C3安全峰会
CYBER | CLOUD | COMMUNICATION

关键信息基础设施安全保护

李新友
国家信息中心

对关键信息基础设施实施重点保护是国家安全战略

C3安全峰会
CYBER | CLOUD | COMMUNICATION

习近平在网信工作座谈会上的讲话（“419讲话”）

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。

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，加快构建**关键信息基础设施**安全保障体系。

《中华人民共和国网络安全法》

- 2017年6月1日起执行
- 第三十一条 国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。

这是我国首次在法律层面提出关键信息基础设施的概念，为我国开展关键信息基础设施安全保护提供了法律依据

什么是关键信息基础设施（CII）？

C3安全峰会
CYBER | CLOUD | COMMUNICATION

- **基础信息网络和重要信息系统（“8+2”）**

  基础信息网络是广电网、电信网、互联网，重要信息系统是银行、证券、保险、民航、铁路、电力、海关、税务等行业的系统

- **关键基础设施（CI）与关键基础设施信息系统（CII）**

  指关系到国家生死存亡的，无论是物理还是虚拟的系统和资产，这些系统和资产的功能丧失或遭到破坏，会对国家安全、经济稳定、国家公众健康与安全或这些要素的任何结合产生严重影响。

  出自《美国爱国者法案》

什么是关键信息基础设施（CII）？

- **关键信息基础设施（CII）**

  指面向公众提供网络信息服务或支撑能源、通信、金融、交通、公用事业等重要行业运行的信息系统或工业控制系统，且这些系统一旦发生网络安全事故，会影响重要行业正常运行，对国家政治、经济、科技、社会、文化、国防、环境以及人民生命财产造成严重损失

  出自《关键信息基础设施确定指南》(试行)

关键信息基础设施的分类

C3安全峰会
CYBER | CLOUD | COMMUNICATION

关键信息基础设施的形态可以是一个信息系统、一个网络、一个工业控制系统，也可以是多个信息系统、网络、工业控制系统的组合。

网站类

- 党政机关网站
- 企事业单位网站
- 新闻网站

平台类

- 即时通信
- 网上购物
- 网上支付
- 搜索引擎
- 电子邮件
- 音视频、地图

生产业务类

- 办公和业务系统
- 工业控制系统
- 大型数据中心
- 云计算平台
- 电视转播系统

关键信息基础设施安全事件

C3安全峰会
CYBER | CLOUD | COMMUNICATION

➢ 乌克兰电力门事件

2015年，乌克兰电力部门遭到恶意代码BlackEnergy（黑色能量）攻击，攻击者入侵了监控管理系统，并攻击了60座变电站，导致乌克兰首都基辅部分地区和乌克兰西部的140万名居民突然发现家中停电。

➢ 海康威视“黑天鹅”事件

2015年，江苏省公安厅各级公安机关使用的海康威视监控设备存在严重安全隐患，部分设备已经被境外IP地址控制。经查明涉及设备的安全问题为弱口令漏洞，需修改初始密码或者升级设备固件解决

关键信息基础设施安全事件

- **史上最大银行网络失窃案**

  2016年，孟加拉国中央银行在美国纽约联邦储备银行开设的账户遭黑客攻击，被盗走约1亿美元。

- **“震网”（Stuxet）病毒事件**

  2010年，黑客利用Windows系统的漏洞开展攻击，改变了伊朗核原料的浓度，使布什尔核电站1/5的离心机报废，该国核发展几乎停滞

美国对关键信息基础设施的保护

C3安全峰会
CYBER | CLOUD | COMMUNICATION

- 《增强关键基础设施网络安全的框架》（引用系列标准）
- 《联邦信息系统和组织机构安全控制建议》（NIST SP 800-53 ）
- 《联邦信息系统中安全控制评估指南》（NIST SP 800-53a ）

- 2003年《关于关键基础设施和资产物理防护的国家战略》
- 2006年《国家基础设施保护计划》
- 2016年白宫《网络安全国家行动计划》

- 1996年克林顿政府第13010号行政令《关键基础设施保护》
- 1998年第63号总统令《克林顿政府对关键基础设施保护的政策》
- 2001年第13231号行政令《信息时代的关键基础设施保护》
- 2008年发布机密级的第54号国家安全总统令
- 2013年发布第13636号行政命令《增强关键基础设施网络安全》

