



サイバー攻撃 自動検知パック



1. サーバへの直接的なログオンチャレンジ
Server

レポートの初期設定値

項目	設定内容
EventID	4625
ユーザー	*\$:*を除外

チューニングのポイント

項目	設定内容
ユーザー	環境に応じて [アカウント] を除外
サーバ	環境に応じて [対象サーバ] を設定
ClientIP	対象外とするクライアントIPがあれば [除外する] に登録 (シス担当者など)

Tips

イベントID : 4625は、攻撃者が侵入しようとした対象の“ローカルコンピュータ”上に記録されます。

攻撃者がサーバへ直接ログオンしようとしていることが分かります。
 攻撃者がログオンしようとして失敗した場合、攻撃されたサーバでは「4625」というイベントIDが出力されます。
 4625は「ログオン失敗」を意味するログであるため、ログオン成功のログが出力されない限り、対象サーバへの侵入は成功していないと考えられます。

ログオン失敗

サーバへのローカル
ログオンチャレンジ

admin

ID:4625

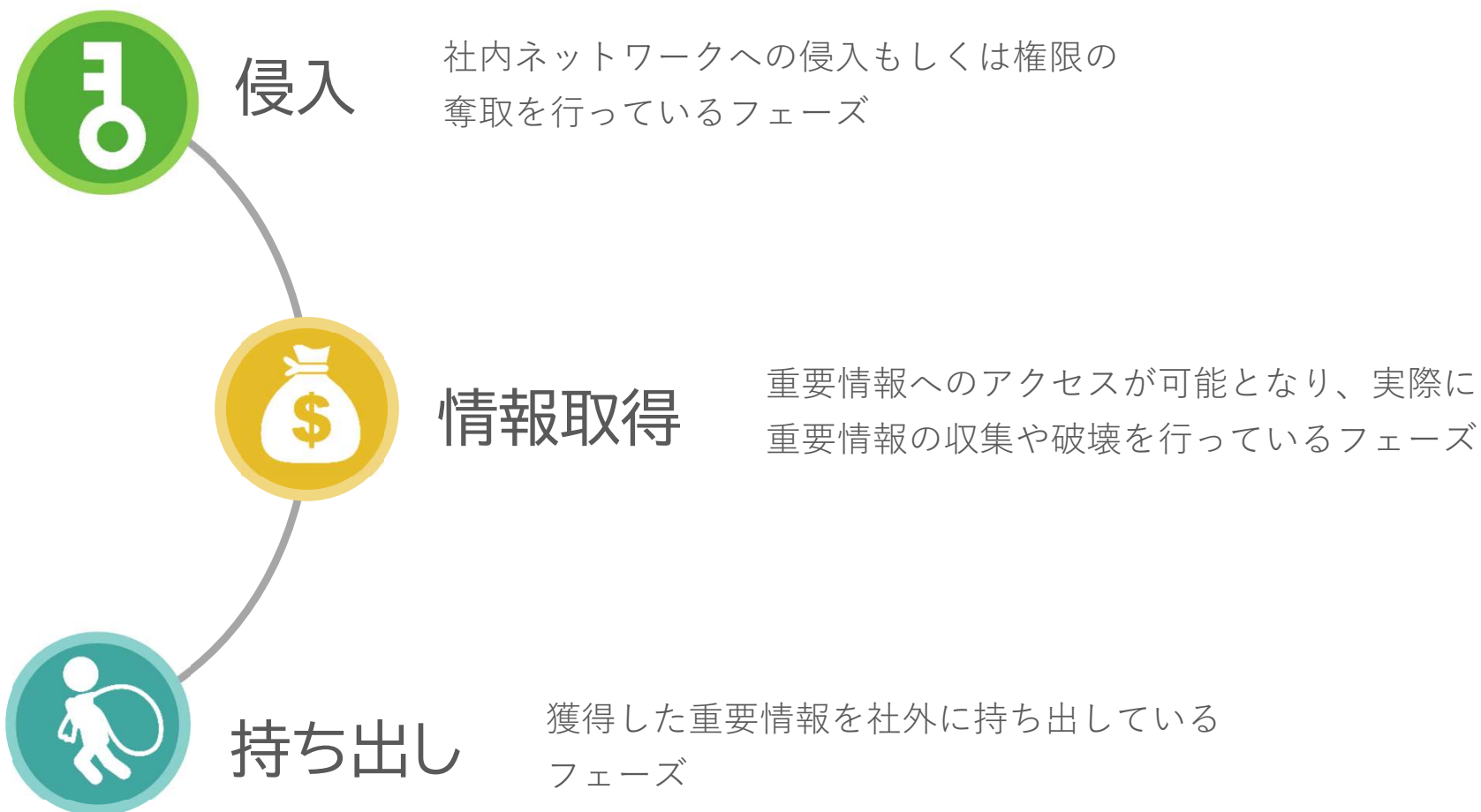
© AMIYA Corporation
1

色付きの部分が検知できる攻撃フェーズを表します。

レポートで設定されている条件の初期値です。

検知パックを利用するユーザーが、自社の環境に応じて設定する必要がある項目です。

レポートをご利用いただく上での役立ち情報など。



ALog EVA	SV	1	サーバへの直接的なログオンチャレンジ	5p
ALog ConVerter	AD	2	短時間に大量に行われたログオンチャレンジ	7p
ALog ConVerter	AD	3	存在しないアカウントでのログオンチャレンジ	9p
ALog EVA	SV	4	イベントログの削除	11p
ALog ConVerter	SV	5	システム監査ポリシーの不審な変更	13p
ALog ConVerter	SV	6	不審なユーザアカウントの作成/削除	15p
ALog EVA	SV	7	特権ユーザのログオン	17p
ALog ConVerter	SV	8	無効なアカウントによるログオンチャレンジ	19p
ALog ConVerter	SV	9	ランサムウェアによる被害範囲の特定	21p
ALog ConVerter	DB	10	規定外ツールによる DB 操作	23p
ALog EVA	Proxy	11	ファイル共有サービスへのアップロード回数	25p
ALog EVA	FW	12	ファイル共有サービスへのアップロードサイズ	27p
ALog EVA	FW	13	業務時間外のアクセス監視	29p
ALog EVA	Proxy	14	不正アクセスの把握	31p

