特集論文

三菱電機グローバルIT基盤サービスのセキュリティ機能の拡充

小野明弘*
羽原　亮*
鎌田真吾*

Additional Functious to Sterngthen Security of Mitsubishi Electric Global IT Platform Service

Akihiro Ono, Ryo Hanehara, Shingo Kamata

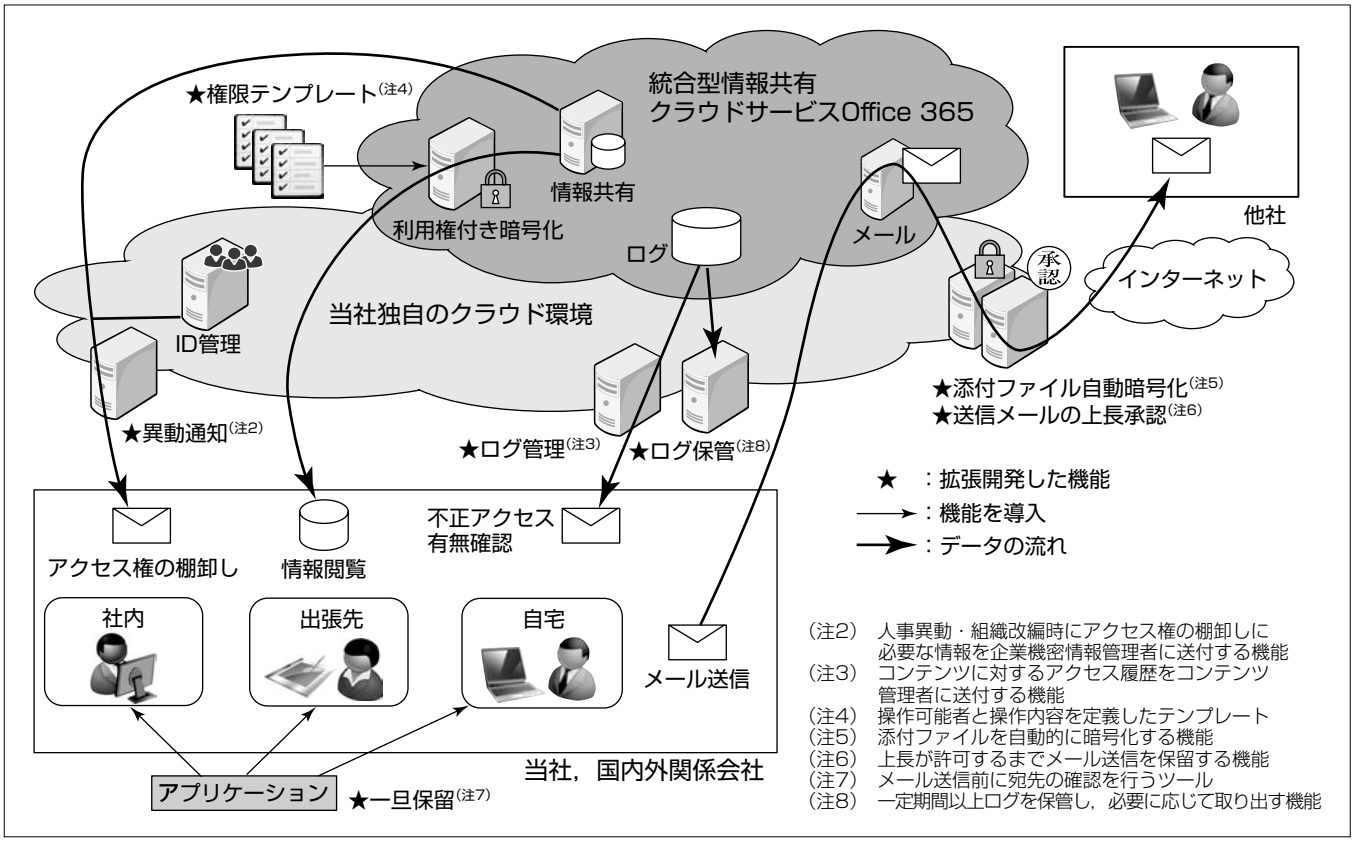
要　旨

三菱電機では，グループ約15万人のIT環境として，セキュリティ強化と業務の生産性向上を実現する“三菱電機グローバルIT基盤サービス“MELGIT（Mitsubishi ELectric Global IT platform service）””を構築した(1)。

