

インターネットは危険がいっぱい!

ネットワーク

出入口に対策

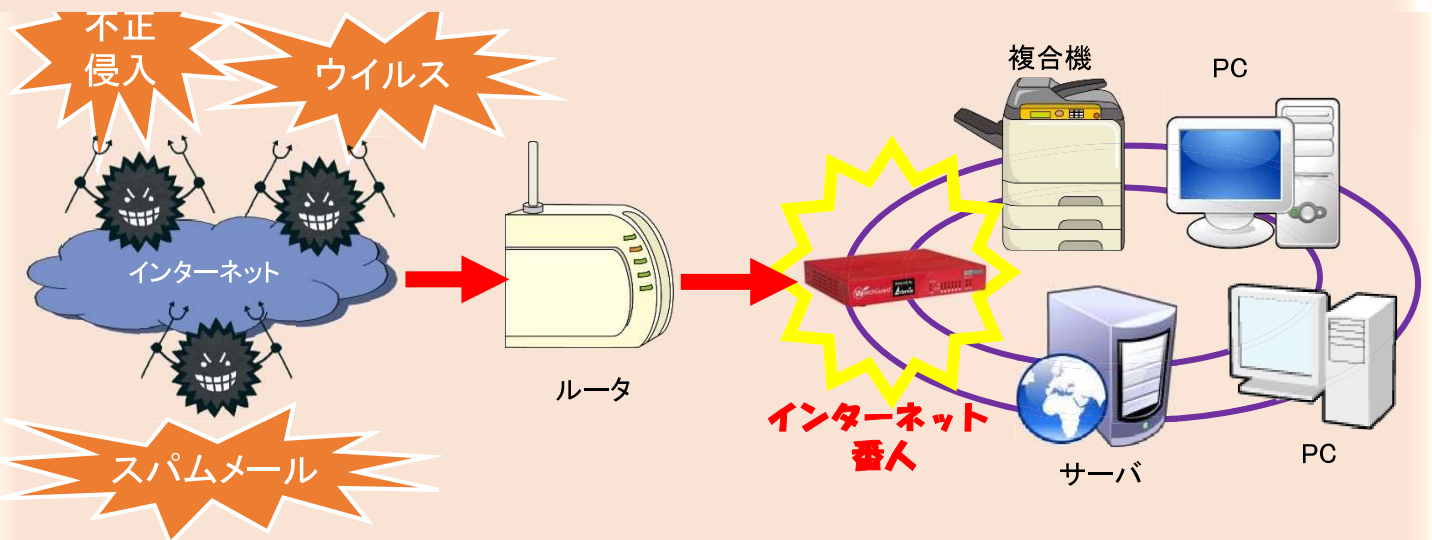
ジューボウにお任せください

下記の3つの質問の中に当てはまる項目ありますか？

パソコンのセキュリティは個別にウイルスソフトのみ

不正侵入やスパムメールなど今後が不安

社内にネットワークに詳しい人が誰もいない



外部からのウイルスを
侵入検知・ブロック

サイトの閲覧管理し
業務の効率化

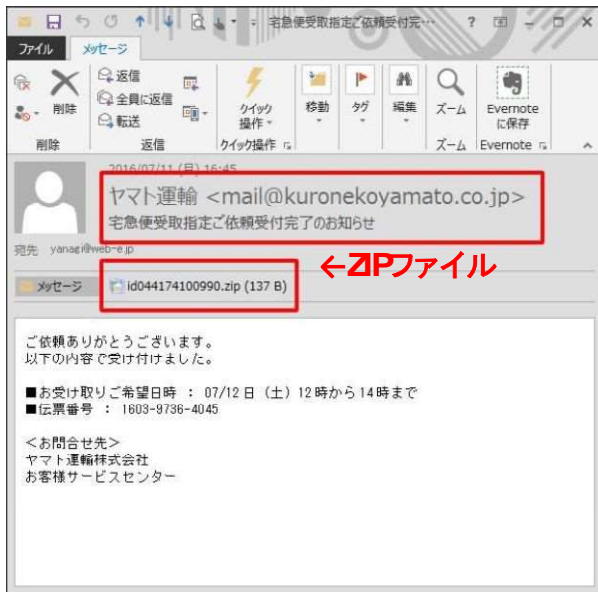
受信した迷惑メールを
自動判別

充実したサポート対応
「Angel」

詳しい情報は裏面をご覧ください。

1. こんなメール見たことないですか？

ヤマト運輸を装う迷惑メール！ ウイルス感染被害に注意



今年に入り、**ヤマト運輸を装う迷惑メール**が多発しています。左の写真のように、差出人に「ヤマト運輸」や「クロネコヤマト配送センター」とあたかもヤマト運輸がメールを送っているように見せかけています。それらには**ZIPファイル**が添付されており、開いてしまうとウイルスに感染する被害も出ています。

