Confidential

文書番号 VSJ-SC-201xxxxx-xx

Sample 御中

プラットフォーム診断報告書

201X 年 XX 月 XX 日

本報告書は、201X 年 XX 月 XX 日から XX 日にかけて、Sample 様のサーバに対してプラットフォーム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。

診断項目	区分	診断詳細項目
ネットワーク調査	TCP	TCP ポートスキャン
		TCP サービススキャン
		パケットフィルタリング調査
	UDP	UDP ポートスキャン
		UDP サービススキャン
サービス調査	サービス	バナー情報収集調査
主要サービス調査	FTP	FTP 匿名接続調査
		FTP パスワード簡易推測調査
	SSH	SSH プロトコルバージョン調査
		SSH 認証調査
		SSH パスワード簡易推測調査
	Telnet	Telnet パスワード簡易推測調査
	SMTP	SMTP 不正中継調査
		SMTP アカウント簡易推測調査
	POP	POP パスワード簡易推測調査
	DNS	DNS 再帰問い合わせ調査
		DNS ゾーン転送調査
	Finger	Finger アカウント情報収集調査
	HTTP/HTTPS	HTTP メソッド調査
		HTTP コンテンツ調査
		HTTP アプリケーションマッピング調査
		WebDAV/FrontPage 調査
		SSL プロトコルバージョン調査
		SSL 暗号強度調査
		SSL 証明書調査
		Proxy 不正中継調査
	Auth	Auth アカウント情報収集調査
	SNMP	SNMP コミュニティ簡易推測調査
	SMB/CIFS	SMB/CIFS アカウント情報収集調査
		SMB/CIFS パスワード簡易推測調査
	RPC	ONC/RPC 情報収集
	IPsec	IKE 情報収集調査
	R	R 認証調査
	Console	リモート管理コンソール調査
脆弱性調査	脆弱性情報収集	脆弱性情報収集
	脆弱性調査	診断ログ精査

2.3. 診断対象

2.3.1. 診断対象 IP アドレス

- 192.168.1.1
- 192.168.1.2

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. 診断対象別評価一覧

IP アドレス	評価	OS 推測	詳細ページ
192.168.1.1	D	Linux Kernel 2.6	P.7
192.168.1.2	D	Linux Kernel 2.6	P.8

3.3. 検出された脆弱性一覧

危険度	脆弱性名称	詳細ページ
High	Sendmail における複数の脆弱性	P.9
High	Apache HTTP Server における複数の脆弱性	P.11
High	Apache HTTP Server におけるサービス運用妨害の脆弱性	P.13
Medium	Apache HTTP Server における HttpOnly 属性 Cookie の値を取得される脆弱性	P.16
Medium	第三者中継が可能な SMTP サービス	P.19
Medium	SSL バージョン 2 プロトコルのサポート	P.21
Low	Web サーバのバージョン情報	P.23

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。また、HttpOnly 属性 Cookie が取得される脆弱性が検出されていることから、HttpOnly 属性が付いた Cookie であっても外部に漏えいする可能性があります。サービスを最新のバージョンにアップグレードすることを推奨します。

その他にも、情報漏洩や攻撃者に有用な情報を与えてしまうような脆弱性が複数検出されました。一つ一つは侵入を許してしまうような脆弱性ではありませんが、攻撃者はこれら複数の情報をもとに的確かつ効率的に攻撃を行ってくることから、設定等を変更してこのような情報を攻撃者に与えないように対策することを推奨します。

4 診断結果詳細

4.1. 診断対象別結果詳細

4.1.1. 診断対象 ：192.168.1.1

(1) 診断対象別評価

D. 危険な状態です

(2) ホスト情報

ホスト名	OS 推測
host1.example.com	Linux Kernel 2.6

(3) 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

(4) 脆弱性一覧

危険度	脆弱性名称	詳細ページ
High	Apache HTTP Server における複数の脆弱性	P.11
High	Apache HTTP Server におけるサービス運用妨害の脆弱性	P.13
Medium	Apache HTTP Server における HttpOnly 属性 Cookie の値を取得される脆弱性	P.16
Medium	SSL バージョン 2 プロトコルのサポート	P.21
Low	Web サーバのバージョン情報	P.23

