Network and Distributed System Security Symposium における研究動向の調査

小手川 祐樹 *　田端 利宏†　堀 良彰 †　櫻井 幸一 †

概要 2004 年 2 月 5 から 6 日にかけてアメリカ合衆国のカリフォルニア州サンディエゴで開催された The 11th Annual Network and Distributed System Security Symposium (NDSS'04) の開催概要の報告および近年の NDSS における研究動向の調査結果を述べる．

キーワード NDSS，参加報告，研究動向

A Survey of Network and Distributed System Security Symposium

Yuki KOTEGAWA *　Toshihiro TABATA †　Yoshiaki HORI †
Kouichi SAKURAI †

Abstract— This paper reports the 11th Annual Network and Distributed System Security Symposium (NDSS'04) held on 5-6 February 2004 in San Diego, California, U.S.A. A survey of research trends on NDSS is also presented.

1 はじめに

本稿では，2004 年 2 月 5 日から 6 日にかけてアメリカ合衆国のカリフォルニア州サンディエゴで開催された The 11th Annual Network and Distributed System Security Symposium (NDSS'04) [1] について，その概要を報告する．また，近年の NDSS において盛んに取り組まれている研究について調査を行った結果を報告する．

2 NDSS 概要

NDSS は Internet Society(ISOC) [2] によって主催されているシンポジウムであり，1999 年以降は 2 月初旬にアメリカ合衆国カリフォルニア州サンディエゴの Catamaran Resort Hotel で開催されている．本シンポジウムは，ネットワークおよび分散システムにおけるセキュリティサービスの研究者や従事者間での情報交換の促進を目指しており，主な参加対象者として，ネットワークセキュリティおよび分散システムセキュリティに関して，理論よりも実際のシステム設計や実装に焦点をあてて興味を持っている者をあげている．そして主な目的の一つは，インターネット・コミュニティを激励し，利用可能なセキュリティ技術を適用・配備・推進できるようにすることである．本シンポジウムは，技術的な論文の発表だけではなく，今後のネットワークセキュリティの動向を示唆するようなパネルディスカッションも多く取り入れられている．

またシンポジウムの前日にはチュートリアルが開かれており，*Network Security Protocol* のようなネットワークセキュリティの全般の動向に関するものと *IPsec* や *Wireless LAN Security* のような個別テーマから構成されている．

なお，本シンポジウムにおける近年の採録論文は ISOC によって公開されている [3].

3 NDSS'04 参加報告

NDSS'04 は 2004 年 2 月 5，6 日にアメリカ合衆国カリフォルニア州サンディエゴの Catamaran Resort Hotel で開催された．投稿論文 98 本のうち採録は 16 本で，採録率は 16.3 % (NDSS'03 は投稿論文 82 本で，採用論文数 17 本の採録率 20.7 %) であった．また査読基準として "研究の新規性"，"分野の重要性"，"研究の質" があげられていた．本シンポジウムの参加人数は 100 名程であり，アメリカ合衆国からの参加者が大半であった．他国からの参加者

* 九州大学大学院システム情報科学府 〒 812-8581 福岡市東区箱崎 6-10-1, Graduate School of Information Science and Electrical Engineering, Kyushu University, 6-10-1 Hakozaki, Higashi-ku, Fukuoka City, Japan: kotegawa@itslab.csce.kyushu-u.ac.jp
† 九州大学大学院システム情報科学研究院 〒 812-8581 福岡市東区箱崎 6-10-1, Faculty of Information Science and Electrical Engineering, Kyushu University, 6-10-1 Hakozaki, Higashi-ku, Fukuoka City, Japan: {tabata,hori,sakurai}@csce.kyushu-u.ac.jp

はカナダ 3 名，イギリス 1 名，ドイツ 1 名，韓国 3 名，シンガポール 1 名，スエーデン 3 名であり，日本からは 4 名であった．また所属については大学関係者が最も多く，続いて企業関係者，政府関係者の順であった．

