動作環境一覧

SHIELDEX SaniTrans Mail

SaniTransメールサーバー

OS	Windows Server 2016 / 2012 R2 Standard
CPU	Intel Xeon E3シリーズ以上(4コア以上推奨)
メモリ	4GB以上(8GB以上推奨)
ストレージ	Eドライブ5GB以上(データ保存領域、ログ使用領域を除く)
ネットワーク	Gigabit Ethernet推奨
ブラウザ	Internet Explorer 11
アプリケーション	インストール時に以下のものを含む。 Microsoft .NET Framework 3.5、Microsoft SQL Server 2012 Express、PostgreSQL 9.4、Tomcat 8

クライアントPC

ブラウザ	Internet Explorer 11、Firefox 53以上、Google Chrome 55以上
ディスプレイ解像度	1024×768以上
その他	ネットワークインターフェースを有する。

※利用ユーザー数1,000までを想定したスペックとなります。ユーザー数など利用条件に応じて必要な値やサーバ台数が変動することがあります。詳細はお問い合わせください。
※上記の要件を満たす、すべての環境での動作を保証するものではありません。

SHIELDEX SaniTrans Net

内部／外部サーバー

OS	Windows Server 2016 / 2012 R2 Standard
CPU	Intel Xeon E3シリーズ以上(4コア以上推奨)
メモリ	4GB以上(8GB以上推奨)
ストレージ	Eドライブ1TB以上の空き領域(データ保存領域として)
ネットワーク	Gigabit Ethernet推奨
ブラウザ	Internet Explorer 11
アプリケーション	インストール時に以下のものを含む。 Microsoft .NET Framework 3.5、Microsoft SQL Server 2012 Express、PostgreSQL 9.4、Tomcat 8

クライアントPC

ブラウザ	Internet Explorer 11、Firefox 53以上、Google Chrome 55以上
ディスプレイ解像度	1024×768以上
その他	ネットワークインターフェースを有する。

※利用ユーザー数1,000までを想定したスペックとなります。ユーザー数やファイル暗号化処理の有無など利用条件に応じて必要な値やサーバ台数が変動することがあります。詳細はお問い合わせください。
※内部／外部サーバ間のデータ受け渡しは、中間サーバを利用したネットワーク経由か、IEEE1394ケーブルで直接連結してご利用下さい。IEEE1394ケーブルをご利用の場合は、別途接続ポートが必要となります。
※上記の要件を満たす、すべての環境での動作を保証するものではありません。

SHIELDEX EnCrypto

SCIサーバー/IPDSサーバー

OS	Microsoft Windows Server 2016 / 2012 R2 Standard Edition
CPU	Intel COREi7以上(4コア以上推奨)、Intel Xeon E3シリーズ以上(4コア以上推奨)
メモリ	4GB以上(8GB以上推奨)
ストレージ	5GB以上(データ保存領域、ログ使用領域を除く)
DB	Microsoft SQL Server 2016 / 2012 R2 / 2012

※利用ユーザー数2,000までを想定したスペックとなります。ユーザー数など利用条件に応じて必要な値やサーバ台数が変動することがあります。詳細はお問い合わせください。
※上記の要件を満たす、すべての環境での動作を保証するものではありません。

クライアントPC/コンソールPC

OS	Windows10 / Windows8.1(32bit/64bit)、Windows Server 2016 Standard / Windows Server 2012 R2
CPU	各OSの最小ハードウェア要件以上
メモリ	1GB以上(2GB以上推奨)

※クライアントはWindows Serverをサポートしません。
※上記の要件を満たす、すべての環境での動作を保証するものではありません。

SHIELDEX

SHIELDEX株式会社 https://www.shieldex.co.jp/
Tel: 03-6712-9950 info@shieldex.co.jp

SHIELDEX

SHIELD Your Company from
Security Threats

SHIELDEX

無害化・暗号化・セキュリティソリューション

SHIELDEX

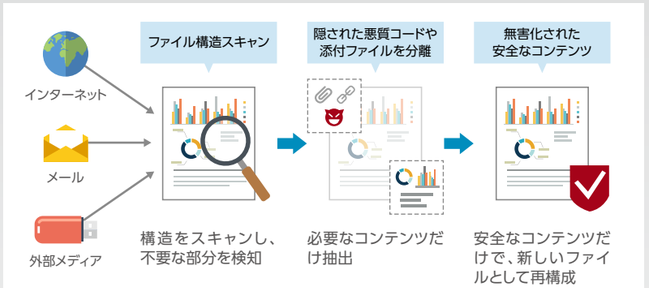
外部脅威と内部脅威。その2つのセキュリティ脅威対策を
SHIELDEXのセキュリティソリューションで一度に実現。

外部脅威対策

メール無害化
SHIELDEX SaniTrans Mail

ファイル無害化
SHIELDEX SaniTrans Net

巧妙化する標的型攻撃やランサムウエアといった代表的な外部脅威は、もはや従来のアンチマルウエア製品では防ぎきれません。SHIELDEXは安全性と利便性を兼ね備えたCDR(Contents Disarm&Reconstruction)技術を取り入れたメール・ファイル無害化サービスを提供します。