(5) 備考

なし

4.1.2. 診断対象 ：192.168.1.2

(1) 診断対象別評価

D. 危険な状態です

(2) ホスト情報

ホスト名	OS 推測
host2.example.com	Linux Kernel 2.6

(3) 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	25	smtp	Sendmail 8.12.11
	587	smtp	Sendmail 8.12.11

(4) 脆弱性一覧

危険度	脆弱性名称	詳細ページ
High	Sendmail における複数の脆弱性	P.9
Medium	第三者中継が可能な SMTP サービス	P.19

(5) 備考

なし

4.2. 脆弱性別結果詳細

4.2.1. Sendmail における複数の脆弱性

(1) 危険度

High

(2) 脆弱性概要

検出した Sendmail のバージョンには、以下のような脆弱性が指摘されています。

IP アドレス	ポート	バージョン情報
192.168.1.2	25/tcp	Sendmail 8.12.11
	587/tcp	Sendmail 8.12.11

Sendmail 8.12.11 における脆弱性

sendmail における X.509 証明書の処理に関する任意の SSL-based SMTP サーバになりすまされる脆弱性	
危険度 ： High	CVE-2009-4565
http://jvndb.jvn.jp/ja/contents/2010/JVNDB-2010-001002.html	
sendmail には、X.509 証明書内の Common Name（CN）フィールドにある '¥0' 文字を適切に処理しないため、任意の SSL-based SMTP サーバになりすまされる、またはアクセス制限を回避される脆弱性が存在します。 本脆弱性は CVE-2009-2408 と関連があります。	
Sendmail のタイムアウト処理における競合状態の脆弱性	
危険度 ： High	CVE-2006-0058
http://jvndb.jvn.jp/ja/contents/2006/JVNDB-2006-000143.html	
Sendmail には、タイムアウト処理における非同期シグナルの取り扱いが不適切であるため、特定のタイミングにおいて競合状態が発生する脆弱性が存在します。	

※他にも複数の脆弱性が指摘されております。

(3) IP アドレス

- 192.168.1.2

(4) 想定される脅威

攻撃者にリモートから任意のコードを実行されたり、サービスの異常停止を引き起こされたりする可能性があります。

(5) 対策

オープンソース版の Sendmail を使用している場合は、現時点で最新のバージョンである Sendmail 8.xx.xx にアップグレードすることを推奨します。

http://www.sendmail.com/sm/open_source/

有償版の Sendmail を使用している場合は、ベンダにお問い合わせください。

(6) 備考

本脆弱性は取得したバージョン情報をもとに検出しているため、本脆弱性を修正するパッチが適用されている場合も脆弱性が検出されます。パッチが適用されているか確認し、パッチが適用されていない場合は最新のバージョンにアップグレードもしくはパッチの適用を推奨します。パッチが適用されている場合は、本脆弱性の影響を受けることはありません。