よく利用するAmazon、巧妙な偽メールで個人情報が抜かれる！



▲ Amazonを装った偽メール

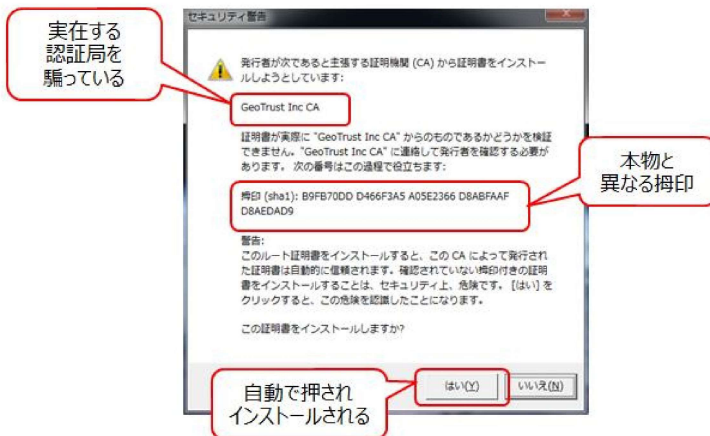


▲ 偽メールから偽サイトへ誘導

偽メールから偽サイトに誘導し、住所や名前、クレジットカード情報や預金口座番号、パスワード等の重要情報を抜き取り、その情報を利用して金銭等を搾取する「フィッシング」という手口。昔からある手法ですが未だに流行しています。普段よく利用するサイトのそっくりなメールがきたら騙されてしまいそうです。個人情報が抜かれたら大変なことになりますので注意が必要です。

よくあるインターネット攻撃

日本郵政を騙るマルウェアスパムが拡散！！



日本郵政からのメールを偽装したスパムが国内で流行。狙いは国内ネットバンキングであり、これらのスパムメールにはZIPファイルが添付されており、展開すると不正プログラムが勝手にインストールされ、不正送金の被害に遭うこととなります。

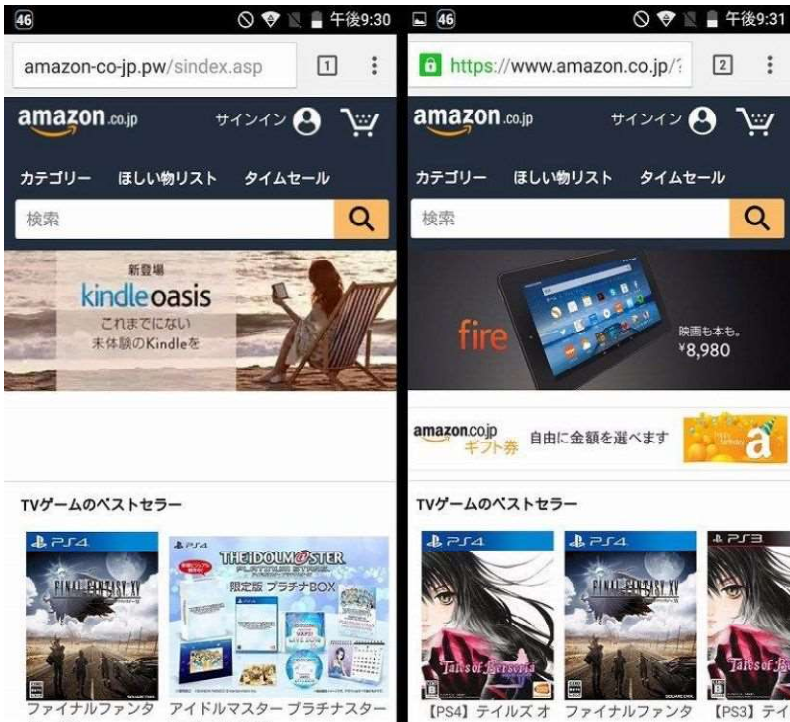
事務職の方はご注意ください！ 仕事の関係先のような迷惑メール



いかにも仕事の関係先のようなメールで、業務上で必要な書類と思わせるものが多く出回っています。こちらも添付ファイルを開くとウイルス感染の危険がある為、十分な注意が必要です。こういったスパムメールは不特定多数に送信されており、文面もどんどん巧妙化しております。

2. こんなサイト見たことないですか？

さてあなたは本物と偽物がどちらかわかりますか？



誰もが利用する有名サイト。その偽サイトが巧妙化しています。先ほどの偽メールと同様に、偽サイトもパッと見ただけでは判断できません。右が正規サイト、左が偽サイトです。見分け方はURLです。本物のAmazonのURLは「amazon.co.jp」となっています。



