相互接続性とセキュリティー
インターネットを超えて広がる脆弱性

齊藤忠夫（東京大学名誉教授）

2016年12月9日

HATSセミナー

通信技術の進歩と相互接続性。

- HATSは1980年代の終わりから約30年の間の通信のデジタル化の時代に、ネットワークとそれにつながる機器の相互接続性を保証する接続試験を通して、ネットワークの発展に寄与してきた。
- この30年間に通信技術の発展と普及は顕著であり、端末機は世界の人口に匹敵する数に増え性能も向上してきた。
- 端末を人ではなく機械とするネットワークはIoTと呼ばれ、ネットワーク市場をさらに大きく成長させることが期待されている。
- IoTではさらに多様な端末が接続されることが期待され、相互接続性は重要な前提となる。
- すべての物がつながるIoTの時代に、従来インターネットを中心に考えられていたセキュリティーの範囲は大幅に広がる。
- この講演では接続に拡大を容易にするHATSに、新たに求められる問題を考えたい。

HATS 2016-12-09 T Saito

セキュリティー問題が生ずる環境

- セキュリティー問題は、インターネットの発展に対応して多様な事例が出現し、大きな問題になっている。
- インターネットの時代にはネットワークによる通信を支える標準プロトコル機能とその実装は、その標準がIETFで決まるときには同時に公開され、オープンに広がる。
- インターネットに接続されるPC等のOSも、少数のベンダーの製品で実現され、バリエーションは小さい。
- アプリケーションの多くでも、オープンシステムとして同一のものが多数広がっている。
- 標準をITUが作り、各メーカがそれぞれ標準を実装した時代にはなかった、フラットな環境が実現された現代では、脆弱性を攻撃者は容易に知ることができ、セキュリティー問題の背景となる。

セキュリティー保護環境

- インターネットのオープン環境では、HATSが努力する相互接続性は自動的に実現されることも多く、相互接続の容易化とセキュリティー問題は相反することが分かる。
- フラットな環境を活用した脆弱性の高い環境では、マルウェアを共通に発見して、協力して対処することが有効である。
- ネットワークを通して流れるセキュリティーを害する情報を共有する組織としては、各国にISAC（Information Sharing and Analysis Center)、CSIRT(Computer Security Incident Response Team) などがあり、それぞれ関係者が協力して対応している。
- このような努力と並行して、システムのバリエーションを保ちながら、相互接続とセキュリティーの両立を保つことも求められる。
- この講演ではインターネット以外の環境での、セキュリティー問題について考えたい。

HATS 2016-12-09 T Saito

接続の条件としてのセキュリティー

- HATSが伝統としている標準が許すバリエーションのなかでの、接続性の確認は今後とも重要である。
- しかしIoTでも実際に接続するときには、その接続でセキュリティー問題が発生したり、性能低下が生じたりしないことを、利用者が確認を求めるのは自然な要求であろう。
- 機械工場の自動化で、IoTによる他の自動機器と一体化で生産性を向上する場合でも、IoTなしでも生産できた経営者はセキュリティー問題を恐れて接続を嫌う例がある。これがIoT推進の阻害要因になっている場合が少なくない。
- 病院の患者のバイオデータを看護師室に伝送するIoTでも、セキュリティー懸念を抱く病院関係者が少なくない。
- HATSの接続性の成果を広げてゆくためには、HATS関係者もセキュリティー問題に寄与することがもとめられよう。

HATS 2016-12-09 T Saito

ネットワークの活用と社会道徳

- 通信技術が低コスト化、高性能化し、普及が進むように多様な努力が行われ、成果が上がったのは最近の4分の1世紀である。進歩するネットワークの相互接続を確保するために標準と実装のずれをなくすことは重要であり、HATSは大きな役割を果たした。
- 通信の普及が進み、社会に浸透してくると、通信が適切に使われないために生ずる通信の悪用が次第に顕著になってきた。
- 通信は人が形成する社会で使われ、サービスが想定しない使われ方をすると、不幸な事件を発生させることもある。
- 直接話をする場合には起きないような対話が、通信を通してならできるような社会マナーの不足も顕著になっている。
- 少年の間のいじめ、自殺などで通信サービスが関連することが報道されることも珍しくなくなっている。

