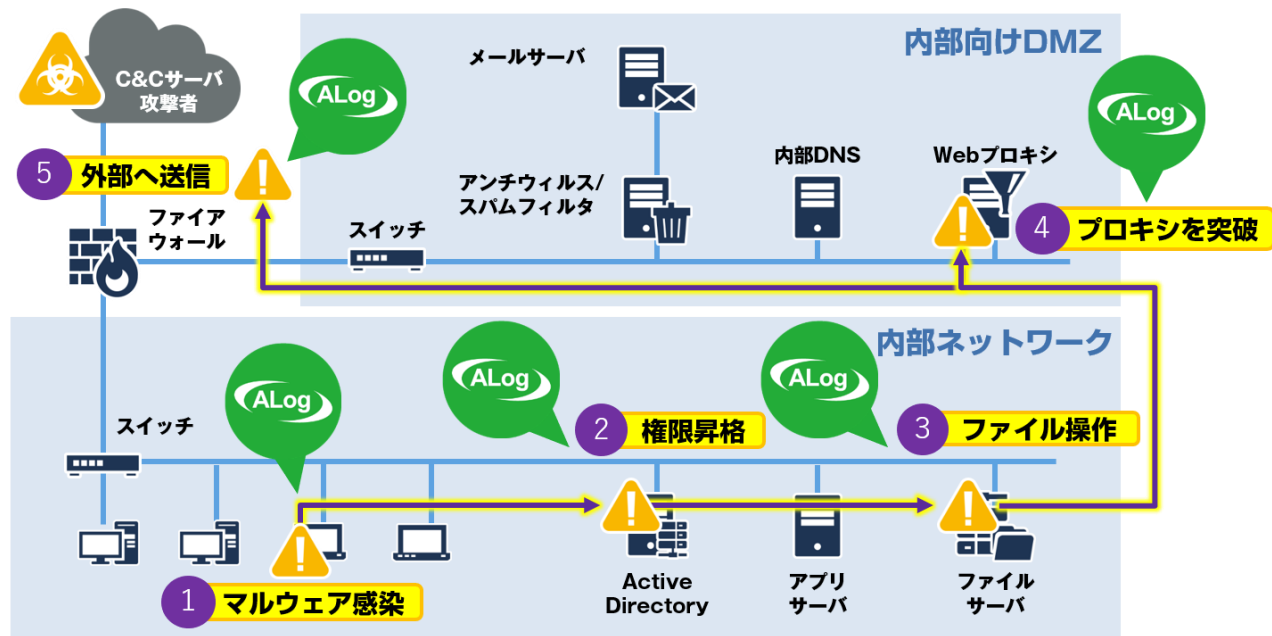


サイバー攻撃自動検知パックV2の内容について

“疑わしく見えないメール”を軽い気持ちで開封してしまい、すんなり侵入/攻撃/拡散されてしまう今、FW/UTMといった入り口対策ではもはや防衛とは言えない。

侵入後の「スピーディな察知+範囲/侵入経路の特定+迅速な隔離」が最善のセキュリティ対策です。



典型的な攻撃パターンを知ることが最も肝要

3つのチェックポイント

侵入行為の特定

不正な権限掌握

大量のログイン失敗
アカウントの作成
管理権限への昇格
ポリシー/パスワードの変更
イベントログの削除



ADサーバ

被害範囲の特定

持ち出しの気配

大量のファイル名変更
深夜休日のファイルアクセス
アクセスの失敗



ファイルサーバ

外部送信の特定

不審な通信

特定のIPへのアクセス急増
異常なHTTPポート通信
時間外のHTTPポート通信



FW/DNS Webプロキシ

ALogなら
テンプレート適用で
即実装&全自動化

種別	リスク	検知内容	対象機器	必要ライセンス
Windows Server 及び Active Directory	乗っ取り	サーバへの直接的なログオンチャレンジ	各種Windows Server Active Directory	ALog EVA
		イベントログの削除		ALog ConVerter for Windows
		特権ユーザのログオン		
		短時間に大量に行われたログオンチャレンジ		
		存在しないアカウントでのログオンチャレンジ		
		システム監査ポリシーの不審な変更		
		不審なユーザアカウントの作成/削除		
		無効なアカウントによるログオンチャレンジ		
ファイルサーバ	情報漏えい	ランサムウェアによる被害範囲の特定	Windows Server / NetApp / Unity / PowerScale (Isilon)	ALog ConVerter各種
データベース	外部攻撃	規定外ツールによる DB 操作	Oracle / SQL Server	ALog ConVerter DB
Webプロキシ	情報漏えい 外部送信	ファイル共有サービスへのアップロード回数	i-Filter	ALog EVA
		ファイル共有サービスへのアップロードサイズ		
		業務時間外のアクセス監視		
		不正アクセスの把握		
ファイアウォール	情報漏えい 外部送信	ファイル共有サービスへのアップロードサイズ	Fortigate	ALog EVA
		業務時間外のアクセス監視		

