脆弱性情報取扱いの具体的事例紹介

2004年7月：脆弱性関連情報取り扱い説明会

JPCERT/CC　鎌田敬介

KAMATA Keisuke

JPCERT CC

ご紹介する内容

- 製品開発者の脆弱性情報への対応の流れ(理想)
- 2004年4月21日(日本時間)に公開されたTCPの脆弱性
  - どのような組織が関係したのか?
  - どのくらいの期間がかかったのか?
  - どのような内容だったのか、また問題点は?
  - どのような製品開発者が対象となったのか?
  - 製品開発者に期待された対応とは?
  - 結果として公表された情報
- その他の事例から

製品開発者の脆弱性情報対応の流れ

1. 脆弱性情報の連絡を受ける
2. 自社製品で脆弱性に該当するものがあるかどうか、また該当する製品の実装を調べる
3. 製品の実装状況次第では対応の有無を検討する
4. 可能であれば、製品の修正プログラム(パッチなど)の作成や回避策(ワークアラウンドの作成を行う
5. それらの情報の、製品利用者への周知を行う

製品の脆弱性該当箇所が外注先や取引先など社外開発の場合、JPCERT/CCに伝えることで、JPCERT/CCからそれらの組織に伝達し情報の共有と対応の依頼をすることも可能です。

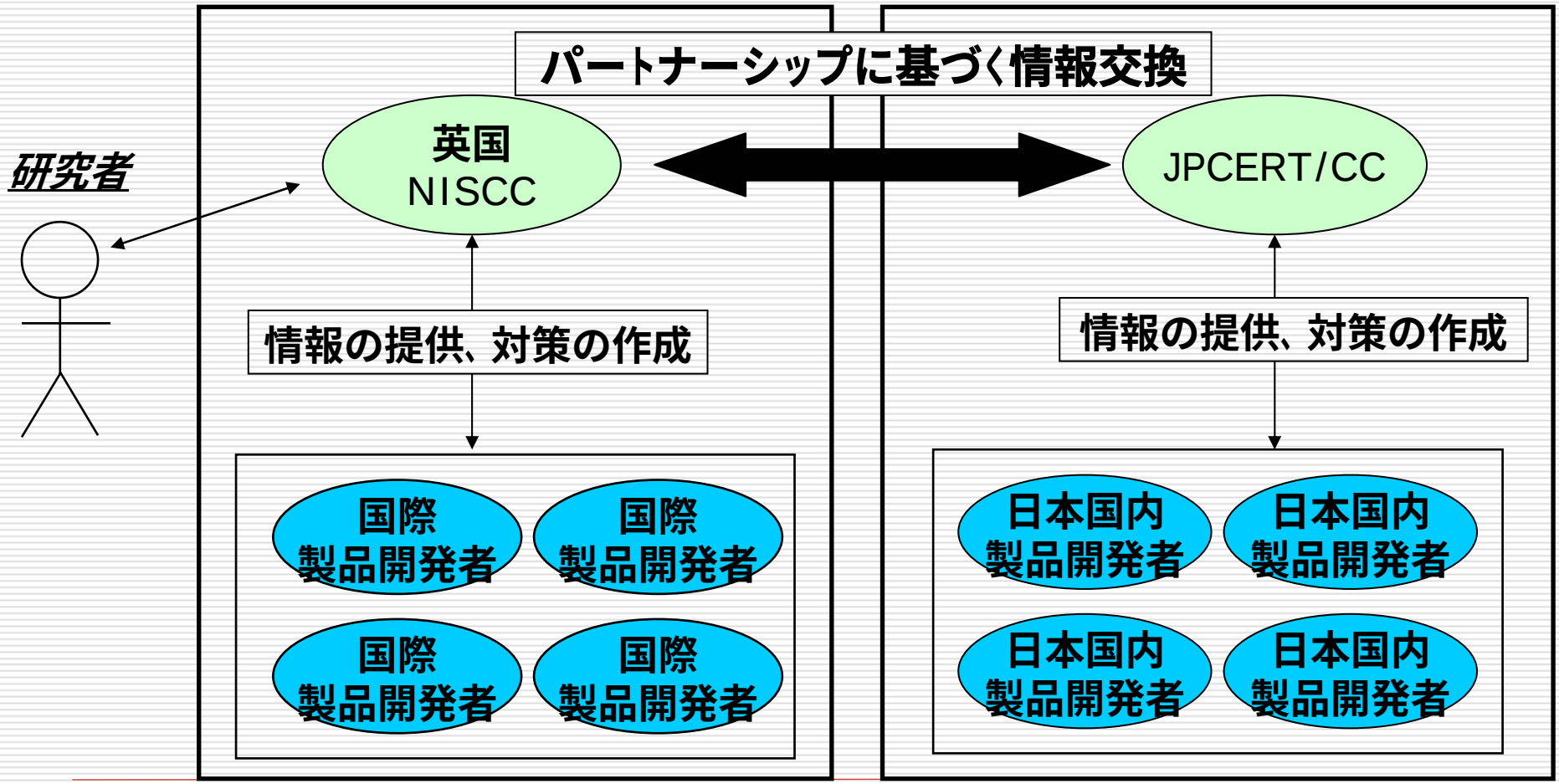
JPCERT CC

具体事例：TCPの脆弱性の背景

- インターネットで広く用いられているプロトコルである、TCPの安全上の問題点が指摘された
  - セキュリティ研究者による論文
  - 問題点だけではなく対応策も提示
  - 特定の製品開発者の問題ではない
- この問題自体は昔から指摘されている問題
  - なぜ今再び？

