京都大学における情報セキュリティ対策ならびに

インシデント対応状況とその評価

尾形 幸亮†, 斎藤 紀恵†, 小澤 義明†, 片桐 統†, 石橋 由子†, 平野 彰雄†

†京都大学　情報部　情報基盤課

ogata.kosuke.7c@kyoto-u.ac.jp, et al.

概要：　京都大学では、安全・安心のキャンパスネットワーク構築を進める一方、ネットワークの 24 時間監視を行うと共に、情報セキュリティ事案（インシデント）の対応においては、関係部局間で連携して調査・対応を行い、情報セキュリティ対策の強化に努めている。本稿では、本学のネットワーク設計や監視体制を説明すると共に、重大なインシデントに際して独自の脆弱性診断の実施及び通知という新たな対策の試みを紹介し、その効果を評価する。

1 はじめに

京都大学では、情報セキュリティの維持向上のため、安全・安心のキャンパスネットワーク設計、構築を進める一方、ネットワークの 24 時間監視を行うとともに、全学の情報セキュリティ対策実施体制の整備を図っている。情報セキュリティ事案(以下、「インシデント」という。）の対応に関しては、全学の情報セキュリティ対策の窓口である情報セキュリティ対策室を中心とした緊急対応体制の構築、運用により情報セキュリティ対策の強化に努めている。

本稿では、本学のキャンパスネットワーク設計の構成・運用、情報セキュリティ監視体制と組織体制、およびインシデント対応の体制と対応実績を紹介する。また、この間に発生した重大なインシデントへの対策として、インシデントの同時多発を未然に防ぐべく、情報セキュリティ対策室が主体的に全学の情報機器に対する脆弱性チェックを実施し、脆弱な情報機器の運用管理者へ通知を行うという新たなフローにより対策を試みた。その事例を紹介すると共に、その効果を評価する。

2 キャンパス・ネットワーク構成

2.1 キャンパスネットワーク設計と構成

京都大学は、吉田、宇治及び桂地区のキャンパスに加え、全国に跨る隔地に教育・研究施設が設置されており、これらの施設、キャンパスをキャンパスネットワーク KUINS (Kyoto University Integrated information Network System)に集約している。KUINS は、本学の全構成員に対する教育・研究・業務のためのネットワーク情報基盤として、整備、運用されている。図 1 に、KUINS の構成の概要を示す。

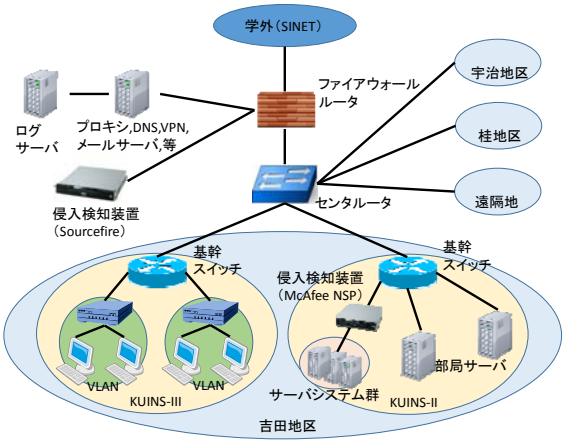

図 1　KUINS ネットワークの構成

KUINS の物理的構成は、各地区に配置する基幹スイッチを吉田地区設置のセンタールータに 10Gbps 及び 1Gbps のバックアップ回線で接続する事で集約しており、対外接続として SINET にファイアウォールルータを介して 10Gbps で接続している。ファイアウォールルータ配下には、ネ

ットワークサービスのための各種サーバ及び侵入検知装置を配置している。

2.2 KUINS の運用とポリシー

KUINS では、グローバルアドレスを持つ KUINS-II とプライベートアドレスを持つ KUINS-III という 2 種類のアドレス体系で管理し、各建物や研究室等に情報コンセントを配備している。情報コンセント、ネットワーク構成情報機器、管理者等の情報は、KUINS 接続機器登録データベース（以下、「KUINS-DB」という。）で一元管理している。

以下に､KUINS の運用ポリシーの要点を示す。

1） KUINS-II (グローバルアドレス)

