InternetWeek 2022
ドメイン名ライフサイクルマネージメント

インターネット資源の組織内管理について ～ComNICご紹介～

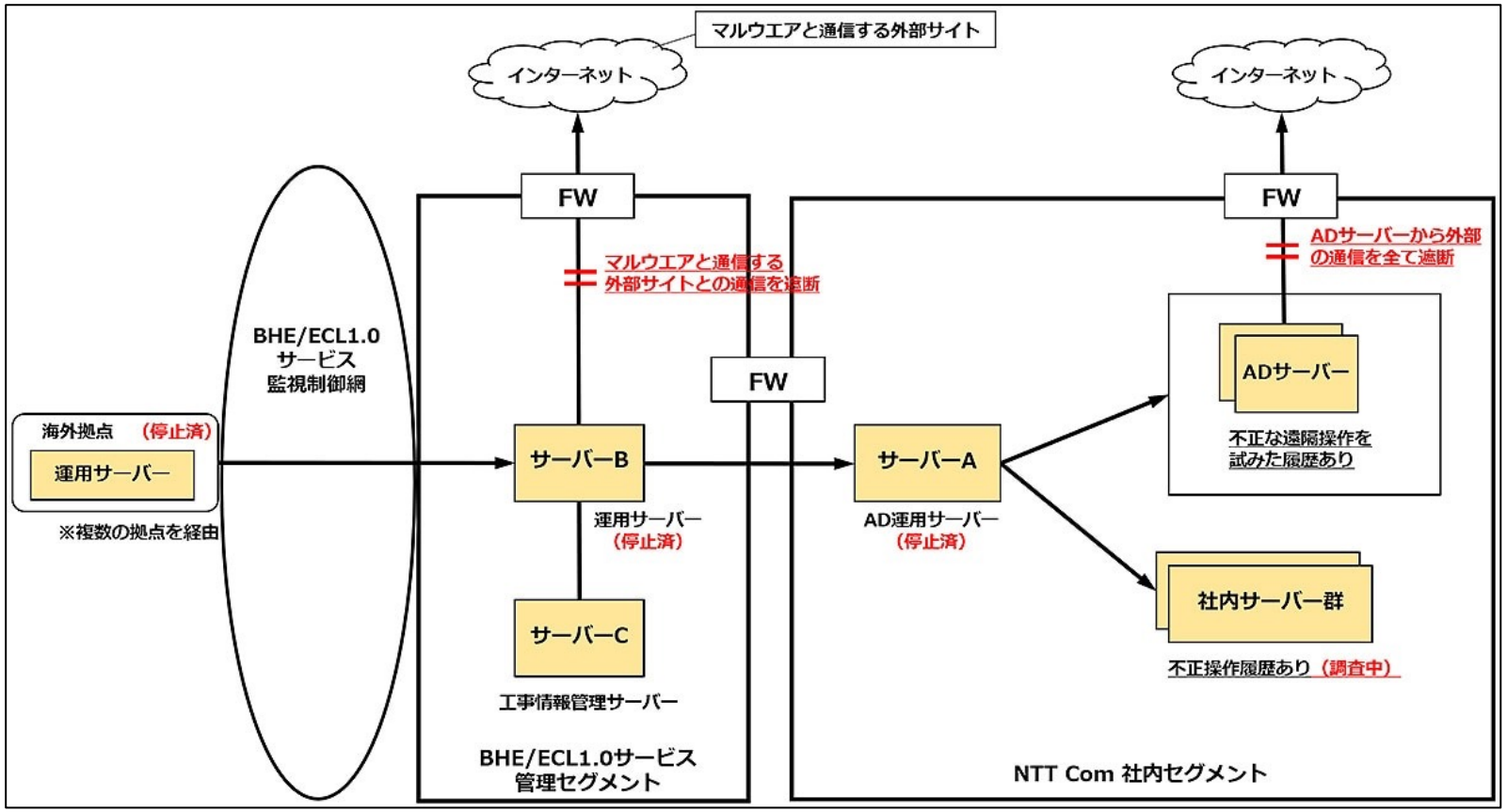
2022年11月29日

NTTコミュニケーションズ株式会社
情報セキュリティ部
藤崎 智宏

ComNIC誕生の経緯

2020年5月 NTTコムにてインシデント発生

- https://www.ntt.com/about-us/press-releases/news/article/2020/0528.html



インシデント対応の際、ネットワーク資源の管理が不十分であったことが課題となる。

ComNICでのネットワーク資源管理

■目的

NTTComが保有するネットワーク資源(IPアドレス、ドメイン等)利用に関する**セキュリティ・マネジメント強化(インシデント発生時の迅速な調査、インターネット資源の不正利用防止等)**、及び**資源利用の効率化・高度化(利用終了時の返却ルールの徹底や最新標準技術の導入等)**を目的とする。

■実施事項

NTTComが保有するネットワーク資源をComNICにて集中管理することで、管理対象の明確化、利用の健全化を行う。主な実施事項は以下とする。

- 管理ポリシー・運用ガイドラインの策定および社内浸透
- 運用体制・運用フローの整備および運用
- 保有資源ごとの利用状況・利用者情報の一元管理と最新化

■管理対象（当初案）

資源分類	資源詳細
IPアドレス	IPv4グローバルIPアドレス
	IPv6グローバルIPアドレス
	NTTグループプライベートIPアドレス
	個別プライベートIPv4アドレス
	IPv4シェアードアドレス
ドメイン	ntt.comサブドメイン
	独自ドメイン
AS番号	AS番号

