ISSN 0917-3668
2001. 11. 20

KUINSニュース

No. 36

京都大学学術情報ネットワーク機構
http://www.kuins.kyoto-u.ac.jp/

安全なギガビットネットワークシステム (KUINS-III) 導入機器 (大型計算機センター)

目　　次

KUINS-III の運用について

学術情報ネットワーク機構事務室

KUINS の新しいキャンパスネットワーク「安全なギガビットネットワークシステム (KUINS-III)」の機器が平成 13 年 10 月末に納入されました.

現在，平成 14 年 1 月からの試験運用に向けての準備作業中です．本運用は平成 14 年 4 月からの予定ですので，もうしばらくお待たせすることになり申し訳ありませんが，ご理解のほどをよろしくお願いします.

スーパー SINET 運用開始について

学術情報ネットワーク機構事務室

国立情報学研究所が新しく構築するネットワーク「スーパー SINET」(基幹部分：10Gbps) が，平成 14 年 1 月から運用開始となります。スーパー SINET は主に研究プロジェクト等に利用されますが，京都大学のキャンパス LAN(KUINS) と 1Gbps(Gigabit Ether) の回線で接続予定となっております.

WCN 線を増速

KUINS ニュース No.26，No.32 でお知らせしましたように，KUINS は商用インターネットサービスプロバイダ WCN (World Computer Network) への対外接続線 (専用線 4.5Mbps) を持っていますが，その回線速度が 11 月より 6Mbps に増速されました．なお，これまで WCN として OMP から提供されていたこのサービスは，10 月の会社再編に伴い，パワードコム (PNJ コミュニケーションズ) によるサービスとなっています.

KUINS ターミナルサーバ用電話回線廃止のお知らせ

学術情報ネットワーク機構

KUINS ネットワーク接続用にサービスしていました KUINS ターミナルサーバ用電話回線ですが，セキュリティ面の問題から，平成 13 年 9 月末日を持って廃止いたしました．長い間，ご利用いただきありがとうございました.

スパムメール不正中継対策フィルタの実施のお知らせ

学術情報ネットワーク機構

前号の KUINS ニュースでお願いしましたスパムメール不正中継対策の徹底に関して，スパムメール不正中継対策済みの届け出がないサブネットについては 2001 年 9 月末をもって **SMTP(25/TCP)** を遮断することをお知らせしていましたが，未だに**約 50** のサブネットからの対策済みの届け出がないため，実施しておりません.

現状を放置すると，学内からのスパムメール不正中継が大量発生する恐れがあるため，**2001 年 11 月末**をもって，全てのサブネットに SPAM メール不正中継対策のフィルタ設定を行います. このフィルタ設定の内容は，すでに届出のあった SPAM メール不正中継対策済みメールサーバ (SMS) 以外への学外からの **SMTP(25/TCP)** を遮断します。なお，届出済みの SMS に対しては，学外からのメールも従来通り着信します.

この件に関する連絡先は次の通りです.

学術情報ネットワーク機構情報システム管理掛 ((075)753-7841)
(大型計算機センター等ネットワーク掛 ((075)753-7432)
spamfilt@kuins.kyoto-u.ac.jp

KUINS-II の Web サーバ届出のお願い

学術情報ネットワーク機構

本年の春以降，Code Red, Code Red II, Nimda などのワーム，ウィルスが大流行しました．KUINS 機構にも，学内の計算機にもいくつか感染の被害が発生したとの報告が寄せられております．幸いにも現在では学内での感染は生じていないようですが，ウィルスに冒された学外の計算機からの攻撃は，いまだ継続的に観測されております.

これらのワームは，特定の Web サーバソフトウェアのセキュリティホールを狙って攻撃を行いますが，KUINS-II では学内外間の **HTTP (80/TCP)** 通信に対して何ら制限を設けていないため，KUINS-II に Web サーバを立ち上げると同時にこれらの攻撃に曝されることになります.

実際，一連の Code Red (I, II) や，Nimda の被害に遭った学内の計算機のうちで，管理者が無意識のうちに Web サーバソフトウェアが起動されており，それがもとで感染に至ったケースがかなりの部分あります.

このように半ば無意識のうちに感染した計算機が学内外に攻撃を開始するケースでは，そもそもサーバとして利用する意図がないため接続届が提出されていない，あるいは計算機管理者にサーバを動作させているという意識がないなどの理由で，該当する計算機の調査と原因究明に非常に多大な時間と労力が費やされました.

