セキュリティ診断サービスについて

エレシーク VA

診断レポートサンプル付き

株式会社コーボー・ホールディングス

東京都新宿区神楽坂 2-13｜TEL:03-3513-7630

文書番号 1309121272

はじめに

情報システム、IT・インターネットは、企業や組織の運営に欠かせないものになりました。しかし、現在の企業や組織は、情報システムへの依存による利便性の向上と引き換えに、大きな危険性を抱え持つことを忘れてはいけません。顧客情報の漏洩（ろうえい）による企業や組織のブランドイメージの失墜、企業の秘密情報の漏えい、情報システムの停止・消失・破壊による損失など、情報セキュリティ上のリスクは、企業や組織に大きなダメージをもたらします。また、インシデントの影響は取引先や顧客などのステークホルダー、関係者へ波及します。 企業や組織にとって、情報セキュリティに対するリスクマネジメントは重要な経営課題のひとつと考えなければなりません。特に、個人情報や顧客情報などの重要情報を取り扱う場合には、これを保護することは、企業や組織にとっての社会的責務でもあります。

組織がイノベーションを実現して成長するに従い、IT 部門への要求が高くなりますが同時に IT 予算に占めるセキュリティコストの割合が増大していることも否めません。これはスマートフォンを代表とするモバイルコンピューティング、ソーシャルメディアの普及などが要因の一つになっています。コスト効率を考慮して企業のセキュリティを確保することは容易ではありませんが、常にセキュリティに対する戦略的思考と恒常的なセキュリティ状況把握、戦略の見直しを積極的に実施する必要があります。

株式会社コーボーホールディングスでは Web サイト・アプリケーションのセキュリティ診断（エレシーク VA）および対策を支援するサービスを展開しています。セキュリティ診断を通してセキュリティの抜本対策、セキュリティの意識向上に繋げるよう、予算を柔軟に踏まえたメニューでサービスを提供しています。セキュリティに関するお問い合わせは是非当社までご連絡ください。

当該ホワイトペーパーでは、次の内容についてセキュリティ診断を検討する材料として提供しています。

１．情報漏えいの被害額一覧（参考）
２．情報セキュリティの脅威 MAP について
３．セキュリティ診断 「エレシーク VA」 メニュー
４．セキュリティ診断レポートサンプル

１． 情報漏えいの被害額一覧（参考）

情報漏えいにより被る被害額の算出にあたり、多種多様なケースが想定され被害額が分かりづらいため、個人情報の取得情報および企業規模に応じて一覧表にまとめました（引用：NPO 日本ネットワークセキュリティ協会（以下 JNSA））

JNSA の調査によると、2011 年に発生した情報漏えい事件の中で、個人情報漏えいの件数は 1551 件、個人情報漏えい者数は、のべ 628 万 4363 人、想定損害賠償額は 1899 億 7378 万円にも及びます。情報漏えい事件 1 件あたりの想定損害賠償額も 1 億 2810 万円となります。特に注目すべきは、1 人あたりの平均想定損害賠償額が年々高くなっているという点です。2011 年の調査では 4 万 8533 円だったのが、2012 年上半期の調査では 5 万 7710 円、1 万円近くも上昇しています。個人情報のビジネスでの利用が増えていること、個人情報を搾取し売買するブラックマーケットが拡大していることなど、個人情報の価値が上がっていることが挙げられます。

大手企業、または大規模サイトが損害賠償額の平均値を上げていることが上げられるため、以下の表では情報漏えい 1 件当たりの単価を一覧表でまとめ企業がセキュリティを考える材料として検討しやすくしています。

個人情報を多く取得しているサイトとしては、SNS、ユーザー登録型 Web サービス、掲示板、EC サイトなどが上げられますが、コーポレイトサイトで問い合わせページを受け付けている Web サイトについても当該対象になりますので、Web サイトを有している企業はセキュリティを十分に考慮の上、事業運営を進めるべきであると言えます。

算出例）EC サイトを運営。“情報漏洩レベル D”に該当する個人情報を取得し、会員数 2 千人の中小企業の場合

個人情報漏えい損害想定額：**3000 万円**（＝15,000 円×2 千人）

情報漏洩レベル	企業規模別損害額/件		情報漏えい対象①				情報漏洩対象②		
	大企業・金融・情報通信・公的機関	中小企業	メールアドレス	氏名	住所	TEL	クレジットカード番号のみ	口座番号のみ	クレジットカード番号＆カード有効期限
A	¥1,000	¥500	○	－	－	－	－	－	－
B	¥3,000	¥1,500	○	○	－	－	－	－	－
C	¥6,000	¥3,000	○	○	○	○	－	－	－
D	¥30,000	¥15,000	○	○	○	○	○	－	－
E	¥30,000	¥15,000	○	○	○	○	－	○	－
F	¥150,000	¥75,000	○	○	○	○	－	－	○
G	¥30,000	¥15,000	○	○	○	○	○	○	－
H	¥150,000	¥75,000	○	○	○	○	－	○	○
※情報漏えい後の対応が適切であったものとして試算（不適切であった場合×２）									

