2006 年 10 月 13 日

「PCから始める 職場のセキュリティ診断」 診断結果レポート

1. 診断概要

各PCからアクセスして頂くことで各種セキュリティ診断を実施させて頂きました。セキュリティ診断内容は、「企業内PCの現状調査」と「利用者の意識調査」の二つに大きく分類しています。

各調査項目における解説は以下の通りです。

1.1. 診断項目

本診断では、下記の5項目に関する診断を実施しております。

項目		解説
ユーザー管理		
	アカウント管理	ID、パスワード、アクセス権限等の設定状況を調査し、なりすましや不正利用に対する危険性を診断します。
デスクトップ セキュリティ		
	クライアント設定	セキュリティ対策に関するPCの設定状況を調査し、情報漏洩の危険性を診断します。
	セキュリティパッチ	セキュリティパッチの適用状況を調査し、未適用のセキュリティパッチを確認します。
	マルウェア対策	ウイルス対策ソフトの設定等を調査し、マルウェア（ウイルス・ワーム等の悪意あるソフトウェア）に感染する危険性を診断します。
	データ保護	利用規則やPC利用状況を調査し、不要なソフトウェアのインストール状況や第三者による不正利用の危険性を診断します。

1.2. 評価基準

診断結果全体より、インフラ成熟度をA～Eの5段階にて、診断項目別の評価を○△×の3段階にて評価します。

A	適切なレベルにあります
B	適切なレベルまであと一歩です
C	セキュリティ対策にモレがあります
D	セキュリティ対策に複数のモレがあります
E	対策全般の見直し、速やかな対策実施が必須です

○	安全
△	普通
×	危険

［備考］

本診断結果レポートは、(株)ラックの「PCから始める 職場のセキュリティ診断」サービスを活用してレポートさせて頂くものです。

尚、診断実施方法は、簡略化を図っているため、各企業のIT資産環境全てを包括するものではありません。

また、本レポートは、セキュリティ診断に関する内容が含まれているため、取り扱いには十分ご注意ください。

本レポートの取り扱いに関する過失による如何なる損害についても、弊社は補償いたしません。

2. 診断期間及び台数

診断期間　：2006 年 09 月 25 日（月）～ 2006 年 10 月 12 日（木）

診断実施PC台数　：35 台

3. 診断結果

3.1. インフラ成熟度評価

インフラ成熟度	短評
E	今回の診断では、多くの問題点が見つかりました。問題を有するＰＣを放置しておくと、情報漏洩などのセキュリティリスクが発生する可能性が高まります。診断レポートを元にセキュリティ対策全般を見直し、クライアントPCのアカウント管理・セキュリティパッチの適用・利用者のセキュリティ教育など早急な対策実施が必要です。

3.2. 主な問題点

診断で検出された代表的な脆弱性(上位10件)を対策優先度別に記載します。

	問題点	不適合率	リスクレベル	診断項目
1	他人から推測されやすいパスワードが設定されています。(利用者の意識調査)	69%	H	アカウント管理
2	ハードディスク暗号化が有効に設定されていません。第三者にPC内のデータを閲覧・搾取されるリスクが存在します。(企業内PCの現状調査)	100%	M	データ保護
3	社内で使用しているコンピュータウイルス対策ソフトで定期的にフルスキャンが行われていません。(利用者の意識調査)	86%	M	マルウェア対策
4	セキュリティログの取得設定に不備があります。情報漏洩等が発生した際に、漏洩経路等を追跡することが困難です。(企業内PCの現状調査)	77%	M	クライアント設定
5	スパイウェア等の迷惑ソフトがPC内に侵入するリスクが存在します。(企業内PCの現状調査)	77%	M	マルウェア対策
6	社内で使用しているパソコンにログオンするためのパスワードが設定されていません。(利用者の意識調査)	49%	H	アカウント管理
7	社外に持ち出すパソコンのハードディスクが暗号化されていません。(利用者の意識調査)	69%	M	データ保護
8	ウイルス対策ソフトのリアルタイム検知が有効になっていないか、ウイルス対策ソフトがインストールされていません。(企業内PCの現状調査)	43%	H	マルウェア対策
9	PC上で、サーバ向けサービスが起動しています。ウイルス・ワームの感染やPCに侵入されるリスクが存在します。(企業内PCの現状調査)	60%	M	クライアント設定
10	ログオン失敗によるロックアウト機能が設定されていません。パスワードクラックに対してリスクが存在します。(企業内のPCの現状調査)	100%	L	アカウント管理