以下に NDSS'04 のチュートリアルおよび採録論文をあげる．

[TUTORIAL]

チュートリアルは 2004 年 2 月 4 日に同会場で行われた．以下にあげる *Network Security Protocols: Today and Tomorrow*, *Selected topics in information security*, *Language-based Security*, *IPsec tutorial* の 4 並列で行われる予定であったが，*Language-based Security* はキャンセルになったため，残りの 3 つが並列して開催された．

"Network Security Protocols: Today and Tomorrow"(Radia Perlman and Charlie Kaufman)

本チュートリアルでは，ネットワークプロトコル全般についての講演が行われた．暗号の基礎から始まり，認証，E メール関連セキュリティ，ファイアウォール，SSL，IPsec などに渡って，幅広くネットワークセキュリティを扱う内容であった．講演は，講演者が 2 人が交代しながら話を進め，質疑応答はいつでも自由に行える形式で行われた．なお，参加人数は 14 人であった．

"Selected topics in information security"(Steven Kent)

本チュートリアルでは，講演者によって選択された認証に関する 6 つのトピックを扱った．バイオメトリクス，PKI, CA(Certification Authority) のセキュリティを高める方法，IPsec，BGP(Border Gateway Protocol) におけるセキュリティについて講演が行われ，最後の一つであるプライバシを集約した認証方式は時間の関係上省略となった．なお，参加人数は 8 名であった．本セッションも上記チュートリアルと同様に，講演の途中で自由に質疑応答が行われる形式であった．

"IPsec: It's simpler than you think!"(Angelos Keromytis and John Ioannidis)

本チュートリアルでは IPsec およびその鍵管理プロトコル IKE の特徴についての講演が行われた．ネットワーク層におけるセキュリティの必要性を述べ，IPsec がどのように利用されるかを理解するために，データグラムカプセル化，トンネリング，および VPN などのオーバレイネットワークを扱った．また IPsec のファイアウォールや NAT との相互作用についても扱われた．本チュートリアルには参加していないため，参加人数や講演形式についての詳細は分からないが，上記の 2 つのチュートリアルとほぼ同様であると思われる．

[SESSION 1: Multicast Authentication]

"DoS Protection for Reliably Authenticated Broadcast"（Carl Gunter et al.）

人為的にパケットロスを発生させることで，攻撃パケットの挿入による DoS 攻撃の効率を軽減できる Selective Authentication を提案．さらに Selective Authentication を用いたブロードキャスト認証のための耐 DoS プロトコルである BAS(Broadcast Authentication Streams) プロトコルを提案し理論的解析や実装評価を行っている．

"Distillation Codes and Applications to DoS Resistant Multicast Authentication"（Chris Karlof et al.）

Erasure Code と同様に前方誤り訂正が可能であり，さらに Pollution Attack へ耐性を持つ Distillation Code を提案．また Distillation Code を用いた認証可能マルチキャストストリームである PRABS(Pollution Resistant Authenticated Block Streams) プロトコルを提案し，理論的および実験的評価を行っている．

[SESSION 2: Invited Talk]

"Hacks, Attacks and eCommerce Fraud"（Michael A. Garduno）

電子商取引におけるクレジットカード利用に対する被害と対策についての講演が行われた．

[SESSION 3: Intrusion Detection]

"Efficient Context-Sensitive Intrusion Detection"（Jonathon T. Giffin et al.）

Model-based 侵入検知に利用するモデルはプログラムの静的解析によって生成されるが，その検知精度と生成効率はトレードオフである．本論文では Dyck Model を提案し実験的評価を行っている．Dyck Model ではプログラムが生成するシステムコールの正しい並びと，関数呼び出し地点で起きる状態変化が記述される．また，模倣攻撃と回避攻撃を検出するための静的解析手法についても述べられている．

"Global Intrusion Detection in the DOMINO Overlay System"（Vinod Yegneswaran et al.）