MELGITでは，“いつでも，どこからでも，安心して，快適に利用できる仕組み”を実現するために，日本マイクロソフト㈱の統合型情報共有クラウドサービス“Office 365(注1)”と当社独自のクラウド環境を用いている。しかし，Office 365の標準機能だけでは，当社のセキュリティ要件となっている“厳密なファイル管理”“強固なメールセキュリティ”“十分な記録保管”などに対応できない部分があった。そこで，不足している機能を開発・拡充することでセキュリティを強化し，より高いセキュリティレベルで活用できるIT環境を整備した。

MELGITは，2018年８月末時点で，国内を中心に220拠点，約10万人が利用しており，新たなIT環境として定着しつつある。今後，利用者の利便性を向上させるOffice 365の新サービスが次々と導入されてくることが見込まれる。これを，“速やか”に活用できるようにセキュリティ機能拡充の継続と実現期間の短縮に取り組んでいく。これによって，“いつでも，どこからでも，安心して，快適に利用できる情報共有基盤”を継続的に改善し，当社グループの成長目標達成に貢献していく。

（注１）　Office 365は，Microsoft Corp.の登録商標である。



当社グローバルIT基盤の拡充とシステム構成

MELGITでは，アクセス権の棚卸しを支援する異動通知，不正アクセス有無の確認を支援するログ管理，利用権付暗号化の操作性を向上させる権限テンプレート，流出などによる情報漏えいを防止する添付ファイル自動暗号化，誤送信などによる情報漏えいを防止する上長承認や一旦保留，サーバに保管された情報へのアクセスの一定期間以上のログ保管などの機能を開発・拡充し，当社独自のクラウド環境などに配置している。

*IT戦略室

1. まえがき

当社グループ約15万人のIT環境として，セキュリティ強化と業務の生産性向上を実現する三菱電機グローバルIT基盤サービスMELGITを構築した。

MELGITでは，“いつでも，どこからでも，安心して，快適に利用できる仕組み”を実現するために，Office 365と当社独自のクラウド環境を用いている。しかし，日本マイクロソフト㈱のOffice 365の標準機能では，当社のセキュリティ要件となっている“厳密なファイル管理”“強固なメールセキュリティ”“十分な記録保管”などに対応できない部分があった。そこで，不足している機能を開発・拡充することでセキュリティを強化し，より高いセキュリティレベルで活用できるIT環境を整備した。

本稿では，MELGITのセキュリティ要件と，それらの開発の取組みについて述べる。

2. セキュリティ要件

サーバへの不正アクセス，ファイルの流出，メールの誤送信，セキュリティ対策の適用不備などのセキュリティリスクに対して，それぞれに具体的な対策を定めている。しかし，このうちの一部は，Office 365の標準機能での対応が困難であったため，不足している機能を開発することで拡充した。不足機能は次のとおりである。

2.1 厳密なファイル管理

・不要IDの残存確認(アクセス権の棚卸し)
・サーバに保管された企業機密情報(注9)へのアクセスログの定期確認(証跡管理)
・企業機密情報への利用権(誰が何をできるか)を設定した保護(利用権付暗号化(注10))

(注9) 企業機密や個人情報が保管されている媒体(ここでは電子ファイルを意味する)
(注10) ファイルに対して利用権を設定して暗号化することで，ファイルを保護する仕組み。

2.2 強固なメールセキュリティ

・他社など宛先に応じた添付ファイル送信時の暗号化(添付ファイル自動暗号化)
・他社への企業機密情報送信時の上長承認及び承認記録保管(上長承認)
・メール送信時の一旦保留と宛先再確認(一旦保留)

2.3 十分な記録保管

・ログの一定期間以上の保管(ログ保管)

3. 厳密なファイル管理

より安全にファイル利用できるようにOffice 365にはない，アクセス権の棚卸し，証跡管理，利用権付暗号化といった機能を開発・拡充し，厳密なファイル管理を実現した(**図1**)。

3.1 アクセス権の棚卸し

不適切な利用者からのアクセスを防止するため，“ファイルの機密等級(注11)に応じて個人単位，組織単位にアクセス権を設定すること”が必要である。

このため，適切なタイミングでアクセス権の設定内容を棚卸しできるようにOffice 365に保管されている企業機密情報の管理責任者に対して，人事異動や組織改編に合わせて，“異動者及び組織改編の情報”と“これらにアクセス権が設定されているフォルダの情報”をメールで通知する機能を開発した。

