SOFTCAMP

SHIELDEX

新しい方式の標的型攻撃対策ソリューション

# 外部流入ファイル管理ソリューションの紹介

**株式会社グローバル・アドバンス**

**TEL:03-5543-3682　FAX:03-5543-3730**

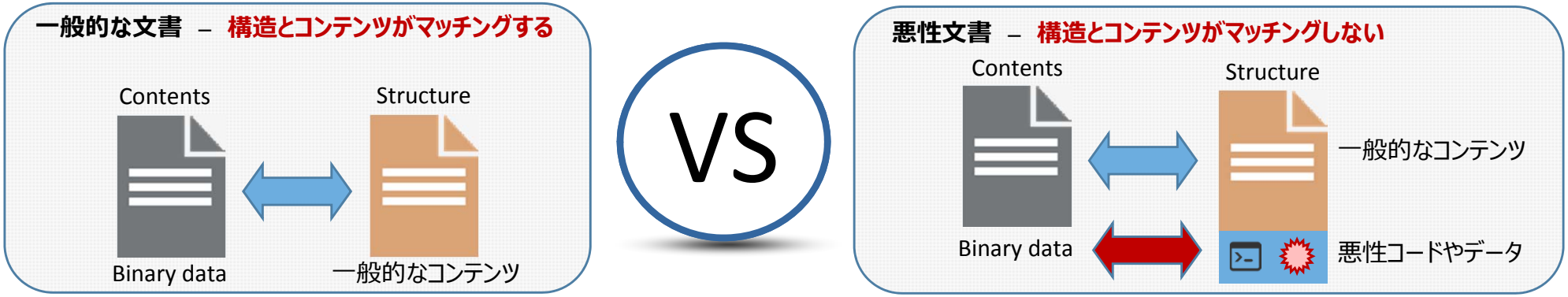
**http://www.g-advance.co.jp/**

## Sanitization (無害化)

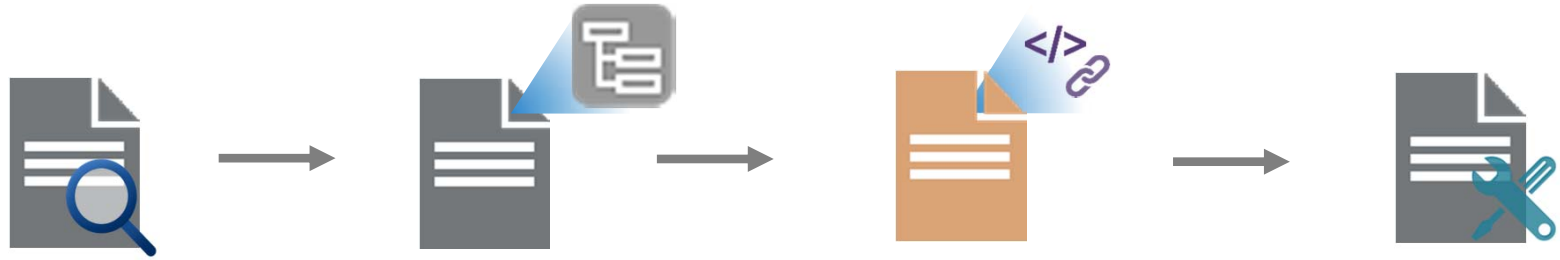
✓ 文書無害化処理エンジンは ① 文書ファイルが一般的な文書ファイルの形であることを確認、② 文書のコンテンツ(文字、イメージなど)構造を検査、③ 安全なコンテンツのみ残して文書を再構成します。

✓ **Sanitization方式を利用した無害化製品は日本で３社が販売しています。そのひとつがSHIELDEXです。**

### 一般的な文書と悪性文書との比較




### 文書の分析 / 再構成の基板説明



**1. Format Verification**
- 対象文書のフォーマット確認
- 拡張子及びヘッダ構造の検査

**2. Structure analysis**
- 文字、図、表など文書内の全ての構成要素の構造を検証

**3. Component Extraction**
- 文書内の構成要素を抽出
- 正しい構成要素かチェック

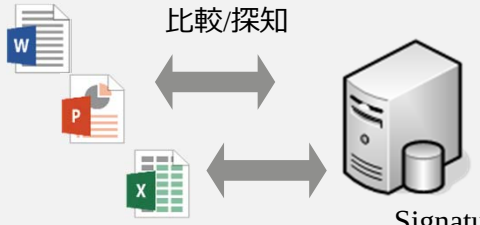
**4. Re-Construction Verification**
- 疑われるコンテンツをチェック及び消去(マクロ、スクリプト、オブジェクト…)
- 抽出された構成要素で文書再構成

