特別論文

MCRにおける情報セキュリティ強化への取り組み

本社　技術推進部　技術管理課
安孫子 喜則

1．まえがき

昨今、情報セキュリティに対する脅威は増すばかりである。これに対し、当社では、情報セキュリティの脅威に対処するための活動として、情報セキュリティレベルの数値化と評価結果に基づく改善に全事業所で取り組んでいる。

当社では、表1に示すとおり、情報セキュリティに関する11の対策項目を選定し、夫々に3～5段階の達成レベルを定義している。

毎年度、各事業所での達成レベルを評価し、改善目標レベルを定め、具体的なアクションプランとして作成し、改善活動を進めている。併せて、情報インフラを活用したセキュリティ強化策も進めている。

本稿では、この改善活動の概要と、下記2点の、情報インフラ強化策を紹介する。

①インターネット利用時のセキュリティ強化
②執務端末のセキュリティ強化

2．情報セキュリティ対策のレベル評価と改善活動

2.1　改善活動の流れ

情報セキュリティ対策は、三菱電機やMCR本社の指示で事業所毎に進めていたが、達成度を十分に評価できておらず、実施内容にバラツキがあった。

そこで、2015年度に対策実施の達成度を自己評価するための管理様式を策定し、各事業所での評価結果から改善するレベルの設定と、目標達成に向けたアクションプランを策定する流れ(図1)とした。

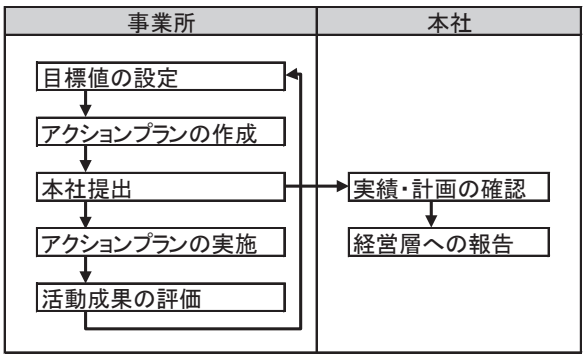

図1．情報セキュリティ対策活動の流れ

2.2　対策項目の選定

情報漏えいの防御や、事故発生による被害の最小化を目的とし、11の情報セキュリティ対策項目(表1)を選定した。

項目選定にあたっては、情報セキュリティ監査での確認項目やこれまでに発生したヒヤリハットや事故発生のリスクを検討し、整理した。

表1．11の情報セキュリティ対策項目

No.	対策項目
1	リモートデスクトップの制限
2	サーバのフォルダ、ファイル管理 ①不要フォルダ、ファイルの削除 ②サーバのドライブマウントの制限
3	フォルダアクセス権限の見直し
4	「受渡し」「公開」フォルダの定期的な削除
5	フォルダ名、ファイル名漏えいに対する防御
6	電子ファイルの暗号化
7	フリーソフトウェアの利用制限
8	電子メールの社外発信制限
9	インターネット接続制限
10	執務PC/開発PCの分離
11	電子メール環境 ①個人アドレス帳への登録に関する運用 ②不要メールの定期削除

各対策項目では、実施すべき事項を細分化し、実施内容として整理した。

例えば、表1のNo.1「リモートデスクトップの制限」では、表2の内容を確認している。

表2．「リモートデスクトップの制限」での実施内容

No.	実施内容
1	リモートデスクトップは禁止設定を標準とし、必要な場合は上長が許可する。
2	許可する場合は、IPアドレス制限、アカウント制限の両方を設定する。
3	リモートデスクトップを使用するユーザのパスワードは17文字以上に設定する。
4	リモートログインを許可した端末は、ログイン履歴を蓄積し、不正なログインが無いことを定期的に確認する。
5	各端末に不要なユーザアカウントが無いことを確認する。

2.3　対策レベルの評価

選定した11の対策項目について、3～5段階で対策レベルの評価基準を整理した。対策の実施範囲(個人や課、事業所など)、対策方法(個人、組織の仕組み、システム化など)、

運用の定着状況などで対策レベルを評価している。

例えば､｢リモートデスクトップの制限｣では、表3の評価基準を設定している。

表３．「リモートデスクトップの制限」での評価基準

Lv.	評価基準
1	端末使用者による設定を確認した（実施のエビデンスなし）
2	端末使用者による設定を確認した（実施のエビデンスあり）
3	レベル2と定期的な棚卸し（エビデンスあり）が行われている
4	第3者による確認が定期的に行われている（エビデンスあり）
5	端末管理ツールが導入され、情シ部門による設定となっている

