「情報セキュリティ」（IS/IC)

学科：　　IC　 学籍番号：　　　 Q15017　　　 　名前：　大西克彦

【課題１】　　我が国における情報セキュリティの政策を司る組織である 内閣官房情報セキュリティセンター (NISC : National Information Security Center)について調査し、設置の経緯、位置づけ、活動内容などをまとめよ。

　ITの急速な発展と普及に伴い、2014年11月サイバーセキュリティ基本法が成立した。同法に基づき内閣官房に「内閣サイバーセキュリティセンター（NISC）」が設置された。活動内容は、平成27年9月に閣議決定された「サイバーセキュリティ戦略」に基づき、サイバーセキュリティ政策に関する総合調整を行いつつ、「自由、公正かつ安全なサイバー空間」の創出に向け、官民一体となって様々な活動を行っています。

【課題２】　　バーナム暗号において，同一の鍵 k を用いて， m1 と m2 を暗号化した。各々の暗号文を c1，c2 とする。c1，c2 からどのような情報が漏れるか 考察せよ。

ｃ１、ｃ２から同一の鍵ｋがもれる可能性がある。

【課題３】　　公開鍵インフラストラクチャPKIがなく、公開鍵が偽物であった時の影響を、（１）ディジタル署名への影響、（２）暗号化への影響　の２点から論じよ。

（１）　署名者B、Bになりすまそうとする不正行為者Z、Zが騙そうとする相手をAとする。

Zからの偽のメッセージが送られた時にディジタル署名を利用して署名検証しても偽物とわからずにAに届いてしまうため、ディジタル署名が意味をなさなくなる。

（２）　平文の送信者A、受信者B、不正行為者Z　とする。

AはZの公開鍵で暗号化してしまい、Bは複合化できずにZに平文を解読されるため、暗号化の意味がなくなる。

【課題４】　　公開鍵暗号を用いたディジタル署名（以下、署名）の利用手順を説明せよ。ただし、署名者をB、署名の受領者をAとする。また、Aは最初に認証局を信頼するものとする。説明においては、指定された用語を一度は使用すること。

準備フェーズ（指定用語：発行局、登録局、Bの公開鍵証明書、認証局の公開鍵証明書）

登録局からの依頼を受けた発行局がBの公開鍵証明書を作成し、発行する。Aは認証局の公開鍵でBの署名を検証して正しいかどうかを確認する。

署名フェーズ（指定用語：署名、検証、ハッシュ関数、Bの公開鍵証明書、Bの秘密鍵、OCSP）

ハッシュ関数を使いハッシュ値を算出し、それをBの秘密鍵を使って署名する。署名はBの公開鍵証明書を使えば検証できる。OCSPでBの公開鍵証明書の状態を確認することもできる。

【課題５】　　授業に関し、感想を述べよ。