

S.E.E. (Secure Execution Engine)

解説と応用例

July 03, 2009

Sarion Systems Research

ソフトウェア開発部 永野 雅史



会社紹介

□社名

株式会社サリオンシステムズリサーチ
Sarion Systems Research

□会社代表

山田 剛(やまだつよし)

□住所

〒101-0054
東京都千代田区神田錦町3-23 西本興産錦町ビル14F

□設立

1989年1月31日

□事業内容

- PKIを中心とした認証システムの構築サービス
- アイデンティティ管理ソフトウェアの開発
- ICカード関連製品および発行システムの開発、製造、販売
- システムセキュリティー監査サービスの提供

□提携

- Thales社 nCipher Strategic Alliance Partner



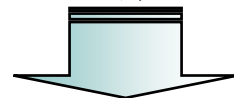
概要

- S.E.E解説と応用例(このセッション)
 - 必要な理由
 - できること
 - 応用例

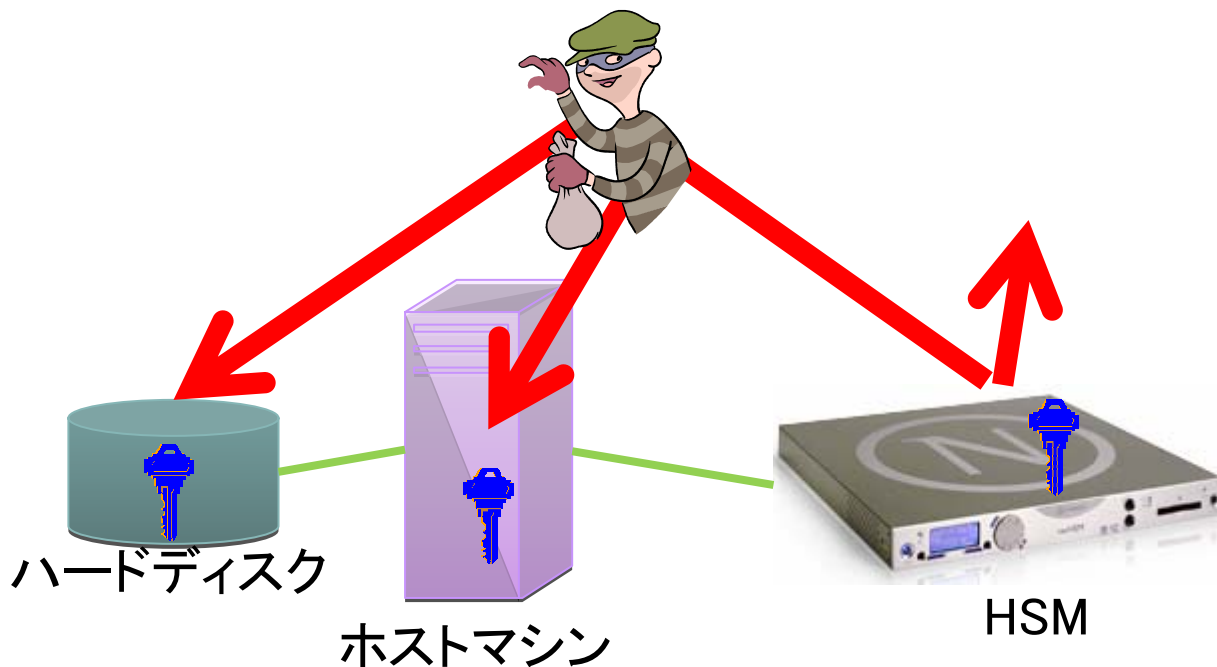
- HSM用ミドルウェアConduit Toolkitの概要と使い方(この後)
 - SEEのプログラミングモデル
 - Conduit Toolkitの機能と利点
 - Conduit Toolkitによる開発の流れ

HSMを導入する理由

- ◆ハードディスクに保存された鍵は持ち出される
- ◆メモリ中に展開された鍵は覗き見される



HSMで鍵を保護する



鍵を保護するだけで十分か？

あなたが利用する情報システムは...

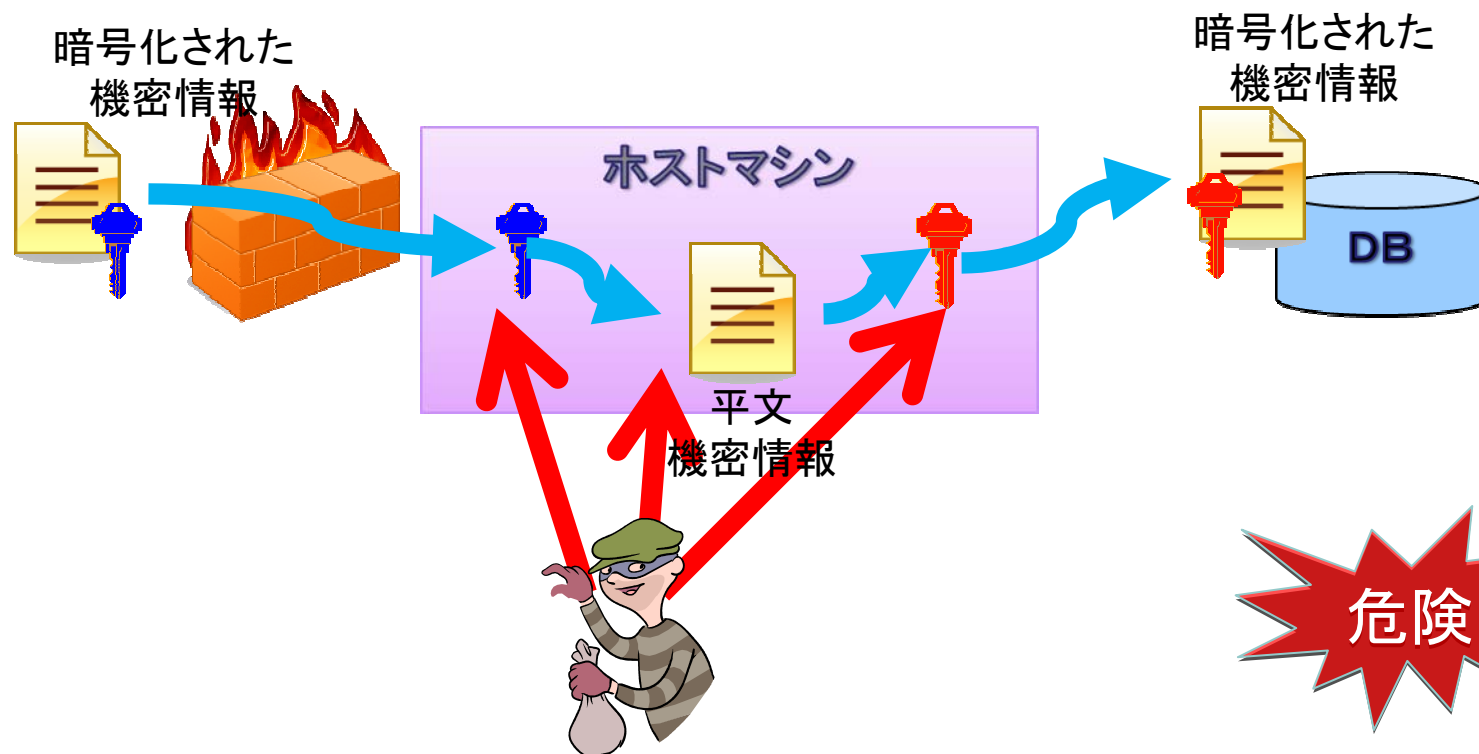
- ユーザのパスワード、クレジットカード番号などのデータは保護されていますか？
 - 内部犯行によるデータ漏洩は？
 - 運用のミス、設定のミス、OSのバグなど、セキュリティホールを利用した不正アクセスがあったら？

