Confidential

株式会社サンプル 御中

セキュリティ診断結果報告書
(プラットフォーム診断)
[会員専用情報サイト]

デジサート・ジャパン合同会社

診断実施日 2020 年 7 月 6 日 ～ 2020 年 7 月 7 日

報告日 2020 年 7 月 8 日

digicert

目次

目次 2

1. はじめに 3
1.1. 本報告書の取り扱いについて 3
1.2. セキュリティ対策の運用について 3

2. セキュリティ診断実施概要 4

3. 総合評価 5
3.1. 評価 5
3.2. 総評 5
3.3. リスクレベル判定基準 6
3.4. 危険度・攻撃難易度判定基準概要 7
3.5. 診断項目概要 8

4. 検出ポート一覧 9

5. 指摘事項一覧 10

6. セキュリティ診断結果詳細 11
6.1. 指摘事項詳細 11
6.1.1. 指摘事項の項目解説 11
6.1.2. 各指摘事項詳細 12
【1】 既知の脆弱性を含むPHPが使用されている（高リスク） 12
【2】 暗号強度の低い通信方式を使用している 13
【3】 POP3 で平文のログインが許可されている 15
【4】 サーバー情報が公開されている 16

7. お問い合わせ 17
7.1. お問合わせ先 17
7.2. 再診断について 17

8. APPENDIX. セキュリティ診断項目詳細 18

9. APPENDIX. 参考文献 23

1. はじめに

1.1. 本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. セキュリティ診断実施概要

- 診断対象

対象：会員専用情報サイト

- 診断期間

診断期間：2020 年 7 月 6 日 から 2020 年 7 月 7 日 まで

診断時間：10 時 から 19 時まで

- 診断方法

エンジニアによるマニュアル診断ならびに診断専用ツールによる自動診断

- 診断形態

リモート診断

- 診断ツール

Nessus	ネットワークサービスの脆弱性を検出するツール
nmap	提供されているネットワークサービスを検出するツール
telnet	Nessus の結果を基に脆弱性の存在を診断者が確認

- 診断元 IP アドレス

39.110.224.144/29

122.216.15.62

- 備考

－

3. 総合評価

3.1. 評価

D	リスクレベル 高 を 1 件以上検出またはリスクレベル 中 を 2 件以上検出

評　価	説　明
A	脆弱性の検出なし
B	リスクレベル 低 のみを検出
C	リスクレベル 中 を 1 件以上検出
D	リスクレベル 高 を 1 件以上検出またはリスクレベル 中 を 2 件以上検出
E	リスクレベル 緊急 を 1 件以上検出またはリスクレベル 高 を 2 件以上検出

3.2. 総評

今回のセキュリティ診断において、リスクレベル 高 を 1 件検出したため総合評価は D となります。

即時にサービスに影響の出る問題点を確認しておりますので、早急にご対応いただくことが望まれます。

3.3. リスクレベル判定基準

本報告書では各指摘事項について、リスクレベルを設定しています。各指摘事項について危険度・攻撃難易度を評価し、さらに下記判定基準にてリスクレベルを決定しています。

リスクレベル		危険度		
		高	中	低
攻撃難易度	易	緊急	高	低
	中	高	中	低
	難	中	低	低

	リスクレベル説明
緊急	攻撃された場合の被害が甚大、または容易に攻撃が実行可能
高	攻撃された場合の影響が大きい、またはある程度の知識や技術があれば攻撃が可能
中	攻撃された場合の影響が限定的、間接的、または攻撃実行の難易度が比較的高い
低	攻撃された場合の影響が軽微、または攻撃を実行するために複数の条件が必要など実現が困難

3.4. 危険度・攻撃難易度判定基準概要

本報告書の指摘事項における「危険度」「攻撃難易度」は、弊社の独自基準になります。

	危険度
高	システムの侵入やページ改ざん、機密情報漏えいにつながる指摘事項 （ソフトウェアの既知の脆弱性、サポート終了ソフトウェアの使用など）
中	システムの停止やシステム設定情報の漏えいにつながる指摘事項 （DoS 攻撃、設定パラメーターの漏えいなど）
低	システムのバナー情報等、直接的にシステムへの侵入につながらない指摘事項 （サーバーサービスのバージョン取得、不要なオープンポートなど）

※指摘事項により想定されるシステムへの影響の大きさを表します。

	攻撃難易度判定基準
易	簡単に手に入るツールなどによって、容易に攻撃を行うことが可能
中	特定の条件をクリアすることによって攻撃を行うことが可能
難	攻撃を行うためには非常に複雑な条件をクリアする必要がある

