

セキュリティの最新トピックス

～ セキュリティ情報公開システムのご案内～

国立情報学研究所

セキュリティ情報公開システムとは

- ◆ セキュリティ情報公開システムとは、国立情報学研究所より、学術情報ネットワーク加入機関のネットワーク管理者及び、各機関所属の研究者・職員に向けての、セキュリティ情報の提供を行うシステムです。
- ◆ 本システムにより提供される情報を元に、学術情報ネットワーク加入機関におけるネットワークセキュリティの向上を図り、延いては学術情報ネットワーク全体のセキュリティレベルの向上を図っていくことを目指しています。
- ◆ 平成16年7月から、セキュリティ情報検索システムの運用を開始し、平成19年5月から、情報提供形態の変更に伴い、セキュリティ情報公開システムとなりました。

セキュリティ情報の内容

分類のカテゴリ	セキュリティホール、ウイルス、アドバイザリ、アプリケーション、バージョン、ニュース
総件数	5000件以上
アプリケーション(OSを含む。)数	440種以上
蓄積期間	1999年～
検索方法	キーワード、危険度、影響範囲、期間

- ◆ セキュリティ情報公開システムは、「学術情報ネットワーク 利用者ポータル」から利用することができます。
- ◆ ポータル利用時に、利用者の認証を行います。
- ◆ 学術情報ネットワークで新たに提供するサービスの利用時に利用者認証を実施します。学術情報ネットワークを利用されている機関のネットワーク管理者及び各機関所属の研究者・職員にサービス利用用のID及びパスワードを申請に基づき随時発行します。ただし、これまでのネットワーク接続(LANの接続)の利用については、変更ありません。

ID発行の申請手続方法について

- ・ 管理者IDおよび利用サービスIDについて
http://www.sinet.ad.jp/document/form/id_guidance
- ・ 管理者ID・利用サービスIDに関するFAQ
<http://www.sinet.ad.jp/faq-ja/faq-11/>

◆ SINETトップページから、利用者ポータルのログイン画面へ移動することができます。

URL <http://www.sinet.ad.jp>



TOP - SINET3 (学術情報ネットワーク) - Windows Internet Explorer

http://www.sinet.ad.jp/

TOP - SINET3 (学術情報ネットワーク)

サイトマップ | お問い合わせ English ログイン

サイト内を検索する 検索

トップページ

- ▶ 学術情報ネットワークとは
- ▶ 提供サービス
- ▶ 申請手続き
- ▶ 各種資料・申請書
- ▶ お知らせ
- ▶ FAQ
- ▶ 関連リンク

Science Information NETwork 3
SINET3 ~学術情報ネットワークの新展開~

SINET3では、従来に比べ格段に豊富なネットワークサービスを利用可能とし、最先端のネットワークアーキテクチャ(光IPハイブリッドアーキテクチャ)を採用しています。

セキュリティ情報公開システム

学術情報ネットワークは、日本全国の大学、研究機関等の学術情報基盤として構築、運用されている情報ネットワークです。
教育・研究に携わる数多くの人々のコミュニティ形成を支援し、多岐にわたる学術情報の促進を図るため、全国にノード(ネットワークの接続拠点)を設置し、大学、研究機関等に対して先進的なネットワークを提供しています。ま

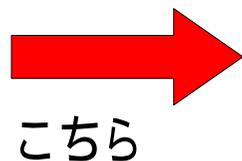
実行しましたが、ページでエラーが発生しました。

インターネット 100%

こちら

◆ ログイン画面で、利用方法 で取得したIDを利用して認証を行います。

URL <https://members.sinet.ad.jp>



学術情報ネットワーク 利用者認証

学術情報ネットワーク 利用者認証

学術情報ネットワークで新たに提供するサービスの利用時に利用者認証を実施します。学術情報ネットワークを利用されている機関のネットワーク管理者及び各機関所属の研究者・職員にサービス利用用のID及びパスワードを申請に基づき随時発行します。ただし、これまでのネットワーク接続(LANの接続)の利用については、変更ありません。

