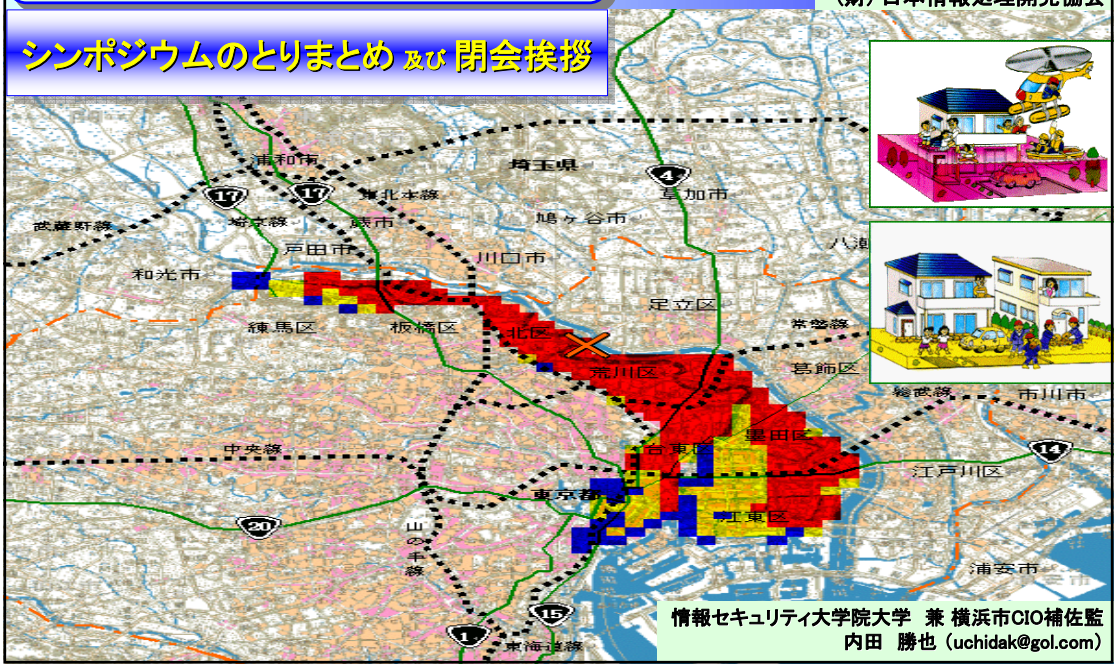
事業継続マネジメントの新たなる出発

～情報セキュリティ総合的普及啓発シンポジウム～

シンポジウムのとりまとめ 及び 閉会挨拶

2009年01月29日
（財）日本情報処理開発協会



情報セキュリティ大学院大学　兼 横浜市CIO補佐監
内田　勝也（uchidak@gol.com）

シンポジウムのとりまとめ及び閉会挨拶

- インシデント
  多様なインシデントを考慮する必要がある
  - 内部でのインシデント
  - 外部からのインシデント
    - 直接的：DDoS攻撃、コンピュータウイルス
    - 間接的：首都圏大停電、ビル内での死者

リスクを
考えるためには必須

事業継続マネジメントの新たなる出発
～ 情報セキュリティ総合啓発普及シンポジウム～

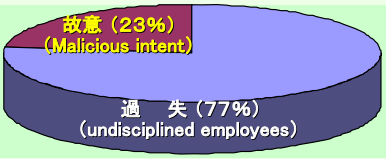
都市伝説（？） その2

情報漏えいの原因

（1）InfoWatchの調査

- 2006年に世界各国で起きた情報流出事件のうち、1回でもメディアで取り上げられたケース145件の調査
- 流出原因は過失によるものが77%と圧倒的に多く、業種や地域による偏りは見られず、大企業や中小企業、政府機関、軍などでも流出が起きた

