新形势下的医院信息安全

詹榜华

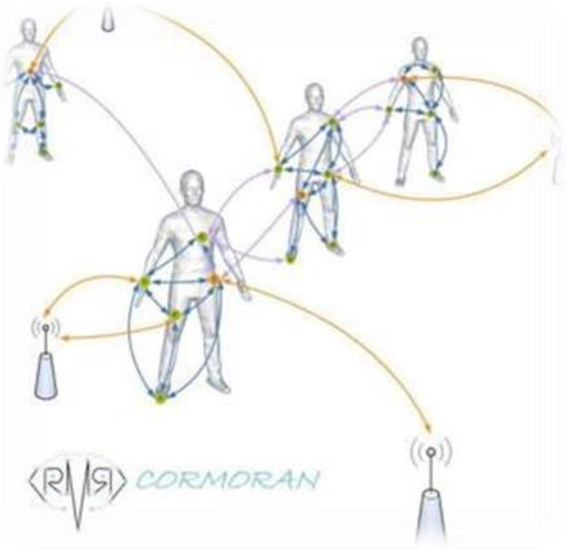
2014年5月

北京数字认证股份有限公司
BEIJING CERTIFICATE AUTHORITY

目录

我们进入信息社会

- 我们已经跨入以社会信息化、设备数字化、通信网络化的信息社会
- 我们的信息社会正在不断的演进，互联网、物联网、无线人体局域网（WBANs）、云计算、大数据、可穿戴设备、智能化技术正在飞速发展，正在推动我们信息社会发生巨大的变化
- 未来可以展望的是，不仅仅我们可以连接到网络，而且我们的身体（至少是衣服或配饰）会变成物联网的关键网络结点。

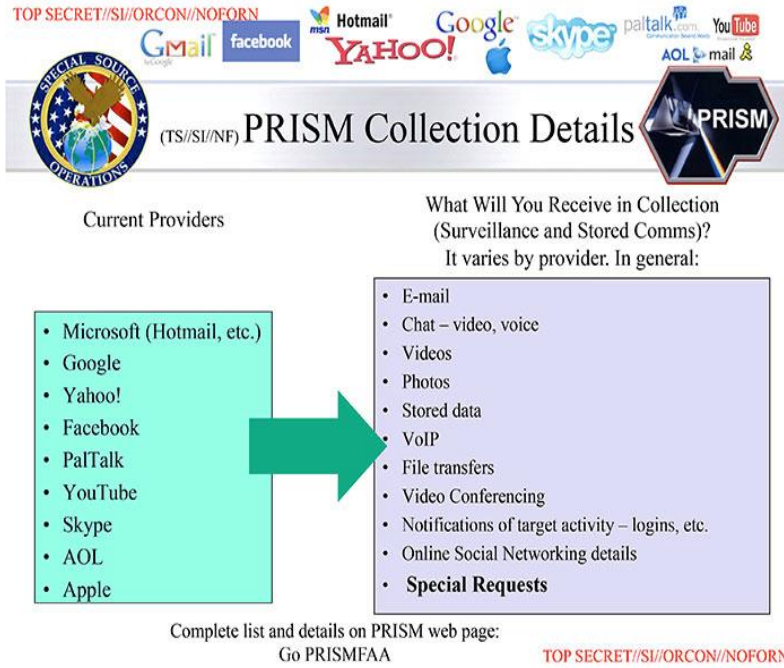


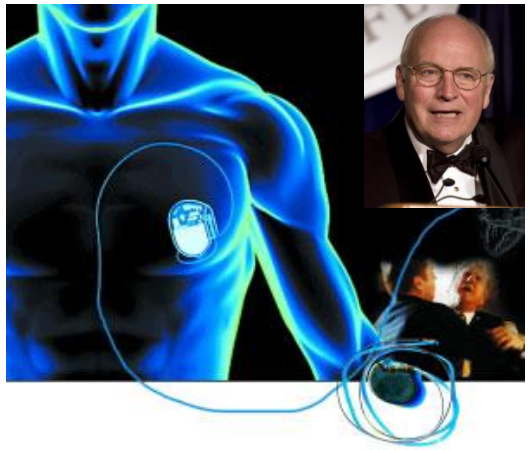
信息安全无处不在

- 过去，网络安全影响的，只有你的电脑；而在现在，网络安全所影响的，是你的电脑、你的手机、你的谷歌眼镜、你的智能手表，你的家电、你家的智能安防系统、你的汽车，甚至更多更多……
- 过去，黑客最多知道，你硬盘里存了多少小电影，而现在，他们可以知道你的手机号、你的银行卡号、你的通讯录，知道你在哪里，在做什么，喜欢做什么……
- 在广泛互联化的IT环境中，大到国家和社会，小到机构和个人都面临着如何保障自身的信息安全的问题

信息安全危害越来越严峻

- 信息安全问题影响和危害国家安全和社会稳定
  - 斯诺登事件
  - 伊朗布什尔核电站“震网”事件
- 信息安全危害到每个人的生命权、财产权和自由权
  - 入侵植入式心脏起搏器
  - 入侵ATM取款机
  - “心脏出血“安全漏洞

