Confidential

株式会社サンプル御中
△△システム
セキュリティ診断レポート

株式会社M&K
セキュリティ事業部

承認者	作成者

contents

はじめに

株式会社M&K (以下「弊社」)は、株式会社サンプル 様（以下「貴社」）との契約に基づきセキュリティ診断（以下「本サービス」）を実施いたしました。本サービスは、下記により構成されています。

- Web アプリケーション診断

本サービスは、対象システムにおいて調査時点に存在するセキュリティ上の脆弱性を検出し、推奨される対策案をご提示することを目的としております。悪意ある第三者の視点で、内部の構造や仕組みに関する情報を一切持たず、入出力のみに着目して結果を分析する「ブラックボックステスト」と呼ばれる手法により、対象システムに影響を及ぼす恐れのある脅威および関連するリスクの顕在化を行います。本サービスの最大の特徴は、高い網羅性を有するツールによる診断と、知識・経験豊かな弊社セキュリティプロフェッショナルによる高精度な手動診断を実施することで、より完全かつ正確な診断結果を導き出すことにあります。

本サービスを実施することで、主に次のような効果が期待できます。

- 「プロアクティブ」なセキュリティ対策が可能
  システムに存在する弱点を事前に検出、修正することで、万が一攻撃を受けた場合にも影響を受けない強固なシステムを実現できます※1。

- 「コンプライアンス」を実現するための情報として活用可能
  企業のセキュリティポリシーや業界のセキュリティ基準に遵守していないシステムを特定できるため、コンプライアンス向上の一助となります。

注意事項

本報告書には情報システムセキュリティに関する重要な情報が含まれております。お取り扱いには十分ご注意ください。なお、本報告書の内容は指定の診断期間における弊社調査方法に基づいた結果を示すものであり、将来的なセキュリティを保証するものではございませんのでご了承ください。

診断手法について

本サービスにおいては、サーバに対する DoS (Denial of Service:サービス不能) 攻撃やデータベースのデータ変更を伴う SQL (UPDATE や DELETE など)の実行といった、Web アプリケーションの可用性およびデータの完全性を損なう危険性のある診断は実施いたしておりません。

診断情報について

本サービスを実施する上で、貴社よりご提供頂いたデータ、ドキュメント等は適切に破棄いたします。

※1 継続的な脆弱性診断を実施している場合。

1. 診断概要

1.1 診断情報

診断対象URL	http://www.×××.co.jp/
診断対象IP	○○○.○○○.○○○.○○○

1.2 診断期間

診断期間　2012/6/1　～　2012/7/1

1.3 診断環境

診断場所	弊社診断ルーム
診断元IP	○○○.○○○.○○○.○○○

1.4 診断担当者

診断担当者	○○××○○××

2. 総評

本診断の結果、外部から攻撃を受ける可能性のある重大な脆弱性が複数発見されました。発見された脆弱性を悪用することにより、任意のプログラムの実行、機密情報や個人情報の漏洩、改竄、なりすましによる不正操作、DoS 攻撃、システム停止等、重大な損害を受ける可能性があります。

以下、主だった点を挙げさせていただきます。

- クロスサイトスクリプティングに対する脆弱性
  入力データの検証処理に不備があり、未検証のデータをそのまま Web ブラウザに送信しているため、任意のプログラムの実行が可能です。外部からのデータに対しての検証処理を徹底すると同時に、入力内容をブラウザに出力する際には、画面出力の直前に特殊文字を無効化することが推奨されます。

- SQL インジェクションに対する脆弱性
  外部から取得した値に対する適切な検証処理が行われていないため、攻撃者がパラメータに不正な文字列を挿入して、実行される SQL 文の内容を変更し、任意のコマンドを実行できる可能性があります。結果として、情報漏洩、データの改竄、DoS 攻撃、および最悪の場合にはシステム停止等の影響が発生する恐れがあります。対策として、シングルクォート(') は確実にエスケープ処理を行うことが推奨されます。バインドメカニズムを使用することで、適切なエスケープ処理が行われるだけでなく、SQL 実行時の速度改善も見込まれます。

結論として、上記、早急な対策を要する項目の修正およびアプリケーションの品質面に対する改修を実施することを推奨いたします。後述します問題点の対策は、ソースコードレベルおよび Web アプリケーションレベル双方の修正が必要です。対策はシステムの運用に影響を及ぼす可能性があるため、対応に際してはシステム管理責任者による検討が必要と考えられます。

