（別紙）

【共同検証の前提条件】

図 2 に本共同検証のシステム構成を示します。図中下に示すように、a 系）ネットワークでリファレンス基準値を測定します。次に、b 系）ネットワークで回線暗号装置（COMCIPHER-Q）がもたらす影響を測定します。c 系）ネットワークでは、ハードウェアで物理的に暗号化を行っていた仕組みを、ソフトウェア用に改善した SW-AES を使用した場合の測定をします。最後に d 系）ネットワークでは、QKD 装置から供給された鍵で OTP 暗号化を行い、鍵残量を確認しながら測定を行います。以上の方式で、それぞれの遅延時間、応答時間を測定し、既存システムの通信性能と比較・検討します。本共同検証で測定した遅延時間、応答時間の用語の定義を表 1 に示します。

本共同検証にあたっての前提条件は、以下の通りです。

① 低遅延通信検証（パフォーマンステスト）

実際の証券会社で扱われる注文件数と同程度の量の取引データをアプリケーションによって生成し、遅延時間、応答時間を検証します。

② 大容量データ通信検証（ボリュームテスト）

顧客による取引注文が集中する場合を想定し、上記の取引件数を 80 倍とした上で、遅延時間、応答時間を検証します。

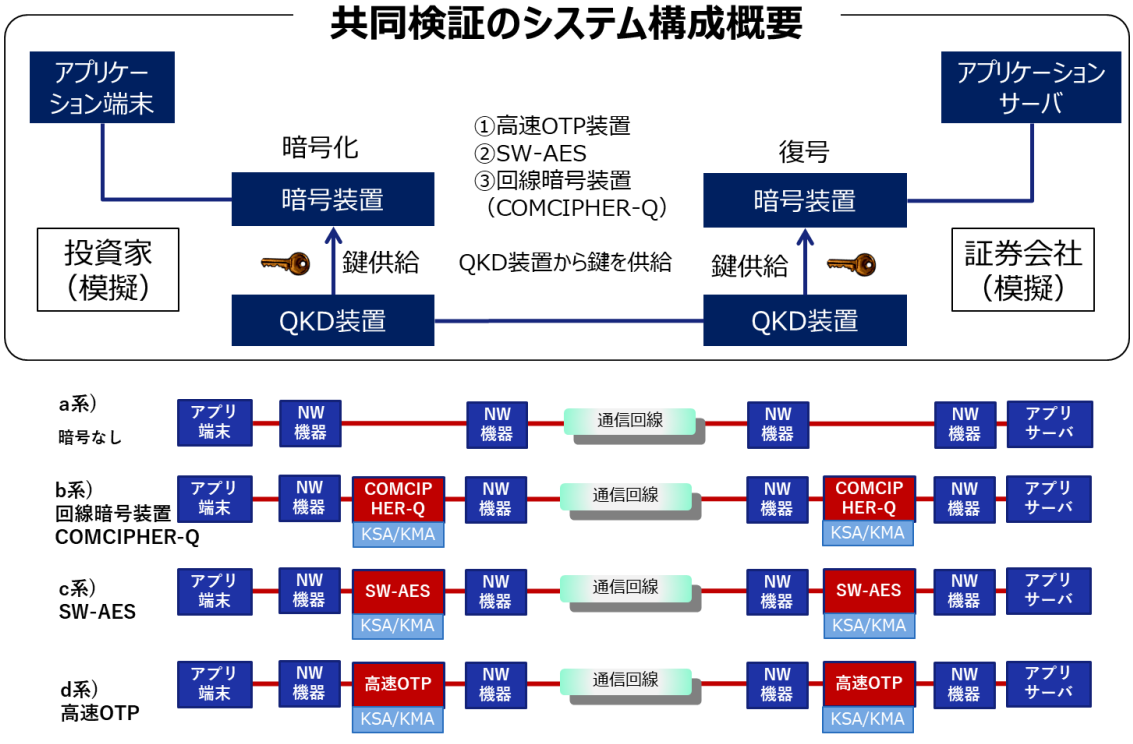

図 2　本共同検証のシステム構成

遅延時間	暗号化なしを基準として、認証局（Certification Authority、CA）などへのドメイン認証の必要ないプロトコル（Transport Layer Security、TLS）を暗号化した場合との差を遅延時間と定義。アプリケーション端末とアプリケーションサーバ間の片道遅延を測定する。
応答時間	アプリケーション端末が問合せメッセージを送信完了した時点（Ts）と、アプリサーバからの応答メッセージがアプリケーション端末で受信され始めた時点（Te）の間隔。（Te-Ts）を応答時間と定義。

表 1　測定のための用語の定義

【共同検証の結果】

検証内容		ネットワーク層の遅延時間測定	低遅延通信検証（パフォーマンステスト10回平均）	大容量データ通信検証（ボリュームテスト80倍）	備考
測定項目		遅延時間	応答時間	応答時間	
回線環境	暗号化なし（a系）	基準（0ms）	1.98 ms	3.60 ms	暗号化なしでリファレンス基準値を求める測定
	COMCIPHER-Q（b系）	0.02 ms	2.04 ms	4.37 ms	ハードウェア系暗号装置がもたらす影響を測定
	SW-AES（c系）	0.22 ms	2.32 ms	4.99 ms	ソフトウェア系暗号装置がもたらす影響を測定