なお、ID発行の申請手続方法については、次をご参照ください。

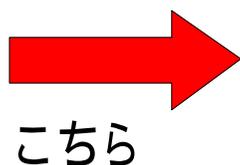
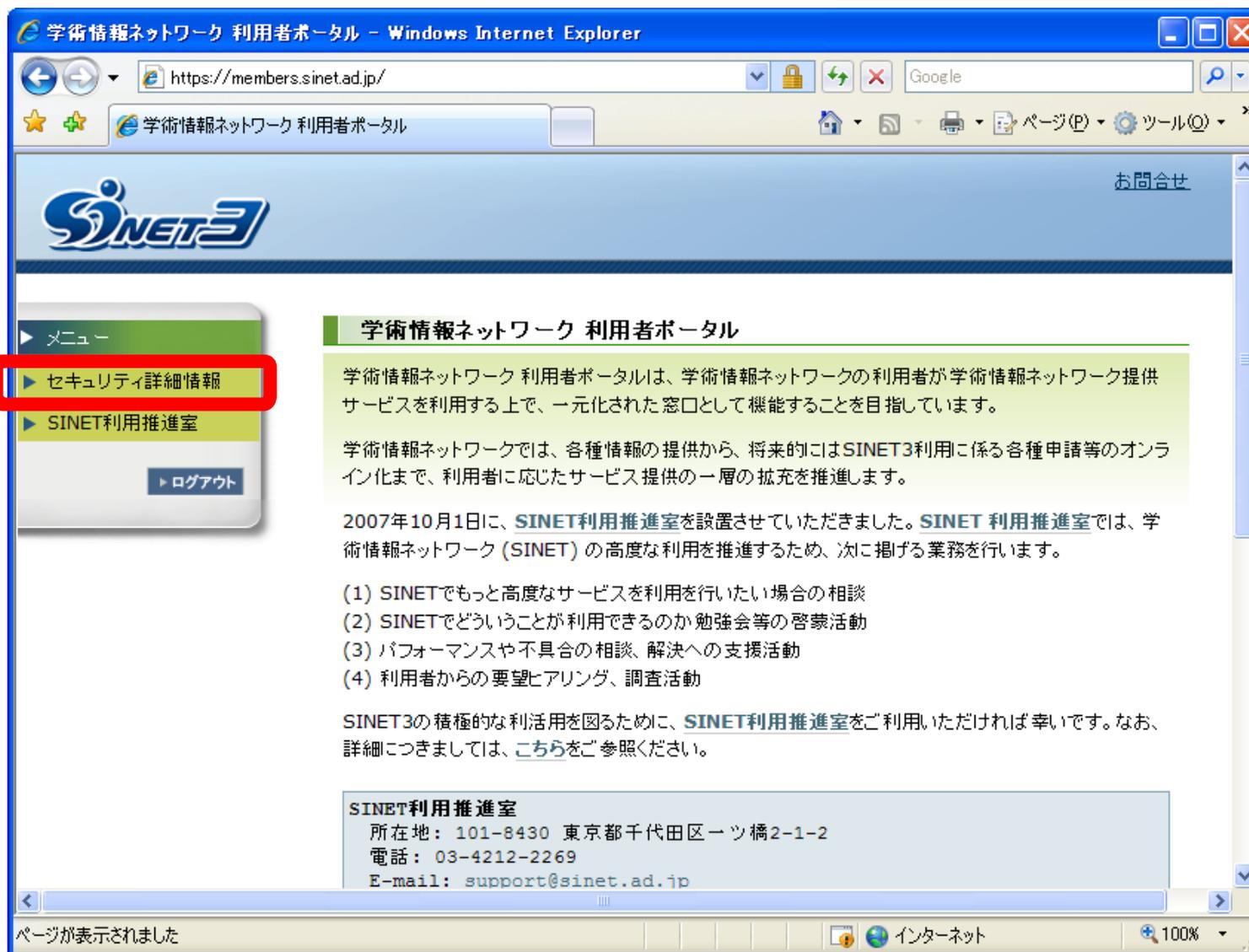
- [管理者IDおよび利用サービスIDについて](#)
- [管理者ID・利用サービスIDに関するFAQ](#)

国立情報学研究所(NII) | 学術情報ネットワーク(SINET) | [リンク及び著作権について](#)
Copyright © 2007 National Institute of Informatics. All Rights Reserved.

◆ ポータルメニューから、セキュリティ詳細情報を選択します。

URL <https://members.sinet.ad.jp>

こちら

学術情報ネットワーク 利用者ポータル

メニュー

- ▶ **セキュリティ詳細情報**
- ▶ SINET利用推進室

ログアウト

学術情報ネットワーク 利用者ポータル

学術情報ネットワーク 利用者ポータルは、学術情報ネットワークの利用者が学術情報ネットワーク提供サービスを利用する上で、一元化された窓口として機能することを目指しています。

学術情報ネットワークでは、各種情報の提供から、将来的にはSINET3利用に係る各種申請等のオンライン化まで、利用者に応じたサービス提供の一層の拡充を推進します。

2007年10月1日に、**SINET利用推進室**を設置させていただきました。**SINET 利用推進室**では、学術情報ネットワーク (SINET) の高度な利用を推進するため、次に掲げる業務を行います。

