

サイバー攻撃に対応する

ネットワーク セキュリティソリューション

特定の組織に的を絞った標的型攻撃など、サイバー攻撃の手口は益々巧妙化しており、もはやマルウェア(ウイルスなど)の侵入を防ぎきることは困難です。

ウイルスや悪意ある社員は既に侵入している。という前提に立ったセキュリティ対策が必要です

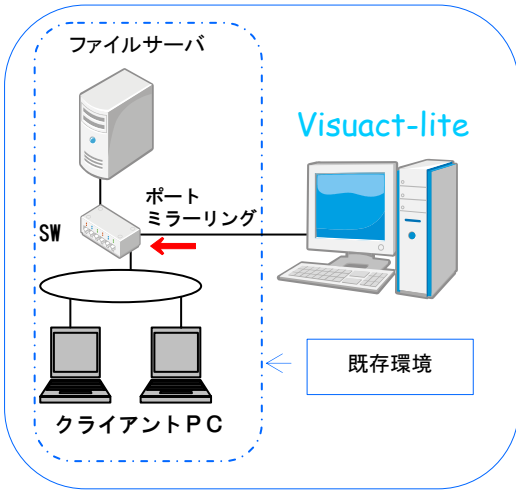
Visuact-lite

サイバー攻撃時代のファイルアクセス監視

サーバ監視+サーバサイドにログが残らない、部門間ファイルアクセスの多点監視に対応

ネットワークパケットからファイルアクセスのログを取得するパケットキャプチャ方式

探したいログがすぐ見つかる

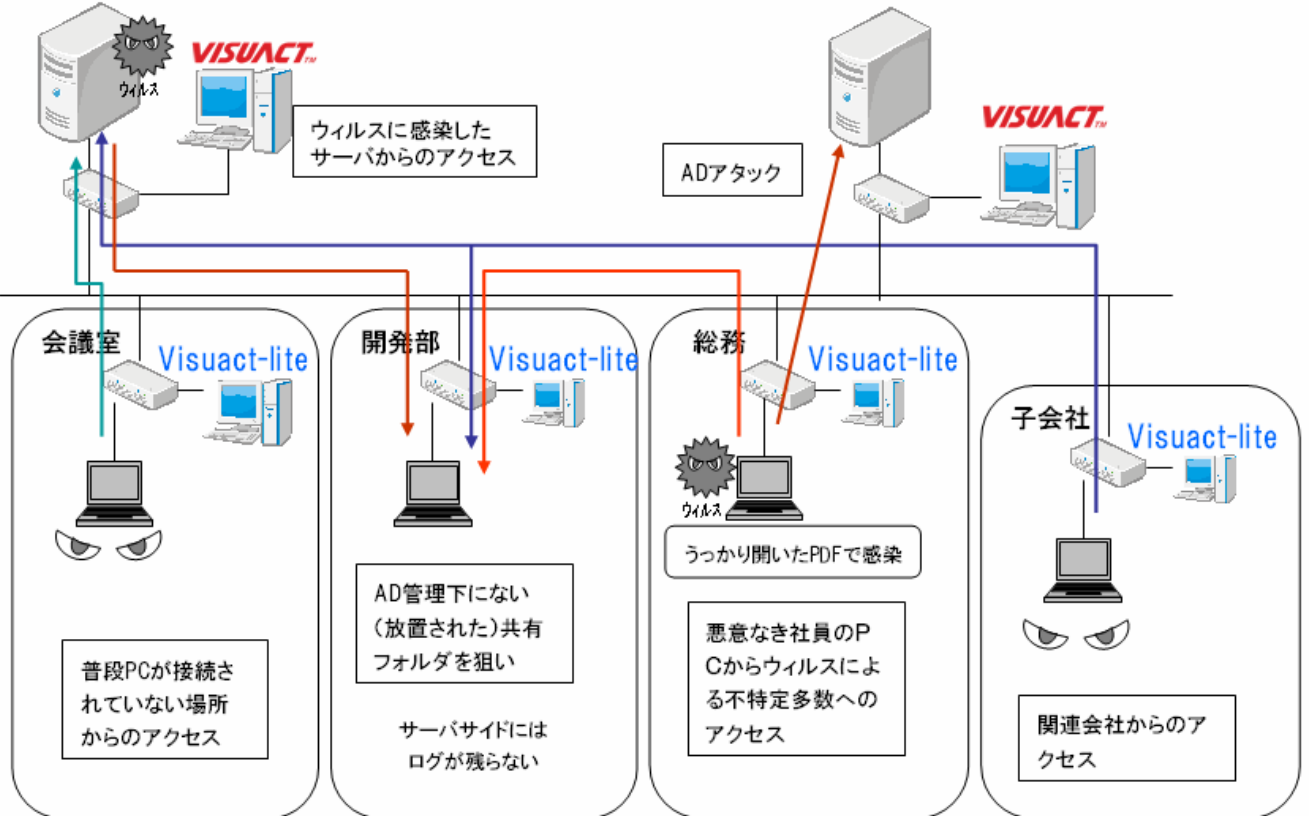


年月日	時刻	クライアント	サーバ	操作内容	共有名	操作対象	付加テータ
2011/08/30	11:57:53.843	192.168.1.107	192.168.1.202	Create File	\\FILE-SERVER1\WS\フォルダ2\1104.doc	201104.doc	0
2011/08/30	11:57:53.843	192.168.1.107	192.168.1.202	Write	\\FILE-SERVER1\WS\フォルダ2\1104.doc	201104.doc	0
2011/08/30	11:57:53.843	192.168.1.107	192.168.1.202	Read	\\FILE-SERVER1\WS\フォルダ2\1104.doc	201104.doc	28572
2011/08/30	11:57:54.718	192.168.1.107	192.168.1.202	Delete File	\\FILE-SERVER1\WS\フォルダ2\1104.doc	201104.doc	0
2011/08/30	11:57:55.656	192.168.1.107	192.168.1.202	Read	\\FILE-SERVER1\WS\フォルダ2\年度計画2011.ppt	201104.doc	53488
2011/08/30	11:57:56.407	192.168.1.107	192.168.1.202	Read	\\FILE-SERVER1\WS\フォルダ2\2010年度業績.pdf	201104.doc	1727474
2011/08/30	11:58:00.390	192.168.1.107	192.168.1.202	Write	\\FILE-SERVER1\WS\フォルダ2\2011年人事	201104.doc	0
