CONFIDENTIAL

SAMPLE

〇〇〇〇〇株式会社　御中

サーバ構成診断
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.....1
1－1　目的.....1
1－2　診断期間および診断内容.....1
1－3　診断対象.....1

2　診断結果.....2
2－1　総合評価.....2
2－2　概要.....3

3　診断結果詳細.....6
3－1　脆弱なパスワードを持つアカウントの存在.....6
3－2　セキュリティパッチの未適用.....7
3－3　脆弱性の存在するアプリケーションの利用.....9
3－4　Everyone グループに書き込みが許可されたファイル・ディレクトリの存在.....10
3－5　パスワードポリシーに関する設定不備.....11

4　総括.....13

5　危険度の判定基準.....14
5－1　Web1.....14

6　付録.....20
6－1　診断項目一覧.....20
6－2　危険度の判定基準.....23
6－3　評価基準.....24

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サーバ構成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、診断対象サーバにおける設定内容や稼動状況の確認を行い、サーバ構成上の脆弱性を特定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
オンサイト診断	〇〇〇〇年〇月〇日（10 時から 18 時まで）	オンサイトにて、脆弱性診断ツールによるポ脆弱性診断と、手動による情報収集・診断を実施しました。

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	web1	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。

D	危険性の高いセキュリティ上の問題が複数確認されており、対策が必要な状態です。

- 脆弱性なパスワードを持つアカウントが複数確認されています
- 危険性の高い脆弱性に対するセキュリティパッチが未適用な状態です
- 脆弱性の存在が報告されている古いバージョンのアプリケーションが存在しています