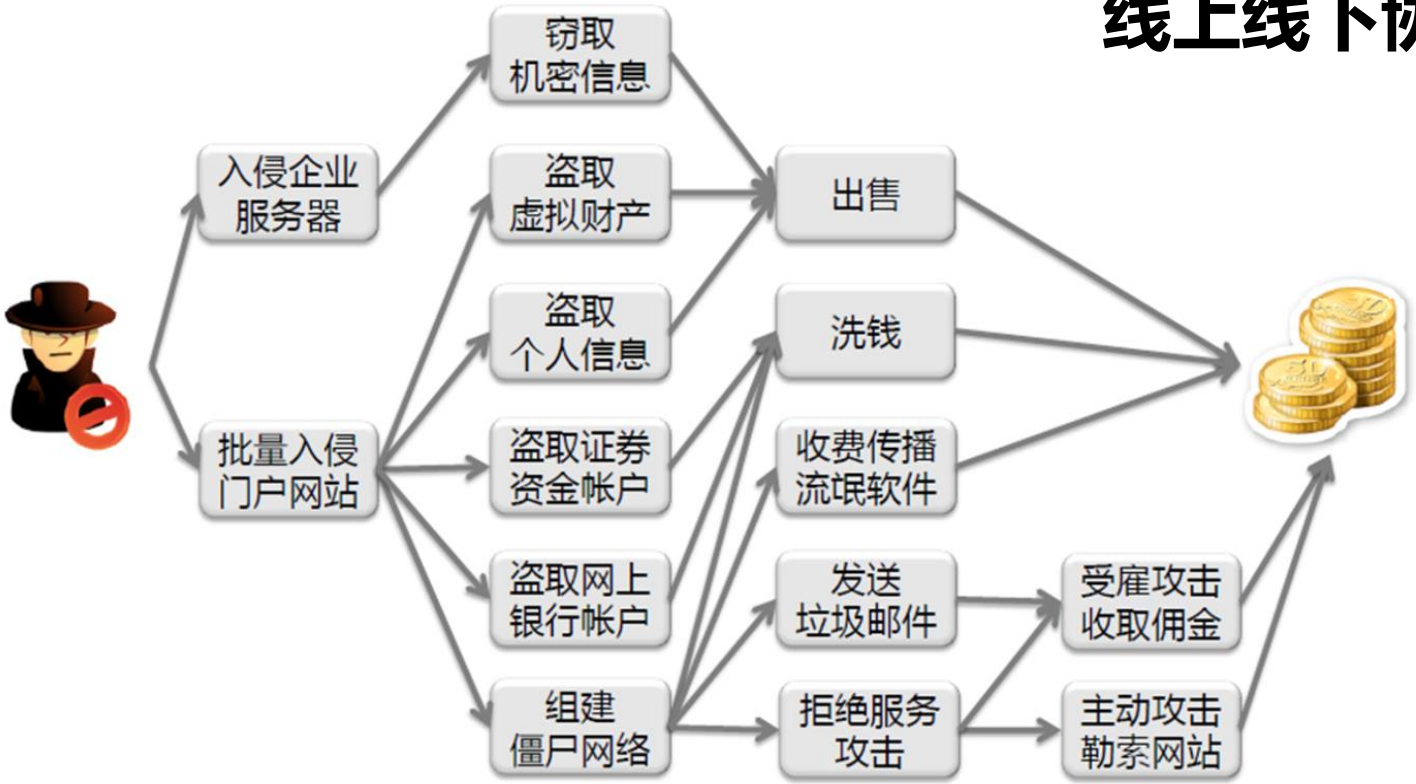




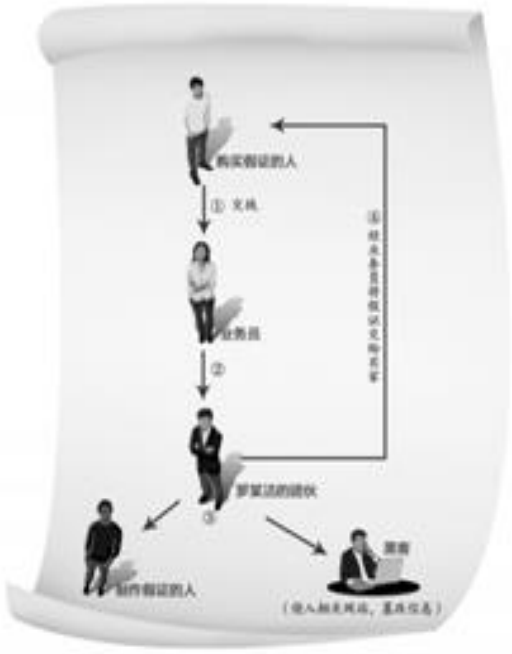
攻击从损人不利己向以获取利益为目的转变

- 2012年，上海警方成功摧毁一个通过互联网倒卖公民信息资料、利用第三方支付平台盗刷信用卡的犯罪网络，涉案金额200万元，受害人数超过30人
- 广东人事考试局网站被黑 黑客称交500元改成绩

线上线下协同



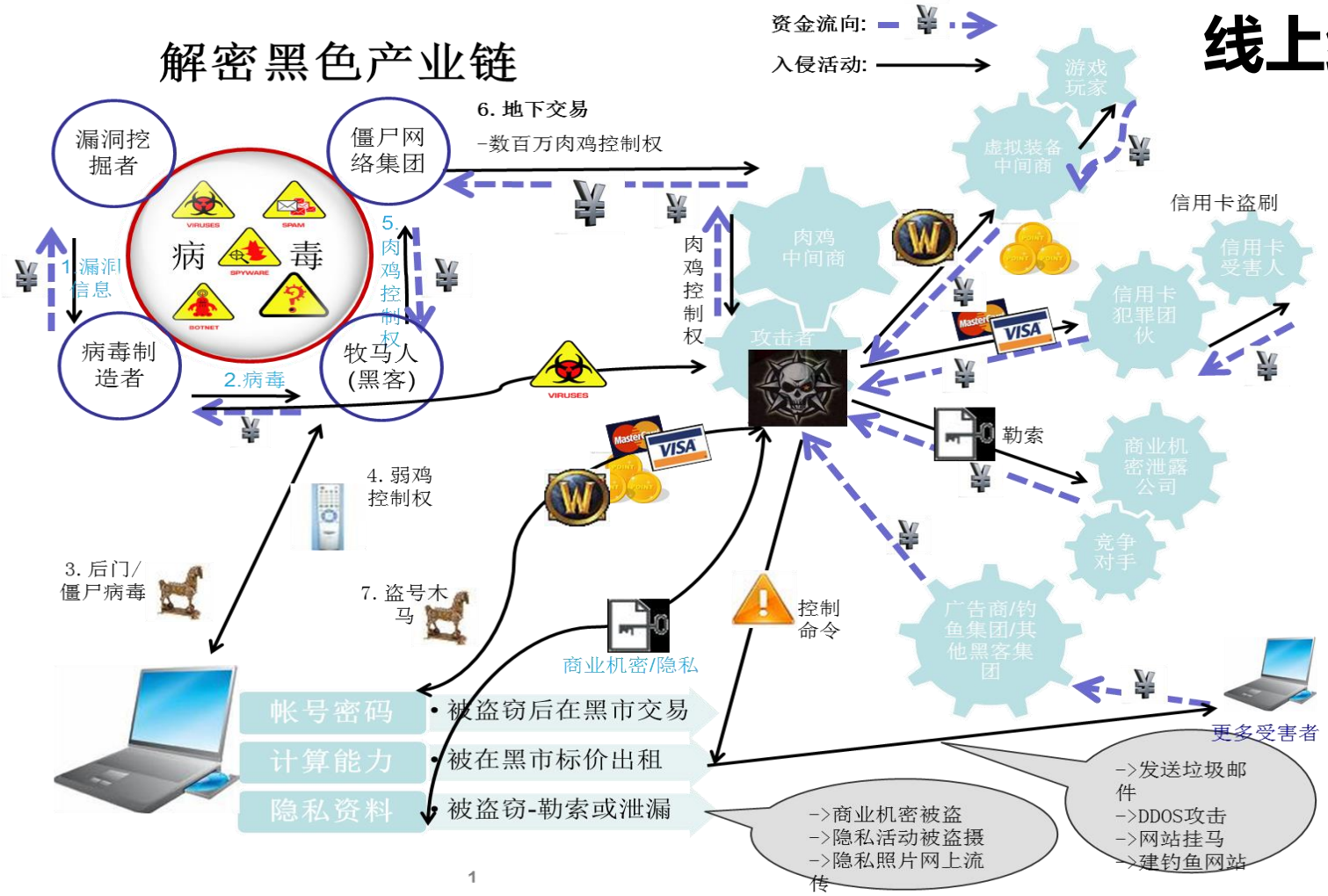
假证团伙入侵185政府网站:165名嫌疑人落网



广东省揭阳警方发现，假证制售团伙让专人入侵政府网站，加装非法链接、篡改信息，令假证购买者能够查询到证件相关信息，信以为真。全国已有**185**个政府网站被入侵过。警方共抓获犯罪嫌疑人**165**名，收缴各类假证书**7100**多本、假印章**10000**多枚。

攻击从个人英雄向组织犯罪转变

- 有组织的攻击犯罪攻击资源更多，更加有效，造成的安全威胁更大



攻击手段体系化

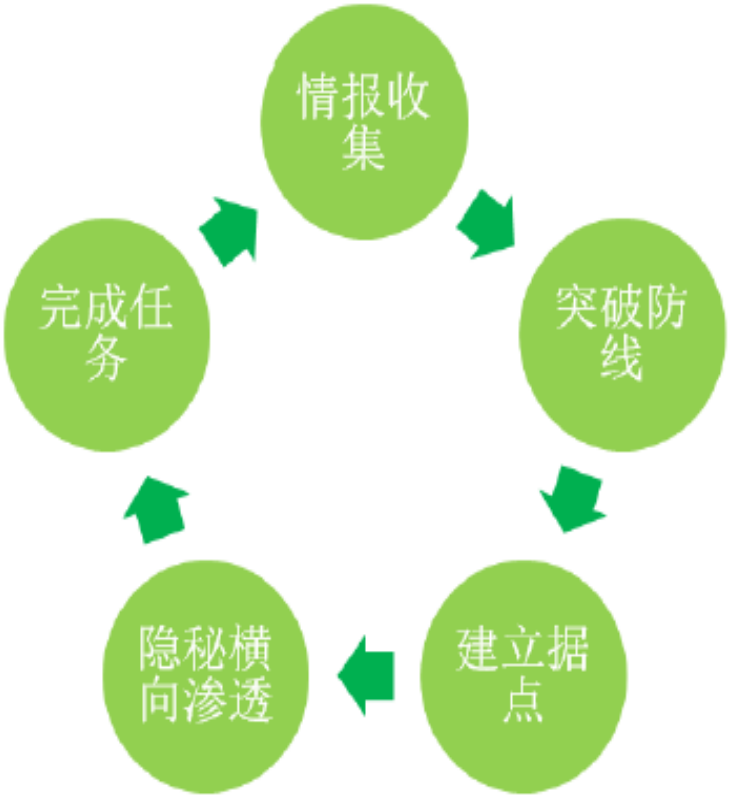
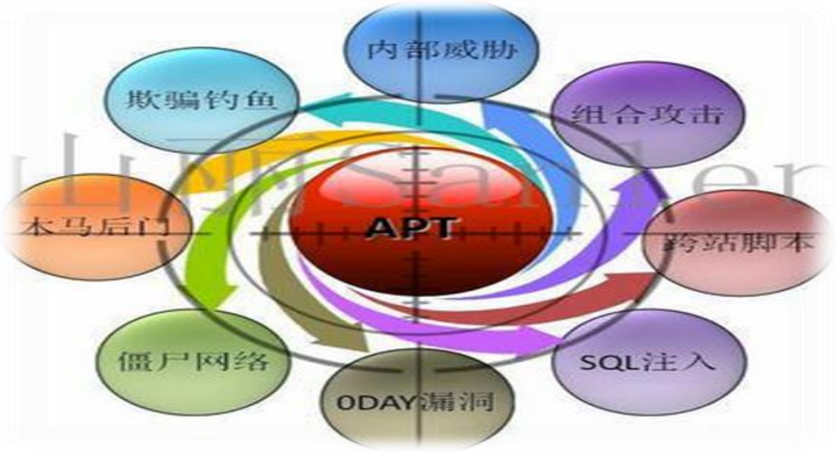


