統合ログ管理システム「Logstorage」
標的型メール攻撃 分析・監視例

Infoscience

インフォサイエンス株式会社
プロダクト事業部

Infoscience Corporation
www.infoscience.co.jp info@logstorage.com
Tel: 03-5427-3503 Fax: 03-5427-3889

標的型メール攻撃とその対策

標的型メール攻撃の本質はメールや添付マルウェアにあるのではなく、

「攻撃核心は組織への侵入拡大」にあります。これを軸にした対策を施し、

監視手段を提供し攻撃されている事に早期に気づき、

組織判断に繋げる体制を整備する事が最大の防御になります。

- IPA 「標的型メール攻撃」対策に向けたシステム設計ガイド 2013年8月

標的型メール攻撃の特徴

攻撃の特徴

■特定企業や政府組織を標的としたスパイ活動

■標的型メールにより、マルウェアを送り込む手口

■派手でないスパイ活動を長期間執拗に行う

対策上の問題点

■標的型メール攻撃への絶対的なセキュリティ対策は無い

- 実在する上司や取引先の名を語ったメールに添付されたPDFファイル
- 誰か一人でも開けば成功。必ず誰かが開いてしまう。

■侵入したスパイウィルスの検出が難しい

- 新しいパターンのウィルスや、狙った企業内でしか発症しない専門プログラム
- 狙った企業が導入しているウィルス対策ソフトに検出されないことを確認済
- アンチウィルスソフトでは、検出できない

■社内に“人に起因する”セキュリティホール多数存在

- 非管理サーバや消し忘れアカウント、非管理共有、脆弱パスワードなど
- 侵入したウィルスやハッカーに狙われる

【 攻撃の手口 】

攻撃プロセス	攻撃の手口（最近の流行）	攻撃のポイント
情報収集	企業のＩＲ情報や所属協会名簿などの公開情報から実在の人物名を入手	入口
侵入	入手した実在の人物名を語り、仕事を装ったメールを関係者へ送信。誰か一人が開けば成功	
外部連絡	バックドアの確立など、外部との連絡経路を確保し、外部からの指示やマルウェア本体のDL、盗み出した情報の漏洩	出口
拡散	感染したＰＣの権限を利用し、他のＰＣやサーバのセキュリティホールを利用して感染を拡大する	内部
工作活動	企業内の重要な情報や、ID/PASSWORDなどを盗聴する	

