DNS関連ホットトピックス

2014年2月1日
IPv6 Summit in SAPPORO 2014
株式会社日本レジストリサービス（JPRS）
森下 泰宏
@OrangeMorishita

事後資料（最終更新：2014年2月2日）

講師自己紹介

- 氏名: 森下 泰宏(もりした やすひろ)
  - 勤務先:株式会社日本レジストリサービス
  - 肩書: 技術広報担当
- 最近の願いごと:平穏無事な7月
  - 7月には毎年必ずDNSに関する何かが・・・

2008年	カミンスキー型攻撃手法公開
2009年	「BINDコロリ」(パケット一発でnamed死亡、回避手段なし)
2010年	ルートゾーン署名直後、BIND 9のDNSSEC実装に致命的なバグ発覚 (バリデーターが権威DNSサーバーに全力で問い合わせを送り続ける)
2011年	「BINDコロリ」パート2(パケット一発で(以下同文))
2012年	BIND 9とNSD 3にそれぞれ2件ずつ、Androidのリゾルバーに キャッシュポイズニング可能な脆弱性発覚(対象:約3億台)
2013年	7月最終週の土曜日早朝にBIND 9の致命的なゼロデイ脆弱性発表

本日の内容

1. DNS Response Rate Limiting（DNS RRL）の概要と現状
2. 第一フラグメント便乗攻撃（1st-fragment Piggybacking Attacks）の概要と対策
3. レジストリ・レジストラへの攻撃の現状

1. DNS Response Rate Limiting（DNS RRL）の概要と現状

Rate Limiting（レート制限）

- 単位あたりにおける何らかの数を制限
- Web技術の分野では従来から一般的
  - 単位時間あたりのAPI実行可能回数
  - 単位時間あたりのダウンロード可能回数
  - 1IPアドレスあたりの同時接続可能数、など

何らかの資源（CPU・ネットワークなど）を
使われすぎないようにするためによく用いられる

DNS Response Rate Limiting（DNS RRL）

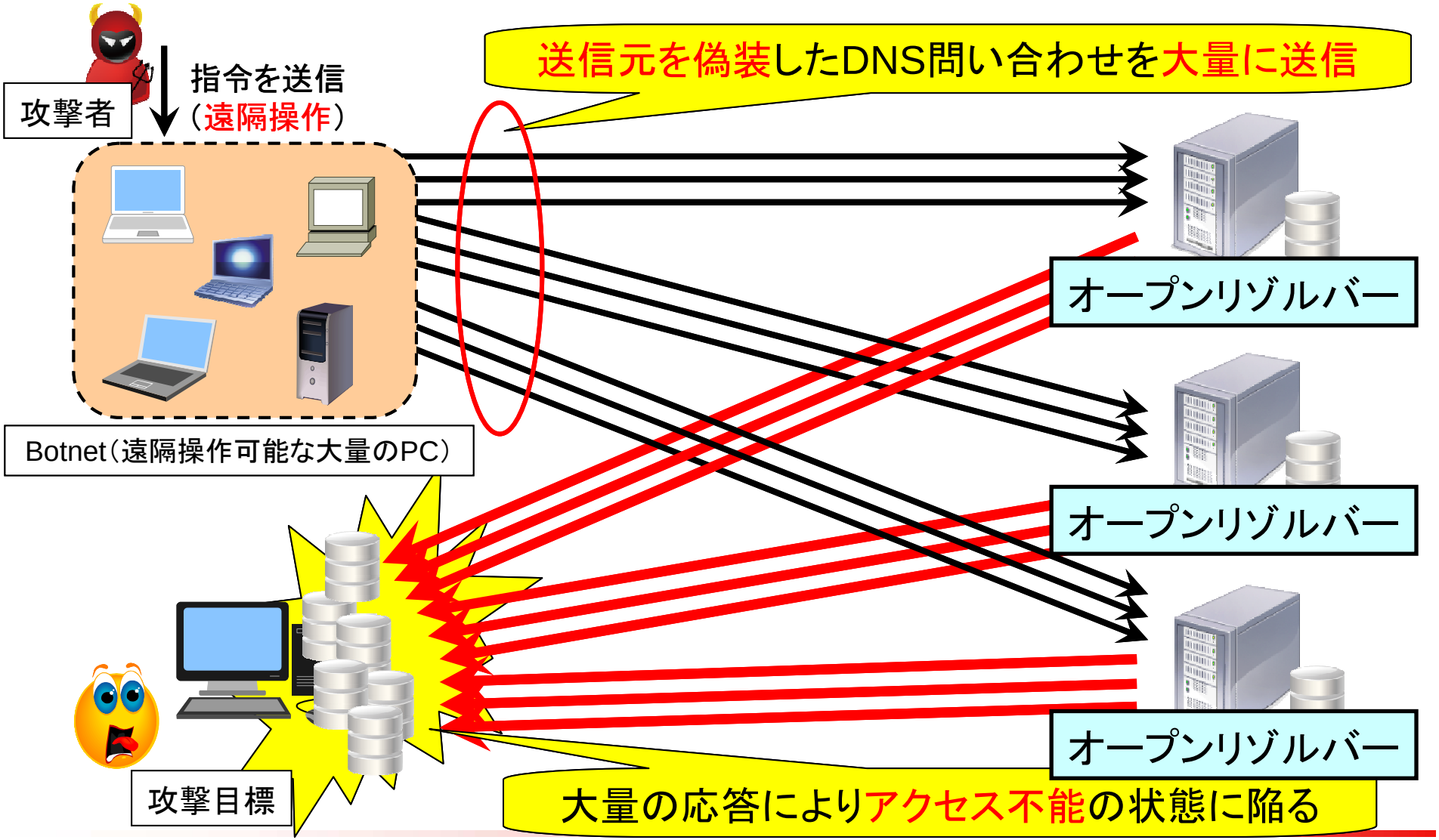
- DNSにおけるレート制限技術の一つ
- DNSの応答レートを制限
  - 単位時間あたりの応答回数
- DNSリフレクター攻撃対策の一つとして注目・導入され始めている

おさらい：DNSリフレクター攻撃

- 別名：DNSリフレクション攻撃、DNS Amp攻撃
  - JPRSではRFC 5358の表記に従い、2013年4月から「DNSリフレクター攻撃」と呼称
    - RFC 5358: Preventing Use of Recursive Nameservers in Reflector Attacks
      <http://www.ietf.org/rfc/rfc5358.txt>
- DNSの持つ特性を利用した攻撃手法

攻撃者が送信元（＝応答先）を偽装した問い合わせを
DNSサーバーに送信し、DNS応答を攻撃目標に送り
付けるように仕向ける攻撃手法

DNSリフレクター攻撃の例（大量の偽装問い合わせによるDDoS）



おさらい：オープンリゾルバー

- インターネット上のどこからの再帰検索要求であっても受け付け、処理してしまうDNSサーバー
  - 再帰検索要求：DNSクライアントからの名前解決要求
- DDoS攻撃の踏み台として悪用
  - 2013年3月には300Gbpsを超える攻撃が発生
    - Spamhaus/CloudFlareを狙った攻撃事例
- インターネット上に多数存在
  - 約2,700万台
    - 2014年1月現在：openresolverproject.org調べ

