

ログ分析演習

満永拓邦/Takuho Mitsunaga

ログとは

●ログとは

- コンピューターシステムやネットワークの活動を記録したデータのことです
- システムが行った操作、ユーザーの行動、エラーメッセージ、重要なイベントなどを記録したものです

●ログの役割と重要性

- システムの動作を監視します
- 問題が発生した時に原因を追跡しやすくします
- 不審アクセスやサイバー攻撃の証拠を見つけることができます

ログの種類

- ログには、Windows、プロキシ、Webサーバ(Apache)のアクセスログをはじめ、たくさんの種類があります
- 今回と次回の講義を通して、以下のログを分析します
 - プロキシログ
 - FWログ
 - ADログ
 - 端末ログ (次回)

ログの分析

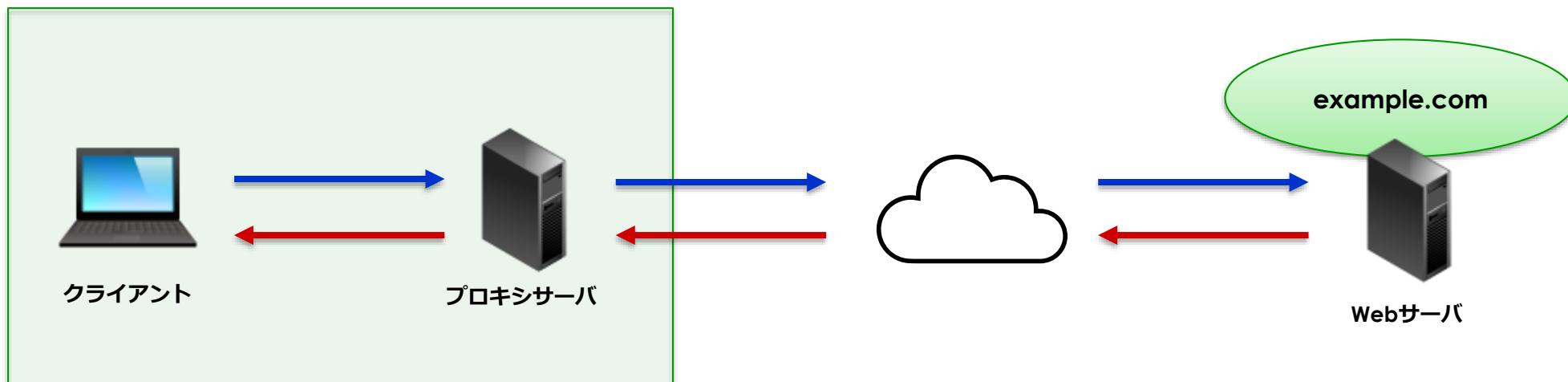
- ログはWebサーバをはじめとする各機器に残っています
- そのため、ログが各所に分散しておりログ調査のたびに該当機器にログインする必要があります
- そこで、ログを集中的に収集、管理、分析するためのツール（SIEM）が販売されており、社会的に注目を集めています
- 今回の演習では、簡易的なログ分析ツールを使用します

ログ分析に必要な観点

- **ログの構成要素理解**: 各機器に残るログには、それぞれ異なる情報が記録されています。各機器で、これらの情報の意味と、それぞれが何を示しているのかを理解することが大切です
- **時間とイベントの関連性**: 特定のイベントが発生した時間を確認し、それが他のシステムイベントや問題とどのように関連しているかを理解することが重要です
- **情報源の比較**: 1つの機器のログだけでなく、他の情報源（例えば、FWログやADログ）と一緒に分析することで、より全面的な視点から問題を理解することができます

プロキシログ

- プロキシサーバに残るログのことです
- プロキシサーバ
 - ネットワーク上でクライアントとサーバの間に位置し、クライアントのリクエストとサーバの応答を**中継する役割**を持つサーバのことです
 - 今回の演習では、内部ネットワークから外部に通信する際に通過する機器と考えてください

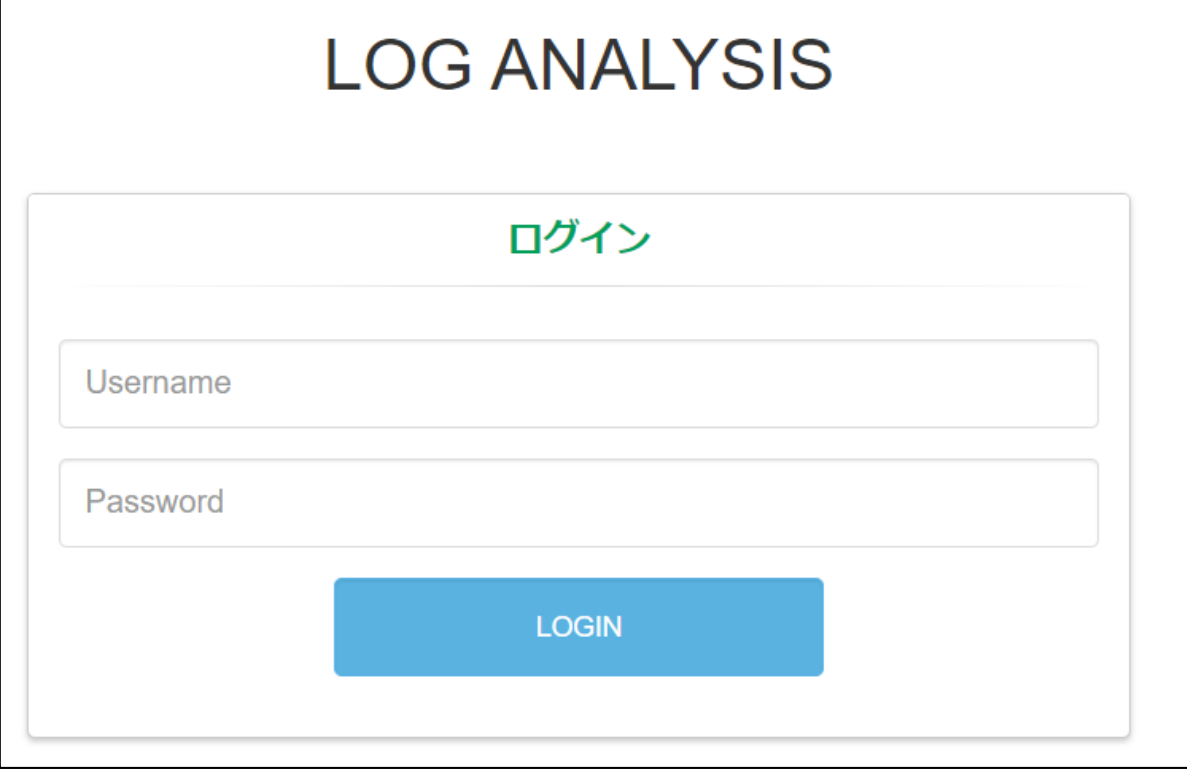


ログ分析ツールへのログイン

● <http://176.34.22.226/users/login> にアクセスしてください

■ Username: admin

■ Password: CoE_Passw0rd!



The screenshot shows a web interface for 'LOG ANALYSIS'. At the top, the title 'LOG ANALYSIS' is displayed in a large, bold, black font. Below the title, the word 'ログイン' (Login) is written in a green font. Underneath, there are two input fields: the first is labeled 'Username' and the second is labeled 'Password'. Both fields are empty. Below the password field, there is a blue button with the text 'LOGIN' in white capital letters.

