那覇商工会議所からのお知らせ

情報セキュリティセミナー 2006

～ 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、PC の紛失や盗難、不正アクセスを受けた Web 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な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、那覇商工会議所では、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、システム運用担当者を主対象に、情報セキュリティの管理面・経営面・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	1月15日(月)	10:00~12:00
	マネジメントコース	1月15日(月)	13:00~16:30
	技術コース 標準編	1月16日(火)	10:00~12:00
	技術コース 専門編	1月16日(火)	13:00~16:30
コース概要は別紙を参照して下さい。			
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		
会 場	那覇商工会議所 2階ホール		
主 催	那覇商工会議所 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		
参 加 費	無料		
副 読 本	「情報セキュリティ読本」(定価¥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。)		
来 場 申 込	申込書に必要事項をご記入のうえ、TEL、FAX よりお申込みください。		

お問合せ：那覇商工会議所企画業務部 担当：又吉
 TEL：098-868-3758

きりとり

FAX：098-866-9834

那覇商工会議所企画業務部 担当 又吉 行

「情報セキュリティセミナー2006」への参加を申込みます

貴社名			
住 所			
氏 名	所属・役職		
T E L	F A X		
E-mail	ITC(補)認定番号		
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

ご記入頂いた情報は、商工会議所からの各種連絡・情報提供のために利用するほか、セミナー参加者の実態調査・分析のために利用することがあります。

コース概要

情報セキュリティ対策 基礎コース			
対象	情報セキュリティ対策の基礎を理解したい方 (一般職員、セキュリティ教育担当者および初心者のセキュリティ担当者・システム管理者)		
ポイント	インターネットにおける脅威と対策		
内容	インターネットにおける脅威の変遷、コンピュータウイルス・スパイウェア・フィッシング・ワンクリック詐欺等の被害事例と被害に遭わないための対策について解説する。		
目次	<table border="0"> <tr> <td style="vertical-align: top;"> 1. 脅威 1.1 脅威とは 1.2 ITにおける脅威の変遷 1.3 ウイルスとは 1.4 スパイウェアとは 1.5 ボットとは 1.6 どこから感染するか 1.7 ウイルス以外の脅威 </td> <td style="vertical-align: top;"> 2. 被害事例 2.1 ファイル交換ソフト利用による情報漏えい 2.2 フィッシング 2.3 ワンクリック不正請求 2.4 偽ウイルス対策ソフト他 2.5 ID/パスワード盗難 3. セキュリティ対策 3.1 組織で規定されたポリシーに従う 3.2 コンピュータのぜい弱性を解消する 3.3 ウイルス対策ソフトの利用 3.4 個人ごとのセキュリティ対策 </td> </tr> </table>	1. 脅威 1.1 脅威とは 1.2 ITにおける脅威の変遷 1.3 ウイルスとは 1.4 スパイウェアとは 1.5 ボットとは 1.6 どこから感染するか 1.7 ウイルス以外の脅威	2. 被害事例 2.1 ファイル交換ソフト利用による情報漏えい 2.2 フィッシング 2.3 ワンクリック不正請求 2.4 偽ウイルス対策ソフト他 2.5 ID/パスワード盗難 3. セキュリティ対策 3.1 組織で規定されたポリシーに従う 3.2 コンピュータのぜい弱性を解消する 3.3 ウイルス対策ソフトの利用 3.4 個人ごとのセキュリティ対策
1. 脅威 1.1 脅威とは 1.2 ITにおける脅威の変遷 1.3 ウイルスとは 1.4 スパイウェアとは 1.5 ボットとは 1.6 どこから感染するか 1.7 ウイルス以外の脅威	2. 被害事例 2.1 ファイル交換ソフト利用による情報漏えい 2.2 フィッシング 2.3 ワンクリック不正請求 2.4 偽ウイルス対策ソフト他 2.5 ID/パスワード盗難 3. セキュリティ対策 3.1 組織で規定されたポリシーに従う 3.2 コンピュータのぜい弱性を解消する 3.3 ウイルス対策ソフトの利用 3.4 個人ごとのセキュリティ対策		
情報セキュリティ対策 マネジメントコース			
対象	企業における管理および経営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 (セキュリティ責任者・担当者、システム管理者)		
ポイント	PDCA サイクルで見る企業のセキュリティ対策の全体像		
内容	情報セキュリティ対策を具体的に解説する。また、被害事例、セキュリティポリシー、評価認証と税制、セキュリティ対策自己診断テスト、事業継続計画等について解説する。		
目次	<table border="0"> <tr> <td style="vertical-align: top;"> 1. 背景と基礎知識 2. 情報セキュリティ対策自己診断テストの活用方法 3. ISMSとPDCAサイクル 4. Plan - 計画する 4.1 情報セキュリティの組織 4.2 情報セキュリティポリシー 4.3 リスクマネジメント 4.4 管理策の選択 </td> <td style="vertical-align: top;"> 5. Do - 導入と運用管理 6. Check - 評価 & Act - 改善 7. 情報セキュリティガバナンス 8. 事業継続計画 9. 法令順守 10. まとめ </td> </tr> </table>	1. 背景と基礎知識 2. 情報セキュリティ対策自己診断テストの活用方法 3. ISMSとPDCAサイクル 4. Plan - 計画する 4.1 情報セキュリティの組織 4.2 情報セキュリティポリシー 4.3 リスクマネジメント 4.4 管理策の選択	5. Do - 導入と運用管理 6. Check - 評価 & Act - 改善 7. 情報セキュリティガバナンス 8. 事業継続計画 9. 法令順守 10. まとめ
1. 背景と基礎知識 2. 情報セキュリティ対策自己診断テストの活用方法 3. ISMSとPDCAサイクル 4. Plan - 計画する 4.1 情報セキュリティの組織 4.2 情報セキュリティポリシー 4.3 リスクマネジメント 4.4 管理策の選択	5. Do - 導入と運用管理 6. Check - 評価 & Act - 改善 7. 情報セキュリティガバナンス 8. 事業継続計画 9. 法令順守 10. まとめ		