- (1) SINETでもっと高度なサービスを利用を行いたい場合の相談
- (2) SINETでということが利用できるのか勉強会等の啓蒙活動
- (3) パフォーマンスや不具合の相談、解決への支援活動
- (4) 利用者からの要望ヒアリング、調査活動

SINET3の積極的な利活用を図るために、**SINET利用推進室**をご利用いただければ幸いです。なお、詳細につきましては、[こちら](#)をご参照ください。

SINET利用推進室
 所在地： 101-8430 東京都千代田区一ツ橋2-1-2
 電話： 03-4212-2269
 E-mail: support@sinet.ad.jp

◆ 次のような画面から、セキュリティ情報をご利用いただけます。

URL <https://members.sinet.ad.jp>



更新: 2007/11/22 (Thu) 11:38

ホーム セキュリティホール ウィルス アドバイザリ アプリケーション バージョン ニュース

サービス総合案内 | レポート | 緊急速報履歴 | お知らせ | FAQ | お申込み/お問合せ | 情報の取扱いについて

24時間以内に登録・更新された情報は**New!!**マークがつかます

What's New

2007/11/12
2007年10月の SIDfm Security Monthly Reportを公開しました。

「月例のMicrosoftのセキュリティ情報は、Internet Explorer, Word, Outlook Express, Kodak Image Viewer...」[\(つづきを読む\[PDF\]\)](#)

2007/10/5
2007年9月の SIDfm Security Monthly Reportを公開しました。

「9月19日に、US-CERT から発表された Apple Quicktime の脆弱性は、ユーザが細工されたファイルを再生した...」[\(つづきを読む\[PDF\]\)](#)

2007/9/15
SIDfm ASP バージョンアップのお知らせ(2007年9月15日)

アラートメールの機能アップと...

SIDfm Ticker 最新セキュリティホール情報

BIND 8 の クエリ ID に DNS キャッシュを汚染
あなたのWebページにもSIDfm Tickerを設置できます。

◆ 最新セキュリティホール情報 [最新セキュリティホール情報一覧](#)

日々、SIDfm データベースに登録されるまたは更新されるセキュリティホール情報のうち、最新3件を表示しています。すべての最新セキュリティホール情報は、「セキュリティホール情報」よりご覧頂けます。また、登録・更新されたセキュリティホール情報は、日ごとに「SIDfm Daily Mail」で受け取ることができます。最新のセキュリティホール情報をいち早く入手し、セキュリティ対策にお役立てください。

Severity	Date/Time	Category	Title
High!!	2007/11/22 11:38 新着	teTeX	リモート teTeX の dvips 等に任意のコードを実行される複数の問題
Medium!	2007/11/22 10:58 更新	Samba	リモート Samba の reply_netbios_packet 関数などに任意のコードを実行される複数の問題

teTeX は、処理の実装が原因で複数のセキュリティホールが存在します。攻撃者にこれらのセキュリティホールを利用された場合、任意のコードを実行されたり、情報が漏洩する可能性があります。

Samba は、reply_netbios_packet 関数などの実装が原因で複数のセキュリティホールが存在します。攻撃者にこれらのセキュリティホールを利用された場合、リモートから任意のコードを実行される可能性があります。

[関連ニュース](#)

システム利用の利点

- ◆ セキュリティ情報の提供は、国立情報学研究所とセキュリティ情報提供者とのサイトライセンス契約の締結に基づくもので、システム利用者は、有償のセキュリティ情報を無償でご利用いただくことができます。

- ◆ システムの次の特長から、セキュリティ情報収集のコスト削減が期待されます。
 1. 世界中に点在する情報源から、信頼に値する情報を抽出
 2. 日本語による情報提供
 3. 専門用語が多くなりがちな技術情報を平易に解説
 4. 多様な情報の蓄積
 5. 検索機能の充実

◆掲載情報の扱い

本システムで検索・表示されたセキュリティ情報は、学術情報ネットワーク加入機関のネットワーク管理者及び、各機関所属の研究者・職員内での閲覧を原則とし、再配布を目的とした他のメディアへの転載等は禁止とさせていただきます。

◆禁止事項

セキュリティ情報公開システムの利用は、学術情報ネットワーク加入機関に所属する方に限定させていただきます。

◆免責事項

NIIIは、本セキュリティ情報公開システムの利用者が本システムによって得られる情報を用い招いた如何なる損害に対しても、一切の責任を負わないものとします。