CSEC12月研究会 2019/12/4

「CSS2019におけるサイバーセキュリティ研究倫理の取り組み」の振り返り

CSS2019研究倫理委員会

秋山満昭，島岡政基

発表内容

- 「CSS2019におけるサイバーセキュリティ研究倫理の取り組み」（CSS2019表彰式前に発表した内容）の復習

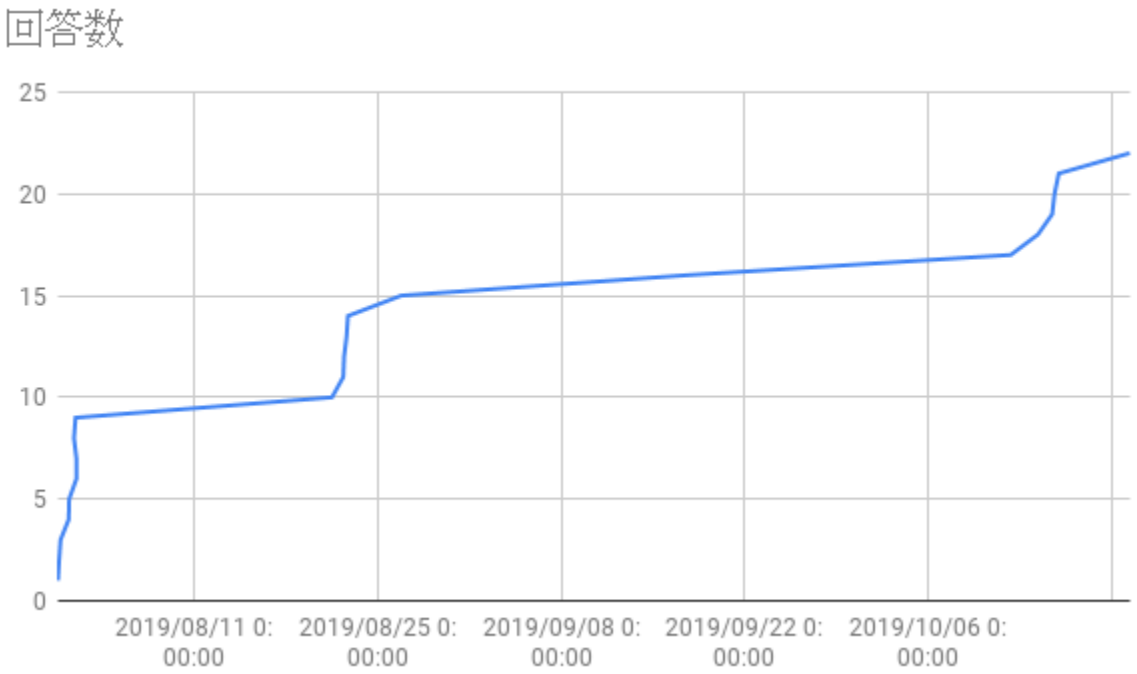
- チェックリストのフィードバック結果

- CSS2019投稿論文で倫理的配慮に関する記述があった論文17件の具体的な紹介

チェックリストのフィードバック

22件の回答

(うち1件は重複回答の可能性あり)



質問項目

(1) 基本的確認

(1-1) 3桁の論文番号を記入してください

(1-2) 情報処理学会の倫理綱領を確認している。

(1-3) 研究・実験に用いた製品やサービスの使用許諾書等に記載されているセキュリティ評価や分析について関連する条項を確認した。

(2) 実験のために収集した機微な情報に関して

(2-1) 個人を特定可能な情報(PII, Personally Identifiable Information)を含む機微な情報の取扱いに配慮したこと、およびその配慮をどのように実施したかについて文中に明記している。

(3) 実験の実施や論文の公開によるネガティブな影響について

(3-1) 事前に(製品名・サービス名や、攻撃対象・攻撃手法などの公開に伴う)ネガティブな影響の検討を行った。

(3-2) 検討結果を踏まえて、関係者への通知(直接通知or届出制度を利用)を事前に行った。

(3-3) 文中に製品・サービスの具体名を表記している、もしくは容易に推測できる記述がある場合、そのように記述することの妥当性を検討した。

(3-4) 上述の“ネガティブな影響”を最小化するための対策について、また論文で取り上げた対象以外に他の製品・サービス等への影響についても検討した。

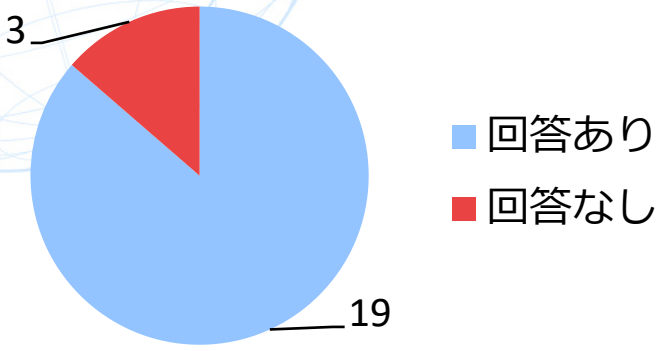
(3-5) (3-1)～(3-4)の検討内容に関して、必要の程度で文中に明記した。

