必要なセキュリティ対策がわかる本

日本コンピュータシステム販売店協会
サポートサービス委員会

目次

Asahi. Com より

コースター脱輪、女性死亡19人けが
大阪・万博公園　2007年05月05日

5日午後0時50分ごろ、大阪府吹田市千里万博公園の遊園地「エキスポランド」で、ジェットコースター「風神雷神（ふうじんらいじん）2」（6両編成）が脱線し、2両目にいた女性客が車両とレール左側の手すりに挟まれて死亡、他の乗客19人が重軽傷を負った。大阪府警は、車軸の一部が折れて車輪が脱落し、車両が左側に傾いたとみて、業務上過失致死傷の疑いで吹田署に捜査本部を設置し、6日にもエキスポランド社（山田三郎社長）など数カ所を家宅捜索する方針。

エレベーター事故から1カ月
「シンドラー離れ」各地に　2006年07月03日

東京都港区で男子高校生（16）がエレベーターに挟まれて死亡する事故が起きて、3日で1カ月。各地の公的施設で、シンドラーエレベータ社製品の設置をやめたり入札から同社を外したりする動きが広がっている。既に結んだ契約を解消するよう求めたところもある。事故原因は特定されていないが、不具合の続発と事故後の同社の対応に批判が高まったことが影響しているようだ。

航空機データ、ネットに流出　ウイルス感染か
海保庁　2007年05月05日

海上保安庁は、海保が購入を決めた捜索・警備用航空機の仕様データの一部が、本庁航空機課に昨年度所属していた職員の私有パソコンからインターネット上に流出したと5日発表した。このパソコンにファイル交換ソフト「Winny（ウィニー）」が導入された結果、ウイルスに感染したとみて調べている。流出分から機密情報や個人情報は確認されていないという。

JISA、情報サービス産業の内部統制へ指針公表

2007年07月31日

情報サービス産業協会（JISA、浜口友一会長）は30日、08年4月から適用が始まる内部統制報告制度（日本版SOX法）を踏まえた「情報サービス産業における内部統制ガイドライン」を公表した。情報サービス産業に関する会計基準などに対応。情報サービス業界各社の内部統制に関する取り組みを支援することで、業界全体の信頼を高める。（中略） さらに内部統制の評価作業に役立つツールを含めたCDも用意した。同CDは作業前の現状を把握するための診断表や業務プロセスおよびIT全般の評価に必要な文書のひな型を、表計算ソフト（エクセル）形式のファイルで提供。このため非上場の中堅・中小企業でも、内部統制の整備に取り組むことができるという。

はじめに

最近、エレベータの事故やジェットコースターの事故など、死亡や重症に繋がる大きな事故が相次ぎ、企業の社会的責任が問われています。この事故原因に、起こり得るトラブルに対する認識の甘さ（例えば定期点検の不備）が上げられています。

事業を進める上では、様々なリスクがあらゆるところに潜んでおり、ひとたび注意を怠ると企業の存続をも脅かすダメージを受けることになります。このようなことにならないためにも、事前に事業を継続する上でのリスクを検討し、ダメージを最小限に抑え予防策を実践する「リスク管理」が必要です。

例えば、PC、サーバ、ネットワークなどからなるITシステムではどうでしょうか。PCやサーバが停止すると、日常の業務が停滞し、最悪の場合には日頃の取引に影響を及ぼします。また、日常のセキュリティ対策を怠ることで、大事なデータを破壊されたり、データを盗まれて公開されたりすることもあるでしょう。PCが遠隔からコントロールされ、知らぬ間に他企業のPCを攻撃することもあります。ITシステムには常にこのようなリスクが潜んでいます。

また、法規制による日常業務に対するリスクも存在します。一部上場企業は2008年4月から、日本版SOX法に対応する内部統制を行うことが義務付けられます。今後、その対象企業が取引のある企業に対し、取引の信頼性の担保として同様の統制を求めることも考えられます。この内部統制は、ITの積極的な活用が期待されており、その分上記のITにおけるリスク管理が重要となります。

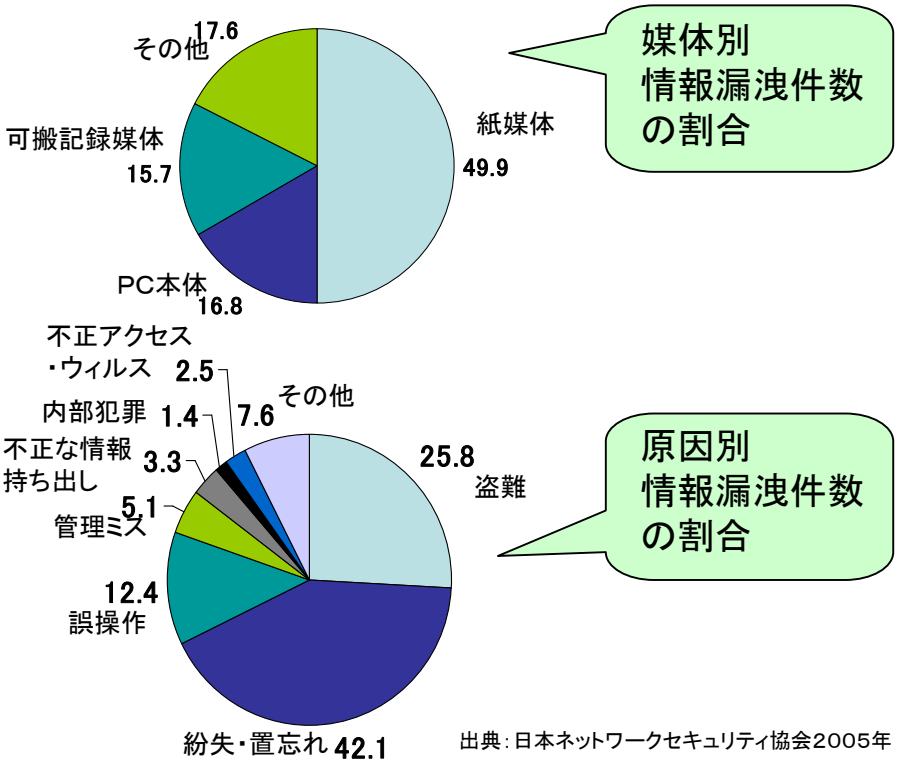
本書では、企業が予め準備しておくべきITにおけるリスク、その中でも特にセキュリティ対策について解説しています。

リスクを事前に理解し、対応策を立てる事でITシステムの信頼性を向上させることは、事業の強みにもなります。
この冊子が貴社ITシステム強化の参考になれば幸いです。

Ⅰ. ITシステムのリスク

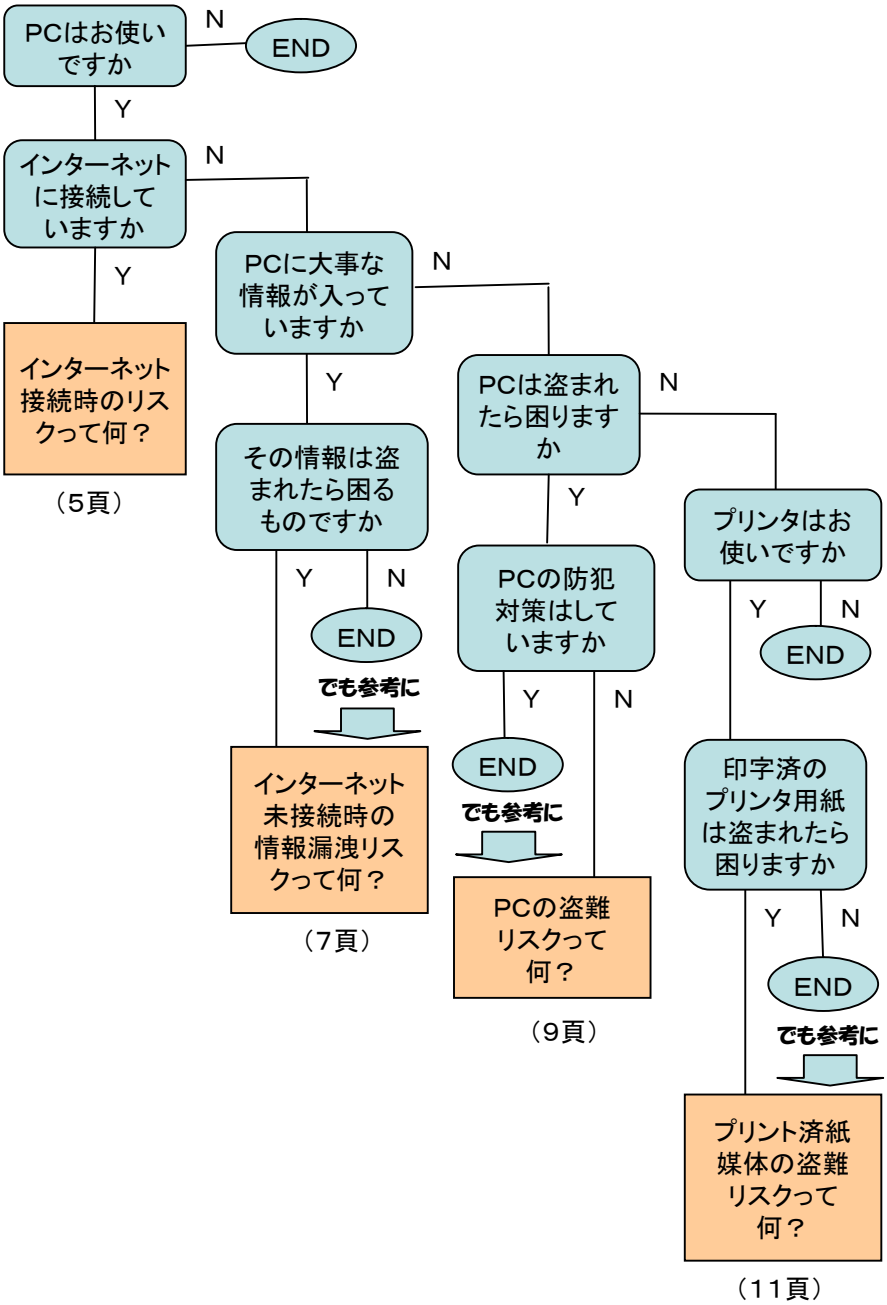
それでは、ITシステムにはどんな危険因子（リスク）が潜んでいるのでしょうか。

お使いのPCやサーバがネットワークやインターネットに接続されていないから、大丈夫だと思っていませんか。最近の統計によると、情報漏洩の原因の半分は、プリンタで印字された紙媒体によるものなのです。その次に多いのがPCの盗難・紛失等です。



出典：日本ネットワークセキュリティ協会2005年

次のページのフローに沿って進んでください。
どんなリスクがあるのかをそれぞれの場合で、見てみましょう。


PCはお使いですか
N
END
Y
インターネットに接続していますか
N
Y
インターネット接続時のリスクって何？
（5頁）
PCに大事な情報が入っていますか
N
Y
その情報は盗まれたら困るものですか
Y
N
END
でも参考に
インターネット未接続時の情報漏洩リスクって何？
（7頁）
PCは盗まれたら困りますか
N
Y
PCの防犯対策はしていますか
Y
N
END
でも参考に
PCの盗難リスクって何？
（9頁）
プリンタはお使いですか
Y
N
END
印字済のプリンタ用紙は盗まれたら困りますか
Y
N
END
でも参考に
プリント済紙媒体の盗難リスクって何？
（11頁）

インターネット接続時のリスクって何？

PCや、PCとサーバで構成される社内システム、そしてシステム上のデータが、インターネットに接続されるということは、堅牢なコンクリートで囲まれていた部屋から、公道に面したプレハブの建物に移動するようなものです。

コンクリートの部屋は外部からの進入に対しては防御は完全です。ですが、公道に面したプレハブでは、車が飛び込んでくる、泥棒も入りやすい、雨漏りもするでしょうし、地震・洪水などにはひとたまりもありません。従ってインターネットに接続したとたんに、社内システム及びシステム上のデータには様々な危険への対策が必要になってくるのです。

外部からの直接的な車の飛び込みに対しては、ファイアーウォール、泥棒の侵入に対してはウィルス対策、泥棒の仕掛ける盗聴装置や時限爆弾にはウィルススキャンによる検査、そして雨漏りに対してはフィルタリング、といったそれぞれのリスクへの対策が必要です。
更にこのような攻撃は、日々新手のものが出て来る為、常にメンテナンスを怠らないようサポートの更新を心がけ、被害にあったときにはすぐに犯人を捕まえるための捜査や、修理の依頼・問合せ、更には従業員に対する教育が必要になってきます。


ザ・インターネット
秘密情報が公開されてしまった！
空きポートから飛び込みが！
有害なアクセスが！
社内ITシステム
時限爆弾が！！

インターネット未接続時の情報漏洩リスクって何？

PCや、PCとサーバで構成される社内システム、そしてシステム上のデータが、コンクリートで囲まれた部屋にあれば、外部からの攻撃については問題ないでしょう。

しかしながら統計によると、情報漏洩の原因の7割は内部の犯行によるものなのです。
PCの盗難のリスクやプリンタ・紙媒体からの情報漏洩リスクについては、次項に説明してありますので、ここでは、それ以外のリスクについて説明します。

最近は、可搬型で小さく、容量の大きい媒体が増加してきています。すなわちCD、DVD、USBメモリ等です。これらは、ポケットにも入る為、紙媒体に比べて大量の情報を持ち出すことが可能です。悪意の無い場合でも家に仕事を持ち帰る為に、USBメモリにデータを入れ、帰る途中で紛失したケースがあります。また、悪意のある場合でも、情報を持ち出させないという抑止策をとることによって、情報漏洩のリスクを少なくすることが出来ます。

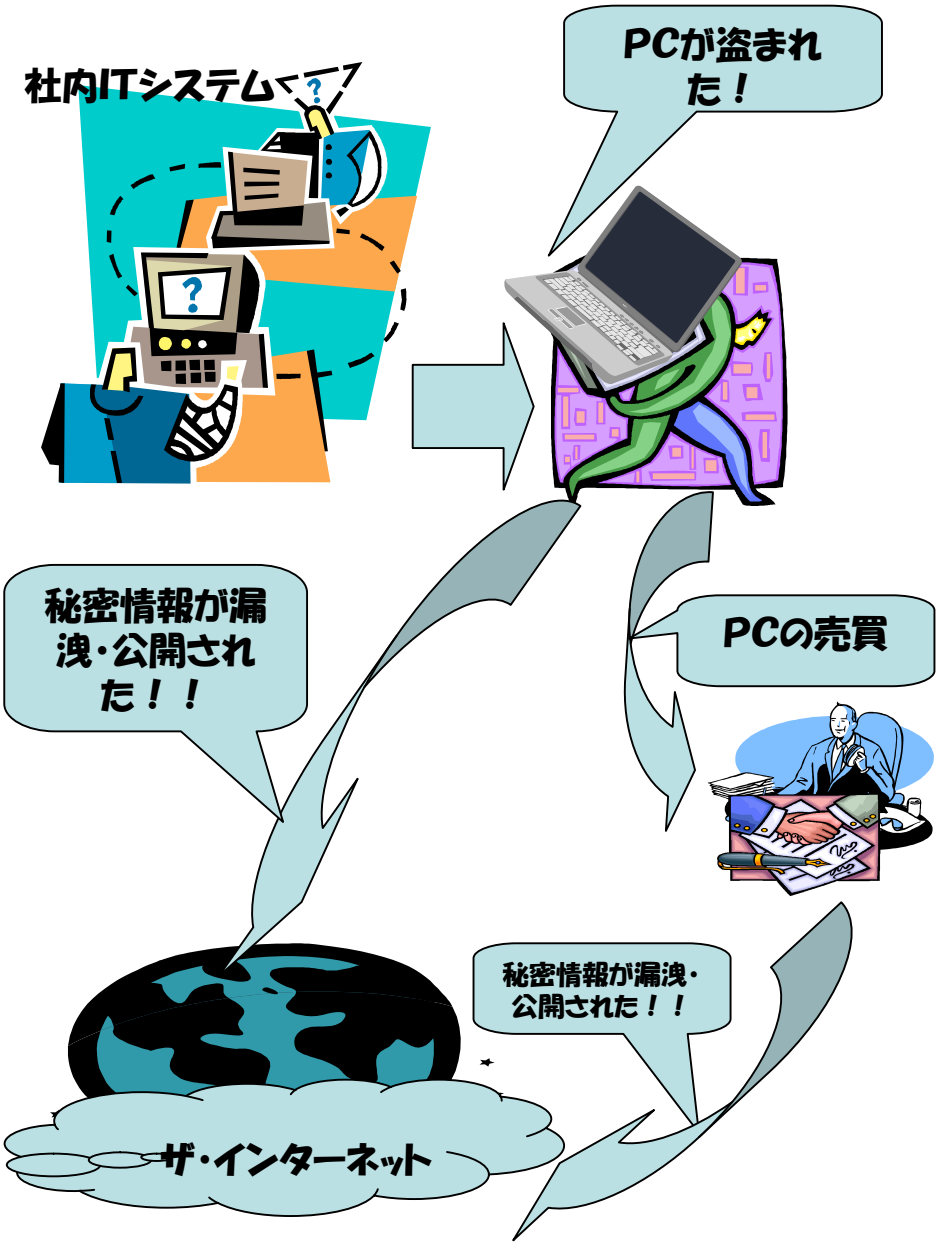

秘密情報が
外部に！！
社内ITシステム

PCの盗難リスクって何？

社内で使われるPCは、ノート型が使われる割合が
多くなってきました。これはデスクトップと比較しても
価格の差があまり無くなってきたこと、性能的にも
遜色がなくなってきたこと、モバイル端末としても使い
易くなってきたこと等に、その要因があると思われます。

ノートPCは、カバンに入れて持ち運びが出来る為、
人の出入りの多い職場では、比較的盗難が
多いと言われています。

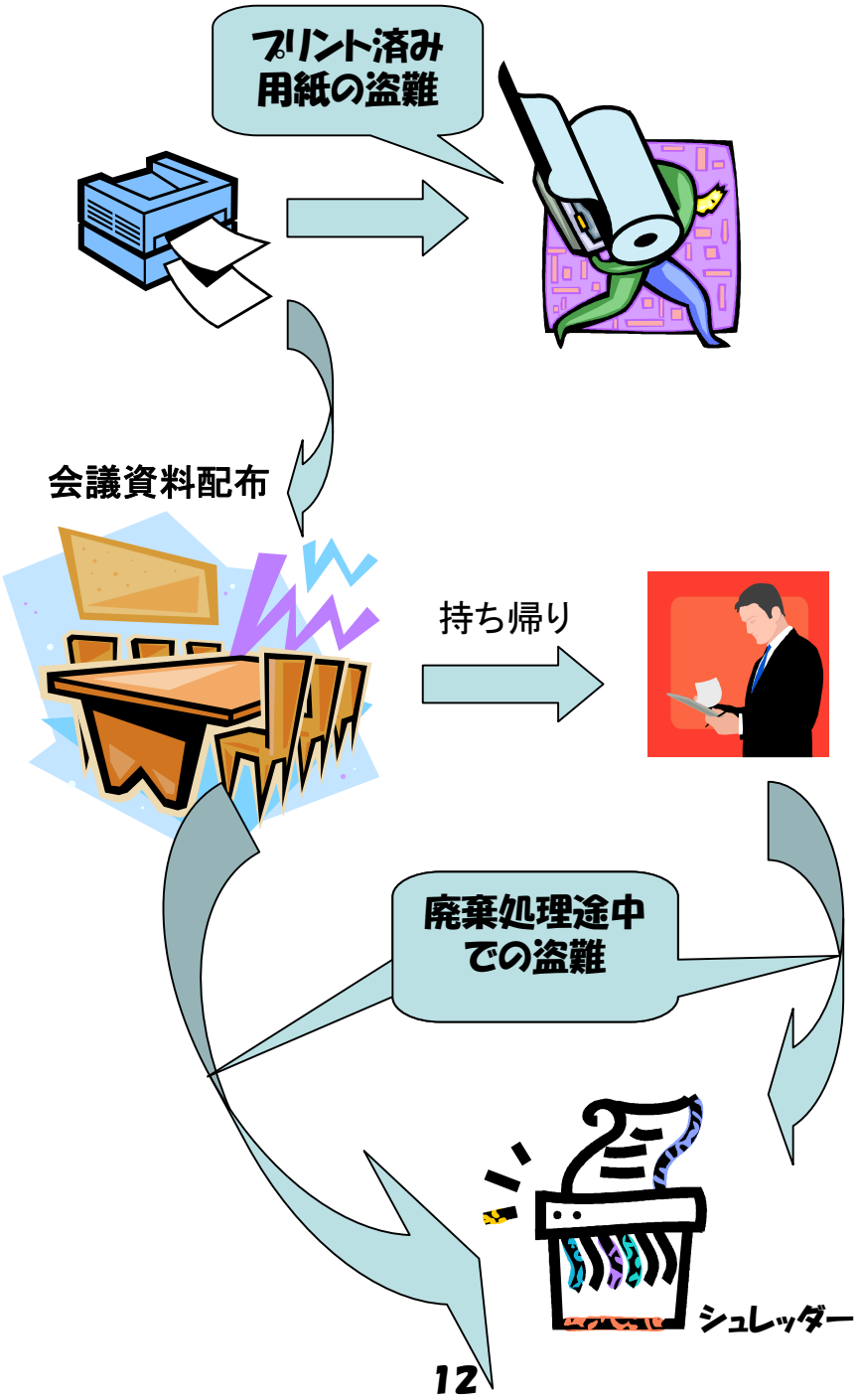
PCの内蔵メモリやディスク等には、通常、多くの情報が
入っています。これらの情報を、PCごと盗まれ、中にある
情報を公開されてしまう可能性があります。 PCの盗難
だけで被る被害よりも、情報の漏洩による被害の方が
格段に大きくなりますし、社会的信用の失墜につながる
ことも考えなければなりません。


社内ITシステム
PCが盗まれた！
秘密情報が漏洩・公開された！！
PCの売買
秘密情報が漏洩・公開された！！
ザ・インターネット

プリント済み紙媒体の盗難リスクって何？

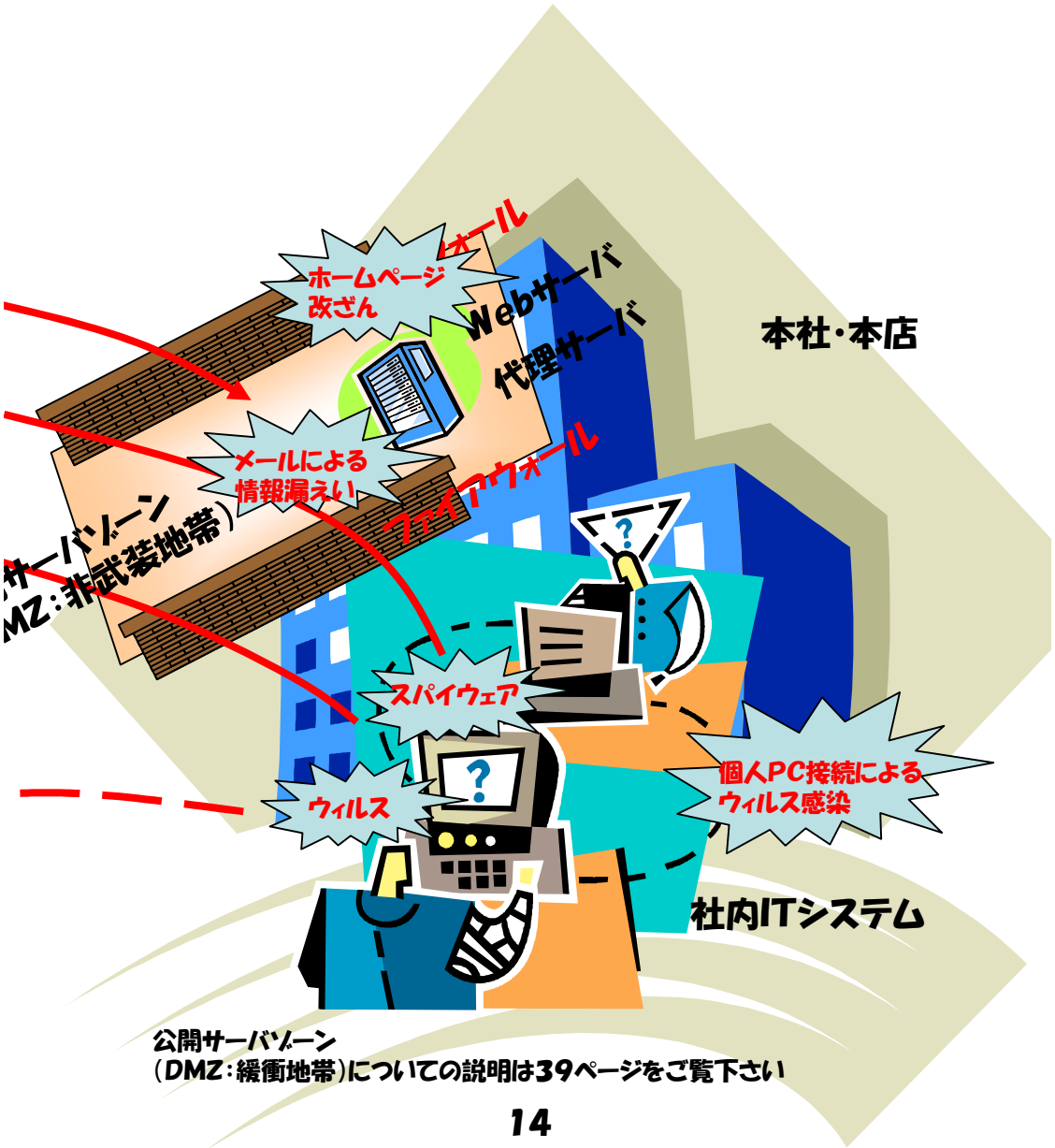
社内会議では会議資料をプリントアウトし、それをコピーして配布することが多くあります。社内会議ですから、その中には社外秘の情報が含まれる場合が殆どです。このプリント済みの紙媒体は、通常、出席者が自席に持ち帰り保管することになります。これらの過程でコピーが外部に流出する可能性もありますが、保管した書類を廃棄処分するときにも漏洩する可能性があるのです。

また、最近ではコピー機そのものに残っているデータを、情報漏洩を避ける為に消去したり、コピーした人を特定できる機能を持ったものも出てきています。


プリント済み
用紙の盗難
会議資料配布
持ち帰り
廃棄処理途中
での盗難
シュレッダー

それでは危険因子(リスク)を少し整理してみましょう
下の図は主に論理的なリスクを表現したものです

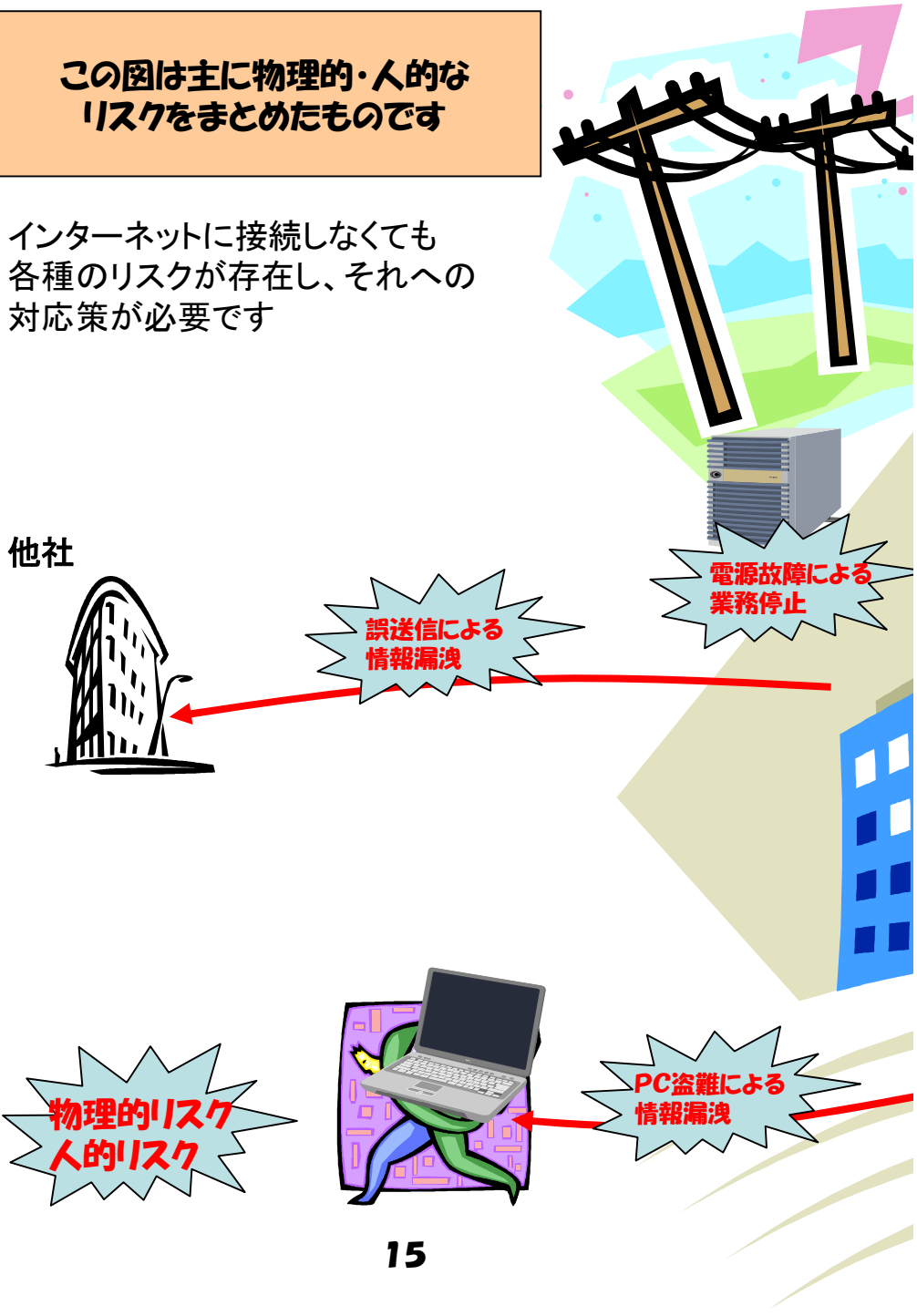
インターネットに接続すると数々の危険に晒される
ことになりますが、企業が現在の社会の中でビジネス
を継続・拡大していく為には、これらの危険を排除し
ながらインターネットを利用していく必要があります。

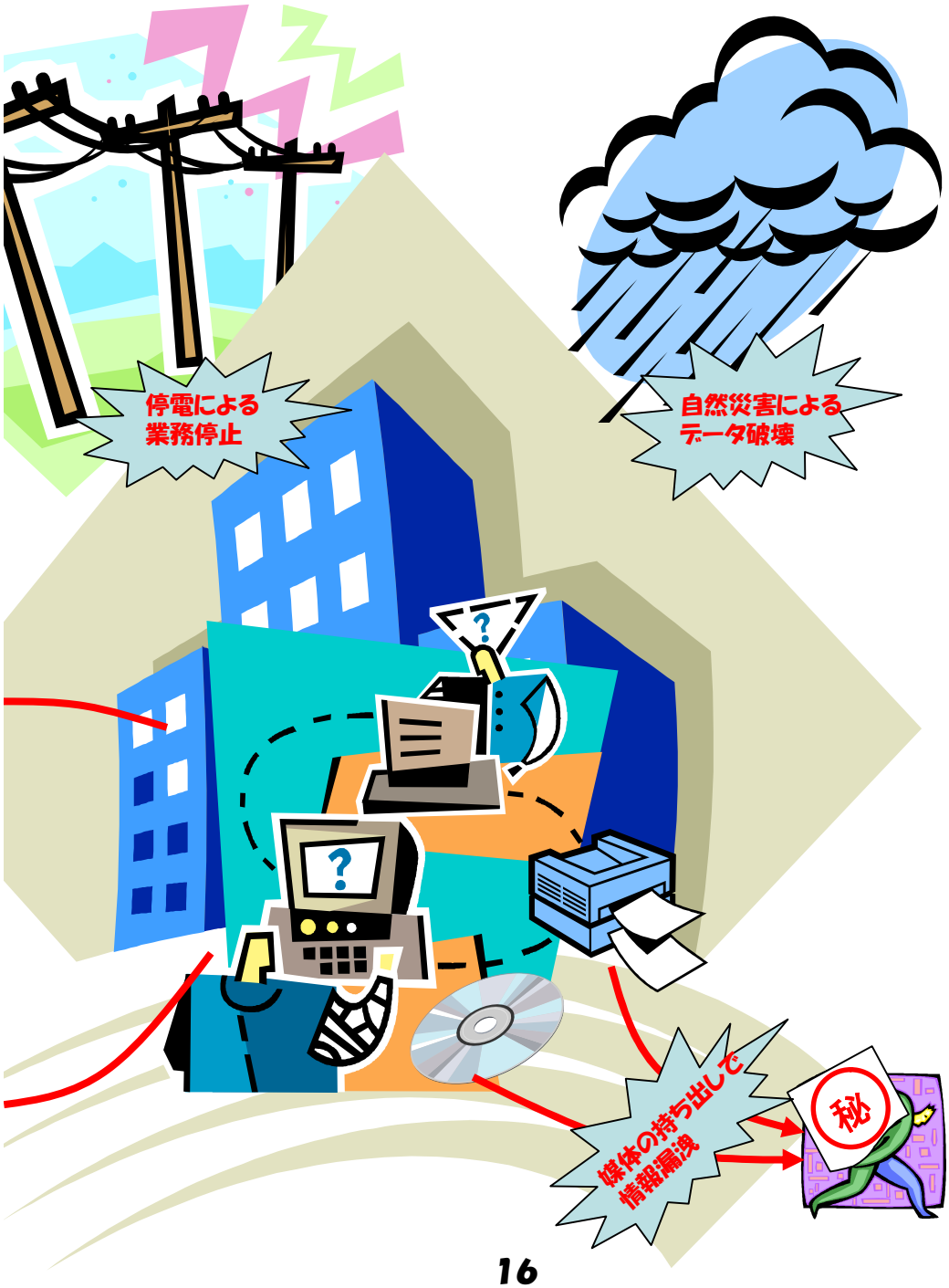


公開サーバゾーン
（DMZ：緩衝地帯）についての説明は39ページをご覧下さい

この図は主に物理的・人的な
リスクをまとめたものです

インターネットに接続しなくても
各種のリスクが存在し、それへの
対応策が必要です




停電による
業務停止
自然災害による
データ破壊
媒体の持ち出しで
情報漏洩
秘

II

ここからはじめよう、セキュリティ対策の第一歩

セキュリティ対策　ステップ　1

ここでは、すぐに実施すべき対策について
説明しています

インターネットに接続している場合はもちろん
接続していない社内システムにも危険因子
（リスク）は存在しています

リスクを認識し、対策をとることによって、情報
漏洩のみならず、企業の信用失墜にいたる
ような事態を、避けることが出来ます。

ステップ1に対応する対策をまとめると、次のようなものになります

1. 不正アクセスとファイアウォール導入
（ファイアウォール対策）
2. ウィルスとウィルス対策
（ウィルス対策）
3. スパイウェアとスパイウェア対策
（スパイウェア対策）
4. ウィルスやスパイウェアに感染しないために
（セキュリティパッチ配信）
5. 人の異動でIDの管理が混乱し、外部からの侵入を容易にするリスクとその対策
（ActiveDirectoryによるID管理）
6. PCに入っている情報の漏洩と対策
（ノートPC対策）
7. 外部からの侵入によりデータ等が改ざん・破壊されるリスクとその対策
（データバックアップ対策）
8. 社員へのセキュリティ教育
（情報セキュリティ教育）

～コラム（社員によるデータ流出リスク）～

II. ここからはじめよう、
セキュリティ対策の第一歩

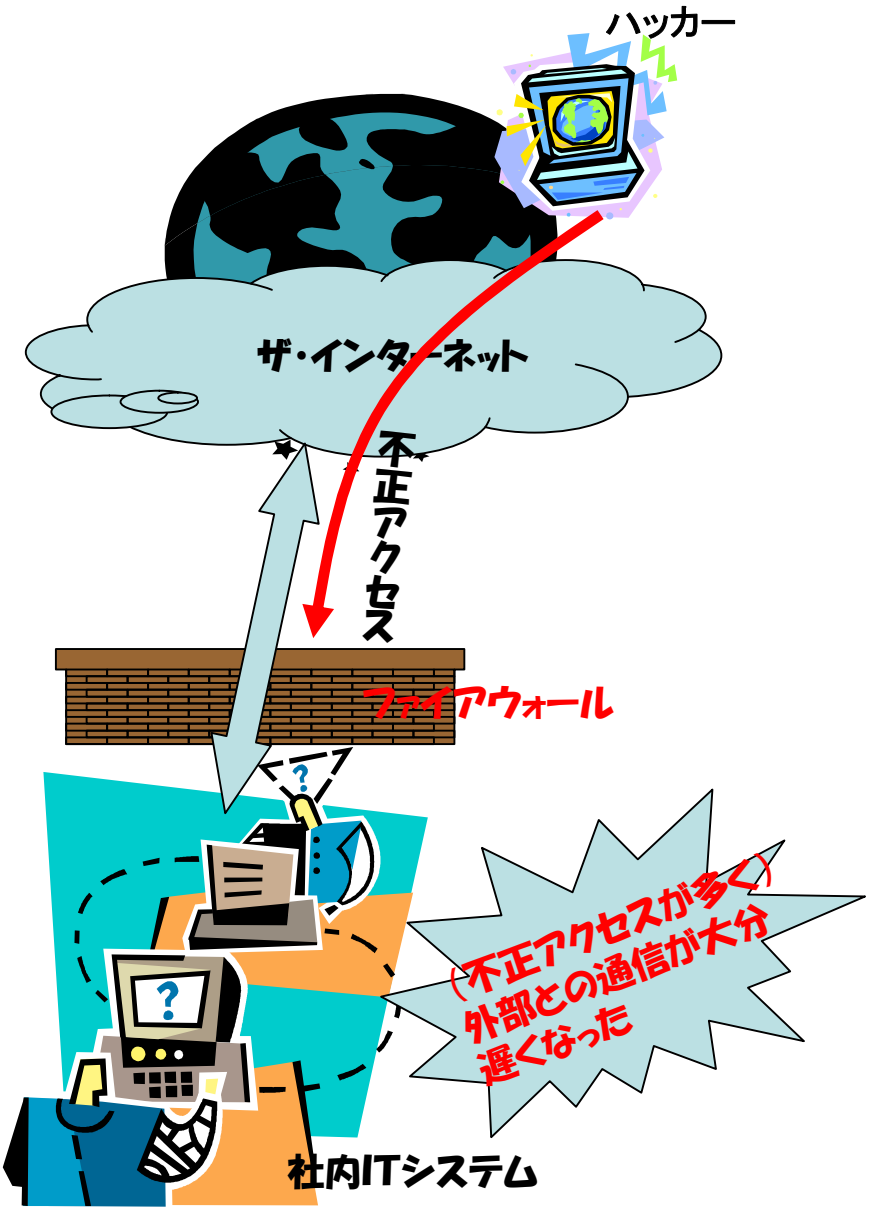
1. 不正アクセスとファイアウォール

ITシステムをインターネットに接続すると、そのITシステムは、全世界に対してオープンされたことになります。
あなたの企業のITシステムは、全世界の中で独自のアドレス（いわば住所）を与えられ、世界中のどの場所にも接続し、情報を得ることが出来ます。しかし、その反面世界中のどこからでも、あなたの企業に接続することができるということです。
世界中にはハッカーと呼ばれる、企業システムに侵入し悪事を働く輩が数多く存在し、常に侵入できるところを狙っているといっても過言ではありません。このハッカーが、色々な手段で企業システムに侵入しようと試みる事、また侵入することを「**不正アクセス**」といいます。

【対策】
この「**不正アクセス**」を少しでも食い止めようとする機能を持っているのが「**ファイアウォール**」と呼ばれるソフトウェア又はその機能を組み込んだ機器です。ハッカーは常に新たな方法で侵入を試みようとしています。「ファイアウォール」を導入した後も、常に状況を監視し必要に応じた対策をとっていく運用が、企業システムを侵入のリスクから守るのです。

【対応するメニュー】
ファイアウォール対策（ファイアウォール対策導入サービス）

セキュリティ対策　ステップ1－1



II. ここからはじめよう、
セキュリティ対策の第一歩

2. ウィルスとウィルス対策

ITシステムをインターネットに接続するためには、メールやWebの通信を行うための出入り口が必要です（これをポートといいます）。このポートを通ってウィルスがやってくるのです。ウィルスの中には、メールやWebを見ただけで感染したり、インターネットを通じて知らない間に感染するワーム型のウィルスもあります。

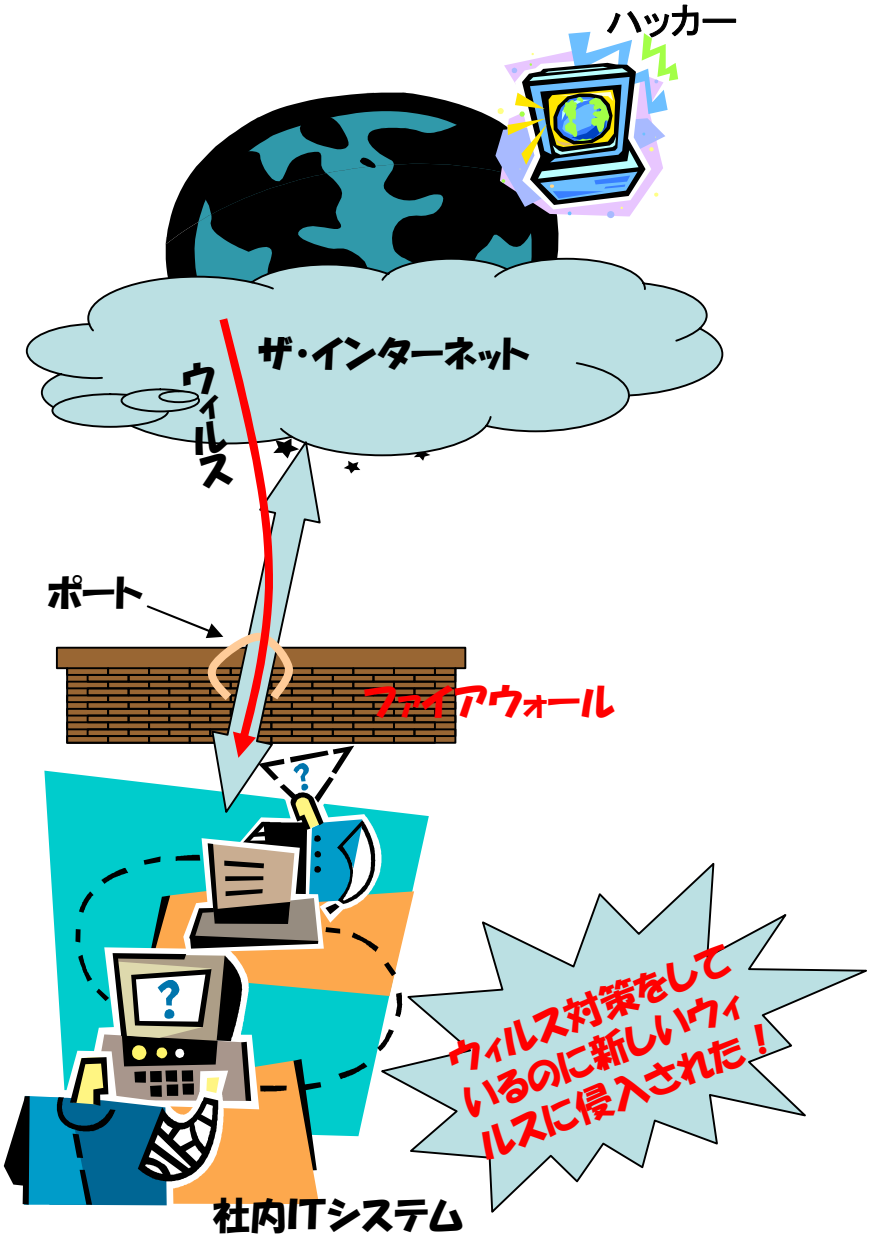
【対策】
ウィルスに感染しないようにする為に、PCやサーバに**ウィルス対策ソフト**を導入する必要があります。

PCによっては、インストールされているソフトウェアにウィルス対策ソフトが含まれている場合があります。また、プロバイダーによっては、ウィルス対策のサービスを提供しているところもありますので、導入前に調べておくのがいいでしょう。

ウィルスは常に新手のものが出てきます。これに対応する為には、**ウィルス検知用データ**（**パターンファイル**といいます）を最新のものに、常に更新しておく必要があります。ウィルス発生からパターンファイル更新までの間が短いほど、ウィルス感染の危険性は少なくなります。パターンファイルの自動更新の設定をお勧めします。

【対応メニュー】
ウィルス対策（ウイルス対策ソフト導入サービス）

セキュリティ対策　ステップ1－2



II. ここからはじめよう、
セキュリティ対策の第一歩

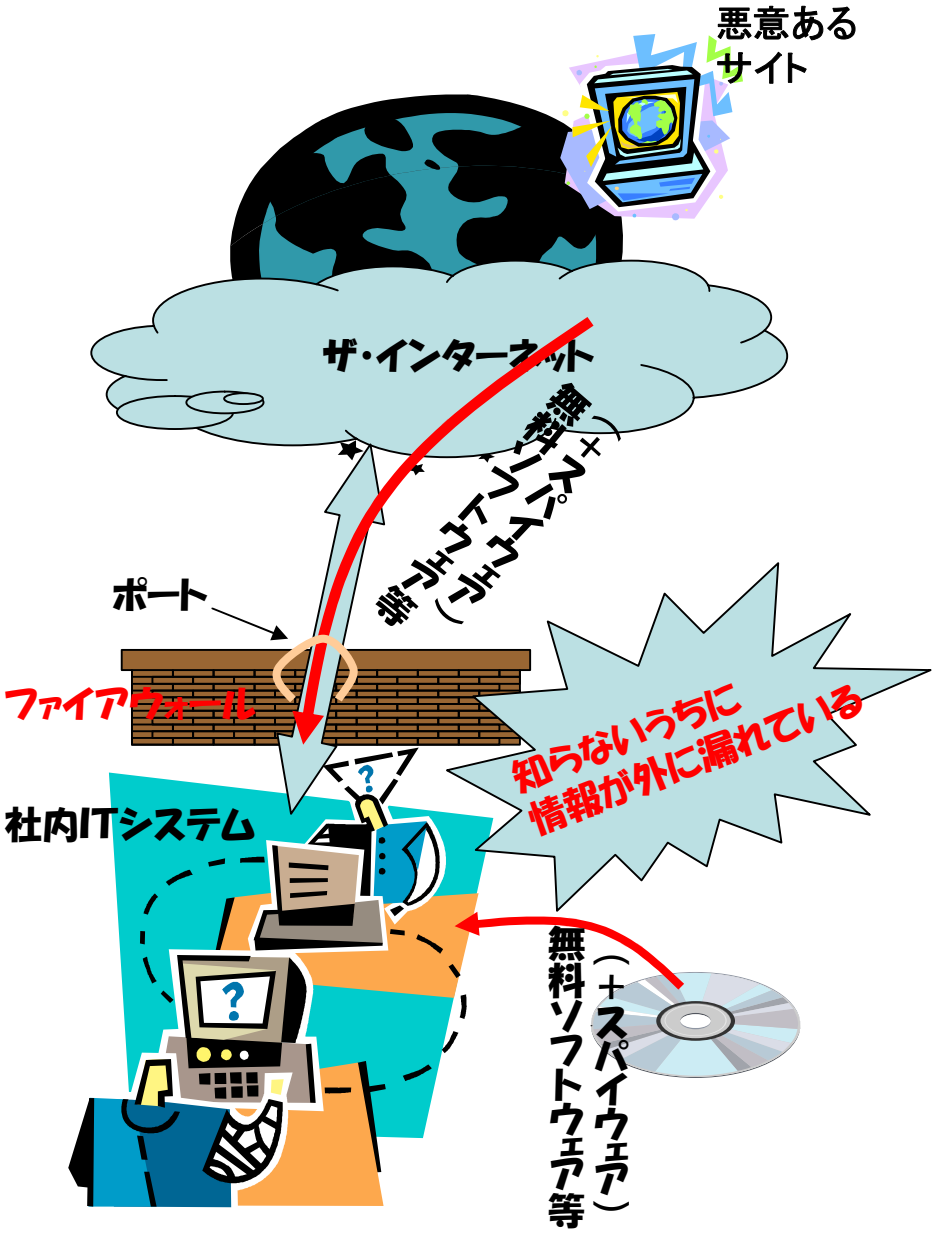
3. スパイウェアとスパイウェア対策

スパイウェアは通常、無料でダウンロード可能なソフトウェアや害のなさそうなソフトウェアに隠れています。このようなソフトウェアをPCにインストールすると、スパイウェアが一緒にインストールされ、知らないうちにPCが遠隔地からコントロールされていたり、各種設定を勝手に変更されたり、メールアドレスなどの個人情報を第三者に送信されたりします。また、PCの性能が低下したり、エラーを起こしたりもします。

