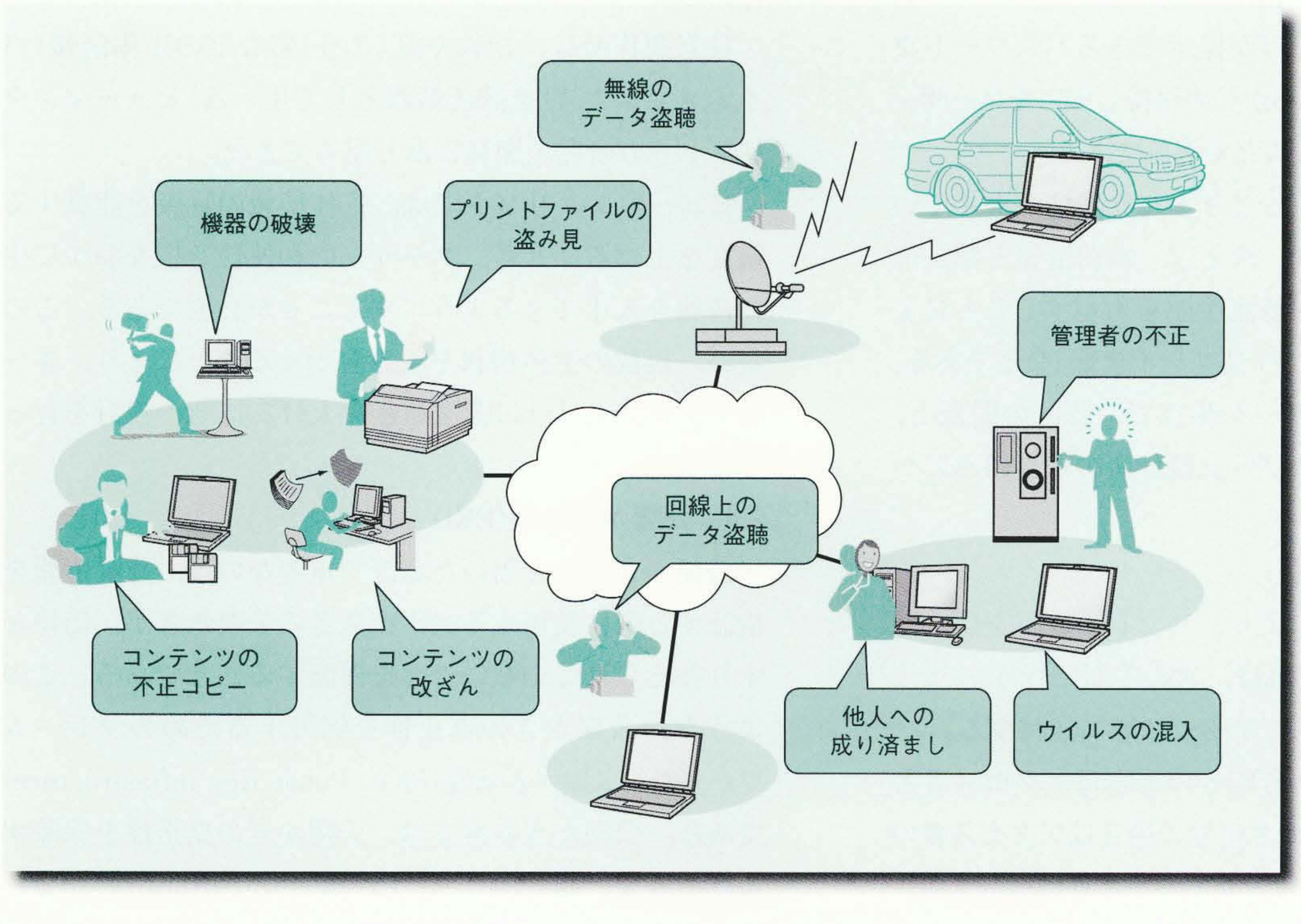
ブロードバンド時代のネットワークセキュリティ

Network Security for the Broadband Era

萱島　信　*Makoto Kayashima*　寺田真敏　*Masato Terada*
永井康彦　*Yasuhiko Nagai*



ブロードバンド時代のリスクとセキュリティ

ブロードバンドネットワークでは，マルチメディアコンテンツなど，資産価値の高い情報が扱われている。それらをねらったウイルスや攻撃用ツールがネットワークを介して即座に広まるため，セキュリティ上のリスクは増大している。

