サイバー攻撃脅威連携のカタチ

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 取締役 技術開発部長)
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)

LAC
株式会社ラック

スピーカー紹介

CYBER GRID JOURNAL VOL.12 座談会にて撮影(2021年6月)

Agenda

1. 組織の現状と課題 – サイバー脅威分析と情報共有・連携
2. SecureGRIDアライアンス構想
3. 実証実験レポート
4. 最後に

01

サイバー脅威分析と情報共有・連携
現状と課題

脅威分析と情報共有・連携

■環境認識

- **高度で複雑なサイバー攻撃の台頭**

→標的型攻撃、二重脅迫型ランサムウェア、サプライチェーン攻撃など、対策が自組織だけでは終わらずにより複雑に。

- **脅威やICT環境の変化スピードが早い**

→クラウド、デバイスの普及、守備範囲が広域

- **セキュリティ製品や見えない脅威に対する対応策の普及**

→EDR/NDR/XDR、サイバー脅威インテリジェンス、脅威ハンティングなどが流行

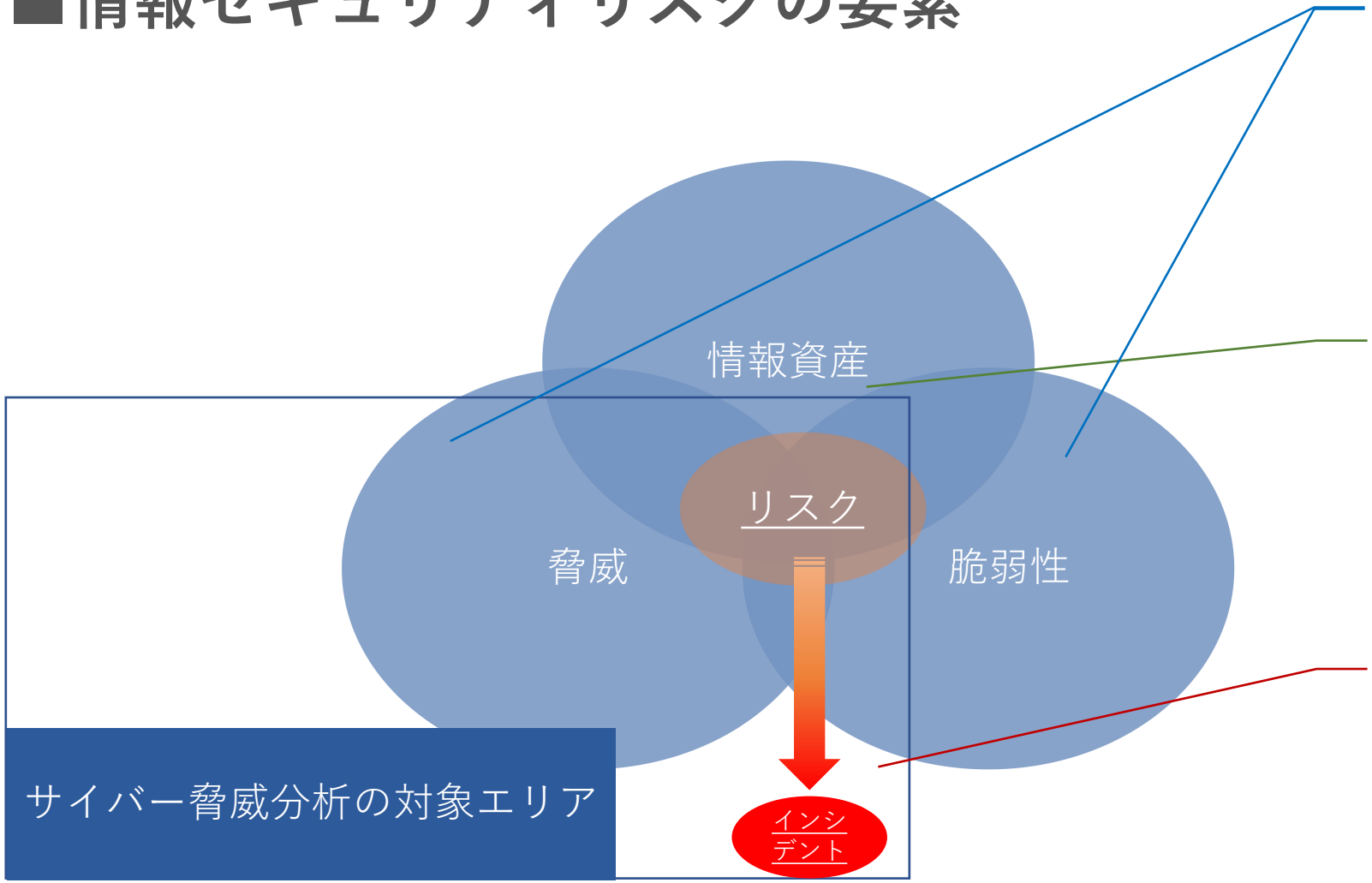
脅威分析と情報共有・連携

■「サイバー脅威分析」とは

- 自組織に対してサイバー攻撃の影響がある、もしくは関連するサイバー脅威を知ること
- その上でどのような**リスク**が発生するか
- **リスク**に対してどのような対策を取れば良いのか

脅威分析と情報共有・連携

■情報セキュリティリスクの要素



