KenConsulting
情 報 ・ 通 信 ・ ビ ジ ネ ス
Webサイト http://www.kenconsul.com　　メール support@kenconsul.com　　携帯 070-5460-5495

ReadNotify 認証メールの法廷での使い方に関するガイド

ReadNotify が認証したメールは検証可能な証拠として法廷で以下の様にお使い頂けます:

1. 当該メールがインターネット網を通して送信された日付と時間の証拠として
2. 当該メールのヘッダーと本体が送信以降書き換えられていないことの証拠として
3. 当該メールがコンピュータ画面上に表示されたことの証拠として。ここでは当該メールを（コンピュータプログラムではなく）人間である受信者が読んだ証拠、及びその行為を行ったおおよその場所、日時、使用したメーラーまたはブラウザに関する情報も提供します。

その他、ReadNotify が独自に設定した信頼性の高い日付とタイムスタンプも有用な情報としてお使い頂けます。

先ず初めに:

以下の2つの質問に対する答えをご理解ください。:-

Q: "ReadNotify の認証メール"とは何ですか？

A: これは通常のメールの終りのところに、そのメールがインターネット上に送信された日時、メールに与えたユニークな連続番号（連番）、メール自体のユニークな暗号識別番号を追加情報として付加したものです。このメールの末端に付けた追加情報を含むメール全体（通常ヘッダーも含む）はデジタル署名されます。この署名はメールに添付され、後で公開されます。この認証メールは受信者のメールサーバに転送され、そのコピーは“送達証明”の添付資料として送信者に戻されます。

Q: "開封証明"とは何ですか？それはどう機能しますか？

A: これは ReadNotify サーバが自動的に作成するメールで、それ自身が証明書になっています。（上の "ReadNotify の認証メール" の項参照）. これは ReadNotify サーバがユニークな暗号識別番号を検出した時作成します。この番号は受信者に送信したメールの中にしか含まれず、人がこのメールを読む為にコンピュータ画面上に表示した時 ReadNotify サーバがそれを検知します。メールの送信者はこの番号を、受信者がメールを開封した時に自動的に検知するか、またはメールの開封者が、自分がメールを開封したことを知らせる旨の操作を指示に従って行った時に検知するか、をオプションとして指定できます。 "開封証明"は（自動か、手動か）どちらの方法で検知したかを分けて報告します。

上記に関連する質問の回答は以下でも解説しています。

ReadNotify は1送信メール当り最大3種類の認証文書を提供します。

1. メールは受信者に配信した時1つ以上の認証情報が添付してあり、転送の途中でデジタル署名されています。
2. 送信者はメール送信の少し後に、認証されデジタル署名された自分のメールのコピーを受取ります。これは送信メールの"送達証明" の添付資料として送信者に送るものです。
3. 送信者は、受信者が送信メールを開封し読んだ時、通常"開封証明" (デジタル署名し、タイムスタンプが付いた“開封通知”) を受けとります。

法廷で ReadNotify の認証文書を使う場合は、以下の手順に慎重に従って下さい。

1. ここにある指示と説明を印刷して下さい。これは法廷で ReadNotify サービスとそのサービスで作成した文書の適用範囲と信頼性を説明するのに必要です。
2. ReadNotify の認証に関するオリジナルの関連文書を全て印刷してください。可能ならメール全てのヘッダー全体も印刷してください。複合形式 (multipart alternative) の MIME メールを使っているなら、メールのテキスト形式のものと HTML 形式のものも印刷してください。
3. あなたの文書が正確に認証されていることをチェックしてください。

