

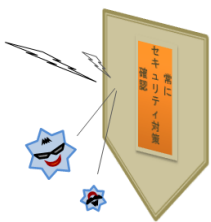


c / i c k !

情報処理センター通信

CONTENTS

- ◆情報処理センターからのお知らせ
 - ・サーバの脆弱性《例年より多い、危険度の高い脆弱性として注意喚起》1-2
 - ・平成26年度卒業生・修了生(及び退学者・除籍者)のアカウント削除について2-3
- ◆情報処理センターレポート
 - ・情報セキュリティへの取り組み ～～ 学生委員会主催「サークルリダ研修」に於いて当センターの森本康彦准教授が「クラウドサービス活用における情報セキュリティ対策」を講演3
 - ・大判プリンタの平成26年使用状況4
- ◆編集後記4



◆情報処理センターからのお知らせ

●サーバの脆弱性《例年より多い、危険度の高い脆弱性として注意喚起》

コンピュータのOSやアプリケーションにて、プログラムのバグ(誤りや欠陥)により、本来設計された機能以外の動作をして発生する情報セキュリティ上の欠陥を脆弱性(*1)と言い、Windows系のOSにて確認された脆弱性はWindowsUpdateを実行し修正プログラムを適用することで改善されることはご存知と思います。サーバ用のOSでも脆弱性は存在しており、特に今年度は危険度の高い脆弱性として注意喚起されたものが例年より多く、情報処理センターでは適宜修正や対策を実施し、関連するシステムの管理担当への注意喚起を行っております。

サーバ用OSとして広く使用されているLinuxには無償で利用できるものがあり、研究等にて使用している方も多いと思いますが、ベンダーや情報セキュリティサイトからの脆弱性や修正プログラムの配布などの情報をこまめに確認し、適切に対応してください。

参考までに今年度深刻な脆弱性として注意喚起されたものとセキュリティ情報提供サイトを挙げますので、サーバ管理担当の方は対応をお願いします。これらの情報は学芸ポータルのお知らせへも随時掲載しています。

《参考》*1脆弱性(ぜいじゃくせい)とは？(国民のための情報セキュリティサイト:総務省)
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/basic/risk/11.html

・DNSキャッシュポイズニング攻撃(2014/04)

DNSサーバが偽のDNS情報で汚染される可能性があります。

【参考】DNS キャッシュポイズニング攻撃に関する注意喚起 (JPCERT/CC)

<https://www.jpcert.or.jp/at/2014/at140016.html>

・OpenSSL脆弱性(Heartbleed)(2014/04)

システムメモリ内の情報や秘密鍵など漏えいの可能性

【参考】ウェブサイト運営者の方へ - OpenSSL 脆弱性対策のお願い (IPA)

<https://www.ipa.go.jp/security/ciadr/vul/20140408-openssl.html>

・Apache Struts2脆弱性(2014/07)

不正なサーバ操作や任意のコード実行の可能性

【参考】Apache Struts2の脆弱性対策について(CVE-2014-0094)(CVE-2014-0112)(CVE-2014-0113) (IPA)

<https://www.ipa.go.jp/security/ciadr/vul/20140417-struts.html>

・bash脆弱性(2014/10)

任意のコード実行の可能性

【参考】bash の脆弱性対策について(CVE-2014-6271 等) (IPA)

<https://www.ipa.go.jp/security/ciadr/vul/20140926-bash.html>

・SSL3.0プロトコル脆弱性(2014/10)

通信の一部が第三者へ漏えいする可能性

【参考】SSL 3.0 の脆弱性対策について(CVE-2014-3566) (IPA)

<https://www.ipa.go.jp/security/announce/20141017-ssl.html>

・NTP脆弱性(2014/12)

任意のコード実行の可能性

【参考】Weekly Report 2014-12-25号【1】ntpd に複数の脆弱性 (JPCERT/CC)

<https://www.jpcert.or.jp/wr/2014/wr145001.html#1>

・glibc脆弱性(2015/01)

任意のコード実行の可能性

【参考】glibc の脆弱性対策について(CVE-2015-0235) (IPA)

