Subject: 偽者サイト見抜けますか？知らないうちに情報漏えいしないために【bizocean】
From: bizocean事務局 <mailmag@bizocean.jp>
Date: 2016/10/12 水曜日 8:00
To: hmiyaz@msh.biglobe.ne.jp

bizocean（ビズオーシャン）

2016年10月12日
bizoceanメルマガ《PR》

NTT東日本　　セキュリティニュース　　NTT東日本

「フィッシングサイト」の脅威をご存知ですか？

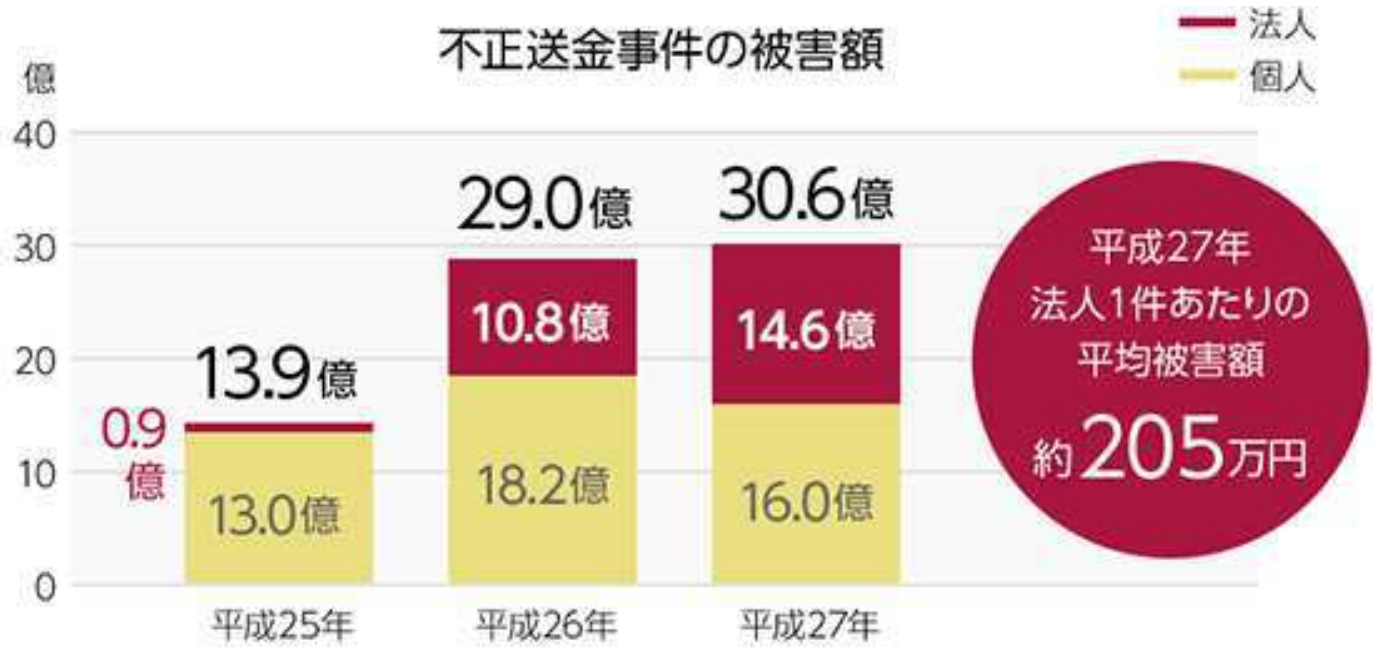
2つのサイトの違い分かりますか？
以下のダミーサイトでフィッシングサイトだと疑われるのはどちらでしょうか？
（答えはメールの1番下にあります）

※「NTT銀行」は実在する銀行およびWEBサイトではございません。

企業がこんなに狙われています！

調査　ネットバンキング利用のリスクが増加

インターネットバンキングを利用した不正送金事件（ウイルス感染やフィッシング詐欺）が増加。特に法人名義口座での被害額の割合が多くなってきています。



参考:警察庁広報資料「平成27年中のインターネットバンキングに係る不正送金事犯の発生状況等について」(平成28年3月)

調査 ウイルス感染の経路が巧妙化!