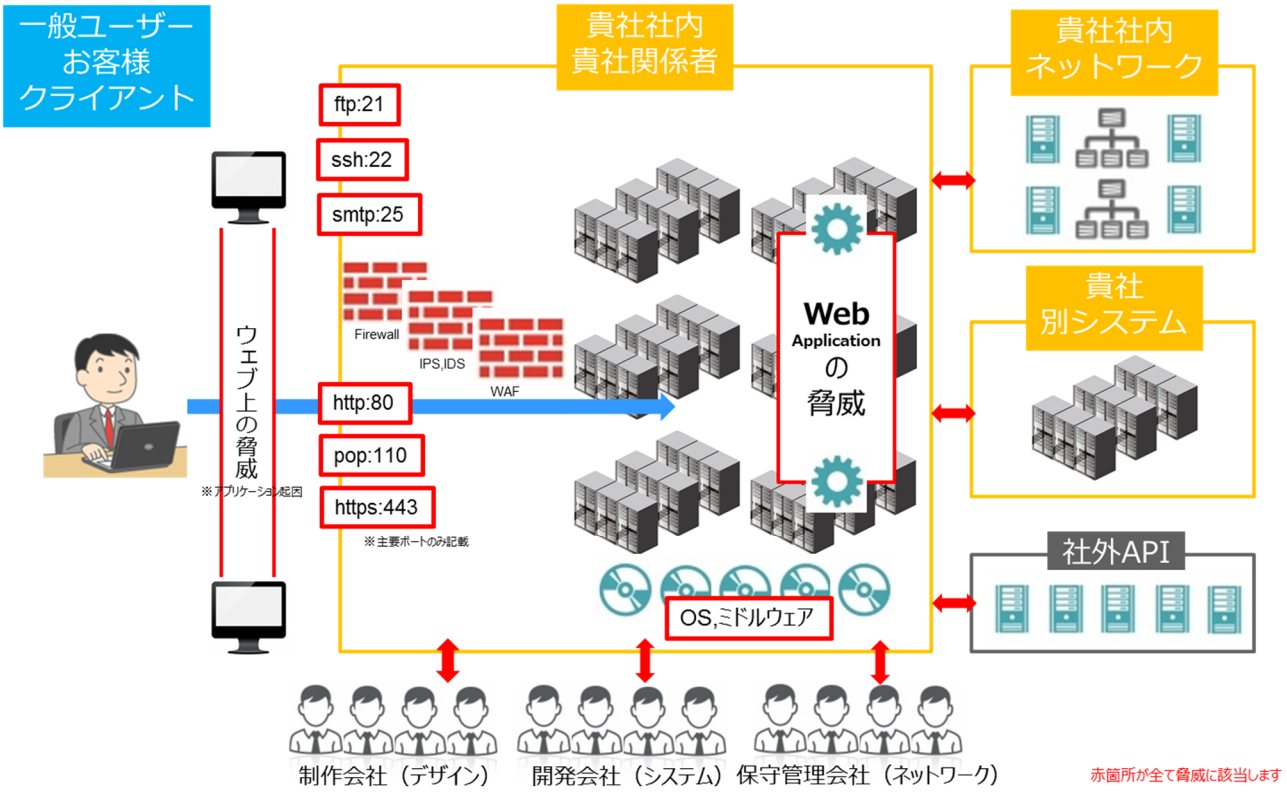
引用：ＮＰＯ日本ネットワークセキュリティ協会

2． 情報セキュリティの脅威 MAP について

次の図は Web アプリケーションにおける脅威の MAP をまとめたものです（赤箇所が脅威箇所）。当社によくある質問として Web サイト上だけの脆弱性について（主にインジェクション系、認証系）議論されることが多いのですが、Web アプリケーションの脆弱性としては多様な脅威を想定すべきであることが理解して頂けるかと思います。

セキュリティ診断をすべき Web サイト・アプリケーションの対象としては、個人情報・決済情報を扱う EC サイト、コーポレイトサイトなどはもちろんのこと、企業内の Wiki、社内スケジュール管理、企業内ポータルサイトなど限定的に利用されているサイト・アプリケーションについてもセキュリティ診断の対象として考えるべきだと言えます。2013 年からは Web サイトの改ざんのインシデントが多く発生しました。改ざんされた Web サイトを閲覧すると、FTP アカウント情報（サーバアドレス、アカウント、パスワードなど）を盗む不正プログラムに感染するなど、Web サイトそのものを乗っ取られる可能性もありますので十分に注意する必要があります。

＊Web アプリケーション脅威 MAP



3． セキュリティ診断 「エレシーク VA」 メニュー

セキュリティ診断サービス「エレシーク VA」は、柔軟なメニューをご用意しております。Web サイト・アプリケーションの提供先、および貴社のご予算を鑑みてご相談頂ければ最適なメニューをご提案させていただきます。

■セキュリティ診断メニュー

ビギナー	ライト	レギュラー	ビジネス	プロ
セキュリティ診断 試してみたい	中小企業の会社HP 制作会社様向け	Webアプリケーション Web制作会社様向け	小規模ECサイト 受託開発企業様向け	個人情報保有企業様向け ペネトレーションテスト
10,000 円	50,000 円	120,000 円	300,000 円	500,000 円から

対象のWebアプリケーション、サイトの利用者・用途(B2B,B2C他)、ご予算に応じて、最適なプランをご提案させていただきます。継続的にどのようなセキュリティ対策をするべきか含め、貴社のセキュリティのサポートをさせて頂きます。

■セキュリティ診断・詳細

全診断項目 40 の内容については、本ホワイトペーパーの診断レポートサンプルの末文に添えています

診断対象（セキュリティの脅威）	ビギナー	ライト	レギュラー	ビジネス	プロ
	1万円	5万円	12万円	30万円	50万円～
SQLインジェクション	○	○	◎	◎	◎
クロスサイトスクリプティング	○	○	◎	◎	◎
クロスサイトリクエストフォージェリ	○	○	◎	◎	◎
認証系	○	○	◎	◎	◎
承認系	○	○	◎	◎	◎
OS/ミドルウェアの脆弱性	○	◎	◎	◎	◎
マルウェアチェック	○	○	◎	◎	◎
ネットワーク	－	○	○	◎	◎
全診断項目（40項目）	－	－	○	◎	◎
診断方法①（Web側からの確認）	○	○	○	○	◎
診断方法②（ツール診断）	－	○	○	◎	◎
診断方法③（エキスパートエンジニアによる診断）	－	－	－	－	◎