● 「ログ分析ツール」 を選択します



ユーザー一覧

追加 +

Id	Name	Password	Created	Modified	Actions
1	admin	\$2a\$10\$IEmdCAw1Wvvr6sjW0yNwA.QcNVk8R0Hqp47pR1mJSQeuOB905MZRu	2015-11-04 10:02:30	2021-01-06 06:53:28	View Edit Delete
2	user01	\$2a\$10\$efrLc9Ffdu1JSLynC2yG0eyvL9dyT8nGBS1yfYGfWX18RAxFP14Le	2015-09-17 09:59:54	2015-09-17 09:59:54	View Edit Delete
3	admin	\$2a\$10\$ghljgcUi03imwP3dtTNfoOoS8mvdKliTg9USOXaYxiT.oilPHkaIK	2015-11-09 17:40:06	2015-11-09 17:40:06	View Edit Delete
4	test	\$2a\$10\$HESFTyraB/FsY61QWGHLaOxPJ5cYXyR5Fbm893XUbuUEu8A3TcJIG	2015-12-14 11:42:40	2015-12-14 11:58:12	View Edit Delete
5	pawa1	\$2a\$10\$2Q2COFqgV0fCOVmcZo4gJ.JDxoGq0/bBFH6HseNr0lwKp9uRbS01a	2016-01-18 16:07:45	2016-01-18 16:11:00	View Edit Delete

- 「案件名」のプルダウンから「hands on」を選択します

ログ分析ツール 機械学習 インディケータ ▼ Upload Process

案件管理

案件名

選択してください ▼

選択してください

新規作成 + hands on

ログ分析ツール

プロキシログ

● プロキシログに残る代表的な情報を以下に示します

- **時刻情報**: 各リクエストと応答の発生時刻が記録されます
- **クライアントIPアドレス**: リクエストを送信したクライアントのIPアドレスが記録されます
- **リクエストの種類**: リクエストのメソッド（GET、POSTなど）が記録されます
- **リクエスト先のURL**: クライアントがアクセスしようとしているURLが記録されます
- **応答コード**: サーバからの応答のステータスコード（200 OK、404 Not Foundなど）が記録されます
- **データ転送量**: リクエストと応答のデータ転送量が記録されます
- **User-Agent**: ウェブブラウザなどのクライアントが、自身の情報を識別するための情報が記録されます

プロキシログを見てみよう

- 「プロキシログ分析画面」を選択します

ログ分析ツール 機械学習 インディケータ Upload Process

案件管理

案件名

新規作成 +

hands on

- データ取り込み
- ADログ分析画面
- プロキシログ分析画面
- ファイアウォールログ分析画面
- ファイルサーバログ分析画面
- データ削除

案件ID	5
案件名	hands on
説明	ログ分析ハンズオン
担当者	admin

編集 削除

プロキシログを見てみよう

- 「検索」を選択します

ログ分析ツール
ログ選択
案件管理
機械学習
インディケータ
Upload Process

プロキシログ

案件名 hands on

ログ検索
ログ解析

検索条件

通常検索
送信元IPアドレス、ホスト

インディケータ検索
☒ 全ての条件に一致
☐ いずれかの条件に一致

検索結果に表示する項目

☒ 送信元IPアドレス、ホスト
☒ メソッド
☒ ステータス
☒ 応答サイズ
☒ 日付
☒ 時刻
☒ 送信先IPアド

検索
リセット

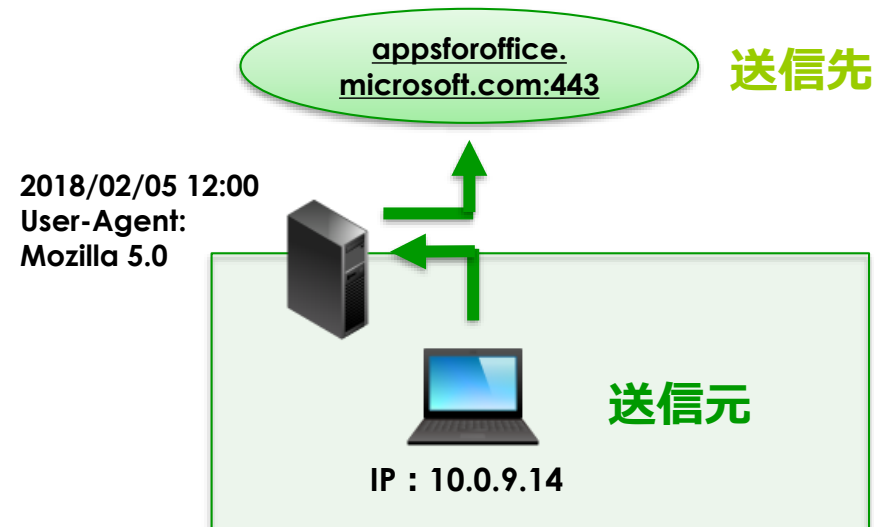
「検索」をクリック

ログ分析ツール

プロキシログを見てみよう

検索結果：4903件

送信元IPアドレス、 ホスト	メソ ド	ステー タス	応答サイ ズ	日付	時刻	送信先IPアドレス、ホスト	Referer	User-Agent
10.0.9.14	connect	200	5576	2018-02-05	09:40:14	appsforoffice.microsoft.com:443		mozilla/5.0 (windows nt 6.1; wow64; trident/7.0; rv:11.0) like gecko
10.0.9.14	connect	200	70922	2018-02-05	09:40:14	appsforoffice.microsoft.com:443		mozilla/5.0 (windows nt 6.1; wow64; trident/7.0; rv:11.0) like gecko
10.0.9.14	connect	200	9287	2018-02-05	09:40:14	appsforoffice.microsoft.com:443		mozilla/5.0 (windows nt 6.1; wow64; trident/7.0; rv:11.0) like gecko
10.0.9.14	connect	200	9635	2018-02-05	09:40:14	appsforoffice.microsoft.com:443		mozilla/5.0 (windows nt 6.1; wow64; trident/7.0; rv:11.0) like gecko



プロキシログの検索

● プロキシログの検索を行う手順

1. 「ログ選択」でプロキシログを選択します
2. 赤枠内に条件を記載します（次スライドで詳しく解説します）
3. 「検索」を選択します

The screenshot shows the 'ログ分析ツール' (Log Analysis Tool) interface. The 'ログ選択' (Log Selection) dropdown menu is open, showing options like 'データ取り込み', 'AD ログ', 'プロキシログ' (highlighted with a blue box and circled with a blue 1), 'FW ログ', and 'ファイルサーバログ'. Below this, the '検索条件' (Search Conditions) section is highlighted with a red box and circled with a blue 2. It contains a search type dropdown set to '送信元IPアドレス、ホスト', a text input field with '10.0.9.15', and a comparison operator dropdown set to '等しい'. There are also radio buttons for '全ての条件に一致' (selected) and 'いずれかの条件に一致'. At the bottom, the '検索結果に表示する項目' (Items to display in search results) section has several checkboxes, all of which are checked. The '検索' (Search) button is highlighted with a blue box and circled with a blue 3.

プロキシログの検索

●検索条件として以下を埋めます

1. プルダウンで対象項目の選択
2. 検索したい値の入力
3. プルダウンで判定基準の選択

①

送信元IPアドレス、ホスト ▼

- 送信元IPアドレス、ホスト
- メソッド
- ステータス
- 応答サイズ
- 日付
- 時刻
- 送信先IPアドレス、ホスト
- Referer
- User-Agent

②

10.0.9.15

いずれかの条件に一致

③

等しい ▼

- 等しい
- 等しくない
- 含む
- 含まない
- 指定した正規表現にマッチ
- より大きい
- より小さい

+

-

プロキシログの検索

- 複数条件で検索したい場合は、赤枠の「+」ボタンを選択し、条件を追加できます

検索条件

通常検索	送信元IPアドレス、ホスト ▼	10.0.9.15	等しい ▼	<div>+ -</div>
インディケータ検索	送信元IPアドレス、ホスト ▼		等しい ▼	

☒ 全ての条件に一致 ☐ いずれかの条件に一致

検索結果に表示する項目

☒ 送信元IPアドレス、ホスト ☒ メソッド ☒ ステータス ☒ 応答サイズ ☒ 日付 ☒ 時刻 ☒ 送信先IPアドレス、ホスト ☒ Referer ☒ User-Agent

検索	リセット
----	------

練習：プロキシログの検索

- 以下の条件を満たすログは何件あるでしょうか。数字で回答してください
 - 応答サイズが「**100,000**」より大きく
 - リクエストメソッドが**POST**

