DM5-05-051

サーバ設定確認実施手順 ウェブサーバ編

策定手引書

2005 年 12 月

内閣官房情報セキュリティセンター

改訂履歴

改訂日	改訂理由
2005/12/21	初版
2006/4/21	各府省庁意見に基づく修正

商標について

Windows Server、FrontPage は、米国 Microsoft Corporation の米国、日本およびその他の国における登録商標または商標です。

Sun、Solaris は、米国 Sun Microsystems, Inc. の米国およびその他の国における登録商標または商標です。

HP-UX は、Hewlett-Packard Company の米国およびその他の国における登録商標または商標です。

Linux は、Linus Torvalds の米国及びその他の国における登録商標又は商標です。

1　本書の目的

本書は、サーバの設定確認を行う場合の手順書（ウェブサーバ編）を策定するための手引書である。本書に基づいて策定される「サーバ設定確認実施手順 ウェブサーバ編」は、ウェブサーバの検収時における設定確認だけでなく、定期的なウェブサーバの設定確認における利用も想定される。また、定期的な設定確認の場合には、ユーザ認証やアクセス制御等の項目のみを部分的・重点的に確認する利用も想定される。

手順書の整備を担当する者は、「サーバ設定確認実施手順 ウェブサーバ編」を策定する際に、本書を参考にすることによって、政府機関統一基準に基づく省庁基準に準拠してこれを効率良く作成することができる。

2　実施手順に記載すべき事項

「サーバ設定確認実施手順 ウェブサーバ編」には、以下の事項を具体化させて記載すること。

2.1　政府機関統一基準（NISD-K303-052）に定める「サーバ設定確認実施手順 ウェブサーバ編」に係る遵守事項

3.2.3　情報の保存（1）格付けに応じた情報の保存
3.2.4　情報の移送（5）電磁的記録媒体に記録された情報の保護対策
3.2.5　情報の提供（1）情報の公表
4.1.1　主体認証（1）主体認証機能の導入
4.1.1　主体認証（2）行政事務従事者における識別コードの管理
4.1.1　主体認証（3）行政事務従事者における主体認証情報の管理
4.1.2　アクセス制御（1）アクセス制御機能の導入
4.1.2　アクセス制御（2）行政従事者による適正なアクセス制御
4.1.3　権限管理（1）権限管理機能の導入
4.1.3　権限管理（2）識別コードと主体認証情報の付与管理
4.1.4　証跡管理（1）証跡管理機能の導入
4.1.4　証跡管理（2）行政事務従事者による証跡の取得と保存
4.1.6　暗号と電子署名（1）暗号化機能及び電子署名の付与機能の導入
4.1.6　暗号と電子署名（2）暗号化及び電子署名の付与に係わる管理
4.2.1　セキュリティホール対策（1）情報システムの構築時
4.2.1　セキュリティホール対策（2）情報システムの運用時
4.2.2　不正プログラム対策（1）情報システムの構築時
4.2.2　不正プログラム対策（2）情報システムの運用時
4.2.3　サービス不能攻撃対策（1）電子計算機、通信回線装置及び通信回線がインターネットからのアクセスを受ける情報システムの構築時

5.2.1　電子計算機共通対策（1）電子計算機の設置時

5.2.1　電子計算機共通対策（2）電子計算機の運用時

5.2.3　サーバ装置（1）サーバ装置の設置時

5.2.3　サーバ装置（2）サーバ装置の運用時

5.3.1　通信回線を介して提供するアプリケーション共通対策（2）サービスの運用時

5.3.3　ウェブ（1）ウェブの導入時

2.2　セキュリティ確保に係るその他の留意事項

2.1 に示す遵守事項のほか、セキュリティ確保に係る留意事項として、以下の項目を考慮すべきである。

- システム領域とデータ領域との分離
- ウェブサーバアプリケーションに付属する不要なコンテンツの削除

3　文書構成例

「サーバ設定確認実施手順 ウェブサーバ編」は、ウェブサーバアプリケーションの動作に関する設定及び運用並びに管理上必要となるアプリケーション（リモート管理、コンテンツ更新、パフォーマンス監視等）の設定等も含めた構成が有効である。文書構成の例を以下に示す。

1 本書の目的

2 本書の対象者
　2.1 対象者

3 オペレーティングシステムに関する確認項目
　3.1 ユーザ認証に関する項目
　　・アカウントの管理
　　・パスワードの管理
　　・認証の管理
　　・アカウントのロックアウト
　　・認証時のメッセージ表示
　3.2 ユーザ権利の割り当てに関する項目
　　・システム管理に関する権利
　　・ログオンに関する権利
　　・監査に関する権利
　3.3 アクセス制御に関する項目
　　・ネットワークレベルでのアクセス制御
　　・ファイルシステムレベルでのアクセス制御
　　・システムリソースレベルでのアクセス制御
　　・デバイスレベルでのアクセス制御
　3.4 サービスに関する項目
　　・サービスの停止
　　・機能の無効化
　3.5 ログ管理に関する項目
　　・取得項目の選択
　　・ログファイルの保存方法及び管理
　　・監査機能の設定
　3.6 セキュリティホール対策に関する項目
　　・既知アップデートの適用
　　・アップデート方法の設定
　3.7 不正プログラム対策に関する項目
　　・アンチウイルスソフトウェアによる対策
　　・システム設定による対策
　3.8 サービス不能攻撃対策に関する項目
　　・システムパラメータの調整
　　・ネットワークパラメータの調整
　3.9 パフォーマンスに関する項目
　　・システムパラメータの調整

・ネットワークパラメータの調整
3.10 暗号及び電子署名に関する項目
・システム全般の暗号化設定
3.11 その他の項目
・要機密情報の保護
・スクリーンセーバーの設定
・バックアップの設定

