Method of information technology administration SME managers should know.

中小企業経営者が絶対知っておくべきIT管理の運用術

～あなたの会社はセキュリティ対策済みですか?～

Does your company implement security measures?

昨今のセキュリティ情勢やIT管理方法から話題のウィルス攻撃に関する用語集などの情報が満載！

社内のセキュリティ状況がわかる
チェックリスト付き！

〔発行元〕シーティーエス株式会社

Method of information technology administration SME managers should know.

はじめに・目次～

はじめに

当冊子では中小企業における IT 管理 の役割の重要性・昨今のセキュリティ情勢、セキュリティ対策の手順・IT 用語集、ネットワーク運用の参考となる情報をご紹介いたします。日々進化する IT 技術に追いつけず、相談相手も見つからないといったことはありませんか？また皆さまの会社では、セキュリティ対策が不足したまま“なんとなく”現状維持を続けていませんか？情報管理は組織全体の問題です。自身の業務に専念できるよう、この機会に IT 管理の見直しを一緒に始めていきましょう！

「中小企業経営者が絶対知っておくべき IT 管理の運用術」目次

P0 ：はじめに・目次
P2 ：あなたの会社は大丈夫？ IT 管理チェックリスト
P3 ：昨今のセキュリティ情勢
P4 ：セキュリティ対策を実施するために
P5 ：コストシミューレション
P6 ：コストシミューレション解説
P7 ：煩雑な業務の数々を月額 2 万円から
P8 ：アウトソーシングを活用している会社様の声・意見・感想
P9 ：IT サポート用語集
P12: おわりに

中小企業経営者が絶対知っておくべきIT管理の運用術

Method of information technology administration SME managers should know.

〔発行元〕シーティーエス株式会社

Method of information technology administration SME managers should know.

あなたの会社は大丈夫?IT管理チェックリスト

早速ですが、あなたの会社での IT 管理におけるセキュリティ対策はどのような状況でしょうか。
下記のチェックリストを活用し、○の数がいくつあるかを数えてみましょう。

業務にまつわるデータや情報をパスワード保護せずに USB やハードディスクに保存して持ち帰ったり、外出先で閲覧したりすることがある。	
データを持ち出す際、社内規定ルールの準拠や上司への報告は不要である。	
パソコンやスマートフォンあるいは書類等を廃棄するときは個人の裁量に任されており重要情報が読めなくなるよう消去するなど破壊・粉砕処分をしていない。	
社内・事務所への人の出入りを管理・把握していない。（誰が出入りしたかを把握していない）	
パソコンの最新版アップデート更新は社員各自のタイミングで気がついたときに実施している。	
パスワードは自分の名前や誕生日などわかりやすい文字列を使用している。	
業務で使用するパソコンやスマートフォンにはセキュリティソフトが未導入である。	
社内においてセキュリティ被害の共有・報告など情報セキュリティに関する教育を実施したことがない。	
会社のネットワーク環境について把握しておらず、トラブルが発生した時には常に業務が止まってしまう。	
サーバーや PC のバックアップ実施は不定期に行っている。	
事故や情報漏えい・データ紛失があった場合の対応手順書や、持ち出し時の盗難・紛失対策について社内規定の事項がない。	
情報セキュリティを維持するための社員の理解度を把握するチェックテストを実施したことがない。	

【○が 0 個の場合～】　：セキュリティ対策はバッチリ！引き続きこの環境を維持できるよう努めましょう。
【○が 1 個以上の場合～】：セキュリティの盲点を付かれる可能性があります。環境の見直しの機会を作りましょう。
【○が 3 個以上の場合～】：情報管理は個人任せになっていませんか？組織全体でセキュリティ対策に取り組みましょう。
【○が 5 個以上の場合～】：リスクが高い状態となります。いつ情報漏洩が発生してもおかしくありません。
意識改革も含め早急に環境を整えることが必要です。