【対策】
スパイウェアをインストールさせない為には、信頼できそうもないソフトウェアを**安易にインストールしない**ことが大切です。またインストールする際も「使用許諾契約書」をよく読んで、「同意します」のボタンを**不用意にクリックしない**事も重要です。
現在では、スパイウェアのインストールを防止してくれるソフトウェアも販売されています。最近では、ウィルス対策のソフトウェアの中にも、この機能が入ったものもあります。
また、通信のやり取りを監視したり、定期的に解析したりすることも、通常の業務を安心して行う為には重要ですがこれは次のステップで解説します。

【対応するメニュー】
スパイウェア対策（スパイウェア対策導入サービス）

セキュリティ対策　ステップ1－3



II. ここからはじめよう、
セキュリティ対策の第一歩

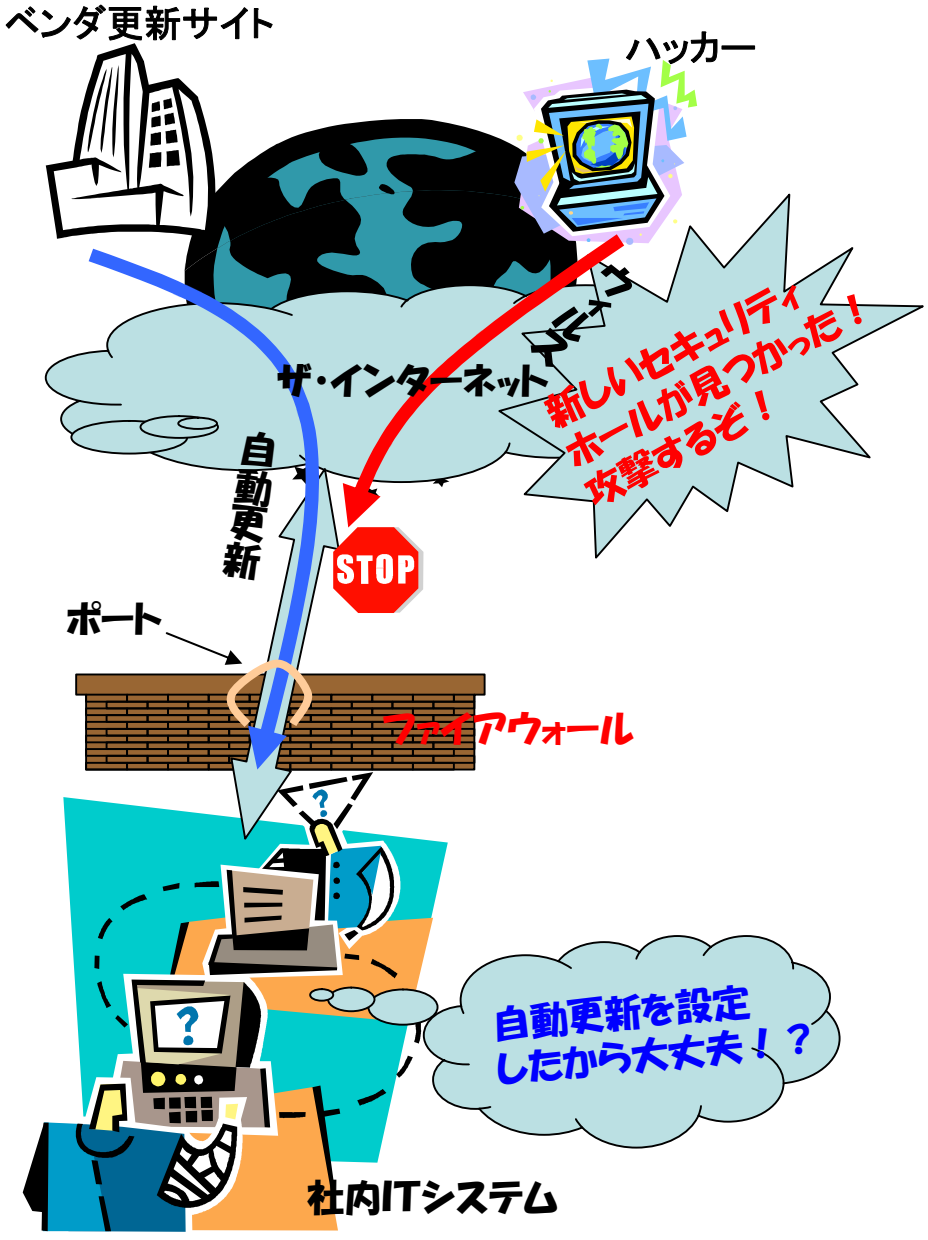
4. ウィルスやスパイウェアに感染しない為に

PCを動かす為にはOSやアプリケーションソフトが必要です。しかしこれらのソフトは常に**セキュリティホールの危険性を内在**しています。新しいOSやソフトウェアには日々、新しいセキュリティホールが見つかっており、これを狙ってハッカーが新しい攻撃を仕掛けてきます。ソフトウェアメーカーは、セキュリティホールの脆弱性をすぐに修正できる体制を持っていますが、それでも修正までの短い時間を狙ってくるハッカーも中にはいます。ベンダーは修正用の**パッチプログラム**をどんどん出してくるので、間違いなくこの修正をPCに適用できるようにしておくことが重要です。

【対策】
WindowsのOSには**自動更新の設定**が出来るような機能が設けられていますので、この機能を有効にしておき毎日更新が出来るようにします。自動更新ができないソフトはリビジョンアップの情報を常に注意し、早めの適用をすることが重要です。最近ではセキュリティパッチがリリースされるまでの間に、攻撃してくるゼロデイ攻撃というものも出てきています。自動更新だけでなく、定期的な内部ファイルのスキャンチェックも重要になってきています。

【対応するメニュー】
特になし（Windowsに含まれる機能）

セキュリティ対策　ステップ1－4



II. ここからはじめよう、
セキュリティ対策の第一歩

5. 人の異動でIDの管理が混乱し、外部からの侵入を容易にするリスクとその対策

頻繁に人が異動（組織間の移動、入社・退社等）する場合ファイルへのアクセスのための、IDやパスワードの変更が多く発生し、管理が出来なくなると、**退職したはずの人のIDが使われて**重要情報が盗み出される場合があります。また複数のシステムを使用しているため、それぞれ異なるパスワードを設定し、混乱してしまう経験をお持ちの方も多いでしょう。これらを簡単に、一元的に管理できれば、管理者の負担も大変軽くなるはずです。

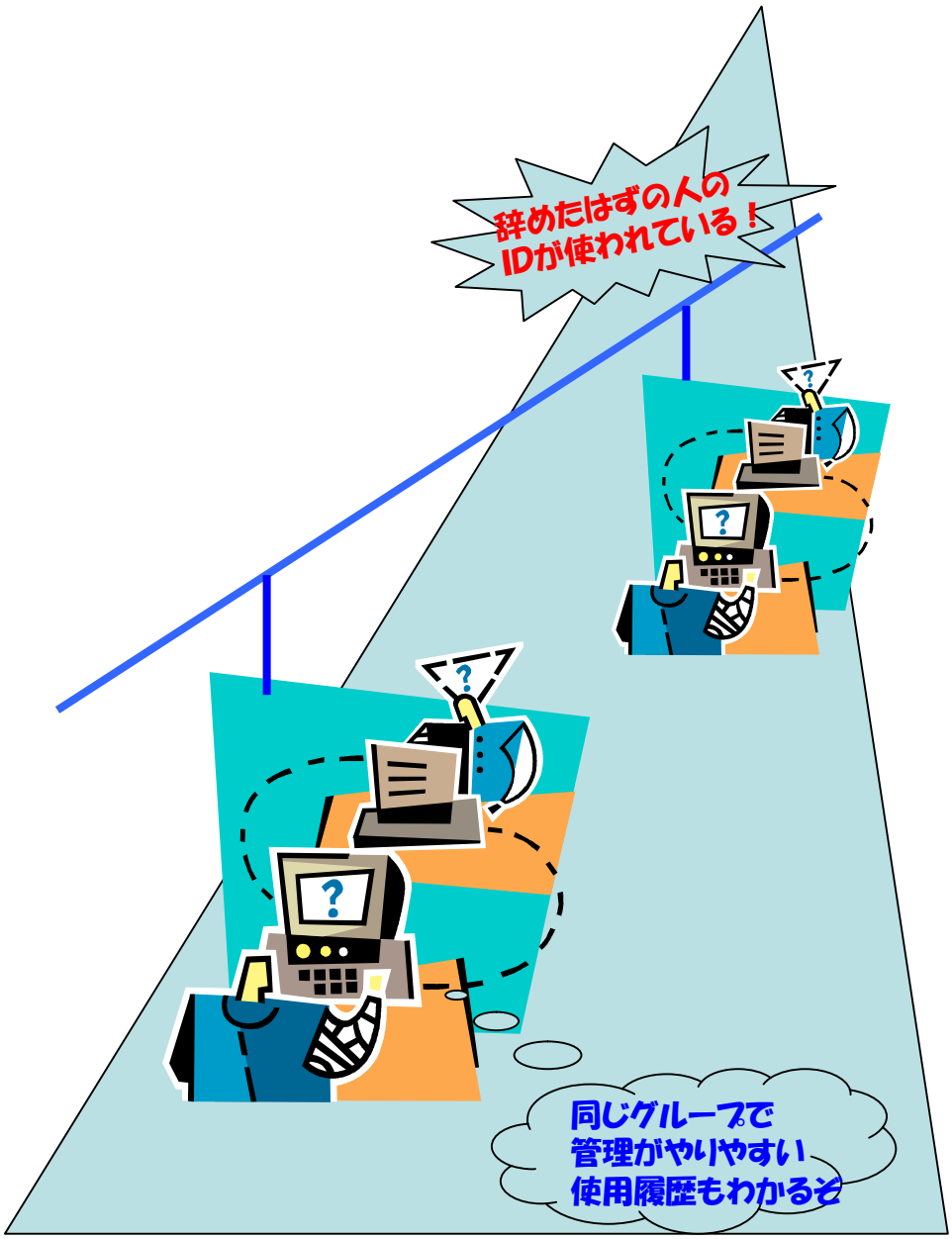
【対策】

複数のシステムへのIDやパスワードを一元的に管理する事の出来るツールが準備されています。**シングルサインオン**という、全てのシステムに共有できるひとつのIDで、複数のシステムにログインでき、アクセス制限もできる為セキュリティ上も好ましいものです。Windows2000のサーバーを使用している場合は、**アクティブディレクトリ**という機能を有効にすることでID・パスワード管理・アクセス管理、アクセスの記録の収集等が可能になります。ID管理は比較的規模が大きく複雑なシステムの管理に向いています。

【対応するメニュー】

ID管理システム構築サービス（アクティブディレクトリ）

セキュリティ対策　ステップ1ー5



II. ここからはじめよう、セキュリティ対策の第一歩

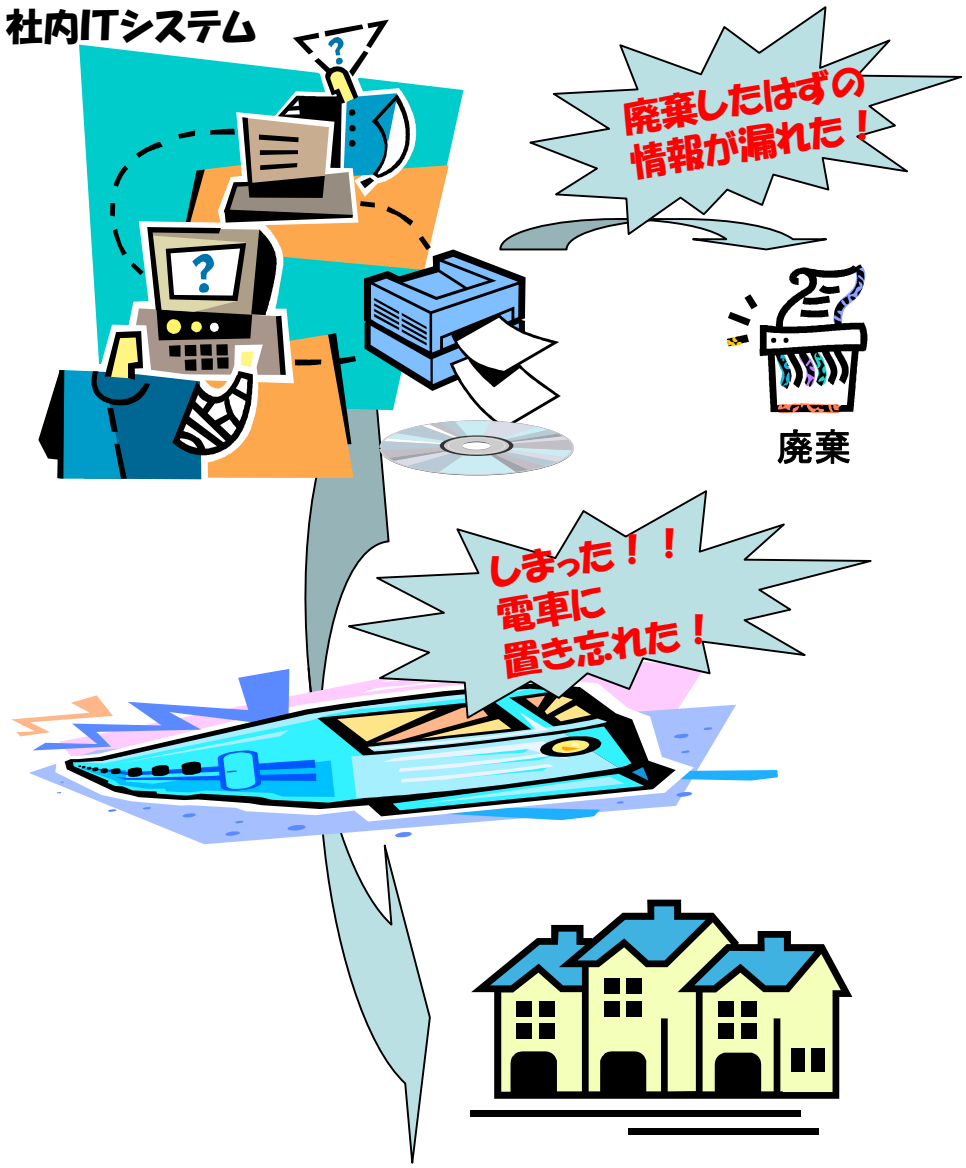
6. PCに入っている情報の漏洩と対策

業務でPCを使用している場合、PC内のディスクには業務で使用している、例えば売上の情報や、顧客情報、技術的な面では設計情報や、特許情報等が入っているのが、通常でしょう。これらの情報の中には、**外部に漏れると困る情報**が沢山含まれています。
これらの情報は、**悪意が無くても**、自宅で仕事の続きをやろうとして、ノートPCをカバンに入れて、帰る途中で電車の中で、つい「うとうと」して盗まれたり、また忘れたりすることが、よくあるのです。

【対策】
紙情報は、持ち帰る場合は、何のデータかわからないように、タイトルを消しておく等の方法があります。紙に比べて情報量の多いノートPCの場合は、**データそのものをディスクに出力時に暗号化**しておく方法があります。こうすれば盗難にあった場合にも、中身を読まれる心配がなくなります。
外部の人による悪意のある犯行を回避する為には、PCそのものを立ち上げるときの**パスワード**を必ず設定しておくことが重要です。内部の人による悪意ある犯行の回避にはファイルへの**アクセスのログ**を必ずとっておき、誰がアクセスしたかが必ずわかることを、公表しておくことで牽制機能を働かせることも必要です。

【対応メニュー】
ノートPC対策

セキュリティ対策　ステップ1－6



II. ここからはじめよう、セキュリティ対策の第一歩

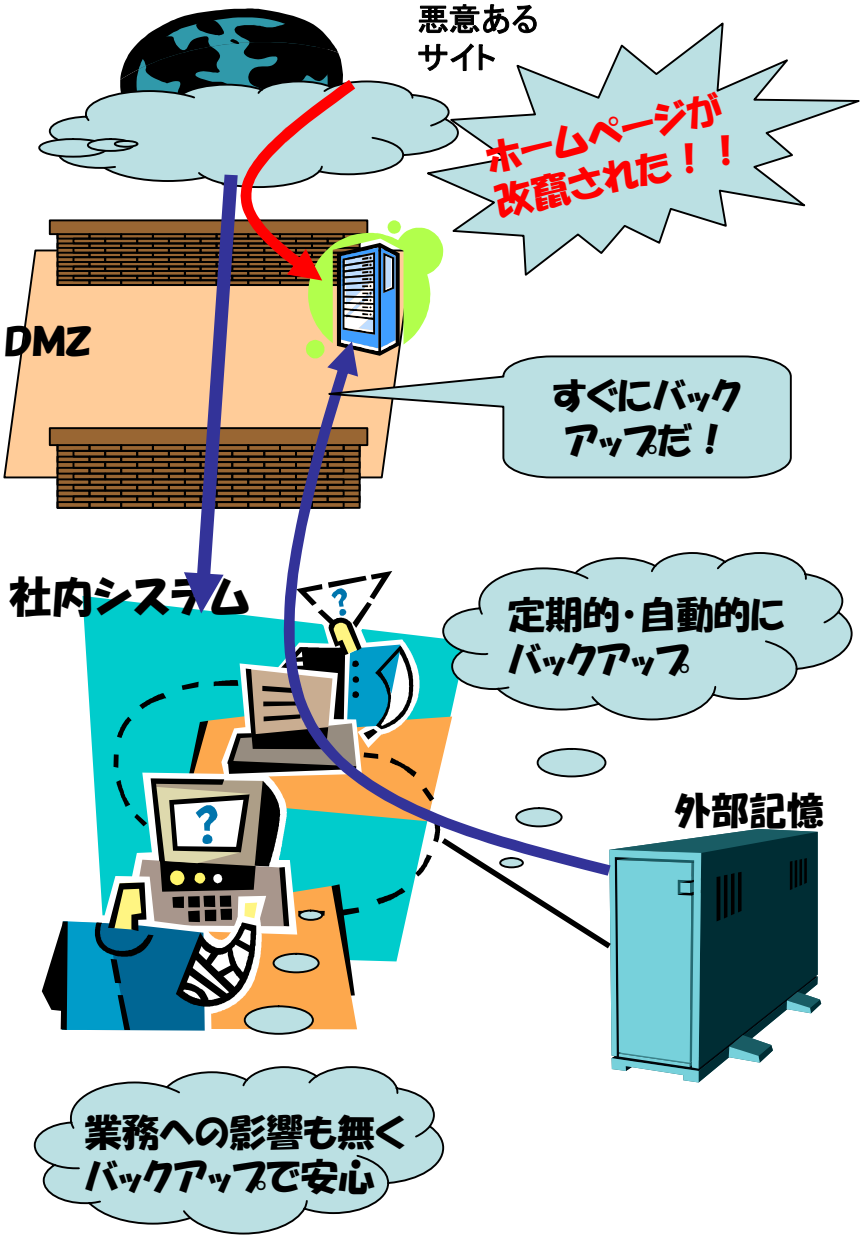
7. 外部からの侵入によりデータ等が改ざん・破壊されるリスクとその対策

外部からの侵入によりデータが壊されたり、改竄される危険に対しては、データ等の**バックアップが有効**です。
過去にはホームページを改竄され、暫く閉鎖せざるを得なくなった例もありました。バックアップがあれば、改竄されたホームページを即座に置き換えることも可能になります。
ホームページならば、会社の業務への影響はそれほど大きくありませんが、重要な経理データが改竄されたら大変なことになります。
これらのリスクに対応する為には、**定期的なバックアップ**が重要です。

【対策】
外部記憶装置への定期的なデータ等のコピーを実施します。コピーする情報は、影響度合いの大きいものから優先順位をつけて、どこまでの範囲をバックアップするかを決めておく必要があります。
社内システムでは、ネットワークを介して、外部記憶（DISK等のストレージ）に、定期的に、また自動的にバックアップをとることのできるツール類が用意されています。

【対応するメニュー】
データバックアップ対策

セキュリティ対策　ステップ1－7



II. ここからはじめよう、
セキュリティ対策の第一歩

8. 社員へのセキュリティ教育

社員の方々は会社の業務を行っている関係上、マル秘の情報に接する機会も多く、また直接それらの情報を取扱うことも多いはずです。しかしながら、あまりにも身近にそういう情報があると、その情報が大切である、という意識が薄れることがあります。仕事を家に持ち帰って続きをやろうと、外部メモリに情報を移して持ち帰る途中で落としたり、失くしたり、盗られたり、という状況は、いつ発生するかわかりません。また自宅のPCに情報を入れたら、ウィルスが、**ファイル交換ソフト（Winny等）**を使って、その情報をインターネットに公開してしまったという事件も後を断ちません。業務用のPCにゲームソフトをインストールして、就業時間中に遊んでいるというケースもあります。これらは全て**社員の意識**の問題であり、いくら色々な対策を施しても、社員の意識が変わらなければ情報漏洩の全てを防ぐことはできません。

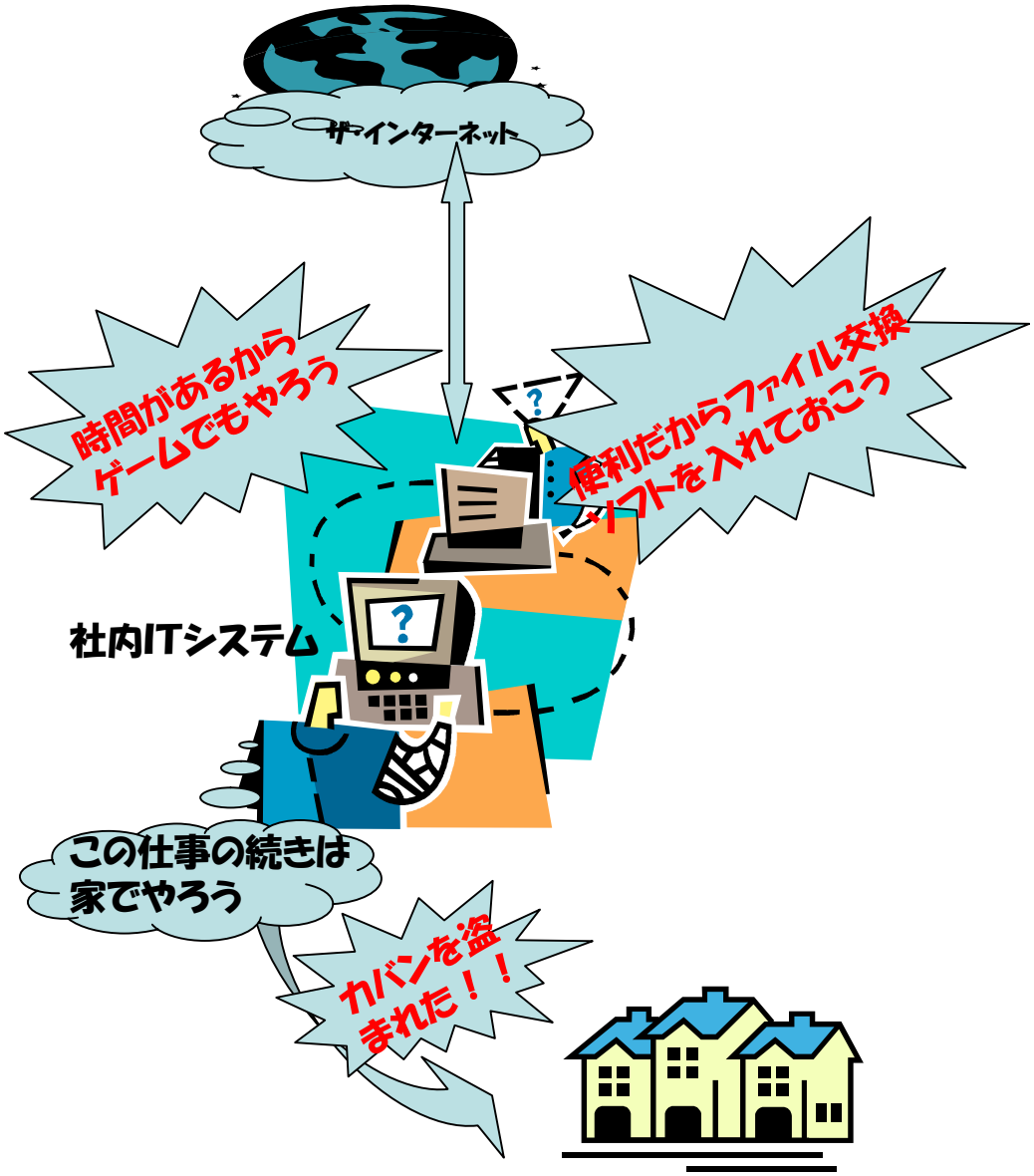
【対策】

社員の方々の会社への**帰属意識の醸成**はもちろんですが、情報の価値や、情報が漏れたときの会社・社会への影響を意識せずにリスクを犯してしまうケースは、避けなければなりません。そのための社員の方々への**意識教育**は重要ですし、ついうっかりを避ける為にも、定期的な注意喚起のための、教育も大切になってきます。

【対応メニュー】

情報セキュリティ教育サービス

セキュリティ対策　ステップ1－8



コラム（社員によるデータ流出リスク）

社員によるデータ流出のリスクとその対策

性善説に立てば、社員は会社のために働き、給料を貰って自分の生活を豊かにする、というのが本来の姿です。それでも、通常の業務を遂行している間に、ついうっかり、ミスをすることがあります。
特にセキュリティに関しては、自分が問題ないと思っていた事が、実は重大な情報の漏洩に繋がっていくということも多いのです。例えば、重要な情報をA社にFAXで送ろうとしたところ、間違ってライバルのB社に送ってしまったなどということが現実に起きています。A社に訴訟を起こされれば、多額の賠償金の支払いというリスクを背負うことになります。

【対策】
「意識せずに」、「ついうっかり」、を失くす為に、社員の方々への情報セキュリティ教育は欠かせません。さらに社内ルールによる確認手順の策定と遵守が必要です。これらを定期的に実施し、社員の意識を常に一定レベルに保っておくことも重要です。


情報
セキュリティ
とは？
社内ルール
やはり
情報セキュリティ教育は必要だ
A社に送るFAXを
B社に送ってしまった！
B社
A社

III

早めにやったほうがいい次の段階のセキュリティ対策

セキュリティ対策　ステップ 2

ここでは、すでにステップ１の対策を実施した、企業の方々に、セキュリティレベルを維持する為に、なるべく早く実施したほうがよい対策を説明しています。
セキュリティ対策を実施していても、外部状況は時々刻々変化しており、常に新しいウィルスが出てきます。これに対応していくことで、現在のセキュリティレベルが維持できることになります。

内部統制に関連する対策としては、アクセス履歴の保存や管理が該当しますので、直接的には7項のファイルアクセス管理が、間接的には外部からの不正アクセス、内部からのメールの管理・保存・監視が対応しています。（**次頁の青字の項目**）

ステップ2に対応する対策をまとめると、次のようなものになります。

0. 対策の前に
外部に対してホームページを公開する場合の
社内ネットワーク構成

1. 不正アクセスによるシステム停止のリスクと
その対策　　（スパムメール対策）
（不正アクセス運用・監視）
2. 不要・不正メールによる悪影響のリスクと
その対策　　（URLフィルタリング）
（メールフィルタリング）
3. データの盗難・紛失のリスクとその対策
（データ暗号化）
4. 障害によるシステム停止のリスクとその対策
（事前保守・監視サービス）
5. 外部からの不正侵入、データ持ち出しのリスク
情報の持ち出し・改ざんのリスクとその対策
（ICカード、各種認証）
6. 不要PCからの情報漏洩のリスクとその対策
（データクリーンサービス）
7. 社員のデータ不正取扱のリスクとその対策
（ファイルアクセス管理）
8. ドキュメントの不正取扱のリスクとその対策
（ドキュメントセキュリティ）

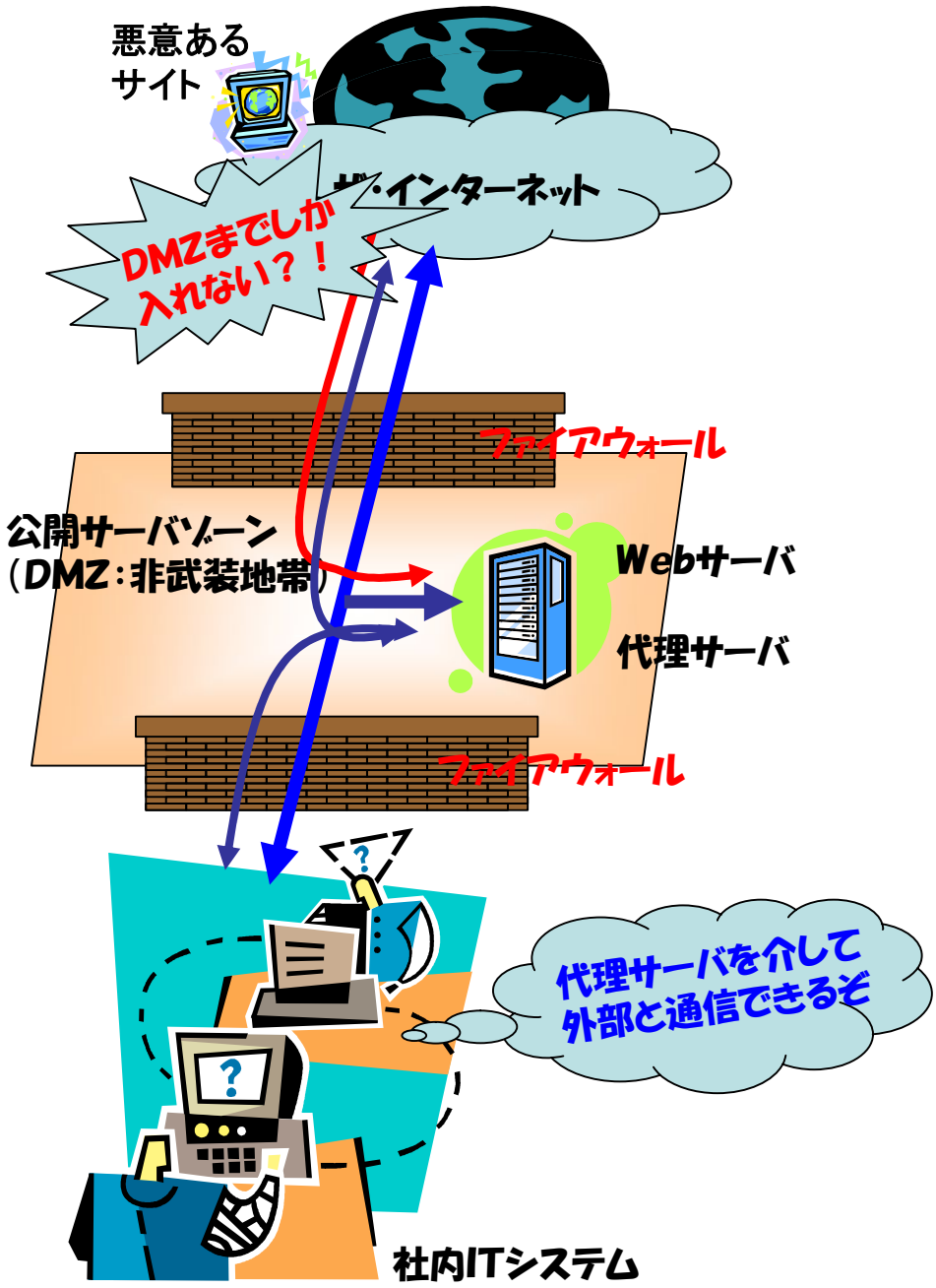
～コラム（VPN）～

III. 早めにやったほうがいい 次の段階のセキュリティ対策

0. 対策の前に 外部に対してホームページを公開する場合の、社内ネットワーク構成

外部に対して、ホームページ等で広く情報を公開する場合、社内システムへの外部からの侵入を阻止する為に、通常、**公開サーバゾーン**（**DMZ**：de-militarized zone：**非武装地帯**）を設けます。
そしてファイアウォールをDMZの前にも設け、外部からのアクセスはDMZまで、内部からのアクセスはDMZのサーバを介して外部と通信するような構造を作ります。
中規模・小規模のシステムでは、一台でDMZを構成できるファイアウォールが主流になっていますが、ここではわかり易くするために二つのファイアウォールで表現しています。

セキュリティ対策　ステップ2－0



Ⅲ．早めにやったほうがいい
次の段階のセキュリティ対策

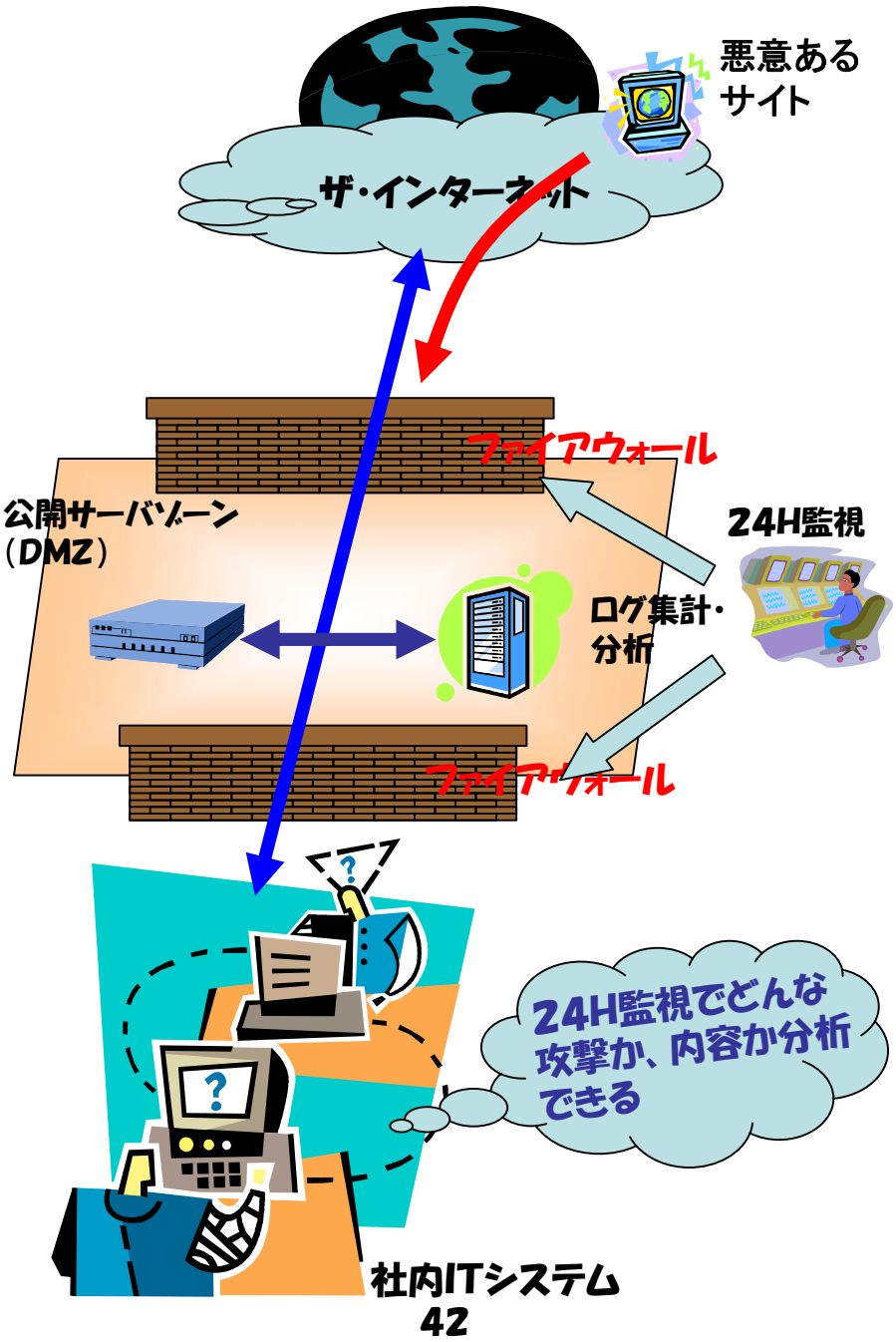
1．不正アクセスによるシステム停止のリスクとその対策

ファイアウォールはインターネットと社内システムとの間に設置され、外部からの不正アクセスから、社内システムを守っています。しかし集中的な負荷を与えるような攻撃や正常な通信を装うアクセスに対しては自身では検出が出来ない為、**外部からの監視が重要**になります。集中的な攻撃は、社内から外部に対する通信を妨害するため、極端に応答が遅れますが、通常はこれが外部からの攻撃によるものか、内部システムの問題なのかがわかりません。そのため解決に時間がかかったり、取引先との商談に影響が出たりすることがあり、業務遂行へのリスクは小さくありません。

【対策】
これらの問題を少しでも早く解決するために、また、**原因分析の為のアクセスログ**をとっておくために、不正アクセス運用・監視のサービスがあります。また、メールやWebサーバのログを合わせてとっておくことも必要です。

【対応メニュー】
スパムメール対策
不正アクセス運用・監視

セキュリティ対策　ステップ2－1



Ⅲ．早めにやったほうがいい
次の段階のセキュリティ対策

2. 不要・不正メールによる悪影響のリスクとその対策

インターネットを通じての情報収集や、得意先との取引、決済等、Webを利用した情報のやり取りは、今や必須の道具となっています。しかしながら全世界のWebサイトには有害なサイトや個人情報を不正に取得するフィッシングサイトが蔓延しており、**不用意にこれらのサイトにアクセスすることは、会社の信用失墜に繋がる恐れがある**と認識しなければなりません。
また、業務時間中にオークション、ショッピングへの参加や出会い系サイトとのやり取りをするケースも想定されます。業務効率の悪化や、会社の信用失墜につながるリスクは極力減らしていく必要があります。
昨今では、個人情報が外部に漏れるのを抑える為、社内から社外へのメールをチェックし、マル秘情報などが流出するリスクを避けるツールも出てきています。

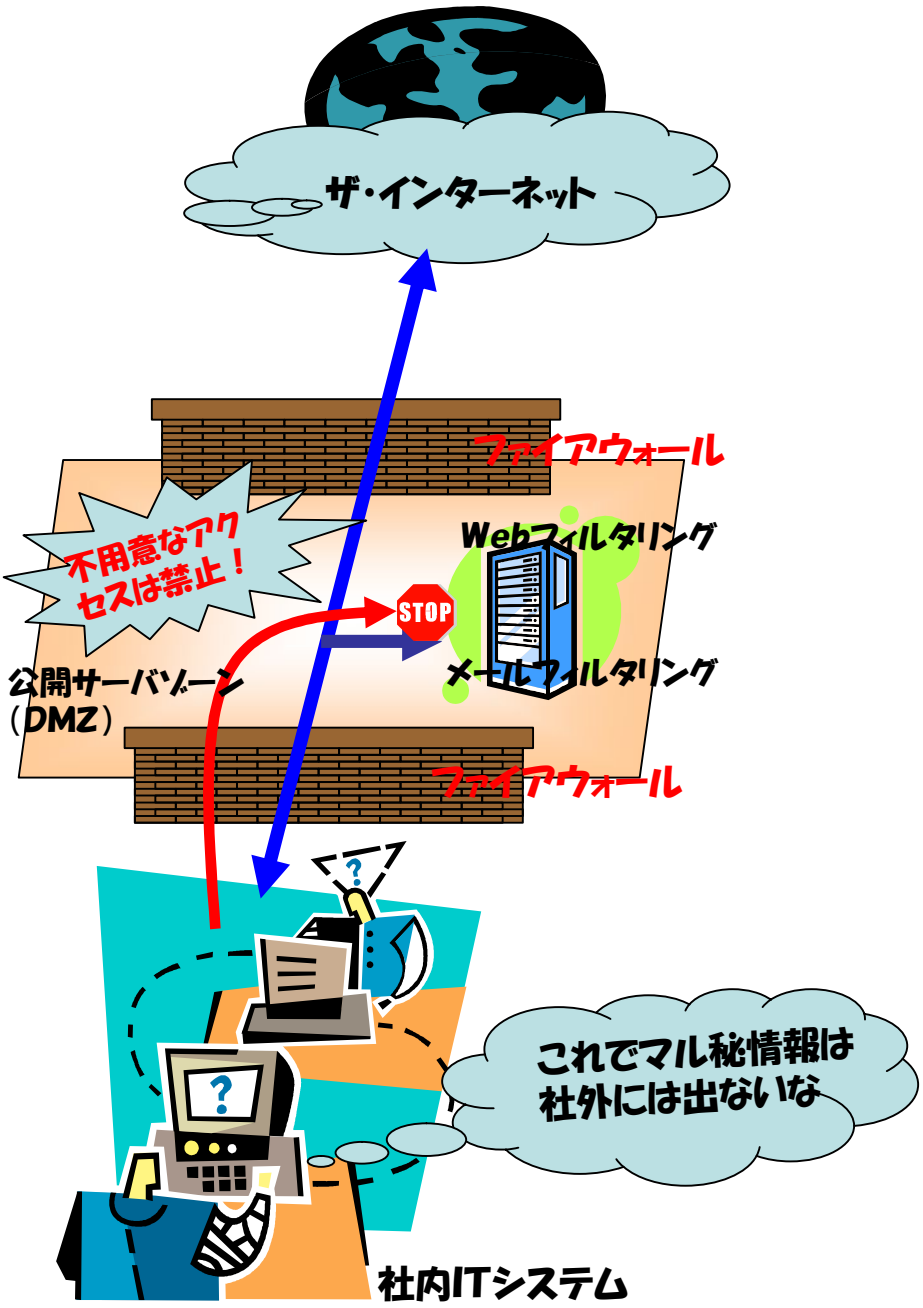
【対策】

これらのリスクを避ける為に、**Webフィルタリング**あるいは**URLフィルタリング**というツールが用意されています。またフィルタリングした結果の履歴も集計・分析できれば、実態が把握できますし、社員に対する牽制機能としても有効になります。また、社内から社外への情報流出を防止する為に、**メールフィルタリング**というツールも準備されています。これは本文や添付文書にマル秘などのキーワードがあった場合、そのメールを保管するか破棄するかを選択できる機能も持っています。

【対応するメニュー】

URLフィルタリング、メールフィルタリング、Webフィルタリング

セキュリティ対策　ステップ2－2



Ⅲ. 早めにやったほうがいい
次の段階のセキュリティ対策

3. データの盗難・紛失のリスクとその対策

情報漏洩の原因の69%は盗難・紛失よるものです。
ひとたび盗難に会うと、社内情報の流出によって、**自企業のみならずお客様にも大きなリスクを負わせる**ことになります。自分では無くさないつもりで持っていた情報でも、「ついうっかり」というのは誰にでもあることです。そしてこのうっかりが、大きな社会問題になることがあるのはこれまでの新聞報道でも明らかです。社会的な信用失墜は、企業にとって大きな損失となります。

【対策】
それでは、盗難・紛失が避けられないとしたらどうすれば良いでしょうか。
持ち歩く情報は全て暗号化することです。PCは通常立上げ時に、パスワードを入力しますがこれだけでは不十分です。よりセキュリティを強固にする為に、PCのハードディスクを暗号化したり、外部メモリに出力するときも暗号化やパスワードの設定で、万が一盗難にあっても情報が使えないようなガードをすることが可能です。
また、社内システム（データ共有サーバ）に暗号化ソフトを導入することで、データをPCに保存するときは強制的に暗号化したりすることも可能です。