■セキュリティ診断サービスご利用の流れ

4．セキュリティ診断レポートサンプル

次々ページ以降に添付しています。

セキュリティでお悩みですか！？

わたしたちへお気軽にお問い合わせください。

TEL 03-3513-7630 (受付：平日10：00～18：00) email info@cobo.jp

会社情報

＊会社名：株式会社コーボー・ホールディングス　Cobo Holdings,Inc

＊本店所在地：東京都新宿区神楽坂 2 丁目 13 番地　スエヨシビル 4 階

＊資本金：3000 万円

＊設立：2003 年 5 月 1 日

＊代表者：代表取締役社長　古城 剛

＊事業概要

情報セキュリティの診断サービス

情報セキュリティ関連ソリューション

ホスティングサービス

ネットワーク・サーバの構築・保守

Web システム開発

（次ページから診断レポートサンプル）

＜セキュリティ診断レポート・サンプル＞

ここから診断レポートのサンプルとなります。

内容については、簡易診断の内容からペネトレーションテストの内容まで含んでおります。

当該診断レポートはサンプルです。レポートサンプルに記載されている脆弱性対策内容については正確性・安全性等、あらゆる点において保証しませんので予めご了承ください

目次

診断レポートの目次です。

診断レポートは大きく総合評価、脆弱性部位の個別評価を報告させていただきます。

事前に診断対象についてのヒアリング内容です。

セキュリティ診断を安心、安全に実施するためにお客様のご要望に応じて診断方法についてヒアリングします。

1.1 診断対象

1.1.1 診断対象

以下の内容に基づきセキュリティ診断をしています。

貴社名	
貴社担当者名	
貴社担当者メールアドレス	
貴社担当者電話番号	
緊急連絡先	

1.1.2. 弊社案件担当者情報

担当者	
メールアドレス	
電話番号（緊急連絡先）	

1.1.3. 診断時連絡体制

連絡体制	□ 弊社⇔貴社 □ 弊社⇔運用ベンダー等（CC 貴社）
開始･終了連絡方法	□メール □電話 □両方
開始･終了連絡先	□１．貴社情報と同じ □１．貴社情報と異なる（備考欄に記入ください）
備考	【開始･終了連絡先】

1.1.4. 案件概要

診断対象サイト	サイト名（http://www.xxxxx.jp）
診断環境	□本番環境　　□テスト環境
サービス／診断対象範囲	□手作業：　5 遷移 □ツール診断： ※詳細は画面遷移図を参照
診断場所	□リモート　　□オンサイト
オンサイト診断場所	住所： 電話番号： 入館・持込等申請：　□あり　　□なし 備考：
診断期間	2013 年 8 月 x 日～2013 年 8 月 x 日
診断実施希望時間	平日 10 時～18 時 （標準は平日 10 時～18 時、土日祝日及び夜間等あればご記入ください。）
診断延長の可否	□可（○○時まで可）　　□否
報告書提出希望期日	2013 年 8 月 x 日（曜日） （診断終了後 5 営業日以降をご記入ください。なお、診断規模等によってはご希望に添えない場合があります。予めご了承ください。）
報告書ファイル形態	□PDF 形式　　□MSWord 形式　　□その他（別途調整となります。）
報告会（オプション）	□実施（希望回数　　回）　　■実施しない

1.1.5. 要望事項等

診断において、要望事項、診断除外事項・注意事項（過去に発生した障害事例）・禁止事項等があれば事前にご連絡をお願いします。

【要望事項】
【除外事項】
【注意事項】
【禁止事項】
【その他】

1.1.6. 事前確認事項

＜共通＞

No.	確認事項	内容	チェック
1	診断当日の対応	診断実施日にご指定の方法にて開始及び終了連絡を行います。また、診断時間中、常時、ご担当者様が待機していただく必要はございませんが、診断に関する問合せや緊急連絡が取れる体制にしていただくようお願いします。	□確認済
2	侵入検知アラート対応	本診断は、不正侵入・攻撃者の立場から、実際に用いられる攻撃手法を用いて行うため IDS/IPS/WAF 等の侵入検知・防御システムが導入されている場合には、大量のアラートが発生することがあります。診断元 IP アドレス(リモートの場合)次の IP アドレスを検知対象から除外する設定変更、または運用監視センターへのアラート無視連絡等の実施をお願いします。 203.141.134.249 203.143.124.64/28 222.151.197.64/28 219.99.141.115 210.166.226.254 121.2.74.250 210.166.226.191	□確認済 （設定・周知済み）
3	侵入防止システム対応	本診断は、不正侵入・攻撃者の立場から、実際に用いられる攻撃手法を用いて行います。 IPS/WAF 等による侵入検知・防止システムが導入されており、かつ IPS・WAF 等による一定時間特定の送信元からの通信を遮断する機能が動作した環境で診断した場合、診断項目すべてを実施できないことがあるため、IPS/WAF 等による対象から診断元 IP アドレスを除外した環境で診断することを推奨します。 なお、IPS/WAF 等が稼働した環境で診断した場合は、診断項目すべてを実施できないことがあることにご留意ください。診断可能な範囲で実施した結果のご報告となります。（制限事項）	□除外して実施 （設定変更確認） □除外せずに実施 （制限事項留意済み）
4	共有サーバ・PaaS 等の利用について	AWS、Google App Engine 等の PaaS サービスや、共有サーバ上で動作しているアプリケーションを診断対象とする場合、事前に運用業者への手続きが必要となりますので、ご確認ください。	□確認済
5	事前バックアップ	診断において、診断対象サーバ等において不測の事態が発生する可能性があります。万一の事態に備えて、事前バックアップ等の対処をお願いします。	□確認済
6	ログの容量	診断において、実際に対象システムへの通信を行うためログが書き出されます。ログを保存するディスク容量にご注意ください。 目安として、1GB 以上の空き容量がログ記録パーティションに必要です。	□確認済

