情報資産の取扱について

ーーーー自分の身を守るためにーーーー

2012/2/21　初版

大阪大学レーザーエネルギー学研究センター
高性能計算機室
http://www.ile.osaka-u.ac.jp/research/cmp/

はじめに

昨今、新聞などで話題の標的型メール攻撃など、いわゆる「情報資産」を狙った犯罪なども増えてきています。一昔前、情報事故と言えば、紛失や誤操作を連想していましたが、今では、悪意と周到な手段を持って、気付かないうちにその「情報資産」が狙われることも想定しなければならない時代になっています。
今回のテキスト作成にあたっては、大阪大学情報推進部情報企画課主催の「情報セキュリティ研修」や下記のホームページを参考にさせていただきました。「情報資産」を取り巻く環境はめまぐるしく変化し続けています。下記のホームページなどから、最新の状況を常に把握することも重要です。

■ IPA　独立行政法人情報処理推進機構
http://www.ipa.go.jp/

■ 警視庁　情報セキュリティ広場
http://www.keishicho.metro.tokyo.jp/haiteku/

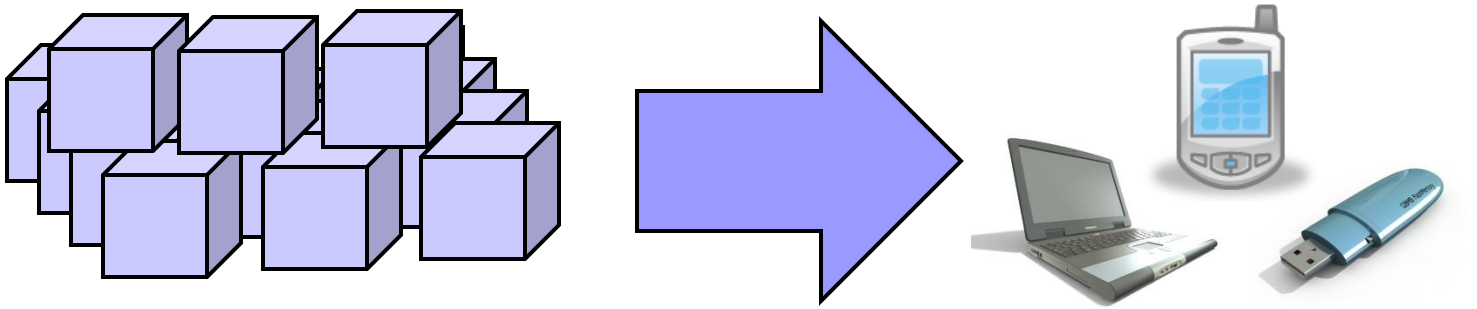
■ JPCERT　コーディネーションセンター
http://www.jpcert.or.jp/

■ 総務省　国民のための情報セキュリティサイト
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/index.htm

情報環境の変化

15年前と比べると･･･

15年前、1万人の個人情報を持ち出そうとすると･･･　　現在では･･･



段ボールで何箱分の情報も、現在ではパソコン1つ、もしくはUSBメモリ1つでラクラクと、
誰でも簡単に持ち出すことができます。

そういった手軽さ、汎用性は、情報セキュリティ上の脅威の対象となる範囲が拡大したともいえるでしょう。

- ◆パソコン、携帯電話、外部メモリ（USBメモリやDVD-R、スマートメモリ等）などの軽量化
- ◆OSやアプリケーションの共通化
- ◆メール、インターネット利用者の増加
- ◆新しい価値（ショップポイントや仮想世界通貨等）や新しいビジネスモデルなどの形態の変化

