〈ソフトウェア〉

Express5800のセキュリティソフトウェア

Security Software for Express5800

清水孝弘* 田中伸佳** 後藤 淳** 下河浩樹*
Takahiro Simizu Nobuyoshi Tanaka Jun Gotoh Hiroki Shimokawa

要 旨

近年，コンピュータセキュリティに対する脅威はますます高まりつつあります。NECは，IAサーバ（Express5800）におけるそれらの脅威を解決するため，各種のセキュリティ対策ソフトウェアを開発しています。サーバのセキュリティが下がることで，業務の停止，個人情報の漏えいといったビジネスにとって致命的な事態を引き起こしかねないからです。本稿では，「情報漏えい」，「サーバへの不正アクセス」といったそれぞれの脅威からExpress5800を守るソフトウェアを紹介します。

Recently, computer security threats are more and more increasing. NEC has developed various security softwares to defuse the threats to IA server (Express5800), because in case the security level of the server goes down, fatal damage (e.g. leakage of personal information, stop of business) can be caused.

This paper introduces our security softwares which protect Express5800 from threats such as “leakage of information” and “illegal server access”.

1．まえがき

増え続けるウイルスや情報漏えいなどの脅威から守るために，NECでは2004年10月にExpress5800/セキュリティソリューションを発表しました。そのセキュリティソリューションの基盤に位置するのが，独自に開発したセキュリティソフトウェアを中心とした，Express5800 SecurePackシリーズです。

今回は，そのSecurePackシリーズのソフトウェアの中から，グループで鍵を共有することができる暗号ソフトウェアInfoCage/ファイル暗号，サーバからファイルを持ち出せないようにして機密情報の漏えいをガードするInfoCage/持ち出し制御，セキュリティレベルが低いPCからの接続を拒否することによりウイルス感染を防ぐServerW@llの3ソフトウェアについて紹介します。

2．InfoCage/持ち出し制御

2.1 InfoCage/持ち出し制御の概要

InfoCage/持ち出し制御は，各種サーバ上に格納されている企業の機密情報をクライアントPCや外部メディアなどへの書き込みや印刷などの方法により持ち出す行為を禁止し，内部からの情報漏えいを防止するシステムです。クライアントからの持ち出しを禁止する既存製品と比較して，InfoCage/持ち出し制御はサーバから外に出させないという制御により，機密情報の散在を防ぎ，より安全な運用，管理を実現しています。

2.2 InfoCage/持ち出し制御のコンセプトと特長

(1) コンセプト

これまでサーバ上の情報は，利用者ごとにアクセス権限を設定することでセキュリティを確保していましたが，昨今の情報漏えい事件では，アクセス権を有する正規ユーザからの漏えいが問題となっています。このような市場環境を受け，InfoCage/持ち出し制御は，情報共有の利便性は損なわず，アクセス権限を有する正規ユーザからの漏えいを防止する，というコンセプトに基づき開発されました。

(2)「移動させない」

従来の同様製品では，クライアントPCからのファイルの持ち出しや印刷禁止などを行っていました。しかし，これでは機密情報のコピーが複数のクライアントPCに存在してしまいます。情報管理の基本は，対象を明確化してそれを分散させないことです。また，個人情報保護法では情報漏えいだけではなく，データの一貫した管理も要求しています。情報の分散を許したのでは，これが不可能になってしまう恐れがあります（**図1**）。

(3) Webサーバへの対応

機密情報が格納されるサーバ（以降，「機密サーバ」）として，ファイルサーバだけではなく，Webサーバにも対応しています。特に，Webベースの業務システムに適用しやすいアーキテクチャのため，CRMや既存の文書管理システ