4.2.2. Apache HTTP Server における複数の脆弱性

(1) 危険度

High

(2) 脆弱性概要

検出した Apache HTTP Server のバージョンには、以下のような脆弱性が指摘されています。

IP アドレス	ポート	バージョン情報
192.168.1.1	80/tcp	Apache/2.0.58
	443/tcp	Apache/2.0.58

Apache HTTP Server2.0.58 における脆弱性

Apache HTTP Server の mod_rewrite におけるバッファオーバーフローの脆弱性	
危険度 ： High	CVE-2006-3747
http://jvndb.jvn.jp/ja/contents/2006/JVNDB-2006-000461.html	
Apache HTTP Server の Rewrite モジュール（mod_rewrite）には、1）リクエストされた URL の一部を使用して URL の内部書き換えの制御を行っている（例えば、書き換える URL が $1 で始まる場合など）、2）Forbidden（F）、Gone（G）、および NoEscape（NE）のいずれの Rewrite Rule フラグも使用していない、RewriteRule を設定している場合、バッファオーバーフローが発生する脆弱性が存在します。	
Apache HTTP Server におけるサービス運用妨害（DoS）の脆弱性	
危険度 ： Medium	CVE-2011-4415
http://jvndb.jvn.jp/ja/contents/2011/JVNDB-2011-002786.html	
Apache HTTP Server の server/util.c 内にある ap_pregsub 関数は、mod_setenvif モジュールが有効な際、環境変数の値のサイズを制限しないため、サービス運用妨害（メモリ消費、または NULL ポインタデリファレンス）状態となる脆弱性が存在します。 本脆弱性は、CVE-2011-3607 の脆弱性とは異なる脆弱性です。	

※　他にも複数の脆弱性が指摘されています。

(3) IP アドレス

- 192.168.1.1

(4) 想定される脅威

攻撃者にサービス運用妨害(DoS)攻撃を受け、サービスが停止する可能性があります。また、パスワードや設定情報などが攻撃者に漏えいする可能性があります。

(5) 対策

現時点で最新のバージョンである Apache HTTP Server 2.2.xx、または 2.4.x にアップグレードすることを推奨します。

http://httpd.apache.org/

(6) 備考

本脆弱性は取得したバージョン情報をもとに検出しているので、本脆弱性を修正するパッチが適用されている場合も脆弱性が検出されます。パッチが適用されているか確認し、パッチが適用されていない場合は最新のバージョンにアップグレードもしくはパッチの適用を推奨します。パッチが適用されている場合は、本脆弱性の影響を受けることはありません。

4.2.3. Apache HTTP Server におけるサービス運用妨害の脆弱性

(1) 危険度

High

(2) 脆弱性概要

Apache HTTP Server の 2.0.64 及びそれ以前のバージョン、2.2.19 及びそれ以前のバージョンには、Range ヘッダ及び Request-Range ヘッダの処理に問題があり、Range ヘッダ及び Request-Range ヘッダに細工をしたリクエストが送信されるとメモリが大量に消費され、サービス拒否(DoS)状態になる脆弱性が検出されました(CVE-2011-3192)。

IP アドレス	ポート	詳細
192.168.1.1	80/tcp	(リクエスト) GET / HTTP/1.1 Host: 192.168.1.1 Range: bytes=0-1, 0-2, 0-3, 1-2, 1-3, 2-3 (レスポンス) HTTP/1.1 206 Partial Content Date: Wed, 29 Feb 2012 08:40:20 GMT Server: Apache/2.0.58 Last-Modified: Fri, 07 Feb 2003 10:13:28 GMT Accept-Ranges: bytes Content-Length: 515 Connection: close Content-Type: multipart/byteranges; boundary=4ba164b3 18be35e74
	443/tcp	(リクエスト) GET / HTTP/1.1 Host: 192.168.1.1 Range: bytes=0-1, 0-2, 0-3, 1-2, 1-3, 2-3 (レスポンス) HTTP/1.1 206 Partial Content Date: Wed, 29 Feb 2012 09:03:26 GMT Server: Apache/2.0.58 Last-Modified: Thu, 27 Aug 2009 01:09:49 GMT Accept-Ranges: bytes Content-Length: 521 Connection: close Content-Type: multipart/byteranges; boundary=4ba169dd 1f1967c6d

(3) IP アドレス

- 192.168.1.1

(4) 想定される脅威

攻撃者にリモートから Range ヘッダ及び Request-Range ヘッダに細工をしたリクエストが送信されると、Apache HTTP Server はサービス拒否(DoS)状態になります。

