活用レポート 31

社内端末上の不審ファイルの検索について

IPAが公的機関からの個人情報漏えい問題に注意喚起を発表！

最近のウイルス感染被害は、外部の機関からの通報等によって初めて感染に気づかされるケースがほとんどの為、自組織内のウイルス感染への懸念が高まっています。IPAでは組織内への感染の突破口となり得る部署の端末など、優先順位の高い端末から、可能な限り検査を進めることを推奨しています。今回は、Catで社内端末に不審なファイルが存在するかを確認する手順をご紹介いたします。

不審なファイルを発見！

LanScope Catでは保守ユーザー様専用サイトよりダウンロードいただけるスクリプトを実行することで、**社内端末に不審なファイルが存在するかを確認することが可能**です。検索結果については、**管理コンソール上で一括確認が可能**です。今回はその詳細な手順をご紹介いたします。

まずは･･･ スクリプトをダウンロードしましょう！(LanScope Cat保守ユーザー様専用サイト)
https://tryweb2.motex.co.jp/cat/ver8/info/info/201507/0717.php

IPAが提示している不審なファイル一覧

leanp.exe／vmatam.exe／GetPassword.exe／mail_noArgv_final.exe／leassap.exe／vmatap.exe／mimikatz.exe／result.log／eassaq.exe／vmater.exe／mimikatzx64.exe／14068.rar／leassnp.exe／vmmat.exe／mimikatz1.exe／ms14-068.exe／mdm.exe vmnatam.exe／gp.exe／kptl.doc／nvsvcv.exe／vmwere.exe／Gp64.exe／kenpo.doc／nvvscv.exe／windump.exe／ps.txt／slwga.exe／ct.exe／msver.exe／upsl.dll／yrar.exe／slwga.exe／ss.exe／vmat.exe／csvde.exe／mailfinal.exe

【 設定ステップ 】

1 配布グループを設置し配信設定を行う　2 スクリプトファイルの配布設定を行う　3 レジストリキー取得情報の設定を行う

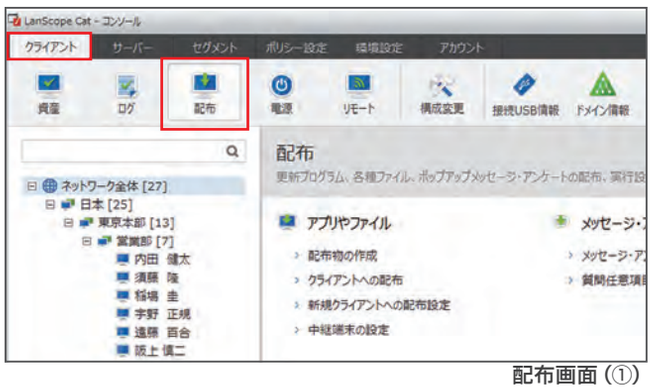
1 配布グループを設定し、配信設定を行う

ここでは、「不審なファイル検索スクリプトファイル」をどのPCに配るかのグループを設定します。

①**【クライアント】**-**【配布】**の**【旧配布設定】**の**【ファイル配布グループの設定】**を選択します。

②ファイル配布グループの設定画面で、右下の**【追加】**を選択し、ファイル配布グループの設定画面で、**【配布グループ名】**を入力、対象の端末を選択、**【設定】**を選択します。

ファイル配布グループの設定画面で、先程の配布グループができていれば成功です。



配布画面（①）

2 スクリプトファイルの配布設定を行う

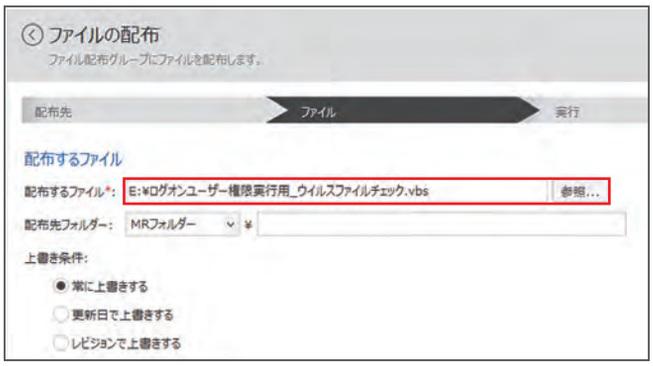
いつ・どのPCに配布・実行をさせるか等の設定を行います。本ページでは、「ログオンユーザー権限実行用_ウイルスファイルチェック.vbs」を配布する設定をご紹介します。