みんなが興味を持つニュースに便乗し悪質な偽サイトが続出

25年ぶり優勝に使来、野球チームの優勝グッズ詐欺サイトが登場

2016年9月度は、25年ぶりに優勝を飾ったプロ野球チームの優勝グッズ販売を装う偽販売サイトを検知しました。優勝が決定したタイミングに合わせて、優勝を記念したスマホケースや本城地の水運局とコラボレーションしたキーホルダーなどを販売する偽販売サイトが確認されました。今までもユニフォームや帽子などを販売する偽販売サイトは多く見られましたが、メディアでの連日の報道やインターネット上での優勝セールが話題となり、犯罪者が話題に便乗して偽販売サイトを作ったものと想定されます。また今後の試合開催によっては、同種の偽販売サイトが登場することも考えられるため注意が必要です。

このような偽販売サイトでは、商品を購入しても商品が届かないなどの被害に遭う危険性があるほか、入力したメールアドレスやパスワード、住所、氏名、クレジットカード番号などの犯罪者にとって有益な個人情報が盗まれ、成り済ましによる不正な商品購入や、個人情報ブラックマーケットで売買される危険性もあり、注意が必要です。

▲ 野球チームの優勝グッズ詐欺サイト

ポケモンGO 超絶情報

233: 以下、お楽しみにかわりましてポケモンGO超絶情報をお送りします 投稿日: 2016/07/22(土) 17:09

230: サイトに無料会員登録する！
http://www.pokemon.co.jp/ex/PokemonG0/item_present/
↓
無料ガチャ引いたり、キャンペーン条件達成してポイント貯める
↓
貯めたポイントをギフトコードに交換
あとはポケコインにするか、現金にするかは自由

234: 以下、お楽しみにかわりましてポケモンGO超絶情報をお送りします 投稿日: 2016/07/22(土) 17:11

231: 以下、お楽しみにかわりましてポケモンGO超絶情報をお送りします 投稿日: 2016/07/22(土) 16:45

232: 以下、お楽しみにかわりましてポケモンGO超絶情報をお送りします 投稿日: 2016/07/22(土) 17:14

▲ 流行のアプリに便乗した偽サイト

3,000円 基礎医療

未来を支える「毎月の寄付」

継続的に毎月、寄付いただく方法です。

7日 今を救う「今」

任意の金額をそのつど、

> 毎月の寄付をする

> 今回の寄付をする

▲ 災害時に義援金を募る偽サイト

新生活を始めるシーズンに便乗する偽サイト

このページは、新生活を始めるシーズンに便乗して作成された偽サイトです。商品画像やテキストが粗雑で、信頼性が低いことが確認されました。

よくあるインターネット攻撃

見た目はそっくり「楽天市場」を偽装した偽サイト！

偽サイトは、楽天市場のロゴやバナーを掲示するなど正規サイトとそっくりに作られており、商品を注文しようとする、**楽天市場の登録フォームにそっくりなページに誘導し、個人情報やクレジットカード情報を盗み取ろうとします。**見分ける方法としては、URLが正規のものとなるのでそこで見分ける必要があります。

URLが、楽天市場のショップとは全く異なります。

「楽天スーパーSALE」と記載されていますが、楽天とはまったく無関係のサイトです。



楽天市場のショップページをそのまま偽装していますが、URLが全く異なり、楽天市場ではないサイトとなります。



このようなリンクはクリックすることのないようご注意ください



偽装サイトで買おうとすると、楽天市場を模した偽装フォームで個人情報の入力を求められます。ご注意ください。



本物のURLとはまったく異なります

本物のフォーム

https://basket.step.rakuten.co.jp/rms/mall/bs/dlvpaychange/

クレジットカード決済

楽天市場でさらにポイントGET!

楽天カードはいつでもポイント2倍

カード会社: 選択してください

カード番号: (例) 1234 - 5678 - 9012 - 3456

有効期限: 月/年 (例) 08/14

名義人: *「TARO YAMADA」もしくは「ヤマダタロウ」などのようにカードの表示どおり入力してください。

楽天市場のクレジットカード情報入力画面では、番号、有効期限、名義人のみご入力いただいております。

偽物のフォーム

http://www.eveiine.com/cart/cart.php?siteswww.eveiine.com&p=352&nms=コーヒークップ&リーサー

クレジットカード決済

楽天市場でさらにポイントGET!

