# ビジネスのための
# ＩＴ環境構築講座 ③

## リスク管理とIT環境
～安全にIT環境を維持するには～

# 本日の内容

- なぜリスク管理が必要なのか
- ところでリスク管理とは
- 無線LANの危険と安全対策（事例紹介）
- 電子メールの危険と安全対策（事例紹介）
- データバックアップと企業リスク（事例紹介）

# ●なぜリスク管理が必要なのか



- なぜリスク管理が必要なのか
- ところでリスク管理とは
- 無線LANの危険と安全対策（事例紹介）
- 電子メールの危険と安全対策（事例紹介）
- データバックアップと企業リスク（事例紹介）

# 経営者に聞きました

■なぜリスク管理が必要なのか

Q：ウィルス対策ソフトは導入していますか？

A：購入したときに〇〇が付属していたからね。

Q：故障を機に新しいパソコンを購入するのですね？

A：そろそろ交換と思っていたのでね。

Q：ところで、故障したパソコンの中に必要なデータがありますか？

A：もちろん。〇〇に、△△だ。

Q：〇〇と△△のバックアップはありますか？

A：バックアップ？　何それ？

本当かな？

それでいいのかな？

# 知らなかったでは済まない

■なぜリスク管理が必要なのか

先日、カラープリンターで両面コピーした千円札をショッピングセンターで使用し、中2女子が偽造通貨行使容疑で現行犯逮捕された。

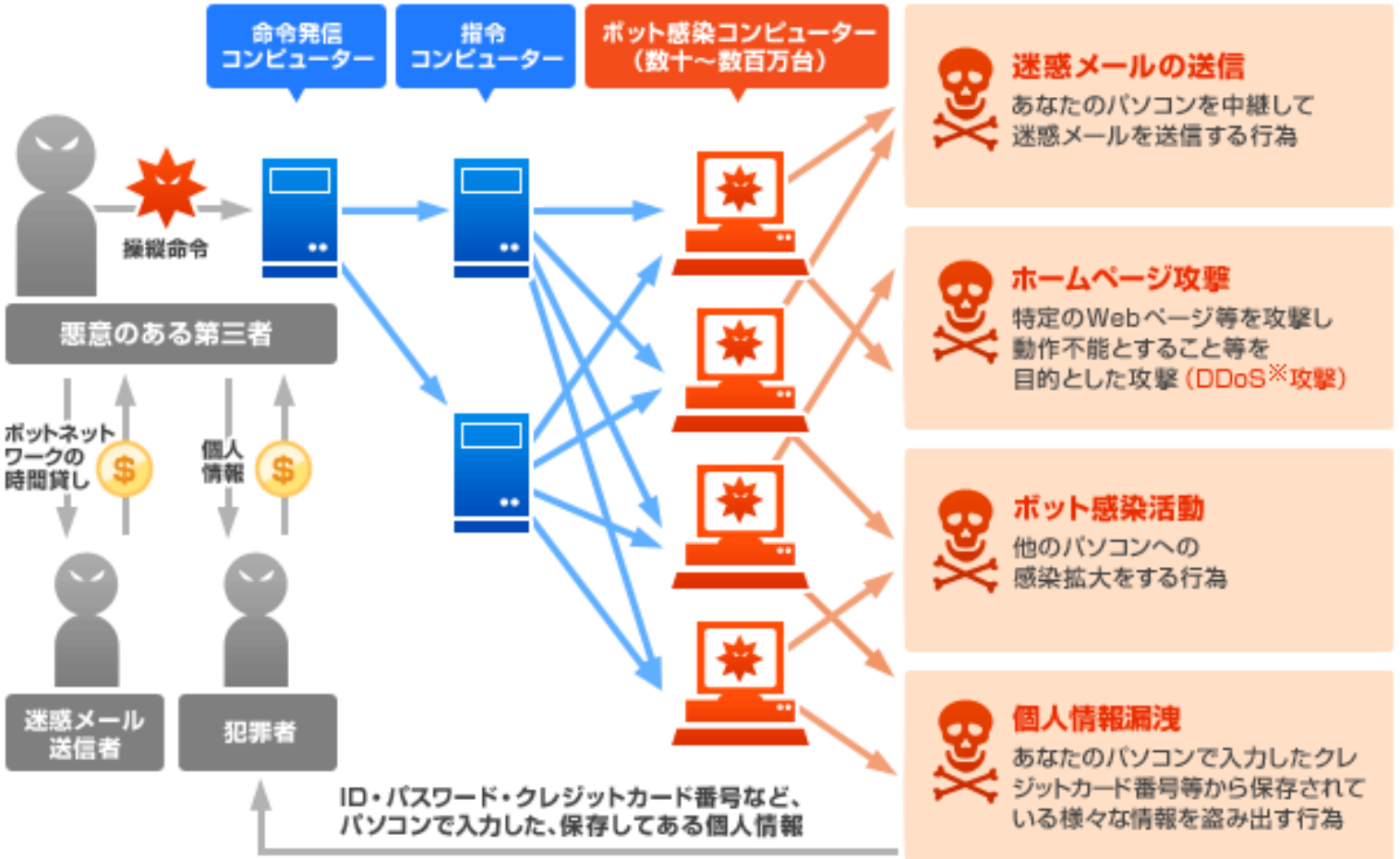
通貨偽造の罪は、「無期又は三年以上の懲役」に処される。偽造通貨の流通は国の信用を揺るがし、最悪の場合、国家の転覆をも生じかねない。このため、金額の多少に関わらず重罰（最低でも懲役三年）が適用される。

便利・手軽さで購入したカラーコピー機が、結果として重罪を引き起こす凶器となった。便利さ（リターン）の裏には必ずリスクがある。便利さ（リターン）が増すほど、リスクも増す。そして万一の場合には、知らなかったでは済まされない、という厳しい現実もある。

# 被害者から加害者へ

■なぜリスク管理が必要なのか

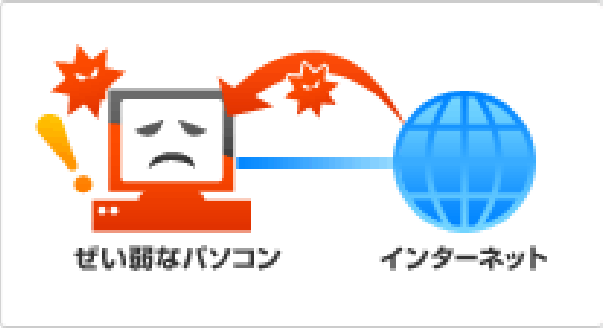
●ボット（BOT）とは




※DDoS（Distributed Denial of Service：分散サービス妨害）

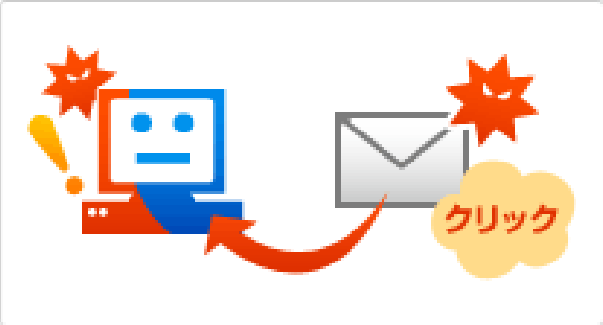
# ボット感染経路(1)

■なぜリスク管理が必要なのか



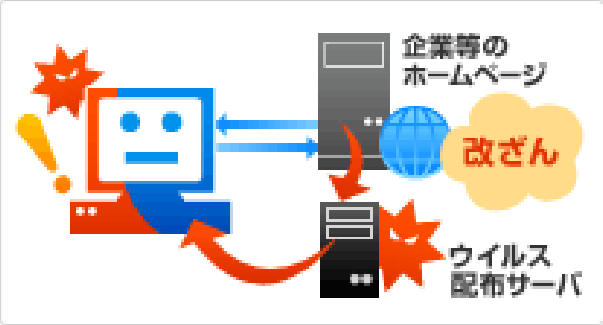

**経路1 ネットワーク感染型**

Windows等の基本ソフトや、その他のプログラムのセキュリティホール(ぜい弱性)や設定の不備を悪用し感染するタイプ。インターネット等のネットワークに接続するだけで感染する。




**経路2 メール添付感染型**

メールの添付ファイルをクリックし感染するタイプ。




**経路3 Web閲覧感染型**

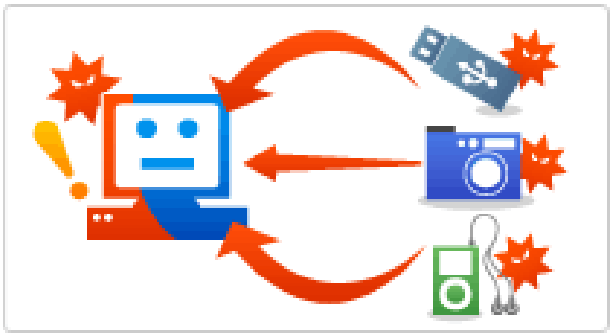
ブラウザで閲覧したホームページに埋め込まれたウィルスをダウンロードして感染するタイプ。ホームページを見ただけで感染することもある。

# ボット感染経路(2)

■なぜリスク管理が必要なのか


**経路4** Web誘導感染型

迷惑メールのURL等をクリックしアクセスしたホームページからウイルスをダウンロードして感染するタイプ。



**経路5** 外部記憶媒体感染型

USBメモリ、デジタルカメラ、ミュージックプレーヤーなどの外部記憶媒体を介在して感染するタイプ。

# 多発する緊急対策情報

■なぜリスク管理が必要なのか

IPA 独立行政法人 情報処理推進機構
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

サイト内検索 検索

IPAについて サイトマップ お問合せ ENGLISH

HOME | 情報セキュリティ | ソフトウェア・エンジニアリング | IT人材育成 | 情報処理技術者試験 | 未 踏 | オープンソフトウェア

HOME >> 情報セキュリティ >> 緊急対策情報・注意喚起 一覧

情報セキュリティ

ENGLISH

- 読者層別
  - 個人の方
  - 経営者の方
  - システム管理者の方
  - 技術者・研究者の方
- 緊急対策情報
- 届出・相談
  - ウイルスの届出
  - 不正アクセスの届出
  - 脆弱性関連情報の届出
- 情報セキュリティ対策
  - ウイルス対策
  - ボット対策
  - 不正アクセス対策
  - 脆弱性対策
  - 対策実践情報
- 暗号技術
- 情報セキュリティ認証関連
  - JISEC
  - JCMVP

緊急対策情報・注意喚起 一覧

2010年度

- 09月21日更新 【緊急対策情報】Adobe Flash Player および Flash を扱う製品の脆弱性について
- 08月05日掲載 【注意喚起】夏休み前に対策を
- 08月03日更新 【緊急対策情報】Windows シェルの脆弱性(MS10-046)について >
- 07月14日更新 【緊急対策情報】Windows のヘルプとサポートセンターの脆弱性(MS10-042)について
- 07月05日掲載 サポートが終了する Windows を利用しているシステム管理者への注意喚起
- 06月30日更新 【緊急対策情報】Adobe Flash Player および Flash を扱うアドビ製品の脆弱性について
- 06月02日掲載 【緊急対策情報】一太郎シリーズの脆弱性を悪用した標的型攻撃について
- 06月02日更新 【緊急対策情報】一太郎シリーズの脆弱性を悪用した標的型攻撃について
- 06月01日掲載 「一太郎シリーズ」におけるセキュリティ上の弱点(脆弱性)の注意喚起
- 05月17日掲載 「CapsSuite Small Edition PatchMeister」におけるセキュリティ上の弱点(脆弱性)の注意喚起
- 05月17日掲載 「WebSAM DeploymentManager」におけるセキュリティ上の弱点(脆弱性)の注意喚起
- 04月22日掲載 【注意喚起】ゴールデンウィーク前に対策を
- 04月20日掲載 複数のサイボウズ製品におけるセキュリティ上の弱点(脆弱性)の注意喚起
- 04月16日掲載 【緊急対策情報】Oracle Sun Java Deployment Toolkit の脆弱性について
- 04月16日更新 ウェブサイト管理者へ：ウェブサイト改ざんに関する注意喚起
  一般利用者へ：改ざんされたウェブサイトからのウイルス感染に関する注意喚起

