エレクトロニックコマース・セキュリティ特集

UDC［681.324：343.45］：061.5.051 OKIDENKI

沖電気社内システムへのセキュリティ適用事例

Security in Oki-Group's Information System

一戸 英希　Eiki Ichinohe
石黒 昇　Noboru Ishiguro

要　旨

沖グループでは，ITセキュリティポリシーに基づき，電子情報管理規程とネットワーク，インターネット，リモートアクセス，Webなどについての電子情報管理規程細則を制定している。沖グループのITセキュリティへの取り組み事例として，ITセキュリティポリシー，インターネット利用におけるファイアウォール，リモートアクセス制御，イントラネットでのWeb利用，各種業務システム利用時のシングルサインオン，芝浦データセンターにおける入退室管理について述べる。

1．ま　え　が　き

ネットワークシステムのオープン化に伴い，地理的に離れた部門間，グループ企業間，グループ外企業とのアライアンスなどによる情報共有や，お客様への情報開示が急速に進展している。沖グループにおいても，グループ経営の強化，カンパニ制の導入，協力会社や派遣社員の増加と組織のフラット化により，従来の閉鎖的なネットワークにおける組織単位の情報セキュリティは形骸化しつつある。情報共有や情報開示の範囲が拡大化，複雑化する中で，セキュリティの対象も会社単位，組織単位から，プロジェクト単位，個人単位へと変化してきている。このため，IT（Information Technology）セキュリティポリシーを策定し，これに基づきさまざまな局面において新たな枠組みのセキュリティ施策に先端技術を用い実践している。ここでは，オープンなネットワークシステムの中での電子情報を主とした沖グループの情報セキュリティへの取り組みと適用事例を紹介する。

一戸英希

（株）沖電気カスタマアドテック　企画ソリューションビジネス準備室

石黒　昇

情報企画部

2．セキュリティポリシーの概要

図１に，セキュリティポリシーの位置付けを示す。

沖グループの外部および内部に起因する不正行為，過失，事故などの脅威から沖グループが管理する情報資産（情報システムおよび電子情報）を保護し，かつ可能な限りの情報資産を公開し，企業活動を活発化させることを目的として，ITセキュリティポリシーを策定した。ITセキュリティポリシーは，沖グループの経営者を含めた全社員と，沖グループの業務遂行に関わる派遣社員および請負社員（以下，利用者）が情報資産を利用する場合に適用される。ITセキュリティポリシーに基づき電子情報管理規程を定めネットワーク，インターネット，リモートアクセス，社内Web，電子メール等の詳細な運用細則を定めている。各運用細則の中では，それぞれの情報システム利用局面におけるセキュリティに関する事項（禁止事項，遵守事項など）が記述されているが，利用者がすべての運用細則に精通することは難しいため，利用者とシステム管理者向けのITセキュリティガイドを作成し徹底を図っている。

