

## 例

この付録は、シスコのコンテンツ セキュリティ管理アプライアンス機能を導入する一般的な方法について数例を説明しています。これらには、次の項を含みます。

- 「例 1 : ユーザの調査」(P.D-1)
- 「例 2 : URL のトラッキング」(P.D-5)
- 「例 3 : アクセス数の多い URL カテゴリの調査」(P.D-6)

## Web セキュリティ アプライアンスの例

ここでは、セキュリティ管理アプライアンスおよび Web セキュリティ アプライアンスを使用した例について説明します。



(注)

これらのシナリオはすべて、セキュリティ管理アプライアンスおよび Web セキュリティ アプライアンスで Web レポートिंगおよび Web トラッキングをイネーブルがイネーブルにされていることを前提としています。Web トラッキングおよび Web レポートिंगをイネーブルにする方法については、[第 5 章「中央集中型 Web レポートिंगおよびトラッキングの使用」](#)を参照してください。

### 例 1 : ユーザの調査

次に、システム管理者が会社で特定のユーザを調査する例を示します。

このシナリオでは、ある従業員が勤務中に不適切な Web サイトにアクセスしている、という苦情を管理者が受け取っています。それを調査するには、システム管理者が Web アクティビティの詳細をトラッキングする必要があります。

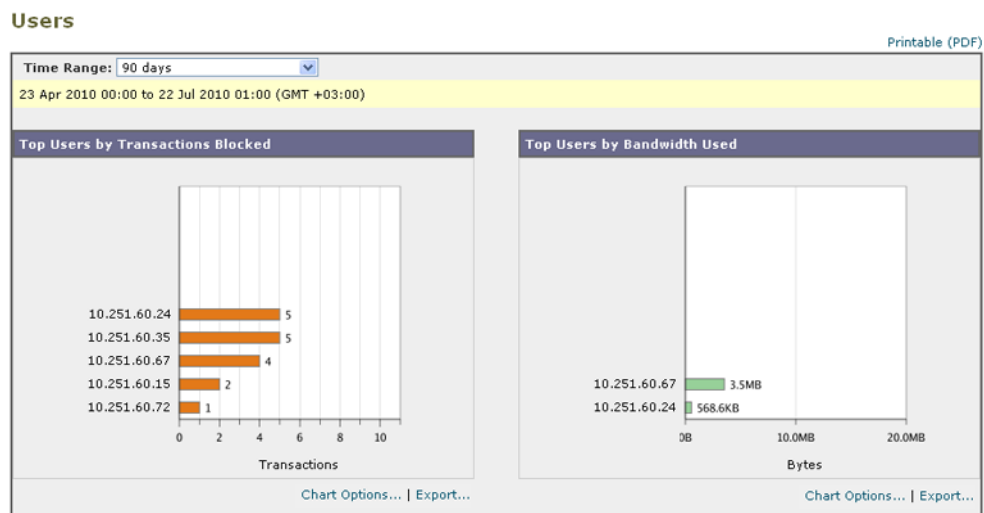
Web アクティビティがトラッキングされると、従業員の参照履歴に関する情報が記載された Web レポートが作成されます。

**ステップ 1** セキュリティ管理アプライアンスで、[Web] > [レポート (Reporting)] > [ユーザ (Users)] を選択します。

**ステップ 2** [ユーザ (Users)] テーブルで、調査する [ユーザ ID (User ID)] または [クライアント IP アドレス (Client IP address)] をクリックします。

ユーザ ID またはクライアント IP アドレスがわからない場合は、ユーザ ID またはクライアント IP アドレスをわかる範囲でテキストフィールドに入力し、[ユーザ ID またはクライアント IP アドレスの検索 (Find User ID or Client IP Address)] をクリックします。IP アドレスが正確に一致していなくても

結果は返されます。[ユーザ (Users)] テーブルに、指定したユーザ ID およびクライアント IP アドレスが入力されます。この例では、クライアント IP アドレス 10.251.60.24 の情報について検索しています。



- ステップ 3** IP アドレス [10.251.60.24] をクリックします。  
10.251.60.24 のユーザの詳細ページが表示されます。

Users > 10.251.60.24

Printable (PDF)

Time Range: 90 days  
 31 Aug 2011 00:00 to 29 Nov 2011 15:00 (GMT -08:00)

#### URL Categories by Total Transactions

URL Category	Transactions
Search Engines and Portals	99
Business and Industry	7
Computers and Internet	5
Advertisements	4
Infrastructure	3

#### Trend by Total Transactions

Chart Options... | Export...