    i. 認証された (未検証の) テキスト形式の文書は全て以下の形で始まります:-

    -----BEGIN PGP SIGNED MESSAGE-----

    ii. 認証された (未検証の) HTML 形式の文書は全て以下の形で始まります:-

    <!--
    -----BEGIN PGP SIGNED MESSAGE-----

    ReadNotify.com time-certified message. Original output headers:-

    iii. どちらの形式でもデジタル署名は以下の様な形で終ります:-

    -----BEGIN PGP SIGNATURE-----
    Version: GnuPG v1.0.6 (ReadNotify.com TimeStamp Server v2.1)
    Comment: Certificate #9900, created Mon, 19 Nov 2001 05:02:23 GMT

    iQBvAwUBO/iSXzanThAdit3tAQGSXwLMD3pcdjoKXEBHYqXpqT0c12B9jagV+lsK
    vzb5Pxa0oFj+ffZOhCGZJwbib5l5DEuNL79FwDtQ0vmUIuOL1d+I4acE2WrsjZrA
    20L4uFXO+BiPw4q+NBnlvHJX

=et1Q

-----END PGP SIGNATURE-----

4. **印刷した文書に付いているデジタル署名を全て検証し、検証した文書のコピーを印刷してください。**

   検証するには署名検証プログラム(例えば Networks Associates Technology, Inc.**の** PGP。**これは** www.pgp.com (**米国**) **や** www.pgpi.com (**国際**)**の** Web **サイトからダウンロードして使えます**)**を入手してください。**

   ReadNotify **の認証文書全体を逐一マークしコピーしてください。もし** HTML **文書を検証するなら、先ず文書を画面表示し、次に"ソース** (**を見る**)" **を選んで認証されている文書のテキスト形式の表示** (literal content) **にアクセスしてください。**

   署名検証プログラムを使ってクリップボード上のコンテンツを検証してください。例えば、この為の PGP **製品の主な操作手順は、**PGP=>Clipboard=>Decrypt&Verify **です。この時** ReadNotify **の公開鍵を検索する様要求されるかも知れません。これは自動的に行うことも、ご希望なら弊社の** Web **サイトから手動でダウンロードすることもできます。弊社のキー**ID **は** 0x1D8ADDED **であり、弊社の** ReadNotify TimeStamper Key fingerprint = 7272 F5EA A903 19B5 74E0 A620 4A02 2DFB **です。これらが正確であることを弊社のパブリックキー** "ReadNotify TimeStamper <stamper@readnotify.com>"**で**"Key Properties"**を選択して確かめてください。**

   この結果としての検証した文書 (**または** HTML **ならソースコード**) **を印刷してください。**

   i. **正確に検証されたテキスト文書は以下の様に始まります** (**適切な日付つきで**)：

      *** PGP Signature Status: good
      *** Signer: ReadNotify TimeStamper <stamper@readnotify.com>
      *** Signed: 19/11/2001 4:02:23 PM
      *** Verified: 19/11/2001 4:55:55 PM
      *** BEGIN PGP VERIFIED MESSAGE ***

   ii. **正確に検証された** HTML **文書は以下の様に始ります**：

      <!--

*** PGP Signature Status: good
*** Signer: ReadNotify TimeStamper <stamper@readnotify.com>
*** Signed: 19/11/2001 4:02:23 PM
*** Verified: 19/11/2001 4:55:55 PM
*** BEGIN PGP VERIFIED MESSAGE ***

iii. **どちらの形式でも元のデジタル署名を置き換え、以下のメッセージで終ります**:

*** END PGP VERIFIED MESSAGE ***

署名した文書が何らかの形で置き換えられているなら、それは"正しく検証されません"。- 例: **以下の状態メッセージを受取ります**:

