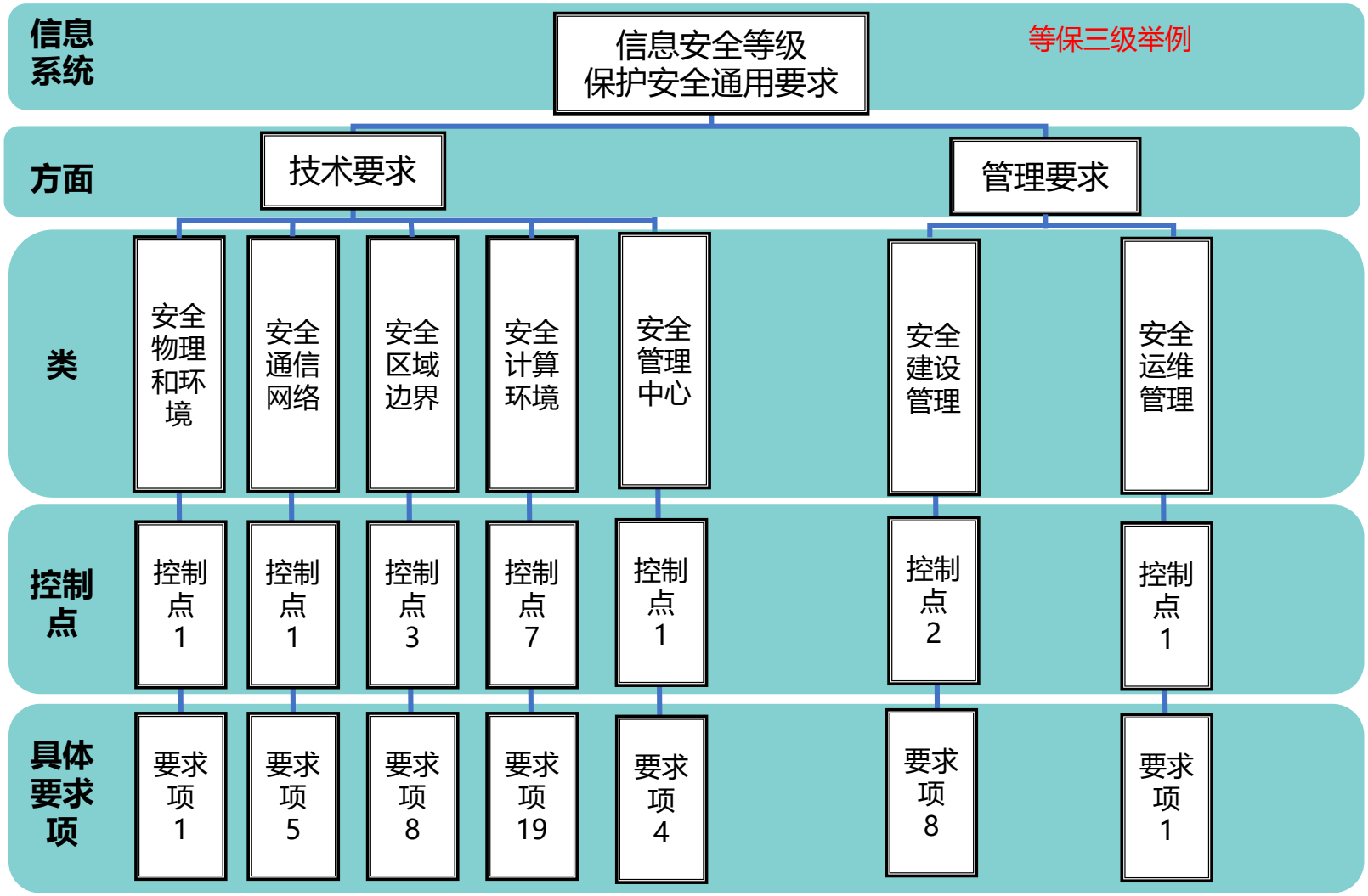
办公环境等保三级建设方案

- **加快构建关键信息基础设施安全保障体系。金融、能源、电力、通信、交通等领域的关键信息基础设施是经济社会运行的神经中枢，是网络安全的重中之重，也是可能遭到重点攻击的目标。**“物理隔离”防线可被跨网入侵，电力调配指令可被恶意篡改，金融交易信息可被窃取，这些都是重大风险隐患。不出问题则已，一出就可能导致交通中断、金融紊乱、电力瘫痪等问题，具有很大的破坏性和杀伤力。**我们必须深入研究，采取有效措施，切实做好国家关键信息基础设施安全防护。**
-
- 全面加强网络安全检查，摸清家底，认清风险，找出漏洞，通报结果，督促整改。
- 金融、能源、电力、通信、交通等领域的关键信息基础设施是经济社会运行的神经中枢，是网络安全的重中之重。

