NTT

SCIS2019企画セッション
プライバシー脅威「Silhouette」への対応を振り返って

2019年1月24日

NTTセキュアプラットフォーム研究所

秋山 満昭、渡邉 卓弥

サイバーセキュリティ攻撃研究

Innovative R&D by NTT

- 攻撃者の視点に立った研究
  - 日々高度化するサイバー攻撃を防ぐためには、常に最先端の攻撃手法を研究し、攻撃者の先手を取る必要がある
  - 実在するサービスやソフトウェアに潜む脆弱性の発見技術、脅威の有無の判定技術、対策技術など
- われわれの研究グループでの攻撃研究
  - 重要度が増すウェブプライバシーなどの幅広い分野で実施
  - 自社グループ内のサービス評価やコンサルティングに活用
  - 研究成果の対外発表・特許化によるプレゼンスの向上

サイバーセキュリティ分野の攻撃研究は実世界への影響が生じるため成果の取扱いには注意が必要

NTT

本日の内容

Innovative R&D by NTT

- 新たなプライバシー脅威「Silhouette（シルエット）」について
- 脅威の Responsible disclosure
- 知見と議論

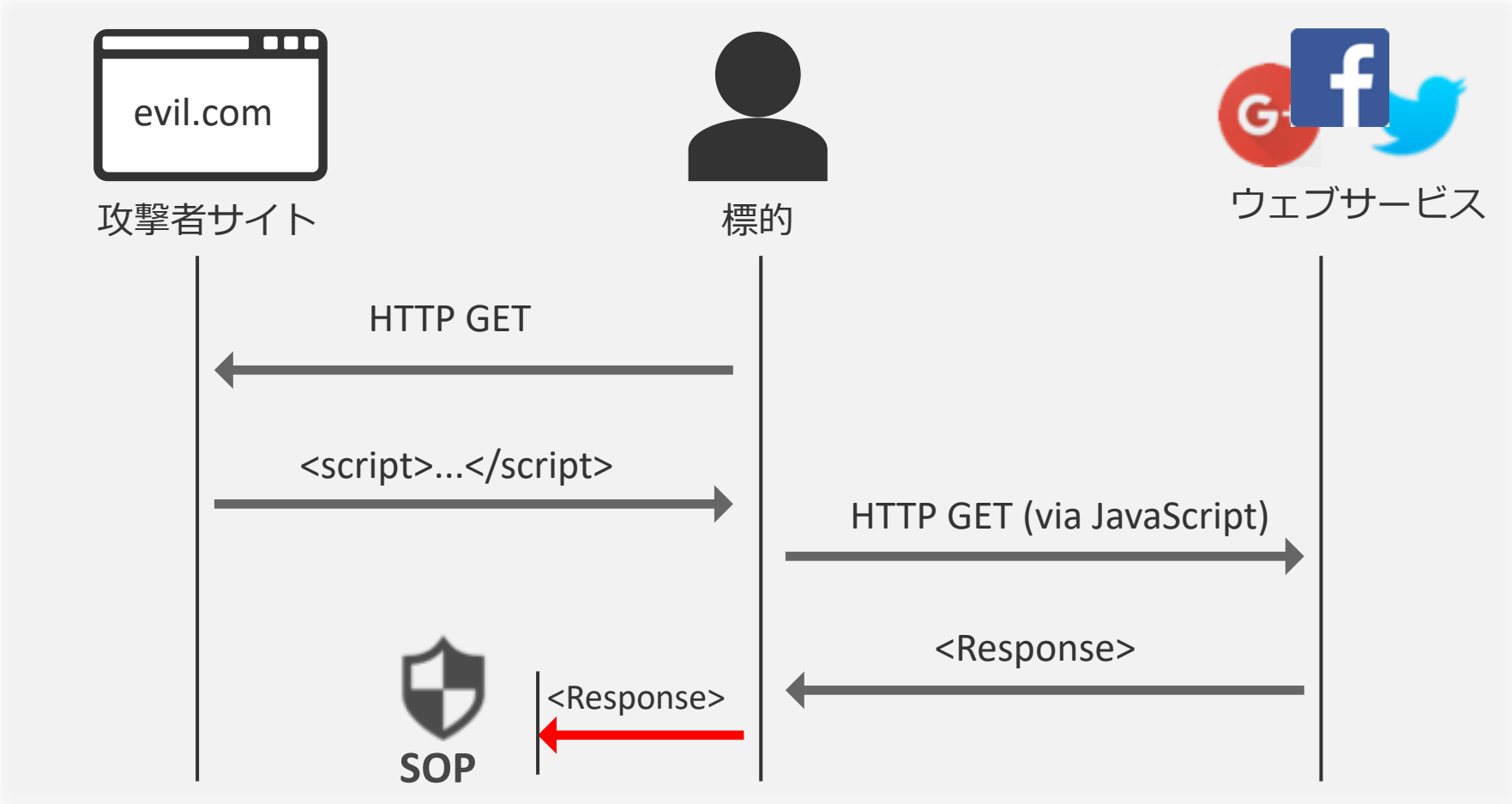
NTT

Silhouette（シルエット）

- ウェブユーザに意図しない通信を送信させるCSRFとレスポンスを通信所要時間から推測するタイミング攻撃を組み合わせた攻撃
- アカウントを一意に識別するためユーザブロック機能を悪用
- 攻撃者が用意したサイトに訪れたユーザのソーシャルサービスのアカウント名が特定されてしまうプライバシー脅威（深刻な被害）
- 特定のサービスに影響せず、世界的に著名なサービスを含む多くのサービスが影響を受ける（広大な影響範囲）

