R&D ホットコーナー ソリューション

NTTグループ向けセキュアファイル転送サービス

NTT情報流通プラットフォーム研究所[†1] / NTT総務部門[†2] / NTT研究企画部門[†3]

阿部 裕文（あべ ひろふみ）[†1] / 伊坂 広明（いさか ひろあき）[†1] / 森下 幸治（もりした こうじ）[†1] / 長田 孝彦（ながた たかひこ）[†1] /
宮城 達也（みやぎ たつや）[†2] / 松岡 正人（まつおか まさと）[†2] / 川村 亨（かわむら とおる）[†3] / 松澤 寿典（まつざわ ひさのり）[†3]

NTTグループ会社間および取引先との間での顧客情報，設備情報，経営情報などの重要情報や大容量データなどの情報流出対策を目的に，大規模セキュアファイル流通基盤システムを用いたoccrueサービスを2009年１月より開始しました．

セキュアファイル転送サービスの必要性

NTTグループは，顧客情報，設備情報など，さまざまな個人情報・経営情報をやり取りしながら幅広い事業を展開しています．また，NTT研究開発部門においては，特許情報やシステム開発・維持管理等にかかわる守秘対象の情報も多く扱われています．一方，情報流通の代表的なツールとして電子メールがあります．これは，利便性に優れ，世界各国どこへでも送信することが可能な反面，誤送信による情報流出，平文送付による盗聴など，セキュリティ脆弱性が大きな課題です（**図１**）．また，メールで添付するファイル容量は数MB程度に制限されることが一般的です．それを超えたファイルを流通する場合には，インターネットのサービスを利用することもあります．このようなサービスの中には安全性が未確認で，情報流出の危険性をはらむ場合もあります．さらに，メール添付でも暗号ツールやOfficeパスワード等で暗号化したうえで送信する例も増えてきていますが，解読ツール等により簡単に復号できる危険性があります．