(4) その他回答への補足など

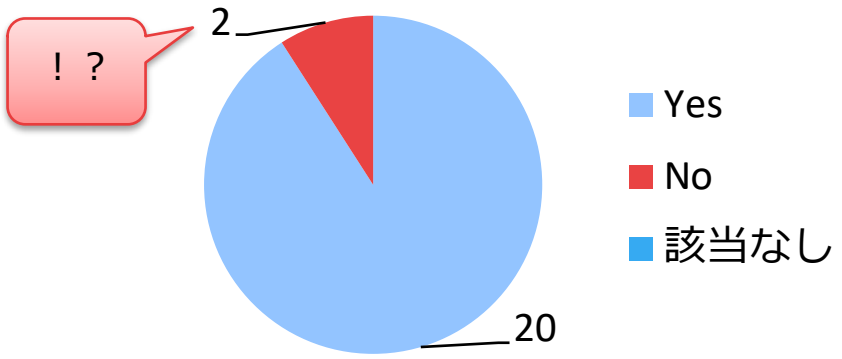
(5) チェックリストへのご意見

(1) 基本的確認

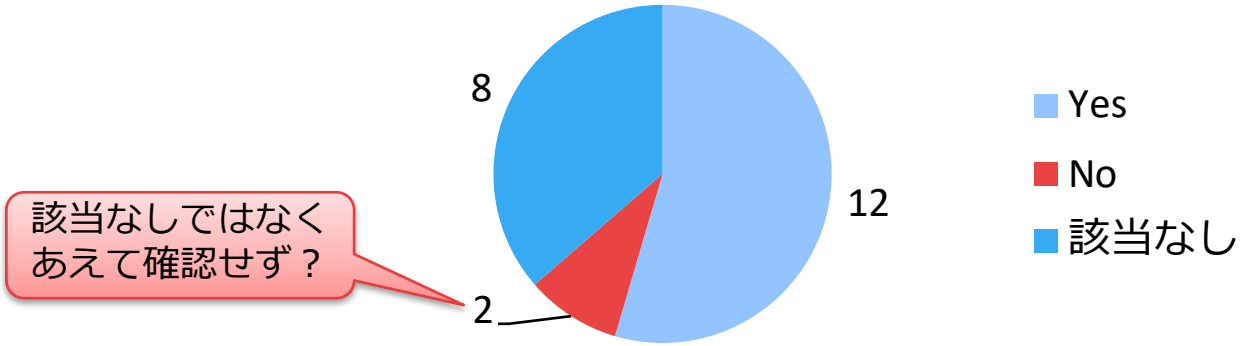
(1-1) 3桁の論文番号を
記入してください



(1-2) 情報処理学会の
倫理綱領を確認している

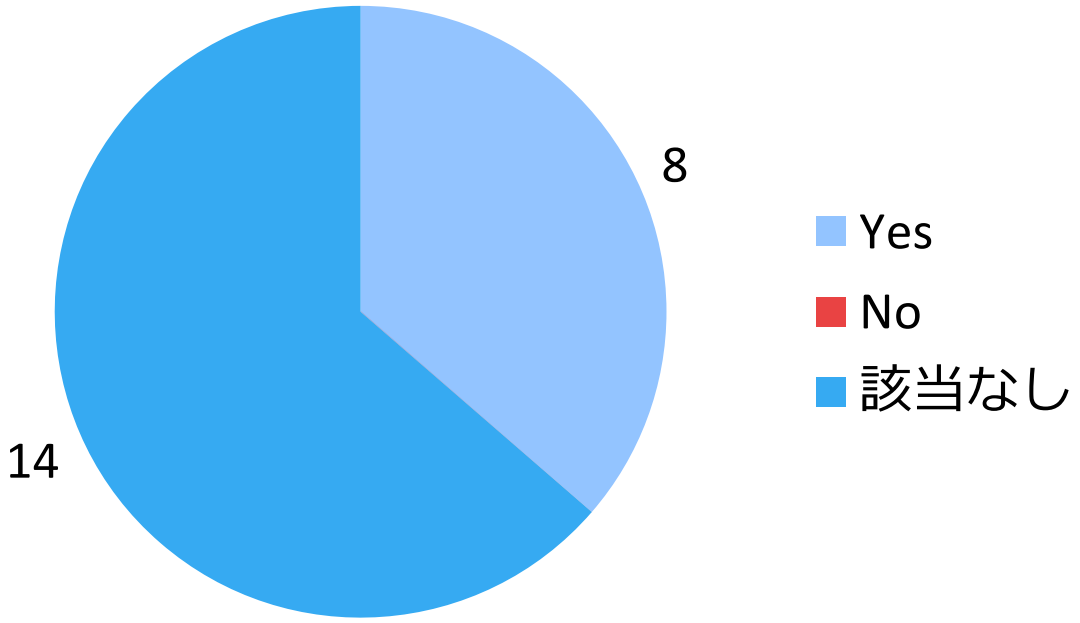


(1-3) 研究・実験に用いた製品やサービスの使用
許諾書等に記載されているセキュリティ評価や
分析について関連する条項を確認した



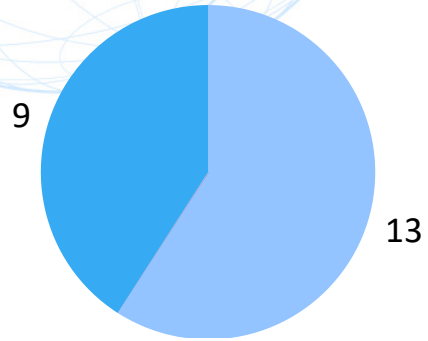
(2) 実験のために収集した機微な情報に関して

(2-1) 個人を特定可能な情報を含む機微な情報の取り扱いに配慮したこと、およびその配慮をどのように実施したかについて、文中に明記している。

