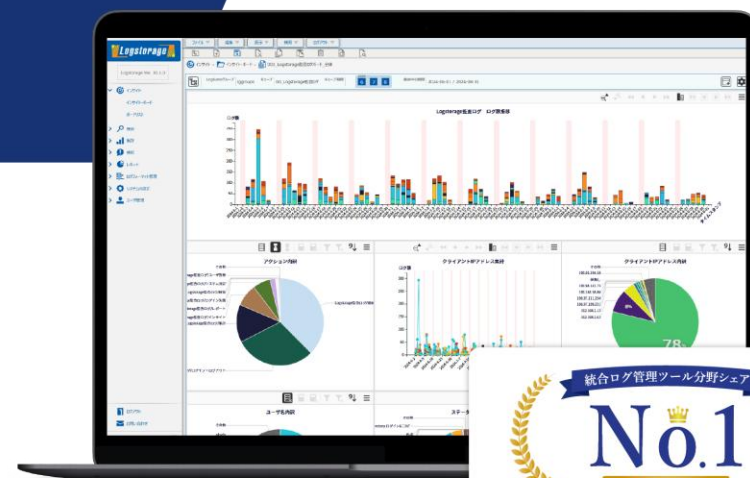


Logstorage

統合ログ管理システム「ログストレージ」

Logstorage Cybereason 連携パック 参考資料



統合ログ管理ツール分野シェア
No.1
18年連続

出典: デロイト トーマツ ミック経済研究所2025年3月発行
内部脅威対策ソリューション市場の現状と将来展望 2024年度 (統合ログ管理ツール部門)
出荷本数でシェア31.2%を獲得 <https://nic-r.co.jp/br/0335/>

Logstorage 連携パックとは

連携パックは、各分野で人気の製品と連携して開発した「ログの収集・分析がすぐにスタートできる」Logstorageのオプション製品です。

連携パックを導入することで、各連携製品のログ管理のセットアップを簡略化できるほか、運用中に、収集対象のログのフォーマット(並び順や表示の仕方)や出力方法に変更があっても、各連携パックのバージョンアップで、変更を反映できます。

「アップデートでログの保管先が変わった」

「出力されるログの内容が変わった」

「保管するログのサイズが増えた」

「仕様変更でログの種類が増えた」

「独自の収集プログラムが
仕様変更で作り直し」



技術者のリソースが
ログ管理に取られすぎる



パッケージ内容

Logstorage 連携パックには、専用のログ収集モジュール・ログフォーマット定義ファイル・分析テンプレートが含まれます。

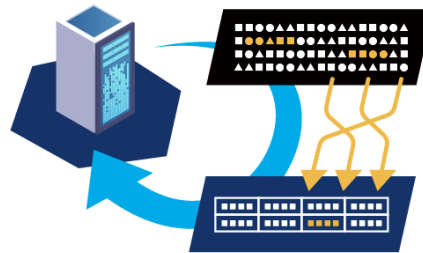
ログ収集モジュール



製品ごとにログの出力方法や出力先は異なります。各製品のログにあわせたログ収集モジュールをご用意しております。

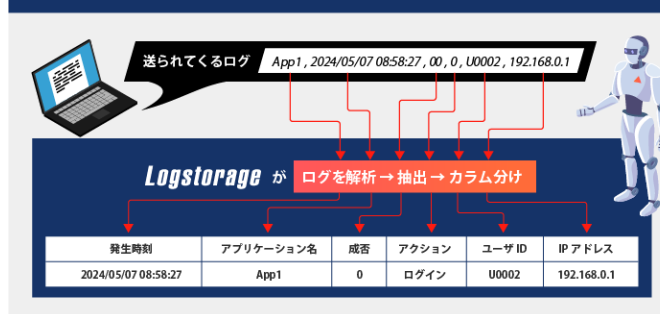
※製品によっては収集モジュールが不要の場合もございます。
その場合、パッケージに含まれませんので、ご了承ください。