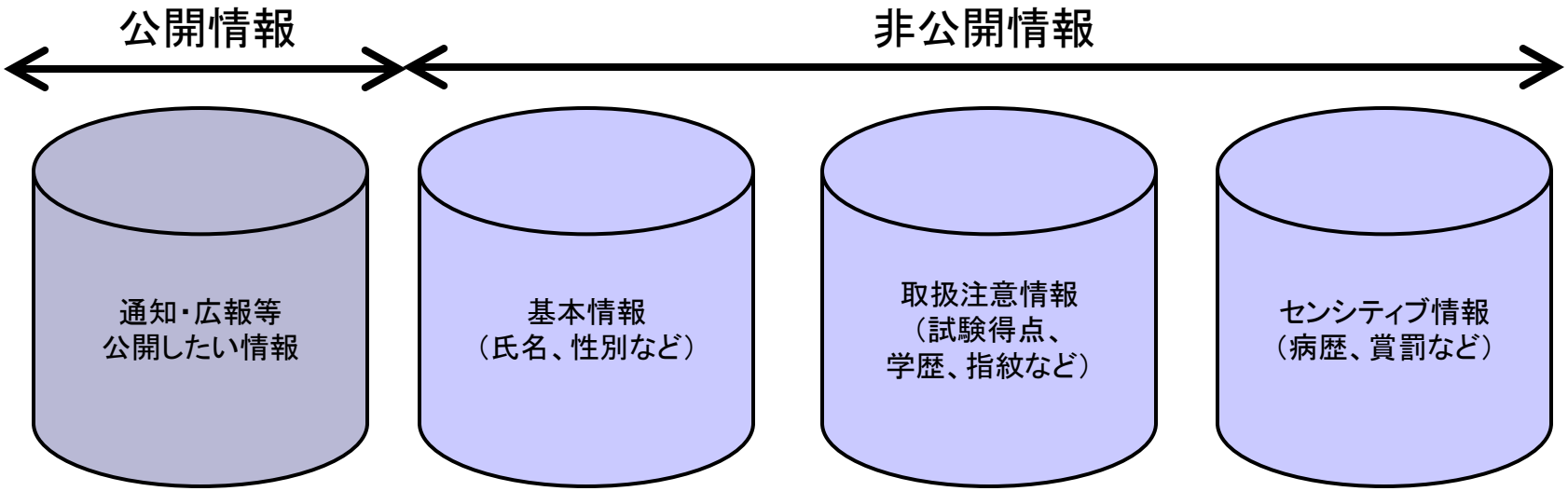
情報通信技術の発展や利用形態の変化により、将来の脅威予測が非常に難しい状況になり、
対象範囲を絞った意図的な攻撃（標的型メール等）が進行するなど、ウイルス感染や情報漏えいを
引き起こす手法が高度化、潜行化してきています。

守るべき情報資産とは・・・　「ひと」「もの」「かね」そして「情報」

「情報資産」とは、パソコンやネットワーク機器、ソフトウェアやデータなどの
「守るべき価値のある資産」のこと。

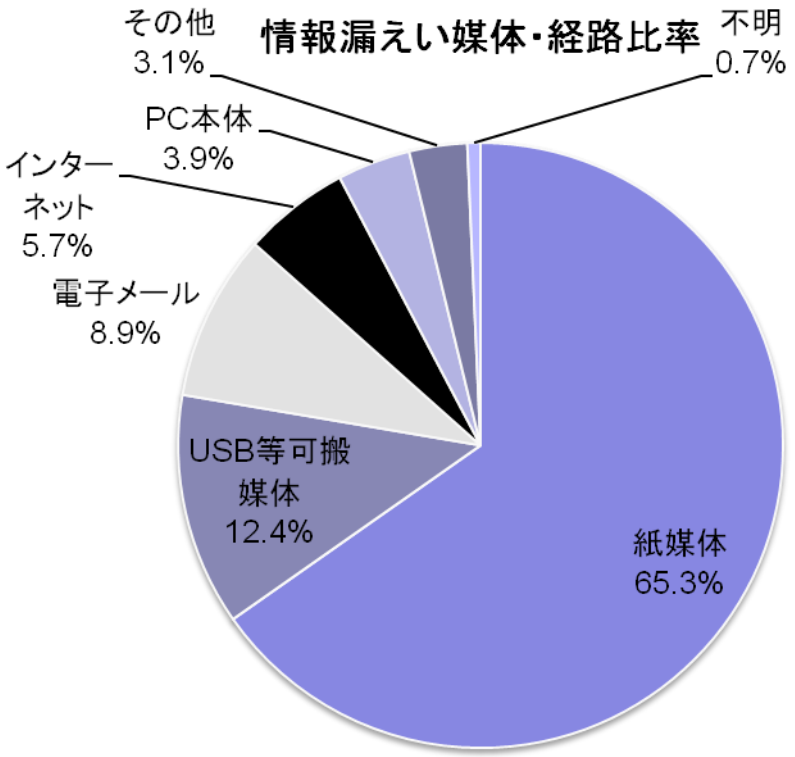
「情報」は極めて慎重に取り扱うべき情報から通知、公開したい情報まで内容は様々です。
「情報」というだけで、すべてが機密情報というわけではないはずです。
まずは「情報」を分類し、分類毎に保管場所を変えたりアクセス権を設定するなど、強弱をつける必要があります。