○の数はいくつでしたか？上記の結果をもとに、状況にあった対策を実施しましょう。

昨今のセキュリティ情勢～

サイバー攻撃を受けたことのある大手企業は 5 割強

インターネットの脆弱性を悪用した改ざん、システムの破壊、機能不全、ネットバンキングの不正送金被害、企業の機密情報を狙った標的型攻撃などサイバー攻撃は日々巧妙化し続けています。攻撃を受けると気づかない間に情報が漏れたり、あるいは情報セキュリティ部門がなければ対応に時間がかかったりなど、時間の経過に伴って状況が悪化するのが現在のセキュリティ被害の実情です。
この数年間、サイバー攻撃を受けたことのある大手企業は 5 割強にものぼります。国立大学や私立大学、研究機関でもホームページ改ざん、個人情報や知的財産を狙った攻撃が相次いでいます。もちろん攻撃は大手企業や政府・公的機関だけではありません。

BYOD の増加とともに

中小企業においても矛先は向けられており、大企業の取引先を狙った踏み台とされるケースが少なくないのです。とりわけ BYOD（Bring your own device：私物のデバイスを業務に持ち込むこと）が積極的に導入されているため業務の効率化や利便性は高まりますが、同時にセキュリティリスクの危険性も高くなります。「中小企業だから攻撃対象として狙われることはないだろう」「従業員が 10 数名程度の会社だから問題ないだろう」と慢心するのは注意が必要です。

中小企業が狙われる理由は「踏み台」として

標的とする大企業の守りが堅い場合、その周辺企業から攻撃を仕掛け乗っ取り、なりすましを行ったりマルウェアを仕込んだりする、その前段階として中小企業が狙われるという仕組みです。つまり『セキュリティ対策』という行為は、自社内のためだけでなく取引先の機密情報を守る行為なのです。
ウィルスや悪意ある攻撃の被害者であると同時に取引先やユーザーに対して加害者となりうる事態も起こるため、中小企業にとっても情報管理・セキュリティ対策を徹底することが重要です。大規模なシステムを導入したり担当者を雇ったりする余裕がないという事実は、セキュリティ対策をしなくて良いという理由になりません。可能な範囲で着実に、対策できるところから取り組んでいきましょう。

セキュリティ対策を実施するために～

セキュリティ対策は「0」か「100」かで考えないこと

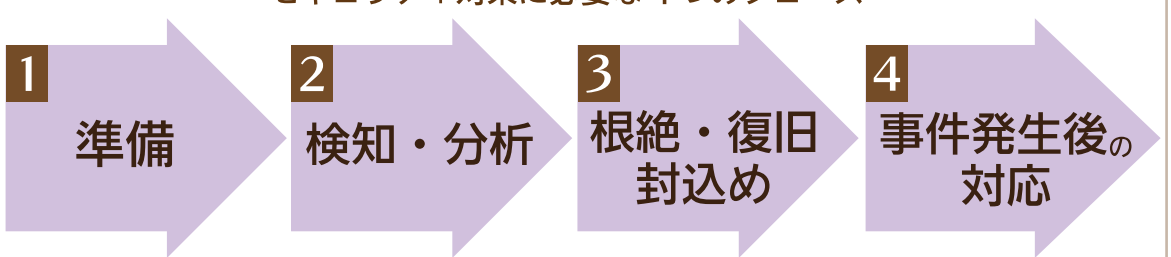
それでは具体的にどのような方法でセキュリティ対策を行えばよいのでしょうか？サイバー攻撃から身を守るためには一体何が必要なのでしょうか？経営者を悩ませるセキュリティ問題。ツールを導入すれば解決するのか、情報セキュリティ部門を立ち上げれば解決するのか、様々な手段はありますが念頭に置いておきたいのは対策を「0」か「100」かで考えないことです。

すべてのサイバー攻撃をシャットアウトすることが第一の目的としてしまえば、万が一防ぐ事ができなかった場合の被害は甚大なものになります。常に「A の状態にならないために B を実施する」「A の状態になった場合はＣを実施する」というように段階を分けて考えましょう。攻撃者が嫌う企業のセキュリティ対策には４段階のフェーズがあります。

1 つ目は「準備」。攻撃者が侵入しないように防御力を向上させます。
2 つ目は「検知・分析」。攻撃・侵入されているかどうかを検知します。
3 つ目は「根絶・復旧・封込め」。サイバー攻撃による被害を軽減します。
4 つ目は「事件発生後の対応」。ファイルの暗号化など最後の水際の対策を行います。

