分散ストレージシステムにおけるノード認証方式 (Node to Node Authentication System for Dispresed Storage)

神田 章継(Akitsugu Kanda) ,石井 陽介(Yosuke Ishii) ,
薗田 浩二(Koji Sonoda) ,岩嵜 正明(Masaaki Iwasaki)

(株)日立製作所 システム開発研究所
(System Development Laboratory, Hitachi Ltd.)

1. はじめに

現在のストレージシステムでは、ファイルのバックアップ等を目的としてレプリケーションやマイグレーション等の処理を SAN(Storage Area Network)や Ethernet 等のネットワークを経由して行っている。しかし、上記ネットワークは接続範囲が広大化することにより、もはやセキュアな区間とは言い難くなり、なおかつシステムの管理範囲も不明瞭なものとなる。

そこで本稿では、ストレージのセキュリティ管理に着目し、そのなかでも特に「なりすまし」に関わる脆弱性に注目したストレージ特有の「認証」基盤について検討した。

なお、現在セキュリティ管理が重要視されているネットワークは主に IP ネットワークであるため、本稿でも上記の検討対象を IP 対応型ストレージシステムに限定する。

2. セキュリティ上の課題と対策

ネットワークを介して接続されたストレージ同士での情報交換(例えばファイルのレプリケーションやマイグレーション等)は、通信区間がセキュアであるという前提で行われているというのが現状である。しかし、ネットワーク（特に IP ネットワーク）は広域化によりもはやセキュアなものではなくなり、これに伴い同一の管理者が一元的にシステムを管理することも困難になってきている。従って、ストレージシステム上の各ノードでセキュリティ対策を実施することは必須である。

ストレージシステム上でのセキュリティ上の課題として、以下の事項が主に考えられる。

① なりすまし
悪意を持った管理者により、ファイルのレプリケーションもしくはマイグレーションする先のストレージ装置のなりすましを構築される。

② 通信路上での盗聴、改竄
ファイルのコピー中（通信中）に Sniffing 等により情報が盗聴もしくは改竄される。

③ 既存プロトコルの脆弱性を突いた盗聴
既存のファイル共有プロトコルの脆弱性をついてストレージ装置がクラッキングされ、情報を盗聴される。

これらの課題のうち、盗聴/改竄に関しては既存の暗号化技術及びハッシュチェック技術を組み合わせることにより対策を講じることが可能であるが、なりすまし対策に関しては既存技術との組合せだけでは不十分であると考えられる。そこで、本件がストレージセキュリティ対策における重要項目と位置づけ、次章以降で当対策に着目したセキュリティ技術について考察する。

3. なりすまし対策

IP に対応するストレージシステムでレプリケーションやマイグレーションを行うための手段としては、今後以下のプロトコルを活用するケースが想定される。

①NFS…UNIX 系 OS 等でサポートしているファイル共有プロトコル
②HTTP…Netspape や InternetExplorer を利用してコンテンツの受け渡しを行うプロトコル。
③HTTPS…HTTP と同様の機能を持ち、なおかつ暗号化や PKI 等のセキュリティ機能を搭載するプロトコル。
④FTP…ファイルの送受信を行うプロトコル
⑤CIFS…MicroSoft 社が提供するファイル共有プロトコル
⑥iSCSI…SCSI コマンドを利用して情報の送受信を行う技術であるが、これらのコマンドは IP ネットワークで通信を行うため IP パケットでカプセリングされる。

一方、上記のプロトコルで実現できるなりすまし対策については以下のように考察される。

① NFS,HTTP,FTP,iSCSI
通信相手の信頼性を検証する手段は存在しない。

② CIFS
「ドメイン参加型」の構成を取ることにより、ドメイン参加時に管理 ID による認証を実施することができ、相手の信頼性を検証することが可能となる。しかし、ID そのものが部外者に漏洩する危険性が著しく高い。

③ HTTPS
PKI の機能が搭載されているため、相手に証明書を要求して信頼性を検証することが可能である。しかし、一部のストレージシステムの管理者が変更になった場合等においては、これらの証明書が漏洩する危険性がある。

上記の考察から、いずれのプロトコルに関しても管理者の異なる IP ストレージ間でファイルのレプリケーションやマイグレーションを行うにあたり、十分ななりすまし対策がなされているとは言えない。従って、上記に変わる強固な認証方式を活用して IP ストレージシステムを運用することは効果的であると考えることができる。

※PKI(PublicKeyInfrastructure:公開鍵認証基盤)
第三者機関がそれぞれの管理者向けに X.509 フォーマットを活用してそれぞれに公開鍵証明書を発行し、お互いが確実に信頼できる相手であることを保証する技術。

4. IPアドレス認証型PKIノード認証方式

前節で記述した方法の中では PKI を活用した方法が最もセキュリティ上安全な方法であると考えることができる。しかし、それでも一部のストレ

ージの管理者が異動もしくは退職し、既存の証明書を悪用して IP ストレージシステムを運用することができてしまうため、PKI を適用するだけでも十分とはいえない。
　そこで、本稿ではこのような問題点も併せて解決する手段について提唱する（以降新方式を「IP アドレス認証型 PKI ノード認証方式」と呼ぶ）。

