情報処理学会論文誌 Vol.59 No.9 1596–1609 (Sep. 2018)

CSIRTのためのWebブラックリストの分類の提案

羽田 大樹[1,2,a)] 後藤 厚宏[1]

受付日 2017年12月11日, 採録日 2018年6月8日

概要：組織における Web アクセスの利用には多くの脅威が存在するため，悪性 Web サイト情報のブラックリストが利用される．悪性 Web サイト情報には登録理由やレピュテーションなどが付与されることがあるが，CSIRT のインシデントレスポンスにおいて合理的な判断を行うために適した情報を提供しているとはいえない．本稿では，インシデントレスポンスの「トリアージ」「対応実施」業務において，既存のブラックリストを活用した業務における課題を示し，合理的な判断を可能とするための「所有者」「コンテンツ」「現在の状態」「最終確認」という 4 項目による悪性 Web サイト情報の分類を提案する．さらに，公開されている 38 種類のブラックリストの仕様について調査し，この分類に相当する情報がほとんど含まれていないことを示す．また，実際にブラックリストに一致してインシデント判定が求められた 400 件の悪性 Web サイト情報について手動で調査を行い，一定数の Web サイト情報が外部からの調査によって定義に従った分類ができることを示す．この分類を活用することで速やかな対応ができることをケーススタディとして紹介し，提案分類が有効に働くことを示す．

キーワード：CSIRT，ブラックリスト

Web Blacklist Classification for CSIRT

Hiroki Hada[1,2,a)] Atsuhiro Goto[1]

Received: December 11, 2017, Accepted: June 8, 2018

Abstract: Because there are many threats of web access in organizations, blacklist of malicious web sites is commonly used. The reason why it was judged to be malicious or the reputation score may be given to web site information, but it doesn't provide suitable information for reasonable judgment in CSIRT's incident response. In this paper, we propose malicious web sites blacklist classification which is composed of "Owner", "Content", "Status", and "Update Time" in order to be able to make a reasonable judgement in the "Triage" and "Response" process of incident response. Furthermore, we surveyed the specifications of 38 blacklists that are published and show that there are not enough information corresponding to this classification. In addition, we manually investigated 400 malicious web sites information that actually matched the blacklist for incident judgement, and indicate it is possible to classify a certain number of web site information under our definition by external investigation. We introduce several case studies that CSIRT can respond promptly by utilizing this classification, and show that proposed classification works effectively.

Keywords: CSIRT, blacklist

1. はじめに

1.1 背景

組織が業務を行ううえでインターネットを利用して Web サイトにアクセスすることは現代では必要不可欠であるが，インターネット上には多くの脅威が存在する．インターネットにおける脅威からユーザや組織を守るために，悪性 Web サイトのブラックリストが活用される場合があり，ユーザのアクセス制御を実現する．

世界中の攻撃者が取得する悪性ドメインや利用する IP アドレスは変化し続けるため，ブラックリストに登録される悪性 Web サイトは膨大となる．マイクロソフト社は 180 億の Web ページをスキャンしたところ，1,000 ページあた

[1] 情報セキュリティ大学院大学
Institute of Information Security, Yokohama, Kanagawa 221–0835, Japan
[2] NTT セキュリティ・ジャパン株式会社
NTT Security (Japan) KK, Chiyoda, Tokyo 101–0021, Japan
[a)] dgs158102@iisec.ac.jp

り 0.17，すなわち 306 万の侵害ページを発見したと報告している [1]．脅威のすべてを網羅しているわけではないが，すでに判明している脅威に対してブラックリストは有効に働くため，ブラックリストに登録する悪性 Web サイトを収集する技術，ブラックリストの精度を評価・向上する技術に関する研究は数多く行われている．

悪性 Web サイトに関する情報は「ブラックリスト」と一括りに表現されることが多い．ユーザのアクセスがブラックリストにマッチした場合，ユーザはその理由についてあまり考える必要はなく，そのサイトへのアクセスを諦めるか，業務を継続するための代替手段を考えればよい．

一方で，CSIRT における担当者の視点で考えた場合に，その意味合いは様々となる．インシデントレスポンスを行うことを考えた場合，そのブラックリストがなぜ登録されたのか理由を考える必要がある．たとえば，正規サイトが攻撃者に改ざんされて攻撃コードが埋め込まれた場合，その改ざんサイトがブラックリストに登録されたことでアクセスが遮断されたのであれば，攻撃が未然に防げたためそれ以上の対応は不要であると考えることができる．ところが，アクセスした Web サイトが C2 サーバであれば，たとえ遮断されていたりサイトが閉鎖したりしていても，すでに感染したマルウェアの活動である可能性が考えられるので，インシデントレスポンスを行う必要がある．これは明確に区別する必要がある．

また，別の事例として 2017 年に WannaCry と呼ばれるランサムウェアが流行したが，特定のハードコーディングされたドメインに Web でアクセスし，応答を受け取ることで動作を停止するキルスイッチと呼ばれる機能を備えていた [2]．キルスイッチへのアクセスは WannaCry の感染端末が存在することを意味するため発見できなければならないが，このアクセスはプロキシサーバで遮断してはいけない．これもブラックリストに登録された意味を明確にする必要がある．

このようにブラックリストを利用する人の立場や求められる対応，脅威として登録された理由によってその意味合いが変わってくるが，一括りにブラックリストと表現されてしまい様々な情報が区別されずに混在している．特に，CSIRT にとって最適な意味づけは行われていない．

本稿では，悪性 Web サイト情報に対して CSIRT の役に立つ分類を与えることで効率的なインシデントレスポンスを実現することを目標とし，以下の 3 点についての貢献を行った．

① CSIRT のインシデントレスポンスにおいて合理的な判断を可能とするための「所有者」「コンテンツ」「現在の状態」「最終更新」という 4 項目による悪性 Web サイト情報の分類を提案した．
② 公開されている 38 種類のブラックリストの仕様について調査し，この分類に相当する情報が十分に含まれていないことを示した．
③ 2017 年 9 月 13 日から 2017 年 11 月 23 日までの期間において，サンプリングした 100 組織で実際にインシデント判定を求められた 400 件の悪性 Web サイト情報について詳細な分析を行い，一定数の悪性情報が定義に従って分類できることを示した．また，この分類を活用することで CSIRT は速やかに対応できることをケーススタディとして示した．

1.2 スコープ

組織における Web 利用者に対する悪性 Web サイト情報のブラックリストを対象とし，CSIRT の主な業務であるインシデントレスポンスにおいて活用することを想定する．本稿における「悪性 Web サイト情報」とは，ユーザに対して脅威と考えられるアクセス先の「URL」「ドメイン」「IP アドレス」で定義する．「ドメイン」には FQDN だけでなく，部分一致で利用する上位のドメインも含まれる．これらはプロキシサーバ，IPS に設定され，該当の通信先に対する HTTP と DNS 通信を検知する．

ワームによる攻撃元やスパムメールの発信源など，能動的な攻撃は対象としない．また，SNS や娯楽サイトへのアクセスなど，正規の用途が考えられ組織のポリシによってアクセスの可否判断が変わるものや公序良俗に反するサイトも対象としない．マルウェアのハッシュ値やファイル名，端末においてマルウェアが操作するレジストリなど端末情報，攻撃者が取得した SSL 証明書のハッシュ値も脅威情報として表現されることがあるが，本稿では対象としない [3], [4]．

本稿では CSIRT におけるインシデントレスポンスの判断に役立つ分類を提案するが，その判断自体は組織のポリシに依存するため議論しない．すでに従来の分類で情報が付与されている場合，この利用を否定するものではないものとする．

2. 前提知識

本章では，本稿において必要となる前提知識を示す．

2.1 ブラックリスト

ブラックリストはアクセスの検知や遮断を目的として悪性 Web サイトの情報を記録したものであり，オープンソースのもの [5], [6], [7]，製品に組み込まれて提供されるもの [8]，ライセンス契約に基づいて提供されるもの [9]，組織が独自に収集するものがある．ブラックリストに登録する悪性 Web サイトの情報は，ハニーポットやハニークライアント，マルウェア解析，Web サイトからの情報収集，発見者からの申告などによって収集される．

悪性 Web サイトに対するレピュテーションを付与したブラックリストが存在する [10]．また，SNS やショッピン

グサイトなど，Webサイトのコンテンツのカテゴリで分類しているものがあり，カテゴリの一部として脅威に関する情報が分類されている [8].