*** PGP Signature Status: bad

注: **検証プログラムが表示する日時情報は特に指定しない限り** UTC **になります。**

5. **この段階で送信したメールが何時送信され、開封されたかを第三者に示せる証拠を印刷しています。この様な文書のソフトコピー** (electronic copy) **を全て保存しておいて、どんな第三者でも上の操作手順を行ってご自身の文書を検証できる様にしておいてください。**
6. ReadNotify **サービスが信頼できるタイムスタンプを生成したことを検証する為に、オプションとして以下の手順を操作して頂けます。**

a. **弊社の署名用** Web **サイト** www.readnotify.com/showsig.asp **にアクセスし、弊社のデジタル認証内に示してあるユニークな連番を**"あなたは ReadNotify のどんな電子署名も参照できます。 ここに連番をいれてください:-"**の下に入力し、**"**署名検索**"**ボタンをクリックしてください。**

b. **ご自身の文書に付けられたのと同じ署名が表示されていることを確認してください。書名された日時情報にもご注意を。**

c. ReadNotify **からの週刊デジタル署名要約報告の対応する部分も参照してください。これは以下の世界中にある何千という** USENET **インターネットニュースグループのサーバ** (alt.computer.security.web-of-trust, comp.security.pgp.announce, alt.security.keydist, gov.usenet.test, aus.net.mail, and chi.mail.) **上に掲載してあります。**
そこには以下の様なサブジェクトラインがあります:-

ReadNotify weekly digital signature summary publication for week ending Sun, 18 Nov 2001 00:00:01 GMT

上のグループの1つである Google WEB によるニュースアーカイブサービスの URL を以下に示します:-

http://groups.google.com/groups?q=alt.computer.security.web-of-trust&hl=en&btnG=Google+Search&meta=

上の手順 2, 3, 4 に従ってこのデジタル署名の広報を印刷、検証、再印刷してください。

d. この週刊要約広報には毎日登録が発生するデジタル署名の要約が載っています。ご利用の個々の認証を含む当該日の要約を印刷、検証、再印刷するには、ご利用の認証連番を含んでいる"ReadNotify weekly digital signature summary publication" の中のリンクをクリックしてください。 例として署名番号9089から9206を表示する URL を以下に示します:-

www. readnotify.com/sigs.asp/show.htm?from=9089&to=9206&sum=9207

この Web ページ表示はそのページの時計での一日の終りにデジタル署名してあるので、マークし、コピーし、検証できます。このページの最後のデジタル認証が USNET ニュースサーバで公開されているものと一致するか二重にチェックしてみてください。

上の手順 2, 3, 4 に従ってこの日刊署名要約を印刷、検証、再印刷してください。

以下は ReadNotify の認証メールとデジタル署名に関する一般的な質疑応答です。これはこの技術資料の法廷での取り扱いの手助けになります。

Q: ReadNotify のタイムスタンプは偽造、変更からどの様に防護していますか？

A: ReadNotify の認証メールは全て、それが何時処理されたか（メールの場合、それは弊社のサービスがメールをインターネットに送信した時刻）を示すタイムスタンプを含んでいます。 タイムスタンプはユ

ニークな連番も含んでいます。この連番は認証処理を行う度に1ずつ増加します。例えば、認証番号 5678 は認証番号 5679 の前、認証番号 5677 の後に作られました。ReadNotify が作成したデジタル署名に関するご説明は www.readnotify.com/postcert.asp で、何時でも誰でも参照して頂けます。タイムスタンプは毎日署名され、各日の署名を更に署名したものが毎週何千というインターネットサーバ上で公開されています。

ReadNotify のタイムスタンプは変更できません。変更するとそのデジタル署名が後で検証できなくなるからです。

ReadNotify のタイムスタンプは、送信者が弊社のサーバにアクセスして日時情報を書き換えることが出来ないので偽造できません。更に、弊社のサーバの日時情報を変更しようとすれば（たとえそれが瞬時であっても）必ず露見します。公開した認証の連番の順番が日付の順番と対応しなくなるからです。時間情報は、逆方向に変更しようとしても、その前の認証との順番がそれによって狂ってしまうので不可能です。（時間を変更しようとした時点で、その前の認証が既にサービスの他のユーザに提供され、ており、その時間で署名され、オンラインで公開される、ということをご記憶ください） 同じ理由で、時間情報は順方向にも変更できません。時間を偽造しようとした人が認証情報の受領者やニュースサーバ全てにアクセスして偽造した時間に合わせる様に変更することは絶対にできないので、偽造した時間は常に露見します。

