【別紙】ランサムウェア対策機能概要

事前設定

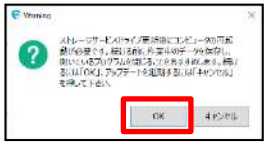
ランサムウェア対策機能を使用するには、「インシデント管理ポリシー」の有効化と共に、ストレージサービスDriveをバージョン1.0.19657以降にアップデートする必要があります。

利用者

本機能提供時にあわせてストレージサービスDriveをリリースします。
以下の手順で最新のバージョンにアップデートしてください。

①Driveにログインするとアップデート通知画面が表示されます。
「今すぐ更新」をクリックします。

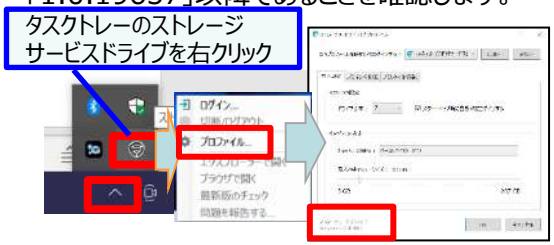
②アップデート確認ダイアログが表示されます。「OK」をクリックします。



③Driveのアップデートが実行されます。終了までお待ちください。

④Driveのアップデート完了後、再起動確認ダイアログが表示されます。
「今すぐ再起動」をクリックします。

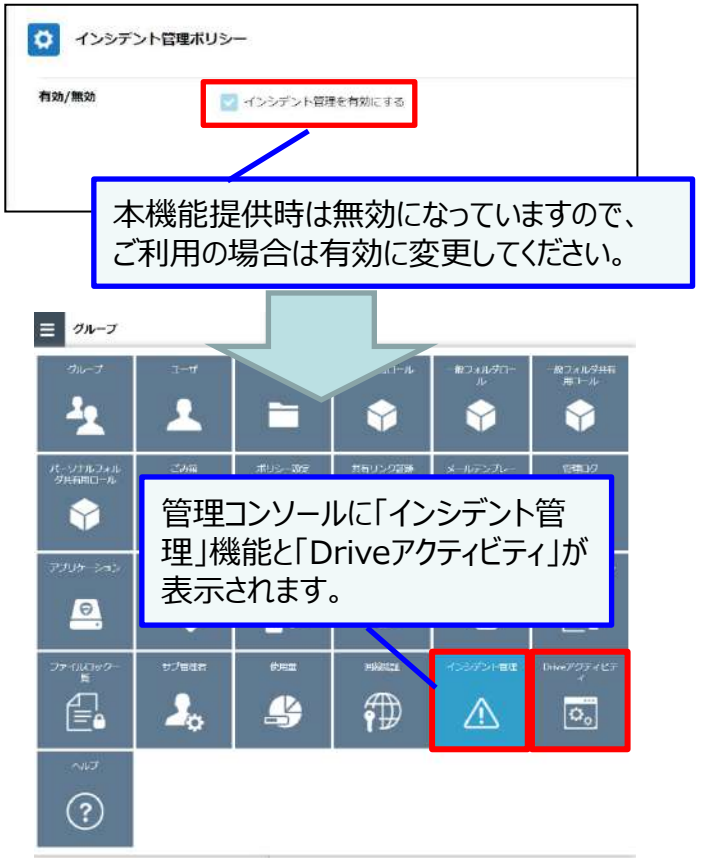
⑤Driveのアップデートを確認します。
プロファイル画面の左下のバージョンが「1.0.19657」以降であることを確認します。



注意事項
ストレージサービスDriveのバージョン1.0.19657から、以下ソフトウェアの必要動作環境が変更となります。
.NET Framework：4.7.2 以上

管理者

管理コンソール「ポリシー設定」から「インシデント管理ポリシー」の有効化



【別紙】ランサムウェア対策機能概要

ランサムウェアを検知した場合

ストレージサービスDrive上でランサムウェアを検知した場合、管理者は、管理コンソール「インシデント管理」機能で被害ファイルの特定と復旧まで実施します。

利用者

ランサムウェア検知時、ストレージサービスDriveから以下のようなダイアログが表示されます。
管理者の方に連絡してください。

また、本サービスから、利用者本人と管理者全員宛にメール通知されます。

```
不審なアクティビティが検出されました。
ランサムウェアの疑いがあるため、こちらのインシデントを確認してください。


インシデントID: 240768c1-47c8-4fff-b206-5a24ad32571a
不審なプログラム情報：
    ファイル名：explorer.exe
    ファイルパス：C:¥Windows¥explorer.exe
    ファイル説明：エクスプローラー
検出元情報：
    端末名：XXXXXX
    端末OS：Windows 10.0.19045
    OSログオンユーザ名：user
    Driveバージョン：1.0.19657.18018596
    メールアドレス：email|XXXXXXXXXXXXXXXXX

---------------------
Sent by ○○
```

この時点で、当該ローカルPCの同じプロセスによるストレージサービスDriveの同期が停止します。

管理者

管理コンソール「インシデント管理」機能で以下の対応を実施します。

①インシデントの確認

②影響範囲の調査

CSV形式のファイルで影響を受けたファイル一覧をダウンロードし、影響が出たファイルを確認します。

③このインシデントを
”悪意のあるプロセス”か”
信頼されたプロセス”かを判定

※信頼されたプロセスと判定されれば
そのタイミングで当該プロセスの同期が
再開されます。

④”悪意のあるプロセス“と判定した場合
ファイルを復旧

⑤結果をダウンロードし、
復旧したファイルの確認

⑥インシデントのクローズ
※管理者から利用者に復旧完了を連絡してください。