最近の大学などにおける 情報セキュリティインシデントの動向とその対処

2008/2/6 情報セキュリティセミナー

有限責任中間法人
JPCERT コーディネーションセンター
小宮山 功一朗, CISSP

内容

- JPCERT/CCとは
  - 組織の概要
  - 自己紹介
- 世界の大学は今
- 日本の大学
  - 外部からの脅威
  - 内なる脅威
- 大学生とSNS
  - 高まるソーシャルエンジニアリングのリスク
- インシデントレスポンス
- 時代に即したセキュリティ教育
- まとめ

JPCERT/CCとは

JPCERT/CCの概要

- JPCERT/CC (ジェーピーサート･コーディネーションセンター)
  - Japan Computer Emergency Response Team Coordination Center
  - http://www.jpcert.or.jp/
  - 非営利組織
- 活動
  - コンピュータセキュリティインシデントに関する調整、連携
  - インシデントや脆弱性に関するコーディネーション
  - 情報収集･分析･発信
  - 国内組織や海外組織との連携(特に各国のCSIRT組織)

活動の概要

インシデント予防

インシデントの予測と捕捉

発生したインシデントへの対応

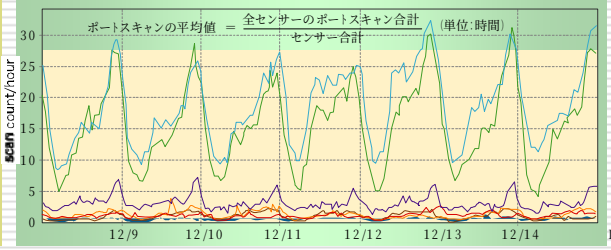
脆弱性情報ハンドリング

未公開の脆弱性関連情報を
製品開発者へ提供し対応依頼
国際的に情報公開日を調整

JVN Japan Vulnerability Notes

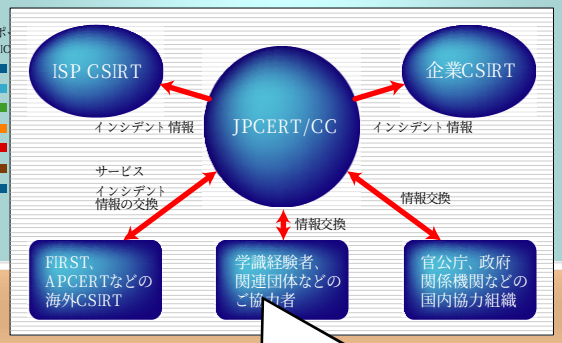
定点観測（ISDAS）

ネットワークトラフィック情報
の収集分析
