インターネット上の海賊版サイトへのアクセス抑止方策に関する検討会
（第２回）資料

資料２－３

アクセス警告方式をISP事業者が行う場合の技術的な検討と課題

2019年6月3日

一般社団法人日本インターネットプロバイダー協会

おことわり

- 技術的な説明については、平易な説明を優先するため、厳密にいえば不正確・不足である点があります。大筋では合っていると思いますが、詳細は技術書などでお調べください。
- JAIPAは理系と文系が入り乱れた組織ですので、内部でも価値観の対立はありますが、お互いを尊重しながらうまくやっています。

もくじ

- webページへのアクセスのしくみ
- 方式ごとの技術的検討
- アクセス警告方式と「セキュアなインターネット」
  - 前提としての技術的動向
  - アクセス警告方式とHTTPS
- まとめ

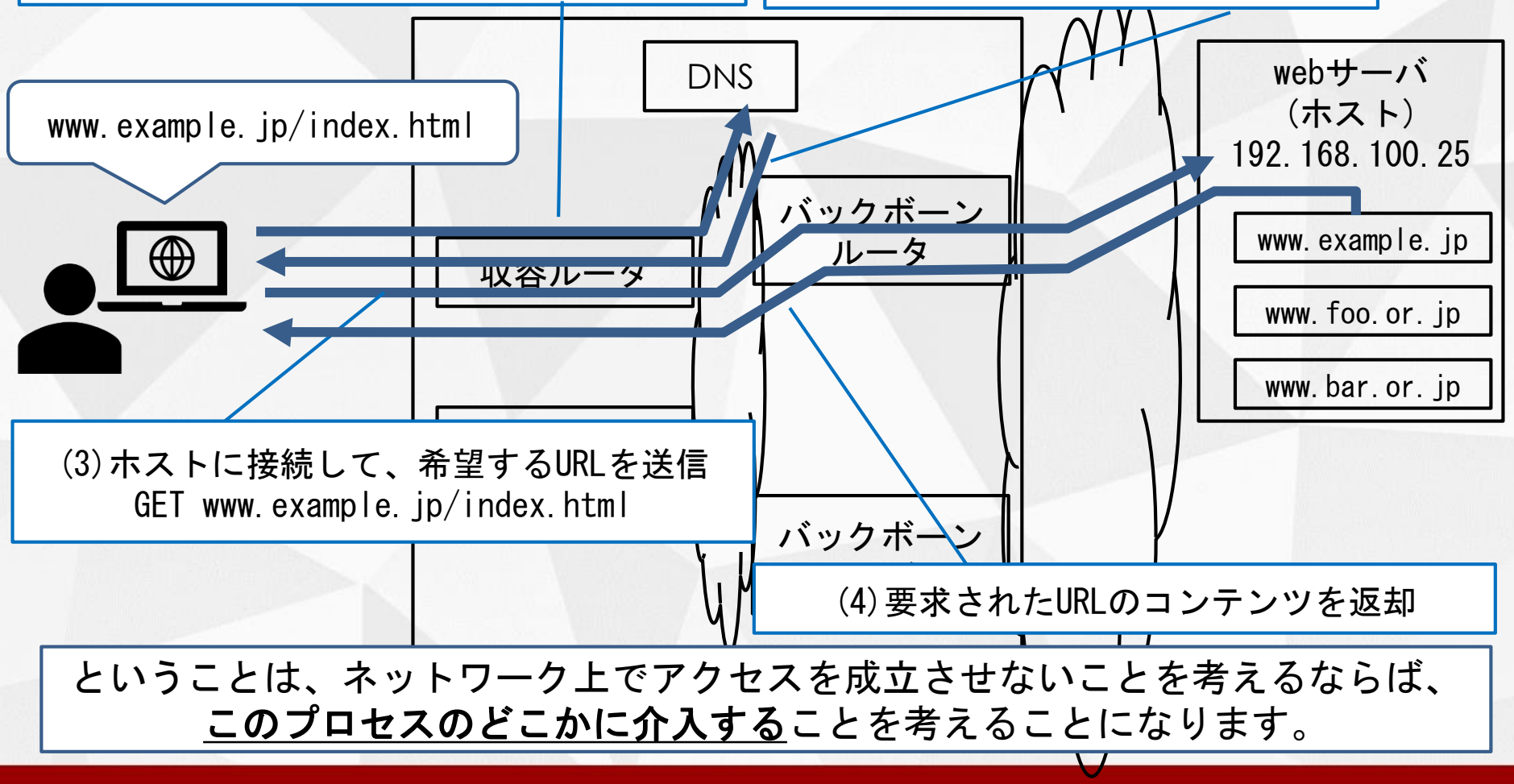
～webページへのアクセスのしくみ～

最初に、webサイトへの接続、webページの閲覧がどのように行われるかをお話しします。

webページへのアクセスのしくみ

(1)ホストのIPアドレスをDNSに問い合わせ
www.example.jp＝？

(2)DNSがホストのIPアドレスを回答
www.example.jp＝192.168.100.25

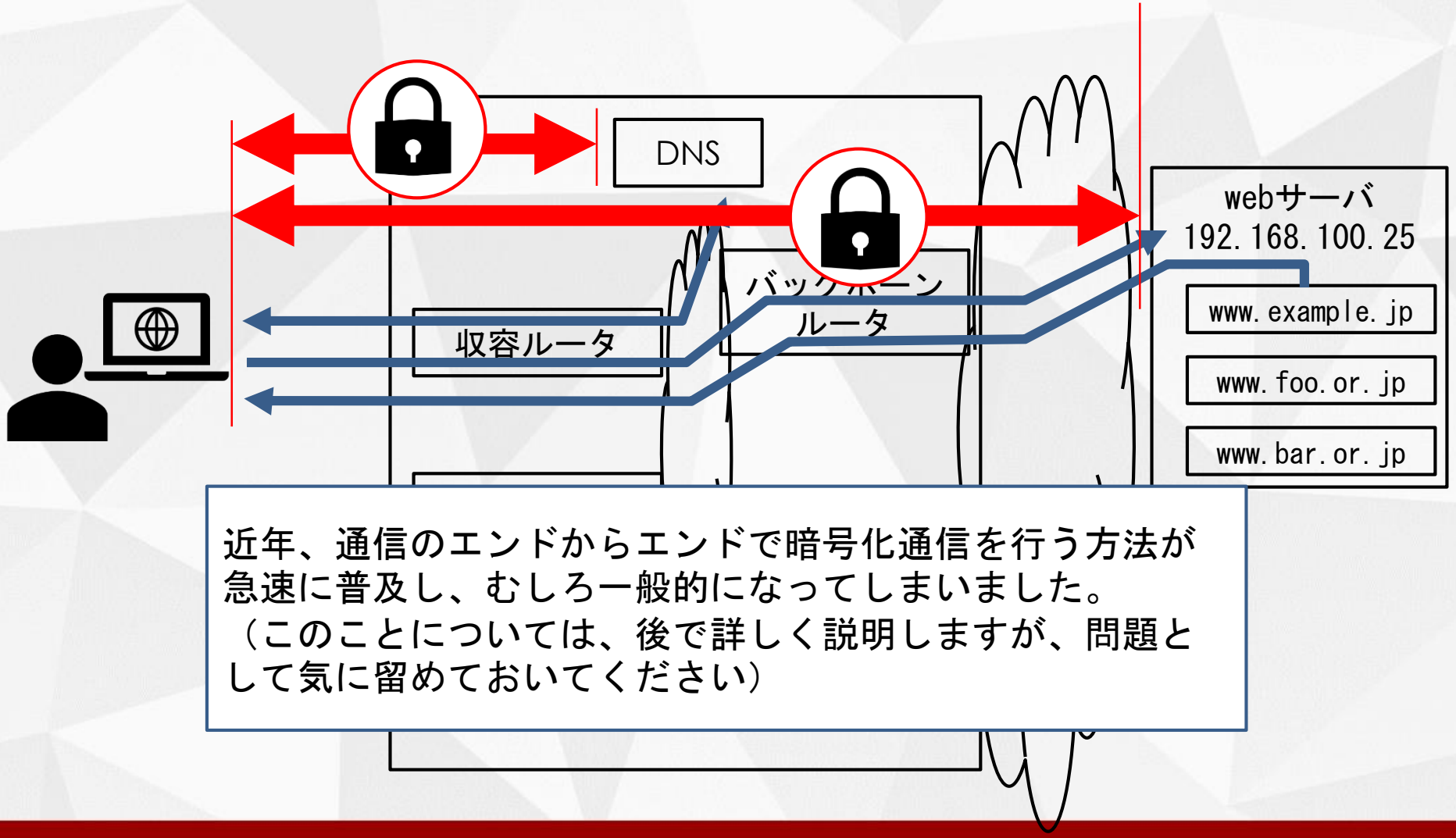


(3)ホストに接続して、希望するURLを送信
GET www.example.jp/index.html

(4)要求されたURLのコンテンツを返却

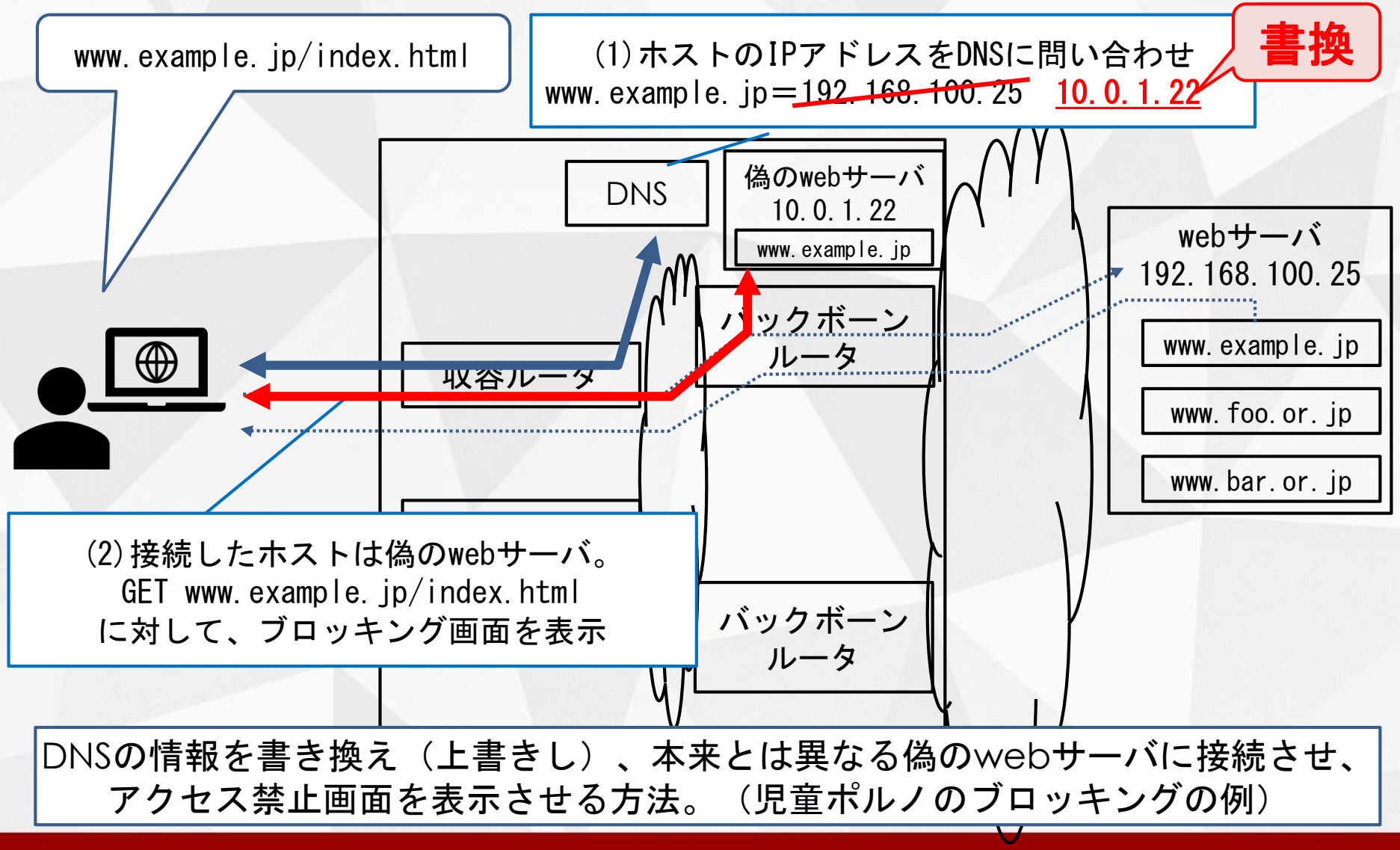
ということは、ネットワーク上でアクセスを成立させないことを考えるならば、
<u>このプロセスのどこかに介入する</u>ことを考えることになります。