(5) 対策

Apache HTTP Server 2.2 系は、2.2.20 以降のバージョンで対策済みですが、2.2.20 はバグが含まれています。2.2 系を利用している場合は現時点で最新のバージョンである Apache HTTP Server 2.2.xx、または 2.4.x にアップグレードすることを推奨します。

http://httpd.apache.org/

2.2 系の 2.2.9～2.2.19 を利用していてアップグレードできない場合や、2.0 系を利用している場合は、以下の URL からパッチをダウンロードして適用することを推奨します。

http://www.apache.org/dist/httpd/patches/apply_to_2.2.14/ (2.2.9～ 2.2.14)
http://www.apache.org/dist/httpd/patches/apply_to_2.2.19/ (2.2.15～ 2.2.19)
http://www.apache.org/dist/httpd/patches/apply_to_2.0.64/ (2.0.55～ 2.0.64)

パッチが適用できない場合は、Range ヘッダを無効化する暫定的な対策を推奨します。以下のように httpd.conf に以下の記述を追加してください。なお、以下の暫定対策を行うと、ダウンロードツールやストリーミングビデオなどで不具合が発生する可能性がありますので、ご注意ください。

```
RequestHeader unset Range
```

また、http://httpd.apache.org/security/CVE-2011-3192.txt を参考にして、httpd.conf に以下の記述を追加してください。

Apache HTTP Server 2.2 系を利用している場合 (mod_setenvif と mod_headers が必要)

```
# Drop the Range header when more than 5 ranges.
# CVE-2011-3192
SetEnvIf Range (?:,.*?){5,5} bad-range=1
RequestHeader unset Range env=bad-range
```



```
# We always drop Request-Range; as this is a legacy
# dating back to MSIE3 and Netscape 2 and 3.
#
RequestHeader unset Request-Range

# optional logging.
CustomLog logs/range-CVE-2011-3192.log common env=bad-range
```

Apache HTTP Server 2.0 系を利用している場合（mod_rewrite と mod_headers が必要)

```
# Reject request when more than 5 ranges in the Range: header.
# CVE-2011-3192
#
RewriteEngine on
RewriteCond %{HTTP:range} !(^bytes=[^,]+(,[^,]+){0,4}$|^$) [NC]
RewriteRule .* - [F]

# We always drop Request-Range; as this is a legacy
# dating back to MSIE3 and Netscape 2 and 3.
#
RequestHeader unset Request-Range
```

(6) 備考

なし

4.2.4. Apache HTTP Server における HttpOnly 属性 Cookie の値を取得される脆弱性

(1) 危険度

Medium

(2) 脆弱性概要

400 Bad Request で自動生成されるエラーページ経由で、HttpOnly 属性のついた Cookie であってもクライアントサイドのスクリプトから読み取れてしまう脆弱性が検出されました(CVE-2012-0053)。

Apache HTTP Server の 2.2.21 及びそれ以前の 2.2 系のバージョンには、Apache HTTP Server 標準のステータスコード 400 のエラーページを使用している場合、HTTP ヘッダにサーバの制限値を超えた非常に長い文字列を含むリクエストを送信すると、問題のあるヘッダが Apache HTTP Server 標準のステータスコード 400 のエラーページに出力されるため、HttpOnly 属性の付いた Cookie の値がクライアントサイドのスクリプトによって取得可能になる脆弱性が存在します。

通常は、クロスサイトスクリプティングの脆弱性があっても HttpOnly 属性の Cookie が読み取られることはありませんが、この脆弱性を利用して、Cookie にサーバの制限値を超えた非常に長い文字列を付加してリクエストを送信すると、Apache HTTP Server 標準のステータスコード 400 のエラーページに Cookie の値が出力され、HttpOnly 属性の付いた Cookie を JavaScript から読み取ることが可能になります。

IP アドレス	ポート	詳細
192.168.1.1	80/tcp	(リクエスト) GET / HTTP/1.0 Connection: close Cookie: SESSIONID=sstdummy12345; z0=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA･･･(約１万文字続く) (レスポンス) HTTP/1.1 400 Bad Request Date: Wed, 29 Feb 2012 08:45:37 GMT Server: Apache/2.0.58 Connection: close Content-Type: text/html; charset=iso-8859-1 <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"> <html><head>

IP アドレス	ポート	詳細

		<title>400 Bad Request</title>
		</head><body>
		<h1>Bad Request</h1>
		<p>Your browser sent a request that this server could not understand.
		