4 ウェブサーバアプリケーションに関する確認項目
4.1 コンテンツに関する項目
・パーティションの分割
・不要なコンテンツの削除
・公開コンテンツの格付け確認
・私的なコンテンツの排除
4.2 機能に関する項目
・スクリプト／ファイル実行の制限
・アプリケーション／バージョン情報表示の制限
・ユーザドキュメントの公開の禁止
・インデックス表示の禁止
・WebDAV／FrontPage®等の機能制限
4.3 アクセス制御に関する項目
・ネットワークレベルでのアクセス制御
・ユーザレベルでのアクセス制御
・コンテンツレベルでのアクセス制御
4.4 ログ管理に関する項目
・取得項目の選択
・ログファイルの保存方法及び管理
4.5 セキュリティホール対策に関する項目
・既知アップデートの適用
・アップデート方法の設定
4.6 暗号に関する項目
・SSL/TLS の利用

5 リモート管理アプリケーションに関する確認項目
5.1 機能に関する項目
・リモート管理機能の設定
・セキュリティ機能の設定
・機能の無効化
5.2 ユーザ認証に関する項目
・認証方法の強化
・認証時のメッセージ表示
5.3 アクセス制御
・ユーザレベルでのアクセス制御
5.4 ログ管理に関する項目
・取得項目の選択
・ログファイルの保存方法及び管理
5.5 セキュリティホール対策に関する項目
・既知アップデートの適用

・アップデート方法の設定
5.6 暗号に関する項目
・暗号機能の強化

4　作成する上での留意事項

「サーバ設定確認実施手順 ウェブサーバ編」は、以下のことに留意して作成する。

(1) オペレーティングシステム、ウェブサーバアプリケーション及び運用・管理上必要となるアプリケーションごとに確認すべき設定項目が異なるため、それぞれに特化した手順書を作成する。

(2) 確認及び結果の判断を的確に行うため、チェックシートの形式で作成し、確認すべき設定項目を具体的に記述する。

(3) 手順書の対象者として十分な技術を有する者を前提とした場合、確認手順を省略して確認すべき内容のみを簡潔に記載する。

(4) 文書構成例に記載された見出しは基本的なものであるため、ウェブサーバの利用目的、構成、環境等に応じた見出しの検討・追加を行い、必要な確認項目を網羅する。

(5) 文書構成例に記載された見出し及び検討・追加された見出しごとに、ソフトウェアの開発元が公開している情報を活用して確認項目を抽出する。

(6) ソフトウェアの開発元が公開している情報を活用する場合には、著作権に注意する。

(7) 手順書は、府省庁内の担当者による検収時の又は定期的な設定確認としての利用が想定されているため、業者に公開せずに行政事務従事者に限り参照できる文書として取り扱う。

(8) 前記２に示す事項を「サーバ設定確認実施手順 ウェブサーバ編」に反映するに当たっては、当該事項の内容に応じて、以下のいずれかの方針で記述する。

[具体化]・・・「ウェブサーバ」に限定されず一般的・抽象的に記述されており、具体化が必要と思われる遵守事項については、これを「ウェブサーバ」に適用し、表現をより具体的に修正・追加する。

[転記]・・・・記述内容が具体性を持ち、変更が不要と思われる遵守事項については、これを転記する。

[詳細化]・・・記述内容が具体性を持っているが、行政事務従事者の利便性を考慮して、より詳細な解説を付すべきと思われる遵守事項については、解説書等を参考に、これを詳細化する。

[背景]・・・・主にセキュリティ機能の実装に関する内容であり、これを背景として行政事務従事者による注意義務が発生すると思われる遵守事項については、これを行政事務従事者の立場から解釈し直す。

[別立場]・・・行政事務従事者の立場ではなく、責任者側又は管理者側の立場から記述されている遵守事項については、これを行政事務従事者の立場から解釈し直す。

[参考引用]・・直接「ウェブサーバ」に関連した内容ではないが、行政事務従事者の理解促進に寄与すると思われる遵守事項については、これを参考引用する。

[一般]・・・・直接「ウェブサーバ」に関連した内容ではないが、一般論として手順書に記載しておくことが望ましいと思われる遵守事項については、これを周辺知識として盛り込む。

5　参考資料

「サーバ設定確認実施手順 ウェブサーバ編」の作成に際しては、以下のような資料が参考となる。

5.1　政府関係の資料

(1) 独立行政法人 情報処理推進機構(IPA)の「セキュアなWebサーバーの構築と運用」
URL: http://www.ipa.go.jp/security/fusei/ciadr.html

5.2　政府以外の資料

(1) マイクロソフト株式会社の「セキュリティガイダンスセンター」
URL: http://www.microsoft.com/japan/security/guidance/default.mspx

(2) マイクロソフト株式会社の「Windows Server™ 2003 セキュリティ ガイド」
URL: http://www.microsoft.com/japan/technet/security/prodtech/windowsserver 2003/w2003hg/sgch00.mspx

(3) サン・マイクロシステムズ株式会社の「Sun® BluePrints Security Publications」
URL: http://www.sun.com/software/security/blueprints/index.xml

(4) サン・マイクロシステムズ株式会社の「Solaris® Security Toolkit」
URL: http://www.sun.com/software/security/jass/

(5) 日本ヒューレット・パッカード株式会社の「ホワイトペーパー：ネットワーク&セキュリティ」
URL: http://h50146.www5.hp.com/products/software/oe/hpux/developer/setup/tips.html

(6) 日本ヒューレット・パッカード株式会社の「HP-UX® Bastille」
http://h20293.www2.hp.com/cgi-bin/swdepot_parser.cgi/cgi/displayProductInfo.pl?productNumber=B6849AA

(7) 「Bastille Linux®」
http://www.bastille-linux.org/