End-to-end暗号化の進展
（後で詳しく説明します）



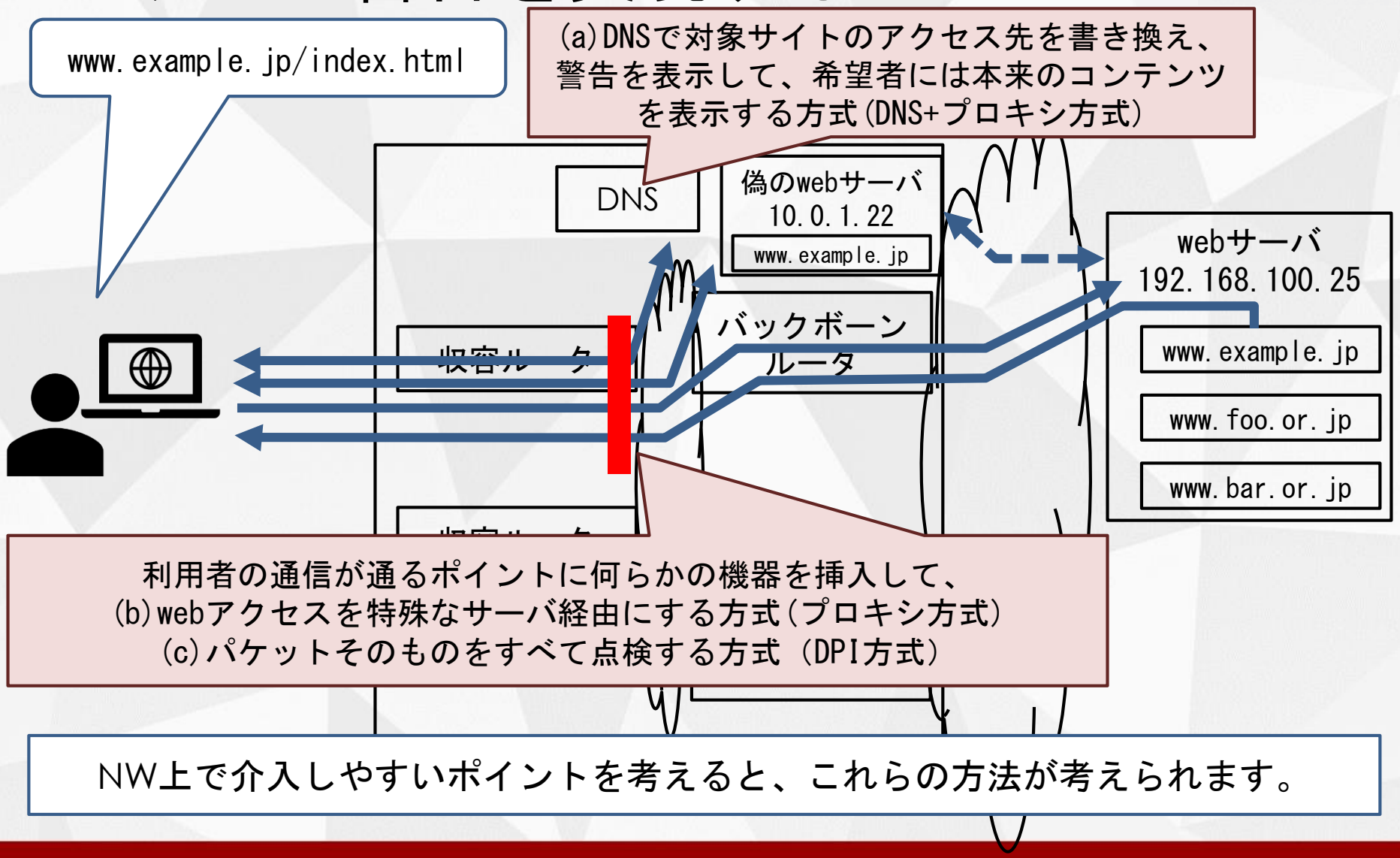
近年、通信のエンドからエンドで暗号化通信を行う方法が急速に普及し、むしろ一般的になってしまいました。
（このことについては、後で詳しく説明しますが、問題として気に留めておいてください）

ブロッキングは何をしているか



DNSの情報を書き換え（上書きし）、本来とは異なる偽のwebサーバに接続させ、アクセス禁止画面を表示させる方法。（児童ポルノのブロッキングの例）

アクセス警告を実現するとしたら



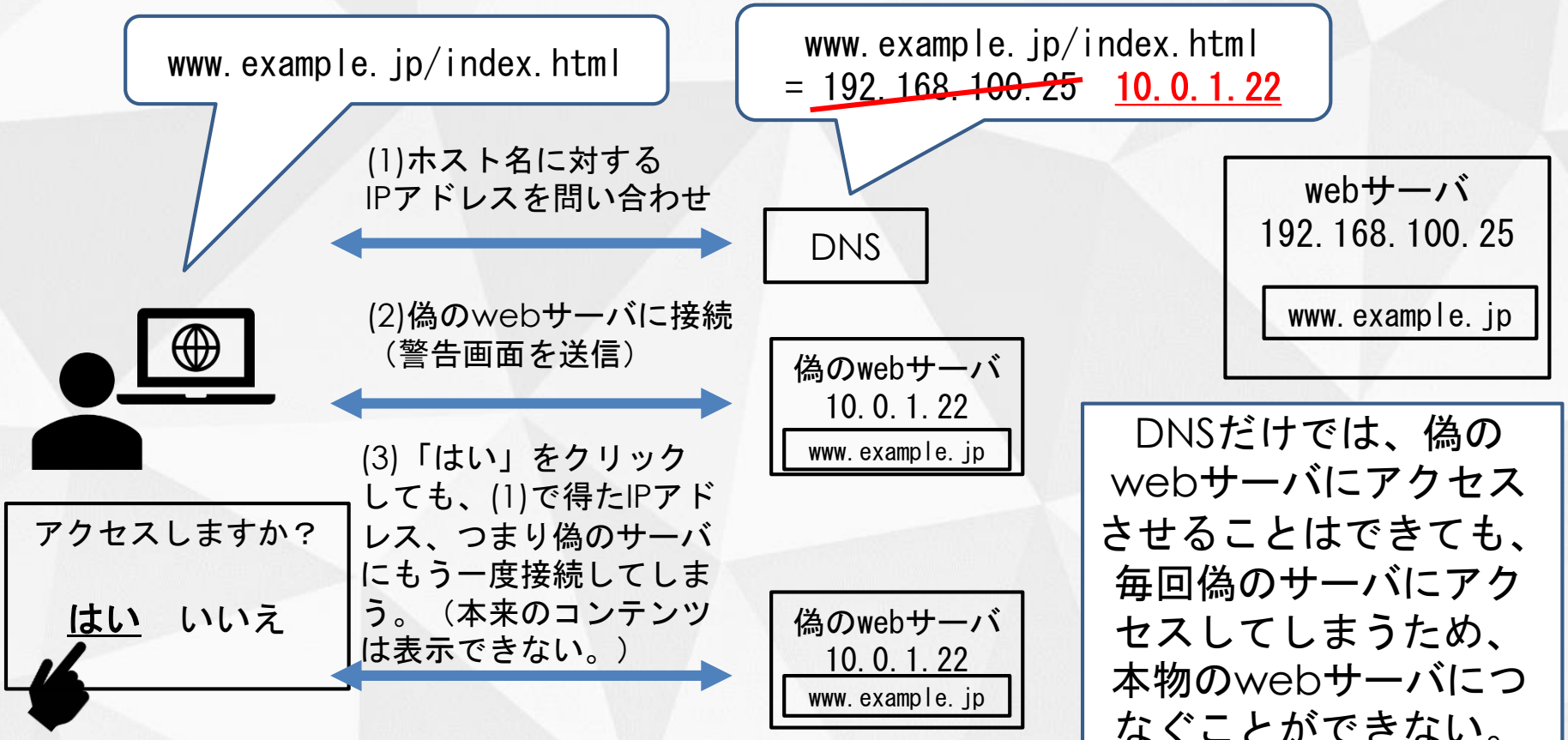
NW上で介入しやすいポイントを考えると、これらの方法が考えられます。

～方式ごとの技術的検討～

ここから、DNS＋プロキシ方式、DPI方式の2つについて、技術的な検討をしていきます。

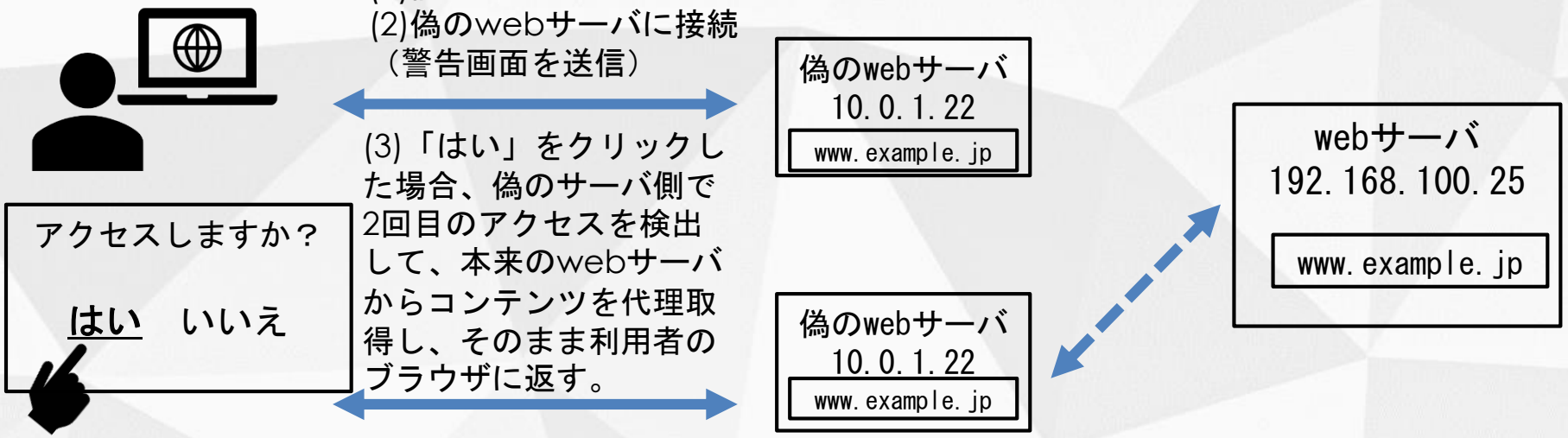
DNS+プロキシ方式(1)

