



### 取扱説明書

### 第3A版

alm(anti-information leak monitor) は、ネットワーク監視を目的として開発したシステムです。

昨今、インターネットを利用する場面が多く、インターネット環境無しでは 仕事に支障をきたします。ただ、インターネットを利用する場合、ウィルスや 情報漏洩というセキュリティー面に関し脆弱となる可能性が高く、この問題の 対応がせまられております。特定の有名なウィルスに関してはアンチウィルス ソフトを導入する事で、ほぼ対応が可能です。ただ、特定の企業をターゲット としたピンポイント・ウィルスにおいて、そこから情報漏洩に繋がったりする 可能性は無いとは言い切れません。また、数台のPCならともかく、数十台の コンピューターを1台1台検査する手間は膨大なものになります。

almはLAN網に流れている通信データを24時間逐次監視を行い、特定の キーワードが発見されるとログ記録、メール通知を行います。どこのPCから どこへ情報が流れてしまったか発見することが可能です。発見後は、送信元の コンピューターの調査を行い問題を解決し、送信先のサイト等へのアクセスを 遮断してしまえば、その後問題はなくなります。

このようなネットワークデータをモニタリングするフリーソフトウェアや、 大手セキュリティ対策企業が提案しているもありますが、導入する為のコスト、 工数、知識、メンテナンス等がネックとなり、なかなか手が付けられないと

いう実情があるかと思われます。

本ネットワーク監視システムは、セキュリティ関連の強化と、対費用効果が望まれるシステムとして開発しました。

HK Corporation. All rights reserved.

- 2 -

【利点・仕様】

- ・LANとWAN間に挟まれないので通信データの負荷がかかりません。
- ・ブラウザ、メールの内容のみという分けでは無く、HTTP、FTP、POP3、SMTP
   等のプロトコルに対応。平文データIP通信であればTCP、UDPも両方
   監視可能。
- ・登録された特定のキーワードが通信上に現れるとログ記録やメール通知できます。
- ・キーワードが送信されたPCのネットワーク接続を著しく阻害できます。
- ・キーワード登録、メールアドレス登録、ログ管理等はブラウザ上で簡単に
   管理できます。
- ・ログは、送信元 I P アドレス、送信先 I P アドレス、送信先ホスト名、 検知キーワード、検知日時等を保存しE X C E L データで管理できます。
- ・検知可能なネットワーク機器のIP、ホスト名の一覧を表示可能。不正な 機器の強制阻害可能。ネットワーク機器台帳としてEXCELデータを 出力し管理できます。
- ・100% pure java で作成されたアプリケーションの為、WindowsやLinux上 でも動作可能です。

・平文データのみの監視です。セキュア通信(SSL、https等)、ZIP等の中身、 WORD, EXCELなどの文章の内容は監視できません。



HK Corporation. All rights reserved.

- 4 -





- a 1 mシステム ・OS:Windows XP Pro以降、Linux(CentOS等) ・Pentium Core2 Duo 3.0GHz以上、メモリ 4GByte以上(最低スペック) ・SUN Java JDK6
  - ・WWWサーバー TOMCAT 6.x
  - ・データベース MS Access、MySQL、PostgreSQL、JavaDB等

●クライアント数 最大250台程度(almシステムPCのスペックによります)

- 5 -

●L3 Switching HUB、若しくはL2 Switching HUB ・ポートミラーリング機能がある機器





ネットワーク監視を行う主要処理。DBに登録されているキーワードをネット ワーク上で検知するとDBに登録されているメールアドレス情報を元に送信、 DBへログ出力。

●管理システム・プロセス キーワード、メールアドレスの入力を行う。ログの管理や監視モニタの状態把握等 を行う。

- 6 -





localhost へ接続		<u>? ×</u>
almSystem のサー/ 。	iー localhost にはユーザー名とパスワ	ワードが必要です
警告: このサーバーは することを要求してい	、ユーザー名とパスワードを安全では ます (安全な接続を使わない基本的	ない方法で送信 な認証)。
ユーザー名(山)	😰 alm	•
パスワード( <u>P</u> )	(XXXXXXX)	
	マ パスワードを記憶する( <u>R</u> )	
	ОКЛ	キャンセル
	1 22 1	

管理システムはブラウザ(IE6以上を奨励)より操作を行います。 ブラウザを起動しURLの部分に、

http://監視システムPCのIPアドレス:8080/almManage と入力します。

するとログインする為のユーザー名とパスワードを入力するダイアログが 表示されますので、ユーサー名を「alm」にし、パスワードを入力して OKボタンを押します。alm管理メニュー画面が表示されます。

- 8 -

※パスワードを記憶するにチェックを入れない事をお勧めします。



🌽 alm管理メニュー – Windows Internet Explorer	A DESCRIPTION OF TAXABLE PARTY.		
C ← I ← Ittp://localhost:8080/almManage/system		💽 🔄 🗙 Live Search	
] ファイル(E) 編集(E) 表示(Y) お気に入り(A) ツール(D)	ヘルプ(日)	10565	
		j 💁 • 🖾	* 🖶 • 🗗 • 🎯 • 🎽
	alm ネットワーク監視システム alm管理メニュー		*
	キーワード入力		
	メールアドレス入力		
	口グ表示		
	防御状況表示		
	IPテーブル表示		
	ステータス表示		
	設定画面		
			-
ページが表示されました		-	100% 👻

