ＢＳＫ第２７－５号

インターネット・ソーシャル・ネットワーキング・リスクについて
― ＳＮＳを利用する上でのリスク ―

FBI Counterintelligence brochure （ＦＢＩ対情報啓発資料）
[Internet Social Networking Risks]

平成２７年９月

公益財団法人　防衛基盤整備協会

はしがき

本小冊子は、２０１５年７月現在で米国連邦捜査局（ＦＢＩ）が、対情報活動のためにウェブ上で公表している９件の一般向け啓発資料のうち、"Internet Social Networking Risks"を「インターネット・ソーシャル・ネットワーキング・リスクについて―ＳＮＳを利用する上でのリスク―」と題して翻訳したものです。

本件は、インターネットの発達によって、インターネット・ソーシャル・ネットワーキング・サイト（ＳＮＳ）が人と人を結びつけ、人々が空間の制約を超えて交流することのできる場を提供していますが、そこでは善良な人々ばかりではなく、詐欺師や犯罪者たちが活動しており、その犯罪者たちの餌食となることの無いように、警鐘を鳴らし、対策を提言する啓発資料です。

個人の情報流出は、直接的な個人の被害ばかりではなく、その個人の勤務する会社、所属する組織及びその顧客に甚大な損害を与える場合があり、その個人を守るためばかりではなく、勤務する職場を守るためにも、会社ぐるみで取り組むべき課題でもあります。

本資料では、犯罪者の使う様々な手口について詳しく解説し、我々に注意喚起してくれるとともに、個人や職場が行うべき予防策についても具体的に述べており、我々が、インターネット犯罪の被害者となることを防ぐ大変有益な資料であると思われます。本小冊子が我が国の情報セキュリティ体制の向上にいささかでも貢献できれば幸いです。

平成２７年９月

公益財団法人　防衛基盤整備協会

理事長　宇田川新一

FBI Counterintelligence brochure　（ＦＢＩ対情報啓発資料）
[Internet Social Networking Risks]

「インターネット・ソーシャル・ネットワーキング・リスクについて
― ＳＮＳを利用する上でのリスク ― 」

公益財団法人　防衛基盤整備協会　訳

１．　はじめに

インターネット上のソーシャル・ネットワーキング・サイトは、社会的に人と人を結びつける上で、革命を引き起こしました。しかしながら詐欺師や、犯罪者、その他の不正直な者たちが、極悪な目的のために、この人と人を引き合わせる能力を悪用しています。

オンライン・ソーシャル・ネットワークを悪用するために、主に二つの戦術が用いられています。

①あなたのコンピュータ又は電話にアクセスしたり、望んでいないソフトゥエアをインストールするためのコンピュータプログラムを作成したり操ったりすることに特化したコンピュータに精通したハッカーたちがいます。

②ソーシャルネットワークを通じて、人脈を悪用することに長けたソーシャル又はヒューマンハッカーたちがいます。ソーシャルハッカーは、社会交流（対面、電話又は文章での）を通じて人を操る「ソーシャル・エンジニア」とも呼ばれています。

人間は、サイバーセキュリティにおける弱点であり、ハッカーやソーシャル操作者はそのことを知っています。彼らは、人をだまして古いセキュリティ・ウォールを入手させようとします。彼らはまた、自分たちの行動を、無害で合法であるかのように見えるように体裁を調えています。

オンライン詐欺やコンピュータ・ハッキングに引っかかるということは、個人的に被害者として損害を被るばかりでなく、被害者が勤務する組織に対しても損害を与えることになります。
例えば、次のようなリスクがあります。

・ＩＤ窃盗／なりすまし
・ハラスメント
・同僚からの圧力
・失職
・会社の評判下落

・個人の評判の下落
・データやネットワークへの損害
・知的財産窃盗／データ窃盗
・ブランド乗っ取り
・生産の遅延や中断
・収益や収入の減少
・侵入窃盗
・スパムやフィッシングのターゲット
・ウェブサイトのコンテンツ変更
・マルウェアとウィルスの散布