ログフォーマット定義ファイル



連携している製品のログフォーマット（並び順や表示の仕方）を分析し、ログを項目ごとに抽出します。

ログフォーマット定義とは？

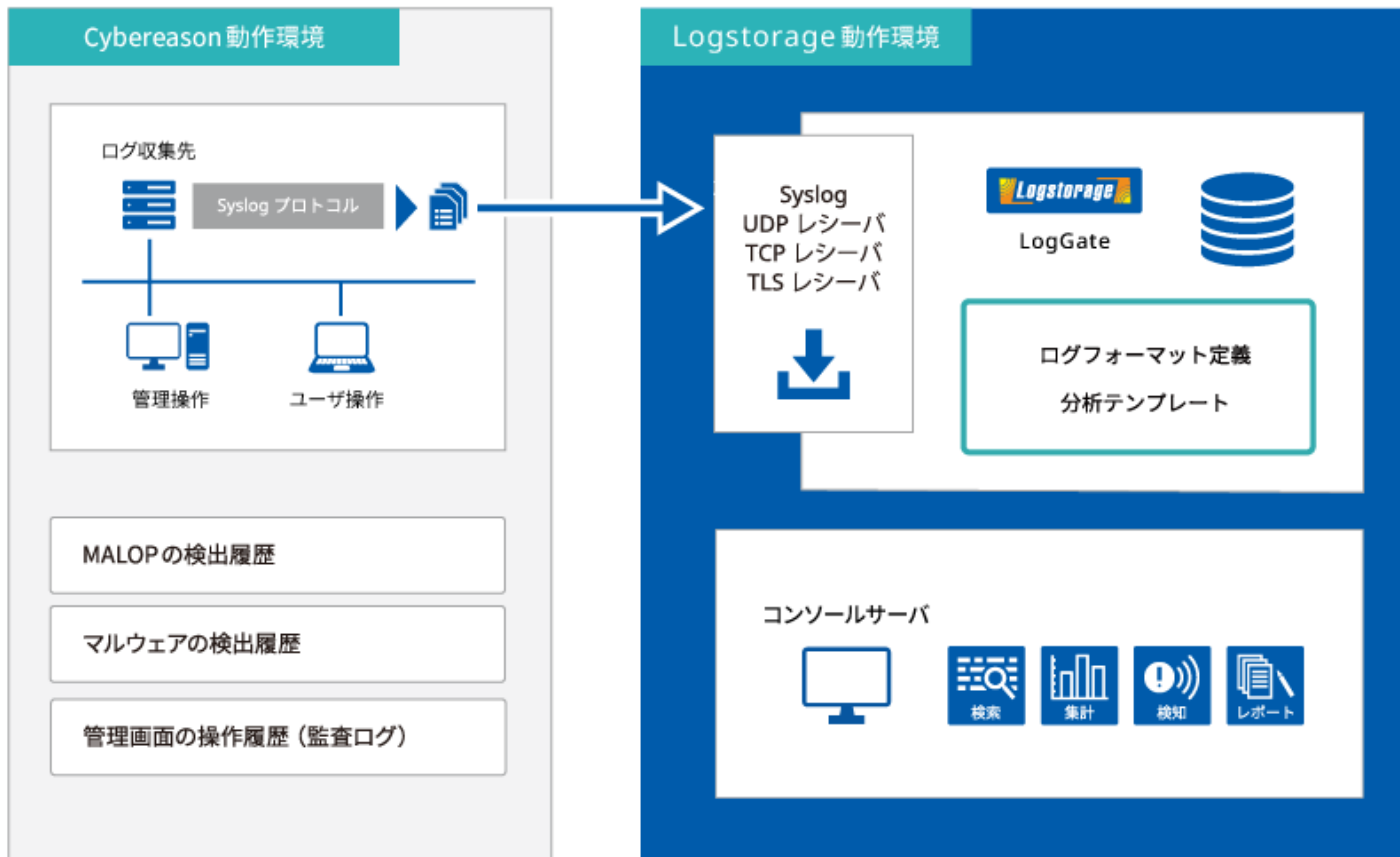


分析テンプレート



各製品から出力される多数のログの中から、どのログを検索すればよいのか・何を集計したらよいのか・どんなレポートを出力すればよいのか、ログ分析をサポートする分析テンプレートをご提供いたします。