#### URL Categories Matched

URL Category	Bandwidth Used	Time Spent	Blocked URL Category	Transactions Completed	Total Transactions
Search Engines and Portals	447.4KB	00:21	0	99	99
Business and Industry	15.5KB	00:06	0	7	7
Computers and Internet	84.4KB	00:06	0	5	5
Advertisements	16.9KB	00:00	0	4	4
Infrastructure	4,540B	00:00	0	3	3
Totals (all available data):	568.6KB	00:33	0	118	118

Find URL Category Columns... | Export...

#### Domains Matched

Domain or IP	Bandwidth Used	Time Spent	Transactions Completed	Transactions Blocked	Total Transactions
google.com	464.5KB	00:36	101	5	106
modules.com	83.1KB	00:06	4	0	4
google-analytics.com	8,272B	00:00	4	0	4
rediffmail.net	15.1KB	00:00	3	0	3
hotmail.com	6,391B	00:06	2	0	2
rediffmail.com	1,365B	00:00	1	0	1
rediffmail.com	1,231B	00:00	1	0	1
quartec.com	1,847B	00:00	1	0	1
rediffmail.com	2,021B	00:00	1	0	1

Find Domain or IP Columns... | Export...

#### Applications Matched

No data was found in the selected time range

#### Malware Threats Detected

No data was found in the selected time range

#### Policies Matched


Policy Name	Policy Type	Bandwidth Used	Completed Transactions	Blocked Transactions	Total Transactions
DefaultGroup	Access	568.6KB	118	0	118
NONE	Access	0B	0	5	5
Totals (all available data):	--	568.6KB	118	5	123

Find Policy Name Columns... | Export...

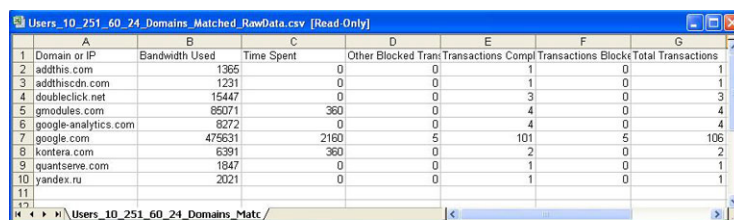
ユーザの詳細ページから総トランザクション別の URL カテゴリ、総トランザクション別のトレンド、一致する URL カテゴリ、一致するドメイン、一致するアプリケーション、検出されたマルウェアの脅威、および一致するポリシーを確認できます。

これらのカテゴリによって、10.251.60.24 のユーザがブロックされている URL (ページの [ドメイン (Domains)] セクションに含まれる [ブロックされたトランザクション (Transactions Blocked)] カラムに表示) にアクセスしようとしていたことなどがわかります。

- ステップ 4** [一致したドメイン (Domains Matched)] テーブルの下の [エクスポート (Export)] をクリックし、ユーザがアクセスしようとしていたドメインおよび URL のリストを表示します。

 **D-1** に、ユーザからエクスポートされた情報のリストを示します。

**図 D-1** エクスポート データの例



A	B	C	D	E	F	G
Domain or IP	Bandwidth Used	Time Spent	Other Blocked Trans	Transactions Compl	Transactions Block	Total Transactions
1			0	0	1	0
2	1365	0	0	0	0	1
3	1231	0	0	1	0	1
4	15447	0	0	3	0	3
5	85071	360	0	4	0	4
6	8272	0	0	4	0	4
7	475631	2160	5	101	5	106
8	6391	360	0	2	0	2
9	1847	0	0	1	0	1
10	2021	0	0	1	0	1
11						

ここから Web トラッキング機能を使用して、この特定のユーザの Web 使用状況をトラッキングし、表示することができます。



**(注)** Web レポートでは、アクセスされる特定の URL に限らず、ユーザがアクセスするすべてのドメイン情報を取得できる点に注意してください。ユーザがアクセスしている特定の URL、その URL にアクセスした時刻、その URL が許可されているかどうかなどの情報を得るには、[Web トラッキング (Web Tracking)] ページの [プロキシ サービス (Proxy Services)] タブを使用します。