グローバル IDS のための DOMINO(Distributed Overlay for Monitoring InterNet Outbreaks) システムを設計し実験的評価を行っている．DOMINO システムでは使用されていない IP アドレスへの接続を検出し，その接続元の IP アドレスなどが特定できる．特定された情報は異種ノード間で交換され，攻撃の分類やリアルタイムなブラックリスト作成などが行われる．

"Building Attack Scenarios through Integration of Complementary Alert Correlation Method"（Peng Ning et al.）

互いに補足しあう複数のアラートを統合することで攻撃シナリオを生成する方式の提案と実験的評価を行っている．アラートの属性の類似性を基にした統合方式および攻撃の必要条件と結果を基にした統合方式の 2 つが提案されている．

[SESSION 4: New Directions]

"Client-Side Defense Against Web-Based Identity Theft"（Neil Chou et al.）

Web の成りすましによる個人情報などの漏洩について議論し，それらの攻撃をクライアント側で防御するためのフレームワーク SpoofGuard を提案し実験的評価を行っている．SpoofGuard はブラウザプラグインとして開発されており，表示している Web ページを検査し結果に応じてユーザに危険を知らせる．

"Using Directional Antennas to Prevent Wormhole Attacks"（Lingxuan Hu et al.）

通信に使われる暗号を破らずに無線ネットワークルーティングを狂わせることのできる Wormhole Attack の解析を行っている．また指向性アンテナを利用した防御プロトコルの提案および実験的評価を行っている．提案プロトコルでは隣接ノードが正しいものか偽のものであるかを特定するために，各ノードは指向性情報を共有する．

“An Effective Architecture and Algorithm for Detecting Worms with Various Scan”（Jiang Wu et al.）

ワームが使用する IP アドレススキャン方式（random scan, selective random scan, routable scan, divide-conquer scan, complete scan）の効率を解析している．またスキャンを受けた被害ホストの数を基にしたワーム検出アルゴリズムの提案とそのアルゴリズムのシミュレーション評価を行っている．

[SESSION 5: Secure Software]

“A Practical Dynamic Buffer Overflow Detector” （Olatunji Ruwase et al.）

C プログラムのための動的バッファオーバラン検出器 CRED(C Range Error Detector) を提案し実装評価を行っている．CRED ではメモリアクセスの境界を直接チェックするため全てのバッファオーバラン攻撃を検出できる．プログラム検査において，OOB(Out-of-bound) オブジェクトを新しく導入することで，既存方式の欠点である OOB を利用しているプログラムが検査によって壊される問題を解決している．また文字列に対しては，バッファオーバラン検査を行わないことで検査はより効率的に行われる．

“Model Checking One Million Lines of C Code” （Hao Chen et al.）

セキュリティが重要なアプリケーションのソフトウェアモデル照合ツールである MOPS(MOdel checking Programs for Security properties) を用いて，UNIX アプリケーションを実験評価している．モデル照合により解析できるセキュリティ脆弱性の例として脆弱性の 5 つの重要なクラスをとりあげ，一時的な安全特性としてそれらを体系化する方法を述べている．

“Ostia: A Delegating Architecture for Secure System Call Interposition”（Tal Garfinkel et al.）

Delegating Architecture によりシステムコールをフックし，アクセス制御を行う Sandbox システム Ostia の提案と実装評価を行っている．Delegating Architecture ではライブラリとエージェントによりユーザレベルでアクセス制御が動的に行われる．また今日の Sandbox に一般的に利用されている Filtering Architecture とこの Delegating Architecture の比較も行っている．

[SESSION 6: Database and Audit Log Protection]

“Authentication and Integrity in Outsourced Databases” （Einar Mykletun et al.）

Outsourced Database(ODB) には，処理の効率性とデータの完全性および信頼性が求められる．デジタル署名を利用してこの問題を解決する方式を提案している．また RSA, DSA および BGLS 署名利用時の署名・検証時間を測定し比較評価している．

