メールウイルススキャンについて

●ウイルスメールについて

ウイルスは、あなたのパソコンにさまざまなかたちで入り込んできます。その中でも、感染リスクの高いものとしてメールを媒体とする種類のウイルスです。一番の安全策はキケンなメールを開かないことですが、最近のウイルスは、メールやファイルを開きたくなるような、魅力的な名前がついていたり、そのつもりがなくても自動的に開いてしまったりするものもあります。

ひとたび感染すると、PC内に保存しておいたはずの大切なファイルが消えたり、パソコンの動作は不安定になったりと、さらにアドレス帳から集めたメールアドレス宛てに、自動的にウイルス自身を潜ませたメールを発信、どんどん被害を拡大させていく、大きな打撃を受けます。最悪の場合は、PCの初期化をしないといけなくなり、また、自分だけでなく他人に迷惑をかけてしまう可能性もあります。

●メールウイルススキャンについて

Kビジョンのメールサービスでは、“メール”にウイルスがついていないかどうか、チェックする仕組みが組み込まれています。それが『メールウイルススキャン』です。

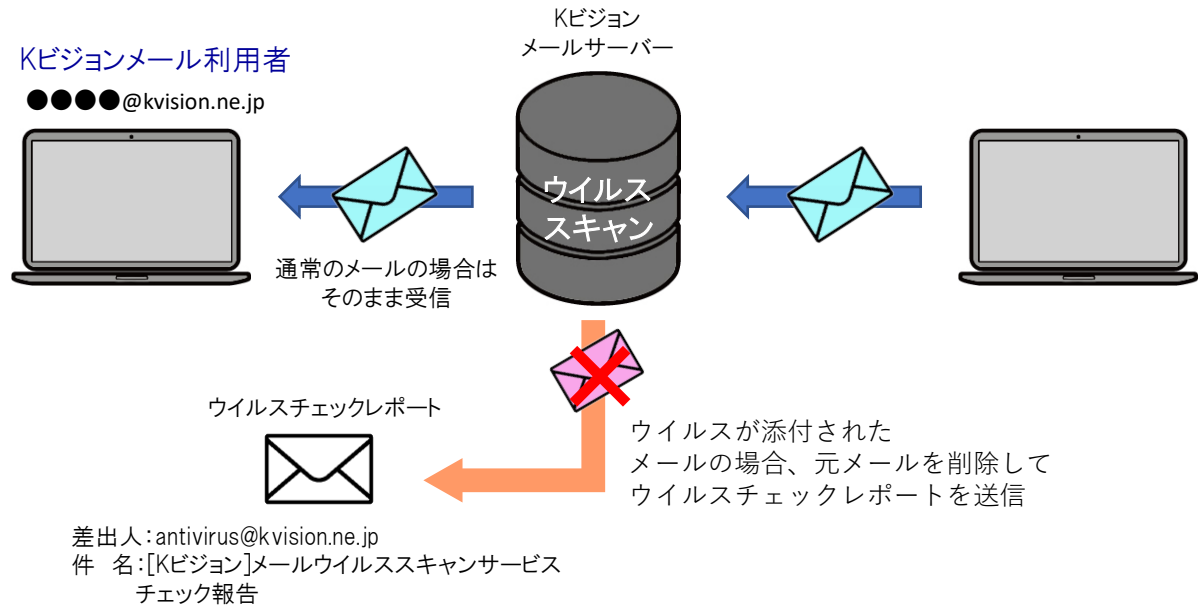
メールに、スキャン時点で認識済みのウイルスがついていた場合は、ウイルスを駆除した上で、ウイルス部分以外は通常のメールと同じように送受信されます。メールサーバーでは、ウイルス定義ファイルの提供状況を毎時確認し最新のウイルスデータベースに更新することにより、チェック体制を整えています。

※未知の新しいウイルスの場合、スキャン対応ができていない場合があります。
※『メールウイルススキャン』は、メールを媒体として感染するウイルスをスキャンするサービスです。ホームページなど他の媒体のウイルスは駆除できません。