3. 調査項目概要

3.1 Web アプリケーション診断

調査項目		具体例	指摘項目
認証			
	総当たり攻撃に関する調査	アカウントロックアウト機能が実装されているか	
	ログインフォームに関する調査	パスワードフィールドがマスクされているか	
	ログイン情報の送受信に関する調査	ログインID、パスワードが平文で送受信されていないか	
セッション管理			
	Cookieの取り扱いに関する調査	secure属性をつけたCookieを利用しているか	
		有効期限の長いCookieを使用していないか	
	セッションIDに関する調査	セッションハイジャック対策が実装されているか	
		推測の容易な文字列をセッションIDに利用していないか	
		セッションIDをユーザ側で指定可能になっていないか	
	クロスサイトリクエストフォージェリ	ユーザに特定の操作を強制することが出来ないか	
入出力処理			
	クロスサイトスクリプティング	Webアプリケーションの各パラメータにおいて、タグ文字列の入力が受け付けられない	✔
	SQLインジェクション	Webアプリケーションの各パラメータにおいて、SQL文字列の入力が受け付けられな	✔
	コマンドインジェクション	Webアプリケーションの各パラメータにおいて、コマンド文字列が受け付けられないか	
	ディレクトリトラバーサル	Webアプリケーションの各パラメータにおいて、パス区切り文字列が受け付けられない	
	ファイルアップロード	想定外のファイル形式でアップロードできないか	
	パラメータ推測	Webアプリケーションの各パラメータに、推測できるものがないか	
一般的な脆弱性			
	ログイン、操作等の履歴に関する調査	ログインおよび、重要情報の変更処理について適切に履歴管理を起こっているか	
	既知のソフトウェア脆弱性	脆弱性を持ったWebアプリケーションソフトウェアがないか	
	キャッシュ制御	重要情報が含まれるページがキャッシュされないようになっているか	
	強制ブラウジング	推測が容易な名前のディレクトリ、ファイルがないか	
		システム管理ツールのWebインターフェイスがないか	
	ディレクトリリスティング	ファイル一覧が閲覧可能なディレクトリがないか	✔
	メール送信	メールの件名や本文が改竄されないようになっているか	
パスワード管理			
	パスワード登録の制限	ユーザIDと同じパスワードを許容していないか	
	世代管理	直近数回のパスワード変更時と同じパスワードを許容していないか	
	パスワード強度	単一文字種や短いパスワードが使用可能か	
Webサーバ設定			
	システム情報の開示	レスポンスヘッダ、エラーメッセージなどからシステム情報が得られないか	✔
	サーバエラーメッセージ	デフォルトのサーバエラーメッセージが表示されないか	

3.2 ネットワーク診断

調査項目	具体例	指摘項目
認証		
総当たり攻撃に関する調査	アカウントロックアウト機能が実装されているか	
ログインフォームに関する調査	パスワードフィールドがマスクされているか	
ログイン情報の送受信に関する調査	ログインID、パスワードが平文で送受信されていないか	
ホストのスキャン		
TCP,UDP,ICMPでのポートスキャン	TCP全ポートに対するポートスキャンにより、ホストの応答を確認	
実行中のサービスの検出	応答の得られたポートに接続を試み、動作しているサービスを特定	
ネットワークサービスの脆弱性		
DNSに関する調査	DNSRecursiveによる脆弱性	
メールサーバに関する調査	メールサーバでの第三者中継の許可	
FTPに関する調査	WS FTP Server のバッファオーバーフロー脆弱性	
RPCに関する調査	RPC portmapperに存在する脆弱性	
ファイル共有に関する調査	Windows デフォルト共有リソースへのアクセス可否	
SNMPに関する調査	SNMPによるシステム情報の取得	
SSHサーバに関する調査	OpenSSH4.1以前に存在するバッファオーバーフロー脆弱性	
データベースサーバに関する調査	Oracle tnsリスナによるシステムデータベースへの接続	
その他サービスに関する調査	squid proxyサーバ 2.5.4以前に存在するサービス妨害脆弱性	
Webサーバの脆弱性		
Webサーバの脆弱性	Apache 1.3.26以前に存在するバッファオーバーフロー脆弱性	
Webアプリケーションサーバの脆弱性	Apache Tomcat 4.0.6以前に存在するサービス妨害脆弱性	
許可されているHTTPメソッド	推奨されないHTTPメソッドが許可されていないか	
暗号化方式に関する調査	脆弱な暗号化方式が許容されていないか	✔
各種OSの脆弱性		
Windowsの既知の脆弱性	Windows Printerサービスに存在するバッファオーバーフロー脆弱性	
Solarisの既知の脆弱性	Solaris telnetdに存在する認証回避の脆弱性	
各種Linuxディストリビューションの既知の脆弱性	Linuxカーネルに存在するTCP/IP処理の脆弱性	
その他各種OSの既知の脆弱性	AIX FTPDに存在するバッファオーバーフロー脆弱性	
悪意あるソフトウェア		
バックドアの調査	バックドアの可能性が高い、非標準ポートで動作しているメールサービスを確認	
P2Pソフトウェアの調査	WinMX P2Pソフトウェアが動作していないか確認	
ネットワーク機器の脆弱性		
各種ルータ機器の既知の脆弱性	Cisco IOS デフォルト管理画面へのアクセス確認	
各種ファイアウォール機器の既知の脆弱性	Checkpoint Firewall-1の管理ポートへのアクセス	
その他各種ネットワーク機器の既知の脆弱性	アライドテレシス社のネットワーク機器のデフォルトパスワード	
その他		
その他ホスト全体の調査	サービスによる内部IPアドレスの表示	
通常実施しない調査		
DoS(サービス妨害攻撃)の実施	ホストに対する、不正なパケット送信によるOSの停止確認	－
BruteForce(総当り攻撃)の実施	管理者アカウントによる、多数のパスワードでの接続試験	－

