

01 Amiya Corporation



Company info

Company Name	AMIYA Corporation
Incorporated	December 1996
Location	Head Office Tornare Nihombashi Hamacho 11F 3-3-2 Nihombashi Hamacho Chuo Tokyo
	Osaka Office Sapporo Institute
Representatives	Chairman: Seiichi Ito CEO: Kouta Ishida
Employees	146
Main Business Activities	<p>< Data Security Division ></p> <ul style="list-style-type: none">• Development of security audit tools / Sales / Implementation Support Consulting• IT control construction / Internal audit / Report creation / Operation support• Construction for information security management / Inspection、 Support <p>< Network Security Division ></p> <ul style="list-style-type: none">• System infrastructure evaluation / Consulting / Design / Construction / Operation• Network security system consulting / Design / Construction / Operation• Network security system • service development / Sales

Vision

SECURE THE SUCCESS.

2 Security Business

Automate security for

Information

Data
Security

Automate security for

Network

Network
Security

キーコンセプトは、

「**?** 難しいを💡かんたんに」

Product planning

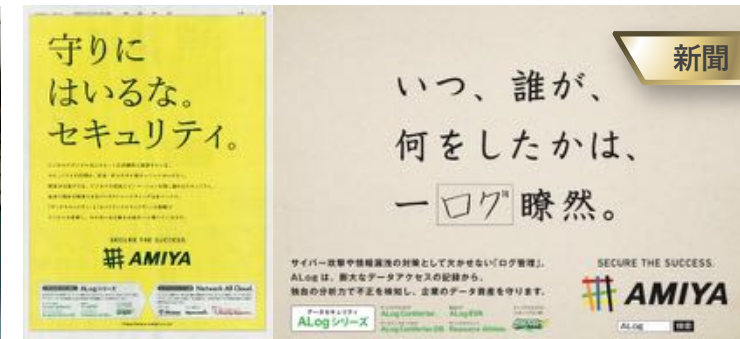
R&D

Product Development

Promotion

Sales

Completed in-house from planning,
development and sales
ま・自社完結



AMIYA's global business

Operational monitoring on Server access
ALog **Con**Verter®



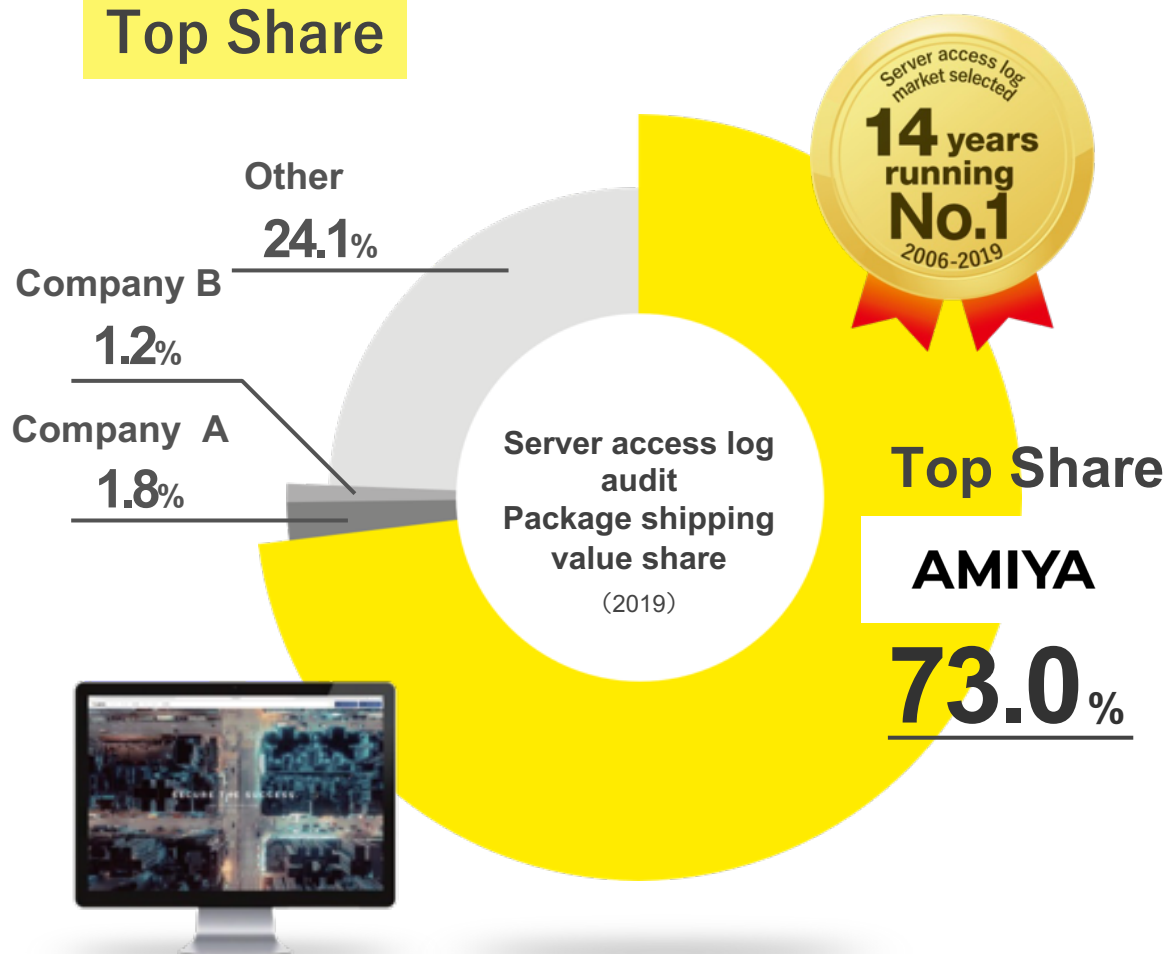
- AMIYA Taiwan corporation
- Overseas partners :
14 partners in 10 countries.