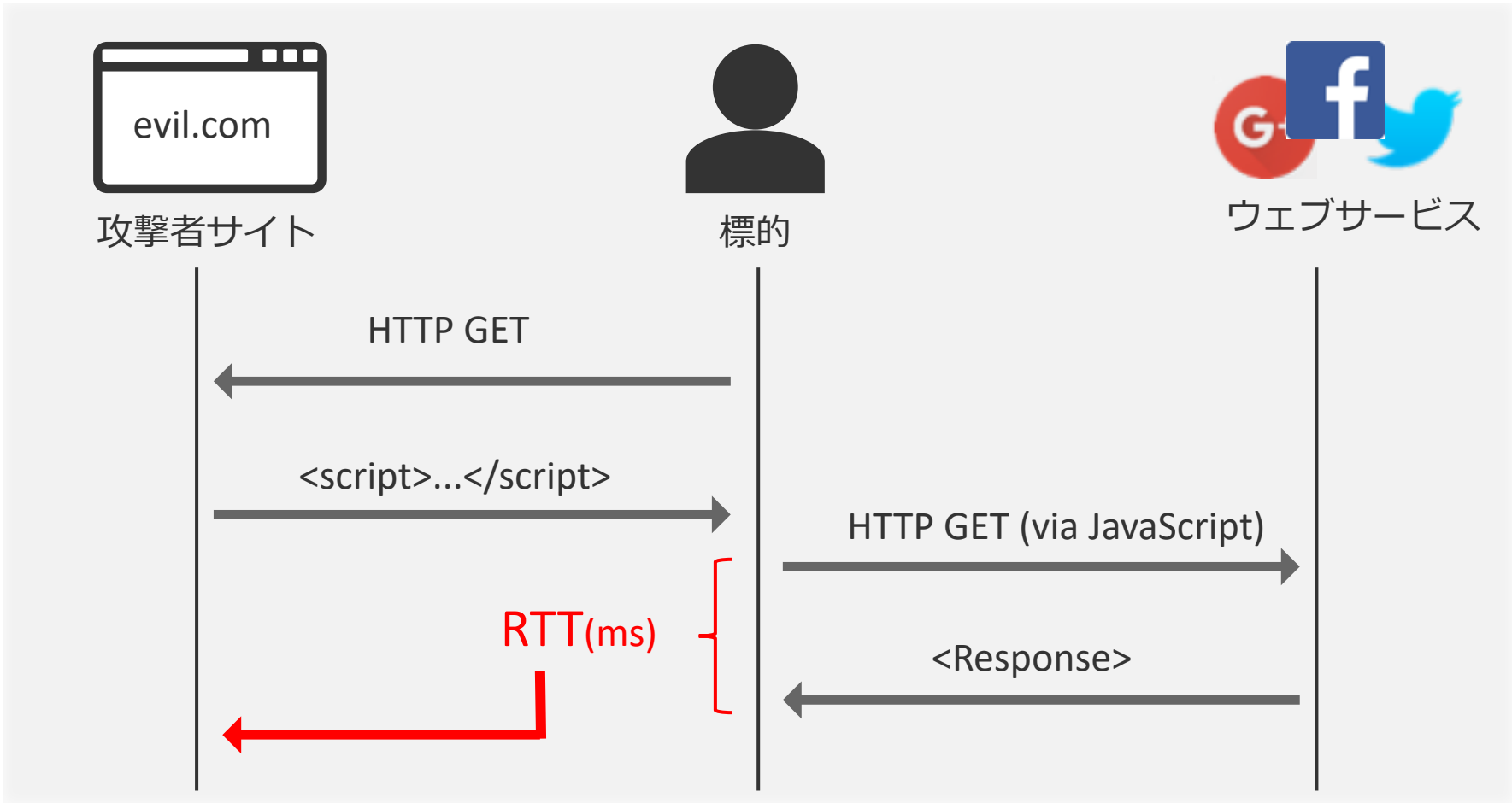
Watanabe et al., User Blocking Considered Harmful? An Attacker-controllable Side Channel to Identify Social Accounts, IEEE EuroS&P'18.

