≫≫ 社団法人 山形県情報産業協会からのお知らせ ≪≪

情報セキュリティセミナー 2007

～情報化社会における企業の情報セキュリティ対策について～

経済産業省・(独)情報処理推進機構(IPA)・日本商工会議所と共同で開催 !!

今日、産業や政府活動、国民生活の多くがコンピュータやコンピュータネットワークに依存し、IT は企業の競争力を高めるために必要不可欠な要素となっています。他方、企業や官公庁からの情報漏えい、パソコンの紛失や盗難、不正アクセスを受けたウェブサイトの一時閉鎖などの事件が相次いで起きています。

このような状況はもはや他人事ではなく、事件に見舞われた時には、顧客に重大な損害を与え、自社に不利益をもたらすだけでなく、社会的責任を問われ、企業としての信用・信頼を失ってしまう恐れがあります。

情報システム上で金銭や個人情報などを狙う手法、コンピュータウイルス、スパイウェアなどの不正プログラムは常に新たなものが生まれています。事業者は事件・事故を未然に防ぐために日々最新の情報を入手し、技術的な対策や社内における人的管理、組織的管理や教育などの対策を講じる必要があります。

このような状況を踏まえ、社団法人山形県情報産業協会では、経済産業省、独立行政法人 情報処理推進機構(IPA)、日本商工会議所と共同で、情報セキュリティ対策の専門家である IPA セキュリティセンターの研究員を講師に迎え、企業や組織において情報セキュリティ対策を実施する、セキュリティ責任者・担当者、システム管理者、ウェブアプリケーション開発者を主対象に、情報セキュリティの管理面・技術面からの対策に関するセミナーを開催します。

◆ 開催概要 ◆

日　　時	・基礎コース　７月１２日（木） 10：00 ～ 12：00 ・マネジメントコース　７月１２日（木） 13：00 ～ 16：30 ・技術コース標準編　７月１３日（金） 10：00 ～ 12：00 ・技術コース専門編　７月１３日（金） 13：00 ～ 16：30　※コース概要は別紙を参照して下さい
会　　場	山形県産業創造支援センター　多目的ホール　（山形県山形市松栄一丁目３番８号）
講　　師	独立行政法人 情報処理推進機構（IPA）セキュリティセンター 研究員
主　　催	社団法人山形県情報産業協会、経済産業省、独立行政法人 情報処理推進機構（IPA）、日本商工会議所
共　　催	山形県
後　　援	山形県商工会議所連合会、特定非営利活動法人 IT コーディネータ協会
参 加 費	無料
副 読 本	情報セキュリティ読本（定価¥500）、情報セキュリティ教本（定価¥2,500）をセミナー会場にて販売します。
募集人数	基礎コース・マネジメントコース・技術コース標準編・技術コース専門編　各５０名 （募集人数に達し次第締め切ります。）
申 込 み	申込書に必要事項をご記入のうえ、E-mail、FAX よりお申込みください。尚、申込みの受付については、連絡は致しません。IT コーディネータ（補）の方は、申込書に認定番号を記入下さい。(4 時間で 1 知識ポイントが年度間の上限なしで付与されます。)

お問合せ：社団法人 山形県情報産業協会　担当：笹原、高橋
〒990-2473　山形県山形市松栄一丁目３番８号（山形県産業創造支援センター内）
TEL：023-647-8131　FAX：023-647-8132　E-mail：info@yiia.or.jp　URL：www.yiia.or.jp

きりとり

ＦＡＸ：０２３-６４７-８１３２　社団法人 山形県情報産業協会　事務局　行

◆◆◆「情報セキュリティセミナー2007」への参加を申込みます◆◆◆

貴社名	ﾌﾘｶﾞﾅ		
住　所	ﾌﾘｶﾞﾅ 〒		
貴　名	ﾌﾘｶﾞﾅ	所属・役職	
ＴＥＬ		ＦＡＸ	
E-mail			
参加希望コース	□基礎コース　□マネジメントコース　□技術コース標準編　□技術コース専門編		
副読本購入希望	□情報セキュリティ読本（定価¥500）　冊　□情報セキュリティ教本（定価¥2,500）　冊		