# セキュリティ対策

■なぜリスク管理が必要なのか

- コンピュータ資源（ハード、ソフト）を自然災害、事故、故障、ミス、外部からの侵入、盗難、改ざんから保護すること
- インターネットの普及で、重要な課題に
- セキュリティポリシー
  - 何を、何から、どの位のコストをかけ、効率とどうバランスさせて、何を行うか

# 不正アクセス

■なぜリスク管理が必要なのか

| 名　称 | 内　　容 |
|---|---|
| DoS攻撃 | 大量のデータを送りつける攻撃。攻撃対象のシステムがサービスを提供できない状態にしたり、システムをダウンさせることを目的とする。 |
| DDoS攻撃<br>（分散サービス妨害） | ウイルスなどによって第三者のマシンに攻撃プログラムを仕掛けて踏み台にし、踏み台とした多数のマシンから標的に大量のバケットを同時に送信する攻撃。 |
| ポートスキャン | ポートを順番にアクセスして応答の有無を検査し、あるサーバでどんなサービスが動作しているかを調べ、不備のあるポートやセキュリティホールを見つけ出す。攻撃の踏み台を探す場合に使われる。 |
| バッファオーバーフロー攻撃 | サーバに許容量を超えるデータを送りつけて、システムを機能停止にしたり、誤動作される。 |
| スニファ | ネットワーク上に流れるパケットをモニタして、ネットワークトラブルの検出などに使うツール。悪意を持ったに人にとっては盗聴ツールになり得る。 |

# マルウェア



ユーザが意図しない動作をおこなう「悪意を持った」ソフトウェアのこと。インストールされていること自体をユーザが自覚していないケースがほとんど。

| 名　称 | 内　容 |
|---|---|
| コンピュータウイルス | 自己増殖能力・潜伏能力・感染能力を持ち、システムに悪影響を与える悪性のプログラム。発見が困難で伝染する性質を持つことから、「ウイルス」をいう名がつけられた。ファイルの破壊、データの改ざんや盗用、仕様以外のメッセージ出力や画面の破壊、異常データのネットワークへの大量送出などを行う。 |
| スパイウェア | システム内に潜伏し、個人情報などのデータを特定のサイトに勝手に送信したり、メールを送ったりするプログラム。 |
| ボット（BOT） | ウィルスの一種で、感染したコンピュータを、ネットワークを通じて外部から操ることを目的としたプログラム。 |
| キーロギング | キーボードのタイピング情報を記録するソフト。入力したIDやパスワードを盗む目的などで使われる。 |

# ウィルス対策7カ条



IPA（独立行政法人情報処理推進機構）から、次のようなウイルス感染防止指針が発表されている

① 最新のウイルス対策ソフトを活用すること

② 万一のウイルス被害に備えるためデータのバックアップを行うこと

③ ウイルスの兆候を見逃さず、ウイルス感染の可能性が考えられる場合ウイルス検査を行うこと

④ メールの添付ファイルはウイルス検査後に開くこと

⑤ ウイルス感染の可能性のあるファイルを扱うときは、マクロ機能の自動実行は行わないこと

⑥ 外部から持ち込まれたフロッピーディスクおよびダウンロードしたファイルはウイルス検査後に使用すること

⑦ コンピュータの共同利用時の管理を徹底すること

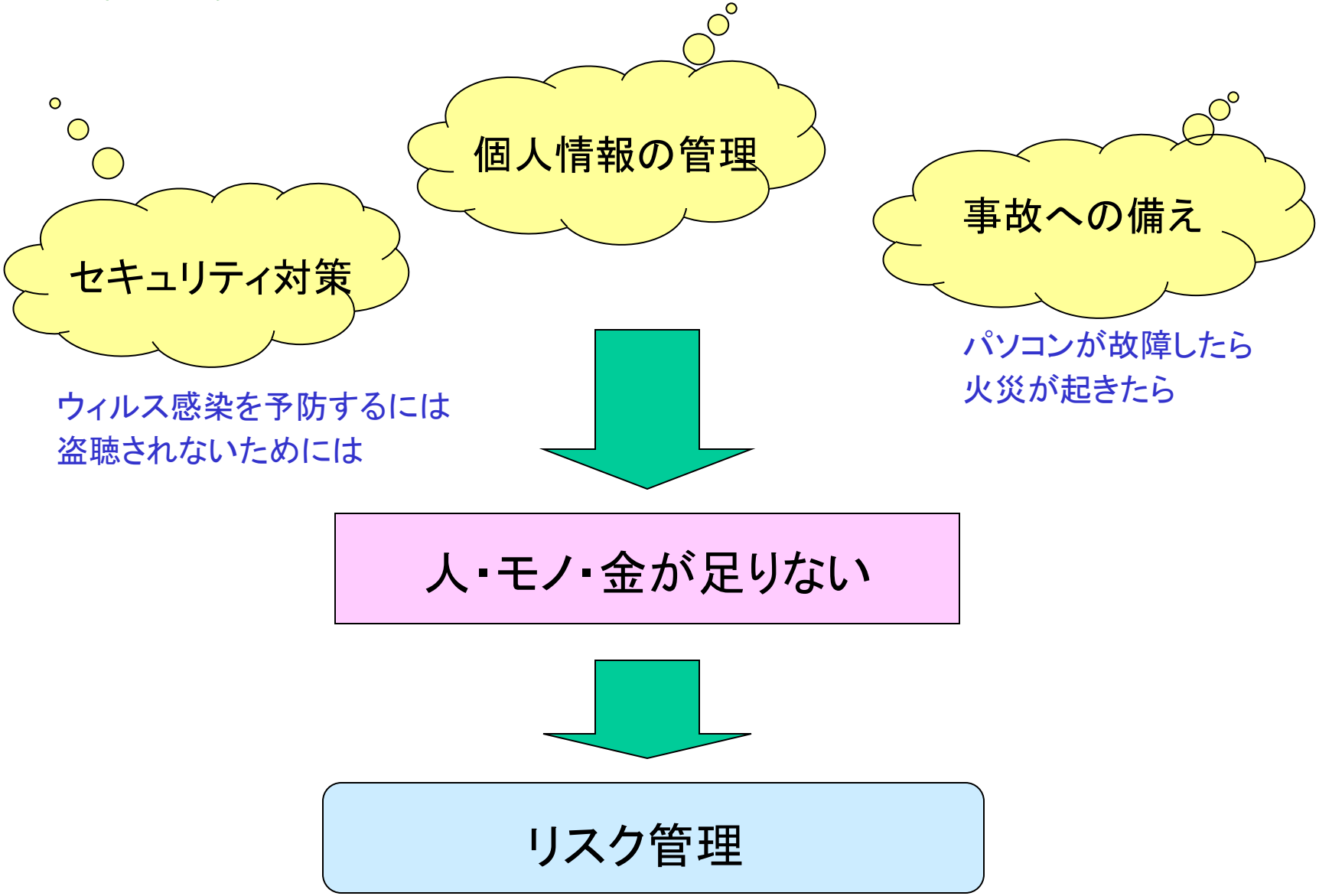
# ウィルスに感染した場合の対処



- 被害を広めないようにネットワークを切断
- コンピュータの電源を切る
- システムを外部ディスクなどから起動し、ウィルスチェックを行う
- 関連部署へ報告する
- ウィルスを駆除する（必要ならディスクを初期化する）
- IPA（情報処理推進機構へ届け出る）

# 現場で出来ることは

■なぜリスク管理が必要なのか



# ●ところでリスク管理とは

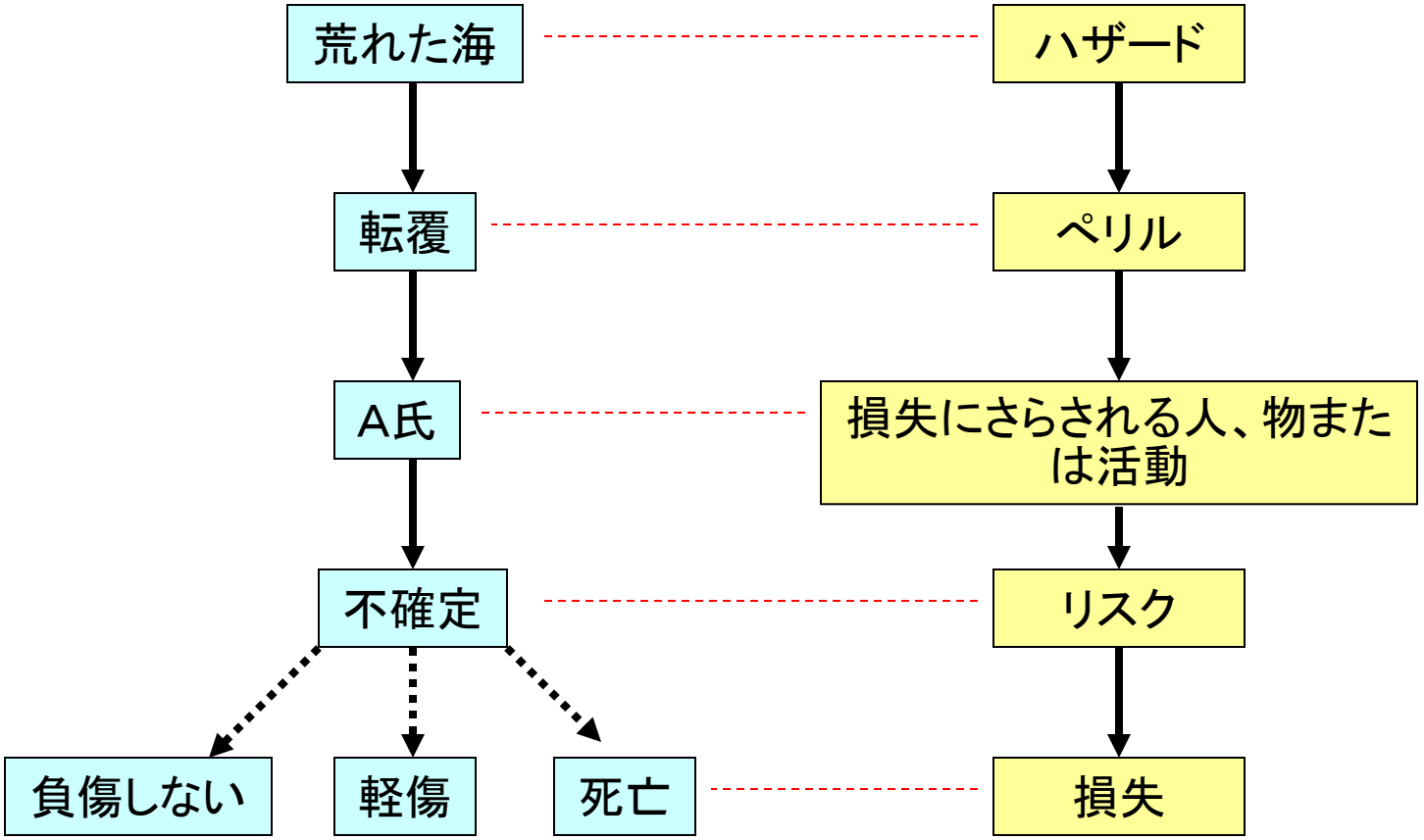


- なぜリスク管理が必要なのか
- ところでリスク管理とは
- 無線LANの危険と安全対策（事例紹介）
- 電子メールの危険と安全対策（事例紹介）
- データバックアップと企業リスク（事例紹介）

