏首字母排序）：陈韵、曹雪花、杜金龙、杜彦慧、顾秋益、金晓嘉、李承雨、李丽、李攀攀、陆方、潘苗、童将、王贵达、徐冬香、夏青、应骏、袁雁飞、翟梦姗、朱军。

本文档顾问：胡希明。

关注我们

连连银通电子支付有限公司

地 址：杭州市滨江区越达巷 79 号

传真：0571-56072618

全球统一服务热线：400-018-8888

业务合作：0571-56073410