※IT コーディネータ（補）の方は、申込書に認定番号を記入して下さい。ITC(補)認定番号＿＿＿＿＿＿＿＿

別紙

◆ コース概要 ◆

情報セキュリティ対策　基礎コース

対象	企業における情報セキュリティ対策の基礎を理解したい方 （企業でパソコンを使って業務をする方、セキュリティ教育担当者、経営者）
ポイント	企業が直面する情報漏えいの脅威とその対策 （クライアントのセキュリティ）
内容	情報漏えいの原因となるコンピュータウイルス・スパイウェア・フィッシング詐欺等の脅威、被害事例、被害に遭わないために個人が行う対策について解説する。
目次	1. はじめに 2. ウイルス関連 ウイルスとは？ スパイウェアとは？ ボットとは？ ウイルス感染の原因 ウイルス被害対策 3. 不正アクセス 不正アクセスとは？ 侵入行為 復旧対策 4. フィッシング フィッシングとは？ 事例 対策 5. 情報漏えい 情報漏えいの原因 ファイル交換ソフトとは？ 情報漏えい対策 6. 個人レベルの対策 ファイルの拡張子とは？ 怪しいファイルの見分け方 セキュリティレベルの設定 パスワードの設定・管理 電子メールのセキュリティ対策 迷惑メールの取り扱い バックアップ Windows 98/Me パソコンの扱い 7. 終わりに

情報セキュリティ対策　マネジメントコース

対象	企業における管理面からの情報セキュリティ対策に関して理解を深めたい方 （セキュリティ教育担当者、経営者、セキュリティ責任者、マネジメントの観点からの対策を担当するセキュリティ担当者、システム管理者）
ポイント	事例を用いたケーススタディによるリスク（脅威・脆弱性）とその対策の解説
概要	具体的な事例を用いて、情報資産を組織的かつ継続的にどう管理すればよいかについて、情報セキュリティ対策ベンチマーク、情報管理等に触れながら説明する。
目次	1. 背景と基礎知識 1.1 情報セキュリティに関わる脅威の傾向 1.2 情報セキュリティ対策の目的、方針 1.3 情報セキュリティマネジメントと PDCA サイクル 1.4 情報セキュリティ対策実施上の問題点と施策ツール 2. 情報セキュリティ対策ベンチマーク 2.1 情報セキュリティガバナンスと自己診断テストの活用 2.2 情報セキュリティベンチマークの概要 2.3 情報セキュリティベンチマークの利用方法 2.4 情報セキュリティベンチマークの診断結果 2.5 情報セキュリティベンチマークの利用状況 3. ケーススタディ ： パソコンの紛失 3.1 事故発生の経緯 3.2 事故対応の流れ 3.3 情報の特定 3.4 事故対応：緊急対策会議での決定 3.5 A 社の事故対応体制 3.6 対外発表のポイント 3.7 再発防止策の例 4. そこにある情報資産－情報資産の洗い出し 4.1 守るべき情報資産とは 4.2 情報資産の例 4.3 情報資産の価値 4.4 情報資産はどこにある？ 4.5 情報資産の洗い出し 4.6 情報の管理責任者、管理担当者、利用者 4.7 機密情報、個人情報、その他の情報 4.8 情報システム、電子文書、紙文書 5. 情報の分類と格付け 5.1 情報の分類と格付けはなぜ必要か？ 5.2 政府機関統一基準の分類と格付け 5.3 機密性、完全性、可用性に応じた情報の分類 5.4 情報の分類と格付けの基準（例） 5.5 情報漏えい防止に留意した情報の分類例 6. 情報のライフサイクルと情報の取扱い 6.1 情報のライフサイクル 6.2 情報の作成と入手 6.3 情報の利用・加工 6.4 情報の保存 6.5 情報の移送（送信と運搬） 6.6 情報の提供 6.7 情報の消去 7. 情報セキュリティポリシーと情報の管理 7.1 情報セキュリティポリシーの構成 7.2 情報セキュリティ基本方針 7.3 情報セキュリティ対策基準 7.4 情報セキュリティ実施手順 7.5 対策基準とガイドライン・実施手順の関係 7.6 情報セキュリティポリシー運用上の留意点 7.7 情報の管理に関する複数の諸規程 8. 情報の管理と対策のヒント 8.1 情報の管理と対策の基本原則 8.2 リスク対応とは 8.3 リスク対応－相互の関係 9. 情報の管理と法令遵守 9.1 IT 社会の変化と法的対応の変遷 9.2 個人情報保護法 9.3 不正競争防止法

