「情報化された組織のセキュリティマネジメントWG」活動報告

只木　進一

佐賀大学総合情報基盤センター

背景と経緯

- 大学・研究所などの業務のICT化
  - 教育、研究、診療、組織業務
  - オンライン化
  - 発生源入力
  - データ連携
- セキュリティ（機密性、可用性、完全性）の向上が必要
  - 機密情報の保持
  - 安定した運用
  - 正確な情報の流通
- 利便性とセキュリティ維持
  - 整合性

業務のICT化の一方で

- 情報漏えい事案の増加
  - 安易なデータ持ち出し
  - 利便性とセキュリティ意識のミスマッチ
  - 教育機関での仕事の在り方
- DNSへの攻撃とフィッシング等の事案
  - 大学・研究所を踏み台にする攻撃
  - DNS情報を汚染する

事業継続計画への関心

- 業務のICT化
- 業務の継続には情報基盤が不可欠
- 情報部門だけでも事業継続計画が必要？
- 業務の整理にも活用できる？

- 東日本大震災の発生
  - 情報基盤の被害状況
  - 対策の指針

WGの構成と日程

- WGの活動期間
  - 2009年10月から2012年3月
- メンバー
  - A班：BCP、情報漏えい

  只木 進一 [班長]、湯浅 富久子、 西村 浩二、 山守 一徳、山下 眞一郎、山路 光昭、櫻井 秀志、須永 知之
  - B班：DNS

  鈴木 聡 [班長]、吉田 和幸、 笠原 義晃、 武藏 泰雄、 長谷川 明生、吉田 真和、 飯島 敏治、 南場 進、 田口 雅晴

事業継続計画
BUSINESS CONTINUITY PLAN

- 災害や事故が起こってしまったとき
  - 事業継続するための計画
  - 事業の選択とその事業に必要な資源
- なぜ、大学・研究機関に先行して、情報基盤部門のBCPが必要？
  - 情報基盤は大学・研究機関の基盤
  - 大学は、避難場所になる
  - 大学は、復興の核

BCP構築へ向けて

- システム・サービスの現状把握
  - システム構成、管理者、保守業者、代替機の可能性
- 情報システム以外の設備の現状把握
  - ラック、電源、防火、施錠
- 重要情報のバックアップ
  - バックアップ情報、バックアップ先
  - 本当にリストアできるか？
- 緊急連絡網整備
  - 多様な媒体：電話、携帯、メール
  - 出勤経路
- 初期行動計画

