

2015年9月15日
第53回JPドメイン名諮問委員会
資料3-2

不正行為に使われているJPDドメイン名への レジストリとしての対応について

2015年9月15日(火)
JPDメイン名諮問委員会事務局

目次

1. インターネットにおける不正行為の概況
2. 不正行為に使われているドメイン名へのTLDでの対応事例
3. JPRSにおけるフィッシングへの対応状況
4. 不正行為に使われているJPDメイン名へのレジストリとしての対応に関する議論

1. インターネットにおける不正行為の概況

インターネットにおける不正行為の状況

- 現在、インターネットにおいて様々な不正行為が氾濫しており、2009～2013年のサイバー犯罪の検挙件数は増加傾向にある
- 時間経過に伴いインターネット上における不正行為による被害が拡大するため、警察による対応の他にも事業者や関係機関などが連携し、対応が進められている

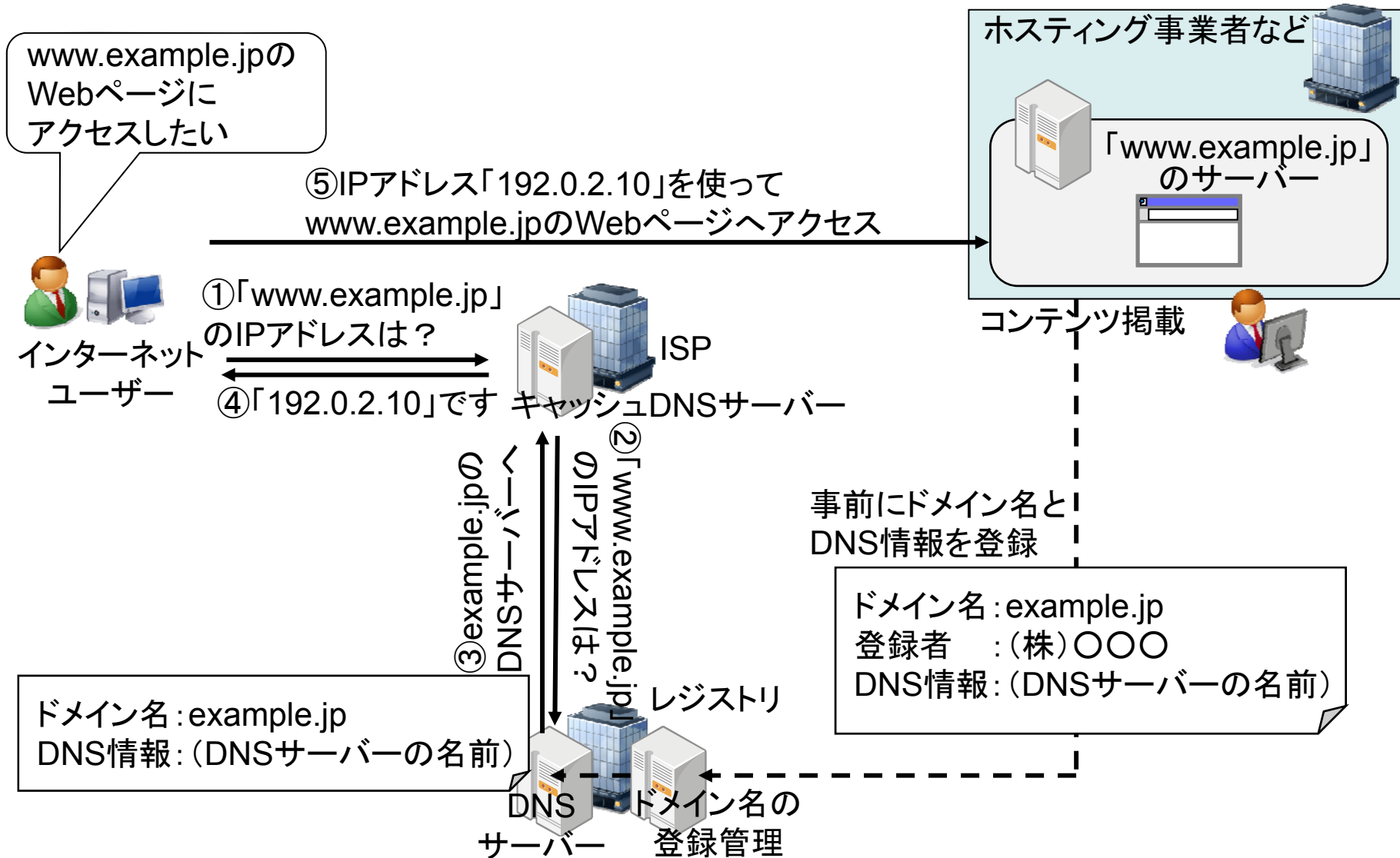
サイバー犯罪の検挙件数の推移

区分	2009	2010	2011	2012	2013
合計(件)	6,690	6,933	5,741	7,334	8,113
不正アクセス禁止法違反	2,534	1,601	248	543	980
コンピュータ・電磁的記録対象犯罪等	195	133	105	178	478
ネットワーク利用犯罪	3,961	5,199	5,388	6,613	6,655
詐欺	1,280	1,566	899	1,357	956
児童買春・児童ポルノ禁止法違反(児童ポルノ)	507	783	883	1,085	1,124
わいせつ物頒布等	140	218	699	929	781
青少年保護育成条例違反	326	481	434	520	690
著作権法違反	188	368	409	472	731
児童買春・児童ポルノ禁止法違反(児童買春)	416	410	444	435	492
出会い系サイト規制法違反	349	412	464	363	339
商標法違反	126	119	212	184	197
その他	629	842	944	1,268	1,345

警察庁「平成26年 警察白書 第3章 サイバー空間の安全の確保」

<http://www.npa.go.jp/hakusyoy/h26/honbun/pdf/08_dai3sho.pdf>をもとに作成

インターネットユーザーのコンテンツへのアクセス



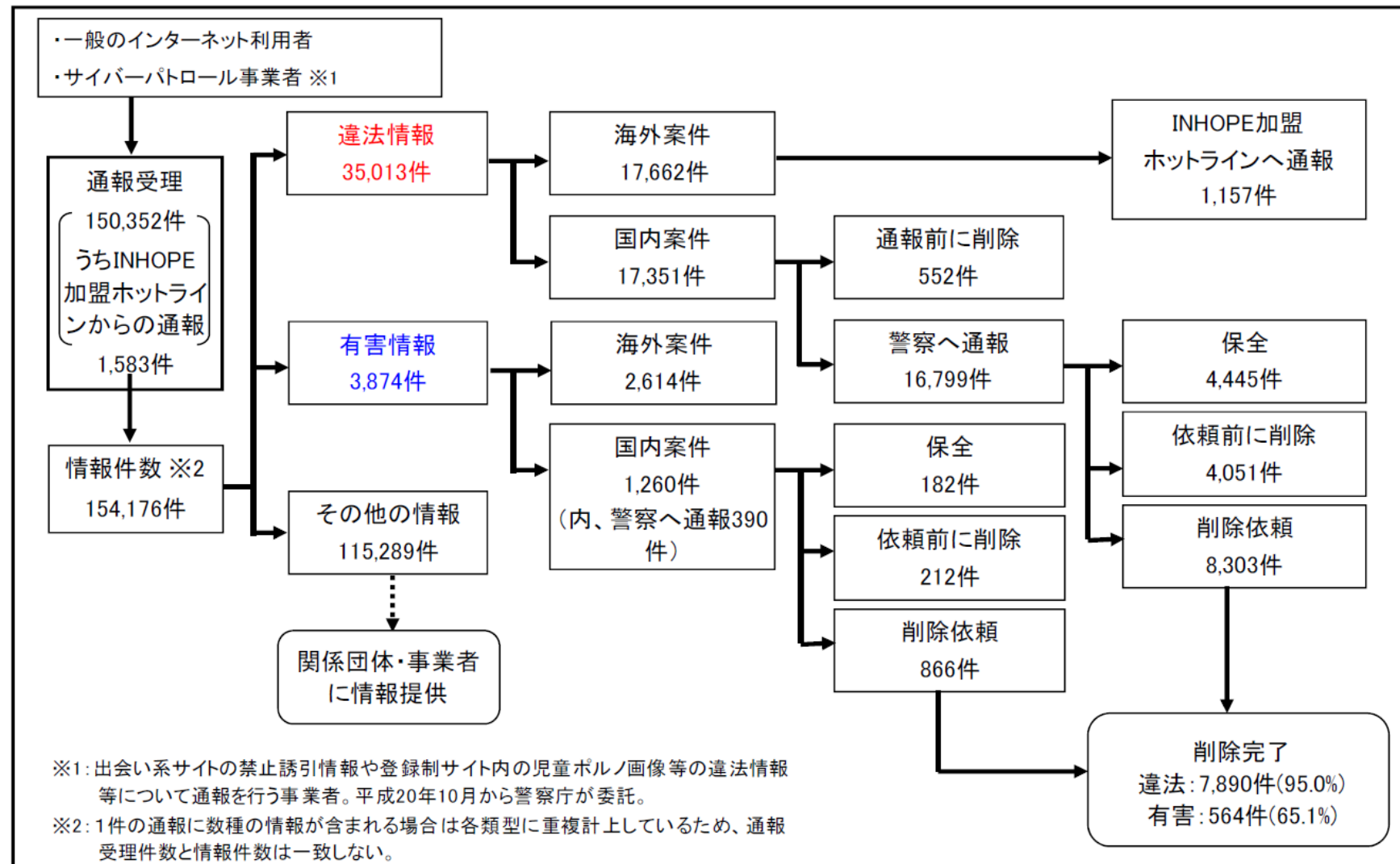
インターネット上におけるコンテンツに関わる不正行為への対応概要

対応	対応者	内容
不正行為者の逮捕	警察	不正なコンテンツを掲載している者を逮捕する。
コンテンツの削除	ホスティング事業者	不正なコンテンツを削除し、インターネットユーザーが不正なコンテンツにアクセスできないようにする。
コンテンツのフィルタリング	インターネットユーザー	セキュリティソフトなどを使って、不正なコンテンツにアクセスしないようにする。
DNSブロッキング	ISP	特定のURLに対応するIPアドレスを返さないようにし、不正行為が行われているコンテンツにアクセスできないようにする。
ドメイン名の廃止・移転	レジストリ	裁判所からドメイン名の使用の差し止めの命令を受けたドメイン名の取り消しやJPDメイン名紛争処理方針(JP-DRP)における裁定に基づき、廃止や移転などの手続きを行う。