Taiwan, US, UK, China, Thailand, Vietnam, Hong Kong, Singapore, Indonesia, Malaysia

02 Data Security Business

Log Management

Top Share



Source : Deloitte Tohmatsu MIC Research Institute Co., Ltd.
Current Status and Future Prospects of the Internal Threat Countermeasure
Solution Market 2020" Published in December 2020

More than

5,100 Contract


Manufacturing

Over

1300



Finance, insurance

Over

1000



Telecommunications

Over

1000



Service

Over

600



Construction industry, real estate industry

Over

380




Public Service group

Over

380



ALog ConVerter.®
ALog EVA

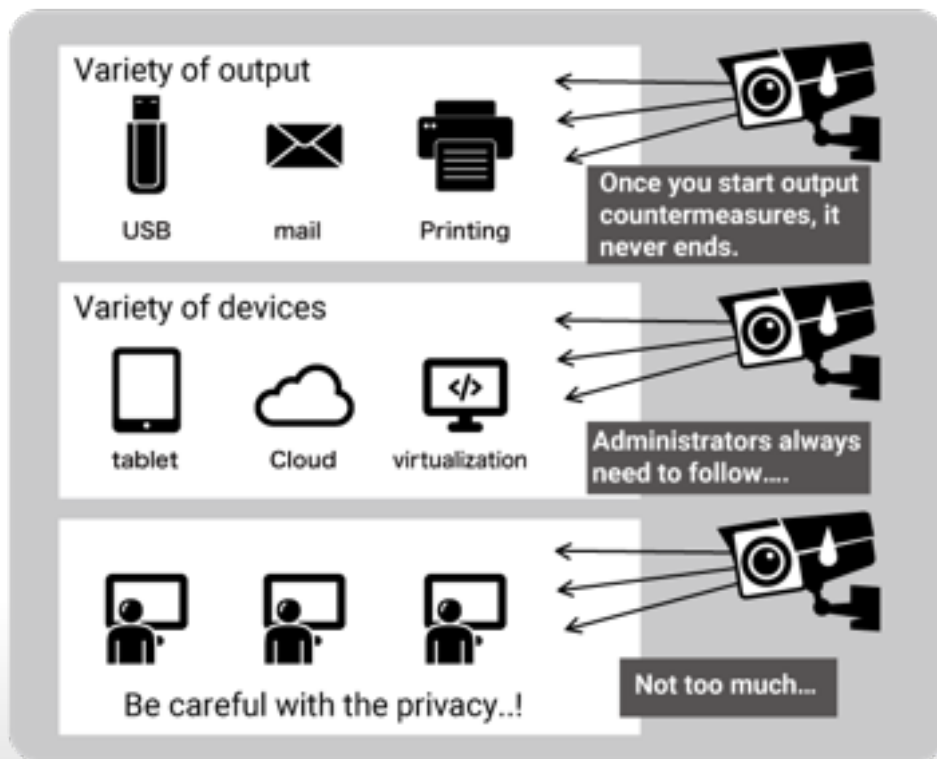
The image features a central composition where a yellow folder, filled with white papers, sits atop a white, three-tiered pedestal. Surrounding this central element are six white, bullet-style surveillance cameras mounted on black brackets, all angled towards the folder. The background is a solid, dark grey. A semi-transparent horizontal band across the middle of the image contains the text.