4. 診断結果一覧

No	指摘項目	レベル	ページ
Web アプリケーション			
W.1	クロスサイトスクリプティング	4:重大	7
W.2	SQL インジェクション	4:重大	9
W.3	総当たり攻撃対策の欠如	3:高	10
W.4	ディレクトリリスティング	1:低	13
W.5	参考情報および推奨事項	情報	15
ネットワーク			
N.1	脆弱な暗号化方式の許容	1:低	18

5. 診断対象別脆弱性詳細

5.1 Web アプリケーション診断による結果

W.1　クロスサイトスクリプティング

4　重大

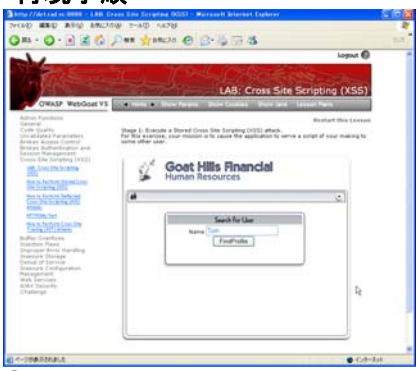
■ CVSS2.0

評価値: 4.0	注意 (0.0～3.9)	警告 (4.0～6.9)	危険 (7.0～10.0)
AV :攻撃元区分	ローカル	隣接	**ネットワーク**
AC :攻撃条件の複雑さ	高	中	**低**
Au :攻撃前の認証要否	複数	**単一**	不要
C :機密性への影響	**なし**	部分的	全面的
I :完全性への影響	**なし**	部分的	全面的
A :可用性への影響	なし	**部分的**	全面的

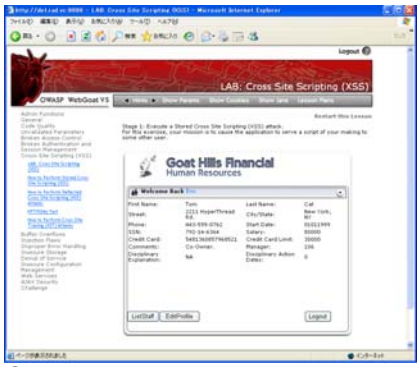
■ 現象

複数個所において、JavaScript を挿入することにより任意のプログラムを実行することが可能です。

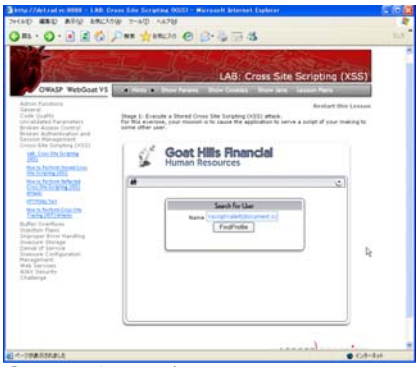
■ 再現手順



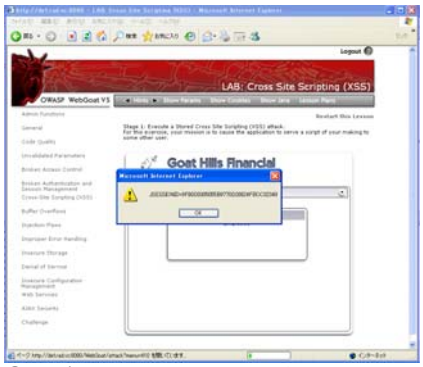
① http://example.co.jp/WebGoat/attack?menu=410 (search staff 画面)へアクセスします。