そこで，KUINS では，KUINS-III の運用開始と同時に，KUINS-II に接続し学外へ情報発信を行う Web サーバをあらかじめ届出ていただくという，Web サーバ登録制の運用を開始いたします.

登録制のポイントは次の通りです.

- **HTTP (80/TCP)** サービスを学外に開放している計算機の IP アドレス，サーバソフトウェア名，管理者名などの情報を KUINS にお知らせいただきます.
- 登録された Web サーバ以外が感染し，学内外への攻撃が観測される，あるいは外部から攻撃の苦情が寄せられることがあれば，当該計算機への HTTP 接続を各サブネットのルータで遮断したうえで，サブネット管理者に調査依頼を行います.
- 登録された Web サーバが感染した場合には，当該管理者に直接通知した上で，管理者からの要望があれば通信遮断を行います.
- さらにご希望がある場合には，登録された Web サーバ以外への HTTP 通信をサブネットのルータにおいて遮断します.

届出については，2001 年 11 月現在行っております KUINS-II に関する調査に対し，該当する計算機を「Web サーバとして利用」と回答していただければ，KUINS-II 上の Web サーバとして登録いたします．また，電子メールを用いた登録申請窓口も今後整備し，ご案内する予定です.

皆様のご理解とご協力をお願いします.

KUINS 接続状況

学術情報ネットワーク機構

平成 13 年 11 月 1 日現在の，KUINS-II/ATM への端末の接続状況をお知らせします.

吉田地区	13231(358) 端末
宇治地区	2009 (53) 端末
遠隔地 (全て)	821 (11) 端末
(合計)	16061 (422) 端末

( ) 内が IP over ATM での接続数です。

接続申請や申請様式の取得については，以下の URL をご参照下さい.

`http://www.kuins.kyoto-u.ac.jp/applications/`

KUINS-II 接続機器の管理体制について

学術情報ネットワーク機構

最近，本学で実際に発生した事例ですが，

> **「130.54.x.x の計算機を使った者が，Web 掲示板にある人の個人情報を暴露し，中傷する内容を掲載した．警察への被害届は提出済みで，さらなる法的手段も検討中なので，実行者を特定して欲しい.」**

との問い合せが被害者の代理人から本学にありました[1]．これに対して，該当する講座の教官が

> **「大変ご迷惑をおかけしました．ただ，本当に申し訳ないのですが，この IP アドレスは DHCP によって発行しており，今回の行為に使用された計算機が分からないため，実行者の特定は困難です.」**

と回答しました.

これを読んで，**「DHCP じゃ仕方ないよな」と思われた方**，面倒だとは思いますが，以下の記事をじっくりと読んでください．今後，不正アクセス防止法に加え，ネットワークおよびその上での情報交換に関する数々の法律が施行されていきます．KUINS に接続される情報機器および部局で設置されたネットワークの管理責任はそれぞれの管理責任者にあり，「専門家じゃないから知らなかった」では免罪されない状況となりつつあります．また，「単語の意味が全く分からない」と言う方は，デジタル用語辞典 (http://yougo.ascii24.com/) 等を参照しながら読んでください．**「今どきそんな言訳をしたら，恥をかくよな」と思われた方**，別の記事を先に読まれて，暇なときにざーっと斜め読みして頂いて結構 … かも知れません.

(DHCP)

さて，先程の回答のどこが恥をかくかと言うことですが，

- 登録済みの MAC アドレスに対してのみ IP アドレスを発行する DHCP サーバプログラム[2]
- IP アドレスの不正利用を検出するプログラム

が無償で公開され，その使用が常識となりつつある時代に，最先端の研究をしている大学が時代遅れの手法でネットワークを運用していると明言していることです．最近では，インターネットに直結する計算機については，MAC アドレスと IP アドレスは 1 対 1 に対応するか，DHCP の場合は発行状況を把握することで，不正アクセスが発生した場合，その行為者を特

[1] 現在，KUINS 機構には，被害者本人だけでなく，警察，弁護士などから，このような問い合せが月に 1 回程度寄せられております.

[2] MAC(Media Access Control) アドレスとは自動車で言えば車台番号のことで，Ethenet カードごとに世界で唯一の番号が与えられています．IP アドレスはナンバープレートに該当すると考えてください.

