金融系マルウェア脅威情報配信の実証と考察

高田 一樹[1,2,a)]　邦本 理夫[1]　山下 知起[4]　寺田 真敏[4,5]　吉岡 克成[2,3]

概要：インターネットバンキングの不正送金やクレジットカード情報の盗取を目的とした金融系マルウェアを用いた攻撃は，2015 年に不正送金被害が過去最高を示した以降も継続している．中でも MITB 攻撃と呼ばれる手法による被害が社会問題となっている．著者らは，金融系マルウェアによる MITB 攻撃対策を目的として，C&C サーバ，マニピュレーションサーバなどの攻撃サーバ情報，および，攻撃対象となる企業サイトの情報を収集する長期観測を実施している．これら金融系マルウェアに関する脅威情報を，関連する組織ならびに組織間での対策に活用していくため，「サイバー攻撃の防御に向けた情報活用基盤」を用いた機械処理可能な形式での情報配信を検討している．本稿では，情報活用基盤で金融系マルウェア脅威情報を配信するための記述仕様および 2017 年 2 月〜2021 年 5 月に配信した脅威情報の概要について述べ，活動の中で明らかとなった課題およびその解決方法の検討結果を示す．

キーワード：STIX/TAXII，脅威情報，金融系マルウェア，MITB 攻撃

Concept and consideration of financial malware threat information sharing

Kazuki Takada[1,2,a)]　Michio Kunimoto[1]　Tomoki Yamashita[4]　Masato Terada[4,5]
Katsunari Yoshioka[2,3]

Abstract: Cyberattacks using financial malware aimed at fraudulent financial transfers and stolen credit card information have continued even after the damage caused by fraudulent financial transfers reached a record high in 2015. In particular, the damage caused by the MITB attack is a social problem. The authors are conducting long-term observations of financial malware to collect information on attack servers such as C&C servers and manipulation servers, as well as information on corporate sites targeted by attacks, for the purpose of countermeasures against MITB attacks. In order to utilize this threat information as a countermeasure among related organizations, we demonstrated that threat information is delivered on the Information-utilization Platform to Defend against Cyberattacks. The description specifications of threat information and the summary of delivered information from 2017 to 2021 are described. The authors also examined the issues and solutions of information delivery about financial malware threat information.

Keywords: STIX/TAXII, Threat information, Financial malware, MITB attack

1. はじめに

インターネットバンキングの不正送金やクレジットカード情報の盗取を目的とした金融系マルウェアを用いた攻撃は，2015 年に不正送金被害が過去最高を示した以降も継続している．中でも，金融系マルウェアによる MITB(Man

1 株式会社セキュアブレイン
SecureBrain Corporation.
2 横浜国立大学先端科学高等研究院
Yokohama National University Institute of Advanced Sciences
3 横浜国立大学大学院環境情報研究院
Yokohama National University Graduate School of Environment and Information Sciences
4 株式会社日立製作所
Hitachi, Ltd.
5 東京電機大学
Tokyo Denki University
a) takada-kazuki-hw@ynu.ac.jp

In The Browser) 攻撃と呼ばれる攻撃手法による被害が社会問題となっている．MITB 攻撃とは，マルウェアが感染した PC 上の Web ブラウザにインジェクションし，通信内容を盗聴・改ざんする攻撃手法で，インターネットバンキングなどの Web サービス利用時の通信内容が盗聴・改ざんされ，不正送金や情報盗取の被害につながっている．MITB 攻撃は，Web サービス利用者の PC 上で通信内容が盗聴・改ざんされるため金融機関などの Web サービス提供者側での対策が困難であり，インターネットバンキングなどの正規サイトへのアクセス時に攻撃活動が発動するため利用者が攻撃に気づき難いなどの理由で対策が進まない状況にある．

このような金融系マルウェアによる MITB 攻撃の被害を低減するためには，アンチウィルスソフトなどによる利用者 PC の感染防止対策だけでなく，一般のマルウェア対策と同様のマルウェアの通信先となる C&C サーバなどの攻撃者サーバの情報に加えて，どの組織のどのサービスが攻撃対象となっているのかといった情報を活用することで多様な対策の検討・適用の推進が必要であると考えている．

