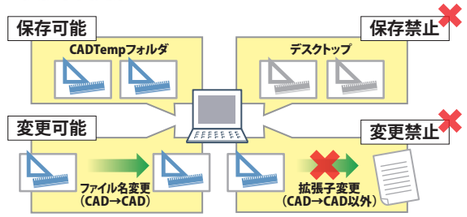
■お客さまでのDigital Guardian活用事例

課題① 設計データの管理強化

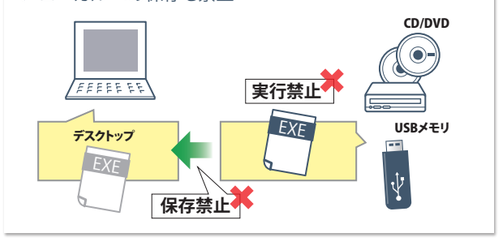
■CAD ファイルの保存ルールを徹底

✓CADファイルは特定のフォルダにのみ保存可能
✓拡張子変更禁止



■不要プログラム(マルウェアなど)の侵入・実行防御

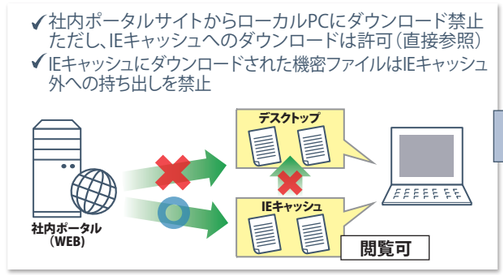
✓外部媒体からの実行ファイル(.exe .bat)を実行禁止
✓ローカルへの保存も禁止



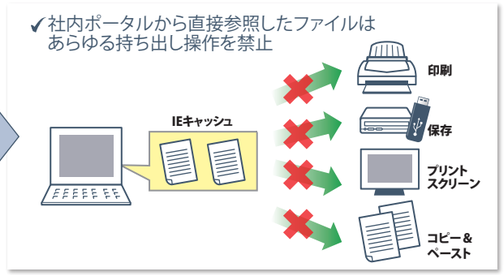
課題② 社内ポータルの情報保護

■社内ポータルサイトで共有された機密ファイルを保護

✓社内ポータルサイトからローカルPCにダウンロード禁止
ただし、IEキャッシュへのダウンロードは許可(直接参照)
✓IEキャッシュにダウンロードされた機密ファイルはIEキャッシュ外への持ち出しを禁止



✓社内ポータルから直接参照したファイルは
あらゆる持ち出し操作を禁止



課題③ 重要データの暗号化徹底(ユーザーの暗号化し忘れ防止)

■特定フォルダへの保存時に自動暗号化

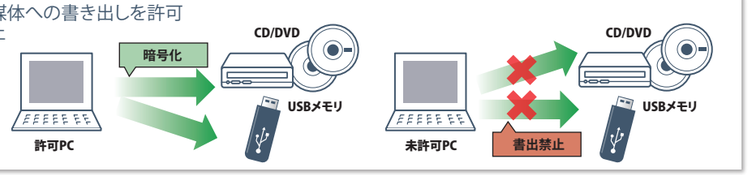
✓指定領域への保存時にファイルを暗号化する
それ以外のフォルダは平文で保存する

■社外メールの自動暗号化

✓社内ドメイン以外へのメール送信時に添付ファイルを
暗号化する
✓社内PCに対してのメール送信は平文のまま送信する

■外部メディアへの保存時に自動暗号化／書込制御

✓許可申請があったPCのみ外部媒体への書き出しを許可
未許可のPCでは書き出しを禁止



●お求め、ご相談は ・・・

パナソニック インフォメーションシステムズ株式会社

本社	〒530-0013	大阪市北区茶屋町19-19	TEL(06)6906-2801
東京支社	〒140-0002	東京都品川区東品川2-3-14	TEL(03)5715-5470
東日本ソリューション営業部	〒140-0002	東京都品川区東品川2-3-14	TEL(03)5715-5477
中部営業所	〒450-8611	名古屋市中村区名駅南2-7-55	TEL(052)561-3120
西日本ソリューション営業部	〒530-0013	大阪市北区茶屋町19-19	TEL(06)6377-0050
九州営業所	〒810-8530	福岡市中央区薬院3-1-24	TEL(092)523-9730

