# オープンAIチャットを制限するためのセキュア アクセスでのDLPの実装プログラミングのため のGPTの使用

内容
<u>はじめに</u>
前提条件
<u>要件</u>
<u>使用するコンポーネント</u>
<u>設定</u>
<u>1. ソースコードデータ識別子を使用するためのデータ分類の作成</u>
<u>2. DLPポリシーを作成し、その中のデータ分類を「ソースコード」と呼びます。</u>
<u>3. 復号化を有効にしたチャットGPTへのトラフィック用のインターネットアクセスポリシーが</u> 設定されていることを確認します <u>。</u>
<u>4.Open Al ChatGPTを使用して、任意のプログラムをダウンロードまたはアップロードしてみて</u> <u>ください。</u>
<u>確認</u>
トラブルシュート
<u>関連情報</u>

### はじめに

このドキュメントでは、プログラミングおよびコーディング用にオープンAI ChatGPTの使用を制限するために、セキュアアクセスにデータ損失防止(DLP)を実装する方法について説明します。

### 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- セキュアなアクセス
- DLP
- AI ChatGPTを開く

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- セキュアなアクセス
- DLP

• AI ChatGPTを開く

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始していま す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して ください。

### 設定

1. ソースコードデータ識別子を使用するためのデータ分類の作成

<u>Secure Access Dashboard</u>に移動します。

 Secure > Data Classificationの順にクリックします。 Add Data Classification Name

55	Overview	Data Classification						
0	Experience Insights	For more information about data classification, see Help 🗭						
**	Connect	Data Classifications Exact Data	Data Classifications Exact Data Matches Indexed Document Matches					
<b>i</b>	Resources							
U	Secure -	Policy	Profiles	Settings				
	Monitor	Access Policy Create rules to control and secure access to private and internet	Endpoint Posture Profiles Configure requirements for end- user devices connecting to private	Threat Categories Choose types of harmful destinations to restrict access to				
20	Admin Workflows	destinations Data Loss Prevention Policy Prevent data loss/leakage with policy rules	resources IPS Profiles Configure settings for intrusion prevention	Notification Pages Configure notifications to present to end users who try to access blocked or warned destinations.				
			Web Profiles Configure web security settings for use in internet access rules	Do Not Decrypt Lists Specify destinations for traffic that must never be decrypted				
				Certificates Provide certificates needed to decrypt traffic, present end-user notifications, and authenticate VPN clients				
			<b></b>	Data Classification Manage rules to prevent sensitive data loss				

• > Select Built-in Data Identifiers > Search forと入力してSource Code、これを選択します

1	For more information about data classification, see Help 다	ADD CUSTOM IDENTIFIE
	Add New Data Classification	
-	Data Classification Name     Description (Optional)       Source Code	
-	Select Boolean Operator          Image: Organ select Boolean Operator         Image: Organ select Boolean Operator	
-	Built-in Data Identifiers      Q Source Code	
	Built-in Identifiers	
-	Source Code	>
	Custom Identifiers	

Data Classifications Exact Data Matches Indexed Document Matches	
For more information about data classification, see Help 🕝	ADD CUSTOM IDENTIFIER
Add New Data Classification	
Data Classification Name Source Code	Description (Optional)
Select Boolean Operator	
Selected Data Identifiers	
Built-in Data Identifiers	
Q Source Code No Data Identifiers found.	
Custom Identifiers	
	CANCEL

2. DLPポリシーを作成し、その中のデータ分類を「ソースコード」と呼びます。

・ Secureをクリックします。 Data Loss Prevention Policy

#### Add Rule

U	Secure	Policy	Profiles	Settings
₩.	Monitor	Access Policy Create rules to control and secure access to private and internet	Endpoint Posture Profiles Configure requirements for end- user devices connecting to private	Threat Categories Choose types of harmful destinations to restrict access to
<b>2</b> 0	Admin Workflows	destinations Data Loss Prevention Policy Prevent data loss/leakage with policy rules	resources IPS Profiles Configure settings for intrusion prevention	Notification Pages Configure notifications to present to end users who try to access blocked or warned destinations.
			Web Profiles Configure web security settings for use in internet access rules	Do Not Decrypt Lists Specify destinations for traffic that must never be decrypted
				Certificates Provide certificates needed to decrypt traffic, present end-user notifications, and authenticate VPN clients
				Data Classification Manage rules to prevent sensitive data loss

• をクリックします。 Real Time Rule

#### Rule Name

	Overview	Data Loss Prevention Policy	ud in unur		
+  ©	Experience Insights	n enabled through its rules, the Uata Loss Prevention policy can monitor or block the data being uploaded to the web. As well, it can discover and protect the sensitive data stored and shared in yild sanctioned applications. Help 🕉			
×*	Connect				
<b>b</b> .	Resources	1 DLP Rule SaaS API Rul	le		