Webセキュリティの大前提:
Same Origin Policy による防御機構



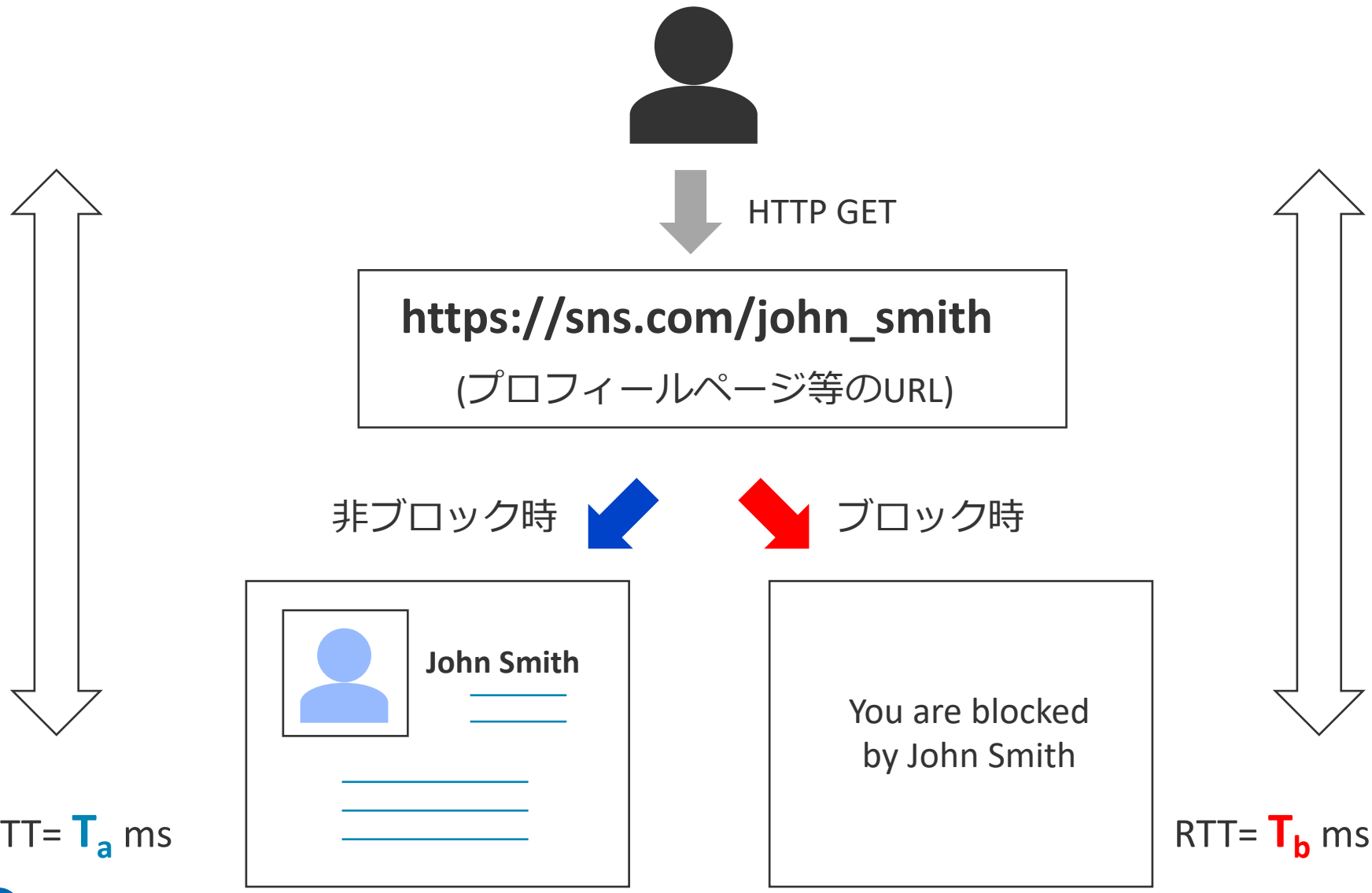
外部サイトとの通信内容はSOPによって保護される
→アカウントIDなどを覗き見ることは通常不可能

