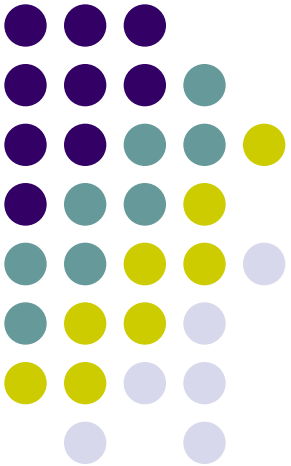
無線ネットワーク
セキュリティーについて

名城大学理工学部
渡邊研究室
070427728　加藤大智

Time:15分



本資料について

- 本資料は下記論文を基にして作成されたものです.
- 文書の内容の正確さは保障できないため，正確な知識を求める方は原文を参照してください.

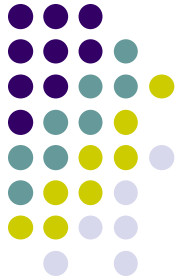
- O'REILY :802．11セキュリティ

参考書籍
(O'REILY :802．11セキュリティ)

- 802.11はセキュリティー面で多くの課題を抱えています。そのセキュリティーの課題と基礎について解説した上でセキュリティーを高める運用形態に関しての方法を説明していきたいと思います。

- 無線LANの仕組み、およびセキュリティを高める運用形態に関して一貫した知識を得ることができるでしょう。

