2A1-3

偽装した名前解決レスポンスを用いた不正サイトアクセス防御システムの実装と評価

2013/10/22
(株)NTTデータ
宮本 久仁男
miyamotokn@nttdata.co.jp

NTT DATA

本日の発表内容

- 本研究の背景
- Webアクセス時の通信概略と攻撃の前提条件
- Webアクセスを安全に行わせるための先行技術と課題
- マルウェアの初期動作と着目すべき点
- 偽装した名前解決レスポンスを用いた不正サイトへのアクセス防御法概要
- 偽装した名前解決レスポンスを用いた不正サイトアクセス防御システムの試作と評価
- むすび

本研究の背景

NTT DATA

● 大前提：

外部通信を行う機会の多くが、個人ユーザ／企業ユーザともにHTTPやHTTPS経由である

企業ユーザの多くが Proxy 経由でHTTPやHTTPS通信を行う

● マルウェアそのもののアクセス特性の変化

- 被害者PCのHTTPアクセスを契機に感染・活動を開始するマルウェアが増加している
- マルウェア自体も HTTP/HTTPS を用いて攻撃者と通信を行う
- マルウェアの通信先指定に、FQDNを使うことが増えている
- 特定の FQDN へのアクセスは、ファイアウォールで止めることは困難である

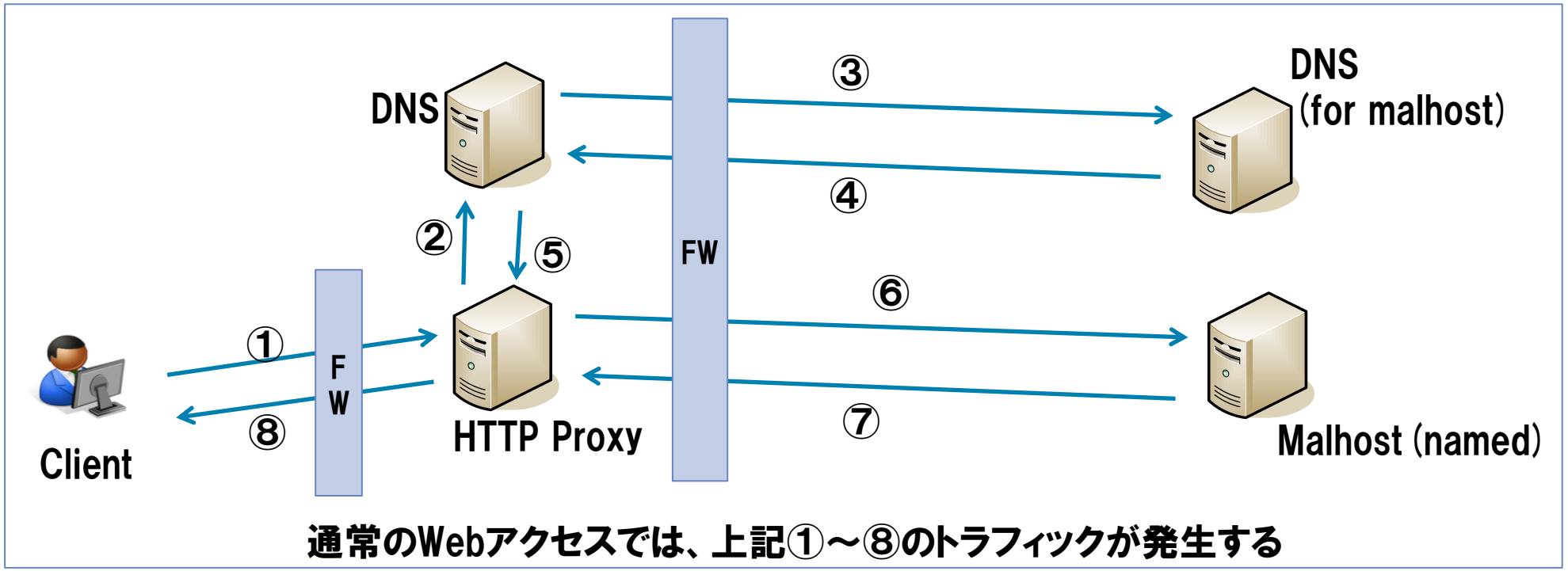
● システムを安定して運用する上の希望

- システムに含まれる既存の機器やソフトウェアには極力手を入れたくない
- 装置故障やメンテナンスに起因する通信停止は避けたい
- 可能な限り通信を行える状態を確保したい

● セキュリティ対応を行う側の希望

- 不審な通信先への通信をタイムリーに止めたい
- 疑わしい通信先に絞って止めたい
- 疑義が晴れた通信先については、止めるべき理由がない限りはタイムリーに通信を再開させたい