脅威・脆弱性
組織に関係がある脅威・脆弱性かは分からない

リスク
組織でインシデントが発生する(してる)可能性が高い

インシデント
インシデントのトリアージと原因究明・影響や攻撃背景

脅威分析と情報共有・連携

■組織に求められる「サイバー脅威分析」とは

- まずは組織の「情報資産」「脆弱性」「脅威」を把握する
- 「リスク」「インシデント」の発生をなるべく無くす
- 万が一「リスク」「インシデント」が発生してもそれを早期発見する

Q. 組織の「サイバー脅威分析」、現状・課題は？

脅威分析と情報共有・連携

■「情報共有・連携」とは

- 情報共有
  - 情報を「蓄積」して「共有」、「活用」すること

- 情報連携
  - 同じ目的において情報のやりとりを行うこと

Q. 組織間で行う脅威情報の共有・連携の必要性は？

02

SecureGRIDアライアンス構想

SecureGRIDアライアンス構想

■SecureGRID(セキュアグリッド)アライアンスとは

- サイバー脅威に対抗すべく、組織間の相互協力を高め、システムを通じた新たな「脅威情報共有・連携体制」実現を目指す取り組み

- もとは、当研究所の新しいSOCモデルの構想から生まれたもの。研究活動とアライアンス参加組織のセキュリティ強化や新しい情報共有・連携のカタチを探究する取り組みへと進化

SecureGRIDアライアンス構想構想

■SecureGRIDアライアンス全体像

- Webポータル「SecureGRID Portal」を介した情報連携
- オープンソース脅威情報共有基盤「MISP」を活用
- ラックによる分析機能による提供

