HITACHI
Inspire the Next

Hitachi Systems Security Journal

VOL.31

株式会社 日立システムズ

Human * IT

Hitachi Systems security Journal VOL.31

TABLE OF CONTENTS

●はじめに
本文書は、株式会社日立システムズ の公開資料です。バックナンバーは以下の Web サイトで確認できます。
https://www.hitachi-systems.com/report/specialist/index.html

説明会開催から結果発表・表彰式までの 10 カ月間を追跡

サイバーセキュリティ小説コンテスト 丸ごとレポート

取材・文・撮影＝斉藤健一

サイバーセキュリティ小説コンテストとは

本年 3 月 3 日、東京・秋葉原において「抗え。この世界（インターネット）の脅威に。」と題するイベントが開催された。NISC（内閣サイバーセキュリティセンター）がサイバーセキュリティ月間（2 月 1 日～ 3 月 18 日）の期間にあわせて主催したものだ。人気漫画が原作の TV アニメ「約束のネバーランド」とタイアップし、作品にまつわるトークセッションや暗号を解きながら秋葉原の街を歩くスタンプラリーなどが行なわれ、多くの参加者を集めた。

このイベントの中では「サイバーセキュリティ小説コンテスト」の表彰式も行なわれた。その模様は後に紹介させていただくこととして、まずはコンテストの概要などをお伝えしたい。

このコンテストは JNSA（特定非営利活動法人日本ネットワークセキュリティ協会）が主催し、KADOKAWA が運営を担当する。セキュリティのコンテンツを目にする機会を増やし、正しいセキュリティ知識の普及、セキュリティ人財育成、セキュリティ意識とリテラシーの向上などを目的としている。

コンテストのキャッチフレーズである「君の物語（ストーリー）で世界（ネット）を救え！」には、サイバーの世界は人間が作り出したものであり、人間が想像力を発揮することによって安全・安心も高められるというテーマが込められている。そして、この想像力をストレートに表現できるのが小説というわけだ。

作品のジャンルは問わないが「サイバーセキュリティに興味がわくような小説」というテーマで募集が行なわれた。応募方法は小説投稿サイト「カクヨム」での作品公開、期間は 2018 年 3 月 31 日～ 8 月 31 日。大賞作品は角川スニーカー文庫より書籍化される他、賞金 100 万円が授与される。

キービジュアルのキャラクターを配したコンテストのポスター

参加者を支援する数々の取り組み

サイバーセキュリティというテーマ、小説という表現手法、そのどちらにも精通している人はわずかだろう。これは主催者も承知しており、コンテストでは参加者を支援するためのさまざまな取り組みが行なわれた。

※ 1 **ハッカーが選んだネタ記事リンク集** https://www.jnsa.org/novel_contest/link.html

・ハッカーが選んだネタ記事リンク集

JNSA の Web サイトで公開された特設ページ※1。コンテスト協賛企業による情報セキュリティの基礎知識、実際に起きたサイバー攻撃事件のニュース、セキュリティ企業が発行する脅威レポートなどがまとめられている。特筆すべきは「小説のネタ」という視点でピックアップされたニュース記事の数々だ。スパイ映画を地で行くようなレポートや、SF の世界に登場するかのようなテクノロジーなど興味深い話題も多く、コンテスト参加者に限らず一般の人が読み物として楽しめるものとなっていた。

・小説の書き方を指南する説明会

2018 年 5 月 13 日、東京・秋葉原で開催され 60 名を超える参加者が集まった。コンテスト参加者を大別すれば 2 つのグループに分かれる。1 つは普段から小説を執筆しているがサイバーセキュリティには精通していない人たち。もう一方は仕事などでサイバーセキュリティに携わっているものの小説の執筆経験を持たない人たちだ。

説明会では両者に向けた情報が提供された。前者に向けた技術的な講演は、名和利男氏（サイバーディフェンス研究所）と加藤雅彦氏（長崎県立大学 教授・コンテスト副実行委員長）が担当し、後者に向けては河野葉月氏（KADOKAWA カクヨム編集部 編集長）が進行役を務めたディスカッションが行なわれた。パネルには前述の名和氏と加藤氏に加え、本川祐治（当社・コンテスト実行委員長）が参加、「テーマ設定」「読者像」「キャラクター」「技術のリアリティ」といった観点から討議が行なわれ、作品作りに役立ちそうなアイデアがいくつも語られた。例えば、テーマ設定ではサイバーセキュリティの他にも恋愛や家族といった普遍的な内容を盛り込み厚みを持たせることや、キャラクターの配置では必ずしも主人公をハッカーにする必要はないといったものだ※2。

