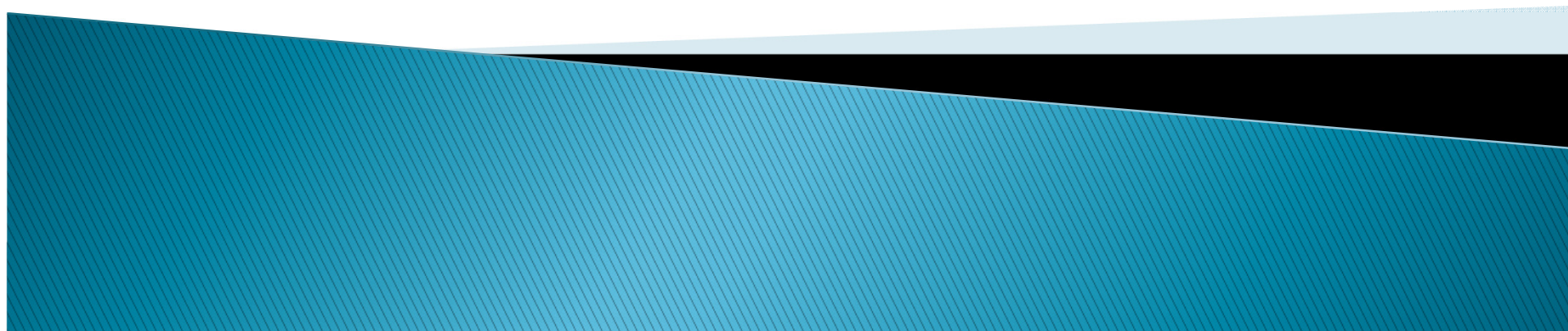


CAUAシンポジウム2014 資料

“私”の大学のセキュリティ に対する印象と パネルで伺いたい質問について

伊藤忠テクノソリューションズ 株式会社
セキュリティビジネス部
佐藤元彦



たとえば。。。 (at 2014 上半期)

- ▶ 金融系 ウェブ脆弱性リスク分析手法策定
 - ▶ 中央省庁 セキュリティ支援
 - ▶ 某商事 セキュリティ支援
 - ▶ 改ざん事案対応
 - ▶ 情報漏えい事案対応
 - ▶ 某サイバー攻撃事案対応
-
- ▶ というようなことを「最前線の現場」で行っています。
 - ▶ 分析、文書作成、法務、調査、監査、時には、検査も。。。セキュリティに関わる様々な業務を担当しております。
 - ▶ 本日は、第二部のパネリストのコーディネイターを努めさせていただきます。よろしくお願いします。

