無害化(CDR)ソリューション

CDR : Content Disarm & Reconstruction

SHIELDEX

メール無害化・ファイル無害化&転送・デバイス無害化

アンチウィルスと ネットワーク分離だけで 標的型攻撃を防護 できると思いますか?

ネットワーク分離環境とメールシステム環境に最適化した標的型攻撃対策ソリューション

SHIELDEXは既存の悪性コード検知方式とは差別されたコンテンツ構造分析(CDR:Content Disarm & Reconstruction)方式を利用して文書内の Visible Contents のみ抽出して文書を再構成するソリューションです。
(無害化できる外部流入ルート : メール添付、USBメモリ、ネットワーク分離環境間のファイル転送、インターネット)

APT(高度な持続型攻撃; Advanced Persistent Threat)は絶えず進化し、企業内の重要データをターゲットしています。

APTに対応するため業務ネットワークとインターネットとの網分離、シグネチャや行為分析、仮想環境での分析などのソリューションを導入して対策を立てていますが、外部から流入されるファイルを分析することだけでは外部からの脅威から完全に防御できません。

SHIELDEX

外部からの攻撃を防御するため既存の方式では新しく生成された悪性コードに対応できない限界があります。
そのため対応方式を変える必要があります。
文書を単純に検査することだけではなく、文書を無害化(CDR)してコンテンツ以外は全て消去するプロセスが必要です。

新しい悪性コードは毎日 **85万個** 生成、 標的型攻撃は去年比 **42%** 増加

最近、悪性コードは、より知能化・組織化され、多様に持続的で新しい変種が出現している。
既存の悪性コード分析方式では新規悪性コードに対して対応不可 。

How does advanced malware act like AI?

CDR(Content Disarm & Reconstruction) コンテンツ無害化&再構成

WIKIPEDIA : Unlike malware analysis , CDR technology does not determine or detect malware's functionality but removes all file components that are not approved within the system's definitions and policies.
WIKIPEDIA : CDR技術はMalware分析方式のようにMalwareの機能性は検知しないが、システムの定義やポリシーで許可されてない全ての構成オブジェクトを消去します。

Because CDR removes all potentially malicious code, it can be effective against zero-day vulnerabilities that rely on being an unknown threat that other security technologies would need to patch against to maintain protection.
新しい攻撃に対応するため他のセキュリティ技術はパッチする必要がある。(パッチされるまでに保護されません。)
CDRは潜在的に悪意のあるコードをすべて削除するため、未知の脅威を利用するゼロデイ脆弱性に対して有効です。

SOFTCAMP

マイナンバー

ISO/IEC 27001：2013

無害化(CDR)ソリューション

CDR：Content Disarm & Reconstruction

SHIELDEX

メール無害化・ファイル無害化&転送・デバイス無害化

01 導入対象

1	ネットワーク分離/メールシステム環境で外部からの流入ファイルに対してセキュリティを考慮している企業及び機関
2	標的型攻撃に対するセキュリティ対策を検討している企業及び機関
3	ゼロディなど未知の攻撃に対する対策の強化を検討している企業及び機関
4	金融/エネルギー/国防などサイバー攻撃からの潜在的対象になりやすい企業及び機関

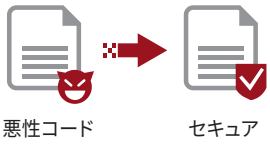
02 主な機能

文書構造スキャン (File Scan)

文書ファイルの構造をスキャンし
文書ファイルの標準構造と違う
疑わしい部分を検知

＋

無害化 (Sanitization)