【商品の情報やお問い合わせは】 https://is-c.panasonic.co.jp/

■ YYA01183-C

Panasonic BUSINESS

エンドポイント型情報漏えい対策
情報セキュリティソリューション

DIGITAL GUARDIAN

**業務を止めず取扱いデータの重要度に沿った強力なアクセスコントロールと
確実なログ監視により、エンドポイントでの"情報漏えい対策"を実現します**

デジタル・ガーディアン商品サイト：
https://is-c.panasonic.co.jp/service/product/dg/

パナソニック インフォメーションシステムズ

エンドポイント情報漏えい対策のスペシャルソリューション

Digital Guardian

「仮想の防御ライン」を構築し、ポリシーに則った柔軟な制御を実現します

Digital Guardian(DG)は、組織における情報漏えい防止ソフトウェアです。

企業の重要情報へのアクセスを “正しく禁止” すれば、情報活用は活性化します。
Digital Guardianは情報の重要度に応じ適切な対応策を施すことができるため、情報の活用価値を損なわず、的確に情報漏洩を防ぐことができます。アプリケーションに依存せず、**見えないセキュリティの防御壁「仮想の防御ライン」**を構成し、その中で行われるあらゆる処理や外から侵入してくる脅威を常にモニターすることで、問題のある処理に対して警告あるいは強制的にブロックすることを可能にします。

Digital Guardian の特長

特長① 検知と防御の統合 *Integration of Detection and Prevention*

データ操作の**「モニタリング」**、**「傾向やリスクの可視化」**、**「制御と暗号化」**の三つの機能を統合

- ●既知の不正な相手あるいは攻撃パターンを判別し、乗っ取り行為をブロックします。内外双方の通信に対して、検知とブロック、必要に応じて通信の暗号化を行います。
- ●エンドポイントにインストールされたDGエージェントが収集する操作ログやイベントログは、フォレンジック※調査に役立てることができます。また55種類を超えるレポート機能を実装し、わかりやすいダッシュボードで現状を一覧で確認することができるので、新種のマルウェアの不審な動きや、急増する不正通信などの検知から潜在リスクを分析し、防御に役立てることができます。

※フォレンジックとは、コンピュータが関係する犯罪が起きた場合に、コンピュータやネットワークシステムのログや記録を収集・分析して証拠とするための技術。

特長② 内部脅威の予防 *Insider Threat Prevention*

他のマシンや外部のアドレスに対する疑わしいコネクションを検知

- ●権限のないユーザーが重要データを操作することをブロックすることができます。
- ●社外へのデータ送信など不用意に行うべきではない操作に対して、警告メッセージの表示や、操作理由の入力などの制御が行えます。
- ●ユーザーにデータの重要性を認識させ、慎重に操作するよう促す効果と、操作が監視されていることを認識させることによる不正なデータ持ち出しを抑止する効果が期待できます。

特長③ 外部脅威の検知 *Cyber Threat Prevention*

ネットワークに侵入してくる脅威を検知、分析

- ●疑わしいネットワーク上のトラフィックを警告し、ブロックします。
- ●標的型ツールが社内に侵入してしまった場合でも、重要データの外部への送信をブロック、あるいは操作理由の入力を求めることにより、バックドアからの情報漏えいを防止することができます。
- ●重要データを自動暗号化することにより、PC や USB メモリなどの紛失・盗難でデータが流出してしまった場合にも安心です。