Webセキュリティの大前提:
Same Origin Policy による防御機構

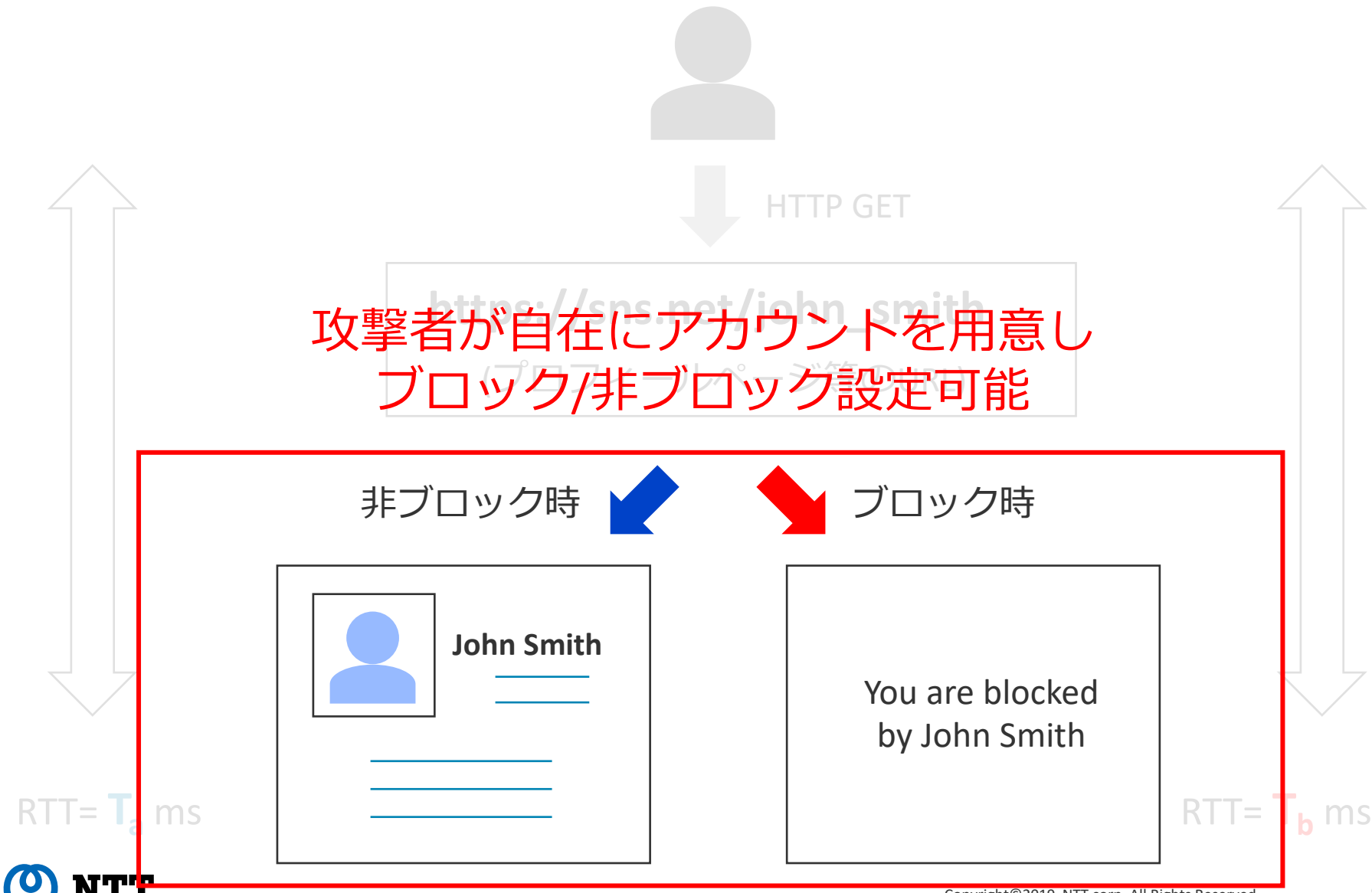


外部サイトとの通信所要時間(≒RTT)は計測可能

Key Idea: ユーザブロック機能



Key Idea: ユーザブロック機能



サイドチャネル制御フェーズ
(攻撃者があらかじめ準備するフェーズ)

ステップ1: ターゲット列挙

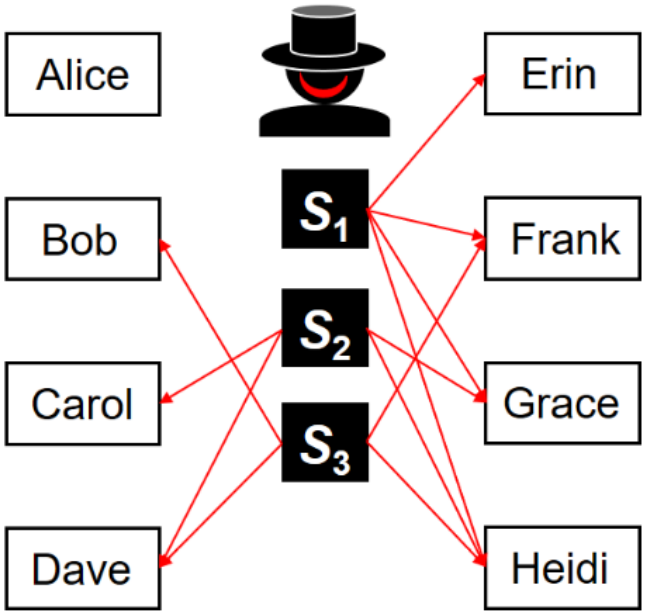
(攻撃者が作ったアカウント)

ソーシャルウェブサービス

ターゲットアカウント	ビット列	シグナルアカウント		
		S_1	S_2	S_3
Alice	000	✅	✅	✅
Bob	001	✅	✅	⛔
Carol	010	✅	⛔	✅
Dave	011	✅	⛔	⛔
Erin	100	⛔	✅	✅
Frank	101	⛔	✅	⛔
Grace	110	⛔	⛔	✅
Heidi	111	⛔	⛔	⛔