ComNICの活動状況

- ComNIC設立後、段階的にネットワーク資源の一元管理を推進

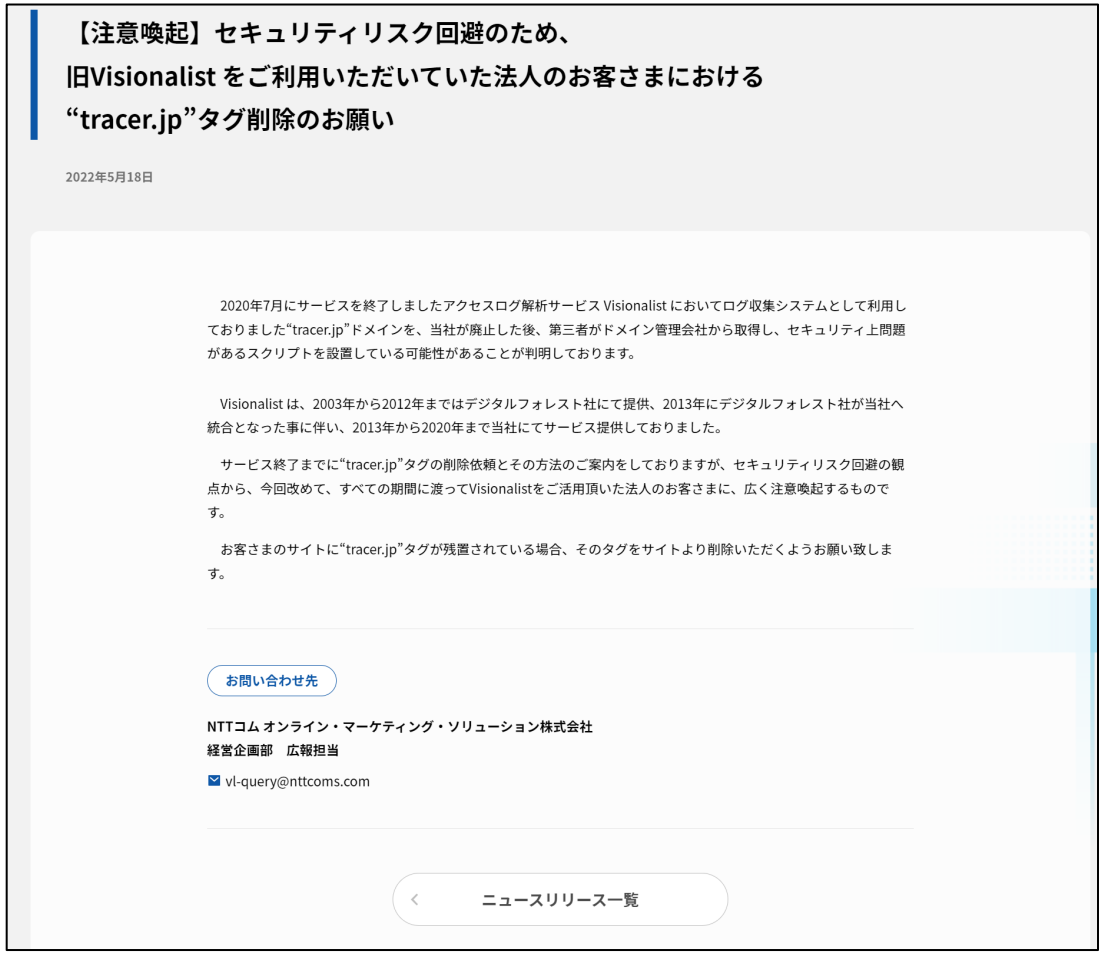
資源管理の現状（2022年10月30日現在）

資源分類	資源詳細	運用状況
IPアドレス	IPv4グローバルIPアドレス	NTTコム保有空間について把握、RIR/NIR窓口も集約
	IPv6グローバルIPアドレス	
	NTTグループプライベートIPアドレス	NTTコム利用空間について把握、ユーザ申請窓口設置、上位組織窓口も集約
	個別プライベートIPv4アドレス	検討中
	IPv4シェアードアドレス	NTTコム利用空間について把握、ユーザ申請窓口設置
ドメイン	ntt.comサブドメイン	NTTコム利用ドメインについて把握、ユーザ申請窓口設置
	独自ドメイン	
AS番号	AS番号	NTTコム利用番号について把握、RIR/NIR窓口も集約

特にドメイン名管理について

ドメイン管理の重要性 1/2

- NTTコムのグループ会社にて、「ドロップキャッチ」に起因するインシデントが発生



【注意喚起】セキュリティリスク回避のため、
旧Visionalist をご利用いただいていた法人のお客さまにおける
“tracer.jp”タグ削除のお願い

2022年5月18日

2020年7月にサービスを終了しましたアクセスログ解析サービス Visionalist においてログ収集システムとして利用しておりました“tracer.jp”ドメインを、当社が廃止した後、第三者がドメイン管理会社から取得し、セキュリティ上問題があるスクリプトを設置している可能性があることが判明しております。

Visionalist は、2003年から2012年まではデジタルフォレスト社にて提供、2013年にデジタルフォレスト社が当社へ統合となった事に伴い、2013年から2020年まで当社にてサービス提供しておりました。

サービス終了までに“tracer.jp”タグの削除依頼とその方法のご案内をしておりますが、セキュリティリスク回避の観点から、今回改めて、すべての期間に渡ってVisionalistをご活用頂いた法人のお客さまに、広く注意喚起するものです。