Stuxnet

- 多くのマルウェアが情報の破壊、盗み出しの機能に留まるのに対して、攻撃相手の機能、構造を知っていて、破壊活動を行う。マルウェアとして、2009年に出現した。
- StuxnetではマルウェアはUSBメモリーを通して運ばれるものであった。IoTが起こす可能性があるセキュリティー被害の実例として、改めて注目されている。
- 2009年にはイランのウラニウム濃縮工場に侵入し、破壊した。
- Stuxnet は、USBメモリーに過去の攻撃の履歴を示すVisiting Recordを残し、これを保守者のPCを介して発信する。その解析結果から攻撃の状況を知ることができる。
- 500kB以上の大規模なプログラムで、1000人日以上の工数をかけて作られたものといわれている。
- Symantec社の分析が知られている。

T.Saito 2016-9-21

IoTでのセキュリティーの困難

- IoTは、人が日常使用する環境にはなく、異常が起きたことを気が付きにくい。
- 常時ネットワークに接続され稼働している。電源を落とすことはないので、いつでも攻撃できる。
- マルウェアが動作できる処理能力を持つ。
- マルウェア対策ソフトが存在しない。たとえ作られたとしてもこれを起動してマルウェア対策を誰がするのかが明確になりにくい。
- 管理用パスワードが初期値として設定されている。
- グローバルIPアドレスでアクセスできるものが多い。
- Stuxnetのようなセキュリティー問題は、管理者が気付かない環境でのセキュリティー問題として、多様な環境に広がる恐れがある。

T.Saito 2016-9-21

SS7信号網の危険性

- 電話網の制御のために交換機間の通信を行う信号網は、クロスバー交換機の時代から通信網制御の基幹ネットワークである。
- 1970年代に標準化されたNo7信号方式（SS7)は、ISDNの開発の時代に標準化され、その後現在も活用されている。
- SS7信号網は初期にはインターネットプロトコルを使用していなかったが、2000年にSS7コマンドがIP上で処理できるようになり、SS7ネットワークは危険にさらされるようになった。
- SS7には通常のインターネットのような認証、正当性検証の機能が不十分な部分がある。その意味でSS7網は危険なネットワークである。
- セキュリティー問題が発生しても管理者が気が付きにくいという、IoTの問題と似た事象が、SS7網には存在する。