Webアクセス時の通信概略と攻撃の前提条件



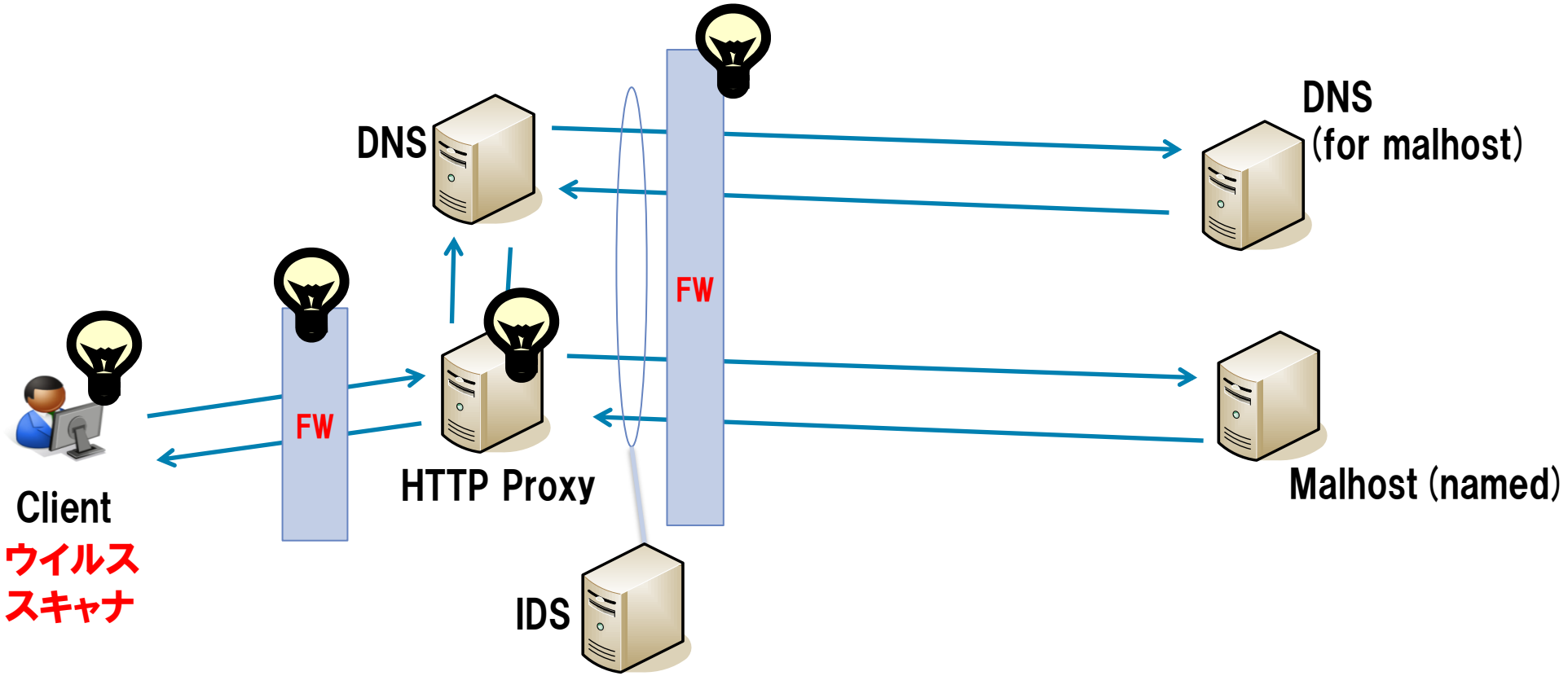
通常のWebアクセスでは、上記①～⑧のトラフィックが発生する

●前提

（1） 特定のFQDNを持つホストが、ウィルス等の配布元になっている

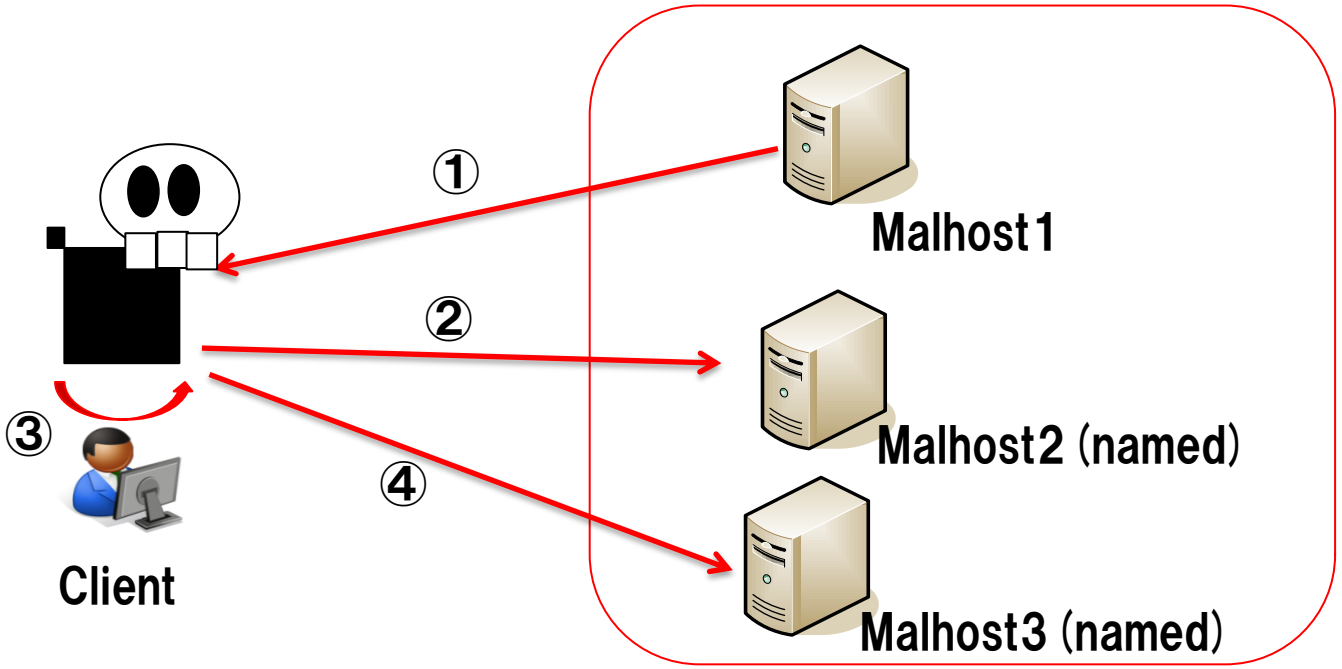
（2） ウィルスを保持している悪性ホスト（図中Malhost）へのアクセスは、通常のWebアクセスと同様にHTTP Proxy経由でアクセス等を行う