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。

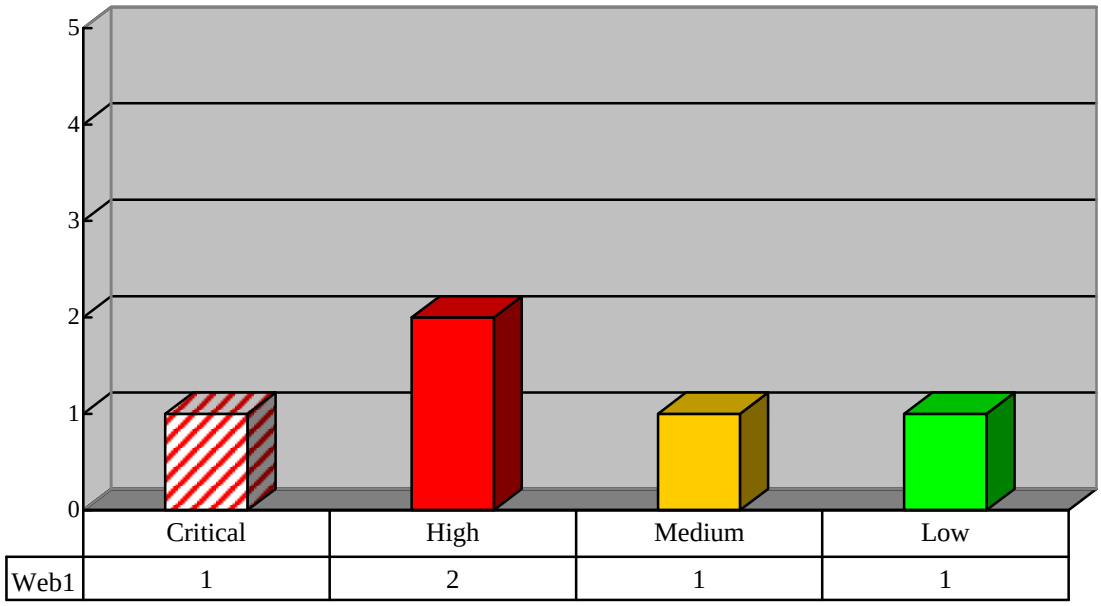


図 2-2-1　危険度別脆弱性検出数

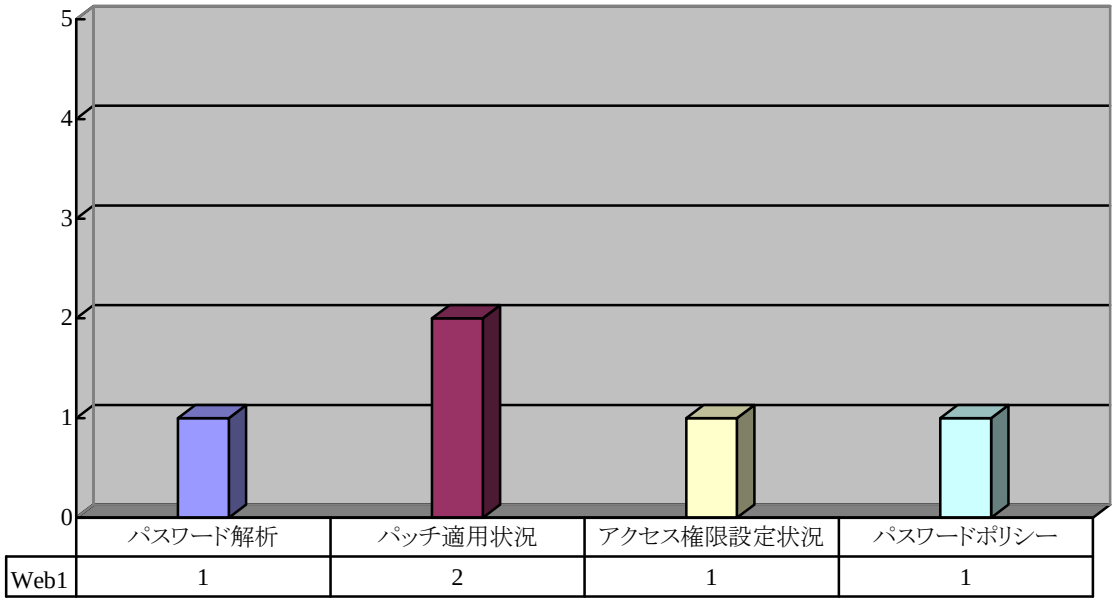


図 2-2-2　診断項目別脆弱性検出数

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	Web1
サーバ設定状況	パスワード解析	Critical	1
	パッチ適用状況	High	2
	アクセス権限設定状況	Medium	1
	カーネルパラメータの設定状況	-	-
	管理者権限のアカウント設定状況	-	-
	アクセスコントロール設定状況	-	-
	アプリケーション設定状況	-	-
サーバ稼働状況	稼働サービス	-	-
	稼働プロセス	-	-
	稼働ポート	-	-
	稼働ネットワーク	-	-
Windows セキュリティポリシー	ローカルセキュリティポリシー	-	-
	パスワードポリシー	Low	1
	アカウント関連ポリシー	-	-
	監査（ログ）ポリシー	-	-
	権限の割当ポリシー	-	-
	セキュリティオプション	-	-
合計		Critical	1
		High	2
		Medium	1
		Low	1

本診断において、脆弱なパスワードを持つアカウントが複数確認されております。

パスワード認証は最も基本的なセキュリティ機構であり、OS のパスワードは多くのサービスで使用されていることから、脆弱なパスワードが存在することで不正侵入を許す懸念があります。

組織内でパスワードポリシーを作成し周知する、モジュールや OS の設定等で脆弱なパスワードの設定を拒否するよう設定する等の対策を行い、脆弱なパスワードが設定されない運用を行うことを推奨します。

また、OS のセキュリティパッチや OS 以外のアプリケーションのバージョンアップが適切に実施されていないことを確認しております。

現在ではセキュリティホールが確認されてから実証コードの公開や実際に悪用が行われるまでの時間が短くなる傾向にあり、セキュリティホールを放置することによるリスクが高くなっております。

特に Web ブラウザやブラウザプラグインの脆弱性は、Gumblar に代表される Web サイトを改竄するウイルス／ワームに悪用されることが多く、脆弱性の放置は潜在的に大きなリスクを負っていると考えられます。

本診断の診断対象はいずれもサーバホストであることから、Web ブラウザを使用することは少ないと推測されますが、万が一使用された場合のことも考え、適切にパッチ適用・バージョンアップを実施することを推奨します。

本診断の結果から、今後の対策として

- 診断結果を元に、緊急性の高い脆弱性から対策を実施
- 定期的な構成診断を行うことで、サーバにおける設定内容や稼動状況の確認実施
- セキュリティホール情報を常に収集し、パッチ適用・バージョンアップを潤滑に実施出来るような運用ルールの検討