<https://www.ipa.go.jp/security/announce/20150129-glibc.html>

●平成26年度卒業生・修了生(及び退学者・除籍者)のアカウント削除について

3月で卒業・修了する学生(及び退学・除籍となる学生)が利用していたアカウントは4月以降は廃止となり利用できなくなります(大学院に進学される学生も対象です)。このことに伴い、在学中に作成・保存したデータもアカウントと共に削除されます。削除されたデータは後日復元することはできませんので大切なデータやメールは各自で全てバックアップしておいて下さい。

【アカウント削除の対象】

- ・平成27年3月に卒業(修了)した学生 (学部/研究生→修士、修士→博士など進学する学生もアカウント削除の対象です。進学時に新規にアカウントが発行されます。)
- ・平成27年3月31日時点で大学の籍を失った退学・除籍等の学生

【アカウント削除の手続きの日程】

平成27年4月1日より順次

《この日の前日までに必要なデータやメールは全てバックアップしておいて下さい》

【利用できなくなるもの】

- ・パソコンの学内ネットワーク接続認証

休学や留学等の理由により在籍期間が延長する学生は削除対象外です。情報処理センターに対して個別に延長の申請等はありません。次年度も継続して利用できます。

≫ 次頁に続く ≫

- ・学内に開設しているウェブサイトの利用 (http://www.u-gakugei.ac.jp/~アカウント名/ 以下のファイル)
(http://local.u-gakugei.ac.jp/~アカウント名/ 以下のファイル)
- ・ファイル共有システムの利用
- ・その他情報処理センターシステムの利用、及びシステムにて作成・保存したデータの利用

【大学メールアドレスについて】

- ・卒業生および修了生 … 引き続きご利用になれます。ただし、一般のYahoo!メールと同様にログイン後のWeb画面には広告が表示されます。
- ・退学者および除籍者 … 大学メールアドレス(xxxxxx@st.u-gakugei.ac.jp)はご利用になれませんが、Yahoo!JAPAN IDおよびYahoo!メールアドレス(yyyyyy@yahoo.co.jp)は引き続きご利用になれます。

◆ 情報処理センターレポート

- **情報セキュリティへの取り組み** ～～ 学生委員会主催「サークルリーダー研修」に於いて
当センターの森本康彦准教授が「クラウドサービス活用における情報セキュリティ対策」を講演



平成26年12月10日(水)、学生委員会主催によるサークルリーダー研修の中で本学情報処理センターの森本准教授から「クラウドサービス活用における情報セキュリティ対策」と題してC410教室にて講演が行われました。参加者は、サークルリーダー等の学生を中心に250名ほどでした。

内容は、米セレブのプライベート写真流出事件を例に情報漏えいの原因について紹介しました。

具体的な情報漏えいの原因として

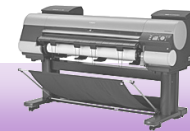
1. 簡単なパスワード設定
2. 「パスワードリセット」機能の悪用
3. パスワードの使い回し
4. フィッシング詐欺によるアカウント情報の窃取

などの事例について具体的に説明の後、結局PCやスマホに侵入する不正プログラムに、それらの認証情報自体を取られてしまっは元も子もないこと、個人情報を狙う脅威からあなたを防護する総合セキュリティ対策ソフトの導入は必須であることの解説がありました。

最後にSNSやスマホを、「楽しく」、「安心して」、使うことができるように、

「パスワード管理を徹底」し、「リスクを考慮した賢いユーザになる」ことを、
いつも頭に置いて、21世紀を生きる者として当たり前の行動ができるようになろう
ということで講演を締めくくりました。