- 《1996年国家信息基础设施保护法案》
- 《2001年关键基础设施保护法案》
- 《2002年联邦信息安全管理法案》
- 《2002年关键基础设施信息保护法》
- 《2014年国家网络安全保护法案》
- 《2015年网络安全法》

日本对关键信息基础设施的保护

C3安全峰会
CYBER | CLOUD | COMMUNICATION

① 2005年，日本发布第一版《关键信息基础设施信息安全措施行动计划》，指导政府、关键信息基础设施运营单位以及其他利益相关方，开展关键信息基础设施保护工作。

① 2005年，日本信息安全规则理事会发布《保护关键基础设施免遭IT中断和确保关键基础设施供应商业务连续性必要决策的基本方向》。

③ 2009年，第二版《关键信息基础设施信息安全措施行动计划》发布，确定了关键信息基础设施保护基本措施和建立公私信息共享的框架，明确了“对环境变化的响应”政策，以应对不断变化的社会和技术环境。

③ 2015年，日本网络安全战略总部发布《关键信息基础设施保护基本政策》，详细描述了对关键信息基础设施运营者需要采取的措施和国家层面采取的行动。

加拿大对关键信息基础设施的保护

① 2004年，加拿大发布《关键基础设施国家战略和行动计划》，该战略的目标是建设一个更安全、稳定和弹性的基础设施环境。

② 2005年，加拿大根据当前关键基础设施信息系统的状况，推出了《应急管理法案》，其目的是促进各部门对威胁的反应能力，并强化各部门协作和信息共享。同时，颁布《识别和标注加拿大政府保密的关键基础设施共享信息》作为具体实施细则 。

③ 2012年，加拿大发布了针对其安全情报服务的报告《加拿大网络安全对关键基础设施威胁的评估》，评价了加拿大四个主要部门（能源设施、交通、金融、信息通信技术）中关键基础设施所面临的网络安全威胁环境。

