网络安全法与信息系统数据安全

北京和力记易科技有限公司

目录

CONTENTS

网络安全法

信息安全系统

容灾备份

安全系统建设

网络安全法

公布与生效

《中华人民共和国网络安全法》是我国第一部全面规范网络空间安全管理问题的基础性法律。2013年10月，列入十二届人大立法规划，2016年11月7日发布，2017年6月1日起施行。

条款

《中华人民共和国网络安全法》共分七章七十九条：第一章 总则；第二章 网络安全支持与促进；第三章 网络运行安全；第四章 网络信息安全；第五章 监测预警与应急处置；第六章 法律责任；第七章 附 则

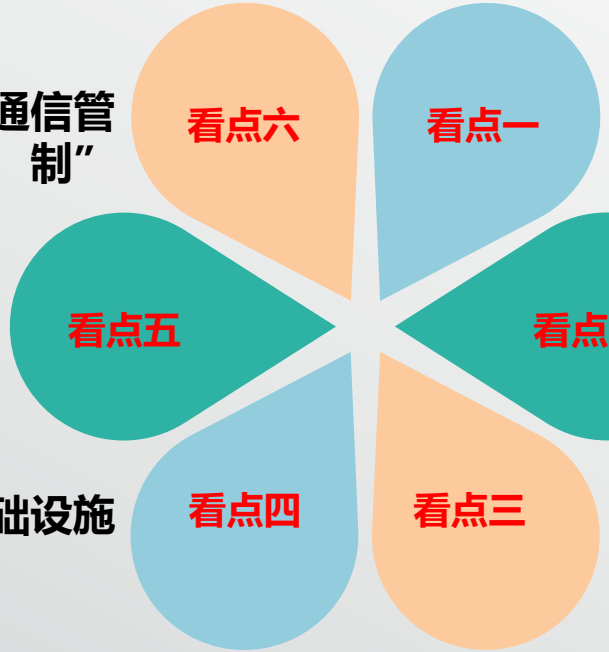
基本原则

第一，网络空间主权原则。适用于我国境内网络以及网络安全的监督管理。
第二，网络安全与信息化发展并重原则。
第三，共同治理原则。政府、企业、社会组织、技术社群和公民等相关者的共同参与。

重点解读

提出制定网络安全战略，明确网络空间治理目标；明确了政府各部门的职责权限，完善了网络安全监管体制；强化了网络运行安全，重点保护关键信息基础设施；完善了网络安全义务和责任，加大了违法惩处力度；将监测预警与应急处置措施制度化、法制化。

网络安全法



重大突发事件可采取“网络通信管制”

不得出售个人信息

惩治攻击破坏我国关键信息基础设施的境外组织和个人

严厉打击网络诈骗

重点保护关键信息基础设施

以法律形式明确“网络实名制”

法律是规则和要求，明确了义务和责任，需要在信息系统建设和运营中落实；
法律是依据和保障，是信息安全建设的后盾，安全事故界定惩处依据；

法律有威慑力，但不能替代信息系统安全建设；
法律解决了“大政方针”，需要具体技术产品应用手段落实；
法律制定了惩处规则，是最后手段，做好预防才可以减少损失；

网络安全法的施行会大大促进我国信息系统安全建设！

信息系统安全

- 物理安全
- 主机及其计算环境安全
- 网络通信安全
- 边界安全
- 应用安全
- 数据安全
- 安全管理与支持
- 安全保密监管

信息系统安全等级

第一级：应能够防护系统免受来自个人的、拥有很少资源的威胁源发起的恶意攻击、一般的自然灾难、以及其他相当危害程度的威胁所造成的关键资源损害，在系统遭到损害后，能够恢复部分功能。

第二级：应能够防护系统免受来自外部小型组织的、拥有少量资源的威胁源发起的恶意攻击、一般的自然灾难、以及其他相当危害程度的威胁所造成的重要资源损害，能够发现重要的安全漏洞和安全事件，在系统遭到损害后，能够在一段时间内恢复部分功能。