Watch Your **Data,
Not Your Employees**

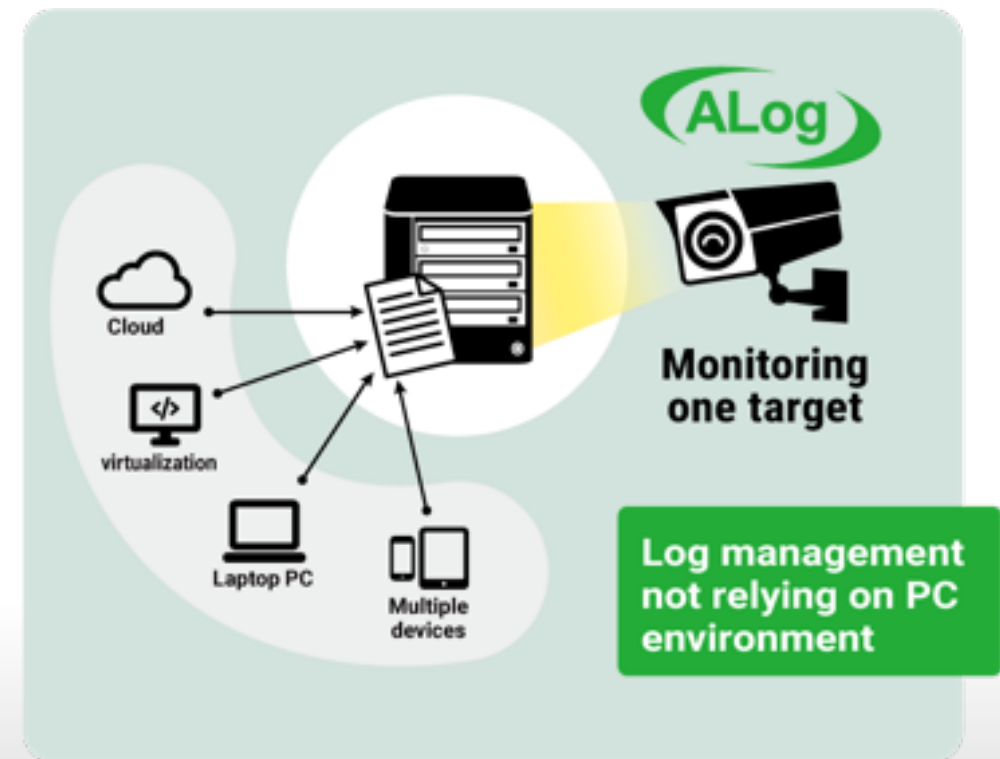
Focus your monitoring target to the vital data

PC asset management ; such as monitor employee's internet browsing and device control is needless to say important. However you need to consider the long term trouble and strain on systems operations, maintenance and high cost. ALog monitors and analyzes users' access to servers and databases at the server level that stores all the critical data, which means greatly effective.

Client PC control/ Monitor



Server data Monitor



Wide range support of ALog

The Advantage of ALog is its wide range support that is able to gather not only operation log for Windows file server but also various records such as Linux/NAS storage server OS log, database application log, syslog from network.



Are user's operation records traceable by raw log data?!

Example: An employee Steve 『**opened**』 an excel file and 『**modified**』 it.
Log data should be indicated as 『**READ**』 and 『**WRITE**』.

Raw log data...

10/25/2011 13:34:10	Microsoft-Windows-Security-Auditing	AUDIT_SUCCESS	Something4656N\YNS-08R2SP1	S-1-5-21-4117455682-877842489-1775433442-001\testuser\YNS-08R2SP1\0x2ba450\Security\File\E:\DATA\client info\customerlist.xls	0x1024\{00000000-0000-0000-0000-000000000000}\%1541 %4416 %4423	%1541: %1801 D:(A;OICI;FA;;;WD) %4416: %1801 D:(A;OICI;FA;;;WD) %4423: %1801 D:(A;OICI;FA;;;WD)	/0x100081/-/0/0x4//
---------------------	-------------------------------------	---------------	----------------------------	---	---	---	---------------------

Accurate action history
can not be taken with
raw log data



Even it's sorted...

