東京工業大学　Webセキュリティのためのガイド

平成25年6月21日
情報セキュリティ監査・危機管理専門委員会

このガイドは、本学「情報セキュリティポリシー」及び「情報セキュリティ規則」に付随するWebセキュリティ運用に特化したガイドです。なお、関連する規則類に部局ごとの設置が義務付けられている「情報セキュリティ実施手順」があります。各部局の「情報セキュリティ実施手順」と本ガイドが整合しない場合は、必要に応じて「情報セキュリティ実施手順」を更新してください。また、本ガイドは緊急版であり、今後更新される予定があります。

A．公開するサーバとコンテンツの要否等の確認

（1）Webサーバを公開する場合は、情報資産管理担当者がその要否を検討し、必要と判断された場合にのみ公開するようにしてください。

（2）情報資産管理担当者は、担当するWebサーバのコンテンツの内容を定期的に把握し、不適切又は不必要なコンテンツが設置されていないことを確認してください。

（3）情報資産管理担当者は、Webサーバ上に設置しているコンテンツに関して、情報セキュリティ規則第４条に示す分類I,II,III,IVのコンテンツの有無を確認してください。分類Iのコンテンツは公開できません。分類II,III,IVのコンテンツを公開する場合はアクセス制限等の適切なセキュリティ設定を施してください。

B．人員配置と責任内容

（4）情報資産管理担当者は、Webサーバの管理のために情報システム管理者を指名してください。

（5）情報資産管理担当者は、情報システム管理者の補佐役として情報システム管理要員を置くことができます。

（6）情報資産管理担当者は、情報システム管理者及び情報システム管理要員に対し本学の情報セキュリティポリシー、情報セキュリティ規則、所属部局が定める情報セキュリティ実施手順及び本ガイドを遵守させるように留意してください。外部委託する場合は委託先企業等の構成員を情報システム管理要員にすることができます。その場合は特に規則等の遵守徹底をお願いいたします。

（7）情報資産管理担当者は、Webサーバ上でセキュリティインシデントが発生した場合、速やかに情報セキュリティ監査・危機管理専門委員会（ﾒｰﾙｱﾄﾞﾚｽ：ac@csi.titech.ac.jp）に報告し、その指示に従ってください。

（8）情報資産管理担当者は、セキュリティインシデント発生等の緊急時に公開情報を遮断するための連絡体制を整備してください。

（9）情報システム管理者は、セキュリティインシデント発生時において（8）で定められた連絡体制に基づき公開情報を緊急に遮断する必要があります。

(10) 情報資産管理担当者は、Webサーバの開発・管理・保守等を外部委託する場合、情報セキュリティ規則第１３条に定める内容の外部委託契約を締結してください。

(11) 情報システム管理者は、定期的に情報資産管理担当者に Web サーバの運用状況を報告してください。
(12) 情報資産管理担当者は、情報システム管理者からの報告に基づき、Web サーバが「C．技術的要件」に示す技術的要件を満たしているかを定期的に確認してください。
(13) 情報システム管理者は、情報セキュリティ監査・危機管理専門委員会からの公開 Web サーバ運用状況調査等に応じてください。
(14) 情報資産管理担当者は、Web サーバ上のアカウント管理ポリシーを定めてください。

C．技術的要件

(15) 情報システム管理者は、OS 及び Web サーバプログラムに関して原則週に１度以上の頻度で最新のセキュリティパッチの公開状況を確認してください。また、必要に応じて、セキュリティパッチを適用してください。
(16) 情報システム管理者は、CGI (Common Gateway Interface)、CMS (Contents Management System)、JAVA アプレット、データベースを利用する場合、原則週に１度以上の頻度で最新のセキュリティパッチの公開状況を確認してください。また、必要に応じて、セキュリティパッチを適用してください。
(17) 情報システム管理者は、ファイヤウォール等のセキュリティ機器を適切に設定してください。
(18) 情報システム管理者は、当該 Web サーバ上で不適切又は不必要なサービスが起動していないことを定期的に確認してください。
(19) 情報システム管理者は、「B．人員配置と責任内容（１４)」で情報資産管理担当者が定めたアカウント管理ポリシーを遵守してください。
(20) 情報システム管理者は、セキュリティインシデントに備えるためにサーバ上で Web サーバのアクセスログをとってください。また、ログは一定期間（例えば３か月間）保存してください。
(21) 情報システム管理者は、利用者からの文字列入力を伴う Web ページを提供する場合、様々なセキュリティ攻撃を防御するために入力文字列のチェックとサニタイジング（無害化）が行われていることを確認してください。

