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

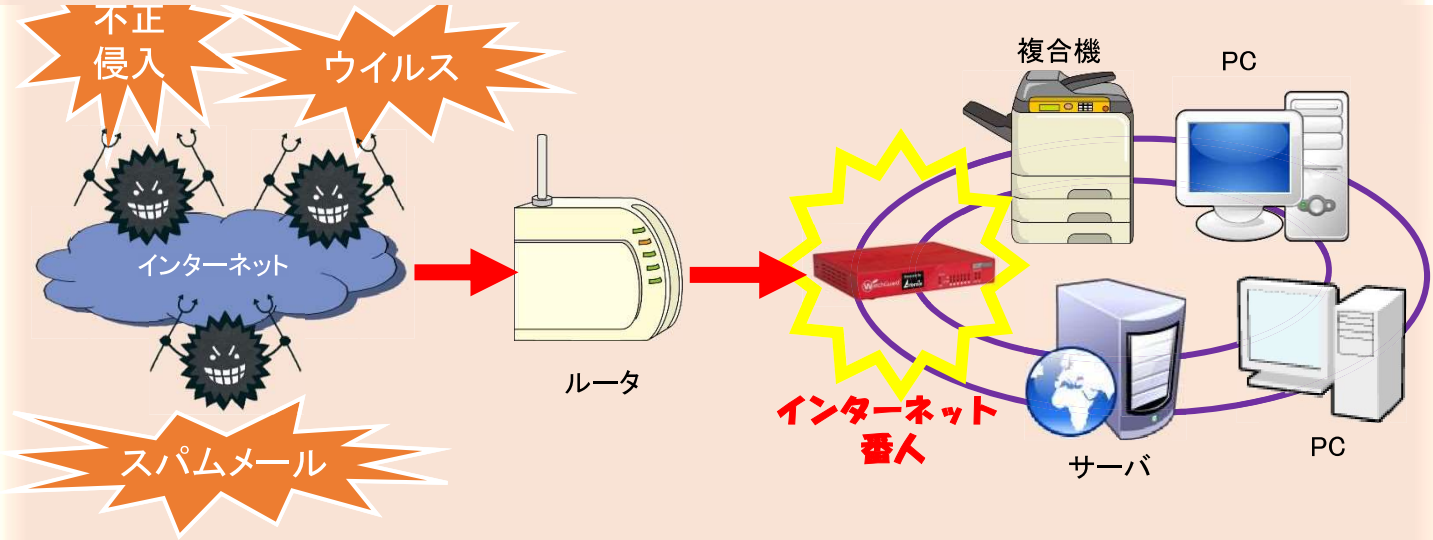
ジュボウにお任せください

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

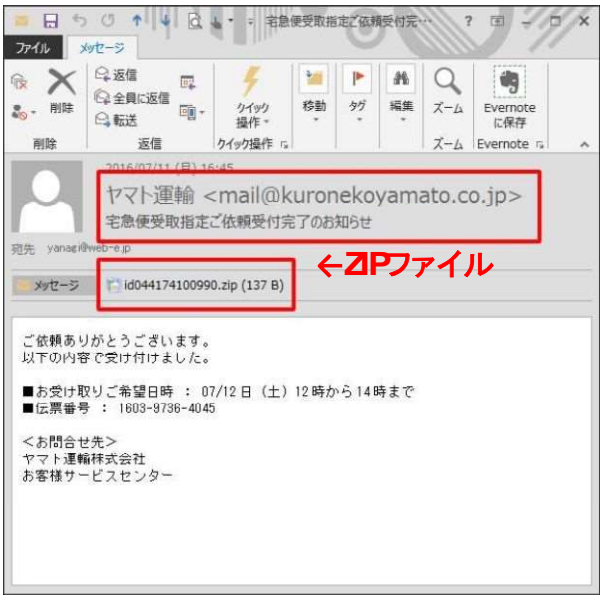
受信した迷惑メールを
自動判別

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便センター」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。

