利用者目線の
企業セキュリティ

会津大学 阿部 泰裕
<yasu-abe@u-aizu.ac.jp>

講義の目標

企業が心掛けるべき情報セキュリティ対策の重点について説明する

企業におけるセキュリティ対策のポイント

- 技術を活用しながら、関係者の全体意識を高めていくことが大切

- セキュリティ対策の専門組織だけでは、具体的な対策は十分にできない

社会全体のセキュリティ意識を高めることにつながる

自分たちには関係のない話ではないか…

- 規模の大きな事業体や、工場など取引先からの求めに応じて国際規格に準拠している

1. 特殊な装置に使われる制御用コンピュータは適切に対応できているでしょうか。
2. 社員のセキュリティ啓発教育は万全でしょうか。

- 使用しているのは通常のパソコン程度で、ウィルス対策ソフトなどは使用している。これで十分ではないか

1. NAS(ネットワーク接続型記憶装置)などに重要な情報は入っていないでしょうか。
2. それら機器への物理的に接触できないようになっているでしょうか。

最近の事案からみるポイント

- ネットワークにつながっているコンピュータから情報が共有できる

外部から侵入された場合には、共有している情報全てが窃取される可能性がある

- 外部からの侵入だけではありません。

内部犯行は非常に低い割合(※)だが、影響度が大きい

(※) 2015年で国内の個人情報漏えい・逸失事案の内、5.2%が内部犯行によるもの。JIPDEC、アイ・ティ・アール株式会社：企業 IT 利活用動向調査 2015

内部犯行と標的型攻撃による犯罪は似ている

標的型攻撃から守るためには

- あやしいメールでないか、常に確認する (手口を知る)
- OS・アプリケーションは常に最新版に保つ
- ウィルス対策ソフトの定義ファイルは常に最新にする

標的型攻撃のポイント

- 組織内部について詳しく調査している

事前調査のためのウィルス攻撃

ソーシャル
エンジニアリング

- 標的となる理由は様々

様々な信条

注目を集めるため

誤解によるもの

- ウィルスに感染した場合、内部の正常な操作と区別が難しい

内部犯行を想定した対策が求められる

企業の情報セキュリティ対応力を向上するために

情報セキュリティとは

- 情報セキュリティ

1. 情報の「機密性、完全性、可用性」 (CIA) を維持すること (JIS)
2. 利用者をCIAの欠如に起因する危害から守ること (OECD 1992年)

- 情報資産

活動の中で生み出される有形無形の価値のある情報(モノ)

- リスク管理

危険にあう可能性や損をする可能性(リスク)に対して備える活動

脅威の種類

悪意を持つ人間と、それ以外の脅威

人為的脅威

家族

知人

偶発的脅威

事故

誤動作

環境的脅威

地震

火事

事故、天災を想定する事も現実世界では重要

情報セキュリティ対策の難しさ

- 普段使わない用語・横文字・似た言葉

インシデント

ランサムウェア

ウィルス ⇔ マルウェア

アプリ　⇔　ソフトウェア

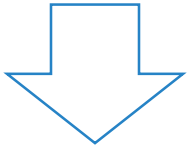
- 具体的に何をすれば良いか分からない。項目が多い

まずは対策を始めて、徐々に改善してゆく

情報セキュリティ対策の難しさ

電子データの特徴

- 電子データのコピーが(事実上)無限にできる
- 電子データのコピーを防ぐ事が(とても)難しい
- 電子データがコピーされた事実を知る方法が(ほぼ)ない
- 電子データのコピーはネットワークを通じて広がる



現実世界では肌感覚で分かるかもしれない変化が水面下で進行

情報セキュリティの基本

- 守るべき**情報資産**を確認する

最初から漏れなく洗い出す事は難しい

- それぞれの情報(グループ)毎のリスク・対策を検討する
- 繰り返し、情報資産の洗い出し、リスク対策を確認
- 事業の継続性を確保するための取り組みとの関連

事業継続計画(BCP)と情報セキュリティ

事業継続管理 (JIS X 5080, ISO/IEC17799:2000 現在廃止)

