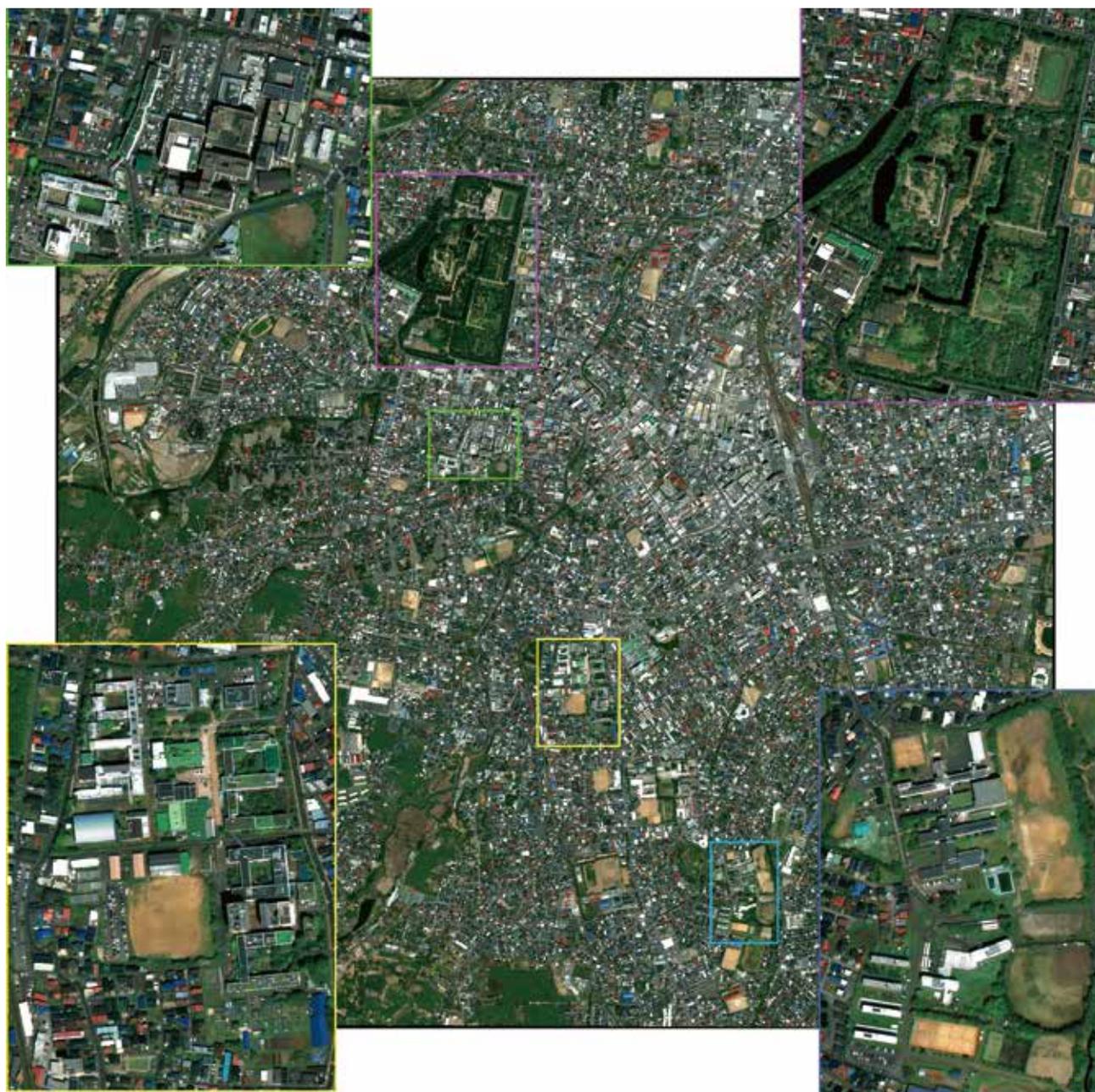


弘前大学総合情報処理センター広報

HIROIN

No.36



Hirosaki University
Computing and Networking Center

2019. 3

表紙の説明

人工衛星搭載高分解能センサによる弘前市街部

理工学研究科 丹波 澄雄

人工衛星に搭載される地表観測センサの分解能の向上には目を見張る物があり、航空機高度からの観測でしか得られなかった高い地表分解能の画像が誰でも入手できるようになってきた。

今回紹介する弘前市街地の画像は米国の Digital Globe 社が運用する人工衛星 WorldView-2 の高分解能光学センサ WV110 によって 2017 年 5 月 9 日 10 時 40 分に撮影された画像である。画像範囲は弘前大学を中心とする東西 5km、南北 5km の範囲である。センサ WV110 は約 50cm 分解能の可視域の白黒画像と約 2m 分解能の複数波長帯の画像を同時に撮影できる。2m 分解能の画像データから青色、緑色、赤色の波長帯の観測画像データを選び出しカラー合成すると我々が見慣れた自然な色合いのカラー画像が生成される。表紙の背景の画像はこのようにして作成した空間分解能約 2m のカラー画像である。1点の大きさが 2m 四方程度なので車両の区別はぎりぎりできるかもしれない。

白黒画像の分解能は約 50cm であり、この情報を用いてカラー画像の分解能を向上させるパンシャープンと呼ばれる技術がある。これは、カラー画像の1画素を縦横ともに 4 倍の合計 16 画素に拡大した画像を用意し、画素値の青、緑、赤の値を色相、彩度、輝度の値に変換した後、輝度の値を対応する白黒画像の画素値で置き換え、さらに青、緑、赤の値に戻すことで実現される。

表紙の左上端の画像は弘前大学本町キャンパスの 50cm 分解能の画像である。また左下端の画像は文京町キャンパスであり、右下端の画像は学園町キャンパスの画像である。右上端の画像は弘前公園の画像であるが、サイズの都合で分解能を 1m に変更してある。

目 次

巻頭言

情報セキュリティの意識向上に向けた課題	福田 眞作	3
---------------------	-------	---

特集

次期弘前大学情報基盤システムに望むこと
本学の情報基盤及びネットワーク環境に関すること
本学の情報システムに関すること
学内の情報化推進に関すること

次期情報基盤システムに望むこと	大橋 忠宏	5
弘前大学情報基盤システムへの疑問点と要望	工藤 武瑠	6
次期弘前大学情報基盤システムに望むこと	上之園 哲也	7
教育と研究の両面から総合情報処理センターへ期待していること	張 樹槐	8
次期弘前大学情報基盤システムに望むこと	鈴木 貴大	9
次期弘前大学情報基盤システムに望むこと	上野 伸哉	10
次期弘前大学情報基盤システムに望むこと	古川 結香	11
弘前大学情報基盤システムに望むことーIoT・AI 世代の ICT 教育ー	野坂 大喜	12
次期弘前大学情報基盤システムに望むこと	陳 彦宇	14
弘前大学情報システムに望むこと	前田 拓人	15
総合情報センターに望むこと	矢野 哲也	17
多要素認証とフィッシングメール	任 皓駿	19

仕事での弘大クラウド利用の勧め	宮元 章匡	21
-----------------	-------	----

弘前大学における標的型攻撃メール対応訓練とフィッシング対策	葛西 真寿	29
	須藤 勝弘	
	小倉 広実	
	竹内 淑怜	

eduroam サービスについて	小倉 広実	51
------------------	-------	----

無線 LAN アクセスポイント		53
-----------------	--	----

総合情報処理センター 事業報告 (2018 年 4 月～2019 年 3 月)		55
---	--	----

編集後記		56
------	--	----

巻 頭 言

情報セキュリティの意識向上に向けた課題

医学部附属病院長 福田眞作

昨年、本学職員を狙ったフィッシングメールによって、個人情報漏洩(疑)事案が発生しました。私個人にもそのメールが何度か配信されており、とても巧妙なものでした。不覚にも何度目かに ID, PW を入力してしまいましたが、偶然にも入力直後に総合情報処理センターからのフィッシングメールを警告するメールを受信し、即座に PW を変更しましたので被害を防ぐことができました。立場上、情報セキュリティの意識は高いつもりでおりましたので、とても恥ずかしくもあり、ショックを受けました。フィッシングメールに騙された病院長・・・ということで、私にこの原稿依頼があったのだらうと憶測しています。

企業や組織にとって、情報セキュリティに対するリスクマネジメントは重要な経営課題のひとつです。本学でも様々な情報セキュリティ対策がとられてきましたが、今回の事案発生によって、残念ながら本学の情報管理体制がまだ不十分であることを認めざるを得ません。もし患者さんの個人情報の漏洩が発生した場合には、附属病院のイメージの失墜につながるだけでなく、賠償や訴訟などの大きな問題にまで発展することが少なくありません。

情報システムやインターネットの普及によって、記録や通信の利便性は飛躍的に向上しました。それと比例して、情報漏洩のリスクも高まっていることを私たちは忘れてはなりません。ますます手口が巧妙化する中で、如何にその利便性を損なうことなく、リスクを回避することができるのか？ 本学では高額な費用負担覚悟で、Office 365 のセキュリティを強化することが検討されていますが、まずは情報セキュリティへの意識の向上が不可欠であると、騙されてみて実感しております。

本学が推奨している「Office 365 多要素認証」の設定率も職員全体の 60%程度(平成 30 年 12 月時点)と聞いています。今回の事案を紹介し、「Office 365 多要素認証の設定」を職員(とくに医師)に呼びかけていて気づいたことがあります。ほとんどの職員が、コンピューター用語をあまり理解していないように思います。PC を購入したときのことを思い出してみてください。業者さんの設定で、即座にメールができて、ワードやエクセルも使えるようになります。説明書なんか読む方は少ないのではないのでしょうか。最近では説明書の同封すらありません。もちろん情報セキュリティに関する説明はほとんどありませんし、職員が情報セキュリティについて自学学習するとは到底思えません。総合情報処理センターの職員(プロ)が、情報セキュリティについて一生懸命に解説したとしても、ホームページ上で様々な情報を公開したとしても、実は前提となるコンピューター用語の意味を理解できていない(しない)職員がほとんどであるという認識に立って、セキュリティ教育を考える必要があります。「ボーっと生きてんじゃねーよ！(by チコ)」と言いたい気持ちを抑えて、粘り強い広報活動を是非とも一緒に行っていただきたいと思います。

次期情報基盤システムに望むこと

人文社会科学部 大橋 忠宏

ohashi@hirosaki-u.ac.jp

1 はじめに

本稿では、人文社会科学部の部局情報技術責任者やネットワーク技術専門委員の立場から感じていることを中心に本学部での情報基盤システム利用の現状と次期システムに望むことについて、以下にまとめる。

2 人文社会科学部での情報基盤システムの利用と次期システムに望むこと

日々の連絡をはじめとして、さまざまな業務がメールにより通知され、連絡・入力作業などについて情報基盤システムを利用する必要がある。

人文社会科学部でも研究活動や教育活動、管理運営などの業務で情報基盤システムの利用が不可欠である。しかしながら、本学部では、情報インフラや情報機器に関して十分な知識や技能を有する職員のみが利用しているわけではなく、業務を行うための情報機器やメール等のアプリの導入や設定等ですら利用者本人が行うのではなく外部の業者が行っている場合が少なくない。また、マニュアル類を参照しながら行う作業が増加しているが、総合情報処理センターから提供されるサービスを含む多くの作業が複雑であったり、マニュアルが整備されていても専門用語が多く利用者にとって平易な記述になっていないことや途中で省略されていて完結していないことがあるため、関係者等による翻訳・解説を必要とする場合がある。

また、本学では、近年、情報セキュリティ対策が強化されており、情報セキュリティポリシーやそれに関連する各種ガイドラインなどへの遵守が求められている。しかし、たとえば、情報セキュリティポリシーに基づくメール利用のガイドライン等によると、HTML メール閲覧や送信は原則禁止されている。しかし、本学部では徹底されていないため、メールを受信しても開けないこともあり、対応に苦慮することがある。さらに、情報セキュリティインシデントが発生した際には、CSIRT から該当者へ連絡されているが、連絡された本人の理解が十分ではなく、部局情報技術責任者が状況を正しく把握することに時間を要することが少なくない。

この他、さまざまなシステム改善や新しいサービスが始まると総合情報処理センターから案内がなされるが、使い方がよくわからなかったり、マニュアルが難しすぎて利用をためらうことや利用をあきらめてしまうことがある。

以前の広報誌 HIROIN の記事で言及されていたが、今後益々情報インフラに関して十分な知識や技能を持っていない利用者の割合は増えていくと考えられるため、このような必ずしも十分な知識や技能を持っていない利用者向けの対応をお願いしたい。

3 おわりに

現在の総合情報処理センターから提供されているサービスについては非常に満足している。さらなるサービス水準の向上のためには、上記で記載したようないろいろな利用者がいることを念頭に利用案内やセミナーの開催が行われることを期待したい。

表紙の説明

人工衛星搭載高分解能センサによる弘前市街部

理工学研究科 丹波 澄雄

人工衛星に搭載される地表観測センサの分解能の向上には目を見張る物があり、航空機高度からの観測でしか得られなかった高い地表分解能の画像が誰でも入手できるようになってきた。

今回紹介する弘前市街地の画像は米国の Digital Globe 社が運用する人工衛星 WorldView-2 の高分解能光学センサ WV110 によって 2017 年 5 月 9 日 10 時 40 分に撮影された画像である。画像範囲は弘前大学を中心とする東西 5km、南北 5km の範囲である。センサ WV110 は約 50cm 分解能の可視域の白黒画像と約 2m 分解能の複数波長帯の画像を同時に撮影できる。2m 分解能の画像データから青色、緑色、赤色の波長帯の観測画像データを選び出しカラー合成すると我々が見慣れた自然な色合いのカラー画像が生成される。表紙の背景の画像はこのようにして作成した空間分解能約 2m のカラー画像である。1点の大きさが 2m 四方程度なので車両の区別はぎりぎりできるかもしれない。

白黒画像の分解能は約 50cm であり、この情報を用いてカラー画像の分解能を向上させるパンシャープンと呼ばれる技術がある。これは、カラー画像の1画素を縦横ともに 4 倍の合計 16 画素に拡大した画像を用意し、画素値の青、緑、赤の値を色相、彩度、輝度の値に変換した後、輝度の値を対応する白黒画像の画素値で置き換え、さらに青、緑、赤の値に戻すことで実現される。

表紙の左上端の画像は弘前大学本町キャンパスの 50cm 分解能の画像である。また左下端の画像は文京町キャンパスであり、右下端の画像は学園町キャンパスの画像である。右上端の画像は弘前公園の画像であるが、サイズの都合で分解能を 1m に変更してある。

