様式 1-4-2 (2020-1)

# 令和元年度研究開発成果概要書

採 択 番 号　　：19001
研究開発課題名　：Web 媒介型攻撃対策技術の実用化に向けた研究開発
副　　題　　：Web 媒介型攻撃の網羅的な観測・分析に基づくユーザ環境のセキュリティ高度化

（1）研究開発の目的

Web サイトを改ざんして攻撃サイトを構築し、当該サイトへアクセスしてきた利用者を攻撃する Web 媒介型攻撃が深刻な問題となっている。Web 媒介型攻撃は、Ⅰ)脆弱性攻撃手法・攻撃ツールの開発や流通、Ⅱ)脆弱サイトの探索や攻撃サイトの構築、Ⅲ)攻撃サイトへのエンドユーザの誘導と乗っ取り、といった一連の不正活動から構成されると考えられる。本研究課題では、これらの不正活動を網羅的に観測、分析することによって、攻撃の構造を正確に把握し、攻撃サイト等を効率的に検出することで利用者を保護する技術を確立することを目的とする。

（2）研究開発期間

平成 28 年度から令和 2 年度（5 年間）

（3）実施機関

株式会社 KDDI 総合研究所＜代表研究者＞
株式会社セキュアブレイン
国立大学法人 横浜国立大学
国立大学法人 神戸大学
株式会社構造計画研究所
国立大学法人 金沢大学
国立大学法人 岡山大学

（4）研究開発予算（契約額）

総額 999 百万円（令和元年度 200 百万円）
※百万円未満切り上げ

（5）研究開発項目と担当

研究開発項目 1：新型ブラウザセンサの研究開発
A. 新規 Windows 系ブラウザセンサ開発 (Safari、Chrome 等) （セキュアブレイン）
B. Mac OS 系ブラウザセンサ開発 (Safari、Firefox、Chrome 等) （セキュアブレイン）
C. ブラウザ内分析機能強化（セキュアブレイン）
D. センサアップデート機能開発（セキュアブレイン）

研究開発項目 2：新型観測機構の研究開発
A-1. AI 技術を応用した大規模クローリング機構
（人間-AI 連携型ディープ/ダーク Web クローラ）（神戸大学）
A-2. AI 技術を応用した大規模クローリング機構

（脆弱・改ざん・攻撃サイトクローラ）（横浜国立大学）
B-1. モバイル機器向け観測機構開発
（Android の Web ブラウザを経由しない Web アクセス観測機構）（岡山大学）
B-2. モバイル機器向け観測機構開発(Android SMS センサ)（セキュアブレイン）
C-1. IoT 機器向け観測機構開発(IoT ハニーポット)（横浜国立大学）
C-2. IoT 機器向け観測機構開発(IoT セキュリティゲートウェイ)（セキュアブレイン）
D. DRDoS 攻撃観測機構（横浜国立大学）

研究開発項目３：攻撃情報分析基盤の研究開発
A-1. 基盤内分析機能強化(プラットフォーム構築)（KDDI 総合研究所）
A-2. 基盤内分析機能強化(機械学習技術を応用した分析)（構造計画研究所）
A-3. 基盤内分析機能強化(プライバシを考慮した分析)（金沢大学）
B. Web プロキシログ、DNS クエリログ等との連携機能開発（KDDI 総合研究所）
C. ユーザ環境へのアクティブクローリング機能開発（横浜国立大学）
D. Web サーバ型ハニーポット開発（横浜国立大学）
E. 基盤アップデート機能開発（KDDI 総合研究所）

研究開発項目４：大規模・長期実証実験
A. 1,000 ユーザ規模（KDDI 総合研究所）
B. 10,000 ユーザ規模（KDDI 総合研究所）
C. ユーザのインセンティブ向上に資する研究開発を実施（KDDI 総合研究所）
D. 個人情報保護等の観点から、技術的及び法的な検討を実施（KDDI 総合研究所）

（6）特許出願、外部発表等

| | | 累計（件） | 当該年度（件） |
|---|---|---|---|
| 特許出願 | 国内出願 | 8 | 2 |
| | 外国出願 | 0 | 0 |
| 外部発表等 | 研究論文 | 25 | 10 |
| | その他研究発表 | 230 | 57 |
| | 標準化提案 | 0 | 0 |
| | プレスリリース・報道 | 136 | 26 |
| | 展示会 | 2 | 0 |
| | 受賞・表彰 | 22 | 5 |

