各種学生情報システム群の脆弱性診断業務　一式

仕　様　書

平成 31 年 1 月

独立行政法人国立高等専門学校機構

１．件名

各種学生情報システム群の脆弱性診断業務　一式

２．目的

独立行政法人国立高等専門学校機構（以下、「機構」という。）は、平成１６年４月に独立行政法人化され、全国５１の国立高等専門学校（以下、「高専」という）が一つの法人格にまとまることによるスケールメリットを活かした管理運営が求められている。

これまで各高専が独自に運用してきた各種学生情報システム群があるが、平成２５年から教務システムの共通化を進めており、平成３１年１０月の全面稼働により、全国の５１高専における教務データの多くが一元的に集約されることになる。また、その集約されたデータを活用して、各種学生情報システム群（教務入試システム、出席管理システム、時間割システム、証明書発行システム、ポートレートシステム、ルーブリック集計システム）が運用されることになる。

本業務においては、そのシステム群が本格運用される前に、脆弱性診断を行うことを目的とする。

３．調査に関する基本方針

１　診断対象一覧

診断対象は、以下6システムとする。

教務入試システム	ページ数：１５０画面
出席管理システム	ページ数：３２画面
時間割システム	ページ数：５０画面
証明書発行システム	ページ数：７画面
ポートレートシステム	ページ数：４画面
ルーブリック集計システム	ページ数：１８画面

２　診断作業

最低限「別紙 診断実施項目一覧」の内容を満たす形でWebアプリケーション診断を実施すること。

2.1　診断方法

診断対象リクエスト通信に対して全診断実施項目の診断を実施すること。なお、正常遷移時の応答と、検査文字列送信時の応答の差異を全て診断員が確認することで脆弱性の有無を判定すること。また、セッションやバリデーションに起因するエラー処理によってWebアプリケーションのロジックに潜む脆弱性の検出ができない可能性があることを踏まえ、各診断対象リクエスト通信においてエラー処理が発生しない、正常な処理が行われるリクエスト通信の内容を改ざんし、診断を実施すること。

2.2　診断評価方法

報告レベルは影響の度合いや再現性を考慮して、分類し報告すること。報告レベルはセキュリティ診断の専門家が分類すること。報告レベルの定義については、

下表を参考にすること。

報告レベル	判断指標
High	緊急性が高く、早急に対策が必要。
Medium	間接的に攻撃に利用される可能性があり複数組み合わせることで実害へと発展する問題点。 対策が必要。
Low	直接的な被害に発展する可能性は低いが、対策することで潜在的なリスクを回避可能な問題点。対策を推奨。
Informational	報告レベルはつかないものの、セキュリティ上好ましくないと考えられる事項。

※1 単純な脆弱性の種類に報告レベルを対応させるのではなく、実際に発生する恐れのあるリスクに対して報告レベルを設定すること。

2.3 診断結果報告書の作成

診断結果をまとめ報告書を作成すること。報告書には最低限以下の事項を記載すること。

- 診断結果全体の評価
- 診断対象ごとの検出された脆弱性の情報
  - 検出された脆弱性の報告レベル
  - 検出された脆弱性の概要
  - 検出された脆弱性による影響
  - 検出された脆弱性の対策方法
  - 脆弱性を検出したすべてのパラメータ
  - 脆弱性を検出した際の入力文字列
- 検出された脆弱性ごとの確認した際のログ

3 診断結果に関するフォローアップ

診断実施中に問い合わせが入った場合、これに対応すること。また、報告書の記載内容に関しての問合せ（脆弱性の説明、脆弱性と判断するに至った根拠、脆弱性確認方法など）を、報告書提出後の翌日から 3 ヶ月後まで電子メール若しくは電話にて行うこと。

４．請負期間

契約締結日～平成３１年３月２７日

５．業務請負場所

契約担当役が指定する場所

６．納入成果物

納品物として、診断結果報告書を行う診断するシステムごとに作成し、電子媒体にて

提出すること。

７．請負条件

請負者は以下の条件を満たしていなければならない。

① 一般財団法人情報マネジメントシステム認定センター，公益財団法人日本適合性認定協会若しくは海外の認定機関により認定された審査登録機関による ISO/IEC27001 又は JIS Q 27001 の認証を受けていること。