- 途中まではブロッキングと同じですが。。。



DNS+プロキシ方式(2)

- でも、技術的に可能な方法を考えてみます



偽のwebサーバへの2回目以降のアクセスを検出し、2回目以降はプロキシとして機能させることで、アクセス警告方式の実装自体は一応可能だと思います。
（ただし、実験したら動かないことはないだろう、というレベルで、これを商用のNWに実装できるかどうかは別問題ですが。。。）
2回目のアクセスを検出する手法として真っ先に考えられるcookieやアクセスログ解析などは、あまり信頼性の高い方法ではありません。

DNS+プロキシ方式(3)

- 最低限用意するもの
  - 偽のwebサーバ（1社1～2台？）
    - 「それでもアクセスする」人が多い場合、追加が必要
    - ただし、プログラムは各社で書く必要があるでしょう
- おそらく必要になるもの
  - オプトアウト用DNS(1社2台～4台？)
- 会社によって必要になるもの
  - 対象ホスト名のリストとDNSの連携機能
  - オプトアウト用DNSの指定を、顧客DBと連携する機能
    - オプトアウトを「別のDNSを指定してください」と案内する場合、不要（説明のPDF1枚程度は必要）
    - （でも、ブロッキングの回避方法とどう違うのか。。。）

「警告画面の表示さえ行わない」という意味でのオプトアウトになります。
DNSは通常、2台1組です。

ここで一旦おことわり

- コストの試算の前提について
  - NWの運用はピンキリですので、どの程度のグレードを考えているかによって、結論は1桁以上変わります。
  - ただ、「設備故障のとき、抑止対象のサイト以外のアクセスに支障するリスクが大きく高まることは合意が得られない」ということを1つの前提にします。
  - ISPはケーブルテレビを含めて1000社と仮定し、ユーザの数やトラヒックは総務省の資料をもとにします。また、協会で情報の集まりやすい固定系を今回の対象としています。
- 試算上の制約について
  - 仕様もよくわからなくて、買うかどうかも全くわからないものの見積もりを、精緻に出してくれるベンダはありません（対価を払えば別です）。よって、これから出てくる価格はすべて概算です。
- 運用コストについて
  - 皆さまのネットが毎日当たり前のようにつながるのは、日頃の保守運用に時間をかけているからです。それなりの教育や訓練を受けた人が運用監視をするコストは、人件費だけでも意外とかかります。
  - 筆者は「とりあえず動く」という程度の安定感でよければ、簡単なものは1日か2日で作り、自分で運用してしまうため、開発費や保守運用費の見積もりはむしろ甘いかもしれません。
  - 一般論として、サーバは激安なものでも一応動くでしょうが、信頼性の低いものを入れるとその後の運用費が上がるという問題が生じてきます。
- 費用負担の考え方について
  - 中には、既存の設備の流用や改修で実現できる機能もありますが、あくまでも本来の用途のために導入した機器を別の用途に転用する場合、妥当な割合をコストに計上するのが普通です。

DNS+プロキシ方式(4)

- コスト(最小構成)

1社（1ネットワーク）あたり導入費

proxyサーバ 30万円	設定・導入 50万円	運用マニュアル・教育 100万円

同　運用増加

サーバ1台 2万円/月

仮に1000社（か所）とすると、初期18億円＋月2千万円
初期費用を5年で償却するとすれば、初期＋運用で年間6億円

上記の仕様は、
・オプトアウトができない（ISPがパブリックDNSの利用を周知？児童ポルノのブロッキングも回避されるおそれ）
・サーバ故障時は、対象サイトへのアクセスがしばらく停止するおそれ
・リスト更新は手動（1回ごとに、各社5000円～1万円の稼働が発生？）

※既存のDNSサーバを別目的に流用するときの費用については、考慮していません。
（本来は利用目的により按分したコストを出すことになると思います。）

DNS+プロキシ方式(5)

- コスト(もう少し現実的)

1社（1ネットワーク）あたり導入費

proxyサーバ 30万円×2	設定・導入 200万円	運用マニュアル・教育 100万円

オプトアウト用DNSサーバ 50万円×2台 （プライマリ・セカンダリ）

※DNSサーバが故障すればすべてのアクセスに支障するため、オプトアウト用であるにしても、それなりに堅牢な装置が必要です。

同　運用増加

proxyサーバ 2万円/月×2

DNSサーバ 3万円/月×2

仮に1000社（か所）とすると、初期46億円＋月1億円
初期費用を5年で償却するとすれば、初期+運用で年間21億円

上記の仕様は、
・ISPのサービスの範囲内でオプトアウトが可能（各自DNSの設定を変更）
・プロキシサーバを冗長化
・リスト更新は自動（ただし、リスト作成管理団体が自動処理に対応する必要性）

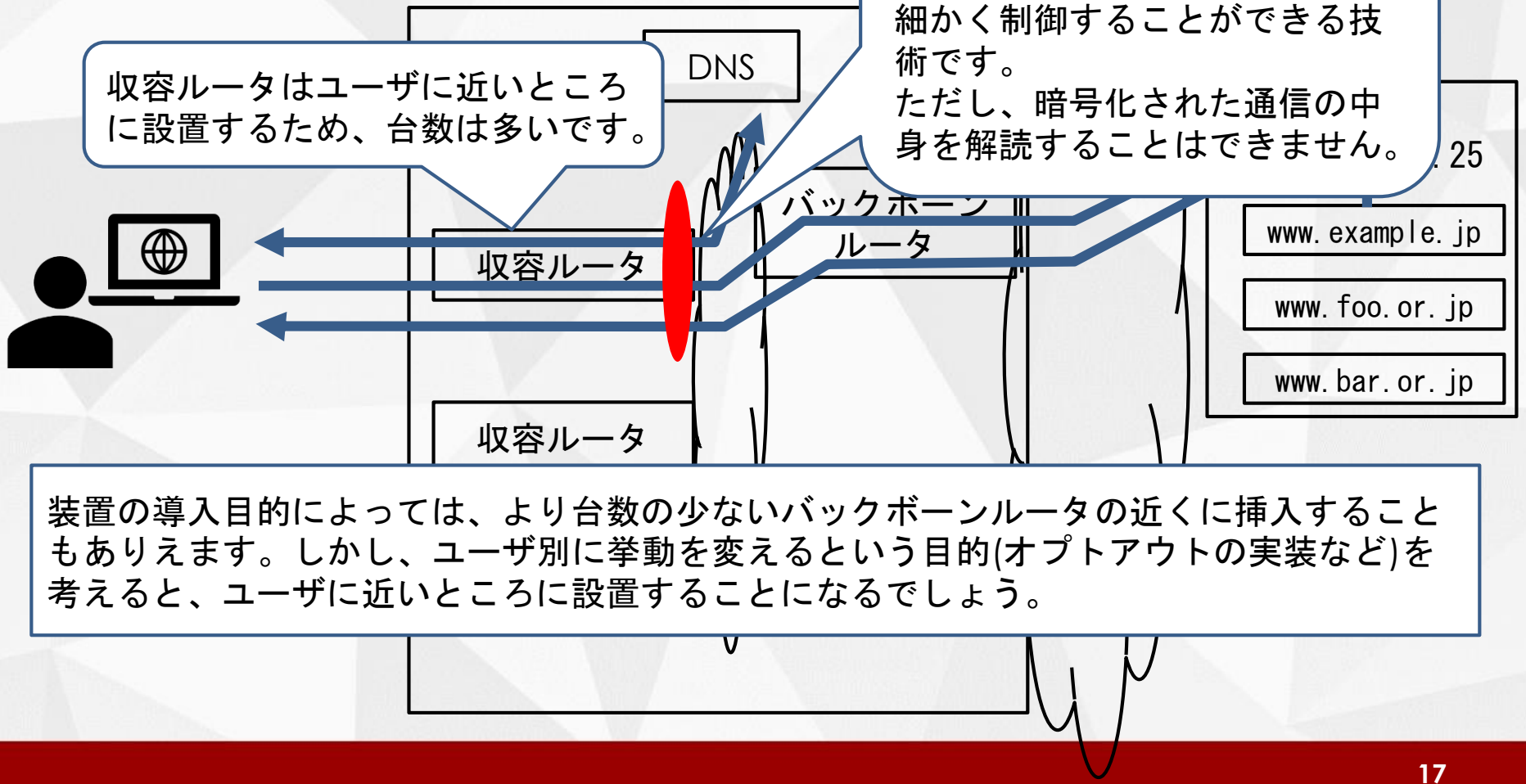
※既存のDNSサーバを別目的に流用するときの費用については、考慮していません。
（本来は利用目的により按分したコストを出すことになると思います。）

DNS+プロキシ方式(6)

- 残る課題
  - ここまで述べた方式は、商用NWでの実績がない
  - 簡易な方式なため、本来通すべき通信（少なくとも、拒絶される理由のない通信）を止めてしまうことがどうしても起こりうる
    - 例：同じホスト名で運用される、一般的でないポート番号を使った通信は遮断される可能性が高い。また、DNSはホスト名単位で設定するため、サイトのメールサーバの運用しだいでは、メールの通信を遮断してしまうことがある。
    - プロトコルもHTTPに事実上限られるため、ストリーミングなどにも対応が難しい。
    - 最近の高機能なwebサイトに十分対応できるか不明
  - パブリックDNS（特にDoH：DNS over HTTPSを採用したパブリックDNS）の利用が普及すると対応できない。
  - HTTPSに対応できない。

DPI方式(1)

- 簡単な原理



装置の導入目的によっては、より台数の少ないバックボーンルータの近くに挿入することもありえます。しかし、ユーザ別に挙動を変えるという目的(オプトアウトの実装など)を考えると、ユーザに近いところに設置することになるでしょう。

