サイバー攻撃を受けた場合の被害を局限するための人的対策について

研究センター　業務部　業務２課
小島　和浩

１　はじめに

この研究のタイトルを見て「“サイバー攻撃の被害を局限？”、攻撃を防ぐ方法について述べるべきだろう。」と思われた方がおられるのではないでしょうか。実は、私もつい最近までは機会あるごとに、「サイバー攻撃の防ぎ方」などのような話をしていました。しかしながら、最近のサイバー攻撃は、攻撃を受ける側が不審感をいだかないように様々な騙しのテクニックを駆使しており、しかもその手口がどんどん変化しています。この変化により、もはやこの攻撃を完全に防ぎきることはほとんど不可能であり、侵入を防止することも大切ですが、被害を局限する手段を構築することの方がより重要だと考えるようになりました。

ここでは、まず最初に、この間までの私と同様に、まだファイアウォール等の導入や最新のウイルス対策ソフトを装備しておけば大丈夫とか、うちの会社はサンドボックスを導入してウイルスチェックを行っているのでウイルスに侵入されることはないと思っている方に、考え方を改め、いざという時の備えに万全を期していただくために、最新のサイバー攻撃の脅威やこれらに対する対策の甘さを紹介します。そして、サイバー攻撃に適切に対処するためには、貴重な情報を守るために強固なシステムを構築することはもちろん重要ですが、サイバー攻撃を受けた場合の被害を局限するために人的な分野においても対策を講じることが必要だということを説明します。サイバー攻撃対処では、この両輪をうまく活用・運用しなければ、極めて高度化、巧妙化した手口からは、貴重な情報を守ることはできません。

サイバー攻撃対処のためには、この両輪の対策が不可欠ですが、本研究では、サイバー攻撃を受けた場合に被害を局限するために比較的早期に対策に取り組め、会社として本気になりさえすれば高い効果が期待できる人的な対策を対象としました。改めて、サイバー攻撃の被害を局限するためにはどうすべきなのかを、この研究成果を基に考える機会にしていただければ幸いです。

２　サイバー攻撃の脅威

サイバー攻撃には、特定の企業・組織を標的とした標的型サイバー攻撃と不特定多数の企業等を狙った無差別型攻撃があります。どちらの攻撃も、パソコンや情報システム内にあらゆる手段を使ってウイルスを侵入させることが、攻撃の第一段階になります。その後、侵入したウイルスを使って外との通信ラインを確保し、外部からウイルスを操作・誘導することによって情報の在りかを探らせ、その

情報を改ざんしたり搾取をしたりします。時には、破壊を目的とした攻撃を行うこともあります。特に注意をしなければならないのは、特定の企業等を狙った標的型サイバー攻撃で、入念な事前調査により狙った企業・組織のセキュリティ上の弱点をしっかりと調べ上げ、その弱みを巧みについて攻撃を仕掛けてきます。そして、その攻撃が成功し大量の情報が漏えいした場合、企業にとっては莫大な金銭的被害が発生するとともに社会的信頼が失墜し、経営に大きな影響を与えてしまいます。

では、このサイバー攻撃の恐ろしさを現実として意識している方がどれだけいるでしょうか。企業の機密情報が漏えいした場合は、企業側が実態を公表しないために、どのような被害が出たというようなことがよく分からない部分がありますが、顧客情報の漏えい等は報道等がなされ表面に出ることがあり、比較的わかりやすいのでその状況について紹介します。ＪＮＳＡ（日本ネットワークセキュリティ協会）の「２０１３年度情報セキュリティインシデントに関する調査報告書」によると、個人情報漏えいの年間想定損害賠償総額は、約１，４３９億円に上るとのことです。被害１件当たりの想定損害賠償額は、約１億１，０００万円になるそうです。サイバー攻撃による情報漏えいではありませんが、２０１４年に発生したベネッセの顧客情報漏えい事件では、被害者への補償で約２４０億、通信費や漏えい防止対策等で約２６０億、合計で約５００億円の経費が掛かったと言われています。

ＪＰＣＥＲＴ／ＣＣ※のＪＰＣＥＲＴ－ＰＲ－２０１５－０３によると、２０１５年の１／四半期に標的型攻撃等の高度なサイバー攻撃に遭っている可能性のある組織が６６あり、それらの組織に対して攻撃を受けている旨の通知を行ったそうです。そのうちの４４の組織が受けた攻撃は、日本年金機構への攻撃にも使われたＥｍｄｉｖｉと呼ばれる遠隔操作マルウエアに関連したものでした。Ｅｍｄｉｖｉを使った攻撃は、多数の国内組織に対して長期間に亘って行われており、個人情報等の様々な情報が搾取される被害も出ています。

