INFORMATION SECURITY

製造業における情報セキュリティ
CADを含む情報セキュリティについて

裁判の判例を踏まえて・・・

Pico Technologies

不正競争行為差止等の請求事件

原告

- 真空ポンプ、真空システム、ブロワー及び関連機器の販売、修理を行う株式会社
- 昭和56年6月設立

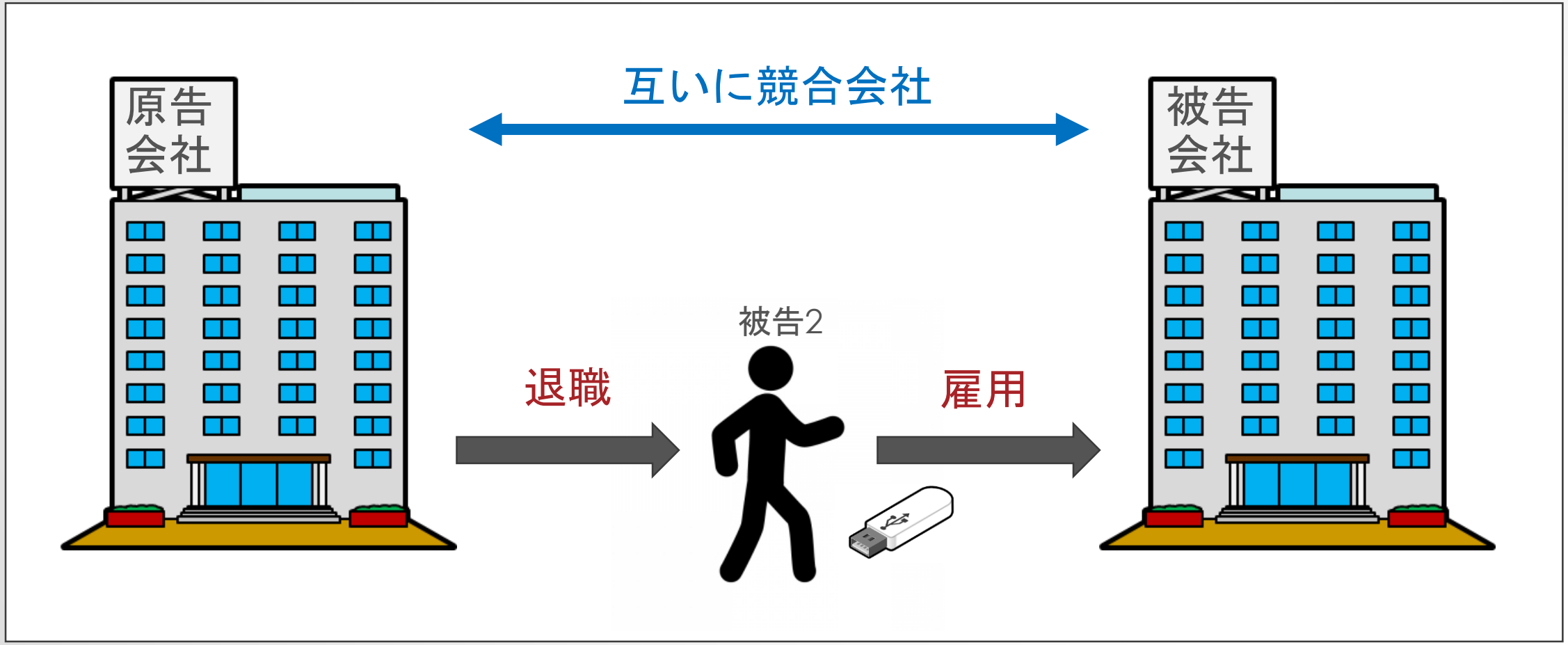
被告１

- 真空ポンプ、ブロワー、その他空気圧縮関連機器の付属品、部品の販売、修理加工及び輸出入を行う株式会社
- 平成6年10月設立

被告２

- 平成25年6月1日に原告に入社し、その後原告を退職する平成27年6月30日までの間、原告におけるセールス本部長、東日本グループのグループリーダーの役職にあった者

