日吉の丘 Vol.19-20 合併号の名刺広告申し込みを受け付けます！　　2023.6.14

本部同窓会広報　　岩渕 雅俊(11 期)
大山 慎介(19 期)
森川 雅浩(30 期)
山口 甚晃(34 期)

首記の様に日吉の丘 Vol.19-20 合併号の名刺広告申し込みを受け付けます。

名刺広告申込み方法

申込みいただける方は、下記に従って応募ください。

1. 同窓会の口座にお振込み下さい。**名刺サイズが¥10,000、名刺を 2 枚横並びにした大きさで応募される場合は ¥20,000** です。この締切は **6 月末**とさせてください。
   振り込み先：下記のいずれかに手数料負担です振り込みください。

北洋銀行	ホクヨウギンコウ	
湯川支店	ユノカワシテン	
普通預金口座	**3456023**	
振込まれる方の名義に卒業期を併記ください	例	11 ﾊｺﾀﾞﾃ ﾀﾛｳ

「ゆうちょ銀行」でも可です。通信欄に「名刺広告」とお書きの上、卒業期とお名前をお書き下さい。

口座記号番号	**02760 1 101377**
加入者名	函館ラ・サール学園同窓会
通信欄に、「名刺広告」とお書きの上、卒業期とお名前をお書きください。	

2. 掲載内容を下記にお知らせください。電子メールの内容に記載いただくか、テキスト・ファイル、ワード、pdf など、お送りください。手書きしたものを郵送いただいても結構です。「名刺広告」とは言っておりますが「名刺」にはこだわりません。フリーフォーマットですが、最低でも卒業期と芳名は入れてください。ご連絡を頂けなかった場合は、期と芳名のみ記させていただきます。

E-mail	iwabuc2@khaki.plala.or.jp
郵便	222-0032 横浜市港北区大豆戸町 803-2 大倉山ハイム 7-405 岩渕 雅俊

今回の名刺広告募集の意図

「日吉の丘」Vol.19-20 合併号を、現在、編集中です。新しい時代を見据え、Vol.19-20 合併号より、函館ラ・サール学園同窓会の公開ページに、電子ファイル（pdf ファイル）の形にした「日吉の丘」を掲載することにしました。見易いカラー版で、一般公開に相応しい内容に致します。尚、オンライン版であると「見れない！」、字が小さすぎてスマホじゃ見辛いという OB の方が多々いらっしゃることを考慮し、或る仕掛けを用意しております。それが何かについては・・・・オンライン版のご案内の時（OB の方に郵送予定です）まで秘密です。

ちなみに、今回の記事は・・・・・・・

1.	「私家版ラサーリアン魂- 同窓会長より」	14 期	森 俊雅 会長
2.	前会長から・・・・	4 期	浜出 雄一さん
3.	「ラ・サールジャパンの創立者」	フェルミン・マルチネス先生	
4.	ブラザー・ランベール講演会 「パルメニー修道院の歴史と今」	2017/10/6 に東京で、函館ラ・サール学園と鹿児島ラ・サール学園共催で行われた講演の実録。	
	東京支部の広報誌に掲載した記事の再掲です。ラベル先生の紹介文（英語）も載せています。		
5.	「地域との絆を深めながら進めた会社の復活と新しい価値づくり」	20 期	野村 文吾さん
	2021/6/12 にオンラインで行われた東京支部同窓会で講演いただいたに内容の実録です。野村さんに掲載することについて快諾いただき、校正のご協力をいただいた版を掲載します。		
6.	『インターネットを、怖がらずに使いこなす為の豆知識』	11 期	岩渕 雅俊
	2012 年に東京支部の月例会で話し、東京支部の HP で公開していた内容を、刷新した記事です。		
7.	COVID-19 の 3 年、函館 OB ラサーリアンの軌跡	テーマを絞った、支部だよりです。	

サンプル

1 枠の場合の掲載イメージ

ある程度有効なんていうことはないので、別の修正になります。

過去に攻撃があったことに起因して、ソフトウェア製品の脆弱性が見つかるということはあるので、万全ではありませんが、「悪い事をするプログラム」の侵入を防ぐには、ちゃんとソフトウェア製品のアップデートをかけておくという事、アップデートの後は速やかにスキャンを行って、以前は見つからなかったマルウェアがあれば排除してもらうという事が、まずは大切です。

「悪い事をするプログラム」かもしれないということをダウンロードの前に見破る方法

インターネット上で提供されているプログラムは、有益なプログラムであれ、マルウェアであれ、しばしば圧縮された形で提供されており、ダウンロードさせたい側は、ホーム・ページ中にダウンロード用のボタンを作っておきます。

ユーザーがそのホーム・ページを見て、プログラムをダウンロードしようと決め、ブラウザーの画面に表示されたボタンを押すと、過去、何回かダウンロードをしていいのかどうか、「あなたがダウンロードしろと言ったんだよ！」という証拠を残すあ（笑）の確認メッセージが出てきて、それらに応えるとダウンロードが始まります。

