令和２年度
情報セキュリティ研修テキスト

沖縄県 企画部　総合情報政策課

研修の目的と概要

- 研修の目的
  - 職員の情報セキュリティの知識および意識レベルを向上し、緊急時に適切な対応を取れるようにすること。
- 目次
  - 県内で発生した情報セキュリティインシデントについて
  - ＣＳＩＲＴ（シーサート）について

県内で発生した情報セキュリティインシデントについて

ホームページへの誤掲載

- 令和元年、浦添市で２件発生
  - いずれもファイルに個人情報が記載されていることに気がつかず、ホームページに掲載してしまった。内１件は担当者が気づいてすぐに差し替えたが、検索エンジンのキャッシュにデータが残っていた。

- 愛知県でも発生
  - 令和２年５月には、愛知県が新型コロナウイルスの患者に関する個人情報をWebページに掲載してしまい、一人当たり2～4万円を賠償することになった。

誤掲載を防止するには？

- 原因はヒューマンエラー
  - ２重チェック体制の整備。掲載するファイルは必ず上司の承認を受けるなど。
  - よくある誤掲載の事例を基に、セルフチェックを行う。
    - □個人情報を消し忘れていないか
    - □掲載するファイルを取り違えていないか
    - □ファイルの別シートに情報が残っていないか
    - □黒塗りした部分にデータが残っていないか
    - □削除した誤掲載の情報が検索エンジンに残っていないか

  - ルールがあっても守られなければ意味が無い。愛知県の事例では、２重チェックの規則はあったものの、ゴールデンウィーク中で他の職員がいなかったため、チェックが働かなかった。

メールの誤送信

- 令和元年11月、沖縄県教育庁で発生
  - 健康診断を委託していた医療機関に、Excelファイルで作成された様式を送ったところ、別シートに個人情報が記載されていた。医療機関からの連絡で判明し、削除依頼を行った。

- 琉球大学の事例
  - 令和２年２月、受験者に面接集合時間のお知らせをメールで送る際、宛先にBccと指定すべきところToのまま誤送信してしまい、メール受信者同士でメールアドレスが見られる状態になった。

誤送信を防止するには？

- 誤送信の種類
  - 多いのがBccとToの指定ミス。誰に送ったかが機密になる場合もあるが、漏えいしたアドレスに対し、迷惑メールが送られたり、リスト型攻撃に使われるなどの二次被害もありえる。個人にとってメールアドレスは、インターネット上の住所にあたる重要情報であるという認識を持つことが必要。
  - 他には、誤って個人情報の入ったファイルを添付する、送信先アドレスの入力をミスして第三者に送信するなど。

  - ヒューマンエラーなので、ミスに繋がる操作を行わないようメールソフトの設定を変更する。
  - 定期的に一斉送信を行う業務ではメーリングリストを活用する。
  - メールアドレスの自動補完機能は解除する。
  - メールアドレスを手入力した場合は、相手方に届くか空メールを送信するなどして、必ず確認を行う。

記憶媒体等の紛失・盗難

- 令和元年１月、豊見城市で判明
  - 新庁舎への引っ越し作業中に、個人情報が記録されているハードディスクが所在不明になった。現在に至るまで発見されていない。

- 沖縄県でもタブレットやUSBの紛失、盗難が発生
  - 主に教育現場において、タブレット端末やUSBメモリ等の紛失、盗難が発生している。

- テレワークの導入が進み･･･
  - 新型コロナの影響により、自治体においてもテレワークの導入が進んでいる。端末等の持ち運びや、情報を外部で扱う機会が増えたことから、紛失、盗難の危険性が増している。

紛失、盗難を防止するには？

■ 人的対策の例

- 情報資産（端末、記憶媒体等）は管理簿により、その所在や利用者の確認を行う。
- USBメモリの注意事項としては、カギ付きの場所に仕舞う、管理簿により出し入れをチェックする、ストラップを付けて首から提げる、保存する情報は暗号化するなど。
- テレワークで情報を持ち出す際は、上司の許可を得ること。また、許可された端末･媒体を使用すること。

- 技術的な対策も可能。本県ではUSBメモリに保存する際の自動暗号化、タブレット端末へのMDM導入（遠隔でデータの消去や、所在の確認が可能になる）、テレワーク用にシンクライアント端末を採用するなど、紛失･盗難時の被害軽減対策を講じている。

ID･パスワードの漏えい

- 沖縄県職員のアカウント情報が外部に漏えい
  - 職員のアカウント情報（ID･パスワード）が外部に漏えいしていないか、委託業者に調査を依頼したところ、１６５件の漏えいが判明した。
- 漏えいの原因は外部サービスの利用
  - インターネット上にあるサービス等を利用する際には、ID（又はメールアドレス）とパスワードの登録が必要になる。その登録した外部サイトがサイバー攻撃を受け、アカウント情報が流出したと考えられる。
- 何が危険なのか？
  - 攻撃者は、入手したアカウント情報を使って他のWebサービスにログインできないか試みる。（リスト型攻撃）
  - パスワード等を使い回していた場合、攻撃者のログインが成功してしまい、なりすましや個人情報が盗まれる等の被害が発生する。