NTT情報流通プラットフォーム研究所では，2005年度より大規模セキュアファイル流通基盤システム（SSS：

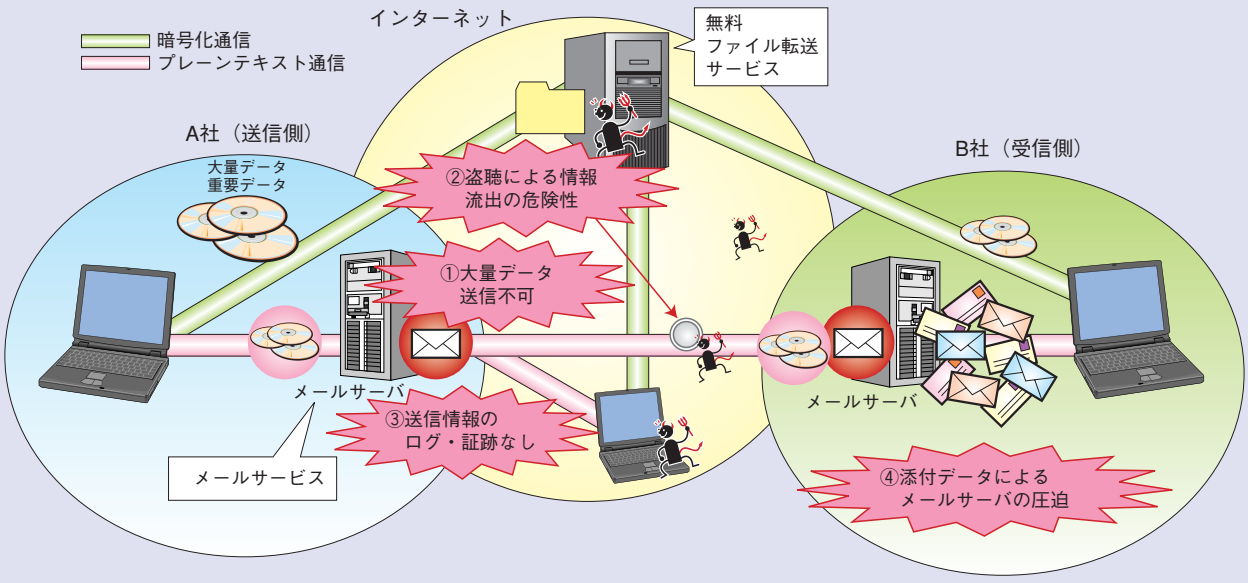


図１　電子メール，インターネットファイル転送サービスの課題

Scalable Secure file Sharing System）の開発に着手してきました．これは，ユーザが特に意識せずに，送受信ユーザの認証，送信データの暗号化，クローズな流通経路の限定が可能で，100 GBまでのファイル送受信を行うことができます[(1)]（**図2**）．

NTTグループ会社およびその取引先で安全なファイル流通を実現することを目的として，NTTコミュニケーションズ，NTTコムウェアの協力により，NTTグループIT基盤サービス「occrue（オクル）」サービスを開始しました．ここでは，その特徴的な機能，サービス内容，共通ルールについて紹介します．

セキュアファイル転送に対する内部統制

従来よりSSSはエンドユーザ間で安全・確実なファイル流通を指向（図2）してきました．これは，エンドユーザにゆだねたセキュリティ施策ですが，各社のセキュリティ管理者がエンドユーザや組織のポリシーをワンストップで管理できるよう，内部統制の観点を拡充しました（**図3**）．これにより，エンドユーザはセキュリティ管理者が規定したポリシーを送信前に自動的に読込み，そのポリシーに合致した範囲でのセキュアファイル転送が可能となります．特に，情報流出のリスクがあるゲスト（主に取引先や顧客等）への送信時や，社外へ送信する情報の証跡管理を実施する際は，蓄積手段を規定することにより流通状況を管理することが可能となります．

occrueサービスと共通ルール

occrueサービスの概要を**図4**に示します．本サービスはNTTグループ共通情報ネットワーク上にSSSサーバを配置し，ネットワークを含めたエンド・ツー・エンドで安全な情報流通を可能とします[(2)]．

NTTグループ会社間を中心としたセキュアな情報流通を図るため，occrueアカウントを登録する正規ユーザ（NTTグループ社員，協働者）とその都度テンポラリなoccrueアカウントを発行することによって一時的にoccrueを利用可能なゲストユーザ（主に取引先，顧客等）を定めました．前者はNTTグループ共通情報ネットワークを経由した接続となりますが，本人認証の強化を目的として，クライアント証明書による認証を可能としています．一方，後者はワンタイムパスワードによるインターネット経由の接続を可能とします．

occrueサービスでは，電子メールのドメインのような概念としてルートグループを各社ごとに払い出し，それにより会社間相互接続，アカウント管理，送受信許可権限，契約などの単位として運用します．グループにはルートグループとサブグループがあり，サブグループはルートグループ配下に階層的に定義できます．本サービスでは，ルートグループ間はNTTグループ会社間の流通向けにフルメッシュ接続で運用しますが，サブグループは各社の協働会社とのローカルな接続を想定しており，各社のポリシーで接続ルールを規定可能となっています（**図5**）．