おさらい：オープンリゾルバー対策

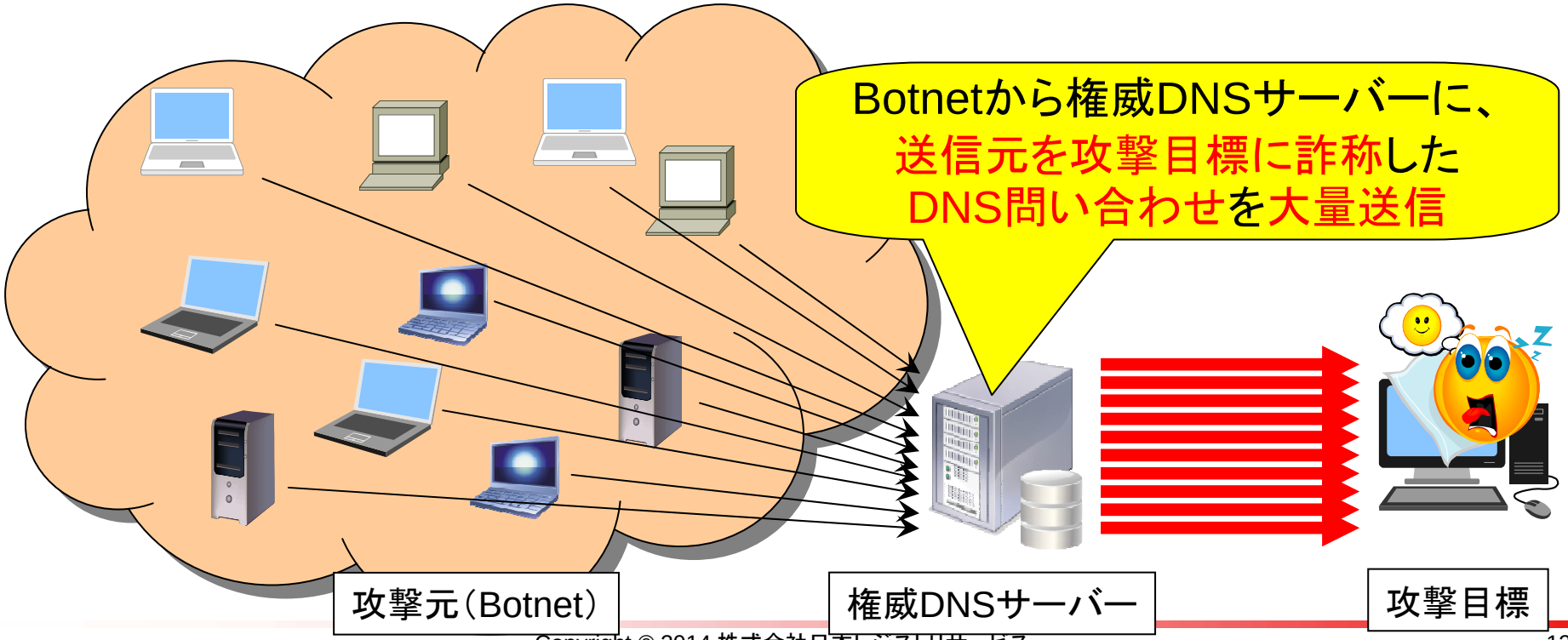
- オープンリゾルバーの出自に注目
  - 適切なアクセスコントロールがされていない キャッシュDNSサーバー
  - 適切な機能制限がされていない権威DNSサーバー
  - WAN側からの問い合わせも処理してしまうホームルーター
- 出自に応じた形で、不適切な状態の解消
  - キャッシュ・権威DNSサーバーを機能分離
  - キャッシュDNSサーバーにおける適切なアクセスコントロール
  - 権威DNSサーバーにおける適切な機能制限
  - ホームルーターのファームウェアやハードウェアの更新
- 本来の王道は「BCP 38/BCP 84の世界中での適用」
  - DNS以外のリフレクター攻撃にも有効

もう一つのDNSリフレクター攻撃

- 最近、オープンリゾルバーを用いたものに加え、権威DNSサーバーを用いたDNSリフレクター攻撃も観測され始めている
  - 2012年頃から、TLDの権威DNSサーバーなどを利用したDNSリフレクター攻撃の事例が報告され始めた
- 権威DNSサーバーの場合、不適切な設定のDNSサーバーでなくても、DNSリフレクター攻撃に利用可能
  - オープンリゾルバーの場合と異なる

権威DNSサーバーを用いた DNSリフレクター攻撃（1/2）

- 権威DNSサーバーのDNS応答を、リフレクター攻撃に直接利用
  - 攻撃の原理はオープンリゾルバーの場合と同様



権威DNSサーバーを用いたDNSリフレクター攻撃(2/2)

- DNSの応答サイズ自身が大きくなる傾向にある
  - DNSSEC、IPv6、SPF/DKIM、DANE(RFC 6698)への対応など
- ルートサーバーやTLDの権威DNSサーバーは、IP Anycast、広帯域回線、複数のトランジットなどの施策により、処理能力の強化が図られている
  - つまり、強力なリフレクターとなりうる
- 何らかの有効な対策を実施する必要がある
  - 権威DNSサーバーの特性に応じた対策が必要

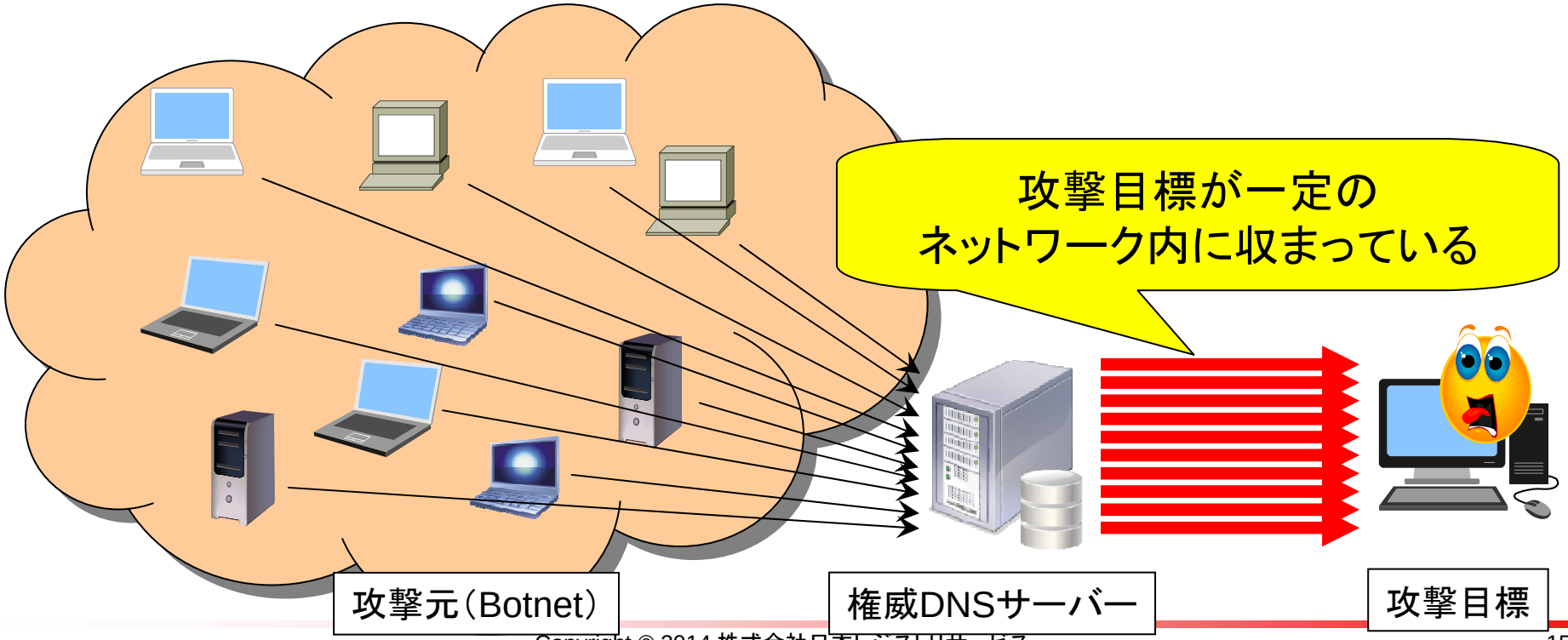
権威DNSサーバーの特性

- サービス対象がインターネット全体
  - キャッシュDNSサーバーの場合、組織/ISP内のみ
- アクセス制限による事前対策は不可能
  - キャッシュDNSサーバーではアクセス制限が可能
- キャッシュDNSサーバー（オープンリゾルバー）の場合とは別の対策方法を考慮・実施する必要がある