【alm管理メニュー画面】

- ・キーワード入力ボタンを押下すると、キーワード入力画面へ遷移します。
- ・メールアドレス入力ボタンを押下すると、メールアドレス入力画面へ遷移します。

- 9 -

- ・ログ表示ボタンを押下すると、ログ表示画面へ遷移します。
- ・防御状況表示ボタンを押下すると、防御状況表示画面へ遷移します。
- ・IPテーブル表示ボタンを押下すると、IPテーブル表示画面へ遷移します。
- ・ステータス表示ボタンを押下すると、ステータス表示画面へ遷移します。
- ・設定画面ボタンを押下すると、設定画面へ遷移します。



(E) ;	(点) まデ(い) お使(こうわ(か) いーリ	L(T) A (1=9(L))				1074-54402-5441		
xD .	##(E) まい(E) 55((こ)()(E) 55) キーワード入力					🟠 • 🖻	) • 🖶 • 🖻	} <b>-</b> 6
		2 ネットワーク!! キーワー	か 盗視システ 一ド入力	<mark>ـــ</mark> ـ				
ュー(語 る文字	₹る 「列林記入してください。最大120文字まで	<u> </u>	୭					
~~; *	(等の特殊記号は監視できません)	· • 🍟		im 중録				
	(1)			lich 755 2003				
No	(1) 監視キーワ	- 「/ 」 ///通知 フード	<u> </u>	通知	防御	変更	nu Ba	
<b>No</b>	(1) 監視キーワ [dummy_file	<u>^</u> -ル通知 <b>ノード</b>	4	道知 回りのみ 💽	防御	<b>変更</b> 変更	削除	
<b>No</b> 1 2	(1) 「dummy_file 陳密情報ファイル	)-F	4	道知 ログのみ メール通知 ・	防御	<b>変更</b> 変更 変更	<b>削除</b> 削除 削除	
No 1 2 3	し	<b>)−k</b>	4	道知	防御	<b>変更</b> 変更 変更 変更	削除           削除           削除           削除	
No 1 2 3 4		<b>) — k</b>	4	通知 回びのみ ▼ メール通知 ▼ ロびのみ ▼ マール通知 ▼	防御     「     □     □     □     □     □     □     □     □     □     □	<b>変更</b> 変更 変更 変更 変更	前時余           前時余           前時余           前時余           前時余           前時余	
No 1 2 3 4 5		)- <b>k</b> .		通知     「ログのみ ▼     「ハール通知 ▼     「ハール通知 ▼     「ハール通知 ▼     「ハール通知 ▼     「ハール通知 ▼		<b>変更</b> 変更 変更 変更 変更 変更 変更	<b>削除</b> 削除 削除 削除 削除	
No 1 2 3 4 5 6		)- <u>k</u>		通知     「ログのみ ▼     「フグのみ ▼     「フグのみ ▼     「メール通知 ▼     「フグのみ ▼     「フグのみ ▼     「瓦グのみ ▼     「衣示のみ ▼	略初 マ ロ マ マ マ マ	<b>変</b> 更 変更更 変更更 変更更 変更更 変更更 変更更	削除           削除           削除           削除           削除           削除           削除           削除           削除	

- 【キーワード入力画面】
  - ・メニューに戻るボタンを押下すると、メニュー画面へ遷移します。
  - ・①は新規に追加したい監視するキーワードを入力します。
  - ・②は下記3つの項目を選択します。

表示のみ : 監視モニター上のログ画面のみに表示します。

ログのみ : 監視キーワードを検知したらログのみ記録します。

メール通知:監視キーワードを検知したらログ記録とメール通知します。

- ・③はキーワードが検出されたら流出したPCをネットワーク防御します。
- ・登録ボタンを押下すると新規キーワードを登録します。
- ④は既に登録されているキーワードを表示し、変更や削除を行います。
   変更:キーワード、通知、防御を変更し、変更ボタンにて更新します。
   削除:該当キーワードを削除します。削除する旨のダイアログで
   「はい」ボタンを押下すると削除します。



JL(E	- 編集(E) 表示(V) お気に入り(A	) ツール(D ヘルプ(H)		
3	∕€ メールアドレス入力		<b>} •</b> 🖾 • 🖷	• 🛃 • 🤇
22	<mark>ネット</mark> メー	<b>名加 ワーク監視システム</b> ールアドレス入力		
する。	メールアドレスを入力してください。 ドレス]	[名前] ①	登録	
する. ルア <b>No</b>	メールアドレスを入力してください。 ドレス] <b>メールアドレス</b>	[名前] ① ② 名前	登録       変更	削除
する. ルア 1	メールアドレスを入力してください。 ドレス] <b>メールアドレス</b> [yamada@aaa.jp	[名前] ① ② 名前 山田課長	登録 <b>変更</b>	<b>削除</b> 削除
する. ルア 1 2	メールアドレスを入力してください。 ドレス] メー <b>ルアドレス</b> [yamada@aaa.jp [i_suzuki@xxxxx.co.jp	[名前] ① ② 名前 山田課長 〕 節木	登録       変更       変更       変更       変更	<b>削除</b> 削除 削除
する. ルア 1 2 3	メールアドレスを入力してください。 ドレス] yamada@aaa.jp [i_suzuki@xxxxx.co.jp [sato_keitai@bbbbb.ne.jp	[名前] ① ② 〇 〇 〇 〇 〇 〇 〇 〇 〇 〇 〇 〇 〇 〇 〇 〇 〇 〇	登録           変更           変更           変更           変更           変更	<b>削除</b> 削除 削除 削除

