Confidential

文書番号 QW-20YYMMDD-01

Sample 御中

クイックウェブ診断報告書

201X 年 XX 月 XX 日

本報告書は、クイックウェブ診断を行った結果をご報告するものです。報告書の内容には、脆弱性に関する情報が含まれますので、報告書の取り扱いにはご注意ください。

デジサート・ジャパン合同会社

目次

1 はじめに

1.1. 当報告書の取り扱いについて

本報告書には、お客様のネットワークに関するセキュリティ上の問題点が記載されています。この情報がひとたび悪意ある第三者に渡ってしまうと、セキュリティ上の問題点を狙った不正アクセス攻撃を受け情報漏えい等の事故が発生する可能性があります。したがって、本報告書のお取り扱いには十分に注意して頂けますようお願いいたします。

1.2. セキュリティ対策の運用について

本報告書は診断時点でのお客様のネットワークのセキュリティ上の問題点を診断した結果が記載されています。ネットワークへの攻撃は日々研究され進化し続けているため、時間経過とともにセキュリティ上の問題が増加することが考えられます。

堅牢なネットワークを継続的に運用するためには、定期的にネットワークに潜んでいるセキュリティ上の問題点を正しく認識し対策を施すことを推奨いたします。

2 診断内容

2.1. 診断環境

2.1.1. 診断方法

リモート診断

2.1.2. 診断日時

- 201X 年 XX 月 XX 日～XX 日　　10:00 ～ 18:00

2.1.3. 診断元 IP アドレス

- XXX.XXX.XXX.XXX
- XXX.XXX.XXX.XXX

2.2. 診断項目

主な診断項目を以下に列挙します。

区分	診断詳細項目
ウェブアプリケーション診断での項目範囲	
認証	信用情報通信時の機能の不備、デフォルトアカウント使用、ロックアウト機能の不備、認証回避、復元可能なパスワードの保存、ログアウト機能の不備や未実装、脆弱なパスワードポリシー、パスワード再発行の不備、パスワードリセットの不備、管理機能の不備 ＜主な対象機能＞ ログイン画面 新規会員登録（ログイン ID やパスワード情報） パスワード再発行 パスワード変更 ログアウト
プラットフォーム診断での項目範囲	
ポートスキャン	対象サイトの TCP や UDP のポートスキャン
サービス調査	対象サイトで動作しているアプリケーションに関してのバージョン情報収集や、アプリケーションの構成等の収集
脆弱性検査	対象サイトの既知の脆弱性調査
サービスアカウント調査	SSH、FTP、Telnet、SMTP、POP 等の汎用サービスの簡易アカウント使用の調整
設定不備調査	不要なディレクトリ公開不備の調査
SPAM リレー調査	SPAM メールの不正中継調査

2.3. 診断対象

2.3.1. 診断対象情報

診断対象情報	
サイト名	サンプル会社ホームページ
IP アドレス	255.255.xxx.xxx
FQDN	www.sample-hp.com
認証機能 URL	
ログイン	https://www.sample-hp.com/login
ログアウト	https://www.sample-hp.com/logout
パスワード再発行	https://www.sample-hp.com/passwordForget
新規会員登録	https://www.sample-hp.com/member/new
パスワード変更	https://www.sample-hp.com/password/edit

上記は、お客様情報を記載しています。

認証機能 URL が、「－」の場合は、対象となる機能がありませんでした。

3 診断結果概要

3.1. 総合評価

D. 危険な状態です

3.1.1. 総合評価について

評価	基準
A	脆弱性が検出されなかった
B	危険度 Low の脆弱性のみ検出
C	危険度 Medium の脆弱性を検出
D	危険度 High の脆弱性を検出
E	危険度 Critical の脆弱性を検出

3.2. サービス一覧

プロトコル	ポート	サービス	バージョン情報
TCP	80	http	Apache/2.0.58
	443	https	Apache/2.0.58

3.3. 検出された脆弱性一覧

危険度	脆弱性概略（有効対策）
High	既知の脆弱性を持つ PHP が使用されている (②)
High	非ログイン状態で、ログインが必要な個人情報ページの参照が行える (①)
Medium	ログイン前と後でセッション ID が書き換わらない (①)
Medium	SSL プロトコルにおける平文データを取得される脆弱性（POODLE） (③、④)
Medium	RC4 の SSL 暗号化アルゴリズムのサポート (③)
Medium	TLS プロトコルにおける暗号アルゴリズムのダウングレード攻撃を実行される脆弱性（Logjam） (③、④)
Low	Apache Tomcat デフォルトページの表示 (③)