1. サーバへの直接的なログオンチャレンジ

Server



攻撃者がサーバへ直接ログオンしようとしていることが分かります。

攻撃者がログオンしようとして失敗した場合、攻撃されたサーバでは「4625」というイベントIDが出力されます。4625は「ログオン失敗」を意味するログであるため、ログオン成功のログが出力されない限り、対象サーバへの侵入は成功していないと考えられます。



レポートの初期設定値

項目	設定内容
EventID	4625
ユーザー	*\$.*を除外

チューニングのポイント

項目	設定内容
ユーザー	環境に応じて [アカウント] を除外
サーバ	環境に応じて [対象サーバ] を設定
ClientIP	対象外とするクライアントIPがあれば [除外する] に登録 (シス担当者など)

Tips

イベントID : 4625は、攻撃者が侵入しようとした対象の“ローカルコンピュータ”上に記録されます。

1. サーバへの直接的なログオンチャレンジ

Server



条件1 + 追加

ユーザー [対象とする] AND OR ✕
複数指定する場合、改行区切りで入力します。

[除外する] *\$:* 「\$:」の入ったシステム用のアカウントは除外

対象 [対象とする] AND OR ✕
複数指定する場合、改行区切りで入力します。

[除外する] AND OR
複数指定する場合、改行区切りで入力します。

操作 選択なし 操作一覧

サーバ [対象とする] 監視対象のサーバを指定
複数指定する場合、改行区切りで入力します。

[除外する]
複数指定する場合、改行区切りで入力します。

EventID [対象とする] EventIDは「4625」を指定
4625

[除外する]
複数指定する場合、改行区切りで入力します。

ClientIP [対象とする] AND OR ✕
複数指定する場合、改行区切りで入力します。

[除外する] 対象外にするクライアントIPを除外設定
複数指定する場合、改行区切りで入力します。

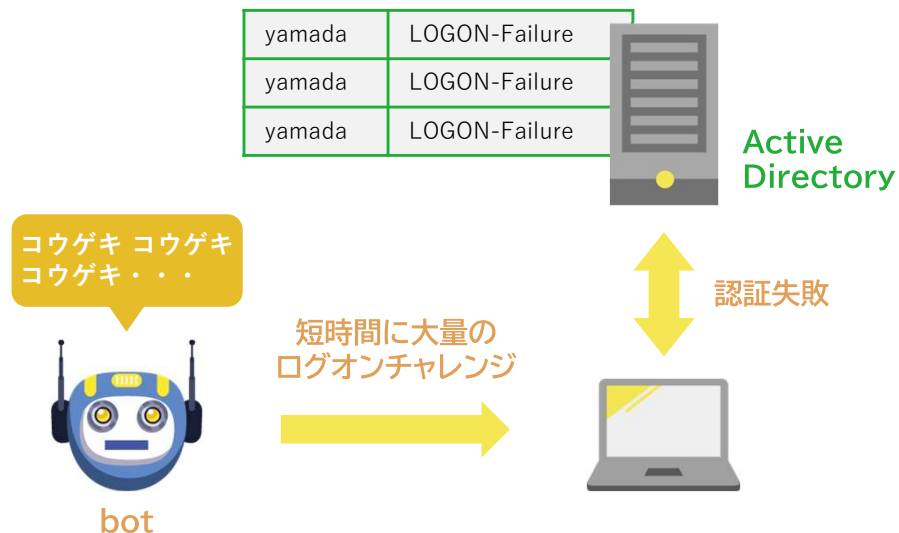
2. 短時間に大量に行われたログオンチャレンジ



機械的なログオンチャレンジが行われていることが分かります。

短時間で大量にLOGON-Failureが出力される場合、該当端末がマルウェアに侵入されていたり、攻撃者に乗っ取られようとしていることを意味します。

ログオンに成功しない限りドメインへの侵入は完了していませんが、該当端末の調査を早期に行う必要があります。



レポートの初期設定値

項目	設定内容
操作	Logon-Failure
しきい値	回数：3 間隔：1日

チューニングのポイント

項目	設定内容
サーバ	Active Directoryを指定
ClientIP	対象外とするクライアントIPがあれば [除外する]に登録
しきい値	運用にあわせて回数を調整