これによって，不正アクセスによる企業機密の漏えい・滅失・き損のリスクを低減している。

(注11) 情報漏えいした際の事業上の影響度に応じて定める等級。当社では極秘，秘，社外秘と定義している。

3.2 証跡管理

不正アクセスの早期発見と牽制(けんせい)による抑止のため，“企業機密情報を保管しているサーバへのアクセス履歴を定期的に確認すること”が必要である。

このため，漏れなく，効率的にアクセス履歴を確認できるように定期的にOffice 365のログからアクセス履歴を抽出し，“同一人物による大量ファイルへのアクセス”や“深夜などの特定時間帯でのアクセス”などの件数を集計した結果を，企業機密情報の管理責任者にメールで通知する機能と，企業機密情報の管理責任者がアクセス履歴の詳細を確認できる機能を開発した(**図2**)。

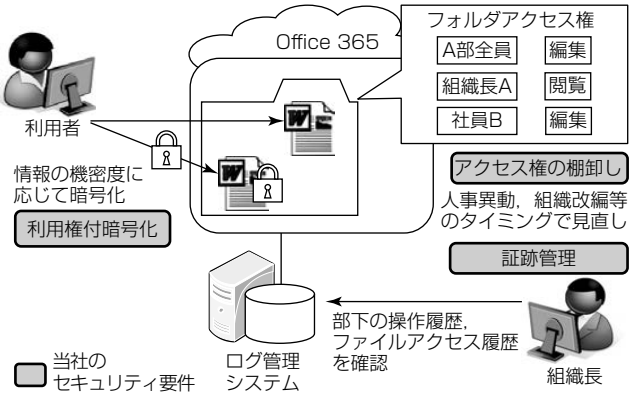


図1．ファイル管理要件

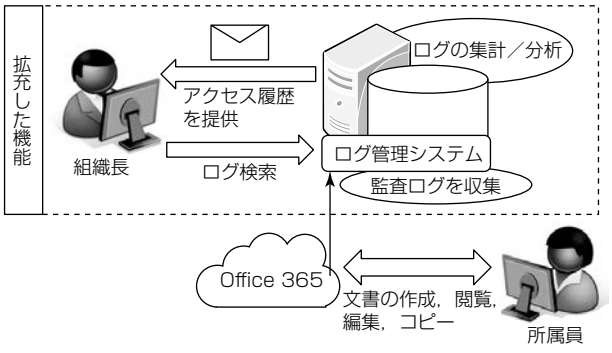


図2．ログ管理システム

これによって，企業機密情報の利用実態を把握して，業務が適切に行われていることを確認している。

3.3 利用権付暗号化

ファイル流出時のリスク対策として，“企業機密情報の機密度に応じた利用権設定と，暗号化して保管すること”，及び“ファイル流出時の追跡と，流出したファイルの閲覧を禁止できること”が必要である。

このため，日本マイクロソフト㈱が提供するAzure(注12) Information Protectionを採用したものの，このツールは，ファイルを暗号化する都度，複雑な利用権設定が必要であり，利用者に作業負荷がかかる仕組みであった。そこで，あらかじめ会社や組織に応じた利用権をテンプレート化しておくことで，利用者はファイル暗号化時に適切なテンプレートを選択するだけで，利用権を設定できる仕組みにした。また，利用権付暗号化ツールと当社グループの認証基盤(2)を連携させることで，アクセスできる利用者の範囲を人事異動に合わせて自動的に更新する仕組みにした。

これによって，適切な利用権の設定と維持ができるようになり，利用者が持ち出したファイルからの二次流出を防止している。

(注12) Azureは，Microsoft Corp.の登録商標である。

4. 強固なメールセキュリティ

より安全にメールを利用できるようにOffice 365にはない添付ファイル自動暗号化，上長承認，一旦保留の機能を開発・拡充し，強固なメールセキュリティを実現した。

4.1 添付ファイル自動暗号化

通信経路上での情報漏えいを防止するため，“インターネット経由で送付するメールにファイルを添付して送信する場合は，添付ファイルを暗号化すること”が必要である。

このため，サードベンダー製のツールを採用したものの，このツールは，暗号化の強度が当社のセキュリティ要件を満たしていなかった。そこで，アメリカ連邦政府標準の暗号方式であるAES(Advanced Encryption Standard)の中でも，より強度が高い“AES 256bit暗号化方式”で暗号化できるようにツールを改修し，当社のセキュリティ要件に対応した。また，インターネット経由で送付するメールの添付ファイルを自動暗号化したい拠点と，インターネット経由の有無によらず，他社に送付するメールの添付ファイルを全て自動暗号化したい拠点の両方の要望に対応できなかった。そこで，インターネット経由せずにメール送付できる会社を定義し，利用各社のポリシーに合わせて暗号化対象を選択できる仕組みにした(**図3**)。