DPI方式(2)

- 利点(通信の制御という技術的な意味において)
  - すべてのパケットを監視するので、漏れが少ない
  - ポート番号などの小手先の監視ではなく、パケットの中身を見ているので、他の通信への偽装（監視すり抜けを意図した偽装）にも対応しやすい（ただし、いたちごっこ）
  - プロキシと異なり、パケットの遅延を起こさずに監視・制御できる。

DPI方式(3)

- 導入のスケール
  - 「すべてのパケットを中身まで監視する」という性質上、仕事の量が何桁も増えてしまい、とんでもない規模になります。。。
  - 「ISPのユーザ側の収容ルータ」のインタフェースの数だけ必要なため、台数が多いです。。。
    - 例：NTT東西（フレッツPPPoE方式）とISPの接続用ルータの台数（NTT側台数の公表値）は、**1万1千台**(*1)
  - 正確な数値を示すのは困難ですが、トラヒック量から推計してみます。

(*1)NTT東西の2019年度接続料認可申請に添付された、網使用料算定根拠(NGN)に記載された、2019年度稼働予測台数（東日本7629台、西日本4014台）。PPPoE方式のルータのインタフェースは1Gbps。

DPI方式(4)

- 必要な台数の見積もり
  - わが国のダウンロードトラヒックは、固定系だけで約11Tbps（2018年11月*1）
  - ただしこれは1日平均なので、ピークは2倍～3倍
  - 設備容量はこの時点で、少なくとも33Tbps分になる
    - 10Gbpsのインタフェースで3300台分
- DPI装置は一般に高価
  - 10Gbps用の装置の価格は1台2000万円～5000万円
  - 保守契約もそれなりに高額（1年ごとに本体価格の1割程度？）
- 固定系のトラヒックは、年に2～3割の勢いで増加中
  - 5年で3倍
  - 上記はあくまでも現在のトラヒックでの必要台数

(*1)総務省調査。52ページ以降に参考資料として収録

DPI方式(5)

- 残る課題
  - パケットの中身まで解析する方式のため、利用者の心理的抵抗感が大きい。また、国によっては国家主導でDPIを使った通信検閲を行っている場合もある。
  - 海賊版対策のためにDPIを導入するならば、過剰設備としか言いようがない。
  - 仮にISPが費用を負担する場合、誰もそんなお金を用意できない
  - HTTPSに対応するのは難しい（少なくとも商用ISPでは）。

方式の比較

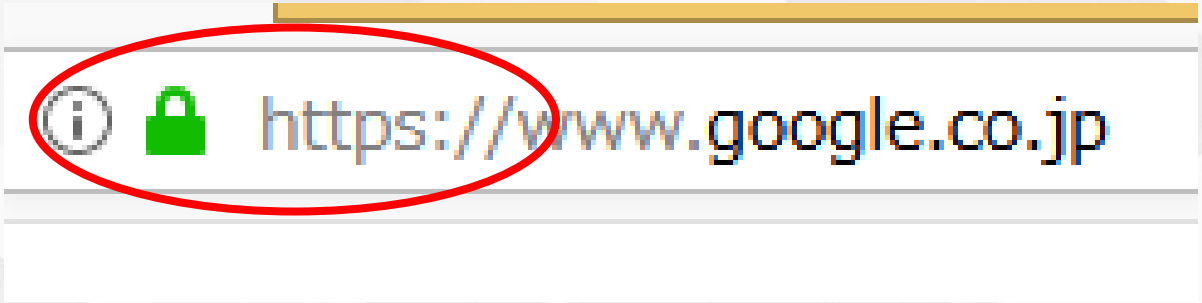
問題点	DNS+Proxy方式	Proxy方式(参考)	DPI方式
処理対象となる通信	・DNSサーバはすべての通信を監視 ・Proxyサーバは DNSで選別した一部の通信を処理	すべての HTTP(HTTPS)通信を処理 ※すべてのweb閲覧等が処理対象	すべてのIP通信を処理 ※メールなどを含むすべての通信が処理対象
処理方法	ソフトウェア	ソフトウェア	ハードウェア
通信の遅延	DNSで対象とされた通信で生じる	すべてのweb閲覧等で生じる	生じない
装置台数	少ない	多い	多い
コスト	少ない	多い	多い
HTTPSへの対応	**困難**	**困難**	**困難**

～アクセス警告方式と「セキュアなインターネット」～

安全なインターネットを実現するための暗号化や電子証明書の技術と、アクセス警告方式の関係をみていきます。

「HTTPSへの対応が難しい」とは？

- 簡単にいうと、SSL(TLS)を使ったwebサイトへの通信は、ブラウザからwebサーバまでの全区間が暗号化されているので、NWの途中で手を加えることができない、ということです。
- ブラウザに南京錠のマークが表示されていれば、それは暗号化通信です。



- でも、主なサイトはほとんどこれなんじゃ。。。

前提としての技術的動向(1)

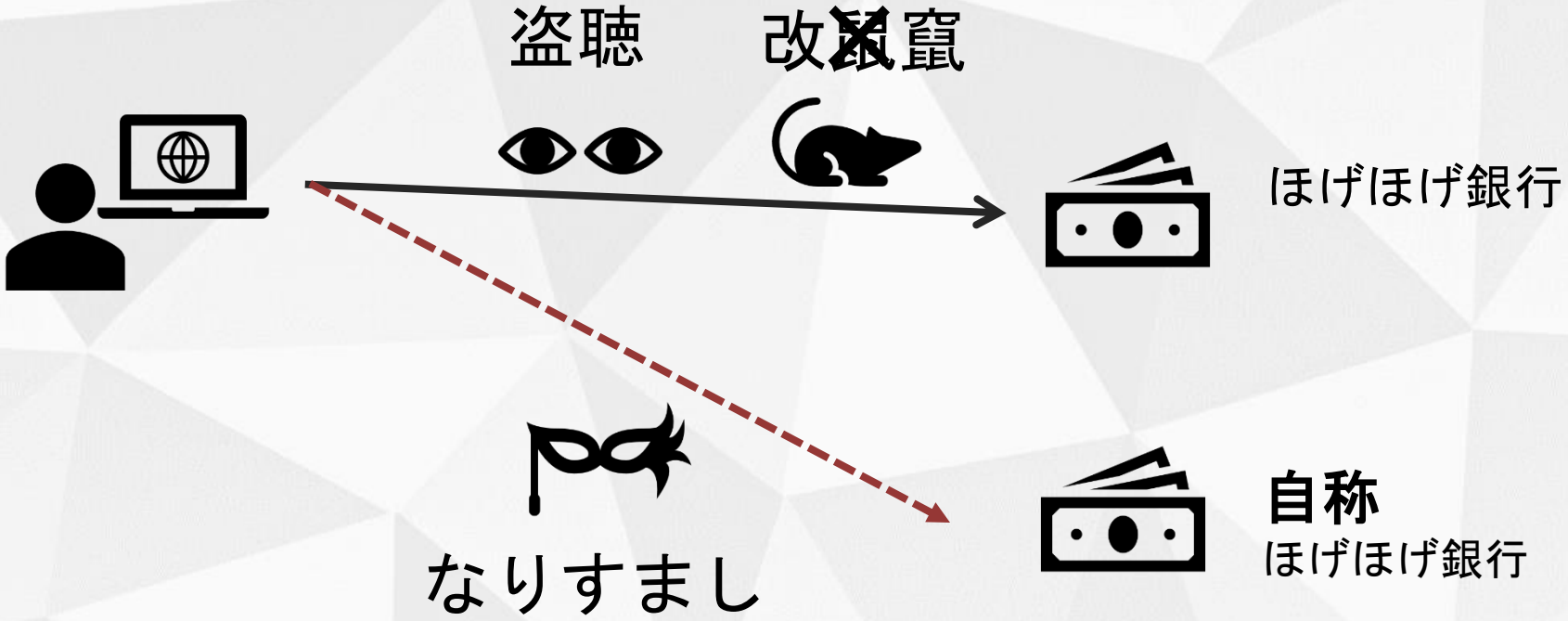
- E2Eの原則(end-to-end principle)
  - 通信の経路では基本的に何もしない。
  - 全てのホストは、途中の通信路が中身に関与せず通ることを前提にふるまう。
  - 違法情報（誰にとっても違法な情報）の規制は、発信側のエンドで行う。（削除、検挙など）
  - 青少年など特定の受信者にとって有害な情報は、受信側のエンドで行う。（フィルタリングなど）

前提としての技術的動向(2)

- ブロッキング(2011)～現在(2019)までに、何が起こったか。
- 常時TLS(SSL)化の進展
  - 火をつけたのはスノーデン氏の告発
- アクセス警告でも(ブロッキングでも)、常時TLS(SSL)化は思いっきり逆風
- そのTLS(SSL)ってなんですか？

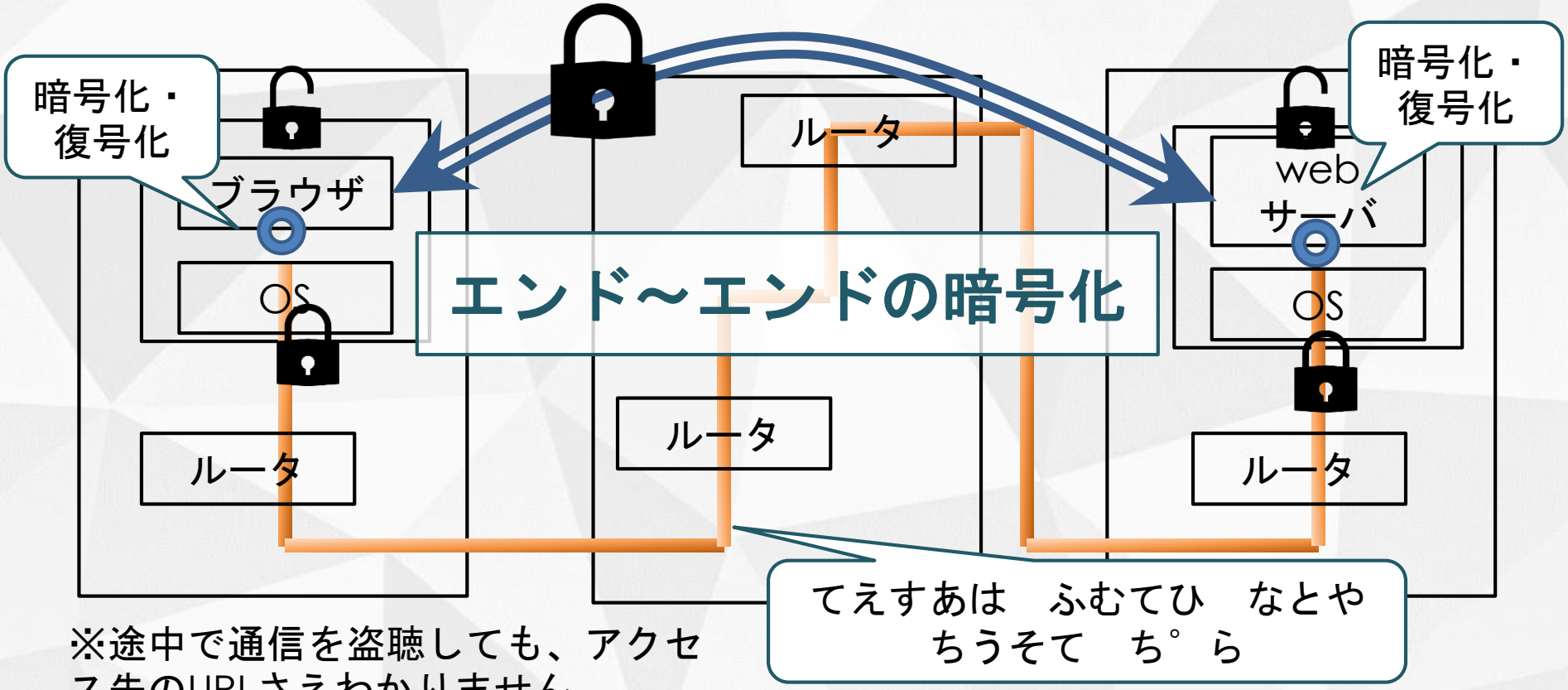
前提としての技術的動向(3)

