緊急速報

この被害にお気を付けください！
『身代金要求型ウイルス（通称ランサムウェア）』について

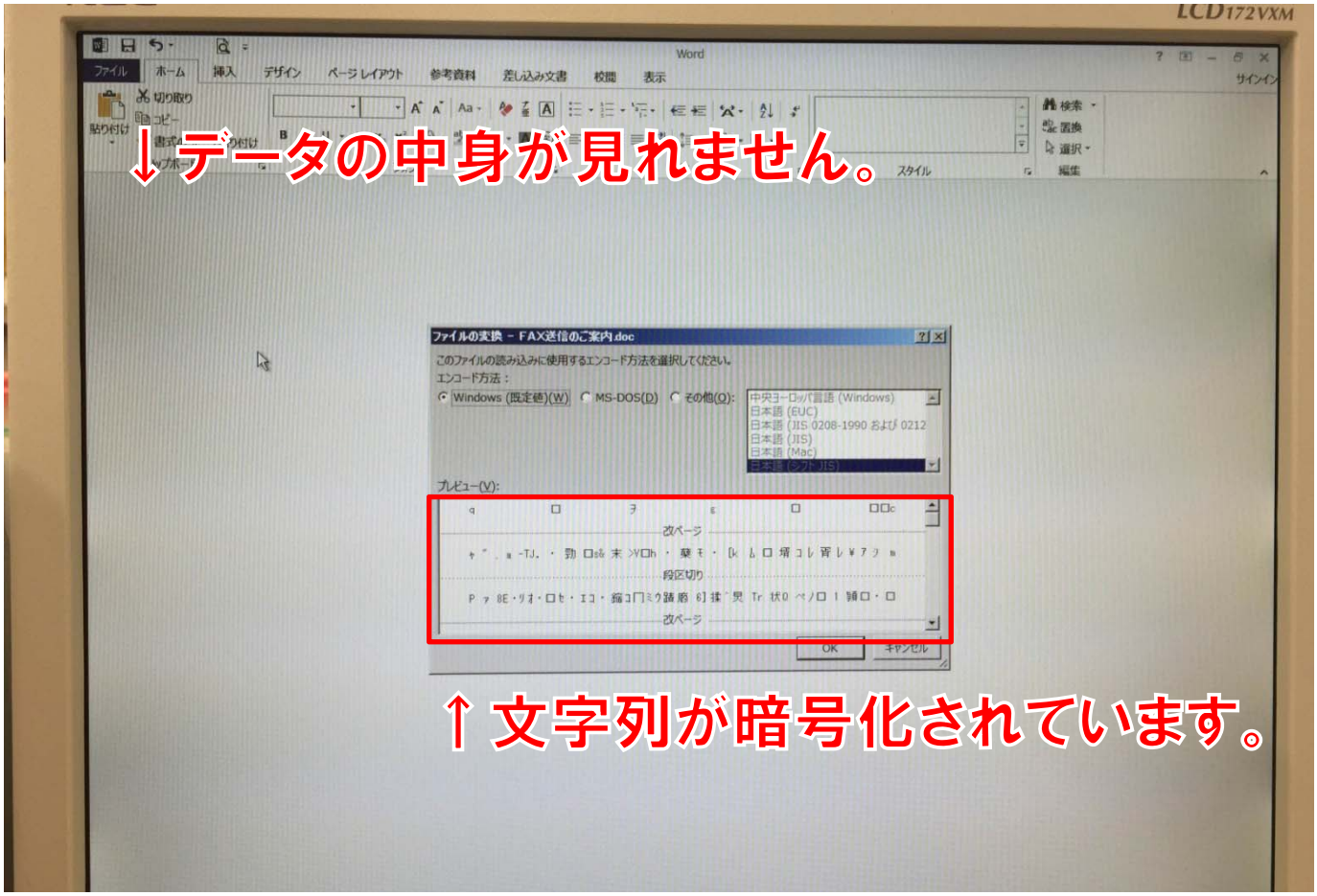
◆身代金要求型ウイルス（ランサムウェア）とは？

身代金要求型ウイルスとは、コンピュータウイルスの一種で、パソコン内のデータを暗号化してロックし、「このデータを返してほしければお金を支払え」という主旨の画面を表示するウイルスです。ウイルスの種類にもよりますが、WordやExcel、PowerPoint、画像、動画、システムファイルなどのデータが使用できなくなります。
いま、企業として最も気を付けなければならないウイルスがこの身代金ウイルスなのです。

