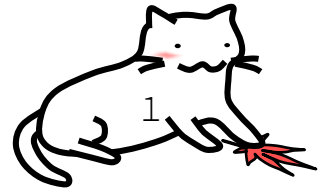
IP Meeting 2018
セキュリティ動向

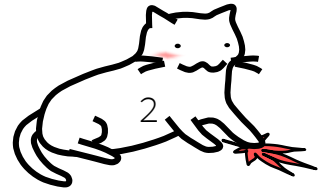
2018/11/30

セキュリティ専門家　中津留　勇
セキュリティ普通科　武井　滋紀



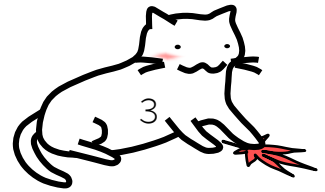
今年の動向（とあるプログラム委員会にて）

いやー、静かでしたね。



今年の動向

否！

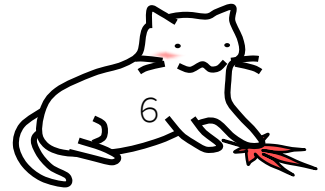



人類は
絶滅するんだよ


な・・・
なんだって
――!!

否！

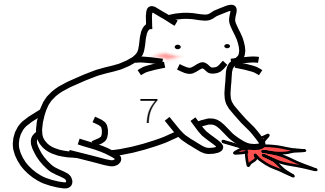
慣れた
or
見えなくなった



慣れた？

» インシデントは起きている！

» 脆弱性も出ている！

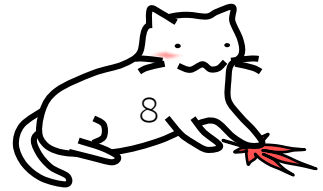


インシデントは起きている

» 「起こる」前提になってきた
» ウイルス感染もする前提になって来た
» 個人情報も漏えいする前提になってきた

むしろ起きた後どう対応したかが問われる時代に

日々準備しているのは当たり前、それでもやられるのは仕方ない
だからこそやられた後の対応も含めて評価される

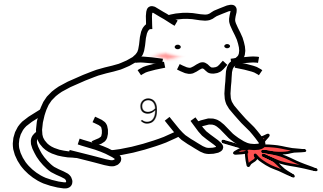


脆弱性情報も出ることに慣れてきた

» いつも出てくる「アレ」は常に見ている

» 影響が大きいか小さいか判断できるようになってきた

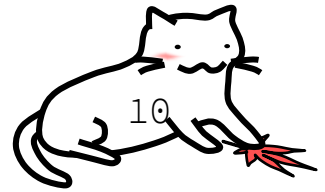
判断もできずにズルズル動かし続けて攻撃を受けると、二度と再起できないほどに信用も評判も落ちる



見えなくなった？

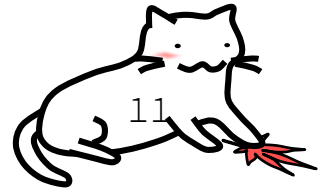
- DDoSよりもCoinhive
- お金が欲しい。脅すよりもこっそり掘る
- 詐欺で騙した方が早い

安全になったPCよりも騙せる人間へ



それでは

今年のIWセッションを振り返ってみましょう

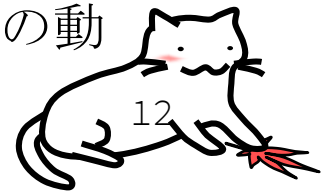


Internet Week流 Security BootCamp

常識変化に向き合おう

- 認証にまつわるセキュリティの新常識
  - 勝原　達也（NRIセキュアテクノロジーズ株式会社）
- TLS1.3時代の新常識
  - 大津　繁樹（ヤフー株式会社）
- TLSのWebブラウザの表示の今とこれからー EVの表示はどうなるのかー
  - 奥田　哲矢（日本電信電話　NTTセキュアプラットフォーム研究所）
- 知っておくべきIPv6とセキュリティの話
  - 中川あきら（日本インターネットエクスチェンジ株式会社）

- レイヤを上から下まで常識変化に向き合う。
- 認証、パスワード。TLS1.3でHTTPS化->EV証明書の表示のあるべき姿をgoogleの動きを考察しながら。IPv6の際の注意点があれこれと。

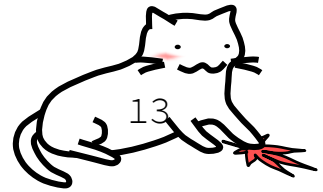


Internet Week流 Security BootCamp

脅威に向き合おう

- 見て学ぶ、標的型攻撃の脅威
  - 玉田　清貴（SecureWorks Japan株式会社）
  - 青木　翔（NPO 日本ネットワークセキュリティ協会）
- 脆弱性ハンドリングと耐える設計
  - 中島　智広（無所属 新）
- 電気通信事業法及び情報通信研究機構法改正等によるサイバー攻撃への対処
  - 後藤　篤志（総務省 サイバーセキュリティ統括官室）

- 対策も必要だが、起きた後の対策や、それを国として見つけて教える仕組みが必要という内容へ。
- 最終的には組織体制や人材育成に話が及ぶ不思議



Internet Week流 Security BootCamp

社会を動かすモノのセキュリティ

- 産業用制御システムを襲うサイバー攻撃の実態・最新動向
  - 佐々木　弘志（情報処理推進機構　産業サイバーセキュリティセンター）
- 産業用制御システムの基本をIT系にわかりやすく解説
  - 目黒　有輝（情報処理推進機構　産業サイバーセキュリティセンター ）
- 産業サイバーセキュリティに関する政府の取り組み（政策担当者の目線から）
  - 木村　隼斗（経済産業省商務情報政策局サイバーセキュリティ課）

