高纲 4078

江苏省高等教育自学考试大纲

14383　物联网信息安全技术

南京信息工程大学编（2024 年）

Ⅰ　课程性质与课程目标

一、课程性质和特点

《物联网信息安全技术》课程是江苏省高等教育自学考试物联网工程专业（专升本）中的必设课程，是为培养和检验考生物联网信息安全技术基本知识和技能而设置的一门专业性课程。

物联网技术是通过物物互连实现感知世界的技术手段。物联网是在现有网络框架基础上的延伸，数量庞大的物联网终端将实现范围更加广阔的互连互通。

本课程主要涉及物联网信息安全技术。物联网信息安全技术旨在解决设备的安全连接问题，可以支持动态组网并灵活实现与上层网络的信息交互功能。该技术定位满足了物联网终端组网，以及物联网终端网络与电信网络互连互通的要求，是物联网信息安全技术在物联网发展背景下彰显活力的根本原因。无线技术已经广泛应用于热点覆盖、家庭办公网络、家庭数字娱乐、智能楼宇、物流运输管理等方面，并以其丰富的技术种类和优越的技术特点，满足了物物互连的应用需求，逐渐成为物联网架构体系的主要支撑技术。因此，学好本课程对物联网工程专业的考生具有重要的意义。

本课程系统介绍信息安全的基础知识，概述物联网的基本概念和主要特征，分析物联网所面临的安全挑战，提出物联网安全的体系结构，同时阐述物联网安全主要的关键技术；分别从感知层安全、网络层安全、应用层安全及安全管理等方面对物联网安全进行了介绍，包括传感器网络安全、RFID 安全、核心网安全、移动通信接入安全、无线接入安全、数据处理安全、数据存储安全、云安全、安全管理等，并举例说明物联网安全技术的典型应用，最后对物联网安全技术的发展趋势进行了总结。通过本课程的学习，使考生对近几年来物联网安全技术的研究成果及其发展趋势有一个整体的了解，为以后从事物联网相关的研发工作打下坚实的基础。

物联网信息安全技术课程设置的目的旨在培养物联网工程专业人才，使其具备基本的无线通信知识和技能。通过对无线通信理论、技术和方法的系统学习和具体操作实践，培养物联网工程专业考生的物联网信息安全技术能力，为将来的学习和工作打下坚实的基础。

二、课程目标

课程设置的目标是使得考生：

1. 了解物联网信息安全技术在物联网工程专业中的地位和作用，发展对物联网信息安全技术的兴趣和热爱，欣赏物联网信息安全技术对经济发展和社会进步的贡献。

2. 理解几种物联网信息安全技术之间的联系和区别，以及物联网信息安全技术与其他物联网技术领域的联系。

3. 掌握物联网信息安全技术的基本概念、基本原理、基本技术和基本方法。

4. 提高分析和解决无线通信实际问题的能力。

三、与相关课程的联系与区别

从技术架构上，物联网可以分为三层：感知层、网络层和应用层。传感器原理及应用课程、嵌入式系统设计课程、射频识别技术与应用课程属于感知层范畴，物联网信息安全技术课程主要涉及物联网的网络层技术，是物联网结构中感知层过渡到应用层的重要课程，主要涉及感知层信息的传输问题。

按照物联网的层次体系分为三大部分：物联网感知层安全、物联网网络层安全和物联网应用层安全。本书共分 8 章：物联网安全概述、网络信息安全技术基础、物联网安全体系结构及物理安全、物联网感知层安全、物联网网络层安全、物联网应用层安全、物联网安全技术应用和典型物联网安全实例。在第 2、4、5、7 章的后面配有物联网安全技术应用实训内容；在第 5 章介绍了 3G、4G 移动通信系统安全机制的分析和应用；在第 6 章介绍了云计算安全的内容以及物联网信息安全标准；在第 7 章重点讲述了物联网安全技术的设计，介绍了 EPCglobal 网络安全技术的应用；第 8 章主要介绍典型物联网应用中的安全案例，重点讲述了物联网和云计算在智慧医院中的应用，例如 WLAN 在医院病床查询中的应用，WBAN 在远程医疗中的应用及其安全技术，无线体域网远程医疗系统的安全实例，此外，还简单介绍了 M2M 安全实例以及车联网的安全分析。