サイバー攻撃に遭うことが、他人事ではなく身近なもので、一度被害が発生するとそれに対する保障や信頼回復に多額な費用と時間が掛かることを理解していただけたでしょうか。それでもまだ、自分が置かれているセキュリティ環境の危うさを実感されていない方に、現状を感じてもらえる例を紹介してみたいと思います。最近、インターネットのサイトにアクセスしたときに、自分の興味のある広告が表示される場合が多いことに気が付いていますか。それは、個人がアクセスした情報が、他のシステムを運用する会社にも送られて、情報共有が行われているからです。例えば、過去に京都について調べたことがあったとしたら、後日

※ＪＰＣＥＲＴ／ＣＣ：Japan Computer Emergency Response Team Coordination Center、コンピュータセキュリティの情報を収集し、インシデント対応の支援、コンピュータセキュリティ関連情報の発信などを行う一般社団法人

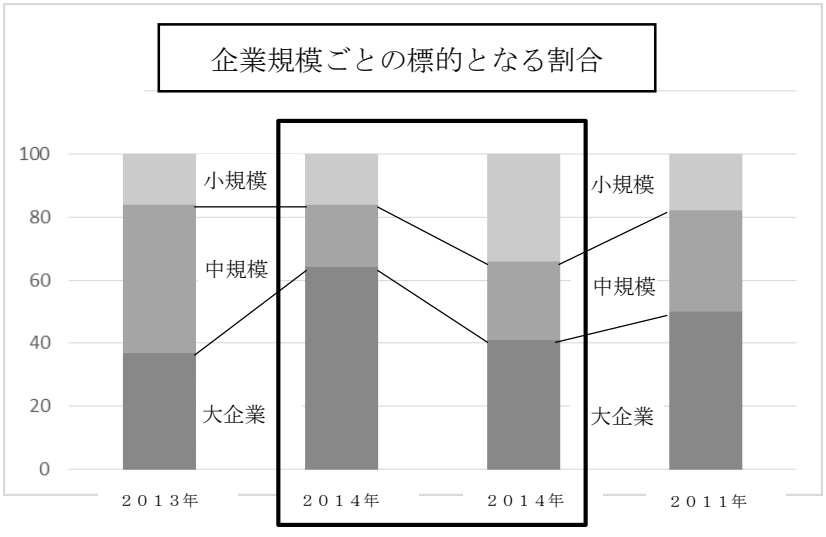
どこかのサイトにアクセスしたときに、京都旅行の広告が表示されたりします。この行為は、違法ではないと思いますが個人や会社の情報は意図しなくても簡単にネットの世界で出回り、それを悪意ある者が見つけた場合、この情報は攻撃の材料に使われます。このように、インターネット上のセキュリティは脆弱で、簡単に個人や会社の情報が取得されています。

３　ウイルス侵入阻止の困難性

サイバー攻撃は、パソコン等をウイルスに感染させることから始まると言いましたが、感染させる手段としては、メール等でウイルスが仕込まれた添付ファイルを送りつけてくる方法やＵＲＬなどを使ってウイルスを仕掛けたサイトに誘導する方法が大半を占めています。その他にも、ウイルスを仕込んだＵＳＢやＣＤなどを直接接続させウイルスに感染させる方法もあります。この様に攻撃の方法が分かっているのであれば、何とかウイルスの侵入を防げるようにも思えるのですが、現実には守る側の対策がしっかり取られていなかったり、攻撃側の騙しのテクニックの進化の方が早すぎて対策が追いついていなかったりして、被害が発生しています。この後、攻撃を受ける側と攻撃を仕掛ける側のそれぞれの立場から、もう少し詳しく述べてみたいと思います。

（１）日本企業のセキュリティ対策の甘さ

下にグラフがありますが、このグラフを見てどのようなことを推測しますか。



企業規模の従業員数
小規模：１－２５０
中規模：２５１－２５００
大企業：２５０１以上
※Symantec インターネットセキュリティ脅威レポートを基に作成

世界規模では、大企業への攻撃の割合が２０１１年には５０％程度を占めていたものが２０１４年では３０％台まで減っているのに対し、日本では増えています。これは、企業責任者の情報セキュリティ対策への取り組みの差から出ているものです。情報を取る側の視点で見ると、価値ある情報を取りやすいところから取ろうとするのは当たり前のことだと思います。ですので、まずは、貴