11の対策項目に対し、個々に評価基準を定め、図2の評価様式で管理している。

No.	対策項目	内容	レベル ※網掛けは必須レベル		16年度実績	17年度目標	17年度実績
1	リモートデスクトップの制限	①リモートデスクトップは禁止設定をデフォルトとし、必要な場合は上長許可とすること。 ②許可する場合は、IPアドレス制限、アカウント制限の両方を設定すること。 ③リモートデスクトップを使用するユーザのパスワードは17文字以上とする。 ④リモートログインを許可した端末は、ログイン履歴を蓄積して、不正なログインが無いことを定期的に確認すること。 ⑤各端末に不要なユーザアカウントが無い状態とすること。	1	端末使用者による設定を確認した（実施のエビデンスなし）	3	5	
			2	端末使用者による設定を確認した（実施のエビデンスあり）			
			3	レベル2と定期的な棚卸し（エビデンスあり）が行われている			
			4	第3者による確認が定期的に行われている（エビデンスあり）			
			5	端末管理ツールが導入され、情シ部門による設定となっている			

図２．情報セキュリティレベルの評価様式（抜粋）

2.4　評価結果に基づく改善活動

各事業所は、前述の評価基準に基づき、対策の実施状況を評価している。現状の確認結果から、改善事項を整理し、毎年度の情報セキュリティアクションプランを作成、改善活動を進め、PDCAを回している。

アクションプランの内容や活動状況は、社内で年2回実施してる内部情報管理監査で確認している。

これまで、情報セキュリテイ対策は、事業所毎に実施され、定性的な評価に留まっていた。対策項目とその実施内容を明確にし、評価基準を整理したことで、定量的な評価が可能となった。これにより全社台でのレベル確認ができ、対策内容に関する情報交換、展開が促進されたと評価している。

2.5　今後の展開

各事業所の対策レベルの推移は、表4のとおりである。2015年度から開始した本活動は、全事業所でレベルが改善され、底上げを図ることができた。

各事業所では、三菱電機の拠点毎にサーバ、端末の運用が異なるため、拠点特有の制約も明確になった。

今後は、一律のレベル評価限界を判断し、現状レベルの維持と、拠点に特化した改善を進めていく。

表４．各事業所の対策レベルと推移

事業所	15年度（評価）	16年度（実績）	17年度（目標）
A	33	44	55
B	29	42	51
C	34	46	52
D	31	44	52
E	19	33	48
F	24	32	46
G	19	32	42
平均	27	39	49

※数値は、11の対策項目で各レベル値を合計した値

３．インターネット利用時のセキュリティ強化

情報セキュリティ対策項目のNo.9｢インターネット接続制限｣の対策レベルを維持しつつ、柔軟なインターネットに利用するため、セキュリティブラウザを導入した。

本章では、導入経緯と構築環境の概要を紹介する。

3.1　MCRのネットワーク環境

当社の事業拠点は、対応する三菱電機の製作所内に所在しており、事業拠点の社内ネットワークは全て、三菱電機のイントラネット網に接続されている。

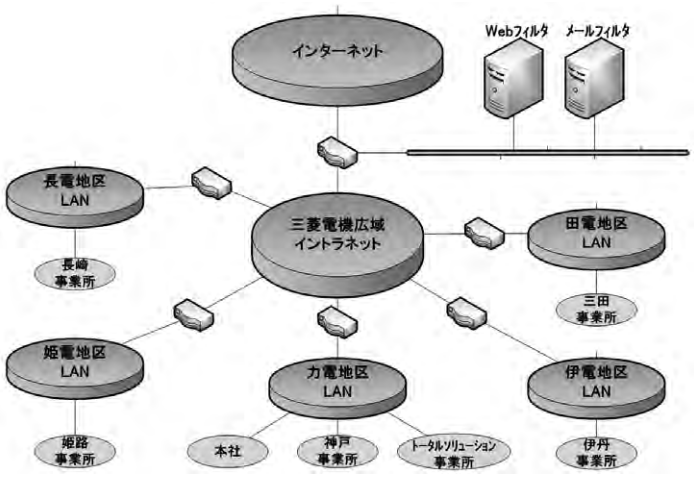

図３．MCRのネットワーク環境イメージ

3.2　リスク低減による作業効率の低下

神戸地区は、機密保持の観点からインターネット利用を制限してきた。情報セキュリティの脅威が高まる中、未知の脅威への対策として、2014年度にインターネット利用時のWebフィルタ運用をブラックリスト方式からホワイトリスト方式に変更した。