E:\DATA\client info\customerlist.xls	READ
E:\DATA\client info\customerlist.xls	READ
E:\DATA\client info\customerlist.xls	WRITE
E:\DATA\client info\customerlist.xls	DELETE
E:\DATA\client info\customerlist.xls	WRITE
E:\DATA\client info\customerlist.xls	READ
E:\DATA\client info\customerlist.xls	READ
E:\DATA\client info\customerlist.xls	WRITE
E:\DATA\client info\customerlist.xls	READ
E:\DATA\client info\customerlist.xls	READ
E:\DATA\client info\customerlist.xls	READ
E:\DATA\client info\customerlist.xls	WRITE
E:\DATA\client info\customerlist.xls	READ
E:\DATA\client info\customerlist.xls	READ
E:\DATA\client info\customerlist.xls	WRITE

READ - 25 lines?
WRITE - 8 lines?
DELETE - 1 lines??

Even after the mapping,
it doesn't show the
actual operation.



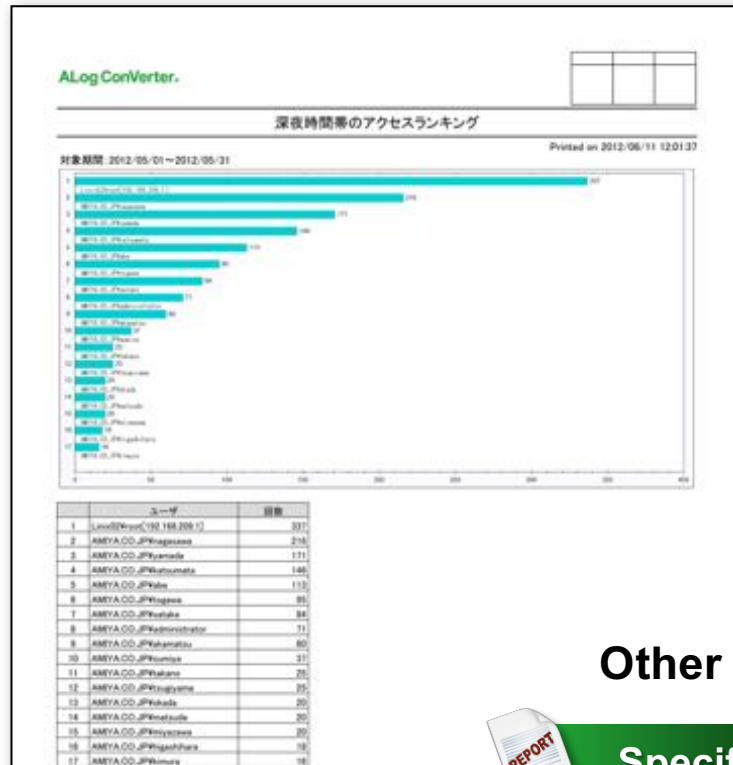
User	File	Operation
Steve	E:\DATA\client info\customerlist.xls	READ
Steve	E:\DATA\client info\customerlist.xls	WRITE

Steve 『**opened**』 the file and 『**wrote**』

Analyzed and converted into
the actual operation history



Access Ranking for Night Hours



Access record to the important folders

ALog ConVerter.