② 一般財団法人日本情報経済社会推進協会からプライバシーマーク制度によるプライバシーマーク（JISQ15001）使用許諾の認証を受けていること。

③ IPA が公開する「情報セキュリティサービス基準適合サービスリスト」の脆弱性診断サービスのサービス分野に登録されていること。

④ 情報システムの WEB サービスの脆弱性に関する診断を過去１年以内に２００件以上実施した実績があること。

⑤ 品質管理体制およびマニュアルが整備されていること。

⑥ 本業務の作業者に求める資質は次のとおり。

(ア)プロジェクトマネージャは情報セキュリティ診断のプロジェクトマネージメントを過去 1 年以内に３件（自社内の社内システムの診断は除く）以上行った実績を持つこと。

(イ)診断のチームリーダは、情報処理安全確保支援士（登録セキスペ）であること。システム監査技術者、CISA、情報セキュリティスペシャリスト、テクニカルエンジニア（情報セキュリティ）、情報セキュリティ監査人のうち、いずれかの資格を有する者でもよしとする。

(ウ)診断のチームリーダは過去 1 年以内に１０件以上の診断経験（自社内の社内システムの診断は除く）を持つこと。

(エ)診断のチームは、最新の WEB サービスに対する攻撃の知識、情報、手法などを有し、それを利活用した診断を実施すること。

８．機密保持

（１） 請負者は、本調達に係る作業を実施するに当たり、機構から取得した資料（電子媒体、文書、図面等の形態を問わない。）を含め契約上知り得た情報を、第三者に開示又は本調達に係る作業以外の目的で利用しないものとする。但し、次のア）ないしオ）のいずれかに該当する情報は、除くものとする。

ア）機構から取得した時点で、既に公知であるもの

イ）機構から取得後、請負者の責によらず公知となったもの

ウ）法令等に基づき開示されるもの

エ）機構から秘密でないと指定されたもの

オ）第三者への開示又は本調達に係る作業以外の目的で利用することにつき、事前に機構に協議の上、承認を得たもの

（２） 請負者は、機構の許可なく、取り扱う情報を指定された場所から持ち出し、あるいは複製してはならない。

（３）　請負者は、本調達に係る作業に関与した請負者の所属職員が異動した後においても、機密が保持される措置を講じるものとする。

（４）　請負者は、本調達に係る検収後、請負者の事業所内部に保有されている本調達に係る機構に関する情報を、裁断等の物理的破壊、消磁その他復元不可能な方法により、速やかに抹消すると共に、機構から貸与されたものについては、検収後１週間以内に機構に返却するものとする。

９．その他留意事項

（１）　本業務の履行について疑義が生じたとき、又は本業務に伴い機構と交わす契約書に定めのない事項については、機構及び請負者の双方で協議の上、決定すること。

（２）　本調達において第三者が有する著作物を巡る紛争が生じた場合には、当該紛争の原因が専ら機構の責めに帰す場合を除き、請負者の責任、負担において一切を処理すること。機構は、当該紛争の事実を知ったときは、請負者に通知し、必要な範囲で訴訟上の防衛を請負者に委ねる等の協力措置を講ずる。