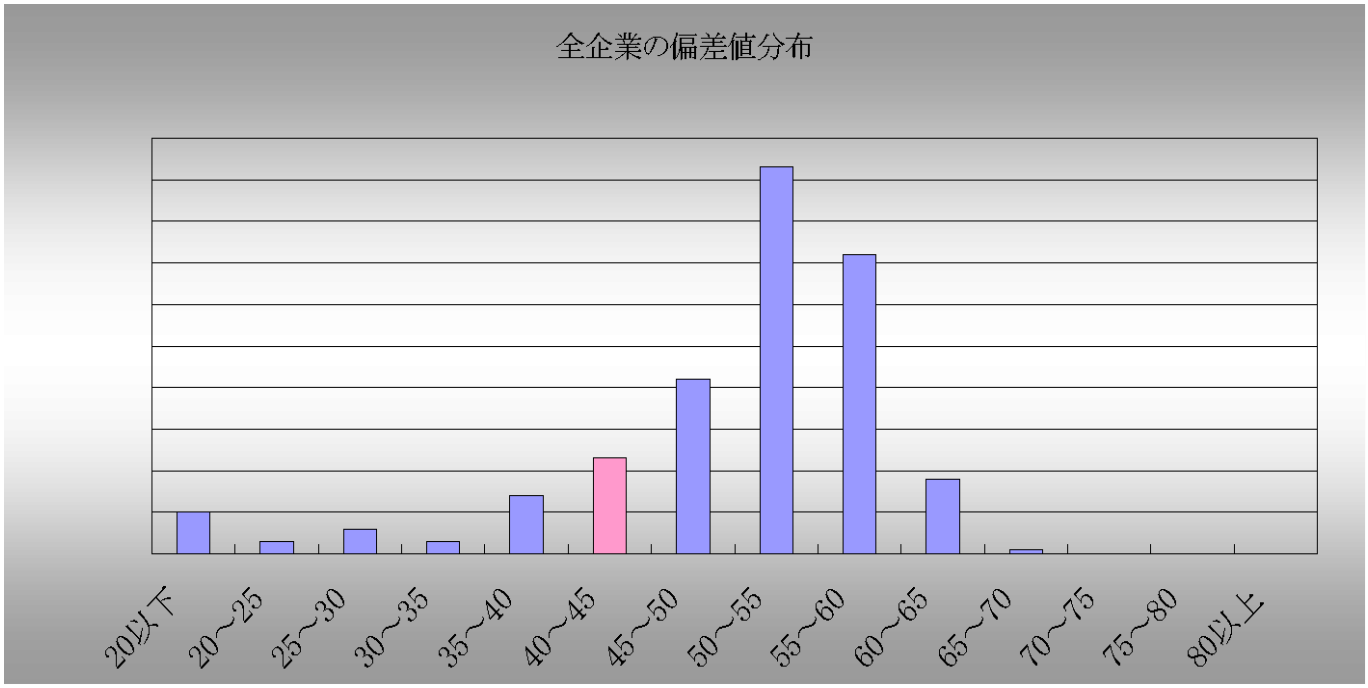
注）不適合率とは、診断対象PCの総数より、問題点が検出されたPCの割合です。

検出された脆弱性のリスクレベルをH・M・Lの3段階で表します。（High, Medium, Low）

3.3.　項目別評価

御社の当診断における総合的な偏差値は、 40.84 です。

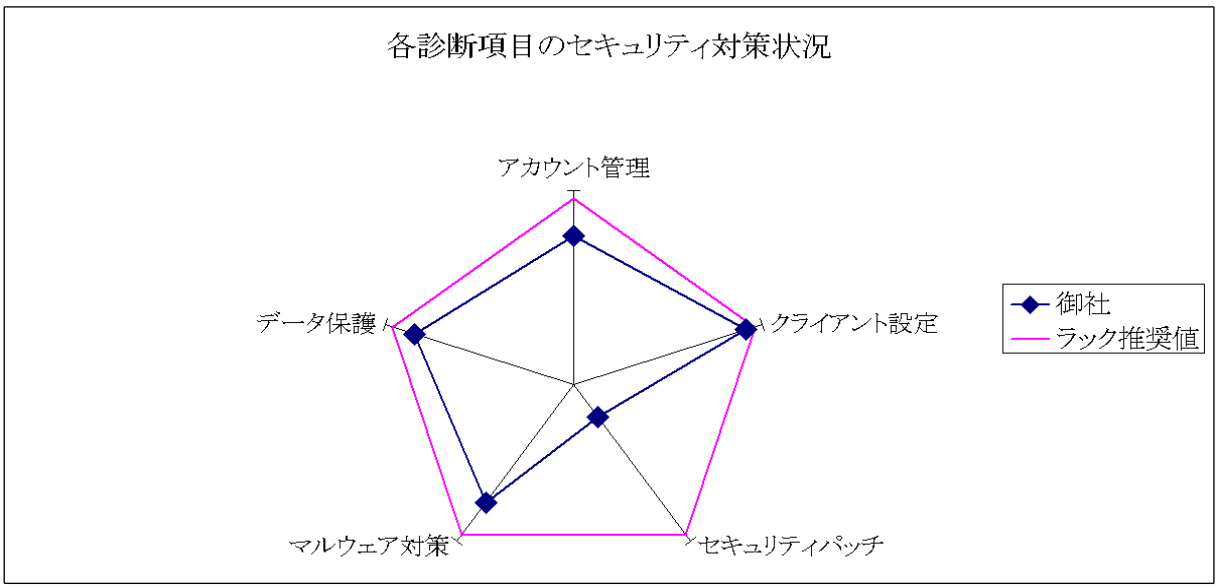
（偏差値は職場のPCセキュリティ診断を診断した全ユーザー別の相対評価です）



各診断項目ごとの偏差値は以下の通りです。（○(安全)、△(普通)、×(危険)の三段階）

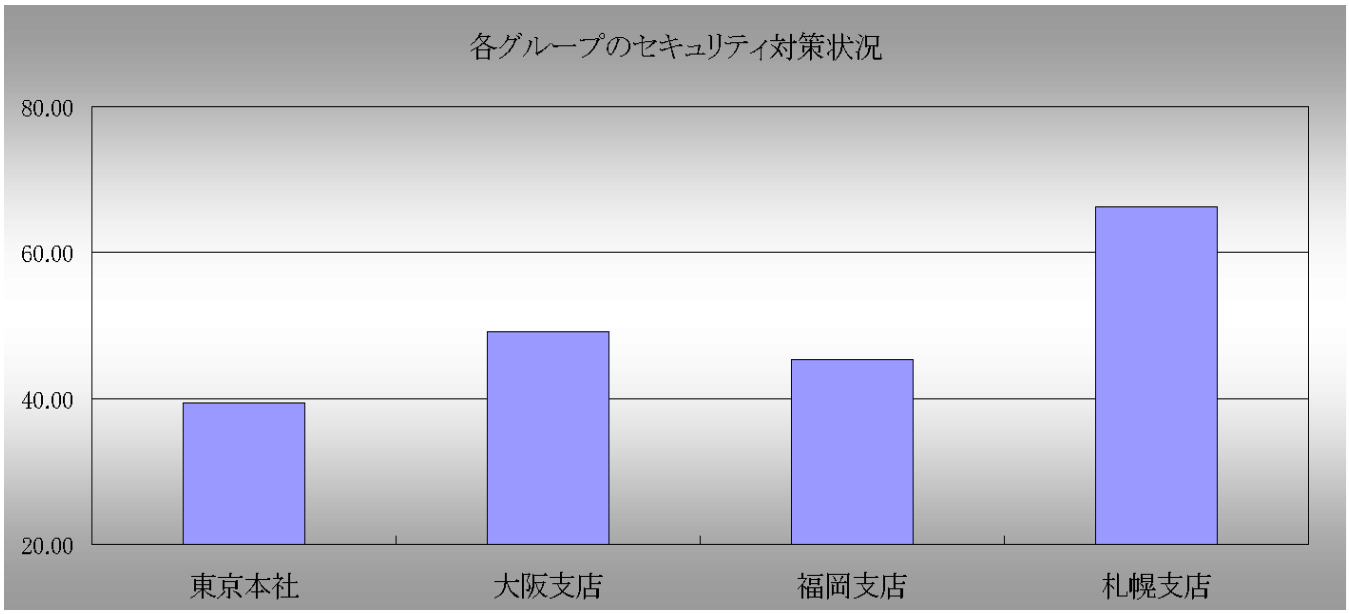
診断項目	評価	偏差値	コメント
ユーザー管理			
アカウント管理	× 危険	55.19	多くのPCで、適切なアカウント管理が行われていません。利用者に対して、アカウントおよびパスワード管理を周知徹底する必要があります。
デスクトップ セキュリティ			
クライアント設定	△ 普通	26.18	一部のPCで、適切なクライアント設定が行われていません。利用者ＰＣにおいて、OS関連のセキュリティポリシーの設定および不要なサービスの無効化等を実施する必要があります。
セキュリティパッチ	△ 普通	38.69	一部のPCで、セキュリティパッチが適用されていません。利用者に対して、セキュリティパッチの適用を行うよう促す必要があります。
マルウェア対策	× 危険	52.00	多くのPCで、マルウェア（悪意あるソフトウェア）対策が適切に行われていません。利用者に対して、適切なマルウェア対策を行うよう促す必要があります。
データ保護	× 危険	53.09	多くのPCで、適切なデータ保護が行われていません。利用者に対して、データ暗号化および不要なアプリの利用禁止等を促す必要があります。

