Central Intercept X with XDR 運用ガイド

セールスエンジニアリング本部

SOPHOS

本資料について

- 本資料はCentral Intercept X Advanced with XDRにおける運用方法の紹介資料となります。
- 本資料はお客様の運用設計を実施される際の参考資料であり、お客様の運用を保証するものではございません。実際の運用方針に合わせて活用いただければと考えております。
- 本資料では下記の略称を用いております。
  - Central・・・・・・・・・・・・・Sophos Central
  - CIXA・・・・・・・・・・・・・・Central Intercept X Advanced
  - CIXA with XDR・・・・・・・・・ Central Intercept X Advanced with XDR
  - CIXA for Server ・・・・・・・・Central Intercept X Advanced for Server
  - CIXA for Server with XDR・・・ Central Intercept X Advanced for Server with XDR

版数	改訂日	改訂内容
初版	2021/12/01	初版として公開
1.1版	2022/05/08	一部改訂

Agenda

- ライセンスについて
- Sophos Centralについて
- グループ（ユーザグループ、デバイスグループ）エンドポイントプロテクションポリシー
- AD連携
- 検知について
  - 検出の種類
  - 検知時の対応
  - 誤検知について
  - 除外の許可
  - 隔離と復元
- EDR/XDRについて
  - Live Discover
  - Live Response
- ログについて
  - ログ、イベント、警告、その他関連情報
  - SDUログ
  - ログ/レポートの長期保存、外部連携

ライセンスについて

SOPHOS

ライセンスアクティベーション

- **アクティベーションは、Central Adminコンソールで行います**

1. Central Adminコンソールにログインします。
2. ログインしたら、右上にあるユーザー名の横にあるドロップダウンメニューをクリックし、「ライセンス」のリンクをクリックします。

3. 「ライセンスキー」の適用をクリックします。

4. ライセンスキーのアクティベートで、ライセンス証書に記載されたライセンスキーを適用します。

この作業をした日から、ライセンス使用開始となります。

（KBA： KB-000035133参照）

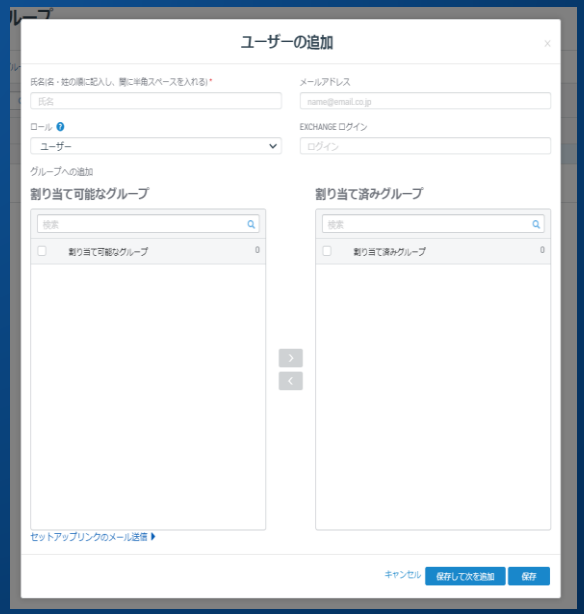
検証用アカウント → 本番用アカウント切替

- **評価時に使ったメールアドレスは使いたくない**

評価版で使用した環境を継続して本番環境として使用する場合、評価時には仮のメールアドレスを登録されている方もいらっしゃいます。その場合、本番用で使用するメールアドレスのユーザをスーパー管理者権限で登録し、そのユーザでCentral Adminにログインして、評価時に用いた仮のアカウントを削除することで対応できます。

「ユーザーとグループ」をクリックし、
追加をクリックします。

新たなユーザ追加後、そのアドレスにアクティベーション用のメールが届きます。



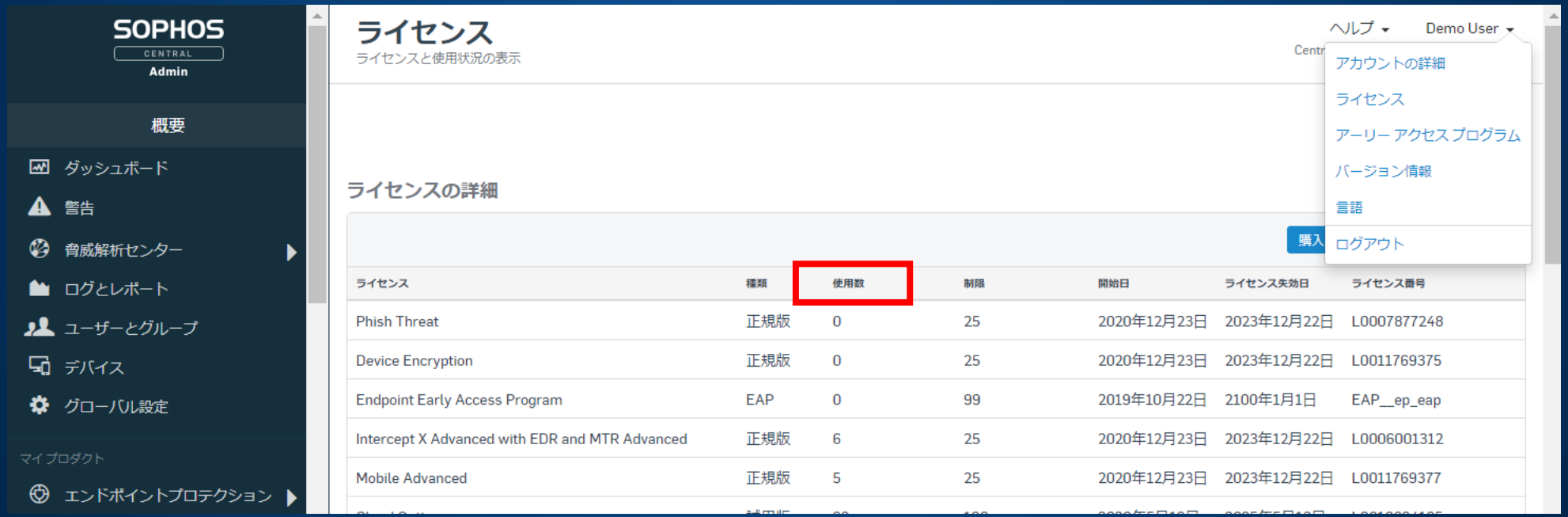
ライセンス消費について
（エンドポイントプロテクション）

SOPHOS

エンドポイントのライセンスはユーザーライセンスです

実際に端末で使用中のもののみカウントします

- 現在使用中のライセンス数は、Central Admin上のログインアカウント名 → ライセンスからご確認いただけます。

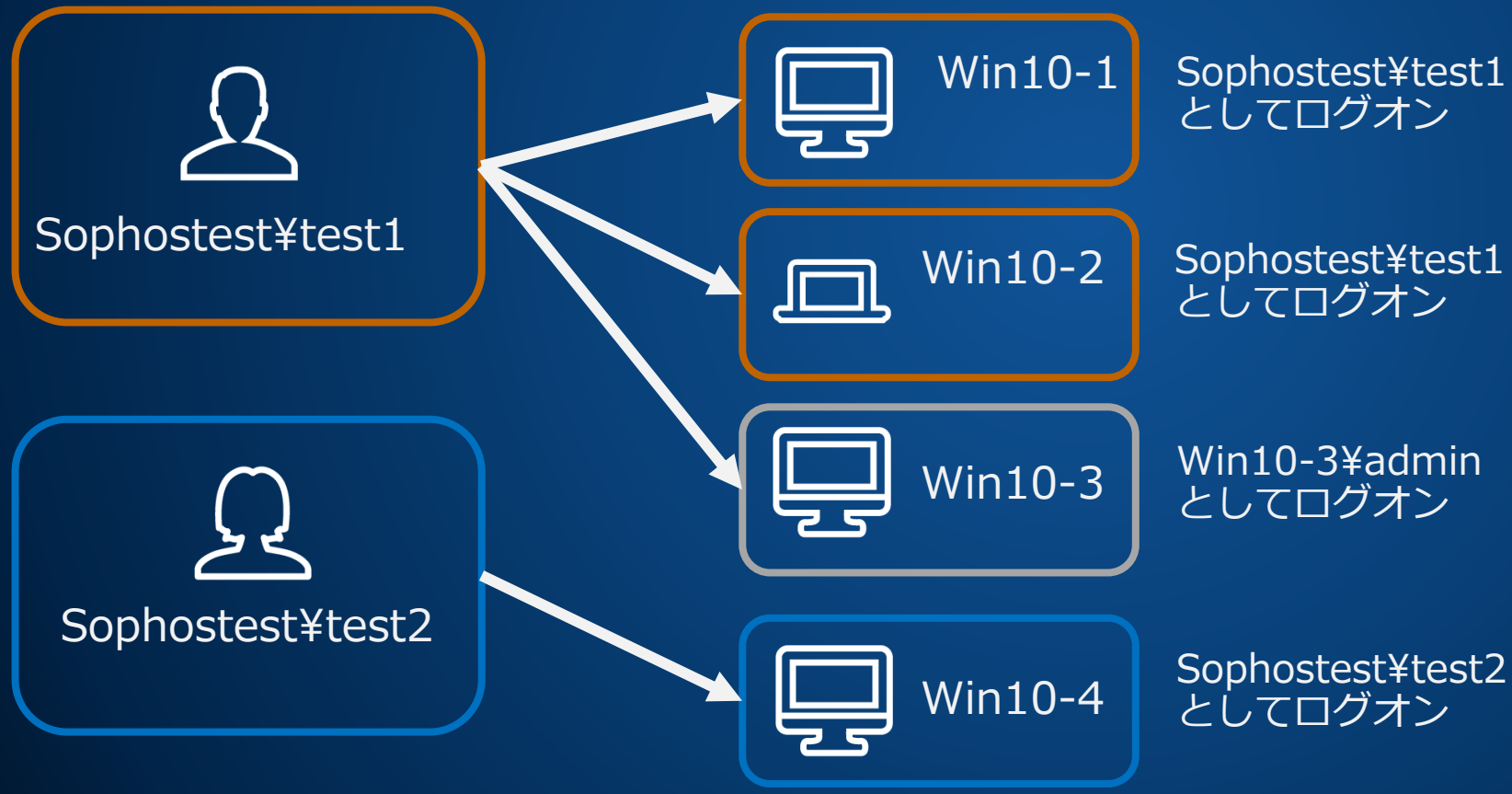


参考)

https://support.sophos.com/support/s/article/KB-000035892?language=ja

同一ユーザーが複数のデバイス使用が可能です

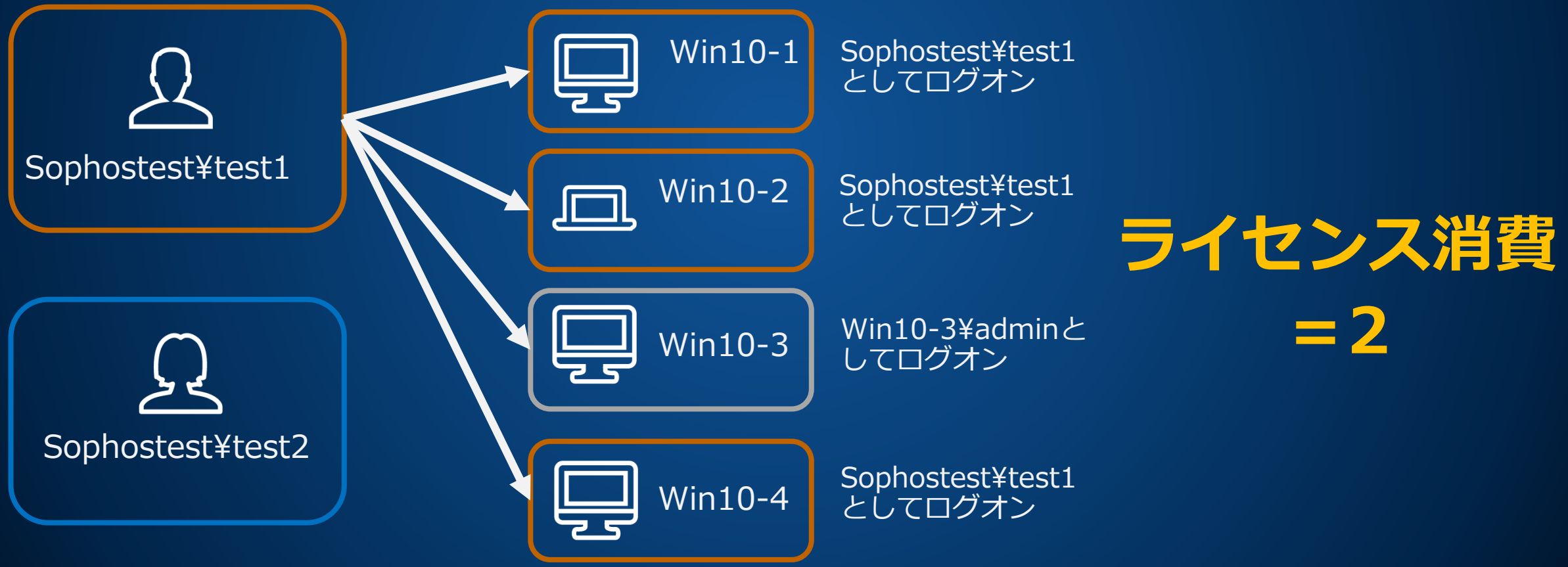
同一ユーザーが複数端末に同時ログオンしてもライセンス消費はされません
（ドメインユーザーの場合）



ライセンス消費
＝ 3

端末にログオンしていないユーザー分は消費しません

端末に誰かがログオンすると、その端末の使用情報はそのユーザーで上書きされます



ライセンス消費＝2

ローカルユーザーは注意が必要

ローカルユーザーはデバイス固有のユーザーです

ローカルユーザーは他のデバイスにはログオンできないので、端末にログオンするとライセンス消費がカウントされます

- win10-1¥adminとwin10-2¥adminは別ユーザとして認識されます
- PCキッティングの際にローカル管理者でログオンした場合は、そのライセンスが消費されます
- ただし、他の誰かがその端末にログオンした時点で、その端末のライセンス使用情報は上書きされます（ライセンス消費の問題は解消します）
- 一時的な目的で使用したローカルユーザーであれば、無視するか、削除して構いません。

ライセンスに関するその他の注意点

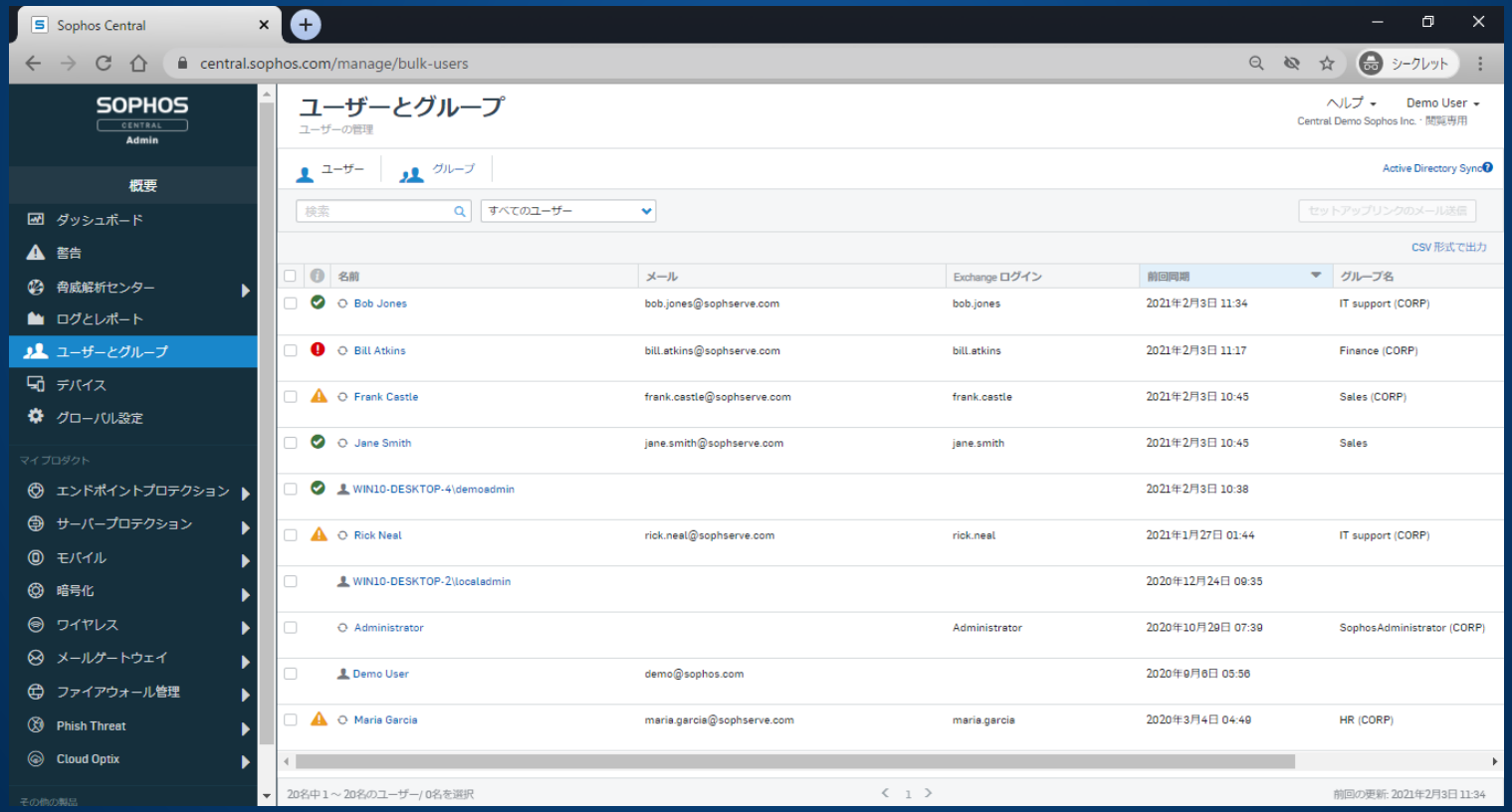
- 30日以上オフラインの端末は、ライセンス消費の対象となりません
- リアルタイム検索が無効な端末は、ライセンス消費の対象になりません
- ライセンス使用数が契約数を超過しても、保護機能の低下はございません。ただしライセンス超過の警告が出力されます
- サーバープロテクションはデバイスライセンスです

Sophos Centralについて

SOPHOS

Sophos Centralについて

「ユーザーとグループ」にSophos Centralで管理されるユーザすべてが含まれます
Central Adminにログインするユーザー、製品の管理で使用するユーザの両方が存在します



ユーザーが作られるタイミング

ユーザーがCentral上で作成されるタイミングは次の通りになります

- Central のアクティベーション時（Central Adminへのログインのため）
- 「ユーザーとグループ」から手動で追加
- CSVファイルでインポート
- AD 同期機能でADから同期（オンプレミスAD & Azure AD）
- エンドポイント製品インストール時に端末にログインしているユーザー
- 管理対象のエンドポイントに新たにログインしたユーザー

ユーザーを使用する目的

Centralがユーザーを使用する目的は次の通りになります

- Central Adminダッシュボードにログインして、ソフォス製品の管理を行う
- Self Service Portalを活用してエンドユーザーに自助してもらう
- エンドポイント製品を使用しているユーザーの管理（2021年1月現在、サーバープロテクションではログオンユーザーを記録しません）
- その他製品の管理（ユーザーライセンスをベースとした製品）

