

情報セキュリティ技術戦略

芦田 元之

情報セキュリティは、安心して信頼できるネットワークソリューションを提供するためのキーとなる技術である。従来の沖電気の情報セキュリティ技術戦略は、DMZ（De-Militarized Zone非武装化地帯）に基づくWebサーバや内部ネットワークの防御が中心であった。しかし、その後、Blasterワームなど不正アクセスの手口の巧妙化や内部関係者による顧客（個人）情報あるいは機密情報漏えいの多発化、住民基本台帳ネットワーク（住基ネット）の本格始動、個人情報保護法成立など、社会環境が大きく変化しつつある。この変化に対応するために情報セキュリティ技術戦略の再検討を行った。本稿ではこの情報セキュリティ技術戦略について報告する。

多様化する情報セキュリティ環境

ブロードバンド、モバイルコンピューティング、iモードの普及やIP電話に代表されるインターネットを利用した技術が急激に進歩し、eビジネスに代表されるようにビジネス形態も急速に変革している。政府も住民基本台帳ネットワークやLGWAN（総合行政ネットワーク）の基盤システム整備を推進している。

ネットワーク利用の拡大に伴い、情報セキュリティへの脅威も増大し、手口も巧妙化している。また、ネットワークを利用した攻撃だけでなく、内部関係者による被害が増大していることにも注意を払う必要がある。特に内部関係者による個人情報や機密情報の漏えいが問題になっている。経済産業省が2003年10月に発表した「情報セキュリティ総合戦略」は、〈情報セキュリティに絶対はない〉との前提の下で、事故の回避（予防）・被害局所化・回復の最適化を図った「事故前提社会システム」の構築を提唱している。

「e社会」は、情報セキュリティへの脅威を伴いながら急速に発展しており、さまざまな角度からセキュリティへの対策が必要である。

情報セキュリティ技術戦略

多様化する情報セキュリティ環境に対応するためには

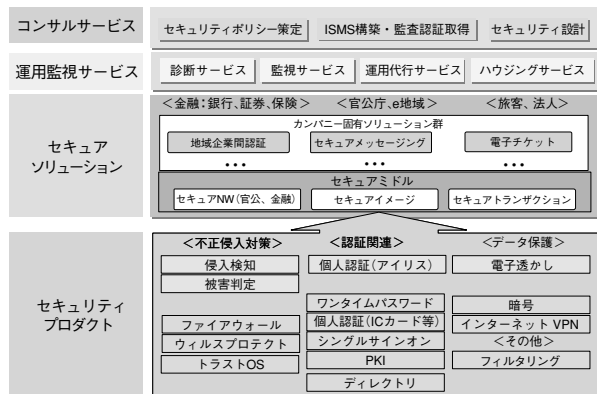


図1 新情報セキュリティフレームワーク

技術対策とセキュリティ管理対策の融合が必要であり、新たな情報セキュリティフレームワークの再構築を行った（図1参照）。

新情報セキュリティフレームワークは、安全で信頼できるネットワークソリューションを構築する際に、多様化する内外からの情報セキュリティへの脅威に柔軟に対処でき、急速に進展している「e社会」の変化速度に対応可能とすることを目的として、セキュアミドルの概念を取り入れたのが特徴である。セキュアミドルは、沖電気の各カンパニーの固有のセキュアソリューション構築のベースとなるコンポーネントである。

セキュアミドルとして、外部と内部の脅威を統合的に防御する「セキュアネットワーク」、ドキュメントの真正性を保証する「セキュアイメージ」およびeビジネスに対応した「セキュアトランザクション」を3本柱として定めた。このセキュアミドルを中心に沖グループとしての新しいセキュリティビジネス像を図2に示す。

ここでは、セキュアソリューションビジネスをカンパニー固有のセキュアソリューションビジネス、セキュアミドルのビジネスおよび情報セキュリティマネジメントシステム（ISMS）を中心としたコンサルティングビジネスに区分する。各カンパニーは、セキュアミドルをミドルソフトとして、カンパニー対応のセキュアソリュー