* 第二コンピュータソフトウェア事業部
2nd Computers Software Division

** ユビキタスソフトウェア事業部
Ubiquitous Software Division

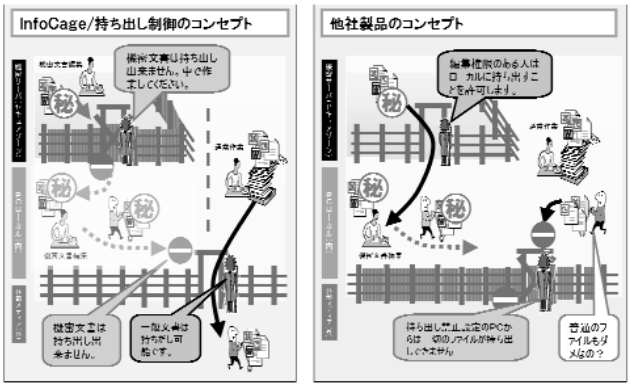

図1　「移動させない」-InfoCage/持ち出し制御のコンセプト
Fig.1　Concept of InfoCage/Information Restrict - Stop moving!

ムなどとの連携が容易です。

（4）業務への影響の少ない持ち出し制御

InfoCage/持ち出し制御は，機密サーバ上の文書のみに対して持ち出し制御を行います。機密サーバ以外のサーバ上にある文書やクライアントPC内の文書に対しては従来通りの操作を許可しています。これにより，自由度は維持しながら，大事な情報のみを守ります。

（5）多様なルートでの持ち出し制御

InfoCage/持ち出し制御では，多様な情報漏えいルートに対応した持ち出し制御が可能です。USBメモリなどの外部メディアへの持ち出しや，印刷といった外部出力への対処に加え，電子メールへの添付，Webアップロードなどのネットワーク経由の漏えいにも対応しています。これらの制御ルールは，セキュリティポリシーとして，ユーザ，およびグループ単位に設定することができます（**図2**）。

2.3　InfoCage/持ち出し制御のシステム構成

InfoCage/持ち出し制御は主に，クライアントPCに常駐するソフトウェアと管理サーバから構成されます。クライアントPC上の常駐ソフトウェアは，管理サーバから配布されたセキュリティポリシーに基づき，機密サーバ上のファイルに対するユーザ操作を監視し，持ち出し制御を行います。管理サーバは，Windowsドメイン管理と連携し，セキュリティポリシーの設定，クライアントPCへの配布，および各クライアントのユーザ操作履歴を収集し，ログの一元管理を行います（**図3**）。

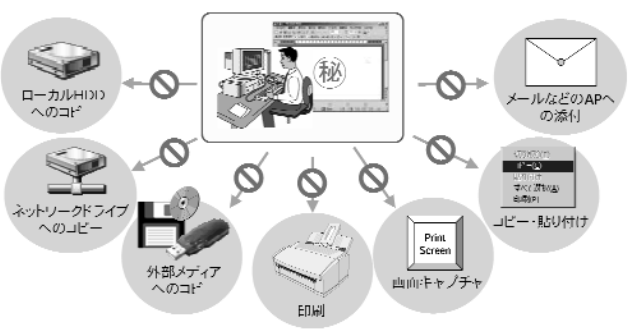

図2　多様なルートでの持ち出し制御
Fig.2　Protecting variety of leakage paths.

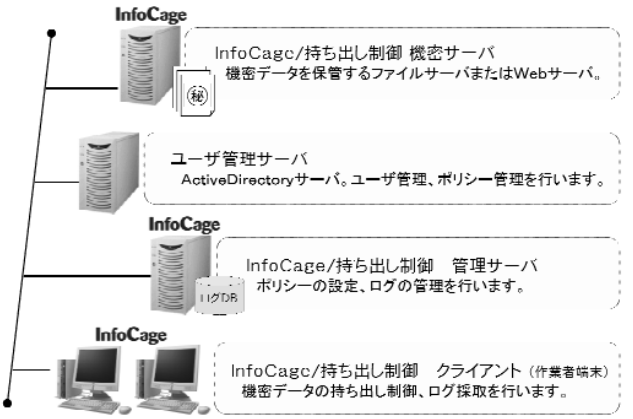

図3　InfoCage/持ち出し制御のシステム構成
Fig.3　Standard configuration of InfoCage/ Information Restrict.