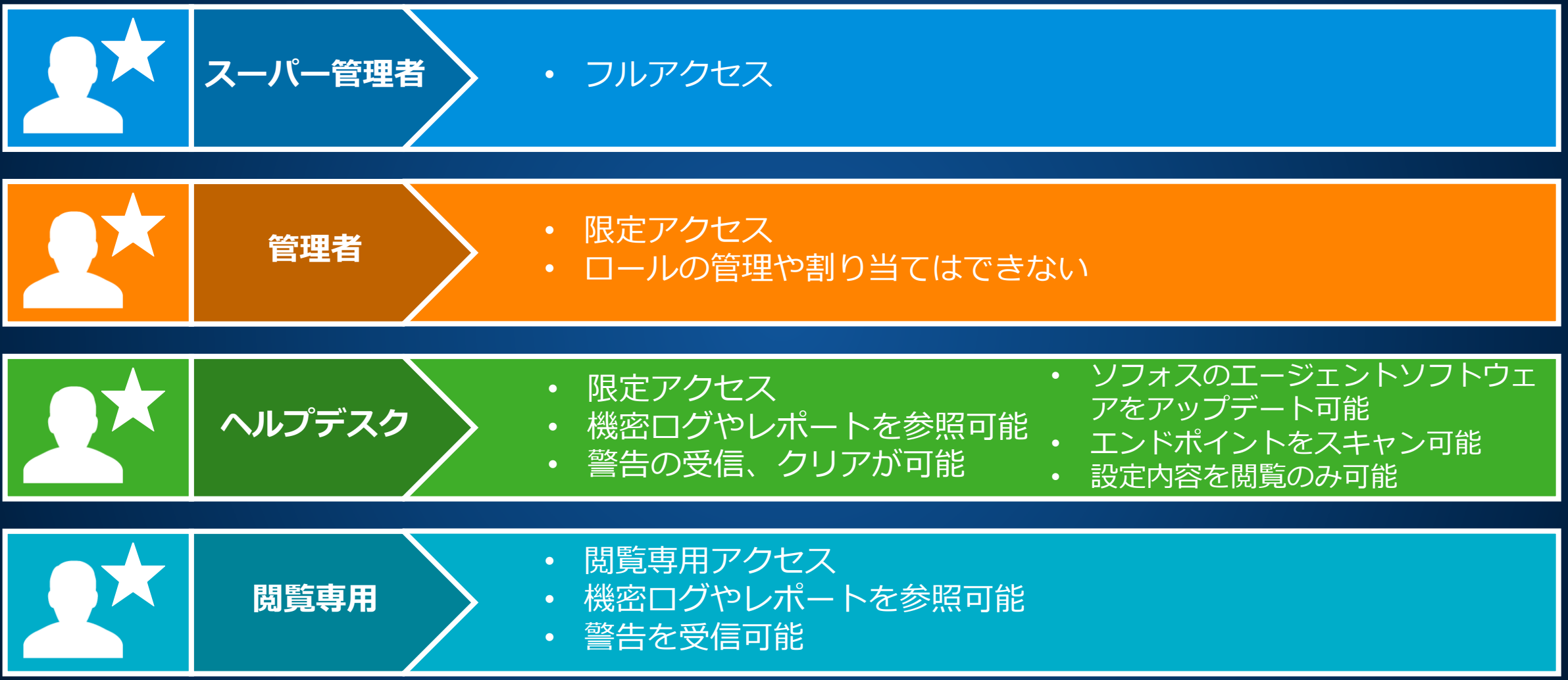
ユーザーのロールについて（管理者）

- ユーザーのロールは、スーパー管理者、管理者、ヘルプデスク、閲覧専用、ユーザーの5つに分かれます
- Central Adminにログインできるのは、スーパー管理者、管理者、ヘルプデスク、閲覧専用です（「ユーザー」ロールではログインできません）
- お客様独自のカスタムロールの作成も可能です。カスタムロールを使うと、Central Adminにログインするユーザーの製品ごとのアクセス設定も可能です

- 管理者ロール
https://docs.sophos.com/central/customer/help/ja-jp/PeopleAndDevices/RoleManagement/AdministrationRoles/index.html

- カスタムロール
https://docs.sophos.com/central/customer/help/ja-jp/PeopleAndDevices/RoleManagement/AddCustomRole/index.html

ロールベースのアクセス



ユーザーのロールについて（一般）

- エンドポイント製品、その他製品で使用するユーザーは「ユーザー」ロールです
- CSVファイルによるインポートや、AD連携で同期されるユーザーも「ユーザー」ロールです
- 一般ユーザーのロールから管理者ユーザーへの変更は可能です（スーパー管理者のみ実行可能）
- Self Service Portalへのログインは「ユーザー」ロールのみ必要です。
- Self Service Portalの使用に当たってはメールアドレスの登録が必要となり、ユーザーにパスワード設定をしてもらう必要があります
- Central Adminにログインできる管理者ユーザ(閲覧専用以上）は、すでにSelf Service Portalにログイン可能な状態なためパスワード設定は不要です。

補足：Self Service Portalについて

- エンドユーザーに、Sophos Central製品の管理を一部任せるものです。（URL：https://www.central.sophos.com/manage/self-service ）
- 事前ユーザー登録と、ユーザー自身によるパスワード設定が必要です（管理者ユーザは不要）。
- エンドポイント製品では使用しません。以下製品で使用します。
  - Central Device Encryption：復旧鍵の参照が可能です
  - Sophos Email：隔離されたメールのリリース、許可/ブロックリスト管理等が可能です
  - Sophos Mobile：各種モバイルタスクが可能です

参考）Sophos Central Admin: エンドユーザーのセルフサービス ポータル (SSP) へのアクセスを有効にする

https://support.sophos.com/support/s/article/KB-000036318?language=ja

グループ
（ユーザグループ、デバイスグループ）
エンドポイントプロテクションポリシー

SOPHOS

グループ（ユーザーグループ、デバイスグループ）

- Central Adminにはデバイスグループと、ユーザーグループの2つのグループがあり、製品によってどのグループを使用するか異なります

	エンドポイントプロテクション	サーバープロテクション	Device Encryption	Sophos Mobile	Sophos Email	Phish Threat
ユーザー/ユーザーグループ	○			○	○	○
デバイス/デバイスグループ	○	○	○	○		

- ユーザーおよびユーザーグループは、AD連携によってActive Directoryからのインポートが可能です

エンドポイントプロテクション デフォルトポリシーについて

すぐに必要なポリシーは有効な状態で用意されています

- あらかじめ「脅威対策ポリシー」、「Webコントロール」ポリシーはデフォルトポリシーが有効に設定されており、保護機能が機能します。
- その他のポリシーは必要に応じて設定を有効化し、ポリシーの適用を行います。

ポリシー適用先（ユーザー or デバイス？）

ポリシーの種類によって、適用できる対象が異なります

	脅威対策	周辺機器コントロール	アプリケーションコントロール	データ流出防止(DLP)	Webコントロール	アップデートの管理	Windows ファイアウォール
ユーザー/ユーザーグループ	○	○	○	○	○		
デバイス/デバイスグループ	○	○	○	○		○	○

カスタマイズポリシー

脅威対策 (6)

	名前	状態	種類 (個別/グループ)	前回更新日時
✣	EXP disabled	✔ 適用済み	ユーザー (0 / 0)	2020/07/04
✣	Main (EDR disabled)	✔ 適用済み	ユーザー (0 / 0)	2020/07/04
✣	Main	✔ 適用済み	ユーザー (8 / 3)	2020/12/24
✣	EXP enabled per device	✔ 適用済み	コンピュータ (0 / 0)	2020/07/04
✣	脅威対策 Win 10	✔ 適用済み	コンピュータ (0 / 1)	2020/07/04
	デフォルトポリシー - 脅威対策	✔ 適用済み		2019/04/24

- ポリシー内容を変更する場合は、デフォルトポリシーを複製しカスタマイズすることをお勧めします
- カスタマイズポリシーは、運用効率化のために個々のユーザ/デバイスではなく、ユーザーグループ/デバイスグループに適用することをお勧めします
- 複数のポリシーが存在する場合は、上から評価され最初にマッチしたものが適用されます

AD連携（オンプレミスAD、Azure AD、Azure AD Federation）

SOPHOS

３つのAD連携

- オンプレミスAD連携
  - AD Sync Utilityツールをダウンロード、インストールして同期（Centralに送信）
  - 同期対象は、ユーザー名、ログイン、メールアドレス、グループとグループメンバーシップ（メンバーが存在する場合のみ）
  - Centralへの接続にはAPI認証が必要
- Azure AD Sync
  - Azure ADへのアクセス権（読み取り専用）設定し、情報をPull
  - オンプレミスAD連携とAzure AD Syncの両方を使用することはできません
- Azure AD Federation
  - Central Admin、Self Service PortalへのSSOを提供
  - 二要素認証はAzure AD Federation側で設定

検知について

SOPHOS

Windows 版 Intercept X Advanced

エンドポイントプロテクション

脅威対策

- Web セキュリティ
- ダウンロードレピュテーション
- ファイルのマルウェア検索
- Live Protection
- 実行前解析とランタイム動作解析 (HIPS)
- 不要と思われるアプリケーション (PUA) のブロック
- マルウェアの自動削除
- Malicious Traffic Detection (MTD)

コントロール

- Web コントロール
- 周辺機器コントロール
- アプリケーションコントロール
- データ流出防止

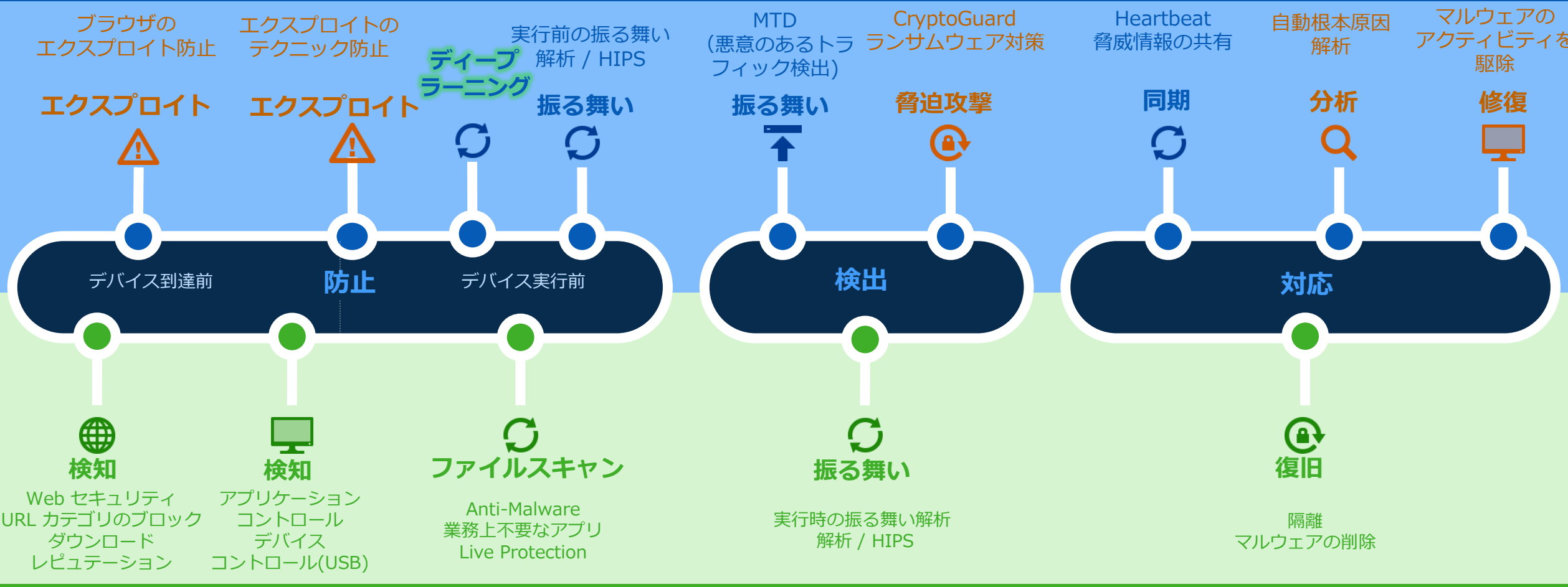
Intercept X

- ディープラーニングによるマルウェア検出
- エクスプロイト対策
- Malicious Traffic Detection
- 持続的攻撃対策
- CryptoGuard
- WipeGuard
- セーフブラウジング
- マルウェアの自動削除
- 根本原因解析を実行する
- Sophos Clean

次世代型エンドポイント保護機能

防止・検出・対応それぞれの観点で必要な保護を実現します

次世代型



従来型マルウェア対策

検出の種類

SOPHOS

検出の種類

Troj/、Mal/、W32/、JS/、VBS/、ELF/	悪意のある既知の脅威が実行前に検出された
Sus/	疑わしいファイル (確実性のしきい値が低い既知の脅威が実行前に検出された)
HIPS/	実行時に検出された不明な脅威からの悪意のある動作が
C2/	悪意のあるネットワークアクティビティを実行時に検出

https://support.sophos.com/support/s/article/KB-000034084?language=ja

検出の種類

HPmal/ HPsus/	実行中の特定のプロファイルと一致する未知の脅威と疑わしいファイルを検出する
CXmail/	実行前に検出されたメール経由の新規の脅威
CXmal/	実行時に検出された既知の脅威の新規の未知の亜種
CXweb/	ダウンロードが行われる前 (実行前) に検出された悪意のあるファイル

https://support.sophos.com/support/s/article/KB-000034084?language=ja

検出の種類

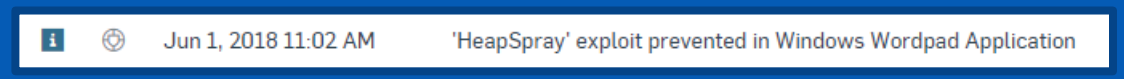
Adware または PUA	実行前に検出されたアドウェアおよび不要と思われるアプリケーション
Controlled Application	ポリシーによってブロックされた悪意のないアプリケーション(実行前)

https://support.sophos.com/support/s/article/KB-000034084?language=ja

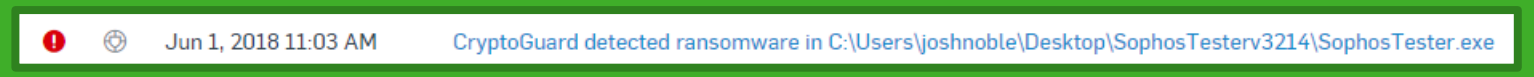
検出の種類

Intercept X

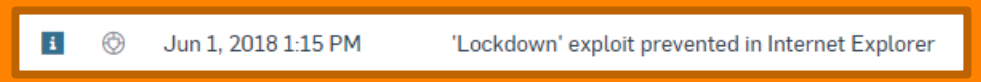
Anti-Exploit



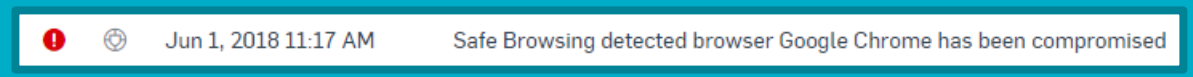
CryptoGuard



Application Lockdown



Safe Browsing



検出の種類

マシンラーニング

ML/PE-A
悪意のある Portable Executable

ML / PUA
不要と思われるアプリケーション:

https://support.sophos.com/support/s/article/KB-000036922

Portable Executable の例：
.exe
.sys
.dll
.scr　　など多数

検知時の対応

SOPHOS

ウイルス検知時の対応の流れ

管理者

③脅威ケース確認

利用者

①マルウェア実行

②脅威駆除

検知

アクセス制限

復旧

自動対応（検知ー隔離ー駆除ー復旧）

ランサムウェア感染時

SOPHOS

タイムライン

管理者

④管理者による確認

⑤脅威ケース確認

②アラート通知

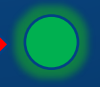
利用者

①ランサムウェア感染

③脅威駆除

検知

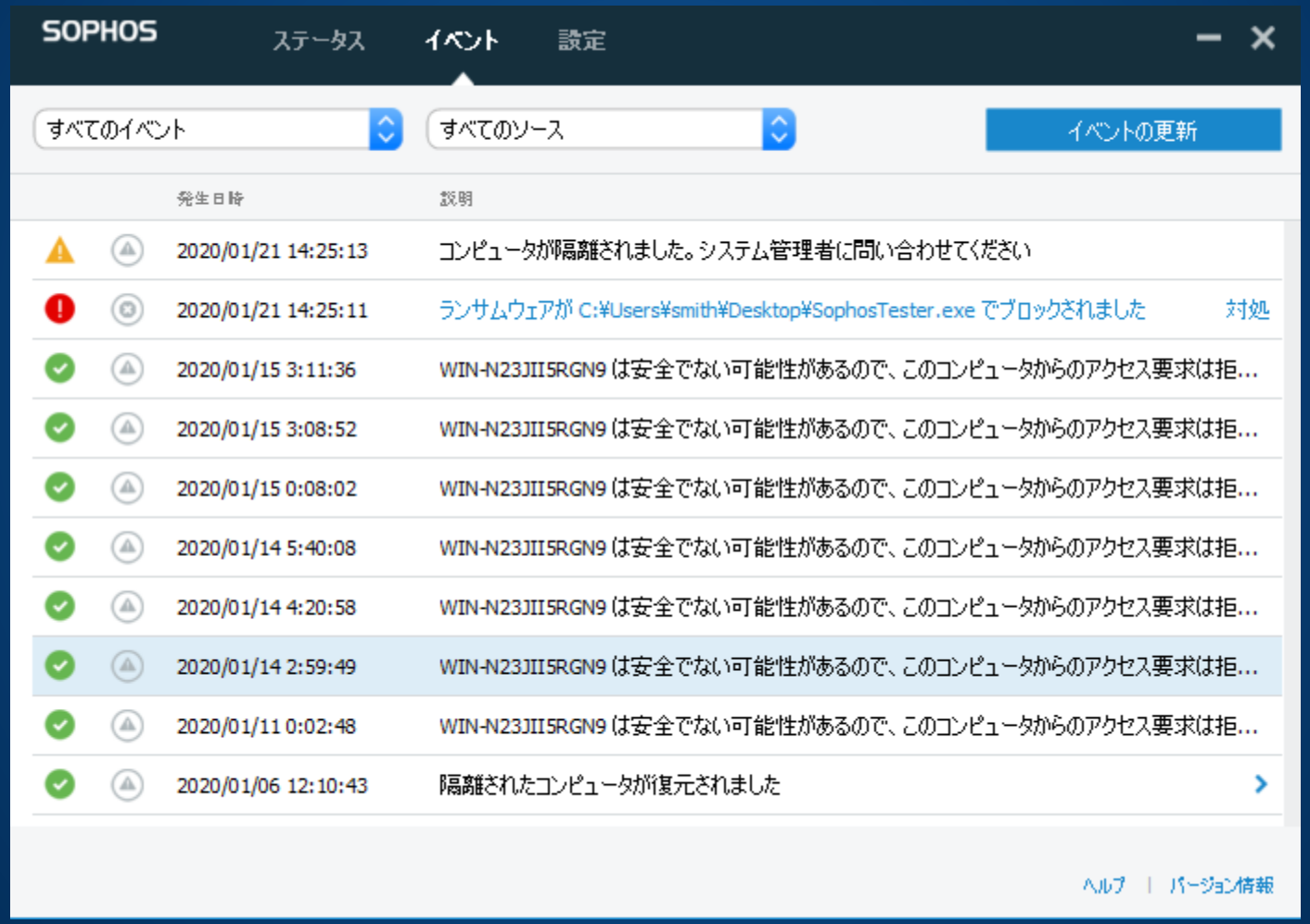
アクセス制限



復旧

自動対応（検知ー隔離ー駆除ー復旧）

①ランサムウェア感染


SOPHOS
ステータス
イベント
設定
すべてのイベント
すべてのソース
イベントの更新
発生日時
説明
2020/01/21 14:25:13
コンピュータが隔離されました。システム管理者に問い合わせてください
2020/01/21 14:25:11
ランサムウェアが C:¥Users¥smith¥Desktop¥SophosTester.exe でブロックされました
対処
2020/01/15 3:11:36
WIN-N23JII5RGN9 は安全でない可能性があるので、このコンピュータからのアクセス要求は拒...
2020/01/15 3:08:52
WIN-N23JII5RGN9 は安全でない可能性があるので、このコンピュータからのアクセス要求は拒...
2020/01/15 0:08:02
WIN-N23JII5RGN9 は安全でない可能性があるので、このコンピュータからのアクセス要求は拒...
2020/01/14 5:40:08
WIN-N23JII5RGN9 は安全でない可能性があるので、このコンピュータからのアクセス要求は拒...
2020/01/14 4:20:58
WIN-N23JII5RGN9 は安全でない可能性があるので、このコンピュータからのアクセス要求は拒...
2020/01/14 2:59:49
WIN-N23JII5RGN9 は安全でない可能性があるので、このコンピュータからのアクセス要求は拒...
2020/01/11 0:02:48
WIN-N23JII5RGN9 は安全でない可能性があるので、このコンピュータからのアクセス要求は拒...
2020/01/06 12:10:43
隔離されたコンピュータが復元されました
ヘルプ
バージョン情報

②管理者へのアラートメール

返信 全員に返信 転送 IM

Tue 1/21/2020 2:29 PM

D

do-not-reply@central.sophos.com

[高レベル] Sophos Central で発生した警告 [Sophos K.K.]: ランサムウェアを検出しました

宛先 Ryuichiro Maruyama

SOPHOS CENTRAL

Sophos Central のイベントの詳細: Sophos K.K.

