In Secure Broadcast Communicatoin in Wired and Wireless Networks (Japanese translation), A. Perrig and J. D. Tygar,
translated by Fumio Mizoguchi and the Science University of Tokyo Information Media Science Research Group,
Kyoritsu Shuppan, 2004

ワイヤード/ワイヤレスネットワークにおける ブロードキャスト通信のセキュリティ

監訳
東京理科大学・教授・溝口文雄

目次

図目次

表目次

プロトコル目次

原著の序文

メディアのストリーミング，センサネットワーク，衛星通信，そして，新たに登場している多くのアプリケーションは，ブロードキャスト通信に依存している．このブロードキャスト通信は本当のブロードキャスト（例えば，100 万の受信者へ送信する衛星）の可能性もあり，IP マルチキャスト上に実装されている可能性もある．セキュリティは，それらの基盤技術を問わず，ほとんどのアプリケーションにおいて不可欠な要件である．

ブロードキャストのためのセキュリティは 2 点間通信と異なる懸案事項を持っており，特に，盗聴は単純に行われてしまう．大規模かつ動的なものとなりうるブロードキャスト加盟者の集合から，困難な鍵管理問題生じる．受信者は異種混合であり，異なる計算資源，異なるバンド幅，そして，異なる遅延が存在する．制限された計算資源を持つ受信者においては，単純な暗号でさえ，重大なオーバヘッド（負荷）を必要となりうる．パケットはしばしばロス（損失）し，ロスしたパケットの再送信は，受信者数が莫大な場合には困難な問題となる．

本書ではセキュア（安全）なブロードキャストのための多くのプロトコルを提示する．本書でワイヤード/ワイヤレス（有線および無線）双方のネットワークについて論議し，ワイヤレスネットワークや，小さい計算能力ではあるが多くのノードからなるセンサネットワークなどの特別なタイプのためのプロトコルの詳細を記述する．そして，鍵配布，認証，否認防止 (non-repudiation) のためのプロトコルを紹介する．また，パケットの不正な挿入，もしくは盗聴する攻撃者から保護する方法を示す．基本的な構成要素としてのプロトコルに焦点を当てていることから，本書は多くのセキュリティレシピを持つ料理本とみなすことも可能である．これらのプロトコルを互いに，もしくはより伝統的なセキュリティプロトコルと組み合わせることにより，セキュアなシステムを構築する方法を示すことができる．

本書の構成は次の二つのレベルからなる．最初に，概念レベルのセキュリティを詳述し，次に，我々の研究を実装するための議論を行うことで例証する．我々は，セキュリティに携わる大学院生，研究者，そしてエンジニアのために本書を執筆した．広範囲の計算量論的な議論は避け，プロトコルの機能的な記述を心がけた．また，自己の学習のために，高度な大学院レベルのセミナにおけるテキストとして，もしくは，大学院生の最初の年のセキュリティないしネットワーククラスにおける補助テキストとして役立てていただきたいと考えている．

謝辞

本書における数々の仕事は同僚との共同研究に由来している．本書の作成の準備に当たり，元の論文と異なり，より理論的または学術的な要素はかなり削除してあるが，これらの研究を利用している．オリジナルは以下の論文で読むことができる[HJP02, HPJ01, HPJ02, MP02, Per01, PCB+02, PCST01, PCST01, PCTS00, PCTS02, PST01, PSW+01, PSW+02, SP01]．特に以下の同僚研究員および共著者たちに深く負うものである．Bob Briscoe, David Culler, Ran Canetti, Yih-Chun Hu, David Johnson, Michael Mizenmacher, Dawn Song, Robert Szewczyk, Victor Wen．彼らの創造的発想，批判，励ましと友情に深く謝意を表したい．

Ross Anderson, Manuel Blum, Nikita Borisov, Eric Brewer, Monica Chew, John Chuang, Yongdae Kim, Hugo Krawczyk らは数々の実りの多い議論、そして元のブロードキャストセキュリティの論文および本書の初稿に対してコメントを行ったことに対し，特に謝意を表したい．