图 3.2 APT 攻击的五个阶段



情报收集	攻击者在社交网站等公开数据源中搜索并锁定特定人员，收集有价值情报并加以研究。
突破防线	收集到足够的情报后，获取第一台受害主机上的代码执行权限。
建立据点	突破防线后，建立 C&C（Command & Control）服务器到第一台受害主机的信道并获取系统的最高权限，将第一个据点变成对内部网络发动后续攻击的前沿阵地。
隐秘横向渗透	在内部网络探测、入侵更多的主机，发掘有价值的资产及数据服务器，并尽可能长时间地避免被发现。
完成任务	设定要完成的任务可能是上传搜集到的敏感信息，或者执行破坏活动。比较高级的 APT 攻击还包括严密的踪迹销毁等撤退策略。

典型案例：震网

资料来源：绿盟科技

信息安全上升到国家安全高度

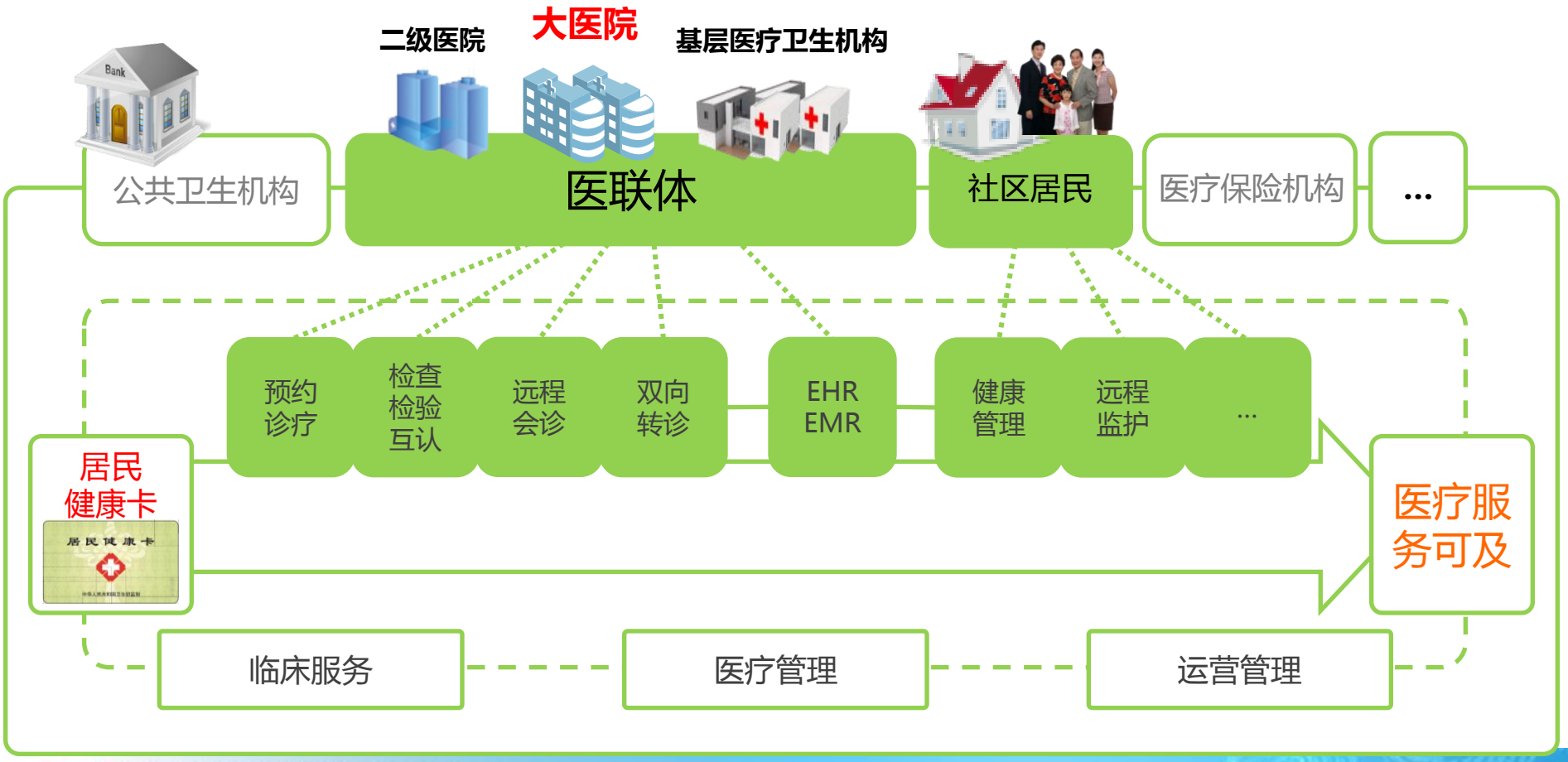
- 美国 --- 《网络空间安全国家战略》，
  - 美国21世纪的经济繁荣依赖于网络空间安全
  - 网络空间安全威胁是最严重的国家经济和国家安全挑战之一
- 英国 --- 《英国网络安全战略》
  - 与制空权、制海权同等重要的制信息权；
  - 帮助塑造一个可供英国大众安全使用的、开放的、稳定的、充满活力的网络空间，并进一步支撑社会开放；
- 中国
  - 十六届四中全会首次明确将信息安全作为国家安全的主要内容
  - 2014年2月27日，中央网络安全和信息化领导小组宣告成立

