

## FAQ集(SafeSecureKeeper)

2006/8/28

番号	キーワード	内容	回答	備考
a-1	評価版 デモ版 トライアル版	SafeSecureKeeperには、評価版はありますか？	SafeSecureKeeperは、Microsoft SQLServerが必須ソフトウェアとして別途必要なこともあり、評価版等事前に試用可能な製品はございません。	
b-1	環境	ファイルサーバエージェントをインストールしたサーバ上で、FTPサーバを運用することはできるでしょうか？	FTPの通信は遮断しませんので、利用できます。	
b-2	環境	SecureKeeperファイルサーバエージェントについては、インストールで動作対象外OSへのインストールができないようになっているのでしょうか？	SecureKeeperファイルサーバエージェントのインストーラでは、インストールしようとしたPCのOSをチェックし、動作対象外のOSの場合終了してしまいます。ファイルサーバエージェントは、動作対象OS以外にはインストールできません。 ※ファイルサーバエージェントのインストーラでは動作OSのチェック以外に、そのサーバがドメインコントローラかどうかともチェックしています。動作OSであっても、ドメインコントローラであるサーバの場合はインストールできません。	
b-3	環境	[共通] 保護対象のファイルサーバのOSは、WindowsNT4.0にも対応しているか？	対応している。(サービスパック6aが適用されていることが前提)	
b-4	環境	[共通] 保護対象のファイルサーバがクラスタリングされている場合、動作するか？	実機検証は実施していないが、理論上は動作すると考えられる。ただし、クラスタリング環境固有の障害に対してはサポート対象外。	
b-5	環境	[共通] 保護対象のファイルサーバに「TX200FT」というシステムが導入されている場合、サポート対象か？ (TX200FTは、2つのサーバをクライアント側から1つに見せるシステムで、サーバへアップロードするファイルは、同時に2つのサーバに書き込まれる)	実機検証は実施していないが、理論上は動作すると考えられる。ただし、クラスタリング環境同様、固有の障害に対してはサポート対象外。	
b-6	環境	[共通] SafeSecureKeeperで保護できるファイルサーバのOSは？	SafeSecureKeeperで保護をおこなうことができるのは、Windows系のサーバOSとなります。 LinuxサーバでのSambaなど、Windowsからアクセス可能な他OSのファイルサーバは保護の対象とすることはできません。 保護できるファイルサーバ用OSは以下のとおりです。 ・WindowsNT4.0Server (ServicePack6以上) ・Windows2000Server ・WindowsServer2003 ※ファイルサーバとしてWindowsServer2003を使用している場合、以下の注意が必要です。 ・WindowsServer2003でフォルダを作成すると、初期状態でWindowsのアクセスコントロールで管理者以外アクセスできない設定になっている場合があるということです。 このとき、SecureKeeperの保護設定 (Desktop.iniを書き込む) ができなくなります (保護設定が不可能になります)。 そのため、WindowsServer2003のファイルサーバがある場合、保護を設定する予定のフォルダを作成したときは、フォルダのアクセスコントロールを確認し、アクセス可能なように設定を変更しておく必要があります。	
b-7	環境	[共通] 保護フォルダのあるファイルサーバに対して、バックアップ製品のBacup EXEC (ベリタス) を使用できるか？	確認した結果、動作は可能と思われませんが、未検証製品のため100%の保証はできないとのことです。 バックアップソフトとしては、以下の製品で実績があるとのことです。 ・BrightStor ARCserve Backup (Computer Associates)	
b-8	環境	[共通] 保護対象であるファイルサーバのOSに Microsoft Windows Storage Server 2003 は対応していますか？	現在はサポート対象となっておりません。 今後サポートOSにするかどうかは現在検討中です。 ※動作検証は未実施。	
b-9	環境	[共通] 対象ファイルサーバとしてWindows Strage Server 2003搭載NASを利用できますか？	出来ません。 (補足) 以前は、ETERNUS NR1000F seriesかつOS: ONTAP6.5での検証は実施していましたが、現行のSKは、ファイルサーバエージェント対応により、非正規クライアントからのアクセス保護をこのエージェント (サーバアプリ) に切り出しているため、上記検証済みNASの場合でも、このエージェントは動作しません。 今後の予定もありません (NASのOSは、多くはLinuxベースの独自OSが多いため)	