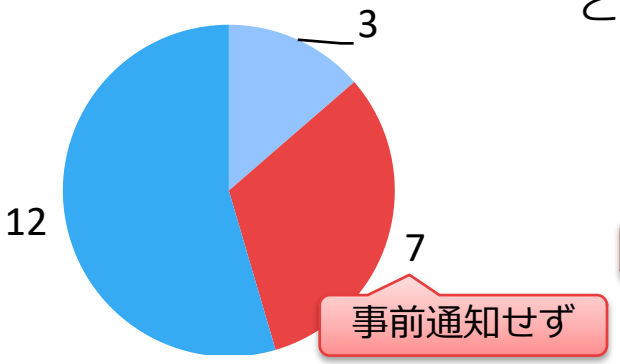


(3) 実験の実施や論文の公開による “ネガティブな影響”について

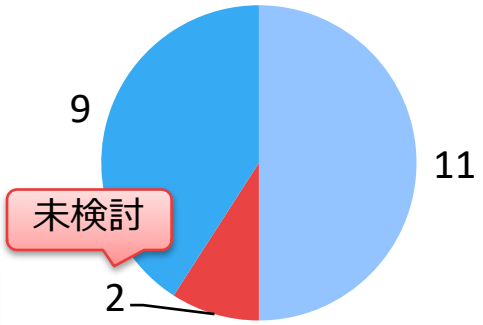
(3-1) 事前に（製品名・サービス名や、攻撃対象・攻撃手法などの公開に伴う）”ネガティブな影響”の検討を行った。



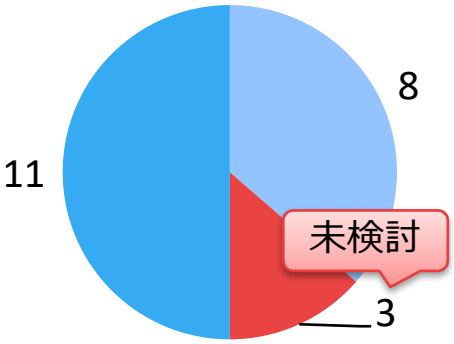
(3-2) 検討結果を踏まえて、関係者への通知（直接通知 or 届出制度を利用）を事前に行った。



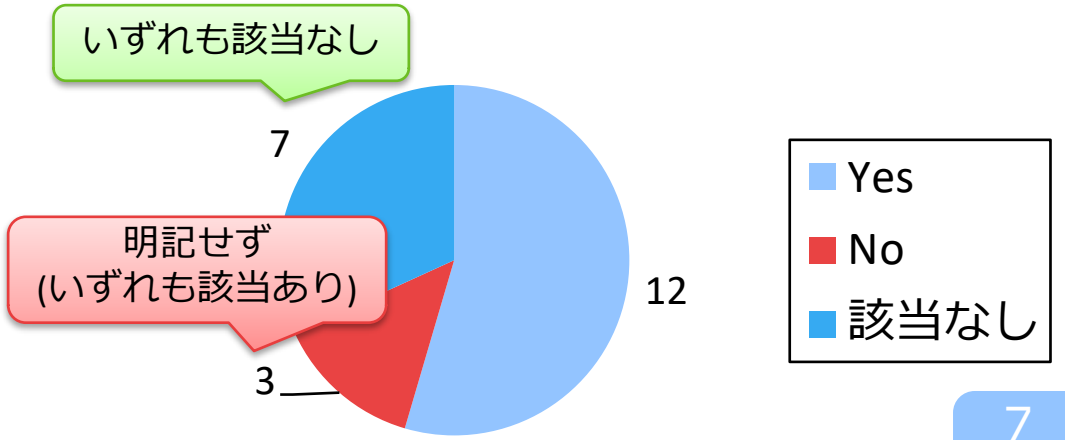
(3-3) 文中に製品・サービスの具体名を表記している、もしくは、容易に推測できる記述がある場合、そのように記述することの妥当性を検討した。



