术语—机密性

CEC 中国电子

机密性

是保证信息系统不被非授权获取以及非授权者不可理解的属性，通常通过加密、访问控制等方法来应对。

术语—可鉴别性

CEC 中国电子

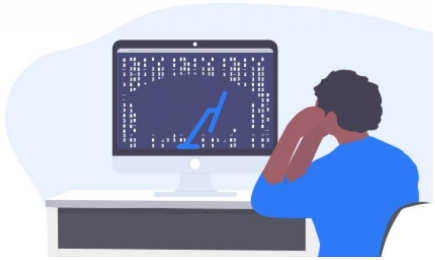
可鉴别性

力保信息的真实状态可鉴别，即信息没有被篡改、身份是真实的、对信息操作不可抵赖。

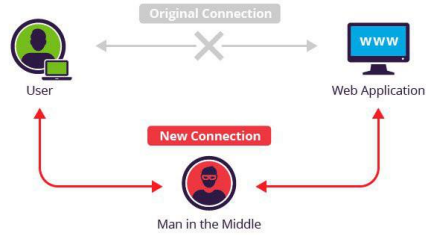
攻击者

不可篡改、不可伪造、不可抵赖

勒索加密



Wiper擦除



中间人攻击

伪造签名

术语—可控性

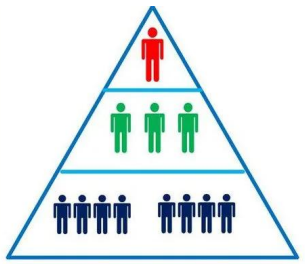
CEC 中国电子

可控性

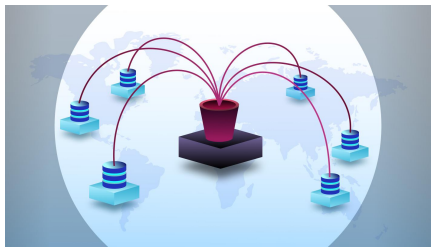
是指信息系统的运行状态与信息流动被所有者所知晓并操控的能力，力保信息系统总能按照所有者的预期运行