これによって，盗聴などによる企業機密の漏えいを防止している。

4.2 上長承認

社外に送付する企業機密情報の内容と宛先の適切さを確認するため，“他社へ企業機密情報を送信する場合は，上長承認と承認記録の保管をすること”が必要である。

このため，サードベンダー製のツールを採用したものの，このツールは，メール送信者と承認者の組合せをツール内部のデータベースで管理するため，人事異動や組織改編に合わせた厳密な管理が困難な仕組みであった。そこで，当社グループの認証基盤との連携機能を開発し，人事異動や組織改編に合わせて，メール送信者と承認者の組合せを自動的に更新する仕組みにした。また，メールの配送経路(インターネット経由か否か)と添付ファイルの有無の組合せによって，上長承認の対象条件を定義したいという利用各社の要望に対応できるようにインターネット経由せずにメール送付できる会社を定義し，各社ポリシーに合わせて上長承認対象を選択できる仕組みにした(**図4**)。

これによって，各社で適切な確認ができるようになり，メールによる企業機密情報の漏えいを防止している。

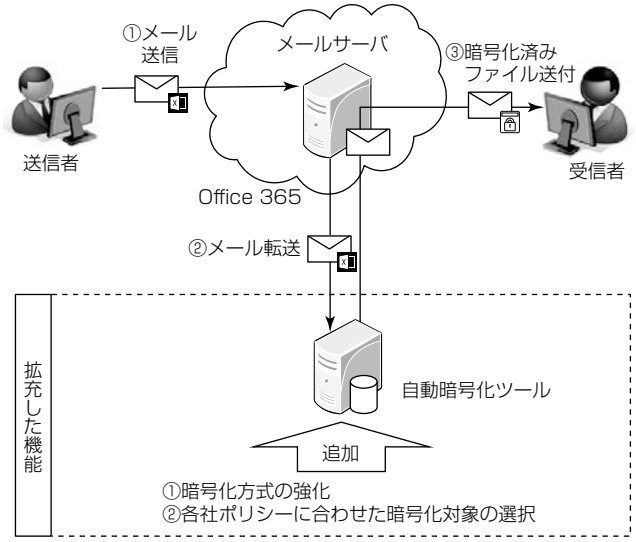


図3．添付ファイル自動暗号化の仕組み

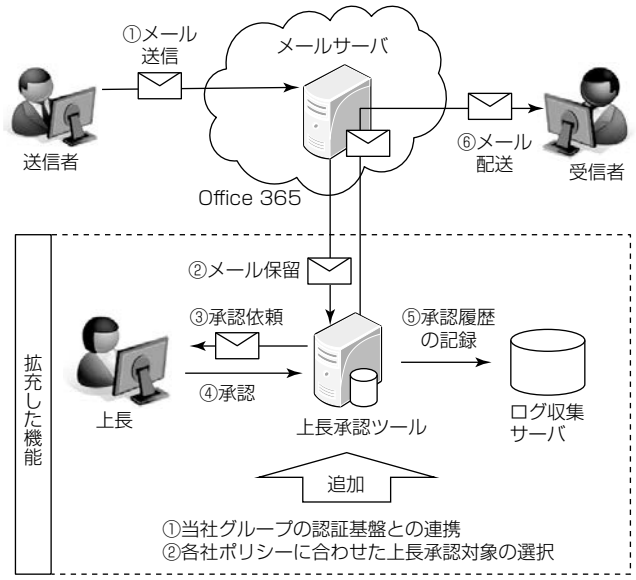


図4．ワークフローによる上長承認機能と承認履歴の記録

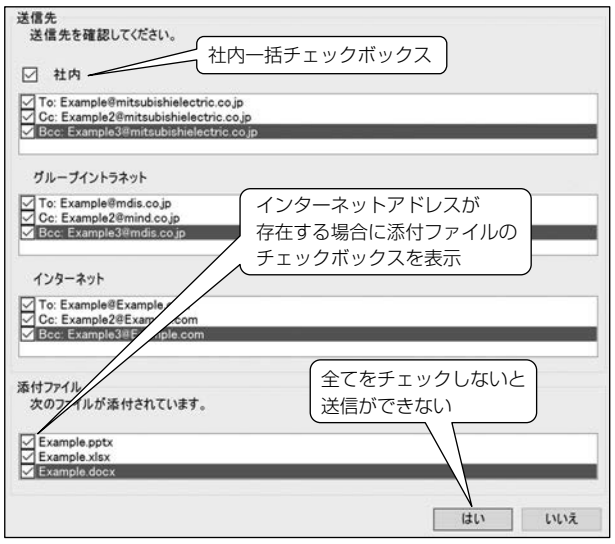


図５．宛先ポップアップツール(標準モード)