※指摘事項を悪用してシステムへの攻撃を成立させる難易度を表します。

3.5. 診断項目概要

	プラットフォーム診断項目
1	ポートスキャン（TCP/UDP） ※全ポート対象
2	バナーチェック
3	バージョンチェック
4	ユーザーリストの作成
5	ユーザー認証
6	FTP 匿名接続調査
7	SSH 認証調査
8	パスワード簡易推測調査（FTP/SSH/Telnet）
9	SMTP 不正中継調査
10	SMTP アカウント簡易推測調査
11	DNS 再帰問い合わせ調査
12	DNS ゾーン転送調査
13	Finger アカウント情報収集調査
14	HTTP メソッド調査
15	HTTP コンテンツ調査
16	HTTP アプリケーションマッピング調査
17	WebDAV/FrontPage 調査

※ サイトの構成などより診断を行わない項目があります。

※ 診断中に技術者が必要と判断した診断内容を行うことがあります。

4. 検出ポート一覧

IP・FQDN （システム名）	ポート	サービス	情報
XXX.XXX.XXX.XXX	22/tcp	ssh	-
	80/tcp	http	Apache httpd 2.2.3 (Red Hat)
	443/tcp	ssl/http	Apache httpd 2.2.3 (Red Hat)

5. 指摘事項一覧

指摘番号	指摘事項	ページ番号	リスクレベル
1	既知の脆弱性を含む PHP が使用されている（高リスク）	12p	高
2	暗号強度の低い通信方式を使用している	13p	中
3	POP3 で平文のログインが許可されている	15p	低
4	サーバー情報が公開されている	16p	低

6. セキュリティ診断結果詳細

6.1. 指摘事項詳細

6.1.1. 指摘事項の項目解説

指摘事項ごとに、下記内容で報告しております。

【指摘番号】指摘事項の概要

リスクレベル	「3.3. リスクレベル判定基準」から評価したリスクレベルを記載	「3.4. 危険度・攻撃難易度判定基準概要」から評価した危険度・攻撃難易度を記載

脆弱性種類	診断結果より判断した脆弱性の項目（種類）を記載
診断内容	プラットフォーム診断の内容を記載
診断結果	診断を行った結果及び結果に対する危険性を記載
対応案	診断結果に対するセキュリティ対策案を記載
再現例	診断を行った結果画像を記載
発生箇所	対象 IP アドレス及び再現手順を記載
備考	特記事項があった場合に記載

6.1.2. 各指摘事項詳細

【1】 既知の脆弱性を含む PHP が使用されている（高リスク）

リスクレベル	高	危険度：高　攻撃難易度：中

脆弱性種類	PHP バージョンの既知の脆弱性
診断内容	対象システムにおいて既知の脆弱性を持っているソフトウェアバージョンが使用されているか確認
診断結果	レスポンスヘッダーから確認した情報によると、対象システムで使用されている PHP のバージョンには、既知の脆弱性が存在します。 当該脆弱性を攻撃者に悪用されることで、情報を取得される、情報を改ざんされる、およびサービス運用妨害（DoS）状態にされる等、複数の脆弱性による影響を受ける可能性があります。
対応案	既知の脆弱性が修正された最新のバージョンに更新することを推奨します。
再現例	＜レスポンスヘッダーを確認した結果＞ [Appirits]$ curl https://XXX.XXX.XXX.XXX/ -I HTTP/1.1 200 OK Date: Mon, 08 Jun 2020 10:19:54 GMT Server: PHP/5.6.32 Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 Connection: close Content-Type: text/html; charset=UTF-8
発生箇所	対象: XXX.XXX.XXX.XXX 手順:対象システムへ接続した際のレスポンスヘッダーにて、使用されている PHP のバージョンを確認することができます。 ＜確認された PHP のバージョン＞ PHP/5.6.32
備考	対象システムの PHP は、下記の脆弱性が存在する可能性があります。詳細は下記 URL をご参照ください。 ・PHP におけるバッファエラーの脆弱性 https://jvndb.jvn.jp/ja/contents/2018/JVNDB-2018-002490.html ・CVE-2018-19935 Detail https://nvd.nist.gov/vuln/detail/CVE-2018-19935 Amazon Linux などベンダーのサポートでパッチが適用されている場合があります。適用状況などは下記 URL をご参照ください。 ・https://alas.aws.amazon.com/