定できることが求められます．これらを実現するものとしては，

Internet Software Consortium の DHCP (`http://www.isc.org/`)

Lawrence Berkeley National Laboratory の arpwatch (`http://ee.lbl.gov/`)

等があります．ソースプログラムは上記の Web サイトを参照し，また，OS 毎のバイナリパッケージは検索エンジン等で探してください．

(NAT 装置)

また，NAT 装置も徐々にですが，そのままでは使えない時代になってきています．NAT は装置の内側の IP アドレス (通常は private IP アドレス) を本学の IP アドレスに変換することで，枯渇状態にある global IP アドレスを有効利用できる便利なものですが，一般的な NAT 装置では「何時，どの private IP アドレスを，どの global IP アドレスに変換し (または，どのポート番号を割り当て)，どこの IP アドレスに接続した」といった記録はできません．そうすると，DHCP と同様に NAT 装置を介して法に触れる行為があった場合，実行者が特定できないことになります．

このため，変換記録を取得できる NAT 装置[3]を導入されるか，application proxy(application gateway) によって，どの private IP アドレスがどこにアクセスしていたかを把握することが常識になりつつあります．例えば，Web proxy や Symantec Enterprise Firewall も application proxy の一種です．

また，NAT 装置を firewall として利用されている場合は，firewall としての利用に耐える仕様になっているかを確認してください．例えば，一部の NAT では，private IP アドレス側で最初に Web にアクセスした計算機に対して，外部から Web アクセスが可能なように作られていて，不正アクセスにさらされるものがあります．

(無線 LAN)

さらに今回は，無線 LAN 基地局についても調査いたします．無線 LAN は非常に便利なものですが，現在一般に普及している規格 (IEEE802.11b) では，WEP による暗号化やクローズドネットワークによる無線 LAN の存在遮蔽機能を用いても，その存在を暴いて暗号を解読することは極めて簡単に行うことができます．このため，個人情報やプライバシー情報を扱うネットワークでは無線 LAN の使用を控えてください．また，一般用途で使用される場合も，private IP アドレスを使用し，先に延べた不正アクセス防止策を講じた NAT と併用してください．

また最近の無線 LAN の普及にともない，顕在化しつつある問題として，チャンネル割当て混乱があり，本学でも無線 LAN の混信が多発する傾向にあります．無線 LAN のチャンネルは 1〜14ch で，それぞれを自由に使えるとの誤解があるようですが，実は表 1 のように周波数帯域が重なるように割り当てられています．例えば，1ch と 2ch を使用する基地局が隣接して設置されている場合，混信等の障害を起こします．

[3] ざっと調査したかぎりでは， 実用に耐えてそのような機能を持つ NAT 装置は現時点ではなさそうです．

表 1: 無線 LAN チャンネルと周波数割り当て

チャンネル	中心周波数 (GHz)	占有周波数帯域 (GHz)	可能な組み合わせ
1ch	2.412	2.401〜2.423	○
2ch	2.417	2.406〜2.428	△
3ch	2.422	2.411〜2.433	□
4ch	2.427	2.416〜2.438	☆
5ch	2.432	2.421〜2.443	◎
6ch	2.437	2.426〜2.448	○
7ch	2.442	2.431〜2.453	△
8ch	2.447	2.436〜2.458	□
9ch	2.452	2.441〜2.463	☆
10ch	2.457	2.446〜2.468	◎
11ch	2.462	2.451〜2.473	○
12ch	2.467	2.456〜2.478	△
13ch	2.472	2.461〜2.483	□
14ch	2.484	2.473〜2.495	-

厳密に言えば，基地局のカバーエリアが重なる場合,「可能な組み合わせ」で同じ記号になっている 3 チャンネルしか利用できないことになります[4]．ただし，14ch だけは他のチャンネルと若干ずれた周波数が割り当てられていますので，○のグループとしても，12 または 13ch の代わりに使用することもでます.

このほかに，この周波数帯域は Bluetooth，電子レンジ，医療機器等が使用するため，その影響も大きく受けます．さらに，柱のそばに基地局を設置したため，建物の鉄筋が外部アンテナとして機能してしまい，離れた階にまで無線 LAN が届いて通信障害が発生した事例もあります．KUINS 機構では，今回の調査を元に無線 LAN のチャンネル割当てを調整することはありませんが，混信が発生した際に，原因究明の資料として使用させていただきます.

