ユナイテッド航空日本語版機内誌
LEADER'S REVIEW「リーダーズレビュー」
vol.75 | January February 2014

未来を読む

クラウド時代の本格到来で変わるITと情報管理

サイバー攻撃の防御は国家的な課題

インターネットが我々の生活に欠かせなくなった今、
個人のデータはもちろんのこと、国家や企業の
通信データをいかに守るかが、急務とされている。
それはクラウド時代に入って顕著化し、
これまで以上にますます重要性を帯びてきた。
玉川大学では、そうしたクラウド技術と光通信の
問題点を見越し、早くから通信回線網を流れる
データの暗号化技術の開発に取り組んできた。

文◎広田 修 text by Osamu Hirota
写真/協力◎玉川大学

see VISIONS

クラウド時代の幕開け

インターネットの形態の変化

法人が所有する無数のLANを世界規模で接続する機構がインターネットである。そこでは個々のPCは独自のソフトウエアで動作し、その処理されたデータは通信回線によってサーバーと呼ばれる大型のPCに一時保存、又はそこで再度の処理が行われ、所望のPCに送られる。このようなシステムがあまりにも巨大なシステムに成長し、秩序の維持が困難になることが予想されたため、1995年頃から、次世代インターネット（現在のクラウド）の構想が創案された。クラウド型のインターネットは巨大なデータセンター（サーバーの集合体）をネットワークの要に配して膨大な種類のソフトウエアの提供や国家規模の情報蓄積・管理などを一括して行い、個人や法人のインターネット活用業務をサポートするシステムである。

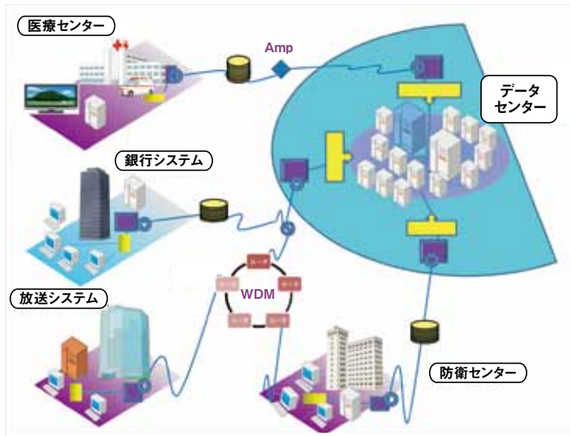
クラウドによる自動車産業とIT企業の融合

クラウドの普及に伴う効果として、自動車産業とIT企業が融合する新産業形態の創成が急速に現実味を帯びてきた。レクサスなどの高級車はすでにPC3台分に匹敵する情報処理機能を持っており、そのほとんどの機能がテレマティクスという通信機能によって管理会社のデータセンターに接続され、自動車の保全から運転に必要な種々の情報の運用・管理が実施されている。運転者の音声によるコマンド機能は、自車のPCではなくネットワークを経由してデータセンターにおける音声認識ソフトによるサービスとして提供される。さらなる高機能である、自動翻訳による自動車間の国際電話機能も現実味を帯びてきている。
一方で、2013年よりメルセデス・ベンツ、ボルボなどはセーフティ・パッケージと呼ばれる自動車運転時の対歩行者や対車に対する被害軽減・衝突回

特徴的な概観を持つ、玉川大学量子情報科学研究所。ここで世界最高性能の「量子エニグマ暗号」の開発に成功した。

避装置をオプションで提供するサービスを開始した。現時点では自車で完結する自立型であるが、テレマティクスと統合され、自動車の制御系がネットワークに接続され、さらなる高度な運転制御ソフトがデータセンターから提供可能になれば自立型自動運転を超えた非常に高度な自動運転システム実現へと繋がる。

このように、自動車自身が超高性能の情報処理機械となりつつあり、もはや、自立型の情報処理では機能的な限界が見えているため、巨大なデータセンターを基盤とするクラウド型インターネットによるテレマティクスの実現に向けた開発がアメリカやイスラエルにおいて進められている。このようなシステムによって運転者の利便性のみならず、交通渋滞や交通事故の軽減、マクロ経済の問題の解決などへの大きな波及性が期待できる。