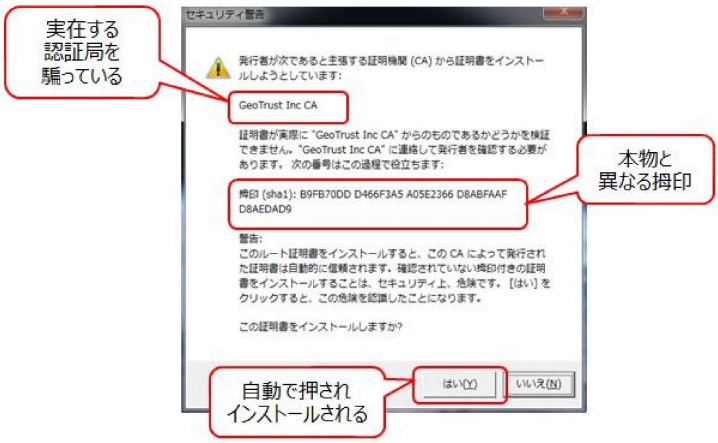
よく利用するAmazon、巧妙な偽メールで個人情報が抜かれる！

▲ 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。

日本郵政を騙るマルウェアスパムが拡散！！



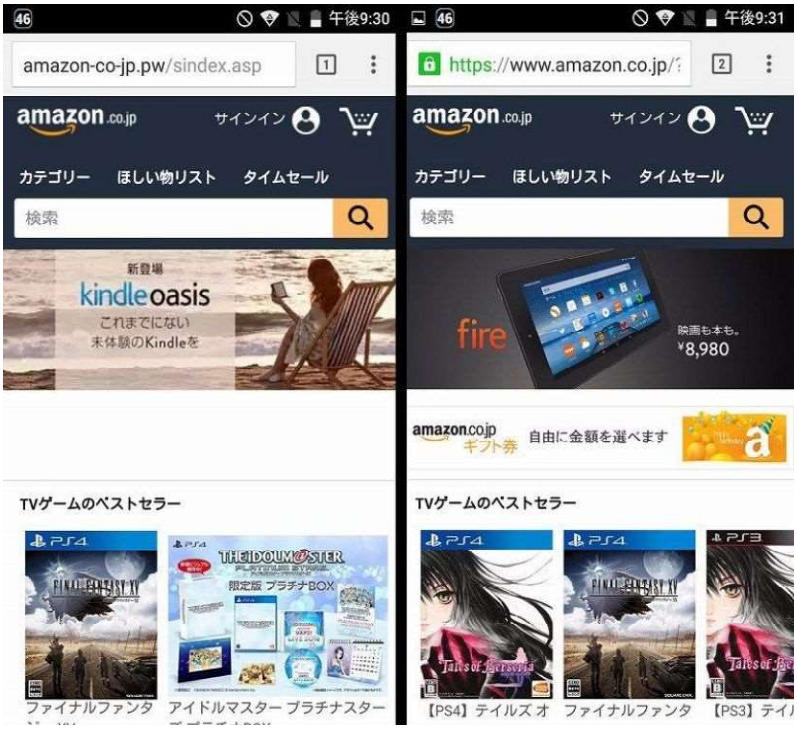
日本郵政からのメールを偽装したスパムが国内で流行。狙いは国内ネットバンキングであり、これらのスパムメールにはZIPファイルが添付されており、展開すると不正プログラムが勝手にインストールされ、不正送金の被害に遭うことになります。

事務職の方はご注意を！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、充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。