・本学では、二つのクラス B のアドレスを取得しており、これをサブネットに分け部局等に割り当てている。

・KUINS-DB に MAC アドレスを登録しないと、学内外の他の情報機器との通信はできない。

･KUINS-II アドレスを割り当てた情報機器は、学内の情報機器からの通信ができる。

・学外通信も KUINS-DB により可否を申請、更に､TCP 25 番ポートの通信も標準では制限している。

2） KUINS-III (プライベートアドレス)

・10.224.0.0/22 を使用し、標準は/26 単位、申請により拡張が可能。

・KUINS-III ネットワークの IP アドレスは、DHCP により配布している。また、必要に応じて固定アドレスが割当てられ、研究室のプリンタ等の共有情報機器に利用されている。

・KUINS-III は VLAN で管理されており、VLAN 同士の通信を原則許可していないが、申請により VLAN 間を接続する事もできる。

・KUINS-III に接続した情報機器は、Proxy サーバや NAT サーバを介して外部ネットワークに接続する。

3） KUINS 課金制度

・KUINS-II の利用時は IP アドレス毎、KUINS-III の利用時は情報コンセント毎に課金し、情報機器の厳密な管理を促すと共に利用の適正化を図っている。

4） P2P 公衆ファイル共有通信の制限

・KUINS-II では原則禁止であるが、教育・研究目的に限り届け出る事で利用できる。

・KUINS-III では、禁止している。

3 本学のセキュリティ対策

3.1 不正アクセス等の監視について

1） 侵入検知装置の配備と監視

本学では､2 台のネットワーク侵入検知装置を配置し、不正アクセスの監視を行っている。図 1 に示すように、1 台はソースファイヤ社製の Sourcefire で、本学と外部との全ての通信を監視している。もう 1 台は、マカフィー社製 McAfee NSP で、本学の情報発信や研究室サーバなどの集約を目的にサービスするホスティングサーバシステム群（以下、「サーバシステム群」という。）の基幹スイッチ配下に配置し、サーバシステム群に対する KUINS-II での全ての通信を監視している。

2） 委託による 24 時間、365 日の監視と通知

侵入検知装置は、不正アクセスの可能性のある通信を検知すると、ログに記録すると共に、新しく検知されたものや急増したものは警報としてメールで通知する。本学では、不正アクセスなどの監視、ログ解析を業者に委託する事で、24 時間、365 日の不正アクセス監視体制を整えている。

委託業者（以下、「監視業者」という。）は、侵入検知装置からの警報、ログ解析の結果、不正アクセス等の可能性を検知すると、攻撃の種類、緊急度、通信の状況を整理した情報をメールで本学の情報セキュリティ対策室（以下、「対策室」という。）に通報する。

3） インシデントの判定と記録及び分類

対策室では、監視業者からのメール通報の内容を精査し、侵入検知装置のログ解析を行う。その結果、インシデントと判定した場合、インシデントの内容を種類や重要度、緊急度で分類すると共に、インシデント事案として記録し、コンピュータ不正アクセス対応連絡要領に基づいてアクションを起

こす。

4) ログ検索システムの構築、運用

インシデント対応においては、侵入検知装置から通知される情報のみならず、Proxy、NAT サーバ及び DHCP サーバのログが必要となるため、各種ログを集約して簡便に検索するためのシステムとして、ログ検索システムを運用している。

侵入検知装置から通知される情報は、通信時刻、始点および終点の IP アドレスのみであり、インシデント調査のためには IP アドレスからネットワークの管理者、情報端末、利用者を特定する必要がある。KUINS-II に接続された情報機器の場合は、グローバル IP であるため管理者と IP アドレスが一対一で特定されるが、KUINS-III の場合は DHCP で配布されるプライベート IP アドレスであり、端末ごとに固定でない。そこで、インシデント発生時点での IP アドレスと情報端末の対応を特定するために、Proxy、NAT サーバ及び DHCP サーバのログなどを横断的に検索する必要がある。そのためにログ検索サーバを運用し、インシデントに対する即応体制の強化及び業務合理化を図っている。

なお、迷惑メールなどメール関連インシデント対応のために、メールログも統合、一元的に管理している。

3.2 ウイルス付メール、迷惑メール対策

メールはネットワークサービスの中で重要なサービスの一つであり、ウイルス、迷惑メール対策が安全、安心のネットワークサービスを運用するうえで非常に重要である。本学に届くメールに対しては、図 1 のファイアウォールルータ配下に、帯域制限サーバを設置し、迷惑メールの流入を制限すると共に、迷惑メールチェックサーバ、ウイルスチェックサーバを配置し、迷惑メールやウイルス付メールの流入を阻止している。