“Building an Encrypted and Searchable Audit Log” （Brent R. Waters et al.）

効率的に検索が可能である暗号化された監査ログの生成手法を提案し実装評価している．効率的な呼び出しのためにハッシュチェーンを用いてログのインデックスを作成する．インデックスはクエリから抽出されたキーワードによって，アイデンティティベースの暗号化が行われる．

[SESSION 7: Panel]

The Legal Landscape and its Impact on Security Management

Moderator: Mike Reiter (Carnegie Mellon)

Panelists: Dan Geer (Geer Risk Services, LLC, and Verdasys, Inc.)，David Lacki (Wireless Facilities, Inc.)，Jeffrey Ritter (Kirkpatrick & Lockhart LLP)

セキュリティ管理における法的指標とその効果についての討議が行われた．

[SESSION 8: Protocols]

“Speeding up Secure Web Transactions Using Elliptic Curve Cryptography”（Vipul Gupta et al.）

楕円暗号は既存の公開鍵暗号システムに比べて，鍵サイズ，消費電力，消費メモリおよび消費帯域の面ですぐれていることを述べている．また SSL における楕円暗号の有効性を実験検証しており，2010 年に必要とされるセキュリティレベルにおいて RSA と比べて 120〜279 %の実行性能を実現できることを示している．

“The Design and Implementation of Datagram TLS” （Nagendra Modadugu et al.）

データグラムプロトコルは，SIP，ビデオ配信，ビデオ会議，SNMP，オンラインゲームなどに利用されている．TLS はアプリケーションの通信を保護するが，データグラムプロトコルには対応が不完全である．TLS と同様の性能を持ちデータグラムプロトコルにも対応可能な DTLS(Datagram TLS) の設計，理論的解析および実験評価を行っている．

“The Perils of Unauthenticated Encryption: Kerberos Version 4” （Tom Yu et al.）

効率的な選択平分攻撃の実装を通して，ケルベロスプロトコル v4 の十分な認証なしで重要な情報を暗号化するという欠点を指摘している．またケルベロスプロトコル自体の欠陥を指摘しており v5 にも関連した脆弱性があるため，その改善方法の提案を行っている．

4 NDSS の研究動向

4.1 近年の主な研究分野

NDSS’00 から NDSS’04 において Intrusion Detection System (IDS)，Multicast セキュリティ，DoS 対策技術，ルーティングプロトコルセキュリティ，アクセス制御技術，Transport Layer Security (TLS)，Wireless and Mobility セキュリティなどの研究が取り組まれている．

これらの研究分野から，採録論文数などから判断して特に研究が行われていると思われる Intrusion Detection System，Multicast セキュリティ，Transport Layer Security (TLS)，Wireless and Mobility セキュリティの 4 つの分野を選択し，以下にその分野における研究の詳細を述べる．

[Intrusion Detection System (IDS)]

近年の NDSS において以下のような IDS に関する論文が発表されている．

2000 年には，監視プロセスによってプロセスのシステムコールをユーザレベルで監視するホストベース IDS *"User-Level Infrastructure for System Call Interposition: A Platform for Intrusion Detection and Confinement"(K. Jain et al.)*，Web サーバの CGI プログラムへのアクセスをデータソースとして利用するホストベース IDS *"A Lightweight Tool for Detecting Web Server Attacks"(M. Almgren et al.)* や複数の IDS を利用した分散オブジェクトの統合管理機構 *"Building Adaptive and Agile Applications Using Intrusion Detection and Response"(J. Loyall et al.)* が発表されている．

2002 年には，侵入検知のための攻撃パターン記述言語と完全非集中型の攻撃パターン検出アルゴリズム *"Distributed Pattern Detection for Intrusion Detection"(Christopher Kruegel et al.)* やサンドボックスによってプロセスの不信な振る舞いをコントロールするホストベース IDS *"BlueBox: A Policy-Driven, Host-Based Intrusion Detection System"(Suresh N. Chari et al.)* が発表されている．