其它国家对关键信息基础设施的保护

C3安全峰会
CYBER | CLOUD | COMMUNICATION

① 2008年，俄罗斯发布《俄罗斯信息社会发展战略》和《确保俄罗斯联邦信息安全的措施》。

② 2005年，德国发布《信息基础设施保护计划》和《关键基础设施保护的极限保护概念》两份关键文件。

③ 2005年，意大利发布《网络安全：从风险到保护战略》和《关键基础设施网络安全工作指南》。

④ 2003年，匈牙利发布《国家信息基础设施发展计划》。

⑤ 2002年，韩国发布《e-韩国2006年展望》，侧重网络空间安全和关键基础设施安全。

⑥ 2001年，澳大利亚发布《澳大利亚国家信息安全章程》和《保护国家信息基础设施政策》。

⑦ 2000年，新西兰发布《安全保护政策框架》和《政府部门安全手册》。

我国关键信息基础设施保护工作的基本思路

C3安全峰会
CYBER | CLOUD | COMMUNICATION

目标：业务连续性（**Business Continuity**）

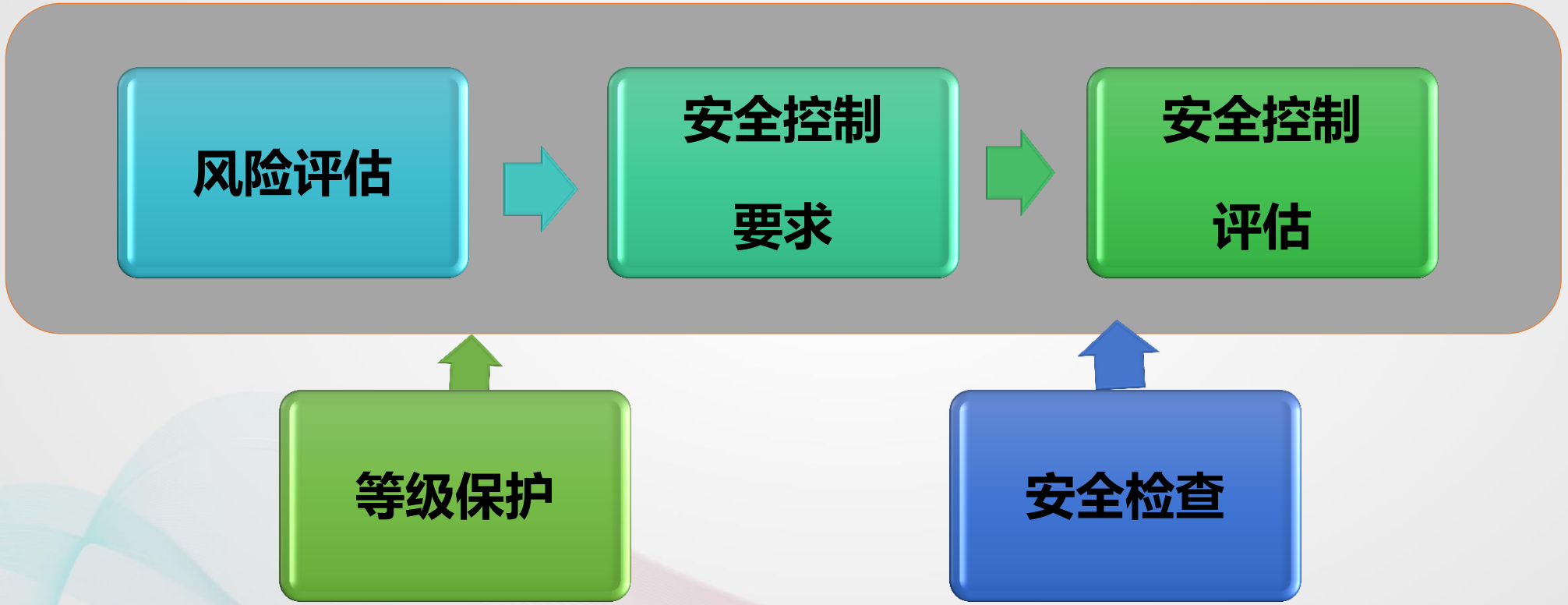
通过实施安全保护手段，关键信息基础设施在任何时候以及任何需要的状况下都能保证业务连续运行