楽天カードはいつでもポイント2倍

カード会社: 選択してください

カード番号: (例) 1234 - 5678 - 9012 - 3456

有効期限: 月/年 (例) 08/14

名義人: *「TARO YAMADA」もしくは「ヤマダタロウ」などのようにカードの表示どおり入力してください。

セキュリティコード: * (例) 999【半角】のようにカードどおり入力してください。

偽物のフォームでは、セキュリティコードの入力を求められます。

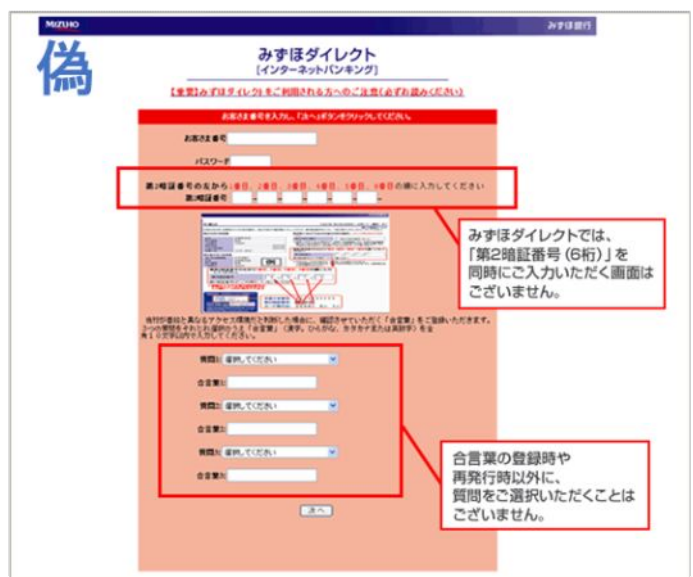
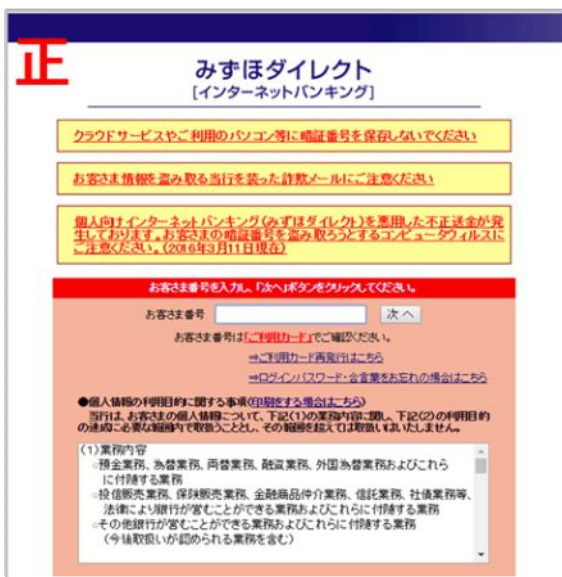
3. 銀行からの連絡でIDパスワードの変更を求められたことはありませんか？

金融機関の偽サイト要注意！！



金融機関の偽サイトからIDパスワードを求められ入力したりしていませんか？
こういった金融機関の偽サイトの増加について警視庁でも注意喚起を行っております。
偽サイトに情報を入力すると犯人側に送られる仕組みになっています。

ログイン時、暗証番号を入力させるのは偽サイト！



不用意に情報を入力しないように気をつけましょう。

データが消える？身代金？ 迫りくるランサムウェアの脅威！！

そもそもランサムウェアって何？

ランサムウェアとはコンピュータ内のデータを暗号化し、データを人質に取った上で元に戻す為に金銭を支払うように誘導するウイルスのこと。**身代金ウイルス**とも呼ばれています。



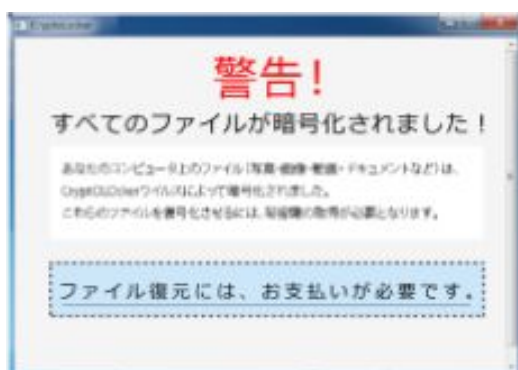
実際に感染するとどんなことが起きるの？

- ・感染したPCの操作ができなくなる
- ・感染したPC内のファイルやネットワーク共有上のファイルが暗号化され利用できなくなる
- ・要求された「身代金」支払うことによる金銭的な被害

金銭を支払ったからと言って、PCやデータが元に戻る保証は一切ありません！



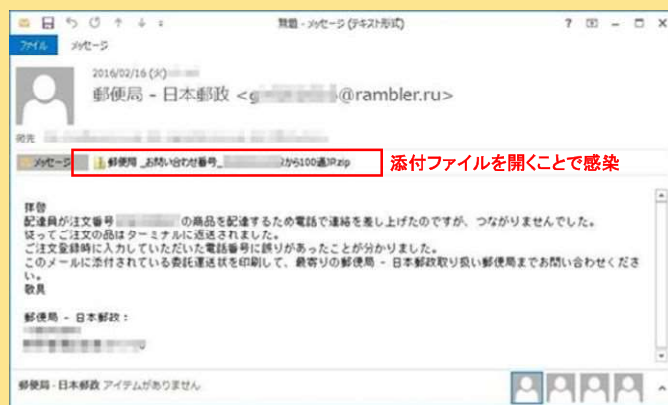
ランサムウェアに感染するとこのように表示が出てデータが暗号化され、身代金を要求されます。