【対応するメニュー】
データ暗号化対策

セキュリティ対策　ステップ2－3

III. 早めにやったほうがいい次の段階のセキュリティ対策

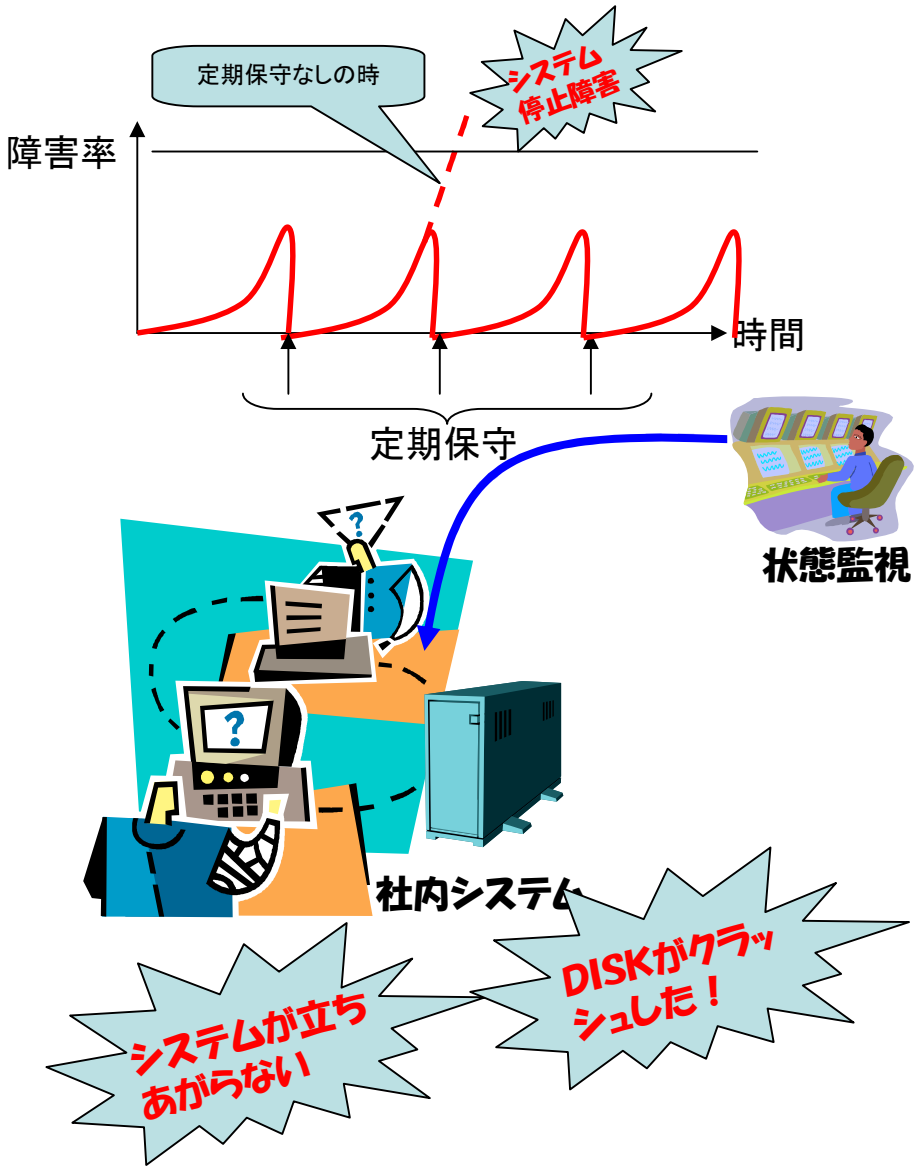
4. 障害によるシステム停止のリスクとその対策

社内システムそのものは、外部からの侵入がなくても、故障することがあります。この故障はもちろん突然のものもありますが、病気と同じように事前に何らかの兆候が現れることが多く、**日頃からこれを監視**しておくことによって致命的な長時間のシステム停止の可能性を少しでも低減することが出来ます。例えばディスクが故障する前には、読み取りエラーが多くなってくるなどです。常時監視をしていなくても、定期的な保守を実施することで、冒頭の事故のような事態に至る前に、未然にシステム停止を防止できます。

【対策】
事前保守を定期的に行うことで、致命的障害に至るまえにその芽を摘み取ることが出来ます。また監視を行うことで障害の兆候を事前に察知し、必要な対策をとることが出来ます。
また、障害の発生したDISKのデータ復旧も障害内容によっては可能となることもあります。

【対応するメニュー】
事前保守・監視サービス

セキュリティ対策　ステップ2－4



Ⅲ. 早めにやったほうがいい次の段階のセキュリティ対策

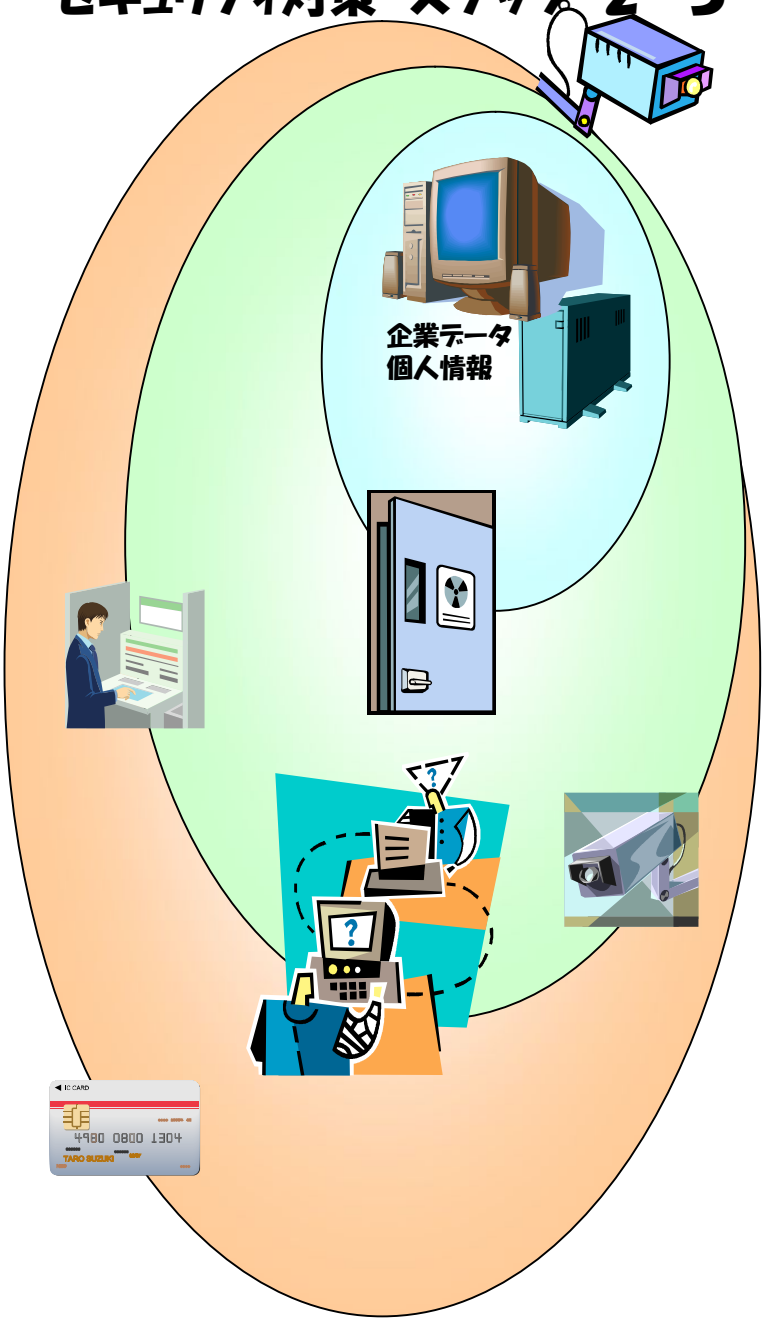
5. 外部からの不正侵入・データ持ち出しのリスク、情報の持ち出し・改竄のリスクとその対策

企業情報を格納してあるPCやディスクは、盗難に遭うとその会社の大きな損失になるのは間違いありません。機器そのものの損害よりも、**内部データの流出による損害のほうが大きい**のです。
外部からの侵入による盗難・個人情報・企業情報の流出を防止する為に、また時には、内部からの情報流出を防止する為に、**入退室の管理**は重要です。

【対策】
鍵の施錠、監視カメラの設置、警備会社の導入等、防犯の対策は既に実施されている企業が多いでしょう。全くの部外者の侵入はこれらの対策で防ぐことができるでしょうが、内部の犯行も考慮に入れる必要があります。その場合は人の入退室の管理を実施する必要があります。これは内部の人の犯行を抑えるだけでなく、**内部統制等、対外的な信用を確保する為にも必要**なのです。対策としてはICカード、指紋認証、静脈認証等による入退室の管理と記録、データの持ち出しの記録などがありますので、必要性と予算の状況によって選択するのがよいでしょう。

【対応するメニュー】
ICカード、入退出管理
（各種認証）

セキュリティ対策　ステップ 2－5



Ⅲ. 早めにやったほうがいい
次の段階のセキュリティ対策

6. 不要PCからの情報漏洩のリスクとその対策

業務用のPCが古くなった。買い換えなければいけないが
古いPCにあるデータを処分しなければなりません。
ファイルやフォルダを全て消去しても**実体のデータは、**
まだDISKに残っているのです。これを完全に消去しないと
残っているデータを悪用される危険性もあります。
個人情報保護法が施行されている現在では、情報は
最後までしっかり管理しないといけない時代になってきて
います。

【対策】
DISKやCDに書かれた情報は、通常の消去用ソフトウェア
では**完全に消去できません**。DISKなど磁気的に記録され
ている情報は、磁気的な方法で消去する必要があります。
また、CDやDVDなどに記録されたものは完全な上書きで
情報を消去する必要がありますが、時間が掛かる為、
物理的な方法で破壊するケースもあります。これらには
一部を除いて、特殊な装置が必要ですので、信用できる
販売店や保守会社にご相談下さい。

【対応するメニュー】
データクリーンサービス

セキュリティ対策　ステップ2－6

III. 早めにやったほうがいい次の段階のセキュリティ対策

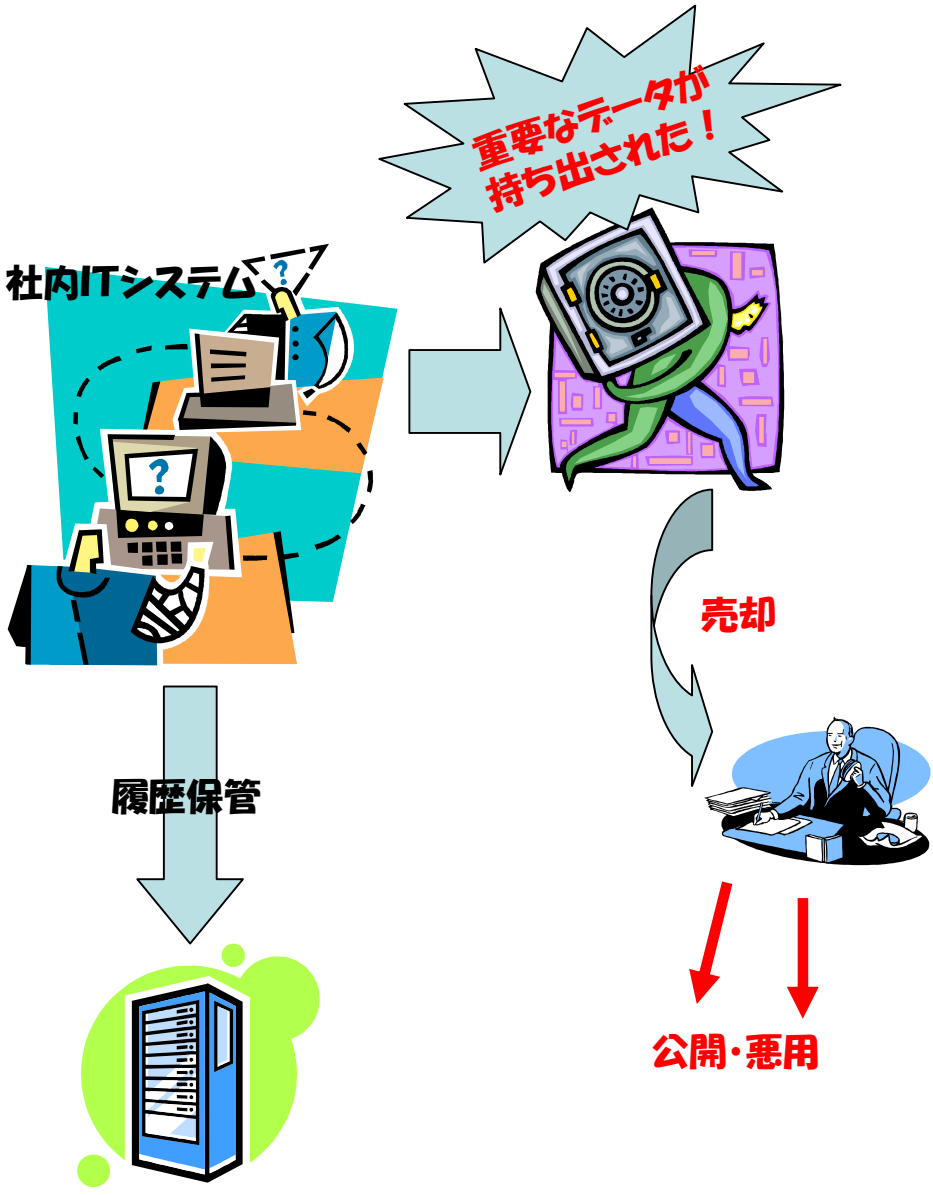
7. 社員のデータの不正取扱のリスクとその対策

一部の社員の方が、故意に情報を外部に持ち出す場合、これは避けることができません。社員のモラルの問題として、社員教育で発生を抑える方法はありますが１００%情報の漏洩を抑えることは出来ません。重要な情報が漏れた場合の損失は、社会的信用の失墜、会社のアドバンテージの崩壊、お客様への多大な賠償等、計り知れません。

【対策】
一つの方法として、**社員に対して牽制機能**を働かせ、情報の持ち出しを抑える方法があります。例えばメールのやり取りを保管しておき、何かあったときには保管データを解析することで犯人を特定する、またファイルへのアクセス履歴を保管しておいて、誰がいつどのファイルにアクセスしたかをわかるようにしておく等です。そして履歴をとっていることを、社員にオープンにしておくことで、犯行に及ぶことを牽制することが出来ます。

【対応するメニュー】
ファイルアクセス管理ツール

セキュリティ対策　ステップ2－7



Ⅲ. 早めにやったほうがいい 次の段階のセキュリティ対策

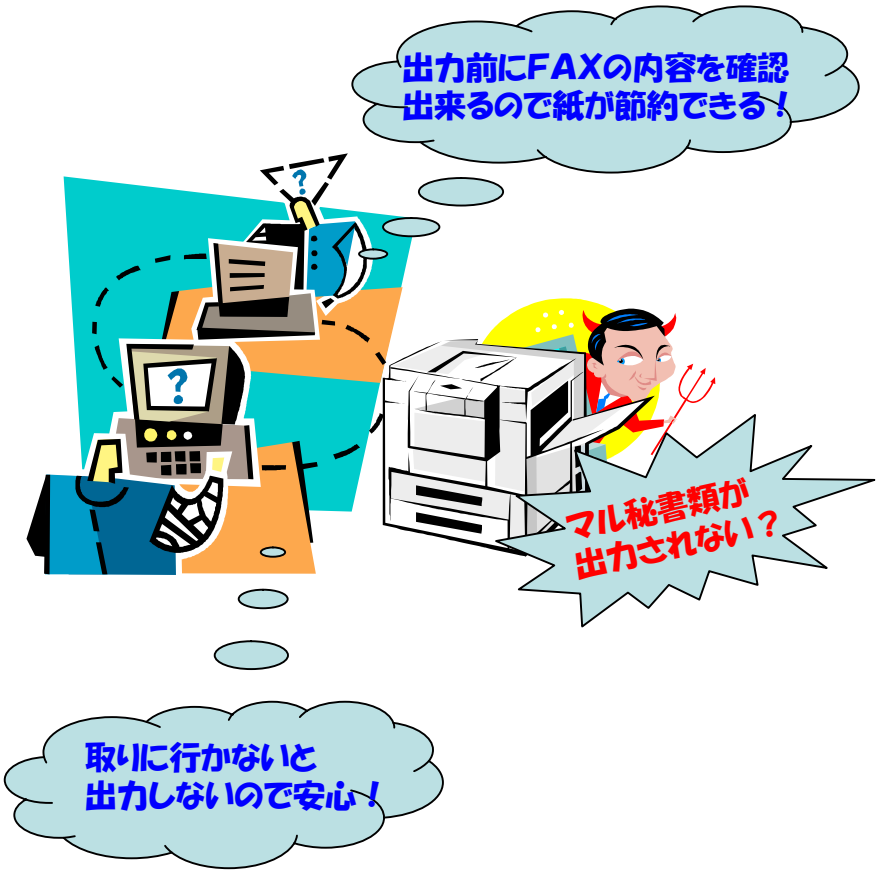
8. ドキュメントの不正取扱のリスクとその対策

統計からも、**紙媒体からの情報漏洩は実に全体の半分**近くを占めています。外部の人が入ってくるフロアで、プリントアウトした直後、電話が掛かってきてしまい、後で取りに行ったら、出力した用紙がなくなっていた、という経験のある方は多いのではないでしょうか。また、秘密書類を鍵のかかる引き出しに入れずに、机上に置いたままにし、翌朝出てきたら、なくなっていたというケースもあります。紙媒体の管理は、益々重要性を増してきています。

【対策】
最近ではプリンタそのものに様々な機能が付加されてきています。これをネットワークプリンタとして接続することで出力管理も容易になってきています。ICカードや生体認証と組み合わせて、**プリンタで個人認証をしないと出力しない**機能や、間違って出力指示を出してしまったドキュメントをプリンタで出力のキャンセルをしたり、FAX機能付のプリンタでは、不要なファックスは出力せずに廃棄し、用紙のムダ使いを避けるという運用も出来ます。

【対応するメニュー】
ドキュメントセキュリティ

セキュリティ対策　ステップ2－8

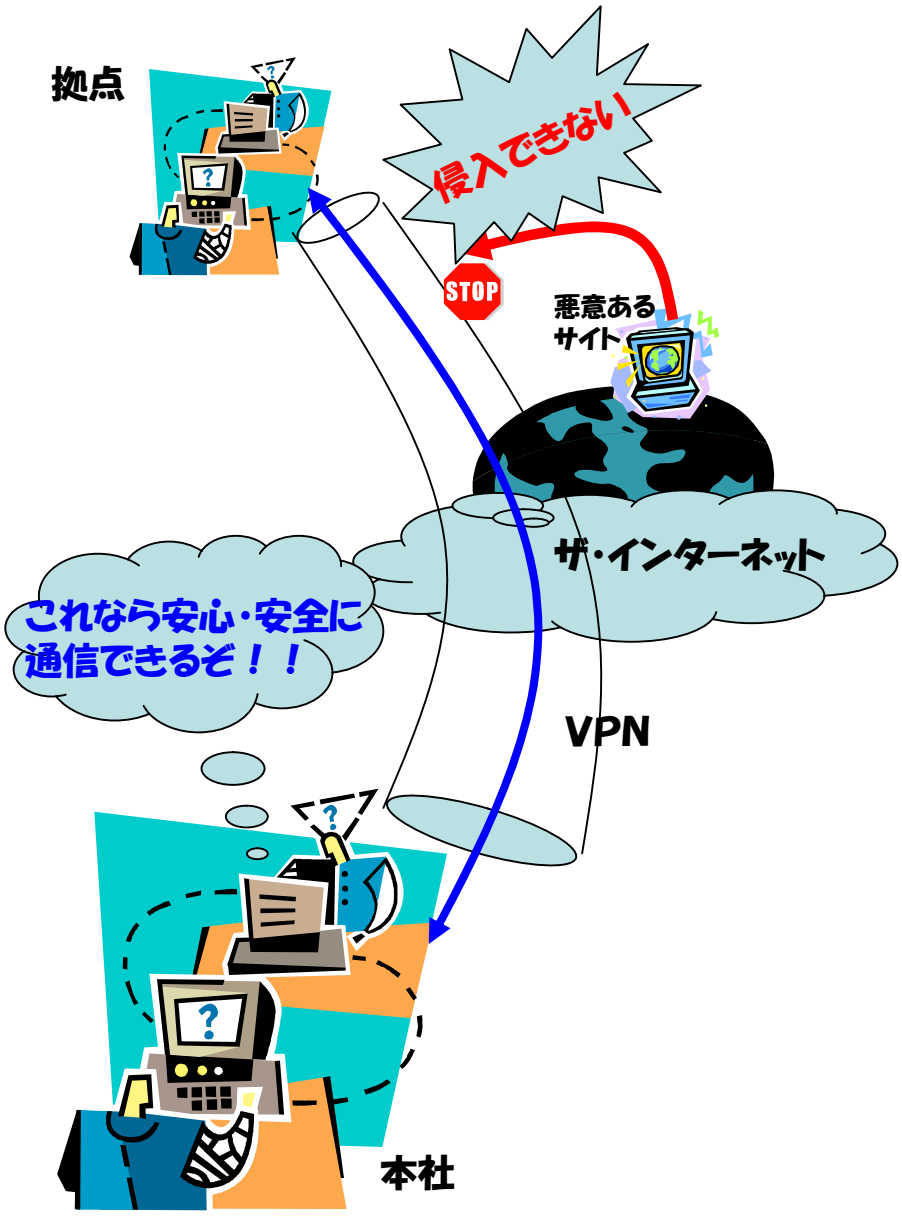


コラム(VPN)

通信中の情報漏洩・改竄のリスクとその対策

本社の他に拠点がある場合、その拠点との情報のやり取りが必要になります。このやり取りには当然、会社の秘密事項や社員の個人情報などが含まれていることが多いでしょう。インターネットはオープンな通信網ですから、世界中どこからでもこの通信を盗聴することが可能と考えておかなければなりません。悪意ある人がこの盗聴データを悪用する危険があります。

【対策】
この通信を安全に相手に届ける手段の一つとして、インターネットの通信網の中に、専用線のような論理的なチャネルを設け、これを通して通信を行うものがあります。これをVPN（バーチャルプライベートネットワークの略）といいます。
このVPNを使うことにより、拠点との通信を、安心・安全に行うことが出来ます。またこの通信をさらに盗聴し難くするための手段として　SSL－VPNという通信手段をとることもできます。


拠点
侵入できない！
STOP
悪意ある
サイト
ザ・インターネット
これなら安心・安全に
通信できるぞ！！
VPN
本社

IV

状況により実施しておく必要のあるセキュリティ対策

セキュリティ対策　ステップ 3

ここでは、システムのおかれた環境、システム構成、重要度等、それぞれの状況により、実施しておく必要のあるセキュリティ対策について述べています。

内部統制に関連する項目としては、2項の不正プログラム対策、6項のPC操作制限、9項のログ・収集解析の項目が該当します。

ステップ3に対応する対策をまとめると、次のようなものになります

1. 不正アクセスによる、業務停止や、悪意のあるコード(トロイの木馬等)を埋め込まれるリスクと、その対策　　(IDS・IPS)
2. 従業員による不正プログラム導入のリスクとその対策　　(不正プログラム対策)
3. ウィルスの配布・拡大のリスクとその対策　　(検疫システム構築)
4. 無線LANデータ漏えいのリスクとその対策　　(無線LAN暗号化)(無線LANシミュレーション)
5. 一般的な認証のリスクとその強化策　　(ユーザ認証強化対策)
6. 外部媒体へのコピーから企業情報が漏れるリスクとその対策　　(PC操作制限)
7. セキュリティ対策不足によるデータ流出のリスクとその対策　(情報・セキュリティ評価・診断)
8. 電源・空調機障害によるシステム不安定のリスクとその対策　　(付帯設備監視)
9. 社員のデータの不正取扱のリスクとその対策　　(ログ収集・解析)
10. 情報漏洩被害による金銭保障のリスクとその対策　　(個人情報取扱事業者保険)
11. 自然災害によるデータ破壊のリスクとその対策　　(データバックアップ対策)　　(転倒防止対策)

Ⅳ. 状況により実施しておく必要のあるセキュリティ対策

1. 不正アクセスによる、業務停止や、悪意のあるコード（トロイの木馬等）を埋め込まれるリスクと、その対策

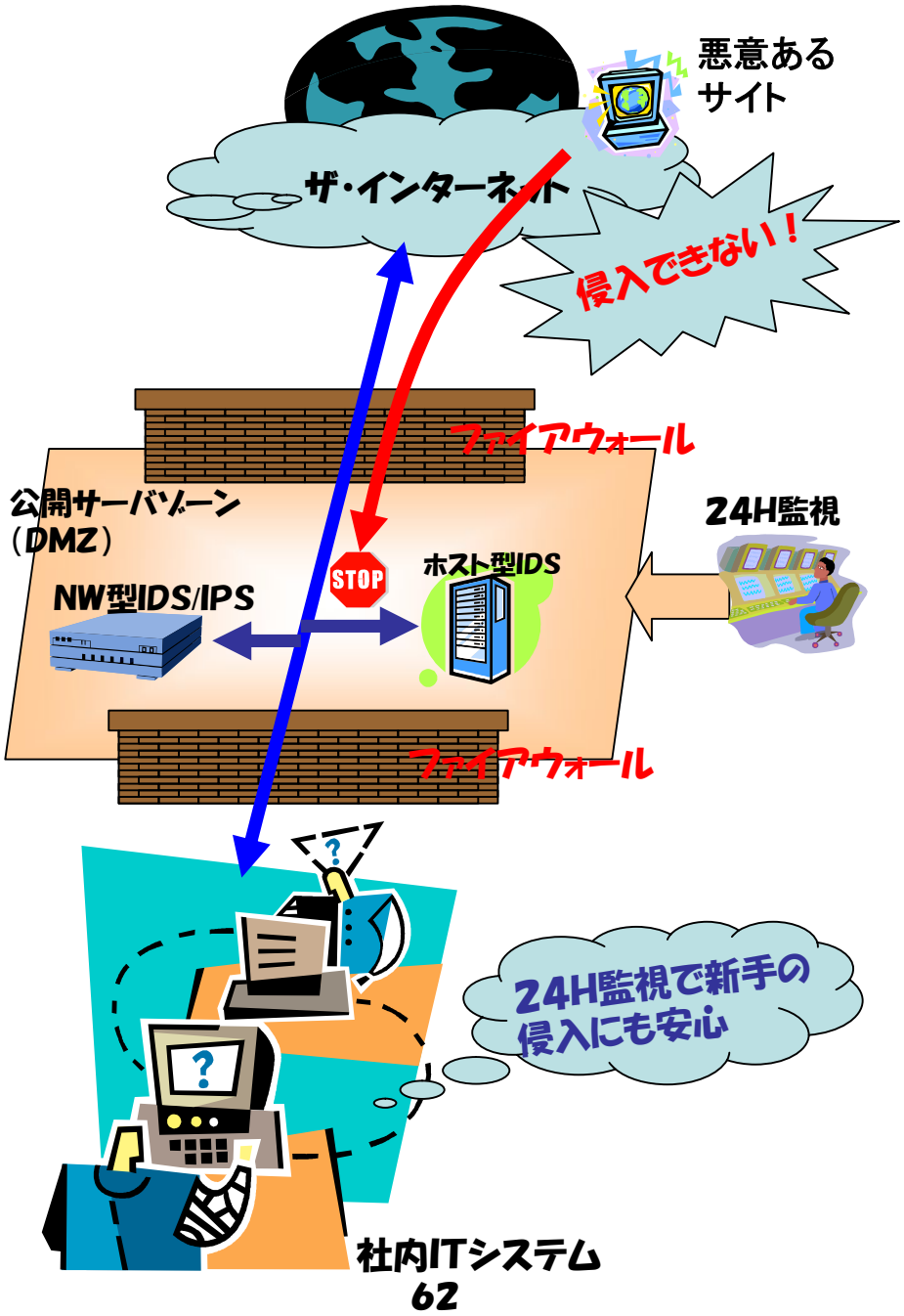
通常のビルで入退室管理を行っても、インターネットからの侵入を防ぐ事はできません。また、ファイアウォールを使用しても、Webサーバやメールサーバなど、業務で使用する通信を使用した不正アクセスには対応出来ません。
この結果、外部から悪意のあるコードが埋め込まれ、攻撃者の不正侵入を許し、ホームページの改ざんや、メールサーバダウンにより業務が続けられない状況になる可能性があります。**インターネットからの侵入を検知**し、対応するためには、そのためのツールが必要になります。

【対策】

これのような攻撃に対応するには、不正侵入を検知することの出来るツールが必要です。このツールは**不正侵入検知システム**（**IDS**：Intrusion Detection System）と呼ばれます。
IDSにはネットワークを流れる通信を監視するネットワーク型（NW型）と、サーバ上で通信を監視するホスト型があります。また、侵入を検知するだけでなく、検知と同時に侵入と思われる通信を自動的に遮断する**不正侵入防止システム**（**IPS**：Intrusion Pre-vention System）といわれるツールも出てきています。これらは、これまでにない攻撃のパターンもある程度検知し、侵入を防御することが出来ます。IDSは侵入を検知したことを、管理者に通知し、対応を求めることが出来ます。このように、常に侵入を監視し即応する為には、24時間の監視体制が有効です。

【対応するメニュー】 IDS・IPS構築

セキュリティ対策　ステップ3－1



Ⅳ. 状況により実施しておく必要のあるセキュリティ対策

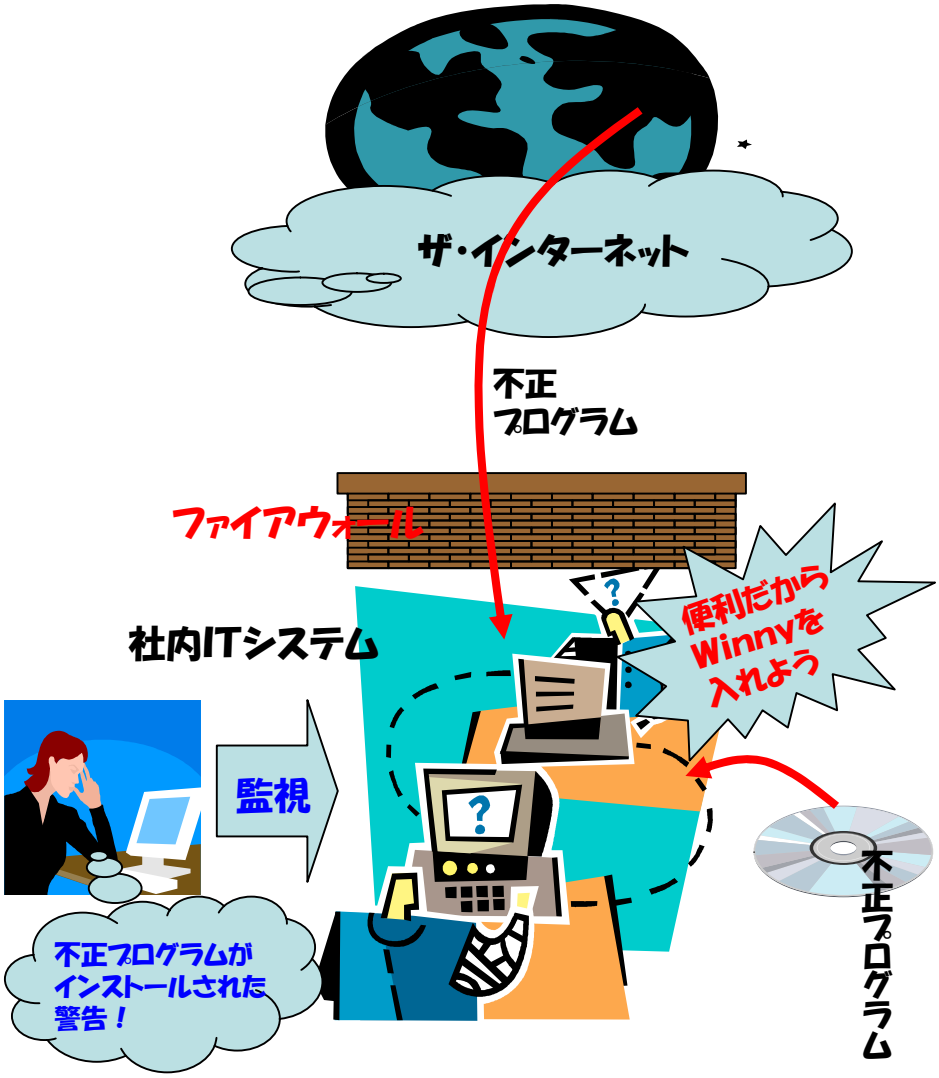
2. 従業員による不正プログラム導入のリスクとその対策

世の中には無料のソフトウェアが沢山、出回っています。有用なものもありますが、中には使えそうもないソフトウェアや使い方によってはセキュリティ的に問題となるソフトウェアもあります。例えば、ファイル交換ソフトは有用なソフトウェアですが、ひとたびウィルスと組み合わさると、情報漏洩によって、多大な被害を企業に与えます。Winnyもそのひとつです。このようなファイル交換ソフトで企業の情報が漏洩すると、これを回収することは不可能といわれています。つまり、いつまでも**漏洩情報が公開され続ける**ことになります。
社内のITシステムとしては、このようなソフトウェアが、持ち込まれることを回避しなければなりません。

【対策】
新しいソフトが持ち込まれたか否かを、常に監視することの出来るツールが準備されています。インターネットを通じて、又は個人が持ち込んだソフトが、社内ITシステムに持ち込まれると、管理者に通知したり、警告を発したりすることが出来ます。

【対応するメニュー】
クライアントPC対策

セキュリティ対策　ステップ　3－2



Ⅳ. 状況により実施しておく必要のあるセキュリティ対策

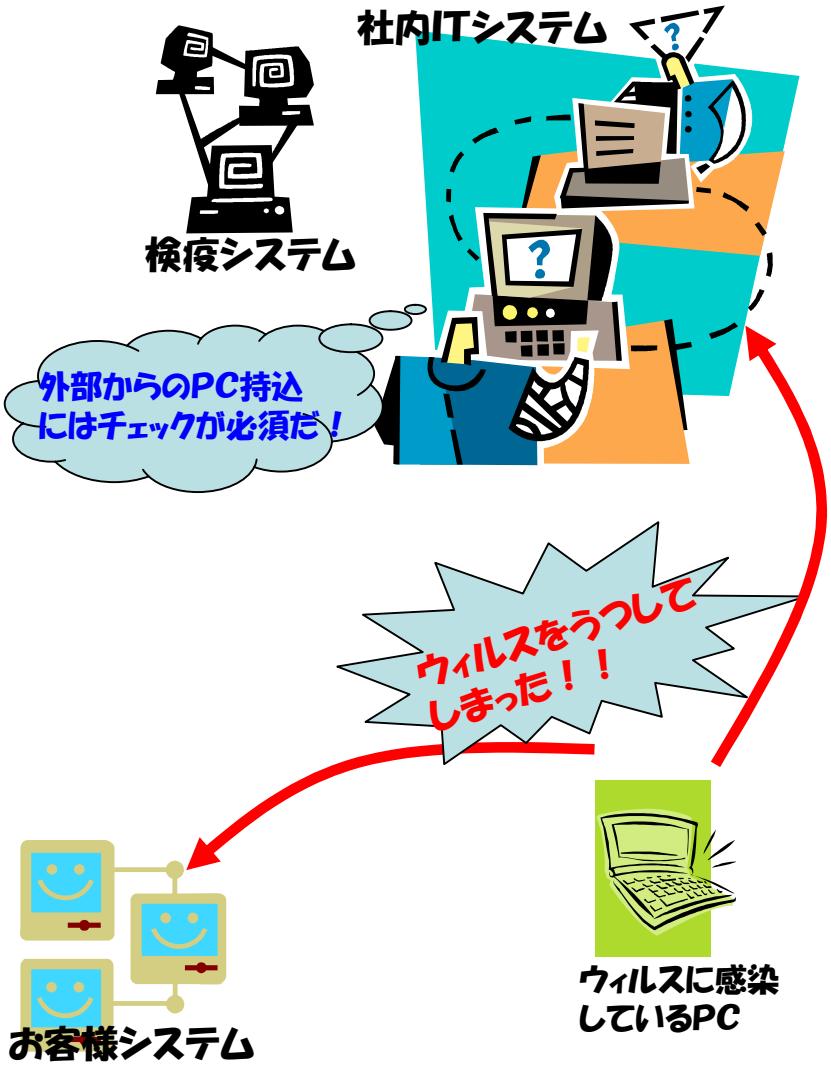
3. ウィルスの配布・拡大のリスクとその対策

社内で十分なウィルス対策を行っていても、ウィルス対策は十分とはいえません。
例えば、ウィルスに感染した個人のPCを社内システムに持ち込んで接続した為に、社内システムにウィルスが蔓延してしまったり、ウィルスに感染したPCを知らずにお客様に持ち込んで、お客様のシステムにウィルスを感染させてしまったケース等、ウィルスに対しては常に感染しないように気を配っていなければなりません。
ウィルスに感染しているか否かを常にチェックしておくことによって、お客様に迷惑をかけるリスクを削減することが出来ます。

【対策】
接続するPCがウィルスに感染していないかどうかをチェックする為には、**検疫システム**が有効です。検疫システムは接続されたPCがウィルスに感染していないか、ウィルス検知用データファイル（パターンファイル）が最新になっているかどうか、PCは接続の許可されたPCか、等についてチェックを行い、必要な条件が整っているPCのみ接続を許可します。こうしたチェックを行うことにより、お客様へ迷惑をかける心配なしに、お客様のシステムへの接続を行うことが出来ますし、社内システムにウィルスを撒き散らことなく安心して業務を行うことが出来ます。

【対応するメニュー】
検疫システム構築

セキュリティ対策　ステップ3－3



Ⅳ. 状況により実施しておく必要のあるセキュリティ対策

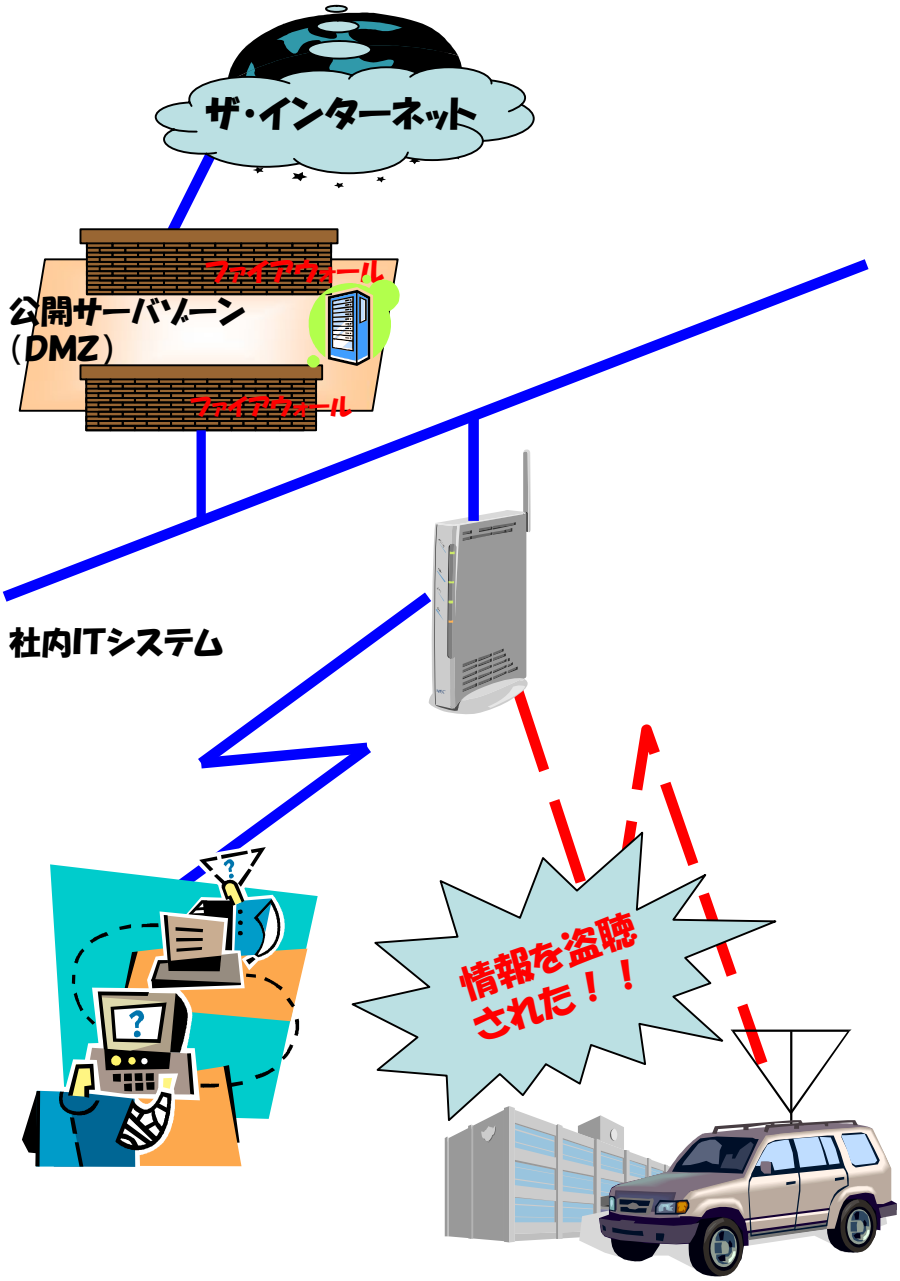
4. 無線LANデータ漏洩のリスクとその対策

最近、レイアウト変更に対してケーブル工事費の不要な無線LANの導入が増加しています。通信速度も速くなってきており、業務にも問題なく使えるようになりました。しかし無線LANでは、通信方法が電波となる為、**TV放送のように誰でも送受信できてしまう**という点に注意が必要です。条件によりますが、見通しの良い場所では数百メートルまで到達する可能性があります。（建物の近くで車に乗せたPCで通信内容を盗聴された例もあります）
また、広い事務室でついたて等の障害物があるフロアでは、アクセスポイント（電波の送受信を集約して行う場所）の位置にも注意が必要です。

【対策】
無線LANを使用する場合、親機と子機の無線通信には必ず暗号化を行う必要があります。暗号化の設定をボタン一つで自働的に行う機種も出てきています。事務所内の無線LANの設置には、置き場所の設計も含め、専門家に依頼するのがよいでしょう。

【対応するメニュー】
無線LAN暗号化
無線LANシミュレーション

セキュリティ対策　ステップ　3－4



Ⅳ. 状況により実施しておく必要のあるセキュリティ対策

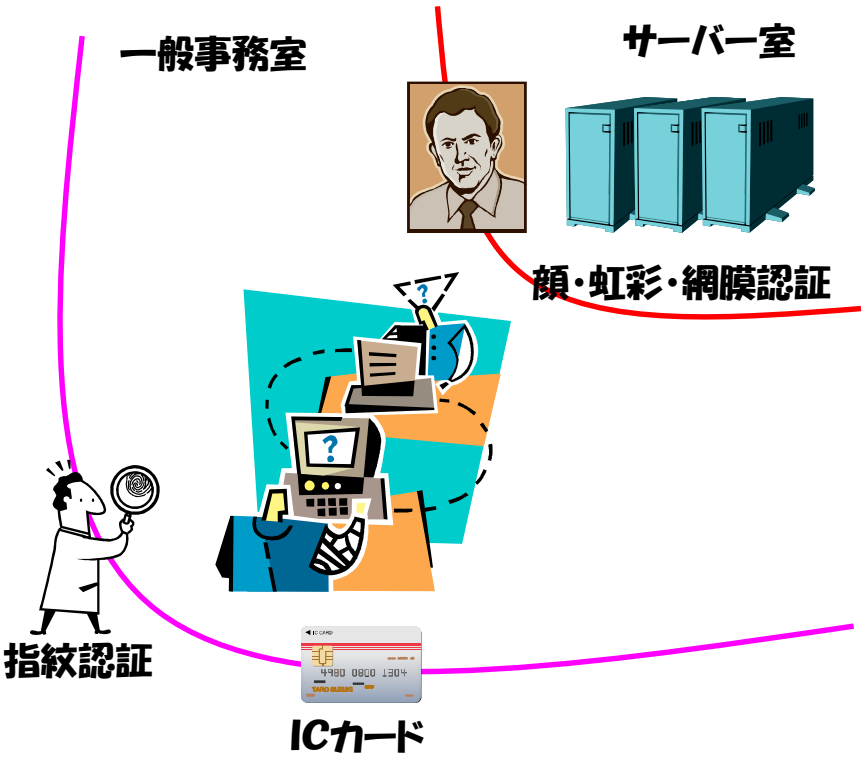
5. 一般的な認証のリスクとその強化策

通常、ユーザー認証には、ユーザIDとパスワードを使うのが一般的ですし、最も使われている認証方式です。
IDパスワードによる認証は、本人以外でも、知っていればその**本人になりすまして**、サーバやPCにログインすることができます。また、システムによっては、認証のための通信を暗号化せず（平文といいます）に行われる為、通信の盗聴により誰でもIDパスワードを入手できてしまいます。

【対策】
最近では、個人認証強化のために、**静脈認証、顔認証、虹彩認証、網膜認証、指紋認証、ICカード**による認証や、その組合せにより、更にセキュリティを高めた認証方式が使われています。
これらの認証方式は、PCへのアクセスだけでなく、その目的によって使い分けがなされています。例えばサーバー室など機密性の高い部屋への入室はICカードと顔認証や虹彩・網膜認証の組合わせで、セキュリティレベルの少し低い場所への入室や、PCへのアクセスは、ICカード、指紋、静脈認証のいずれかで行う等です
このような高度な認証方式を用いることで、第三者が本人になりすましてシステムにアクセスするのを防ぐことが可能になります。

【対応するメニュー】
ユーザー認証強化対策

セキュリティ対策　ステップ　3－5



ビルのロビーなど
オープンエリア

警備員

Ⅳ. 状況により実施しておく必要のあるセキュリティ対策

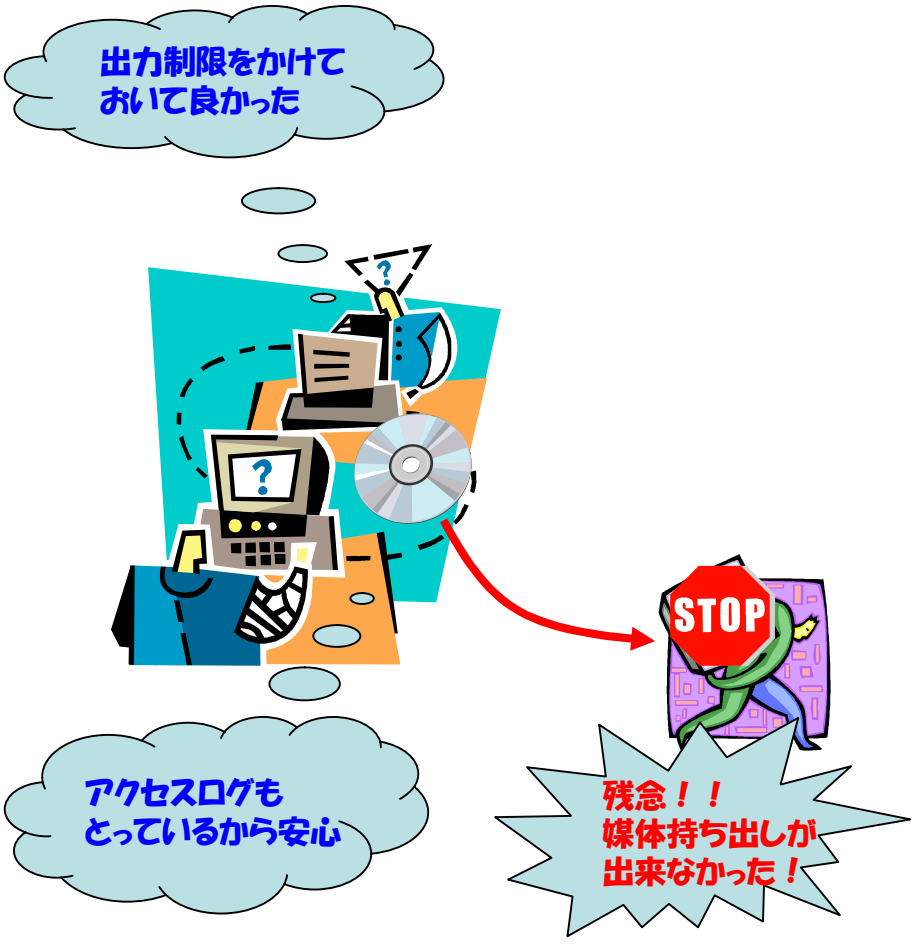
6. 外部媒体へのコピーから企業情報が漏れるリスクとその対策

会社の仕事が終わらない。通常は禁止されているのだが、仕事の続きを、うちにもって帰ろうと外部媒体に出力してカバンに入れたが、そのカバンを電車に置き忘れてしまったというようなケースがあります。最近は外部媒体も容量が大きくなり、多くの企業情報をコピーすることが出来ます。これは、とりもなおさずリスクがそれだけ大きくなっていることを意味しています。また、従業員以外の方がPCを使う可能性がある場合、本来閲覧してはいけないファイルを閲覧されたり、持ち出されたりしてしまう危険性があります。