原则：在网络安全等级保护制度的基础上，实行重点保护

手段：**可控性（controllability）**

对关键信息基础设施的信息、软硬件和活动实施安全监控管理，控制授权范围内的行为方式，保证业务连续可靠正常运行

关键信息基础设施工作定位



关键信息基础设施安全控制

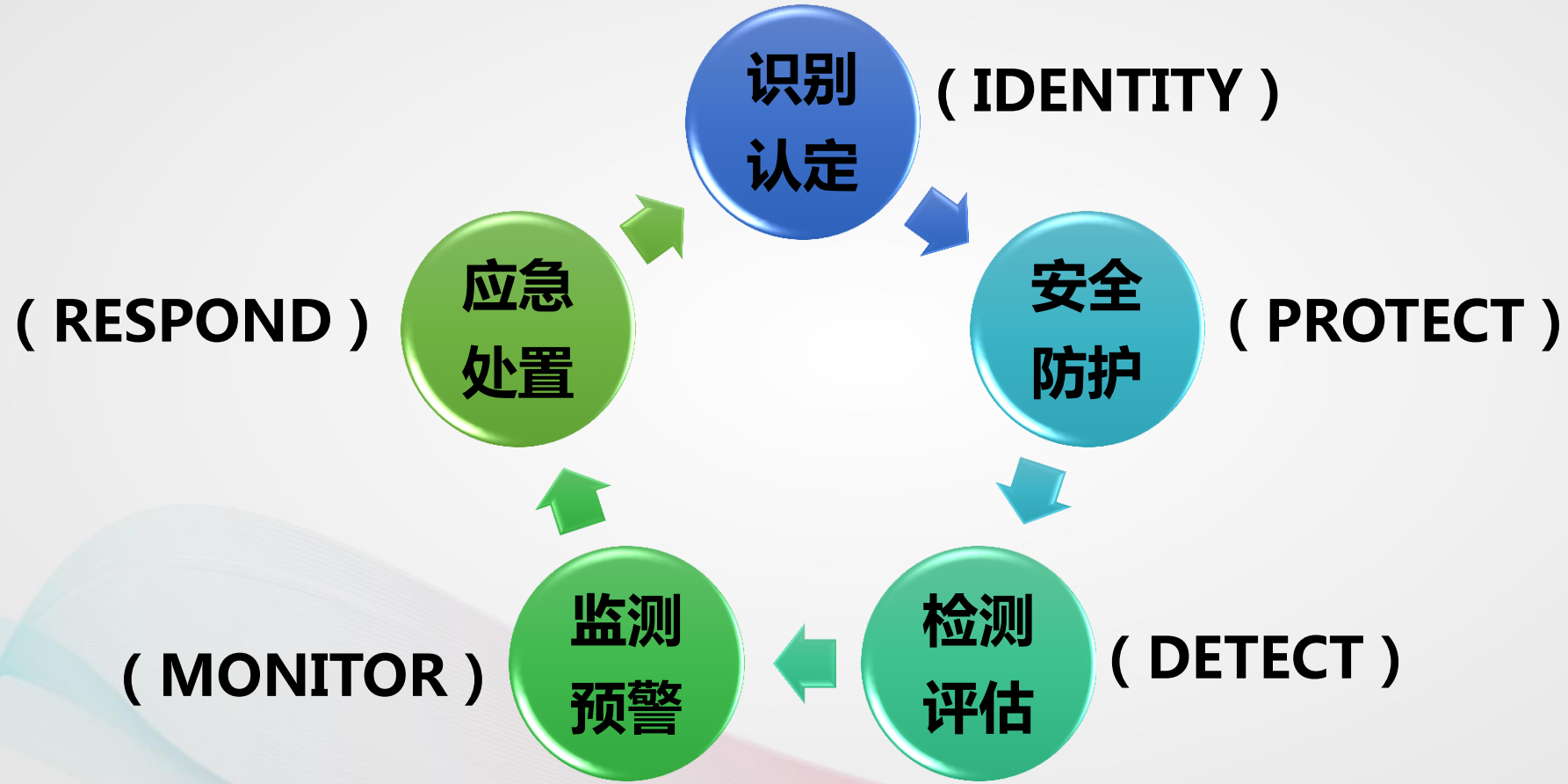
① 安全控制 Security Control

为保障关键信息基础设施的业务连续性和可控性采取的措施。

② 安全控制评估（ Security Control Assessment ）

用来评价关键信息基础设施所采取的安全控制措施的有效性，以判定其安全控制能力。

安全控制模型（IPDMR）



识别认定（IDENTITY）

C3安全峰会
CYBER | CLOUD | COMMUNICATION

① **资产管理**

控制内容包括关键信息基础设施资产清单、关键信息基础设施信息系统组件清单、网络安全架构、关键信息系统连接和资源优先级排序。

② **运营环境**

控制内容包括供应链保护、业务活动优先事项、安全资源。

③ **安全治理**

控制内容包括网络安全计划、安全规章制度、第三方网络安全角色和职责、符合法律法规要求。

④ **风险识别**

