ASIS インターナショナル日本支部
広報担当理事　　長瀬　泰郎

ASIS インターナショナル日本支部便り

月次セミナー　8月度　「IT プラットホームセキュリティ」

8 月の月次セミナーは、株式会社日本高信頼システム研究所の代表取締役社長　澤田　栄浩氏による講演、題して「IT プラットホームセキュリティ」です。情報セキュリティ分野の非常にディープなテーマでした。

講演する 澤田　栄浩　氏

澤田さんは、自称『プラットホーム屋』。この場合の“プラットホーム”とは、われわれがコンピュータのソフトウェア（電子メール、会計システムなどのアプリケーションソフト）をコンピュータで利用するために必要な、基本ソフト（OS）やハードウェアの組合せと設定のことをいいます。澤田さんは、コンピュータ基盤技術の評価と応用の研究に始まって、商社や銀行で世界規模の IT インフラ構築とセキュリティ対策を主導された経験を経て、セキュア　OS（安全性の高い基本ソフト）の研究開発を行う会社を設立されました。その後、プラットホームセキュリティのコンサルティングを行いながら、政府機関や学会の委員、主査を複数務めておられセキュアな IT プラットホーム技術の専門家として活躍されています。

今回は、インターネットが世界のお金を動かす大動脈となりつつあり、その脆弱性を攻撃するプロ化したハッカーの出現といった、IT　化とそのリスクの動向が解説され、その防御のためにはウェブサーバや OS といった IT プラットホームのセキュリティ対策がひじょうに重要であることを解説していただきました。以下はその概要です。

■　インターネットとマネー

巨額のマネーが、インターネット上でデータとして流れています。2007　年度の調査でわが国の電子商取引の取引額は　162　兆円（BtoB）。米国の約　1.5 倍で、世界一大きな市場です。さらに、BtoC　の取引額は 5.3 兆円、前年比 21.7%の伸び率で急速に拡大しています。

インターネットバンキングやインターネットショッピングを利用される方は多いと思います。これらは、インターネットとブラウザをインフラとして使用する“ウェブシステム”と呼ばれるものです。電子商取引の市場で膨大なマネーを動かすのに使用する情報システムとして、ウェブシステムが急激に普及しています。

■　ウェブの脆弱性に対処するには

ウェブシステムは必ずしも強固なものではありません。この脆弱性を悪用して、プロのハッカーがネットに流れる膨大なマネーを掠め取る犯罪が多発しています。

独立行政法人　情報処理推進機構（IPA）がこの春に発表した情報セキュリティ事故の調査報告では、

情報システムの脆弱性の最大の原因が『ウェブアプリケーションの脆弱性』であり、この脆弱性を突く『任意のスクリプトの実行』が最大のリスクとして挙げられています。ウイルス対策ソフトのベンダーのウェブサイトが、ウェブアプリケーションの脆弱性を悪用して改ざんされた、あるいは未公表の財務情報を盗まれた、という笑えない事件が起きています。

では、われわれ企業はどう防御すればいいのでしょう。できることはつぎのようなことです。

- OS やアプリケーションの脆弱性情報に気をつける。セキュリティパッチ等の対策を、自社のウェブサイトにも適用する
- アクセスログを分析し、不正アクセスやウイルス感染の形跡がないか、監視する
- 外部からの脆弱性診断を受ける
- 自社のウェブサイトの脆弱性を指摘されたら、すぐに調査する

特に企業として留意すべきは、自社のウェブサイトで十分な安全管理を怠っていた場合、脆弱性を突かれて利用者である顧客や取引先に被害をもたらしたとき、訴訟を受けるリスクがあるということです。

■ プラットホームのセキュリティ対策

コンピュータの利用者は、特権ユーザーと一般のユーザーに大別されます。企業のシステム管理者などは、特権ユーザーとして、ユーザーの登録やアクセス範囲の設定などができます。

特権ユーザーは、OS のすべての機能と情報を自由に利用できるので、コンピュータ上でできることは、なんでもできてしまいます。従って、特権ユーザーが攻撃者となったとき、あるいは、ハッカーが特権ユーザーになりすましてシステムを攻撃したとき、その被害は非常に大きくなります。攻撃をした痕跡を消すことまで、できるのです。

この対策として、つぎの４つの方策があります。これらは、「政府機関の情報セキュリティ対策のための統一基準」にも記載されています。

- 最小特権：特権ユーザーに付与するアクセス権を必要最小限にする。これにより、被害の範囲を最小にする
- 強制アクセス制御：特権ユーザーであっても、アクセスできる範囲や使用できる機能を制限する。これにより、被害の範囲を最小にする
- デュアルロック：二人の特権ユーザーが操作者と操作の承認者となることで、単独で重要な操作をできないようにする
- 情報の流れ制御：例えば、企業内の職位と所属によりアクセスできる情報を限定する

以上のように特権ユーザーを制御すること（特権制御）は、現在市場に出回っているサーバー用の OS のほとんどが装備する機能です。会社出入りの IT 業者さんに相談し、みなさんもぜひ活用してください。

■ この他の気になる問題

この他、最近の情報セキュリティ関連の問題としてつぎのことに注目しています。

- 偽造サイトの横行：偽造のレベルが上がっており、正規のウェブサイトと見分けが付かない。認証情報や個人情報を入力するときには、細心の注意を
- Bot（ボット）：手元のパソコンに悪意のあるプログラムを埋め込まれ、遠隔操作で SPAM メール送信の中継地に仕立てるというように悪用される
- SSL 脆弱性：医療情報界では、SSL のみでは

十分なセキュリティが確保できないと評価

- DLL インジェクション：最近発見された攻撃手法で、クライアント PC を攻撃してメモリ上のプログラムを改ざんし、送金先をすり替えるといった事件が起きている

攻撃者は、共通基盤であり情報の多い IT プラットホームを攻撃します。個別のアプリケーションを攻撃することはまずありません。情報セキュリティの実現には、IT プラットホームを意識した安全対策が肝心です。

以上、澤田さんによるセミナーでした。
9 月はコクヨファニチャー株式会社セキュア推進室長広常　猛さんに、「オフィスセキュリティの現状とオフィスセキュリティマーク認証制度」について話していただきます。

■ ASIS インターナショナル日本支部の月次セミナーへのお誘い

ASIS インターナショナル日本支部は、月次セミナーを開いています。産業セキュリティに興味がある方ならどなたでも参加できます。お申し込みはホームページから！

■ 開催日

毎月第三火曜日　午後 6 時半より

■ 場所

国際文化会館（六本木）
東京都港区六本木 5-11-16
TEL: 03-3470-4611
http://www.i-house.or.jp/jp/ihj/access.html

■ 参加費

2,000 円（ASIS 会員・非会員同一料金）

このコーナーへのお問い合わせや入会お申込みは
ASIS インターナショナル日本支部　事務局まで

〒101-0021　東京都千代田区外神田 2-2-17
日本保安人事株式会社内
TEL　03-3255-3468　　FAX　03-3258-7630
E-Mail info@asis-japan.org

www.asis-japan.org