物联网信息安全技术课程与数据通信基础同属于网络层范畴，都涉及感知层信息的传输问题，但两者所讲述的技术不同。物联网信息安全技术课程侧重于感知层信息通过无线通信网传输的相关技术，而数据通信基础课程侧重于感知层信息通过计算机网络传输的相关技术。

四、课程的重点和难点

本课程的重点：物联网的概念和关键技术；各种物联网信息安全技术特点的比较；网络安全基本概念；网络层安全协议 IPSec；入侵防御技术；统一威胁管理 UTM；物联网安全体系结构；物联网安全技术措施；感知层安全；EPCglobal 网络安全技术应用。

本课程的难点：物联网的安全层次模型及体系结构;物联网的安全技术分析;无线传感器网络的安全攻击与防御；传感器网络安全防护主要手段；近距离无线低速接入网安全；有线网络接入安全；卫星通信接入安全；云计算安全问题；云计算安全需求；EPCglobal 物联网的网络架构。

II　考核目标

本大纲在考核目标中，按照识记、领会、简单应用和综合应用四个层次规定其应达到的能力层次要求。四个能力层次是递升的关系，后者必须建立在前者的基础上。各能力层次的含义是：

识记：要求考生能够识别和记忆本课程中有关物联网信息安全技术的基本概念、技术特点、应用范围及发展状况的主要内容，并能够根据考核的不同要求，做正确的表述、选择和判断。

领会：要求考生能够领悟和理解本课程中各种物联网信息安全技术的基本原理和关键技术以及分析方法，理解各种物联网信息安全技术的区别和联系，并能根据考核的不同要求对物联网信息安全技术的相关内容进行融汇贯通，做出正确的判断、解释和说明。