解答：プロキシログの検索

●A.20件

- 「応答サイズ」が「100,000」「より大きい」、「メソッド」が「post」と「等しい」ログを検索することでたどり着けます

検索条件

通常検索	メソッド	post	等しい	+	-
インディケータ検索	応答サイズ	100000	より大きい		
<input checked="" type="radio"/> 全ての条件に一致 <input type="radio"/> いずれかの条件に一致					

検索結果に表示する項目

☒ 送信元IPアドレス、ホスト ☒ メソッド ☒ ステータス ☒ 応答サイズ ☒ 日付 ☒ 時刻 ☒ 送信先IPアドレス、ホスト ☒ Referer ☒ User-Agent

検索	リセット
----	------

検索結果：20件

proxylog_search.csv

エクスポート

FWとは

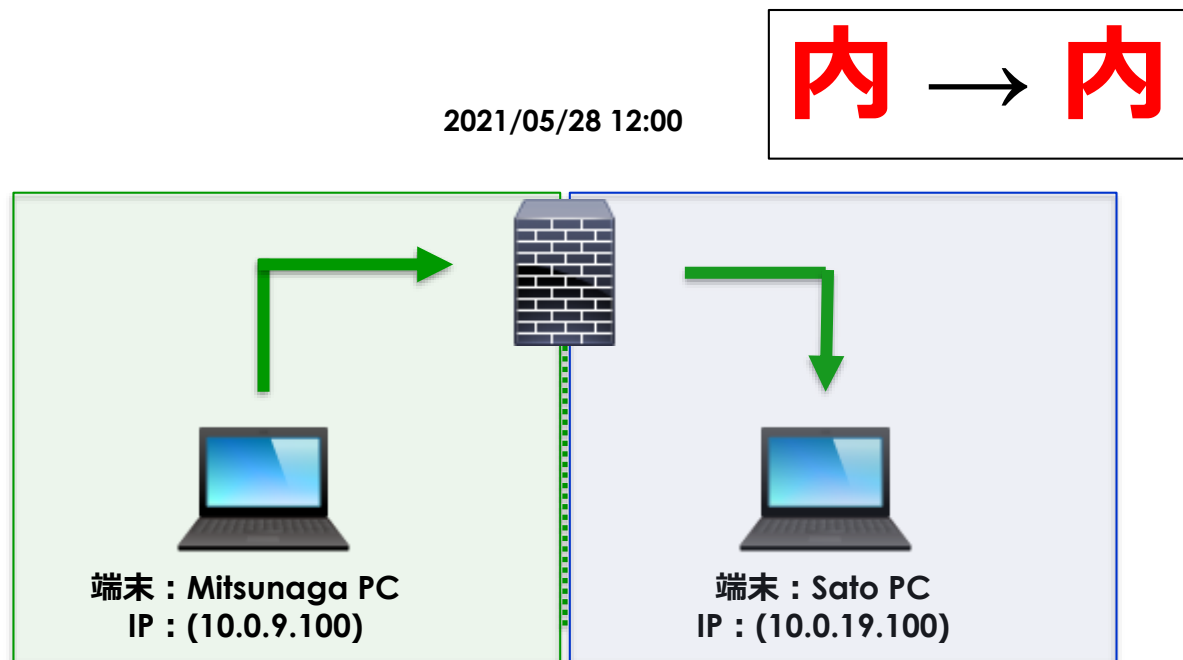
- FW(ファイアウォール)とは、ネットワークの通信を制御できるデバイスまたはソフトウェアのことです
- FWを通過する通信を制御し、許可された通信のみを通過させることができます
 - IPアドレス、ポート番号、プロトコルなどの情報に基づいて通信を制御します
 - パケットの内容まで検査することができるものもあります
- FWが置かれる場所は、以下の2つが代表的です
 - 企業の内部ネットワークとインターネットとの間
 - **ネットワーク内の異なるセグメント間：今回の演習で使用**

FWログ

- FWログは、ファイアウォールが処理した通信の詳細を記録したものです
- 通信の送信元と宛先のIPアドレス、通過したポート番号、その通信が許可されたか拒否されたかなどの情報が含まれています
- ネットワークの問題を診断したり、不審なアクセスや攻撃を検出したりするために使用されます
- 今回の演習で扱うように、**セキュリティインシデントの調査**にも使用されます

本演習でのFWログの役割

- 内部ネットワークから内部ネットワーク（別セグメント）への通信が記録されています



プロキシログとFWログの違い

●FWログ

- ファイアウォールが許可または拒否した通信を記録します
- 通信の送信元と宛先、および通過したポート番号などの情報を含みます

●プロキシログ

- プロキシサーバーを経由した全ての通信を記録します
- ユーザーがアクセスしたURL、アクセスした日時、ブラウザの種類などの**詳細な情報を含みます**
- インターネットの使用状況を監視することを主目的としています

FWログを見てみよう

- 「ログ選択」 からFWログを選択します



ログ分析ツール ログ選択 ▼ 案件管理 機械学習 インディケータ ▼ Upload Process パスワード変更 ログアウト

ファイアウォール
案件名 hands on

ログ検索

データ取り込み
AD ログ
プロキシログ
FW ログ
ファイルサーバログ
データ削除

プロトコル ping 自由入力 ▼ + -

● 全ての条件に一致 ○ いずれかの条件に一致

FWログを見てみよう

- 「日毎のアクセス数サマリ」を選択します

ファイアウォールログ

案件名 hands on

ログ解析

送信元IPアドレス、ホスト

自由入力

☒ 全ての条件に一致 ☐ いずれかの条件に一致

日毎のアクセス数サマリ

送信先IPアドレス毎の送信元IPアドレスのアクセス数

10.0.9.105

相関分析▼

送信元IPアドレス毎のアクセス数

リセット

日毎のアクセス数サマリ

export.csv

エクスポート

送信先IPアドレス、ホスト	Source IPの数	2018-02																											
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
10.0.19.1	1					2100																							
10.0.19.52	2				84			3																					
10.0.9.1	1				4200																								
10.0.9.10	1				2348																								
10.0.9.100	1				4932																								
10.0.9.101	1				8																								
10.0.9.102	1				8																								
10.0.9.103	1				8																								
10.0.9.104	1				8																								

FWログを見てみよう

- 日毎の送信先IPアドレス別のアクセス数が表示されます
- これを見ることで、当該IPアドレスにどれだけアクセスがあったかを確認できます

export.csv

エクスポート

送信先IPアドレス、ホスト	Source IPの数	2018-02																											
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
10.0.19.1	1					2100																							
10.0.19.52	2					84			3																				
10.0.9.1	1					4200																							
10.0.9.10	1					2348																							
10.0.9.100	1					4932																							
10.0.9.101	1					8																							
10.0.9.102	1					8																							
10.0.9.103	1					8																							
10.0.9.104	1					8																							

練習：FWログの検索

- 2018/02/05に10.0.9.129へ何回アクセスがあったでしょうか

解答：FWログの検索

A.8回

- 先ほど紹介した「日毎のアクセス数サマリ」で送信先IPアドレスが「10.0.9.129」のものを探します

10.0.9.120	1			8
10.0.9.121	1			4070
10.0.9.122	1			8
10.0.9.123	1			10
10.0.9.124	1			8
10.0.9.125	1			8
10.0.9.126	1			8
10.0.9.127	1			8
10.0.9.128	1			8
10.0.9.129	1			8

Active Directory (AD) とは

- マイクロソフト社が提供するWindowsコンピュータを集中管理するサービスです
(Windows以外では、利用できません)
- アカウントの認証と認可を管理することができます
 - ユーザがシステムにログインできるかの判定
 - ユーザがアクセスできるリソースの判定