GB/T 22239-2019 等级保护云计算安全扩展要求

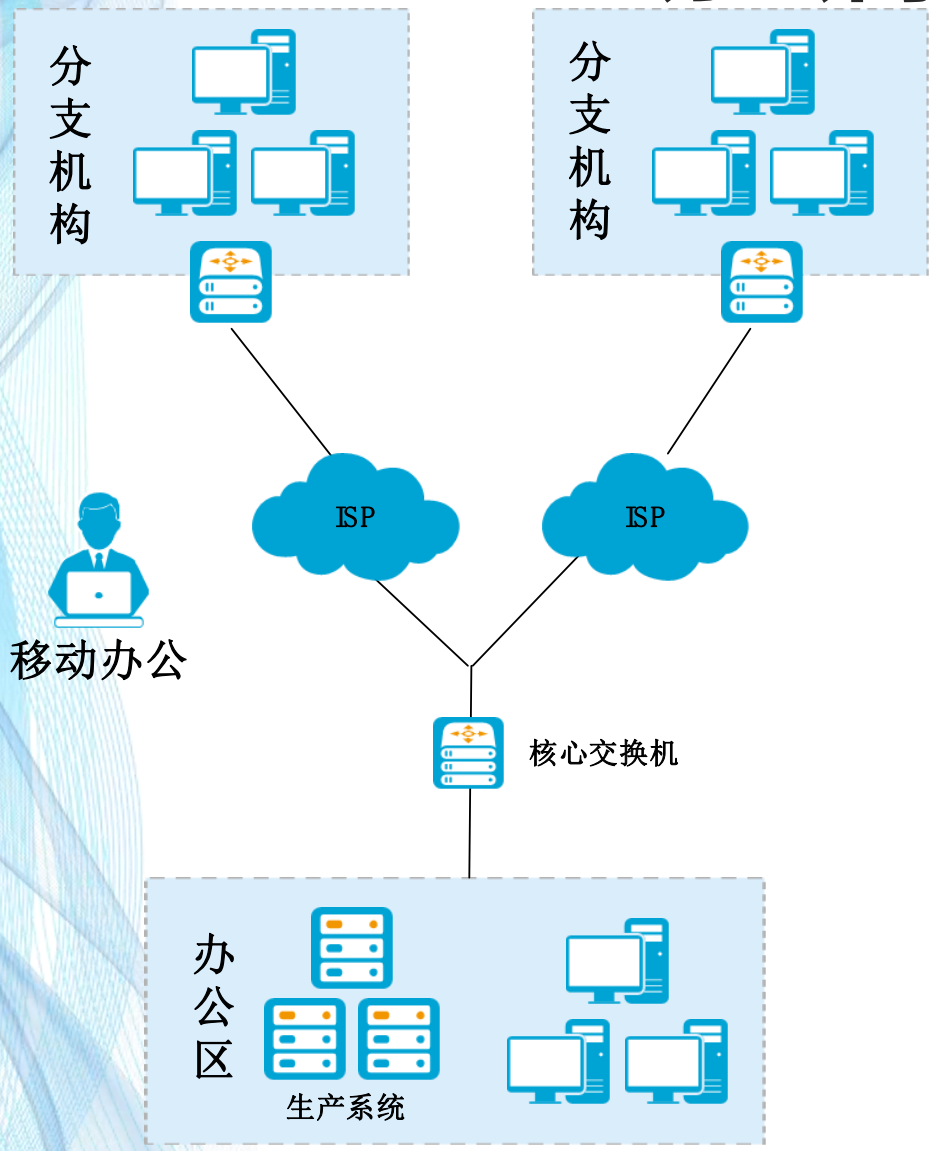


确定本地区、本部门、本行业的关键业务

行业		关键业务
能源	电力	• 电力生产（火电、水电、核电等） • 电力传输 • 电力配送
	石油石化	• 油气开采 • 炼化加工 • 油气输送 • 油气存储
	煤炭	• 煤炭开采 • 煤化工
金融		• 银行运营 • 证券期货交易 • 清算支付 • 保险运营
交通	铁路	• 客运服务 • 货运服务 • 运输生产 • 车站运行
	民航	• 空运交通管控 • 机场运行 • 订票、离岗及飞行调度检查安排 • 航空公司运营
	公路	• 公路交通管控 • 智能交通系统(一卡通、ETC收费等)
	水运	• 水运公司运营（含客运、货运） • 港口管理运输 • 航运交通管控

行业	关键业务
水利	• 水利枢纽运行及管控 • 长距离输水管控 • 城市水源地管控
医疗卫生	• 医院等卫生机构运行 • 疾病控制 • 急救中心运行
环境保护	• 环境监测及预警（水、空气、土壤、核辐射等）
工业制造（原材料、装备、消费品、电子制造）	• 企业运营管理 • 智能制造系统（工业互联网、物联网、智能装备等） • 危化品生产加工和存储管控（化学、核等） • 高风险工业设施运行管控
市政	• 水、暖、气供应管理 • 城市轨道交通 • 污水处理 • 智慧城市运行及管控
电信与互联网	• 语音、数据、互联网基础网络及枢纽 • 域名解析服务和国家定级域注册管理 • 数据中心/云服务
广播电视	• 电视播出管控 • 广播播出管控
政府部门	• 信息公开 • 面向公众服务 • 办公业务系统

