事例から学ぶ情報セキュリティ対策

名城大学理工学部情報工学科
渡邊研究室
新家悠介

書籍紹介

- 題目： 企業のための情報セキュリティ
- 著者： 石田淳一、吉田直可
- 発行： 平成25年8月2日
- 発行所： レクシスネクシス・ジャパン株式会社

全体の流れ

- セキュリティは攻撃対策？
- 事例から学ぶセキュリティ対策
- 今できること
- まとめ

全体の流れ

- セキュリティは攻撃対策？
- 事例から学ぶセキュリティ対策
- 今できること
- まとめ

セキュリティ対策はなぜ必要か

トラブルを避けるため！

対策を怠ると……　→　機密情報の漏洩

→ 陳謝・賠償・二次被害

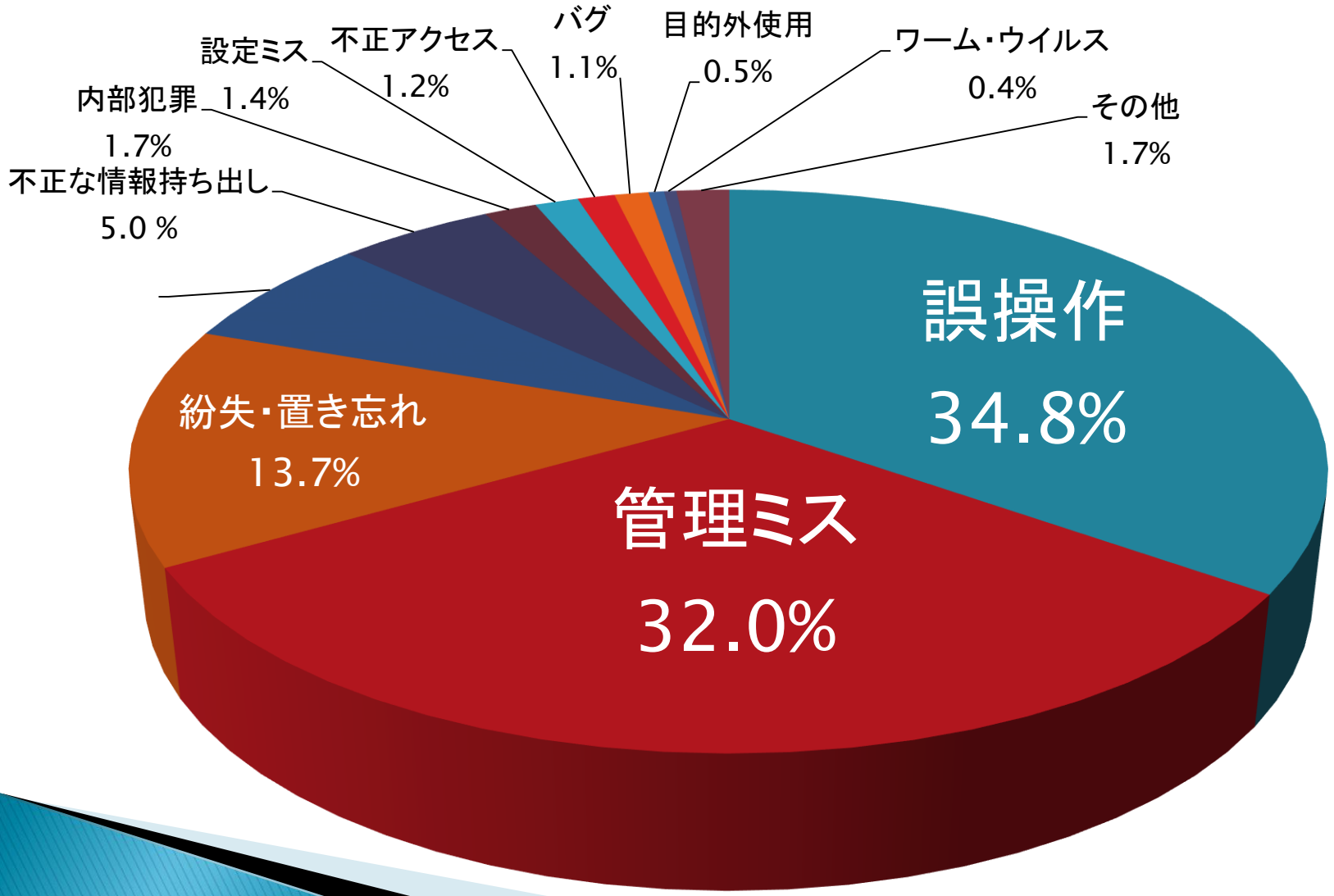
→ 信用失墜

→ 企業に大ダメージ

↓

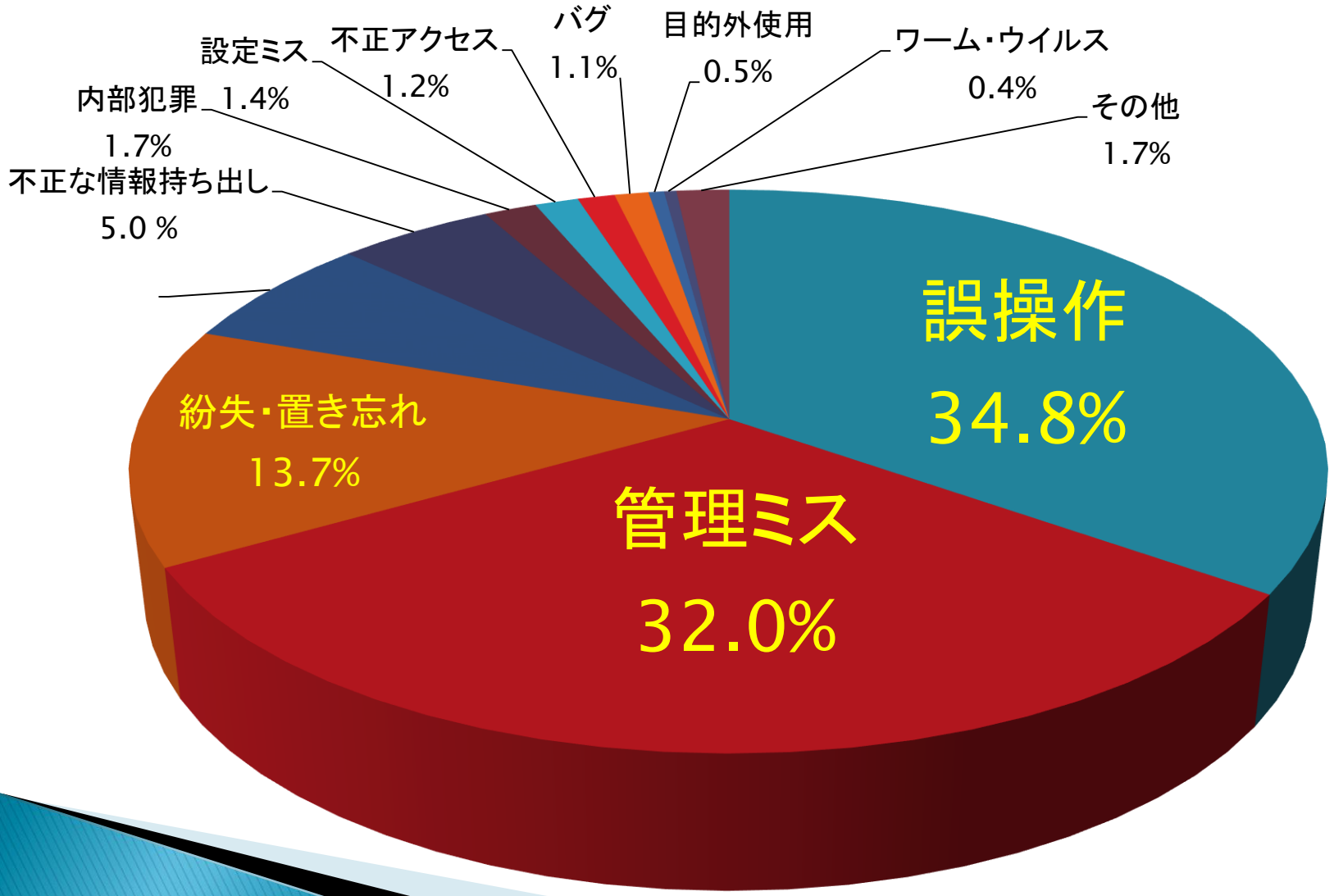
攻撃に備えれば安心？

なぜ起こる？　情報漏洩の主な原因



個人情報漏えいに関する調査報告書

なぜ起こる？　情報漏洩の主な原因



個人情報漏えいに関する調査報告書

セキュリティ対策に重要なこと

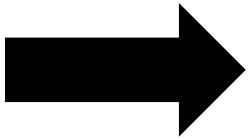
- 外部からの攻撃に備える！

ことも大事だが……

- 管理者自身が情報の重要性を認識すること！

そのために

- リスクの分析
- 徹底教育
- アクセス権者の指定



企業の努力次第！

全体の流れ

- セキュリティは攻撃対策？
- 事例から学ぶセキュリティ対策
- 今できること
- まとめ

Case1　メール誤送信による情報漏洩

- 被害状況

  お客様にサービスの案内するメールを送信した結果、受信者全員が他のお客様の氏名とメールアドレスが閲覧可能な状態になった

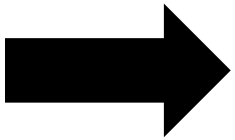
⇒「CC」「BCC」欄への入力の誤操作が原因

想定されるリスク

- 詐欺や迷惑メールがお客様に送信される
- メールアドレスリストを作成され、不正販売される
- 顧客流出

Case1　メール誤送信による情報漏洩

- 対応
  - メール送信先の特定
  - 陳謝及びメールアドレスの削除以来
  - 個人情報が含まれている場合、監督官庁に報告
  - ホームページに事故内容記載、記者発表など
  - 原因究明
  - 再発防止策の検討