ブラックリストには，URL，ドメイン，IPアドレスが混在して登録される．URLは最も細かい制御であり，同じWebサイトであってもコンテンツ単位で情報を記録できる．ドメインが記録された場合はそのドメインが提供するWebサイトそのものが悪性と判断される．ドメインは階層構造で定義されるが，悪性情報を含む最大の長さのものが利用される．同じIPアドレス上に複数のドメインでWebサイトが構成されることもあるが，これらを包括するためにIPアドレスを記録する場合がある．

ブラックリストより広い概念として脅威情報がある [11], [12]．これは必ずしも機器に設定してログを記録するための情報とは限らず，データベースに格納して参照することを目的とした情報を含んでいる．さらに，ハッシュ値やファイル名，攻撃者のプロファイル情報など，脅威に関連する広い情報が含まれる．

2.2 攻撃モデル

攻撃者は組織的に活動しており，役割分担がなされている [13]．エクスプロイトキットによるドライブバイダウンロード攻撃では，Webサイトが改ざんされてリダイレクト処理が埋め込まれる．攻撃サイトから攻撃コードがダウンロードされ，攻撃が成功した場合にマルウェア配布サイトからマルウェアをダウンロードして感染する．マルウェアはC2サーバから命令を受け取って処理を行う [14].

また，メールに添付された悪性ファイルを実行してマルウェアに感染する場合がある [15]．文書ファイルのマクロ機能やJavaScriptなどのスクリプトが添付され，これを実行するとマルウェアをダウンロードして感染する場合と，実行ファイルが添付され，これを実行して感染する場合がある．マルウェアに感染するとC2サーバから命令を受け取って処理を行うものがある．

2.3 HTTPとDNS

Webアクセスにおける通信ではHTTPとDNSのプロトコルが使用される．DNSによりドメインの名前解決を行い，HTTPによりコンテンツの要求とダウンロードが行われる．どちらもネットワーク層でIPアドレスを用いて通信する．ドメインはDNSのペイロードとHTTPプロトコルのHostヘッダに現れる．SSLを使用したHTTPS通信が用いられる場合もある．

2.4 プロキシサーバとIPS

プロキシサーバはDNSによる名前解決とHTTP通信をユーザの代理で行う．URL，ドメイン，IPアドレスをブラックリストとして登録することで，Webサイトへの通信を制御できる．単純に通信をドロップする，ユーザのアクセスに対してエラー画面を返す，ユーザに対して本当にアクセスしてよいか確認を促す，アクセス自体は許可するがログを記録するといった方法で脅威の防御や発見，監査を行う．HTTPS通信を中継する際にSSLを一時的に復号して中のHTTP通信をチェックする機能を備えているシステムもある [16].

IPS（Intrusion Prevention System）ではDNSの名前解決を検知もしくは遮断することができる．メーカが提供するシグネチャの中には，ドメイン単位で検知や遮断ができるものがある [17].

ユーザの操作が介在しないマルウェアによるアクセスはバックグラウンドで自動的に行われるが，直接インターネットへアクセスすることは一般的にはファイアウォールで禁止されているため，このようなアクセスはプロキシサーバを経由すると想定する．マルウェアの中には端末に設定されたプロキシサーバを認識せずに直接DNSサーバに名前解決を行おうとするものがある．このようなマルウェアについてブラックリストを適用する場合はファイアウォールやDNSサーバのログを活用する必要がある．本稿ではこのケースについて言及しないが，この場合においても議論は同様となる．

3. CSIRTにおけるブラックリスト利用の課題

3.1 ブラックリストにおける課題

CSIRTが行う「トリアージ」業務において担当者は必ずしも正しい判断が下せるとは限らないが，合理的な思考に基づいて対応の要否と優先度を判断する必要がある．

まず，ブラックリストに登録されたWebサイトへのアクセスが発生した場合，これが本当にインシデントとして認識すべきかどうか見極める必要がある．たとえば，これがマルウェアを配布するWebサイトであった場合，アクセスを遮断していれば脅威は未然に防げたと考えられる．ところが，これがC2サーバの場合は，アクセスが遮断されていたとしてもマルウェア感染した端末の存在が疑われるため脅威が残存していると考えられる．ブラックリストにはこのような情報が求められる．

次に，インシデント対応の優先度を決定する．たとえば，ブラックリストに記録されたあるIPアドレスに対する通信が発生した場合を考える．実はこのIPアドレスに紐づくWebサーバが300サイトあり，そのうちの1つだけが改ざん被害を受けていたという場合，このアクセスが危険であるという可能性は低いと判断できる．ところが，ブラックリストがこのような情報を含んでいない場合，優先度が正しく判断できない．

ブラックリストにおけるレピュテーションを数値で表現するものがあるが，その根拠は開示されないため，この値に基づいた判断は合理的とはいえない．サイバーキル

チェーンによる攻撃の進行度によって重大さが表現されることもあるが，アクセスしたドメインに付与された情報がサイバーキルチェーンにおける初期工程の「配送」段階を示していても，それだけで優先度が低いとは判断し難い．マルウェア名や攻撃者像を提供する脅威情報サービスがある [19]．脅威という視点で情報が分類されているが，必ずしもインシデントレスポンスという視点で十分に活用できる情報ではない．

「対応実施」においても同様の問題が発生する．何でも遮断するよう設定して，さらにアクセスを遮断するたびにCSIRT がインシデントレスポンスを行うといった業務プロセスを想定することは現実的ではない．すでに感染したマルウェアによる活動であれば，たとえアクセスが遮断されていても CSIRT はインシデントレスポンスを行うべきであるし，すでに修正された改ざんサイトへのアクセスが成功している場合は必ずしも CSIRT はインシデントレスポンスを行う必要があるとは限らない．また，共用サービスや侵害された Web サイトを遮断する場合は，業務通信を誤遮断するリスクを覚悟しなければならない．

このように，CSIRT が合理的な思考に基づいて対応の要否や優先度を判断するための情報が不足していることがいえる．

4. 提案

4.1 提案分類

本稿では，ブラックリストにおける悪性 Web サイト情報が CSIRT にとって有益となるために，**表 1** のとおり分類することを提案する．これは過去 1 年間の実績においてインシデント判定を求められた悪性情報の事例をもとに作成したものである．(1) で Web サイトの所有者で分類する．(2) ではコンテンツの種別について重複選択を許してラベルを付与し，(3) で現在の状態について分類する．さらに，この情報を最後に調査した日時 (4) を記録する．インシデント対応では脅威の種類によって対応方針を決定する．その際に，情報の精度と鮮度をふまえて，より確からしいインシデントから対応する．脅威の種類は (2) に，精度は (1)，鮮度は (3)，(4) にそれぞれ対応する．悪性 Web サイト情報は「URL」「ドメイン」「IP アドレス」のいずれかの形式で登録されるが，たとえ同じ脅威を示しているものであっても，どの形式で登録するかによって分類が異なる場合があることに注意する．

4.2 CSIRT におけるブラックリストの活用

CSIRT ではインシデントを「トリアージ」「事象の分析」「対応計画」「対応実施」というプロセスで行う [18]．「トリアージ」では，検知したすべてのインシデントが対応すべきインシデントとは限らないため，CSIRT の資源を有効に活用するようインシデント対応の要否や優先度を判断する．「対応実施」では，発生したインシデントの収束に加えて再発防止に向けた改善活動を行う．

CSIRT において悪性 Web サイト情報のブラックリストは主に 2 つの用途で使用される．「トリアージ」では，プロキシサーバや IPS で発見したインシデント対応の優先度を決定するために，ブラックリストに紐づく悪性 Web サイト情報や脅威情報を活用する．「対応実施」では，再発防止や新たな脅威の発見を目的として，プロキシサーバや IPS に悪性 Web サイト情報をブラックリストとして設定する．その際に，アクセスを遮断すべきかそうでないか，CSIRT がその事象を把握するべきかそうでないか，ということを考慮する．

表 1 提案する Web ブラックリストの分類
Table 1 Proposed classification of web blacklist.