Tips

Logon-FailureはALog ConVerter独自のロジックで生成されるログです。

2. 短時間に大量に行われたログオンチャレンジ

Active Directory



条件1 + 追加

ユーザー

[対象とする] AND OR ✕
複数指定する場合、改行区切りで入力します。

[除外する] AND OR
複数指定する場合、改行区切りで入力します。

対象

[対象とする] AND OR ✕
複数指定する場合、改行区切りで入力します。

[除外する] AND OR
複数指定する場合、改行区切りで入力します。

操作 1 selected ▼ LOGON-Failureを指定

サーバ

[対象とする] AND OR ✕
複数指定する場合、改行区切りで入力します。

[除外する]
複数指定する場合、改行区切りで入力します。

ClientIP

[対象とする] AND OR ✕
複数指定する場合、改行区切りで入力します。

[除外する]
複数指定する場合、改行区切りで入力します。

しきい値 ? + 3 - しきい値の間隔 1日 ▼ 運用状況で大量に出て異常の判断ができない場合などは調整

3. 存在しないアカウントでのログオンチャレンジ



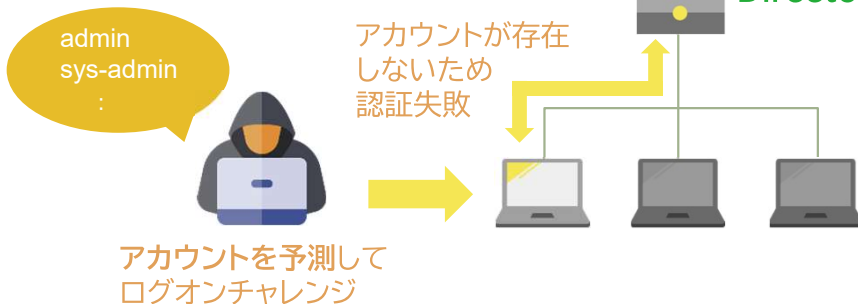
攻撃者が憶測のアカウントでログオンチャレンジを行っていることが分かります。

Active Directoryに存在しないアカウントを使って、ドメイン配下のPCにログオンしようすると、ログオン失敗の理由として「0xC0000064」などがログに書き込まれます。

アカウントIDを固定としてパスワードだけを入力させる設定としている場合、高確率で攻撃を受けている可能性があります。

admin	LOGON-Failure	*0xC0000064*
sys-admin	LOGON-Failure	*0xC0000064*
administrator	LOGON-Failure	*0xC0000064*

Active
Directory



レポートの初期設定値

項目	設定内容
操作	LOGON-Failure
ErrorCause	*0xC0000064* *0xC000006E*

チューニングのポイント

項目	設定内容
対象	環境に応じて [アカウント] を設定
サーバ	環境に応じて [対象サーバ] を設定

Tips

「*0xC0000064*」「*0xC000006E*」はアカウント間違いで出力されるため、IDを都度入力させる設定になっていない場合は攻撃の可能性が高いと考えられます。

3. 存在しないアカウントでのログオンチャレンジ

Active Directory



条件1 + 追加

ユーザー	<div>[対象とする] AND OR ✕ 複数指定する場合、改行区切りで入力します。</div> <div>[除外する] AND OR 複数指定する場合、改行区切りで入力します。</div>
操作	<div>1 selected ▼ 操作一覧</div>
サーバ	<div>[対象とする] AND OR ✕ 複数指定する場合、改行区切りで入力します。</div> <div>[除外する] 複数指定する場合、改行区切りで入力します。</div>
ErrorCause	<div>[対象とする] AND OR ✕ *0xC0000064* *0XC000006E*</div> <div>[除外する] AND OR 複数指定する場合、改行区切りで入力します。</div>

LOGON-Failureを指定

Active Directoryを指定

アカウントが存在しないことを意味する
メッセージを指定



攻撃者が痕跡を消すために、イベントログを削除したことが分かります。

イベントログを削除した場合にイベントID「1102」または「104」のログが出力されます。

イベントログの削除は、攻撃の最終フェーズで行われることが多く、システム管理者などが意図してログを削除したのでなければ、攻撃を疑う必要があります。



レポートの初期設定値

項目	設定内容
EventID	1102, 104

チューニングのポイント

項目	設定内容
対象	環境に応じて [アカウント] を設定
サーバ	環境に応じて [対象サーバ] を設定

Tips

ログを削除する際は、事前に申請を行うというルールにしておくと、より精度の高い運用が可能となります。

4. イベントログの削除

Server



条件1 + 追加

対象	<div><div>[対象とする]</div><div>複数指定する場合、改行区切りで入力します。</div></div> <div><div>[除外する]</div><div>複数指定する場合、改行区切りで入力します。</div></div>	AND	
操作	<div>選択なし ▾</div> <div>操作一覧</div>		
サーバ	<div><div>[対象とする]</div><div>複数指定する場合、改行区切りで入力します。</div></div> <div><div>[除外する]</div><div>複数指定する場合、改行区切りで入力します。</div></div>	AND	
EventID	<div><div>[対象とする]</div><div>1102 104</div></div> <div><div>[除外する]</div><div>複数指定する場合、改行区切りで入力します。</div></div>	AND OR	