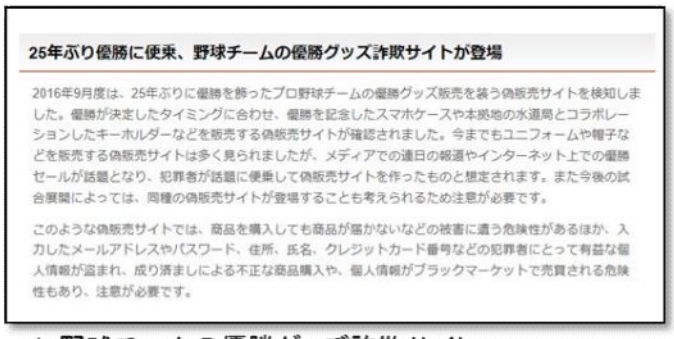
その偽サイトが巧妙化しています。

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



▲ 野球チームの優勝グッズ詐欺サイト

▲ 流行のアプリに便乗した偽サイト

▲ 災害時に義援金を募る偽サイト

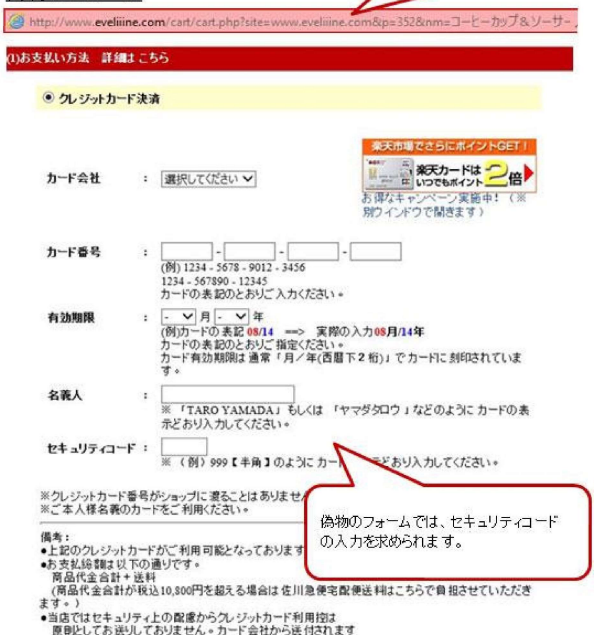
▲ 新生活を始めるシーズンに便乗する偽サイト

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と、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が正規のものとことなるのでそこで見分ける必要があります。

本物のフォーム

偽物のフォーム



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？

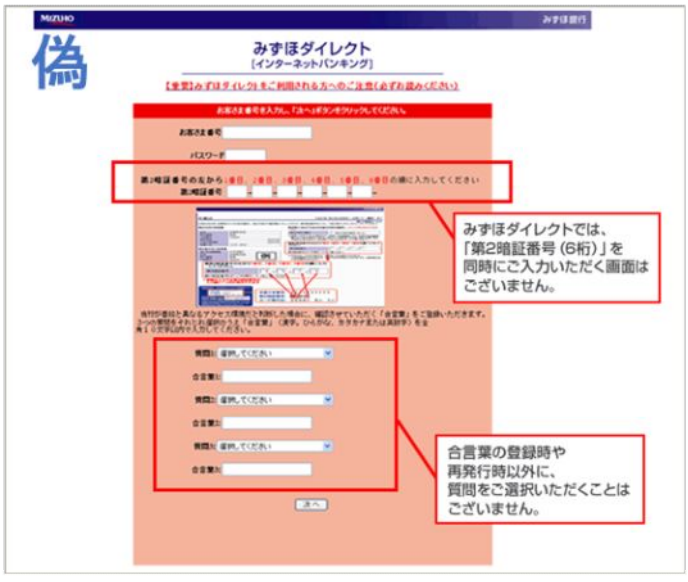
金融機関の偽サイト要注意！！

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？

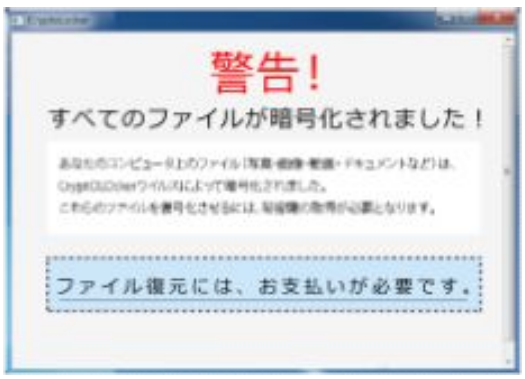
ランサムウェアとはコンピュータ内のデータを暗号化し、
データを人質に取った上で元に戻す為に金銭を支払うように
誘導するウイルスのこと。身代金ウイルスとも呼ばれています。

