ilovex

Newsletter
第８号 若手向け College

発行：株式会社アイロベックス
〒160-002 新宿区新宿２丁目 12 番４号
アコード新宿ビル 7F
TEL : 03-3357-5111 / FAX : 03-3357-5511
E-mail : inq@ilovex.co.jp
URL : http://www.ilovex.co.jp

Vision of ilovex

卓越した技術力の追求

わたしたちアイロベックスは卓越した技術によって新しい価値を創造し
取り巻くすべての人々に幸せを与えられるリスペクトカンパニーを目指します。

卓越した技術力とは、何でしょうか？それは、当社であれば１年生社員でも身についている力です。
プログラムの正確さと素早さ、要するにバグを出さない。納期を守る。この２点に私達は全力を注ぎます。

ilovex college

2005.6.7　担当：髙山

ザ・セキュリティ　No.1

はじめに

情報システムにとって『セキュリティ』は、なくてならないインフラです。今回は、より良いセキュリティインフラを構築し、運用するための基礎を学びます。
ＳＥは、「セキュリティに関して、どこにリスクがあり、どのように対処するか」を頭に叩き込んでおく必要があります。リスクの種類を把握し適切に対応することで、より安全な情報システムを構築できるのです。

リスクの種類とは？

■リスクの種類
- ●環境的脅威
  - 地震、火災、落雷、洪水
- ●人為的脅威
  - －偶発的脅威
    - 入力ミス、データ削除等によるデータの破壊、不正侵入を誘発
  - －意図的脅威
    - 改ざん、不正アクセス、コンピュータウィルス等の情報システムの脆弱性を利用した侵入を誘発

１．脅威の種類

脅威は４種類に定義付けられます。
- ●セキュリティホール
- ●コンピュータウィルス
- ●スパイウェア
- ●ソーシャルハッキング

１）セキュリティホール

ソフトウェアの設計ミス等による、システムにおけるセキュリティ上の弱点（脆弱性）をいう。広義には弱いパスワードや設定ミスによってもたらされるセキュリティ上の欠陥を指す。セキュリティホールが発見されるとシステムの製造元から**パッチが無償で提供**される。

２）コンピュータウィルス

コンピュータ内で**ファイルを破壊したりするプログラム**をいう。
広義ではワームも含まれている。
ウィルスの感染に利用者は**大抵気付かない。**感染したまま使用していると被害が拡大することもある。

裏面へ

講師紹介

髙山　和明　IT プロフェショナル部
2005/3 に入籍したばかりの新婚。SE として日夜修行に励む日々。中国関連の事情通でもある。

■クラッカー Cracker
ハッカーの中でも悪意を持って、他人のシステムを不正に使用したり、それを破壊する目的でネットワークに侵入したり、データやプログラムを改変したり、盗み見、破壊するなどの犯罪行為を行う者。

■コンピュータウィルスの種類
- ・コンピュータウィルス（狭義）
  コンピュータに侵入し、システム障害をもたらす寄生プログラム
- ・トロイの木馬
  自己増殖せずに、実行直後に発病する不正な独立プログラム
- ・コンピュータワーム
  ネットワーク上で自己増殖する不正な独立プログラム

ilovex

Newsletter
第８号 若手向け College

発行：株式会社アイロベックス
〒160-002 新宿区新宿２丁目12番４号
アコード新宿ビル 7F
TEL : 03-3357-5111 / FAX : 03-3357-5511
E-mail : inq@ilovex.co.jp
URL : http://www.ilovex.co.jp

卓越した技術力とは、何でしょうか？それは、当社であれば１年生社員でも身についている力です。
プログラムの正確さと素早さ、要するにバグを出さない。納期を守る。この２点に私達は全力を注ぎます。

ilovex college

2005.6.7　担当：高山

ザ・セキュリティ　No.2

３）スパイウェア
ＰＣを使用するユーザの行動や**個人情報を収集する**など何かしらのデータを取得するアプリをいう。取得された**データは大抵作成元に送られる**。
※アドウェア
広告を表示する代わりに無料で使用できるアプリ。スパイウェアの機能を持つものが多い。

４）ソーシャルハッキング
ハードウェアやソフトウェアの弱点を突くのではなく社会工学（ソーシャルエンジニアリング）によって必要な情報を得る行為をいう。
近年では強い悪意のあるハッキングはＰＣを介するよりも**ソーシャルハッキングの方が多くなっている。**

①ショルダーハック
肩越しにパスワードの入力を盗み見する方法。
慣れてくると多少長いパスワードであっても、指の動きから読み取ることが出来る。画面で行っている作業内容を盗み見することも含まれる。

②スカビンジング
オフィスから出された**紙ゴミを漁ることによって機密情報などを探し出す**方法。
廃棄されたハードディスク、フロッピーディスクや CD-ROM などから情報を引き出す場合もある。

③なりすまし
電話等を用いて**言葉巧みにパスワードなどを聞き出す**方法。振り込め詐欺も同類である。
※フィッシング（Phishing）詐欺
送信者詐称機能を用いてメールを送信し、リンク先の画面でクレジット番号やパスワードを不正に取得するもの。

④内部犯行
実際にハッキング対象の**組織・団体に入り込み、内部の人間となる**方法。
投棄されている機密文書やパソコン周りのパスワードのメモなどから情報を収集する。