（7）具体的な実施内容と成果

<u>研究開発項目１：新型ブラウザセンサの研究開発</u>
<u>A. 新規 Windows 系ブラウザセンサ開発（Safari、Chrome 等）（セキュアブレイン）</u>
現在実証実験において配布している Web ブラウザセンサに対して以下の対応を行った。

- 閲覧履歴情報のプライバシー対応を行った。
- 横浜国立大学の研究課題である危険検索ワード検知についてのブラウザセンサでの実装を行った。

Chrome 自身のアップデートに起因する問題に対して以下の対応を行った。

- 閲覧履歴生成を阻害するアップデートによる影響を回避するための対応を行った。
- 悪性サイト警告画面表示を阻害するアップデートによる影響を回避するための対応を行った。

B. Mac OS 系ブラウザセンサ開発（Safari、Firefox、Chrome 等）（セキュアブレイン）

研究項目 1-A と同様の対応に加えて、MacOS に起因する問題への対応を行った。

C. ブラウザ内分析機能強化（セキュアブレイン）

ブラウザ内分析機能の強化に向け、昨年の調査を元に Web 閲覧履歴からページ URL や遷移タイプ等の特徴量を抽出し、悪性サイトを識別/分類する研究を行った。悪性サイトに実際に接続した場合だけでなく、悪性サイトに遷移する前の段階で検知を行う手法を構築し、ブラウザセンサから収集したデータを利用した検証の結果正答率 0.904、F-measure 0.894 の検知結果を得られた。

D. センサアップデート機能開発（セキュアブレイン）

センサアップデート機能により、実証実験ユーザに対して研究項目 1-A、1-B で行った機能拡充が行われたブラウザセンサへのアップデートを行った。

研究開発項目２：新型観測機構の研究開発

A-1. AI 技術を応用した大規模クローリング機構
（人間-AI 連携型ディープ/ダーク Web クローラ）（神戸大学）

URL およびウェブ閲覧時に実行される JavaScript の悪性判定を行う機械学習モデルを開発した。URL 悪性判定は再現率で 66.7%を達成し、Google Safe Browsing よりも約 60 日早く悪性サイトを発見できた。また、JavaScript 悪性判定は一定レベルの難読化されたコードであっても、再現率で 95.1%の検知精度を達成した。

A-2. AI 技術を応用した大規模クローリング機構
（脆弱・改ざん・攻撃サイトクローラ）（横浜国立大学）

ブラウザセンサ、大規模実運用システム(PhishWall)および、Web 検索エンジンから得られる膨大な検査対象 URL から Web 媒介型攻撃に悪用される恐れのある脆弱サイト、既に脆弱性が攻撃されて改ざんされているサイト、クライアントに対して脆弱性を突いて攻撃をしてくる攻撃サイトを抽出するための方式として前年度までに検討、構築したシステムを用いて悪性 URL や悪性ドメインを抽出し、これらの悪性サイト群をブラックリストとしてブラウザセンサ導入ユーザに配信した際のシミュレーションを行い、その結果から悪性サイト検出手法の改良を行った。また、ブラウザセンサ導入ユーザが悪性サイトに到達するのを未然に防ぐため、危険サイトに誘導される可能性の高い検索ワードを抽出する手法を提案し、その評価を行った。

B-1. モバイル機器向け観測機構開発
（Android の Web ブラウザを経由しない Web アクセス観測機構）（岡山大学）

モバイル機器向け観測機構のうち、Web ブラウザを経由しない Web アクセス観測機構を用いた脅威分析と特定 Web サイトへのアクセスをブロックする手法の実現を行った。脅威分析から、偽警告画面（図１）を表示する Web ページへの遷移を詳細に分析し、遷移の仕組みを明らかにした。

特定 Web サイトへのアクセスをブロックする手法では、WebView における Web アクセスにおいて、ドメイン名や IP アドレスにより Web アクセスをブロックする機構を実現した。さらに、Android における Web ブラウザの URL バーの切り替わり間隔に着目して、利用者の意図しない Web サイトへの遷移を検知する手法（図２）を提案した。提案手法は、利用者の意図しない Web サイトへの遷移が一定時間中に複数回の Web ページの遷移を伴うことに着目し、URL バーの切り替わり間隔と切り替わり