DNS Response Rate Limiting（DNS RRL）は、
そのための有力な対策の一つ

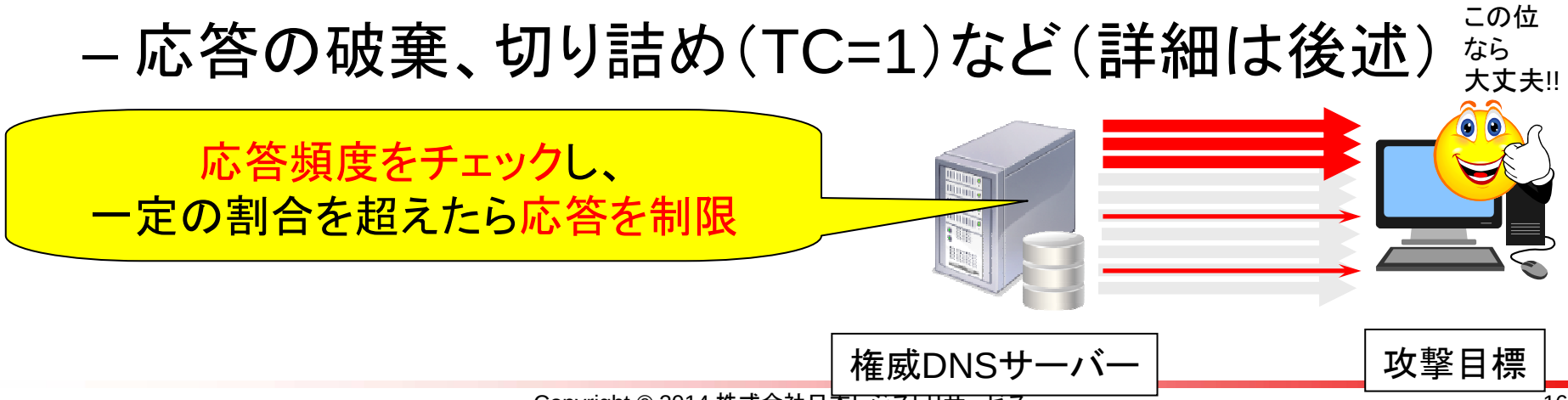
DNS RRLの仕組み（1/3）

- 攻撃目標（となるIPアドレス）が一定のネットワーク（IPアドレスブロック）内に収まっている点に着目



DNS RRLの仕組み（2/3）

- 事前に決めたルールにより、応答レートを制限
- 制限の方法：
  - あるIPアドレスブロック宛の、
  - 単位時間あたりの同一名に対する同一ステータスの応答が所定の頻度を超えた場合に、
- 所定の制限を発動させる
  - 応答の破棄、切り詰め（TC=1）など（詳細は後述）



DNS RRLの仕組み(3/3)

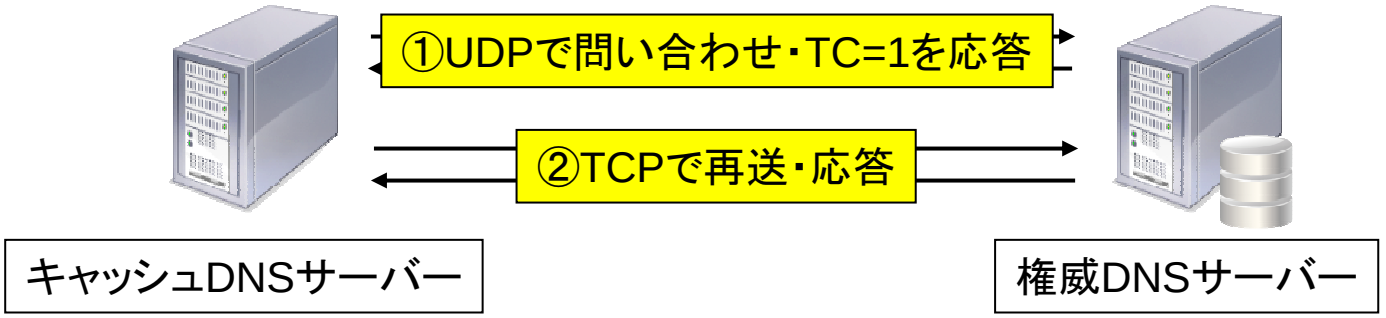
- 考え方:短時間のうちに、同じ宛先に同じ応答を何度も返すのはおかしい(はず) → 応答を返すのを制限
- DNS問い合わせは制限しない
  - 権威DNSサーバーの特性に対応
    - サービス対象がインターネット全体
- 「同じ応答」と判断する部分を工夫(不在応答対策)
  - サブドメインの不在応答(NXDOMAIN)は、同じ応答と判定
  - 例:jpゾーンを管理するJP DNSの場合
    - example1.jp、example2.jp、example3.jpのAレコードに対する応答(いずれもNXDOMAIN)を、同じ応答と判定
  - 名前を変えながら攻撃することを(ある程度)検知可能

False Positive発生の抑制(1/3)

- False Positive(偽陽性)
  - 本来検出すべきでない事象を誤検出してしまうこと
- DNS RRLのような検出型の攻撃対策では、False Positiveの発生をどのように抑制するかがポイントとなる
- DNS RRLでは、DNSプロトコルの仕組みを利用することでこの問題への対応を図っている
  - TCPフォールバックの仕組みを利用

False Positive発生の抑制(2/3)

- 制限の際応答の破棄に替え、DNS応答の切り詰めが発生(TC=1)した旨の応答を返す
  - この動作をslipと呼ぶ
- この応答を正当なキャッシュDNSサーバーに受信させることでTCPでの問い合わせ再送を促し、正常に名前解決させることを期待している



False Positive発生の抑制(3/3)

- slip設定では、サーバーの処理コスト・ネットワークの負荷・対False Positiveの観点でのトレードオフを考察する必要がある
  - 毎回slipを返すのは処理コスト・ネットワーク負荷の点で不利
- BIND 9のDNS RRLのデフォルトでは、該当する応答2回に1回の割合でslip応答を返す(slip:1/2)
  - slipの比率(分母を指定)は設定で変更可能

	応答の破棄	TC=1(slip)応答
サーバーの処理コスト	低	高
ネットワークの負荷	低	中
対False Positive	対応不可	対応可

DNS RRLが効果を発揮する状況

- 権威DNSサーバーにおいて特に効果を発揮
  - 問い合わせ元はキャッシュDNSサーバーである（はず）
  - キャッシュDNSサーバーにはキャッシュがある（はず）
  - TTL時間内は同内容の問い合わせを再送信しない（はず）
- キャッシュDNSサーバーへのDNS RRLの安易な導入は、サービスの提供に悪影響を及ぼす危険性あり
  - 導入できないわけではない
  - Google Public DNSでは、独自に実装したRRLを導入しているとのこと
    - <https://developers.google.com/speed/public-dns/docs/security?hl=ja#rate_limit>

DNS RRLの実装状況

- 権威DNSサーバーを中心に実装が進んでいる
  - BIND 9
    - 9.9.4以降においてRRLを標準実装
      - デフォルトでは無効、コンパイル時に--enable-rrlを指定
      - 9.10系では指定不要になる予定
    - それ以前のバージョンに対するパッチも提供
  - NSD
    - 3.2.15以降においてRRLを標準実装
      - デフォルトでは無効、コンパイル時に--enable-ratelimitを指定
  - Knot DNS
    - 1.2.0-rc3以降においてRRLを標準実装

DNS RRLの導入状況

- JP DNSサーバー
  - 2013年11月以降、DNS RRLを導入済
  - ただし、セキュリティ上の理由により具体的な設定内容（設定値など）は非公開
- JP DNSサーバーのほか、いくつかの著名な権威DNSサーバーにおいて導入済
  - かつ、効果を発揮した旨の報告あり

DNS RRLの注意点

- 実運用する際には運用ノウハウの蓄積や、各パラメーターのチューニング・リファインが必要
  - ドキュメントにもその旨の記述あり
  - ログオンリーモードで動作させ、各サーバーの状況に合わせてパラメーターをチューニングすることが有効
  - JP DNSサーバーにおいても検討・評価を事前実施
- 「いたちごっこ（cat-and-mouse game）」の技術
  - 攻撃者がより洗練された形（DNS RRLをかいくぐる）に攻撃方法を改良してくることが予想される