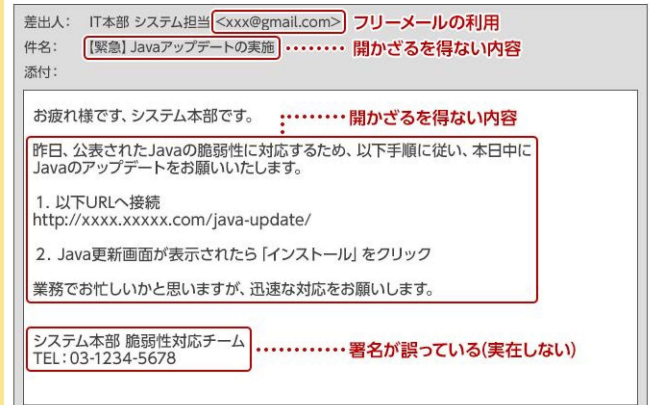
主な感染経路

- ・HPサイト経由(正規サイト、広告サイト、危険性が高いサイト等)
- ・WEBサイトに表示されている広告経由
- ・電子メール経由(ウイルス添付、サイト誘導等)

こういったスパムメールからランサムウェアに感染の危険！！

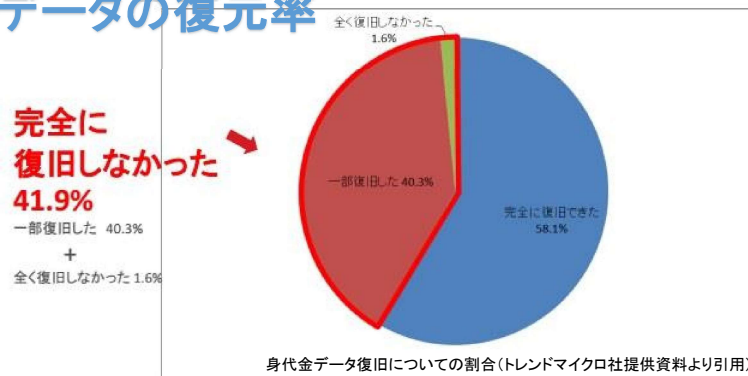


▲日本郵政を装ったスパムメール



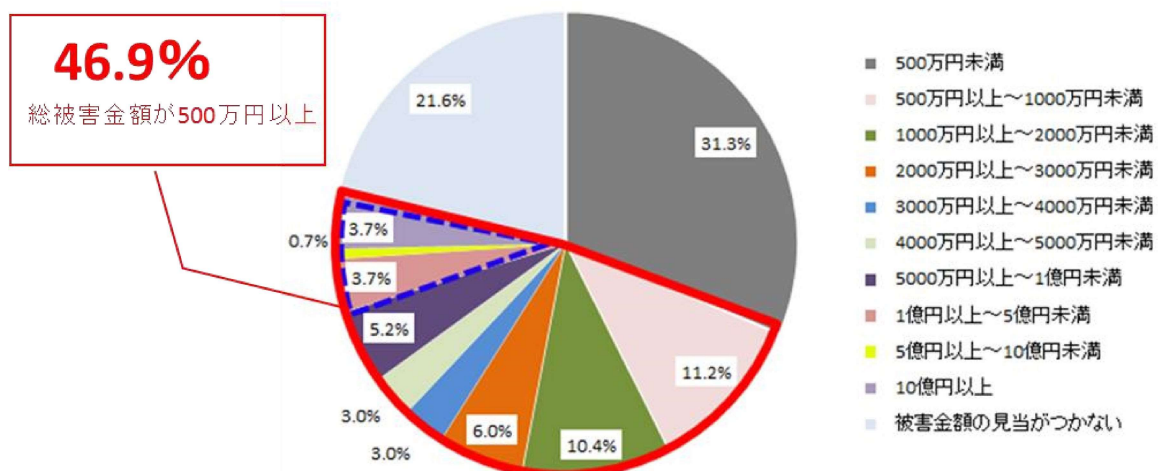
▲アプリのアップデートを促すような偽メール

データの復元率



トレンドマイクロ社は、イギリスの企業(従業員1000人以上)のIT担当者を対象にランサムウェアに感染した際にデータの復旧に成功したか調査結果を発表しました。左のグラフの割合でもわかるように、高額な身代金を支払っても、データが元に戻る保証は全くありません。

