# 机器学习的定义：

机器学习就是让机器帮我们找一个人类写不出来的复杂函数，比如语音辨识、影像辨识、阿尔法狗等都是通过找函数来实现的。

# 课程重点：

课程主要着重在机器学习中的深度学习，其函数是用类神经网络的类型，输入可以是向量、矩阵、序列等，输出可以是数值、类别、句子、图片等，课程会讲解如何用类神经网络制造这些函数。

# 监督学习：

使用监督学习，以宝可梦和数码宝贝的分类为例，需要收集大量训练资料并做标记，让机器自动找出函数，但其缺点是做标记耗费人工，收集的标记资料往往不多。

# 自监督学习：

为解决监督学习的问题，提出自监督学习，先通过预训练让机器练好基本功，再做下游任务，以影像辨识为例，练基本功时不需要标注，只需大量影像资料，机器通过学习基本任务，如分辨左右反转、变色的图片是否相同，就能在下游任务上有好的结果。

# 生成式对抗网络：

生成式对抗网络，其关键应用是在没有大量成对资料时，只需收集大量X和Y，机器就能自动找出它们之间的关联，比如语音辨识，无需声音讯号和文字一一对应，机器也能学会。

# 强化学习：

当不知道怎么标注资料但可以判断好坏时用强化学习，比如下围棋，人类不知道最佳落子位置，但可以定义赢为好，输为坏，就可用强化学习技术。

# 进阶课题：

课程还会讲异常检测、可解释性AI、模型攻击、领域自适应、模型压缩、终身学习、元学习等进阶课题。异常检测让机器具备回答“不知道”的能力；可解释性AI让机器不仅能回答正确答案，还能说明原因；模型攻击展示对模型的攻击技术和防御可能性；领域自适应解决训练资料和测试资料分布不同的问题；模型压缩让巨大模型能在手机等设备上运行；终身学习探讨机器不断学习新技术的挑战；元学习让机器从大量任务中自己发明新的演算法。