

脆弱性報告と公開のポリシー



2003年8月1日改訂



目的

このポリシーは、株式会社ラック SecureNet Service チームが情報セキュリティに関わる脆弱性を発見した場合、どのようにしてそれをベンダに対して報告をし、情報の公開を行うのかということについて詳述しています。なお、このポリシーの最大の目的は脆弱性の影響を受けるすべてのユーザへの脅威を最大限に緩和することにあります。

本ポリシーの対象は市販製品になります。特定の事業者によるところの大きい情報システム及び情報機器に関しましては、本ポリシーの各条項を適用することはありません。これらの本ポリシーの適用外の情報システム及び情報機器は、以下のものを含みます。

(a) 特定のチャンネルを通じて、最終顧客に提供される製品

(例：キャリアからのレンタル製品)

(b) 受注ベースで事業者などの組織体に SI した上で納入されるシステムコンポーネント

(例：ミドルウェア)

(c) 運用されているサービス及びシステム

(例：インターネットバンキングや特定の ISP が使用しているサーバなど)

ただし、偶発的に発見したものに関しては、例外として報告のみを行います。

注意していただきたいことは、このポリシーは脆弱性の報告を受けた側へ、個々の規定を遵守することを求めるものではありません。すなわち、相互にコミュニケーションをはかりながら、その時の状況にあわせた対応を脆弱性の報告を受けた側へ促すものです。



脆弱性の報告および公開のプロセス

脆弱性の報告および公開のプロセスは、通常、次のようなフェーズを経ます。

1. 発見

- SecureNet Service チームが偶発的に、あるいは調査・研究中に脆弱性を発見

2. 報告

- 当該ベンダに報告

3. 検証

- 当該ベンダ側での脆弱性の検証

4. 解消

- 脆弱性を解消するためのパッチないし何らかの手段が当該ベンダ側より提供

5. 公開

- 当該ベンダ側より情報が公開された後、SNS Advisory ないし SNS Spiffy Reviews として株式会社ラック Web ページおよびセキュリティ関連メーリングリストで公開



ポリシー

- フェーズ1: [発見] -

SecureNet Service チームは脆弱性の発見時において、それに類似した問題の有無について、当該ベンダの Web サイトから提供されている情報などを利用し、可能な限りの調査を行います。この調査において類似点を見出せなかった場合、当該ベンダへ報告を行います。

- フェーズ2: [報告] -

SecureNet Service チームは原則的に脆弱性の報告を電子メールで行います。当該ベンダより公開鍵暗号化方式で利用される公開鍵が提供されている場合は、報告およびその後の電子メールによる連絡は全てその公開鍵を使用して暗号化を行います。

報告先の電子メールアドレスは、当該ベンダの Web サイトなどから報告先として適切なものが確認された場合には、それを使用します。報告先の電子メールアドレスとして適切なものが確認できなかった場合、あるいは、適切だと思われる電子メールアドレス宛てに報告を行った後、7日以内に当該ベンダから脆弱性の報告に対する反応であると推察可能な電子メールないし同等の連絡手段による連絡を得られなかった場合は、次の電子メールアドレス宛てに報告を行います。

- * info@(当該ベンダの使用しているドメイン名)
- * sales@(当該ベンダの使用しているドメイン名)
- * secure@(当該ベンダの使用しているドメイン名)
- * security@(当該ベンダの使用しているドメイン名)
- * security_alert@(当該ベンダの使用しているドメイン名)
- * security_alerts@(当該ベンダの使用しているドメイン名)
- * support@(当該ベンダの使用しているドメイン名)
- * vulnerabilities@(当該ベンダの使用しているドメイン名)
- * webmaster@(当該ベンダの使用しているドメイン名)

これらの電子メールアドレス宛てに送信した後、何らかの反応を得られないままさらに30日が経過した場合、JPCERT/CC や CERT/CC に脆弱性の報告を行ったうえで脆弱性の影響を最大限に考慮し、当該脆弱性情報の公開に踏み切る場合があります。