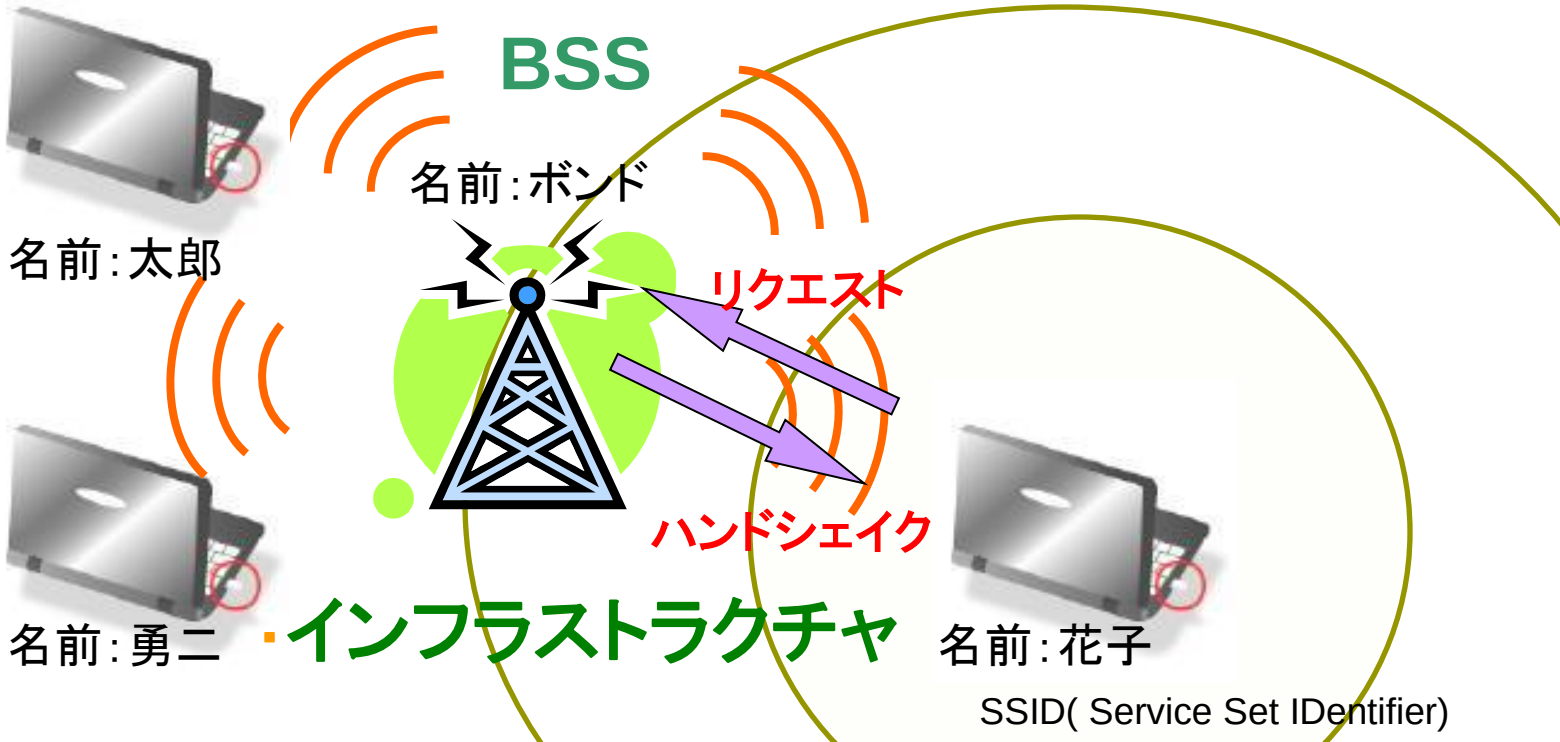
無線規格
「 802.11 」とは何か？



- 規格（802.11）
  - 802.11(IEEEにより策定された、広く普及している無線LAN関連規格)
  - Wi-Fi(Wireless Ethernet Compatibility Allianceという業界団体で相互接続性が確認されたもの）
    - Wireless-Fidelity(802.11製品で、相互接続性確認済みの意味）
- その他の規格（PCS・WAP・Bluetooth）
  - PCS（Personal Communication Systems）携帯電話での通信のための規格[USA.canada]
  - WAP(Wireless Application Protocol)小型通信無線器用の通信プロトコル
  - Blutooth(デジタル機器用の近距離無線通信規格)