ソーシャル・ネットワーキングの場を通じて、人が情報を提供したり、情報にアクセスする許可を与えてしまうように、騙すための戦術には沢山のものがあります。全てを網羅しているわけではありませんが、この小冊子は、これらの内のいくつかを取り上げ、オンライン・ネットワーキング・リスクを軽減する方法を紹介します。

例１
・あなたの利用しているソーシャル・ネットワーキング・サイト上の友人から、あなたは１通のメッセージを受け取ります。そのメッセージは、あなたに他のサイトのビデオをレビューするように指示します。あなたがそのサイトに行くと、ポップアップメッセージが現れ、ソフトウェアを更新するためにダウンロードする必要があると語ります。しかしながらそのソフトウェア更新は、本当は、一度ダウンロードしてしまうとあなたのコンピュータのコントロールを、マルウェアの制作者に引き渡してしまうマルウェアなのです。（いくつかの事例では、単にそのサイトを訪問しただけで、マルウェアをダウンロードしてしまいます。）その後、マルウェアは、ソーシャル・ネットワーキング・サイト上のあなたの全ての「友人」に、マルウェアの仕込まれているその同じサイトを訪問するよう仕向けるメッセージを送信してしまいます。マルウェアの制作者は、直ぐに、いわゆるボットネットと呼ばれる、彼らのコントロール下に置く複数のコンピュータを手に入れることになります。

２．　ソーシャル・ネットワーキング・サイトの脆弱性

ソーシャル・ネットワーキング・サイトとは、人々がグループ内で交流したり情報を共有することのできるインターネットベースのサービス

のことです。

リスク：
・一度情報がソーシャル・ネットワーキング・サイトに掲示されたら、それは最早プライベートなものではなくなります。より多くの情報を掲示すればするほど、あなたはより脆弱になります。たとえ高いセキュリティ設定をしたとしても、友人あるいはウェブサイトが、不注意であなたの情報を漏えいさせるかもしれません。
・あなたが共有した個人情報が、あなたやあなたの友人に対して攻撃するのに使用される可能性があります。より多くの情報が共有されればされるほど、誰かがあなたをかたり、あなたの友人をだまして、個人の情報を共有させたり、マルウェアをダウンロードさせたり、制限されたサイトにアクセスするよう仕向けたりされる可能性が高くなります。
・略奪者、ハッカー、ビジネス上の競争者や外国政府の要員は、付け入るためのターゲットとなる人物や情報を探して、ソーシャル・ネットワーキング・サイトをうろつきまわっています。
・ソーシャル・ネットワーキング・サイトで拾い集めた情報は、ソーシャル・ネットワーキング・サイトの通常の方法では使われないようなやり方で、特別な攻撃を仕掛けるために利用されるかもしれません。

戦術：
「Baiting：おびき寄せ・餌撒き」
・誰かがあなたに、マルウェアを仕込んだＵＳＢドライブや他の電子媒体をくれるかもしれません。そして、あなたがそのデバイスを使うことにより、あなたのコンピュータを乗っ取ることが出来ることを期待しているのです。
・あなたは、いかなる電子的記憶媒体であれ、その出所が正統で安全であることが分かっている場合でなければ、使ってはいけません。そして、使用前には、全てウイルスチェックをしてください。

「Click-jacking：クリック・ジャッキング」
・クリックできる正規なコンテンツの下に、もしクリックしてしまうと、マルウェアをダウンロードしたり、サイトにあなたのＩＤを送信してしまうことを、知らない間に実行してしまうような隠されたハイパーリンクが張られていることがあります。大量のクリック・ジャッキング詐欺が、ソーシャル・ネットワーキング・サイトの「好き」ボタンや「共有」ボタ