Webアクセスを安全に行わせるための先行技術と課題



ソリューション	機能／可能な処理	課題
ウイルススキャナ	個々のPCにダウンロードされるウィルス等の検知・駆除	すでに把握されているウィルス等の挙動や特徴をもとに、エンジンやパターンファイルが作られている
Proxy	悪意あるWebアクセスの防止をおこなう仕組みを追加可能	アクセス禁止先のタイムリーな追加が困難
FW（ファイアウォール）	特定のIPアドレスやポートへのアクセス遮断	ホスト名を用いたアクセス遮断が困難
IDS	攻撃につながる通信を検知可能	攻撃時の通信挙動や特徴を事前に把握する必要がある

マルウェアの初期動作と着目すべき点



①被害PCに感染（外部ホストMalhost1との通信がトリガ）

②攻撃者が準備したコンピュータ（Malhost2／外部）と通信

③被害PCを中心とした情報収集活動

④攻撃者が準備したコンピュータ（Malhost3／外部）と通信

②や④の通信を検出後タイムリーに止められるしくみが必要

偽装した名前解決レスポンスを用いた不正サイトへのアクセス防御法概要

名前解決の妨害によるWebアクセス制御（1/2）

NTT DATA

- 従来のWebアクセス制御：Proxy等に実装

  Proxyにブラックリストを保有する形で実現

  従来機器に、**ブラックリストによるアクセス制御機能を付加する必要あり**。

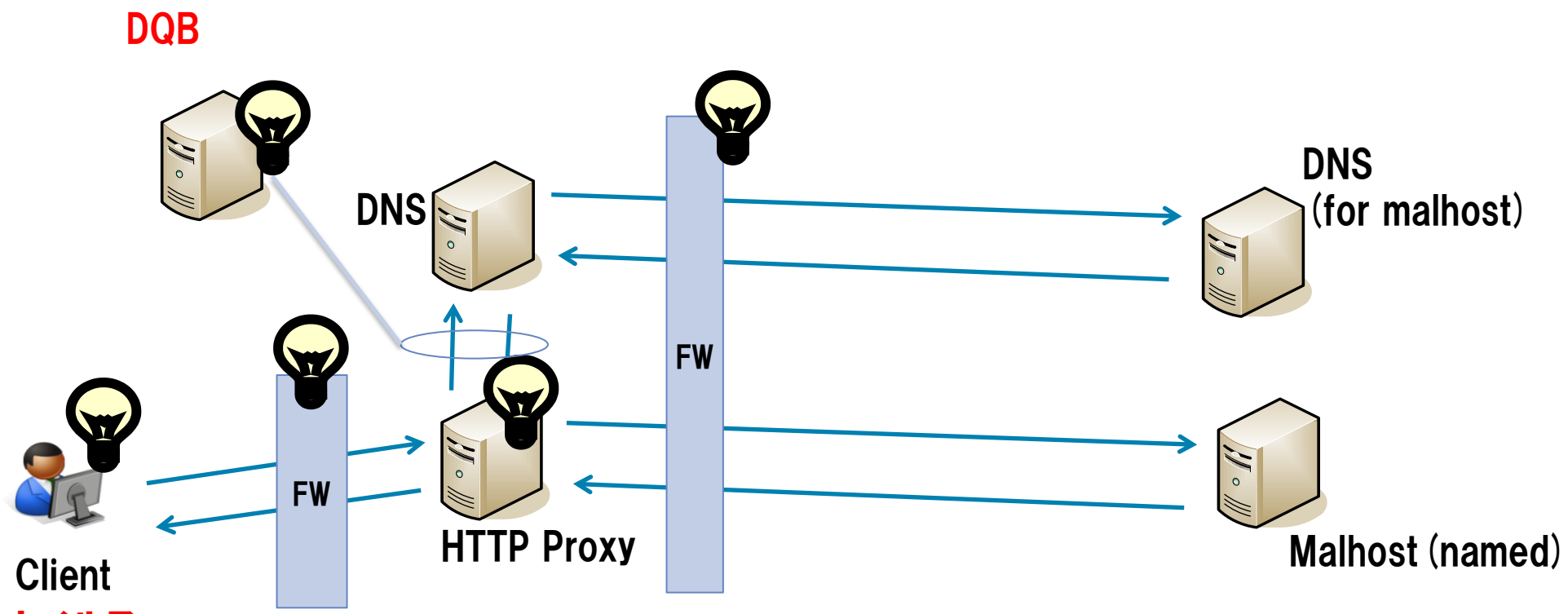
  付加した後の運用にもよるが、タイムリーなアクセス制御対象の追加は、**運用上難しい**ことが多い