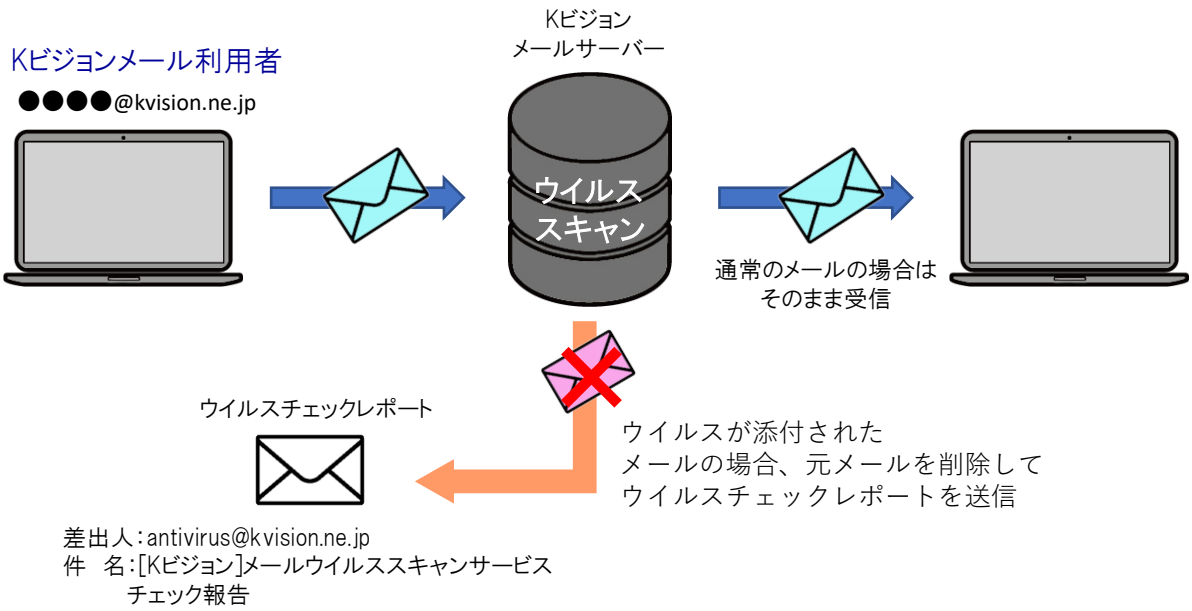
メールウイルススキャンサービスの概要

「メールウイルススキャンサービス」は、メールの送受信時にウイルスをメールサーバでスキャンし、ウイルスが発見された場合は自動削除します。

メール受信時



メール送信時



ご利用上の注意点

◆「メールウイルススキャンサービス」は、Kビジョンのメールアドレス（～@kvision.ne.jp）でご利用いただくことができます。
◆「メールウイルススキャンサービス」は、メールを媒体として感染するウイルスをスキャンするサービスです。ホームページやフロッピーディスクなど他の媒体のウイルスは駆除できません。
◆ウイルス、もしくは該当ファイルの削除を行った場合、システム管理者よりウイルスチェックレポートが送付されます。
◆以下の形式の圧縮ファイルに潜むウイルスの検知、削除を行います。
ARJ、Z、TAZ、GZ、TGZ、RAR、TAR、ZIP、LHA、LZH、EXE、BIN、HQX、UUE、BZ2、TBZ、TBZ2、SIT、CHM、HXS、RPM、A、CAB、XSN
◆送信者の添付したファイルが下記のパターンに一致する場合は、ウイルスを検出できない為、ウイルススキャンを行なわずにそのまま送信されます。
1.パスワードで保護されたファイル
2.分割メール
3.暗号化されたメール
4.ウイルススキャンが対応していない新種のウイルス、未知のウイルス、圧縮ファイル
◆送信者の添付したファイルが、下記のパターンに一致する場合やその他の理由により正常にウイルススキャンが実行できなかった場合はメール全体を削除します。送信先、送信元へは通知いたしません。
1.圧縮レベルが6階層以上の圧縮ファイル
2.破損したファイル

ウイルススキャンによりウイルスを検知した場合の
ウイルスチェックレポートサンプル

======= メールウイルススキャンサービス チェック結果報告 ======

このメールからウイルスが検知されたため、ウイルスを削除いたしました。

ウイルス(″<ウイルス名>″)が(″<検出場所>″)から検出されました。
実行された処理:メールの削除

差出人: <オリジナルメールの差出人>
件名: <オリジナルメールの件名>
送信日時: <オリジナルメールの日時>
検出場所:
ウイルス名:

メールウイルススキャンサービスに関する詳しい情報は、
http://www.kvision.ne.jp/knet/services/virusscan/function.html
の「メールウイルススキャン:メールウイルススキャンの概要」をご参照ください。

※メールウイルスチェックレポートはシステムより自動配信されています。
このメールに返信されても、内容の確認およびご返答ができません。
==========

Kビジョン株式会社