b-10	環境	[共通] ファイルメーカーのファイルを保護できるか？	保護対象外。	
b-11	環境	[共通] アクセス制限はWindowsログインIDと連動しているのか？ (アクセス制限は別のID連用となるのか)	SecureKeeperのアクセス制限で使用するユーザIDはWindowsログオンIDとなります。ただし、SecureKeeperサーバに登録するユーザIDは、SecureKeeperの管理コンソール上で手動で入力することになります。	
b-12	ネットワーク	[共通] SafeSecureKeeperは、無線LAN環境で運用できますか？	・SafeSecureKeeperは、無線LAN環境では運用できません (現在制限事項)。 ・以下の現象が発生しています。 ⇒クライアント、サーバ間の接続ができません。 ⇒サーバからクライアントへのポリシー配信など下り電文が送信できません。 ⇒ネットワーク内で、製品の想定外の通信動作が発生します。	
b-13	ネットワーク	[共通] SafeSecureKeeperは、VPN環境で運用できるでしょうか？	SafeSecureKeeperは、VPN環境での運用はサポート外となります。 以下、開発元よりの回答となります ・VPN接続に関しては、VPNサービス自体、常に安定した通信を保障できるとは限りませんし、VPNサービスにおいても一般のLAN接続と比べ制限事項もある場合があります。 また開発元でも検証を行っていないこともあり、SecureKeeperではサポート外とさせて頂きたいと思っております。	

番号	キーワード	内容	回答	備考
b-14	ネットワーク	<p>[共通] ネットワーク環境が、CiscoカタリストのL3スイッチを介して、クライアントがファイルサーバへアクセスするという状況だが、問題はないか？</p>	<p>L3スイッチの設定次第なのですが、スイッチを通過するパケットをスイッチ側にて不要パケットとして処理される場合がございます。 SecureKeeperでは、定期的にSecureKeeperクライアント同士で通信を行い端末の状態を確認しますので、このパケットがスイッチ側にて破棄されてしまった場合には、正常に動作しない可能性が考えられます。 ・この機能を使っているのかが一番のポイントになるかと思えます。</p> <p>・スバニングツリーを利用しているか。利用している場合には経路情報が正しく設定されているか。</p> <p>・ファイルサーバへのアクセスがUNC形式で行われているか。 (IPアドレス指定でのアクセスはSecureKeeperは対応していません)</p> <p>&lt;&lt;ご参考&gt;&gt; またL3に限った話ではありませんが、Microsoft Windows Networkで確認できるネットワークの範囲とSecureKeeperで利用するUDPパケットの到達範囲を一致させなければ非正規端末の検知機能は正しく表示されません。(ネットワークの設定が困難と判断され、この機能を利用されないお客様もいらっしゃいます。) 全ての端末にSecureKeeperを導入するか、SecureKeeperを導入する端末と導入しない端末でネットワークを別にしてしまうのが理想ではありますが、しかし、現状は一部の端末に導入というのがほとんどです。正しく表示されないだけで、ログは収集しているため分析に時間を要せば非正規端末を見つけることができるので、既存ネットワークのまま非正規端末の検知機能を利用されているお客様がいらっしゃるのも事実です。</p>	
b-15	ネットワーク	<p>[共通] b-11.の例など、ネットワーク環境によって、クライアント同士の通信による端末の状態の確認が正常に動作しない場合、クライアントからファイルサーバの保護フォルダへのアクセス制限など、ポリシーに関する通信も正常に動作しないのか？</p>	<p>スイッチの設定で、管理サーバとクライアント間の通信で使用するポートが使用可能であれば、端末の状態の確認が正常に動作しない環境でも、ポリシーに関する通信は正常に動作する。 保護フォルダに対するアクセス制限などの動作に関しては運用は可能となる。</p>	
b-16	ネットワーク	<p>[共通] SecureKeeperサーバから、データの送信をおこなうことができないクライアントは、SecureKeeperで正常に管理できるでしょうか？</p>	<p>サーバからのクライアントへのポリシー反映処理ができないため、SecureKeeperは正常には動作しません。</p>	