我々は，金融系マルウェアによる MITB 攻撃対策を目的として，金融系マルウェアを長期観測しており [1]，この長期観測によって，金融系マルウェアの通信先である C&C サーバなどの攻撃サーバ，攻撃対象および攻撃手法を継続的に把握することが可能である．これら金融系マルウェア脅威情報を，多様な対策の検討・適用に活用していくためのアプローチのひとつとして，異なる組織間でサイバー対策に関する情報を活用するための情報活用基盤を利用した情報配信の実証を行った．

本稿では，金融系マルウェア脅威情報を配信するために策定した記述仕様について示した後，策定した記述仕様を用いて 2017 年 2 月〜2021 年 5 月に情報活用基盤を利用して配信した脅威情報の概要を述べる．また，情報配信の実証を通して明らかとなった課題とその解決方法について検討した結果を述べる．

2. 関連研究

サイバーセキュリティにおける様々な脅威情報共有の取り組みにあたっては，情報共有を機械処理するためのデータ形式などの標準化が行われている．

STIX(Structured Threat Information eXpression) は, 脅威情報を記述するための技術仕様である．STIX を用いることで，サイバー攻撃によって観測された事象に加えて，サイバー攻撃活動を鳥瞰するために必要となる様々な脅威情報の記述が可能となる．TAXII(Trusted Automated eXchange of Indicator Information) は，脅威情報を交換するための手順を定めた技術仕様である．TAXII を用いることで STIX で記述した脅威情報の交換を機械処理することが可能となる．STIX/TAXII は，v1.x[2][3] が MITRE[4] を中心に策定され，v2.x[5] は OASIS CTI[6] が中心となって策定している．

脅威情報を共有するためのシステムや枠組みの動向について述べる．

脅威情報を共有するための情報共有基盤を構築するオープンソースとして MISP(Malware Information Sharing Platform)[7] がある．MISP は，標的型攻撃の IoC(Indicator of Compromise)，金融詐欺，脆弱性，テロ対策情報などの情報を共有・蓄積し，情報の相関を取ることを可能とする．様々な形式でのデータのインポート/エクスポートが可能で情報利用の自動化や外部連携が効率化できる．同様の情報共有基盤を構築するオープンソースとして OpenCTI[8] がある．

米国国土安全保障省 (DHS) では，米国連邦政府と米国内外の企業，団体などの組織間で脅威情報を共有するためのシステムとして AIS(Automated Indicator Sharing)[9] を運用している．

CTA(Cyber Threat Alliance)[10] は，脅威情報を共有するためのコミュニティであり，主にサイバーセキュリティプロバイダーが参加する非営利組織として運用されている．会員は財政的支援に加えて共有可能な脅威情報を保有していることなどの条件を満たす必要がある．脅威情報を共有することで脅威に迅速に対処することを目的としているが脅威情報の共有は，会員組織および条件を満たしたパートナーのみで行われる点が他の取り組みとは大きく異なる点である．

AIS や CTA では，STIX を用いた脅威情報共有を行っており，人手を介さないことによる迅速な情報展開や情報の関連付けなどの点から，サイバー攻撃の対策において脅威情報共有の機械処理の重要性は，非常に高いと考えている．本研究では，社会問題となっている金融系マルウェアに関する脅威情報を多様な対策の検討・適用に活用していくため，機械処理可能な形式で配信するための記述方法の策定と共に，情報活用基盤を利用した情報配信を検証した．

3. 情報活用基盤の概要と本研究の目的

金融系マルウェア脅威情報を共有するにあたっては，前述の情報共有基盤を構築するオープンソースや脅威情報を共有するためのコミュニティが有する情報共有基盤を利用する必要がある．本研究では，情報共有基盤として，総務省と一般社団法人 ICT-ISAC が連携してサイバー攻撃の防御に向けた情報共有基盤に関する実証事業 [11][12] で運用している情報共有基盤（以降，情報活用基盤）を使用した．情報活用基盤の概要を**図 1** に示す．この情報活用基盤は，複数の組織間でサイバー攻撃に関連する情報を速やかに配信することで，迅速に対策の検討・適用に活用することを目的としている．金融系マルウェア脅威情報も，情報活用基盤に投稿することで，情報利用者へと配信できる．