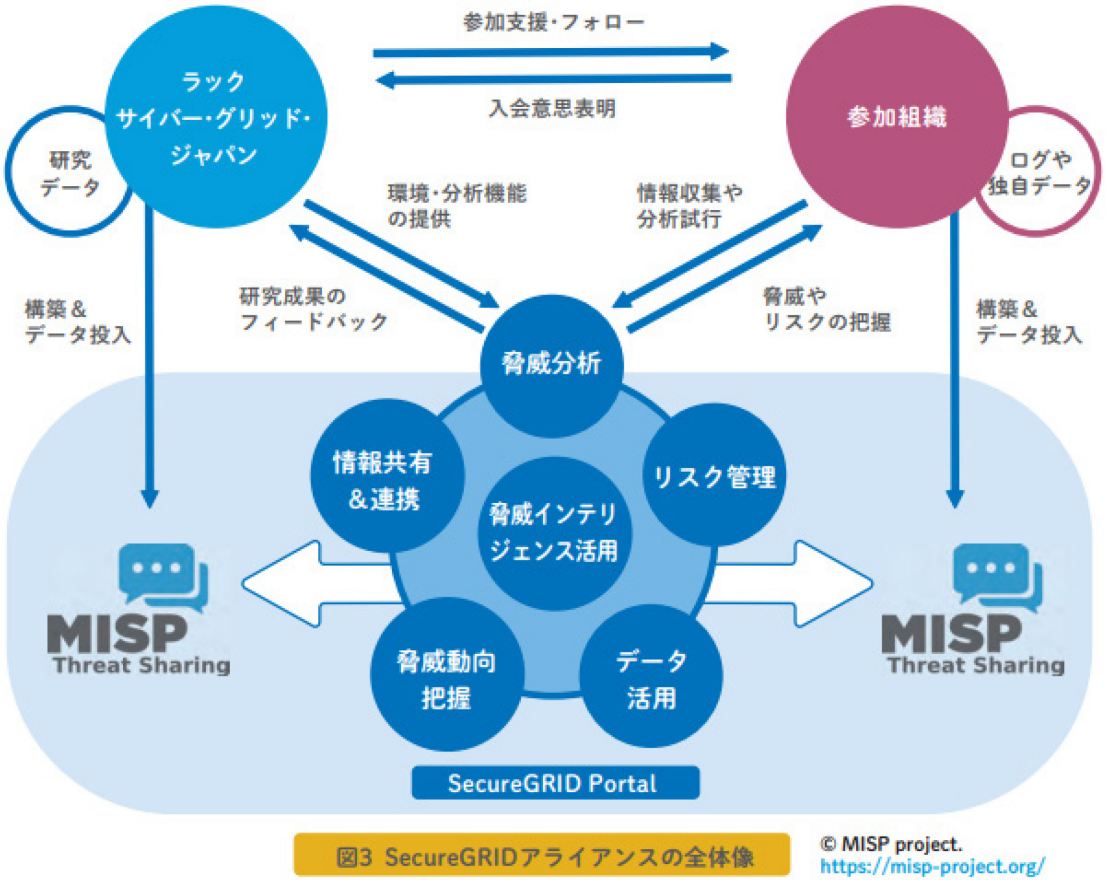


図3 SecureGRIDアライアンスの全体像

SecureGRIDアライアンス構想

■活動概要

- 脅威情報共有基盤「MISP」とそこに入れるデータをご用意いただく
- 「SecureGRID Portal」とMISPをAPIによって連携
- メンバーは「SecureGRID Portal」にログインして自組織を含めた参加組織のMISPに対して横断検索を実行することができる。

