知らないとキケン！

メール利用に潜むリスクと対策とは?

Chatwork

目次

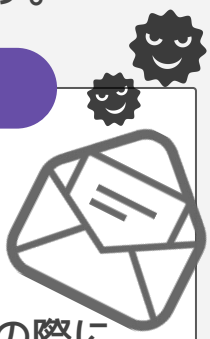
01

メールに潜む
リスクを考える

メールのリスク対策が必要な理由

メールは、幅広く利用されている息の長い「コミュニケーション手段」ですが、それだけにビジネスで利用する際には”情報管理”や“セキュリティ面”に責任を持って利用する必要があります。普段は気づかないリスクが、何気ないやりとりに潜んでいることを忘れないようにしましょう。本資料では、大事故につながらないためのメールのリスクを明らかにし、打てる対策を紹介します。

リスク対策が必要な主な理由



01 外部からの予期せぬ攻撃にあう可能性がある

メールは第三者からの攻撃対象として、格好の的です。初期設定のままでメールを利用している場合は、送受信の際に「POP3」「SMTP」「IMAP」といったメール専用のプロトコルが採用されていますが、「暗号化」などのセキュリティ対策がなされていないケースが多いために、外部からの予期せぬ攻撃にあうリスクが高まります。

02 無駄な時間や精神的労力を伴う非効率業務に陥る

標準の設定では、メール送信後の取り消しが不可能なためミスなく送信するために気をつけるだけでも、多くの時間や精神的な労力を消費します。安心して効率よく日常業務が遂行できる対策は不可欠です。

03 取引先などの関係者に迷惑をかける場合がある

取引先の機密情報をメールで漏えいしてしまった場合など、自社経由のトラブルは、たとえ意図していなくても関係者に迷惑をかけ“信頼”を失ってしまいます。賠償問題に発展するケースもあり、一度無くしてしまった信頼の回復には多大な努力が必要になります。

メール利用に潜むリスクの種類（01）

本資料で取り上げる「6つのリスク」は、メールをビジネスで利用している社会人が、日常の業務活動で直面する可能性がある項目をとりあげています。
知識として正しく理解し、対策を講じる際に役立てましょう。

ビジネス利用の「6つのリスク」

01：メールの盗聴・改ざん

メールの盗聴とは、攻撃的な第三者が「暗号化」されていないテキストの内容をのぞき見ている状態を指します。

送信者から受信者に届けられる経路はネットワークでつながったメールサーバーを複数経由しますが、その間に盗聴されるリスクが発生します。
また、受信されるまでの経路でテキスト内容を書き換えられる被害が報告されています。

02：フィッシング詐欺

悪意のある第三者が偽装のウェブサイトに誘導するために、送信者名や内容自体を偽装して無差別に送るメール詐欺です。

記載されたURLなどをクリックすると、遷移先が本物のウェブサイトに真似て作られているため、気づかないうちにクレジットカードや暗証番号を入力してしまうケースがあります。

メール利用に潜むリスクの種類（02）

03：標的型攻撃メール

攻撃的な第三者が、事前に“ターゲット”を絞り、そのターゲットのビジネスに関連のありそうな件名のメールを送信してきます。内容に具体性が見られるため、より巧妙です。

フィッシング詐欺のメールが不特定多数をターゲットにしているのに対し、ある程度の狙いを定めて接触してくるのがこのタイプです。

04：なりすましメール

攻撃的な第三者が、”実在する人物や会社”を偽り、本人とは別のメールアドレスを設定して、メールがあたかもその関係者から送信されたように見せかけるものを指します。

差出人に見慣れた氏名や、本物と紛らわしいアドレスで送られてくると、リスクをともなうメールであることを見抜くのが困難になります。

特に、”関連会社や自社のCEO／CFOなど、組織トップの人間”と偽って受信者を欺き、社外に送金させたり情報を盗み取る被害として、ビジネスメール詐欺（BEC / Business Email Compromise）が報告されています。
綿密な事前計画のもとに連絡してくるため、心理的な隙や判断ミスを誘発し、至って悪質です。

メール利用に潜むリスクの種類（03）

05：マルウェアに感染する

マルウェアは、利用者にとって不利益になる挙動を実行する目的で作られた、悪意のあるソフトウェアやプログラムを指します。それによってPCやタブレット、スマートフォンなどの不具合を引き起こし誤作動を生じさせたり、端末に保存されたデータを盗み取る被害も起きています。