インターネットは，現在，組織の情報基盤として欠かせないものになっている。また，ADSLやケーブルテレビなど，ブロードバンドネットワークの基盤や，マルチメディアアプリケーションもしだいに整いつつあり，そこでは重要なサービスが展開されてきている。

しかし，その一方で，ウイルスや攻撃用ツールを用いた不正アクセスが世界中で急増していることも事実である。ブロードバンドネットワークを安全に維持管理するためには，正しい知識に基づいた情報セキュリティが重要になってきている。

セキュリティの維持管理を行ううえで重要な基盤となるのが，「セキュリティ3A」と呼ばれる技術である。セキュリティ3Aとは，Authentication(認証)，Authorization(権限付与)，Administration(管理)の頭文字をとったものである。セキュリティ3Aを確立するためには，暗号や認証といった要素技術の開発から，製品やシステム構築に至るまで，幅広いセキュリティへの取り組みが必要となる。

日立製作所は，きたるべきブロードバンド時代に向けて，セキュリティ3Aに対するさまざまな取り組みを進めている。

1　はじめに

インターネットは今や，組織の情報基盤として欠かせなくなっている。また，ADSL(Asymmetric Digital Subscriber Line)やケーブルテレビなどのブロードバンドを提供する基盤や，動画，音声などのマルチメディアデータを処理するアプリケーション環境もしだいに整ってきており，このような環境の下でさまざまなサービスが実施されるようになってきている。

同時に，世界中でウイルスや攻撃用ツールを用いた不正アクセスが急増している。そのような中で，ブロードバンドネットワークを安心して維持，管理するためには，正しい知識に基づいた情報セキュリティの実践が必要である。

そのために注目されているのが，「セキュリティ3A」と呼ばれる技術である。3Aとは，Authentication(認証)，Authorization(権限付与)，およびAdministration(管理)のそれぞれの頭文字をとったものである。

ここでは，ブロードバンド時代においてセキュリティ3Aが果たす役割と，日立製作所の取り組みについて述べる。

2 ネットワークと認証

認証とは，人や物がまちがいなく本物であることを確認する技術である。人の認証は，認証者が，ユーザー名などの識別情報と，本人だけが提示できるパスワードなどの認証情報を受理し，あらかじめ保持していたユーザーの認証情報と突き合わせることで実施できる。

ネットワーク環境には，さまざまな危険性が潜んでいることはよく知られている。例えば，識別情報と認証情報を通信経路上で入手し，認証手順を再現することにより，アクセス者に成り済ます「リプレイ攻撃」などである。

ブロードバンドネットワーク時代での認証の問題と，その対抗技術の概略，および日立製作所の取り組みについて以下に述べる。

2.1 暗号技術を用いた認証

暗号技術を用いることにより，リプレイ攻撃を防ぐ認証を行うことができる。それは，次の手順で行う。

(1) 認証者が乱数を生成し，アクセス者に送付する。

(2) アクセス者は，共通かぎ暗号の場合はアクセス者と認証者の共通かぎで，公開かぎ暗号の場合はアクセス者の個人かぎで乱数をそれぞれ暗号化し，認証者に返送する。

(3) 認証者は暗号化された乱数を，共通かぎ暗号の場合は共通かぎを，公開かぎ暗号の場合はアクセス者の公開かぎを用いてそれぞれ復号化し，期待した乱数が得られた場合に，アクセス者を本人と認証する。