現象: ファイルを暗号化しようとするランサムウェアを検出しました。

発生場所: DESKTOP-3MIQBCT

パス: C:\Users\smith\Desktop\SophosTester.exe

検出された項目: CryptoGuard

デバイスに関連付けられているユーザー: DESKTOP-3MIQBCT\smith

深刻度: 高レベル

ソフォス製品で実行された処理: ランサムウェアによるファイルシステムへのアクセスをブロックしました。コンピュータが Windows クライアントマシンまたはサーバーの場合、ランサムウェアは自動的にクリーンアップされます。Mac の場合は、手動でクリーンアップを実行する必要があります。

必要な対応:

- Windows コンピュータの場合:
  1. サンプルの自動送信が有効になっていない場合は、ランサムウェアのサンプルファイルをソフォスに送信してください。分類先を確認後、場合によってはソフォスのルールを更新します。マルウェアの場合は、以後 Sophos Central でブロックされます。
  2. Sophos Central の「**警告**」で、この警告を対処済みとしてマークします。

- Mac の場合:
  1. 他のコンピュータに危険が及ぶ恐れのないネットワークに、コンピュータを一時的に移動します。対象のコンピュータに移動し、隔離エリアを開きます。検出されたランサムウェアを探して手動で削除します。
  2. Sophos Central の「**警告**」で、この警告を対処済みとしてマークします。

参考情報:

Sophos Central に関するサポートデータベースの文章: https://community.sophos.com/kb?TopicId=9000。

Sophos Central よくある質問 (FAQ) - https://community.sophos.com/kb/ja-jp/119598。

詳細は、https://central.sophos.com/ にサインインしてご確認ください

注: 選択した警告メールの送信頻度に応じて、警告は、各種類 (例: 保護に失敗したイベントなど) につき 24時間に 1件のみ送信されるか、1種類につき 1件のみ送信されます。一方、Sophos Central コンソールのダッシュボードには、同じ種類の警告が複数表示される可能性もあります。

必要なアクション

ソフォス製品で実行された処理: ランサムウェアによるファイルシステムへのアクセスをブロックしました。コンピュータが Windows クライアントマシンまたはサーバーの場合、ランサムウェアは自動的にクリーンアップされます。
Mac の場合は、手動でクリーンアップを実行する必要があります。

必要な対応:

- Windows コンピュータの場合:
  1. サンプルの自動送信が有効になっていない場合は、ランサムウェアのサンプルファイルをソフォスに送信してください。分類先を確認後、場合によってはソフォスのルールを更新します。マルウェアの場合は、以後 Sophos Central でブロックされます。
  2. Sophos Central の「警告」で、この警告を対処済みとしてマークします。

Mac の場合:

1. 他のコンピュータに危険が及ぶ恐れのないネットワークに、コンピュータを一時的に移動します。対象のコンピュータに移動し、隔離エリアを開きます。検出されたランサムウェアを探して手動で削除します。
2. Sophos Central の「警告」で、この警告を対処済みとしてマークします。

Central Admin ダッシュボードへの通知

④デバイス上のイベントの確認

警告の確認と承認

エンドポイントの種類: コンピュータ

OS: Windows

デバイス: DESKTOP-3MIQBCT

ランサムウェア:

family_id: 4f20e8ed-019a-d203-f6d0-b852e7ec5641

process_version: 3.7.15

thumbprint: 00f76dcfecffd82a4a78696d531cb8b925c20cdec735061dd2a389ee2561d9c1

type: CryptoGuard

process_pid: 8884

version: 3.7.14.40

uid: fbfe75f6-1882-0131-aeac-68dfb5c4cbb1

app_name: Sophos Tester

process_alias_path: $desktop\SophosTester.exe

process_name: Sophos Tester

details: Mitigation CryptoGuard
Timestamp 2020-01-21T05:25:11

Platform 10.0.18362/x64 v40 06_2a*
PID 8884
Application C:\Users\smith\Desktop\SophosTester.exe
Created 2020-01-21T05:23:34
Modified 2020-01-21T05:21:28
Description Sophos Tester 3.7.15

Filename C:\Users\smith\Desktop\SophosTester.exe

C:\Users\smith\AppData\Local\Sophos Tester\Locky\test_02.rtf
C:\Users\smith\AppData\Local\Sophos Tester\Locky\test_01.rtf
C:\Users\smith\AppData\Local\Sophos Tester\Locky\test_00.rtf

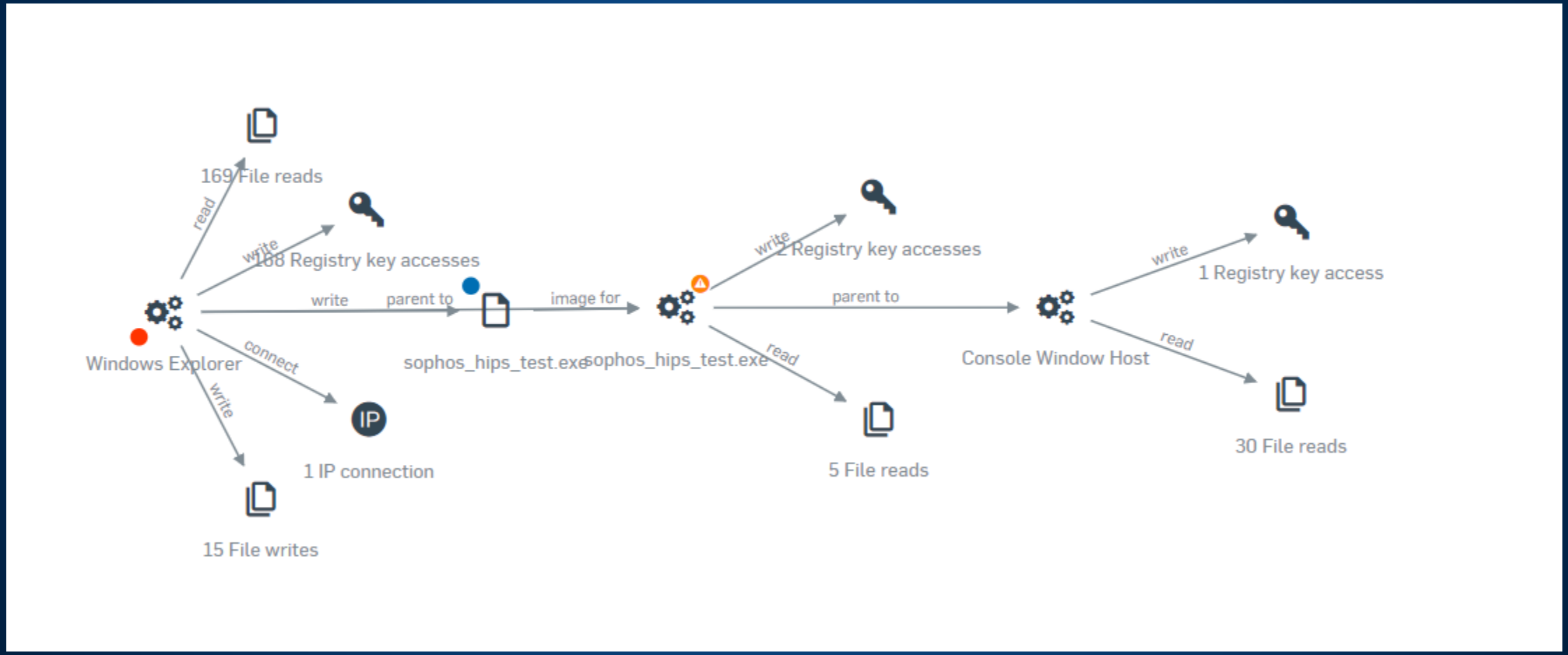
WBHs
e6d4d1d5d0ded7c6dbd8c6d6ecd4d0ded5dfd1c6dbd8c6d6ecd4d0d0d0d7d4c6dbd8c6d6ec

Process Trace
1 C:\Users\smith\Desktop\SophosTester.exe [8884]
"C:\Users\smith\Desktop\SophosTester.exe" /target
2 C:\Users\smith\Desktop\SophosTester.exe [196]
"C:\Users\smith\Desktop\SophosTester.exe" /elevated
3 C:\Users\smith\Desktop\SophosTester.exe [3576]
4 C:\Windows\explorer.exe [4880]
5 C:\Windows\System32\userinit.exe [3736]

Thumbprint
00f76dcfecffd82a4a78696d531cb8b925c20cdec735061dd2a389ee2561d9c1
Digital signature certificate based thumbprint
fdafe5c4927cab9f045810ae8c58388e3938758bb46646ab7c2d94e83af62756

process_path: C:\Users\smith\Desktop\SophosTester.exe

⑤脅威感染の詳細情報参照（脅威ケース）



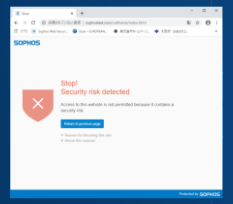
C2通信検出時

SOPHOS

タイムライン

管理者

②アラート通知



④管理者による確認

⑤脅威ケース確認

利用者

①C2サーバーアクセス

③脅威検出なし

検知

アクセス制限

復旧

自動対応（検知ー隔離ー駆除?）

②管理者へのアラートメール

返信 全員に返信 転送 IM

Fri 1/17/2020 11:39 PM

D do-not-reply@central.sophos.com

[高レベル] Sophos Central で発生した警告 [Sophos K.K.]: 悪質なトラフィックが検出されました

宛先 Ryuichiro Maruyama

このメール警告は Sophos Central より自動配信されています。このメールには返信しないでください。

SOPHOS CENTRAL

Sophos Central のイベントの詳細: Sophos K.K.

現象: コンピュータが悪質なトラフィックを送信しています。これは、このコンピュータが外部のコンピュータと通信を行っていることを意味し、外部のコンピュータ (悪意があると思われる) にデータを送信したり、指示を受け取ったりしている可能性があります。

発生場所: DESKTOP-VA83BLA

パス: C:\program files (x86)\google\chrome\application\chrome.exe

検出された項目: C2/Generic-C

デバイスに関連付けられているユーザー: DESKTOP-VA83BLA\RyuichiroMaruyama

深刻度: 高レベル

ソフォス製品で実行された処理: エンドユーザーに通知しました。コンピュータが実行しているプロセスも解析しましたが、既存のマルウェアは検出されませんでした。サンプルの自動送信が有効になっている場合は、分析用に SophosLabs にサンプルファイルが送信されました。

必要な対応: コンピュータに移動して確認をします。サンプルの自動送信が有効になっていない場合は、検出されたトラフィックの原因となっているアプリケーションのサンプルファイルをソフォスに送信してください。ソフォスでサンプルが分類されると、アプリケーションが安全であるか悪意のあるものであるかを識別するルールが更新されます。その後、悪意のあるアプリケーションにアクセスしようとすると、Sophos Central でブロック・削除されます。

参考情報:

Sophos Central に関するサポートデータベースの文章: https://community.sophos.com/kb?TopicId=9000。

Sophos Central よくある質問 (FAQ) - https://community.sophos.com/kb/ja-jp/119598。

詳細は、https://central.sophos.com/ にサインインしてご確認ください

注: 選択した警告メールの送信頻度に応じて、警告は、各種類 (例: 保護に失敗したイベントなど) につき 24時間に 1件のみ送信されるか、1種類につき 1件のみ送信されます。一方、Sophos Central コンソールのダッシュボードには、同じ種類の警告が複数表示される可能性もあります。

必要なアクション

ソフォス製品で実行された処理: エンドユーザーに通知しました。コンピュータが実行しているプロセスも解析しましたが、既存のマルウェアは検出されませんでした。サンプルの自動送信が有効になっている場合は、分析用に SophosLabs にサンプルファイルが送信されました。

必要な対応: コンピュータに移動して確認をします。サンプルの自動送信が有効になっていない場合は、検出されたトラフィックの原因となっているアプリケーションのサンプルファイルをソフォスに送信してください。ソフォスでサンプルが分類されると、アプリケーションが安全であるか悪意のあるものであるかを識別するルールが更新されます。その後、悪意のあるアプリケーションにアクセスしようとすると、Sophos Central でブロック・削除されます。

誤検知について

SOPHOS

誤検知が起こり得る理由（代表例）

- ハッシュ値衝突
  → 旧来型SAV（レアケース）

- ML/PE-AまたはML/PUA
  → 自社開発アプリ等でレピュテーションなし、AIによるスコアが低評価

- エクスプロイト対策
  → 自社開発アプリ（Excelマクロ等）で潜在的な脅威となりうるアクションを検知。
  →実際に潜在的な脆弱性を検知（アプリケーション自体の脆弱性の修正で対応が必要）

除外と許可

SOPHOS

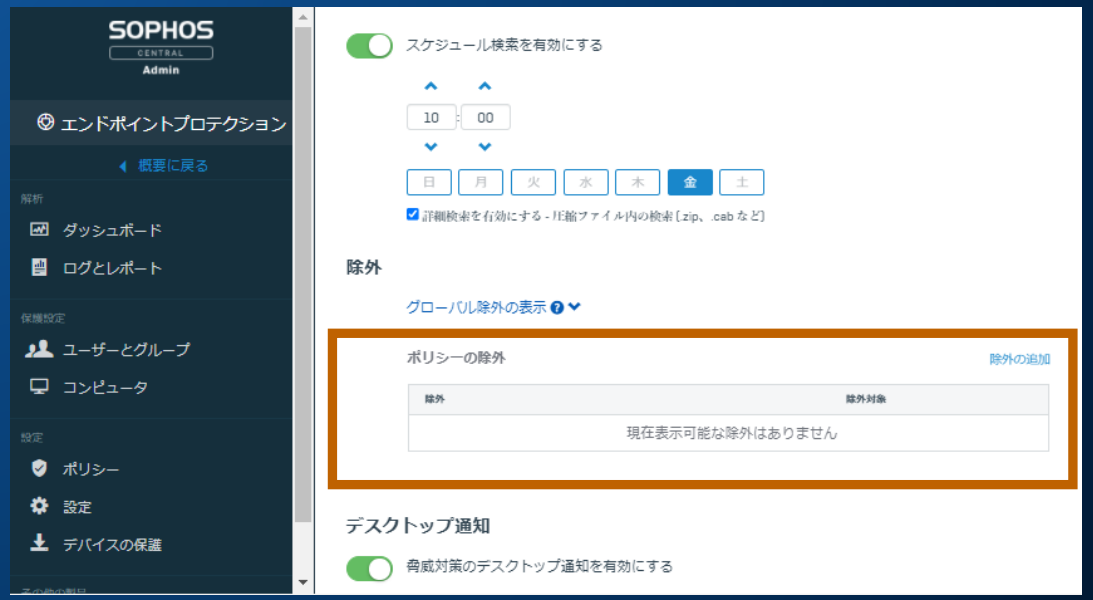
除外設定箇所

- グローバル設定
  > グローバル除外

  組織のすべての端末に設定が反映されます

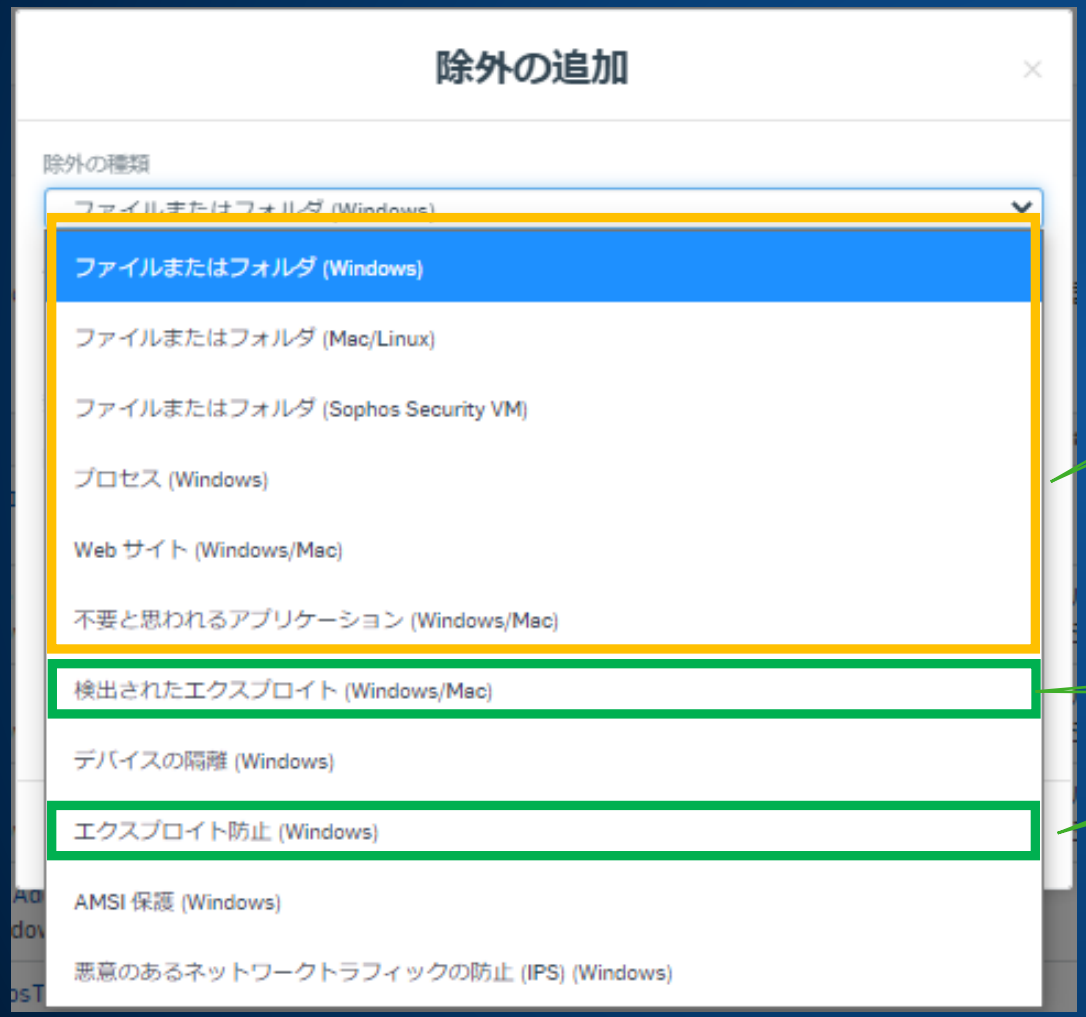
- エンドポイントプロテクションor
  サーバープロテクション
  > ポリシー
  > 脅威対策ポリシー

  ポリシー適用先のみに設定が反映されます



検索から除外する項目

グローバル設定 > グローバル除外



Sophos Anti-Virus
（従来型）検知機能

エクスプロイト対策
検知機能

Sophos Anti-Virus（従来型アンチウイルス機能）での除外設定

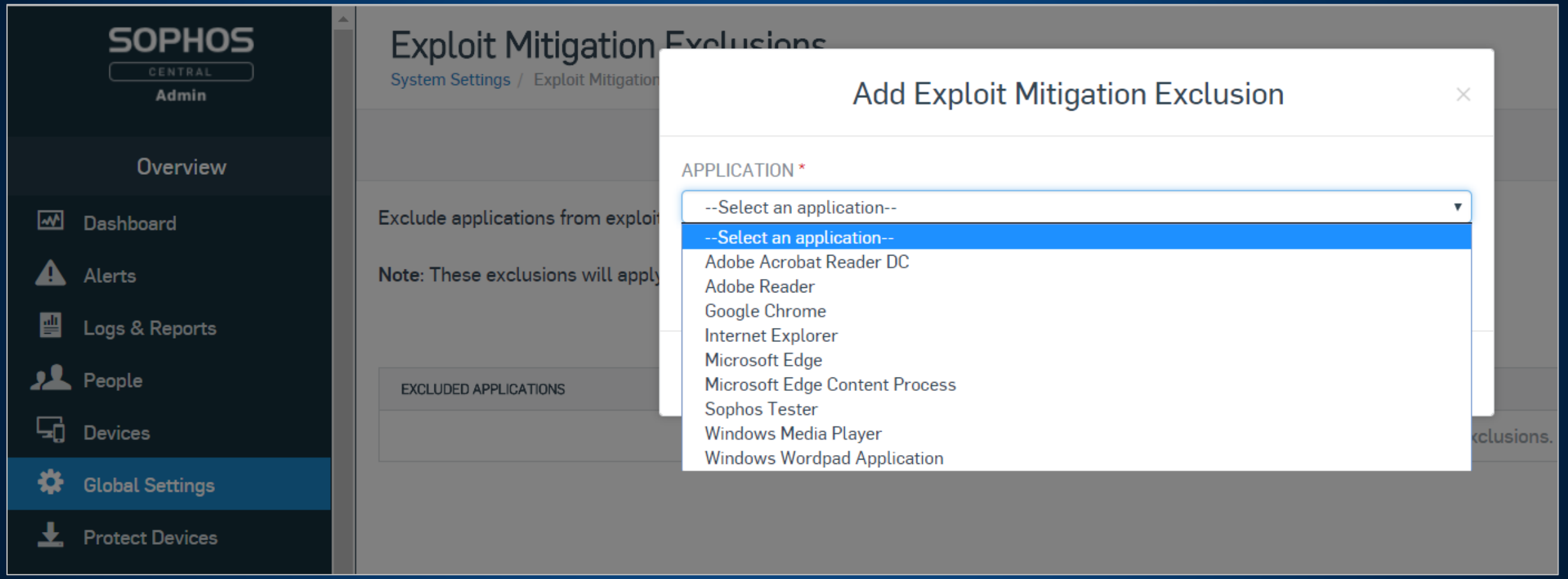
- ファイルパス/フォルダパス（リアルタイム/スケジュールスキャン対応）
  例）C:¥programdata¥adobe¥photoshop¥

https://docs.sophos.com/central/customer/help/ja-jp/ManageYourProducts/Overview/GlobalSettings/GlobalExclusions/ExclusionVariablesWindows/index.html