简单应用：要求考生能根据有关物联网信息安全技术的协议、工作原理、组网技术、安全问题，对具体无线通信问题进行分析和讨论。

综合应用：要求考生能够面对具体、实际的通信需求，搭建简单的通信网络，进行相应的分析和讨论。

III　课程内容与考核要求

第 1 章　物联网安全概述

一、学习目的与要求

理解物联网的概念和物联网安全的概念；掌握物联网的体系结构和关键技术；熟悉物联网安全层次模型及整体安全架构。

二、考核知识点与考核要求

（一）物联网安全概述

识记：①物联网安全的概念。

领会：①物联网的体系结构；②物联网安全的关键技术。

（二）物联网安全问题分析

识记：①物联网安全与相关学科的关联；②物联网安全威胁；③物联网安全需求分析。

（三）物联网的安全架构

识记：①物联网的安全层次模型及体系结构模型。

领会：①物联网的安全层次模型及体系结构；②物联网安全的总体概貌与整体安全架构。

（四）物联网安全的技术分析

领会：①物联网安全技术分析方法。

三、本章的重点和难点

本章重点：①物联网的概念和关键技术；②各种物联网信息安全技术特点的比较。

本章难点：①物联网的安全层次模型及体系结构；②物联网的安全技术分析。

第 2 章　网络信息安全技术基础

一、学习目的与要求

理解网络信息安全基础知识；掌握网络安全的数字加密技术、数字签名技术以及网络层安全协议 IPSec；正确分析防火墙技术、入侵检测和入侵防御等技术。

二、考核知识点与考核要求

（一）网络安全基本概念

识记：①网络安全基本概念；②网络安全简介。

领会：①网络安全面临的威胁。

简单应用：①网络安全策略与防护体系；②网络安全的发展趋势。

（二）数字加密技术

识记：①数据加密技术；②加密基本概念。

领会：①古典加密方法；②对称加密方法；③非对称密码算法的原理。

（三）数字签名

识记：①数字签名的概念。

领会：①常用的数字签名体制介绍、认证技术。

综合应用：①数字签名的应用。

（四）网络层安全协议 IPSec

识记：①网络层安全协议综述。

领会：①IPSec 协议；②IPSec 安全体系结构；③IPSec 存在的问题。

综合应用：①利用 IPSec 实现 VPN。

（五）防火墙技术

识记：①防火墙的基础。

领会：①防火墙的实现方法；②防火墙的分类；③防火墙的发展与新技术。

综合应用：①黑客攻击技术。

（六）入侵检测技术

识记：①入侵检测的概念。

领会：①入侵检测技术的发展趋势；②入侵检测的步骤；③入侵检测系统的结构；④几种常见的入侵检测系统。

综合应用：①入侵检测的方法。

（七）入侵防御技术

识记：①入侵防御系统 IPS。

领会：①入侵防御系统的设计思想以及其应该具备的特征。

综合应用：①入侵防御系统的设计；②入侵防御系统的应用部署。

（八）统一威胁管理 UTM

识记：①统一威胁管理 UTM 提出的背景。

领会：①统一威胁管理 UTM 的定义、功能、特征；②UTM 的优势；③UTM 目前存在的问题；④UTM 的适用场合及产品；⑤UTM 的发展趋势。

综合应用：①UTM 的典型技术；②UTM 的一个典型应用解决方案。

三、本章的重点和难点

本章重点：①网络安全基本概念；②网络层安全协议 IPSec；③防火墙技术；④入侵检测技术；⑤入侵防御技术；⑥统一威胁管理 UTM。

本章难点：①数字加密技术；②数字签名。

第 3 章　物联网安全体系结构及物理安全

一、学习目的与要求

理解物联网安全体系结构的概念、特点和应用目标；掌握物联网安全技术措施；正确分析物理安全威胁与防范。

二、考核知识点与考核要求

（一）物联网安全体系结构

识记：①物联网安全整体结构。

领会：①感知层安全体系结构；②传输层安全体系结构；③应用层安全体系结构。

（二）物联网安全技术措施

识记：①物联网安全技术。

领会：①物联网安全管理。

（三）物理安全威胁与防范

识记：①物理安全概述；②环境安全威胁与防范；③设备安全问题与策略。

领会：①RFID 系统及物理层安全；②数据存储介质的安全。

（四）无线局域网 WLAN 物理层安全

识记：①IEEE 802.11 标准中的物理层特点。

领会：①IEEE 802.11 标准中的 MAC 层；②CSMA/CA 协议；③对信道进行预约的 RTS/CTS 协议；④WAPI 协议。

三、本章的重点和难点

本章重点：①物联网安全体系结构；②物联网安全技术措施；

本章难点：①物理安全威胁与防范；②无线局域网 WLAN 物理层安全。

第 4 章　物联网感知层安全

一、学习目的与要求

理解感知层安全的地位和安全威胁；掌握 RFID 安全威胁、安全技术、轻量

级密码算法；正确分析传感器网络安全；正确应用分析物联网终端系统安全。

二、考核知识点与考核要求

（一）感知层安全概述

识记：①感知层的安全地位。

简单应用：①感知层的安全威胁。

（二）RFID 安全

识记：①RFID 安全威胁。

简单应用：①RFID 安全技术；②RFID 安全密码协议；③轻量级密码算法。

（三）传感器网络安全

识记：①无线传感器网络简介。

综合应用：①传感器网络安全威胁分析；②无线传感器网络的安全需求分析；③无线传感器网络的安全攻击与防御；④传感器网络安全防护主要手段；⑤传感器网络典型安全技术；⑥无线传感器网络的密钥管理；⑦无线传感器网络安全协议 SPINS；⑧轻量级公钥密码算法 NTRU。