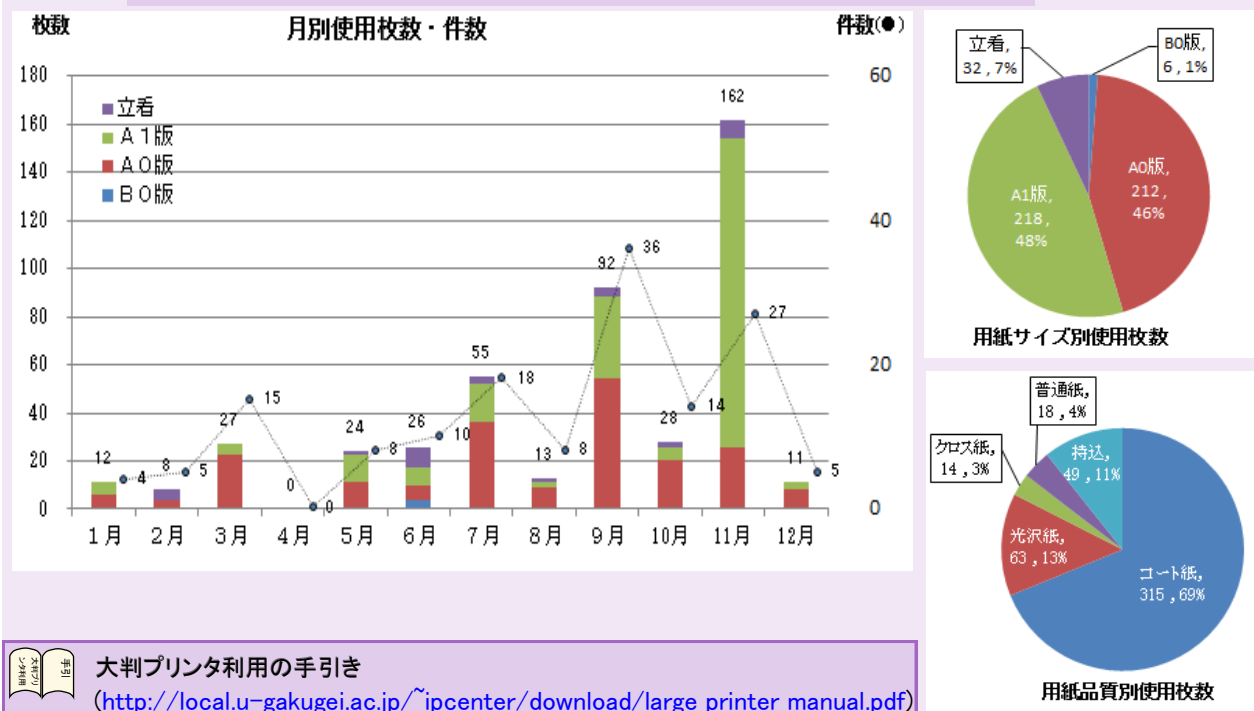


● 大判プリンタの平成26年使用状況

大判プリンタでは、最大B0ノビ(1118mm×1580mm)相当のポスターや、立て看板・横断幕などの印刷を行うことができます。但し、[大判プリンター利用の手引き](#) (学内のみ下記URLからダウンロード可)にも記載してあるとおり大判プリンタの利用は教職員に限られています(教員指導による印刷時の学生使用は可)。

平成26年も利用は多く、150件457枚(*1)の印刷となり、ほぼ平成25年に同じ(150件450枚)です。このように多くの方に利用していただけるのはありがたいことですが、利用マナーについてのご協力もよろしくお願いいたします。特に発表会などが集中する時期は、事前予約かつ予約通りのご利用を心がけて下さい。

注. (*1)B1サイズは2枚でB0サイズ1枚、A2サイズは2枚でA1サイズ1枚に換算して集計。



大判プリンタ利用の手引き

(http://local.u-gakugei.ac.jp/~ipcenter/download/large_printer_manual.pdf)

編集後記

TwitterやYouTubeなど普段何気なく使っているSNSや共有サービスですが、海外にての痛ましい事件で加害者側の発信手段としても利用されている様を見て、なんだか使うことが薄気味悪くなってしまいました。もちろん適切に使用していればまず問題が起こることはないのですが、意見の捉え方も人それぞれですし、思いもつかない所から個人情報特定される場合もあるということも本号記載の森本先生による講演にもありました。便利さや楽しさばかりに目を奪われがちですが、システムの特長やリスクも意識しながら慎重に利用しなければいけませんね。(竹)



国立大学法人 東京学芸大学

[情報処理センター](#)

☐TEL 042-329-7710 ☐FAX 042-329-7711

☐URL <http://www.u-gakugei.ac.jp/~ipcenter/>

☐E-mail ipcenter@u-gakugei.ac.jp