ブラックリスト方式は、Webフィルタリングによる既知の不正サイトへのアクセス制限を行うことで、外部からの

不正侵入を防御するものである。

また、ファイアウォールやproxyサーバによる外部からの侵入防御や、メールフィルタリングも既知の事象に対する防御策である。

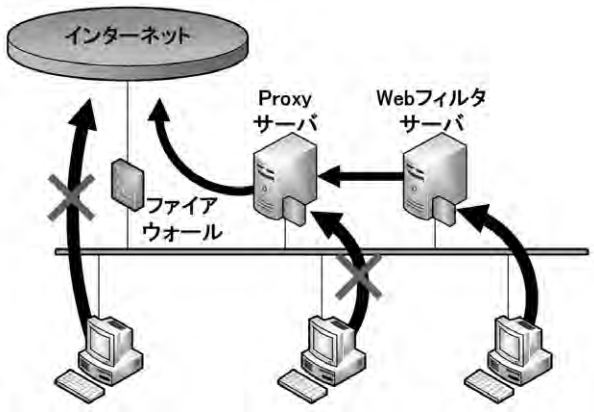

図４．Webフィルタリングによる接続構成

しかし、安全性が未確認の不正サイトに接続し、未知のウィルスをダウンロードした場合、ウィルス対策ソフトで検知できず、ウィルスに感染する可能性がある。

その対策として、Webフィルタリングをホワイトリスト方式での運用に変更した。ホワイトリスト方式は、安全性が確認されたサイトのみに接続する方式である。この方式の採用により不正サイトへの接続が不可となり、ウィルス感染した場合の情報流出も防ぐことが可能となった。

任意のインターネット検索は､執務LANと別のネットワーク環境に専用端末を設置し、作業する運用とした。

この結果、開発業務や事務作業を進める際に、インターネット検索で、作業効率の低下を招いた。

3.3　セキュアなインターネット環境の利用

情報セキュリティレベルを低下させることなくインターネットを利用するため、セキュリティブラウザを導入した。

セキュリティブラウザは、サーバ上に作成された仮想コンテナでブラウザを実行し、端末に画面情報のみを転送することで、安全なインターネット環境を提供する。

インターネット接続で仮想コンテナがウィルスに感染した場合、端末へは画像転送のみが行われているため、端末へのウィルス感染を防止できる仕組みである。

また、仮想コンテナは他の社内システムにアクセスできないネットワーク構成としており、ウィルス感染した仮想コンテナからウィルスが拡散されることはない。さらに、仮想コンテナは端末からの接続時に作成され、端末からのセッションが切断されると仮想コンテナは削除される。これによりセキュリティブラウザサーバ､仮想コンテナにウィルスが残存することもない。

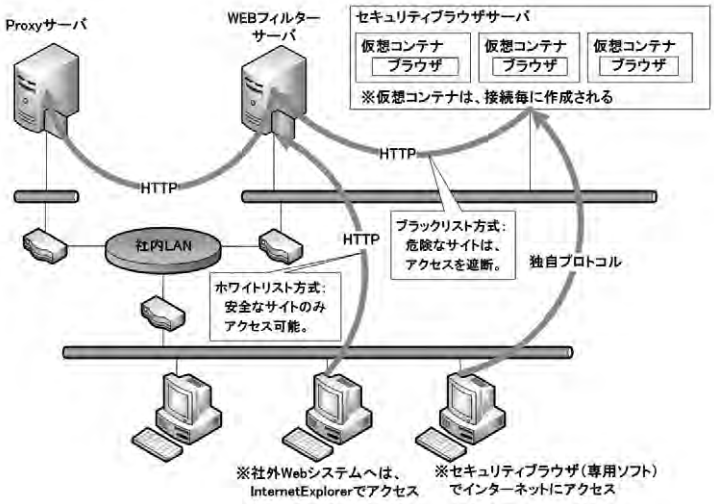

図５．セキュリティブラウザの仕組み

神戸地区で、セキュリティブラウザを導入し約1年が経過した。導入以降は、インターネット利用によるウィルス感染やウィルス検疫(発見)は発生していない。

４．執務端末のセキュリティ強化

情報インフラとしてのセキュリティ向上施策として、シンクライアント環境について紹介する。

4.1　シンクライアント環境の導入

執務端末のセキュリティを確保するためには、各種のパッチ適用や、定期的なウィルス検索を実施している。各実施状況は、台帳やサーバログの確認などで把握していたが、その確認作業や実施フォローに多くの時間を要していた。