対策の考え方

前提条件： **マルウェアは必ず侵入する**

⇒ **マルウェアやハッカーは、既に社内に居る**という前提に立った対策が必須

■ **侵入されても情報を盗まれなければいい**

侵入してもすぐに盗まれるわけではない。何ヶ月、あるいは何年か掛かるケースも！

■ **「入らせない」よりも、侵入したウィルスの拡散防止や、早期発見が現実的かつ本質的な対策**

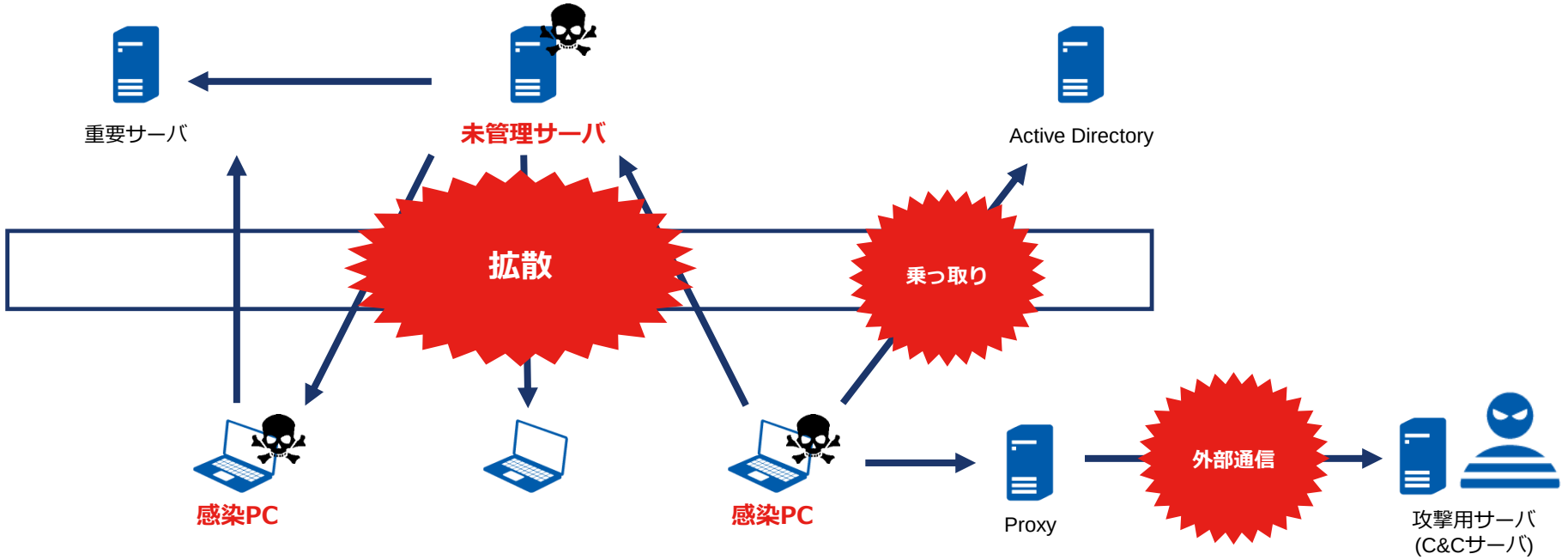
そのためには内部ネットワークの **強化と監視** が重要

監視：多点・多重のログ取得（リアルタイム検出は必ずしも必要ではない）

強化：ポリシー通りの確実な運用を可視化・管理

ログのモニタリングによる対策

