CONFIDENTIAL

SAMPLE

〇〇〇〇〇株式会社　御中

プラットフォーム診断
診断結果報告書

脆弱性診断後 10 営業日以内に提出いたします。本診断結報告書では診断結果の総括に加え、脆弱性と認められた根拠、脆弱点の技術的な対処方法・対策方法の説明を盛り込んでおります。

〇〇〇〇年〇月〇日

株式会社サイバーセキュリティクラウド

SAMPLE

【資料改編履歴】

日 付	内 容	承 認	作成/更新
○○○○年○月○日	第一版作成	○○	○○

目　　次

1　はじめに

本診断結果報告書は、〇〇〇〇年〇月〇日～〇日の期間で実施したプラットフォーム診断の診断結果についてご報告するものです。

1－1　目的

本診断の目的は、診断対象サーバに対して、インターネットを経由したリモートからの脆弱性診断を行い、インターネットからの不正アクセスに対するセキュリティ強度を確認することにあります。

また、脆弱性が検出された場合、そのリスク評価および脆弱性への対策を支援する情報の提供も行います。

1－2　診断期間および診断内容

本診断は、表 1-2-1 の日程で実施いたしました。

表 1-2-1　診断期間および診断内容

診断種別	診断期間	診断内容
リモート診断	〇〇〇〇年〇月〇日（10 時から 18 時まで）	リモートにて、脆弱性診断ツールによるポートスキャン及び脆弱性診断と、手動による情報収集・診断を実施しました。
	〇〇〇〇年〇月〇日（10 時から 18 時まで）	

1－3　診断対象

本診断における診断対象は以下の通りです。

No	IP アドレス	サーバ名	備考
1	192.168.1.1	公開用 Web サーバ	
2			
3			
4			

2　診断結果

2－1　総合評価

今回実施した診断の診断結果に基づき、弊社の評価基準に照合した総合評価を脆弱性診断に対して行いました。以下に評価クラスと評価の根拠となった診断結果を示します。

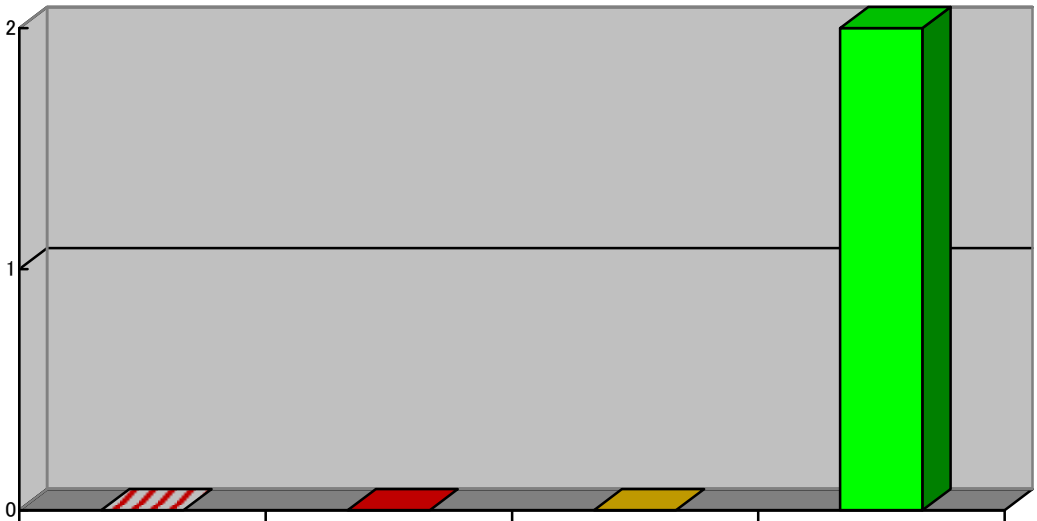
B	危険性の高い脆弱性は確認されておらず、公開サーバとしてセキュリティ上問題の少ない状態です。