- セキュリティホール情報を常に収集し、パッチ適用・バージョンアップを潤滑に実施出来るような運用ルールの検討

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　脆弱なパスワードを持つアカウントの存在

対象サーバ	web1
検査項目	パスワード解析
危険度	Critical

診断対象サイトにおいて、脆弱なパスワードを持つアカウントが存在することを確認しています。

現時点までの解析で検出された、脆弱なパスワードが設定されているアカウントの一覧を表 3-1-1 に示します。ホスト名やアカウント名等がパスワードの一部もしくは全部に使用されており、推測可能であることを確認できます。

表 3-1-1　脆弱なパスワードが設定されているアカウント

対象サーバ	アカウント名	パスワード	備考
web1	root	toor	アカウントから類推可能なパスワード
	tanaka	tanakaweb1	アカウントとホスト名から類推可能なパスワード

脆弱なパスワードを持つアカウントが存在する場合には、コンソールからの不正ログインのみならず、ログイン認証を利用するネットワークサービス経由での不正ログインも考えられます。

一般ユーザ権限のアカウントであっても、他の脆弱性を併用して一般ユーザ権限から特権ユーザへの権限上昇が行われることも考えられることから、早急に推測困難なパスワードへ変更することを推奨します。

3−2　セキュリティパッチの未適用

対象サーバ	web1
検査項目	パッチ適用状況
危険度	High

診断対象サイトにおいて、OS ベンダから公開されているセキュリティパッチが未適用であることを確認しています。

一般的に、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パッチの適用が遅くなる傾向にありますが、現在ではセキュリティホール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いる傾向にあり、セキュリティホールを放置することによるリスクが高くなってきています。

今回の診断対象は、数年前からのセキュリティパッチが適用されないまま運用されている傾向にあります。安定運用優先させるため、サーバが稼動するネットワーク環境や、サーバ上で利用するアプリケーション環境等を考慮した上での現状かと推測しますが、もし可能であれば、セキュリティ情報の公開から検証・適用までの手順をマニュアル化する等、可能な限りセキュリティパッチ未適用の状態の期間を減らすような対策を検討することを推奨します。

Web1 で使用されている Windows Server 2008 R2 については、Microsoft が提供している MBSA（Microsoft Baseline Security Analyzer）を使用してセキュリティパッチ適用状況を確認することを推奨します。
MBSA について、詳しくは以下のページをご参照下さい。

Microsoft Baseline Security Analyzer (MBSA)
http://technet.microsoft.com/ja-jp/security/cc184924.aspx

なお、弊社ではセキュリティ情報を総合的に収集・確認を行えるセキュリティホール情報サイト SIDfm（https://sid.softek.co.jp/）も提供しておりますので、必要に応じてご利用をご検討下さい。

Web1 において確認されたセキュリティパッチの未適用について、代表的なものを表 3-2-1 に示します。

表 3-2-1　未適用なセキュリティパッチ一覧

文書番号	技術情報番号	文書名	深刻度	公開日	最終更新日
MS12-035	KB2604121 KB2604111	.NET Framework の脆弱性により、リモートでコードが実行される (2693777)	緊急	2012/05/08	2012/05/15
MS12-034	KB2656405 KB2658846	Microsoft Office、Windows、.NET Framework、Silverlight 用のセキュリティ更新プログラムの組み合わせ (2681578)	緊急	2012/05/09	2012/05/09
MS12-033	KB2690533	Windows Partition Manager の脆弱性により、特権が昇格される (2690533)	重要	2012/05/09	2012/05/09
MS12-032	KB2688338	TCP/IP の脆弱性により、特権が昇格される (2688338)	重要	2012/05/09	2012/05/11

