2016 年 12 月 16 日
株式会社セキュアソフト

『SecureSoft S-コンテナ』の活用方法のご紹介

2016 年はランサムウェアがとても話題に上がった 1 年になりました。SecureSoft では 3 月に『SecureSoft i-コンテナ』（以下、i-コンテナ）をリリースしてから、マルウェア対策として非常に多くの引き合いをいただいております。2016 年 10 月には、i-コンテナのブラウザ専用版である『SecureSoft mamoret』(以下、mamoret）を発表しました。マルウェアの脅威から業務システムを守るソリューションとして 12 月 6 日に ITPro Active に掲載していただきました。詳しくは下記の URL をご参照ください。

~ITpro Active 掲載記事~
『最終手段は業務 PC とインターネットとの分離。低コストで実現する方法とは』
http://itpro.nikkeibp.co.jp/atclact/activesp/16b/111600052/

今回は、i-コンテナと同時にリリースした『SecureSoft S-コンテナ』（以下、S-コンテナ）について紹介させていただきます。S-コンテナは情報漏えいに特化した製品（ソフトウェア）です。業務 PC に S-コンテナをインストールすると、次世代仮想化技術で安全な環境を業務 PC に実現します。企業は業務 PC 単体で業務を行っているのではなく、組織のネットワーク内で業務を行っています。そうした組織を意識した S-コンテナによる安全な環境の活用例について以下に記載いたします。

～S-コンテナの３大活用例～

①ポリシーの一元管理できめ細やかな内部統制の実現

企業では各システムの管理サーバを管理ネットワークに設置します。S-コンテナでも同様に管理サーバである SecureSoft Control Center（以下、SCC）を管理ネットワークに設置して、ネットワーク内の全クライアントのデバイスコントロールを行うことができます。デバイスコントロールのポリシーは、営業ネットワークには「ポリシーA」、開発ネットワークには「ポリシーB」というように、グループごとに設定できるので、グループに応じた最適なポリシーを簡単に管理できます。

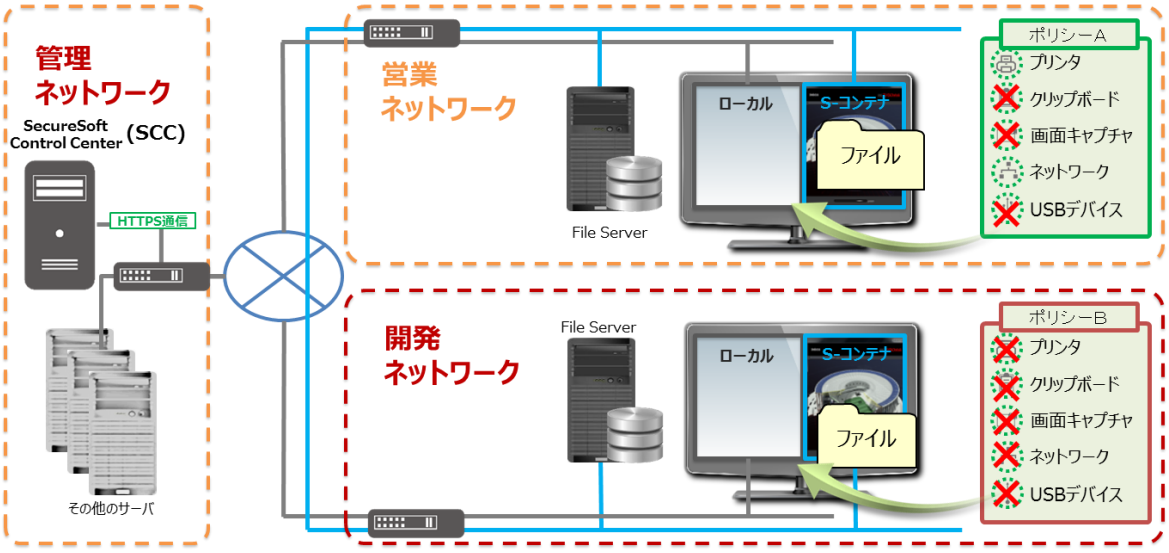

図 1 内部統制強化イメージ

②PC 紛失時でも重要データの漏えいを防止

S-コンテナで使用するデータは AES256（Advanced Encryption Standard）を採用しています。万が一 PC を紛失し、HDD 内のデータを不正読み出された場合でも、S-コンテナ内のデータが解析されて重要な情報が漏えいする心配はありません。また、通常 S-コンテナは SCC と通信してオンラインで使用しますが、客先や出張などの外出先で SCC と通信できない場合はオフラインで使用できます。ポリシー設定でオフラインの使用日数を制限することで S-コンテナへのログインを最小限に制限でき、持ち出し PC のセキュリティ統制に役立ちます。

