サイバー犯罪の現状と対策

福島県警察本部
サイバー犯罪対策室

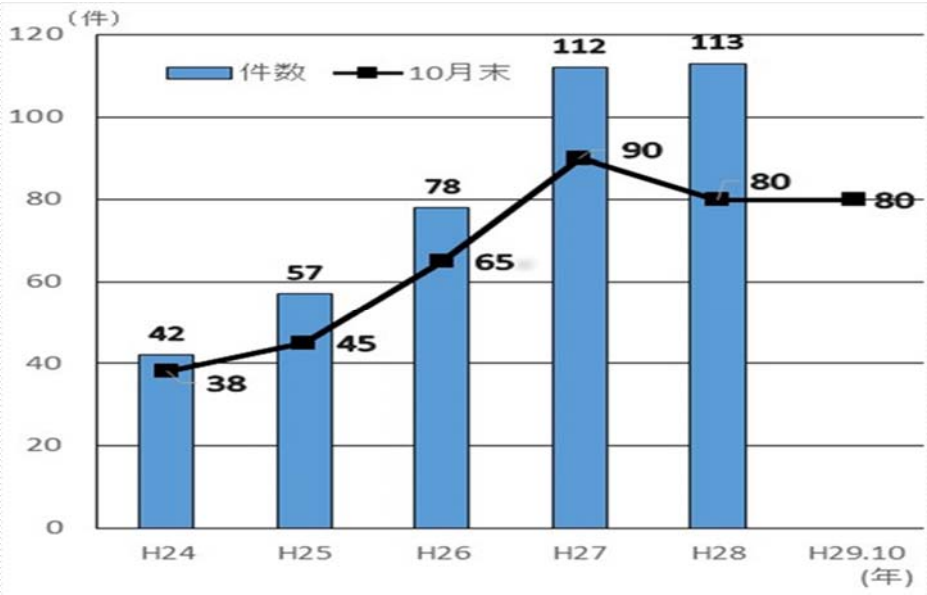
インターネットの危険性

「つながる」ことのデメリット

- **ツイッターなどのSNS**を通じて知り合い、命を奪われることも。

- 誰とつながるのか。言葉のやりとりだけでは、その裏に潜む危険性は分からない。

サイバー犯罪検挙統計（10月末現在）



最多の昨年と横ばい

児童被害＝約半数（児童ポルノ等）

児童被害の現状

【児童買春・児童ポルノ、県青少年育成条例違反 】

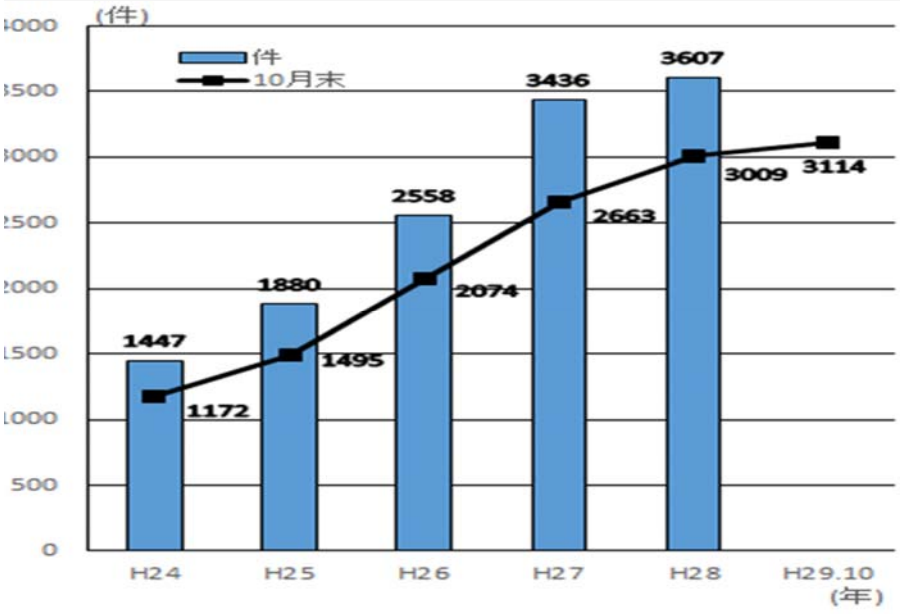
＜主な特徴＞

- **SNS、アプリ**等を通じて知り合う
- **自画撮り**による被害が多い

スマホの約束６か条

「あ」・・・会わないで！（知らない人と）
「と」・・・撮らないで！（自分の裸を）
「が」・・・画像を送らないで！
「こ」・・・個人情報を載せないで！
「わ」・・・悪口を書き込まないで！
「い」・・・いじめないで（ネットを使って）

サイバー犯罪相談統計（10月末現在）



過去最多
のペース

詐欺関係＝７割超
（架空請求・ワンクリック）

事例①

急増！

【 LINE 乗っ取り・電子マネー詐欺】

友人から、LINEで、
「ちょっと手伝ってほしい。ビットキャッシュを買ってほしい。
２万円分でいい。」
とお願いされた。
そのまま購入し、ＩＤ番号を教えてあげたが・・・

勝利の方程式（１００％疑う）

LINE、Twitter、Facebook等
＋
お金の話（電子マネー含む）
↓
詐　欺を疑う

事例②

【SMS(ショートメール)架空請求】

「未払い料金」を請求される。
支払いは「電子マネーで」！

対応①

無視

対応②

相談

おまけ～詐欺サイト

【ネットで商品を買ってお金を支払ったのに、商品が届かない】

私はもう騙されない！①

商品の画像をネット検索してみる

私はもう騙されない！②

会社名をネット検索してみる

(**電話番号**検索も有効)

私はもう騙されない！③

個人名義の口座に振り込まない

（外国人・日本人不問）

3つのポイント　まとめ

その1　商品画像検索 → ネット上に複数存在 ！

その2　会社名を検索 → 詐欺サイト！

その3　振込口座確認 → 個人口座！

インターネットバンキングマルウェア

- 標的型メール（添付ファイルやリンクのURL）

「DreamBot」（ドリーム・ボット）

金融機関のインターネットバンキング用認証情報を窃取するなどの機能がある。

感染した端末から、インターネットバンキングにログイン

→「セキュリティ上の理由」を装う偽画面

→ ID・パスワードを窃取

感染チェックサイトの紹介

- JC3（日本サイバー犯罪対策センター）

→ 「JC3」 「感染チェック」で検索！

ウイルス感染を確認して被害防止！

対策①

- **ワンタイムパスワード**
  - ① キーホルダー型の「セキュリティトークン」
  - ② スマートフォン用アプリの「ソフトウェアトークン」

- **二経路認証**
  - ① パソコンで振込・振替データを作成・確定
  - ② スマホでワンタイムパスワードアプリを起動、ログイン

対策②

＜完全分離＞

- インターネットやメールをするPC
- インターネットバンキングに使うPC

例：お金を扱う端末　→　専用のタブレット端末
（WindowsOSよりもウイルス感染のリスクの低いOSを搭載した端末を数万円で購入）

対策③

金融機関が指定した正規の手順で

電子証明書

を利用すると、より有効な対策となります。

ありがとうございました。

今後とも、県民の被害を防止するため、お力を貸していただきたいと思います。

よろしくお願いいたします。