- ステップ 5** [Web] > [レポート (Reporting)] > [Web トラッキング (Web Tracking)] を選択します。

- ステップ 6** [プロキシ サービス (Proxy Services)] タブをクリックします。

- ステップ 7** [ユーザ/クライアント IP アドレス (User/Client IP Address)] テキスト フィールドにユーザ名または IP アドレスを入力します。

この例では、ユーザ 10.251.60.24 の Web トラッキング情報を検索します。

検索結果が表示されます。

## Web Tracking

Search	
Available: 13 Jul 2010 01:00 to 14 Jul 2010 23:59 (GMT +03:00)	
Time Range:	90 days
User/Client IP:	10.251.60.24 (e.g. jdoe or DOMAIN\jdoe)
Website:	(e.g. google.com)
Transaction Type:	All Transactions
<input type="checkbox"/> Advanced Search transactions using advanced criteria.	
<input type="button" value="Clear"/>	<input type="button" value="Search"/>

Results					
Displaying 1 - 8 of 8 transactions.					
Time (GMT +03:00) ▼	Transaction	Display Details...	Disposition	Bandwidth	User / Client IP
14 Jul 2010 22:58:32	http://safebrowsing.clients.google.com/safebrowsing/downloads?cli...		Allow	6,354B	10.251.60.24
14 Jul 2010 22:27:37	http://safebrowsing.clients.google.com/safebrowsing/downloads?cli...		Allow	5,131B	10.251.60.24
14 Jul 2010 21:56:02	http://safebrowsing.clients.google.com/safebrowsing/downloads?cli...		Allow	8,148B	10.251.60.24
14 Jul 2010 21:28:05	http://kon5.kontera.com/KonaGet.js?u=1279132089362&p=1429248...		Allow	6,291B	10.251.60.24
14 Jul 2010 21:27:49	http://k830suiki628goudg944806bp0tpu5r3.a.friendconnect.gmodules....		Allow	83.1KB	10.251.60.24
14 Jul 2010 21:27:44	http://www.google.com/url?sa=t&source=web&cd=1&ved=DC...		Allow	244.3KB	10.251.60.24
14 Jul 2010 21:27:04	http://www.google.com/search?q=%D0%BF%D0%BE%D0%BB%D1%8C%D0%BA%D0%...		Allow	28.4KB	10.251.60.24
14 Jul 2010 21:26:58	http://suggestqueries.google.com/complete/search?output=firefox&a...		Block	14.6KB	10.251.60.24
Displaying 1 - 8 of 8 transactions.					
Columns...					

このページから、IP アドレス 10.251.60.24 に割り当てられているコンピュータのユーザがアクセスしたトランザクションおよび URL のすべてのリストを確認できます。

## 関連項目

表 D-1 に、この例で説明した項目を示します。各項目の詳細については、リンクをクリックしてください。

表 D-1 ユーザの調査の関連項目

機能名	機能情報
[ ユーザ (User) ] ページ	「[ ユーザ (Users) ] レポート (Web)」 (P.5-17)
[ ユーザの詳細 (User Details) ] ページ	「[ ユーザの詳細 (User Details) ] (Web レポートティング)」 (P.5-20)
レポート データのエクスポート	「レポート ティング データおよびトラッキング データの印刷およびエクスポート」 (P.3-10)
[ Web トラッキング (Web Tracking) ] ページの [ プロキシ サービス (Proxy Services) ] タブ	「Web プロキシ サービスによって処理されたトランザクションの検索」 (P.5-56)

## 例 2 : URL のトラッキング

このシナリオでは、セールス マネージャが、会社のサイトへのアクセスで、先週の上位 5 位を知りたい場合を考えます。さらに、どのユーザがこれらの Web サイトにアクセスしているかについても知りたいとします。

**ステップ 1** セキュリティ管理アプライアンスで、[ Web ] > [ レポート (Reporting) ] > [ Web サイト (Web Sites) ] を選択します。

- ステップ 2** [時間範囲 (Time Range) ] ドロップダウン リストから [週 (Week) ] を選択します。
- ステップ 3** [ドメイン (Domains) ] セクションをスクロール ダウンすると、アクセスされているドメインまたは Web サイトが表示されます。
- アクセス上位 25 位までの Web サイトは、[一致したドメイン (Domains Matched) ] テーブルに表示されます。同じテーブルで [ドメイン (Domain) ] または [IP] カラムのリンクをクリックすると、特定のアドレスまたはユーザが参照した実際の Web サイトを確認できます。