主な通報相談機関

通報相談機関	窓口で扱う情報
警察	一般からのサイバー犯罪に関する情報
インターネット・ホットラインセンター (IHC) ※一般財団法人インターネット協会が 警察庁からの委託を受け、運用	一般からのインターネット上の違法・有害情報
一般社団法人セーファーインターネット協会 (SIA) ※IHCや関係機関・団体と協力しながら、 純粋な民間活動として独自の取組を進め、 新たな選択肢を提供することを目指している	一般からのインターネット上の違法・有害情報
一般社団法人 JPCERT コーディネーション センター (JPCERT/CC)	一般からのコンピュータセキュリティインシデント(情報システムの運用におけるセキュリティ上の問題として捉えられる事象)の情報
一般社団法人インターネットコンテンツセーフティ協会 (ICSA)	IHCからのインターネット上の児童ポルノの情報

IHCにおける通報処理状況



IHC「平成26年中のインターネット・ホットラインセンターの運用状況について」
<<https://www.internethotline.jp/statistics/2014.pdf>>

IHCにおける違法情報と判断した通報の処理結果

違法情報	処理結果件数			
	通報前に削除された件数	IHCが警察庁へ通報した件数	IHCがプロバイダなどに対して削除を依頼した件数	その結果、削除に至った件数
わいせつ電磁的記録記録媒体陳列	312	12,712	6,114	6,059
児童ポルノ公然陳列	138	1,233	390	384
売春目的等の誘引	3	209	113	108
出会い系サイト規制法違反の禁止誘引行為	0	1,137	648	536
薬物犯罪等の実行又は規制薬物の濫用を、公然、あおり、又は唆す行為	0	120	91	72
規制薬物の広告	10	655	531	406
指定薬物の広告	5	148	91	72
危険ドラッグに係る未承認医薬品の広告	0	7	2	2
預貯金通帳等の譲渡等の勧誘・誘引	7	335	287	217
携帯電話等の無断有償譲渡等の勧誘・誘引	1	41	28	26
識別符号の入力を不正に要求する行為	76	202	8	8
不正アクセス行為を助長する行為	0	0	0	0
合計	552	16,799	8,303	7,890

IHC「平成26年中のインターネット・ホットラインセンターの運用状況について」
 <<https://www.internethotline.jp/statistics/2014.pdf>>をもとに作成

IHCにおける有害情報と判断した通報の処理結果

公序良俗に反する情報(有害情報)	処理結果件数			
	IHCが警察庁へ通報した件数	依頼前に削除された件数	IHCがプロバイダなどに対して削除を依頼した件数	その結果、削除に至った件数
違法行為を直接的かつ明示的に請負・仲介・誘引等する情報	190	91	379	233
違法情報該当性が明らかであると判断することは困難であるが、その疑いが相当程度ある情報	200	116	316	253
人を自殺に誘引・勧誘する情報	0	5	171	78
合計	390	212	866	564

IHC「平成26年中のインターネット・ホットラインセンターの運用状況について」
 <<https://www.internethotline.jp/statistics/2014.pdf>>をもとに作成

SIAにおける通報対応

- 国民から提供を受けた情報をガイドラインに照らし分類を行い、違法な情報や有害な情報が掲載された国内、海外のプロバイダに対して、迅速な削除措置を要請するとともに、警察への通報を実施
- また、海外プロバイダのサーバーにアップロードされている、児童ポルノ画像等の深刻な被害をもたらすデータに対しては、対応が行われるまで継続して削除要請を実施



SIA「運用ガイドライン」
<<http://www.safe-line.jp/guideline/>>

JPCERT/CCにおけるインシデント対応状況

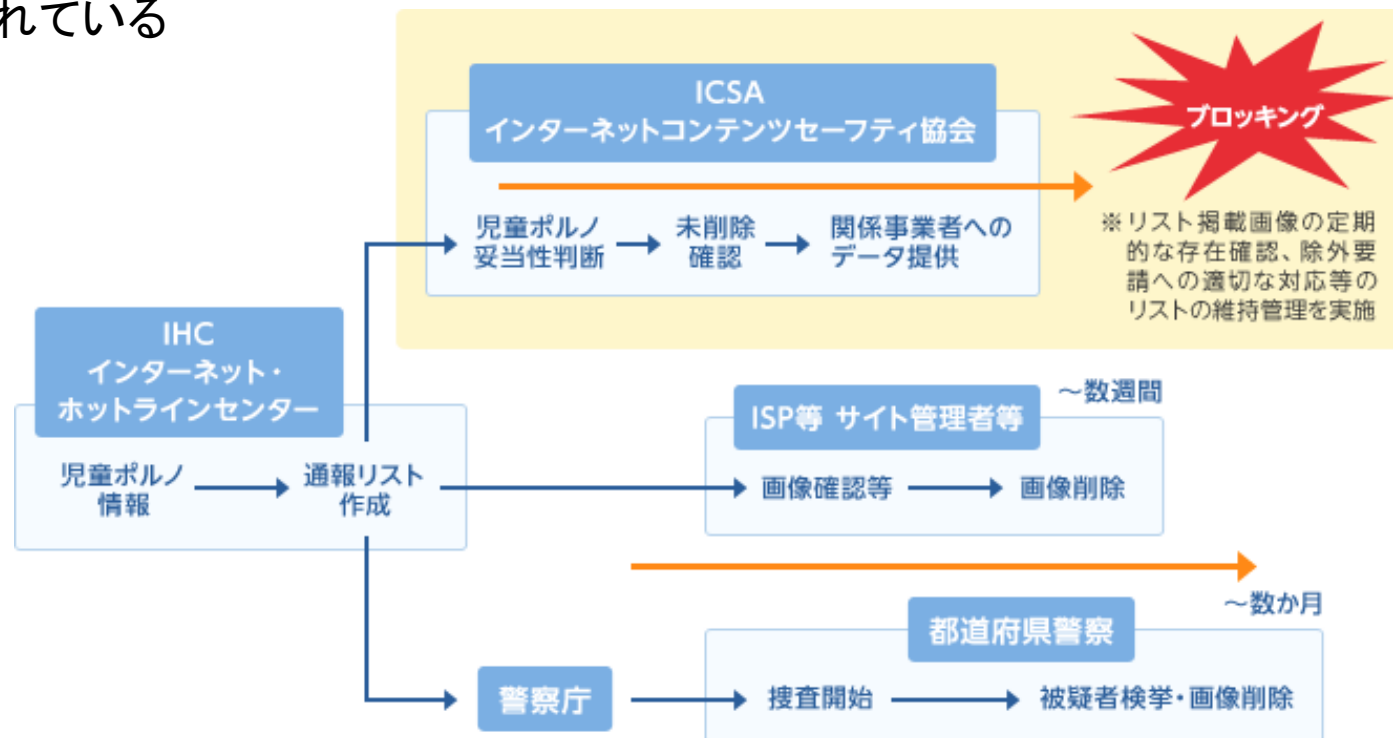
- JPCERT/CCに対し、2015年4月1日～6月30日に寄せられたコンピュータセキュリティインシデント報告件数
 - コンピュータセキュリティインシデントとは、情報システムの運用におけるセキュリティ上の問題として捉えられる事象、コンピュータのセキュリティに関わる事件、できごとの全般をいう

インシデント	4月	5月	6月	合計	前四半期 合計
フィッシングサイト	191	144	156	491	466
Web サイト改ざん	209	175	265	649	792
マルウェアサイト	56	59	82	197	260
スキャン	976	823	643	2,442	2,980
DoS/DDoS	61	3	7	71	32
制御システム関連	0	4	0	4	5
標的型攻撃	12	21	27	60	-
その他	116	91	67	274	950

JPCERT/CC「JPCERT/CCインシデント報告対応レポート[2015年4月1日～2015年6月30日]」
 <https://www.jpccert.or.jp/pr/2015/IR_Report20150714.pdf>をもとに作成

ICSAにおける児童ポルノ流通対策(1/2)

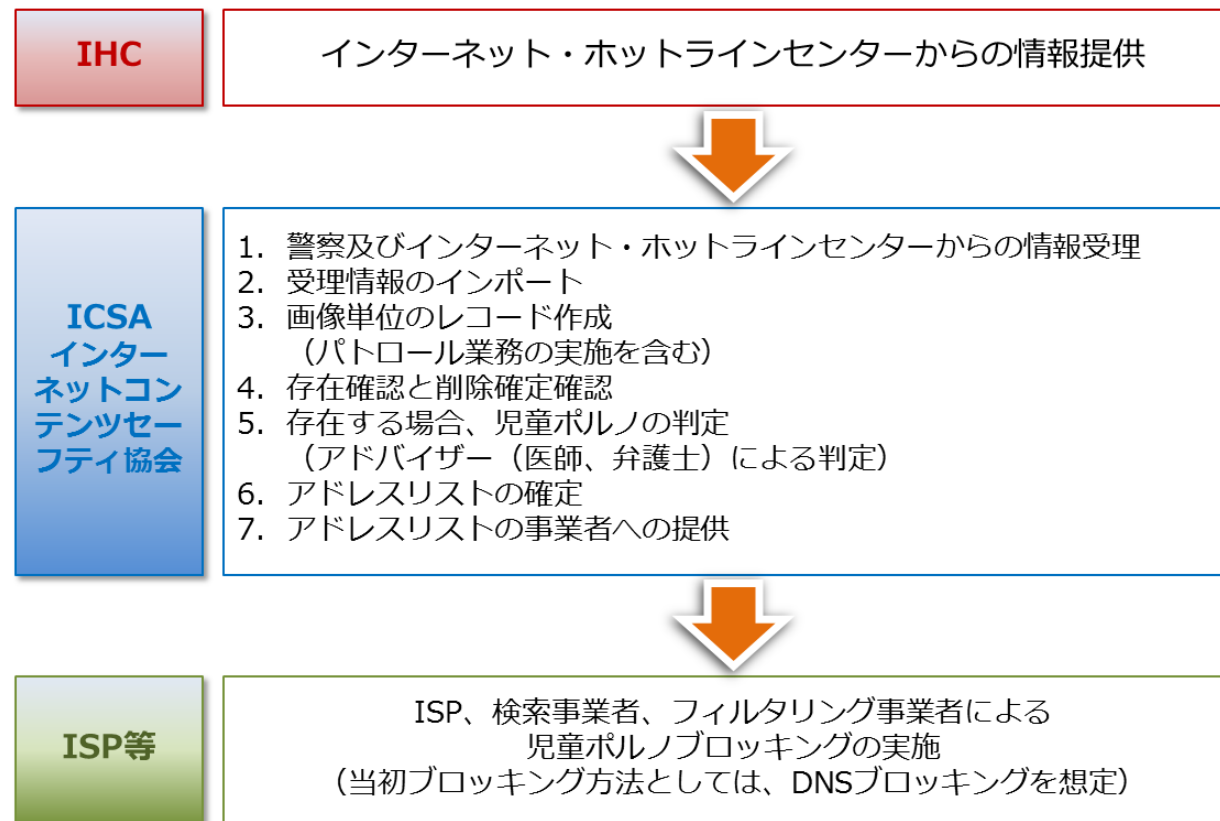
- 児童ポルノの流通対策として以下の取り組みが行われている
- その中では、被害の拡大を防ぐために、児童ポルノが掲載されているURLサイトへのアクセスを遮断するブロッキングが行われている
- ブロッキングは、通信の秘密を侵害する行為であるが、違法性阻却事由として「緊急避難」が成り立つ場合に限り、一定の範囲で可能であるとの整理の上で行われている