- 【メールアドレス入力画面】
  - ・メニューに戻るボタンを押下すると、メニュー画面へ遷移します。
  - ①は新規に追加したいメールアドレスと誰のメールアドレスか認識する為の名前 を入力します。
  - - 変更:該当メールアドレス・名前を変更した後、変更ボタンを押下すると 変更します。 削除:該当キーワードを削除します。削除する旨のダイアログで
      - 削除:該当キーワードを削除します。削除する旨のダイアログで 「はい」ボタンを押下すると削除します。



-	or windows internet cxpit					
E	🕽 👻 🙋 http://localhost:8080/a	ImManage/system		<ul> <li>★ Live Search</li> </ul>		
P-11	√E) 編集(E) 表示(⊻) お気(;	:入り(白) ツール(D ヘルプ(日)				
द्वि	🏉 ログ表示			🗇 • 6	3 * 🖶	• 🗗 🎯
		<b>2</b> ネットワークリ ログ	<b>か</b> 素視システム 表示			
<u>×=</u>	ユーに戻る					
EXC	жына 1 ~	* VVVV/\\\/DD#/=	で指定			
EXC		※ YYYY/MM/DD形式	で指定 atke			
EXC 範囲	迷し出力 見ログクリア 」 「 一 ~ 「 ~ 「 ~ 「 ~ 「 ~ 「 ~ 「	※ YYYY/MM/DD形式	で指定。			
EX( 範囲 全音	ンEL出力 / ~/ <u>1ログクリア / </u> ~/ 豚ログクリア /	※ YYYY/MM/DD形式	で指定			
EX( 範囲 全部	CEL出力 / ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~	※ YYYY/MM/DD形式 ※ YYYY/MM/DD形式 送信先	で指定 で指定 <b>キーワード</b>	日時	防御	Mail
EX( 範囲 全部	CEL出力 / ~ / 引ログクリア / ~ / 野口グクリア / 野口グクリア / 送信元 192.168.0.152 M1210	※ YYYY/MM/DD形式 ※ YYYY/MM/DD形式 送信先 114.111.71.185 asprov06.search.vip.kks.yahoo.co.jp	で指定 で指定 <b>キーワード</b> 監視用ファイル	日時 2010/01/29 12:42:23	防御無	Mail
EX( 範囲 全部 1 2	CEL出力 ~ ヨログクリア ~ 野ログクリア ~ 野ログクリア ~ 「 野口でクリア ~ 「 ジョン・ 「 ジョン・ 「 ジョン・ ジョン・ ジョン・ ジョン・ ジョン・ ジョン・ ジョン・ ジョン・ ジョン・ ジョン・ ジョン・ ジョン・ ジョン・ マー ~ 「 ・ 「 ・ 「 ・ 「 ・ 「 ・ 「 ・ 「 ・ 「 ・ 「 ・ 「 ・ 「 ・ 「 ・ 「 ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	※ YYYY/MM/DD形式 ※ YYYY/MM/DD形式 ※ YYYY/MM/DD形式 114.111.71.185 asprov06.search.vip.kks.yahoo.co.jp 124.83.187.219 beacon01.search.vip.ogk.yahoo.co.jp	で指定 で指定 <u>キーワード</u> 監視用ファイル 監視用ファイル	日時 2010/01/29 12:42:23 2010/01/29 12:42:26	防御 無 無	Mail 無
EX( 範囲 全部 1 2 3	DEL出力 / ~ / 引口グクリア / ~ / 掛口グクリア / 掛口グクリア / 超信元 192.168.0.152 M1210 192.168.0.152 M1210 192.168.0.152 M1210	※ YYYY/MM/DD形式 ※ YYYY/MM/DD形式 114.111.71.185 asprov06.sarch.vip.kks.yahoo.co.jp 124.83.187.219 beacon01.search.vip.ogk.yahoo.co.jp 124.83.141.29 bo30.logs.vip.ogk.yahoo.co.jp	で指定 で指定 <b>キーワード</b> 監視用ファイル 監視用ファイル 監視用ファイル	日時 2010/01/29 12:42:23 2010/01/29 12:42:26 2010/01/29 12:42:27	防御 無 無	Mail 無 無
EX( 範囲 全部 1   2   3   4	CEL出力 回ログクリア 原ログクリア 第ログクリア 送信元 192,168.0,152 M1210 192,168.0,152 M1210 192,168.0,152 M1210 192,168.0,152 M1210	※ YYYY/MM/DD形式 ※ YYYY/MM/DD形式 ※ YYYY/MM/DD形式 114.111.71.185 asprov06.search.vip.kks.yahoo.co.jp 124.83.187.219 beacon01.search.vip.ogk.yahoo.co.jp 124.83.181.29 be03.logs.vip.ogk.yahoo.co.jp 203.216.243.211 wrs2.search.vip.trz.yahoo.co.jp	で指定 で指定	日時 2010/01/29 12:42:23 2010/01/29 12:42:26 2010/01/29 12:42:27 2010/01/29 15:32:28	防御 無 無 有	Mail 無 無
EX( 範囲 全部 10 2 3 4 5	DEL出力 ~ 回口グクリア ~ 第ログクリア ~ ~ 第ログクリア ~ 第ログクリア ~ 第ログクリア ~ 第ログクリア ~ 第ログクリア ~ 第ログクリア ~ 第ログクリア ~ 第ログクリア ~ 第ログクリア ~ 第ログ ~ 第ロ~ 第四~ 第二~ 第二 第二 第二 第二 第二 第二 第二 第二	※ YYYY/MM/DD形式 ※ YYYY/MM/DD形式 ※ YYYY/MM/DD形式 114.111.71.185 asprov06.search vip kks yahoo.co.jp 124.83.187.219 beacon01.search vip ogk yahoo.co.jp 124.83.141.29 bo30.loss vip ogk yahoo.co.jp 203.216.243.211 wrs2.search.vip.trz.yahoo.co.jp 192.168.0.152 M1210	で指定 で指定 <b>キーワード</b> 監視用ファイル 監視用ファイル 監視用ファイル dummy_file dummy_file	日時 2010/01/29 12:42:23 2010/01/29 12:42:26 2010/01/29 12:42:27 2010/01/29 15:32:28 2010/01/29 15:32:28	防御 無 無 有 有	Mail 無 無 無
EX( 範囲 全部 1 2 3 4 5	DEL出力 ~ 回口グクリア ~ 第ログクリア ~ ~ 第ログクリア ~ ~ ~ 第ログクリア ~ ~ 第ログクリア ~ ~ ~ 第ログクリア ~ ~ ~ ~ 第ロ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~	※ YYYY/MM/DD形式 ※ YYYY/MM/DD形式 ※ YYYY/MM/DD形式 114.111.71.185 asprov06 search vip kks yahoo co.jp 124.83.187.219 beacon01 search vip ogk yahoo co.jp 124.83.141.29 be30.logs vip ogk yahoo co.jp 203.216.243.211 wrs2.search.vip thz yahoo co.jp 192.168.0.152 M1210 124.147.43.196	で指定 で指定 <b>キーワード</b> 監視用ファイル 監視用ファイル 監視用ファイル dummy_file dummy_file	日時 2010/01/29 12:42:23 2010/01/29 12:42:26 2010/01/29 12:42:27 2010/01/29 15:32:28 2010/01/29 15:32:28 2010/01/29 15:32:28	<b>防御</b> 無 無 有 有	Mail 無 無 無