		Size of a request header field exceeds server limit.
		
		<pre>
		Cookie: SESSIONID=sstdummy12345; z0=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA・・・(約 8000 文字続く)

	443/tcp	(リクエスト)
		GET / HTTP/1.0
		Connection: close
		Cookie: SESSIONID=sstdummy12345; z0=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA・・・(約 1 万文字続く)
		
		(レスポンス)
		HTTP/1.1 400 Bad Request
		Date: Wed, 29 Feb 2012 08:45:40 GMT
		Server: Apache/2.0.58
		Connection: close
		Content-Type: text/html; charset=iso-8859-1
		
		<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
		<html><head>
		<title>400 Bad Request</title>
		</head><body>
		<h1>Bad Request</h1>
		<p>Your browser sent a request that this server could not understand.
		
		Size of a request header field exceeds server limit.
		
		<pre>
		Cookie: SESSIONID=sstdummy12345; z0=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA・・・(約 8000 文字続く)

(3) IP アドレス

- 192.168.1.1

(4) 想定される脅威

Web アプリケーションにクロスサイトスクリプティングの脆弱性がある場合、HttpOnly 属性の付いた Cookie が攻撃者に漏えいする可能性があります。

(5) 対策

現時点で最新のバージョンである Apache HTTP Server 2.2.xx、または 2.4.x にアップグレードすることを推奨します。もしくは、ステータスコード 400 のカスタムエラーページを使用することを推奨します。

http://httpd.apache.org/

(6) 備考

この脆弱性は Apache HTTP Server 2.2.22 で修正されていることから、このホストの Apache HTTP Server のバージョンはそれより古いと考えられます。Apache HTTP Server 2.2.21 を含むそれ以前のバージョンにおいて複数の脆弱性が報告されているため、この Web サーバにもそれらの脆弱性が存在している可能性があります。

4.2.5. 第三者中継が可能な SMTP サービス

(1) 危険度

Medium

(2) 脆弱性概要

メールの第三者中継が可能な SMTP サービスが検出されました。

メールの第三者中継が可能な SMTP サービスは、スパムやウイルス等を送信する際に身元を隠すための踏み台として使用されます。

IP アドレス	ポート	詳細
192.168.1.2	25/tcp	# nc 192.168.1.2 25 HELO securesky-tech.com 220 host2.example.com ESMTPSendmail 8.12.11/8.12.11 250 host2.example.com Hello [210.189.108.67], pleased to meet you MAIL FROM: <webtest1@securesky-tech.com> 250 2.1.0 <webtest1@securesky-tech.com>... Sender ok **rcpt to: <sst46@securesky-tech.com>** **250 2.1.5 <sst46@securesky-tech.com>... Recipient ok** data 354 Enter mail, end with "." on a line by itself Open Relay Test . 250 2.0.0 xxxxxxxxxxxxx Message accepted for delivery quit 221 2.0.0 host2.example.com closing connection
	587/tcp	# nc 192.168.1.2587 HELO securesky-tech.com 220 host2.example.com ESMTPSendmail 8.12.11/8.12.11 250 host2.example.com Hello [210.189.108.67], pleased to meet you MAIL FROM: <webtest1@securesky-tech.com> 250 2.1.0 <webtest1@securesky-tech.com>... Sender ok **rcpt to: <sst46@securesky-tech.com>** **250 2.1.5 <sst46@securesky-tech.com>... Recipient ok** data 354 Enter mail, end with "." on a line by itself Open Relay Test .