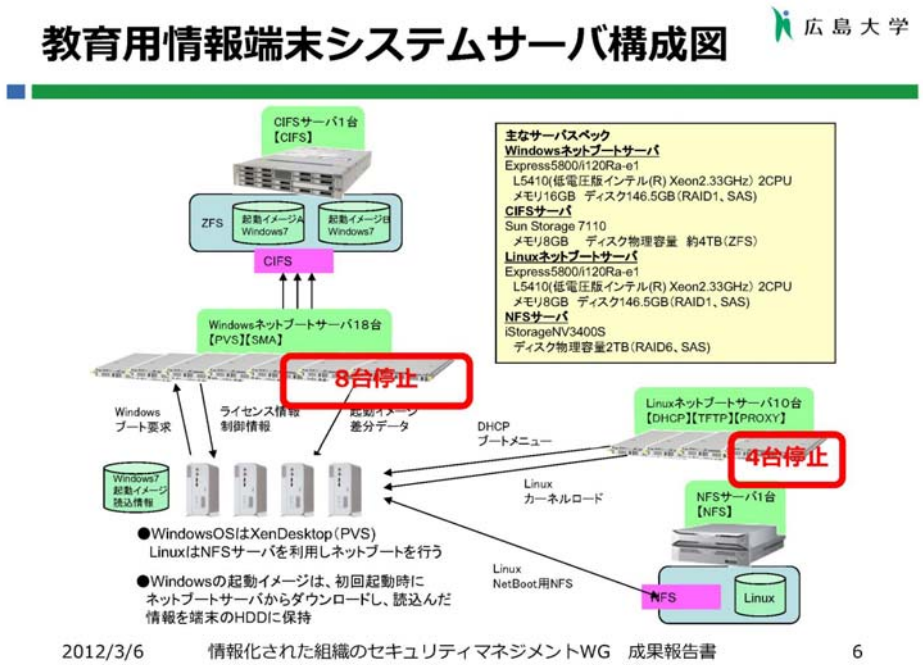
例：システム・サービスの現状把握

対象情報システム			設置場所	ハードウェア			代替機	再インストール可能性	バックアップ状況				管理者		復旧手段	備考	他システムへの依存	
名称	サービス内容	主管部門	建物	機種名	ラック等	保守業者			分類	バックアップ	媒体	場所	主	副				
ネットワーク基盤	コアスイッチ	情報基盤センター	情報基盤センター本館	Cisco Catalyst 6509	ラック1	○○ネットワークシステムズ	なし	対象外	設定内容	あり	CD	情報基盤センター本館	鍋島次郎	三日月二郎				
ネットワーク基盤	DNSサーバ	情報基盤センター	情報基盤センター本館	Sun Fire X2100	ラック1	××システム	なし	可	OS及びアプリ	あり	CD	情報基盤センター本館	三日月二郎	鍋島次郎			コアスイッチ	
								可	設定内容・データ	あり	CD	情報基盤センター本館						
認証基盤	ユーザデータベース	情報基盤センター	情報基盤センター本館	Sun Fire X2100	ラック1	△△コンピューティング	なし	可	OS及びアプリ	あり	CD	情報基盤センター本館	三日月二郎	鍋島次郎			DNSサーバ	
								可	設定内容・データ	なし								
認証基盤	LDAP主サーバ	情報基盤センター	情報基盤センター本館	Sun Fire X2100	ラック1	△△コンピューティング	あり	可	OS及びアプリ	あり	CD	情報基盤センター本館	佐賀太郎	鍋島次郎	内部に準備済み		ユーザデータベース	
								可	設定内容・データ	あり	CD	情報基盤センター本館						
電子メール	IMAPサーバ	情報基盤センター	情報基盤センター本館	Sun Fire X2100	ラック1	△△コンピューティング	あり	可	OS及びアプリ	あり	CD	情報基盤センター本館	鍋島次郎	嘉瀬一子		旧機材あり	LDAP主サーバ	
								可	設定内容	あり	CD	情報基盤センター本館						
								対象外	データ	なし								
									OS及び		C	情報基盤セ						LDA

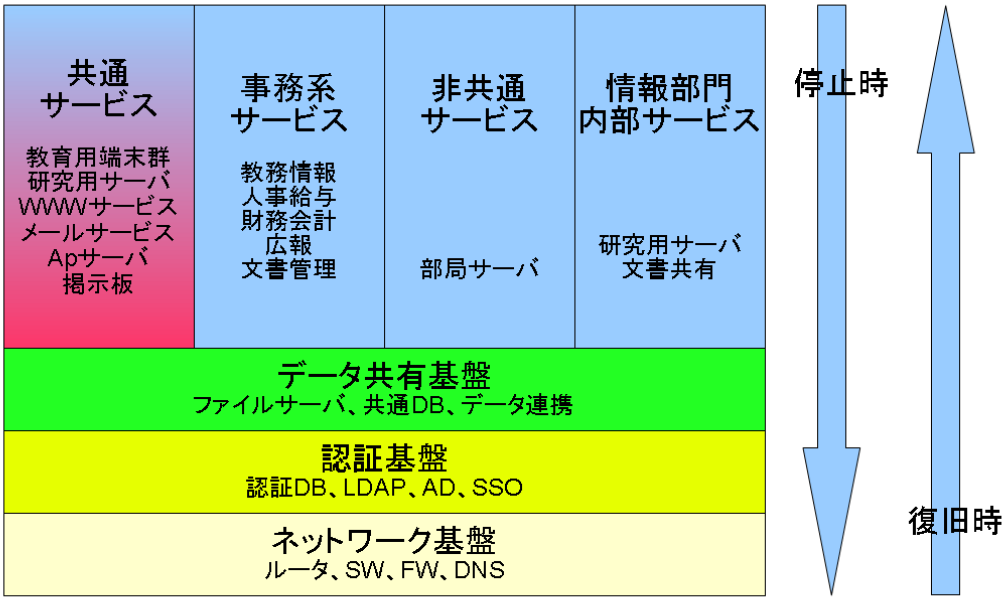
BCPとシステム把握・日常運用

- システム状況把握
  - 資源の配置状況、課題の発見
  - システム依存関係の把握
  - 属人的サービスの把握と改善
- 電源管理
  - 電源状況の把握
  - 縮退運転への応用
- 起動・停止手順の明確化