大学のセキュリティについて

▶ 私の印象

THE



ROO

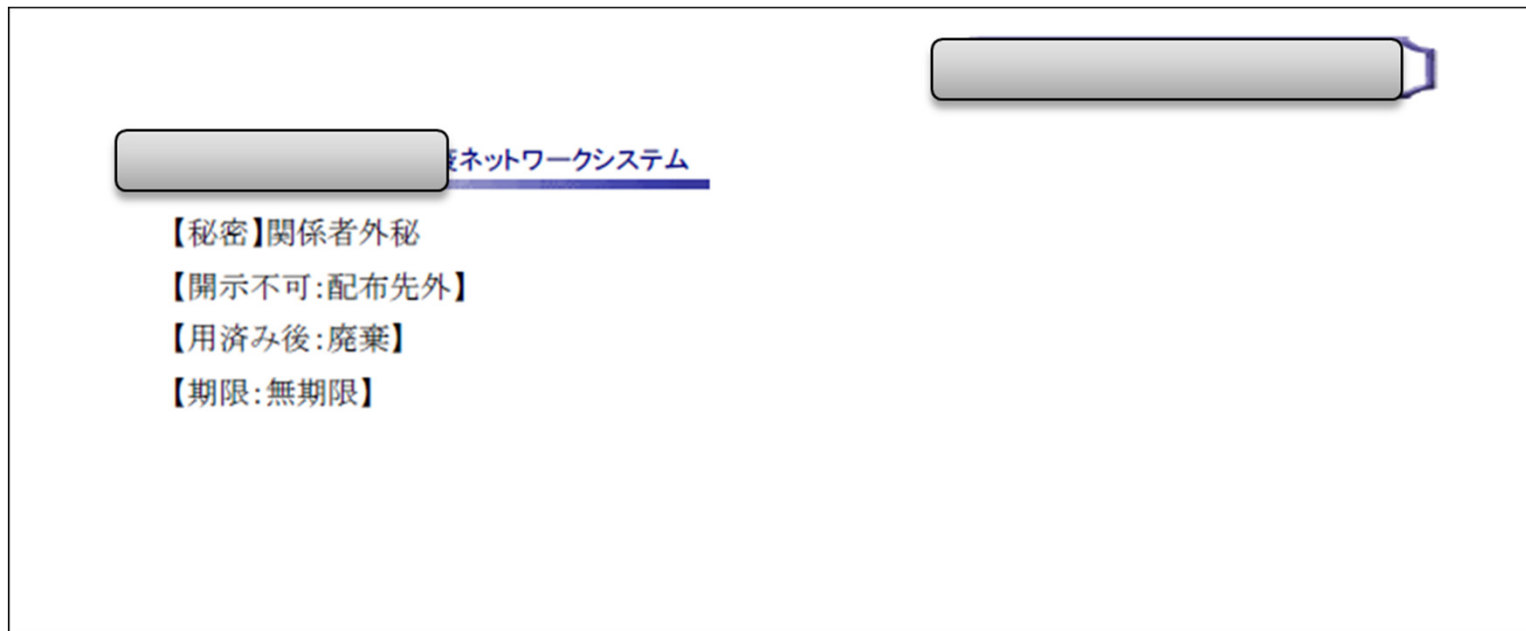


WHY?



現実には厳しい(1)

- ▶ @Google
- ▶ site:ac.jp "関係者外秘"



現実には厳しい(2)

- ▶ @Google
- ▶ site:ac.jp "スーパーコピー"

The screenshot shows a web browser window displaying a BBS page. At the top, there are navigation tabs: 研究室 (Research Room), 研究科 (Research Institute), 大学 (University), and 戻る (Back). Below these are more tabs: トップ (Top), 研究 (Research), 論文 (Papers), リンク (Links), プロフィール (Profile), and その他 (Others). A search bar contains the text 385590. The main heading is 何でもBBS. Below the heading is a notice: (まほ日記です。投稿内容に規程はありません。宣伝などの迷惑投稿を避けるために、パスワード制限を設けています。宣伝とかは見つけ次第、削除します。メールアドレスのリンクは文字毎にランダムにHTMLエンティティ形式に変更しています。). The form includes fields for: パスワード (Password) with a note (パスワードは nandemo), 名前 (Name), 題名 (Title), E-mail, URL, and コメント (Comment). There are buttons for 投稿する (Post) and リセット (Reset). Below the form is a post listing for 'スーパーコピーブランド2014年最新作' [12485] with a 返信 (Reply) button. The post details are: 投稿者:[人気] 投稿日:[2014年10月23日(木) 23時02分28秒]. The post content includes: スーパーコピーブランド2014年最新作, ルイヴィトンコピーモノグラム?ヴェルニバッグ最新作, and ルイヴィトンアンプラントレザーハンドバッグ2014新作.

現実には厳しい(3)

▶ @Google

- プリンタを見つける文字列で検索

The screenshot shows a web interface titled "リモートUI" (Remote UI) for printer management. The breadcrumb trail is "トップページ > ジョブ管理 > 印刷履歴". The main content area is "ジョブ管理" (Job Management) with a sub-section for "印刷履歴" (Print History). A table lists print jobs with columns for document name, user name, total page count, print time, result, and interface name. Two vertical grey bars redact the user names in the table. A sidebar on the left contains navigation links: "管理者パスワード:" (Admin Password), "ログイン" (Login), "トップページ" (Home), "デバイス管理" (Device Management), "ジョブ管理" (Job Management), "印刷ジョブ" (Print Jobs), "印刷履歴" (Print History), and "サポートリンク" (Support Links).

