

BMLinkS
〈セキュリティホワイトペーパー〉
Version 1.0.0
2008.05.20

おことわり

本書における情報は、参考情報として、如何なる保証も伴うことなしに、JBMI Aよりユーザーの皆様方に提供されるものであります。

従って、本書に含まれる情報の使用・利用等により何らかの問題（セキュリティ問題等を含む）が発生したとしても、JBMI Aはユーザーの皆様方に対して、保証責任及び損害賠償責任等を含む一切の責任を負いません。

■商標

- 製品名、名称は各社の商標または登録商標です。

■Copyright

- BMLinkS、および、ロゴは、社団法人ビジネス機械・情報システム産業協会の登録商標です。
- 本書の著作権は、社団法人ビジネス機械・情報システム産業協会が所有しています。
- 本書の一部または全部を、著作権者の許可なしに、複製、転載することを禁止します。

目次

1. はじめに.....	4
1.1. 本ホワイトペーパーの目的	4
1.2. 本ホワイトペーパーの対象者	4
2. オフィス機器におけるセキュリティ上の脅威とは？	5
2.1. ネットワーク通信データの盗聴、改ざん	5
2.2. ユーザ詐称によるデータの盗聴、改ざん	5
2.3. サーバ詐称によるデータの盗聴、改ざん	5
2.4. 不揮発性メモリ上のデータの盗難・改ざん.....	6
2.5. 入力中の操作の盗み見	6
2.6. 印刷した紙の持ち去り	6
3. BMLINKS のセキュリティへの取り組み	7
3.1. 通信経路の暗号化.....	8
3.2. ユーザの認証.....	8
3.3. サーバの認証.....	9
3.4. 各種設定データのアクセス制御.....	9
3.5. 不揮発性メモリ上のデータの保護	9
3.6. 資産データのアクセス制御	9
3.7. 入力中の操作の盗み見防止	10
3.8. 機密印刷機能.....	10
4. BMLINKS セキュリティ機能の使い方	11
4.1. 機密印刷について.....	11
4.2. ストレージサービスへの格納における経路暗号化について	13
5. BMLINKS セキュリティ機能の運用.....	14
6. おわりに.....	16
7. 参考文献・関連リンク	17

1. はじめに

1.1. 本ホワイトペーパーの目的

昨今、情報機器の普及するに伴い、ネットワークを介した情報漏えいが新聞を賑わす等、情報セキュリティに関する社会的関心が高まっています。複合機も単なる複写機やプリンタ、スキャナの機能を超えて、情報機器としての機能を備え、BMLinkS もその流れの中にあります。

このような状況の変化を踏まえ、BMLinkS では、お客様に安心してサービスをご利用いただけるよう、BMLinkS 機器のセキュリティに基準を設けてセキュリティの課題に対処しています。

本ホワイトペーパーは、上記の取り組みを分かりやすく説明することを目的としています。

1.2. 本ホワイトペーパーの対象者

BMLinkS 機器を導入しようとする管理者および BMLinkS 機器をご利用になる一般ユーザを対象としています。

2. オフィス機器におけるセキュリティ上の脅威とは？

新聞等で報道されているように、情報流出は、組織内部のセキュリティ不備を突いて起こることが多くなっています。よって、入退室管理されたオフィスにおいてもセキュリティを考慮する必要があります。

オフィス機器を利用するにあたり、管理者および利用者は、少なくとも以下の脅威を意識する必要があります。

これらの脅威はオフィス機器一般に対する脅威であり BMLinkS 機器に特有のものではありませんが、BMLinkS 機器もオフィス機器である以上、これらの脅威を意識する必要があります。

2.1. ネットワーク通信データの盗聴、改ざん

お客様の PC とオフィス機器間のネットワーク上に流れる通信データを盗聴（パケットスニフリング）することにより、お客様の文書データ、アドレス帳、統計情報などのセキュリティ管理情報、通信中のパスワードなどが盗まれてしまう、またはデータを改ざんされてしまう危険性が考えられます。