下記のグラフは各診断項目のセキュリティ対策状況を表しています。赤線(ラックの推奨値)より
御社のセキュリティ状況が内側の場合、セキュリティ対策が必要です。



グループ別のセキュリティ状況は、以下の通りです。
(偏差値は御社の全グループ別の相対評価です)

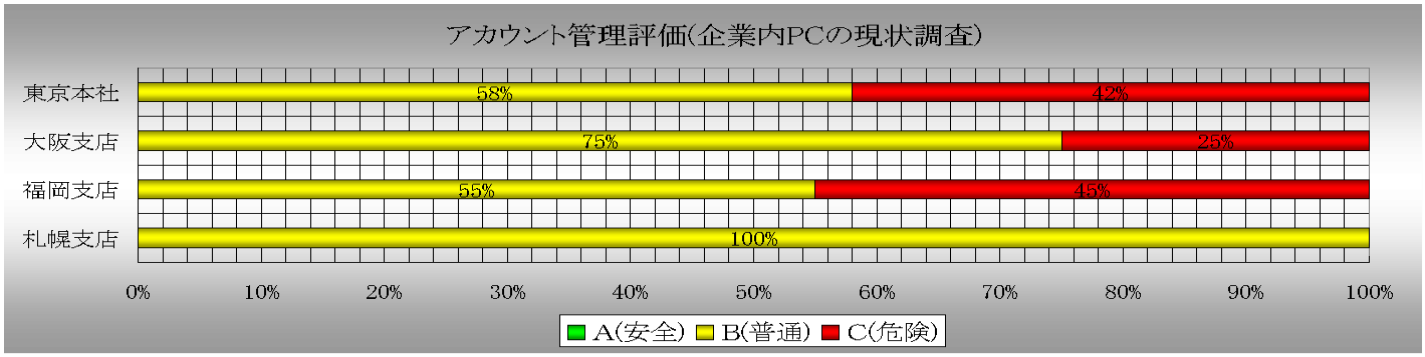
グループ	偏差値
東京本社	39.33
大阪支店	49.14
福岡支店	45.29
札幌支店	66.23

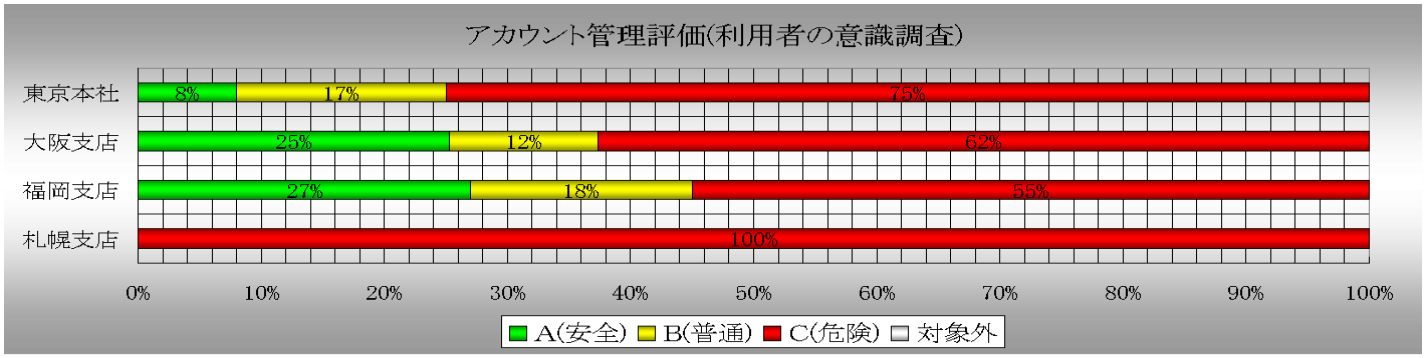


3.4.　診断項目別結果一覧

3.4.1.　アカウント管理

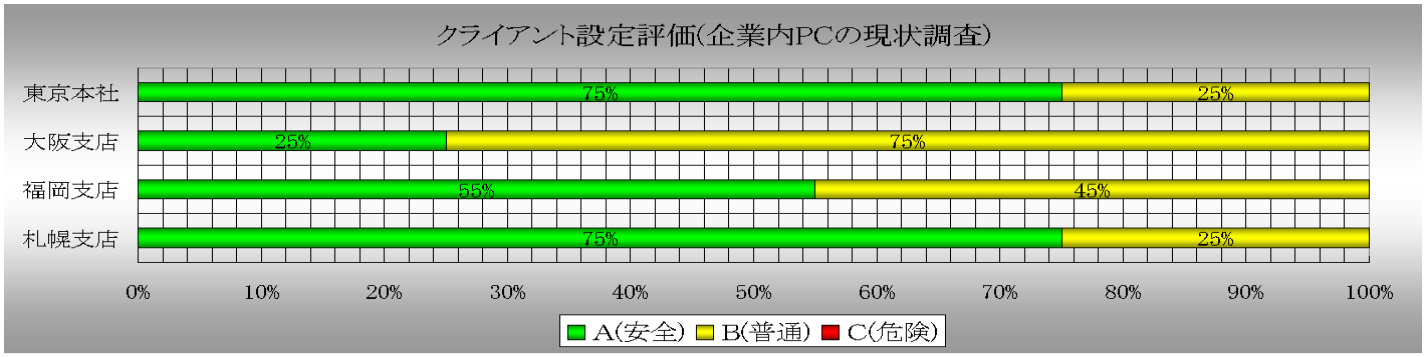
各PCにおいて、適切なアカウント管理が実施されているか評価しています。上のグラフはPCの現状調査を表し、下のグラフは利用者の意識調査を表しています。両グラフによる結果の差異が大きい場合には、PCの現状と利用者の意識にずれが生じていることを表します。