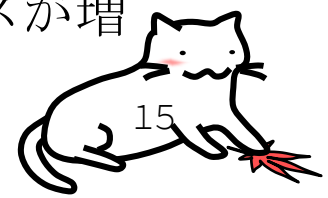
- 防御に向けては人とのコミュニケーションをまずなんとかしよう。多層防御という意味ではサプライチェーンまでやろう。サプライチェーンまでやるなら国が指針を示して大企業から中小企業まで、人材育成の指針も示してセキュリティビジネスのエコシステムを創造しよう

企業のサイバーセキュリティ最新戦略

サイバー攻撃最前線2018

- 迫り来る標的型攻撃に備えて
  - 輿石　隆（一般社団法人 JPCERTコーディネーションセンター）
- 日本の組織を狙うビジネスメール詐欺
  - 松坂　志（独立行政法人情報処理推進機構）
- サイバー攻撃による不正な仮想通貨マイニングの実態
  - 西尾　裕哉（株式会社セキュアスカイ・テクノロジー）
- Roaming Mantis – DNS設定改ざんから始まった大規模な攻撃活動の調査結果
  - 石丸　傑（株式会社カスペルスキー）
  - 二関 学（NTTセキュアプラットフォーム研究所）

- TSCookieに関連したダイナミックDNSや独自ドメイン。ビジネスメール詐欺の手口、Drive by Miningやサーバ側でのMiningといった攻撃が今後増えるのでは、悪性DNSによるPCやモバイルへの攻撃
- 直接金銭を狙う詐欺や、見えにくい低リスク低リターンのマイニングを行うケースが増えている。

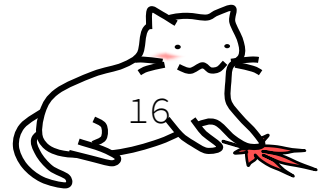


企業のサイバーセキュリティ最新戦略

もう一人で困らない！セキュリティ対応のアウトソース

- 第一部+第二部
  - 武井　滋紀（ISOG-J、NTTテクノクロス株式会社）
  - ももいやすなり（ISOG-J、株式会社インターネットイニシアティブ）
  - 早川 敦史（ISOG-J、NECソリューションイノベータ株式会社）
  - 田中 朗（ISOG-J）
  - 河島 君知（ISOG-J、NTTデータ先端技術株式会社）
  - 阿部 慎司（ISOG-J、NTTセキュリティ・ジャパン株式会社）
  - 砂田 浩行（ISOG-J、株式会社　日本総合研究所）
  - 亀田 勇歩（ISOG-J、SCSK株式会社）
  - 伊藤　彰嗣（ISOG-J）

- アウトソースまでの流れをおさらい。アウトソースには選ぶ前、選ぶ際、運用を始めてからの3つの段階で選ぶポイントがある
- 監視運用は買ったらゴールじゃない、スタートだ！

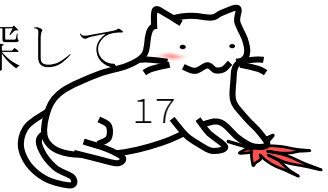


企業のサイバーセキュリティ最新戦略

知れば組織が強くなる！ペネトレーションテストで分かったセキュリティ対策の抜け穴

- 丸ごと分かるペネトレーションテストの今
  - 石川 朝久（NRIセキュアテクノロジーズ株式会社）
- Sansanがペネトレーションテストを受けてきた3年間の記録
  - 河村 辰也（Sansan株式会社）
- 座談会
  - 小河 哲之（三井物産セキュアディレクション）
  - 北原 憲（株式会社ラック）
  - 大塚 淳平（NRIセキュアテクノロジーズ株式会社）
  - サイフィエフ ルスラン（株式会社イエラエセキュリティ）
  - 中津留 勇（ SecureWorks Japan 株式会社）

- 物理的なペネトレーションテストもあるよ、やってる会社は何度かやって弱点を探しているよ、座談会の内容は危なすぎるので中津留さんにお任せで。

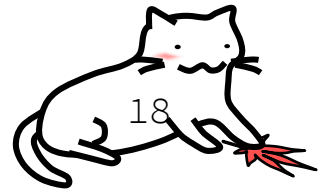


実録CSIRT24時！その時何が起きたか！

「Chatham House Rule」のため詳細は非公開

- 原子拓（NCA/ラック）
- 西村卓也（株式会社KADOKAWA）
- 猪俣敦夫（東京電機大学/大阪大学　教授）
- 齋藤衛（株式会社インターネットイニシアティブ）
- 北村達也（大成建設株式会社）
- まっちゃだいふく（セキュリティ専門家）

- 講演者それぞれの立場で事例を紹介し、そこからの知見を会場で共有。その場で活発にやり取りがあり、突っ込んだ内容も。
- 体制を作っただけではなく、普段からの監視や対応の努力を続けるが、1社だけで頑張るのではなく、情報を共有しながら各社のポリシーにあったベストプラクティスを作り上げることが重要と認識。



まとめ

» 状況や常識は変化している。

» 静かな今だからこそできることもある

終わりの始まりなのか、嵐の前の静けさなのか。
大事故が起きてから慌てるのではなく、普段から
訓練や連携を続けることが大事。