Webアプリケーションセキュリティ WG

加藤雅彦

株式会社アイアイジェイテクノロジー

2007 年 6 月6日

全般報告

2006年度活動総括

✓2006年度は啓発コンテンツ作成を中心に活動
✓月1回程度のペースでWGを開催
✓目次が確定
✓6月よりJNSAバイヤーズガイドにて企画フェーズから順次公開予定

啓発コンテンツ概要

- コンテンツ概要
  - Webサイトのライフサイクルに着目し、それぞれのフェーズ（企画、設計、テスト、運用）で考慮すべきセキュリティを「ケーススタディ」方式で解説
- 対象読者像
  - 中小企業の情報システム部責任者／担当者

想定ケース

- JNSA商事
  - 社員100名程度
  - Webサイトで商品問い合わせの受付と人材募集を行うことに
  - 情報システム部がサイト構築を行う
  - しかし、インターネットと連携するWebアプリケーションは今回が初めて

1-3) 共通の設定

舞台：JNSA 商事

JNSA 商事株式会社は、二輪の外車やパーツ、その他の様々な用品を仕入れ小売店に販売している中堅輸入ディーラーである。
10 年前に数名で始めた会社だが、現在の組織構成は以下のようになっており、従業員 100 名、年商 20 億円になるまでに成長した。

```
                          +---- 総務グループ（総務、購買、法務等）
        +---- 管理部 ----+---- 人事グループ（人事、採用等）
        |                 +---- 情報システムグループ --+-- 運用チーム
（社内システム運用）
        |                                             +-- 開発チーム
（社内システム開発）
社長----+---- 営業部 ----+---- 販売グループ（営業、販売等）
        |                 +---- 商品開発グループ（商品開発）
        |
        +---- 技術部（修理、保守、サポート）
```

図1：組織図

現在各部には部長、各グループにはグループ長が置かれ、それぞれの組織[illegible]ている。日常業務における重要決定事項は、社長、部長、グループ長[illegible]「幹部会議」で承認される仕組みとなっている。

その中で、情報システムグループは社内システムの開発、運用を行うグループとして、グループ長以下「運用チーム」(リーダーとエンジニア2名)、「開発チーム」(リーダーとエンジニア4名)で構成されている。実際には上記メンバーだけでは人員が不足するため、開発、運用を委託しているSIベンダも含めてチーム構成されている。社内システムの要となっているグループである。

＜サイト更新のニーズ＞

さて、 JNSA 商事は数年前からインターネットで自社の概要、沿革を紹介するだけのシンプルな Web サイトを営業部が半ばボランティア的に運用していた。しかし、コンテンツの更新等に関する責任範囲が不明瞭なまま運用が続いていることや、効果の程は定かではないものの業務の拡大や効率化に伴ってインターネットを今以上に活用していきたい、といったことを様々に検討した結果、Web サイトに以下の２つの機能を追加することとなった。

■ 人材募集

現在、通年での中途採用募集を雑誌等に掲載したり、新卒募集を行ったりしている

が、費用がかかる割に採用人数が増えていない。そこで、より多くの採用人数確保や雑誌掲載の経費削減のために、自社 Web サイトでも人材募集を行うことが幹部会議で決議された。

Web サイトのイメージとしては、応募者が入力フォームに希望職種や連絡先等の必要事項を入力し、レジュメデータを添付してアップロードするという形式が想定された。

■ 問い合わせ

現在、各種問い合わせは電話/FAX/電子メールで受け付けている。これらの問い合わせ方法以外にも、Web フォームでも問い合わせを受けつけるということが決議された。

問い合わせ件数や手間を減らすために FAQ を整備したり、商品カテゴリを選択して問い合わせを受けたりする機能を実装する方針が決まった。

＜業務責任範囲＞

また、最終的な責任範囲をどうするかで幹部会議で話し合いが行われた。今まで営業部で運用されていたとか、インターネットを使ったシステムだとかはあまり関係なく、これは重要な業務システムである、という意見が多数を占めた。従来は完全に社内に閉じたシステムしか開発したことがない情報システムグループではあるが、他に適切な部署も見当たらないことから、不慣れながらもリーダーシップをとることとなり、SI ベンダの協力のもとサイト更新プロジェクトに臨むこととなった。

さらに、Web サイトオープン後の運用責任をどうするかについては、インターネットシステムの運用ノウハウが無いことから情報システムグループ長は外部への運用委託を提案[illegible]の議論[illegible]コスト等の問題から、情報システムグループが開発だけではなく、[illegible]運用責任もまとめて負うということが幹部会議で決められた。

＜顧客のニーズ＞

上記のように人材募集と問い合わせ用の Web サイトを構築するということが幹部会議で決められ、具体的にどういった機能が必要かといった議論に入り始めたところ、各部署から様々なニーズが寄せられてきた。

■ 人材募集

－ 人事担当の判断だけでなく、配属予定先の判断もふまえて書類選考結果としたい。そのため、人事担当者以外に、応募職種に応じた部門の部門長(部長、グループ長)にも同時に応募内容を送付してほしい。

－ 応募者のデータは、社内の人事管理システムで管理したい。せっかくシステム導入するのであれば、自動入力するようにしてほしい。

■ 問い合わせ

－ 商品種別により、担当部署(グループメンバー全員)に問い合わせ内容を振り分けて配信してほしい。

－ あとから情報の整理を行いやすいように、回答日や問い合わせ内容を自動的に社内グループウエアに蓄積するようにしてほしい。

以後の予定

- 企画フェーズ以降のコンテンツについては以下のスケジュールで公開を予定しています
  - 8月　設計フェーズ公開
  - 10月　テストフェーズ公開
  - 12月　運用フェーズ公開