重な情報を持っているはずである大企業を狙いますが、今世界の一流企業では、トップ自身が情報セキュリティの重要性を理解し、これを経営基盤の一環としてとらえ、予算や人をつけてセキュリティを確保しようとしています。ですので、世界規模の攻撃では、大企業の方が価値のある情報を持っているのは分かっているけど、ガードが固いので取れるところから情報を取るために、中小の企業へ攻撃を仕掛けているということが分かります。

一方で日本の企業では、トップを含め会社全体がそれほど情報セキュリティについての意識が高くなく、企業の責任者が積極的にセキュリティ対策に関与していることは少ないように思われます。ＩＰＡ※の「サイバーリスク管理の実態調査」によると、経営リスク分析を行っている会社は全体の３４％であり、ＣＩＳＯ（情報セキュリティ管理の担当役員）を設置している企業は２３．４％というのが現状とのことです。このような状況では、日本の企業は、セキュリティ対策に十分な経費を支出し、適正な人物を配置しているとは思われず、攻撃者は、日本の大企業からは情報が取れると踏んで攻撃を仕掛けているのだと思われます。

（２）攻撃の進化・多様化

最近のサイバー攻撃の手法は、新旧織り交ぜながら進化し、攻撃形態も直接・間接の攻撃を巧みに操りながら行うなど多様化してきています。特に、巧みに人の心理的な隙や行動のミスにつけ込むソーシャルエンジニアリングと呼ばれる攻撃手法は、いろいろな要素やジャンルを使いウイルスが付いた添付ファイルを開けさせようします。実際に行われた攻撃の例をまとめたものが、ＩＰＡテクニカルウォッチ「標的型攻撃メールの例と見分け方」で掲載されています。それを参考として“これまでに検出された標的型攻撃メールの特徴”をカテゴリに区分して作った表を添付資料として付けていますので、サイバー攻撃を見分ける参考にしてください。

また、攻撃の形態も変化してきています。攻撃者は、欲しい情報を持っている官公庁や大企業を直接狙ってきましたが、最近はそこのガードが堅ければ標的とする相手先を、関連する団体や下部の組織に属する企業にして攻撃するやり方が増えてきました。セキュリティの弱い業界団体や中小の企業を攻撃し、そこを通じて本命である企業の弱点を探し出し、または最初に侵入した企業を踏み台として関連する企業への攻撃を仕掛ける方法です。この攻撃は、「標的型サイバー攻撃の連鎖」と呼ばれ、これに関する注意喚起を関連する企業に通知している省庁もあります。

※ＩＰＡ（Information-technology Promotion Agency）：**独立行政法人情報処理推進機構**　日本における IT 国家戦略を技術面、人材面から支えるために設立された、経済産業省所管の中期目標管理法人たる独立行政法人

そして、攻撃の起点となるＣ＆Ｃサーバ※は、海外に設置されるケースがほとんどでしたが、最近は国内に作られるケースが急増しています。２０１３年では、攻撃ために使用されたＣ＆Ｃサーバのうち、日本国内に設置されたものは全体のわずか６％でしたが、２０１４年には６６％と大幅に増えています。海外との通信は、一般的ではないために不審な通信が発生していると判定されることがありますが、通信先を国内にすることで、攻撃の検知を回避しようとしているものだと思われます。

４　被害を局限するために実施すべき事項

守る側の弱点をなくし、攻撃側の攻め方に対応した防御を実施するためにはどうしたらよいのでしょうか。攻撃が複雑化・巧妙化する現時点においては、一つの手段だけで情報を守りきることは不可能です。情報を守るためには、複数の防御手段を構築すること、しかも攻撃を完全に防ぐことは困難であることを考慮して侵入をされた場合でも、被害を局限出来るような対策を講じなければなりません。そして、それを出来るだけ多くの人に理解してもらうことが必要です。特に、情報システムを利用する人たちに、不審な状況を簡単に見過ごすのではなく、ウイルスに侵入されたのではないかと疑う意識を持たせる環境を作り上げることが重要です。兆候は、極めて小さく、気付くことが難しい場合が多いので、個人個人の資質に任せるのではなく、全社を挙げてそれができるように風土や人材を育てることが必要です。そして、その気付きにより上がってきた情報を、素早く社内で共有し的確に対処できる態勢を構築しておかなければなりません。以下、そのために実施すべき事項について詳しく説明します。