(3-4) 上述の“ネガティブな影響”を最小化するための対策について、また論文で取り上げた対象以外に他の製品・サービス等への影響についても検討した。



(3-5) (3-1)～(3-4)の検討内容に関して、必要の程度で文中に明記した。



(4) その他回答への補足など

- 設問(3-2)に対しての補足です．関係者への通知は開始しておりますが，完全な対応は間に合わないと思われます．研究倫理委員会に相談をさせて頂きます．

  ←結果相談なし (相談期限に間に合わず)

- セキュリティ関連機能の実装有無を確認する調査を実施したが脆弱性に直結するものではないと判断したため，個別製品名の秘匿に留める判断とした

(5) チェックリストへのご意見

- 特になし

フィードバックのまとめ

- チェックリストがほぼ無関係(?)だった回答が3件
  - (1-3)以降すべて該当なし
- 機微情報を扱ったものは8件，いずれも論文で明記済
- ネガティブな影響を扱った論文は15件
  - ネガティブな情報を一通り明記した論文は6件
  - 一部明記しなかった論文は6件
  - 明記しなかった論文は3件

CSS2019投稿論文で倫理的配慮に関する記述があった論文17件の具体的な紹介

- パスワード生成アシスト技術の有効性評価: 異なる言語圏のユーザを対象とした追試研究（早大・NTT）
- Voice Assistant アプリの大規模実態調査（早大・NICT・NTT）
- 単語レベルの言語モデルを用いた悪性 PowerShell の検出（防衛大）
- 深層学習を用いたパッシブフィンガープリンティング手法の 提案と実装（明治大）
- OAuth/OpenIDConnect 実装におけるセキュリティ状況 の調査（明治大）
- ドメインパーキングを利用するドメイン名の大規模実態調査（早大・NTT）
- ハードウェアベース暗号鍵管理に関する日本向け Android プラットフォームの調査（セコム）
- ログイン関連画面に潜む脅威: センシティブサービスにおけるアカウント所有の特定（NTT）
- IoT 機器に対する効率的な広域ネットワークスキャンを実現する ための機器推定用データ作成手法（NTT-AT）
- 金融系ウェブサイトにおける認証画面デザイン分析: デザインメトリクスとユーザ認知（早大・NICT・セコム）
- WebView 搭載 Android アプリケーションにおける ユーザへの Cookie コントロール機能提供状況の調査 (セコム)
- プログラミング言語に対するホモグリフ攻撃の実現可能性評価（早大・JPRS）
- サーバ証明書解析によるフィッシングサイトの発見手法（早大・NTT）
- 悪性 Web サイトに到達しやすい危険検索単語の検知 （横国大・セキュアブレイン・NTT）
- 標的ユーザによる URL アクセスを必要としない インプラントメール攻撃の概念実証（横国大・東大）
- カーネル仮想記憶空間における排他的ページ参照による カーネルの攻撃耐性の実現と評価（岡大・セコム）
- 広域スキャンで収集した応答を用いた 全ポート待受型 Web ハニーポット（横国大）

パスワード生成アシスト技術の有効性評価: 異なる言語圏のユーザを対象とした追試研究（早大・NTT）

- 論文中での研究倫理に関する記載
  - 本調査では参加者に擬似パスワードの生成を依頼し，提出された擬似パスワードを解析をした.
  - 参加者には調査を いつでも辞退できること，収集したデータは研究目的での み使用されること，調査結果が公表される場合でも参加者 のプライバシーに関わる情報は守れられることを事前に説明し，参加への同意を得た.
  - また，疑似パスワード生成に 関して，決して実サービスで使用しているパスワードを使 用しないよう注意喚起を行った.
  - 収集したデータは限られた研究者のみがアクセスできる環境で安全に保管した.具体的には，擬似パスワードは暗号化された状態で保管し，解析段階で復号されたパスワードを参加者と紐づけた状態で目視で確認することはしなかった.