また、セキュリティパッチの未適用一覧については、以下の添付資料をご参照下さい。

「添付資料 3-2-1_未適用セキュリティパッチ一覧(Web1)」

3−3　脆弱性の存在するアプリケーションの利用

対象サーバ	web1
検査項目	パッチ適用状況
危険度	High

診断対象サーバにインストールされているアプリケーションについて、脆弱性が存在するバージョンが使用されていることを確認しております。

診断対象サーバにおいて確認された、既に脆弱性が公開されているアプリケーションの一覧を表 3-3-1 に示します。

表 3-3-1　脆弱性の存在するアプリケーションの一覧

対象サーバ	アプリケーション名	インストールされているバージョン	脆弱性が確認されているバージョン（※1）	最新バージョン
Web1	Adobe Flash Player	10.0.42.34	10.2.159.1	10.3.181.14
	Adobe Reader	9.0.0	9.4.3	9.4.4
	Adobe Shockwave Player	11.5.2.602	11.5.9.615	11.5.9.620
	Tera Term	4.66	4.68	4.69

※1　記載されているバージョンとそれ以前のバージョンで脆弱性が確認されています。

サーバにサードパーティ製品やフリーのアプリケーションをインストールする場合、セキュリティのチェックも管理者が自分で行う必要があります。

もし不要なアプリケーションであればアンインストール、必要なアプリケーションであれば定期的にアプリケーションのサポートページから脆弱性の情報を収集しアプリケーションの更新を行うことを推奨します。

3−4　Everyone グループに書き込みが許可されたファイル・ディレクトリの存在

対象サーバ	web1
検査項目	アクセス権限設定状況
危険度	Medium

診断対象サーバにおいて、Everyone グループに書き込みが許可されたファイルやディレクトリが存在することを確認しています。

Everyone グループに書き込みが許可されている場合、システム上の任意のユーザの権限でファイルの操作や作成等が可能となり、特権の奪取やサービスの妨害、ログの改竄等の影響を受ける可能性があります。

少なくとも任意のユーザが書き込み可能とならないよう、ファイルのパーミッションを変更することを推奨します。
なお、アプリケーションによっては意図的に任意のユーザに書き込みを許可している場合もありますので、十分な検証・確認を行った上でパーミッションの変更を行うかご検討下さい。

診断対象サーバにおいて確認された、Everyone グループに書き込みが許可されたファイル・ディレクトリの一覧については、以下の添付資料の内容をご参照下さい。

「添付資料 3-4-1_Everyone グループに書き込みが許可されたファイルディレクトリ一覧(Web1)」

3−5　パスワードポリシーに関する設定不備

対象サーバ	web1
検査項目	パスワードポリシー
危険度	Low

診断対象サーバにおいて、パスワードポリシーに対する設定内容が十分なセキュリティ強度を保持する内容でないことを確認しています。

パスワードポリシーに対する設定内容が、十分なセキュリティ強度を保持する内容ではないことが確認された一覧を表 3-5-1 に示します。なお、Microsoft による推奨値があるものについては合わせて記載しています。

Microsoft の推奨値と比較した場合、パスワードのポリシーに関する設定内容がセキュリティ的に強度の低い設定が行われている傾向にあります。
パスワードのポリシーが不適切な場合には、安全でないパスワードの設定が許可されることで、システムのセキュリティレベルを下げる結果となることがあります。

表 3-5-1　確認された「パスワードのポリシー」の設定

サーバ名	設定名称	設定値	推奨値
Web1	パスワードの長さ	0 文字以上	8 文字以上
	パスワードの変更禁止期間	0 日	1 日間
	パスワードの有効期間	42 日	42 日間
	パスワードの履歴を記録する	0 回	24 回
	パスワードは要求する複雑さを満たす	無効	有効

「パスワードの長さ」、「パスワードの有効期間」、「パスワードは要求する複雑さを満たす」等のパスワードのポリシーに関する設定内容について、再度ご確認をいただくことを推奨いたします。

なお、「パスワードの有効期限」については、設定した期間毎にパスワードの再設定を要求されるようになりますので、推奨値に固執せず運用に合わせて設定を行うようご注意下さい。

詳しくは以下のページをご参照下さい。

Windows Server 2003 セキュリティ ガイド　第 3 章 :ドメイン ポリシー　パスワードポリシー
http://www.microsoft.com/japan/technet/security/prodtech/windowsserver2003/w2003hg/s3sgch03.mspx#E4D

４　総括

本診断の結果から、内部からの不正アクセスによる侵入や攻撃を受ける可能性のある脆弱性（脆弱なパスワードを持つアカウントの存在、セキュリティパッチの未適用等の危険性の高い脆弱性が確認されております。