控 制 者

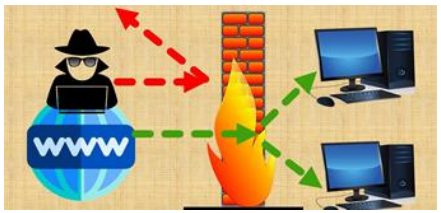
信息阻断、系统操控



权限分配



数据流动管理



防止恶意操控

系统状态监控

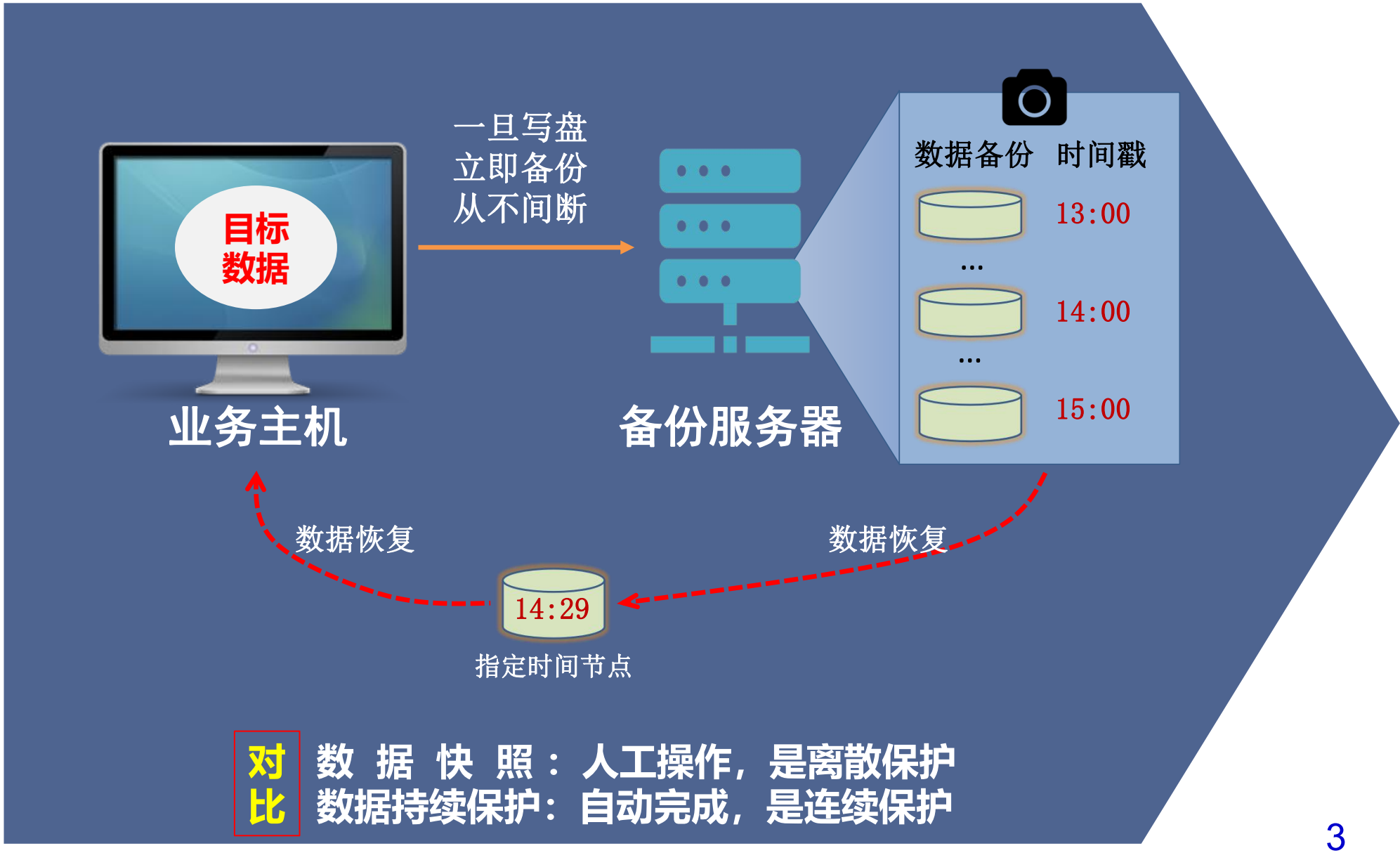
敏感信息、重要系统

术语—数据持续保护

CEC 中国电子

数据持续保护

自动、实时的对目标数据进行细粒度的持续备份，并且能将目标数据恢复到任意指定的时间节点。



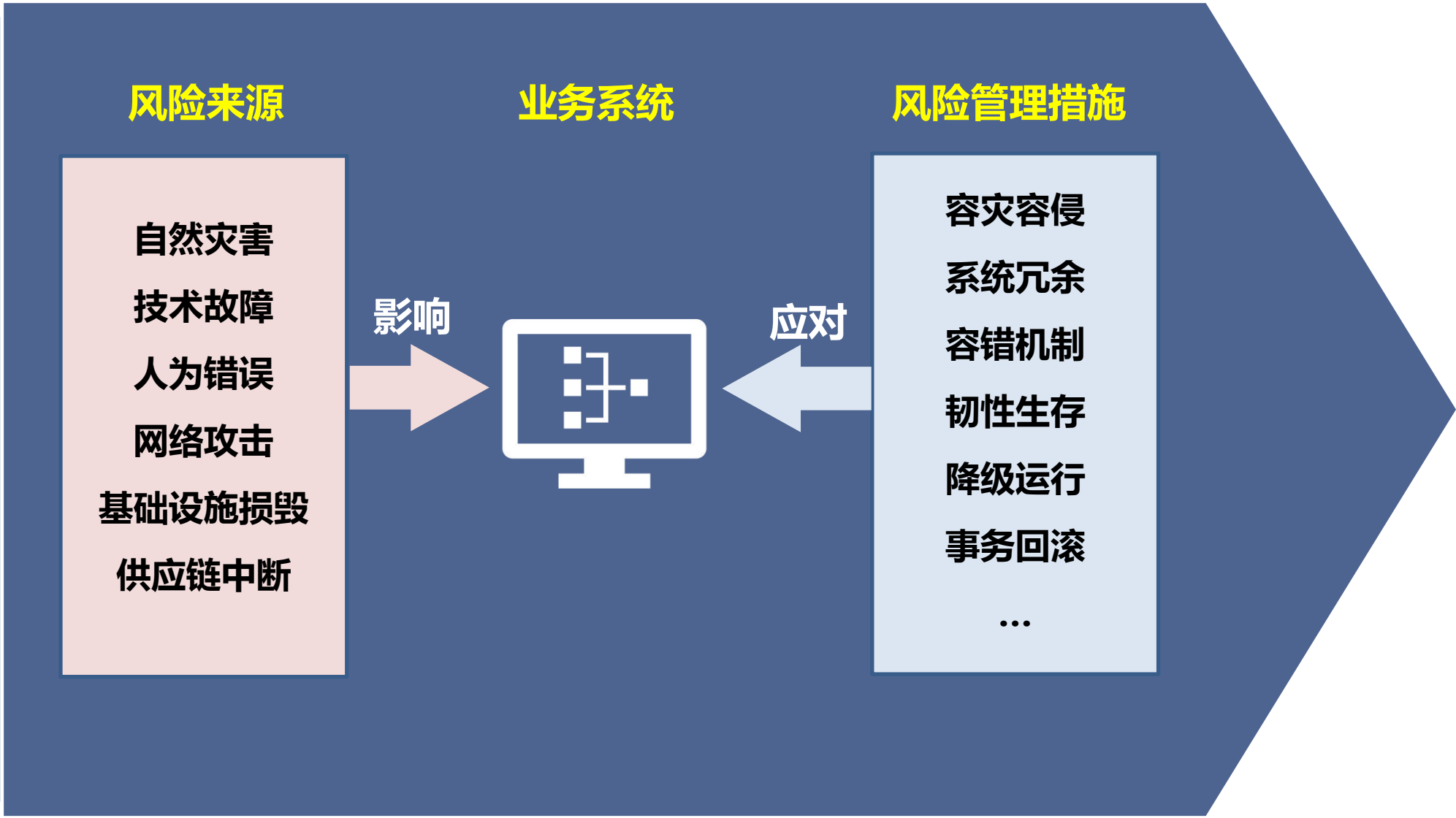
对比 数 据 快 照：人工操作，是离散保护
数据持续保护：自动完成，是连续保护

术语—业务可连续运行

CEC 中国电子

业务可连续运行

在面对自然灾害、设备故障、人为失误、网络攻击等干扰时，通过风险管理措施，力保业务系统在一定程度上保持正常运行。