- 災害及びセキュリティ障害（例えば…，**事故，装置の故障及び悪意による行為の結果による中断**）を，…許容可能なレベルにまで抑えるために，事業継続管理手続を実施することが望ましい。

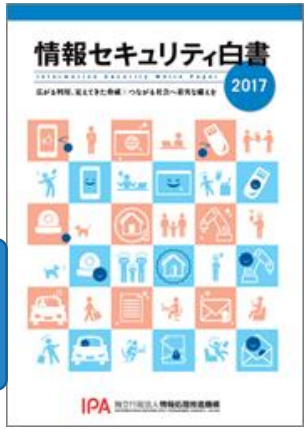
- 国際規格は、2005年・2013年に改訂され、経済産業省が2016年3月に「情報セキュリティ管理基準（平成28年改正版）」を策定

※ 情報セキュリティ管理基準（平成28年改正版）
http://www.meti.go.jp/press/2015/03/20160301001/20160301001.html

組織全体を強くする観点から、対応に取り組む

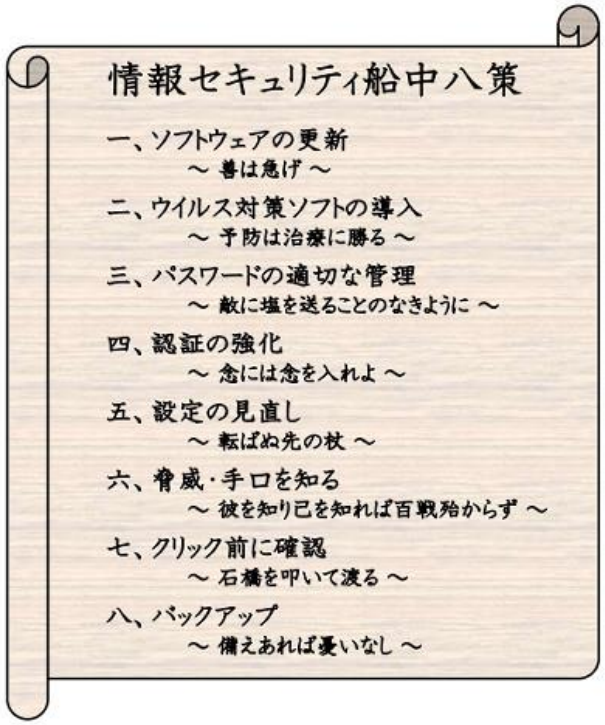
情報セキュリティ強化に向けた確認項目

最新情報の確認
IPA 情報セキュリティ白書2017



一般的な情報セキュリティ対策

1. ソフトウェアの更新
2. ウィルス対策ソフトの導入
3. パスワードの適切な管理
4. 認証の強化
5. 設定の見直し
6. 脅威・手口を知る
7. クリック前に確認
8. バックアップ



※ IPA セキュリティ10大脅威2015　"付録:情報セキュリティ船中八策"
https://www.ipa.go.jp/files/000044680.pdf

二. ウィルス対策ソフトの導入

- 多数ある対策ソフトから何を導入するか
  - iPhone, iPad, iPod touchでは対策ソフトは許可されていない
  - Appleモバイル製品では、Jailbreak(脱獄)をしない、公式ストアからのアプリ導入が基本

- 基本的には何(どの製品)を導入するかよりも、定期的にアプリやパターンファイルを最新に更新しているかどうかが大切

- ウィルス対策ソフトでは、良く知られている攻撃パターンを防ぐ事ができるのが共通の特徴

過去には、以下のような情報が発信され、誤解を生んでいる
- 「Appleの製品は安全なのでウィルス対策ソフトは不要です」
- 「大事な情報は入っていないので、対策ソフトは導入しない」

三. パスワードの適切な管理

1. パスワードは常に違うものを利用する
   - Google, Yahooなどのセキュリティは強固で、直接IDやパスワードを窃取する事は難しい
   - 同じパスワードをセキュリティの脆弱なWebサイト(例:小規模商店の通販サイト)等で使用すると、犯罪者が入手しやすくなる
   - 結果、弱いところからID(通常はメールアドレス)とパスワードが漏洩して、Google, Yahooなどのサイトでもなりすましが発生する可能性がある