本学から発信されるメールについてもウイルスチェックを行っている。また、学外から受信した迷惑メールを各構成員のメール転送設定により無条件に学外に配信すると、結果として本学が迷惑メール発信ドメインと認定されてしまい正常なメール通信の制限を受ける可能性がある。これを避けるため、本学の迷惑メールチェクサーバで、迷惑メールと判定したメールは、無条件に削除し、発信されないような設計としている。

4 インシデント対応

4.1 インシデント対応組織及び体制

本学の不正アクセス等のインシデント対応体制を図 22 に示す。本学の最高情報セキュリティ責任者 CISO ((Chief Information Security Officer), 情報担当理事)を委員長とする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）が不正アクセス等のインシデント対応を統括する。

学内外からの不正アクセス等の通報窓口として、対策室が設置されている。

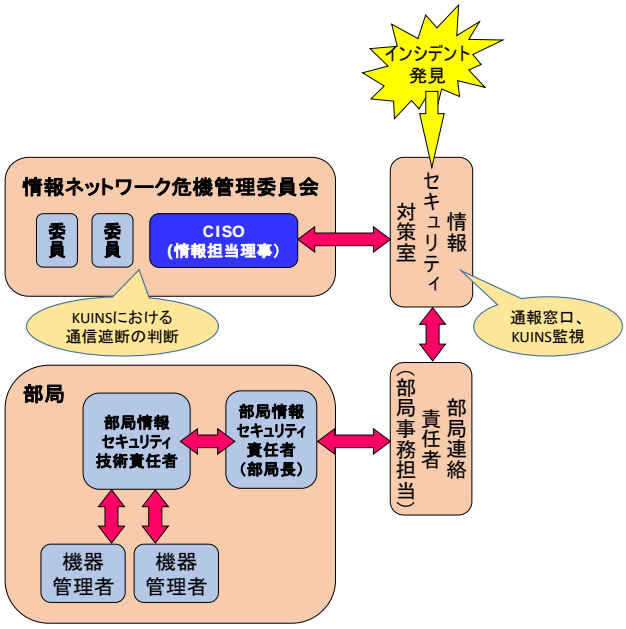

図 2 インシデント対応体制

また、各部局は、部局情報セキュリティ委員会を設置し、部局情報セキュリティ責任者（部局の長）、部局情報セキュリティ技術責任者、不正アクセスなどの窓口である部局連絡責任者を置く。

