講演②
「非営利組織の情報セキュリティ対策」

認定NPO法人イーパーツ
東京電機大サイバーセキュリティ研究所 研究員
千葉大・成蹊大非常勤講師
会田和弘

1

1. この対策は「？」

2

1. この対策は「？」

講座でわかった「？」な対策

(1) メールで機密情報を送る時は、まず機密ファイルを暗号化し、次のメールでパスワードを送る。

3

1. この対策は「？」

講座でわかった「？」な対策（続き）

(2) パスワードは、ノートに書き留めてはいけない
(3) パスワードは、使い回しが便利だ
(4) パスワードは、こまめに更新が必要
(5) PCは、インターネットには接続しないで使用するのが一番安心等

現状にあわない対策がとられている場合もあるのかも？

4

1. この対策は「？」

テレワークは、時間や場所の制限をうけにくい活動を可能とする魅力的なもの。どのような対策が必要なのか？

– まずは、PCの使い方、情報の保護の仕方のルールから

テレワークで特に注意すべきルール

安全なクラウドサービスの選び方のルール

PCの使い方、情報の保護の仕方についてのルール

5

5

ヒアリングでわかった

2 非営利組織の「５つの困りごと」から対策を試みる

6

6

2. 非営利組織の５つ困りごと①

①私たちに関係あるの？

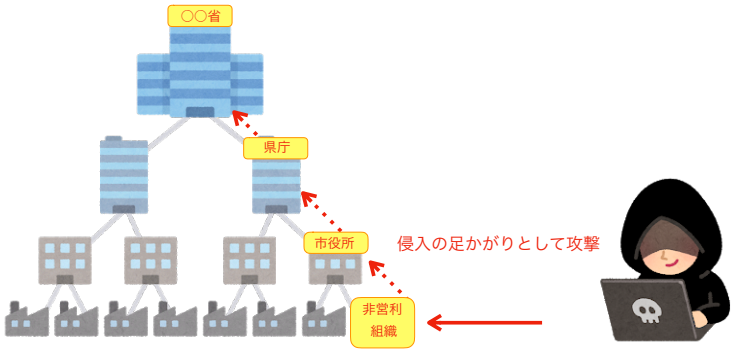
- 報道などで、ウイルス感染などは知っている。
- 怖いなとは思う。気をつけなければならないと思っている。
- でも、どこか遠い所の話、狙われているという実感はあまりない。
- このままではダメなのだろうか？

7

7

2. 非営利組織の５つの困りごと

- 状況は変わってきています。大企業や行政だけではなく、中小企業も狙われはじめています。



8

8

2. 非営利組織の５つの困りごと②

②何をやればいいの？

- アップデートの実施やウイルス対策ソフトは導入している
- それだけでいいの？、他にできることはあるのか？、不安
- 扱いを間違えると大変なことになるのでは？
- やるべきことをリスト化してほしい

2. 非営利組織の５つの困りごと②

- まずは、団体のセキュリティレベルを診断してみましょう

-IPA「新 5分でできる！　情報セキュリティ自社診断」

https://www.ipa.go.jp/files/000055848.pdf

2. 非営利組織の５つの困りごと②

- 解説をよみ、団体の運用ルールにくわえましょう。

診断編　NO.3　パスワード管理

強固なパスワードを使用する

解説

パスワードが推測や解析されたり、ウェブサービスから流出した ID・パスワードが悪用されたりすることで、不正にログインされる被害が増えています。パスワードは「長く」、「複雑に」、「使い回さない」ようにして強化しましょう。