- コードの改ざんやトロイの木馬のような攻撃からのコードの保護は？
 - 機密情報ファイルを転送、削除
 - 発注システムにおいて、注文数を書き換える
 - 集計結果の送信先を、攻撃者宛てに変更

セキュアな実行環境が求められる理由

問題例1: 機密情報の漏洩(HSMなし)

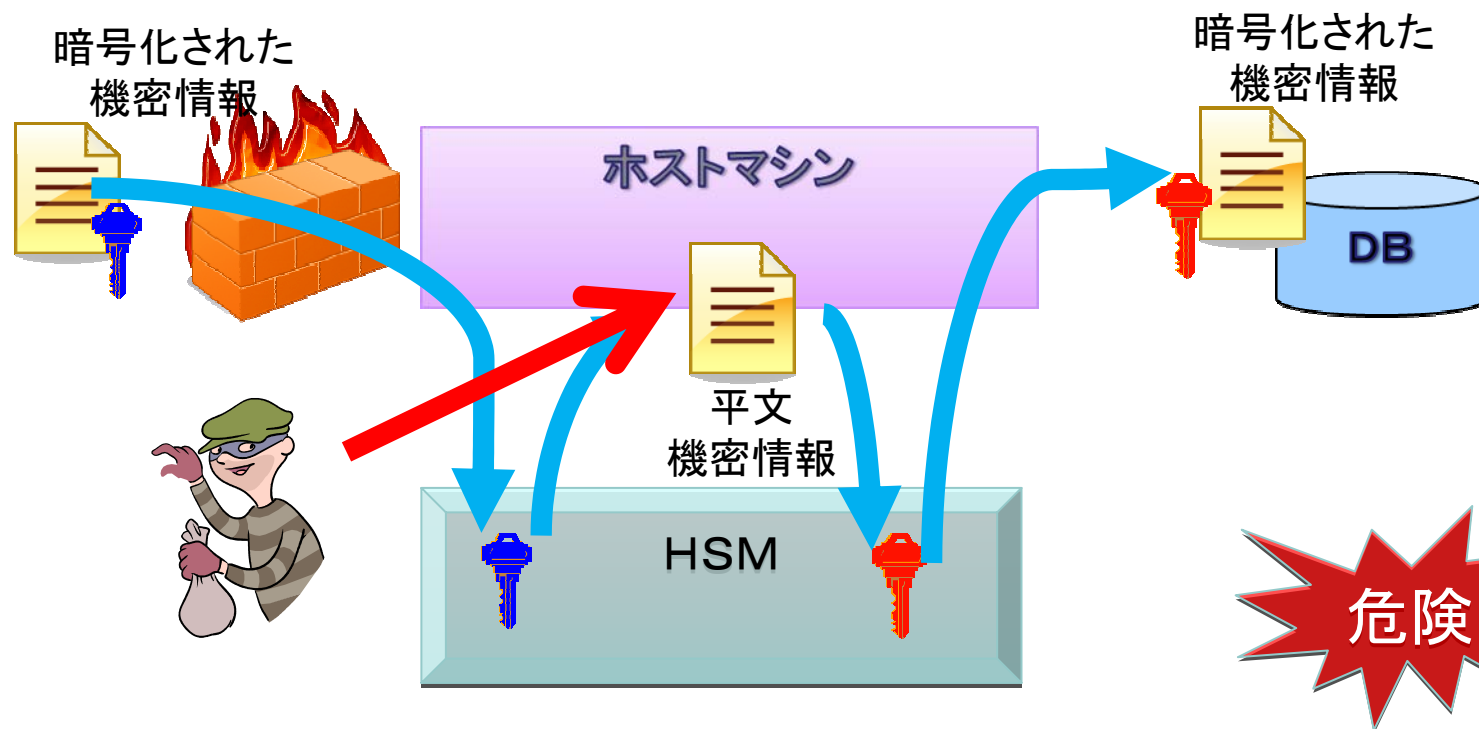
ホストマシン上で、鍵も機密情報も盗まれる



セキュアな実行環境が求められる理由

問題例1: 機密情報の漏洩(HSMあり)