#### • を入力し、適切な値に設定します Severity

Data ClassificationsContent

22	Overview	Data Loss Prevention Policy	BACK TO DLP RULES	
+  ©	Experience Insights	erience Insights When enabled through its rules, the Data Loss Prevention policy can monitor or block the data being uploaded to the web. As well, it can discover and protect the sensitive data stored and shared in your cloud sanctioned applications. Help 🗹		
,s <sup>4</sup>	Connect			
h.	Resources	Edit Real Time Rule		
0	Secure	Configure this rule to set the criteria as to what triggers its enforcement. The Realtime DLP inspects the content of outbound web requests that match this rule's identities ar destinations. If a data violation is detected, this rule's Action setting is automatically enforced. Help C	nd	
k	Monitor	Rule Name Description (Optional)		
2o	Admin	Panadar		
A	Workflows	High		

• selectで次を選択します。 Source Code

## Data Classifications

Select where to search for the selected data classifications.

Ontent

٠

O File Name

O Content and File Name

### Select data classifications to add them to this rule.

Q Search Classifications		
Built-in GDPR Classification	PREVIEW	
Built-in HIPAA Classification	PREVIEW	
Built-in PCI Classification	PREVIEW	
Built-in PII Classification	PREVIEW	
Source Code	PREVIEW	

#### 必要に応じて必要なIDをIdentities選択します

Identities Select identities to add them to this rule.	
Search Identities	5 Selected REMOVE ALL
All Identities	Roaming Computers 4
AD Groups	microsoft.com)
Z Network Tunnel Groups	
□ ♣ Networks 1>	
✓ □ Roaming Computers 4>	

・ [通知先]で、次の項目を選択します Select Destination Lists and Applications for Inclusion

#### Application Categories

• > SelectGenerative AI > SelectOpenAI API (Vetted)を選択し、「OpenAI ChatGPT (Vetted)」で Outbound and InboundDirection

#### Destinations

Manage destination lists and vetted applications for this rule.

[	<ul> <li>All Destinations Selecting All Destinations will scan the traffic to any app</li> <li>Select Destinations Lists and Applications for Inclusio Scans selected destination lists and vetted applications</li> </ul>	nication or website the user i n	is b	rowsing to.	
	Destinations			2 Selected for Inclusion	REMOVE ALL
	Destination Lists	1 >		Applications Categories	
-	Application Categories	4802 (2 SELECTED) >		OpenAl API / Generative Al, Outbound & Inbound	×
				OpenAl ChatGPT / Generative Al, Outbound & Inbound	×

• 選Action 択下 Block

User Notifications

• では、ルールがトリガーされたときにエンドユーザに送信される電子メール通知を設定できます(オプション)

### Action

Choose to monitor or block content for this rule.



The Default Block Page Applied

## User Notifications

When enabled, the system sends an email to recipients notifying them that this rule has been triggered.



・ クリック Save

				1
DELETE		CANCEL	SAVE	
			•	

3. 復号化を有効にしたチャットGPTへのトラフィック用のインターネットアクセスポリシーが設定されていることを確認します。

以下に例を挙げます。

Chat GPT	$\times$
Internet	
General	
Action	Allow
Last modified	
Rule order	1
Logging	Enabled
Hits	216
Sources Any	
<b>Destinations</b> 2 destinations	^
Application Settings	(2)
OpenALAPI Open	AI ChatGPT

サンプルのPythonプログラムを要求すると、この要求はブロックされます。

GhatGPT	×	+	
→ C S chatgpt.com			
ChatGPT Explore GPTs	Â	ChatGPT ~	An error occurred. Either the engine you requested does not exist or there was another issue processing your request. If this issue persists please contact us through our help center at help.openai.com.
:h			$\Box \simeq \Delta \sim$

• プログラムが正しいかどうかを尋ねると、この要求はブロックされます。

```
25 chatgpt.com
            C
                     ChatGPT ~
                                                                        Is this program correct?
                                                                        # Python program to swap two variables
                                                                        x = 5
                                                                        y = 10
                                                                        # To take inputs from the user
                                                                        #x = input('Enter value of x: ')
                                                                        #y = input('Enter value of y: ')
                                                                        # create a temporary variable and swap the values
                                                                        temp = x
                                                                        x = y
                                                                        y = temp
                                                                        print('The value of x after swapping: {}'.format(x))
                                                                        print('The value of y after swapping: {}'.format(y))
                                    $
                                              (i) An error occurred. Either the engine you requested does not exist or
                                                  there was another issue processing your request. If this issue persists
                                                  please contact us through our help center at help.openai.com.
                                            < 2/2 > ① ご ⑦ ~
```

