KDS 国大協サービス

国立大学リスクマネジメント情報

2015(平成27)年12月号　　http://www.janu-s.co.jp/

特集テーマ

情報セキュリティ最新情報

今年は、大規模な情報漏えい事件・事故が発生し、世間の注目を集めた年でした。
今年最後の１２月号では、情報セキュリティに関する最新の情報をお伝えします。

１．高まる情報リスク

１）頻発する大学を狙ったサイバー攻撃

本誌の「大学リスクマネジメント News PickUp」のコーナーを振り返ってみても、今年は、ＵＳＢメモリの紛失といったおきまりの情報漏えい以外に、大学への執拗な攻撃が報道されています。

＜サイバー攻撃の踏み台＞

2/ 2 ○○大学は、学内のNAS（ネットワーク接続ストレージ）が悪用され、約10万通の迷惑メール（スパムメール）を学外に送信していたと発表。

6/ 7 ○○大学のサーバが海外の3つの国から相次いで不正なアクセスを受け、アメリカの企業へのサイバー攻撃の中継点として悪用されていたことが判明。

6/ 9 ○○研究所のサーバがサイバー攻撃の踏み台に使われていたことが判明。民間事業者のサーバを試用していたが動作確認のためアクセス制限を一時的に緩めていた。

＜ホームページの改ざん＞

4/21 ○○大学医学部のホームページがシリアのハッカー集団とみられる組織に改ざんされたことが判明。県警が不正アクセス禁止法違反の容疑で捜査を開始。

＜標的型メール攻撃＞

6/22 ○○大学の事務用のパソコンが去年12月に標的型メールによってウイルスに感染し、2300人余りの学生や教職員の個人情報（名前や学籍番号など）が流出していたことが判明。

＜不正アクセス＞

7/13全国の6つの大学でホームページを狙ったサイバー攻撃が相次いで確認。メールマガジンに登録されたメールアドレスが流出したり、ホームページを管理するためのIDが流出。未公開情報へのアクセスを許してしまうシステムの欠陥を狙ったとみられる。

7/16 ○○大学は、学内の業務用パソコンに不正アクセスがあり、学生の氏名や学生証の番号など最大で3万6000件余りの情報が流出したと公表。職員に会議に関するメールが届き、添付ファイルを開き感染。

7/24 ○○大学は、学内メールへの接続パスワードを何者かが不正取得し、学生や教職員ら1116人分の名前、電話番号、就職先などの情報が漏えいしたと発表。ロシア経由で不正接続されたことを突き止めたが、パスワードを取得できた理由は不明。不正取得された教員のメールアドレスには、大量のメールが送り付けれらており、このアドレスから少なくとも6万件のメールが送信された。

＜ウイルス感染＞

8/ 6 ○○大学は、大学所有の業務用パソコンがウイルスに感染したと発表。当該パソコン内には環境省委託調査に協力した母親、父親、子供の数千人分の個人情報が含まれており、外部流出の有無について調査。環境省専用パソコンで情報管理することになっていたが、大学の業務用パソコンを使用。

Tel:050-3533-8794, 03-5283-0051 Fax:03-5283-0052 E-mail:info@janu-s.co.jp

2）近年のサイバー攻撃の特徴

増加するインターネットにおけるハッカー等の攻撃は、高い能力を持つ訓練された組織的なものであるといわれています。また、国家が関与する攻撃が戦争のように行われているともいわれています。

株式会社シマンテックが公表した「インターネットセキュリティ脅威レポート第 20 号」（ISTR：Internet Security Threat Report, Volume20）のプレスリリースでは、最近のインターネットにおける攻撃者の傾向として、次のようなものを挙げています。

攻撃において高まったスピードと正確性

2014 年には過去最高となるゼロデイ脆弱性が記録されました。シマンテックの調査では、ソフトウェア企業がプログラム修正のためのパッチの作成と公開を行うまでに必要な日数は、2013 年にはわずか 4 日であったのに対し、2014 年には平均で 59 日であったことが明らかになりました。これがシステムのゼロデイ脆弱性です。攻撃者はこうした遅延を利用し、Heartbleed というソフトウェアのバグのケースでは 4 時間以内に脆弱性の悪用が急増しました。2014 年には全部で 24 のゼロデイ脆弱性が発覚し、パッチが提供される前に攻撃者に既知のセキュリティ上のすき間（ギャップ）を悪用させる抜け穴となっていました。