また、説明会の最後には登壇者への個別相談の時間も設けられた。セキュリティの専門家の前には自分のアイデアが技術的に成立するかどうかを確認したい参加者が並び、カクヨムスタッフの前には小説の書き方を質問する参加者が列を作っていた。

施設見学会の日程

日付	見学施設名
5 月 29 日	制御システムセキュリティセンター（宮城県多賀城市）
5 月 30 日	カスペルスキー　東京本社（東京都）
6 月 4 日	サイボウズ 東京オフィス（東京都）
6 月 5 日	日立システムズ 統合 SOC（東京都）
6 月 6 日	日立システムズ 千里データセンター（大阪府豊中市）
6 月 7 日	ラック JSOC（東京都）
6 月 12 日	長崎県立大学 セキュリティ演習室（長崎県西彼杵郡）
6 月 13 日	セコム ショールーム MIRAI（東京都）

・関連施設の見学会

コンテスト協賛企業の協力などにより、小説の舞台となり得る場所の見学会も行なわれた。IT 企業のオフィス、データセンター（DC）、セキュリティ・オペレーション・センター（SOC）など、部外者が立ち入ることのできない所も多い。施設によっては物理セキュリティの観点から所在地すら明らかにされていないものも含まれていたので、見学会は貴重な機会だったと言える。

見学施設のリストは表のとおりだ。筆者も制御システムセキュリティセンター（CSSC）、当社 統合 SOC および千里 DC の見学会に参加した。CSSC では液体の流量を制御するプラントやタンク内の気圧を調整するシステムを例に攻撃のデモを見学した。後者のデモではタンクに見立てられたゴム風船が攻撃で制御機能を失い膨張・破裂するといった演出もあり、わずかではあるがサイバーテロをリアルに感じることができた。

一方、統合 SOC や千里 DC では施設の性質を踏まえ、建物の安全性（災害・停電への対策）や入退管理といった物理セキュリティについてもレクチャーが行なわれた。

どの見学会も平日に行なわれたため参加者は少なめだったそうだが、参加者によるレポートがカクヨム内で公開されていたので、創作の参考にした人は多かったのではないだろうか。

※ 2 本稿では紙幅の都合で具体的な内容は割愛させていただくが、カクヨムユーザーの橘ミコト氏がパネルディスカッションの内容を詳細をまとめている。このコンテストは 2019 年度も開催されることが決定しているので、次回の参加を検討している人は必読だろう。
https://kakuyomu.jp/works/1177354054885635376/episodes/1177354054885883133

表彰式終盤の様子　舞台上手に主催者側、下手に受賞作作家陣が並んでいる

・Twitter による質問窓口

コンテストでは参加者が技術面で疑問に感じたことを質問できる環境が Twitter で整えられていた。もちろん回答は技術的な内容に限られる。主催者によれば、これを利用した参加者も多かったそうだが、作品のネタバレにつながるケースもあり、質問・回答のやり取りの多くはダイレクトメッセージで行なわれたという。

優秀作品の発表と表彰式

コンテストの応募総数は 248 作品で、主催者の予想を大きく上回ったという。まず一次選考としてカクヨム編集部がふるいにかけ 27 作品が選出、さらに二次選考を経て 6 作品にまで絞られた。最終選考では JNSA・協賛各社・スニーカー文庫編集部・赤野工作氏（作家）が加わり、多角的な視点から審査が行なわれ、受賞 4 作品が決定し、2018 年 12 月 19 日に開催された SECCON 2018 において発表された。

記事冒頭で紹介した受賞式には、当社 本川祐治、長崎県立大学 加藤雅彦氏、KADOKAWA 河野葉月氏、NISC 文月涼氏、日本マイクロソフト 藤本浩司氏、サイボウズ 明尾洋一氏が登壇。各作品の講評が行なわれた※3。

