〈製品/ソフトウェア〉

UNIVERGEセキュリティソフトウェア

UNIVERGE Security Software

福田光司* 中田浩章* 酒井雅啓**
Koji Fukuda Hiroaki Nakada Masahiro Sakai
宮崎義昭* 後藤 淳* 藤沢哲也***
Yoshiaki Miyazaki Jun Gotoh Tetsuya Fujisawa

要 旨

近年，悪質なウイルスやワームによる被害，個人情報の漏えい事件が社会問題化してきています。NECでは，これらに対応するためのソフトウェア製品を提供しています。

本稿では，これらのソフトウェアについて紹介します。

Recently, damages caused by brutal viruses and worms have become huge and leakage of personal information has been recognized as a social issue. NEC has provided various software products as countermeasures against these incidents.

This paper introduces these software products.

1. はじめに

最近になって，ウイルスやワームはますます凶悪化し，企業に大きな被害を与えるようになってきています。一方，個人情報漏えい事件も毎日のように新聞やテレビをにぎわせています。こちらは，金銭的被害だけではなく，企業イメージというお金にかえがたい財産にも大きなダメージを与えることになります。NECでは，UNIVERGEハードウェアと連携して，これらの被害を防止するUNIVERGEソリューションを実現するセキュリティ製品群を提供しています。

本稿では，これらソフトウェアのなかから，サイバーアタック対策製品CapsSuite，SecureVisor，情報漏えい対策製品InfoCage，CryptSec（SecureWare/ファイル暗号化ツール），MobileProtectを紹介します。

2. サイバーアタック対策統合管理ソフトウェア CapsSuite

CapsSuiteは，企業のネットワーク（NW）上のIT資産をすべて洗い出し，各クライアントマシンやサーバのセキュリティ状態（セキュリティパッチやウイルス対策ソフトの更新状況）を総合的に計数管理するシステムです（図1）。

CapsSuiteの主要機能は，統合管理サーバ，NW管理サーバ，PC管理サーバから構成されます。NW管理サーバは，ブロードキャストセグメントにエージェントを配置し，セグメント上のすべての資産をリストアップし統合データベース（DB）に送付します。また不正接続パソコン（PC）の検出・遮断が可能です。

PC管理サーバは，各クライアントやサーバに「パソコン見張り隊」というエージェントをインストールし，セキュリティ情報や資産情報を収集し，統合DBに送付します。また，ITの知識がない人にもパッチ適用を可能にする「パッチチェックビューア」により，パッチ適用の促進を図ります。

統合管理サーバはNW管理サーバ，PC管理サーバの収集した情報をWebシステムで，総合的に管理します。2つの情報を使用することにより，エージェントの入っていないパソコンのリストアップや，ネットワークセグメントごと

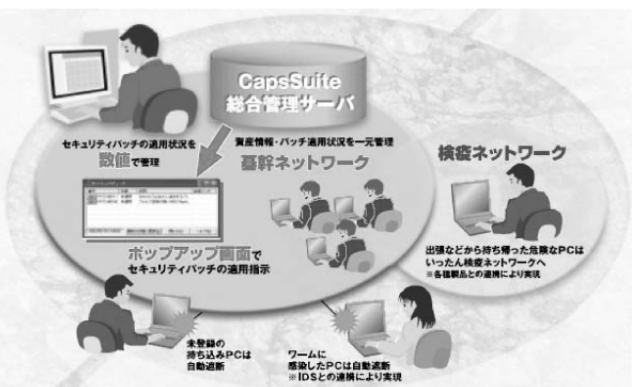

図1 CapsSuiteの概要
Fig.1 Overview of CapsSuite.

＊ ユビキタスソフトウェア事業部
Ubiquitous Software Division
＊＊ 市場開発推進本部
Market Development Division
＊＊＊ NECシステムテクノロジー エンベデッドソフトウェア事業部
NEC System Technologies, Ltd.

のセキュリティ状態の管理を実現します。

さらにCapsSuite V3では，強制的にパッチを配信することにより，パッチ適用を促進可能な「強制配信オプション」が追加されています。

また，持ち出しPCからのウイルス持ち込み対策に有効な，ネットワーク接続時にセキュリティ状態をチェックし，セキュリティレベルの低いPCを「検疫ネットワーク」に振り分けウイルス持ち込みを水際で阻止する「検疫機能」や，ウイルスを持ち込んだ際にUNIVERGE WormGuard IPシリーズと連携し，ウイルスに感染したPCをネットワークから切断する機能，各資産のリース管理やライセンス管理を実現する資産管理製品との連携が追加されています。

以上のように，CapsSuiteは，NEC社内のサイバーアタック対策システムCAPSの実績をベースに，より進んだ企業のセキュリティ対策を実現する製品です。

3. 不正接続防止システムSecureVisor

SecureVisorは，LANに接続されているネットワーク機器の台帳情報収集，不正接続検知/遮断，各クライアントにインストールされているウイルスチェックソフトの状況を収集するソフトウェアです。DomainManager，Site Manager，NetworkAgent，HostAgentから構成されます。