HATS 2016-12-09 T Saito

SS7網の悪用

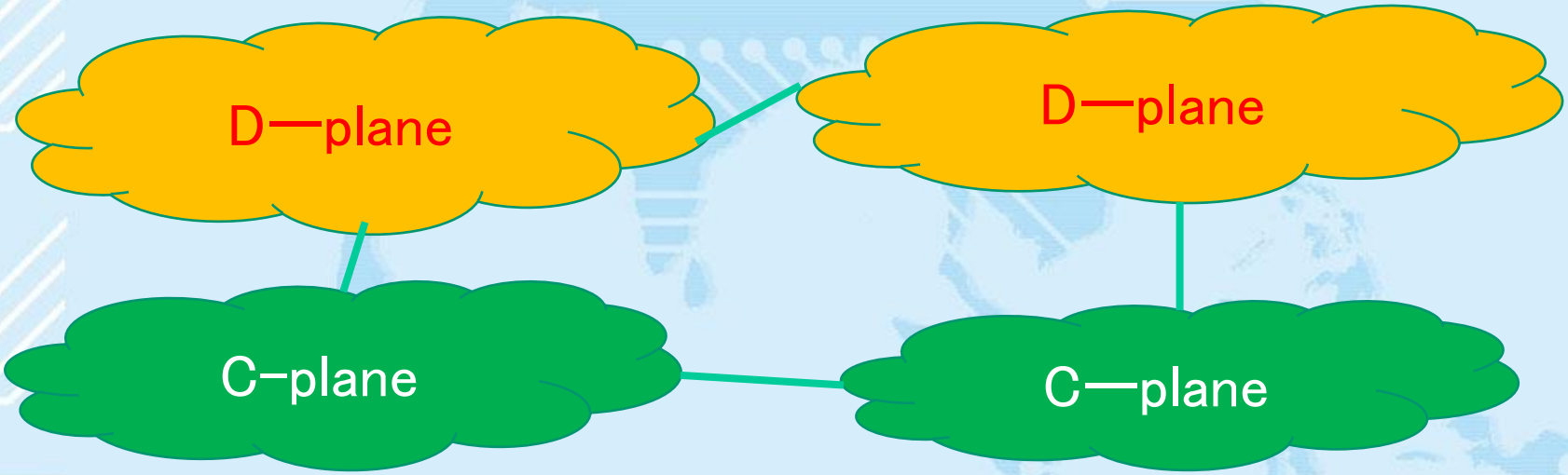
- SS7信号網脆弱性については各国で調査が行われている。事業者ライセンスは国によっては簡単に発行され、事業者としてならネットワークに接続するバリアは低くなる。
- モバイルネットワークでは、これによってSIMカード情報、電話番号、位置情報が取得できてしまう。
- 発信者からの信号を着信者に伝えるのに、他の地点を経由する操作が可能であり、信号の傍受も可能になる。
- 2013年にはヨーロッパの首脳の携帯電話の盗聴が国際的に話題になったが、これもSS7ネットワークの悪用によって可能になる。
- 加入者位置情報が書き換えられると、加入者は別の場所に移動したことになり、その場所の基地局から呼び出されるが、電波は到達せず、電話が使えなくなる妨害となる。

ITU本部でのワークショップ

- SS7ネットワークの脆弱性は、日本では大きな話題にはなっていないが、ITUでは重大性が認識されており、2016年6月29日にはジュネーブのITU本部でこの問題に関わるワークショップが開催された。
- このワークショップでは、主として携帯電話網における悪用の問題が興味を持って議論された。
- 通信自由化によって各国で参入の規制緩和が行われたこと、国際化によって網間接続が促進されたことが、問題の基本にある。
- VoIPなどの新しいアプリケーションがまた新しい問題につながることもあると思われる。
- 日本ではIP電話ルータの脆弱性によって、利用者が認識しない海外通話が発生することが問題とされているが、それがSS7悪用の結果である可能性も否定できない。

ネットワーク制御プレーン分離の注意

- インターネットでは、制御信号も情報も一つのネットワークを流れる。セキュリティーの危険性を避け、情報ネットワークの性能を改善するために制御を情報と分離することが提案されている。この場合にも、国際接続でサービス事業者がどのように認可されているかについて、十分精査しなければならない。



制御プレーン分離型インターネットの注意

- インターネットの性能を向上する技術として多様なアイデアがある。その中で実用化が始まりつつあるのはSDN（Software Defined Network）である。
- SDNではネットワークのルーティングでは、ネットワーク全体を見るコントローラで制御するOpen Flowが採用され、製品化されている。
- この場合にも多数の事業者が出現して、相互接続が行われるようになったとき、SS7と同様な危険を防止する方策が求められる。
- ネットワークセキュリティーの問題は、その方式が成功して世界的に広がった時に発生する。技術が世界的に広がる前に、単一ネットワークの時代から、成功後の時代を見据えた準備が求められることになる。

適切な接続性を求めて

- HATSは30年弱の間ネットワークの接続性を求めてネットワークの技術の進展に努力してきた。
- ソフトウェアを中心に発展する情報環境では、標準化と同時に作られるオープンソフトウェアで、接続性の保証は自動的に実現されることも多くなったが、超高速伝送技術のような、物理的性能が鍵になる標準では、HATSの相互接続性の検証は今後とも重要である。
- 同時に、ネットワークが社会的に健全性を保ち、生産性を向上するためには、相互接続性と共に、安全性の実現が求められる。
- 大量情報を世界的なスケールで、費用を気にすることなく通信できるようになった今日、新たな課題が発生していると言えよう。