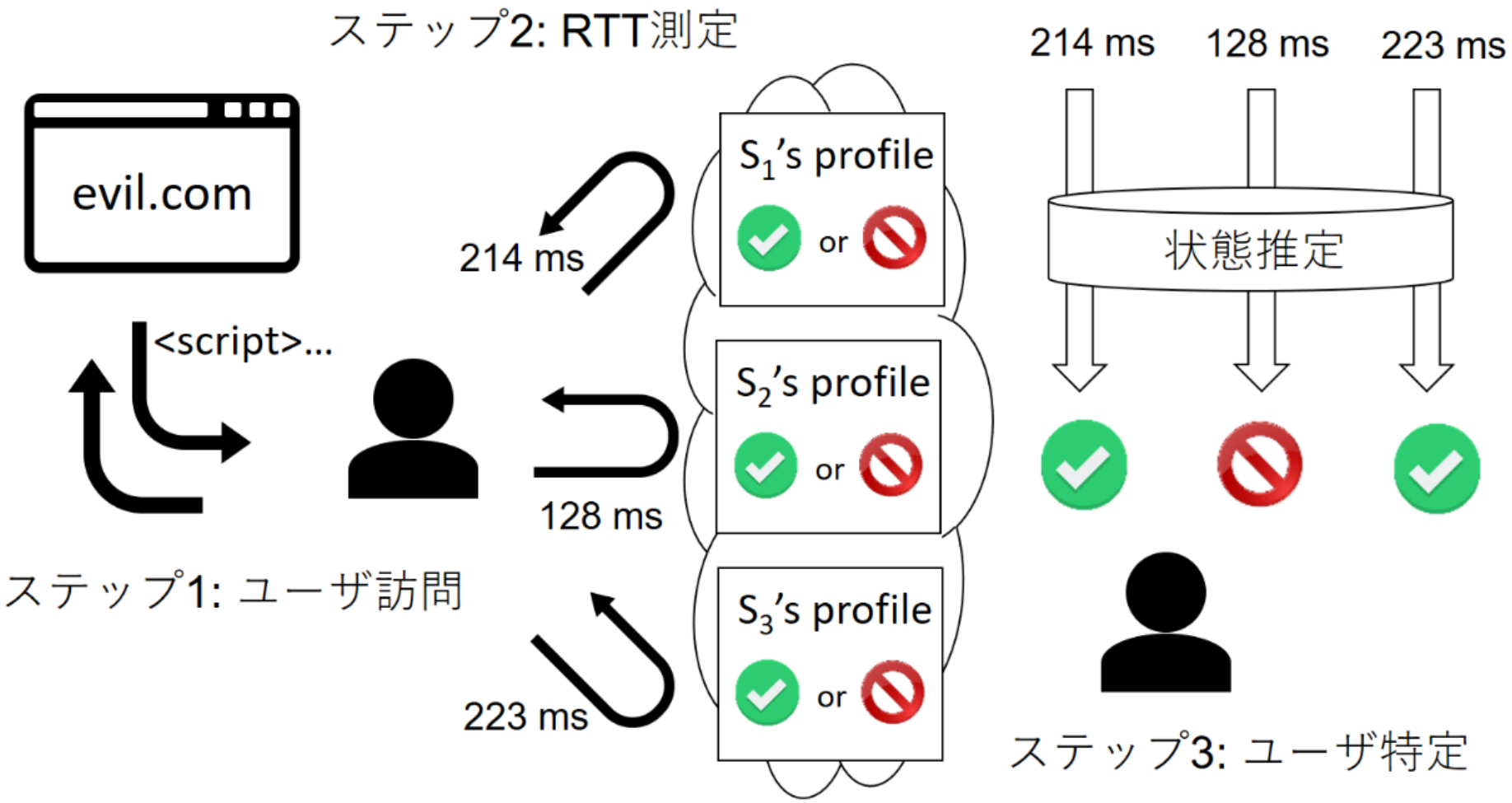
ステップ2: ビット割当

✅非ブロック / ⛔ブロック



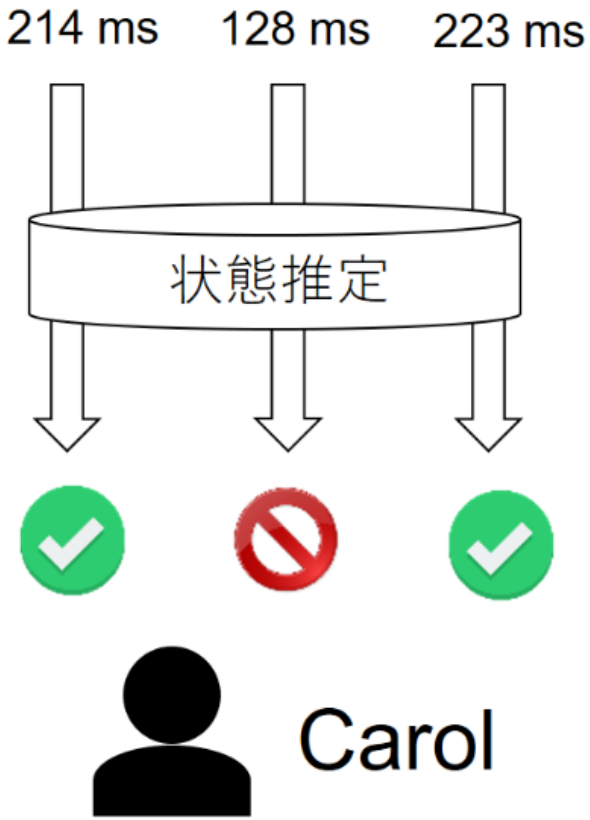
ステップ3: ユーザブロック実行

サイドチャネル復元フェーズ
(ユーザが訪問してきた時に実行するフェーズ)



サイドチャネル復元フェーズ
(ユーザが訪問してきた時に実行するフェーズ)

ターゲットアカウント	ビット列	シグナルアカウント		
		S_1	S_2	S_3
Alice	000	✓	✓	✓
Bob	001	✓	✓	✗
Carol	010	✓	✗	✓
Dave	011	✓	✗	✗
Erin	100	✗	✓	✓
Frank	101	✗	✓	✗
Grace	110	✗	✗	✓
Heidi	111	✗	✗	✗



ステップ3: ユーザ特定

Silhouetteへの対策

- ウェブサービス
  - **アクセス正当性の検証** ←実際に導入
  - 処理時間の制御・ランダマイズ
  - ブロック機能の撤廃
- ブラウザ
  - **アクセス正当性の検証** ←実際に導入
  - 処理時間の制御・ランダマイズ
  - サードパーティCookieの禁止
- ユーザ
  - NoScript
  - プライベートモード
  - ログアウト
- いずれも利便性やパフォーマンス面のトレードオフ