- 名前解決の妨害によるWebアクセス制御：DNS等に実装

  名前解決を行う際に、悪意あるホストに関する名前解決を行わない／安全なホストへの誘導を行えるような形での名前解決を行う

・後者に着目し、名前解決を阻害するだけの装置によって、DNSクエリリクエストの送出を監視の上、対応する**DNSクエリリクエストが送られたら偽装レスポンスを送る**ようにする
　以降、本提案を「DNSクエリブロッカ（DQB）」と称する
・DNSクエリリクエストの監視については、Proxyのような形ではなく**ネットワークトラフィックを監視する形**で実現可能

名前解決の妨害によるWebアクセス制御（2/2）



ウィルススキャナ：個々のPC

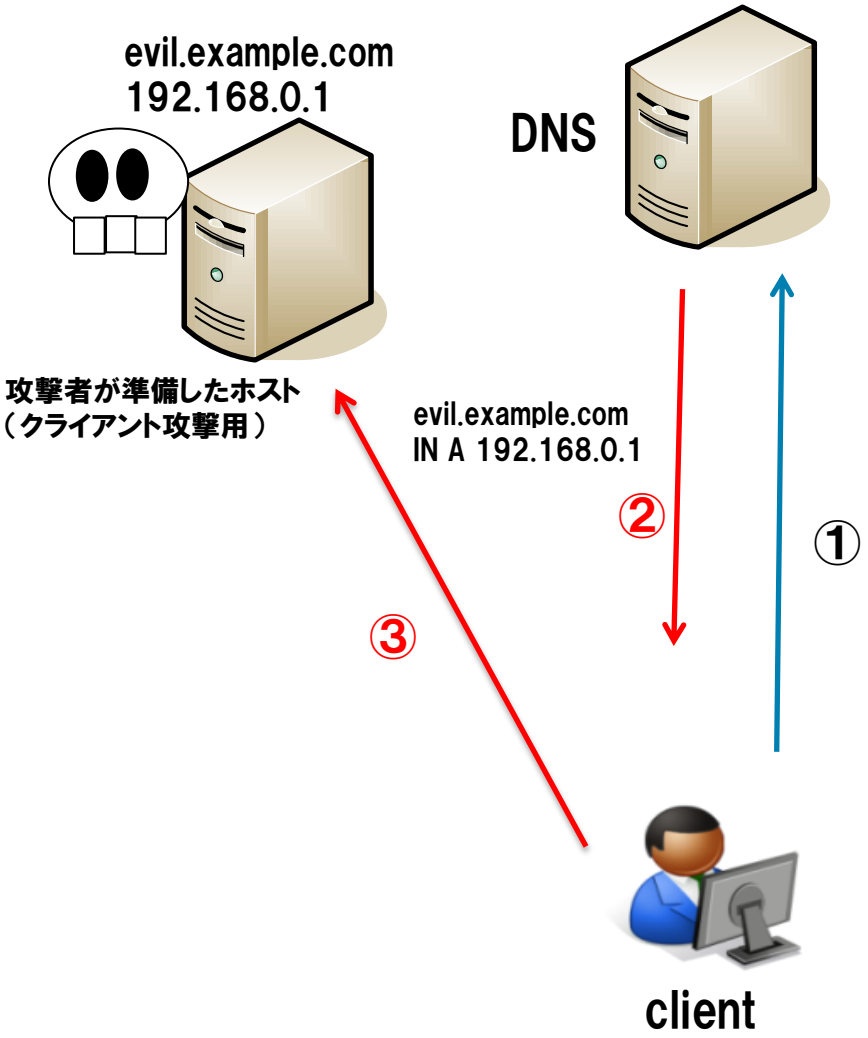
Proxy：悪意あるWebアクセスの防止をおこなう仕組みを追加可能

FW（ファイアウォール）：特定のIPアドレスやポートへのアクセス遮断

IDS：攻撃につながる通信を検知可能