侵入したウィルスの拡散防止、早期発見 をログを利用した可視化により実現する



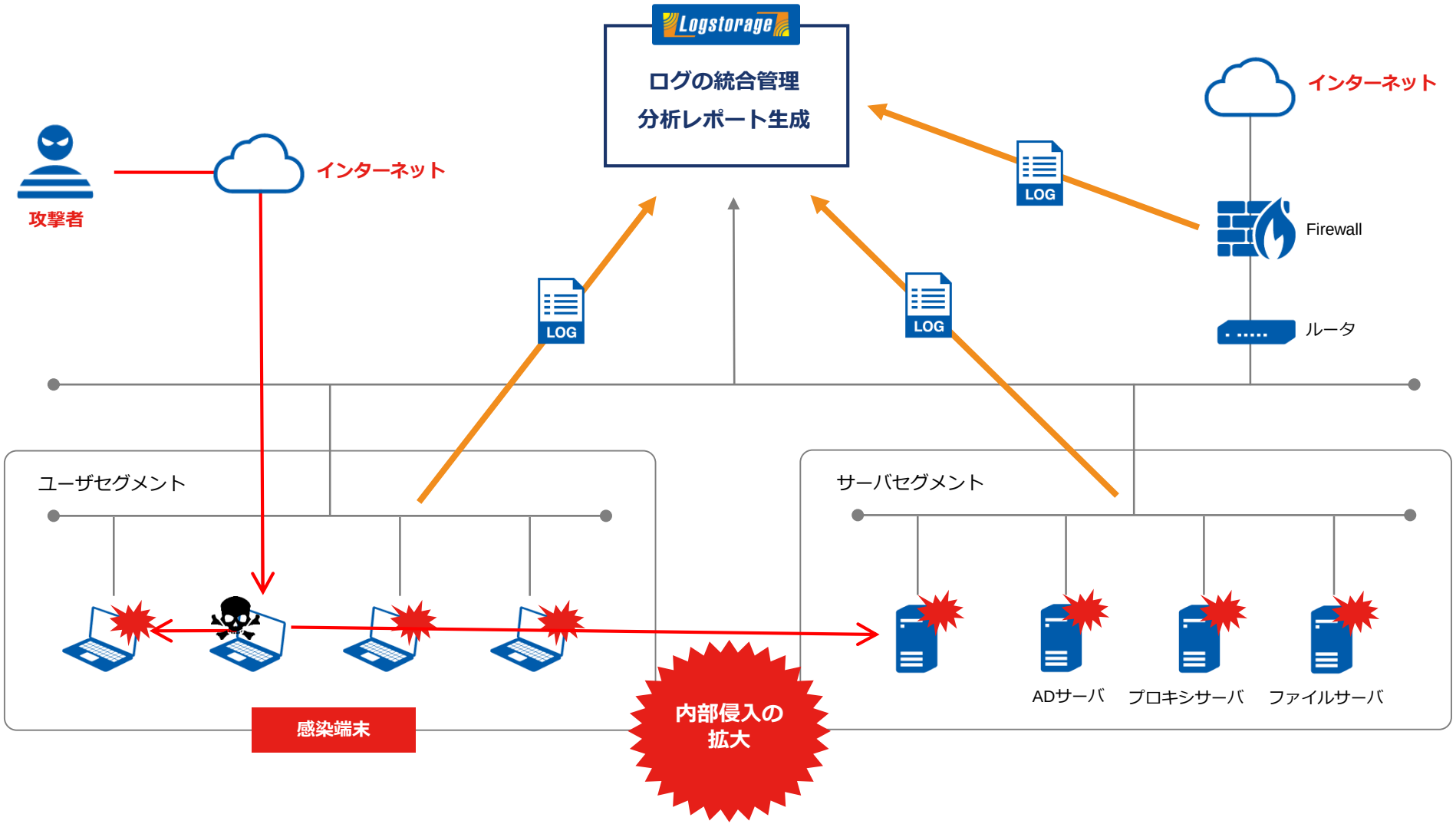
【 ログから見るポイント 】

マルウェア感染後の検知（拡散防止・早期発見）		対象ログ
Active Directory へのログオンアタック	マルウェアは真っ先にActive Directoryの乗っ取りを狙う	ADサーバ
マルウェアの拡散	マルウェアは他のPCやサーバへの拡散（感染）を行う	サーバ/ユーザ端末
外部への情報持ち出し	マルウェアは取得した情報を、外部の攻撃用サーバに送信する	Proxy サーバ
予防的対応		**ログ収集対象**
未管理PC・サーバの抽出	未管理サーバや未使用アカウントはマルウェアに悪用されやすい	サーバ/ユーザ端末
未使用アカウントの抽出		