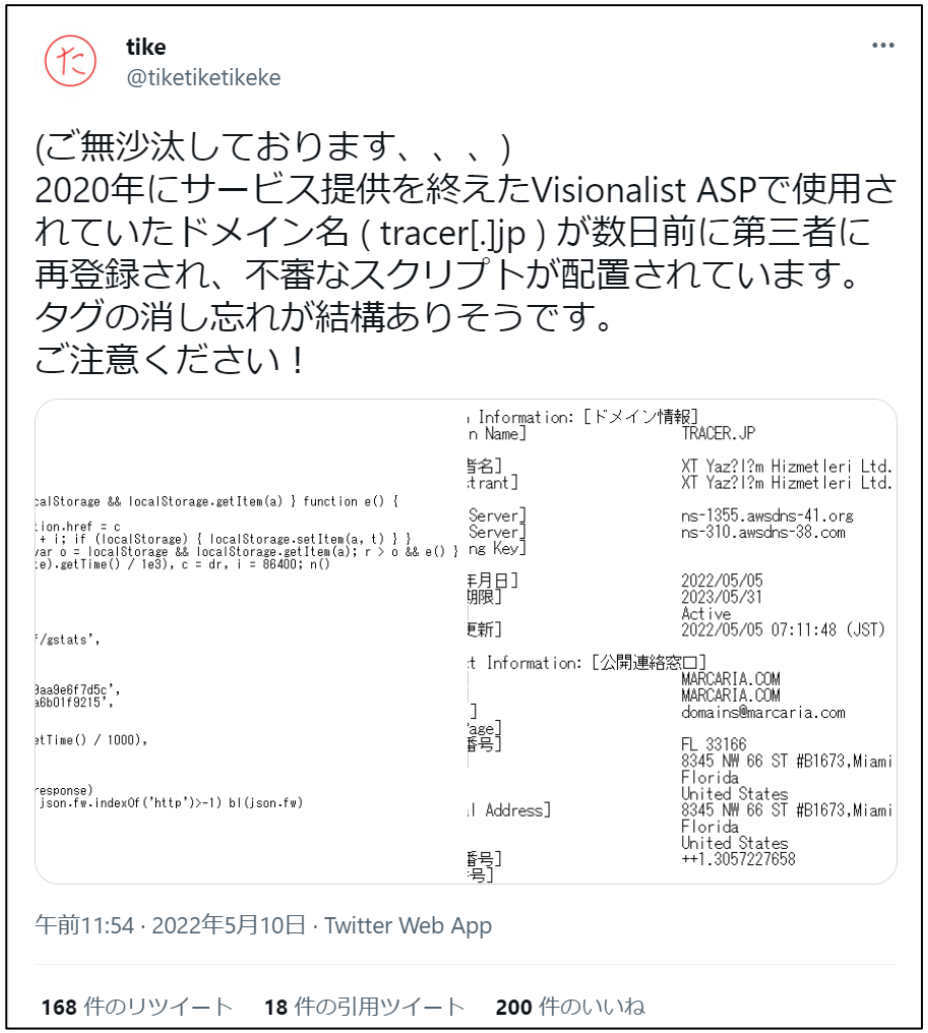
お客さまのサイトに“tracer.jp”タグが残されている場合、そのタグをサイトより削除いただくようお願い致します。

お問い合わせ先

NTTコム オンライン・マーケティング・ソリューション株式会社
経営企画部　広報担当
vl-query@nttcoms.com

ニュースリリース一覧

https://www.nttcoms.com/news/2022051801/



tike
@tiketiketikeke

(ご無沙汰しております、、、)
2020年にサービス提供を終えたVisionalist ASPで使用されていたドメイン名 (tracer[.]jp) が数日前に第三者に再登録され、不審なスクリプトが配置されています。
タグの消し忘れが結構ありそうです。
ご注意ください！

午前11:54 · 2022年5月10日 · Twitter Web App

168 件のリツイート　**18** 件の引用ツイート　**200** 件のいいね

https://twitter.com/tiketiketikeke/status/1523858880073469955

ドメイン管理の重要性 2/2

- コムにおいても、終了したサービスで利用していた廃止済ドメインに起因する課題が発生

事象

- “ntt.com” サブドメインのURL（http[:]//www[.] example[.]ntt[.]com）から、悪性サイトへの誘導が発見された
- 当該URLは、過去のニュースより参照されていた