２．脅威から身を守るためには
組織の構成員の中に、たった一人でもリスク意識のない人間がいることによって、組織全体が脅威にさらされてしまう、ということを自覚する。
→ それを**監視する体制が必要不可欠**

１）自己防衛方法を知る
セキュリティの三大原則を理解することにより、脅威から身を守ることが出来る。
- ●機密性（Confidentiality）
- ●完全性（Integrity）
- ●可用性（Availability）

①機密性【情報漏洩を防ぐ】
- ・離席時のコンピュータロックの実施
- ・ネットワーク上の共有フォルダの設定をしない
- ・パスワードの管理の徹底
- ・資料などの取り扱い（保管、廃棄）の厳密化
- ・暗号化技術の導入

二枚目へ

大屋　千春
.NET チーム
Q：今回のカレッジの感想は？
A：改めてセキュリティの意義や大切さを認識しました。
Q：特に気になった点は？
A：ソーシャルハッキングの怖さを痛切に感じました。個人だけでなくリーダーとして、組織的な真摯な取り組みをしていきます。

■セキュリティポリシー
情報システムの利用者の情報セキュリティに対する意識向上、これらの情報に関して利用者個人の裁量で、その扱いが判断されることのないよう、組織として意思統一され、明文化された文書。

・情報セキュリティ基本方針
・情報セキュリティ対策基準
・情報セキュリティ実施手順等

適切に導入・運用されないポリシーは策定されていないのと同じである。

ilovex

Newsletter
第８号 若手向け College

発行：株式会社アイロベックス
〒160-002 新宿区新宿２丁目 12 番４号
アコード新宿ビル 7F
TEL : 03-3357-5111 / FAX : 03-3357-5511
E-mail : inq@ilovex.co.jp
URL : http://www.ilovex.co.jp

ilovex college

2005.6.7　担当：髙山

ザ・セキュリティ　No.3

②完全性【データの改竄等を防ぐ】
・ウィルス対策の実施
・共有フォルダの権限の厳密化
・バックアップファイルの作成
③可用性【常に正常に利用できる状態を保持する】
・不正アクセスの防止
・ソフトウェアのバージョンアップの対応
・セキュリティパッチの適用

2）社内教育を実施する
社内教育を実施し、社員全員のセキュリティ意識を向上させる。

①管理者だけでは不十分
・一部の管理者がセキュリティ対策を行うのではなく、ＩＴに携わる**全ての人が対策**を行う必要がある。
②Trustworthy Computing の浸透
・信頼できるコンピューティング。
安全なアプリケーション開発のための教育が必要。プロジェクト単位で安全な開発技法について事前に準備、教育を行うことも求められる。

3）罰則を設ける
社内規定にセキュリティの罰則を設け、違反への抑止効果を高める。

①就業規則や賞与規定などに予め盛り込んでおく必要がある。
・所属する管理者（上司）から是正を促す。
・情報システムの利用を停止させる。（期限付き）
・規則に則った罰則を適用させる。
→ 不審な行動をとる、実際に情報を漏洩させる等情報リスクが高い人であると判断された場合は、規定に則って処罰される必要がある。なぁなぁに済まさない。
手口が悪質であったり、被害が甚大であった場合は民事責任・刑事責任に問われるケースもある。

4）法律
セキュリティ関連の法律は、次のものがある。
■不正アクセス禁止法
・不正アクセスを行った場合　→　一年以下の懲役又は 50 万円の以下の罰金
・不正アクセスを助長した場合　→　30 万円以下の罰金
■個人情報保護法
主に個人情報を取り扱う団体に対する法律。
個人情報の不正利用やずさんな管理を行わないように義務を課している。

まとめ

最も理想的なのは、被害が発生する以前に、無理なく**脅威の芽を摘み取る**ことです。
そのためには日々組織として、どのような情報の取り扱いが求められているか、ということを構**成員全てに周知徹底**することが求められます。
また、**セキュリティ意識の向上が、他の脅威を未然に防ぐ**ことに繋がるのです。
組織としての取り組み姿勢が問われています。

前田　信次
Java&.NET の二刀流
Ｑ：今回のカレッジの感想は？
Ａ：月並みになりますが、システム開発において、最も大事で疎かにできないと再認識しました。
Ｑ：興味深かった点は何ですか？
Ａ：セキュアなシステムは技術だけでなく、セキュリティポリシーによる教育や規則な全社的な運営が必須である点です。

■情報関連の資格
●技術者向け
・情報セキュリティアドミニストレータ
・ＭＣＡ セキュリティ
・ＣＣＳＰ
●企業向け
・ＩＳＭＳ
・プライバシーマーク

編集後記

セキュリティに関しては「つい、うっかり」が許されない。対応方法いかんでは、新聞沙汰になり、ひいては企業の存続を脅かします。　社員の意識向上が必須です。　　編集担当　野﨑
・アイロベックスカレッジ（SE 向け）　毎月第三月曜日 19:00～21:00

2005 年 8 月 16 日発行
Vol.01 NO.8

アイロベックスニュースレター
発行責任者：杉山　淳子

Ilovex Newsletter は毎月第一・三火曜日に発行します。詳細は当社営業または担当までお問合せください。