【ログ表示画面】

- ・メニューに戻るボタンを押下すると、メニュー画面へ遷移します。
- ・ログは送信元と送信先の I P アドレス、ホスト名、何のキーワードを検知したか、 検知日時、ネットワーク防御の有無、メール送信の有無を表示します。
- ・EXCEL出力ボタンを押下すると、全ログをEXCEL形式で出力します。 ファイルのダウンロード・ダイアログが表示されます。開くを選択すると EXCELが起動しログが表示されます。保存を選択するとファイルとして保存 できます。※管理 P C 側にEXCELやOpenoffice.org Calc等をインストール していないと表示されません。
- 指定した日付範囲で出力できます。未入力の場合、全ログを出力します。
- ・範囲ログクリアは指定日付の範囲のログのみ削除します。
- ・ログクリアボタンを押下すると、ログを消す旨のダイアログが表示されますので、 「はい」を選択すると全ログをデータベース上から全削除します。

HK Corporation. All rights reserved.

- 12 -



2010年01日26日13時32公日1

8	771N(E)	編集(E) 表示(V)	挿入(1) 書式( <u>0</u> ) ツール( <u>1</u> ) データ( <u>D</u>	) ウィンドウ(W) ヘルナ	(H)		質問を入力	してください	2 - 1	5 ×
	÷ 🖬 🕯	a na la la 💖 🛛	x 🖻 🖻 + 🍼   10 - 10 - 🙀 )	Σ • ≜↓ ⅔↓ 🛍 🗛	100% • 🕐 MS 明朝	• 10 • B I U = =	= <b>A 9</b> % , % (		ð - A	• »
Ca M	9: Microsoft Office Live (活動する 間K・ 保存・									
i ca m										
-	FID	▼ 7× 0	Jummy_ne		-	-		2.2		
-	A	В	C	D	E.	F	G	H	I.	<b>_</b> _
1							1	-1.0-		
2	NO	発信元IP	発信元ホスト名	発信先 I P	発信先ホスト名	キーワード	日時	防御	メール	
3	1	192.168.0.152	M1210	203.216.227.249	wrs.search.vip.tnz.yahoo.co.jp	dummy_file	2010/01/25 17:23:49	無	無	
4	2	203.216.227.249	wrs.search.vip.tnz.yahoo.co.jp	192.168.0.152	M1210	dummy_file	2010/01/25 17:23:53	<u></u>	黒	-
5	3	192.168.0.152	M1210	203.216.231.214	gamma.search.vip.tnz.yahoo.co.jp	dummy_file	2010/01/25 17:23:58		黒	
6	4	192.168.0.152	M1210	124.83.187.219	beacon01. search. v ip. ogk. yahoo. co. jp	dummy_file	2010/01/25 17:24:02		二	
1	5	192.168.0.152	M1210	124.147.46.5	bsU2.logs.vip.kcd.yahoo.co.jp	dummy_file	2010/01/25 17:24:07		黒	
8	6	192.168.0.152	M1210	203.216.231.214	gamma.search.v1p.thz.yahoo.co.jp	dummy_file	2010/01/25 17:28:23	<u></u>	二二 二	
9	7	192.168.0.152	M1210	124.83.187.219	beacon01. search. vip. ogk. yahoo. co. jp	dummy_Tile	2010/01/25 17:28:28	無	無	
10	ŏ	192.168.0.152	M1210	124.147.46.5	bsUZ.logs.vip.kcd.yahoo.co.jp	dummy_file	2010/01/25 17:28:32		二二 二	
11	9	192.168.0.152	M1210	203.216.227.249	wrs.search.vip.tnz.yahoo.co.jp	dummy_Tile	2010/01/25 17:31:44	無	無	
12	10	203.216.227.249	wrs.search.vip.tnz.yahoo.co.jp	192.168.0.152	M1210	dummy_file	2010/01/25 17:31:48		二二 二	- 1
13	11	192.168.0.152	M1210	203.216.231.214	gamma.search.vip.tnz.yahoo.co.jp	dummy_file	2010/01/25 17:31:53		黒	_
14	12	192.168.0.152	M1210	124.83.187.219	beacon01. search. vip. ogk. yahoo. co. jp	dummy file	2010/01/25 17:31:58	<u></u>	二	
15	13	192.168.0.152	M1210	124.147.46.5	bsU2.logs.vip.kcd.yahoo.co.jp	dummy file	2010/01/25 17:32:02		黒	_