- プロセス名指定（リアルタイムスキャンのみ）
  例）%PROGRAMFILES%¥Microsoft Office¥Office 14¥Outlook.exe

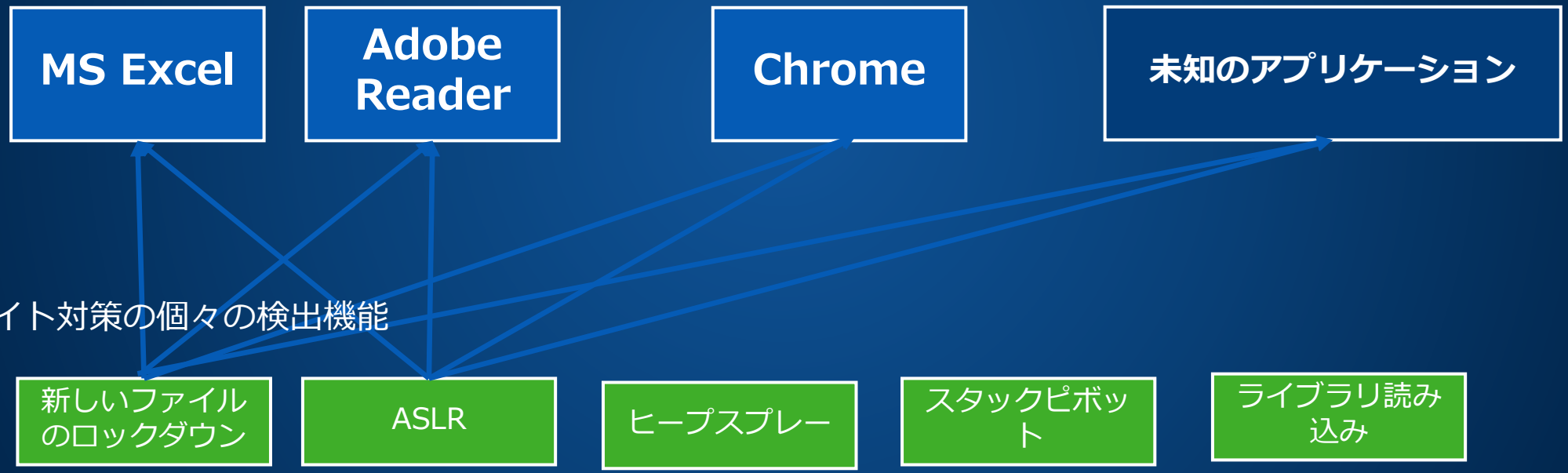
https://docs.sophos.com/central/customer/help/ja-jp/ManageYourProducts/Overview/GlobalSettings/GlobalExclusions/ProcessExclusions/index.html

エクスプロイト防止の除外



エクスプロイト対策の検出機能とアプリケーション

アプリケーション （エンドポイント側で自動検出）



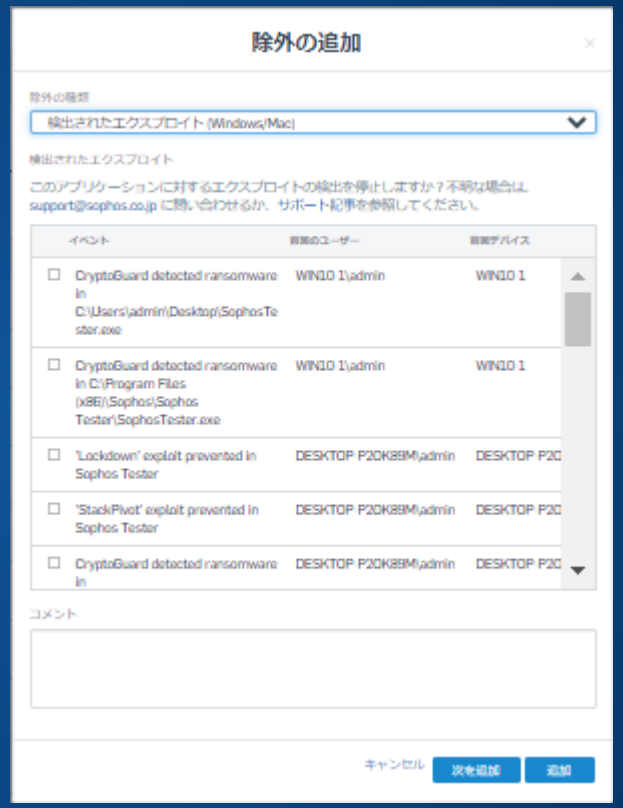
エクスプロイト対策機能の除外設定

- 検出単位で除外
  1) 検出されたエクスプロイト
     - 実際に検出が発生した後に設定が可能
     - 除外の範囲が最小
     - ファイル属性が変わると再検出発生可能性あり

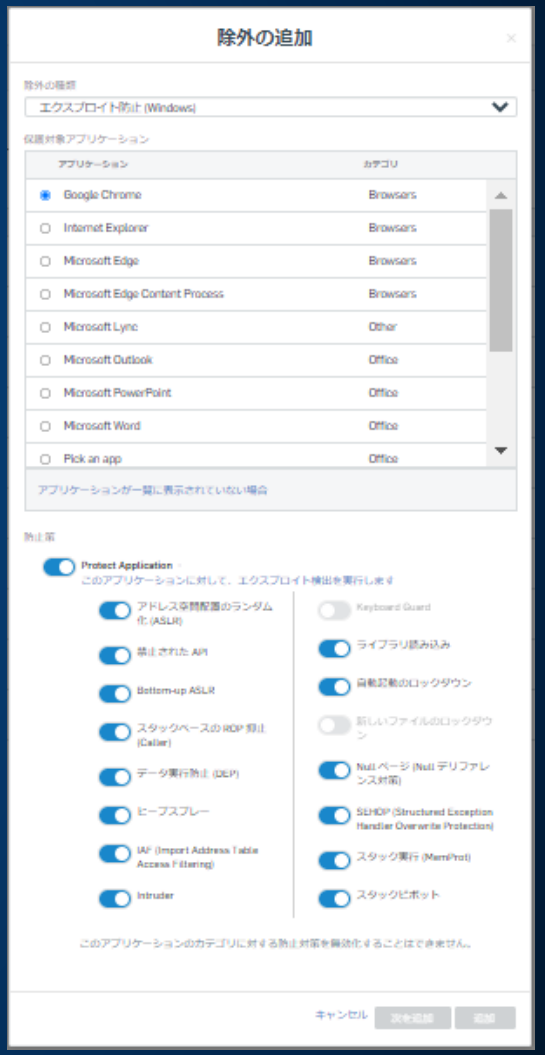
- アプリケーションに対する除外
  → 検知後、検知前問わず設定可能
  2) 既知のアプリに対する特定検出除外
  3) 既知のアプリに対する全般除外
  4) 不明アプリに関する全般除外

- 検出機能の無効化
  → 非推奨（最終手段または問題切り分け）
  5) 脅威対策ポリシーで個々の検出機能を無効化

検出されたエクスプロイト

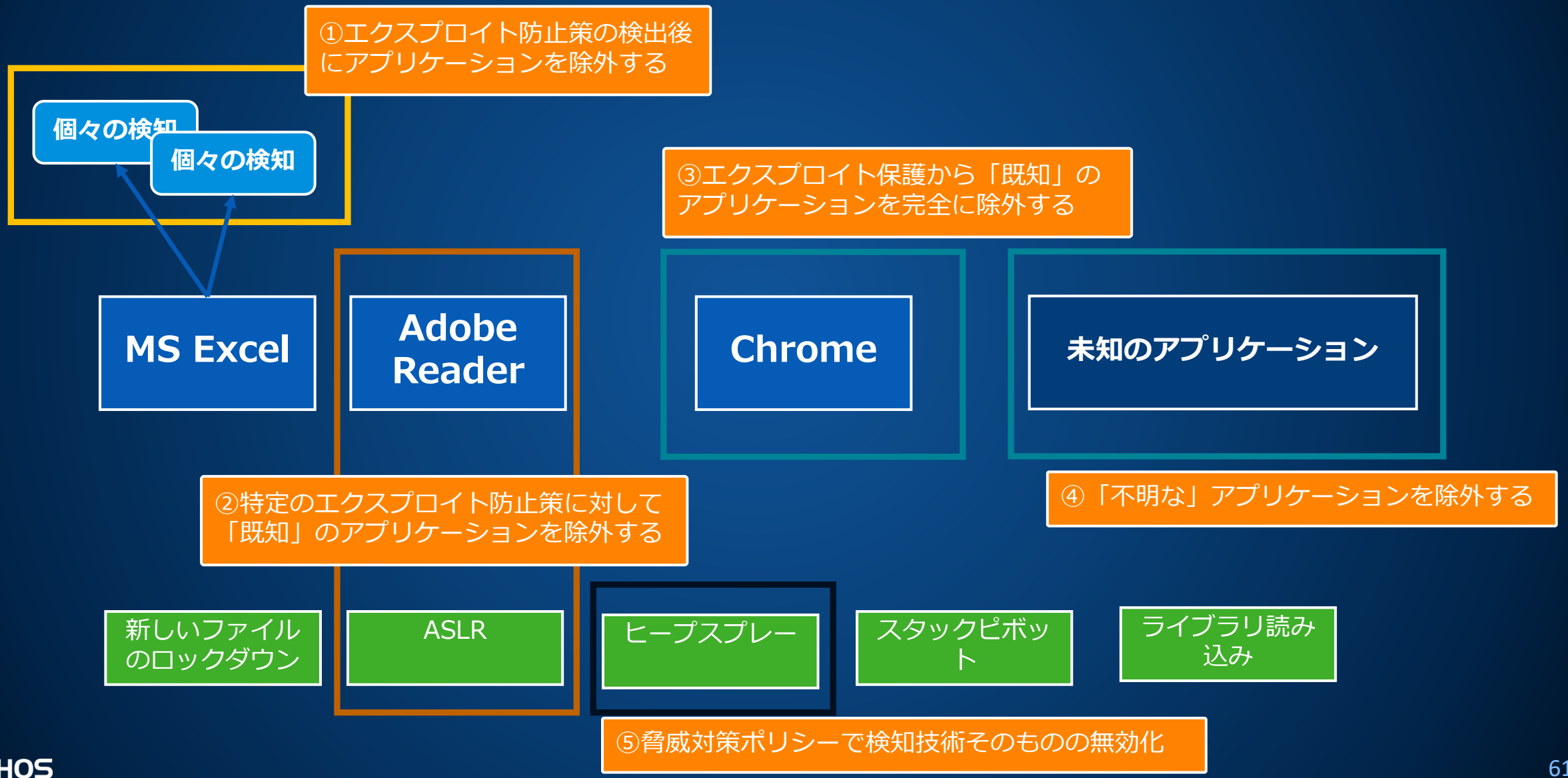


アプリケーションに対する除外



https://support.sophos.com/support/s/article/KB-000039185?language=ja

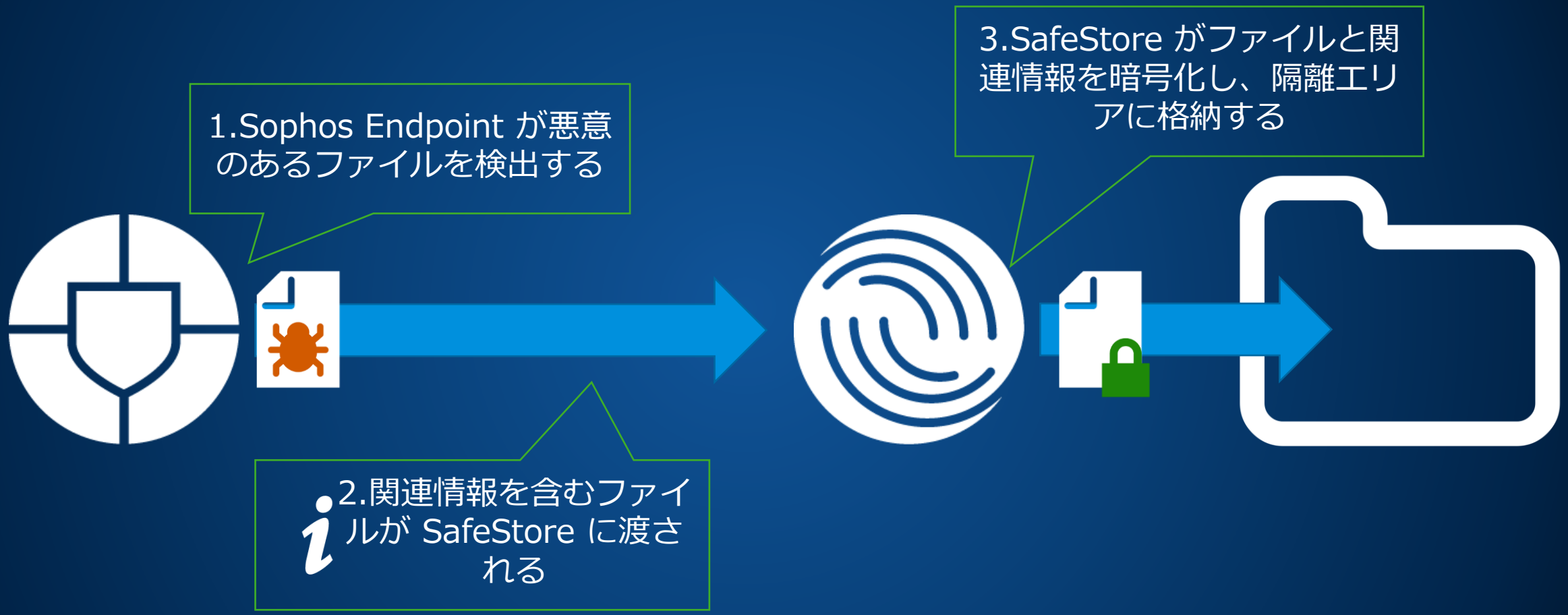
エクスプロイト対策の除外方法（相関図）



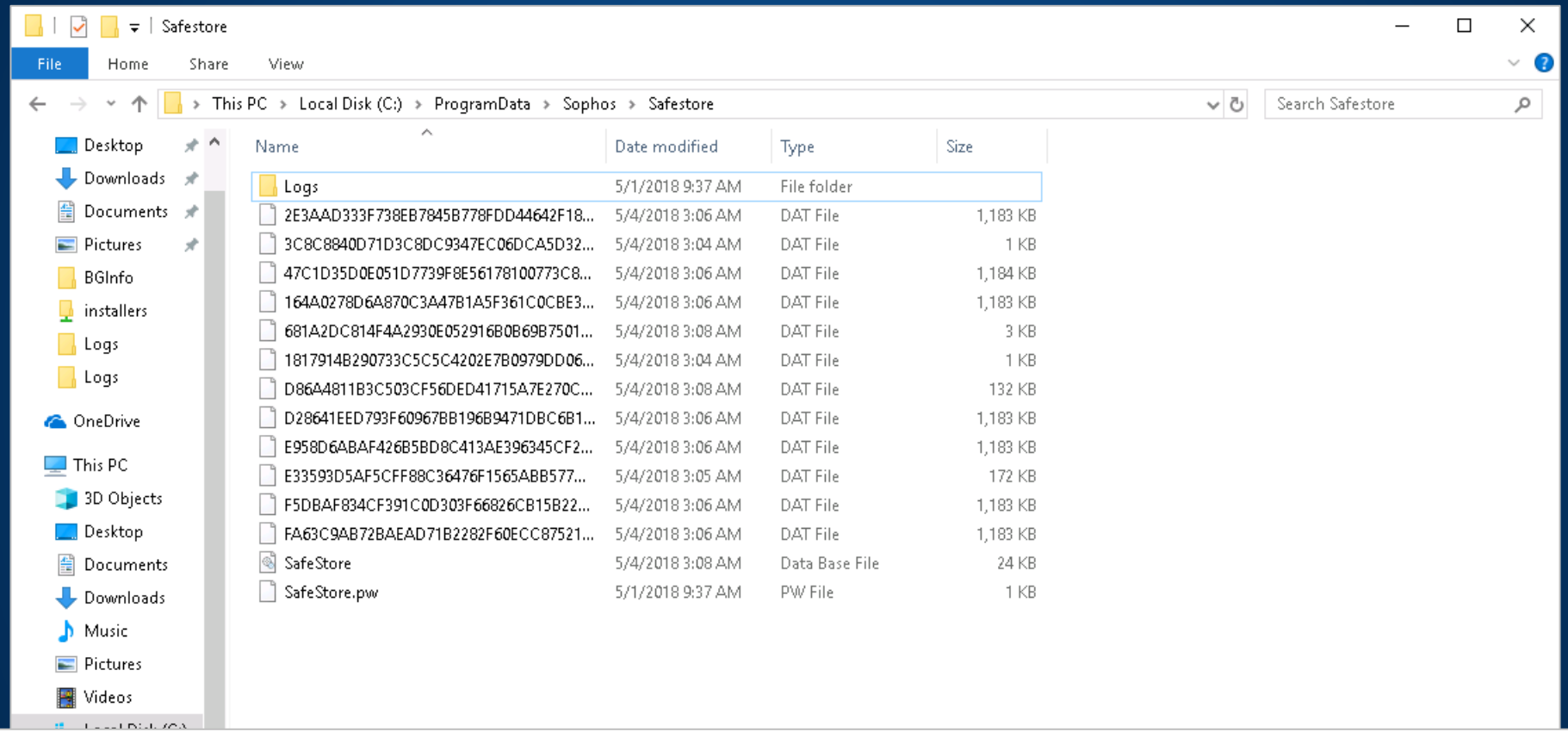
隔離と復元

SOPHOS

隔離の概要


1.Sophos Endpoint が悪意のあるファイルを検出する
2.関連情報を含むファイルが SafeStore に渡される
3.SafeStore がファイルと関連情報を暗号化し、隔離エリアに格納する

SafeStore




```
2018-05-04T03:08:43.347Z GetContext context: 0073B018
2018-05-04T03:08:43.347Z Task: "savefile" (component 16)
2018-05-04T03:08:43.347Z Savefile: C:\Users\Administrator.SOPHOS\Downloads\pskill.exe
2018-05-04T03:08:43.441Z Task successful (time spent: 84ms)
```