別紙　診断実施項目一覧

1. データベースへの不正アクセス

No	診断実施項目	概要	診断実施項目の詳細	政府セキュリティ統一基準群
1-1	SQLインジェクション	データベースと連動する処理において、任意のSQLコマンドが実行可能かどうかを診断する。	データ型が文字列型の部分に対して、特定の文字列を送った場合に、データベースを不正に操作し、情報が漏えいするかを確認する。	a) SQL インジェクション脆弱性
			データ型が文字列型の部分に対して、特定の文字列を送った場合に、情報漏えいまで確認はできないが、データベースを不正に操作できるかを確認する。	
			データ型が数値型の部分に対して、特定の文字列を送った場合に、データベースを不正に操作し、情報が漏えいするかを確認する。	
			データ型が数値型の部分に対して、特定の文字列を送った場合に、情報漏えいまで確認はできないが、データベースを不正に操作できるかを確認する。	
			SQL文をクライアント側に受渡している場合に、SQL文を改ざんして送ることにより、データベースを不正に操作し、情報漏えいするかを確認する。	
			SQL文をクライアント側に受渡している場合に、SQL文を改ざんして送ることにより、情報漏えいまでは確認はできないが、データベースを不正に操作できるかを確認する。	
1-2	SQLエラーの発生	エラーメッセージ内にSQL文が含まれたメッセージが表示されるかどうかを診断する。	不正な操作を行った場合に、詳細なSQLエラーが画面に表示され、必要の無い情報が攻撃者に閲覧されないかを確認する。	a) SQL インジェクション脆弱性

2. サーバシステムへの不正アクセス

No	診断実施項目	概要	診断実施項目の詳細	政府セキュリティ統一基準群
2-1	OSコマンドインジェクション	Webサーバ上から任意のOSコマンドが実行可能かどうかを診断する。	OSコマンドをWebアプリケーションに送った場合に、Webアプリケーションが動作しているサーバを不正に操作して、その結果を閲覧できるか確認する。	b) OS コマンドインジェクション脆弱性 k) eval インジェクション脆弱性 (※) ※ インジェクション系の問題点のひとつとして、eval インジェクションも確認しています。
			OSコマンドをWebアプリケーションに送った場合に、Webアプリケーションが動作しているサーバを不正に操作できるかを確認する。	
			SSIタグをWebアプリケーションに送った場合に、Webアプリケーションが動作しているサーバを不正に操作して、その結果を閲覧できるか確認する。	
			SSIタグをWebアプリケーションに送った場合に、Webアプリケーションが動作しているサーバを不正に操作できるかを確認する。	
2-2	ディレクトリトラバーサル	本来公開していないディレクトリ等へのアクセスが可能かどうかを診断する。	../../../etc/passwdなどの文字列をWebアプリケーションに送った場合に、サーバ上にある本来公開していないファイルにアクセスし、閲覧することにより情報が漏えいするかを確認する。	c) ディレクトリトラバーサル脆弱性
			../../../etc/passwdなどの文字列をWebアプリケーションに送った場合に、サーバ上にある本来公開していないファイルにアクセスし、閲覧はできないものの存在確認が可能かを確認する。	

3. 利用者に被害を与える恐れ

No	診断実施項目	概要	診断実施項目の詳細	政府セキュリティ統一基準群
3-1	クロスサイトスクリプティング	ユーザのブラウザ上で任意のスクリプトを実行できるかどうかを診断する。	スクリプトをWebアプリケーションに送った場合に、スクリプトが実行されるかを確認する。	f) クロスサイトスクリプティング脆弱性
			HTMLタグをWebアプリケーションに送った場合に、タグがページに挿入され、見た目のページが変更可能かを確認する。	
			属性値に出力がある場合に、スクリプトが実行されるかを確認する。	
			出力箇所が引用符で囲まれていないために、スクリプトが実行されるか確認する。	
			href属性に出力がある場合に、スクリプトが実行されるかを確認する。	
			DOM(document object model)の仕組みを使って、スクリプトが実行されるかを確認する。	
			不完全なマルチバイト文字列を送信し、記述されているクォートを無効化することで、スクリプトが実行されるかを確認する。	
			UTF-7などの場合に、スクリプトが実行されるかを確認する。	
			Javascript内に出力がある場合に、スクリプトが実行されるかを確認する。	
			バイナリデータを正しく扱うことができない関数がある場合に、スクリプトが実行されるかを確認する。	
			本来存在しないパラメータを追加した場合に、スクリプトが実行されるかを確認する。	
			アップロードされたファイルにおいて、スクリプトが実行されるかを確認する。	
			ブラウザがContent-Typeを無視することを利用し、スクリプトが実行されるかを確認する。	
3-2	改行コードインジェクション	Webサーバのレスポンスヘッダ、もしくはメールヘッダに不正なヘッダの追加・本文の改ざんが可能かどうかを診断する。	レスポンスヘッダに改行や任意のヘッダを追加されることで、任意のCookieを利用させることなどができるかを確認する。	j) HTTP ヘッダインジェクション脆弱性 i) メールヘッダインジェクション脆弱性
			メールヘッダに改行や任意のヘッダを追加されるか、または宛先を追加できるかを確認する。	
3-3	クロスサイトリクエストフォージェリ	重要な最終確定処理において、Cookieのみでセッション管理が行われていないかどうかを診断する。	ログイン認証があるサイトのユーザ情報変更画面のような重要な確定処理において、セッションIDであるCookieのみでセッション管理が行われているかを確認する。その結果、ユーザが意図せず情報を変更させられてしまうかを確認する。	g) クロスサイトリクエストフォージェリ脆弱性
			重要な最終確定処理において、セッションIDであるCookieとワンタイムトークンであるhidden値で対策している場合に、Cookieとhidden値が紐づいていないかを確認する。	
			重要な最終確定処理において、Refererをチェックしている場合に、チェックを回避できるかを確認する。	