2003 年には，仮想マシン (VM) を用いて監視対象ホストとそのホストに導入されている IDS を隔離することで IDS への直接攻撃を遮断する機構 *"A Virtual Machine Introspection Based Architecture for Intrusion Detection"(Tal Garfinkel et al.)* が発表されている．

2004 年には，3 章で述べた Dyck Model を利用したモデルベースの異常検知手法 *"Efficient Context-Sensitive Intrusion Detection"(Jonathon T. Giffin et al.)*，インターネット規模で連携を行うグローバル IDS *"Global Intrusion Detection in the DOMINO Overlay System"(Vinod Yegneswaran et al.)* や互いに補足しあう複数のアラートから新しい攻撃シナリオを生成する手法 *"Building Attack Scenarios through Integration of Complementary Alert Correlation Method"(Peng Ning et al.)* が発表されている．

[Transport Layer Security (TLS)]

近年の NDSS において以下のような TLS に関する論文が発表されている．

2000 年には，TLS プロトコルにおいて公開鍵の代わりに DH-EKE(Diffie-Hellman Encrypted Key Exchange) を利用した手法 *"Secure Password-Based Cipher Suite for TLS"(P. Buhler et al.)* が発表されている．

2002 年には，Web サーバにおける TLS のオーバヘッドの評価 *"Performance Analysis of TLS Web Servers"(Christian Coarfa et al.)*，TLS においてクライアントがサーバの公開パラメータ，ネゴシエイトパラメータや利用可能なハンドシェイクをキャッシュすることで高速にハンドシェイクを行えるメカニズム *"Fast-Track Session Establishment for TLS"(Hovav Shacham et al.)* や TLS ハンドシェイクプロトコルを拡張し複数の証明書を利用した認証ができるなどの利点をもつ TNT(Trust Negotiation in TLS) プロトコル *"Advanced Client/Server Authentication in TLS(Adam Hess et al.)* が発表されている．

2004 年には，3 章で述べた TLS と同様の性能を持ちデータグラムプロトコルにも対応可能な DTLS *"The Design and Implementation of Datagram TLS"(Nagendra Modadugu et al.)* が発表されている．

[Multicast セキュリティ]

近年の NDSS において以下のようなマルチキャストに関する論文が発表されている．

2000 年には，セキュア IP マルチキャストプロトコルのための非中央集中型で耐故障性をもつ効率的なグループ鍵管理アルゴリズム *"Optimized Rekey for Group Communication Systems"(O. Rodeh et al.)*，IPsec を利用したセキュア IP マルチキャストのためのホスト機構 *"An IPsec-based Host Architecture for Secure Internet Multicast"(R. Canetti et al.)* が発表されている．

2001 年には，マルチキャスト認証プロトコルである TESLA(Timed Efficient Stream Loss-tolerant Authentication) プロトコルの改良 *"Efficient and Secure Source Authentication for Multicast"(A. Perrig et al.)* が発表されている．

2003 年には，Erasure Code を利用した実質的に受信者数に制限のないリアルタイムマルチキャスト認証方式 *"Efficient Multicast Packet Authentication"(Alain Pannetrat et al.)* や分散センサネットワークにおけるブロードキャスト認証方式である μ TESLA の改良 *"Efficient Distribution of Key Chain Commitments for Broadcast Authentication in Distributed Sensor Networks"(Dongang Liu et al.)* が発表されている．

2004 年には，3 章で述べたブロードキャスト認証のための耐 DoS プロトコルである BAS(Broadcast Authentication Streams) プロトコル *"DoS Protection for Reliably Authenticated Broadcast"(Carl Gunter et al.)*，Erasure Code と同様に前方誤り訂正が可能であり，さらに Pollution Attack へ耐性を持つ Distillation Code *"Distillation Codes and Applications to DoS Resistant Multicast Authentication"(Chris Karlof et al.)* が発表されている．