b-17	ネットワーク	<p>[共通] SecureKeeperの管理サーバで、サブネットが異なる場所にあるファイルサーバを管理をしたいが、問題はあるか？</p>	<p>SecureKeeperサーバとサブネットが異なる場所のファイルサーバに関して管理は可能です。 ただし、SecureKeeperサーバから管理できるファイルサーバに関しては、以下の制限があります。</p> <ul style="list-style-type: none"> <li>・SecureKeeperサーバをインストールしているサーバ機で、管理対象にしたいファイルサーバが「マイネットワーク」→「ネットワーク全体」→「Microsoft Windows Network」→「ドメイン (Workgroup)」の順で選択していき、参照できる必要があります。</li> <li>・サブネットは異なっても管理できますが、SecureKeeperサーバとドメインが異なるファイルサーバは管理できません。</li> <li>・SecureKeeperクライアントに関してもSecureKeeperサーバ、ファイルサーバと同じドメインにいる必要があります。 SecureKeeperクライアントから、保護フォルダのあるファイルサーバを「コンピュータの検索」で検索したときに、ホスト名による検索に成功しないファイルサーバ内の保護フォルダに対しては、中のファイルへのアクセス権がなくなります。(ファイルオープンもできなくなります)</li> </ul>	
b-18	端末監視機能	<p>[共通] SecureKeeperの端末監視機能で非正規PC(不正接続PC)を検出する方法は？</p>	<ul style="list-style-type: none"> <li>・端末監視機能によって、非正規PCを検出する場合、管理コンソールの「端末状態」で、PCの一覧を表示します。 このとき非正規PCを表示するように設定すると、非正規PC(不正接続PC)はコンピュータ名の前に*がついた形で表示されます。</li> </ul>	
b-19	端末監視機能	<p>[共通] SecureKeeperの端末監視機能で非正規PC(不正接続PC)を検出するときに注意する必要がある点は？</p>	<ul style="list-style-type: none"> <li>・端末監視機能は、同一セグメントにあるSecureKeeperクライアントの内、1台が親端末として監視を実行します。</li> <li>・その親端末が監視をおこなうとき、正規PCとして認識するのは、SecureKeeperクライアントがインストールされており、かつ端末監視機能がONになっているPCとなります。</li> <li>・一方で、SecureKeeperクライアントがインストールされているPCは、端末監視機能のON/OFFに関係なく、SecureKeeperサーバと通信してポリシーを取得するときに正規PCとして認識されます。</li> <li>・このため、端末監視機能を実行する親端末がいる場合、その監視下のクライアントに端末監視機能をOFFにしたSecureKeeperクライアントPCがあると、そのPCはSecureKeeperサーバからは正規PCであり、かつ非正規PCであると認識されます。</li> <li>・このようなPCは、管理コンソールの「端末状態」のPC一覧に「正規PC」「非正規PC(*付き)」両方として、二重に表示されてしまいます。</li> <li>・この状態で本当の非正規PC(SecureKeeperクライアント未インストールPC)を検出するには、「端末状態」のPC一覧で、「コンピュータ名」によるソートを行います。「コンピュータ名」でソートすると、「正規PC」と「非正規PC(*付き)」は並んで表示されます。 この状態で、(*がついている)非正規PCとしてのみコンピュータ名画表示されているPCが、本当の非正規PCということになります。</li> </ul>	<p>※端末監視機能のON/OFFはクライアントインストール時でのみ設定できます。 一部のクライアントのみ端末監視機能をONにするといった運用は、端末監視機能の正規の運用ではありません。 通常の運用では、クライアントの端末監視機能は、全てON、全てOFFのどちらかの設定にしてください。</p>
b-20	制限仕様	<p>[共通] 制限事項「5-1持ち出し抑止」の「(1)エクスプローラ」で、「ネットワークドライブへの書き込み抑止はできません。」とあるが、具体的にどのような 操作をすると書き込みができてしまうのか？</p>	<ul style="list-style-type: none"> <li>・ネットワークドライブとして割り当てているドライブを書き込み抑止しても抑止はかかりません。</li> <li>・SecureKeeperはエンドポイントの情報漏洩対策ソフトですので、他のサーバやPCへの書き込みを抑止する必要はないという考え方です。</li> </ul>	