まとめ：DNS RRL

- 権威DNSサーバーにおいて特に効果を発揮
  - キャッシュDNSサーバーへの安易な導入は、サービスの提供に悪影響を及ぼす危険性あり
- 有力かつ巧妙な仕組みであると言える
  - DNSの動作の細部に至るまで緻密に考慮されている
- ただし、実運用にはノウハウの蓄積や、状況に応じた各パラメーターのチューニング・リファインが必要
  - 枯れている技術であるとは（まだ）言えない
- 「いたちごっこ」の技術であり、RRLを回避する形での攻撃方法の洗練が予想される

参考リンク（DNS RRL関連技術資料）

- JPRSの技術解説
  - 「DNS Reflector Attacks（DNSリフレクター攻撃）」について
    <http://jprs.jp/tech/notice/2013-04-18-reflector-attacks.html>
- DNS RRLの技術仕様
  - DNS Response Rate Limiting (DNS RRL)
    <http://ss.vix.su/~vixie/isc-tn-2012-1.txt>
- W. Matthijs Mekking氏（NLnet Labs）の発表資料
  - DNS Rate Limiting
    <http://www.guug.de/veranstaltungen/ffg2013/talks/DNS_Rate_Limiting__Matthijs_Mekking.pdf>
- 山口崇徳氏（IIJ）の発表資料
  - DNS Response Rate Limiting (DNS RRL)
    <http://www.dnsops.jp/event/20130529/dnssec2013springforum-yamaguchi-1.pdf>

2. 第一フラグメント便乗攻撃（1st-fragment Piggybacking Attacks）の概要と対策

第一フラグメント便乗攻撃（1st-fragment Piggybacking Attacks）とは

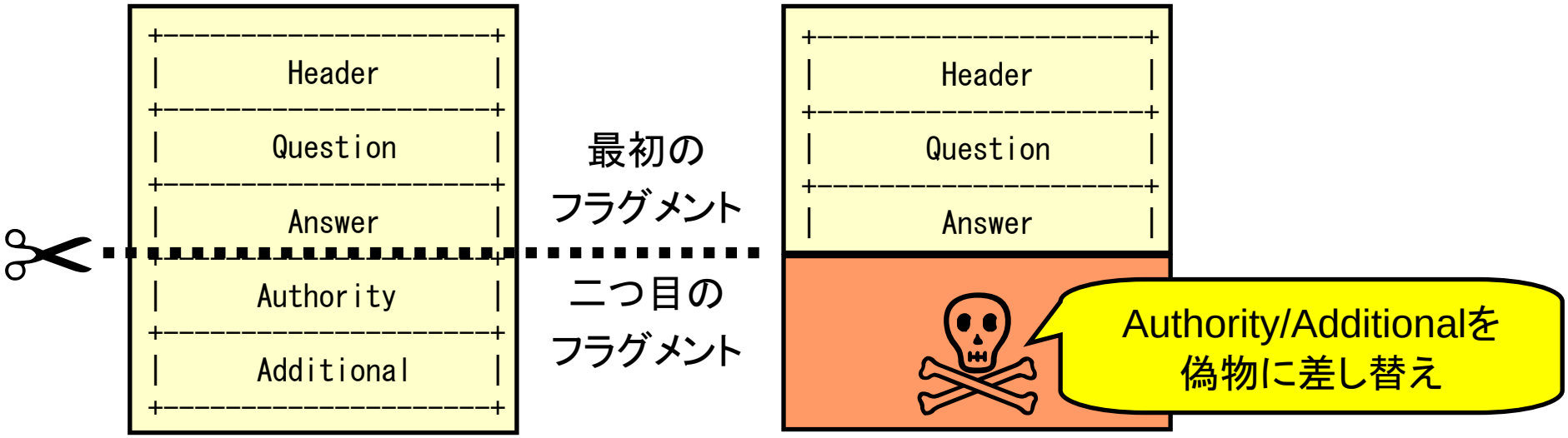
- イスラエル・バル＝イラン大学のAmir Herzberg教授とHaya Shulman氏により発表された論文において初めて報告（2012年5月17日公開）
  - Fragmentation Considered Poisonous
    <http://arxiv.org/abs/1205.4011>
- 発表直後は大きな話題とはならず
  - DNS関係者の間で認識されていなかった可能性あり

第一フラグメント便乗攻撃とは（続き）

- その後、IETF 87 saag（Security Area Advisory Group）の招待講演において、Shulman氏がこの攻撃の詳細を発表（2013年8月1日）
  - DNS Cache-Poisoning: New Vulnerabilities and Implications, or: DNSSEC, the time has come!
    <http://www.ietf.org/proceedings/87/slides/slides-87-saag-3.pdf>
- 発表から1カ月後あたりから、dns-operationsメーリングリスト（dns-oarc.net）で大きな話題に
  - [dns-operations] DNS Attack over UDP fragmentation
    <https://lists.dns-oarc.net/pipermail/dns-operations/2013-September/010625.html>
  - 100通以上の投稿

攻撃の概要

- IPフラグメンテーションの仕様を悪用した、新たなDNSキャッシュポイズニング攻撃手法
  - フラグメントされたUDPのDNS応答が攻撃対象
- 応答の二つ目（以降）のフラグメントを偽物に差し替えることで、応答のAuthority/Additionalを偽物に差し替え

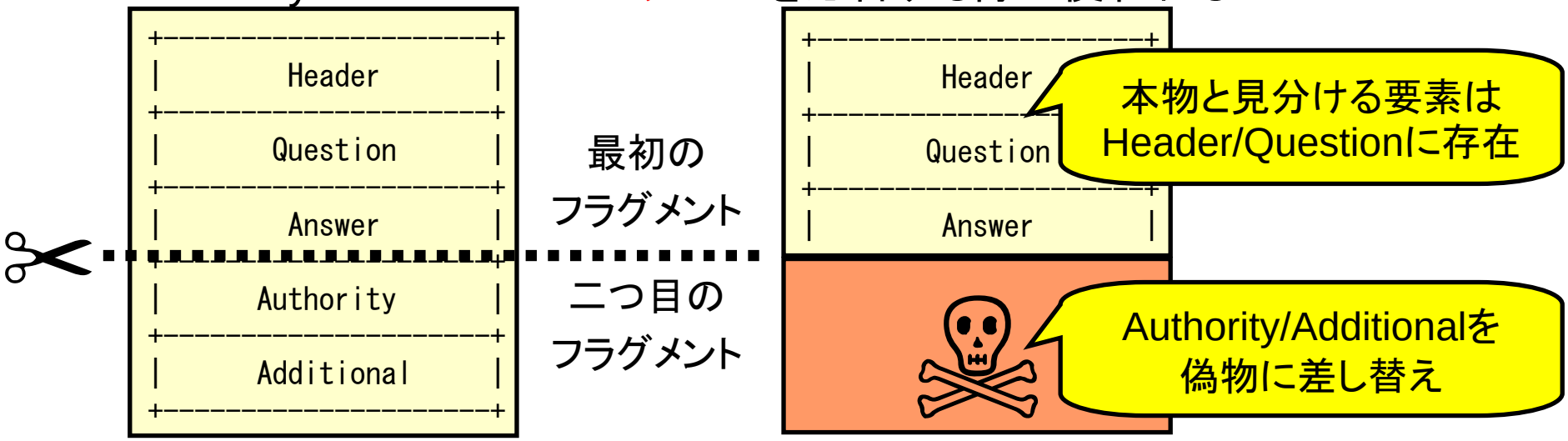


おさらい：IPフラグメンテーション

- IPにおいて1回で送れる最大の単位（MTU）よりも大きなデータを送る場合に発生
  - 経路（Path）MTUより大きなUDPパケットの送信時に必ず発生
- IPの仕様上有害であることは古くから認識
  - Fragmentation Considered Harmful（1987年）
    <http://www.hpl.hp.com/techreports/Compaq-DEC/WRL-87-3.pdf>
- DNSでは、フラグメンテーションが起こり得る大きなUDPパケットをDNS応答で使用
  - EDNS0（RFC 2671 → RFC 6891）