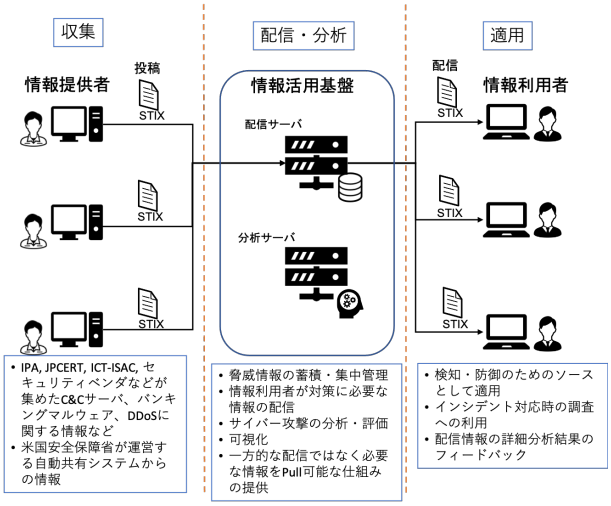


図 1: 情報活用基盤の概要

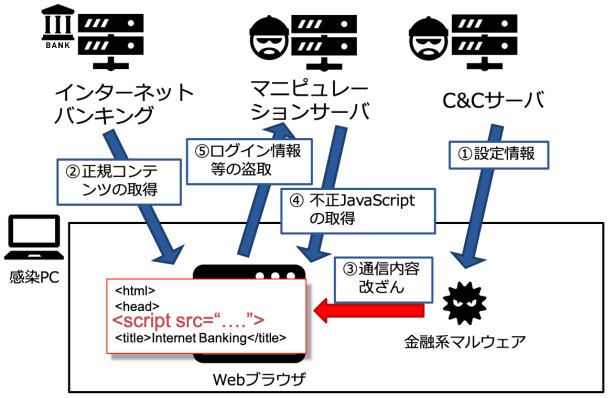


図 2: MITB 攻撃のイメージ

情報活用基盤では，STIX/TAXII 形式での情報配信を採用しており，脅威情報を機械的に処理することが可能となる．これによって，情報の提供者，利用者が共に手間を掛けずにサイバー攻撃対策に必要な情報の配信や利活用ができる．

情報活用基盤は，図 1 に示すように情報を「配信」するための機能と情報の有効性などを「分析」するための機能の 2 つの機能を提供する基盤として構成されている．情報の配信機能では，多くの情報を迅速に配信することに重点を置き，情報の正確性や有効性を分析機能で判断することで情報を活用するための基盤である．

本研究では，情報活用基盤の配信機能を用いて金融系マルウェア脅威情報を配信することを目的とする．そのために，金融系マルウェアの長期観測環境で収集した情報を迅速に情報活用基盤で配信するための記述仕様を策定した．その際，配信された情報を分析・活用するためには，人間による概要の把握が必要と考える．そのため，記述仕様は，機械処理と人間による一定の理解が可能という 2 点を考慮したものとしている．

4. 金融系マルウェア脅威情報

配信対象とする金融系マルウェア脅威情報について述べる．

4.1 金融系マルウェアによる MITB 攻撃および脅威情報の概要

金融系マルウェアによる MITB 攻撃の概要について述べる．MITB 攻撃は，C&C サーバが配信する攻撃設定情報に従って制御されている．攻撃設定情報は，マルウェアのファミリによってデータの形式が異なるが，攻撃対象サイトの URL と攻撃手法が格納されている．下記，①〜⑤に，代表的な MITB 攻撃の流れを示す（**図 2**）．

① 攻撃設定情報の取得
金融系マルウェアが C&C サーバと通信をして，MITB 攻撃の攻撃設定情報を取得する．

② Web ブラウザ通信の監視
金融系マルウェアは，Web ブラウザの通信を常時監視し，攻撃対象のインターネットバンキングなどの Web サービスへの接続を待つ．

③ 通信内容の改ざん
①の攻撃設定情報に従って，通信内容を改ざんする．主に，不正な JavaScript を取得するためのコード片を挿入する．

④ 不正 JavaScript の取得・実行
マニピュレーションサーバ（以降，M サーバ）と呼ばれる悪性サーバから不正 JavaScript を取得した後，実行する．