目 次

巻頭言

情報セキュリティの意識向上に向けた課題	福田 眞作	3
---------------------	-------	---

特集

次期弘前大学情報基盤システムに望むこと
本学の情報基盤及びネットワーク環境に関すること
本学の情報システムに関すること
学内の情報化推進に関すること

次期情報基盤システムに望むこと	大橋 忠宏	5
弘前大学情報基盤システムへの疑問点と要望	工藤 武瑠	6
次期弘前大学情報基盤システムに望むこと	上之園 哲也	7
教育と研究の両面から総合情報処理センターへ期待していること	張 樹槐	8
次期弘前大学情報基盤システムに望むこと	鈴木 貴大	9
次期弘前大学情報基盤システムに望むこと	上野 伸哉	10
次期弘前大学情報基盤システムに望むこと	古川 結香	11
弘前大学情報基盤システムに望むことーIoT・AI 世代の ICT 教育ー	野坂 大喜	12
次期弘前大学情報基盤システムに望むこと	陳 彦宇	14
弘前大学情報システムに望むこと	前田 拓人	15
総合情報センターに望むこと	矢野 哲也	17
多要素認証とフィッシングメール	任 皓駿	19

仕事での弘大クラウド利用の勧め	宮元 章匡	21
-----------------	-------	----

弘前大学における標的型攻撃メール対応訓練とフィッシング対策	葛西 真寿	29
	須藤 勝弘	
	小倉 広実	
	竹内 淑怜	

eduroam サービスについて	小倉 広実	51
------------------	-------	----

無線 LAN アクセスポイント		53
-----------------	--	----

総合情報処理センター 事業報告 (2018 年 4 月～2019 年 3 月)		55
---	--	----

編集後記		56
------	--	----

巻 頭 言

情報セキュリティの意識向上に向けた課題

医学部附属病院長 福田眞作

昨年、本学職員を狙ったフィッシングメールによって、個人情報漏洩(疑)事案が発生しました。私個人にもそのメールが何度か配信されており、とても巧妙なものでした。不覚にも何度目かに ID, PW を入力してしまいましたが、偶然にも入力直後に総合情報処理センターからのフィッシングメールを警告するメールを受信し、即座に PW を変更しましたので被害を防ぐことができました。立場上、情報セキュリティの意識は高いつもりでおりましたので、とても恥ずかしくもあり、ショックを受けました。フィッシングメールに騙された病院長・・・ということで、私にこの原稿依頼があったのだらうと憶測しています。

企業や組織にとって、情報セキュリティに対するリスクマネジメントは重要な経営課題のひとつです。本学でも様々な情報セキュリティ対策がとられてきましたが、今回の事案発生によって、残念ながら本学の情報管理体制がまだ不十分であることを認めざるを得ません。もし患者さんの個人情報の漏洩が発生した場合には、附属病院のイメージの失墜につながるだけでなく、賠償や訴訟などの大きな問題にまで発展することが少なくありません。

情報システムやインターネットの普及によって、記録や通信の利便性は飛躍的に向上しました。それと比例して、情報漏洩のリスクも高まっていることを私たちは忘れてはなりません。ますます手口が巧妙化する中で、如何にその利便性を損なうことなく、リスクを回避することができるのか？ 本学では高額な費用負担覚悟で、Office 365 のセキュリティを強化することが検討されていますが、まずは情報セキュリティへの意識の向上が不可欠であると、騙されてみて実感しております。

本学が推奨している「Office 365 多要素認証」の設定率も職員全体の 60%程度(平成 30 年 12 月時点)と聞いています。今回の事案を紹介し、「Office 365 多要素認証の設定」を職員(とくに医師)に呼びかけていて気づいたことがあります。ほとんどの職員が、コンピューター用語をあまり理解していないように思います。PC を購入したときのことを思い出してみてください。業者さんの設定で、即座にメールができて、ワードやエクセルも使えるようになります。説明書なんか読む方は少ないのではないのでしょうか。最近では説明書の同封すらありません。もちろん情報セキュリティに関する説明はほとんどありませんし、職員が情報セキュリティについて自学学習するとは到底思えません。総合情報処理センターの職員(プロ)が、情報セキュリティについて一生懸命に解説したとしても、ホームページ上で様々な情報を公開したとしても、実は前提となるコンピューター用語の意味を理解できていない(しない)職員がほとんどであるという認識に立って、セキュリティ教育を考える必要があります。「ボーっと生きてんじゃねーよ！(by チコ)」と言いたい気持ちを抑えて、粘り強い広報活動を是非とも一緒に行っていただきたいと思います。

次期情報基盤システムに望むこと

人文社会科学部 大橋 忠宏

ohashi@hirosaki-u.ac.jp

1 はじめに

本稿では、人文社会科学部の部局情報技術責任者やネットワーク技術専門委員の立場から感じていることを中心に本学部での情報基盤システム利用の現状と次期システムに望むことについて、以下にまとめる。

2 人文社会科学部での情報基盤システムの利用と次期システムに望むこと

日々の連絡をはじめとして、さまざまな業務がメールにより通知され、連絡・入力作業などについて情報基盤システムを利用する必要がある。

人文社会科学部でも研究活動や教育活動、管理運営などの業務で情報基盤システムの利用が不可欠である。しかしながら、本学部では、情報インフラや情報機器に関して十分な知識や技能を有する職員のみが利用しているわけではなく、業務を行うための情報機器やメール等のアプリの導入や設定等ですら利用者本人が行うのではなく外部の業者が行っている場合が少なくない。また、マニュアル類を参照しながら行う作業が増加しているが、総合情報処理センターから提供されるサービスを含む多くの作業が複雑であったり、マニュアルが整備されていても専門用語が多く利用者にとって平易な記述になっていないことや途中で省略されていて完結していないことがあるため、関係者等による翻訳・解説を必要とする場合がある。

また、本学では、近年、情報セキュリティ対策が強化されており、情報セキュリティポリシーやそれに関連する各種ガイドラインなどへの遵守が求められている。しかし、たとえば、情報セキュリティポリシーに基づくメール利用のガイドライン等によると、HTML メール閲覧や送信は原則禁止されている。しかし、本学部では徹底されていないため、メールを受信しても開けないこともあり、対応に苦慮することがある。さらに、情報セキュリティインシデントが発生した際には、CSIRT から該当者へ連絡されているが、連絡された本人の理解が十分ではなく、部局情報技術責任者が状況を正しく把握することに時間を要することが少なくない。

この他、さまざまなシステム改善や新しいサービスが始まると総合情報処理センターから案内がなされるが、使い方がよくわからなかったり、マニュアルが難しすぎて利用をためらうことや利用をあきらめてしまうことがある。

以前の広報誌 HIROIN の記事で言及されていたが、今後益々情報インフラに関して十分な知識や技能を持っていない利用者の割合は増えていくと考えられるため、このような必ずしも十分な知識や技能を持っていない利用者向けの対応をお願いしたい。

3 おわりに

現在の総合情報処理センターから提供されているサービスについては非常に満足している。さらなるサービス水準の向上のためには、上記で記載したようないろいろな利用者があることを念頭に利用案内やセミナーの開催が行われることを期待したい。

弘前大学情報基盤システムへの疑問点と要望

人文学部経済経営課程 工藤 武瑠

h15h3030@hirosaki-u.ac.jp

1 はじめに

昨今では、情報の価値が上昇し、個人情報漏えいやサイバーテロ、ハッキングなどの言葉がニュースを騒がせている。これらは大学の情報に対しても同じことが言え、研究次第では多くの影響を与えることを考えると非常に重大な問題である。筆者は情報セキュリティに関して専門的な知識を有しているわけではない。よって、利用者の視点から疑問に思ったことや要望をまとめる。

2 弘前大学情報基盤システムへの疑問点

まず、疑問に思ったのは USB の管理である。どこの大学でも同じであると思うが、弘前大学では弘前大学情報システムと接続しているパソコンへの USB の使用が認められている。しかし、USB にウイルスが感染している可能性もあり、その対処どうしているのだろうか。

次に、メールアドレスの管理である。筆者が就職活動をした際、企業の評価や口コミを確認したことがあった。その時、個人のメールアドレスではなく、大学のメールアドレスを要求されることがあった。このように学生の大学メールアドレスが大学側の確認できないところで第三者に漏れることには問題はないのだろうか。

また、メール自体の取り扱いではプロトコルについて注意を受けた記憶が私自身無い。しかし、メールを開いた瞬間プログラムが実行されるものもある。

これらの問題はインターネットの知識不足が原因である。もちろん、ある程度の知識を有していれば、あるいは何らかの対策があれば問題はない。しかしそのどちらにも当てはまらない場合、弘前大学では情報の科目が必修となっており、その時間にこのような知識を補うことは可能であると思う。

3 弘前大学情報基盤システムへの要望

まず、一つ目の要望はノートパソコンの各学部での貸し出しである。現在、弘前大学では図書館内でのみノートパソコンが貸し出されている。しかし、各学部で貸し出してくれるのであれば、急なディスカッションや議論の際より役に立つだろう。

次にインターネット経由での印刷である。現在、弘前大学内で印刷のみを実行する場合でも大学内のインターネットと接続しているパソコンを立ち上げる必要がある。これは時間や場所を制限され、不便であると感じている。よって、クラウドなどの活用を検討してほしい。

4 おわりに

筆者は前述したとおり、情報セキュリティに関して専門的な知識を有しているわけではない。よって、あくまでも、利用者としての視点から疑問と要望を述べた。よって、実際にはすでに対策されているもの、実行不可能なものもあるだろう。筆者は勉学に励みやすい環境として、現在より弘前大学情報基盤システムが安全で快適なものになることを望む。

次期弘前大学情報基盤システムに望むこと

教育学部 上之園 哲也
uenosono@hirosaki-u.ac.jp

1 はじめに

平成 20 年(2008 年)の学習指導要領改訂以降、情報教育、ICT を活用した教科指導など、教育の情報化に関わる内容の充実が図られてきた。また、教育の情報化のもう一つの要素である校務の情報化についても一定の予算措置の基に進められてきた。しかし、現在ではその後の継続的な予算措置が十分とは言えず、附属小学校における ICT 環境の整備は遅れており、その状況はかなり深刻と言える。ましてや一般公立学校のモデルとなりうる水準からは程遠い。本学の情報基盤システムの更新に伴って、附属学校園への予算的、技術的支援が求められる。

2 附属小学校の IT 基盤の現状と課題

附属小学校に設置されている児童のための教育用コンピュータ、教員のための校務用コンピュータのほとんどは平成 22 年(2010 年)に導入されたままで更新されていない。不具合を起こしたものをから随時購入によって入れ替えてきたため、数種類の機種及び仕様のコンピュータが混在している。また、コンピュータ教室ではネットワークの通信速度が遅いため 40 台あるコンピュータの内、インターネットに同時接続できるのは 10 台程度である。この環境では ICT を活用した授業を展開するのは不可能に近い。さらに、児童用コンピュータを教師用コンピュータから一元管理するためのシステムが構築されていないことやタブレット端末とデスクトップ端末間でファイル、システムの同期・共有ができないために、本来期待される教育効果が得られていない。今後もより求められる ICT を活用した教科指導の遂行と共に、2020 年度から完全実施となるプログラミング教育を遂行するためには、早急な環境整備が望まれる。

さらに、このような不十分と言わざるを得ない環境は次のような問題も生んでいる。

附属小学校には、校務用 45 台、教育実習用 10 台、教育用 63 台、計 118 台のコンピュータが設置されている。それら全てのコンピュータにセキュリティのための Fセキュアをインストールしたり、パスワードを変更したり、認証したりする作業が求められる。しかし、その作業は複雑で躓く職員も多く、事務職員の協力も得ながら管理担当者が対応している。特に年度初めはこれらの作業が集中するが、対応する管理担当者は教員である。授業や教材研究、児童への対応等の本務が優先されるため、更新作業やメンテナンスは勤務時間内ではなし得ない。そのため大幅な残業や休日出勤を余儀なくされており、その勤務の振替もままならない。このような業務は教員への負担が大きいだけでなく、これにかけられる時間は教員に支払われる教職調整額の範囲を超えていると考えられ、看過できない。

また、現在、コンピュータ教室の教育用コンピュータ 40 台全てと、職員室の校務用コンピュータ 36 台の内 19 台が Windows7 のままである。今後、サポートが終了する 2020 年 1 月 14 日までに全ての OS を更新する必要がある、管理担当者の負担が増えることが考えられる。また、幼稚園、小学校、中学校、特別支援の附属 4 校園では 2019 年度より小学校にサーバーを設置し、校務支援システムを導入する。それに伴って、本学の情報基盤システムとの連携等の問題が発生することも考えられ、管理業務はさらに複雑さ、煩雑さを増すと予想される。総合情報処理センターからの専任職員の配置が望まれる。

3 おわりに

以上のように、附属小学校の IT 基盤は、機器及びシステムの老朽化と機種、仕様の混在のため、非効率化と機能低下を招いている。その結果、ICT を活用した教科指導による教育効果は得られにくく、校務においては IT の恩恵を享受するというよりはむしろ、IT の不具合によって効率低下を被るという状況になっている。文京地区の情報基盤システムが更新されるに従い、附属小学校の IT 基盤との差はさらに広がり、まさにガラパゴス化することが懸念される。附属学校園は教育学部の附属施設ではあるものの、IT 基盤は大学全体の資産であるという視点に立ち、本学情報基盤システムの一部に組み入れ、大学全体でバランスの取れた情報基盤システムになることが強く望まれる。

教育と研究の両面から総合情報処理センターへ期待していること

農学生命科学部 張 樹槐

zhang@hirosaki-u.ac.jp

1 はじめに

以前 21 世紀教育の「情報」という必修科目と学部専門教育の「コンピュータ演習」を担当していた関係で、前後期とも総合情報処理センターをフルに利用していたが、その後の教養教育への名称変更などに伴う科目削減で、全学の情報関連科目の担当でなくなり、現在後期に実施している「コンピュータ演習」を定期的にセンターで行っているだけになる。それ以外、基礎ゼミ、研究室のゼミや大学院の授業などで、農学生命科学部のサテライト教室を不定期で利用することもある。

研究の面においては、直接センターの情報機器を利用するというより、ネットワークを通じて、メールや検索等々で無意識的にほぼ毎日接している。

今回、以上の両面から日頃感じたこと、ぜひ検討してほしいことを述べさせていただきます。

2 教育の面から

教養教育の「情報」科目が必修でなくなった主な理由は高校での必修化と聞く。しかし、所属学科 2 年生の「コンピュータ演習」で接した学生などのレベルを見る限り、多くの学生が基礎的な知識さえマスターできているとは到底言えない状況にあると感じる。例えば、ファイルの拡張子がどんな役目であるかと聞くと、多数の学生が答えられないでいる。実験系の場合、これを少々意識しないと、卒業研究などで計測機器などから出力されたデータファイルの管理などで大変困惑することになる。学生によっては、大学の 4 年間、本人が情報関連の科目を選択しない場合、情報リテラシーに関連した講義に一度も関わることなく、卒業して社会に出てしまう。

