JNSA

NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

Webアプリケーションセキュリティ WG

二木真明
住商情報システム(株)

2006 年 5 月 30日

全般報告

- 2005年度の活動
  - 複数のテーマを設定、分科会形式で作業
    - 啓発コンテンツ分科会
      - Webアプリケーションセキュリティについての啓発を行うためのコンテンツを開発
    - 受発注ガイドライン分科会
      - アプリケーション開発における、受注側、発注側相互に合意可能なセキュリティガイドラインの検討
    - 技術分科会
      - 必要と思われる技術的テーマについて検討

Copyright (c) 2000-2006　NPO日本ネットワークセキュリティ協会

啓発コンテンツ分科会

- ２００５年4月当時、まだまだWebアプリ脆弱性についての認識が不足していた
  - まず啓発が必要と考え、これをテーマにしたセミナーを開催できる程度のコンテンツ開発を目標とした。
    - 総合コンテンツ　(全般的なユーザ啓発)
    - 開発系コンテンツ (開発者への啓発)
    - 運用系コンテンツ (運用者への啓発)

Copyright (c) 2000-2006　NPO日本ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ協会

受発注ガイドライン分科会

- アウトソース主流の開発における仕様へのセキュリティ要件組み込みを意識
- 受注側、発注側の不公平感が動機でもある
  - 漠然、抽象的な記述→結果的に発注側有利
  - 具体的な（すぎる）記述→受注側有利
  - 安全性を高めるという目的を第一に、相互のバランスがとれた落としどころは？

Copyright (c) 2000-2006　NPO日本ネットワークセキュリティ協会

技術分科会

- 検査技法、防御技法などの研究
- 他の分科会からの検討依頼に基づく技術的研究

Copyright (c) 2000-2006　NPO日本ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ協会

活動の総括

- 啓発コンテンツ分科会
  - 総合コンテンツのたたき台作成
  - 開発系については、人員の関係で対応できず。
  - 運用系について議論は行ったが具体的な作業着手はできなかった。
- 受発注ガイドライン分科会
  - 問題の本質についての議論
  - いくつかのアプローチについての検討
  - 前提となる脅威、リスクの分類作業を進めた
- 技術分科会
  - 検査ツール、講師を招いてのSOAP/SOA勉強会、WAFなどの検証イベントを各一回開催したが、メンバー多忙により充分な活動はできなかった。

Copyright (c) 2000-2006　NPO日本ネットワークセキュリティ協会

活動の総括

- 全般的に活動は低調だった
  - Web関連インシデント激増によるメンバー多忙も一因か？
  - 出席するメンバーが数名に固定されてしまっていた
- 反省点
  - テーマ設定はよかったのか
  - 参加への動機付けが足りなかった・・・（成果、過程の積極的な公開、メンバー企業名などを含む露出など）
  - 多忙な中で活動を続けられるような工夫（MLや掲示板の活用など）が足りなかった・・・

Copyright (c) 2000-2006　NPO日本ネットワークセキュリティ協会

新年度の方向性

- 新リーダー：加藤氏を中心に再検討
- より、参加する意欲がわくような形を追求していく
  - より社会的に評価が得られる（目立つ）ような方向
- 一旦メンバーをリセットし、再募集する

Copyright (c) 2000-2006　NPO日本ネットワークセキュリティ協会

2005年度の成果物紹介

- 啓発コンテンツ分科会　総合コンテンツ
  - 「Webサイトが今、危ない！！」
  - （後日 JNSAサイトに公開）
- 受発注ガイドライン分科会
  - 議論の経過紹介
  - リスクツリー（後日JNSAサイトに公開）

Copyright (c) 2000-2006　NPO日本ネットワークセキュリティ協会

活動参加企業、参加者

- IIJテクノロジー株式会社　加藤氏、根岸氏
- NTTコムウエア株式会社　丸尾氏
- セコム株式会社　新井氏
- 株式会社ディアイティ　坂本氏
- 日商エレクトロニクス株式会社　松尾氏
- 富士通株式会社　奥原氏
- 三菱電機株式会社　河内氏
- ＪＮＳＡ
  - 安田氏（ディアイティ、事務局）、佐藤氏（IRI, 技術部会長）
- 住商情報システム株式会社　二木　（WGリーダー）