①**【クライアント】**-**【配布】**の**【旧配布設定】**の**【ファイルの配布】**を選択します。

②ファイルの配布設定一覧画面右下の【追加】選択します。

③配布するグループ画面では 1 で作ったグループを選択。
次に、配布するファイル画面では、ダウンロードしたスクリプトを選択します。
ファイルの実行画面では、実行権限をログオンユーザーに選択し、実行のタイミングを決め、【設定】を選択します。

ログインユーザー権限・Localsystem権限の2種のスクリプトをご用意。環境に合わせてお使いください。



配布するファイル画面（③）

3 レジストリキー取得情報の設定を行う

レジストリに書き込まれた不審ファイルの有無の結果を取得するための設定を行います。2 の設定、32bitOSか64bitOSかによってもレジストリキーが異なります。本ページでは（32bitでログオンユーザ環境での結果取得設定）でご紹介します。

①【クライアント】-【資産】-【レジストリキー取得情報】を選択し、左下の『取得設定..』を選択し【追加】します。

②【表示名】に名前を入力、【取得対象】として【全OSで共通の設定を行う】を選択し、次の情報を入力し、【OK】ボタンを選択します。

キー：HKEY_LOCAL_MACHINE\SOFTWARE\MOTEX\LanScope Cat MR\CurrentVersion\Profile
名前： FileCheckList1

レジストリキーの取得設定の追加画面（②）

数字がでていたら要注意！すぐに詳細を確認し、対策を行ってください。

【クライアント】-【資産】-【レジストリキー取得情報】を選択し、【レジストリキー取得情報】画面から確認できます。
「該当ファイルは見つかりませんでした」と表示されていれば、安全の証拠です！

管...	登録No	グループ名	クライアント名	不審ファイル確認
1	2	日本¥東京本部¥営業部	内田 健太	2
1	5	日本¥東京本部¥営業部	須藤 隆	該当のファイルは見つかりま
1	7	日本¥東京本部¥サポート部	秋田 千尋	該当のファイルは見つかりま
1	8	日本¥東京本部¥サポート部	弘瀬 孝明	該当のファイルは見つかりま
1	13	日本¥大阪本社¥サポート部	堂島 奈緒	該当のファイルは見つかりま
1	15	日本¥東京本部¥システム部	高橋 稔	（なし）

数字：ウイルスが侵入している可能性があります！
空白：端末から資産情報が送信されていない状態
なし：スクリプトがまだ実行されていない

詳細の手順はこちらを確認してください

◆設定手順マニュアル（保守サイト）：https://tryweb2.motex.co.jp/cat/ver8/info/info/201507/0717.php
◆概　要（Catサイト）：http://www.lanscope.jp/cat/about/viruscheck/

活用レポート 32

年末年始休暇に合わせた対策について

長期休暇前後のセキュリティ対策を徹底しましょう！！

長期休暇の際は、システム管理者が不在になりがちなため、トラブル発生時の対処が遅れたり、適切なセキュリティ対策を行っていないとウイルス感染の被害が及ぶ可能性があります。社員が自宅で仕事を行ったり、監視体制が手薄になり、不正アクセスや不正操作が発生するなどのトラブルを未然に防ぐために対策を事前に行いましょう。

休暇前後で抑えるチェックポイント

休暇前にチェックすべきポイント

1. PCにインストールされているソフトウェアを把握しておきましょう。
2. サーバーやPCのソフトウェアやOSに修正プログラムを適用し、最新のバージョンに更新しましょう。
3. 組織の情報へのアクセス権が適切に割り当てられているか確認しましょう。

休暇後にチェックすべきポイント

1. 長期休暇中にOSや各種ソフトウェアの修正プログラムがあるか確認し、必要な修正プログラムを適用しましょう。
2. 長期休暇中に電源を切っていたパソコンに、セキュリティソフトの定義ファイルを更新し、最新の状態にしましょう。
3. サーバ等の機器に対する不審なアクセスが発生していないか、各種ログを確認しましょう。