【2】 暗号強度の低い通信方式を使用している

リスクレベル	中	危険度：中　攻撃難易度：中

脆弱性種類	暗号化通信時の暗号化強化による問題
診断内容	暗号化通信時の方式を確認
診断結果	対象システムでは SSL 通信においてセッションキーを 128bit 未満で生成することができる設定となっております。 128bit 未満ですと解読が容易に行えるため攻撃者が正規利用者の暗号化通信を傍受した場合、個人情報を奪取される可能性があります。
対応案	128bit 未満の暗号化強度を使用しないよう Apache の設定することを推奨します。
再現例	＜セッションキー40bit の暗号化方式で接続を行った結果＞

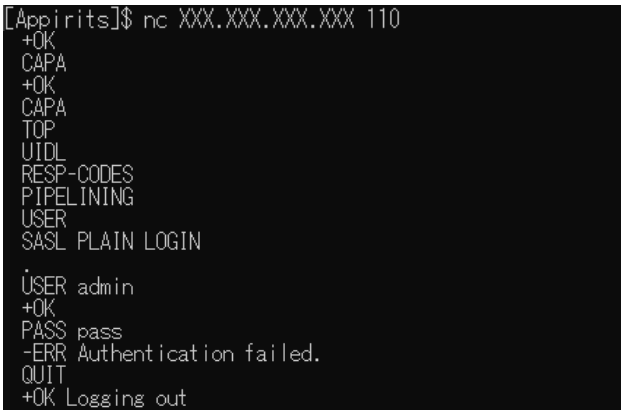
```
[root@CSL-Server ~]# openssl s_client -connect XXX.XXX.XXX.XXX:443 -cipher
EXP-RC2-CBC-MD5 -ssl3 < /dev/null
CONNECTED(00000003)
depth=0 C = JP, ST = Tokyo, O = APPIRITS INC, CN = example.com
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 C = JP, ST = Tokyo, O = APPIRITS INC, CN = example.com
verify error:num=27:certificate not trusted
verify return:1
depth=0 C = JP, ST = Tokyo, O = APPIRITS INC, CN = example.com
verify error:num=21:unable to verify the first certificate
verify return:1
---
Certificate chain
 0 s:/C=JP/ST=Tokyo/O=APPIRITS INC/CN=example.com
   i:/C=JP/ST=Tokyo/L=Shibuya-ku/O=Appirits Inc/OU=CyberSecurityLaboratory
/CN=CSL Private CA/emailAddress=xxxx@example.com
---
subject=/C=JP/ST=Tokyo/O=APPIRITS INC/CN=xxxx@example.com
issuer=/C=JP/ST=Tokyo/L=Shibuya-ku/O=Appirits
Inc/OU=CyberSecurityLaboratory/CN=CSL Private
CA/emailAddress=xxxx@example.com
---
No client certificate CA names sent
---
SSL handshake has read 1369 bytes and written 202 bytes
---
```

（次ページへ続く）

再現例	New, TLSv1/SSLv3, Cipher is EXP-RC2-CBC-MD5 Server public key is 1024 bit Secure Renegotiation IS supported Compression: NONE Expansion: NONE SSL-Session: Protocol : SSLv3 Cipher : EXP-RC2-CBC-MD5 Session-ID: CF07E348DC19549B4B00811AE03C2D9E063F412928961B815F47FFE880F140E6 Session-ID-ctx: Master-Key: 2CD5DD7C6C34B96F6DB003DD27BC51C074F456BC1D9910D02BBA436F441D9A064C3E8DC7E841A82F25F827653AB3A880 Key-Arg : None Krb5 Principal: None PSK identity: None PSK identity hint: None Start Time: 1398220753 Timeout : 7200 (sec) Verify return code: 21 (unable to verify the first certificate) --- DONE
発生箇所	対象：XXX.XXX.XXX.XXX 手順：openssl コマンドより短いセッションキーの暗号化方式を指定した状態で接続を行うことで 128bit 未満のものを使用することができることを確認できます。 ＜確認された 128bit 未満の暗号化方式＞ ・EXP-RC2-CBC-MD5(SSLv3) ・EXP-RC4-MD5(SSLv3) ・EXP-RC2-CBC-MD5(TLSv1) ・EXP-RC4-MD5(TLSv1) ・DES-CBC-SHA(SSLv3) ・DES-CBC-SHA(TLSv1)
備考	