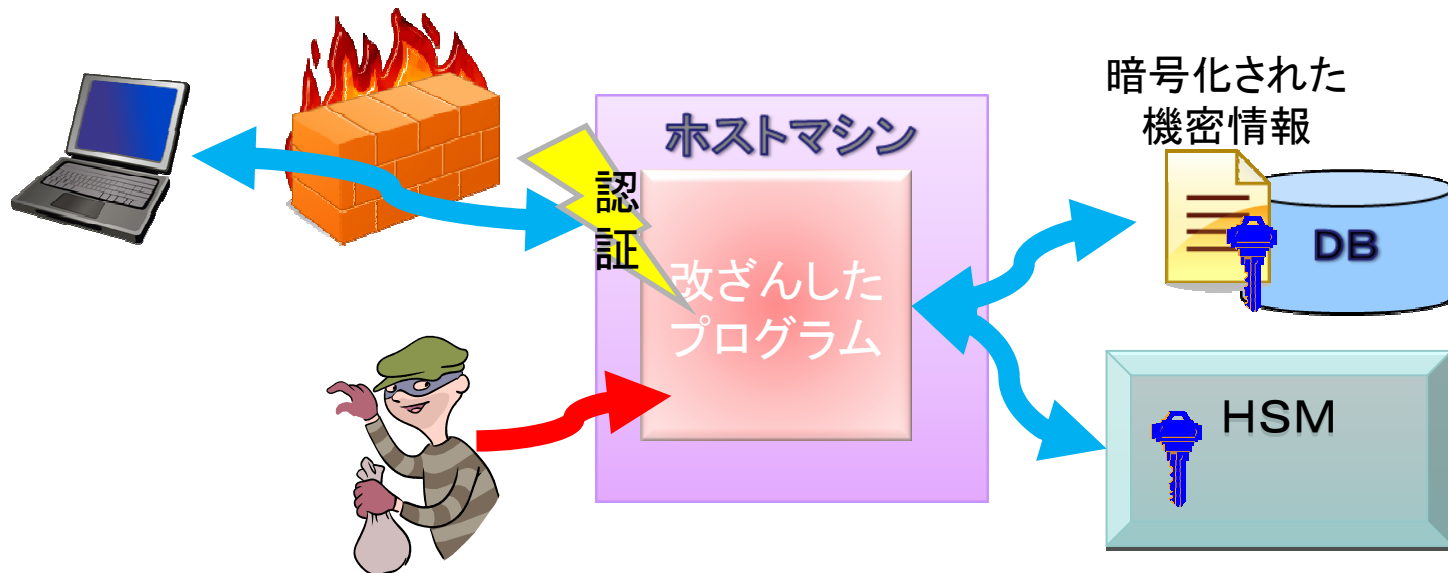
鍵は保護されるが、平文に戻された機密情報が盗まれる



セキュアな実行環境が求められる理由

問題例2: プログラムの改ざん

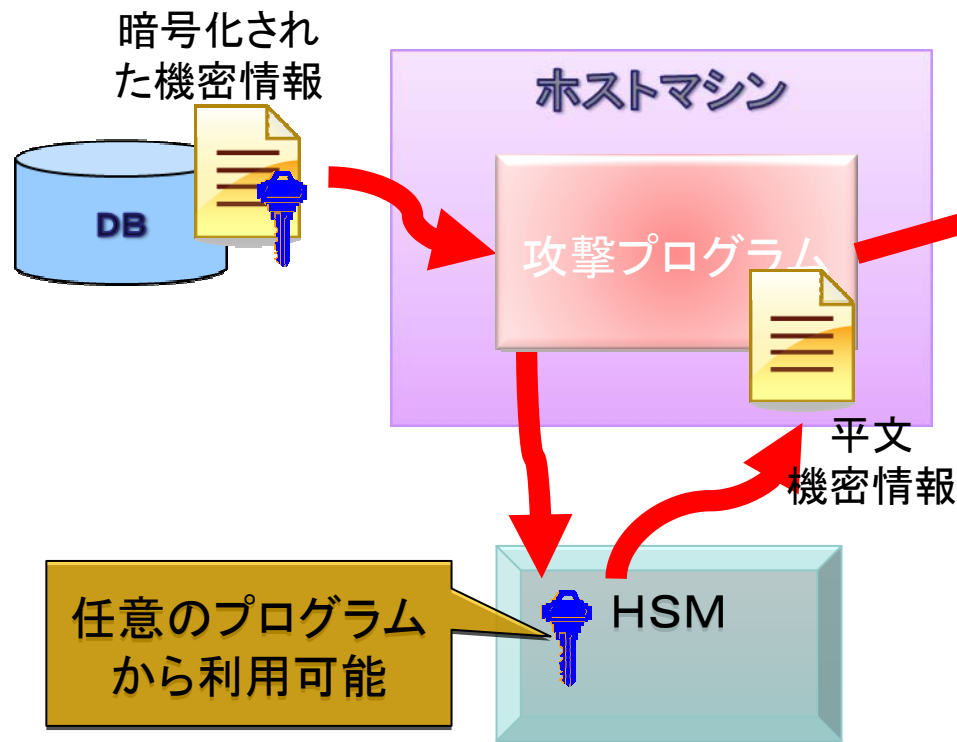
プログラムを改ざんして、認証を回避。
機密情報を取得



セキュアな実行環境が求められる理由

問題例3: 鍵の不正利用

鍵を不正に利用して、
暗号化された機密情報を取得

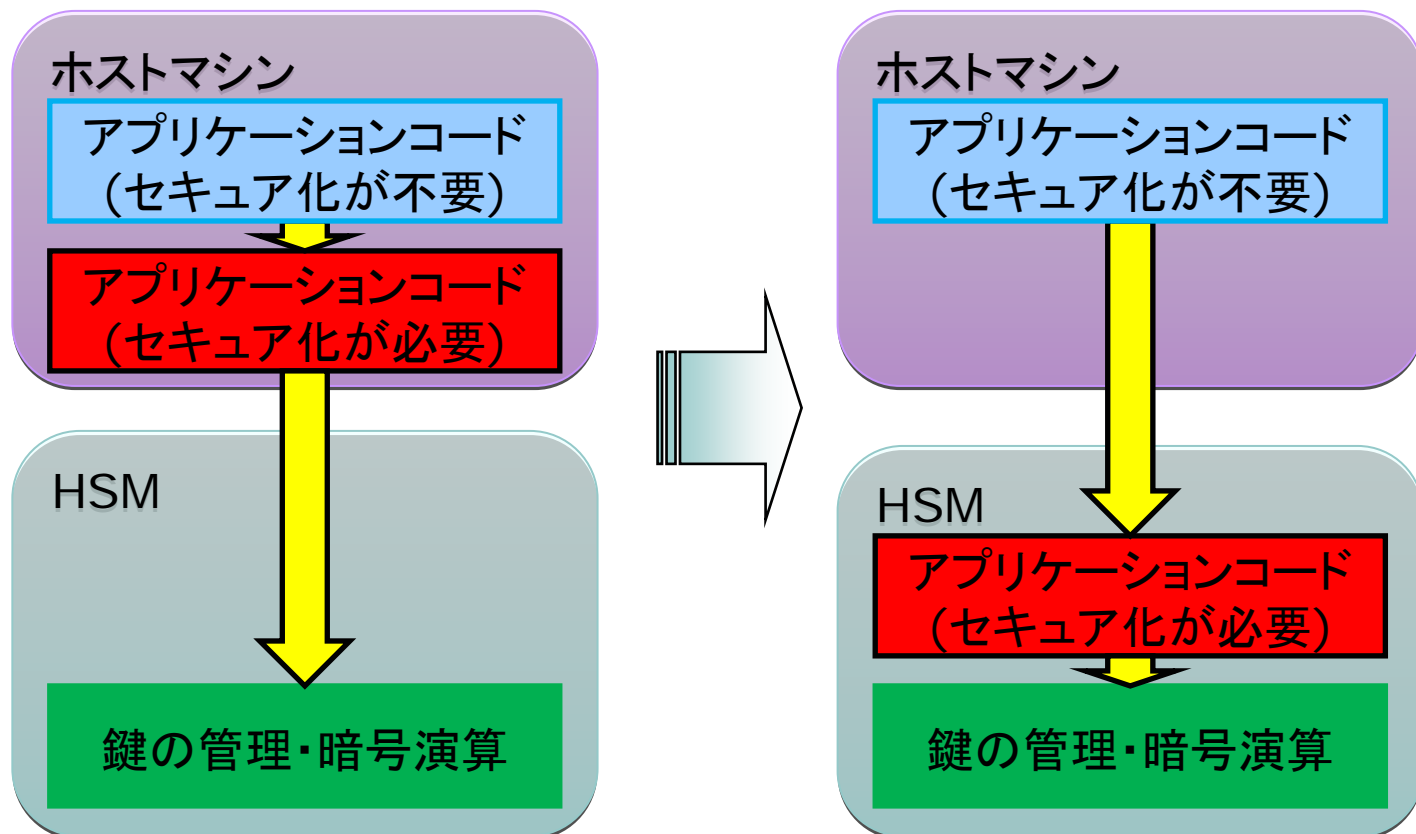


HSMだけでできること

	HSMなし	HSMあり
鍵の保護	×	◎
データの保護	×	×