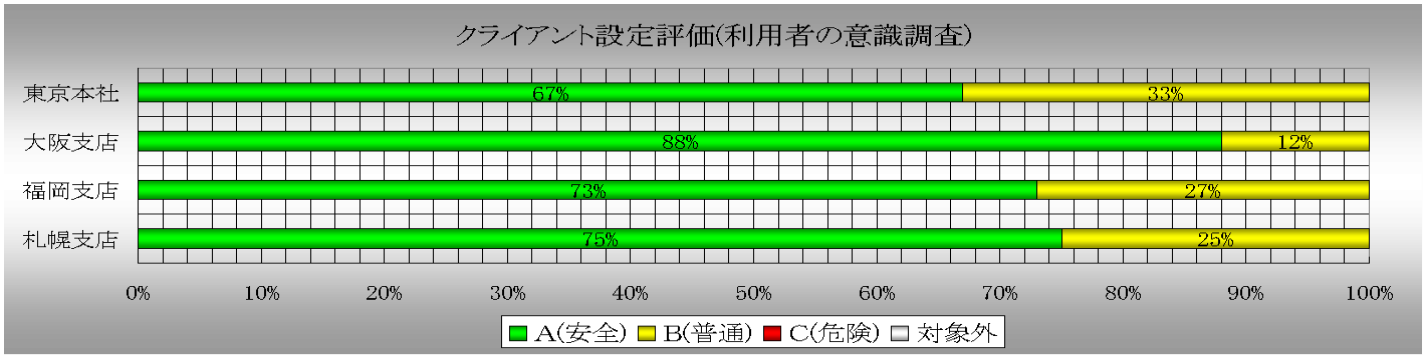




3.4.2. クライアント設定

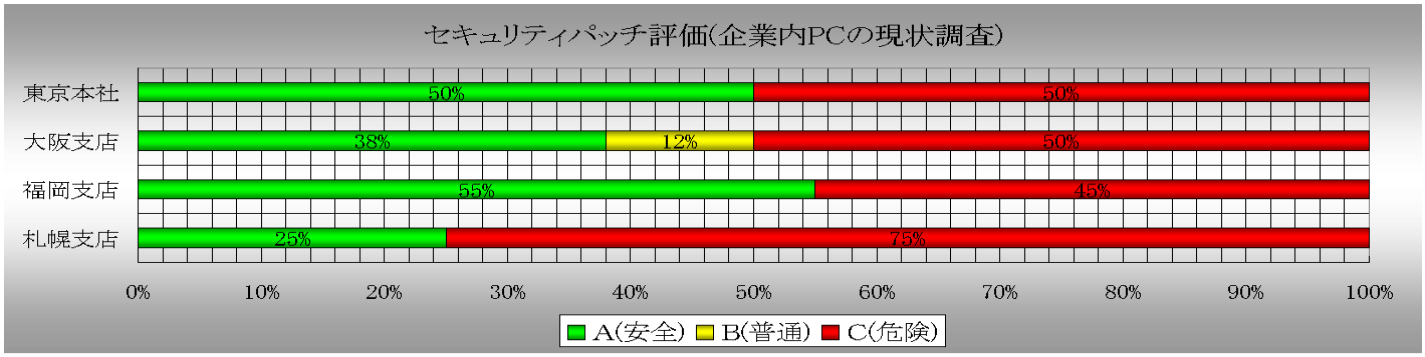
各PCにおいて、適切なクライアント設定が実施されているか評価しています。上のグラフはPCの現状調査を表し、下のグラフは利用者の意識調査を表しています。両グラフによる結果の差異が大きい場合には、PCの現状と利用者の意識にずれが生じていることを表します。

