NWセキュリティを加速する
A10 Secure Gatewayパートナーの活動について

2022年 2月

SCSK株式会社　ネットワーク部　営業第三課

SCSK
夢ある未来を、共に創る。

アジェンダ

- 会社紹介
- OPSWAT製品紹介
- 性能試験の結果報告とサイジングヒント
- 弊社検討サービスについてのご案内

会社紹介

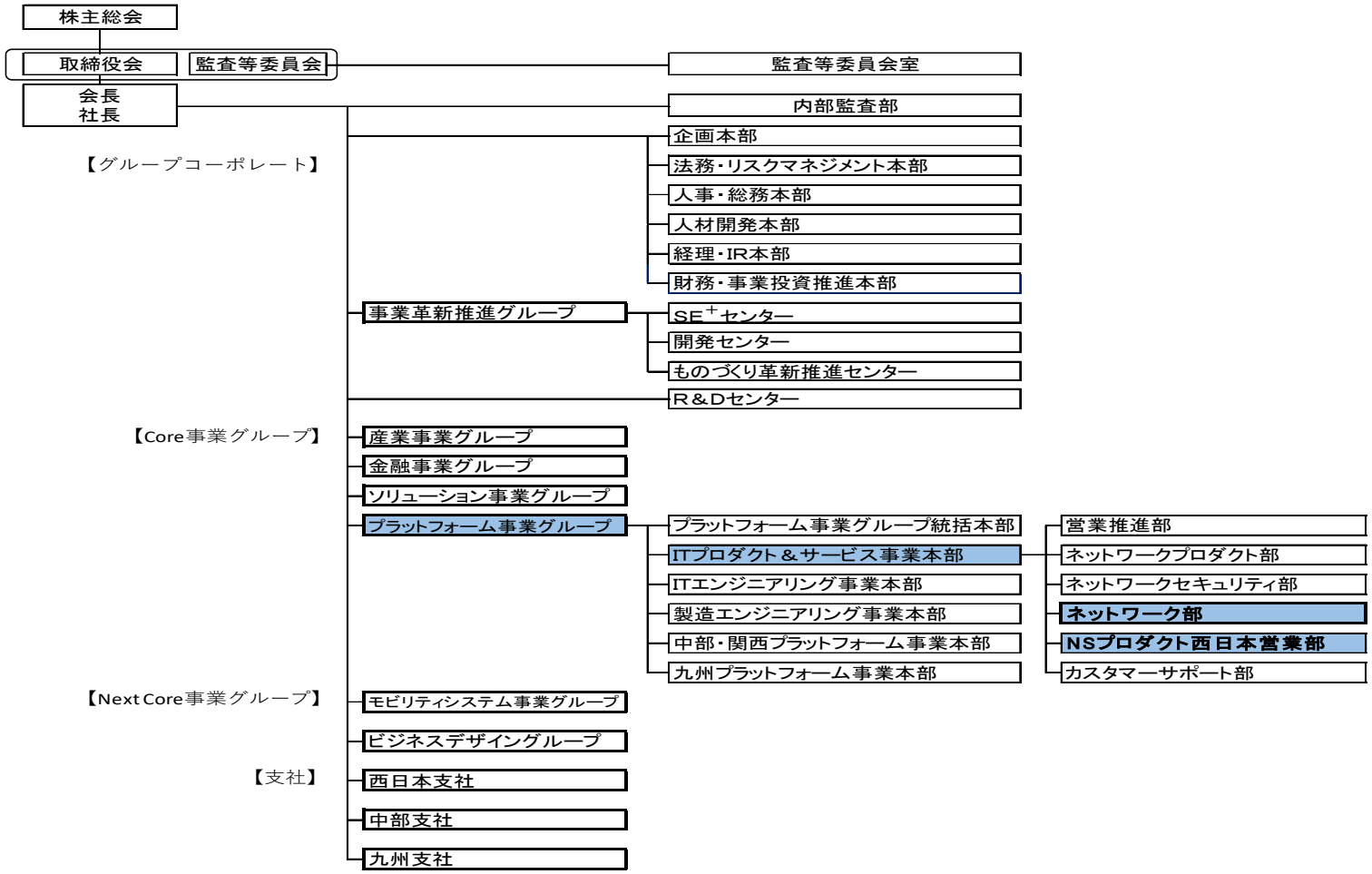
会社紹介

【会社概要】
ＳＣＳＫ株式会社（ＳＣＳＫ　Ｃｏｒｐｏｒａｔｉｏｎ）
本社所在地　〒135-8110 東京都江東区豊洲３丁目２番２０号 豊洲フロント
会社設立　1969年（昭和44年）10月25日
従業員数　14,550名 (連結)　8,357名（単体）　（2021年3月31日現在)
売 上 高　396,853百万円（2021年3月期 連結）
資 本 金　21,152百万円

【事業内容】
コンサルティング、システム開発、検証サービス、ITインフラ構築、ITマネジメント、ITハード・ソフト販売、BPO（Business Process Outsourcing）まで、ビジネスに必要なすべてのITサービスを、フルラインアップでご提供します

【事業拠点】
豊洲本社　晴海オフィス　お台場オフィス　北浜オフィス　千里オフィス　堺筋本町オフィス
中部オフィス　広島オフィス　九州オフィス　多摩センターオフィス

会社紹介



会社紹介

プラチナ・インダイレクト・ディストリビューターは、プラチナ・パートナーの中で間接販売に特化したパートナーであり、システム・インテグレータ様向に特化した販売・保守体制と支援プログラムを有します。

セキュアゲートウェイソリューションは、セキュリティ製品に負荷をかけずにSSLに隠れた脅威を可視化する「SSLインサイト」をはじめとしたゲートウェイでのセキュリティを実現するソリューションです。

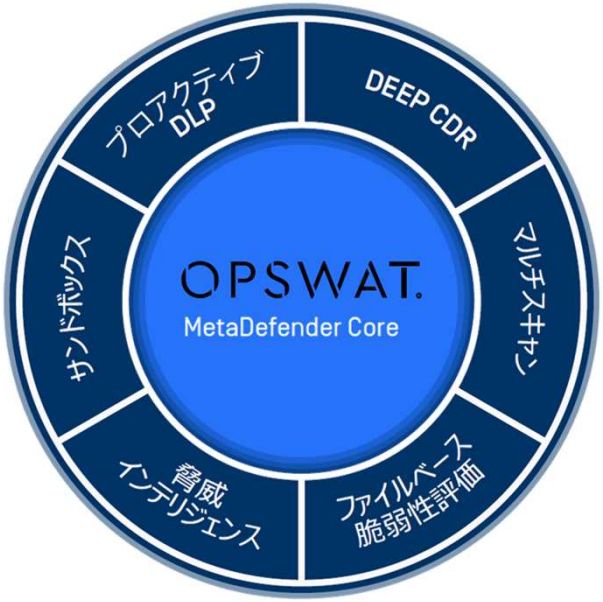
セキュアゲートウェイソリューションパートナーは、セキュリティおよびネットワーク双方に関する専門的な知見を有しており、お客様に専門的なサービス提供を行うことができるA10の認定パートナーです。