（１）情報セキュリティの風土作り

情報セキュリティの風土作りとは、会社全体で「情報セキュリティを守る」という企業風土を作り上げることです。そのためには、まず情報セキュリティ活動の目的は何か、何を、何故守るのかを明確にして、会社としての方針を定める必要があります。その目的は、究極的に言えば「情報を守る」ための活動になりますが、その活動を行うことが「会社を守る」ことになり、最終的には「社員一人一人を守ること」につながることを、会社で働く人たち全員に理解させることが大切です。目的を理解することにより、会社としてのどのようにして情報を守るのか、そのために自分たちが果たすべき役割が何かということが他人事としてではなく、自分たちのこととして考えられるようになります。そして、それを理解させるだけではなく実際の活動として普及してゆくことも必要

※Ｃ＆Ｃサーバ（command and control server）：外部から侵入して乗っ取ったコンピュータを利用したサイバー攻撃で、踏み台のコンピュータを制御したり命令を出したりする役割を担うサーバコンピュータのこと。

です。最近は、情報セキュリティの方針を定める会社も多くなってきましたが、風土が出来るまでには至っていません。それは、情報セキュリティ方針を定めたことで安心してしまい、それを定着させられるように普及するという部分の活動が不足しているからではないでしょうか。情報セキュリティの活動は、経営層や一部の者が実施するのではなく、会社全体で行う活動であることの理解を徹底できれば、企業としての情報セキュリティ風土が出来上がり、会社全体のセキュリティレベルが向上します。

この情報セキュリティの風土を築き上げることによるセキュリティレベルの向上は、攻撃者が攻撃を躊躇するなどウイルスの侵入防止にも役立ちますが、侵入された場合でも、その後にかすかに発生する不審な状況に敏感に反応し、間髪をおかず会社全体で対応する態勢につながっていきます。

（2）社員のセキュリティ意識の向上

強固な情報システムを構築し、ウイルスの侵入を防げる装置を設置したとしても、そのシステムを使用する人は失敗を犯したり、設計者が予期しなかった行動をとることもよくあります。これを防止するためには、情報を取り扱う社員一人一人のセキュリティに対する意識を向上させておくことが大切です。

そのために最も有効な方法は、教育です。情報を守ることの意義や重要性を理解させ、それぞれが実施すべき手順や定められた規則を教えることでセキュリティ意識を向上させます。教育を実施する場合には、画一的な伝達行為で終わることなく、教育を受ける人たちが最も理解しやすい方法で、しかもその気になる手法を使うことが必要です。理解のしやすい方法としては、言葉だけで伝えるのではなく、ビジュアル的な要素を折り込んだ教材を活用し、目と耳の双方で理解させることが必要です。また、個人の理解度やレベル、取り扱う情報の関わり方に応じた教育ができるよう、ガイドブックを作成したり、ｅラーニングのような教材を活用することも効果的な方法です。

その気にさせる教育では、その会社のキーパソンになる人物を講師にあてたり、刺激を与えるために部外から著名な専門家を招いた講習を実施する等、教育受講者が情報保全の重要性を意識し、会社が抱いている危機感を共有できるような手法を工夫することが必要です。

その他では、保全強化期間を設定したり、ポスターや標語の募集を行いそれを掲示したりするのも有効な方法です。社員に情報セキュリティ活動というものが身近で、ごく普通に行うものだと感じさせることが必要です。そうすることによって、必然的に社員一人一人の情報セキュリティ意識が向上し、規則等の確実な履行や不審な事象に対する気づきが出来るようになってきます。

しかも、社員のセキュリティ意識を向上させることは、先に述べた情報セキュリティの風土作りにも直接関係しますので、会社として最も努力を傾注すべき事項だと思っています。

（３）連絡・報告態勢の整備

最近のサイバー攻撃は、手口が巧妙化され知らないうちにウイルスが侵入していると述べましたが、それでも攻撃が成功して貴重な情報が窃取されるまでには、何らかの兆候が見られることがあります。その兆候に気づくためには、先に述べた２つの事項が出来ていることが大事なのですが、一方で気づくことが出来た時に、直ちに会社全体で対処できるように連絡・報告態勢を整備しておくことも、被害を局限するために重要な事項です。サイバー攻撃への対処としては、いかに早く、しかもどのように組織的に対処するか、いわゆる初度対応が被害局限の成否を分けるといっても過言ではありません。