	高速OTP（d系）	0.22 ms	2.34 ms	4.72 ms	OTP暗号化する装置がもたらす影響を測定

表 2　共同検証の結果（パフォーマンステスト及びボリュームテスト）

最初に、メッセージ伝送フォーマット（FIX フォーマット）を模擬したアプリケーションを使用しない状態で、暗号化なし（a 系）を基準として、3 種類の暗号方式（b,c,d 系）とを比較したところ、ミリ秒（0.22ms）以下の範囲の遅延時間に収まり、要求事項の通信性能をネットワーク層以下で有していることを確認しました（表 2）。

①低遅延通信検証（パフォーマンステスト）の結果から、量子暗号通信を適用しても基準となる暗号化なし（a 系）の結果と比較して遜色のない通信速度が維持できることが確認できました。

表 2 から、①低遅延通信検証（パフォーマンステスト）において、3 種類の暗号方式（b,c,d 系）を用いた場合と、暗号なし（a 系）の場合の遅延時間を比較した結果、い

ずれも 1ms 以下の遅延に収まり、暗号方式の違いを問わず、安定した応答時間でアプリケーションが稼働できていることを確認しました。

②大容量データ通信検証（ボリュームテスト）の結果から、大量の株式取引が発生した場合においても暗号鍵を枯渇させることなく高秘匿・高速暗号通信が実現できることが確認できました。

表 2 から、顧客による取引集中に合せて取引メッセージ件数が増加する場合において、暗号なし（a 系）の場合でパフォーマンステストと比べ応答時間は増加しましたが、同様に暗号化した場合（b,c,d 系）においても、暗号方式にかかわらず、同等程度の増加時間に収まり、それぞれに差異はみられませんでした。その上で、回線暗号装置（COMCIPHER-Q）による暗号方式（b 系）の場合においては、応答時間が暗号化なし（a 系）と比べても 1ms 以下の遅延で収まりました。

表 2 の測定結果については、今後のロングランテストやストレステストの測定時に再検証を行い、再現性や信頼性を高めていきます。特に、今回のボリュームテストの大容量時の注文殺到時間を増加させ、ストレステストと併せて応答時間、スループットに与える影響を検証していきます。

以上の検証データを基に、上記 3 つの暗号方式を組み合わせることによって、金融アプリケーションを高速暗号化できる条件を導出していきます。さらに次のステップとして、これらに、非常時対応に備えたメインシステム・バックアップシステム間の経路切り替えを可能とするルーティング機能を備えれば、冗長性が向上します。ルーティング機能については、次回以降の応用検証として並行して準備を進めています。