DNSクエリブロッカ：名前解決の妨害によるWebアクセス制御を実現する

通常のWebアクセス時の名前解決処理の流れ

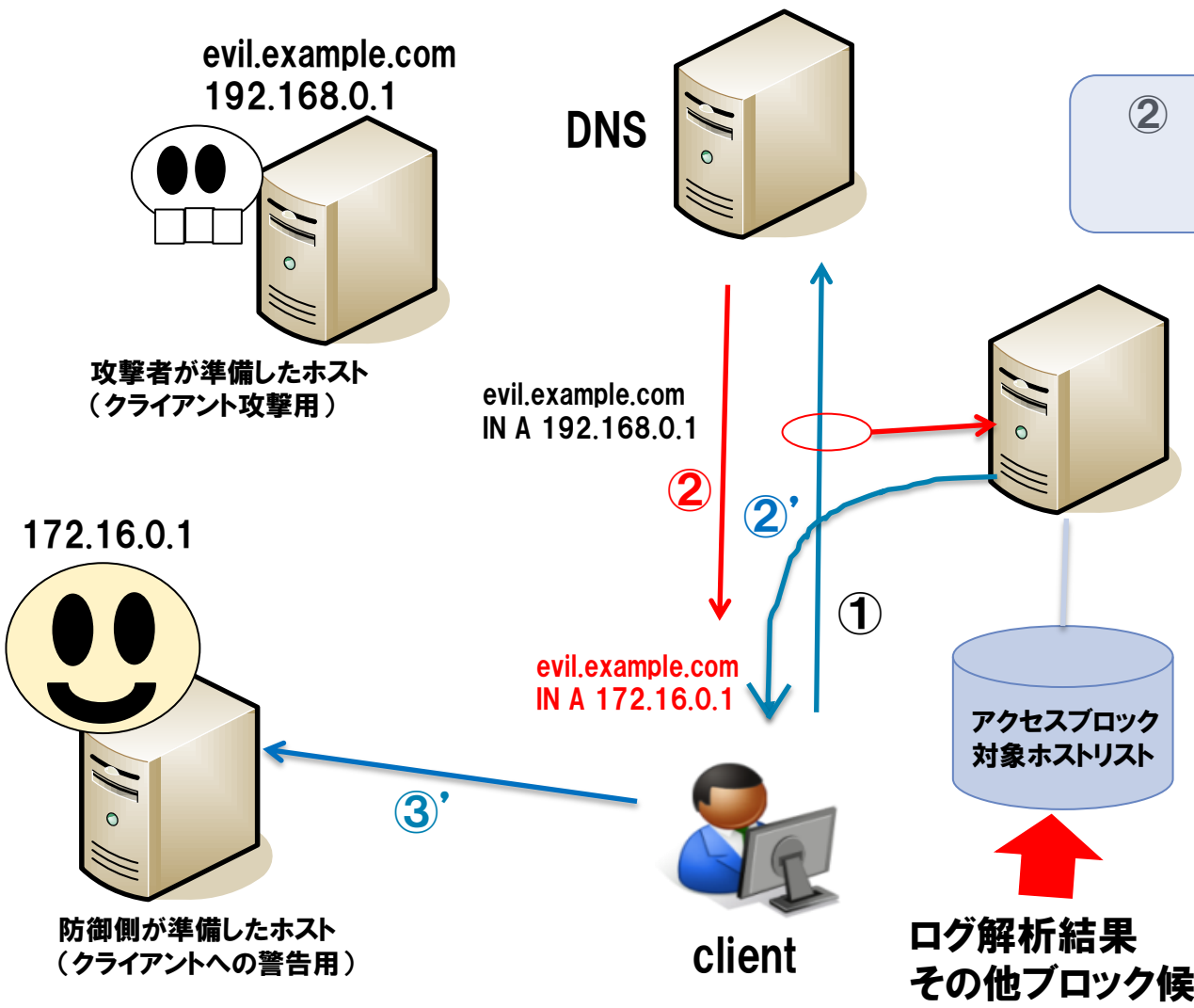


① clientはDNSに対し、evil.example.comのアドレスを要求（要求1）

② DNSはclientに対し、evil.example.comのアドレスを回答（192.168.0.1）（応答1）

③ Clientは攻撃者が準備したホストにアクセス

DNSクエリブロッカ動作時の名前解決処理の流れ



① clientはDNSに対し、evil.example.comのアドレスを要求（要求1）

② DNSはclientに対し、evil.example.comのアドレスを回答（192.168.0.1）（応答1）

この点に着目して

①のリクエストをモニタし、アクセスブロック対象ホストリストにアドレス解決リクエストを行われてるホストが存在したら、②が到達する前に②'を送出（172.16.0.1）（応答1'）