原告の主張



INFORMATION SECURITY

原告が主張している事件の全容

社内のファイルサーバ

被告2

被告2

平成26年12月18日と平成27年3月27日の2回にわたり、サーバに不当な目的をもってアクセスし、

営業情報をUSBメモリにコピーをして持ち去った。

Pico Technologies

原告の請求

損害賠償請求

本件情報の窃取について、調査及び対応に費やした作業等の費用の合計１，４６４，６７６円を請求

不当利得返還請求

被告２の原告在職中の就業規則違反に対する減給処分として、合計４２，６７６円の給与返還を請求

原告が提示した証拠

- SKYSEAの資産管理情報から、「被告２が使用していた端末の特定」証拠
- SKYSEAの操作ログから、「被告2使用端末のサーバアクセス記録」証拠
- SKYSEAの操作ログから、「被告2使用端末のUSBメモリコピー記録」証拠

SKYSEA Client View

原告に対する裁判所の指示

立証

- 営業機密と主張している情報が秘密に当たるかを立証せよ。

裁判所の判断基準

- 有用性（秘密内容）
- 秘密管理性

裁判所の主張

- 情報の持出しが不当競争行為に当たるのであれば、情報に接したものを明確に認識できる程度に管理されていたのかが重要な点

INFORMATION SECURITY

判決と判決に至る経緯

原告会社

全ての情報を秘密情報として立証するのは困難と判断	被告会社がアプローチしていたと思われる特定の顧客に本件を絞り込む

被告会社

原告会社が特定した顧客は、以前に展示会に来てアンケート用紙に記入していたことを証拠として提出

裁判所

原告会社の秘密を被告会社が流用したことは認めがたいと判断	被告会社に提訴取り下げもしくは和解を提案

Pico Technologies

判例から抑えるべき重要なポイント

- ✓ **「有用性」**

  その秘密情報が、「役立つ傾向」「有効に機能する性質」「有益な性能を持つ性質」であることが必要

- ✓ **「秘密管理性」**

  その保有者が主観的に秘密にしておく意思を有しているだけではなく、従業者、外部者から、客観的に秘密として管理されていると認められる状態にあることが必要

- ✓ 「秘密管理規定」の有無

秘密管理性の判断の傾向

1．アクセスできる者が限定され、権限のない者によるアクセスを防ぐような手段が取られている（アクセス権者の限定・無権限者によるアクセスの防止）

2．アクセスした者が、管理の対象となっている情報をそれと認識し、またアクセス権限のある者がそれを秘密として管理することに関する意識を持ち、責務を果たすような状況になっている（秘密であることの表示・秘密保持義務等）