【対策】
このようなリスクに対しては、PCの操作を制限することの出来るツールを使用することで、情報漏洩のリスクを低減することができます。このようなツールを使用することで、**ファイルへのアクセス制限や出力制限をかける**ことが可能です。この種類のツールは外部記憶（リムーバブル媒体）への出力制限の他に、アクセス履歴等も収集している為、これを周知しておくことで**不正な情報持ち出しに対する従業員への牽制機能**を働かせることも可能です。

【対応するメニュー】
PC不正操作対策

セキュリティ対策　ステップ　3－6



Ⅳ. 状況により実施しておく必要のあるセキュリティ対策

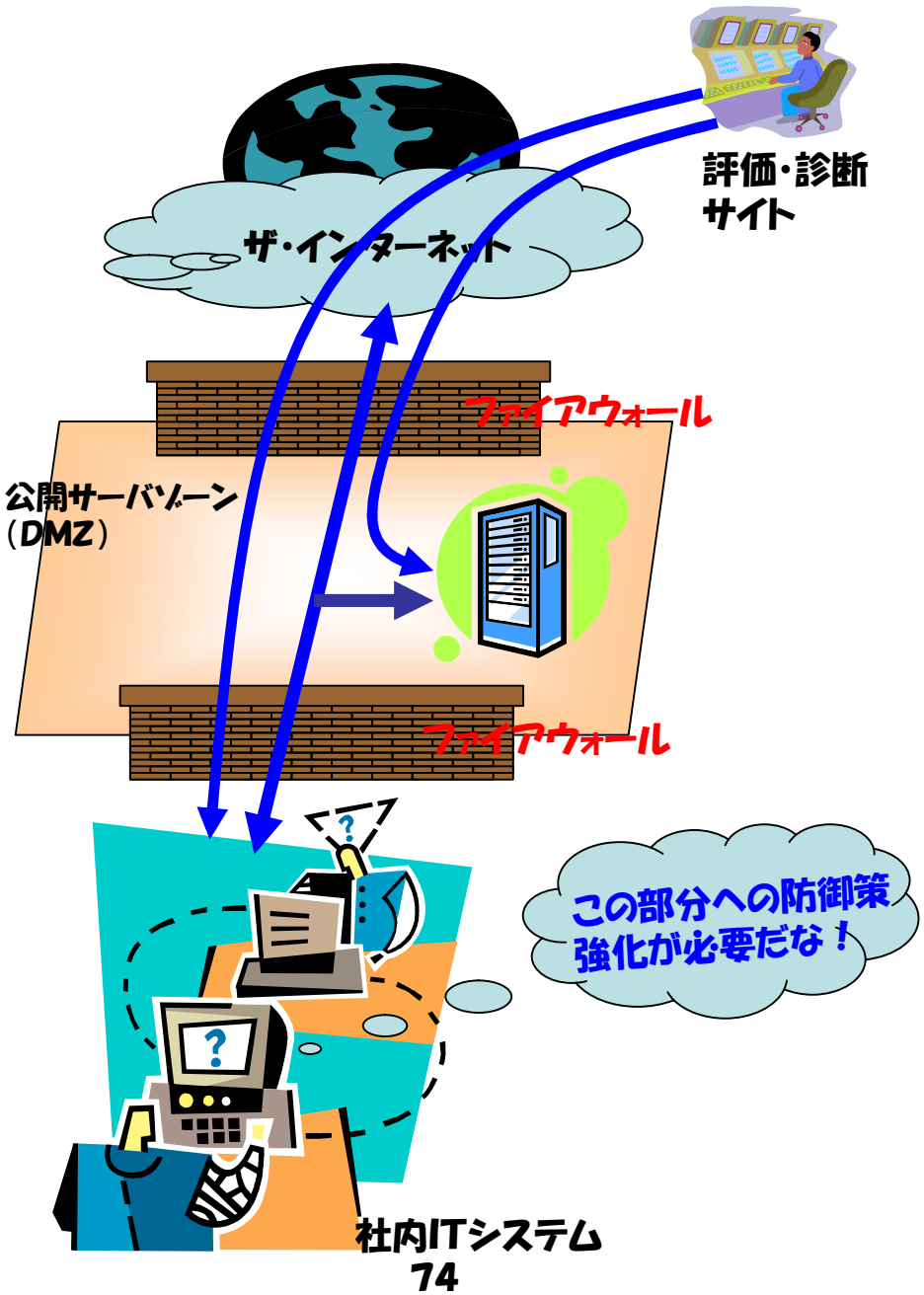
7. 対策不足によるデータ流出のリスクとその対策

現在、お客様が適用しているセキュリティ対策は情報漏洩の点から見て十分でしょうか。**ハッキングの手法は日々新しく**なり、ソフトウェアにも新しい脆弱性（セキュリティホール等）が見つかっています。ハッカーは常に新しい脆弱性を狙って攻撃をしてきます。この脆弱性をつかれてスパイウェアが社内システムに入り込み、情報を流出させるリスクがあります。

【対策】
現在の社内システムに対する対策が十分かどうか、外部から見つける方法があります。
インターネットを介して、目的の企業システムに対して擬似的なアタックを試み、**防護策の行き届いていない箇所を検出**、結果を分析し対策を含めて報告するというものです。
これにより、不足している防護策を検討・追加することが出来ます。

【対応するメニュー】
情報セキュリティ評価・診断サービス

セキュリティ対策　ステップ3－7



Ⅳ. 状況により実施しておく必要のあるセキュリティ対策

8. 電源・空調機障害によるシステム不安定のリスクとその対策

社内システムは、雷・停電等の影響を極力受けないようにする為、電源の安定供給を行う**安定化電源の設置**や、性能が向上し、集積度が上がってきているPC・サーバの発熱による、動作不安定を防ぐための**空調機を設置**することが多くなっています。しかし、安定化電源は、雷・停電等が頻繁に発生したり経年変化によりコンデンサが劣化したりすると、供給電源が不安定になることがあります。また、空調機についても、故障による環境温度や停止時の結露等に注意する必要があります。電源や空調機の動作が不安定になると、その影響でPC・サーバの動作も不安定になり、システムが停止することもあります。

【対策】
特に停電の多い地区や環境の厳しい地区では、電原や空調機へのストレスも大きくなるため、**システム停止やデータ破壊を避ける為**に、設備関連の状況を監視しておくことが、安全・安心です

【対応するメニュー】
付帯設備監視

セキュリティ対策　ステップ　3－8

Ⅳ. 状況により実施しておく必要のあるセキュリティ対策

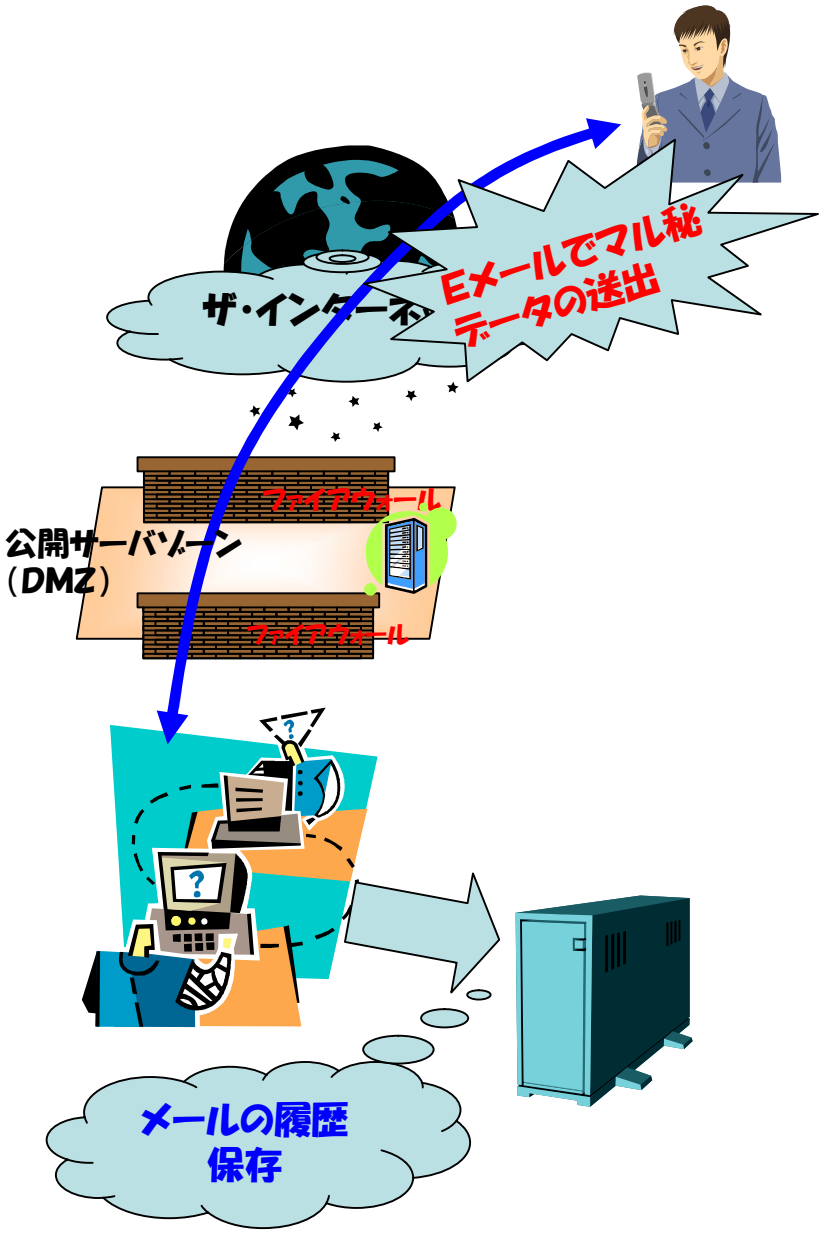
9. 社員のデータの不正取扱のリスクとその対策

情報漏洩の7割以上は内部犯行によるもの、というデータが発表されています。PCやデータの故意の持ち出しだけでなく、うっかりミスにより、**重要なメールを社外に送ってしまう**こともあります。この結果、秘密情報が社外で勝手に使われ、企業の信用問題や損害賠償等で多大な被害をもたらす危険性があります。

【対策】
このリスクを防止する為には、何かあったときの調査・分析に使用できるようにするために、社員がやり取りしたメールの**履歴を全て保存**しておく必要があります。さらに送信先のアドレスや添付ファイルの有無によって、**メールの送信を制御**することもできます。
また、この履歴をとっている事を、社員に周知することで、メール送信に対する**従業員への牽制機能**を働かせることが出来ます。
製品の種類によってはメールを改竄不可能なデータとして保存する機能を持っているため、**監査の証跡**として使用することが出来ます。

【対応するメニュー】
ログ収集・解析
（メール証跡保存対策）

セキュリティ対策　ステップ　3－9



Ⅳ. 状況により実施しておく必要のあるセキュリティ対策

10. 情報漏洩被害による金銭保障のリスクとその対策

万が一、情報漏洩が発生したとき、その情報が個人情報やお客様の情報で漏洩により大きな被害をかけてしまった場合、その賠償額は多大なものになる可能性があります。情報漏洩では、漏洩そのものによる**社会的信用の失墜**の他に、**賠償による企業への大きな負担**のリスクを抱えなければなりません。

【対策】
現在では、個人情報漏洩に特化した保険も用意されています。大手の保険会社では、この保険を取り扱っていますのでご相談下さい。

【対応するメニュー】
個人情報取扱事業者保険

セキュリティ対策　ステップ　3－10

Ⅳ. 状況により実施しておく必要のあるセキュリティ対策

11. 自然災害によるデータ破壊のリスクとその対策

日本は、地震や、台風による浸水等、自然災害の多い国です。
地震による装置落下や、浸水による装置の水没等への対策を実施しておく必要があります。自然災害の場合、その地域全体が被害に遭うことが多く、**重要な情報は地理的にも別の場所に保管する**ことが望ましいです。

【対策】
本社が東京で支社が大阪等にある場合、情報の二重化は、回線を通して比較的簡単に出来ます。一箇所にしか会社がない場合は、別の場所にある**データセンターを利用**することも出来ます。リアルタイムでの二重化が必要なければ、定期的に重要情報を遠くの倉庫に預ける方法もあります。
また、システムそのものの災害対策も重要です。地震で機器が転倒しない様な、**転倒防止策**も準備されています。浸水で水没しないように重要な社内システムは、**2階以上のフロアに設置**する等の考慮も必要ですし、建物そのものに、耐震対策がなされていれば申し分ありません。また、**電源設備**についても同じような考慮が必要であることも忘れてはいけません。

【対応するメニュー】
データバックアップ対策
転倒防止対策

セキュリティ対策　ステップ3－11

V

より強固なシステムを構築するためのセキュリティ対策

セキュリティ対策　ステップ　4

ここでは、より強固なシステム、あるいはマネジメントを構築するためのセキュリティー対策について説明しています。その必要性に応じて選択する事が大切です。

ステップ4に対応する対策をまとめると、次の
ようなものになります

1. なりすましによる情報漏洩のリスクと電子認証
（電子認証構築）
2. PCからの情報漏洩のリスクとその防止策
（シンクライアント構築）
3. 自然災害による業務停止のリスクとその対策
（システム二重化対策）
（ホスティング）
4. 装置故障による業務停止のリスクとその対策
（システム冗長化）
5. 社員への徹底不備のリスクとその対策
（セキュリティポリシー策定）
6. 資格なし、による入札停止のリスクとその対策
（ISMS認証取得支援）

Ⅴ．より強固なシステムを構築するためのセキュリティ対策

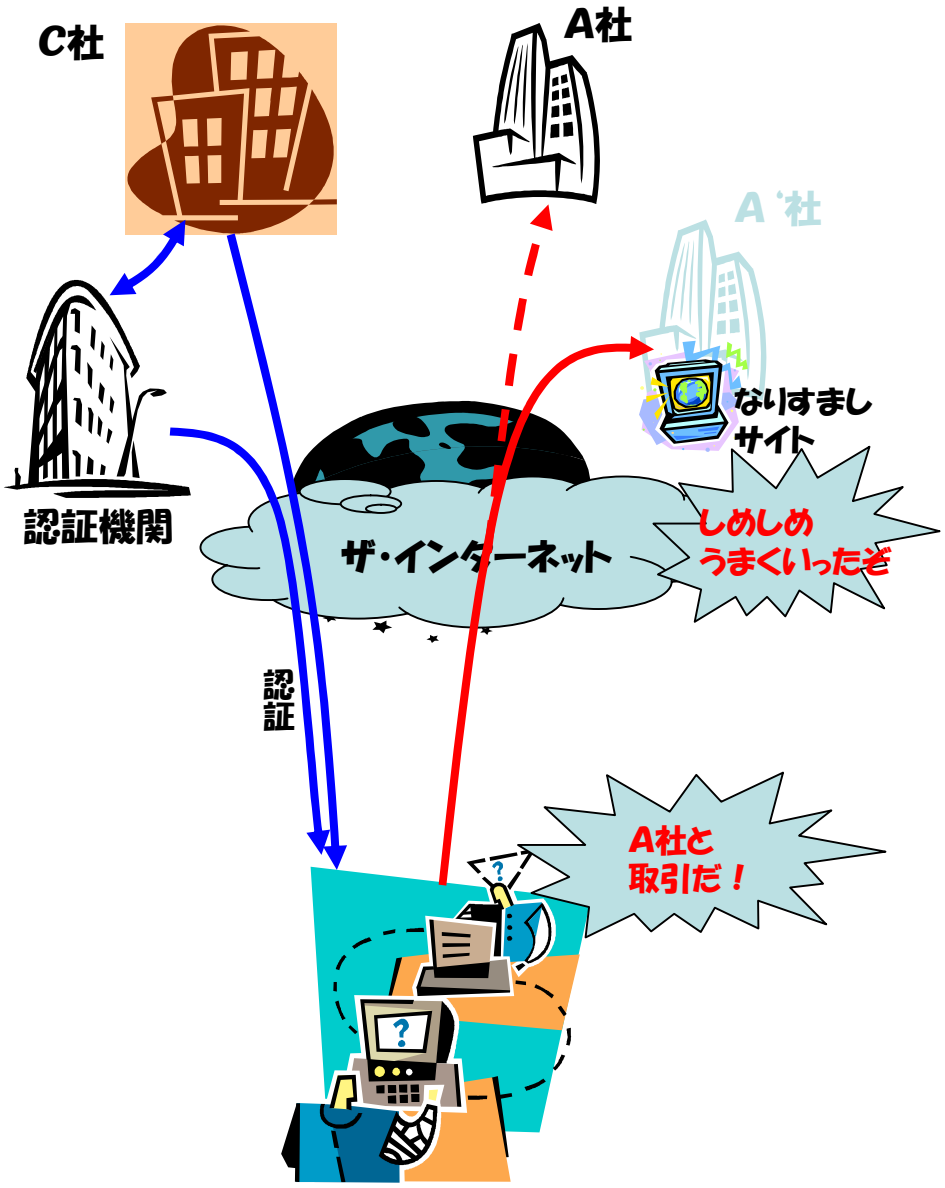
1．なりすましによる情報漏洩のリスクと電子認証

インターネットは、現在、色々な企業情報や取引に利用されるようになってきていますが、一方ではそれらの情報を横取りして、不正に利用しようとする、なりすましによる**フィッシング詐欺**や、個人情報の不正取得などが、増加してきています。情報をやり取りする相手が少なく、その素性がわかっている場合は良いのですが、商売となると多くの取引相手とやり取りをする機会が増加し、そこになりすましの相手が紛れ込んでいた場合、情報を不正に取得されるリスクが大きくなります。

【対策】
情報の漏洩を避ける為に、通信の相手が、確かにその相手であることを確認する為の手段として、公開鍵による**電子証明書**の送信文書への添付を行う方法があります。このためには、認証局による電子証明書の発行が必要です。企業内でこのシステムを構築することもできますが、準備と運用に多くの時間を必要とします。
認証の機能を外部の認証機関にアウトソースすることで構築の手間や、運用の煩わしさを避けることが出来ます。

【対応するメニュー】
電子認証構築

セキュリティ対策　ステップ4－1



Ⅴ．より強固なシステムを構築するためのセキュリティ対策

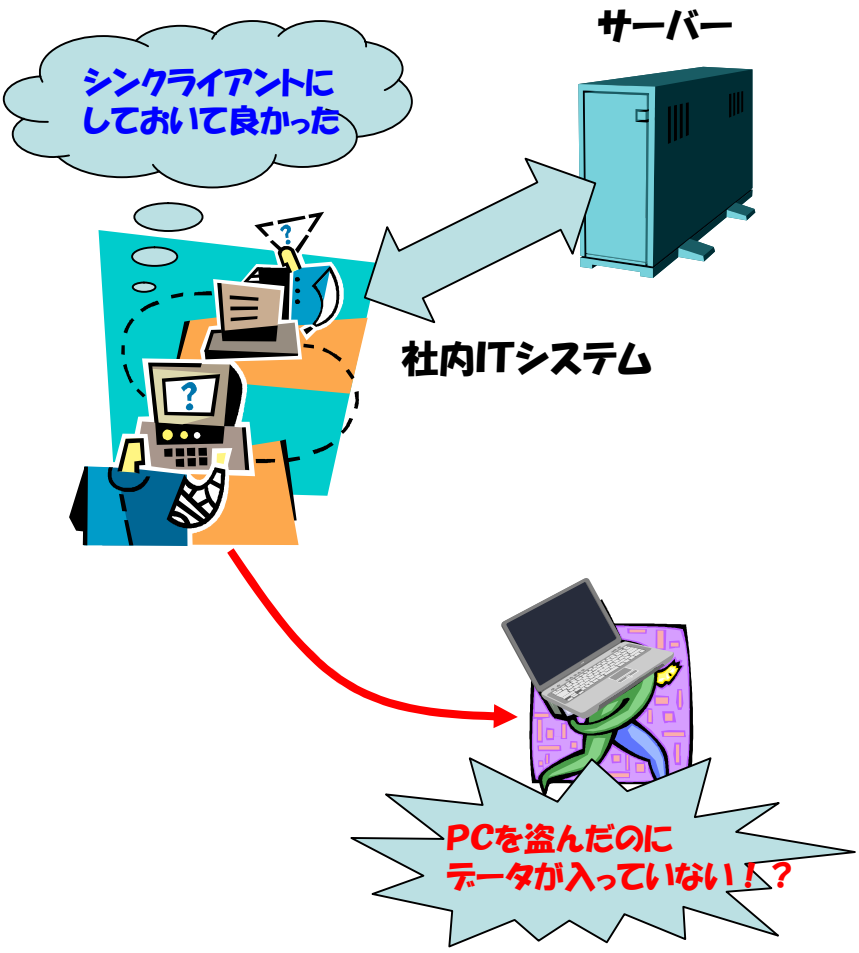
2. PCからの情報漏洩のリスクとその防止策

PCには通常、業務遂行のためのOS、アプリケーションと各種データが取り込まれています。PCが盗難に遭ったときに重要な情報が漏洩しないようにする方法は、暗号化、アクセス制御等、いくつかありますが、ここではPCそのものに、必要なとき以外はデータを入れないようにする事で情報漏洩のリスクを回避する方法について説明します。

【対策】
PCにデータや、方式によっては、アプリケーションを入れないで使う場合、このPCを**シンクライアント**と呼びます。PCそのものは通常のものと比べて不必要な機能は削除してあり、必要なアプリケーションやデータをサーバからダウンロードして使います。作業が終了すると、データ、又場合によってはアプリケーションはサーバーに戻し、PCには何も残らない為、盗難、または紛失しても情報漏洩に繋がることはありません。どこまでをサーバーで持ち、どの部分をPCに入れておくかは、その業務の使用環境を考慮し最適な方法を選択する必要があります。

【対応するメニュー】
シンクライアント構築

セキュリティ対策　ステップ4－2



Ⅴ．より強固なシステムを構築するためのセキュリティ対策

3．自然災害による業務停止のリスクとその対策

地震・浸水等自然災害の多い日本では、発生した場合への対策を充分検討して置く必要があります。地震に対しては、従業員の方々の被害防止がまず第一ですが、ITシステムに関して言えば、建物その物の倒壊、ITシステムの転倒・落下によるシステム停止、電力会社からの危険防止のための電力供給停止、等のリスクが考えられます。また、浸水に対しては、ITシステムの水没、漏電防止の為の電源供給の停止等のリスクがあります。

【対策】

地震に関しては、建物そのものの**耐震強度**は確保されているか、揺れに対して**転倒防止策**は打たれているか、さらに電力供給のための、**予備の電源設備**（発電機も含む）は準備されているか等が、浸水に関しては、被害に遭い難い2階以上に設備を置いておくことと、電源設備の準備があります。また大規模災害時には現地での業務継続は困難ですので、同じ業務の出来るシステムを、**ASP**に確保しておくという手段も考えられます。

【対応するメニュー】

システム二重化対策
ＡＳＰによるホスティング
（転倒防止対策）

ASP：アプリケーション・サービス・プロバイダの略。お客様の業務を代替できるシステムを提供する。

セキュリティ対策　ステップ　4－3

Ⅴ．より強固なシステムを構築するためのセキュリティ対策

4. 装置故障による業務停止のリスクとその対策（システム冗長化）

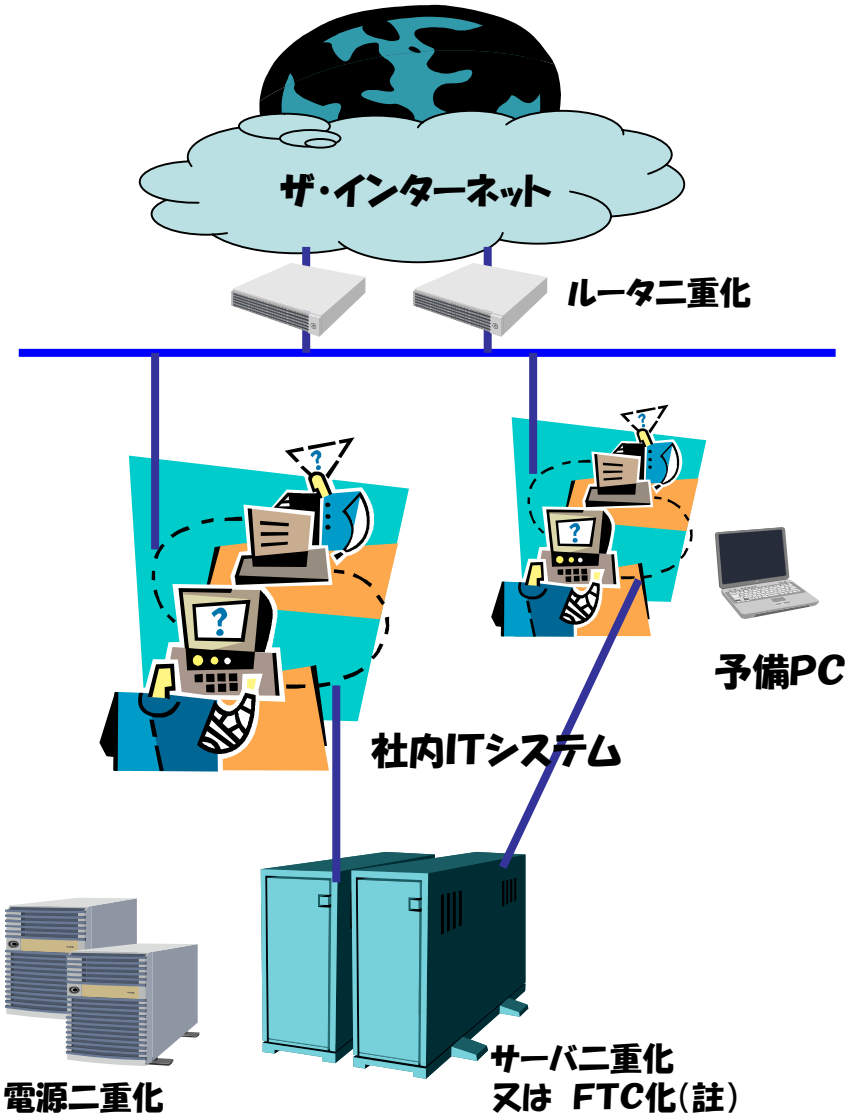
PCやサーバーは業務処理の中でも重要な情報を扱うようになってきています。ソフトウェアの安定化も重要ですが、PC・サーバーも電子機器であるため、故障は避けられません。この故障が、重要な業務処理中に発生した場合、故障修理がすぐにできたとしても、数時間の遅れが、又最悪の場合は数日間の遅れが発生することがありますし、重要なデータが入っているディスクがクラッシュした場合、**データの復元が出来ない**こともあります。

【対策】
故障が発生した場合に、業務処理に大きな影響を与える機器（例えばサーバー、ディスク、回線のインターフェース機器（ルーター、スイッチ）等）の**一部または全体を二重化**しておくことができます。

【対応するメニュー】
システム冗長化

註：FTC：フォールト・トレラント・コンピュータの略
構成が全て二重化されており、故障時もダウンしない

セキュリティ対策　ステップ4－4



Ⅴ．より強固なシステムを構築するためのセキュリティ対策

5. 社員への徹底不備のリスクとその対策

情報セキュリティの社員教育は重要ですが、その他各種対策が社内システムに対して施されていることでしょう。それでは、その情報セキュリティに対する**会社としての基本的な考え方**はどんなものでしょうか。「我が社は、情報セキュリティに関してこういう方針で臨む」という柱を立てることで会社全体の方向性が明確になり、各種対策の遂行方針も明確になってきます。これがないと、場当たり的な対策のつぎはぎとなり、全体として抜けが出たり、余分な投資をすることになります。

【対策】
会社としての「**情報セキュリティ方針**」を定め、従業員に徹底しておく必要があります。
例えば
・当社は、情報セキュリティ管理体制を確立し、情報資産の適切な管理に努めます。
・当社は情報セキュリティの確保に必要な教育を行います
など

【対応するメニュー】
情報セキュリティポリシ策定

セキュリティ対策　ステップ4－5

情報セキュリティ方針

1. 当社は:、情報セキュリティ管理体制を確立し、情報資産の適切な管理に努めます
2. 当社は情報セキュリティの確保に必要な教育を行います
3.
4.
5.
6.

Ⅴ．より強固なシステムを構築するためのセキュリティ対策

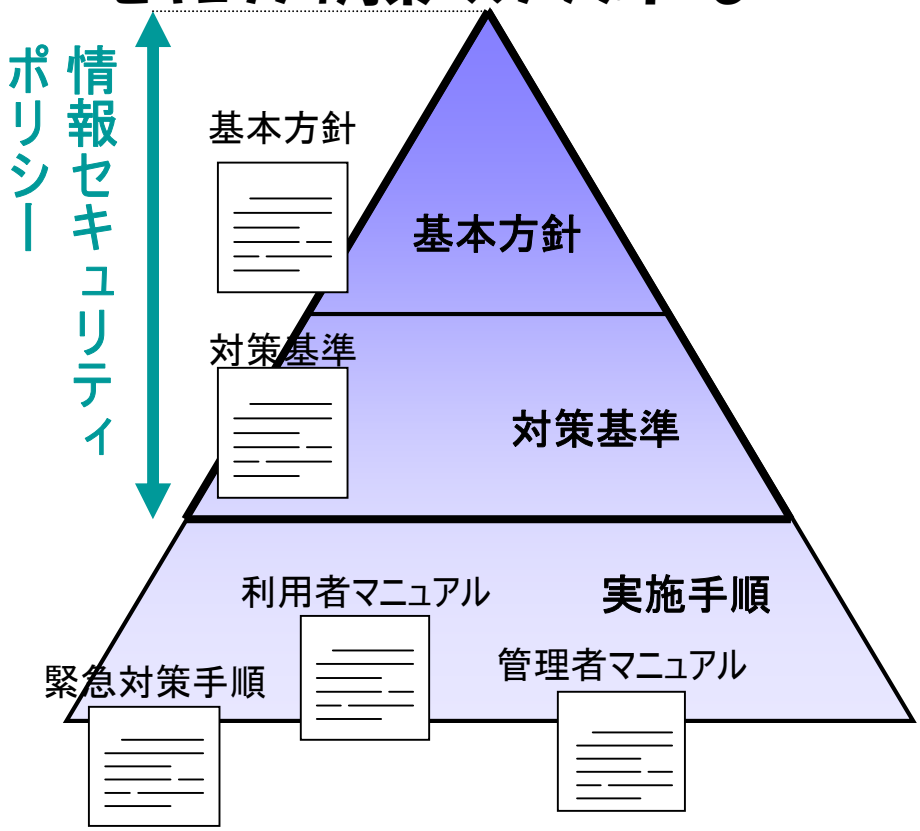
6．資格なしによる入札停止のリスクとその対策

政府のｅ－JAPAN構想により、政府・自治体への入札には、**ISMS（ISO27001）認定**が必要となってきています。
この認定は、企業内でセキュリティの管理体制が存在し、管理体制のPDCAサイクルを構築しているなど、セキュリティ対策を積極的に行っているという、外部への証明となります。
また、政府・自治体に牽引される形で銀行や大手企業においても、取引をする相手としてISMS認定を求められ始めており、中小企業でも間接的に、要求の度合いが高くなってくることが予想されます。
しかしながら、ISMS認定を取得するのは非常に時間・労力がかかり、自力では取得できないのが現状です。

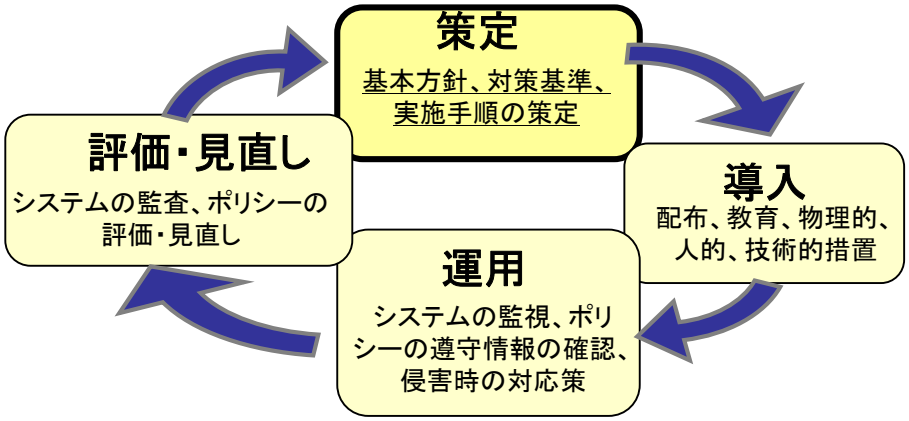
【対策】
ISMS認定を取得するには、場合によっては、数百ページに渡る資料作成や内部監査などノウハウが必要となることがあります。自力で取得を目指すことも出来ますが、早期の資格取得が必要な場合には、**ISMS認定取得支援**を依頼する方法が良いでしょう。

【対応するメニュー】
ISMS認定（認証）取得支援

セキュリティ対策　ステップ4－6



情報セキュリティマネジメントサイクル



VI

メニューの説明

ここでは、これまで説明してきた、各種対策に
対して、標準的なメニューとその構成、及び
費用項目（一時的なものと継続的なもの）について
ふれています。

メニューについては、各ベンダー、販売店により
独自の考え方で提供されているので、それぞれ
異なるはずです。
ここでは、その共通的な部分を標準的なメニュー
として紹介していますので、これを参考に、実際
には、各販売店と相談しながら対策を検討して
頂ければ幸いです。

内部統制に関連すると思われるメニューを青字で
表しているので、参考にしてください。

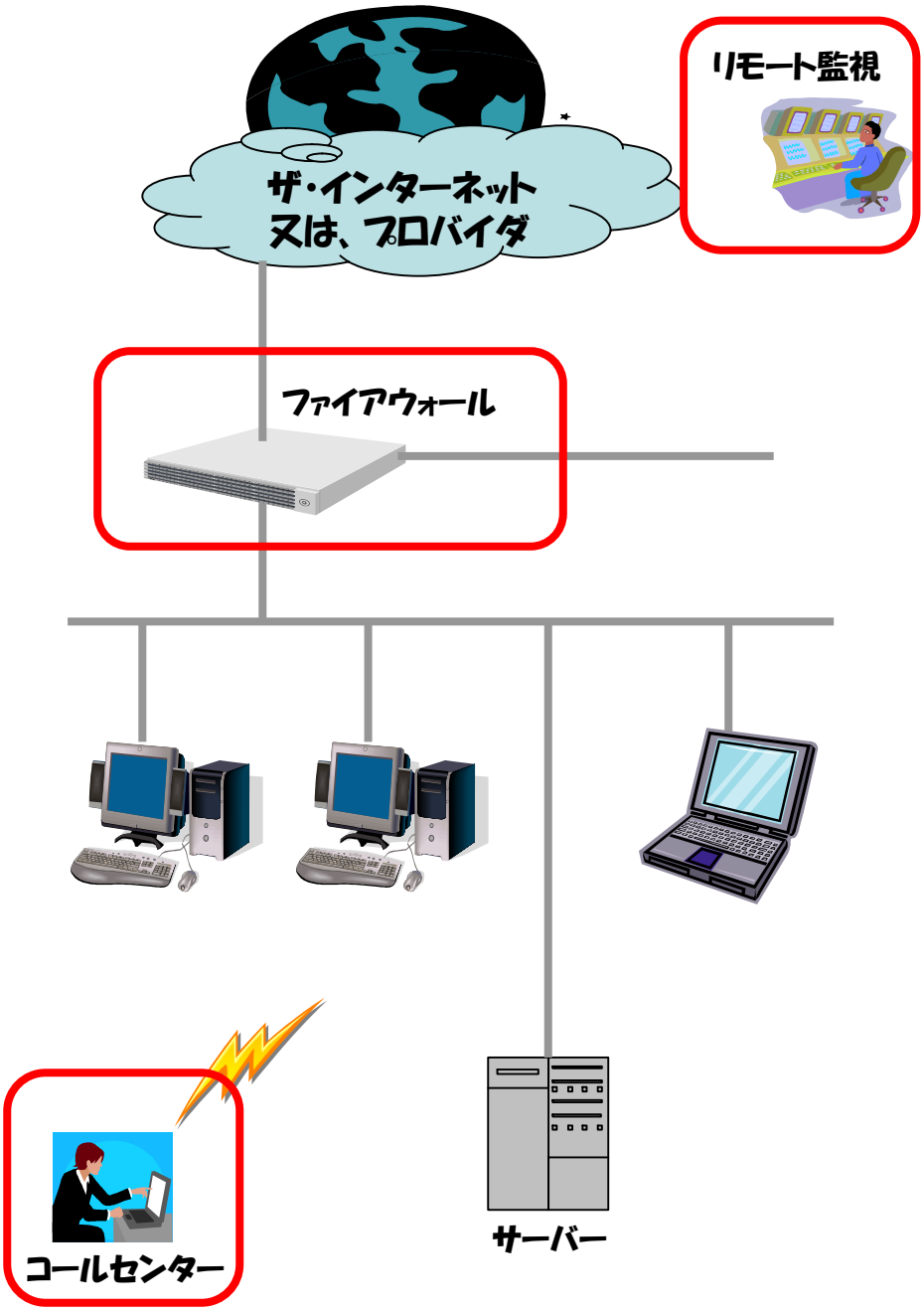
1. ファイアウォール対策
2. ウイルス対策ソフト導入サービス
   スパイウェア対策導入サービス
3. データバックアップ対策（外部侵入、電源故障など）
4. アクティブディレクトリによるID管理
5. ノートPC対策
6. 情報セキュリティ教育
7. スパムメール対策／不正アクセス運用・監視
8. URLフィルタリング／メールフィルタリング
9. データ暗号化対策
10. 事前保守・監視サービス
11. ICカード・入退出管理
12. データクリーンサービス
13. ファイルアクセス管理ツール
14. ファイルアクセス管理ツール（ドキュメントセキュリティ）
15. IDS・IPS構築
16. クライアントPC監視
17. 検疫システム構築
18. 無線LAN暗号化
19. ユーザ認証強化対策
20. PC不正操作対策
21. 情報セキュリティ評価・診断サービス
22. 付帯設備監視
23. ログ収集・解析（メール証跡保存対策）
24. 個人情報取扱事業者保険
25. 自然災害時のデータバックアップ対策
26. 電子認証構築
27. シンクライアント構築
28. システム二重化対策／ASPホスティング
29. システム冗長化
30. 情報セキュリティポリシ策定
31. ISMS認証取得支援

Ⅵ. メニューの説明

1. ファイアウォール対策

現状調査＋最適な装置の選択＋設置＋設定＋動作確認
＋メンテナンス（ハード及びソフト）
　＋（Opt）リモート監視
　＋（Opt）コールセンターサポート

【内容説明】
不正アクセス防止のためにファイアウォールを構築します。
簡単な現状調査と、ご要望に適した機器の選択から設置・
確認までを行います。ファイアウォール装置は、新手の
攻撃に対応する為、内蔵するハード・ソフト等の新バージョン
への定期的な入れ替えメンテナンスが必須です。
オプションとして
攻撃状況を常に監視し、状況をお客様にお知らせする、
リモート監視の機能を準備しています。
また、攻撃により業務遂行に支障が発生し、原因が判らない
ような状況から、早期に抜け出す為、コールセンターサポート
機能も準備しています。
【費用項目】
一時費用
ファイアウォール装置（小規模用）
その他、調査、設置、設定、確認の費用は別途見積
継続的費用
ファイアウォールメンテナンス費
（Opt. ）リモート監視：回線費用（VPN）、常時監視、ログ
管理等
（Opt. ）コールセンタサポート費用

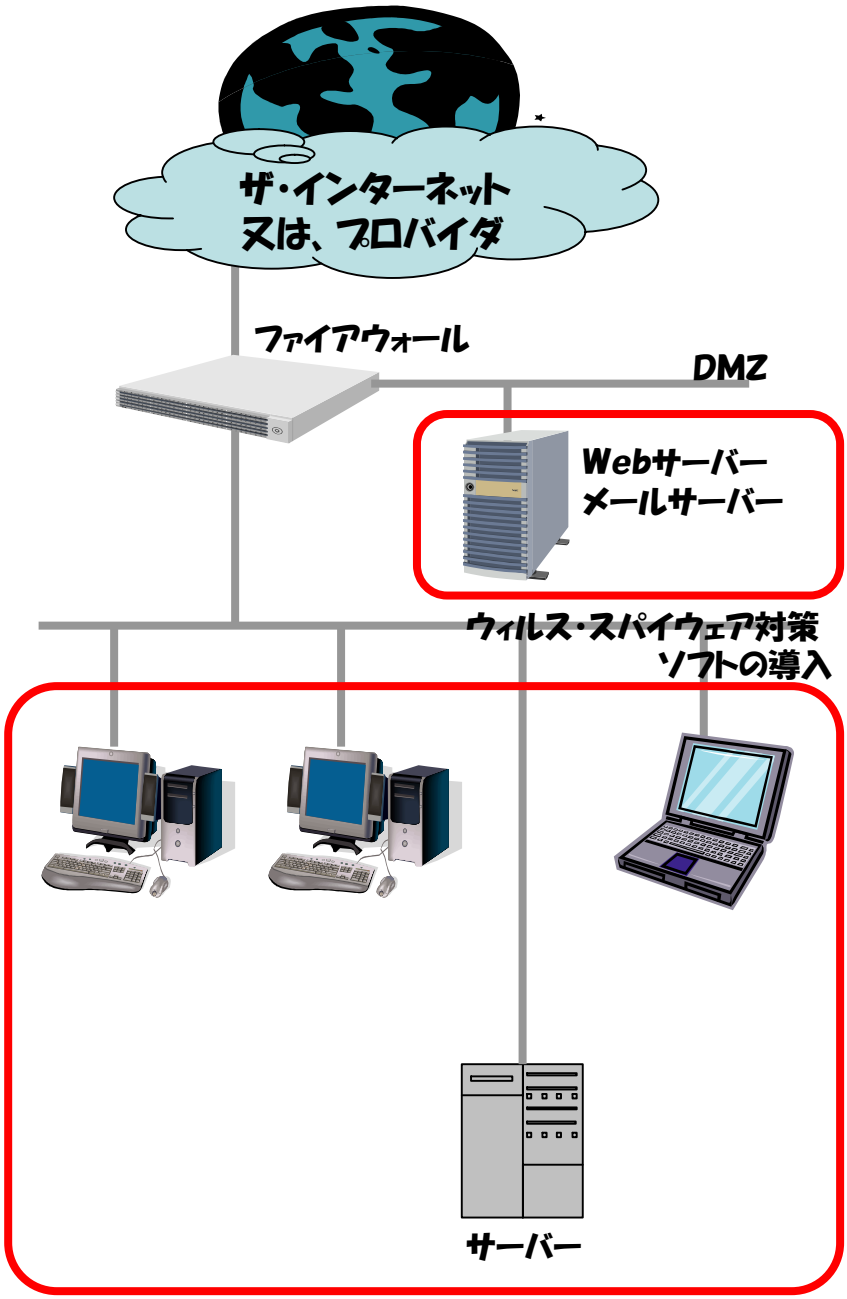

リモート監視
ザ・インターネット
又は、プロバイダ
ファイアウォール
コールセンター
サーバー

VI. メニューの説明

2. ウイルス対策ソフト導入サービス
スパイウェア対策導入サービス

現状調査＋最適なソフトの選択＋導入＋動作確認
＋メンテナンス（定期バージョンアップ）

【内容説明】
ウィルス対策のソフトには、サーバーに導入するものと
クライアントPCに導入するものとがあります。またインター
ネット経由で入ってくるメール、Webアクセス時に検出する
タイプのものもあります。どのタイプも基本的にはパターン
ファイルというほぼ毎日アップデートされる、ウィルス対策用
ファイルを参照しながらウィルスを検出するので、パターン
ファイルの確実なアップデートが必要です。パターンファイ
ルの自動的なアップデートも設定できます。
スパイウェアについても、メールやWebに混入して、入って
くるもの、外部媒体から入ってくるものがありますが、これら
の対策ソフトでリアルタイムにチェックしておくことで、混入の
チェックを行うことが出来ます。
【費用項目】
一時費用
クライアント対策ソフト
サーバ対策ソフト
クライアント・サーバー対策ソフト
その他、調査、設定、導入、確認の費用は別途見積
継続的費用
メンテナンス費（バージョンアップ）
　　（Opt）：コールセンタサポート費


ザ・インターネット
又は、プロバイダ
ファイアウォール
DMZ
Webサーバー
メールサーバー
ウィルス・スパイウェア対策
ソフトの導入
サーバー

Ⅵ. メニューの説明

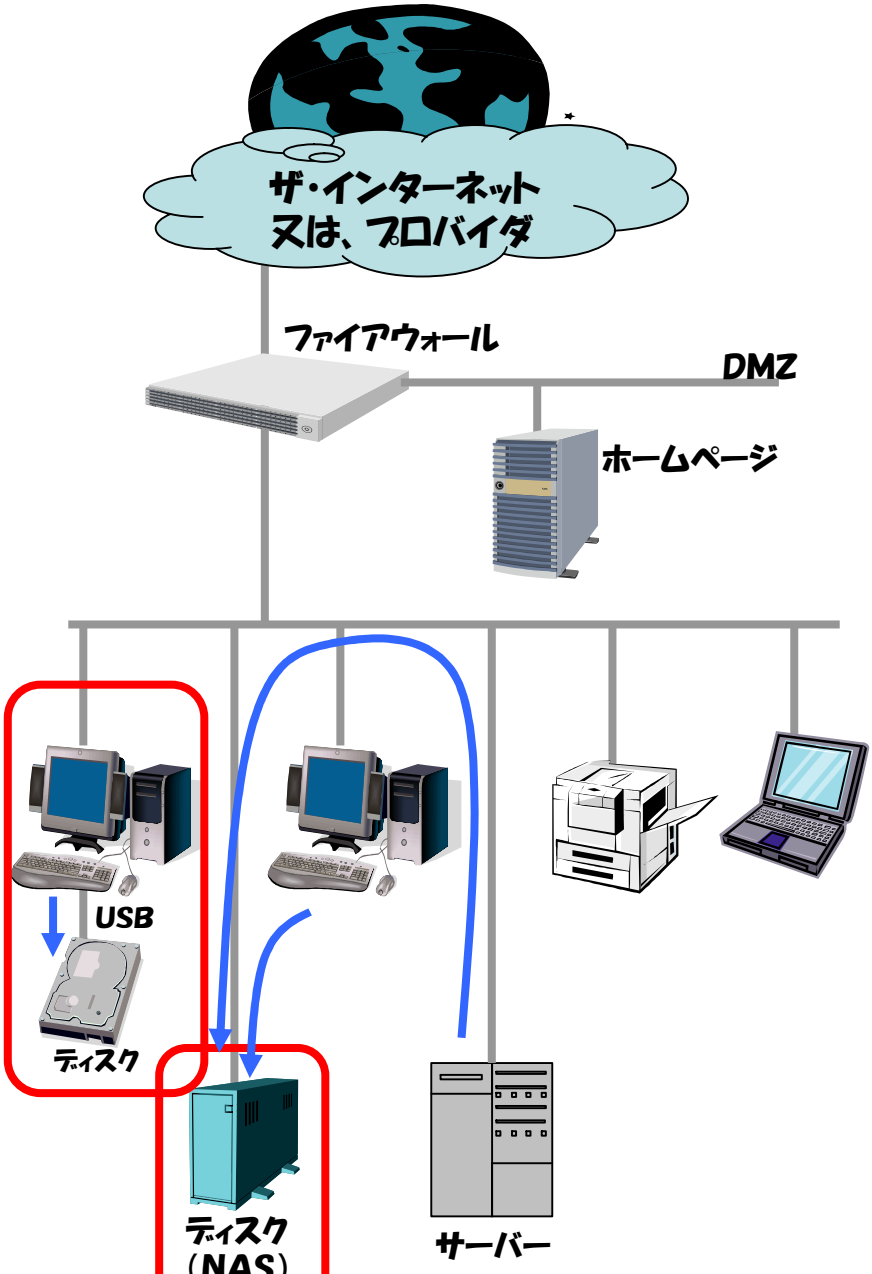
3. データバックアップ対策（外部侵入、電源故障など）

現状調査＋バックアップ機器＋ソフトウェア＋設定＋確認
　＋メンテナンス（バージョンアップ）・サポート

【内容説明】
外部からの侵入により、ホームページが改ざんされたり、
PC内の重要な情報が壊されたりした場合には、バックアップ
データとの置き換えが必要になります。
更に、装置故障や、電源の故障で作成途中のデータ等が
失われる可能性があります。従って常に最新の状態の
バックアップ情報を持っておくために、定期的なバックアップ
が重要になります。
ツールにはUSB接続での簡単なバックアップを行うものから
サーバのバックアップをとる本格的なものまで各種準備され
ています。