監視対象を絞り込む場合は指定

監視対象を絞り込む場合は指定

EventIDは「104」「1102」を指定

5. システム監査ポリシーの不審な変更

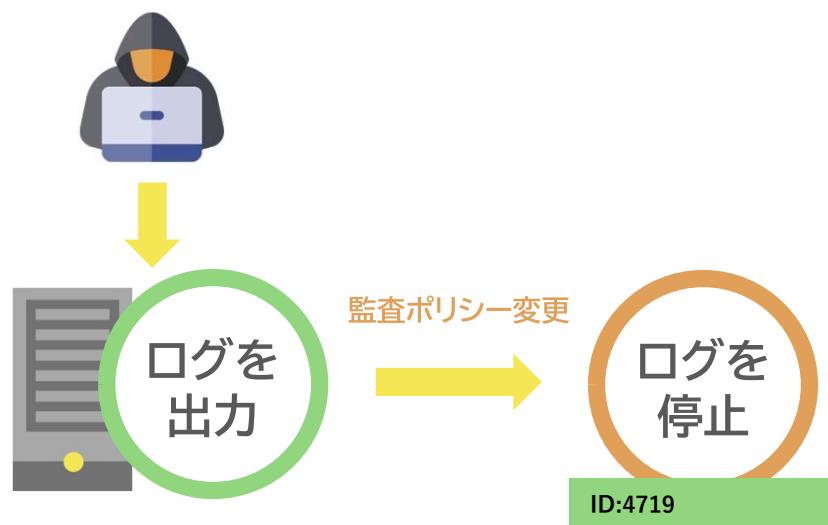
Server



攻撃者が活動しやすい環境を作ろうとして、監査ポリシーを変更したことが分かります。

システム監査ポリシーを変更すると、イベントID「4719」のログが出力されます。

サーバ管理者が作業申請していないタイミングで出力された場合、攻撃者がターゲットサーバへ侵入したのちに活動しやすい設定に変更したことが想定されます。



レポートの初期設定値

項目	設定内容
操作	ADMIN
EventID	4719

チューニングのポイント

項目	設定内容
サーバ	環境に応じて [対象サーバ] を設定

Tips

管理者用端末を指定している場合は、「管理者端末以外からのポリシー変更」という条件でレポートを作成することも効果があります。

5. システム監査ポリシーの不審な変更

Server



条件1 + 追加

ユーザー

[対象とする] AND OR ✕
複数指定する場合、改行区切りで入力します。

[除外する] AND OR
複数指定する場合、改行区切りで入力します。

操作

1 selected ▼ 操作一覧

サーバ

[対象とする] AND OR ✕
複数指定する場合、改行区切りで入力します。

[除外する] AND
複数指定する場合、改行区切りで入力します。

EventID

[対象とする] AND OR ✕
4719

[除外する] AND
複数指定する場合、改行区切りで入力します。

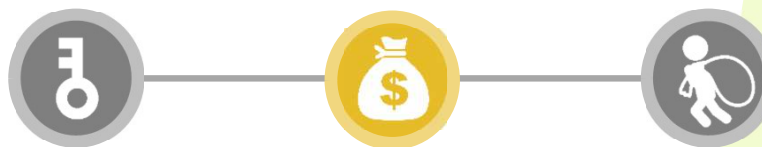
ADMINを指定

ADなど監視対象サーバを指定

EventIDは「4719」を指定

6. 不審なユーザアカウントの作成/削除

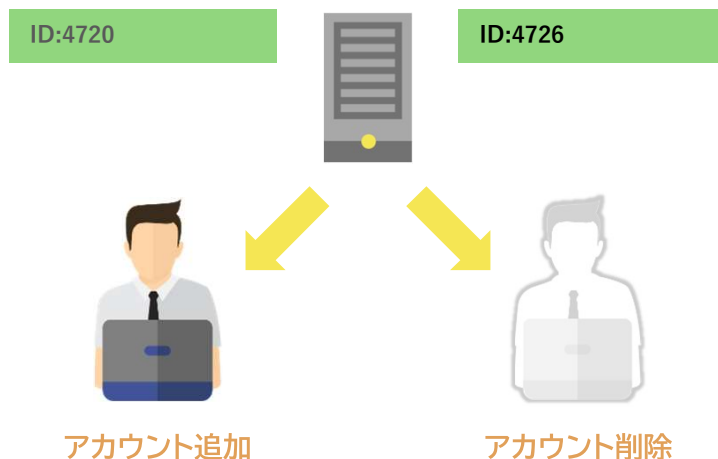
Server



攻撃者が攻撃に有利なアカウントを作成したり、不要となったアカウントを削除したことが分かります。

ADサーバにてユーザアカウントを作成/削除すると、イベントID「4720/4726」のログが出力されます。

サーバ管理者が作業申請していないタイミングで出力された場合、攻撃者がターゲットサーバへ侵入したのちに活動用アカウントを作成/削除したことが想定されます。



レポートの初期設定値

項目	設定内容
操作	ADMIN
EventID	4720, 4726

チューニングのポイント

項目	設定内容
サーバ	環境に応じて [対象サーバ] を設定
項目	設定内容

Tips

管理者用端末を指定している場合は、「管理者端末以外からのポリシー変更」という条件でレポートを作成することも効果があります。

6. 不審なユーザアカウントの作成/削除

Server



条件1 + 追加

ユーザー

[対象とする] AND OR ✕
複数指定する場合、改行区切りで入力します。

[除外する] AND OR
複数指定する場合、改行区切りで入力します。

操作

1 selected ▼ 操作一覧

EventID

[対象とする] AND OR ✕
4720
4726

[除外する] AND OR
複数指定する場合、改行区切りで入力します。

サーバ

[対象とする] AND OR ✕
複数指定する場合、改行区切りで入力します。

[除外する] AND OR
複数指定する場合、改行区切りで入力します。

ADMINを指定

EventIDは「4720」「4726」を指定

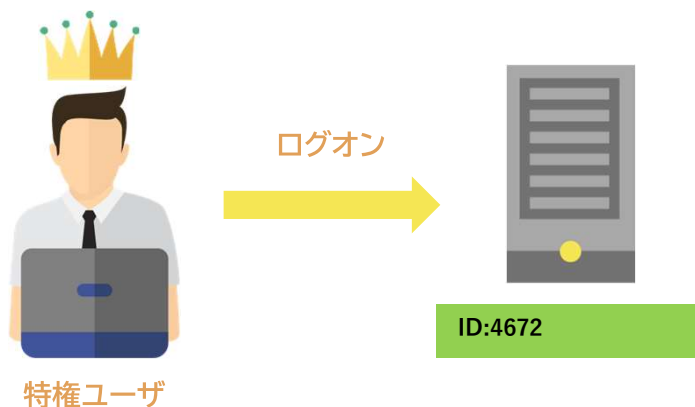
ADなど監視対象サーバを指定



攻撃者が不正に取得した特権ユーザでサーバにログオンしたことが分かります。

管理者権限およびそれと同等の権限（SeBackup Privilege 権限など）が割り当てられたアカウントがログオンすると、対象サーバではイベントID「4672」のログが出力されます。