3．それらが機能するように組織として何らかの仕組みを持っている（組織的管理）

結論

「秘密管理性」を実証するのは困難

結果として「取られ損」になる可能性が高い

↓

情報を取られることを前提にした対策が必要

INFORMATION SECURITY

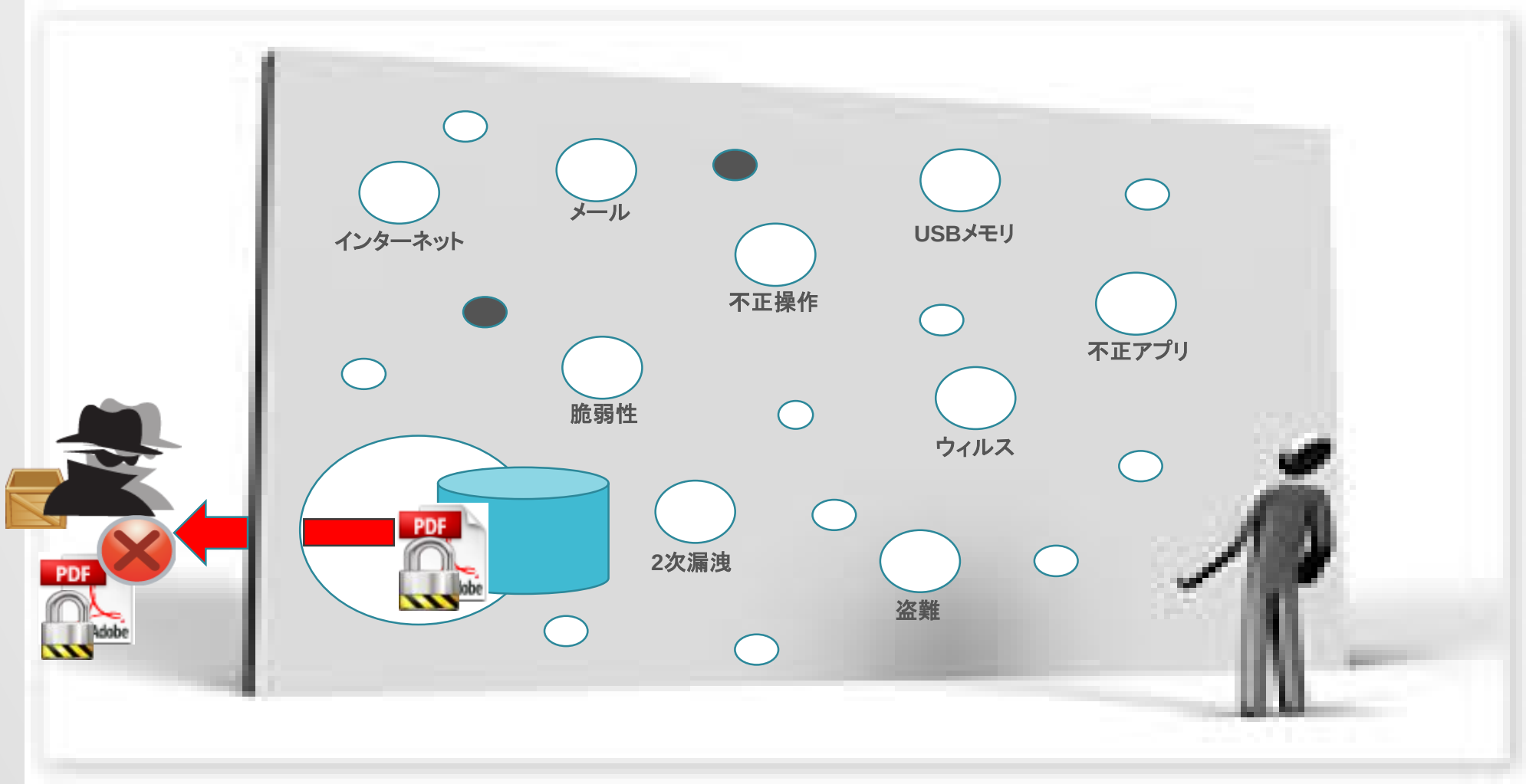
情報漏洩対策の手法

操作ログ収集とログ監査	•秘密管理性の観点から情報漏洩対策にはならない。
PCの操作制御と機能制限	•大幅に仕事のやり方を変える必要がある。 •セキュリティを重視することで、機能制限が多くなり業務効率が低下する。
ファイル暗号の活用	•適応範囲と運用ルールを決めることは必要だが、社内のみならず社外の運用も考慮したセキュリティ対策が可能 •段階的且つ、ルールやポリシーの強弱の調整も可能。
シンクライアントの活用	•仕事環境がVDIにより統一でき、かつ情報の閉鎖的運用ができれば有効な手段となる。 •コスト高が唯一の欠点。