以上のように，InfoCage/持ち出し制御は，業務効率を維持しながら，企業内の情報システムからの情報漏えいを防止する製品です。また，今後，暗号化製品やファイル操作追跡機能との連携を強化し，いっそう充実した情報漏えい対策機能を提供していきます。

3．InfoCage/ファイル暗号

3.1　InfoCage/ファイル暗号の概要

InfoCage/ファイル暗号は，重要データを安心してグループ内で共有するための暗号化ツールです。個々のファイル単位に暗号化を行い，暗号化に利用する鍵をグループで共有することで，組織内や組織間で流通する情報（ファイル）を守ります。また，簡単に導入することができるよう，ICカードやUSBトークンなど特別なハードウェアを必要としません。暗号アルゴリズムには，次世代暗号アルゴリズムであるAES（128ビット，192ビット，256ビット）および3DESを採用し，重要なファイルを強固に保護します。

3.2　InfoCage/ファイル暗号の特長

（1）簡単操作

暗号化ソフトウェアは，導入しても使われなければ意味がありません。InfoCage/ファイル暗号は，簡単な操作や自動暗号化フォルダ設定機能で暗号化の利用を促進します。ファイルの暗号化・復号は，ファイルを右クリックで選択して表示されるメニューから簡単に実行できます。また，任意のフォルダを自動暗号化フォルダに設定することが可能です。暗号化フォルダにファイルをドラック＆ドロップすると自動的に暗号化されるので，明示的な暗号化操作もほとんど必要ありません（**図4**）。暗号化フォルダ内では，ファイルをダブルクリックすることでファイルを復号し，拡張子に関連付けられたアプリケーションを起動する機能

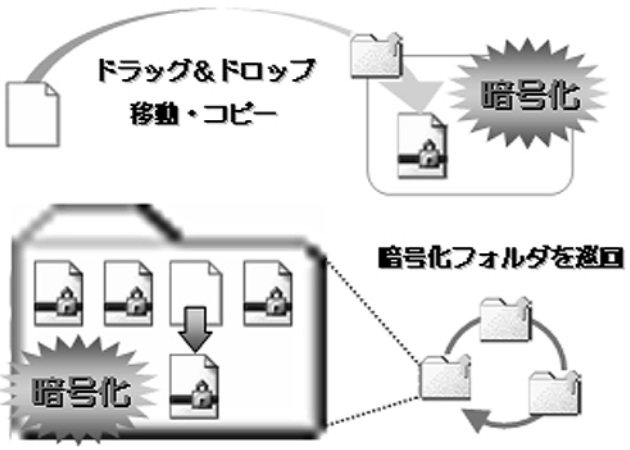

図4　簡単操作
Fig.4　Simple operation.

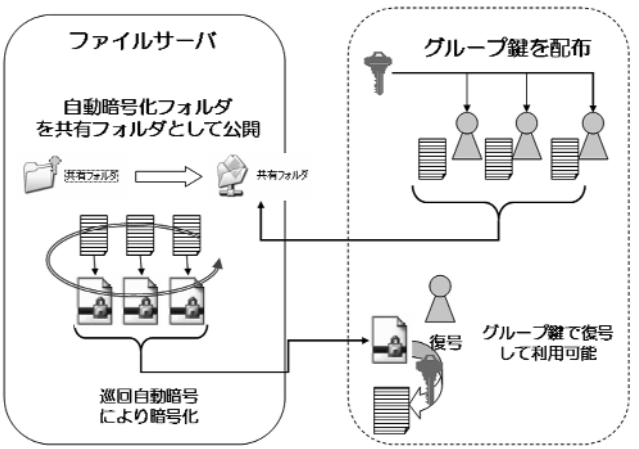

図5　ファイルサーバを用いた運用例
Fig.5　Application to file server.