この方式では，認証者が送付する乱数で認証情報が毎回変わるので，リプレイ攻撃を防ぐことが可能になる。

共通かぎ暗号を用いた認証技術では，送付する情報のフォーマットがISO/IEC9798-2[1]として標準化されている。日立製作所は，ISO/IEC9798-2による認証機能を備えたVPN(Virtual Private Network)製品[2]を提供している。

2.2 コンテンツの認証

ブロードバンド時代の到来とともに，インターネットを介してさまざまなマルチメディアコンテンツが送受信されるようになりつつある。しかし，ディジタル化されたコンテンツは複製が容易なことから，コンテンツの素性や利用条件を確認(コンテンツ認証)し，正しく使用されていることを保証する技術が必要である。日立製作所は，静止画像や動画像で使う電子透かし技術を利用し，コンテンツ認証を可能にする技術の開発を行っている。

2.3 ヒューマンクリプト

インターネットを使用するユーザー層の広がりに伴い，セキュリティの意識が低いユーザーが，不注意に認証情報を漏えいさせてしまう事例が増えてきている。このような事態を防ぎ，アクセス者が簡単・安全に認証作業を行えるようにすることが求められている。

日立製作所は，指紋や虹(こう)彩などの生体情報(バイオメトリクス)を認証情報として用いる「ヒューマンクリプト」[3]の研究・開発に取り組んできた。

ヒューマンクリプトでは，生体情報の特徴を認識する精度を上げることと，ユーザーの利便性を損なわずに生体情報を入手できるようにすることが必要である。このため，複数の生体情報を組み合わせることにより，ユーザーフレンドリーに認証精度を上げる技術の検討を行っている。

2.4 公開かぎ基盤(PKI)

公開かぎ技術を用いた認証で重要なのは，認証情報を検証する際に使用するアクセス者の公開かぎが，偽物とすり替えられていないことを保証することである。このような，公開かぎの真正性を保障するためのフレームワークが，公開かぎ基盤(PKI：Public Key Infrastructure)である。公開かぎ基盤では，公開かぎの真正性を保障する証明書を，認証局(CA：Certificate Authority)が発行するようになっている。

電子政府のような大規模なシステムでは複数の認証局が設置されており，異なる認証局が証明書を発行したユーザーどうしで認証できるようにするため，認証局どうしが相互認証をする仕組みが必要となる。日立製作所は，このような大規模な公開かぎ基盤を実現するための研究・開発にも取り組んでいる。

3 権限付与

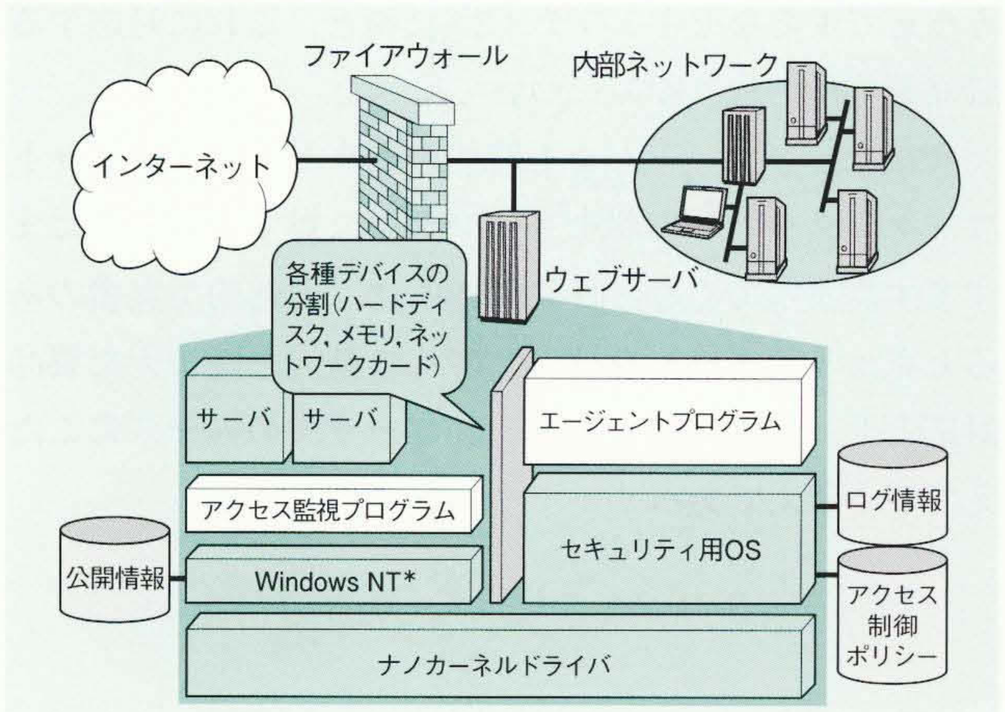
権限付与とは，ファイルシステムなどのリソースにアクセスできる範囲を，アクセス者に応じて制御する技術である。認証されたアクセス者は，与えられた実行権限内でリソースへの書込みや読取りをすることができる。