データセンターを基盤とするクラウド型インターネット

企業や国家、自治体などの公的機関のクラウド型インターネットの概念。データセンターとの通信を攻撃されたり、盗聴される危険性を回避する必要がある。

クラウドの技術の現状と問題点

クラウドを支えるデータセンターと光通信

数百万もの自動車や端末に対する上記のようなサービスを実現するには、超高機能のソフトウエアを集約し、それによるユーザーが要求する制御などを瞬時に処理するデータセンターが必須となり、それらを要所に配置することが求められる。

一方、あらゆるデータがそのデータセンターに集中するため、それらのデータが消滅したときの被害は計り知れないくらいに大きくなる。そのため、巨大データセンターのデータのコピーを予備のデータセンターに瞬時に伝送し、幾つかのデータセンターが機能不全となっても、瞬断することなく対応できるようにする必要がある。

巨大なデータを瞬時に他のデータセンターに伝送する技術が超大容量の光ファイバ通信である。一本の光ファイバは100個の波長の光信号を同時に伝送できる。1つの波長に10ギガビット毎秒のデータを乗せることができ、1本の光ファイバで100個の波長により一度に1テラビット毎秒のデータを伝送できる。したがって、光ファイバ回線網はデータセンター間の超大容量通信の必須技術であることを理解していただけよう。

光ファイバ回線網へのサイバー攻撃

自動車のデジタルデータや携帯電話による会話情報は無線中継局で集められ、光ファイバ回線網を介してデータセンターで分類・処理され、それらを目的地の近くで無線に変換して通信が完結する。

データセンターでは、どのデータが誰のものであるかを瞬時に正確に特定することが必要であるため、全てのデータは識別番号を持っている。

したがって、第三者でも、データセンターに入ってくる信号や保存されている信号を取り出せば、個人の情報を正確に入手することができる。一般にデータセンターは管理権限を有する人によって管理されており、誰もが直接操作できるものではない。

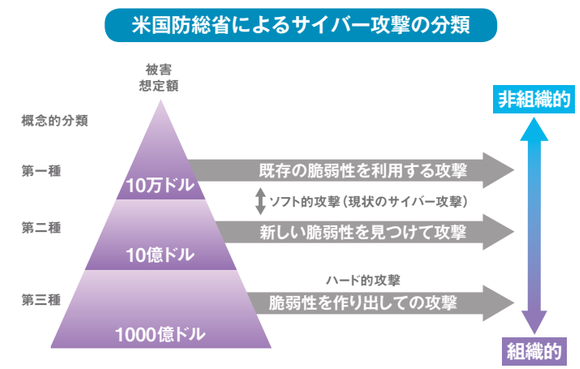
しかし、ネットワークに接続されていれば、世界のどこからでもそのサーバーにアクセスすることが原理的には可能である。

現在、政府が考えているサイバー攻撃の対策は、そのアクセス検査を突破するソフトウエア技術を迎撃するソフトの開発である。後で述べるが、このようなサイバー攻撃は大きな課題ではあるが致命的な被害とはならない。

一方、クラウド用のデータセンターを結ぶ光ファイバ回線網はデータセンターの全てのデータを一括して伝送しており、この光ファイバ回線網の数カ所から通信信号がコピーされ攻撃者のデータセンターに蓄積されれば、データセンターが丸ごとコピーされたことに等価となり、スーパーコンピュータが一台あれば、瞬時にあらゆる個人データやインフラ制御情報を峻別・処理することが可能になる。

ここまでに述べたように、クラウド型のインターネットの恩恵として、テレマティクスなどに見られる自動車や端末機器のグローバルなネットワーク化などによって、これまでには不可能と考えられていたサービスが展開され、今まで以上に豊かな社会を実現できることが期待できるが、それは、同時に、ネットワークの要である光ファイバ回線網へのサイバー攻撃によって、特定のターゲットへの攻撃（遠隔操作による故意の事故の誘発など）や、ネットワーク化された全ての自動車や端末が一斉に操作され、社会秩序が壊滅的な被害をこうむる危険性を排除できないことになる。

