プロトコルの脆弱性の実例
～TCP の脆弱性から～

2004年10月5日(火)

JPNIC・JPCERT/CCセミナー2004

JPCERT/CC　鎌田敬介

KAMATA Keisuke

JPCERT CC

TOPIC

- 2004年4月21日に公開されたTCPの脆弱性
  - Transmission Control Protocol: TCP について
  - 脆弱性発見の背景
  - 脆弱性情報の流通過程
  - 脆弱性の内容について
  - 実際の脆弱性への対応
    - 脆弱性の対象となる製品
    - 脆弱性の回避策と対策
    - 公開情報
- 2004年5月13日に公開されたIEEE802.11の脆弱性
- まとめ：プロトコルの脆弱性について

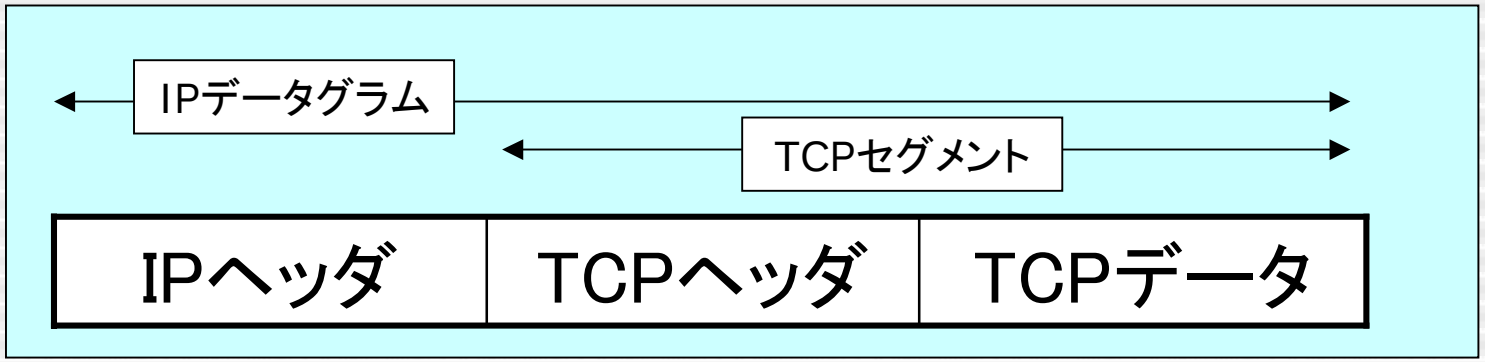
Transmission Control Protocol TCPについて-1

- オリジナル仕様はRFC793 にて定義
  - 1981年9月に出されたRFC
  - インターネットの前身である米国DoDのARPAネットワークで使われていたものがベース
  - コネクション型で、信頼性の高い通信を実現
  - Internet Protocol (IP) の上位層に位置するプロトコル
- TCPの主な構成要素
  - ポート番号(Port Number)
  - シーケンス番号(Sequence Number)
  - 確認応答番号(Acknowledgment Number)
  - ウィンドウサイズ(Window)
  - フラグ(URG,ACK,PSH,PST,SYN,FIN)

Transmission Control Protocol
TCPについて-2

・TCPセグメントはIPデータグラムにカプセル化される
・上位層のプロトコル(HTTP,FTP,SMTPなど)の下位に位置する
・実際の電気信号の伝達等は下位層に任せる

上位層
TCP
IP
下位層



Transmission Control Protocol
TCPについて-3

[TCPセグメント]

<table>
<tr><td colspan="8">Source Port (16bit)</td><td colspan="8">Destination Port(16bit)</td></tr>
<tr><td colspan="16">Sequence Number(シーケンス番号) 32bit</td></tr>
<tr><td colspan="16">Acknowledgment Number(確認応答番号) 32bit</td></tr>
<tr><td colspan="4">Data Offsetヘッダ長4bit</td><td colspan="4">Reserved
予約済み
6bit</td><td>URG</td><td>ACK</td><td>PSH</td><td>PST</td><td>SYN</td><td>FIN</td><td colspan="8">Window
ウィンドウサイズ
16bit</td></tr>
<tr><td colspan="8">Checksum
チェックサム 16bit</td><td colspan="8">Urgent Pointer
緊急ポインタ 16bit</td></tr>
<tr><td colspan="16">オプション部</td></tr>
<tr><td colspan="16">データ部</td></tr>
</table>