# リスクとは

■ところでリスク管理とは

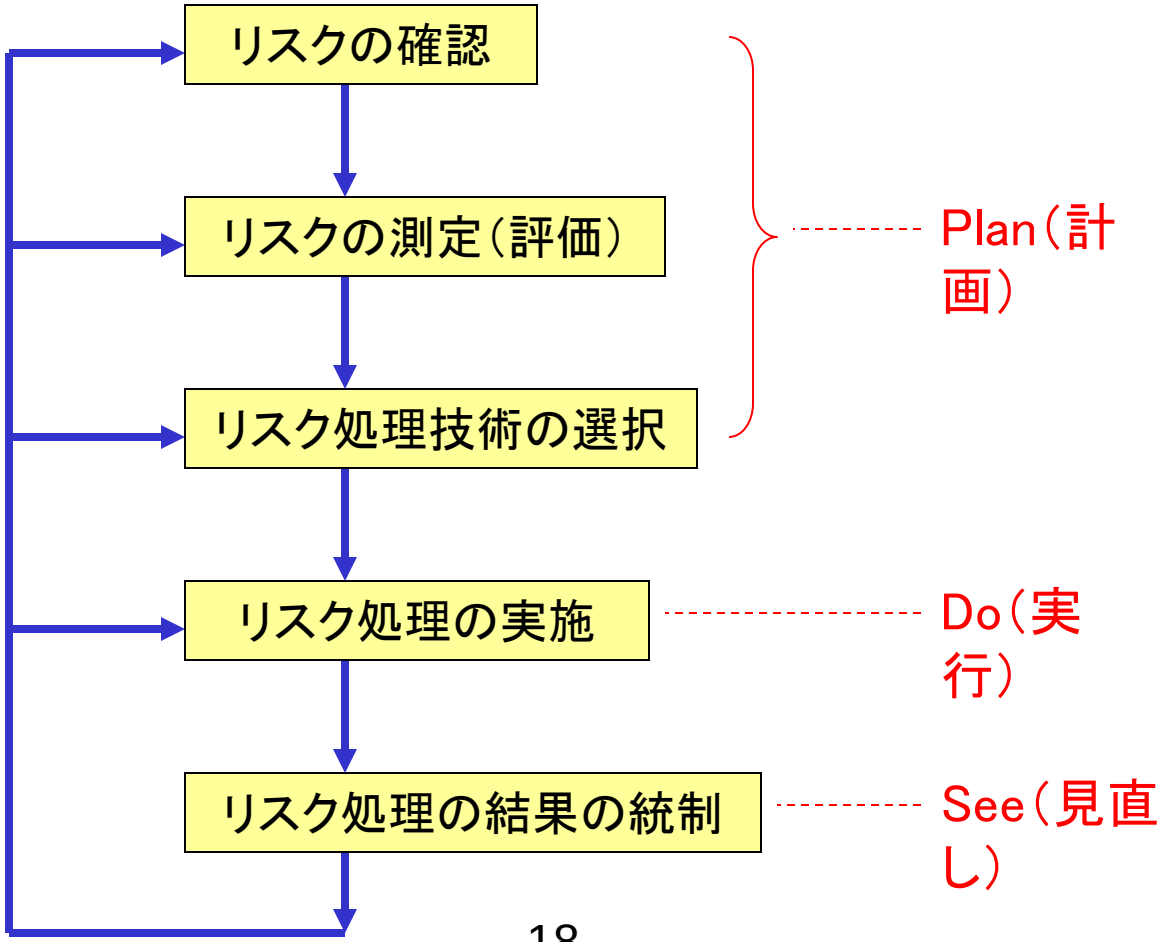
リスクとは、偶然の出来事により生じる、経済的な損失を発生させるような不確実性



# リスク管理の概要

■ところでリスク管理とは

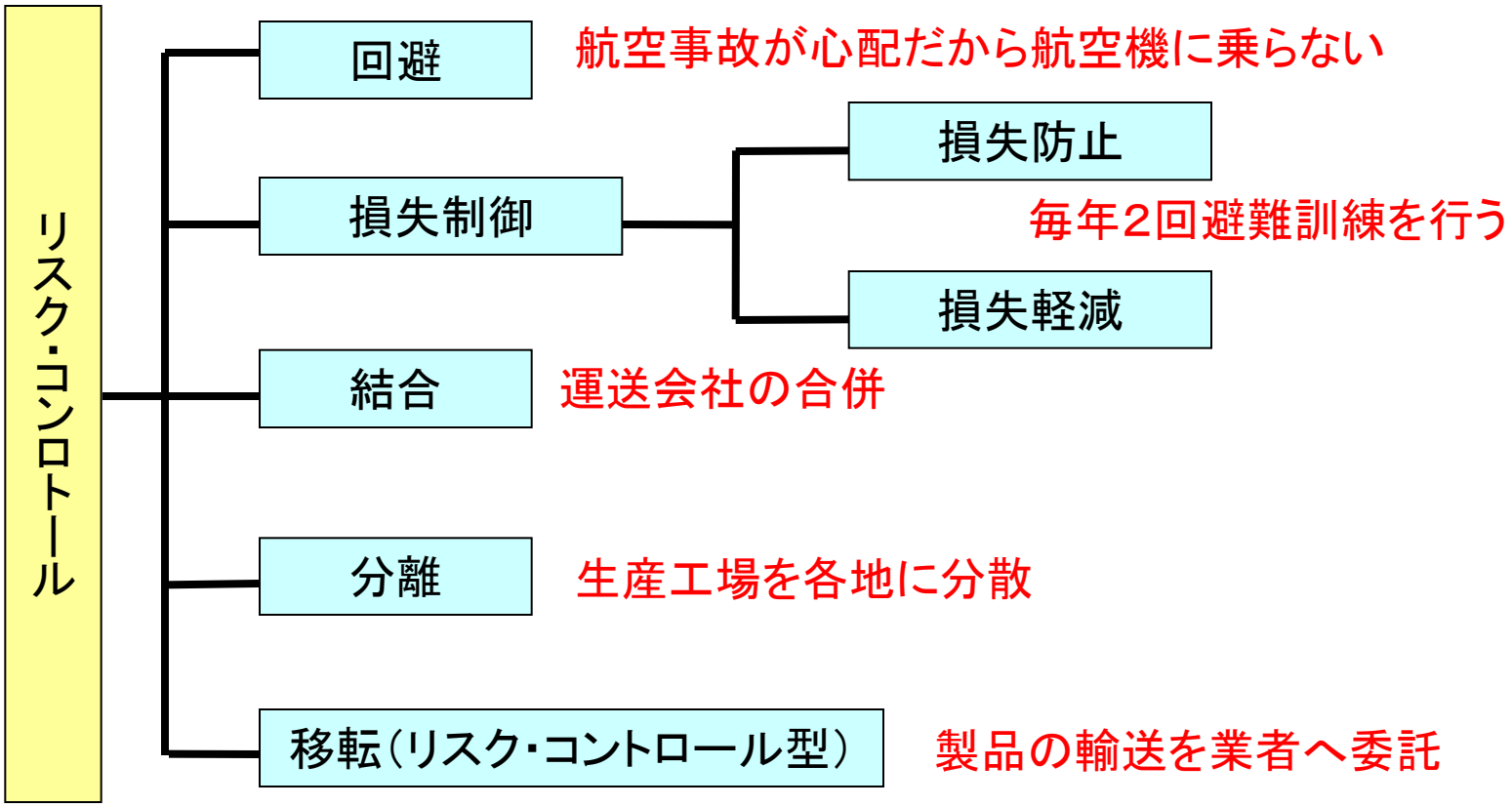
リスク管理とは、リスクの軽減・回避をめざすために、各リスクが生じた場合の損失・損害に対して合理的に効果をあげるための方法を検討・計画そ実行するプロセス。



# リスク管理の手法（１）

■ところでリスク管理とは

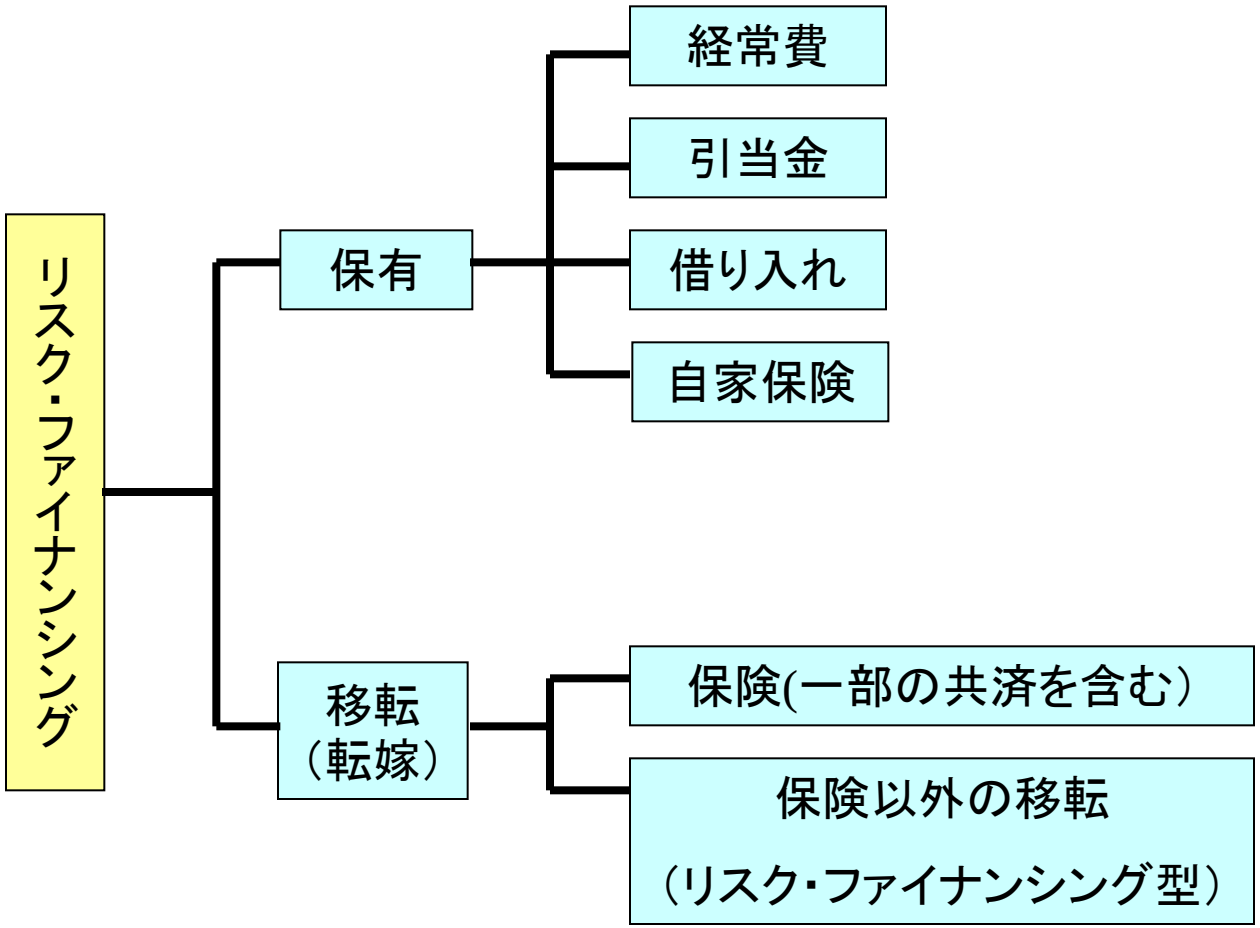
リスクの発生頻度・規模を軽減させたり、最小限のコストでリスクの可能性そのものを変える方法。