また、経費削減という観点から、各学部を設置しているサテライト教室を整理したいとの提案があった。確かに、サテライト教室の稼働率が低いとの問題点があるけれど、少人数の基礎ゼミや研究室ゼミなどで利用する際、身近にあること、統一した操作性が何より重要となる。

言うまでもなく益々重要となる情報関連の基礎知識を学生達に身近に体験していただけるように、教養教育科目の増設や気軽に利用できるパソコンなど情報機器の合理的な設置をぜひご検討願いたい。

3 研究の面から

ネットワークを通じた利用がほとんどであるため、個人的に重要と思われるのは、①海外を含め、学外での利用利便性、②セキュリティ対策の向上、③トラブル対応の迅速化である。

学外での利用利便性については、具体的に国内外での出張時のメール確認とクラウドサービスになる。例えば、セキュリティの関係で弘大クラウドには海外から接続できない設定となっており、Office 365 の OneDrive も大変煩雑になってきた。

セキュリティ対策とトラブル対応については、スタッフの皆さんのご努力でかなり改善された。しかし、その反面、認証などの手続きが煩雑になり、教員によってはしばらくメールが受信できないとの話も聞いた。セキュリティとの兼ね合いで仕方がないことではと思うが、ぜひ情報の周知徹底と一層のサポート支援をお願いしたい。

4 おわりに

総合情報処理センターで提供されているサービスに大いに満足している中、改善して頂きたいことをいくつか述べてさせて頂いた。センターの皆さんもより良いサービスを提供していくために、職員一人ひとりに協力してほしいことが今後も生じるでしょう。その際に、ぜひ丁寧な説明とサポートを引き続きお願いする。

次期弘前大学情報基盤システムに望むこと

岩手大学大学院連合農学研究科 鈴木 貴大
takahiro.suzuki.ppvd@gmail.com

1 はじめに

大学(院)生・研究者にとって、情報収集は必須である。情報収集するツールとして、書籍、インターネット等があげられる。そしてインターネットの普及と社会の情報化に伴い、書籍・文献の電子化が進み、紙媒体よりも、インターネットを介した情報のダウンロードで、パソコンの画面上で情報を得ることがほとんどとなった。一方で、研究者の大事な情報をインターネットを介して扱ったり(eメール等)、ほとんどの場合を電子情報としてパソコンに保存する。筆者の書きかけの論文(世紀の大発見につながるかもしれない)もその一つである。これらのことにより、情報漏えいを防ぐためのシステムが必要である。

2 弘前大学情報基盤システムの問題点

筆者はHiroin Wi-Fiや弘前大学のメールシステムをほとんど使ったことがない。筆者は弘前大学の修士に進学したのだが、引き続きHiroin Wi-Fiや学内のメールシステムを使うには再登録が必要である。それが面倒である。そこで現在は、研究室のWi-Fiを使い、メールもGoogleメールを使っている。また上記したが博士課程進学後、筆者は弘前大学の学籍番号がないので、学内の情報システムを引き続き利用するためには別途アカウント申請が必要となる。しかし、総合情報処理センターからは案内がなく、ホームページに記載があるだけである。これでは連大生が実質的に利用できない状態に等しい。これらのことより、筆者は大学院生にも使いやすい(使える)学内システムと丁寧な案内を目指して欲しいと考える。

3 おわりに

研究者にとって情報は財産である。情報の電子化により、誰でもインターネットを介して情報を得ることが容易になった。しかしその一方で、情報の不正利用・漏えいの危険性が増した。筆者は、情報を守るためにより一層強固なセキュリティシステムを望む。

次期弘前大学情報基盤システムに望むこと

医学研究科 上野 伸哉
shinyau@hirosaki-u.ac.jp

テーマとして、“次期弘前大学情報基盤システムに望むこと”で依頼がありました。以下に示す内容が依頼のお題と合致するかは疑問あるところですが、

- ①コンテンツ利用のための情報提供の改善
- ②著作権に対する具体的指針
- ③学生・教員のデジタル情報、ネット利用のリテラシー向上

この3点が、今後弘前大学システムの充実、とくに運用面を高めるには必要があると思っています。

主に講座コンピュータを利用する教員として情報基盤システムに関連して思い浮かぶのは、学内ネットワーク、e-mail および web サイトの利用等でしょうか。これらの普段の利用として、ネットワーク上で論文検索、データベース検索、出張旅費の処理、会計処理、さまざまな事務処理があります。私の講義での利用として、医学英語でのアルク教材、生理学シュミレーションソフトを学生が端末を用いて学習することや、担当する教養教育、専門教育講義での Moodle も用いた講義資料、小テストの提供などがあげられます。また医学部においては、統計ソフトを用いた実習・演習講義、医師国家試験対策ソフトの利用、文科省による医学部学生のための準国試扱いとなっている CBT (Computer Based Test) の実施など情報システムの利用に依存しています。これらの利用時に実感するのは、特にハード面では最近では随分よくなっているように思います。私が弘前大学に来て 16 年目となります。その間、インターネットの普及、学内 LAN、無線 LAN が学内で使えるようになってきました。また医学部の端末も 150 台を超えるまでに増えました。しかしながら、ネットワーク上でなにか新たに始める際の手順等はまだまだわかりにくいし、ハードルの高さを感じています。最近の経験でいうと、Moodle の使用の際に弘前大学サイトにマニュアルはなく、他大学サイト等を利用したり検索したりと、なかなかとつきにくい状況が続いています。また教育関係の資料は、アクセス制限設定、著作権の問題で、どこまでデジタルとして載せられるのか、あいまいなことも多く悩むところです。また、本学において情報流出の事例があり、最後は使用している人の認識、理解に依存しています。学生にも、1 年次の基礎ゼミナールの時間にいろんな事例、特にネット上の注意点を紹介はしていますが、まだまだ十分ではないかなと感じています。

予算の問題はついてまわりますが、ハード面を生かすヒト、ノウハウの共有、リテラシー向上のための学ぶ機会を増やすことを望んでいます。

次期弘前大学情報基盤システムに望むこと

医学部医学科 古川 結香

h16m1039@hirosaki-u.ac.jp

1 はじめに

フィッシングメールによる個人情報の漏えいの件から、学生として第一に望むことは、個人情報を守る強固なセキュリティである。大学側へは、信頼関係から様々な情報が集められているので、技術面での改善は不可欠であると感じる。

2 つぎに

一方で、学生側もこれを機に個人情報の管理を見直すべきであると思う。大学は、多くの学生にとって初めての立ち場である。個人情報が自分だけでなく家族によって守られてきた人も、大学では多くの事柄が自己責任となる。義務教育や高校生活で情報の授業を習ってきたが、学生側が個人情報を大学に預けるにあたって、もっと詳細な情報管理の説明や指導を受けても良いと思う。日進月歩の「情報」社会であるので、まずは学生側が正しい知識を得て、それぞれが危機感を持つことが情報管理の第一歩であると思う。

3 おわりに

現代、パソコンやスマートフォンなどの電子機器の進化が進み、たった1台で色々なことができるようになった。これらの機械を持つ学生は非常に多い。大学生としての生活に必要な存在と言えるかもしれない。そんな中で、スマホ世代の私たちは、電子機器に個人情報を詰め込み過ぎているように思う。現に私も、知り合いの連絡先やSNSのアカウントのログインIDの記録、様々なパスワード、スケジュール帳など、今の「わたし」に関する情報は全て電子機器の中に入れてしまっている。これでは危ない。被害に遭う前に、各々が電子機器との関係を省みる必要がある。便利な機械とこれからも上手に付き合っていけるように、今こそ学生一人一人が個人情報保護について考え直すべきである。

弘前大学情報基盤システムに望むことーIoT・AI 世代の ICT 教育ー

保健学研究科 野坂 大喜
hnozaka@hirosaki-u.ac.jp

1 はじめに

近年、金融・医療・農業など多くの産業において IoT や AI の活用が進んでいる。文部科学省では、2020 年度からの小学校プログラミング教育の全面実施に向けて、平成 30 年 3 月に「小学校プログラミング教育の手引」を作成し、その中では総合的な学習の時間や情報以外の教科との連携指導例として、理科では「身の回りには電気の性質や働きを利用した道具があること等をプログラミングを通して学習する場面」を、総合的な学習の時間では「『情報技術を生かした生産や人の手によるものづくり』を探究課題として学習する場面」を示している。これらの指導例が示しているのは、既に情報教育は単に情報機器の操作を学ぶ学問の段階を過ぎ、鉛筆や定規あるいは金槌やドライバーなどと同じように、一つの道具(手段)として情報機器を他の学問と融合させて利用していくことである。しかしながら、大学など高等教育機関においては未だ「情報」の授業は独立した科目とされており、今後は農業や医療などの専門分野と融合させた教育課程の実現が求められている。一方で内閣府は、産学と連携して人工知能(AI)の開発や運用に精通した人材を認証する制度の新設を検討している。AI 人材は 2020 年に 5 万人ほど不足するとの試算もあり、文系・理系を問わず、全大学生を対象に IT(情報技術)を活用したデータ教育の必修化も検討されている(図 1)。このような時代背景において、次期弘前大学情報基盤システムが担う役割は非常に大きいと考え、専門教育との融合における観点からの次期情報基盤システムへの要望について考えてみたい。

2 弘前大学情報基盤システムの課題と期待

現在保健学科学生が弘前大学情報基盤システムを利用して受講している講義は、主に情報処理入門、統計学に限定されており、専門教育において十分な IoT 活用型授業や AI 関連授業は展開されていない状況にある。一方で、過去 3 年間で医療分野における AI 関連研究報告は急激に増加しており、医療現場においても AI による業務効率化

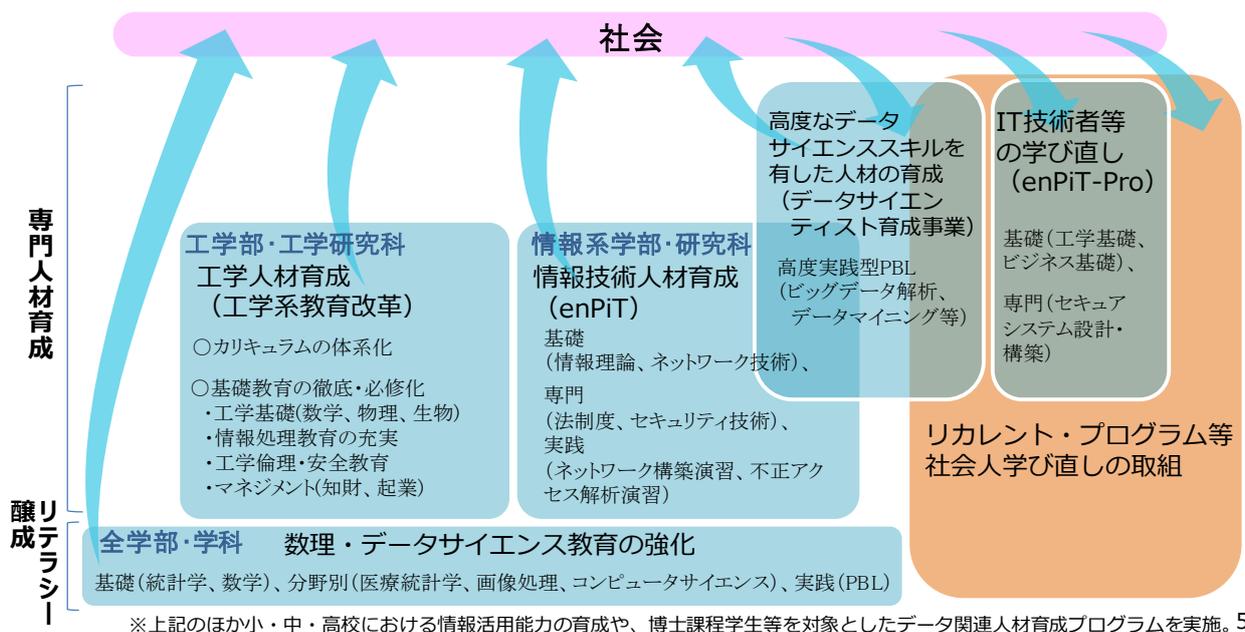


図 1 未来投資会議 構造改革徹底推進会合「AI 人材育成について」(平成 30 年 4 月)資料より抜粋

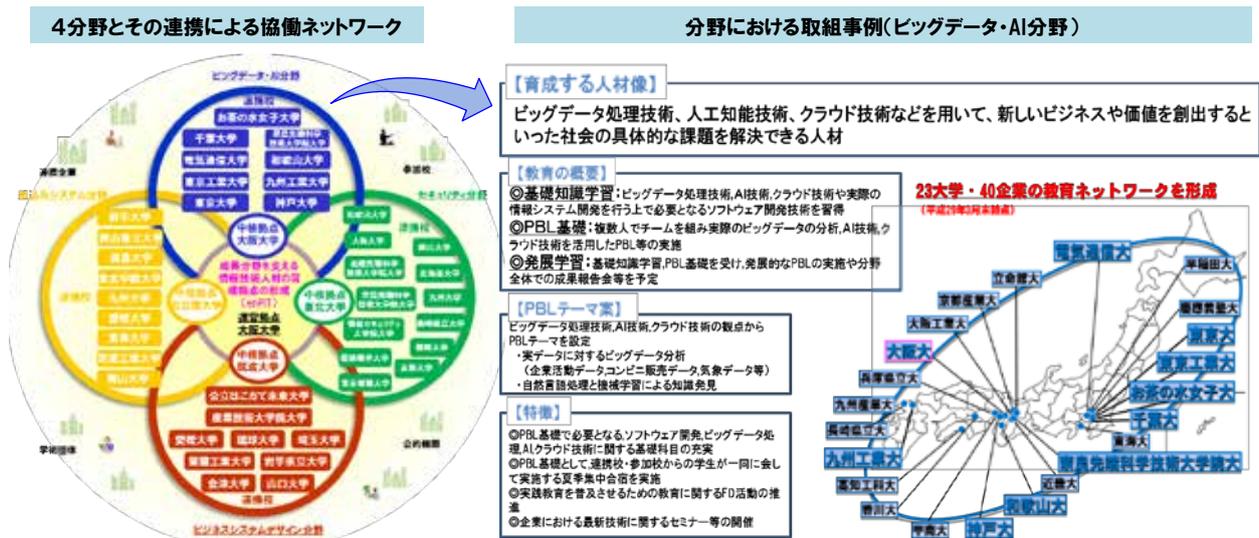


図2 未来投資会議 構造改革徹底推進会合「AI人材育成について」(平成30年4月)資料より抜粋

や診断の自動化への取り組み, またその臨床応用も既に始まっている。そのことから医療用 AI については, 理工学系学生への開発者教育だけでなく, 利用者側となる医療者に向けたトレーニングも今後必要不可欠となることが想定される。特に各医療職能団体においては現職者再教育を含め医療用 AI 教育のあり方についての検討に入っていることから, 今後は医療技術者を目指す学生にとって AI や IoT は避けて通れない知識となる。