没有网络安全就没有国家安全

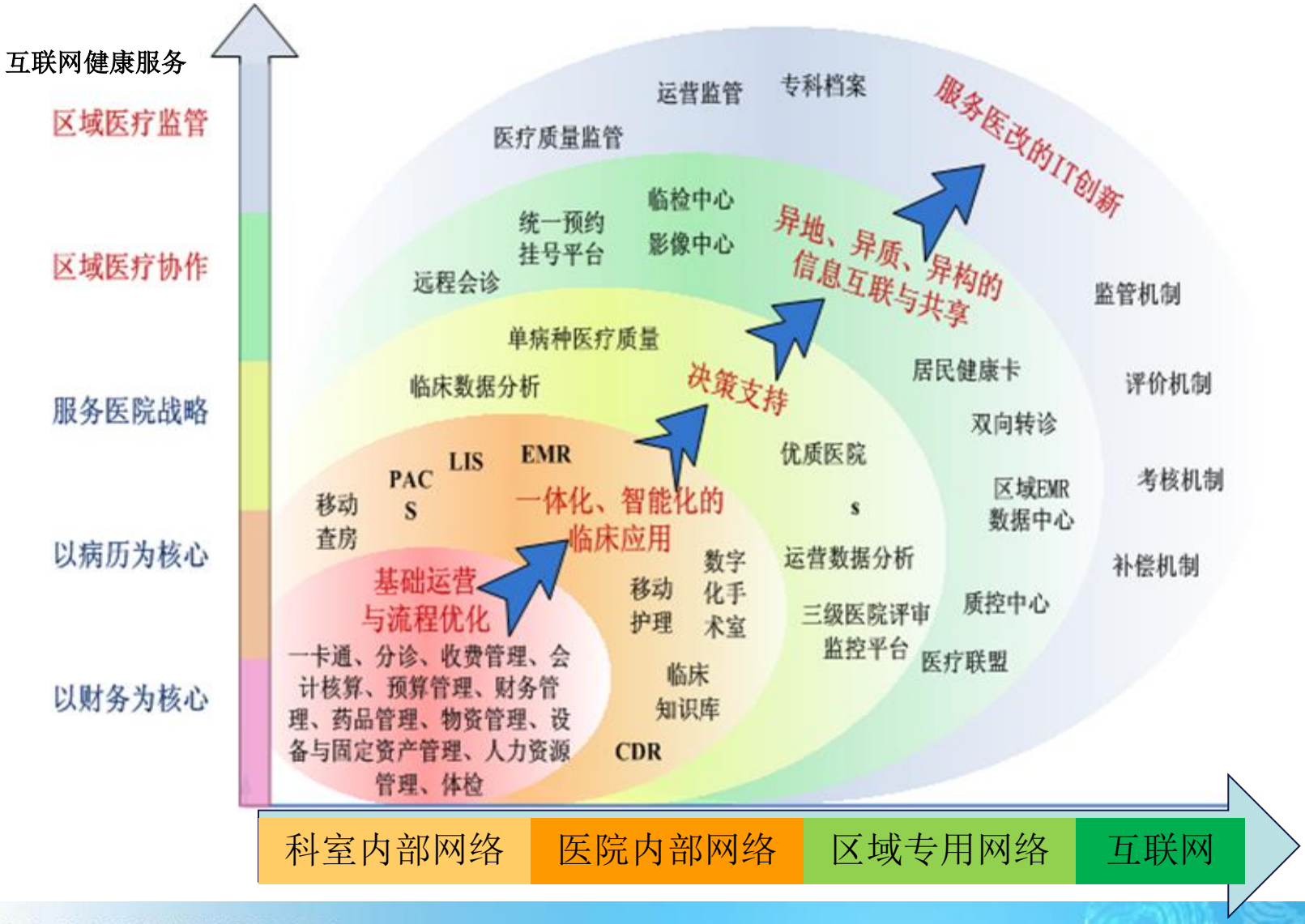
目录

新医改催生医院信息化变革

以电子病历为核心，优化流程、互联共享、上下联动、方便就医



独善其身的信息安全策略不再适应



信息安全事件对医院运营影响越来越大

- 系统服务中断？ —— NO
- 电子病历数据丢失、破坏、泄露？ —— NO

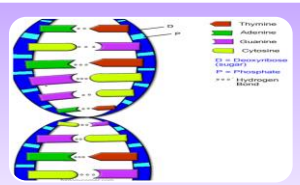
医院电子病历价值越大安全越重要

临床决策支持

- 检查所有患者的数据以便优化照护
- 协助医护人员开展诊疗活动

以病人为中心的照护和疾病管理

- 了解生活方式改进医疗保健成果
- 评价健康状况征兆和诊断信息



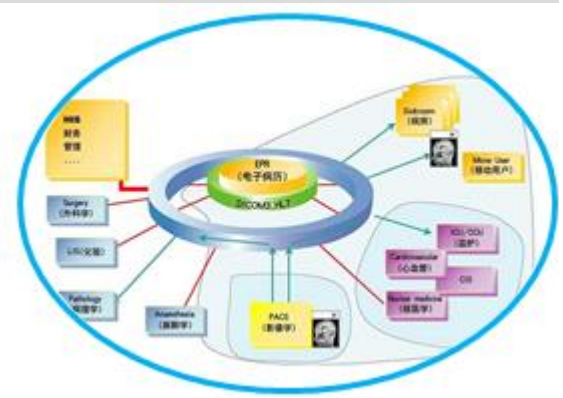
药物发现与基因分析

- 综合临床、医院和日志信息
- 临床数据与患者基因结合分析

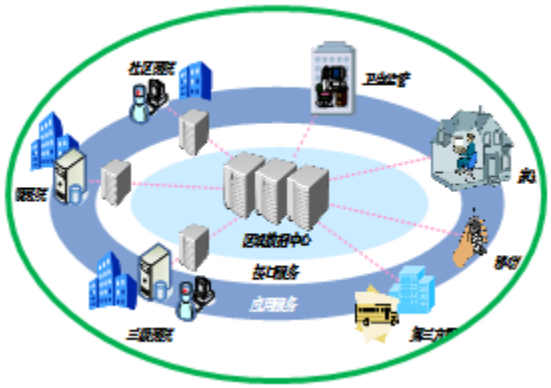
如今，大医院每天门诊上万，年住院病人数万，年数据量HIS 30~50GB, LIS 50~100GB, PACS 10~30TB等，医疗大数据价值凸显。

医疗大数据风险威胁趋势

医院信息系统



区域卫生信息平台



国家卫生信息平台

数据的变化趋势

基础病种统计

居民健康档案

卫生数据统计

威胁的变化趋势

敏感数据

个人隐私数据

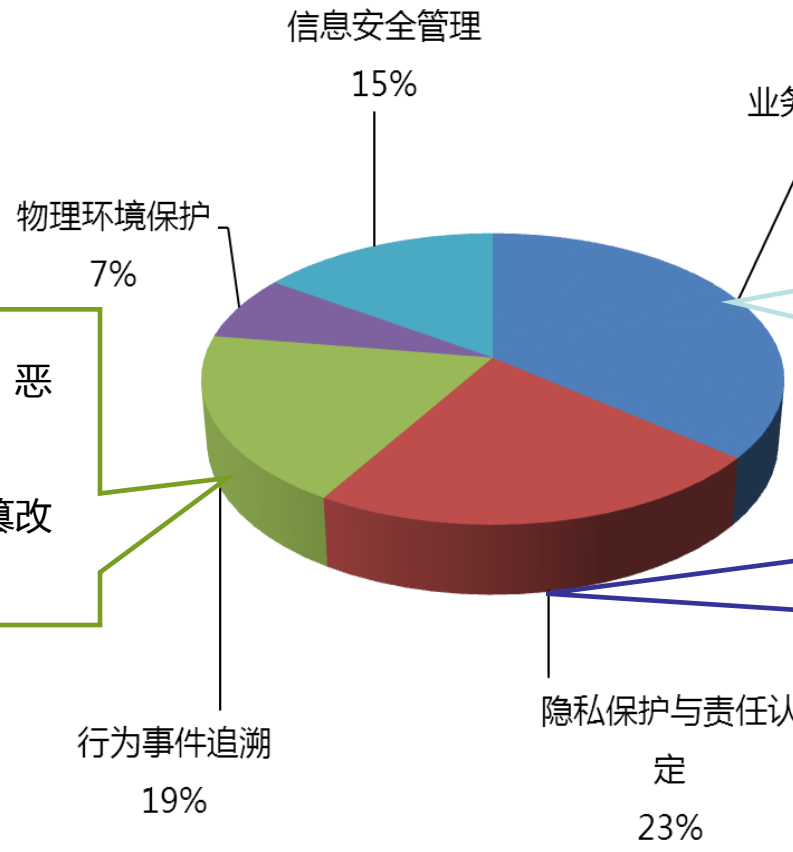
国家秘密数据

医院信息系统面临的安全威胁日趋复杂多样

- 新技术应用使得边界变模糊、开放，攻击更容易

医疗私有云
移动查房
医疗物联网
微信预约挂号
在线查询结果
……

当前医院面临的主要安全问题



-关键设备单点故障、
-资源非授权访问
- 网络的非法攻击
-缺少应急必要的技术支持及备机资源
-系统故障、数据丢失
....

-越权访问、误操作、恶意破坏行为无法追溯
-日志文件被破坏、篡改
...

- 患者健康信息隐私外泄
- 医护人员诊疗行为无法界定
- .....