ICSA「インターネット上の児童ポルノ流通対策の全体イメージ」
<<http://www.netsafety.or.jp/blocking/index.html>>

ICSAにおける児童ポルノ流通対策(2/2)

- ブロッキングのための児童ポルノアドレスリスト作成フロー



ICSA「インターネット上の児童ポルノ流通対策の全体イメージ」
<<http://www.netsafety.or.jp/blocking/index.html>>

2. 不正行為に使われているドメイン名 へのTLDでの対応事例

gTLDでの対応事例

- Verisignが運用するTLD(.com/.netなど)
対象: 裁判所や法執行機関が対象とする不正行為すべて
対応:
 - レジストリは裁判所や法執行機関の命令を受けそれに従った対応を実施
 - レジストリ自ら廃止などの対応はせず、登録者とやり取りできる立場にいるレジストラに依頼
- Afiliasが運用するTLD(.asia/.info/.mobi/.orgなど)
対象: フィッシング/ファーミング/ボットネット運用/マルウェア配布/スパムメール配信/Fast-Fluxホスティング/不正アクセス/児童ポルノ画像・映像の掲示・配布/違法行為・詐欺的行為/その他
対応:
 - CERTなどから連絡を受け不正利用確認後、レジストリはレジストラにDNSサーバー設定削除などの対応を要請
 - レジストラが24時間以内に対応しない場合、レジストリがDNSサーバー設定削除などの対応を実施

ccTLDでの対応事例

- .de(ドイツ)
 - 対象: 裁判所や法執行機関が対象とする不正行為すべて
 - 対応: レジストリは裁判所や法執行機関の命令を受けそれに従った対応を実施
- .hk(香港)
 - 対象: 裁判所や法執行機関が対象とする不正行為すべて
 - 対応: HKCERT、警察からの連絡に基づいて、レジストリがフィッシングに使われているドメイン名を検証、停止
- .ru(ロシア)
 - 対象: 不明
 - 対応: 中立な会員機関(政府機関、セキュリティ会社、インシデント対応組織などが加入)で問題ある登録者／関係者を絞り込み、ドメイン名の停止を実施
- .sg(シンガポール)
 - 対象: 不明
 - 対応: レジストリが以下の項目についてチェックし、「不正利用」と判断された場合はISPやWebホスティング事業者と協力して対処
 - 登録情報の正確性・完全性／怪しい登録傾向に合致するか／オークションや販売サイトで売られていないか／有名文字列との類似性／マルウェア配布やフィッシングに利用されていないか(CERTと協力して検証)

3. JPRSにおけるフィッシングへの対応状況

フィッシングの被害防止に関する答申を 踏まえたJPRSの活動方針

- JPRSは、JPDメイン名諮問委員会に2007年8月23日に諮問し、2008年3月18日に以下の主旨の答申を受領
 - これまでと同様に、JPRSは、ドメイン名の文字列や使い方の妥当性を自ら判断することによりドメイン名を使用停止にすることはせず、指定事業者の協力を得て対処することが適切である
 - ただし、インターネット利用者の安心・安全を守るため、重大かつ緊急の場合には、信頼できる第三者機関の判断に基づき、JPRSがドメイン名の使用停止を行えるようにしておくことも必要である

→ 現在のJPRSの活動方針となっている

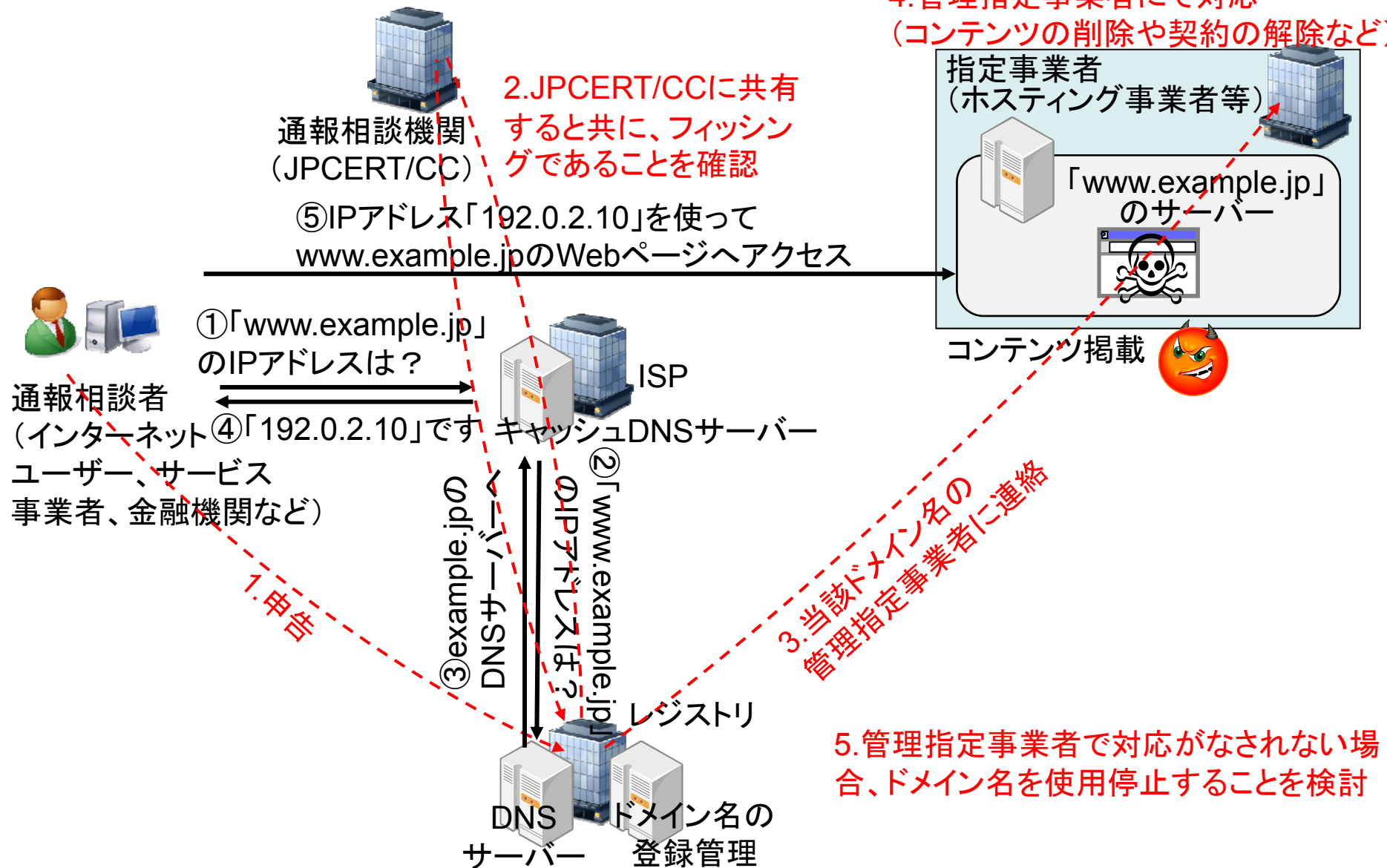
JPRSにおけるフィッシング対応手順

1. インターネットユーザー、サービス事業者、金融機関などからの申告
2. JPCERT/CCに共有すると共に、フィッシング確認
3. 当該ドメイン名の管理指定事業者に連絡
4. 管理指定事業者にて対応(コンテンツの削除や契約の解除など)
5. 管理指定事業者で対応がなされない場合、登録を取り消すことを検討

※実際には、5に至るまでに解決し、このプロセスで取消を行ったケースはまだ無い

JPRSにおけるフィッシング対応手順

4. 管理指定事業者にて対応
(コンテンツの削除や契約の解除など)



JPRSにおけるフィッシング対応件数

- 2008年6月26日～2015年8月1日の間に、JPRSに申告のあった件数は59件で、そのうち当該ドメイン名の管理指定事業者に連絡した件数は44件

年	JPRSへの申告件数	対応不要の件数(※)	指定事業者への連絡件数
2008	20	1	19
2009	12	1	11
2010	6	3	3
2011	2	0	2
2012	2	0	2
2013	2	1	1
2014	1	1	0
2015	14	8	6
合計	59	15	44

※JPCERT/CCにてフィッシングではないと判断されたもの、
管理指定事業者への連絡前にフィッシングサイトが消えていたもの

JPRSにおけるフィッシングへの対応の結果

- ほぼすべてのフィッシングサイトが停止される
 - 停止に至る代表的なパターン
 - Webを乗っ取った者によって引き起こされたフィッシングの場合、ISPやWebホスティング事業者の顧客に連絡すれば、適切な対応をして正しいWebに置き換えられる
 - ISPやWebホスティング事業者が、その顧客に連絡しようとして、連絡先が虚偽であることが発覚し、解約する
 - ISPやWebホスティング事業者が登録者などと交わしている契約の中に「不適切なコンテンツは削除する」との条項があり、それに抵触したとみなし、解約する
- しかし、フィッシングの被害は年々増えており、今まで以上に重大かつ緊急な対応を要するものが増えることが危惧される
- 一方で、フィッシング以外の不正行為も社会問題として大きくなっており、マルウェアの配布や児童ポルノの流通といった早期に対応しなければ被害が急速に深刻化するものが増えている