b-21	制限仕様	<p>[共通] 制限事項「5-2 保護フォルダ」の「(1)保護フォルダ制限」の「・保護フォルダ上のファイルをオープンした状態で通常のフォルダの同種別のファイルをオープンした場合、保護フォルダの権限が継承されます。」とは、具体的にどのようなことなのか？</p>	<ul style="list-style-type: none"> <li>・具体例としては、オープン権しかない保護フォルダのEXCEL A.XLSをオープンし、ローカルドライブのEXCEL B.XLSをオープンした場合、B.XLSに対してもA.XLSの権限(オープン権のみ)が継承されます。これは権限がファイル単位ではなく起動されたアプリケーションに対して付与されるためです。 このため、A. XLSを開くと、B. XLSは元の通常のEXCELファイルとして操作できるようになります。</li> </ul>	
b-22	制限仕様	<p>[共通] メールの添付ファイル禁止の対応メールソフトはOutlookのみとあるが、「Becky」はどうか？</p>	<p>SecureKeeperで対応しているメールクライアントは、OutlookExpressとなります。 「Becky」など、OutlookExpress以外の製品でも対応できる可能性はありますが、動作の保証はできません。 また、Webメールには、対応できません。</p>	

番号	キーワード	内容	回答	備考
b-23	保護フォルダ	[共通] 保護フォルダ内のファイルに対して、直接アドレス(フルパス)を指定してアクセスした場合、アクセス権の制御はどうか？	・SecureKeeperはエクスプローラを制御することによってアクセス権を制御しております。 ・ファイルのアドレスを直に指定し、エクスプローラが介されないアクセスを行った場合正常動作を保障できません。	
b-24	保護フォルダ	[共通] 保護を設定したフォルダをクライアントからアクセスする場合、保護フォルダのファイルサーバを「コンピュータの検索」でIPアドレス(192.168.0.1など)による検索を行なった場合、検出したファイルサーバ内の保護フォルダ下のファイルをオープンすることができないのは仕様でしょうか？	・仕様です。 ・SecureKeeperではUNC形式(\\ファイルサーバ名\共有フォルダ名\保護フォルダ名)にて動作するため、ファイルサーバ名にて指定する必要があります。 ・IPアドレスによってコンピュータの検索を行い、その中の保護フォルダ下のファイルへアクセスすると、「アクセスログ」の「区分」が「違反(未遂)」となることで確認できます。	
b-25	保護フォルダ	[共通] 保護フォルダへの書き込み時はどのような制限があるか？ ・新規作成ファイル保存時 ・既存ファイルを上書き保存する場合 …など。	・保護フォルダへの書き込みに関しては、以下の制限があります。  →保護フォルダへのファイルのコピー(アップロード) ・保護フォルダ内へのファイルコピーに関してはSecureKeeperのアクセス権によらず可能です。 ・保護フォルダ内へファイルをコピーした場合、コピー元ファイルは自動的に削除されます。 ・そのため、形態としてはコピーではなく移動ということになります。  →既存のファイルと同名のファイルを保護フォルダへコピーする場合 ・コピー元のファイルは自動的にファイル名が変更された状態でコピーされます。  →ファイルの新規作成 ・保護フォルダ内では、アクセス権に関係なくファイル、フォルダの新規作成はできません。 ・制限をおこなうフォルダへファイルを作成する場合は、ローカルで作成したファイルをそのフォルダへコピーする必要があります。  →既存ファイルを上書き保存する場合 ・既存ファイルに対し、オープンしたアクセス権を持つユーザは、そのファイルの内容変更と上書き保存する権限を自動的に得ます。 ・ファイルの参照のみ可能で、書き換えが不可といった設定はできません。 ・上書き保存を禁止したい場合は、Excelのシートのパスワードによる保護などの対策が別途必要です。	
c-1	バックアップ/リカバリ	[サーバ] SafeSecureKeeperを運用するにあたって、SafeSecureKeeper管理サーバ(SKServer)のバックアップ、リカバリ手順について教えてください。	SecureKeeperは、クライアントのポリシー・ログ情報などシステムの動作に必要な設定値・記録をSQLServerのDB内に保持しています。 したがって、SQLServer内の各テーブルのバックアップがあれば緊急時のリカバリが可能です。 (手順例としては以下の通り) バックアップ手順 ・SQLServerの管理ツール(Enterprise Manager)で、管理サーバ用のデータベース(SecureDB)のバックアップ(データベースのアイコン上で右クリックメニューから「すべてのタスク」⇒「データベースのバックアップ」を選択)を実施しておく。  リカバリ手順 ・OSから再インストールしたサーバにSQLServerをインストールする。 ・管理サーバを新規インストールする。 ・SQLServerの管理ツールで管理サーバ用のデータベース(SecureDB)の復元(データベースのアイコン上で右クリックメニューから「すべてのタスク」⇒「データベースの復元」を選択)を実施する。	