近年は、ランサムウェアと呼ばれる身代金を要求するウイルス被害も増えています。

06：従業員による情報漏えい

メールによる情報漏えいは、攻撃的な第三者による外部起因のリスクだけでなく、意図する・しないに関わらず、従業員のメール利用から発生するケースが多数報告されています。

よくありがちな事例は、意図しない誤送信です。予期しない相手に謝って送信してしまう場合など、アドレス欄に宛先の候補が表示される「オートコンプリート機能」を利用している場合に頻発しています。他にも「一斉送信」する際、本来であればBCCで受信者同士のアドレスが閲覧できないようにするものをTOで配信してしまうといった事例では、多くの受信者に迷惑をかけてしまうために何度も確認するなど注意が必要です。

特に、重要な機密情報や個人情報などを本文に直接記載したり、添付ファイルにパスワード設定をせずに誤って送信した場合には、重大なインシデントに発生する可能性があり、会社の信頼度を低下させます。

02

メール利用のリスクを回避する対策法

セキュリティ対策の有無が明暗を分ける

明確な対策をせず、メールを介して重大なインシデントが発生した場合には、業務やサービスの停止を余儀なくされたり、取引先や関連会社への二次被害につながり、信頼関係に支障が出たり、損害賠償や行政指導にまで発展するといった散々な事態に見舞われることが起こりえます。
また、情報の漏えいや改ざん・紛失の回復には多大な時間やコストがかかり、会社のマイナス成長につながり、著しい生産性の低迷を引き起こします。

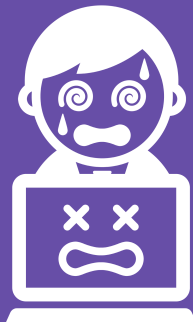
差出人を偽造したり、送受信の過程で盗聴される可能性がともなうメールの利用には、さまざまなセキュリティのリスクが存在していますが、最新の知識を事前に調べ、はやめの対策をおこなうことで、脆弱なセキュリティホールを防げる施策が数多くあります。

特に、次々と新しい脅威を巻き起こす、第三者からの攻撃的メールのリスクを回避するために、実現性を考慮した上で、可能な限りの“事前対策”を実施してください。

対策は“2つの側面”から攻略する

外部からの
「不正侵入・不当攻撃」

内部からの
「人的ミス・認識不足」



メールに潜むリスクには、「外部」と「内部」の両面に向けた対策をそれぞれ講じる必要があります。

リスク回避の対策法（01）

メール利用のリスクを回避するために、会社で取り入れたい対策法を6つと、参照情報を紹介します。

リスクを回避する「6つの対策」

☑ ウイルス対策ソフトを導入する

サイバー攻撃を検知して駆除するウイルス対策のソフトウェアを導入することが有効です。脆弱性の対策やインターネットを通して侵入してくる不正なアクセスを阻止する「ファイアウォール」など、総合的な機能を備えた製品を導入することが肝心です。また、利用の際には、自動更新されるように設定するなど全社的な対応が望まれます。

☑ メールを暗号化する

暗号化は、メール本文や添付ファイルの内容を、他者に知られないように加工・処理する技術です。現在では、標準で暗号化されているメールサービスも増えてきています。まずは自社の利用しているサービス状況を把握しましょう。

暗号化のポイントは「通信経路」や「メール本文」だけでなく、「添付ファイル」にも暗号化が施されていることです。
また、暗号化の機能がついていないサービスを採用している場合は、暗号化の専門ツールを別に採用することが可能です。
無料版のツールも存在しますが、アカウント数が限定されていたり、互換性がないものもあります。

導入には別途コストが発生することも想定し、十分考慮して検討する必要があります。

リスク回避の対策法（02）

HTMLメールを利用しない

HTMLメールは、Webサイトなどで利用されているプログラム言語（HTML）を用いて、「テキストメール」では実現できない、文字の色や太さを個別に装飾するなど、表現豊かなメール形式です。メールマガジンなど、見栄えを重視する用途でよく利用されていますが、HTMLメールはプログラムを記述できるため、マルウェアなどのターゲットになりやすい面があります。安全性を考慮して、極力HTMLメールを避け、テキストメールでの使用がおすすめです。

迷惑メールフィルターを設定する

多くのメールシステムでは、「なりすまし」などの有害メールを、誤って開封しないように、迷惑メール（スパムメールとも呼ばれる）として任意のフォルダに振り分ける「フィルター機能」が用意されています。