[Wireless and Mobility セキュリティ]

近年の NDSS において以下のような無線ネットワークやモビリティに関する論文が発表されている．

2002 年には，Fluhrer，Mantin，Shamir らによって提案された WEP に対する攻撃法を実装 *"Using the Fluhrer, Mantin, and Shamir Attack to Break WEP"(Adam Stubblefield et al.)* や PKI を必要としないアドホック無線ネットワークにおけるセキュアな通信と認証方式 *"Talking to Strangers: Authentication in Ad-Hoc Wireless Networks"(Dirk Balfanz et al.)* が発表されている．

2003 年には，セキュアな距離ベクトルとパスベクトルルーティングプロトコルの提案 *"Efficient Security Mechanisms for Routing Protocols"(Yih-Chun Hu et al.)* や HLP/HIP(Host Layer Protocol/Host Identity Payload) を利用した，エンドホストマルチホーミングとエンドホストモビリティに関するセキュリティ問題の解決法 *"Integrating Security, Mobility and Multi-Homing in a HIP Way"(Pekka Nikander et al.)* が発表されている．

2004 年には，3 章で述べた指向性アンテナを利用した Wormhole Attack に対する防御プロトコル *"Using Directional Antennas to Prevent Wormhole Attacks"(Lingxuan Hu et al.)* が発表されている．

4.2 引用回数による重要論文の抽出

他の論文からの引用回数は，その論文がもつ影響力を量る指標の一つとして考えられる．そこで 1996 年から 2004 年の過去 9 年間における NDSS の採録論文について，科学論文デジタルライブラリ CiteSeer [4] を用いて引用回数の調査を行った．その結果として，引用数が 20 件を越え

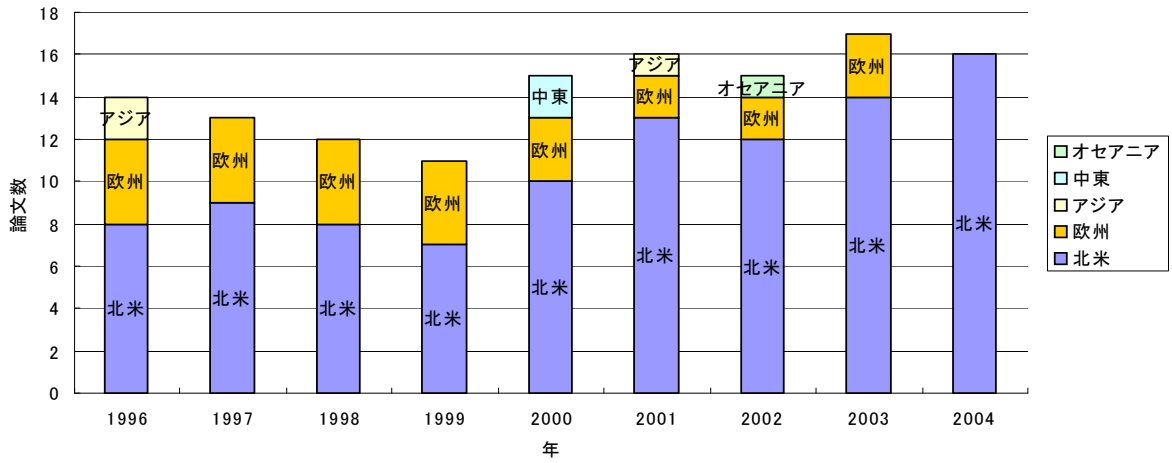

図 1: 地域別採録論文数

た論文を以下にあげる．書式は “題目”(著者)，採録会議名およびセッション名，引用件数となっている．

“Digital Signature Protection of the OSPF Routing Protocol”（S. L.Murphy et al.），NDSS’96 Network Security，26 件