⑤ ログイン情報の盗取や不正な送金
不正 JavaScript によって，入力した認証情報の盗取や利用者 PC 上で意図しない不正送金など MITB 攻撃による攻撃活動の目的を達成する．

この MITB 攻撃において，C&C サーバや M サーバなどの攻撃者サーバ，攻撃設定情報や不正 JavaScript は，絶えず変更されていることが分かっており，金融系マルウェア長期観測システムを用いて金融系マルウェアに関する脅威情報を継続的に収集している．本研究では，情報活用基盤を多様な対策の検討・適用に活用していくために，収集した金融系マルウェア脅威情報の STIX 形式変換機能，および，TAXII での投稿機能を長期観測システムに追加することで，情報活用基盤へ情報を配信する．長期観測システムからの情報投稿の概要を**図 3** に示す．

4.2 金融系マルウェア脅威情報の概要および STIX/TAXII 仕様

金融系マルウェアの長期観測で取得する主な脅威情報は，次のとおりである．

- 金融系マルウェアのファイル Hash 値
- C&C サーバ情報

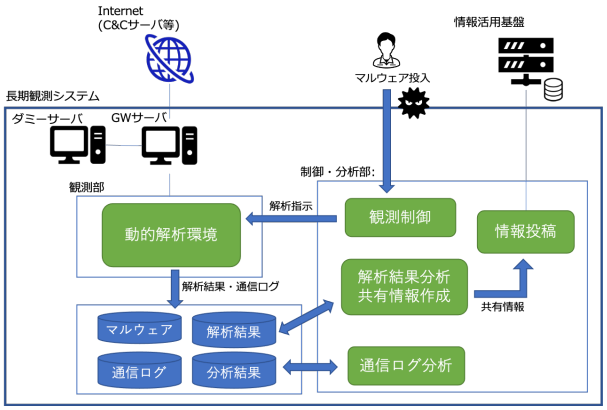


図 3: 長期観測システムからの情報投稿の概要

- M サーバ情報
- 攻撃対象 URL 情報
- 不正 JavaScript

これらの脅威情報の内，不正 JavaScript は容量が大きいことや難読化などの要因で共有が困難であることから配信対象とはしていない．金融系マルウェアに関する脅威情報は，C&C サーバ，M サーバ，攻撃対象 URL の 3 種類に分けて配信する．3 種類の脅威情報の概要と共有目的を下記（1）～（3）に示す．

（1）C&C サーバ情報

金融系マルウェアの動的解析中に発生した通信から，抽出した C&C サーバと思われるドメイン・IP アドレス情報である．動的解析中に，発生した通信から抽出して投稿するため，悪性の通信が発生しない場合は投稿されない．ICT-ISAC や通信事業者で，通信先のブロックなどの対策に活用することを想定している．

（2）M サーバ情報

C&C サーバから取得した攻撃設定情報に含まれる不正 JavaScript の配信や盗取した認証情報などのアップロード先となる M サーバの URL・IP アドレス情報である．ICT-ISAC や通信事業者で，通信先のブロックなどの対策に活用することを想定している．

（3）攻撃対象 URL 情報

C&C サーバから取得した攻撃設定情報に含まれる攻撃対象サイトの URL 情報と，攻撃対象 URL に対応する（2）M サーバ情報である．金融 ISAC や金融機関で，注意喚起などの対策に活用することを想定している．

（1）～（3）それぞれの情報に，情報の収集源である金融系マルウェアのファイル Hash 値 (SHA-1) を付与して脅威情報とする．

情報活用基盤への金融系マルウェアに関する脅威情報の投稿は，STIX/TAXII v1 形式を用いている．脅威情報の STIX/TAXII 仕様について述べる．

金融系マルウェアの脅威情報の配信にあたっては STXI/TAXII 共通のプレフィックスとして

表 1: 脅威情報の Collection 名

区分	Collection 名
C&C サーバ情報	BKMW_CONF
M サーバ情報	BKMW_MANU
攻撃対象 URL	BKMW_ATTK

(a) C&C サーバ情報

(b) M サーバ情報

(c) 攻撃対象 URL 情報

図 4: 各脅威情報の Indicator Title

“BKMW”(**B**an**k**ing **M**al**w**are) を付与する．TAXII では，共有する情報を Collection という単位で管理する．情報提供者は，自分の情報が何の脅威情報であるか Collection 名を指定して投稿し，情報利用者は，必要な Collection 名を指定して取得する．それぞれの Collection 名を**表 1** に示す．