テンプレートの利用方法について (EVAテンプレの取り込み)

- ActiveDirectory、i-Filter、FortiGateのログを初めて取得する場合、各フォルダに**取り込み用EVAテンプレート**が格納されておりますので、レポート定義をインポート頂く前に「取り込み用EVAテンプレート」をインポートの上、対象機器の登録をお願い致します。

参考としてActiveDirectoryの画面を添付しています。

名前		更新日時	種類	名前		更新日時
99_取り込み用EVAテンプレ		2022/08/09 15:25	ファイル フォルダー	SecurityTemplate(RawLine)		2020/07/30 14:43

テンプレートの利用方法について (EVAテンプレの取り込み)

◆テンプレートのインポート手順

The screenshot shows the ALog web interface. The top navigation bar includes 'ホーム' (Home), '検索' (Search), 'レポート / アラート' (Report / Alert), and '管理' (Management). The '管理' tab is highlighted with a red box and a callout bubble labeled '① 管理タブをクリック' (Click the Management tab). The left sidebar contains various settings categories, with '設定のインポート / エクスポート' (Import/Export Settings) highlighted with a red box and a callout bubble labeled '② 「設定のインポート/エクスポート」タブをクリック' (Click the 'Import/Export Settings' tab). The main content area shows the 'ステータス' (Status) section, which includes a table of tasks and their execution details.

サーバ	タスクの種類	タスクの状態	次の実行日時	前回の実行日時	前回の実行結果	アクセスログ...	
S-2019SK	ログ変換	準備完了	2019/10/16 16:40:00	2019/10/16 16:30:00	正常終了	0	タスクの操作▼
S-2019SK	インポート	準備完了	-	2019/10/16 16:30:00	正常終了		タスクの操作▼
S-2019SK	レポート	準備完了	2019/10/17 2:00:00	2019/10/16 16:33:00	正常終了		タスクの操作▼
S-2019SK	AD情報取得	準備完了	2019/10/17 1:00:00	2019/10/16 16:33:00	正常終了	2545	タスクの操作▼
S-2019SK	メンテナンス	準備完了	2019/10/17 3:00:00	-			タスクの操作▼
S-2019SK	リスク学習	準備完了	2019/11/01 0:00:00	-			タスクの操作▼

テンプレートの利用方法について (EVAテンプレの取り込み)

設定のインポート / エクスポート

設定のインポート/エクスポートを行います。

① エクスポート

② レポート / アラート

レポート名
<input type="checkbox"/> サーバアクセスランキング
<input type="checkbox"/> ファイルアクセスランキング
<input type="checkbox"/> ファイルの読込
<input type="checkbox"/> ログオン失敗
<input type="checkbox"/> 時間別アクセス
<input type="checkbox"/> 土日のアクセス
<input type="checkbox"/> 夜間のアクセス

③ 休日・祝日設定

名称
<input type="checkbox"/> 年末の休業日
<input type="checkbox"/> 年始の休業日

④ EVAテンプレート

テンプレート名
<input type="checkbox"/> NetApp (NFSv4)
<input type="checkbox"/> Webサーバ((IIS7)
<input type="checkbox"/> Webサーバ((IIS8)

⑤ エクスポート

⑥ インポート

⑦ インポート

③参照ボタンをクリック

名前	更新日時
01_認証ログ調査_大量のログオン失敗(4625)	2020/09/07 11:15
02_不審なログの確認_イベントログ消去(1102)	2020/09/07 11:15
03_不審なログの確認_Kerberos認証もしくはサービスチケットの要求(4768_4769)	2020/09/07 11:15
04_不審なログの確認_...	2020/09/07 11:15
05_不審なログの確認_...	2020/09/07 11:15
06_認証ログ調査_特権ユーザのログオン(4672)	2020/09/07 11:15
99_取り込み用テンプレ	2020/09/07 13:04