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！

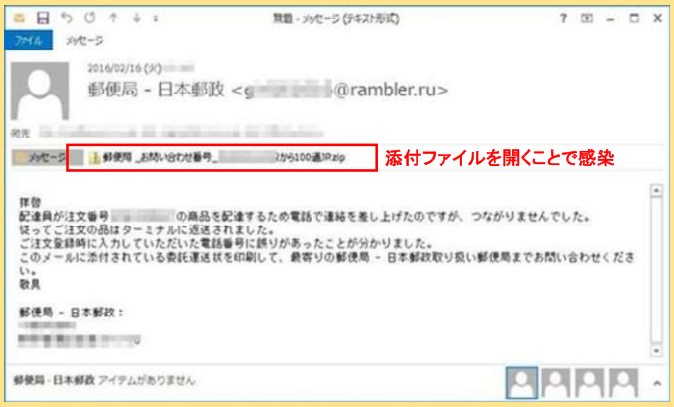
ランサムウェアに感染すると
このように表示が出て
データが暗号化され、
身代金を要求されます。



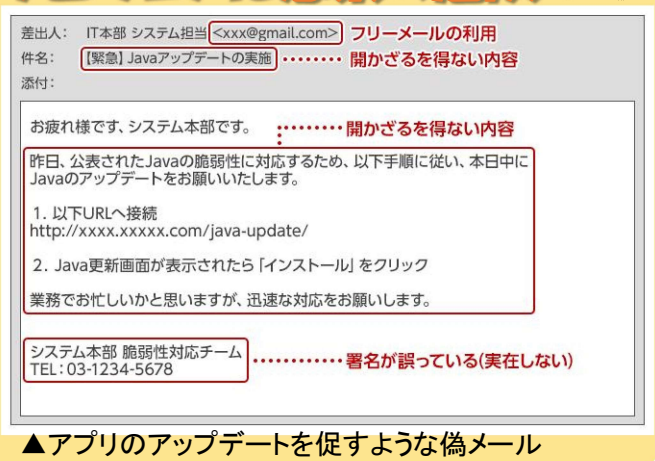
主な感染経路

・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！！

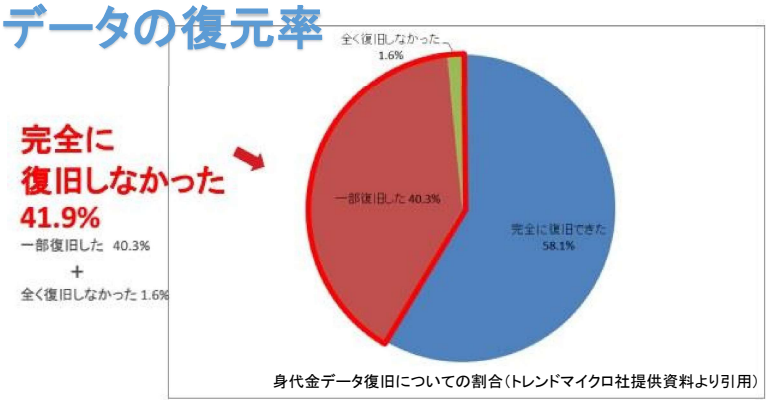


▲日本郵政を装ったスパムメール



▲アプリのアップデートを促すような偽メール

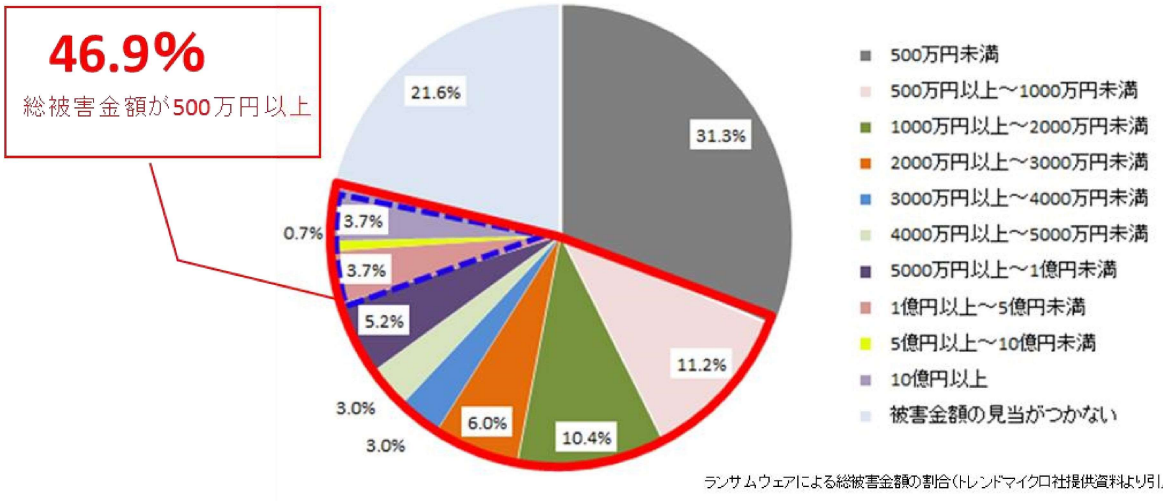
データの復元率