术语—应急响应

CEC 中国电子

应急响应

通常是指一个组织为了应对各种意外网安事件的发生所做的准备以及在事件发生后所采取的措施。

术语—应急响应

CEC 中国电子

应急响应

通常是指一个组织为了应对各种意外网安事件的发生所做的准备以及在事件发生后所采取的措施。

术语—隐私保护

CEC 中国电子

隐私保护

通过法律、技术等手段保护个人或团体不愿泄露的敏感信息，以防止其被未经授权的访问和利用。

术语—合规使用

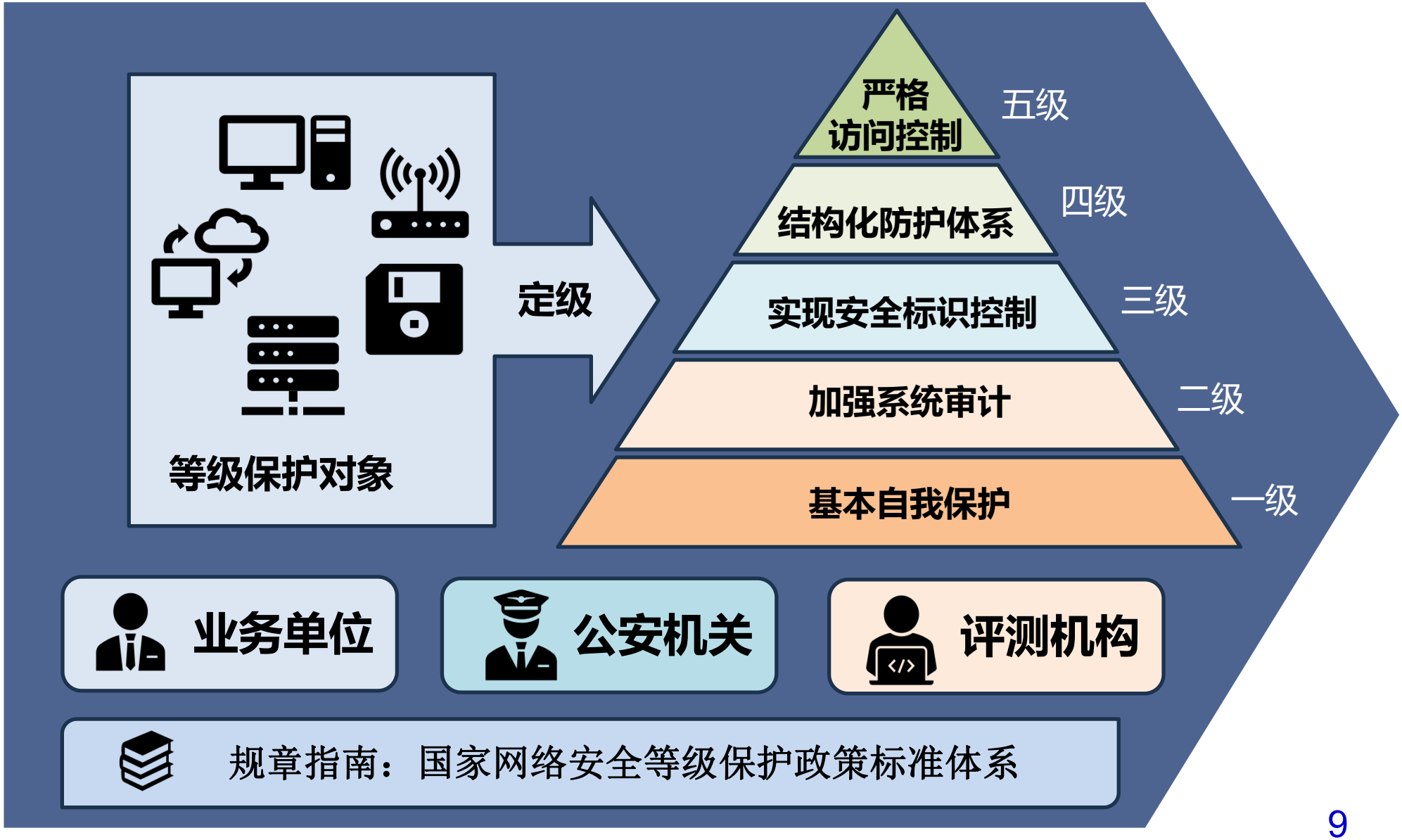
CEC 中国电子

合规使用

根据法律法规、政策规定以及组织内部制定的安全政策和规程，正确、合法地使用计算机系统、网络设备和信息资源的行为。

术语—等级保护