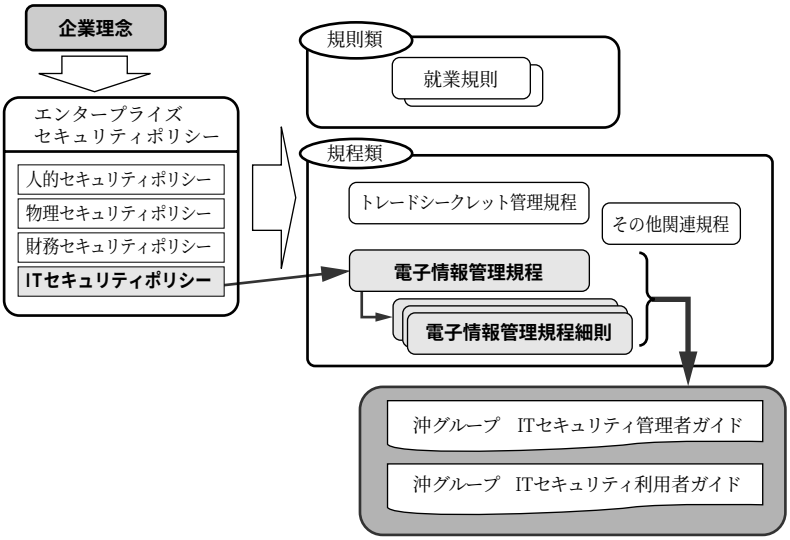

図1　セキュリティポリシーの位置付け
Fig. 1　Position of security policy

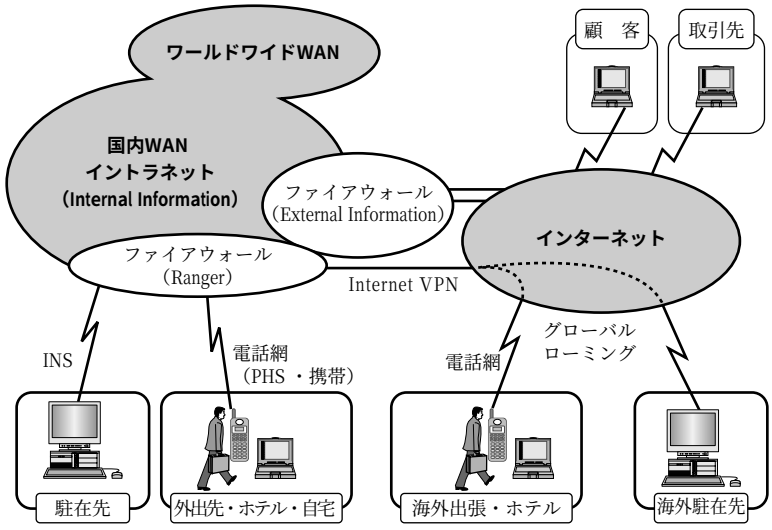

図2　沖グループのネットワーク
Fig. 2　Network of Oki-group's

3．グループ企業向けファイアウォール

沖グループのネットワークは，図2に示すように，国内WAN(Wide Area Network) と海外WANで構成され，インターネットへの接続とリモートアクセスの接続は一元化し集中管理されている。

3.1　目的別ファイアウォール

日本国内においては，インターネット接続用ファイアウォールとリモートアクセス接続用ファイアウォールを分離して構築している。また，インターネット接続用のファイアウォールは，お客様向けの情報公開用と沖グループ内からのインターネット利用など目的別に構築し，それぞれ異なるファイアウォールポリシーに基づき運用している。

3.2　グループ企業向けファイアウォール

沖グループの一元管理されたファイアウォールは，oki.co.jp以外の独自ドメインを利用する沖グループの国内各企業（約50社）に対し，ISP（Internet Service Provider）に相当するインターネットサービスを提供している。各社ごとのDNS（Domain Name System）サービス，メール配送サービス，公開Webサービス等は統一されたファイアウォールポリシーに基づき構築されているが，沖グループにおけるインターネット利用が多目的化するにつれ，目的に合った専用のファイアウォールの必要性がますます高くなると予想される。

また，海外のグループ企業でのファイアウォール構築については，ソフトウェア・ハードウェアの指定を行い，ファイアウォールポリシーの設定をインターネット統括管理者が行なうことにより一元管理を行なっている。

3.3　セキュリティホール

外部からの進入やアタックを未然に防ぐため，ファイアウォールやインターネット用サーバのセキュリティホール検出やアクセスログの解析を行うため，監視ロボットを導入し，各ファイアウォールの維持管理を実施している。

4．リモートアクセス制御

沖グループでのリモートアクセスは，RAS（Remote Access Service）接続とインターネットVPN（Virtual Private Network）接続をRANGER（Remote Access

Network for OKI-group User's)により提供している。RASは公衆網，ISDN，PHS，携帯電話に対応しており，主に日本国内でのモバイル環境に利用している。インターネットVPNは，海外WANに接続していない拠点の利用者や海外出張者向けのモバイル環境に利用している。