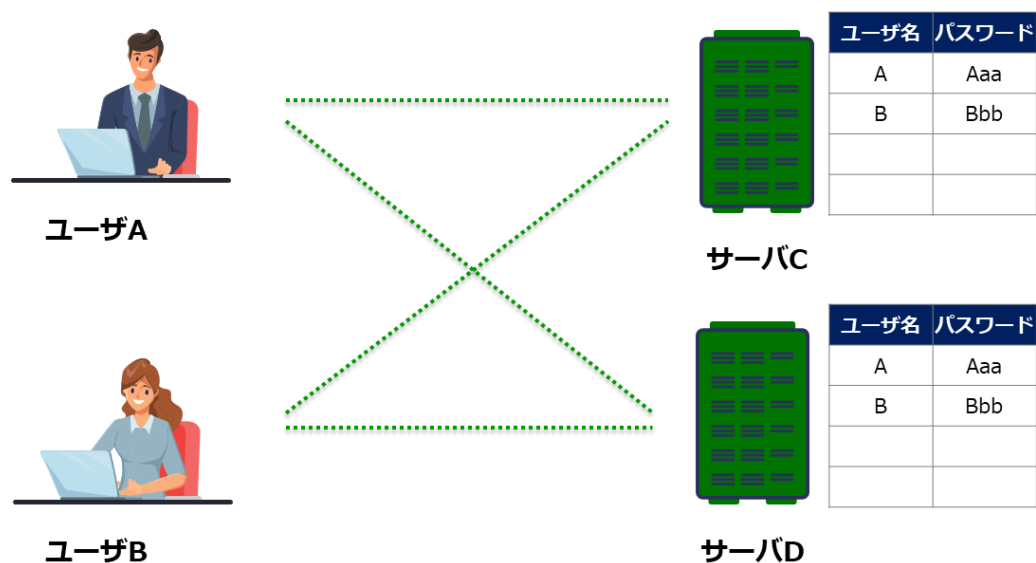
名前	所属	メールアドレス
鈴木 太郎	営業部	suzuki@hoge.jp
中村 好子	営業部	nakaura@hoge.jp
佐藤 一郎	人事部	satou@hoge.jp
横井 潤	開発部	yokoi@hoge.jp



ADを使うメリット

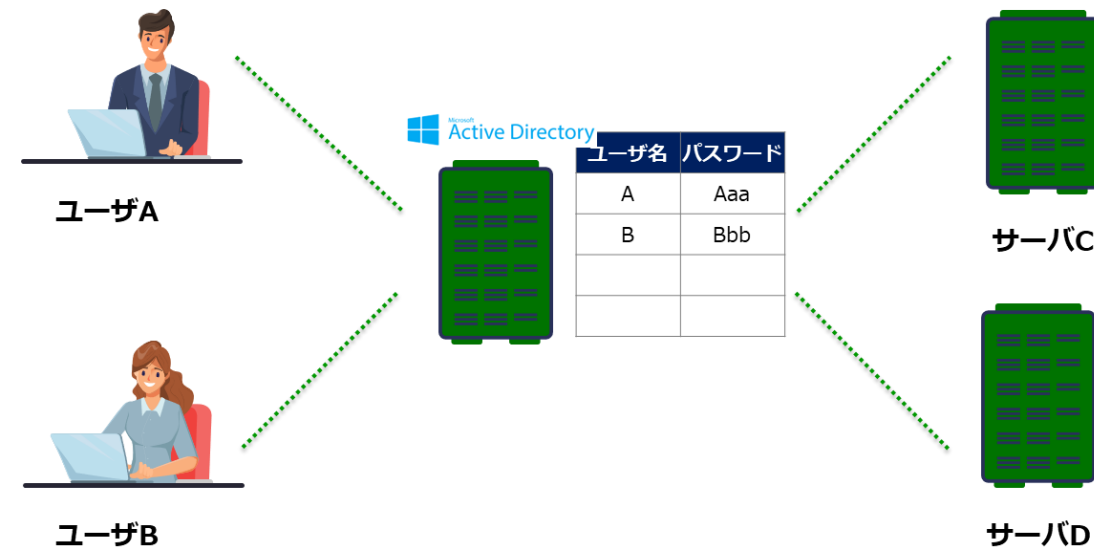
●ADが無い環境

ADが無い環境であれば、もし100台のサーバがあった場合、**それぞれのサーバにユーザを登録**する必要があります



●ADがある環境

ユーザは**ADサーバに登録**をすれば、サーバが100台あったとしても、ADサーバに登録した認証情報でAD環境にある**すべてのサーバにログイン**することができます



ADを使うデメリット

- ADによるアクセス制限が厳しい場合、操作に対して管理者の許可が都度必要になります
- AD導入時に初期コストがかかります
- ADの機能を使いこなすためには、専門的な知識や技術が必要になります
- ADに対する不審アクセスにより、AD環境のコンピュータが乗っ取られる可能性があります

ADログ

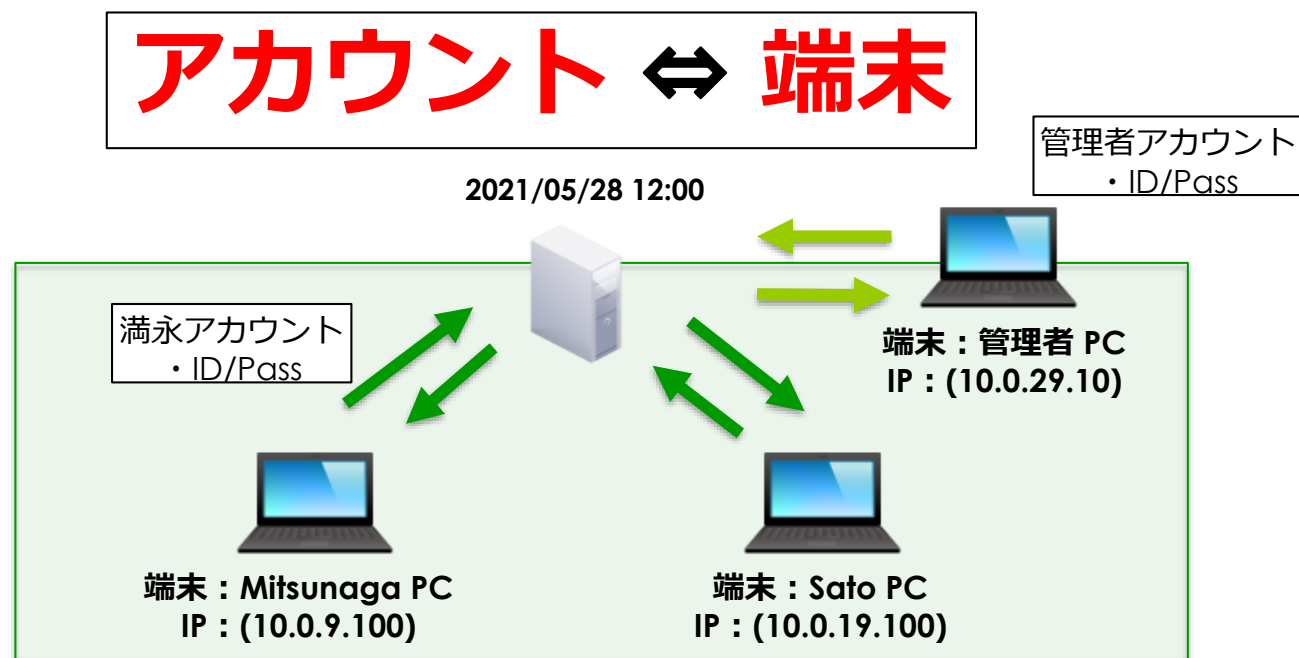
- ADログは、該当AD環境の以下のようなイベントの詳細を記録したものです
 - ユーザのログオンおよびログオフ
 - アカウントの作成や削除
 - パスワードの変更 など
- イベントの管理には固有のイベントIDが使われます
 - 例) ユーザ作成は、ID : 4720で表されます