本書の仕事の大半は，著者たちが UC バークレイに在籍したときに成されたものである。UC Berkeley の電気工学およびコンピューターサイエンス学部および情報経営システム校は，本題材を進展させるのに素晴らしい場所であった。特に Randy Katz， Rechard Newton，Christos Papdimitrious, Shankar Sastry および Hal Varian は，バークレイの研究環境をよりよくしてくれたことに謝意を表したい．著者の一人 Perring はこの本における研究の一部を IBM の T. J. ワトソン研究ラボおよびデジタル財団にて報告をしており，この研究を継続させてくれたことに対して謝意を表明したい．研究基金の助成を受けた全米科学財団，米国防総省高等研究局および米国郵政局は，当題材の進展に十分な貢献した契約を行ったことに対し，改めて感謝の意とともにここに記しておきたい．

賢明な助言および本書を完成まで導いてくれた Kluwer の編集者 Alexander Greene には特に謝意を表したい．Perrig は Down に，そして Tygar は妻 Xiaoniu にこの本を捧げる．彼らの愛および忍耐に対して言葉にできないほど恩義を受けている．

本書における間違えはすべて我々に帰する。本書に対するコメントおよび訂正を歓迎する.

アドリアン・ペリング (adrian.perrig@cs.cmu.edu)
J. D. タイガー (tygar@cs.berkeley.edu)

日本語版への序文

溝口文雄教授と彼の研究室の皆さんのご尽力によって，我々のテキストの素晴しい日本語版が生まれたことを大変光栄に思います．溝口教授と彼の学生および研究者の皆さん（とりわけ平石広典助手）の努力には深く感謝致します．

インターネット上の攻撃の増加や，ブロードバンドやセンサ，Web，およびそれらの関連技術の急速な発展により，ブロードキャスト認証の問題はこの１年でさらに重大な問題となっています．我々はこの問題に取り組む日本の技術者や研究者にとって，このモノグラフが有益なものとなることを心より願っています．

本書の英語版の出版以降，我々はこの研究を更に発展させたので，ここで簡単に紹介したいと思います．我々の同僚との最近の研究により，本書で提示した枠組みを，サービス妨害 (denial of service) 問題への対処にも拡張しました．この種の問題は，受信者に対する妨害を目的として攻撃者が大量の偽のパケットをブロードキャストすることによって発生します．Merkle ハッシュ木を用いることにより，この種の攻撃を防止することが可能であり，その防御手法について次の論文で議論しています．

- Distillation Codes and Applications to DoS Resistant Multicast Authentication, Chris Karlof, Naveen Sastry, Yaping Li, Adrian Perrig, and J. D. Tygar, *Proceedings of the Eleventh Annual Network and Distributed Systems Security Symposium (NDSS2004)*, February 2004.

この論文のコピーは World Wide Web 上にいくつか存在しており，Google を使えば簡単に見つけることができます．現時点（2004 年 4 月）では，以下から入手可能です．

- http://www.cs.berkeley.edu/~ckarlof/papers/NDSS2004-final.pdf

　いつものごとく読者からのコメントや質問を両著者とも歓迎します．我々が考えるのと同様に，皆さんも安全なブロードキャスト認証の問題が興味深いものであると認めてくれることを願っています．

Addrian Perrig (perrg@ece.cmu.edu)
Doug Tygar (tygar@cs.berkeley.edu)

監訳者の序文

監訳者が原著の著者にお会いしたのは，いまから 2 年前の米国科学財団が主催したセキュリティ関係のワークショップに参加したときであった．当時，カリフォルニア大学バークレイ分校のダク・タイガー教授の博士過程の学生であったアドリアン・ペリングさんはそのワークショップでは会議録係であった．ダグ・タイガー教授がそのワークショップの主催者であった．

このワークショップへの日本からの他の参加者は東京大学の米澤明憲教授であり，米国側を含めて以下の 28 名であった．

ダグ・タイガー教授

Bellovin Steve, AT&T
Blaze Matt, AT&T
Dhamija Rachna, UC Berkeley
Feigenbaum Joan, Yale University
Felten Ed, Princeton University
Fisher Darleen, NSF/UCB
Gligor Virgil, University of Maryland
Kemmerer Richard, UC Santa Barbara
Landwehr Carl, NSF
Lee Peter, Carnegie Mellon University
Levitt Karl, UC Davis
Lunt Teresa, Xerox Parc
Lynch Nancy, MIT
Maughan Doug, DARPA
Millen Jon, SRI
Mizoguchi Fumio, Tokyo Univ. of Science
Neumann Peter, SRI
Perrig Adrian, UC Barkeley
Paxson Vern, ICSI
Reiter Mike, Lucent
Smith Jonathan, Univ of Pennsylvania
Smith Sean, Dartmouth
Tygar Dug, UC Berkeley
Wagner David, UC Berkeley
Wallach Doien, Rice University
Yee Bennet, UC San Diego
Yonezawa Akinori, University of Tokyo
Znati Taieb, NSF