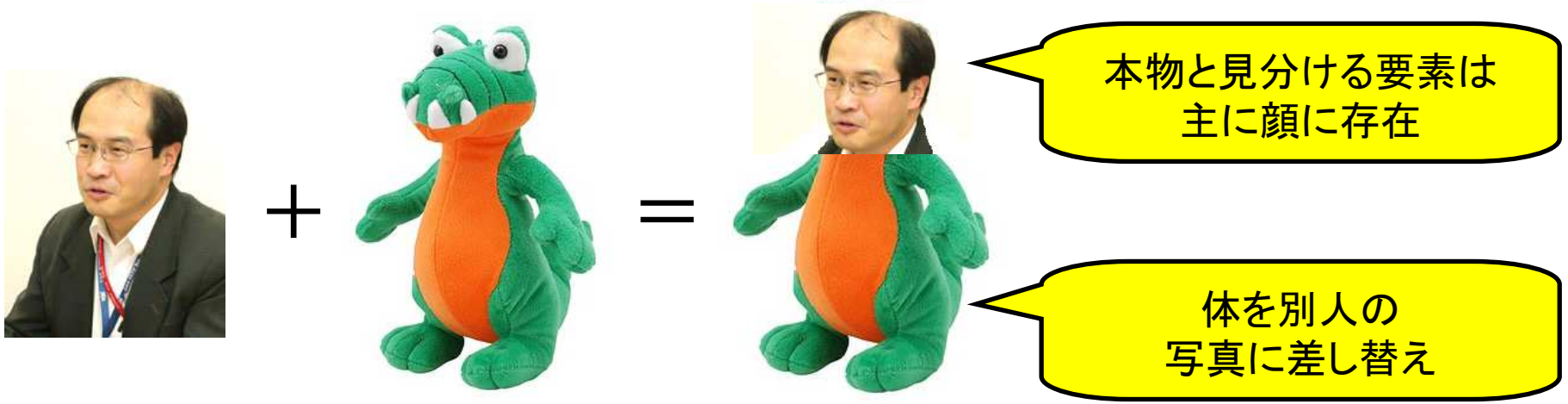
攻撃のポイント（DNSにおける従来の対策の無効化）

- DNS応答の同定に使える要素が、最初のフラグメントにしか存在しなくなることを悪用
  - ポート番号（UDPヘッダー）
  - 問い合わせID、問い合わせ名（Header/Question）
- Authority/Additionalを偽物に差し替えることで、偽の権威DNSサーバー（NS）に誘導させられる危険性あり
  - Authority/AdditionalはNS/グルーを応答する際に使われる



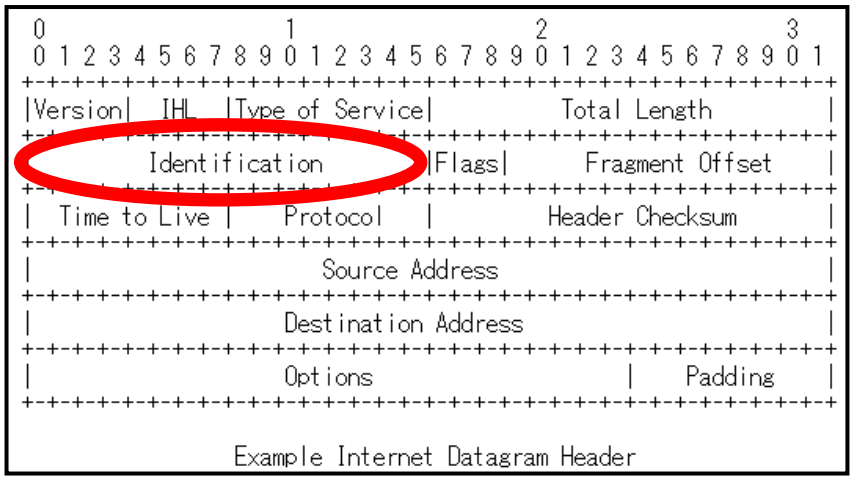
人物のコラージュ作成に類似

- 人物のコラージュを作成する行為に類似
- 人物を見分ける要素が主に顔にのみ存在することを利用、体を別人の写真に差し替え
  - 顔はむしろ、本物であると判定させることに活用



IPフラグメンテーションの弱点（Identificaionフィールドの仕様（IPv4））

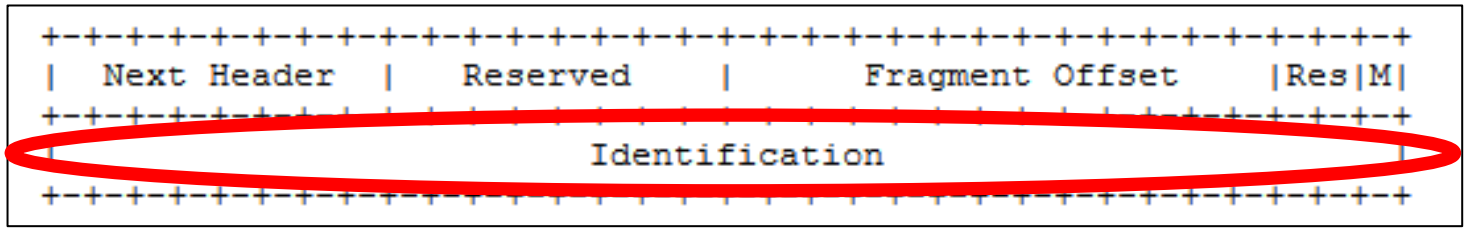
- リアセンブリーにおいて使用されるIdentificationフィールドの大きさが、IPv4では16ビットしかない
  - 二つ目のフラグメントを2の16乗個作成して送り込む、総当たり攻撃が成立しうる
- ただし、二つ目のフラグメントを大量に送りつけられたOSのプロトコルスタックが具体的にどう振舞うかは未確定



Example Internet Datagram Header（RFC 791より引用）

IPフラグメンテーションの弱点（Identificaionフィールドの仕様（IPv6））

- IPv6ではIdentificationフィールドの大きさは32ビットだが、これだけで安全であるとは言えない
  - その理由は・・・



IPv6 Fragment Header（RFC 2460より引用）

IPv6のIdentificationフィールドの仕様

- IPv6の仕様（RFC 2460 4.5 Fragment Header）には、以下の記述がある
  - Rather, it is assumed that the requirement can be met by maintaining the Identification value as a simple, 32bit, "wrap-around" counter, incremented each time a packet must be fragmented. It is an implementation choice whether to maintain a single counter for the node or multiple counters, e.g., one for each of the node's possible source addresses, or one for each active (source address, destination address) combination.
- つまり、RFC 2460に従った実装では、Identificationの値が外部から予測可能となる場合がある

Identificationを予測可能な実装

- Fernando Gont氏による調査結果
  - Identificationの値が外部から予測可能な実装が複数存在
  - “Security Implications of Predictable Fragment Identification Values” Appendix B.
    （draft-ietf-6man-predictable-fragment-id-00）
- OSごとの実装状況（上記I-Dより引用）
  - 予測不能：FreeBSD 9.0、Linux-current、NetBSD 5.1、OpenBSD-current
  - 予測可能：Linux 3.0.0-15、Solaris 10、Windows XP SP2、Windows Vista (Build 6000)、Windows 7 Home Premium
- 予測可能な場合、総当たり攻撃が不要になる

CVE-2011-2699

事後資料で追加（2014年2月2日）

- Linux 3.1以前のIPv6のIdentificationが予測可能な脆弱性は、CVE-2011-2699として報告、Linux 3.2以降で対策済
  - ipv6: make fragment identifications less predictable
    <https://github.com/torvalds/linux/commit/87c48fa3b4630905f98268dde838ee43626a060c>
  - JVNDB-2012-002538 Linux Kernel の IPv6 の実装における サービス運用妨害 (ネットワーク障害) の脆弱性
    <http://jvndb.jvn.jp/ja/contents/2012/JVNDB-2012-002538.html>
- RHEL 5/6には上記修正がバックポートされており、対策済
  - Bug 723429 – CVE-2011-2699 kernel: ipv6: make fragment identifications less predictable
    <https://bugzilla.redhat.com/show_bug.cgi?id=723429>
- CentOS 6.5にも同様の対策が適用されているとのこと
  <https://twitter.com/hdais/status/429560330948071424>