加えて、電子メールなどによる連絡が続いていたとしても、最初に SecureNet Service チームがベンダに報告した日より 60 日が経過しており、かつ、ユーザを尊重した対応が見られないと我々が判断した場合には、ベンダにその旨を通告し、JPCERT/CC や CERT/CC に脆弱性の報告を行った後に、情報を公開することがあります。これはたとえば、リモートから任意のコードを実行可能である等の、ユーザに深刻な被害が生じることが懸念されているにも関わらず、最初の報告日から 90 日以上経過しても『調査中である』とだけの連絡があり、その進捗状況や内容についてベンダから明示していただけない場合といった状況です。

この状況下における公開に関しては、慎重な熟慮を重ねた結果、ユーザのセキュリティ確保に情報公開が適当であると判断した場合にのみ、当該ベンダからの代替策ないしパッチの有無に関わらず行われます。

- フェーズ3、フェーズ4: [検証および解消] -

報告を行った脆弱性の解消を目的とした検証が当該ベンダ側で行われる際には、SecureNet Service チームはその検証の支援を惜しみません。

また、導入モジュールなどによって、当該ベンダ以外の組織等の第3者の協力が必要な場合は、SecureNet Service チームによって報告された問題に関する情報を、この第3者に提供することが可能です。この場合には、SecureNet Service チームへの通知は特に必要ありません。

同時に、SecureNet Service チームによって報告された問題の影響範囲が複数ベンダに及ぶことが判明した場合は、第一報告先のベンダの了承を得たうえで、CERT/CC ならびに JPCERT/CC に通知し、これら中立公平な組織の主導のもとで、円滑かつ円満な問題解決をはかります。



- フェーズ5: [公開] -

報告を行った脆弱性に関する代替策ないしパッチが当該ベンダ側から提供された後に、SecureNet Service チームは Bugtraq や NTBugtraq 、 Bugtraq-JP 、 news@securiteam.com などのセキュリティ関連メーリングリストおよび株式会社ラック Web サイトを通じ、SNS Advisory ないし SNS Spiffy Reviews として脆弱性の公開を行います。

また、前節[検証および解消]において、報告を行った脆弱性が、その設計上ないし仕様上の問題であるとの結論を当該ベンダから得た場合や、あるいは当該製品のユーザへの影響が明白にも関わらず、報告された脆弱性に対する対応が進展しないまま、脆弱性の報告に対する最後の我々からの進捗確認の問い合わせを行った電子メールの送信日時より 45 日が何の応答も無く経過した場合には、JPCERT/CC や CERT/CC に脆弱性の報告を行った上で対応策について検討を行います。この対応策には、当該ベンダからの代替策ないしパッチの有無に関せず、その情報を公開することが含まれます。

Bugtraq Mailing List	http://www.securityfocus.com/archive/1
NTBugtraq Mailing List	http://www.ntbugtraq.com/
Bugtraq-JP Mailing List	http://www.securityfocus.com/archive/79
Beyond-Security's SecuriTeam.com	http://www.securiteam.com/



本ポリシーに対する各ベンダからのコメント

各ベンダから本ポリシーに対していただいた公式のコメントをここでは記載しています。記載の順番は、コメントをいただいた時系列順になっています。SecureNet Service チームは公式のコメントをいただいた各ベンダに深い感謝の意を表します。

なお、ここにコメントを掲載した以外の多くのベンダからも、本ポリシーの策定におきまして多大なるご支援をいただきました。SecureNet Service チームはこれらの各ベンダにも深い感謝の意を表します。

[マイクロソフト社からのコメント]

本ポリシーに関しては的確な内容であり、マイクロソフトとしても明確にポリシーを公開していただいた事に感謝をしたい

Microsoft Security Response Center
Microsoft PSS Security Response Team
Microsoft Japan GTSC Security Response Team (JPSRT)

- * マイクロソフト社の製品に関する脆弱性の報告先は secure@microsoft.com です。
上記報告先の利用法に関しては次の URL を参照ください。
<http://www.microsoft.com/japan/technet/security/bulletin/alertus.asp>



[トレンドマイクロ株式会社からのコメント]

トレンドマイクロは本ポリシーの公開を歓迎いたします。本ポリシーにより、脆弱性の対処に一定の基準ができたことは、コンピュータセキュリティ・インシデントへのレスポンスを高め、情報セキュリティ向上につながるものと考えます。