【費用項目】
一時費用
機器費用：USBディスク
簡易型（USB接続）ソフト費
基本型（NAS接続）ソフト費
バックアップサーバ
調査・設定・確認の費用は別途

継続的費用
メンテナンス（バージョンアップ等及び機器保守）費



NAS:Network Attached Storageの略

Ⅵ. メニューの説明

4. アクティブディレクトリによるID管理

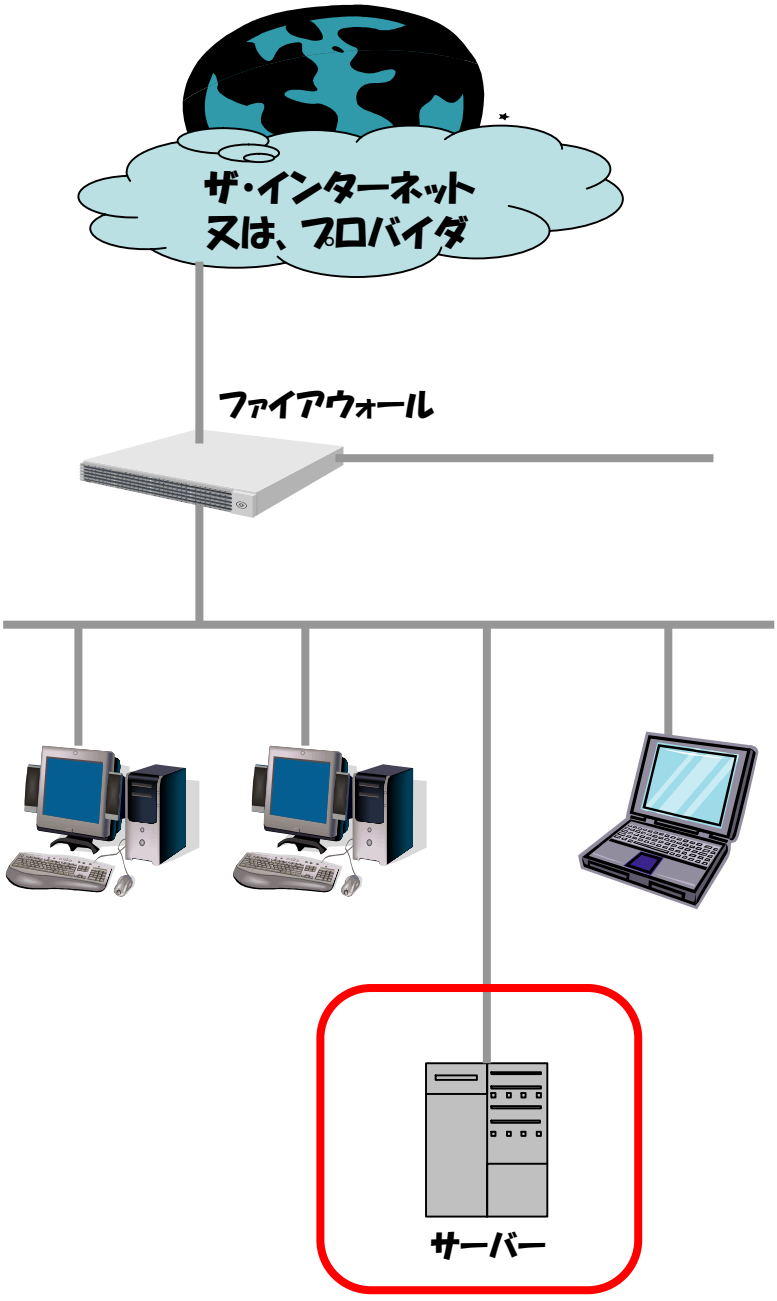
Windows2000サーバを導入している、又は導入予定の場合は、アクティブディレクトリによるID管理が可能です。

現状調査＋設定（カストマイズ）＋動作確認
　＋メンテナンス（変更対応）

【内容説明】
アクティブディレクトリはネットワークに接続された資源を一括管理できるツールであり、大規模システムにも対応できるようになっています。使用者側から見ると複数のIDとパスワードを管理しないで済むので、使いやすいということになります。（シングルサインオン）

【費用項目】
一時費用
調査・方針決定等のコンサルテーション費用

継続的費用
更新が必要な場合の更新費用のみ



106

Ⅵ. メニューの説明

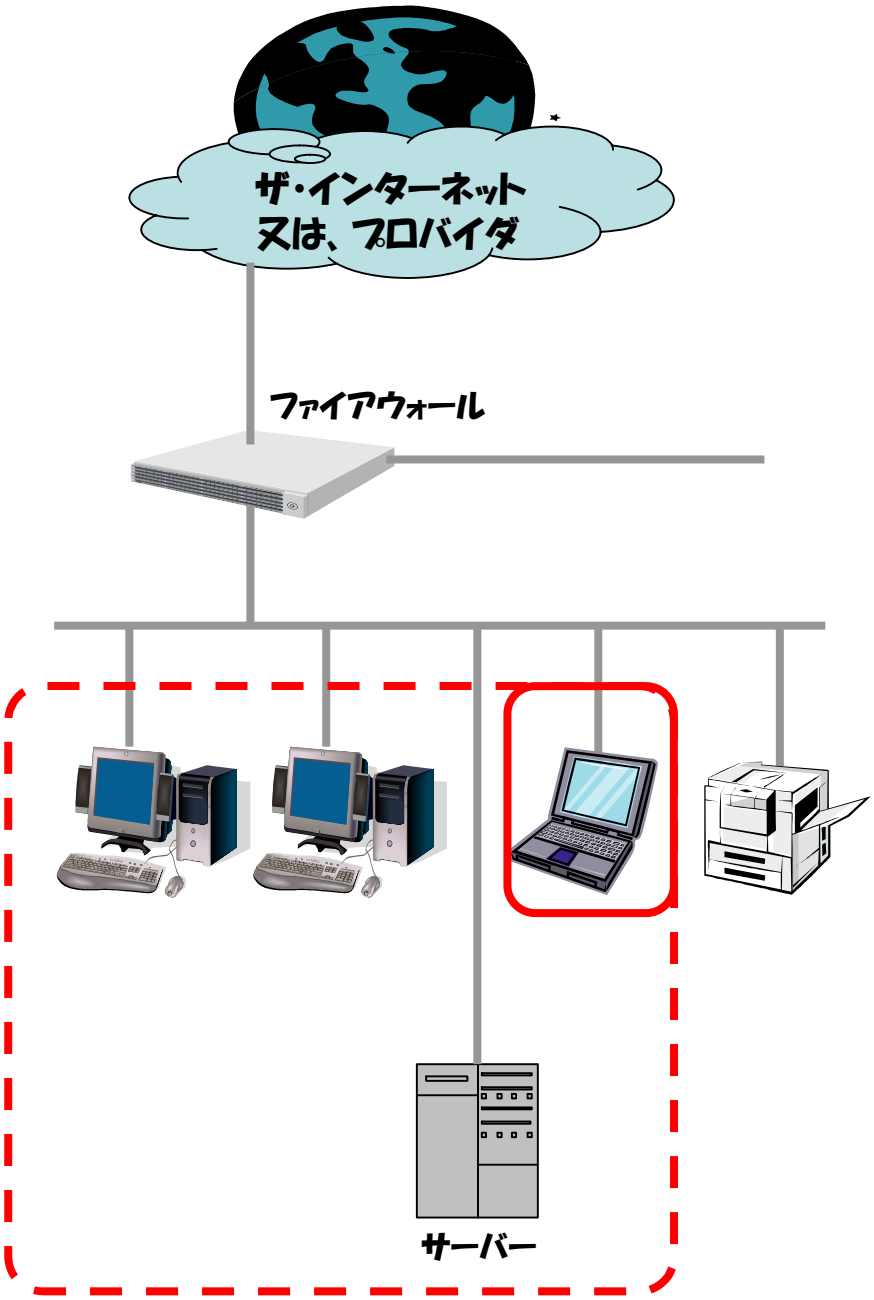
5. ノートPC対策

現状調査＋暗号化ソフト費＋設定＋動作確認
　＋メンテナンス・サポート費

【内容説明】
ここではPCそのものに入っている情報と、それを持ち出すときの対策を説明します。
ノートPCにはハードディスクが内蔵されており、通常の作業は、このディスクを使って行うことが多いのです。そのためPCが盗難に遭うと、このディスクから重要な情報が漏洩する可能性が高くなります。これを避ける為に、ディスクに入る重要情報を全て暗号化するツールが用意されています。
暗号化ツールには、その他、外部メモリの暗号化、認証機能・印刷抑止・メールへの添付の抑止等の機能が含まれるものが多くあります。

【費用項目】
一時費用
基本機能（暗号化のみ）：１クライアント当り
拡張機能（各種）：サーバ＋クライアント当り
調査・設定・確認の費用は別途

継続的費用
メンテナンス（バージョンアップ等）及びサポート費


ザ・インターネット
又は、プロバイダ
ファイアウォール
サーバー

VI. メニューの説明

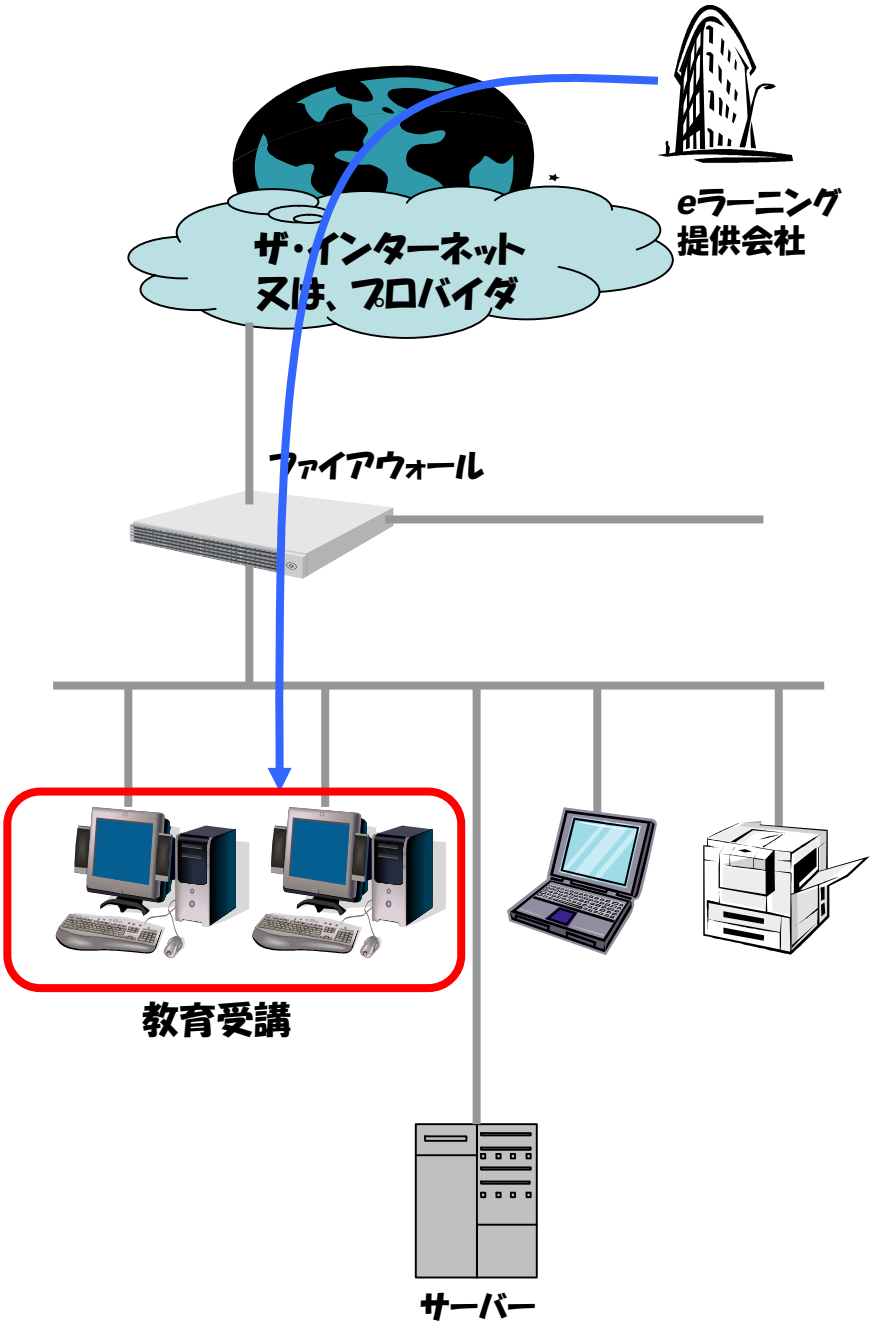
6. 情報セキュリティ教育

eラーニングコース
eラーニング＋スクーリングコース
集合教育コース　　等
販売店・ベンダーから提供されているものが多数あります。

【内容説明】
eラーニングの形で行う教育は遠隔地でも、受講できる
メリットがあります。集合教育との組み合わせで行う
コースも準備されています。また技術認定を行うコース
もありますので、必要性に応じて選択するのが良いで
しょう。
最も重要なのは、従業員の意識レベルを高く維持する
為に教育を定期的に行うことですが、維持の為には社
内の事例を使って資料を作成し、従業員に徹底させる
という方法も有効です。

【費用項目】
一時費用
eラーニング：インターネット対応版クライアント当り費用

継続的費用
１年間に数回の意識レベル維持教育費用（eラーニング使用
の場合は上記と同様）


eラーニング
提供会社
ザ・インターネット
又は、プロバイダ
ファイアウォール
教育受講
サーバー

Ⅵ. メニューの説明

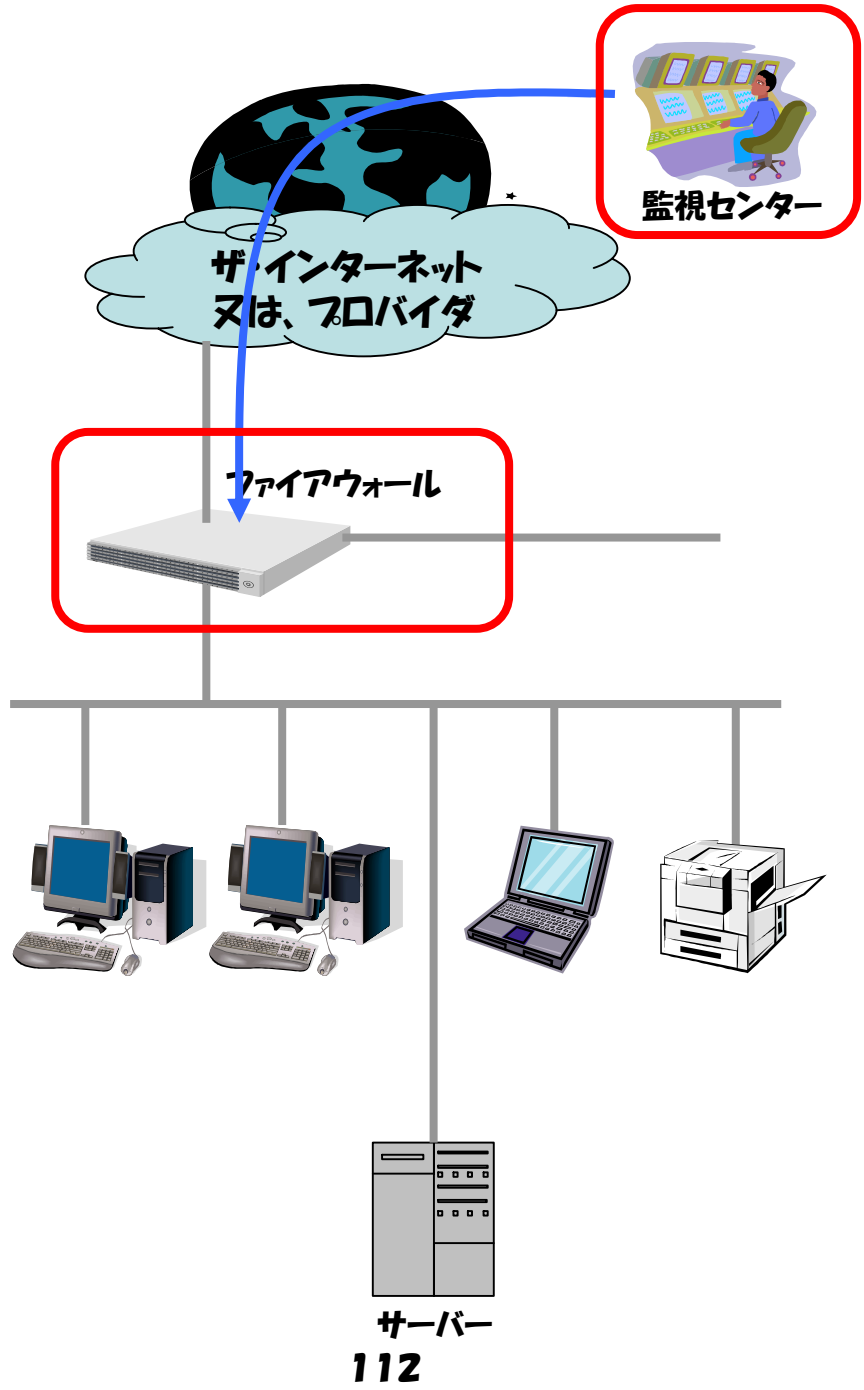
7. スパムメール対策／不正アクセス運用・監視

現地調査＋ファイアウォール機器＋設置＋動作確認
　＋リモート監視

【内容説明】
インターネットから送られてくる大量の迷惑メール対策
では、この迷惑メール（スパムメール）を自働的に振り分け
てくれるフィルタリング対応ソフトが準備されています。
また、プロバイダでもスパムメールを振り分けてくれる
機能を提供しています。さらにこれらの不正アクセスに
混じって、悪意のある攻撃を仕掛けてくる相手に対して、
対策をとる為に24時間の監視と分析を行うことが出来ます。
この監視サービスによりアクセスログの集計・分析や
必要なパッチの適用なども行うことが出来ます。

【費用項目】
一時費用
ファイアウォール装置（小規模用）
その他、調査、設置、設定、確認の費用は別途見積

継続的費用
メンテナンス(機器保守・ソフト設定変更等）
リモート監視費


監視センター
ザ・インターネット
又は、プロバイダ
ファイアウォール
サーバー
112

Ⅵ. メニューの説明

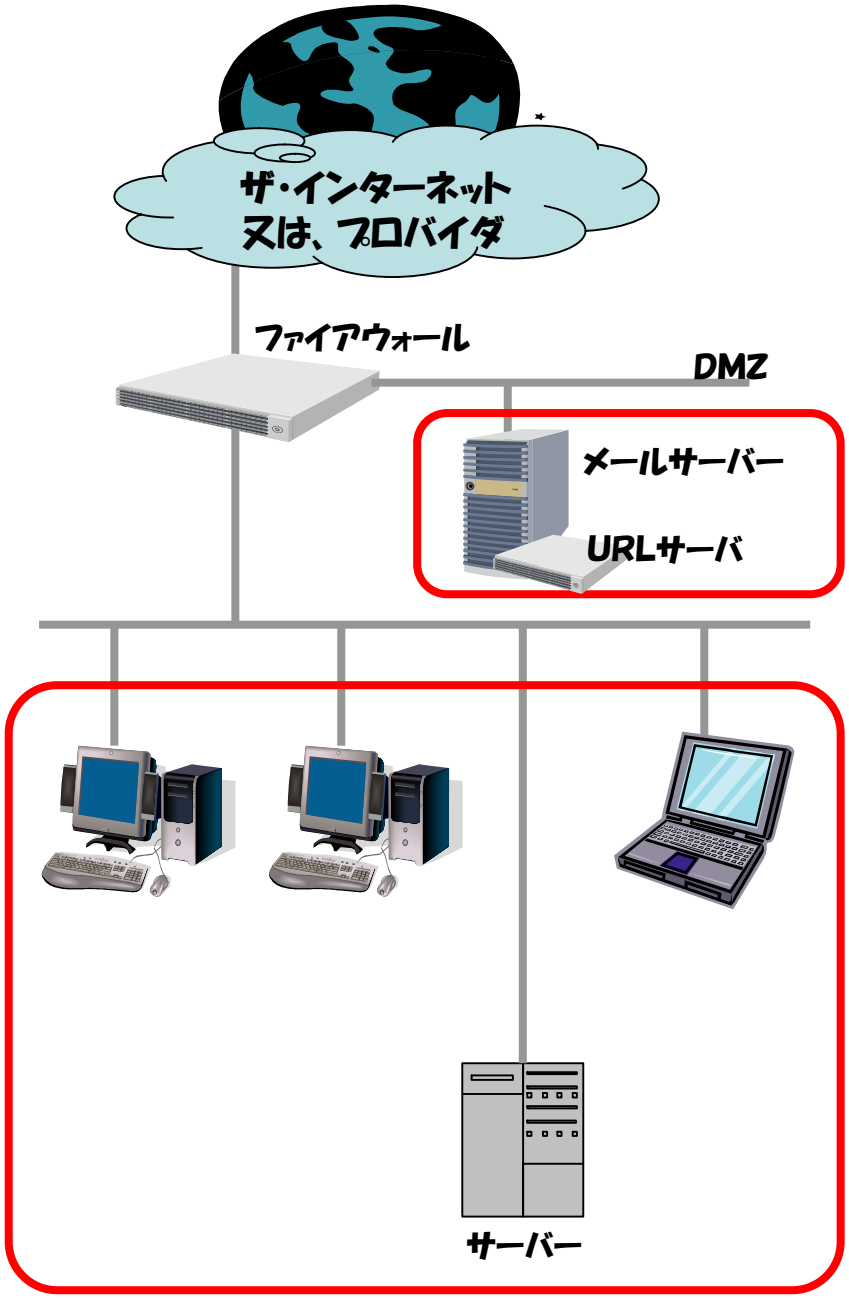
8. URLフィルタリング／メールフィルタリング

現状調査＋フィルタリングソフトの選択＋導入＋動作確認
＋メンテナンス（定期バージョンアップ）

【内容説明】
URLフィルタリングソフトは、業務外のWebアクセスを制限したり、ログ情報をレポートしたりする機能を持っています。プロバイダによっては、フィルタリング機能を無料で提供しているところもあります。
メールフィルタリングソフトは、インターネットに出入りするメールを振り分けたり、止めたりする機能を持っています。メール内の言葉を検出して制御できるので、社内のマル秘情報の流出を止めることも出来ます。

【費用項目】
一時費用
専用サーバ（含むソフト）費
メールフィルタリングソフト費
その他、調査、設定、導入、確認の費用は別途見積

継続的費用
小規模事業者向けにはサーバ不要のASPサービスもあり。
ライセンス料は規模・ソフトにより異なる為、販売店またはベンダーに問合せをお願いします。
メンテナンス費用も必要です。


ザ・インターネット
又は、プロバイダ
ファイアウォール
DMZ
メールサーバー
URLサーバ
サーバー

Ⅵ. メニューの説明

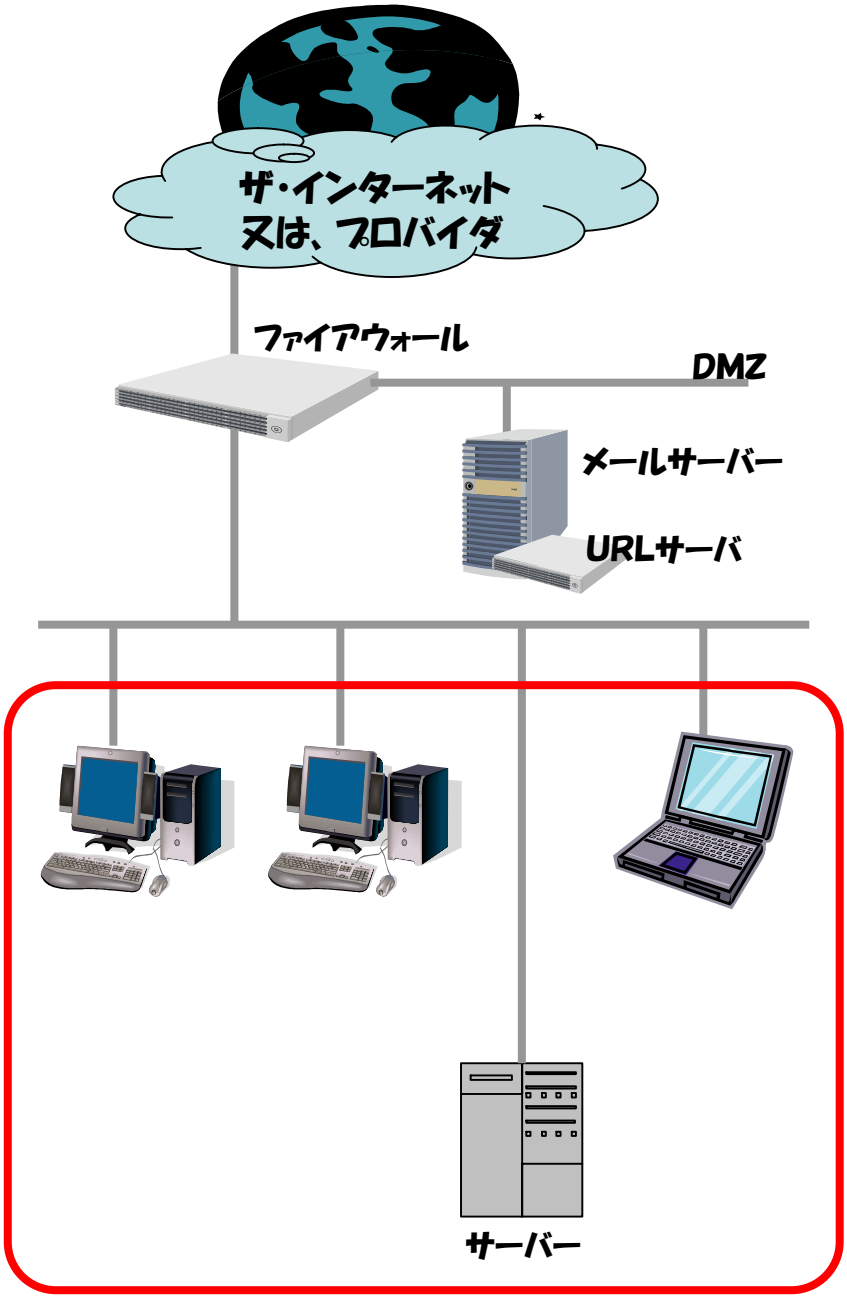
9. データ暗号化対策

現状調査＋暗号化ソフトの選択＋導入＋動作確認
＋メンテナンス（定期バージョンアップ）

【内容説明】
暗号化のソフトにはメール、内部ファイル、外部ファイルをそれぞれ又は全てを対象としたものがあります。ファイル系の暗号化ソフトには、メールへの添付ファイルの抑止や外部持ち出しの禁止、又、持ち出しのログ管理を行う物もあります。
重要なのは何を守りたい（暗号化したい）のかを明確にし最適なソフトを選ぶことです。

【費用項目】
一時費用
暗号化ソフト：小規模1クライアント当り
各種追加機能つきもあり
その他、調査、設定、導入、確認の費用は別途見積

継続的費用
メンテナンス（バージョンアップ及び設定変更等）費用


ザ・インターネット
又は、プロバイダ
ファイアウォール
DMZ
メールサーバー
URLサーバ
サーバー

Ⅵ. メニューの説明

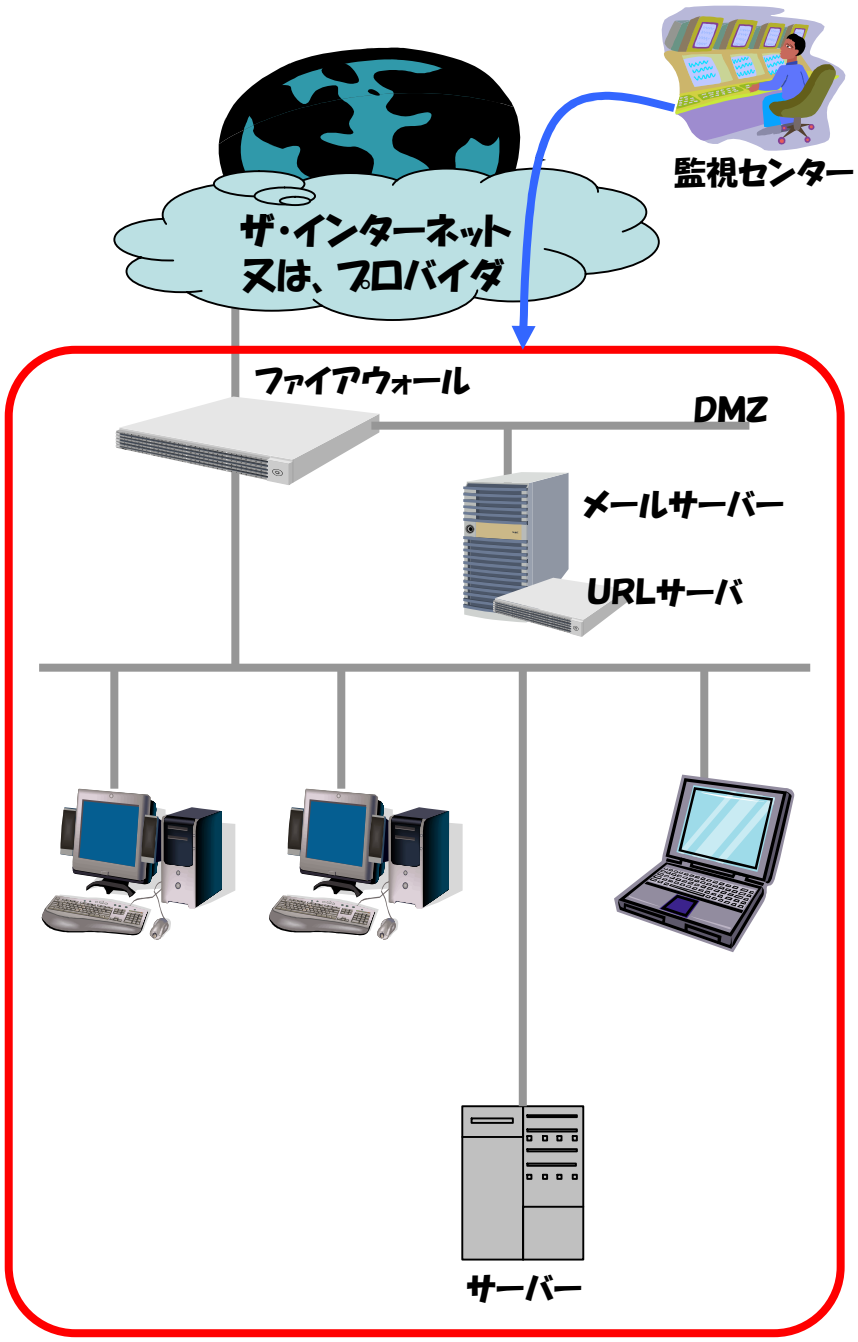
10. 事前保守・監視サービス

現状調査（監視対象明確化）＋監視ソフト＋導入＋動作確認
＋監視・メンテナンス

【内容説明】
最近のITシステムは、マルチベンダが当然となっている為
事前の調査で監視できる機器と出来ない機器、監視を実施
するものとしないものを明確にしておくことが必要です。
事前保守や監視で、障害によるデータ破壊等を防ぐことが
出来ます。

【費用項目】
一時費用
監視ソフト：小規模1クライアント当り
　　各種追加機能つきもあり
その他、調査、設定、導入、確認の費用は別途見積

継続的費用
定期保守費用
監視サービス費用


監視センター
ザ・インターネット
又は、プロバイダ
ファイアウォール
DMZ
メールサーバー
URLサーバ
サーバー

Ⅵ. メニューの説明

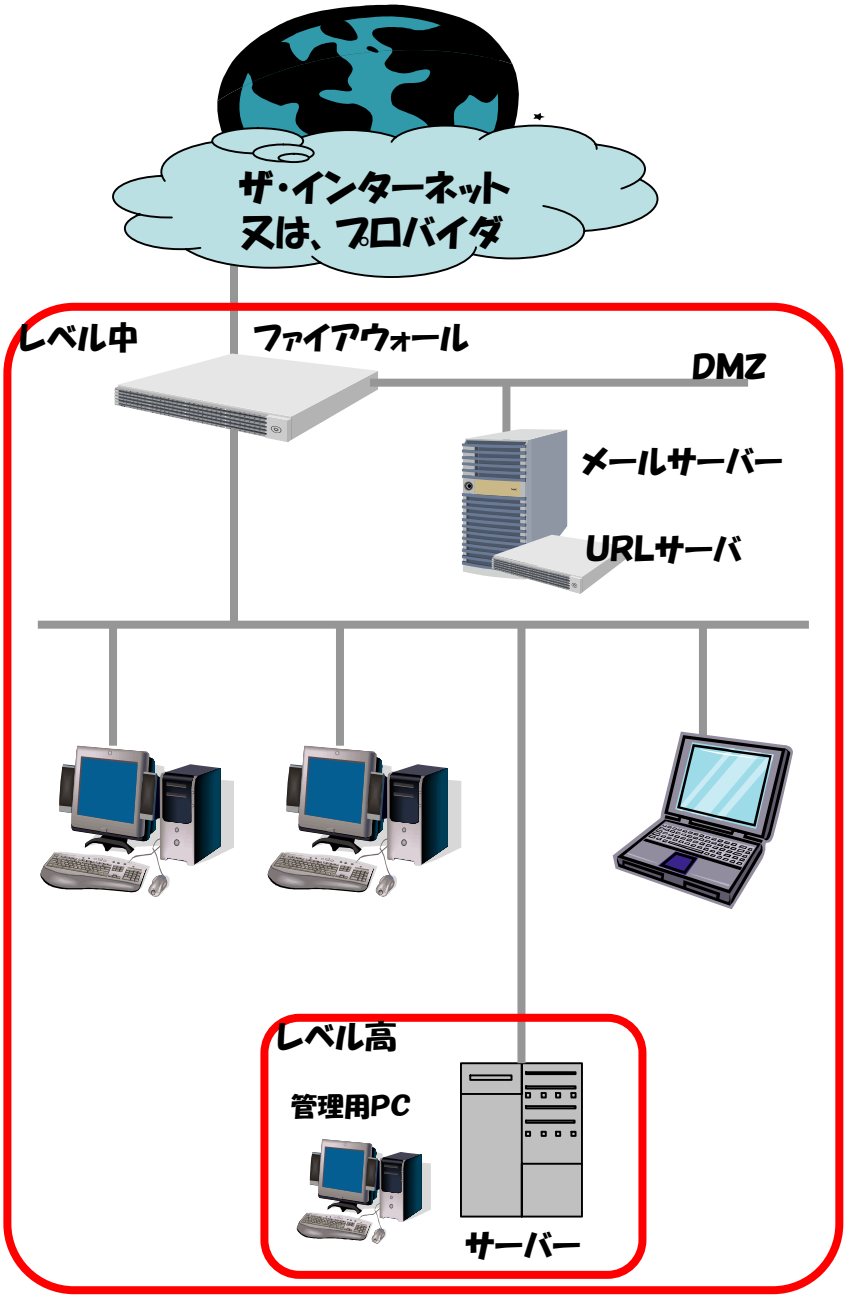
11. ICカード・入退出管理

現状調査＋認証用機器（ハード及びソフト）＋設置工事
＋設定＋動作確認
＋メンテナンス

【内容説明】
ICカード等の認証機器は設置の為の工事を伴います。
また監視用のソフト及びPCも必要です。認証の為に、
従業員のデータの入力も必要ですが、セキュリティの
レベルによって登録する情報を絞り、情報の漏洩の可
能性を低くすることも重要です。

【費用項目】
一時費用
認証用機材：ICカード：基本作成費
カード１枚当り費用×枚数
管理ソフト費用
その他、調査、設置、設定、確認の費用は別途見積

継続的費用
メンテナンス（機器保守及び設定変更等）費用


ザ・インターネット
又は、プロバイダ
レベル中
ファイアウォール
DMZ
メールサーバー
URLサーバ
レベル高
管理用PC
サーバー

VI. メニューの説明

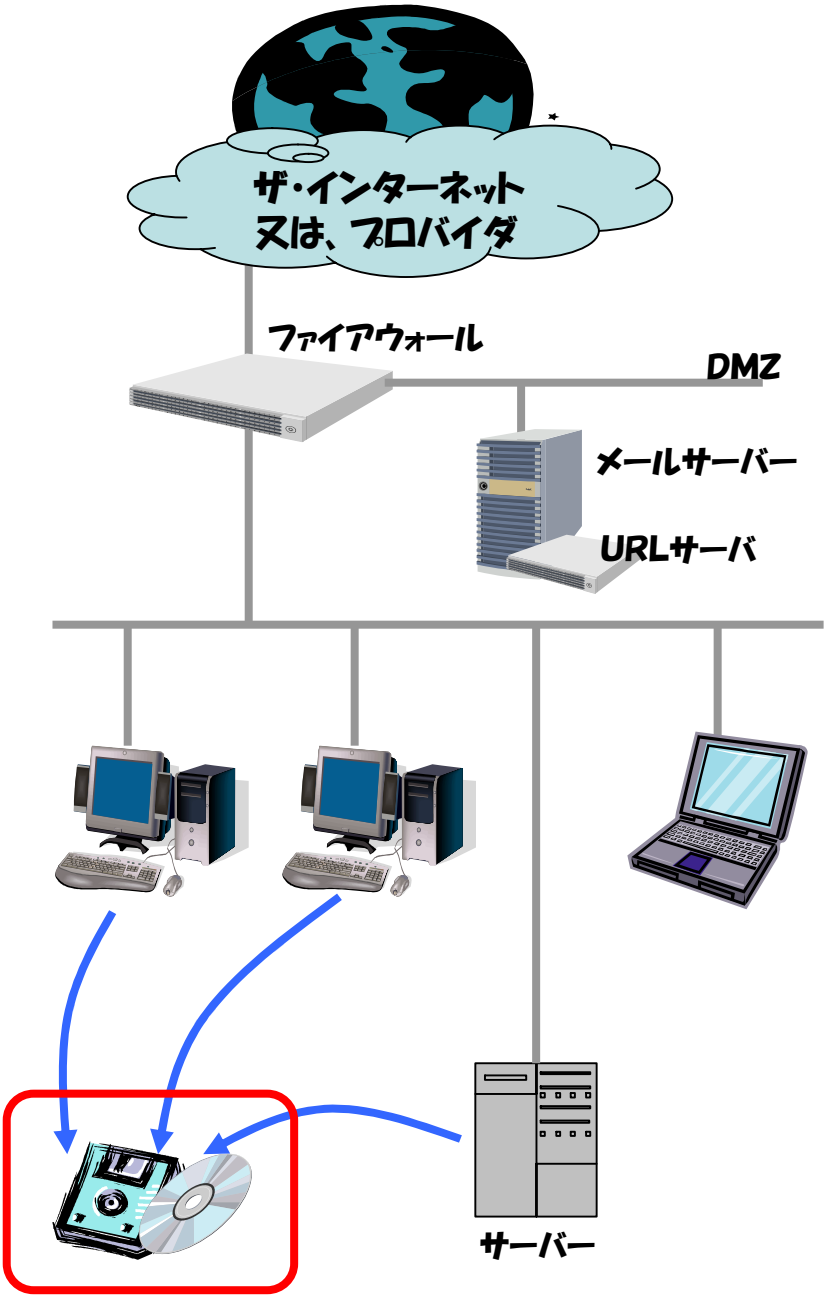
12. データクリーンサービス

現状調査＋消去レベルの決定＋消去作業＋廃棄処理
　＋（Opt）消去証明の発行

【内容説明】
媒体によって消去方法が異なります。
PCに組み込まれているハードディスクについては
PCごと消去機で消去する方法、ディスクを取り出して
ディスクだけデータを消去する方法、データを上書きして
いく方法、等があり、それぞれかかる時間や消去のレベル
が異なります。
CDについては、物理的に破壊する方法が最も簡単です。

【費用項目】
一時費用
ハードディスク単体費用
ノートPC全体消去費用
消去証明書費用
その他、調査の費用は別途見積

継続的費用
なし


ザ・インターネット
又は、プロバイダ
ファイアウォール
DMZ
メールサーバー
URLサーバ
サーバー

Ⅵ. メニューの説明

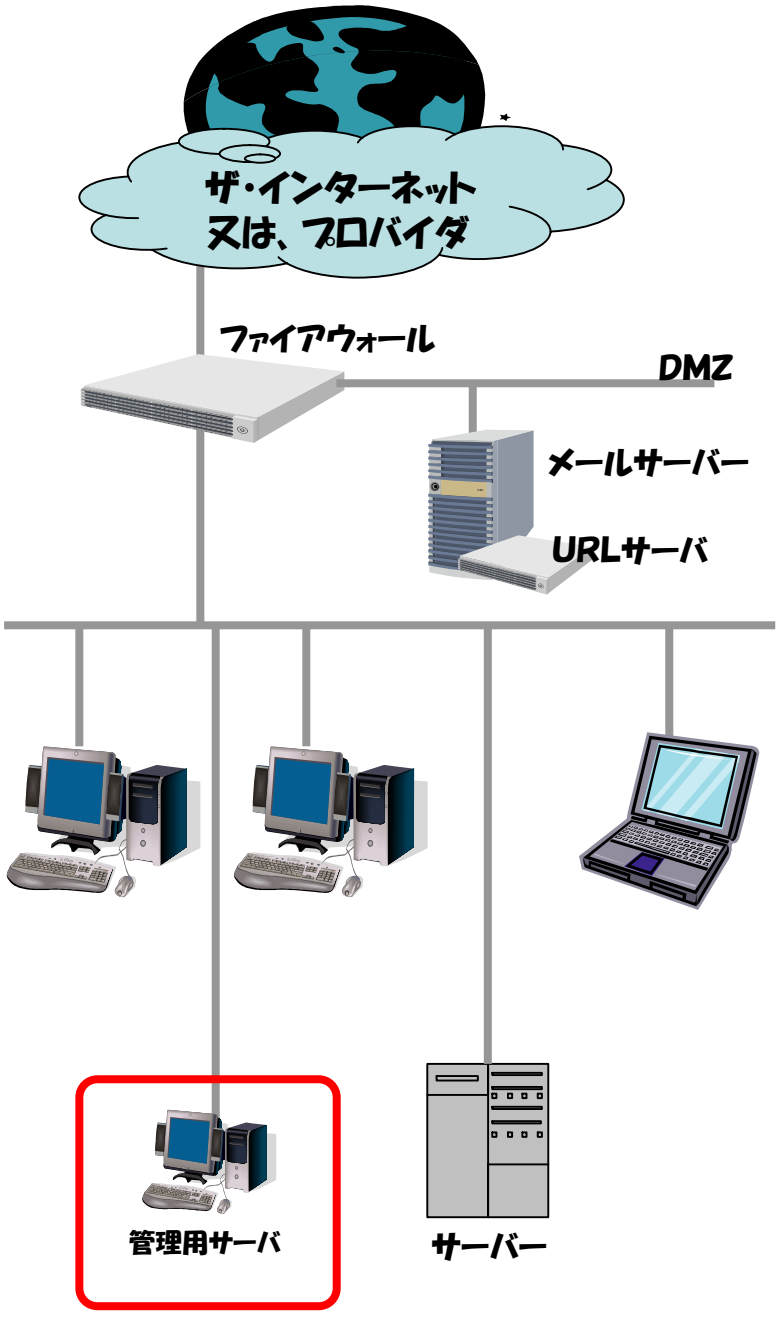
13. ファイルアクセス管理ツール

現状調査＋管理用サーバ（含むソフト）＋設置・導入
　＋動作確認
　＋メンテナンス（バージョンアップ・サポート）

【内容説明】
基本的には専用サーバにソフトをインストールし設置します。
機能アップに伴うバージョンアップや問合せサポートも
必要です。

【費用項目】
一時費用
専用管理サーバの導入費用
（既存のものを使用する場合、機能・性能仕様に注意）
ソフトのライセンス費用：マネージャー
　　クライアント
その他、調査、設置・導入・確認の費用は別途見積