（四）物联网终端系统安全

识记：①嵌入式系统安全。

简单应用：①智能手机系统安全。

三、本章的重点和难点

本章的重点：①感知层安全；②RFID 安全；③传感器网络安全；④物联网终端系统安全。

本章难点：①传感器网络安全威胁分析；②无线传感器网络的安全需求分析；③无线传感器网络的安全攻击与防御；④传感器网络安全防护主要手段。

第 5 章　物联网网络层安全

一、学习目的与要求

理解网络层安全需求技术特点；掌握近距离无线接入安全——WLAN 安全和远距离无线接入安全——移动通信网安全两种规范；掌握扩展接入网的安全、物联网核心网安全——6LoWPAN 和 RPL 的安全性。

二、考核知识点与考核要求

（一）网络层安全需求

识记：①网络层安全威胁。

简单应用：①网络层安全技术和方法。

（二）近距离无线接入安全——WLAN 安全

识记：①无线局域网 WLAN 的安全威胁。

综合应用：①无线局域网的安全机制。

（三）远距离无线接入安全——移动通信网安全

识记：①无线移动通信安全简介。

综合应用：①2G（GSM）安全机制；②3G 安全机制；③4G 安全机制简介。

（四）扩展接入网的安全

识记：①近距离无线低速接入网安全。

综合应用：①有线网络接入安全；②卫星通信接入安全。

（五）物联网核心网安全——6LoWPAN 和 RPL 的安全性

识记：①核心 IP 骨干网的安全。

综合应用：①6LoWPAN 适配层的安全。

三、本章的重点和难点

本章重点：①网络层安全需求；②近距离无线网接入安全；③远距离无线网接入安全；④扩展接入网的安全；⑤物联网核心网安全。

本章难点：①近距离无线低速接入网安全；②有线网络接入安全；③卫星通信接入安全。

第 6 章　物联网应用层安全

一、学习目的与要求

理解物联网应用层安全需求、Web 安全、中间件安全；理解数据安全、云计算安全关键技术。

二、考核知识点与考核要求

（一）物联网应用层安全需求

识记：①应用层面临的安全问题。

领会：①应用层安全技术需求。

（二）Web 安全

识记：①Web 结构原理。

领会：①Web 安全威胁。

简单应用：①Web 安全防护。

（三）中间件安全

识记：①中间件。

领会：①物联网中间件。

综合应用：①RFID 中间件安全。

（四）数据安全

识记：①数据安全概述。

综合应用：①数据安全保护；②数据库安全；③虚拟化数据安全；④数据容灾。

（五）云计算安全

识记：①云计算概述。

综合应用：①云计算安全问题；②云计算安全需求；③云计算的存储安全；④计算虚拟化安全；⑤云计算安全标准。

（六）物联网信息安全标准

识记：①国际信息技术标准化组织；②国际信息安全标准体系；③中国信息安全标准化现状；④中国安全标准组织机构；⑤电子标签国家工作组；⑥传感器网络标准工作组；⑦泛在网技术工作委员会；⑧中国物联网标准联合工作组。