標的型メール攻撃
対策レポート例

システム構成イメージ

侵入したマルウェアの拡散防止、早期発見 をログを利用した可視化により実現する



対策レポート例①
マルウェア内部拡散検出レポート

マルウェア内部拡散検出レポート概要

侵入したマルウェアの拡散防止、早期検出

【 ログ解析の観点 】

■サーバログ

・サーバが発信元のログ（かつアクセス先がサーバでない）

⇒ **サーバがマルウェアに感染している可能性**

・短時間に大量に「 Logon failuer 」が出ている端末

⇒ **マルウェアに感染したサーバ/ユーザ端末がドメイン アタックをしている可能性**

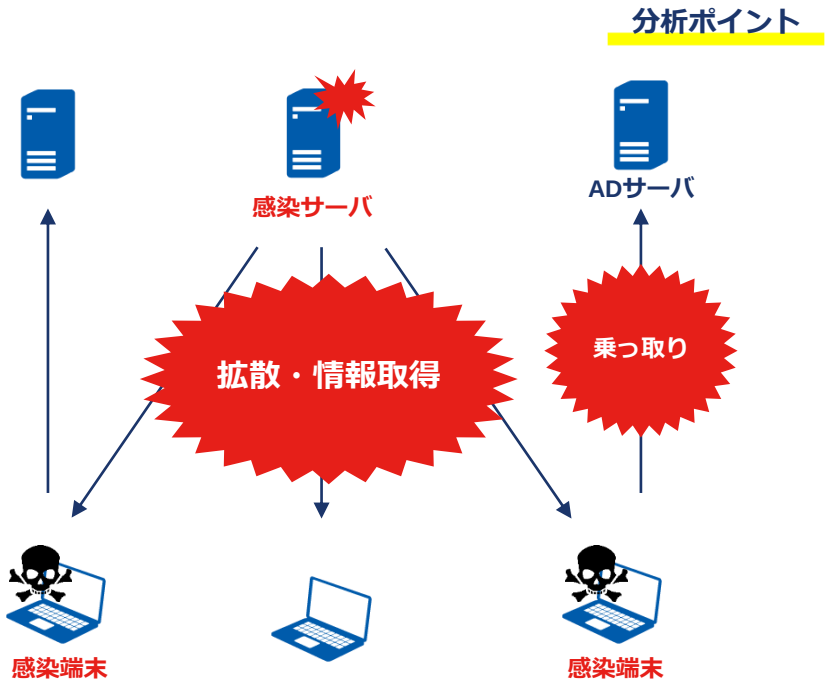
■ユーザ端末ログ

・宛先がサーバでない

・不特定多数のユーザ端末にアクセスしている

・トラップアカウントが使用されている

⇒ **ユーザ端末がマルウェアに感染している可能性**



【 レポート一覧 】

レポート名	レポート内容	ログ取得・分析対象
サーバからクライアントへのアクセス	認証ログ（LogonまたはLogonFailer）の宛先がサーバでないアクセスを発見する。	サーバ
ADへのログオンアタック	クライアント毎のLogOnFailer件数を集計し、大量のアクセス試行を発見する。	サーバ / ユーザ端末
クライアントからクライアントへのアクセス	宛先がサーバでないアクセスを発見する。	ユーザ端末
不特定多数へのアクセス	クライアント毎のアクセス先件数を集計し、大量のアクセス試行を発見する。	ユーザ端末
トラップアカウントを利用したアクセス	企業内の重要な情報や、ID/PASSWORDなどを盗聴する	ユーザ端末

対策レポート例②
マルウェア外部通信検出レポート

マルウェア外部通信検出レポート概要

マルウェアの外部通信を検出

【 ログ解析の観点 】

■ファイアウォールログ

・プロキシサーバを経由しないアクセス

⇒ **接続元端末がマルウェアに感染している可能性**

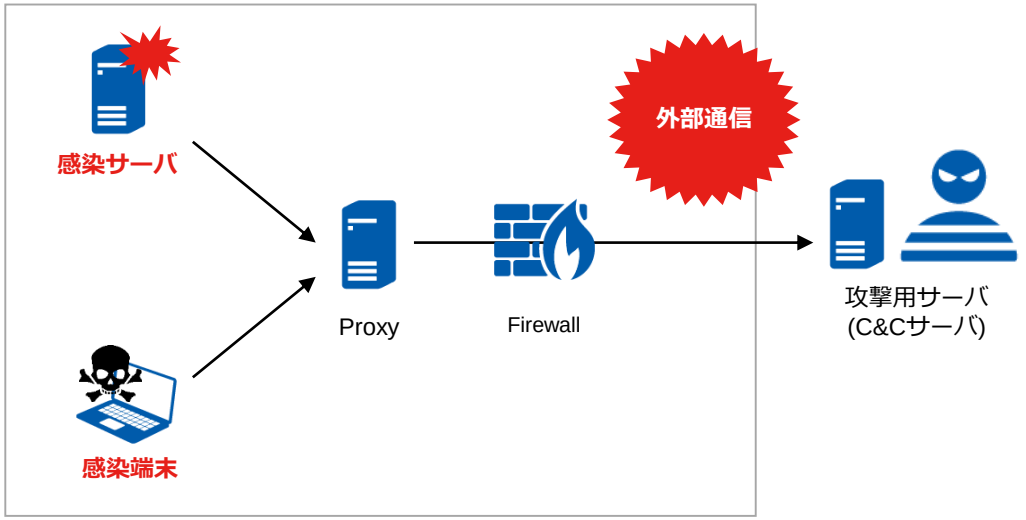
■プロキシサーバログ

・短時間に大量にプロキシサーバへの認証に失敗している端末

・コネクトバック通信を行っている端末

⇒ **接続元端末がマルウェアに感染している可能性**

分析ポイント



【 レポート一覧 】

レポート名	レポート内容	ログ取得・分析対象
ファイアウォール遮断ログ	Proxyサーバを経由せず、直接外部に80,443ポートで通信を行おうとしたユーザ端末を発見する。	ファイアウォール
プロキシサーバへの認証失敗	Proxyサーバの認証ログを分析し、コネクトバック通信の予兆を発見する。	プロキシサーバ
コネクトバック(*)通信	プロキシサーバ経由の通信を一度切断し、強制切断時に発生するログから、C&Cサーバへの再接続を行うコネクトバック通信を発見する。	プロキシサーバ

(*)コネクトバック： 侵入者がコンピュータへ侵入する時の通信方式として、侵入者側ではなくコンピュータ側が接続元となって通信を発し、それに応答する形で侵入者がコンピュータに接続し、侵入すること。
主に侵入者がファイアウォールをすり抜けるために用いられる。