D．守ってほしいこと等

（１）情報資産管理担当者、情報システム管理者及び情報システム管理要員

・情報資産管理担当者が備えなければならない要件は、部局ごとに「情報セキュリティ実施手順」で規定してください。例としては常勤職員及び特任講師以上の非常勤職員と規定することが考えられます。より具体的には、研究室の管理者である教員や事務局の課長等が考えられます。
・情報システム管理者は、資産管理担当者の指示により実際に情報システムを管理する担当者です。具体的には、研究室の助教、事務部門のスタッフ等を充てることが考えられます。情報システム管理者はシステム管理上の責任が発生するので、大学院生等の学生に行わせることは適当ではありません。ただし、情報システム管理者に指名可能な職員がいない場合は、資産管理担当者自身が情報システム管理者を兼務し、大学院生等を情

報システム管理要員に充てる体制とすることが考えらます。

・情報システム管理要員は、情報システム管理者の補佐役として必要に応じて設けることができる Web サーバ管理の担当者です。具体的には、Web サーバ運用管理を外部委託している場合に委託先企業等の構成員を Web サーバ管理メンバーにする場合に、又は研究室の大学院生等に Web サーバ管理をさせる場合に利用することが考えられる。ただし、学生を情報システム管理要員にする場合は、本人の同意を必ず取り付け、学業に支障が出ないよう十分な配慮をしてください。

（2）アカウント管理ポリシーの例

・本ポリシーで規定するアカウントは、Web サーバに ssh 等でログインするアカウントと BASIC 認証等でコンテンツ配布時に必要なアカウントの双方を対象とします。

・学外からのリモートログインを許す場合は、ssh public-key authentication を用いてください。

・不必要なアカウントは必ず削除してください。(構築業者等が構築時に利用したアカウントが攻撃に使われる例が多数あるので、構築などを外部委託した場合は特に注意してください)

・アカウント名と等しいパスワードを用いないでください。

・パスワード長は 8 文字以上にしてください。

・パスワードには英大文字、英小文字、数字、記号をそれぞれ 1 文字以上含めてください。

・パスワードは定期的に（例えば３か月に１度）変更してください。

（3）セキュリティパッチについて

・Web サーバに関連するソフトウェアのセキュリティパッチの公開状況は、１週間に１度の確認が必要です。そのため、複数名での分担管理体制を組むことが望ましい状況です。

・一方複数名での分担がどうしても難しい場合は、自動的更新を利用する方法がありえます。

・例えば Ubuntu では Synaptic や unattended-upgrades を用いると自動的更新が可能となります。

・Windows Server では、自動更新を有効にすると自動で再起動することがあるので、自動再起動を抑制する設定を入れた方がよい場合があるので注意してください。

・CGI, CMS 等で自動更新を有効にした場合、急にコンテンツの表示に不具合が出る可能性があるので注意してください。

・CGI は、PHP, Perl, Python 等の Web 用のプログラミング言語を利用するもので、動的な Web ページを構成する場合等に利用されます。

・CMS は、技術的な知識がなくてもブログのように簡単にコンテンツ管理を行え、なおかつ、コンテンツのデザインをテンプレートによってカスタマイズ可能な Web サーバ上のソフトウェアです。

・CMS は、通常、PHP 等のプログラミング言語や SQL サーバ等のデータベースと連携して動くことが多く、セキュリティ上の注意が必要です。

（４）利用者からの文字列入力を伴うWebページを提供する場合について

・利用者からの文字列入力を伴うWebページでは、以下のセキュリティリスクが考えられます。

(a) SQLインジェクション攻撃（SQLデータベースを利用する場合に発生の可能性がある攻撃）

(b) バッファオーバフロー攻撃（バッファ量以上の文字列等を入力する攻撃）

(c) ディレクトリ・トラバーサル攻撃（通常はアクセスできない場所にあるシステムファイル等を不正に入手する攻撃）

(d) OSコマンドインジェクション攻撃（OSコマンドを不正に実行させる攻撃）

(e) クロスサイトスクリプティング攻撃（複数のサイトが連携した複雑な攻撃）

・このようなセキュリティリスクを低減するためには、入力文字列をチェックし、危険な文字のサニタイジング（無害化）を行う必要があります。

・例えば、SQLインジェクション攻撃であれば、入力された文字列中に「'」（シングルクォート）が含まれていないか確認し、含まれていればシングルクォート2文字に変更することで無害化することが可能になります。

・詳しくは「（５）解説文書について」を参考にしてください。

（５）解説文書について

・独立行政法人情報処理推進機構が提供している以下の解説文書を参考にするとより高度なWebサーバの管理が可能になると考えられます。必要に応じて参考にしてください。

情報セキュリティ早期警戒パートナーシップガイドライン2010年版
http://www.ipa.go.jp/security/ciadr/partnership_guide.html

安全ウェブサイトの作り方
http://www.ipa.go.jp/security/vuln/websecurity.html

（６）外部委託の運用について

・これまで、外部資金を受けている研究プロジェクト等のWebサイトを外部委託により構築している事例が多くあります。

・このようなWebサイトにおいて、構築時には予算を利用しているが、その後は特に予算措置をしておらず、結果的に運用はなおざりになっているケースが多くみられます。

・可能な限り運用や保守の予算を確保するよう心がけてください。

以上。