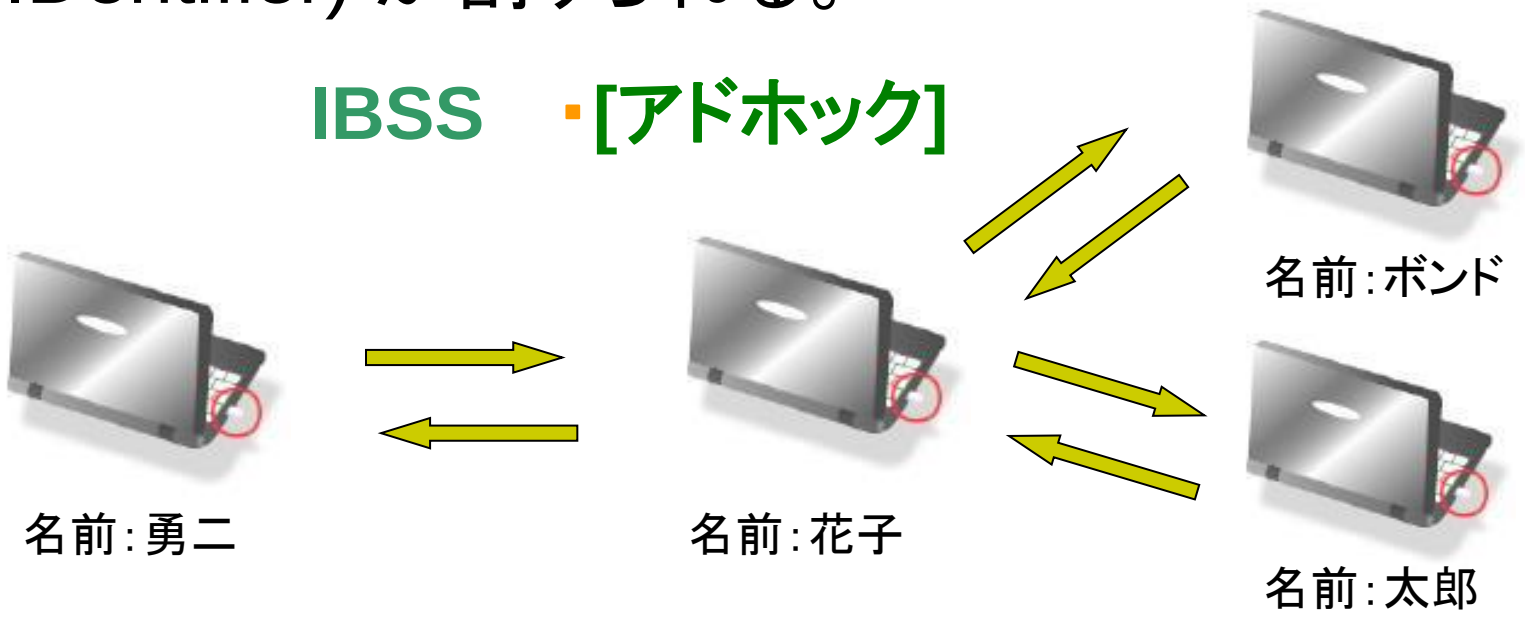
802.11ネットワーク　構成

- 802.11ネットワークは基本的にアクセスポイントとクライアントステーションから構成されている。この二つをあわせてBSSという。



802.11ネットワーク　構成-2

- クライアントステーションとクライアントステーションから構成されているものもある。この二つをあわせてIBSSという。
- 各BSS、IBSSには固有のSSID(Service Set IDentifier) が割りられる。



無線のメリット・デメリット

- メリット
  - 行動が自由になり生産性が向上
  - 構築が短時間でできる
  - 有線のネットワークに比べてインフラのコストが安く済む
  - オフィスや住宅の美観が損なわれない

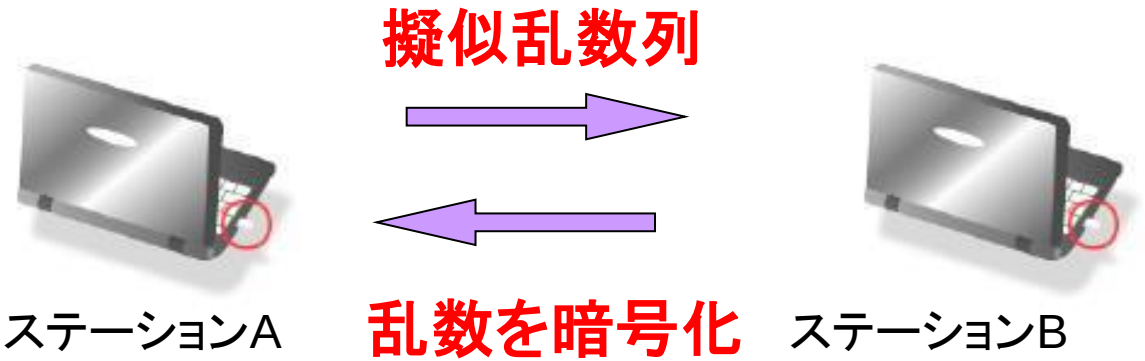
- デメリット
  - セキュリティが有線ネットワークに比べ弱い

無線と有線セキュリティーの違い
データを傍受するには…

- **有線ネットワークセキュリティー**
  - ケーブルに物理的に接続する
  - ケーブルから発せられる微弱な電磁波からデータを再現
- **無線ネットワークセキュリティー**
  - 離れた場所でも電波からデータを傍受できる