控制内容包括安全控制措施评估识别、风险评估识别、系统文档识别、内外部威胁识别、潜在业务影响、风险决策。

安全保护（ PROTECT ）

① **访问控制**：控制内容包括帐户管理、帐户及设备标识管理、鉴别凭证管理、密码模块鉴别、远程访问、移动设备访问控制、最小特权等。

② **数据安全**：控制内容包括静态数据保护、传输数据保护、剩余数据保护、数据维护能力、数据完整性、不同环境数据分离、重要数据保护等

③ **维护**：控制内容包括受控维护、维护工具管理、远程维护、维护人员、及时维护管理、缺陷修复。

④ **审计**：控制内容包括可审计事件、审计记录内容、审计记录存储、审计过程失败时响应、时间戳、审计信息保护、审计报告等。

检测评估（ DETECT ）

C3安全峰会
CYBER | CLOUD | COMMUNICATION

① **安全检测**

控制内容包括自评估、检测评估、安全抽查、系统安全计划、测试演练和监视活动。

② **风险评估**

控制内容包括安全控制措施评估、风险评估、风险决策、风险反映排序。

监测预警（ MONITOR ）

C3安全峰会
CYBER | CLOUD | COMMUNICATION

① 持续监测

控制内容包括持续监测计划、信息系统监测、垃圾信息监测、物理访问监测、信息泄漏监测、用户软件监测、恶意代码监测资产监控与追踪、脆弱性扫描、渗透性测试。