したがって、光ファイバへのサイバー攻撃の防御は緊急の社会問題であり、その防御の研究開発は国家的な課題と考えなければならない。



サイバー攻撃の分類

サイバー攻撃による被害を金額に置き換えると、かなりの額にのぼることが分かる。重大な情報漏洩は、ほとんどが通信データのやり取りの間で発生している。（出典：Defence Science Boad, 2013）

量子エニグマ暗号の開発

新量子暗号の提案

通信回線網を流れるデータを守る技術は暗号であるが、光ファイバ回線網を流れるデータは数百ギガビット毎秒以上の超高速であるため、そのような超高速なデータを安全性を保証しながら暗号化するには、これまでの暗号技術を超えた、全く発想の異なる暗号技術が必要となる。

米国政府は、1998年頃から、上記の事態を見越して超高速でかつ、これまでの安全性の概念を変えてしまう新暗号の研究開発を2000年に国防高等研究計画局（DARPA）プロジェクトとしてノースウエスタン大学を拠点に据え、研究を開始した。

当時、世界最大の量子情報科学の国際会議を運営していた筆者に協力要請が来たため、玉川大学の量子通信研究グループは新暗号（超高速な量子暗号）の研究に着手した。当時、量子暗号とは光子1個に情報を乗せ、データを暗号化する鍵使い捨て暗号用の鍵を配送するBB84型量子鍵配送技術を意味していた。

これは光子1個という極めて微弱な光信号で通信するため、原理的に100キロビット毎秒程度の速度しか出ないし、実用上の通信距離も10kmが限界である。米国の考え方は、世界各国にはこのBB84型の量子暗号を開発させ、自国は超高速な新量子暗号を開発するというものであり、これは大成功であった。2012年5月に米国DARPAは突然、量子暗号の仕様性能は、速度が1～10ギガビット毎秒、通信距離は千km～1万kmでなければ意味がないと発表した。日本では、BB84型量子暗号に数百億円の研究費が投じられ、東京都内には巨大な試験運用の量子暗号通信システムが完成したが、速度が10キロビット毎秒で通信距離が数十kmであり、全く実用的価値の無いものとなっている。

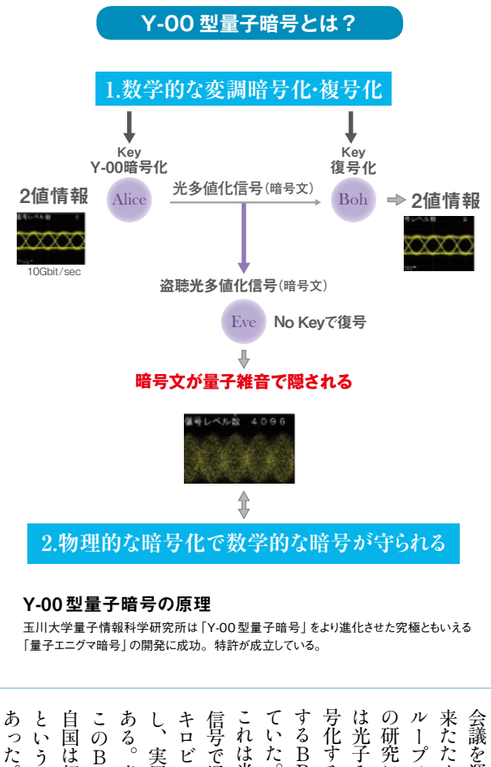
一方、新量子暗号は、概念を発明した米国ノースウエスタン大学のYuen教授の名前から、筆者がYuen-2000プロトコル（Y-00）と命名した。ここで、この暗号の原理を簡単に説明する。

この暗号はデータの情報を運ぶ光信号を発生する通信装置の変調機能を数学的な暗号によってスクランブルする機構と、そのスクランブルされた信号を、変調に利用された数学のパスワードを持たずに受信すれば、光の量子雑音によって完全に破壊され、光信号が運んでいる情報を見ることができないように設計されることで強力な暗号として機能する。

パスワードを持った正規受信者の受信機で受信すれば量子雑音の効果を無視できる。したがって、正規の送信・受信機は通常の光通信と同じ超高速な光通信として動作する。正規の通信者間には、どこにも量子現象が無いように見え、盗聴しようとするものだけに量子効果による妨害が発生する機構であることが、このアイデアの素晴らしさである。