④取り込みたいEVAテンプレを選択

名前	更新日時
SecurityTemplate(RawLine)	2020/07/30 14:43

⑧ インポート

C:\fakepath\setting-2020-0619-173102890.xml

☒ レポート: 1 件

⑨ インポート

⑤インポートボタンをクリック

対象機器の追加（※対象機器のログを未取得のお客様）

◆サイバー攻撃自動検知パックV2 検知リストに記載されている対象機器のログを初めて取得する場合、対象機器の追加が事前により必要となります。

ALog ホーム 検索 レポート / アラート リスクスコアリング WorkTime 管理

対象サーバ

ログの収集対象となるサーバの設定を行ないます。
サーバの追加/削除やログの収集タスクの設定を行ないます。

+ 追加 削除 エージェントのアップデート 収集タスクの設定

サーバ	サーバ種別	収集タイプ	バージョン	アカウント	収集タスク	ログ種別
<input type="checkbox"/> AMIYADemo	Windows	エージェントレス方式	8.1.5	Administrator	●無効	ファイルアクセスログ, ログオンログ
<input type="checkbox"/> Blue_Coat_ProxySG	EVA	エージェントレス方式	8.1.5	-	●無効	-

設定 対象サーバ

「管理」タブ - 「対象サーバ」 - 「追加」をクリック頂くと、「対象サーバ追加ウィザード」が開きますので、対象機器の登録をお願いします。詳細はユーザガイドをご参照下さい。
※ログ取得対象の機器によって、必要ライセンスが変動致します。

テンプレートの利用方法（取り込み編）

◆テンプレートのインポート手順

The screenshot shows the ALog management interface. The top navigation bar includes 'ホーム' (Home), '検索' (Search), 'レポート / アラート' (Report / Alert), and '管理' (Management). The '管理' tab is highlighted with a red box and a callout bubble labeled '①管理タブをクリック' (Click the Management tab). The left sidebar contains various settings categories, with '設定のインポート / エクスポート' (Import / Export Settings) highlighted with a red box and a callout bubble labeled '②「設定のインポート/エクスポート」タブをクリック' (Click the 'Import/Export Settings' tab). The main content area shows the 'ステータス' (Status) section, which includes a table of tasks and their execution status.

サーバ	タスクの種類	タスクの状態	次の実行日時	前回の実行日時	前回の実行結果	アクセスログ...	
S-2019SK	ログ変換	準備完了	2019/10/16 16:40:00	2019/10/16 16:30:00	正常終了	0	タスクの操作▼
S-2019SK	インポート	準備完了	-	2019/10/16 16:30:00	正常終了		タスクの操作▼
S-2019SK	レポート	準備完了	2019/10/17 2:00:00	2019/10/16 16:33:00	正常終了		タスクの操作▼
S-2019SK	AD情報取得	準備完了	2019/10/17 1:00:00	2019/10/16 16:33:00	正常終了	2545	タスクの操作▼
S-2019SK	メンテナンス	準備完了	2019/10/17 3:00:00	-			タスクの操作▼
S-2019SK	リスク学習	準備完了	2019/11/01 0:00:00	-			タスクの操作▼

テンプレートの利用方法について (レポートテンプレ取り込み編)

設定のインポート / エクスポート

設定のインポート/エクスポートを行います。

① エクスポート

② レポート / アラート

レポート名
<input type="checkbox"/> サーバアクセスランキング
<input type="checkbox"/> ファイルアクセスランキング
<input type="checkbox"/> ファイルの読込
<input type="checkbox"/> ログオン失敗
<input type="checkbox"/> 時間別アクセス
<input type="checkbox"/> 土日のアクセス
<input type="checkbox"/> 夜間のアクセス

③ 休日・祝日設定

名称
<input type="checkbox"/> 年末の休業日
<input type="checkbox"/> 年始の休業日

④ EVAテンプレート

テンプレート名
<input type="checkbox"/> NetApp (NFSv4)
<input type="checkbox"/> Webサーバ((IIS7)
<input type="checkbox"/> Webサーバ((IIS8)

⑤ エクスポート

⑥ インポート

⑦ インポート

③参照ボタンをクリック

名前	更新日時	種類
02_4649 リプレイ攻撃が検出	2020/06/23 10:30	ファイル フォルダー
03_47		
04_47		
05_47		
06_47		
07_48		
08_4964 特殊グループは、新	2020/06/23 10:30	ファイル フォルダー
09_5124 OCSP レスポンス サー	2020/06/23 10:30	ファイル フォルダー
10_1102 イベントログ消去	2020/06/23 10:30	ファイル フォルダー
11_4768 4769 Kerberos サービスチケットが要求	2020/07/07 11:19	ファイル フォルダー
12_4672 Golgen Ticket Silver Ticketの使用...	2020/06/23 10:30	ファイル フォルダー
13_		
14_		
15_		
16_		
17_4770 INILIM総延	2020/06/19 17:31	XML ドキュメント

④取り込みたいレポート定義を選択
(フォルダ毎の指定が可能です)