よく使われるイベントIDの一覧

カテゴリ	Event ID	概要	結果	補足
認証ログ	4624	ログインの成功	-	ログインが成功した際に、ログイン先のコンピュータから記録される
	4625	ログインの失敗	-	ログインが失敗した際に、ログイン先のコンピュータから記録される
	4768	Kerberos認証(TGT要求)	成功 (結果コード: 0x0)	TGT要求が行われた際にログイン元のコンピュータから記録される
			失敗 (結果コード: 0x0 以外)	
	4769	Kerberos認証(ST要求)	成功 (結果コード: 0x0)	ST要求が行われた際にログイン元のコンピュータから記録される
			失敗 (結果コード: 0x0 以外)	
	4776	NTLM認証	成功 (結果コード: 0x0)	NTLM認証が行われた際に、ログイン元のコンピュータから記録される
			失敗 (結果コード: 0x0 以外)	
プロセス	4672	特権の割り当て	-	特権を使用したアクセスを行った際に記録される
	4674	特権を使ったプロセスの実行	-	特権を使用してプロセスの実行を行った際に記録される
	4771	Kerberos事前認証失敗	原因に応じた結果コード	パスワード誤りなど、認証エラーが起きた際に記録される
プロセス	4688	プロセスの生成	-	プロセスが起動された際に記録される
ファイル共有	5140	共有ファイルへのアクセス	-	共有ファイルにアクセスした際に記録される
ユーザ追加	4720	ユーザの追加		ユーザが追加されたときに記録される

本演習でのADログの役割

- どの端末で、どのアカウントが使われてたかを確認することができます
- 通常時、Mitsunaga PC では **満永アカウント** を利用していましたが、突然、Mitsunaga PC から **管理者アカウント** の認証リクエストが送られてくるようなことがあれば怪しいと考えられます



ADログを見てみよう

- 「ログ選択」 からADログを選択し 「検索」 を押します

ログ分析ツール ログ選択 ▼ 案件管理 機械学習 インディケータ ▼ Upload Process パスワード変更 ログアウト

Active Directory

案件名 hands on

ログ検索

AD ログ

プロキシログ

FW ログ

ファイルサーバログ

データ削除

イベント検索 Kerberos 検索 利用アカウント分析 認証回数解析 特権利用分析

検索条件

ドメイン名

等しい

☒ 全ての条件に一致 ☐ いずれかの条件に一致

検索結果に表示する項目

☒ 案件名 ☒ イベントID ☒ 端末 ☒ アカウント ☒ 日付 ☒ 回数 ☒ エラーコード

検索 リセット

ADログを見てみよう

●ADログの一覧が表示されます

案件名	イベントID	端末	アカウント	日付	回数	エラーコード
5	4672		dc	2018-02-05	438	
5	4672		kobayashi	2018-02-05	5	
5	4672		system	2018-02-05	3	
5	4672		dcadmin	2018-02-05	5	
5	4672		akiyama	2018-02-05	3	
5	4624	10.0.9.16	kobayashi	2018-02-05	4	-
5	4769	10.0.9.19	fujimoto@example.local	2018-02-05	9	0x0
5	4769	10.0.9.15	akiyama@example.local	2018-02-05	10	0x0
5	4769	10.0.9.16	dcadmin@example.local	2018-02-05	7	0x0
5	4769	10.0.9.19		2018-02-05	2	0x20
5	4769	::1	dcadmin@example.local	2018-02-05	1	0x0
5	4769	10.0.29.102	fsadmin@example.local	2018-02-05	5	0x0
5	4769	10.0.29.102		2018-02-05	2	0x20
5	4769	10.0.9.16	kobayashi@example.local	2018-02-05	7	0x0
5	4769	10.0.19.52	mitsunaga@example.local	2018-02-05	4	0x0
5	4768	10.0.9.16	kobayashi	2018-02-05	4	0x0

ADログの検索

- プロキシログと同様に検索条件を入力できます
- 複数条件で絞り込みをしたい場合は、「+」ボタンを押してください

検索条件

アカウント ▼

ドメイン名

日付

イベントID

端末

アカウント

エラーコード

等しい ▼

等しい

等しくない

含む

含まない

指定した正規表現にマッチ

+

-

検索条件に一致

アカウント ☒ 日付 ☒ 回数 ☒ エラーコード ☐

検索 リセット

練習：ADログの検索

- アカウント「akiyama@example.local」を使用している端末のIPアドレスを解答してください

解答：ADログの検索

A.10.0.9.15

- 「アカウント」が「akiyama@example.local」に等しいログを検索します

検索条件

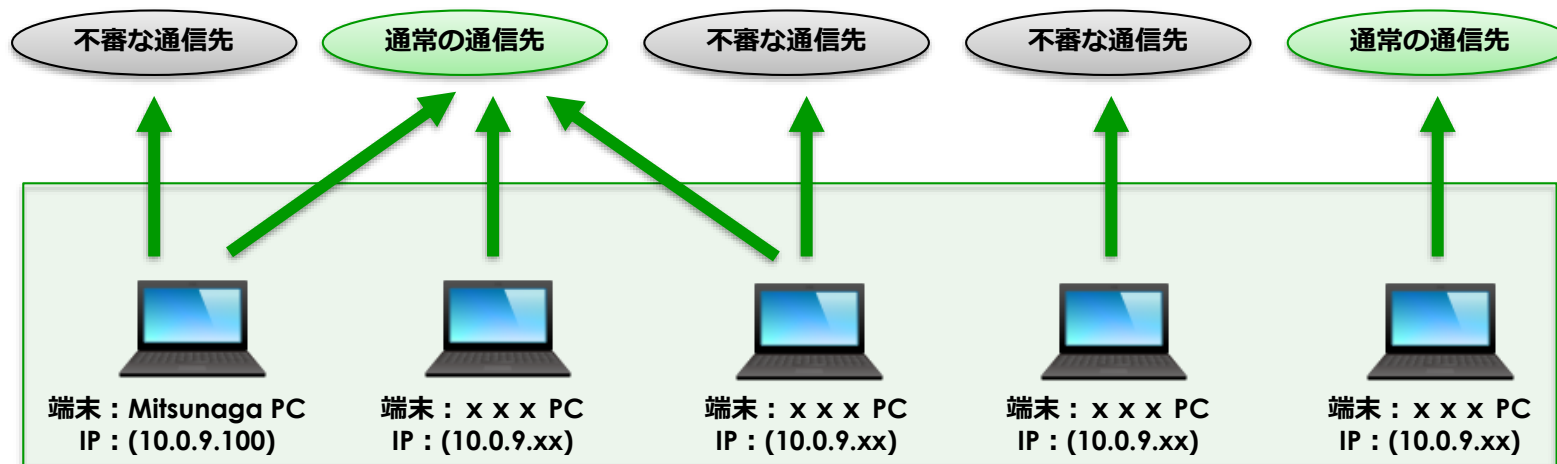
アカウント ▼ akiyama@example.local 等しい ▼ + -

☒ 全ての条件に一致 ☐ いずれかの条件に一致

案件名	イベントID	端末	アカウント
5	4769	10.0.9.15	akiyama@example.local
5	4769	10.0.9.15	akiyama@example.local
5	4769	10.0.9.15	akiyama@example.local

演習の目的/ゴール

- 標的型攻撃における内部展開調査を通じて原因の追究方法を理解し、インシデント対応の勘所を掴む
- 講義時間内に演習が終わるように影響範囲については以下の通りヒントを与える
 - 不審な通信先 3種（サブドメインレベルで分けています）
 - 感染端末 3台



使用するログ

- 先ほどから使用している案件名「hands on」のログを使用します
- 「hands on」ログは、ある組織で起きた標的型攻撃のログの一部を抜粋したものです
- ここまで紹介した以下のログを用いて、インシデント調査を行います
 - プロキシログ
 - FWログ
 - ADログ