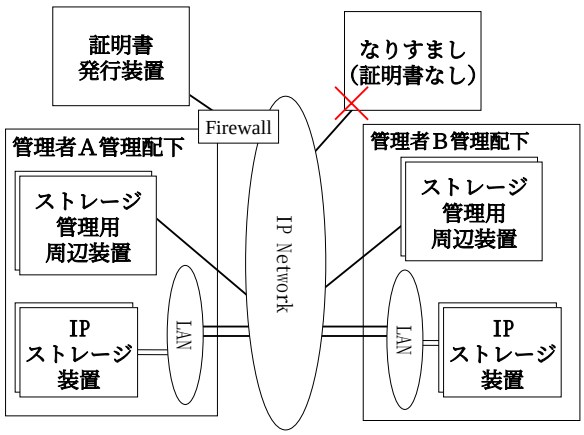

図１：基本ネットワークモデル

　図１は、IP アドレス認証型 PKI ノード認証方式を活用する場合における基本的なネットワークモデルである。管理者が異なる IP ストレージ装置に対してデータのレプリケーション等を行う場合は図２のパケットフォーマットを活用して事前にお互いの証明書の交換を行い、相手が信頼できるかどうかを検証する。なお、レプリケーション先の IP アドレスはそれぞれの装置内に事前に登録されている。具体的な検証条件は以下の通りである。

① 証明書を取得した証明書発行装置が互いに同一のものであること。
② 証明書が有効期限期間中のものであり、なおかつ失効されていないこと。
③ お互いの IP ストレージが、証明書内に記載されている IP アドレスと同一のアドレスを使用して運用されていること。
④ お互いの署名が証明書発行装置によって認可された署名であること。

ＩＰ ヘッダ	TCP /UDP ヘッダ	ID ペイ ロード	証明書 ペイ ロード	署名 ペイ ロード

図２：証明書検証用 IP パケット

※ID ペイロードには、IP ストレージシステムを運用するために必要な IP アドレス情報を付加する。
※証明書ペイロードには、証明書発行装置から取得した公開鍵証明書を付加する（この公開鍵証明書は証明書発行装置の秘密鍵で暗号化されている）。
※署名ペイロードには、自身の署名を付加する（この署名は証明書発行装置によって認可された鍵により暗号化されている）。

＜検証方法＞
相手から図２のパケットを受け取った IP ストレージ装置では、以下の手順に従って検証を実施する。
①証明書の中身が改竄されていないかをどうかをチェックした後、証明書発行機関の公開鍵で復号化する。復号化に成功したら同一の証明書発行装置から証明書を取得した相手とみなす。
②図２の送信用パケットの IP ヘッダ上に付与される送信元 IP アドレスと ID 及び登録されている IP アドレスが同一のものであるかを確認する。
③送られてきた署名が証明書に付与された公開鍵で復号することができるかどうかを確認する。復号化に成功したらデジタル署名が本人のものと見なす。

※上記の検証全てに成功したら信頼できる相手とみなす。途中で検証に失敗した場合は、その時点で相手との通信を拒否し、セッションを強制切断する。
※反対方向の検証も上記と同様の手順で行う。

5. 本方式を活用する効果

異なる管理者が保有する IP ストレージにファイル等の情報をレプリケーションする場合、既存のプロトコルを活用するケースでは、セキュリティ上以下の問題点があった。
①「ドメイン参加型」の構成を取ることにより、ドメイン参加時に管理 ID による認証を実施することができ、一応相手の信頼性を検証することが可能となるが、ID そのものが部外者に漏洩する危険性が著しく高い。
②PKI の機能を利用することにより、相手に証明書を要求して信頼性を検証することが可能であるが、一部のストレージシステムの管理者が変更になった場合等においては、これらの証明書が漏洩し、悪用される危険性がある。

一方、IP アドレス認証型 PKI ノード認証方式では、上記の問題点を下記の手段で解決できる。
①管理者が変わったときに証明書を失効することができるため、共通のキーワードを活用する方式と比べて管理者が変更されたときの移行、引継ぎが容易である。
②正当な IP アドレスを付与しなくては運用することができないため、仮にシステム内の運用上有効な証明書を横領できたとしても異なるセグメントになりすましノードを配置することができない。

　以上のことから、本方式により IP ストレージシステム運用することで「なりすまし防止」に効果をあげることができる。
　なお、IP アドレス認証型 PKI ノード認証方式は証明書の交換などの処理を全て IP のレイヤで行うため、第３節であげたいずれの技術とも容易に併用することが可能である。

6. おわりに

　データのバックアップ等を目的として情報交換を行う際の IP ストレージシステムのなりすまし行為に対する対策として、高信頼なノード認証方式を検討した。今後は、本件に関する実装方式等を考察していく予定である。

7. 参考文献

Internet X.509 Public Key Infrastructure Certificate and CRL profiles(RFC2459)