c-2	環境	[サーバ] SafeSecureKeeperは、ファイルサーバとの共有可能か？	・ファイルサーバとSafeSecureKeeperサーバ ファイルサーバとのSecureKeeperサーバの同居は可能です。 ただし、Windowsサーバですので、定期的な再起動が必要になります。 運用に影響がないよう十分にサーバ設計、運用設計をお願い致します。  ・ファイルサーバとSafeSecureKeeperクライアント SecureKeeperクライアントとファイルサーバの同居は保障外となります。 SecureKeeperではファイルサーバをサーバOSにて動作していると判断しております。 サーバOSはSecureKeeperクライアントの動作OSには入っておりませんので保障外となります。 クライアントOSのフォルダ共有に制限をかけることに関しては保障できません。	
c-3	ログ	[サーバ] 印刷ログについての詳細な仕様は？	■全体ログ内の印刷ログと、アクセスログ内の印刷ログの関係 ・(保護フォルダ内のファイルを印刷した場合、印刷ログは)二重に収集します。  ■全体ログ内の印刷ログと、アクセスログ内の印刷ログに記録される情報について ・印刷に関する詳細な情報は全体ログ側にて収集されます。 印刷枚数などはWindows標準スプーラに入った時点で取得するためです。 ・アクセスログ側では、保護フォルダ内のファイルで印刷というアクションがとられたことのみを収集しております。	
c-4	ログ	[サーバ] 管理コンソールの「全体ログ」に記憶される「印刷情報ログ」の内容で、「所有者」の項目にはなんの情報が記録されるか？	・印刷のログの中の「所有者」には、印刷を実行したクライアントへのWindowsのログオンユーザー名が入ります。 ＜例＞ 1.クライアントに「USER1」でWindowsログオンを実行。 2.ログオンしたクライアントで印刷を実行。 3.「所有者」には「USER1」が記録されます。  ・プリンタサーバーを使用した印刷の時に、プリンタサーバーとの接続にログオン認証が必要だった場合、そのログオン認証をおこなったユーザー名が入ります。 ＜例＞ 1.クライアントに「USER1」でWindowsログオンを実行。 2.印刷をおこなうプリンタサーバーへ接続しようとして、ログオン認証が発生。 3.プリンタサーバーへ「USER2」でログオンを実行。 4.プリンタサーバーで印刷を実行。 5.「所有者」には「USER2」が記録されます。  ※印刷ログの例の中に、「総ページ数」という項目がありますが、現在のバージョンでは「総ページ数」に関しては記録しないようになっています。	

番号	キーワード	内容	回答	備考
c-5	ログ	[サーバ] 管理コンソールの「全体ログ」に記憶される「ログイン、ログオフ」は、Windowsログオン、ログオフの記録か？	・管理コンソールの「全体ログ」に記憶される「ログイン、ログオフ」は、以下の記録です。 ・SecureKeeperクライアントがインストールされているPCが電源ONしたとき、SecureKeeperサーバーへ「ログイン」を通知します。 ・SecureKeeperクライアントがインストールされているPCでWindowsのシャットダウン処理がおこなわれたとき（「Windowsのシャットダウン」で「シャットダウン」が「再起動」が選択されたとき）、SecureKeeperサーバーへ「ログオフ」を通知します。 ※ログを記録するのはSecureKeeperサーバーなので、SecureKeeperクライアントからの「ログイン、ログオフ」通知が届かない（ネットワークが切断されているなど）場合、ログは記録されません。 ※「ログオフ」は、Windowsのシャットダウンが発生したときに通知するため、PCの電源コードを抜いたりして電源をOFFした場合はログは記録されません。	