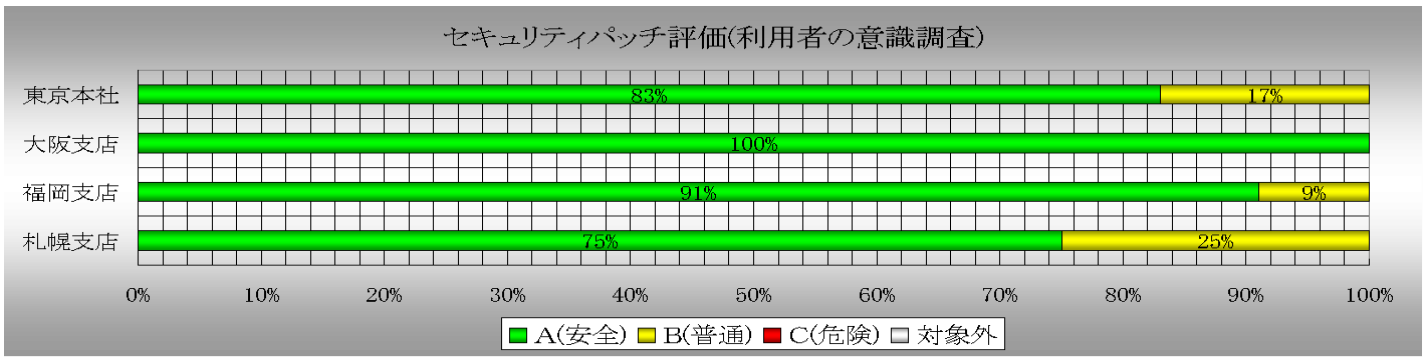




3.4.3. セキュリティパッチ

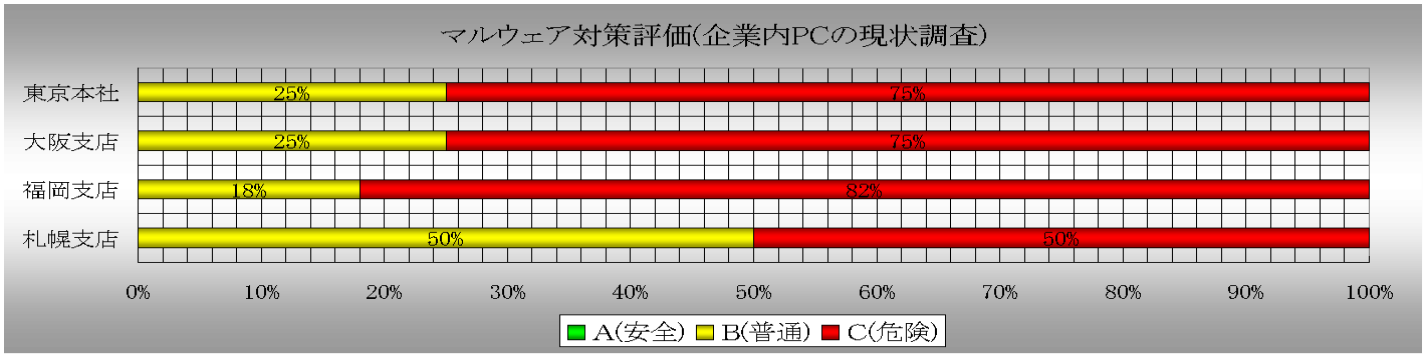
各PCにおいて、セキュリティパッチの適用が実施されているか評価しています。上のグラフはPCの現状調査を表し、下のグラフは利用者の意識調査を表しています。両グラフによる結果の差異が大きい場合には、PCの現状と利用者の意識にずれが生じていることを表します。

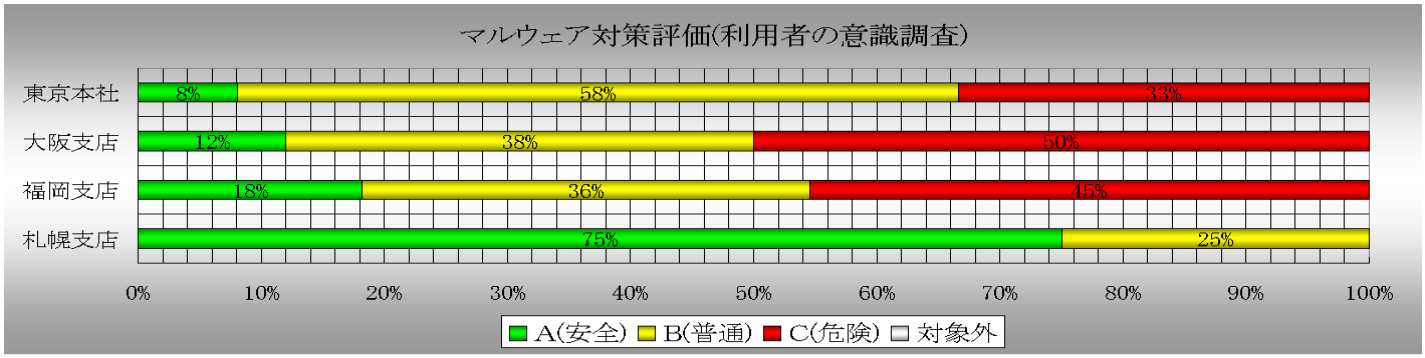




3.4.4.　マルウェア対策

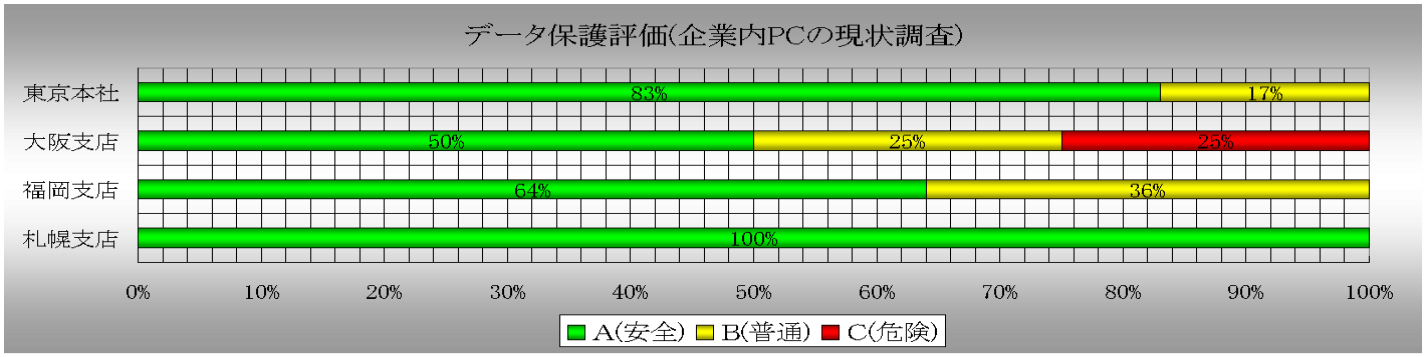
各PCにおいて、適切なマルウェア対策が実施されているか評価しています。上のグラフはPCの現状調査を表し、下のグラフは利用者の意識調査を表しています。両グラフによる結果の差異が大きい場合には、PCの現状と利用者の意識にずれが生じていることを表します。