10	14	192.168.0.152	M1210	203.216.227.249	wrs.search.vip.tnz.yahoo.co.jp	dummy_file	2010/01/25 17:32:10		二	_
1/	15	203.216.227.249	wrs.search.vip.tnz.yahoo.co.jp	192.168.0.152	M1210	dummy_file	2010/01/25 17:32:14	悪	黒	
18	16	192.168.0.152	M1210	203.216.231.214	gamma.search.vip.tnz.yahoo.co.jp	dummy_file	2010/01/25 17:32:19	悪	悪	_
19	17	192.168.0.152	M1210	124.83.187.219	beacon01. search. vip. ogk. yahoo. co. jp	dummy_file	2010/01/25 17:32:23	悪	黒	
20	18	192.168.0.152	M1210	124.147.48.5	bs02.logs.vip.kcd.yahoo.co.jp	dummy_file	2010/01/25 17:32:28	悪	悪	_
21	19	192.168.0.152	M1210	203.216.227.249	wrs.search.vip.tnz.yahoo.co.jp	dummy_file	2010/01/25 17:32:32	潕	黒	
22	20	203.216.227.249	wrs.search.vip.tnz.yahoo.co.jp	192.168.0.152	M1210	dummy_file	2010/01/25 17:32:37	無	黒	
23	21	192.168.0.152	M1210	203.216.231.214	gamma.search.vip.tnz.yahoo.co.jp	dummy_file	2010/01/25 17:32:41	悪	無	
24	22	192.168.0.152	M1210	124.83.187.219	beacon01. search. vip. ogk. yahoo. co. jp	dummy_file	2010/01/25 17:32:46	無	無	
25	23	192.168.0.152	M1210	124.147.46.5	bs02.logs.vip.kcd.yahoo.co.jp	dummy_file	2010/01/25 17:32:50	無	無	
26	24	192.168.0.152	M1210	203.216.227.249	wrs.search.vip.tnz.yahoo.co.jp	dummy_file	2010/01/25 17:32:55	無	無	
27	25	203.216.227.249	wrs.search.vip.tnz.yahoo.co.jp	192.168.0.152	M1210	dummy_file	2010/01/25 17:32:59	無	黒	
28	26	192.168.0.152	M1210	203.216.231.214	gamma.search.vip.tnz.yahoo.co.jp	dummy_file	2010/01/25 17:33:04	無	無	-
14 4	N N	heet1/Sheet2/Sheet	3/	104 00 107 010	here and an and the second	dimensi fila	1 0010701705 17:00:001	-	<b>**</b>	
図形の	D調整(R)	- は オートシェイプ(U)	• 🔪 🗆 🔿 🔛 🖪 📣 🔅 🛛	8 🔜 🔕 - 🔟 - 🛆	·==:::::::::::::::::::::::::::::::::::					
ועדב	-						1 1 1	NUM		11.

※ EXCEL出力し表示したイメージ



🌈 ネットワーク防御材	況表示 - ₩	'indows Internet Explorer			
😋 🕘 👻 🙋 ht	tp://localhost	:8080/almManage/system		😽 🗙 Live Search	P-
」ファイル(E) 編集(J	5) 表示(⊻)	お気に入り( <u>A</u> ) ツール(① ヘル	プ( <u>H)</u>		
אפג 🚳 🔹 😫	フーク防衛科大沢	很表示		<u>0</u> • 5 •	🖶 • 🗗 🎯• 🞯•
<u>۲۵۵-۲۵</u>	1	<u>ネッ</u>			<u></u>
	- Net	Rtanozela	全防御停止	Pt: 御信. L	
	1	192.168.0.153	2010/01/13 13:30:10	停止	
	2	192.168.0.154	2010/01/13 13:31:06	停止	
	3	192.168.0.150	2010/01/13 13:32:48		
	<u>.</u>				
ページが表示されました					100% +

【防御状況表示画面】

- ・メニューに戻るボタンを押下すると、メニュー画面へ遷移します。
- ・ネットワーク防御しているPCの一覧を表示します。
- ・ 全防御停止ボタンを押下すると、現在防御している全PCの防御を解除します。
- 各項目にある停止ボタンを押下すると、その項目にあるPCの防御を解除します。