No.	確認事項	内容	チェック
7	データの削除	診断時に登録したデータについては、診断終了後、必要に応じて貴社側で削除してください。弊社側では特段の対応を行いません。 例) ・ユーザアカウント ・メールマガジン登録 ・掲示板への書き込みデータ 等	□確認済
8	完了処理の実施可否及び関係部署・担当者への連絡	診断業務では、診断対象のページに繰り返しアクセスを行うため、特定のページ(例：問い合わせ、資料請求、商品購入等)において、業務担当者様に電子メールなどの通知が大量（数百件～数千件）に行われる場合があります。 該当処理が診断対象になる場合、ご担当部署・業務担当者様へ事前に通知をお願いします。 具体的な箇所、内容につきましては、画面遷移図および確認事項をご参照ください。	□可（通知済） □不可（完了処理は実施しません） □制限付き可（通知済） (条件を入力　　) □対象外
9	回数制限のある処理の診断準備	ユーザ 1 人につき 1 回のみ実行可能な機能等、処理の実行に回数制限がある処理があればお伝えください。診断時においては通常、数百～数千回の処理を行う必要があるため、在庫数の調整等のご対応をいただく必要があります。 具体的な箇所、内容につきましては、画面遷移図および確認事項をご参照ください。	□確認済
10	決済処理の形態	決済機能が対象になる場合、決済処理の形態をご提示いただく必要があります。クレジットカード決済の場合は、テスト用のクレジットカード番号をご提示いただく必要があります。 具体的な箇所、内容につきましては、画面遷移図および確認事項をご参照ください。	□代引決済 □カード決済 (テスト用カード番号) □コンビニ決済 □その他決済 (　　) □対象外

1.1.7　テストアカウント

No.	確認事項	内容	チェック
1	アカウント登録の可否	診断において、アカウント作成が必要な場合にアカウント登録の可否についてご連絡ください。	□可 □不可 □制限付き可
2	アカウントロックの有無	ログイン時におけるアカウントロックの有無についてご連絡ください。	□有 □無
3	テストアカウントの提示	テストアカウント（2 つ以上）の準備をお願いします。 特に、権限や所属により利用できる機能が異なるアプリケーションの場合は、権限ごとにアカウント（2 つ以上）の準備をお願いします。 診断においては、「一般ユーザが管理者機能を使用できるかどうか」「会社 A のユーザが会社 B の登録情報を参照できるかどうか」等、アクセス制御の範囲を超えたアクセスについて調査をおこないます。 個人利用を想定したアプリケーションにおいて、ユーザ登録が可能な場合には、診断中に弊社側で作成させていただきます。 例) ・「管理者」と「一般ユーザ」の区別がある場合、それぞれ 2 つ以上ご用意ください。 ・「会社 A」と「会社 B」のユーザが使用するアプリケーションの場合、会社毎に 2 つのユーザをご用意ください。	
4	Basic 認証等	診断対象サイトに Basic 認証等が設定されている場合は、当該認証の ID/PW をご提示ください。	□有 □無

1.2 診断方法および診断結果について

本診断は、弊社診断環境からインターネット経由で実施しました。脆弱性スキャナ・ツールを用いて、サーバ・ネットワーク機器への不正侵入に対する脆弱性の調査を行いました（対象システムの運用に対し故意に支障及び損害を与える診断（DoS 攻撃等）は実施していません）

脆弱性診断ツールは、弊社独自開発によるものでありマーケットで一般的に使用されているツールよりも非常に多くの診断パターンを有していることが強みです。ただ、診断ツールは誤検知をする場合があり当該報告書においても情報システムと診断結果を十分に照らし合わせて確認頂けます様、お願いします。

本診断は、全ての脆弱性に対する診断をするものではなく、その診断結果の内容についても、改ざんが全くないことおよびセキュリティ上の弱点が全くないことを当社が保証するものではありません。また、診断および診断結果の通知までを行うものであり、診断の結果発見された問題点について、対処方法の提示および修繕や修理手配を行うものではありません。

IT システムは時間の経過と共に脆弱性が発見・報告されます。セキュリティ対策に関する情報収集、古いバージョンの OS ミドルウェアを更新されることはもちろんのこと、定期的にセキュリティ診断・対策をされることを推奨します。

Web アプリケーションの運営を停止することなく、負荷もほとんど掛けることなくセキュリティ診断を実施することも可能です。

2．診断結果概要

2．1　　総合評価

本報告書では、診断対象の Web アプリケーションについて評価し、発見された脆弱性について結果を報告します。

セキュリティレベル 総合評価	ネットワーク経由で不正侵入やサービス停止等につながる危険度高の脆弱性が存在します。可能な限り早い段階でセキュリティ対策を実施することが望まれます。	D

2．2　　総論

診断結果の総合評価を A~E の 5 段階で実施します。

2．2．1　　CVSS による脆弱性評価

共通脆弱性評価システム（CVSS）により当該診断 Web アプリケーションの脆弱性について評価した結果です。

深刻度	脆弱性に対して想定される脅威	CVSS基本値	深刻度	該当件数
危険 （レベルIII）	・リモートからシステムを完全に制御されるような脅威 ・大部分の情報が漏えいするような脅威 ・大部分の情報が改ざんされるような脅威 ・例えば、全てのシステムが停止するようなサービス運用妨害(DoS)、OSコマンドインジェクション、SQLインジェクション、バッファオーバフローによる任意の命令実行など	7.0～10.0	9.0～10.0	2
			8.0～8.9	2
			7.0～7.9	
警告 （レベルII）	・一部の情報が漏えいするような脅威 ・一部の情報が改ざんされるような脅威 ・サービス停止に繋がるような脅威 ・例えば、ディレクトリ・トラバーサル、一部のシステムが停止するような、サービス運用妨害(DoS)など ・その他、レベルIIIに該当するが再現性が低いもの	4.0～6.9	6.0～6.9	
			5.0～5.9	1
			4.0～4.9	
注意 （レベルI）	・攻撃するために複雑な条件を必要とする脅威 ・その他、レベルIIに該当するが再現性が低いもの	0.0～3.9	3.0～3.9	
			2.0～2.9	1
			1.0～1.9	
			0.0～0.9	

個別に判定された脆弱性を CVSS の 10 段階評価にて深刻度をレポートします。10 段階のうち、さらに危険、警告、注意、3 区分の報告において危険に区分される脆弱性が判定された場合は早急な対応をお勧めします。