		250 2.0.0 xxxxxxxxxxxxx Message accepted for deliv ery quit 221 2.0.0 host2.example.com closing connection

(3) IP アドレス

- 192.168.1.2

(4) 想定される脅威

スパムやウイルス等を送信する踏み台に利用される可能性があります。また、第三者中継が可能な SMTP サーバを収集している RBL.JP などのリストに登録されると、当該 SMTP サーバから送信される正規のメールが、スパムとして扱われ受信拒否される可能性があります。

(5) 対策

第三者中継を停止するような設定に変更することを推奨します。運用上の都合で第三者中継を停止できない場合は、個別のアドレスやドメインからのメールのみ中継を許可することや、IP アドレスでアクセス制限を行うなどの対策を推奨します。また、SMTP AUTH や POP before SMTP などを導入することで、外部から第三者中継を利用される可能性を低減することが可能です。

(6) 備考

なし

4.2.6. SSL バージョン 2 プロトコルのサポート

(1) 危険度

Medium

(2) 脆弱性概要

SSL バージョン 2 プロトコルのサポートが検出されました。SSL バージョン 2 プロトコルでは中間者攻撃によって通信を不正に操作される可能性があります。

IP アドレス	ポート	サポートしている SSL/TLS
192.168.1.1	80/tcp	・SSLv2 ・SSLv3 ・TLSv1
	443/tcp	・SSLv2 ・SSLv3 ・TLSv1

(3) IP アドレス

- 192.168.1.1

(4) 想定される脅威

通信を不正に操作される可能性があります。

(5) 対策

Apache HTTP Server を利用している場合

httpd.conf もしくは ssl.conf にある SSLCipherSuite ディレクティブの最後に「!SSLv2」を追加し、SSLv2 を有効化する「+SSLv2」は削除してください。

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

また、httpd.conf もしくは ssl.conf にある SSLProtocol ディレクティブに「+SSLv2」と書かれている場合は、「-SSLv2」に変更してください。


```
SSLProtocol all -SSLv2
```

(6) 備考

なし

4.2.7. Web サーバのバージョン情報

(1) 危険度

Low

(2) 脆弱性概要

Web サーバのバージョン情報が検出されました。

IP アドレス	ポート	検出箇所	バージョン情報
192.168.1.1	80/tcp	レスポンスヘッダ	Apache/2.0.58
	443/tcp	レスポンスヘッダ	Apache/2.0.58

(3) IP アドレス

- 192.168.1.1

(4) 想定される脅威

サーバにおけるシステム関連情報が漏えいします。

(5) 対策

Apache HTTP Server を利用している場合

httpd.conf の ServerTokens ディレクティブに Prod を設定することで、Server ヘッダへの Apache HTTP Server のバージョン情報の表示を抑制することが可能です。

```
ServerTokens Prod
```

また、httpd.conf の ServerSignature ディレクティブに Off を設定することで、エラーページへの Apache HTTP Server のバージョン情報の表示を抑制することが可能です。

```
ServerSignature Off
```


(6) 備考

なし

5 補足

5.1. お問合せについて

本報告書の内容に関するお問合せは、以下のメールアドレスまでご連絡ください。お問合せの対応期間は、報告書提出から 1 ヶ月以内に限らせていただきます。なお、電話や FAX でのお問合せは受付けておりませんので、ご了承ください。

example@example.com

5.2. 再診断について

弊社が指摘した脆弱性発生箇所をお客様にて修正された後に無料で再診断をご利用可能です。なお、再診断実施に当たっては以下の条件がございますので、ご注意ください。

- 再診断実施回数　1 回
- 期間　報告書提出から 1 ヶ月以内
- 診断箇所　弊社より指摘した脆弱性発生箇所(危険度 Medium 以上のもののみ)
- 成果物　報告書（報告会は実施しません）

5.3. 脆弱性の危険度判定基準

脆弱性の危険度の判定は、脆弱性に対する攻撃を受けた場合に起こりうる被害の大きさにより、以下の表のように 4 段階のレベルに分けております。

危険度	基準
Critical	確実にリモートからの侵入を許してしまう脆弱性
High	リモートからの侵入を許してしまう可能性のある脆弱性
Medium	情報漏えいやサービスの異常停止を許してしまうような脆弱性
Low	攻撃者に有用な情報を与えてしまうような脆弱性

なお、実際に被害が発生するかどうかは、脆弱性に対する攻撃が発生する頻度に影響を受けます。