# リスク管理の手法(2)

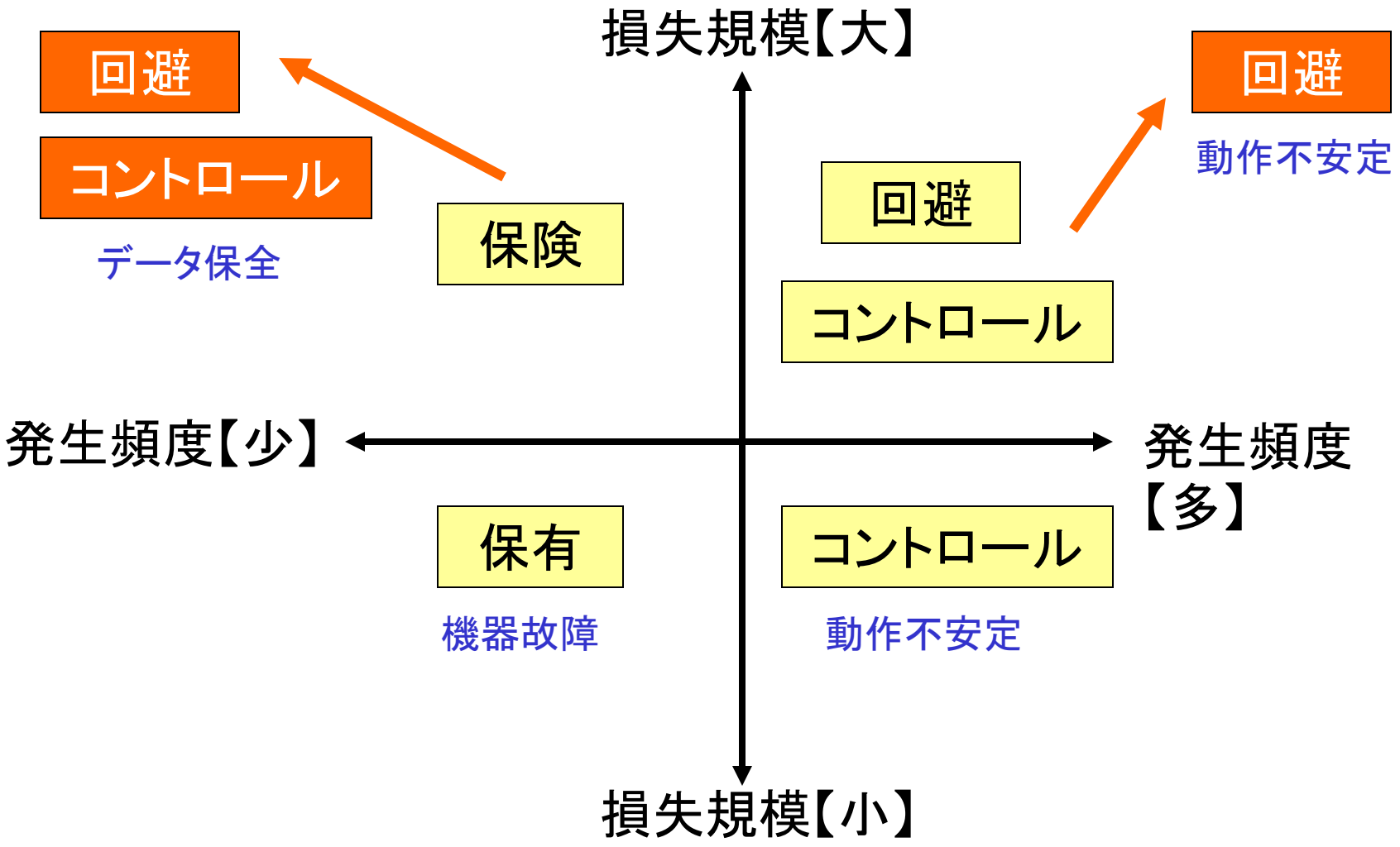
■ところでリスク管理とは

リスクの発生にともなう経済的損失の影響を軽減させる。



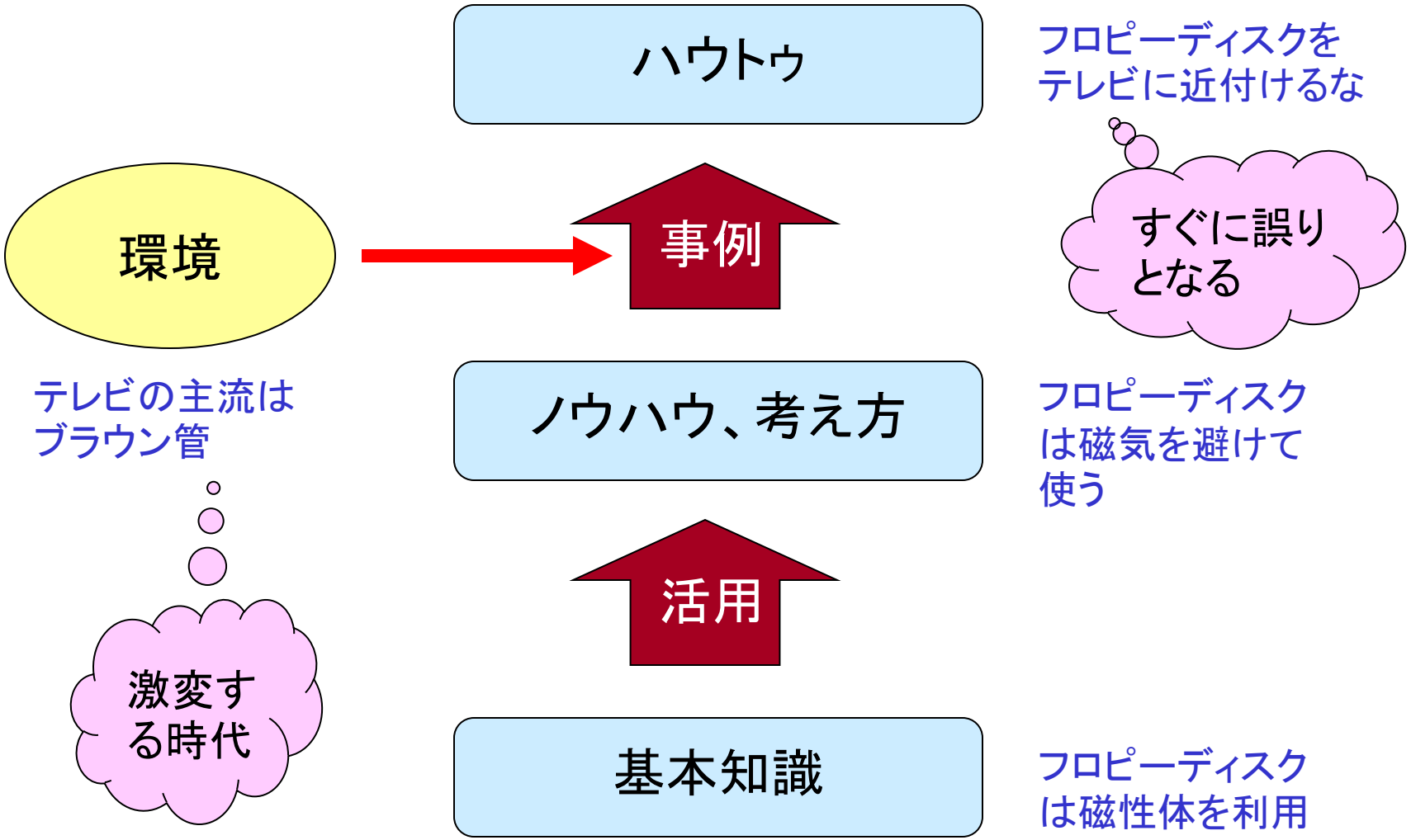
# リスク処理技術の選択




損失規模【大】
回避
コントロール
データ保全
保険
回避
動作不安定
回避
コントロール
発生頻度【少】
発生頻度【多】
保有
機器故障
コントロール
動作不安定
損失規模【小】

# リスク処理技術と基本知識

■ところでリスク管理とは



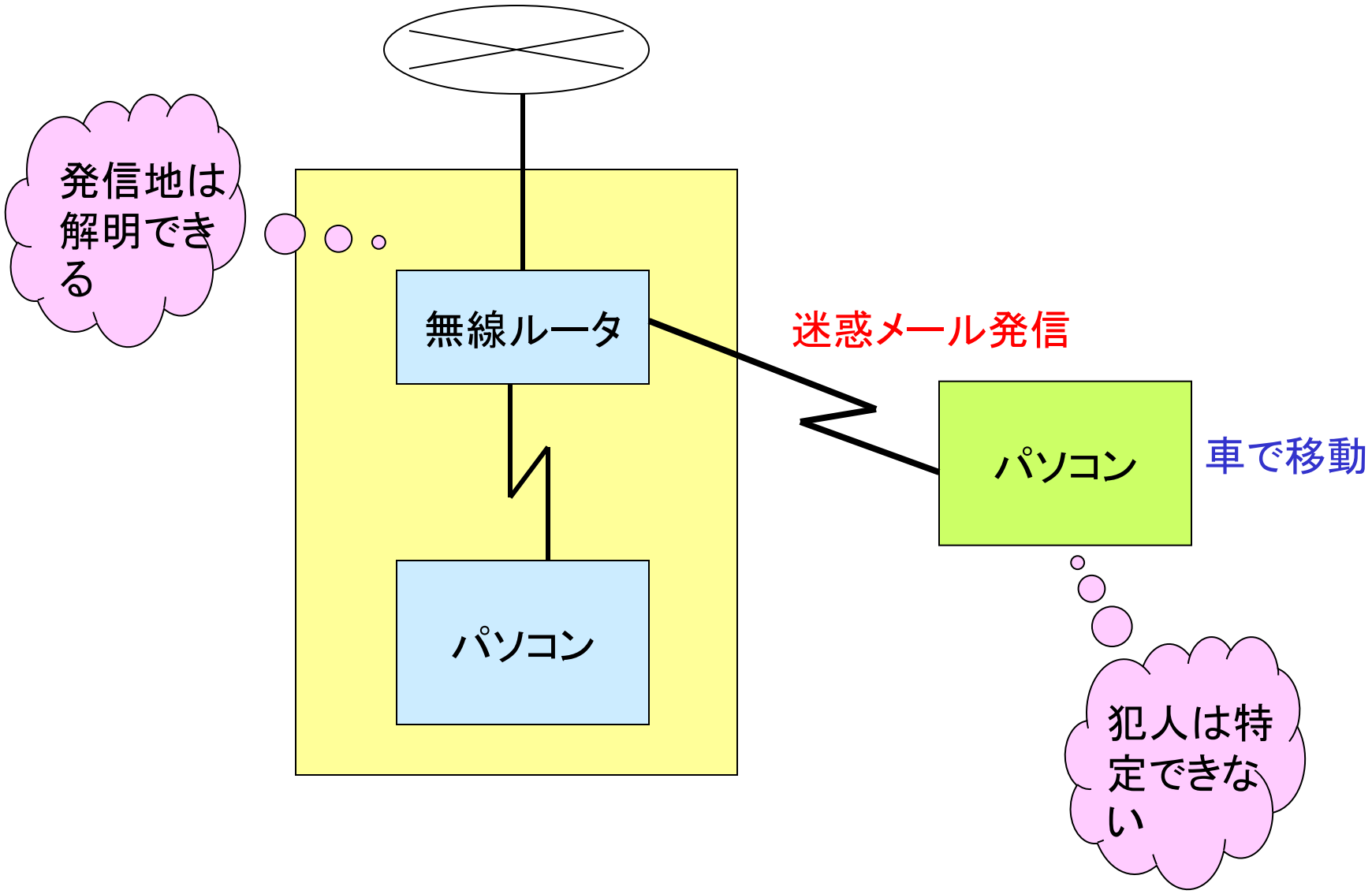
# ●無線LANの危険と安全対策（事例紹介）



- なぜリスク管理が必要なのか
- ところでリスク管理とは
- 無線LANの危険と安全対策（事例紹介）
- 電子メールの危険と安全対策（事例紹介）
- データバックアップと企業リスク（事例紹介）