身代金データ復旧についての割合（トレンドマイクロ社提供資料より引用）

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

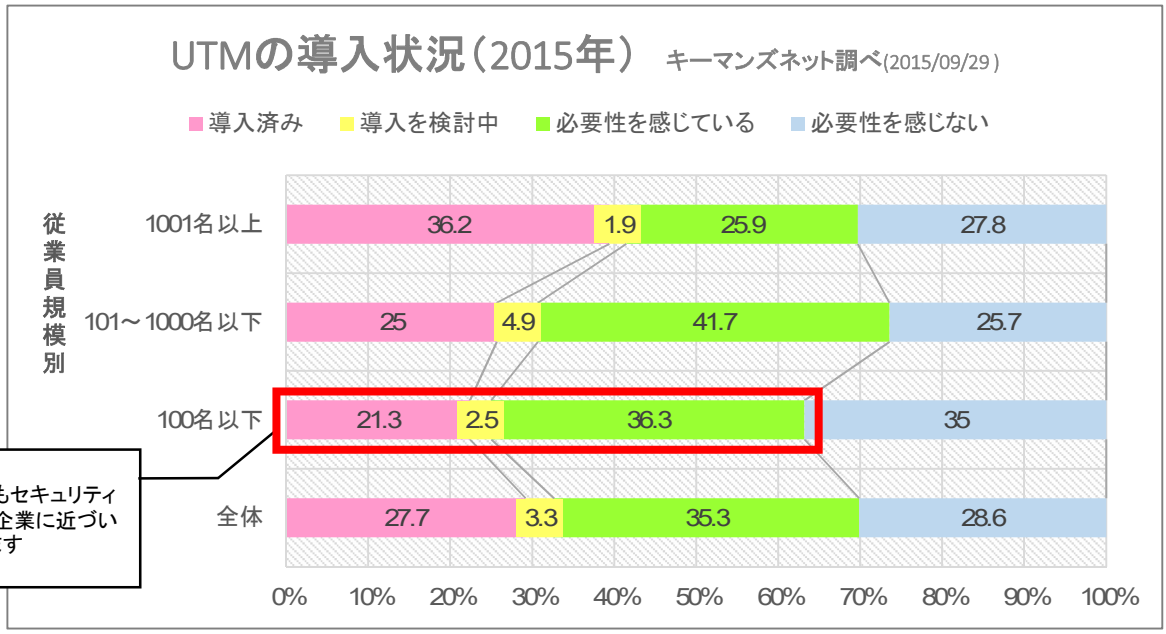


ランサムウェアによる総被害金額の割合（トレンドマイクロ社提供資料より引用）

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-CP(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います（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う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！！