※オプションが指定されない限りヘッダは通常20バイト

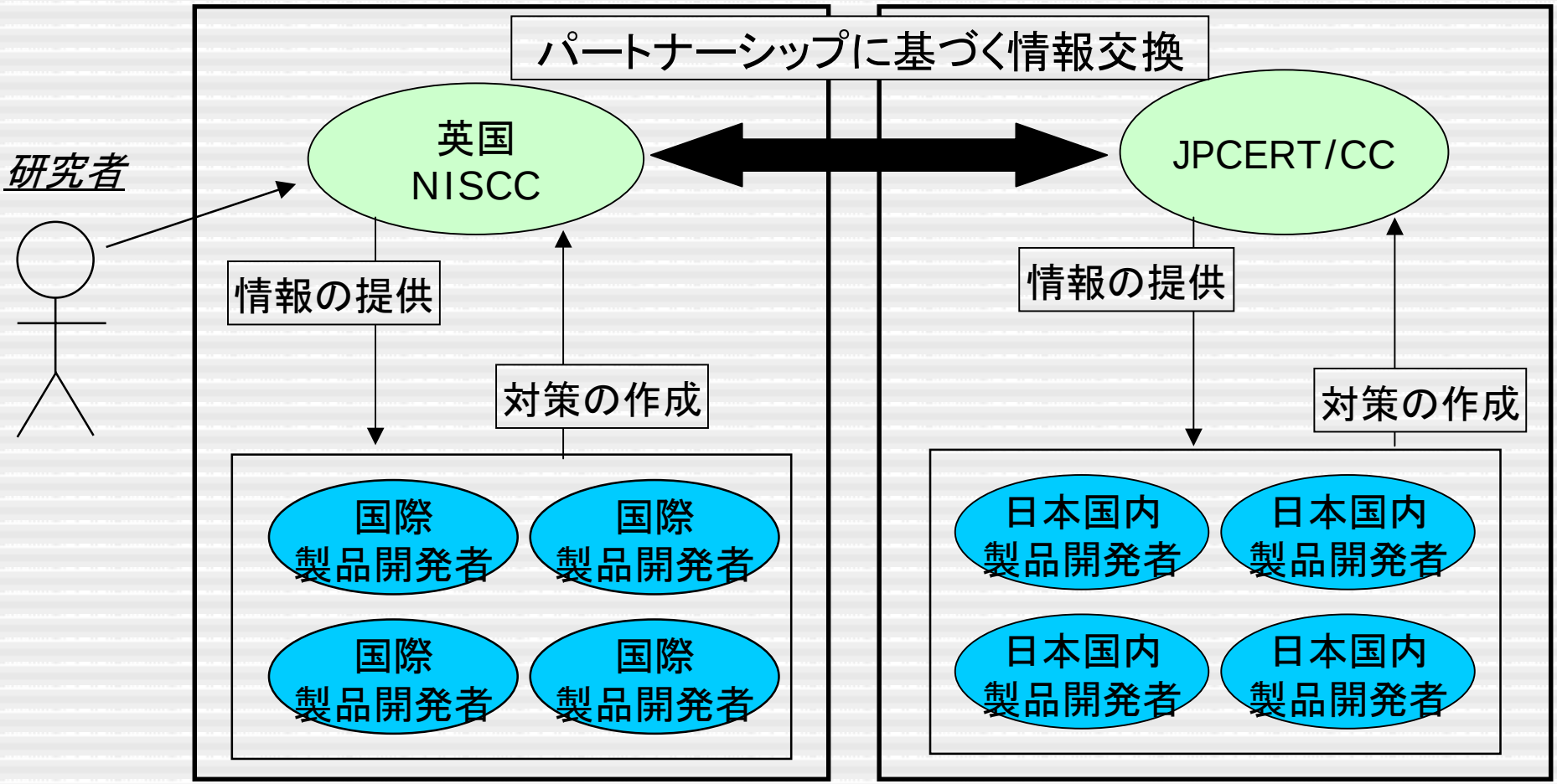
Transmission Control Protocol
TCPについて-4

パケットキャプチャ結果を用いた解説

脆弱性発見の背景
コーディネーションの背景

- セキュリティの研究者による指摘
  - 論文の発表が目的
  - 製品開発ベンダとのモチベーションの違い
- 昔から指摘されている既知の問題
  - ネットワークの高速化による攻撃の現実化
  - OSやアプリケーションの設計の問題
    - window サイズの増加
    - シーケンス番号や送信元ポートの規則性
  - 現実社会のインターネットへの依存度の高まり
- 既知の問題が再び脚光を浴びる
  - マスコミによる報道
  - 実際の攻撃の危険性

脆弱性情報の流通過程概要図



脆弱性情報の流通過程

- 2004年2月下旬
  - 英国NISCCよりJPCERT/CCに情報が入る
  - この時点での情報の公開日は7月に設定
  - JPCERT/CCから日本国内製品開発者へ連絡を開始
- 2004年3月下旬
  - 英国NISCCより公開日変更の連絡、英国時間で4/21に設定
  - 日本国内にて製品開発者を集めたミーティング
- 2004年4月：特にBGPを対象とした回避策（TCP MD5)の情報提供
  - JPCERT/CC Weekly Report での紹介
  - ネットワークの運用グループ(ASホルダ)を集めたミーティング
- 2004年4月21日
  - 情報の公表日が英国時間で4/21と設定されていたが、情報リークによりマスコミの報道があり、4/20に早まる(日本時間4/21)

