CONFIDENTIAL

SAMPLE

○○○○○株式会社　御中

サーバ構成診断
診断結果報告書
【速報】

脆弱性診断後 3 営業日以内に提出いたします。
本診断結報告書では危険度の高い脆弱性(Medium 以上)の技術的な対処方法・対策方法の説明を報告いたします。

平成○○年○月○日

株式会社 ソフテック

CONFIDENTIAL

SAMPLE

【資料改編履歴】

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

CONFIDENTIAL

SAMPLE

目　　次

1　目的

本診断結果報告書【速報】は、平成〇〇年〇月〇日に実施したサーバ構成診断において、深刻な影響を与えることが懸念される脆弱性をより早くご報告するために、診断結果の一部を抽出、要約したものです。

深刻な影響を与えることが想定される脆弱性をより早くご報告することで、正式な診断報告を待つことなく、脆弱性への対応を行うことが可能です。

なお、本診断結果報告書【速報】はあくまでも現時点での調査結果・要約という位置付けの報告であり、最終的な診断結果報告書とは内容が異なる場合もございますので、ご了承下さい。

2　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			

3　診断結果要約

現時点で本診断において確認されている脆弱性の内、危険性が高いと考えられる脆弱性について以下に示します。

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。

現時点において確認されたセキュリティパッチの未適用一覧について、表 3-2-1 に示します。現時点での調査結果という位置付けになりますので、最終的な診断結果報告とは内容が異なる場合もございますので、予めご了承下さい。

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

文書番号	技術情報番号	文書名	深刻度	公開日	最終更新日
MS12-033	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

4　その他の脆弱性一覧

現時点で本診断において検出されている脆弱性の内、「3　診断結果要約」にて示した危険性の高い脆弱性以外に検出されているものはありません。

5　危険度の判定基準

本診断結果報告書【速報】では検出された各脆弱性について、表 5-1 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 5-1　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　実施した診断項目一覧

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。

項目名	内容
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。
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。

以上