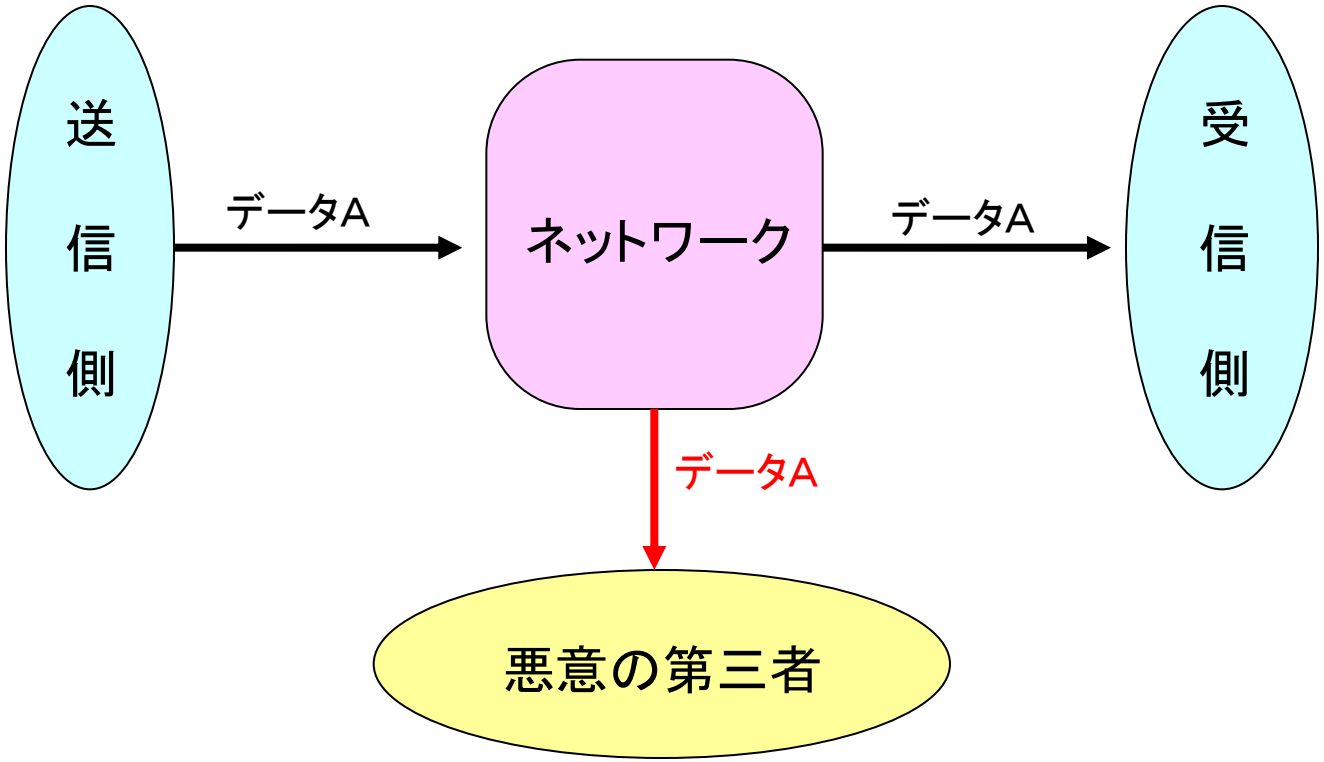
# 迷惑メールの発信源





# 盗聴

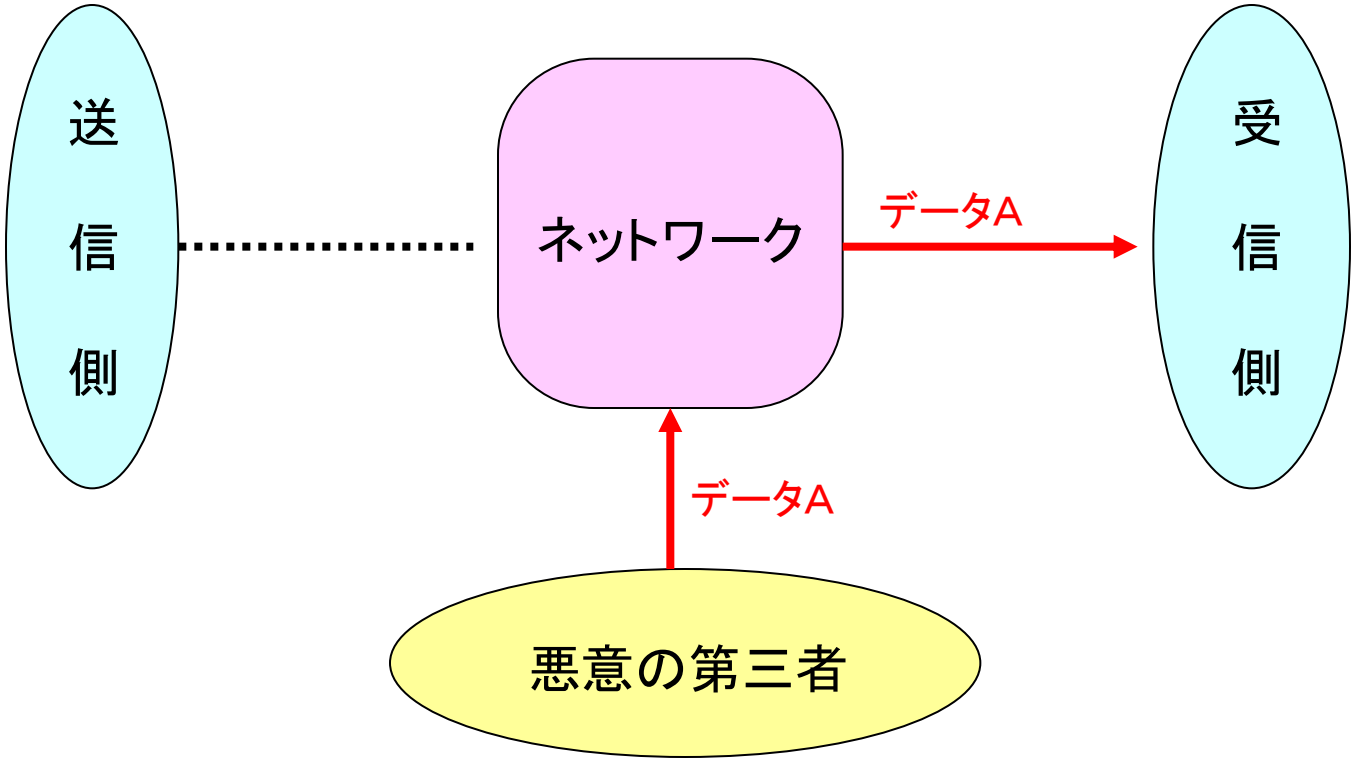





ネットワーク上を流れるデータを傍受して、情報を不正に入手する行為です。傍受されても内容を解読できないように、通信データを暗号化するなどの対策が必要です。

# なりすまし

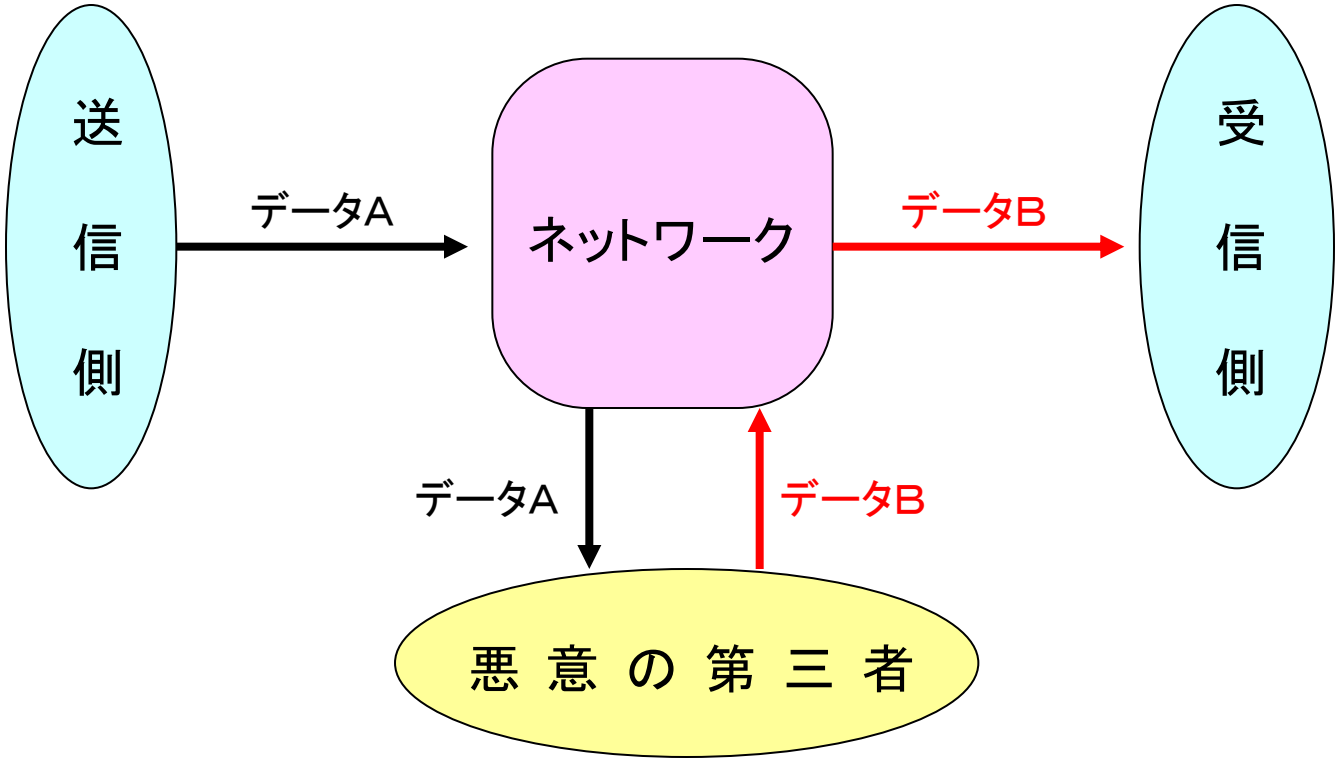





悪意の第三者が正当な利用者であるかのようにふるまい、システムへの不正侵入や不正な取引を行う行為です。対策として、相手を確認する認証や、相手の正当性を保証するディジタル署名を利用します