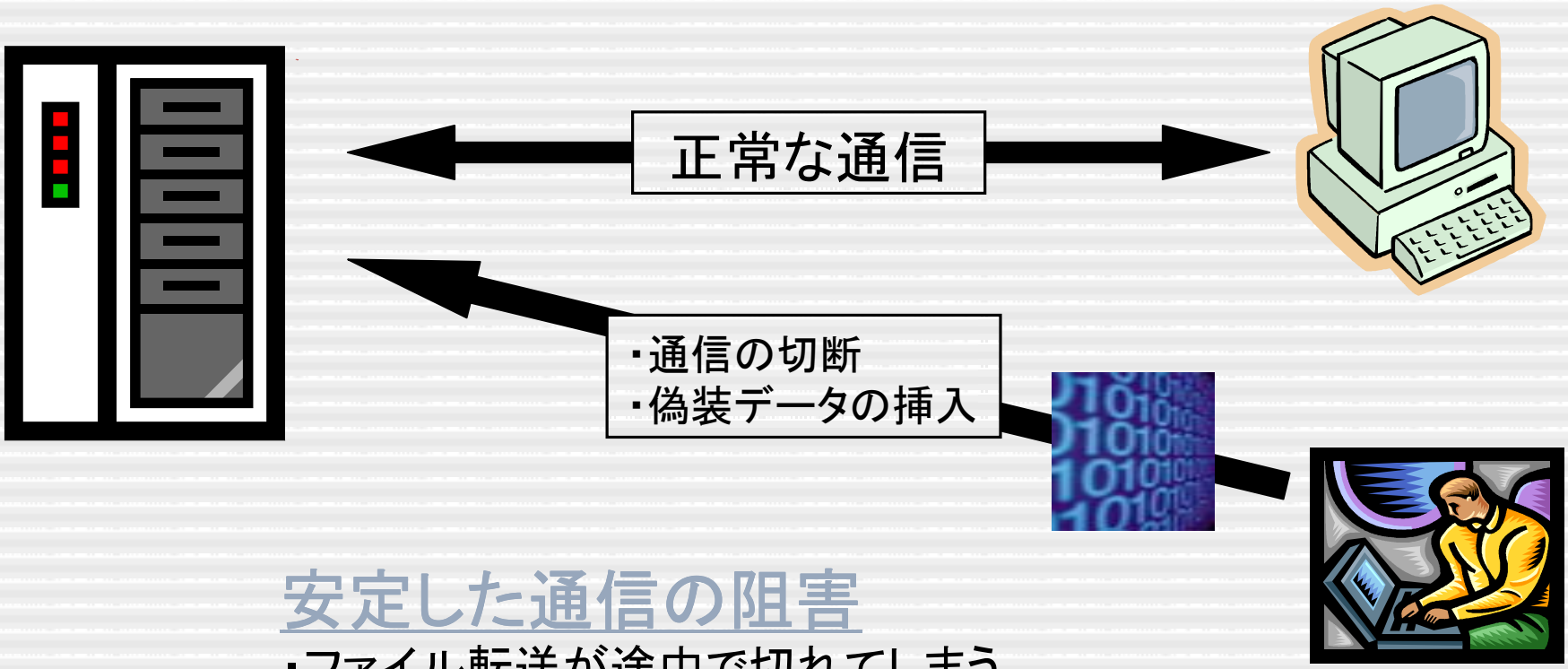
調整の期間は、およそ2ヶ月

JPCERT CC

脆弱性の内容
概要

- 研究者が指摘した問題は以下の3点
  1. RST セグメントによってセッションを切断できる
  2. SYN セグメントによってセッションを切断できる
  3. ねつ造されたデータセグメントで、データの差し込みを行うことができる
- 特定のセッションをターゲットとした攻撃
  - 攻撃の成立には以下の情報が必要
    - IPアドレスの対(送信元、送信先)
    - ポート番号(送信元、送信先)
    - windowの範囲内に収まるシーケンス番号