OPSWAT製品紹介

OPSWAT 製品ポートフォリオ

MetaDefender Core：複数の防御機能を搭載

- **ファイル無害化 (Deep CDR)** ―110種類*1のファイル形式に対応し、ユーザビリティを維持したまま安全なコンテンツを再構築
- **マルチスキャン** ―30種類を超える実績あるアンチマルウェアエンジンのシグネチャ、ヒューリスティック、機械学習により、マルウェア脅威の99%*2以上をプロアクティブに検知
- **プロアクティブ DLP** ―40種類以上のファイルタイプで個人を特定できる情報（PII）を検査し、機密データのリダクション、ウォーターマークを組み込み
- **ファイルベース脆弱性評価** ―バイナリとインストーラーを実行する前に検査分析し、既知のアプリケーション脆弱性を検出
- **脅威インテリジェンス** ―新しい脅威の調査とレピュテーション判定
- **サンドボックス** ―マルウェアの動作を分析

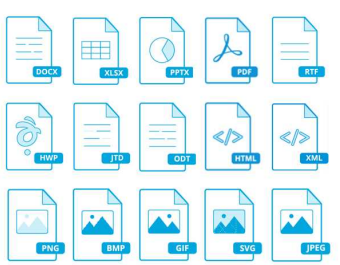


※1 2020年10月現在 110のファイルタイプに対応（ベータ版含む）
※2 当社テスト結果の数値です。
※3 2020年8月現在サンドボックスは MetaDefender Cloud でリリース

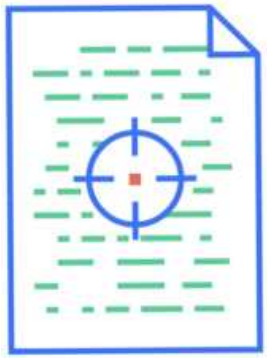
ファイル無害化

Deep CDR (Content Disarm and Reconstruction)

OPSWAT のファイル無害化（Deep CDR）とは?



115種類以上の
ファイル
形式をサポート



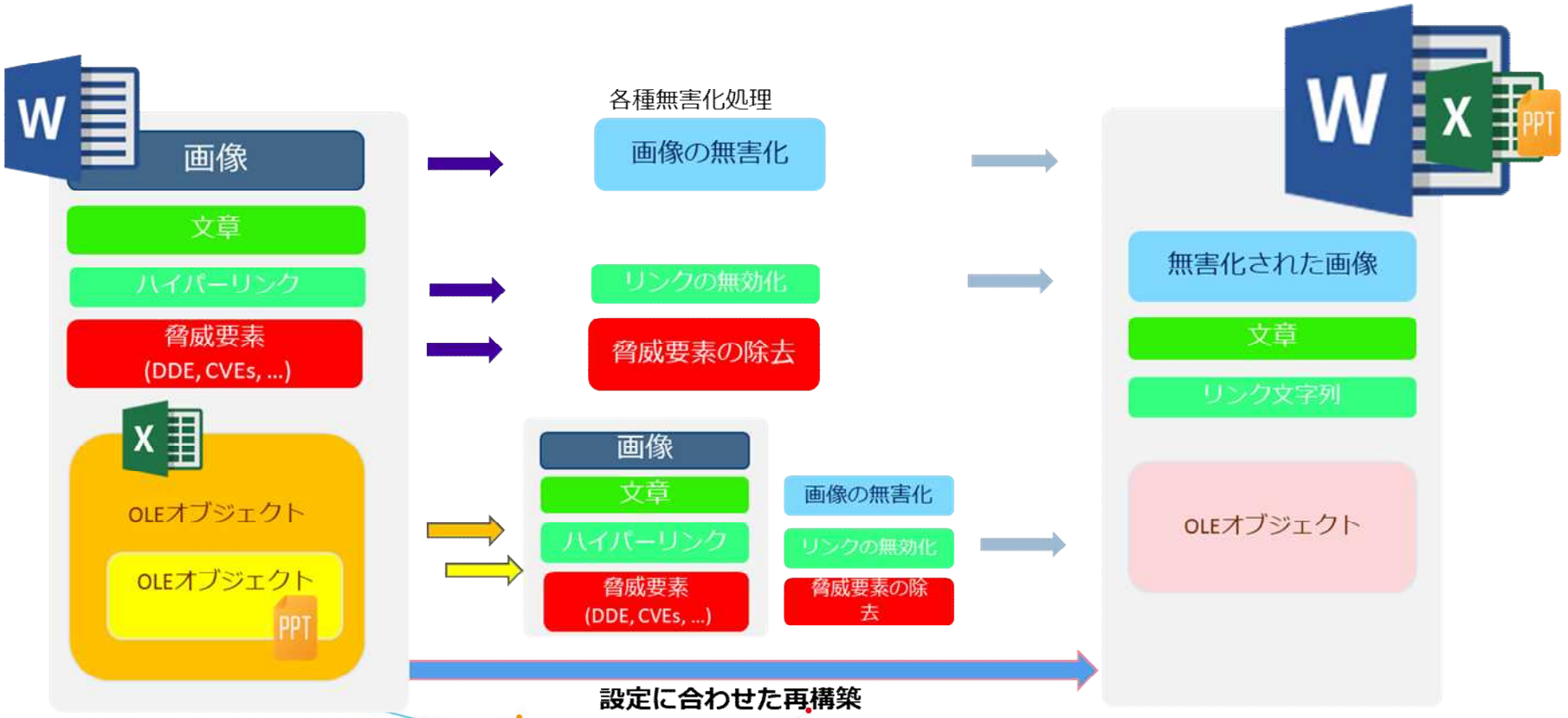
潜在的に悪意のあ
るコンテンツを削
除

ユーザビリティを維持したまま
ファイルを再構築

※出力ファイル形式はオプションで
選択することも可能

Deep CDR無害化の工程

- ファイルを展開、それぞれの要素に分解し、脅威が潜む可能性のある箇所を削除/無効化し、再構築
- OLEオブジェクトも対象
  - ネストした（OLE in OLE）にも対応可能（例：Word /Excel//PPT）



