

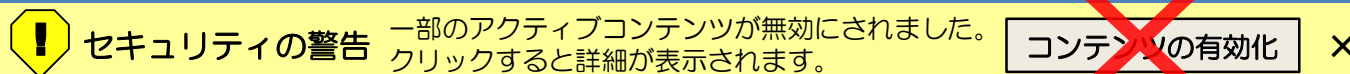
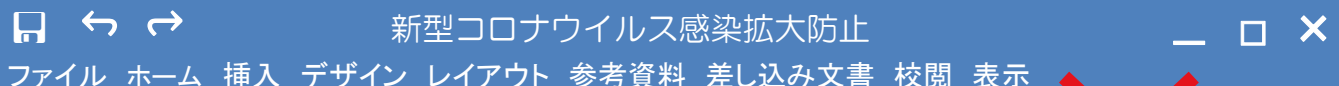
## 日本国内の組織を狙ったマルウェア LODEINFO (ロードインフォ) に注意!

LODEINFOは、感染した端末から情報を盗み取るマルウェアです。令和元年12月頃に新たに確認されましたが、頻繁にバージョンが更新されており、今後も日本国内の組織を狙った攻撃が予想されますのでご注意ください。

### 【手口】

LODEINFOは添付ファイル付きの標的型攻撃メールに用いられます。添付ファイルにはWord文書やExcel文書が使用されており、添付ファイルを開き、マクロを有効化するとマルウェアが実行されます。

### ・添付ファイル例



### CAUTION

文書ファイルに埋め込まれているマクロ（プログラム）等の実行を許可するという意味のボタンです。このボタンをクリックすると、悪意のあるマクロが動作し、ウイルスに感染するおそれがあります。

LODEINFOを用いたメールや添付ファイルは日本語で作成されているものが多く、その内容は、

- ・新型コロナウイルスを題材にしたもの
- ・日露や日韓の外交を題材にしたもの
- ・企業へのエントリーシートや履歴書を装ったもの

等様々なものがあります。

標的型攻撃メールの手口は日々変化していますが、基本的に実施すべき対策は共通しているので、下記の被害防止のポイントを参考に対策を講じてください。



## 被害防止のポイント

- OSやアプリケーション、セキュリティソフトを常に最新の状態にする。
- 身に覚えのないメールの添付ファイルは開かない。
- 自分が送信したメールへの返信に見えるメールであっても、不自然な点があれば添付ファイルは開かない。
- 信頼できないメールに添付されたWord文書やExcel文書を誤って開いても、警告が表示された場合「コンテンツの有効化」等のボタンはクリックしない。
- 身に覚えのないメールや添付ファイルを開いてしまった場合は、すぐにシステム管理部門に連絡する。