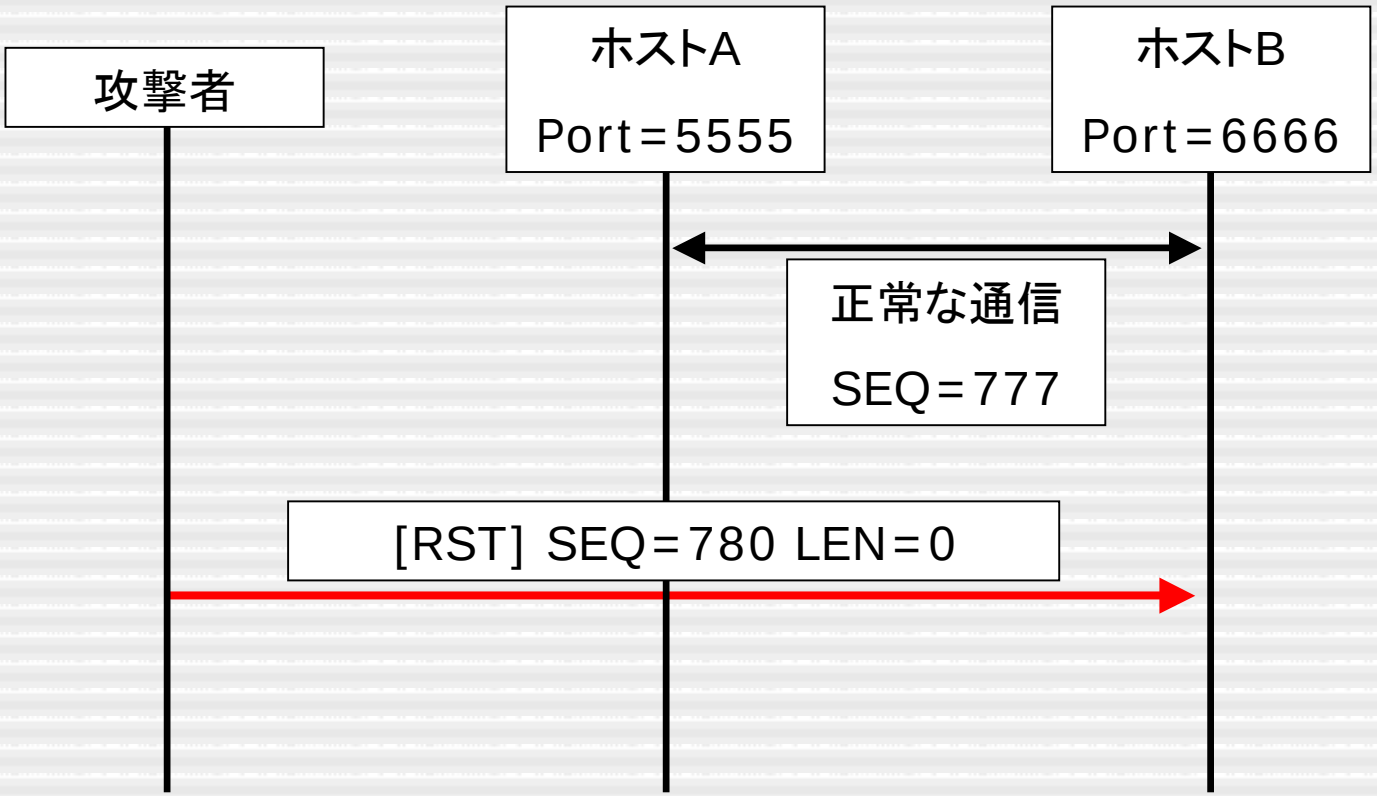
脆弱性の内容
概要図



安定した通信の阻害

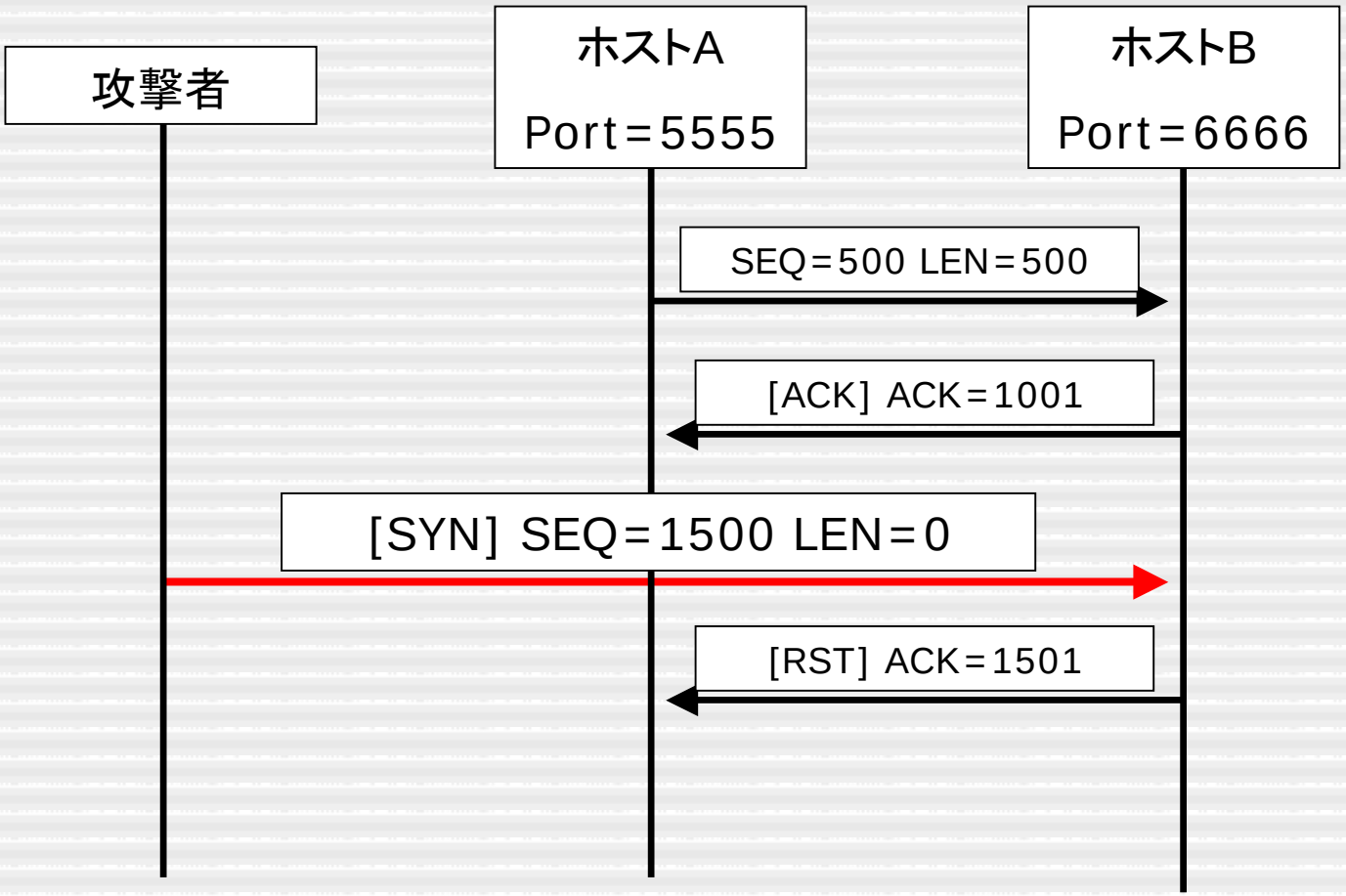
・ファイル転送が途中で切れてしまう
・ログイン中のセッションが途切れてしまう
・オンラインショッピングが完了できない