4. 不正行為に使われているJPDメイン名 へのレジストリとしての対応に関する議論

どのような不正行為を対象とすべきか

- 不正行為であることを明確に判断できるか
 - IHCでは、取扱対象とする違法・有害情報の範囲について次のように述べている
 - 対象とする違法情報の範囲として、「インターネット上における流通が社会問題化している違法情報であって、ホットラインセンターにおいて適切かつ円滑に違法情報該当性を判断することができる情報を対象とする」
 - 対象とする有害情報の範囲として、「インターネット上における流通が社会問題化している情報であって、ホットラインセンターにおいて適切かつ円滑に、公序良俗に反する情報であるか否かを判断することができるものを対象とする」。また、「表現の自由等と公共の福祉とのバランスに配慮」する

IHC「ホットライン運用ガイドライン」

<<http://www.iajapan.org/hotline/center/20150401guide.pdf>>

- 過剰な対応となる恐れはないか
 - 不正行為への対応は、不正行為ではない部分に影響することはないか
- 上記のような点を考慮し、レジストリが第三者機関や指定事業者と連携して有効な対応を行うことができるか

(参考)IHCが取扱対象とする違法・有害情報

違法情報:社会法益侵害情報

【わいせつ関連情報】

1. わいせつ電磁的記録記録媒体陳列
2. 児童ポルノ公然陳列
3. 売春目的等の誘引
4. 出会い系サイト規制法違反の禁止誘引行為

【薬物関連情報】

5. 薬物犯罪等の実行又は規制薬物(覚せい剤、麻薬、向精神薬、大麻、あへん及びけしがら)の濫用を、公然、あおり、又は唆す行為
6. 規制薬物の広告
7. 指定薬物の広告
8. 指定薬物等である疑いがある物品の広告
9. 危険ドラッグに係る未承認医薬品の広告

【振り込め詐欺等関連情報】

10. 預貯金通帳等の譲渡等の勧誘・誘引
11. 携帯電話等の無断有償譲渡等の勧誘・誘引

【不正アクセス関連情報】

12. 識別符号の入力を不正に要求する行為
13. 不正アクセス行為を助長する行為

有害情報:公序良俗に反する情報

1. 情報自体から、違法行為(けん銃等の譲渡等、爆発物等の製造、児童ポルノの提供、公文書偽造、殺人、脅迫等)を直接的かつ明示的に請負・仲介・誘引等する情報
2. 違法情報該当性が明らかであると判断することは困難であるが、その疑いが相当程度認められる情報
3. 人を自殺に誘引・勧誘する情報(集団自殺の呼びかけ等)

※取扱対象としない違法・有害情報

【違法情報:権利侵害情報】

名誉毀損、プライバシー侵害、著作権侵害、商標権侵害、etc

【有害情報:青少年にとって好ましくない情報】

残虐、グロテスク、ポルノ、暴力、etc

IHC「ホットラインセンター紹介リーフレット[150514版]」
<<http://internethotline.jp/about/about20150514.pdf>>

個別の事象が不正行為であるか否かを誰が判断すべきか

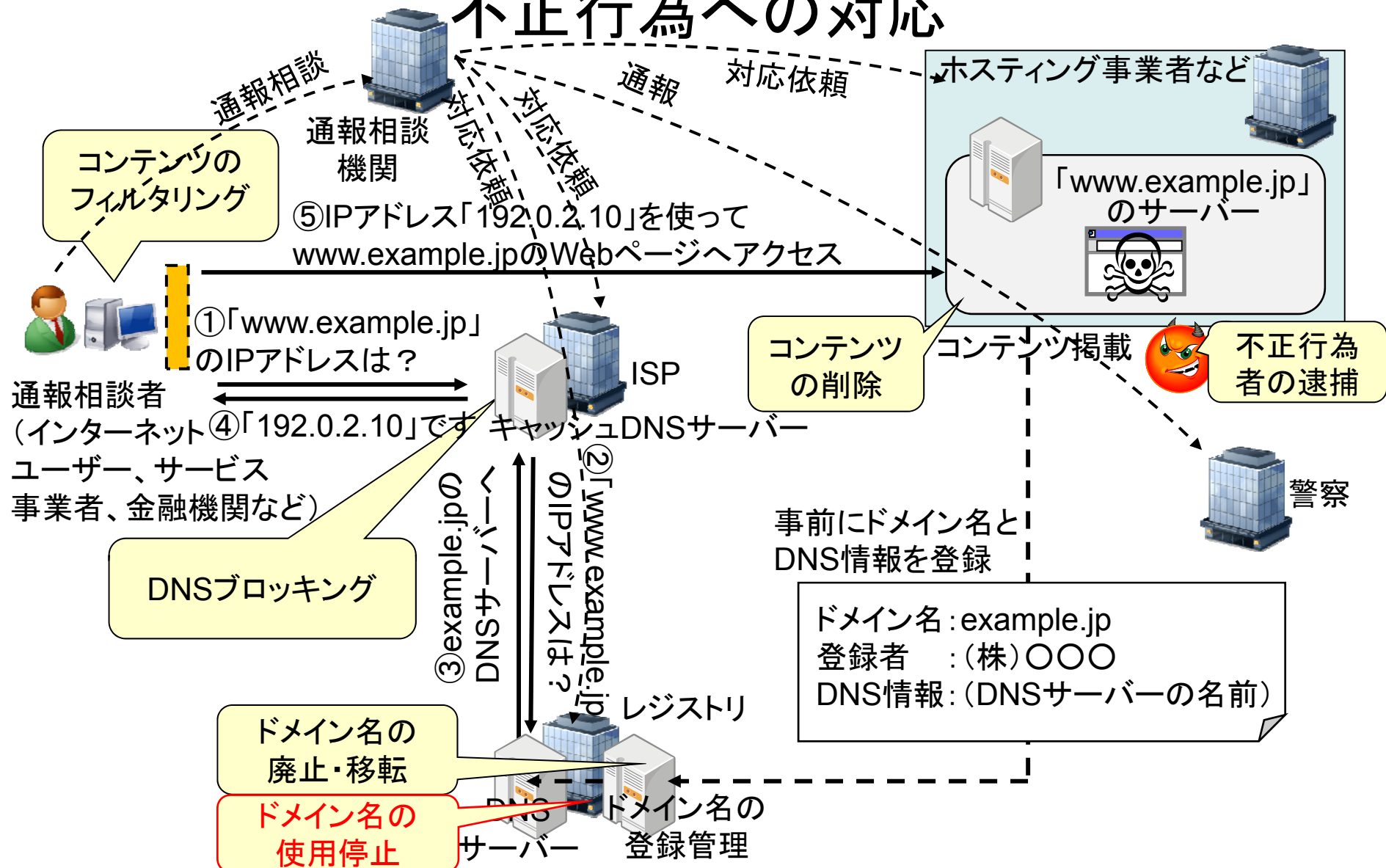
(案1)レジストリが判断する

- 現在、JPRSはドメイン名の文字列や使い方の妥当性には関与しないという方針としており、その方針から逸脱することになる
- 不正行為を判断する専門家ではないため、判断を誤る可能性がある