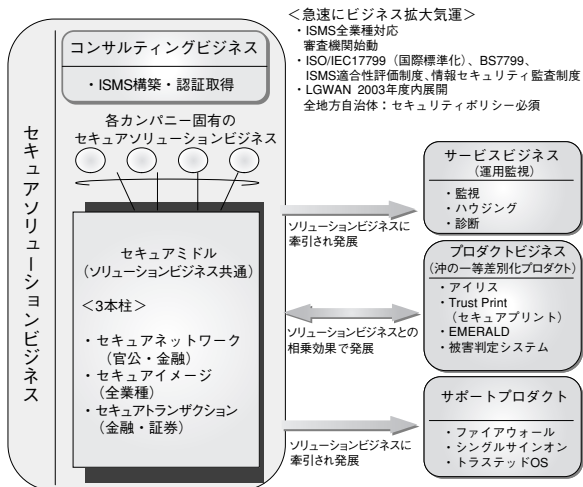


図2 新セキュリティビジネス全体観

ションを開発し、セキュリティビジネスを行う。

セキュアソリューションを構築するためには、部品となるセキュリティプロダクトと運用および監視を行うためのサービスが必要である。セキュリティプロダクトについては、沖の一等差別化製品をビジネスとするプロダクトビジネスと品揃えとして必要なサポートプロダクトに区別している。プロダクトビジネスは、ソリューションビジネスとの相乗効果による発展、サポートプロダクトについては、ソリューションビジネスの牽引によりビジネスを拡大する。サービスビジネスは、セキュリティソリューション提供後の運用代行や監視を行うサービスである。このサービスもソリューションビジネスに牽引されての発展を期待している。

セキュアミドル

セキュアミドルを選定するにあたり、セキュアミドルを以下のように定義した。

「カンパニー固有のセキュアソリューション間で共通となり、かつ沖電気の特徴が十分に発揮できるセキュアソリューション」

セキュリティに関する沖電気の特徴を以下に示す。

- ①堅牢なセキュリティが要求されている市場に強い。
 - 官公庁市場
 - 金融市場
 - キャリア市場
- ②国家レベルのセキュリティ強度が要求される行政・国防・警察のシステム構築で培ったセキュリティ技術ノウハウを擁している。
 - 外務省、総務省、防衛庁、警察庁

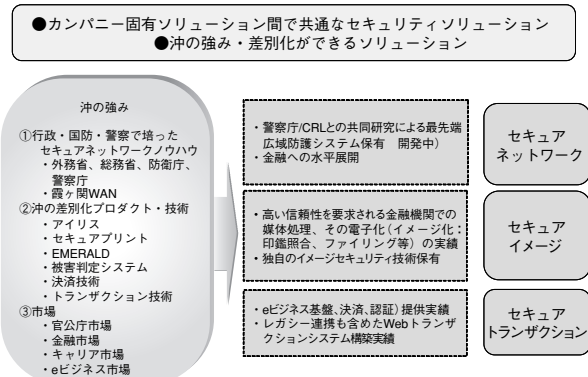


図3 セキュアミドルの選択

③沖電気の独自技術による製品・実績

- アイリス（虹彩による個人認証）
- 電子透かし
- 侵入検知システム
- 被害判定システム
- 決済技術
- トランザクションシステム構築

これらの沖電気の特徴を活かし、かつ共通化できるソリューション（セキュアミドル）として、「セキュアネットワーク」、「セキュアプリント」、「セキュアトランザクション」の3つのセキュアミドルを選択した（図3参照）。

「セキュアネットワーク」は、警察庁と通信総合研究所（CRL）との共同開発による最先端の広域防御システムで官公庁や金融機関への水平展開を行っている。「セキュアプリント」は、高い信頼性を要求される金融機関での媒体処理、そのイメージ化（印鑑照合、ファイリング等）の実績と独自の電子透かし技術を融合させたイメージセキュリティ技術に基づいている。「セキュアトランザクション」は、eビジネス基盤（決済、認証）とWebトランザクションシステム構築実績を統合させたソリューションである。