そのために、それぞれの部署ごとに連絡を受ける担当者を定め、その先に責任を持って報告に対処する責任者を明示しておくことが必要です。最初の第一報を受ける人は、職場単位ごとに定め、お互いが知っている範囲の人を担当とすることが一つのキーポイントです。これによって、不審情報かどうかの判定が難しいものでも気軽に連絡でき、かつ同じ職場なので素早い通知に至ります。さらにその先の責任者は、情報セキュリティに関する知識があり、的確な判断ができる人を当てる必要があります。これにより、疑わしき情報を見逃すことなく、しかも迅速かつ確実に対処できるようになります。

また、連絡・報告系統をチャートのような図にして、職場で社員が良く見えるところに掲示しておくことも、緊急時等に素早く通報等をさせる良い方法です。そして、人事異動等の際には、必ず報告・連絡系統を見直すことを習慣化する等により最新の状態にしておくことも、確実に情報を伝えるためには重要な事項です。

（４）履行状況の確認

情報セキュリティをしっかり行おうという風土が高まり、社員一人一人のセキュリティ意識が向上したとしても、同じような業務を長く続けていると隙やほころびが出てきます。これを防止するために、教育を行ったり強調月間を設けたりのような刺激を与えることも大切ですが、別の効果的な方法としては、実際に行っている業務の履行状況を確認するやり方があります。例えば、監査を実施するとした場合、受ける側は、指摘などを受けないために、事前に自分たちの行っている業務が規則等に則っているかどうかを自分たち自身で確認するようになります。一方で、確認を実施する側は、規則等できっちり規定したつもりでも、その解釈は人によって違うことがありますので、自分たちが意図したとおりのことが実際に行われているかどうかを実地に確認することができます。この様に、監査を行うことは、双方の面から業務の見直しが実施できる良い機会になります。

また、現場で実際にやっていることを見ることで会社の定めたセキュリティ対策が適切なのか、有効に機能しているのかが確認できます。セキュリティ対策

が業務の阻害要因になっているようであれば、その規則や手順はいつか守られなくなります。必要なセキュリティ対策を実施するため、ある程度の規制はやむを得ないことですが、必要以上の縛りをかけていることがあります。セキュリティは大切ですが、守られない規則等は全く無意味です。セキュリティ対策と業務の効率化の微妙なバランスを保ちつつ、セキュリティを確保するためにも、履行状況の確認を実施する必要があります。

決められた規則を確実に守るということは、ウイルスの侵入を防止するために重要な事項ですが、更なる効果として定められたことが常に適正に実施されていると、異常な状態に気がつきやすくなります。業務を行う者が、普段自分がシステム等を操作しているときに起こる事象をしっかり把握していると、不審な状況が発生したときに、いち早く察知できます。現場の履行状況の確認は、サイバー攻撃の気づきにも役立ち被害を局限するためにも不可欠です。

5　まとめ

信じられないような話ですが、２０１５年５月に発生した日本年金機構へのサイバー攻撃の際は、年金機構からの報告が厚生労働省の担当の係長のところで止まっていたということが判明しました。これは、ウイルスに感染するような事態を想定していなかったから、当然報告態勢の整備もできていなかったことが原因だと考えられますが、せっかく貴重な異常情報がもたらされたにもかかわらず、組織的に対処することが出来ませんでした。また、現場で実施していた業務も、規則に合致しない方法で行われていたこともわかりました。

現在のサイバー環境では、「自分の会社は攻撃を受けない。自分たちが狙われることはない。」と思うことは、自分勝手な判断であり、甘い考え方です。インターネットの世界では、無防備な個人や会社の情報が飛び交い、それを悪意ある者が探っているといった状況です。悪意ある者に狙われないようにすること又はサイバー攻撃を受けた場合も被害を局限するためには、人的な隙を作らないことが大切です。攻撃者に、この会社は手ごわいぞと思わせることが重要で、経営者自身がセキュリティ対策の実施に対する強い意志を表明し、それを中心に会社が一丸となって情報セキュリティ対策に取り組んでいる姿勢を見せる必要があります。

そのために、しっかりとした情報セキュリティ方針のもと社員一人一人に何をなすべきかを理解させた上でそれを実践させることにより、情報を確実に守るという情報セキュリティの風土を作り、教育等を通じて社員の意識を向上させ、何かあった時にすぐに対処するための連絡・報告態勢を整備する。そして、それらの状況を定期的に確認することで、規則等で定めた手順等が確実に実施されている態勢を常に確保しておくことが重要です。これらが欠けることなく機能することで、もしサイバー攻撃を受けたとしても、いち早く気づきその被害を局限することが出来ます。