継続的費用
メンテナンス費用（バージョンアップ及び設定変更等）


ザ・インターネット
又は、プロバイダ
ファイアウォール
DMZ
メールサーバー
URLサーバ
管理用サーバ
サーバー

Ⅵ. メニューの説明

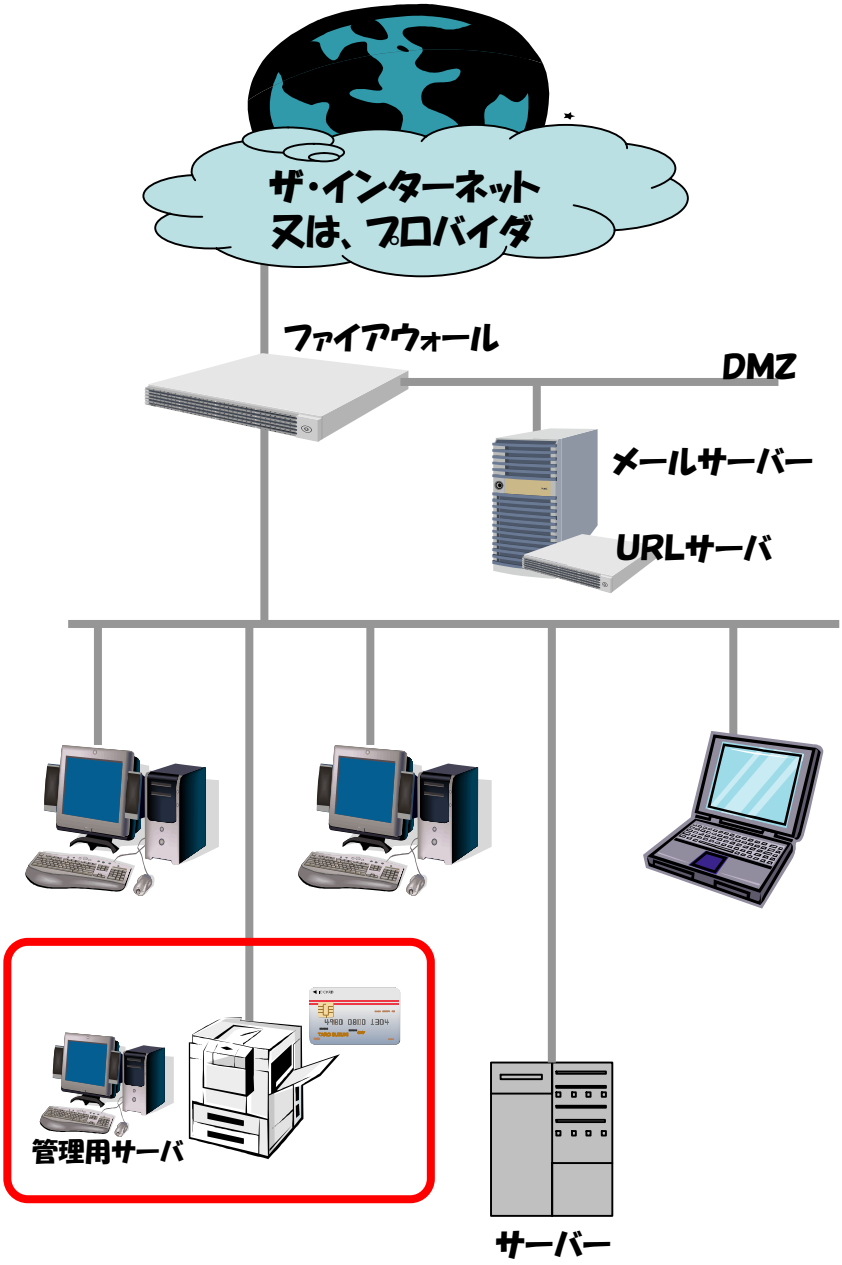
14. ファイルアクセス管理ツール(ドキュメントセキュリティ)

現状調査＋管理可能プリンタ＋サーバソフト＋設置・導入
　＋動作確認
　＋メンテナンス(プリンタ＋バージョンアップ・サポート)

【内容説明】
セキュリティ機能付のプリンタの導入と、管理用サーバソフトの導入が必要です。また、ICカードの準備も必要になります。

【費用項目】
一時費用
プリンタ費用
サーバの導入費用
(既存のものを使用する場合、機能・性能仕様に注意)
管理用ソフト費用
ICカード作成費用
その他、調査、設置・導入・確認の費用は別途見積

継続的費用
メンテナンス費用(バージョンアップ、機器保守及び設定変更等)


ザ・インターネット
又は、プロバイダ
ファイアウォール
DMZ
メールサーバー
URLサーバ
管理用サーバ
サーバー

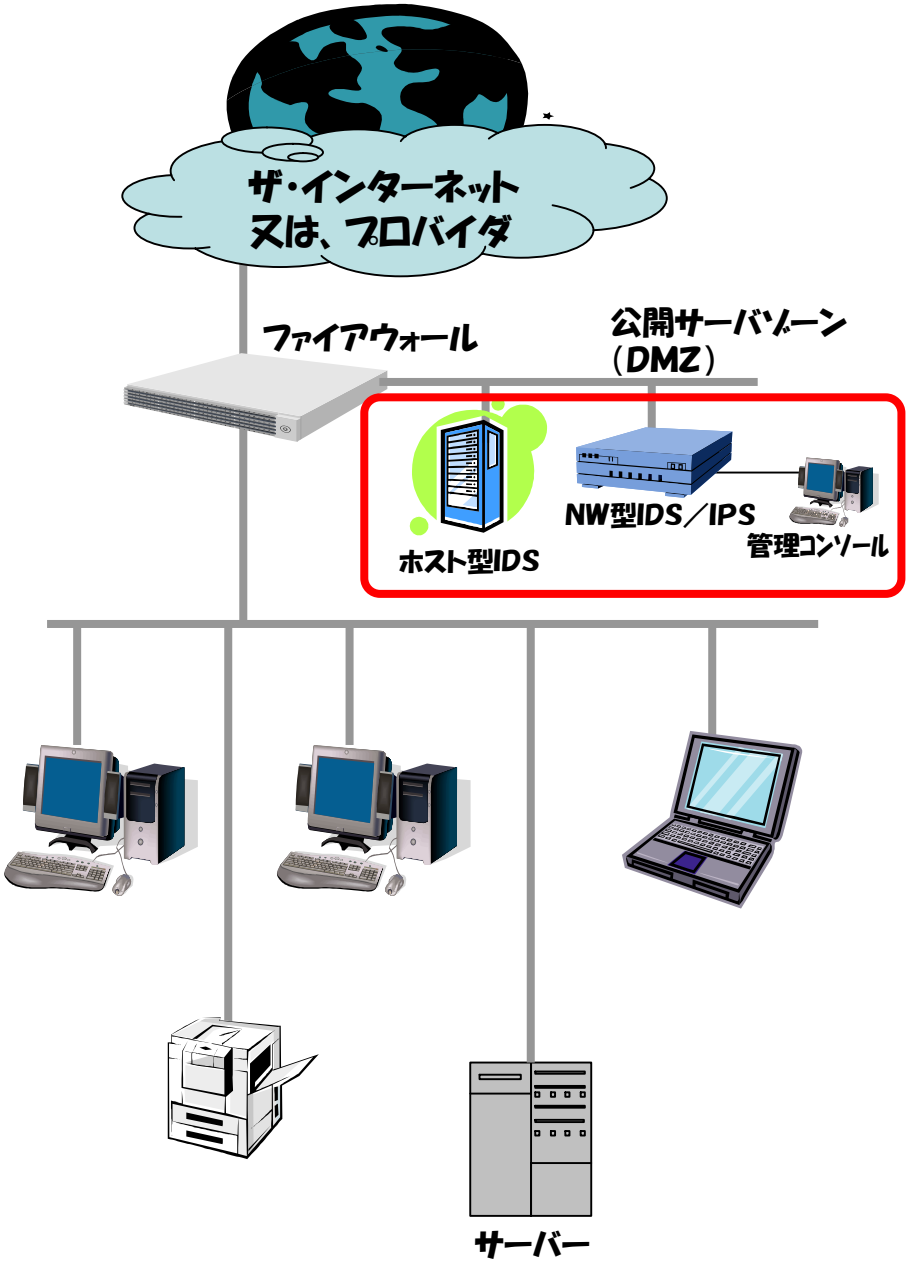
Ⅵ. メニューの説明

15. IDS･IPS構築

現状調査＋IDS又はIPS導入＋設置・設定＋動作確認
　＋メンテナンス（バージョンアップ・サポート）
【内容説明】
IDS（不正侵入検知システム）のネットワーク型（NW型）は、ネットワーク上に設置した機器で不正な通信を検知し、管理者に通報します。ホスト型IDSは、そのサーバに対する攻撃を検知します。NW型IDSはネットワーク全体を監視でき、ホスト型IDSはサーバ毎に柔軟な対応を図ることが可能です。
IPS（不正侵入防御システム）はIDSの検知機能に防御の機能を加えたもので、不正侵入があった時に自動的に防止する仕組みを持っています。
いずれもチェックしながら通信を通すので、性能的には若干の低下を考慮する必要があります。また、誤検知もあるためシステム毎に設定のチューニングを行います。

【費用項目】
一時費用
IDS導入費用
IPS導入費用
管理コンソール費用
その他、調査、設置・導入・確認の費用は別途見積

継続的費用
メンテナンス費用（バージョンアップ、機器保守及び設定変更等）


ザ・インターネット
又は、プロバイダ
ファイアウォール
公開サーバゾーン
（DMZ）
ホスト型IDS
NW型IDS／IPS
管理コンソール
サーバー

Ⅵ. メニューの説明

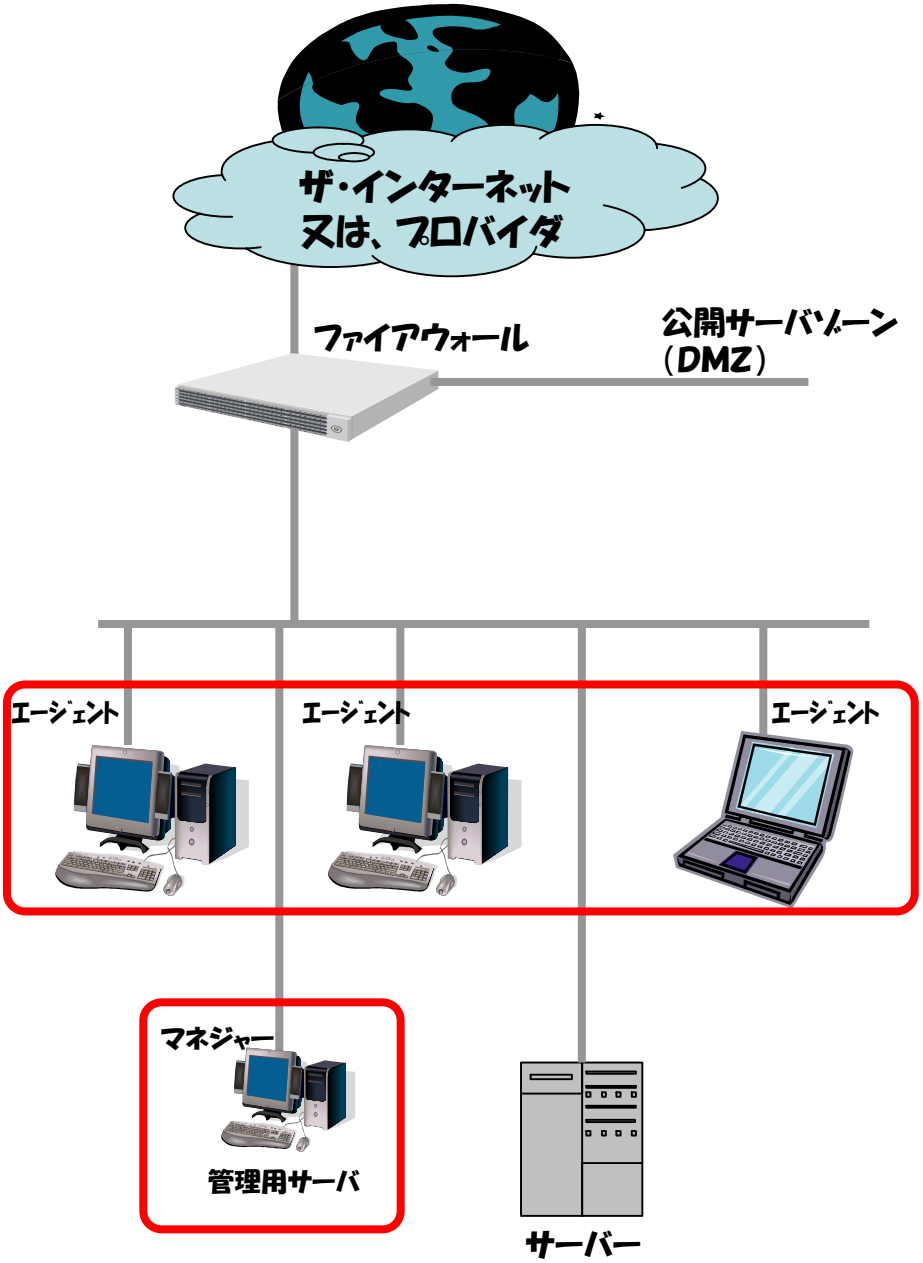
16. クライアントPC監視

現状調査＋クライアント監視ソフト＋設置・設定＋動作確認
　＋メンテナンス（バージョンアップ・サポート）

【内容説明】
クライアントPCへの不正なプログラムのインストールを監視するために、各PCに監視ソフトを導入します。これにより、従業員のPCのリアルタイム監視を行います。
また、各PCにインストールしたエージェントを管理するための、管理サーバ及びマネージャーのインストールを行います。
各PCへのエージェントインストール時には、正しく設定通りの監視を行うか動作確認を行います。

【費用項目】
一時費用
専用管理サーバの導入費用
（既存のものを使用する場合、機能・性能仕様に注意）
ソフトのライセンス費用：マネージャー
　　クライアント
その他、調査、設置・導入・確認の費用は別途見積

継続的費用
メンテナンス費用（バージョンアップ及び設定変更等）


ザ・インターネット
又は、プロバイダ
ファイアウォール
公開サーバゾーン
（DMZ）
エージェント
エージェント
エージェント
マネジャー
管理用サーバ
サーバー

Ⅵ. メニューの説明

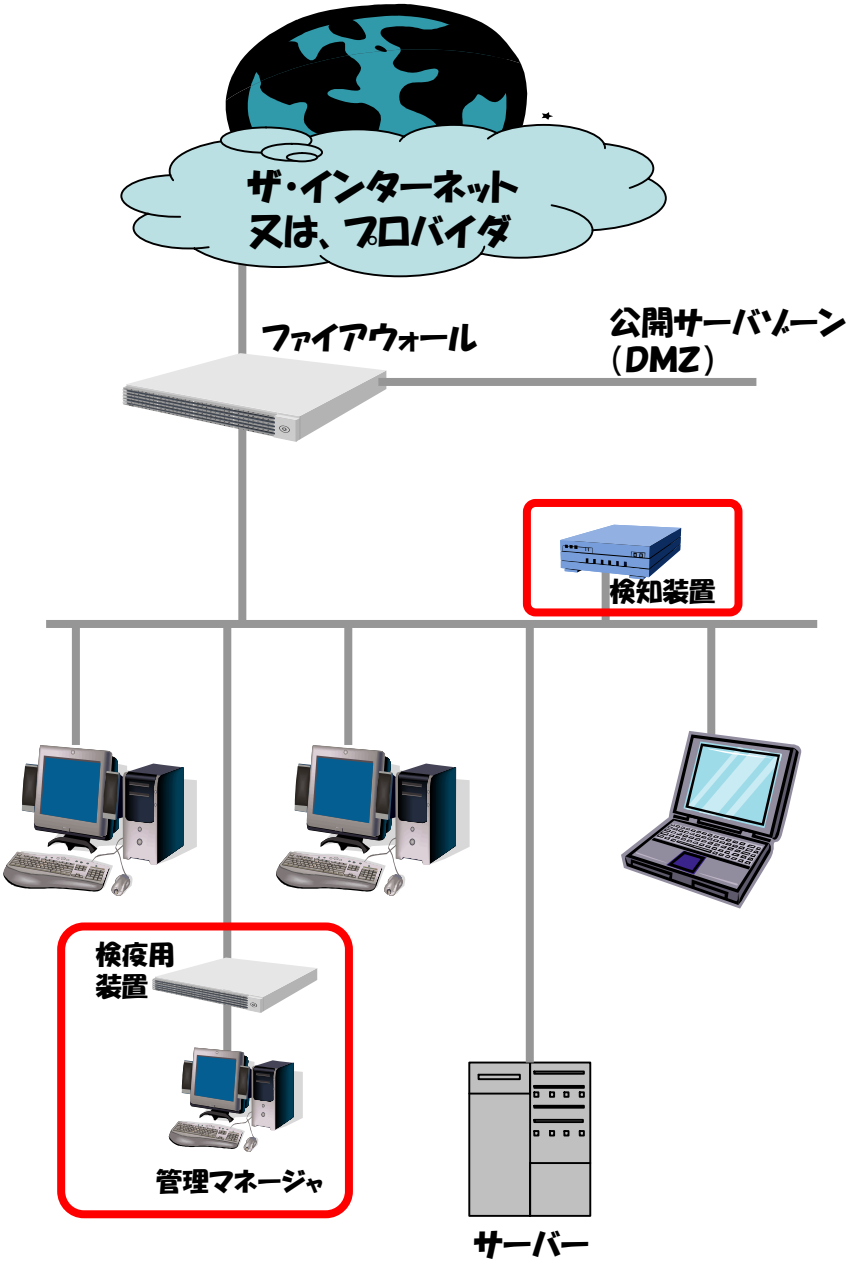
17. 検疫システム構築

現状調査＋検疫装置＋管理マネージャ＋設置・設定
　＋動作確認
　＋メンテナンス（バージョンアップ・サポート）

【内容説明】
クライアントPCのIPアドレスとMACアドレスをチェックすることで登録されていないPCがネットワークに接続された場合にアラームをあげる、簡易型検疫装置から、セキュリティパッチ等の未適用を検出してアラームをあげる検疫システムまで様々な種類があります。
導入に当たっては、ネットワーク構成の調査を行う必要があります。また、クライアントPC側での設定変更が必要な場合もあります。

【費用項目】
一時費用
簡易型検疫装置費用
検知装置費用
検疫用装置費用
管理マネージャソフト費用
その他、調査、設置・導入・確認の費用は別途見積

継続的費用
メンテナンス費用（バージョンアップ、機器保守及び設定変更等）


ザ・インターネット
又は、プロバイダ
ファイアウォール
公開サーバゾーン
（DMZ）
検知装置
検疫用
装置
管理マネージャ
サーバー

VI. メニューの説明

18. 無線LAN暗号化

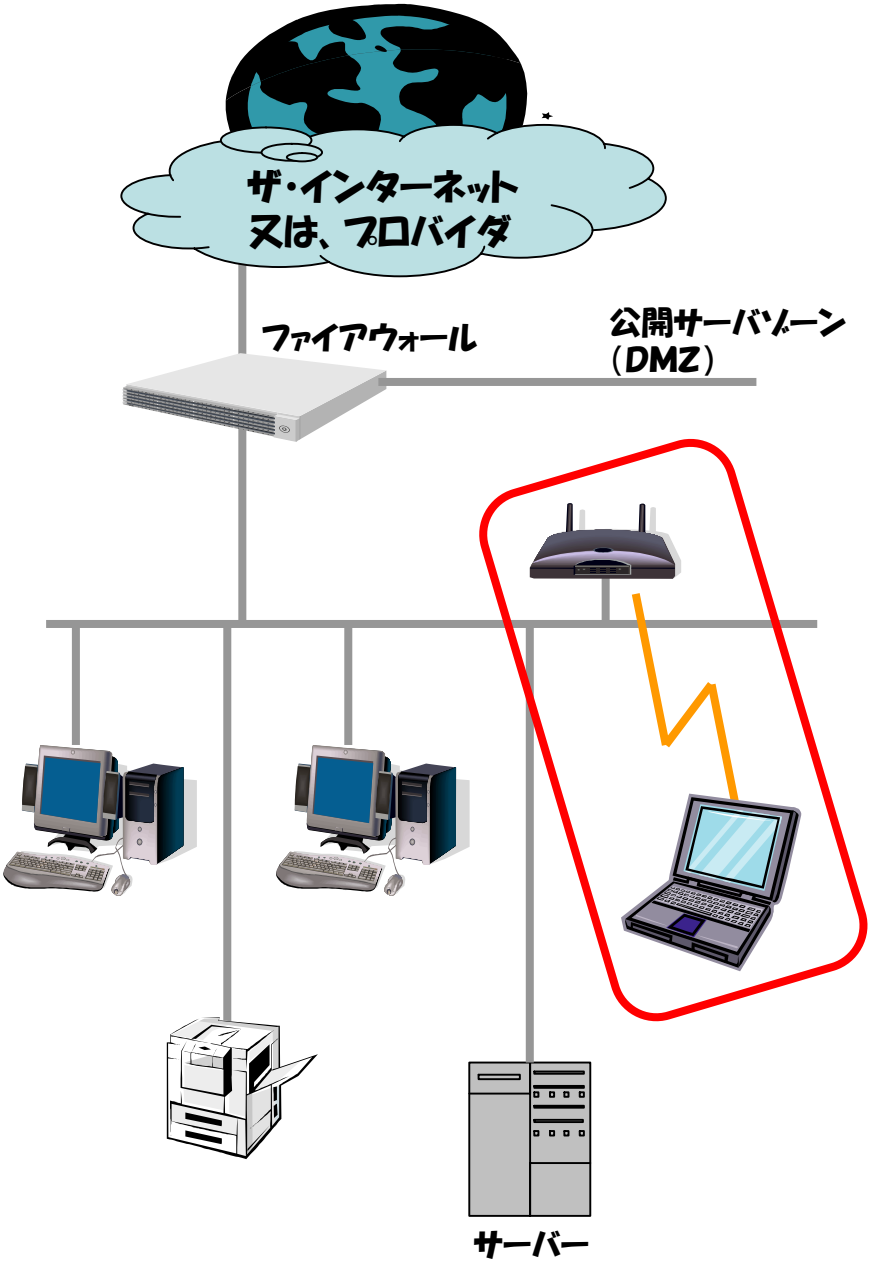
現状調査＋無線ルータ＋設置・設定＋動作確認
　＋メンテナンス（バージョンアップ・サポート）

【内容説明】
無線ルータには通常、暗号化機能が組み込まれています。
規定値は無効になっていることが多いので、必ず設定を行う必要があります。
事務所が大きく、複数の無線ルータ（アクセスポイント）が必要な場合は電波干渉で、通信が出来なくなる場合もありますので、無線シミュレーションにより電波環境の調査を行うことをお勧めします。

【費用項目】
一時費用
無線ルータ（アクセスポイント）費用
その他、調査、設置・導入・確認の費用は別途見積

継続的費用
メンテナンス費用（バージョンアップ、機器保守及び設定変更等）

【参考】
無線シミュレーションを行う場合は別途費用が掛かります


ザ・インターネット
又は、プロバイダ
ファイアウォール
公開サーバゾーン
（DMZ）
サーバー

VI. メニューの説明

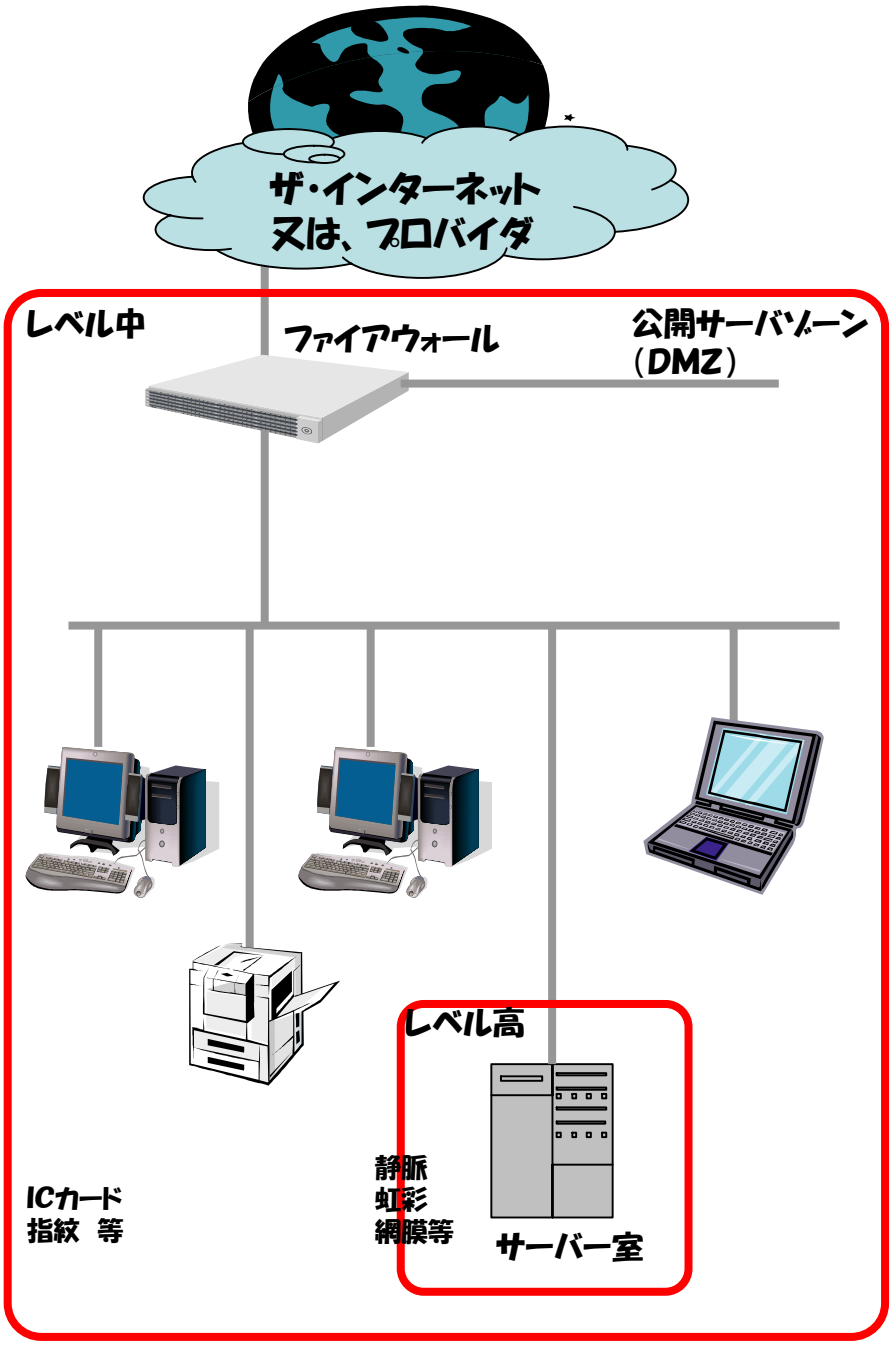
19. ユーザ認証強化対策

現状調査＋各種認証装置＋設置工事・設定＋動作確認
　＋メンテナンス（バージョンアップ・サポート）

【内容説明】
認証の強化対策としてICカードの他に、指紋、静脈、顔、網膜、虹彩等の認証方法があります。
サーバ室等重要な情報のある部屋への入出には、高度な認証方式や、複数の認証を組み合わせる方法があります。
クライアントについても、IDパスワードでのユーザ認証に変えて、ICカードや指紋にて行うことも可能です。
サーバ室等への認証装置等の設置は工事を伴いますので、テナントビルの場合には管理会社の了解を得る等の注意が必要です。

【費用項目】
一時費用
各種認証装置費用
工事費用：建物の状況・構造で異なりますので、業者との相談が必要です
その他、調査、設置・導入・確認の費用は別途見積

継続的費用
メンテナンス費用（バージョンアップ、機器保守及び設定変更等）


ザ・インターネット
又は、プロバイダ
レベル中
ファイアウォール
公開サーバゾーン
（DMZ）
レベル高
静脈
虹彩
網膜等
サーバー室
ICカード
指紋　等

Ⅵ. メニューの説明

20. PC不正操作対策

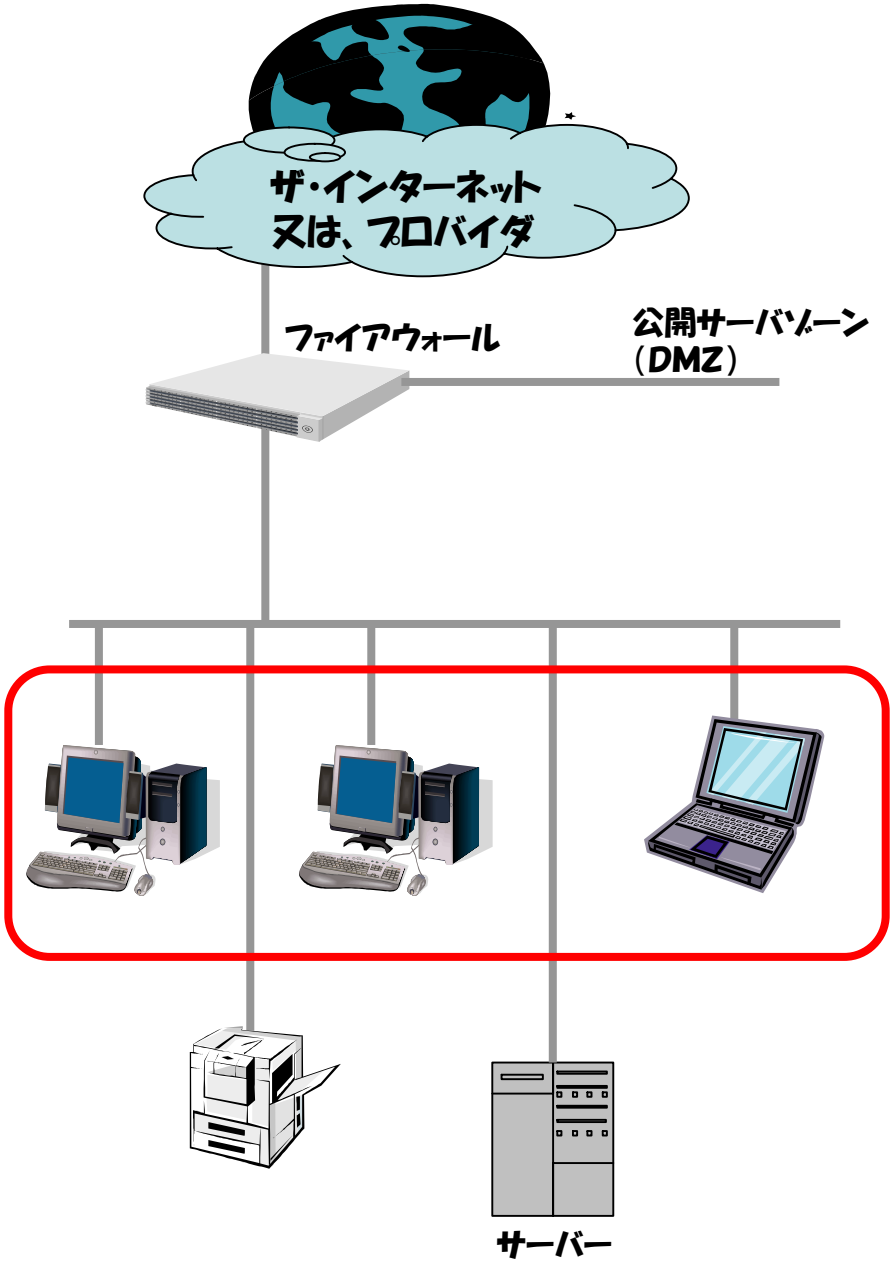
現状調査＋不正操作防止ソフト導入＋設定＋動作確認
　＋メンテナンス（バージョンアップ・サポート）

【内容説明】
USBメモリなど外部媒体への出力を制限したり、印刷を制限したりする不正操作防止ソフトをインストールします。
制御する内容をユーザ・グループ単位で変えたり、または組織ごとに変えることが可能です。
管理サーバによる集中管理を行えるソフトウェアもあります。

【費用項目】
一時費用
防止ソフト費用
（導入対象PCが動作条件を満たしているか要確認）
管理用サーバ機費用
管理サーバソフト費用

その他、調査、設置・導入・確認の費用は別途見積

継続的費用
メンテナンス費用（バージョンアップ及び設定変更等）


ザ・インターネット
又は、プロバイダ
ファイアウォール
公開サーバゾーン
（DMZ）
サーバー

VI. メニューの説明

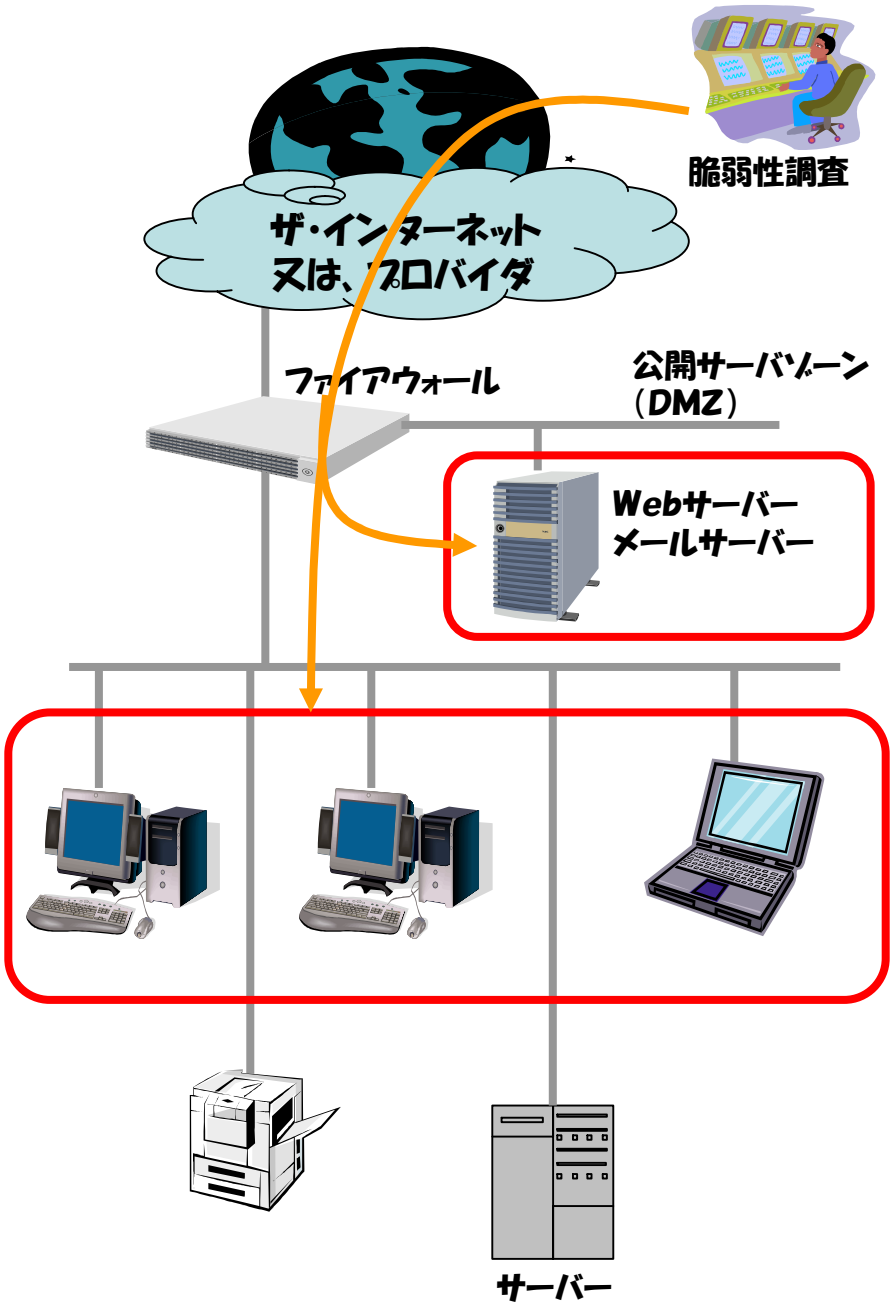
21. 情報セキュリティ評価・診断サービス

現状調査＋外部からの情報セキュリティ診断
　＋状況報告

【内容説明】
外部から診断の為の擬似アタックをかけ、Webサーバやメールサーバなどに脆弱性が開いていないか、セキュリティ対策用のパッチ適用が正しく行われているか、などのセキュリティ状況を調べます。
調査結果は、一般的な対策手法と合わせて報告書として纏め・提出します。

【費用項目】
一時費用
診断費用：スポット診断費用
　　定期診断費用
　　（診断対象の装置・台数によって変わります）
その他、調査、設置・導入・確認の費用は別途見積

継続的費用
定期診断実施の場合はその費用


脆弱性調査
ザ・インターネット
又は、プロバイダ
ファイアウォール
公開サーバゾーン
（DMZ）
Webサーバー
メールサーバー
サーバー

Ⅵ. メニューの説明

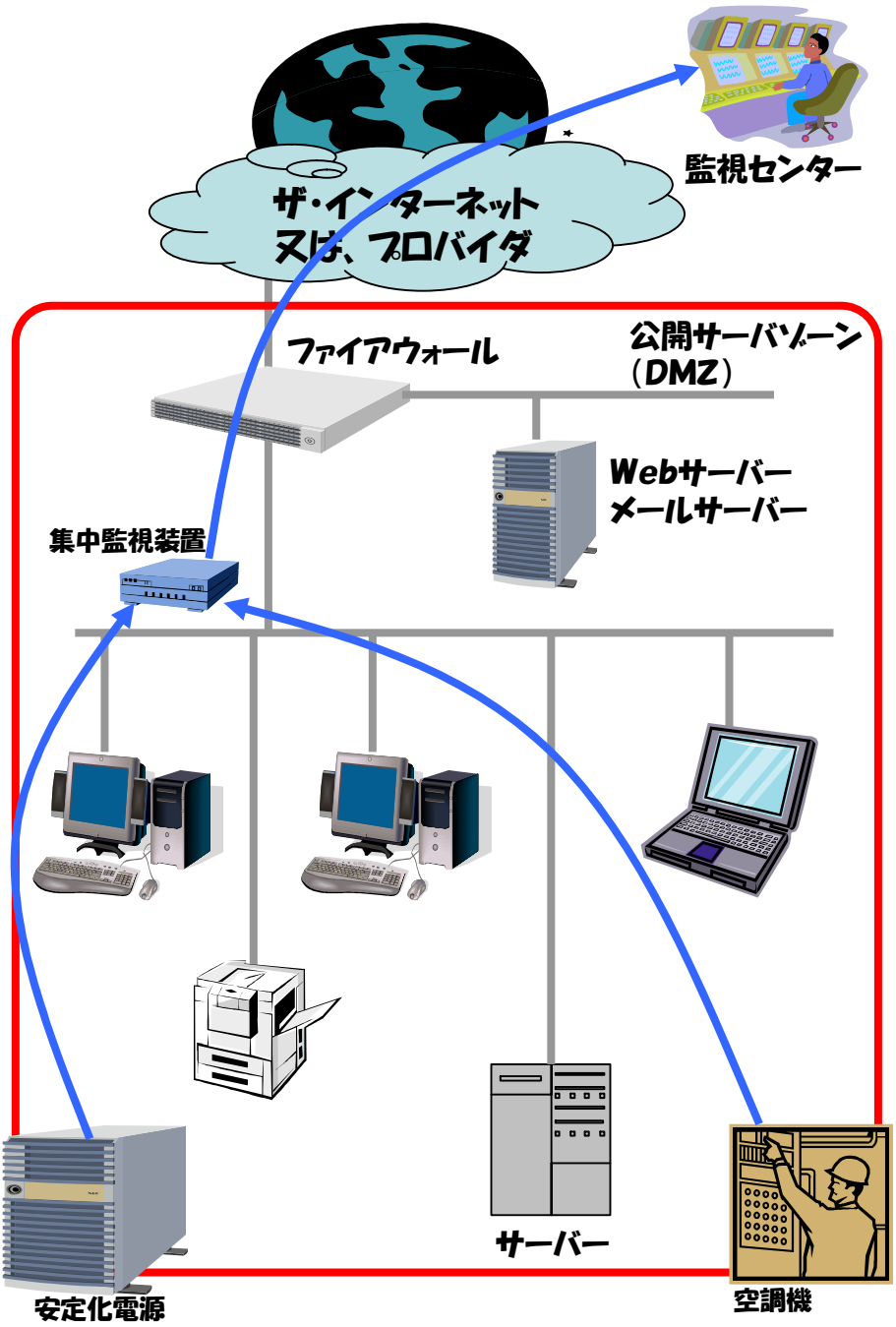
22. 付帯設備監視

現状調査＋集中監視装置＋設置・調整＋動作確認
　＋メンテナンス（バージョンアップ・サポート）

【内容説明】
電源・空調機の状況を監視し、異常があれば、早めに対処することで、社内ITシステムの稼動を継続させます。
地方拠点等、複数拠点を集中的に管理する場合に有効です。
監視センターにて24H365日の監視を行い、障害発生時には電子メール、携帯メールなどで管理者に通知します。

【費用項目】
一時費用
集中監視装置費用
その他、調査、設置・導入・確認の費用は別途見積

継続的費用
24H365日監視費用


監視センター
ザ・インターネット
又は、プロバイダ
ファイアウォール
公開サーバゾーン
（DMZ）
Webサーバー
メールサーバー
集中監視装置
サーバー
安定化電源
空調機

Ⅵ. メニューの説明

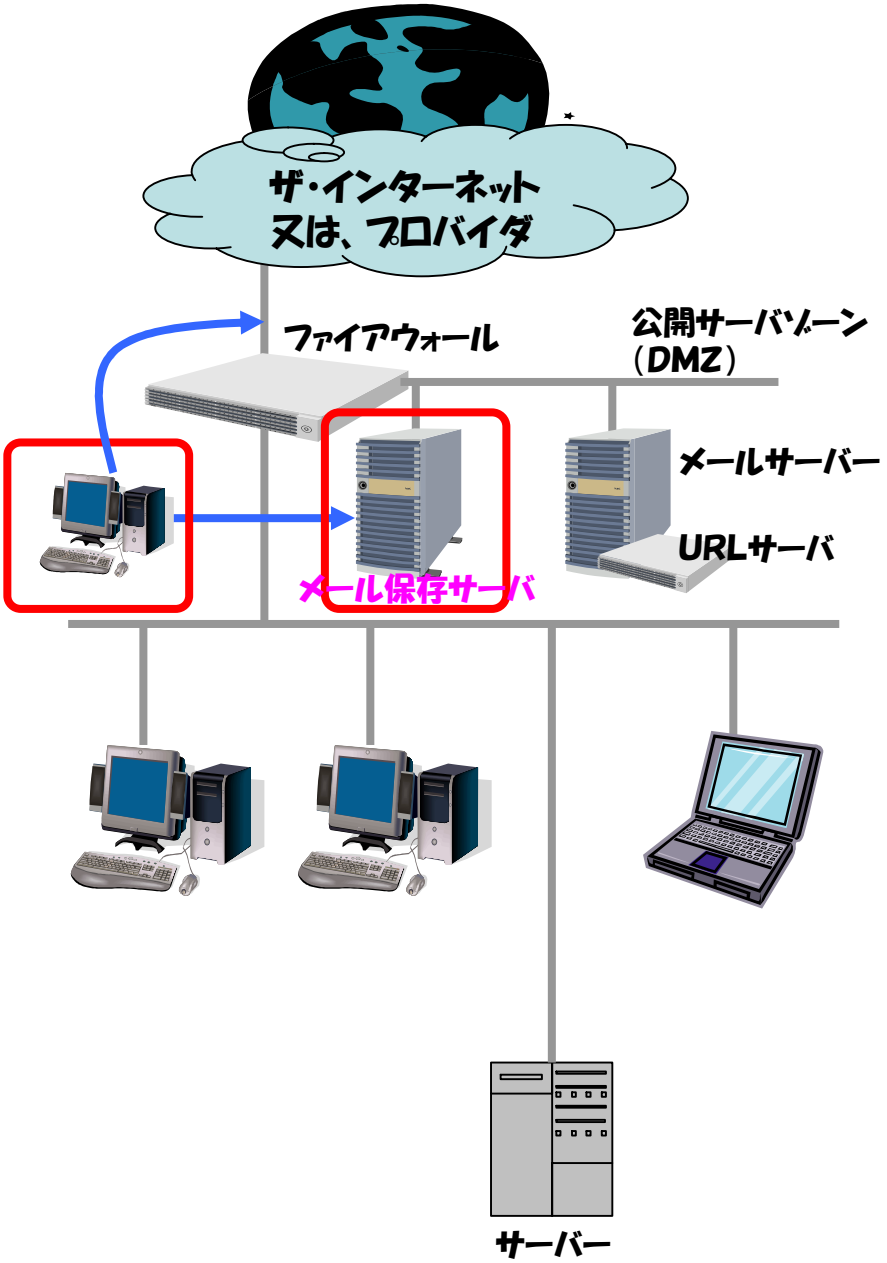
23. ログ収集・解析（メール証跡保存対策）

現状調査＋管理用ソフト＋設置・導入＋動作確認
　＋メンテナンス（リビジョンアップ・サポート）

【内容説明】
クライアント上でメールを複製するタイプと、サーバ上で
複製するタイプがあります。価格・機能が異なりますので、
導入にあたっては十分な検討が必要です。
収集したログは管理者が検索することが可能です。
添付ファイルを含めて全文を保存する場合、メールの
容量が膨大になる可能性があるため、既存のサーバを
使用する場合はバックアップ装置のあるものを使用する
必要があります。

【費用項目】
一時費用
クライアント型ソフト費用
サーバ機費用
サーバ型ソフト費用
（既存のものを使用する場合、機能・性能仕様に注意）
その他、調査、設置・導入・確認の費用は別途見積

継続的費用
メンテナンス費用（バージョンアップ、機器保守及び設定
変更等）


ザ・インターネット
又は、プロバイダ
ファイアウォール
公開サーバゾーン
（DMZ）
メールサーバー
URLサーバ
メール保存サーバ
サーバー

VI. メニューの説明

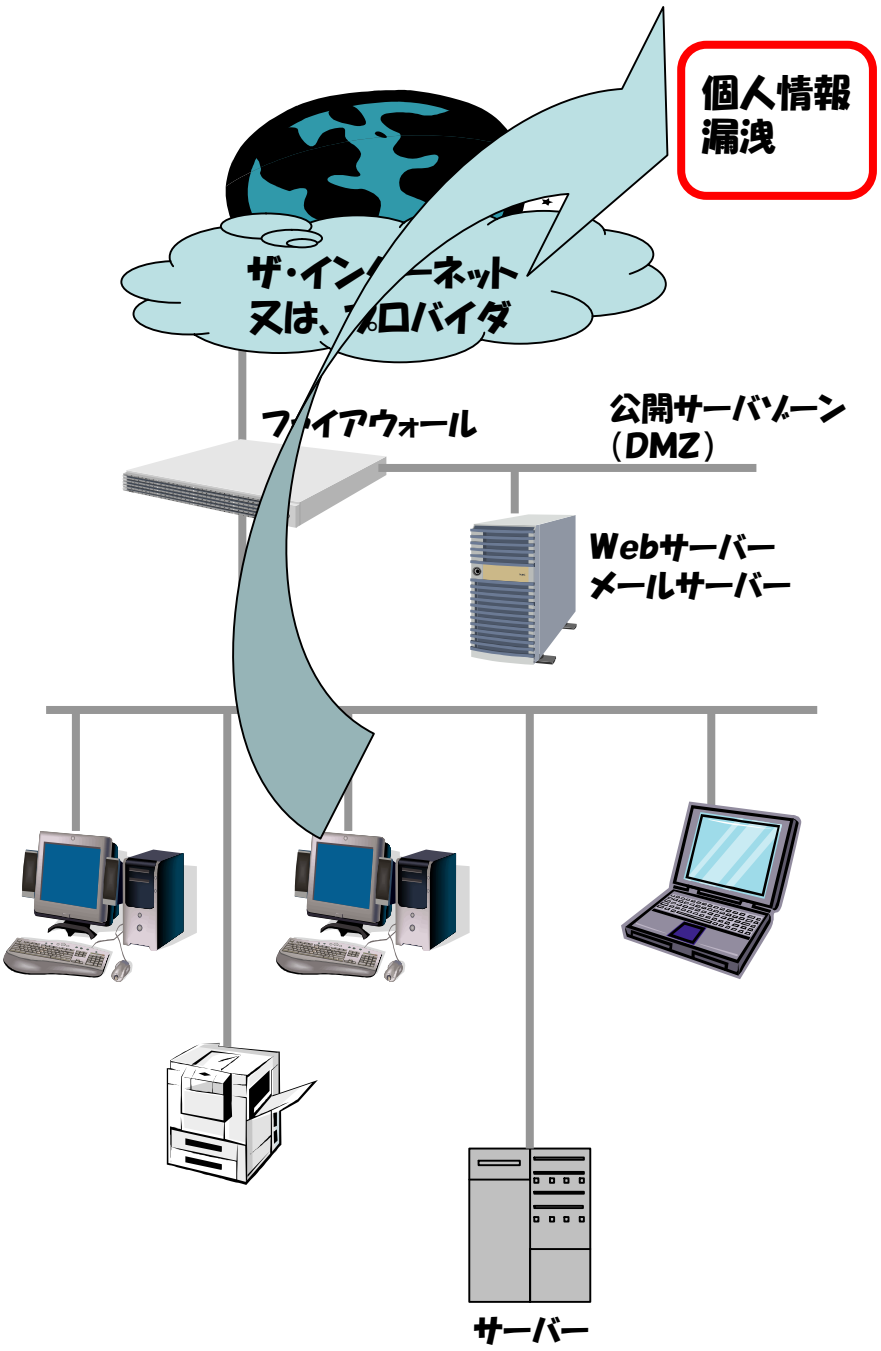
24. 個人情報取扱事業者保険

現状調査＋保険対象の整理

【内容説明】
個人情報が漏洩した場合、補償内容に応じて保険金が
支払われます。
主な支払い対象は以下の通りです。
・危機管理コンサルティング費用補償
　被害者対応やメディア対応に関するアドバイスのご提供
・危機管理実行費用補償
　謝罪文作成、事故原因調査費用等、対応に必要な費用
　を補償
・損害賠償金及び争訟費用補償
　損害賠償請求を受けた場合の賠償金や訴訟にかかる
　弁護士費用等を補償