## 既存ソリューションと違う点

✓ 既存のアンチウィルスやAPT攻撃対策ソフトは静的解析(Static Analysis)と動的解析(Dynamic Analysis)の方式を利用して悪性コードを検知しますが、SHIELDEXは文書内のVisible Contentsのみ抽出して文書を再構成する**「コンテンツ分析方式」**を使用します。コンテンツの構造を分析して安全なコンテンツで再構成するため、従来のAPT対策ソフトが探知できないファイルに対する対策が可能です。

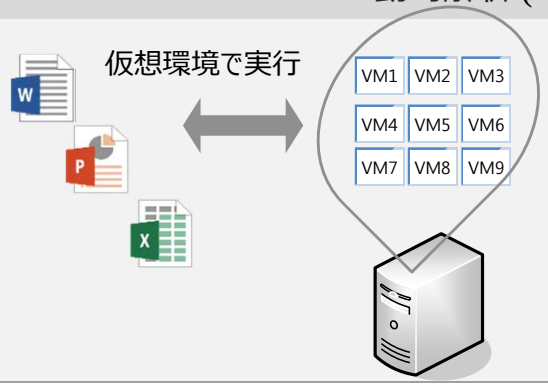
### 既存ソリューションの分析方式

#### 静的解析 (Static Analysis)




- 悪性コードのパターン及びファイル情報をDBに保存して、ファイルを比較して検査する方式
- DBに保存されてない悪性コードが流入される場合、**検知に失敗**します。新規悪性コードの情報がDBに更新されるまで**攻撃に無防備**

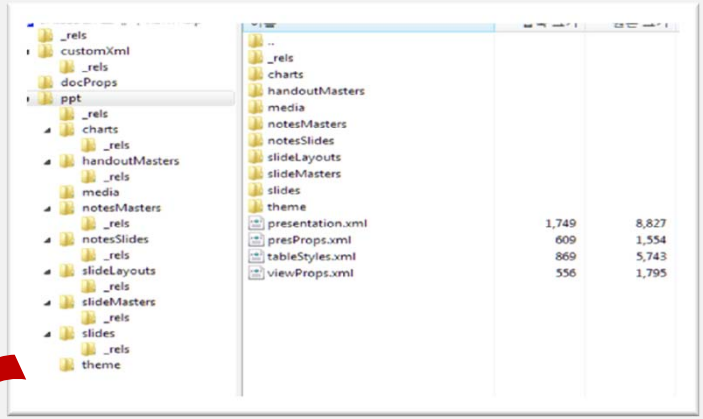
#### 動的解析 (Dynamic Analysis)




- Client環境と同様な仮想環境を複数生成して、ファイルを直接実行しながら悪性可否を検査する方式
- Clientと完全に同じ環境は構成できないし、実行時間設定(ゼロデイ攻撃)や仮想環境上の実行を回避する悪性コードは**検知不可**