情報活用基盤では，脅威情報を機械処理することに加え，人手による分析などを可能とするために人間がどのような脅威情報であるかを識別可能とする必要がある．そのため，STIX における各脅威情報のタイトル (Indicator Title) は，Collection 名と同様のプレフィックスと IoC 情報を組み合わせたものを記載する．**図 4** に 3 種類の脅威情報の Indicator Title を，**図 5** に，C&C サーバ情報の主要な脅威情報の STIX 記述例 (抜粋) を示す．加えて，通信先の AS 情報，国情報やマルウェアの VirusTotal 登録情報などの詳細情報を JSON 形式で付与することで分析に必要な情報収集を代行している．

4.3 投稿した脅威情報

金融系マルウェアの脅威情報については，4.2 節の記述仕様を用いて 2017 年 2 月から投稿を開始した．2017 年 2 月から 2021 年 5 月までに投稿した脅威情報の統計を**表 2** に示す．表 2 に示すように計 43 検体（C&C サーバ情報 4,763 ドメイン，M サーバ情報 37,526URL，攻撃対象 URL 情報 489URL）の情報を 4 年以上に渡って投稿しており，この活動は 2021 年 8 月時点も継続している．ここでは，2021 年に投稿した 3 検体の中から Zloader 1 検体，Ursnif 1 検体の脅威情報の概要を**表 3** に示し，投稿した Ursnif の C&C サーバ情報の STIX データを**図 6** に，M サーバ情報の STIX データを**図 7** に示す．

```
<indicator>
    <indicator:Title>__BKMW_CONF__ sample.cnc.com</indicator:Title>
    <DomainNameObj:Value>sample.cnc.com</DomainNameObj:Value>
    <AddressObj:Address_Value>1.0.0.2</AddressObj:Address_Value>
    <cyboxCommon:Simple_Hash_Value>c589f ··· </cyboxCommon:Simple_Hash_Value>
</indicator>
```

図 5: C&C サーバ情報の STIX 記述例 (抜粋)

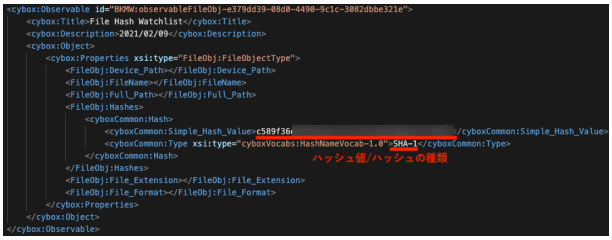
表 2: 投稿した全脅威情報のユニーク情報数

配信年	検体数	C&C サーバ情報	M サーバ情報	攻撃対象 URL 情報
2017	19 検体	1625 ドメイン	6971 URL	120 URL
2018	6 検体	45 ドメイン	11857 URL	44 URL
2019	14 検体	480 ドメイン	14787 URL	116 URL
2020	1 検体	165 ドメイン	3901 URL	3 URL
2021	3 検体	2448 ドメイン	10 URL	206 URL
合計	43 検体	4763 ドメイン	37526 URL	489 URL

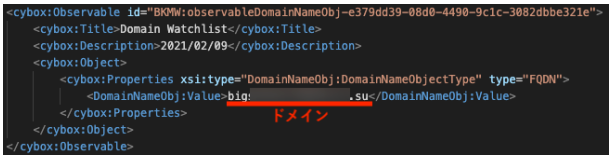
※複数年に渡って観測した検体や通信先は，初年のみでカウント

表 3: 2021 年中に投稿した脅威情報（各 1 検体毎のユニーク情報数）

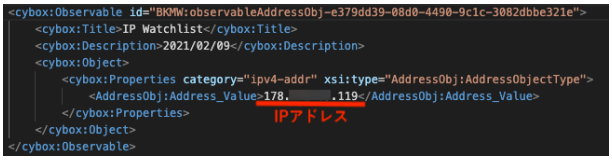
マルウェア名	C&C サーバ	M サーバ	攻撃対象 URL	期間
Zloader	2462 ドメイン	2 URL	200 URL	2021.01.13 - 2021.05.31
Ursnif	70 ドメイン	9 URL	120 URL	2021.02.09 - 2021.05.31



