情報セキュリティと人間

情報社会とセキュリティ
2024 年度前期
佐賀大学理工学部 只木進一

情報漏洩などは内的要因が多い

- 重要情報を故意に持ち出し、売却する
  - 動機は?
- 重要情報を自宅に持ち帰る
  - 故意ではない場合が多い
  - 業務過多
  - 重要情報の扱いを意識していない
- 技術や法律だけでは防ぎきれない
- 心理、行動、倫理の側面の理解も必要

ソーシャルエンジニアリング: Social Engineering

- 人の心理・行動の特性を利用して、セキュリティ対策を無効化する行為全般
  - なりすまし: 他人になりすまして、電話、メールなどを使って、情報を取得する
  - ゴミ箱あさり: ゴミ箱から、書類、CD などを拾い、重要情報を取得する
  - 敷地・建物への侵入: 清掃業者、工事担当者、警備員などになりすまして、侵入する
  - のぞき見: 作業中の画面をのぞき見る
  - メーリングリスト、SNS 等の利用: 応答を見て、対象組織の技術力やセキュリティ対策レベルを知る

なりすまし: Impersonation

- システム管理者になりすまして、パスワードを聞く
- 公的機関の担当者になりすまして、口座番号を聞く
- 捜査関係者になりすまして、内部情報を取得する
- 過去のメールの相手になりすました攻撃例: Emotet
  https://www.ipa.go.jp/security/announce/20191202.html

なりすまし事例: 2023/6

- 名刺管理クラウドサービス
- サービス事業者になりすまし、ID とパスワードを窃取
  https://cybersecurity-info.com/news/leaked-business-cards-kawasaki-equipment-industry/

ビジネスメール詐欺

- 取引先になりすまし、偽口座へ送金
- 担当者になりすまし、企業の証明書を騙し取る
- 社長になりすまし、グループ企業の役員に企業買収資金を送金させる

https://www.ipa.go.jp/security/announce/2020-bec.html

ゴミ箱あさりへの対策

- 重要書類の処理: シュレッダー処理など
- CD や DVD 等の媒体: 専用のシュレッダー
- ディスク: 内容の消去、物理的破壊
- 神奈川県での情報漏えい事例
  https://www.pref.kanagawa.jp/docs/fz7/cnt/p0273317.html

敷地・建物への侵入への対策

- 管理区域の設定
  - 通常の執務室: 不在時の施錠、離席時の画面ロックなど
    - IC カード等を用いた端末のロック解除
  - ホストマシン室: ID カード等を用いた入退室管理、監視カメラ
    - 通常の鍵や記録簿で不十分な理由は?
  - 特に重要なデータのある部屋:
    - 生体認証等を用いた入退室管理
    - 監視カメラ
    - デジタルデバイスの持ち込み制限
- 名札、制服の着用

質問

情報系企業に限らず、大きな企業では職員全員が IC チップのついた ID カードを首から下げています。なぜでしょう。

内部からの流出例

- 2014/3: 東芝のパートナー企業の技術者が、転職先に企業秘密を持ち出し。転職を有利にすすめようとした動機。
- 2014/6: ベネッセのグループ企業の派遣エンジニアが、会員情報を売却。借金返済が動機。
- 2019/8: 平塚市議選挙に立候補した元市職員が、市民情報を持ち出し。有権者へのハガキ送付が動機。
- 2022/8: 島根県立中央病院で患者データ流失の疑い。端末修理時に、当該端末が行方不明。

2022/6: 尼崎市の事案

- 住民税非課税世帯等への臨時特別給付金対応業務のために全市民のデータの入った USB
- 再々委託先の職員が持ち帰り、途中で泥酔し、USB を紛失
- 再々委託は、市の許可を得ていなかった

https://www.city.amagasaki.hyogo.jp/kurashi/seikatusien/1027475/1030947.html

2024/6: 防衛省

- 特定機密漏えい
- 機密情報の取り扱い範囲への理解不足
  https://www.mod.go.jp/j/press/news/2024/04/26b.html

故意の情報漏洩の動機

- 組織への不満: 待遇、評価
- 金銭的見返り
- 転職先での活用

https://www.ipa.go.jp/files/000059582.pdf
「組織における内部不正とその対策」(IPA)