一方で高度な攻撃者は、ターゲットを絞りこんだスピアフィッシング攻撃によるネットワーク侵害を続けており、2014 年には合計 8%の増加となりました。昨年特に興味深かったのはこのような攻撃の正確性であり、ターゲットに到達するために使用された電子メールは 20%減少し、より多くのマルウェアのドライブバイダウンロードと、その他の Web ベースの攻撃に起因するものでした。

- ある企業から盗んだメールアカウントを使用し、より規模の大きい企業にスピアフィッシング攻撃を仕掛ける。
- 企業の管理ツールとプロセスを利用し、企業ネットワークから出ていく前に盗んだ IP を動かす。
- 被害者のネットワーク内部で自前の攻撃ソフトウェアを作成し、攻撃者の行動を隠蔽する。

デジタルの世界で金銭や個人情報の盗難が増加傾向

サイバー犯罪者はソーシャルメディアを使った詐欺で素早く現金を入手出来ますが、一方でランサムウェアなどのより利益が得られる積極的な攻撃手法を利用する者もあり、それらは昨年 113%増加しました。特に、ランサムウェアの CryptoLocker による攻撃の被害は 2013 年に比べて 45 倍増えました。従来のランサムウェアに見られるように違法コンテンツに対して法的な罰金を科すふりをするのではなく、攻撃者の意図を隠さず被害者のファイルや写真などのデジタルコンテンツと引き換えに金銭を要求する悪意あるランサムウェアの CryptoLocker による攻撃が多くなっています。

※ ゼロデイ攻撃
　修正プログラムが公開される前に公表されたソフト等の脆弱性を攻撃する手法。
※ スピアフィッシング攻撃、標的型攻撃、水飲み場型攻撃
　不特定多数にメールを送りつけてウイルスに感染させるのではなく、特定の企業や組織に対してターゲット用にカスタマイズされた手法で感染を狙うのがスピアフィッシング攻撃。研究を重ねターゲットが開封するように工夫されたメールを送りつけたり（標的型攻撃）、ターゲットが閲覧するサイトにウイルスを忍ばせる（水飲み場型攻撃）手法が用いられる。
※ ドライブバイダウンロード
　Web サイトにアクセスしたユーザが気が付かないうちにウイルスをダウンロードさせる。
※ ランサムウェア
　感染した PC 等を制御できないようにし、その解除のための金銭を要求するウイルス。

＜参考＞　（株）シマンテック「インターネットセキュリティ脅威レポート第 20 号」プレスリリース
http://www.symantec.com/ja/jp/about/news/release/article.jsp?prid=20150414_01