(a) マルウェアのハッシュ値

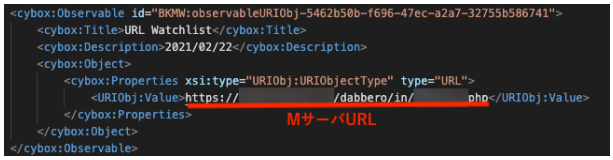


(b) C&C サーバのドメイン

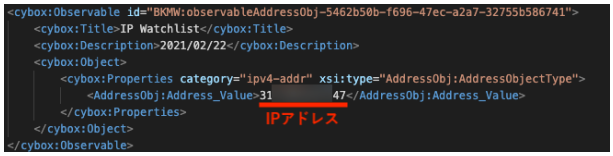


(c) C&C サーバの IP アドレス

図 6: Ursnif の C&C サーバの STIX データ



(a) M サーバの URL



(b) M サーバの IP アドレス

図 7: Ursnif の M サーバの STIX データ

5. 考察

金融系マルウェアに関する脅威情報配信の課題と解決方法について考察する．

(1) 攻撃をされている側（被害者側）の情報を配信するための記述仕様が用意されていない

本研究の配信で取り上げている攻撃対象 URL のような攻撃をされている側（被害者側）の情報を記述する仕様が用意されていないことに帰着する課題である．なお，MITB 攻撃の場合，攻撃をされている側（被害者側）には，改ざん対象のサイトの運用者（企業）と金融系マルウェアに感染する PC の一般利用者の 2 種類がある．情報活用基盤では，前者との連携を想定している．

本研究では，金融系マルウェア脅威情報として，C&C サーバ情報，M サーバ情報，攻撃対象 URL 情報の 3 種類を STIX 形式で配信することで，情報活用基盤を介した機械処理可能な環境整備を先導した．3 種類の金融系マルウェア脅威情報は，攻撃活動に帰する情報であることから，いずれも STIX 形式の Indicator タグを利用したが，本来 Indicator タグは，検知に有効なサイバー攻撃を特徴付け

る指標，すなわち攻撃をしている側（攻撃者側）の活動検知するための情報を記述することを意図している．この場合，C&C サーバ情報，M サーバ情報は攻撃をしている側の情報，攻撃対象 URL 情報は攻撃をされている側の情報で違いがあるにも関わらず，既存の STIX 解釈では，3 種類の金融系マルウェア脅威情報を同等に取り扱ってしまう可能性がある．

今後，配信した金融系マルウェア脅威情報を適切に処理するためには，攻撃対象 URL 情報のような攻撃をされている側（被害者側）の情報を記述するための仕様が必要である．この課題に対しては，ICT-ISAC の情報活用基盤の実証で試行中の STIX 2.1 の ICT-ISAC 拡張エリアを用いて攻撃対象 URL 情報を記述することで解決することが可能と考える．**図 8** に STIX 2.1 の ICT-ISAC 拡張エリアを用いた攻撃対象 URL の記述仕様案を示す．金融系マルウェア脅威情報のうち C&C サーバ情報，M サーバ情報については，STIX2.1 の IoC 記述仕様を用いて表現し，攻撃対象 URL 情報については，図 8 を用いて表現することで脅威情報の攻撃者側と被害者側の違いを踏まえた情報活用基盤ならびに機械処理の普及が可能となる．

（2）分析のための配信情報を拡充していく必要がある

金融系マルウェア脅威情報を処理する上で重要なこととして，配信された情報を分析するための様々な情報を収集することが挙げられる．本研究においては，金融系マルウェアの長期観測から得られた C&C サーバ情報，M サーバ情報，攻撃対象 URL 情報を配信している．これらの情報を投稿する際に，通信先の AS 情報，国情報やマルウェアの VirusTotal 登録情報など分析に必要と思われる情報の収集を代行しているが，この情報のみで十分とは言えない．例えば，C&C サーバなどの攻撃者サーバで他にどのようなサービスが稼働しているかといった情報は，攻撃者サーバに対してポートスキャンによる調査をする必要がある．また，長期観測システムで観測中の金融系マルウェアの通信先が変化した場合に，変化前の攻撃者サーバに関しては，稼働し続けているのか停止しているのかなど死活に関する時間的な追跡も必要となる．このように脅威情報の分析に必要と思われる情報は，多岐に渡り，継続して収集する必要があるが，単独組織で運用することは，情報収集の効率性と信頼性の点から難しいと考えている．