２．２　　総論

危険度ごとの脆弱性の検出数を見ると、不正侵入やサービス停止につながる可能性のある危険度高の脆弱性が○件検出されています。また、注意が必要な危険度中の脆弱性が 48 件、危険度低の脆弱性が○件検出されており、セキュリティ対策に改善の余地が残っています。セキュリティ侵害が発生するリスクを減らし、セキュリティレベルを向上させるためにも検出された脆弱性について対策を実施することを推奨します。
なお、危険度情報の脆弱性を 10 件検出しています。これは必ずしもセキュリティ侵害につながる脆弱性として検出しているわけではありません。本診断にて確認できた情報として検出しています。システムを現状よりセキュアな環境にするうえでの参考にしてください。

＊ソフトウェア脆弱性（危険度高～低）
ソフトウェアの脆弱性に関する危険度高～低の脆弱性が検出されています。
既知の脆弱性に対する修正の行われた新しいバージョンのソフトウェアがベンダーから公開されているもののバージョンアップが行われておらず古いバージョンのまま動作していることが原因です。
本診断では、Web サーバソフトウェア ApacheHTTPServer 及び汎用スクリプト言語 PHP のバージョンが古いため危険度高の脆弱性が検出されています。不正侵入やサービス停止等につながるため、早期にバージョンアップまたはパッチを適用することを推奨します。
特に検出された Apache の脆弱性は、「Apache Killer」と呼ばれる攻撃ツールが公開されており、遠隔の第三者によって、サービス運用妨害（DoS）攻撃を受ける可能性があります。なお、バージョンアップ及びパッチ適用ができない場合には回避策による対策を実施することを推奨します。
システムの認証および承認において Java Script を使用しているため、システムが脆弱な状態であり、XSS,XSRF を実施される脆弱性を含んでいます。継続して同システムを使用するのであれば、サーバサイドのサニタイジングをしっかりと設定し対策されることをお勧めします。
※ツール診断は JS で遷移するサイトには通常対応していません。次回からは別途費用が発生しますのでご注意ください

ソフトウェアは、今後時間の経過と共に脆弱性（セキュリティホール）が発見・報告されることは避けられません。そのため、今回検出された古いバージョンのソフトウェアをバージョンアップするとともに、今後の運用においても、日々発見される新たな脆弱性に対し定期的にセキュリティ対策が行えるように、最新のセキュリティ情報を収集し、現行のソフトウェアメンテナンスまたはセキュリティ対策の実施周期やタイミングについて検討・改善することを推奨します

全体的な総論評価を報告させていただきます。

2．3　　参考

2.3.1　総合評価基準

次の 5 段階の評価基準で総合評価をしています。

レベル	評価基準
A	脆弱性は検出されませんでした。適切なセキュリティ対策が実施されています。 脆弱性が全く検出されなかった場合に該当します。
B	危険度低の脆弱性が存在します。概ね適切なセキュリティ対策が実施されていますが、セキュリティ対策に改善の余地があります。 危険度緊急・高・中の脆弱性が一つも検出されず危険度低の脆弱性が一つ以上検出された場合に該当します。
C	場合によっては機密情報へのアクセスや、情報の改ざん等の深刻な被害を受ける可能性のある危険度中の脆弱性が存在します。セキュリティ対策を実施することが望まれます。 危険度緊急・高の脆弱性が一つも検出されず危険度中の脆弱性が一つ以上検出された場合に該当します
D	ネットワーク経由で不正侵入やサービス停止等につながる危険度高の脆弱性が存在します。可能な限り早い段階でセキュリティ対策を実施することが望まれます。 危険度緊急の脆弱性が一つも検出されず危険度高の脆弱性が一つ以上検出された場合に該当します。
E	ネットワーク経由で容易に不正侵入、サービス停止、個人情報等の機密情報漏洩に直接つながる危険度緊急の脆弱性が存在します。早急にセキュリティ対策を実施することが望まれます。 危険度緊急の脆弱性が一つ以上検出された場合に該当します。

評価における具体的な基準について当該ページを元に判定しています

2.3.2　共通脆弱性評価システム（CVSS：CommonVulnerabilityScoringSystem）

共通通脆弱性評価システム（CVSS：CommonVulnerabilityScoringSystem）は、情報システムの脆弱性を共通の指標で評価するものです。オープンで汎用的な評価手法で、特定のベンダーに依存しない共通の評価方法として、脆弱性[illegible]

CVSS は、コンピュータセキュリティの非営利団体「FIRST(Forum ofIncident Response and Security Teams)」の CVSS-SIG（SpecialInterest Group）で管理されており、現在は 2007 年 6 月に公開されたバージョン、CVSS2.0 となっています。また、CVSS は 30 を超える組織で採用されています。

（参考 URL：http://www.first.org/cvss/eadopters.html）

CVSS では、「基本評価基準（Base Metrics）」「現状評価基準（TemporalMetrics）」「環境評価基準（EnvironmentalMetrics）」の 3 段階の基準があります。

「基本評価基準（Base Metrics）」は、脆弱性そのものの特性を評価する基準であり、情報システムに求められる 3 つのセキュリティ特性、「機密性（ConfidentialityImpact）」、「完全性（IntegrityImpact）」、「可用性（AvailabilityImpact）」に対する影響を、ネットワークから攻撃可能かどうかといった基準で評価し、CVSS 基本値(Base Score)を算出します。CVSS 基本値は最小の 0.0 から最大の 10.0 で表され、脆弱性の危険度として 10.0 が最も危険な値となります。この基準による評価結果は固定しており、時間の経過や利用環境の違いによって変化しない値となります。

3． 診断結果詳細

3.1　　脆弱性拠出対象

1.1. SQL インジェクション

【危険度】

【リスク内容】

攻撃者が不正な値をクエリーパラメータに入力し、実行される SQL 文を一部改変することにより、データベースに格納されている情報の漏洩、改竄、破壊等の被害が発生する恐れがあります。

【問題のある画面】

以下のサイトで確認されました。

・申込サイト

【詳細説明】

SQL インジェクション脆弱性が検出されました。

ただし、本診断中にデータベースから具体的な値を取り出そうと試みましたが、データベース内の任意の情報を取得することはできませんでした。

管理画面サイト「ログイン処理」画面のパラメータ「user_id」は、ログイン処理時のユーザ ID を格納するために利用されていますが、このパラメータ「user_id」において SQL インジェクションの原因となる「'（シングルクオート）」を含む文字列や複数の SQL 文断片を入力したところ、次のような結果が得られました。