- 危険性の高い脆弱性は確認されていません
- 「設定不備によるシステム情報漏洩」等の、軽微な脆弱性が検出されています

評価基準につきましては、付録の「6－3　評価基準」として添付しておりますので、必要に応じてご参照下さい。

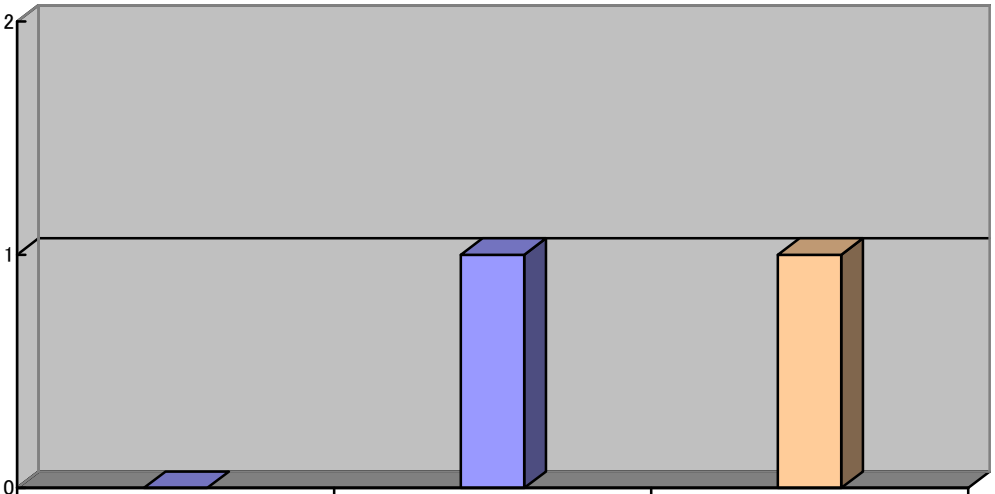
2－2　概要

本診断の診断対象範囲において検出された脆弱性を危険度別に集計したものを図 2-2-1　危険度別脆弱性検出数に、診断項目別に集計したものを図 2-2-2　診断項目別脆弱性検出数、表 2-2-1　診断項目別脆弱性検出数一覧に示します。



	Critical	High	Medium	Low
192.168.1.1	0	0	0	2

図 2-2-1　危険度別脆弱性検出数



	サーバプログラムのバージョン取得	設定不備によるシステム情報漏洩	既知の脆弱性による情報漏洩
192.168.1.1	0	1	1

図 2-2-2　診断項目別脆弱性検出数

表 2-2-1　診断項目別脆弱性検出数一覧

カテゴリ	診断項目	危険度	192.168.1.1
不正侵入	不正なログイン	-	0
	プログラム実行	-	0
	特権ユーザ権限の奪取	-	0
	アクセス制御の不備	-	0
	バックドアプログラムの存在	-	0
サービス妨害	サービス妨害・停止	-	0
	DDoS エージェントの存在	-	0
情報漏洩	ファイル取得	-	0
	不要なサービスの動作	-	0
	サーバプログラムのバージョン取得	-	0
	設定不備によるシステム情報漏洩	Low	1
	既知の脆弱性による情報漏洩	Low	1
	盗聴による情報漏洩	-	0
合　計		Critical	0
		High	0
		Medium	0
		Low	2

本診断において、サーバの設定不備や既知の脆弱性等により、システム情報が漏洩する危険度 Low の軽微な脆弱性が検出されておりますが、サーバの設定変更で対策を実施することが可能なことから、メンテナンスのタイミング等での対策を検討することを推奨します。

危険度につきましては、付録の「6－2　危険度の判定基準」として添付しておりますので、必要に応じてご参照下さい。

3　診断結果詳細

本章では、検出された脆弱性について解説を行います。

3−1　推測可能な SNMP コミュニティ名の使用

診断項目	設定不備によるシステム情報漏洩
危険度	Low
対象サーバ	192.168.1.1 [161/udp]

対象サーバにおいて、推測可能なコミュニティ名による SNMP プロトコルでの情報取得が可能であることを確認しております。

SNMP（Simple Network Management Protocol）とは、ネットワークに接続された通信機器（ルータやコンピュータ等）をネットワーク経由で監視・制御するためのプロトコルです。
SNMP におけるコミュニティ名は、監視・制御の対象機器と通信する際に使用されるものでパスワードと同じように重要な意味を持つものです。
SNMP 製品の多くはデフォルト値として public を使用していることから、コミュニティ名をデフォルト値のまま使用している場合、ネットワーク機器に関するシステム情報等が漏洩する可能性があります。