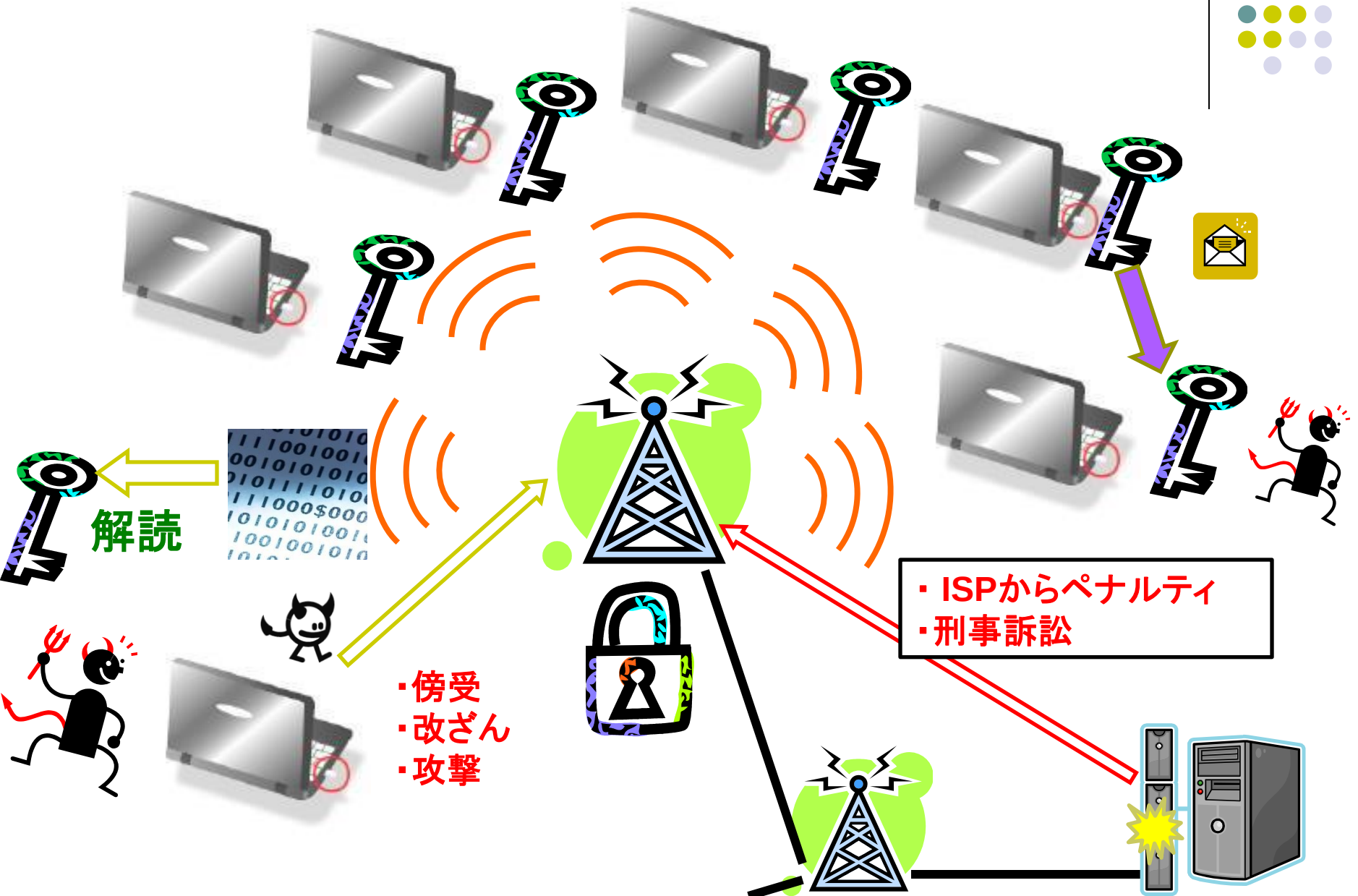
WEP（Wire Equivalent Privacy）

- WEP:暗号化プロトコル
- データの機密性保持と認証の役割を果たす.
- 認証



- 問題点
  - WEPではLANユーザー全員に同じ鍵を持たせることになるため、ユーザー数が増えるとそれだけ安全性も低くなります.
  - ブルートフォース（総当り）攻撃によって暗号を見破ることができる

・WEPではLANユーザー全員に同じ鍵を持たせることになるため、
ユーザー数が増えるとそれだけ安全性も低くなります.
・ブルートフォース（総当り）攻撃によって暗号を見破ることができる

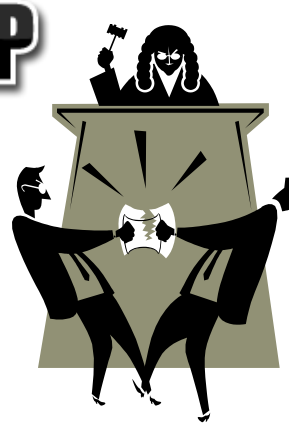


WEPが使われている理由

- トラフィックを傍受した後に、暗号を解読するという仕事をしなければネットワークにアクセスできない。

  （多少なりとも時間がかかる）

- 不正アクセス禁止という警告になるため、攻撃を行った人の言い逃れを防ぐことができる。
- キーローテーションといったセキュリティーを高めるテックニックも使えるように様になってきた



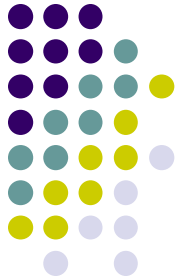
APのセキュリティー

- 管理インタフェース
  - telnetを使用した管理機能はOFFにする。
  - APのリモート管理が必要ない場合は、そのための機能を全てOFFにする。
  - 特に必要なければ管理サーバーもOFFにする。