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 (技術面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、システム運用担当者)	
ポイント	現実的な脅威の解説とその対策	
内容	組織における情報セキュリティについて、ソフトウェア自体の脆弱性や設定の不備等から生じる脆弱性、脆弱性への攻撃によるサーバ・ネットワークへの脅威を解説する。また、それらの脅威への対策について解説する。	
目次	<ul style="list-style-type: none"> ・ネットワーク上の脅威と対策 1. はじめに <ul style="list-style-type: none"> 1.1 そこにコンピュータがあればすべて狙われる 2. 現実的な脅威とそのポイント <ul style="list-style-type: none"> 2.1 コンピュータウイルスからの攻撃 2.2 ポットによる外部への攻撃の強制 2.3 DNS サーバの設定ミスを狙う攻撃 2.4 その他の特徴的なアクセス 3. ネットワーク上の脅威への対策 <ul style="list-style-type: none"> 3.1 セキュリティ対策の基本 3.2 サーバのセキュリティ対策 3.3 ネットワークのセキュリティ対策 3.4 その他のセキュリティ対策 	<ul style="list-style-type: none"> ・ウェブアプリケーションの脅威と対策 1. ウェブアプリケーションを取り巻く脅威 <ul style="list-style-type: none"> 1.1 ウェブサイトに関連する事件 1.2 ウェブサイトに関連する事件の原因 1.3 ウェブサイトに関連する事件の被害 1.4 ウェブアプリケーションの運用形態 1.5 なぜ今注目すべきか 1.6 ぜい弱性関連情報の届出状況 2. ウェブアプリケーションのセキュリティ対策 <ul style="list-style-type: none"> 2.1 対策の基本方針 2.2 ウェブアプリケーション開発時 2.3 設定・運用時 2.4 外部委託する場合 3. ぜい弱性ごとの具体的対策 <ul style="list-style-type: none"> 3.1 SQL インジェクション 3.2 クロスサイト・スクリプティング
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、ネットワークの安全性向上に関して理解を深めたい方 (技術面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、システム運用担当者)	
ポイント	ウェブおよびネットワークの安全な運用管理のケーススタディ	
内容	ウェブサイトやネットワークの安全な運用管理方法について、ケーススタディを通して具体的に解説する。	
目次	<ul style="list-style-type: none"> 1. ファイル共有ソフトに絡んだ情報流出 <ul style="list-style-type: none"> 1.1 情報流出はいかにして起こるのか？ 1.2 事例：ファイル共有ソフトに絡んだ情報流出 1.3 原因は何だったのか？ 1.4 Winny による情報流出への対策 1.5 流出した情報への対応 1.6 それでも収束しない情報流出 1.7 IPA で対応した、実際の相談事例 2. SSH 経由の不正アクセス <ul style="list-style-type: none"> 2.1 減らない不正アクセス 2.2 事例：SSH 経由の不正アクセス 2.3 原因は何だったのか？ 2.4 何をしていたら防げたのか？ 2.5 どのようにすれば検知できたのか？ 2.6 自前で調査する場合の材料は？ 2.7 対応、調査のために必要な事前準備 	<ul style="list-style-type: none"> 3. SQL インジェクション <ul style="list-style-type: none"> 3.1 SQL インジェクション概要 3.2 事例：SQL インジェクション 3.3 問題のポイント整理 3.4 なぜ SQL 文の挿入が可能か？ 3.5 エラーメッセージについて 4. クロスサイトスクリプティング <ul style="list-style-type: none"> 4.1 事例：クロスサイトスクリプティング 4.2 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 4.3 改善前のクロスサイト・スクリプティング対策 4.4 改善後のクロスサイト・スクリプティング対策 <p>付録 ウェブアプリケーションの安全性向上のためのポイント</p>

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/>