clientは②'の回答を受け取り、偽のevil.example.com（172.16.0.1）にアクセス誘導される（③'の部分）

DNSクエリブロッカの利点と課題

NTT DATA

●DNSクエリブロッカの利点

（1）故障時も通信を妨げない

インライン型の装置と異なり、パケットキャプチャを行うことが基本となるため、基本的な通信を妨げない

（2）並列化による高速化が容易

同時にDNSクエリをモニタする装置を増やせば、増やした装置数分のリクエスト処理を行える

●DNSクエリブロッカの課題

（1）性能面

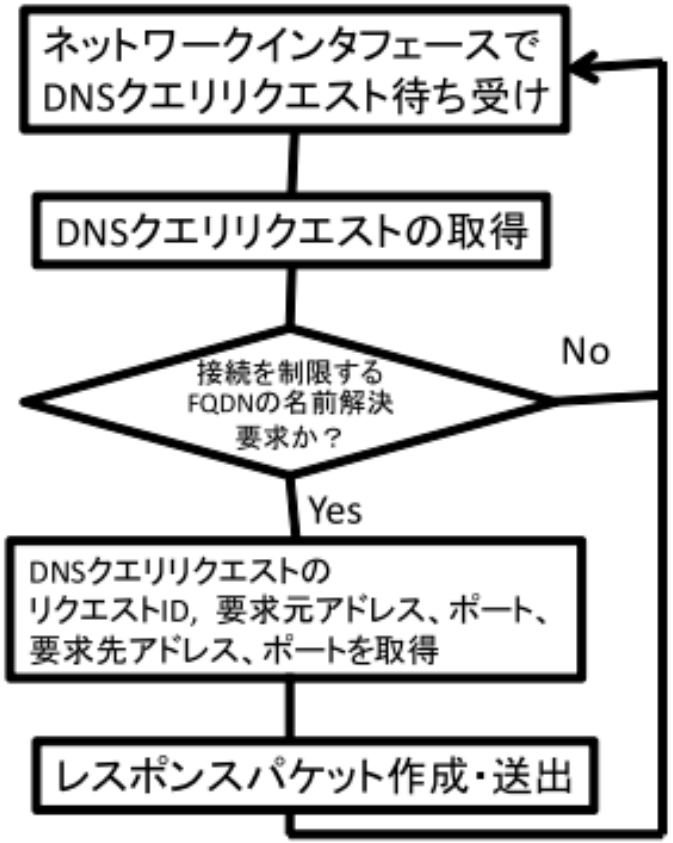
DNSのレスポンスパケットが返ってくる前に、DNSクエリブロッカからの偽のレスポンスパケットを返却しなければならないため、達成すべき性能目標がシビアである