② last name 入力欄に「<script>alert(document.cookie)</script>」を入力します。



③ Go ボタンを押下します。



④ 挿入した JavaScript が作動します。

■この脆弱性によるリスク

この脆弱性を悪用して、システムおよび利用ユーザに被害が発生することが懸念されます。悪用例としては以下のことが考えられます。

- セッションハイジャックによる機密情報、個人情報の漏洩
- ユーザが意図しない情報の送信
- 悪質なページへの誘導
- 表示ページの改竄

また、モバイル環境を対象としたサイトなど、JavaScript が実行される可能性が低いサイトであっても、HTMLを直接書き換えることで、ページの改竄、悪質なページへの誘導といった攻撃に利用される可能性があります。

■対策方法

この脆弱性に対応するには、Web アプリケーションにおいて出力部分に応じた文字列の適切なエスケープ/エンコード処理を行うことが必要です。また、Web アプリケーション開発時に以下を原則とすることで、クロスサイトスクリプティングを含め、多くの脆弱性による影響を大幅に緩和することが可能です。

- 入力値の形式や文字種別、桁数を厳密に定義し、正しい入力値のみを受け付けるように処理する。
  例：電話番号の値には10-12 桁の半角数字のみを許可等
- JavaScript 等を使用したクライアント側での入出力チェックに依存せず、サーバ側で入出力チェックを行う。

なお、クロスサイトスクリプティングの原因は文字列処理が適切にされていないことに起因するため、本指摘事項以外にも、文字列処理を行う全ての部分に注意する必要があります。そのため指摘部分への対策だけではなく、アプリケーション全体の確認と対策を推奨します。

上記に加えて見落としや文字列処理の漏れを防止するため、以下のような対策が望まれます。

- アプリケーションの出力に応じ、エスケープやエンコード処理を行う関数・ライブラリ・クラスを整備して使用する。
- Web アプリケーションフレームワークを使用し、文字列処理やデータベースアクセスなどの重要な処理を一元化する。

また、システムの仕様上HTMLタグの入力を許可する場合は、全てのタグを許可するのではなく、必要最低限のタグのみを許可してください。

許可すべきではない要素例

- スクリプトタグ
- フレーム関連タグ
- イベントハンドラ

W.2　SQL インジェクション

4　重大

■ CVSS2.0

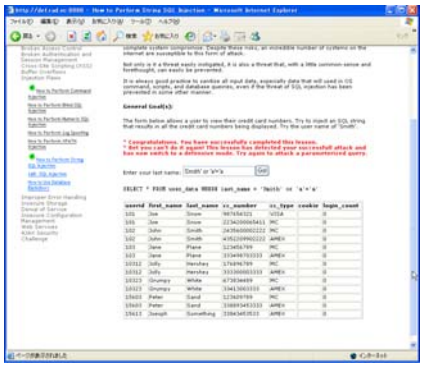
評価値: 5.0	注意 (0.0～3.9)	警告 (4.0～6.9)	危険 (7.0～10.0)
AV :攻撃元区分	ローカル	隣接	**ネットワーク**
AC :攻撃条件の複雑さ	高	中	**低**
Au :攻撃前の認証要否	複数	単一	**不要**
C :機密性への影響	なし	**部分的**	全面的
I :完全性への影響	**なし**	部分的	全面的
A :可用性への影響	**なし**	部分的	全面的

■ **現象**

外部の入力の値がそのまま SQL クエリに使用されています。

■ **再現手順**

手順 1


手順 2

■ **この脆弱性によるリスク**

外部から受け渡される値を変更することにより、本来の条件とは違う条件でデータの取得ができます。想定しない値の表示や、データの更新・削除が可能になっています。

■ **対策方法**

外部から入力される値に対しては、確実にエスケープ処理を行って下さい。

W.3　総当たり攻撃対策の欠如

3	高

■ **CVSS2.0**

評価値: 5.0	注意 (0.0～3.9)	警告 (4.0～6.9)	危険 (7.0～10.0)
AV :攻撃元区分	ローカル	隣接	**ネットワーク**
AC :攻撃条件の複雑さ	高	中	**低**
Au :攻撃前の認証要否	複数	単一	**不要**
C :機密性への影響	なし	**部分的**	全面的
I :完全性への影響	**なし**	部分的	全面的
A :可用性への影響	**なし**	部分的	全面的

