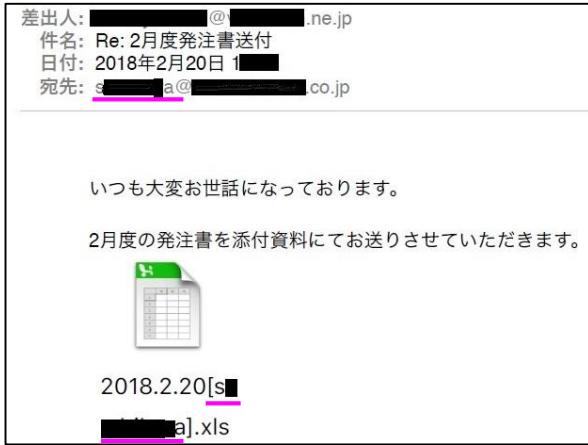


あさまセキュリティニュースレター



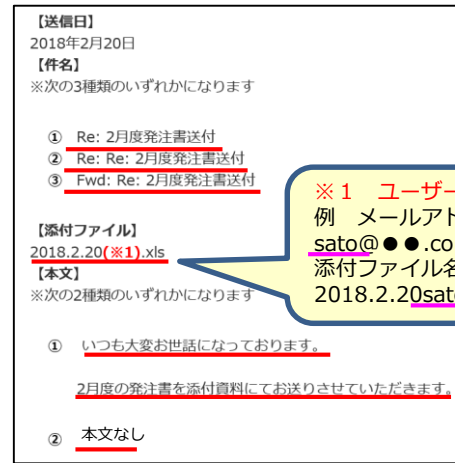
添付ファイル名に自分の名前が入ったメールに再要注意！！(2018年2月21日)

今年も添付ファイルに自分の名前が？



※実際にお客様先に届いたメールを一部加工

JC3のウイルス付きメール情報と一緒に



※1 ユーザー名
例 メールアドレス
sato@●●.co.jpの場合
添付ファイル名
2018.2.20sato.xls

添付ファイル名に自分の名前
(自身のメールアドレスの@
の前の部分)が付与されてた
メールが再度出現！！



弊社お客様先
でも検知済み

処置	時間	コンテンツ名	RECIPIENTS/POP3 USER
削除済み	2018-02-19 17:38:08	19.2.18[eigyout].xls	eigyout@[redacted].com
削除済み	2018-02-20 16:45:01	2018.2.20[eigyout].xls	eigyout@[redacted].com

攻撃のパターン

- メール受信者に関係する添付ファイルと思わせ、ファイルを開かせる
- 不正送金、キーローガー、ボット（遠隔操作）、情報搾取、ランサムウェア等攻撃を実行

被害

不正送金被害

入力した情報の搾取、情報の不正利用

遠隔操作による第三者へ勝手に攻撃、外部へ情報送信

ファイルの暗号化、身代金の要求等の可能性

対策

- 件名や添付ファイル名に惑わされない、差出人が知人の場合、相手に確認する
- 不審なメールは開かない、開いてしまった場合でも、添付やリンクはクリックしない
- 最新の脅威を知る、手口を知る、全社員がセキュリティに対し意識をもつ

最新のウイルスメールの具体例があるJC3のサイトで情報収集を！
https://www.jc3.or.jp/topics/vm_index.html

情報源

JC3 日本サイバー犯罪対策センター <https://www.jc3.or.jp/>

ウイルスメール INDEX版

※青字は右記のランダムな文字列が入ります A: 英字 X: 英字または数字 0: 数字

※赤色の表示はウイルス検出は、ブラウザの機能(CSP)が動作していません 最新の身体例はこちら

送信年月日	件名	添付ファイル	本文
2018/02/20	①Re: 2月度発注書送付 ②Re: Re: 2月度発注書送付 ③Fwd: Re: 2月度発注書送付	2018.2.20[※1].xls [※1]ユーザー名	本文
2018/02/19	①Re: 2月度発注書送付 ②Re: Re: 2月度発注書送付 ③Fwd: Re: 2月度発注書送付	19.2.18[※1].xls [※1]ユーザー名	本文
2018/02/16	あなたのApple IDがセキュリティ問題で再設定してください。		本文
2018/02/14	①Re: 2月度発注書送付 ②Re: Re: 2月度発注書送付 ③Fwd: Re: 2月度発注書送付	2018.02[※1].xls [※1]ユーザー名	本文
2018/02/06	カード利用の取戻し		本文