JPCERT CC

関係した組織等



JPCERT CC

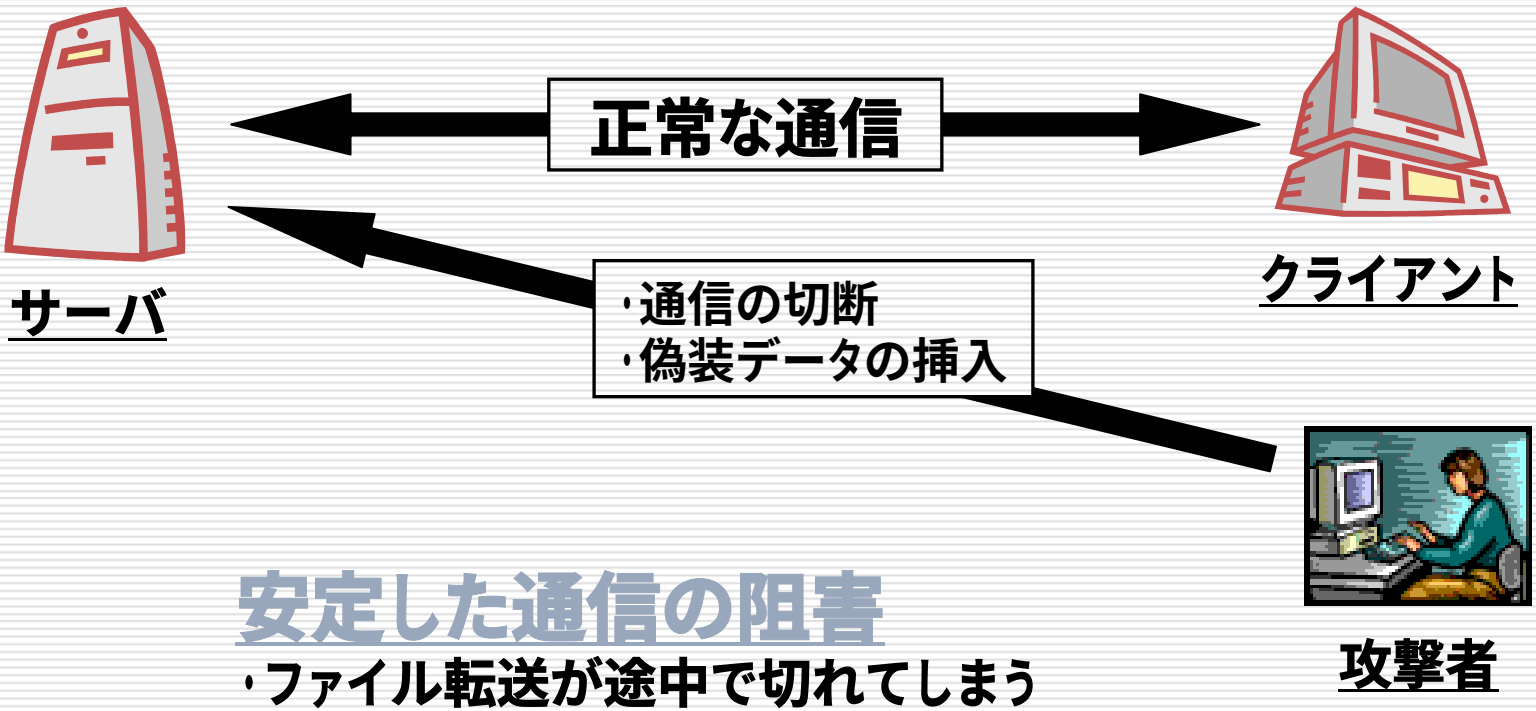
全体の時間の流れ

- 2004年3月上旬
  - 英国NISCCよりJPCERT/CCに情報が入る
  - この時点での公開日は7月に設定
  - JPCERT/CCから日本国内製品開発者へ連絡を開始
    - JPCERT/CCよりコンタクト可能であった製品開発者
- 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
  - 脆弱性情報を伝えた製品開発者を集めたミーティング
- 2004年4月回避策 (TCP MD5)の情報提供
  - ネットワークの運用グループ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

脆弱性の問題点



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
・ホームページを見ることが出来ない
・メールが届かない

JPCERT CC

この問題の対象となった製品開発者

- 対象となるのはTCPのプロトコル実装
  - TCPプロトコルスタックを自社開発している製品開発者
  - TCPプロトコルスタックを安全な実装に修正することが可能な製品開発者
- 製品としては
  - ルータやOSそのものなど
  - 場合によってはゲーム機やインターネット家電も

プロトコルスタックは社外製品を利用している場合が多い

自社内では対応しきれない場合もある

JPCERT CC

実際の対応

- 実際には対応の難しい脆弱性でした
  - TCPの問題としては既知のもの
  - 対応策として提示されている内容の問題
- 可能な限りの対応

最終的に公開された情報

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

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
- 各種メディアからの反応

JPCERT CC

その他の事例から

- その他の取り扱い事例
  - S/MIME
  - H.323
  - SSL/OpenSSL
  - X.400
- 脆弱性検証ツールの提供
- 検証実験の結果情報の提供

付録：外部情報へのリンク集

NISCC - **Vulnerability Issues in TCP**
http://www.uniras.gov.uk/vuls/2004/236929/index.htm

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

US-CERT - Vulnerabilities in TCP
http://www.us-cert.gov/cas/techalerts/TA04-111A.html

OSVDB – **TCP Reset Spoofing**
http://www.osvdb.org/4030

CVE - **CAN-2004-0230**
http://cve.mitre.org/cgi-bin/cvename.cgi?name=2004-0230

Transmission Control Protocol security considerations
http://www.ietf.org/internet-drafts/draft-ietf-tcpm-tcpsecure-01.txt