回数を観測することで、端末への導入が容易であり、かつ一定の悪性 Web サイトを検出できることを示した。


**図 1　偽警告画面の例**

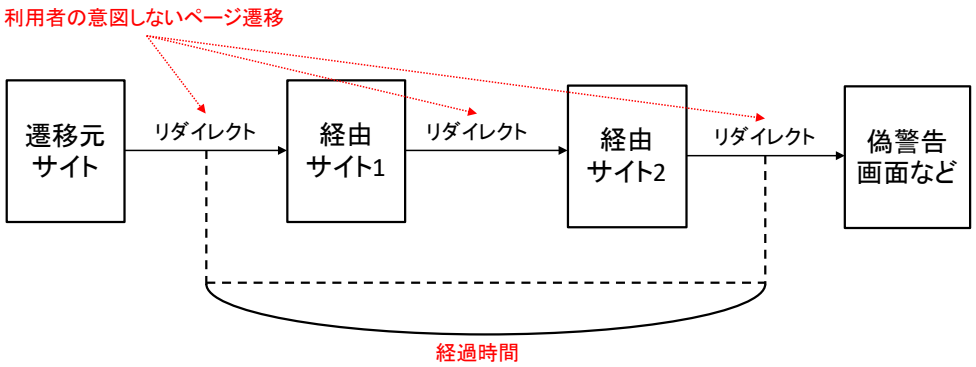


図２　URL バーの遷移間隔に着目した利用者の意図しない Web サイトへの誘導の検知

これらに加えて、観測機構による解析結果を基に、モバイル機器向けの悪性 Web サイトのブラックリスト構築手法（図３）と Web アクセス可視化手法（図４）を提案した。ブラックリスト構築手法では、SNS を起点とした Web サイトの探索により 200 件の遷移元サイト（うち FQDN は 108 件）を発見した。また、Web アクセス可視化手法により、悪性 Web サイトの効率的な解析を補助する仕組みを構築できた。