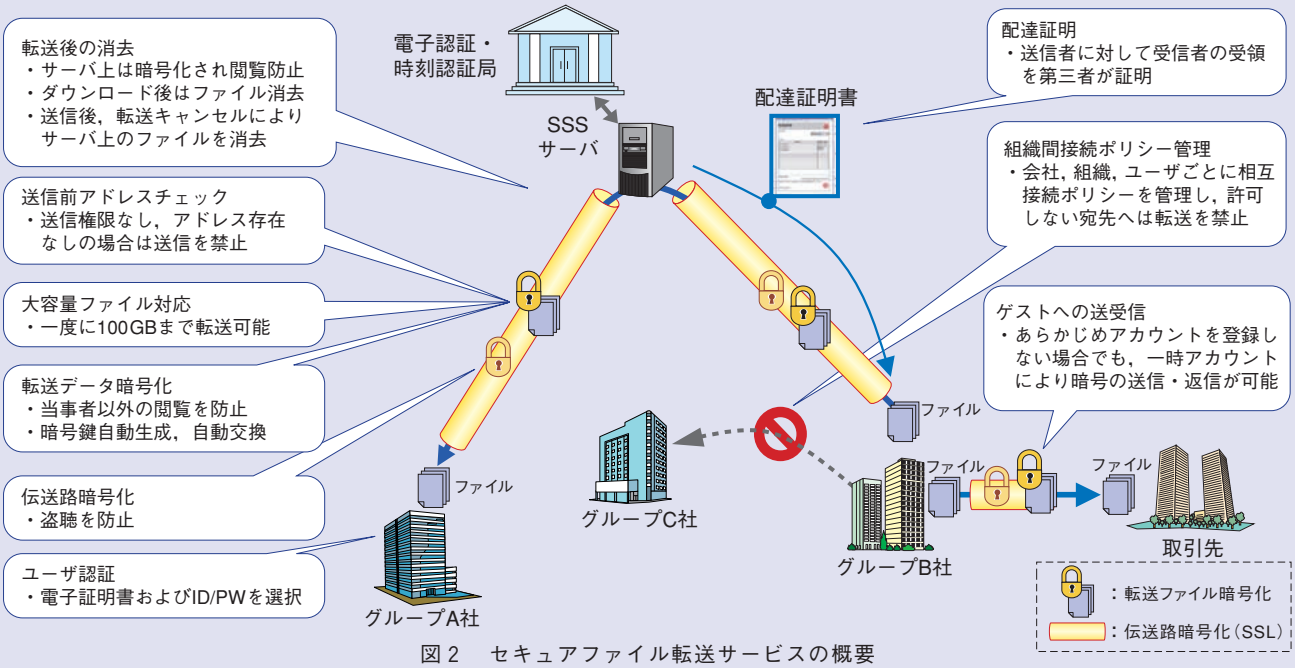
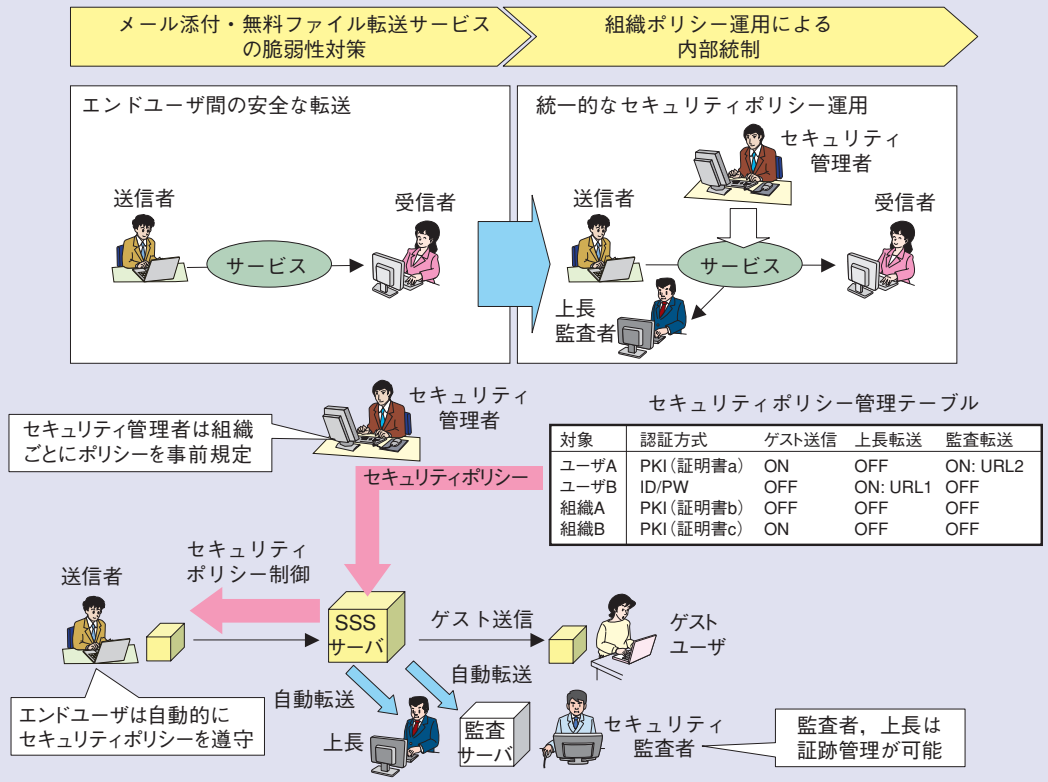