今後とも株式会社ラック SecureNet Service チームと強力なパートナーシップのもと、システムのセキュリティ向上に努めてまいります。

トレンドマイクロ株式会社

*トレンドマイクロ株式会社の製品・サービスに関する脆弱性の報告については、以下のメールアドレスにご連絡ください。

secure@trendmicro.co.jp

*トレンドマイクロ株式会社では製品のサポート情報を以下のサイトで公開しています。

<http://www.trendmicro.co.jp/support/index.asp>

[白水啓章様からのコメント]

私は、本ポリシーが、適切かつ妥当なものであると評価します。さらに、今後も LAC SNS チーム様による、脆弱性検出および脆弱性解消のための検証支援により、多くの脆弱性が大きな混乱なく解消されていくことを期待します。

[日本ヒューレット・パカード株式会社からのコメント]

* ヒューレット・パカード製品に関する脆弱性の報告先は security-alert@hp.com です。上記報告先の利用方法（暗号メールの送信方法等）に関しては次の URL を参照ください。

http://welcome.hp.com/country/us/eng/software_security.html

（将来、URL が変更になった場合には、<http://www.hp.com/> より、search: にて "report security" で検索していただければと思います。）



参考文献一覧

RFPolicy 2.0

<http://www.wiretrip.net/rfp/policy.html>

Internet-Draft, "Responsible Vulnerability Disclosure Process"

<http://www.ietf.org/internet-drafts/draft-christey-wysopal-vuln-disclosure-00.txt>

Bugtraq Frequently Asked Questions

<http://www.securityfocus.com/popups/forums/bugtraq/faq.shtml>

NTBugtraq Disclosure Policy

<http://ntbugtraq.ntadvice.com/default.asp?sid=1&pid=47&aid=48>

CERT/CC Vulnerability Disclosure Policy

<http://www.kb.cert.org/vuls/html/disclosure/>

ACROS ASPR Notification and Publishing Policy

http://www.acros.si/aspr_policy.html

NMRC policy

<http://www.nmrc.org/advise/policy.txt>

@stake Security Advisory Disclosure Policy

<http://www.atstake.com/research/policy/index.html>

Internet Security Systems X-Force Vulnerability Disclosure Guidelines

http://documents.iss.net/literature/vulnerability_guidelines.pdf



株式会社ラックについて

株式会社ラックは、いち早くネットワーク社会の到来を予測して1986年9月3日に設立されました。ネットワークセキュリティソリューション分野でのリーディングカンパニーを目指し、コンピュータセキュリティ研究所の先進セキュリティテクノロジーをJSOC 事業本部、セキュアネットサービス事業並びにシステムインテグレーション事業が提供するサービスに付加して、官公庁・企業・団体等の顧客にセキュリティソリューションサービスを提供しています。

コンピュータセキュリティ研究所について

株式会社ラックの一部門であるコンピュータセキュリティ研究所(Computer Security Laboratory : CSL)は、オペレーティングシステムやアプリケーション、あるいはハードウェアに潜在的に存在している脆弱性ないし設計上の問題点を発見、報告、開示することに特化した日本有数の研究機関です。本部門を中心とした SecureNet Service チームによって発見された各種のセキュリティ情報は、SNS Advisory および SNS Spiffy Reviews として株式会社ラックの顧客、およびインターネット上の重要なシステムを保護することを目的として発行されています。

SNS Advisory

SNS Advisory には、コンピュータセキュリティ研究所の調査によってもたらされた脆弱性情報が含まれています。この情報には、問題の詳細、影響を受けるソフトウェア、そして対策が盛り込まれています。SNS Advisory は株式会社ラックの Web サイト上の次の URL にて公開されます：

<http://www.lac.co.jp/security/intelligence/SNSAdvisory/index.html>

SNS Spiffy Reviews

SNS Spiffy Reviews には、コンピュータセキュリティ研究所独自の研究によりもたらされた各種の情報が含まれています。この情報には、脆弱性の再現、あるいはセキュリティに関する統計情報や、調査中において偶発的に発見された第三者サイトの設計上の問題点などを含んでいます。SNS Spiffy Reviews は株式会社ラックの Web サイト上の次の URL にて公開されます：

<http://www.lac.co.jp/security/intelligence/SNSSpiffy/index.html>



更新履歴

2003年8月1日：初版公開

2003年8月1日：日本ヒューレット・パカード株式会社からのコメントを追加