■ **現象**

総当り攻撃対策に関して、以下の脆弱性が検出されております。

W.3.1　アカウントロックアウト機能の欠如
W.3.2　脆弱なパスワードの許容

W.3.1　アカウントロックアウト機能の欠如

■ CVSS2.0

評価値: 5.0	注意 (0.0～3.9)	警告 (4.0～6.9)	危険 (7.0～10.0)
AV :攻撃元区分	ローカル	隣接	**ネットワーク**
AC :攻撃条件の複雑さ	高	中	**低**
Au :攻撃前の認証要否	複数	単一	**不要**
C :機密性への影響	なし	**部分的**	全面的
I :完全性への影響	**なし**	部分的	全面的
A :可用性への影響	**なし**	部分的	全面的

■ 現象

ログイン画面において、総当り攻撃を防止する機能が存在しません。

■ この脆弱性によるリスク

総当り攻撃によりアカウント情報が特定される可能性があります。

■ 対策方法

サーバでログイン連続失敗回数をカウントし、失敗回数が閾値を超えた場合にその会員のアカウントをロックアウトします。

ロックアウトを解除する方法例は、以下のとおりです。

- 一定時間経過後に自動的に解除します。
- ヘルプデスクに電話、またはメールにて連絡し管理者が手動で解除します。

W.3.2　脆弱なパスワードの許容

■ CVSS2.0

評価値: 5.0	注意 (0.0～3.9)	警告 (4.0～6.9)	危険 (7.0～10.0)
AV：攻撃元区分	ローカル	隣接	**ネットワーク**
AC：攻撃条件の複雑さ	高	中	**低**
Au：攻撃前の認証要否	複数	単一	**不要**
C：機密性への影響	なし	**部分的**	全面的
I：完全性への影響	**なし**	部分的	全面的
A：可用性への影響	**なし**	部分的	全面的

■ 現象

セキュリティ上推奨されないパスワードが許容されています。

設定	現状	推奨
最小文字数	6文字	8文字以上
最小構成文字種	2種類	3種類以上
ユーザIDと同様のパスワード登録	一部許容※	許容しない
パスワード変更履歴管理	なし	あり

※ ユーザ ID として使用しているメールアドレスのアカウント（sample@example.co.jp の場合の「sample」部分）と同一のパスワードを許容しています。

■ この脆弱性によるリスク

脆弱なパスワードが使用されている場合、パスワードが推測されてアカウントが奪われる可能性が高くなります。

また本システムでは「W.3.1 アカウントロックアウト機能の欠如」も検出されているため、パスワード特定が可能です。

■ 対策方法

パスワードに要求する複雑さのレベルを上げて、脆弱なパスワードが設定されることを防いでください。

W.4 ディレクトリリスティング

1 低

■ CVSS 2.0

評価値: 5.0	注意 (0.0～3.9)	警告 (4.0～6.9)	危険 (7.0～10.0)
AV :攻撃元区分	ローカル	隣接	**ネットワーク**
AC :攻撃条件の複雑さ	高	中	**低**
Au :攻撃前の認証要否	複数	単一	**不要**
C :機密性への影響	なし	**部分的**	全面的
I :完全性への影響	**なし**	部分的	全面的
A :可用性への影響	**なし**	部分的	全面的