昨年あたりから、標的型攻撃によるサイバー攻撃が多発しており、その被害が深刻化の一途を辿っています。今後不正アクセスのリスクは増大していくことが懸念されますので、診断結果を元に緊急性の高い脆弱性から対策を実施することを推奨します。

個人情報漏洩や不正侵入により組織が受ける被害・損失は、直接的（個人に対するお詫び金、サーバ再構築費用、セキュリティ対策費用等）・間接的（ブランドイメージの悪化等）に多大なものになることが想定されますので、常に大きなリスクを抱えていることを十分に理解し、必要なセキュリティ対策を実施していく必要があります。

以上で本診断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。

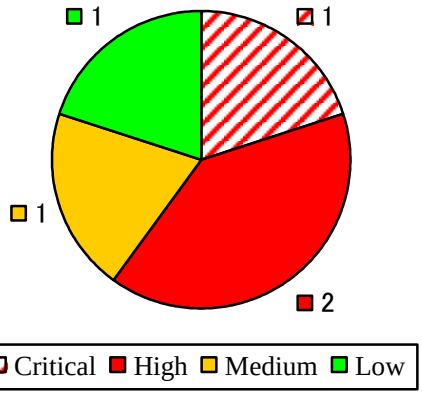
5　危険度の判定基準

本章では、本診断で検出された脆弱性の詳細を示します。

5－1　Web1

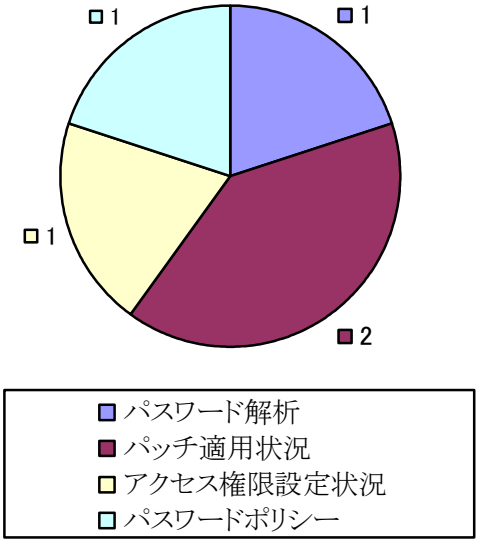
脆弱性危険度別検出数一覧／分布

危険度	検出数
Critical	1
High	2
Medium	1
Low	1
合計	5



診断項目別検出数一覧／分布

カテゴリ	診断項目	検出数
サーバ設定状況	パスワード解析	1
	パッチ適用状況	2
	アクセス権限設定状況	1
	カーネルパラメータの設定状況	0
	管理者権限のアカウント設定状況	0
	アクセスコントロール設定状況	0
	アプリケーション設定状況	0
サーバ稼働状況	稼働サービス	0
	稼働プロセス	0
	稼働ポート	0
	稼働ネットワーク	0
Windowsセキュリティポリシー	ローカルセキュリティポリシー	0
	パスワードポリシー	1
	アカウント関連ポリシー	0
	監査（ログ）ポリシー	0
	権限の割当ポリシー	0
	セキュリティオプション	0
合計		5



指摘事項

脆弱なパスワードを持つアカウントの存在

診断項目：パスワード解析

概要

診断対象サーバにおいて、脆弱なパスワードを持つアカウントが存在することを確認しております。

脆弱なパスワードを持つアカウントが存在する場合には、コンソールからの不正ログインのみならず、ログイン認証を利用するネットワークサービス経由での不正ログインや、一般ユーザ権限のアカウントであっても、他の脆弱性を併用して一般ユーザ権限から特権ユーザへの権限上昇が行われる等が考えられます。

対策

早急に推測困難なパスワードへ変更することを推奨します。

対象

対象サーバ

Web1

危険度

Critical

検出根拠

〇〇〇〇年〇月〇日から〇月〇日の期間でパスワード解析を行った結果、以下に示すように、脆弱なパスワードを持つアカウントが存在することを確認しました。

アカウント名	パスワード	備考
root	toor	アカウントから類推可能なパスワード
tanaka	tanakaweb1	アカウントとホスト名から類推可能なパスワード