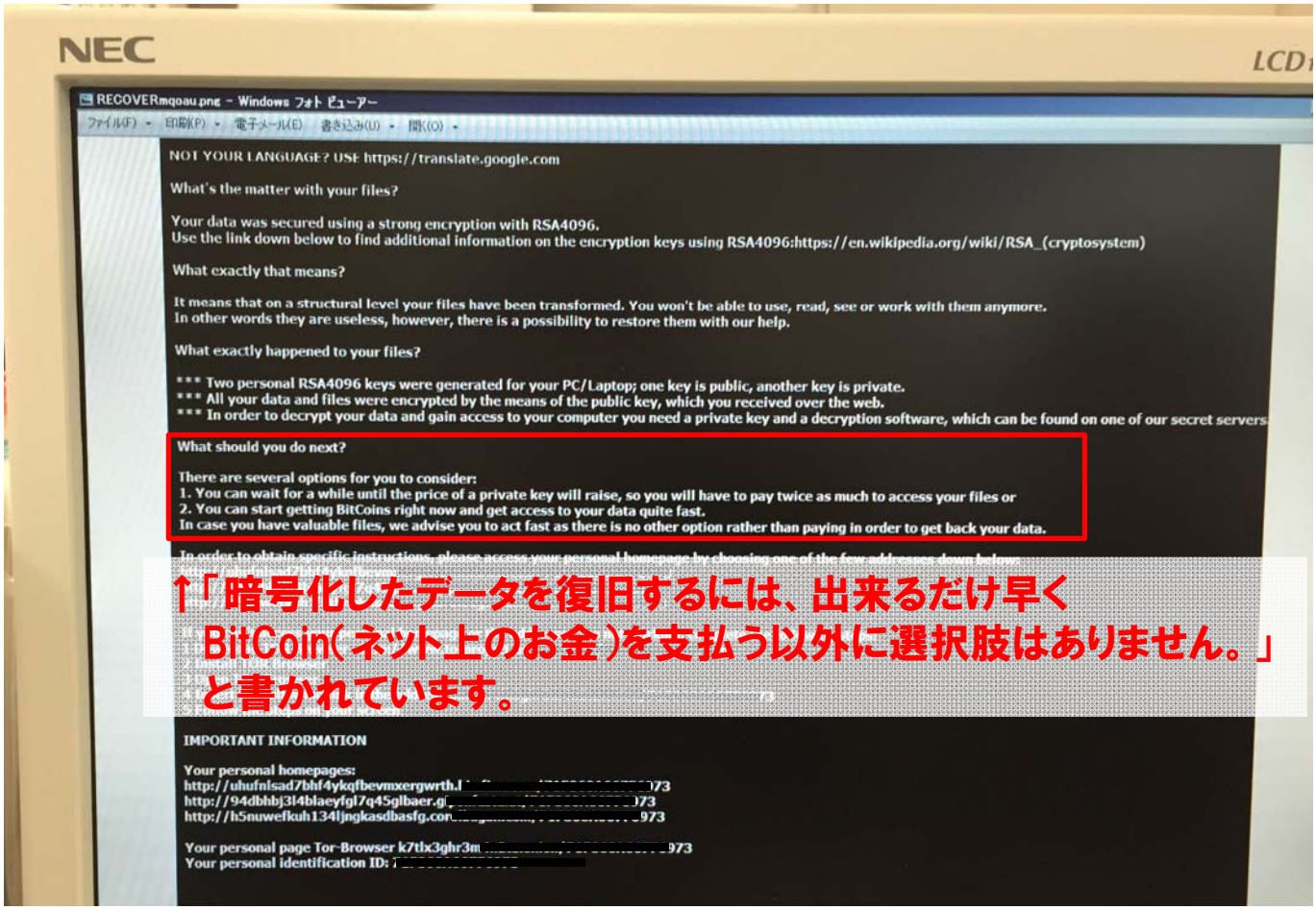
2016年2月　広島市内　某企業で発生した被害の概要

◆会社概要　・・・　業種：介護事業　事務所保有パソコン台数：10台（内1台が感染）
◆感染経緯　・・・　**Yahoo!の検索エンジンで「介護ベッド」というキーワードで検索していくつかのWebサイトを閲覧した。**その後ふとデスクトップの画面を見ると、身に覚えのない英語のテキスト等があり、パソコン内のデータが暗号化されていた。
このことから、**Webサイト閲覧時に、強制的にウイルスに感染させられた**ものと見られる。
◆攻撃パターン　・・・　不正広告の表示、またはドライブ・バイ・ダウンロード攻撃の1種
◆被害状況　・・・　パソコン1台が感染。**「RECOVERgbkcu.txt」というファイルが3つ画面上に出現**し、さらに**文書ファイル（.txt .pdf .doc .xls）、画像ファイル（.jpg）、圧縮ファイル（.zip .rar）が暗号化・破壊され、データを閲覧できない状態**になった。
◆対策状況　・・・　他の端末に感染は確認されていない。
ウイルス対策ソフトを導入済み。しかし**ウイルススキャンを実施してもウイルスは検知されず**被害に遭った。

［実際の被害画面1］　Wordファイルを開くと、中身のデータが閲覧できない状態に