【原因】

サブドメインのDNSを委譲していた外部ドメインがドロップキャッチされ，DNSサーバを設置された

参考

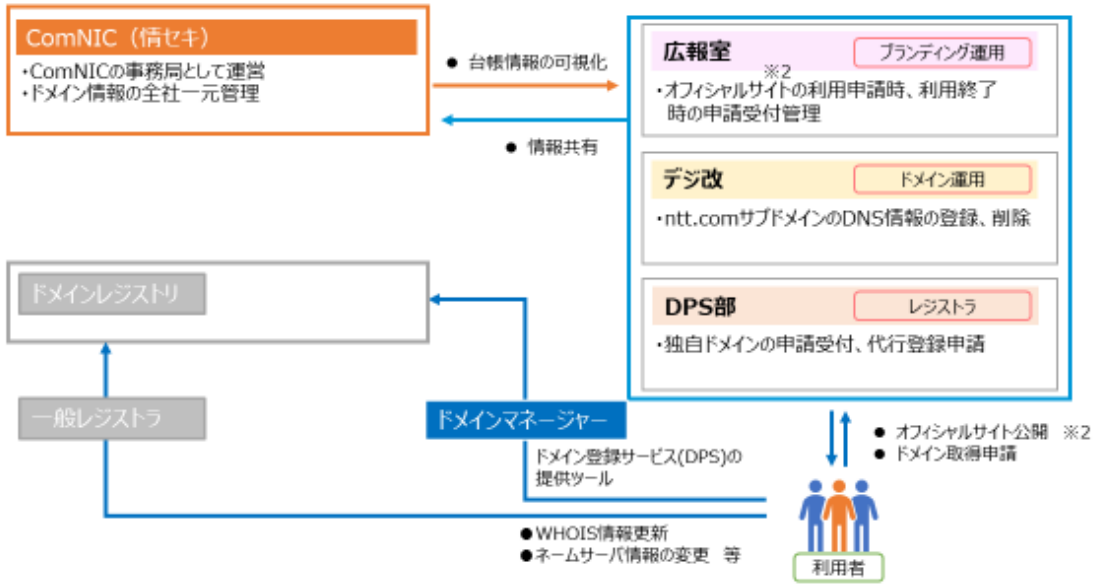
- https://www.e-ontap.com/summary/

NTTコムにおけるドメイン管理

広報担当、ドメインの運用チームと連携し、管理を実施

5. ドメイン運用の管理体制

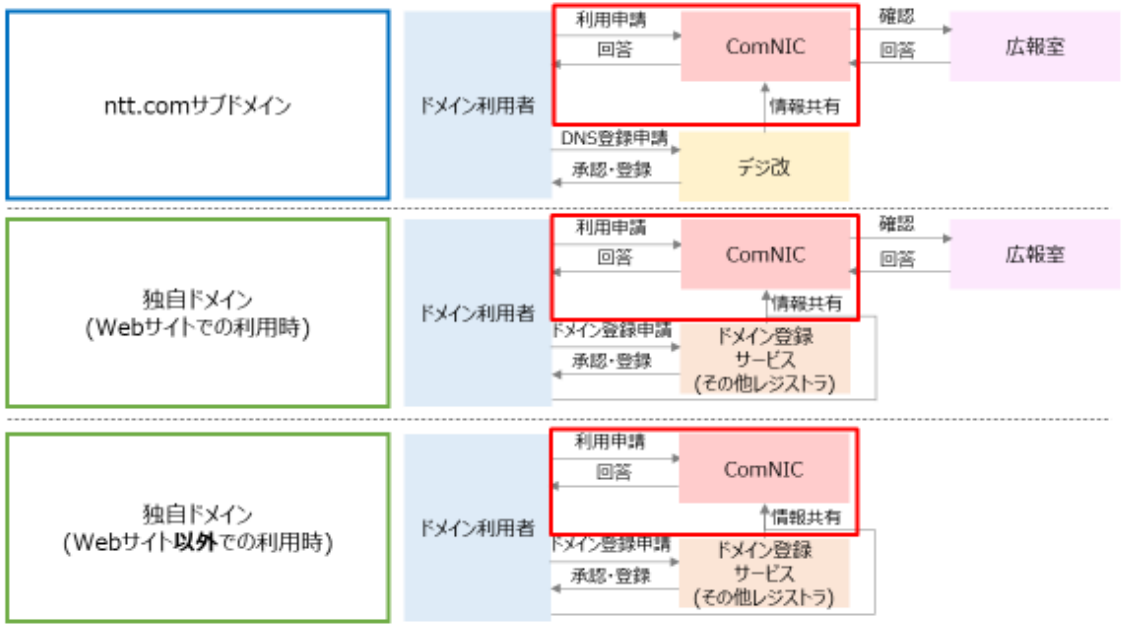
ドメインの管理体制は以下の通り。オフィシャルサイトのチェックを行う広報室、ntt.comサブドメインの運用を担当するデジ改、独自ドメインの登録サービス主管であるDPS部との情報連携により、ntt.comサブドメイン、独自ドメインに関わらず、全てのドメインを対象とした一元管理を実施。
利用者がどのレジストラを利用しているかについても管理対象とする。