Pico Technologies

INFORMATION SECURITY

ファイル暗号化の有用性



Pico Technologies

INFORMATION SECURITY

ファイル暗号化と情報の「秘密管理性」

秘密管理性

暗号ファイルにアクセスできる者を限定できる

ファイルを暗号化することで、情報が秘密として管理される

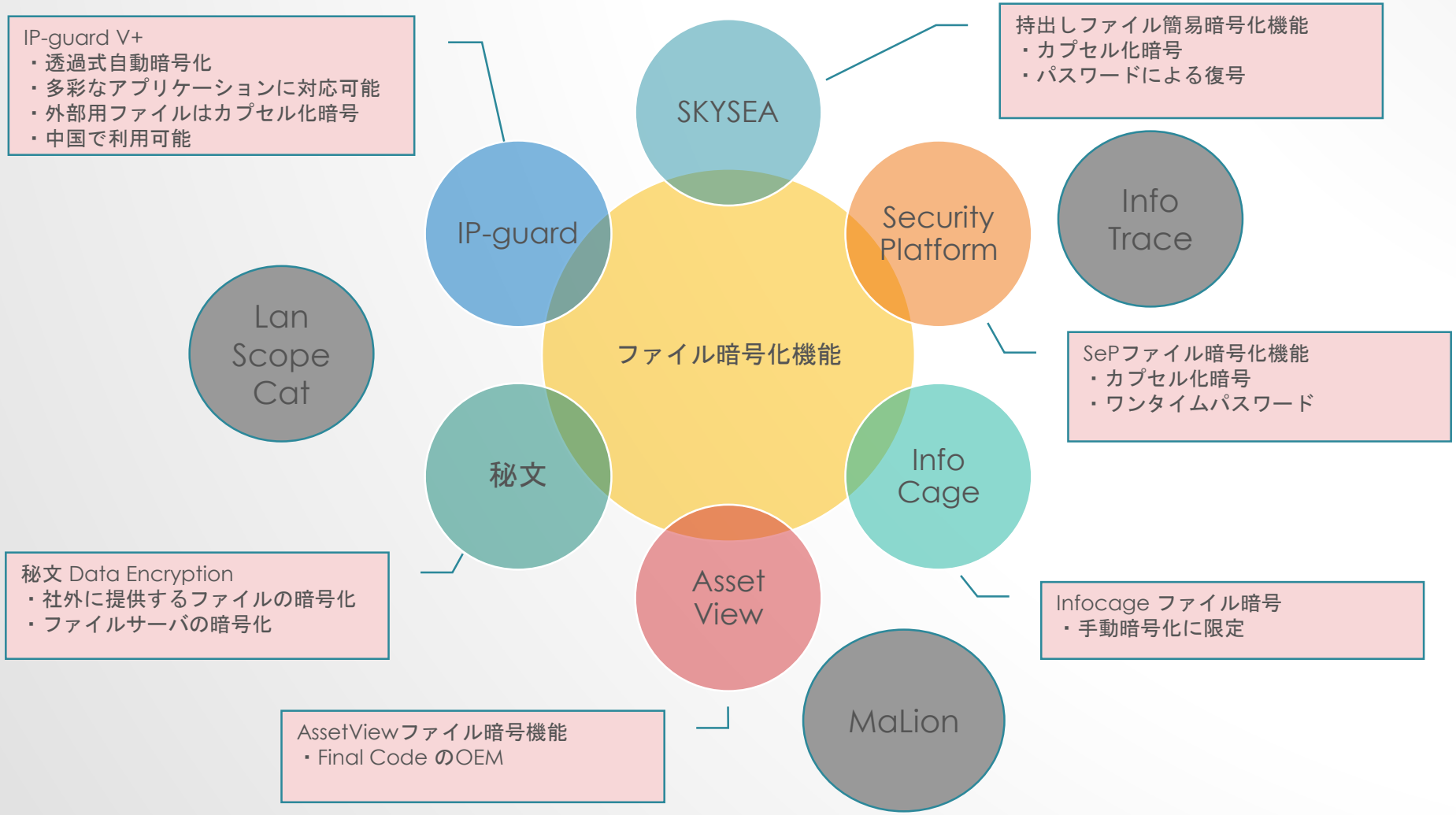
暗号ファイルを扱う者に、秘密情報であることを意識させることができる

暗号ファイルの組織的管理ができる

Pico Technologies

INFORMATION SECURITY

資産管理製品のファイル暗号化機能



Pico Technologies

INFORMATION SECURITY

ファイル暗号化製品一覧（参考資料）

製品名	特長
Total File Guard (SECWARD)	ファイル自動暗号化に特化したセキュリティ製品。 ファイル作成時から自動的に暗号化し、暗号化ファイルを暗号化状態のまま扱える為、ユーザが意識せずに運用できる。 ほぼ全てのWindowsアプリケーションに対応可能。 フォルダ監視型の暗号・復号機能あり。 利用環境における制限は少なく、オフライン環境（外部端末）にも対応。 ファイル形式を変えずに暗号化されるため、アプリケーションでそのまま暗号ファイルを開くことができる。
IP-guardV+ (TEC Solitions Limited)	ファイル自動暗号化に特化したIP-guard 製品の１モジュール。ファイル暗号化以外で「資産管理」「端末制御」「操作ログ」などのエンドポイントセキュリティモジュールと合わせて利用可能。 ファイル暗号化機能は、Total File Guardとほぼ同等。 また外部においては、専用のOEA形式のファイルを利用する事でアプリケーションとロケーションを問わずエージェントレスで暗号化ファイルを利用できる為、現状の運用に合わせて使用できる製品。