办公网的整体网络结构



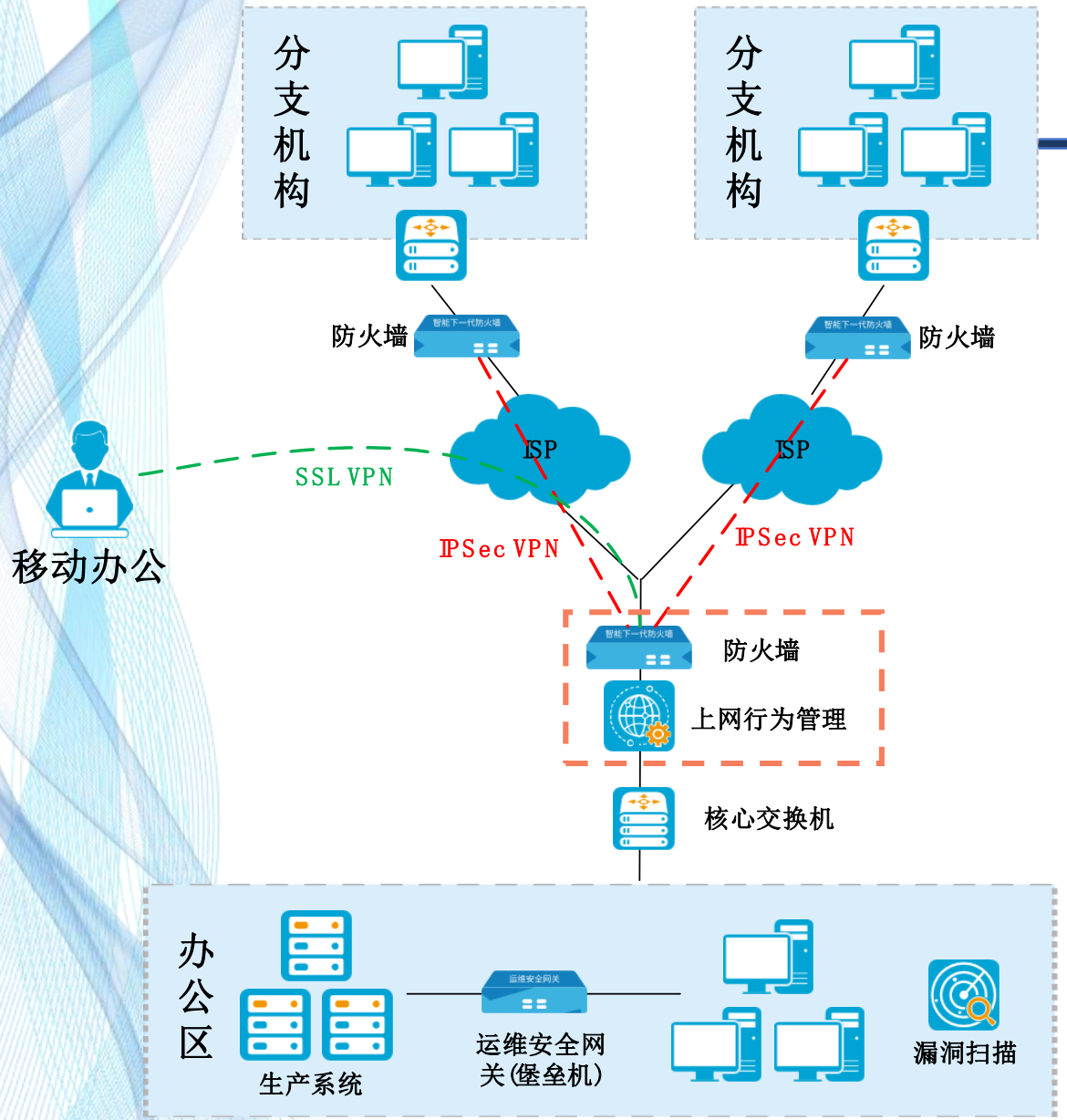
办公网的结构一般比较简单，大多互联网公司也很少有严格的区域划分，多为混合网络，按照网段做逻辑划分。

部分互联网公司会将生产系统（用户相关的业务系统）部署在办公网内，而非在远端的数据中心。

办公网的结构特点：

- 存在远程移动办公接入的应用场景。
- 会有分支互联、或办公网与数据中心远程互联的应用场景。

网络边界安全&网络访问合规



需求：

- 网络边界安全：办公网边界区域主要需要考虑如何抵御来自互联网的各类攻击行为。
- 网络访问合规：员工使用办公网期间，要对员工在互联网上的行为做规范化管理，避免由于员工不当言论或动作，导致公司形象受损，或被网安部门追责。

方案建议：

- 边界防御：防火墙作为重要的边界防护设备是必不可少的配置，此外，防火墙还可以承担对外业务发布所必须的NAT功能。
- 行为管理：建议部署上网行为管理，对员工的互联网访问行为进行管理和审计，确保能够一定程度限制不当行为，且能够追溯到员工个人。