プログラムの保護	×	×
鍵の不正利用防止	×	×

S.E.E.とは？

S.E.E.とはSecure Execution Engine™の略で、セキュアなHSM内部にて、任意のアプリケーションコードを実行する機能



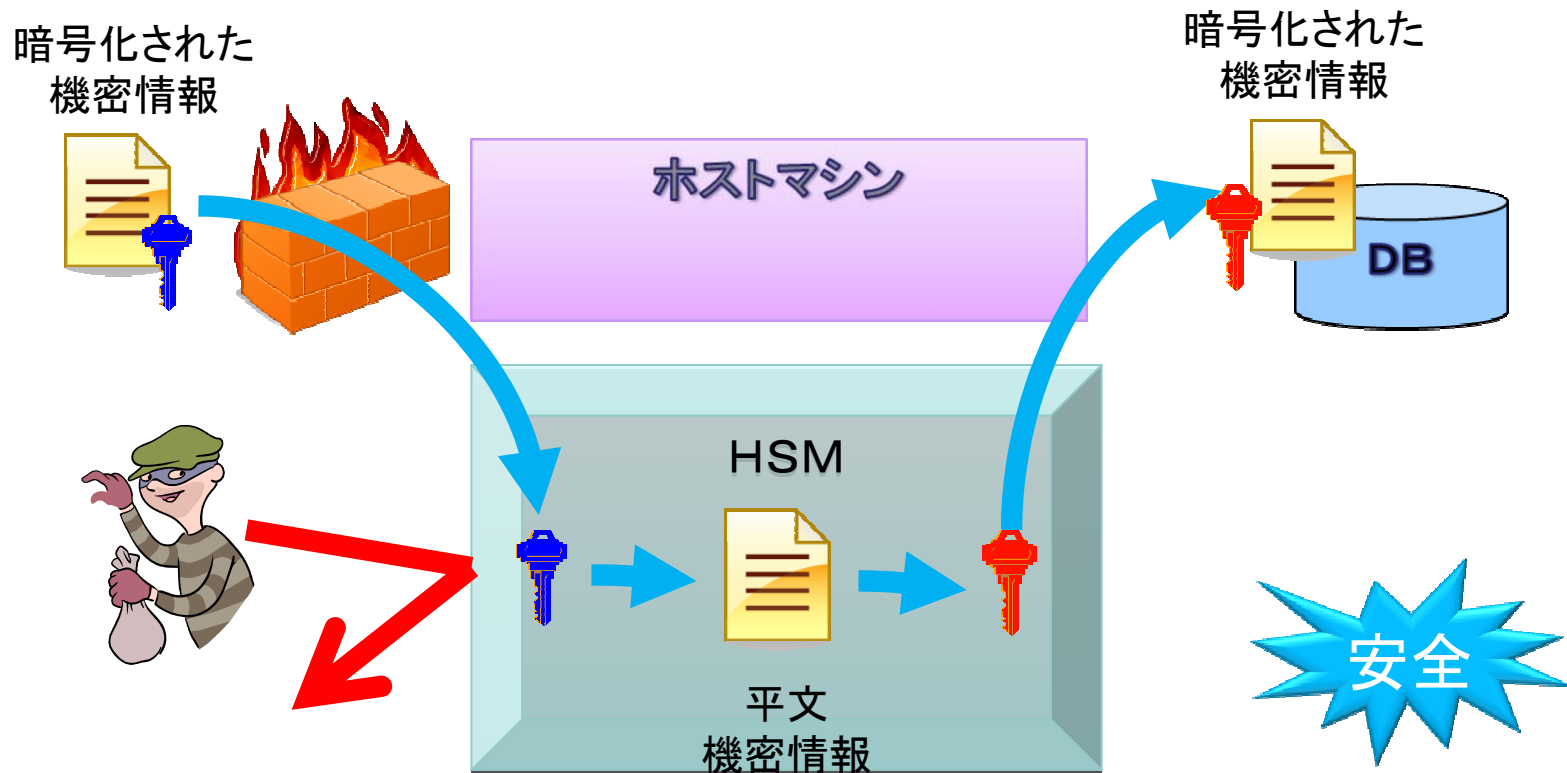
S.E.E. の機能

- セキュアなHSM内部で、C言語で記述したプログラム (SEEアプリ)を安全に実行する
- SEEアプリからのみ利用可能なSEE専用鍵が作れる
- SEEアプリに署名でき、改ざんされたSEEアプリの実行を防止できる
- HSM提供の暗号演算機能を利用できる
- その他
 - SEEアプリ暗号化
 - SSLライブラリ