2011/08/30	11:58:00.453	192.168.1.107	192.168.1.202	Write	\\FILE-SERVER1\WS\フォルダ2\2010年度業績.pdf	201104.doc	0
2011/08/30	11:58:00.453	192.168.1.107	192.168.1.202	Write	\\FILE-SERVER1\WS\フォルダ2\2011年度業績.pdf	201104.doc	0
2011/08/30	11:58:00.609	192.168.1.107	192.168.1.202	Read	\\FILE-SERVER1\WS\フォルダ2\2011年度業績.pdf	201104.doc	1727474
2011/08/30	11:58:00.609	192.168.1.107	192.168.1.202	Access Denied (NG)	\\FILE-SERVER1\WS\フォルダ2\1104.doc	201104.doc	0
2011/08/30	11:58:00.609	192.168.1.107	192.168.1.202	Read	\\FILE-SERVER1\WS\フォルダ2\2011年度業績.pdf	201104.doc	10488039
2011/08/30	11:58:00.656	192.168.1.107	192.168.1.202	Access Denied (NG)	\\FILE-SERVER1\WS\フォルダ2\1104.doc	201104.doc	0
2011/08/30	11:58:00.656	192.168.1.107	192.168.1.202	Access Denied (NG)	\\FILE-SERVER1\WS\フォルダ2\1104.doc	201104.doc	0
2011/08/30	11:58:00.656	192.168.1.107	192.168.1.202	Access Denied (NG)	\\FILE-SERVER1\WS\フォルダ2\1104.doc	201104.doc	0
2011/08/30	11:58:05.156	192.168.1.107	192.168.1.202	Access Denied (NG)	\\FILE-SERVER1\WS\フォルダ2\2010年度業績.pdf	201104.doc	0
2011/08/30	11:58:05.250	192.168.1.107	192.168.1.202	Create Directory	\\FILE-SERVER1\WS\フォルダ3	201104.doc	0