強固なシステムの構築には、専門の知識が必要ですが、今まで述べてきたような人的対策については、やる気さえあれば実施可能です。一人でも多くの人をその気にさせ、セキュリティに対する高い意識を保持させなければなりません。そして、万が一サイバー攻撃を受けた時にはいち早く気づき、会社の各部門が組織的に活動して被害局限が図れる態勢を整備しておくことが、会社やそこで働く人を守るために必要な手段です。攻撃はいつ起こるか分かりません。人的対策を含めたセキュリティ対策の必要性を理解する人を増やし、セキュリティを確保して、サイバー攻撃に備えておくことが肝要です。

（参考資料）

IPA　ＩＰＡテクニカルウォッチ「標的型攻撃メールの例と見分け方」
　　企業におけるサイバーリスク管理の実態調査２０１５
JPCERT　JPCERT/CC 活動概要【２０１５年４月１日から２０１５年６月３０日】
JNSA　「２０１３年度情報セキュリティインシデントに関する調査報告書」
Panasonic　情報セキュリティ教育（ブレンディング教育活用）
Symantec　インターネットセキュリティ脅威レポート
TREND MICRO　標的型サイバー攻撃の段階的手口を徹底解説

添付資料

標的型攻撃メールの例と見分け方

番号	区　　分	これまでに検出された標的型攻撃メールの特徴
1	メールのテーマ	① 知らない人からのメールだが、メール本文のURL※や添付ファイルを開かざるを得ない内容 ※Uniform Resource Locator：ウェブサイトのようなインターネット上のリソース（情報等）を表すために使われるもの （例1）新聞社や出版社からの取材申込や講演依頼 （例2）就職活動に関する問い合わせや履歴書送付 （例3）製品やサービスに関する問い合わせ、クレーム （例4）アンケート調査 （例5）やり取り型メール※ ※普通の問い合わせメール等を送り、その後何回かメールをやり取りして、相手が安心した時にウイルスが付いた添付ファイルを送りつける攻撃方法
		② 心当たりのないメールだが、興味をそそられる内容 （例1）議事録、演説原稿などの内部文書送付 （例2）VIP 訪問に関する情報
		③ これまで届いたことがない公的機関からのお知らせ （例1）情報セキュリティに関する注意喚起 （例2）インフルエンザ等の感染症流行情報 （例3）災害情報
		④ 組織全体への案内 （例1）人事情報 （例2）新年度の事業方針 （例3）資料の再送、差替え
		⑤ 心当たりのない、決裁や配送通知（英文の場合が多い、ただし昨年末から日本郵政を騙った不審メールが急増する等日本語を使った攻撃も増加） （例1）航空券の予約確認 （例2）荷物の配達通知
		⑥ ID やパスワードなどの入力を要求するメール （例1）メールボックスの容量オーバーの警告 （例2）銀行からの登録情報確認
2	差出人のメールアドレス	① 企業等からのメールを装っているが、フリーメールアドレスから送信されている

番号	区　　分	これまでに検出された標的型攻撃メールの特徴
		② 差出人のメールアドレスとメール本文の署名に記載されたメールアドレスが異なる
3	メールの本文	① 日本語の言い回しが不自然である
		② 日本語では使用されない漢字（繁体字、簡体字）が使われている
		③ 実在する名称を一部に含む URL が記載されている
		④ 表示されているURLと実際のリンク先のURLが異なる（例えばHTMLメール※の形式で送ってきたものなど） ※HTML（Hyper Text Markup Language）メール：電子メールの本文をHTML形式で作って、ウェブページのような見た目にしたもの
		⑤ 署名の内容が誤っている （例1）組織名や電話番号が実在しない （例2）電話番号がFAX番号として記載されている
4	添付ファイル	① ファイルが添付されている
		② 実行形式ファイル(exe/scr/cpl など)が添付されている
		③ ショートカットファイル(lnk など)が添付されている
		④ アイコンが偽装されている （例1）実行形式ファイルなのに文書ファイルやフォルダのアイコンとなっている
		⑤ ファイル拡張子が偽装されている （例1）二重拡張子となっている （例2）ファイル拡張子の前に大量の空白文字が挿入されている （例3）ファイル名にRLO※が使用されている ※RLO（Right-to-Left Override）：Unicode制御文字の一種で、横書き文字の左右の並びを逆にするために用意されている記号 （例4）エクスプローラで圧縮ファイルの内容を表示するとファイル名が文字化け