4.2 インシデント対応の流れ

本学におけるインシデント対応のフローを図 3 に示す。

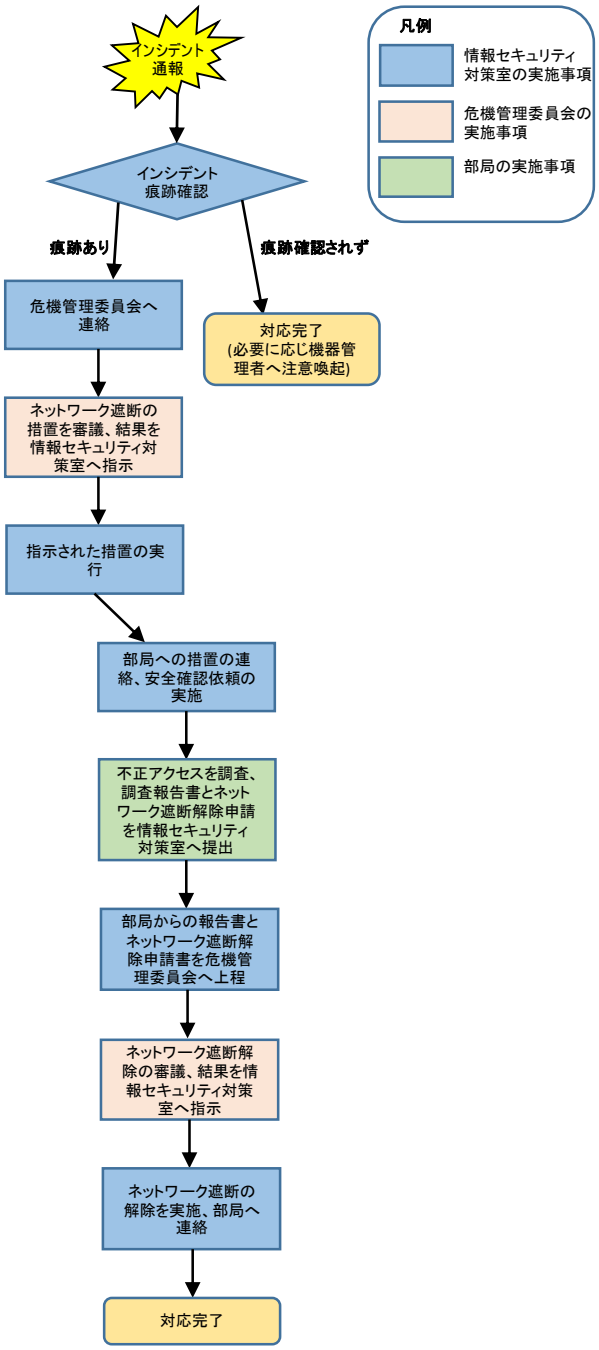

図 3　インシデント対応の流れ

① 対策室が不正アクセス等の通知を受けた場合(侵入検知装置がインシデントを検知した場合も同様)、事実関係の把握、証拠保全に努めると共に、インシデント発生の痕跡が確認された場合は、危機管理委員会に連絡する。

② 同時に、インシデント発生元の情報機器の管理部局の部局情報セキュリティ委員会に対し、部局連絡責任者を通じて、インシデント発生の通知および「安全確認」の依頼を行い、対策及び状況の報告を求める。

③ 危機管理委員会は、インシデントの重大性、影響範囲などを判断し、必要な場合には、別途定める手順に従って、ネットワークからの遮断などの決定を行い、対策室に対し指示する。

④ 対策室はネットワークからの遮断指示を受け、遮断措置を実施すると共に、当該部局の情報セキュリティ委員会に、部局連絡責任者を通じて危機管理委員会からのネットワークからの遮断指示を実施した主旨を文書で通知する。

⑤ 当該部局の情報セキュリティ委員会は、ログなどにより不正アクセスの調査を行い。必要なログ等の証拠の保全と共に、不正アクセスの原因解明を行い、必要な対策を実施し、これらの対応状況を「不正アクセス等報告書」にまとめ、部局情報セキュリティ委員会の審議の後、部局連絡責任者を介して対策室に提出する。ネットワークからの遮断措置を受けている場合、合わせて遮断解除の申請書を提出する。

⑥ 対策室は、提出された「不正アクセス等報告書」及び遮断解除の申請書を危機管理委員会に報告、審議を依頼する。

⑦ 危機管理委員会は、「不正アクセス等報告書」を精査し、対策が適切と判断した場合、対策室にネットワークからの遮断措置の解除を指示する。

⑧ 対策室は、通信遮断解除の措置を実施後、その主旨を当該部局情報セキュリティ委員会に通知し、インシデント対応は完了する。

以上が、重大な不正アクセス等のインシデント

対応フローである。

なお、インシデントの中で軽微な事象は、危機管理委員会より対策室に対応が委任されており、対策室が部局情報セキュリティ委員会および機器管理者に「安全確認」を依頼し、不正アクセス等の事実が無かった場合には「安全確認報告書」、インシデント事案の場合には「不正アクセス等報告書」を提出する事になっている。これらの対策室によるインシデント対応は、その内容、件数を取りまとめて最高情報セキュリティ責任者に報告する簡便なフローにより処理している。

4.3 対応実績及びインシデント傾向

2012 年度と 2013 年度の不正アクセス発生および対処の状況を表 1 に示す。

表 1　不正アクセス発生および対処の状況

年度			2012	2013
通報	IDS監視委託業者		459	906
	部局または学外		16	46
依頼	安全確認調査依頼件数		110	166
	内容	ウイルス感染疑い	39	72
		P2P通信疑い	47	31
		その他	24	63
報告	安全確認報告書提出件数		41	45
	不正アクセス等報告書提出件		31	71

安全確認依頼の件数は、年度ごとに増加傾向にあり、サイバー攻撃の脅威が拡大していることが伺える。危機管理委員会による通信遮断の実施件数も年々増加しており、サイバー攻撃の凶悪性も増大していると考えられる。