・大賞「目つきの悪い女が眼鏡をかけたら美少女だった件」noisy（ノイジー）

NISC 文月氏：この作品はサイバーセキュリティ、学園モノ、ボーイ・ミーツ・ガールの側面を持つ。少女がハッカーで主人公の少年は彼女がしていることを理解するために勉強して成長していく。NISC としては若い人がハッカーに興味を持ち技術を磨くことを望んでいるが、この作品にはリアルな人間を感じることができた。描かれている技術的な部分もリアルで好印象だった。作品の緊張感を和らげるためのコミカルな場面・掛け合いなどもあり、小説として完成している点や、作家に対する今後の期待を込めて大賞に推した。

・マイクロソフト賞「ハクスタジア」半藤一夜（はんとう・いちや）

藤本氏：長編でありながら細部にいたるまで作り込まれておりロジックの破綻もない完成度の高い作品だと感じた。

※3 最終選考 6 作品のあらすじと総評はカクヨムで公開されている
https://kakuyomu.jp/contests/cyber_security

大賞受賞者 noisy 氏のコメント

大賞作品「目つきの悪い女が眼鏡をかけたら美少女だった件」の著者である noisy 氏は、IT コンサルタントを務めると同時に IT ジャーナリストとしての顔も持つ。ライトノベルのコンテストにはこれまで何度か挑戦してきたというが、今回はサイバーセキュリティがテーマということで、まるで自分のために存在するコンテストかのように思えたという。

執筆で苦労したのはホワイト（ハット）ハッカーをいかに魅力的に描写するかという点だったそうだ。というのも多くの作品でカッコ良く描かれるのはブラック（ハット）ハッカーだからだ。正義のハッカーを増やすというコンテストの趣旨と作品のダイナミズムとの間で悩んだという。

また、この作品は中編の連作という形になっているが、これにも狙いがあったという。何より長編に比べてテンポ良く書けるといった点や、複数のストーリーを描くことで自らの引き出しの多さをアピールできる点だったそうだ。

これらの狙いは間違っておらず見事に大賞を射止め、現在は書籍化に向け改稿を進めているという（編注：角川スニーカー文庫から本年 5 月 1 日の発売が決定。「噂の学園一美少女な先輩がモブの俺に惚れてるって、これなんのバグですか？」に改題。著者名も瓜生聖に変更となった）。

・サイボウズ賞「電脳剣客カプリッチオ」HerBert（ヘルベルト）

明尾氏：サイバーセキュリティの要素が少なく大賞には選ばれにくい作品だが、その世界観やキャラクター、さらにはストーリー展開にいたるまで候補作品の中でいちばん楽しく面白いと感じた。

・日立システムズ賞「電子の海の aLiCE」村雲唯円（むらくも・ゆいえん）

本川：ライトノベルらしい作り。世界の IT 産業において日本企業がプレゼンスを発揮できていない現実の中、日本企業が世界を席巻するような OS を作っているという作品の設定に希望を感じた。

表彰式後半では受賞作品の作家陣を交えたトークセッションが行なわれた。主催者側からは選考の舞台裏が明らかにされた。大賞を決定する投票では図らずも 2 作品の得票が同数となってしまい、苦肉の策として選考委員を 1 人減らして改めて投票を行なったそうで、それぞれの賞が白熱の議論の末に決まったことが述べられた。

一方、作家陣からはコンテストに応募した経緯や執筆で苦労した点などが語られた。特にサイバーセキュリティとライトノベルをどのような割合でミックスしていくのか、そのバランスの難しさ複数の作家が述べてるのが印象的だった。

そして、表彰式の最後には 2019 年度のコンテスト開催もアナウンスされた。5 月には詳細が発表されるとのこと。

作品の投稿はハードルが高いことだが、カクヨムに投稿された小説を読むことはそれほど難しいことではないはずだ。スマートフォンにカクヨムのアプリを入れてテキスト読み上げ機能を使えば漢字の読み間違いが多少はあるものの気軽に気軽に触れることができる。興味がある方には是非ともお勧めしたい。

Splunk CTF “BOTS” に挑戦

文 =A&T

はじめに

こんにちは。日立システムズの A&T です。今回は、2018 年 12 月 21 日に開催された、“BOTS v1” にチャレンジしてきましたので、ここに報告します。