等级保护针对不同重要程度的网络系统，根据安全风险大小划分不同安全保护等级，制定相应的安全要求，从而提高系统的安全防护能力。



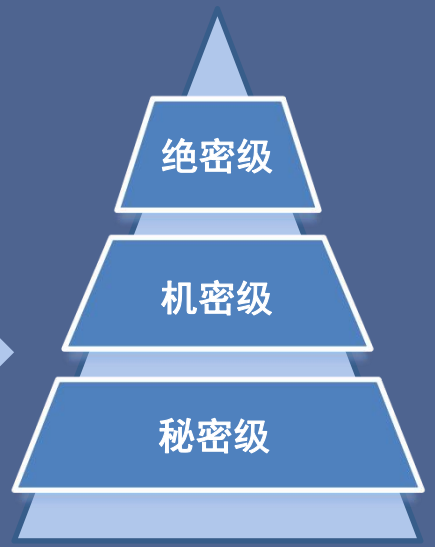
术语—分级保护

CEC 中国电子

分级保护

涉密信息系统的建设和使用单位根据分级保护管理办法和有关标准，对涉密信息系统分等级实施保护，力保系统和信息安全。

涉密信息系统



分级保护级别

秘密级、机密级：
每两年至少一次

绝密级：
每年至少一次

测评与检查

《涉及国家秘密的信息系统分级保护管理办法》
《涉及国家秘密的计算机信息系统分级保护技术要求》
《涉及国家秘密的信息系统分级保护管理规范》

术语—数据治理

CEC 中国电子

数据治理

面向不同类型数据，通过一系列手段，覆盖全生命周期开展的管控活动，旨在满足不同场景下数据应用的需求