図 3-1-1 および図 3-1-2 は、192.168.1.1 の UDP ポート番号 161 に対して snmpwalk コマンドを用いて情報の取得を行った結果です。
デフォルト値のコミュニティ名 public を指定して snmpwalk コマンド（図 3-1-1）を実行した結果、対象サーバより情報が取得されることから（図 3-1-2）、デフォルトのコミュニティ名 public が有効であることを確認できます。

```
snmpwalk -v 1 -c public 192.168.1.1
```

図 3-1-1　コミュニティ名をデフォルト値の public と指定した snmpwalk コマンド

```
SNMPv2-MIB::sysDescr.0 = STRING: Linux www2 2.6.32-131.17.1.el6.x86_64 #1 SMP Thu
 Sep 29 10:24:25 EDT 2011 x86_64
SNMPv2-MIB::sysObjectID.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (192103548) 22 days, 5:37:15.48
SNMPv2-MIB::sysContact.0 = STRING: Root <root@localhost> (configure /etc/snmp/snmp.lo
cal.conf)
SNMPv2-MIB::sysName.0 = STRING: www2
…（以下省略）…
```

図 3-1-2　図 3-4-1 の snmpwalk コマンドを実行した結果（192.168.1.1 の応答）

図 3-1-2 の出力結果より、Linux のカーネルバージョンを始めとしたシステム情報が容易に取得可能な状態であることから、SNMP のコミュニティ名について推測困難な文字列に変更するか、UDP ポート番号 161 へのアクセス制限を行うことを推奨します。

対象サーバでは NET-SNMP が使用されていることから、設定ファイル snmpd.conf の com2sec セクションの設定によりデフォルトコミュニティ名の変更が可能です。

詳細については、以下のページをご参照下さい。

SNMPD.CONF:Section: Net-SNMP (5)
http://www.net-snmp.org/docs/man/snmpd.conf.html

検出箇所の詳細情報につきましては「5　脆弱性詳細」をご参照下さい。

3－2　TLS 1.0 が有効

診断項目	既知の脆弱性による情報漏洩
危険度	Low
対象サーバ	192.168.1.1 [443/tcp]

対象サーバに TLS 1.0 プロトコルでアクセスした結果、通信可能であることを確認しております。

TLS 1.0 プロトコルには、第三者によるマン・イン・ザ・ミドル攻撃（中間者攻撃）によって通信内容を傍受される脆弱性があることが公表されております。
詳しくは以下の情報をご参照下さい。

NVD - CVE-2014-8730
https://nvd.nist.gov/vuln/detail/CVE-2014-8730

SSL 3.0 Protocol Vulnerability and POODLE Attack
https://www.us-cert.gov/ncas/alerts/TA14-290A

SSL および初期の TLS からの移行
https://ja.pcisecuritystandards.org/_onelink_/pcisecurity/en2ja/minisite/en/docs/Migrating-from-SSL-Early-TLS-Info-Supp-v1_1.pdf

図 3-2-1 は、対象サーバの TCP ポート番号 443 にアクセスした際に確認された「TLS 1.0 が有効」について検証を行ったものです。

対象サーバに TLS 1.0 プロトコルでの通信を試みた結果、エラーとならずに正常に通信が行われることを確認（図 3-2-1）できます。

```
# openssl s_client -host 192.168.1.1 -port 443 -tls1
CONNECTED(00000003)
（中略）---
---
No client certificate CA names sent
Server Temp Key: ECDH, P-256, 256 bits
```

図 3-2-1　対象サーバに TLS 1.0 プロトコルでアクセスした際の通信内容（抜粋）

```
---
SSL handshake has read 3540 bytes and written 301 bytes
---
New, TLSv1/SSLv3, Cipher is ECDHE-RSA-AES256-SHA
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol  : TLSv1
    Cipher    : ECDHE-RSA-AES256-SHA
    Session-ID: 5C6B746D83FDA4B7C598BB766B6F4D095A51BDB06364FCEEEF4C0085FE93F825
    Session-ID-ctx:
    Master-Key: B744867EE4C81C6345D5342C5D59A5E7D60A5F9BE5D7DD6B1231F137D40DA7778
318C5193355544ACEFA42DF6C4A9C4C
    Key-Arg   : None
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    Start Time: 1550546029
    Timeout   : 7200 (sec)
    Verify return code: 0 (ok)
---
HEAD / HTTP/1.0

HTTP/1.1 200
Set-Cookie: JSESSIONID=FF67F830CEB2147A78827CEFDCD8D91A; Path=/; Secure; HttpOnly
Content-Type: text/html;charset=UTF-8
Date: Mon, 18 Feb 2019 03:13:57 GMT
Connection: close

closed
```