【費用項目】
一時費用
調査費

継続的費用
業種・売上金額及び申告書の内容により異なる
情報通信関連：年間売上額によっても異なる


個人情報
漏洩
ザ・インターネット
又は、グローバイダ
ファイアウォール
公開サーバゾーン
（DMZ）
Webサーバー
メールサーバー
サーバー

VI. メニューの説明

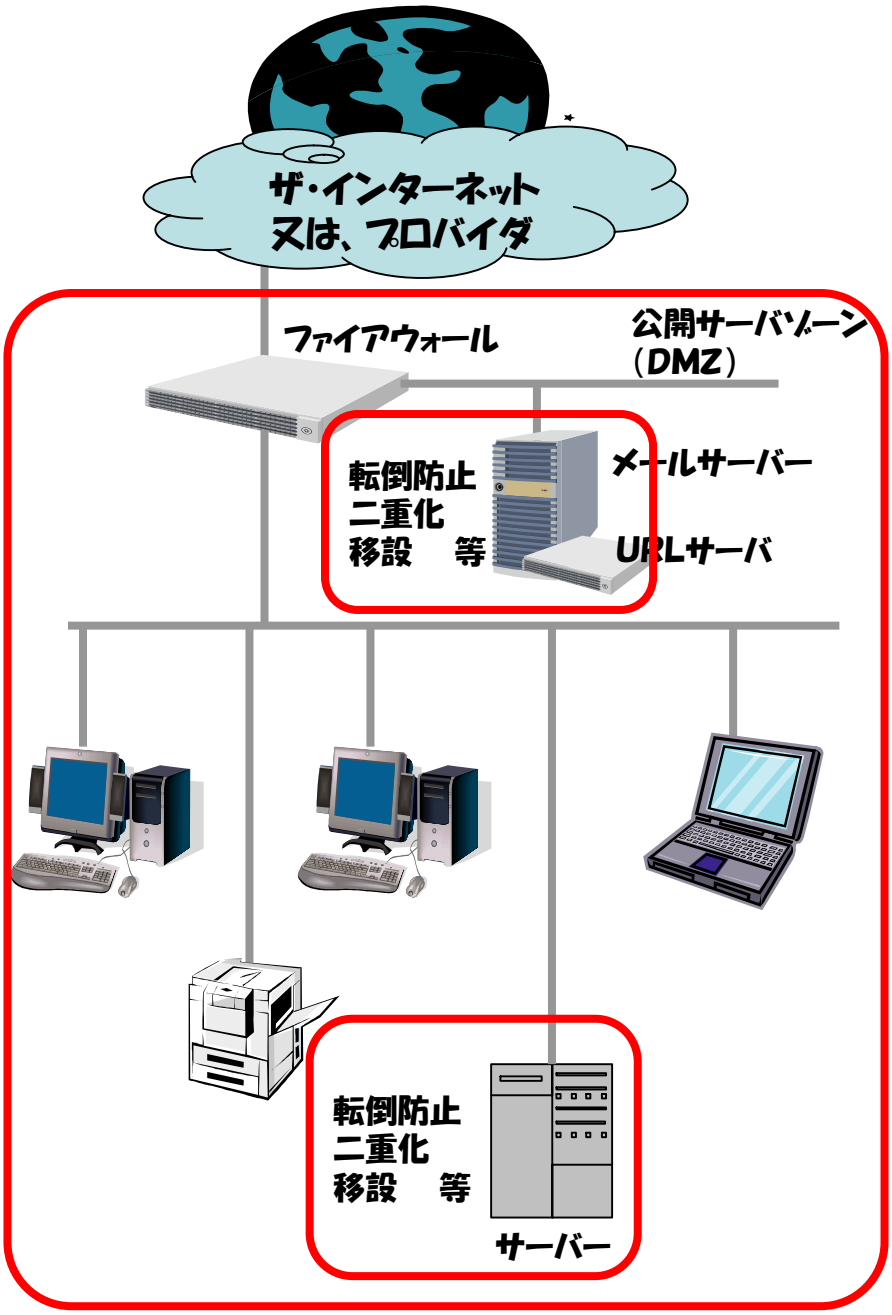
25. 自然災害時のデータバックアップ対策

現状調査＋各種対策＋設置・導入＋動作確認（移設時）
　＋メンテナンス（サポート）

【内容説明】
対策には、転倒防止対策、重要情報の二重化（バックアップ）、浸水に遭わない場所への設置（移設）等がありますが、現状の状況によって対策がそれぞれ異なります。
また、自然災害への対策が完備されているデータセンターを利用する方法もあります。
具体的な対策については、販売店、又はベンダーとご相談下さい。

【費用項目】
一時費用
各種対策費：転倒防止具費用
　　データの二重化費用
　　既存サーバの移設費用
　　対策のコンサルティング費用
（環境により費用が異なります。詳細については販売店・ベンダーにご確認下さい。
その他、調査、設置・導入・確認の費用は別途見積

継続的費用
なし


ザ・インターネット
又は、プロバイダ
ファイアウォール
公開サーバゾーン
（DMZ）
転倒防止
二重化
移設　等
メールサーバー
URLサーバ
転倒防止
二重化
移設　等
サーバー

Ⅵ. メニューの説明

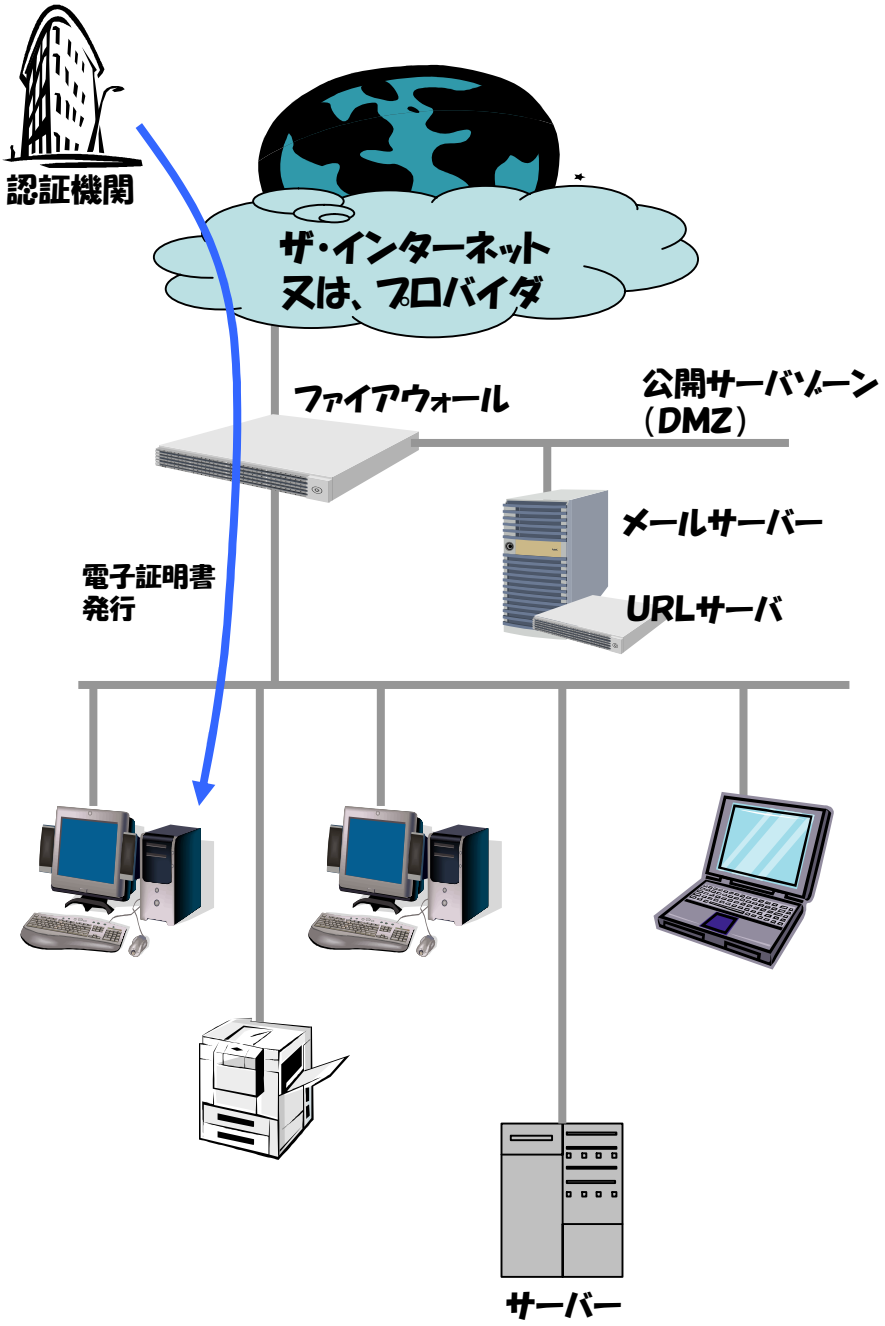
26. 電子認証構築

現状調査＋認証機関への申請＋対応ソフト導入＋設定
　＋動作確認
　＋メンテナンス（リビジョンアップ・サポート）

【内容説明】
認証の仕組みを取り込むために認証用のソフトの導入と
認証機関への証明発行の依頼の手続きが必要です。

【費用項目】
一時費用
対応ソフト導入費用
その他、調査、設置・導入・確認の費用は別途見積

継続的費用
電子証明書発行継続費用


認証機関
ザ・インターネット
又は、プロバイダ
ファイアウォール
公開サーバゾーン
（DMZ）
メールサーバー
URLサーバ
電子証明書
発行
サーバー

Ⅵ. メニューの説明

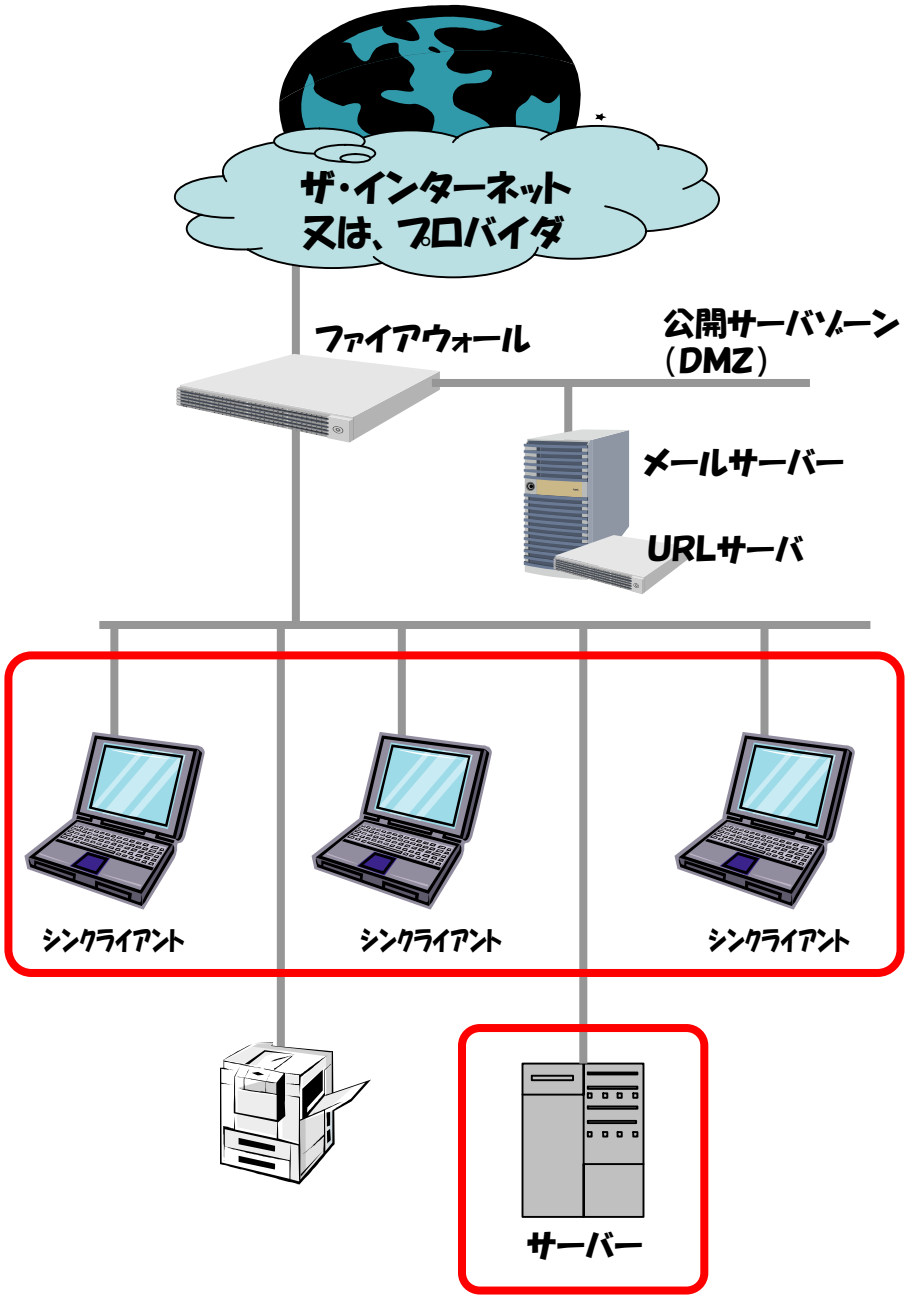
27. シンクライアント構築

現状調査＋シンクライアント設置＋対応ソフト導入＋設定
　＋動作確認
　＋メンテナンス（バージョンアップ・サポート）

【内容説明】
シンクライアントへの置き換えと、サーバの負荷が大きくなるため、状況によってはサーバーの増設又は置き換えも必要になります。

【費用項目】
一時費用
シンクライアント導入費用
対応ソフト費用
その他、調査、設置・導入・確認の費用は別途見積

継続的費用
メンテナンス費用（バージョンアップ、機器保守及び設定変更等）


ザ・インターネット
又は、プロバイダ
ファイアウォール
公開サーバゾーン
（DMZ）
メールサーバー
URLサーバ
シンクライアント
シンクライアント
シンクライアント
サーバー

Ⅵ. メニューの説明

28. システム二重化対策／ASPホスティング

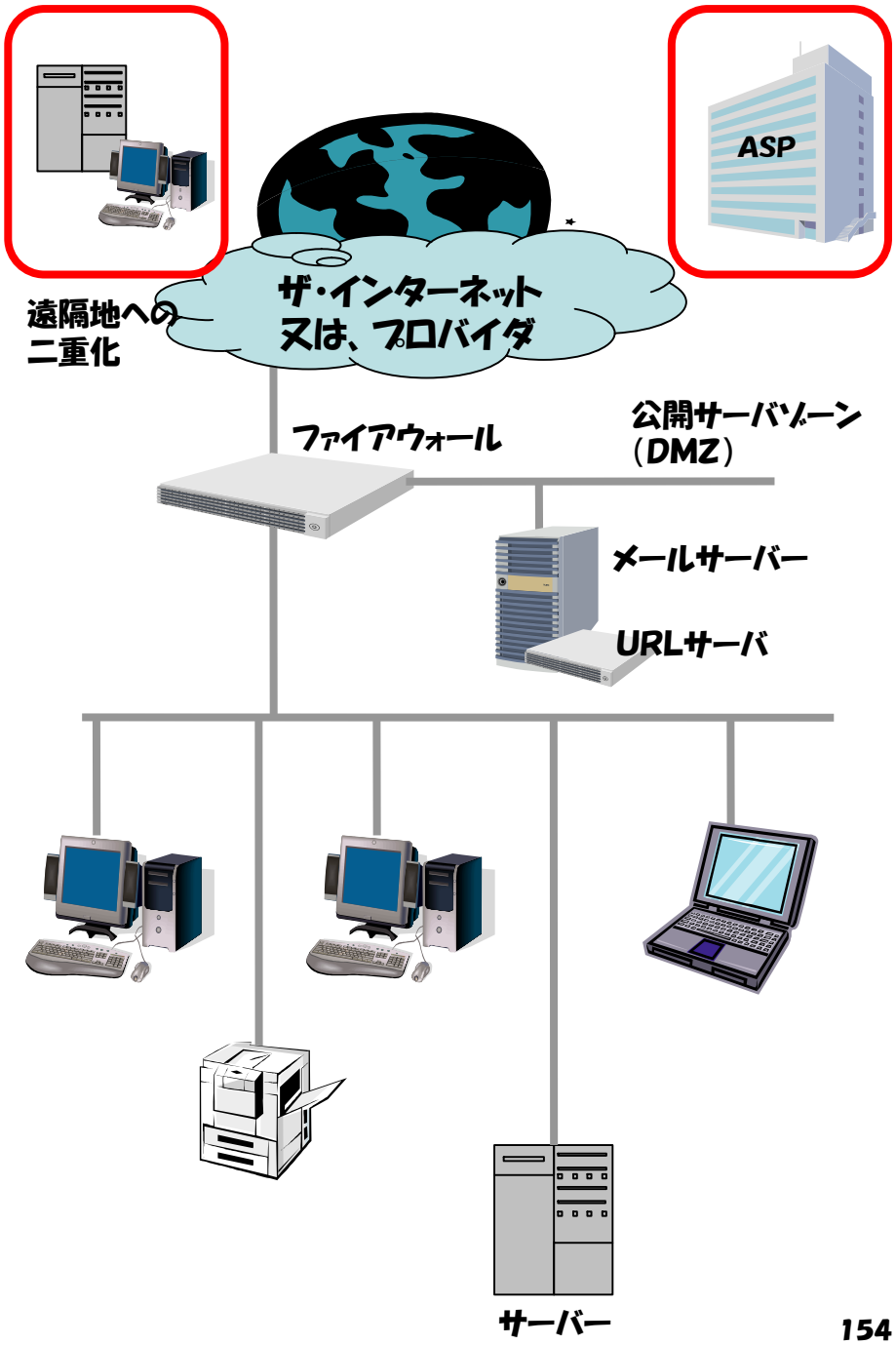
現状調査＋必要な機器の選定（・導入）＋対応ソフト導入
　＋設定＋動作確認
　＋メンテナンス（リビジョンアップ・サポート）

【内容説明】
必要なシステム又はデータの遠隔地への二重化を行うか
機能の代替をさせるためのホスティング契約を行います。

【費用項目】
一時費用
二重化の場合：必要なシステム又は機器費
対応ソフト費用
その他、調査、設置・導入・確認の費用は別途見積

継続的費用
二重化の場合の遠隔地システムの維持費用
回線費用

ASPとの契約維持費用
回線費用


ASP
ザ・インターネット
又は、プロバイダ
遠隔地への
二重化
ファイアウォール
公開サーバゾーン
（DMZ）
メールサーバー
URLサーバ
サーバー

154

VI. メニューの説明

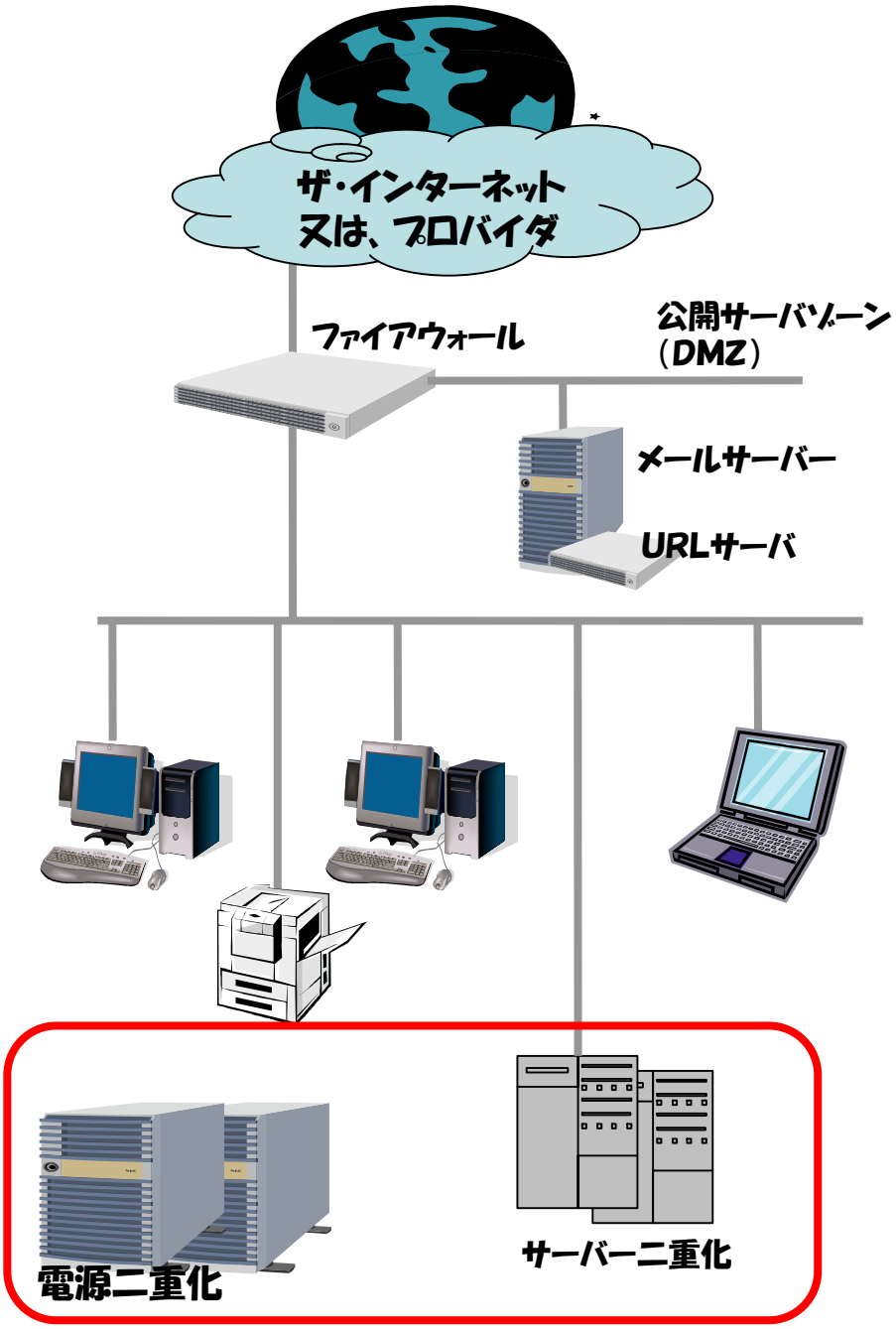
29. システム冗長化

現状調査＋冗長化機器の選定・導入＋対応ソフト導入
　＋設定＋動作確認（評価試験）
　＋メンテナンス（バージョンアップ・サポート）

【内容説明】
重要な装置・電源等の二重化を行うことで、故障時の事業継続を図ります。二重化に対応できるソフトの導入とデータの二重化も必要。アプリケーションなどの切り替え時の動作評価は必須。

【費用項目】
一時費用
二重化機器費用
対応ソフト費用
その他、調査、設置・導入・確認の費用は別途見積

継続的費用
メンテナンス費用（バージョンアップ、機器保守及び設定変更等）


ザ・インターネット
又は、プロバイダ
ファイアウォール
公開サーバゾーン
（DMZ）
メールサーバー
URLサーバ
電源二重化
サーバー二重化

VI. メニューの説明

30. 情報セキュリティポリシ策定

現状調査＋セキュリティポリシー策定支援

【内容説明】
お客様の情報セキュリティポリシー策定のお手伝いをします。また見直しが必要になったときのアドバイスを行います。

【費用項目】
一時費用
策定支援費用：策定モデル文書の提供費用

継続的費用
定期的見直し費用

Ⅵ. メニューの説明

31. ISMS認証取得支援

現状調査＋ISMS人称取得支援

【内容説明】
お客様のISMS認証取得のお手伝いをします。また見直しが必要になったときのアドバイスを行います。

【費用項目】
一時費用
策定コンサルティング費用
（内容により個別見積もり）

継続的費用
定期的見直し費用（個別見積もり）

Ⅶ

導入事例と費用例

ここでは、具体的な構成に対して、セキュリティ対策の費用がどのくらい必要なのかの事例の基本的なものを掲載しました。

セキュリティ対策の構成や費用は、既存のシステム構成や、何を守るのか・何から守るのか・誰が守るのか、そしてそれをどう実現するのか、の考え方によって異なってきます。

また、セキュリティ対策は、これで100%という事はありません。新手のウィルスや未知のセキュリティホールへの対応を継続的に行う為には日々の運用をしっかりと行うことが重要です。

お客様のシステムへの具体的なセキュリティ対策については、ベンダー又は販売店にご相談下さい。

1. システム構築事例ー1（小規模システムー1）
（不正アクセス・ウィルス・スパイウェア対策）
2. システム構築事例ー2（小規模システムー2）
（メール・WEB導入）
3. システム構築事例ー3（小規模システムー3）
（メール・WEBサーバを自前で構築）
4. システム構築事例ー4 （中規模システムー1）
（不正アクセス・ウィルス・スパイウェア対策）

5. システム構築事例ー5
（メールフィルタ・URLフィルタ）
6. システム構築事例ー6
（ノートPC対策）
7. システム構築事例ー7
（無線LAN構築）
8. システム構築事例ー8
（情報セキュリティ教育）

システム構築事例ー1（小規模システムー1）
（不正アクセス・ウィルス・スパイウェア対策）

ー始めてインターネットに接続し、ウィルス対策・不正アクセス対策・スパイウェア対策を導入した場合ー

既存システム

・クライアント30台
・Windowsサーバ1台
・ネットワークプリンタ1台

新規要件

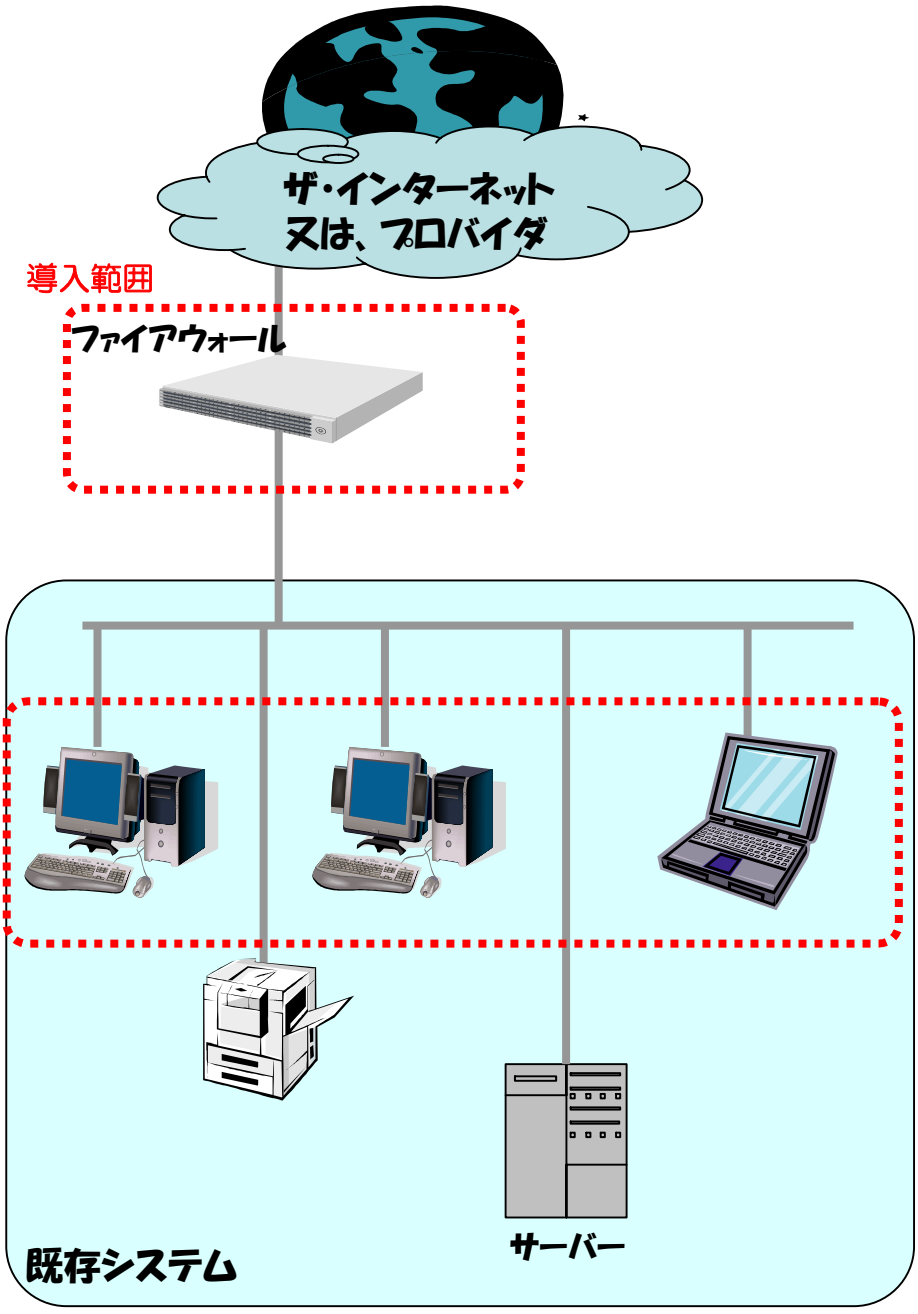
・不正アクセス対策
・ウィルス・スパイウェア対策
・インターネット接続

一時費用

事前調査費：全体の見積もりに含まれる場合が多い
ファイアウォール（装置・設計・設置費）：66万円～
ウィルス対策ソフト（クライアント用）：24万円～
ウィルス対策ソフト導入費用：9．2万円～

継続的費用

ファイアウォール維持保守：4万円～／月
ファイアウォール運用サービス（ハートウェアレンタル込み）
：1．8万円～／月
ウイルス対策維持費（更新料）：13．2万円～／年
ウイルス監視サービス：2．6万円～／年
インターネット接続維持費：50万円～／年


ザ・インターネット
又は、プロバイダ
導入範囲
ファイアウォール
既存システム
サーバー

システム構築事例ー2（小規模システムー2）
（メール・WEB導入）

ーメール及びWebをプロバイダ設備で構築ー

既存システム

・クライアント30台
・Windowsサーバ1台
・ネットワークプリンタ1台
・ファイアウォール・ウィルス対策は実施済み

新規要件

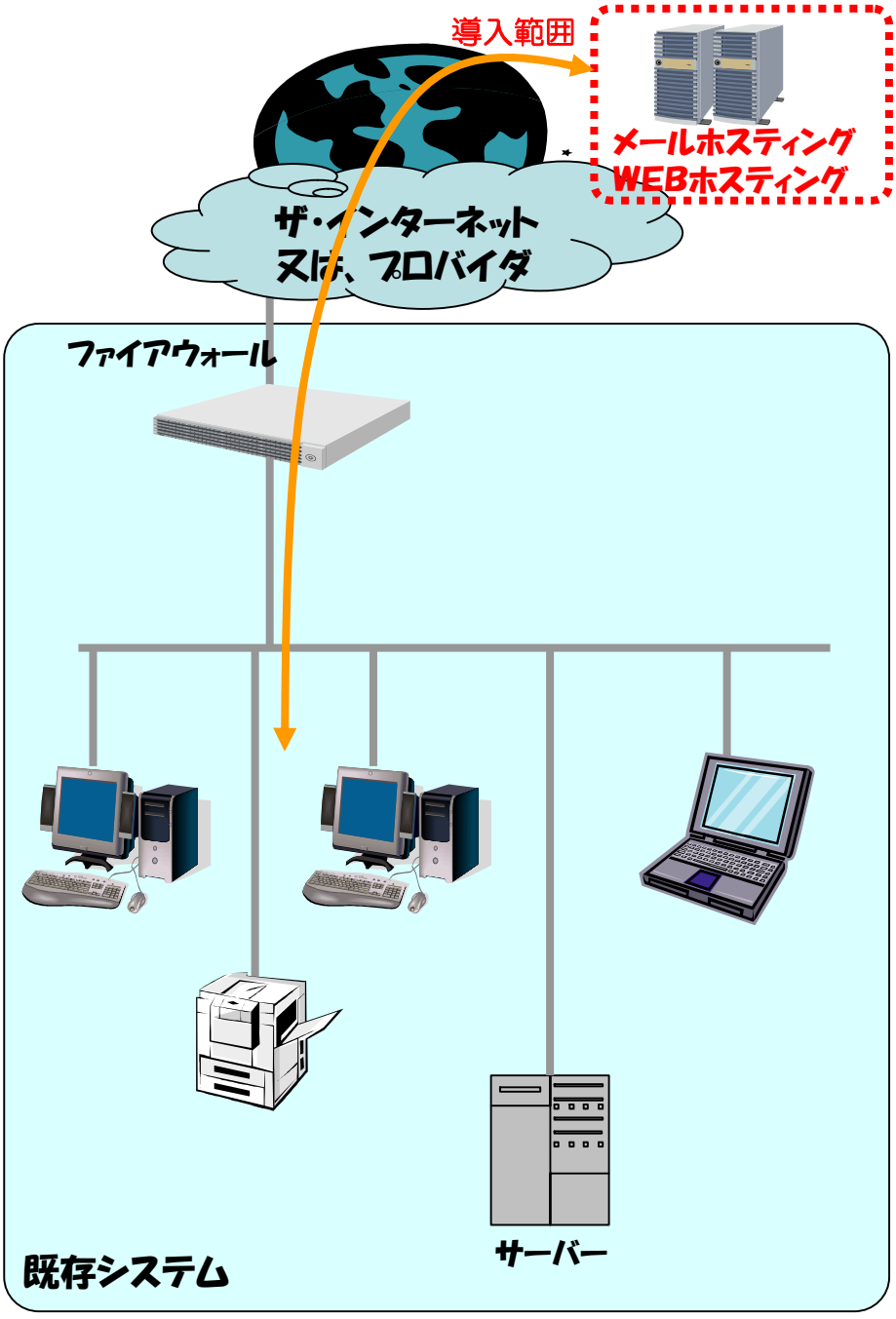
・メールホスティング
・WEBホスティング

一時費用

・事前調査費：全体の見積もりに含まれる場合が多い
・メールホスティング構築費：5万円～
・WEBホスティング構築費：3万円～

継続的費用

・ホスティング維持費： 50万円～／年


導入範囲
メールホスティング
WEBホスティング
ザ・インターネット
又は、プロバイダ
ファイアウォール
サーバー
既存システム

システム構築事例ー3（小規模システムー3）
（メール・WEBサーバを自前で構築）

ーメールサーバ・WEBサーバを自前の設備で導入
する場合ー

既存システム

・クライアント30台
・Windowsサーバ1台
・ネットワークプリンタ1台
・ファイアウォール・ウィルス対策は実施済み

新規要件

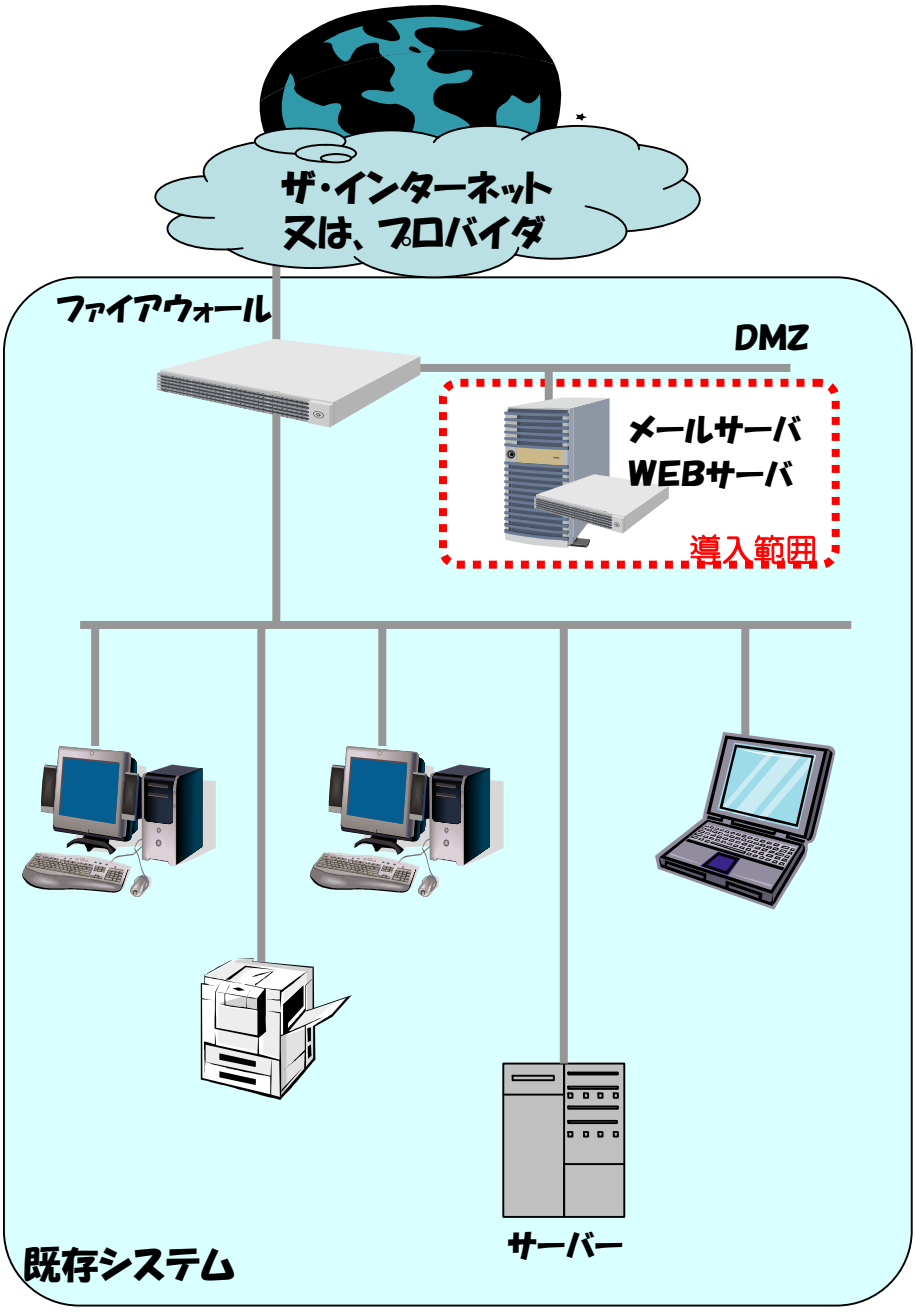
・事前調査
・メールサーバ導入
・WEBサーバ導入
・対応するセキュリティ対策導入

一時費用

・事前調査費：全体の見積もりに含まれる場合が多い
・サーバ（機器・設計・構築）：200万円～
・セキュリティ対策導入費：上記に含む

継続的費用

・サーバ保守費：12万円～／年
・セキュリティ対策維持費：40万円～／年


ザ・インターネット
又は、プロバイダ
ファイアウォール
DMZ
メールサーバ
WEBサーバ
導入範囲
サーバー
既存システム

システム構築事例ー4 （中規模システムー1）
（不正アクセス・ウィルス・スパイウェア対策）

ー小規模から中規模にシステム拡張ー

既存システム

・クライアント100台（30台から増設）
・Windowsサーバ2台（1台から増設）
・ネットワークプリンタ2台（1台から増設）
・スィッチ2台（4セグメント）（1台から増設）
・ファイアウォール・・ウィルス対策（クライアント）は実施済
・メール・WEBサーバは自前で構築済み

新規要件

・不正アクセス対策/ウィルス・スパイウェア対策等は
UTM装置に置き換え（但し、クライアント側のウィルス
対策は維持・増設分は新規購入）
・ルータ又はスィッチ増設
・インターネット接続

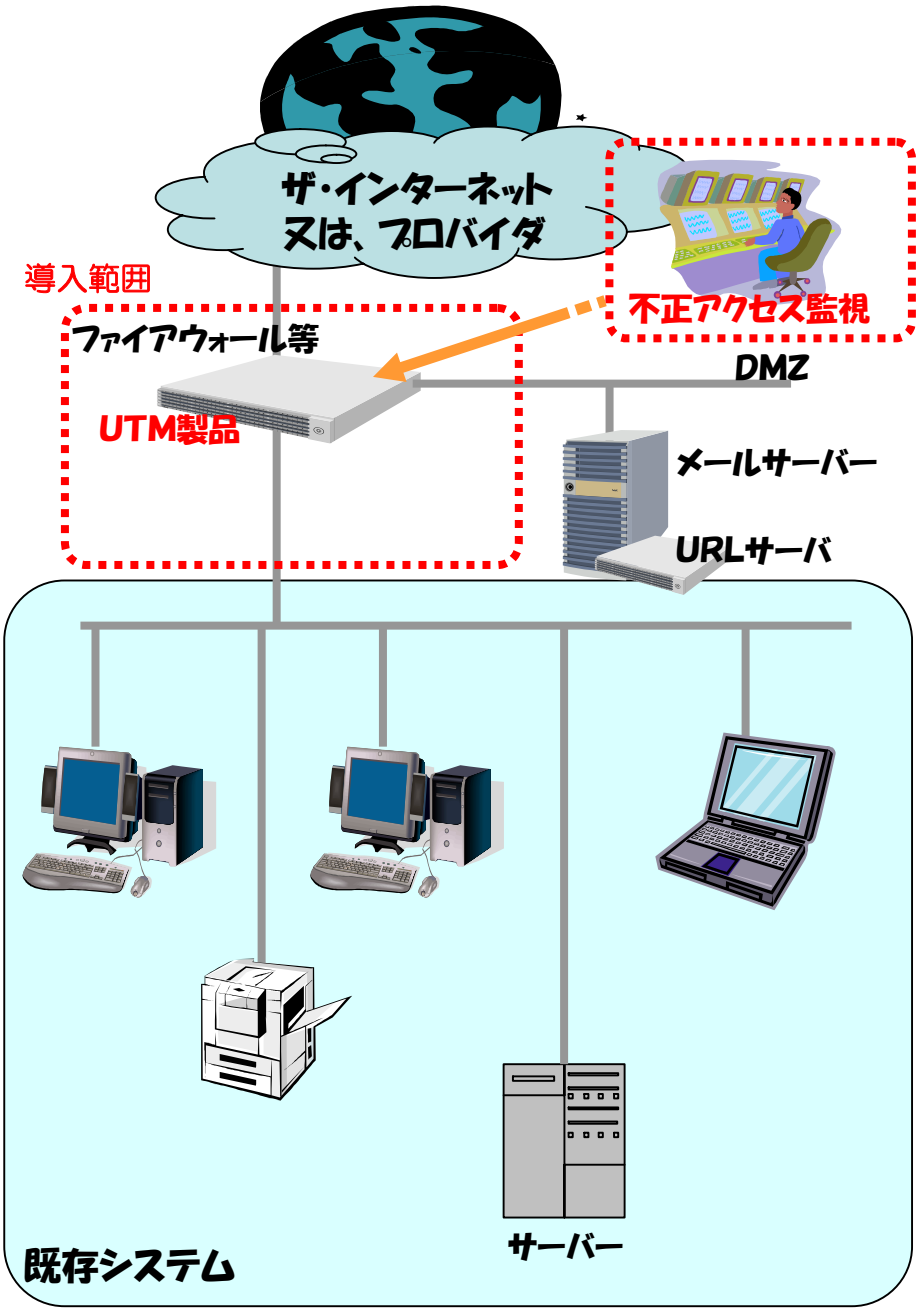
UTM1台で実現

一時費用

・事前調査費：全体の見積もりに含まれる場合が多い
・UTM製品（装置・設計・導入）：106万円～
・不正アクセス監視導入設計費：22万円～
・クライアントウィルス対策：事例1に準ずる