InterSafeIRM (ALSI)	ファイル暗号機能は、Total File Guard , IP-guard V+とほぼ同等。 利用環境における制限が多く、CAD のような大容量ファイルには不向き。 ユーザ側でアプリケーション対応設定が可能だが、あくまでユーザ責任の対応となる。
FinalCode (Digital Arts)	社外に出すファイルを対象とするファイル暗号製品。 ファイル利用者はオンライン認証が必要な為、外部であってもオンライン環境が必要。 ファイルの暗号化は自動ではなく、対象ファイルを手動で暗号化するか、指定フォルダに対象ファイルを入れることで暗号化される。 暗号ファイルは専用のファイル形式になるため、CAD のような構造体のファイルは扱えない。 特殊なアプリケーションの対応が難しいため、暗号ファイルを復号化してからアプロケーションで扱うことが多い。
InfoCage FileShel (NEC)	ActiveDirectoryのRMS機能を拡張した暗号化製品。 AD認証がベースの為、オフライン時やワークグループPCがある場合、使い方が変わる為注意が必要。 ファイルの暗号化操作は、特定フォルダに入れるもしくは手動で設定。 標準機能では社外で暗号化ファイルを開く為に「エージェント ＋ オンライン認証」が必要。 社外用暗号化オプション（持出閲覧形式保護オプション）はファイル形式が変わる為、アプリケーションを立ち上げてからファイルを読み込むことができない。
DataClasys (NESCO)	暗号化ファイルを直接扱えるアプリケーションが多い事が特長。 ファイルの暗号化は自動ではなく、対象ファイルを手動で暗号化するか、指定フォルダに対象ファイルを入れることで暗号化される。 外部利用については、パスワード付きファイルのみの運用になる。