このような課題に対して対応を求められた場合, 現在の弘前大学情報基盤システムでは e-Learning や演習も含め AI 教育に対応可能な資源が提供されていないため, 誰もが簡単に利用できる AI 教育環境の整備が必要となると考えられる。図2は大学学部学生を対象とした Society5.0 に対応した人材育成事業(enPiT)の概要図であるが, 既に本学周辺の大学では道具としての情報教育から, 社会実装型の学部学生情報教育へ展開されており, 社会実装型情報教育に対応できる情報基盤サービスが本学においても必要と考える。

以上のことから, 次期弘前大学情報基盤システムにおいては AI 教育へも対応したシステムの構築を望んでいる。特に近年は AI を利用とした場合, Google 社の AUTO ML や IBM 社の WATSON などクラウドサービスが各産業分野で活用されていることから, 学内の教員・学生を問わず AI を教育や研究開発に利用できるよう最先端の AI クラウドサービスを学内で導入していただけることを期待している。

次期弘前大学情報基盤システムに望むこと

医学部保健学科 陳 彦宇

h17m2326@hirosaki-u.ac.jp

1 はじめに

昨年度はフィッシングメールによる個人情報の漏洩が発生し、多大な問題が生じたことをもとに、次期弘前大学情報基盤システムに望むこと、漏洩防止の対策について考える。

2 フィッシングメールとは

フィッシングメール(Fishingmail)とは、地面上のように、エサをばら撒いて、利用者(User)を釣り上げるような意味合いである。具体的な手法としては、使用者がクリックしそうなソース(使用者が信頼する機関など)になりすまして、使用者にメールを送り、メールの開封及びリプライに誘導することで、個人情報を獲得するものがある。

3 フィッシングメール対策

弘前大学情報システムの利用者として、年間に通じて数十回の使用上では、フィッシングメールを受信することは一度もなかったが、そうした事例があったことには、予防する方策を考えなければならない。使用者側の力で被害を未然に予防するためには、フィッシングメールによる個人情報漏洩の防止としては、ソースの怪しげなメールはクリックせずに削除すること、思いの当たらないメールを受信した場合は当担当者に即座に確認すること、変に個人情報の入力を要求する旨のメールには厳重に確認をすることなどがある。それらを、習慣的に熟せることで、被害の予防に役立つと考える。

4 期望

上記3では使用者側の個人的なセキュリティー保護の習慣が被害の予防となることについて述べたが、学校側、情報基盤システムには、電子工学的な技術層のセキュリティーを向上させることと相まって、より被害を確実に減らすことができるのではないかと考える。

弘前大学情報システムに望むこと

理工学研究科 前田 拓人

tktmyd@hirosaki-u.ac.jp

1 はじめに

みっともないようだがまずは言い訳から。筆者は2018年4月に弘前大学に着任したばかりの新人である。研究の一部で大規模数値シミュレーションに携わっているものの、計算機そのものが専門というわけでもなく、コンピュータの一利用者に過ぎない。したがって、本来はこのような大それたことを書くような立場でも、その知識があるわけでもない。そこで、本稿では筆者なりに本学の計算機システムを1年間弱のあいだ利用してみた経験を振り返りつつ、特に教育用システムを中心にいくつか思うところを述べてみたい。

2 充実した教育用システムとBYODの懸念

筆者は今季より学部2年生にLinuxおよびプログラミングの演習を担当している。どの端末でログインしても共通のファイルが利用できるファイルシステムはもとより、簡単に使えるWindows-Linux間ファイル共有(導入時期の関係だろうか、ややバージョンが古くなっているものもあるが)、充実したフリーソフトウェア・ライブラリ群、確実に出席の判定ができる必要十分な出席管理システムなど、総合情報処理センター職員の皆様の助けを借りながら存分に活用させてもらっている。

特に、実習室の環境は大変使いやすい。プログラミングではどうしても細かい文字を読み書きするため、プロジェクトで教室前方のスクリーンに投影しても視認性が悪い。ところが、実習室では端末2台に1台の割合でプロジェクト投影した画面が表示されるサブディスプレイがあり、この問題が解決されている。講義では持ち込みのノートPCからHiroin Wi-Fi経由でセンターのLinuxにVNC(画面共有)で接続し、受講学生のLinux端末と同等の画面を表示して、その場でLinux操作やプログラムを実演する、ということを行っている。学生にはその実演を見ながらまずは真似をしてもらい、そこから実習課題へと進んでもらっている。配布資料やスライドだけを用いるよりも学生の反応も良いようで、手応えを感じている。

さて、そうすると最大の懸念は「この環境がいつまであるだろうか」ということである。他大学に目を向けると、Bring Your Own Device (BYOD)の掛け声のもとに、学生向けの計算機環境の提供をやめてしまうところが複数現れているようである。たしかに、身の回りの学生に聞くと、多くが大学入学時にPCを購入しているようだ。だが、本当にそれでよいのだろうか？それで前述のような効果的な教育ができるだろうか？筆者の分野では、LinuxあるいはUNIX系OSの利用やプログラミング、X11によるGUIを前提としたソフトウェアの利用が、研究活動のために必須である。理系では同様の分野も多いだろう。Windowsが中心で、かつ一人ひとり環境がばらばらな持ち込みPCでは、環境を整備するだけでも大変な労力がかかるであろう。個人PCの持ち込みとそれらの学内ネットワークへの接続が増えることで、セキュリティのリスクも増大すると懸念される。現在の水準の教育用計算機環境を維持してほしいと、切に願う次第である。

3 研究への活用について

ところで、筆者は本学の計算機システムは、自身の研究にはほとんど使っていない。筆者の行う数値シミュレーション研究では、少し計算規模を大きくしようとすると、あつというまに必要なメモリサイズ数百TBに膨れ上がり、それをカバーするために数千~数万のCPUが必要に、といった具合で、莫大な計算機資源を消費するようになってしまう。そのような大規模計算を保有する組織は少なく、必然的に競争的計算機資源の公募や、共同利用に基づいて外部の大型計算機を利用することになる。したがって「弘前大学の計算機システムで大規模数値シミュレーションをしたい」と要望するつもりはない。

だが、いつも大規模計算ばかりしているというわけでもない。比較的小規模の計算やデータ解析、あるいは卒研究生や大学院生の研究で、講義時以外はあまり利用されていない大量の計算機資源を活用できないものか…と置いていたところ、まさにそのような検討をしている旨を耳にした。期待して続報を待ちたいと思う。

4 ネットワークとセキュリティについて

Hiroin Wi-Fi はキャンパス内カバーしており、しかも同じアカウントで学外の eduroam も透過的に利用でき、学内外ともに便利に利用している。しかし、Hiroin Wi-Fi はどうやら少々線が細いようで、頻繁に通信が途絶えてしまう。もちろん独自に Wi-Fi ルータを導入すれば快適な Wi-Fi が手に入るわけだが、その結果だろうか、筆者のいる理工学部一号館には大量の Wi-Fi アクセスポイントがずらりと並んでいる。自分もやっているのに文句を言えた筋合いではないのだが、この大量のアクセスポイントの設置が、Wi-Fi のつながりにくさに拍車をかけているのではないだろうか。次期システムでは Wi-Fi が強化されることを望んでいる。また、外部からの VPN 接続もやや線が細いように感じている。

ところで、昨今の大きな話題といえば弘大メール(Office 365)での多要素認証の導入であろう。これがセキュリティ上必要なことであるというのは十分に理解できるし、筆者個人として利用している他のオンラインアカウントの多くでも二段階認証を利用している。しかし、Office 365 の多要素認証は、他のサービスとくらべてより厳格なように感じる。二段階認証の有効期間は 2 週間だけで、それをすぎるとスマートフォン等を用いた再認証が必要となる。そのことによりより強固なセキュリティを実現しているのだろうが、利便性とはトレードオフの関係にある。たとえば、数週間にわたる海外出張で、かつ何らかのトラブルでスマートフォンが使えなくなったら？多要素認証に反対するものではないが、せめて認証後の有効期間だけでも、もう少し伸ばせないものだろうか。

5 おわりに

不満らしきことも少しは書いたが、総合情報処理センターが提供しているサービスには大変満足している。少人数にもかかわらずこのような充実したサービスを実現している総合情報処理センタースタッフに深く感謝したい。

総合情報処理センターに望むこと

理工学研究科 矢野 哲也

yano@hirosaki-u.ac.jp

1 はじめに

理工学部および教養の講義, 実習で総合情報処理センターの実習室を使用させていただいております。ここでは、センターの1ユーザーの立場で、教育環境整備のために総合情報処理センターに望むことを以下に記させていただきます。

2 総合情報処理センター実習室について

2.1 利用状況

2017年度から機械科学設計(理工学部機械科学科2年次必修科目)の実習に、総合情報処理センター実習室のPCを使用させていただいております。実習では主にAutodesk社のコンピュータ支援設計(CAD, Computer-Aided Design)ソフトウェアInventorを使用し、機械部品のモデリング(3次元構造をコンピュータ上に構築する)、アセンブリ(複数部品をコンピュータ上で組み立てる)を行っています。3次元CADは製造業の設計の現場で広く利用され、その運用技術は、機械工学系の学生が身に付けておくべきとされるものとなっています。本実習は、また、作成したモデルファイルをもとに自動機械加工を行うコンピュータ支援製造(CAM, Computer-Aided Manufacturing)についての学習も含まれます。具体的にはマシニングセンタによる切削加工、3Dプリンタによる熱溶解樹脂積層造形を行っています。特に後者は迅速で安価な試作(ラピッドプロトタイピング)を実現する手法として普及が急速に進み、様々な用途で使われています。

2.2 現状と改善の要望

3次元CADソフトウェアを用いた設計を快適に行うためには、十分なグラフィック性能のPCと大画面ディスプレイが必要です。センター実習室には、現時点では十分な性能のPCと比較的大きなディスプレイが用意されており、実習を行うにあたり支障はありません。ただ、学生端末の脇に置かれ、教員側のPC操作を供覧するために用いられているディスプレイのサイズが非常に小さく、CAD操作において不都合が生じることもあります。

CADソフトウェアのアセンブリ機能で部品間に適切な拘束を適用して組み立てることにより機構を構成し、シミュレーション機能でその機構の動作をシミュレートし、不具合なく動作するか確認することができます。このとき、衝突判定により部品間の干渉を確認することができますが、部品点数が多い場合や部品間の接触部分の形状が複雑である場合には、計算負荷が大きくなり、長時間の計算が必要となります。特に、歯車列の動作のシミュレーションなど、バックラッシュを考慮しながら歯の噛み合わせを逐次接触判定を要する場合には時間を要するようです。より大規模で高度な設計が必要な場面では、現状よりも高性能なPCが必要になりそうです。

設計の高度化が進み、実機の製作および実機を用いた評価の前に、計算機上で性能評価を行うことが行われるようになってきました。機械の実使用環境において起きる様々な物理現象を詳細にシミュレートするために、構造解析、流体解析、伝熱解析、電磁界解析などの単体の物理シミュレーションに加え、これらを連成したマルチフィジックスシミュレーションが行われるようになってきています。時代とともに着実に設計法の高度化が進み、講義内容もそれに合わせてアップデートしていくこととなります。これらに対応できるように、今後、順次端末が更新されていくことを期待しております。

2.3 提案

3Dプリンタは近年、低価格化が急速に進み、製造業に限らず一般にも普及しつつあり、ホビー用途やDIYでも使

用されるようになってきています。その製作対象のモデルデータを作成するための CAD のニーズは、機械工学系に限らず、様々な分野の学生さんにもあると思います。専門を問わず興味のある学生さんに向けた簡単な CAD ソフトウェアの操作マニュアルが用意されていると、気軽に利用してもらえませんか。センターの PC には CAD のほか数多くの有用なソフトウェアがインストールされているようです。マニュアルの整備や利用講習の実施など、利用に際してのハードルを下げる仕掛けを用意することで、利用者の増加につながると思われます。また、学生さんが実費程度の料金で利用できる 3D プリンタ出力サービスを用意していただくと、学生さんの創造的な活動の助けになるかもしれません。実際には保守管理にコストや人手が掛かり、実現は難しいかもしれませんが、検討いただければと思います。

3 Microsoft Office 365 について

大学発行のアカウントで利用できる Office 365 で提供されている Outlook, OneDrive, SharePoint などの Web アプリケーションをよく使用しております。OneDrive や SharePoint は講義資料の共有や研究室内の情報共有などに重宝しております。インターネットに接続された端末と Web ブラウザがあればどこからでもアクセスして作業ができ、大変便利です。最近 Office 365 アカウントへの不正アクセス対策のための二段階認証が導入され、ログイン時に従来のパスワード入力に加え、スマートフォンにインストールした Microsoft Authenticator アプリを使用した承認操作をしております。二段階認証が必須とされるようになってからはまだ経験しておりませんが、海外出張などでスマートフォンをインターネットに接続できない状況になることも考えられます。そのような場合、どのように対処したらよいか不明な点があり、少々不安を感じております。セキュリティの問題を解消しつつ、より簡便で確実な方法があれば積極的に導入を検討していただきたいと思っております。

4 学修ポートフォリオシステムについて

学修ポートフォリオシステムと呼ばれる、学生さん自身が学修の過程や成果物(レポート, 作品, 論文等)を継続的に蓄積しておくことができる Web システムの導入を検討いただければと思います。他大学で導入されているシステムでは、教員側からは、講義資料、演習問題、課題の提示のほか、レポートの回収もシステム上で行え、提出状況の管理も容易に行えるようです。学生さん自身も継続的かつ定期的に学びを振り返ることを通じて学修の到達度を確認し、取り組むべき課題を発見することができるかとされています。現在は、講義資料等の電子データの配布は、講義ごとに用意した Web サイトや、Office 365 の OneDrive 等を通して行っております。学修ポートフォリオシステムに一元化されれば、学生さんにとっては学修の振り返り、学び直しも容易になるでしょうし、教員にとっては、学生さんの理解度を確認しながら講義を進められ、最近推奨されているアクティブラーニングやインタラクティブラーニングを実施するのにも役立つと思われます。