全25項目、下記の三種類がある
・全員が実施すべき基本的対策
・スタッフが守るべき対策
・組織としてやるべき対策

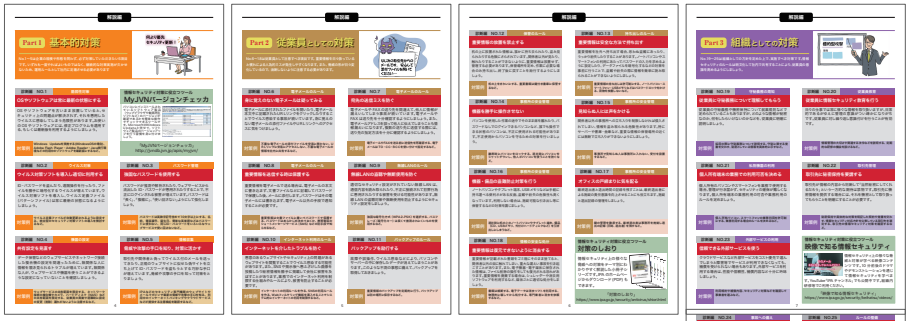
対策例　パスワードは英数字記号含めて10文字以上にする、名前、電話番号、誕生日、簡単な英単語などはパスワードに使わない、同じID・パスワードをいろいろなウェブサービスで使い回さないなど。

自分の組織に合わせて変更

IPA「新 5分でできる！　情報セキュリティ自社診断」

https://www.ipa.go.jp/files/000055848.pdf

2. 非営利組織の５つの困りごと②

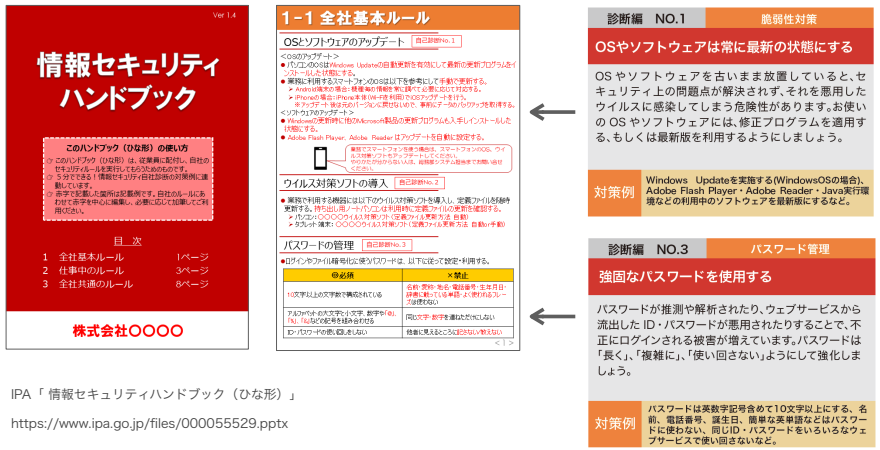


- 前提条件

■経営者（代表者）が対策方針を直接指示・確認することができる
■従業員全員が顔見知りである
■複雑な設定を必要とするサーバーやネットワーク機器を自社所有していない
・電子メールやのホームページは外部サービスを利用するなどのように、インターネットに直接接続しているサーバーを自社所有していない
・市販のアプリケーションソフトだけを利用しているなどのように、自社で独自に開発したアプリケーションソフトはない

2. 非営利組織の５つの困りごと②

- ルールをまとめやすくする雛形もある。



IPA「 情報セキュリティハンドブック（ひな形）」

https://www.ipa.go.jp/files/000055529.pptx

2 非営利組織の５つの困りごと③

③私物のPCでの活動は

- 団体のPCは限られていて、個人使用のPCを使うしかない
- 外部の人に作業をお願いする場合、どうしたらいいのか

2 非営利組織の５つの困りごと③

- 技術的な対策を施すだけではなく、保護の必要性を理解してもらうことが必要。
- ルールの一例
  - –守秘義務・機密保護の必要性を理解してもらうような教育を行う。
  - –どのような情報が秘密なのか、何をしたらいけないのかなどを明確に説明する。
  - –個人所有のPCを無断で業務に使用してはいけない。
  - –個人所有のPCを事務所内のネットワークに接続してはならない。
  - –個人使用のメールアドレスに、業務用メールアドレスで受診したメールを転送してはならない。
  - –業務終了後は、業務データを、組織が指定する専用ツールで削除する。