Document Security (SOFTCAMP)	ファイル単位で細かい制限を設定できるのが特長。 Word,Excel,PowerPoint,Acrobat以外のアプリーションは自動暗号化ができない為、それ以外のアプリケーションで暗号化の運用をする場合、手動暗号→利用者が手動暗号解除してファイルを扱うことになる。
秘文Data Encryption (HITACHI)	ディスク暗号（HDDやフォルダ、USB）がメインの製品の為、「内部PCの紛失・盗難対策」には適している製品。反面、ファイルでは無く環境を守る製品の為、内部で扱うファイルは暗号化されておらず、ファイルが持ち出されてしまうと守ることができない。外部に対して「自己復号化型暗号化ファイル」を渡す製品だが設定はパスワードのみの為、パスワードを解読すると誰でも自由に使用できてしまう。 最新の機能としては、社外用暗号化機能を FinalCode を OEM として組み込んでいる。 加えて、使用できる環境は英語版／日本語版OSのみで、中国の暗号化規制に引っかかる製品の為、グローバルの使用には向いていない。

INFORMATION SECURITY

製造業で多くの実績を持つファイル暗号化製品

IP-guard V+

ファイル暗号機能と記録・制御・資産管理機能を合わせ持つ統合セキュリティソフト

TotalFileGuard

ファイル暗号に特化したシンプルなセキュリティツール

Pico Technologies

INFORMATION SECURITY

共通的な特徴

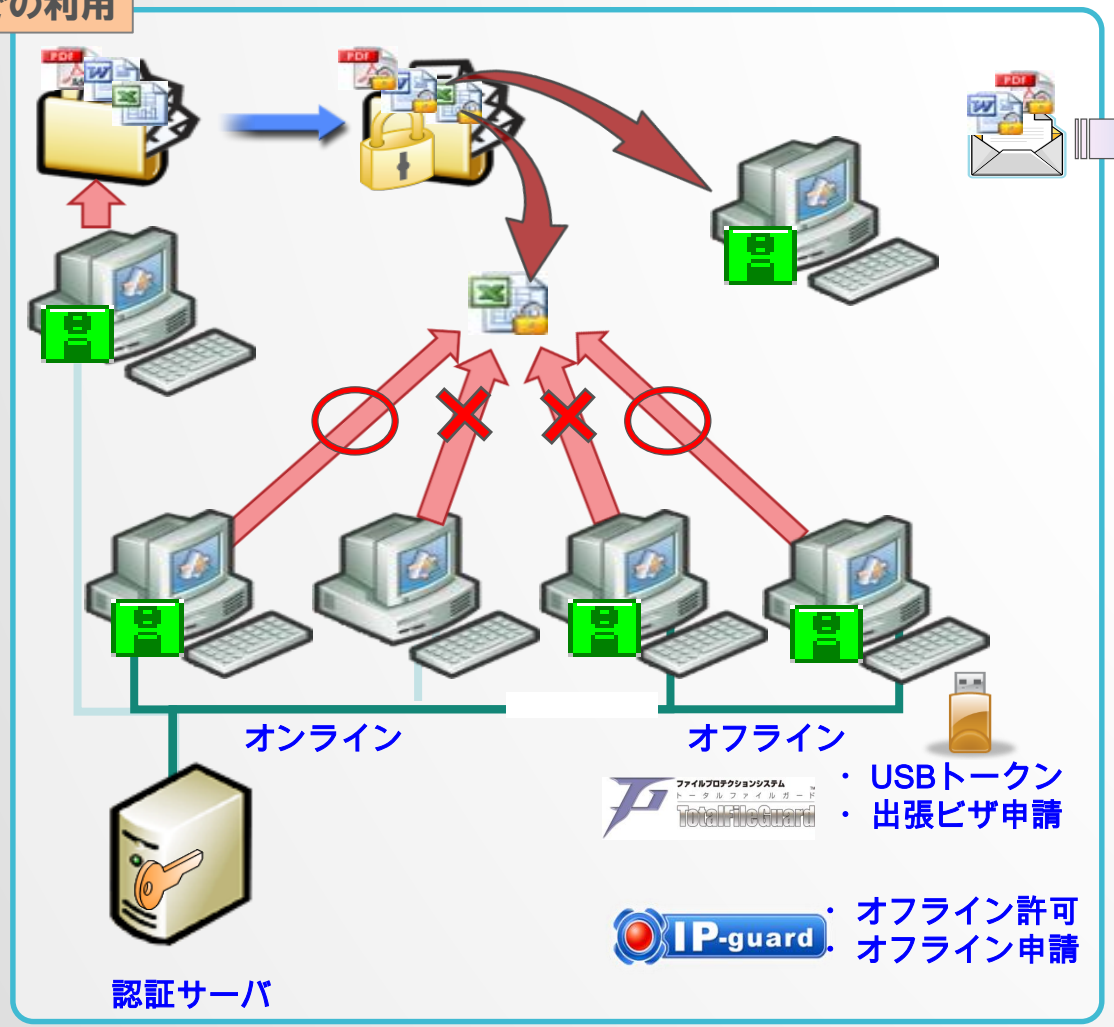
- Windowsのほぼ全てのアプリケーションに対応（許可アプリの設定機能あり）
- ユーザに意識をさせない自動暗号と内部復号
- ファイルのタイムスタンプを変えない暗号化
- ファイル形式やファイル拡張子を変えない暗号化
- ファイル容量やファイルを開く速度も気にならない
- フォルダ暗号機能あり
- オフライン対応あり
- 中国国内でも申請なしで使用可能