図2　セキュアファイル転送サービスの概要

また，本サービスのユーザアドレスは，ユーザ名とフル・グループ名の２つに分けて付与します．前者はユーザが使用するメールアドレスを定義します．また，後者は会社ごとに割り当てたルートグループ，またはルートグループ配下に別途定義したサブグループとともに定義します（**図６**）．



対象	認証方式	ゲスト送信	上長転送	監査転送
ユーザA	PKI（証明書a）	ON	OFF	ON: URL2
ユーザB	ID/PW	OFF	ON: URL1	OFF
組織A	PKI（証明書b）	OFF	OFF	OFF
組織B	PKI（証明書c）	ON	OFF	OFF

図３　内部統制強化への拡張

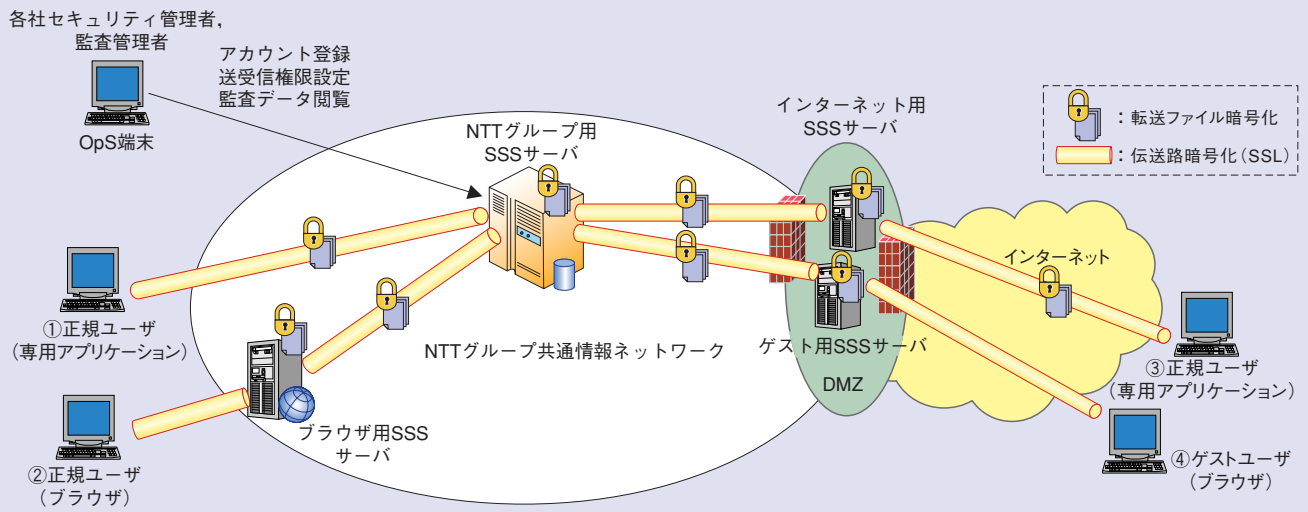


図４　occrueサービスの概要

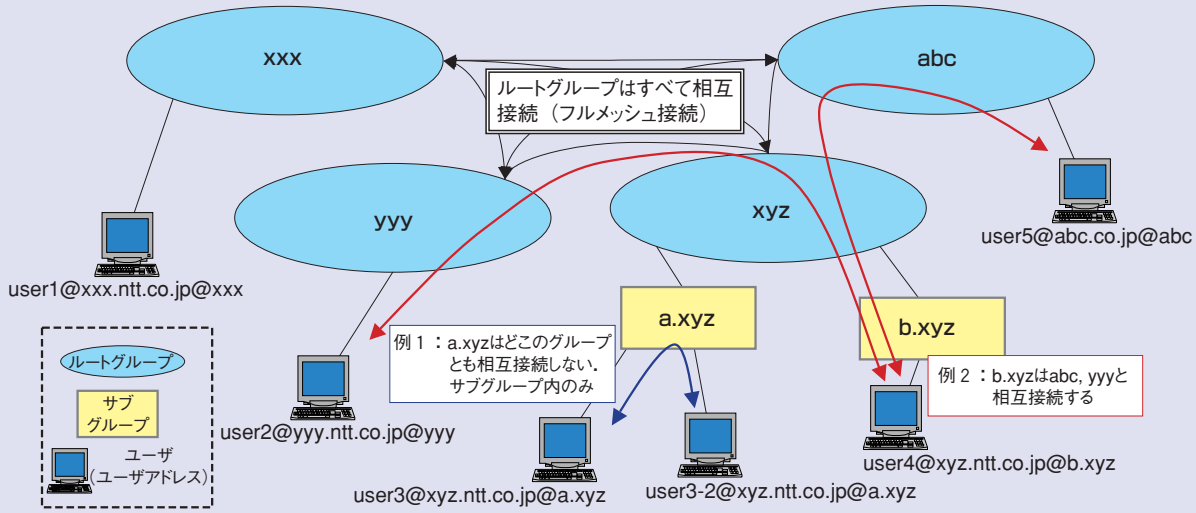


図５　NTTグループ会社間相互接続のイメージ

セキュアファイル転送ユーザアドレス基準

セキュアファイル転送に使用するユーザアドレスは以下に定めます．

＜ユーザ名＞@＜フル・グループ名＞
①　②

①ユーザ名　：ユーザ（クライアント）を一意に識別できる「セキュアファイル転送ユーザ名」です（ユーザが使用するメールアドレスを使用します）．または，同報通信で使用する「エイリアス名」．
②フル・グループ名：セキュアファイル転送の情報管理，ファイル送受信範囲，ルーチングを規定するグループ名です．ルートグループそのものの場合と，その配下にサブグループを設定する場合があります．