SecureGRIDアライアンス構想

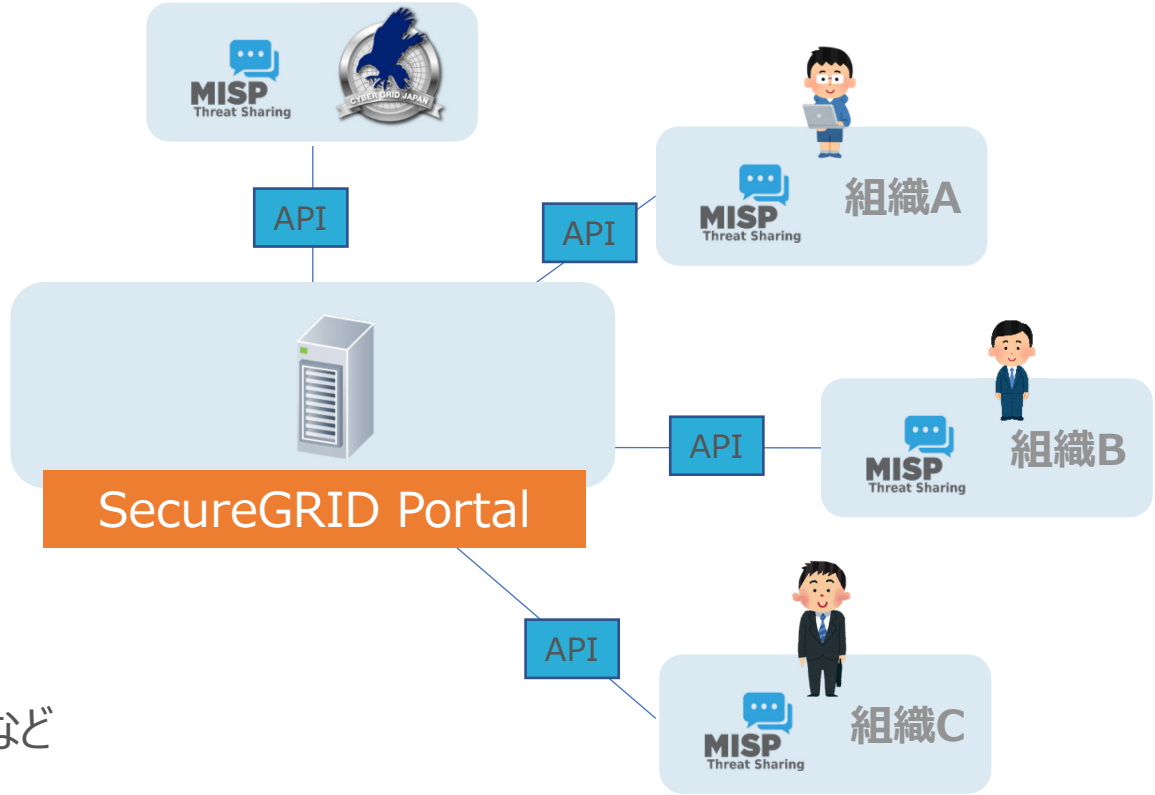
■活動概要

参加組織・メンバーは、２つの役割としての活用方法がある。

SecureGRID Portal利用者

- IPアドレス
- ドメイン名
- URL
- ファイルハッシュ値　など

MISPオーナー



SecureGRIDアライアンス構想

■特長

- [Portal利用者]、MISP横断検索を実行することができる。（他組織のMISPにはログインできない）