非公開情報をいかにして守るか！！



※情報分類のサンプルです　実際の基準は組織ごとに確認してください

情報漏えいの経路



日本ネットワークセキュリティ協会
『2010年情報セキュリティに関する調査報告書【上半期速報版】』より

実は情報漏えいの大半が、紙媒体から漏えいしている！

紙媒体は、組織外の他人の手に渡ったと同時に漏えいが発生します。

デジタル媒体の紛失や盗難事故がよく報じられていますが、データの暗号化やパスワード設定などの保護により情報漏えいを水際で防げているケースが多いのです。

この点で、紙媒体の紛失や盗難は、それ自体が情報漏えいにつながる可能性が高いといえます。

◆離席時には、重要情報が記載された用紙などがデスクに放置されたままの状態にならないよう、ファイリングを行う。
◆トラッシング（清掃員を装ってゴミ箱等から情報を収集する手口）に注意し、安易にゴミ箱に捨てない
◆重要情報を廃棄するときは、シュレッターを利用する

情報セキュリティ事故の実例

◆名簿等の個人情報が入ったパソコンが盗難される
◆教員が、氏名・試験の点数や連絡先などの個人情報が入ったUSBメモリを紛失する

置き忘れ、盗難のほか、車上荒らしなどのような「強奪」の事例も発生しています。
情報資産の取扱方については、“人の注意”を喚起するだけでは不十分であり、
仮に紛失や盗難に遭遇しても、情報が外部へ漏れないような対策が必要です。

例：データの暗号化、パスワードによる利用者認証など

強奪されても大丈夫な仕組みが必要！！

◆ファイル交換ソフトを媒介として、取扱注意情報がインターネット上に流出した
◆FTPソフトの操作を誤り、個人情報を公開フォルダに保存した

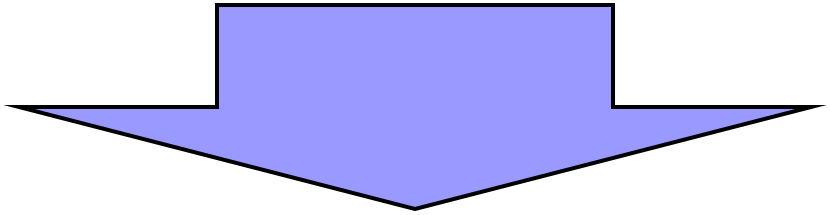
その他、電子メールの誤送信による情報漏えいも後を断ちません。
インターネットに接続されたコンピュータで重要情報を取り扱う際は、“重要情報”が
世界と結びつく可能性を認識しなければなりません。