(案2)適切に判断できる警察・裁判所・第三者機関に判断を委ねる

- それぞれの機関が、それぞれの役割や立場から適切に判断する
- 場合によっては判断に時間がかかる

インターネット上におけるコンテンツに関わる不正行為への対応

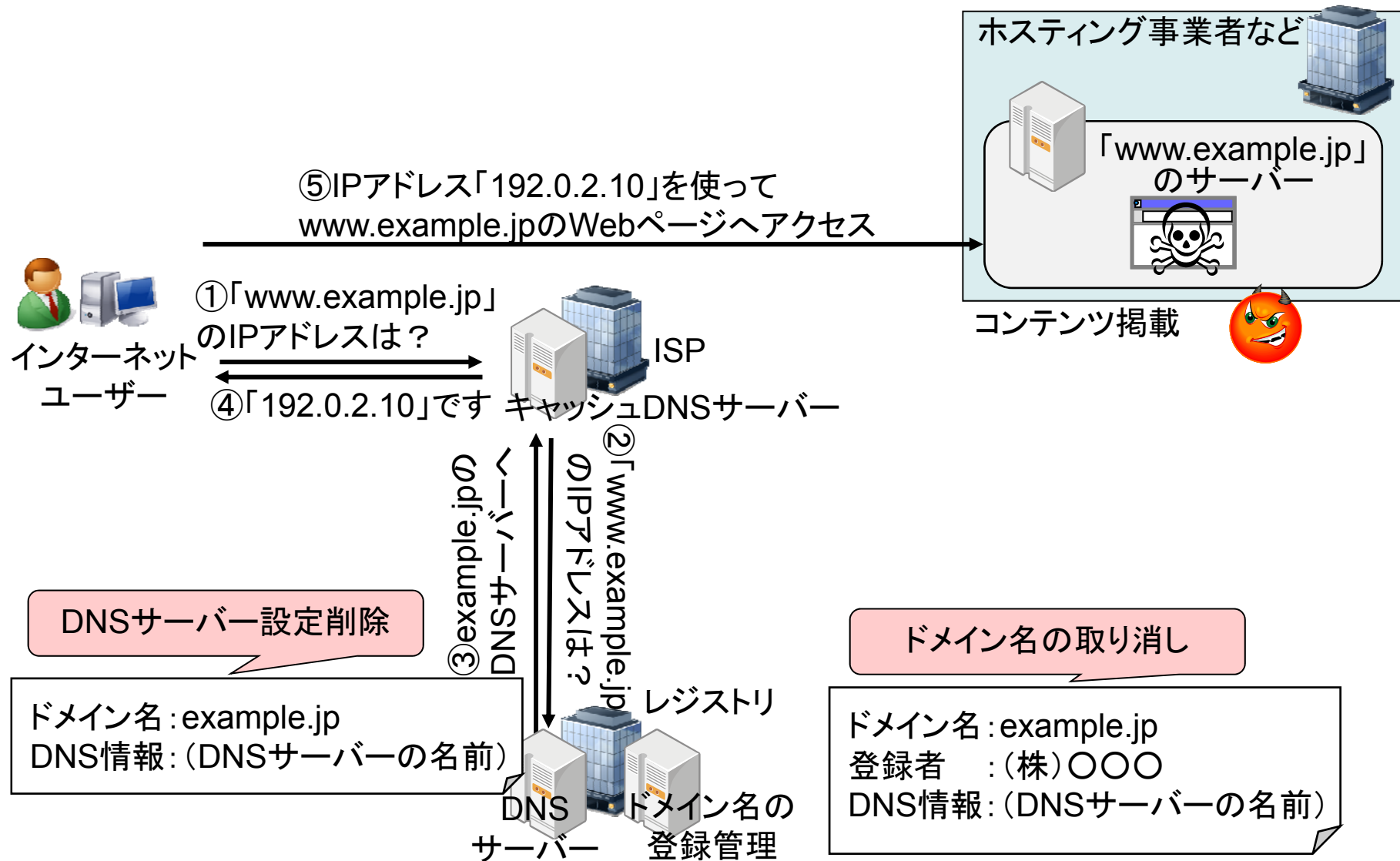


不正行為への対応のメリット／デメリット

対応内容	対応者	メリット(+)/デメリット(-)
不正行為者の逮捕	警察	<ul style="list-style-type: none"> + 逮捕によりそれ以上コンテンツは増えない - 海外のホスティングの場合、対応・連携が難しい場合がある
コンテンツの削除	ホスティング事業者	<ul style="list-style-type: none"> + 不正なコンテンツそのものだけを削除することができる - 海外のホスティングの場合、対応・連携が難しい場合がある
コンテンツのフィルタリング	インターネットユーザー	<ul style="list-style-type: none"> + フィルタリングを行っているユーザー単位になるが不正なコンテンツへのアクセスを防ぐことができる(海外発信にも有効) - フィルタリングを行っているユーザーのみにその効果は限定される
DNSブロッキング	ISP	<ul style="list-style-type: none"> + ISP単位になるがインターネットユーザーの不正なコンテンツへのアクセスを防ぐことができる(海外発信にも有効) - 当該ドメイン名を使っているすべてのコンテンツやサービスが使えなくなり、過剰対応となる可能性がある
ドメイン名の使用停止 (DNSサーバー設定削除、ドメイン名の取り消し)	レジストリ	<ul style="list-style-type: none"> + インターネット全体に対してそのドメイン名を使用停止にすることができる(DNSの仕組み上、効果を及ぼすには数時間から1日を要する) - 当該ドメイン名を使っているすべてのコンテンツやサービスが使えなくなり、過剰対応となる可能性がある - 不正行為を行っていない登録者のドメイン名を取り消すことは過剰対応となる

→後述

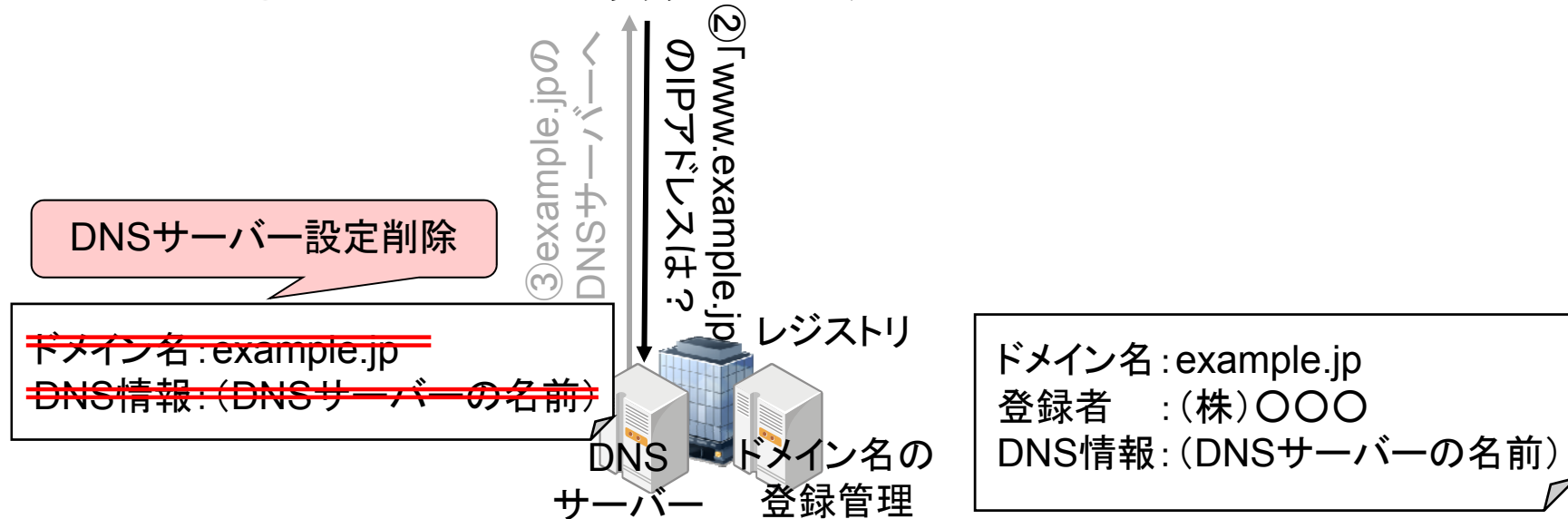
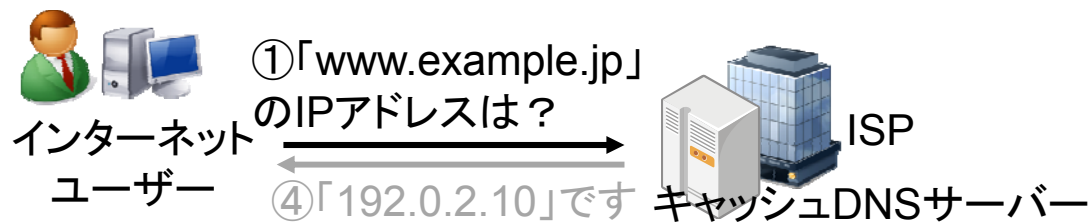
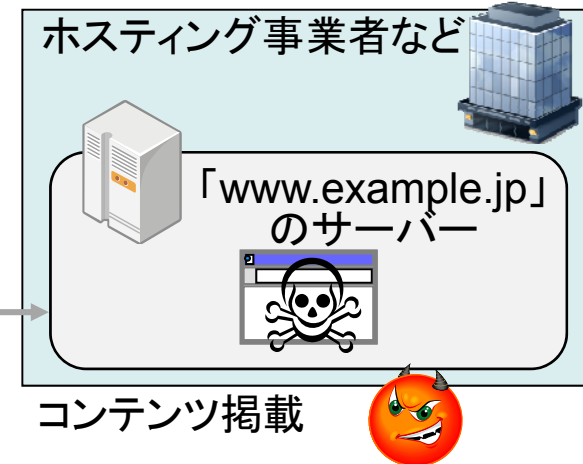
レジストリとして考えられる対応方法



1. DNSサーバー設定削除による対応

レジストリが、ドメイン名に対応するDNSサーバーの情報を削除し、③の応答を返さないようにすることで、そのドメイン名を用いたすべてのコンテンツやサービスにアクセスできないようにする

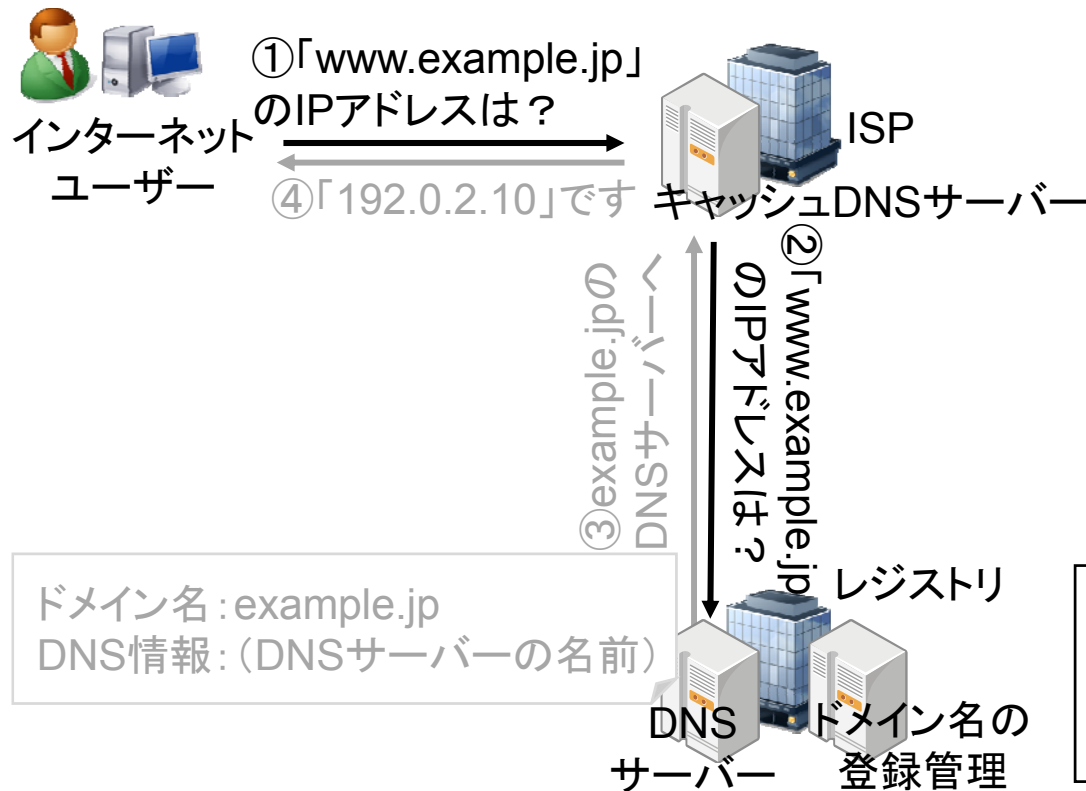
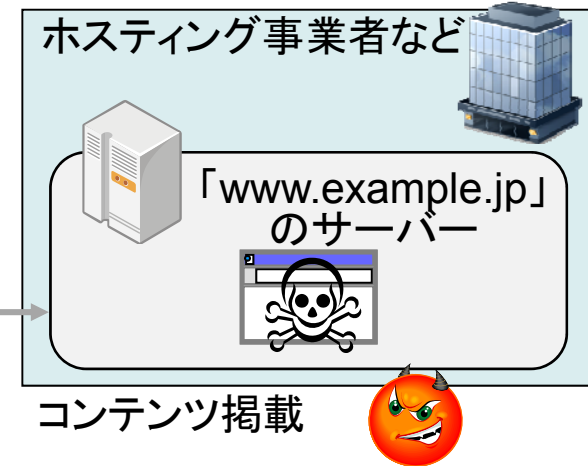
⑤ IPアドレス「192.0.2.10」を使って
www.example.jpのWebページへアクセス



