SOMPO SHERIFF 主要アラート
対応方法早見表 Ver1.2

SOMPO CYBER SECURITY

SOMPOリスクマネジメント株式会社

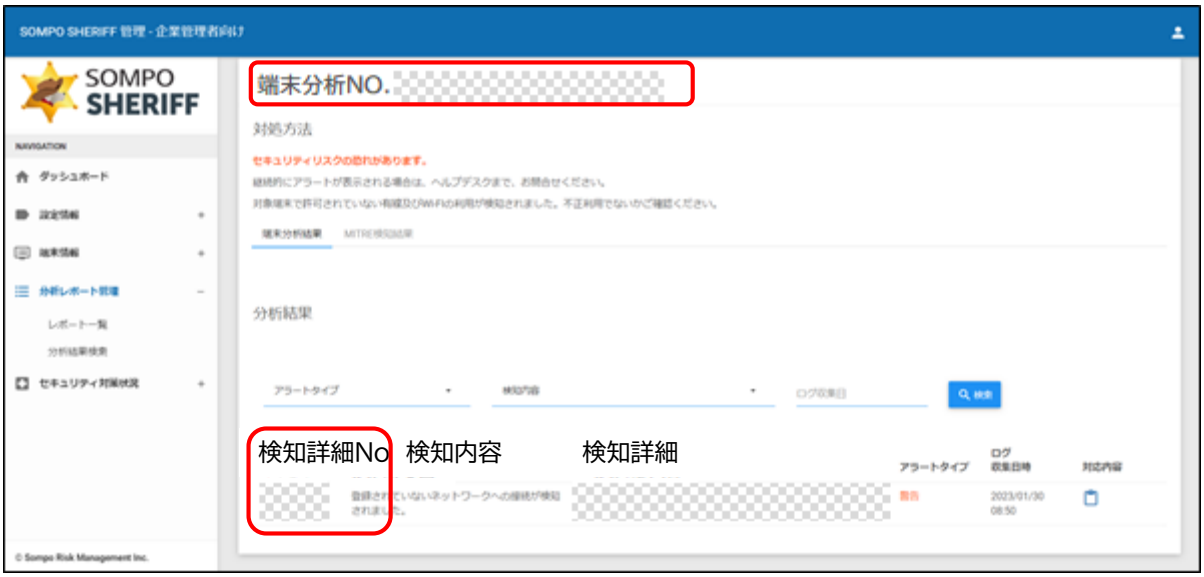
＜目 次＞

SOMPO SHERIFF 主要アラート早見表

検知内容	検知理由	アラート	対処方法
攻撃者が悪用する可能性があるツールの動作を検知しました。	リモートホスト上でのコマンド（PsExec）の実行の痕跡	警告	心当たりが無い場合、最新状態のウイルス対策ソフトでスキャンをお薦めします。継続してアラートがでる場合はSOMPO SHERIFFサポート窓口へ連絡ください。
	イベントログ削除の検知	警告	クリーンアップツール含めて心当たりが無い場合は、最新状態のウイルス対策ソフトでスキャンをお薦めします。継続してアラートがでる場合はSOMPO SHERIFFサポート窓口へ連絡ください。
USBの利用が検知されました。	USB接続の痕跡	警告	USBが不正利用でないかを確認してください。
登録されていないネットワークの接続が検知されました。	登録されていないネットワークの接続の痕跡	警告	業務で継続利用される安全なネットワークは登録をお薦めします。登録されたネットワークは検知対象外となります。
マルウェアの接続と思われる接続を検知しました。	ブラックリストのC&Cサーバーへの IPアドレス接続の痕跡	警告	接続先に心当たりが無い場合は、最新状態のウイルス対策ソフトでスキャンをお薦めします。詳しく確認をされたい場合は、下記の情報をSOMPO SHERIFFサポート窓口へ連絡ください。 **・端末分析NO ・検知詳細No**
不正と思われるレジストリ情報の書き換えを検知しました。	アクセス補助機能の悪用の挙動痕跡 【T1546.008】	注意	最新状態のウイルス対策ソフトでスキャンをお薦めします。詳しく確認をされたい場合は、項目名のデータに記載にあるファイルが存在するかの確認いただき、「**ハッシュ値**」を取得して、SOMPO SHERIFFサポート窓口へ、**端末分析NO、検知詳細No**を添えてご連絡ください。
不正と思われるレジストリ情報を検知しました。	インジェクション（IFEO）/端末の機能を不正利用したコマンドの実行 【T1546.012】	注意	最新状態のウイルス対策ソフトでスキャンをお薦めします。詳しく確認をされたい場合は、下記の情報をSOMPO SHERIFFサポート窓口へ連絡ください。 **・端末分析NO ・検知詳細No**
	端末のUAC（ユーザーアクセス制御）の無効化や回避実行 【T1548.002】	注意	検知内容がUACの無効化の場合はセキュリティ観点から有効化にすることをお薦めします。UACの回避の可能性のあるレジストリ情報の変更を検知した場合は最新状態のウイルス対策ソフトでスキャンをお薦めします。詳しく確認をされたい場合は、レジストリキーから対象のファイルパスを確認して「**ハッシュ値**」を取得して、SOMPO SHERIFFサポート窓口へ、**端末分析NO、検知詳細No**を添えてご連絡ください。
	ツールの無効化、セキュリティリスクの上昇挙動の検知 【T1562.001】	注意	Microsoft製品でのアラートの場合、基本保護ビューの設定し、マクロはセキュリティチェックの設定をすることをお薦めします。Microsoft Defenderでのアラートの場合は意図的に無効にしてなければサイバー攻撃の可能性もありますが、他のウイルス対策ソフトの設定による無効化の可能性もございます。
攻撃と疑われるレジストリの情報の更新を検知しました。	スタートアップフォルダやrunレジストリキーの悪用 【T1547.001】	注意	表示されている値名のアプリケーションをインストールや利用されている場合は問題ございません。心当たりが無い場合は、最新状態のウイルス対策ソフトでスキャンをお薦めします。詳しく確認をされたい場合は、「**ハッシュ値**」を取得して、SOMPO SHERIFFサポート窓口へ**端末分析NO、検知詳細No**を添えてご連絡ください。
不正と思われるコマンド実行を検知しました。	WindowsのVBスクリプトの実施の痕跡 【T1059.005】	注意	VBスクリプトの実行に心当たりがある場合は問題ありません。心当たりが無い場合は、最新状態のウイルス対策ソフトでスキャンをお薦めします。詳しく確認をされたい場合は、下記の情報をSOMPO SHERIFFサポート窓口へ連絡ください。 **・端末分析NO ・検知詳細No**
	Windowsのコマンドプロンプト、PowerShellの実行の痕跡 【T1018.001】	注意	Windowsのコマンドプロンプトの実行等に心当たりがある場合は問題ありません。心当たりが無い場合は、最新状態のウイルス対策ソフトでスキャンをお薦めします。詳しく確認をされたい場合は、下記の情報をSOMPO SHERIFFサポート窓口へ連絡ください。 **・端末分析NO. ・検知詳細No**