正常なファイルアクセスはもちろん、ウィルス等による不信なアクセスも全て記録

グループ統合
ファイルサーバ

Active Directory



PromiScan IV

PromiScanは、サイバー攻撃、ウィルス、悪意ある社員によるネットワーク盗聴を、外部から検出する画期的なソフトウェアです。盗聴可能な状態(プロミスキャスモード)になっているPCをネットワーク側から検出することが可能です。

侵入してしまったスパイウィルスのスパイ活動を検出

➤ マルウェア(スパイウィルス等)の侵入は防ぎきれない

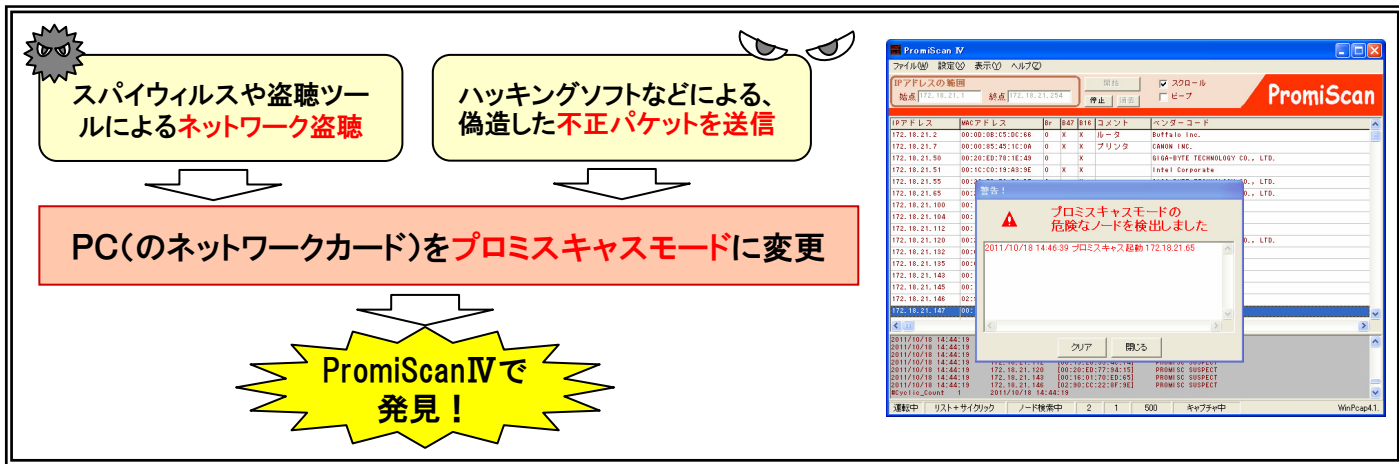
- ・特定の企業を狙った標的型のサイバー攻撃など、手口は多数かつ巧妙
- ・何らかの経路で侵入したウィルスが、スパイ活動していることを前提に、これを監視する必要性

➤ 悪意有る社員によるネットワーク盗聴

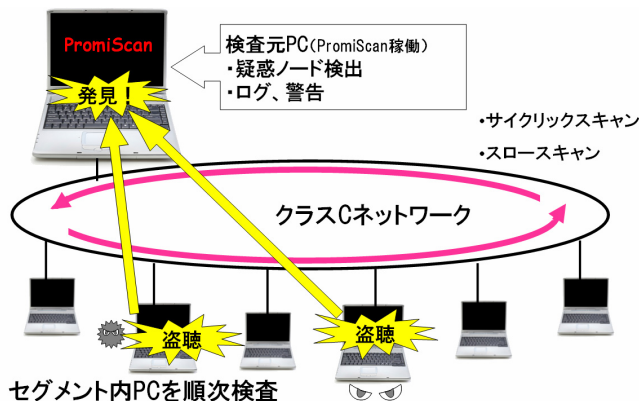
- ・ネットワーク盗聴は、ネットワーク上にその痕跡が残らず、発見が困難
- ・盗聴ソフトウェアによって、プロミスキャスモードに変更されたPCを検出

PromiScan IVの特長

- 盗聴ソフトウェアやスパイウィルスにより、盗聴モードになったPCを発見
- 不正なパケットを送信するハッキングプログラムの挙動を検出



ローカルネット上のPCをPromiScanが監視



PromiScanMC or 汎用SYSLOGモニタで集中監視