ID･パスワードの悪用を防ぐ

- 外部サービスからの漏えいは防げない
  - サイバー攻撃への対策は各サイトにより異なるので、事前にサービス内容を確認し、セキュリティ対策の甘いサイトは利用しない、くらいしか方法が無い。

- パスワードの使い回しは禁止
  - 不正アクセスを防ぐため、システムにログインする際に入力しているＩＤ、パスワードを、他のサービスやプライベートで利用しているＳＮＳ、ネットバンキング等で使い回すことを禁止する。

- 強固なパスワードを設定する
  - ＩＤだけが流出している場合、攻撃者はパスワードを総当たりで入力（ブルートフォース攻撃）してくる。これは強固なパスワードを設定（10文字以上、大文字･小文字の組み合わせ、数字･句読点･記号入り）することで防げる。

SNSによる情報漏えい

- 職場の写真を投稿→機密情報が漏えい
  - 兵庫県姫路市の資産税課職員が、職場で自分の机の上を撮影しTwitterに投稿したところ、写真に税務情報が映り込んでいた。外部からの通報で判明。

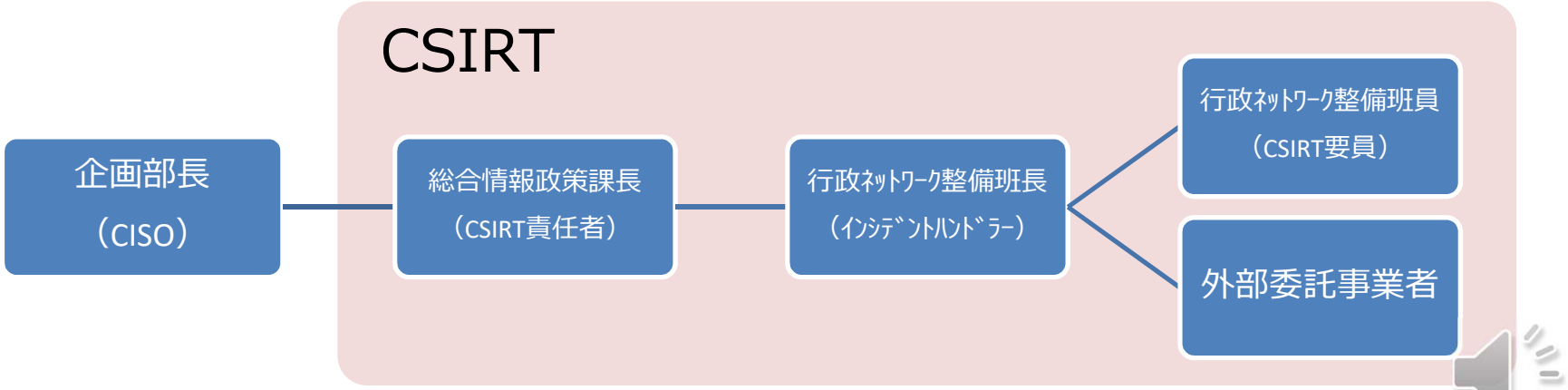
- 本人が書き込まなくても？
  - 某お菓子メーカーの未発表の新作パッケージがTwitterに流出。取引先に勤める父親が試作品を自宅に持ち帰り家族に話したところ、その娘が書き込んでしまった。

- SNSの利用には注意が必要
  - 仲間内のやり取りのつもりで無警戒に投稿してしまう。
  - 業務上知り得た秘密は、プライベートのつもりでも、匿名だったとしても、SNSで公開した時点で守秘義務違反になる。
  - 家族や友人にも情報セキュリティ意識を。

CSIRT（シーサート）について

CSIRT（シーサート）の定義

- CSIRT（Computer Security Incident Response Team）
  - 情報システムに対するサイバー攻撃等の情報セキュリティインシデントが発生した際、発生した**情報セキュリティインシデントを正確に把握・分析し、被害拡大防止、復旧、再発防止等を迅速かつ的確に行う**ことを可能とするための機能を有する体制



情報セキュリティの事件・事故はCSIRTへ

- CSIRTの仕事
  - システム停止、サイバー攻撃、盗難・紛失などの事件・事故が発生した際に、所属と連携して初動対応・復旧・再発防止策の検討を行う。
  - 平常時はインシデント対応に必要な事前準備・予防や訓練を行う。

- インシデントを発見したら
  - 職員等はインシデントを発見した場合、速やかにCSIRT及び情報管理者（所属の課室長）に連絡する。

- CSIRTの連絡先
  - メール：csirt@pref.okinawa.lg.jp
  - 電　話：098-866-2036（総合情報政策課）