NetworkAgentはLANを流れるパケットを常に監視・解析し，MACアドレスやプロトコルアドレス，コンピュータ名などの情報を取得します。また，パケットの癖から，各クライアントのOS種別を推測することもできます。取得した情報はSiteManager上でホスト一覧として表示されます（図2）。

管理者が承認していないクライアントがLANに接続された場合，NetworkAgentがLANに流れるパケットからこのクライアントを瞬時に検知し，SiteManager経由で管理者に通知します。また，管理者が不正接続防止機能を有効にしていた場合，この不正接続されたクライアントのネットワークへのアクセスを遮断することもできます。ネットワークへのアクセス遮断は，承認されていないMACアドレスに関するARPパケットを収集した際，偽装ARPパケットを送信することで実現されています。

ウイルスチェックソフトの状況を収集する場合には，各クライアントにHostAgentをインストールします。このHostAgentが各クライアントにインストールされているウイルスチェックソフトの製品名，バージョン，DATバージョン，エンジンバージョン，最終ウイルスチェック日の情報を収集し，ホスト一覧に情報が表示されます。

このように，SecureVisorは様々なネットワークセキュリティソリューションを提供します。また，当製品はNEC内のサイバーアタック対策システムCAPSおよびCAPSの製品版CapsSuiteにも活用されています。また，最新版のV2.0では，UNIVERGE WormGuard IPシリーズと連携し，ワームに感染したPCをネットワークから切断する機能をサポートしています。

4. 内部情報漏えい対策システム InfoCage

InfoCageは，各種サーバ上にあ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（図3）。

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。

製品の特長は次の3点です。

1）機密情報が格納されるサーバ（機密サーバ）として，

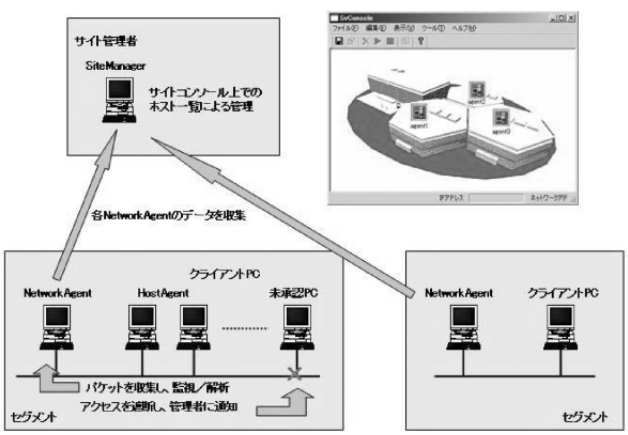

図2　SecureVisorの概要
Fig.2　Overview of SecureVisor.

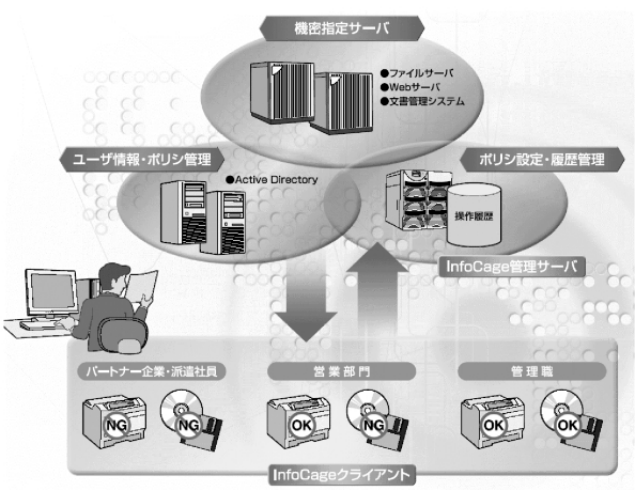

図3　InfoCageの概要
Fig.3　Overview of InfoCage.

ファイルサーバ，Webサーバの双方に対応しています。また，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，既存の文書管理システムなどとの連携が容易です。

2）機密サーバ上の文書のみに対して持ち出し制御を行い，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。

3）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。これらおのおのの制御ルールは，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。

InfoCage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。

以上のように，InfoCageは，業務効率を維持しながら，企業内のあらゆる情報システムからの情報漏えいを防止する製品です。

5. CryptSec（SecureWare/ ファイル暗号化ツール）

CryptSecは，機密データを安心して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，端末自身ではなく，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，様々な組織やプロジェクトで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。CryptSecは，簡単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。この暗号化フォルダにファイルをドラッグ＆ドロップすると自動的に暗号化されます（図4）。

機密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。CryptSec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に設定された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発見すると，そのフォルダに設定された暗号鍵でファイルを自動的に暗号化する機能です。