VS

### SHIELDEXのコンテンツ分析方式



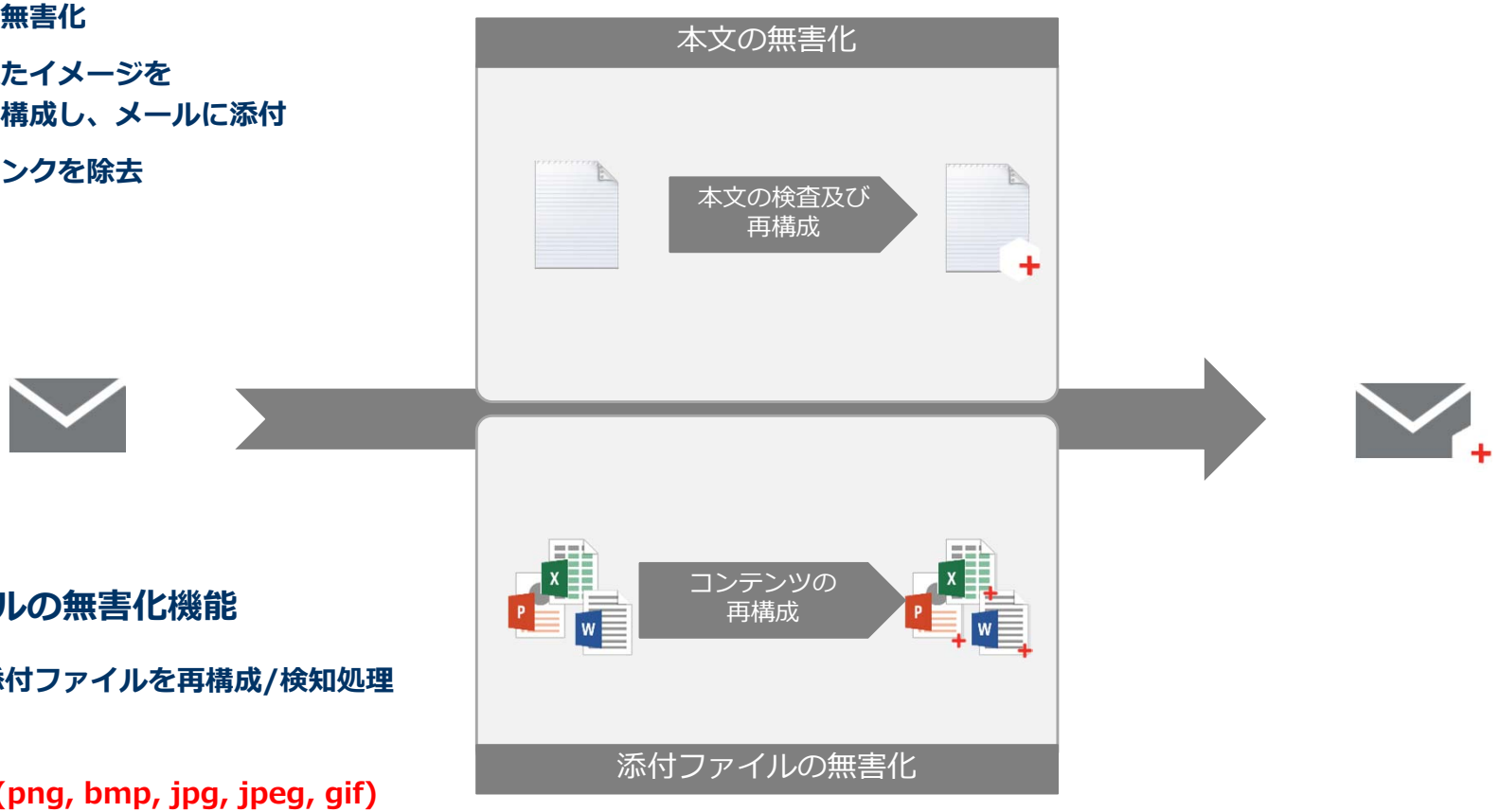

<pptxファイルの構造>

- 文書ファイルの構造を確認して、文書ファイル内のコンテンツを検査
- 文書ファイル内のチャート、スライドレイアウト、スライドマスター、ボディテキストなど必要な情報で安全なコンテンツだけ抽出して文書を再構成(無害化)
- 最近、増加する文書ファイルの形の悪性コード対策に**最適化**