2．政府の対応

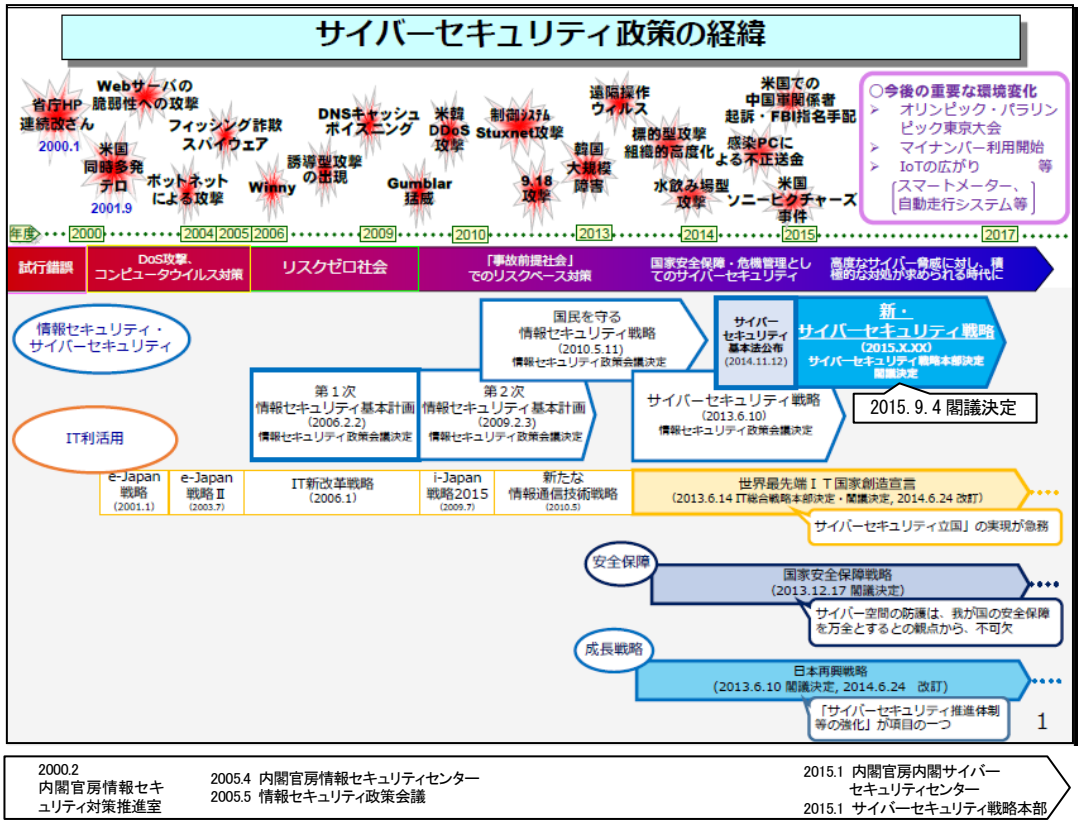
政府機関や重要インフラ、企業へのサイバー攻撃の深刻化、外国の国家機関の関与が疑われる攻撃の顕在化等、スマートフォンや機械の制御システム（モノのインターネット（IoT））の普及に対応するため、政府は、サイバーセキュリティの確保に向けて、サイバーセキュリティ基本法を制定、平成 27 年 1 月、サイバーセキュリティ戦略本部、内閣官房内閣サイバーセキュリティセンター（NISC）が司令塔として設置され、9 月 4 日新「サイバーセキュリティ戦略」が閣議決定されました。

今年５月に起こった日本年金機構の不正アクセスによる個人情報の流出事案に関しては、NISC が日本年金機構と外部との不審な通信をキャッチし、いち早く対応を行いました。また、日本年金機構、厚生労働省による報告書作成に加え、サイバーセキュリティ対策本部が原因究明調査結果の報告書を公表し、攻撃の特徴と対策、サイバーセキュリティ戦略本部及び NISC がとるべき再発防止対策を示しています。

⇒ **「不正アクセスによる情報流出事案に関する調査結果報告」**
（平成 27 年 8 月 20 日　日本年金機構不正アクセスによる情報流出事案に関する調査委員）
http://www.nenkin.go.jp/files/kuUK4cuR6MEN2.pdf

「検証報告書」
（平成 27 年８月 21 日　日本年金機構における不正アクセスによる情報流出事案検証委員）
http://www.mhlw.go.jp/stf/shingi2/0000095311.html

「日本年金機構における個人情報流出事案に関する原因究明調査結果」
（平成 27 年 8 月 20 日　サイバーセキュリティ戦略本部）
http://www.nisc.go.jp/active/kihon/pdf/incident_report.pdf



（H27.2.10 サイバーセキュリティ戦略本部第１回会合資料４に補足）

また、経済産業省では、ＩＴを利活用する企業の経営者を対象として、サイバー攻撃から企業を守る原則や重要項目をまとめた「サイバーセキュリティ経営ガイドライン（案）」を取りまとめ、12月15日にパブコメが締め切られ、今後、策定の作業が進められます。

⇒　「サイバーセキュリティ経営ガイドライン（案）［初版］」
（経済産業省・独立行政法人情報処理推進機構）
http://search.e-gov.go.jp/servlet/Public?CLASSNAME=PCMMSTDETAIL&id=595215022&Mode=0

3．大学の情報セキュリティ

大学等をターゲットにしたサイバー攻撃が増加していることについては、１．１）で報道事案を紹介しましたが、大学が狙われる要因として次のようなことが考えられます。

① 学生、患者の膨大な個人情報が保存されている
② 科学技術に関する重要な情報を保有している
③ 一方、開かれた大学として、外部への窓を開いておかねばならず、
④ かつ、学部学生、大学院生、研究員、医療従事者等の構成員が多く短期間に入れ替わる