故意ではない情報漏えいの原因

- 多忙による、情報の自宅への持ち帰り
- 情報の取り扱いへの意識欠如
- 個人情報持ち帰り事例
  - 2018/7: 三重県
  - 2022/5: 岩手県釜石市
  - 2022/9: 徳島県牟岐町

内部からの情報漏洩を防ぐには

- 物理的制限を含むアクセス制限
- ID の棚卸し: 権限の無い者の ID を削除
- 周辺機器の使用制限: データ持出の抑制
- 教育
- 職員へのケア

行動に影響を及ぼす6つの要素: R. B. Cialdiniによる研究

- 返報性: 好意に応えたい
- 一貫性: 自分の行動に一貫性を持たせたい
- 社会的証明: 他の人と同じ行動をとる
- 好意: 親しい人からの提案や推薦を信じる
- 権威: 権威あると思える情報を信頼する
- 希少性: 少ないと価値があると思う

Heinrich の法則

- 一つの重症以上の災害の裏に
  - 29 件の軽症の災害
  - 300 件の「ひやり」「はっと」
- 「ひやり」「はっと」の分析と防止が重要
- 例えば
  - SMS を使ったフィッシングメールの多発 ⇒ 被害者が発生?
  - USB を使った情報持ち出し案件増加 ⇒USB 使用の規制が必要

割れ窓理論

- 一つの割れ窓を放置すると、他のガラスも割られてしまう
- 綻びを放置すると、被害が大きくなる
- 例えば
  - FW 設定に漏れがあり、不正侵入を受ける ⇒ 他にも侵入されている?
  - malware を持っている PC を放置 ⇒malware 感染が広がる

情報リテラシの重要性

- 情報機器の適切な操作
- 情報メディアとの適切な付き合い方
- デジタル情報の特性の理解
- 危険性の理解
- 適切な対策

情報資産を守るためのサイクル

- PDCA サイクル
  - Plan: 情報資産の洗い出し、リスク評価を通じて、対策計画を策定する
  - Do: 対策計画を実行する
  - Check: 対策計画の効果を計測し、目標達成度を評価する
  - Act: 評価結果を次の計画に反映する

政府機関等のサイバーセキュリティ対策のための統一基準（令和５年度版）

2.4.1 情報セキュリティ対策の見直し

情報セキュリティを取り巻く環境は常時変化しており、こうした変化に的確に対応しないと、情報セキュリティ水準を維持できなくなる。このため、機関等の情報セキュリティ対策の根幹をなす情報セキュリティ関係規程は、実際の運用において生じた課題、自己点検・監査等の結果や情報セキュリティに係る重大な変化等を踏まえ、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び顕在時の損失等を分析し、リスクを評価し、適時見直しを行う必要がある。
また、情報セキュリティに係る取組をより一層推進するためには、上記のリスク評価の結果を対策基準及び対策推進計画に反映することも重要である

内部統制

- 業務の有効性と効率性を高める
- 財務報告の信頼性を高める
- 法令遵守
- 資産の保全

内部統制の基本的要素

- 統制環境: 組織の気風を決定し、構成員に統制への意識付けや統制活動への協力などに影響する基盤
- リスクの評価と対応: 組織の目標達成に影響する事象について、リスクとしての識別、分析、評価。
- 統制活動: トップの命令・指示が適切に実行されるための方針・手続き
- 情報と伝達: 必要な情報が識別・把握され、関係者に正しく伝えられる
- モニタリング: 内部統制が機能していることを継続的に評価するプロセス

組織活動と情報セキュリティの課題

- 個々の対策の積み上げとして始まったため、組織的対応が遅れがち
- 情報セキュリティの投資効果が見えない
- 個々の対策の必要性が分かりにくい
- 経営者が情報セキュリティリスクを把握・理解することが困難
- 的確なリスク判断が困難
- 情報セキュリティ対策の全体最適化が困難

課題

組織が業務を外部へ委託する際に、再委託、再々委託などが発生すると、情報セキュリティ上のリスクが発生します。なぜでしょうか。