特定プロジェクトのフォルダアクセス履歴

対象期間: 2010/04/01 ~ 2010/04/30 Printed on 2010/12/01 9:40:20

対象件数: 16件

No	日時	ユーザ	パス	操作
1	2010/04/01 10:15:12	AMYA.CO.JP@nada	D:\プロジェクト\XX\顧客情報\技術一課管理情報.xls	READ
2	2010/04/01 10:15:12	AMYA.CO.JP@nada	D:\プロジェクト\XX\顧客情報\技術二課管理情報.xls	READ
3	2010/04/01 10:15:12	AMYA.CO.JP@nada	D:\プロジェクト\XX\顧客情報\技術三課管理情報.xls	READ
4	2010/04/01 10:15:12	AMYA.CO.JP@nada	D:\プロジェクト\XX\顧客情報\技術一課ライセンス情報.xls	READ
5	2010/04/01 10:15:12	AMYA.CO.JP@nada	D:\プロジェクト\XX\顧客情報\技術二課ライセンス情報.xls	READ
6	2010/04/01 10:15:12	AMYA.CO.JP@nada	D:\プロジェクト\XX\顧客情報\技術三課ライセンス情報.xls	READ
7	2010/04/01 10:15:12	AMYA.CO.JP@nada	D:\プロジェクト\XX\顧客情報\販売管理一課.xls	READ
8	2010/04/01 10:15:12	AMYA.CO.JP@nada	D:\プロジェクト\XX\顧客情報\顧客管理一課.xls	READ
9	2010/04/01 10:15:12	AMYA.CO.JP@nada	D:\プロジェクト\XX\顧客情報\顧客管理一課.xls	READ
10	2010/04/01 14:00:00	AMYA.CO.JP@nada	D:\プロジェクト\XX\顧客情報\技術二課管理情報.xls	READ
11	2010/04/01 14:00:00	AMYA.CO.JP@nada	D:\プロジェクト\XX\顧客情報\技術二課ライセンス情報.xls	READ
12	2010/04/01 20:00:00	AMYA.CO.JP@nada	D:\プロジェクト\XX\顧客情報\顧客管理一課.xls	READ
13	2010/04/01 20:00:00	AMYA.CO.JP@nada	D:\プロジェクト\XX\顧客情報\2004年度経費報告.xls	READ
14	2010/04/01 00:00:00	AMYA.CO.JP@ngsusa	D:\プロジェクト\XX\顧客情報\新規開発事業部管理情報.xls	READ
15	2010/04/01 00:00:00	AMYA.CO.JP@ngsusa	D:\プロジェクト\XX\顧客情報\地域企業事業部管理情報.xls	READ
16	2010/04/01 00:00:00	AMYA.CO.JP@ngsusa	D:\プロジェクト\XX\顧客情報\ネットワーク事業部管理情報.xls	READ

Other report...

Specific folders' data deletion

Schedule Retirees Access

Several times log-on failure

Authorized user's operation

- Mail Service
- Syslog notification
- API link

Chatwork slack

TEAMS など

ALog ConVerter is a tool to obtain access history of the vital data without re-siding any agent.
You can have low cost and efficient log management as ALog ConVerter collects log data from the server side where the vital data is stored.



Analyze law log, To the actual operation

ALog's conversion engine creates a clear story of actual user actions that tells you the Who, the When, and the What about file accessed, based on the complex raw logs.



日時	ユーザー	サーバ	対象	操作
2015/3/12 15:04:50	amiyaKawasaki	amiya001	D:\fsvol\W企画部\作業中\WY13事業計画.doc	WRITE
2015/3/12 20:04:03	amiyaYamai	amiya001	D:\fsvol\W経理部\給与計算\4月給与明細_途中.xls	READ
2015/3/12 22:34:23	amiyaNakayama	amiya001	D:\fsvol\W営業部\顧客管理\製品別購入一覧.xls	DELETE



Automatic Super compact

ALog's conversion engine log compress even more the minimized access and store.
Super compact means you can keep a large amount of data for a long period of time.



Intuitive Search/Analyze

Intuitive search by using Web browser.
Not only for IT manager, Anybody can easily operate.



Reason to be selected

Only ALog can **respond to both internal fraud and external attacks**

If you do not comprehensively handle information leakage / audit response / cyber attack detection, it will be a wasteful diversified investment.



ALog ConVerter®

Audit Purpose

Internal fraud

File operation



ALog EVA

Cyber Attack

Trouble Shooting

Cloud Service Operation

ALOG UNIQUENESS

- 1) Less than third the price of other SIEM software in the market with awesome quality (Japanese quality standard).
- 2) For users with existing other SIEM software, ALog can co-exist with other SIEM, thereby customers can benefit of paying less and enjoy double protection.

ALOG UNIQUENESS

- 3) Reachable time-zone for support services.
- 4) Dedicated support personnel assigned. NOT unknown, virtual "issue-ticket" support with no specific personnel assigned.

ALOG UNIQUENESS

- 5) Comprehensive Internal Fraud and External Attack Protection in one platform and single sign-in.
- 6) Advanced, Patented Log Compression technology that allows logs to be stored and retrieved efficiently

ALOG UNIQUENESS

- 7) Raw logs can be easily readable, understandable and visualised by non-technical end users.
- 8) Simple to use search engine makes auditing, emergency incident cases identification and management reporting very fast to accomplish.

A record that surpasses memory



AMIYA

Amiya Global Sales Unit
 Asako Yonezawa
 Mail: as-yonezawa@amiya.co.jp
<https://www.amiya.co.jp/english/>