リスクの最小化

インフォームドコンセント

データの管理

Voice Assistant アプリの大規模実態調査（早大・NICT・NTT）

- 論文中での研究倫理に関する記載
  - 本研究の調査の結果判明した，プライバシーリスクの懸念があるVA アプリ及び開発者に関して，個別の実名は公表せず，統計値のみの記述に留めた.
  - 幸い，本研究の調査 では悪性度がきわめて高い VA アプリの発見には至らな かったが，今後調査を継続する課程でそのような悪性 VA アプリを発見した場合は，JPCERT/CC への報告・相談を 進めるとともに，該当するアプリ事業者，Voice Assistant 事業者との相談・調整を進めた上で，適切な方法で情報開 示を行う予定である.

匿名化

Responsible disclosure

単語レベルの言語モデルを用いた悪性PowerShellの検出（防衛大）

- 論文中での研究倫理に関する記載
  - 本研究で使用したgensim，scikit-learn等のモジュールは無償提供されており，コンシューマー用途のコンピュータで使用可能である.また，PowerShellのサンプルの収集はウェブスクレイピングを用いて行ったため，データセットの再現性についても確保できると考える.以上のことから，提案した手法は，一般的なコンピュータでも実装可能であり，再現性が高いといえる.

再現性

深層学習を用いたパッシブフィンガープリンティング手法の 提案と実装（明治大）

- 論文中での研究倫理に関する記載
  - 我々は，Menlo report[3] の精神に則り，倫理的配慮をして実験を行った.
  - 実験を行う際，個人識別はせず，プライバシーを遵守した.
  - 本論文で使用されたデータセットの提供元はデータセットの利用目的を理解している.
  - また，研 究に使用されたデータセットは，学術的な目的にのみ使用 し，我々の研究室にて厳重に保管されており，他者への売 却および提供をしない.

匿名化

インフォームドコンセント

データの管理

OAuth/OpenIDConnect 実装におけるセキュリティ状況 の調査（明治大）

- 論文中での研究倫理に関する記載
  - 本論文では，調査対象のサービスに対して悪影響を及ぼ さないように注意して実験を行った.
  - また，論文を執筆す る際は上位 500 サイト中の特定のサービス名を特定できな いように配慮した.

リスクの最小化

匿名化

ドメインパーキングを利用するドメイン名の大規模実態調査（早大・NTT）

- 論文中での研究倫理に関する記載
  - 我々の研究は，研究倫理の観点で受動的な観測のみを利用し，

リスクの最小化

ハードウェアベース暗号鍵管理に関する日本向け Android プラットフォームの調査（セコム）

- 論文中での研究倫理に関する記載
  - 本稿では 3 章で述べた目的を達成するため，市販されるデバイス実機に対する調査ならびにアプリの静的解析を行った.
  - 研究倫理への対応として，コンピュータセキュリティシンポジウム(CSS)2019 の「サイバーセキュリティ 研究における倫理的配慮のためのチェックリスト [17]」を 利用した.
  - 本稿の各調査における細かな倫理的配慮事項 は，下記の通りである.
    - デバイス調査に関する倫理的配慮：今回の調査で対象とした市販デバイスに関して，調査対象群の網羅性を示す観点からデバイスメーカの具体名を表 3 にて示している.個別のデバイスの調査結果(対応状況) に関しては，特に非対応機種への不利益を最小化する観点 から本稿での記載は行っていない.また，結果の記載では 個別の機種の判別に至らぬよう機種数のみを示す形式を採 用した.
    - アプリ調査に関する倫理的配慮：アプリ調査では，文献 [11] と同様の倫理的配慮を行った.

ガイドライン等の遵守

匿名化

利用規約の遵守

ログイン関連画面に潜む脅威: センシティブサービスにおけるアカウント所有の特定（NTT）

- 論文中での研究倫理に関する記載
  - 実態調査では，実サービスへの負荷を低減するために，ログイン試行回数を最小限に抑えるよう注意深く評価プロ セスを設計した.また，我々が用意した調査専用メールアドレスおよびアカウントのみを利用したため，一般ユーザ がこの調査に関わることは一切なかった.
  - ユーザ調査は所属組織の承認を得て実施した.
  - 本研究で扱った各種ログイン関連メッセージの欠陥は，個別のソフトウェアの脆弱性でなく，サービス全般の設計 に起因する問題である.このため，個別の事業者に対する 通知よりも，本研究で明らかにした問題と対策方法をアプリケーション設計のガイドライン等に追記して広く世の中 に普及させることが効果的だと考えた.よって本研究内容 をIPA，JPCERT/CC，OWASP に情報共有し，これまで に OWASP が発行するアプリケーション設計のガイドライ ンである ASVS [7] および Authentication Cheat Sheet [8] に問題提起と対策方法を追記して改定することに貢献し た.さらに IPA の“安全なウェブサイトの作り方”について も改定の追加項目の一つとして調整を進めている.