図 3-2-1　対象サーバに TLS 1.0 プロトコルでアクセスした際の通信内容（抜粋）（続き）

マン・イン・ザ・ミドル攻撃は攻撃を成功させることが容易ではないため、現時点では危険度は高いものではありませんが、現在普及している多くの Web ブラウザ（Microsoft Internet Explorer 7 以降

や Mozilla Firefox 2.0 以降）ではより上位の TLS 1.2 が使用可能であることから、TLS 1.0 プロトコルにつきましては Web サーバ等の設定により無効にすることを推奨します。

Web サーバに Microsoft IIS（Internet Information Services）が使用されている場合、レジストリ内容の変更により今回検出された TLS 1.0 プロトコルでの通信を無効にすることが可能ですので、修正を行うことを推奨します。

詳細については、以下のページをご参照下さい。

インターネット インフォメーション サービスで PCT 1.0、SSL 2.0、SSL 3.0、または TLS 1.0 を無効にする方法
https://support.microsoft.com/ja-jp/help/187498/how-to-disable-pct-1-0-ssl-2-0-ssl-3-0-or-tls-1-0-in-internet-information

SSL/TLS 暗号設定ガイドライン～安全なウェブサイトのために（暗号設定対策編）～
https://www.ipa.go.jp/security/ipg/documents/ipa-cryptrec-gl-3001-2.0.pdf

SSL/TLS 暗号設定 サーバ設定編
https://www.ipa.go.jp/security/ipg/documents/ssltls_server_config_20150803.pdf

検出箇所の詳細情報につきましては「5　脆弱性詳細」をご参照下さい。

4　総括

本診断の結果、危険性の高い脆弱性は確認されていないことから、各診断対象サーバにおいては安全な状態にあると考えられます。検出された脆弱性はいずれも設定等の問題であり軽微なものですが、システムについての推測等に利用される可能性があることから、設定変更等による対策の実施を推奨します。

運用中のサーバでは、サービスの安定運用を優先しセキュリティ対策が遅くなる傾向にありますが、現在では脆弱性が確認されてから実証コードや実際に悪用が始まるまでの期間が短くなっており、脆弱性を放置することにより不正アクセスの被害を受ける危険性が高くなります。

近年の攻撃トレンドはウイルスやワームなどのように不特定多数に無差別攻撃を仕掛ける方法は減少しつつあり、攻撃対象を絞って Web アプリケーションを狙う攻撃が増加傾向にありますが、DNS サーバ BIND の脆弱性のように、影響が広範囲に渡る脆弱性が公開される場合もあるため、物理レベル、ネットワークレベル、アプリケーションレベル、それぞれのレイヤーにおいて一定水準のセキュリティを保つことが重要です。