あらかじめ、メールシステム側で設定した、高機能の振り分け技術の機能を活用したり、差出人や件名の文字を指定しておくことで、該当するメールを受信しないように設定することも可能です。メールシステムのサービス業者は日々進化している脅威に対応できるように対策していますが、フィルターをくぐり抜けようとしてくる攻撃的な第三者との「いたちごっこ」であるため、怪しいメールは絶対に開かないという姿勢が大切です。

以前は日本語が不自然などわかりやすいケースが大半でしたが、近年は人事採用受付メールに、応募者を装ってマルウェアを仕込むなど巧妙化しています。初めて送信されてきた宛先からの開封には十分な注意が必要です。

リスク回避の対策法（03）

☑ 誤送信防止の機能を活用する

メールの誤送信は、人的ミス（ヒューマンエラー）として認識されているトラブルの代表格ですが、1日に大量のメールをやりとりする必要がある利用者の場合には、本人の注意力のみに頼るだけでは防ぎきれません。

大抵のメールシステムでは、送信メールを一時保留してから送信できる「時間差」機能や、添付ファイルを「自動暗号化」してくれる機能を備えています。

☑ 全社包括的な注意・喚起

どこか1つの抜け穴があれば全社的に被害が拡大します。
そのため全社的に注意喚起を促すために「社内のガイドライン」を作成して共有したり、 最新のセキュリティ情報を調べて定期的に注意喚起する担当者がいるとリスク軽減に役立ちます。

- **セキュリティ情報例：情報セキュリティ10大脅威 2021**

https://www.ipa.go.jp/security/vuln/10threats2021.html

社内で「コンプライアンス研修」を実施している会社も増えていますが、メールのリスクなどについての項目を追加し、定期的な注意喚起の機会の場として活用することも有効です。
また、万一トラブルが発生した場合は、速やかに詳細を調査したのちに、全社員に情報共有する体制が重要です。

リスク回避の対策法（参考情報：その1）

参照情報

その1：DMARC（ドメイン認証技術）

一般の従業員にはあまり馴染みがなく、専門的な内容になりますが、攻撃的な第三者からの有害メールをより厳格に排除しようとする場合、DMARCが有効です。この技術は以下2つの技術（SPFおよびDKIM）の機能を拡張した「ドメイン認証技術」として活用されています。

SPF
受信するメールの通信経路や差出人が正当かどうかを、任意の情報に問い合わせ・判断する技術。

DKIM
送信するメールに「電子署名」を発行し、受信者がそれを検証した場合に、万一ドメイン自体やメール内容の改ざんがおこなわれていた場合に、検知する技術です。

DMARCは“受信する立場”と“送信する立場”として、大きく2つの機能を持っています。

- **受信する立場として、メール受信時にSPFやDKIMがうまく機能せず、対象のメール検証に失敗した場合、その後の処理を指定できます。**
  （例えば「受信を拒否する」「迷惑メールとして隔離する」などの指定が可能です）
- **送信する立場として、自社のメールドメインになりすましたメールが発信された際、その情報を受け取る機能があります。**

特に後者は、取引先などの関係者への被害を食い止める役割を果たすために、対策強化として用いられています。自社を名乗った被害が確認された場合には、特に有効な対策手段です。