2. ドメイン名の取り消しによる対応

レジストリが、ドメイン名を取り消すことで、DNSサーバー設定も削除され、③の応答を返さないようにすることで、そのドメイン名を用いたすべてのコンテンツやサービスにアクセスできないようにする

⑤ IPアドレス「192.0.2.10」を使って
www.example.jpのWebページへアクセス



ドメイン名の取り消し

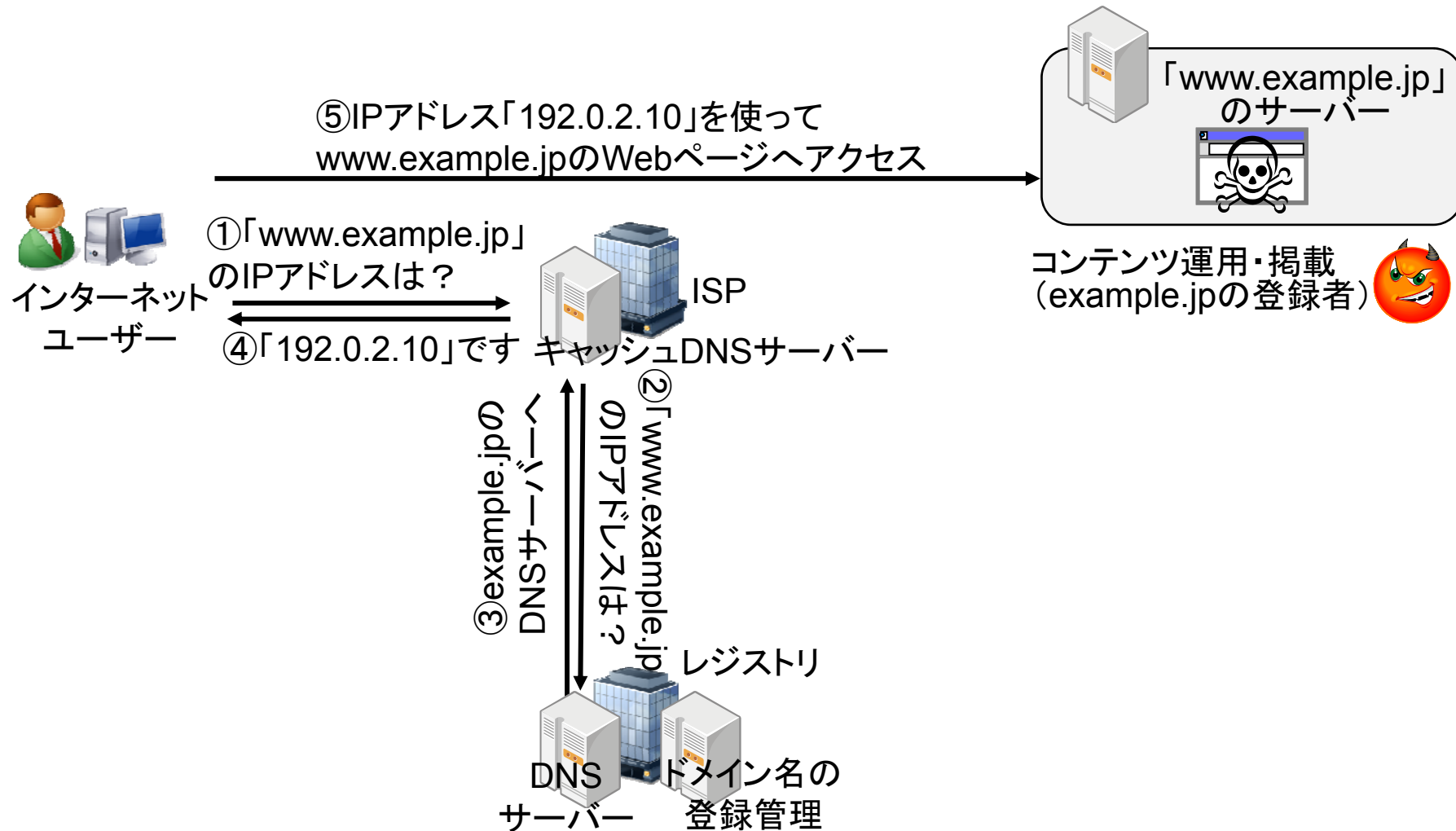
~~ドメイン名: example.jp~~
~~登録者: (株)〇〇〇~~
~~DNS情報: (DNSサーバーの名前)~~

インターネット上におけるコンテンツに関わる 不正行為の方法の類型

- (ア)不正行為者がドメイン名を登録し、不正なコンテンツを運用・掲載
- (イ)不正行為者がブログサービスなどで不正なコンテンツを掲載
- (ウ)不正行為者が正当なコンテンツの一部に不正なコンテンツを掲載
- (エ)不正行為者がドメイン名を乗っ取り不正なコンテンツに誘導

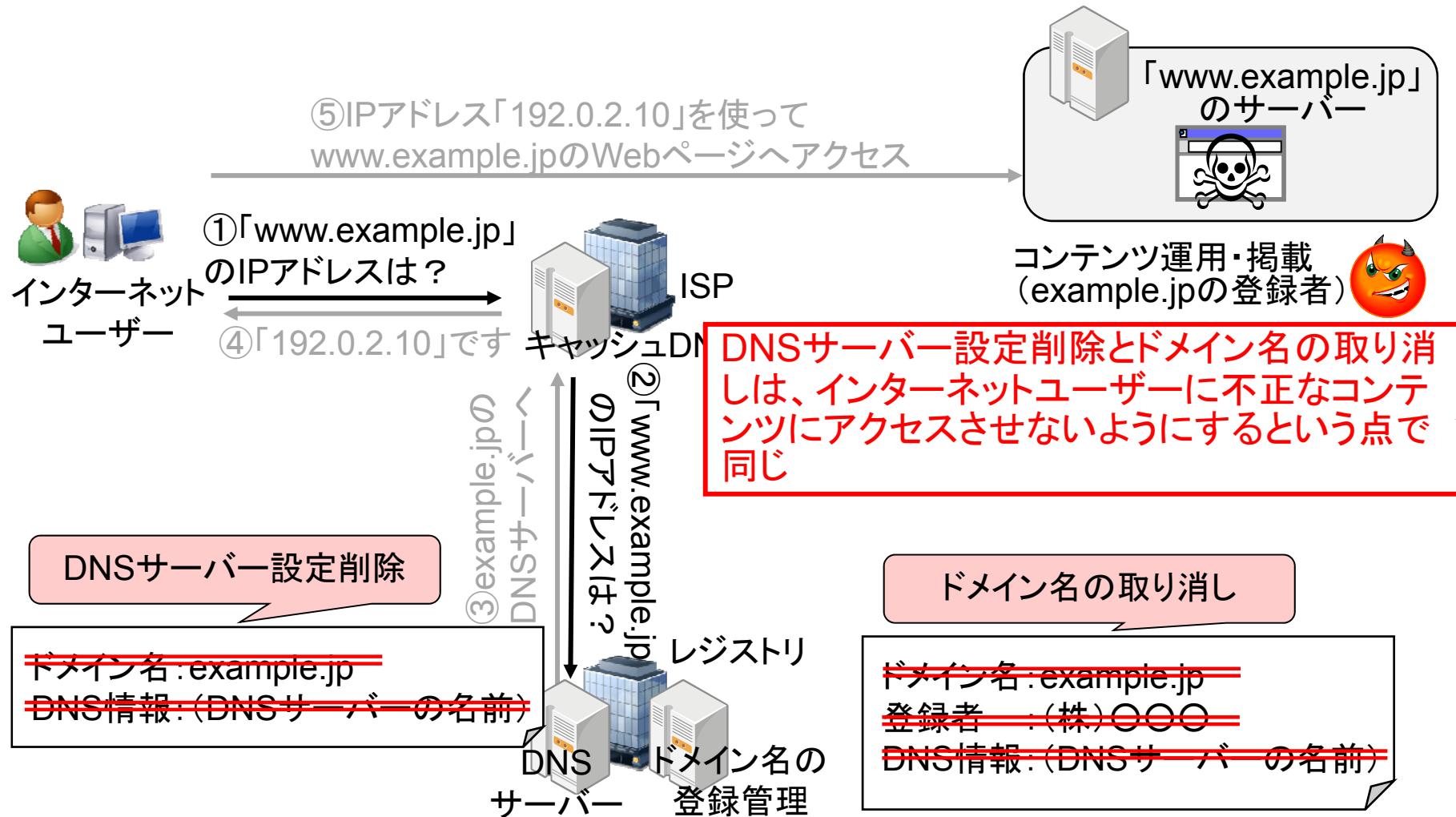
不正行為の方法の類型(ア)