定期的なセキュリティ予防情
報の提供



インシデントハンドリング

インシデントレスポンスの時間短
縮による被害最小化
再発防止に向けた関係各関の
情報交換および情報共有



早期警戒情報

重要インフラ事業者等の特定組織向け情報発信

CSIRT構築支援

企業内のセキュリティ対応組織の構築支援

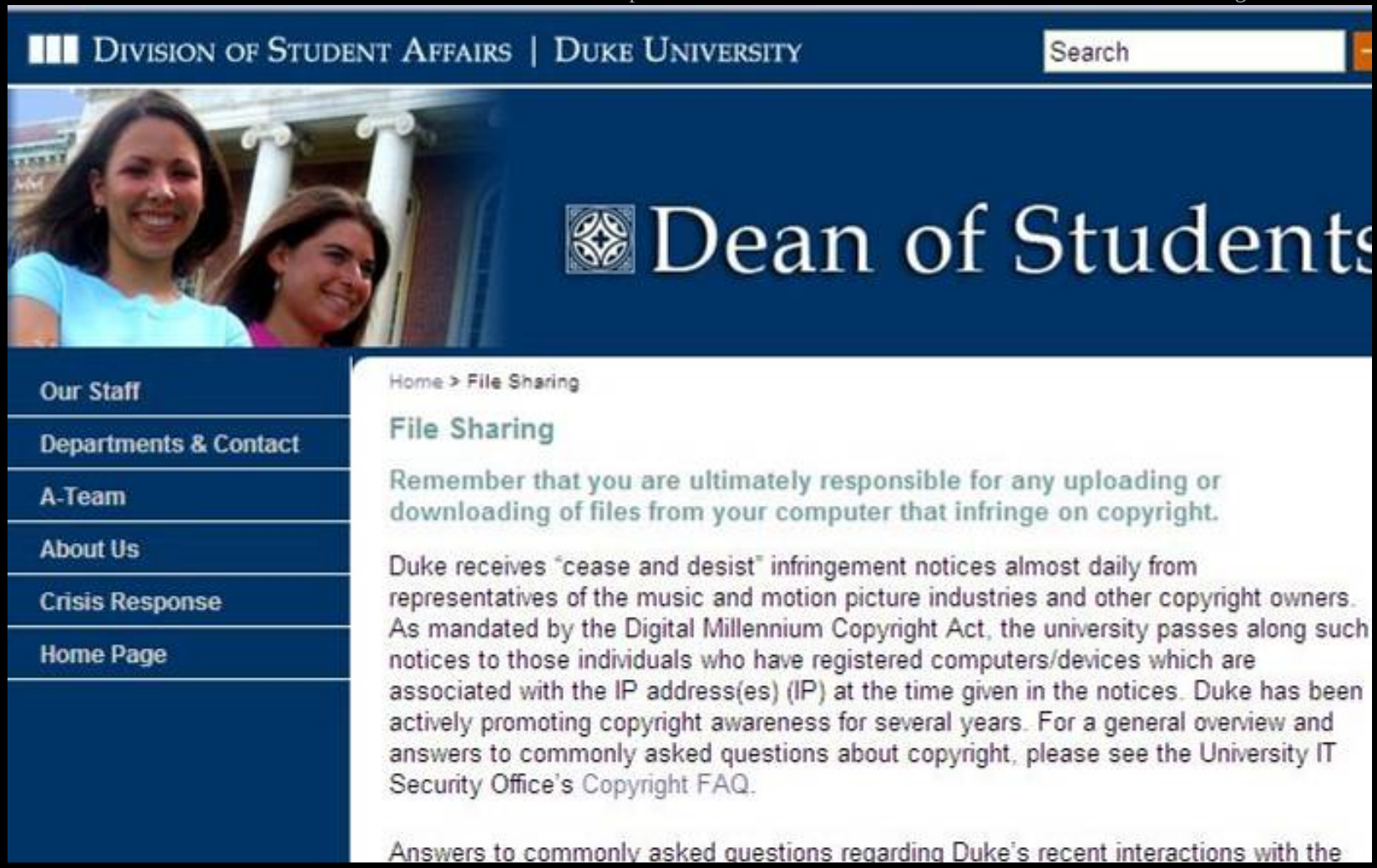
インシデントレスポンスの一環として **フィッシングサイトの停止(テイクダウン)** 依頼業務を行う

私について

- 在学時、研究室のサーバ管理を任されていました
- 放置していました
- 乗っ取られました
  - Webサーバ → オンラインゲームサーバ
  - トラフィック急増
- 復讐のため、セキュリティ業界の門を叩く

世界の大学は今

http://deanofstudents.studentaffairs.duke.edu/filesharing/index.html



RIAA

http://images.google.com/

コンテンツフィルタ

Botのない大学

まとめ: 世界の大学は今

- 大学は色々、悩みも色々
  - 予算
  - 情報システム担当にあたえられた権限
  - ユーザのITリテラシ
- 大学の問題を一口に語ることは難しい。

日本の大学

外部からの脅威

- 標的型攻撃
  - アメリカ、オークリッジ国立研究所
  - アメリカ、ロスアラモス国立研究所
- 国立研究所系の職員への教育(と防御)は急務

Source: ABC News: Chinese Suspected in U.S. Cyberattack (http://abcnews.go.com/TheLaw/story?id=3966047)