この後、セキュリティ・ソフトが動いている場合、圧縮されているのであれば復元がされ、できたファイルの内容がスキャンされます。セキュリティ・ソフトってこんなことをしているんです。

セキュリティ・ソフトは、ファイルがウィルスで汚染されているか、内容が、過去に世界で報告されている「悪い事をするプログラム」だった場合、警告を出すか、ダウンロードしたファイルないしウィルスを削除してくれます。

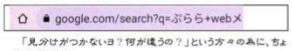
よって、セキュリティ・ソフトが動いていれば、一応は安心なのですが、未だ世界でも報告がされていない「悪い事をするプログラム」だった場合、警告程度は出るかもしれませんが、それにOKと応えるとダウンロードは完了し、圧縮されたファイルが解凍される際に、ワーム、トロイの木馬ないしボットの侵入を許してしまいます。

こういう眠に遭わない様にするには、どうしたらいいのか？結論を先に言います。

ホーム・ページを閲覧している時、画面の上を見てください。そこには文字列が表示されている筈です。

この文字列が「https://」始まっているホーム・ページの中にある「ダウンロード」ボタンであれば、信頼がおけます。ですから、パソコンでは「https://」始まっている事を確認してください。

スマホ（アンドロイド）では「どこにアクセスしているのか？」という情報が表示される場所（画面の最上段）に南京錠が閉じている絵（アイコン）が「https://」の代わりに出ます。



「見分けがつかないヨ？何が違うの？」という方々の為に、ちょっと説明します。

最近は、Google などが提供するホーム・ページに、キーワードを入れてアクセスすることが多いので、「えっ！」と思うかもしれませんが、ホーム・ページを閲覧するには、下記の例の様な指定（これを URI（ユニバーサル・リソース ID）と言います）をするのであり、Google などを使った場合は、ユーザーがタイプした値から URI を探してくれています。

URI はユニバーサル・リソース ID の略で、下記の構造になっており、IP アドレスが直接か間接かへっています。

ホーム・ページがサーバーから取り寄せられると、同様の値がブラウザーの一番上に表示されますが、http://と指定したのにhttps://に変わっていることがあります。

http://**www.example.com**/over/there
https://**www.example.com**/over/there

この例で「example.com」というのはホーム・ページを提供しているサーバーの IP アドレスに対応した値であり、その後の/over/there は、そのサーバーのどのフォルダーにホーム・ページがあるのかという情報です。

最初の「www」は、「ホーム・ページのアクセスだよ！」と相手に伝える為のキーワードで、その前の http://は「http（ハイパー・テキスト・トランスファー・プロトコル）という IETF で決めた規則に従って、データのやりとりをします！」という意味です。

「https://」は「http://」と何が違うかという点ですが、いずれも「どういう方式でホーム・ページを取得するのか？」という指定でスキームとなります。

「https://」という指定の場合、ホーム・ページの取得にかかる前に、ホーム・ページを公開しているサイトは、自分の「デジタル証明書」と言うファイルを送って来ます。

デジタル証明書とは、インターネットの世界の「身分証明書」であり、そのサイトが由緒正しいサイトであることを保証する組織が作ってサインをしたファイルです。

サイトから送られてきたデジタル証明書は、受け取った側にしてみると「勝手に送って来やがった！」ファイルなので、その内容が信じるに足るか否かを、まずは疑かる必要があります。

実は、この検証をインターネット・ブラウザーは自動的にやってくれるのです。そのデジタル証明書が、サイトで勝手に作った証明書か、有効期限が過ぎた証明書であると、インターネット・ブラウザーは警告のメッセージを出します。

どういう仕組みになっているかと言うと、デジタル証明書のサインは、証明した組織が持っている「秘密キー」で暗号化されているが故にサインになっているので、その組織のデジタル証明書を、インターネットで入手して、その中に入っている「公開キー」を使えば復号できます。復号してできた値と、サイトが送って来たデジタル証明書を要約した値が合致すれば、「サインは本物だ！」ということになります。

サイトが送って来たデジタル証明書のサインが由緒正しいか否を調べる為に取り寄せたデジタル証明書は、そのデジタル証明書を書いた組織がサインしていますので、その組織のデジタル証明書を書いた、更に上の組織のデジタル証明書が必要ということになり、これが何回か続く事になります。

xx 期　面館　次郎

xx 期の兄弟たちよ！同期会に集結しよう！
期日：xxxx 年 x 月 xx 日
場所：面館山山頂！

連絡先：abcdefg@abc.def.or.jp
090-1234-5678（日吉 麻吉郎）

横並び 2 枠の場合の掲載イメージ

実はインターネットでは、すべての、デジタル証明書のサインをした組織（認証組織）が、階層構造上のどこかに位置づけられており、インターネット・ブラウザーは、階層構造を下から上にたどって、認証組織のデジタル証明書を取得し、各々のサインが正しいかどうか検証してくれるのです。