項目		分類	
(1)	所有者（重複不可）	1	侵害
		2	共有型
		3	攻撃者
		4	不明
(2)	コンテンツ（重複可）	a	リダイレクト
		b	エクスプロイト
		c	悪性ファイル配布
		d	C2
		e	キルスイッチ
		f	権威 DNS サーバー
		g	DNS シンクホール
		h	ソーシャルエンジニアリング
		i	正規コンテンツ
		j	不明・誤登録
(3)	現在の状態（重複不可）	1	現在も悪性
		2	現在は無害
		3	不明
(4)	最終確認	日時	

4.3 提案分類の詳細

各項目の定義と具体例，CSIRT においてこれを明示的に区別する理由について述べる．

(1) 所有者（重複不可）

悪性情報を所有者によって分類する．侵害，共有型，攻撃者，不明の 4 種類に分類され，いずれか 1 つが選択される．

(1)-1 侵害

悪意を持たない一般の Web サイトが攻撃者によって侵害された，もしくは，元々提供しているサービスが悪用された結果，悪性情報として記録されるようになったことを示す．元から存在するページを改ざんして悪性コードを埋め込んだ，新たにファイルとしてマルウェアを設置した場合や，C2 サーバとしてのプロセスが動作し感染端末に命

令を送信するようになった場合などがある．

当該 Web サイトは業務で使用している可能性があるので，脅威情報として記録された場合であっても，ドメインごと遮断すべきか，悪性と認められたコンテンツだけ遮断すべきか，すでに修正されたと考え遮断しないか，といった対応の判断は CSIRT に委ねられる．また，侵害サイトは一般的に修正，改善されることが期待されるため，ブラックリスト提供者は定期的な見直しによる除外が求められるが，実際はブラックリストから除外されずに残り続けることも多い．そのため，ブラックリストの登録時期が極端に古い場合や対処済みというニュースリリースが公開されるなど，現在は影響がない可能性が高いという判断も期待でき，登録時期を考慮して現在の侵害の可能性を分析することもできる．

不特定多数のユーザがファイルを公開できるアップローダといったサービスがあり，ここにマルウェアがアップロードされる場合もある．広告サービスや短縮 URL サービスも悪性サイトへの転送に使用される．元々提供しているサービスを侵害したという意味でここに分類する．

(1)-2　共有型

悪性として記録された情報に対して悪性とは限らない他のリソースが紐づいてしまう場合がある．名前ベースのバーチャルホストでは，同一の IP アドレスに対する HTTP リクエストの中で Host ヘッダに記載された FQDN により応答するコンテンツを識別する．Web スペースを提供するサービスでは，同一のドメインに対して複数の Web サイト所有者を URI のパスで識別する．

このような状況において悪性情報に一致するアクセスが発生したとしても，本当に悪性であるリソースにアクセスしたかどうかは不明である．そのためトリアージの優先度は他よりも低くなる．このアクセスを遮断する場合の業務影響の予測は難しく，慎重に実施する必要がある．

ファイル共有アップローダやブログサービス，匿名通信に使用する Tor ノードの IP アドレス，短縮 URL サービス，ダイナミック DNS サービスで提供される親ドメイン，CDN や IaaS 型クラウドサービスが内部的に割り当てるドメインもこちらに分類される．

(1)-3　攻撃者

攻撃者が自前で調達した Web サイトやドメイン，攻撃者が設置した悪性ファイルの URL はこちらに分類する．たとえば，攻撃者がドメインを取得する際に同一のメールアドレス使いまわすことがあり，whois データベースを参照することでドメインが悪性と判断できる場合がある．

悪意を持たない一般の Web サイトを攻撃者によって模倣された場合，または一見して実在しそうな組織を装ったコンテンツが設置された場合もこちらに分類する．この分類におけるアクセスは問題なく遮断できることが期待できる．

(1)-4　不明

悪性 Web サイト情報を調査してもその素性がまったく分からない場合はこちらに分類する．

(2)　コンテンツ（重複可）

Web サイトから応答されるコンテンツによって分類する．ドライブバイダウンロード攻撃の進行度によって，リダイレクト，エクスプロイト，悪性ファイル配布，C2 という 4 種類に分類する．また，過去の実績から他にもキルスイッチ，権威 DNS サーバ，DNS シンクホール，ソーシャルエンジニアリング，正規コンテンツ，不明・誤登録という 5 種類の分類が事例として必要であることが分かった．複数の役割を持つ場合があるので，適合するものすべてを選択する．

(2)-a　リダイレクト

悪性サイトへの転送機能を持つ Web ページで，エクスプロイトキットにおける初期の攻撃段階としてよく使用される．リダイレクト自体は直接的な被害を受けるものではないため，後続のアクセスが失敗していればインシデントレスポンスが不要であると判断してもよい．

(2)-b　エクスプロイト

端末の脆弱性を悪用して制御を奪う悪性コードを返す Web ページである．この通信は攻撃であるため，パッチが適用されていないなど，一定の条件を満たした場合に侵害される．影響を調査するためには，被害端末を特定して端末を調査する必要があるため，区別する必要がある．

(2)-c　悪性ファイル配布

マルウェアを呼び込むためのダウンローダ，マルウェアを生成するドロッパ，マルウェア，アドウェアを返すものを分類する．

(2)-d　C2

すでに端末に感染したマルウェアが外部からコマンドを受信するためにアクセスする Web ページである．HTTP の上に独自のプロトコルを構成するものや，ブログ記事のように一見して Web コンテンツに見えるが実はコマンドとして機能するものも存在する．C2 通信は必ずしも HTTP とは限らず，DNS の TXT レコードを用いた DNS トンネリングによる通信の場合もある．

感染端末の存在が疑われるためアクセスが遮断されていた場合であってもインシデントレスポンスが求められる．一方で，ユーザが意図的にアクセスした場合には影響がある可能性は低い．ブラウザでアクセスすると，同時に favicon.ico へのアクセスが出る．ユーザが調査目的や興味本位でアクセスする場合，このような挙動を示す．接続先が C&C サーバの場合，入手であることが推測されれば影響ないと判断できる場合がある．

(2)-e　キルスイッチ

マルウェアがサンドボックスにおける動的解析環境を検知するために行うアクセス先である．

動的解析は存在しないドメインに対しても応答を返す機能を持つものもあるため，キルスイッチからの応答を受信して動作を停止するため，アクセスを遮断してはいけない．

(2)-f 権威 DNS サーバ

ドメインではなく，名前解決を行う権威 DNS サーバが悪性と判断される分類である．悪性ドメインは匿名で購入可能なレジストラで取得されることがあり，このようなサービスを利用して取得した場合の名前解決は特定の権威 DNS サーバによる名前解決を経由するが，この通信をブラックリストとして検知することがある．

(2)-g DNS シンクホール

テイクダウンされた，もしくは有効期限が切れた悪性サイトのドメインをセキュリティ研究者が取得し，アクセスしても問題がない IP アドレスを応答するように設定したものである．すでに無害化したドメインである．

(2)-h ソーシャルエンジニアリング

機密情報を送信させるフィッシングサイトや偽ショッピングサイト，パソコンのトラブル解決を装って偽のサポートツールのインストールを誘導するサイトなど，ソーシャルエンジニアリングとしての脅威を分類する．

この分類における影響はユーザの操作に起因するため，被害者へのヒアリングが必要となる．

(2)-i 正規コンテンツ

侵害されていない一般の Web サイトがブラックリストに登録されることがある．マルウェアがインターネットによる Web アクセスが可能かどうか疎通確認を行う場合や，外部アクセスを行うグローバル IP アドレスを調査するため環境情報表示サイトにアクセスする場合がある．