これは，リソースに付与されたアクセス許可に基づいて，アクセス者の権限に応じた操作をオペレーティングシステムで認可することによって実施される。

ネットワークでの権限付与における各種「攻撃」の脅威と，それらに対抗するための日立製作所の取り組みについて以下に述べる。

3.1 バッファオーバフロー攻撃とその対策

バッファオーバフロー攻撃とは，設計時に想定したバッファ長を超える入力データを外部から与えることにより，



注：略語説明ほか
OS(Operating System)
＊Windows NTは,米国およびその他の国における米国Microsoft Corp.の登録商標である。

図1　権限確認の強化
あらかじめ指定したプログラムでのアクセスや，指定された時間内だけのアクセスを認可するように，権限確認機能を強化する。

ソフトウェアの誤動作を引き起こすものである。例えば，ウェブサーバに入力バッファ長を超えたデータを送り込み，その中に「シェルコード」と呼ばれるプログラムを含ませると，ネットワーク上の攻撃者は，サーバにアカウントを持つユーザーの実行権限でリソースにアクセスできる。

バッファオーバフロー攻撃を回避するには，誤動作を起こさないソフトウェアを利用することが重要である。しかし，サードパーティのソフトウェアを含めて，すべてバッファオーバフローを起こさないソフトウェアだけでネットワークシステムを設計，開発することは困難である。

日立製作所は，誤動作を起こしたソフトウェアによる被害を最小限に抑えるため，アクセスの権限付与機能を強化するツール[4]の開発を行っている(**図1**参照)。

このツールでは，単にアクセス者を認可，拒否するだけでなく，予期しないプログラムからのアクセスを拒否する機能も提供している。

3.2　クロスサイトスクリプティング攻撃とその対策

クロスサイトスクリプティング攻撃[5]は2000年に入ってから見つかったものである。これは，ウェブサーバの掲示板に不正な処理を行うスクリプトを含むデータを書き込むことにより，そのウェブサーバにアクセスしたユーザーが使用しているブラウザに，想定外の動作を引き起こさせる攻撃である。この攻撃により，ネットワーク上の攻撃者は，ウェブサーバにアクセスしたユーザーのクライアントパソコンの内部情報にアクセスすることもできるようになる。

クロスサイトスクリプリティング攻撃を回避するには，次の二つの方法が考えられる。

(1) ウェブサーバからダウンロードしたスクリプトを，クライアントパソコン側でむやみに起動しない。

(2) 外部から送り込まれたデータを基にコンテンツを生成するウェブサーバでは，作成されたコンテンツが問題を起こさないことを確認する。

日立製作所は，クロスサイトスクリプティング攻撃などに対するセキュリティと，その対策に関する情報収集を行い，検査ツールを開発している。これらの情報やツールは，システム開発を行う技術者に提供され，最新のセキュリティ問題に対応する体制作りに役立っている。