S.E.Eのメカニズム

解決例1: 機密情報の保護

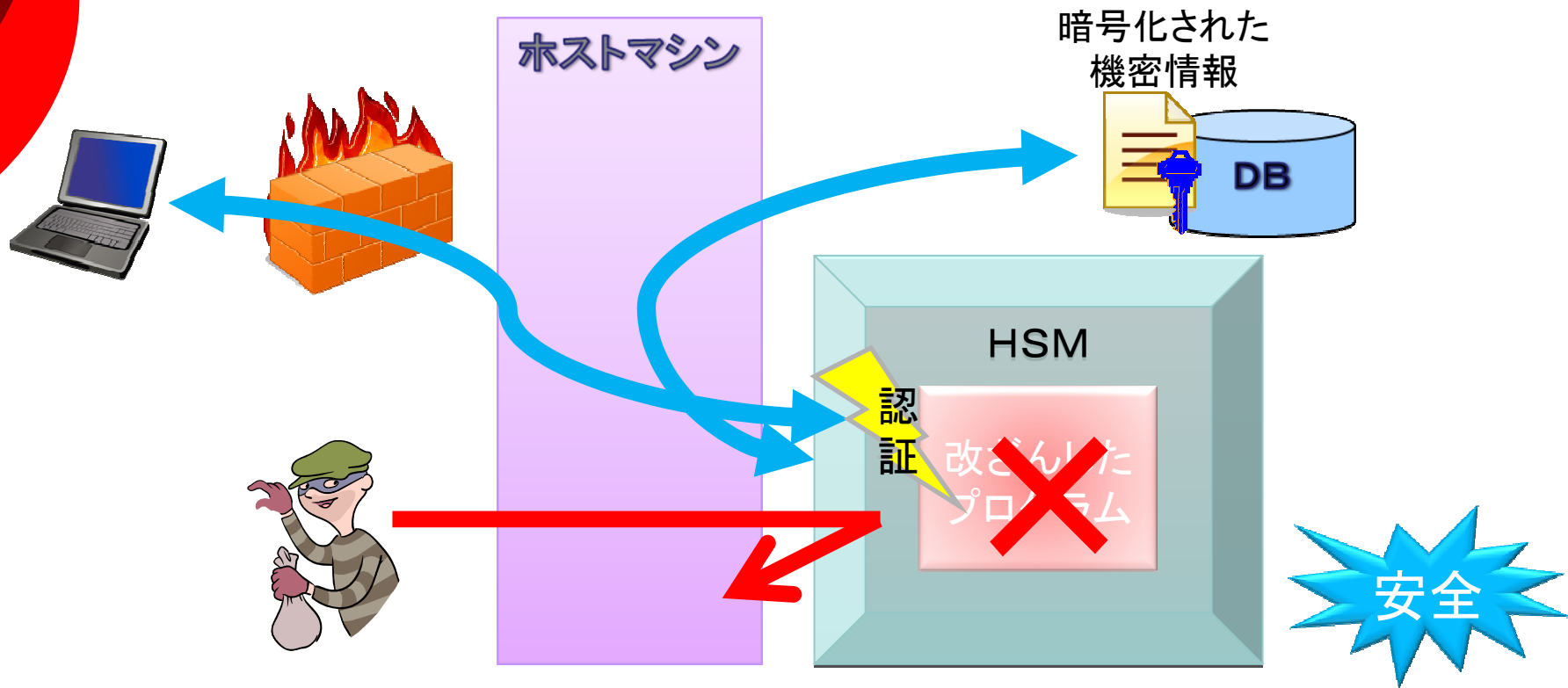
平文に戻るのはセキュアなHSMの中だけ



S.E.Eのメカニズム

解決例2: プログラムの改ざん検出

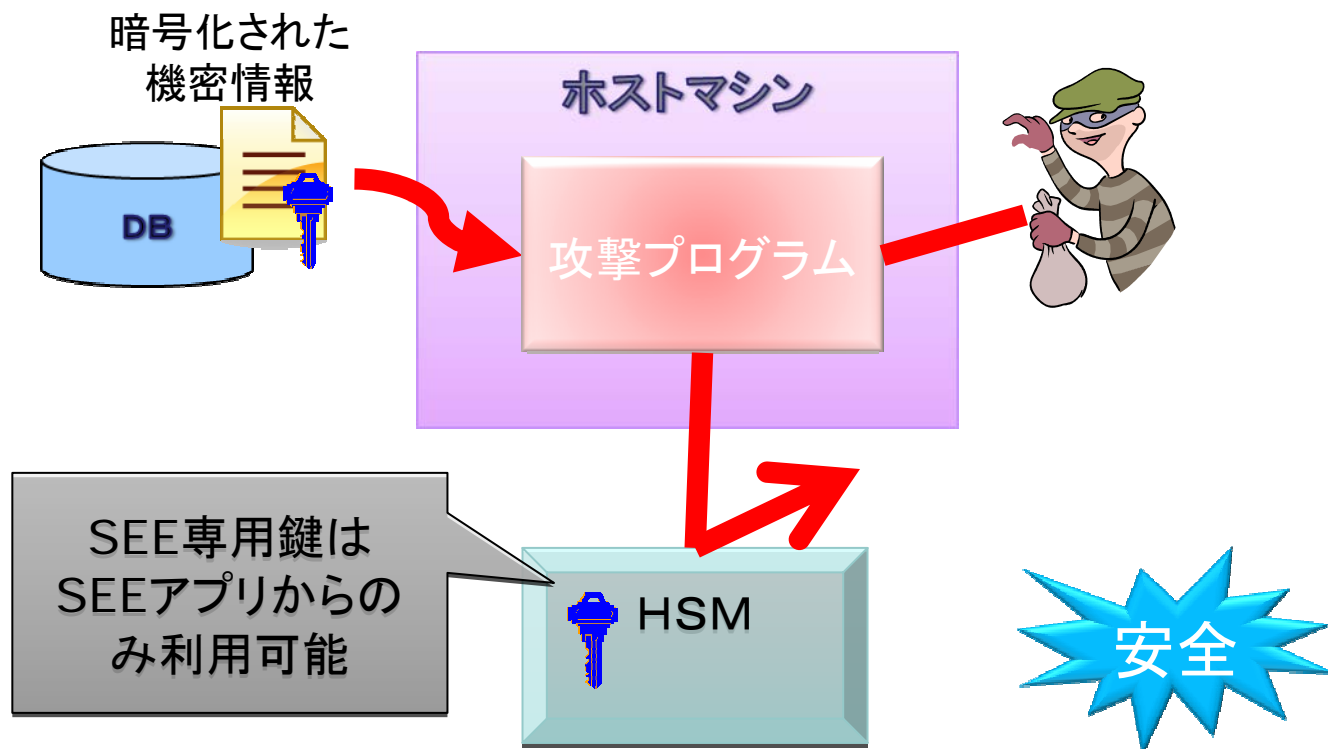
改ざんしたSEEアプリは実行できない



S.E.Eのメカニズム