2.2. ユーザ詐称によるデータの盗聴、改ざん

攻撃者が正規ユーザ／管理者になりすまし、オフィス機器に認証を行うことによりお客様の文書データ、アドレス帳、統計情報などのセキュリティ管理情報が盗聴される、またはデータを改ざんされてしまう危険性が考えられます。

2.3. サーバ詐称によるデータの盗聴、改ざん

お客様の PC とオフィス機器間で行われているネットワーク通信において、正当な接続認証および通信が行われている間に第三者である攻撃者が介入し、サーバになりすましお客様の文書データ、パスワードなどが盗まれてしまう、またはデータを改ざんされてしまう危険性が考えられます。

2.4. 不揮発性メモリ上のデータの盗難・改ざん

お客様のPCとオフィス機器の不揮発性メモリ（ハードディスク、メモリ等）に保存されているお客様の文書データ、アドレス帳、統計情報などのセキュリティ管理情報、各種設定情報（パスワード、サーバ証明書）などが、攻撃者により盗まれてしまう、またはデータを改ざんされてしまう危険性が考えられます。

2.5. 入力中の操作の盗み見

お客様がオフィス機器を利用中に、パスワード入力操作において、攻撃者によりパスワードを盗み見されてしまう危険性が考えられます。

2.6. 印刷した紙の持ち去り

お客様がオフィス機器で印刷した紙を他人に持ち去られてしまう危険性が考えられます。

3. BMLinkS のセキュリティへの取り組み

前章で説明したオフィス機器に一般的なセキュリティ上の脅威に対抗するため、BMLinkS では、BMLinkS 機器が保護すべき利用者の資産を定義し、その資産の可用性、完全性、機密性を保持するために、BMLinkS 機器が実施すべきセキュリティ機能を定義しています。

その上で、マルチベンダーのオフィス機器間で共通した安全性と操作性、接続性を維持するために、BMLinkS 機器が実施するセキュリティ機能の詳細な規定を行っています。

BMLinkS 機器間を通信され、BMLinkS 機器に蓄積される**お客様の文書データ**、および、BMLinkS 機器に記録されている**アドレス帳**や統計情報などを、保護すべき利用者の資産と定義しています。

また、機器の設定などを変更されて、BMLinkS 機器が持つセキュリティ機能を無効とされると、資産を保護することが難しくなりますので、**資産を保護するための機能を維持すること**も考慮しています。

第2章で挙げた脅威に対して、本章ではその対策を説明しますが、脅威と対策の対応関係は以下の通りです。

脅威	対策
2.1 ネットワーク通信データの盗聴、改ざん	3.1 通信経路の暗号化
2.2 ユーザ詐称によるデータの盗聴、改ざん	3.2 ユーザの認証
2.3 サーバ詐称によるデータの盗聴、改ざん	3.3 サーバの認証 3.4 各種設定データのアクセス制御
2.4 不揮発性メモリ上のデータの盗難、改ざん	3.4 各種設定データのアクセス制御 3.5 不揮発性メモリ上のデータの保護 3.6 資産データのアクセス制御
2.5 入力中の操作の盗み見	3.7 入力中の操作の盗み見防止
2.6 印刷した紙の持ち去り	3.8 機密印刷機能

3.1. 通信経路の暗号化

BMLinkS では、ネットワーク通信データの盗聴、改ざんの脅威への取り組みとして、通信経路を暗号化することを定義しています。現在、通信経路の暗号化技術には、SSL / TLS / IPsec / WEP (無線通信) など多くの標準があります。

BMLinkS では、これらの中から、現在最も普及している TLSv1.1 (RFC4346) を利用することを規定しています。また、使用する暗号強度については下記に列挙する以上のものを搭載することを規定しています。

- ・ 非対称鍵暗号化方式: RSA 暗号
- ・ 対称鍵暗号化方式: TripleDES
- ・ ハッシュアルゴリズム: SHA-1

さらに、その他の暗号化方式については以下を推奨としておりますが、各ベンダーによりサポートする暗号化方式等を制限するものではありません。

- ・ 対称鍵暗号化方式: AES
- ・ ハッシュアルゴリズム: SHA256、SHA384、SHA512

これらの暗号化方式等については、定期的な基準の見直しを行います。

3.2. ユーザの認証

セキュリティを考慮する上で、ユーザを識別認証することは、重要な意味を持ちます。ユーザを識別することによって、そのユーザのみが利用可能な資産を選択することができるようになります。