# メール無害化（本文ならびに添付ファイルの無害化）

## メール本文の無害化機能

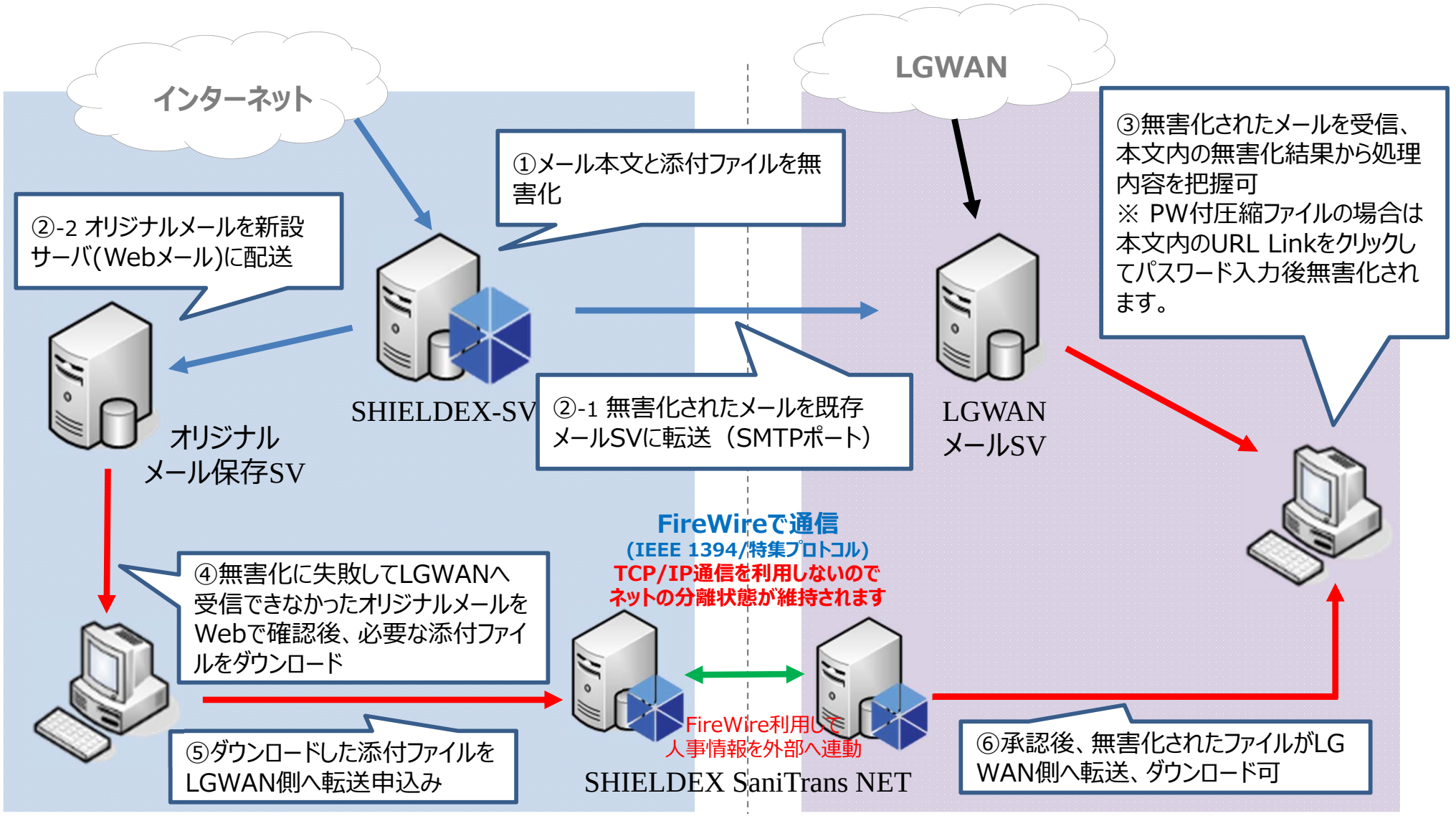
- 本文内容を検知/再構成
- 本文内にスクリプトの有無を確認/除去
- 本文内のイメージを無害化
- 本文内のリンクされたイメージを
  ダウンロードして再構成し、メールに添付
- 本文内のハイパーリンクを除去