会議には事前にポジションペーパを提出していくだけで，あとは会場のカリフォルニア大学のファカルティクラブでの昼食とコーヒーブレイクがあるという進行であった．参加者はポジションペーパに沿って約 10 分程度のプレゼンテーションをし，その後，全員でブレインストーミングを行い，課題を抽出するという内容がそのワークショップであった．ブレインストーミングの方法は，大きな白い紙にテーマをリストしていき，それを次第に整理するという方法で，これは日本も米国も変わりないやり方であった．

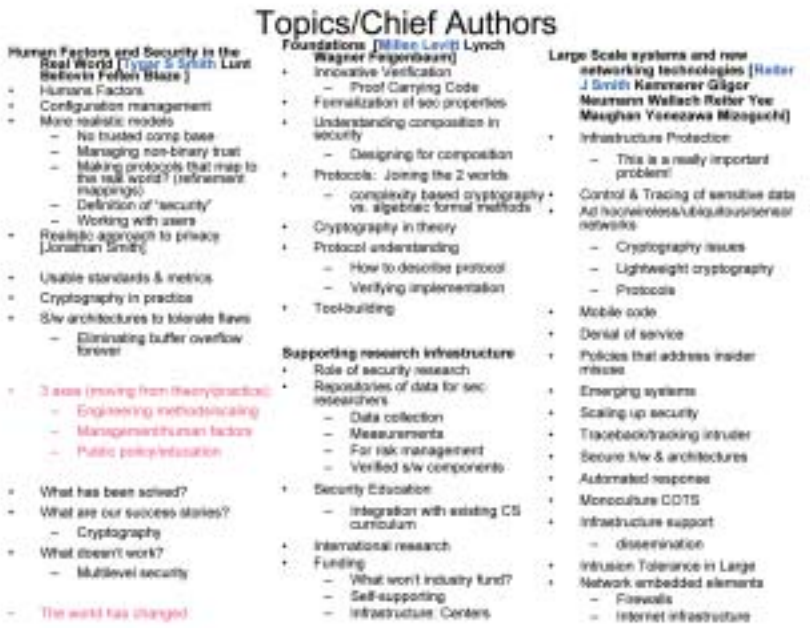
司会進行のタイガー教授が大きな白い紙にテーマを書いて整理されていた．その様子をすべて記録していたのがタイガー教授の大学院生であったペリングさんであった．彼の同僚であり，共同研究者がダンソン（Dawn Song）さんである．

ダンソンさんも西華大学の物理出身の才媛で，高速の定理証明器である athena の設計者として知られ，様々な新しい論文をペリングさんと書

カリフォルニア大学のファカルティクラブ

ミーティングの様子

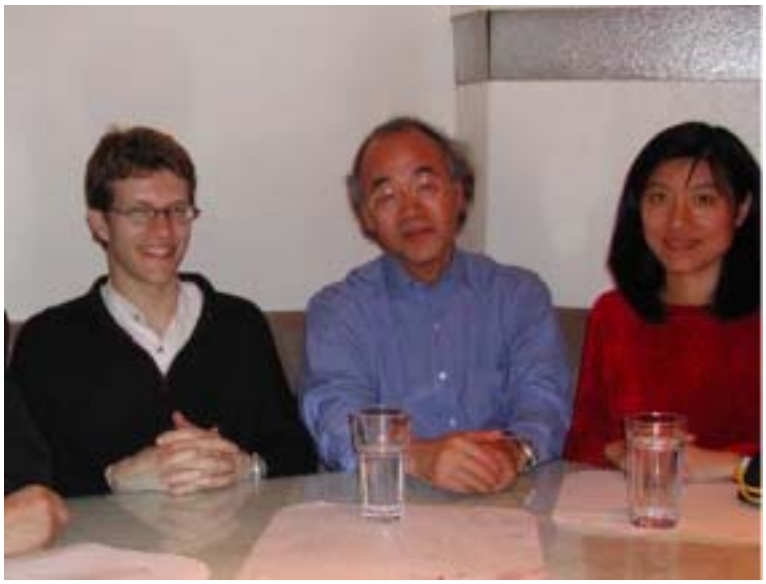
いている．ペリングさんの博士論文の背景になっているセンサネットワークはカリフォルニア大学のバークレ分校で盛んに研究されており，そのセ