- [MISPオーナー]は、他のメンバーがMISP横断検索を実行した検索値を確認することができる（自組織のMISPでヒットした値のみ）

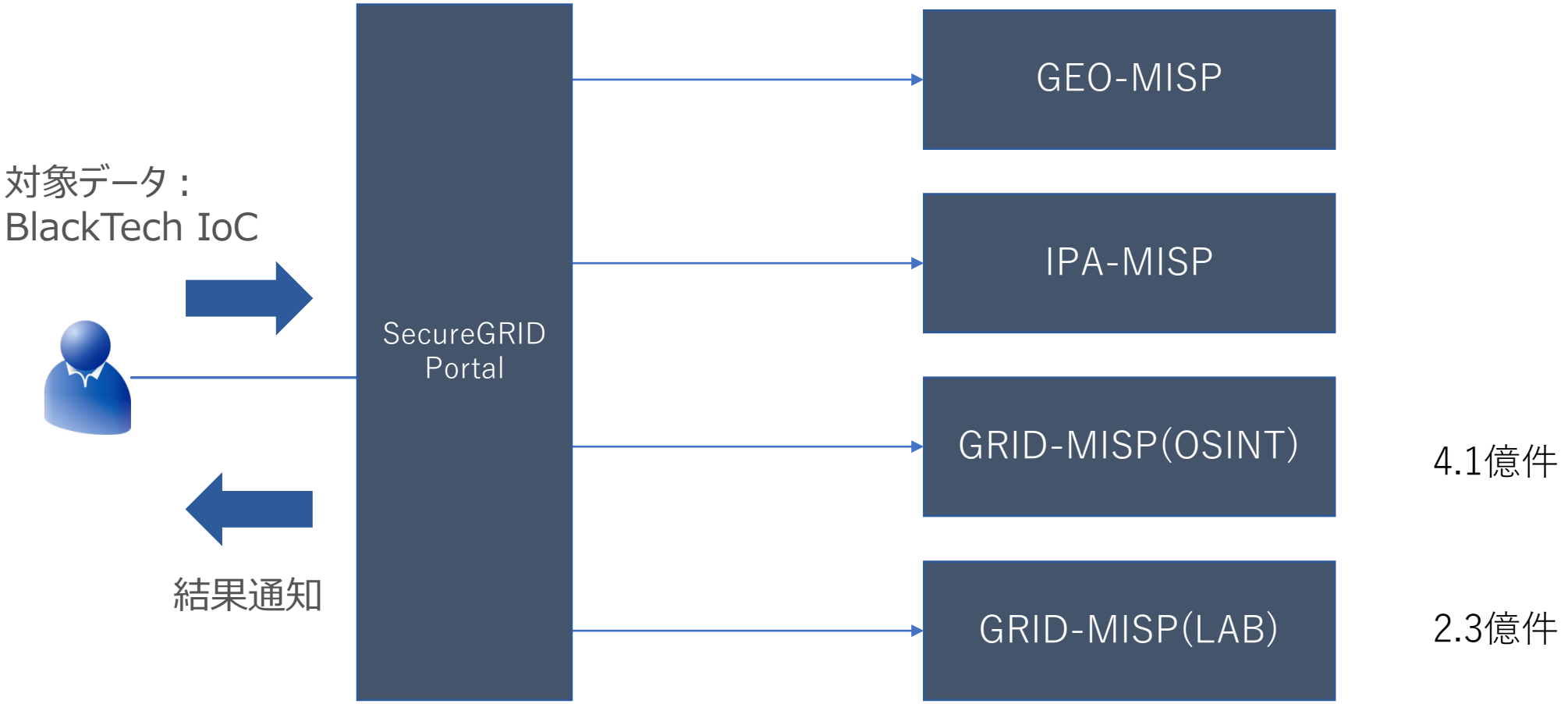
- 本活動を活性化させるツールや分析機能などの提供
  - 「Exploit分析」や「フィード連携機能」のツール提供
  - 研究成果として脅威情報配信や情報提供(コンテンツは検討中)