- 14 -



😔 🔻 🙋 htt	p://localhost	:8080/almManag	;e/system			• +	X Live Sear	ch	
(ル( <u>E</u> ) 編集( <u>E</u>	) 表示(火)	お気に入り(A)	ツール(J)	ヘルプ(日)					
🔉 🏾 🏉 Pī-	ブル表示						J	<b>⊡</b> • <b>□</b> •	•••
				ネットワー IPテー	///// ク監視システム -ブル表示				
ニューに戻る	ſ								
XCEL出力					ーブル削除				-15
XCEL出力		IP7Fレス			ーブル削除		LIST削除	強制防御	
XCEL出力		<b>IPアドレス</b> 192.168.0.1			ーブル削除 ホスト名 MEBIUS		LIST <b>削除</b>	<b>強制防御</b> 防御	
XCEL出力		<b>IPアドレス</b> 192.168.0.1 192.168.0.150	)		ーブル削除 ホスト名 MEBIUS HP2133		LIST削除 削除 削除	<b>強制防御</b> 防御 防御	
XCEL出力		<b>IPアドレス</b> 192.168.0.1 192.168.0.150 192.168.0.152	)		ーブル削除 ホスト名 MEBIUS HP2133 M1210		LIST削除 削除 削除 削除	<b>強制防御</b> 防御 防御 防御	
XCEL出力		<b>IPアドレス</b> 192.168.0.1 192.168.0.152 192.168.0.28	2		ーブル削除 ホスト名 MEBUS HP2133 M1210 M1210		LIST削除 削除 削除 削除 削除	強制防御           防御           防御           防御           防御           防御           防御           防御	
XCEL出力		<b>IPアドレス</b> 192.168.0.150 192.168.0.152 192.168.0.152 192.168.0.28 192.168.0.37	2		ーブル削除 ホスト名 MEBIUS HP2133 M1210 M1210 LUC2		LIST削除           前10余           前10余           前10余           前10余           前10余           前10余	強制防御           防御           防御           防御           防御           防御           防御           防御	
XCEL出力		<b>IPアドレス</b> 192.168.0.1 192.168.0.152 192.168.0.28 192.168.0.37 192.168.0.37	) 2 8		<ul> <li>ブル削除</li> <li>ホスト名</li> <li>MEBIUS</li> <li>HP2133</li> <li>M1210</li> <li>M1210</li> <li>LUC2</li> <li>Lucretia</li> </ul>		LIST前除           前時           前時           前時           前時           前時           前時           前時	強制防御           防御           防御           防御           防御           防御           防御           防御           防御           防御	
XCEL出力		<b>ІР7ГЬ 2</b> 192.168.0.1 192.168.0.150 192.168.0.152 192.168.0.37 192.168.0.37 192.168.0.7 192.168.1.7	2		ーブル削除 ホスト名 MEBIUS HIP2133 M1210 M1210 LUC2 LUC2		LISTŇI ŇIFA ŇIFA ŇIFA ŇIFA ŇIFA ŇIFA	強制防御           B方御	
KCEL出力		IP7FL2 192.168.0.1 192.168.0.150 192.168.0.152 192.168.0.28 192.168.0.37 192.168.0.7 192.168.1.7 192.168.1.7	) 2 2		ーブル削除 ホスト名 MEBIUS HP2133 M1210 M1210 LUC2 LUC2 LUCRETJ		LISTŘIJ ŘIJFA ŘIJFA ŘIJFA ŘIJFA ŘIJFA ŘIJFA ŘIJFA	強制防御           防御           防御	

- 【IPテーブル表示画面】
- ・メニューに戻るボタンを押下すると、メニュー画面へ遷移します。
- ・検知できたPCのIPアドレスとホスト一覧を表示します。
- ・ホスト名に---かIPアドレスがそのまま表示されてしまう場合がありますが、 これは、そのPCの電源がOFFになっているか名前解決できなかった場合です。
- ・EXCEL出力ボタンを押下すると、全ログをEXCEL形式で出力します。 ファイルのダウンロード・ダイアログが表示されます。開くを選択すると EXCELが起動しログが表示されます。保存を選択するとファイルとして保存 できます。※管理PC側にEXCELやOpenoffice.org Calc等をインストール していないと表示されません。
- ・全IPテーブル削除ボタンを押下すると、IPテーブル一覧を全消去します。
- ・削除ボタンを押下すると、IPテーブル一覧より選択したPCを削除します。
- ・防御ボタンを押下すると、選択したPCのネットワーク接続を強制的に著しく 阻害します。(約1時間防御します)※但し、防御は慎重に行ってください。

# 管理システム9

🔀 Mic	rosoft Exc	cel - IPTBL2010年01月29日16時03	纷[1] xls		
图 7	77イル(E) 新	編集(E) 表示(Y) 挿入(I) 書式(Q)	ツール(D) データ(D) ウィンドウ(	W) ヘルプ(H) 質問を入力してください	) 8 ×
	÷ 🖬 🔒	•2	1 × · · · · · · · · · · · · · · · · · ·	100% 🔹 🗊 🚛 🔳 📃 🔹	A -      A
193 M	icrosoft Offi	ce Live (ご移動する   開く +   保存 + 🖕			
	C13	<b>→</b> <i>f</i> ×			
	A	В	C	D	E
1			IPテーブル表		
2	No	IP	HOST		
3	1	192.168.0.1	MEBIUS		
4	2	192.168.0.150	HP2133		
5	3	192.168.0.152	M1210		
6	4	192.168.0.28	M1210		
7	5	192.168.0.37	LUC2		
8	6	192.168.0.7	lucretia		
9	7	192.168.1.7	lucretia		<u> </u>
10	8	192.168.66.1	LUCRETIA		
11	9	192.168.88.1	LUCRETIA		
12					
13					
14					
15					
16					
17					
18					
19					
20					
21					
22					
23					
24		1			
20				- Ial	
114 4 1	<ul> <li>N \Shee</li> </ul>	ti/aneet2/Sheet3/			
図形の	D調整( <u>R</u> ) →	là   オートシェイプ(U) • ∕ × □ C	) 🖹 🛍 🐗 🎲 🕼 🖾 🤌 ·	• 🚄 • 📥 • 🚍 🚍 🛱 🗑 🚽	
コマンド				NUM	1

※ EXCEL出力し表示したイメージ

ネットワーク機器管理台帳に便利です。右端の空欄は備考等で ご自由に使用できます。

HK Corporation. All rights reserved.

