机器学习基本知识：

随着承载人们工作、生活的移动互联网、云计算、大数据、物联网、机器学习等技术的迅猛发展，网络空间安全所面临的环境日益复杂，面对的安全威胁也日益升级。在这种复杂环境下，传统的以分析安全问题、固定规则设定的研究方法变得效率低下、甚至无能为力。例如依靠安全专家人工修复方法无法解决零日漏洞问题;传统依靠固定规则的网络人侵检测方法，面对不断增大的数据维度和复杂的网络行为，出现大量误判警告或判别时间较长;依靠固定规则或黑自名单过滤的垃圾邮件检测方法存在检测效率低，规则更新不及时等问题。随着网络空间安全问题的复杂度越来越高，数据维度不断增加，对网络空间安全问题的研究提出了新的需求。近年来，机器学习在计算机视觉、语音识别、自然语言处理、医疗数据分析等方面的应用取得了瞩目的研究成果，展现了机器学习在解决分类、预测以及辅助决策中强大的能力。机器学习技术为解决传统方法难以建模的网络空间安全问题提供了可能性。

机器学习作为人工智能的核心体现，简单来看即为一组可以通过

经验数据对系统本身性能进行一定程度优化的算法合集。机器学习的

基本方式即指使计算机对人类行为进行模拟，并通过学习的方式，使

计算机功能与知识体系更加人性化、智能化、丰富化发展。机器学习

在实际研究中具有许多方向，在整体上来看，机器学习与推理过程具

有十分紧密的联系，所以在机器学习方式的分类上具有一定的共识。

考虑到该学习的内容复杂性、范围广泛性、学科交叉性等特点，其包

含了多样技术与知识体系的融合渗透，比方说概率论、统计学、逼近

学等等。进行具体分类主要有五种，一是从学习方式不同包括了实例

学习、类比学习、传授学习、机械学习、归纳学习等;二是由知识获

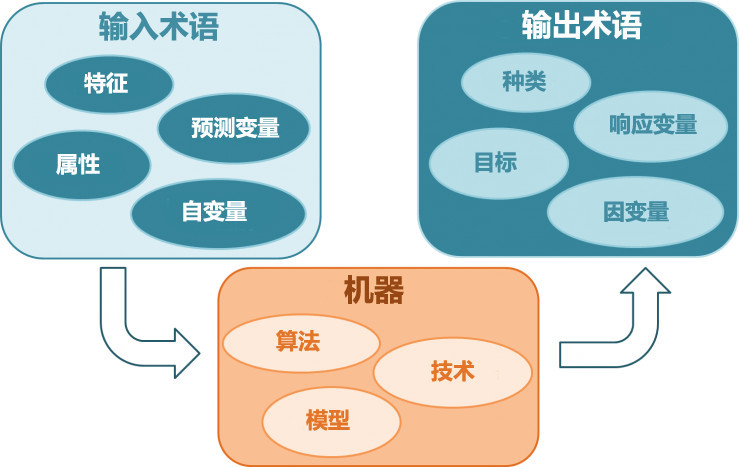
得表现的形式差异，包括决策树、形式文法、逻辑表达式、图和网络、

计算机程序、框架和模式以及其他的编程形式等;三是根据应用领域

内容，包含自然语言、认知模拟、数据挖掘、故障诊断、专家系统等;

四是从综合分类角度，包括了类比算法、遗传算法、连接学习、分析

学习等;五即是学习形式分类，有监督与非监督之分。



机器学习在网络空间安全研究中的应用：

机器学习在入侵检测中的应用：

在机器学习中，分类方法的任务就是要确定待分析的数据中，哪些对象属于哪个预定义的目标类。将机器学习的分类方法应用到入侵检测中，就是把入侵检测看作一种分类问题，其目标就是将待检测的源数据分类为正常活动和人侵行为。

基于分类方法的人侵检测过程可以归纳为:首先使用包含正常和各种人侵的历史数据作为训练模型，再应用分类算法在数据上进行学习，建立分类模型，分类模型可以转化为识别正常活动和各种人侵行为的规则;最后使用这些规则对新的待检测数据进行分类判断，判断它是正常活动还是人侵行为。

机器学习中的分类方法能够从大量的审计数据和网络数据中抽取出能充分描述网络连接和主机会话的特征，并学习出分类模型，发现待检测数据中隐藏的人侵行为的分类规则。机器学习的分类方法已在人侵检测中得到广泛的应用，其中决策树、贝叶斯定理、最邻近、支持向量机、人工神经网络等经典分类方法都已被应用到人侵检测中。

机器学习在恶意软件检测中的应用：

近年来，出现了许多基于机器学习算法的恶意软件检测的研究，同时机器学习以大量应用于恶意软件检测中，并取得了良好的成果。目前，研究人员将机器学习技术用于检测恶意软件比较成熟的技术有分类技术、聚类技术等。

分类技术在恶意软件检测中的基本原理是对已知的恶意软件和正常样本数据进行学习，采用合适的分类算法构建恶意软件的分类模型，再通过这个分类模型对未知文件进行监测，判断其是否为恶意软件。基于分类技术的恶意软件检测过程包含两个步骤:训练恶意软件分类模型和检测恶意软件。在训练恶意软件分类模型中首先从文本训练样本中提起文本特征，然后构建样本特征数据库，最后采用一定的机器学习算法训练处恶意软件分类模型。当恶意软件分类模型生成后，提取待检测样本中的特征数据来构建文本样本检测数据集，结合训练好的恶意软件分类模型对待检测数据集进行分类，最终得到检测结果。在机器学习中，决策树分类算法、贝叶斯分类算法、关联分类算法在恶意软件检测中均以成功应用。