# 改ざん

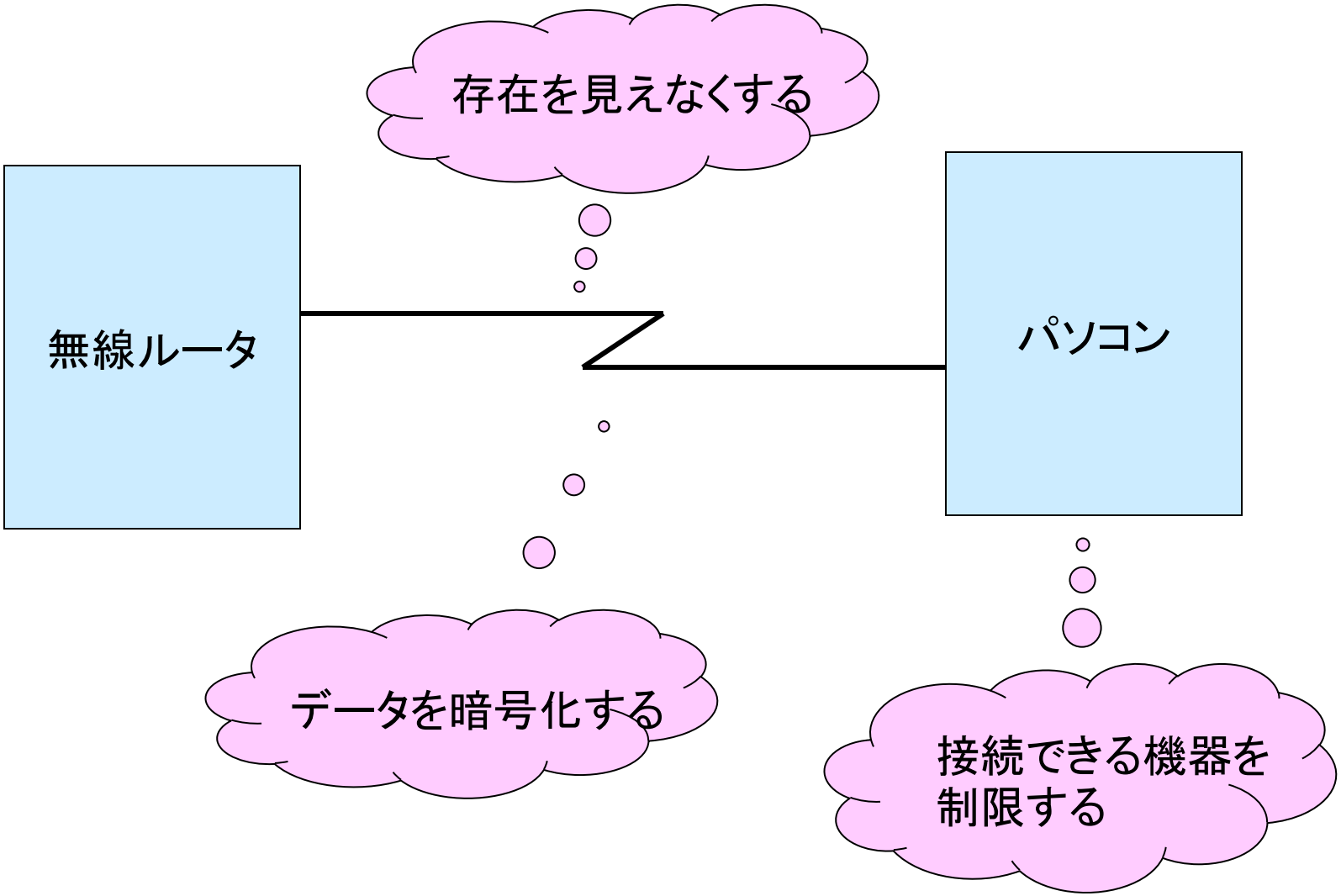





不正な手段でデータ（電子メール、ファイルなど）を書き換える行為です。対策として、伝送データとそこから生成されたダイジェストの整合性によって改ざんの有無を検出するメッセージ認証や、ディジタル署名が有効です

# 無線LANの安全対策





# 存在を見えなくする




ANY接続を禁止

# データを暗号化する




AESで、パスワードを設定

# 接続できる機器を制限する



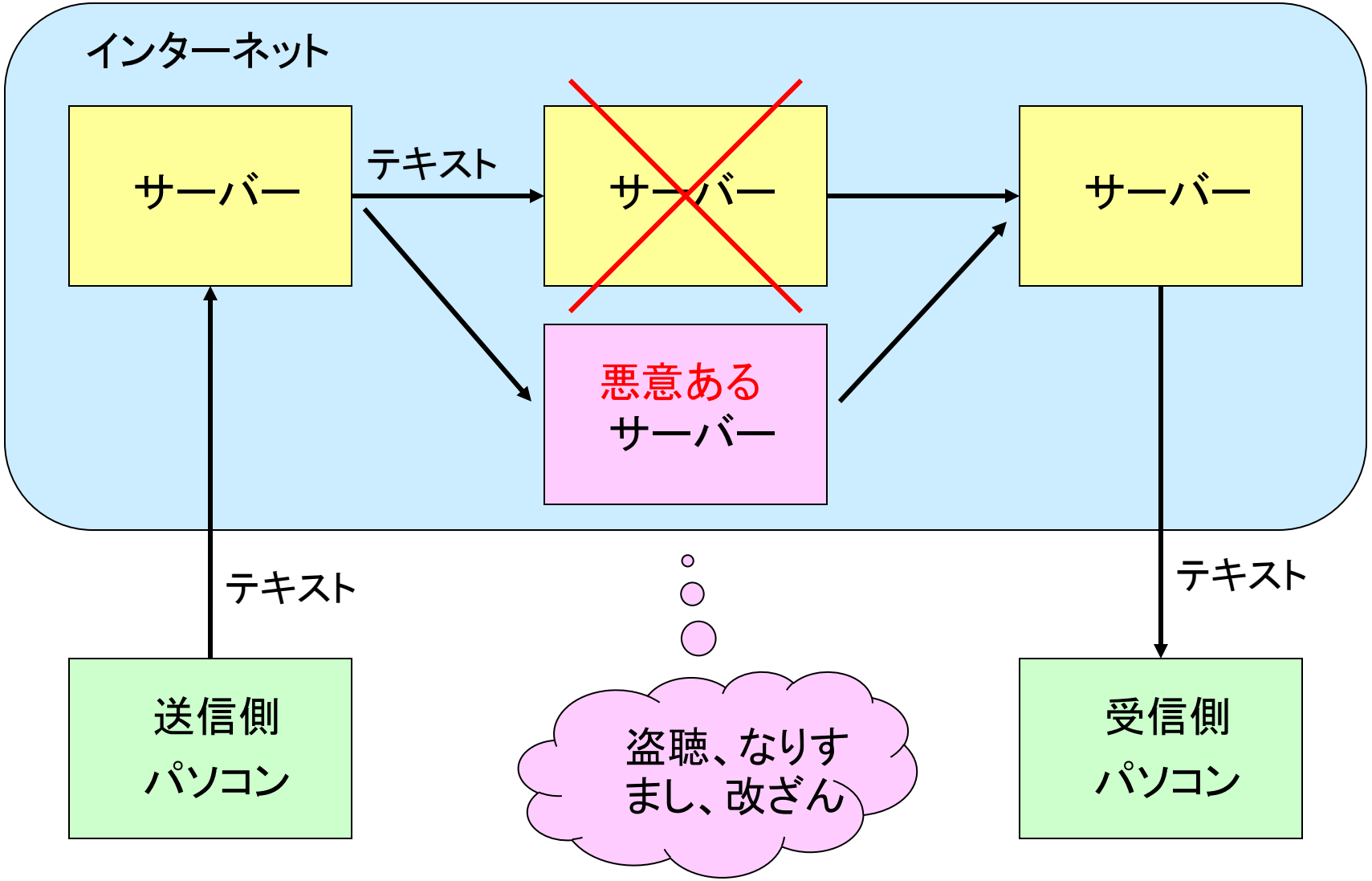
# ●電子メールの危険と安全対策（事例紹介）



- なぜリスク管理が必要なのか
- ところでリスク管理とは
- 無線LANの危険と安全対策（事例紹介）
- 電子メールの危険と安全対策（事例紹介）
- データバックアップと企業リスク（事例紹介）

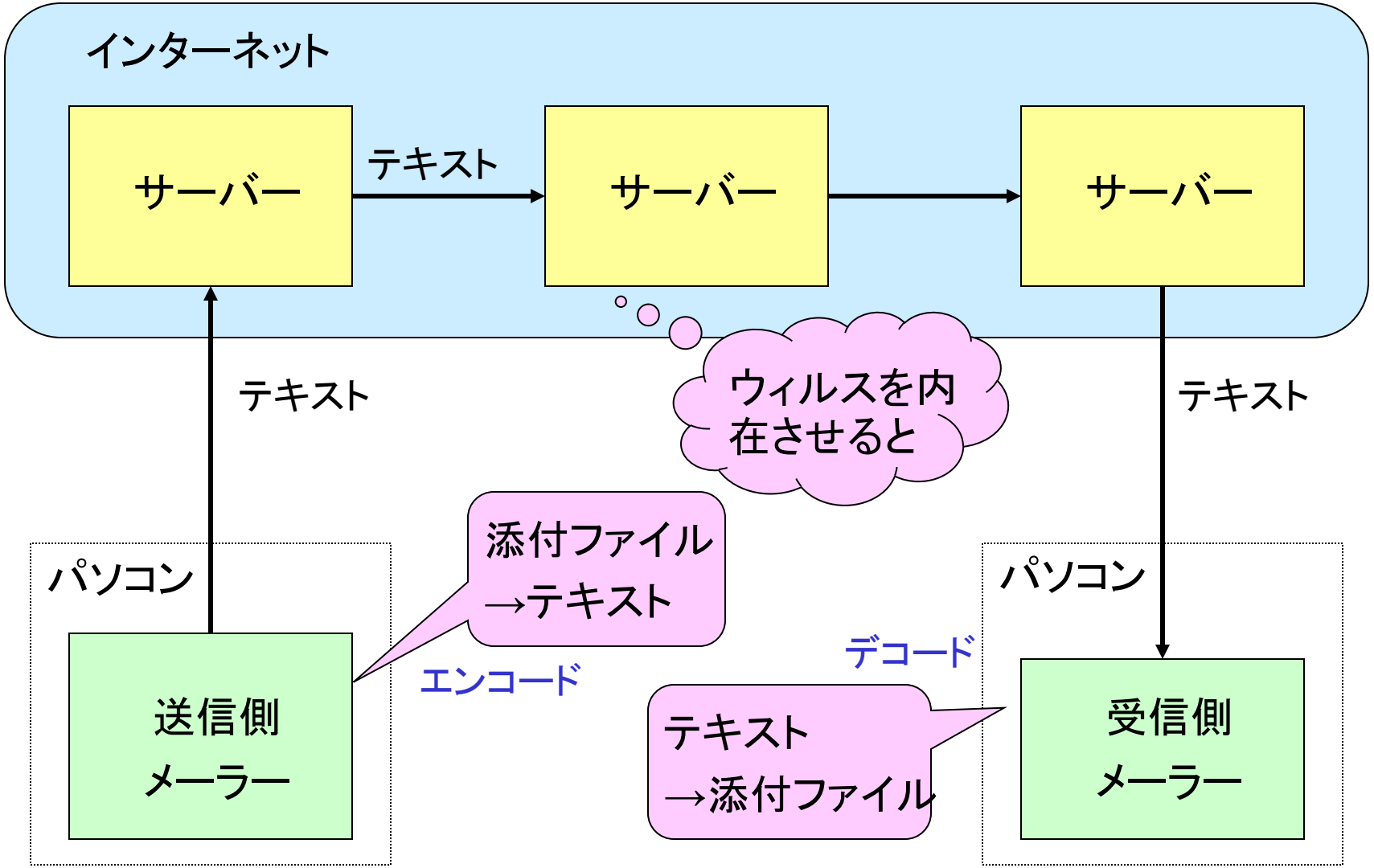
# 電子メールのしくみ




インターネット
サーバー
テキスト
サーバー
サーバー
悪意ある
サーバー
テキスト
テキスト
送信側
パソコン
盗聴、なりす
まし、改ざん
受信側
パソコン

# MIMEのしくみ




インターネット
サーバー
テキスト
サーバー
サーバー
テキスト
ウィルスを内
在させると
テキスト
パソコン
添付ファイル
→テキスト
エンコード
送信側
メーラー
デコード
テキスト
→添付ファイル
パソコン
受信側
メーラー