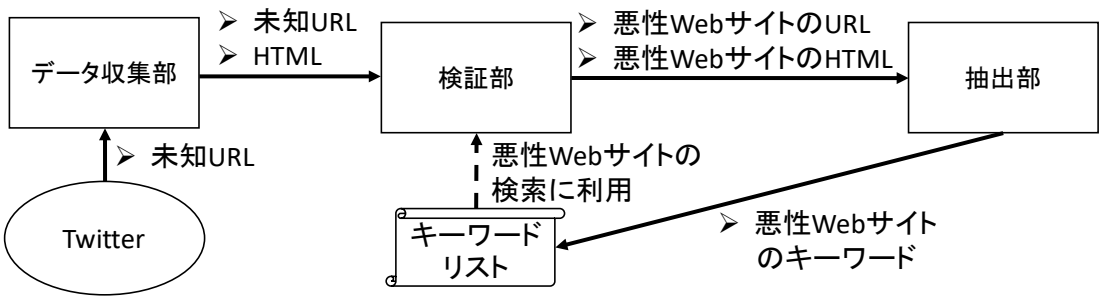


図 3　モバイル機器向けの悪性 Web サイトのブラックリスト構築手法の全体像

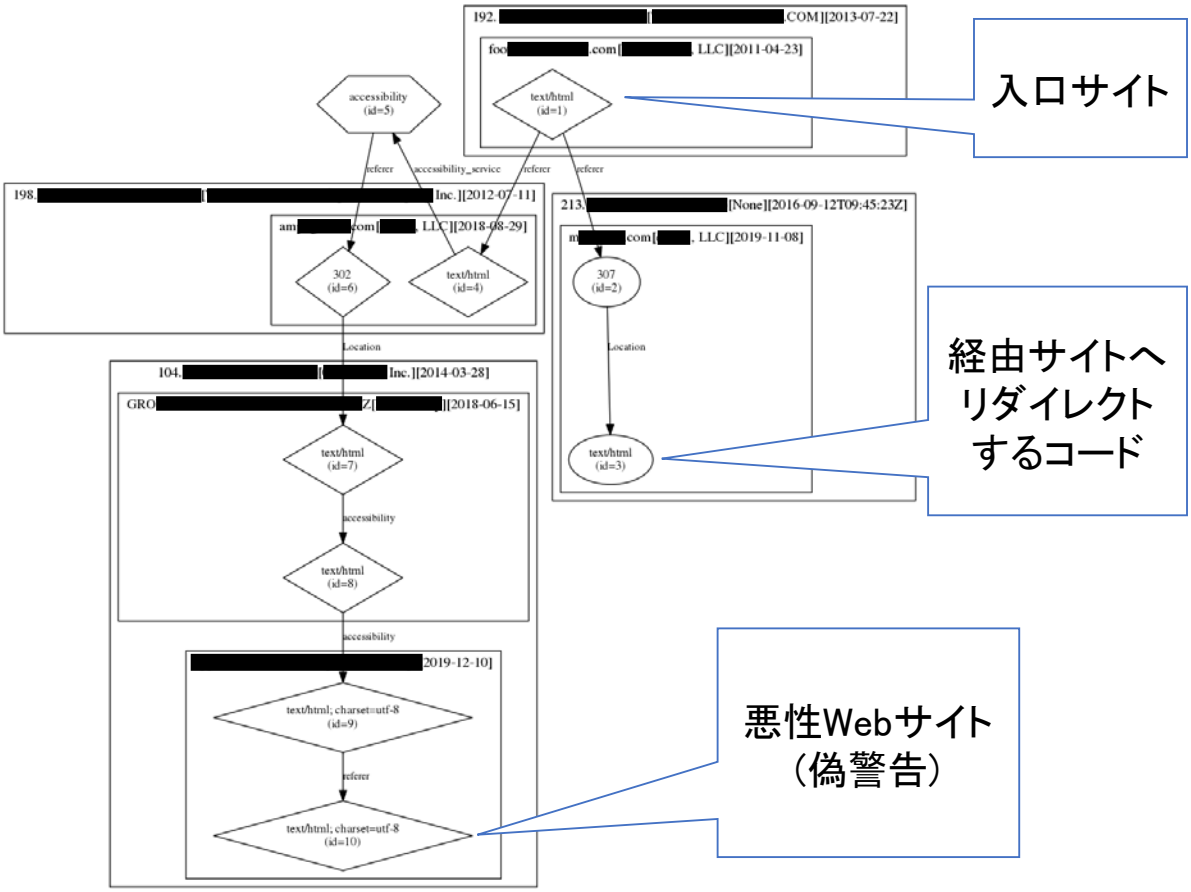


図 4　Android における Web アクセス可視化の例

## B-2. モバイル機器向け観測機構開発(Android SMS センサ)（セキュアブレイン）

実証実験向けモバイルセンサの開発、および、公式ストア以外で配布される Android アプリ（APK）の継続調査を行った。モバイルセンサ開発では、攻撃遭遇の実態把握を目的とする情報収集機能の実装を完了し、令和元年度の実証実験向けに提供を行った。また、次年度の研究に向けて、情報収集項目の拡充と脅威検知機能の実装を開始した。公式ストア外における APK 配布の調査としては、Twitter で情報周知・共有される APK の収集を継続し、ソーシャルネットワーク（SNS）上で情報が共有された APK の配布サイトに関する調査を実施した。また、当該調査で取得した情報を特徴量とする分類器の構築および評価実験を行い、悪質な APK を識別する上で一定の効果があることを確認した。

C-1. IoT 機器向け観測機構開発(IoT ハニーポット)（横浜国立大学）

ルータ、IP カメラ、情報家電をはじめとする IoT 機器の有する管理用の Web インターフェイスに対する攻撃を観測する方式として前年度までに実装・評価を行ったシステムを改良し、様々な IoT 機器の Web インターフェイスからの応答を広域スキャンにより収集し、ハニーポットの応答として適用する機能を追加し、攻撃の観測を行った。

C-2. IoT 機器向け観測機構開発(IoT セキュリティゲートウェイ)（セキュアブレイン）

エンドユーザ LAN 内のセキュリティ向上と健全化に向け、IoT セキュリティゲートウェイに関する下記研究及び社内環境での試験運用を行った。これらにより、IoT セキュリティゲートウェイの実用化のための要素技術の有用性を実証した。