リスクの最小化

IRB承認

Responsible disclosure

IoT 機器に対する効率的な広域ネットワークスキャンを実現する ための機器推定用データ作成手法（NTT-AT）

- 論文中での研究倫理に関する記載
  - 本研究では，日本国内の IoT 機器のセキュリティ状況について網羅的な調査を行うための広域ネットワークスキャ ンを実施しているが，実施の目的および調査に使用する IP アドレス等については弊社のニュースリリースにて公開の 上，実施している(https://www.ntt-at.co.jp). 本ニュースリリ ースや whois 情報に連絡先情報を記して，スキャン対象先 等からの問い合わせには適切に対応するとともに，対象除 外の申請があった場合は確実に除外設定を行っている.
  - また，スキャン対象とする IP アドレスをランダマイズ化・分 散化することにより，対象先ネットワークにおいて本スキ ャンによる負荷を低減するよう調整している.
  - 本スキャンにおいては IoT 機器から得られるバナー等の情報を蓄積・活用するが，それらの情報については必要な セキュリティ管理を行い，漏洩等が起こらないようにして いる.
  - 弊社が実施するスキャンでは，IoT機器等からの返 答パケットの確認まで行うが，その後のログインその他のアクセスは実施しない.

インフォームドコンセント

リスクの最小化

データの管理

金融系ウェブサイトにおける認証画面デザイン分析: デザインメトリクスとユーザ認知（早大・NICT・セコム）

- 論文中での研究倫理に関する記載
  - 本研究におけるユーザスタディでは，早稲田大学が設置する研究倫理オフィスが定める「人を対象とする研究に関 する倫理規程」および同オフィスが提供するフローチャー トに則り，実験参加者に一切の不利益が生じることがないよう，慎重に実験を設計した.
  - 具体的には，実験参加は強 制ではなく任意であること，参加者あたりの負荷や謝金の バランスを適切なものとしたこと，
  - そして実験は匿名で行い，個人情報を一切収集しないことを遵守した.

IRB承認

インフォームドコンセント

匿名化

WebView 搭載 Android アプリケーションにおける ユーザへの Cookie コントロール機能提供状況の調査（セコム）

- 論文中での研究倫理に関する記載
  - 本稿では 2.4 節で述べた目的を達成するため，クローリングによるアプリの取得，アプリの静的解析，アプリの動 的解析を行った.
  - 研究倫理への対応として本稿では，コン ピュータセキュリティシンポジウム(CSS)2019 の「サイ バーセキュリティ研究における倫理的配慮のためのチェッ クリスト [22]」を活用した.
  - また，本稿は提出前に社内審 査によって，記載内容に法的・倫理的問題がないかの審査 を実施している.本稿の各調査における細かな倫理的配慮事項は，下記の通りである.
  - アプリ取得時の倫理的配慮：本稿の Android アプリ取得は，Google 社が運営するGoogle Play に対して行った.Google Play に過度な負荷 をかけないよう，アプリのダウンロードリクエストは，最低 でも 1 分の間隔を開け実行した.本調査中に Google Play への接続が遮断されるようなことは起こっていない.
  - 静的解析時の倫理的配慮：静的解析においてアプリのデコンパイル(リバース・エ ンジニアリング)を行った.2019 年 1 月 1 日に改正された 著作権法の一部を改正する法律 [23] では，「プログラムの 調査解析を目的としてプログラムの著作物を利用する行為 (いわゆる「リバース・エンジニアリング」)」は認められているか，アプリの説明欄に明示的に「リバース・エンジニ アリング禁止」等の文言がある場合，当該アプリの解析は 行っていない.
  - 動的解析時の倫理的配慮：動的解析においては，アプリの改変は行わず，Cookie の 挙動を観測している.

ガイドライン等の遵守

リスクの最小化

利用規約の遵守

ログラミング言語に対するホモグリフ攻撃の実現可能性評価（早大・JPRS）

- 論文中での研究倫理に関する記載
  - 本研究におけるユーザスタディでは，早稲田大学が設置する研究倫理オフィスが定める「人を対象とする研究に関 する倫理規程」および同オフィスが提供するフローチャー トに則り，実験参加者に一切の不利益が生じることがない よう，慎重に実験を設計した.具体的には，実験参加は強 制ではなく任意であること，参加者に対する負荷をかけな いように時間制限を設けたこと，そして実験は匿名で行い， 個人情報を一切収集しないことを遵守した.
  - また，本研究で考察した新たな攻撃ベクトルは特定のアルゴリズムやシステムの脆弱性が対象となるものではなく，ホモグリフの悪用に起因する一般的な攻撃である.また，現時点において，プログラミング言語に対するホモグ リフ攻撃は，脅威が顕在化した攻撃ではない.プログラミ ング言語を対象としたホモグリフ攻撃のリスクや対策を広 く公開することにより，脅威が顕在化する前に対策を確立 する利点が見込まれる.以上の洞察に基づき，本研究の発 表は公益性にかなうものであると考える.