ランサムウェアによる金銭被害総額



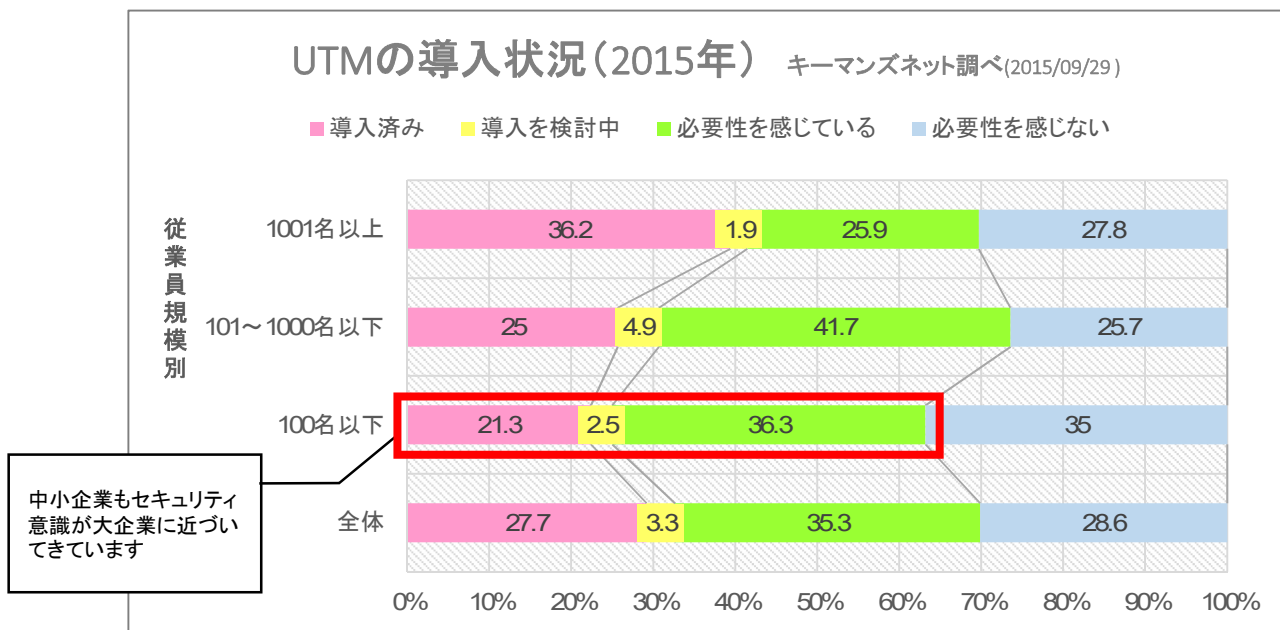
ランサムウェアによる総被害金額の割合(トレンドマイクロ社提供資料より引用)

ランサムウェアの攻撃を受けたと回答した134名を対象に、データやシステムの復旧や売上機会の損失の対応費用などを含めた総被害金額を聞いたところ、「500万円以上」と回答した人が対象者の半数近い46.9%に上ることが判明しました。

標的型攻撃には多層防御で！

今はアンチウイルスソフトとUTM併用の時代

アンチウイルスソフトはウイルスを45%程しか防げないと言われている中で近年、あらゆる脅威に対応できる**X-OP(UTM)**の注目が集まっています。下記のグラフは企業におけるUTMの導入状況です。年々導入済み企業は増加傾向にあり、なかでも中小企業の導入数は近年伸びつつあります。



複雑化するあらゆる攻撃に対して
過半数がUTMの必要性を感じています！！

対策① 侵入させない ⇒ 高度なアンチウイルスエンジン

Check Point社のUTMテクノロジーを採用。グローバルベースで脅威情報を集積している「ThreatCloud」エンジンと、カスペルスキー社のアンチウイルスエンジンを搭載することで、450万以上のマルウェアシグネチャと30万以上の不正Webサイトを検出。ネットワークの手前で阻止し、ネットワーク内への感染を防御します。

※カスペルスキー社は「.vvvウイルス」を2015年2月に既に検知し対策済みであったといえます(2015/12/8インターネットコムの記事より)。ベンダーの実力をこらいった対応の迅速性から計り知ることができます。



対策②③ 活動させない・通信させない ⇒ アンチボット機能

攻撃先に侵入したランサムウェアは、外部の指令サーバー(C&Cサーバー)と通信してファイル暗号化鍵を入手し、暗号化処理を行うというのが典型的な特徴です。侵入先を「ロボット」のように操ることから「ボット」とも呼ばれています。

InformationGuardのアンチボット機能では、このようなボットに感染したPCを検出すると指令サーバーとの通信を遮断します。万が一ランサムウェアに感染しても、暗号化処理を走らせないようにブロックすることができます。