この通信自体は無害であるため積極的に利用しないが，マルウェアの活動の兆候の可能性として考えることもできる．

(2)-j 不明・誤登録

ブラックリストに登録した根拠がまったく不明なものが分類される．明確な根拠がないため，誤登録の可能性も考えられる．この分類は第三者が評価を行う場合のみ使用する．

(3) 現在の状態（重複不可）

現在の状態によって分類する．現在も悪性，現在は無害，不明の 3 種類に分類され，いずれか 1 つが選択される．

(3)-1 現在も悪性

悪性情報が登録，もしくは最後に再調査された時点で意図したとおり悪性であったことを示す分類である．

悪性サイトは修正される，攻撃者が活動を停止するといった理由で無害となる．逆に，再発防止策が十分でなく再び侵害される，活動を再開するといった理由により再び悪性サイトとなる場合がある．そのため，ここに分類された情報は必ずしも正しいとは限らないが，最後に調査された時期とあわせた場合にどこまでを正しいと想定するか考えておくために必要な情報である．DGA で生成されたドメインのうち実際に名前解決されるものもここに分類される．悪性コードを配信してしまう広告があるが，いくら審査を厳しくしても根本的な対策は困難であり，今後も悪性挙動を示す可能性があることから，ここに分類する．

(3)-2 現在は無害

現在は無害であると報告されているものを指す．テイクダウンされたサーバや DNS シンクホール，ドメインの有効期限が切れているものはここに分類される．また，侵害サイトにおいて事象が修正されたと考えられるものはここに分類される．必ずしも適切な再発防止策がなされているとは限らないため，この分類を信用するかどうかは組織のポリシに委ねられる．

(3)-3 不明

悪性や無害といえる根拠がないものがここに分類される．サービスのポートが応答しないもの，サーバとしては動作しているが何も応答しないもの，無害なコンテンツを応答するものである．一見して無害に分類してもよいように思えるが，アクセス元の IP アドレス，User-Agent や Referer のような HTTP ヘッダなど，特定の条件に一致した場合にのみ悪性コンテンツを応答するものがあるため，不明として分類する．DGA で生成されたドメインで名前解決されないものもここに分類される．この分類における判断は組織のポリシに委ねられる．

(4) 最終確認

最後に確認した日時を記載する項目である．これは現在の状態における評価結果の確からしさを判断するための情報として利用される．

5. 調査・評価

5.1 公開ブラックリストにおける登録情報

公開されている 38 種類のブラックリストについて，その登録情報の項目を調査した．結果を**表 2** に，その詳細を付録の表 A·1 に示す．表 2 では，各ブラックリストについて，その項目を，記載あり，一部記載あり，記載なしの 3 つで評価した．

(1) 所有者に関する情報は多くのブラックリストにおいて記載がされていなかったが，4 つのブラックリストにおいては一部記載がされていた．ZeroCERT では Web サイトの状態を表す「State code」の 1 項目として「compromised」とい

表 2 公開ブラックリストにおける登録情報
Table 2 Registered information in public blacklists.

項目	記載あり	一部あり	記載なし
(1) 所有者	0	4	34
(2) コンテンツ	0	24	14
(3) 現在の状態	16	0	22
(4) 最終確認	22	1	15

う情報が区別されていた [20]．ZeuS Tracker では「Level」という項目に「Hacked webserver」「Free hosting service」という情報が区別されていた [21]．ThreatCrowd では直接的な項目を含まないが，Passive DNS 情報を活用してドメイン，IP アドレスなどの要素をグラフ表示する機能を持ち，これを確認することで共有サーバの存在が判明する場合がある．いずれのブラックリストにおいても，独立した項目として所有者の有無が区別されていたものではなく，カテゴリの分類の 1 つとして侵害サイトや共有サーバが選択できるという状態であった [22]．

(2) コンテンツに関する情報は 6 割以上のブラックリストにおいて一部記載されていた．HijackedUrls は悪性サイトにリダイレクトする Web サイトの情報を収集しており，リダイレクト先の URL が記載されていた [23]．Ransomware Tracker はランサムウェアに関する Web サイトの情報を収集しており，「Distribution Sites」「Botnet C&Cs」「Payment Sites」が区別されていた [24]．WebSecurityGuard では，不特定のユーザによるコンテンツの評価と「Yes/No」といったレピュテーションが記載されていた [25]．その他のブラックリストにおいてもエクスプロイトと悪性ファイル配布が区別されているものが多かったが，いずれも分類項目は一部にとどまっていた．

(3) 現在の状態については約 4 割，(4) 最終確認は約 6 割のブラックリストが記載していた．Malc0de では 30 日以内に登録されたことが分かるが，具体的な日付に関する情報がないため一部記載ありに集計した [26]．

5.2 インシデント判定が求められた悪性情報の分析

2017 年 9 月 13 日から 2017 年 11 月 23 日までの期間でサンプリングした 100 組織において実際にインシデント判定が求められた 400 件の悪性情報を対象として，手動で調査して分類した．インシデント判定が求められた事象の検知元を**表 3** に，インシデント判定の結果，対応が必要と判断された 31 件の事象に関連するマルウェアを**表 4** に示す．

調査は以下の手法で行った．悪性情報は通信が発生した時間と調査を行った時間の差が大きいと情報が不正確となるため，実通信がブラックリストにマッチした時点で速やかに調査を開始した．

- インターネット上の情報を検索する

検索エンジンで悪性情報を検索する．悪性情報に関する調査結果は公開されていることも多い．悪性情報そのものだけでなく，これをホスティングしている事業者について調査することで Web サイトの所有者について分かる場合もある．

- whois 情報や名前解決結果を確認する

whois 情報やドメインの名前解決，ドメインの逆引きから Web サイトの所有者について調査を行う．Passive DNS を活用すると，過去の時点での名前解決結果や，IP アドレスに紐づく他のドメインの情報が得られ，これだけで悪性と判断できる場合や，IaaS 型クラウドサービスで多くの利用者が紐づいていて悪性といえる根拠が少ないことが分かる場合もある．

- 脅威情報データベースを確認する

レピュテーションや脅威情報データベースの登録情報，アンチウイルスの検知名，Web サイトのカテゴリを参照する．

- 実際にアクセスする

動的解析サンドボックスから実際に Web サイトにアクセスを行い，応答されるコンテンツや悪性挙動の有無を調査する．何度もアクセスすることで攻撃者に調査であることが気づかれ挙動を変えるものがあるため，大量の IP アドレスを保有し 1 分ごとに送信元がユニークに変わる環境を使用した．ただし，水飲み場型攻撃でアクセス元などの条件が一致した場合のみ攻撃を受ける場合や，めったに攻撃が発動しない場合に無害に見えてしまうことがある．必要に応じて Web Archive を利用し，ブラックリストに登録された当時の Web サイトを調査する．

- パケットキャプチャを確認する

ブラックリストにマッチした実通信のパケットキャプチャが取得できている場合は活用する．水飲み場型攻撃のように特定の環境でしか発動しない脅威も調査できる可能性がある．

- マルウェアや悪性スクリプトを解析する

必要に応じてマルウェア解析や Web サイトに埋め込まれた悪性スクリプトの解析を行う．マルウェアの接続先や

表 3 インシデント判定が求められた悪性情報の入手元
Table 3 Devices that detected malicious activity to judge incident.

検知機器	検知手法	件数
Proxy	ブラックリストとの照合	82
Firewall	ブラックリストとの照合	11
IPS	シグネチャ検知	207
Sandbox	動的解析の通信先	10
SIEM（上記全ての相関分析）	継続的な通信	54
	DGA マルウェアの名前解決	12
	その他	24

表 4 インシデントに関連するマルウェア
Table 4 Malware related to the incident.

マルウェア名	件数
Locky	6
Ramnit	2
Hancitor	2
Loki	1
Daserf	1
WannaCry	1
Ursnif	1
不明	17

表 5 評価結果
Table 5 Evaluation result.