IPフラグメンテーションの弱点（先回り攻撃による確率の向上）

- 二つ目の偽フラグメントを一つ目のフラグメントよりも先に送り込む「先回り」攻撃が可能
  - 攻撃者が攻撃対象の名前解決をトリガーできる場合（オープンリゾルバーや接続先ISPのキャッシュDNSサーバーを攻撃する場合など）において、
  - DNS問い合わせの直後に偽造した二つ目のフラグメントを送り込むことで、
  - 本物のフラグメントよりも（そして、一つ目のフラグメントよりも！）確実に先回りさせられる
  - つまり、攻撃成功（毒入れ）の確率を上げられる

IPフラグメンテーションの弱点（DNSサーバーの応答ログ）

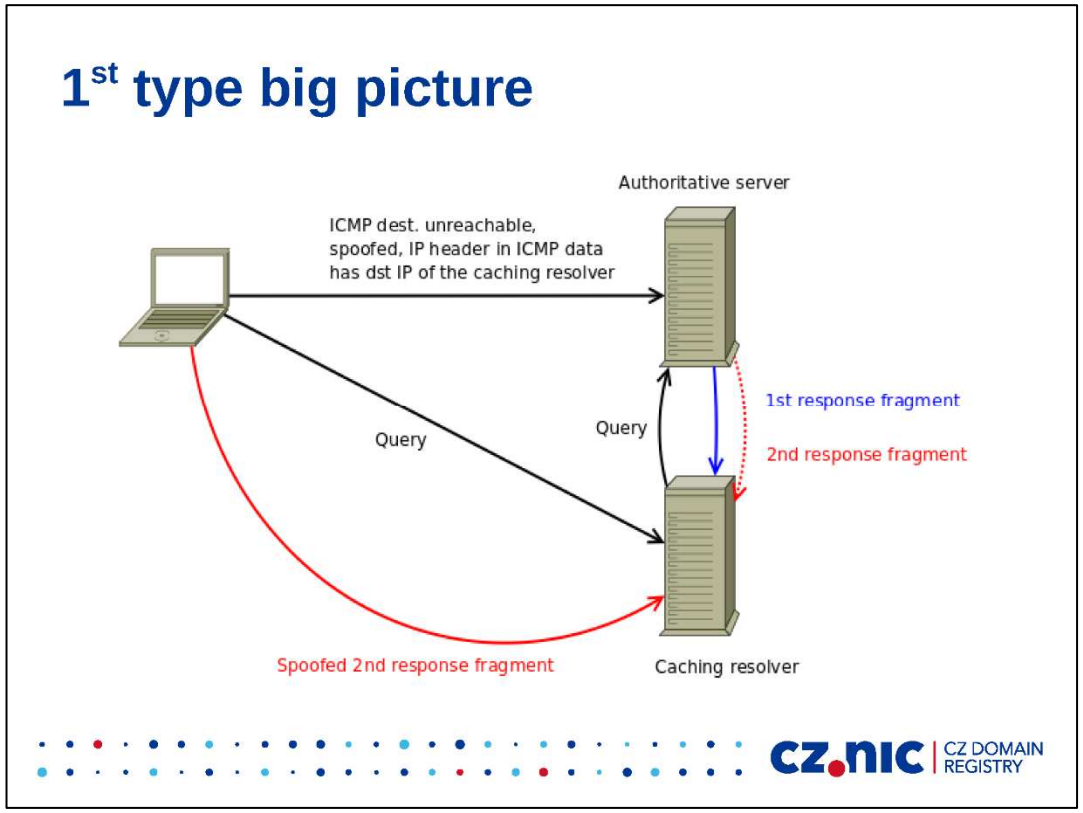
- キャッシュDNSサーバーの応答ログには、攻撃の痕跡が残らない
  - リアセンブリーされなかったフラグメントはIP層で捨てられ、リアセンブリーされた応答のみが上位層に到達する
  - これに対し、カミンスキー型攻撃手法では複数のDNS応答が上位層に到達するため、攻撃の痕跡が残る
- IP/データリンク層には痕跡が残る
  - netstatコマンドやtcpdumpコマンドなどである程度、確認可能

二種類の攻撃手法（アタックベクター）

- 大きなDNS応答を狙う
  - Shulman氏の論文に書かれている方法
    - DNSSECに対応したドメイン名のDNSKEY RR
    - 登録済ドメイン名に長い名前のNSを多数登録
- IPフラグメンテーションを意図的に発生させる
  - 2013年10月のRIPE Meetingにおいて、CZ.NICのT. Hlavacek氏が発表した方法
    - IP fragmentation attack on DNS
      <https://ripe67.ripe.net/presentations/240-ipfragattack.pdf>
    - ICMPを偽造し、事前送信

ICMPの偽造と事前送信

- 偽のICMP PacketTooBigを事前送付してMTUが小さいとOSに誤認させ、応答パケットをフラグメントさせる



引用元：IP fragmentation attack on DNS <https://ripe67.ripe.net/presentations/240-ipfragattack.pdf>

攻撃成立の必要条件

- ip_off（フラグメントオフセット）の確定（予測）
  - 応答の内容とMTUがわかれば確定可能
  - コラージュにおける「つなぎ目が不自然にならないようにする」ことに相当
- チェックサムの調整（同じ値になるように）
  - ペイロードやヘッダーの一部を工夫することで調整可能
  - NAT66（RFC 6296）において同様の調整を採用済
  - コラージュにおける「全体として違和感なくつなげられる体（フラグメント）」を準備しておくことに相当

上記二つはいずれも、不可能な条件ではない

これまでに提案・実装された対策

- DNSSECの導入
- IPフラグメンテーションの仕様拡張
- キャッシュDNSサーバーにおける対策
- 権威DNSサーバーにおける対策
- UDPにおける最大ペイロード長の抑制
- DNSメッセージサイズの抑制
- Linuxカーネルにおける機能拡張

対策：DNSSECの導入

- DNSSECの導入により、「コラージュ済み」応答が不正なものであると検知できるようになる
  - キャッシュポイズニング攻撃は成立しなくなる
- 現在のDNSSECの実装では不正な応答を検知した場合、即座にSERVFAILエラーになる
  - 意図的なDoS攻撃（当該の名前へのアクセス妨害）は、現在のDNSSECの実装では防止不可
    - DNSSECの本来の仕様

対策：IPフラグメントの仕様拡張

- IPフラグメントの仕様を拡張する
  - IPv6 Stateless Fragmentation Identification Options（draft-andrews-6man-fragopt）
- コラージュに対し「体（フラグメント）にも顔と同じ効力を持つ目印を付け、受け取り側でチェックする」ことに相当
  - 非現実的

対策：キャッシュDNSサーバーの実装

- キャッシュポイズニングの影響を小さくする
  - 応答のauthority sectionに設定されたNSレコードのホスト名に、ランダムなprefixを付けてキャッシュする
    - additional sectionに付与されるグルー（A/AAAA）も、それに併せて変更する
  - 上記により、NS/グルーが同一であっても、各委任先ゾーンごとに別扱いになるようにする
- Google Public DNSにおいて採用済
  - カミンスキー型攻撃手法への対策として導入
    - Security Benefits - Public DNS — Google Developers <https://developers.google.com/speed/public-dns/docs/security#nonce_prefixes>

対策：権威DNSサーバーの実装

- 応答にランダムなRRを付与する
- EDNS0のバッファーサイズを毎回変更する
  - いずれの対策も「コラージュを成立しにくくするため、継ぎ目を一定でなくす」ことに相当

対策：最大ペイロード長の抑制

- DNSのUDPにおける最大ペイロード長を、IPフラグメンテーションが発生しない大きさに抑制する
  - max-udp-size（BIND 9）やudp-max-size（Unbound）など
- 現在のデフォルト値はBIND 9/Unboundともに4096
  - DNSSEC（RFC 4035）では「少なくとも1220のサポート必須」「4000をサポートすべき」と規定
- 設定値の参考となるもの
  - 1220：DNSSEC対応リゾルバーにおける、最小のEDNS0バッファーサイズ（RFC 4035）
  - 1280～1410：EDNS0（RFC 6891）における「Ethernetにおけるリーズナブルな値」