- 16 -



🌈 ステータス – Windows Internet Explorer	And the second second second			
🚱 🕤 👻 http://localhost:8080/almMan	age/system	💌 🐓 🗙 Live	Search 🥖	•
] ファイル(E) 編集(E) 表示(V) お気に入り(A	り ツール(D) ヘルプ(H)			
😭 🏟 🍘 ८५ – ७२			🛛 🙆 • 🖾 • 🖶 • 🔂 • 🎯 • 🖉	•
	- ネットワー ス:	ク <u>が</u> ク監視システム テータス		A
				-
E E	視モニター状態	Ver100118A		
alr	miii半細情報取得	取得		
	視モニター起動	起動		
	;視モニター停止	停止		
	OS再起動	再起動		
【レポート欄】				
ページが表示されました			-ネット 🔤 🔍 100%	•

【ステータス画面】

- ・メニューに戻るボタンを押下すると、メニュー画面へ遷移します。
- ・監視モニター状態:監視モニターの状態を表示します。 VerXXXXXXX:監視モニターのバージョンが表示されている時は動作中です。 停止!:監視モニターが動作していません。
- ・alm詳細情報取得:監視モニターの詳細情報を取得しレポート欄へ表示します。
- ・監視モニター起動ボタンが有効になっている場合、ボタン押下で監視モニターを 起動します。起動している時はボタンが無効になっています。
- ・監視モニター停止ボタンが有効になっている場合、ボタン押下で監視モニターを 停止します。停止している時はボタンが無効になっています。
- ・OS再起動ボタンを押下すると、ネットワーク監視システムPCのOS再起動を 行います。確認ダイアログにて「はい」を選択すると再起動します。

- 17 -

・レポート欄は本画面で操作した結果を表示します。



C Richard - Western Adversed Explanet		
🚱 🕞 🔹 🕼 (Mto://localhost5555)/almManaga/torstem	3 ** •	A Die Samen
SHARE WALLE WITH GIRL CALL	14.70B)	
🔐 🕼 🗿 Dezikin		10 * 12 - An + 14 * 10 *
	<mark>8/加</mark> 30/2	
LAN影漫种外投定	p.	
POPSU-IS-	from with	-
SMTP12-/5-		
ユーザーの	Fill	
/3.9-F		
SMITPUT	E67-	
POP before SMTP	P	
	BERT	
		-

【設定画面】

- ・メニューに戻るボタンを押下すると、メニュー画面へ遷移します。
- ・LAN内(LAN⇔LAN)の通信監視を全て対象外とします。
   LAN内にてファイル共有のコピーでも監視されます。内部LANのキーワード監視を
   全て除外したい場合、必要に応じチェックを入れてください。
   (LAN⇔WANは監視されます)
- ・POP3サーバーはメール通知で使用するサーバーを指定します。
- ・SMTPサーバーはメール通知で使用するサーバーを指定します。
- ・ユーザーIDはメール通知で使用する I Dを指定します。
- ・パスワードはメール通知で使用するパスワードを指定します。
- ・SMTPポートはメール通知で使用するSMTPサーバーのポートNoを指定します。
- ・POP before SMTPはメール通知で使用するサーバーがPOP before SMTPであった 場合、チェックを入れます。

- 18 -

・設定保存を押下すると、設定した内容を保存します。



【防御について】

・防御にチェックが入ったキーワードがネットワーク上で検出した場合、監視モニターは
 流出させたPCのネットワーク接続を約30秒後1時間の間、著しく妨害します。
 ※該当PCのネットワークデータを100%妨害はできません。

※設備・環境によって妨害できない場合があります。

- ・防御されているPCは管理システムの防御状況画面で確認できます。流出したPCにて 原因を究明後、問題が無いようなら防御を解除できます。
- ・IPテーブル表示画面より強制防御できますが、不正では無い機器のネットワーク接続 も阻害できてしまいます。本当に未知な機器であるか特定してから、防御操作は慎重 に行ってください。

【メール通知について】

- ・メール通知に設定したキーワードがネットワーク上で検出した場合、登録されている
   メールアドレスへメールを送信します。但し、同じキーワードで同じ流出PCであった
   場合、1日につき1回のみとなります(メールが大量に送られるのを防ぐ為)。
- ・同じキーワードで違うPCで検出した場合や、違うキーワードで同じPCで検出した場合 はメール送信されます。同じキーワードで同じPCで翌日再び検出された場合、再び メールが送信されます。
- ・ログデータからメール送信の判断を行ってます。ログを消去した場合、既に送られた メールであっても検知されるとメールが送信されます。
- ・設定画面のメール関連の設定は、メール通知を行う際に使用するメールサーバーを設定 します。間違えて設定されるとメール通知されませんのでご注意ください。