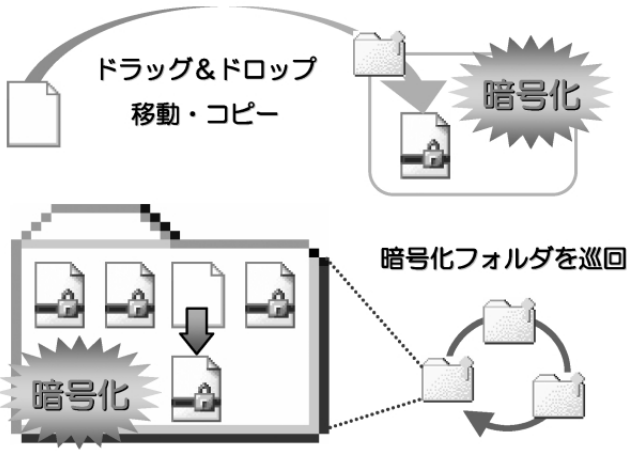

図4　CryptSecによる暗号化
Fig.4　Encryption with CryptSec.

CryptSecで暗号化されたファイルは，メールに添付しても暗号化されたままですので，機密状態を保持したままほかのメンバーにファイルを送付することができます。また，間違った相手に届いてもファイルの内容を見られる心配がありません。

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ことがあります。CryptSecは，複数の鍵を作成する機能と鍵を安全に配布する機能を提供しています。これにより，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です。

以上のように，CryptSecは，組織内や組織間で機密情報（ファイル）の共有を素早く手軽に実現できる製品です。

6. モバイル情報保護MobileProtect

MobileProtectは，情報漏えい対策のなかでも関心の高い課題の1つである，モバイル情報の保護を目的とした製品です。市販の安価なリムーバブルメディアを利用し，PCの認証機能による不正利用の防止や，データの暗号化によるPCやリムーバブルメディアの盗難・紛失時の情報流出を防止する機能を提供します。

MobileProtectは，PCとリムーバブルメディアがお互いの鍵となる設定をすることで，相互認証の仕組みを利用した強固な情報保護を実現しています。以下に，MobileProtectの主な利用方法を説明します（USBメモリを利用した例）。

1つ目は，PCの起動制御にUSBメモリを利用する方法で，あらかじめ鍵として設定されたUSBメモリがポートにさされた状態でなければ，PCへのログインをできなくすることができます。また，離席時にUSBメモリを抜くことで，PCをロック（第3者が利用できない）することが可能です。

2つ目は，データの暗号化で，PC内部に保管された機密情報をUSBメモリの鍵で暗号化することができます。万が一，PCが盗難にあった場合でも，鍵であるUSBメモリが

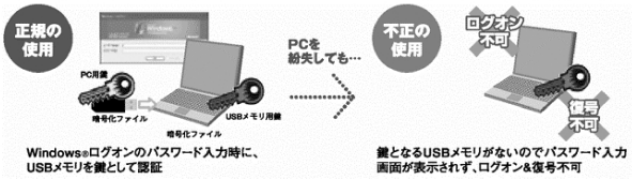

図5　MobileProtectによる認証と暗号化
Fig.5　Authentication and encrypting by MobileProtect.

なければ，データの中身を盗まれる心配はありません。また逆に，USBメモリに書き込む情報を，PCや別のUSBメモリに保管された鍵で暗号化することも可能です（図5）。

MobileProtectの暗号化機能は，ファイルの拡張子やサイズに影響を与えず，また暗号/復号時に特別な操作を必要としないため，利用者に意識させることなく安全なデータ保護を実現できます（暗号化アルゴリズムはAES 128bit）。

3つ目は，データの抜き取り防止で，これはあらかじめPCに利用登録したUSBメモリ以外へのデータの書き出しを防ぐ機能で，第3者によるPCからのデータの抜き取りを防止することができます。

また，これまで説明したUSBメモリに鍵を格納する方法のほかに，ネットワーク上の共有サーバに鍵を格納する設定が可能で，この場合には，社内ネットワークに接続されている状態でのみ，暗号化データへのアクセスを許可するような利用が可能となります。

以上のように，MobileProtectは，大がかりな環境を必要とせず，モバイル環境における情報保護を簡易に低コストで実現する製品です。

7. むすび

以上，NECが提供するサイバーアタック対策製品，情報漏えい対策製品を紹介しました。

来たるサイバー社会，ユビキタス社会ではセキュリティの重要性がよりいっそう増してきます。NECは，ネットワークとIT，ハードウェアとソフトウェア，サービスをすべて提供できる企業として，今後もセキュリティ製品を強化し，UNIVERGEソリューションとして提供していきます。

筆者紹介

Koji Fukuda
福田　光司　1982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エンジニアリングマネージャー。

Hiroaki Nakada
中田　浩章　2000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主任。

Masahiro Sakai
酒井　雅啓　1992年，NEC入社。現在，ソリューション開発研究本部市場開発推進本部マネージャー。

Yoshiaki Miyazaki
宮崎　義昭　1987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エンジニアリングマネージャー。

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。

Tetsuya Fujisawa
藤沢　哲也　1984年，NECソフトウェア関西入社。現在，NECシステムテクノロジー プラットフォーム事業本部エンベデッドソフトウェア事業部長。