BMLinkS では、ユーザ詐称によるデータの盗聴、改ざんの脅威に対する取り組みとして、ユーザ認証機能を搭載することを拡張仕様として規定しています。その具体的な仕様は機器ベンダーやモデルにより異なりますが、推奨する内容は以下の通りです。

- ・ BMLinkS サービスに関する操作を行う際は、必ずユーザ認証を行うこと。
- ・ 認証に使用するパスワードは最低 8 文字以上であること。

BMLinkS が提供するサービスには、利便性を優先するため、認証されたユーザがサービスの全ての機能を利用できるようになっているものがあります。このようなサービスにおいて、ユーザ毎にアクセスする資産を別々にしたい場合は、ユーザ毎に分けて同じサービスを起動させる必要があります。

3.3. サーバの認証

ネットワーク上でのサーバ詐称によるデータの盗聴、改ざんの脅威への対策として、SSL/TLS 通信確立時に、サーバ認証を行う機能を搭載することを拡張仕様として規定しています。その具体的な仕様は機器ベンダーやモデルにより異なりますので、ご利用の機器のマニュアル等を参照下さい。

3.4. 各種設定データのアクセス制御

サーバ詐称によるデータの盗聴、改ざんや不揮発性メモリ上のデータの盗難、改ざんの脅威への対策として、BMLinkS では、サービスに関する設定情報については、一般ユーザとは区別された管理者のみが操作可能とすることを規定しています。

BMLinkS が提供するサービスをセキュアに運用するために、BMLinkS 機器の管理者は、各機能を正しく設定するとともに、管理者のためのパスワードを初期値から変更する等、他の人に分からないように管理して下さい。

3.5. 不揮発性メモリ上のデータの保護

不揮発性メモリ上のデータの盗難、改ざんの脅威への対策として、BMLinkS では不揮発性メモリ上に保管されるデータについても何らかの手段を用いて保護することを規定しています。

保護方法としては、不揮発性メモリ全体の暗号化や保管されるデータの暗号化の他にもさまざまな方式が考えられますが、暗号化技術を用いる場合には、AES128bit 以上を使用することを推奨しています。実際の不揮発性メモリ内のデータ保護方法については、ご利用の機器により異なります。

3.6. 資産データのアクセス制御

不揮発性メモリ上のデータの盗難、改ざんの脅威への対策として、BMLinkS ではお客様の文書

データやアドレス帳情報、統計情報などを、権限のないユーザによって参照、変更等されないよう適切にアクセス制御できることを規定しています。実際の設定方法については、ご利用の機器により異なります。