- ネットであってはならないこと



前提としての技術的動向(4)

- 盗聴、改ざん、なりすましへの対策



※途中で通信を盗聴しても、アクセス先のURLさえわかりません

前提としての技術的動向(5)

- 盗聴の防止
- 改ざん、なりすましの防止
- TLS(SSL)は、これらを一気に可能にする技術

とりあえず、暗号化できればよい

電子署名や電子証明書の技術が必要

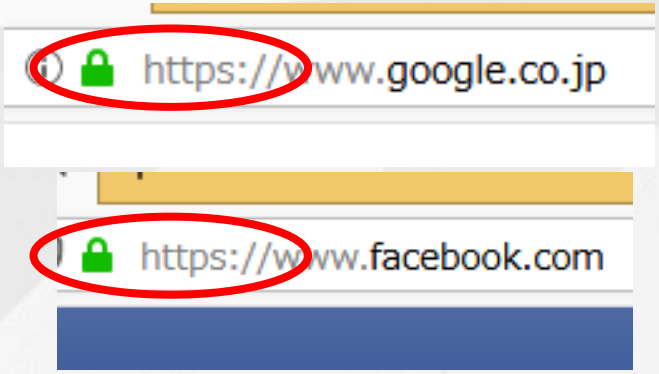
とりあえずここでは
「TLS=SSL=HTTPS」 と思っていただいて大丈夫です。
HTTPは暗号化なし、HTTPSは暗号化ありです。

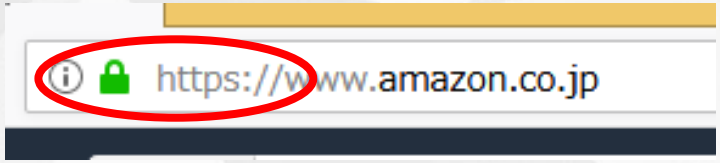
前提としての技術的動向(6)

- おなじみの南京錠のマーク

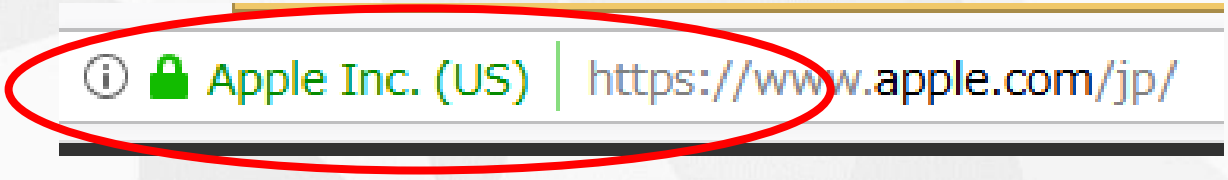
前提としての技術的動向(7)

- サイトにアクセスするときは、「安全な接続」を示す南京錠のマークをご確認ください

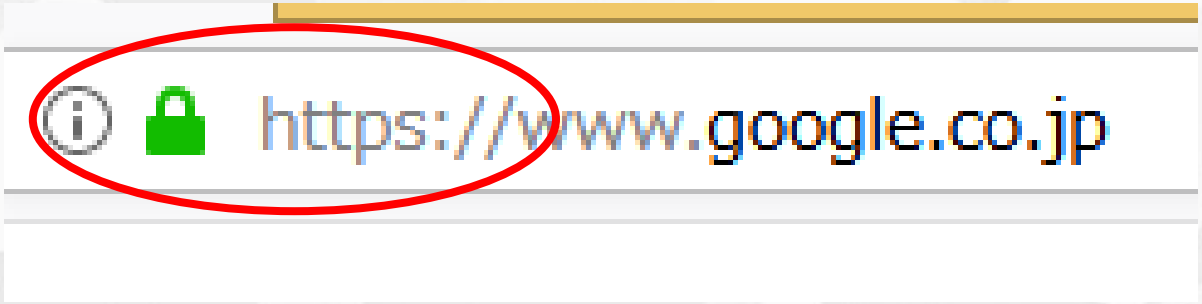




- 一部（主に銀行など）では、サイト運営者の登記簿などを確認したうえで発行される証明書も普及



前提としての技術的動向(8)



- 南京錠のマークが保証すること
  - 内容が暗号化され、途中で盗聴されないこと
  - 途中で改ざんされたら、それを検出できること
  - **接続先が確かに、そのサイトであること**
    - 意外と意識されていないのですが、ここがすごく重要な役割なのです。
    - 電子証明書を使っています。

前提としての技術的動向(9)

- 「なりすまし防止」について簡単に

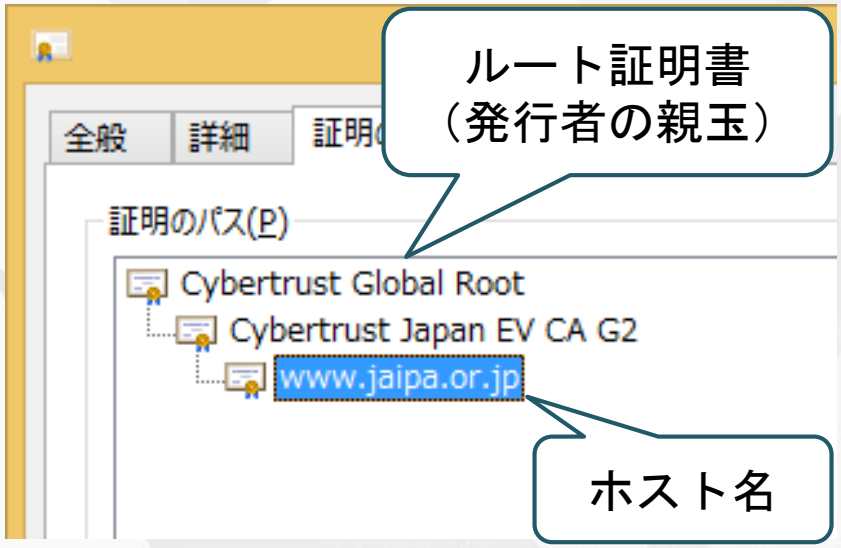
ほげほげ銀行
webサーバ

自称ほげほげ銀行
webサーバ

TLS(SSL)は通信の前にサーバの証明書を検証し、本物であれば通信を継続するしくみ。

前提としての技術的動向(10)

- 証明書の安全性を守る
  - 偽のwebサーバが横行すると電子商取引の基盤も一気に崩壊するので、証明書の発行プロセスは決まっている。
- ブラウザは、きちんとした発行者の証明書を信用する。
  - ドメインの管理者、法人の代表者などの意思を確認するプロセスを守るところでないと、ブラウザは信用しない。



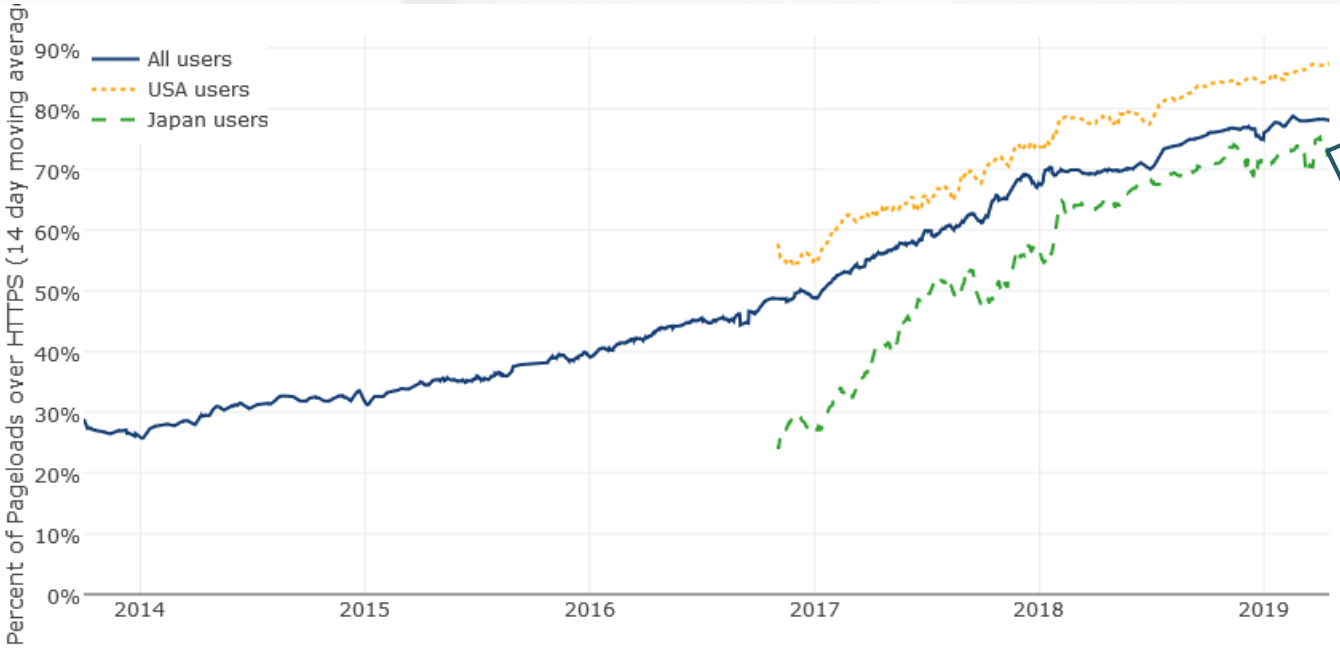
前提としての技術的動向(11)

- 今、HTTPS未対応のサイトはここまで言われる

(出典)ある中央省庁のwebページ（一部モザイク）

前提としての技術的動向(12)

- TLS(SSL)を利用したwebアクセスは急増



日本のユーザのHTTPSアクセス割合
26%(2016.11)
→**73%**
(2019.4)

Firefoxでのアクセス統計。
(出典) https://letsencrypt.org/stats/

前提としての技術的動向(13)