公式のデジタル証明書を発行してもらっていないサイトは「https://」というスキームが指定された要求を受けた場合、私的なデジタル証明書を相手に渡すことはできますが、デジタル証明書がサイトで勝手に作った証明書か、有効期限が過ぎた証明書であると、警告のメッセージが出ますので、ここでボロがでます。

扨って、公式のデジタル証明書を持っていないサイトは、スキームとして「http://」を指定してもらわざるを得ないのです。こうすると警告は出ませんから…、でも、ユーザーにとってみると警告が出ないからこそ、最注意なのです。

必ず URI が「https://」で始まっていることを確かめてください。

時々、「本物そっくりの、偽のホーム・ページがあるので注意せよ！」という情報が流れてくることがありますが、如何に画面に応がるイメージはそっくりであっても、ホーム・ページの閲覧中にブラウザーの最上段に表示される URI の先頭が「https://」となっていなければ「偽もの だ！」と思ってください。

加えて、URI の先頭が「https://」になっているホーム・ページであれば、災われるメッセージが暗号化されますが、URI の先頭が「http://」になっているホーム・ページであれば、盗聴されるメッセージは暗号化されませんので、送信中に漏洩すると、内容が読み取られてしまいます。

どんなに見た目が本物の様に見えていても、URI が「http://」で始まっている場合、悪意あるサーバーの可能性があるので、個人情報を入力してはいけません、ダウンロードのボタンを押してはいけません。

デジタル証明書が送られてきていないのにダウンロード・ボタンを押した場合、セキュリティ・ソフトは「https://じゃないから危ない！」として（たぶん…）警告を上げます、それを無視してダウンロードすると、既知の「悪い事をするプログラム」などであればセキュリティ・ソフト中のファイルのチェックして、無毒化してくれますが、新手の「悪い事をするプログラム」などであれば、そのチェックをすり抜けてしまうのです。

既にボタンをクリックしてしまった、個人情報を入力してしまったという場合、パソコンであればブラウザーの右上にある x をクリックしてください。

スマホの場合は、常時ブラウザーが動いていますので、スマホをシャットダウンしてください。

フィッシング（Phishing）被害に遭わないために

次に、2010 年ころから増えた、フィッシングについてお話します。メールやホーム・ページにハイパーテキスト（下線がある文字列）があり、そこをクリックすると、あやしいサイトの偽のホーム・ページ、ないし危険したホーム・ページとは全く関係がないページが現れることがあります。

実は、ホーム・ページ上でハイパーテキストになっている箇所の裏に、本当に使われる URI が隠れており、ハイパーテキストで見える URI とは異なっている事があるのです。

「ハイパーテキストをクリックすると、どの URI にアクセスが行くか？」ということは、パソコンであれば、ブラウザー或いはメール・ソフトの機能を使って「ソース表示」すると（その箇所を探すのが簡単ではないものの）わかります。

画面で下記に表示されていて、指示通りにハイパーテキストをクリックしたとしてみましょう。

下記をクリックしてください！
https://www.todoshii.site/over/there
Good Job!

ひょっとして、とんでもないサイトのホーム・ページが現れるかもしれません、何故かとすると、ハイパーテキストとして表示されている文字列は、この例では URI の形になっていますが、ソースが下記の様になっているとすると、実際に暴承が飛ぶのは、別の URI（下記の href=に注目してください）なのです。

```
<p>下記をクリックしてください！</p>
<a href="http://x.x.x.x/bots/this">
  https://www.todoshii.site/over/there
</a>
<p>Good Job!</p>
```

こういう手法で、悪いサイトにユーザーを導いて個人情報などを盗むことをフィッシングと言い、そういうサイトをフィッシング・サイトと言います。

フィッシング被害に合わない様にするには、ハイパーテキストは、無闇にクリックしないことです。

https でアクセスしているホーム・ページ上のハイパーテキストであれば、クリックしても殺ねん大丈夫ですが、最近のホーム・ページでは、広告があります、広告各々は、実は URI が全く別で、実際の URI が何なのかについてはソースを見ないと分からないので注意してください。一応、メインのホーム・ページを提供している企業と提携しているのですが、統制まではされていないかもしれません。

では、ハイパーテキストをクリックする代わりにどうするかという事ですが、組織名などを、Google などの信頼が置けるサーチ・エンジンに入力して、自分でアクセスするのです。そして、URI が https://で始まっていることを確かめてください。

まとめ

この文書に書いたことは、網羅的ではありませんが、読んでいただいた皆さんが、「セキュリティ恥罪に気を付けてください！」という、テレビなどで耳にするアドバイスに「何を、どう気を付けるとうんだよ！」と切れる事がなくなる‥‥と期待して、筆をおく事にします。

xx 期　面館　次郎

xx 期の兄弟たちよ！同期会に集結しよう！
期日：xxxx 年 x 月 xx 日
場所：面館山山頂！

連絡先：abcdefg@abc.def.or.jp
090-1234-5678（日吉 麻吉郎）