03

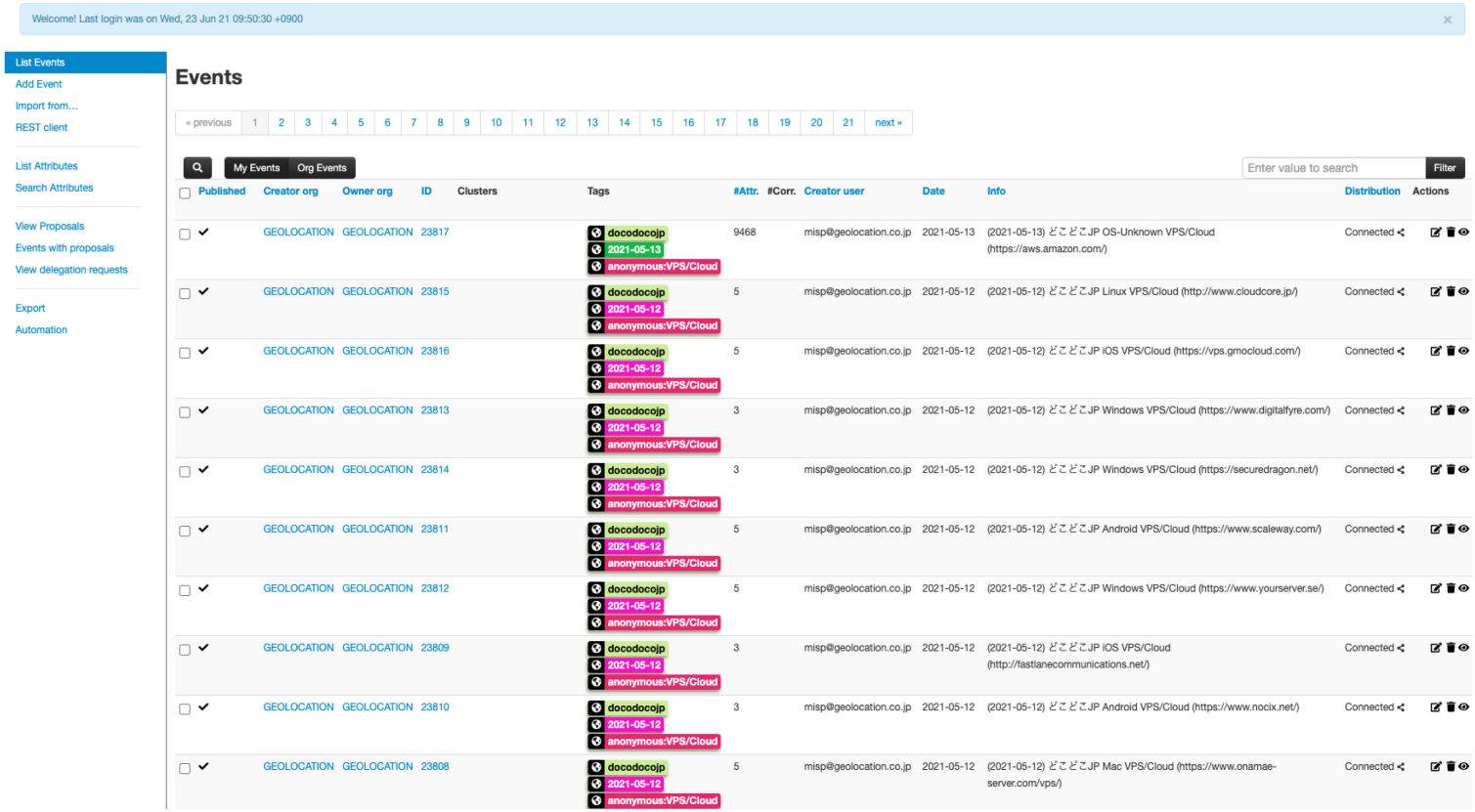
実証実験レポート

実証実験レポート

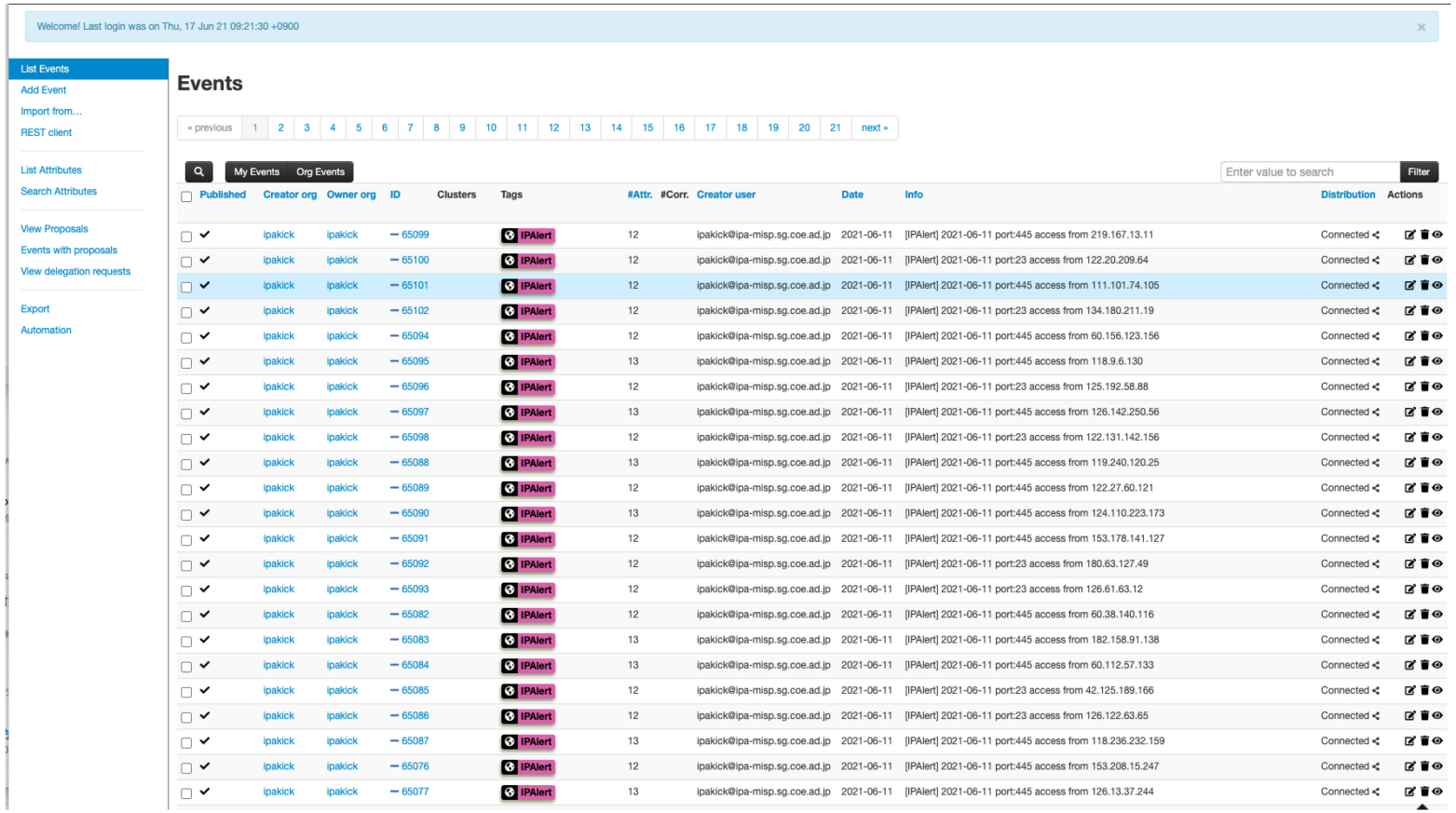
■実施方法



■GEO-MISP
「どこどこJP」のアクセスログ→匿名属性に該当する送信元IPを投入



■IPA-MISP
ハニーポット「IPAlert」→攻撃元IPをMISPに投入



■検索値について

- 当研究所の別の研究結果を活用

サイバー攻撃集団「BlackTech」のIOC

タイプ		IP/Domain件数
public	公開済みIOC	361件
lac_original	ラックが発見した信頼性の高いIOC	153件
suspicious	ラックが発見、疑い・可能性があるデータ	196件
合計		710件