項目		URL	ドメイン	IP	合計
		35	348	17	400
(1)	1	16	132	0	148
	2	2	18	17	37
	3	5	80	0	85
	4	12	118	0	130
(2)	a	2	9	0	11
	b	0	4	0	4
	c	16	105	2	123
	d	6	41	0	47
	e	0	1	0	1
	f	0	0	1	1
	g	0	6	1	7
	h	4	88	1	93
	i	5	2	0	7
	j	3	103	13	119
(3)	1	10	78	1	89
	2	15	95	4	114
	3	10	175	12	197

悪性スクリプトのリダイレクト先が判明する．

ブラックリストは，製品の一部として提供されるもの，インテリジェンスサービスとして提供されるもの，無償で公開されているもの，組織の通信ログから独自に収集したものを使用している．この悪性情報を分類したところ，この内訳は**表 5** に示すとおりとなった．

この結果において，「(1) 所有者」の 67.5%，「(2) コンテンツ」の 70.2%，「(3) 現在の状態」の 50.7%が「不明」以外に分類され，ブラックリスト作成者が本定義に従って分類することが一定の割合で可能であることが示せた．今回はインシデント判定が求められてから第三者の立場として悪性情報を評価しているが，ブラックリスト作成者本人であればリアルタイムかつ登録した理由が明確であるため，より高い割合となる可能性がある．

今回の調査において，ブラックリストで検知した脅威情報で登録理由が不明なものは「(2)-j 不明・誤登録」「(3)-3 不明」に分類したが，ブラックリストの登録者であれば理由が分かると考えられる．

5.3 CSIRT における効果

本分類は CSIRT における「トリアージ」業務においてインシデント対応の要否や優先度を決定するため，また「対応実施」業務においてプロキシサーバや IPS にブラックリストとして設定するかどうか判断するために使用する．この分類に基づく対応方針はあらかじめ組織のポリシに従ってマニュアルとして策定することができる．シンプルな基準でインシデント対応を行いたい CSIRT を想定した場合の簡易マニュアルとその具体的な対応の例を付録 2 に紹介する．たとえば，このマニュアルを想定して 400 件のインシデントに対応した場合，281 件（70.3%）のインシデントは「不明・誤登録」以外に分類され，CSIRT の担当者に対して論理的な思考に基づいた明確な対応方針を即座に与えられる．

今回は 400 件の悪性情報をすべて調査する必要があったため「最終確認」は評価時点での日時となったが，実際はブラックリスト作成時刻となるため情報が古くなる可能性がある．ドライブバイダウンロード攻撃における悪性サイトの 80%は生存期間が 170 日以下であると報告されている [28]．これをどのようにとらえるかは組織のポリシに従うところであるが，「リダイレクト」「エクスプロイト」「悪性ファイル配布」「C2」に関して悪性と判断された場合，半年間は悪性と考えた方がよいととらえることができる．ただし「C2」に関しては，所有者が「攻撃者」の場合は感染端末が疑われるため最終確認に関係なく対応すべきである．

「ソーシャルエンジニアリング」に関して，JPCERT/CC は国内外へのフィッシングサイトの通知を行っているが，97%は 10 営業日以内に対処されたと報告しており，生存期間は非常に短いことが分かる [29]．ただし，実際にアクセスして比較的容易に確かめられるため，最終確認に頼らなくてもよい．

「キルスイッチ」「DNS シンクホール」「正規コンテンツ」は一般的に変化しないため，運用上は最終確認に関係なく現在の情報として活用する．逆に「権威 DNS サーバ」は匿名レジストラで取得したドメインなど，これ自体が必ずしも悪性であることを示すものではないため，最終確認に関係なくそのつど調査を行う必要がある．

6. 関連研究

本章では，ブラックリストの分類に関連する標準技術，関連研究について示す．

6.1 標準技術

サイバー攻撃活動における脅威を構造的に表現するために策定された STIX という記述形式がある [27]．バージョン 1 では脅威情報を Campaigns，Threat_Actors，TTPs，Indicators，Observables，Incidents，Courses_Of_Action，Exploit_Targets といった構成で表現するが，「(1) 所有者」において侵害サイトであることを明確に示す項目がない．「(3) 現在の状態」を示すものとしては「Campaigns: Status」が近いが，これは攻撃者の活動を示している．すでに活動が終了したキャンペーンであっても Web サイトにマルウェアが残っている場合があるため，CSIRT の活動に対して直接的には結び付かない．また，STIX において脅威はロッキードマーティンが提案しているサイバーキルチェーンの 7 段階モデルで表現されることがあるが，攻撃の初期段階だからといってインシデントレスポンスが不要と考えるこ

ともできない．

脅威情報を共有するための基盤として開発された MISP というソフトウェアがある [30]．脅威情報に対してラベルを付与することができるが，どのようにラベルを定義して脅威を表現すべきかといった規定や主張はない．ただし，Taxonomy（分類法）という機能があり，デフォルトで用意されている 30 種類を含む様々な既存のフレームワークをインポートして利用することができ，この中に脅威の種別や状態を表現するものがある．SANS はマルウェアの種類を分類している [45]．ENISA は物理的な脅威や法的リスクを含めたビジネス上の脅威を表現している [31]．eCSIRT はマルウェアの種類や侵入方法などを定義している [32]．FIRST や CIRCL はインシデントの種別を定義している [33], [34]．NATO は情報の信頼度を定義している [46]．また，出典元の記載がないが adversary というフレームワークを利用しており，インフラの所有者やその状態について定義している．これは「(1) 所有者」と「(3) 現在の状態」に近いが，悪性 Web サイト情報に対紐づく内容ではなく，攻撃者が利用するインフラについて紐づく情報である．

6.2 関連研究

ブラックリストを評価する研究として，Kührer らはブラックリストを収集するシステムを構築し，49 種類のブラックリストを提供するサイトから 41 万件以上のユニークな URL を収集してその共通度合いや IP アドレスを用いた関係性を報告している [35]．さらに，マルウェアブラックリストの有効性を評価するため，非使用（パーク）ドメインとシンクホールという分類で 19 種類のブラックリストを分析している [36]．Sheng らは，191 個のフィッシング URL を調査し，フィッシングサイトがブラックリストに登録されるまでの時間を調査している [37]．これらは CSIRT にとって有用かどうかという視点では調査していない．

マルウェア関連ドメインを検出する研究として，Antonakakis らは TLD サーバおよび大規模な機関で動作するシステムを構築し，IP レピュテーションなどと組み合わせることでマルウェア関連ドメインを早期に検出する機能を提案している [38]．さらに，クラスタリングを用いて C2 通信に用いられる DGA ドメインを検出する手法を提案している [39]．Bilge らは，パッシブ DNS を用いることにより判明した悪性ドメインを調査している [40]．Rahbarinia らは，無効化したドメインを発見してシンクホール，パーキング，NX-Domain Rewriting の 3 種類に分類する SinkMiner というシステムを提案している [41]．

Sinha らは，スパムメールの送信元ブラックリストを調査するため，レピュテーションベースによる複数のブラックリストの有効性を調査している [42]．Rossow らは，スパムメールの送信元の IP アドレスの評価において，ブラックリストとホワイトリストの両方に登録されたものについて調査している [43]．Thomas らは，ソーシャルネットワークなどの Web サービスに投稿されるコメントに含まれる URL がスパムかどうかを判定するシステムを提案している [44]．

7. まとめと今後の課題

本稿では，Web サイトの脅威に対して CSIRT がかかえるブラックリストの課題を示し，CSIRT にとって有用な 4 項目による分類を提案し，公開されている 38 種類のブラックリストにおいてこの分類に相当する情報がほとんど含まれていないことを示した．また，100 組織において実際にインシデント判定を求められた 400 件の悪性情報について手動で調査を行い，提案する分類に妥当性があることを示した．結果として，ブラックリスト作成者が CSIRT のために提供すべき情報を示すことができた．