4. セッション管理・認証の問題

No	診断実施項目	概要	診断実施項目の詳細	政府セキュリティ統一基準群
4-1	セッションIDの扱い	適切にセッションIDが扱われているかどうかを診断する。	URLにセッションIDが含まれているかを確認する。	d) セッション管理の脆弱性
			セッションIDが推測可能かを確認する。	
			HTTPとHTTPSが混在しているサイトの場合に、適切にセッション管理が行われているかを確認する。	
			セッションIDの有効期限が長すぎるかを確認する。	
			ログアウト時にセッションが破棄されたかを確認する。	
			ログアウト機能があるかを確認する。	
4-2	Cookieの扱い	Cookieの設定項目に対して診断する。	HTTPSサイトにおけるCookieにSecureフラグが付加されているかを確認する。	―
4-3	強制ブラウジング・認証回避	ログイン画面以降のURLに直接アクセスし、認証を回避することが可能かどうかを診断する。	ログイン認証後の画面をログインせずに操作できるかを確認する。	d) セッション管理の脆弱性
			ログイン認証後の画面をログインせずに閲覧できるかを確認する。	
4-4	セッションフィクセイション	発行済みのセッションIDを利用させることが可能かどうかを診断する。	ログイン時に新規セッションIDが発行されているかを確認する。	d) セッション管理の脆弱性
			URLRewriting機能のようにURLにセッションIDを含むことができるかを確認する。	
4-5	認証時のアプリケーションのレスポンス内容	ユーザ認証の際のメッセージの内容からユーザの存在確認が可能かどうかを診断する。	ログイン画面における認証時に、ログイン失敗時のメッセージから存在するログインIDを確認する。	―
4-6	権限昇格	制限されたリクエストを直接サーバへ送信することにより、権限を越えた処理が実行可能かどうかを診断する。	想定外の操作を行うことにより、権限を越えた操作ができるかを確認する。	e) アクセス制御欠如と認可処理欠如の脆弱性
			想定外の操作を行うことにより、権限の無い画面にアクセスできるかを確認する。	