例：user1@xxx.ntt.co.jp@xxx
①　②

例：user4@xyz.ntt.co.jp@b.xyz
①　②

注意点：ユーザアドレスは１ユーザで１アドレスを付与することとします．

図６　ユーザアドレス構造

今後の予定

今後は，グループ各社へのさらなる利用拡大によりセキュリティ向上を図るとともに，市販メーラと連携したアプリケーションを開発する予定です．具体的には，到着通知メールを受信してからSSSクライアントを起動するなどのユーザの手間の軽減や，メーラとSSSクライアントで二元的に管理している送受信データを１つに統合することにより，さらなるユーザビリティ向上を図っています．

■参考文献

⑴　吉田・谷川・高屋・森下・藤原・牛島・武田：“大規模セキュアファイル流通基盤システム（SSS），”NTT技術ジャーナル，Vol.18，No.8，pp.36-39，2006.
⑵　occrue事務局：“occrueサービス仕様書1.0，”2008.

（上段後列左から）森下　幸治/ 伊坂　広明
（上段前列左から）阿部　裕文/ 長田　孝彦
（下段左から）川村　　亨/ 松澤　寿典/
宮城　達也/ 松岡　正人

occrueサービスは3月末時点で，NTT持株会社を中心にNTTグループ会社8社が利用を開始しており，大容量ファイルを簡単かつ安全に送信する手段としてご好評をいただいています．皆様のご利用をお待ちしています．

◆問い合わせ先

NTT情報流通プラットフォーム研究所
第二推進プロジェクト
TEL　0422-59-6670
FAX　0422-59-3885
E-mail　sss-support@lab.ntt.co.jp