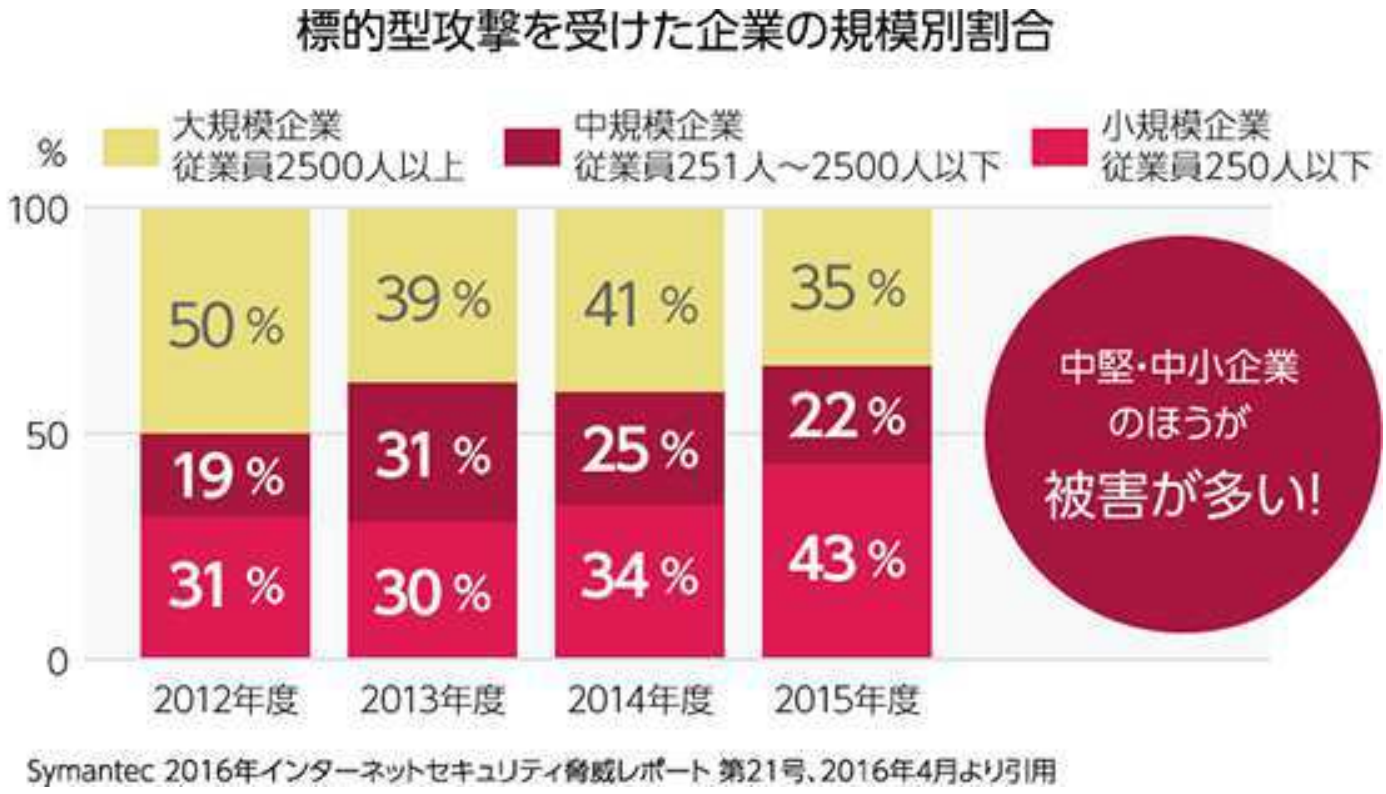
webサイトの改ざんの特徴

- 不正アクセスによって改ざんされていたサイトを正規のサイトと思い、アクセスしただけでウイルスに感染してしまう

標的型攻撃メールの特徴

- 送信者として実在する信用できそうな組織名や個人名を詐称
- 日本語によるメールでwordやpdfなど馴染みのあるファイルを添付
- 従業員のパソコンからネットワーク情報を収集、さらに権限の高いアカウント情報を利用し、ターゲットのサーバーに侵入

インターネットセキュリティの事故は増えています!