- 昨年度提案した IoT マルウェア駆除手法において明らかになった以下の 3 つの課題について検討した。
    - 擬似 C&C サーバのシステム化
        - 擬似 C&C サーバの基本設計を行なった。仮想環境上で概念実証を行い、IoT マルウェアである mirai，BASHLITE，tsunami 各数検体に対して駆除が可能であることを示した。
    - キルコマンドによらない駆除手法
        - IoT 機器のコマンドを利用した駆除手法及び、マルウェアの脆弱性を突いた駆除手法の２つを検討した。これにより、キルコマンドを持たない IoT マルウェアにおいても駆除できる可能性を示した。
    - IoT マルウェア内から駆除情報等を自動抽出する手法
        - キルコマンドなどの駆除情報等の自動抽出の調査として、公開されている BASHLITE のソースコードを静的解析した。その結果、駆除情報である“LOLNOGTFO”とプロセスの終了を行う exit 関数が近傍に存在していることを確認した。これにより、駆除情報等の自動抽出を行うための方針を示した。
        -
- IoT マルウェアの一つである BASHLITE を対象とした駆除情報等の自動抽出手法を提案した。実験の結果、提案手法を用いて駆除情報の抽出が可能であった検体は 88.9%の駆除率を得た。

IoT セキュリティゲートウェイおよび情報提供サーバの試作・評価を行なった。試験運用では、ARM か MIPS のアーキテクチャを持つ IoT 機器類において複数の IoT マルウェアに対して駆除が可能であることを示した。

D. DRDoS 攻撃観測機構（横浜国立大学）

Web サイトへの DoS(サービス妨害)攻撃の１つである DRDoS 攻撃(反射型分散サービス妨害攻撃)を観測する方式と攻撃対象の Web サイトの分析方法として前年度までに実装を行ったシステムの改良を行い、攻撃対象への攻撃のインパクトを分析する機能拡張を行った。

研究開発項目３：攻撃情報分析基盤の研究開発

A-1. 基盤内分析機能強化(プラットフォーム構築)（KDDI 総合研究所）

- モバイル版実証実験のための機能強化を行った。具体的には、モバイル版のアプリから提供される Web アクセス履歴・アプリ操作履歴・インストールアプリなどの収集データを受信するインターフェースを実装した。また、全文検索エンジン ElasticSearch を用いて収集したデータを検索・閲覧できる仕組みを実装した。
- モバイル版の実証実験のためのサーバ機能を実装した。モバイル版アプリには、セキュリティな

どの質問を定期的に行う機能、ユーザからスパムや悪性サイトの報告を受け付ける機能、ユーザのスマートフォンの利用状況を表示する機能がある。これらの機能のサーバ部分を実装した。
- PC 版の実証実験基盤を用いて、課題 3-C のユーザ環境へのアクティブクローリングの実証実験を行った。

A-2. 基盤内分析機能強化(機械学習技術を応用した分析)（構造計画研究所）

Web ブラウザ拡張によってリダイレクトに関する情報を効率的に収集する方式、および複数のユーザから収集したリダイレクト情報を横断的に分析することによって構造分析する方式を提案した。提案方式は、ブラウザ拡張を用いることによって収集した膨大な Web リクエストおよび関連するブラウジング情報全体から悪性 Web ページアクセスを効率的に抽出し、抽出結果からリダイレクトに関する情報を横断的に構造分析する方式である。分析した結果、「Microsoft を騙った偽警告サイト」「Apple を騙った偽警告サイト」というフィッシング攻撃事例を発見し、リダイレクトによるページ遷移の特徴を確認した。

さらに、複数の Web ブラウザにおいて収集したブラウジング情報を全文検索エンジン ElasticSearch によって分析した。分析した結果、「年間ビジターアンケート」というソーシャルエンジニアリング攻撃事例を発見し、攻撃シグネチャの変化についての観測を行った。

A-3. 基盤内分析機能強化(プライバシを考慮した分析)（金沢大学）

プライバシ評価指標として、どの仮名に対応するデータも少なくとも k ユーザのデータの部分集合となることを保証する、k-包含という概念を定義し、k-包含を満たす分割手法について検討を行うと共に、実データへ適用して評価を行った。また、位置情報を考慮したプライバシリスク分析とそのリスク分析結果に基づいてプライバシ保護データ分析を行うためのデータ匿名化手法の検討を行い、その効果について検証を行った。更に、実データを用いた時系列特性に係わる検討の開始や、プライバシ保護に係わるパーソナルデータ利活用に関するユースケースや法制度との関係などについて考察を行った。