発見された攻撃のうち、監視業者による発見が約 8 割（セキュリティ対策担当職員による発見分含む）、部局または学外からの通報が約 2 割となっている。攻撃の内容は、概ねウイルスの感染疑いが 4 割、許可されていない P2P 通信疑いが 2 割、その他が 4 割となっている。

部局からの調査報告書は、例年、安全確認報告書が 6 割以上であり、不正アクセスによる通信が観測されても、実際の被害は発生していないケースが多い。2013 年度については、NTP の脆弱性対策における後述の新たな試みとして、脆弱なシステムを運用している部局を調査して安全確認依頼を行い、部局で対策が実施された（脆弱なシステムの運用は実害がなくとも事案と見なされるため、不正アクセス等報告書を提出頂いた）。そのため、例年より不正アクセス等報告書の件数が増えている。

5 情報セキュリティ対策強化のための新たな対応策とその実施

2013 年度、従来の侵入検知装置による通信監視といった不正アクセス対応フローでは対処できない重大なインシデントが発生し、独自に対応を行ったので、これらの事例を紹介する。

5.1 IME のオンライン機能利用による情報漏洩

本件は、2013 年 12 月 17 日、IIJ-SECT（IIJ group Security Coordination Team）の Security Diary に掲載された「IME のオンライン機能利用における注意について」の記事に端を発する。記事の内容は、日本語入力ソフト（IME）のオンライン機能がユーザの入力文字列をインターネット上の外部サーバに送信しており、外部サーバでの情報蓄積による情報漏洩、更に、通信経路の盗聴による情報漏洩の危険性を指摘するものであった。

特に、Baidu IME については、①デフォルトでオンライン機能有効になっており、②他のソフトウェアに同梱されてインストールされるなど、ユーザが意図せず情報漏洩をしてしまう危険性を指摘するものであった。

本学では、教職員の Baidu IME 使用により、情報漏洩の危険性があると判断し、全教職員に告知した。また、本学の情報端末（PC）は、KUINS-III に接続されている事から、Proxy ログから外部サーバとの通信履歴を解析し、通信元の IP アドレスから使用端末を特定して、KUINS-III VLAN 管理者宛に、注意喚起、アンインストールを要請した。

1 月初旬のログ解析では事務業務端末を含む 84 端末での使用が観測されたが、2 月初旬に行った解析では、38 端末に減少しており、事務業務端末

での使用は無くなったことを確認した。

5.2 ntpd の monlist 機能を使った DDos 攻撃

本件は、2014 年 1 月 15 日、JPCERT により「ntpd の monlist 機能を使った DDoS 攻撃に関する注意喚起（JPCERT-AT-2014-0001)」として掲載された。ntp (Network Time Protocol)は、UDP プロトコルで通信するために、容易に送信元 IP アドレスを詐称できるが、本件はこれを悪用した物である。サーバ（ntpd)の monlist 機能は、リモートからサーバ状態を確認する機能であり、応答として大きなサイズのパケットを送信元 IP アドレスに返すために、攻撃対象のサーバ IP アドレスを送信元に偽装した問合せパケットを ntp サーバに送る事で DDoS 攻撃を行うことができる。

本学でも 2013 年 10 月頃以降、海外のサーバ管理者より本学のサーバ情報機器による DDoS 攻撃の被害と対処要請を受け、不正アクセス等対応手順に従って「安全確認」依頼により対応してきた。しかし、KUINS では ntp サーバが多数動作しており、今後も容易に DDoS 攻撃の踏み台にされる可能性が高いと判断し、部局情報セキュリティ委員会を通じて、各サーバ管理者に注意喚起を行った。

さらに、脆弱性診断ツールを使用し、KUINS-II 接続の情報機器への診断を実施した。その結果、DDoS 攻撃の踏み台になる可能性のある 13 台の情報機器を特定し、管理者に対して注意喚起及び対処要請を実施した。これ以降、本学のサーバ情報機器から DDoS 攻撃に加害したとの通報は無い。