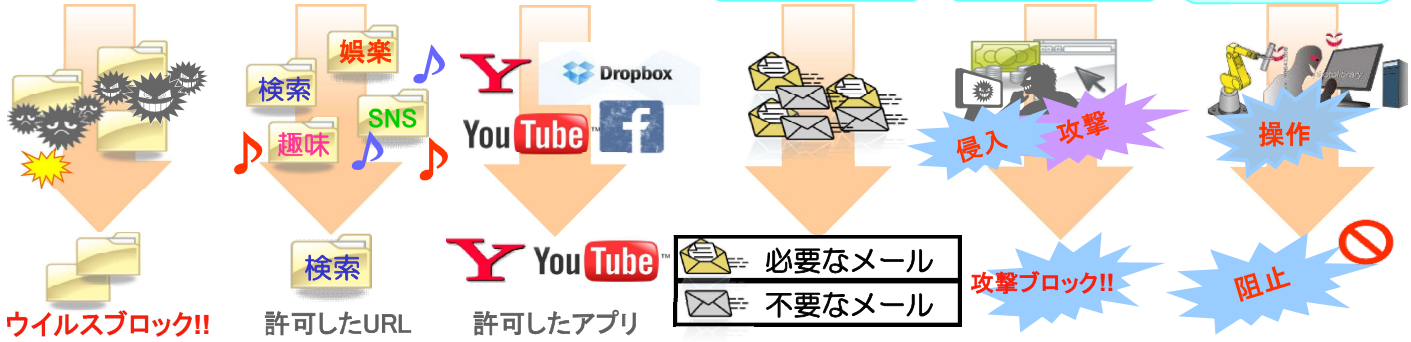
X-CPとは**ネットワークの出入口を守るセキュリティ機器**です。
次のような機能があります。

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

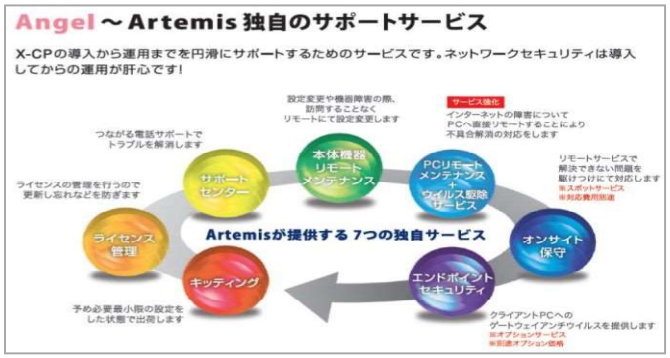
アンチウイルス	URL フィルタリング	アプリケーション コントロール	アンチスパム＆E メールセキュリティ	IPS侵入防止	アンチボット
ウイルスをブロックする機能です	URL閲覧を制限制御する機能です	アプリケーションのアクセス拒否や使用制限をする機能です	スパムメールの識別をし、ウイルス感染を未然に防ぐ機能です	侵入防止システムにより、不正侵入を防ぐ機能です	ボットウイルスによる遠隔操作を防ぐ機能です