(1) セキュアネットワーク

セキュアネットワークは、ネットワークの内外からの脅威に対抗するためのセキュリティ統合監視ソリューションである。総合接続によって形成された広域イントラネットなどの横断型ネットワーク全体の安全を保つために以下の新技術を採用している。

- 統一的ポリシー制御
- 不正トラフィック遮断
- 横断的アクセス制御
- 高度な侵入検知、攻撃追跡
- 防御情報の有効活用

図4にセキュアネットワークソリューションの概念図を示す。

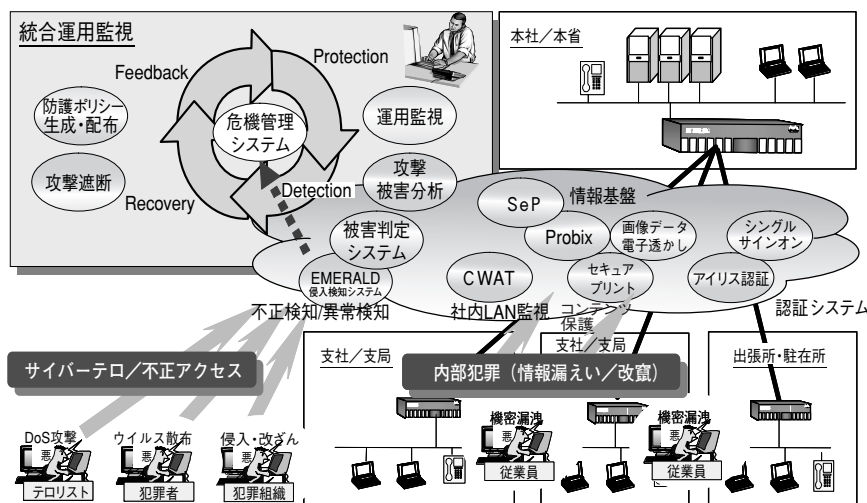


図4 セキュアネットワーク概念図

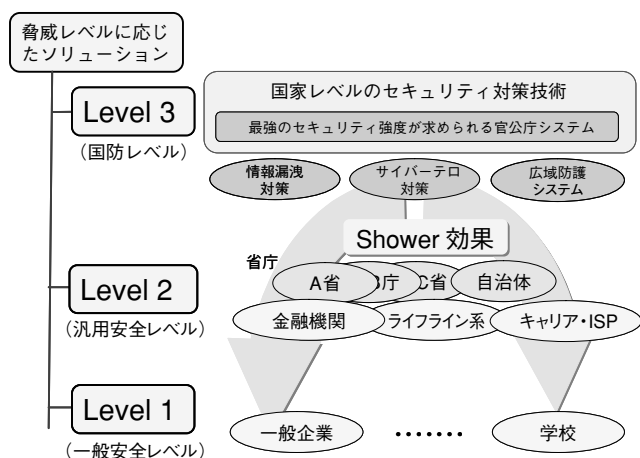


図5 セキュアネットワーク展開シナリオ

セキュアネットワークで採用されている国家的な視点からの高度なセキュリティ技術を他の市場に展開するために、セキュアネットワークのサブ

セット化、部品化を進めている (図5参照)。

セキュアネットワークの詳細については、参考文献¹⁾を参照されたい。

(2) セキュアプリント

セキュアプリントは、電子透かし技術を使用して、イメージデータの読み込みからデータ処理、蓄積処理および印刷結果にいたるまで、常に情報が正しい (真正性) ことを保証するソリューションである。それぞれのプロセスにおいて不要な情報を隠蔽することにより情報の漏えいを防止する (図6参照)。セキュアプリントの特徴は、印刷情報だけで印刷後の紙面の改ざん検知ができ、紙面情報を保護する。改ざんされた場合は、改ざん位置も特定できる。さらに、紙面に別の情報を埋め込んで印刷し、スキャナーでこの情報が取り出せ、情報の機密性を保護できる。利用分野としては、証明書、印刷物 (チケット、書面等) やカルテ等の真正性、原本性保証がある。セキュアプリントは、GUI (Graphical User Interface) 層、コンポーネント層およびエンジン層のパッケージから構成され、容易に固有ソリューションに実装することができる。