4　セキュリティ管理

上述した認証や権限付与の技術は，ブロードバンド時代のネットワークのセキュリティを確保するうえで必須の基盤技術である。最近は，これらの基盤技術をシステムに組み込み，システム内で有効に活用されていることを保証する「セキュリティ管理技術」が脚光を浴びている。

セキュリティ管理の標準化動向と，日立製作所の取り組みについて以下に述べる。

4.1　ISO15408対応

ISO15408は，情報関連製品・システムの基本的なセキュリティ機能要件と，その機能品質の保証要件，および7段階の保証レベルを規定した国際評価基準である。ネットワークシステムを構築する際には，構成要素となる製品の開発はもちろんのこと，システム設計でもISO15408で規定される要件集から要件を選択し，セキュリティ基本仕様書(ST：Security Target)を作成することが必要である。

日立製作所は，このセキュリティ基本仕様書の作成作業を効率的に行い，作業内容の均一性や妥当性を保証するための「統合構築手順」を開発し，開発者・システム構築者用のマニュアルとして提供している[6]。この手順を利用することにより，セキュリティ分析・評価の専門家ではない一般の開発者やシステム構築者でも，セキュリティ基本仕様書を効率的に作成することができる。

4.2　ISO17799対応

セキュリティ管理の運用面での基準として，英国規格“BS7799”をベースとするISO17799が国際標準化されている。この規格では，「管理目的・管理策を明確に文書