B. Web プロキシログ、DNS クエリログ等との連携機能開発（KDDI 総合研究所）

- Web サイトを構成するリソース情報の統計によるフィッシングサイト検知アルゴリズムの実装評価を行った。フィッシングサイトは、元のサイトを模倣して構成されるため、元のサイトとリソース情報の統計が類似しているという特徴がある。また、フィッシングサイトは、一つのテンプレートから多数のサイトが生成される場合があり、それらのサイトのリソース統計情報が類似している。そこで、Web サイトのリソース統計情報が類似しているサイトをフィッシングサイトとして判定する方式を考案して、実証実験において収集したデータを用いて評価した。この結果、従来報告されていないフィッシングサイトを発見することができた。
- Web サイトのリソース統計情報に基づいてフィッシングサイトを検知する方式について、KDDI 総合研究所の親会社である KDDI 株式会社の社員用の Web プロキシサーバのデータを用いて評価を行った。Web プロキシサーバでは、実証実験のデータに比べて、取得できる情報が少ないため、パラメータチューニングなどを行う必要があることが分かった。

C. ユーザ環境へのアクティブクローリング機能開発（横浜国立大学）

ブラウザセンサのユーザに対して能動的にアクセスを行い、ルータ等のゲートウェイ機器のセキュリティ設定や脆弱性の有無を検査する方式として、前年度までに枠組みの構築・実装を行ったアクティブクローリング機能とブラウザセンサを介したユーザへのクローリング結果の通知を実際に行い、効果を検証した。

D. Web サーバ型ハニーポット開発（横浜国立大学）

脆弱な Web サーバ、および、Web アプリケーションを模した囮システムにより、Web サーバ、Web アプリケーションへの攻撃とコンテンツの改ざんを観測するための方式として前年度までに検討、構築した囮システムを用いて攻撃の観測と検体の収集を行った。また、研究項目２-C の IoT 機器向け観測機構開発で提案した手法を用いて Web サーバや Web アプリケーションの応答を分析し、その結果からシステムの改良を行った。

E. 基盤アップデート機能開発（KDDI 総合研究所）

研究項目 3-A-1 の機能は、基盤アップデート機能を用いて、実証実験の基盤へと追加した。

研究開発項目４：大規模・長期実証実験

A. 1,000 ユーザ規模（KDDI 総合研究所）

PC 版の実証実験を 2018 年の６月に開始し、登録ユーザ数が現在 2020 年３月の時点で 9000 名を超えている。1,000 規模は、2018 年６月に達成している。

B. 10,000 ユーザ規模（KDDI 総合研究所）

モバイル版の実証実験を 2020 年３月 16 日に開始した。2020 年の３月末の段階で、1700 名の登録ユーザを集めており、PC 版のユーザを合わせると合計 10,000 名のユーザを集めた。

C. ユーザのインセンティブ向上に資する研究開発を実施（KDDI 総合研究所）

- ユーザインセンティブとして、アニメ作品である攻殻機動隊 S.A.C.（Stand Alone Complex）と連携して PC 版の Web ブラウザセンサおよびモバイル版のアプリセンサを配布した。
- モバイル版のアプリでは、攻殻機動隊 S.A.C.のキャラクターであるタチコマをホームに表示できるほか、ユーザの貢献度に応じたタチコマのカラーやエモート（あらかじめ登録された特徴的な動作）を提供した。
- 図５にモバイル版センサのユーザインターフェースを示す。モバイル版センサは、ホーム画面にタチコマが常駐する形式として表示される。このタチコマのカラーやエモートが追加されていく。また、悪性サイトに遭遇した場合や、マルウェアのインストールがあった場合には、このキャラクターを通じて警告が伝えられる。


図５　アプリ画面

D. 個人情報保護等の観点から、技術的及び法的な検討を実施（KDDI 総合研究所）

- モバイル版の実証実験の開始にあたって実証実験の計画を策定して、NICT にて設置しているPD（Personal Data）委員会にて審議されて承認を得た。
- モバイル版の実証実験にあたって「実証実験規約」「データ取扱規約」「ソフトウェア利用規約」を策定した。
- データの取扱いでは、収集データのなかに名前やメールアドレスなどの個人情報が混入する恐れがあるため、それらを自動的に削除する個人情報フィルタを実装することとした。
- 収集データにおける URL の取扱いについて、悪性サイト情報として第三者へ提供する場合、第三者セキュリティ監査サービスを利用する場合、Web クローリングする場合に分けて検討を行い、パーソナルデータを保護しながら研究開発ができるバランスのとれた方針を策定した。