これら 4 つの対策を行うことで攻撃が成功しづらく、仮に成功してもすぐに検知することができる。くぐり抜けてもファイルを暗号化していれば読まれることはない、というように攻撃をシャットアウトできる扉を複数配備する対策と運用が求められます。
セキュリティ対策は入り口だけ実施すれば良いわけではありません。多層的に実施するほど強固なものとなります。「1: 準備」や「2：検知・分析」についてはセキュリティソフト等ツールで導入している企業は多いかもしれません。しかしその先の「3: 根絶・復旧・封込め」「4: 事件発生後の対応」についてはその重要性に反比例してまだ少ないとされています。既に自社で包括的なセキュリティ対策を行っている企業はこの 4 段階のフェーズに、現在の運用管理をマッピングしてみると環境が俯瞰して把握できますので、ぜひ一度お試しください。

セキュリティ対策に必要な４つのフェーズ



コストシミュレーション～

情報セキュリティ担当者を雇う場合とアウトソーシングする場合

セキュリティ対策を実施する上でどれほどの費用がかかるのか。当然ながら企業規模によってコストは異なりますが、今回は自社内で情報セキュリティ担当者を付ける、あるいは専門の外部企業にアウトソーシングするという 2 つの点から考察します。

①社内で情報セキュリティ担当者を付ける場合、セキュリティインシデント対応経験豊富な人材の雇用に主な費用が発生します。アプリケーション・システム・ネットワークや基盤運用の知見を有する、かつ機密情報を任せるため信頼の置ける人材が求められますので採用段階から人物をしっかりと見極めなければなりません。社員を 1 人雇うので月あたりのコストは 30 万以上～となります。

②専門の外部企業にアウトソーシングする場合、セキュリティ対策の設計・構築・運用・保守の外注に主な費用が発生します。専任の体制でスキルを持った要員が対応を行うためサービスレベルの継続的な維持が可能です。初期設備投資にコストがかかりますが、運用維持として月あたり 10 万円程度～となります。

情報セキュリティ担当者を雇う場合

POINT

- セキュリティインシデント対応経験豊富な人物
- アプリケーション、システム、ネットワークや基盤運用の知見を有する人物
- 機密情報を任せられる信頼できる人物

月額コスト

雇用に対する費用 約 30 万以上～

専門の企業にアウトソーシングする場合

POINT

- セキュリティ対策の設計、構築、運用、保守
- 専任体制でスキルを持った技術要員
- サービスレベルの継続的な維持
- 初期設備投資がかかる

月額コスト

運用維持に対する費用 約 10 万程度～

コストシミュレーション解説～

第三者がチェックすることにより安全な IT 環境づくりへ

先ほどのコストシュミレーションをもう少し詳しく見ていきましょう。

①社内で情報セキュリティ担当者を付ける場合、人的コストが最も大きな費用を占めます。人を 1 人（もしくは複数人）雇うわけですから企業は給料や通勤費、または健康保険や厚生年金・雇用保険などの社会保険料を負担する必要があります。その他に人材の採用募集に掛かる費用、セキュリティソフトや設備導入にかかる費用、セキュリティスキル維持のための費用が発生します。人材を新規雇用しない場合には、システムに詳しい社員や総務を情報セキュリティ担当として兼任させるケースも多いでしょう。「2014 年度情報セキュリティ事象被害状況調査」（独立行政法人情報処理推進機構）によると現在、情報セキュリティ担当と他業務とで兼務を行う担当者は過半数にのぼります。しかしながら情報セキュリティ業務は外部からの攻撃だけでなく社内における不正行為など全体を俯瞰して管理・把握する必要があるので専任の人材を設けることが推奨されています。情報セキュリティ責任者は CISO（Chief Information Security Officer：最高情報セキュリティ責任者）とよばれ、社内においても取締役会の一員としての位置付けが求められています。

②専門の外部企業にアウトソーシングする場合、外注コストが最も大きな費用を占めます。どの程度のセキュリティ内容をカバーできるか、価格体系は適正か、サービスレベルや機密保持に関する取扱い等は委託先によって異なりますので、サポートを依頼する際には十分に熟慮した上で外部委託先企業を決定することが重要です。サービス内容そのものだけでなくその企業は定期的に情報発信を行っているか、営業部員や技術者とは信頼できる関係性を築き上げられるかどうかなど様々な点を考慮し検討しましょう。事前にしっかりと情報が共有できていなかった場合、または意思疎通ができなかった場合には後でトラブルに発展する可能性が高くなります。