デジタル署名の利用によって OSPF ルーティングプロトコルを保護する方式の提案を行っている．送信されるルーティング情報は非対称暗号アルゴリズムによって署名され，各ルータは受信した情報の送信元と完全性をチェックする．また本提案では解決できない残りの脆弱性についても議論している．

“SKEME: A Versatile Secure Key Exchange Mechanism for Internet”（Hugo Krawczyk），NDSS’96 Key management，36 件

鍵交換プロトコルである SKEME の設計を行っている．SKEME は拡張性と柔軟性をもち，インターネット上の様々な状況とセキュリティモデルに適用できる．公開鍵と鍵配送機関または手動導入を基にした鍵交換が行え，選択的に PFS(Perfect Forward Secruity) も提供可能である．また匿名性，否認可能性，高速鍵更新を提供する．RFC2409:IKE の一部分として取り入れられている．

“Blocking Java Applets at the Firewall”（David M. Martin Jr. et al.），NDSS’97 Things That Go Bump In The Net，23 件

悪意を持つ Java アプレットからインターネット上のサイトを保護する問題について述べており，ファイアウォールに対する新しい攻撃として Java アプレットをあげている．またファイアウォールを抜けた Java アプレットをブロックするためのプロキシアプリケーションの実装を行っている．

“Reducing the Cost of Security in Link-State Routing”（Ralf Hauser et al.），NDSS’97 Routing Security，25 件

Link State ルーティングプロトコルにおける 2 つのアップデート技術 SLS(Stable Link State) と FLS(Fluctuating Link State) を提案している．また安全性と効率性について理論的な評価を行っている．

“The Secure Remote Password Protocol”（Thomas Wu），NDSS’98 Protocols，40 件

新しいパスワード認証および信頼されていないネットワーク上のユーザ認証と鍵交換に適した鍵認証プロトコル AKE(Asymmetric Key Exchange) を提案している．また AKE を利用した SRP(Secure Remote Password) プロトコルを提案し実装評価を行っている．SRP は非対称暗号を利用する検証ベースのゼロ知識プロトコルであり辞書攻撃に耐性をもつ．

“A First Step Towards Automated Detection of Buffer Overrun Vulnerabilities”（David Wagner et al.），NDSS’00 Software Assurance，25 件

セキュリティが重要な C 言語のコードに潜むバッファオーバラン脆弱性の静的解析ツールを提案し実装評価を行っている．文字列を抽象的なデータタイプとして扱うことと整数の範囲を追跡することによって検出精度を向上している．

“Efficient and Secure Source Authentication for Multicast”（Adrian Perrig et al.），NDSS’01 Security Protocols，21 件

送信者と受信者が緩く同期しているという仮定の下で，対象鍵によるパケット認証を行う TESLA プロトコルの拡張を行っている．従来の TESLA ではパケットはバッファされるためその認証は遅れていたが，パケットの到着と受信者による認証を同時に行えるようにしている．また，サービス否認攻撃へより耐性を持たせるためにメモリ空間のオーバヘッドを削減している．

“An Algebraic Approach to IP Traceback”（Drew Dean et al.），NDSS’01 Packet Flows，24 件

IP パケットにおける Traceback 問題を多項式復元問題として再構成し，代数符号化理論の技術を利用することで，雑音除去およびマルチパスの復元のための強健な方式を提案している．また実装におけるセキュリティと効率のトレードオフについても議論している．

表 2: 地域別発表論文数 (詳細)

地域	国	1996	1997	1998	1999	2000	2001	2002	2003	2004
北米	アメリカ合衆国	7	9	7	6	10	13	11	14	16
	カナダ	1		1	1			1		
欧州	スイス	1	1	1		2				
	イギリス	3	1	2						
	ベルギー		1							
	スペイン		1		1					
	ドイツ			1				1		
	スエーデン				1				1	
	ノルウェー				1					
	イタリア				1					
	フィンランド					1	1		1	
	ポルトガル						1			
	フランス							1	1	
アジア	日本	2								
	韓国						1			
中東	イスラエル					2				
オセアニア	オーストラリア							1		
計		14	13	12	11	15	16	15	17	16