第三级：应能够在统一安全策略下防护系统免受来自外部有组织的团体、拥有较为丰富资源的威胁源发起的恶意攻击、较为严重的自然灾难、以及其他相当危害程度的威胁所造成的主要资源损害，能够发现安全漏洞和安全事件，在系统遭到损害后，能够较快恢复绝大部分功能。

第四级：应能够在统一安全策略下防护系统免受来自国家级别的、敌对组织的、拥有丰富资源的威胁源发起的恶意攻击、严重的自然灾难、以及其他相当危害程度的威胁所造成的资源损害，能够发现安全漏洞和安全事件，在系统遭到损害后，能够迅速恢复所有功能。

第五级：最高等级，略

信息安全系统常用设备系统

事前——防范

安全网关
防火墙

防病毒系统

电子签名/签章系统
身份鉴别系统

数据备份系统

安全保密评估

事后——处理解决

容灾系统

安全审计系统
杀毒系统

数据安全

数据是信息系统的重要组成部分，是重要的资产。

容灾备份

数据级灾备

数据级灾备侧重的是数据的备份和恢复，包括数据的复制、 备份、 恢复等在内的数据级灾备是所有灾备工作的基础，在灾备恢复的过程中，数据恢复是最底层的。

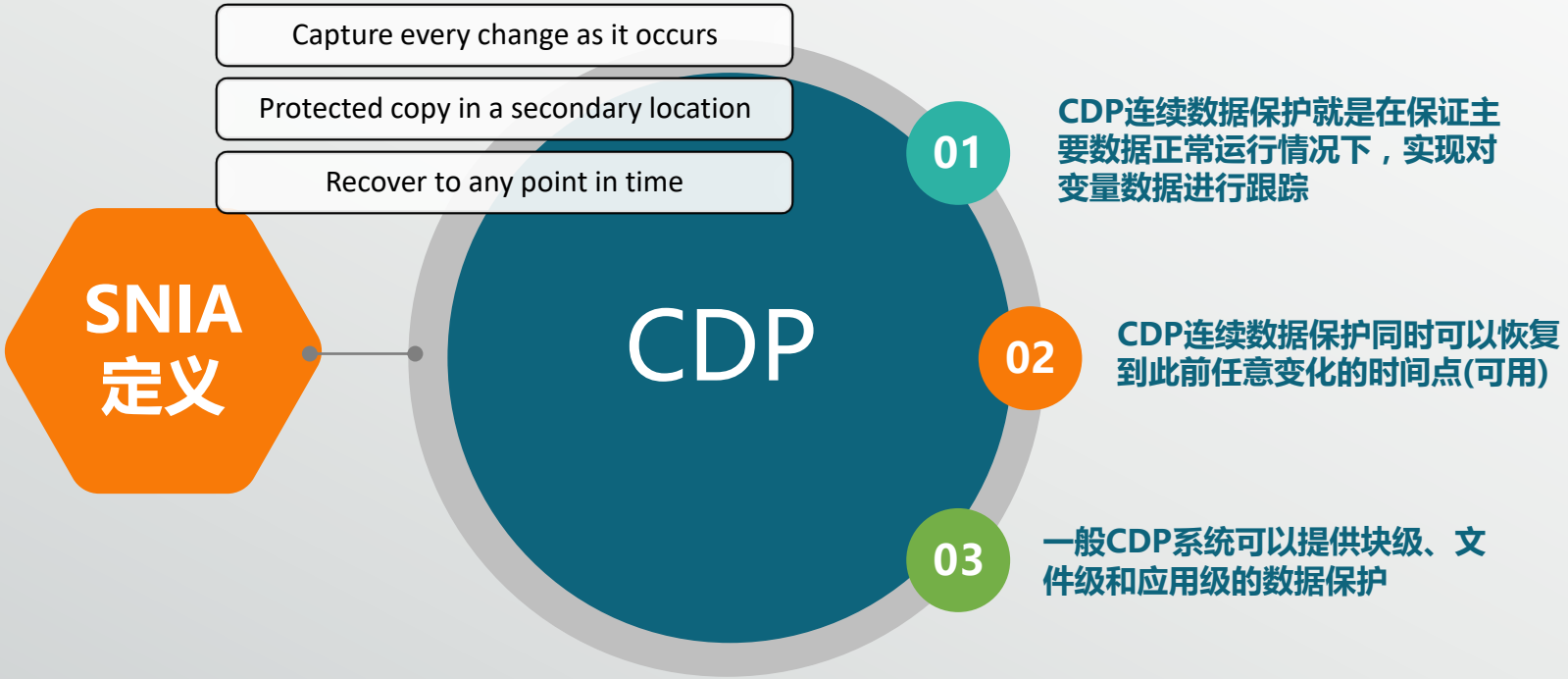
应用级灾备

应用级灾备则是侧重于具体的功能，提供比数据级灾备更高级别的业务恢复能力，同时也是业务级灾备的基础，只有具体应用得到恢复，后续的业务才能有效进行。

业务级灾备

业务级灾备则是最高级别的灾备，如果说数据级灾备、 应用级灾备都是在IT系统的范畴之内的话，业务级灾备则是在以上应用级灾备的基础上，还需考虑到 IT 系统之外的业务因素。

CDP——持续数据保护


Capture every change as it occurs
Protected copy in a secondary location
Recover to any point in time
SNIA
定义
CDP
01
CDP连续数据保护就是在保证主要数据正常运行情况下，实现对变量数据进行跟踪
02
CDP连续数据保护同时可以恢复到此前任意变化的时间点(可用)
03
一般CDP系统可以提供块级、文件级和应用级的数据保护

CDP——持续数据保护

- **应用级CDP**

应用CDP系统只针对受保护应用系统，典型的比如 ：备特佳、My SQL主从复制，Oracle DataGuard等。