http://www.itmedia.co.jp/news/articles/0702/17/news011.html

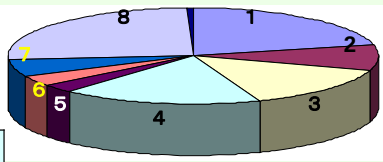


InfoWatchの調査
http://www.infowatch.com/threats?chapter=162971949&id=207784626

（2）内閣府国民生活局　個人情報の保護に関する事業者の取組実態調査 より

- 調査は平成19年3月実施、回答数4,060件（回収率 20.3%）

http://www5.cao.go.jp/seikatsu/shingikai/kojin/20th/20070425kojin2.pdf



内閣府国民生活局の調査

内閣府国民生活局の調査　漏えい発生原因	回答割合 %		
1. 従業者の置忘れ、施錠忘れ等の過失	21.3		1～3 合計 65 %
2. 従業者のインターネット利用上の過失（メール誤送信、HPへの誤掲載等）	8.6		
3. 従業者（含 退職者）が盗難にあった（含 車上荒し等）	14.2	(44.1)	
4. 委託先・運送業者の漏えい等	17.6	61.7	4～6 合計 35 %
5. サーバ／PCへの攻撃（ハッキング・ウイルス感染等）	2.8		
6. 従業者の個人情報持出し、売却・譲渡・漏えい等	3.6	6.4	
7. 原因は未だに不明である	5.4	5.4	
8. その他	25.8	25.8	
9. 無回答	0.7	0.7	

事業継続マネジメントの新たなる出発
～ 情報セキュリティ総合啓発普及シンポジウム～

シンポジウムのとりまとめ及び閉会挨拶

首都圏大停電

2006年8月14日午前7時38分頃、首都圏（東京、千葉、神奈川）で大停電が発生。約140万戸が停電し、JR、私鉄、地下鉄等の交通機関、信号機、エレベータ等が止まった。
停電の原因は、東京都江戸川区南葛西7丁目の旧江戸川の中央部分で、航行中のクレーン船（全長36メートル、幅12メートル、380トン）が、水面から約16メートルの高さの送電線と接触したため。
送電線は2系統あり、一方が損傷しても、もう一方が予備の役割を果たすが、クレーンは送電線を2系統とも損傷させたという。この送電線は、発電所から送電する50万ボルトに次ぐ2番目に大きな送電線。この送電線につながる各変電所では、損傷によって過電流保護装置が働いて電流が遮断されたため、次々に停電が起きた。

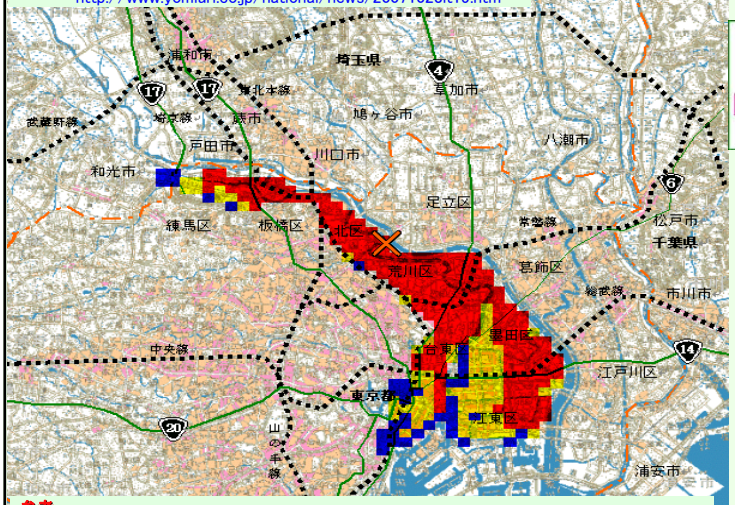
- 東京株式市場の日経平均株価（225種）が午後1時半ごろから算出不能に
- コンビニ店内のATM（セブン銀行）が、最大2時間半、送金・入金不能に
- インターネットデータセンターのビットアイルでシステム停止（JTBの旅行予約サービスが午前8時過ぎから午後2時まで停止）
- 大田花きでは、競りが2時間停止。電源の2重化が機能せず、シャットダウン中にUPSのバッテリーが切れて異常終了

Institute of Information Security　Katsuya Uchida, Professor Ph.D.　uchidak@gol.com