マルチスキャン（複数のマルチスキャンエンジンによる高度な脅威防止）

- MetaDefender Core の１つのコンポーネント
- シグネチャとヒューリスティックスキャンにより、既知・未知の脅威に対応
- 柔軟なパッケージオプションから選択可能
- Deep CDR + マルチスキャン = セキュリティをさらに強化

世界で実績のある

30以上のアンチマルウェアエンジンを利用可能

マルチスキャンで利用できるAVエンジンの特性

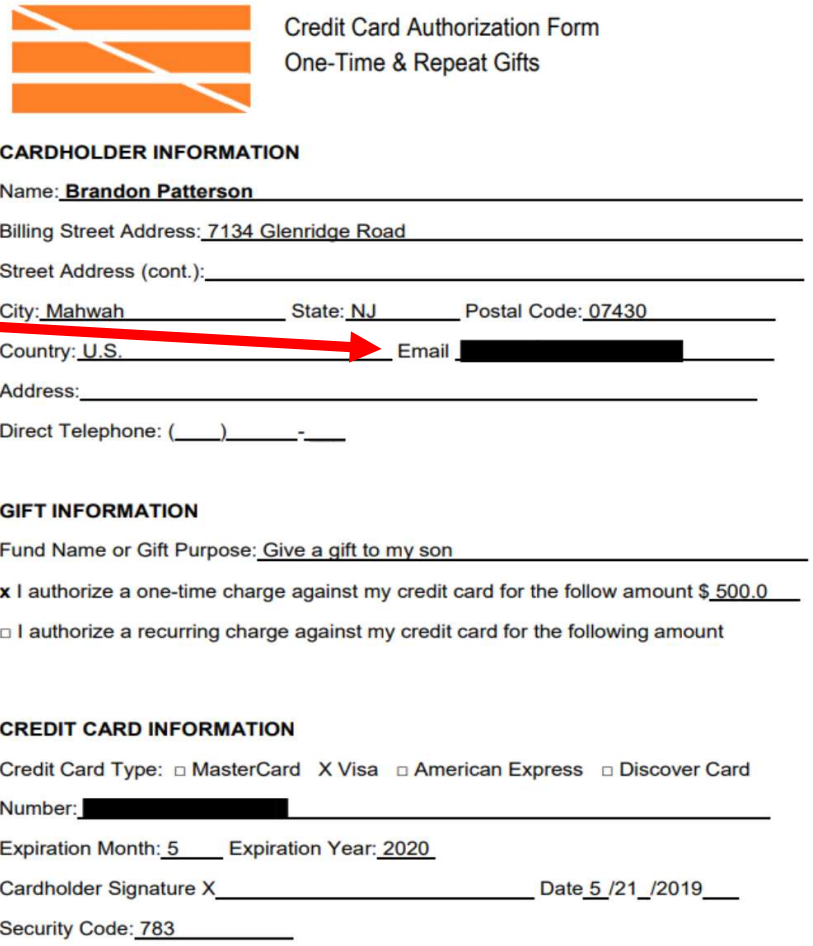
- それぞれのエンジンが異なる検出ロジックでマルウェアを検知
  - Signature
  - Heuristic
  - Potentially Unwanted Application / Program (PUA / PUP)
  - Cloud
  - Artificial Intelligence / Machine Learning (AI / ML)

- エンジンのアップデートは各エンジンベンダーのアップデートタイミングと同時
  - 定義ファイルはOPSWATから提供
  - オフライン更新も可能

	Engine Name	Vendor Name	Headquarters	Detection				
				Signature	Heuristic	PUA/PUP	Cloud	AI / ML
1	Aegis Lab	Lionic Corp	Taiwan	■			□	
2	AhnLab	AhnLab	South Korea	■		□	□	
3	Antiy	Harbin Antiy Technology	China	■	□			
4	Avira	Avira	Germany	■	■	■		□
5	Bitdefender	BitDefender	Romania	■	■			
6	ByteHero	Epoolsoft	China		■			
7	ClamAV	ClamAV	USA	■	■	□		
8	Comodo	Comodo	USA	■				
9	CrowdStrike	CrowdStrike	USA					■
10	Cyren	Cyren	Israel	■		□		
11	Emsisoft	Emsisoft	New Zealand	■	□			
12	Eset	ESET	Slovakia	■	■	■		
13	Filseclab	Filseclab Corporation	India	■				
14	Huorong	Beijing Huorong Network Technology	China	■				
15	Ikarus	IKARUS Security Software	Austria	■				
16	K7	K7 Computing Private	India	■	□			
17	Kaspersky	Kaspersky Lab	Russia	■	■			■
18	Kicom AV	Nurilab	South Korea					
19	Lavasoft	Adaware	Canada	■	■			
20	McAfee	McAfee	USA	■	■	□		
21	Microsoft Security Essentials	Microsoft	USA	■				
22	Windows Defender	Microsoft	USA	■	■		■	■
23	NANO	Nano Security	Russia	■	■			
24	Netgate		USA	■				
25	Tachyon	INCA Internet	South Korea	■	■			
26	Quick Heal	QUICK HEAL TECHNOLOGIES	India	■	□	□		
27	RocketCyber	RocketCyber	USA					■
28	Sophos	Sophos	UK	■	□	□		
29	SparkCognition	Spark Cognition	USA					■
30	Symantec	Symantec	USA	■	■	□		
31	Systweak	Systweak	India	■				
32	Trend Micro	Trend Micro Incorporate	Japan	■				
33	Trend Micro HouseCall	Trend Micro Incorporate	Japan	■				
34	VirIT	TG Soft	Italy	■		■		
35	VirIT ML	TG Soft	Italy					■
36	Virus Blokada	VirusBlokAda	Belarus	■				
37	Webroot SMD	Webroot	United States					■
38	Xvirus	XVirus	Portugal	■				
39	Zillya	Brandon Universal	Ukraine	■	□			
	Legend	■ Enabled by default	□ Available, disabled by default					

Proactive DLP

- 40種以上のファイルタイプに対応
- クレジットカード番号などの
  センシティブな情報を検出
  - ファイルをブロック
  - 該当部分をマスキング
  - 透かしを入れるなど
- メタデータ内部の
  センシティブデータを除去
  - 例：Exif内部のデータ（GPS、Author、Title/dateなど）
- センシティブデータとしてユーザ独自の
  正規表現を定義可能
- OCRを使用可能：画像化された文字列も
  OCRにより文字認識



Credit Card Authorization Form
One-Time & Repeat Gifts

CARDHOLDER INFORMATION

Name: Brandon Patterson

Billing Street Address: 7134 Glenridge Road

Street Address (cont.):

City: Mahwah State: NJ Postal Code: 07430

Country: U.S. Email [redacted]

Address:

Direct Telephone: (____)_____-____

GIFT INFORMATION

Fund Name or Gift Purpose: Give a gift to my son

x I authorize a one-time charge against my credit card for the follow amount $ 500.0

□ I authorize a recurring charge against my credit card for the following amount

CREDIT CARD INFORMATION

Credit Card Type: □ MasterCard X Visa □ American Express □ Discover Card

Number: [redacted]

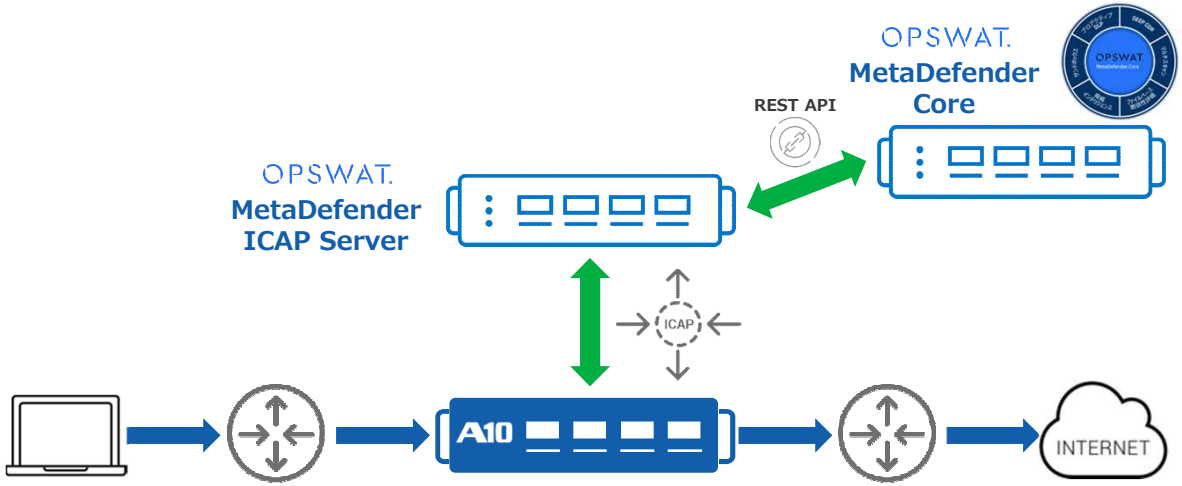
Expiration Month: 5 Expiration Year: 2020

Cardholder Signature X_____ Date 5 /21 /2019

Security Code: 783

A10 × OPSWAT

- ICAPでOPSWAT社のMetaDefenderに接続する構成
- 不可能であったSSL/TLS通信に対するウィルススキャン、無害化、データ損失防止を実現



暗号化トラフィック
平文トラフィック

OPSWAT MetaDefenderが
平文化したトラフィックに以下を適用
- ウィルススキャン（マルチスキャン）
- コンテンツ無害化（CDR）
- データ損失防止（DLP）

https://www.a10networks.co.jp/download/files/A10-SB-19199-JA-01_NOV_2019.pdf

https://www.opswat.com/partners/a10-networks

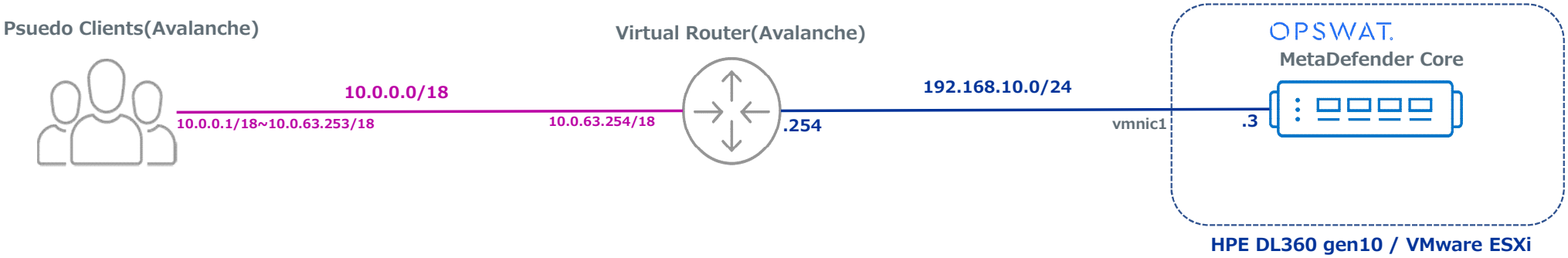
性能試験の結果報告と
サイジングヒント

性能検証前提

★検証環境サンプルおよび試験方法

疑似クライアント(Avalanche)から、 MDcoreに対してAPI(POST /file)経由で直接オブジェクトをアップロード

※MDcoreに割り当てるHWリソース(cpu, memory, disk)をESXi上で調整
※MDcoreに割り当てるライセンスは、8,12,16,20 AV-engines 各パターンで計測
※一般的なインターネット利用を想定した疑似HTTPトラフィックを作成（コンテンツサイズは、1オブジェクトあたり約30Kbyteと仮定）
https://httparchive.org/reports/page-weight?start=latest&view=list



【参考/Tips】MetaDefender Core：Process API

★Process API実行サンプル(python3.7.6, 一部抜粋)