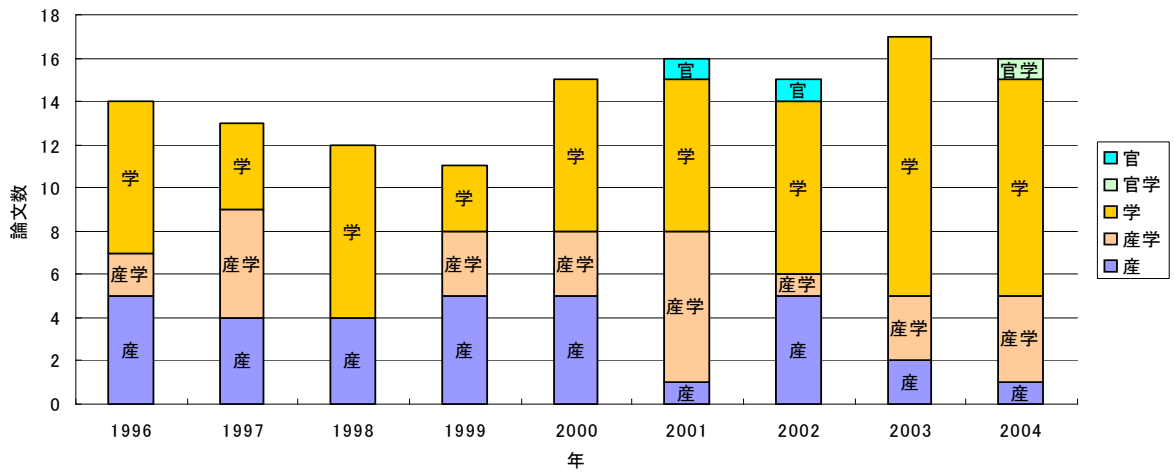

表 3: 所属別採録論文数

4.3 採録論文の地域・所属分類

1996 年から 2004 年にかけて開催された NDSS における採録論文を，その第一著者の所属地域 (北米・欧州・アジア・中東・オセアニア) に基づいて分類した (図 1)．過去から北米と欧州からの論文が多くを占めている．また，2004 年では全ての採録論文が北米からとなっている．表 2 に地域の詳細を示す．

また，採録論文をその著者の所属組織 (産・官・学) に基づいても分類した (図 3)．過去から産と学からの論文がほとんどであるが，近年では大学からの採録論文が増加している．

4.4 CSEC との関連

CSEC では暗号理論，セキュアプラットフォームやバイオメトリクス，IDS，マルチメディアセキュリティなど幅広いコンピュータセキュリティ分野が取り組まれている．NDSS は，この分野のなかでも特に，Web アプリケーションのセキュリティやネットワークプロトコルにおけるセキュリティのようにネットワークセキュリティに特化した学会である．NDSS'04 における論文採録率 16.3 %からも分かるように発表論文の質は高く，CSEC 研究会参加者にとっても，有益な論文が数多くあると思われる．

5 おわりに

以上，The 11th Annual Network and Distributed System Security Symposium (NDSS'04) の開催概要の報告および NDSS における研究動向の調査結果の報告を行った．なお NDSS'97-'03 の論文の詳細については ISOC の Web [3] から参照できるため，そちらも参考にして頂きたい．NDSS04 の論文は現在 (2004 年 4 月) 参照できないが，近いうちに参照できるようになると思われる．

参考文献

[1] NDSS'04, http://www.isoc.org/isoc/conferences/ndss/04/

[2] Internet Society, http://www.isoc.org/

[3] NDSS Conferences, http://www.isoc.org/isoc/conferences/ndss/

[4] CiteSeer.IST, http://citeseer.ist.psu.edu/