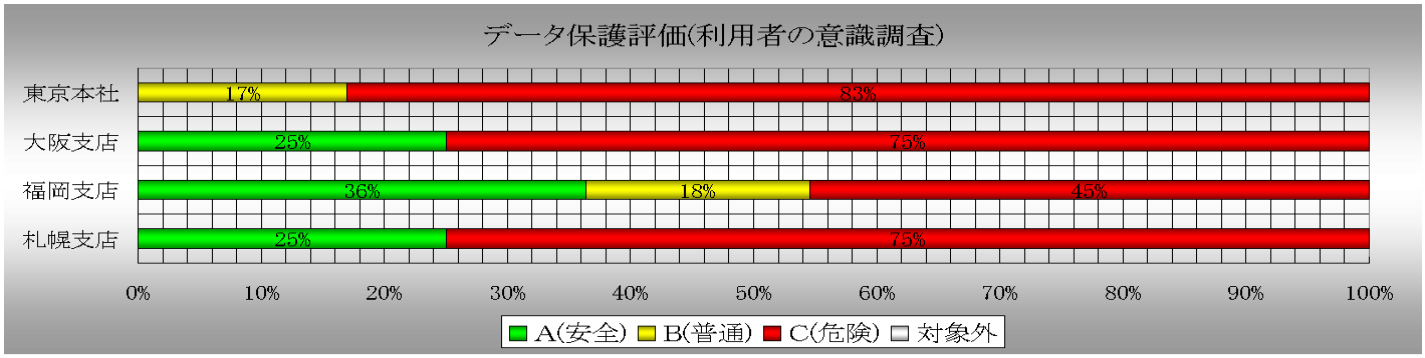




3.4.5.　データ保護

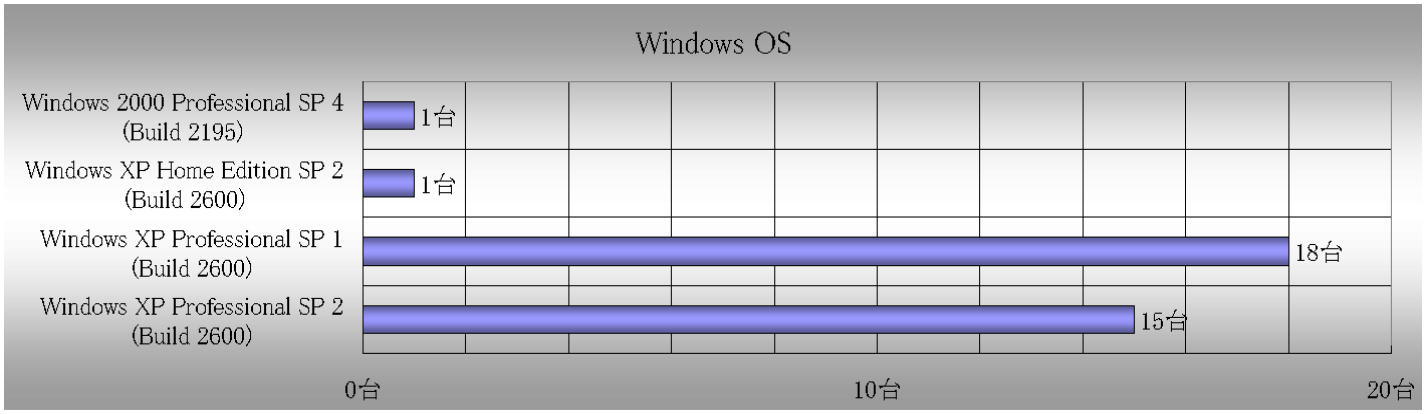
各PCにおいて、適切なデータ保護が実施されているか評価しています。上のグラフはPCの現状調査を表し、下のグラフは利用者の意識調査を表しています。両グラフによる結果の差異が大きい場合には、PCの現状と利用者の意識にずれが生じていることを表します。



