情報セキュリティ概論8
リスクマネジメント

帝塚山学院大学情報メディア学科教授/ICTセンター長
大阪市立大学名誉教授

中野秀男[検索]

今日の話

- ITサービスのセキュリティ対策
- リスクマネジメントの手順と考え方
  - 事故を発生させないための対策
  - 事故の影響を最小にするための対策
  - リスクの受容レベルを設定する
  - SLA策定への活用
  - 対策検討への4つの視点
  - 対策が実施されていることを保証する
  - リスクマネジメントの相関
  - PDCAサイクルを活用した対策の改善
- 脅威と脆弱性
- 参考図書

ITサービスのセキュリティ対策

- ITサービス事業者にとってのセキュリティ対策
  - クラウドサービスを対象にした本を参考にしたため
- 事故をゼロにするのはIT分野では難しい
  - 技術者としてはゼロにしたい
  - しかし技術の進歩が速い、扱う範囲が広すぎる
- 事故発生時の損失を最小にする
- リスクマネジメント
  - 事故をなるべく発生させないようにする
  - 事故が起こった場合の損失を最小にする

事故を発生させないための対策

- リスクの要因は「脅威」と「脆弱性」
- 「脆弱性」は管理下にあるが、「脅威」はほぼ外部
- 発生することが予想または起こった事象「インシデント」
- 脅威と脆弱性が合致してインシデントができる
- 対策は「脆弱性」にするのが効率的
- 事故の発生に関するリスクアセスメント
  - インターネットなどで脅威情報を収集
  - 収集した脅威に対する脆弱性を洗い出す
  - 洗い出した脆弱性が自組織で起こるか判断

事故の影響を最小にするための対策

- 事故の発生をゼロにするのは難しい
  - 技術的に、費用的に
- コストパーフォマンスに合わないものは対策しない
  - 技術者からすると辛いけど、経営的には正しい
- リスク受容レベル
  - 受け入れることのできる損失のレベル
  - 損失
    - サービスの停止だけであく顧客対応、企業の評判
- 機密性：情報を見られたり盗まれた場合の損失
- 完全性：改ざんなどによる影響
- 可用性：サービス停止やパーフォマンス不足による影響

リスクの受容レベルを設定する

- 「予防」や「検知」を組み合わせた「階層防御」
- 予防：事故が起こらないための対策
- 検知：事故の発生に気付くための対策
- 例：ホームページの改ざん
  - 予防：
    - 関係ソフトウェアを最新バージョンに
    - 最新セキュリティパッチの適用
  - 検知
    - アクセスログからの異常発見
  - 影響：利用者にウィルスが。フィッシングサイトへのクリック
  - 受容レベル：改竄後回復または停止までの時間
    - 利用者の利用頻度

SLA策定への活用

- 最大許容停止時間もSLA
  - Service Level Agreement
- SLA策定のための復旧手順策定シート
  - フェーズ
    - 発見
    - 報告
    - 封じ込め
    - 影響判断
    - 復旧
    - 回復
  - フェーズのそれぞれに
    - 作業内容、持続期間、作業時間、担当者

対策検討への4つの視点

- 1.リスク評価の結果、そのリスクを受容すると判断
  - 例：個人所有のスマホの紛失、持ち出さないPCの暗号化
- 2.リスク受容できないので、脆弱性、損失を軽減の対策
- 3.自社では対応できないので、誰かに任せる
  - アウトソース、保険
- 4.リスク回避できないので、ビジネスやサービス停止
  - USBメモリの利用禁止、PCの持ち出し禁止、BYOD禁止

対策が実施されていることを保証する

- 「しないこと」のルールから
- 「すること」のルールへ
- ルールも明快に
- 例：パスワード
  - 「パスワードを破られないこと」
  - 「複雑なパスワードにすること」
  - 複雑なパスワードの定義やルールを策定
  - 定義やルールの作成が受容レベルを作ったことになる
    - それで破られたら仕方がないという受容レベル
    - 破られた場合の速やかな処置体制

リスクマネジメントの相関

- 事故の発生：脅威 x 脆弱性(対策)
  - ↓
- 事故の影響：機密性、完全性、可用性 ⇄ 対策
  - ↓
- 受容：受容レベル
- リスクマネジメントの3つの指標
  - コスト
  - 影響
  - リスク
- 参考図書の図1.2

PDCAサイクルを活用した対策の改善

- PDCAサイクル
  - P(計画): Plan
  - D(実施): Do
  - C(点検): Check
  - A(改善): Act
- ルール策定も数値化して点検できること
  - 例：パスワード
    - 複雑なパスワードなく具体的に何文字以上とか内容とかAgingとか
    - 実際に守られているかチェック
    - ITの進化によるパスワードのルールの見直し

脅威

- IPAの2015年10大脅威
  - https://www.ipa.go.jp/files/000044680.pdf
  - 1.インターネットバンキングやクレジットカードの不正利用
  - 2.内部不正により情報漏洩
  - 3.標的型攻撃による諜報活動
  - 4.ウェブサービスへの不正ログイン
  - 5.ウェブサービスからの顧客情報の窃取
  - 6.ハッカー集団によるサイバーテロ
  - 7.ウェブサイトの改ざん
  - 8.インターネット基盤技術を悪用した攻撃
  - 9.脆弱性公表に伴う攻撃
  - 10.悪意のあるスマートフォンアプリ

脆弱性

- MicrosoftのTechNet
  - https://technet.microsoft.com/ja-jp/library/gg983510.aspx
- 総務省の＠脆弱性とは」
  - http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/basic/risk/11.html
- IPAの脆弱性対策
  - http://www.ipa.go.jp/security/vuln/

参考にした本

- 「クラウドセキュリティ：クラウド活用のためのリスクマネジメント入門」河野省二他
  - 翔泳社, 2014年5月