例：縮退運転



例:システムの起動・停止手順の整理



東日本大震災時の情報系センター

- 26のセンター等に回答頂きました。
- 情報システムの被害は意外と少ない
  - ラックマウントされていたシステムは大丈夫
  - 電源復帰後に短時間でサービス再開
- 都内の計画停電のほうが被害甚大
  - 要員の疲弊
  - データ破壊
- 緊急連絡網の不備
  - 複数の媒体が必要
  - 適宜更新

震災後に課題として挙げられている事柄

- 停止・再稼働・復旧のマニュアル化
  - 属人性の低減
  - 関係書類の紙化
- 電力
  - 可視化
  - 緊急用電源

情報漏えい対策

- 大学・研究機関の持つ機密情報
- 大学・研究機関の特殊性
- 持ち出させないための対策
- 誤って持ち出させないための対策
- 条件を定めて持ち出させるための方法

大学・研究機関の持つ機密情報

- 大学・研究機関はけっこう機密情報をもっている
- 学生情報
  - 学生の氏名、連絡先、出身地、帰省先
  - 要注意学生：成績、行動、家庭
- 附属学校の児童・生徒の情報
- 附属病院の患者情報
  - 電子カルテシステム
  - 診療データ、X線写真
- 人事応募情報
- 研究情報
  - 企業との共同研究
  - 特許

大学・研究機関の特殊性

- 機密情報に関わる人間が多い
  - 教員・教諭が様々な形の学生情報を保有
- 「自宅で仕事」が常態化
  - 持ち出す機器に機密情報が入り込む
    - ノートPC、USBメモリ
- 一元管理が困難
  - 「組織業務」の意識が希薄
  - 事務と教育・研究の分離が中途半端

持ち出させないための対策

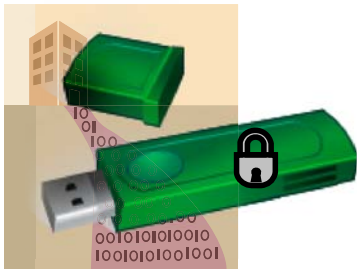
- 情報を持ち出す必要を無くす
  - シンクライアント
  - 共有ファイルサーバ
  - 外部媒体利用の抑止
  - VDI
- 印刷の抑止
- 情報へのアクセスの管理
  - 認証基盤
  - ロール管理
- 情報アクセス状況の把握
  - 証跡管理
  - 通信内容監査

誤って持ち出させないための対策

- PC等の廃棄手順
  - 確実なデータ消去
- 印刷物の放置抑制
  - 認証付プリンタ
- メール誤送信の抑止
  - 送信先等の再確認システム

条件を定めて持ち出させるための方法

- 持ち出し用USB
  - だれがどのUSBを持っているかの管理
  - PW・指紋等でのアクセス制限
  - ウィルス対策内臓USB
- 持ち出しPCの管理
  - データ暗号化



課題

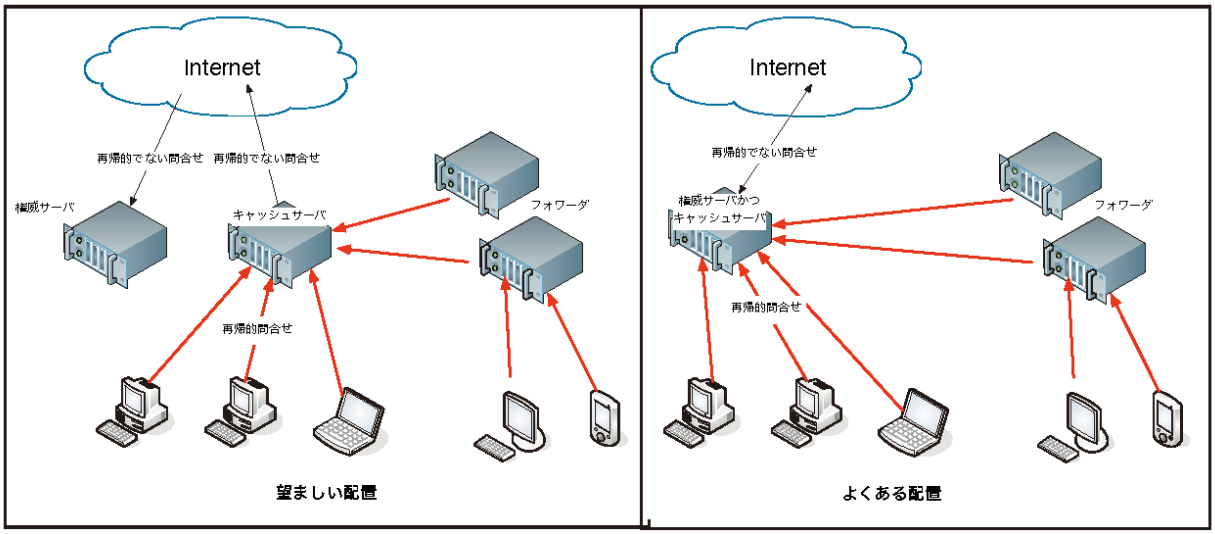
- 大学・研究所では徹底が難しい
  - 組織の管理する機密情報を個人が持たないための工夫
  - 業務オンライン化の徹底
  - シンクライアントの普及
  - 在宅勤務への積極的対応
- スマートフォーン等への対応
  - 個人所有の情報デバイスへ情報が拡散
- 個人向けクラウドサービスへの対応
  - リスクの周知
  - 利用ルールの策定