配信情報の拡充には，情報活用基盤を利用する組織による相互協力が有効と考える．ここでは，相互協力を実現する方法として検討した，利用組織の役割分担による配信情報の拡充モデルの概要を**図 9** に示す．図 9 に示すとおり，利用組織は，情報の投稿者，更新者，利用者のいずれかの役割を持つ．例えば，金融系マルウェアを観測する組織は，投稿者として金融系マルウェア脅威情報を投稿する．悪性サーバを観測する組織は，更新者として C&C サーバの死活情報などを付与・更新する．利用者は，配信情報を自組織ネットワークの通信先遮断リストに追加することを通して，C&C サーバなどへの接続発生状況をフィードバックする．このように，利用組織が相互協力することで，配信情報の拡充が可能になり，情報活用基盤の維持可能性の向上にもつながると考える．今後，利用組織の役割分担による配信情報の拡充の実現方法について継続して検討する．

（3）脅威情報の可読識別子が必要である

2 章に示した情報共有の取り組みをはじめとする多くの情報共有では，脅威情報の識別子に UUID のような機械的に判別可能な識別子を用いることが一般的である．これは，情報を機械処理することを前提に仕様策定されているためと考えられる．共有された脅威情報に対して，どのように対策すべきかが決定している場合，すなわち，脅威情報の機械処理だけを前提としている場合には問題ない．しかし，情報活用基盤のように，脅威情報の機械処理だけではなく，配信された脅威情報を人手で分析することを想定している場合には，人間による判別や検索ができる可読識別子の付与が必要と考える．また，可読識別子は課題（2）で提示した役割分担による配信情報の拡充を実現する上でも必要である．

本研究では，金融系マルウェア脅威情報を配信する際に “BKMW-<CONF|MANU|ATTK>” のプレフィックスを付与することで，可読識別子の課題解決を図っている．今後も課題（1）（2）の解決と合わせて脅威情報の可読識別子の仕様について検討し，利用者が脅威情報をより簡便に共通に取り扱うことを可能とする必要がある．

6. まとめと今後の課題

本研究では, 総務省と一般社団法人 ICT-ISAC が連携してサイバー攻撃の防御に向けた情報共有基盤に関する実証事業で運用している情報共有基盤を使用し金融系マルウェア脅威情報を投稿・配信する実証を行った．この実証を通して，金融系マルウェア脅威情報を配信するための STIX 記述仕様を提案し，情報活用基盤を介して配信した．2017 年 2 月～2021 年 5 月に投稿した脅威情報の配信数は，計 43 検体（C&C サーバ情報 4,763 ドメイン，M サーバ情報 37,526URL，攻撃対象 URL 情報 489URL）であり，情報活用基盤を介した金融系マルウェア脅威情報の配信が可能であった．今後，配信された脅威情報が意図したとおりに処理される仕様となっているかに着目して実証を行う必要がある．

金融系マルウェア脅威情報の配信に関する課題については，攻撃をされている側（被害者側）の情報を配信するための記述仕様，分析のための配信情報の拡充，脅威情報の可読識別子の 3 つの視点から検討した．その結果，攻撃をされている側（被害者側）の情報を配信するための記述仕様については，攻撃対象 URL 情報を取り扱うための記述仕様を提案した．分析のための配信情報の拡充については，

```
{
    “type”:“observed_data”,
    “spec_version”:“2.1”,
                ⋮
    “name”:“BKMW_ATTK_<攻撃対象 URL>”,
    “number_observed”:“2”,
    “objects”:{
        “0”:{
            “type”:“url”,
            “value”:“<攻撃対象 URL>”,
            “extensions”:{
                “x-ict-isac.jp”:{
                    “attack_target”:{
                        “url”:“<攻撃対象 URL>”,
                        “files”:[ {“SHA-1”:“<マルウェアファイル SHA-1 値>”,} ]
        }}}},
        ‘1”:{
            “type”:“file”,
            “hashes”:{
                “MD5”:<マルウェアファイル MD5 値>”,
                “SHA-1”:<マルウェアファイル SHA-1 値>”,
                “SHA-256”:<マルウェアファイル SHA-256 値>”,
}}}}
```

