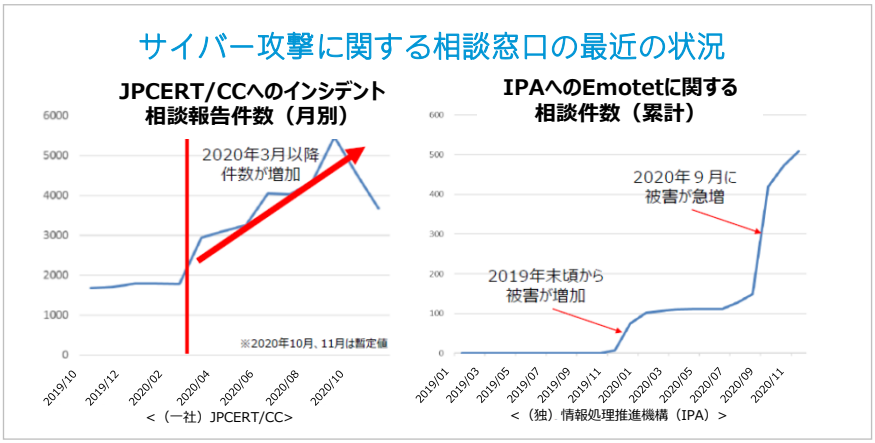
Emotet型のマルウェアから守る！セキュリティ対策

拡散力の高いEmotet（エモテット）と呼ばれるマルウェアの被害が急増しています。脅威への感度を上げ、新たな攻撃手法を理解した上でセキュリティ対策を確実に実施することが、あらゆる規模の企業にとっての急務となっています。