BOTS とは、主に Splunk※1 を用いて行なう Jeopardy 形式の CTF（Capture The Flag）で、初回は Splunk 社が米国で開催したカンファレンス “.conf” 内にて、2016 年に行なわれました。BOTS は、Boss of the SOC の略称で、SOC アナリストなどのセキュリティ運用経験者を対象として、3 ～ 5 名程度でチームを組み競います。

BOTS は、日本においても 2017 年に 1 度、2018 年には 2 度開催され、当社は 2018 年から参加させていただいております。今回私たちは、Splunk 代理店業務に携わっているメンバーや、SOC で分析業務を担当している若手メンバーなど、社内で Splunk を取り扱う有志を募り、チームを組んで参加しました。なお、日本で開催されている BOTS は、米国にて開催された内容と同等のものであり、いわば出張版 CTF となっています。

結果から報告しますと、惜しくも全 10 チーム中 3 位という結果でした（図 1）。Splunk 社によると、BOTS では 1 万点を越えるのはハードルが高いところ、今回は、1 万点越えが 4 組もいたそうで、いつもよりも参加者のレベルは高めとのことでした。

事前準備

私たちは 2018 年から BOTS に参加しています。前回出場した際、私たちは Splunk を利用開始したばかりで、Splunk のサーチ処理言語である SPL

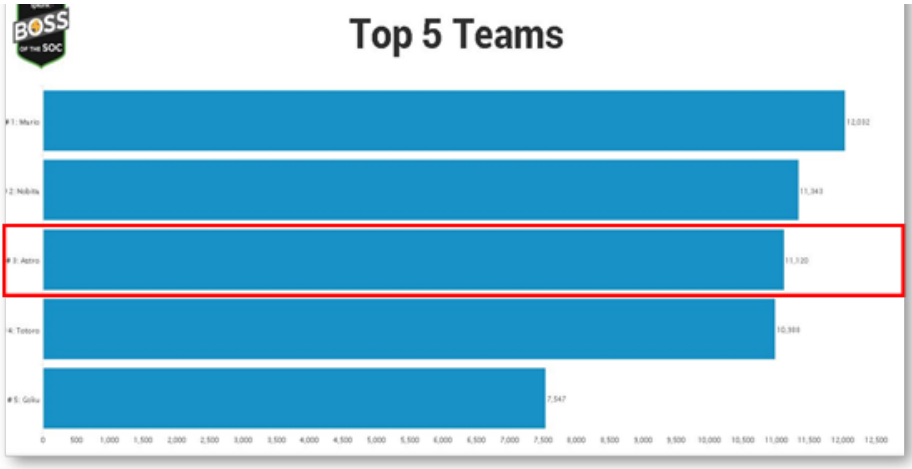

図 1 BOTS の結果（上位 5 チームのみ）

※ 1 Splunk とは、さまざまなテキストデータを取り込み、検索、監視、分析、可視化を可能とし、大量のデータの中から、得たい情報だけを瞬時に探し出せることを製品コンセプトとする、IT システムのためのマシンデータ分析プラットフォーム。

について基本的な操作方法しか知識がない状態でした。また、事前準備も十分とはいえない状態で大会に臨んだため、太刀打ちできない問題も多くありました。

今回の挑戦では、前回の反省を生かして、簡易的ではあるものの実際に Splunk が動作する検証環境を構築し、Splunk の操作方法や SPL について学習しました。また、実際に Splunk を利用しているメンバーに対して Splunk でよく使う SPL に関して質問し、その意味を理解するなど、しっかりと事前準備を行なってから競技に臨みました。

BOTSv1 のシナリオと出題例

BOTSv1 では、下記のシナリオのどおり競技が行なわれます。

> ウェイン社（架空企業）は、サイバー攻撃を防御すべく、アナリスト、アリス・ブルバードを雇っています。今回、あなたはアリス・ブルバードとなり、ウェイン社で発生したセキュリティインシデントの調査を行ない、サイバー攻撃の全貌を明らかにする必要があります。

このシナリオの下、Splunk 社が出題する問題を解くことにより、少しずつ調査が進み、サイバー攻撃による侵害の経緯の詳細が判明していきます。この際、調査に必要なログはすべて Splunk 社によって、用意されております。また、調査に有用な Splunk もあらかじめ用意されており、参加者これを用いて調査を進めます。