事業継続マネジメントの新たなる出発
～ 情報セキュリティ総合啓発普及シンポジウム～

自 然 災 害

2007年10月、中央防災会議が荒川の洪水はん濫時の浸水想定を発表
大規模水害対策に関する専門調査会-内閣府防災情報の頁
http://www.bousai.go.jp/jishin/chubou/suigai/index.html
荒川決壊160万人被害、銀座浸水2m…中央防災会議想定
http://www.yomiuri.co.jp/national/news/20071023it15.htm



参考
- シカゴ川の改修工事中の作業ミスと市の判断ミスで、シカゴのビジネス街（ダウンタウン）地下が浸水。ビジネス機能が1週間以上麻痺（1992年4月）
- 中央防災会議：荒川堤防決壊時 地下鉄等の浸水想定（2009年1月）

1993年に当時の建設省が荒川下流地域で200年に1回程度発生すると考えられる降雨量：「3日間に548mm」があった場合、荒川下流域で破堤が発生すると想定した中の最悪のものが、荒川右岸16．75Kmが破堤した時で、左図はその時の浸水区域を示したもの

もし2m以上浸水したら‥
まず家屋の1階がすべて水につかってしまい、家財道具などに重大な被害が出ます。また、2階も水につかり、国民の社会・経済活動が壊滅的なダメージを受けます。

もし50cm以上浸水したら‥
家屋が床上浸水します。また、自動車の走行が不可能となるばかりか歩くことも困難になり、市民生活に重大な影響がでます。

浸水深
赤：2．0メートル以上
黄：0．5 ～ 2．0メートル未満
青：0．5メートル以下

全被害状況	
浸水面積	82．8 Km²
浸水区域内人口	1，163，031 人
床下浸水戸数	18，085 戸
床上浸水戸数	456，052 戸
被害額	384，947 億円

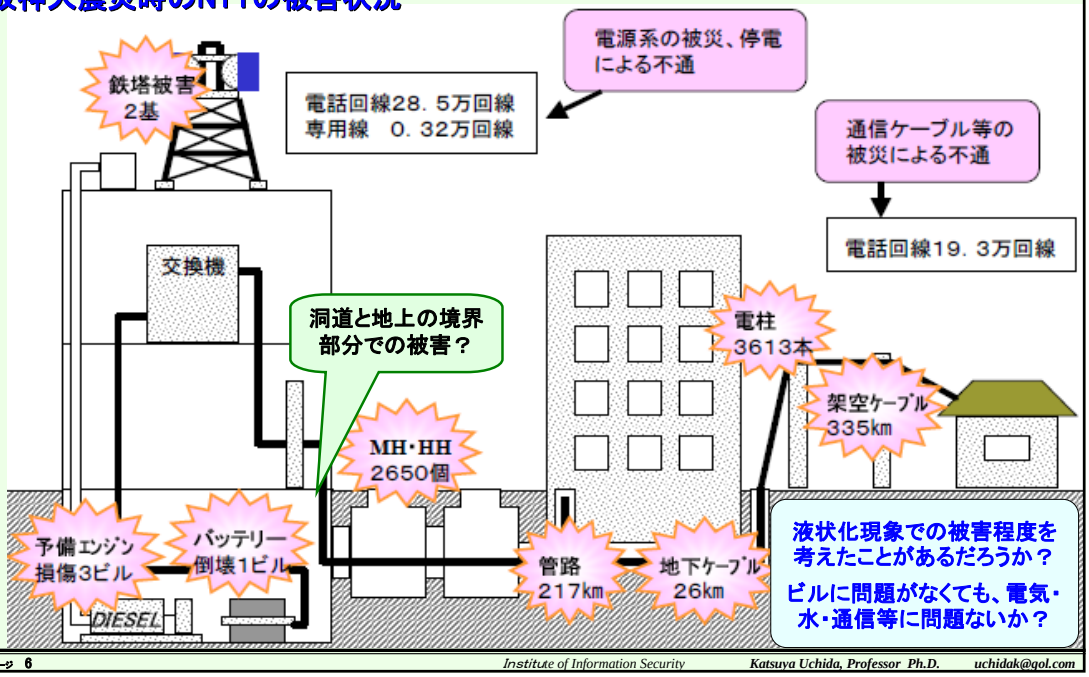
阪神大震災の被害金額10兆円の約4倍に相当

Institute of Information Security　Katsuya Uchida, Professor Ph.D.　uchidak@gol.com