*Source: **標的型攻撃についての調査** (http://www.jpcert.or.jp/research/2007/targeted_attack.pdf)*

内なる脅威

- P2Pソフトの使用
- 幅広い知識レベルのユーザ
  - 永遠の初心者
  - ヘビーユーザ
- 組織内での独立性の高さ
  - 他学科、他学部、他キャンパスとの連携
- 物理セキュリティレベルの低さ
- 担当者が少ない/異動が頻繁

- アクセス回線潤沢/ネットワークアドレス大量所持
  - →学内にBot多数

大学生とSNS

～高まるソーシャルエンジニアリングのリスク～

SNS隆盛

- 氏名、住所
- 勤務先、学校
- 趣味
- 家族構成 / 交友関係
- 年齢
- 顔写真

電話、メール、インスタントメッセンジャーと同列の連絡手段

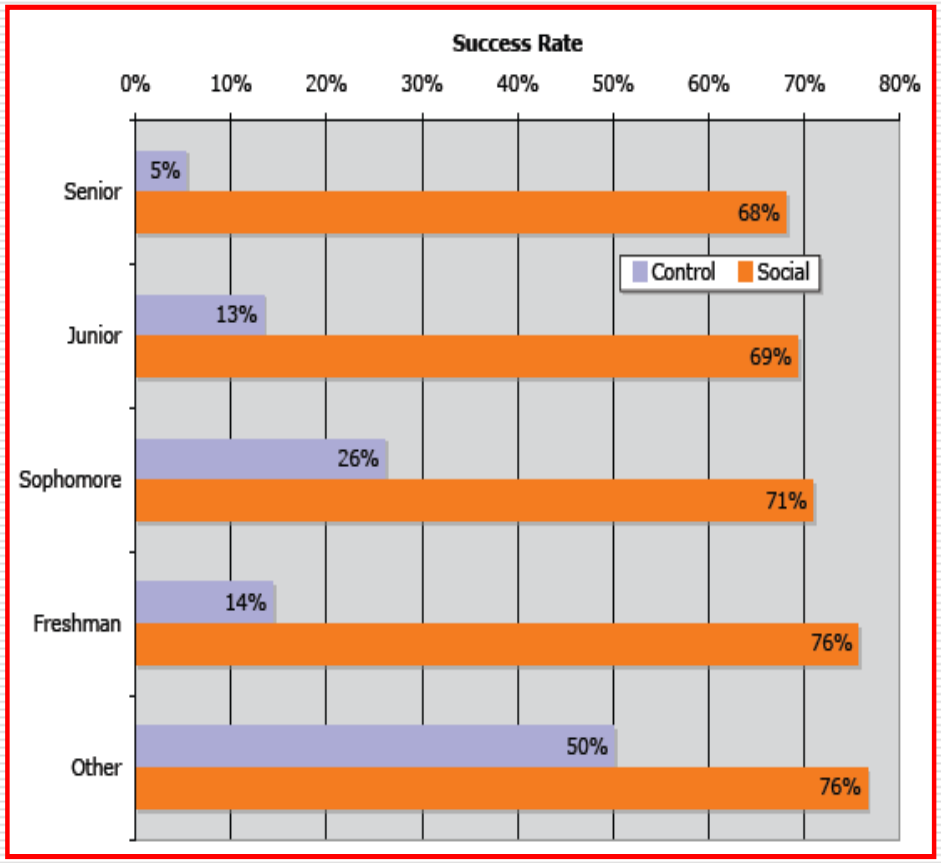
『電話くれたみたいだけど、用件は?』

SNSの情報が悪用されると・・・

- インディアナ大学で2005年12月に行われた実験
  - 学生900名にフィッシングメールを送りつける
  - SNS（myspace.com, facebook.com, ebay）を利用 → Social Phishing
  - ソーシャルエンジニアリングを使うと攻撃成功率が4倍に

出典: Social Phising, Indiana University (Dec 12, 2005)
http://www.indiana.edu/~phishing/social-network-experiment/phishing-preprint.pdf