社内で管理されているユーザ以外が管理者権限でアクセスしたり、不自然なタイミングでの特権ユーザのアクセスは攻撃者による侵入の可能性があります。



レポートの初期設定値

項目	設定内容
EventID	4672

チューニングのポイント

項目	設定内容
対象	対象外とするユーザがあれば [除外する] に登録 (システムアカウントなど)
サーバ	環境に応じて [対象サーバ] を設定

Tips

管理者用端末を指定している場合は、「管理者端末以外からのポリシー変更」という条件でレポートを作成することも効果があります。

7. 特権ユーザのログオン

Server



条件1 + 追加

ユーザー

[対象とする] AND OR ×
複数指定する場合、改行区切りで入力します。

[除外する] AND OR
複数指定する場合、改行区切りで入力します。

対象

[対象とする] AND OR ×
SeBackupPrivilege
SeCreateTokenPrivilege

[除外する] AND OR
複数指定する場合、改行区切りで入力します。

操作

選択なし 操作一覧

サーバ

[対象とする] AND ×
複数指定する場合、改行区切りで入力します。

[除外する] AND ×
複数指定する場合、改行区切りで入力します。

EventID

[対象とする] AND ×
4672

[除外する] AND ×
複数指定する場合、改行区切りで入力します。

検知する管理者権限を
絞り込む場合は指定

対象サーバを絞り込む場合は指定

EventIDは「4672」を指定

8. 無効なアカウントによるログオンチャレンジ

Server



無効なアカウントを用いて、ログオンチャレンジを試みていることが分かります。

無効設定、期限切れ、またはロックアウトされた状態のアカウントを用いてログオンチャレンジすると、LOGON-Failureのログに「無効、期限切れ、またはロックアウト」というコメントが記録されます。

攻撃者が当該アカウントを不正に利用して、ドメインに侵入しようとしている可能性があります。

レポートの初期設定値

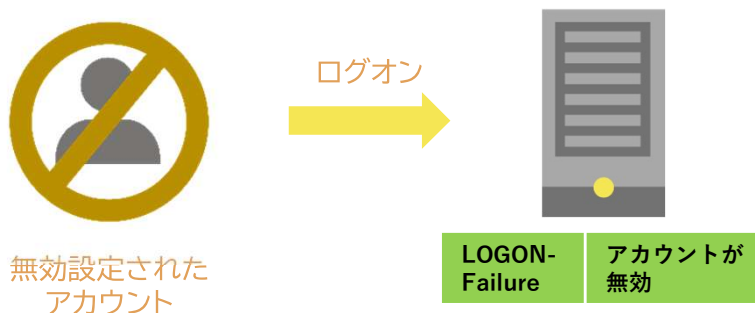
項目	設定内容
操作	LOGON-Failure
ErrorCause	*無効、期限切れ、またはロックアウト*

チューニングのポイント

項目	設定内容
サーバ	環境に応じて [対象サーバ] を設定

Tips

無効、期限切れアカウントなど不要なアカウントの放置は攻撃者に利用されるリスクとなるため、定期的なメンテナンスをすることをお勧めします。



8. 無効なアカウントによるログオンチャレンジ

Server

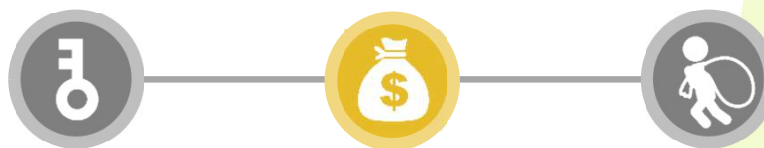


条件1 + 追加

操作	1 selected ▼ 操作一覧	LOGON-Failureを指定
サーバ	[対象とする] AND	EventIDは「4672」を指定
	複数指定する場合、改行区切りで入力します。	
ErrorCause	[除外する] AND	抽出条件のコメントを指定 ※前後に「*」を入れる点に注意
	複数指定する場合、改行区切りで入力します。	