対策レポート例③

ITデータ棚卸レポート

ITデータ棚卸レポート概要

狙われやすい 未使用アカウント 、非管理PC・サーバ を検出

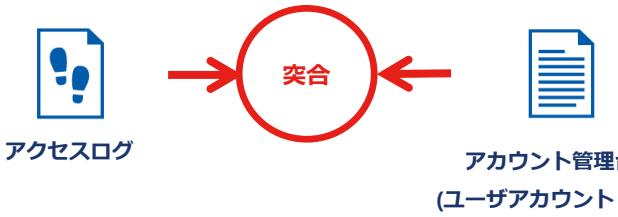
【 ログ解析の観点 】

■アクセスログと各種台帳／マスタ

・管理台帳とアクセスログを突合せ、未使用アカウント、
非管理サーバ、PCを検出。

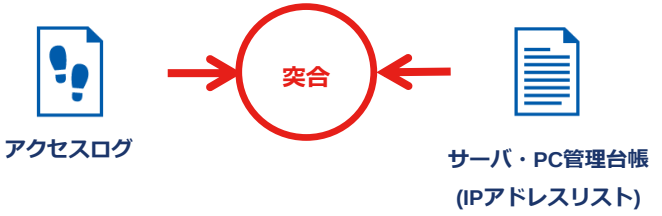
⇒ **未使用アカウント、非管理サーバは不正に利用され易い**

分析ポイント



指定期間中、一度も使用されていないアカウントがある！

＜未使用アカウント抽出レポート＞



管理台帳にないPC・サーバへのアクセスがある！

＜非管理サーバ・PC抽出レポート＞

【 レポート一覧 】

レポート名	考えられるリスク	レポート内容
未使用アカウント抽出レポート	退職者アカウントなど、未使用アカウントの利用。	管理台帳とアクセスログを突合せ、未使用アカウントを抽出。
非管理PC・サーバレポート	社内に許可無く設置されたサーバ、PCのウィルス感染。	管理台帳とアクセスログを突合せ、非管理PC・サーバを抽出。

レポートイメージ

マルウェア行動検出レポートサンプル

レポートイメージ

サーバからクライアントへのアクセス

概要　サーバからクライアントへのアクセス履歴を出力する
作成日　2012-05-15 03:30:03
対象期間　2012-05-14 00:00:00 - 2012-05-14 23:5959

検索条件名	サーバからクライアントへのアクセス	
概要	サーバからクライアントへのアクセス履歴を出力する	
タイムスタンプ	サーバIPアドレス	クライアントIPアドレス
2012-05-14 05:55:31	10.0.0.1	192.168.0.1
2012-05-14 06:30:02	10.0.0.1	192.168.0.2
2012-05-14 06:55:14	10.0.0.1	192.168.0.3
2012-05-14 07:10:55	10.0.0.1	192.168.0.10

非管理アカウント抽出レポート

概要　アカウント管理台帳とアクセスログを突合せ、非管理アカウントを抽出する
作成日　2012-05-15 03:35:42
対象期間　2012-05-14 00:00:00 - 2012-05-14 23:5959

検索条件名	非管理アカウントを抽出する	
概要		
サーバIPアドレス	ユーザID	
10.0.0.1	admin0	
10.0.0.1	yamada01	
10.0.0.1	testuser	
10.0.0.2	yamada01	

クライアントからクライアントへのアクセス

概要　クライアントからクライアントへのアクセス履歴を出力する
作成日　2012-05-15 03:35:42
対象期間　2012-05-14 00:00:00 - 2012-05-14 23:5959

検索条件名	クライアントからクライアントへのアクセス	
概要	クライアントからクライアントへのアクセス履歴を出力する	
タイムスタンプ	クライアントIPアドレス（接続元）	クライアントIPアドレス（接続先）
2012-05-14 14:55:31	192.168.0.100	192.168.0.1
2012-05-14 15:30:02	192.168.0.100	192.168.0.2
2012-05-14 15:55:14	192.168.0.100	192.168.0.3
2012-05-14 17:10:55	192.168.0.100	192.168.0.10

非管理サーバ・PC抽出レポート

概要　PC管理台帳とアクセスログを突合せ、非管理サーバ・PCを抽出する
作成日　2012-05-15 03:35:42
対象期間　2012-05-14 00:00:00 - 2012-05-14 23:5959

検索条件名	非管理サーバ・PCを抽出する	
概要		
タイムスタンプ	IPアドレス	
2012-05-14 14:55:31	10.0.0.100	
2012-05-14 15:30:02	10.0.0.101	
2012-05-14 15:55:14	10.0.0.102	

開発元

インフォサイエンス株式会社
〒108-0023
東京都港区芝浦2-4-1 インフォサイエンスビル
https://www.infoscience.co.jp/

お問い合わせ先

インフォサイエンス株式会社
プロダクト事業部
TEL 03-5427-3503　　FAX 03-5427-3889
https://logstorage.com/
mail : info@logstorage.com