を提供します。

(2) 自動巡回暗号機能

重要な情報を流通させるためには，暗号化を忘れないような対策が重要です。InfoCage/ファイル暗号は，暗号化忘れ対策として自動巡回暗号機能を提供します。この機能は，常駐プロセスが暗号化フォルダを定期的に巡回し，暗号化されていないファイルをそのフォルダに設定された暗号鍵で自動的に暗号化する機能です。

もう一つの暗号化忘れ対策機能として，リムーバブルメディアへの書き出しに対する自動暗号化機能を提供します。リムーバブルメディア（FD，USBメモリなど）へのファイルのドラッグ＆ドロップの操作を自動検知し，暗号化を促す確認ダイアログを表示します。これにより重要な情報をうっかり平文で持ち出してしまうことを防ぎます。

(3) 鍵共有による安全な情報共有

同じ社内でも取引先が違う場合や異なるプロジェクト間など，情報を秘匿化しなければいけない場合があります。InfoCage/ファイル暗号は，複数の鍵を作成する機能と鍵を安全に配布する機能で組織内での情報の閲覧制御を実現します。鍵配布は，簡単かつセキュアな方式として，鍵をパスワードで暗号化して配布する機能を提供します。また，よりセキュアな鍵配布方式として，公開鍵暗号方式を利用して送付先の公開鍵でファイル暗号化用の鍵を暗号化して送付する機能を提供します。これらの機能により，取引先ごと，プロジェクトごとのファイルの秘匿化が実現可能となります。

3.3　ファイルサーバを用いた運用例

自動巡回暗号機能と鍵共有の仕組みを応用することで，ファイルサーバの共有フォルダを使った安全な情報共有を実現できます。Windowsファイルサーバの共有ディレクトリ配下のフォルダを暗号化フォルダに設定し，そのフォルダに設定された鍵をメンバーで共有します。ファイルサーバに格納された共有情報はその鍵を持っているメンバーしか見ることができないので，安全な情報共有を実現できます（**図5**）。

3.4　InfoCage/ファイル暗号の効果

昨今の情報漏えい対策は，一般的な組織では何年も前から予見された事態ではありません。したがって，情報漏えい対策を実施しようとすると，予算を確保していない状況下での対策費の捻出を要求されます。さらに，クライアントに対しアクセス制御や利用制限をかけることになるので，利便性への影響や運用負担について慎重に検討する必要があります。このような状況に対し，InfoCage/ファイル暗号は手ごろな導入費と簡単な操作で，組織内や組織間で重要な情報（ファイル）の共有をすばやく手軽に実現します。

4．ServerW@ll

4.1　ServerW@llの概要

ServerW@llは，サーバへのアクセス条件をあらかじめ定義し，条件にあったPCのみをサーバへアクセスを許可することでサーバのセキュリティを向上させます。サーバ上のパケットフィルタでネットワーク経由のアクセスを制御しますが，IPアドレス/ポート/プロトコルによるフィルタだけでなく，クライアントPCのウイルス対策状況やMACアドレスによっても制限できることを特長としています。

4.2　ServerW@llの効果

次の2つの効果が期待できます。

・ウイルス対策
・許可されていないPCからの防御

(1) ウイルス対策

ウイルス対策の基本は，セキュリティパッチを適用することです。しかし，次のような理由から実際にはパッチがリリースされてもすぐに適用するのは難しいのが現実です。

・パッチの副作用を確認するために，事前評価が必要であること
・ベンダ製品のパッチ評価報告が必要であること

・24時間運用で再起動を要するパッチを適用できない

セキュリティパッチを適用できない状態は，ウイルス感染のリスクが大きく，何らかの対策が必要となります。サーバへのウイルス感染は，ウイルスに感染したクライアントPCを経由して感染することが多く，ウイルスに感染したPCをサーバにアクセスさせないようにできれば効果が期待できます。しかし，ウイルスに感染しているかどうかを正確に知る手段はありませんので，代わりに，ウイルス対策が不十分なPCはウイルスに感染している可能性が高いと判断し，サーバへのアクセスを制限します。

ウイルス対策を十分行っているかどうかは，

・OSのセキュリティパッチを全て適用していること

・最新のワクチンエンジン，パターン定義ファイルに更新されていること

で判断します。

ワクチンに関しては，3日以内に更新すればOKというように，運用性を重視した設定も可能としています。

(2) 許可されていないPCからの防御

情報漏洩対策やサイバーアタック対策として，サーバにアクセス可能なクライアントPCを必要最小限に制限することは，有効な手段です。ユーザ認証による制限だけでなく，ネットワークのレベルでアクセス制限することで，許可されないPCからのセキュリティホールを利用した侵入を防ぐことができます。