2. 2段階認証の利用 (利用できる会社は限られる)
   - パスワードと携帯ショートメール(SMS)の組み合せで、認証を行なう
   - ID・パスワードが漏洩しても、携帯を持っていないとSMSで届くパスワード(毎回異なる4桁の数字など)が分からず、ログインできない

可能であればパスワード以外の生体情報の併用も検討する

(続き) 三. パスワードの適切な管理

- パスワード管理方法の例 - **パスワード管理ソフト**を利用する
  - 暗号化をしてデータを保存 (**ファイルの窃取への対応**)
  - 暗号を解除するためのパスワードだけ覚える (**守るべきものを減らす**)
  - ランダムなパスワードを作る機能 (**考える手間の軽減**)
  - コピー&ペースト(切り貼り)機能 (**入力する手間を省き、盗み見を防止**)

- 弱点 - パスワード管理ソフトで防げない事、苦手な事
  - ウィルスの中にはキーボードの入力を盗み取るものがある
  - ウィルスの中には画面を盗みみるものがある
  - ソフトのセキュリティ突破されると、全てのパスワード情報が盗まれる可能性がある

六. 脅威・手口を知る

- 講座などで知る事ができる範囲は限定的
- 継続的に、IPA・経済産業省などの啓発資料を確認する
- 国民生活センターでも最新の手口が確認できる

組織の中にある守るべき情報を把握しているのは現場の方々です。

情報セキュリティに関するニュースなどを取り上げて、自分たちの組織だったら、どう対応するか、防衛手段は十分か、議論をして取り入れてください。

八. バックアップ (事故への備え)

- バックアップは、万が一にそなえる保険
- しかし想像を越えた場合(社屋全体が失なわれてしまう)には、対応できない場合がある

- 本当に大事な情報を守るために、適切な想定をしましょう！

1. IT機器(パソコン等)が盗難・壊れる場合を想定
   - バックアップを同じ機器に保存していると、同時に失なう場合がある
2. 災害(火事など)の場合を想定
   - バックアップを遠隔地に保管しなければいけない場合がある
3. 復旧に使える時間を想定し、実際に復旧してみる
   - 事前に確認をして、問題がある場合は代替案を探す

情報セキュリティ強化に向けた確認項目

- 一般的な情報セキュリティ対策をまず全社員対象に徹底する
- 組織に必要な情報を把握しているのは現場
- 定期・不定期にセキュリティに対する備えを確認する
- 既知の脅威・手法について、自組織に当てはめて議論する

担当者や担当組織を割り当てて、安心しないこと

まとめ ～ 利用者目線の企業セキュリティ

1. 自社の保有するデータを確認する
2. 情報毎のリスク・対策を検討する
3. 過去の事案から、自組織で同様の事象が発生した想定で、対策を検討しておく
4. 現在の対策が十分か見直し、(1,2,3)を繰り返し行なう

お客様・関係者への影響を最小限にする考え方が、
自組織を強くし、信頼を得ることにつながります

参考資料

スマートフォン乗っ取りのポイント

- アプリケーションを導入させようとする
- 公式サイト以外からアプリケーションをダウンロードしない
- 人間の欲求を利用した詐欺的な手法で、アプリケーションを導入させる事例もある
- ランサムウェアの中には対策が容易なものもあるため、似た事例を検索したり、専門家に協力を求める

コンピュータ・ウィルスに関連する法律

- ウィルス作成、保管などの行為は禁止されています

コンピュータ・ウィルスの作成・提供罪は,
① 正当な理由がないのに,
② 無断で他人のコンピュータにおいて実行させる目的で,
コンピュータ・ウィルスを**作成，提供した場合**に成立するものです。

出典: 法務省 - いわゆるサイバー刑法に関するＱ＆Ａ
http://www.moj.go.jp/content/000073750.htm

- 作成・提供・供用
  ３年以下の懲役又は50万円以下の罰金

試験用のウィルスであっても、イタズラ目的で使用した際には罪に問われる可能性があります。

リスク・マネージメント(管理)の概要

リスク(脅威の可能性)の対応方法をまとめたもの