システム構成



検索テンプレート一覧

Logstorage Cybereason 連携パック の検索テンプレートは以下の通りです。

ファイル名	検索条件テンプレート名
MALOP	MALOPが検出されたマシン
MALOP	MALOP全ログ
MALOP	初めて検出されたMALOP
MALOP	更新されたMALOP
マルウェア	マルウェア全ログ
マルウェア	新規マルウェアの検出
マルウェア	更新されたマルウェアの検出
マルウェア	検出ステータスのマルウェア
マルウェア	駆除したマルウェア
マルウェア	駆除に失敗したマルウェア
監査ログ	MALOP調査ファイルの取得
監査ログ	リモートシェルによるコマンド実行
監査ログ	リモートジェルの接続
監査ログ	監査ログ全て
監査ログ	管理画面へのログイン

集計・レポートテンプレート一覧

Logstorage Cybereason 連携パック の集計及びレポートテンプレートは以下の通りです。

ファイル名	集計・レポート条件テンプレート名
MALOP	MALOPが検出されたマシン
MALOP	MALOPの新規／更新検出数の推移
MALOP	初めて検出されたMALOP
MALOP	更新されたMALOPの実行元
MALOP	更新されたMALOPの種類
マルウェア	新規マルウェアの検出推移
マルウェア	更新されたマルウェアの検出推移
マルウェア	検出したマルウェア_重大度別
マルウェア	駆除したマルウェア
マルウェア	駆除に失敗したマルウェア
監査ログ	ポリシー変更状況
監査ログ	ユーザごとのログイン失敗件数
監査ログ	ユーザ／接続元IPアドレスごとのログイン失敗件数
監査ログ	リモートシェルによるコマンド実行
監査ログ	リモートシェルの接続

