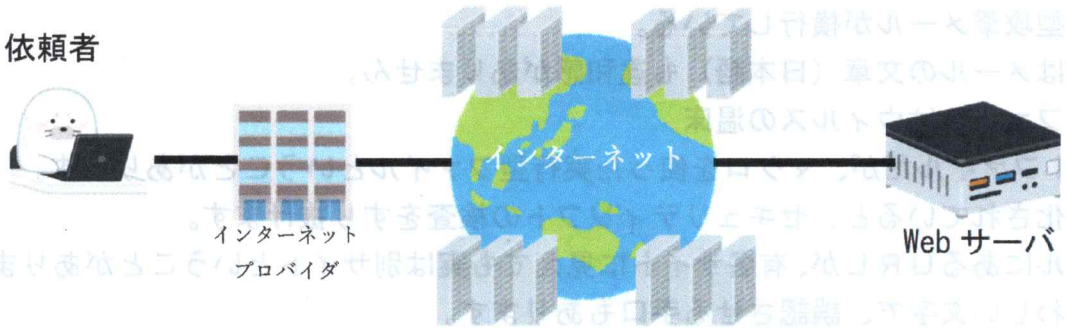
ネットワークセキュリティの防犯勉強会

印西市防犯組合牧の原支部　　２０２５年９月

～自分の身は自分で守るしかありません～

◎　インターネットは便利なネットワーク（実は犯罪者にも便利なのです！）

皆さんが使っているインターネットで世界中のネットワークが利用できます。
インターネットで買い物や送金も利用可能です。



ＵＲＬというインターネット上の住所を頼りに目的のサイト（サーバ）と通信します。
データには、依頼者の端末へ届けるための情報も含まれています。

＜安全ポイント＞

★盗聴防止のためインターネットのＵＲＬを確認しよう！

http://www　暗号化されていない

https://www　暗号化されている　　（安全なサイトとは限らない）

★ＩＤ・ＰＷはしっかり管理しよう！

★サーバ証明書を確認しよう！

鍵マークをクリックするとサーバ証明書が表示されます。（下図は Edge の場合）

◎　電子メールは、なりすまし可能です

どこにでも誰にでも届く便利なツール。
メールには、便利な機能が盛りだくさん。
・差出人を変更出来ます。（詐称が可能）
・添付ファイルを付けられる。（ウィルスも付いてくる）
・ＵＲＬを直付けして、直接Ｗｅｂ画面に移れます。（フィッシングサイト等）

＜危険ポイント＞
■電子メールは、原則平文です。（暗号化されていません）
メールサーバ管理者は読み放題です。
■標的型攻撃メールが横行している。
最近はメールの文章（日本語）も違和感がありません。
■添付ファイルはウィルスの温床
Excel ファイルだが、マクロを使った実行型ファイルということがあります。
暗号化されていると、セキュリティソフトの検査をすり抜けます。
■メールにあるＵＲＬが、有名サイトに見えても実は別サイトということがあります。
紛らわしい文字で、誤認させる手口もあります。
yahoo.co.jp　→ YAHOO.CO.JP
apple.com　→ app1e.com
amazon.co.jp → arnazon.co.jp

＜安全ポイント＞
★差出人名ではなく、差出人のメールアドレスを確認する。
★電子署名やＳ／ＭＩＭＥを確認する。（改ざん検知・暗号化）
★添付ファイルは開かない。（知人でも危険です）
迷惑メールフォルダに入れてから開くと安全です。（Outlook の場合）
Zip などで暗号化されているファイルは、さらに危険。
★メールのＵＲＬをクリックしない。（フィッシングサイト等へ誘導）
★メールに個人情報を直書きしない。
★不安をあおるメールや急がせるメールは、特に注意が必要。
★特定のメール以外は、メール受信ルールにより迷惑メールフォルダで受信する。