- 19 -



【監視PCについて】

- ・監視システムーが実行されているPCは、監視の対象となりません。
- ・有線LANのみの対応。無線LANには対応しておりません。
- ・かなりのネットワークトラフィックの場合、PCのスペックによっては処理が追いつか なくなり不具合が発生する可能性があります。管理システム画面が異常になったり、 監視モニターの詳細情報取得にて異常が発生した場合、監視PCの再起動をお勧めします。 頻発する場合、トラフィック状況の把握や、監視PCのスペックアップの検討をお勧め します。
- ・ポートミラーリングによるSwitching HUB等の機器とルーター等の機器の間を監視します。 ポートミラーリングされているポート以外の通信は監視されません。

【管理システムについて】

- ・管理システムは複数PCからアクセス・設定可能です。但し、キーワード変更している している時に、別PCからそのキーワードを削除してしまう場合等が考えられ、適切な キーワードやメール管理ができなくなる可能性があります。設定・変更等は単一管理PC より行ってください。
- (設定・変更等の操作ですので、ログ表示や防御表示等は複数 PC でも閲覧可能です)
- ・キーワードやメールアドレスの設定は、設定した直後から反映されます。
- ・管理システムヘログインしたPCは、監視の対象外となり監視されません。 但し、日付が変わる事で監視対象PCとなります。
- ・本システムの操作を終えましたら、なるべくalm管理メニュー画面へ一旦戻った後操作を 終えてください。(セキュリティの問題上、セッションを切る為です)



【その他】

・ゲートウェイ機器は、監視の対象となりません。

- ・監視モニターの表示ログは、日付が変わるとクリアされます。 ※DB上のログは消去されません。
- ・キーワードの誤検知(たまたま流出してしまった場合等)は防ぎようがありません。運営しながら状況に応じたキーワードを設定する必要があります。
- ・キーワードには「<>&" 、\*%」の半角文字が使用できません。

「!#\$()-+/=^~¥|@`[]{};:,.\_?」の半角文字は使用出来ます。

- ・ステータス画面より監視モニターを停止し再び起動を行うと、監視PCには監視モニター の画面は表示されません。裏プロセスとして起動していますので監視は行います。
- ・IPテーブルは、監視モニターで検知できたネットワーク機器の一覧です。ポートミラー リングされているポートに接続されたネットワークデータのみ検知できます。よって電源 が入っていない機器やルーター等にデータが流れていない機器は検知できません。
- ・IPテーブルは削除されるまで残ります。また、15分毎にIPテーブル更新を行います。 自動削除されませんので、一覧にあるネットワーク機器を廃棄した場合、手動にて削除 してください。全削除しても15分毎にIPテーブルの更新を行いますので、接続されて 検知できたネットワーク機器については、再びIPテーブルへ登録されます。

- 21 -



各クライアントのハードディスク上、頻繁に使われるフォルダへ特定のファ イルを置いておきます。

監視キーワードに、ファイル名、若しくはファイル内容を登録しておきます。 なんらかの情報漏洩ウィルス等で、そのファイルがインターネット上へ流出 した途端、アラートが挙げる事ができます。

そのログを見てクライアントの特定と流出先を割り出すことが可能です。

運営方法 例②



インターネット検索や、特定のURLを指定した場合、それを監視しアラート を挙げる事が可能です。

FTP転送においても、ファイル名等をキーワードに登録する事によりアラートを挙げる事が可能です。

- 23 -



電子メールの内容、件名、宛先、添付ファイルのファイル名等を特定のキー ワードで監視する事ができます。電子メールによって特定の情報が漏洩した事 を検知します。

HK Corporation. All rights reserved.

- 24 -





意図しないネットワーク機器が接続され、ルーターを介して外部へ機密データ等 を流出されてしまう可能性もあります。 I Pテーブル表示画面にて予期しない機器 が接続されていないかチェックできます。 何の機器か特定できなく、不正なアクセス等を行っている場合、防御により著しく 不正機器のネットワーク接続を阻害できます。

※但し、防御については極めて慎重に行ってください。

## 本システムの取扱について

#### ●免責

- ・本システムにおける損害、故障、事件、事故、第三者からの請求は、弊社では一切その 責任を負えません。
- ・本システムにおいて万一不具合にて生じた損害、故障、事件、事故、第三者からの請求 は、弊社では一切その責任を負えません。本システムを、改善するよう努力いたします。
- ・本システムにおいてお客様の設定ミス、操作ミス等で発生した、いかなる損害、故障、
   事故、事件、第三者からの請求は、弊社では一切その責任を負えません。

●著作権

- ・本システムに関する著作権、取扱説明書、資料、プログラム、設定内容、知的財産権、
   その他権利の実施・使用等は株式会社エイチケーに帰属します。
- ・本システムを株式会社エイチケーに許可なく、全部または一部を複製・解読・改変・ 公衆配信することは、著作権法上、禁止されております。

●本システムのご利用に関する留意点

・本システムを不正アクセス禁止法やハイテク犯罪に該当するような目的で使用を行った
 場合、本システムの使用禁止処置、場合により警視庁へ報告いたします。

●その他

- ・本システムは予告なしに変更する事がありますのでご了承ください。
- ・本システムで使用したJava、TOMCAT、データベース等の著作権につきましては、それぞれの団体に帰属します。

●お問合せ

株式会社エイチケー <u>http://www.hkl.co.jp</u> メール: info@hkl.co.jp