IT戦略の中に情報セキュリティ対策を位置付けることの重要性

yosihiro.com

佐藤　慶浩

twitter.com/4416sato

Copyright 1995-2012 佐藤慶浩

発表者紹介

よしひろ.com

佐藤　慶浩（さとう　よしひろ）
日本ヒューレット・パッカード　個人情報保護対策室　室長

社外の活動
- 元　内閣官房 情報セキュリティ指導専門官
- 厚生労働省　社会保障分野サブワーキンググループ　構成員
- デジタル・フォレンジック研究会　理事
- 情報ネットワーク法学会　副理事長
- JIPDEC　ISMS適合性評価制度技術専門部会　委員
- JIPDEC　プライバシーマーク推進センター　客員研究員
- 杉並区　住基ネット運用監視委員会　委員
- など

Copyright 1995-2012 佐藤慶浩

本研究会で佐藤から行なった発表経緯

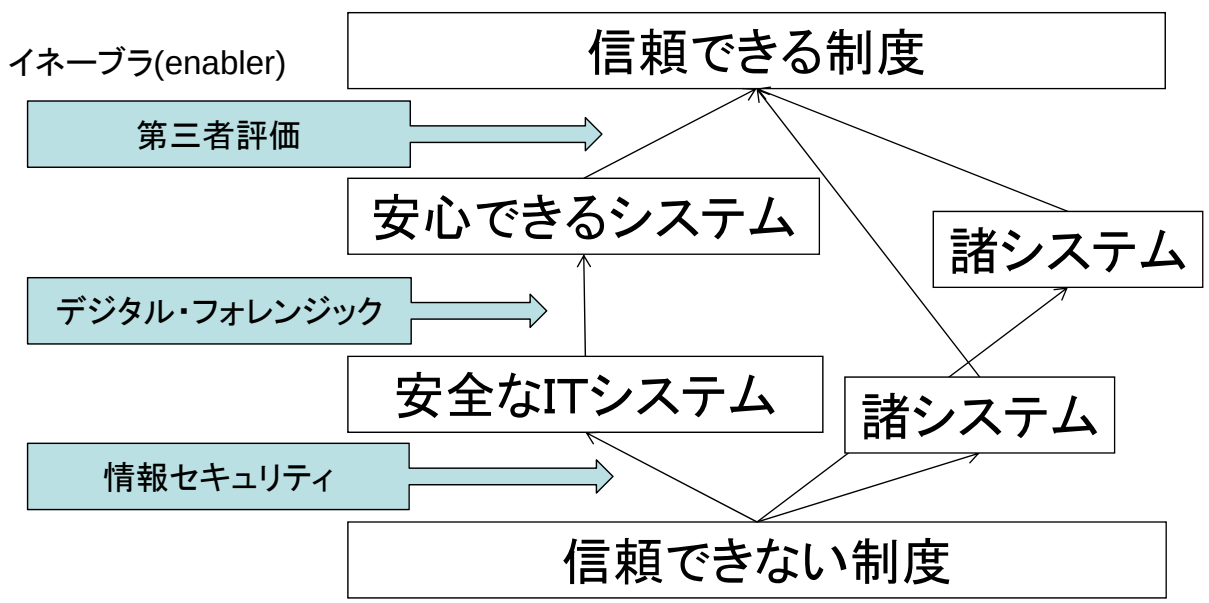
2008年11月23日
　アイデンティティ復元機能付き匿名処理
2009年7月30日
　デジタル・フォレンジックの位置づけと課題
2010年3月17日
　つぎはぎシステムを防ぐセキュリティアーキテクチャ
　証跡とログの違い
2010年11月20日
　説明可能な情報管理の考え方とその技法について
2011年11月22日
　今さら聞けない？セキュリティ関連用語の解説
2012年1月31日
　情報セキュリティとデジタル・フォレンジックの関係

左記の過去の発表の資料や録音については、最後のスライドに掲載したウェブページからダウンロードできます。

Copyright 1995-2012 佐藤慶浩

前回のまとめ

情報セキュリティとデジタル・フォレンジックの関係



Copyright 1995-2012 佐藤慶浩

目次

制度設計をするときの注意事項

情報セキュリティ産業の課題

IT戦略の中に情報セキュリティ対策を位置付ける事例
　事例説明のポイント
　モバイルIT環境の事例紹介
　事例説明のまとめ

Copyright 1995-2012 佐藤慶浩

制度設計をするときの注意事項

●FISMA妄信はアメリカ・コンプレックス
→米国でFISMAが徹底しているとは言い難い
→現場が対策するときの根拠にできる効果は高い
→FISMAの強制力で実施しているという見方は要注意
●DoDのAPT(ADVANCED PERSISTENT THREATS)
→内容は重要であるが、このような戦略を作成できるCISOがいることの方が重要（よい時計があることより、時計を作れるよい職人がいることが重要という喩え）
→参考資料参照
●DoDのRACE(Rapid Access Computing Environment)
→サプライチェインのIT化に投資していることが重要
→そのためにパブリックに提供するプライベート・クラウドを実現するセキュリティ要件を定めて運用している