(モデム・ISDN/TA 装置，学外接続ルータ)

モデム・ISDN/TA 装置，学外接続ルータの調査が必要な理由は次の通りです．最近，発信元が 130.54.x.x であるパケットが学外から学内へ流入しようとする事象が発生しております．IP アドレスの偽造も考えられるのですが，パケットの挙動から推測して，これらの機器が本来流してはならない本学へのルーティング情報等を漏らしている可能性が高いと考えています．このためルータ等に利用している IP アドレスを把握させていただきます．また，これらの機器で直接，学外と通信されると，不正アクセスを受けた場合でも KUINS 機構による保護や対策は行なえません．これらの機器に関わる不正アクセスは設置者の責任で対処してください.

[4]実際には，占有周波数帯域の端の方は互いに重なっても影響は小さいため，1ch と 5ch を併用することも可能なものもあります.

以上に列挙した機器で，十分な不正アクセス防止策が取られていないものについては，近い将来 KUINS-II および III への接続を禁止する予定です．これらの機器の他に，来年度以降も KUINS-II に存続する情報機器については，MAC アドレスに基づく乗取り防止策を施す予定ですので，必ず提出してください．現在のところ，これらの対策は平成 15 年 4 月 1 日の実施を予定しておりますが，不正アクセスや IP アドレスの乗取りが急増するなど情勢の急変により，前倒しで実施することもあり得ますので，皆様のご理解とご協力をお願いします．

KUINS-III の利用について

学術情報ネットワーク機構

ここでは，KUINS-III を利用するにあたって，どのような機器が必要になるかについて解説します．

まずは一般的な使い方をされる場合に必要となる物は，

- 10Base-T または 100Base-T イーサネットのインタフェースを持つ計算機 (1 台だけを情報コンセントに接続する場合)
- 10Base-T または 100Base-T イーサネットのインタフェースを持つハブやスイッチ (複数の計算機やプリンタを情報コンセントに接続する場合)

最近のデスクトップパソコンや A4 サイズノートパソコンでは，100Base-T イーサネットインタフェースは標準装備されているものが多くなりました．搭載されていない場合でも，数千〜1 万円程度でイーサネットインタフェースボード (カード) が入手できます．また，イーサネットハブも数千円から製品があります．

これらの機器を使用する際に必要となる各種サーバ (DHCP，DNS，Web や ftp のための proxy サーバ) は KUINS 機構で設置致しますので，部局のみなさまが用意する必要はありません．ただし，KUINS 機構ではメールサーバは用意しませんので，部局や総合情報メディアセンターなどのメールサーバを利用してください．なお具体的な設定方法については，次号以降の KUINS ニュースで解説していきます．

講義室などのオープンスペースやアクセス制限を申請された部屋を除けば，KUINS-III から KUINS-II の計算機へのアクセスは今まで通り自由に行えます．一方，KUINS-III から利用可能な学外のネットワークサービスは Web と ftp のみです．このため，これ以外のアプリケーションを使用する場合は，部局で KUINS-II と KUINS-III の間に何らかの変換装置を設置していただく必要があります．ただし，今号の「KUINS-II 接続機器の管理体制について」の解説にあるように，この機器は KUINS-II にも接続することになるため，万全のセキュリティ対策が施されなければなりません．以下に揚げる例は，それぞれ数十万円〜数百万円の

導入費用と，これを維持管理する人件費と保守費が必要となります．単なるルータや安価な NAT 装置を設置されますと，KUINS-III 全体のセキュリティを脅かすだけでなく，不法行為があった場合の責任が VLAN 管理責任者と当該機器の管理責任者に及びますので，これらの機器を設置される前に KUINS 機構にご相談下さい．

KUINS-II - KUINS-III 間に部局でアプリケーション proxy を設置

一般的な通信は KUINS-III のルータを経由し，特定のアプリケーションのみ KUINS-II を経由する必要がある場合は，KUINS-II と KUINS-III の間にアプリケーション proxy(アプリケーションゲートウェイ) を設置し，KUINS-III から学外に対するアクセスを中継させてください．ただし，アプリケーション proxy は「何時，どの KUINS-III 側の IP アドレスがどこにアクセスした」という記録を保持できるものに限ります．