暗号学の限界打破への挑戦

このような暗号の暗号学的な意味は次



Y-00 型量子暗号の原理

玉川大学量子情報科学研究所は「Y-00 型量子暗号」をより進化させた究極ともいえる「量子エニグマ暗号」の開発に成功。特許が成立している。

のように説明できる。数理暗号はデータを複雑な数学でスクランブルするが、そのスクランブルされた信号を暗号文と言う。その暗号文のランダムさによって暗号の強さが評価される。しかし、数学のみでは、シャノン限界と呼ばれる暗号学的な限界があり、全数探索によって原理的には解読可能となる。Y−00プロトコルは、上記暗号文を量子雑音によって再度スクランブルするため、シャノン限界を超える事が可能である。

しかし、開発当初、このようなY−00暗号機構を実現する方法が存在するのかどうかは不明であった。Yuen教授の同僚のKumar教授と玉川大学は独自の実現法を開発し、それぞれ2・5ギガビット毎秒の暗号装置を実現した。これらは、超高速データを物理的に暗号化する、世界初の量子暗号であった。

しかし、この段階では、暗号文の隠れる量が小さく、期待された性能を達成できないことが判明した。暗号文が完全に量子雑音によって隠れる暗号は、特別に暗号の王様を意味する「量子エニグマ暗号」と呼ばれる。これは、暗号文が完全な真正乱数になるということであり、究極的な暗号となる。最近、超高速性を維持しながら、それを実現する方法が玉川大学量子情報科学研究所によって提案され、特許が成立している。

現在、実験的に上記提案を実証する研究が二見史生准教授、加藤研太郎准教授、臼田毅准教授らによって進められている。一方、米国のベル研究所もまた、光ファイバの特性を利用した超高速光通信を安全にする方法を提案しており、光ファイバ通信網の安全化の開発は激しい競争に突入した。それを踏まえて、本年より、ベル研究所と本学との定期的な意見交換会がスタートした。

安心・安全なネット環境の実現の責務

求められる正しい現状認識

情報技術の発展は社会構造を大きく変貌させ、インターネットは社会のインフラとなった。前述のように、この社会インフラを背景としたサイバー戦争は現実味を帯びているため、防御技術の開発を加速させる必要がある。しかし、ITの安全性に関係する日本の関係者の認識は必ずしも正しいものではない。すなわち、米国国防総省が定義している3種のサイバー攻撃の内、ソフト的な攻撃のみが対象となっており、最も深刻な通信回線保護の概念が欠落している。

小原芳明・玉川大学学長は早くから、この問題に警鐘を発し、本学研究所の活動に精力的な援助を行っている。その効果として、最近では、日本の通信事業者も、自らの通信回線の保護の必要性について、言及するようになってきた。

以上より、政府は、進化しつつあるインターネットの安心・安全を確保する技術開発を進めるに当たり、全てのサイバー攻撃対策を統合した研究チームを編成し、ネットの安全性意識の啓蒙を活発化することが望まれる。

2013年からベル研究所と玉川大学との定期的な意見交換会がスタートした。加藤准教授と二見准教授は、ベル研究所で行われた両研究所間の意見交換会で講演した。

see VISIONS

広田 修
玉川大学量子情報科学研究所 所長

ひろた おさむ／1948年、富山県生まれ、工学博士（東京工業大学）。1975年ごろより、米国のMITとソビエトのモスクワ大学と同時期に量子通信の研究を開始し、今日の量子情報科学の基盤となる量子通信理論で顕著な貢献を残している。1990年、量子情報科学分野の創設となる量子通信国際会議を創設し、20年間会長。2002年、MITより量子情報科学顕彰。総務省量子情報通信技術推進会議委員などを歴任。

参考文献

〔1〕G.Borbosa, et al, Physical Review Letters, vol-90, 227901, 2003.

〔2〕O.Hirota, M.Sohma, M.Fuse, K.Kato, Physical Review A, vol-72, 22335, 2005.

〔3〕広田 修・二見史生「量子エニグマ暗号」万葉舎 2013.