＊原則、2回以上、イベント、会合に参加された方を記載しています

Copyright (c) 2000-2006　NPO日本ネットワークセキュリティ協会

啓発コンテンツ分科会

- 分科会リーダー
  - 二木（住商情報システム（株））が兼任

Copyright (c) 2000-2006　NPO日本ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ協会

啓発コンテンツ議論の経緯

- 総合コンテンツの必要性
  - 対象
    - 当初、対策の原資をにぎる経営層を・・・と考えたが、少し技術よりの内容を前提で考えれば、たとえば、技術的なバックグラウンドのあるCI(S)Oもしくは「情シス部長」くらいのレベルへの啓発が最も必要との結論
  - 開発、運用などの全般を掌握、予算化等に責任を負う立場の人への啓発に主眼
  - アプリケーション脆弱性の危険性への認識と対策全般についてのオーバビューを提供

Copyright (c) 2000-2006　NPO日本ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ協会

「総合」コンテンツの内容

- Web事故頻発の状況を明らかにし、その影響、リスク、原因の変化について解説する。
  - 実際の報道事例を一部匿名化または仮想化して紹介
  - 客観的な統計資料を利用
- アプリケーションに含まれる可能性のある主要な脆弱性と、そのリスクについて解説する。
  - あまり技術的に突っ込まず、「容易に攻撃できる」「情報漏洩などのリスクに直結する」ことを強調
- その対策について、開発、運用の両面からアウトラインを述べる
  - あくまで「アウトライン」、詳細な技術論は個別のコンテンツに委ねる

Copyright (c) 2000-2006　NPO日本ネットワークセキュリティ協会

コンテンツの紹介

- 別途、内容を紹介します。

Copyright (c) 2000-2006　NPO日本ネットワークセキュリティ協会

JNSA

NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

受発注ガイドライン分科会

議論の経緯と成果

分科会リーダー：奥原氏　(富士通)

目的

- Webアプリケーション開発の多くの場面で、セキュリティ対策をここまではやっておくべきという合意が発注者と受託者の間で取れないことが多い。
- 特に、デザイン上の要求により、セキュリティ対策が妥協されてしまうこともしばしばである。
- セキュリティガイドラインはOWASP、IPAをはじめすでに各種提唱されているが、利害が対立する場の合意基準として利用できるだけの客観性および具体性を持ったものは少ない。
- セキュリティ要求に応じて数段階のガイドラインがあるとよい。

Copyright (c) 2000-2006　NPO日本ネットワークセキュリティ協会

当初方針

- 仕様書上の要件である以上、客観性が第一。（後で「瑕疵だ」「仕様だ」「欠陥だ」という議論が発生することを防ぐのが目的）
- 例えば「できれば～」「～が望ましい」「～という危険性がある」「例えば～」「～のような脅威」「必要に応じて」「留意する必要がある」といった記述方法は原則として避ける。
- 受け取り手によって意味が変わる可能性がある言葉は、定義なしで使用しない。（例えば「クロスサイトスクリプティングがないこと」という要件は、「何がクロスサイトスクリプティングか」が議論になる）

Copyright (c) 2000-2006　NPO日本ネットワークセキュリティ協会

アプローチA：Web脆弱性カタログを作る

- A-1「起こる現象」で分類する。
  - 例えば「クロスサイトスクリプティング」。
  - 疑問：すべての現象を「厳密に定義」できるだろうか。
- A-2「望ましくないコードの書き方」で分類する。
  - 例えば「インプットをチェックせずクエリ文に渡す」。
  - 疑問：言語や処理方式に依存する。網羅的に書き出せるか。
- A-3「チェック方法」で分類する。
  - 例えば入力フィールドに「<script>document.alert(“hello,world”)（以下略）」と入れて現象出現したらアウト。
  - 疑問：チェック方法以外で出現する脆弱性はどうする？

Copyright (c) 2000-2006　NPO日本ネットワークセキュリティ協会

アプローチB：他の方法で要件を確定する

- B-1 **検査ツールを指定する。**
  - **例えばツール（AppScanとか）で重大度「高」が出たらアウト。**
  - **疑問：特定のツールにそこまで依存してよいか。**
- B-2 **外部リソースを参照する。**
  - **例えばOWASPガイドラインとか、IPAガイドラインとか**
  - **疑問：JNSAとしての意義はどこにあるのか。**