# 電子メールを安全に使うために



ウィルスを検査する

ウィルス対策ソフト

ウィルスを含む添付ファイルを開かない

不信なファイルは無視

不信なメールを開かない

プレビューは使わない

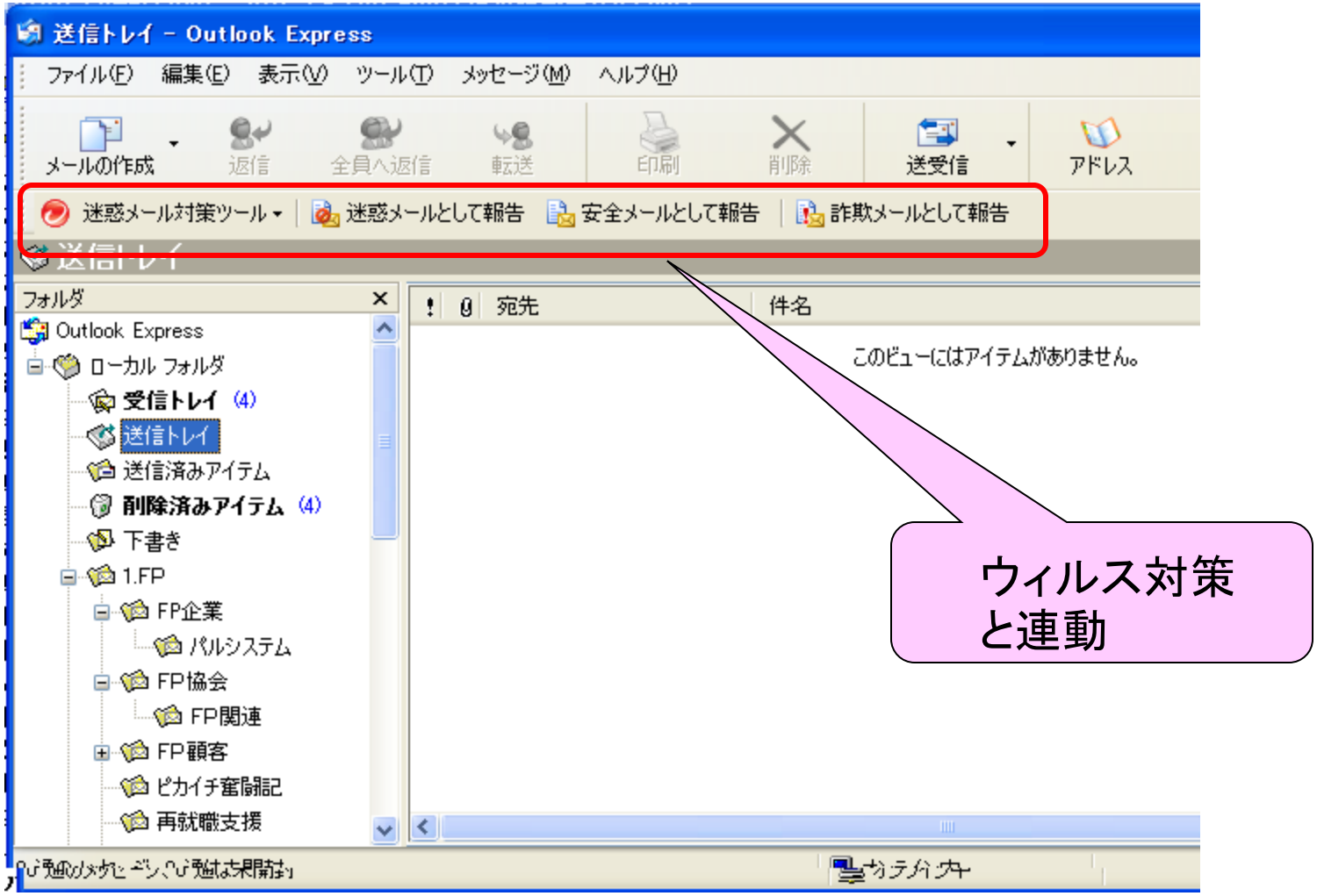
ハイパーテキストのメールを慎む

迷惑メールを効率的に廃棄する

ウィルス対策ソフト

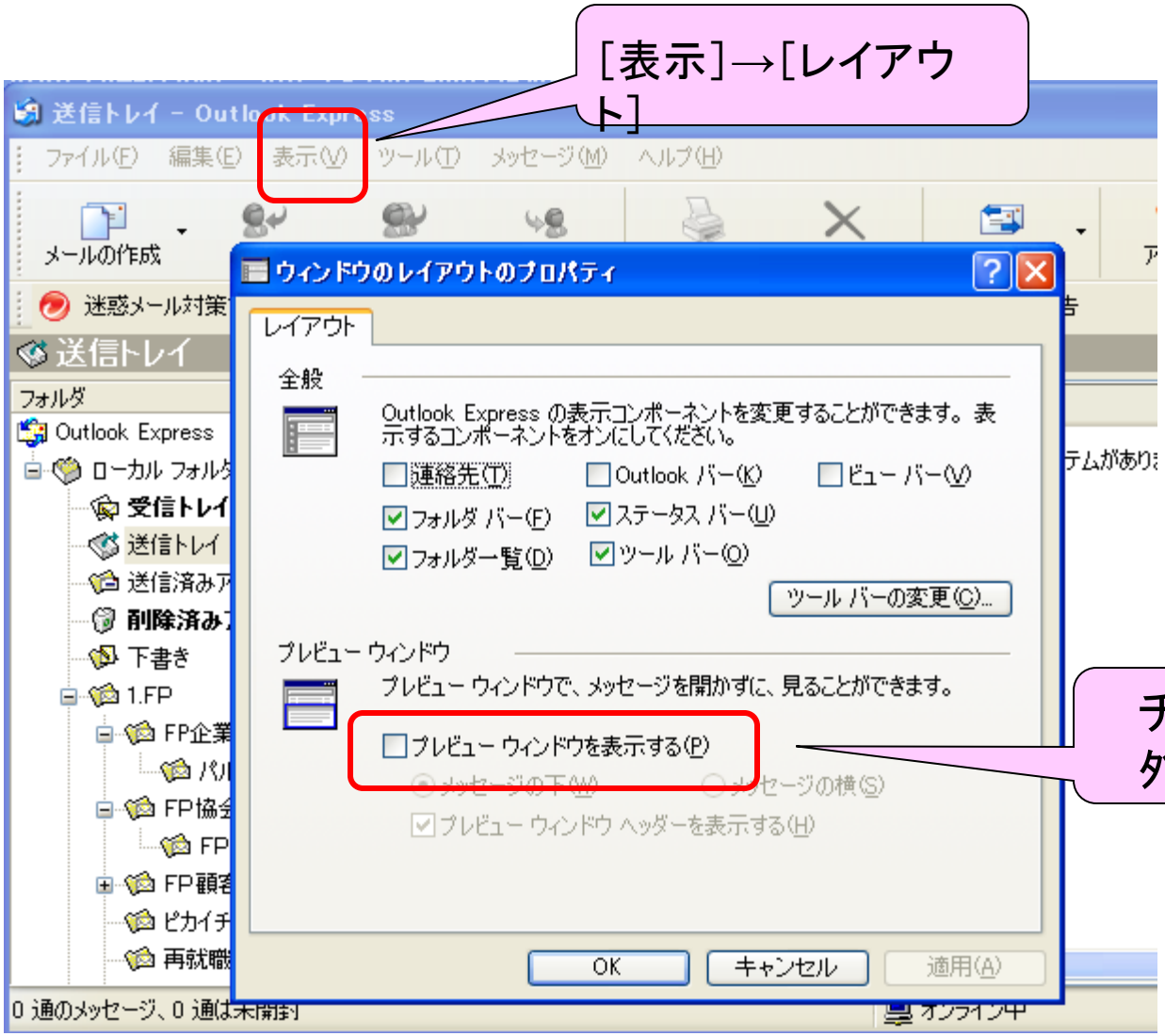
# ウィルス対策ソフトの導入

■電子メールの危険と安全対策



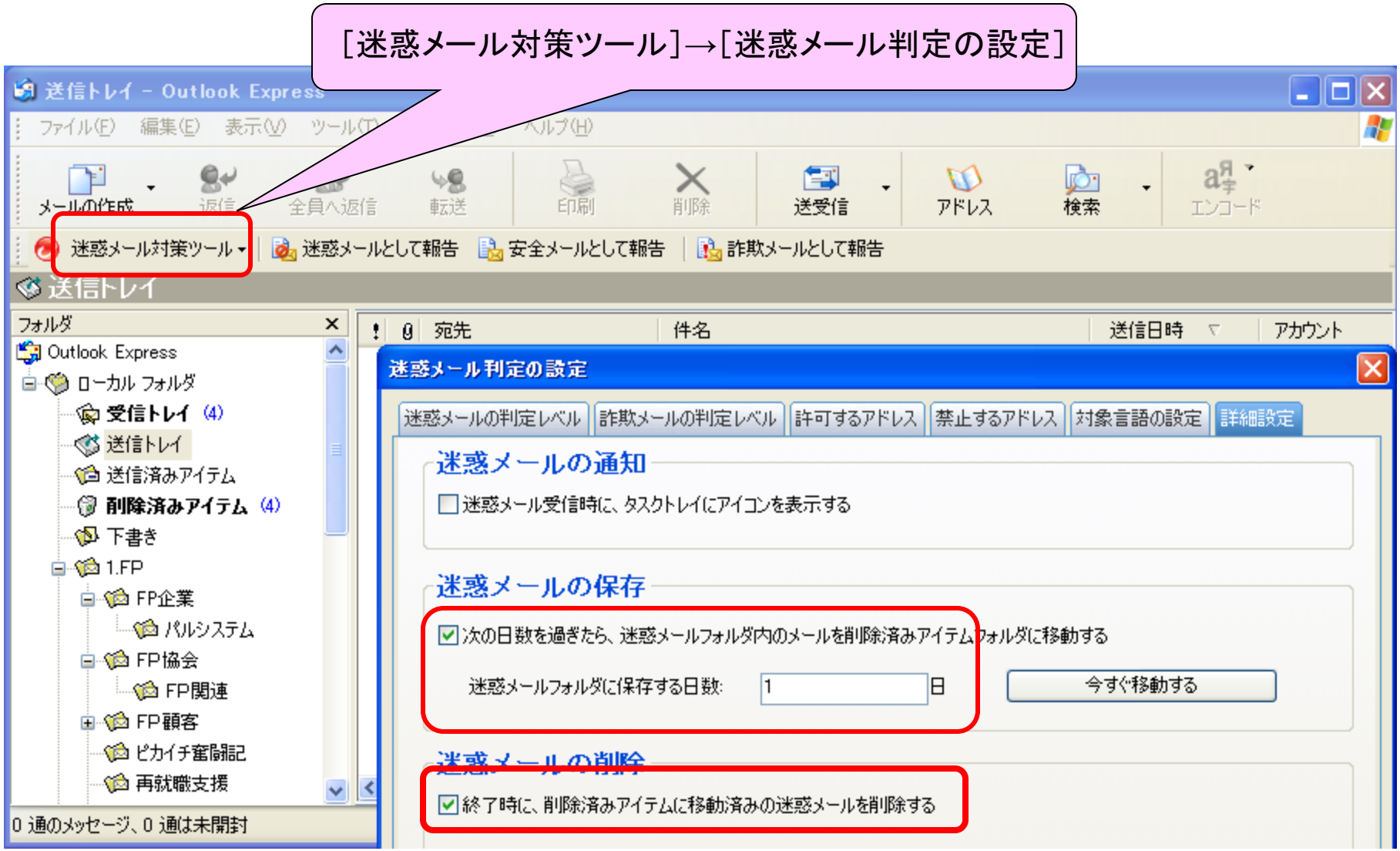
# プレビューは使わない




[表示]→[レイアウト]
送信トレイ - Outlook Express
ファイル(F) 編集(E) 表示(V) ツール(T) メッセージ(M) ヘルプ(H)
メールの作成
迷惑メール対策
送信トレイ
フォルダ
Outlook Express
ローカル フォルダ
受信トレイ
送信トレイ
下書き
1.FP
ウィンドウのレイアウトのプロパティ
レイアウト
全般
Outlook Express の表示コンポーネントを変更することができます。表示するコンポーネントをオンにしてください。
連絡先(T)
Outlook バー(K)
ビュー バー(V)
フォルダ バー(F)
ステータス バー(U)
フォルダー一覧(D)
ツール バー(O)
ツール バーの変更(C)...
プレビュー ウィンドウ
プレビュー ウィンドウで、メッセージを開かずに、見ることができます。
プレビュー ウィンドウを表示する(P)
プレビュー ウィンドウ ヘッダーを表示する(H)
OK
キャンセル
適用(A)
0 通のメッセージ、0 通は未開封
オンライン中
チェックを外す