⑧ インポート

C:\fakepath\setting-2020-0619-173102890.xml

☒ レポート: 1 件

⑨ インポート

⑤インポートボタンをクリック

テンプレートの利用方法について（レポートテンプレ取り込み編）

◆ 注意点

- ・ 全ての**レポートテンプレート**を取り込みたい場合、以下フォルダ内のファイル（setting-2022-0809-CyberReport.xml）をインポートして下さい。

名前	更新日時
01_Active Directory	2020/10/01 14:46
02_ファイルサーバ	2020/09/07 11:15
03_データベース	2020/10/01 14:12
04_Webプロキシ	2020/09/07 11:15
05_Firewall	2020/09/07 11:15
99_一括インポート	2020/09/07 11:15
サイバー攻撃自動検知バックレポート設定参考資料	2020/10/06 14:13
自動化バックの内容及び取り込み方法について	2020/08/17 12:40

名前	更新日時
setting-2022-0809-CyberReport	2022/03/17 9:38

※個別機器のレポートテンプレートのみを取り込みたい場合、各フォルダに格納されているxmlファイルを取り込んで下さい。

テンプレートの利用方法（確認編）

① レポート/アラートタブをクリック

ホーム 検索 レポート / アラート

フィルター 確認済みにする 操作▶

新規作成 編集

■ お気...	レポート名	概要説明	未確認ア...	最終更新日時	状態	有効な機能	PDF...	CSV...	メー...	編集
<input type="checkbox"/> ☆	イベントログ削除		🔔 未確...	2022/08/08 17:33	✓	📄 🔔 🛡️				

② 新規作成をクリック

新規作成 - テンプレート選択

標準テンプレート

基本監査パック

サイバー攻撃自動検知パック

Microsoft 365 パック

サイバー攻撃自動検知パック

ライセンスを登録してからレポートを設定してください

③ レポートテンプレがインポートされている事を確認

サイバー攻撃自動検知パック

AD : 存在しないアカウントでのログオンチャレンジ_103

AD : 短時間に大量に行われたログオンチャレンジ_102

DB : 規定外ツールによる DB 操作_110

FortiGate : ファイル共有サービスへのアップロードサイズ_115

FortiGate : 業務時間外のアクセス監視_116

このイベントは、アカウントがログオンに失敗し、間違ったパスワードでログオンしています。

このイベントは、アカウントがドメインに対するログオンに失敗したときに記録されます。本レポートでは同一アカウントが1日に3回以上、ログオン失敗した場合、レポート出力する設定としています。 ※スローアタックなど、断続的なログオンチャレンジを検知 しいき値及びしいき値の間隔はお客様環境に合わせて調整して下さい。

<監査基準/管理要求例> 定期的にアクセス記録の点検を行い、不正アクセスの有無、異常アクセスの有無を確認すること。特に通常時、利用されないアプリケーションなどのアクセスを確認すること。 <確認項目> 規定外ツールによるDBへのアクセスを集計し、レポート。SQLCMDなどを利用し、DBに対する不正アクセスが無いかを確認する。

同一IPのアップロード大量発生をレポートすることで、ポリシー違反行為もしくはリスクの可能性が高い通信を検知します。

勤務時間外などのVPN接続を監視することで、リスクの可能性が高い通信を把握する。

テンプレートの利用方法（作成編）

◆取り込んだレポートテンプレートをもとに、お客様環境に合ったレポートを作成しましょう。※別ファイル「レポート設定参考資料」を参照下さい。

ホーム 検索 レポート / アラート 管理

フィルター

確認済みにする

操作

■ お気…

レポート

☐

★

イベントログ削除

新規作成 - テンプレート選択

標準テンプレート

ライセンスを登録してからレポートを設定してください

基本監査パック

サイバー攻撃自動検知パック

AD : 存在しないアカウントでのログオンチャレンジ_103

このイベントは、アカウントがドメインに対するログオンに失敗したときに記録されます。本レポートでは同一アカウントが1日に3回以上、ログオン失敗した場合、レポート出力する設定としています。 ※スローアタックなど、断続的なログオンチャレンジを検知 しい値及びしい値の間隔はお客様環境に合わせて調整して下さい。

サイバー攻撃自動検知パック

AD : 短時間に大量に行われたログオンチャレンジ_102

このイベントは、アカウントがドメインに対するログオンに失敗したときに記録されます。本レポートでは同一アカウントが1日に3回以上、ログオン失敗した場合、レポート出力する設定としています。 ※スローアタックなど、断続的なログオンチャレンジを検知 しい値及びしい値の間隔はお客様環境に合わせて調整して下さい。