無効、期限切れ、またはロックアウト

9. ランサムウェアによる被害範囲の特定



短時間で大量にRENAMEログが出力される場合は、ランサム攻撃が疑われます。

ファイル名や拡張子の変更をすると、「RENAME」のログが出力されます。

ランサムウェアに感染した端末を特定し、暗号化された被害範囲を特定することができます。

レポートの初期設定値

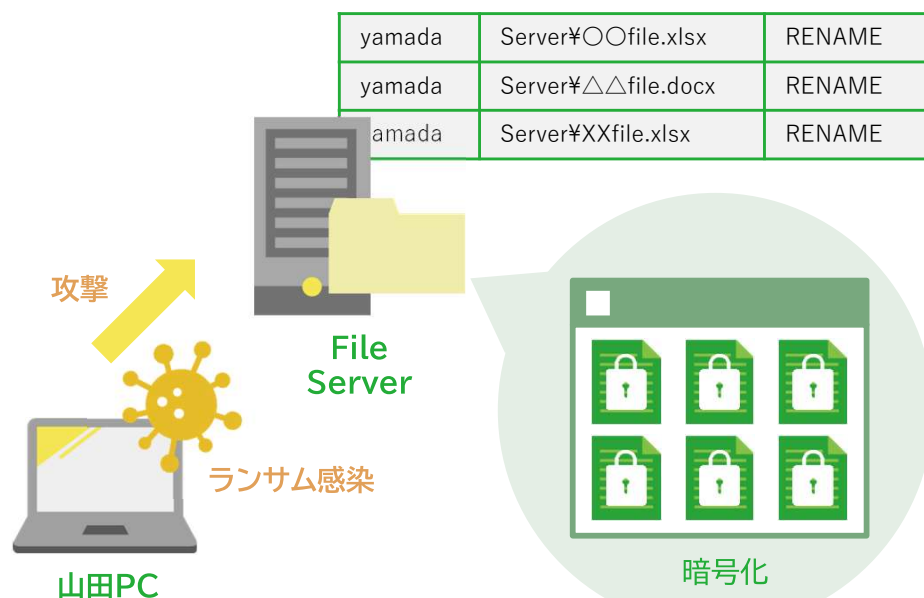
項目	設定内容
操作	RENAME
しきい値	100回/h

チューニングのポイント

項目	設定内容
ユーザー	対象外とするアカウントがあれば [除外する] に登録 (システムアカウントなど)
サーバ	環境に応じて [対象サーバ] を設定

Tips

RENAMEログをチェックすることで感染端末と攻撃範囲を迅速に特定できます。



9. ランサムウェアによる被害範囲の特定

File Server



条件1 + 追加

操作	1 selected ▼	操作一覧
ユーザー	[対象とする] 複数指定する場合、改行区切りで入力します。	AND OR ✕
	[除外する] 複数指定する場合、改行区切りで入力します。	AND OR ✕
サーバ	[対象とする] 複数指定する場合、改行区切りで入力します。	AND OR ✕
	[除外する] 複数指定する場合、改行区切りで入力します。	AND OR ✕

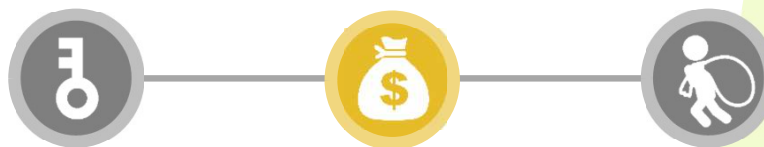
しきい値 ? + 100 - しきい値の間隔 1時間 ▼

RENAMEを指定

**バックアップシステム用のアカウントなど
対象外とするアカウントがあれば登録**

監査対象を絞る場合は指定

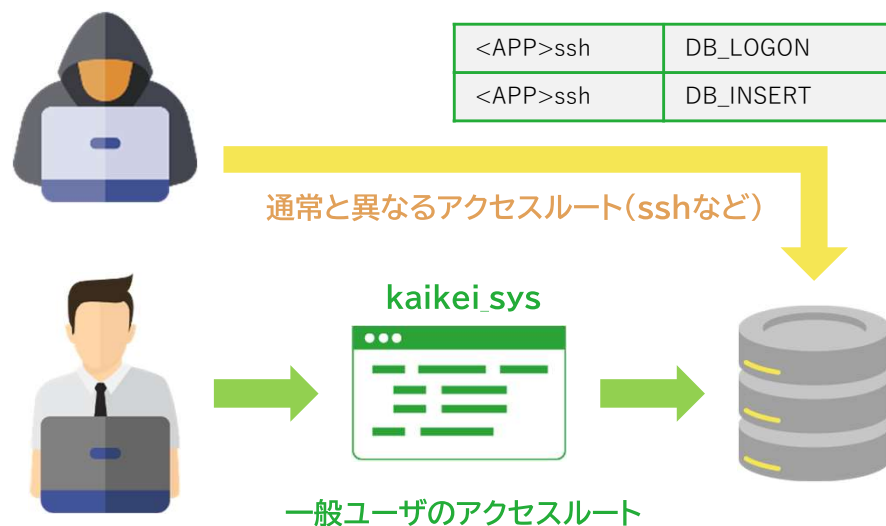
ファイル数などで調整



攻撃者が不正にDBへのアクセスを行っていることが分かります。

許可されたツール（システム）以外を経由してDBにアクセスした場合、レポートिंगされます。

メンテナンスなどの明確な理由がなく、通常と異なるツールを経由したログが出力された場合、攻撃者による不正侵入の疑いがあります。



レポートの初期設定値

項目	設定内容
操作	DB_*（DBで始まる操作全て）

チューニングのポイント

項目	設定内容
サーバ	環境に応じて [対象サーバ] を設定
AppName	規定アプリを除外する

Tips

DBへの通常のアクセスルートをフィルタすることで、不審なDBアクセスを効率的に発見できます。

10. 規定外ツールによる DB 操作

Database



条件1 + 追加

操作	16 selected ▼ 操作一覧	「DB」で始まる操作を指定
AppName	<div>[対象とする] AND OR ✕ 複数指定する場合、改行区切りで入力します。</div> <div>[除外する] 複数指定する場合、改行区切りで入力します。</div>	一部アプリ経由のアクセスを除外する場合は指定
サーバ	<div>[対象とする] AND OR ✕ 複数指定する場合、改行区切りで入力します。</div> <div>[除外する] 複数指定する場合、改行区切りで入力します。</div>	対象を絞る場合は指定