② 安全预警

控制内容包括事件管理、事件报告、在线预警、预警信息共享、与特定相关方联系。

应急处置（ RESPOND ）

C3安全峰会
CYBER | CLOUD | COMMUNICATION

① 计划

控制内容包括应急响应计划、事件响应计划、灾难恢复计划。

② 培训和演练

控制内容包括应急培训、应急演练、事件演练。

③ 处置

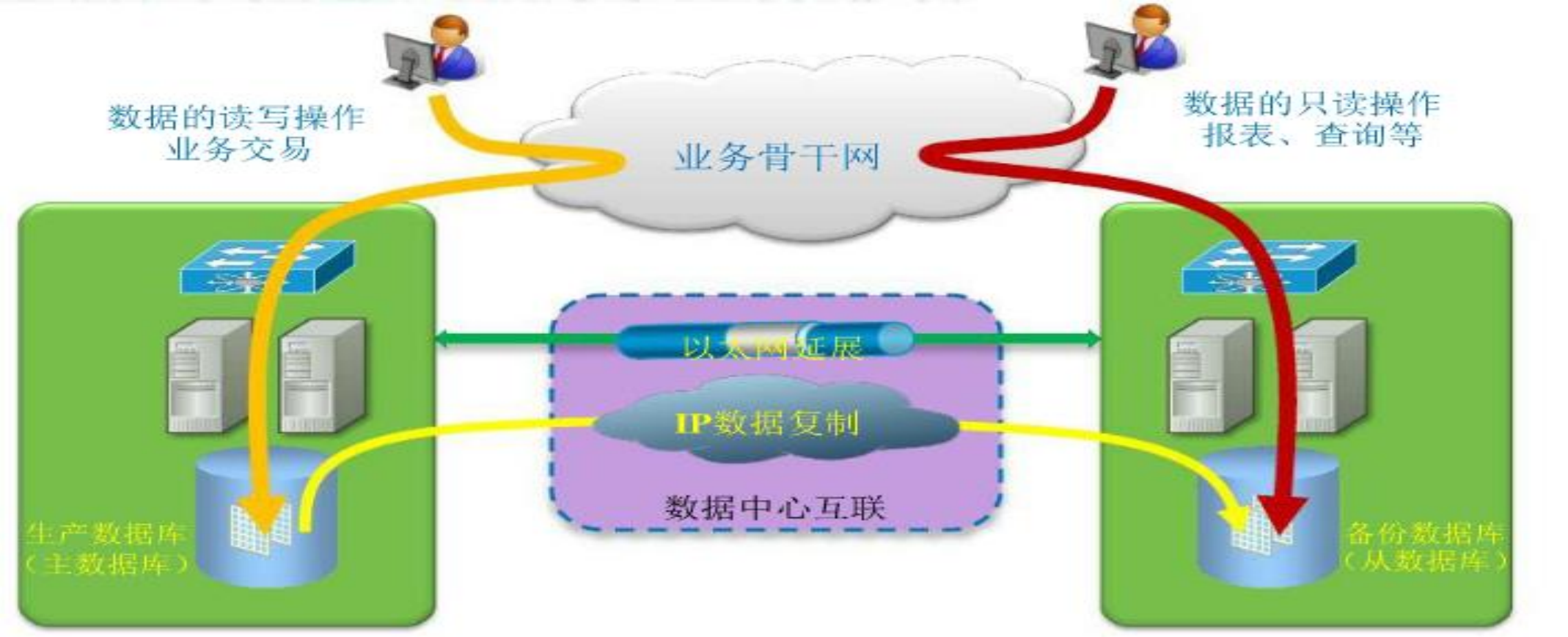
控制内容包括事件处置、事件处置支持、错误处理、信息系统恢复和重构。

④ 改进

控制内容包括事件处置报告、事件追溯、事件学习、事件配合。

案例一 国家海关双控中心打造异地灾备双保险

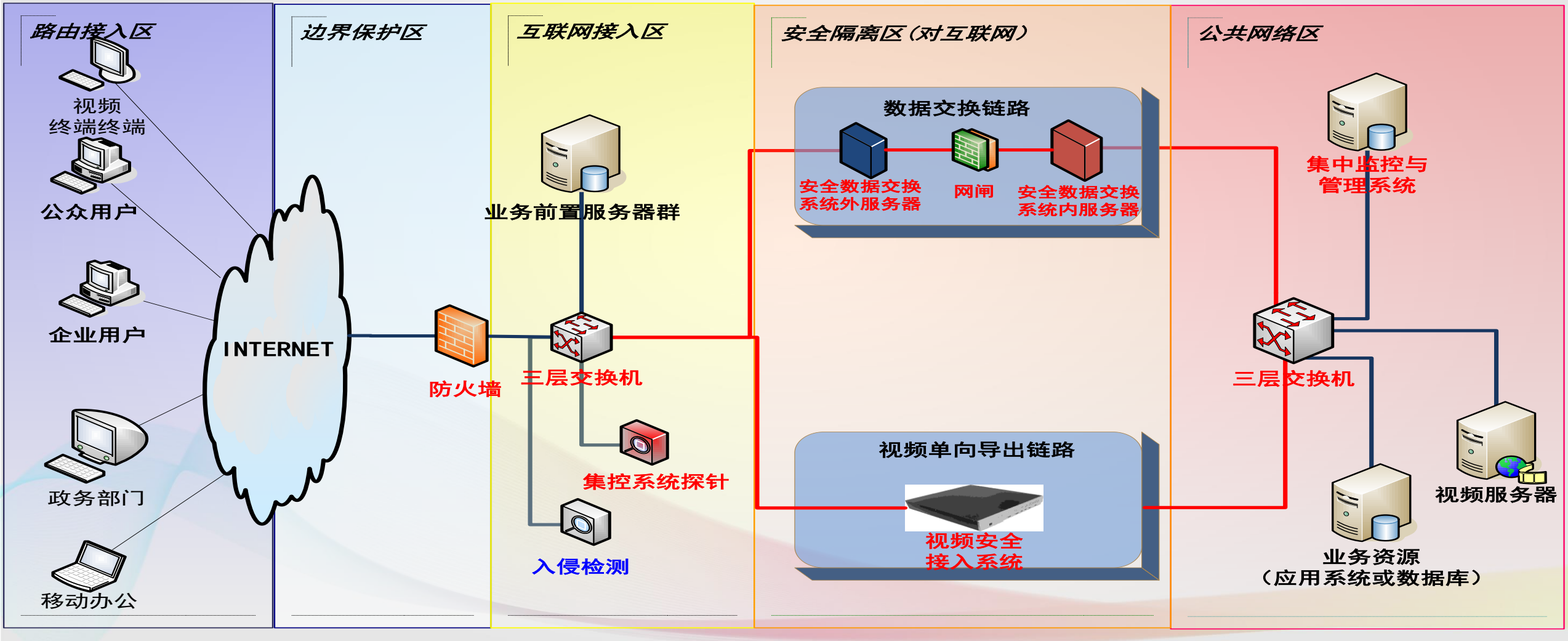
C3安全峰会
CYBER | CLOUD | COMMUNICATION



- 两中心数据库实时同步
- 应用数据与两中心畅通
- 每4个月异地容灾切换
- 主要业务切换时长8min

案例二 外网安全交换平台保障跨网数据安全交换

C3安全峰会
CYBER | CLOUD | COMMUNICATION



案例分析三 阿里云完整的安全防护控制体系

C3安全峰会
CYBER | CLOUD | COMMUNICATION

Thank You