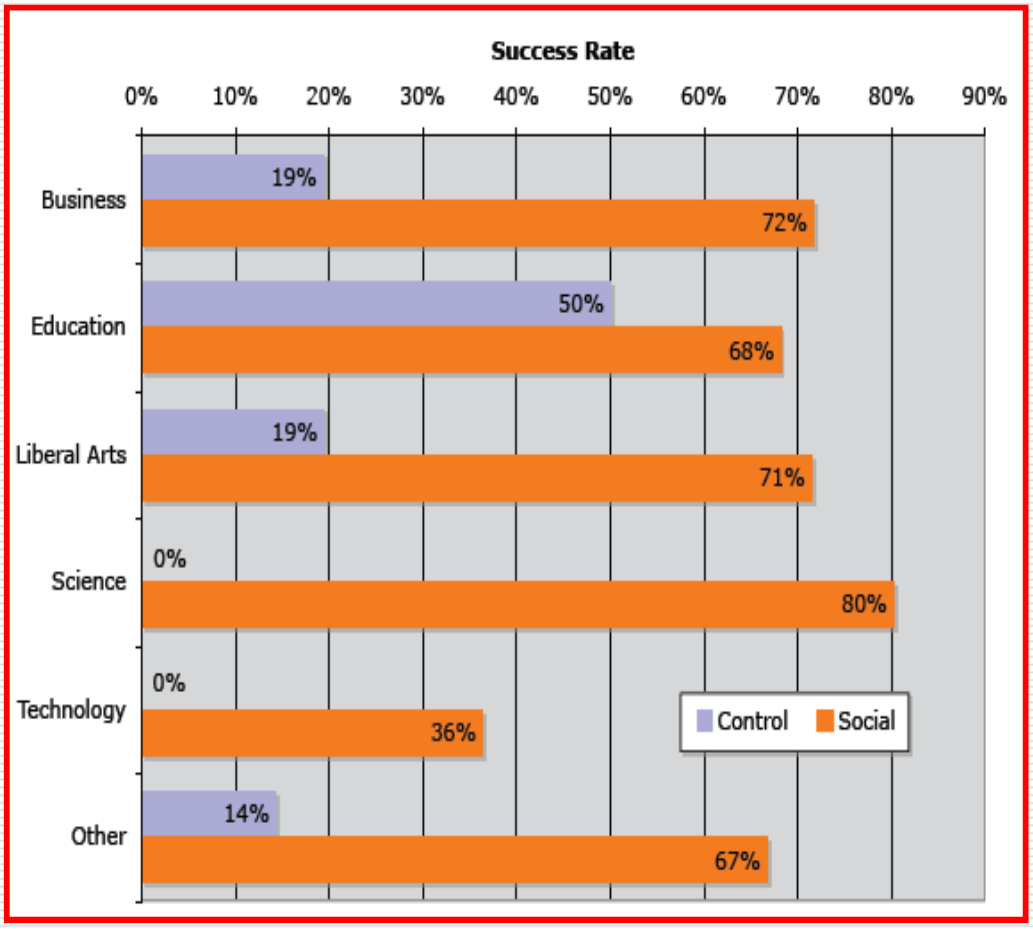
釣られやすい1年生



- 学年が上がるにつれ、フィッシングの成功率は低くなっていく。

出典: Social Phising, Indiana University (Dec 12, 2005)