そこで、執務端末について、セキュリティパッチの確実な適用や管理作業のレベルアップを目的として、2015年度に本社でシンクライアント環境を導入した。以降、段階的に拡充を進めている。2017年度末には全社員の執務端末は、約70%がシンクライアント化される見込みである。

表５．シンクライアント端末導入数の推移（単位：台）

事業所	15年度（実績）	16年度（実績）	17年度（見込み）	18年度（計画）
本　社	84	5		
神戸地区		101	720	
長　崎			220	
伊　丹			180	
姫　路				130
合　計	84	106	1120	130
累　計	84	190	1310	1440

4.2　シンクライアント環境の導入効果

これまでセキュリティパッチは、端末の電源投入時に適用されていた。これに対して、シンクライアント環境では夜間に自動適用し、担当者が不在の場合も適用する仕組みとした。また、ウィルス対策ソフトの予約検索も夜間に実施することにした。これまで、日中に実施していた予約検索での端末負荷が、これにより大きく軽減され、作業効率を改善できた。

4.3　高可用性を考慮したシンクライアント環境

シンクライアント環境は、各事業所にサーバを設置している。2016年度に神戸地区で構築した環境は、3台のサーバ構成とした。各サーバはハイパーバイザー(注1)をインストールしており、同一のクラスタグループで構成し、HA(High Availability)を実現している。HAとは、物理サーバの障害発生時に、そのサーバ上で動作していた仮想マシンを別の物理サーバで自動的に再起動する機能である。

この機能を活用し、継続的にサービスを提供する構成としている。

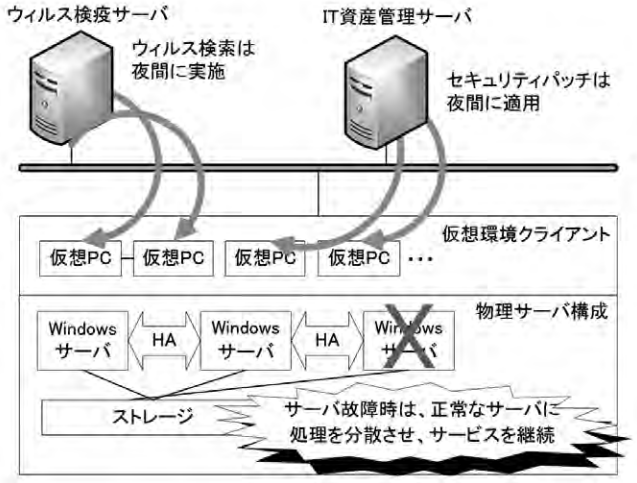

図6．シンクライアント環境

5．むすび

情報セキュリティのレベル評価は、2015年度から開始し、3年間の改善活動を経て、全事業所でレベルアップを図ることができた。

また、インターネット利用環境の分離におけるセキュリティブラウザの導入は、神戸地区での取り組み成果を2017年度に長崎事業所、伊丹事業所へ展開した。

シンクライアント環境は、2017年度中に1,300名余りの社員環境に導入する見込みである。

今後は、これまでに実施してきた対策の運用維持と、拠点特性を考慮した強化を進めて行く。

また、新技術を評価し、継続的な強化、改善に適用していく。

最後に、MCR全社での情報セキュリティ強化に際し、評価・分析・改善に取り組んでいただいている事業所情シ責任者、担当者をはじめ、関係各位に深く感謝申し上げる。

(注1) ハイパーバイザーとは、物理サーバ上で仮想サーバ（ゲストOS）を実行するためのソフト。

執筆者紹介

安孫子　喜則　　アビコ　ヨシノリ
1989年入社。主に情報ネットワークインフラの構築に従事。現在、本社技術推進部技術管理課。