セキュリティ向上のためのDNS設定

- DNSを介した攻撃手法の拡がり
- 脆弱性を利用した乗っ取り
- キャッシュポイズニング
  - DNSキャッシュデータに嘘データを混入
  - フィッシングサイト等への誘導
- DNS Amplifier DoS
  - 脆弱なDNSサーバを乗っ取る
  - 大きなデータを、他のキャッシュサーバに記憶させる
  - 攻撃対象のホストからの参照を偽装し、DNSからの戻りのデータで攻撃する

対策の基本：サーバー配置

- 権威サーバとキャッシュサーバの切り離し
- 権威サーバ
  - 外部からの問い合わせに必要
  - 再帰問い合わせを許可しない
    - 他サーバへの問い合わせ時に毒を盛られる危険性がある
- 内部からの問い合わせ
  - キャッシュを持つサーバへ
  - 組織外へ問い合わせ

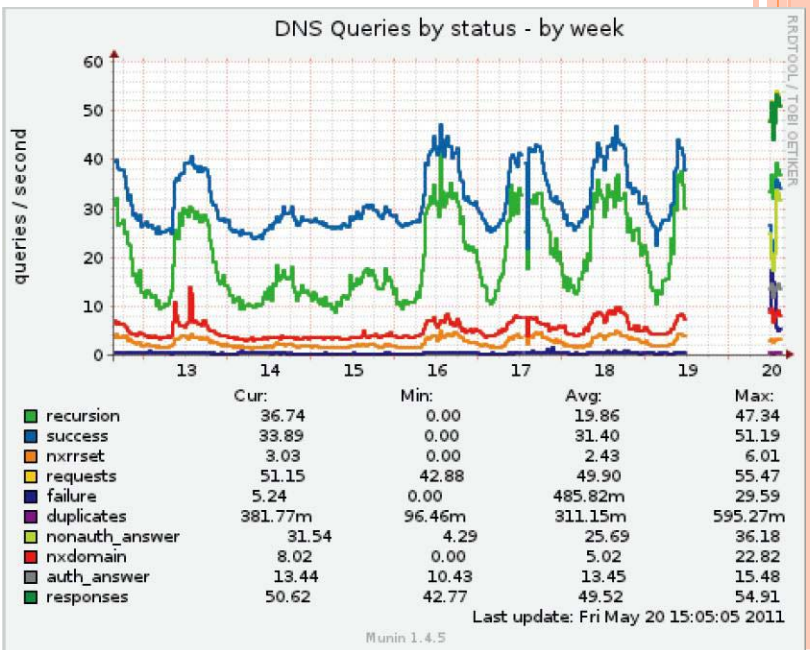


対策の基本:ACL

- 問い合わせの許可
  - ネットワーク
  - サーバのNIC
- 再帰の許可
  - 許可するネットワーク
- キャッシュへの問い合わせ許可

状況を知るための道具

- ログの取得
  - DNSにログ取得設定をする
- 統計情報
  - Muninの活用



まとめ

- 事業継続計画
  - 情報システム・サービスの把握
  - 基盤（電源、要員、保守業者等）の把握
  - 体制の整備
- 情報漏えい対策
  - 技術的対応：シンクライアント、セキュアUSBなど
  - 制度的対応：徹底が難しい
  - 新規技術・サービスへの対応
- DNS設定
  - 攻撃の足場になる
  - サーバ構成の確認
  - ログの確認