4.3 一 旦 保 留

宛先誤りの混入を抑止するため,“メール送信時には，一旦保留して宛先の確認をすること”が必要である。

このため，メール送信時に宛先を再確認するツール“宛先ポップアップ”を開発した。このツールは，利用者がメール送信ボタンを押すと，メールを内部保留して，宛先の確認をするポップアップを表示し，利用者が確認チェックした後で，内部保留していたメールを送信する仕組みである。

開発に当たっては,“標準モード”と“強化モード”の２種類を用意し，各拠点のポリシーによって選択できるようにした。標準モードは，宛先の確認を１回としている。これに対して，強化モードは，宛先の確認を複数回実施することで，より誤りに気付きやすくしている。標準モード，強化モードのいずれも，宛先誤りを検出しやすいように，社内宛，当社グループイントラネット接続会社宛，インターネット接続会社宛の三つに分けて表示している。また，インターネット接続会社宛の宛先がある場合は，添付ファイル欄にもチェックボックスを用意して暗号化要否を確認する仕組みにしている(**図５**)。

これによって，メール誤送信による企業機密の漏えいリスクを低減している。

5. 十分な記録保管

より高いレベルで記録管理できるようにOffice 365にはない，ログの長期保管と迅速な抽出を実現する機能を開発・拡充し，十分な記録保管を実現した。

セキュリティ問題発生時の影響範囲・問題箇所特定を迅速化するため,“ログを一定期間以上保管すること”，及び“ログを利用した調査が必要になった際には迅速に各拠点のセキュリティ担当者・責任者に提供すること”が必要である。

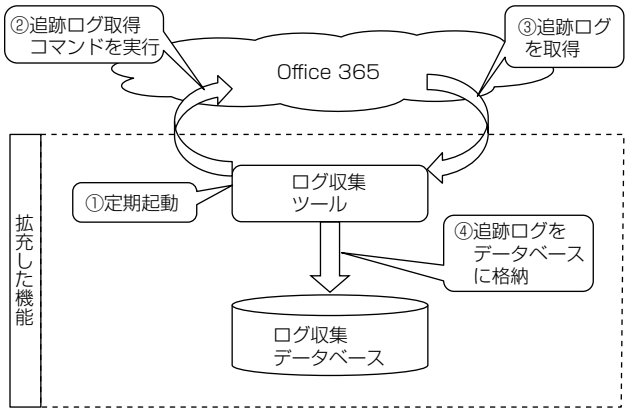


図６．Office 365からのログ抽出

このため，Office 365のログを定期的に取得して保管し，必要に応じて迅速にログを抽出する仕組みを開発した(**図６**)。また，各拠点でもログを分析したいという要望に対応して，ログの定期提供も実施している。

これによって，セキュリティ問題発生時の影響拡大を抑止している。

6. む す び

MELGITのセキュリティ機能の開発・拡充によって，より高いセキュリティレベルで活用できるIT環境を整備した。MELGITは，2018年８月末時点で，国内を中心に220拠点，約10万人が利用しており，情報漏えいなどのセキュリティリスクを低減し，拠点や会社をまたいだ情報共有やコミュニケーションが容易になっている。この結果，社員の日々の業務が効率化され，働き方に変化が出てきている。

今後，利用者の利便性を向上させるOffice 365の新サービスが次々と導入されてくることが見込まれる。これを，“速やか”に活用できるように，セキュリティ機能拡充の継続と実現期間の短縮に取り組んでいく。

当社グループの更なる発展のためには，事業間連携の強化によるシナジー効果の創出や働き方改革の実現が不可欠であり，これを支援するMELGITへの期待が高まってきている。今後も,“いつでも，どこからでも，安心して，快適に利用できる情報共有基盤”の継続的改善と，当社グループへの更なる展開を進めることで，当社グループの成長目標達成に貢献していく。

参 考 文 献

(1) 米岡靖浩，ほか：三菱電機グローバルIT基盤サービス“MELGIT”の構築と展開，三菱電機技報，**92**，No.12，665～668 (2018)
(2) 長尾　剛，ほか：グループ認証基盤の構築，三菱電機技報，**86**，No.12，679～682 (2012)