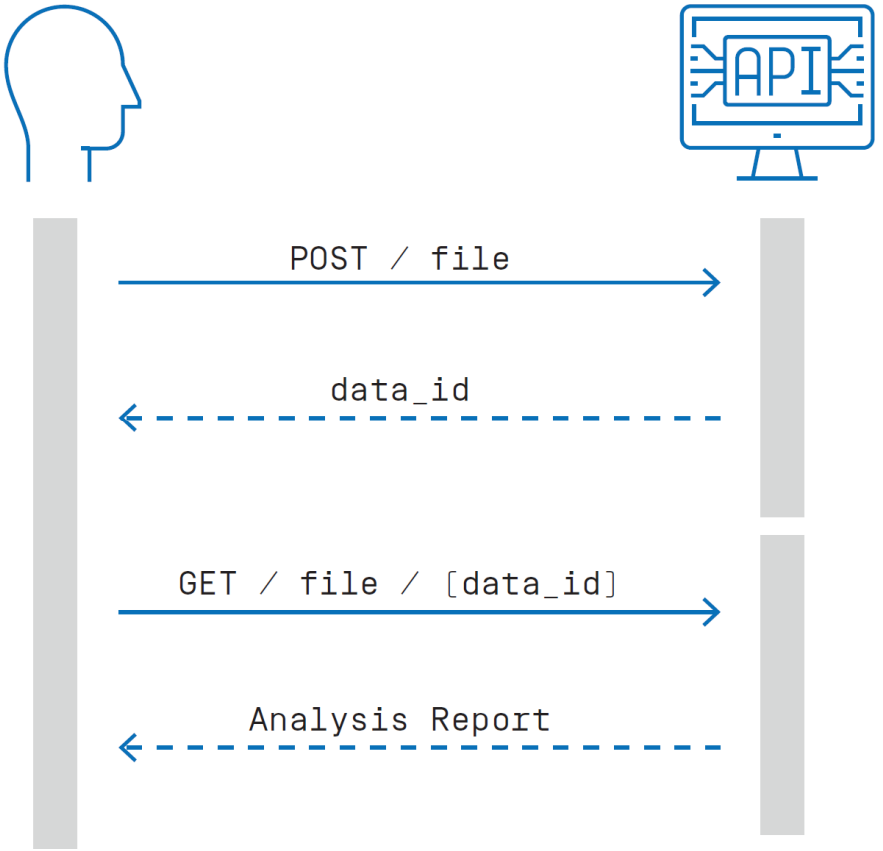
```python
def proc_files():
    url = 'http://{}/file'.format(MDCORE_HOST)
    binary = open(FILE, 'rb').read()
    payload = {'uploadfile': (FILENAME, binary)}
    headers = {
        'filename': FILENAME
    }
    r = requests.post(url, headers=headers, files=payload)
    r_payload = json.loads(r.text)
    if r.status_code == 200:
      print('file successfully accepted!!')
      return r_payload['data_id']
    else:
      print('HTTP status code: {0}, message: {1}'.format(r.status_code, r_payload))

# >>>>>>>> return: {'data_id': 'aa43c1bd016847c49b0bf6c53583fb25'}

def get_proc_results(data_id):
    url = 'http://{0}/file/{1}'.format(MDCORE_HOST, data_id)
    r = requests.get(url)
    r_payload = json.loads(r.text)
    if r.status_code == 200:
      print('scan result is: {}'.format(r_payload['scan_results']['scan_all_result_a']))
    else:
      print('HTTP status code: {0}, message: {1}'.format(r.status_code, r_payload))

# >>>>>>>> stdout: scan result is: No Threat Detected

if __name__ == '__main__':
  data_id = proc_files()
  time.sleep(5)
  get_proc_results(data_id)
```

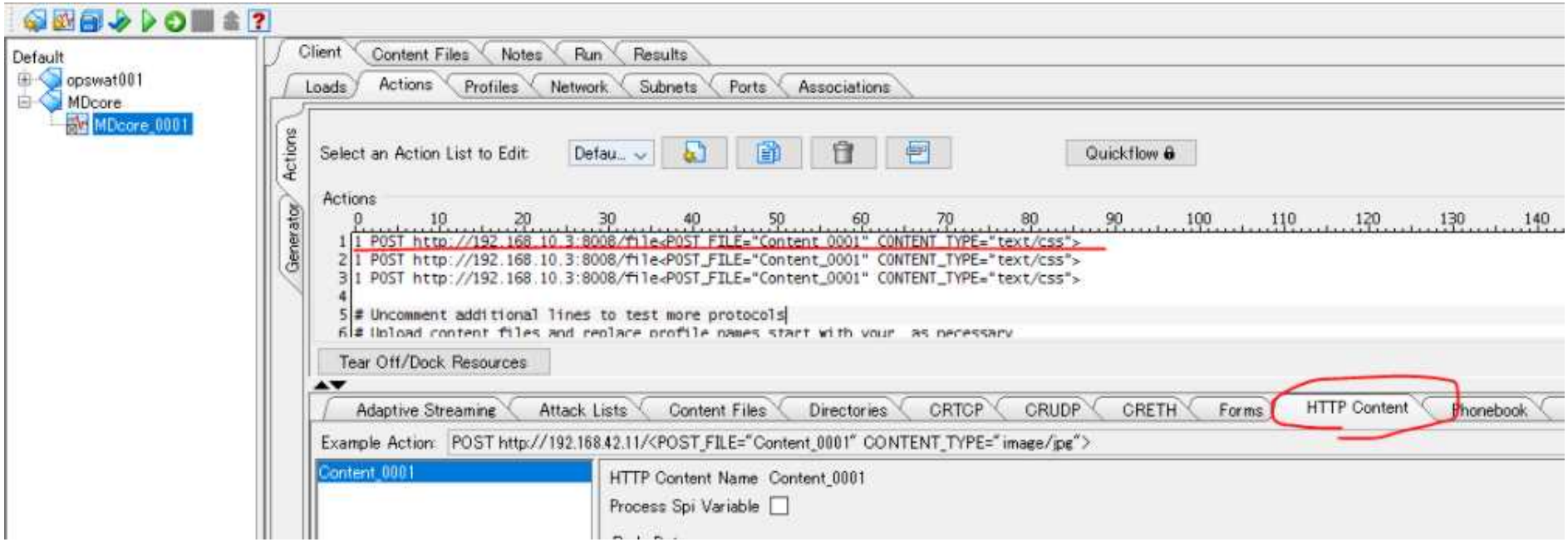


【参考/Tips】Avalanche CommanderでMDcoreのProcess APIを叩く方法

★Avalanche設定サンプル

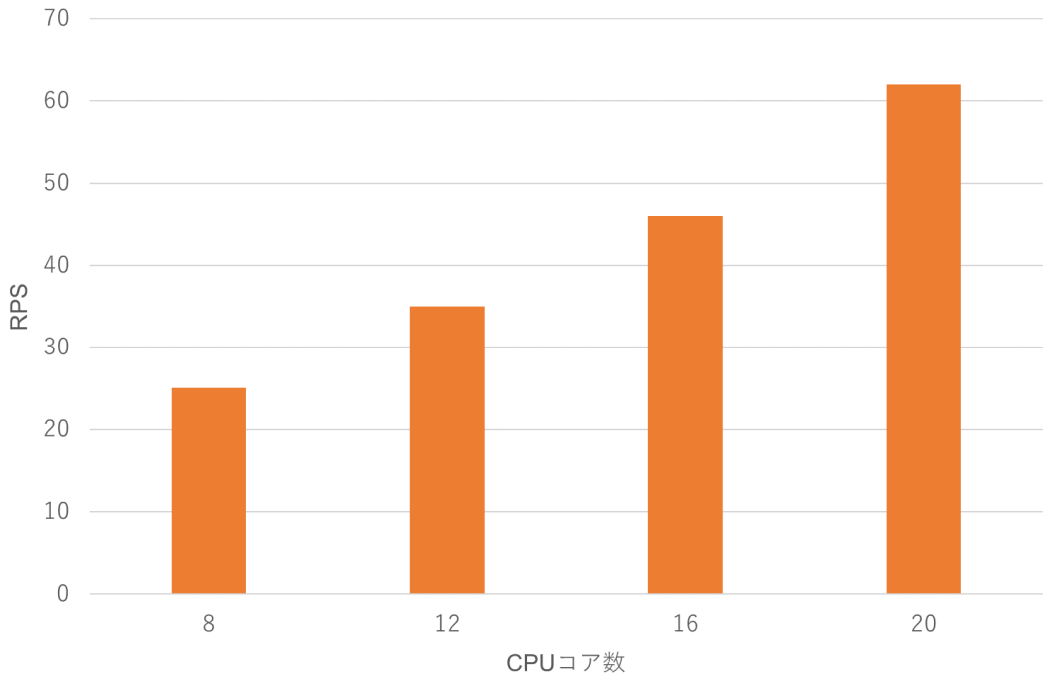
・[Client]-[Actions]
1 POST http://<MDcore IP:port>/file<POST_FILE="xxx" CONTENT_TYPE="xxx/xxx">