Pico Technologies

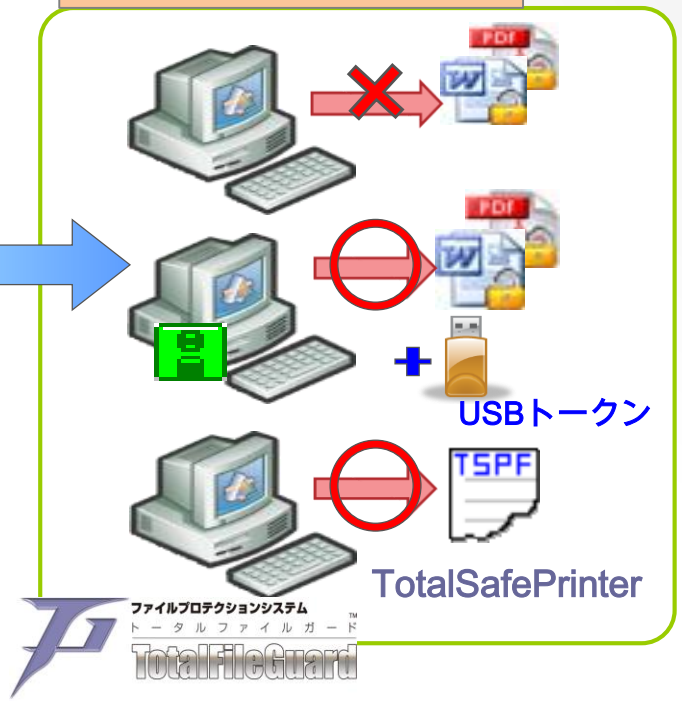
INFORMATION SECURITY

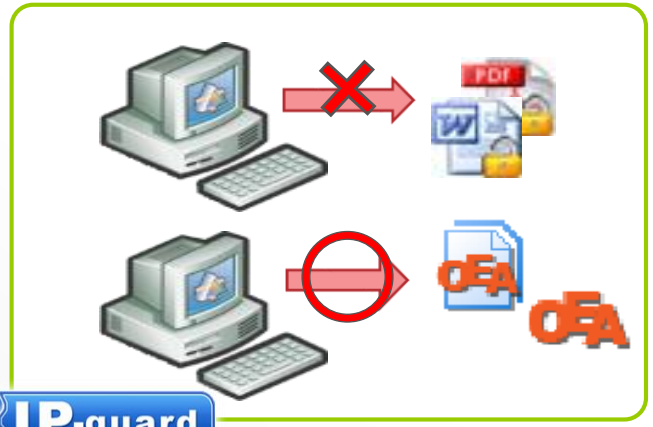
２つの製品でできること

社内での利用



メールでファイル送信（社外）





Pico Technologies

INFORMATION SECURITY

オフライン機能の違い

◆IP-guard V+のオフライン機能

- オフラインはカプセル化技術を採用
- ID登録によるオフライン認証
- オフラインPC側でOEA Viewerを起動するだけで利用可能
- カプセル化できるファイルのファイル構造によっては一部利用制限あり
（1つのファイルが複数ファイルで構成される場合、全てのファイルをカプセル化しておく必要がある）
- 利用者側のアプリケーションを把握する必要なし

◆TotalFileGuardのオフライン機能

- オフラインは直接暗号技術を採用
- USBトークンによるオフライン認証
- オフラインPC側には専用ソフトのインストールが必要
- 暗号化できるファイルのファイル構造に制限なし
- 利用者側のアプリケーションを把握し、専用ソフトに使用アプリケーションの設定が必要

Pico Technologies

INFORMATION SECURITY

海外の暗号化事情（中国）

製品	対象使用	使用規制	必要な手続き
中国国内で生産された暗号化製品	中国国内の組織	中国国内で自由に使用できる。	なし
	中国国内の個人		
中国国外で生産された暗号化製品	中国国内の組織	外商投資企業（注）に限り、 中国国外の投資者との間で、内部業務情報に対する暗号化保護 又は安全認証のためにのみ使用できる。	国家暗号管理機構に、国外製造の暗号化製品使用登記 を行い、「国外生産の暗号化製品使用許可証」を取得 しなければならない。
	中国国内の個人	中国国内で使用してはならない。	申請を受け付けない。

（注）「外商投資企業」とは、外国投資者が出資して設立した現地法人を指す。合弁企業、合作企業、100%外資 企業などがある。

Pico Technologies

海外の暗号化事情（ロシア）

利用すべき暗号方式

連邦技術規制・計測庁が標準化している以下の暗号方式をGOST 標準暗号として利用しなければならない。

- GOST 28147-89：ブロック暗号
- GOST R 34.10-94：公開鍵暗号(署名)
- GOST R 34.10-2001：公開鍵暗号(署名)
- GOST R 34.11-94：ハッシュ関数(メッセージダイジェスト)

暗号の輸出入規制

- 共通鍵アルゴリズムの場合で鍵長56 ビット以下、公開鍵暗号アルゴリズムの場合 で鍵長512 ビット(素因数分解・離散対数)以下のもの
- 一般に提供されている OS のコンポーネントでありユーザが変更不可なもの
- 金融機関などの利用に限定されるもの
- 無線通信装置(伝達距離400m 以下)

INFORMATION SECURITY

欧州連合の一般データ保護規則(GDPR)

- 2018年5月25日より適応
- EEA加盟国における「個人データ」の「処理」と「移転」に関する法
- 個人データとは
  - 自然人の氏名、識別番号、所在地データ、メールアドレス、オンライン識別子(IPアドレス、クッキー識別子)
  - 身体的、生理学的、遺伝子的、精神的、経済的、文化的、社会的固有性に関する要因
- 処理の定義
  - クレジットカード情報の保存
  - メールアドレスの収集
  - 顧客の連絡先詳細の変更
  - 顧客の氏名の開示
  - 上司の従業員業務評価の閲覧
  - データ主体のオンライン識別子の削除
  - 全従業員の氏名や社内での職務、事業所の住所、 写真を含むリストの作成
- 移転の定義
  - 個人データを含んだ電子形式の文書を電子メールでEEA域外に送付することは「移転」に該当

「処理」または「移転」により取得した個人データの取り扱いにおいて、管理者は、GDPRの個人データ処理に関係する諸原則を遵守することに責任を負い、かつ当該諸原則の遵守を実証することを義務付けている。すなわち、企業や団体の側に GDPRを遵守していることを証明することが義務付けられているのであり、この証明ができなければ、GDPR 違反が認定されやすいということになる。

Pico Technologies

INFORMATION SECURITY

導入を成功させるためのステップ

ファイル暗号化運用の実現のために、各ステップごとの検討が必要となります。

- ■セキュリティポリシーを検討
- ■運用ルールを検討
- ■暗号化対象アプリケーションの制御設定
- ■制御設定できないアプリケーションについては、対策を検討