5 おわりに

今後の講義内容のアップデートに対応する端末の更新や、新しい学修管理システムの導入など個人的な希望を記させていただきました。今後も情報教育のための環境整備や教育支援システム等の運用を宜しく願いいたします。

多要素認証とフィッシングメール

理工学研究科 任 皓駿

hojun@hirosaki-u.ac.jp

1 はじめに

本記事では、最近、本学でネットワークのセキュリティの強化のため始まった多要素認証とフィッシングメールについて一人のユーザーとしての意見を述べてみたいと思います。

2 多要素認証を利用して

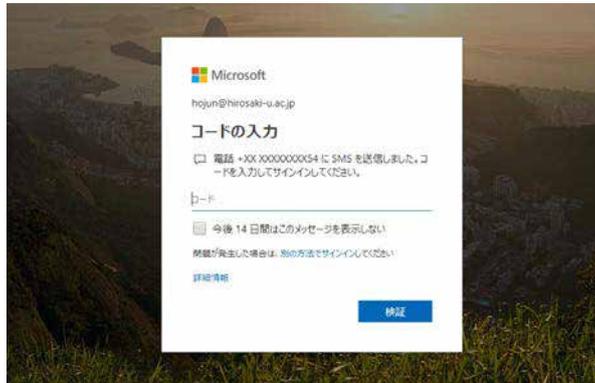


図:携帯番号の SMS を用いて多要素認証した際のログイン画面

多要素認証は 2 種類以上の要素(知る要素, 持つ要素, 備える要素)^[1]を用いてログインの認証を行うことですが, 個人的にはウェブ上でのクレジットカードの決済以外ではあまり経験がありませんでした。昨年 11 月ごろ, 本学で多要素認証の設定を始めたとき, 率直にいえば馴染みのない方法で少し戸惑いました。最初, 認証方法として研究室の電話番号を登録し, 帰宅後, 弘大メールに接続しようとする追加認証の画面が現れ, 進むことが出来なかった覚えがあります。次の日, 認証方法を研究室の電話番号から自分の携帯電話番号の SMS に変更することで解決が出来ました。一方, 使っていくに連れて, セキュリティがしっかりしている安心感を持つようになりました。弘大メール (Office 365) では, 上記の 2 種類の方法以外でも専用のアプリケーションを利用した認証方法もあり, 個人の状況に合わせて設定が出来て大変助かると思います。しかし, 上記に述べた多要素認証の優れた機能にも関わらず, フィッシングメールは各職員宛に直接に来るので, 被害に巻き込まれる可能性は相変わらず残っています。例えば, リンク先をクリックして思わぬ接続をしたり, 個人情報などを入力したりする恐れがあります。特に, 本学の機関名や職員名に成り済ましたメールは注意が必要です。不審なメールを受信した際には, 弘前大学 CSIRT (csirt@ml.hirosaki-u.ac.jp) に積極的に報告するなど, 各職員が高いセキュリティ認識を持つことが何より大事だと思います。

3 おわりに

短い文書ですが, 最近始まった多要素認証の経験談とフィッシングメールの対策についての意見を述べました。多要素認証は一手間掛かることで少し面倒なところはあると思いますが, セキュリティの側面から見るとその価値は十分あると思います。しかし, フィッシングメールの対策は利用者一人一人の認識が大事であり, 何よりもお互いの協力が第一要素だと思います。

参考文献

[1] Wikipedia から (<https://ja.wikipedia.org/wiki/多要素認証>)

仕事での弘大クラウド利用の勧め

学務部教務課教務企画グループ 宮元 章匡

miyamoak@hirosaki-u.ac.jp

1 はじめに

(以下は、事務で使用している WindowsPC を前提にしています。他 OS ユーザの方々には申し訳ありません。)

総合情報処理センターが提供しているサービスに弘大クラウドがあります。これはファイルの共有・保存に最適です。業務での PC 使用に関して生じる、不意の停電や PC の故障等によるデータ消失の不安から解放されます。記録容量もデフォルトで一人 30GB まで使用でき、個人が業務で使用するほとんどの場合において十分な容量です。自分のファイル・フォルダを公開することができるため、課・グループ・担当単位でファイル共有することもできます。Hiroin ID によるログイン認証があるため、勝手に自分のファイル・フォルダを覗かれる心配はありません。公開するかしないか、読み書き可能かどうかというようなファイルへのアクセス制御を Hiroin ID を元に行うことができます。2018 年 11 月より、教務課学務情報担当では弘大クラウドを学務情報担当共有ファイルサーバとして、また個人の業務 PC のファイルサーバとして使用してきました。そこで、これまでに NAS と弘大クラウドについて調べたこと、使用中に気づいたこと等を報告させていただきます。

2 NAS とクラウド

2.1 NAS は壊れる

ファイル共有であれば既に NAS を使用している所は多いと思います。過去には学内にテラステーション(株式会社バッファロー製の NAS)が配られたことがあります。NAS とは Network Attached Storage の略称で、ネットワーク接続した外付け HDD のことです。ただし実際にはファイル共有に特化した計算機です。NAS は学内 LAN に接続するだけで簡単に使用できます。PC 側で NAS のフォルダに対してネットワークドライブの割当をするだけです。学務部ではこのテラステーションを一部の課・担当がファイル共有のために使用しています。

計算機はいつかは壊れます。壊れればデータは失われます。データを失わないためにはバックアップを行います。では計算機である NAS はバックアップしているでしょうか。NAS に自分の PC からファイルをコピーして、これでバックアップした気持ちになっていませんか。NAS は決して PC のバックアップ装置ではありません。複数の PC で使用する共有ファイルサーバが基本の役目なのです。NAS 自体のバックアップが必要なのです。その証拠に、例えばテラステーションの発売元であるバッファロー社の Web サイトには、テラステーションのバックアップ方法が掲載されています。インターネット上には NAS のバックアップについて多くの情報が存在します。実際に学務情報担当が管理していた NAS は、HDD の制御部分が壊れたため使用不能となりました。使用開始から間もなかったため、NAS のバックアップは行っていませんでした。しかし幸いなことに大量にデータが蓄積される前でしたので被害は軽微で済みました。

バックアップはしていますか。停電対策として UPS を使っていますか、故障したときの対策は考えていますか。これらは NAS の管理者が行わなければなりませんが、NAS の管理者はどれくらいいるのでしょうか。大多数の職員にとって、NAS の管理などというものは本来やるべき仕事ではありません。本来の仕事を楽にできるようにするために NAS を導入したのに、NAS の管理という面倒な仕事が増えてしまった。しかし弘大クラウドであれば解決してくれます。面倒な NAS の管理から解放されるのです。弘大クラウドの利用者は単に利用するだけです。管理は必要ありません。

2.2 NAS と弘大クラウドの比較

思いっくままに NAS と弘大クラウドを比較してみます。

	NAS	弘大クラウド
使用を開始する場合に行うこと	学内 LAN に接続して、PC でネットワークドライブを割り当てる。	Hiroin ID でログインする。
ファイル・フォルダの公開	デフォルトでは、同じネットワークセグメントならば他人から見える。公開設定はアクセス制御を使用して行う。ファイル単位かフォルダ単位かは NAS による。	デフォルトは自分のみファイル・フォルダを使用可能。公開設定を行うことにより他者に公開可能となる。
アクセス制御	ユーザ認証を設定した場合可能。PC に設定した Windows ログインユーザと同じユーザを NAS に設定。大規模に行うには ActiveDirectory 等のユーザ認証サーバが必要になる。	公開とアクセス制限は Hiroin ID により設定可能。
記録容量	NAS のディスク容量次第で記録容量は選択できる。記録容量が足りない場合は、NAS ユーザ自身が大容量 HDD への交換・USB HDD 増設等により容量を増やすことができる。	デフォルトで30GB。容量の変更は可能。
停電・瞬時電圧低下(瞬電)対策	NAS ユーザが UPS を設置する。	必要ない。クラウド側で対応。
データの実体の場所	NAS に置かれる。ローカル PC との同期機能設定をした場合は、ローカル PC と NAS 上に共に置かれる。	ローカル PC とクラウド上に共に置かれる。(デフォルト)。
故障によるデータ消失の可能性	有り。	ローカル PC 側は有り。クラウド側は対応。
ローカル PC とのファイルの同期機能	有り。	有り。デスクトップクライアント利用で自動的に同期をとることができる
セキュリティ対策	有料のアンチウイルスソフト等有り。	クラウド側で対応。アクセス制御に関しての総当たり攻撃対応。Hiroin ID のセキュリティ対策有り。
学外から	(通常は)使用できない。(ただし方法はあ)	使用できる。(ただし日本国内のみ)

3 弘大クラウドを使いましょう

3.1 NAS と併用したい

NAS を使っていても弘大クラウドを利用しましょう。既に NAS に共有ファイル・フォルダが存在しデータをため込んでいる場合、弘大クラウドを NAS のバックアップにしましょう。グループ・担当等の共有データならば、係長等の職名アカウントの弘大クラウド上のフォルダを公開設定しましょう。公開範囲は担当に所属する人の Hiroin ID に対して公開設定をすれば、NAS と同じ様に使用できます。同期設定をしなければ、クラウド上には過去のファイルを残すことができます。PC で間違えて削除してしまった場合でも、ファイルが残っていれば安心できます。また、フォルダ単位で公開設

定を行えるので、職名アカウントのフォルダ中でサブフォルダを公開フォルダとすれば、個人用のファイル・フォルダは非公開とできます。

3.2 個人のバックアップとして

個人の PC にデータをため込んでいる場合、今すぐに弘大クラウドをバックアップにしましょう。この原稿を作成しているとき、Windows の異常により自分のファイルが消えてしまったという事態が発生しました。幸い、ユーザプロファイルが読み込めなかったため、仮ユーザプロファイルでログインしたことになりファイルが消えてしまったように見えただけでした。再度ログインすると本来のユーザプロファイルでログインすることができました。元通りにはなりませんが原因は不明です。再発するかもしれません。このときは慌てました。これまで仕事で蓄積してきた文書データが全て失われたかもしれないからです。PC の故障、Windows の障害等はいつ発生するかわかりません。バックアップはとりましょう。

3.3 その他

事務用 PC の更新が行われる場合でも、弘大クラウド上にファイルをコピーしておく、新しい PC に必要なファイルをコピーして仕事ができるように設定することも簡単にできます。

デスクトップクライアントをインストールして、弘大クラウドへのログインを気にせずに使用するならば、完全に自分のローカル PC 上のフォルダで作業している場合と同じ感覚で使用できます。ローカル PC 上のフォルダと弘大クラウドの同期をとるようにすれば、リアルタイムでファイルの変更・削除・作成等が反映されます。同期をとった場合、ローカル PC に弘大クラウド上のファイル・フォルダがコピーされます。このコピーはリアルタイムで弘大クラウド上のオリジナルと同期がとられます。また、このコピーはネットワーク接続ができない環境でも使用することができます。

出先でインターネット接続ができるならば、直接弘大クラウドにアクセスして仕事ができます。インターネット接続ができなくてもローカル PC 上のコピーを使用して仕事ができます。便利です。

学務情報担当では、職名アカウント gakujou について共有設定を行っています。新入生向けの学務情報システム利用の手引き作成などについて、簡単に共同作業を行うことができます。

3.4 Web かデスクトップか

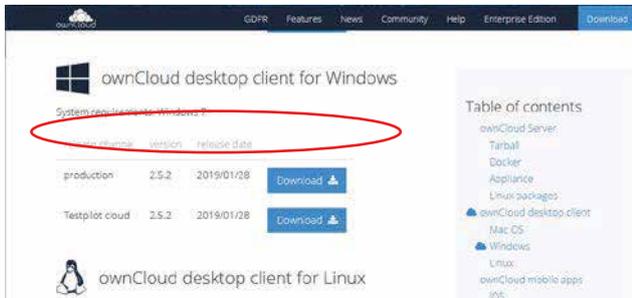
Web から使用するか、デスクトップクライアントから使用するかはどのように判断すれば良いのでしょうか。ファイルの同期が必要なく NAS と同じ様に使うのであれば、ログインの手間はありますが Web からの使用を勧めます。ローカル PC のファイル・フォルダと同じ様に扱いたいのであれば、デスクトップクライアントの導入を勧めます。インストールの手間はありますが、やはり使い勝手が良いです。ログインの手間もなくローカル PC のファイルと同様に使用できます。

4 おわりに

色々書いてきました。まずは使ってみましょう。そろそろバックアップしようと思っていたときに PC が壊れるということはあることです(マーフィーの法則)。ローカル PC のデータを弘大クラウドにコピーしてバックアップしましょう。ここで一つ注意することがあります。弘大クラウドは Hiroin ID で認証していることと、学外からアクセスできることから、Hiroin ID のパスワードは長いものをつけましょう。総合情報処理センターのパスワード変更のための注意書にしたがって強度のあるパスワードを使ってください。

5 Windows へのデスクトップクライアントのインストール方法

単純にバックアップ用に弘大クラウドを使用するのであれば、Web ブラウザから利用するのが一番です。Web ブラウザ経由での利用については、総合情報処理センター「弘大クラウドを利用したファイルの受け渡し・共有と同期」(<http://www.cc.hirosaki-u.ac.jp/hirodai-cloud-howto>)を参照してください。ここではデスクトップクライアントのインストールについて説明します。上記ページからクライアントダウンロードサイトへと移動します。



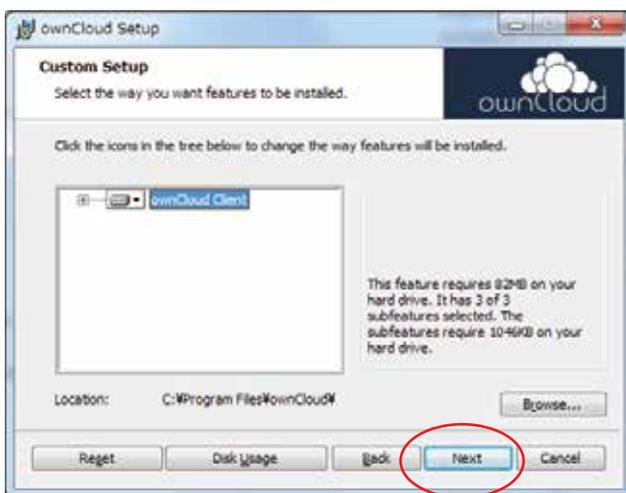
1.Windows 版のクライアントソフトをダウンロードする。ダウンロードしたファイルは必ずウイルスチェックをする。異常が確認されなかったら、ファイルを実行しインストールを行う。以下の例では、Windows ユーザー miyamoto にデスクトップクライアントの設定を行う。