事業継続マネジメントの新たなる出発
～ 情報セキュリティ総合啓発普及シンポジウム～

自 然 災 害

阪神大震災時のNTTの被害状況



Institute of Information Security　Katsuya Uchida, Professor Ph.D.　uchidak@gol.com

事業継続マネジメントの新たなる出発
～ 情報セキュリティ総合啓発普及シンポジウム～

業務継続計画

米国 9月11日の同時多発テロからの教訓

- 今回の同時テロではオフィスビルが崩壊し、テナント企業では、そこに勤務していた多くの従業員が被害を受け、更に、米国では重要な交通手段である航空機の運行が数日間止まり、再開後も大きな混乱が続きました。
  - ① 緊急時対応計画の必要性：緊急時対応計画の策定を行い、最低でも年1回程度の訓練を行う必要がある。コンピュータの利用が日常的になっており、大きな災害・事故等で通常の処理が不可能になった場合に、どの様な対応を行うかを事前に計画・立案し、実際に訓練を行うことにより、対応計画が想定通りに行うことが可能か確認し、問題があれば、対応計画を見直す必要がある。緊急時対応計画も従来のホストコンピュータだけでなく、イントラネットを含めた緊急時対応計画の必要性が明らかになった。
  - ② 人の重要性の認識：緊急時対応を行う場合、それに携わる人間が重要であり、担当要員を複数設けて、人的な面からのバックアップの必要性が明らかになりました。今回の同時多発テロでは緊急時の対応要員が全て同一場所にいたため、それらの要員すべてが犠牲者になってしまったケースもあり、同一業務に関して、複数の要員が必要であると同時に、それらの要員が別の場所に勤務していることが望まれました。
  - ③ イントラネットへの配慮：イントラネットで扱うデータが次第に重要になってきましたが、それらのデータ管理システムが確立されていませんでした。例えば、データのバックアップを行っていても、そのデータの保管は同一ビル内に保管してあったため、バックアップデータも同時に消滅してしまいました。実際、ある日本企業が委託していた法律事務所では作成した契約書が紛失したため、急遽、顧客である日本企業に連絡して、日本から契約書データを送ってもらったといった事も発生しています。

9.11では、PTSD（心的外傷後ストレス障害）が、BCM担当者に発生した。
勿論、重傷・死亡された方々もいたが・・・

Institute of Information Security　Katsuya Uchida, Professor Ph.D.　uchidak@gol.com

事業継続マネジメントの新たなる出発
～ 情報セキュリティ総合啓発普及シンポジウム～

シンポジウムのとりまとめ および 閉会挨拶

- インシデント
  多様なインシデントを考慮する必要がある
  - 内部でのインシデント
  - 外部からのインシデント
    - 直接的：DDoS攻撃、コンピュータウイルス
    - 間接的：首都圏大停電、ビル内での死者

リスクを
考えるためには必須

- 人の問題
  - マネジメント体制の構築：セキュリティ文化
    - 事象発生時の連絡＆連絡先
    - 事前想定と想定外対応
    - 担当が不測の事態になる可能性
  - 想定外をなくす努力も必要では？　⇒ 広く関心を持つことが大切
- マネジメントシステム
  - 小さく産んで、大きく育てる（？）
  - BCM構築のための基準（クライテリア）として考えては？
  - SCM（サプライチェーン）を考えた構築も
  - BCMSでは、（机上）演習も大切
- 認証制度の課題
  - ３月３日（火）13:30～ JISR（ISMS審査機関協議会）セミナー　神谷町パストラル

事業継続マネジメントの新たなる出発
～ 情報セキュリティ総合啓発普及シンポジウム～

ありがとうございました

ご質問・コメントがございましたら ・・・・

電子メールでのご質問・コメントはいつでもどうぞ

情報セキュリティ大学院大学
（http://www.iisec.ac.jp/）

教授　内田　勝也

uchidak@gol.com
http://www2.gol.com/users/uchidak/

内田研究室：　http://lab.iisec.ac.jp/~uchida_lab/