また，サーバにアクセス可能なPCを制限することで，ウイルスに感染したPCからアクセスされる可能性も少なくしますので，ワクチンが未対応の新種ウイルスの対策としても有効です。

4.3 ServerW@llの実現方法

サーバへのアクセス制限を実現するために，ServerW@llは，次の3つのコンポーネントで構成されます。

・サーバ上でアクセス制御を行うパケットフィルタ

・クライアント上でウイルス対策情報を収集するエージェント

・エージェントより収集した情報によってパケットフィルタにアクセス可否の指示を出す管理サーバ

動作概要は次のようになります（**図6**）。

① サーバ上のパケットフィルタは，初期状態としてすべてのアクセスを拒否する

② エージェントは，クライアントPCの起動時にウイルス対策状況をチェックし，管理サーバに報告する

③ 管理サーバは，サーバへのアクセス条件を満たしていれば，パケットフィルタに対して該当するPCをアクセス許可にするよう設定変更指示を出す

④ パケットフィルタは設定を更新し，指示のあったクライアントPCからのアクセスを許可する

MACアドレスでのフィルタの実現は以下のようになります。②でPCのMACアドレスを管理サーバに報告し，③で管理サーバは登録済みのMACアドレスかどうか判断します。登録済みだった場合，パケットフィルタに対して対応するIPアドレスのアクセス許可指示を出します。

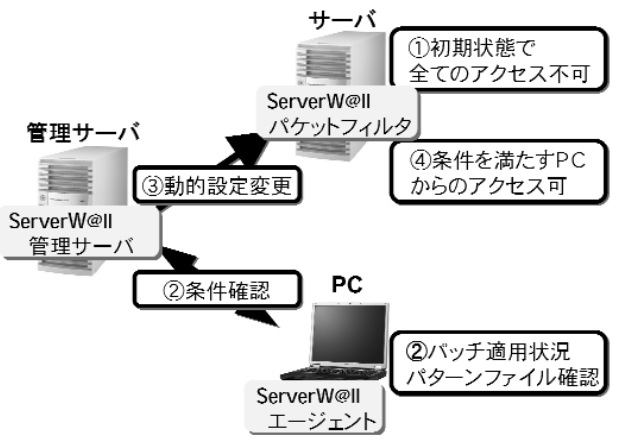

図6 ServerW@ll動作フロー
Fig.6 Operation flow of ServerW@ll.

社内ローミングを行う無線LANなど，IPアドレスを固定化できない場合にも，MACアドレスを条件とすることでサーバにアクセスできるPCを限定することができます。

4.4 ServerW@ll今後の強化

サーバにアクセスするための条件として必要なものは，今後も強化します。たとえば，PCが登録されたものかどうかを確実に識別するための手段として，セキュリティチップ（TPM）搭載PCでは，H/Wと連携した証明書による識別を予定しています。

セキュリティと運用性はバランスをとることが大切です。サーバによってアクセスするためのポリシーを柔軟に設定可能とし，運用性をあまり損なわずにセキュリティを向上させられるような製品を，今後も提供していきたいと考えています。

5．むすび

以上，Express5800 SecurePackシリーズのソフトウェアの紹介をしました。

これらのソフトウェアを使うことにより，セキュアなサーバを構築することができます。

今後も，前述のソフトウェアを強化していくとともに，さまざまなセキュリティソフトウェアの開発をしていきます。

筆者紹介

Takahiro Simizu
清水 孝弘（しみず たかひろ） 1986年，NEC入社。現在，コンピュータソフトウェア事業本部第二コンピュータソフトウェア事業部エキスパート。

Nobuyoshi Tanaka
田中　伸佳　1984年，NEC入社。現在，システムソフトウェア事業本部ユビキタスソフトウェア事業部シニアマネージャー。

Jun Gotoh
後藤　　淳　1999年，NEC入社。現在，システムソフトウェア事業本部ユビキタスソフトウェア事業部勤務。

Hiroki Shimokawa
下河　浩樹　1987年，NEC入社。現在，コンピュータソフトウェア事業本部第二コンピュータソフトウェア事業部主任。