サイバー犯罪対策通信

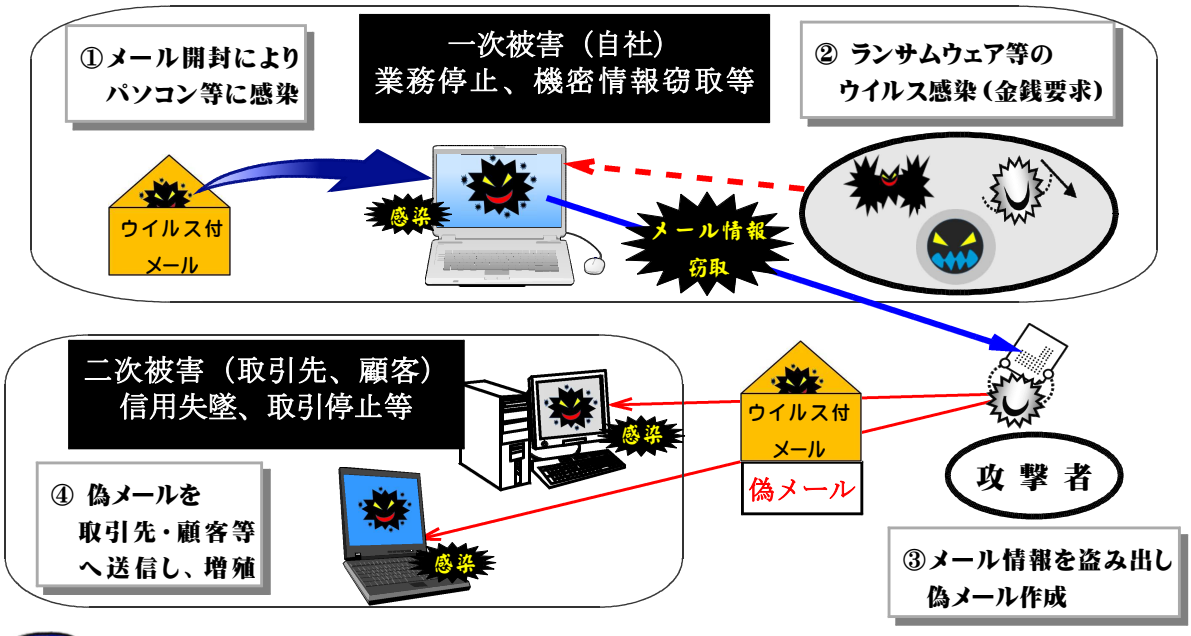
大阪府警察本部サイバー犯罪対策課

巧妙な偽メールで拡散するウイルス感染多発

最近、企業や行政機関等のパソコンに対し、実在のメールデータを流用して業務連絡を装い、「エモテット（Emotet）」と呼ばれるウイルスを添付した偽メールが送りつけられ感染してしまう被害が多発しています。

エモテットの特徴は、感染したパソコンに登録している取引先等のメールアドレスに同様のメールを自動的に送信し、さらに感染を拡大させる点です。

また、添付ファイルを開くと、パソコン内のデータを暗号化して使用できなくするランサムウエア等に感染し、復旧名目の金銭を要求されてしまいます。



自社の業務停止や機密情報が盗まれるだけでなく偽メールをばらまく“**間接的な加害者**”となってしまいます。

対策方法を確認！

ウイルスが添付される偽メールは、確認されているだけでも
取引先等からの正規の返信メール、セキュリティ関連会社のアンケート依頼
保健所からの新型コロナウイルス予防の呼びかけ
等、多種多様で、文面や差出人等から怪しい点を見分けることは非常に困難なため

◎ 身に覚えのないメールの添付ファイルは開かず、メール本文のURLリンクもクリックしない

◎ 自分が送信したメールへの返信メールのように見えても、返信のタイミングや内容に違和感があれば、添付ファイルを開かない

等の対策をしてください！

「Ｅｍｏｔｅｔ」についてさらに詳しい情報を大阪府警ホームページ上に掲載しています！
【https://www.police.pref.osaka.lg.jp/seikatsu/saiba/cyber_cyuikanki/9749.html】
『メールの情報を盗み出すマルウエアに注意！』