このような機能を持つものとしては，Web proxy の他に，Microsoft の Internet Security and Acceleration (ISA) Server や Symantec の Enterprise Firewall があります．また，**ルーティングを行なわない**ように設定した計算機を KUINS-II と KUINS-III の両方に接続し，この計算機にログインして，学外・KUINS-II と KUINS-III の相互乗り入れをするものも一種のアプリケーション proxy です．

KUINS-III をレイヤー 2(VLAN) としてのみ使用

アプリケーション proxy で対応できない場合，KUINS-III の回線と VLAN だけを利用し，KUINS-II や学外とのルーティングは部局の責任で行うことも可能です．この場合は，当該 VLAN で KUINS-III と異なる private IP アドレスを使用し，KUINS-II と KUINS-III の間に NAT/IP masquarade 装置を設置してください．当該 VLAN の IP アドレスは部局で管理して頂き，KUINS-III の DHCP サービスを停止する必要がありますので，事前に KUINS 機構に相談してください．

また，NAT/IP masquarade 装置は MAC アドレスと IP アドレスの対応状況の管理，および,「何時，どの private IP アドレスがどこにアクセスした」という記録を装置単体で保持できるか，保持できる仕組みが構築されているものに限ります．

不正アクセスがあれば，当該 VLAN の管理責任者に全ての対応 (調査や関係者との対応) をお願いすることになりますが，NAT/IP masquarade では，不正アクセス実行者の特定が極めて困難ですので，この手法はあまり推奨できません．

オープンスペースから KUINS-II のサーバを利用

オープンスペースから KUINS-II に設置した計算機を利用したい場合，KUINS-II に Microsoft の PPTP を稼働させたサーバを設置してください．PPTP は暗号通信により，レイヤー 2 としての Virtual Private Network (VPN) を実現します．PPTP により，オープンスペースの計算機を仮想的に PPTP サーバが設置されている LAN に接続することができます．例えば，オープンスペースから研究室のファイルサーバやプリンタを利用できます．

これを応用すれば，**ルーティングを行なわない**ように設定した計算機を KUINS-II と KUINS-III の両方に接続し，この上で PPTP を稼働させれば，異なる KUINS-III の VLAN 間でも VPN を構築することができます.

繰り返しになりますが，単に KUINS-II と KUINS-III の間をルーティングする装置の接続は禁止します．そのような装置を設置した KUINS-III VLAN は，他の KUINS-III セキュリティ維持のため，発見次第，事前警告無しに KUINS-III から切り離させていただきます.

なお，KUINS-III の DHCP サービスでは，IP アドレス発行の際に，当該 IP アドレスを使用した MAC アドレスを記録します．このため，何らかの不正アクセスが発生した場合，KUINS 機構は MAC アドレスによって VLAN 管理責任者に照会いたしますので，VLAN 管理責任者は MAC アドレスの管理を徹底していただくようお願いします.

コンピュータ不正アクセス対応連絡要領の改訂について

情報ネットワーク危機管理委員会

標記のことについて，平成 12 年 10 月 16 日付け経情処第 72 号「コンピュータシステムの不正アクセス等への対応について（通知）」でお知らせしました「コンピュータ不正アクセス対応連絡要領」を情報ネットワーク危機管理委員会において次のとおり改訂しましたので，今後はこの要領により対応の方よろしくお願いします.

記

コンピュータ不正アクセス対応連絡要領

(趣旨)

第 1　本学に設置されたコンピュータへの不正侵入（データ破壊，ホームページ改ざん，メール不正中継（スパムメール）等）やコンピュータウィルス等により，被害が発生（以下「不正アクセス」という。）した場合において，連絡体制を整備することにより被害拡大の防止を計る等必要な措置を講ずるために「不正アクセス対応連絡要領」（以下「要領」という。）を定めるものである。

(被害発生時の連絡)

第 2　不正アクセス（不正アクセスか否か判断できない場合も含む。）があった場合は，発見者は，被害の現況について第一報を情報ネットワーク危機管理委員会（以下「危機管理委員会」という。）及び当該部局連絡責任者に連絡するものとする。

2　発見者から前項の連絡のあった場合は，危機管理委員会は速やかに別紙 1「不正アクセス発生時連絡網」に基づき，対応するものとする。

(危機管理委員会の対応)

第 3　危機管理委員会は，学術情報ネットワーク機構の担当者を通じ，次の措置を行うものとする。

(1) 被害状況の通知

(2) 復旧等への指示，技術情報提供

(3) 防止策対応状況の通知

(各部局の対応)

