

## 情報セキュリティに関する最新動向調査

データベース部門 上繁 義史

いまでは、様々なサービスがネットワーク（インターネット）を介して提供されています。本学においても、学習・研究環境や様々な業務システム等がネットワーク化されて提供されています。また、ネットワークに接続される情報端末も PC だけではなく、携帯電話や情報家電など多岐にわたってきました。その中で、情報セキュリティはいまや必要不可欠の要素です。その一方でソフトウェアの脆弱性をついた情報インシデント（情報漏洩等の事故）は悪質化・巧妙化の一途をたどっていて、常に最新情報を収集しておくことが必須となっています。

そこで、本センターでは、情報セキュリティの要素技術、法整備状況、運用について、最新の動向を調査するために、下表に示すシンポジウム、研究会などに参加・聴講しました。それぞれの参加概要については次項の資料編に掲載しています。

表：情報セキュリティに関するシンポジウム、研究会等

番号	開催日	シンポジウム、研究会等の名称
1	平成21年2月28日(土)	第3回 JSSM セキュリティ公開討論会
2	平成21年3月27日(金)	平成20年度新世代情報セキュリティ研究開発シンポジウム
3	平成21年3月28日(土)	日本セキュリティマネジメント学会 平成20年度第4回 ITリスク研究会
4	平成21年6月19日(金)	第9回 ISS スクエア水平ワークショップ 情報漏えい対策シリーズ第2回「事例に学ぶ情報漏えい対策」
5	平成21年7月17日(金)	おおいたネットあんしんセミナー

資料 情報セキュリティに関する最新動向調査の概要

「情報セキュリティに関する最新動向調査」で紹介しました、シンポジウム、研究会等の参加・聴講の概要を以下にご紹介いたします。

番号	1	開催日	平成 21 年 2 月 28 日
名称	第 3 回 JSSM セキュリティ公開討論会		
会場	東京電機大学神田キャンパス 7 号館		
主催	日本セキュリティマネジメント学会 (JSSM)、(協賛：情報セキュリティ大学院大学、後援：情報セキュリティ政策会議、総務省、文部科学省、経済産業省)		
参加者数	約 150 名		
概要	<p>本公開討論会は 2 月 2 日の「情報セキュリティの日」の関連行事として開催されました。前半は、行政サービス、ICT の利用、新型インフルエンザ対策、食品業界におけるリスクや課題について講演がありました。後半は電子マネーと電子決済について、技術面、法制面の視点からの基調講演があり、その話題を受けてのパネルディスカッションが行われました。</p> <p>この公開討論会では、IT リスク学の確立と電子マネー・電子決済の話題が特に興味深い内容を含んでいました。長崎大学においても教育、業務等の IT 化が促進されていますが、その中でシステムを構築・導入する段階、運用する段階、万一システムに起因する事故が起こった時など、IT リスクに対する認識を深めておくことが重要と言えるでしょう。</p>		

番号	2	開催日	平成 21 年 3 月 27 日
名称	平成 20 年度新世代情報セキュリティ研究開発シンポジウム		
会場	東京ステーションコンファレンス 503 会議室		
主催	経済産業省 (実施事務局：みずほ情報総研株式会社)		
参加者数	約 100 名		
概要	<p>本シンポジウムは経済産業省が平成 17 年 4 月より実施している「新世代情報セキュリティ研究開発事業」の一環として、平成 20 年度採択された 5 件の研究テーマについて研究開発の状況に関する報告会として開催されました。なお、各研究テーマは 2 年間の期間が設けられており、今回の発表はその中間報告に当たります。採択されたテーマは以下の 5 件です：</p> <ol style="list-style-type: none"> <li>(1) 「既存 OS に挿入可能な仮想マシンモニタによる異常挙動解析とデバイス制御の研究開発」</li> <li>(2) 「モデル検査による組み込みソフトウェア検証とモデリング・パターン化の研究開発」</li> <li>(3) 「組み込みシステムに対するセキュリティ評価技術の研究開発」</li> <li>(4) 「証明可能な安全性を持つキャンセルラブル・バイオメトリクス認証技術の構築とそれを利用した個人認証インフラストラクチャ実現に向けた研究開発」</li> <li>(5) 「生体認証サービスにおける情報漏洩対策 (キャンセルラブル・バイオメトリクス) の研究開発」</li> </ol>		

本シンポジウムでは、複雑化する一方の ICT において、一般ユーザに負担をかけることなく安全性を向上させる研究について発表が行われていました。いずれの研究も、実用化に至るまでには様々なハードルがあるものの、喫緊に必要とされるものであったことを付け加えておきたいと思います。