※2：オフィシャルサイトは、NTTComが運営主体となり、インターネット公開されているWebサイト

6. ドメイン管理 運用フロー（概要）

ComNICのドメイン管理におけるスコープは、ドメインの種類に限らず、NTTComが所有するドメインのすべてが対象です。以下に運用フローを整理しました。既存フローからの変更点は、赤枠部分です。

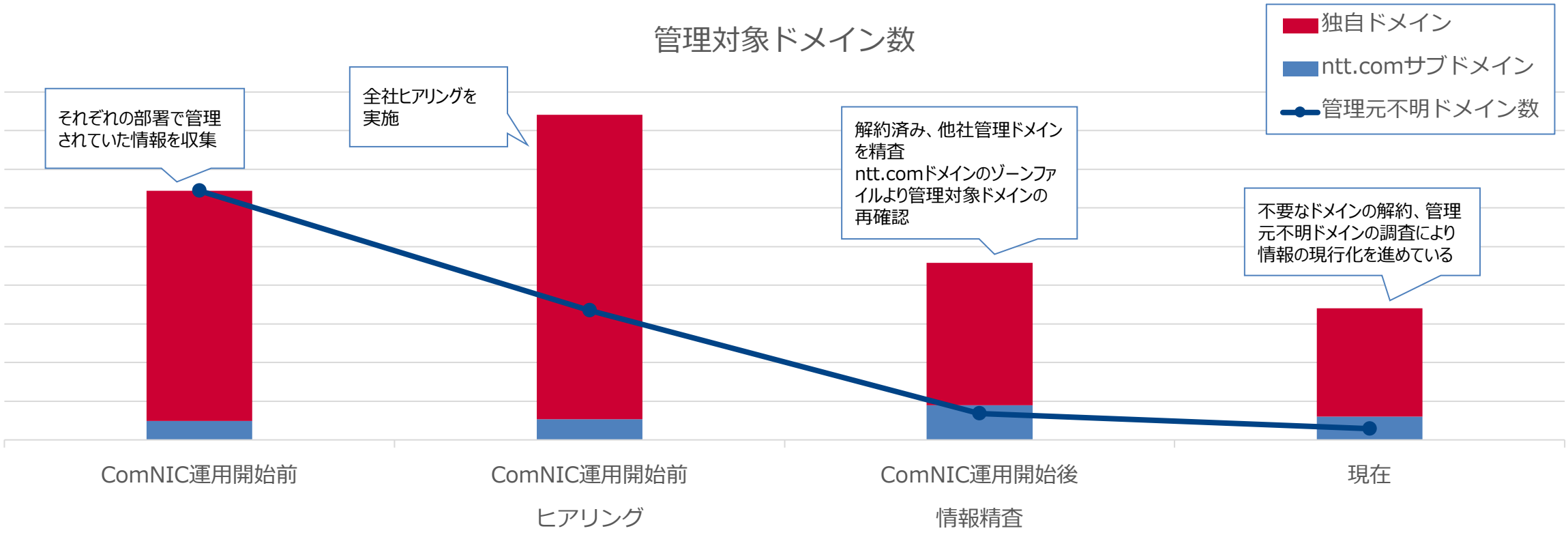


※オフィシャルサイト利用は別途広報室へ申請する

社内向けドメイン管理説明資料より

NTTコムにおけるドメインの現状

ドメイン情報については、全体件数の把握、管理部門の調査を継続対応中。



ドメイン管理ルール（取得）

ドメイン利用の際、独自ドメインでなく、会社ドメインのサブドメインを利用することを推奨

■独自ドメインのリスクについて

ComNICでは新規のドメイン発行について、可能な限りntt.comサブドメインの利用を推奨しております。独自ドメイン利用については、下記リスクがあると考えるためです。独自ドメインを申請される際は、下記をご確認いただいた上でntt.comサブドメインではなく、独自ドメインを利用する理由をメールに明記の上、申請してください。