情報セキュリティ対策　技術コース標準編	
対象	企業における技術面からの情報セキュリティ対策に関して理解を深めたい方 （技術の観点からの対策を担当するセキュリティ担当者、システム管理者、ウェブアプリケーション開発者）
ポイント	情報漏えいを含むセキュリティ事故を防止するために必要な技術的対策方法の整理 （サーバ、ネットワークおよびウェブアプリケーションのセキュリティ）
概要	セキュリティ事故防止の視点から、サーバおよびネットワークの運用に関する技術的対策方法について最新トピックスを交え体系的に解説する。
目次	1. はじめに 1.1 2006 年の情報セキュリティ 10 大脅威 1.2 セキュリティ脅威の傾向 1.3 セキュリティ脅威への対策方針 2. サーバ･ネットワーク系の脅威と対策 2.1 考慮すべき脅威や問題点の整理 2.2 技術的視点からの対策 2.3 管理運用的視点からの対策 3. クライアント管理系の脅威と対策 3.1 考慮すべき脅威や問題点の整理 3.2 技術的視点からの対策 3.3 管理運用的視点からの対策 4. ウェブアプリケーション系の脅威と対策 4.1 考慮すべき脅威や問題点の整理 4.2 導入側視点からの対策 4.3 開発側視点からの対策 5. まとめ

情報セキュリティ対策　技術コース専門編	
対象	企業のウェブサイト公開やネットワーク運用の安全性向上に関して更に理解を深めたい方 （技術の観点からの対策を担当するセキュリティ担当者、システム管理者、ウェブアプリケーション開発者）
ポイント	セキュリティ事故のケーススタディによる脅威および対策の技術的解説 （サーバ、ネットワークおよびウェブアプリケーションのセキュリティ）
概要	企業におけるウェブサイト公開やネットワーク運用の際に考慮すべきセキュリティ対策について、セキュリティ事故のケーススタディを通してより深く具体的に解説する。
目次	1. SSH 経由の不正アクセス 1.1 事例:SSH 経由の不正アクセス 1.2 何が起きていたのか？ 1.3 原因は何だったのか？ 1.4 何をしていたら防げたのか？ 1.5 どのようにすれば検知できたのか？ 1.6 対応、調査のために必要な事前準備 2. SQL インジェクション 2.1 SQL インジェクションとは 2.2 事例:ショッピングサイトでウイルス感染？ 2.3 SQL インジェクション対策のポイント 2.4 エスケープ処理について 2.5 他、被害を軽減する方法 3. クロスサイト・スクリプティング 3.1 事例:クロスサイト・スクリプティング 3.2 スクリプトを埋め込まれやすいウェブアプリケーションについて 3.3 改善前のクロスサイト・スクリプティング対策 3.4 改善後のクロスサイト・スクリプティング対策

IPA セキュリティセンターについて

IPA は経済産業省の外郭団体です。IPA セキュリティセンターでは、経済産業省の情報セキュリティ政策を実行に移すため、情報セキュリティに対する具体的な対策情報・対策手段を提供するとともに、セキュアな情報インフラストラクチャの整備に貢献するための様々な活動を行っています。

URL　http://www.ipa.go.jp/security/