業務が滞り、企業にとってマイナス

Case1　メール誤送信による情報漏洩

- 対策

①電子メール送受信のルールの徹底

・メール送信時に必ず上長をCcに入れる

・社外送信メールをサーバに保存、手動で確認

②電子メール誤送信防止システムを導入

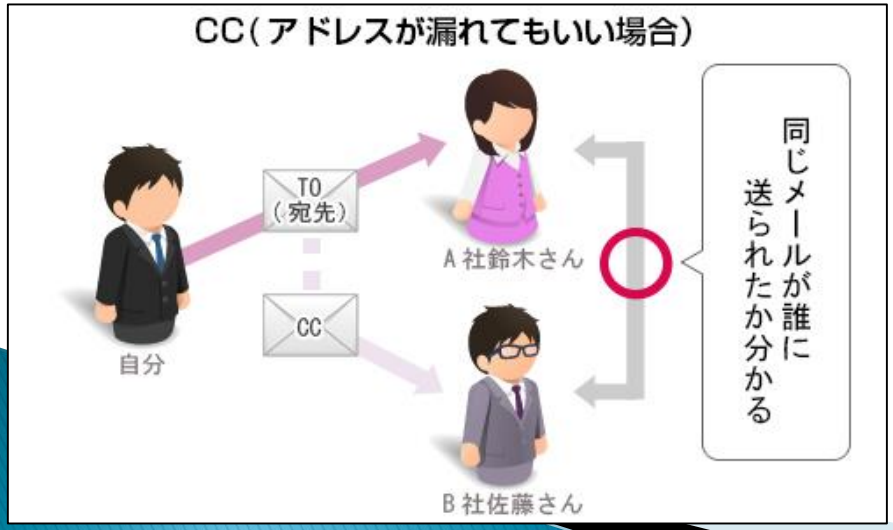
・外部送信する際に警告画面を出す

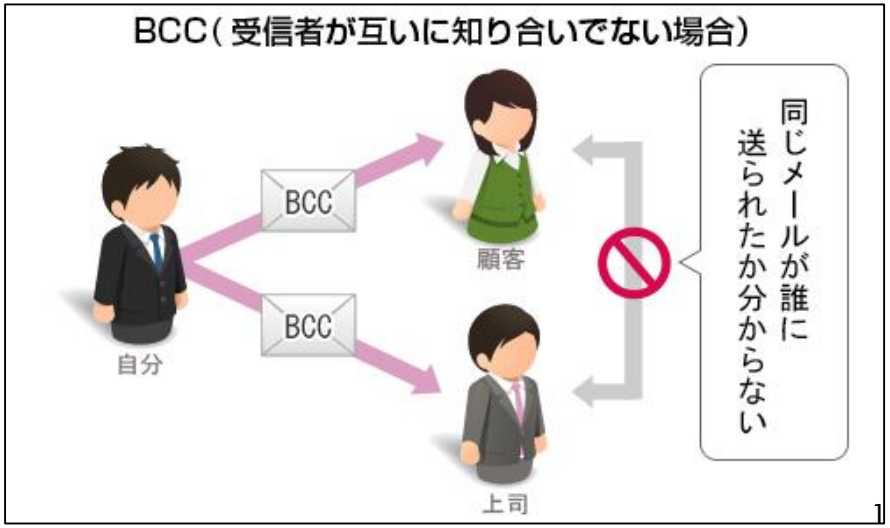
・送信にキャンセル機能を付ける

～Study～ 「CC」と「BCC」の違い

CC（Carbon Copy）・・・To（宛先）に指定した人と一緒にそのメールの内容を他の人にも知らせたい時や、同時に報告したい時に使う

BCC（Blind Carbon Copy）・・・ToやCC受信者に、他に受信者がいることを隠したい時や、面識が無い複数の相手に送りたい時に使う





Case2　車上荒らしで情報流出

- 被害状況

  社員が、個人情報が記載された重要書類を会社に無断で持ち出したところ、車上荒らしに遭い重要書類の入った鞄が盗まれた

⇒住所、氏名、電話番号などの約1400人分の個人情報が流出

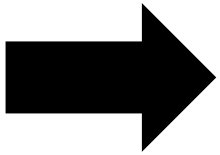
➡ 車上荒らしの犯人が悪い？

Case2　車上荒らしで情報流出

- 対応
  - 個人情報の該当者に謝罪文を送付
  - 不審な電話があれば市に連絡するよう要請

しかし…

会社には個人情報を外部に持ち出す時には
上司の許可が必要だと言うルールがあった

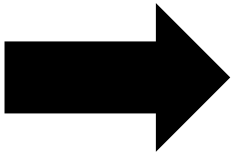


ルールを無視した社員が悪い？

Case2　車上荒らしで情報流出

- 対策
- セキュリティは人の教育から始まる！
  - ルールを作っても遵守意識が無ければ意味無し

⇒「車に鍵を掛ければ大丈夫」ではなく、
「窓を割って盗まれる危険があるかも」
という「想定外」を想定する訓練が必要



個人情報を持ち出す時の危機意識を持たせる教育が大事！

Case3　捨てたパソコンから情報漏洩

- 被害状況

  リース会社が小中学校にリースしていたパソコンを処分するため産廃業者に引き渡したところ、これらのパソコンから児童・生徒の写真や成績等の個人情報6000人分が流出した

⇒業者の保管状態が不適切だったことが原因

➡ 業者が全て悪いのか？

Case3　捨てたパソコンから情報漏洩

- 対応
  - 対象の児童・生徒にお詫びと説明
  - 問い合わせの窓口を設置
    - 流出した情報から児童・生徒に嫌がらせはないか
    - 自分が流出の対象者なのか
  - 他のリース返却パソコンの確認
    - パソコンの保存データを確認
    - データが読み込まないよう処理

Case3　捨てたパソコンから情報漏洩

- 対策

・ハードディスクを初期化
  - ゴミ箱やキーによる削除では不十分