【3】 POP3 で平文のログインが許可されている

リスクレベル	低	危険度：低　攻撃難易度：難

脆弱性種類	平文によるログイン情報の通信
診断内容	平文でログイン情報の通信が行われていないか確認
診断結果	対象システムは、暗号化されていない平文でのログインを許可する POP3 サービスが動作しています。 安全性の低い認証メカニズムを使用する際、攻撃者が POP3 への盗聴を行うことにより、ユーザー名とパスワードを明らかにすることができます。
対応案	SSL/TLS 利用してトラフィックを暗号化する POP3S などの利用を推奨します。
再現例	＜POP3 へ平文で認証を試行した様子＞ 
発生箇所	対象：XXX.XXX.XXX.XXX 手順：nc コマンドなどにより POP3 のポートへ接続を行うことで、利用可能であるかを確認できます。 ＜利用できる平文利用のログインコマンド＞ USER SASL PLAIN LOGIN
備考	

【4】 サーバー情報が公開されている

リスクレベル	低	危険度：低　攻撃難易度：難

脆弱性種類	プログラムの潜在的脆弱性
診断内容	サーバー情報が表示されるか確認
診断結果	対象システムにアクセスした際に、サーバー情報が表示されます。サーバー情報を表示させていることで、攻撃者に既知の脆弱性を含んでいるバージョンであるか確認される状態といえます。
対応案	レスポンスの内容にサーバー情報を表示させないよう設定することを推奨します。
再現例	＜レスポンスヘッダーを確認した結果＞ [Appirits]$ curl https://XXX.XXX.XXX.XXX/ -I HTTP/1.1 200 OK Date: Mon, 08 Jun 2020 10:19:54 GMT Server: PHP/5.6.32 Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 Connection: close Content-Type: text/html; charset=UTF-8
発生箇所	対象：XXX.XXX.XXX.XXX 手順：curl コマンドにより接続を行いレスポンスを表示することで、サーバー情報が確認できます。 ＜確認されたサーバー情報＞ PHP/5.6.32
備考	

7. お問い合わせ

7.1. お問合わせ先

本報告書に関するお問合わせは以下メールアドレスまでご連絡をください。お問合わせの対応は報告書提出から１カ月間無料で対応をいたしております。なお、お電話（Skype 等の通話含む）での対応や報告会での対応は別途となりますのでご了承ください。

お問合わせ先メールアドレス	csl@appirits.com

7.2. 再診断について

弊社が診断をしたセキュリティ診断についてお客様にて修正を行った後に、再診断を行うことができます。なお、弊社より報告書を提出したのち、１か月以内の１回の診断実施となりますのでご了承ください。

8. APPENDIX. セキュリティ診断項目詳細

1. ポートスキャン（TCP/UDP）

診断内容

外部から接続可能なポートを確認して、不要なポートを解放していないか診断します

発生する可能性のあるリスク

不正アクセスが行われやすい状態にあり不正アクセスがされた場合、情報漏えい・改ざん・サービス停止の危険性があります

2. バナーチェック

診断内容

サーバーで実行中のサービスに対してコマンドを実行することで、使用中のソフトウェア情報が表示されるか診断します

発生する可能性のあるリスク

使用しているソフトウェア情報を表示させていることで、攻撃者へのヒントになる可能性があります

3. バージョンチェック

診断内容

サーバーで使用されているソフトウェアのバージョンが既知の脆弱性を持っているバージョンか診断します

発生する可能性のあるリスク

既知の脆弱性を持っているソフトウェアを使用していた場合、当該脆弱性を突いた攻撃を受ける可能性があり、情報漏えい・改ざん・サービス停止の危険性があります

4. ユーザーリストの作成

診断内容

サーバー内に作成されているユーザーを、OS コマンド等を使用することで洗い出しが行えるか診断します

発生する可能性のあるリスク

サーバー内で使用されているユーザーの洗い出しが行える場合、当該ユーザーを利用して辞書攻撃に利用される危険性があり、管理者になりすましてアクセスが行われる危険性があります