～不正行為者がドメイン名を登録し、不正なコンテンツを運用・掲載～



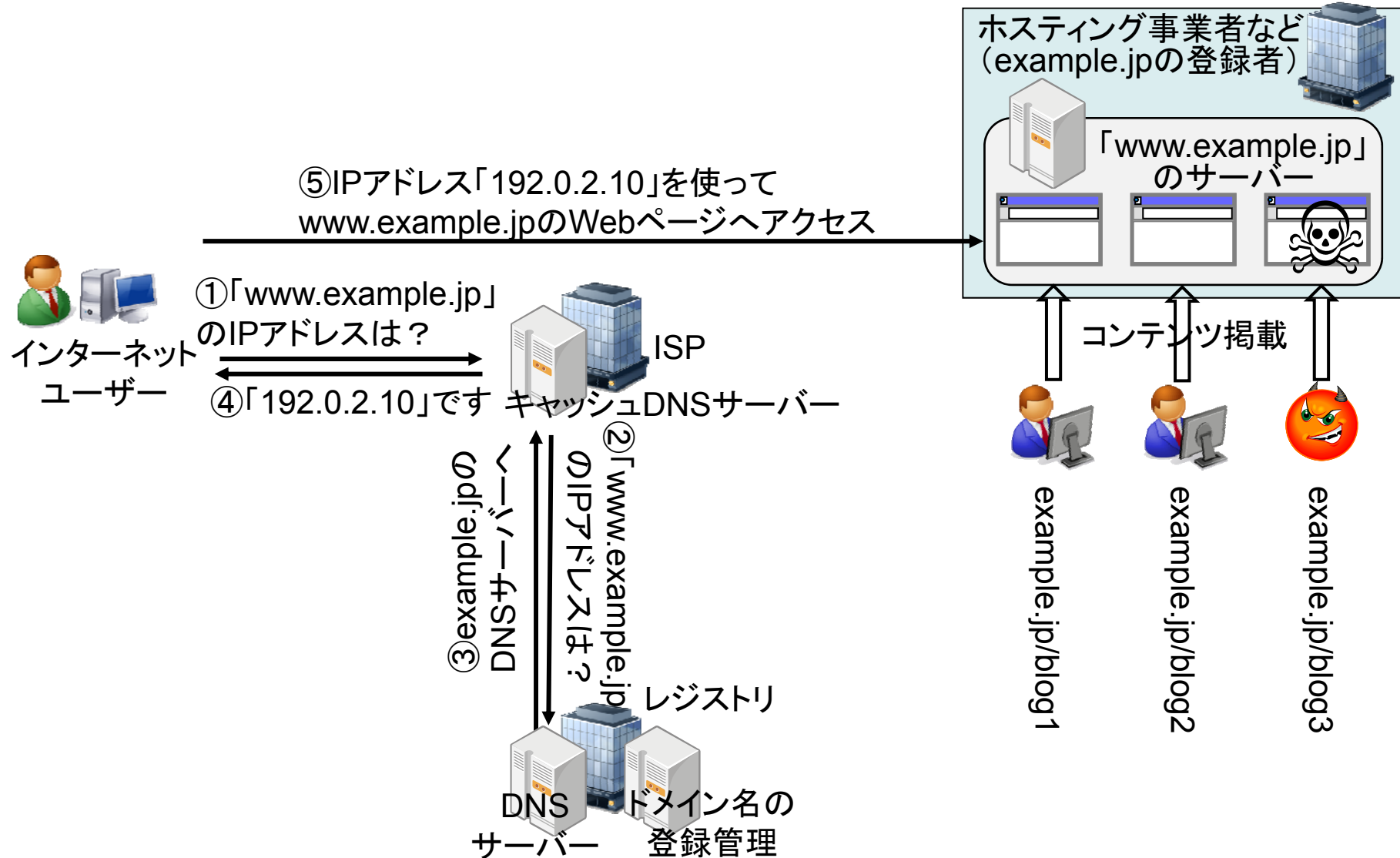
類型(ア)へのレジストリの対応

～不正行為者がドメイン名を登録し、不正なコンテンツを運用・掲載～



不正行為の方法の類型(イ)

～不正行為者がブログサービスなどで不正なコンテンツを掲載～

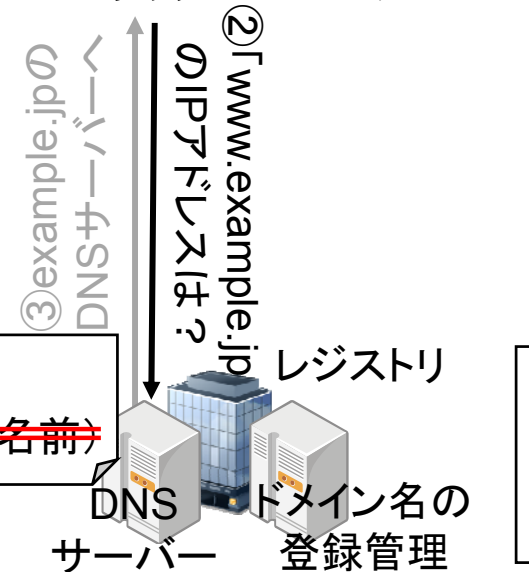
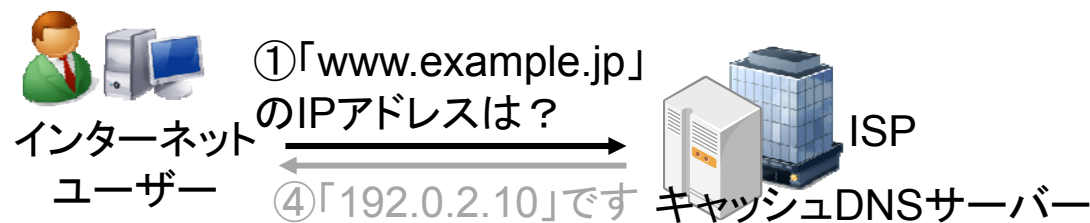
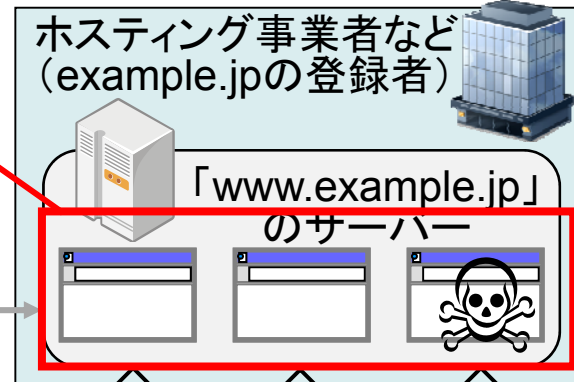


類型(イ)へのレジストリの対応

～不正行為者がブログサービスなどで不正なコンテンツを掲載～

DNSサーバー設定削除、ドメイン名の取り消しにより、そのドメイン名を用いたすべてのサービスにアクセスできなくなる(過剰対応)

⑤ IPアドレス「192.0.2.10」を使って
www.example.jpのWebページへアクセス



DNSサーバー設定削除

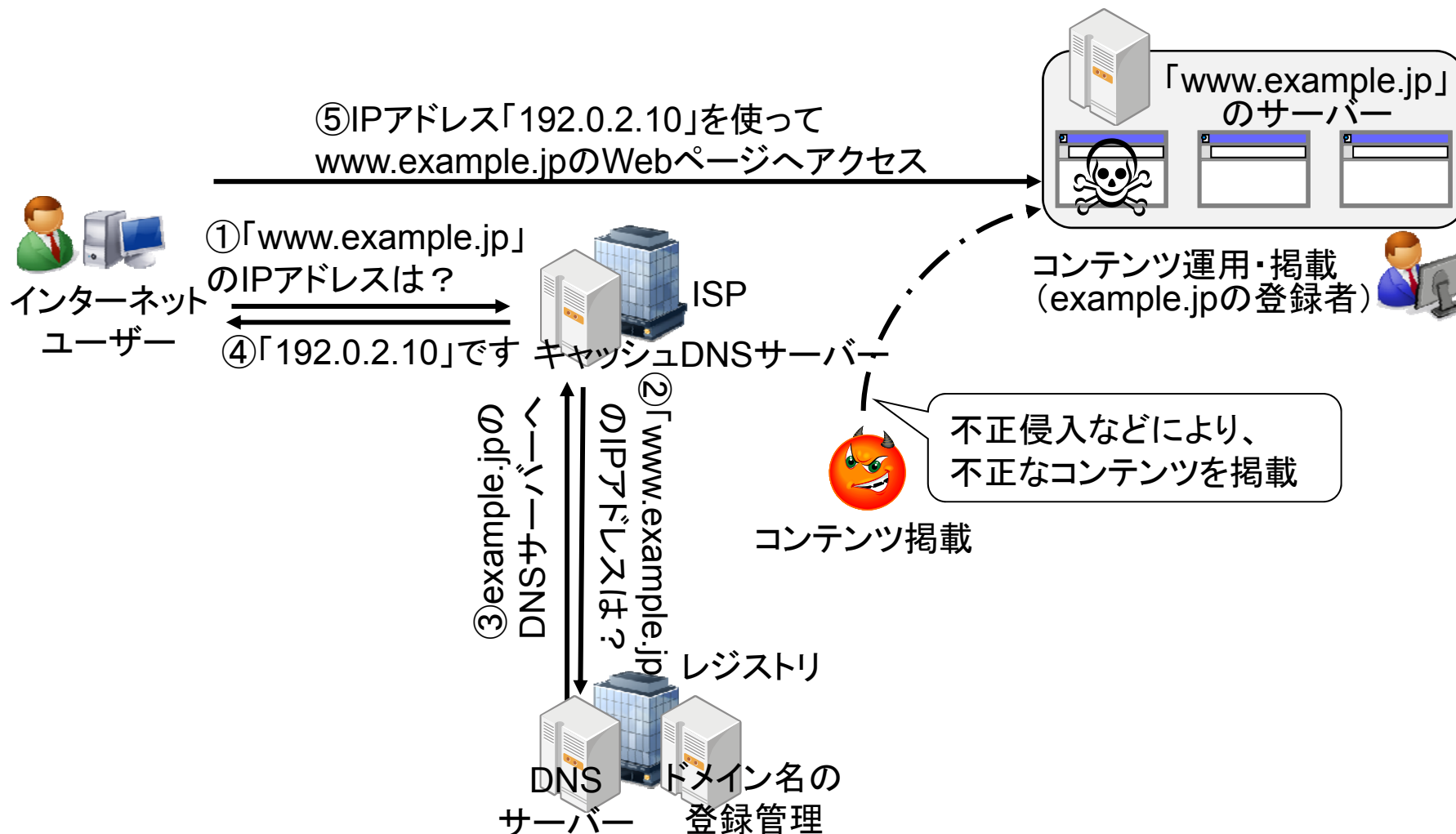
~~ドメイン名: example.jp~~
~~DNS情報: (DNSサーバーの名前)~~

ドメイン名の取り消し

~~ドメイン名: example.jp~~
~~登録者: (株)〇〇〇~~
~~DNS情報: (DNSサーバーの名前)~~

不正行為の方法の類型(ウ)

～不正行為者が正当なコンテンツの一部に不正なコンテンツを掲載～



類型(ウ)へのレジストリの対応

～不正行為者が正当なコンテンツの一部に不正なコンテンツを掲載～

DNSサーバー設定削除、ドメイン名の取り消しにより、不正なコンテンツ以外もアクセスできなくなる(過剰対応)

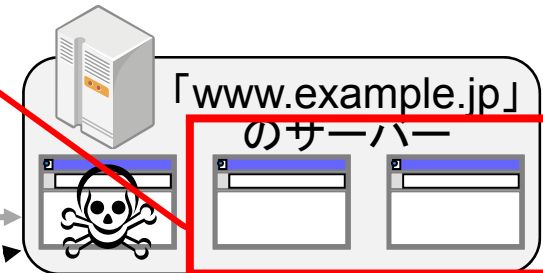
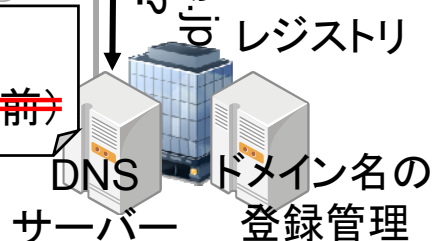
⑤IPアドレス「192.0.2.10」を使って
www.example.jpのWebページへアクセス



①「www.example.jp」
のIPアドレスは?
④「192.0.2.10」です



②「www.example.jp」
のIPアドレスは?
③example.jpの
DNSサーバーは?