備考

なし

セキュリティパッチの未適用

診断項目：パッチ適用状況

概要

診断対象サーバにおいて、OS ベンダから公開されているセキュリティパッチが未適用であることを確認しております。

一般的に、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パッチの適用が遅くなる傾向にありますが、現在ではセキュリティホールが確認されてから実証コードの公開や実際に悪用が始まるまでの期間が短くなっており、セキュリティホールを放置することによるリスクが高くなってきています。

対策

今回の診断対象は、1 年以上前のセキュリティパッチが適用されないまま運用されている傾向にあります。安定運用を優先させるため、サーバが稼動するネットワーク環境やサーバ上で利用するアプリケーション環境等を考慮した上での現状かと推測しますが、もし可能であれば、セキュリティ情報の公開から検証・適用までの手順をマニュアル化する等、可能な限りセキュリティパッチ未適用の状態の期間を減らすような対策を検討することを推奨します。

対象

対象サーバ
Web1

危険度
High
検出根拠
診断対象サーバにおいて、収集したパッチ情報から OS ベンダから公開されているセキュリティパッチが未適用であることを確認しております。
備考
確認された未適用セキュリティパッチの一覧は「添付資料 3-2-1_未適用セキュリティパッチ一覧(Web1)」をご参照下さい。

脆弱性の存在するアプリケーションの利用

診断項目：パッチ適用状況

概要

診断対象サーバにインストールされているアプリケーションについて、脆弱性が存在するバージョンが使用されていることを確認しております。

対策

サーバにサードパーティ製品やフリーのアプリケーションをインストールする場合、セキュリティのチェックも管理者が自分で行う必要があります。

もし不要なアプリケーションであればアンインストール、必要なアプリケーションであれば定期的にアプリケーションのサポートページから脆弱性の情報を収集しアプリケーションの更新を行うことを推奨します。

対象

対象サーバ

Web1

危険度

High

検出根拠

診断対象サーバにおいて、収集したインストール情報から以下に示すアプリケーションに脆弱性が存在することを確認しております。

アプリケーション名	インストールされているバージョン	脆弱性が確認されているバージョン（※1）	最新バージョン
Adobe Flash Player	10.0.42.34	10.2.159.1	10.3.181.14
Adobe Reader	9.0.0	9.4.3	9.4.4
Adobe Shockwave Player	11.5.2.602	11.5.9.615	11.5.9.620
Tera Term	4.66	4.68	4.69

備考

なし

Everyone グループに書き込みが許可されたファイル・ディレクトリの存在

診断項目：アクセス権限設定状況

概要

診断対象サーバにおいて、Everyone グループに書き込みが許可されたファイルやディレクトリが存在することを確認しています。

Everyone グループに書き込みが許可されている場合、システム上の任意のユーザの権限でファイルの操作や作成等が可能となり、特権の奪取やサービスの妨害、ログの改竄等の影響を受ける可能性があります。

対策

少なくとも任意のユーザが書き込み可能とならないよう、ファイルのパーミッションを変更することを推奨します。

なお、アプリケーションによっては意図的に任意のユーザに書き込みを許可している場合もありますので、十分な検証・確認を行った上でパーミッションの変更を行うかご検討下さい。

対象

対象サーバ
Web1

危険度
Medium
検出根拠
診断対象サーバにおいて、収集したサーバ情報から Everyone グループに書き込みが許可されたファイル・ディレクトリに脆弱性が存在することを確認しております。
備考
確認された Everyone グループに書き込みが許可されたファイル・ディレクトリの一覧は「添付資料 3-4-1_Everyone グループに書き込みが許可されたファイル･ディレクトリ一覧(Web1)」をご参照下さい。

パスワードポリシーに関する設定不備

診断項目：パスワードポリシー

概要

診断対象サーバにおいて、パスワードポリシーに対する設定内容が十分なセキュリティ強度を保持する内容でないことを確認しています。

対策

「パスワードの長さ」、「パスワードの有効期間」、「パスワードは要求する複雑さを満たす」等のパスワードのポリシーに関する設定内容について、再度ご確認をいただくことを推奨いたします。

なお、「パスワードの有効期限」については、設定した期間毎にパスワードの再設定を要求されるようになりますので、推奨値に固執せず運用に合わせて設定を行うようご注意下さい。