以上で本報告を総括させて頂きますが、本診断報告書について指摘された脆弱性を修正するのみではなく、今後のセキュリティ対策に活用して頂ければ幸いです。

5　脆弱性詳細

本章では、本診断で検出された脆弱性の詳細を示します。

なお、「ポートスキャン結果一覧」に記載されているサービスポートの状態については表 5-1 をご参照下さい。

表 5-1　サービスポートの状態

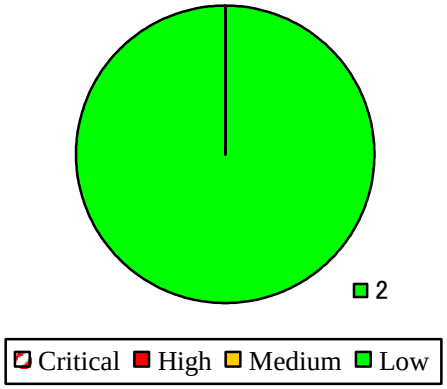
状態	意味
open	診断対象 IP アドレスのホストにおいてサービスポートが開いている状態を表します。 ファイアウォールについてもフィルタされずに通過している状態です。
closed	診断対象 IP アドレスのホストにおいてサービスポートが閉じている状態を表します。 診断元 IP アドレスのホストに対して閉じていることを確認可能な応答パケットがあったことを示しているため、ファイアウォールについてはフィルタされずに通過している状態です。
filtered	ファイアウォールやその他パケットフィルタ等によりフィルタされている状態を表します。
open/filtered	診断対象 IP アドレスのホストにおいてサービスポートが開いているか、もしくはファイアウォール等によりパケットがフィルタされている状態を表します。 ICMP や UDP 等、サービスが開いていても特に応答を返さない、もしくは意図的に応答を返さないように設定される可能性のあるサービスでは、診断元 IP アドレスのホストからはサービスが開いているのか、パケットがフィルタされたのか判別することが困難なため、このような状態で表すことになります。

また「ポートスキャン結果一覧」のサービス名は、ポートスキャンに使用した nmap の nmap-services ファイルによるものです。

5－1　192.168.1.1

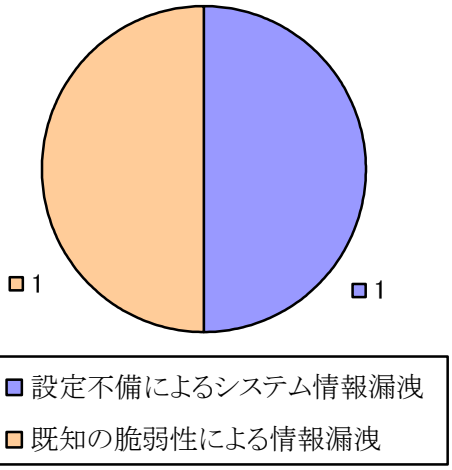
脆弱性危険度別検出数一覧／分布

危険度	検出数
Critical	0
High	0
Medium	0
Low	2
合計	2



診断項目別検出数一覧／分布

カテゴリ	診断項目	検出数
不正侵入	不正なログイン	0
	プログラム実行	0
	特権ユーザ権限の奪取	0
	アクセス制御の不備	0
	バックドアプログラムの存在	0
サービス妨害	サービス妨害・停止	0
	DDoS エージェントの存在	0
情報漏洩	ファイル取得	0
	不要なサービスの動作	0
	サーバプログラムのバージョン取得	0
	設定不備によるシステム情報漏洩	1
	既知の脆弱性による情報漏洩	1
	盗聴による情報漏洩	0
その他	その他	0
合計		2



ポートスキャン結果一覧

ICMP

パケット送信の結果、対象サーバより応答が返らないことを確認しております。

TCP

ポートスキャンの結果、以下のサービスポートについて応答が返ることを確認しております。

ポート	状態	サービス名	備考（バージョン情報等）
22/tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)
80/tcp	open	http	Apache httpd
443/tcp	closed	https	

※ 上記以外のサービスポートは全て filtered です。

UDP

ポートスキャンの結果、以下のサービスポートについて応答が返ることを確認しております。

ポート	状態	サービス名	備考（バージョン情報等）
161/udp	open	snmp	

※ 上記以外のサービスポートは全て open/filtered です。

但し UDP ポートの場合ネットワークや対象サービスの状態により正しく結果を評価することが出来ない場合がありますので、予めご了承下さい。

指摘事項

推測可能な SNMP コミュニティ名の使用

診断項目：設定不備によるシステム情報漏洩

概要

対象サーバにおいて、推測可能なコミュニティ名による SNMP プロトコルでの情報取得が可能であることを確認しております。

SNMP（Simple Network Management Protocol）とは、ネットワークに接続された通信機器（ルータやコンピュータ等）をネットワーク経由で監視・制御するためのプロトコルです。

SNMP におけるコミュニティ名は、監視・制御の対象機器と通信する際に使用されるものでパスワードと同じように重要な意味を持つものです。

SNMP 製品の多くはデフォルト値として public を使用していることから、コミュニティ名をデフォルト値のまま使用している場合、ネットワーク機器に関するシステム情報等が漏洩する可能性があります。

対策

SNMP のコミュニティ名について推測困難な文字列に変更するか、UDP ポート番号 161 へのアクセス制限を行うことを推奨します。

対象サーバでは NET-SNMP が使用されていることから、設定ファイル snmpd.conf における com2sec セクションの設定によりデフォルトコミュニティ名の変更が可能です。