番号	3	開催日	平成 21 年 3 月 28 日
名称	日本セキュリティマネジメント学会 平成 20 年度第 4 回 IT リスク研究会		
会場	東京電機大学神田キャンパス 11 号館 16 階 1601 室		
主催	日本セキュリティマネジメント学会		
参加者数	約 30 名		
概要	<p>この研究会では、「リスクの評価」に焦点を当てて、4 件の講演が行われました。特別講演として、原子力分野で行われているリスク分析の考え方と操作員等の人間によるリスクの影響について紹介が行われました。また、研究発表としてネット情報をリスク分析に応用する手法、リスクコミュニケーションの一手法、電子文書の長期保存における暗号の危殆化によるリスクについて発表が行われました。</p> <p>組織の運営にリスクの分析、評価は欠かすことのできない事柄です。今回の講演では、原子力分野と IT 要素技術の研究について発表がありましたが、大学のような、企業と異なる組織文化を持つ組織における IT リスク評価についての検討は興味深いテーマとなると考えられます。</p>		

番号	4	開催日	平成 21 年 6 月 19 日
名称	第 9 回 ISS スクエア水平ワークショップ 情報漏えい対策シリーズ第 2 回 「事例に学ぶ情報漏えい対策」		
会場	情報セキュリティ大学院大学 3 階 303/304 教室		
主催	情報セキュリティ大学院大学		
参加者数	約 100 名		
概要	<p>本ワークショップでは、大日本印刷（株）、パナソニックシステムソリューションズ社、NTT ソフトウェア（株）の情報漏えい、メールや FAX の誤送信といった、情報セキュリティインシデントの経験から構築された、情報セキュリティの取り組みが紹介されました。また、情報セキュリティ大学院大学の板倉教授より情報漏洩対策に関する総括的な講演が行われました。</p> <p>各社に共通している点は、技術的対策、物理的対策はもちろんのこと、人的対策にコストを割いている点です。例としては、以下が挙げられます。</p> <ul style="list-style-type: none"> <li>・ 個人情報を取り扱う人員を特定少数に絞り込む</li> <li>・ 媒体の持ち出しを防止するために警備員に金属探知機を使用させる</li> <li>・ 「ひやり・ハット」に起因するインシデントの分析</li> <li>・ 情報セキュリティインシデント発生後、現場の ISMS の PDCA サイクルに取り込むと同時に、必要に応じて全社の PDCA サイクルにも反映させる</li> </ul> <p>各社の事業内容や事情に応じた、情報セキュリティ対策の考え方、実施体制の構築、その定着までの労苦が語られ、いかに企業が情報セキュリティに投資を行っているかを知ることができました。</p>		

**情報セキュリティマネジメントシステム(ISMS)**：情報セキュリティに対する組織的な取り組み方を体系化したもの。技術の導入だけでなく、運用、監査、セキュリティ上の事故の際の行動などを、組織の実情に即して計画、運用し、随時アップデートを図ることで、組織のセキュリティ管理能力を向上させていくことが期待されている。現在 ISMS は ISO/IEC 27001 にて国際規格となり、第三者認証機関の審査に基づいて認証が行われる。

番号	5	開催日	平成 21 年 7 月 17 日
名称	おおいたネットあんしんセミナー		
会場	大分第 2 ソフィアプラザビル 2 階 ソフィアホール		
主催	大分県、財団法人ハイパーネットワーク社会研究所（後援：大分県商工会議所連合会、大分商工会議所、大分県商工会連合会、大分県中小企業団体中央会、JPCERT コーディネーションセンター、日本ネットワークセキュリティ協会		
参加者数	約 100 名		
概要	<p>地域に根差した情報セキュリティの啓発活動の拠点として、大分県は「ネットあんしんセンター」を設立しました。本セミナーはそれを記念する行事として開催されました。</p> <p>同センターの設立までの経緯や主要業務の紹介とともに、情報セキュリティの最前線とも言うべき国際的窓口 JPCERT/CC の業務や最近の脅威の傾向分析に関する講演、セキュリティ監視センターによる顧客企業のセキュリティ監視事業から見えてきた、企業ユーザや一般ユーザの取り組むべき事柄に関する講演、セキュリティソフトのベンダの視点から見た地域で取り組む情報資産に対するリスク管理の考え方に関する講演がありました。</p> <p>また、講演者をはじめとするパネラにより「今ネットの問題に地域でいかに取り組むか」というパネルディスカッションにて、韓国と日本の情報セキュリティに関する認識と投資・実施の実情の異同や、どのように実施に向かわせたら良いか、活発な議論が行われました。</p> <p><b>JPCERT/CC (Japan Computer Emergency Report Team Coordination Center)</b> : JPCERT/CC は、インターネットを介して発生するコンピュータへの不正アクセスやサービス妨害等のセキュリティ事故について、日本国内のサイトに関する報告の受け付け、対応の支援、発生状況の把握、攻撃方法の分析、再発防止のための対策の検討や助言などを、技術的な立場から行なう機関です。各国に同様の組織があり、セキュリティ事故の内容次第で、国際的に連携して対応することもあります。</p>		