SafeStore からファイルをリリースする

SafeStore からファイルをリリースする必要があるのはなぜか？

不要な検出
例：PUA

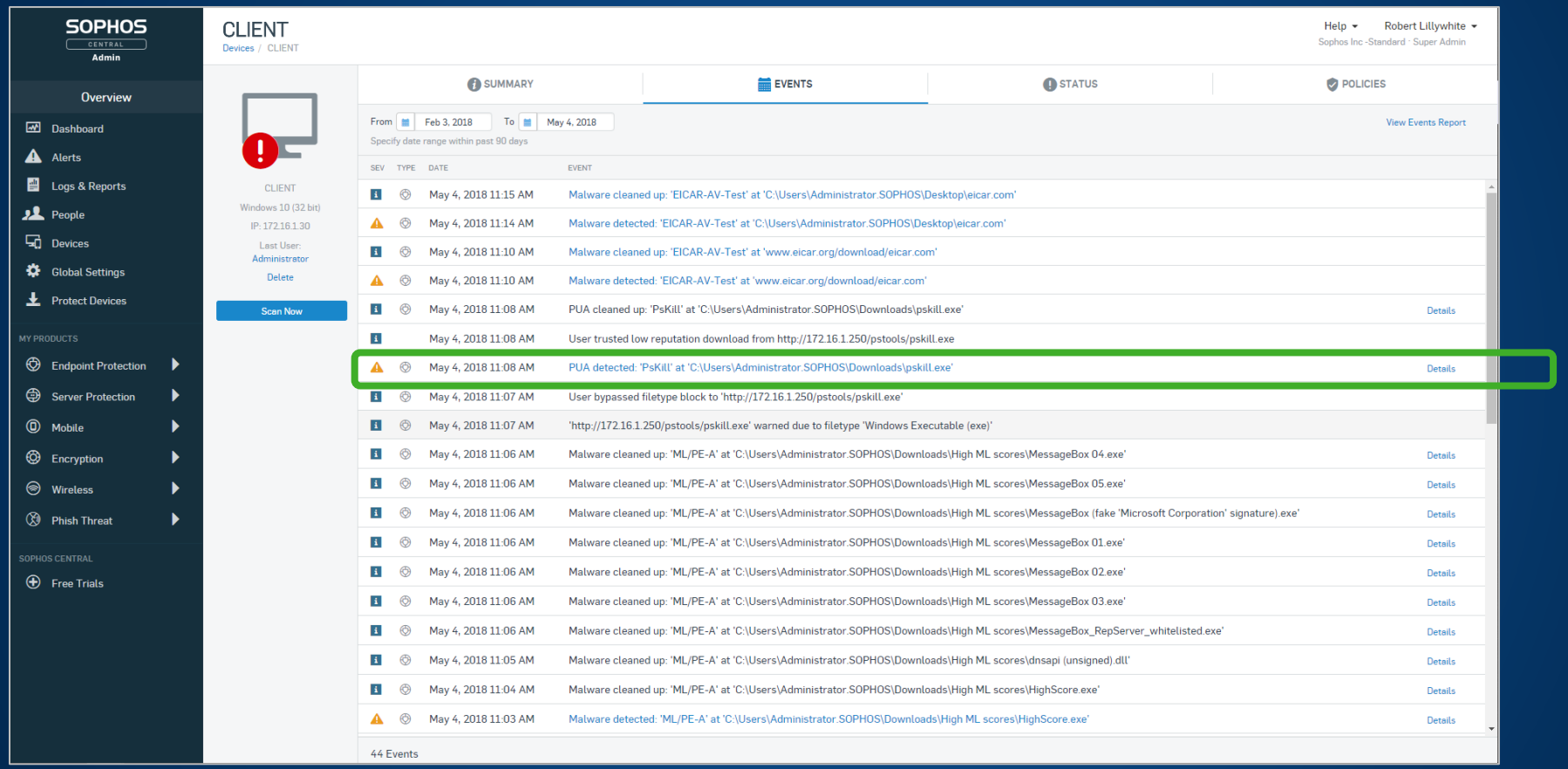
→ 例外を作成する

誤検知
例：カスタム内部アプリケーション

→ KB-000037167

管理画面経由で SafeStore から PE ファイルのみを復元できる

SafeStore からファイルを復元する



https://docs.sophos.com/central/customer/help/ja-jp/PeopleAndDevices/Devices/FindOutSHA-256Hash/index.html

SafeStore からファイルを復元する

- SHA256
- パス
- 証明書 (利用可能な場合)

ファイルの SHA 256 ハッシュ

アプリケーションの種類を使用規模で分類する

SafeStore からファイルを復元する

```
2018-05-04T06:54:50.088Z Command: restorethreat
2018-05-04T06:54:50.088Z GetContext context: 0073B018
2018-05-04T06:54:50.088Z Task: "restorethreat" (component 16)
2018-05-04T06:54:50.088Z 1 objects belonging to threat_id a3dd2872-4a5a-42ac-88e4-f198af8d804d
2018-05-04T06:54:50.776Z 1 objects restored
2018-05-04T06:54:50.791Z Restored: C:\Users\Administrator.SOPHOS\Downloads\pskill.exe
2018-05-04T06:54:50.791Z Task successful (time spent: 692ms)
```

ファイルは元の場所にのみ復元可能

制限事項

50 MB — SafeStore が保持できるファイルのサイズは 50 MB 以下です

1 GB — SafeStore が使用するディスク容量は 1 GB 以下です

200 ファイル — SafeStore が保持できるのは200ファイルまでです

注:

- 制限に達すると、古いアイテムから削除されます
- 一部のデータが損失する可能性があります

EDR/XDRについて

SOPHOS

EDR/XDRの利用について

- フェーズ１：事象発生端末の確認と対応
  - Intercept X Advanced
  - Intercept X Advanced for Server

検知した内容を確認

- フェーズ２：組織内の他の端末への影響確認と対応
  - Intercept X Advanced with XDR
  - Intercept X Advanced for Server with XDR

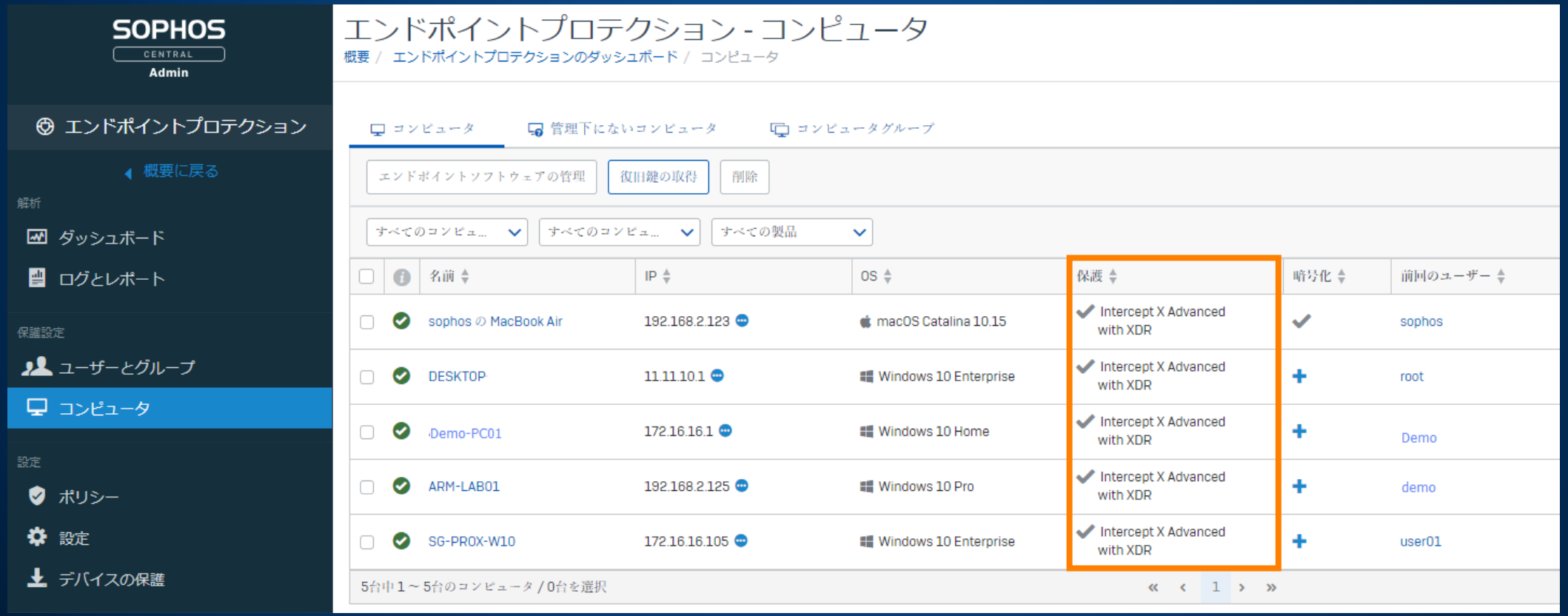
他の端末は大丈夫なのか
脅威は完全に除去したのか

- フェーズ３：プロアクティブな調査（ハンティング）
  - Intercept X Advanced with XDR （Live Discover/Live Response）
  - Intercept X Advanced for Server with XDR （Live Discover/Live Response）
  - Sophos Managed Threat Response

今、侵入されていないか

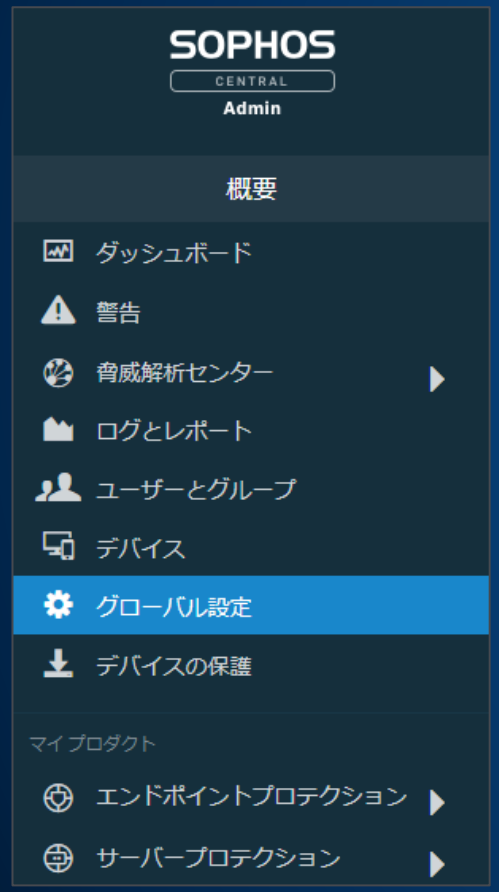
Sophos EDR/XDR利用方法①

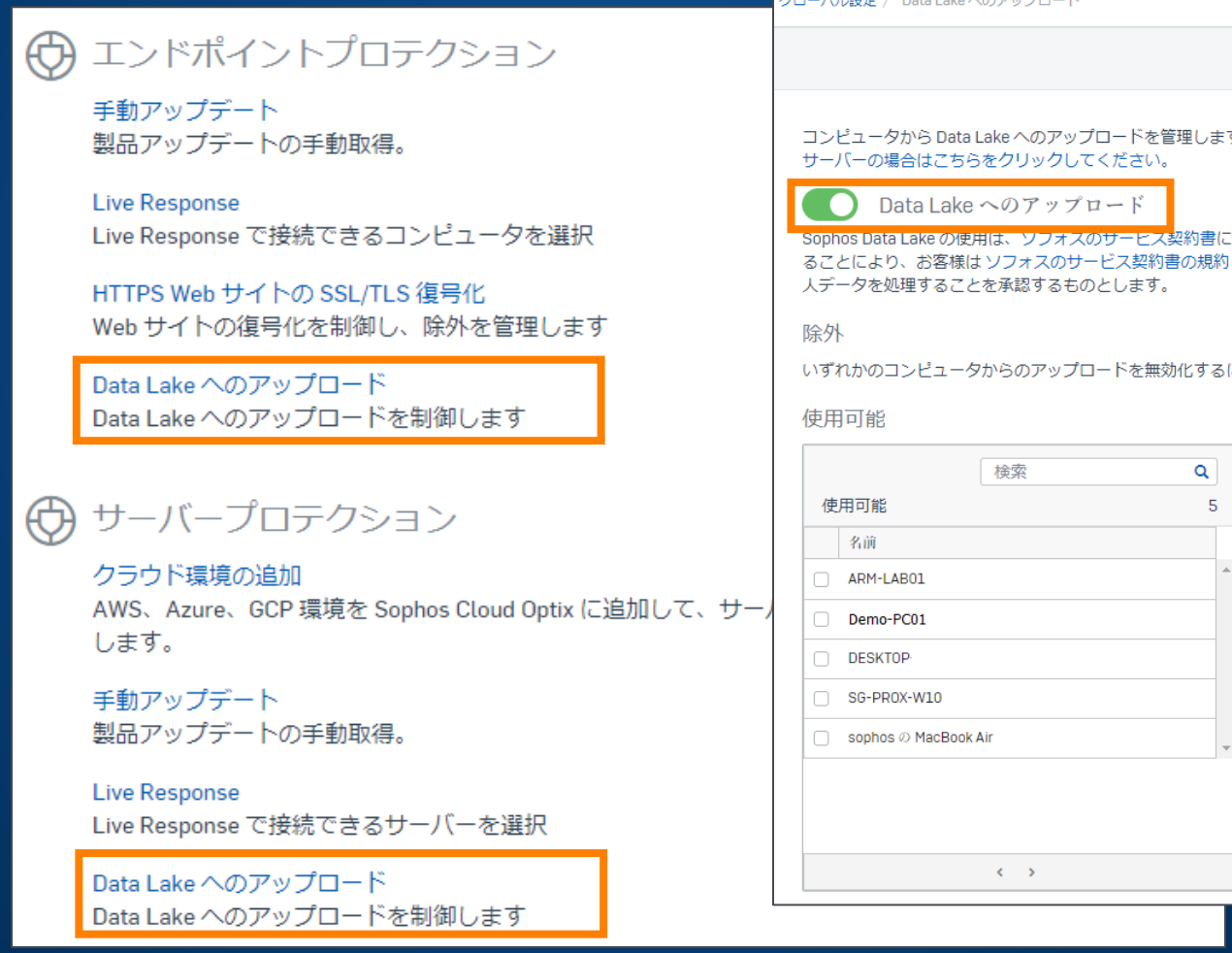
Intercept X Advanced with XDRライセンスをお持ちの場合はXDR機能を利用することができます



Sophos EDR/XDR利用方法②

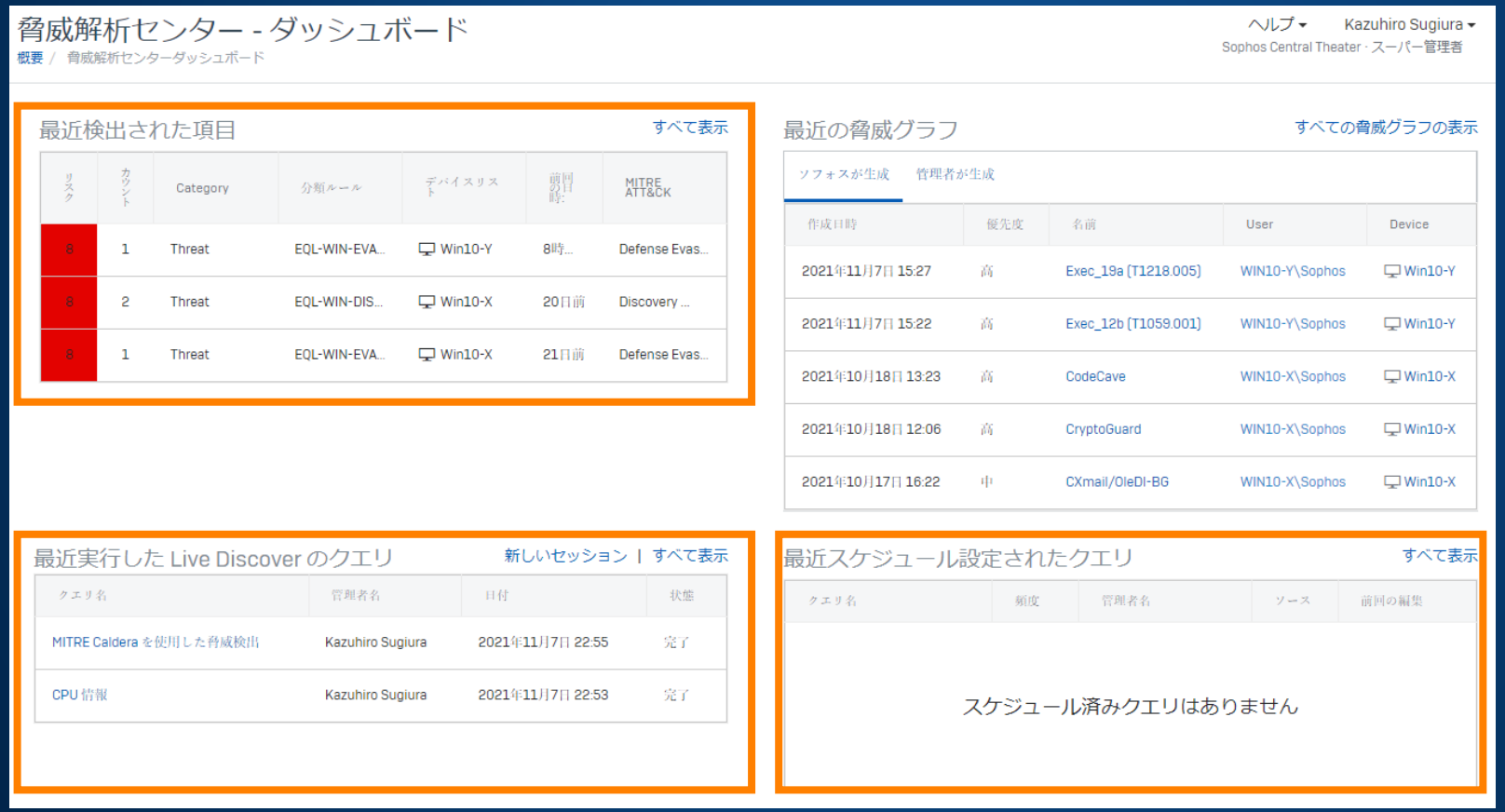
「Data Lakeのアップロード」を有効にすることでXDR機能が利用できます





脅威解析センター

XDRライセンスをお持ちの場合、脅威解析センターに4つの表が表示されます
XDRで検知したものは左上の表に表示されます



“検出”画面について①

- Data Lakeに上がったログから脅威を検出します
  - リスクを10段階で表示し、影響度が高いものほど数字が大きくなります
  - リスク7以上の内容がデフォルトで表示されます

“検出”画面について②


表示対象を選択
MITER ATT&CKマトリクス内の戦術と技術
フィルタ
リスクレベル
0 - 未定
1 - 最低
2 - 低
3 - 低
4 - 中
5 - 中
6 - 中
7 - 中
8 - 高
9 - 高
10 - 最大
分類ルール
種類
MITRE ATT&CK
種類
すべてクリア
適用
リスク
カウント
Category
分類ルール
デバイスリスト
初回表示
最終表示
説明
MITRE ATT&CK
8
1
Threat
EQL-WIN-EVA-PRC-MSHTA-HTTP
Win10-Y
-
2021年11月7日 15:23:25
This detection looks for MSHTA connecting to a URL. This is a living off the land technique for...
Defense Evasion
Mshta
検出日時: 2021年11月7日 15:23:25
デバイス: Win10-Y
種類: computer
IPv4 アドレス: 11.11.10.102
ジオ位置情報: Kobe, Hyōgo, Japan
OS: Microsoft Windows 10 Ente...
ログインしているユーザー: Sophos
端末情報
プロセス: mshta.exe
パス: C:\Windows\SysWOW64\mshta.exe
プロセスの所有者: Sophos
署名者情報:
SophosPID: 7876:132807395086693389
ML スコア: -1
グローバルレピュテーション: -1
ローカルレピュテーション: -1
SophosLabs Intelix 脅威スコア: 98
親プロセス: WINWORD.EXE
C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
親 SophosPID: 4900:132807394938020480
検知対象の情報
コマンドライン:
mshta http://www.netfliix.com/Launcher.hta
入力されたコマンド
8
2
Threat
EQL-WIN-DIS-PRC-NLTEST-DOM...
Win10-X
2021年10月18日 10:50:01
2021年10月18日 13:25:30
Nltest is a command line utility that can be used by threat actors during discovery. This rule looks for the fla...
Discovery
Domain Trust Discovery

補足：MITER ATT&CKのフレームワーク

https://attack.mitre.org/

Tactics（戦術）

Technics（技術）

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Clear Command History	Credentials from Web Browsers	File and Directory Discovery	Internal Spearphishing	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	Code Signing	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Compile After Delivery	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Supply Chain Compromise	Execution through Module Load	Bootkit	Elevated Execution with Prompt	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery
Trusted Relationship	Exploitation for Client Execution	Browser Extensions	Emond	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Input Capture	Fallback Channels		Network Denial of Service
Valid Accounts	Graphical User Interface	Change Default File Association	Exploitation for Privilege Escalation	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Man in the Browser	Multi-hop Proxy		Resource Hijacking
	InstallUtil	Component Firmware	Extra Window Memory Injection	Connection Proxy	Input Prompt	Process Discovery	Replication Through Removable Media	Screen Capture	Multi-Stage Channels		Runtime Data Manipulation
	Launchctl	Component Object Model Hijacking	File System Permissions Weakness	Control Panel Items	Kerberoasting	Query Registry	Shared Webroot	Video Capture	Multiband Communication		Service Stop
	Local Job Scheduling	Create Account	Hooking	DCShadow	Keychain	Remote System Discovery	SSH Hijacking		Multilayer Encryption		Stored Data Manipulation
	LSASS Driver	DLL Search Order Hijacking	Image File Execution Options Injection	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Security Software Discovery	Taint Shared Content		Port Knocking		System Shutdown/Reboot
	Mshta	Dylib Hijacking	Launch Daemon	Disabling Security Tools	Network Sniffing	Software Discovery	Third-party Software		Remote Access Tools		Transmitted Data Manipulation
	PowerShell	Emond	New Service	DLL Search Order Hijacking	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote File Copy		
	Regsvcs/Regasm	External Remote Services	Parent PID Spoofing	DLL Side-Loading	Private Keys	System Network Configuration Discovery	Windows Remote Management		Standard Application Layer Protocol		
	Regsvr32	File System Permissions Weakness	Path Interception	Execution Guardrails	Securityd Memory	System Network Connections Discovery			Standard Cryptographic Protocol		
	Rundll32	Hidden Files and Directories	Plist Modification	Exploitation for Defense Evasion	Steal Web Session Cookie	System Owner/User Discovery			Standard Non-Application Layer Protocol		