ウイルス対策にお困りのあなたに X-CPなら一括管理で怖いもの無し！！

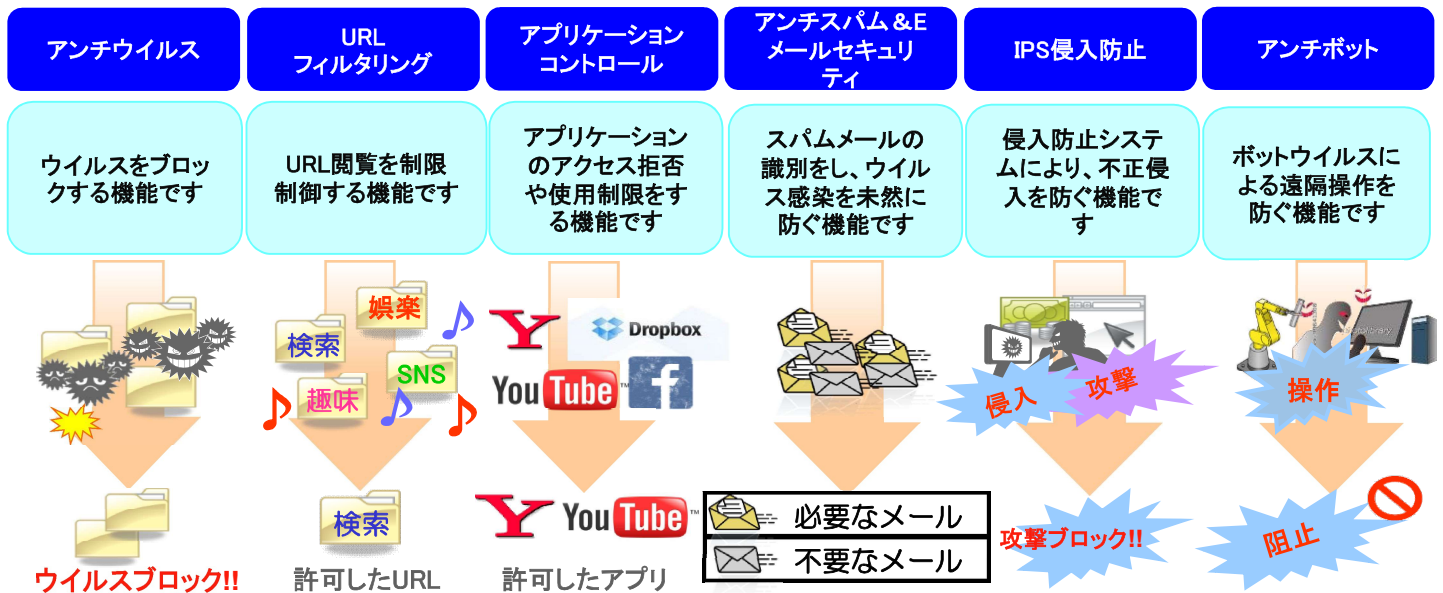


X-CPとはネットワークの出入口を守るセキュリティ機器です。
次のような機能があります。

オールインワンシステムで
コストが安く
運用・管理が簡単に

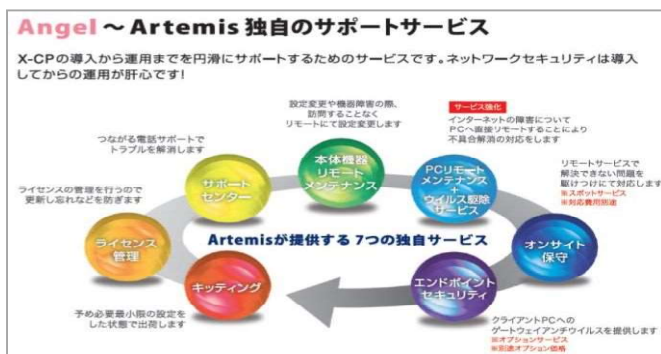
「多層化セキュリティ」を実現
従来のウイルスソフトで
対応しきれない複雑化された
ネットワーク攻撃に対応

インターネットに接続され
ており、常に最新のセキュ
リティへ自動更新



X-CPのプラスの機能

◎独自のサポートサービス ~ Angel ~
X-CPなら導入、運用、設定変更等あらゆる物事に対応
することができるAngelサポートを標準で搭載しており
ますので導入後も安心してご使用頂けます。