- web閲覧だけではありません！

おなじみのスマホアプリも、裏ではほとんど暗号化通信。
銀行はもちろんですが、ゲームもチートを防ぐために、おそらくTLSだと思います。

アクセス警告方式とHTTPS(1)

- 法的にはともかく、技術的には。。。

アクセス警告方式は、
・利用者のアクセス先がどこであるかを確認して、
・警告サーバが正規のアクセス先の代わりに、
・本来のコンテンツを警告画面に差し替える
ことが必要。

アクセス警告方式とHTTPS(2)

- 法的にはともかく、技術的には。。。

アクセス警告方式は、
・利用者のアクセス先がどこであるかを確認して、
・警告サーバが正規のアクセス先の代わりに、
・本来のコンテンツを警告画面に差し替える
ことが必要。

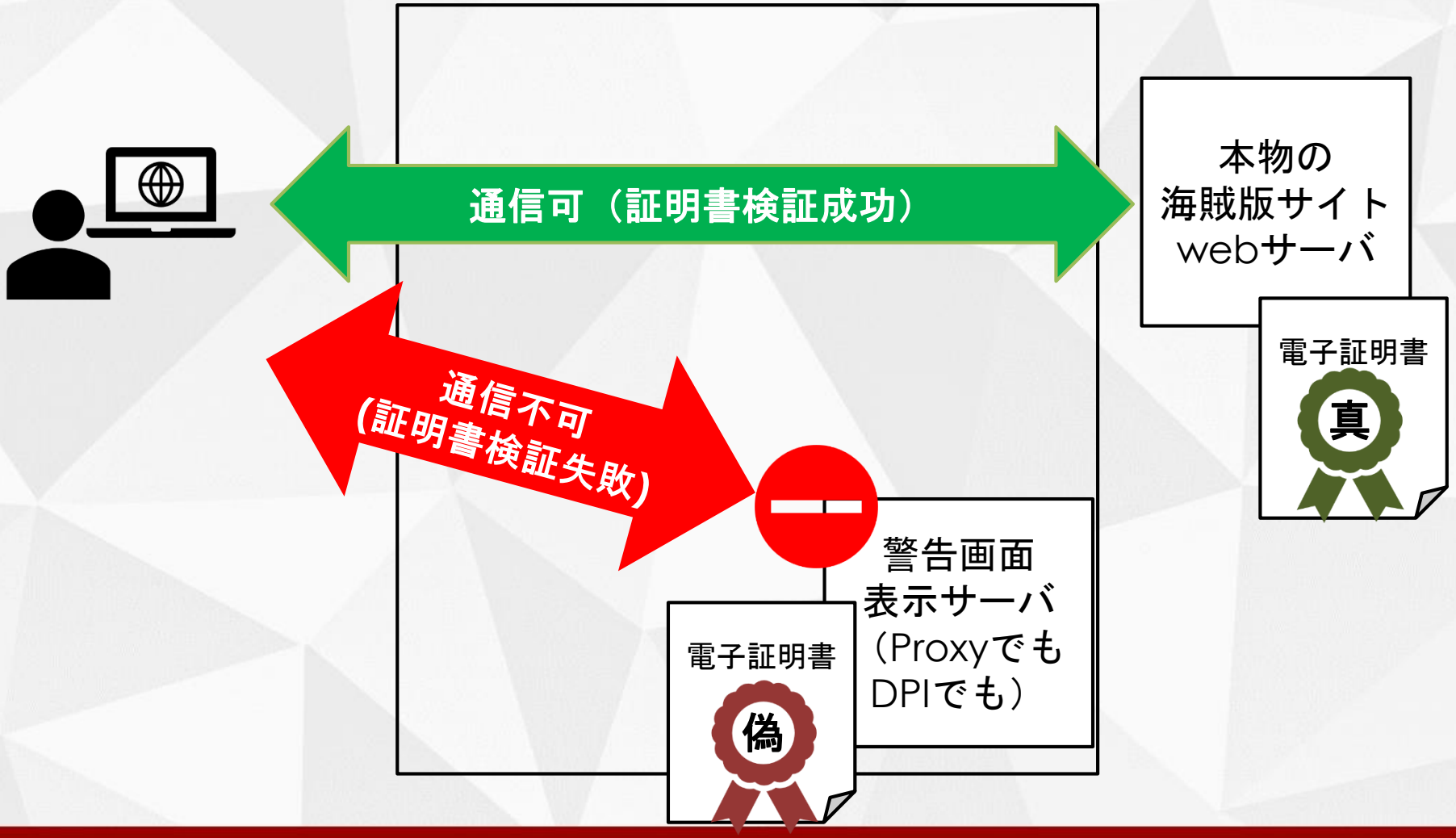
盗聴

なりすまし

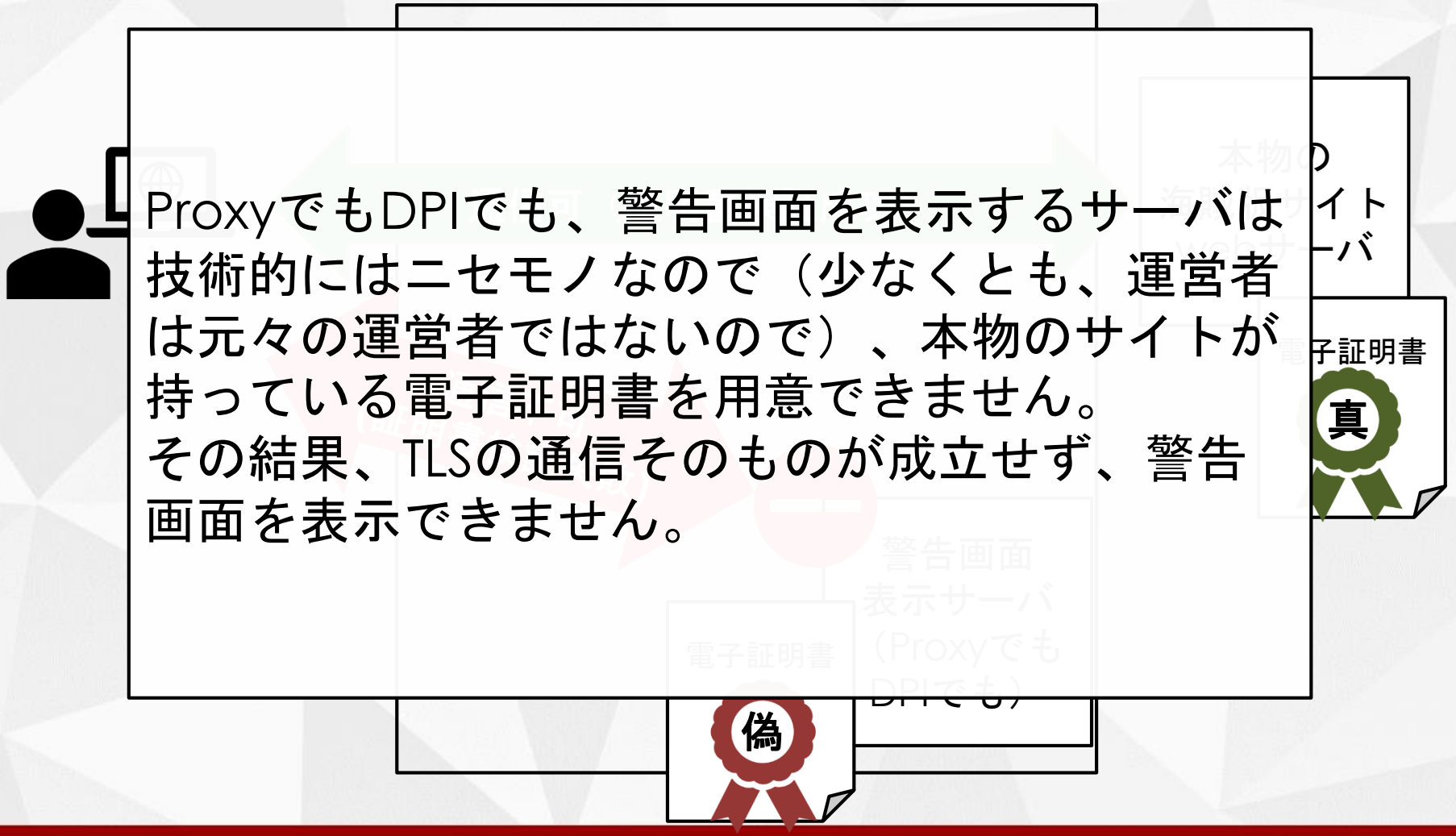
改ざん

→どれも、SSL(TLS)で防御する対象そのもの

アクセス警告方式とHTTPS(3)



アクセス警告方式とHTTPS(4)



アクセス警告方式とHTTPS(5)

- webアクセスの73%がTLS(SSL)化されている中で、技術的には「盗聴・改ざん・なりすまし」と同じことをしようとしていることは、一応ご理解いただいて損はないと思います。。。
- それが世の中で許される行為かどうかは、多分に法的な価値判断でありまして、、、技術的には「盗聴・改ざん・なりすまし」と区別できません。。。

アクセス警告方式とHTTPS(6)

- 常時SSL(TLS)化が進むのは、改ざん・なりすまし防止の点で望ましいこと。
  - 銀行のサイトがなりすまされたら・・・
- 実際に安全であるし、監視されるのは誰でも気持ち悪いので、この流れは止めようがない。
- ということは、NW上で通信をコントロールすることは不可能になっていく。

アクセス警告方式とHTTPS(7)

- DNS＋Proxy方式でもDPI方式でも、アクセス警告方式を適用できるのは、残り少なくなったHTTPS未対応サイト。

Firefoxでのアクセス統計。
（出典）https://letsencrypt.org/stats/

アクセス警告方式とHTTPS(8)