コンテンツ掲載
(example.jpの登録者)



ドメイン名の取り消しを行った
場合には、不正行為を行って
いない登録者のドメイン名を取り
消すことになる(過剰対応)

DNSサーバー設定削除

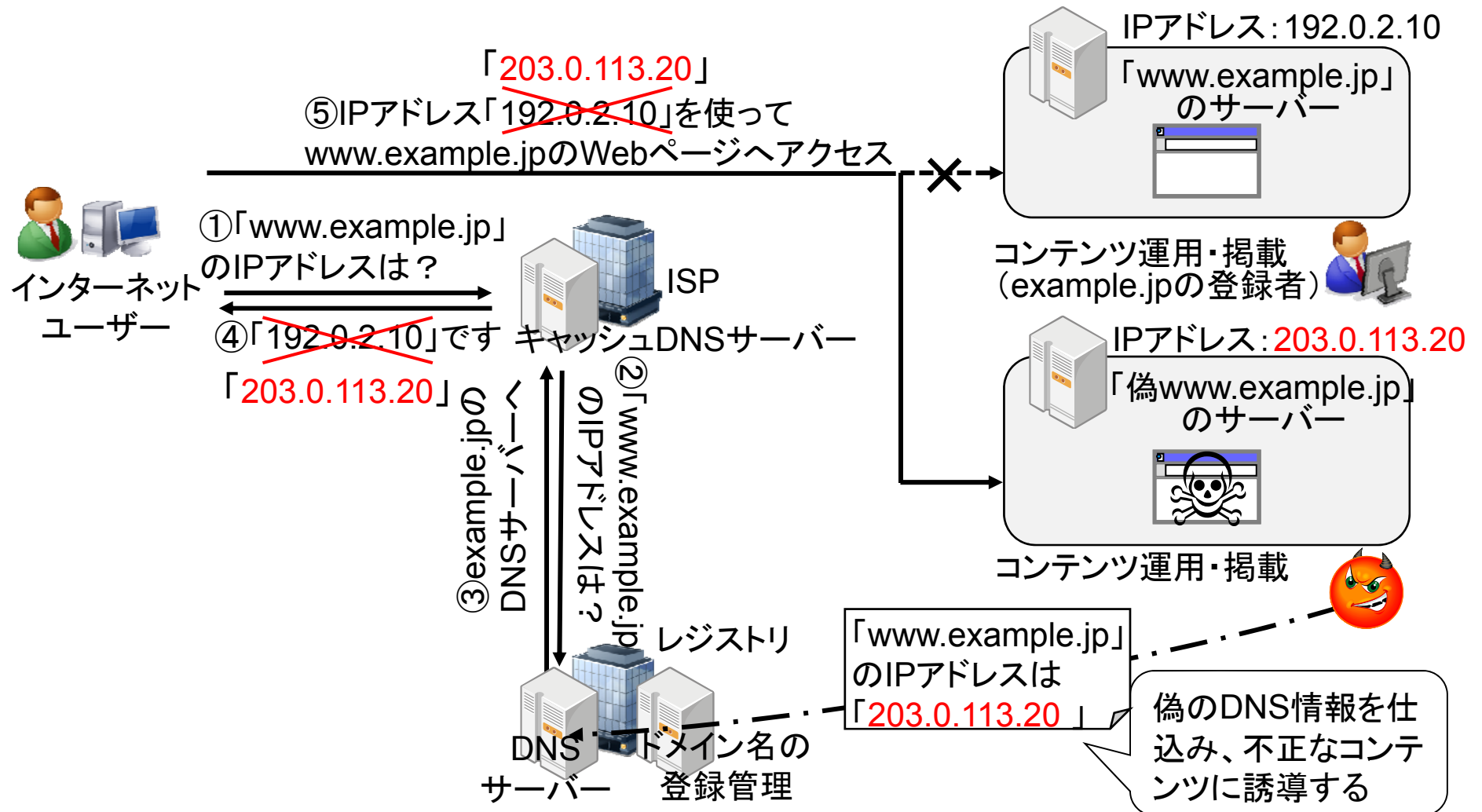
~~ドメイン名: example.jp~~
~~DNS情報: (DNSサーバーの名前)~~

ドメイン名の取り消し

~~ドメイン名: example.jp~~
~~登録者: (株)〇〇〇~~
~~DNS情報: (DNSサーバーの名前)~~

不正行為の方法の類型(エ)

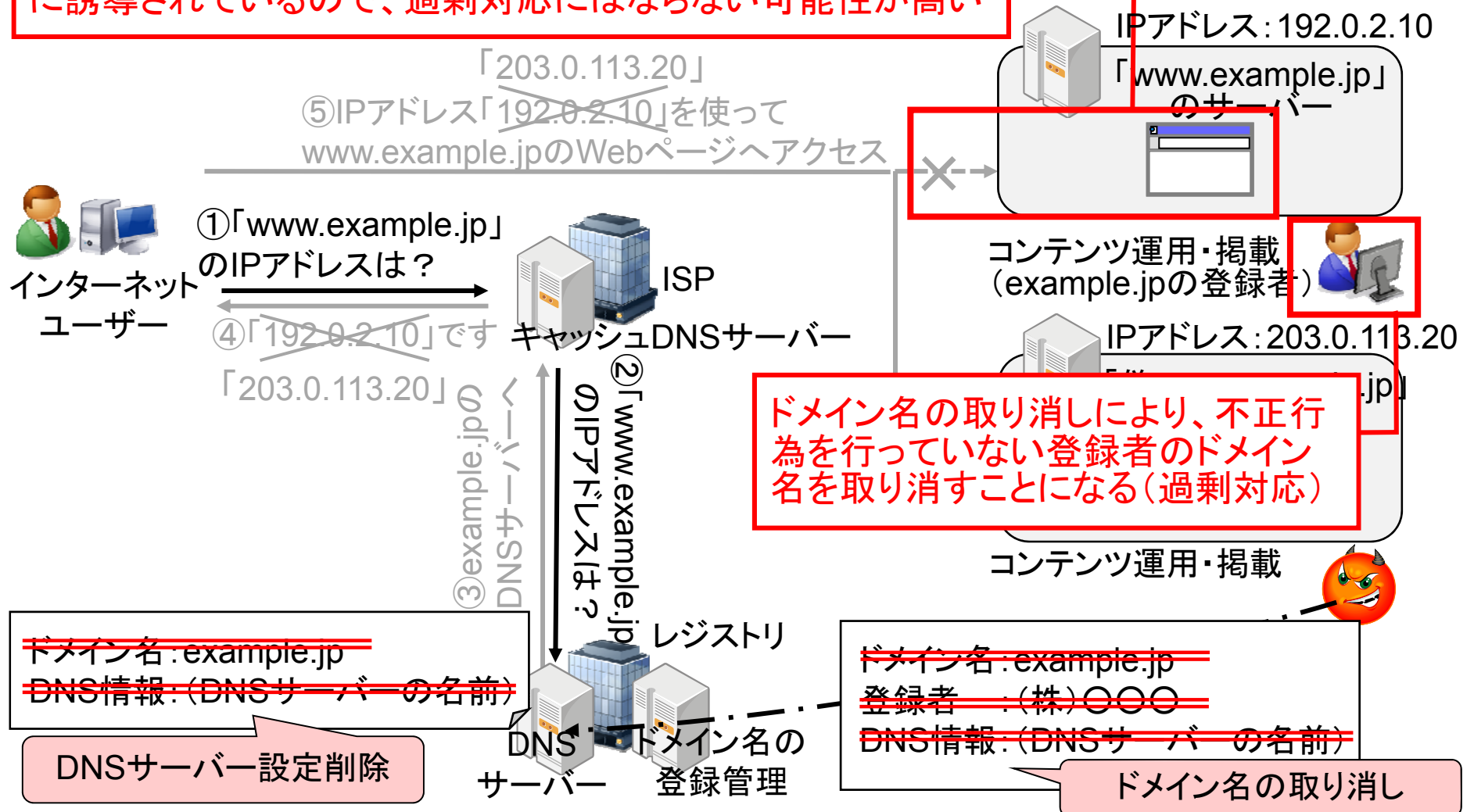
～不正行為者がドメイン名を乗っ取り不正なコンテンツに誘導～



類型(エ)へのレジストリの対応

～不正行為者がドメイン名を乗っ取り不正なコンテンツに誘導～

DNSサーバー設定削除を行っても、もともと不正なコンテンツに誘導されているので、過剰対応にはならない可能性が高い



不正行為に使われているJPDドメイン名への レジストリとしての対応における考慮点

- レジストリとしての対応(ドメイン名の取り消し、DNSサーバー設定削除)は、ドメイン名単位での使用停止
 - 過剰対応とならずに対応できるかどうかは、不正行為の種類ではなく、不正行為の方法の類型に依存する
 - 過剰対応の恐れから、すべての不正行為にレジストリとしての対応が有効とはならず、既存の他の対応を補完するものである

主な論点

次のような観点を踏まえ、不正行為に使われているJPDドメイン名へのレジストリとしての対応に関する方針及び留意点について議論をお願いしたい。

1. どのような不正行為を対象とすべきか。
2. 個別の事象が不正行為であるか否かを誰が判断すべきか。
3. 不正行為に使われているJPDドメイン名に対し、どのような連携・対応を行うべきか。

JPRSとしての連携・対応の一案

1. 広く通報を受け付けている通報相談機関と連携し、不正行為の情報を得る
 - 不正行為の申告窓口としてJPRSの認知を得ることは難しく、広く認知されている通報相談機関との連携が必須
2. 不正行為について適切な判断を行うことができる第三者機関と連携し、迅速に判断
 - この連携の枠組みが構築可能な不正行為より取り組む
3. 不正行為に用いられているJPDメイン名の管理指定事業者に連絡、適切な対応を依頼
 - 過剰対応を避けるため、不正行為の現場に近いところで対応
4. 過剰対応とならない範囲で対応可能なものについてはJPRSにてDNSサーバー設定を削除