◎　ＳＭＳは注意が必要（スミッシング）

電話番号宛てに送れるので、電話の所持者に届きます。
ネットでの申込時等にＳＭＳを利用してコードが送られてきます。

＜危険ポイント＞
宅配業者を装った通知が送られました。
内容は、「ご本人様不在のため、お荷物を持ち帰りました。ご確認ください。」とＵＲＬが書かれていました。
そのＵＲＬにアクセスすると、ウィルスに感染させるサイト等に繋がります。
また、「ご利用料金の支払い確認が取れておりません。本日中に 050-****-**** ＊＊フィナンシャルサービス迄ご連絡ください。」という内容も確認されています。
電話番号に折り返しかけると、振り込め詐欺にあったりする場合があります。

＜安全ポイント＞
★書かれたＵＲＬをクリックしない。
★表示されている番号に折り返しの電話をしない。
★すぐに削除する。

◎　検索連動型広告

インターネットで検索を行うと、その検索ワードから広告が表示されます。
この広告は、入力された検索ワードを元に、登録されたサイトを表示します。
この表示された広告をクリックすると、広告主から広告料が支払われます。
高い広告料を払えば、優先的に表示されますので、犯罪者はこの制度を利用し、偽サイトに誘導できるよう、広告料を高く設定して優先度を上げています。

＜安全ポイント＞
★広告をクリックするのではなく、そのサイトに直接アクセスしましょう。

◎　ＳＮＳで気軽に情報発信

Facebook、X、Instagram、YouTube やブログ等で、今や誰でも簡単に情報発信ができてしまいます。

友人、知人に近況報告をしたり、自分の趣味などを全世界に情報発信できます。

＜危険ポイント＞

■誹謗中傷が行われている。
■偽の情報等に惑わされたり、偽の情報を発信してしまう。
■ロマンス詐欺や投資詐欺に巻き込まれる。
■記述内容により炎上して、個人情報がアップされることがある。
　→事件に巻き込まれることも・・・。
■複数のＳＮＳから個人が特定される。（ストーカー被害も発生）
■画像データやリアルタイム発信（生配信・つぶやき等）により場所が特定される。
■インターネット上に出た情報は取り消しが出来ない。（デジタルタトゥー）
■ＳＮＳの個人情報が漏れる。（FaceBook 事案）

＜安全ポイント＞

★ネット上の情報は、そのまま信用しない。（客観的事実を確認）
★一部でも個人情報につながる書き込みをしない。
★利用範囲を狭い範囲にする。（これは現実的でないか・・・）
★実際に会ったことのない人にお金は送らない。
★画像データにＧＰＳデータを付けない。
★自宅近辺の画像データやリアルタイムの情報発信は避ける。