政府对医院信息安全的要求不断增强

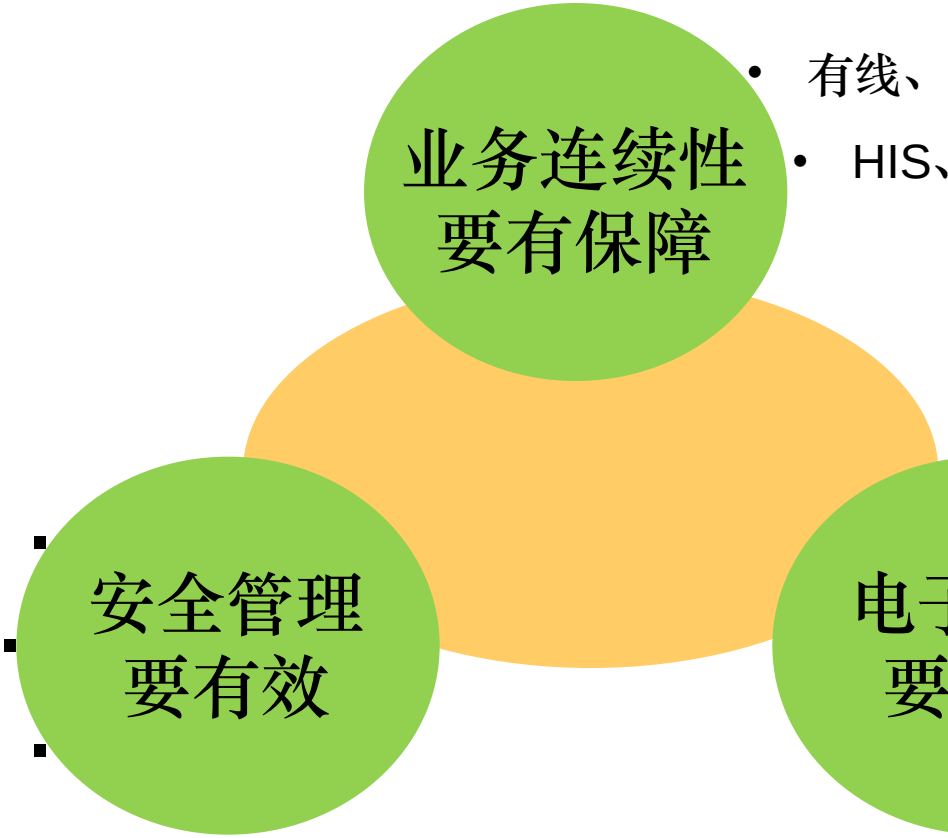
- 《关于加快推进人口健康信息化建设的指导意见》
  ——安全要同步规划、同步设计、同步实施
  ——等级保护、网络信任体系、隐私保护