3つのポイント

- ☑ 高性能なCDR技術で完全な無害化を実現
- ☑ 無害化エンジンだけでなく、ファイル無害化後の転送システムや承認システムも一括でご提供
- ☑ 無害化後も拡張子はそのまま

サポート対象のファイル形式

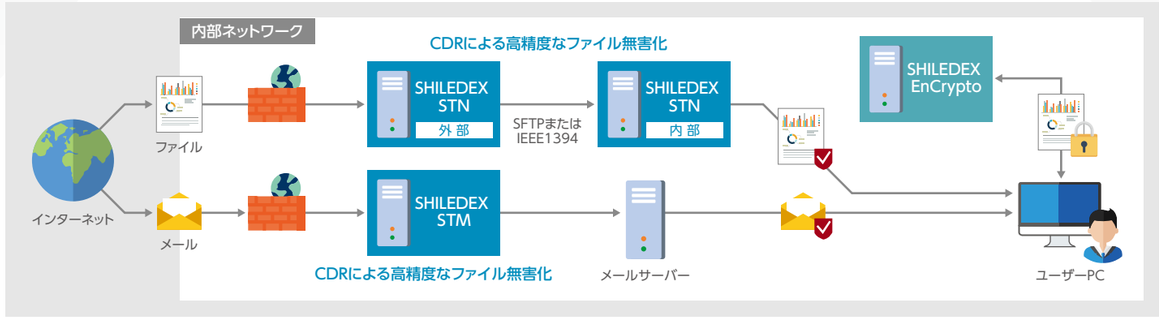
文書ファイル	Microsoft Word：doc、docx、docm Microsoft PowerPoint：ppt、pptx、pptm Microsoft Excel：xls、xlsx、xlsm Adobe PDF：pdf Text ：txt、rtf、csv 一太郎：jtd ※オプション対応
画像ファイル	jpg、jpeg、gif、tif、tiff、bmp、png、ico
圧縮ファイル	zip、lzh
メール	msg、eml
CADファイル	AutoCAD：dwf、dwg、dxf ※オプション対応

CDR技術とは?

一口にメール・ファイルの無害化といっても、HTMLメールや文書ファイルのテキスト化や画像化、別拡張子への変換、マクロ/メタ情報の消去などといった様々な方式があります。しかし、画像化や拡張子を変換されたファイルは、内容の確認はできても編集はできません。またマクロ/メタ情報の除去だけでは未知・変種の悪性コードに対抗できない場合もあります。
CDRとは、メールやファイルをスキャン後、標準構造上で不要な部分を取り除き、必要なコンテンツだけを抽出した上で新たなファイルに再構成する技術です。拡張子の変換もないので、業務上不便になることもありません。

無害化 & 暗号化

SHIELDEXのセキュリティソリューション 導入イメージ(メール・ファイル受信時)



※各サービス単体でのご契約も可能です。

内部脅威対策

ファイル自動暗号化
SHIELDEX EnCrypto

脅威は外部だけではなく、組織内部にも潜んでいます。内部不正のほかにも、誤操作や管理ミスといったヒューマンエラーから機密情報が漏えいする可能性があります。そのような内部脅威対策として、SHIELDEXはファイル暗号化サービスをご提供。SHIELDEXの無害化サービスとシームレスに連携し、暗号化ファイルの無害化も対応しています。

作成したファイルは保存時に自動暗号化され、開く際は自動的に復号化されます。拡張子の変更もありません。

特定のフォルダに暗号化の対象となるファイルを入れると、自動的に暗号化されるように設定できます。
※オプション対応

3つのポイント

- ☑ 暗号化後も拡張子はそのまま
- ☑ ファイル検索、ログ管理が可能
- ☑ SHIELDEX無害化製品とシームレスに連携

サポート対象のファイル形式

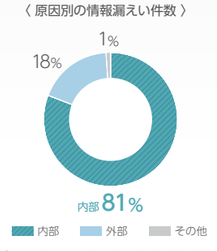
文書ファイル	Microsoft Word：doc、docx Microsoft PowerPoint：ppt、pptx、pps、ppsx Microsoft Excel：xls、xlsx、xlsm、xlsb Adobe PDF：pdf Text：txt、rtf、csv 一太郎：jtd
画像ファイル	jpg、jpeg、gif、tif、tiff、bmp、png、dib

column ファイル暗号化の重要性

個人情報漏えい原因の約80%が組織内部で起こったものとされています。働き方改革の一環としてテレワークの普及が求められている今、内部脅威の対策がより必要とされており、ファイル暗号化やログの管理は有効な対策の1つとして重要視されています。

内部	誤操作	97件	25.1%
	紛失・置忘れ	84件	21.8%
	管理ミス	50件	13.0%
	不正な情報持ち出し	25件	6.5%
	盗難	25件	6.5%
	設定ミス	18件	4.7%
	内部犯罪・内部不正行為	8件	2.1%
外部	不正アクセス	67件	17.4%
	バグ・セキュリティホール	5件	1.3%
	ワーム・ウイルス	2件	0.5%
その他	その他	3件	0.8%
	不明	2件	0.5%

〈 原因別の情報漏えい件数 〉



参考：2017年 情報セキュリティインシデントに関する調査報告書【速報版】第1.0版2018年6月13日 P4図(3):漏えい原因 特定非営利活動法人日本ネットワークセキュリティ協会(JNSA)