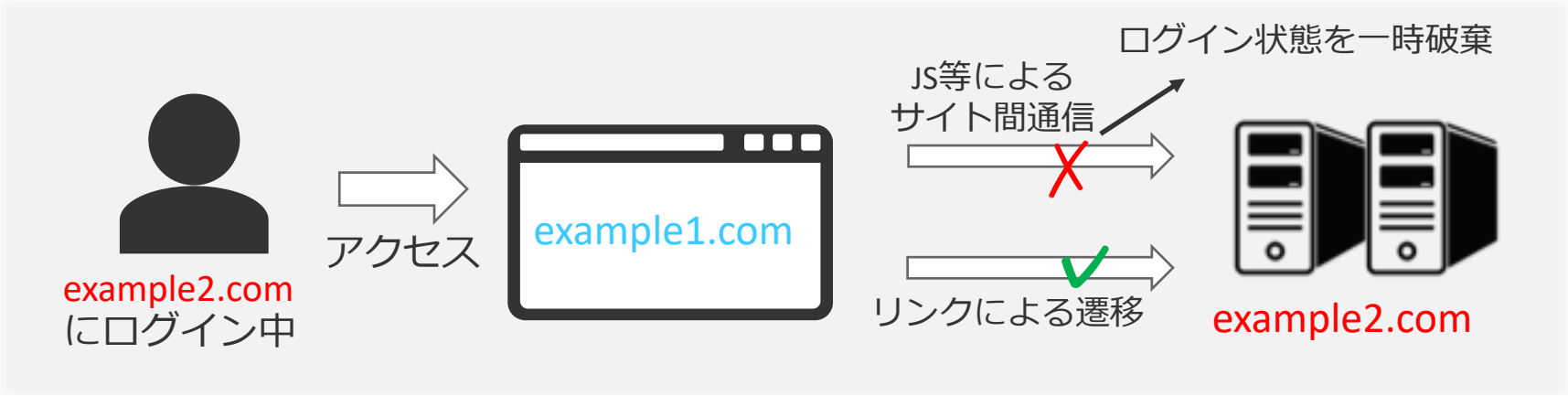
典型的なCSRF対策と問題点

- RefererやCSRF Tokenの検証によって不正リクエストを弾く
  → 「掲示板への書き込み」のような不正リクエストの対策に有効

- 問題点: 本攻撃のCSRF先はプロフィールページ等である
  → 検索エンジンやブログからのリンクまで遮断してしまうと困る

SameSite属性による対策

- サイトをまたぐ通信においてCookieの送信を止めるオプション



- サービス側はSameSite属性をHTTPヘッダで宣言するだけ

```
Set-Cookie: sid=xxxx; path=/; samesite=lax
```

※ samesite=strictを指定するとリンクによる遷移でも破棄する

- 当初はChromium系ブラウザのみで利用可能
  →ブラウザベンダを巻き込んで対策を推進

次善の策: クッションページ

- あるサービスではSameSite対応までに「つなぎ」の対策が導入された
  - CCS'15で紹介された*Placeholder*という対策とほとんど同じ

  "The Clock is Still Ticking: Timing Attacks in the Modern Web"
  Goethem et al. 参照