1：RST セグメントによる攻撃



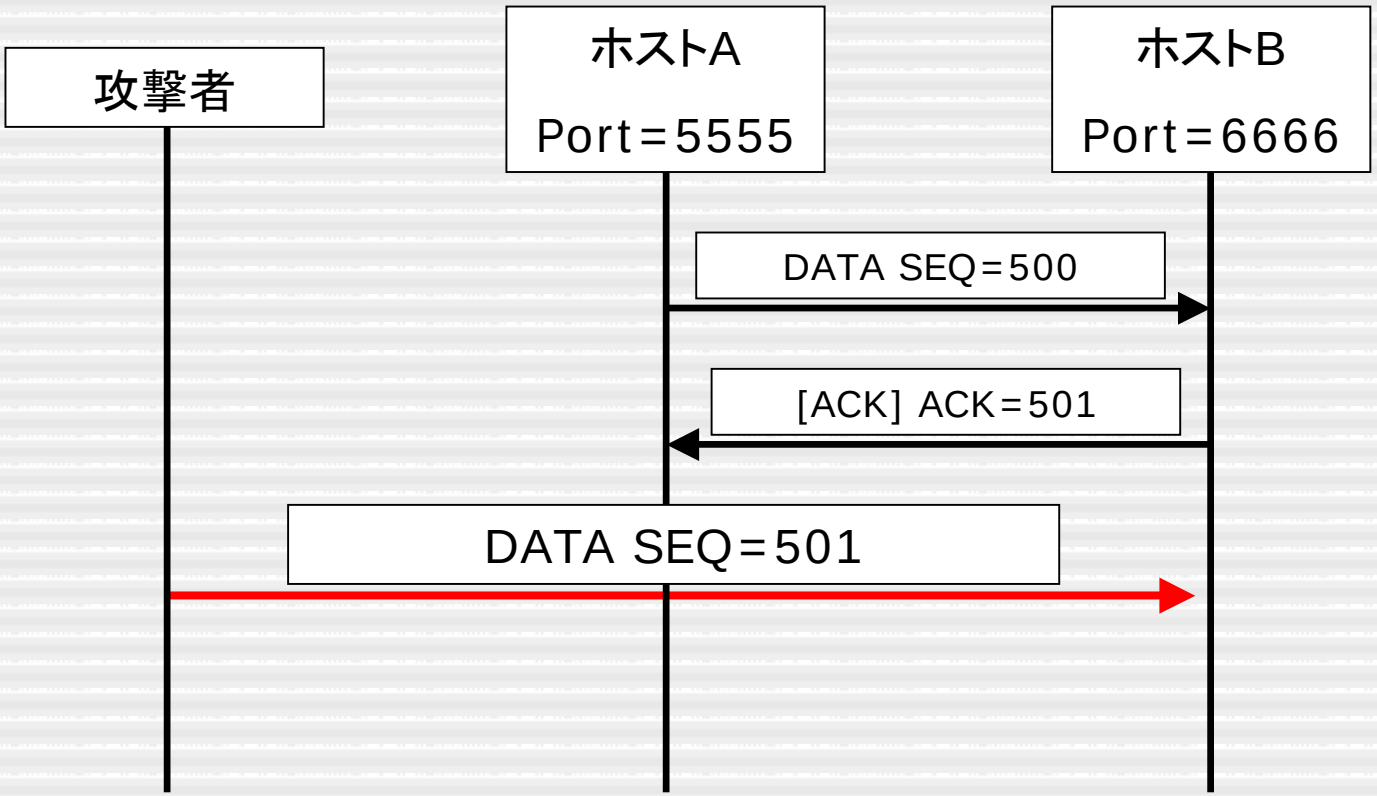
上手い具合に **RST** を飛ばすと受信側ホストが受理してしまう

2：SYN セグメントによる攻撃



上手い具合にSYNを飛ばすと、セッションが切れてしまう

3:データの差し込み



上手い具合にデータセグメントを飛ばすと、データの差し込みが行えてしまう

脆弱性の内容
実際の攻撃方法

- 攻撃の成立には以下の情報が必要
  - IPアドレス対
  - ポート番号対
  - セッションで使用中のシーケンス番号
- シーケンス番号は総当たり
  - windowが大きいのでそれほど困難ではない
  - ネットワークが高速
  - マシンの性能も高い

脆弱性の内容
実際の攻撃方法

パケットキャプチャ結果を用いた解説

脆弱性の内容
対象になりやすいサービス

- 経路情報を流しているBGP
  - 経路情報を送受信するルータのIPアドレス対
  - 受け側ルータは179/tcp 送り側は??番
  - シーケンス番号は??番
- リモートログイン(telnet や ssh など)
  - ログイン先のIPとログイン元のIP
  - ログイン先のポート番号は22/tcp、ログイン元は??番
  - シーケンス番号は??番

→ DNS(TCP)やIRC,果てはオンラインゲームなど
長時間に渡るセッションを張るようなサービスが対象となる

脆弱性の検証結果

- 実際に切断することの出来たOS
  (IPアドレス対、ポート番号がわかっているSSHのログインセッションを対象としてシーケンス番号総当たり)
  - NetBSD1.5
  - Darwin 7.5.0 (MacOS X 10.3)
  - Linux-2.2.20
    - Windowサイズが大きいことを利用してシーケンス番号総当たり的にRSTセグメントを投げ続けて90秒以内で切断
    - 攻撃の対象とするサービスが決まれば、src_port も総当たりで攻撃可能。OSによって範囲がある程度推測可能。
- OpenBSD 2.5, 3.5 は切断できず。