ンに仕掛けられています。
・あなたが使っているインターネットブラウザが何であれ、スクリプティングとアイフレームを無効にしてください。

「Cross-Site Scripting(XSS)：クロスサイト・スクリプティング(XSS)」
・悪意のあるスクリプトコードが、有益な又は信頼できると思われるウェブサイトに、仕込まれていることです。
・格納型ＸＳＳ攻撃は、悪意のあるスクリプトコードを攻撃者あるいは第三者のサーバに、永続的に格納して行う攻撃です。ユーザーが閲覧のためにサイトに格納されたデータを要求すると、悪意あるスクリプトコードを含むコンテンツが返信され、それを実行することでユーザーのコンピュータが感染させられるというものです。
・反射型ＸＳＳ攻撃は、ユーザーが悪意あるリンクをクリックするよう騙すことで行う攻撃です。ユーザーがそのリンクをクリックすると、ユーザーはそのサイトから、悪意あるスクリプトコードを挿入された新たなリクエストを、スクリプトを排除しないという欠陥を持つウェブサイトに転送されます。その欠陥を持つサイトからは、その悪意あるスクリプトコードが今度は実行可能な状態でユーザーのコンピュータに返信され、感染してしまいます。ユーザーのコンピュータは、そのスクリプトコードを信頼できるソースからのものと見なして実行してしまうからです。
・全てのウェブサーバの「ＨＴＴＰトレース」サポートを、無効にしてください。そして、更に、ＸＳＳ攻撃の被害者にならないための方法を探してください。

「Doxing：個人情報の盗み取り」
・氏名、誕生日、住所及び写真を含む公開されている、個人を特定可能な情報は、当然のことながらソーシャル・ネットワーキング・サイトから検索して取得されます。
・あなた自身や家族、友人について、どんな情報をあなたが共有（オンライン上で、印刷物で、対面で）しようとしているかについて、注意深くなってください。

「Elicitation：情報の聞き出し」
・本人たちに、自分たちが尋問されていると感じさせることなく、人々の情報を引き出す戦略的な会話の使い方のことです。
・聞き出し戦術つまり、ソーシャル・エンジニアが個人情報を入手しよ

うと試みるやり方に気づいてください。

「Pharming：なりすまし」
・正規のウェブサイトではなく、不正サイト（例えば偽の銀行ウェブサイト）へ、秘密データを抜き取る目的で、ユーザーに接続させることです。
・ウェブサイトのURLsを良く見てください。スペルやドメインネームが少し違うかもしれません。あるいは、「.gov」ではなく「.com」となっているかもしれません。リンクをクリックするより、ウェブサイトのアドレスを直接入力するようにしてください。

例２
・ほとんどのコンピュータ感染は、ウェブサイトからのものです。ウェブサイトを訪れただけで、例えあなたがファイルやプログラムをダウンロードしなくても、マルウェアにあなたのコンピュータをさらすことになります。正規のサイトが気づかないうちに感染させられているかもしれません。
・有名人に関する情報や最新の注目されるニュース関連事項を掲載するウェブサイトは、しばしば犯罪者によってハイジャックされます。いや、犯罪者たちが、獲物をおびき寄せるために、そのようなサイトを立ち上げます。

「Phishing：フィッシング」
・通常正当な組織や個人から来たかのように見えるＥメールですが、実はそうではなく、マルウェアのリンクやファイルが添付されています。典型的なフィッシング攻撃は、ランダムに被害者を引っかけるために行われます。スピア・フィッシング攻撃は、特定の個人や組織をターゲットとして行われます。
・あなたの知らない人から送られてきたＥメールやＥメールの添付ファイルを開いたり、Ｅメールに添付されているリンクをクリックしてはいけません。もし疑わしいＥメールを知り合いから受け取った場合は、それを開く前に本人に確認してください。

例３
・２０１１年３月、ハッカーが、セキュリティ会社ＲＳＡ社の従業員の小グループに、２通のスピア・フィッシングＥメールを送りました。ハ

ッカーにとっては、一人の従業員が感染したファイルを開き、マルウェアを始動させるだけで十分でした。マルウェアは、ＲＳＡ社から情報をダウンロードし、その情報は、ハッカーがＲＳＡ社のセキュリティ・トークンをどのように破るのかを学ぶ助けとなりました。２０１１年５月及び６月に、多数の国防関連企業のネットワークがＲＳＡ社のトークンの脆弱性により破られ侵入されました。

「Phreaking：フリーキング」
・通信システムに対する非承認のアクセスを獲得することです。
・社内交換機に直接接続したり、公衆交換機を経由して公衆電話網に接続する、公開していない電話番号を提供してはいけません。