IRB承認

インフォームドコンセント

匿名化

公益性

サーバ証明書解析によるフィッシングサイトの発見手法（早大・NTT）

- 論文中での研究倫理に関する記載
  - 発見した証明書を詳細に調査すると，これらの証 明書はあるアンダーグラウンド企業が販売するフィッシングサイト生成サービスにより発行された可能性が非常に高 いことが分かった. Web 上で検索することでその企業名は 判明するが，研究倫理の観点からその実名は本論文では伏せる.

匿名化

悪性 Web サイトに到達しやすい危険検索単語の検知 （横国大・セキュアブレイン・NTT）

- 論文中での研究倫理に関する記載
  - 本稿において検索単語として挙げられた一部の固有名詞はマスクしている.これは特定の企業名や商標が含まれて おりそれらは攻撃の主体ではないこと，検索回数が少ない 検索単語からユーザが特定される危険を考慮したためで ある.また，Web ログ中の URL にはクエリパラメータ中 に個人情報が含まれているケースがあるため外部サービス にクエリパラメータが直接含まれる URL を公開しないように留意した.

匿名化

標的ユーザによる URL アクセスを必要としないインプラントメール攻撃の概念実証（横国大・東大）

- 論文中での研究倫理に関する記載
  - 本研究は，標的マシンでのみ動作するマルウェアに対するセキュリティの向上を目的としている.
  - したがって，本 研究成果をサンドボックスオペレータやセキュリティベン ダに正確かつ詳細に伝えると共に，攻撃者に悪用される恐 れを減らすために，以下のような方策をとることを予定し ている.
  - まず，本研究成果による直接的な影響があると予 想される，実験にて画像キャッシュのファイルサイズが一 定であることが分かった web ブラウザのデベロッパ 2 社 と，受信メール情報内のメールアドレスが暗号化されてい ないことが分かったメーラのデベロッパ 1 社に対して，画像キャッシュや受信メール情報を利用することで標的マシ ンが判別される恐れがある点を指摘し，対策方法の情報提供を行う.次に，サンドボックスアプライアンスを研究開 発しているセキュリティベンダ計 14 社に対して情報提供 を行う このように，本研究はセキュリティアプライアンス の性能向上に貢献すると考えられる.

Responsible disclosure

カーネル仮想記憶空間における排他的ページ参照による カーネルの攻撃耐性の実現と評価（岡大・セコム）

- 論文中での研究倫理に関する記載
  - 本稿の研究について，コンピュータセキュリティシンポ ジウム 2019 サイバーセキュリティ研究における倫理的配 慮のためのチェックリスト [6] に基づき，情報処理学会 倫 理綱領の準拠 [7]，ならびにチェックリストのいずれの項目 にも該当しないことを確認した.