セキュリティ対策の設計・構築・運用・保守を行うにはまず初期段階で IT 管理の状況を把握し可視化する必要がありますが、外部の技術員が第三者の視点から行うことによって客観的かつ盲目的にならない環境づくりが可能です。

POINT

自社内に CISO（情報セキュリティ責任者）を置くことができない中小企業にとっては費用や技術力などにおいて外部企業にアウトソーシングするほうがメリットが高い。

煩雑な業務の数々を月額2万円から〜

従業員 20 人以下の小規模企業では情報セキュリティ担当者が 2 割弱

独立行政法人情報処理推進機構 (IPA) が中小企業経営者、IT 担当者、従業員を対象に行ったセキュリティ対策に関するアンケート調査では、企業の規模が小さいほど情報セキュリティ対策担当者を置いている割合が低く、従業員 20 人以下の小規模企業では 2 割弱にとどまることがわかりました。そして小規模企業の 7 割が社内・社外の「情報セキュリティの相談窓口が特にない」と回答しています。(「2015 年度 中小企業における情報セキュリティ対策に関する実態調査」)

弊社ではそのような企業・店舗・事務所様を対象に月々 2 万円からできる情報管理及びセキュリティ対策として「IT サポート & サービス」をご提案いたします。ウィルス対策を実施したい、重要なデータの保管方法に悩んでいる、社内のセキュリティ対策を強化したいといった方はもちろん、パソコンが動かない、インターネットに繋がらない、メールが送受信できない、プリンタなど周辺機器の接続方法がわからない、社内ネットワークの構築が複雑で整備できない、といった IT 環境に関するトラブルもご相談を受け付けております。専門の技術員がお電話またはメール・リモートアクセスにて対応。ご要望に応じて技術員訪問による定期点検や再調査も実施いたします。

PC およびサーバー台数が 20 台以下の場合ならばサポート価格【20,000 円 / 月額】。21 台以降は、1 台あたりサポート価格【1,000 円 / 月額】です。つまり 50 台であれば 50,000 円 / 月額、100 台であれば 100,000 円と簡単にお見積もりが可能です。店舗・支社・支店など複数個所する場合は 10 台以下が【10,000 円 / 月額】11 台以降は同様に 1 台あたりサポート価格【1,000 円 / 月額】。情報セキュリティ担当者を雇う場合から比べておよそ 10 分の 1 の値段で IT 環境を整備することができます。※サポート価格は全て税抜き表記です。

サポートの流れは、まず「①初期現場調査 (IT 資産調査)」を行います。プロの技術者が IT 資産の状態およびネットワーク環境を調査。次に「② IT 資産管理台帳を作成」調査結果をもとに、論理・物理的ネットワーク構成図やサーバー・パソコンの状態、ルーター・ハブなど周辺機器の接続状況をこまかく台帳にまとめます。その結果「③調査結果と改善点のアドバイス」を実施。セキュリティ対策や改善点、今後管理していく上で重要なポイントをアドバイスします。そして「④ IT サポートセンターを開設」。IT 資産の状態をまとめ、安全な運用方法を構築した上でお客様用の IT サポートセンターを開設します。万一トラブルが発生した場合は、電話で気軽にサポートセンターに相談することができます。

社内・メールサーバー運用代行や定期メンテナンスを行うことも可能です。自社内の業務に注力するため、情報セキュリティ対策コスト削減のためにアウトソーシングする。より安全で安心できる社内 IT 環境づくりを行いましょう。

アウトソーシングを活用している会社様の声・意見・感想～

情報管理・セキュリティ対策をアウトソーシングすることについて弊社に寄せられたご意見やご感想を紹介いたします。

「環境が把握できるようになったことが良いですね」

以前は起業時にネットワーク構築をした人間が情報管理を担当していましたが、専門ではないため管理の手法が整理されていませんでした。トラブルが発生した際は都度その人に相談をしていました。今回システム管理をアウトソーシングすることによって情報管理が可視化され環境が把握できるようになりました。全体を IT 管理台帳で見渡せ、ネットワークで何と何が繋がっているのかが明確に、かつスタッフとも情報の共有が容易となりました。

「電話で気軽に相談できる」「自分自身の作業に注力できる」

管理部門の人材が情報管理も兼務していたため、業務の比重を減らすことを目的としてアウトソーシングを行いました。以前は不明点があるたびに停滞が起きていましたが、電話で気軽に相談できることで次のアクションにすぐ移行できるので非常に助かっています。確実に 1 台 1 台のパソコンの管理が行き届くようになりました。