Copyright (c) 2000-2006　NPO日本ネットワークセキュリティ協会

アプローチC：プロセスを整備

- C-1 開発プロセスを指定
  - Webアプリケーションに詳しいメンバの参画
  - レビューの実施、承認プロセス、テストの実施
- C-2第三者検証
  - 第三者による診断 Web診断士（仮称）
  - 受注企業認証制度
- 問題：コンテンツを考えると結局アプローチAまたはBが必要になる

Copyright (c) 2000-2006　NPO日本ネットワークセキュリティ協会

検討(1):発注者と受注者の利害

- カタログ形式(A-1など)は、受注者(開発者)にとってとても不利である。「脆弱性がないこと」を仕様とされてしまうと、開発者が保証できない。
- 一方、コーディング方式(A-2)だと、逆に発注者が不利になる。発注者が欲しいのはあくまで安全なシステムである。
- 発注要件と検収要件を分けて考えたほうがいいかも知れない。

Copyright (c) 2000-2006 NPO日本ネットワークセキュリティ協会

検討（2）：トップダウンとボトムアップ

- 脆弱性のカタログを作り、そこから必要な要件を選び出すアプローチ（ISO15408的）と、あらかじめ適切なレベルを定義してあげるアプローチ（TCSEC的）がありうる。後者のほうが利用者にはわかりやすいの ではないか。
- 仕様提示という意味ではレジュメA-1の方法が、開発時はA-2が、テスト時には A-3の方法が必要になる。その意味では全部必要なのではないか。
- 全部は関係しているが、そのいずれかを「正」としなければ受発注の合意事項 としては使いにくい。

Copyright (c) 2000-2006　NPO日本ネットワークセキュリティ協会

検討(3):チェックツール

- WebLint(HTMLの文法チェックツール)のようなセキュリティチェックツールを作る方法はどうか。
- WebLintはHTMLの文法が厳密に決まっているから採点ロジックができる。セキュリティに応用するには工夫が必要。
- →今年度の検討からはとりあえず除外。

Copyright (c) 2000-2006 NPO日本ネットワークセキュリティ協会

議論集約

- 受注側と発注側、トップダウンとボトムアップ、両方をつなぐモデルができないか
- 出発点は発注側が意識する「リスク」がわかりやすい
- リスク（発注側）から対策（受注側）までブレークダウンを試みる
- 例：業務情報の改ざん

外部犯行----　不正アクセス　----インフラへの不正
内部犯行　　物理的不正行為　　アプリへの不正 -----SQL Injection ....

Copyright (c) 2000-2006　NPO日本ネットワークセキュリティ協会

ツリーの検討

- ツリーの左側に行くと発注者視点、右に行くと受注者視点
- 当初はブレークダウンしただけのツリーだったが、各レベルに次第に性格が現れて来た
- 各レベルに名称を付け、性格を明確にして再整理
- カテゴリ、分類などを議論しながら調整