「Scam：詐欺」
・取引と見せかけて、他人からお金、情報、サービスを提供させるでっち上げの取引のことです。
・実際のところ、うますぎる話に思えたら、それはほとんど詐欺に違いありません。サイバー犯罪者たちは、人々に感染Ｅメールを開かせたり、感染ウェブサイトを訪問させたり、嘘のチャリティに寄付させたりするために、有名なイベントやニュースストーリーを利用します。

例４
・２０１０年のワールドカップ前に、サイバー犯罪者たちは、チケットを売りますとか、あなたにチケットが当たりましたとかというフィッシングＥメールを送りつけました。
・オサマ・ビンラディンの死後、ビンラディンの拘束された時の映像と称するビデオがフェイスブックに掲載されました。そのビデオは偽物で、ユーザーがそのビデオへのリンクをクリックすると、ユーザーは自分たちのブラウザのバーに Java スクリプトコードをコピーするように指示されました。それによって、自分たちの友人にこのうそを自動的に送信させられ、しかも自分たちのアカウントがハッカーたちによってフルアクセスされてしまいました。

「Spoofing：スプーフィング」
・自分のＩＤを隠したり、他人になりすまして、コンピュータやコンピュータユーザーをだますことです。Ｅメールスプーフィングは、偽のＥメールアドレスや本物に似せたＥメールアドレスを使用します。ＩＰス

プーフィングは、コンピュータのＩＰアドレスを隠したり、マスクしたりします。
・あなたの同僚や顧客を良く知ることで、会社情報や個人情報を得るために、スタッフメンバーやサービスプロバイダを騙る人物に気を付けてください。

３．　職場における予防策

・重層防御―コンピュータネットワーク全体に多層的セキュリティを施してください。
・今までにデータを失った事例を特定して、それらの脅威を減殺してください。従業員に対して、これらの脅威について教育し、必要であれば、将来の損失を防ぐために、彼らの行動をどのように変えるかを教育してください。
・あなたのネットワーク上のデータの動きを絶えず監視してください。
・会社ネットワーク上の侵入検知システムについての方針と手順を確立してください。
・ブログや個人のウェブページで、どこまで会社の情報を共有できるかについての方針を確立してください。
・従業員に対して、自分たちのオンライン上での行動が会社にいかにインパクトを与えうるかについて、教育してください。
・毎年、セキュリティ訓練を行ってください。
・疑わしい事象があった場合は、速やかに報告するように従業員に要請してください。

４．　追加の予防策

・あなたが保全したいと思っている情報は、インターネットにつながっているいかなるデバイスの中にも記憶させてはいけません。
・ソーシャル・ネットワーキング・サイトでは、常に高いセキュリティ設定にして、あなたが共有しようとする個人情報は非常に限られたものにしなければなりません。他の人が、彼らのオンライン会話の中で、あなたについて何を載せているかをモニターしてください。
・アンチウイルスソフトとファイアーウォールソフトを使用してください。あなたのブラウザとＯＳにパッチを当て更新し続けてください。
・定期的にあなたのパスワードを変更し、古いパスワードを再使用してはいけません。複数のシステムやサービスに、同じパスワードを使い回してはいけません。例えば、もし誰かがあなたのＥメールのパスワードを手に