今後はより多くのデータで分類の網羅性を検証することができる．特に，新しい脅威や今回の評価には存在しなかった想定しない事例が出現し，「コンテンツ」において適切な分類がない事態が考えられる．現状では「不明」に分類することになっており，数が少ないうちはそれでも有効に機能すると考えているが，将来的には分類を見直す必要が出てくる可能性もある．また，実データを用いた評価において悪性 Web サイト情報の分類を手動で行ったが，実際の運用ではコストにつながるため，分類作業を自動で行う技術が求められる．CSIRT における実際のインシデントレスポンスの負荷の軽減を評価し，またヒアリングなどを実施することで，CSIRT にとってより適切な分類を考えることができる．

悪性ファイルの中でも広告を表示するアドウェアや仮想通貨を採掘するマイニングツールなどは Potentially Unwanted Program（PUP）などと呼ばれる．PUP はほとんどマルウェアと同等の挙動を示すものから，広告を表示するだけのものまで様々であるが，組織のポリシによって CSIRT のトリアージにおける優先度を下げられるものがあるため，さらなる分類を検討することができる．

侵害サイトは何らかの脆弱性があると考えられるため，複数の攻撃者に侵害される場合がある．そのため，ブラックリスト作成者が付与したラベルは脅威の 1 つにすぎず，別の脅威を含むかもしれない．このような場合を考慮するフレームワークも検討できる．

参考文献

[1] Microsoft: Security Intelligence Report Volume 22 (online), available from ⟨https://www.microsoft.com/en-us/security/intelligence-report⟩ (accessed 2017-12-10).
[2] CERT-MU: THE WANNACRY RANSOMWARE, available from ⟨http://cert-mu.govmu.org/English/

Documents/White%20Papers/White%20Paper%20-%20The%20WannaCry%20Ransomware%20Attack.pdf⟩ (accessed 2017-12-10).
[3] SANS Institute: Using IOC (Indicators of Compromise) in Malware Forensics (online), available from ⟨https://www.sans.org/reading-room/whitepapers/forensics/ioc-indicators-compromise-malware-forensics-34200⟩ (accessed 2017-12-10).
[4] abuse.ch: SSL Blacklist (online), available from ⟨https://sslbl.abuse.ch⟩ (accessed 2017-12-10).
[5] Xylitol: Cybercrime Tracker (online), available from ⟨http://cybercrime-tracker.net⟩ (accessed 2017-12-10).
[6] Malware Domain List (online), available from ⟨http://www.malwaredomainlist.com⟩ (accessed 2017-12-10).
[7] RiskAnalytics: Malware-Domains (online), available from ⟨http://www.malware-domains.com⟩ (accessed 2017-12-10).
[8] Blue Coat: Blue Coat WebPulse (online), available from ⟨https://www.bluecoat.com/sites/default/files/editor_files/bcs_WebPulse_Tech_Overview_wp_v1b.pdf⟩ (accessed 2017-12-10).
[9] FFRI: BlackURL (online), available from ⟨http://www.ffri.jp/assets/files/services/ctrg/BlackURL_brochure.pdf⟩ (accessed 2017-12-10).
[10] Cisco: IronPort AsyncOS 7.7.5 for Web (online), available from ⟨https://www.cisco.com/cisco/web/support/JP/docs/SEC/WebSecur/WebSecurAppliance/UG/002/WSA_7.7.5_UserGuide-J.pdf⟩ (accessed 2017-12-10).
[11] FireEye: iSIGHT Intelligence Subscriptions (online), available from ⟨https://www.fireeye.com/products/isight-cyber-threat-intelligence-subscriptions.html⟩ (accessed 2017-12-10).
[12] PaloAlto Networks: AutoFocus (online), available from ⟨https://www.paloaltonetworks.com/products/secure-the-network/subscriptions/autofocus⟩ (accessed 2017-12-10).
[13] Nappa, A., Rafique, M.Z. and Caballero, J.: Driving in the Cloud: An Analysis of Drive-by Download Operations and Abuse Reporting, *Proc. 10th International Conference on Detection of Intrusions and Malware & Vulnerability Assessment* (*DIMVA 2013*), pp.1–20, Springer (2013).
[14] Kotov, V. and Massacci, F.: Anatomy of Exploit Kits Preliminary Analysis of Exploit Kits as Software Artefacts, *Proc. 5th International Conference on Engineering Secure Software and Systems* (*ESSoS 2013*), pp.181–196, ACM (2013).
[15] Malwarebytes Labs: State of Malware Report 2017 (online), available from ⟨https://www.malwarebytes.com/pdf/white-papers/stateofmalware.pdf⟩ (accessed 2017-12-10).
[16] A10 Networks: Thunder SSLi (online), available from ⟨https://www.a10networks.com/products/thunder-series/ssl-decryption-encryption-and-inspection-ssl-insight⟩ (accessed 2017-12-10).
[17] PaloAlto Networks: Blocking Suspicious DNS Queries with DNS Proxy Enabled (online), available from ⟨https://live.paloaltonetworks.com/t5/Management-Articles/Blocking-Suspicious-DNS-Queries-with-DNS-Proxy-Enabled/ta-p/66037⟩ (accessed 2017-12-10).
[18] JPCERT/CC：インシデントハンドリングマニュアル（オンライン），入手先 ⟨https://www.jpcert.or.jp/csirt_material/files/manual_ver1.0_20151126.pdf⟩（参照 2017-12-10）.
[19] CrowdStrike: Falcon Intelligence (online), available from ⟨https://www.crowdstrike.com/products/falcon-intelligence⟩ (accessed 2017-12-10).
[20] ZeroCERT: Safeguard (online), available from ⟨https://center.zerocert.org/safeguard⟩ (accessed 2017-12-10).
[21] abuse.ch: ZeuS Tracker (online), available from ⟨https://zeustracker.abuse.ch⟩ (accessed 2017-12-10).
[22] ALIEN VAULT: ThreatCrowd (online), available from ⟨https://www.threatcrowd.org⟩ (accessed 2017-12-10).
[23] NoVirusThanks: Hijacked Urls Database (online), available from ⟨http://www.hijackedurls.com⟩ (accessed 2017-12-10).
[24] abuse.ch: Ransomware Tracker (online), available from ⟨https://ransomwaretracker.abuse.ch⟩ (accessed 2017-12-10).
[25] Web Security Guard: Website Database (online), available from ⟨http://www.websecurityguard.com/database.aspx⟩ (accessed 2017-12-10).
[26] Malc0de: Malc0de Database (online), available from ⟨http://malc0de.com/database⟩ (accessed 2017-12-10).
[27] MITRE: Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX) (online), available from ⟨https://www.mitre.org/sites/default/files/publications/stix.pdf⟩ (accessed 2017-12-10).
[28] Tanaka, Y. and Goto, A.: Suspicious FQDN Evaluation based on Variations in Malware Download URLs, *Proc. IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining* (*ASONAM 2017*), pp.811–818 (2017).
[29] JPCERT/CC：インシデント報告対応レポート（オンライン），入手先 ⟨https://www.jpcert.or.jp/pr/2018/IR_Report20180116.pdf⟩（参照 2018-04-01）.
[30] MISP project: Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing (online), available from ⟨http://www.misp-project.org⟩ (accessed 2017-12-10).
[31] ENISA: Threat Taxonomy. A tool for structuring threat information (online), available from ⟨https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/etl2015/enisa-threat-taxonomy-a-tool-for-structuring-threat-information⟩ (accessed 2017-12-10).
[32] eCSIRT: European CSIRT Network IST-2001-37558 (online), available from ⟨http://www.ecsirt.net/eCSIRT-WP1-final-report.pdf⟩ (accessed 2017-12-10).
[33] FIRST: CSIRT Case Classification (online), available from ⟨https://www.first.org/resources/guides/csirt_case_classification.html⟩ (accessed 2017-12-10).
[34] CIRCL: Taxonomy – Schemes of Classification in Incident Response and Detection (online), available from ⟨https://www.circl.lu/pub/taxonomy⟩ (accessed 2017-12-10).
[35] Kührer, M. and Holz, T.: An Empirical Analysis of Malware Blacklists, *Praxis der Informationsverarbeitung und Kommunikation* (*PIK 2012*), Vol.35, No.1, pp.11–16 (2012).
[36] Kührer, M., Rossow, C. and Holz, T.: Paint it Black: Evaluating the Effectiveness of Malware Blacklists, *Proc. 17th International Symposium on Research in Attacks, Intrusions and Defenses* (*RAID 2014*), pp.1–21, Springer-Cham (2014).
[37] Sheng, S., Wardman, B., Warner, G., Cranor, L.F. and Hong, J.: An Empirical Analysis of Phishing Blacklists, *Proc. 6th Conference on Email and Anti-Spam* (*CEAS*