Symantec 2016年インターネットセキュリティ脅威レポート 第21号、2016年4月より引用

実例1　突然パソコンなどにロックをかけられ、使えるようにするために「身代金」を要求される!

ウイルスを侵入させてパソコン内のデータフォルダをロックしてしまい、解除するための「身代金」を要求。この手口を「ランサムウェア」といい、今年に入ってから相談件数が増加しています。

参考:独立行政法人情報処理推進機構「コンピュータウイルス・不正アクセスの届出状況および相談状況 2016年 第2四半期(4月～6月)

ランサムウェアについて詳しくはこちら ➡

実例 2

JTB、標的型攻撃メールでマルウエア侵入 顧客情報約793万件分が外部流出

取引先を装ったメールの添付ファイルをサーバーに繋がったパソコンで開いたことによりマルウェアに感染。オンライン予約サービスなどを利用した約793万件分の顧客情報が外部へ流出した可能性があることがわかった。流出したと思われるデータには、氏名や性別、生年月日、メールアドレス、住所、電話番号、パスポート番号、パスポート取得日などが含まれる。

標的型攻撃メールについて詳しくはこちら

セキュリティリスクを動画で紹介します！

Movie 1

インターネットバンキングに潜む恐怖

Movie 2

標的型攻撃メールの恐怖

Movie 3

個人のUSBメモリに潜む恐怖

Movie 4

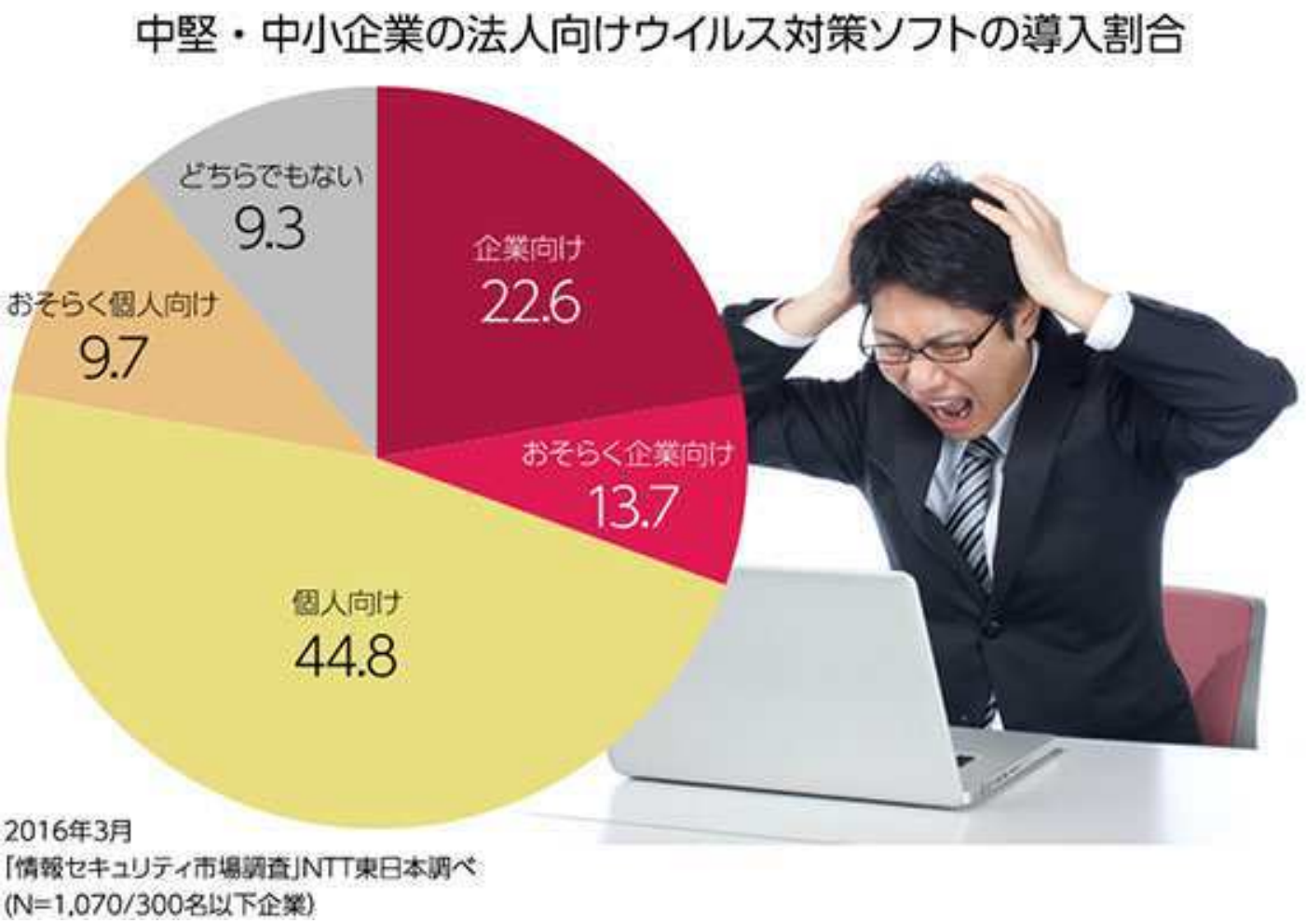
コンピューターウイルスの恐怖

このような不安に対する対策はあります！

NTT東日本にお任せください！

NTT東日本のページへ ➡

個人向けセキュリティソフトでは限界があります！



端末に対する個別のセキュリティ設定はかなりの手間がかかります。個人向けウイルス対策ソフトを利用している場合、一元管理ができていないと個人で設定を変更してしまったり、バージョンを更新せずに古いまま使用してしまう可能性があります。またセキュリティ対策に専念できる担当者がいない場合、ウイルス感染時に対応の遅れが出てしまい大変危険な状態となります。

対策 端末のセキュリティポリシーの一元管理を可能にしたい！

おまかせまるごとアンチウイルス

端末のウイルス対策の面倒な設定や監視を任せられます。

まるごとアンチウイルス