検索例

検索条件名: [Cybereason 20.1]MALOP全ログ										
概要:										
検索条件 検索結果 カラムセットアサイン										
ログ カラム 1-1,000件目表示 (全1,325件) < 1 2 > 表示数: 1000件▼ 拡張トラッキング ログを折り返す										
タイムスタンプ	アクション	Severity	cs1Label	cs1	cn1Label	cn1	cs2Label	cs2	deviceCustomData1Label	
2021-03-30 06:43:45	Malop Machine Information	10	malopId	11.-6943022224392816335	affectedMachinesCount	1	affectedMachine	DESKTOP-HNFCV00	malopUpdateTime	
2021-03-30 06:43:45	Malop Updated	10	malopId	11.-6943022224392816335	affectedMachinesCount	1	malopDetectionType	MALICIOUS_PROCESS	malopCreationTime	
2021-03-30 06:21:32	Malop Machine Information	10	malopId	11.4227166198132201309	affectedMachinesCount	1	affectedMachine	DESKTOP-HNFCV00	malopUpdateTime	
2021-03-30 06:21:32	Malop Updated	10	malopId	11.4227166198132201309	affectedMachinesCount	1	malopDetectionType	PROCESS_INJECTION	malopCreationTime	
2021-03-30 06:09:41	Malop Machine Information	10	malopId	11.-6943022224392816335	affectedMachinesCount	1	affectedMachine	DESKTOP-HNFCV00	malopUpdateTime	
2021-03-30 06:09:41	Malop Created	10	malopId	11.-6943022224392816335	affectedMachinesCount	1	malopDetectionType	MALICIOUS_PROCESS	malopCreationTime	
2021-03-30 00:19:02	Malop Machine Information	10	malopId	11.-7654381878891358490	affectedMachinesCount	1	affectedMachine	DESKTOP-HNFCV00	malopUpdateTime	
2021-03-30 00:19:02	Malop Updated	10	malopId	11.-7654381878891358490	affectedMachinesCount	1	malopDetectionType	KNOWN_MALWARE	malopCreationTime	
2021-03-30 00:19:01	Malop Machine Information	10	malopId	11.-7654381878891358490	affectedMachinesCount	1	affectedMachine	DESKTOP-HNFCV00	malopUpdateTime	
2021-03-30 00:19:01	Malop Created	10	malopId	11.-7654381878891358490	affectedMachinesCount	1	malopDetectionType	KNOWN_MALWARE	malopCreationTime	
2021-03-30 00:19:01	Malop Machine Information	10	malopId	11.-4732597625411635672	affectedMachinesCount	1	affectedMachine	DESKTOP-HNFCV00	malopUpdateTime	
2021-03-30 00:19:01	Malop Created	10	malopId	11.-4732597625411635672	affectedMachinesCount	1	malopDetectionType	KNOWN_MALWARE	malopCreationTime	
2021-03-29 07:18:44	Malop Machine Information	10	malopId	11.4227166198132201309	affectedMachinesCount	1	affectedMachine	DESKTOP-HNFCV00	malopUpdateTime	
2021-03-29 07:18:44	Malop Created	10	malopId	11.4227166198132201309	affectedMachinesCount	1	malopDetectionType	PROCESS_INJECTION	malopCreationTime	
2021-03-29 07:16:34	Malop Machine Information	10	malopId	11.5240990757781037569	affectedMachinesCount	1	affectedMachine	DESKTOP-HNFCV00	malopUpdateTime	
2021-03-29 07:16:34	Malop Created	10	malopId	11.5240990757781037569	affectedMachinesCount	1	malopDetectionType	MALICIOUS_PROCESS	malopCreationTime	
2021-03-25 05:23:05	Malop Machine Information	10	malopId	11.-1123202683924010469	affectedMachinesCount	4	affectedMachine	win-du23veer73g	malopUpdateTime	
2021-03-25 05:23:05	Malop Machine Information	10	malopId	11.-1123202683924010469	affectedMachinesCount	4	affectedMachine	desktop-0oq2rp3	malopUpdateTime	