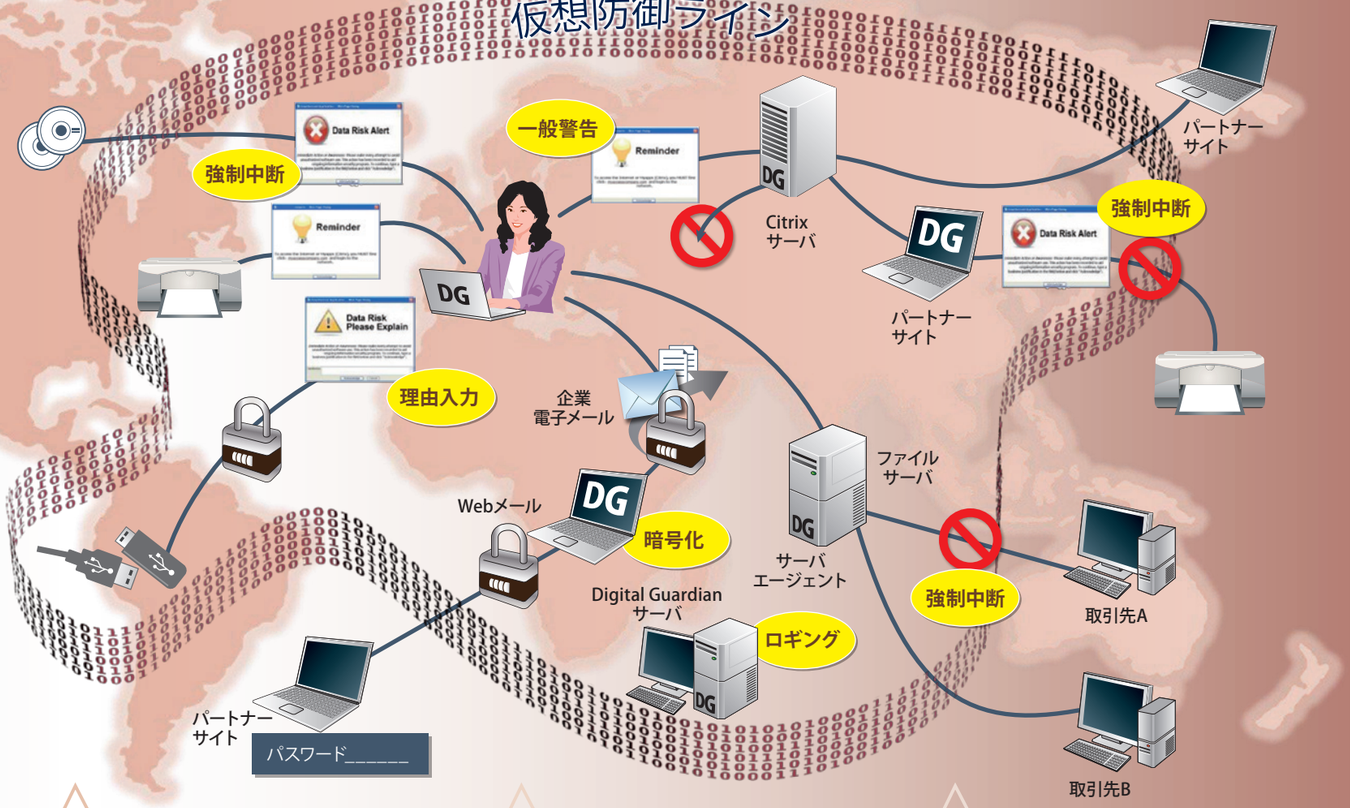
■ Digital Guardian はユーザーの行動ごとに次のアクションを実行します

【一般警告】操作に対する警告

重要度「中」のデータの操作に警告を与えます。ユーザーの操作に対してリアルタイムに対応し、重要データの流出を防ぎます。

【強制中断】操作を強制的にブロック

重要度「高」のデータの持ち出しを強制的にブロックします。ユーザーの操作にリアルタイムに対応し、重要なデータの流出を未然に阻止します。



【理由入力】操作の理由報告を要請

重要度「中」のデータの操作に警告を与えます。理由入力を行うことによりユーザーのリスクを伴う行動を抑止します。

【ロギング】操作ログの記録

仮想環境(VDI)での行動を含め、DGはユーザーのすべての行動を記録します。監査ログとしてご利用いただけます。

【暗号化】Email／Fileの暗号化※

重要度「高」のデータを暗号化することによりお客様の情報を守ります。

※Email/File の暗号化はオプション

タグ付けによるデータ分類

DGは機密ファイルをそれ以外のファイルと識別できるようタグを付与することができ、タグごとに重要度に応じた安全な情報活用が実現できます。