ReadNotify のタイムスタンプは偽造できません。タイムスタンプ文書は特種なパブリックキー指紋情報を含んでいるからです。この情報は ReadNotify の署名検証キーだけがアクセスでき、このキーを使って ReadNotify が認証した文書を検証するからです。 弊社のプライベートキーは強力に防護してあり、上で述べたいかなる方法で時間を偽造、変更しようとしても、いかなる場合でも発見されます。

Q: ReadNotify が認証したメールの偽造や書き換えに対する防護はどの様に行っていますか?

A: ReadNotify が認証したメールは全てデジタル署名内にメール本体を含んでいます。 このメール本体を書き換えようとすると必ず"Verify Status" が"bad" 状態になります。その理由はタイムスタンプが偽造、書き換えできないのと全く同じです。

ReadNotify サーバを通して送信しないと検証可能な ReadNotify 認証メールを生成することはできません。しかしながら、他のインターネットメールと同様にメールの送信者が自分のメールの差出人のメールアドレスを変更し、ReadNotify 認証メールを作成し、そのメールを送っていない誰かがそのメールを送った様に見える様に偽造することを防ぐことはできません。この成りすましが発生すると、成りすまされた人に警告が送られることにご注目下さい。何故なら ReadNotify はどの ReadNotify 認証メールに対しても（本当の送信者ではない）メールに指定された送信者に対して「送達証明」を返送するからです。

Q: デジタル署名とは何ですか?

A: デジタル署名は複雑な数学的なアルゴリズムで署名対象物の内容を処理して生成したものです。(ここではそれはメール、そのヘッダー、添付した認証情報を意味します) デジタル署名は保護された秘密の鍵情報の持ち主だけが作成できます。 保護された個々の秘密の鍵情報に対して対応する公開鍵情報があり、これを使って誰でもデジタル署名が検証できます。 この2つの特別な鍵情報を使うと、例えば銀行の金庫室の一部の中が見えてしまうことも有り得ます。片方の鍵情報だけでは金庫室を施錠できますが、それだけでは金庫室は開錠できません。一方、他の鍵情報だけでは開錠はできますが施錠はできません。これがデジタル署名の背景になっている公開鍵、秘密鍵理論です。秘密鍵だけがデジタル署名を作成でき、公開鍵だけがそれを検証できます。

デジタル署名を使うと、誰かまたは何者か (弊社の場合それは ReadNotify 認証メールサービスです) がある物に署名できて、それは後で誰でも検証できる、ということが可能になります。

通常の紙の上に書いた署名と違って、デジタル署名は偽造に対する防護になります。デジタル署名を使って署名した文書をいかなる方法を使っても一旦改変するとその署名が読めなくなるからです。(更に、署名した人意外は秘密鍵を知らないので、その持ち主だけがそれを使って署名できます)

Q: 私が送信したオリジナルのメールと送達証明、開封証明はどういう関係にありますか？

A: 以下に弊社の認証がどの様に“関係し合って”検証可能な証拠の偽造できない追跡情報を生成するかをご説明します:

1. オリジナルのメールはユニークなメッセージ ID を含んでいます。(メッセージ ID は通常使っているメールプログラムが挿入します。送信したメールを“送信済み”フォルダに入れ、どの様なメッセージ ID がオリジナルのメールに付けられたか見ることができます)
2. 弊社はメールを“認証“する時、メールに新しいユニークな識別子 (”スタンプ“と呼んでいます) を作ります。弊社はこのスタンプ用に MD5 チェックサムを作り、メールの後ろに認証情報を付加します。この認証情報はメッセージ ID と弊社のスタンプの MD5 チェックサムを含みます。(これを"ReadNotify 参照"と呼びます) 次に弊社はメール本体のデジタル署名を行います。(このデジタル署名はメッセージ ID と ReadNotify 参照を含みます。ところで、この時点でメール本体はメールヘッダーのコピーも (HTML コメントの内側に) 含みます。このヘッダー全体もデジタル署名されます。)
3. 弊社はこの“認証”したメール本体を“送達確認”として送信者に送ります。この署名はお好きな OpenPGP プログラムを使って法廷での使用の準備として検証して頂けます。
4. 弊社は受信者の追跡用のメール変更の一部としての弊社のユニークなスタンプを、認証したメールのヘッダーと本体内に (署名後に) 追加し、送信します。(スタンプは暗号化してあり、推測等では解読できません)

5. この時点 - 送信者と受信者は新規に認証したメール本体の同じコピー（とオリジナルのヘッダー）を持っている – で、受信者のコピーは弊社のユニークなスタンプを基にした追加の追跡データを含んでいます。受信者はスタンプの MD5 チェックサムを持っていますが、受信者は何れがスタンプなのか分かりません。（従って受信者は開封確認を偽造することは出来ません。） 認証メールが宛先不明の場合、弊社は宛先不明メールを送信者に返す前にスタンプを削除し、送信者にはスタンプの存在が絶対分からない様にし、誤った開封確認報告が発生しない様にします。
6. 次に受信者はメールを開封しますが、この時点で弊社の追跡システムはスタンプを含む追跡情報を受信します。ここで存在するのはこのユニークな暗号化スタンプを中に含んでいる、配信した認証メールだけです。従って、弊社はこの情報が弊社に戻ってきた時には受信者メールを表示したことが分かると確信を持って言えます。弊社は次にこの追跡データをパッケージにして送信者に開封通知として送信します。
7. この開封証明はオリジナルのユニークなメッセージ ID とスタンプ MD5 チェックサムを（メールの後ろの"認証"ボックスに）含みます。弊社が作成したこの新メールはタイムスタンプされデジタル署名され、従って新しい認証用連番を含みます。弊社は受信者がメールを開封したという確実な事実を報告する為に、他の多くの詳細な追跡情報（受信者の IP アドレス、PC の詳細、ISP の詳細等）を報告に含めます。

メールとその開封確認の関係を多忙で技術に詳しくない法律家に説明する最も容易な方法は、認証したメールのオリジナルなメッセージ ID が関連する認証文書内の“認証”情報を表示する場所全てに現れるということ、オリジナルのメールが、正当な受信者以外には誰もアクセスしなかった"ReadNotify 参照"のプレインテキストを経由して開封証明に紐付けされていることを示すことです。更に、開封証明が開封時の受信者の IP、ISP、場所、その他の情報を記録していることを示すことです。これは（A）受信者が現実にメールを読んだ者であること、（B）その結果受信者のコンピュータ内の認証メールにアクセスしない限り誰にも（例えば送信者にも）偽造できないことを特定する助けになります。

署名は全て OpenPGP を使って検証しているので、上記のどれも不正に書き換えされることはありませんでした。

Q: ReadNotify 社はどうして自分で認証メール検証サービスを提供しないのですか?

A: 弊社は検証サービスを提供しません。 検証サービスを提供すると弊社は“偽りの”検証ができることになります。送信者は信頼できる OpenPGP 互換の暗号化製品を使って認証を検証する必要があります。これにより弊社の認証に対して誰にも不正を働くチャンスが無いことが確実になります。

弊社は御自分の認証メールを全て検証し、その結果を法廷での訴訟用の資料として印刷する様お勧めします。署名の正当性が裁判官に信じてもらえない場合は（地元の学校か大学などの、訴訟とは無

関係の）数学者に非対称の暗号手法がどう機能するかについて、そして何故提出したメールが全て認証資料内で示している時点でのオリジナルなものであるかを説明してもらっても良いでしょう。

以上