(連絡責任者)

第 4　各部局は，不正アクセスがあった場合の連絡・周知が速やかに行える体制を講ずるものとし，併せて連絡責任者を置くものとする。

2 連絡責任者は，次の措置を行うものとする。

(1) 発見者からの被害状況の把握

(2) 部局長等への被害・復旧状況の報告

(3) 端末管理責任者 (KUINS-II) 又は VLAN 連絡担当者 (KUINS-III) への通知

3 連絡責任者は，特別の理由がないかぎり中央事務室の職員を選任して，官職，氏名，電話番号，メールアドレスを書面で危機管理委員会 (経理部情報処理課) へ通知する。
また，交替があった場合も同様とする。

(端末管理責任者 (KUINS-II) 又は VLAN 管理責任者，連絡担当者 (KUINS-III))

第 5　該当する計算機の端末管理責任者又は VLAN 管理責任者，連絡担当者は，計算機管理者と連携し，状況の把握，防止策対応，報告の措置を行うものとする。

(防止策対応済みの連絡)

第 6　部局長は不正アクセスに対する防止策対応等の措置がされた場合は，速やかに別紙 2「防止策対応済み報告連絡網」に基づき，別に指定する様式「不正アクセス報告書」(別紙 3) により危機管理委員会に報告するものとする。

(経理部情報処理課の対応)

第 7　経理部情報処理課は，危機管理委員会より通知された事項について，次の措置を行うものとする。

(1) 総長，事務局長等への報告

(2) 文部科学省への報告

(3) 情報処理振興事業協会への報告

(その他)