脆弱性の対象となる製品

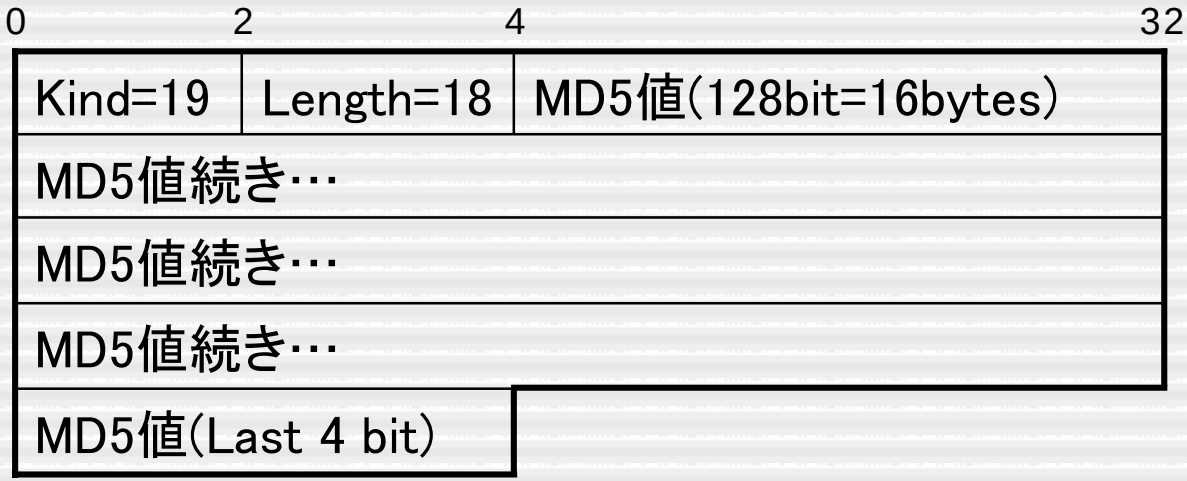
- 対象となるのはプロトコルの実装部分
  - TCPのプロトコルスタックそのもの
  - 多くの場合OSレベルの実装に影響
  - 具体的にはルータやOSそのものなど
- 複数のベンダに影響の及ぶ脆弱性
  - OSだけでなくハードウェアベンダも

プロトコルスタックとして社外製品を利用している場合は、
実際に製品を販売している社で対応しきれない場合がある

脆弱性の回避策

- TCP MD5 Signature Option
  - RFC2385にて定義
  - BGPセッションを保護するために考えられた
  - TCPヘッダのオプションフィールドへの拡張
  - 相手から送られてきたパケットの認証機構
- GTSM(Generalized TTL Security Mechanism)
  - RFC3682にて定義
  - IPパケットのTTL値を用いた一種の認証方法
- IPSec
  - RFC2401など多数のRFCで定義
  - 通信の暗号化、相手の認証も可能