項番 2 において SQL エラーを起こしうる文字列「'」を入力すると正常に遷移しませんでした。
また、項番 3 より SQL 文で使用される文字列連結文「||'」が有効に機能していることがわかります。
このことから、SQL インジェクションの可能性が示唆されます。項番の比較において、条件文が、項番　より、SQL にて用意されている関数が使用可能であることがわかります。

本診断期間中にはデータベースの値の取り出しには至りませんでしたが、攻撃が成功した場合、データベース内部の情報の取り出しやデータベースの操作をされる恐れがあります。

【改善策】

データベースにアクセスする際に、アプリケーション実行環境に用意されている、「準備済み SQL 文(Prepared Statement)」を使用して、プレースホルダ方式で SQL 文を構成するようにしてください。データベースの種類や入力値の種類によらず、安全にデータベースクエリを実行することが可能となります。

脆弱性が発見された具体内容について状況、場所、対策について報告させていただきます

尚、詳細の対策についてはペネトレーションテストのメニューにおいての対応とさせていただきます。

※当該診断レポートはサンプルです。レポートサンプルに記載されている脆弱性対策内容については正確性・安全性等、あらゆる点において保証しませんので予めご了承ください

やむを得ず上記の方式が利用できない場合には、SQL インジェクション対策として、データベースクエリ実行前に以下のような処理を行う必要があります。

□ エスケープ処理の徹底
SQL 文で使用される特殊文字をエスケープ処理する必要があります。エスケープが必要な文字種に関しては、データベースサーバの種類やアプリケーション環境に依存します。

□ 入力値チェック処理の徹底
入力に不適切な文字を拒否します。例えば「値段」を入力するテキストボックスからの入力の場合には、入力値として数字以外の文字を受け付ける必要はないと考えられます。数字以外の文字が入力された場合には、エラー処理を行うようにアプリケーションを修正します。数字に限らず、入力文字種や文字列の長さが制限できる場合には、指定した制限規則外の文字列を受け付けないようにします。

1.2. クロスサイトスクリプティング
【危険度】
【リスク内容】
正規ユーザのログイン情報を格納した Cookie を不正に入手される場合があります。その結果、ユーザのなりすましが行われる恐れがあります。
また、任意の HTML タグを挿入することにより、Web ページの見た目上の改ざんがおこなわれ、不正な広告の表示やフィッシング詐欺の手段として悪用されてしまう恐れがあります。

【問題のある画面】
以下のサイトで確認されました。
・管理サイト
・申込サイト
・決済サイト
該当 URL およびパラメータは別添のツール診断検出結果一覧をご覧ください。

【詳細説明】
別紙のツール診断検出結果一覧速報に示した各画面に遷移する際に、入力パラメータの値として、HTML タグを含む文字列を入力すると、入力した HTML タグがそのまま有効な状態で画面表示されました。<script>タグを挿入することで任意のスクリプトの実行が可能です。また、偽物の画面をユーザの Web ブラウザ上に表示させることも可能であり、フィッシング詐欺の手段として悪用される恐れもあります。

決済サイトの「決済処理」画面において、パラメータ「user_tel」に対し
「"><script>alert('XSS')</script>」と入力した結果を示しています。スクリプトが実行されている様子がわかります。
また、管理画面サイトの「決済状況検索結果表示」画面において、パラメータ「order_number」では、入力された<script>タグ等は全角変換等がされますが、「'(シングルクォート)」が、エスケープされていないため、次のような入力をすることにより、出力先の HTML タグに属性値の追加が可能となり、スクリプトを実行させることが可能です

【改善策】
一般に、アプリケーションに入力される値には、悪意のあるデータが含まれることも想定し、エスケープ処理や入力値チェックを漏れなく行う必要があります。クロスサイトスクリプティングについては、以下の様な点に注目して対策を行う必要があります。

□ エスケープ処理の徹底
入力された文字列を出力に反映させる場合には、適切なエスケープ処理を行う必要があります。HTML の本体部分に出力する場合には、「&」「<」「>」「"」「'」をそれぞれ「&」「<」「>」「"」「'」に変換します。
他にも、URL として出力する場合や JavaScript 内部に出力する場合等、出力される場所に応じて適切なエスケープ処理を行う必要があります。
□ 入力値チェックの徹底
入力として不適切な文字を拒否します。例えば「値段」を入力するテキストボックスからの入力の場合には、入力値として数字以外の文字を受け付ける必要はないと考えられます。数字以外の文字が入力された場合には、エラー処理を行うようにアプリケーションを修正します。数字に限らず、入力文字種や文字列の長さが制限できる場合には、指定した制限規則外の文字列を受け付けないようにすることで Web アプリケーションの安全性が高まります。
□ HTML の書き方の注意
タグ属性値は必ず「"」か「'」で囲むようにします。例えば、入力値として「abcde.jpg」が入力された場合には、以下のようになります。
危険な例) <img src=abcde.jpg>
安全な例) <img src="abcde.jpg">
属性値を「"」か「'」で囲むことを怠ると、onError や onMouseOver などのイベントハンドラを用いたスクリプトの実行が可能となる場合があります。

４.留意事項

本報告書は診断実施時点における脆弱性情報や攻撃手法により得られた結果を述べたものであることをご理解ください。新しい脆弱性や攻撃手法は日々発見されており、診断実施時点では問題点が存在しなかった対象においても、将来において新たな脆弱性が報告される可能性があります。新たな脆弱性や攻撃手法の発見に伴い、セキュリティレベルは時間の経過とともに低下します。本診断を実施した結果「問題なし（安全）」の評価が出たとしても、その評価結果は診断実施以降、攻撃を受けない、もしくは攻撃を受けたとしても何らの問題も生じないということを保証するものではありませんので、予めご了承ください。