SOMPO SHERIFF「端末分析NO.」「検知詳細No 」の確認方法

SOMPO SHERIFF管理画面 ⇒ 分析レポート管理 ⇒ レポートNO. ⇒対処方法で
端末分析NO、検知詳細Noが確認できます。



SOMPO SHERIFF サポート窓口への確認方法

アラートに関して詳しく確認をされたい場合は、
「端末分析NO.」「検知詳細No.」「ハッシュ値」の情報を、SOMPO SHERIFF
お問い合わせフォームの＜検知アラート照会・検知対応依頼＞よりお問い合わせください。

※ アラート毎、お送りいただく情報は異なりますのでP3の主要アラート表でご確認ください。
※「ハッシュ値」の確認方法はP5に記述してますので参照してください。

SOMPO SHERIFFお問い合わせフォーム：
https://srm.sompocybersecurity.com/lp/sheriff/contact/index.php

対応時間：9:00～17:00（土日祝を除く）

ハッシュ値の確認方法

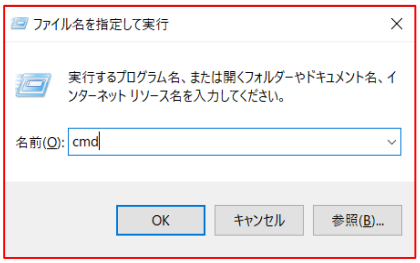
※ ハッシュ値はコマンドプロント画面で確認することができます。

コマンドプロンプトの起動方法

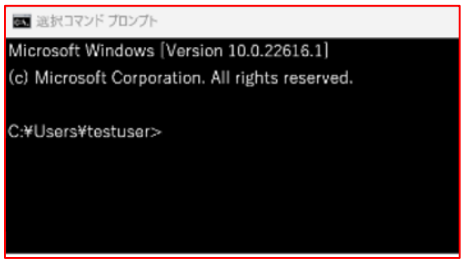
① キーボードの[Windows]キーを押しながら、[R]キーを押します。
② 「名前」欄に「cmd」と入力し、[OK]ボタンをクリックします。
③ コマンドプロントの画面が起動します。