セキュアプリントの特徴は、印刷情報だけで印刷後の紙面の改ざん検知ができ、紙面情報を保護する。改ざんされた場合は、改ざん位置も特定できる。さらに、紙面に別の情報を埋め込んで印刷し、スキャナーでこの情報が取り出せ、情報の機密性を保護できる。利用分野としては、証明書、印刷物 (チケット、書面等) やカルテ等の真正性、原本性保証がある。セキュアプリントは、GUI (Graphical User Interface) 層、コンポーネント層およびエンジン層のパッケージから構成され、容易に固有ソリューションに実装することができる。

(3) セキュアトランザクション

セキュアトランザクション (Webインテグレーション) は、インターネットから基幹システムまでの一貫したEnd-

To-Endのセキュリティと高信頼性を実現するトランザクション構築ソリューション²⁾である (図7参照)。

セキュアトランザクションの特徴を以下に示す。

- 高信頼・高性能なトランザクション処理
- セキュリティコードとビジネスブロックを分離し、セキュリティ対策を簡易化
- セキュアネットとの連携による高度なセキュアシステムを構築

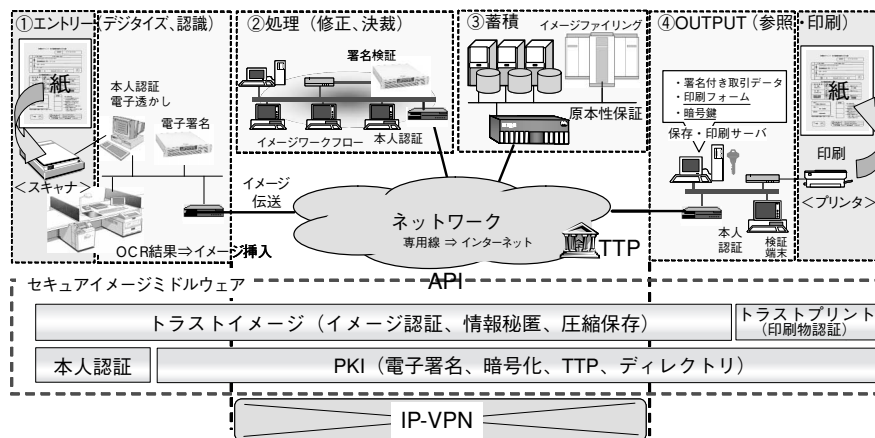


図6 セキュアプリントコンセプト

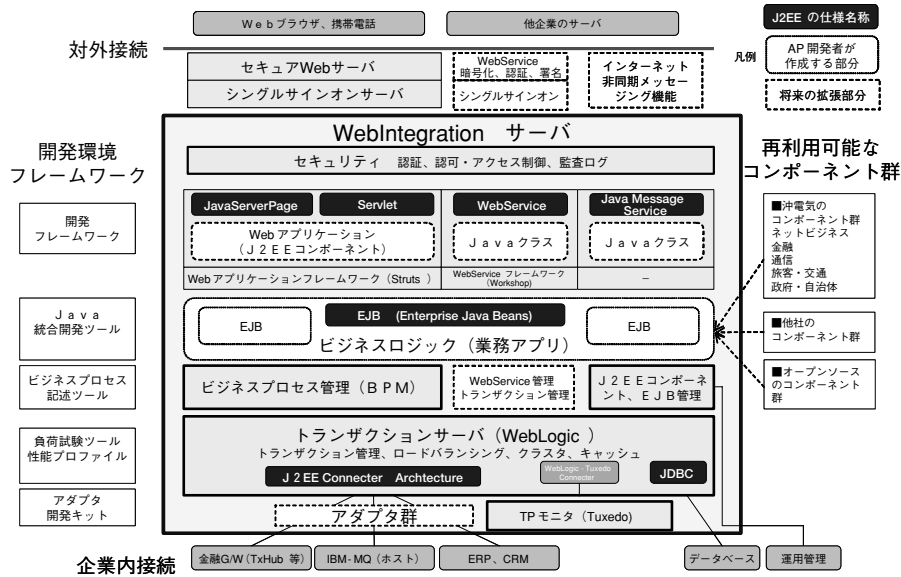


図7 セキュアトランザクションアーキテクチャ

セキュアトランザクションをベースに電子書面システム、目論見書交付サービスシステム申請業務システム等が開発されている。

コンサルティングビジネスの展開

情報セキュリティ関連施策は、技術だけでなく情報セキュリティマネジメントシステム(ISMS)を主とする「企業・個人のセキュリティ向上」が重要である。政府はISMSを定着させるために数々の政策を実施している。平成14年4月に「ISMS適合性評価制度」、平成15年4月に「情報セキュリティ監査制度」をスタートさせた。総務省は、各地方自治体に対し平成16年度から監査制度を行う意向である。防衛庁は、調達企業に対するセキュリティ