ITサポート用語集

セキュリティや攻撃の種類などの用語をご紹介いたします。

アドウェア【adware】

強制的に不要な商品の広告を表示するソフトウェアを意味します。ユーザーのアクセス行動履歴や情報を読み取り、内容を判別して広告を一定期間何度も繰り返し表示するので、悪質なものはマルウェアとも呼ばれます。

SQL インジェクション【SQL injection】

セキュリティ上の不備を利用し、本来想定されていない SQL 言語の文を実行させてデータベースに不正な操作を加えることを意味します。被害の例として、Web サイトの改ざんや顧客情報の漏えいが上げられます。攻撃手法は「SQL コマンドインジェクション」とも呼ばれており、意図しない SQL 文を受け入れないよう対策が必要です。

SPF【sender policy framework】

Sender Policy Framework の頭文字をとったもので、メールの送信元アドレスを偽装していないかチェックするための送信ドメイン認証技術です。送信元のドメイン名とメールサーバーの IP アドレスを整合し認証。スパムメールを排除することができます。

ガンブラー【gumblar】

ウィルスを感染させる攻撃の一種をあらわします。Web サイトを改ざんしたり脆弱性を狙って攻撃します。不正なサイトへ誘導し、ウィルスに感染させる手法で 2009 年から急激に拡大しつつあります。

クロスサイトスクリプティング【cross site scripting】

Web アクセスを通じて、セキュリティ上の脆弱性を利用した攻撃のことを意味します。フォーム入力などのデータを改ざんすることで本人になりすましたり、ユーザーの意図しないスクリプトを実行させられたりすることがあります。動的な Web サイトに取り込まれることが多いため、注意が必要です。

辞書攻撃【ジショコウゲキ】

パスワードを解読する攻撃手法の一つを意味します。辞書にある単語を片端から入力して試すというもので、コンピューターに自動処理をさせれば短時間で行うことが可能です。小文字や大文字を混ぜたり数字も加えたりしてパスワードを割り出します。

スパイウェア【spyware】

コンピューター内部より、ユーザー情報をインターネットに自動送信するソフトウェアを意味します。ソフトをインストールした際に組み込まれているものや、ユーザーの知らない間に自動的にインストールされたものなどがあります。

ゼロデイ攻撃【ゼロデイコウゲキ】

ソフトウェアの修正パッチが提供される前に、そのセキュリティホールを悪用して攻撃されたり不正プログラムが働いたりすることです。修正パッチが提供された日を 1 日目と計算すると、それ以前に攻撃が行われるという意味でゼロデイと表します。

タイポスクワッティング【typosquatting】

現存する Web サイトのドメイン名によく似せたものを取得し、タイプミスを悪用して別サイトへ誘導することです。タイプ（Typo）ミスと占有（Squatting）をあわせた造語のことです。

タブナビング【tabnabbing】

ブラウザのタブ表示機能を利用して、ID やパスワードを盗むフィッシング詐欺の一つです。バックグラウンドでタブを動かし、銀行や SNS のログインページに化けてユーザーを騙し、情報を入手する手法を意味します。

DKIM【domainkeys identified mail】

Domainkeys Identified Mail の頭文字をとったもので、正当な送信者から送られているかチェックする電子署名方式の送信ドメイン認証技術です。メール送信時に秘密鍵によって生成した署名情報を付与して正当性を確認します。

ドライブ・バイ・ダウンロード【drive-by download】

閲覧するだけで感染するタイプの攻撃をあらわします。悪意のあるツールやアプリケーションなどを隠しておき、閲覧者がアクセスすると自動的にダウンロードされてしまったり勝手に実行されたりするので、気づきにくいことが特徴です。

トロイの木馬【トロイノモクバ】

コンピュータに侵入してデータを消したり攻撃を行い破壊活動を行うソフトウェアの一つです。システムの一部として潜伏する有害なウィルスとして知られています。

2 段階認証【ニダンカイニンショウ】

アカウントとパスワードの組み合わせに加えて「認証コード」の入力を行なうことです。認証コードは、ログインをする際に、テキストや音声通話等で携帯電話に送信されます。発行されたのは一度しか使えないコードとなっており、セキュリティ強化のひとつとして多くのサービスで広く利用されています。