例：宛先（TO、BCCの使い分け）や添付ファイルの再確認

情報セキュリティ確保の目的

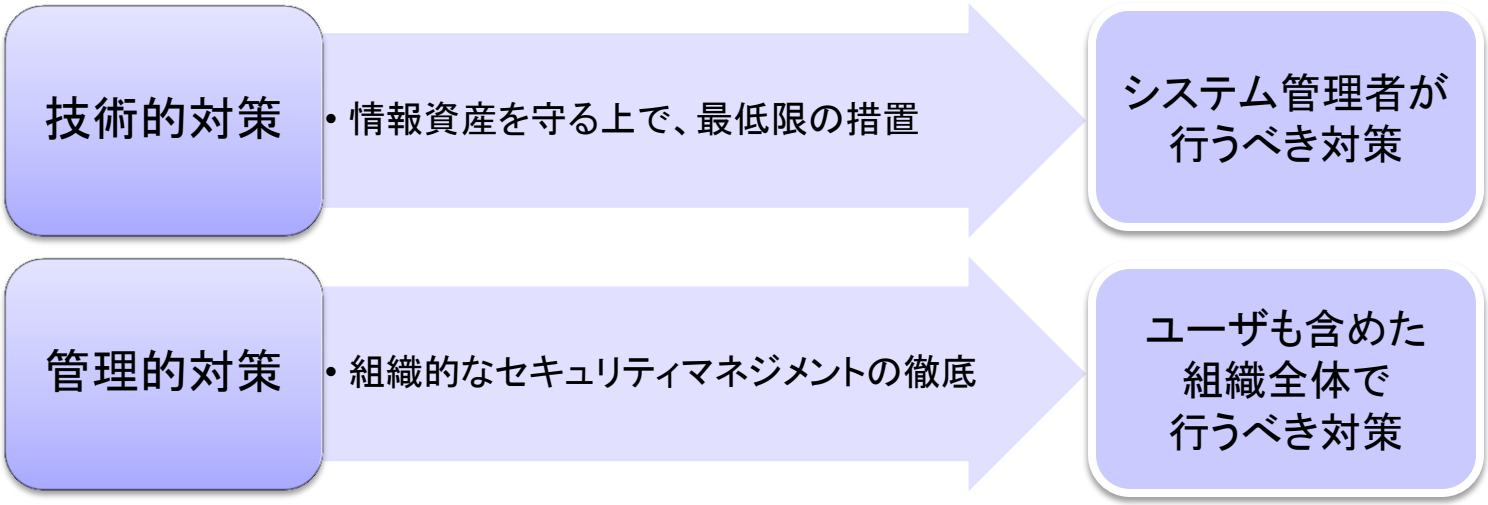
- 情報漏えい事故が起こると… **信用失墜！！**
  - ✓ 被害者の情報が悪用される
  - ✓ 果たすべき義務が果たされない→民法上の争議
  - ✓ 損害賠償支払い
  - ✓ 個人情報保護法による罰則
  - ✓ 裁判諸費用や業務回復に係る費用など…

- 収拾するのに手間、コストがかかる ⇔ 起こらなければ日常業務が行える



情報セキュリティに注力することは、本務とする活動の
妨げを回避し、自身および組織の活動をスムーズに
推進するために必要不可欠なものである

具体的対応策



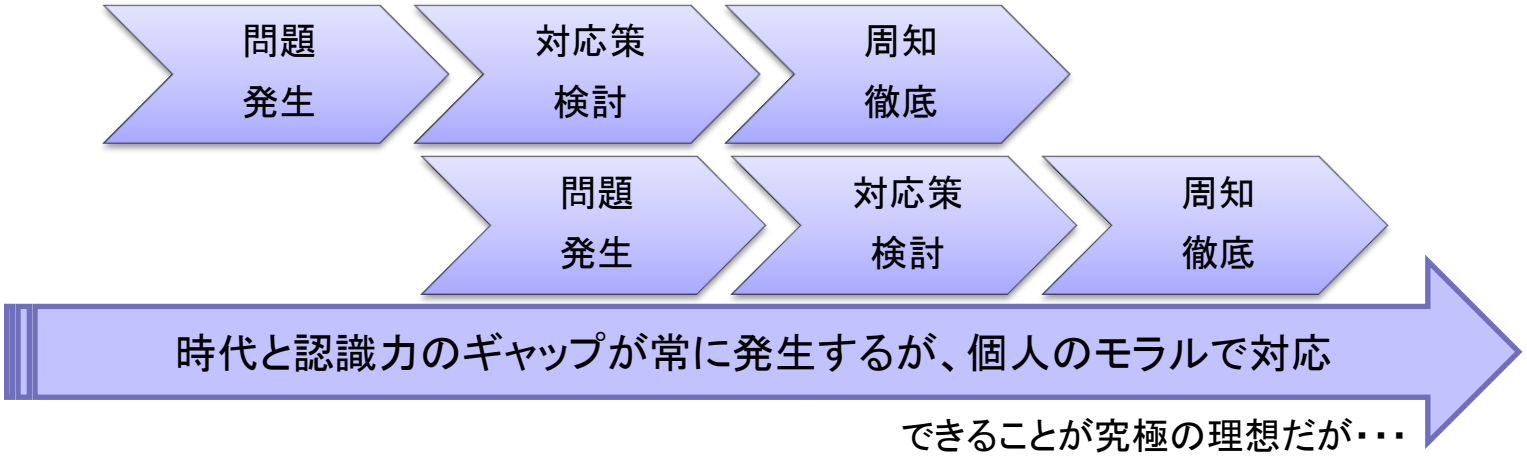
ファイアウォールなどネットワーク機器の導入や、HDDの暗号化など
システム管理者が行うべき環境づくり　⇒　技術的対策