※有効対策一覧

① ウェブアプリケーションの修正

② ミドルウェアのパッチ適用、又はバージョンアップ

③ 設定変更

④ WAF（ウェブアプリケーションファイアウォール）

⑤ 改ざん検知

⑥ 侵入検知／遮断（IDS／IPS）

3.4. 総評

インターネット経由のリモート診断を行った結果、確実にリモートからの侵入を許してしまう脆弱性は検出されませんでした。しかしながら、診断対象で稼動しているサービスのバージョンが古いため、攻撃者にリモートからの侵入を許してしまったり、サービスの異常停止につながったりするような脆弱性が検出されました。さらに、非ログインでの個人情報ページ閲覧が確認できましたので、早急に対応を行うことを推奨します。

3.5. 有効対策による補足

「ウェブアプリケーションの修正」が必要な脆弱性のうち、危険度 High の脆弱性を 1 件検出しました。サイト全体に対してウェブアプリケーション診断を実施することを推奨します。

「ミドルウェアのパッチ適用、又はバージョンアップ」が必要な脆弱性のうち、危険度 High の脆弱性を 1 件検出しました。サイトを構成する機器すべてに対して、プラットフォーム診断を実施することを推奨します。

「設定変更」が必要な脆弱性のうち、危険度 Medium の脆弱性が 2 件以上検出しました。サイトを構成する機器すべてに対して、プラットフォーム診断を実施することを推奨します。

「WAF」にて対策可能な脆弱性のうち、危険度 Medium 以上の脆弱性が検出しました。いま直ぐに導入までを検討する必要はありませんが、将来的な脆弱性に対しても、WAF は有効な対応のひとつとなりますので、検討することは推奨します。

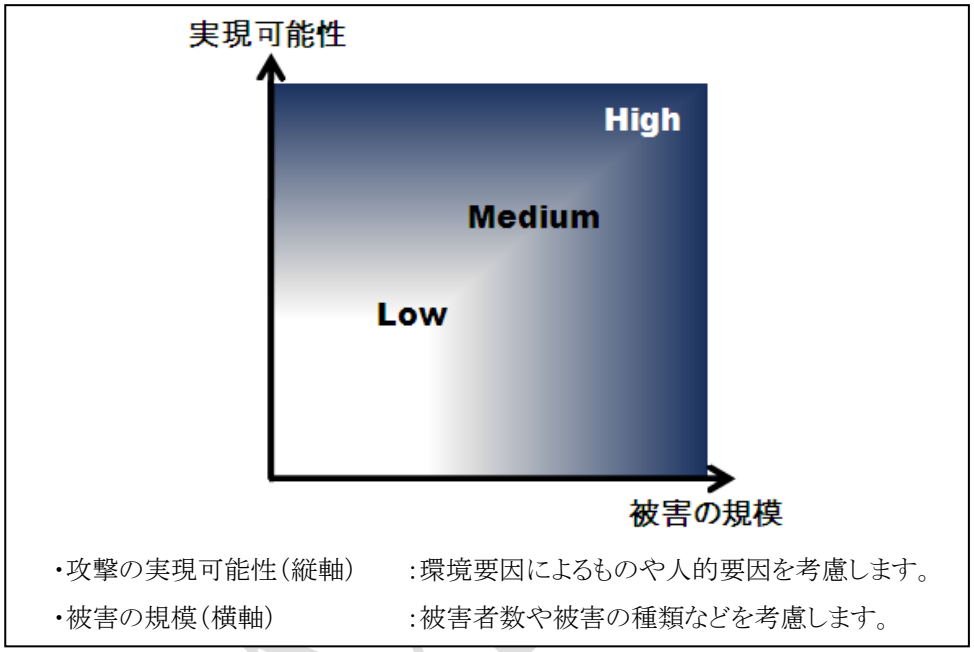
4 補足

4.1. お問合せについて

本報告書の内容に関するお問合せは、担当営業までご連絡ください。

付録 A 危険度の判定基準

脆弱性の危険度は、以下の図のように攻撃の実現可能性と被害の規模を軸として High, Medium, Low の 3 段階の値に分けています。



- High　攻撃の実現可能性が高く、被害の規模も大きい
- Medium　攻撃の実現可能性が低いかまたは被害の規模が小さい
- Low　攻撃の実現可能性が低く被害の規模も小さい