集計・レポート例 1

MALOPの検出状況やMALOPの影響を受けたマシン情報を確認することができます。

起動タイミング: 定期

範囲: 毎日

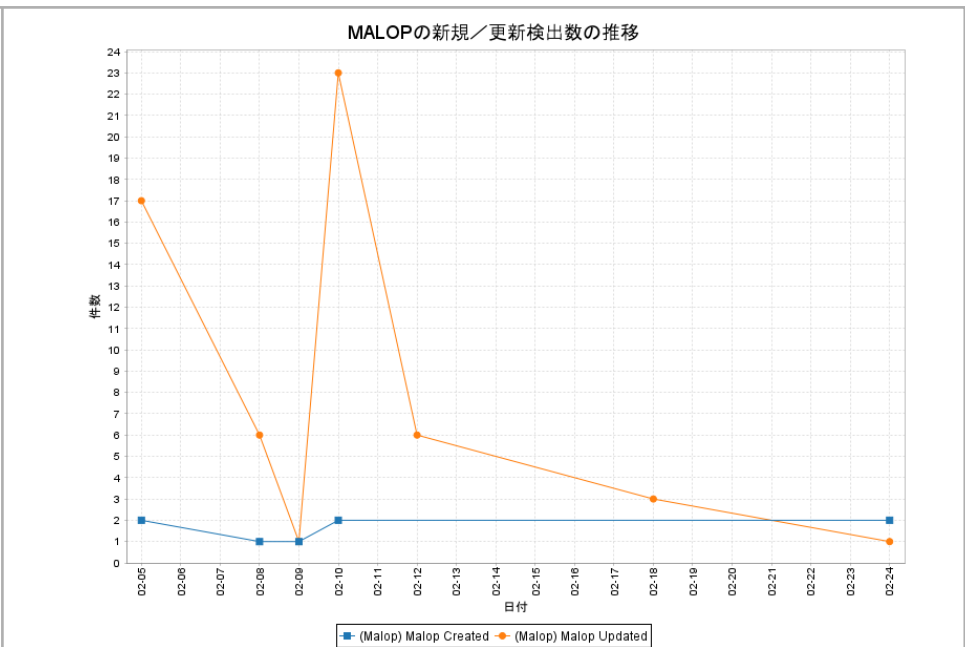
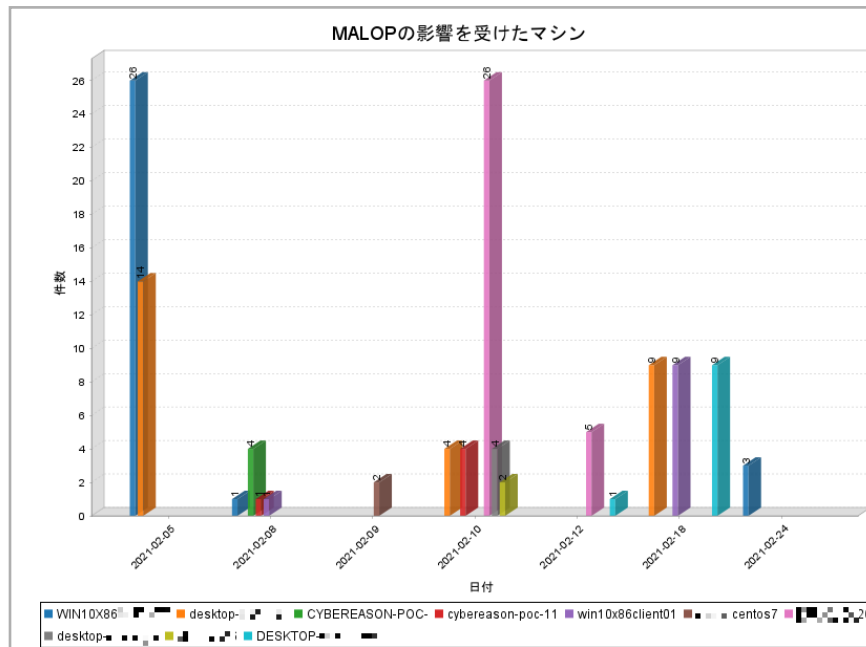
実行時間: 0 時 0 分

対象期間: 1 日間前の 0 時 0 分 0 秒 から 24 時間

プレビュー:

次の実行時間: 2021-04-20(火) 00:00:00

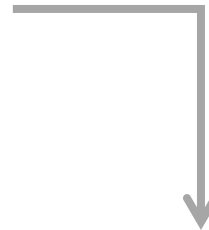
次の実行の対象期間: 2021-04-19(月) 00:00:00 から 2021-04-19(月) 23:59:59 まで