2 非営利組織の５つの困りごと④

④スタッフ研修はどうしたらいい？

- スタッフ全体のスキルを底上げしないと、私にはできない
- 機会、教える人材、資金がない！
- スタッフが一堂に集まることはないので、講座は非効率…
- ついつい他の業務が優先

2 非営利組織の５つの困りごと④

- オンラインで学習できる教材が多く公開されている。
  - –先に紹介した「新 5分でできる！　情報セキュリティ自社診断」の各項目を学習できるビデオが公開されている。自分のペースで学習できる。
  - –https://security-shien.ipa.go.jp/eLearning/user/frameset.cfm

17

17

2 非営利組織の５つの困りごと④

- オンラインで学習できる教材が多く公開されている。
  - –最近、多くの被害がでている標的型攻撃などについての啓発用動画
    - –映像で知る情報セキュリティ ～映像コンテンツ一覧～
      https://www.ipa.go.jp/security/keihatsu/videos/index.html

	内容	再生時間	公開日
ウイルス・サイバー攻撃対策			
1	組織の情報資産を守れ！ -標的型サイバー攻撃に備えたマネジメント- 組織の情報資産を守るためには経営者のリーダーシップによって対策を進める必要があります。本映像では経営者の視点で標的型サイバー攻撃に備えた組織マネジメントのポイントを説明します。 (詳しい説明へ)	約10分	2016/03/31
2	見えざるサイバー攻撃 -標的型サイバー攻撃の組織的な対策- 標的型サイバー攻撃で組織的な対応ができなかったケースの再現ドラマを通じて、標的型サイバー攻撃の組織的な対策のポイントを説明します。 (詳しい説明へ)	約13分	2017/04/03
3	そのメール本当に信用してもいいんですか？ -標的型サイバー攻撃メールの手口と対策- 企業内の標的型攻撃メールの訓練を舞台に、ウイルスが含まれている添付ファイルを開かせる標的型標的型サイバー攻撃メールの手口を示し、その対策を説明します。 (詳しい説明へ)	約10分	2016/03/31

18

18

2 非営利組織の５つの困りごと⑤

⑤誰にきいたらいいの？

- PCのことを教えてくる人はそこそこいるが、セキュリティについては…
- 何かあった時に相談できる人は？

19

19

2 非営利組織の５つの困りごと⑤

- セキュリティについての情報の多くはWebで公開されている。
  - –特に次が信頼性が高い
    - ‣ここからセキュリティ
      https://www.ipa.go.jp/security/kokokara/
    - ‣独立行政法人情報処理推進機構（IPA）「重要なセキュリティ情報」
      https://www.ipa.go.jp/security/
    - ‣Japan Vulnerability Notes（JVN）「脆弱性対策情報ポータルサイト」
      https://jvn.jp/
    - ‣一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC）
      https://www.jpcert.or.jp/

20

20

2 非営利組織の５つの困りごと⑤

- 電話やメールで相談に乗ってくれる窓口
  - IPA　「情報セキュリティ安心相談窓口」

    https://www.ipa.go.jp/security/anshin/index.html

3. 本日の資料とさらに学ぶために

- IPA 「中小企業の情報セキュリティ対策ガイドライン」
  - https://www.ipa.go.jp/security/keihatsu/sme/guideline/
  - 特に参考になるのが
    - 「５分でできる！情報セキュリティ自社診断」
      - https://www.ipa.go.jp/files/000055848.pdf
    - 「情報セキュリティハンドブック（ひな形）」
      - https://www.ipa.go.jp/files/000055529.pptx
    - 「クラウドサービス安全利用の手引き」
      - https://www.ipa.go.jp/files/000072150.pdf
  - さらに、学ぶために
    - 「中小企業の情報セキュリティ対策ガイドライン第3版」
      - https://www.ipa.go.jp/files/000055520.pdf