しておくことです。利用者のパソコンにインストールされている主なアプリケーションのバージョンが最新であるか分からない場合は、簡単な操作で確認できるツールが無料で公開されています。　※独立行政法人情報処理推進機構（ＩＰＡ）　ＭｙＪＶＮ　バージョンチェッカ

②標的型メール

サイバー空間では、政府機関や企業など標的となるコンピューターやネットワークに不正に侵入して機密情報を盗み出したり、データの破壊、改ざんなどを行ったりして、大きな被害をもたらすサイバー攻撃も起きています。一般の個人ユーザーが使っているパソコンが気が付かないうちに狙われ、犯罪者の活動に荷担してしまう可能性があります。さらに、組織の機密情報を盗み出すために組織内の個人を狙ったサイバー攻撃も発生しています。

事例：組織の機密情報を盗み出す場合、攻撃者はある社員が使っているパソコンに実在する社員の名前を騙って打合せの資料など、疑いを持ちにくい内容のメールを送ります。実は、このメールには不正プログラムを含むファイルが添付されています。これが標的型メールと呼ばれるものです。標的型メールに添付されているファイルを開くと受信者パソコンは不正プログラムに感染してしまいます。パソコンに入り込んだ不正プログラムはインターンネット経由で、攻撃者があらかじめ準備したサーバーと通信を行います。攻撃者はサーバーを介して感染したパソコンに命令を送ることができるようになり、パソコンは攻撃者に乗っ取られた状態となるのです。こうして攻撃者は、パソコンに入っている情報や通信を盗み見て得られた情報を使い、より機密情報をもつ他の社員のパソコンや社内ネットワークへ侵入し、企業の重要な情報を盗み出していきます。実際に、平成２４年中には、１００９件の標的型メールが日本の民間業者等に送付されていました。攻撃者は、機密情報を保有する組織のセキュリティをかいくぐるため、関係しそうな人物に次々に攻撃を仕掛けており、誰もが狙われる可能性があります。重要な情報を扱っていないからといって、標的にならないと安心してはいけません。

対策：パソコンの防御を強固にすると同時に、メールの添付ファイルを安易に開かない。メールやＳＮＳなどで、メッセージに添えられたリンクを安易にクリックしないなど、サイバー攻撃者が仕掛ける罠に近づかないようにすることが大切です。

③スマートフォンと不正アプリケーション

サイバー空間を使った犯罪者の攻撃対象は、パソコンだけではなく、パソコンに近い性質を備えた携帯端末であるスマートフォン、タブレット端末にも広がっています。スマートフォンが不正プログラムに感染し、端末上の情報を盗み取られたり、詐欺サイトで情報や金銭を盗まれたりするリスクはパソコンと同じです。平成２４年には、スマートフォンに対する不満や不安を解消する電波改善、バッテリー管理などの便利ツールを装って不正なアプリケーションをインストールさせる手口が登場しました。

アンドロイド端末に感染する不正アプリケーションの数
平成２３年１２月時点で、　１，０００個
平成２４年１２月時点で、３５０，０００個

対策：不正なアプリケーションの被害にあわないための対策としては、通信事業者などが運営するアプリケーションの審査、不正アプリケーションの排除を実施している信頼できる場所からアプリケーションをインストールしましょう。スマートフォンやタブレット端末を利用する場合は、ウィルス対策ソフトを導入する事も大切です

３．まとめ

サイバー空間の危険性は、決して他人事ではありません。
パソコンやスマートフォンを安全で快適に利用するためにも、利用者一人ひとりがサイバー空間に潜むリスクに対する正しい知識と予防の実践が重要です。

社会奉仕基金 3,364円　　《会報編集委員》高橋 修・織田証・大川隆永・渕上啓太

2013 — 2014年度

国際ロータリー第2790地区第12分区

松戸北ロータリークラブ

四つのテスト

言行はこれに照らしてから
１・真実かどうか
２・みんなに公平か
３・好意と友情を深めるか
４・みんなのためになるかどうか

第1991回　例会 2013年11月26日（火）

■国際ロータリー会長　ロンD.バートン
■第2790地区ガバナー　関口 徳雄
■第12分区ガバナー補佐　渡辺 敏弘
■松戸北ロータリークラブ会長　児山 守治
■松戸北ロータリークラブ幹事　平田 洋一
■例会日－ 毎週火曜日12：30より（第1例会18：30）
■例会場－ 松戸市八ヶ崎1-10-6　「びわ亭」
■事務所－ 松戸市八ヶ崎1-11-13　ｻﾝﾗｲｽﾞﾊｲﾂ101
■TEL/FAX- 047-711-5950 / 047-711-5910
■Web/Mail- www.rc2790-12.jp / kanji@rc2790-12.jp

＜第1991回:例会プログラム＞

12:30　点鐘　児山守治会長
ロータリーソング斉唱　【♪我等の生業】
12:33　お客様紹介　崎谷延好会長エレクト
12:35　会食
12:55　例会再開
会長挨拶･報告　児山守治会長
13:00　幹事報告　平田洋一幹事