次に、実際に解いた問題例について紹介します。

＜問題＞
ブルートフォースアタックに利用された**最初のパスワード**は？

＜解答例＞

本問題は、セキュリティにかかわる方には、基本的でもあるブルートフォースアタック（総当たり攻撃）にかかわる問題です。ブルートフォースアッタクは、ID やパスワードを 1 文字ずつずらして、ログインを試行するなど、理論的にありうるパターンすべてを入力する攻撃手法です。そのため、短時間内に大量のアクセスがある可能性があります。また、ログインに必要なアカウント情報を POST パラメータに含めるなどにより、クエリを送信していることことが想定されました。実際に、Splunk を用いて確認すると、ログイン認証に必要なアカウント情報は、「form_data」フィールド内の username と passwd のパラメーターでクエリを送っていることが分かります。

ここで私たちは以下の点に着目して、問題を解きました。

1. Splunk の SPL を利用することで、ユーザー名とパスワードは、ワイルドカード (*) を使って検索する（例：form_data=*username*passwd*）
2. 検索結果を見やすくするために table コマンドを利用してデータをテーブルで表示させる（| table）
3. 最初のパスワードを検索するために時間を分かるようにする（_time）

これらの点に含めた SPL は以下のとおりです。

```
index=botsv1 sourcetype=stream:http form_data=*username*passwd* | table _time form_data
```

この SPL を用いて検索を実施すると図 2 の結果が得られます。

しかし、この結果は最近のログから順に表示されているため、最初のパスワードを検索することができません。今回の設問は「最初のパスワード」のため、reverse コマンドを利用して順序を入れ替えます。

```
index=botsv1 sourcetype=stream:http form_data=*username*passwd* | table _time form_data  | reverse
```

この SPL を用いて検索を実施すると古いものから表示されることから、回答である「12345678」を得ることができました（図 3）。

日光尾瀬かたしなエクスプレス号【東武日光駅～中禅寺温泉～湯元温泉～日光白根山
湯元温泉線【湯元温泉～日光白根山ロープウエイ～鎌田～旭待峠行バス連絡所】

2018年5月1日(火)～2018年10月28日(日)の間の毎日運行

	停留所名	湯元鎌田	日光駅鎌田EXP	湯元日光白根	湯元旭待連	中禅寺鎌田EXP	
bk01	東武日光駅		8:35				
bk03	中禅寺温泉 着		9:17				
	中禅寺温泉 発		9:22			15:35	
bk06	光徳温泉日光アストリアホテル		9:36			15:49	
bk07	湯元温泉 着		9:45			15:58	
	湯元温泉 発	8:40	9:48	11:15	13:15	16:01	1
bk08	菅沼	8:55	10:03	11:30	13:30	16:16	1
bk09	丸沼温泉曙湖荘	9:10	10:18	11:45	13:45	16:31	1
bk10	丸沼ダム	9:15	10:23	11:50	13:50	16:36	1
bk11	日光白根山ロープウエイ	9:18	10:26	11:53	13:53	16:39	1
bk12	丸沼高原第1ペンション村	9:19	10:27		13:54	16:40	1
bk13	丸沼高原第2ペンション村	9:20	10:28		13:55	16:41	1
-	唐沢	9:22	↓	↓	13:57	↓	1
-	発電所入口	9:24	↓	↓	13:59	↓	1

図 2 認証試行に関するログの抽出結果

_time	form_data
2016/08/11 06:45:21.226	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=12345678&9d873c2becd118318849d13cf18b60ff=1
2016/08/11 06:45:21.247	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=qwerty&af4df60674155567dee0566f87045251=1
2016/08/11 06:45:21.250	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=1234&aaf6297ae5c1e3df78a421bc55548d16=1
2016/08/11 06:45:21.241	username=admin&863349a657c211fbfeb90ebe9427654c=1&task=login&return=aW5kZXgucGhw&option=com_login&passwd=letmein
2016/08/11 06:45:21.260	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&76e93e8488d9a46878468d88954a0d54=1&passwd=123456
2016/08/11 06:45:21.263	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=football&d1181413b1a70460b8d425cec799cdca=1
2016/08/11 06:45:21.826	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=michael&bd5d773b68cdb015b021218ff36a2c4a=1
2016/08/11 06:45:22.000	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=master&0a5d789b1af633e3de4b3dc95daa1877=1
2016/08/11 06:45:22.002	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=superman&cab483edaec06d4e888547d33f57becb=1
2016/08/11 06:45:22.012	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=dragon&45b663f3374634ca3fd860101177601c=1