ドキュメント名	ユーザ名	総ページ数	印刷日時	印刷結果	インタフェース名
見積書.pdf	[Redacted]	1	2014 10/23 14:26	OK	
第92回日本... 会大会 演題登録	[Redacted]	3	2014 10/23 08:47	OK	
集談会順序... 5.pdf	[Redacted]	1	2014 10/22 19:30	OK	
新棟マウス 2...	[Redacted]	1	2014 10/21 12:41	OK	
新棟マウス 2...	[Redacted]	1	2014 10/21 12:41	OK	
新棟マウス 2...	[Redacted]	1	2014 10/21 12:41	OK	
新棟マウス 2...	[Redacted]	1	2014 10/21 12:41	OK	
新棟マウス 2...	[Redacted]	1	2014 10/21 12:41	OK	
Microsoft W... 5研	[Redacted]	1	2014 10/21 11:39	OK	
Microsoft W... 前回の	[Redacted]	6	2014 10/20 14:51	OK	
zt18d1_1.pdf	[Redacted]	1	2014 10/20 16:18	OK	
zt18d1_2.pdf	[Redacted]	1	2014 10/20 16:18	OK	
zt18d2_1.pdf	[Redacted]	1	2014 10/20 16:18	OK	
zt18d2_2.pdf	[Redacted]	1	2014 10/20 16:18	OK	

現実には厳しい(4)

- ▶ @Google
- site:ac.jp 初期パスワード

ユーザ名と初期パスワードは次のように決められています。

- ・ユーザ名:学籍番号(7桁)
- ・パスワード:生年月日8桁(西暦年4桁+月2桁+日2桁)

○統合認証アカウントの初期パスワードは次の通りです。

小文字 tg に「学生番号(7桁)」もしくは「教職員番号(7桁)」と「生年月日(8桁)」を足して それを整数部分(6桁)を加えたもの。

例) (1234567 学生番号もしくは教職員番号 + 19700101 生年月日) ÷ 97 = 215821.3195...
→パスワードは、tg215821

現実には厳しい(5)

▶ @Google

- site:ac.jp "index of/" "last Modified" 名簿
怖いので画像なし

▶ @Google

- site:ac.jp "index of/" "last Modified" 新年会
怖いので画像なし

無力感ありありですが。。。。

セキュリティ-1.0
の世界のまま。。。。

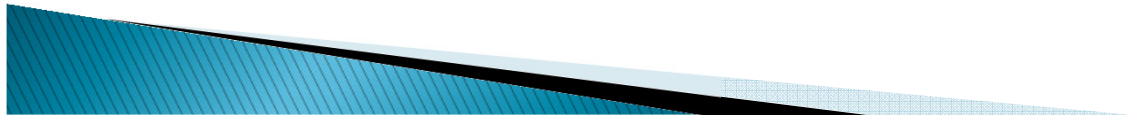
なぜ？



私の仮説

1. 大学は透明性が重要だから!!
(セキュリティなんて似合わない)
2. 大学は勉強の場。失敗も勉強!!
(こうやってセキュリティやプライバシーを覚えて学生は賢くなって社会に巣立っていくのです)
3. 大学に狙われるものなどないから!!
(リスクとコストを考えれば、コスト優先。ノーガードでOK)

そんなことは
ないですよ



私の帰無仮説

1. 先生・学生が勝手に研究室にサーバなどをおいてしまう。セキュリティを気にせずに。
2. 全ネットワークがグローバルIPなので、LANに繋がったら即座に世界の人々とお友達になれるネットワーク設計になっている。なので、世界からハッカーのお友達が来る。
3. 学部ごとにセキュリティ管理責任がばらばらで、調整が大変。全学のセキュリティの責任を誰もとりたがらない。

※注：帰無仮説です

大学は

1. 知の宝庫
2. 個人情報情報の宝庫
3. コンピュータリソースの宝庫

企業と提携した研究の成果、多年にわたって蓄積された実験データ、新たな発見を記載した論文案、悪用すると効果の高いコンピュータリソース

そして、「そこそこのセキュリティ」

攻撃者にはなかなか狙いがいがあるのでは？

“そこそこのセキュリティ”
を
“まあまあのセキュリティ”
にするには

どうすればよいのでしょうか？



パネルのテーマ

今回のパネルでパネリストの皆様にお伺いしたいことは二つです。

1. 大学のセキュリティを底上げするにはどうしたらよいか？
2. 大学も高度化・巧妙化する攻撃に晒される時代。何をどうしたらよいか？

コーディネーターの私見(1)

1. 大学のセキュリティを底上げするにはどうしたらよいか？

今や、学生の方がレベル高くなってきたんだから、学生でITに優れた学生を、学内ハッカーとして雇いましょう!!

で、社内のあるあれこれ調べてもらって、どんどん直していく。

かつ、その学生はセキュリティスキルがどんどんあがるため、就職に困らない!!