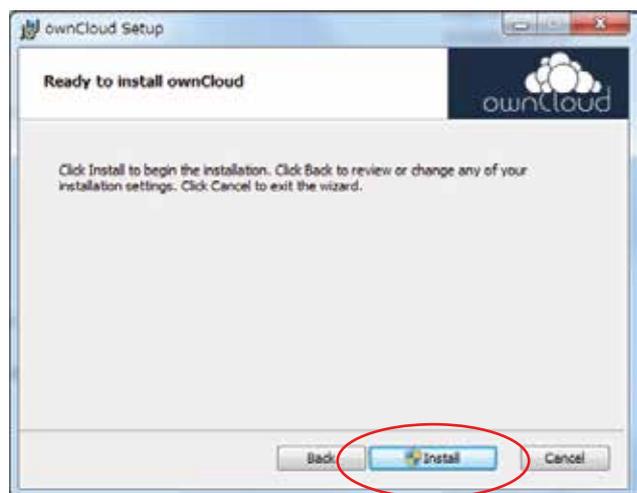
2.実行をクリック。



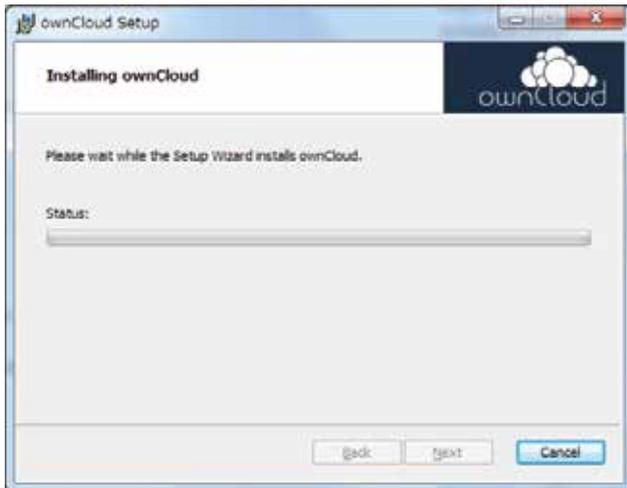
3.Next をクリック。



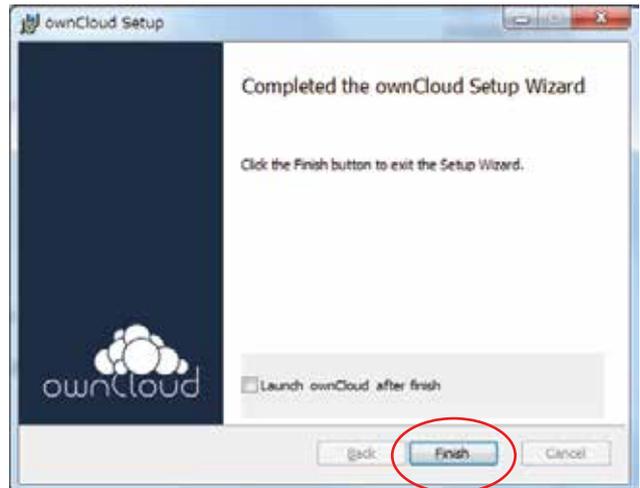
4.Next をクリック。



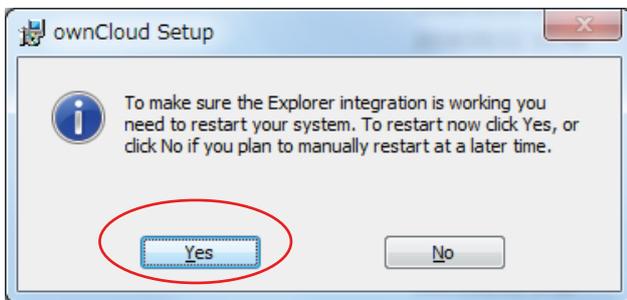
5.Install をクリック。



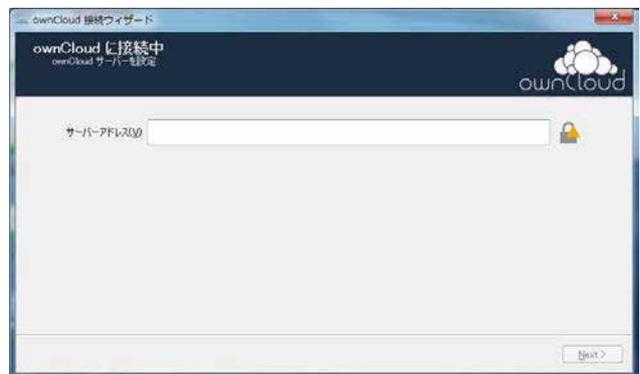
6.インストールが始まる。このときプログラムの変更可否をきかれるので可とする。



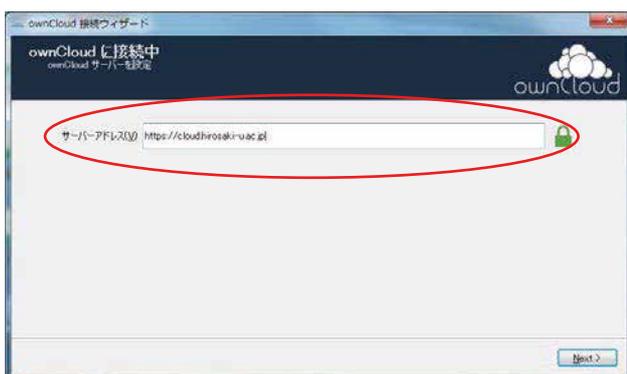
7.終了。Finish をクリック。



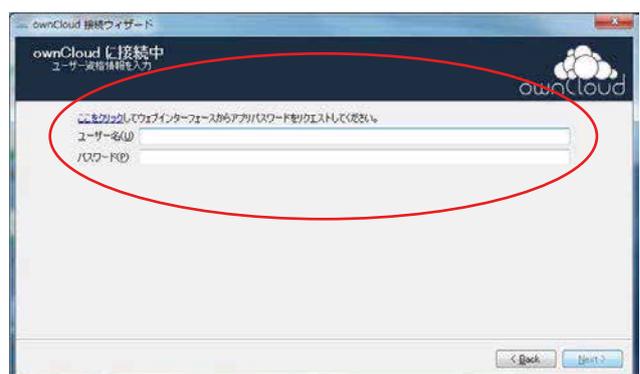
8.セットアップダイアログが表示される。
Yes をクリック。
Windows を再起動する。



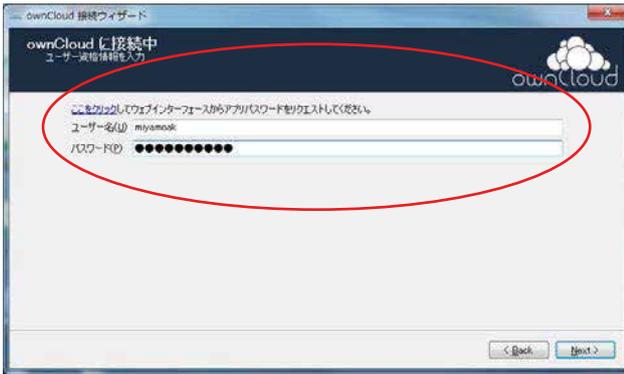
9.接続ウィザードが起動するので設定を行う。



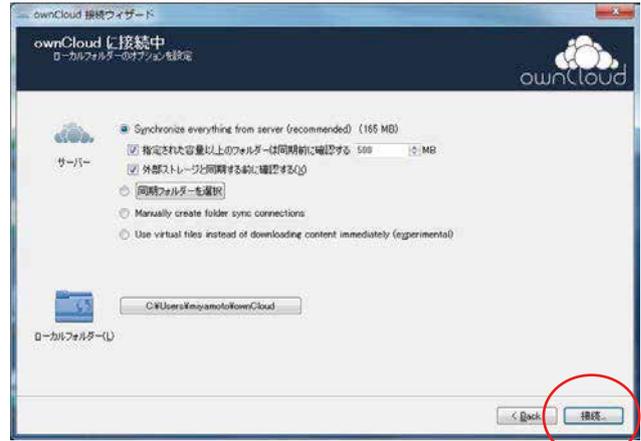
10.サーバアドレスを入力する。
<https://cloud.hirosaki-u.ac.jp>
Next をクリック。



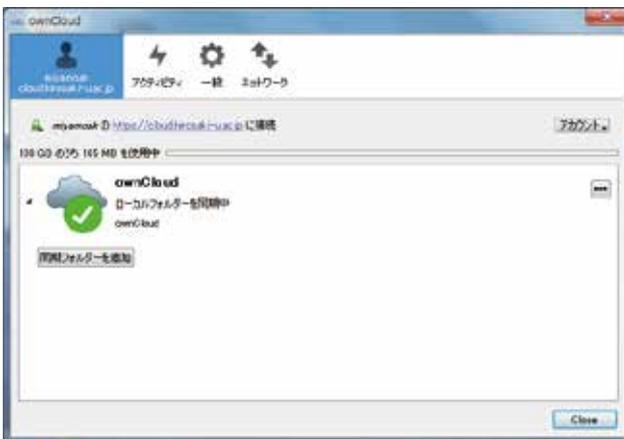
11.Hiroin ID のユーザ名とパスワードを入力する。



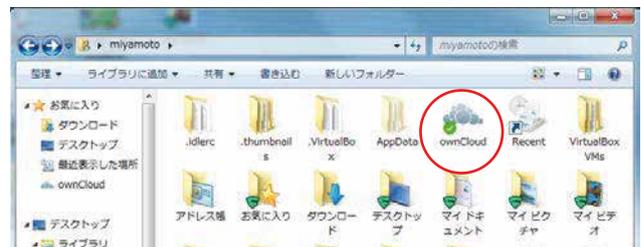
12.この例では、Hiroin ID は miyamoak で設定する。
Next をクリック。



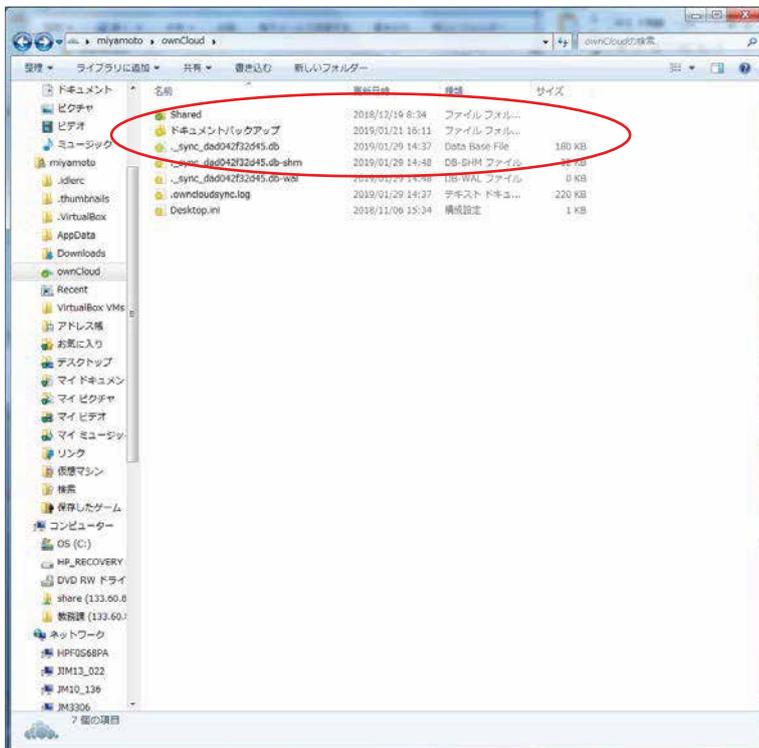
13.初期設定をする。デフォルトでよい。
接続をクリック。



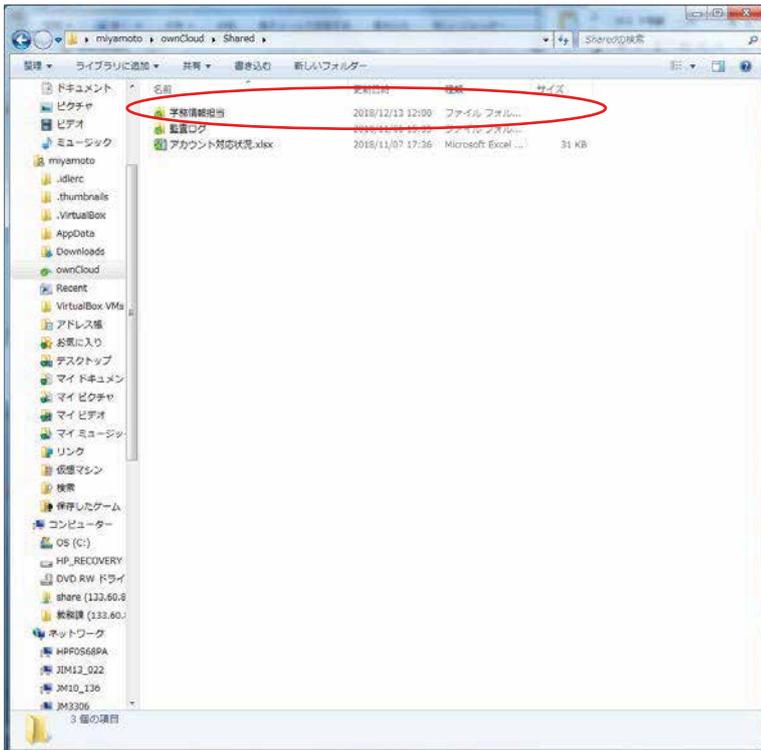
14.弘大クラウド上のフォルダが自分の PC 上のローカルフォルダに同期される。



15.エクスプローラーで確認すると、確かにフォルダ miyamoto の下にフォルダ ownCloud が表示されている。チェックはローカルフォルダと弘大クラウド上のフォルダが同期していることを示す。



16.Windows ユーザ miyamoto のローカルフォルダとして ownCloud が表示されている。サブフォルダとして Shared とドキュメントバックアップがある。Shared は他のユーザの公開フォルダがマウントされる場所である。このフォルダには自分のファイル等をコピーしてはいけない。緑色のチェックマークはクラウドとローカルフォルダが同期していることを示す。ドキュメントバックアップは Hiroin ID miyamoak で設定したクラウドに作成したサブフォルダである。同期させていないのでチェックマークがついていない。ローカル PC のバックアップ用途として使用している。



17.フォルダ Shared の下にサブフォルダ 学務情報担当がある。これは、職名アカウント gakujou に作成した教務課学務情報担当で使用する共有フォルダである。gakujou が miyamoak に公開設定と同期許可をしている。

