GFI Zero Sec Pac 案

20 Mar. 2021

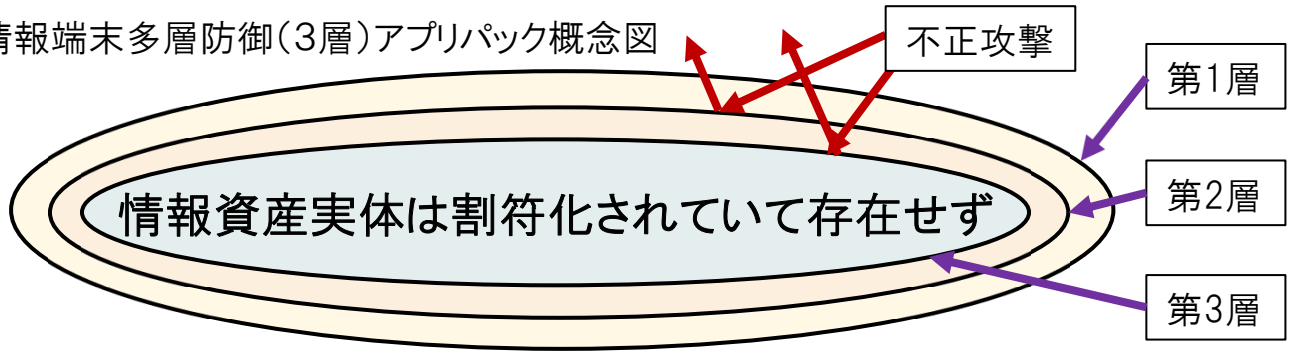
特許出願準備中

ゼロトラスト対応セキュリティアプリPac商品

情報端末セキュリティの一線を突破されても漏洩等が発生しない！

ーISMSやNIST SP800-171 CSF等への対処を検討する皆様へー

情報端末多層防御(3層)アプリパック概念図



◎第３層が突破され感染等しても情報自体は割符化されて存在せず安全

◎感染時は別端末で割符から情報復元し即実務復旧（BCP対処）が可能

第１層：

これまで最多の不正攻撃を受け、それに対処し続けてきたのはOSやPC、ネットワーク機器等を長期にわたり市場供給してきた会社です。攻撃者との長期間の攻防ノウハウは容易に真似できるものではありません。先ずは**OSの推奨するセキュリティ機能**と、市場で一定の評価を受ける**アンチウイルス等**のセキュリティ対策を実施します。

第２層：

第１層の基本的な対策を行ったとしても、更に巧妙化する攻撃やゼロデイのリスク等を完璧に防ぎきれるとは限りません。そこで、不正な動きをするプログラムの活動を検知し、その動きを制するセキュリティソフトウエアを導入します。それがOSプロテクト型エンドポイントセキュリティ、**AppGuard®**です。

第３層：

第１層や第2層の対策をしても、その防御線を突破されてしまうような残存リスクは存在します。攻撃者が最後の一線を突破しても、**そこには「何もない」か、「一部の割符ファイルしかない」**そうした安全確保の根拠背景が異なる最後の切り札が、GFI電子割符®を実装した情報資産管理アプリである**「割りふってますTM」**です。

◎基本Pacは第２層と第３層のアプリのセット　◎ PCセットも検討中

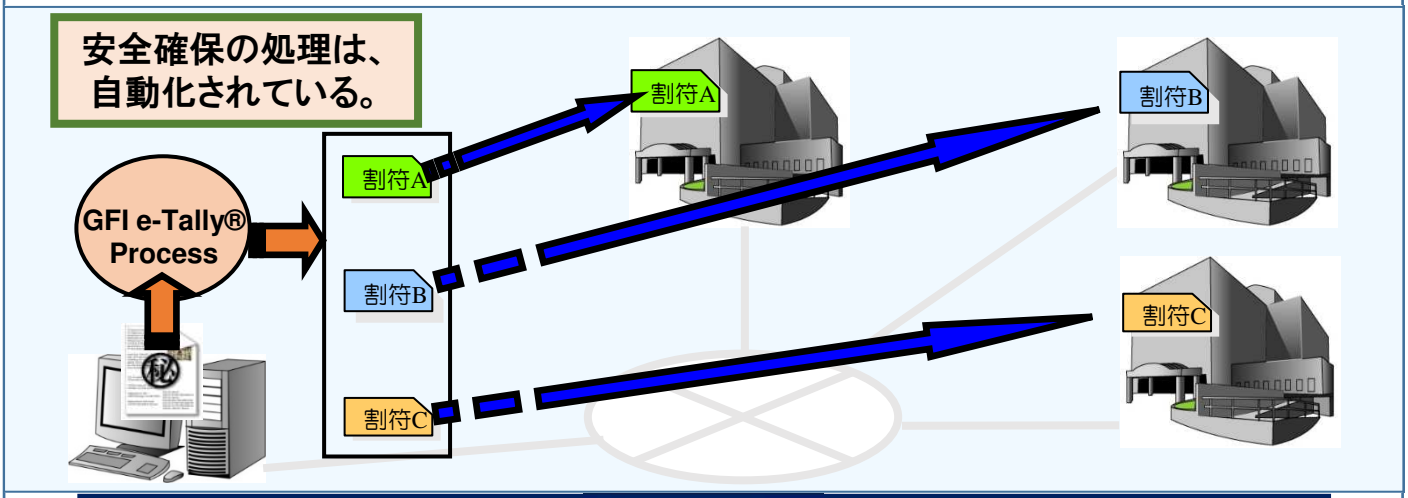
結局情報管理責任は人、PCリスク最小化が必須

EUのGDPRや改正個人情報保護法が定める漏洩時の対処義務等の例：①対象者全員への通知、②当局への報告、③違反時の制裁金や処分・罰則等

「政府機関等の対策基準策定のためのガイドライン」に準拠する２製品初のセット化

「３.１.１ 情報の取扱い」と、「6.2.2 不正プログラム対策」の２か所
出典：NISC（内閣サイバーセキュリティセンター）H30年7月25日公布

①20年を超える実績を有する代表的秘密分散技術GFI電子割符®実装アプリ
②米国政府機関でも採用されるOSプロテクト型エンドポイントセキュリティAppGuard®



①人は騙されますしミスもします。
②ネットワークやクラウドは「道」や「場」でしかありません。
③ハードは壊れますし欠陥がある可能性もあります。
④ソフトに完璧はありません。
攻撃者は弱点を狙います。本丸に侵入された際の安全が必要です。

商品企画･販売元：
グローバルフレンドシップ株式会社
東京都渋谷区笹塚1-32-2ソネット笹塚102
Email：info@gfi.co.jp

営業代理店：