情報セキュリティマネジメントコース

サイバー攻撃への危機意識の共有と連携体制の検討

「情報セキュリティ201X」
Ⅱ 情報セキュリティを取り巻く環境の変化～より

情報セキュリティ2011

- **①大規模なサイバー攻撃事案等の脅威の増大**
- ②社会経済活動の情報通信技術への依存度の増大
- ③新たな技術革新への対応
- ④グローバル化等
- ⑤東日本大震災の発生

情報セキュリティ2012

- **①本格的なサイバー攻撃の発生と深刻化**
- ②社会経済活動の情報通信技術への依存度の更なる高まりと**リスクの表面化**
- ③新たな技術革新に伴う**新たなリスクの出現**
- ④重要な情報システム障害の**リスク回避に向けた取組**の必要性の高まり
- ⑤諸外国における取組の強化

(参考) http://www.nisc.go.jp/active/kihon/pdf/js2011.pdf
http://www.nisc.go.jp/active/kihon/pdf/is2012.pdf

情報セキュリティ政策会議

「サイバーセキュリティ戦略」より①

はじめに

- 情報セキュリティを取り巻く環境変化は，極めて急速である．全戦略策定後の3年間で，リスクは甚大化し，拡散し，グローバルレベルのものとなった．**国家や重要インフラに対する「サイバー攻撃」が現実のものとなり，「国家安全保障」や「危機管理」上の課題となっている．**今や，国家や重要インフラの防護に最善の措置の導入が不可欠となっている．
- 国民生活のあらゆる側面において，情報セキュリティ対策が不可欠の時代となった．**情報セキュリティは「国民生活の安定」や「経済発展」に直結する課題となっている．**
- 従来の「情報セキュリティ」確保のための取組はもとより，広くサイバー空間に係る取組を推進する必要性と取組姿勢を明確化するため，本戦略の名称は「サイバーセキュリティ戦略」とした．

1．環境の変化

- (1)サイバー空間の拡大・浸透
  - ①サイバー空間と実空間の「融合・一体化」の進展
  - ②サイバー空間を取り巻く「リスクの深刻化」
    【甚大化するリスク】【拡散するリスク】【グローバルリスク】

(参考) http://www.nisc.go.jp/active/kihon/pdf/cyber-security-senryaku-set.pdf

情報セキュリティ政策会議

「サイバーセキュリティ戦略」より②

2．基本的な方針
(3)各主体の役割
③企業や教育・研究機関の役割

- 企業や教育・研究機関は，技術情報，財務情報，製造技術や図面等の知的財産関連情報，顧客名簿，人事情報や学習指導情報等の個人情報などを保有している．
- 我が国産業の国際的な競争力の源としても重要な情報が，サイバー攻撃等により窃取や破壊等された場合，我が国の社会経済発展を阻害する可能性がある．
- 企業や教育・研究機関においては，個々における情報セキュリティ対策に加え，業務の委託先や提携先とも連携しつつ，**サイバー攻撃に関する情報共有など業界団体等による集団的な対策に取り組むことが期待される．**
- 各々の主体において情報セキュリティ対策に取り組む際には，**第三者専門機関から，評価，監査を受けて，マネジメント標準を取得する等により，対策を向上していくことが期待される．**
- 技術開発と人材育成の中核になる主体として・・・世界を率先する強靭で活力のあるサイバー空間を構成する高度な技術や人材等を供給することが期待される．

(参考) http://www.nisc.go.jp/active/kihon/pdf/cyber-security-senryaku-set.pdf

【実習】

前半・グループワーク

- インシデントの発生を想定した
  対応シミュレーション

後半・グループディスカッション

- インシデント対応に関する
  情報の共有・連携についての検討

【グループワーク】
インシデント対応のシミュレーション

- 「詐欺を狙った標的型攻撃メールの受信」

- ｸﾞﾙｰﾌﾟが危機管理対策本部・委員会と想定
- 届いた緊急連絡票を元に
  適切な部署・人へ適切な指示を与える
  - ⇒内容をインシデント対応指示書に記入

インシデント対応の検討事項

- 必要とされる連絡窓口・管理体制
- 判断に必要な情報
- 関係部署への伝達事項・対応指示
- 重要な判断

【グループディスカッション】 インシデント情報の共有・連携についての検討

- インシデント対応の検討(及び経験)を元にして必要性の検討
  - 教職員の危機管理意識の醸成
  - 情報セキュリティ対策の強化・リスクの管理
  - サイバー攻撃の動向
- 理由，課題・問題点を検討
  - 運用可能な体制・仕組み・取扱情報とは？

インシデント情報の共有・連携検討マトリクス

必要性	あり	なし
理由		
課題・問題点		

～ｲﾝｼﾃﾞﾝﾄ事例と対処方法について情報を一元化する仕組みの必要性～

(私情協の調査結果より)

- 情報を一元化する仕組みが必要か？
  - アンケートでは約9割が必要と回答
- 但し，約7割が「仕組みの内容次第」と回答
  - どのような仕組みが相応しいのか？
    - 体制・・・IPA? 私情協? または適切な組織とは?
    - 仕組み・・・守秘義務，情報の送受信・公開のルールは?
    - 取扱情報・・・多過ぎず少な過ぎず，ﾏｽｸをかけるのはどこ?
- 仕組みがないこと(現状)の課題・問題点は？