対策：DNSメッセージサイズの抑制

- DNSSECの鍵や署名をできるだけ短くする
  - 鍵長やロールオーバーの方式を工夫する
    - JP DNSサーバーに設定されるDNSSEC関連情報の内容一部変更について
      <http://jprs.jp/tech/notice/2011-07-29-jpdns-dnskey-and-rrsig-change.html>
  - アルゴリズムとしてECDSA（楕円関数）を使用する
    - すべてのバリデーターが楕円関数に対応しているわけではないことに注意

対策：Linuxカーネルにおける機能拡張

- PMTUDの結果を無視するソケットオプションを新設
  - これにより、偽のICMP PacketTooBigを受け入れないように設定可能
- Linux-currentに導入済
  - Linux 3.14においてリリース版にも導入予定
- 想定される使用方法
  - max-udp-size 1220などによりフラグメントが起こらない状態に設定
  - かつ、このソケットオプションを使用し、偽のICMP Packet too Bigを受け入れないように設定
- 参考：dns-operations ML投稿されたサマリー
  - [dns-operations] summary of recent vulnerabilities in DNS security.
    <https://lists.dns-oarc.net/pipermail/dns-operations/2014-January/011249.html>

IPフラグメンテーション回避による影響

- IPフラグメンテーションを回避する設定を各DNSサーバーに適用した場合、TCPの問い合わせ数の増加が予想される
- ルートサーバーやJP DNSサーバーなどの負荷増大につながる
  - どの程度増加するのかについては検証が必要
- IP Anycastの運用に影響を与える可能性がある
  - どの程度影響があるのかについては検証が必要

まとめ：第一フラグメント便乗攻撃（1/4）

- IPフラグメンテーションの仕様を悪用
  - DNS応答の二つ目（以降）のフラグメントを差し替え
- DNS応答の同定に使える要素を無効化
  - 同定に使える要素は最初のフラグメントに存在
- IPフラグメンテーションの弱点
  - Identificationフィールドの仕様（IPv4/IPv6）
  - 先回り攻撃
  - DNSサーバーの応答ログ

まとめ：第一フラグメント便乗攻撃（2/4）

- 二つの攻撃手法（アタックベクター）
  - 大きなDNS応答を狙う
    - DNSKEY RR、長い名前のNSレコード
  - IPフラグメンテーションを意図的に発生させる
    - 偽のICMP PacketTooBigを送付

まとめ：第一フラグメント便乗攻撃（3/4）

- 提案・実装された対策
  - DNSSECの導入
  - IPフラグメンテーションの仕様拡張
  - DNSサーバー実装における工夫
    - キャッシュDNSサーバー
    - 権威DNSサーバー
  - IPフラグメンテーションの回避
    - UDPにおける最大ペイロード長の抑制
    - DNSメッセージサイズの抑制
    - OSカーネル（プロトコルスタック）における対策

まとめ：第一フラグメント便乗攻撃（4/4）

- IPフラグメンテーション回避による影響
  - TCPの問い合わせ数の増加
  - ルート/TLDのサーバーの負荷増大
  - IP Anycastの運用への影響の可能性

3. レジストリ・レジストラへの攻撃の現状

登録情報に対する攻撃

- 最近、レジストリ･レジストラの登録情報に対する攻撃事例が発生している

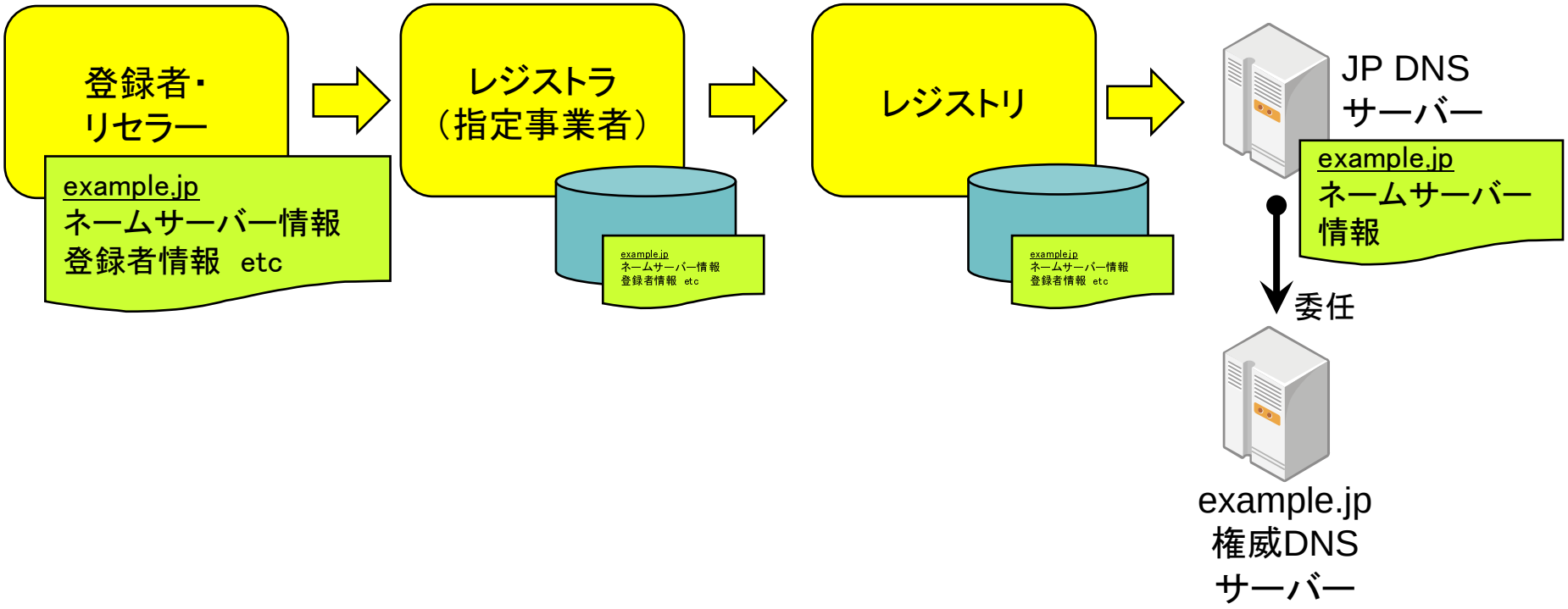
具体的には
NSレコードの
不正書き換え

```
Domain Information: [ドメイン情報]
[Domain Name]                   JPRS.JP

[登録者名]                      株式会社日本レジストリサービス
[Registrant]                    Japan Registry Services Co.,Ltd.

[Name Server]                   ns1.jprs.jp
[Name Server]                   ns2.jprs.jp
[Name Server]                   ns3.jprs.jp
[Signing Key]                   13747 8 2 (
                                DCD3F2BD0CB8A555CFC4D0866029A25C
                                4F79CEE38846DDE0A2B96AD6B6D7FD6B )
[Signing Key]                   13747 8 1 (
                                63000ECBA3DAD01FC3DFEA7DB67578DE
                                480EE0EB )

[登録年月日]                    2001/02/02
[有効期限]                      2014/02/28
[状態]                          Active
[最終更新]                      2013/03/01 01:05:07 (JST)

Contact Information: [公開連絡窓口]
[名前]                          株式会社日本レジストリサービス
[Name]                          Japan Registry Services Co.,Ltd.
[Email]                         dom-admin@jprs.co.jp
```