上記作業につきましては、コンサルティングサービスとして提供

Pico Technologies

INFORMATION SECURITY

運用立ち上げ支援の一例

	項目	担当
STEP2:CATIAデータの保護		
1	暗号対象データの検討と決定	お客様
2	暗号対象アプリケーションの検討と決定	お客様
3	アプリケーション対応作業と動作検証	PICO
4	暗号ファイルのファイル管理系システムへの影響範囲を調査	お客様
5	ファイル管理系システムへの対応方法の検討	お客様
6	ファイル管理系システムの対応作業と動作検証	PICO
7	ファイル暗号化運用の組織的範囲の検討	お客様
8	社内運用上の不具合の洗い出しと対策の検討	お客様
9	運用ルールの策定	お客様
10	テスト運用	お客様
11	本番運用スタート	お客様
STEP3:全データの保護及び関連会社間データ授受		
1	暗号対象データの検討と決定	お客様
2	暗号対象アプリケーションの検討と決定	お客様
3	アプリケーション対応作業と動作検証	PICO
4	暗号ファイルのファイル管理系システムへの影響範囲を調査	お客様
5	ファイル管理系システムへの対応方法の検討	お客様
6	ファイル管理系システムの対応作業と動作検証	PICO
7	ファイル暗号化運用の組織的範囲の検討	お客様
8	社内運用上の不具合の洗い出しと対策の検討	お客様
9	運用ルールの策定	お客様
10	社外運用上の不具合の洗い出しと対策の検討	お客様
11	社外運用ルールの策定	お客様
12	社内外のテスト運用	お客様
13	本番運用スタート	お客様

- 第二、第三ステップの具体的なスケジュールは別途ご相談させて下さい。
- 第一ステップの経験を活かし、第二、第三ステップはお客様単独の検討が可能と想定しています。
- 但し、ご依頼いただければ弊社との共同作業も可能です。
- アプリケーション対応作業につきましては、弊社が実施いたします。

Pico Technologies

INFORMATION SECURITY

ファイル暗号化運用の落とし穴

ファイル暗号技術を取り入れるのは簡単だが、セキュリティレベルと運用レベルはトレードオフの関係となるため、**ファイル暗号化運用**を十分理解することが重要

【運用レベルを下げる要因】
・今までできていたコピー＆ペーストができない。
・今までできていたキャプチャー（プリントスクリーン）ができない。
・今までできていたPDF変換ができない。
・今までできていた他種アプリテーションへの取り込みができない。
・今までできていたファイルの提供や共有ができない。

これって、できるようにするべき？

それで情報流出守れるの？

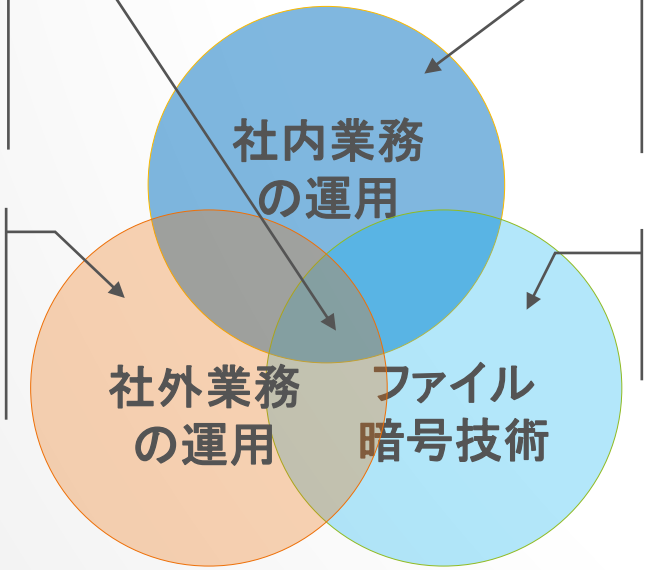
Pico Technologies

INFORMATION SECURITY

導入を成功させるための秘訣

社内外の業務の運用把握とファイル暗号技術でできることを理解する

社外業務の運用をどこまで把握できるか？
制限できるか？



社内業務の運用をどこまで把握できるか？
制限できるか？

ファイル暗号技術に求められる機能を定義する

モノづくりの業務と運用を理解したセキュリティ製品に詳しいコンサルタントを活用

Pico Technologies

INFORMATION SECURITY

Pico Technologies

http://www.pico-t.co.jp

Mailto:Info@pico-t.co.jp

TEL:03-6403-0906

Pico Technologies