案件管理

案件名

hands on



新規作成 +

hands on

① データ取り込み

Q ADログ分析画面

Q プロキシログ分析画面

Q ファイアウォールログ分析画面

Q ファイルサーバログ分析画面

🗑 データ削除

案件ID 5

案件名 hands on

説明 ログ分析ハンズオン

担当者 admin

編集

削除

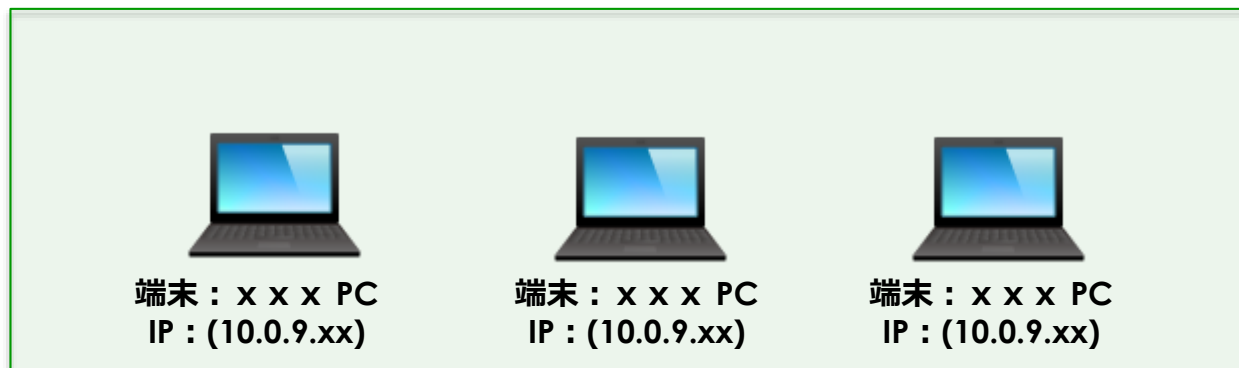
課題

- 前スライドで説明したログから以下を探し出して下さい

■ 3つの不審な通信先

■ 3つの感染端末

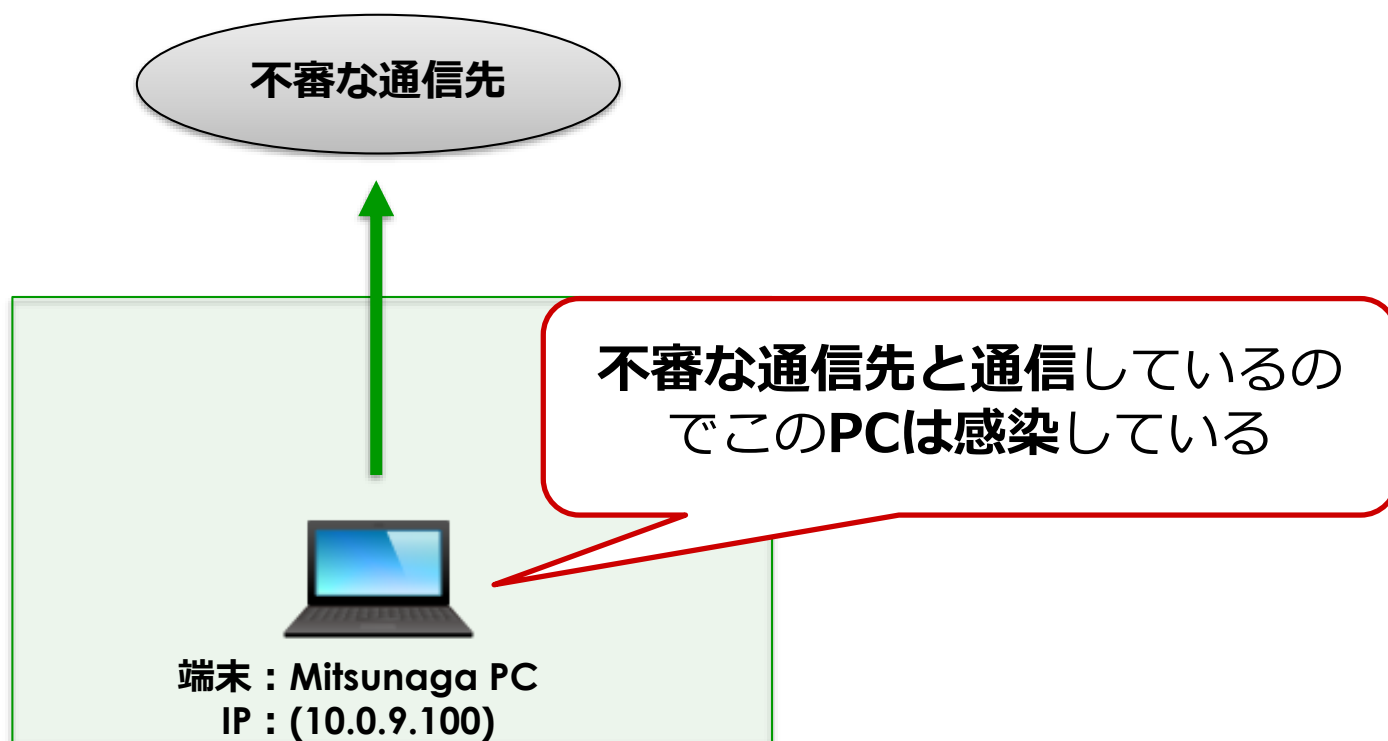
3種類の通信先



3台の感染端末

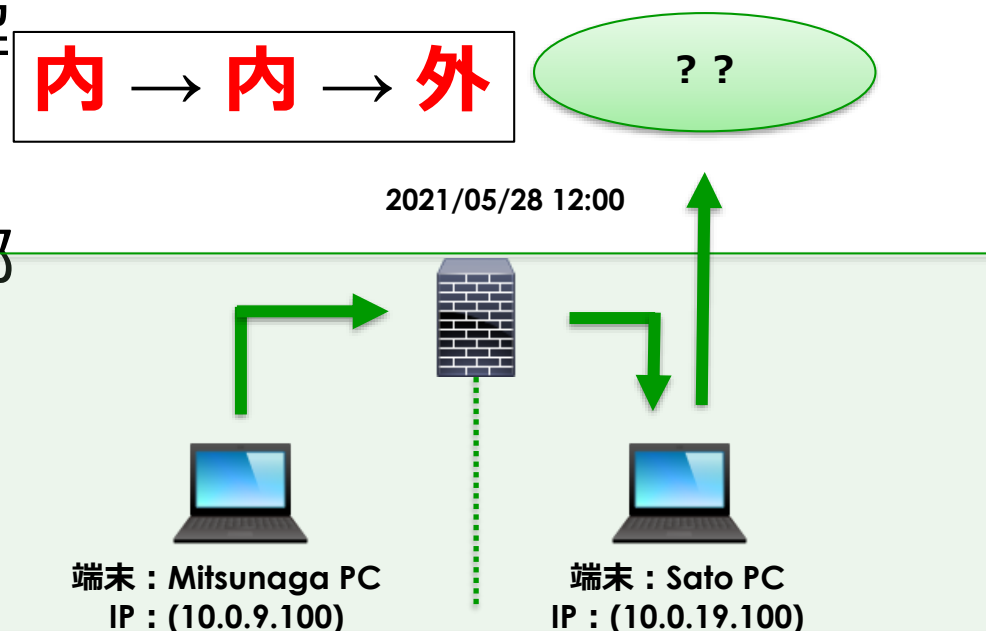
調査の前提

- 本演習では不審な通信先と通信している端末は怪しい（感染している）とします
- ネットワーク構成やログについて、効果的な演習実施を目的として単純化しています（実際のシステム環境は複雑なことも多い）



相関分析

- 1つの機器のログだけでなく、他の機器のログと一緒に分析（**相関分析**）することが重要です
- 講義で利用するツールは相関分析の機能を持っているため、うまく活用して課題を解いてください
- 攻撃者が内部で展開した先の端末から外部への通信を確認できます



調査対象の環境表

- 調査対象組織では、通常時は以下のように運用されています

仮想組織のシステム環境

端末名	端末利用ユーザ	ドメイン管理者のログイン	インターネットアクセス	ローカル管理者IDとパスワード
dc 10.0.29.101	kobayashi (Domain Admins)	許可	不可	
filesv 10.0.29.102	fsadmin (ファイルサーバ管理者)	許可	不可	
fujimotoPC 10.0.9.19	fujimoto (Domain Users)	禁止 (運用ルール上)	可	ID:Administrator パスワード:Passw0rd!
matsudaPC 10.0.9.10	matsuda (Domain Users)	禁止 (運用ルール上)	可	ID:Administrator パスワード:Passw0rd!
satoPC 10.0.9.14	sato (Domain Users)	禁止 (運用ルール上)	可	ID:Administrator パスワード:Passw0rd!
akiyamaPC 10.0.9.15	akiyama (Domain Users)	禁止 (運用ルール上)	可	ID:Administrator パスワード:Passw0rd!
kobayashiPC 10.0.9.16	kobayashi (Domain Admins)	許可	可	ID:Administrator パスワード:Passw0rd!
mitsunagaPC 10.0.19.52	mitsunaga (Domain Users)	禁止 (運用ルール上)	可	ID:Administrator パスワード:Passw0rd!