①

②



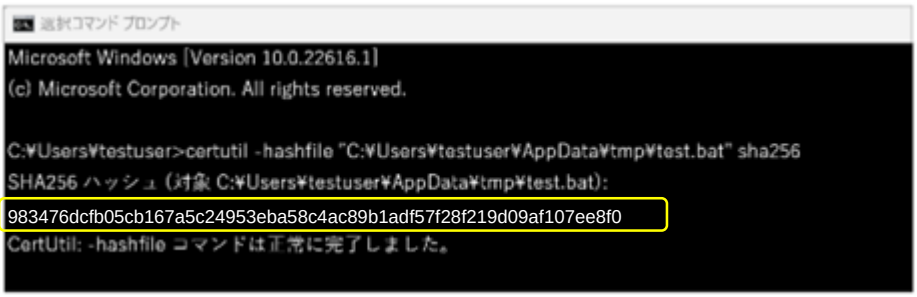
③



※ コマンドプロント画面

④ ハッシュ値を確認にはコマンドプロンプト画面に下記のコマンドを入力します。

certutil -hashfile “対象ファイルのパス”sha256



ハッシュ値(例)

⑤ 矢印枠内に表示されている箇所がファイルのハッシュ値となります。
（対象ファイルのパスは管理画面の検知詳細に記載されております。）

※ 検知詳細のファイルのパス記述は検知内容によって異なります。
（直接パスの記載や、データ、プロセスパスの項目等で表示。）

準備期間中に良くあるアラートの解説

「USBの利用が検知されました。」

検知詳細No	検知内容	検知詳細	アラートタイプ	ログ収集日時	対応内容
[redacted]	USBの利用が検知されました。	マウントされたデバイスが確認されました。[redacted]	警告	2022/12/23 09:55	

SOMPO SHERIFFの「USB利用検知」の初期設定はUSBを利用した場合には、必ず警告アラート履歴として、分析レポートや管理画面に表示されます。

※マルウェアの感染、個人情報や機密情報の流出の多くはUSBからの持ち出しとなることが多く見受けられるので、SOMPO SHERIFFにおいてはUSBを利用された場合は毎回、警告アラートとして検知します。

※お客さまが「USB利用検知」設定をOFFにしたい場合は、SOMPO SHERIFF管理画面の設定情報＞企業情報＞監視設定のUSB利用制限のチェックを外していただければ、「USB利用検知」をOFFとなります。

「登録されていないネットワークへの接続が検知されました。」

検知詳細No	検知内容	検知詳細	アラートタイプ	ログ収集日時	対応内容
[redacted]	登録されていないネットワークへの接続が検知されました。	2022/12/22 [redacted]登録されていないMACアドレスの接続を確認しました。	警告	2022/12/23 00:00	

SOMPO SHERIFFの「ネットワークの接続検知」の初期設定は登録されていないネットワークに接続した場合は、必ず警告アラート履歴として、分析レポートや管理画面に表示されます。

SOMPO SHERIFFはインストール後の準備期間中に検知したネットワーク接続については、お客さまが問題の無いネットワークであることを確認いただいてMACアドレスの追加登録をお願いします。

※ SHERIFF管理画面の設定情報＞企業情報＞監視設定のネット接続制限にて問題の無いネットワークとして、MACアドレスの追加をしていただければ以後は検知しないように除外設定となります。

「不正と思われるコマンド実行を検知しました。」

この注意アラートは、お客さま自身がコマンド実行した覚えが無い場合においても、業務でご利用のアプリケーション(例:ウイルス対策ソフト・マクロファイル)等にて端末管理用のコマンドやVB(Visual Basic)スプリクトが実行されているケースにおいても「不正と思われるコマンド実行検知」の注意アラートとなりますので問題はございません。

詳しくご確認されたい場合は、下記の情報をSOMPO SHERIFFサポート窓口まで、お送りください。

- 端末分析NO.
- 検知詳細No.
- ご利用中のウイルス対策ソフト名

※ 端末分析NO、検知詳細Noの確認方法はP.4を参照ください。

※ この検知の除外については、各会社様ごとの固有の設定として除外する登録を行いますので、SOMPO SHERIFFサポート窓口まで、ご連絡をください。

攻撃者が悪用する可能性があるツールの動作を検知しました。

リモートホスト上でのコマンド(PsExec)の実行やイベントログの削除した痕跡がある場合に警告アラートとして、分析レポートや管理画面に表示されます。
PsExecの実行や、イベントログの削除に心当たりがありましたら問題ございません。

何も心当りが無い場合は、最新状態にしたウイルス対策ソフトでのスキャンをお薦めします。また継続してアラートがでる場合は、SOMPO SHERIFFサポート窓口まで、ご連絡ください。

※ PsExecはWindows OSにおけるリモートプログラム実行ツールです。正規のツールであるため、セキュリティツールによる検知を回避しやすいことから、環境寄生型(LotL)攻撃などにしばしば悪用されていますので、SOMPO SHERIFFでは警告アラートとして検知します。

※ イベントログの削除はサイバー攻撃を隠ぺいするために実行されるケースがございますのでSOMPO SHERIFFでは警告アラートとして検知します。

SOMPO SHERIFFお問い合わせフォーム:

ご不明点・ご質問は、下記お問い合わせフォームよりお問い合わせください。

https://srm.sompocybersecurity.com/lp/sheriff/contact/index.php

対応時間:9:00~17:00(土日祝を除く)
SOMPOリスクマネジメント株式会社