詳細については、以下のページをご参照下さい。

SNMPD.CONF:Section: Net-SNMP (5)
http://www.net-snmp.org/docs/man/snmpd.conf.html

対象

対象サーバ [対象ポート]
192.168.1.1 [161/udp]

危険度
Low

検出根拠
対象サーバ[ポート]に対して、snmpwalk コマンドのコミュニティ名に public を指定して SNMP プロトコル通信を試みた結果、システム情報を含む応答が返ることを確認しました。

```
SNMPv2-MIB::sysDescr.0 = STRING: Linux www2 2.6.32-131.17.1.el6.x86_64 #1 SMP
 Thu Sep 29 10:24:25 EDT 2011 x86_64
SNMPv2-MIB::sysObjectID.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (192103548) 22 days, 5:37:15.4
8
SNMPv2-MIB::sysContact.0 = STRING: Root <root@localhost> (configure /etc/snmp/sn
mp.local.conf)
SNMPv2-MIB::sysName.0 = STRING: www2
…（以下省略）…
```

	備考
	なし

TLS 1.0 が有効

診断項目：既知の脆弱性による情報漏洩

概要

TLS 1.0 プロトコルが有効になっていることを確認しております。

TLS 1.0 プロトコルには、第三者によるマン・イン・ザ・ミドル攻撃（中間者攻撃）によって、通信内容を傍受される脆弱性があることが公表されております。
詳しくは以下の情報をご参照下さい。

NVD - CVE-2014-8730
https://nvd.nist.gov/vuln/detail/CVE-2014-8730

SSL 3.0 Protocol Vulnerability and POODLE Attack
https://www.us-cert.gov/ncas/alerts/TA14-290A

SSL および初期の TLS からの移行
https://ja.pcisecuritystandards.org/_onelink_/pcisecurity/en2ja/minisite/en/docs/Migrating-from-SSL-Early-TLS-Info-Supp-v1_1.pdf

本脆弱性を悪用した攻撃には、パケット盗聴や通信経路上のサーバへの不正侵入のような、特殊な条件が必要になることから、危険性は低いものと考えられますが、利用者が十分に安全に設定されていない無線 LAN 環境から対象サイトを利用する等により、実際に影響を受ける可能性もありますので、TLS 1.0 プロトコルについては無効にすることを推奨します。

対策

Web サーバに Microsoft IIS（Internet Information Services）が使用されている場合、レジストリ内容の変更により今回検出された TLS 1.0 プロトコルでの通信を無効にすることが可能ですので、修正を行うことを推奨します。

詳細については、以下のページをご参照下さい。

インターネット インフォメーション サービスで PCT 1.0、SSL 2.0、SSL 3.0、または TLS 1.0 を無効にする方法

https://support.microsoft.com/ja-jp/help/187498/how-to-disable-pct-1-0-ssl-2-0-ssl-3-0-or-tls-1-0-in-internet-information

SSL/TLS 暗号設定ガイドライン～安全なウェブサイトのために（暗号設定対策編）～

https://www.ipa.go.jp/security/ipg/documents/ipa-cryptrec-gl-3001-2.0.pdf

SSL/TLS 暗号設定 サーバ設定編

https://www.ipa.go.jp/security/ipg/documents/ssltls_server_config_20150803.pdf

対象

対象サーバ [対象ポート]
192.168.1.1 [443/tcp]

危険度
Low
検出根拠
対象アドレス/ポートに対して、TLS 1.0 プロトコルでの通信を試みた結果、エラーとならずに対象サーバとの通信が可能となることを確認しました。
備考
なし

6　付録

6－1　診断項目一覧

本診断において行った診断項目一覧を以下に示します。

不正侵入

不正侵入が想定される脆弱性に関わる診断を行います。

項目名	内容
不正なログイン	ログイン権限を持たない、もしくは、正規のユーザでないユーザが不正にログイン出来ることが想定される脆弱性に関わる診断を行います。デフォルトアカウント（アプリケーションインストール時等に自動的に登録されるアカウント）の放置や、脆弱なパスワードを持つアカウント等、不適切なユーザ管理についての診断を含みます。
リモートからのプログラム実行	リモートから不正なプログラムを実行可能なことが想定される脆弱性に関わる診断を行います。
特権ユーザ権限の奪取	一般ユーザから正規の手順以外の方法で管理者権限やその他特別な権限を取得することが想定される脆弱性に関わる診断を行います。
アクセス制御の不備	主にリモートからの診断において、ファイアウォールやルータ等によるアクセス制御設定が適切であるかどうか診断を行います。
バックドアプログラムの存在	バックドア（裏口）プログラムが動作していないか診断を行います。