なお、実現度が低くても被害の規模が過度に大きいようであれば High と判定し、また実現度が高くても、被害の規模が小さいようであれば Low と判定します。

付録 B JNSA 想定損害賠償金額算定式

(1)算定式

想定損害賠償額 ＝ 漏えい個人情報価値

× 情報漏えい元組織の社会的責任度

× 事後対応評価

(2)漏えい個人情報の価値

漏えい情報価値 ＝ 基礎情報価値 × 機微情報度 × 本人特定容易度

(ア) 基礎情報価値

基礎情報価値は一律、「500」ポイントで設定します。

(イ) 機微情報度

機微情報度は、精神的苦痛レベルと経済的損害レベルを考慮して算出します。算出の基礎となる漏えいした情報の精神的苦痛レベルと経済的損害レベルは下表の上部（x、y）から、下記の式に代入して求めます。レベルの異なる複数の漏えい情報がある場合は、全情報のうちでもっとも大きなｘの値と、ｙの値を採用します。

算出式：機微情報度 ＝ $（10^{x-1} + 5^{y-1}）$

経済的損失レベル	1	2	3
3	口座番号/暗証番号, クレジットカード番号, カード有効期限, 銀行アカウント/パスワード	遺言書	前科前歴, 犯罪歴, 与信ブラックリスト
2	パスポート情報, 購入記録, ISPのアカウント/パスワード	年収, 年収区分, 資産, 建物, 土地, 残高, 借金, 所得, 借入れ記録	
1	氏名, 住所, 生年月日, 性別, 金融機関名, 住民票コード, メールアドレス, 健康保険証番号, 年金証書番号, 免許証番号, 社員番号, 会員番号, 電話番号, ハンドル名, 健康保険証情報, 年金証書情報, 介護保険証情報, 会社名, 学校名, 役職, 職業, 職種, 身長, 体重, 血液型, 身体特性, 写真(肖像), 音声, 声紋, 体力診断	健康診断, 心理テスト, 性別判断, 妊娠経験, 手術歴, 看護記録, 検査記録, 身体障害者手帳, DNA, 病歴, 治療法, 指紋, レセプト, スリーサイズ, 人種, 地方なまり, 国籍, 趣味, 特技, 嗜好, 民族, 日記, 賞罰, 職歴, 学歴, 成績, 試験得点, メール内容, 位置情報	加盟政党, 政治的見解, 加盟労働組合, 信条, 思想, 宗教, 信仰, 本籍, 病状, カルテ, 痴呆症, 身体障害, 知的障害, 精神的障害, 保有感染症, 性癖, 性生活

精神的苦痛レベル

(ウ)　本人特定容易度

本人特定容易度は、漏えいした個人情報から被害者本人の特定しやすさをあらわします。

判定基準	本人特定容易度
個人を簡単に特定可能。 「氏名」「住所」が含まれること。	6
コストをかければ個人が特定できる。 「氏名」または「住所＋電話番号」が含まれること。	3
特定困難。 上記以外。	1

(3)情報漏えい元組織の社会的責任度

社会的責任度は、「一般より高い」と「一般的」の 2 つから選択します。

判定基準		社会的責任度
一般より高い	個人情報の適正な取り扱いを確保するべき分野の業種（医療、金融、情報通信など）および公的機関、知名度の高い大企業	2
一般的	その他一般的な企業および団体、組織	1

(4)事後対応評価度

事後の対応の評価値を求めます。

判定基準	事後対応評価度
適切な対応	1
不適切な対応	2
不明、その他	1

付録 C 参考文献

1.「安心・安全な情報経済社会の実現のための行動計画」の発表について

http://www.meti.go.jp/press/20060302002/20060302002.html

2.セキュアプログラミング講座

http://www.ipa.go.jp/security/awareness/vendor/programming/

3.新版 セキュアプログラミング講座

http://www.ipa.go.jp/security/awareness/vendor/programmingv2/

4.情報処理推進機構 安全なウェブサイトの作り方

http://www.ipa.go.jp/security/vuln/documents/ウェブ site_security.pdf

5.情報処理推進機構 安全な SQL の呼び出し方

http://www.ipa.go.jp/security/vuln/documents/ウェブ site_security_sql.pdf

6.NPO 日本ネットワークセキュリティ協会「2009 年 情報セキュリティインシデントに関する調査報告書」

http://www.jnsa.org/result/incident/2009.html