- 《卫生行业信息安全等级保护工作的指导意见》
  ——三甲医院核心系统不低于三级

- 《人口健康信息管理办法》
  ——强调电子病历的安全和隐私保护

目录

医院信息安全要重点关注几个方面



- 有线、无线网络不中断
- HIS、CIS等关键系统不中断

- 安全策略得当
- 执行落实到位
- 管理手段有效

- 隐私信息不泄露
- 数据不被篡改
- 数据随时可用

抓住医院信息安全建设的关键

- 组织
- 制度
- 人才

- 身份可信
- 行为可信
- 数据可信

- 可感知
- 可分析
- 可管控

组织体系建设重点

- 建立分工明确、职责清晰的组织管理机制

全员负责

- 信息安全职责要落到每个人身上
- 全员参与，全员负责，不留缺口

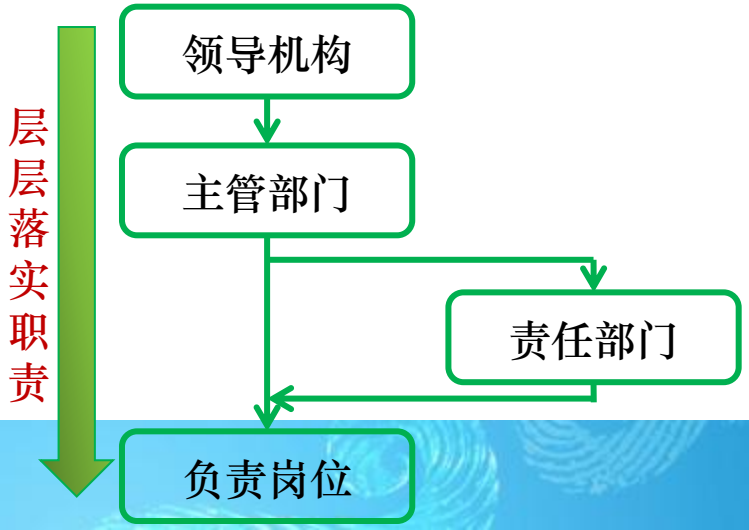
领导带头

- 院领导要亲自带头、主抓
- 各科室领导也要带头、落实

专业支撑

- 院内培养一批专业技术支撑队伍
- 依托院外第三方专业力量提供技术支撑

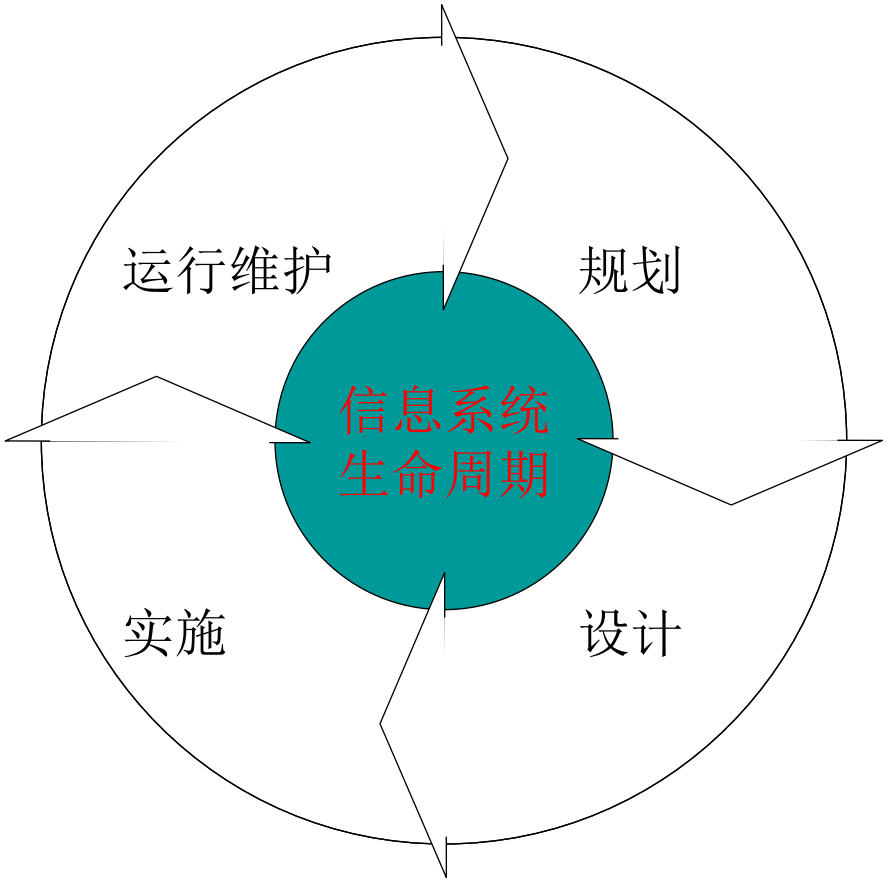
信息安全是有组织的对抗！！！



组织体系建设重点

- 围绕信息系统生命周期建立安全组织体系

- 人员管理
- 机房管理
- 介质管理
- 日常维护
- 数据备份
- 应急响应
- ……



- 安全策略
- 安全规划
- 安全设计
- 安全开发
- 安全验收
- 上线安全
- ……

组织体系建设重点

- 人是关键因素

提升人员安全意识

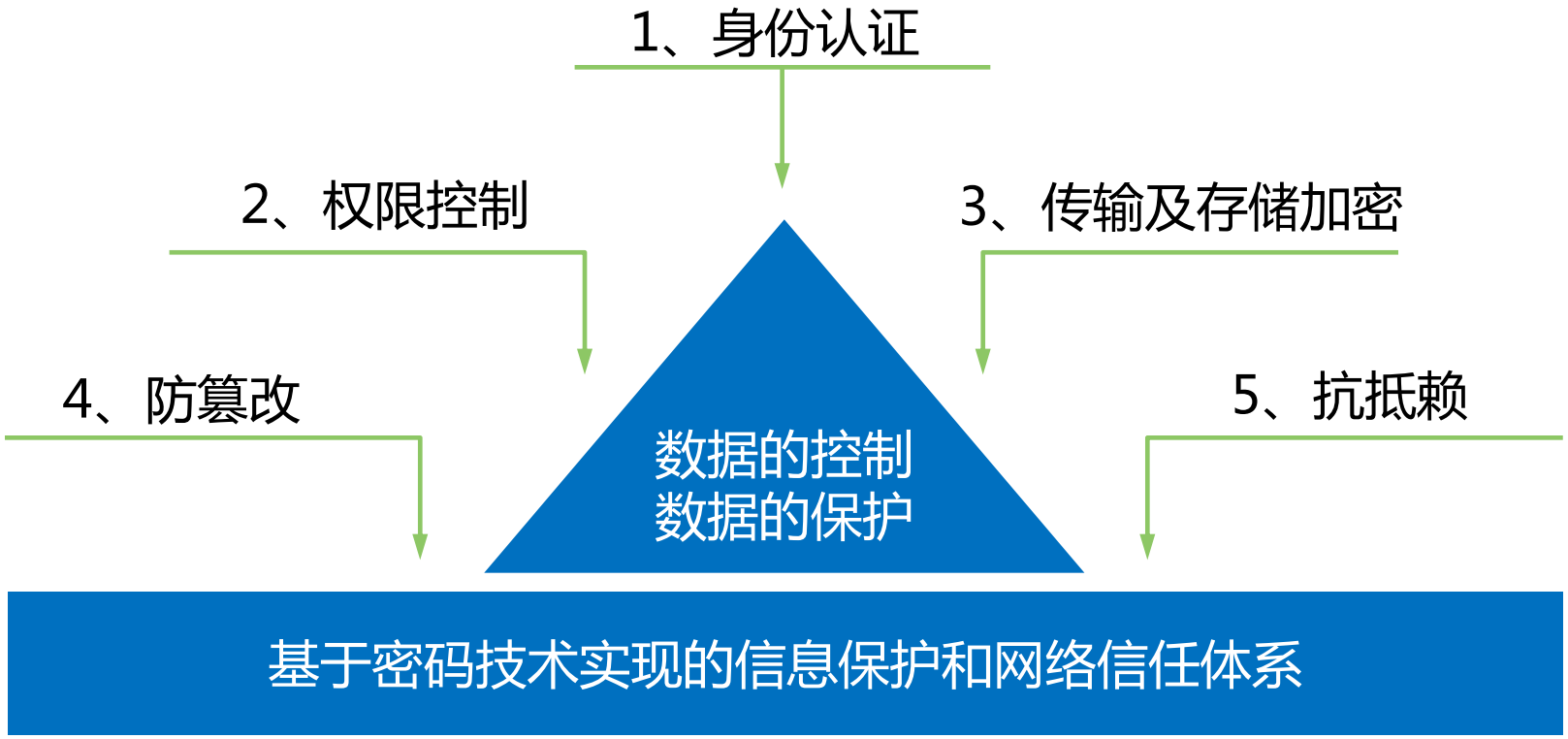
提高队伍安全技能

大数据时代信息安全需求

大数据信息安全核心业务需求

数据的控制：确定数据由谁使用，确定使用者的身份

数据的保护：落实责任，防止泄露



网络信任体系建设——数字身份管理

今天，你可以逃跑，却无处可藏

1993年
在互联网上，没有人知道你是一条狗。

"On the Internet, nobody knows you're a dog."

2013年
在互联网上，每个人都知道你时一条狗。

KPCB

Source: Quote – Joe Louis (American heavyweight boxer), 1946. Left image – Peter Steiner, cartoonbank.com, The New Yorker, 1993. Right image – Tumblr user cachorro no computador.