ネットワーク経由における検出可能な脆弱性は、ネットワーク経由での攻撃や不正アクセスが可能であるものに限られます。また、脆弱性はサーバから取得したバージョン情報に基づいて報告される場合があります。バージョン情報以外の手法により脆弱性の有無が確認できる場合は、脆弱性の有無の確認を行いますが、バージョン情報以外に脆弱性を検証する手法が存在しない場合もあります。サーバによっては、パッチが適用されているにもかかわらずバージョン番号が変化しないものもあるため、パッチが適用されている場合でも脆弱性が検出されることがあります。

本報告書において記述されている脆弱性危険度の評価や検出された脆弱性によるリスク内容は、運用の方針（セキュリティポリシーなど）・環境・状況等により変化いたします。ただし本報告書では、セキュリティ診断の性質上、運用の方針（セキュリティポリシーなど）・環境・状況等は考慮せずに診断対象機器単体の視点から脆弱性危険度の評価やリスク内容を記載しておりますことをご理解ください。そのため、脆弱性への対応につきましては、運用の方針（セキュリティポリシーなど）・環境・状況等を考慮していただき対応策を検討してください。

本報告書に記述されている問題点の対策方法は、独立行政法人情報処理推進機構（IPA）やソフトウェアベンダーにより推奨されているものなど一般的なものです。環境によっては、対策を実施することによりアプリケーションの依存関係等に不[illegible]実施してください。

セキュリティを担保するためには非常に多くの要素が存在するため、予算と担保すべき脆弱性の見極めを進めた上で”定期的”に実施されることをお勧めします。

セキュリティレベルを維持するためには、使用している機器・ソフトウェアのベンダーから提供されるセキュリティ情報を収集し、適宜[illegible]ともに、定期的にセキュリティ診断を行うことが必要です。

次のページからは、セキュリティ診断で実施する脆弱性の項目一覧です。お客様の状況に合わせて実施する脆弱性診断対象を決定させていただきます。

5．参考

5.1　診断項目

次の診断項目の中で当該診断レポートは、38、40 を除く全ての診断を実施しています。

■クライアント側での攻撃 Client-side Attacks
攻撃手法として最も多いとされているクロスサイトスクリプティング(XSS)など、クライアント側から行われる攻撃に対する診断を行います。

No.	診断内容	脆弱性が存在することによって被る被害
1	クロス・サイト・スクリプティング	サイトをまたがって不正な要求を送り、ユーザが意図していないスクリプトを実行させられてしまいます。その結果、例えば偽ページを表示することが可能になり、フィッシング詐欺などに悪用されてしまいます。
2	クロス・サイト・リクエスト・フォージェリ	サイトをまたがって不正な要求を送り、ユーザが意図していない操作を実行させられてしまいます。例えば、ユーザが意図しないままオンラインショップで買い物をさせられたりしてしまいます。
3	クロス・サイト・トレーシング	ウェブのヘッダ情報を不正に読み出されてしまいます。これにより、他の脆弱性を利用して管理者や他のユーザに成りすまされてしまいます。
4	コンテンツの詐称	偽のコンテンツをあたかも正式なものであるかのように装ってウェブサイトに表示し、ユーザを欺きます。これにより、パスワードを抜き取られたり、フィッシング詐欺サイトへ誘導されたりする危険性があります。
5	セキュアでない cookie の使用	セッション・クッキーが類推可能な簡単なものであったり、セキュアでない通信経路で送られた過程で盗まれたりすると、セッション自体が盗まれる可能性があります。これにより、個人情報が盗まれたり、コンピュータに侵入されたりする危険性があります。
6	hidden フィールドの不正操作	Hidden フィールドを不正に改ざんされてしまう可能性があります。例えば商品の価格などを Hidden で受渡ししている場合に、価格を任意に変更されてしまうなどの可能性があります。

■コマンドの実行 Command Execution
攻撃手法としても多い SQL インジェクションなど、DB サーバへのアクセスを不正に実行できるかどうかを診断します。脆弱性有りとなると、ウェブサイトからの情報漏えい、改ざん等の危険性があります。

No.	診断内容	脆弱性が存在することによって被る被害

7	SQL インジェクション	DB サーバへのアクセスを不正に実行されてしまいます。これにより、ウェブサイトからの情報漏えい、改ざん等の危険性があります。
8	SSI インジェクション	SSI コマンドを不正に実行されてしまいます。これにより、ウェブサイトからの情報漏えい、改ざん等の危険性があります。
9	メールヘッダインジェクション	問い合わせフォームなどのメールを送信する画面で、メールの内容を改ざんし、迷惑メールの送信などに悪用されてしまう可能性があります。
10	HTTP ヘッダインジェクション	動的に HTTP ヘッダを生成する機能の不備を突いてヘッダ行を挿入することで不正な動作が発生し、セッションハイジャック、XSS 等につながる可能性がある攻撃。
11	XML インジェクション	XML データにスクリプト等を混入して攻撃されてしまいます。これにより、ウェブサイトからの情報漏えい、改ざん等の危険性があります。
12	LDAP インジェクション	LDAP コマンドを不正に使用されてしまいます。これにより、ウェブサイトからの情報漏えい、改ざん等の危険性があります。
13	コマンドインジェクション	サーバ内の OS のコマンドを不正に実行されてしまいます。これにより、ウェブサイトからの情報漏えい、改ざん等の危険性があります。
14	バッファ・オーバフロー	アプリケーションの予期しないデータを送り、アプリケーションを異常終了させられてしまいます。これにより、ウェブサーバのサービスが停止する、ウェブサーバを乗っ取られる危険性があります。
15	ディクショナリアタック	入力された文字列を書式加工する際にプログラムをクラッシュする、また不正なコードを実行させられてしまいます。これにより、ウェブサーバのサービスを停止させられる、ウェブサーバを乗っ取られる危険性があります。
16	パラメータ改ざん	パラメータを不正に改ざんされてしまいます。その結果、管理者や他のユーザに成りすまされてしまいます。
17	スクリプトの実行	許可していないスクリプトを実行されてしまうため、情報の漏えいやウェブサイトの改ざんを許してしまいます。