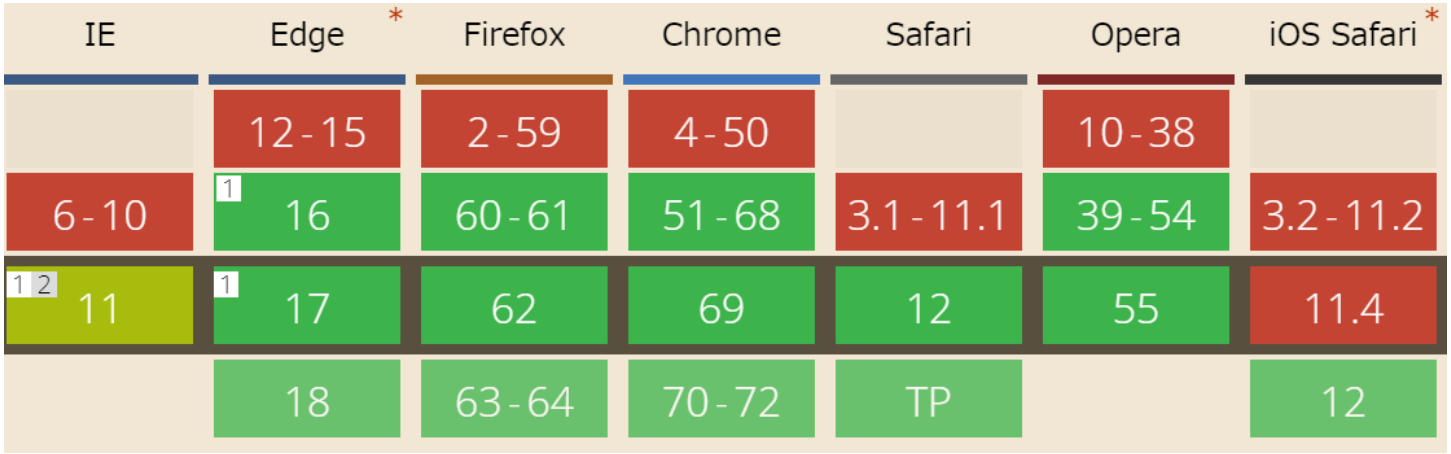
- RefererやCSRF Tokenがおかしいときに、アクセスを遮断する代わりにクッションページをはさむ手法
  - 正当なアクセスならば目的のページにリダイレクトされる
  - 攻撃者はクッションページまでのRTTしか計測できない
  - ページ遷移が増えるため、ユーザ/サービスにやや負担増

対策実施状況

- ウェブサービス
  - Twitterをはじめとする複数社
    - Twitterは特に協力的、対策手法の議論、ブラウザベンダへの呼びかけ、詳細なブログ記事執筆など

記事: https://blog.twitter.com/engineering/en_us/topics/insights/2018/twitter_silhouette.html