Copyright 1995-2012 佐藤慶浩

制度設計をするときの注意事項（つづき）よしひろ.com

●セキュリティ人材の育成という幻想
→米国の見習うべきは、「育成しようとしていない」こと。
→成長する適材(4%)を確保するという「割り切り」
→このモデルも参考に、本来はNISCは構想された。
→「人は育てるものではなく、育つもの」ということが基本
●サイバーセキュリティ産業の創出は逆効果
→BITA(Business IT Alignment)の推進とIT産業の活性化が先決
→セキュリティを別建てにすることが、人材の成長を妨げ、
人材層の閉塞を生んでいる
→IT人材の各層にセキュリティ各層の役割を担わせることが
結果的に、セキュリティ人材の増強に寄与する

制度設計をするときの注意事項（つづき）よしひろ.com

まとめ

1. セキュリティシステムやセキュリティ人材、産業の創出は避けるべきであり、IT戦略の策定とそれの構築に必要となるセキュリティ対策の導出が必要

2. 情報セキュリティ技術立国ではなく、組織の運営目的を達成するためのイネーブラーとしてのIT全般利活用の促進と、それを設計するIT戦略策定能力の醸成が必要

3. 具体的なIT戦略の確固たる作成が喫緊の課題である
情報セキュリティ対策はその中で消化されるべき課題

制度設計をするときの注意事項（つづき）

まとめ（つづき）

4. 産業は自立するべきであり、国家予算で擁護すべきものではない
   過保護に育てられた産業は国際競争力を持ち得ない
   （大航海プロジェクトからの教訓→後悔すべき方策）

5. 大学には講座を設けてもらい、政府職員のスキル向上に
   講座履修義務を設けるべき（米国のCIOユニバーシティ）
   大学の講座も競争の中で充実させるべき

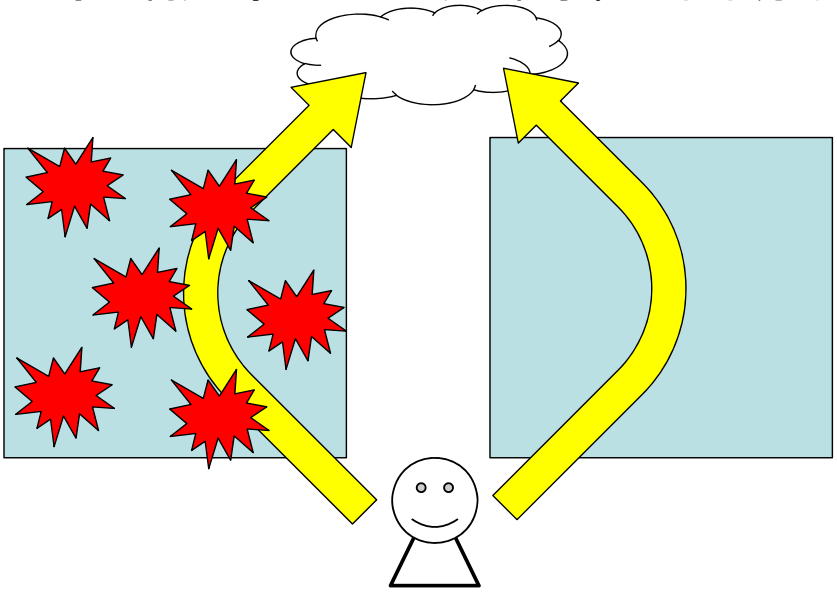
6. 人員の集約ではなく、スキルを整理して方法論を確立すること
   による知見の集約が必要

情報セキュリティ産業の課題

●リスクマネジメント教条主義
→インパクトアセスメントはリスクマネジメントの一部ではない
●視野狭窄傾向
→他分野で解決すべきことを、あたかも情報セキュリティ特需の
ように啓発活動する傾向がある
→しかも、それを悪意なく、狂信しているように見える
例）
個人情報保護
→本来は、CRM屋への特需であるべきはずだった
J-SOX法対応
→本来は、SCM屋、BCP屋などへの特需であるべきだった

情報セキュリティ産業の課題

●マッチポンプ営業： ホームユーザ課題と企業課題の区別
→スマートフォン利用時のセキュリティ対策の不十分な説明



この発表の録音など

http://yosihiro.com/speech/#2012-04-20

お問い合わせ

twitter

http://twitter.com/4416sato