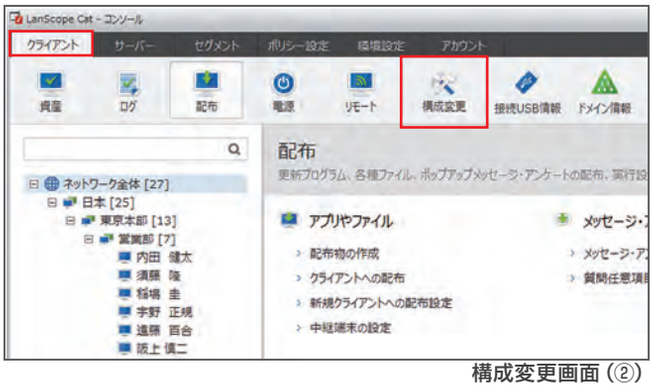
事前 休暇中に持ち帰った PC の操作を確認するための設定

仕事を持ち帰り、自宅で業務を行う場合も考えられます。ネットワークに繋がっていない場合の操作履歴を取得する方法をご紹介します。

①**【クライアント】**-**【クライアント】**の**【構成変更】**を選択し**【クライアントタイプの一括変更】**を選択します。

②クライアントタイプの一括変更画面で、**【MR端末のタイプを変更する】**を選択し、**【MRタイプ】**を変更します。

あらゆるシーンを想定し「LANオフラインMR」に設置しておくことをおススメします。



構成変更画面（②）

MRタイプ	主に対象となる端末・特徴	
LANオフライン	社内から持ち出されるPC	サブマネージャーとの通信に関わらずログを取得。通信が不能な場合はログを端末に一時的に保存。サブマネージャーとの通信が確立されたときにログをサブマネージャーへ送信。
RASオフライン	社内LANにPHS等で接続するPC	サブマネージャーとの通信に関わらずログを取得。通信が不能な場合はログを端末に一時的に保存。ダイヤルアップ接続時にログをサブマネージャーに送信。
オフライン	LANにもRASにも接続するPC	サブマネージャーとの通信に関わらずログを取得。通信が不能な場合はログを端末に一時的に保存。サブマネージャーとの通信が確立されたときにログをサブマネージャーへ送信。
常駐	常にネットワークに接続されている	端末サブマネージャーとの通信が可能な場合にだけログを取得。通信が不能な場合はログは保存されない。
スタンドアロン	ネットワークに接続されない端末	資産情報や操作ログを端末内にテキストファイルで保存。保存されたログは統合コンソールから手動でインポート。操作の制御はできないことに注意。
SBCタイプ	シンクライアントサーバー用	XenApp やリモートデスクトップサービスのようなSBC 方式の仮想環境のサーバー用。サブマネージャーとの通信に関わらずログを取得。通信が不能な場合はログを端末に一時的に保存。

各 PC にインストールされているソフトウェアを把握しましょう

Webコンソールから社員のアプリケーションインストール状況を確認しましょう。業務に必要なアプリケーションがインストールされているか、また不必要なものをインストールしている社員に対しては、注意してアンインストールを促しましょう。

①Webコンソールブラウザの **[インストールアプリケーション]** をクリックします。

②**[インストールアプリケーション画面]**　の左側のツリーから、取り出したい部署を選択し、画面右側の**[アプリケーションインストールTOP20]** の **[グラフ表示]ボタン**をクリックします。

Webコンソール画面 (①)

③インストールアプリケーションのランキンググラフと、一覧が表示されます。表内のアプリケーションをクリックするとインストールされている端末が確認できます。

セキュリティパッチなど必要なアプリケーションがインストールされていなければ社員にインストールを促すか、ファイル配布機能を活用し、インストールを行いましょう。

Webコンソール (③)

最新のセキュリティパッチが当たってなければ、休暇前までに必ず当てましょう

各サイトより最新パッチ情報が公開されていますので、データを収集後、ファイル配布機能を活用し、最新の状態にしておきましょう。また、市場動向などセキュリティに関連したトレンド情報も発信されているので、確認しておきましょう。(以下は参考例です)

サイト	概要	URL
IPA 情報処理推進機構	IPAが発信している、市場のセキュリティ状況や危機回避のための対策方法などを発信する情報ポータル	http://www.ipa.go.jp/security/
Microsoft社 セキュリティ TechCenter	Microsoft社製品のセキュリティ情報やセキュリティパッチの提供などを行っているページ	https://technet.microsoft.com/ja-jp/security/bb291012
TrendMicro社 セキュリティ情報	セキュリティに関連する最新情報と対応パッチ・方法などを発信しているポータルサイト	http://www.trendmicro.co.jp/jp/security-intelligence/index.html
内閣府 サイバーセキュリティセンター	内閣府がサイバーテロに備えて発足させた「標的型攻撃」などに関する情報を発信しているサイト	http://www.nisc.go.jp/index.html