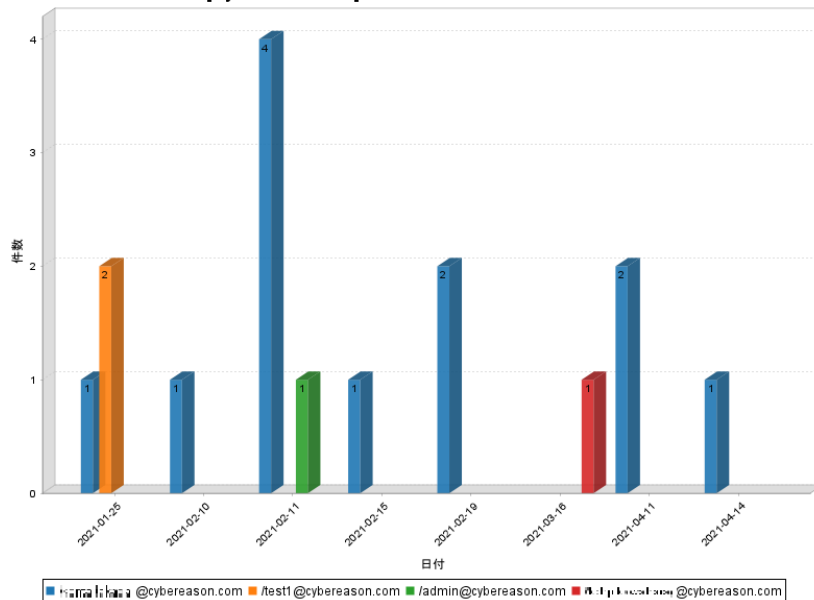
集計・レポート例 2

管理画面へのログインやポリシーの変更状況を確認することができます。

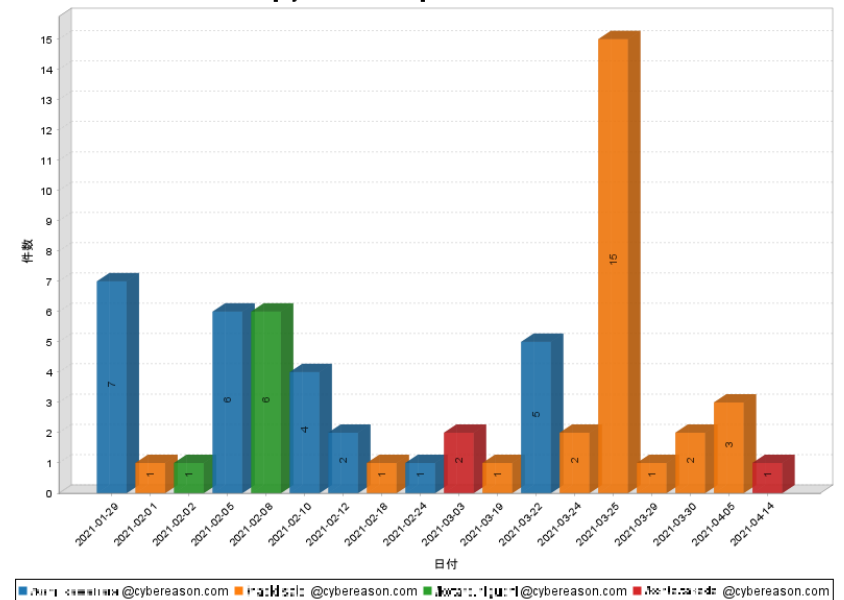
日付	ユーザID	件数
2021-01-25	/admin@cybereason.com	1
	/test1@cybereason.com	2
2021-02-10	/admin@cybereason.com	1
2021-02-11	/admin@cybereason.com	1
	/kanti.kakui@cybereason.com	4
2021-02-15	/admin@cybereason.com	1
2021-02-19	/kanti.kakui@cybereason.com	2
2021-03-16	/kanti.kakui@cybereason.com	1
2021-04-11	/kanti.kakui@cybereason.com	2
2021-04-14	/admin@cybereason.com	1
総合計		16



[Cybereason 20.1]ユーザごとのログイン失敗件数



[Cybereason 20.1]ポリシー変更状況



お問い合わせ

ご不明点、ご相談につきましては、下記お問い合わせ先からご連絡ください。

電話でのお問い合わせ

03-5427-3503

【受付】 平日 9:00～17:30

メールでのお問い合わせ

info@logstorage.com

会社名・氏名・メールアドレス・電話番号を
ご記入の上、お問い合わせください

当社のホームページでも資料請求・お問い合わせができます。

<https://logstorage.com>