演習開始

- それでは、不審な通信先と感染端末を探してみましょう！
- 手が出ない人は、まず、プロキシログから不審な通信先を見つけてみましょう！

3種類の通信先



3台の感染端末

外部からの情報共有

- ヒントなしで不審な通信先を見つけることは容易ではありません
- 特に実案件では調査対象の端末が10,000台を超える場合があり、プロキシログのみでは調査は困難です
- 実案件では、外部からの情報提供で、不審な通信先（攻撃者のサーバ）情報が共有されることがあります

情報共有

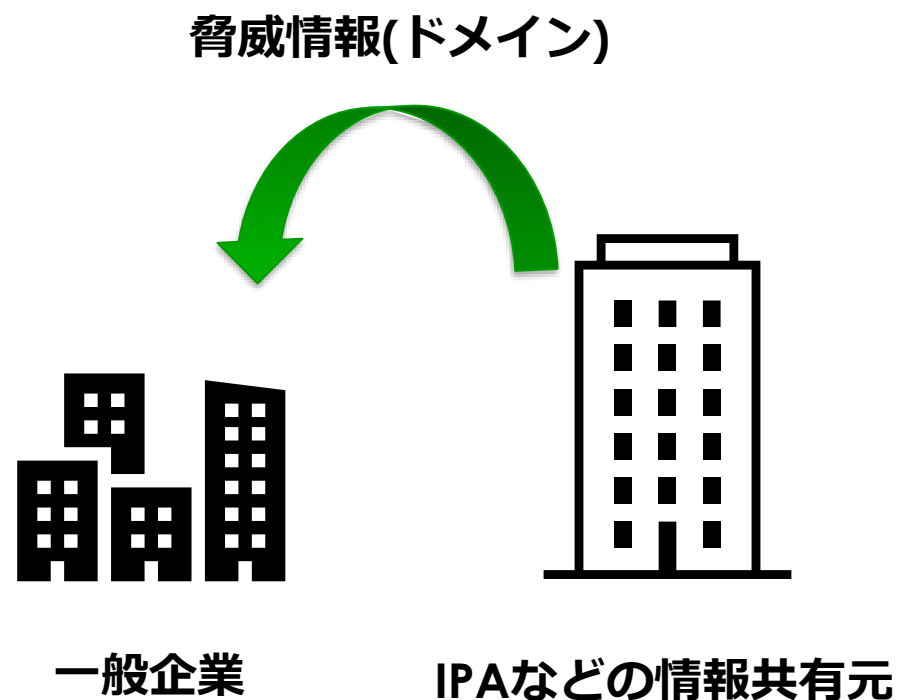
- サイバー攻撃による脅威情報を共有するスキームが存在します

- ISAC（通信、金融、貿易 etc）

- 日本シーサート協議会

- NISC/C4TAP/JISP

- IPA/J-CSIP



ヒント：情報共有

不審な通信先 1 は

watarunrun.com:443

と情報の提供を受けました

3 種類の通信先

watarunrun.
com:443

不審な通信先

不審な通信先



端末：x x x PC
IP：(10.0.9.xx)



端末：x x x PC
IP：(10.0.9.xx)



端末：x x x PC
IP：(10.0.9.xx)

3 台の感染端末

不審な通信先①

- プロキシログの分析で「送信先」が **watarunrun.com:433** と等しいログを検索する

プロキシログ

案件名 hands on

ログ検索

ログ解析

検索条件

通常検索

送信先IPアドレス、ホスト ▼

watarunrun.com:443

等しい ▼

+

-

インディケータ検索

☒ 全ての条件に一致 ☐ いずれかの条件に一致

検索結果に表示する項目

☒ 送信元IPアドレス、ホスト ☒ メソッド ☒ ステータス ☒ 応答サイズ ☒ 日付 ☒ 時刻 ☒ 送信先IPアドレス、ホスト ☒ Referer ☒ User-Agent

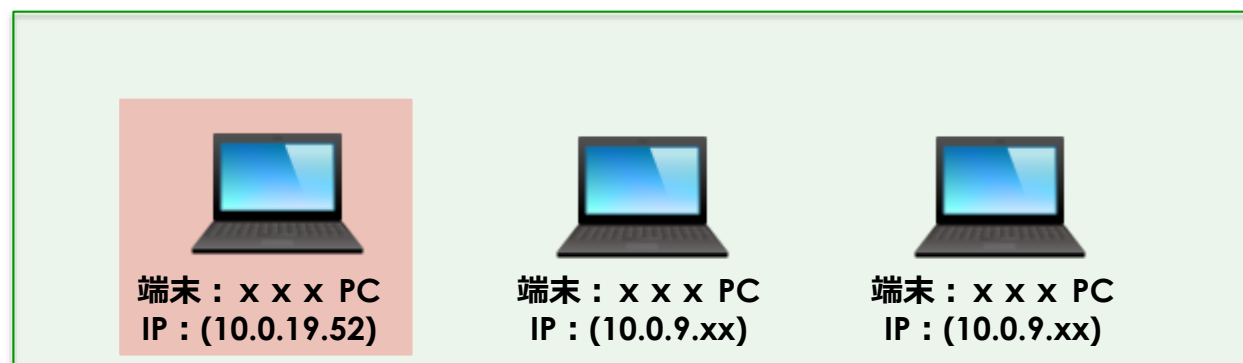
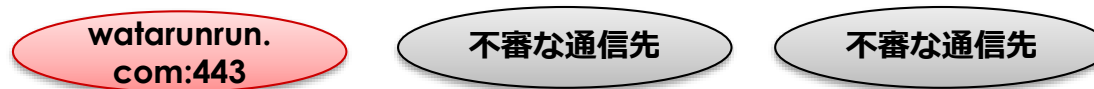
検索

リセット

感染端末①

- 検索結果から、不審な通信先①（watarunrun.com:443）に通信している端末のIPアドレスは**10.0.19.52**と判明しました

3種類の通信先



3台の感染端末

調査継続

- 引き続き調査を進めましょう
- ここまでわかった情報をもとに調査すると仮定すると、どのようなアプローチが考えられますか？

考えられるアプローチ

- watarunrun.com:433 に通信している他の端末を探す
- 10.0.19.52が通信している他の不審な通信先を探す
- 残念ながら上記の2つは、見つけれませんでした。次に考えられる調査方法は何でしょうか

ヒント：相関分析

- プロキシログだけではこれ以上調査が進まないなので、FWログを使い相関分析を行いましょう
- 感染端末①(10.0.19.52)から内部端末への通信を見てみましょう

ファイアウォールログ

案件名 hands on

ログ解析

送信元IPアドレス、ホスト

10.0.19.52

自由入力

☒ 全ての条件に一致 ☐ いずれかの条件に一致

日毎のアクセス数サマリ

送信先IPアドレス毎の送信元IPアドレスのアクセス数

送信元IPアドレス毎のアクセス数

リセット

Search for...