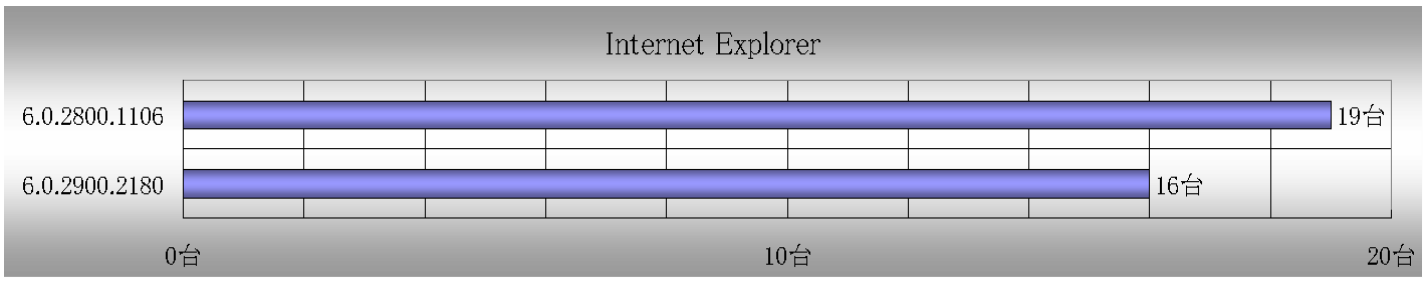


3.5.　診断対象PC関連情報

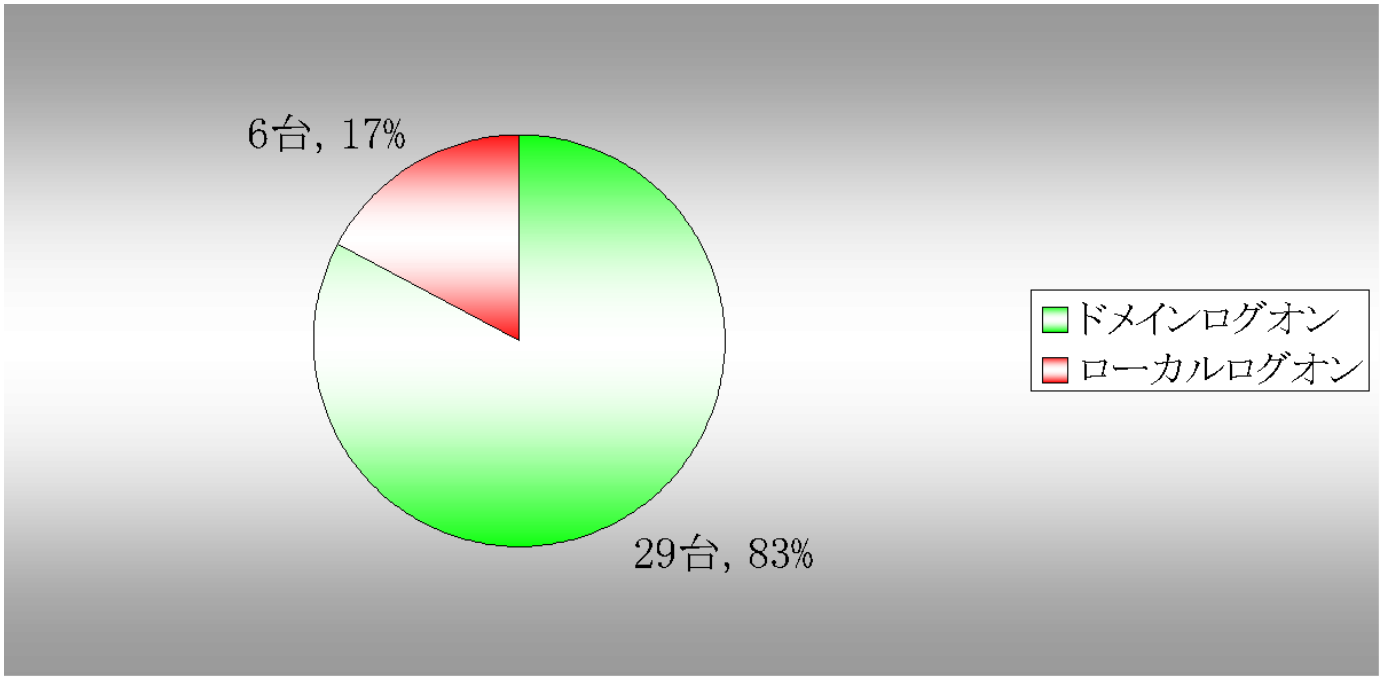
3.5.1.　企業内のOS分布



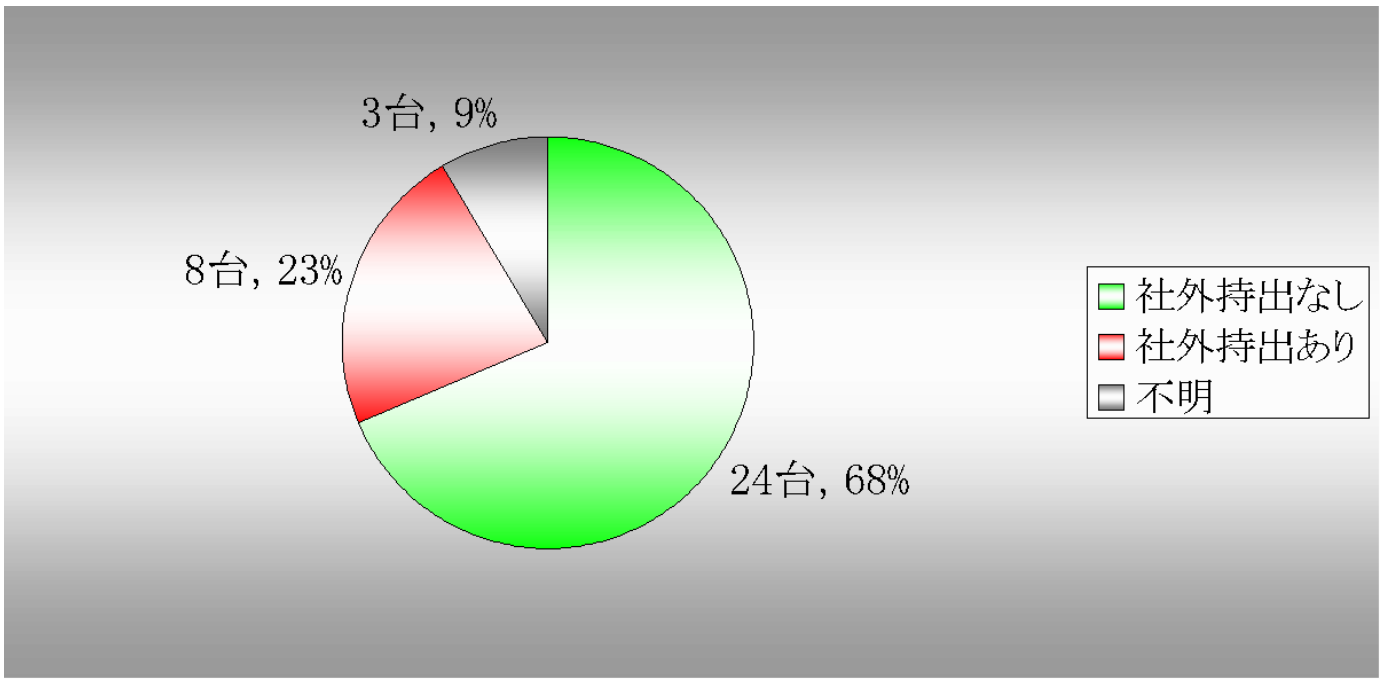
3.5.2.　企業内のブラウザ分布



3.5.3. 企業内のログオン分布



3.5.4. 持ち出しPCの利用状況分布



3.6.　グループ別個別診断結果

・東京本社

IPアドレス	コンピュータ名	ユーザー管理	デスクトップ セキュリティ			
		アカウント管理	クライアント設定	セキュリティパッチ	マルウェア対策	データ保護
172.17.10.22	TOKYO-05	✕ 危険	○ 安全	○ 安全	✕ 危険	△ 普通
172.17.10.28	TOKYO-07	✕ 危険	△ 普通	✕ 危険	✕ 危険	✕ 危険
172.17.10.34	TOKYO-06	✕ 危険	✕ 危険	✕ 危険	✕ 危険	△ 普通
172.17.10.36	TOKYO-09	✕ 危険	△ 普通	✕ 危険	✕ 危険	✕ 危険
172.17.10.38	TOKYO-08	✕ 危険	○ 安全	○ 安全	✕ 危険	✕ 危険
172.17.10.44	TOKYO-01	✕ 危険	△ 普通	○ 安全	✕ 危険	✕ 危険
172.17.10.46	TOKYO-02	✕ 危険	✕ 危険	✕ 危険	✕ 危険	✕ 危険
172.17.10.49	TOKYO-03	✕ 危険	△ 普通	△ 普通	✕ 危険	✕ 危険
172.17.10.101	TOKYO-10	✕ 危険	✕ 危険	✕ 危険	✕ 危険	✕ 危険
172.17.10.102	TOKYO-11	△ 普通	○ 安全	✕ 危険	✕ 危険	✕ 危険
172.17.10.106	TOKYO-12	✕ 危険	○ 安全	○ 安全	✕ 危険	✕ 危険
172.17.10.131	TOKYO-04	✕ 危険	○ 安全	○ 安全	✕ 危険	✕ 危険

・大阪支店

IPアドレス	コンピュータ名	ユーザー管理	デスクトップ セキュリティ			
		アカウント管理	クライアント設定	セキュリティパッチ	マルウェア対策	データ保護
172.17.20.24	OSAKA-04	△ 普通	✕ 危険	✕ 危険	✕ 危険	✕ 危険
172.17.20.29	OSAKA-05	✕ 危険	△ 普通	✕ 危険	△ 普通	✕ 危険
172.17.20.35	OSAKA-02	✕ 危険	△ 普通	○ 安全	✕ 危険	✕ 危険
172.17.20.41	OSAKA-03	✕ 危険	△ 普通	○ 安全	✕ 危険	✕ 危険
172.17.20.72	OSAKA-07	✕ 危険	△ 普通	✕ 危険	✕ 危険	✕ 危険
172.17.20.73	OSAKA-06	✕ 危険	✕ 危険	○ 安全	✕ 危険	○ 安全
172.17.20.75	OSAKA-08	✕ 危険	△ 普通	✕ 危険	✕ 危険	△ 普通
172.17.20.238	OSAKA-01	✕ 危険	△ 普通	△ 普通	✕ 危険	✕ 危険