■ 現象

ファイルの一覧が取得できるディレクトリが複数存在します。

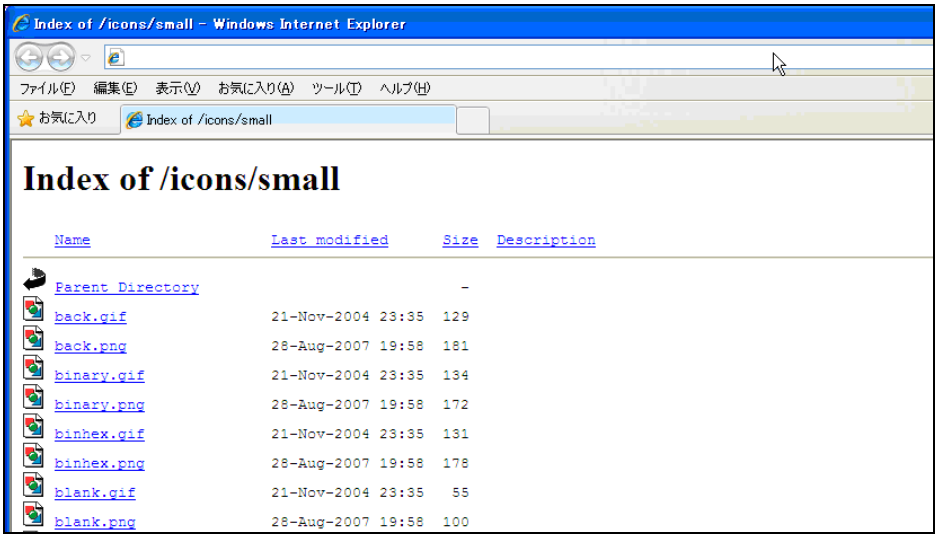


図 1 ディレクトリリスティング画面

■ この脆弱性によるリスク

不用意にディレクトリにファイルを保存した際にファイル名を特定される恐れがあります。そのため意図しない情報漏洩につながる可能性があります。

■ 対策方法

httpd.conf の設定で Indexes オプションを削除してください。<Directory>ディレクティブが複数存在する場合それぞれのディレクティブで Indexes の指定を削除する必要があります。

■該当箇所

No.	URL
1	http://www.example.jp/icons/
2	http://www.example.jp/icons/small/
3	https://www.example.jp/icons/

W.5 参考情報および推奨事項

情報

1． バージョン情報の開示

レスポンスヘッダにバージョン情報が表示されています。バージョンの開示自体が脆弱性にはなりませんが、セキュリティ対策のされていないバージョンの情報が表示されることにより、攻撃手法を絞ることが可能となります。

図 2 「入力フォーム画面一覧」サイトのレスポンス例

図 3 レスポンス例

以下の設定にすることを推奨いたします。

- Apache の httpd.conf ファイルの ServerSignature および ServerTokens ディレクティブ

  ServerSignature Off
  ServerTokens ProductOnly

- PHP の php.ini ファイル

  expose_php = Off

また、現在表示されているバージョンのアプリケーションは複数の脆弱性が報告されているため、最新バージョンに更新することを推奨いたします。

※ 参考情報
各アプリケーションの 2010 年 9 月 13 日現在の最新バージョンは以下の通りです。

製品名	最新バージョン
Apache2.0	2.0.63
Apache2.2	2.2.16
PHP5.3	5.3.3
PHP5.2	5.2.14

２． 前回ログイン日時と利用履歴の非表示

前回ログイン日時やサイトの利用履歴を確認する機能が存在しません。このことにより、情報漏洩等の被害につながるわけではありませんが、前回ログイン日時と利用履歴を表示することで以下の 2 つの効果が期待できます。

1） 利用者自身がログイン日時・利用履歴を確認することで、不正ログイン・不正利用が行われた場合に速やかにその事実に気づくことができます。

2） 不正ログイン・不正利用を行う攻撃者の行為を抑制できます。

※クロスサイトリクエストフォージェリによる間接的な不正利用も含みます。

5.2 ネットワークセキュリティ診断結果

xxx.xxx.xxx.xxx

HOST FQDN	○○○○.co.jp
オープンポート	80/tcp、443/tcp
機器・用途	N/A

N.1 脆弱な暗号化方式の許容

1	低

■ CVSS 2.0

■

評価値: 5.0	注意 (0.0～3.9)	警告 (4.0～6.9)	危険 (7.0～10.0)
AV :攻撃元区分	ローカル	隣接	**ネットワーク**
AC :攻撃条件の複雑さ	高	中	**低**
Au :攻撃前の認証要否	複数	単一	**不要**
C :機密性への影響	なし	**部分的**	全面的
I :完全性への影響	**なし**	部分的	全面的
A :可用性への影響	**なし**	部分的	全面的

■ 現象

443/tcp の SSL 通信において、強度の不十分な暗号化方式がサポートされています。56 ビット未満の鍵が使用されている SSL 通信は以下のとおりです。

```
Low Strength Ciphers (< 56-bit key)
SSLv3
EXP-DES-CBC-SHA     Kx=RSA(512)     Au=RSA     Enc=DES(40)     Mac=SHA1     export
EXP-RC2-CBC-MD5 Kx=RSA(512) Au=RSA Enc=RC2(40) Mac=MD5 export EXP-RC4-MD5
Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 export
TLSv1
EXP-DES-CBC-SHA     Kx=RSA(512)     Au=RSA     Enc=DES(40)     Mac=SHA1     export
EXP-RC2-CBC-MD5 Kx=RSA(512) Au=RSA Enc=RC2(40) Mac=MD5 export EXP-RC4-MD5
Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 export
```