综合应用：①信息安全标准体系研究特点；②中国在信息安全管理标准方面采取的措施；③信息安全管理体系。

三、本章的重点和难点

本章重点：①物联网应用层安全需求；②Web 安全；③中间件安全；④数据安全；⑤云计算安全。

本章难点：①云计算安全问题；②云计算安全需求；③云计算的存储安全；④计算虚拟化安全。

第 7 章　物联网安全技术应用

一、学习目的与要求

理解物联网系统安全设计，物联网安全技术应用；掌握 EPCglobal 网络安全技术应用。

二、考核知识点与考核要求

（一）物联网系统安全设计

识记：①物联网面向主题的安全模型及应用。

综合应用：①物联网公共安全云计算平台系统。

（二）物联网安全技术应用

识记：①物联网机房远程监控预警系统。

综合应用：①物联网门禁系统。

（三）EPCglobal 网络安全技术应用

识记：①EPCglobal 物联网的网络架构。

综合应用：①EPCglobal 网络安全。

三、本章的重点和难点

本章重点：①物联网公共安全云计算平台；②物联网安全技术应用；③EPCglobal 网络安全技术应用。

本章难点：①物联网面向主题的安全模型及应用；②EPCglobal 物联网的网络架构。

第 8 章 典型物联网安全实例

一、学习目的与要求

理解物联网在医疗系统中的应用、智慧医院的 WLAN 无线查房系统与安全、基于无线体域网 WBAN 的远程医疗安全；掌握 M2M 安全、车联网及其安全简介。

二、考核知识点与考核要求

（一）智慧医院——物联网在医疗系统中的应用

识记：①智慧医院概述。

领会：①智慧医院建设云计算数据中心需求分析；②智慧医院的云计算平台设计；③云平台网络安全设计；④物联网和云计算在医疗领域的应用。

（二）智慧医院的 WLAN 无线查房系统与安全

识记：①无线查房系统介绍。

领会：①无线查房系统的无线网络结构设计；②无线查房系统的 WLAN 安全设计。

（三）基于无线体域网 WBAN 的远程医疗安全

识记：①无线体域网 WBAN。

领会：①无线体域网 WBAN 的特征；②WBAN 安全分析。

（四）M2M 安全

领会：①M2M 概述。

识记：①M2M 安全。

（五）车联网及其安全简介

识记：①车联网的概念及其发展；②车联网系统存在的问题及其关键技术。

综合应用：①车联网的体系结构与应用；②车联网的信息安全问题与安全威胁；③车联网的安全架构设计。

三、本章的重点和难点

本章重点：①智慧医院建设云计算数据中心需求分析；②智慧医院的云计算平台设计；③云平台网络安全设计；④物联网和云计算在医疗领域的应用。

本章难点：①车联网的体系结构与应用；②车联网的信息安全问题与安全威胁；③车联网的安全架构设计。

Ⅳ 关于大纲的说明与考核实施要求

一、自学考试大纲的目的和作用

课程自学考试大纲是根据专业考试计划的要求，结合自学考试的特点而确定。其目的是对个人自学、社会助学和课程考试命题进行指导和规定。

课程自学考试大纲明确了课程学习的内容以及深广度，规定了课程自学考试的范围和标准。因此，它是编写自学考试教材和辅导书的依据，是社会助学组织进行自学辅导的依据，是考生学习教材、掌握课程内容知识范围和程度的依据，也是进行自学考试命题的依据。

二、课程自学考试大纲与教材的关系

课程自学考试大纲是进行学习和考核的依据，教材是学习掌握课程知识的基本内容与范围，教材的内容是大纲所规定的课程知识和内容的扩展与发挥。课程内容在教材中可以体现一定的深度或难度，但在大纲中对考核的要求一定要适当。

大纲与教材所体现的课程内容应基本一致；大纲里面的课程内容和考核知识

点，教材里一般也要有。反过来教材里有的内容，大纲里就不一定体现。

三、关于自学教材

本课程使用教材为：《物联网信息安全》，李永忠编著，西安电子科技大学出版社，2016 年版。

四、关于自学要求和自学方法的指导

本大纲的课程基本要求是依据专业考试计划和专业培养目标而确定的。课程基本要求还明确了课程的基本内容，以及对基本内容掌握的程度。基本要求中的知识点构成了课程内容的主体部分。因此，课程基本内容掌握程度、课程考核知识点是高等教育自学考试考核的主要内容。

为有效地指导个人自学和社会助学，本大纲已指明了课程的重点和难点，在章节的基本要求中一般也指明了章节内容的重点和难点。

根据本课程的学习要求及本课程的特点，本大纲提出如下学习方法：

1. 本课程内容涉及多种物联网信息安全技术，内容丰富，知识范围广泛。考生应当在全面系统学习的基础上，熟练掌握物联网信息安全技术的基本概念、基本原理、各种技术及分析方法。