RANGERでは，個人認証の精度を上げるため，OTP(One Time Password)カードを使用している。この方式は，利用者が物理的なOTPカードに暗証番号を入力した結果の答え(1分ごとに変わる)をパスワードとして利用するため，万が一利用者のユーザIDと暗証番号を第三者に知られても，その利用者が持つOTPカードがなければRANGERを利用できない。また，利用者の端末とファイアウォール間の通信(電子メール，Web等)はすべて暗号化されているため，ネットワーク上での漏洩を防御している。将来的には，現在当社が開発中のパーソナルユース用の小型・低価格のアイリス認識システムに移行する予定である。

5．シングルサインオン

従来の情報システムにおける認証は，人事情報，会計情報などの基幹業務システム，電子メール，グループウェアなどがそれぞれ個別にユーザID／パスワードを持ち，電子情報へのアクセス権限を管理していた。このため，利用者が各システムへログインする際には，利用者はそれぞれのシステムごとのユーザID／パスワードを記憶し，入力する必要があった。

また，各情報システムでは利用者の所属や役職などの属性によってアクセス権限を付与，コントロールしているが，その属性情報の変更も各情報システムごとになっているので，タイムリーな変更ができなかったり，管理作業が非常に複雑になっていた。このような問題を解決するための仕組みとしてLDAP(Lightweight Directory Access Protocol)対応のコーポレートディレクトリィを導入した。LDAPを利用することにより利用者，コンピュータ，プリンタ，アプリケーションなどの属性情報を一元的に管理でき，LDAP対応の情報システムの利用は同一の認証(シングルサインオン)で可能となる。

図3に，シングルサインオンの概念図を示す。

5.1　PANDA

LDAPの導入に際し，個人情報を管理する手段としてPANDA (Personal Information Database)を開発した。PANDAは，利用者個人の属性(ユーザID，姓名，所属，役職，電話番号，電子メールアドレスなど)と利用者が任意に決めたパスワードを管理しており，これらの情報をリアルタイムにコーポレートディレクトリィに反映している。また，氏名検索や電話番号検索機能などを提供することにより，正確な情報をタイムリーに提供している。

5.2　デジタル証明書

沖グループ外の顧客や企業との通信における電子印鑑(デジタル証明書)の要求は電子取引の増大や暗号化通信の必要性により日々高まっている。沖グループにおいても，特許事務所や公開入札での暗号通信，お客様や業者との電子取引などを行なう利用者に対し，公的デジタル証明書を発行している。今後，沖グループ内部の通信においてもデジタル署名が必要となってくるため，沖グループ内CA(Certificate Authority)の導入を検討している。