- ログの管理
  - Swatchを使用してログの監視を自動化する。

（どのようなデータを危険とするかはユーザが設定する。）

Swatchとは



- syslog 等のログファイルのリアルタイム監視プログラム。
- ログ中に興味をひく文字列を見つけた場合、それを通知する。
- ユーザーへの通知手段は、電子メールを送る、ベルを鳴らす、指定されたコマンドを実行するものがある。
- 不正なアクセスを監視し、トラブルを素早く察知するのに役立つ。

Swatchの導入方法

- Swatchのインストール
  - cd/usr/ports/security/swatch

    make

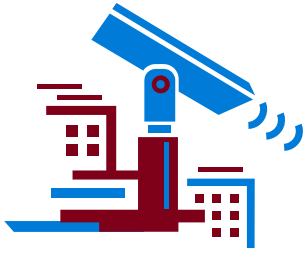
    make install
- Swatchの設定
  - ローカルマシンへの接続要求の証拠となるログエントリが見つかるたびにコンソールに表示してベルを鳴らす。
  - Watchfor　/Deny TCP 192.168/ (/文字列/ "アクション“)

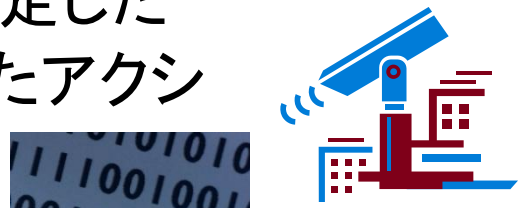
    echo　red

    bell 3

Swatch コマンド（設定）-1

- **Watchfor　[文字列]**
  - 監視しているlog ファイルにwatchfor で指定した文字列が現れた場合に、続いて指定されたアクションを行います。





- **Ignore [文字列]**
  - ignore に続いて指定された文字列は無視されます。これは不要な情報をフィルタリングするために使用されます。

    （例)ignore /sendmail/,/nntp/,/xntp/

Swatch コマンド（アクション）-2

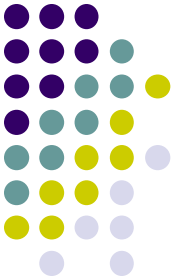
- **bell [N]:**
  - N 回ベルを鳴らします。

- **mail=[user](,subject=[title]):**
  - user にメールを送ります。その際件名は title になります。
    （例）watchfor /warning/mail=AAA@CCC.co.jp:subject=[swatch] mail:warning

- **echo [modes]:**
  - キーワードにマッチしたログの文字列をエコーバック（画面に出力）します。Modes: normal,black,red,underscore

Swatch コマンド（オプション）-3

指定したアクションに更に以下のオプションを指定可能です。

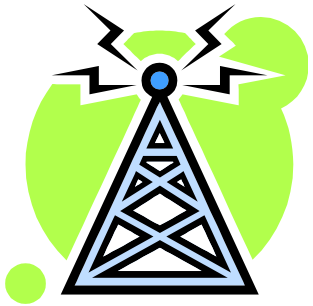


- **continue:**
  - 通常設定ファイルでのマッチングは文頭から行われ、一度でもマッチしたら照合はそこまでです。continueを使用することによって照合を続けさせることができます。
- **throttle [hh:mm:ss] (hh:時間 mm:分 ss:秒):**
  - メッセージの中にはsyslog に繰り返し表示されるものもあります。この時アクションでメール送信するように設定(mail=)していた場合はメールを多数送信してしまいます。これを防ぐために、[hh:mm:ss]で指定した時間が過ぎるまでは同じメッセージを無視するという設定ができます。

Swatch コマンド（オプション例）-3

- Continue:
  - watchfor /LOGIN/
    echo red
    bell 3
    continue
- **throttle [hh:mm:ss] (hh:時間 mm:分 ss:秒):**
  - watchfor /file system full/
    mail=AAA@BB.CCC.co.jp,subject=[swatch]
    file system full throttle 09:00:00
    (“file system full” にマッチした時、9 時00 分00 秒迄はメール送信を行いません。)

ご清聴ありがとうございました



END