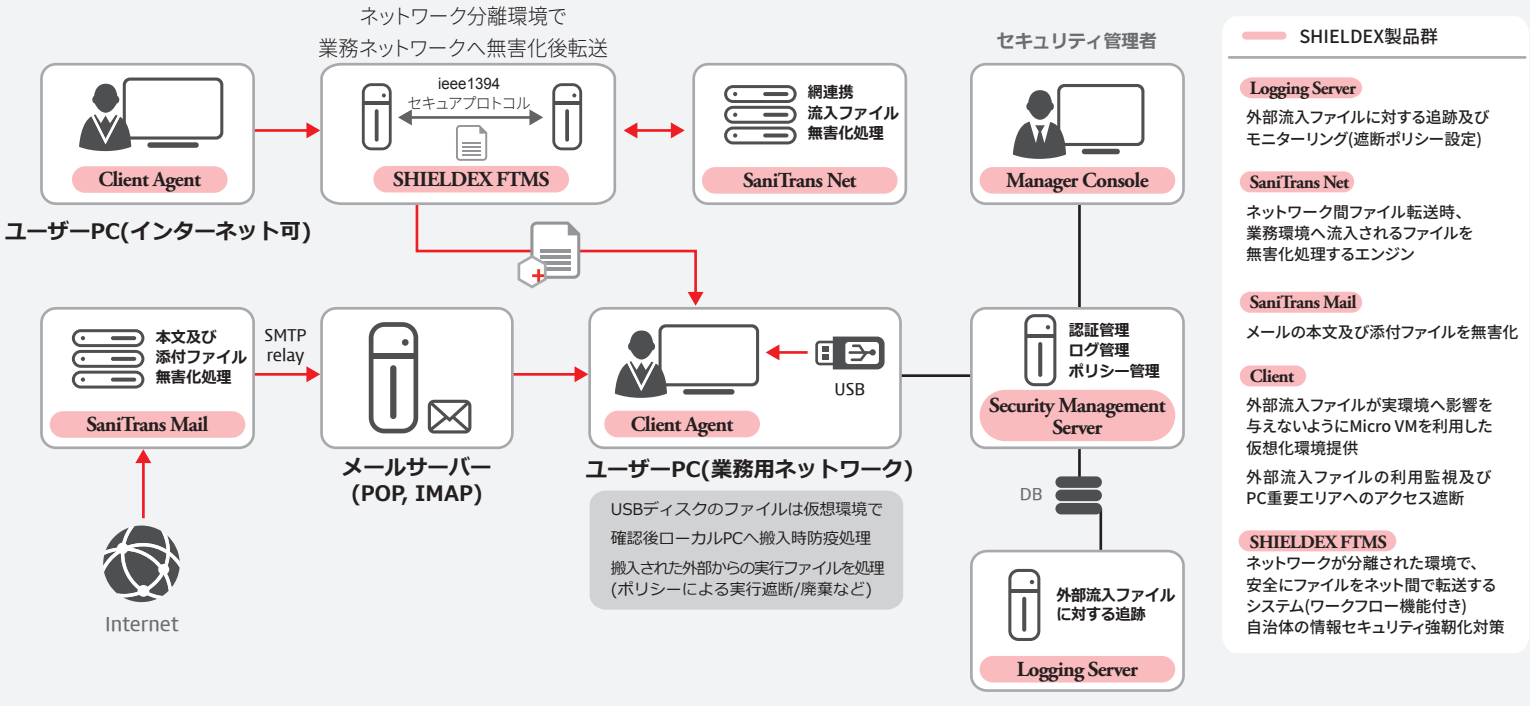
無害化技術を適用し、
疑わしい部分を消去して
安全な文書へ再構成

＋

使用履歴管理 (Logging)

原本ファイルのハッシュコードを
基準にして多様な無害化
処理情報を提供

03 システム構成



SHIELDEX製品群

Logging Server
外部流入ファイルに対する追跡及び
モニターリング(遮断ポリシー設定)

SaniTrans Net
ネットワーク間ファイル転送時、
業務環境へ流入されるファイルを
無害化処理するエンジン

SaniTrans Mail
メールの本文及び添付ファイルを無害化

Client
外部流入ファイルが実環境へ影響を
与えないようにMicro VMを利用した
仮想化環境提供

外部流入ファイルの利用監視及び
PC重要エリアへのアクセス遮断

SHIELDEX FTMS
ネットワークが分離された環境で、
安全にファイルをネット間で転送する
システム(ワークフロー機能付き)
自治体の情報セキュリティ強靭化対策

SOFTCAMP