身份难识别

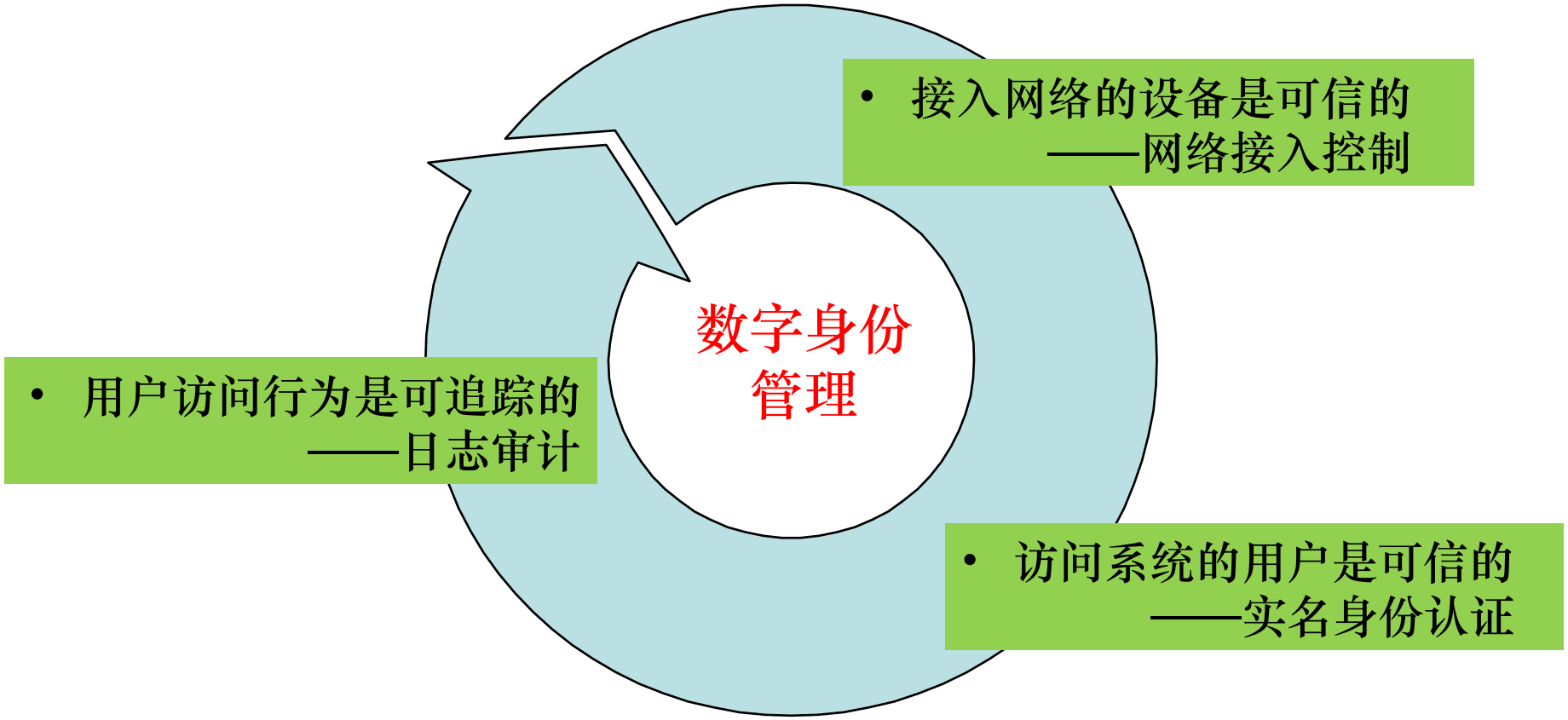
责任难确定

权力难控制

隐私难保护

网络信任体系建设

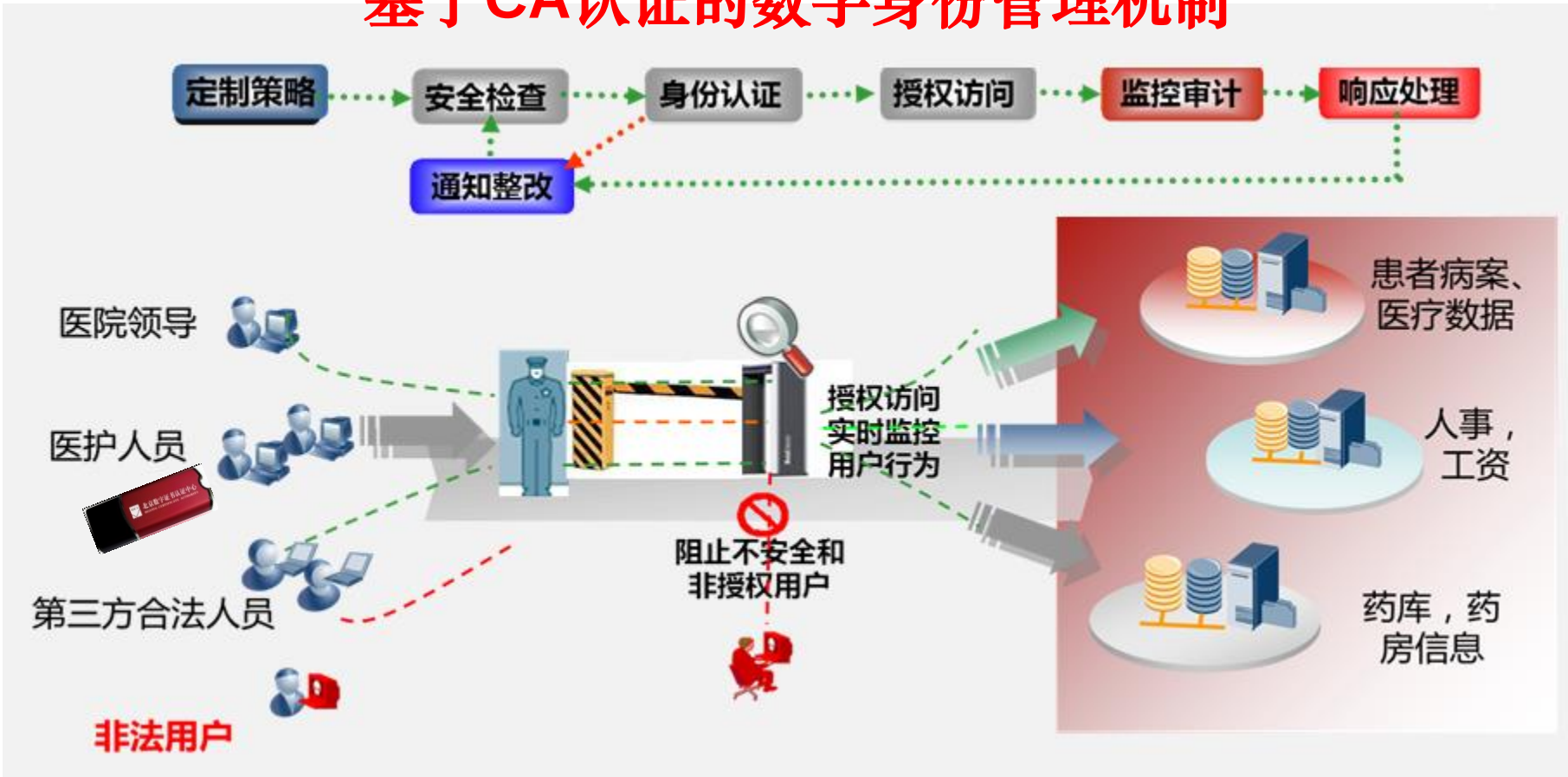
- 建立可信的数字身份管理机制



网络信任体系建设重点

- 建立可信的数字身份管理机制

基于CA认证的数字身份管理机制

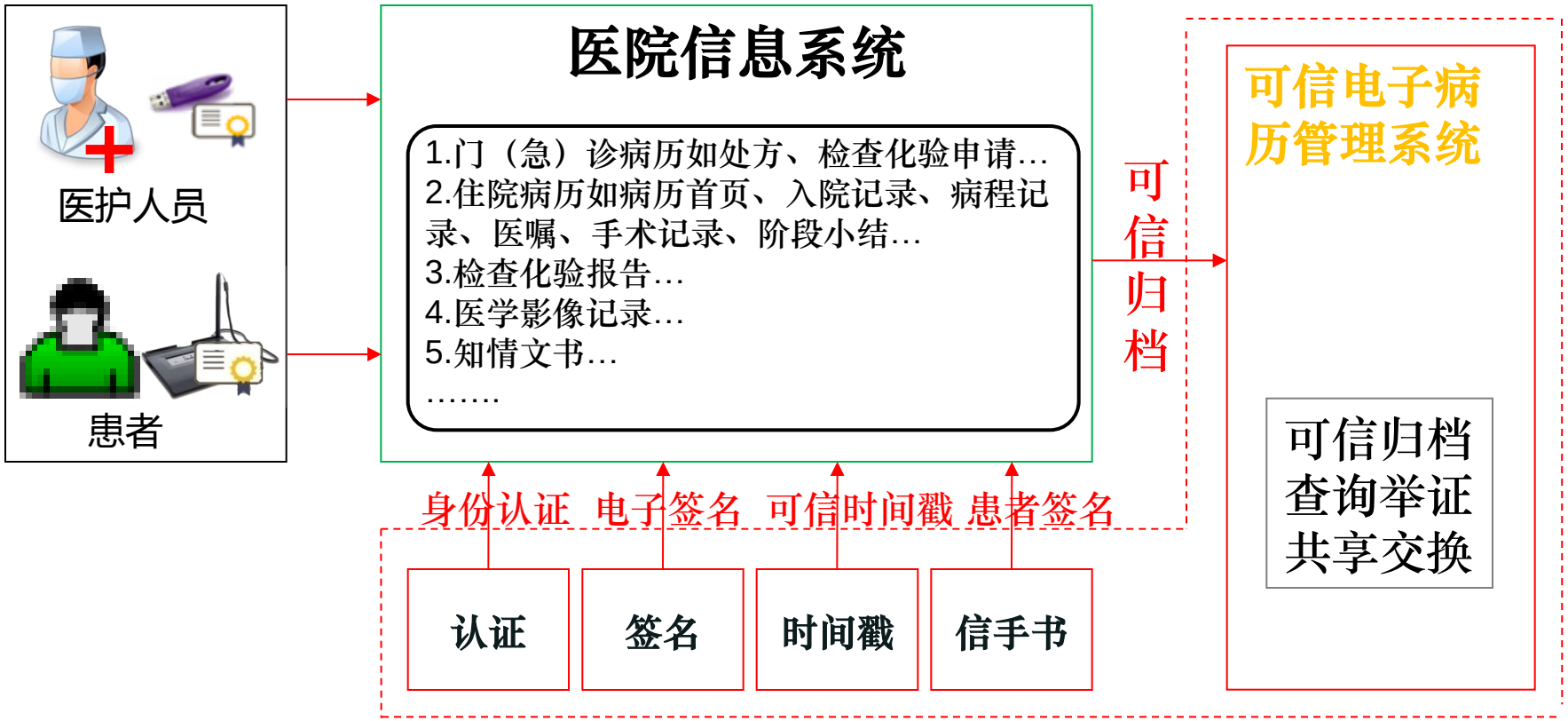


网络信任体系——可靠电子签名

- 《人口健康信息管理办法（试 行）》：符合《中华人民共和国电子签名法》 等有关法律 有关法律 法规 规 定的人口健康 电子 信息，与纸质 文本 具有同等法律效力。
- **可靠电子签名**
  - 签名制作数据由签名人专有
  - 仅由签名人控制
  - 签名改变能识别
  - 内容改变能识别

网络信任体系建设重点（二）

基于可靠电子签名，建立身份可信、行为可信、数据可信的业务环境



- 三个关键：医护人员对电子病历进行电子签名、患者对知情文书进行电子签名、电子病历可信归档

网络信任体系为医院无纸化奠定安全基础和法律基础

全部医疗过程记录实现电子化，包括电子化医嘱、电子化病程记录、电子化检查报告、电子知情同意书等。

病案归档实现电子化，包括已有纸质文件的电子化、电子化查阅、电子化封存、电子化举证等。

核心

保障电子病历的合法可信，使电子病历与纸质病历具有同等的法律效力。

电子签名

- 《电子签名法》从国家法律层面上保证了电子病历的法律有效地位
- 《人口健康信息管理办法》明确规定符合电子签名法要求的电子病历与纸质病历具有同等法律效力，从行业部门规章层面再次确认

