EndRun TECHNOLOGIES "Smarter Timing Solutions"

A P P L I C A T I O N N O T E

タイムサーバーの安全を確保する為の最善の方法

ネットワークタイムサーバーは通常のマルチユーザーアプライアンスやサーバーではありません。タイムサーバーは信頼しうる、正確な時刻を提供するという、非常に特化した機能を提供します。ユーザーデータがタイムサーバーに保存されることはありません。

我々は現在提供されている最も安全なタイムサーバーであると信じています。これはある意味、その単純化の哲学からくるものです。我々は完成度の高いOSを使い、不要なプロトコルは使っていません。利便性のためのプロトコル、たとえば httpd, snmpd, telnetd そして sshd ですら無効にすることができます。またシステム設定をsnmpやhttpから書き換えることはできません。

以下は、我々がファイアーウォールの背後のプライベートネットワークに置かれたタイムサーバーをより安全にするために推奨する手順です。パブリックネットワークに置く場合は、ユーザーアカウントを変更するなどのさらなるセーフガードがなされるべきです。このペーパーではそのようなさらなるセーフガードについては触れません。

NOTE: このペーパーはSonomaを例に取り書かれていますが、同じ手順はEndRunのTempus LX, Unison, Meridian, Meridian IIやTycho IIといった他の製品にも適用できます。

パスワードを初期設定値から変えてください

タイムサーバーは納入時に2つの初期設定パスワードを持っています。パスワードは passwd　コマンドを使い、できるだけ速やかに変更すべきです。通常、ネットワーク管理者以外がタイムサーバーにログインすることはありません。ですから、変更したパスワードを知る人は一人か二人で良いはずです。

`passwd` ルートユーザーのパスワードを変更 (特権ユーザー)
`passwd ntpuser` ntpuserのパスワードを変更 (非特権ユーザー)

必要としないプロトコルを停止してください

タイムサーバーは次のプロトコルがそれぞれのポートに有効な状態で出荷されます：

NTP (UDP 123)
TELNET (TCP 23)
Daytime (TCP/UDP 13)
Time (TCP/UDP 37)
SSH (TCP 22)
SNMP (UDP 161 and 162)
HTTP (TCP 443)
Optional Precision Time Protocol (UDP 319 and UDP 320)

Network Time Protocol (NTP) は停止しないでください。それ以外の必要としないプロトコルは停止してください。ユーザーマニュアルの第5章にその方法が書かれています。ユーザーマニュアルへのリンクは以下の通りです。日本語版マニュアルは弊社情報システム営業部までお問い合わせください：

Sonoma D12 (GPS):	http://www.endruntechnologies.com/pdf/USM3027-0000-000.pdf
Sonoma D12 (CDMA):	http://www.endruntechnologies.com/pdf/USM3026-0000-000.pdf
Sonoma N12 (GPS):	http://www.endruntechnologies.com/pdf/USM3029-0000-000.pdf
Sonoma N12 (CDMA):	http://www.endruntechnologies.com/pdf/USM3028-0000-000.pdf

アクセスの制限

タイムサーバーはシステムの中でももっとも安全性の高いものであるべきです。多くのユーザーがネットワークタイミングプロトコル（たとえばNTP）でアクセスできても、それ以外の方法では一人か二人のネットワーク管理者だけがアクセスを許されるべきです。それゆえ、アクセスは特定のホストと一人か二人のユーザーに制限すべきです。

アクセスを制限する方法はユーザーマニュアルの第5章を参照ください。

最も厳格な状況では、NTPと必要とするタイミングプロトコルを除いて全てのプロトコルを停止して、タイムサーバーの設定と監視はRS-232コンソールから行います。

セッションを暗号化する

アクセスには常に SSH (secure shell) を使うべきであり、Telnet は停止すべきです。初期値の SSH キーは納品時に各個体毎に設定されています。

認証を使う

NTPクライエントにはMD5認証を使うことを求め、認証しないユーザーにはNTPアクセスさせないようにするべきです。納品時にはMD5認証をするユーザーにもしないユーザーにも応答するように設定されています。MD5キーを独自のものに変更し、クライエントをそのキーを使うように設定することを推奨します。

その手順はユーザーマニュアルの第3章にあります。

キーパッドへアクセスできなくします

Sonoma D12 では、ユーザーマニュアルの第9章にある **lockoutkp** と **kp-lockstat** ユティリティーを使いキーパッドを無効にします。これにより許可なく設定を変更できなくなります。

ログファイルを保存する

システムログはトラブルシューティングに欠かせません。ログファイルはもしも被害に遭った際の調査に重要な役割を果たします。Sonomaはsyslogサーバーにログを送ることができますので、これを検討されることを推奨します。これにより誰かが侵入しようとした際には、それが侵入元のIPアドレスと共に記録されることです。

設定方法については、syslogの関連文書を参照ください。設定を行ったファイルは、次のリブートで読み込まれるように、 /boot/etc ディレクトリにコピーすることを忘れないでください。

脆弱性への対応

Sonomaはモノリシックなlinuxカーネルを使っており、モジュールを受け付けません。これにより多くの脆弱性を回避しています。

セキュリティースキャンにより見つかる侵入の可能性があるとされる脆弱性はタイムサーバーには存在しない状況における脅威でしかありません。多くのセキュリティースキャンは開いているポートとプロトコルバージョンを調べるだけで、たとえばSonomaのSSHを脆弱性として列挙するかもしれません。しかし、その脆弱性が外部に曝されるようにSonomaのSSHが設定されることはありません。タイムサーバーはマルチユーザーワークステーションではありませんから、スキャンで列挙された脆弱性の多くは問題にはなりません。

脆弱性の可能性もこの文書に述べた回避策を適用することで対応できます。

ファームウェアの更新

タイムサーバーはマルチユーザーコンピュータではなく、非常に特化した機能を組み込んだアプライアンスです。組み込み環境においてパッチを適用したり、頻繁にLinuxのオープンソースバイナリーをリビルドすることから何がえられるかには疑問があります。新しいビルドに脆弱性がないとは保証されず、新しい脆弱性が潜んでいるかもしれず、以前のバージョンにはなかった新たなバグが見つかるかもしれません。

妥当な対応策で解決できない深刻な脆弱性についてはファームウェアの変更で可能な限り速やかに対応します。それ以外の脆弱性については、上記の対応策を施すことを推奨します。

EndRun は深刻な脆弱性に対応し、製品を改善し、バグを修正する新しいファームウェアを随時リリースします。ファームウェアは以下のページからダウンロードできます：

Sonoma GPS:
http://www.endruntechnologies.com/upgradesonomaG.htm
Sonoma CDMA:
http://www.endruntechnologies.com/upgradesonomaC.htm

NTP クライエント

NTPクライエントソフトは最新版にアップデートしてください。全てのクライエントがMD5認証を使うように設定してください。

お問い合わせ

ご質問は弊社あるいは EndRun のテクニカルサポートで受け付けております：

昌新 情報システム営業部
03-3270-5926
IS@shoshin.co.jp
EndRun Technical support.
1-877-749-3878 (U.S. & Canada)
707-573-8633 (International)
support@endruntechnologies.com