質問です。海賊版サイトがHTTPSになることはあるのでしょうか？

サーバ証明書はサイトの管理者なら誰でも最短15分で取得できます。

海賊版サイト運営者は、身分証明書とか出せないのでは。。。

一番簡単な証明書は、ホストの管理権限（サーバを自由に操作できる権限）が確認できれば発行されます。

そんな簡単で、証明書の意味があるのでしょうか。。。

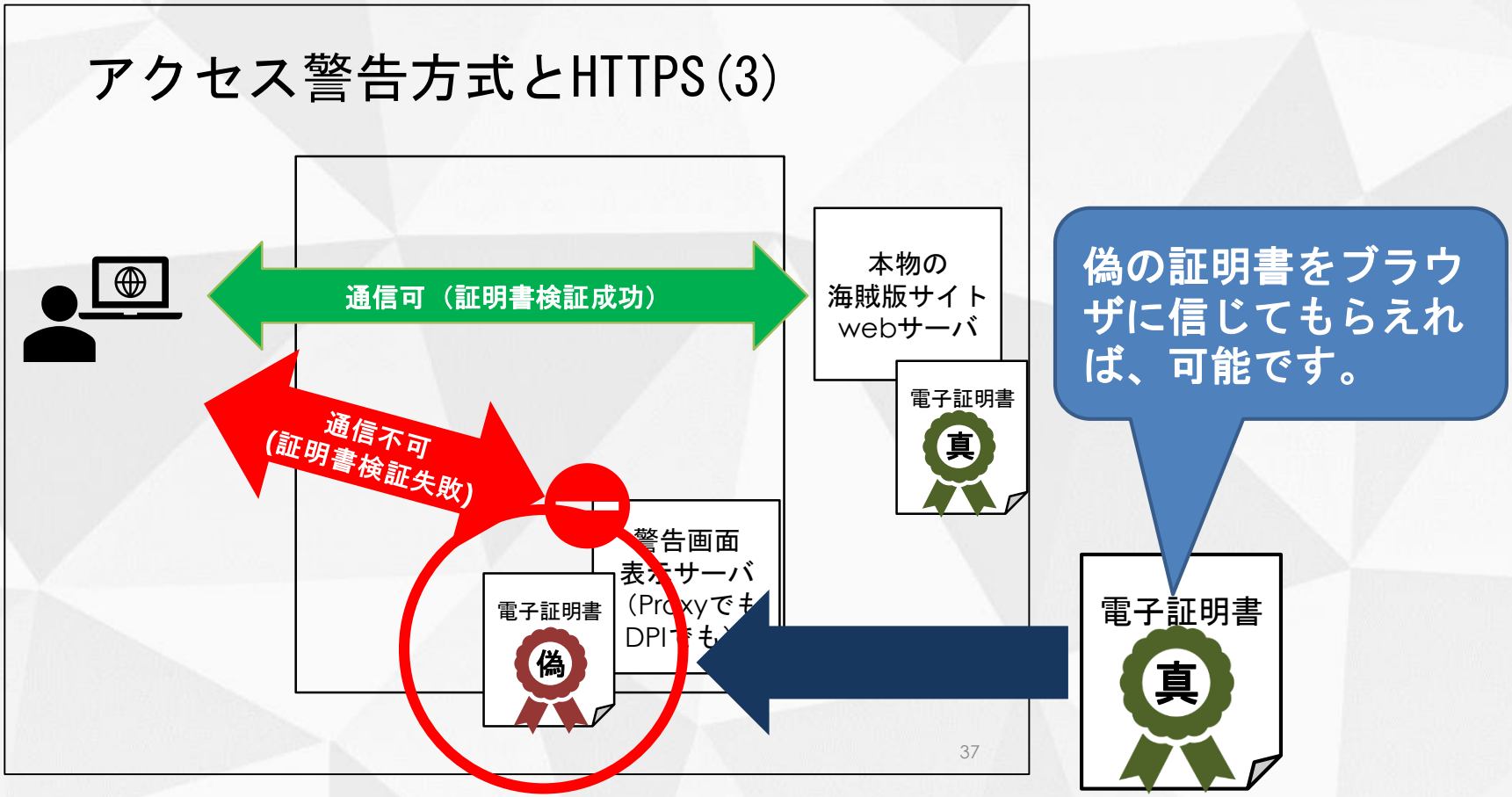
まずはサーバのなりすましが防げればいいので、管理権限があれば大丈夫ということなんだと思います。

アクセス警告方式とHTTPS(9)

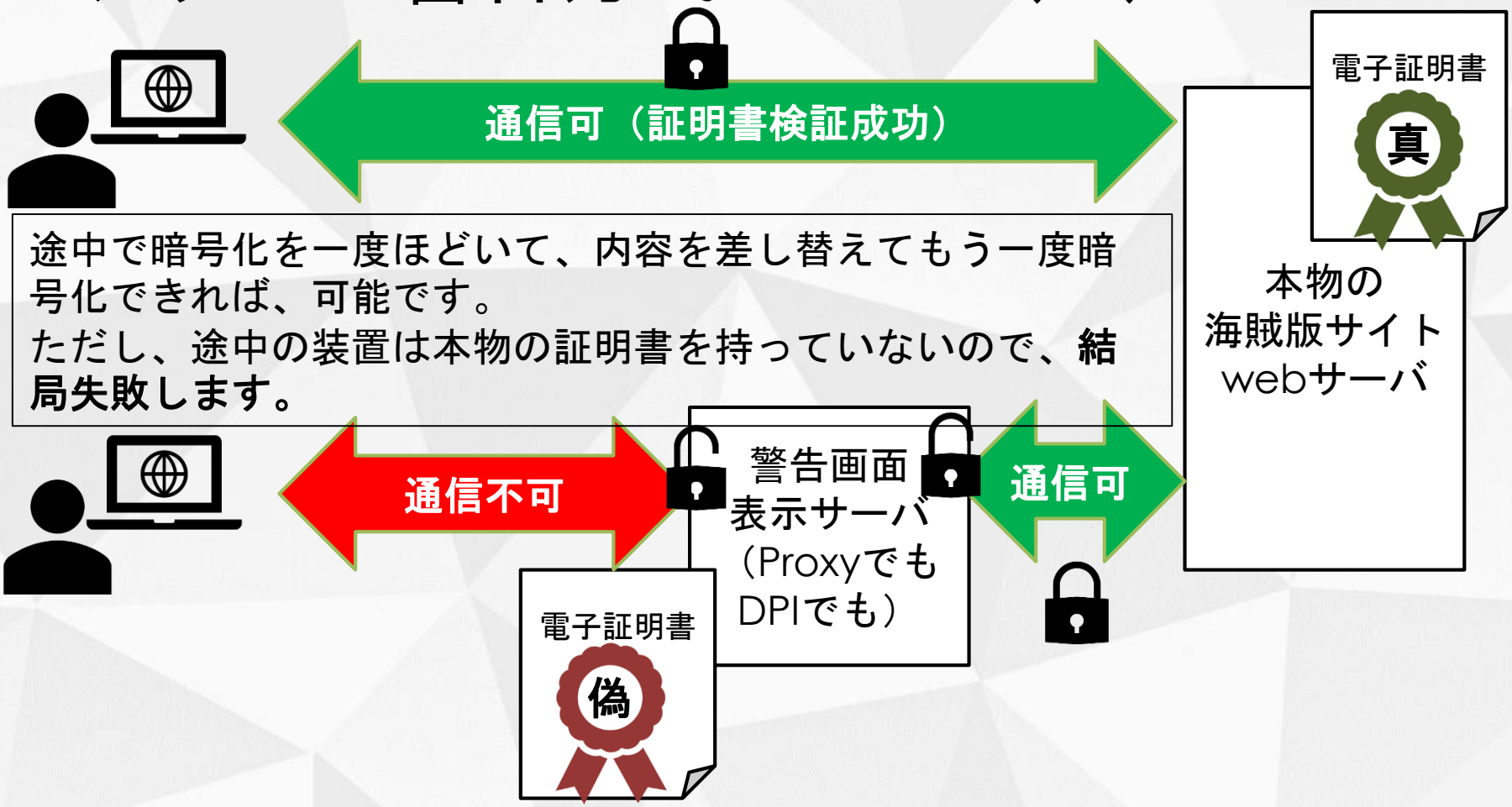
質問です。私の勤めている会社では、HTTPSでも転職サイトや業務に関係のないサイトがフィルタリングされるそうです。HTTPSでは、通信の途中でコントロールできないのではないですか。

利用者が特定の人に限られた、企業内LANなどの環境であれば可能です。

アクセス警告方式とHTTPS(10)

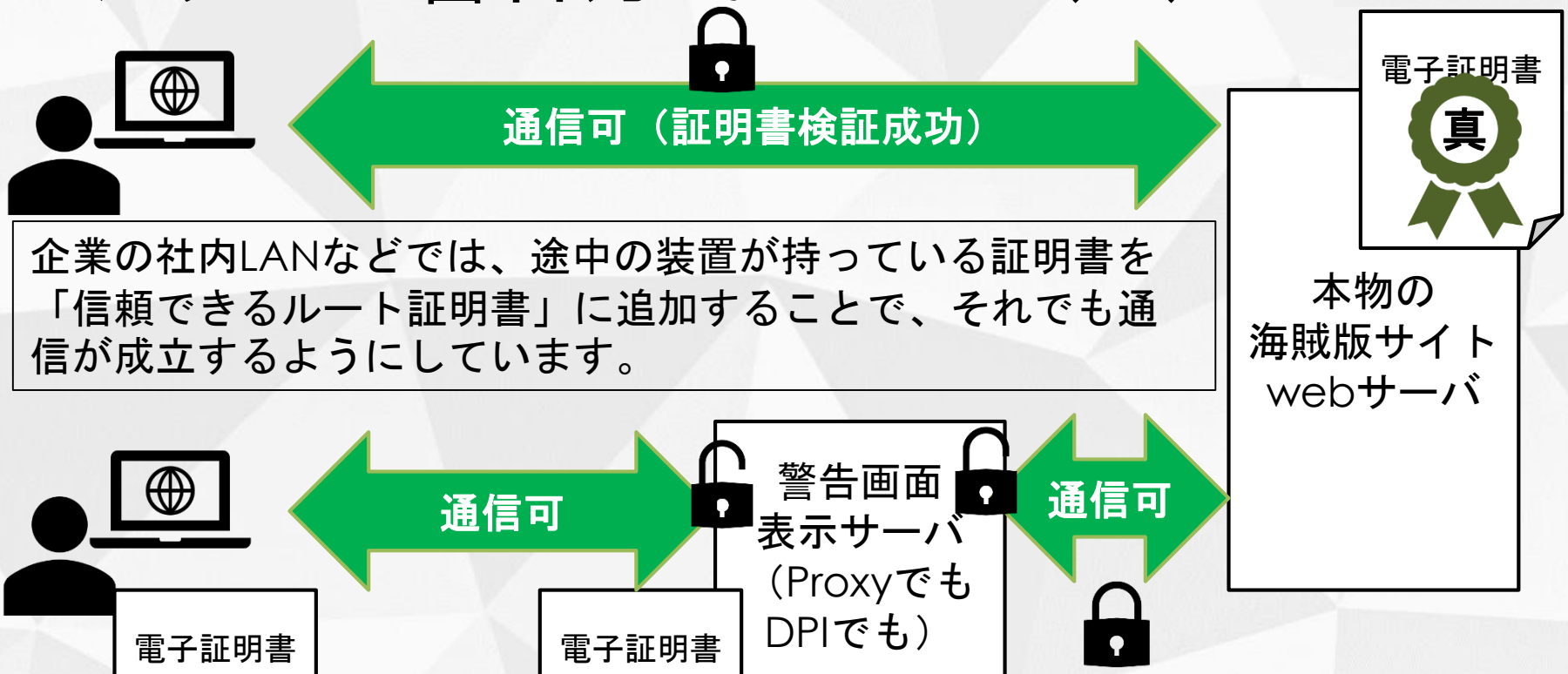


アクセス警告方式とHTTPS(11)



実際にはサイトの証明書を途中の装置で動的に生成し、装置が持っている証明書で再署名する方法がとられていますが、ここでは簡略化しています。

アクセス警告方式とHTTPS(12)