◎詳細なセキュリティレポート機能

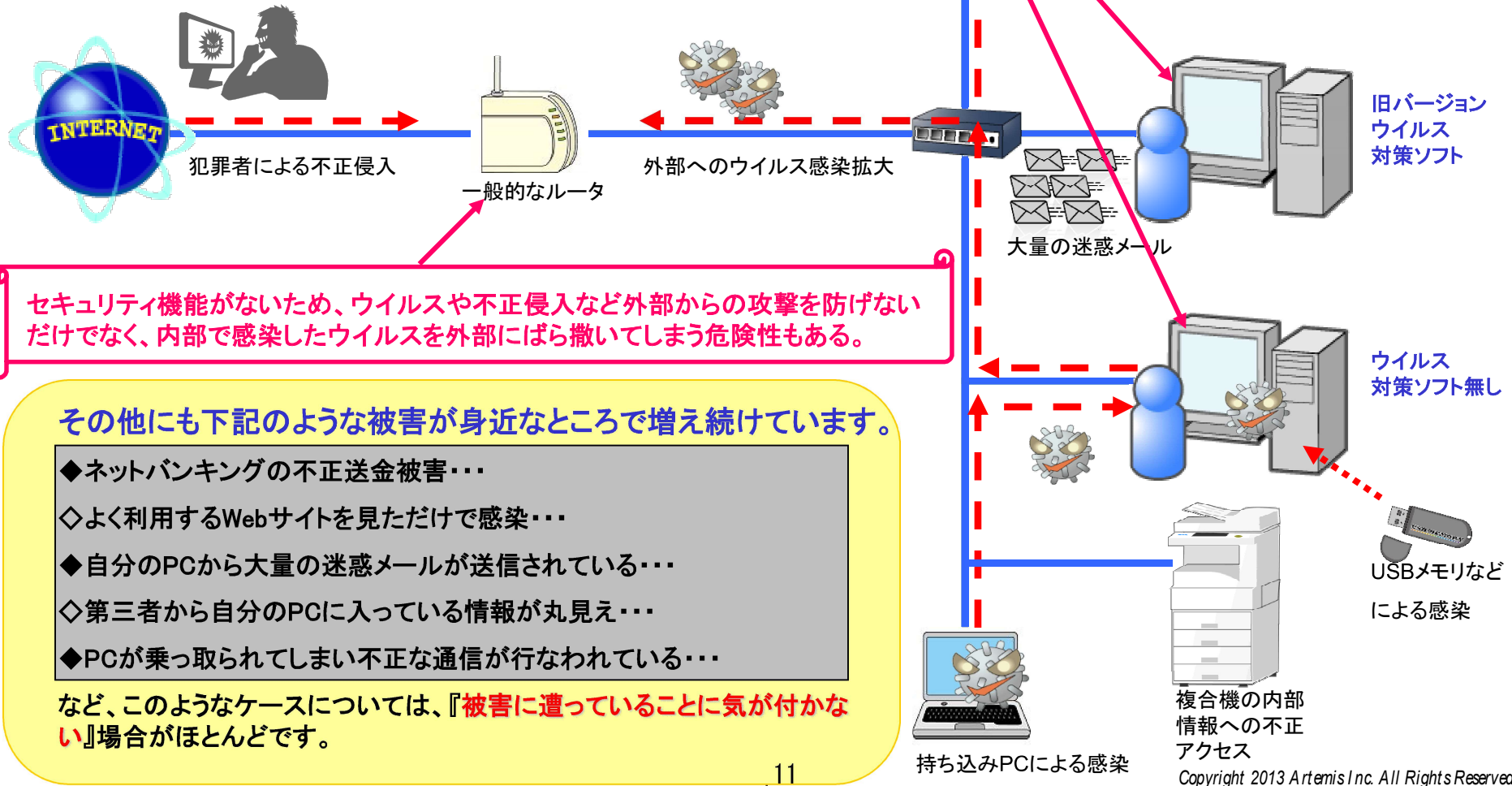
標準でセキュリティレポート機能を搭載しておりますので、実
際の通信や使用状況をお客様自身のPCで確認できます。



多くの中小オフィスにみられるセキュリティ対策状況



ウイルス対策ソフトは導入しているものの、定期的な更新は行なっておらず、バージョンが古いまま利用している。中にはソフト自体をアンインストールしているPCもある。



セキュリティ機能がないため、ウイルスや不正侵入など外部からの攻撃を防げないだけでなく、内部で感染したウイルスを外部にばら撒いてしまう危険性もある。

その他にも下記のような被害が身近なところで増え続けています。

- ◆ ネットバンキングの不正送金被害...
- ◇ よく利用するWebサイトを見ただけで感染...
- ◆ 自分のPCから大量の迷惑メールが送信されている...
- ◇ 第三者から自分のPCに入っている情報が丸見え...
- ◆ PCが乗っ取られてしまい不正な通信が行なわれている...

など、このようなケースについては、『被害に遭っていることに気が付かない』場合がほとんどです。

X-CP導入後のセキュリティ対策イメージ



クライアントPCの対策として、必要最低限のウイルス／マルウェア対策の機能だけを残し、余分な機能はX-CPにて一元管理をします。PCに掛かる負荷を最小限に抑えつつ、最新の状態を保ちます。



X-CPの導入により、外部からのあらゆる攻撃(ウイルス・不正アクセス・迷惑メールなど)からオフィスセキュリティの環境を守ります。さらに、内部感染したウイルスを外部に拡大させることを防ぎます。

- その他にも下記のようなメリットが挙げられます。
- ◆ 経理用のPCは他のネットワークと分けることができます。
 - ◇ ウイルス感染したWebサイトにアクセスした際にX-CPがブロックします。
 - ◆ メール送信の際にも迷惑メールのチェックしています。
 - ◇ 強固なファイアウォールにより、外部からの不正なアクセスを防ぎます。
 - ◆ 不正な通信が発生した場合は、通信を遮断し被害を食い止めます。