2. 本课程内容共分 8 章，除第一章外，其他 7 章分别讲解一种物联网信息安全技术，内容相对独立但又有一定的关联，建议考生在自学时把不同的物联网信息安全技术的相关内容进行比较记忆，加强整体上的把握和理解。

3. 物联网信息安全技术是一门理论和实践很强的课程。因此，自学时应注重理论与实践的结合，可以通过一些具体的应用实践操作（比如硬件设计、软件仿真）来加深对教材内容的理解。

五、应考指导

1. 如何学习

很好的计划和组织是你学习成功的法宝。如果你正在接受培训学习，一定要跟紧课程并完成作业。为了在考试中作出满意的回答，你必须对所学课程内容有很好的理解。使用“行动计划表”来监控你的学习进展。你阅读课本时可以做读书笔记。如有需要重点注意的内容，可以用彩笔来标注。如：红色代表重点；绿色代表需要深入研究的领域；黄色代表可以运用在工作之中。可以在空白处记录相关网站，文章。

2. 如何考试

卷面整洁非常重要。书写工整，段落与间距合理，卷面赏心悦目有助于教师评分，教师只能为他能看懂的内容打分。回答所提出的问题。要回答所问的问题，而不是回答你自己乐意回答的问题！避免超过问题的范围。

3. 如何处理紧张情绪

正确处理对失败的惧怕，要正面思考。如果可能，请教已经通过该科目考试的人，问他们一些问题。做深呼吸放松，这有助于使头脑清醒，缓解紧张情绪。考试前合理膳食，保持旺盛精力，保持冷静。

4. 如何克服心理障碍

这是一个普遍问题！如果你在考试中出现这种情况，试试下列方法：使用“线索”纸条。进入考场之前，将记忆“线索”记在纸条上，但你不能将纸条带进考场，因此当你阅读考卷时，一旦有了思路就快速记下。按自己的步调进行答卷。为每个考题或部分分配合理时间，并按此时间安排进行。

六、对社会助学的要求

1. 社会助学者应根据大纲规定的考试内容和考核目标，认真钻研指定教材，明确本课程与其他课程不同的特点和学习要求，合理安排课时，对考生进行切实有效的辅导和引导，把握社会助学的正确方向。

2. 要正确处理基本知识与应用能力的关系，努力引导考生将识记、领会同应用联系起来，引导考生将各章节相关内容结合起来分析和理解。在辅导的基础上，要着重培养和提高考生的素质和技术水平。

3. 要正确处理重点和一般的关系。课程内容有重点与一般之分，但考试内容是全面的，而且重点与一般是相互影响的，不是截然分开的。社会助学者应指导考生全面系统地学习教材，掌握全部考试内容和考核知识点，在此基础上再突出重点。总之，要把重点学习同兼顾一般结合起来，不要孤立地抓重点，把考生引向猜题押题。

七、对考核内容的说明

1. 本课程要求考生学习和掌握的知识点内容都作为考核的内容。课程中各章的内容均由若干知识点组成，在自学考试中成为考核知识点。因此，课程自学考试大纲中所规定的考试内容是以分解为考核知识点的方式给出的。由于各知识点

在课程中的地位、作用以及知识自身的特点不同，自学考试将对各知识点分别按四个能力层次确定其考核要求。

2. 课程考试比例按章节分配，分为 8 部分，分别为概述、网络信息安全技术、物联网安全体系结构及物理安全、物联网感知层安全、物联网网络层安全、物联网应用层安全、物联网安全技术应用、典型物联网安全实例，考试试卷中所占的比例大约分别为：6%、15%、15%、15%、15%、15%、15%、4%。

八、关于考试命题的若干规定

1. 本课程考试方式为闭卷、笔试，考试时间为 150 分钟。评分采用百分制，60 分为及格。考生只准携带 0.5 毫米黑色墨水的签字笔、铅笔、圆规、直尺、三角板、橡皮等必需的文具用品。不可携带计算器。