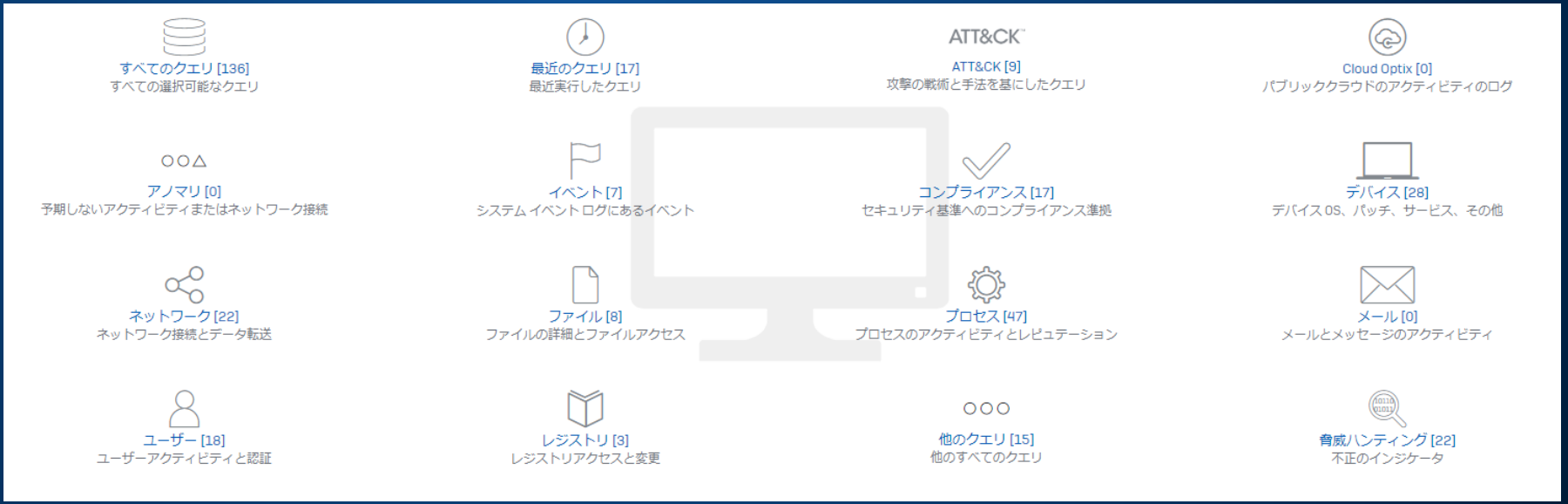
Live Discover

SOPHOS

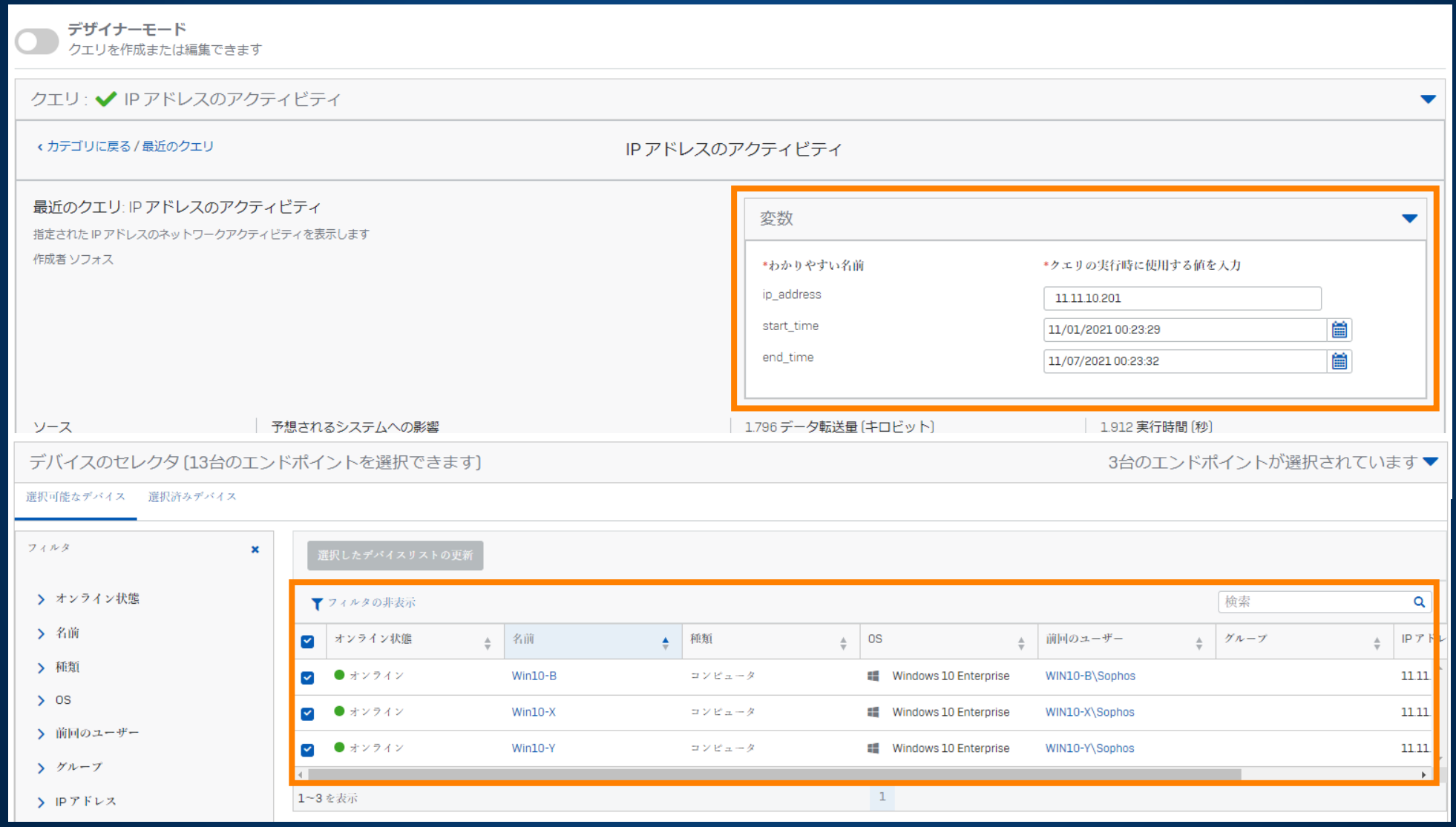
Live Discover①

- 豊富な探査機能
  - IT インサイト
  - 脅威ハンティング
  - マルウェア以外の脅威
- SQL クエリによる詳細な情報の入手
  - 事前設定されたクエリ
  - カスタムクエリ
  - Data Lakeクエリ

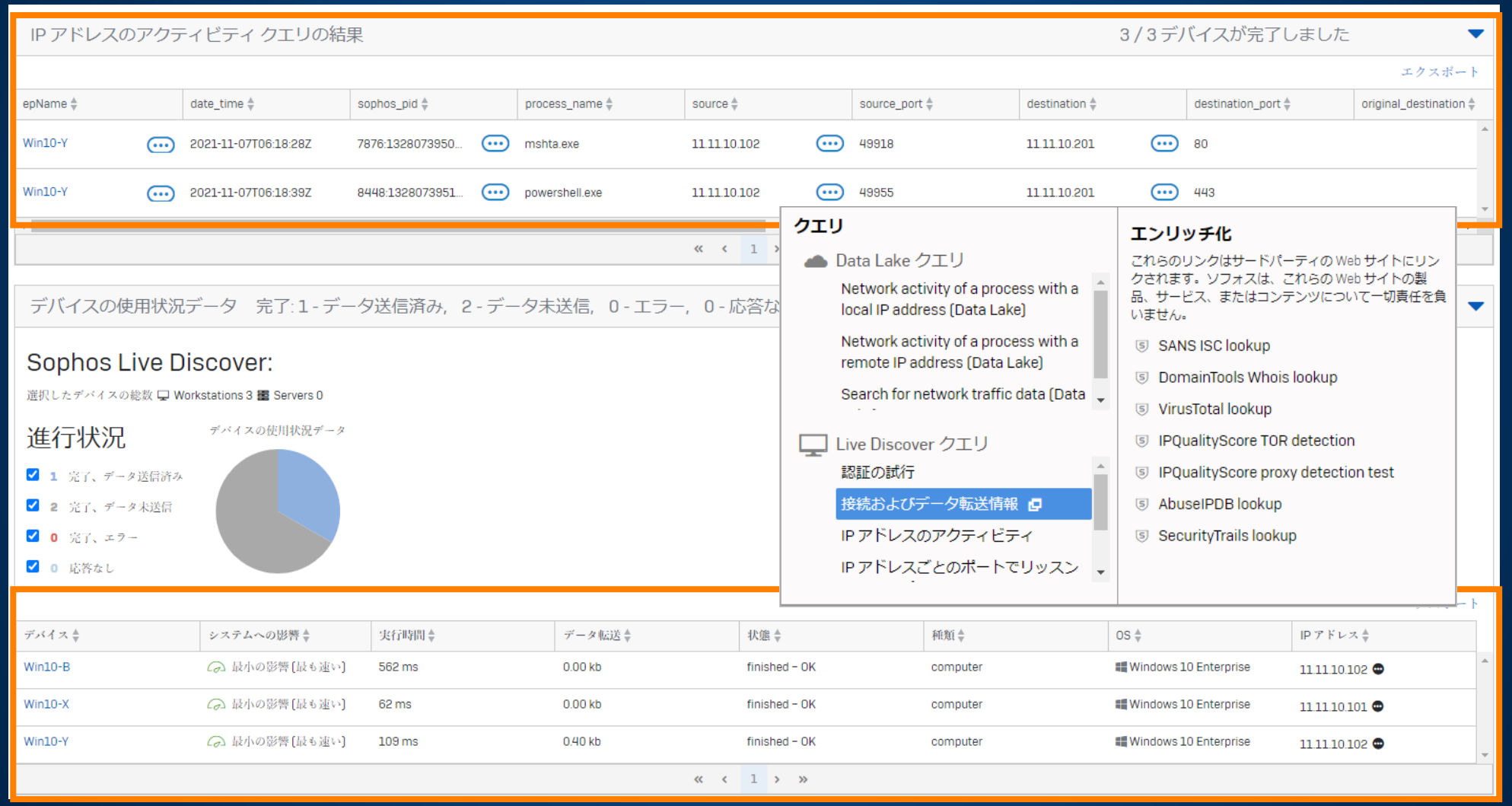
- クラウドホストでの30日間、ディスク上で最大 90 日間の保存されたデータから調査
- Windows/Linux/Mac