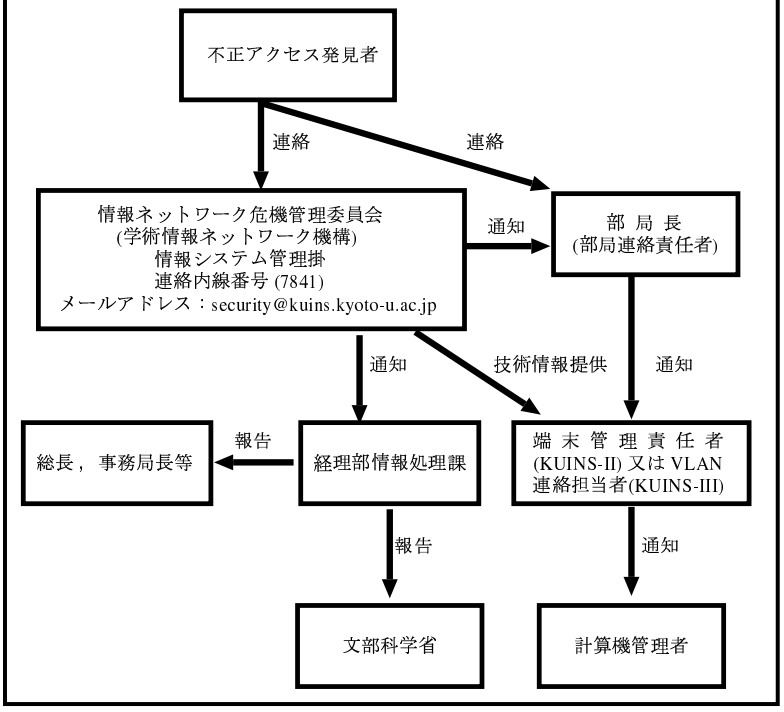
第 8　この要領に定めるもののほか，実施に関し必要な事項は，別に定める。

附　則

この要領は，平成 13 年 10 月 1 日から実施する。

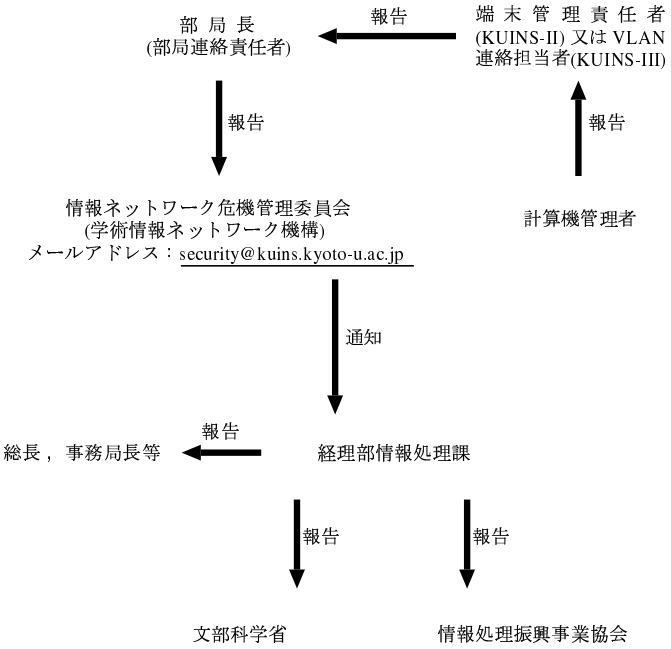
別紙 1

不正アクセス発生時連絡網



別紙 2

防止策対応済み報告連絡網



別紙 3

不正アクセス報告書

1. 報告年月日　　年　　月　　日
2. 被害を受けたシステム
   (機種)
   □ IBM PC(含む互換機、□ Mac、
   □その他 (機種名:　　)
   (OS)
   □ Windows-□ 3.1、□ 95、□ 98、□ ME、□ NT、□ 2000、□ XP □ Mac、□ Unix(名称・バージョン)
   □その他 ( )
   (利用目的)
   □ 学術研究、□事務、□情報公開 (Web 等)、□その他 (　　)

3. 発見年月日　　年　　月　　日
4. 発見の方法又は疑いを持った状況
   □ 自身で発見 (発見方法　　)
   □ 京都大学情報ネットワーク危機管理委員会より通知
   □ その他 (　　)

5. 侵入手口 (推定) □パスワード盗用
   □セキュリティホール悪用 (悪用されたソフト名・バージョン　　)
   □設定不備 (不備のあったソフト名・バージョン　　)
   □その他 (　　)

6 被害の状況被害を受けた期間　　年　　月　　日～　　年　　月　　日
   被害内容
   　□改竄・削除 (ファイル、Web コンテンツ)、□外部への不正アクセス
   　□その他 (　　)
   実施していたセキュリティ対策 (　　)
   直ちに講じた再発防止策
   　□パッチ・サービスパック適用
   　□その他 (　　)

A. 情報ネットワーク危機管理委員会からの通知日:
B. 防止策の措置日:
C. 端末の所属部局:
D: 端末管理責任者 (職名・氏名):
E: 計算機管理者 (職名・氏名):
F: 計算機名および IP アドレス:
G: 不正アクセス防止策の詳細:
□ パッチ・サービスパック適用 (パッチ・サービスパックの全てを以下に列挙してください。)
□ソフトウェア・プログラム設定変更 (設定変更を行なった場合は、対象となるソフトウエア・プログラムの名称、および、どのような設定作業を行なったかを以下に明記してください。)
□ソフトウェア・プログラム更新・削除 (改竄されたものを回復した場合も含む。ソフトウエア・プログラムの名称を以下に明記してください。)
□機器撤去 (永久使用しない場合のみ)
□その他 (以下に詳細を明記してください。)
(作業内容)
注意: 十分な防止策が確認できない場合、解除決定ができません。

提出先: security@kuins.kyoto-u.ac.jp または 075-753-7450 (FAX)

KUINS 会議日誌

平成 13 年 8 月 6 日～平成 13 年 11 月 19 日

KUINS ネットグループ連絡会議

平成 13 年 8 月 28 日（第 93 回）

- KUINS 接続端末数について
- KUINS 接続状況報告
- KUINS 障害報告
- セキュリティ関連報告について
- KUINS 機器の管理体制の調査について
- KUINS ダイヤルアップ回線の廃止について
- その他

平成 13 年 10 月 10 日（第 94 回）

- KUINS 接続端末数について
- KUINS 接続状況報告
- KUINS 障害報告
- セキュリティ関連報告について
- KUINS-II 機器の管理体制の調査について
- その他

平成 13 年 11 月 16 日（第 95 回）

- KUINS 接続端末数について
- KUINS 接続状況報告
- KUINS 障害報告
- セキュリティ関連報告について
- その他

お知らせ

KUINS ニュースへの寄稿を歓迎します．詳細は

`kuins-news@kuins.kyoto-u.ac.jp`

または下記までお問い合わせください．

問い合わせ先

学術情報ネットワーク機構情報システム管理掛 ((075) 753-7841)
（大型計算機センター等ネットワーク掛 ((075) 753-7432)）