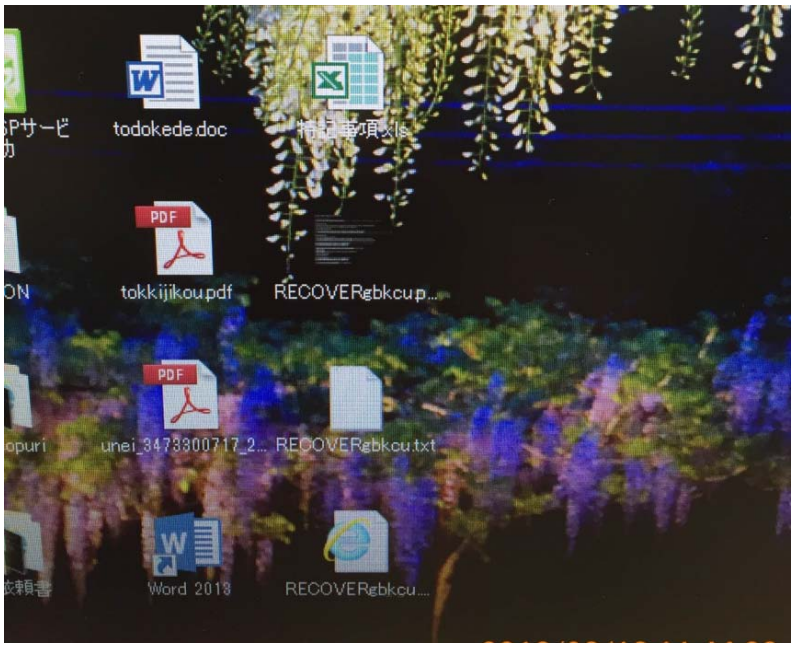


［実際の被害画面2］ デスクトップに置かれた脅迫文の内容



↑「暗号化したデータを復旧するには、出来るだけ早く
BitCoin（ネット上のお金）を支払う以外に選択肢はありません。」
と書かれています。

［実際の被害画面3］ インターネットの回遊後にデスクトップに出現したデータ



←
デスクトップに突如出現した
「RECOVERgbkcup」のファイル。
脅迫文が書かれています。

悪意のあるWebサイトに訪問した際、
強制的に身代金ウイルスに感染させ
られたものと見られています。

こうした情報セキュリティ被害に遭わないための対策方法は？

このようなウイルスによる被害に遭わないための対策方法があります。**1．ウイルス対策ソフトを"常に"最新状態に保つ**こと、**2．JavaやFlashなどのソフトウェアを"常に"アップデートする**こと、**3．インターネットの入り口にUTMを設置し、ウイルスや不正侵入の対策を施す**こと、**4．万一被害に遭った場合のためにバックアップを取得する**こと　などです。
情報セキュリティ対策には、企業それぞれに最適な形があります。詳しくは、弘法の営業担当にお尋ねください。

【発行】株式会社弘法
広島　弘法　検索
本社：〒730-0052　広島市中区千田町1丁目3-4
TEL：082-243-4455（代）FAX：082-249-6925