対象

対象サーバ

Web1

危険度

Low

検出根拠

診断対象サーバにおいて、Microsoft の推奨値と比較した場合、パスワードのポリシーに関する設定内容がセキュリティ的に強度の低い設定が行われている傾向にあることを確認しております。

設定名称	設定値	推奨値
パスワードの長さ	0 文字以上	8 文字以上
パスワードの変更禁止期間	0 日	1 日間
パスワードの有効期間	42 日	42 日間
パスワードの履歴を記録する	0 回	24 回
パスワードは要求する複雑さを満たす	無効	有効

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。

サーバ設定状況

サーバにおける設定状況に関する診断を行いました。

項目名	内容
パスワード解析	サーバに登録されているアカウントに対するパスワード情報の解析を行い、必要なセキュリティ強度を持っているかの調査を行いました。
パッチ適用状況	脆弱性に対する修正プログラム（セキュリティパッチ）の適用状況の確認を行い、サーバのセキュリティ強度が適切に保持されているかの調査を行いました。
アクセス権限設定状況	サーバ上に存在するファイル／ディレクトリに対するアクセス権限の設定状況の確認を行い、適切にアクセス権限が設定されているかの調査を行いました。
カーネルパラメータの設定状況	サーバ上で稼働する OS におけるカーネルパラメータの設定状況の確認を行い、カーネルのセキュリティ強度が適切に保持されているかの調査を行いました。
管理者権限のアカウント設定状況	管理者権限アカウントにおける環境設定の確認を行い、必要なセキュリティ強度が適切に設定されているかの調査を行いました
アクセスコントロール設定状況	サーバ上で設定されている各ファイルやネットワークに対するアクセスコントロールの確認を行い、適切に設定されているかの調査を行いました。
アプリケーション設定状況	サーバ上で稼働するアプリケーションの設定状況の確認を行い、適切に設定されているかの調査を行いました。
パスワード解析	サーバに登録されているアカウントに対するパスワード情報の解析を行い、必要なセキュリティ強度を持っているかの調査を行いました。

サービス稼働状況

サーバ上で稼動しているサービスに関わる診断を行いました。

項目名	内容
稼動サービス	サーバ上で稼動しているサービスの確認を行うことで、セキュリティ強度を保持するために必要なサービスが適切に稼動しているかの調査を行いました。
稼動プロセス	サーバ上で稼動しているプロセスの確認を行うことで、セキュリティ強度を保持するために必要なプロセスが適切に稼動しているかの調査を行いました。
稼動ポート	サーバ上でアクセスが許可されているポート番号の確認を行うことで、セキュリティ強度を保持するために必要なポートが適切に許可されているかの調査を行いました。
稼働ネットワーク	サーバ上で設定されているルーティング等のネットワークの確認を行い、セキュリティ強度を保持するために必要なネットワークが適切に設定されているかの調査を行いました。

Windows セキュリティポリシー

Windows 環境において設定されているセキュリティポリシーに関わる診断を行いました。

項目名	内容
ローカルセキュリティポリシー	ローカルセキュリティポリシーの設定状況を確認することで、サーバにアクセス可能なユーザやそのユーザが利用可能なリソース、及びイベントログへの記録レベル等の制御が適切に行われるかの調査を行いました。
パスワードポリシー	パスワードポリシーの設定状況を確認することで、パスワードの変更履歴や有効期間、変更禁止期間の管理、及びパスワード強度の設定が適切に行われているかの調査を行いました。
アカウント関連ポリシー	アカウント関連ポリシーの設定状況を確認することで、アカウントロックアウト期間や失敗回数のしきい値の設定等が適切に行われているかの調査を行いました。
監査（ログ）ポリシー	監査ポリシーの設定状況を確認することで、監査が必要なセキュリティ関連のイベントのカテゴリに対する設定が適切に行われているかの調査を行いました。
権限の割当ポリシー	権限の割当ポリシーの設定状況を確認することで、ユーザに対してログオン方法やシステム内で許可されるアクションへの権限が適切に設定されているかの調査を行いました。

項目名	内容
セキュリティオプション	セキュリティオプションの設定状況を確認することで、セキュリティオプションを構成しているセキュリティ関連システムパラメータに対する設定が適切に行われているかの調査を行いました。

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