11. ファイル共有サービスへのアップロード回数

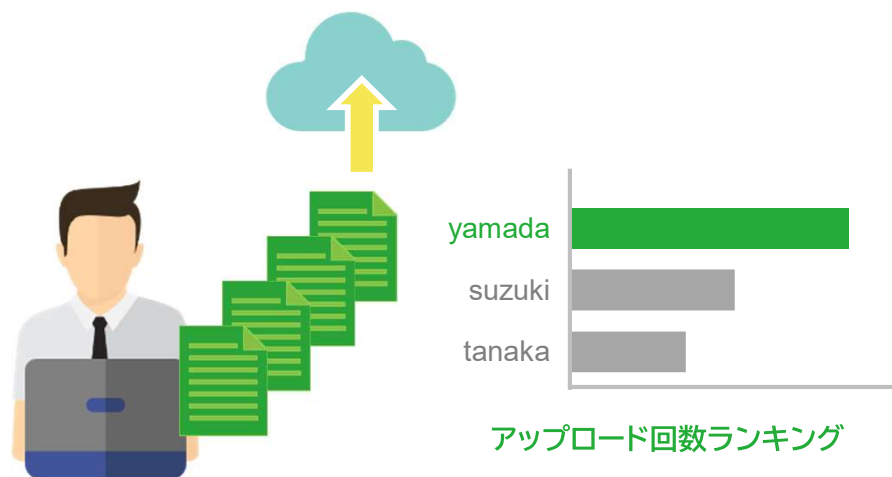
WEB Proxy



ファイル共有サービスへのアップロード回数をランキングします。

不自然にファイルアップロードの回数が多い場合は、情報漏えいのリスクが高くなります。

急激にアップロード回数が増えたユーザは、情報の不正な持ち出しや外部の攻撃者によるアカウントの乗っ取りを疑う必要があります。



レポートの初期設定値

項目	設定内容
サーバ	WEB Proxyの名称を記載
CategoryIDs	116、104、85、86
集計キー	ClientIP

※i-Filterを想定した設定

チューニングのポイント

項目	設定内容
CategoryIDs	カテゴリIDの取捨選択をしてください

Tips

サイバー攻撃に限らず、社内情報を不用意に外部ストレージにアップロードする行為は注意する必要があります。

11. ファイル共有サービスへのアップロード回数

WEB Proxy



レポートの詳細設定 ?

表示形式 ☒ ランキング ☐ 時系列

集計キー 第1キー ClientIP [v] [+] [-]

集計方法

☒ アクセスログの行数をカウントする

☐ 特定項目を合計する

出力件数 ? [+] 30 [-] ☐ 制限しない

フィルター追加 ユーザー [v] [追加]

条件1 [v] [追加]

操作 [選択なし v] [操作一覧]

サーバ [対象とする]

iFilter

[除外する]

複数指定する場合、改行区切りで入力します。

CategoryIDs [対象とする]

116

104

85

86

[除外する]

複数指定する場合、改行区切りで入力します。

ClientIPを指定

Web Proxyを指定

「116」「104」「85」「86」で始まる操作を指定
※i-Filterの場合
他に指定するカテゴリや他製品の場合は、
アクセスを不許可としている
カテゴリを指定

12. ファイル共有サービスへのアップロードサイズ

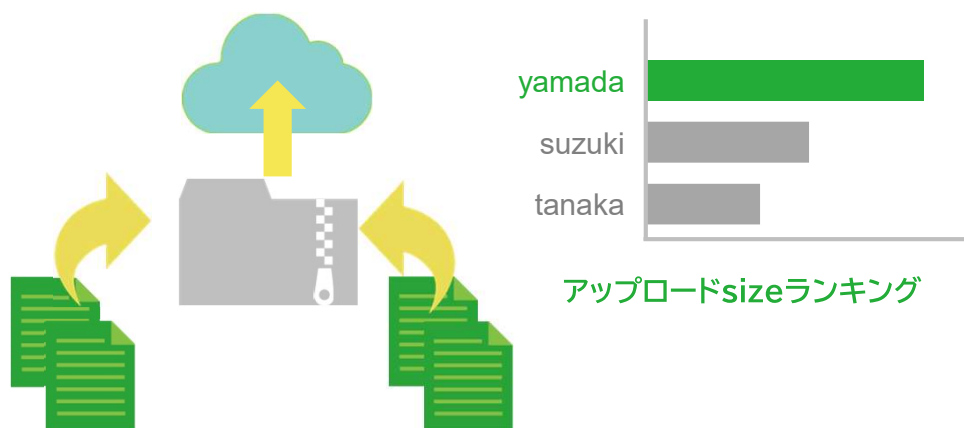
FW / WEB Proxy



ファイル共有サービスへアップロードしたデータ量をランキングします。

複数のファイルをzip化した場合など、1回のアップロードで複数のファイルを送っていることを判断できない場合は、アップロードしたデータサイズをみるのが有効です。

不自然に大きなファイルをアップロードしている場合などは、アップロードファイルの内容を調査する必要があります。



複数のファイルをまとめてzip化

⚙ レポートの初期設定値

【Firewallの場合】

項目	設定内容
集計キー	SrcIP
集計方法	SentByte

※Fortigateを想定した設定

【PROXYの場合】

項目	設定内容
CategoryIDs	116、104、85、86
集計キー	サーバ
集計方法	RequestSize
しきい値	10000000 (10MB)

※i-Filterを想定した設定

🔧 チューニングのポイント

項目	設定内容
サーバ	FirewallもしくはPROXYを選択
CategoryIDs	カテゴリIDの取舍選択をしてください
しきい値	運用にあわせて値を調整

12. ファイル共有サービスへのアップロードサイズ

FW / WEB Proxy



[Firewall(Fortigate)]

レポートの詳細設定 ?

表示形式 ☒ ランキング ☐ 時系列

集計キー 第1キー SrcIP

集計方法

☐ アクセスログの行数をカウントする

☒ 特定項目を合計する SentByte

出力件数 ? 30 ☐ 制限しない

フィルター追加 ユーザー

条件1

操作

サーバ

[対象とする]

[除外する]

複数指定する場合、改行区切りで入力します。

SrcIP指定

SentByte指定

Firewallを指定

12. ファイル共有サービスへのアップロードサイズ

FW / WEB Proxy



[Proxy(i-Filter)]

レポートの詳細設定 ?