Microsoft 365 パック

DB : 規定外ツールによる DB 操作_110

このイベントは、アカウントがドメインに対するログオンに失敗したときに記録されます。本レポートでは同一アカウントが1日に3回以上、ログオン失敗した場合、レポート出力する設定としています。 ※スローアタックなど、断続的なログオンチャレンジを検知 しい値及びしい値の間隔はお客様環境に合わせて調整して下さい。

FortiGate : ファイル共有サービスへのアップロードサイズ_115

FortiGate : 業務時間外のアクセス監視_116

FS : ランサムウェアによる被害範囲の特定_109

<監査基準/管理要求例> 定期的にアクセス記録の点検を行い、不正アクセスの有無、異常アクセスの有無を確認すること。特に通常時、利用されないアプリケーションなどのアクセスを確認すること。 <確認項目> 規定外ツールによるDBへのアクセスを集計し、レポート。SQLCMDなどを利用し、DBに対する不正アクセスが無いかを確認する。

同一IPのアップロード大量発生をレポートすることで、ポリシー違反行為もしくはリスクの可能性が高い通信を検知します。

勤務時間外などのVPN接続を監視することで、リスクの可能性が高い通信を把握する。

コンピュータウイルス感染、不正アクセスの監視を目的とし、大量のファイル名変更ログを監視します。本レポートでは、1時間あたり100回以上のファイル名変更が行われた際、アラート発報する設定としています。

作成したいレポートをクリック

テンプレートの利用方法について（作成編）

新規作成 - AD : 短時間に大量に行われたログオンチャレンジ_102

状態 ☒ 有効 ☐ 無効

機能 ☒ レポート ☒ アラート ☐ リスクスコアリング

レポート名 AD : 短時間に大量に行われたログオンチャレンジ_102

概要説明

このイベントは、アカウントがドメインに対するログオンに失敗したときに記録されます。本レポートでは同一アカウントが1日に3回以上、ログオン失敗した場合、レポート出力する設定としています。
※スローアタックなど、断続的なログオンチャレンジを検知

出力件数

「制限しない」がONの場合、大量のアクセスログがヒットした際にパフォーマンスが悪化する可能性があります。フィルター条件が厳しく、ヒットするアクセスログが限られているレポートでの利用を推奨します。

クエリでフィルター

フィルター条件を入力してください

項目でフィルター

ユーザー

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

操作一覧

条件1

しきい値

+

3

-

しきい値の間隔

1日

▼

レポート名及び概要説明はお客様環境に応じてわかりやすいよう指定して下さい。

当レポートでは、操作項目にLOGON-Failureを指定しております。

当レポートではしきい値を「3」、しきい値の間隔を「1日」としております。お客様環境に合わせて変更をお願いします。

テンプレートの利用方法について (作成編)

新規作成 - AD: 短時間に大量に行われたログオンチャレンジ_102

状態 ☒ 有効 ☐ 無効

機能 ☒ レポート ☒ アラート ☐ リスクスコアリング

レポート名 AD: 短時間に大量に行われたログオンチャレンジ_102

概要説明 このイベントは、アカウントがドメインに対するログオンに失敗したときに記録されます。本レポートでは同一アカウントが1日に3回以上、ログオン失敗した場合、レポート出力する設定としています。
※スローアタックなど、断続的なログオンチャレンジを検知
しきい値及びしきい値の間隔はお客様環境に合わせて調整して下さい。

出力件数 ☒ 制限しない

「制限しない」がONの場合、大量のアクセスログがヒットした際にパフォーマンスが悪化する可能性があります。フィルター条件が厳しく、ヒットするアクセスログが限られているレポートでの利用を推奨します。

クエリでフィルター

項目でフィルター ユーザー

条件1

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。

[除外する]
複数指定する場合、改行区切りで入力します。

検索

Q プレビュー(レポート) ☒ プロパティ ☐ ファイル出力 ☐ メール通知 ☐ 詳細設定 ☐ 高度な設定

OK キャンセル

現在のレポート定義でどのようなレポート出力が出来るか確認する為に「プレビュー (レポート)」をクリック。



プレビュー

2020/07/01 - 2020/07/31

1件中 1 - 1件

時刻	ユーザー	サーバ	EventID	対象
2020/07/28 14:09:12	PC-2015-09-254.amiya.co.jpSecurity	PC-2015-09-254.amiya.co.jp	1102	S-1-5-21-1608715392-750736408-2091147243-78101minod

レポート定義に問題が無く、該当のログがDBに保存されている場合、レポート結果を確認する事が可能です。

<ご不明な点があればこちらまでお問い合わせ下さい>

MAIL : bv-support@amiya.co.jp

TEL : 03-6822-9910