◎　Free-Wifi を使用時は個人情報等入力不可

Free-Wifi は通信料を使わずにインターネットに接続でき、お金もかからずにたいへん便利です。

＜危険ポイント＞

■パスワードのない Free-Wifi は、通信内容が盗聴されている場合があります。
■個人が勝手に設置している Free-Wifi もあります。

＜安全ポイント＞

★Free-Wifi を利用するときは、個人情報を入力しない。
★インターネットバンキングへのログインや送金等の操作は止めましょう。

◎　QR コードには注意

QR コード決済は、とても便利です。飲食店での注文や寺社のお賽銭にも QR コードが使われています。また、Web サイトを直接参照できるので便利です。

＜危険ポイント＞

■QR コードは、読み取り後のサイトを確認している人が少ない。

■QR コードが張り替えられていると、偽サイトや詐欺サイトに誘導され、ウィスルをダウンロードされたり、勝手に送金されてしまう。

＜安全ポイント＞

★QR コードが差し替えられていないか確認をする。

★投げ込み等のチラシなどの QR コードは利用しない。（野良 QR コードも危険）

◎　匿名投稿による誹謗中傷

匿名投稿による誹謗中傷が、よくニュースになっています。本当に匿名でしょうか。

データを発信すれば、発信者と受信者の情報のやりとりがネットワーク上で行われており痕跡が残っています

裁判所による情報開示請求等の手続きが必要の場合がありますが、発信した端末の特定は、ＩＰアドレス、ＭＡＣアドレス、ポート番号等により判別可能です。

発信された情報は、匿名ではありません。

＜安全ポイント＞

★誹謗中傷は、いいことがありません。絶対にやめましょう。

◎　パスワードはあなたを証明するカギです。

不正利用や被害にあわないため、しっかりと管理しましょう。
不正ログインの試みは、日常的にあると思ってください。

＜攻撃方法＞

■ブルートフォースアタック
あるＩＤに対して、パスワードを複数回入力する。
→パスワードを一定回数間違えるとログインできなくなる。

■リバースブルートフォースアタック
パスワードを固定にして、ＩＤを変えていく。
→１つのＩＤに１回しかアクセスしないので不正アクセスに気づきにくい。
定型区のパスワードは危険。

■パスワードリストアタック
他のところの情報漏洩データをもとに不正アクセスを試みる。
→１つのＩＤに１回しかアクセスしないので不正アクセスに気づきにくい。
＝例＝
あるサイトでＩＤ（メールアドレス）とパスワードの情報漏洩が発生。
このサイトは対応策を実施するが、情報は漏れたまま。
メールアドレスをＩＤとする他のサイトに、不正入手したＩＤとパスワードで不正アクセスを試みる。

＜安全ポイント＞

★類推できるパスワードは使用しない。
電話番号、生年月日、名前等個人から類推できるもの。
★定型句なパスワードは使用しない。
Password、qwertyui、12345678 など。
★パスワードの桁数は多いほど安全性が増します。
できれば８桁以上にしてください。（推奨１５桁）
★英（大文字・小文字）、数字、記号を組み合わせる。
大文字は途中に入れたほうが効果的。（inZai など）
★違うサイトで同じパスワードを使用しない。
他所の情報漏洩から２次被害を出さない。

同時に実施

◎　ジュースジャッキング（チョイスジャッキング）

空港や新幹線など、USB 接続で充電できる装置が付いていて、バッテリーの残量を気にせずネットワークに接続できます。

＜危険ポイント＞

■スマホのデータがハッキングされます。
■ウィルスを仕込まれ、スマホが乗っ取られます。
■アメリカでは公衆の USB ポートを使わないようにアナウンスしている所もあります。

＜安全ポイント＞

★USB ケーブルは充電専用のケーブルを使う。
★モバイルバッテリーに充電する。

◎　発信者番号スプーフィング

いわゆる「ナンバーディスプレイ」で表示される電話番号です。NTT がデジタル交換機を IP 電話用に変更しました。汎用的な通信方式となりました。契約者側は何も変更することはありません。（詐欺に注意）一部のサービスは廃止になりましたが、ナンバーディスプレイは継続されています。

＜危険ポイント＞

■警察からの電話の下４桁は「0110」であることが多いですが、IP 電話になったことで詐称できてしまう。

＜安全ポイント＞

★表示された電話番号を信用しない。
★お金の話やクレジットカード等の話が出たら電話を切る。
★警察に相談する。
★番号を調べて、折り返しで電話をかける。

本日のまとめ

◎　ネット犯罪は、攻撃者・犯罪者が有利です。防御は後手・・・。

◎　犯罪者になることがないように、自分の身は自分で守りましょう。

★正しいサイトにアクセスしよう！
★インターネットで個人情報やＩＤやパスワードは安易に入力しない！
★リアルタイム情報や画像の投稿には注意しよう！
★パスワード管理は厳重にしよう！
★ＯＳやプログラムのアップデートはしっかり行う！
★セキュリティソフトのバージョンは常に最新にしよう！
★メールに書かれているリンクや添付ファイルをむやみにアクセスしない！
★インターネットは匿名ではない。誹謗中傷はやめよう！
★押し返しの電話は、電話番号を調べてからかけましょう！

◎　利用者に便利なサービスは、犯罪者にとっても便利なサービスです。注意しながら利用しましょう。

◎　インターネットには危険が潜んでいると自覚して利用しましょう。

資料作成　印西市防犯組合牧の原支部　石川延幸