サブフォルダ学務情報担当は同期しているため、自分の PC での作業結果がリアルタイムに反映される。

弘前大学における標的型攻撃メール対応訓練とフィッシング対策

葛西 真寿^{1),2)}, 須藤 勝弘³⁾, 小倉 広実³⁾, 竹内 淑伶³⁾

- 1) 弘前大学 大学院理工学研究科
 - 2) 弘前大学 総合情報処理センター
 - 3) 弘前大学 附属図書館 情報基盤グループ
- cnc-director@hirosaki-u.ac.jp

The trainings against the targeted attack e-mails and anti-phishing measures in Hirosaki University

Masumi Kasai^{1),2)}, Katsuhiro Suto³⁾, Hiromi Ogura³⁾, Sumire Takeuchi³⁾

- 1) Graduate School of Science and Technology, Hirosaki Univ.
- 2) Computing and Networking Center, Hirosaki Univ.
- 3) Hirosaki University Library

概要

本稿では、本学が策定した情報セキュリティ対策基本計画に基づいて平成 28 年度と 29 年度に実施した標的型攻撃メール対応訓練について事例紹介する。また、平成 30 年 6 月に発生したフィッシングメールによる情報漏えいを受けて本学が実施した対策や、有効性が期待されるフィッシング対策についてもあわせて紹介する。

1 はじめに

昨今多発している情報セキュリティインシデントを受け、中長期的な視点を持って情報セキュリティ対策の強化を組織的かつ計画的に実施するため、本学は平成 28 年度を起点とした弘前大学情報セキュリティ対策基本計画を策定し、学長了承のもと全学情報総括責任者（企画担当理事）の指示により全学体制で実施している。本稿では、この基本計画に基づいて平成 28 年度と 29 年度に実施した標的型攻撃メール対応訓練について事例紹介する。

また、平成 30 年 6 月に発生したフィッシングメールによる情報漏えいを受けて本学が実施した対策や、有効性が期待されるフィッシング対策についてもあわせて紹介する。

2 平成 28 年度標的型攻撃メール対応訓練

平成 28 年度の標的型攻撃メール対応訓練は、本学役員並びに課長級以上の幹部職員から抽出した 105 名を対象として実施した。訓練メールの配信は、平成 29 年 2 月 27 日と 3 月 6 日の 2 回行った。第 1 回及び第 2 回の訓練メール本文は以下の通りである。



図 1. 平成 28 年度第 1 回訓練メール本文

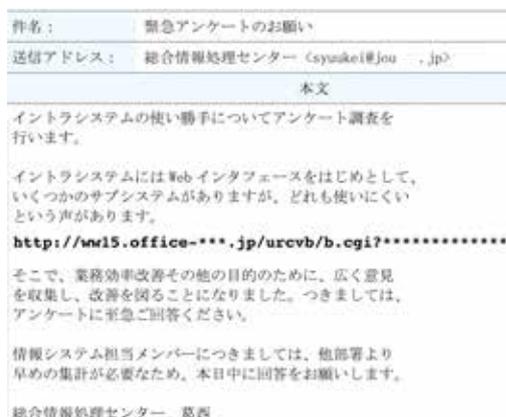


図 2. 平成 28 年度第 2 回訓練メール本文

訓練結果の概要を紹介する前に注意しておくが、平成 28 年度の訓練は、受注した業者がいうところの（難易度が高く、ひっかかりやすい）「レベル 3」模擬攻撃メールであった。ご本人の快諾を得て実在する理事の実名で送信したことや、一斉送信メールによる事前予告なく送信したこともあり、受信した役員・幹部職員が模擬攻撃メールと思わず、非常に高い関心を持って受け止められ、文中のリンク先についても極めて迅速なクリックが行われたため、「開封率」（本文中の不審リンクをクリックする率）が高くなった。

3 平成 28 年度訓練結果概要

第 1 回の訓練メールについては、実在する理事の実名で送信したこともあり、受信した役員・幹部職員の多くから非常に高い関心を持って受け止められたため、比較的多くの受信者が本文中のリンク先をクリックして開封してしまった。冷静に見れば、送信者のアドレスが弘大メールアドレス（***@hirosaki-u.ac.jp）ではないことから、不審メールであることは判断可能である。しかし、役員が使用しているスマートフォンのメールアプリでは、デフォルトでは送信者のメールアドレスまで確認できないため、実在の理事からのメールと信じたまま、本文中のリンクをクリックしたとの報告が事後にあったように、実在の理事の表示名に反応してクリックしてしまうことが開封率を上げた要因と考えられる。

第 2 回の訓練メールでは開封率は大きく下がったが、第 1 回の訓練メールの送信者である理事に比べれば役職的に下位である総合情報処理センター長の実名で送信したためなのか、2 回目であることによる訓練の効果なのか、判断が難しい。

訓練で重要視したのは開封率そのものよりも、不審メールを受信した際の対応状況である。不審メールを受信した旨を弘前大学 CSIRT に報告した件数は、第 1 回、第 2 回とも少なかった。一つの理由として、訓練メール受信者が役員・幹部職員だということがあげられる。通常業務では報告を受ける側であることも留意する必要があるかもしれない。

4 平成 29 年度標的型攻撃メール対応訓練

平成 29 年度の訓練は、本学職員からランダムに抽出した 1000 アカウントに対して、平成 30 年 1 月 30 日および 2 月 14 日の 2 回にわたって模擬攻撃メールを送信することで実施した。今回は 1000 アカウント対象の大規模な訓練であるため、一斉送信メール等で

事前に十分な訓練予告の周知を行った上で実施した。訓練メール本文を以下に示す。

Subject: 震災時の行動マニュアルについて
 Date: Tue, 30 Jan 2018 10:37:40 +0900
 From: 危機管理担当 <info_***@yah00co.jp>
 Reply-To: kunren_***@yah00co.jp
 To: ***@hirosaki-u.ac.jp

東日本大震災の経験を踏まえ、大規模地震が発生した場合の行動マニュアルを整備しました。

内容を確認いただき、適切に対応いただくようお願いいたします。

http://www1.***.co.jp/cgi-bin/check.cgi?code..

以上

図 3. 平成 29 年度第 1 回訓練メール本文

Subject: ホームページのリニューアルについて
 Date: Wed, 14 Feb 2018 10:13:06 +0900
 From: 営業担当 <support_***@yah00co.jp>
 Reply-To: kunren_***@yah00co.jp
 To: ***@hirosaki-u.ac.jp

各位

お疲れ様です。

このたび営業活動の一環として、ホームページをリニューアルしました。

なかなかの出来栄です。取引先やお客さまにご紹介するなど、営業活動に活用してください。

http://www1.***.co.jp/cgi-bin/check.cgi?code=..

図 4. 平成 29 年度第 2 回訓練メール本文

平成 28 年度訓練と比較すれば、平成 29 年度の模擬攻撃メールは「レベル 1」相当であり、実名を使用せず、明らかに怪しそうな文面とした。またメール形式をテキストメールとし、リンク URL が明らかに不審とわかるようにした。そのために、デフォルトでは弘大メールが迷惑メールと判断してしまい、訓練にならないため、ホワイトリストに入れて迷惑メールフォルダに落ちないようにする必要があった。

5 平成 29 年度訓練結果概要

模擬攻撃メール本文中のリンクをクリックして開封した受信者の割合は、第 1 回が 14.5%、第 2 回が 4.0% であり、2 回目の不審 URL のクリック率が減少したことがわかり、模擬攻撃メールを 2 回受信したことによる一定の抑止効果が見られる。また、不審メール報告者の割合は、第 1 回が 17.9%、第 2 回が 15.3% と、どちらも一定の不審メール報告があり、しかも 2 回目もそれほど低下していない。理由の一つとしては、訓練開始と終了を一斉送信で十分に周知したこと、不

審メール報告者全員に対して報告に対する謝辞と不審メールを受信した際の対応策を含む回答メールを送信したことで、訓練に対する参加意識が低下しなかったことが考えられる。

6 不正転送による情報漏えいと対策

平成 30 年、本学職員に対してフィッシングメールの送信があり、本学が利用している電子メールサービスのログイン画面に似せた偽サイトへの誘導により、パスワードが詐取され、12 名の職員のアカウントに対して、本人になりすまして不正な転送設定が行われるという事態が発生した。これらのメールアドレスに届いたメールが不正に外部へ転送され、メールアドレス情報を含む情報漏えいが発生した [1]。

本学 CSIRT および総合情報処理センターでは、事態把握後ただちに当該フィッシングメール受信者全員に対して、不正転送設定の有無を確認後、不正に設定された転送先については削除し、当該メール受信者全員のパスワード変更をおこなった。

さらに、本学の全ての構成員に対して、学外へのメール転送設定を禁止し、全ての学外へのメール転送設定を削除した。(ただし、スマートフォンではない携帯電話のみを利用している学生の事情を考慮し、学生に対しては、携帯電話 3 社へのキャリアメールへの転送に限り転送を許可する例外措置を設けている。) 禁止措置後も学外へのメール転送設定を行った場合には管理者へアラートがあがり、その都度利用者への事前通告なしに管理者が転送設定を削除している。

7 フィッシング対策

以上の措置で、不正転送設定による情報漏えいを防止しているが、フィッシングメールによってパスワードが詐取されれば、本人になりすましてログインされて(不正転送設定以外の方法で)メール等の不正な閲覧が可能になってしまう。

訓練や教育啓蒙によってフィッシングメールによるパスワード詐取被害は減少させることはできてもゼロにすることは現実的には不可能である以上、パスワードが詐取されることを前提とし、たとえパスワードを詐取されても不正なアクセスを阻止できるようなフィッシング対策が必要である。

本講演では、有効性が期待できるフィッシング対策のうちの以下の項目について、概要を紹介する。

- 多要素認証

- 高度なフィッシング脅威防御オプション
- 不正アクセス保護機能を含む包括契約

8 おわりに

セキュリティ強化、利用者の利便性確保、経費節減、これら 3 点はどれも重要な要素であるが、実際にはこれらの 3 点を「全て同時に」満たすフィッシング対策を立案することは極めて困難な作業である。たとえば、セキュリティ強化は当然すべきこととして、利用者の利便性も確保するとなると、経費節減は困難であり一定の支出は避けられない。また、経費節減をはかりながらセキュリティ強化を推進するとなれば利用者の利便性の確保が困難になる。

情報セキュリティ強化対策の立案については経営判断が必須であり、実施にあたっては全学的な合意形成が肝要と考える。

参考文献

- [1] 【お詫び】フィッシングメールによる個人情報の漏えいについて | 弘前大学
<https://www.hirosaki-u.ac.jp/35460.html>
 に掲載の報道発表資料。

AXIES 大学ICT推進協議会 2018年度 年次大会
[TC1-1]

弘前大学における 標的型攻撃メール対応訓練と フィッシング対策



弘前大学 総合情報処理センター長



葛西 真寿

標的型攻撃メール対応訓練

「開封率」(ひっかかり率)の多少に
一喜一憂するのが目的ではない!

標的型攻撃メール対応訓練

目的：標的型攻撃メールを受信したときに
どう対応するかを体験し確認すること

本番と同様の手順・同様の対応で…

- CSIRT への通報
- CSIRT の対応（通報に対する回答）

本学で実施した訓練の 概要と見えてきた課題

平成28年度 役員・幹部職員に実施

対象者数

105名

実施日時

第1回

訓練メール配信 : 2017年 2月 27日 13:00

集計締め切り : 2017年 2月 28日 17:00

第2回

訓練メール配信 : 2017年 3月 6日 13:00

集計締め切り : 2017年 3月 7日 17:00

・第1回訓練メール (URL型)

件名 : アンケートに関するご協力をお願い

送信アドレス : 理事 (企画担当) 吉澤 <pcsecurity@office-enq.jp>

本文

職員の皆様

日々の業務お疲れ様です。
昨今、企業におけるウイルス感染等による情報漏えい事件が度々報道されておりますが、本学においてもセキュリティ対策の一環としてウイルス対策ソフトの運用、並びに個人PCのセキュリティアップデートに関する状況についてアンケート調査を行います。

以下の「アンケート票」に必要事項をご記入の上、明日16時まで各自回答ください。なお、本件に関する問合せは、情報システム担当へ行わないようご注意ください。

お忙しいところ大変恐縮ですが、ご協力をお願いいたします。

[\[URL\]](http://ww15.office-enq.jp/urcvb/b.cgi?62GXhQKo2vOGNR3cKwhfxw) <http://ww15.office-enq.jp/urcvb/b.cgi?62GXhQKo2vOGNR3cKwhfxw>

理事 (企画担当) 吉澤

・第2回訓練メール (URL 型)

件名： 緊急アンケートのお願い
 送信アドレス： 総合情報処理センター <syuukei@jousys.jp>

本文

イントラシステムの使い勝手についてアンケート調査を行います。

イントラシステムには Web インタフェースをはじめとして、いくつかのサブシステムがありますが、どれも使いにくいという声があります。

[\[URL\]](http://ww15.office-enq.jp/urcvb/b.cgi?62GXhQKo2vOGNR3cKwhfxw) <http://ww15.office-enq.jp/urcvb/b.cgi?62GXhQKo2vOGNR3cKwhfxw>

そこで、業務効率改善その他の目的のために、広く意見を収集し、改善を図ることになりました。つきましては、アンケートに至急ご回答ください。

情報システム担当メンバーにつきましては、他部署より早めの集計が必要なため、本日中に回答をお願いします。

総合情報処理センター 葛西

3 訓練結果概要

[開封率について]

第1回の開封率は **55.2%** でした。弊社の標的型攻撃メール対応訓練サービスにおける第1回訓練での平均開封率(20.1%)と比較して、高い数値でした。

第2回の開封率は **20.0%** でした。弊社の標的型攻撃メール対応訓練サービスにおける第2回訓練での平均開封率(13.6%)と比較して、やはり高い数値でした。

第1回の訓練で開封した方が第2回で開封しなかった割合(学習効果)は **77.6%** でした。訓練を通して標的型攻撃メールに対する認識が高まっていたものと思われます。

しかし、**第2回でも21名の方が開封されており、開封率も高い状況です**ので、**標的型攻撃に対する備えという点ではまだ不十分と言えます**。このような訓練を継続的に実施いただくことで、常に標的型攻撃メールへの警戒心を高め、脅威に備えるようにしてください。

今回の訓練でメールを開封された方々(特に両方とも開封してしまった13名の方)については、セキュリティ教育などを通して標的型攻撃メールについて再認識いただくとともに、不審なメールに気付くためにはどういったことに注意を払えばいいかといった知識を身に付けていただく必要があるものと考えます。(後述の『**不審なメールを見極める方法**』をご参照ください。)