# 迷惑メールを自動的に廃棄





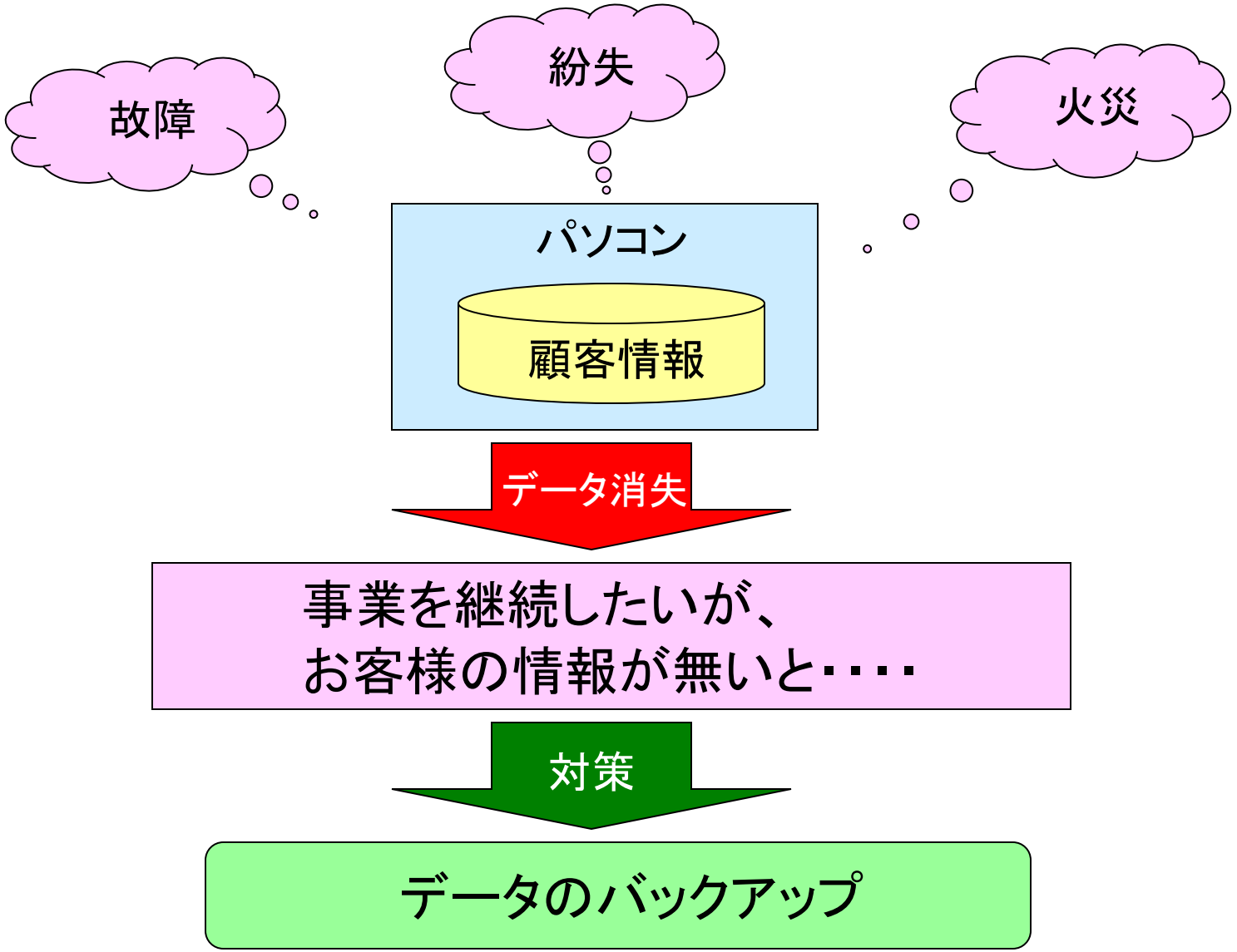
# ●データバックアップと企業リスク（事例紹介）



- なぜリスク管理が必要なのか
- ところでリスク管理とは
- 無線LANの危険と安全対策（事例紹介）
- 電子メールの危険と安全対策（事例紹介）
- データバックアップと企業リスク（事例紹介）

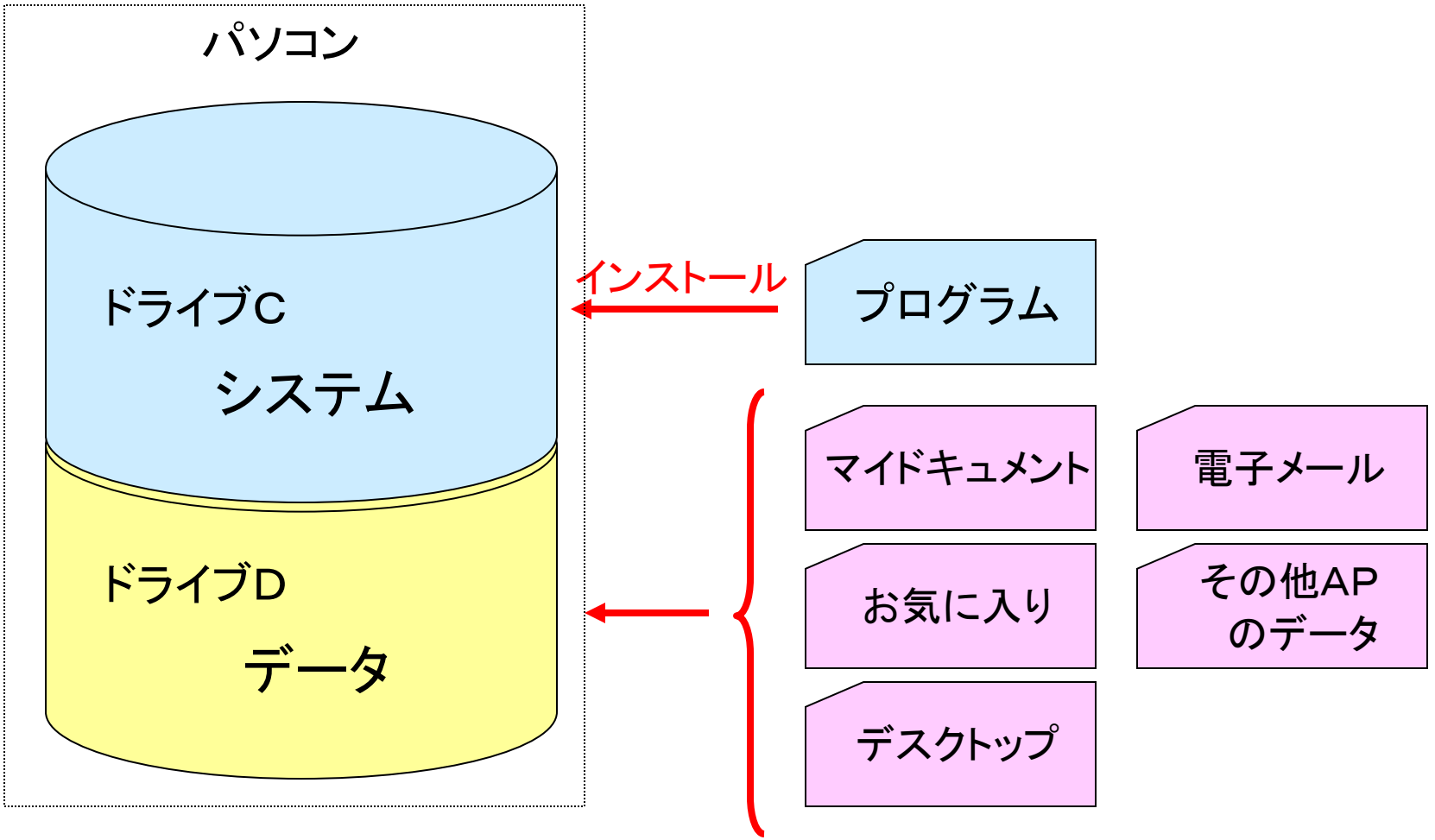
# なぜバックアップが必要か

■データバックアップと企業リスク



# システムとデータの分離

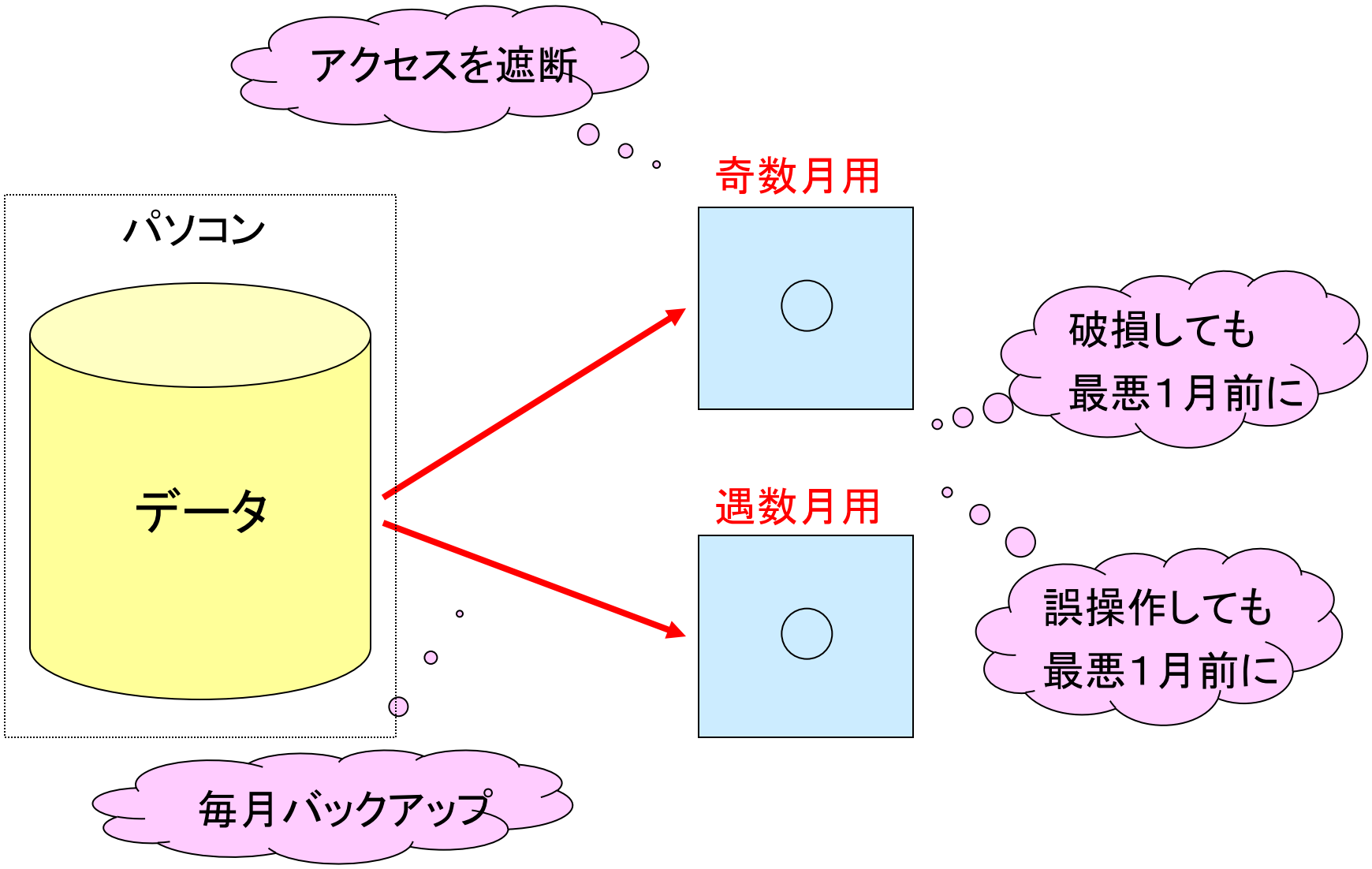
■データバックアップと企業リスク




Dドライブ全体をバックアップする

# バックアップの手順




アクセスを遮断
パソコン
データ
奇数月用
破損しても
最悪1月前に
遇数月用
誤操作しても
最悪1月前に
毎月バックアップ

# システムの再インストール