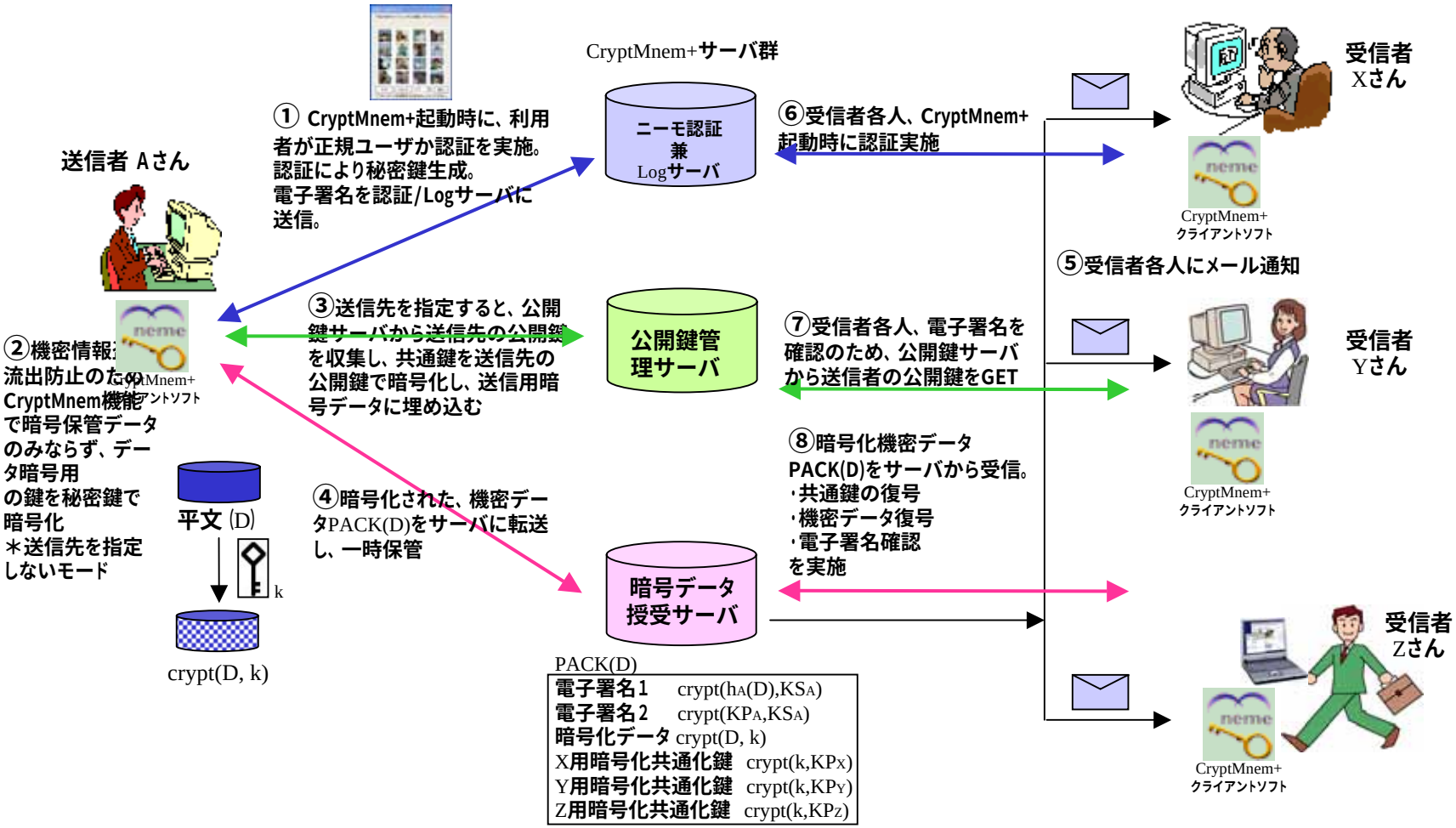
CryptMnem+ セキュアデータ伝送システム

クリプトニーモ＋ による秘密鍵の厳重管理を用いて、PKIベースの安全なデータ伝送を実現
「クリプトニーモ＋」 ＝ 「ニーモニック認証」 ＋ 「秘密鍵管理」 ＋ 「ハイブリッド暗号」

SSLやIPSecを信頼して利用できない環境でも安全にデータを送受信可能



概　要

・クリプトニーモ＋ による秘密鍵の厳重管理を用いて、PKIベースの安全なデータ伝送を実現
　「クリプトニーモ＋」 ＝ 「ニーモニック認証」 ＋ 「秘密鍵管理」 ＋ 「ハイブリッド暗号」

・ CryptMnem+アプリ ⇔ CryptMnem+サーバ群間のアプリ層での暗号通信により、SSLやIPSecすら信頼して利用できないネット上でも安全にデータを送受信可能　(SSL, IPsecとの併用も問題なく可能)

・ニーモニック認証 (サーバ) により、CryptMnem+アプリ起動者が、本人である事を検証可能

・クリプトニーモ (ニーモニック認証　ローカル＋秘密鍵生成) によるOn the flyの秘密鍵生成技術により、必要時にのみ秘密鍵を本人認証から生成し、常態として秘密鍵が存在しない安全な状況を実現

・CryptMnem+鍵管理サーバによる、ユーザアカウントと公開鍵管理により煩雑な鍵管理を解放

・CryptMnem+鍵管理サーバの柔軟なユーザ/グループ機能により、ユーザの階層設定が可能
- 一般ユーザ, グループ･リーダ, スーパーユーザの3レベルを設定可能
- グループ･リーダーはグループ･メンバー宛の暗号データはすべて復号可
　送信先は UserName@GroupName で指定
- スーパーユーザー (CrypytMnem+システムを経由するすべての暗号データを復号可能)
　(スーパーユーザの権限分散化は次期課題)
- ユーザには複数のタイトル属性 (例えば、職責タイトル, 専門タイトル等) を設定可能
- グループは、ユーザアカウントあるいは、タイトルで設定可能
　(タイトル設定機能により、人事異動の際のアカウント管理の手間を大幅に削減できる)
- ユーザは複数のグループに所属可能
- グループは階層定義可能

・CryptMnem+データ授受サーバにすべての授受データを保存
　(保存データの割符分散管理は次期課題)

・CryptMnem+認証兼Logサーバにより、厳重なLog管理を実現
　(CryptMnem+サーバ群のHA性は、クラスター等の別途技術にて確保)