平成28年度役員・幹部職員向け 訓練に関する注釈

- 訓練開始の具体的日時通知なし
- 「レベル3」の模擬攻撃メール
- **実在の理事の実名で送信**
非常に高い関心と迅速なクリック

3 訓練結果概要

[不審なメールを受信した際の対応状況について]

報告件数

第1回:	8件	(7.6%)
第2回:	6件	(5.7%)

**課題は、URLクリック数よりも
不審メールの報告件数の少なさ**

平成29年度 職員1000名対象の大規模訓練実施

以下の内容を全教職員に事前通知

訓練名称：標的型攻撃メール対応訓練

実施対象：本学職員からランダムに抽出した1000アカウント

実施時期：平成30年1月30日 10:00 から 11:00,

および 2月14日 10:00 から 11:00

実施内容：上記実施期間の間に、対象者に擬似攻撃メールを計2回送付

訓練メール1

Subject: 震災時の行動マニュアルについて

Date: Tue, 30 Jan 2018 10:37:40 +0900

From: 危機管理担当 <info_express@yah00co.jp>

Reply-To: kunren_info@yah00co.jp

To: ****@hirosaki-u.ac.jp

東日本大震災の経験を踏まえ、大規模地震が発生した場合の行動マニュアルを整備しました。

内容を確認いただき、適切に対応いただくようお願いします。

<http://tameswww1.toinx.co.jp/cgi-bin/hbusguwz/check.cgi?code=...>

以上

訓練メール2

Subject: **ホームページのリニューアルについて**
Date: Wed, 14 Feb 2018 10:13:06 +0900
From: **営業担当 <support_helpdesk@yah00co.jp>**
Reply-To: kunren_info@yah00co.jp
To: ****@hirosaki-u.ac.jp

各位

お疲れ様です。
このたび営業活動の一環として、ホームページをリニューアルしました。
なかなかの出来栄です。
取引先やお客さまにご紹介するなど、営業活動に活用してください。

<http://tameswww1.toinx.co.jp/cgi-bin/hbusguwz/check.cgi?code=177003020002621816>

以上

- **第1回開封者：145名（14.5%）**
- **第2回開封者：40名（4.0%）**

- **第1回メール報告者：179名（17.9%）**
- **第2回メール報告者：153名（15.3%）**

**本番と同じ通報先へ報告依頼
1回目も2回目も
ある程度の不審メール報告数**

- 第1回開封者：145名（14.5%）
- 第2回開封者：40名（4.0%）

- 第1回メール報告者：179名（17.9%）
- 第2回メール報告者：153名（15.3%）

**メール報告者に対しては
全て一人一人に回答し、
センターWeb記事の参照を周知**

179名+153名の報告者全員への回答メール

○○○○様,

弘前大学 CSIRT です。

平素より情報セキュリティ確保に御協力いただき、ありがとうございます。

この度は、不審メールのご報告をいただき、ありがとうございます。
不審メールを受信した際の対応については、センター Web サイトの
以下の記事に記載しましたので、今一度ご確認願います。

「標的型攻撃と思われる不審メールを受信した際の対応について【訓練】」
<http://www.cc.hirosaki-u.ac.jp/blog/12897>

自動応答ではなく、人力で

--

葛西 真寿 弘前大学 CSIRT リーダー

KASAI Masumi cnc-director@hirosaki-u.ac.jp

迷惑メールフィルタや 危険な添付ファイル削除機能

それでも100%遮断は
困難

利用者一人一人の**気づき**
だけではなく

**利用者一人一人の気づき
だけではなく
標的型攻撃は防げない
ことを前提とした対策を！**

本学で決定した対策

全学情報システム運用委員会審議事項

- 構成員全体の情報セキュリティの意識レベルの向上 (1)~(8)
- 弘大メール(Office365)におけるセキュリティ強化 (1)~(2)
- インシデントを未然に防止するための対策 (1)~(3)
- 弘大CSIRTへの報告 (1)~(2)

1. 全教職員の パスワード変更

**未変更者はメール使用不可
(今週実行済：経費不要)**

2. 全教職員の多要素認証 移行決定 (来週より実行：経費不要)

多要素認証

- Office 365 の現在の契約プランでも追加費用なく多要素認証を導入可能
- パスワード以外に追加のセキュリティ確認
 - スマホアプリで通知
 - スマホアプリに表示されるパスコードを入力
 - 携帯電話にSMSで送信されたパスコードを入力
 - 携帯電話に電話をかけてくるので#を入力
 - 固定電話に電話をかけてくるので#を入力

多要素認証導入の意義

**パスワード詐取をゼロには
できないことを前提に**

多要素認証導入の意義

**パスワード詐取をゼロには
できないことを前提に**

**たとえパスワードを詐取されても
不正ログインできないようにする**

3. Office 365 フィッシング防護オプション 導入決定 (来月より：経費要)

Microsoft 365 A5

- 国外からのアクセス制限ができないか…
に対するマイクロソフト社からの提案
- フィッシングメール対策や不正アクセス保護機能
を含む**包括契約**
(ATP や Office クライアントアプリを含む)
- 一人当たり参考価格 円/年 ×
(常勤非常勤を問わず) ナレッジワーカー数

Advanced Threat Protection

- 未知のマルウェア・ウイルスに対する保護
- 悪意ある URL に対するクリック時の保護
- 1アカウント当たり参考価格  円/年

Trend Micro Cloud App Security

- 未知のマルウェア・ウイルスに対する保護
- 悪意ある URL に対するクリック時の保護

4. 本年度メール訓練 全教職員対象に実施 (本年12月実施予定)

あなたのメールが送信されませんでした

メール利用者各位,

現在、送信サーバの障害により、あなたのメールが送信できない状態が続いていますこと
をお詫びします。再送を希望する場合は>>[ここをクリック](#)<<してサインインしてくだ
さい。

メールチームは現在、原因究明に取り組んでいます。ご迷惑をおかけしていることをお
詫びします。

The Office365 team

訓練用メール文案は、
6月インシデントのフィッシングメールのパクリ

差出人 Mail Delivery System <MAILER-DAEMON@messagelabs.com>

件名 Message Delivery Failure

Your Messages Has Not Been Sent

Dear @hirosaki-u.ac.jp

We coherently encountered outgoing server failure which left Most of your mails undelivered. Some of your mails were affected and can be resent now.
>>[Click here](#) << to resend these mails.

Microsoft and Office365 team are always working to give you the best email experience. We are sorry for any inconvenience caused.

Thank you,

The Office365 team

5.組織体制の強化

現行総情センターの機能も含む

「情報連携統括本部」設置

(平成31年4月設置予定)

終



葛西 真寿

弘前大学 総合情報処理センター長

cnc-director@hirosaki-u.ac.jp

eduroam サービスについて

附属図書館情報基盤グループ 小倉 広実

ogura@hirosaki-u.ac.jp

1. eduroam とは

eduroam (Education Roaming) とは、国立情報学研究所が提供するローミングサービスです。高等教育機関や研究機関等において、国際的にキャンパス無線 LAN の相互利用が可能となり、本学も加盟しています。大学等から発行される ID があれば、eduroam を提供している日本国内の大学のみならず、世界中の大学から無線 LAN を経由してインターネットに接続することが可能になります。本学に訪問する学生や研究者は、所属先のユーザ ID とパスワードを使い、弘前大学に設置された無線 LAN アクセスポイントを経由してインターネットに接続することが可能になります。

2. 来学者の利用

学外からの来学者が持ち込み機器で無線 LAN を使用したい場合、eduroam アカウントをお持ちであれば eduroam サービスが利用できます。使用する場所に総合情報処理センターが提供する無線 LAN のアクセスポイントからの電波が届いていれば、Hiroin Wi-Fi、Hiroin Wi-Fi 5GHz のほかに eduroam という SSID が見えると思います。この eduroam に接続してご利用いただくことが可能です。



eduroam アカウントを持っていない来学者には、一定期間、学内でのみ使用可能な臨時の eduroam アカウントを発行することができます。利用には本学役職員(役員、教員、事務職員等)が責任者となり、当センターが用意している以下の申請ページから事前に申し込む必要がありますので、来学前に訪問先の役職員へご依頼ください。

- 来学者のための臨時 eduroam アカウント申請(学内限定)
<http://www.cc.hirosaki-u.ac.jp/rinji-eduroam-shinsei>
- 学内開催学会等のための複数臨時 eduroam アカウント申請(学内限定)
<http://www.cc.hirosaki-u.ac.jp/group-rinji-eduroam-shinsei>

3. 本学役職員の利用

Hiroin ID を有する本学役職員は、特別な申請なしに eduroam を利用できます。他大学(外国を含む)で eduroam を使う際には弘大メールアドレス(hiroin-id@hirosaki-u.ac.jp)とパスワードを入力してください。Hiroin ID だけでなく、@hirosaki-u.ac.jp まで入力する必要があります。eduroam 利用の際には、個人にひもづいた Hiroin ID(個人 ID)を使用してください。

4. 参考

eduroam の利用方法や参加機関等については、国立情報学研究所が公開している以下のウェブページを参考にしてください。

- 利用者向け情報

https://www.eduroam.jp/for_users/

無線LANアクセスポイント

	設置場所	設置台数
文 京 町 地 区 （ 3 9 6 台 ）	理工学部1号館	53
	理工学部2号館	23
	コラボ弘大・コラボレーションセンター	34
	農学生命科学部	42
	総合情報処理センター	18
	教育学部	71
	大学会館	11
	合宿所	1
	附属図書館	14
	人文社会科学部	34
	総合教育棟	63
	事務局	12
	保健管理センター	3
	50周年記念会館	9
遺伝子実験施設	4	
本 町 地 区 （ 2 0 1 台 ）	医学部基礎校舎	48
	社会医学講座研究施設	7
	健康未来イノベーションセンター	4
	医学部コミュニケーションセンター	6
	臨床研究棟	28
	エネルギーセンター	1
	学生支援センター1号棟	14
	学生支援センター2号棟	4
	本町地区共同利用施設	3
	動物実験施設・RI施設	3
	臨床講義棟	4
	保健学研究科・総合研究棟	64
	附属病院外来診療棟	14
	附属病院第1病棟	1
附属病院第2病棟	2	
女性医師職場復帰支援施設	2	
（ 3 2 台 学 校 ） 園	附属小学校	12
	附属中学校	13
	附属幼稚園	1
	附属支援学校	6
	計	629

総合情報処理センター 事業報告

(2018年4月～2019年3月)

講演・口頭発表

- 葛西 真寿, “標的型攻撃メール対応訓練と「実戦」における対応”, 平成30年度TOPICネットワーク担当職員研修会, 東山グランドホテル, 2018年9月
- 葛西 真寿, “フィッシングメールによる 情報漏えいと対策”, 平成30年度弘前大学情報セキュリティセミナー, 弘前大学, 2018年10月
- 葛西 真寿, “弘前大学における標的型攻撃メール対応訓練とフィッシング対策”, 大学ICT推進協議会 2018年度年次大会, 札幌コンベンションセンター, 2018年11月

実施事業(情報セキュリティ対策)

- 全教職員のパスワード変更 2018年11月
- 全教職員の多要素認証導入 2018年11月
- Office 365 フィッシング防護オプションの導入 2019年2月
- 標的型攻撃対応訓練の実施 2019年2月
- 情報セキュリティセミナーの実施 2018年10月, 2019年3月

編集後記

今回の特集では、現行、そして 2020 年に更新が予定されている次期の本学情報基盤システムに望むこととして、利用者の皆様からいろいろとご意見ご要望をいただきました。経費の必要なものについては、すぐに対応！とはいきませんが、センタースタッフのスキルと創意で改善できる点については、知恵を出し合って改善していきたいと思えます。

(葛西)

研究教育を含むあらゆるところで情報基盤システムの利用が必須になっている一方で、さまざまな情報セキュリティの脅威にもさらされています。次期情報基盤システムでは、よりよい環境整備が図られることが期待すると共に、自分自身も情報に翻弄されないように気をつけようと考えています。

(大橋)

8 年前に着任した頃、教育学部はまだ Wi-Fi 圏外、有線でも接続が不安定。音楽関係の授業中にウェブ上の資料を視聴することにはリスクがあり、すべて一旦ローカルに保存していました。今や、どの教室でも Wi-Fi 接続でストリーミングを快適に再生できるどころか、学生たちがそれぞれスマホで検索して、こちらが用意しなかったものまで聞かせ合っています。10 年後にはどうなっているのか想像もつきませんが、更なる環境整備に期待しつつ、自分が IT 落伍者にならないよう精進いたします。

(朝山)

農業の分野でも農業×IoT によるスマート農業が行われるようになってきています。しかしながら、IoT で「見える化」された環境データをしっかり読み切る目もまた必要になってきています。デジタルとアナログは、永遠の友達だなんて思っているのは小生のみでしょうね。ますます発達する情報技術を上手に利用していくために、総合情報処理センターがもつ機能をさらに充実させていくことが極めて重要だと思います。

(松山)

今号は「情報基盤システムに望むこと」のテーマで教員・学生からたくさんの方々のご意見を頂いています。コンピューター言語を全く理解していない小生にとって附属病院長のお話は非常に耳が痛いところです。といった横からおそらくは訓練用のフィッシングメールが届き、即座にゴミ箱に投げています。「君子危うきに近寄らず」なのでしょうが、不安な時にすぐに相談・対応をお願いできるご相談センターがあれば、ポーっと生きている小生は、悪い癖と知りつつ、つい考えてしまいます。

(下田)

一昔前までは不審な電話に要注意でしたが、不審メールに要注意、不審なサイトに要注意など、身の回りが不審だらけになってきました。最近では本物ってなんだろう・・・と思う有様です。結局真実は自分で直接見つけに行くしかないのかもしれませんが。不審なメールの送付主にならないように気を配る毎日です。

(野坂)

今年も例年並とは言えないお天気で推移してきましたが、異常が続くとこれが通常と錯覚してしまいます。メールも不要なものや怪しげなものをゴミ箱に直行する設定にしていると流行っていることに気が付かないでいることとなります。センターの更新でセキュリティ対策の強化が望まれているようですが、機械も万能ではないので今一度自分自身取っている対策を見直そうと思う今日このごろです。

(丹波)



弘前大学総合情報処理センター広報

HIROIN 第36号

平成31年3月 発行

編集 弘前大学総合情報処理センター
教育広報専門委員会

発行 弘前大学総合情報処理センター
〒036-8561 青森県弘前市文京町3番地
Tel 0172-39-3721
Fax 0172-39-3722

印刷 やまと印刷株式会社
〒036-8061 青森県弘前市神田4-4-5
Tel 0172-34-4111
Fax 0172-36-3299