■情報漏洩 Information Leakage

本来外部から見ることができない情報が閲覧できる状態かどうか脆弱性の有無を診断します。

ウェブサーバから情報が漏えいすると攻撃の糸口になる、また場合によってはサイトそのものを搾取される可能性があります。

No.	診断内容	脆弱性が存在することによって被る被害
18	ディレクトリ・トラバーサル	ウェブサーバ内のファイルを閲覧されることにより、ウェブサーバ攻撃の足がかりとされてしまいます。
19	情報漏洩	ウェブサーバから意図していない内部情報が外部に漏えいしてしまいます。
20	不適切なコメント記載	HTML や可読可能なスクリプトファイルへの不適切なコメントが記載されており、外部から侵入のきっかけを与えています。
21	パスフレーズジャック	ウェブブラウザのアドレスバーやファイル名を指定するパラメータなどの箇所から任意のパスを受け付けてしまうため、機密情報などが保管されているパスを指定されることにより情報漏えいにつながります。
22	推測可能なリソースの位置	フォルダ名やファイル名が推測可能な簡単な名称になっているなど、内部のリソースの配置が推測可能な場合、重要な情報や機能が外部に漏えいする危険性があります。
23	ウェブサーバ・アプリケーションの特定	ウェブサーバ、ウェブアプリケーションの種類やバージョン情報から脆弱性が探り出され、攻撃の足がかりとされてしまいます。
24	ディレクトリ・リスティング	サーバ内のディレクトリ情報が外部から閲覧できる状態になっています。機密情報が含まれている場合は直接問題となり、内部のディレクトリの推測等に使用されるなどの間接的な脆弱性にも繋がります。
25	リクエストヘッダによる情報漏洩	リクエストヘッダにシステムの内部情報が外部から閲覧できる状態になっています。

■認証 Authentication

認証を使用しているウェブサイトで適切に認証がされているか診断を行います。成りすましや情報漏洩の危険性があります。

No.	診断内容	脆弱性が存在することによって被る被害

26	総当たり攻撃	ID やパスワードが簡単に推測可能であり、管理者や他のユーザに成りすまされてしまいます。
27	認証関連が不適切	サーバのセッション管理等により正常なログイン処理を介さずにログイン後の画面にアクセスされてしまうため、成りすましや情報漏えいの危険性があります。（セッションジャック等）
28	パスワード復元が不適切	ユーザがパスワードを忘れた際の回復方法に問題があり、パスワードの情報が外部に漏えいしてしまいます。

■承認 Authorization

認証後のセッション管理に適切か診断を行います。

推測しやすい場合などは、アカウントの乗っ取りが可能となり様々な攻撃の糸口として利用される危険な箇所です。

No.	診断内容	脆弱性が存在することによって被る被害
29	セッションの推測	セッション情報が推測しやすい値の場合、攻撃者は正しい値を推測し、管理者やユーザに成りすますことができます。
30	承認が不適切	承認が不適切だと、アクセス権限の高いコンテンツや機能へのアクセスを認めてしまいます。これにより、攻撃者が他のユーザや管理者に成りすます危険性があります。
31	セッション期限が不適切	セッション期限が不適切である場合、ユーザのセッション情報を盗用しやすくなり、攻撃者が管理者やユーザに成りすますことができます。
32	セッションの固定	攻撃者が任意のセッション情報を使って管理者やユーザに成りすますことができます。
33	セッションの盗難	SSL 等を使用して暗号化をしていない場合、攻撃者はセッション情報を容易に取得することができ、管理者やユーザに成りすますことができます。

■ロジックを狙った攻撃 Logical Attacks

ウェブサーバやウェブアプリケーションの持つ機能を狙った攻撃が可能か診断を行います。

有名な Dos 攻撃等が該当し、サイト・サービスの継続が難しくなるだけではなくサイトの乗っ取り、情報漏洩などに繋がる危険性があります。

No.	診断内容	脆弱性が存在することによって被る被害
34	機能の悪用	ウェブサーバ、ウェブアプリケーションの持つ機能を不正に実行されてしまいます。その結果、SPAM（メールを大量配信すること）の中継地点に使われるなど、悪用されてしまいます。
35	サービス拒否	ウェブサーバのサービスを停止、もしくは低下させられてしまいます。（Dos 攻撃）

36	自動化の停止が不適切	ロボットなどによるウェブサーバへの連続攻撃を受け、正しい ID やパスワードを探られたり、ウェブサーバに負荷をかけられたりしてしまいます。
37	不適切なプロセス検証	正常な画面遷移を無視して特定の画面にアクセスされてしまうため、成りすましや情報漏えいの危険性があります。

■異常検出 outlier detection

診断パターンを大量にテストすることによりセキュリティ対策ツールの設定の抜けを確認します。

また、既に攻撃者に侵入されている場合などの異常について検知します。

No.	診断内容	脆弱性が存在することによって被る被害
38	サードパーティ製品の設定ミス	IPS,IDS,WAF の導入を行なっても、設定が十分ではなく内包している脆弱性を防げていないことがあります。
39	バックドア、デバッグオプション	既に侵入されバックドアを仕掛けられている危険な状態です。
40	マルウェアの検知	マルウェアの検知を行い、マルウェアの種類やリンク先とリンク数を表示する。

5．2　　JVN 脆弱性情報について、CVE について

本報告書では、脆弱性情報データベースである JVN、および CVE の情報を参考情報として引用しています。JVN は、日本で使用されているソフトウェアなどの脆弱性関連情報とその対策情報を提供しています。

本診断で発見された脆弱性は JVN、CVE の情報についても十分に確認しながらセキュリティ対策を進めてください。

※JVN は、JPCERT コーディネーションセンターと独立行政法人情報処理推進機構 (IPA)が共同で運営しています。

※共通脆弱性識別子 CVE(Common Vulnerabilities and Exposures)は、個別製品中の脆弱性を対象として、米国政府の支援を受けた非営利団体の MITRE 社採番している識別子です。脆弱性検査ツールや脆弱性対策情報提供サービスの多くが CVE を利用しています。

※CVSS：IPA 引用 http://www.ipa.go.jp/security/vuln/CVSS.html