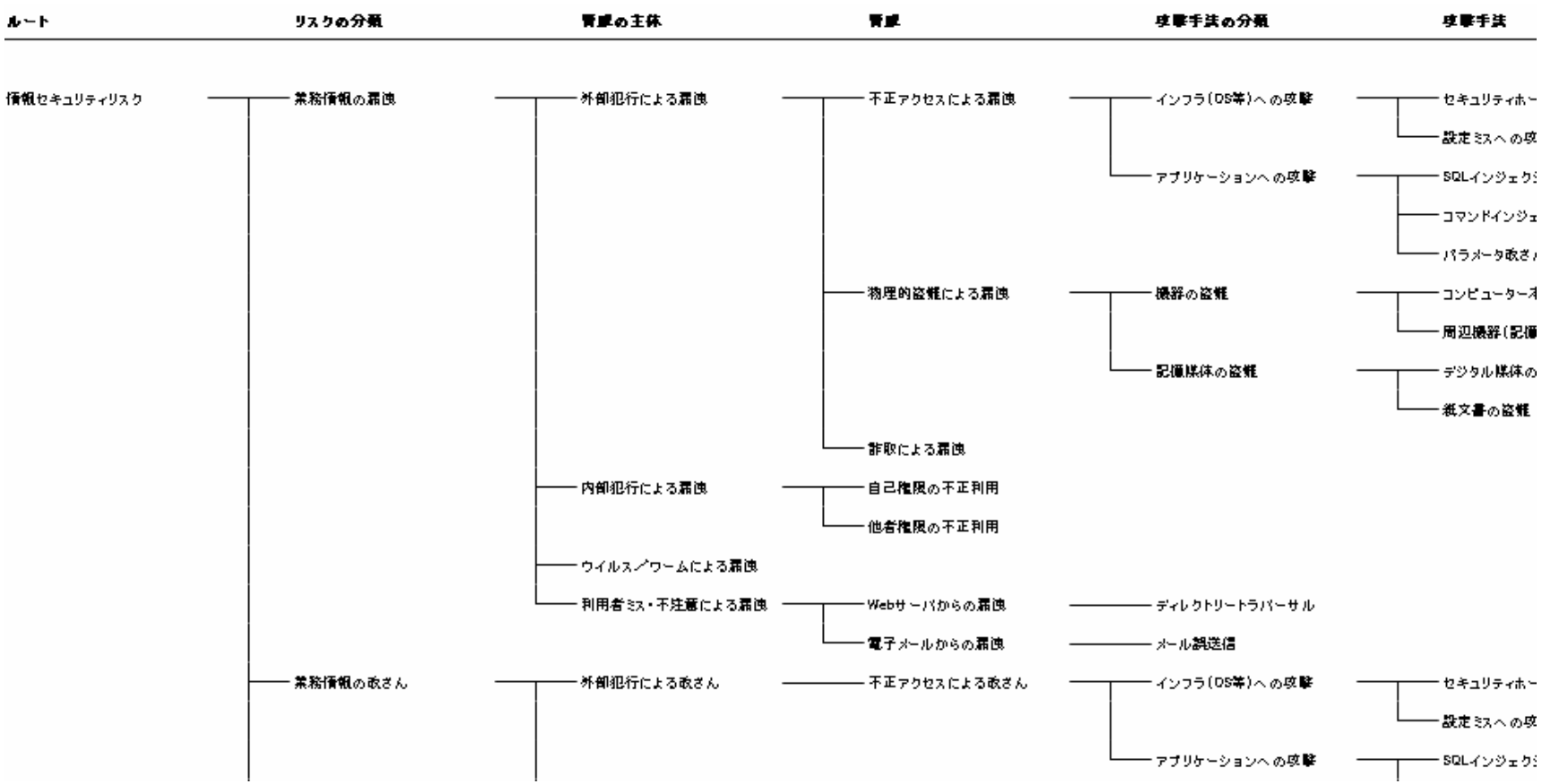
Copyright (c) 2000-2006　NPO日本ネットワークセキュリティ協会

成果

- Webセキュリティリスクの「ツリーモデル」を作成
- リスク側から対策側まで連続した5個のレベルでWebセキュリティリスクを記述
- どのレベルで語るかを明確にすることで受発注における意識のズレを防止する

Copyright (c) 2000-2006　NPO日本ネットワークセキュリティ協会

Webアプリケーションのセキュリティリスクツリー（部分）



Copyright (c) 2000-2006　NPO日本ネットワークセキュリティ協会

セキュリティリスクツリーの使い方

- ツリーのレベルを受発注双方で合意し、対策内容にズレがないようにする
  - RFPに記載
  - 契約書付帯文書として利用
  - 検収時の参考資料として利用
- Webアプリケーションに起因するセキュリティリスクの全体像を把握する

Copyright (c) 2000-2006 NPO日本ネットワークセキュリティ協会

今後の展開

- セキュリティリスクツリーの拡張および精度向上
- 有効性検証
  - シミュレーション、ケーススタディー
  - 実地適用
- 関連資料の開発･整備
  - 広報資材、教育資材、適用支援ツール
  - 認証制度？　Web診断士制度？？

Copyright (c) 2000-2006　NPO日本ネットワークセキュリティ協会

Copyright (c) 2000-2006　NPO日本ネットワークセキュリティ協会