优势：数据传输量/处理量小、接管、双活

劣势：每套软件只适应特定应用、无法解决应用底层的损坏

- **卷CDP**

卷CDP采用在磁盘驱动层完成写入分离，复制，重放，备份。

优势：能适应更多的数据类型，结构化数据（数据库），非结构化数据（文件、目录），操作系统、数据分区。任意秒级回退，RPO=0。

劣势：需独立解决应用的逻辑性。

各种灾备技术的比较

方案	应用冗余	数据0丢失	数据冗余	数据100%可用	任意时间点回退	指定时间点回退	远距离异地容灾
定时备份	否	否	是	否	否	是	是
单柜HA方案	是	否	否	否	否	否	否
双柜HA方案	是	是	是	否	否	否	否
镜像方案	否	是	是	否	否	否	否/异步的可以
快照方案	否	否	是	否	否	是	否
日志重做	否	否/是-同步模式	是	是	否	否	是异步模式
CDP方案	是	是	是	是	是	是	是

数据灾备重要性

永恒之蓝病毒（ WannaCry ）：勒索病毒，加密用户文档，2017年5月全球大爆发。100多个国家和地区超过10万台电脑遭到了勒索病毒攻击、感染。至少150个国家、30万名用户中招，造成损失达80亿美元，已经影响到金融，能源，医疗等众多行业，造成严重的危机管理问题。中国部分Windows操作系统用户遭受感染，校园网用户首当其冲，受害严重，大量实验室数据和毕业设计被锁定加密。部分大型企业的应用系统和数据库文件被加密后，无法正常工作，影响巨大。

信息安全建设

1 规划设计

依据：国家政策法规、行业规范等
设立目标、解决急所、长期战略、分步实施
最好有专业人士/公司整体设计

2 选型采购/开发

技术、产品、服务、使用、维护、价格、兼容、时效；
供应商实力、口碑、研发能力

3 安装实施

按时供货实施
安装使用培训
系统接口兼容
严格测试验收

4 运维使用

应急预案及安全事故处理规则
日常运维+厂商保障
安全演练
安全审计

5 升级改造

业务系统增加、软硬件增加造成安全系统增加
信息安全系统升级
信息系统安全等级升级

软硬兼施

预防与解决并重

分阶段持续建设

既要在硬件上投入，也要加大软件投入，还要在运维服务上投入；

系统设计侧重防范，也要注意事故之后能快速应对，保证业务连续性；

高目标，分阶段，区分业务重要性，从数据级到应用级，从本地到异地到两地三中心

Thank You

谢 谢