#### 確認

ユーザがサンプルPythonプログラムをChatGPTに要求しようとすると、要求がブロックされます。 Secure Access Data Loss PreventionログでDLPイベントがトリガーされたことを確認できます。

• Monitorに移動します。 Data Loss Prevention

.1 1.1 1. cisco	Secure Access							
	Overview	Activity Se	earch					
1  O	Experience Insights							
**	Connect	FILTERS	Q Search by	domain, ide	ntity, or URL			
<b>i</b>	Resources	Q Search filte	rs		1,965 Tota	Ó	Vie	
U	Secure	Response	Advanced	Select All	Request	Source		
<u>~</u>	Monitor	Reports		Manage	ement			
		Remote Access Lo	gs	Export	ed Reports			
20	Admin	Activity Search		Scheduled Reports				
		Traffic logs		Saved Searches				
		Security Activity Security events and to	p threats	Admin	Audit Log			
		Total Requests						
		Activity Volume						
		App Discovery Discover and analyze applications	network					
		Top Destinations Top domains visited b	y DNS					
		Top Categories Top security and cont categories by DNS	ent					
		Third-Party Apps						
		Cloud Malware View and manage det malware events	ected					
		Data Loss Prevent Data violations detect the Real Time and Saa	on ed through IS API rules					

• DLPイベントが表示されます。

Data Loss Prevention									Schedul	LAST 24	HOURS *	
Events Discovery												
FILTERS	Colort All	Q Search			Advanced	~						
Real Time		6 Total Events	Viewing activit	y from Aug 6, 2024 at 9:53 AM to	Aug 7, 2024 at 9:	53 AM						\$
SaaS API		Event Type	Severity	Identity	File Owner	Event Actor	File Name 🔻	Destination	Rule	Action	Detected V	
Action		Real Time	• High	L Windows11-ZTNA	N/A	N/A	Form	OpenAl ChatGPT	Chat GPT DLP	Blocked	Aug 7, 2024 at 9:52 AM	

• イベントログの最後にある3つのドットをクリックして、イベントの詳細を確認します。

Data Loss Prevention									Schedu	) (1) ule Download	LAST 24 HOURS ¥	
Events Discovery												
FILTERS		Q. Search			Advanced	~						
Event Type	Select All											
Real Time		6 Total Events	Viewing activity	ty from Aug 6, 2024 at 9:53 AM to	Aug 7, 2024 at 9:	53 AM						⇔
SaaS API		Event Type	Severity	Identity	File Owner	Event Actor	File Name 🔻	Destination	Rule	Action	Detected V	
Action		Real Time	• High	L Windows11-ZTNA	N/A	N/A	Form	OpenAl ChatGPT	Chat GPT DLP	Blocked	Aug 7, 2024 at 9:52	АМ

• クリック View details.

Event Type	Severity	Identity	File Owner	Event Actor	File Name 🔻	Destination	Rule	Action	Detected <b>V</b>	
Real Time	• High	Windows11-ZTNA	N/A	N/A	Form	OpenAl ChatGPT	Chat GPT DLP	Blocked	View details	•••

• これで、イベントの詳細全体が表示されます。

## **Event Details**

# Detected

Aug 7, 2024 at 9:52 AM

# Action



## File Name

Form

# Identity

Windows11-ZTNA

# Application

**OpenAl ChatGPT** 

**Application Category** 

Generative AI

**Destination URL** 

http://chatgpt.com/backend-api/conversation



	X
Rule Chat GPT DLP	$\sim$
<ul><li>Severity</li><li>High</li></ul>	
Direction Inbound	
Classification	
Source Code	
def calculate_year_of_century(age):, def main():	$\overline{\mathbf{S}}$

× /

• DLPポリシーの分類子/分類に一致したコンテンツのすべての詳細が表示されます。

Source Code

8 Matches Source Code

def calculate\_year\_of\_century(age):, def main():...

age, then calculates the year they will turn 100 yea rs old:\n\n```python\ndef calculate\_year\_of\_centu ry(age):\n \"\"\"Calculate the year the user will tu rn 100.\"\"\n current\_year = = 100 - age\n year\_of\_century = current\_year + y ears\_until\_100\n return year\_of\_century\n\ndef m ain():\n # Ask the user for their name and age\n name

トラブルシュート

• Open AI ChatGPTのWeb要求を照合するアクセスポリシーで復号化が有効になっていることを確認します。

• SSEがOpen AI ChatGPTのトラフィックを復号化しているかどうかをすばやく確認するには、共通名にキーワード「 Cisco Secure Access」が含まれていることを示すWebサイトの証明書を確認します。