図 4 弱い暗号化方式のサポート

```
---
New, TLSv1/SSLv3, Cipher is RC4-MD5
Server public key is 1024 bit
Compression: NONE
Expansion: NONE
SSL-Session:
    Protocol  : SSLv3
    Cipher    : RC4-MD5
    Session-ID: 345D705490541ODB005C39D4EAE1863D14F85E440AD834261ED143813E0BBE

    Session-ID-ctx:
    Master-Key: 8CF0995B3ED0E045B98A4A75EBED43AB9B0E0B30A4210CDFCA15A2E2122E17
80571199FA096894B621A288E055444D
    Key-Arg   : None
    Start Time: 1268033614
    Timeout   : 300 (sec)
    Verify return code: 20 (unable to get local issuer certificate)
---
read:errno=0
```

図 5 弱い暗号化方式のサポート

■この脆弱性によるリスク

ビット数の少ない鍵により暗号化された場合、MITM（中間者）攻撃によるセッションハイジャックや盗聴および、暗号化・復号時の処理時間を利用したタイミング攻撃などのターゲットとなりえます。

なお、MD5 アルゴリズムによる暗号化方式がサポートされていますが、MD5 アルゴリズムについては、2008 年に 認証局（CA） によって署名された証明書をもとに中間 CA 証明書の偽造に成功したことが報告されています。

■対策方法

SSL による通信の保護に 128 ビット以上の暗号鍵の利用を推奨いたします。例えば Apache で設定ファイル ssl.conf を使用している場合は、設定ファイル ssl.conf の「SSLCipherSuite」ディレクティブで使用する暗号化方式を指定します。

設定例

```
SSLCipherSuite ALL:!ADH:!EXPORT56:!EXPORT40:RC4+RSA:+HIGH:
!MEDIUM:!LOW:!SSLv2:+EXP
```

※一行で記述。

なお、古いバージョンのブラウザ等、一部のクライアントでは、強力な暗号化方式の利用に制約が存在する場合があります。特に携帯サイトの場合、一部の古い携帯端末は 128 ビット以上の暗号鍵に対応していません。接続を許容する端末によって 40 ビット等の暗号鍵を許可する必要があります