図 8: STIX 2.1 ICT-ISAC 拡張エリアを用いた攻撃対象 URL の記述仕様案

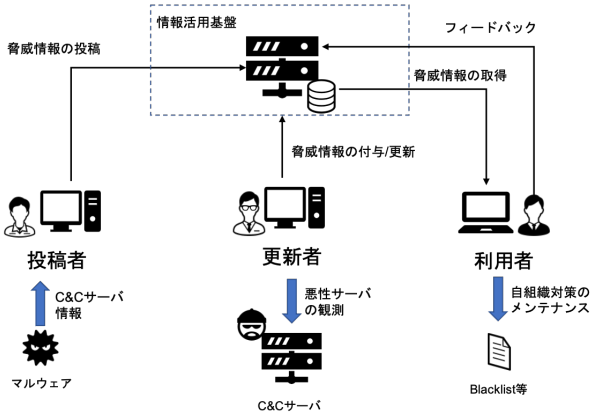


図 9: 役割分担による配信情報の拡充のモデル

利用組織の相互協力を実現する役割分担のモデルを提案すると共に，情報活用基盤で配信情報を分析・活用するためには，脅威情報の可読識別子が必要であることを明らかにした．今後，記述仕様の改善や配信情報の拡充と合わせて脅威情報の可読識別子について検討をすすめる．

本研究では，金融系マルウェアに関する脅威情報の配信に着目したが，配信した脅威情報の分析・活用についても検討する必要がある．

謝辞 本研究にあたって，有益な助言を頂いた総務省「ソフトウェア脆弱性を狙ったサイバー攻撃の防御に向けた情報共有基盤に関する実証実験」の関係者各位に深く感謝いたします．

参考文献

[1] 高田一樹，岩本一樹，遠藤　基，奥村吉生，岡田晃市郎，西田雅太，吉岡克成，松本　勉：静的解析と挙動観測を組み合わせた金融マルウェア長期観測手法の提案，情報処理学会論文誌，Vol. 59, No. 12 (2018).

[2] MITER: STIX 1.X, (online), available from ⟨https://stixproject.github.io/⟩ (accessed 2021-03-11).

[3] MITER: TAXII1.X, (online), available from ⟨https://taxiiproject.github.io/⟩ (accessed 2021-03-11).

[4] MITRE: The MITRE Corporation, (online), available from ⟨https://www.mitre.org/⟩ (accessed 2021-03-14).

[5] MITER: STIX2.x/TAXII2.X, (online), available from ⟨https://oasis-open.github.io/cti-documentation/⟩ (accessed 2021-03-11).

[6] OASIS: OASIS Cyber Threat Intelligence (CTI) TC, (online), available from ⟨https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti⟩ (accessed 2021-03-11).

[7] MISP Project: MISP Threat Sharing, (online), available from ⟨https://www.misp-project.org/index.html⟩ (accessed 2021-03-11).

[8] LUATIX: OpenCTI, (online), available from ⟨https://www.opencti.io/en/⟩ (accessed 2021-03-11).

[9] CISA: Automated Indicator Sharing, (online), available from ⟨httpshttps://www.cisa.gov/ais⟩ (accessed 2021-03-11).

[10] Cyber Threat Alliance: Cyber Threat Alliance Official, (online), available from ⟨https://www.cyberthreatalliance.org/⟩ (accessed 2021-03-11).

[11] 総務省：サイバー攻撃の防御に向けた情報共有基盤に関する実証事業の成果の公表，（オンライン），入手先 ⟨https://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000153.html⟩ （参照 2021-03-08）．

[12] 一般社団法人 ICT-ISAC：サイバー攻撃の防御に向けた情報共有基盤に関する実証事業について，（オンライン），入手先 ⟨https://www.ict-isac.jp/news/news20180629.html⟩（参照 2021-03-08）.