解決例3: 鍵の不正利用防止

SEEから利用可能なSEE専用鍵を使うことで、
鍵の不正な利用を防止



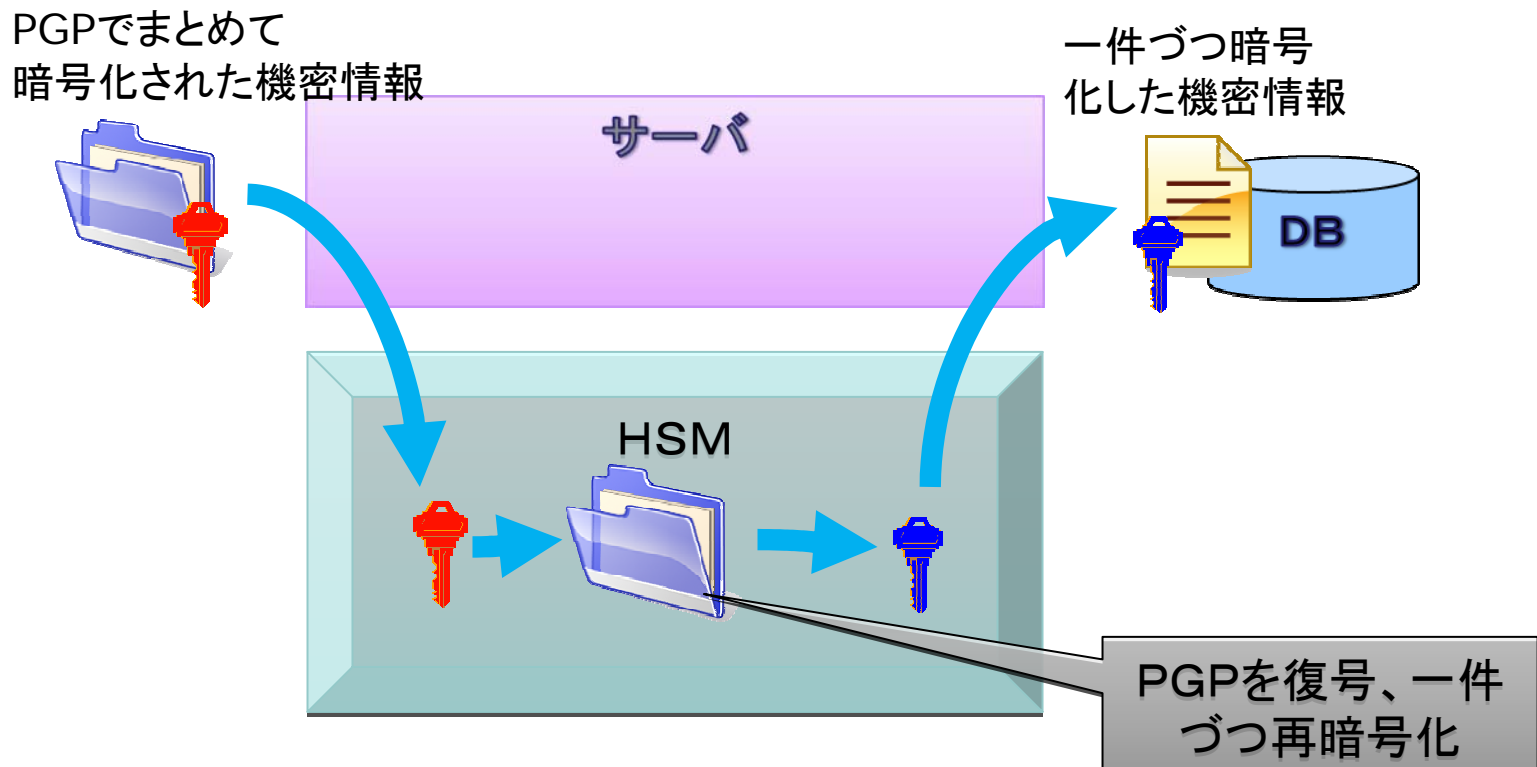
S.E.Eのメリット

	HSMなし	HSMあり、SEEなし	HSM、SEEあり
鍵の保護	×	◎	◎
データの保護	×	×	◎
プログラムの保護	×	×	◎
鍵の不正利用防止	×	×	◎

S.E.Eの応用例(1)

