

# あさまセキュリティニュースレター



請求書や注文書メールに再度要注意を！！ (2018年11月14日)

## JC3の最新のウイルス付きメールの具体例 抜粋

送信年月日	件名	添付ファイル	本文
2018/11/12	Apple IDアカウントを回復してください		<a href="#">本文</a>
2018/11/12	こんにちは！		<a href="#">本文</a>
2018/11/11	こんにちは！		<a href="#">本文</a>
2018/11/10	【楽天市場】注文内容ご確認（自動配信メール）		<a href="#">本文</a>
2018/11/6	①立替金報告書の件です。	Doc06112018200000000.xls	<a href="#">本文</a>
	②申請書類の提出		
	③注文書の件		
	④請求データ送付します		
	⑤納品書フォーマットの送付		
2018/11/6	①請求書	2018110600000.xls	青数字はランダムな数字
	②10月5日付の管理費請求書		
	③別注お支払いの件		
	④ご請求書		
	⑤10月課金請求リスト		
	⑥～請求書11月1日～		
	⑦【再送】30年10月分請求書		
	⑧10月請求書 郵送のご連絡		
	⑨11月請求書連絡		

件名 **請求書**というメールで、**添付のエクセルを開き確認し、経理担当にメール転送。**

経理担当のPCに入っていたウイルス対策ソフトでウイルス検知したため、ご相談が・・・

開いた方のPCは**OS標準のウイルス対策のみ**で、警告・検知もなかったため、経理担当と同じウイルス対策ソフトで検査し、**3件検知・駆除！**

他のお客様でも、同様なメールを検知削除した履歴が！！

処置	時間	脅威レベル	コンテンツ名
削除済み	2018-11-06	high	2018110665985.xls
処置	時間	脅威レベル	コンテンツ名
削除済み	2018-11-06	high	2018110699311.xls
処置	時間	脅威レベル	コンテンツ名
削除済み	2018-11-07	high	2018110644810.xls

複数社で同様な脅威を検知済み



## 攻撃のパターン

- 業務に関係する添付ファイルと思わせ、ファイルを開かせる
- 不正プログラムがダウンロードされ、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

不正アクセス  
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

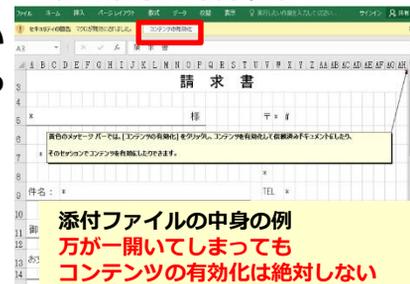
- 件名や添付ファイル名に惑わされない、差出人が知人の場合でも、不審なメールは相手に確認する
- 不審なメールを開いてしまった場合でも、添付やリンクはクリックしない
- 最新の脅威を知る、手口を知る、**全社員**がセキュリティに対し意識をもつ

## 情報源

お客様より

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

ウイルスメールの具体例が載ってます  
定期的にご確認を！！



添付ファイルの中身の例  
万が一開いてしまっても  
コンテンツの有効化は絶対しない