脆弱性診断のイメージを図 4 に示す。

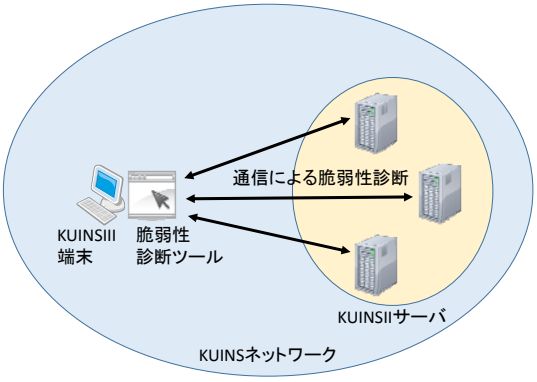

図 4 脆弱性診断のイメージ

なお、この診断によりネットワークが過負荷にならないよう、サーバに対する診断間隔を充分にとった。

5.3 OpenSSL（Heartbleed)の脆弱性を狙った攻撃

本件は、2014 年 4 月 8 日、JPCERT により「OpenSSL の脆弱性に関する注意喚起(JPCERT-AT-2014-0013)」として掲載されたものである。OpenSSL は暗号化通信ライブラリであり、http サーバなど多くの暗号化通信で利用されている。また、4 月 11 日には、既に本脆弱性を使用する攻撃コードが公開されており、ネットワーク経由での攻撃が成功するとサーバの秘密鍵や暗号化通信で交換した ID,パスワードなどの情報漏洩の可能性がある重大な脆弱性である。

本学では、情報セキュリティ実施責任者名で、全学の部局情報セキュリティ責任者宛に、各部局の教職員に、本脆弱性の重大性を周知し、適切な対応を実施するよう注意喚起を行った。

また、緊急対応が重要な事案であると判断したため、脆弱性診断ツールを使用して KUINS-II 接続情報機器への脆弱性診断を実施した。

診断の結果、42 台の情報機器について脆弱な OpenSSL が運用されている可能性がある事が判明したため、各情報機器の管理者に対応を依頼した。

なお、テレビ会議システムは、KUINS-II に接続され、Web インターフェースの管理機能（必須では無い）を備えるため、本脆弱性の対象となる機種もあった。しかし、テレビ会議システムは、常時稼働しておらず、利用時だけ電源を入れる運用が多いため、今回実施した脆弱性診断では検知できていない情報機器が残っている事が明らかになった。これらは、KUINS-DB の機器情報をもとに、管理者に対して、随時通知を行った。

5.4 新たな対応策の評価

新たな対応策では、情報セキュリティ対策室が主体的に脆弱な情報機器を特定し、機器管理者への注意喚起及び対処要請を行ったことで、これまでの侵入検知装置の警報や外部からの通報を受けたインシデント調査に比べ、インシデントの同時

多発を未然に防ぐことができたと考える。実際、5.1 節で説明した IME のオンライン機能利用による情報漏洩の件では、事務業務端末での使用を無くすことに成功した。また、5.2 節で説明した ntpd の monlist 機能を使った DDos 攻撃への対応では、対応完了以降は本学のサーバ情報機器から DDoS 攻撃に加害したとの通報はない。以上のように、新たな対応策には一定の効果があったと考える。

一方、新たな対応策を通じて判明した課題として、テレビ会議システムといった常時稼働していないアプライアンス機器への対応があげられる。このような機器は、脆弱性診断時に停止していると脆弱かどうか検知できないため、機器のソフトウェアバージョンといった情報の定期的な把握など、今後の対応を検討する必要があると考えられる。

6 まとめ

本稿では、本学のキャンパスネットワーク設計の構成・運用、情報セキュリティ監視体制と組織体制、およびインシデント対応の体制と対応実績を紹介した。そして、この間に発覚した重大脆弱性への対策として、インシデントの同時多発を未然に防ぐべく、情報セキュリティ対策室が主体的に全学の情報機器に対する脆弱性チェックを実施し、脆弱性の可能性のある情報機器の運用管理者への通知という新たなフローにより対策を試みた事例を紹介した。

参考文献

[1] IIJ-SECT、「IME のオンライン機能利用における注意について」、
https://sect.iij.ad.jp/d/2013/12/104971.html
(2014 年 10 月 21 日アクセス)
[2] JPCERT/CC、「ntpd の monlist 機能を使った DDoS 攻撃に関する注意喚起」、
https://www.jpcert.or.jp/at/2014/at140001.html
(2014 年 10 月 21 日アクセス)
[3] JPCERT/CC、「OpenSSL の脆弱性に関する注意喚起」、
https://www.jpcert.or.jp/at/2014/at140013.html
(2014 年 10 月 21 日アクセス)