（2）運用面

（1）の性能をクリアするための性能を維持しつつ、最小限の配置を行うための設計方法を確定させる必要がある

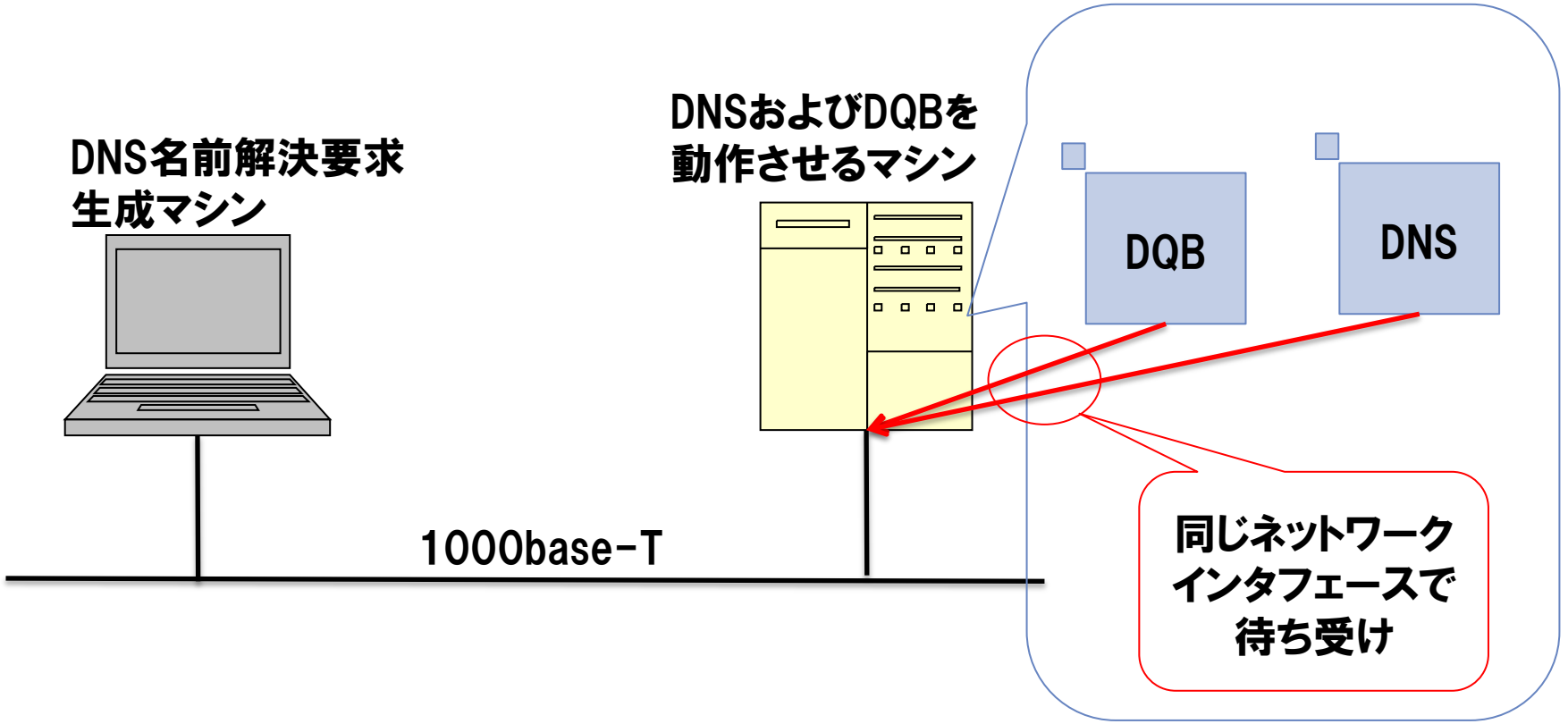
偽装した名前解決レスポンスを用いた不正サイトアクセス防御システムの試作と評価

DQB実装の処理の流れ

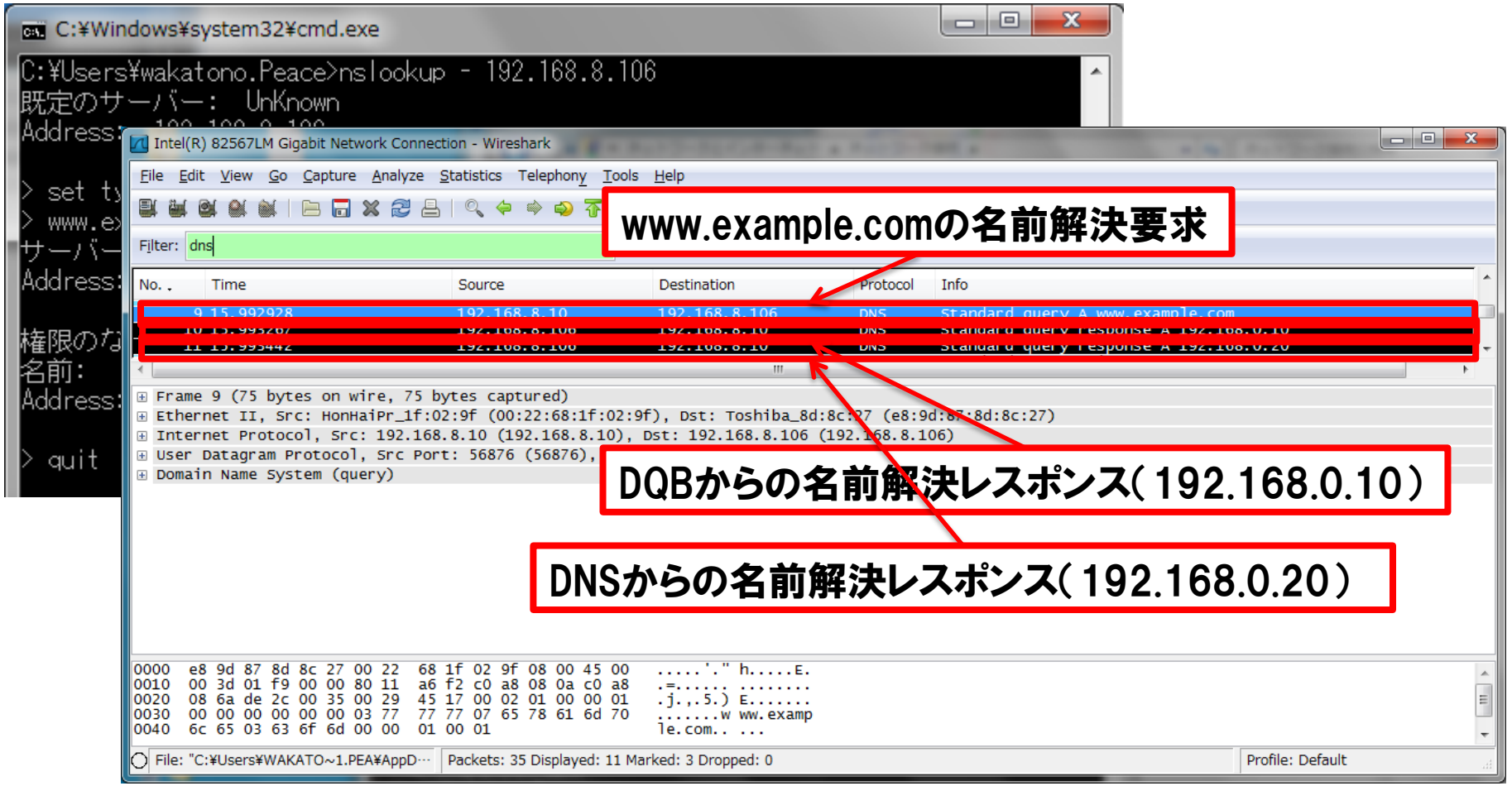


高速に動作させるため、
処理はシンプル

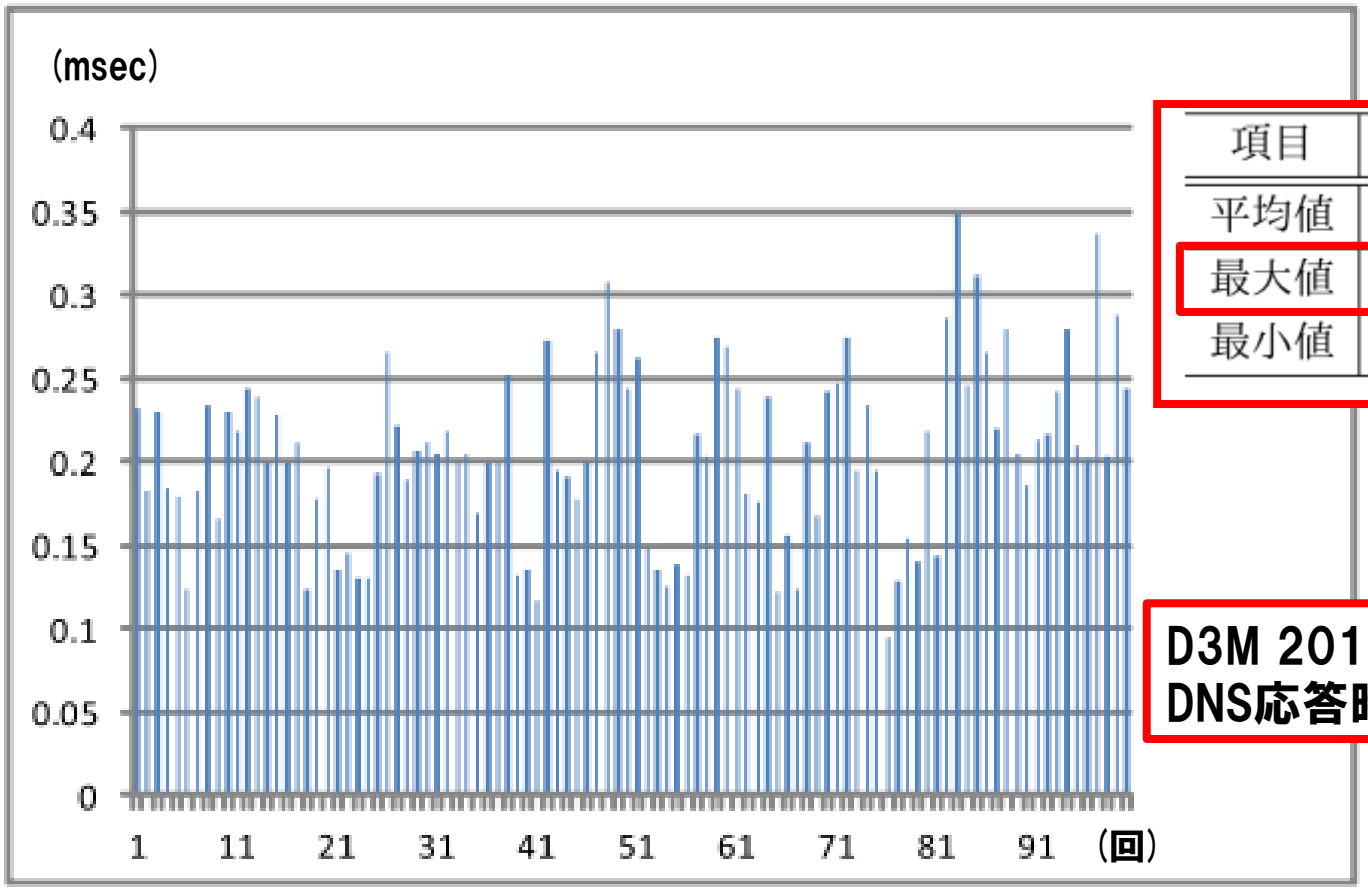
検証環境



実際の動作の様子



DQBからの応答時間計測結果



項目	値
平均値	0.206(msec)
最大値	0.348(msec)