5.3　コーポレートディレクトリィ

コーポレートディレクトリィは，PANDAの情報を用

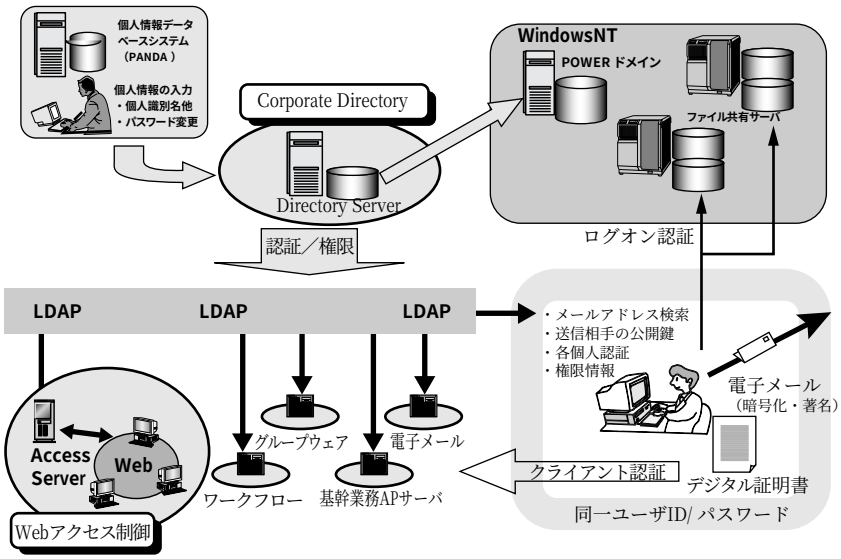

図3　シングルサインオンの概念図
Fig. 3　Concept of single sign on

い，リアルタイムに利用者の個人情報を更新し，電子メールやイントラWebの利用者識別に提供している。また，利用者のデジタル署名も管理している。今後，基幹業務システムやグループウェアなどの権限設定の機能を追加し，順次これらのシステムの利用者識別にも適用していく予定である。

5.4 NTドメイン

沖グループ内には，非常に多くのWindowsNT[＊1)]サーバがファイル共有およびプリンタ共有を目的として設置されている。従来は，情報共有の範囲が限定されていたため個別のWindowsNT[＊1)]ドメイン配下で利用者のアカウントを管理することでこと足りていたが，情報共有の範囲が拡大するのに伴い管理が煩雑になり，運用に耐えられなくなってきた。

このため，将来のWindows2000[＊1)]への移行も考慮しつつシングルマスタドメイン方式を採用し，沖グループ全体を管理するドメイン（POWERドメイン）を立ち上げた。利用者は，利用資源ごとに再接続やPCの再起動を行なうことなくファイル共有が可能となった。

6．Webのアクセス制御

沖グループのイントラネット内では，多数のWebサーバからさまざまな情報が公開されている。これらの情報のうち，ある種のものは限定された利用者にしかアクセスできないようにアクセス制御を行なう必要がある。このため，複数のアプリケーションやプラットフォームに分散されて提供されている電子情報に対して，役職や職務などにより適切なアクセス制御を行なうためのWebサーバアクセス制御の仕組みを導入している。これは，幹部社員限定ページやプロジェクト専用ページなどに適用されているが，適用範囲の順次拡大を推進中である。

このアクセス制御のための認証には先に述べたLDAPを使用し，シングルサインオンの仕組みを使用することにより，Webサーバが異なっていても，１回の個人認証を行なうだけで閲覧権限が与えられている情報へアクセスすることができる。今後さらに，セキュリティを強化するために，重要な情報へのアクセスに関してはデジタル証明書を使用した認証システムなどの仕組みも適用していく予定である。

7．入退室管理

沖グループの中核となる芝浦データセンタの入室・退室管理には，当社の開発した目の虹彩（アイリス）による個人認識技術を利用したゲート管理システム「アイリスパス®[＊2)]－Sゲート管理システム」を用いた。個々人固有のアイリスコードを用い，入場・退場それぞれにゲート装置を設置することにより，従来のIDカード，暗証番号方式のゲートシステムに比較しセキュリティレベルを飛躍的に向上できた。また，これらのシステム機器は無停電化装置より電源供給し，通電時開錠方式の電気錠を用い，停電時の入退室の安全性を保証している。

8．あ と が き

沖グループにおける情報システムのセキュリティへの取り組みと適用事例を紹介した。沖グループで用いているセキュリティの考え方や先端技術はあらゆる企業にも適用可能である。これが，お客様へのモデルケースとしてお役に立てれば幸いである。

今後の課題として，電子情報の階層化（電子情報におけるセキュリティレベルの設定）がある。コーポレートデータベースでは各データの階層化とリンクして利用者個人への権限付与が実施されているが，その他の情報システムで扱う電子情報は階層化が不十分である。電子商取引の拡大，企業間のアライアンスの増加，グループ内企業間や協力会社との情報共有が進むにつれ，個人認証はもとより電子情報の階層化とリンクした権限の設定がますます重要になる。

9．参 考 文 献

1） 羽鹿健，他：アイリス認識システムの金融機関への適用，沖電気研究開発第181号，Vol66，No.2，pp.47～50，1999

＊1）WindowsNT，Windows2000は米国Microsoft Corporationの商標。　＊2）アイリスパス®は沖電気工業（株）の商標。