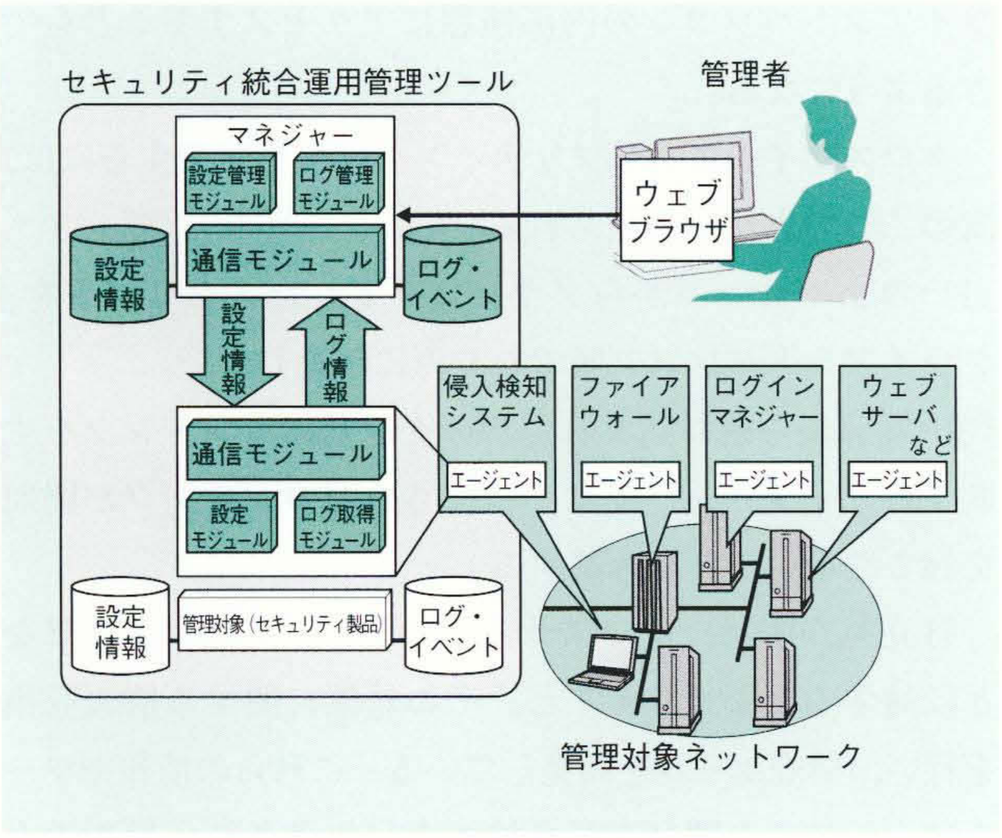


図2 セキュリティ統合運用管理機能の実現イメージ
各種セキュリティ機器の設定やログ・イベントの管理などを，抜けや漏れなく一括して実施する。

化することで管理枠組を確立し，選択された管理目的・管理策を実行する」ために，ISMS(情報セキュリティ管理システム)を確立することが求められている。

日立製作所は，この要求にこたえて，ユーザーサイトのセキュリティ運用管理を実現するコンサルテーションサービスを提供している。

4.3 セキュリティ統合運用管理ツール

ブロードバンド時代のネットワークシステムでは，ホストやコンテンツに認証や権限付与を行うため，さまざまなセキュリティ機器が利用される。これらの機器はISO15408に基づいたセキュリティ要件を満足するものであるが，これらの機器を適切に使用し，ISO17799に基づいたシステム運用管理を行うには，高度なスキルが要求される。

日立製作所は，各種のセキュリティ機器を効率的に利用できるようにするため，「セキュリティ統合運用管理機能」の研究・開発を進めている(**図2**参照)。セキュリティ機器には，ファイアウォールや侵入検知システムなど幾つかのカテゴリーがあり，さまざまなベンダーが独自に設定したGUI(Graphical User Interfase)やログ・セキュリティイベントの管理などを実現している。セキュリティ統合運用管理機能は，これらの管理を統合的に実施するためのフレームワークとして検討されているものである。

5 おわりに

ここでは，ネットワークセキュリティの維持管理を行ううえで重要なセキュリティ3A技術と，これに対応する日立製作所の取り組みについて述べた。

今後は，ブロードバンド時代の到来とともに，ネットワークシステムの情報セキュリティに対するニーズはますます高まってくる。日立製作所は，先進的で実績のあるセキュリティ技術を核に，時代の動向を踏まえた製品対応とサービス体制を確立し，ユーザーのニーズにこたえていく考えである。

参考文献など

1) ISO/IEC：Information Technology-Security Techniques-Entity Authentication Mechanisms-Part2：Mechanisms Using Symmetric Encipherment Algorithms, ISO/IEC9798-2
2) SecureSocket, http://www.hitachi.co.jp/Prod/comp/soft1/secsoc/
3) 瀬戸：ヒューマンクリプト認証技術の現状と今後の展開，月間バーコード，2001年3月増刊号
4) 佐々木，外：マルチOS環境を利用したアクセス制御システムの実装と性能評価，情報処理学会CSEC研究会予稿集(2001.7)
5) 高木，外：クロスサイトスクリプティング攻撃に対する電子商取引サイトの脆弱さの実態とその対策，情報処理学会CSEC研究会CSS2001シンポジウム予稿集(2001.10)
6) 永井，外：情報システムに対するセキュリティ国際評価基準の動向と日立製作所の対応，日立評論，**81**，6，433～438(1999.6)

執筆者紹介

萱島 信
1989年日立製作所入社，システム開発研究所 第7部 所属
現在，セキュリティ運用管理システム技術の研究・開発に従事
情報処理学会会員，電子情報通信学会会員，日本ソフトウェア科学会会員，人工知能学会会員
E-mail：kayashi @ sdl. hitachi. co. jp

永井康彦
1985年日立製作所入社，システム開発研究所 第7部 所属
現在，セキュリティシステム構築・評価技術の研究・開発に従事
電気学会会員，電子情報通信学会会員，日本航空宇宙学会会員
E-mail：y-nagai @ sdl. hitachi. co. jp

寺田真敏
1986年日立製作所入社，システム開発研究所 第7部 所属
現在，インターネット，ネットワークセキュリティ技術の研究・開発に従事
情報処理学会会員
E-mail：terada @ sdl. hitachi. co. jp