・福岡支店

IPアドレス	コンピュータ名	ユーザー管理	デスクトップ セキュリティ			
		アカウント管理	クライアント設定	セキュリティパッチ	マルウェア対策	データ保護
172.17.30.11	FUKUOKA-09	✕ 危険	△ 普通	○ 安全	✕ 危険	✕ 危険
172.17.30.12	FUKUOKA-04	✕ 危険	△ 普通	✕ 危険	✕ 危険	○ 安全
172.17.30.19	FUKUOKA-03	✕ 危険	○ 安全	○ 安全	✕ 危険	△ 普通
172.17.30.21	FUKUOKA-10	✕ 危険	△ 普通	✕ 危険	✕ 危険	✕ 危険
172.17.30.22	FUKUOKA-11	✕ 危険	△ 普通	○ 安全	✕ 危険	✕ 危険
172.17.30.27	FUKUOKA-07	✕ 危険	△ 普通	✕ 危険	✕ 危険	✕ 危険
172.17.30.34	FUKUOKA-08	✕ 危険	✕ 危険	○ 安全	✕ 危険	○ 安全
172.17.30.73	FUKUOKA-01	✕ 危険	○ 安全	✕ 危険	✕ 危険	△ 普通
172.17.30.74	FUKUOKA-02	✕ 危険	✕ 危険	✕ 危険	✕ 危険	✕ 危険
172.17.30.75	FUKUOKA-06	✕ 危険	✕ 危険	○ 安全	✕ 危険	✕ 危険
172.17.30.76	FUKUOKA-05	△ 普通	△ 普通	○ 安全	✕ 危険	○ 安全

・札幌支店

IPアドレス	コンピュータ名	ユーザー管理	デスクトップ セキュリティ			
		アカウント管理	クライアント設定	セキュリティパッチ	マルウェア対策	データ保護
172.17.40.21	SAPPORO-01	✕ 危険	✕ 危険	✕ 危険	△ 普通	✕ 危険
172.17.40.72	SAPPORO-02	✕ 危険	△ 普通	✕ 危険	✕ 危険	✕ 危険
172.17.40.73	SAPPORO-03	✕ 危険	○ 安全	△ 普通	✕ 危険	✕ 危険
172.17.40.74	SAPPORO-04	✕ 危険	△ 普通	✕ 危険	✕ 危険	○ 安全

3.7.　情報漏洩につながる可能性があるソフトウェアをインストールしているPC一覧

ソフトウェア名	グループ名	IPアドレス	コンピュータ名
Winny	大阪支店	172.17.20.24	OSAKA-04
		172.17.20.41	OSAKA-03

以上

4. 対策

検出された問題点に対して、Windows Vista を用いて対策を実施する方法をガイドします。

対策実施に際しては、対策ガイド参照先(※1)をご確認ください。

Windows Vista には、豊富なセキュリティ機能が標準搭載されているため、検出された問題点の多くを

OS自体が備える機能のみで対策することができます。

（※1）PCから始める職場のセキュリティ対策ガイド

検出された問題点		Windows Vistaにおける対策ポイント	対策ガイド参照先
1	他人から推測されやすいパスワードが設定されています。(利用者の意識調査)	パスワードポリシーの「パスワードは、複雑さの要件を満たす必要がある」を有効にすることで、安易で推測されやすいパスワードが設定されるのを防ぐことができます。	2.1.1.2
2	ハードディスク暗号化が有効に設定されていません。第三者にPC内のデータを閲覧・搾取されるリスクが存在します。(企業内PCの現状調査)	Vistaに標準搭載されているBitLockerを用いれば、追加製品を購入することなくハードディスク暗号化の実現が可能です。(※本機能はVistaのEnterpriseエディション以上に搭載)	2.2.4.2
3	社内で使用しているコンピュータウイルス対策ソフトで定期的にフルスキャンが行われていません。(利用者の意識調査)	一般的なウイルス対策ソフトには定期スキャン機能が備わっています。週に一度程度の頻度で、自動スキャンが行われるように設定してください。	2.2.3.3
4	セキュリティログの取得設定に不備があります。情報漏洩等が発生した際に、漏洩経路等を追跡することが困難です。(企業内PCの現状調査)	監査ポリシーにてセキュリティログ全般の設定を行います。ログの取得内容だけではなく、ログファイルのサイズについて注意が必要です。	2.2.1.8
5	スパイウェア等の迷惑ソフトがPC内に侵入するリスクが存在します。(企業内PCの現状調査)	Vistaに標準搭載されているWindows Defender（迷惑ソフト 防御ツール）を用いれば、追加製品を購入することなくスパイウェアなどの迷惑ソフトからPCを保護することができます。	2.2.3.2
6	社内で使用しているパソコンにログオンするためのパスワードが設定されていません。(利用者の意識調査)	コントロールパネルのパスワード変更ダイアログより、ユーザに任意のパスワードを設定できます。	2.1.1.2
7	社外に持ち出すパソコンのハードディスクが暗号化されていません。(利用者の意識調査)	Vistaに標準搭載されているBitLockerを用いれば、追加製品を購入することなくハードディスク暗号化の実現が可能です。(※本機能はVistaのEnterpriseエディション以上に搭載)	2.2.4.2
8	ウイルス対策ソフトのリアルタイム検知が有効になっていないか、ウイルス対策ソフトがインストールされていません。(企業内PCの現状調査)	ウイルス対策ソフトをインストールしてください。既に、インストール済の場合は、ウイルス対策ソフトのリアルタイム検知機能を有効に設定します。	2.2.3.4
9	PC上で、サーバ向けサービスが起動しています。ウイルス・ワームの感染やPCに侵入されるリスクが存在します。(企業内PCの現状調査)	Windowsコンポーネントのインストール画面から、不要なサーバ向けサービスをアンインストールすることができます。	2.2.1.3
10	ログオン失敗によるロックアウト機能が設定されていません。パスワードクラックに対してリスクが存在します。(企業内のPCの現状調査)	アカウント ロックアウトのポリシーにて、ロックアウトのしきい値やロックアウト期間を任意に設定することができます。	2.1.1.4