2. 本大纲各章所规定的基本要求、知识点及知识点下的知识细目，都属于考核的内容。考试命题既要覆盖到章，又要避免面面俱到。要注意突出课程的重点、章节重点，加大重点内容的覆盖度。

3. 命题不应有超出大纲中考核知识点范围的题目，考核目标不得高于大纲中所规定的相应的最高能力层次要求。命题应着重考核考生对基本概念、基本知识和基本理论是否了解或掌握，对基本方法是否会用或熟练。不应出与基本要求不符的偏题或怪题。

4. 本课程在试卷中对不同能力层次要求的分数比例大致为：识记占 20%，领会占 50%，简单应用占 20%，综合应用占 10%。

5. 要合理安排试题的难易程度，试题的难度可分为：易、较易、较难和难四个等级。每份试卷中不同难度试题的分数比例一般为 2:3:3:2。

必须注意试题的难易程度与能力层次有一定的联系，但二者不是等同的概念。在各个能力层次中对于不同的考生都存在着不同的难度。

6. 本课程考试试卷中可能采用的题型有：单项选择题、判断改错题、简答题、论述题等。

附录　题型举例

一、单项选择题

1. 物联网体系结构划分为四层，传输层在（　　）

A. 第一层　　B. 第二层　　C. 第三层　　D. 第四层

参考答案：B

2. 物联网中感知层的关键技术是（　　）

A. RFID 标签　　B. 阅读器　　C. 天线　　D. 加速器

参考答案：A

二、判断改错题

1. 感知层是物联网识别物体采集信息的来源，其主要功能是识别物体采集信息。（　　）

参考答案：√ 。

2. 物联网的感知层主要包括：二维码标签、读写器、RFID 标签、摄像头、GPS 传感器、M2M 终端。（　　）

参考答案： × ，改为：物联网的感知层主要包含各种传感器、RFID、智能终端等。

三、简答题

1. 简述智能电网的安全机制。

参考答案：

通过智能电表、广域测量系统、电网设备的在线监测等技术保障智能电网的设备安全；通过身份认证技术、访问控制技术等保障进入电网的系统认证安全；通过数据加密、数据完整性保护等保障通信安全。

四、论述题

1. 什么是无线体域网 WBAN? 论述安全面临的问题。

参考答案：

（1）无线体域网（WBAN ,Wireless Boay Area Network），是以人体为中心，以采集人体各种生理参数为目的，由分布在人体表面或植入人体内部的传感器及个人数据采集处理终端组成的通信网络。通过 WBAN 人可以和其身上携带的个人电子设备（如 PDA、手机等）进行通信、数据同步等。

WBAN 可以和其它数据通信网络（比如其他人的 WBAN、无线/有线接入网络、移动通信网络等）成为整个通信网络的一部分，和网络上的任何终端（如 PC、手机、电话机、媒体播放设备、数码相机、游戏机等）进行通信。

（2）安全面临的问题：

①节能技术：由于现实状况，很多节点在植入体内后便无法轻易取出，因此对节点的长期持续供能便成为体域网设计时所要考虑的最重要问题之一。低功率低电压，高集成度是节点的设计目标。另外，考虑到节点与个人数据终端的数据传输，一个好的无线电接口及其

优化策略的设计也能很好地促进传感器节点操作上低能耗的性能。

②传感器及终端的安全问题：WBAN 的传感器及终端多分布于人体体内或表面，因此不伤害人体组织是产品研发的先决条件，除了材料本身的安全，通信过程中所产生的各种辐射对人体的影响也要考虑在内。也因此此类产品的生产会受到严格的约束。

③数据的整合：持续而全面的数据采集将产生大量的数据，如何筛选整合有用的数据，剔除冗余信息，将是 WBAN 发展中的一大难题。

④信息的安全：信息安全是各个领域所面临的共同问题。体域网收集并传递大量人体生理数据，一旦这些数据泄露，将带来严重的后果。尤其是在体域网已应用于军事等领域的今天，信息安全的问题便更加凸显了出来。