【機密性1】

独自ドメイン利用のリスク（デメリット）

情報セキュリティ部　ComNIC
DPS部　ドメイン登録サービス担当

事業者としてのリスク（デメリット）

①利用終了したドメインを第三者に取得され（ドロップキャッチ※）悪用されるリスク

- ドメインを広告に利用される（ドメインパーキング）
- ドメイン名をオークションで売買する（ドメインオークション）
- フィッシングサイトなどへの悪用

②維持管理コストの増加

- ドロップキャッチ対策の為、長期間ドメインを保持する必要がある
- ドメイン、TLS証明書の維持管理が必要

※ドロップキャッチ：
失効したドメイン名を第三者が再登録すること

ユーザとしてのリスク（デメリット）

①ドメインが乱立することにより、ユーザにとってどれがコムの正規ドメインか、紛らわしい悪性ドメイン(フィッシングサイト等)か見分けがつかなくなる恐れ
②これまで正規だったドメインが信用できなくなる恐れ（利用終了ドメインのドロップキャッチ）

独自ドメイン申請の際の注意点

- セキュリティや運用に関する実績の観点及び、上記のリスクからntt.comドメインの利用を勧めている。
- 閉じたネットワーク内で独自ドメインを利用するとしても、コムが取得しているドメインと公開されるようになる(WHOISなど)ため、コムとしての管理が必要。
- 独自ドメインの取得にドメイン登録サービスを利用した場合にも、コムからのキャッシュアウトが発生する。
- 独自ドメイン利用の場合、ドロップキャッチ対策として、2年間保持すること、とComNICにて定めている。その分の保持コストもかかる。

ComNIC Webページより

ドメイン管理ルール（廃止）

ドメイン廃止後、2年は保持するよう、ルールで規定

3.7. ドメインの利用終了

管理情報更新の結果、利用終了予定を過ぎているドメインに関しては、利用終了報告を要請し、廃止、もしくは解約を行う。

また、次の場合、ComNIC が利用者のドメインの登録を停止、取り消し、移転、修正する権利を保持することを承諾する。

A) 利用者が紛争処理方針、およびこの利用ポリシーに違反し、ComNIC による注意があったにもかかわらず、その違反を是正しないとき
B) ドメイン登録を停止、取り消し、移転、修正する法律的な根拠がある場合
C) レジストリ、ドメイン登録業者の管理者により、あらゆる種類のエラーを修正する場合
D) ドメインに関する紛争を解決する場合

ntt.com サブドメインに関して、一度使用したドメインの再利用は広報室により利用可否について判断するものとする。

独自ドメインに関して、第三者が再取得し悪用した際の風評被害等のリスクを考慮し、利用終了から２年保持したのち、解約、廃止することとする。

組織における資源管理に関する課題等

- 全社への継続的周知、認知度維持が重要
  - シャドウ資源を作らないように。。。
- 管理情報の鮮度維持は難しい
  - 担当者情報、利用者情報など
  - 社内利用IPアドレスの管理
- 特にドメイン管理について
  - ドメイン廃止後2年たった後に課題が発生することも
  - 2年の保持では不十分？
    - 廃止の際、ドメインの利用状況に応じた対応を検討
      - 「タグ」利用等、登録情報が広く拡散していそうな場合への対応
      - 利用FQDNへのトラフィックや、DNSアクセスの状況のモニタ等

組織における資源管理のToBe

- 利用者（運用者）への対応（ルール化等での施策推進）
  - DNSSEC対応、リソース証明書対応の必須化等
  - https 対応
- せっかく集めた情報を有効活用したい
  - 実データに基づく各種チェック
    - 公開Webの証明書管理
    - https対応チェック
    - プロトコル脆弱性チェック（TLS1.2以上とか）

ご清聴、ありがとうございました