登録情報の例

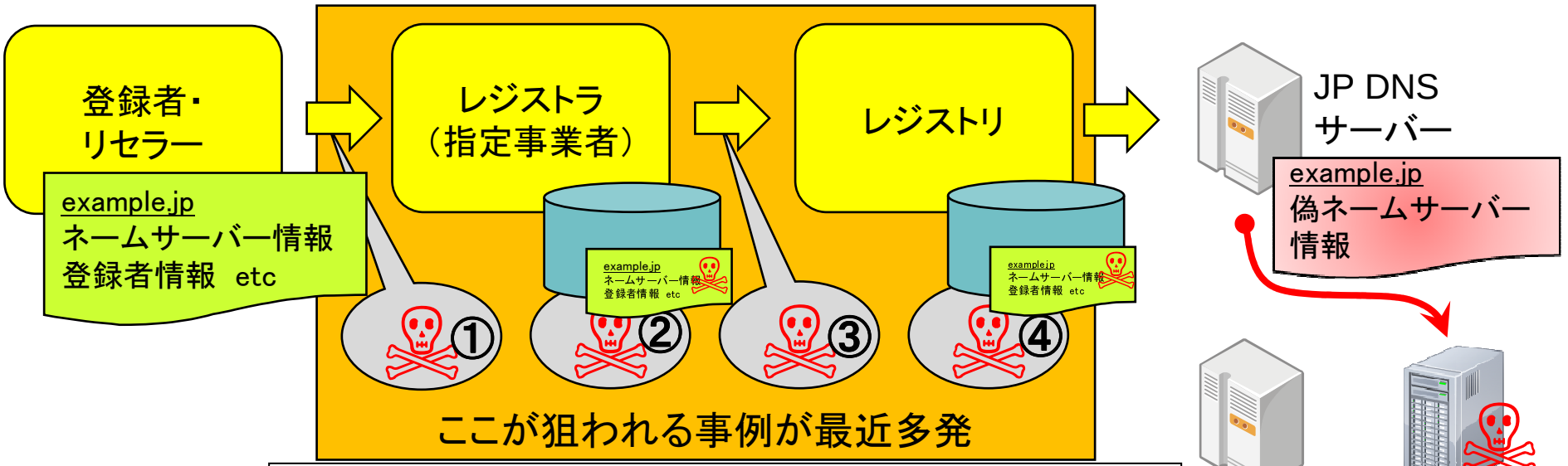
おさらい：登録情報の流れ

- 登録者（リセラー）⇒レジストラ⇒レジストリ
- レジストリが登録情報から、自身が管理する権威DNSサーバーを設定



登録情報の不正書き換え

- 流れのどこかで登録情報を不正に書き換え
- レジストリ･レジストラが狙われる事例が最近多発



例：
①登録者になりすまして、レジストラのデータベースを書き換え
②レジストラのシステムの脆弱性を突き、データベースを書き換え
③レジストラになりすまして、レジストリのデータベースを書き換え
④レジストリのシステムの脆弱性を突き、データベースを書き換え

最近の攻撃事例（2012年10月以降）

年月	対象TLDレジストリ、レジストラ
2012年10月	.ie（アイルランド）
2012年11月	.pk（パキスタン）、.ro（ルーマニア）
2012年12月	.rs（セルビア）
2013年1月	.tm（トルクメニスタン）、 .lk（スリランカ）
2013年2月	.pk（パキスタン、2回目）、 .mw（マラウイ）、.edu（gTLD）
2013年3月	.bi（ブルンジ）、.gd（グレナダ）、 .tc（英領タークス・カイコス諸島）、 .vc（セントビンセントおよび グレナディーン諸島）
2013年4月	.kg（キルギスタン）、.ke（ケニア）、 .ug（ウガンダ）、.ba（ボスニア）、 .om（オマーン）、.mr（モーリタニア）

注：JPRSにおいて把握しているもののみ

年月	対象TLDレジストリ、レジストラ
2013年5月	.mw（マラウイ、2回目）
2013年7月	.my（マレーシア）、 .nl（オランダ）、 .be（ベルギー、同一月内に2回、 登録情報には被害なし）、 Network Solutions（gTLDレジストラ、 登録情報には被害なし）
2013年8月	.nl（オランダ、2回目）、 .ps（パレスチナ）、 Melbourne IT（gTLDレジストラ）
2013年9月	.bi（ブルンジ、2回目）、 .ke（ケニア、2回目）
2013年10月	Network Solutions（gTLDレジストラ）、 Register.com（gTLDレジストラ）、 .my（マレーシア、2回目）、 .cr（コスタリカ）、.qa（カタール）、 .rw（ルワンダ）
2014年1月	.me（モンテネグロ）

主な被害（1/4）

- .tm、.lk（2013年1月）
  - 登録者の電子メールアドレスと平文パスワードが流出
    - .tm：約5万件、うち.jpのメールアドレス約1000件
    - .lk：約1万件
  - 原因：登録画面のSQLインジェクション脆弱性
- .edu（2013年2月）、.nl（2013年7月）
  - 全登録者・レジストラのパスワードの強制リセット
  - パスワードファイルの外部流出が疑われたため
    - 同年1月末のmit.eduのドメイン名ハイジャック事例との関連性
    - 同年8月の.nlの事例（後述）との関連性

主な被害（2/4）

- .nl（2013年8月）
  - あるレジストラのパスワードがクラック
    - レジストラが管理するドメイン名数千件がハイジャックの被害に
  - マルウェア配布サイトに誘導
    - ドライブ＝バイ＝ダウンロードの手法を利用
      （当該Webページを開いただけでマルウェアを強制ダウンロード）
  - 前回（2013年7月）の事件で流出したID/ハッシュパスワードがクラックに使われた可能性あり（未確認）
    - 流出したパスワードは.nlレジストリ（SIDN）により強制変更済
    - パスワードを元に戻したレジストラがあった可能性

主な被害（3/4）

- Melbourne IT（2013年8月）
  - 「シリア電子軍」を名乗る者による犯行
  - あるリセラーのアカウント情報を盗まれ、リセラーの登録システムに不正侵入
  - リセラーの登録システムに存在した脆弱性を突き、本来は書き換えることのできない、別アカウントが管理するドメイン名登録情報を不正書き換え
    - nytimes.com、twimg.comなどがドメイン名ハイジャックの被害に
  - 不正書き換えされたNSレコードのTTLが長かったため、DNSキャッシュが長時間にわたって残存し、影響が長時間に及んだ

主な被害（4/4）

- Network Solutions、Register.com（2013年10月）
  - パレスチナに関する政治的声明が書かれたWebページにアクセスを誘導
  - アンチウイルスベンダー・著名なWebサービス・セキュリティベンダーなどが被害に
    - avira.com, avg.com
    - alexa.com, leaseweb.com, redtube.com, whatsapp.com
    - metasploit.com, rapid7.com
  - レジストラへのFAXによりメールアドレス設定・パスワードをリセットする手口が使われた
    - レジストラのサービスを悪用

攻撃の特徴(1/2)

- いわゆるドメイン名ハイジャックがほとんどを占める
  - NSレコードの不正書き換え
- 著名な(インパクトの大きい)ドメイン名が狙われやすい
  - google.TLD、yahoo.TLD、microsoft.TLDなど
- 主な手口は既知の(防御可能な)脆弱性の悪用や、ソーシャルエンジニアリングによるアカウントの盗難など
- 現時点では、攻撃者による示威行為が主流
  - 「Hacked by ○○○○」といったページ、政治的メッセージを表示するページなどへの転送
- 利用者からのクレームにより状況が発覚
  - 登録情報の切り戻しにより、数時間～1日程度で復旧

攻撃の特徴(2/2)

- 運営基盤の弱いレジストリやレジストラが狙われやすい
  - しばらくはこの傾向が続くと考えられる
- 一度やられた組織が再度やられるケースがある
  - 根本的な脆弱性対策を実施せずサービスを再開
  - 別の脆弱性を狙われる場合もあり
- レジストラ・リセラーが標的になるケースがある
  - レジストリ・レジストラだけでは防ぎきれない
- DNSSECでは防げない
  - DNSSECの設定も書き換え可能

有効な対策・ポイント（1/2）

- 基本はWebセキュリティにおける対策と同様
  - 多くの攻撃は既知の脆弱性を悪用したもの
  - 既知の脆弱性は必ず対策しておくこと
  - ソーシャルエンジニアリングにも注意
- 著名なドメイン名の登録情報の変更に注意
  - 著名な企業・団体や政府機関など

有効な対策・ポイント(2/2)

- チェック機構を活用することも有効
  - メールなどによる事前警告、人による事前チェックなど
- 一部のTLDでは「レジストリロック」を活用可能
  - 通常の方法での登録情報変更を禁止する仕組み
- DNSSEC関連の設定変更には要注意
  - DSレコードの削除・書き換え
  - 不正書き換えの早期発見につながる可能性

JPRSにおける取り組み

- 脆弱性情報の収集と対応
- システムに対する脆弱性試験の実施
- 情報提供・広報・注意喚起
  - 今している発表（まさに！）
  - 指定事業者に認証情報管理の徹底を注意喚起
- レジストリロックの導入検討

Q and A