表示形式 ☒ ランキング ☐ 時系列

集計キー 第1キー サーバ + -

集計方法

☐ アクセスログの行数をカウントする

☒ 特定項目を合計する RequestSize

出力件数 ? + 30 - ☐ 制限しない

フィルター追加 ユーザー 追加

条件1 + 追加

操作 選択なし 操作一覧

サーバ [対象とする] AND OR ✕

iFilter ✕

[除外する] AND OR

複数指定する場合、改行区切りで入力します。

CategoryIDs [対象とする] AND OR ✕

116

104

85

86

[除外する] AND OR

複数指定する場合、改行区切りで入力します。

しきい値 ? + 100000(- しきい値の間隔 1日

Proxyを指定

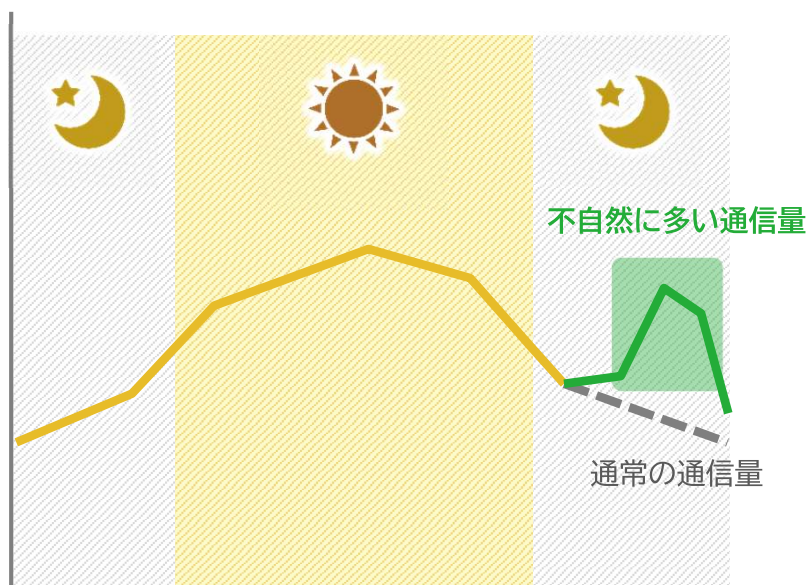
RequestSizeを指定

「116」「104」「85」「86」を指定

運用状況を見てしきい値を調整



本来トラフィックが少なくなる業務時間外に、異常なトラフィックが発生していないかを把握できます。
普段のトラフィック傾向を把握し、これと比較して異常な増加がないかを把握することで、不審な通信を発見することに役立てることができます。



レポートの初期設定値

項目	設定内容
時間帯	18 : 00～7 : 59

チューニングのポイント

項目	設定内容
サーバ	FirewallもしくはProxyを選択
時間帯	環境に応じて時間帯を変更

Tips

業務時間外は、夜間だけではなく休日のレポートも用意すると、より効果的です。

13. 業務時間外のアクセス監視

FW / WEB Proxy



条件1 + 追加

対象

[対象とする] AND OR ✕
複数指定する場合、改行区切りで入力します。

[除外する] AND OR
複数指定する場合、改行区切りで入力します。

操作

選択なし ▾ 操作一覧

サーバ

[対象とする] AND OR
iFilter

[除外する] AND
複数指定する場合、改行区切りで入力します。

時間帯

18:00 - 7:59

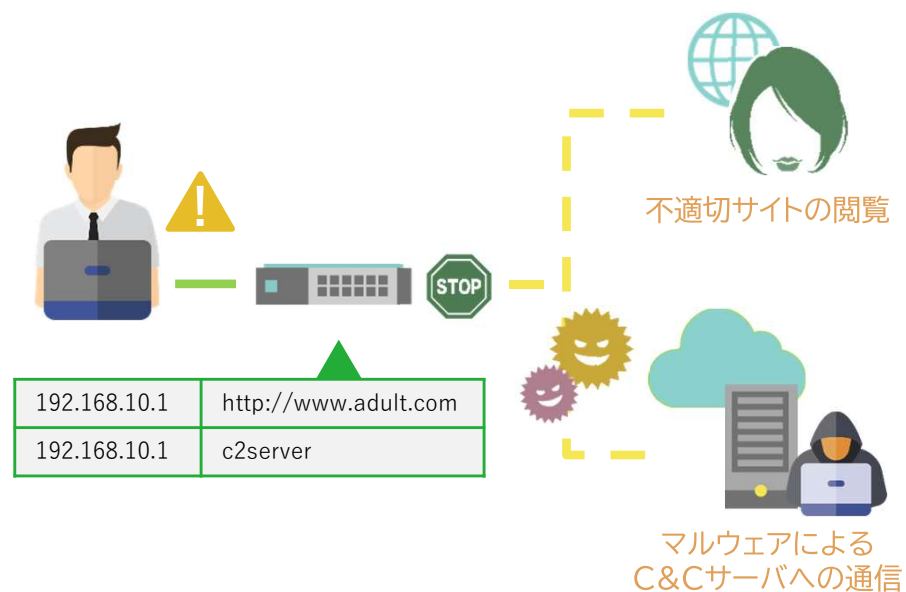
対象となるFWもしくはProxyを指定

監視する時間帯を指定



不正サイトへのアクセス状況から、従業員のサボタージュや、マルウェア感染の可能性を把握できます。

「不正サイト」にカテゴライズされたサイトへのアクセス行為は、どの端末がどのURLへアクセスしようとしたかという内容でログに記録されます。



レポートの初期設定値

項目	設定内容
操作	BLOCK

チューニングのポイント

項目	設定内容
サーバ	WEB Proxyの名称を記載

Tips

不自然なサイトへのアクセスや、心当たりのないサイトへのアクセスが極端に多い場合は、マルウェア感染によりC&Cサーバへ誘導されている可能性も検討する必要があります。

条件1 + 追加

操作 1 selected ▼ 操作一覧 「BLOCK」を指定 ※i-Filterの場合

サーバ [対象とする] AND OR * 対象となるProxyを指定

ifilter

[除外する] AND

複数指定する場合、改行区切りで入力します。