安全运管体系建设重点

- 建设可感知、分析、展示、管理和指挥的信息安全运管体系

信息安全是高技术的对抗！！！

医院信息安全管理变轻松

- 医院信息安全态势一目了然，快速定位风险，有效调度应对

[指数化的安全风险度量]

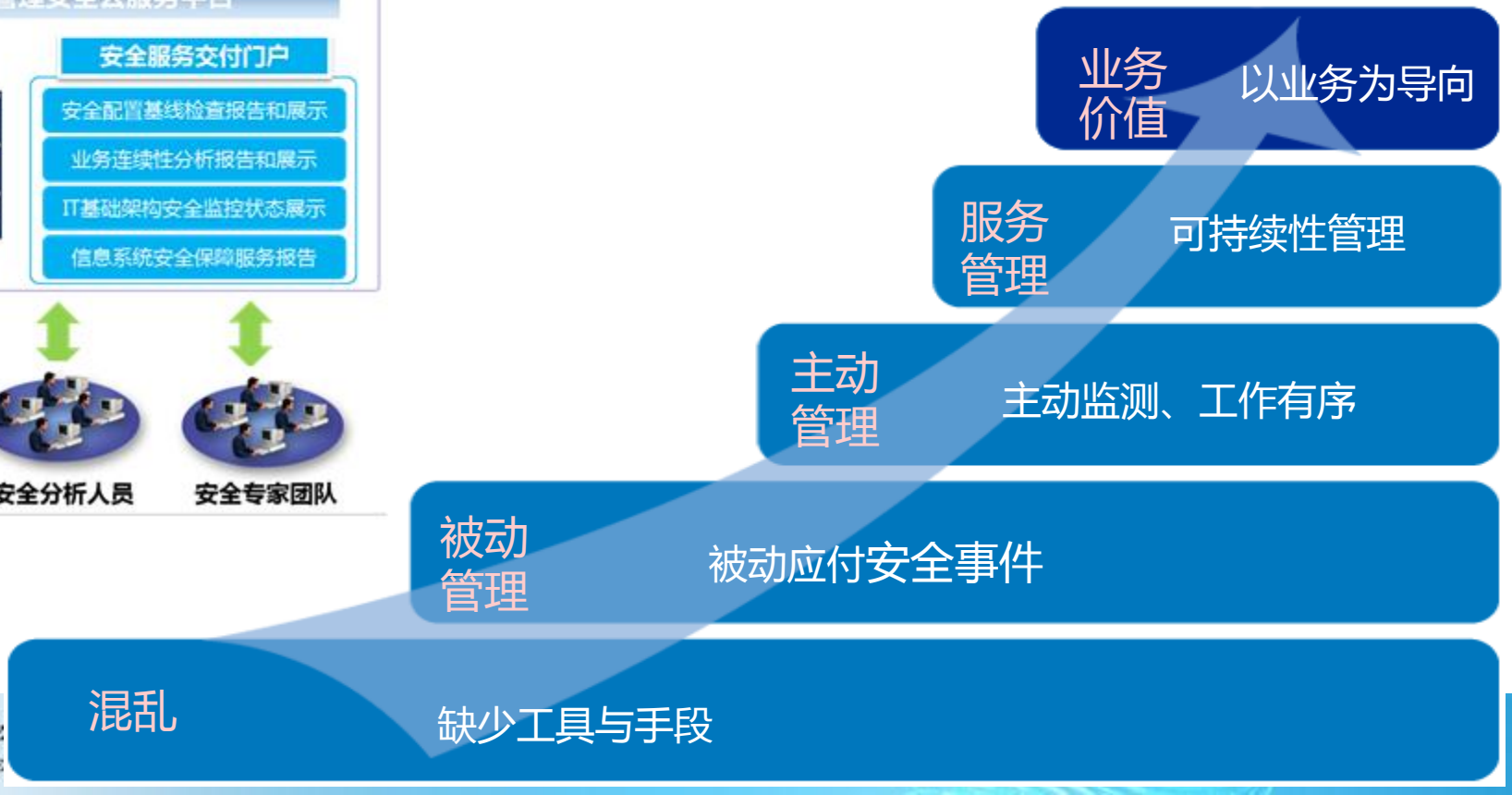
[长期的态势跟踪分析]

[漏洞分布情况总体掌握]

[不同信息系统的横向对比]

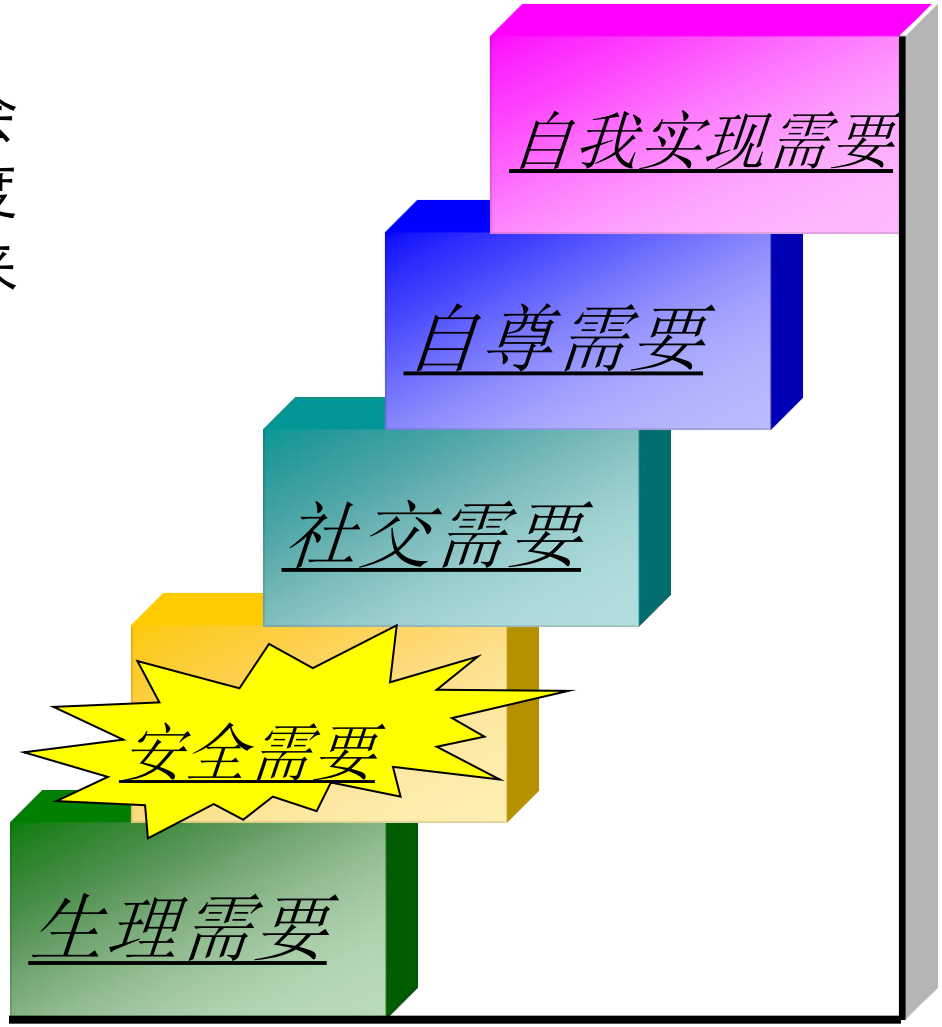
安全服务为医院信息安全提供持续保障

- 全面掌握、运筹帷幄
- 科学管理、有效调度
- 智能分析、有效支撑
- 让信息安全变得简单、可管理



总结

- 信息安全是人类在信息社会的基本需求，我们必须高度重视、科学应对，用安全来保发展、促发展



可信规范的运营

随需应变的服务

谢谢

www.bjca.org.cn