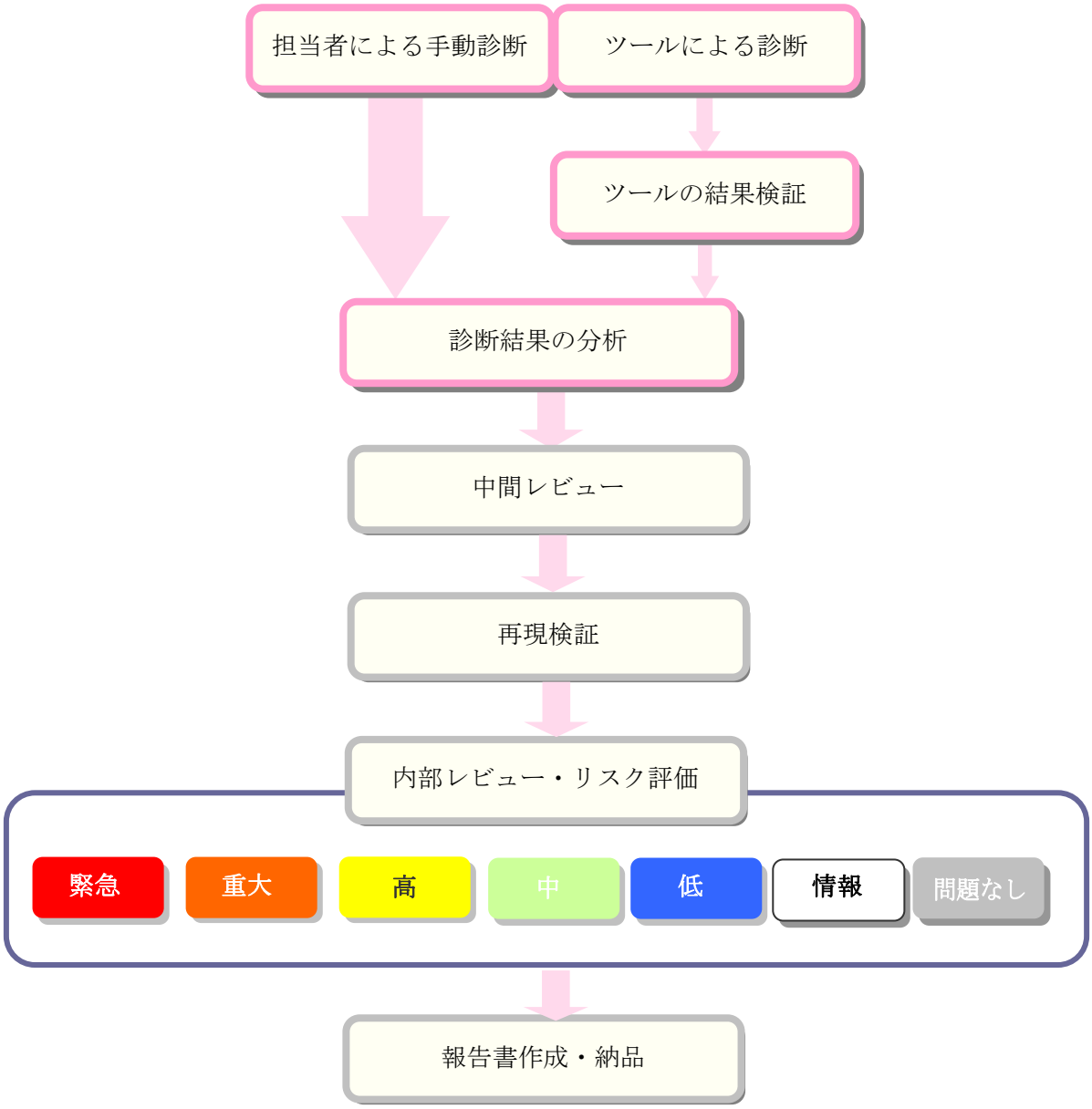
使用すべき暗号化方式の選定については、以下の URL を参照してください。

CRYPTREC ｜電子政府推奨暗号リスト
http://www.cryptrec.go.jp/list.html

APPENDIX

I.診断手法イメージ

診断対象として提示されたホストに対し、インターネットを経由したアクセスによるセキュリティ診断を実施致しました。



本診断は、あらかじめ期間を指定し、その期間中に起こりうる事象を常時監視し評価する「一定期間監視型」ではなく、突発的に調査を行い、そこから情報を収集する「一点集中型」の調査方法を採用しています。そのため、調査実施後システムに変更が発生している場合、発見された脆弱性が適用されない場合もありますのでご了承ください。

II.脆弱性評価基準

国際的な脆弱性評価基準をもとに弊社独自の基準を作成しランク付けを行っております。

・CVSS（Common Vulnerability Scoring System）
※共通脆弱性評価システム CVSS は、情報システムの脆弱性に対するオープンで包括的、汎用的な評価手法の確立と普及を目指し、米国家インフラストラクチャ諮問委員会によって作成されました。

・PCIDSS（Payment Card Industry Data Security Standard）
※クレジットカードにおけるセキュリティ基準 PCI データセキュリティスタンダード

・OWASP Top10 (Open Web Application Security Project)
※安全な Web アプリケーションや Web サービスを実現するためのツールの開発やドキュメントの作成，知識の共有を行うプロジェクト

重大性	説明
5 緊急	パスワード漏えい、管理者権限昇格など、システム全体に影響する問題です。これらの問題が発生する可能性が極めて高く、即日対応する必要があります。
4 重大	情報漏洩や、なりすましなど、ユーザ被害が発生する可能性が高い問題です。 このレベルには、クロスサイトスクリプティングや SQL インジェクションなどの問題があり、インシデント報告や OWASP TOP10 などで上位を占めるセキュリティ上の問題です。このことから、早急に対応する必要があります。
3 高	総当たり攻撃や認証回避など、セキュリティ上の問題が発生する可能性があります。 システムの仕様などにより、セキュリティ上必要な対策が実施されていない場合このレベルに分類されます。問題が発生する可能性があるため、対応を必ず行うことを推奨します。
2 中	システムの設定情報や管理情報の漏洩等、システムに対する攻撃手段を提供する可能性がある問題です。 直接被害が発生する可能性は高くないですが、他のセキュリティ上の問題と組み合わさるとレベルが上がる可能性があります。 問題になる可能性があるため対策を検討してください。
1 低	バージョン情報表示や、バナー情報表示など、攻撃者の興味を引く可能性のある問題です。 直接悪用されるよりは、このレベルの情報から攻撃手法を絞っていくことがあります。 予防するうえで対策を検討してください。
情報	品質やセキュリティのさらなる向上のために弊社が推奨する項目です。