図 2 PC の紛失対策イメージ

③企業間で安全なデータ共有環境を実現

業務を協力会社に委託する場合は、協力会社の業務 PC に S-コンテナをインストールすることで、コンテナ環境のネットワークが構築できます。それぞれの会社の S-コンテナ間を VPN で接続することで、重要な情報を安全に共有できる空間を実現できます。

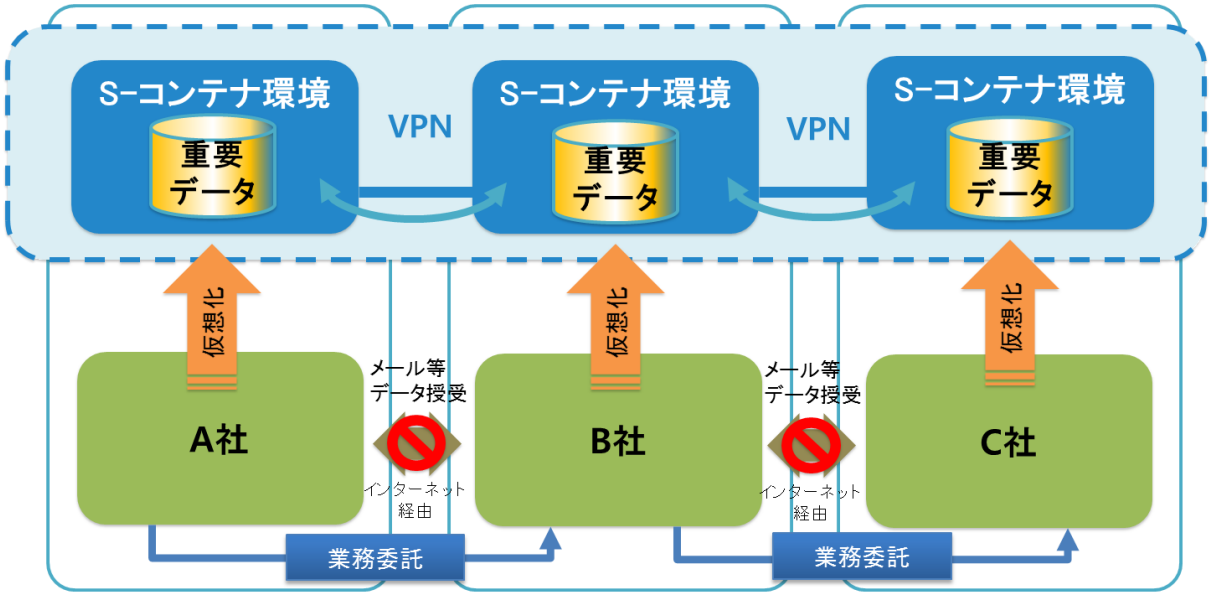

図 3 企業間の安全な業務連携イメージ

以上が S-コンテナの 3 大活用となります。その他コンテナシリーズについてのご質問や情報セキュリティ対策についてのご相談を随時受け付けておりますので、下記連絡先までお気軽にお問合せください。
また、i-コンテナ、mamoret についてのわかりやすい動画を公開しておりますので是非ご覧ください。

■SecureSoft i-コンテナ 『SecureSoft i-コンテナ ご紹介動画』
https://www.securesoft.co.jp/products/i-container/outline/

■SecureSoft mamoret 『SecureSoft mamoret ご紹介動画』
https://www.securesoft.co.jp/products/mamoret/

株式会社セキュアソフト
〒150-0011
東京都渋谷区東 3 丁目 14 番 15 号 MO ビル 2F
TEL 03-5464-9966
FAX 03-5464-9977
sales@securesoft.co.jp