各大学では、情報基盤センター等の担当部署を中心に、セキュリティ対策を講じていますが、執拗な攻撃にさらされたり、構成員の不注意による個人情報の流出や紛失の事案が引き続き起こっています。

膨大な対策のなかで、構成員全員が対策を講じられるのは、ウイルス感染の防止と感染時の初動対応です。
ウイルスに感染しないためには、ＯＳやセキュリティソフトを最新のものに常に更新する、不審なメールは開かない、不審なサイトは閲覧しないということが常識です。
しかし、対策ソフトに検知されない最新のウイルスを送り込んだり、日常のメールのやり取りを監視、知人を差出人にして内容もそれらしくする等、安心して開封してしまうようなメールを巧妙に偽装する手口も使われます。

⇒　独立行政法人情報処理推進機構（ＩＰＡ）「標的型攻撃メールの例と見分け方」
http://www.ipa.go.jp/files/000043331.pdf

現状では、高度な能力により執拗に繰り返される攻撃を防ぐことは不可能といわれており、セキュリティ対策においては、ウイルスへの感染を想定し、感染後の被害の回避や低減の対策を多重に導入することが提唱されています。独立行政法人情報処理推進機構（ＩＰＡ）では、次のような対策を紹介しています。

１）ウイルス感染リスクの低減

① ソフトウェアの更新の習慣化および徹底
② セキュリティソフトウェア（ウイルス対策ソフト）の導入
③ メールの添付ファイルのブロック
④ ウェブフィルタリング
⑤ 教育や訓練

２）重要業務を行う端末やネットワークの分離

① 一般の端末と重要業務システムとの分離

② 部署など業務単位でのネットワークの分離

３）重要情報が保存されているサーバでの制限

① 共有フォルダのアクセス権の設定

② データの暗号化やパスワードによる保護

４）事後対応の準備

① 有事の際に迅速に対応するための体制の整備

② 手順書や外部連絡先の準備

⇒ 独立行政法人情報処理推進機構（ＩＰＡ）
「ウイルス感染を想定したセキュリティ対策と運用管理を」
http://www.ipa.go.jp/security/ciadr/vul/20150602-secop.html

各大学では、セキュリティ・ポリシーや規程を定め、情報セキュリティの強化に努めておられると思いますが、現実に起こる事案を見てみると、内規に違反した個人情報の取扱いや USB の持ち出し等が原因であるものも散見します。

割れ窓を放置すると全ての窓が割られるという割れ窓理論を持ち出すまでもなく、いくら立派な規程やマニュアルをつくっても、規則に反する行為を放置すれば、いずれはそれが常態化してしまいます。日本年金機構の個人情報の取扱いも規則が守られていれば最小限の流出で済んだといわれています。

日々の業務や教育・研究において、常にセキュリティを念頭においた行動ができるように、大学全体で意識を高めることが必要です。

情報セキュリティマネージメントシステム（ＩSMS）の第三者認証を取得大学する大学も増えてきています。ＩSMSは、適用範囲内の全ての情報資産について、その機密性、完全性、可用性の維持を行い、情報セキュリティレベルを自ら向上させるシステムであり、一般社団法人日本情報経済社会推進協会がＩSO規格、ＪＩS規格による第三者認証を行っています。

ＩSMS認証取得国立大学

静岡大学情報基盤センター
宇都宮大学総合メディア基盤センター
山口大学
徳島大学情報センター
九州大学学術情報基盤センター
長崎大学
鹿児島大学学術情報基盤センター
岡山大学情報統括センター
横浜国立大学情報基盤センター
室蘭工業大学情報メディア教育センター
広島大学情報メディア教育研究センター
琉球大学総合情報処理センター

（取得順）

⇒ 一般社団法人日本情報経済社会推進協会 ＩSMS認証取得組織検索
http://www.isms.jipdec.or.jp/lst/ind/

参照

「国立大学リスクマネジメント情報」（2011（H23）年２月号）
＜特集＞ 情報セキュリティ、個人情報関連事故
http://www.janu-s.co.jp/mail_magazine_html_data/110230.html