- ブラウザ



出典: https://caniuse.com/#feat=same-site-cookie-attribute

SameSite対応バージョン　SameSite非対応バージョン

情報セキュリティ早期警戒 パートナーシップガイドライン

Innovative R&D by NTT

本ガイドラインは、次のものに係る脆弱性であって、その脆弱性に起因する影響が不特定または多数の人々におよぶおそれのあるものに適用します。

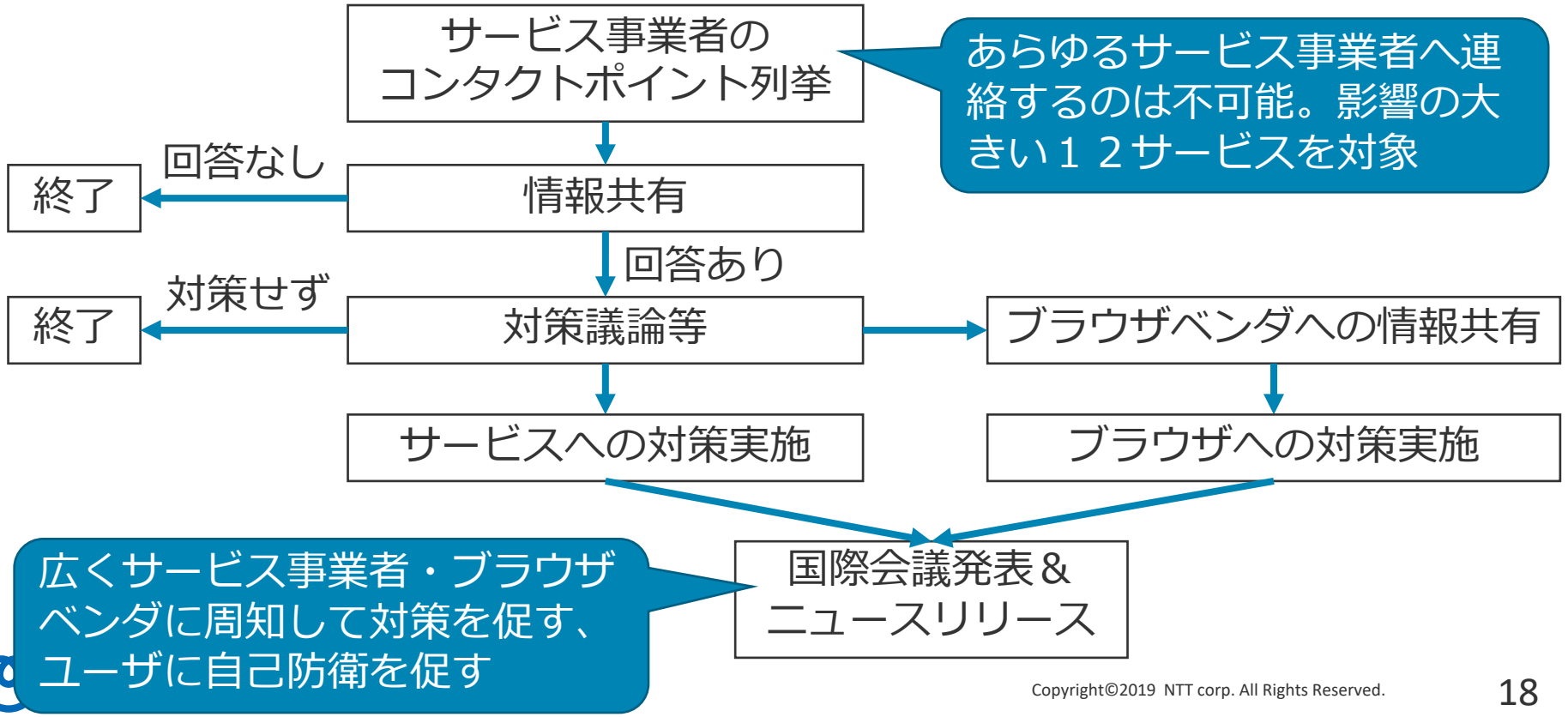
○日本国内で利用されているソフトウエア製品
・「暗号アルゴリズム」や「プロトコル」を実装しているものも含みますが、一般的な「暗号アルゴリズム」や「プロトコル」等の仕様そのものの脆弱性は含みません。（プロトコルの実装に係わる脆弱性については付録１に示します。）
・ソフトウエア製品に係る脆弱性関連情報の取扱いは、Ⅳ. で記述します。

○主に日本国内からのアクセスが想定されているウェブサイトで稼働するウェブアプリケーション
・例えば、主なコンテンツが日本語である、あるいは URL のホスト名の最上位ドメインが「jp」であるウェブサイト等を指します。
・ウェブアプリケーションに係る脆弱性関連情報の取扱いは、Ⅴ. で記述します。

NTT

Responsible disclosure

- 本脅威はソフトウェアの脆弱性ではなく、ソーシャルWebサービスの仕様に起因するオンラインプライバシー脅威
  - 「情報セキュリティ早期警戒パートナーシップ」は活用していない
  - 発見者自身でステークホルダに情報共有を行った



知見・議論

- 「情報セキュリティ早期警戒 パートナーシップ」が全ての脅威を取り扱えるわけではない
  - 発見者自身がResponsible disclosureの方法を把握してことも時には必要
- 発見者自身が responsible disclosure をすることで初めてわかったこと
  - コーディネータの苦労
  - (英語)論文が「脅威・脆弱性の手順書」の代わりになる
  - ベンダとの議論の中で新しい対策を思いつくことも
- ベンダの内側で実際に何をどのようにやっているのか
  - 守秘義務があるので難しいのは理解できる
  - 内側での大変さもわかれば発見者・研究者も対応の参考になる

Kenneth Kufluk

@kpk

Sr. Software Engineer,
Twitter

Gregory Baker

@equanimityhow

Sr. Staff Software Engineer,
Twitter

Insights

Protecting user identity against Silhouette

By Kenneth Kufluk and Gregory Baker

Tuesday, 18 September 2018

The security of Twitter users and their data is important to us. One aspect is securing your Twitter identity from other websites you may visit.

A user may accidentally visit a malicious website via a link from an email or Tweet, from an advertisement on another website, or from a hacked version of a familiar site. The malicious nature of a site may not be apparent, because the site may perform actions in the background.

If a website is able to find your Twitter identity, they may use that information for tracking or association between other accounts. It may enable them to connect your offline names to your online identities. In some regions, this may put users at great risk.

まとめ

- 「攻撃の実証」が実サービスを堅牢にした
  - Silhouette（および類似した攻撃）を対策
    - サービス改善（数億人へ影響）
    - ブラウザ改善（未来のサービスまで影響）
  - 学術成果を実社会に還元できた
    - 著名国際会議への採録が事業者を動かすトリガーになった印象
- 研究責任を果たしながら引き続き取り組んでいきたい
  - 攻撃者の視点に立つことで、未知の脅威を発見する
  - 得られた知見を展開し、被害が発生する前に防ぐ