TCP MD5 の構造

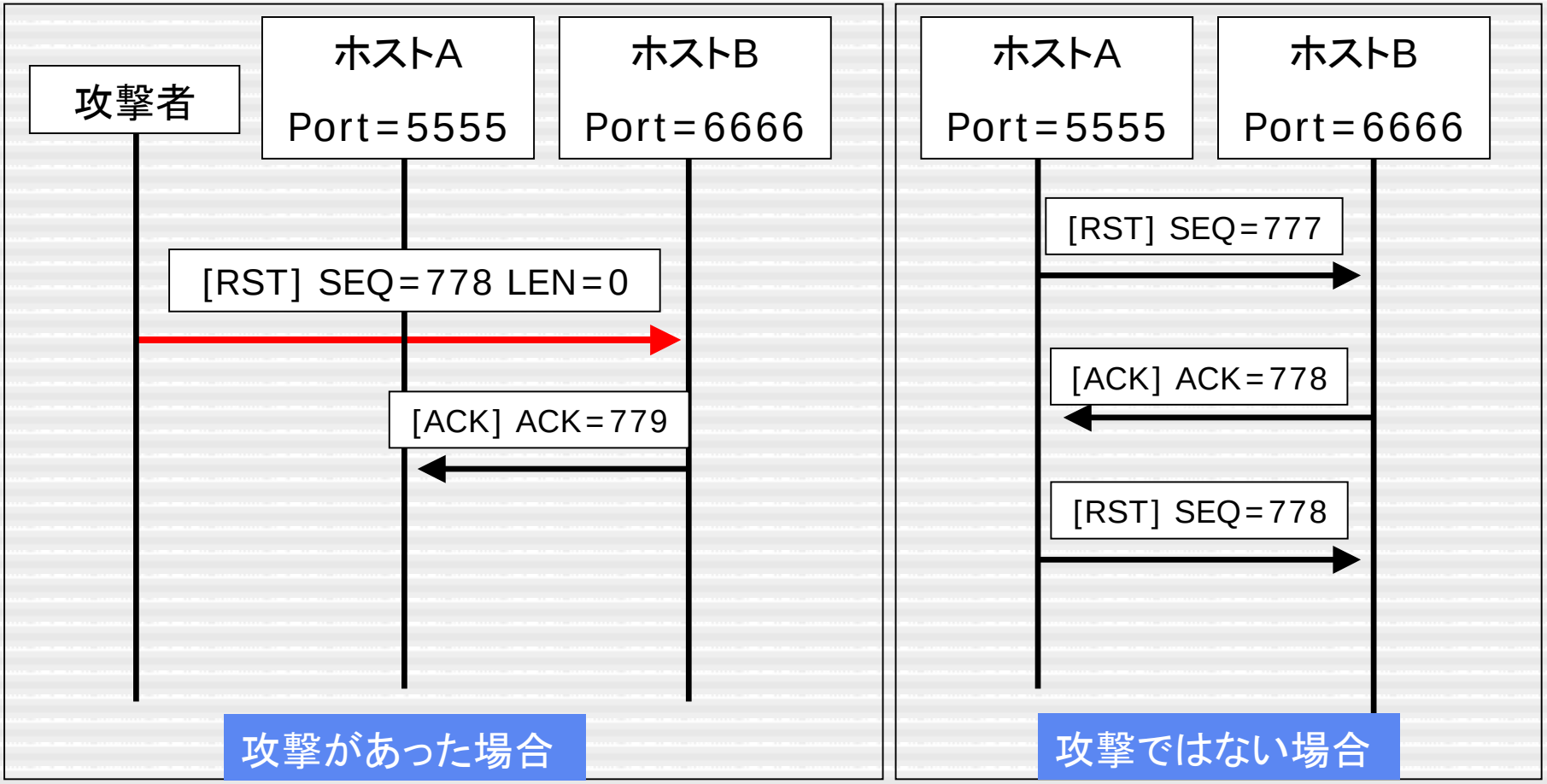


- MD5 digest を TCP オプションとして格納
- TCPオプションフィールドの kind(タイプ)は19、length(データ長) は18(=1+1+16)bytes
- 後ろに MD5 digest (16バイト)を付ける

脆弱性への対策
1：RST Attack

1. 期待しているシーケンス番号の範囲外(windowの外)にあるRST bitがセットされたセグメントが来た場合には、そのまま捨てる
2. RST bit がセットされており、期待しているシーケンス番号そのもの(window 範囲内であっても不可)である場合にはコネクションをリセットする
3. RST bit がセットされており、期待しているシーケンス番号ではないがwindow範囲内である場合には、ACKを返す