5. アプリケーション固有の問題

No	診断実施項目	概要	診断実施項目の詳細	政府セキュリティ統一基準群
5-1	パラメータ改ざんによるシステムの不正利用	Webアプリケーションに応じたシステムの不正利用が可能かどうかを診断する。	リクエストを改ざんすることによって、システムを不正に利用できるかを確認する。 例） ・商品価格を改ざんして、購入処理が完了することを確認する。 ・メールの宛先を変更して、メールを送信できるかを確認する。 ・リクエストを改ざんすることにより、転送先を改ざんすることができるかを確認する。	e) アクセス制御欠如と認可処理欠如の脆弱性
5-2	アップロード機能の不正利用	アップロード機能において、実行ファイルがアップロード可能かどうかを診断する。また、アップロードしたファイルがWebアプリケーション上から実行可能かどうかを診断する。	スクリプトファイルをアップロードし、サーバ側でスクリプトが実行可能かを確認する。	―
5-3	バッファオーバーフロー	長い文字列を送信することにより、メモリ容量を超え不正な操作が可能かどうかを診断する。また、サーバ側で妥当性チェックがおこなわれているか診断する。	長い文字列を送った場合に、サイトに負荷がかかり応答が遅くなることや、サイトが停止することを確認する。	m) バッファオーバーフロー及び整数オーバーフロー脆弱性
5-4	内部サーバエラー	不正な文字列を含むリクエストを送信した場合、エラーハンドリングが適切に行われているか診断する。	不正な文字列を送信した場合に、内部サーバエラーが発生するかを確認する。	―

6. セキュリティへの配慮

No	診断実施項目	概要	診断実施項目の詳細	政府セキュリティ統一基準群
6-1	コモンファイルエクステンション	WebアプリケーションのURLに応じたファイルやディレクトリの存在の確認を診断する。	通常公開していないURLにアクセスした場合に、重要なファイルが閲覧可能かを確認する。	―
			通常公開していないURLにアクセスした場合に、バックアップファイルが取得可能かを確認する。	
			通常公開していないURLにアクセスした場合に、ソースコードが閲覧可能かを確認する。	
			通常公開していないURLにアクセスした場合に、ディレクトリが存在する反応があるかを確認する。	
			ディレクトリにアクセスした場合に、ディレクトリ内のファイル一覧が閲覧可能かを確認する。	
6-2	SSLの設定	重要情報が適切にHTTPSで保護されているか診断する。	本来HTTPS通信で行われる処理に対し、HTTP通信で処理が行われるかを確認する。	―
			HTTPSサイトにアクセスした場合に、ブラウザに鍵マークが表示されるかを確認する。	
6-3	サーバの設定	適切なサーバ設定が行われているかどうかを診断する。	不正な操作をした場合に詳細なデバック情報などの詳細なエラーが表示されないかを確認する。	h) クリックジャッキング脆弱性
			想定外の操作、もしくは正常動作において、内部IPアドレスが表示されるかを確認する。	
			想定外の操作、もしくは正常動作において、内部パスが表示されるかを確認する。	
			TRACE/TRACKメソッドが有効かを確認する。	
6-4	重要情報の扱い	重要情報が適切に扱われているかどうかを診断する。	重要な情報の通信時にHTTPSで通信が行われているかを確認する。	l) レースコンディション脆弱性 ※明示的には診断項目に含まれていませんが、当該脆弱性に起因すると考えられる問題が確認できた場合は報告させていただきます。
			サイトにアクセスしたPCブラウザのキャッシュに重要な情報が残るかを確認する。	
			Cookieに個人情報などの重要な情報があるかを確認する。	
			URLにアカウント情報や個人情報などの重要な情報があるかを確認する。	
			クレジットカード情報などの重要な情報が画面に全て表示されるかを確認する。	
6-5	妥当性チェック	入力値に対して適切な妥当性チェックが行われているかどうかを診断する。	セレクトボックスなどの固定値の部分に対し、任意の値をサーバに送り、正常に動作するかを確認する。	―
			ラジオボタンなどの固定値の部分に対し、任意の値をサーバに送り、正常に動作するかを確認する。	
			通常ブラウザから任意の入力を想定していない部分に対し、任意の値を送り、正常に動作するかを確認する。	
6-6	不適切な画面設計	セキュリティ上好ましくない画面設計が行われていないどうかを診断する。	アドレスバー・ステータスバーが表示されているかを確認する。	―
			右クリックメニュー（コンテキストメニュー）の表示を規制しているかを確認する。	
			パスワード入力時にパスワード属性が使用されているかを確認する。	
			HTTPのフレーム内にHTTPSのフォームが存在するかを確認する。	