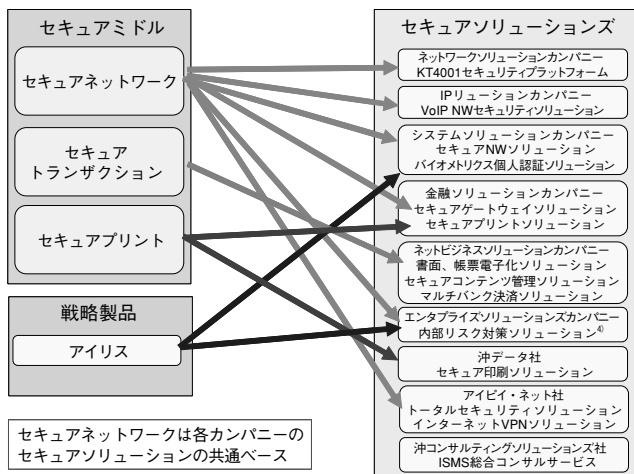


図8 セキュアソリューションとセキュアミドル

監査の実施を予定している。コンサルティングビジネス³⁾は、ISMSに関連した以下のサービスを官公庁、地方自治体および企業に展開している。

- セキュリティポリシー策定支援
- ISMS認証取得支援
- 企業向け情報セキュリティ内部監査
- 防衛産業向け情報セキュリティ内部監査
- 地方自治体向け情報セキュリティ内部監査

コンサルティングサービスと各カンパニーのセキュアソリューションとの連携でセキュリティビジネスの拡大を図っている。

まとめ

セキュアミドルの3本柱を中心とする情報セキュリティ戦略に基づいて、沖電気グループの各カンパニーおよび関連企業でセキュアソリューションが開発されている(図8)。

沖電気グループのセキュリティビジネスを更に発展させるためには、市場競争力のあるセキュアミドル、これを支える特徴ある製品およびソリューションの開発が必須である。

参考文献

- 1) 大多和篤夫 他：「セキュアネットワークソリューション」沖テクニカルレビュー197号
- 2) 碓氷明寿：「Webインテグレーションソリューションにおける次世代トランザクション処理のアーキテクチャ」沖テクニカルレビュー195号, Vol.70 No.3, pp.10-13, 2003年7月
- 3) 武内春夫 他：「情報セキュリティポリシーコンサルティングビジネス」沖テクニカルレビュー195号, Vol.70 No.3, pp.64-67, 2003年7月
- 4) 山越俊也 他：「情報セキュリティ管理の意義と内部リスク対策ソリューション」沖テクニカルレビュー195号, Vol.70 No.3, pp.40-43, 2003年7月

筆者紹介

芦田元之：Asanobu Ashida 沖コンサルティングソリューションズ株式会社 金融グループ