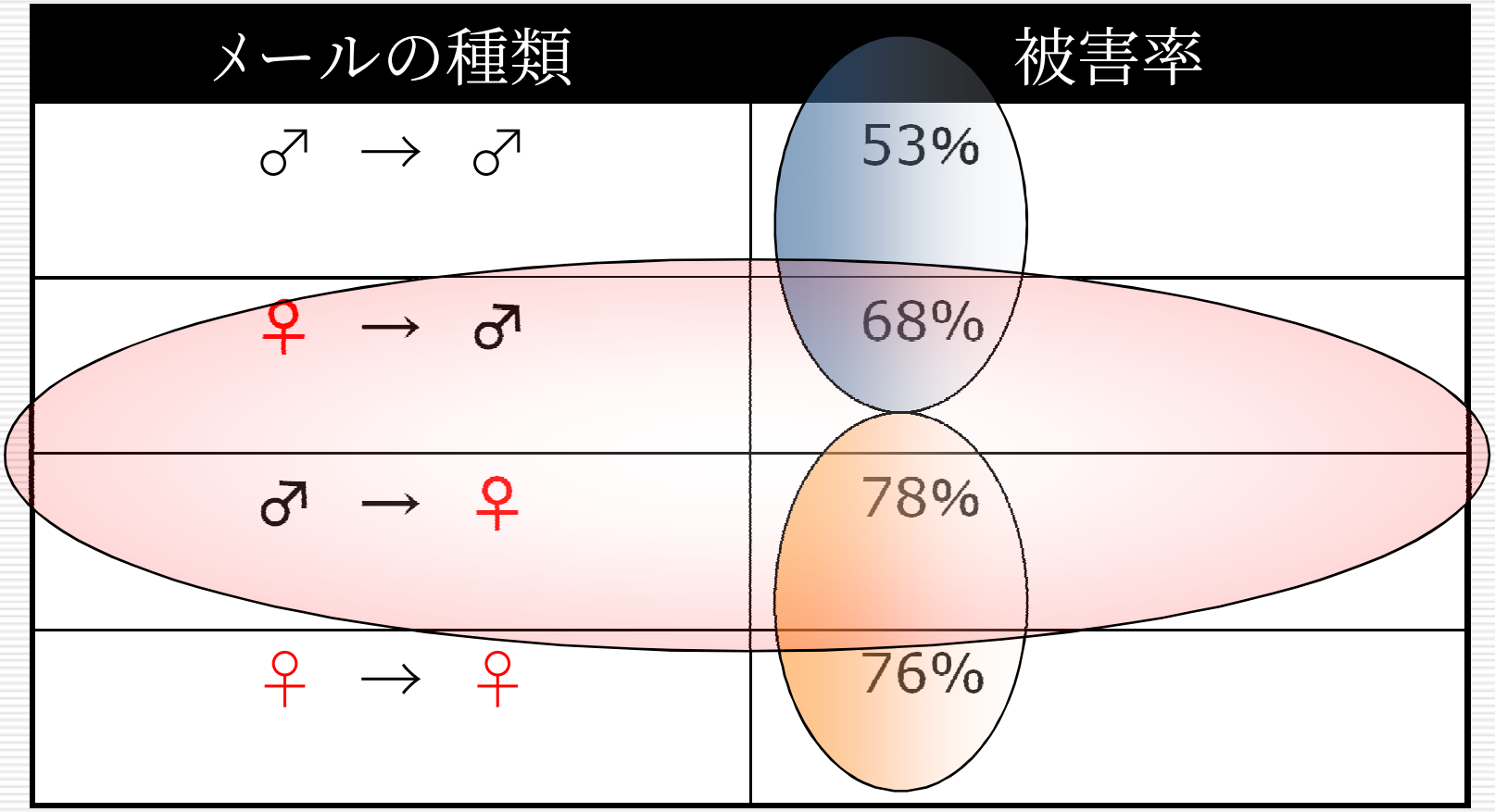
“知り合い”に弱い理学部



- ITリテラシーの低い教育学部
- さすが工学部
- まじめすぎる理学部

出典: Social Phising, Indiana University (Dec 12, 2005)

性差



“ソーシャルネットワーク”というもの

- マイミクシィの数は81
  - コミュニティに1つも参加していないマイMixiの数：10
- マイミクシィが参加しているコミュニティの総数（重複除く）：2163

コミュニティ名	参加数	総参加者数	マイミク含有率
[redacted]	9	11	81.8%
	8	8584	0.1%
	7	11	63.6%
	7	869	0.8%
	6	7	85.7%
	6	38	15.8%
	6	1904	0.3%
	5	40	12.5%
	5	243	2.1%
	5	112882	0.0%