サービス妨害

動作しているサービスを妨害もしくは停止させることが想定される脆弱性に関わる診断を行います。

項目名	内容
サービス妨害・停止	サービスを妨害もしくは停止される可能性のある脆弱性について診断を行います。なお、本項目での診断では実際に攻撃は行わず、主にサーバのバージョン情報等から脆弱性を推測して検出します。
DDoS エージェントの存在	DDoS（分散型サービス妨害攻撃）に使用されるエージェントプログラムが動作していないか診断を行います。

情報漏洩

システム情報、ユーザ情報等の漏洩が想定される脆弱性に関わる診断を行います。

項目名	内容
リモートからのファイル取得	リモートからファイルが取得可能な脆弱性について診断を行います。主に NFS（Network File System）や FTP（File Transfer Protocol）、Windows のファイル共有等、リモートホスト間でファイルを送受信することが可能なサービスの設定不備によるファイル取得について検出を行います。
不要なサービスの動作	ポートスキャンを行い、一般的に動作させておく必要が無いと思われるサービスが動作していないか診断を行います。
サーバプログラムのバージョン取得	ヘッダ情報等によるサービスプログラムのバージョンの取得について診断を行います。
設定不備によるシステム情報漏洩	OS やサーバプログラムの設定不備によるシステム・ユーザ情報漏洩の存在について診断を行います。
既知の脆弱性による情報漏洩	FTP サーバや Web サーバ等、サーバ事態に存在する基地の脆弱性による情報漏洩について診断を行います。

6－2　危険度の判定基準

本報告書では検出された各脆弱性について、表 6-2-1 を基に危険度を判定し記載しています。

危険度は、検出された各脆弱性への対策の際に、どの脆弱性を優先的に修正すべきか判断するための目安として記載しているものです。

表 6-2-1　危険度の判定基準

危険度	判定基準
Critical	ネットワーク経由で管理権限を奪取される等、深刻な被害を受けることが懸念される脆弱性。
High	潜在的に重大な被害を受ける可能性のある脆弱性。
Medium	単体では被害を受ける可能性は低いが、他の脆弱性と組み合わせることで被害を受けることが想定される脆弱性。
Low	Medium 以上には該当しない、現時点では被害を受ける可能性が低いと考えられる脆弱性。

判定基準はあくまでも目安であり、脆弱性の検出された箇所・内容等により判定基準とは異なる危険度を脆弱性に与えることもありますので、ご了承下さい。

6－3　評価基準

本報告書における総合評価は、表 6-3-1 に規定される絶対評価と、診断対象の環境を考慮して評価される相対評価によるものです。

絶対評価は、A、B、C、D のいずれかのアルファベット 1 文字で表記され、診断結果を絶対評価の評価基準に照合し適合するクラスが評価として与えられます。

表 6-3-1　絶対評価の評価基準

クラス	評価基準
A	脆弱性が検出されていない。
B	システム情報の漏洩を始めとした、単体では被害を受ける可能性が低いと考えられる脆弱性以外の検出が無い。
C	危険性の高い脆弱性が検出されており、被害を受ける可能性がある。
D	個人情報の漏洩に繋がる深刻な脆弱性が検出されている。または、検出されている複数の脆弱性を組み合わせることで個人情報の漏洩に繋がることが懸念される状態である。

相対評価は、絶対評価では表すことが出来ない診断対象の環境やリスト対象等、外的要因について考慮されて評価されるものであり、＋（プラス；より安全）、－（マイナス；より安全でない）を絶対評価に付与することで表されます。

なお、上記評価基準は、弊社の診断実績を基に、診断結果を簡潔に表現するために作成された、弊社独自基準になります。上記評価基準による評価は、あくまでも診断結果を簡潔に表現するためのものであり、弊社は評価に対しての保証や責任は負いかねますのでご了承下さい。

以上