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。

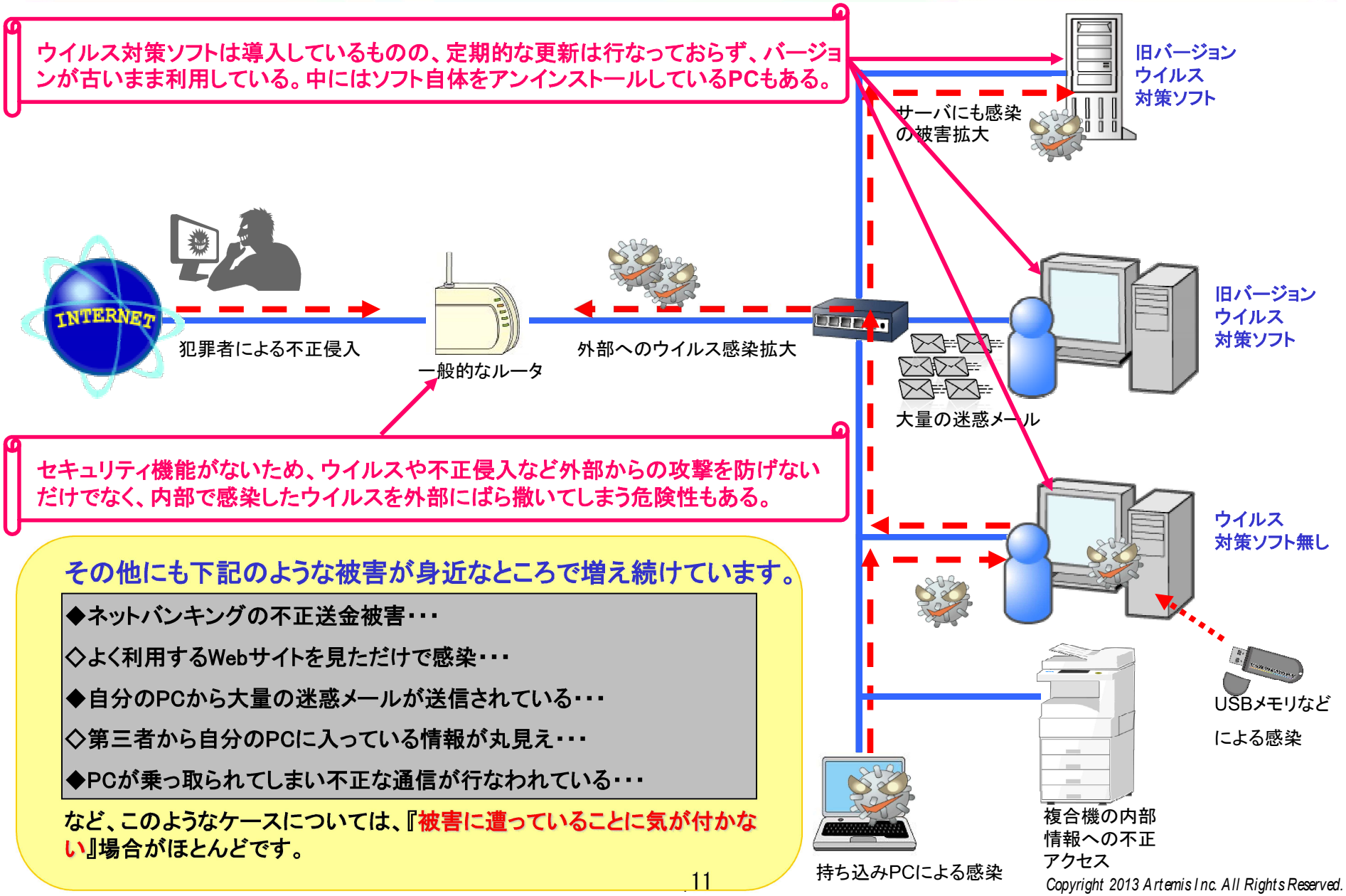


◎詳細なセキュリティレポート機能

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。

UTM設置前の姿（次ﾍﾟｰｼﾞは設置後の姿）

多くの中小オフィスにみられるセキュリティ対策状況