c-6	管理サーバ	[サーバ] SafeSecureKeeperでは、管理サーバがダウンすると各クライアントから保護フォルダ内のファイルへのアクセスはできるのでしょうか？	SafeSecureKeeperでは、管理サーバがダウンすると各クライアントから保護フォルダ内のファイルへのアクセスができなくなります。 これは、SafeSecureKeeperでは、クライアントから保護フォルダ内のファイルへアクセスする時に逐次クライアントと管理サーバとの通信が必要なためです。  このような状態になった場合、保護フォルダ内のファイルへのクライアントからのアクセスを可能にするには、管理サーバを復活させる必要があります。 管理サーバの復活がすぐにできない時に、保護フォルダ内のファイルが緊急必要になった場合は、保護フォルダ内の必要なファイルを別途作成したフォルダへコピーし、そのフォルダをネットワーク共有で公開することで、クライアントからのアクセスを可能にすることはできます。 ただし、この場合はSafeSecureKeeperの保護はできず、ログを収集することもできません。	
d-1	環境	[クライアント] NECのPC98シリーズ製品（OSはWindowsNT4.0）で正常に運用できるか？	NECのPC98シリーズ製品に関しては未検証。 NECのOSは、他社OSと別体系であった時期が長くあるため、同じWindowsNT4.0とはいっても別OSと考える必要があり、検証できていないということからサポート対象ということではできない状況です。	
d-2	環境	[クライアント] SecureKeeperクライアントは、OSがWindowsMeのPCに対して導入できるでしょうか？（動作OSには98SEがあってMeはないですが、動作するのでしょうか）	Meは動作対象外OSです。動作保障できません。	
d-3	環境	[クライアント] SecureKeeperクライアントを動作対象外Windows系OS（WindowsMe）にインストールしようとしたところ、インストーラが「動作対象OSではないので終了します」といった意味のメッセージを表示して終了してしまいました。 動作対象外OSに、SecureKeeperクライアントはインストールできないのでしょうか？	SecureKeeperクライアントのインストーラでは、インストールしようとしたPCのOSをチェックし、動作対象外のOSの場合終了してしまいます。 SecureKeeperクライアントは、動作対象OS以外にはインストールできません。	
d-4	環境	[クライアント] SecureKeeperクライアントは、インストーラで動作対象外のOSへのインストールができないようになってきているということですが、SecureKeeperサーバと管理コンソールについては、インストーラで動作対象外OSへのインストールができないようになっていないのでしょうか？	SecureKeeperサーバ、および管理コンソールのインストーラでは、インストール先のOSをチェックしていません。 そのため、SecureKeeperサーバ、および管理コンソールは、動作対象外のOS（WindowsXPなど）にもインストールできます。 ただし、動作対象外のOS上での動作に関しては保証できませんので、必ず動作対象のOSにインストールしてください。	3.05.0009にて対処済み
d-5	環境	[クライアント] アクセス制限はWindowsログインIDと連動しているのか？（アクセス制限は別のID運用となるのか）	SecureKeeperのアクセス制限で使用するユーザIDはWindowsログオンIDとなります。ただし、SecureKeeperサーバに登録するユーザIDは、SecureKeeperの管理コンソール上で手動で入力することになります。	
d-6	保護フォルダ	[クライアント] 保護フォルダへの書き込み時はどのような制限があるか？ ・新規作成ファイル保存時 ・既存ファイルを上書き保存する場合 ・・・など。	・保護フォルダへの書き込みに関しては、以下の制限があります。  →保護フォルダへのファイルのコピー（アップロード） ・保護フォルダ内へのファイルコピーに関してはSecureKeeperのアクセス権によらず可能です。 保護フォルダ内へファイルをコピーした場合、コピー元ファイルは自動的に削除されます。 そのため、形態としてはコピーではなく移動ということになります。  →既存のファイルと同名のファイルを保護フォルダへコピーする場合 ・コピー元のファイルは自動的にファイル名が変更された状態でコピーされます。  →ファイルの新規作成 ・保護フォルダ内では、アクセス権に関係なくファイル、フォルダの新規作成はできません。 制限をおこなうフォルダへファイルを作成する場合は、ローカルで作成したファイルをそのフォルダへコピーする必要があります。  →既存ファイルを上書き保存する場合 ・既存ファイルに対し、オープンしたアクセス権を持つユーザは、そのファイルの内容変更と上書き保存する権限を自動的に得ます。 ファイルの参照のみ可能で、書き換えが不可といった設定はできません。 上書き保存を禁止したい場合は、Excelのシートのパスワードによる保護などの対策が別途必要です。	