相関分析▼

相関分析

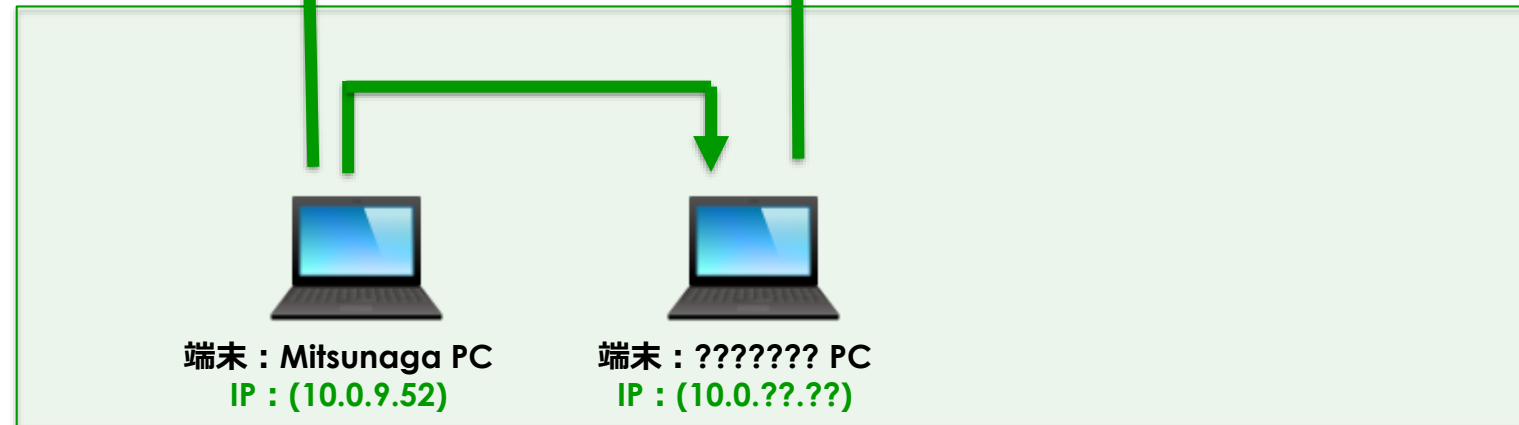
内 → 内 → 外

送信先

watarunrun.
com:443

???

送信元



ヒント：内部ネットワークの通信

- 攻撃者は、ネットワーク内の端末情報を得るために大量のパケットをネットワーク内に送信することがあります
- mitsunaga PC(10.0.9.52)から次の端末に大量な通信を行っていることが判明しました
- 相関分析を行ってみて、感染している端末があるか確認してみよう
 - 10.0.9.10
 - 10.0.9.100
 - 10.0.9.121
 - 10.0.9.15
 - 10.0.9.16

不審な通信先②

- 送信元IPが「10.0.9.15」のプロキシログを調べると不審な通信先①のサブドメインである「**coe.watarunrun.com:443**」が見つかります

プロキシログ

案件名 hands on

ログ検索 ログ解析

検索条件

通常検索 インディケータ検索

送信元IPアドレス、ホスト 10.0.9.15 等しい

全ての条件に一致 いずれかの条件に一致

検索結果に表示する項目

☒ 送信元IPアドレス、ホスト ☒ メソッド ☒ ステータス ☒ 応答サイズ ☒ 日付 ☒ 時刻 ☒ 送信先IPアドレス、ホスト ☒ Referer ☒ User-Agent

検索 リセット

proxylog_search.csv エクスポート

検索結果 : 2050件

10.0.9.15	connect	200	1860723	2018-02-05	17:15:27	coe.watarunrun.com:443
-----------	---------	-----	---------	------------	----------	------------------------

感染端末②

- 検索結果から、不審な通信先② (coe.watarunrun.com:443) に通信している端末のIPアドレスは**10.0.9.15**と判明しました

3種類の通信先



3台の感染端末

ヒント：ADログを見てみよう

- FWログとプロキシログの相関分析では、これ以上の情報を得ることはできませんでした
- 次は、ADログに注目して調査を進めてみましょう

感染端末③

- ADのアカウントの不正利用がないか調べていきます
- 各IPアドレスごとに検索し、アカウントの利用状況を調べます

Active Directory ログ

案件名 hands on

ログ検索

MS推奨イベント検索

Kerberos 検索

利用アカウント分析

認証回数解析

特権利用分析

検索条件

端末

10.0.9.16

等しい

☒ 全ての条件に一致 ☐ いずれかの条件に一致

5	4769	10.0.9.16	dcadmin@example.local	2018-02-05	7	0x0
5	4769	10.0.9.16	kobayashi@example.local	2018-02-05	7	0x0
5	4768	10.0.9.16	kobayashi	2018-02-05	4	0x0
5	4769	10.0.9.16	kobayashi@example.local	2018-02-09	13	0x0

調査対象の環境表（再掲）

- 調査対象組織では、通常時は以下のように運用されています

仮想組織のシステム環境

端末名	端末利用ユーザ	ドメイン管理者の ログイン	インターネット アクセス	ローカル管理者IDと パスワード
dc 10.0.29.101	kobayashi (Domain Admins)	許可	不可	
filesv 10.0.29.102	fsadmin (ファイルサーバ管理者)	許可	不可	
fujimotoPC 10.0.9.19	fujimoto (Domain Users)	禁止 (運用ルール上)	可	ID:Administrator パスワード:Passw0rd!
matsudaPC 10.0.9.10	matsuda (Domain Users)	禁止 (運用ルール上)	可	ID:Administrator パスワード:Passw0rd!
satoPC 10.0.9.14	sato (Domain Users)	禁止 (運用ルール上)	可	ID:Administrator パスワード:Passw0rd!
akiyamaPC 10.0.9.15	akiyama (Domain Users)	禁止 (運用ルール上)	可	ID:Administrator パスワード:Passw0rd!
kobayashiPC 10.0.9.16	kobayashi (Domain Admins)	許可	可	ID:Administrator パスワード:Passw0rd!
mitsunagaPC 10.0.19.52	mitsunaga (Domain Users)	禁止 (運用ルール上)	可	ID:Administrator パスワード:Passw0rd!

感染端末③

- IPアドレスが「**10.0.9.16**」の端末で本来使われるはずのない「dcadmin@example.local（管理者アカウント）」が使われています

Active Directory ログ

案件名 hands on

ログ検索

MS推奨イベント検索

Kerberos 検索

利用アカウント分析

認証回数解析

特権利用分析

検索条件

端末

10.0.9.16

等しい

☒ 全ての条件に一致 ☐ いずれかの条件に一致

5	4769	10.0.9.16	dcadmin@example.local	2018-02-05	7	0x0
5	4769	10.0.9.16	kobayashi@example.local	2018-02-05	7	0x0
5	4768	10.0.9.16	kobayashi	2018-02-05	4	0x0
5	4769	10.0.9.16	kobayashi@example.local	2018-02-09	13	0x0

不審な通信先③

- IPアドレスが「10.0.9.16」の端末から怪しい通信がないかをプロキシログから調べます
- 目視ではわかりにくいので、これまでの不審な通信先との通信の特徴で検索します

不審な通信先③

- 不審な通信先①・②の共通点として「User Agent」の項目が「mozilla/4.0」であることが挙げられます
- User Agentの項目に「mozilla/4.0」かつ、送信元IPが「10.0.9.16」の通信を検索します

プロキシログ

案件名 hands on

ログ検索

ログ解析

検索条件

通常検索

インディケータ検索

User-Agent

mozilla/4.0

含む

+

-

送信元IPアドレス、ホスト

10.0.9.16

等しい



全ての条件に一致



いずれかの条件に一致

不審な通信先③

- 1つのログが検索結果として出力されます
- <https://reverse-edge.com/uploader/upload.php>

検索結果：1件

送信元IPアドレス、ホスト	メソッド	ステータス	応答サイズ	日付	時刻	送信先IPアドレス、ホスト	Referer	User-Agent
10.0.9.16	post	200	478	2018-02-05	19:12:19	https://reverse-edge.com/uploader/upload.php		mozilla/4.0 (compatible; msie 8.0; windows nt 6.0)

解答：課題

- 不審な通信先と感染端末は以下でした

3種類の通信先

watarunrun.com:443

coe.watarunrun.com:443

https://reverse-edge.com/uploader/upload.php



端末：xxx PC
IP：(10.0.19.52)



端末：xxx PC
IP：(10.0.9.15)



端末：xxx PC
IP：(10.0.9.16)

3台の感染端末

グループディスカッション

- 時系列に沿って、今回、攻撃者が何を行ったかを説明できるようにホワイトボードに書いてみましょう
- 併せて報告用にスライドを作ってみましょう

- 年金機構の事例では、攻撃者は窃取したIDやアカウントを悪用して、被害を拡大させてたとされる
- 同様のサイバー攻撃被害事例でもID・アカウントの悪用が確認されている（土曜・夜間など想定していないアクセスも多い）