## 関連項目

表 D-2 に、この例で説明した項目を示します。各項目の詳細については、リンクをクリックしてください。

**表 D-2 URL のトラッキングの関連項目**

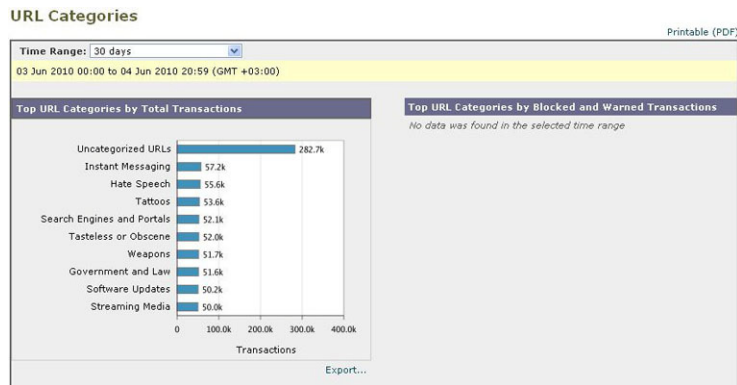
機能名	機能情報
[Web サイト (Web Sites) ] ページ	<a href="#">「[Web サイト (Web Sites) ] レポート」 (P.5-24)</a>

## 例 3 : アクセス数の多い URL カテゴリの調査

このシナリオでは、従業員が最近 30 日間にアクセスした上位 3 位までの URL を、人事部長が知りたい場合を考えます。また、ネットワーク管理者が、帯域幅の使用上をモニタしたり、ネットワークで最も帯域幅を使用している URL を特定したりするためにこの情報を取得するとします。

次の例は、複数の観点を持つ複数の人のためにデータを収集するが、生成するレポートは 1 つだけで済む方法を示します。

- ステップ 1** セキュリティ管理アプライアンスで、[Web] > [レポート (Reporting) ] > [URL カテゴリ (URL Categories) ] を選択します。



**URL Categories Matched** Items Displayed 10

URL Category	Bandwidth Used	Time Spent	Blocked by URL Category	Transactions Completed	Total Transactions
Uncategorized URLs	4.2GB	13117:33	0	282.7k	282.7k
Instant Messaging	1.2GB	2688:57	0	57.2k	57.2k
Hate Speech	1.3GB	2653:54	0	55.6k	55.6k
Tattoos	1.3GB	2563:36	0	53.6k	53.6k
Search Engines and Portals	682.2MB	2419:30	0	52.1k	52.1k
Tasteless or Obscene	717.9MB	2412:33	0	52.0k	52.0k
Weapons	964.6MB	2428:57	0	51.7k	51.7k
Government and Law	1.0GB	2430:15	0	51.6k	51.6k
Software Updates	788.9MB	2334:24	0	50.2k	50.2k
Streaming Media	701.5MB	2318:42	0	50.0k	50.0k
Totals (all available data):	45.0GB	132107:42	0	2.8M	2.8M

Columns... | Export...

この例の [URL カテゴリ (URL Categories)] ページによると、総トランザクション別の上位 10 の URL カテゴリ グラフから、Instant Messaging、Hate Speech、Tattoo サイトなどの他に、282 k の未分類の URL にアクセスしていることがわかります。

ここで、[エクスポート (Export)] リンクをクリックして raw データを Excel スプレッドシートにエクスポートすると、このファイルを人事部長に送信できます。ネットワーク マネージャに URL ごとの帯域幅の使用量を知らせる必要があります。