– PGPアルゴリズムの実装

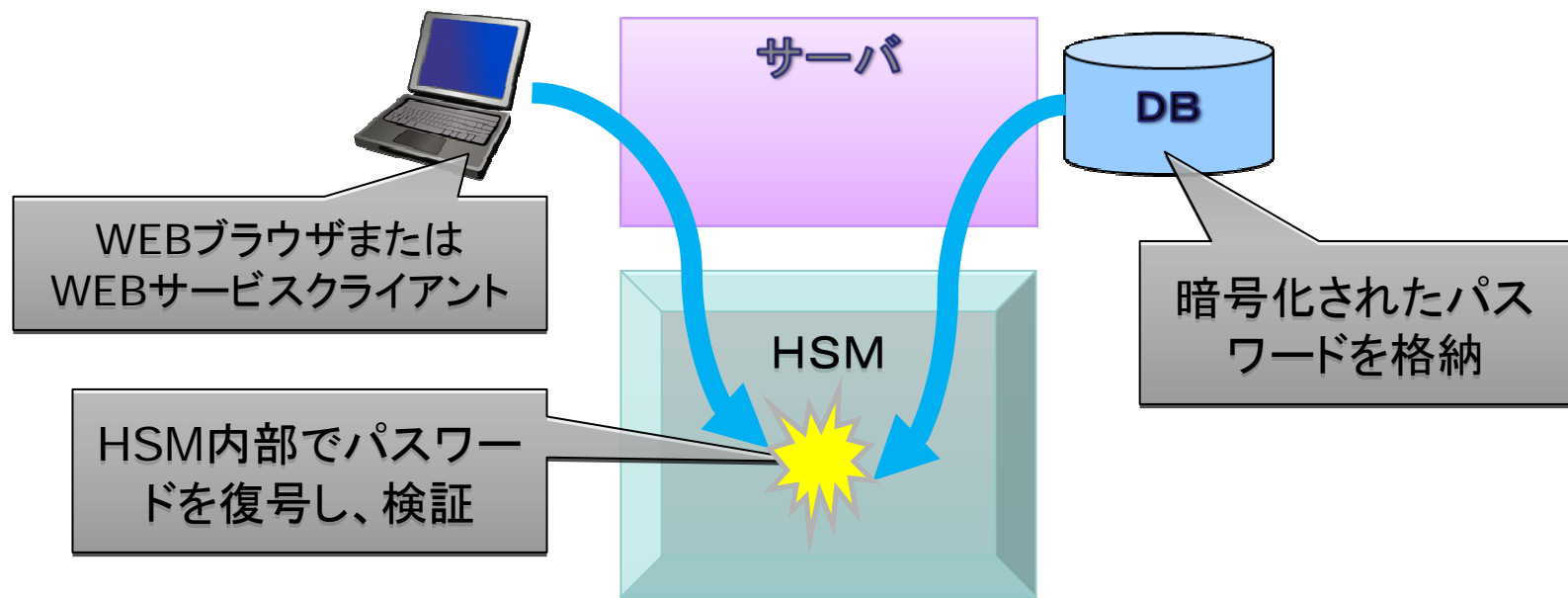
- PGPアルゴリズムをSEEアプリで実装し、PGP暗号で保護されたデータを復号、再暗号化することで、機密情報の漏洩を防止



S.E.Eの応用例(2)

- オンラインユーザ認証

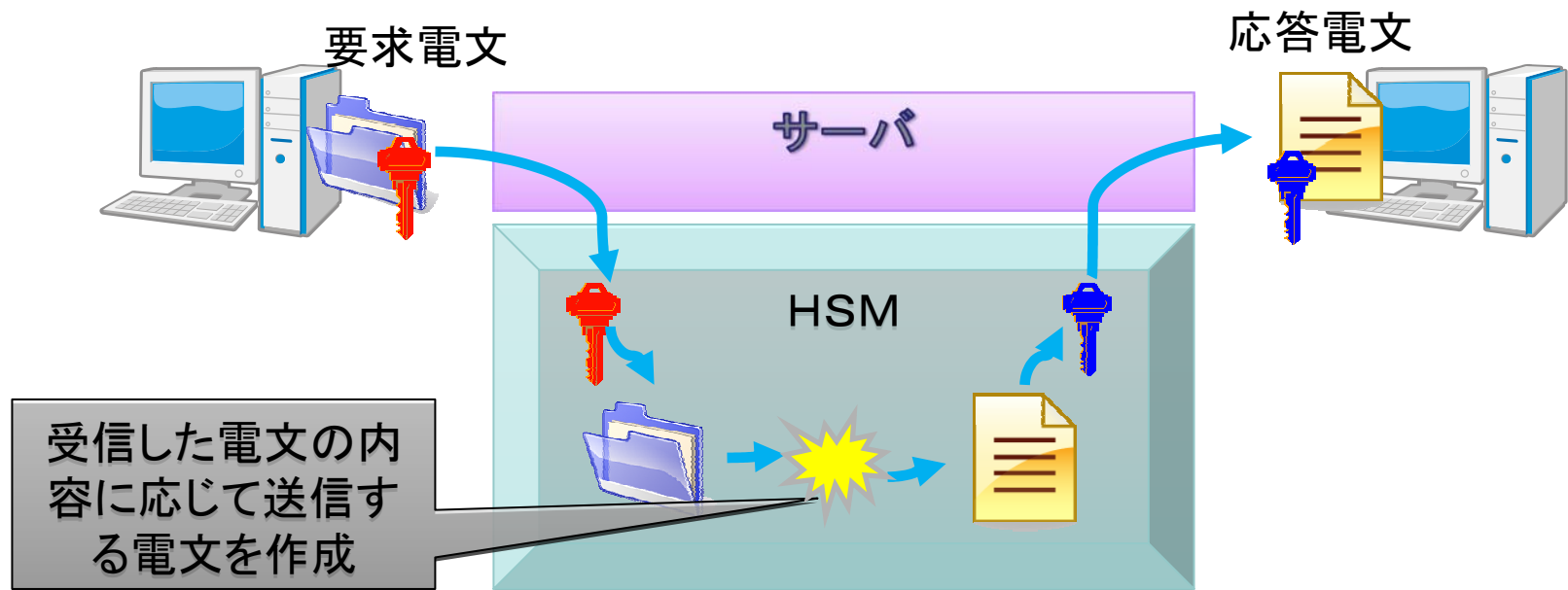
- 送信されてきたパスワードと保存されているパスワードをHSM内部で検証することで、パスワードの漏洩を防止



S.E.Eの応用例(3)