最小値	0.095(msec)

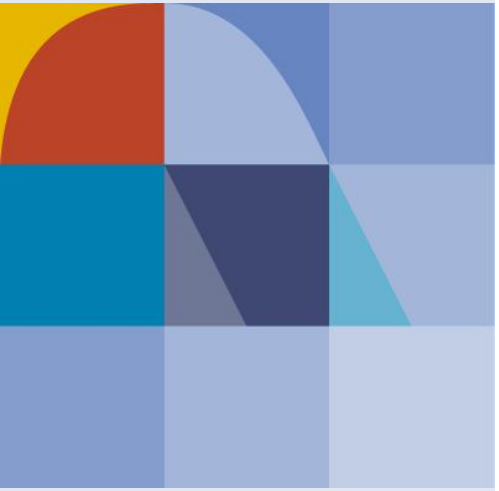
D3M 2010～2013での
DNS応答時間：全て10msec以上

むすび

- 名前解決に着目した、通信妨害のための方式を試作して、正しく機能することを明らかにした

- 検証環境での性能評価および、性能評価結果とMWS2013 DATAsets に含まれるDNSパケットから算出した名前解決レスポンスを取得する時間の最小値との比較を行い、試作システムが性能要件も満足することを確認した

- 今後は、より実環境に近い名前解決トラフィックが発生する環境で評価を行い、本システムの有用性を確認していくこととする



NTT DATA

Global IT Innovator