安全管理措置の徹底など個人のモラル不足による事故を防ぐための
セキュリティマネジメント強化　⇒　マネジメント的対策

最近はこちらが重要視されています

各自の責任と自覚の重要性

- 情報環境を利用する上での原則
  - ✓ 何気ない情報の取り扱いミスが大きな被害を及ぼすことを認識する
  - ✓ 情報の価値、取扱い方法について、その情報を保有している組織や個人が正しく理解し、管理においては責任を問われることを認識する
- 普段からの自覚が重要
  - ✓ ルールが追いつかなくても自制できる知識と習慣
  - ✓ 刻々と変化する情報環境に追いつく努力も必要



情報セキュリティの意識、自覚を高める意味でも講習会は重要です

講習会は「人間ドック」「健康診断」のようなもの・・・？

受けるだけでは意味が無い、結果を見て悪いところは改め、普段から生活改善を心がけ、翌年の結果がよくなるよう努力工夫する必要があります。そして繰り返し継続しましょう。

情報の持ち出し・持ち込み時の留意点

PCやUSBメモリの持ち出し・持ち込みは必要最低限にしましょう
どうしても必要な際は、所属部署のルールに従いましょう

置き忘れや盗難、強奪が発生した場合のことを考慮し、情報漏えいしないよう
次のような対策を行うことが重要です。

- パソコンにBIOSパスワードを設定する
- パソコンにログオンパスワードを設定する
- 重要なデータは暗号化またはパスワードを設定
- ハードディスク全体を暗号化するツールの導入
- 暗号化機能付きUSBメモリなどを利用する

万が一、紛失（盗難）にあった場合に重要なのは、
被害にあった情報（内容）を正確に把握できているか
ということです。持ち出す際には、再度確認しましょう。

どの情報が、被害にあったのかわからないというのでは、被害の状況がつかめず、
対策の取り方が大きく変わってきます。

情報取扱いの留意点　その1

情報資産が紛失や持ち出しに遭遇しない環境を構築すること
不要となった情報資産は確実に破棄すること

- ノートPCなど可搬PCは盗難防止ワイヤなどで固定する
- 職場からの帰宅時に重要情報が記載された用紙などが
  机上に放置されたままの状態にならないようファイリングする
- 重要情報を記載した紙媒体はシュレッダー等で粉砕する
- 重要情報が1度でも記録されたデジタル媒体は、完全に
  情報が読み取れなくなるよう対策を講じた上で破棄する

ファイルへのアクセス管理（制限）を徹底すること
暗号化・パスワードの設定ルールやパスワード発行対象者の管理を行うこと

- 共有環境に保管されるファイルは、誰もが閲覧できることを認識する
- ファイルの利用者を制限する必要のある情報資産には、暗号化や
  パスワードを設定し、誰もが利用できない体制を構築する
- パスワードは定期的に変更する。そのルールの作成
- 異動により過去に所属していた職員のIDやパスワードを放置しない

情報取扱いの留意点　その2

重要なデータはバックアップを行いデータ保全を行うこと
バックアップのスケジュール管理や媒体管理を徹底すること

- 定期的（毎日、毎週、毎月）に行う
- 業務処理の終了時など効果的なスケジューリング
- 時間や費用を考慮して対象データが全て格納できる媒体を選択する
- 消失を防ぐため、正副の2つのバックアップを作成し、別場所に保管する