13:05　卓話　千葉県松戸東警察署　生活安全課
「インターネット犯罪の現状と対策」について　警部補　堀出知弘様
巡査　宗像将史様

13:25　【委員会報告】
◆ 社会奉仕委員会　高崎卓哉委員長
本日の社会奉仕基金発表
◆ ニコニコ委員会　小林弘委員長
本日のニコニコ発表

13:30　点鐘　児山守治会長

＜会長挨拶：児山守治会長＞

皆さん　ご機嫌如何でしょうか？
晩秋の候　一段と寒さが身にしみてまいりました。どうぞお身体ご自愛いただきたいと思います。
　本日は卓話がございますので挨拶は短くしたいと思います。
後程　実践的な卓話が聞けることを楽しみにしております。
東警察署の皆様は年末お忙しい中、卓話に来て頂きまして真にありがとうございます。
　さて、フィリピンでは台風30号の被害で多数の方が亡くなったり、被災された人がたくさんおります。亡くなられた方々のご冥福をお祈り申し上げます。
RI本部からも、義援金の協力の要請の通知が届いております。
この件につきましては12月3日の理事会を経て、協力させていただきたいと思います。
本日の例会、宜しくお願い致しまして、挨拶とさせていただきます。

＜幹事報告：平田洋一幹事＞

◆松戸ローターリークラブ:
平成25年12月18日(水)･･･クリスマス家族例会に変更
点鐘　18:30
場所　聖徳大学　生涯学習貢献センター14F
松戸市松戸1169　℡　047-309-5300
平成25年12月25日(水)･･･定款第6条第1節により休会
平成26年1月1日(水)･････祝日のため休会
◆2013年12月のロータリーレートは、1ドル＝100円です

■ロータリーの奉仕哲学「超我の奉仕」Service above self■
　このServiceの意味は人のためにつくすこと。ビジネスでもServiceの心がけはシェルドンの言葉を借りれば「永続的な顧客を得る道」であり、信用を増して繁栄への道につながる。

WEEKLY REPORT

＜卓話:千葉県松戸東警察署･生活安全課:警部補:掘出知弘様＞

「サイバー犯罪の現状と対策」について

1．サイバー犯罪の現状

　平成２４年中はサイバー犯罪が多発するとともに、インターネットを利用した犯罪予告・ウィルス供用事件（一連の誤認逮捕事件）やインターネットバンキングに対する不正アクセス事件、スマートフォンアプリを悪用した個人情報の流出事件（電話帳流出アプリ）等が発生し、その脅威が深刻化している状況にあります。
　事実、２４年中にインターネットホットラインセンターが受理した違法情報該当件数は、３万８９３３件で、前年より6.5%増加しました。また、２４年中のサイバー犯罪の検挙数は７３３４件と前年に比べて27.7%増加と過去最高を記録し、さらに１４年中の１６０６件から１０年間で4.6倍となりました。
　具体的な内訳は
★他人のＩＤやパスワードを盗んで他人になりすましてサイトにアクセスする不正アクセス禁止法違反事件は、全国で５４３件
★コンピューターウィルスを作成したり保管したり提供したりするウィルスに関する罪の検挙件数は、全国で１７８件
★ネットワーク利用詐欺や児童ポルノ、わいせつ物に関する罪、ネットワークを利用した脅迫や名誉毀損等の犯罪が全国で６６１３件
　となっています。
　このような、私たちに身近で直接の被害に遭いやすい犯罪のほか、政府機関、重要インフラ事業等の基幹システムを機能不全に陥れ、社会の機能を麻痺させるサイバーテロや情報通信技術を用いて政府機関や最先端技術を有する企業から機密情報を窃取するサイバーインテリジェンスといったサイバー攻撃が世界的規模で頻発するなど、サイバー空間における脅威は深刻化している状況にあります。

2．事例紹介と対策

①フィッシング事案(ネットバンキングに対する不正アクセス)
◆偽メールからの誘導
事例:　インターネットバンキング利用者のもとに、銀行の名前でメールが届きます。メールの内容は「重要なお知らせ」として、セキュリティ向上に伴うシステム変更のため、IDとパスワードを再登録してください。と書かれていて、再登録用のサイトURLも表示されていました。そのため、メールの指示通りに情報更新のためのサイトにアクセスしてIDとパスワードなどの情報を入力し、再登録の手続きを行いました。その後、しばらくして預金口座から預金が不正に引き出される被害にあってしまったのです。
　フィッシングとは、金融機関などからの正規のメールやウェブサイトを装い、IDやパスワードなどを盗み取る手口で、平成23年は約3億円の被害が確認されています。
対策:　メールに表示される送信者の名前は簡単に詐称できるので実在する金融機関名が表示されているからといって油断せずに慎重に取り扱う事が重要です。金融機関やクレジット会社が個人情報を電子メールで紹介することはありませんので、もし不審なメールが来たら、当該金融機関のホームページから問い合わせ窓口に確認しても良いでしょう。
◆偽画面を利用した手口
事例:　インターネットバンキングの偽の画面を利用した手口としては、まず、ウィルスを添付したメールを受け取ったり、ウィルスが埋め込まれたウェブを閲覧した利用者のパソコンにウィルスを感染させます。そして、ウィルスに感染したパソコンで正規のインターネットバンキングのサイトにログインしようとすると、途中から偽の画面が現れます。利用者は偽の画面だと気付かずに乱数表や合言葉などを入力してしまいます。こうして入力された情報は悪意のある者へ渡ってしまう仕組みになっています。
対策:偽の画面に騙されないためには、とにかく利用者がウィルス感染からパソコンを防御すること。そしてインターネットバンキングを利用するときに、普段と違う情報を求めているなどの不自然さはないか等注意を払う事で被害に遭う可能性は低くなります。パソコンをウィルス感染から防御するための対策としては、必ずウィルス対策ソフトを導入し、またOSやインストールしているアプリケーションを最新の状態に