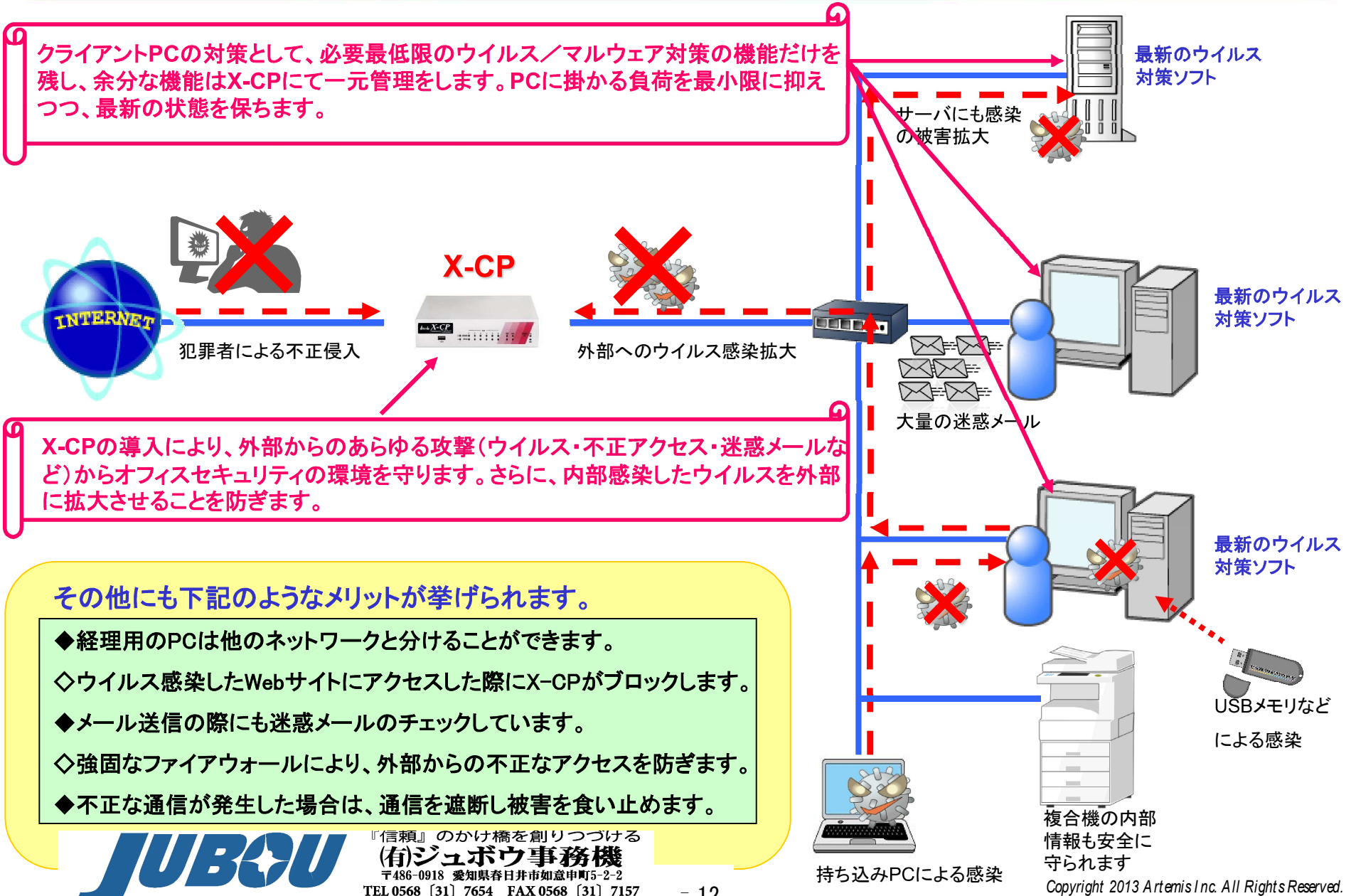
その他にも下記のような被害が身近なところで増え続けています。

- ◆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。

JUBOU Quality & Response
『信頼』のかけ橋を創りつづける
(有)ジュボウ事務機
〒486-0918 愛知県春日井市如意申町5-2-2
TEL 0568〔31〕7654 FAX 0568〔31〕7157
URL http://jubou.com