山梨CS促進ネットワーク通信

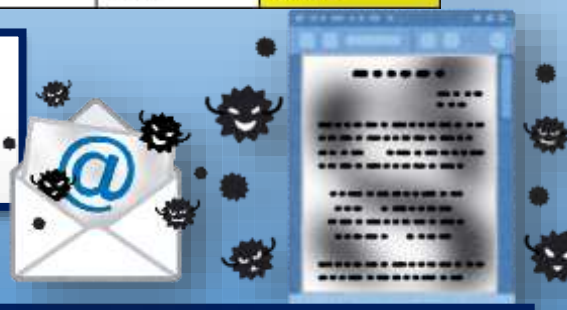
山梨県警察本部
生活安全捜査課
サイバー犯罪対策室

山梨県警察　公式ツイッターアカウント
https://twitter.com/YamanashiPolice

「Emotet」の感染を狙った攻撃メールが激増

項番	項目	2019年	2020年		
		10月～12月	1月～3月	4月～6月	7月～9月
1	IPAへの情報提供件数	1,042件	602件	325件	4,988件
2	参加組織への情報共有実施件数※1	40件	56件	55件	29件※2

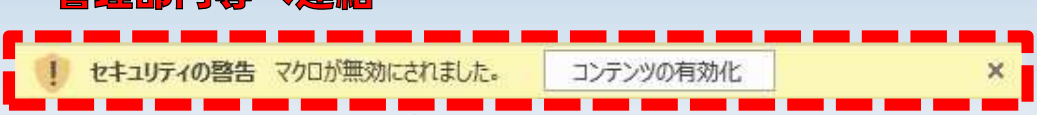
IPAは、日本の主要事業者団体と連携し、不審メール・不正通信・インシデント等の情報共有(J-CSIP)を行っています。7～9月期に寄せられた情報は、前四半期から激増し、うちEmotetに関する情報が9割以上を占めています。



Emotetとは、感染した端末の情報窃取に加え、さらに他のウイルスへの感染のために悪用されるウイルスです。その手口は、取引先や組織の役員を装ったメールに、悪意あるマクロを仕込んだワード文書ファイル等を添付して送信する手法で、受信者が正規のメールと誤信しマクロ機能を有効にしてしまうと、Emotetがダウンロードされ感染させられてしまう、というものです。日本では2017年頃から観測され、メール内容を時事ごとに変化させながら、断続的に感染拡大を繰り返してきました。

●感染対策

- **身に覚えのないメールの添付ファイルは開かない、リンクを触らない**
- **返信に見えるメールでも、不自然な点があれば添付ファイルは開かない**
- **OSやアプリケーション、セキュリティソフトは常に最新の状態にする**
- **添付されたWord文書ファイル・Excelファイルを開いた時「マクロを有効にする」「コンテンツの有効化」ボタンはクリックしない**
- **メールや文書ファイル閲覧中、身に覚えのない警告ウインドウが表示された際、その警告の意味が分からない場合は操作を中断する**
- **身に覚えのないメールや添付ファイルを開いた場合、すぐシステムの管理部門等へ連絡**



絶対に有効にしない！！

本年9月以降には、ワード文書に替わりパスワード付き圧縮ファイルを添付し、セキュリティ対策製品の検知をすり抜ける攻撃メールが観測されています。引き続き、セキュリティ製品・技術による対策、受信者の自己防衛を徹底していくよう、注意喚起しましょう。

出典：IPA サイバー情報共有イニシアティブ（J-CSIP） 運用状況[2020年7月～9月]