感染拡大するEmotet（エモテット）の脅威

⚠ **経済産業省**からサイバーセキュリティの取組の強化に関する注意喚起が行われています



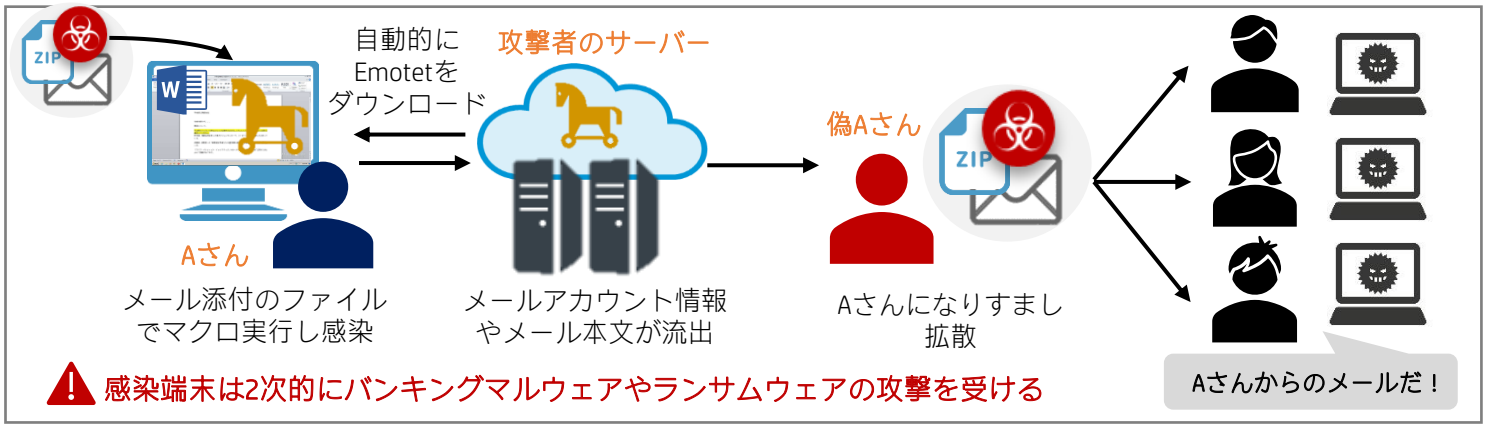
大企業だけでなく中小企業もターゲットに

特に日本が狙われている！

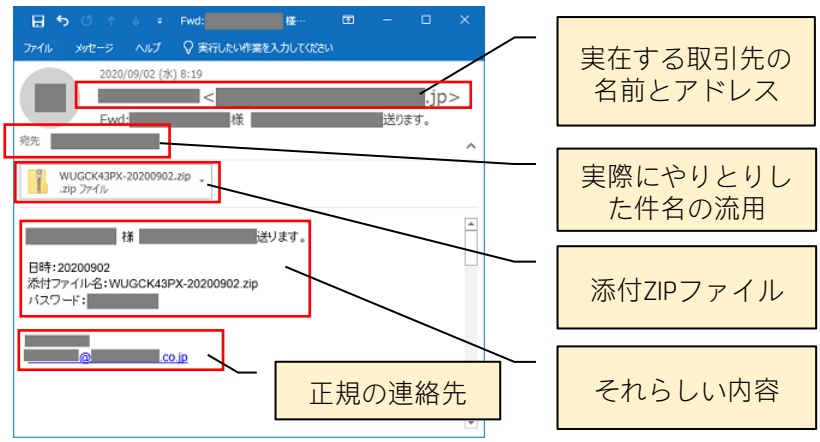
- 200年3月以降相談件数が増加
- 特に Emotetによる被害が急増

Emotetとは？

- Emotetは「なりすましメール」を介して拡散するマルウェア
- 添付ファイルを開きマクロを実行すると感染。ZIPで暗号化されウイルススキャンにかかりづらい
- 攻撃は **正規のメールに見せかける** 巧妙な手口で気づかずに開いてしまう

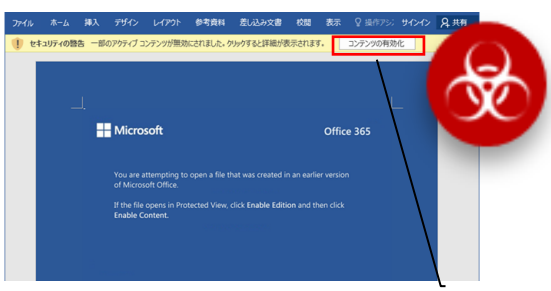


フィッシングメールの例



実際に過去にやりとりした内容がついていることも！

メールに添付されたWordファイルの例



有効化するとマクロが実行され感染！

Emotet型のマルウェアから守る！セキュリティ対策

なりすましが巧妙でうっかり添付ファイルを開けてしまうケースがあとをたちません。アンチウイルスだけでは防ぎきれないEmotetから守るには、初期段階で防御が可能なHP Proactive Securityのアプリケーション隔離機能が有効です。

防ぐのは困難に思える「Emotet」から守るには？

アンチウィルスだけでは不十分

⚠ 未知のマルウェアを検知できない
⚠ 既知のマルウェアも検知の
タイミングで大きな影響が出てしまう

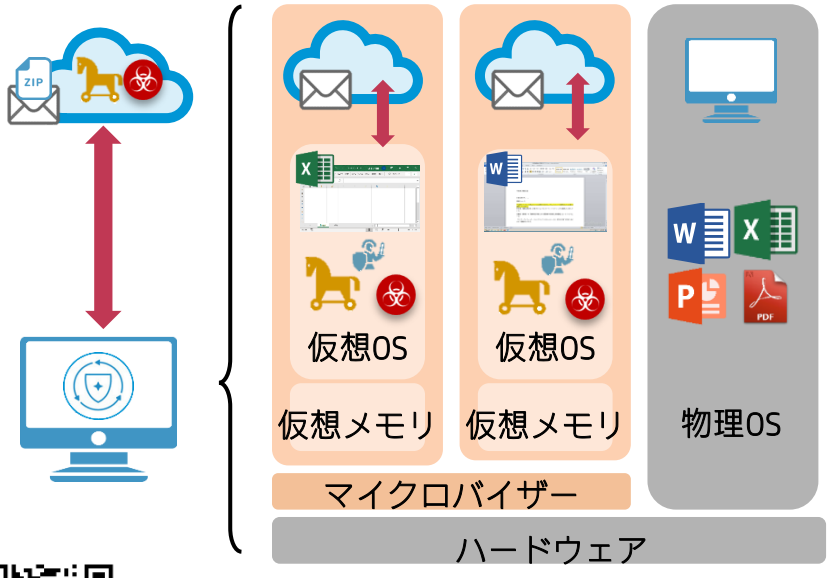
＋αのセキュリティ対策が必要

Emotetを初期段階で防御するには
アプリケーションを隔離して
感染を止めるのが最善策！

HP Proactive Security が守ります！

PC内の仮想マシン（マイクロVM）でアプリを動作させ**マルウェアを完全に隔離**して感染したブラウザやファイルからPCを守ります

Proactive SecurityのマイクロVMによる隔離技術



その感染、なかったことに！

不正なふるまいをするページを閉じれば、マルウェアは**自動的に削除**されます！

詳しくはWebをご覧ください！

https://jp.ext.hp.com/services/business/daas/value_security.html

2021.02.10 制作