アクセス警告方式とHTTPS(13)

お客さまへお願い

平素、〇〇ネットをご利用くださいましてありがとうございます。

当社では、一層のセキュリティ向上と、海賊版サイトへの接続抑止のため、**お客さまのブラウザに、以下の通りルート証明書をインストールしていただくことをお願いすることとなりました**。

つきましては、次のページに示すリンクに従って・・・・

株式会社〇〇ネット

アクセス警告方式とHTTPS(14)

プロバイダがルート証明書インストールしろとか、胡散臭すぎるだろｗｗｗ

フィッシングメールかと思った

これで総務省OKしたの？

怖っwww

まったく誇張ではなく、セキュリティの観点からは、みなさんが最低限、これくらいのリテラシをお持ちであることを期待したいものです。。。
ルート証明書をインストールするという手段は、商用NWでは難しいです。

アクセス警告方式とHTTPS(15)

質問です。プロバイダのプロキシやDPI装置が持っている証明書を、最初からブラウザの「信頼できるルート証明書」に入れてもらえばいいのではないですか？

ブラウザの開発元が応じてくれれば、可能です。

ただし、相手にされない上に、世界の笑いものになってしまう可能性が高いですが。。。

・そもそもTLS(SSL)のしくみが、途中での盗聴やなりすましを許さないという目的であるため、いくら目的が（日本において社会的に）正当だといっても、「途中で一度暗号化をほどいて再署名したいから」という理由は、まったく受け入れられないと思います。
・主要なブラウザは世界中で使われており、技術的にも世界標準に準拠しています。日本での海賊版対策のために例外が受け入れられるならば、他国の政府が「国家の安全を守るために検閲をしたい」といっても拒否する理由がないため、標準化の枠組みでも「通信経路での介入は一律受け入れない」ということになるでしょう。

～まとめ～

アクセス警告方式に限らず、ネットワークの途中で何かをするということ自体が、技術的には難しくなっていきます。

まとめ(1)

- DNS+Proxy方式、DPI方式いずれであっても、技術的にはHTTPSへの対応が難しいことが課題となります。
- HTTPS自体は安全な通信を実現する技術で、電子商取引の基盤としても、基本中の基本です。
- HTTPS通信の割合は急上昇しており、今の段階ですでに「webのアクセスのほとんどは、途中で制御できない」という状態です。
  - さらにいうと、DNS通信にも暗号化や署名を付けるようにしよう、という流れになっています。
- お金や労力をかけてアクセス警告方式を導入しても、制御可能な通信が現時点で2割～3割程度しか残っていないことは、議論の前提事実といえるでしょう。

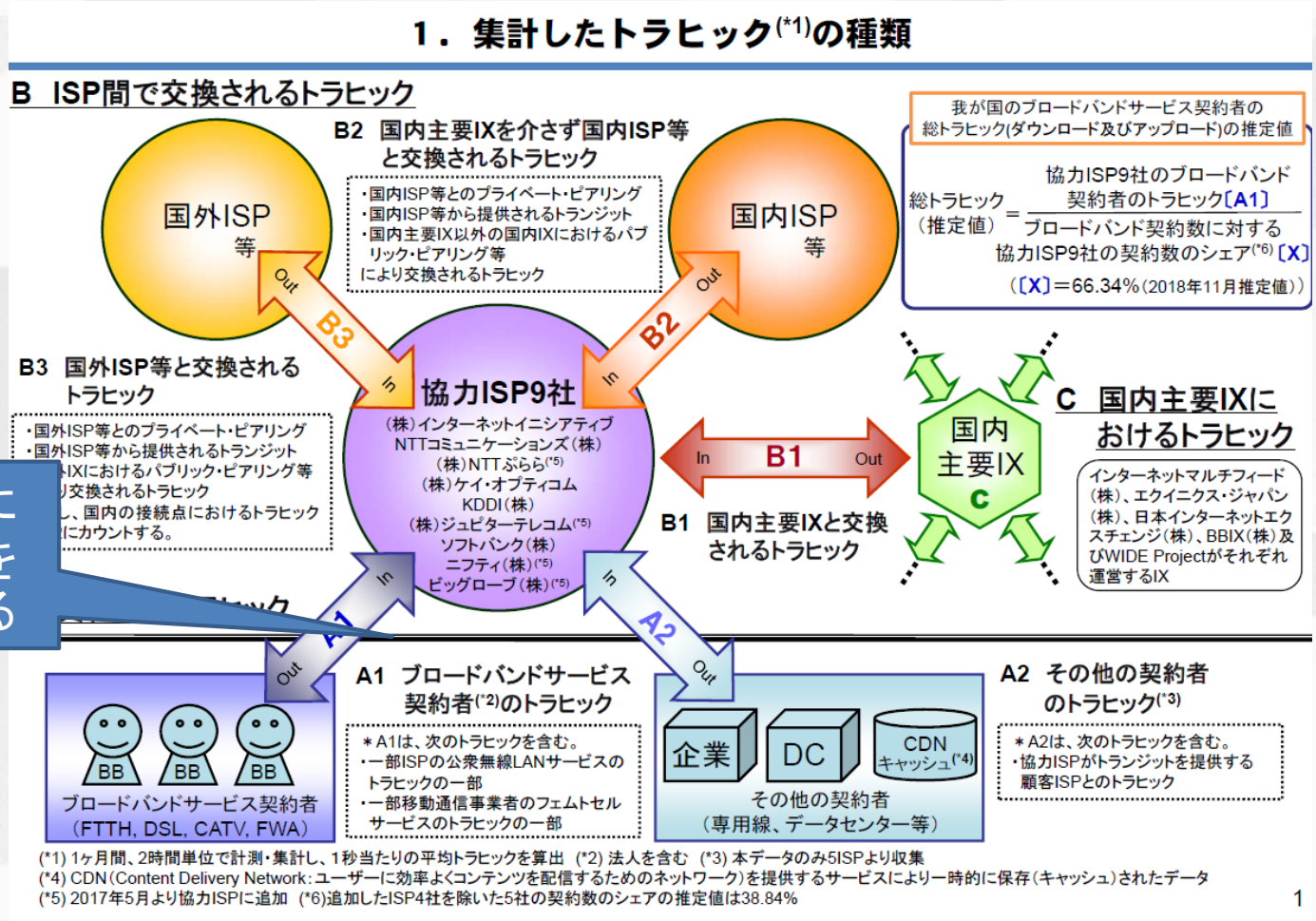
まとめ(2)

- 根本的には、end-to-endの原則が徹底する方向で技術的には一貫しています。
- ネットワークの途中で通信をコントロールすることは、この流れと真っ向から対立することになります。
- 仮に誰かがNWの途中で何をしようとしても、それを意に介さず通信が通るようなプロトコルや方式が開発され、標準になってしまうのが、ネットの技術史といっても過言ではないです。
- ネットにおける不正行為対策は、やはり通信のエンドで行うことを基本に考えていただくのがよいでしょう。そのほうが結局成果を出せると思います。

参考資料

総務省　平成31年(2019年)3月5日公表　我が国のインターネットにおけるトラヒックの集計・試算

2018 年11 月の集計結果



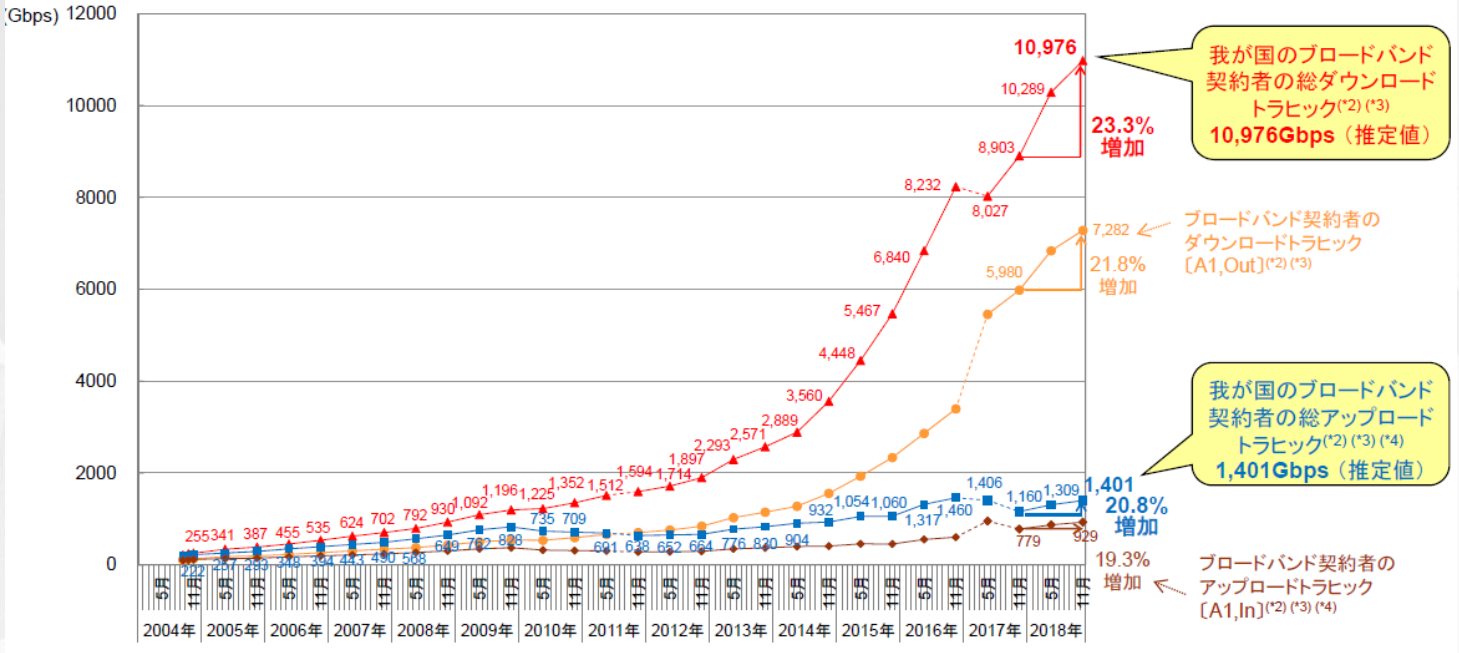
(※)電気通信サービスの契約数及びシェアに関する四半期データの公表（平成30年度第2四半期（9月末））より

対象となるトラヒックは2018年11月時点で11Tbps*
ただし、これは24時間平均のため、装置はピーク時を考慮して、最低でもその3倍程度は必要と思われる。

*ダウンロードとアップロードは同じ箇所を通るが、多いほうに合わせる

2．我が国のブロードバンド契約者の総トラヒック

○ 我が国のブロードバンドサービス契約者(*1)の総ダウンロードトラヒックは推定で約11.0Tbps（1日あたり約119PB。前年同月比23.3%増）。
○ また、総アップロードトラヒックは推定で約1.4Tbps（1日あたり約15PB。前年同月比20.8%増）。



(※)電気通信サービスの契約数及びシェアに関する四半期データの公表（平成30年度第2四半期（9月末））より