コーディネーターの私見(2)

2. 大学も高度化・巧妙化する攻撃に晒される時代。何をどうしたらよいか？

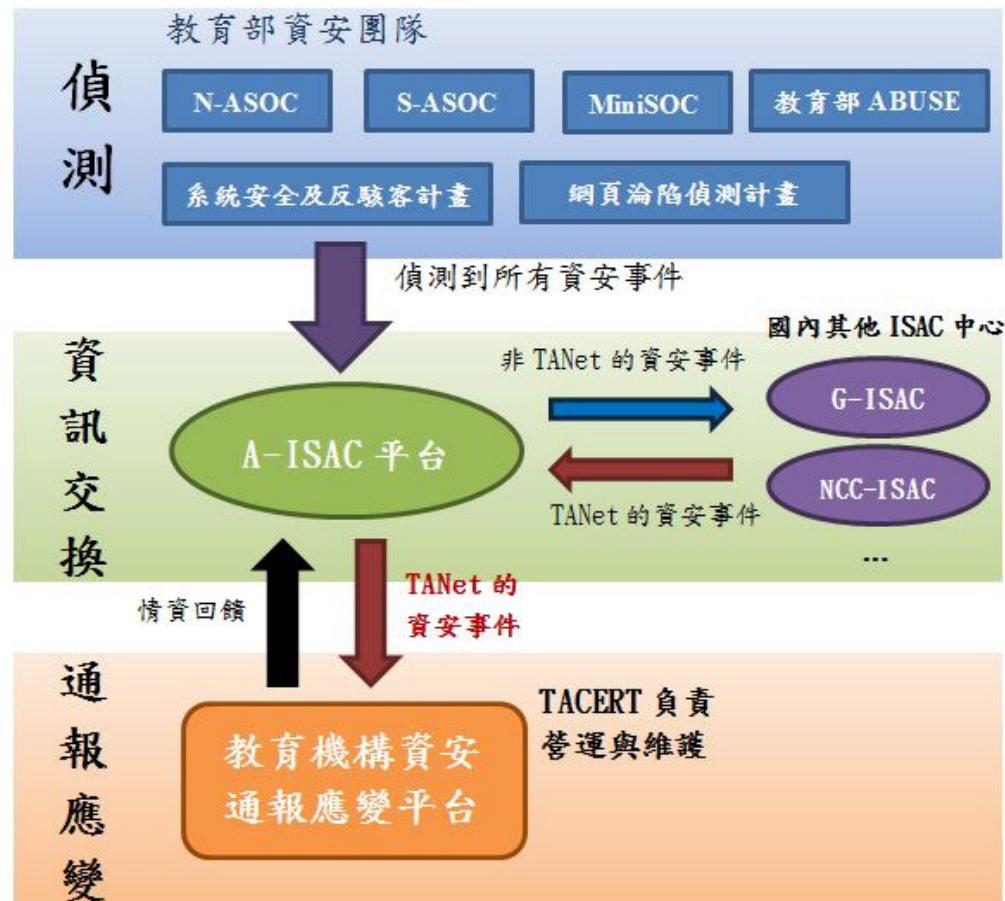
みんな悩みながら対策しているのではないか？
うちではこうだった、こうした。こんなことに困っている。このソフトのこんな脆弱性が攻撃された、危ない。こんな製品が有効だった。などなど。。。

担当者が意見や情報交換できるISAC
(Information Sharing and Analysis Center)
があると、相互扶助できるのではないか？

お互いを助け合わないと、単独の大学だけでは、
もうセキュリティが維持できないのではないか？

コーディネーターの私見(2)

台湾では仕組みが既にある？



休憩後に討論



問1

1. 大学のセキュリティを底上げするにはどうしたらよいか？

どのような設計・対応をすべきか。

そもそも、その設計・対応は、システムを対象とするだけでよいのか、制度も必要なのか、人を育てるべきなのか。そんな大変なことはしてられないから、丸投げした方がよいのか(クラウドへ!!)。

など

皆さんのお立場からの提言をお伺いさせていただきます。

問2

2. 大学も高度化・巧妙化する攻撃に晒される時代。何をどうしたらよいか？

うちの製品/サービスを導入すればすべて安全なのです。任せてください!! (ですよね?)

いや、製品・サービスだけではダメだ。それを活かす仕組みがなければ!!

高度化・巧妙化する攻撃に大学は耐えられない。
インターネット鎖国を検討しては??

など

こちらも、皆さんのお立場からの提言をお伺いさせていただきます。