2009) (2009).
[38] Antonakakis, M., Perdisci, R., Lee, W., Vasiloglou II, N. and Dagon, D.: Detecting Malware Domains at the Upper DNS Hierarchy, *Proc. 20th USENIX Conference on Security* (*SEC 2011*), p.27, Berkeley (2011).
[39] Antonakakis, M., Perdisci, R., Nadji, Y., Vasiloglou, N., Abu-Nimeh, S., Lee, W. and Dagon, D.: From Throw-Away Traffic to Bots: Detecting the Rise of DGA-Based Malware, *Proc. 21st USENIX Conference on Security Symposium* (*Security 2012*), p.24, Berkeley (2012).
[40] Bilge, L., Kirda, E., Kruegel, C. and Balduzzi, M.: EXPOSURE: Finding Malicious Domains Using Passive DNS Analysis, *Proc. 18th Annual Network and Distributed System Security Symposium* (*NDSS 2011*) (2011).
[41] Rahbarinia, B., Perdisci, R., Antonakakis, M. and Dagon, D.: SinkMiner: Mining Botnet Sinkholes for Fun and Profit, *Proc. 6th USENIX Workshop on Large-Scale Exploits and Emergent Threats* (*LEET 2013*) (2013).
[42] Sinha, S., Bailey, M. and Jahanian, F.: Shades of Grey: On the effectiveness of reputation-based "blacklists", *Proc. 3rd International Conference on Malicious and Unwanted Software* (*MALWARE 2008*), pp.57–64 (2008).
[43] Rossow, C., Czerwinski, T., Dietrich, CJ. and Pohlmann, N.: Detecting Gray in Black and White, *MIT Spam Conference 2010* (*SC 2010*) (2011).
[44] Thomas, K., Grier, C., Ma, J., Paxson, V. and Song, D.: Design and Evaluation of a Real-Time URL Spam Filtering Service, *Proc. IEEE Symposium on Security and Privacy* (*SP 2011*), pp.447–462 (2011).
[45] SANS Institute: InfoSec Reading Room, Malware 101-Viruses (online), available from ⟨https://www.sans.org/reading-room/whitepapers/incident/malware-101-viruses-32848⟩ (accessed 2018-04-04).
[46] Department of the Army: FM 2-22.3 (FM 34-52) HUMAN INTELLIGENCE COLLECTOR OPERATIONS (online), available from ⟨https://fas.org/irp/doddir/army/fm2-22-3.pdf⟩ (accessed 2018-04-04).

付　　録

A.1 公開ブラックリストにおける登録情報について

5.1 節「公開ブラックリストにおける登録情報」において，公開されている 38 種類のブラックリストについて調査した結果を**表 A·1** に示す．各項目について，○は記載あり，△は一部記載あり，×は記載なしを意味している．

A.2 ケーススタディ

本提案における分類を用いたインシデント対応の例をケーススタディとして示す．**表 A·2** はユーザ企業においてブラックリストに付与されたラベルから比較的シンプルな基準でインシデント対応の判断を行いたい CSIRT を想定した場合の対応判断マニュアルを例として示したものである．このマニュアルにおいて「対応する」という文言は，トリアージにおいては端末やユーザを特定してヒアリングやウイルススキャン，再インストールなどの処置を行うことを意味し，対応実施においてはプロキシサーバなどに遮断設定を行うことを意味する．

実際に発生しうる代表的なインシデントを想定し，このマニュアルに従って合理的な判断が行えることをケーススタディとして示す．この例では便宜上，最初のアラートを検知した日時を「2017 年 11 月 23 日 12:00」として説明する．

(1) 被害の可能性が低い例

被害の可能性が低く，一般的には対応が不要であると考えられるインシデント対応の例を 2 つ示す．

(1-1) DNS 名前解決要求を IPS で検知したことをトリガにトリアージを開始した．このドメインは「コンテンツ：リダイレクト」「現在の状態：現在も悪性」「所有者：侵害」「最終確認：2015 年 6 月 8 日 15:38」に分類されている．CSIRT の担当者はプロキシサーバのログからこの悪性ドメインにアクセスしたユーザの IP アドレスを特定したが，この IP アドレスからはそれ以降のアクセスは行われていなかった．CSIRT 担当者が調べたところ，このサイトは日本の企業が公開している公式サイトであったが，登録された日時が 2 年以上前と古く，すでに修正されているためリダイレクトはされなかったと考えられる．ユーザは改ざんサイトへのアクセスは行ったものの，攻撃サイトへのリダイレクトは行われず特に被害は受けなかったためクローズした．

(1-2) プロキシサーバで悪性ドメインへの通信を検知した．このドメインは「コンテンツ：C2」「現在の状態：悪性」「所有者：侵害」「最終確認：2017 年 5 月 27 日 20:19」に分類されている．CSIRT の担当者がこのドメインについて調査を行ったところ，このサイトは誰でも無料でアカウントが作成できるブログサイトであったが，このサイトに関する追加の脅威情報は特に見当たらなかった．このサイトのどこかに悪性コンテンツが埋め込まれている，もしくは特定のブログ記事にコマンドを埋め込んでボットを操作するマルウェアに感染している可能性があるが，通常のブログ記事を閲覧しただけの状況も十分に考えられ，単純にこのドメインにアクセスしたという事実だけで影響があると判断するには材料が乏しい．またこの前後に関連するアクセスは存在しなかったため，インシデント対応としてはクローズしてよいと判断した．

(2) 被害が疑われる例

被害がほぼ確実に発生している，もしくは被害を受けている可能性があり，何らかの対応が必要であると考えられるインシデント対応の例を 3 つ示す．

(2-1) プロキシサーバで悪性 URL へのアクセスを検知してトリアージを開始した．この悪性 URL は「コンテンツ：悪性ファイル配布」「現在の状態：現在も悪性」「所有

表 A·1 公開ブラックリストにおける登録情報の詳細
Table A·1 Details of registered information in public blacklists.