« 前へ 1 2 3 4 5 6 7 8 9

図 3 先の抽出結果の順番を入れ替えた結果

なお、回答のみ表示させる SPL は、以下のとおりです。

```
index=botsv1 sourcetype=stream:http http_
method=POST
| rex field=form_data
 “passwd=(?<userpassword>\w+)”
| search userpassword=*
| reverse
| head 1
| table userpassword
```

おわりに

今回は、途中で 1 位に浮上するも残りの 15 分程度で他チームに追い抜かれてしまい、残念ながら最終的には 3 位という結果に終わりました（次頁図 4）。

前回参加時は 3,000 点台だったことを考えると、今回大きく点数を伸ばすことができました。問題は前回と異なるものの、事前準備の成果があったと考えます。

BOTS は、ある架空の会社でセキュリティインシデントが発生したことを想定し、より実業務に近い形で CTF を実施します。通常の CTF では、さまざまな解析ツールを使用して解決の糸口を探しますが、Splunk を中心に調査するなど、SOC を含めた実際のセキュリティ運用の現場に近い形で、技術力を図れる点が興味深い点です。BOTS への参加はセキュリティ運用を実施している企業の方に限られていますが、今回ご紹介した BOTSv1 のデータセットはインターネット上に公開されており誰でもこの問題に取り込むことができます。ぜひ興味のある方は、データセットをダウンロードして、取り組んでみてはいかがでしょうか（問題と答えを表示するアプリも用意されています）。

最後に余談となりますが、本稿の執筆にあたっ

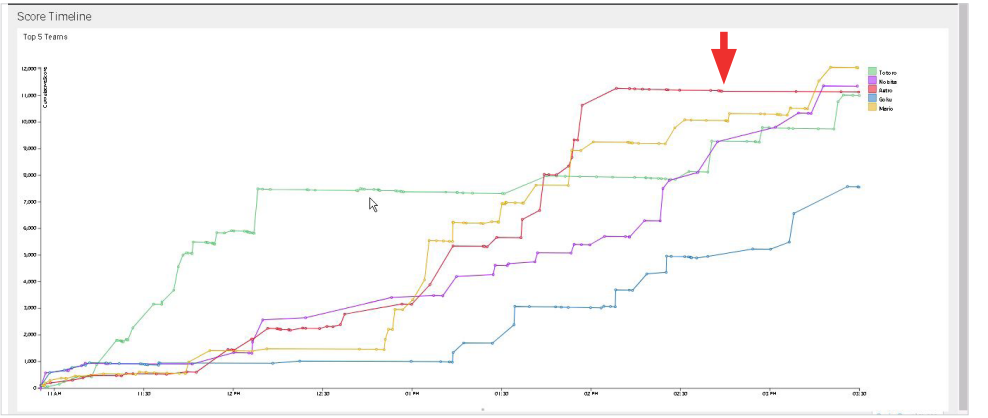

図 4 得点獲得の状況（ゲーム後半に首位に立つが、その後得点を重ねることができずに 3 位でフィニッシュ）

ては Splunk 社に連絡を取り、BOTS の問題と解答例を掲載する許可を得ました。この時、Splunk 社から以下のような提案がありました。

BOTS への参加は原則としてセキュリティ運用を実施している企業の方に限られるそうですが、Splunk の導入を戦略的に検討している企業の方がおられれば、個別の開催も可能とのこと。

問い合わせは同社 Web サイトのフォームで受け付けています。検討されている担当者には良い機会だと思います。

参考 URL

1. BOTSv1 DataSet https://github.com/splunk/botsv1
2. Splunk 社 問い合わせ窓口 https://www.splunk.com/ja_jp/talk-to-sales.html

Human * IT

人と IT のチカラで、驚きと感動のサービスを。

Hitachi Systems Security Journal VOL.31

株式会社 日立システムズ
本社 〒141-8672 東京都品川区大崎 1-2-1