データの紛失や障害だけでなく、誤った操作による上書きやウイルスによる改ざんにも備える必要があります。

公共の場での会話からの情報漏えいなどにも注意を払うこと
情報の紛失や漏えいが発覚した際の報告先を全員が常時認識していること

- エレベータ内での会話や、飲食店（特に飲酒時）での会話は、関係者以外が聞いている可能性があることを認識する
- 職場外での業務情報の紛失や漏えいが発覚したら、まずは所定の連絡先へ連絡し状況報告を優先する。自分自身で状況回復を図ろうとしない
- 異動や役割の変更に伴い、組織体制は常に変化するため、常に緊急時の連絡先を認識しておく

情報を守るためのパスワード

パスワード管理の必要性
■情報資産へ適切な人がアクセスすることをコントロールするため
■組織が保有する情報資産を守るためのもの

理想のパスワードとは･･･
- •他人に予想されにくく、自分は覚えやすいもの
- •簡易なパスワードは使用しない
- •英字（大文字、小文字）、数字、記号を混在させる

パスワード保護の対策
- •パスワードは他人に教えない ← システム管理者でも！
- •紙や付箋に書き留めない
- •定期的に変更する ← クラック防止のため
- •いろんな場面で同じパスワードを設定しない ← 一つクラックされたら･･･？

盗まれた時の深刻度に応じたパスワード（長さ、難易度）を設定するのも一つの重要な手段です。

組織内の一人のパスワード漏えいが、組織全体の漏えいにつながる可能性も？
各個人のモラルと危機意識がとても重要です。

2011年10月に発覚した衆議院のネットワークがサイバー攻撃を受けた問題でも、標的型メールから全ての衆院議員と秘書のパスワードが盗まれ、メールの中身が盗み見されていた可能性があるとのことです。
こまめなパスワード変更をすれば、被害を最小で抑えられたかもしれません。

付録：パスワードクラックの危険性

情報処理推進機構Webページより引用

使用する文字の種類	使用可能文字数	最大解読時間			
		入力桁数			
		4桁	6桁	8桁	10桁
英字（大文字、小文字区別無）	26	約3秒	約37分	約17日	約32年
英字（大文字、小文字区別有）+数字	62	約2分	約5日	約50年	約20万年
英字（大文字、小文字区別有）+数字+記号	93	約9分	約54日	約1千年	約1千万年

※すべての組み合わせを試すために必要な時間を計算
記号は31文字使用できるものとした場合
使用パソコン：Windows Vista Business
Intel Core 2 Duo T7200 2.00GHz
メモリ：3GB

終わりに

あらゆるツールのIT化が進み、メールでの伝達や、インターネットやネットワークを利用した情報共有、保有する情報資産の活用が、身近で一般的になってきた一方で、その手軽さは、標的型メール攻撃に代表されるようなサイバー攻撃や、情報漏えいなど大きな危険性も併せ持っていることを私たちは認識せねばなりません。
日々進化するIT技術に対応するには、その進化に対応した最新の機械にお任せするのではなく、各人の情報セキュリティ対策に対するモラルが高い組織であることが根底になければ、最新の機械をもってしても、それらの大きな危険性から逃れることはできないかもしれません。
この「情報資産の取扱について」のテキストは、そういったコンセプトで作成されました。技術的な対策も大切ですが、組織が大きくなればなるほど、一人ひとりの危機意識やモラルがなければ、情報資産の安全は保てないと言っても過言ではありません。一年に一度は、人間ドックのように、身の回りの情報資産への危険性を今一度再確認する機会を持つべきだと考えました。
このテキストが情報資産の在り方、日常作業の見直しなどをするきっかけになれば、うれしく思います。

2012年2月21日　林　麗美

情報資産の取扱について

初版　　2012.2.21　　林　麗美

大阪大学レーザーエネルギー学研究センター
高性能計算機室
http://www.ile.osaka-u.ac.jp/research/cmp/