・[HTTP Content]に上記POST_FILEで指定するFileをupload



性能検証結果（一部抜粋）

マルチスキャン(8 AV-engines)＋Deep CDR＋Proactive DLPの性能検証結果



・MetaDefender CoreはCPUコア数に応じて性能が向上（※NUMAを超えないことが前提）
・16コアで約50RPS(HTTP Requests /sec)処理可能

結果の数値をどう見るか

Thunderはデフォルトでは全てのHTTPリクエスト/レスポンスをICAPで投げる
（.html, .js, .jpg, .png, .css, .json, .xml, .txt, .woff2　などなど・・・）

⇒全てのwebトラフィックを処理してしまうとMetaDefenderの処理可能性能とマッチせず、
大量のサーバーが必要になってしまう

・そもそもHTTPでやりとりされる全オブジェクトをスキャン/無害化する必要はない

・通常、プロキシ製品などではICAPで連携する通信を制限できる

・従来のネットワークセキュリティ機器等でもアンチマルウェアの処理対象は
ファイルの種別等で選択するのが一般的

ICAP処理対象トラフィックの制御

SCSK
夢ある未来を、共に創る。

A10 ThunderからMetaDefenderに投げるICAPリクエストを制限することで、処理対象を減らす
★ファイルコンテンツを含むHTTPリクエスト/レスポンスのみをICAPで渡し、スキャン/無害化する

＜aFlexによる制御例＞
・POSTメソッドを用いた通信のみをICAP処理する
＃HTTPリクエストで実コンテンツを含むのは基本的にPOSTメソッドであるという考え方

・ Content-Lengthが存在しない、あるいはContent-Length: 0のHTTPリクエスト/レスポンスはICAP処理しない
＃コンテンツがないものは予め排除する。MDicapで「No Content to Scan」となるのは無駄な処理
＃Content-Lengthが存在しないチャンク転送（Transfer-Encoding: chunked）は例外的にICAP処理させる

・Content-Typeが存在し、かつ当該ヘッダに特定のMIMEタイプを含むHTTPリクエスト/レスポンスのみを処理する
＃OPSWATで検査させたいファイルタイプを洗い出し、class-listに対応するMIMEタイプをstringとして定義する

＜その他方法による制御＞
セキュリティ担保が可能なクラウドサービス向けの通信（MS365, G-suite etc..）はSSL可視化をbypass

ICAP処理対象トラフィックの制御

SCSK
夢ある未来を、共に創る。

★aFlex + class-list サンプル

```
# Filter for ICAP REQMOD
when HTTP_REQUEST {
    set req_method [HTTP::method]

    if { not ($req_method == "POST") } {
        ICAP::disable
    }
    if { not ([HTTP::header exists "Content-Length"]) } {
        if { not ([HTTP::header exists "Transfer-Encoding"]) } {
            ICAP::disable
        } else {
            if { not ([HTTP::header "Transfer-Encoding"] equals "chunked") } {
                ICAP::disable
            }
        }
    } else {
        set con_len [HTTP::header "Content-Length"]
        if { $con_len == 0} {
            ICAP::disable
        }
    }
    if { not ([HTTP::header exists "Content-Type"]) } {
        ICAP::disable
    } else {
        set con_type [HTTP::header "Content-Type"]
        if { not ([CLASS::match $con_type contains inspect_mime]) } {
            ICAP::disable
        }
    }
}
```

```
# Filter for  ICAP RESPMOD
when HTTP_RESPONSE {
    if { not ([HTTP::header exists "Content-Length"]) } {
        if { not ([HTTP::header exists "Transfer-Encoding"]) } {
            ICAP::disable
        } else {
            if { not ([HTTP::header "Transfer-Encoding"] equals "chunked") } {
                ICAP::disable
            }
        }
    } else {
        set con_len [HTTP::header "Content-Length"]
        if { $con_len == 0} {
            ICAP::disable
        }
    }
    if { not ([HTTP::header exists "Content-Type"]) } {
        ICAP::disable
    } else {
        set con_type [HTTP::header "Content-Type"]
        if { not ([CLASS::match $con_type contains inspect_mime]) } {
            ICAP::disable
        }
    }
}
```

```
!
class-list inspect_mime string
  str application/vnd.openxmlformats-officedocument.wordprocessingml.document
  str application/vnd.openxmlformats-officedocument.presentationml.presentation
  str application/vnd.openxmlformats-officedocument.spreadsheetml.sheet
  str multipart/form-data
  str application/pdf
!
```