リスク回避の対策法（参考情報：その2）

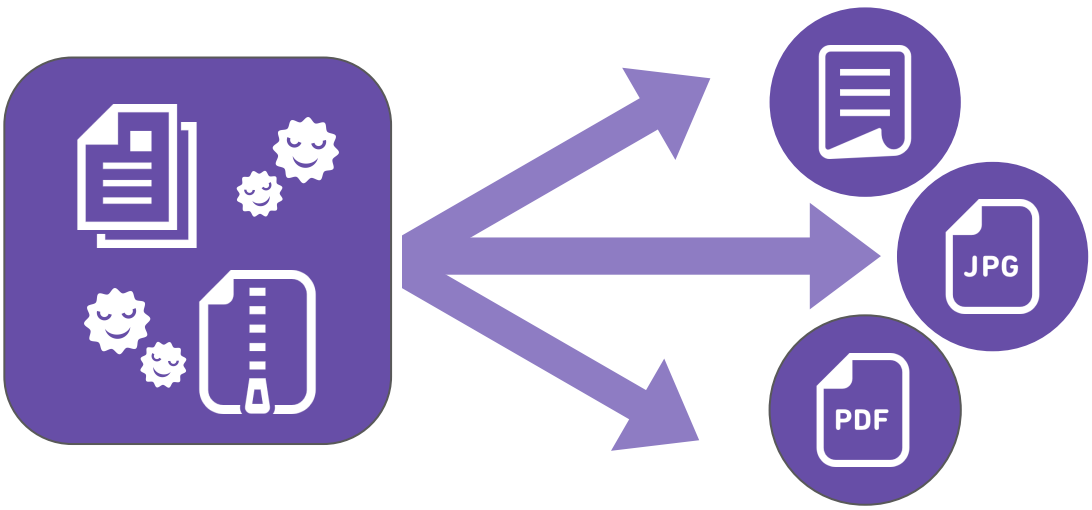
参照情報

その2：メールの添付ファイル無害化

多くのマルウェアや不正なプログラムは、メールの「添付ファイル」に仕込まれています。

被害を受けないためには、不審な添付ファイルは開かないことが大切ですが、業務で確認しなければならないケースが多々あります。安全に中身を確認したい場合、ファイルの内容を「テキスト」に変換して表示したり、「画像」や「PDF」として変換したのちに確認できるサービスがあります。

不特定多数からのメールを受信する業務がある場合には、このような無害化に特化したメールサービスを利用するのも有効な手段です。メールの本文やURLが記載れているリンクなども無害化する機能を備えているものもありますので、用途に合わせて検討してください。



マルウェアなどが仕込まれている攻撃的な添付ファイルなどを
本文のテキストや画像・PDFファイルに変換して無害化する！

ビジネスチャットでリスク回避

ビジネスチャットで、情報漏えいなどの重大なインシデントの機会を削ぐ

現在、メールを起点とした情報漏えいやトラブルが増えています。社外での利用が一般化されており、今後も継続利用が想定されますが、「社内環境」をメール脅威の連鎖から断ち切る方法として、「ビジネスチャット」に置き換えるという選択肢があります。

ビジネスチャットでは、従業員や社外の関係者もあらかじめ設定した人しかアクセスできないため、不明な相手から連絡がくることがありません。

また、宛先を指定して入力する手間や時間もカットして効率よく連絡することが可能で、トラブルの回避だけでなく、気軽なコミュニケーション手段として活用できる機能が充実しており、業務効率をアップさせます。
そのため「社内のコミュニケーション」を、メールからビジネスチャットに切り替えている会社が増えています。

安心のセキュリティ
ビジネスチャット「Chatwork」

Chatworkは、銀行レベルのセキュリティ水準を満たしています。

https://go.chatwork.com/ja/security/

ITスキルに不安のある従業員も利用できる、わかりやすい画面設計のため、余分な負荷がかからず本来業務に集中してもらえます。特に度重なる「メール対策」に追加コストがかかりすぎている場合は、社内のコミュニケーション改善案として一度検討ください。

01章：メールに潜むリスクを考える
まず最初に、コミュニケーション手段として定着しているメールのやりとりには注意が必要で、「リスク対策」が不可欠な理由を3つ紹介しました。
次にビジネスで利用する場合に想定されるリスクを6つにまとめ、対策の準備知識として理解していただきたい内容を掲載しました。

02章：メール利用のリスクを回避する対策法
リスク回避の対策を立てる考え方として、2つの側面（1つは「外部」に起因した“第三者からの攻撃的なメール”に対するもの、もう1つは「内部」に起因する“人的なミスや過失、あるいは認識不足”の側面）からのアプローチが必要であることと、具体的な対策法について明記しました。

メール・セキュリティの見直しを
現代は「テレワーク」などに代表される“従来とは違う働き方”が求められる時代になりました。今までは会社のオフィス内で作業することで頑丈に守られていた“セキュリティ対策”も、働き方の多様化により、硬い守りを維持しきれなくなってきています。
従来型とは別の「ゼロトラスト（全ての通信ネットワークやデバイスなども“信頼できないもの”として捉える考え方）」としての見直しを迫られています。
特にメールは「送信者を特定できない不特定の入り口」であるため、大きなリスクも抱えています。
正しい知識と対策で時代に即したコミュニケーション手段を実現してください。

会社概要

社名	Chatwork株式会社
所在地	〒105-0003 東京都港区西新橋１丁目１-１ WeWork 日比谷FORT TOWER
設立	2004年11月11日（創業：2000年7月15日）
資本金	1,374,906,693円
代表者	山本正喜
事業	Chatworkの開発運営 ソフトウェア販売（ESETセキュリティソフト）
URL	https://corp.chatwork.com/ja/

シゴトがはずむ

Chatwork

本資料についての問い合わせや相談は
以下まで連絡ください。

問い合わせフォーム

Chatwork製品サイト
https://go.chatwork.com/ja/