5. ユーザー認証

診断内容

ディレクトリやファイルへアクセスする際の認証方法を確認し、アクセス制限を適切に行っているか診断します

発生する可能性のあるリスク

アクセス制限を適切に行っていないことで、第三者に閲覧権限の無い情報が閲覧できてしまう可能性があり、情報漏えいの危険性があります

6. FTP 匿名接続調査

診断内容

匿名アカウント（Anonymous）による FTP 接続が行えるか診断します

発生する可能性のあるリスク

匿名アカウントでの接続が行える状態にある場合、第三者から容易に接続が行えてしまう状態にあり、情報漏えい・改ざんの危険性があります

7. SSH 認証調査

診断内容

SSH 接続時の認証方法を確認し、認証を容易に突破できるような方式をとっていないか診断します

発生する可能性のあるリスク

不正な操作により認証が突破できる場合、不正アクセスにより情報漏えい・改ざん・サービス停止の危険性があります

8. パスワード簡易推測調査

診断内容

FTP、SSH、Telnet サービスなどで使用されている各アカウント（ID/パスワード）が想定されやすい文字列を使用しているか診断します

発生する可能性のあるリスク

想定されやすいアカウント（ID/パスワード）を使用している場合、辞書攻撃により管理者アカウントを奪取されやすい状態にあり、管理者になりすましてアクセスが行われる危険性があります

9. SMTP 不正中継調査

診断内容

迷惑メールの送信に使用することができるか診断します

発生する可能性のあるリスク

メールの不正中継が行える場合、第三者により大量の迷惑メール送信に使用される可能性があり、サービス停止などの危険性があります

10. SMTP アカウント簡易推測調査

診断内容

メールコマンドを使用して、メールの使用が可能なユーザーの洗い出しが行えるか診断します

発生する可能性のあるリスク

メール使用可能なユーザーが洗い出せることで、当該ユーザーになりすまし大量の迷惑メール送信に使用される可能性があり、サービス停止などの危険性があります また、奪取されたアカウントに届くメールデータを閲覧できる可能性があり、情報漏えいの危険性があります

11. DNS 再帰問い合わせ調査

診断内容

他のドメインから受け取った DNS の応答内容を一時的に保存することができ、不正な応答内容を送り込むことで、間違った名前解決が行えるか診断します

発生する可能性のあるリスク

攻撃者が不正な応答内容を送り込むことで、間違った名前解決が行えてしまう可能性があり、サービスに支障をきたす危険性があります

12. DNS ゾーン転送調査

診断内容

指定されたサーバー以外へのゾーンの転送が行えるか診断します

発生する可能性のあるリスク

意図しないサーバーへゾーン情報を転送できる場合、サイトの構成情報が漏えいする危険性があります

13. Finger アカウント情報収集調査

診断内容

Finger プロトコルが使用でき、そこからアカウント情報の収集が行えるか診断します

発生する可能性のあるリスク

サーバー内で使用されているユーザー情報が収集できた場合、当該ユーザーを利用して辞書攻撃に利用される危険性があり、管理者になりすましてアクセスが行われる危険性があります

14. HTTP メソッド調査

診断内容

不必要な HTTP メソッドが使用でき、サーバー情報の確認、改ざん等が行えるか診断します

発生する可能性のあるリスク

不要なメソッドが使用できる場合、攻撃者により改ざんが行われる危険性があります

15. HTTP コンテンツ調査

診断内容

デフォルトで作成されるような不要なコンテンツを表示させたままになっていないか、そこからサーバー情報が確認できるか診断します

発生する可能性のあるリスク

不要なコンテンツを表示させたままにしておくことで、攻撃者へのヒントになる可能性があります

16. HTTP アプリケーションマッピング調査

診断内容

IIS を使用している場合、使用していないファイル形式の拡張子に対してマッピングが有効になっており、それによる改ざん等が行えるか診断します

発生する可能性のあるリスク

不要なファイル形式の拡張子に対してマッピングがされていることにより、攻撃者に不正利用された場合、改ざんが行われる危険性があります

17. WebDAV/FrontPage 調査

診断内容

アクセス制限、認証が適切に設定されているか、サーバー情報等の取得、改ざんが行えるか診断します

発生する可能性のあるリスク

アクセス制限、認証が適切に設定されていないことにより、攻撃者に不正に利用される可能性があり、改ざんが行われる危険性があります

9. APPENDIX. 参考文献

- IPA(情報処理推進機構セキュリティセンター)
  http://www.ipa.go.jp/security/

- 安全なウェブサイトの作り方　情報処理推進機構
  http://www.ipa.go.jp/security/vuln/websecurity.html

- JVN iPedia - 脆弱性対策情報データベース
  http://jvndb.jvn.jp/

- JPCERT/CC
  http://www.jpcert.or.jp/

- 日本ネットワークセキュリティ協会（JNSA）
  http://www.jnsa.org/

- マイクロソフト セキュリティ レスポンス センター
  https://www.microsoft.com/ja-jp/msrc