## メール添付ファイルの無害化機能

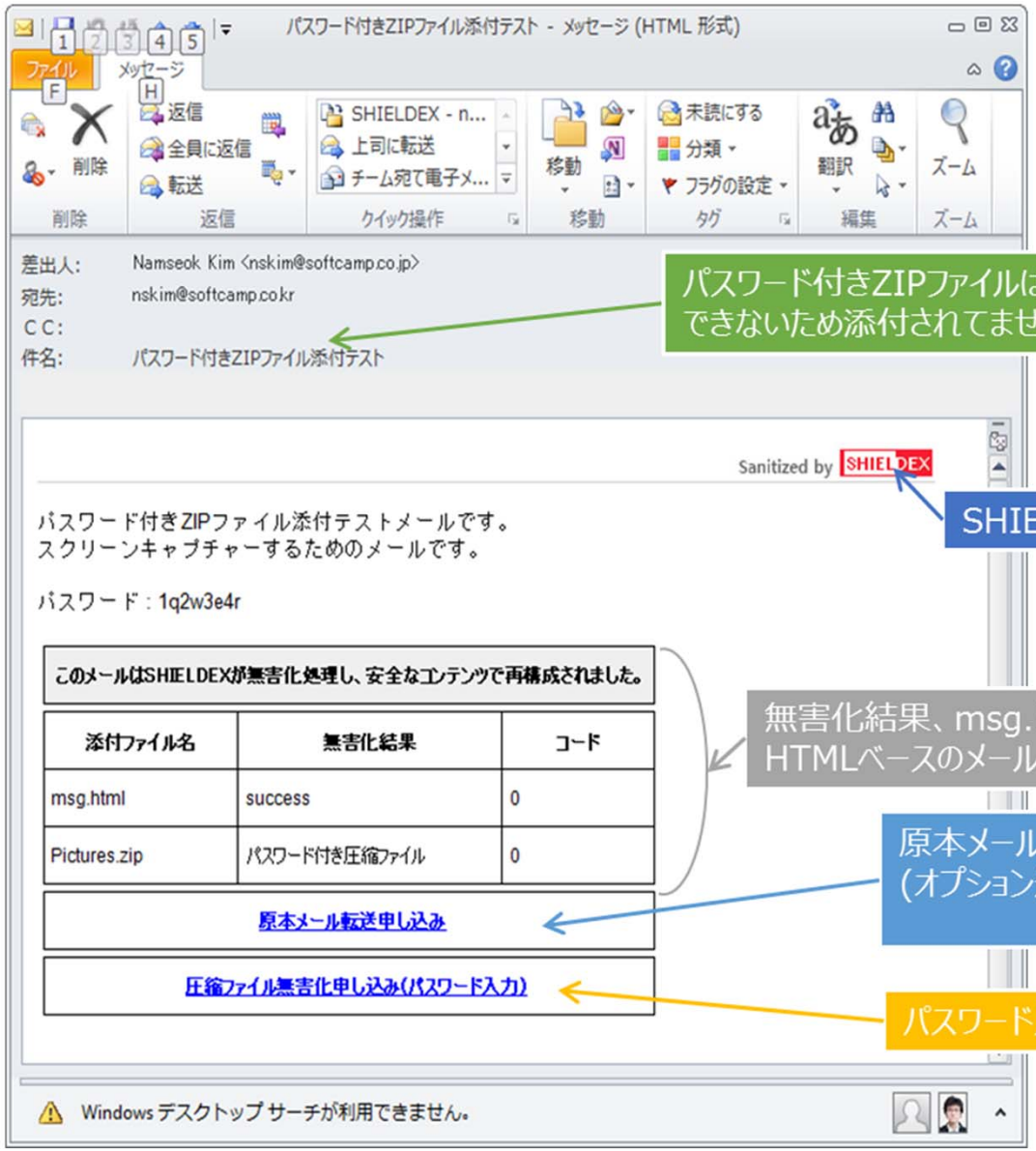
- 受信したメールの添付ファイルを再構成/検知処理
- サポート拡張子
  - PDF, Image (png, bmp, jpg, jpeg, gif)
  - MS Office (doc, docx, docm, xls, xlsx, xlsm, csv, ppt, pptx, pptm)　※オプション(有償)で一太郎のサポートが可能です
  - メールファイル (msg), 圧縮ファイル (zip, lzh)
- 圧縮ファイルは圧縮ファイル内のファイルフォーマットを確認し、無害化処理後に再圧縮にてユーザーへ提供
- 無害化処理結果‘result.txt’ファイルを添付ファイルとしてユーザーへ提供

# メール無害化、ファイル転送・無害化システムの構成例



# SHIELDEXメール無害化システムの特長

## メール無害化結果の表示




◆ 無害化結果の表示

- メール本文の下段にメールの無害化結果及びパスワード付きZIPのパスワード入力URLなどの情報をつ けて送信します。
- ユーザはメール下段の情報をみて添付ファイルの情報や無害化処理結果などがわかります。
- 無害化失敗など安全性が担保できなかった添付ファイルはInternet系のWEBメールで確認
- メール本文がテキストベースの場合、無害化の処理結果は追加で添付されるResults.txtファイルから確認できます。

※ 左記のイメージはメールがHTMLベースの場合の例です。