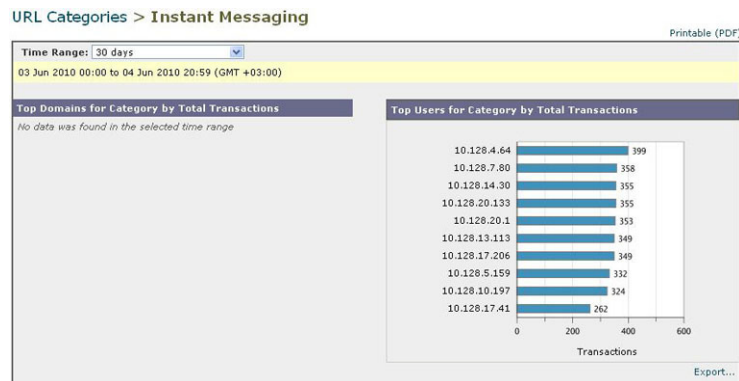
**ステップ 2** [一致した URL カテゴリ (URL Categories Matched)] テーブルをスクロールダウンし、[使用済み帯域幅 (Bandwidth Used)] カラムを表示します。

**URL Categories Matched** Items Displayed 10

URL Category	Bandwidth Used	Time Spent	Blocked by URL Category	Transactions Completed	Total Transactions
Uncategorized URLs	4.2GB	13117:33	0	282.7k	282.7k
Instant Messaging	1.2GB	2688:57	0	57.2k	57.2k
Hate Speech	1.3GB	2653:54	0	55.6k	55.6k
Tattoos	1.3GB	2563:36	0	53.6k	53.6k
Search Engines and Portals	682.2MB	2419:30	0	52.1k	52.1k
Tasteless or Obscene	717.9MB	2412:33	0	52.0k	52.0k
Weapons	964.6MB	2428:57	0	51.7k	51.7k
Government and Law	1.0GB	2430:15	0	51.6k	51.6k
Software Updates	788.9MB	2334:24	0	50.2k	50.2k
Streaming Media	701.5MB	2318:42	0	50.0k	50.0k
Totals (all available data):	45.0GB	132107:42	0	2.8M	2.8M

Columns... | Export...

[一致した URL カテゴリ (URL Categories Matched)] テーブルで、すべての URL カテゴリの帯域幅の使用量を確認することができます。もう一度 [エクスポート (Export)] リンクをクリックして、このファイルをネットワーク管理者に送信します。さらに細かく調べるには、[インスタント メッセージ (Instant Messaging)] リンクをクリックすると、どのユーザが帯域幅を大量に使用しているかが特定されます。次のページが表示されます。



**Domains Matched**

Data below is not available for the full time range selected. Data for this table is available for 03 Jun 2010 16:00 to 03 Jun 2010 18:59 (GMT +03:00). Click to change the time range of this report to reflect the data available. Change Time Range

No data was found in the selected time range

**Web Users**

Items Displayed 10

User ID or Client IP	Bandwidth Used	Time Spent	Transactions Completed	Transactions Blocked	Total Transactions
10.128.4.64	10.1MB	19:57	399	0	399
10.128.7.80	15.3MB	17:54	358	0	358
10.128.14.30	18.4MB	17:45	355	0	355
10.128.20.133	21.4MB	17:45	355	0	355
10.128.20.1	10.2MB	17:39	353	0	353
10.128.13.113	17.6MB	17:27	349	0	349
10.128.17.206	12.1MB	17:27	349	0	349
10.128.5.159	12.3MB	16:36	332	0	332
10.128.10.197	16.8MB	16:12	324	0	324
10.128.17.41	10.1MB	13:06	262	0	262
<b>Totals (all available data):</b>	<b>1.2GB</b>	<b>2688:57</b>	<b>57.2k</b>	<b>0</b>	<b>57.2k</b>

Find User ID or Client IP Columns... Export...

このページから、ネットワーク管理者が Instant Messaging サイトの上位 10 ユーザを知ることができます。

このページから、最近 30 日間で 10.128.4.64 のユーザが Instant Messaging サイトに 19 時間 57 分アクセスしており、この期間の帯域幅の使用量が 10.1 MB であることがわかります。

## 関連項目

表 D-3 に、この例で説明した項目を示します。各項目の詳細については、リンクをクリックしてください。

**表 D-3**                    **アクセスの多い URL カテゴリの調査の関連項目**

機能名	機能情報
[URL カテゴリ (URL Categories) ] ページ	「URL カテゴリ レポート」 (P.5-26)
レポート データのエクスポート	「レポート データおよびトラッキング データの印刷およびエクスポート」 (P.3-10)