Webで扱われる一般的なファイルタイプとMIMEタイプ

SCSK
夢ある未来を、共に創る。

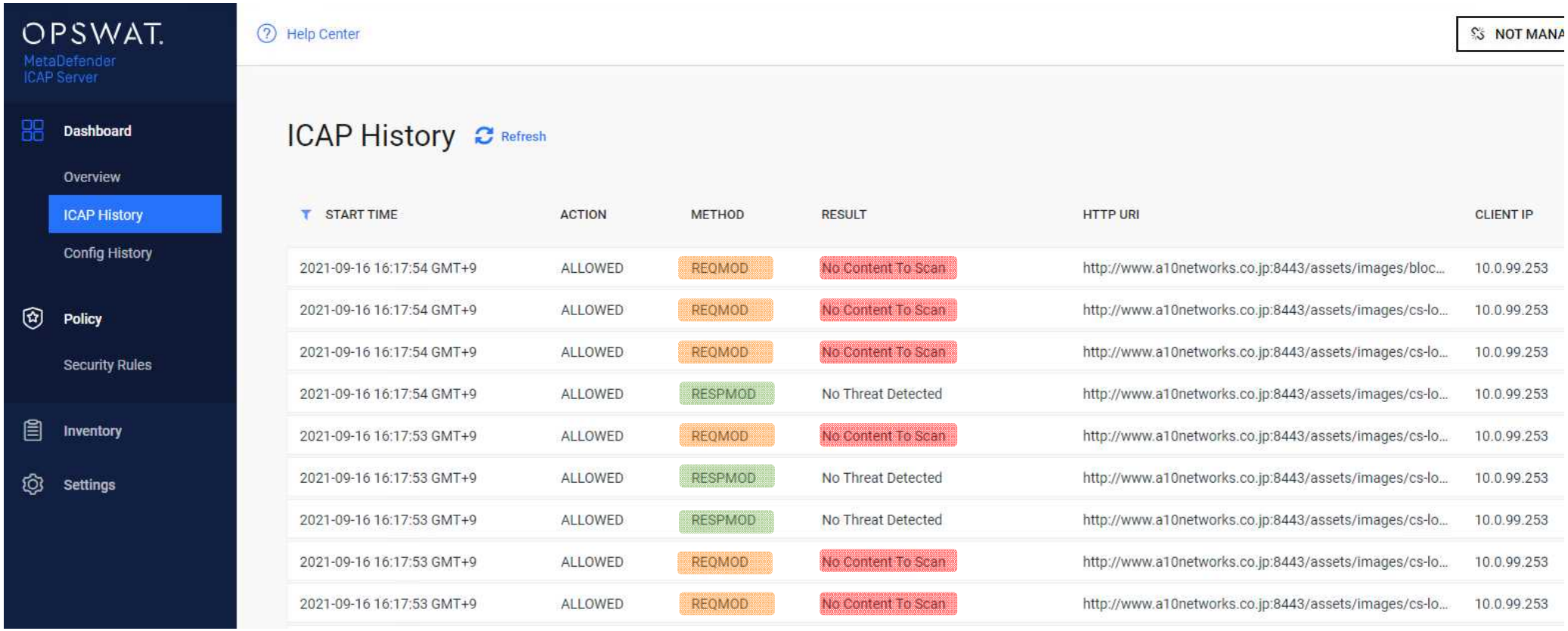
ごく一般的なドキュメントファイルや画像ファイル（以下例）に対して悪意のあるスクリプトやマクロが埋め込まれる

拡張子	種類	MIMEタイプ
.doc, .docx	Microsoft Word Doc	application/msword, application/vnd.openxmlformats-officedocument.wordprocessingml.document
.xls, .xlsx	Microsoft Excel	application/vnd.ms-excel, application/vnd.openxmlformats-officedocument.spreadsheetml.sheet
.ppt, .pptx	Microsoft PowerPoint	application/vnd.ms-powerpoint, application/vnd.openxmlformats-officedocument.presentationml.presentation
.pdf	Adobe Portable Document Format	application/pdf
.jpg, .png, .svg, .gif	Image	image/jpeg, image/png, image/svg+xml, image/gif
.vsd	Microsoft Visio	application/vnd.visio
.mp4	MPEG-4 Part 14	video/mp4
.zip, .7z	Archive	application/zip, application/x-7z-compressed
※ANY(POST)	※ANY(POST)	※multipart/form-data

ICAP処理対象トラフィックの制御

SCSK
夢ある未来を、共に創る。

【aFlexによる通信最適化 実施前】
大量のICAPリクエストが飛び、更に大半が No Content to Scan であり非常に非効率



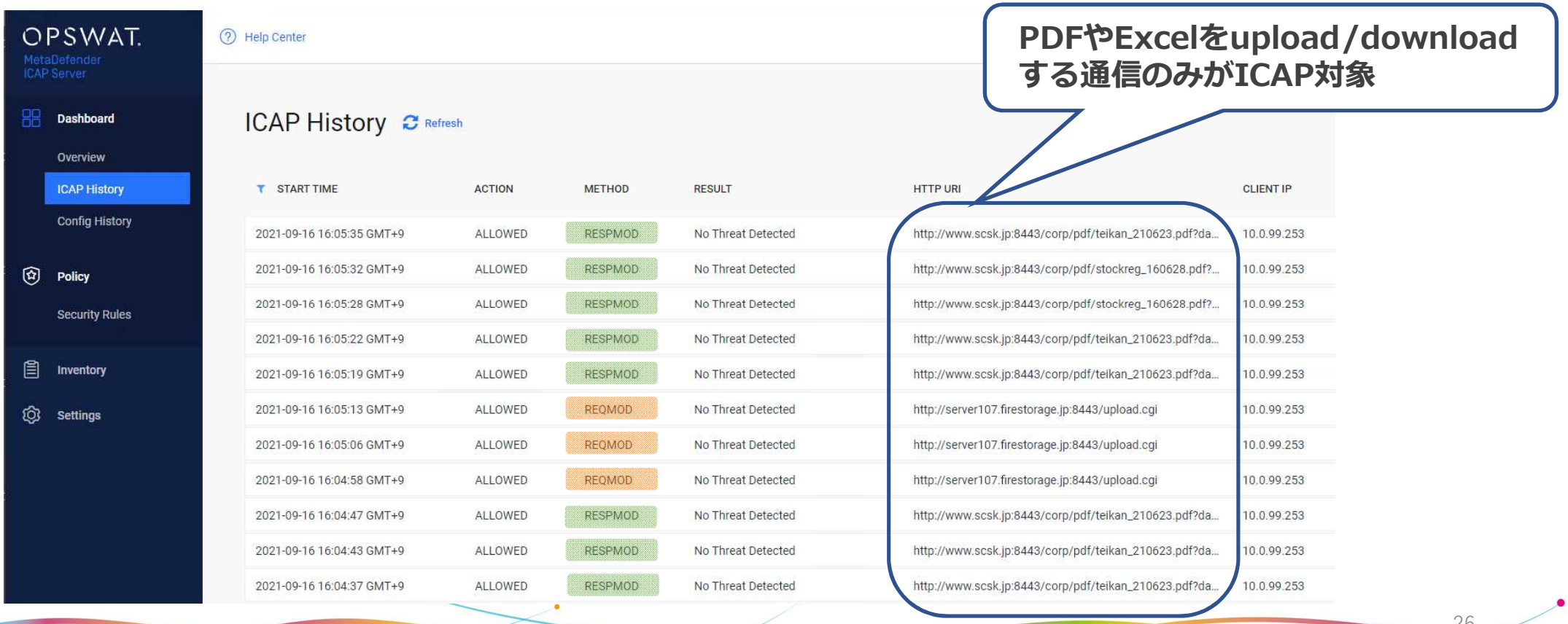
START TIME	ACTION	METHOD	RESULT	HTTP URI	CLIENT IP
2021-09-16 16:17:54 GMT+9	ALLOWED	REQMOD	No Content To Scan	http://www.a10networks.co.jp:8443/assets/images/bloc...	10.0.99.253
2021-09-16 16:17:54 GMT+9	ALLOWED	REQMOD	No Content To Scan	http://www.a10networks.co.jp:8443/assets/images/cs-lo...	10.0.99.253
2021-09-16 16:17:54 GMT+9	ALLOWED	REQMOD	No Content To Scan	http://www.a10networks.co.jp:8443/assets/images/cs-lo...	10.0.99.253
2021-09-16 16:17:54 GMT+9	ALLOWED	RESPMOD	No Threat Detected	http://www.a10networks.co.jp:8443/assets/images/cs-lo...	10.0.99.253
2021-09-16 16:17:53 GMT+9	ALLOWED	REQMOD	No Content To Scan	http://www.a10networks.co.jp:8443/assets/images/cs-lo...	10.0.99.253
2021-09-16 16:17:53 GMT+9	ALLOWED	RESPMOD	No Threat Detected	http://www.a10networks.co.jp:8443/assets/images/cs-lo...	10.0.99.253
2021-09-16 16:17:53 GMT+9	ALLOWED	RESPMOD	No Threat Detected	http://www.a10networks.co.jp:8443/assets/images/cs-lo...	10.0.99.253
2021-09-16 16:17:53 GMT+9	ALLOWED	REQMOD	No Content To Scan	http://www.a10networks.co.jp:8443/assets/images/cs-lo...	10.0.99.253
2021-09-16 16:17:53 GMT+9	ALLOWED	REQMOD	No Content To Scan	http://www.a10networks.co.jp:8443/assets/images/cs-lo...	10.0.99.253