No.	ブラックリスト	所有者	コンテンツ	現在の状態	最終確認	備考（△となった理由）
1	Shalla's Blacklists	×	×	×	×	
2	AVGThreatLabs	×	×	○	○	
3	Bambenek Consulting	×	△	○	○	C2 ドメインと DGA ドメインが区別される．
4	BitDefender	×	×	×	×	
5	CyberCrime	×	△	×	○	マルウェア名で分類される．
6	security-research	×	×	○	○	
7	DNS-BH	×	△	○	○	カテゴリの中でフィッシングなどが分類される．
8	Fortinet	×	△	×	×	カテゴリの中でフィッシングなどが分類される．
9	GoogleSafeBrowsing	×	△	×	○	悪性と判断した簡単な理由が記載されている．
10	HijackedUrls	×	△	○	○	リダイレクトサイトであることが区別される．
11	Malc0de	×	×	×	△	過去 30 日以内に確認されたことが分かる．
12	MalwareDomainList	×	△	×	○	マルウェアの種類で分類される．
13	OpenPhish	×	×	○	×	
14	PhishTank	×	×	○	○	
15	Quttera	×	×	○	○	
16	Ransomware Tracker	×	△	○	○	ランサムウェアに限定されているが，Distribution Sites、Botnet C&Cs、Payment Sites が区別される．
17	SCUMWARE	×	△	×	○	マルウェア名で分類される．
18	Spam404	×	△	×	○	カテゴリの中でフィッシングなどが分類される．
19	ThreatCrowd	△	△	×	×	マルウェア名で分類される．Passive DNS 情報を活用してドメイン，IP アドレスなどの要素をグラフ表示する機能を持ち，これを確認することで共有サーバーの存在が判明する場合がある．
20	ThreatLog	×	△	○	○	カテゴリの中でフィッシングなどが分類される．
21	URLVir	×	×	○	○	
22	VXVault	×	×	×	○	
23	WebSecurityGuard	×	△	×	×	カテゴリの中でフィッシングなどが分類される．不特定のユーザーによるコンテンツの評価と「Yes/No」といったレピュテーションを含む．
24	ZeroCERT	△	△	×	○	Web サイトの状態を表す「State code」の 1 項目として「compromised」という情報を含む．カテゴリの中でフィッシングやマルウェア名などが付与される場合がある．
25	ZeuS Tracker	△	△	○	○	ZeuS に限定されているが，「Level」において「Hacked webserver」「Free hosting service」という情報を含む．
26	Artists Against 419	×	×	○	○	
27	CLEAN-MX	×	△	○	○	マルウェア名で分類される．
28	Certly Guard	×	△	×	×	カテゴリの中でフィッシングなどが分類される．
29	hpHosts File	△	△	×	×	カテゴリの中に「hijack sites」という情報を含む．
30	Malware Patrol	×	×	×	×	
31	MalwareURL List	×	△	×	×	マルウェアの種類で分類される．
32	Site Safety Center	×	△	×	×	カテゴリの中でフィッシングなどが分類される．
33	Safe Web	×	△	×	×	カテゴリの中でフィッシングなどが分類される．
34	Web Inspector	×	△	○	○	カテゴリの中でフィッシングやマルウェアの種類などが分類される．
35	VirusDesk	×	△	×	×	悪性と判断した簡単な理由が記載されている．
36	Gred	×	△	×	×	カテゴリの中でフィッシングなどが分類される．
37	SiteCheck	×	×	○	○	
38	MESD blacklists	×	×	×	×	

表 A·2 ユーザ企業の CSIRT におけるインシデント対応判断マニュアルの一例
Table A·2 An example of incident response manual in CSIRT of user company.

コンテンツ	現在の状態	所有者	「トリアージ」における対応（○対応する，△調査結果次第で対応する，－対応しない）	「対応実施」における対応（○対応する，△調査結果次第で対応する，－対応しない）
リダイレクト	現在も悪性・不明	攻撃者	△プロキシサーバーで前後の通信を確認する．関連する通信がある場合はその通信先に対して調査を行い，脅威情報が存在する場合はその分類に従って対応する．	○対応する．
		侵害・不明		△業務利用を確認する．影響が想定されなければ対応する．
		共有型		△トリアージにおける追加調査の結果に従い対応する．
	現在は無害	攻撃者	—対応しない．	○対応する．
		侵害・不明		—対応しない．
		共有型		
エクスプロイト	現在も悪性・不明	攻撃者	△プロキシサーバーで前後の通信を確認する．関連する通信がある場合はその通信先に対して調査を行い，脅威情報が存在する場合はその分類に従って対応する．	○対応する．
		侵害・不明		
		共有型		△トリアージにおける追加調査の結果に従い対応する．
	現在は無害	攻撃者	—対応しない．	○対応する．
		侵害・不明		—対応しない．
		共有型		
悪性ファイル配布	現在も悪性・不明	攻撃者	○対応する．	○対応する．
		侵害・不明		
		共有型	△プロキシサーバーで前後の通信を確認する．関連する通信がある場合はその通信先に対して調査を行い，脅威情報が存在する場合はその分類に従って対応する．	△トリアージにおける追加調査の結果に従い対応する．
	現在は無害	攻撃者	—対応しない．	○対応する．
		侵害・不明		
		共有型		—対応しない．
C2	現在も悪性・不明	攻撃者	○対応する．	○対応する．
		侵害・不明		
		共有型	△脅威情報に対する現時点の追加調査を行う．該当する脅威情報があった場合は対応する．	△トリアージにおける追加調査の結果に従い対応する．
	現在は無害	攻撃者	○対応する．	○対応する．
		侵害・不明		
		共有型	△脅威情報に対する現時点の追加調査を行う．該当する脅威情報があった場合は対応する．	△トリアージにおける追加調査の結果に従い対応する．
ソーシャルエンジニアリング	現在も悪性・不明	攻撃者	△プロキシサーバーで POST 通信の有無などを調査する．情報送信が疑われる場合は対応する．	○対応する．
		侵害・不明		△業務利用を確認する．影響が想定されなければ対応する．
		共有型	△プロキシサーバーで POST 通信の有無などを調査する．可能であればどのような場合に脅威となるか詳細を調査する．情報送信が疑われる場合は対応する．	△トリアージにおける追加調査の結果に従い対応する．
	現在は無害	攻撃者	—対応しない．	○対応する．
		侵害・不明		△業務利用を確認する．影響が想定されなければ対応する．
		共有型		—対応しない．
キルスイッチ	任意	任意	○対応する．	○プロキシサーバー等で通信を確保する．
権威 DNS サーバー	任意	任意	△脅威情報に対する現時点の追加調査を行う．該当する脅威情報があった場合はその分類に従って対応する．	△トリアージにおける追加調査の結果に従い対応する．
DNS シンクホール	任意	任意	△プロキシサーバーで前後の通信を確認する．関連する通信がある場合はその通信先に対して調査を行い，脅威情報が存在する場合はその分類に従って対応する．	○対応する．
正規コンテンツ	任意	任意	△プロキシサーバーで前後の通信を確認する．関連する通信がある場合はその通信先に対して調査を行い，脅威情報が存在する場合はその分類に従って対応する．	△トリアージにおける追加調査の結果に従い対応する．
不明・誤登録	任意	任意	△調査を継続し，個別に判断する．	△トリアージにおける追加調査の結果に従い対応する．

者：不明」「最終確認：2017 年 11 月 9 日 6:35」に分類されている．この悪性ファイルはダウンロードが成功しており端末上で動作している可能性があるため，ユーザを特定してマルウェア感染を調査する．

(2-2) DNS 名前解決要求を IPS で検知したことをトリガにインシデント対応を開始した．この悪性ドメインの分類は「コンテンツ：C2，DNS シンクホール」「現在の状態：現在は無害」「所有者：攻撃者」「最終確認：2017 年 8 月 19 日」であった．また，このサーバに対して 5 分ごとに定期的にアクセスを行い始めた．通信先は現在 C2 としての役割を果たしていないものの，感染端末が潜んでいることが強く疑われたためインシデント対応を開始した．

(2-3) DNS 名前解決要求を IPS で検知したことをトリガにインシデント対応を開始した．この悪性ドメインの分類は「コンテンツ：正規コンテンツ」「現在の状態：現在は無害」「所有者：不明」「最終確認：2016 年 4 月 8 日 19:03」であった．CSIRT 担当者が調べたところ，これはアクセスすると自分の IP アドレスを表示してくれる無害なサイトであった．ところが，前後のプロキシサーバのログを調べてみるといくつかのドメインに対するアクセスが含まれていたため，脅威情報を検索エンジンで調べた．これは C2 であることが分かったため，すでにマルウェアに感染していると考えてインシデント対応を行った．IPS が検知したドメインは通常の用途も考えられこれ自体では悪性といえるものではないが，マルウェアが活動する際に自分の環境を調べるために利用していたサイトであったためブラックリストとして登録されていた．

羽田 大樹 （正会員）

2006 年東京工業大学大学院修士課程修了．同年 NTT コミュニケーションズ株式会社入社．2016 年 NTT セキュリティ・ジャパン株式会社出向，セキュリティログ分析業務に従事．2013 年情報セキュリティ大学院大学修士課程修了．2015 年同大学院博士課程入学．

後藤 厚宏 （正会員）

1984 年東京大学大学院博士課程修了（情報工学博士）．NTT 研究所で並列・分散処理アーキテクチャ，インターネットセキュリティ技術，高信頼クラウドコンピューティグ技術等の研究開発等に従事．2011 年 7 月より情報セキュリティ大学院大学教授．本会フェロー．