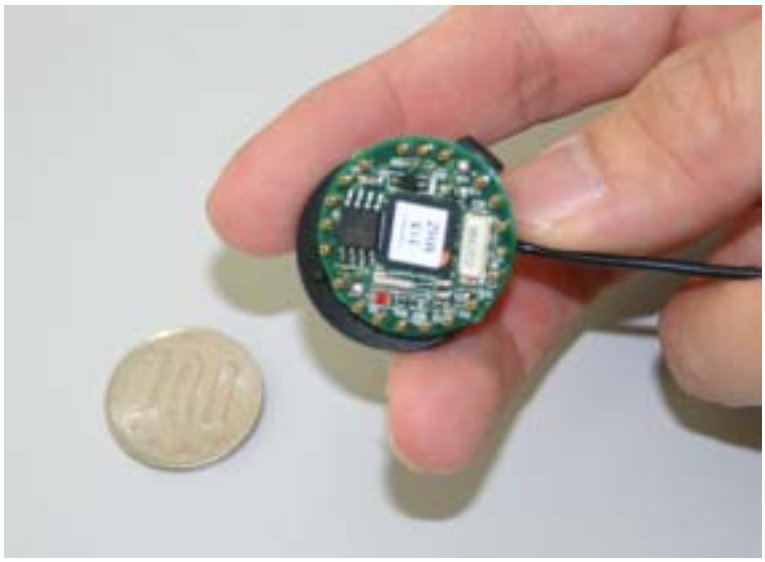
ブレインストーミングによって抽出された課題

ンサネットワークのセキュリテイプロトコルが彼の博士論文の一部になっているのである．ちょうどペリングさんが博士論文を書き終えて，その論文のドラフトを読む機会があり，この論文が基となって本になるということを聞き及んだ．翻訳をするには良い内容と判断して，そのことをペリングさんとタイガー教授に伝えたところ，ぜひお願いしたいということになり，この翻訳に取り組んだ次第である．ところで，この分野は日本でもまだ研究者が少なく，この本の背景である「センサネットワーク」に関連する情報は最近になってリリースされたようである．その元になっているのは，Smart Dust と呼ばれるプロジェクトでのセンサチップである．Dust というイメージでいうと粉のように小さいチップを想像しがちだが，実際は 500 円硬貨ほどの大きさである．

こうしたセンサチップが環境にばらまかれると，自律的にネットワークを作り，その環境内の情報を取りだすような働きをするというものらしい．そのときに使われるセンサ内のセキュリティプロトコルを研究していたのがペリングさんである．このプロトコルは μTESLA と呼ばれ，このプロトコルが tinyOS で作成されているので，理論だけでなく実際面での



バークレイでの夕食にて（左から，ペリング，溝口，ダンソン）



センサチップ

応用性がテストされているのである．こうした背景にはカリフォルニア大学のバークレイ分校の研究背景と先端性を伺うことができる．

なお翻訳にあたりすばやい対応でこの企画を実現してくれた共立出版とその担当の小山透さんに感謝する．また，タイガー先生は日本語を読むことができるとのことで，本書の原稿をお送りしたところ，丹念に赤入れをしていただいたことには，驚きと同時にたいへん感謝する次第である．翻訳の分担は以下のとおりである．第 1 章から第 3 章を東京理科大学情報メディアセンター・助手・平石広典，第 4 章を東京理科大学理工学部助手・西山裕之，第 5 章を東京理科大学情報メディアセンター・ポスドク・大林真人，第 6 章を東京理科大学理工学研究科・博士課程・山崎航，第 7 章から第 9 章を東京理科大学理工学研究科・博士課程・嶺行伸が担当した．監訳者は全体の調整を行った．素早い対応をしてくれた分担者に感謝する．また，訳のミス等が無いよう，監訳者の溝口は，翻訳が完成した段階で，非専門の立場から，監訳者の長男である，溝口哲郎（オタワ大学経済学博士課程）の協力を得た．同君により，翻訳の漏れを確認してもらった．しかしながら，最終的な訳の誤りは監訳の責任である．

本書は今後急速に進展し普及するであろうブロードキャスト通信：ワイヤード／ワイヤレスネットワークやセンサネットワークなどに不可欠であるセキュリティ技術の詳細，特にプロトコルの設計を具体的に知り得る貴重な文献である．本書の出版が我が国のセキュリティ研究に一層のはずみがつく一助となれば幸いである．

2004 年 4 月 溝口文雄