“ソーシャルネットワーク”というもの 続き

- Weakest link theory
  - 一番弱い輪の強度＝鎖全体の強度
  - ネットワーク内で最も情報を開示している人間

インシデントレスポンス

CSIRTというアプローチ

- 情報セキュリティ委員会との違い
  - 発生した事象から防止策・管理策を検討する組織
  - 被害拡大を防ぐためのレスポンス
- レスポンスサービス
  - くさいものに蓋をしない
- CSIRTに必要なもの
  - → 戦略性
  - → 内部調整能力
  - → 外部との協力

FiRST加盟の大学CSIRT

- FiRST
- University of Wisconsin-Madison
- Indiana University CERT
- Northwestern University
- The Ohio State University Incident Response Team
- Oxford University IT Security Team
- Pennsylvania State University
- Stabsstelle DV-Sicherheit der Universitaet Stuttgart
- Stanford University Information Security Services
- The University of Georgia Computer Incident Response Team
- University of Michigan CERT
- The University of Chicago Network Security Center
- CERT for the Technical University of Catalunya

JPCERT CC®

時代に即したセキュリティ教育

コミュニケーション手段の変化

- 死語 ネチケット
- 学校裏サイト
- “やりとりはmyspaceかチャットで”
  - ドン・タプスコット / アンソニー・D・ウィリアムズ (2007)『ウィキノミクス マスコラボレーションによる開発・生産の世紀へ』 日経BP社

技術の変化

- Exeを実行しないでください
  - Doc,pptでも感染。Webにアクセスした際にjava scriptを経由して攻撃を受けることも
- 自分が被害者にならないために
  - 自分が加害者にならないために

ターゲットに応じた情報発信

- ガートナーのアナリストが考える、セキュリティ啓発活動を改善する方法
- メッセージを伝えたいのは誰か?
  - 経営層
  - ITエンジニア → 理工系のスタッフ/学生
  - エンドユーザ → 一般学生
- 伝える相手を絞り込み、最適化したメッセージを発信する

経営層向け

- 媒体
  - 多くの経営層は活字の情報を重視する。(直接のコミュニケーションを重視する人も)
- 態度
  - 知的、温厚に、絶対に脅してはならない
- 頻度
  - 何もないときでも四半期に一度 問題発生時やプロジェクト中は月に一度

ITエンジニア

- 媒体
  - 直接会って話すのが一番
- 態度
  - 情報提供、仲間として、
    2話したら8聞く
- 頻度
  - 月に一度、多くのエンジニアは既に情報過多であると感じている

エンドユーザ

- 媒体
  - 動画、対面のプレゼンテーション、冊子、リマインドはEメール
- 態度
  - 「面倒を見る」という気持ちを持って接する
  - チアフル、カラフル
- 頻度
  - 新人教育，年次更新教育，確認のための試験など

経済産業省 CHECK PC! キャンペーン
http://www.checkpc.jp/top.html

共通:メッセージを作るときには

- 伝えたいグループを絞る
- メッセージを10単語で (英語の場合)
- 何度も送らない

まとめ

- 大学はいろいろ
- 特にSNSがもたらした変化に、ユーザの意識が置いて行かれがち
- 組織的な対応を(教育/インシデントレスポンス)
- セキュリティ教育
  - コミュニケーションツールの適切な選択
  - 攻撃技術の動向を理解
  - 相手に応じたメッセージ

お問い合わせ先

- JPCERTコーディネーションセンター
  - Email：office@jpcert.or.jp
  - Tel：03-3518-4600
  - http://www.jpcert.or.jp/

- インシデント報告
  - Email：info@jpcert.or.jp
    PGP Fingerprint：BA F4 D9 FA B8 FB F0 73 57 EE 3C 2B 13 F0 48 B8
  - 報告様式
    http://www.jpcert.or.jp/form/

JPCERT CC®

ご清聴ありがとうございました