- 鍵配信・更新システム

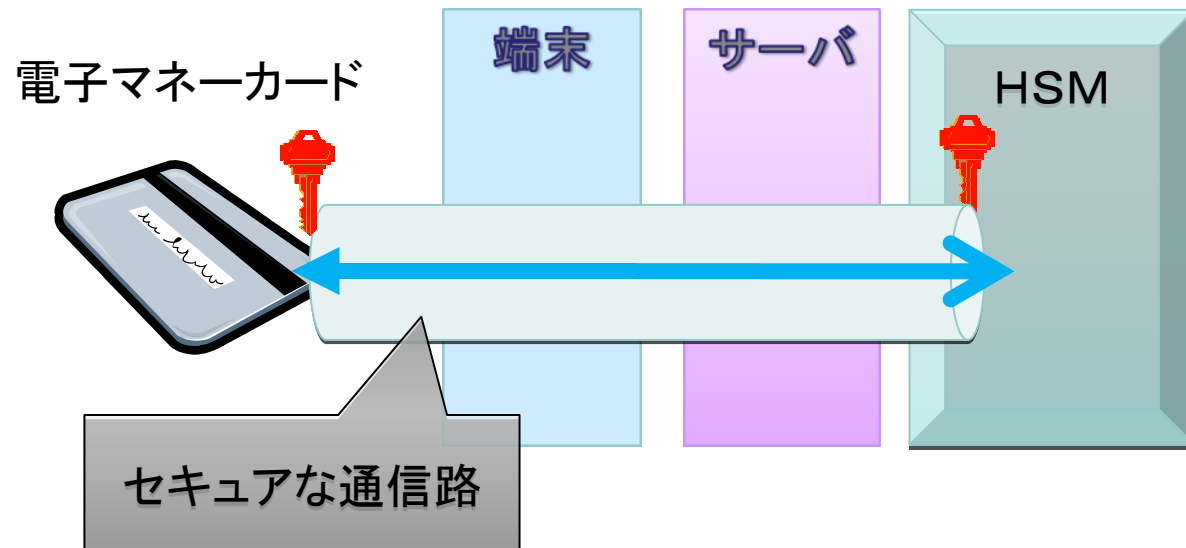
- 電文の読み取り・作成、すべてHSM内部で実行することで、電文の漏洩を防止
- 独自フォーマット、独自の処理でも実現可能



S.E.Eの応用例(4)

-End to Endでのセキュアな通信

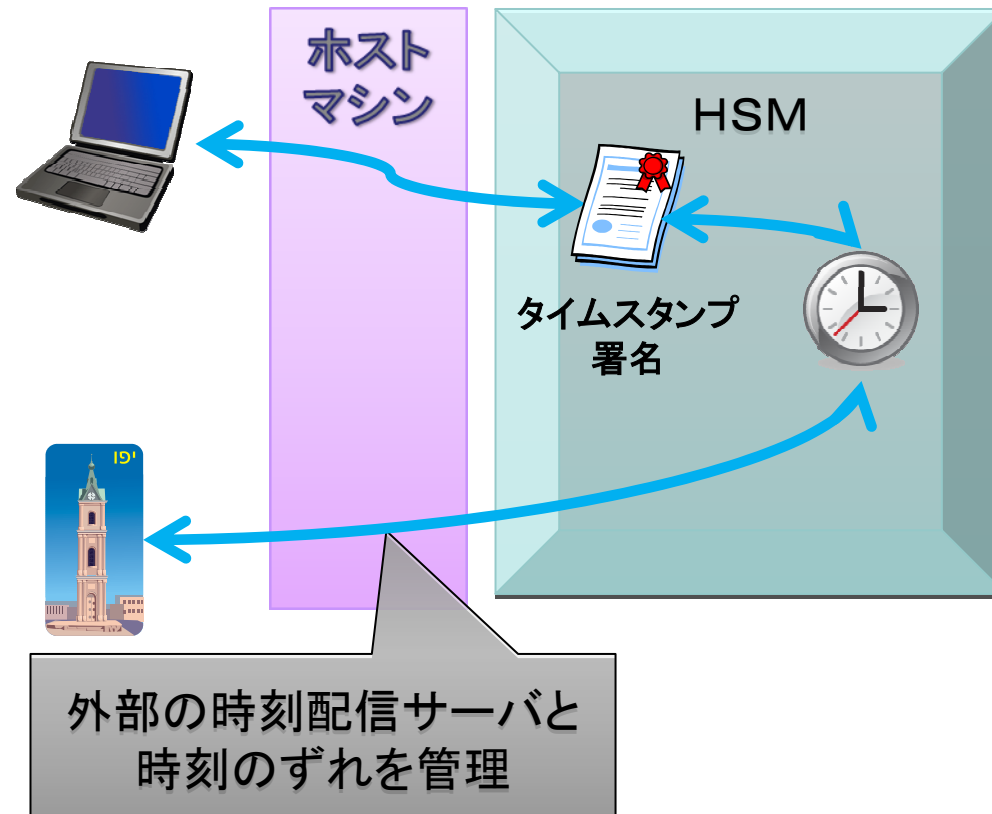
- SEEと電子マネーカードが直接、セキュアな通信路を確立し、端末、サーバまで含めた途中経路での情報漏洩を防止



S.E.Eの応用例(5)

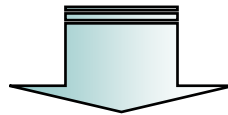
- タイムスタンプサーバ

- HSMのリアルタイムクロックを使用してタイムスタンプ署名
- 外部の時刻配信サーバと時刻のずれを管理



まとめ

- 鍵の漏洩防止が必要
- 鍵の不正利用防止も必要
- 鍵だけではなく、データの漏洩防止も必要
- 鍵だけではなく、プログラムの改ざん防止も必要



nCipher HSMのS.E.Eを用いることにより、
鍵、データ、プログラムコードをすべて保護し、
セキュアなシステムを構築することができる。

お問い合わせ

- 株式会社サリオンシステムズリサーチ
- 〒101-0054 東京都千代田区神田錦町3-23 西本興産錦町ビル14F
- 電話: 03-5217-2980(代) FAX: 03-5217-3590
- Web: <http://www.sarion.co.jp>
- お問い合わせ: prod_contact@sarion.co.jp