・リース会社にデータの取り扱いを事前に確認

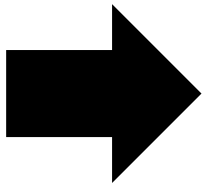
・セキュリティルールの徹底
  - チェックリストを設ける等

➡ データの完全消去で情報漏洩は防げた！

※キーによる削除とは、ここでは「Shift」+「Delete」を指します

～Study～　データの消去方式

- ゴミ箱に入れる
- ゴミ箱から削除（Shift＋Delete）



安全性無し

- ゼロフィル：HDD全領域に「00」を書き込む
- 標準方式：HDD全領域に乱数を1回書き込む
- NSA（米国家安全保障局）推奨方式：乱数→乱数→「00」の順に、HDD全領域に3回書き込む
- NATO標準（NATO規格）方式：「00」→「FF」→「00」→「FF」→「00」→「FF」→固定値の順に、HDD全領域に7回書き込む

Case4　誹謗中傷で信頼失墜

- 被害状況

スポーツ用品メーカーに勤務する社員が来店したプロサッカー選手と一緒にいた女性に対する中傷をTwitterに書き込み炎上

⇒企業名が特定され信頼の失墜に

⇒中傷した社員の本名、出身大学、顔写真まで突き止められ、掲示板に公開される事態に

⇒出身大学にも風評被害が発生

Case4　誹謗中傷で信頼失墜

- 対応
  - 勤務先の企業は選手及び所属チームに報告および謝罪
  - ホームページ上においても正式に謝罪
  - SNSで業務内容の投稿禁止を定めたルールの見直し
  - 中傷した社員を処分

それでも社員の個人情報はインターネットに残ったまま…

Case4　誹謗中傷で信頼失墜

- 対策
- 従業員の教育は不可欠
  - SNSを正しく使うことは自分を守ること
  - 自分の個人情報が漏洩するだけじゃない
    - 友人や同僚、出身校にも影響が及び、友人の個人情報までも特定されることもあり
  - インターネット上の書き込みは半永久的に残る
    - 書き込みの削除で無かったことにはできない

    ⇒魚拓が掲示板に貼られるなどして一気に広まる
- SNS利用のガイドラインを制定し周知徹底を行う

全体の流れ

- セキュリティは攻撃対策？
- 事例から学ぶセキュリティ対策
- 今できること
- まとめ

今からできるセキュリティ対策

- メールの添付ファイルは必ずウイルスチェック
- OSやウイルス対策ソフトの更新は忘れずに
- 勝手に利用できる無線LANは利用しない
- スマートフォンにパスコードロックを設定
- 位置情報サービスに注意
- 安易にURLを踏まない
- 掲示板の情報を安易に信じない
- 使用しないアプリは削除する

全体の流れ

- セキュリティは攻撃対策？
- 事例から学ぶセキュリティ対策
- 今できること
- まとめ

まとめ

- セキュリティ対策は教育から始まる
- 管理者が正しく作業を行えば8割以上の情報漏洩事件が減る
- 情報の重要性を認識し、常に危機意識を持つ
- セキュリティ対策は今からできる

ご静聴ありがとうございました