入れた場合、その人物が同じパスワードで、あなたのオンラインバンキングにアクセスできるようになってはいませんか？
・後になってあなたが困ることになるかもしれないことや、あなたが見知らぬ他人に知られたくないことは、掲載してはいけません。
・あなたがやり取りしている相手を確かめてください。インターネット上では、誰でも身分を偽るのは簡単なことです。
・自動的にダウンロードしたり、ウェブサイトのコンテンツに回答したり、Ｅメールに返事しないでください。ソーシャル・ネットワーキング・サイトからのものだと称するＥメールメッセージに張られているリンクをクリックしてはいけません。その代り、直接サイトにアクセスしてメッセージを検索してください。
・信頼できる良く知られたサイトからのアプリケーションやソフトウェアだけをインストールするようにしてください。フリーソフトウェアにはマルウェアが仕込まれているかもしれません。アプリケーションが情報にアクセスできるようになる前に、どんな情報にアクセスすることになるか確かめてください。一度インストールした後は、更新し続けてください。もしもう使わなくなった場合は、削除してください。
・ＧＰＳ符号化機能を無効にしてください。多くのデジタルカメラは、撮影場所のＧＰＳ位置を符号化します。もしその写真がサイトに掲示されれば、ＧＰＳ座標が明らかとなるので、誰でもがその正確な位置を知ることとなります。
・可能であればいつでも、ウェブサイトとの間は暗号通信を行ってください。ソーシャル・ネットワーキング・サイトもあなたが暗号通信できるような機能を持っていると思います。
・公開の場で誰でも使用することのできるように設置されているコンピュータや一般の WiFi 回線を通してあなたの個人アカウントにアクセスするのは避けてください。
・会社や個人のデータを欲しがるような人物からの、対面でのあるいは電話での又はインターネット上での、こちらから求めたわけではないコンタクトには注意してください。
・あなたの銀行の取引記録、残高、クレジットカード報告書をモニターしてください。
・ユーザー名、パスワード、社会保険番号、クレジットカード、銀行情報、給料、コンピュータネットワークの詳細、セキュリティクリアランス、自宅及び会社の物理的セキュリティやその計画、業務用システムの能力や限界、スケジュールや旅行日程については、共有してはいけません。

◎注意！！

「正規のサービスあるいはネットワーク管理者は、決してあなたにパスワードを聞くようなことはありません。」

・「パスワードを忘れた方へ」の案内時に尋ねられる、本人確認のための質問に誰かが答えてしまうことが出来るような、あなた自身に関する情報を提供してはいけません。

・職場の肩書、住所、趣味、好き嫌い、家族や友人・同僚の名前や詳細のようなあなたが共有する個人情報は、良く考えたうえで、限られたものにすべきです。

5．　教育資料

沢山の組織やウェブサイトが、インターネット・ソーシャル・ネットワーキングの脅威から、あなたとあなたの職場をどのように守るかについて、更なる詳細情報を提供してくれています。

www.LooksTooGoodToBeTrue.com

www.OnGuardOnline.gov

www.us-cert.gov

www.ic3.gov

www.dhs.gov

www.ftc.gov

www.fbi.gov

平成２７年発刊資料

ＢＳＫ 第２７－４号『企業が国際共同開発に参加する場合の契約制度上の課題等(その２)』
ＢＳＫ 第２７－３号『防衛施設建設関係業務へのプロジェクト管理手法の導入に関する調査研究（平成２６年度)』
ＢＳＫ 第２７－２号『サイバーセキュリティのための水準の引き上げ（平成２７年３月)』
ＢＳＫ 第２７－１号『情報セキュリティの現状と動向について（平成２６年度)』
本報告書の中で意見にわたるものは、委託研究先の見解であることをお断りしておきます。

インターネット・ソーシャル・ネットワーキング・リスクについて
― ＳＮＳを利用する上でのリスク ―

平成２７年９月発行
非売品　　禁無断転載・複製
発　行　：　公益財団法人　防衛基盤整備協会
編　集　：　防衛基盤研究センター刊行物等編集委員会
〒160-0003　東京都新宿区本塩町２１番
電　話　：　０３－３３５８－８７５４　　ＦＡＸ　：　０３－３３５８－８７３５
メール　：　koueki@bsk-z.or.jp
ホームページ　：　https://www.bsk-z.or.jp

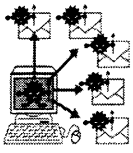
平成27年度情報セキュリティ川柳入選作品

主催　公益財団法人　防衛基盤整備協会

最優秀賞

友好が
写真アップで
絶交に

ペンネーム　友情報



佳作

そのサイト
白雪姫も
実は魔女

ペンネーム　三郎

佳作

「同意する」
規約長すぎ
ついボタン

ペンネーム　楓すず

佳作

四季問わず
国境超えて
サギの群れ

ペンネーム　三郎

佳作

『重要』の
疑似餌が踊る
詐欺メール

ペンネーム　ばいなりい

ヤング奨励賞

詐欺かもよ
そのワンタッチ
考えて

ペンネーム　頭川成葉