RST Attack
対策1について



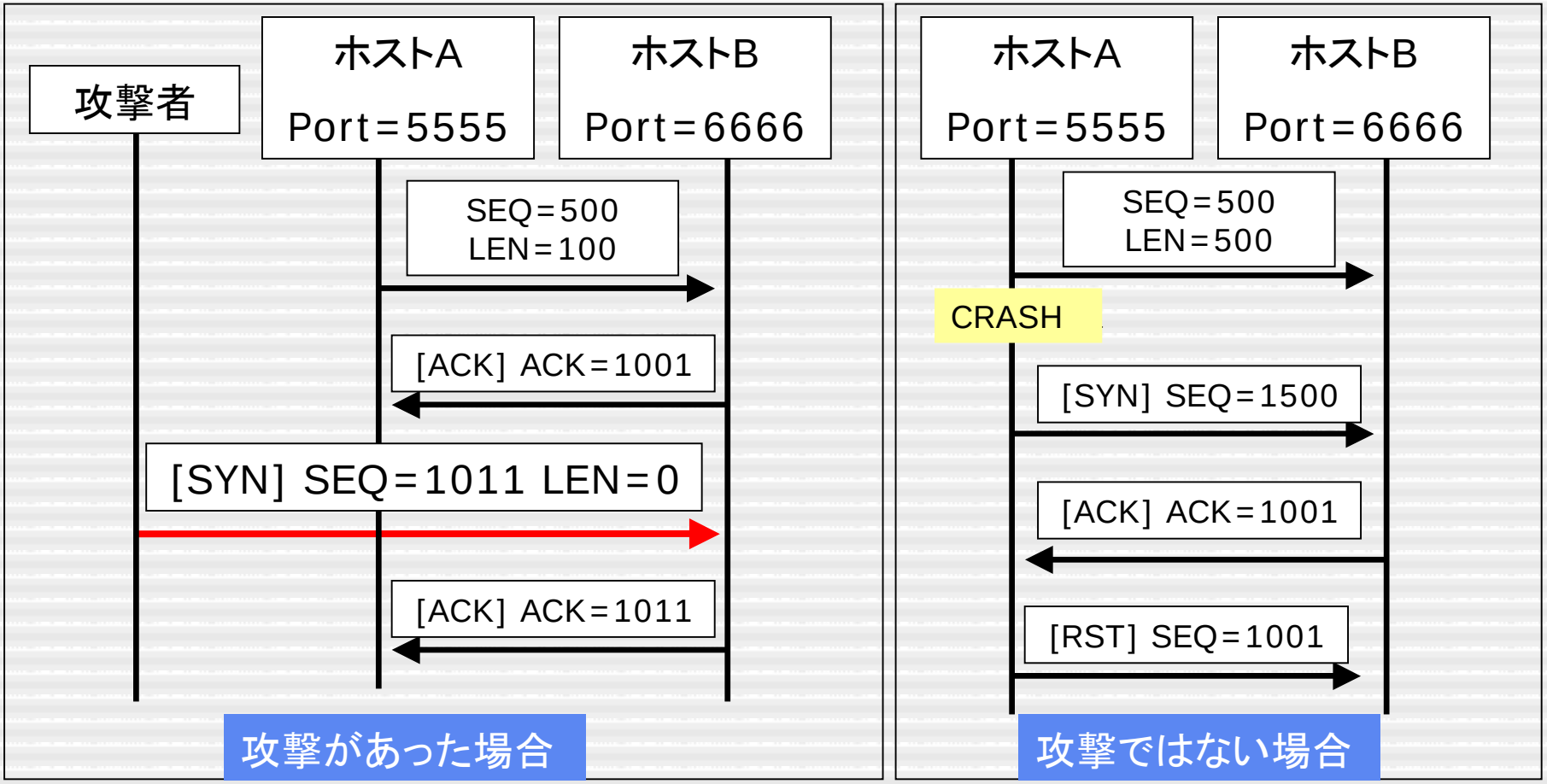
脆弱性への対策
2：SYN Attack

1. SYN bit がセットされたセグメントを受け取った場合には、シーケンス番号にかかわらずACKを返すようにする

※ 1/(2^32) の確率で問題が発生する

詳細は付録[6]の3.2 をご覧ください

SYN Attack
対策2について



脆弱性への対策
3：データの差し込みを防ぐ

1. 入力されたデータセグメントに関しては、通常よりも厳重なチェックを行うようにする。
   - 適切なACK値になっていることをチェックすることで、シーケンス番号の推測だけでは攻撃が成立できなくなるという効果がある

※詳細は付録[6]の4.2をご覧ください

公開情報
NISCCによるアドバイザリ

Vendor Information

The following vendors have provided information about how their products are affected by these vulnerabilities.

Please note that JPCERT/CC have released a Japanese language advisory for this vulnerability which contains additional information regarding Japanese vendors. This advisory is available at http://www.jpcert.or.jp/at/2004/at040003.txt.

Alcatel	Innovaphone	NEC
Certicom	Internet Initiative Japan, Inc	NetBSD
Check Point	InterNiche	Nortel
Cisco	Juniper Networks	Polycom
Cray Inc	Lucent Technologies	QNX Software Systems
Fujitsu	Mediatrix	Secure Computing Corporation
Hewlett-Packard	Mitel Networks	Siemens Subscriber Networks
Hitachi	MRLG	Yamaha

http://www.uniras.gov.uk/vuls/2004/236929/index.htm

NISCCの情報公開ページから抜粋

- 英国NISCCより公開され世界的に注目された
- 日本の製品開発者の情報も紹介
- 各国各種メディアからの反応

公開情報
IETFによるインターネットドラフト

- この問題を受けてIETFのtcpmのグループからドラフトが公開されている(付録[6])
- TCPの実装への対策方法にCiscoの特許が存在する可能性がある
- IETF60での議論の末、現在考えられている以外の対策も視野に入れ現在活動中…
- ゆくゆくはRFC化?

2004年5月13日公開 IEEE802.11 DSSS無線機器の脆弱性

- 研究者の論文として発表
- 低速モードで動作する無線LAN機器が対象
  - 802.11 と 802.11b 及び、20Mbps 以下の低速で通信を行う 802.11g が該当
- DSSSという変調方式自体の脆弱性
  - DoSが成立する
  - 無線LANを止めることができてしまう
- 製品開発者のレベルでは対処不可能
- 回避策は??
  - 重要なネットワークへの無線LAN利用の回避

まとめ
プロトコルの脆弱性について

- プロトコルの脆弱性=標準仕様の脆弱性
  - 標準仕様の変更が必要になる上に、完璧な対応は難しい
  - 製品を開発しているベンダでは直接対応しにくい
  - 回避策があっても妥当かどうかわからない
    - 十分な検証も難しい
- 複数のベンダにまたがる問題である
  - 製品開発ベンダとの調整に時間がかかる
  - 問題が深いため各社内でも対応に時間がかかる
  - 社内にて脆弱性を取り扱う体制の構築を
- 今後、プロトコルの脆弱性は増える?
  - 発見者(研究者?)のモチベーション
  - 製品開発ベンダのモチベーション

付録:外部情報へのリンク集

[1] NISCC - Vulnerability Issues in TCP
http://www.uniras.gov.uk/vuls/2004/236929/index.htm
[2] JPCERT/CC - TCP プロトコルに潜在する信頼性の問題
http://www.jpcert.or.jp/at/2004/at040003.txt
[3] US-CERT - Vulnerabilities in TCP
http://www.us-cert.gov/cas/techalerts/TA04-111A.html
[4] OSVDB - TCP Reset Spoofing
http://www.osvdb.org/4030
[5] CVE - CAN-2004-0230
http://cve.mitre.org/cgi-bin/cvename.cgi?name=2004-0230
[6] Transmission Control Protocol security considerations
http://www.ietf.org/internet-drafts/draft-ietf-tcpm-tcpsecure-01.txt
※リビジョンが上がると 01 が 02,03,04... となっていきます
[7] IEEE 802.11 DSSS 無線機器における DoS の脆弱性
http://www.jpcert.or.jp/at/2004/at040007.txt
[8] AA-2004.02 -- Denial of Service Vulnerability in IEEE 802.11 Wireless Devices
http://www.auscert.org.au/4091
[9]インターネットセキュリティに関する RFC の日本語訳
http://www.ipa.go.jp/security/rfc/RFC.html

以上です

ありがとうございました

JPCERT コーディネーションセンター

[Web] http://www.jpcert.or.jp/

[Mail] office@jpcert.or.jp