ICAP処理対象トラフィックの制御

SCSK
夢ある未来を、共に創る。

【aFlexによる通信最適化 実施後】
★REQMODはPOST通信のみ、REQMOD RESPMODどちらも特定のMIMEタイプデータをupload/downloadする通信のみ

※「No Threat Detected」＝ 検査すべきコンテンツが存在



想定するサーバーと収容可能ユーザー数の目安

SCSK
夢ある未来を、共に創る。

▽Server
HP ProLiant DL360 Gen10 Plus
1P16コア Xeon 6208U 2.9GHz CPU、32GBメモリ、960GB SSD （RAID1）
Windows Server OS
想定価格：250万円/台（5年保守費込）

▽ユーザー数目安
1日8時間で処理可能なリクエスト数と収容可能ユーザー数の想定

50（RPS）× 3,600（秒）×8（時間）＝1,440,000（リクエスト）

平均して1ユーザーあたり、1日に約1,000回特定のドキュメントファイル（+画像ファイル）をupload/downloadする想定と仮定すると、

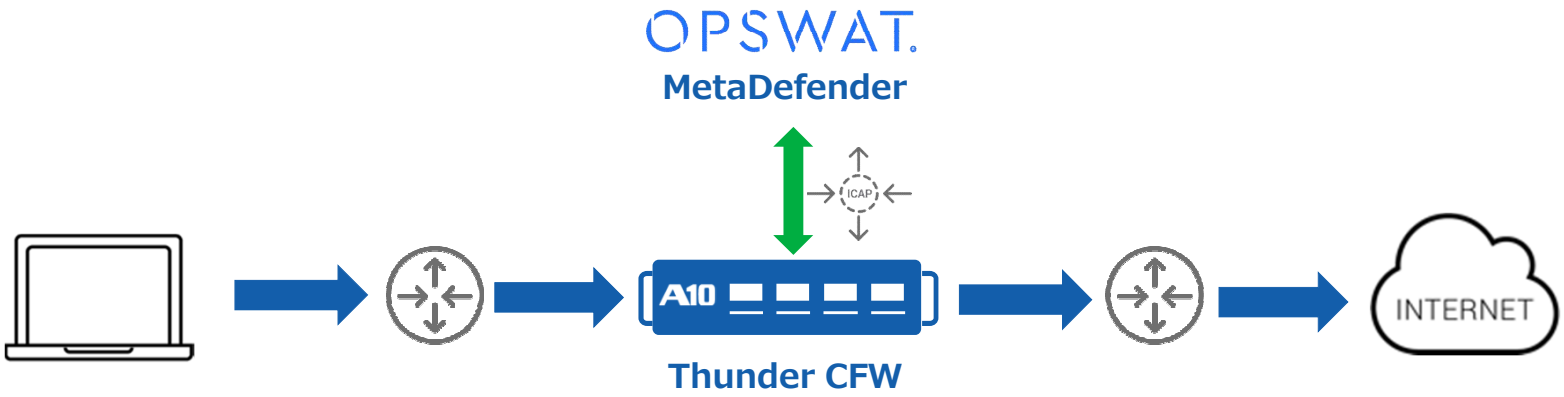
上記の1サーバーあたり1,440ユーザーまで収容可能
（※冗長構成（Active×Active）で2,880ユーザー程度）

弊社サービスについてのご案内

OSWAT検証サービスについてのご案内

「SCSK OPSWAT 検証サービス」

A10 Secure Gateway with OPSWAT検討のお客様向けにPOC支援
最適な導入を図る



Engineer as a Service

初期導入支援サービス（ADC、クラウドアクセスプロキシ、SSLi）
詳細設計や構築時のA10に関するご質問に、A10専門エンジニアがお答えしながら、
コンフィグ作成から設置当日のリモート立会いまでご支援いたします。

① 設計支援打合せ
② QA対応
③ パラメータシート作成
④ コンフィグファイル作成
⑤ リモート設置立会い

<納品物>
＊ QA表
＊ パラメータシート
＊ 単体試験表
（コンフィグ動作確認[MS365振り分け確認など]）
＊ コンフィグファイル

<ご提供条件>
＊ 想定用途：ADC、クラウドアクセスプロキシ、SSLi
＊ QA工数：3人日程度（オプション除く）
＊ サービス提供期間は、設置翌営業日までとなります。
＊ サービス対象は、原則SCSKよりご購入いただくA10機器に限ります。
＊ コンフィグファイル作成においては、必要な情報を事前にご提供頂きます。
＊ コンフィグファイルのお客様のご都合による修正は、1回まで。（実環境チューニング時含む）
＊ ご質問件数及び内容により想定が大幅に超える場合には、事前にご相談の上、
以降の作業工数の削減または追加御見積等の調整をさせて頂きます。

SCSK株式会社
ITプロダクト&サービス事業本部
ネットワーク部　営業第三課
03-5859-3034
A10-info@ml.scsk.jp
www.scsk.jp