継続的費用

・UTM製品保守：4．5万円～／月
・不正アクセス監視費用：9万円～／月
・クライアントウィルス対策維持費用：事例1に準ずる
・増設文の装置維持保守費用


ザ・インターネット
又は、プロバイダ
導入範囲
ファイアウォール等
UTM製品
不正アクセス監視
DMZ
メールサーバー
URLサーバ
サーバー
既存システム

システム構築事例ー5（メールフィルタ・URLフィルタ）

既存システム

・クライアント30台
・Windowsサーバ1台
・ネットワークプリンタ1台
・メール・WEBサーバ

新規要件

・メールフィルタ構築
・URLフィルタ構築

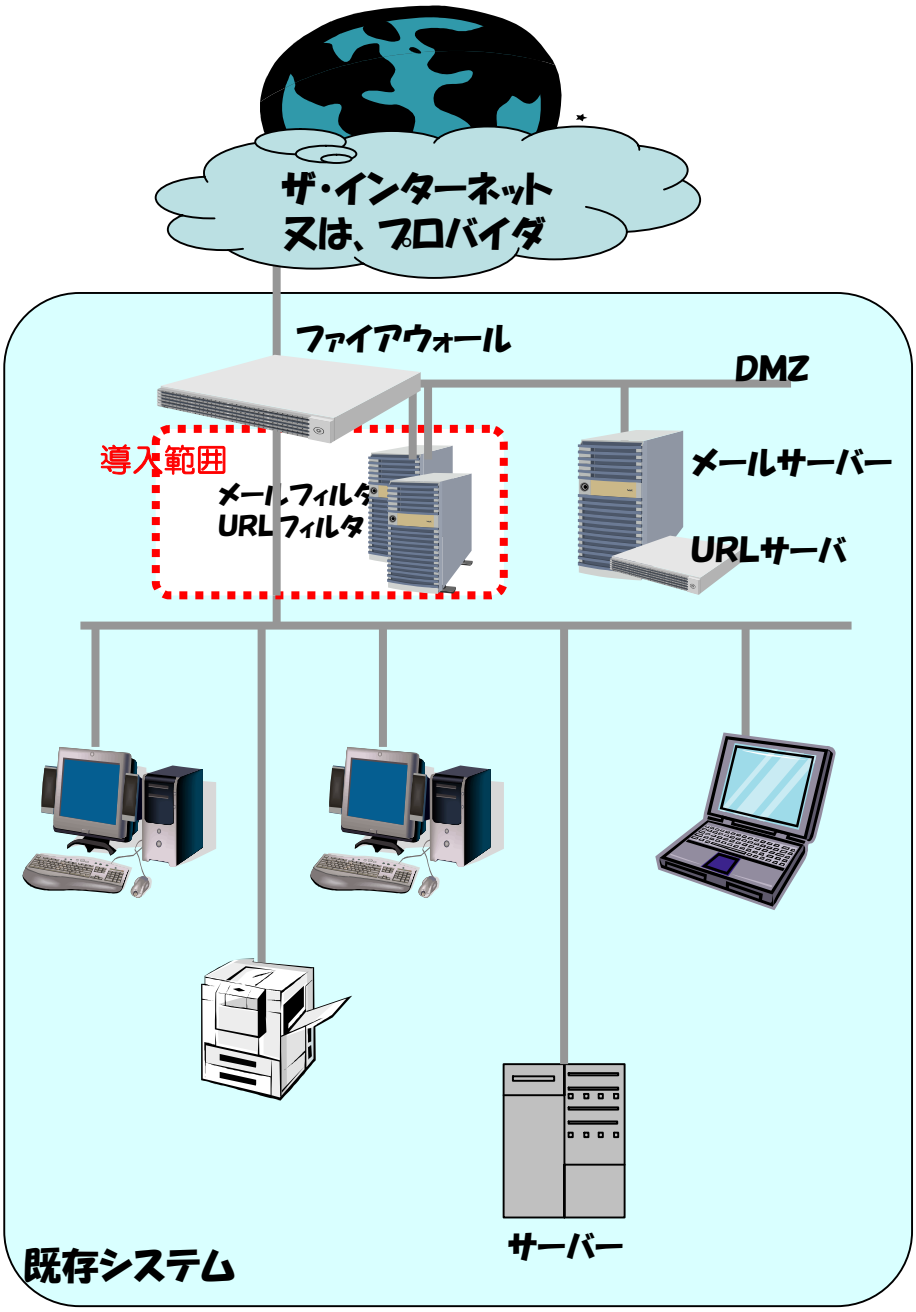
一時費用

・事前調査費：全体の見積もりに含まれる場合が多い
・メールフィルタ：140万円～
・URLフィルタ：54万円～

・フィルタリング用機器と設計導入費込みで
約300万円の事例もある

継続的費用

・メールフィルタメンテナンス：54万円～／年
・URLフィルタメンテナンス：17万円～／年


ザ・インターネット
又は、プロバイダ
ファイアウォール
DMZ
導入範囲
メールフィルタ
URLフィルタ
メールサーバー
URLサーバ
サーバー
既存システム

システム構築事例ー6（ノートPC対策）

ー暗号化対策ー

既存システム

・クライアント30台
・モバイルノート10台（暗号化対象）
・Windowsサーバ1台
・ネットワークプリンタ1台

新規要件

・ノートPC10台時のデータ暗号化対策

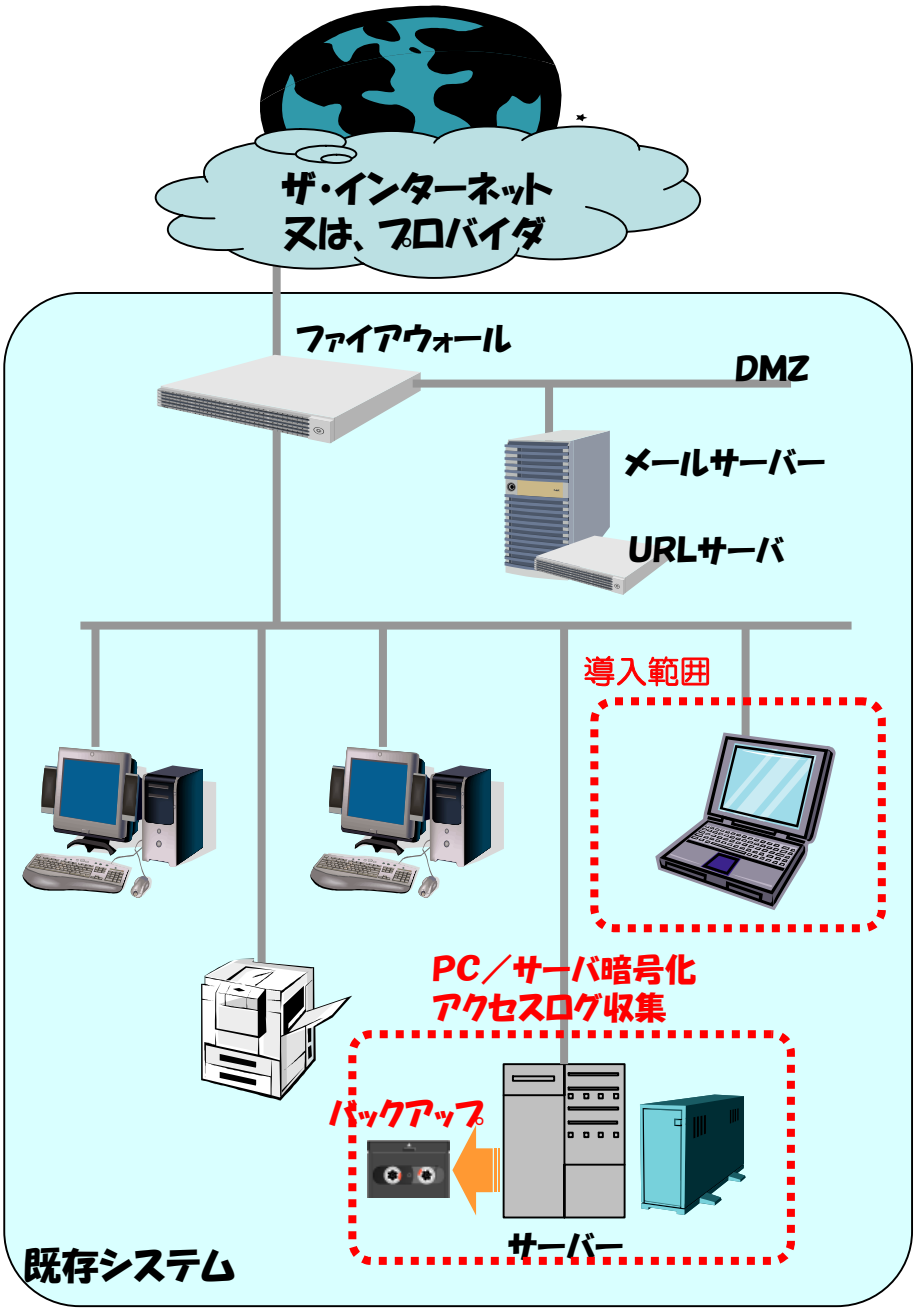
一時費用

・事前調査費：全体の見積もりに含まれる場合が多い
・暗号化導入費：73万円～

継続的費用

・暗号化メンテナンス：9．6万円～／年

上記に加え重要データバックアップも実施した場合
（PC・サーバ暗号化ソフト／アクセスログ収集ソフト
／サーバ機／バックアップ装置／設計導入費）
全て込みで
一時費用　270万円
継続的費用　25万円（機器／ソフトウェア保守費）
の事例もある


ザ・インターネット
又は、プロバイダ
ファイアウォール
DMZ
メールサーバー
URLサーバ
導入範囲
PC／サーバ暗号化
アクセスログ収集
バックアップ
サーバー
既存システム

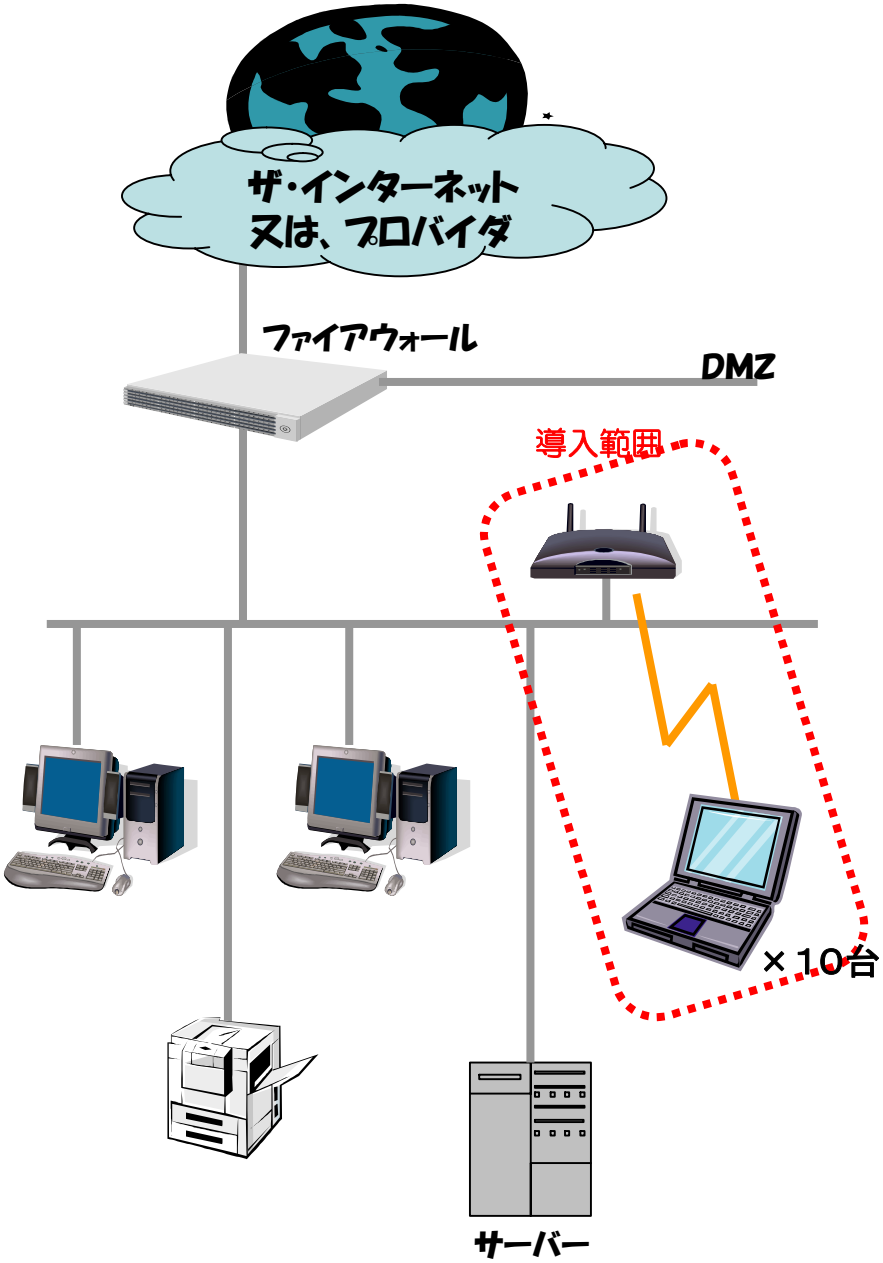
システム構築事例ー7（無線LAN構築）

既存システム
・クライアント30台
・モバイルノート10台（無線化対象）
・Windowsサーバ1台
・ネットワークプリンタ1台

新規要件
・無線ルータ設置（事務所／会議室各1台）
・無線暗号化等設定
・シミュレーション費用
（設置場所に衝立等各種什器が置かれている場合
電波の届かない場所を特定したり、アクセスポイント
の設置場所の設計の為に必要となる）

一時費用
・事前調査費：全体の見積もりに含まれる場合が多い
・無線LANルータ機器：36万円～
・無線暗号化等設定：68万円～
・シミュレーション費用：30万円～

継続的費用
・無線ルータメンテナンス：8万円～／年
・レイアウト変更前のシミュレーション費用：30万円～／回


ザ・インターネット
又は、プロバイダ
ファイアウォール
DMZ
導入範囲
×10台
サーバー

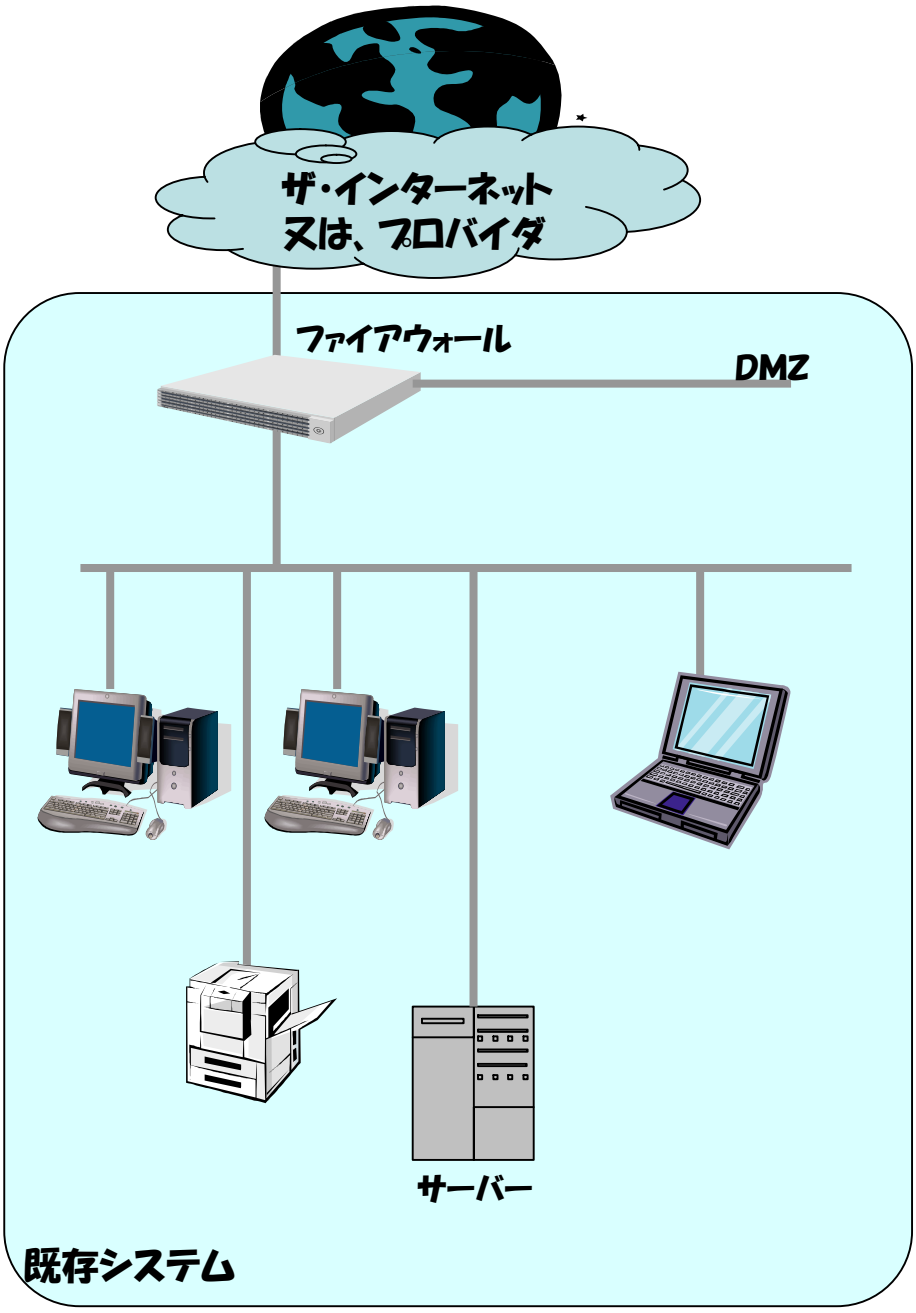
システム構築事例ー8（情報セキュリティ教育）

既存システム
・クライアント100台
・Windowsサーバ2台
・ネットワークプリンタ2台
・従業員150名

新規要件
・情報セキュリティ教育（eラーニング）
　・ASPコンテンツ 150 ID
・管理者向けセキュリティ教育（集合教育）

一時費用 （有効期間：1年間）
・ASPコンテンツ 150 ID：71万円程度
・管理者向け：集合10名：12万円程度

継続的費用
・上記は1年間の費用です。継続の場合は同額が必要です。また、コンテンツの開発は、別途見積もりとなります。


ザ・インターネット
又は、プロバイダ
ファイアウォール
DMZ
サーバー
既存システム

Ⅷ

用語の整理

ここでは、これまでに出てきた専門的な用語について、解説しています。

解説はあいうえお順になっています。

Ⅶ. 用語の整理

＜A～Z（アルファベット）＞

◆Active Directory

Windows 2000に搭載されているディレクトリサービス。ネットワーク上に存在するサーバ、クライアント、プリンタなどのハードウェア資源や、それらを使用するユーザの属性、アクセス権などの情報を一元管理することができる。これまでWindows NTは、これらの資源の管理を「ドメイン」と呼ばれる単位で行なってきたが、複数のドメインを相互運用する場合には、いちいちお互いに信頼関係を結ばなければならず、大規模なネットワークの管理には向かなかった。Active Directoryを利用すれば、ドメインや資源に階層構造を設けて管理することができるため、ネットワークの規模が大きくなっても容易に管理できる。

◆ASP、ASPホスティング

ビジネス用のアプリケーションソフトをインターネットを通じて顧客にレンタルする事業者のこと。ユーザはWebブラウザなどを通じて、ASPの保有するサーバにインストールされたアプリケーションソフトを利用する。

レンタルアプリケーションを利用すると、ユーザのパソコンには個々のアプリケーションソフトをインストールする必要がないので、企業の情報システム部門の大きな負担となっていたインストールや管理、アップグレードにかかる費用・手間を節減することができる。

◆DMZ（DeMilitarized Zone）

直訳して“非武装地帯”と呼ばれ、インターネットなどの信頼できないネットワークと、社内ネットワークなどの信頼できるネットワークの中間に置かれるセグメント。

社内ネットワークをインターネットに接続する際に、Webサーバやメールサーバなどインターネットに公開しなければならないサーバは、DMZセグメントに設置する。

インターネットからの不正なアクセスから保護されるとともに、内部ネットワークへの被害の拡散を防止する。最近では内部犯行による被害の増加から、内部ネットワークからの不正なアクセスを防ぐという目的で使用する場合もある。

◆eラーニング

パソコンやコンピュータネットワークなどを利用して教育を行なうこと。教室で学習を行なう場合と比べて、遠隔地にも教育を提供できる点や、コンピュータならではの教材が利用できる点などが特徴。一方で、機材の操作方法など、実物に触れる体験が重要となるような学習はeラーニングには向かない。

eラーニングは企業の社内研修で用いられているほか、英会話学校などがインターネットを通じて教育サービスを提供している例などがある。Webブラウザなどのインターネット・WWW技術を使うものを特に「WBT」(Web Based Training)とか「Webラーニング」などと呼ぶ。

◆FTC（フォールト・トレランス・コンピュータ）

フォールトトレランスとは、システムに障害が発生した場合にも正常に機能し続けることであり、耐障害性などと和訳されることが多い。

通常のコンピュータは、システムの一部に支障を来たすと機能が停止してしまう。大規模なシステムやミッションクリティカルな業務のシステムには障害の発生は許されない。そのため、システムにある程度の冗長性を持たせることによって異常を回避する仕組みがとられる場合がある。

例えば電源を多重化したり、ハードディスクを多重化したり（RAID）、無停電電源装置（UPS）を用いたりすることで、フォールトトレランスなシステムを実現することができる。

フォールトトレランスなシステムを構築する技術は、フォールトトレラント技術と呼ばれる。フォールトトレラント技術を用いたコンピュータはフォールトトレラントコンピュータと呼ばれる。

◆ICカード

CPUやメモリなどを構成したICチップを内包したカードのこと。カード自体にCPUが内包されているものもあるため、カード単体で不正なアクセスを拒否できるなどその構造上セキュリティ分野で個人認証などに応用されてきている。

特にカード自体が物理的に複製が困難なこと、カード内部のメモリ領域へのアクセスが困難なためデータ改ざんや不正な読み取りが困難なこと、カード単体とカードリーダ間で相互認証機能があるため不正なデバイスを検出しやすいといった特徴がある。しかしカードの盗難などによるなりすましの危険性があるため、カード面に顔写真などを貼るといった対策もあるが、人との対面ではなく機械による認証のみの利用に際してはICカードも含めた複合的な認証をしなければならないという欠点もある。

◆IDS／NW型IDS

IDS（Intrusion Detection System）

不正アクセス監視システム、または侵入検知システムと呼び、ネットワークを流れるパケットを監視して、不正アクセスと思われるパケットを発見したときにアラームを表示するとともに、当該通信記録を収集し保存する仕組みのこと。

ツールによっては、アラームを表示すると同時に当該セッションを切断したり、ファイアウォールやルータのルールを変更するなどの機能を持っている。

IDSのタイプには、ネットワーク型監視（ネットワーク上のパケットを監視）とサーバ型監視（サーバのI/Oパケットを監視）がある。ネットワーク型監視では、既設のネットワーク構成を変更することなく導入が可能だが、サーバ型監視では、サーバに監視ソフトウェアを導入する必要があるため、すでに動作しているアプリケーションへの影響の有無を事前に検証することが望ましい。

◆IPS／NW型IPS

サーバやネットワークへの不正侵入を阻止するツール。ネットワークの境界などに設置する専用の機器(アプライアンス)や、サーバに導入するソフトウェアなどの形で提供される。ネットワーク型のIPSは、侵入を検知するIDSの機能を拡張し、侵入を検知したら接続の遮断などの防御をリアルタイムに行なう機能を持っている。ワームやサービス拒否攻撃(DoS)などのパケットが持つ特徴的なパターンが記憶されており、該当する接続を検知するとこれを遮断し、管理者へ通知(アラート)したり記録(ログ)を取ったりする。

◆ISMS

（Information Security Management System）

企業や組織が自身の情報セキュリティを確保・維持するために、ルール（セキュリティポリシー）に基づいたセキュリティレベルの設定やリスクアセスメントの実施などを継続的に運用する枠組みのこと。

ISMSに求められる範囲は、技術的な情報セキュリティ対策のレベルではなく、組織全体に渡ってセキュリティ管理体制を構築・監査し、リスクマネジメントを実施することである。

現在、日本情報処理開発協会（JIPDEC）を中心に2002年より正式運用されている。

ISMSの認定取得を希望する事業者は、JIPDEC（日本情報処理開発協会）の指定する審査登録機関に、認定取得に当たっての申請を行い、ISMSに基づく審査と監査を行う。審査機関からの結果報告を受けて、JIPDECが事業者を認定済み事業者としての登録を行う。

◆ISO27001

情報セキュリティマネジメントシステムに関する国際規格のことであり、正式な規格名は、ISO/IEC27001:2005といい、2005年10月にISO化された。

◆PDCAサイクル

PDCAサイクルとは、Plan（計画）、Do（実行）、Check（検証）、Action（改善）の頭文字を取った「計画・実行・検証・改善」を繰り返す継続的な活動のことをいう。事業を行う際にまず計画(Plan)を立て、それを実施(Do)し、計画内容通りに実行されたかどうか、点検し(Check)、問題や改善点などがあれば、是正処置を（Action）行うという一連の流れのことである。マネジメントシステム（方針及び目標を定め、それを達成するためのシステム）用語であり、ISOのマネジメントシステムは必ずこの流れに沿っていることが求められる。

◆P2P（Peer to Peer）

不特定多数のコンピュータが相互に接続され、直接ファイルなどの情報を送受信するインターネットの利用形態。また、それを可能にするソフトウェアやシステム。映像や音楽、ソフトウェアなどの海賊版が個人間で違法に流通する温床になっているとして世界的に大きな問題となった。

◆*VPN*

インターネットを利用して仮想的に構築する独自ネットワーク。元々は、公衆網を専用網のように利用できるサービスの総称であったが、最近では、各支社・支店のLANをインターネット経由で接続し、セキュリティを確保した通信形態をVPNと呼ぶことが多くなった。従来のサービスと比較して“インターネットVPN”と呼ぶこともある。VPNの導入により、実際に専用回線を導入するより通信コストを抑えることができる。インターネット上でVPNを実現するVPN専用機のほか、ルータやファイアウォールにVPN機能を備える製品が増えてきた。

◆*SSL－VPN*

SSL-VPN（Secure Socket Layer Virtual Private Network）とは、暗号化にSSLを採用して構築されたVPNである。

ネットワークを結ぶ拠点間を専用回線やフレームリレーで構築するよりも、インターネットを利用することで安価に構築することができるが、インターネットでは盗聴、なりすまし、改ざんによるリスクがあるため、SSLを使ったSSL-VPNの技術を使用する。

SSL-VPNの利点は、SSLが利用するトランスポート層より上位で動くアプリケーション（ブラウザ）があれば使用でき、サーバ側がSSL-VPNに対応していれば、クライアント側は、VPN専用の特別なソフトウエアを導入せずにVPNを利用することができる点である。

◆urlフィルタリング
　◆フィルタリング　を参照

◆webフィルタリング
　◆フィルタリング　を参照

◆Winny
　Winnyとは、日本で開発された、優れた匿名性を有するファイル共有ソフトであり、巨大掲示板サイトの「2ちゃんねる」に書き込みをしていた「47氏」により開発された日本製のファイル共有ソフトである。
　現在は、Winnyと掲示板機能を強化したWinny2がリリースされており、どちらも利用することはできるが、それぞれの通信に互換性はない。
　Winnyのネットワークは全体がツリー状に形成されており、中央のサーバーが無くてもどのようなファイルが共有されているのかを調べることができ、目的とする共有ファイルが検索できたときは、ファイルを持っているコンピュータや中継するコンピュータとピアツーピア（Peer to Peer）接続してデータを転送することになる。ただし、ファイル共有ソフトで転送されるデータのほとんどは著作権を侵害しており、2003年11月には、Winnyを使ってソフトウェアと映画を共有した著作権違反容疑で逮捕者が出ている。

（続き）
2004年5月には逮捕者の著作権侵害行為を幇助した疑いで、Winnyの作者である「47氏」が逮捕され、2006年末に著作権侵害幇助罪で150万円の罰金を命じる有罪判決が、京都地裁から下されている。
現在では、WinnyをターゲットにしたAntinnyと呼ばれるウイルスがWinnyネットワークに蔓延しており、このウイルスは、Winnyが起動しているPCのHDD上にある任意のファイルを勝手にアップフォルダにコピーし、持ち主が知らないうちにほかのWinnyユーザーがダウンロード可能な状態にしてしまう。これによって多くの個人情報や営業秘密、あるいは自衛隊や警察などの機密事項を含んだファイルが漏洩し、無数のキャッシュフォルダに蓄積され、Winnyネットワークを漂うことになってしまった。
一度、漏洩してしまうとファイルはどんどん増殖するため、完全に削除するのが難しく、この情報漏洩の深刻さは、内閣官房の情報セキュリティセンターが「Winnyの使用は危険！」という緊急アピールを出すまでに至っている（2006年3月）。

＜あ～お＞

◆アクティブディレクトリ

アルファベット欄の **◆Active Directory** を参照

◆ウイルス

他人のコンピュータに勝手に入り込んで悪さをするプログラム。画面表示をでたらめにしたり、無意味な単語を表示したり、ディスクに保存されているファイルを破壊したりする。

ウイルスは、インターネットからダウンロードしたファイルや、他人から借りたフロッピーディスクなどを通じて、大抵は使用者の知らないうちに感染する。また、ウイルスに感染したことに気付かずにコンピュータを使用し続けると、他のコンピュータにウイルスを移す危険性がある。

◆ウイルス検知用データ（パターンファイル）

ウイルス対策ソフトがウイルスを検索、駆除するための参考とするファイルがパターンファイルである。パターンファイルにはさまざまなウイルスの特徴が記され、ワクチンソフトのメーカーは新しいウイルスが見つかるたびに、パターンファイルを更新することで新種のウイルスに対処する。多くのウイルス対策ソフトにはインターネットを使ったパターンファイルの自動更新機能があるので、これで最新のウイルスにも対処できる。

◆ウィルススキャン
ウィルススキャンとは、各セキュリティ対策会社が行っているウィルス発見、駆除サービスである。定期的にウィルススキャンを起動し、コンピュータ内のデータファイルをウィルスチェックすることで、事前にウィルスの動きを封じることができる。

◆ウィルス対策ソフト
コンピュータウイルスを除去するソフトウェア。ウイルスに感染したファイルを修復し、コンピュータを感染前の状態に回復するアプリケーションソフトのこと。「ワクチンソフト」「アンチウイルスソフト」などとも呼ばれる。

＜か～こ＞

◆擬似アタック
擬似アタック（Pseudo Attack）とは、コンピュータシステムのセキュリティ上の脆弱性を確認するため、不正侵入等を試みるテスト手法のことです。疑似アタックの内容としては、不正侵入の他、DoS攻撃に対する耐久性の確認、不正侵入により踏み台にされないか、等のテストを行います。

◆検疫システム

システムに甚大な被害が及ばないよう、事前に内部ネットワーク上につなぐクライアントPCやサーバーなどがウイルスやワームなどに感染しないような適切な対策がとられているか、パッチの適用状況などを検査し、セキュリティポリシーに準じたものだけの接続を許可するシステムを総称して「検疫システム」と呼ぶ。

例えば、社内ネットワークにつながろうとしているクライアントPCにウイルス感染の可能性が確認されれば、そのPCを自動的に隔離し、必要に応じてそのPCの復旧作業を行わせることが可能となる。そのため、検疫システムのデータベース内には最新のパッチ情報やウイルス検知ルールの情報が設定されており、接続してきたクライアントPCの状態を確認して、接続許可の判定を下す。「MS-Blaster」ワームの発生時には、多くのシステムが停止に追い込まれ、経営に大きなダメージを与えたが、この原因として一度外部に持ち出したノートブックPCがワームに感染し、これを社内システムに持ち込んだことが原因とされる。このようなPCの安全性を確保するソリューションとして検疫システムに対するニーズが高まっている。

◆公開鍵

公開鍵暗号では暗号化に使う鍵と復号に使う鍵が分離されており、暗号化に使った鍵で復号を行なうことはできず、片方からもう一方を割り出すことも容易にはできないようになっている。鍵の持ち主は復号に使う鍵のみを他人に知られないように管理し、暗号化に使う鍵は公開する。このため、暗号化に使う鍵は公開鍵、復号に使う鍵は秘密鍵と呼ばれる。

公開鍵暗号で秘密のメッセージを送受信する場合、送信者は受信者が公開している公開鍵を入手して暗号化を行なう。暗号化されたメッセージは受信者の持つ秘密鍵でしか復号できないため、途中で第三者に傍受されても中身を解読されることはない。

◆個人情報保護法

個人情報の保護に関する法律であり、本人の意図しない個人情報の不正な流用や、個人情報を扱う事業者がずさんなデータ管理をしないように、一定数以上の個人情報を取り扱う事業者を対象に義務を課す法律のこと。2005年4月より全面施行されており、以下の5つの原則から成り立つ。

・利用方法による制限（利用目的を本人に明示）
・適正な取得（利用目的の明示と本人の了解を得て取得）
・正確性の確保（常に正確な個人情報に保つ）
・安全性の確保（流出や盗難、紛失を防止する）
・透明性の確保（本人が閲覧可能なこと、本人に開示可能であること、本人の申し出により訂正を加えること、同意なき目的外利用は本人の申し出により停止できること）

◆緩衝地帯

アルファベット欄の◆DMZ（DeMilitarized Zone）を参照

◆検疫システム

システムに甚大な被害が及ばないよう、事前に内部ネットワーク上につなぐクライアントPCやサーバーなどがウイルスやワームなどに感染しないような適切な対策がとられているか、パッチの適用状況などを検査し、セキュリティポリシーに準じたものだけの接続を許可するシステムを総称して「検疫システム」と呼ぶ。

例えば、社内ネットワークにつながろうとしているクライアントPCにウイルス感染の可能性が確認されれば、そのPCを自動的に隔離し、必要に応じてそのPCの復旧作業を行わせることが可能となる。そのため、検疫システムのデータベース内には最新のパッチ情報やウイルス検知ルールの情報が設定されており、接続してきたクライアントPCの状態を確認して、接続許可の判定を下す。

＜さ～そ＞

◆冗長化

通信系統の予備系や、通信機器の予備機を設置することを冗長化や二重化という。特に重要な通信経路において基幹をなすものについては、常に業務を瞬時に代行可能なシステムとしておくことが望ましい。これをホットスタンバイと呼ぶ。ほかにネットワークから切り離した状態で予備機を持つことをコールドスタンバイという。

◆シンクライアント

企業の情報システムにおいて、社員が使うコンピュータ(クライアント)に最低限の機能しか持たせず、サーバ側でアプリケーションソフトやファイルなどの資源を管理するシステム、または、そのようなシステムを実現するための、機能を絞った低価格のクライアント用コンピュータ。

シンクライアントの端末側にデータを持てない特性が、情報漏洩対策に効果的であるとして注目を集めるようになっている。

◆シングルサインオン

ユーザーが1回のログインで、複数のサーバにアクセスできるようにする機能。複数のサーバが個々に認証を行なうと、ユーザーはさまざまなユーザーIDとパスワードを使い分ける必要が生じる。また管理という観点からも、複数パスワードを定期的に更新する手間を考えると、好ましくない。こうした環境において、ユーザーの利便性と管理機能を向上させるため、ディレクトリサービスと同期して、複数サーバの認証とユーザーのアクセス制御を一元管理するのがシングルサインオンと呼ばれる機能である。

◆スパイウェア

意図しないプロセスによりユーザーの行動を監視し、その情報を第三者に送信するソフトウェアの総称。

ウイルスの場合は愉快犯で増殖自体が目的であることが多いが、スパイウェアは金銭的利益を目的としているものが多い。スパイウェアに感染した場合、ウイルスとは異なり表面的な活動が見えないことが多く、感染に気がつかないように工夫されている。感染してしまうと除去が困難であるだけではなく、社会的信用の失墜、財産・金銭の喪失など被害が甚大になる場合がある。

◆スパムメール

不特定多数の相手に対して、無差別に一方的に送信される広告・宣伝メールであり、迷惑メールとも言う。スパム メールの中には "このメールの配信が不要なお客様はお知らせください" などの内容で返信を促すものがあり、これに返信をしてしまうとメールの内容を読んだことをスパム メールの業者に対して知らせる結果となり、新たにスパム メールが送られてくる原因になることもあるため、注意が必要である。また、ハッカーやクラッカーが行うメール爆弾は、スパムメールとして第三者のサーバを中継して発信されることが多く、メールサーバのセキュリティをしっかり行っていないと気が付かないうちに中継者になってしまう場合も多い。こうした不正利用される第三者のサーバを踏み台と呼ぶ。スパムは、受信者側にとって迷惑なものであるため、踏み台となった組織は対外的に信用を損なうことにもなる。

◆生体認証（バイオメトリクス認証）

人間1人1人に固有の特徴、つまり「その人物であると認識するに十分な身体的特徴を使って認証を行う仕組み」のこと。認証システムをだますことが非常に難しいなどのメリットがある。利用される身体的特徴は、指紋・手形・網膜・虹彩・声紋・顔・署名・手の甲の静脈パターンなどがある。主にバイオ認証は静的生体特徴（経時的変化がほとんどないと見なせるもの）のみを対象にしている。

◆セキュリティーパッチ

ソフトウェアに保安上の弱点(セキュリティホール)が発覚した時に配布される修正プログラム。通常はインターネットなどを通じて無償で配布される。

◆セキュリティーホール

“セキュリティ上の欠陥”を指し、通常は、プログラムのバグに起因する不具合を指す。ハッカーはこのセキュリティ・ホールを狙って攻撃してくる。オープン系システムで使用されているほとんどのソフトウェア（WindowsやUNIXなどのOS、sendmailやファイアウォールなどのミドルウェア）には必ずセキュリティ・ホールがあるといっても過言ではない。

セキュリティ・ホールの情報は、当該ソフトウェアを提供しているメーカーや、コンピュータ緊急対応センター（JPCERT/CC）などから逐次提供されており、一般に修正プログラム（セキュリティパッチ）も無償で提供されている。セキュリティ管理者は、情報収集とともに、ソフトウェアを最新の状態にしておくことが運用管理では欠かせない。

◆ゼロデイ攻撃
セキュリティーホールを狙った攻撃が、セキュリティーホールの修正プログラムや修正バージョンが提供される前に起こること。

＜た～と＞

◆電子証明書
公開鍵暗号方式を使うとき、公開鍵自体が本当に持ち主のものだということを証明するためのもの。
　電子証明書は、認証局から発行され、パスポート、運転免許証、印鑑証明書など、身分証明書に相当する。情報にアクセスするときの身元証明に役立つし、暗号を使っているため、プライバシー保護にも役立てることができる。

◆トロイの木馬
　正体を偽ってコンピュータへ侵入し、データ消去やファイルの外部流出、他のコンピュータの攻撃などの破壊活動を行なうプログラム。ウイルスのように他のファイルに寄生したりはせず、自分自身での増殖活動も行わない。トロイの木馬は自らを有益なソフトウェアだとユーザに信じ込ませ、実行するよう仕向ける。これにひっかかって実行してしまうとコンピュータに侵入し、破壊活動を行なう。実行したとたん破壊活動を始めるものもあるが、システムの一部として潜伏し、時間が経ってから「発症」するものや、他のユーザがそのコンピュータを乗っ取るための「窓口」として機能するものなどもある。トロイの木馬から身を守るためにはアンチウイルスソフトが必要である。

＜な～の＞

◆内部統制

内部統制とは、会社自らが業務の適正を確保するための体制を構築していくシステム（組織形態や社内規定の整備、業務のマニュアル化や社員教育システムの運用、また規律を守りつつ目標を達成させるための環境整備、そして株主など外部への正確かつ有益な財務報告など）を指す。

内部統制（システム）は経営者と労働者との間における仕組み（規律）とも言え、業態や時代の変化とともに適確に変化していくことが望ましい。日本（に限らず世界中）の多くの企業がこうした仕組みについて未整備であり、さきがけとして知られる米国のSOX法を参考に、日本でも法制化され、2008年（平成20年）4月1日から適用される。

◆日本版SOX法（J-SOX法、日本版企業改革法）

相次ぐ会計不祥事やコンプライアンスの欠如などを防止するため、米国のサーベンス・オクスリー法（SOX法）にならって整備された日本の法規制のこと。上場企業およびその連結子会社に、会計監査制度の充実と企業の内部統制強化を求めている。

◆認証局（CA：Certificate Authority）
主にネットワーク上において、データを交換する際、データの発行元が信頼のおける組織であることを証明するための署名を発行することを目的とした組織。認証局、CA局またはCAセンターと呼ぶ場合もある。CAには、“パブリックCA”と“プライベートCA”があり、前者は本人性を第三者が発行する証明書により証明するもので、電子商取引など不特定多数の広い範囲で運用される。

＜**は～ほ**＞

◆パターンファイル
◆ウイルス検知用データ　を参照

◆ハッカー、ハッキング
正確にはコンピュータ技術に精通した人を意味するが、コンピュータ技術を悪用して他人のコンピュータに侵入・破壊を行なう者を指すことが多い。
本来、「ハッカー」という用語には悪い意味はなく、むしろ高い技術を持った人々に対する尊称として使用されていたことから、古参の技術者などの間には、技術を悪用する人々は「クラッカー」(破壊者)と呼んで「ハッカー」とは区別すべきであるとする主張も根強くある。ハッキングを行なう者を「ハッカー」、クラッキングを行なう者を「クラッカー」と呼ぶ。

◆パッチ、パッチプログラム

パッチ（Patch）とは、完成したプログラムを修正するためだけに作られる専用のプログラムやデータのこと。導入したプログラムに不具合が見つかった場合やバージョンアップする場合など、プログラムに修正を加えるときはプログラム全体を入れ替えるのは効率が良くない。そこで、変更が加えられた部分だけを抜き出し、元のプログラムと違っている部分のデータをパッチとして用意する。すでに導入されているプログラムに差分のデータを組み込むことで、少ないデータ容量で最新のプログラムに変更することが可能となる。パッチを使ってプログラムの修正を行うことを「パッチを当てる」と表現する。

◆非武装地帯

アルファベット欄の◆DMZ（DeMilitarized Zone）を参照

◆ファイアウォール

インターネットなどの信頼できないネットワークからの攻撃や、不正アクセスから組織内部のネットワークを保護するためのシステム。

ファイアウォールの目的は、必要な通信のみを通過させ、不要な通信を遮断することであり、通常内部のネットワークから外部はアクセスできるが、外部から内部のネットワークにアクセスができないような制御が一般的である。

◆ファイル交換ソフト

インターネットを介して不特定多数のコンピュータの間でファイルを共有するソフト。著作権侵害をはじめとする違法な情報流通の温床になっているとして非難の対象となっている。

◆フィッシングサイト

オンラインバンクやクレジットカード会社の名前をかたって、ユーザーからIDやパスワード、銀行口座番号、クレジットカード番号などの個人情報を盗み取る犯罪。一斉送信されたメールを使って、あらかじめ用意した本物そっくりの偽サイトへ誘導する。ユーザーは本物のサイトだと思ってユーザー名やパスワードを入力してしまう。えさを使っておびき寄せる行為が「釣り（Fishing)」に似ていることからフィッシングと呼ばれるようになった。

不自然な行動を要求するメールには注意が必要であり、フィッシング詐欺を防ぐためにはユーザーのセキュリティ意識向上が必須である。

◆フィルタリング

＜webフィルタリング＞

Webページの内容をチェックし、有害と思われるページへのアクセスを防止するアプリケーションソフト。

＜urlフィルタリング＞

インターネット上で「閲覧にふさわしくない」と判断されたWebサイトを、URLのブラックリストに基づいてアクセスできないように遮断することである。

＜メールフィルタリング＞

コンピュータを出入りする電子メールを監視し、特定の種類のメールを自動的に選別し、通過させたり遮断したりするソフトウェア。

◆不正侵入検知システム(IDS)

不正アクセス監視システム、または侵入検知システムと呼ぶ。ネットワークを流れるパケットを監視して、不正アクセスと思われるパケットを発見したときにアラームを表示するとともに、当該通信記録を収集し保存する仕組み。

ツールによっては、アラームを表示すると同時に当該セッションを切断したり、ファイアウォールやルータのルールを変更するなどの機能を持っている。

◆不正侵入防御システム(IPS)

サーバやネットワークへの不正侵入を阻止するツール。ネットワークの境界などに設置する専用の機器や、サーバに導入するソフトウェアなどの形で提供される。

ネットワーク型のIPSは、侵入を検知するIDSの機能を拡張し、侵入を検知したら接続の遮断などの防御をリアルタイムに行なう機能を持っている。ワームなどのパケットが持つ特徴的なパターンが記憶されており、該当する接続を検知するとこれを遮断し、管理者へ通知したり記録を取ったりする。

◆踏み台

あるサーバのセキュリティ・ホールを悪用して、不特定多数の第三者に攻撃を行うこと。踏み台にされたサーバがもともとの被害者であるにもかかわらず、実際に攻撃を受けた側からは、踏み台にされたサーバからの攻撃のように見えてしまう。

踏み台行為そのものは他人のサーバの不正利用であるが、当該サーバを踏み台にされるような状態にしておいたこと自体も問題であることから、当該サーバも加害者となる危険性を含んでいる。

踏み台にされると、社会的信頼やブランドイメージの失墜につながるため、サーバ管理者は、OSやミドルウェアソフト（sendmailなど）を、最新状態にしておく、パスワードの運用管理を徹底するなどの対策が必要である。

◆ポート／ポートスキャン

TCP/IPではアプリケーションごとにポート番号が用意されていて、クライアントは当該ポート番号を通じてサーバのアプリケーションと接続する。このポートを外部から順番にアクセスして、応答の有無を検査することをポートスキャンと呼ぶ。

ポートスキャンにより、あるホストにどんなサービスが動作しているかを調べることができる。ポートからの応答があるとき（ポートが開いているとき）は当該サービスが稼働中、ポートからの応答がないとき（ポートが閉じているとき）は当該サービスが停止中であることを意味する。

＜ま～も＞

◆迷惑メール、スパム

公開Webサイトなどから手に入れたメールアドレスに向けて、営利目的のメールを無差別に大量配信することであり、インターネットを利用したダイレクトメールのこと。また、同じ内容を複数の人に送る意味のないメールもスパムメールと呼んでいる。

スパムは、受信者側にとって迷惑なものであり、受信者の都合を考慮せず一方的に送られてくるため、極めて悪質な行為とされている。

◆メールフィルタリング

◆フィルタリング を参照

＜わ＞

◆ワーム型ウイルス

自己増殖を繰り返しながら破壊活動を行なうプログラム。以前はCD-ROMやフロッピーディスクなどに潜伏して感染するものが主流だったが、近年ではインターネットの普及により、電子メールなどを介して爆発的な速度で自己増殖するものが出現している。

IX. その他補足事項

セキュリティ対策と内部統制

本書に記載してあるセキュリティ面からの各種対策は、内部統制のなかのIT全般統制に属するものです。
IT全般統制はIT業務処理の正確性を保障する為に整備・運用するもので、システムの運用・管理における履歴の保管、内外からのアクセスに対する履歴の保管や安全性といった事項を統制するものです。
本書にあげた対策は、上記のように、内部統制に関してはその一部分をカバーしているのみですので、ご注意をお願いします。

索引

あ～お

か～こ

さ～そ

た～と

な～の

は～ほ

ま～も

や～わ

本書は下記の方々のご協力により作成しました

加藤　誠　　NECフィールディング　株式会社
亀田　匡司　　株式会社　富士通エフサス
渡辺　裕二　　株式会社　大塚商会
西浪　一雅　　日本事務器　株式会社
和田　孝司　　東芝情報機器　株式会社
海老沢　久行　リコーテクノシステムズ　株式会社
島村　宗一　　株式会社　ブロードリーフ
藤本　昌宏　　株式会社　シー・シー・ダブル
吉村　秀樹　　株式会社　シー・シー・ダブル
板見谷　剛史　CompTIA日本支局
山本　幸司　　NECフィールディング　株式会社
内藤　剛　　NECフィールディング　株式会社

斎藤　久雄
奥田　和男

古田　正武　　日本コンピュータシステム販売店協会
山田　勝正　　日本コンピュータシステム販売店協会

必要なセキュリティ対策がわかる本

発行　社団法人　日本コンピュータシステム販売店協会
東京都文京区湯島１－９－４　鴫原ビル2階
電話　03－5802－3198
ホームページ　http://www.jcssa.or.jp

発行日　　平成19年12月（初版）