パソコン・タブレット・スマートフォンなどのマルチデバイスに対応した一元管理が可能な法人向けのクラウド型セキュリティ対策サービス。

オフィスまるごとサポート (ITサポート&セキュリティ for MA)

まるごとアンチウイルスの設定・監視代行にプラスして、IT全般のサポートも付いたサービス。

※MA(=まるごとアンチウイルス)はダイワボウ情報システム株式会社の「ウイルスバスタービジネスセキュリティサービス Powered by DIS」です。

「おまかせまるごとアンチウイルス」について詳しくはこちら ➡

imgに関する技術的・物理的対策は
NTT東日本にお任せください！

NTT東日本のページへ ➡

答え 下のダミーサイトが、フィッシングサイトだと疑われます。

アドレスバーにあるURLが「http://」から始まっており、かつ「ntt-bank」ではなく「nnt-bank」となっている。
フィッシングサイトかどうかを見極めるには、ブラウザのアドレスバーにあるURLを確認する。暗号化を行っているサイトのURLは、通常よく見る「http」の最後に「s」をつけた「https://」で始まっており、会員登録フォーム、ログイン画面など、個人情報やパスワードの入力が必須にも関わらず、URLが「http://」で始まっている場合は、フィッシングサイトである可能性が高い。

※「NTT銀行」は実在する銀行およびWEBサイトではございません。

NTT東日本が運営する、日々の業務に役立つサイトです。
セキュリティ対策に関するアドバイスも掲載しておりますのでぜひご覧ください。

提供企業
東日本電信電話株式会社
〒163-8019 東京都新宿区西新宿3-19-2
電話番号：03-5359-5111

発行者
bizocean（ビズオーシャン）事務局（株式会社ビズオーシャン）
〒104-0045 東京都中央区築地4-1-17 銀座大野ビル8F

- このメールは、登録のメールアドレス宛に自動的に送信されています。本メールにそのまま返信されても対応できませんのでご了承下さい。お問い合わせはこちらまでお願いします。
- メールマガジンの配信停止をご希望の場合には、マイページより「メルマガの配信停止」へお進みください。

※情報を反映するタイミングによっては、退会後最大3営業日ほどメールが配信される可能性がございます。あらかじめご了承下さい。

- パスワードを忘れた方はこちらから