## Certificate Viewer: chatgpt.com

General

Details

### Issued To

Common Name (CN)
Organization (O)
Organizational Unit (OU)

chatgpt.com Cisco Systems, Inc. <Not Part Of Certificate>

### Issued By

Common Name (CN)	Cisco Secure Access Secondary SubCA p-apse210-SG
Organization (O)	Cisco
Organizational Unit (OU)	<not certificate="" of="" part=""></not>

### Validity Period

Issued On	Monday, August 5, 2024 at 10:14:04 PM
Expires On	Saturday, August 10, 2024 at 10:14:04 PM



Certificate Viewer: ch	atgpt.com ×	
General Details		
Issued To Common Name (CN)	chatgpt.com	
Organization (O)	Cisco Systems, Inc.	
Organizational Unit (OU)	<not certificate="" of="" part=""></not>	
Issued By		
Common Name (CN)	Cisco Secure Access Secondary SubCA p-apse210-SG	
Organization (O)	Cisco	
Organizational Unit (OU)	<not certificate="" of="" part=""></not>	
Validity Period		
Issued On	Monday, August 12, 2024 at 10:52:16 PM	
Expires On	Saturday, August 17, 2024 at 10:52:16 PM	
SHA-256 Fingerprints		
Certificate 4572 5764	2b5f7a356b5a3c4292a587a130936a3e01990453c22cfdde138e736c 47	;
Public Key 6503 13bo	324e564bdddcf3b09426edfa866449e81c6c79d5d406b23a44e458b d62	

- ChatGPTを開く> Open developer tools > Select Network > NextサンプルのPythonプログラムをChatGPTに要求する
- 要求の結果がブロックされることを確認します。ドメインの下に「block.sse.cisco.com

← → ♂ ts chatgpt.	com		* 0	:
ChatGPT	ć	ChatGPT ~	Image: Sources     Network     Performance     Memory     Image: Sources     Network     Performance     Memory     Image: Sources     Image: Sources     Image: Sources     Network     Image: Sources     Image: Sources	×
80 Explore GPTs	Explore GPTs	O An error occurred. Either the engine you requested does not exist or	4	
			there was another issue processing your request. If this issue persists please contact us through our help center at help.openai.com.	Time 46 63
			のごのマレー         01         200         chatgst.com         900 8         00 1         900 8         00 1         1348	27
			dip/fserver.mps-3768774963-dth/p.sigerov.gend_wws.TC. 200 blockse.cico.com 0.8     for rgstr         202 ab.chrtgpt.com 1.3.48	44
			(2) num1ddsourceirbrowser/äddtagsinisdk, version/K3A520,0%	43

- プログラムコードが正しいかどうかをChatGPTに確認します。
- 要求の結果がブロックになり、「domain」の下に「block.sse.cisco.com」と表示されることを確認します。

chatgpt.com							☆	3	:
ChatGPT	Ú.		61	Image: Console         Sources         Network           Image: Console         Sources         Network           Image: Console         Image: Console         Disable cache           Image: The second s	Performance M No throttling • ta URLs	femory >>	8 🔺 41 🗖 5		×
		Is this program correct? # Python program to swap two variables x = 5 y = 10		All         Fetch/NHR         Dec:         CSS         15         Fent         Img         Media         M           Blocked requests         3rd-party requests         3rd-party requests         500 ms         100 ms         200 ms	2500 ms 30	m Other Blocked re	4000 ms	4500 ms	
		<pre># To take inputs from the user #x = input(Enter value of x: ) #y = input(Enter value of y: ) # create a temporary variable and swap the values temp = x x = y y = temp print(The value of x after swapping: ():format(x)) print(The value of y after swapping: ():format(y))</pre>		Name Ø obta-requirements Ø memoriesTinclude_memory_entriessfalse ■ den/terversmps-3786776964-9g7d8.sigprony.prod_envs_t Ø dp/Terversmps-5786776964-9g7d8.sigprony.prod_envs_t Ø rigstr ■ rigstr	Status 200 200 202 202 202 200 202 (pending)	Domain chutgpt.com chutgpt.com blod.se.cisco.com blod.se.cisco.com ab.chutgpt.com ab.chutgpt.com	Size	7.3 k8 1.0 k8 8198 08 08 1.3 k8 08	Time 83 25 41 41 16 Pe
	<ul> <li>An error occurred. E there was another is please contact us the</li> <li>2/2 &gt; O C Q </li> </ul>	ither the engine you requested does not exist or sue processing your request. If this issue persists rough our help center at help.openai.com.							



- <u>Cisco Secure Accessユーザガイド</u>
- シスコテクニカルサポートとダウンロード

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。