H27.11月

大学リスクマネジメント　News PickUp

＜Web 上のニュースから検索＞

＜大学の管理・経営＞

11．11　労使協定を超えた時間外労働と休日労働、深夜割増賃金の不払いなどの法令違反により、労働基準監督署が○大学病院に対し是正勧告を行っていたことが判明。

＜事件・事故＞

11．2　建設会社が杭工事の施工データを偽装していた問題で、○大学の教室棟の工事でデータ偽装が確認。その後、他の複数の大学で学生寮、セミナーハウス、大学会館の偽装が発覚。

11．3　○大学病院で頭部の手術を受けた患者が手術後に脳梗塞で死亡したのは医師に過失があったためとして、患者の遺族が大学に慰謝料約5700万円の損害賠償を求める訴を提起。

11．11　○大学病院は、腎臓の機能を調べる検査値について4年間にわたり電子カルテの表示に誤りがあったと発表。患者221人分が確認されたが、治療は適切と説明。

＜入試等ミス＞

11．24　○大学は、今月実施した公募制推薦入試で、選択肢の中に正解がない出題ミスがあったと発表。

＜情報セキュリティ＞

11．6　○大学は、講師が担当科目の履修者情報（528人の学籍番号、氏名など）入りのUSBを紛失したと発表。

11．10　○大学病院の医師が患者665人分の個人情報（手術を受けた患者の氏名、生年月日、病名など）を記した書類約30枚分を紛失したと発表。バッグに入れて帰宅途中に飲食し、タクシーに乗った。

11．27　○大学病院は、医師が輸血を受けた患者584人分の個人情報（氏名、住所、電話番号など）が記録されたUSBを紛失したと発表。

＜ハラスメント＞

11．10　○大学は、新歓コンパ後、女子学生の胸を触るセクハラ行為をしたとして教授を停職5か月の懲戒処分。

11．27　○大学は、同僚にセクハラやパワハラに当たる発言を繰り返していたとして、職員を停職3か月の懲戒処分。

＜学生・教職員の不祥事＞

11．9　○大学の名誉教授が、指定暴力団の元幹部から海外での投資に充てる資金として2000万円を借り今も返済していないことが判明。大学は、10日、非常勤講師の職を解雇。

11．26　○大学は、授業中にデモの練習と称して現政権や安全保障関連法を批判する言葉を学生に言わせたとして、准教授を停職3か月の懲戒処分。

11．27　○大学は、学内の宿泊施設の利用者から徴収した宿泊料約2300万円を着服したとして職員を懲戒解雇したと発表。大学は刑事告訴の方針。

＜不正行為＞

11．4　学内の研究紀要に掲載した論文2本に一部盗用があったとして○大学が、教授を諭旨解雇処分にしていたことが判明。

11．5　○大学は、教授の執筆した5つの論文に盗用があったと発表。

11．11　○大学の准教授が発表した論文に教え子の修士論文からデータなどを無断使用する不正行為があったことが判明。大学は、停職4か月の懲戒処分とする方針。

配信について

本誌は、各国立大学・大学共同利用機関の国大協保険ご担当者、国大協連絡登録先、ご登録いただいた方にメールで配信させていただいております。（無料）　配信登録、解除は弊社ホームページからお願いします。⇒ http://www.janu-s.co.jp/

情報提供のお願い

各大学等でのリスクマネジメントに関する取組み、事故・事件への対応のご経験、ご感想、ご要望等をお寄せください。
⇒　info@janu-s.co.jp

バックナンバー

15.11月　過労死等防止大綱とストレスチェック
15.10月　人を被験者とする研究と補償措置
15．9月　台風、豪雨、落雷と保険
15．8月　国大協保険の保険金支払概況（２）
15．7月　ICT活用教育と法律問題
15．6月　国際交流活動対応支援セミナー報告
15．5月　学生生活とトラブル
15．4月　大学生のための安全・安心基礎講座
15．3月　研究者の倫理
※弊社ホームページからダウンロードできます。

発　行　有限会社　国大協サービス
東京都千代田区神田錦町３−２３
協　力　株式会社インターリスク総研
三井住友海上火災保険株式会社