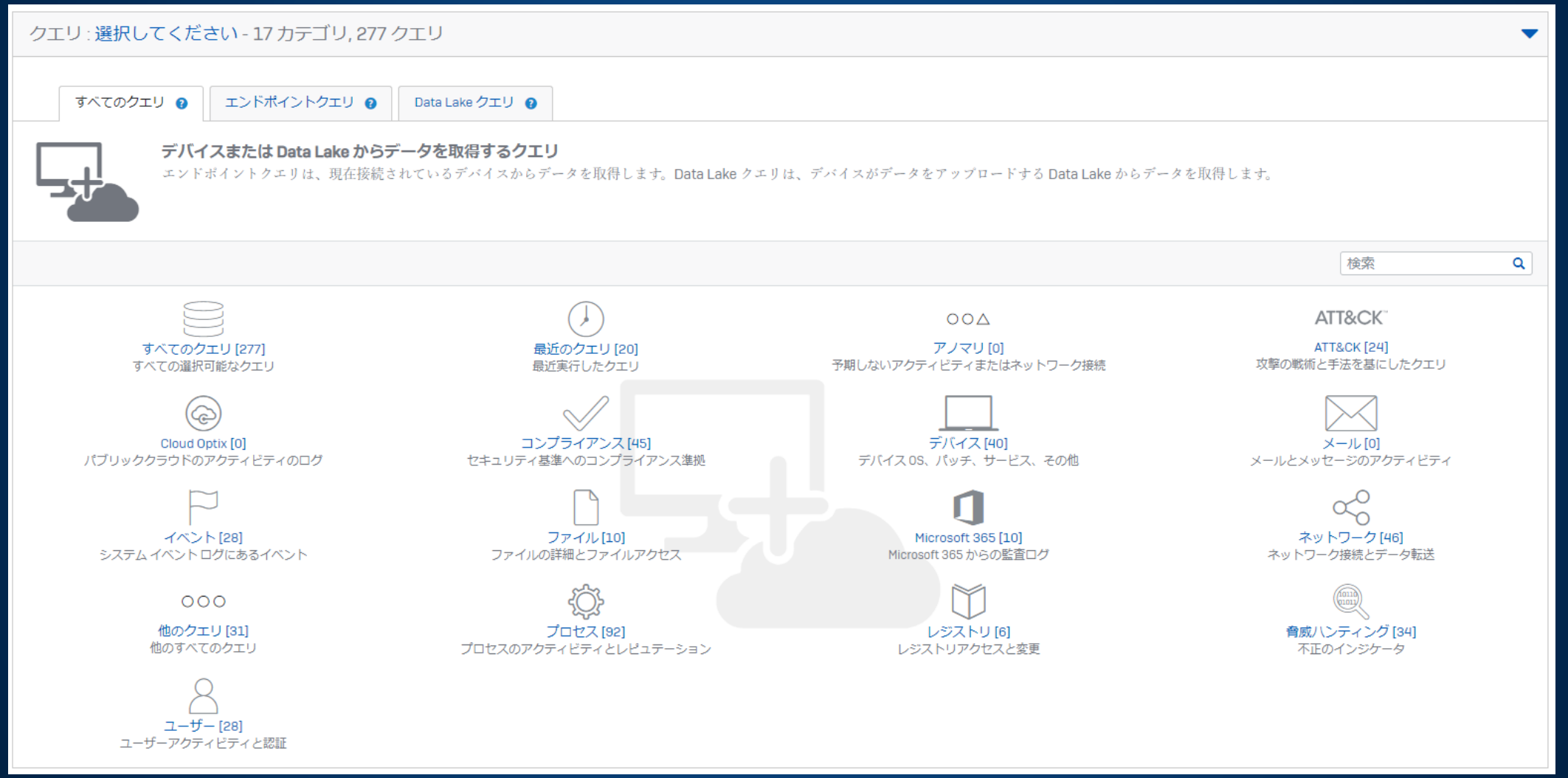
Live Discover②



Live Discover③



すぐに利用可能なクエリテンプレート

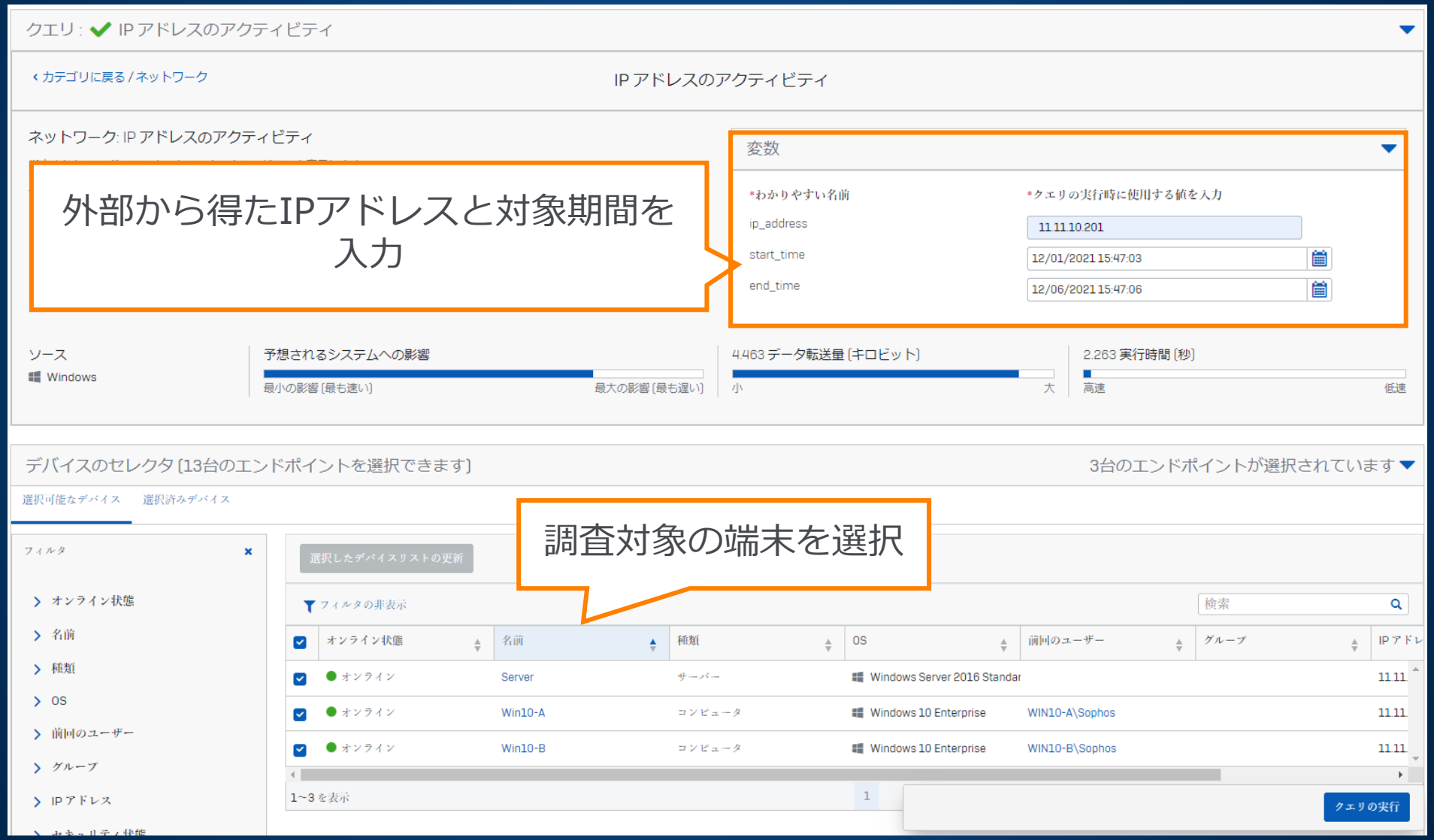


Live Discover利用例

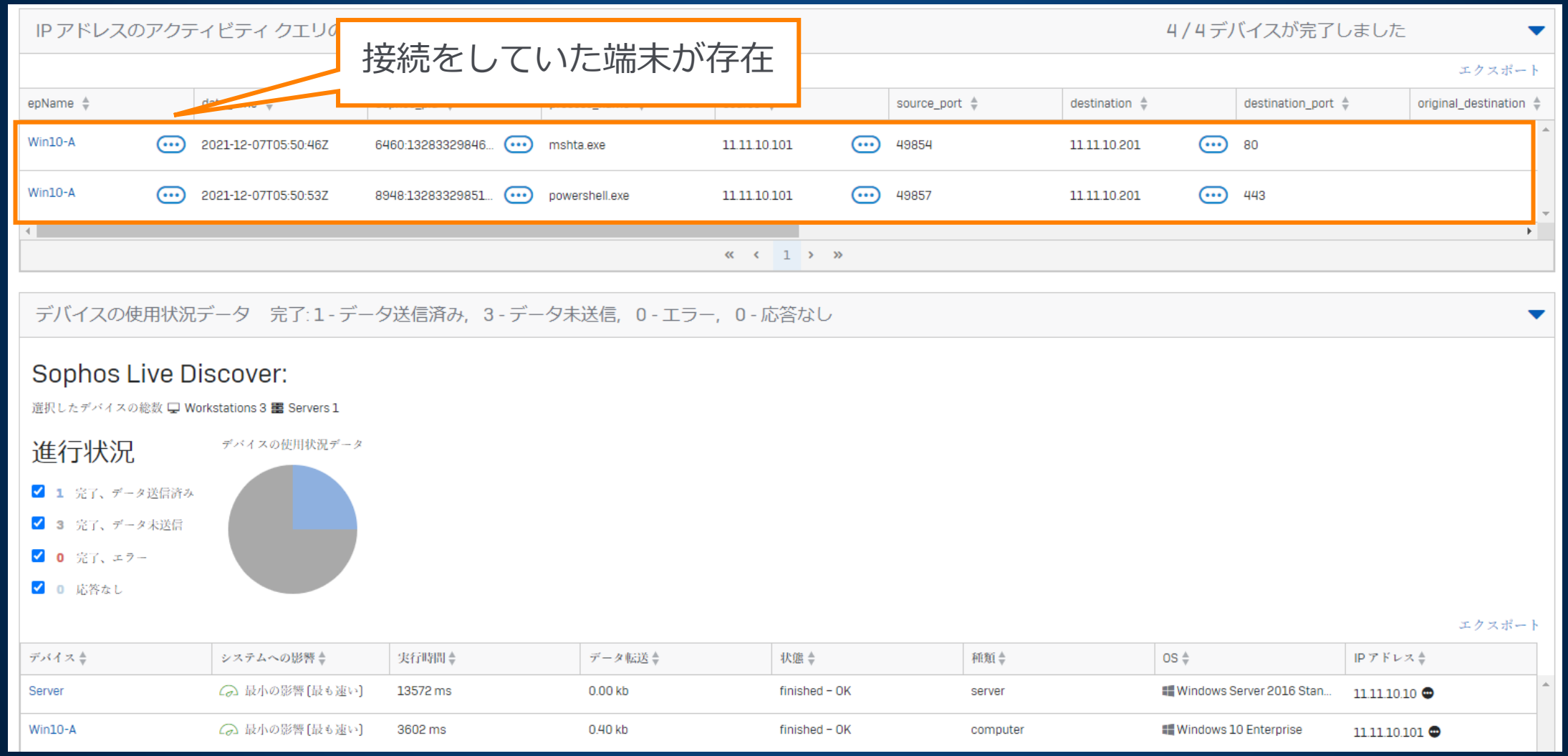
きっかけ

他社がサイバー攻撃に遭ったことが報告された。被害に遭った場合、接続するC&Cサーバーのアドレスが公開されたため、「うちは大丈夫か？」と経営者から調査を指示された

Live Discover利用例（クエリの実行）

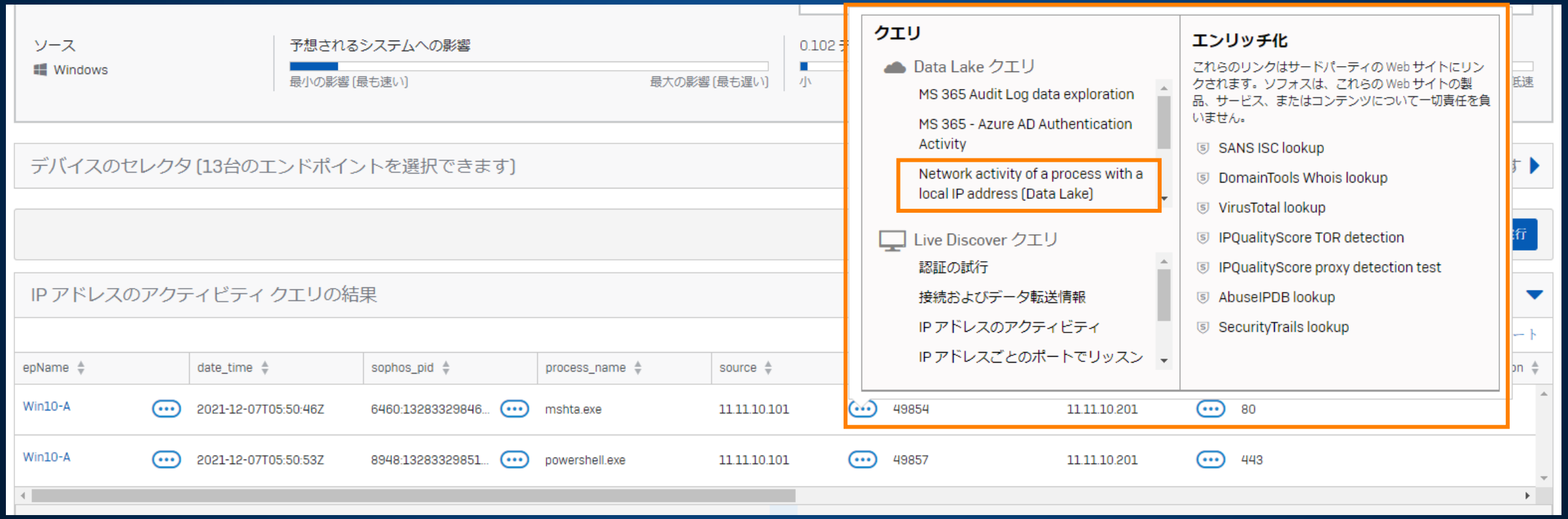


Live Discover利用例（実行結果）

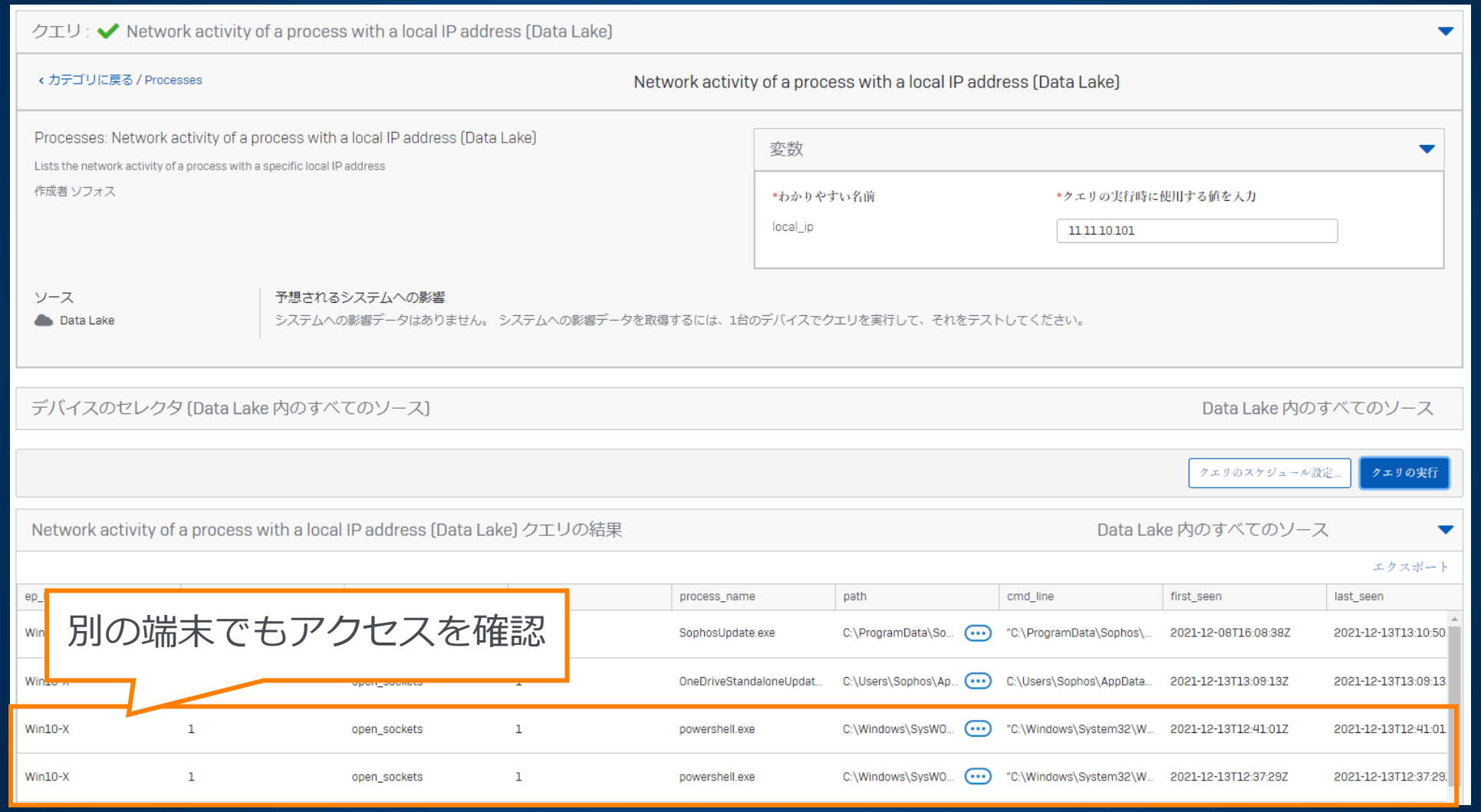


影響範囲の確認

オフラインの端末を含め、同一のIPアドレスにアクセスした端末がないかData Lakeに保存されているログから確認し、影響範囲を確認します



影響範囲の確認



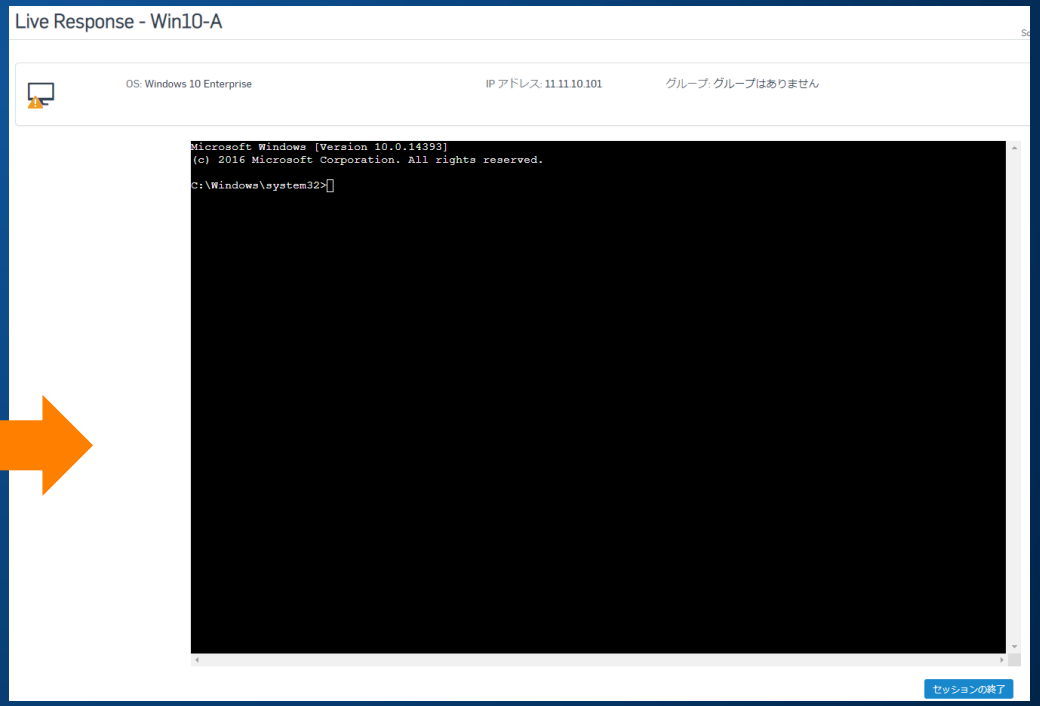
ep_				process_name	path	cmd_line	first_seen	last_seen
Win				SophosUpdate.exe	C:\ProgramData\So...	"C:\ProgramData\Sophos\...	2021-12-08T16:08:38Z	2021-12-13T13:10:50
Win10-X			1	OneDriveStandaloneUpdat...	C:\Users\Sophos\Ap...	C:\Users\Sophos\AppData...	2021-12-13T13:09:13Z	2021-12-13T13:09:13
Win10-X	1	open_sockets	1	powershell.exe	C:\Windows\SysWO...	"C:\Windows\System32\W...	2021-12-13T12:41:01Z	2021-12-13T12:41:01
Win10-X	1	open_sockets	1	powershell.exe	C:\Windows\SysWO...	"C:\Windows\System32\W...	2021-12-13T12:37:29Z	2021-12-13T12:37:29

封じ込め～根絶：端末の隔離～脅威の除去

デバイス画面に移動し、デバイスの隔離を行います

これにより、被害の最小化を行い、また詳細な調査を行うことが可能となります

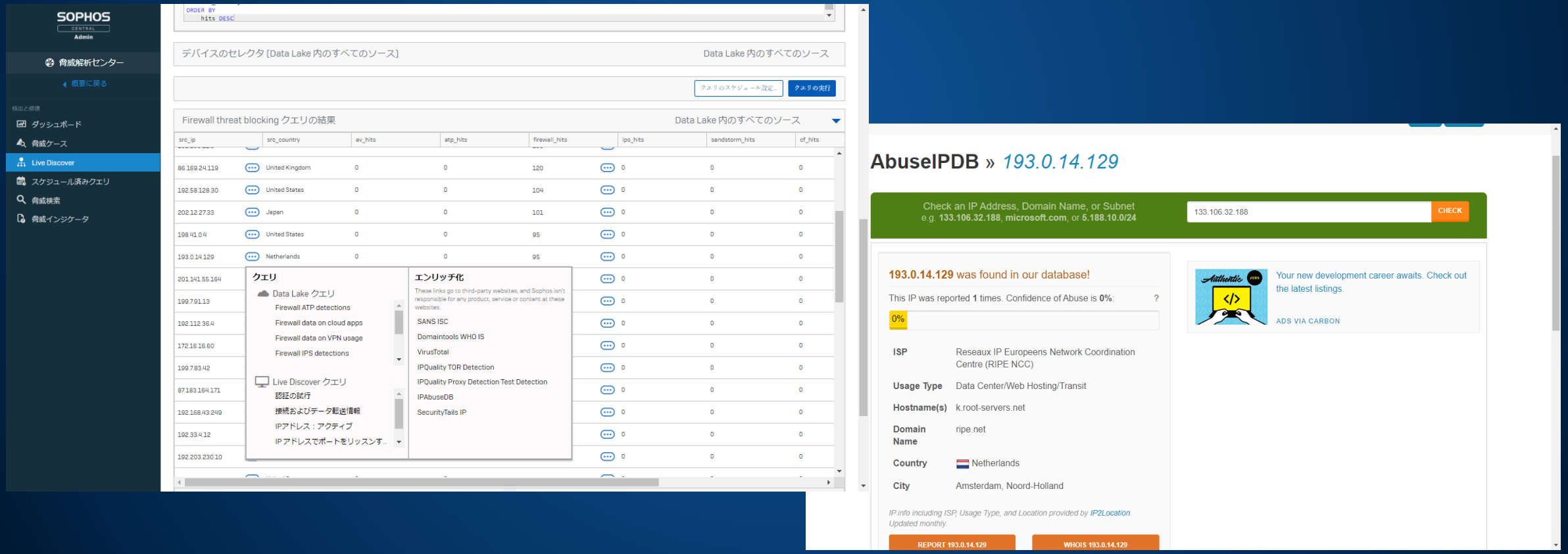
その上で、Live Responseを使って脅威の除去を行います



ピボット(クエリで得られた結果から次の調査継続)

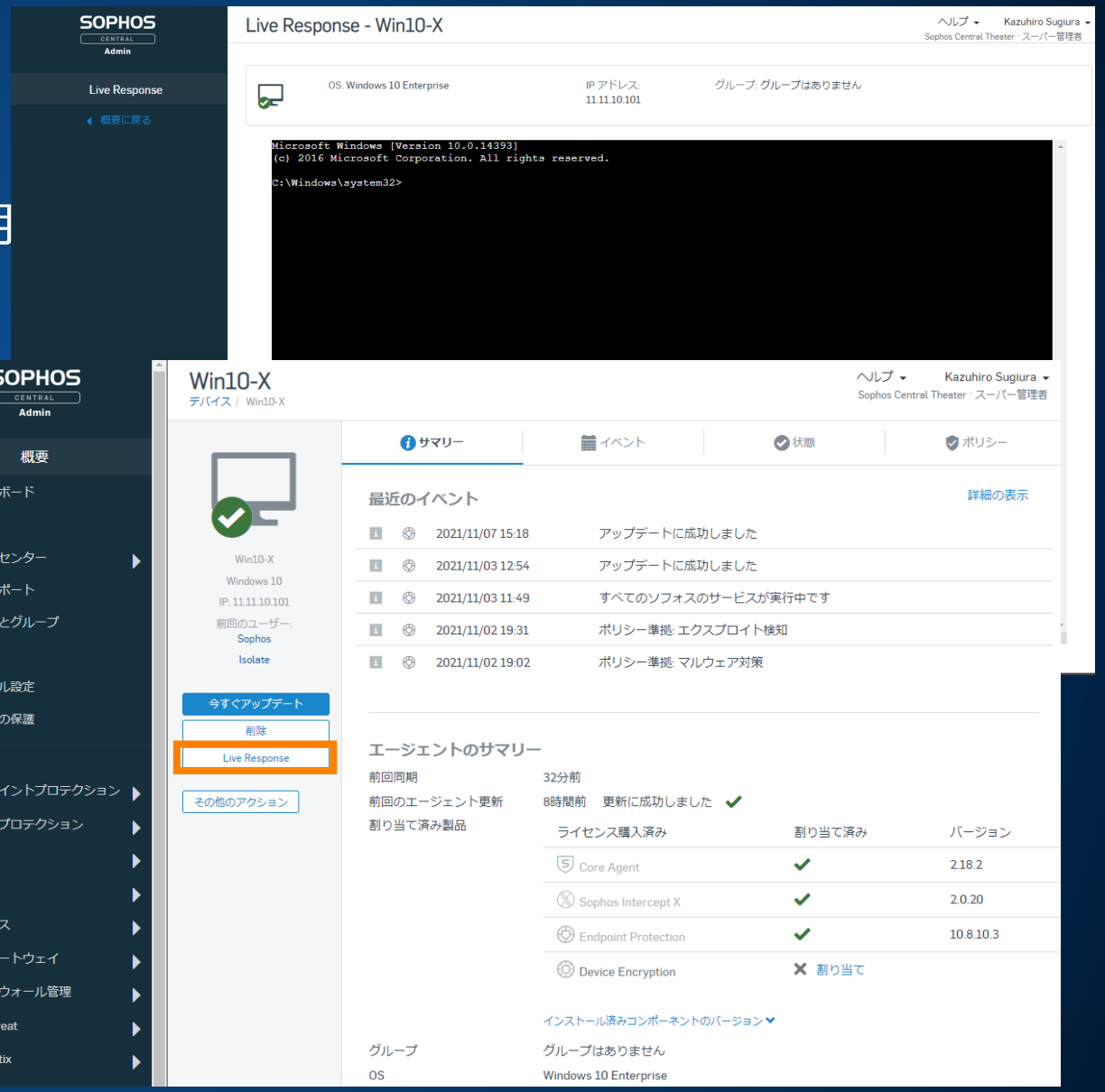
EDR/XDRを利用した調査では、クエリで得られた結果から次の仮説を立て、継続調査を行います

調査の過程で、外部ソースを利用した確認を行う場合は「エンリッチ化」の中にある外部リソースを選択して調査をすることができます



Live Response

- コマンドラインインターフェースを使用して管理対象デバイスをリモート修正する際に利用します
  - デバイスの再起動
  - アクティブプロセスの終了
  - スクリプトまたはプログラムの実行
  - 構成ファイルの編集
  - ソフトウェアのインストール/アンインストール
  - フォレンジックツールの実行
- Windows/Mac/Linux対応
- 多要素認証が必須