フィッシング【phishing】

インターネットや電子メールを利用し暗証番号などの個人情報を詐取する詐欺を意味します。銀行やクレジットカード会社を装い、偽サイトに誘導するなどして個人の住所や電話番号を盗み出します。

マルウェア【malware】

ウィルスやワーム、スパイウェアなどの悪質なソフトウェアを意味します。メールや Web サイトから感染して情報を外部に漏えいします。システムの脆弱性を付くので、こまめなアップデートをしてセキュリティを強くすることが大切です。

ランサムウェア【ransomware】

マルウェアの一種でファイルなどのデータを暗号化して身代金を要求するソフトウェアを意味します。感染した PC はシステムのアクセスを制限・使用不能にして、復旧と引き換えに金銭を要求します。

ワンタイムパスワード【one-time password】

1 度しか使えないランダムな文字列のパスワードを意味します。一定時間のみ有効で、セキュリティを向上させることができます。認証文字列を生成する機器をトークンと呼びます。

おわりに～

『中小企業経営者が絶対知っておくべきIT管理の運用術』をお読みいただきありがとうございました。セキュリティリスクが日々高まる状況の中で、企業はどのような対策を行うべきか早急な判断が求められています。今日明日いつ自分自身がセキュリティ被害を受けるか、あるいはいつ自分自身が加害者になるかは分かりません。その間も攻撃者は攻撃のタイミングを見計らい、狙い、準備をしているのです。様々な状況を想定し、事故が発生しないためには何が必要かひとつひとつ着実に対策を実行しセキュリティレベルの高い社内 IT 環境を構築しましょう。

社内 IT 環境の状況を共有することで組織全体の意識が高まり、社員全体に安心をもたらし本来の業務に注力することができるようになります。
当冊子が皆さまにとって、IT 環境を見直し、適切な情報セキュリティ対策を行い、個人情報や知的財産を守るためのきっかけの一助となれば幸いです。

引用文献・出典

「組織のおよそ 9 割が攻撃に気づけない」（ZD NetJapan 特別連載記事）
http://japan.zdnet.com/extra/trendmicro_201605/35082641/

「2015 年度 中小企業における情報セキュリティ対策に関する実態調査」報告書について（2016 年 3 月 8 日 IPA 記事）
https://www.ipa.go.jp/security/fy27/reports/sme/index.html

「データ漏えいによる企業の損害額は平均 400 万ドル、米調査」（2016 年 6 月 16 日 ITpro 記事）
http://itpro.nikkeibp.co.jp/atcl/news/16/061601753/

「日常における情報セキュリティ対策」（2015 年 12 月 21 日 IPA 記事）
https://www.ipa.go.jp/security/measures/everyday.html

「セキュリティレベルを維持するためには？」（2008 年 9 月 18 日 NEC ネクサスソリューションズ記事）
http://www.nec-nexs.com/outsourcing/column/article17/index.html#h2-3

「『2015 年度 中小企業における情報セキュリティ対策に関する実態調査』報告書について」（2016 年 3 月 8 日 IPA 記事）
https://www.ipa.go.jp/security/fy27/reports/sme/

「ネットワークセキュリティ入門編」（情報通信振興会　第 3 版 (2015.7.10)）Eric Maiwald 著 金澤薫、竹田義行訳

「新・もしも社長がセキュリティ対策を聞いてきたら」（日経 BP 社）日経コミュニケーション 2016.4

「企業のリスクマネジメント調査 2015 年の調査結果」（デトロイト トーマツ企業リスク研究所）
2016.4 第 51 号　Deloitte 企業リスク

中小企業経営者が絶対
知っておくべきIT管理の運用術

～あなたの会社はセキュリティ対策済みですか?～

2016 年 7 月 25 日　第一刷発行
発行　シーティーエス株式会社

Method of information technology administration SME managers should know.

IT の保守サポート・IT 管理・アウトソーシングのご相談は

シーティーエス株式会社におまかせください！

Does your company implement security measures?

【お問い合わせ】シーティーエス株式会社
〒101-0036　東京都千代田区神田北乗物町 18 神田東栄ビル 3F
TEL : 03-6823-4075　FAX : 03-6823-4076　MAIL:information@e-cts.jp