IPアドレス、ドメイン名のIOCで実施

■実施結果

- 当研究所の別の研究結果を活用
サイバー攻撃集団「BlackTech」のIOC

タイプ	853件中のヒット件数
GEO-MISP	13
IPA-MISP	0
GRID-MISP(OSINT)	355
GRID-MISP(LAB)	177

■GEO-MISP 13件のヒット結果

No	ヒット	source	GRID-MISP	OSINT-MISP	GEO-MISP	asn_country_code	GEO-MISP
1	13.249.153.121	publicな検体 4e6d5983775d52215ab6779a928796c60f57321b9c65f4b89135bc0c9b880103 の通信先として観測されたIP。	0	0	2	US	どこどこJP OS-Unknown VPS/Cloud (https://aws.amazon.com/)(2)
2	184.168.221.70	yasonbin[.[info→dxc.yasonbin[.]info の2018年ごろの紐づくIP	9	0	1	US	どこどこJP OS-Unknown VPS/Cloud (https://jp.godaddy.com/)(1)
3	184.168.221.86	wesogo[.]com→forum.wesogo[.]com　の2019.5の紐づくIP	12	6	1	US	どこどこJP OS-Unknown VPS/Cloud (https://jp.godaddy.com/)(1)
4	3.223.115.185	wesogo[.]com→sakura.wesogo[.]com	31	15	18	US	どこどこJP OS-Unknown VPS/Cloud (https://aws.amazon.com/)(18)
5	40.81.188.85	ubnotes.ignorelist[.]com→に紐付くIP	1	17	2	US	どこどこJP OS-Unknown VPS/Cloud (https://azure.microsoft.com/)(2)
6	45.32.43.59	https://teamt5.org/tw/posts/mjib-holds-briefing-on-chinese-hackers-attacks-on-taiwanese-government-agencies/	0	15	1	US	どこどこJP OS-Unknown VPS/Cloud (https://www.vultr.com/)(1)
7	45.76.102.145	http://blog.jpcert.or.jp/2018/03/malware-tscooki-7aa0.html https://www.macnica.net/file/mpressioncss_2018-1h-report_mnc_rev3_nopw.pdf https://www.lac.co.jp/lacwatch/people/20180425_001625.html	2	1	1	US	どこどこJP OS-Unknown VPS/Cloud (https://www.vultr.com/)(1)
8	45.76.189.109	https://teamt5.org/tw/posts/mjib-holds-briefing-on-chinese-hackers-attacks-on-taiwanese-government-agencies/	0	15	1	US	どこどこJP OS-Unknown VPS/Cloud (https://www.vultr.com/)(1)
9	50.63.202.81	linestw[.]com→cypd.linestw[.]com　の紐づくIP。2019.7	24	7	2	US	どこどこJP OS-Unknown VPS/Cloud (https://jp.godaddy.com/)(2)
10	52.25.92.0	yasonbin[.[info→dxc.yasonbin[.]info の2018年ごろの紐づくIP	62	13	2	US	どこどこJP OS-Unknown VPS/Cloud (https://aws.amazon.com/)(2)
11	54.208.77.124	publicな検体 9db1aae1529ba8fa372634943c928cbb43ebd0c1e8002f2e1a36c0790482e111から	18	36	2	US	どこどこJP OS-Unknown VPS/Cloud (https://aws.amazon.com/)(2)
12	79.124.78.101	publicな検体 4e6d5983775d52215ab6779a928796c60f57321b9c65f4b89135bc0c9b880103	9	7	1	BG	どこどこJP OS-Unknown VPS/Cloud (https://www.blueangelhost.com/)(1)
13	79.124.78.105	publicな検体 4e6d5983775d52215ab6779a928796c60f57321b9c65f4b89135bc0c9b880103	4	4	1	BG	どこどこJP OS-Unknown VPS/Cloud (https://www.blueangelhost.com/)(1)

■結果考察

- IP視点で攻撃インフラとして「VPS/Cloud」の利用を再認識した。
- 他組織が持つデータにヒットするとその理由に興味が湧き、探究心が再熱する。
- 運営立場として検索時のレスポンスタイムを再確認
- 分析用プログラム開発側の観点でも改善課題が浮き彫りになった。(必要最低限のデータをある程度のルールを設けて、それにあったデータ登録してもらうこと)

04

最後に

最後に

■私たちは仲間を求めています！

一緒に脅威連携カタチ、作りませんか？

アライアンスにご参加ください！

今後の展望について

最後に

■詳細とアライアンス参加の申込について

- 「CYBER GRID JOURNAL VOL.12」
https://www.lac.co.jp/lacwatch/report/20211004_002720.html

- **参加申込について**
参加受付は**12月中旬**を予定。
※株式会社ラックのプレスリリースをお待ちください。