ログについて

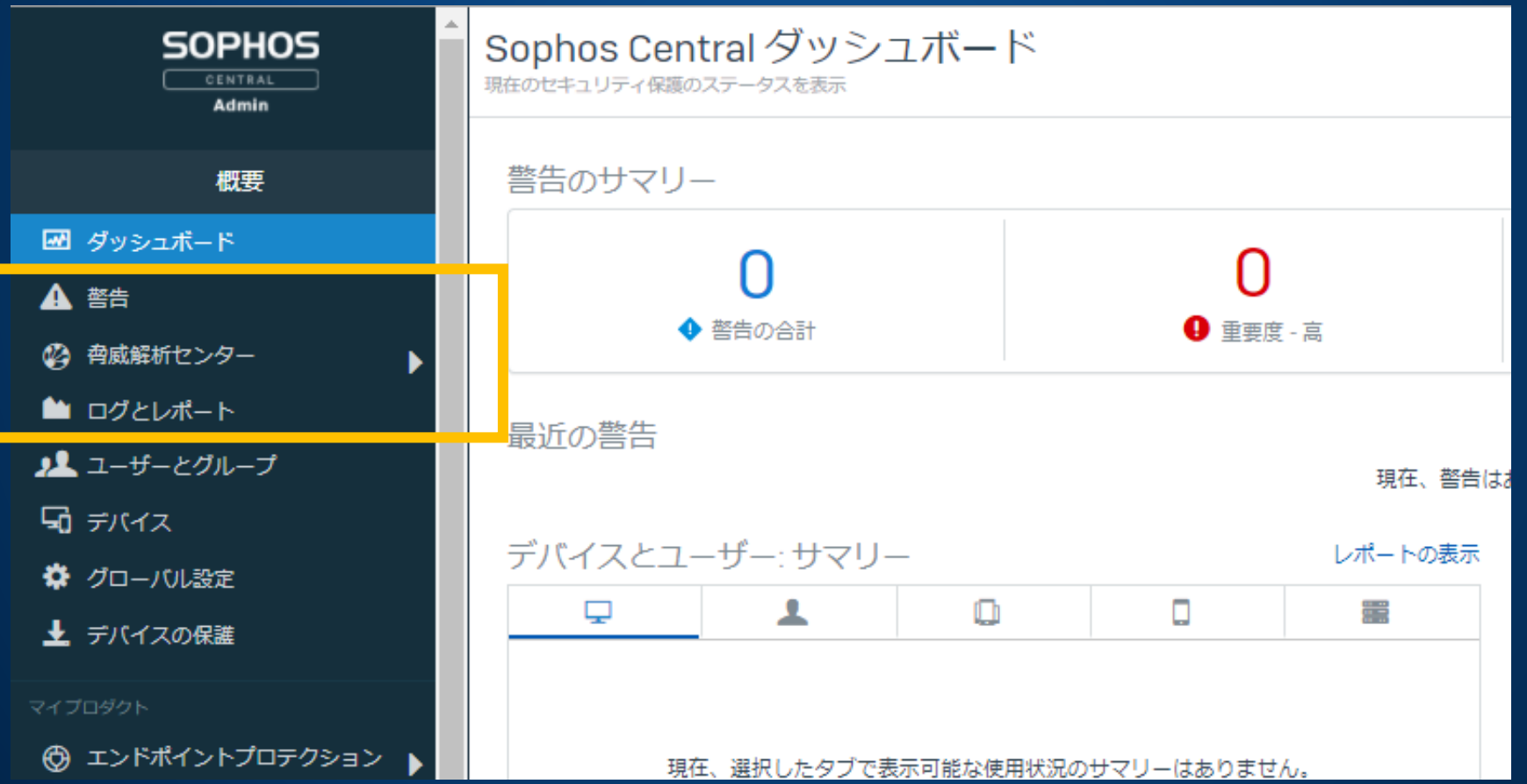
SOPHOS

管理コンソール表示、通知機能に期待されていること

- 端末全体の健康状態を把握したい
- 特定の端末の状態推移を確認したい
- 端末ではなく、ユーザー単位で状態を知りたい
- マルウェアの検知イベントがあれば、すべて把握したい
- マルウェア検知の月次件数、推移を把握したい
- 重要な情報は直ちに通知が欲しい
- 特定のマルウェア検知の詳しい情報を知りたい
- レポートが欲しい
- メール通知機能が欲しい
- EDRのログを見たい
- ログの保存期間を知りたい
- 外部システムへの通知連携がしたい

Central Admin管理画面

- 必要な情報は、主に、Central Adminダッシュボード画面左側のメニュー「警告」、「脅威解析センター」、「ログとレポート」にまとめられています。
- それ以外の場所の確認場所についても、適宜触れつつ紹介します。



ログ、イベント、警告、その他関連情報

SOPHOS

ログ、イベント、警告

- ログ
  製品が出力する様々な情報。あとから調査や確認を目的としたデータ。通常は確認する必要のない情報も含まれる。時系列で出力されるため、一連の流れが分かる。

- イベント
  特定の通知すべき内容を含んだ情報。状態変化や検知といった情報、警告に該当する情報が含まれる。

- 警告（アラート）
  管理者が知っておくべき内容を含んだ情報。対処が必要な情報も含まれる。

情報の多さ
ログ ＞ イベント ＞ 警告（アラート）

ログとは？ログの種類

- エンドポイント製品ログ
  エンドポイント製品インストールログ、インストール後のエンドポイント製品が出力するログは、端末側に保存されます。各コンポーネント毎に起動時、終了時、処理実行に関する情報が出力されます。また、マルウェア検知やサービス起動・停止といった情報については、イベントログにも出力されます。

  Sophos Central Endpoint: Thin インストーラログの詳細
  https://support.sophos.com/support/s/article/KB-000034888?language=ja

  Sophos Central Endpoint: Windows のログファイルに関する情報
  https://support.sophos.com/support/s/article/KB-000038787?language=ja

  これらのログに加えて様々なシステム情報は、SDU (Sophos Diagnostics Utility) で収集することが可能です。
- Central側のログ
  Sophos CentralはSaaS型の管理コンソールとなります。Central Adminへのログインや、Central Admin上で行った各種管理タスクを記録する監査ログが提供されます。

  Sophos Central Admin ヘルプ [監査ログ]
  https://docs.sophos.com/central/customer/help/ja-jp/ManageYourProducts/LogsReports/Logs/AuditLogs/index.html

EDRに関するデータ（ログではない）

- プロセスジャーナル（Windowsのみ）
  Intercept X Advanced (EDRなし)であっても、ローカルディスクにすべてのプロセスのアクティビティを90日間記録します。このデータを元に、マルウェア検知時の「脅威ケース」の生成を行います。
  XDRライセンスがある場合(評価ライセンス含む）、「Live Discover」機能でCentral AdminからOSQueryを通じて、オンライン端末に対してアクセス可能です。
  また、JSONファイル、SQLite形式への変換、AWS S3 bucketへのアップロードも可能です。

  Sophos Intercept X Advanced with EDR: フォレンジック スナップショットに関するヘルプ
  https://support.sophos.com/support/s/article/KB-000038358?language=ja

  Live Discoverでオンライン端末上に対してアクセス可能なジャーナルのスキーマ
  https://docs.sophos.com/central/References/LiveDiscoverSchema.html

- Data Lake(Windows / Linux / Mac)
  クラウド上のData Lakeには、定期的にOSQueryによって脅威検索、脅威ハンティングに必要な情報がアップロードされ、30日間保存されます。Data Lakeに収集されたデータは「Live Discover」機能でCentral AdminからOSQueryを通じて、アクセスが可能です。このとき、端末はオンラインである必要はありません。Data Lakeへのアップロードは既定は無効です。有効にして初めてアップロードが開始されます。

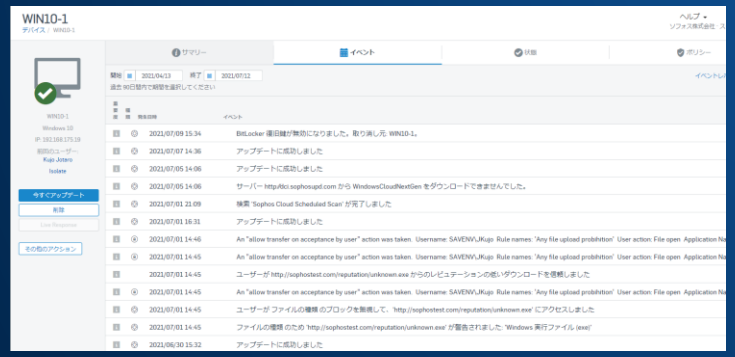
  Sophos Central Admin ヘルプ [Data Lakeクエリ]
  https://docs.sophos.com/central/customer/help/ja-jp/ManageYourProducts/Overview/ThreatAnalysisCenter/LiveDiscover/DataLakeQueries/index.html
  Sophos Central Admin ヘルプ [Data Lake へのアップロード]
  https://docs.sophos.com/central/customer/help/ja-jp/ManageYourProducts/Overview/ThreatAnalysisCenter/LiveDiscover/DataLakeUploads/index.html

イベント

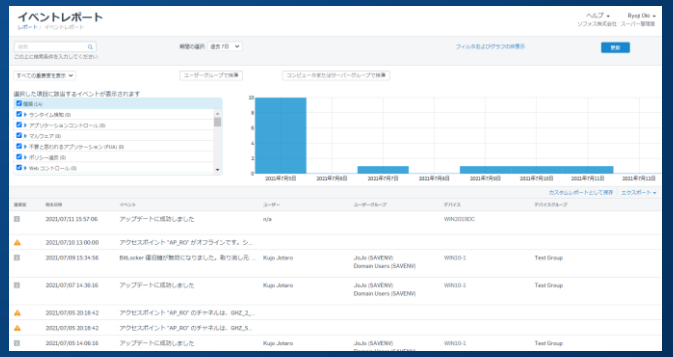
- Central上のイベント
  エンドポイント保護製品の状態変化、検知、Central上での出来事がイベントとして記録されます。
  エンドポイント製品を含むすべてのイベント情報の種類は、以下の技術文書に記載されています。

  Central Admin: Sophos Central API に対するイベントの種類と説明
  https://support.sophos.com/support/s/article/KB-000038309?language=ja

- エンドポイントに関するイベント
  特定のエンドポイントに関するイベントは、個々の端末から確認することが可能です。
  管理対象のエンドポイント全体のイベントは、レポート > イベントレポートより確認することが可能です。



個々の端末上でのイベント確認



レポート > イベントレポートでの
端末全体のイベント確認

警告（アラート）

- 警告（アラート）の特徴

✓ 警告＝アラート(英語)です。管理者への注意喚起を目的とした機能となっています(例：マルウェアの検知のすべてが警告とはなりません）。

✓ 同一の警告はグループ化されて表示されるため見やすく、対処がしやすくなっています。グループ化の解除も可能です。

✓ 重要度に応じて、「高」、「中」、「低」に分けられます。

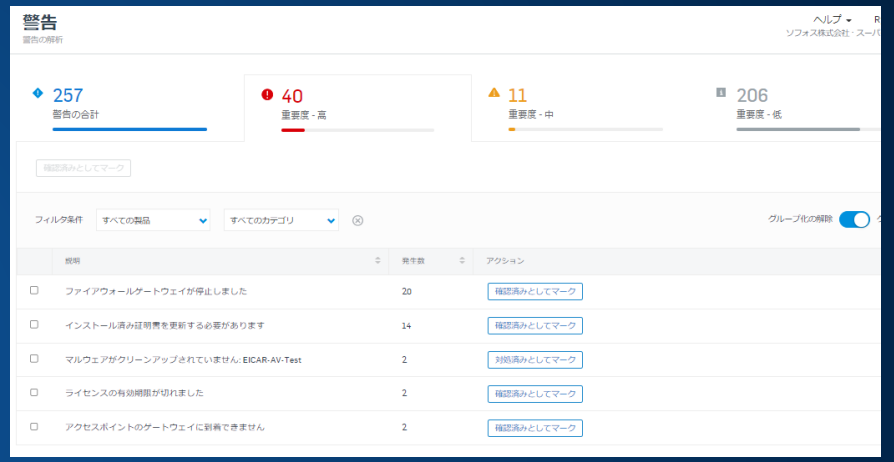
✓ 警告の中には、対処すべき内容が自己修復して自動的に削除されるものがあります。

✓ 管理者の対処が必要な警告（例：ランサムウェア検知）には、対処を行うためのリンク、または確認したことを返答する機能が備わっています。これらを行わない限り、警告がCentral Adminの画面上に表示し続けられます。

Sophos Central Admin: 警告ページと警告設定のページ
https://support.sophos.com/support/s/article/KB-000038133?language=ja

Sophos Central Admin ヘルプ [警告]
https://docs.sophos.com/central/customer/help/ja-jp/ManageYourProducts/Overview/Alerts/index.html

警告画面



警告に対するアクション画面

警告メールの送信

警告メールの特徴

- ✓ メール通知される警告は、「中」以上で管理者の対処を必要としているもののみが対象となります。タイミングは即時です(一部除く、例：ポリシー違反状態の場合150分後)。
- ✓ メール通知される警告は、重要度、製品、頻度といったカスタマイズが可能です。宛先も追加可能です(Central Admin管理者である必要はありません。パートナー様のメールアドレスでも可）。評価ライセンスでは配布リストの編集ができません。
- ✓ 同じ種類の警告が既にメール送信されている場合は、24時間経過しないと、新たに送信されません。これは多数のメール送信によって情報が埋没してしまうことを避けるためです。ただし、メール警告の設定変更で頻度を「毎日」から「今すぐ」に変更することで、同じ内容の警告でもメールを受け取ることが可能になります。
- ✓ あくまで「警告」に関するメール通知であるため、“マルウェア検知イベントすべて”を通知といったことはできません。

メール警告の設定画面

Sophos Central Admin: 警告ページと設定に関するよくある質問 (FAQ)
https://support.sophos.com/support/s/article/KB-000038134?language=ja

Sophos Central Admin ヘルプ [メール警告の設定]
https://docs.sophos.com/central/customer/help/ja-jp/ManageYourProducts/Overview/GlobalSettings/AlertEmailSettings/index.html

脅威グラフ

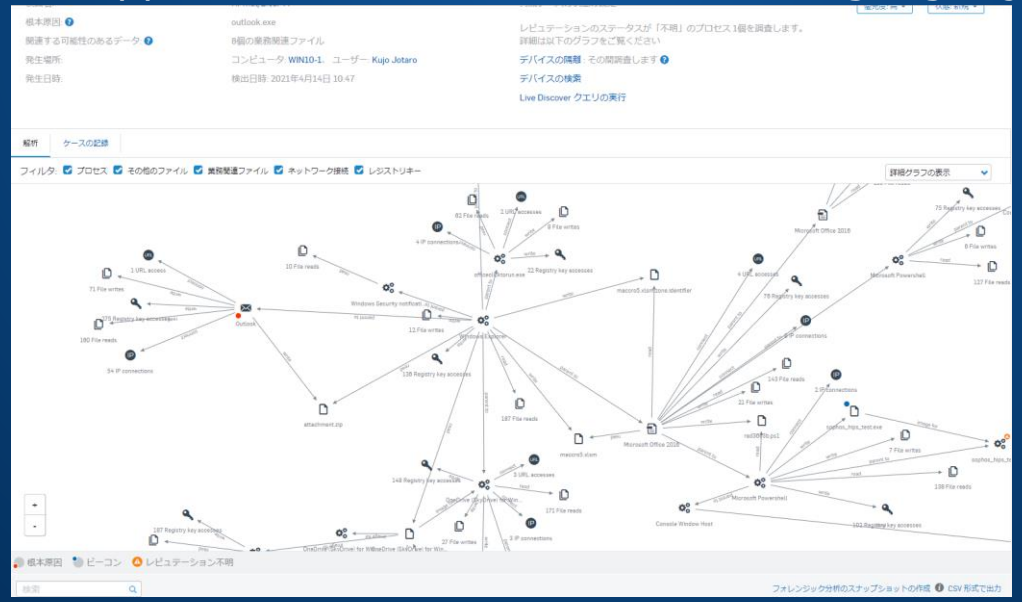
- 脅威インシデントの可視化、マルウェアの振舞いおよび影響の分析ツール

✓マルウェア検知時に（または管理者起点で）生成される脅威インシデントの可視化機能

✓EDRの機能なしでもマルウェア検知時の特定条件下（悪意のある検出時）で生成されます

✓プロセスジャーナルを元に、どのようなファイル、レジストリ、IPアドレス、URLにアクセスしたのかが視覚的に把握できます

脅威グラフの例: マルウェアの検出
https://support.sophos.com/support/s/article/KB-000036359?language=ja



レポート

ログとレポート機能

- ✓ Sophos Centralに登録されているログ、イベントを一覧で時系列に表示します。
- ✓ サマリーレポート、監査ログ、イベント全般、マルウェア検知、その他セキュリティイベント情報が幅広く網羅されています
- ✓ 「警告」ではカバーされないような内容も把握したい場合に、有効な機能です
- ✓ 「警告」にならないマルウェア検知は、「イベント」から“ランタイム検知”、“マルウェア”（または“PUA”も）をフィルター選択するか、「ブロックされたマルウェア/不要と思われるアプリ」から確認が可能です。
- ✓ 「ブロックされたマルウェア/不要と思われるアプリ」では、脅威ケースが生成された検知イベントも確認可能です。

Sophos Central Admin ヘルプ [ログとレポート]
https://docs.sophos.com/central/customer/help/ja-jp/ManageYourProducts/Overview/LogsReports/index.html

レポートの保存・メール送信

ログとレポート機能

- ✓ 各種レポートを表示するだけでなく、PDF、 CSV形式でのエクスポート、メールでのスケジュール配信も可能です。
- ✓ レポートへのリンクまたは添付ファイル（PDF、CSV）の選択が可能
- ✓ カスタムレポートを作成しスケジュールすることで、特定の期間(エンドポイント製品導入フェーズ)の検知または過検知の把握、エグゼクティブサマリーの送信の自動化といったことが可能になります。
- ✓ 「警告」のメールと異なり、保存したレポートをメール送信する場合は、最大頻度が1日に1回となるので、即時性はありません。（頻繁にCentral Adminコンソールにログインアクセスするか、SIEM連携で取り込む頻度を増やすことによって解決）
- ✓ 設定されたスケジュールは6か月間のみ有効です

Sophos Central Admin: 「ログとレポート > サマリーレポート」
https://support.sophos.com/support/s/article/KB-000038693?language=ja

SDUログ

SOPHOS

SDU (Sophos Diagnostics Utility)

SDUとは？

- ✓ トラブルシューティング、状態調査等を目的としたログ、構成情報収集ツールです
- ✓ Windows、Mac、Linuxそれぞれでツールが用意されており、実行するとSophos エンドポイント保護製品の情報、システムの構成やログファイルをまとめて収集し、Zipファイルを生成します
- ✓ Windows、Mac向けにはSDUを手動ダウンロードして実行する方法と、Central Adminからリモートで実行する方法があります。Linuxは製品に組み込まれています

  Sophos Diagnostic Utility (SDU): ユーティリティを見つけてダウンロードする手順
  https://support.sophos.com/support/s/article/KB-000033500?language=ja

- Windows / MacでのSDU手動ダウンロード実行場面

- ✓ インストール時のトラブル。SDUが未インストールなため、スタンドアロン版の利用が必要です
- ✓ Central との管理通信トラブル時(Centralからの実行が不可なため)。エンドポイントのステータスが更新されない等の場面
- ✓ Windows / MacでのCentral Adminからの自動実行場面
  上記以外のトラブルに有効です。SDUログは自動的にSophosのストレージにアップロードされます

ログ/レポートの長期保存、外部連携

SOPHOS

ログ、その他データの保存期間

種類	保存期間
ローカル（製品ログ、イベントログ）	製品コンポーネントによって異なる
Central、イベント、監査ログを含むすべてのデータ	90日
プロセスジャーナル(Windows)	90日
XDR Data Lakeデータ	30日

製品のログ保存期間やローテーションについては、以下にて詳細をご確認ください
Sophos Central Endpoint: Windows のログファイルに関する情報
https://support.sophos.com/support/s/article/KB-000038787?language=ja

- ✓Data Lakeへのデータ保存はデータ量に関わらず、一律30日です(製品ライセンスに含まれます)
- ✓30日以上のデータ保存を目的としたData Lakeデータのアーカイブ機能は、近い将来の実装を予定しております

ログ、その他データの外部連携

組織が所属する業界標準のコンプライアンス要件によっては、データの保存期間が定められていることもあります。その場合、外部連携や外部出力機能を用いてアーカイブ保存を行うことが可能です。またSIEM等に情報を取り込んで、他の情報ソースと突き合わせて分析を行うといった目的にも使用ができます。

種類	格納場所	確認場所	メール通知	外部連携
ログ	端末側	各種製品ログ格納フォルダ	なし	端末側のEventログはログ監視ツール等で取得可能
	監査ログ	Central: ログとレポート	なし	PDF、CSVへの出力が可能
イベント	Central	Central:ログとレポート	レポート	SIEM連携可能
警告	Central	Central: 警告	警告メールとして送信	APIで取得可能
EDRデータ	端末、Data Lake	Central: 脅威解析センター > Live Discover	なし	APIで取得可能

イベントのSIEM連携については、以下のナレッジベースから詳細をご確認ください
Sophos Central API: 警告およびイベントデータを SIEM に送信する方法
https://support.sophos.com/support/s/article/KB-000036372?language=ja

SIEM連携以外のCentral API、XDRクエリAPI等は以下から詳細をご確認ください
https://developer.sophos.com/apis
https://developer.sophos.com/whatsnew

https://community.sophos.com/intercept-x-endpoint/edr-data-lake-eap/b/announcements/posts/api-guide---getting-started

SOPHOS

Cybersecurity evolved.