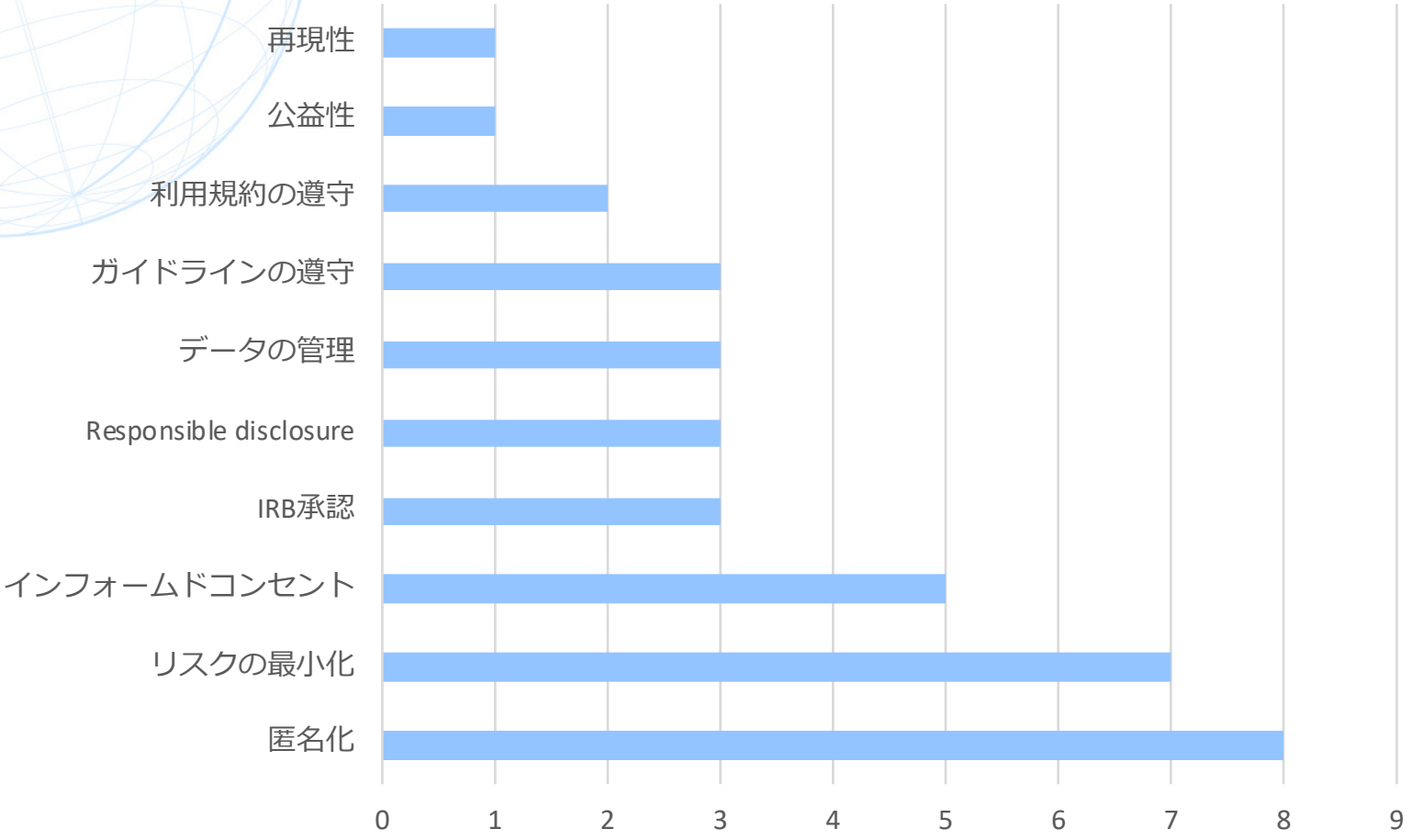
ガイドライン等の遵守

広域スキャンで収集した応答を用いた 全ポート待受型 Web ハニーポット（横国大）

- 論文中での研究倫理に関する記載
  - 本研究では，観測した攻撃情報をもとにインターネット 上に存在するホストに対してネットワークスキャンを行っ ている.そのため，送信される HTTP リクエストが外部 への攻撃となる可能性がある.また，広範囲にネットワー クスキャンを行うため，スキャン先のネットワークに負荷 をかけてしまう可能性がある.そこで，本研究では以下の 対策を行なっている.
  - （1）HTTP リクエストについて：ハニーポットで観測した攻撃情報をもとにホストに対 してスキャンを行っているが，送信されるHTTPリクエストによっては外部への攻撃となってしまう可能 性がある.そこで，ログイン試行やエクスプロイトが 含まれる可能性があるクエリ文字列を取り除き，リク エストヘッダ，データ部を自作している.また，送信 する HTTP リクエストは手動で確認し，不正なリク エストとならないことを確かめている.
  - （2）ネットワークスキャンの影響について：広範囲にネットワークスキャンを行うため，スキャン 先ネットワークによっては帯域を圧迫してしまう可能 性がある.そこで，スキャンレートを 10,000pps 程度 に抑え，スキャンに使用するサーバの IP アドレスを 固定し，スキャンを行なっている旨やその目的，また，連絡先を明記した Web サーバをたてることで，連絡 があった際に，特定のネットワークをスキャン対象か ら外すことができるようにしている.

リスクの最小化

記述のまとめ


再現性
公益性
利用規約の遵守
ガイドラインの遵守
データの管理
Responsible disclosure
IRB承認
インフォームドコンセント
リスクの最小化
匿名化
0
1
2
3
4
5
6
7
8
9
言及されている論文数

まとめ&考察

- CSSにおいて倫理的配慮について言及する論文が増加している（昨年９件→今年17件）
- チェックリストを活用したことを明示的に言及する論文が３件あった
  - チェックリストが研究コミュニティにおけるある種の行動指針になりうる可能性
  - 相談窓口への問い合わせについても言及してもらってもいいのではないか？
    - IRBのような”承認”とまではいかないが、相談窓口では専門家によるレビューとアドバイスを著者に提示しているため、それを実践している場合は倫理的配慮に関する一定の説明にはなるのではないか