3.7. 入力中の操作の盗み見防止

入力中の操作の盗み見の脅威への対策として、BMLinkS では、サービス利用時のユーザ ID/パスワード入力時の防御方法について、以下を規定しています。

- ・ 入力された文字の、画面上への入力フィードバックを行わない
- ・ 入力された文字の画面上へのフィードバックは、“*” など、意味を持たないものとする。

3.8. 機密印刷機能

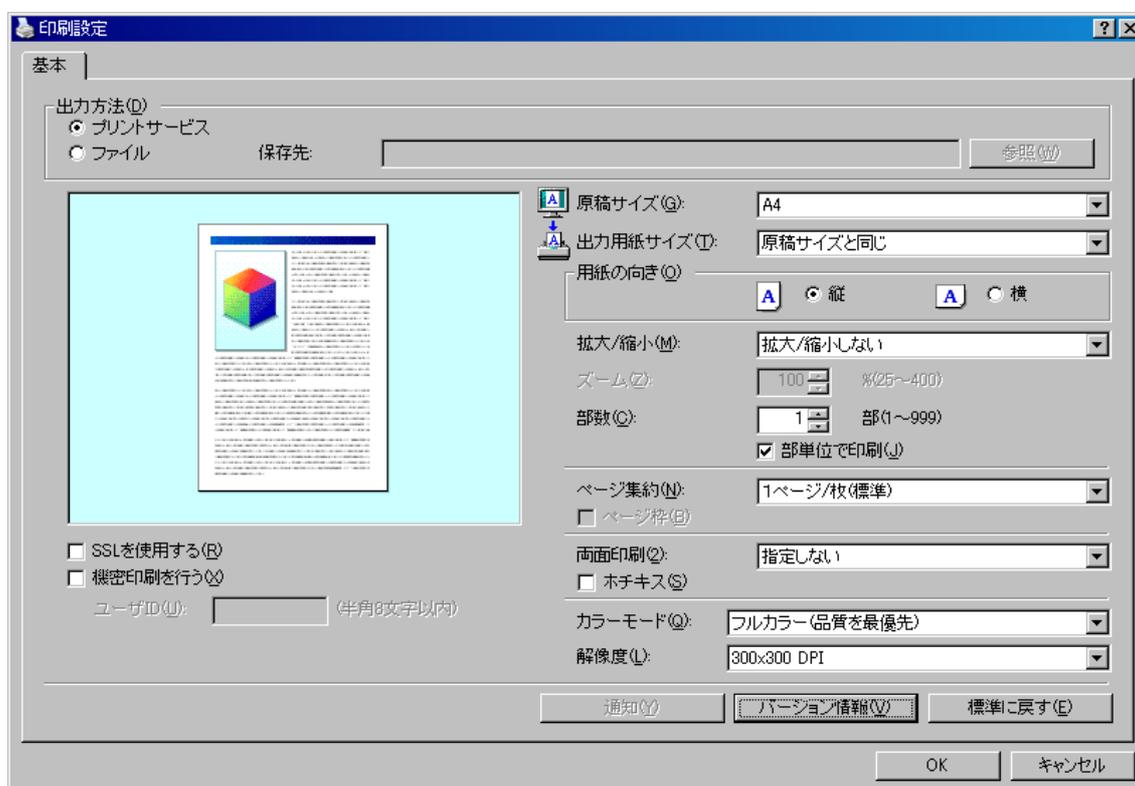
印刷した紙の持ち去りの脅威への対策として、BMLinkS では機密印刷機能を規定しています。機密印刷機能の説明は、第4章「BMLinkS セキュリティ機能の使い方」で解説します。

4. BMLinkS セキュリティ機能の使い方

4.1. 機密印刷について

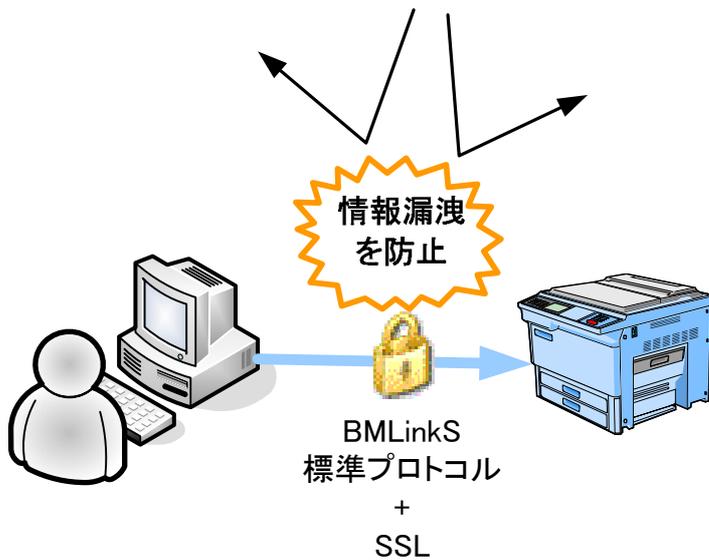
BMLinkS では、より強固なセキュリティレベルを求める利用者のために、通常の印刷方式に加えて、機密印刷方式での印刷を行うことができます。

以下に示す図は、BMLinkS 共通プリンタドライバにおける印刷設定ダイアログです。



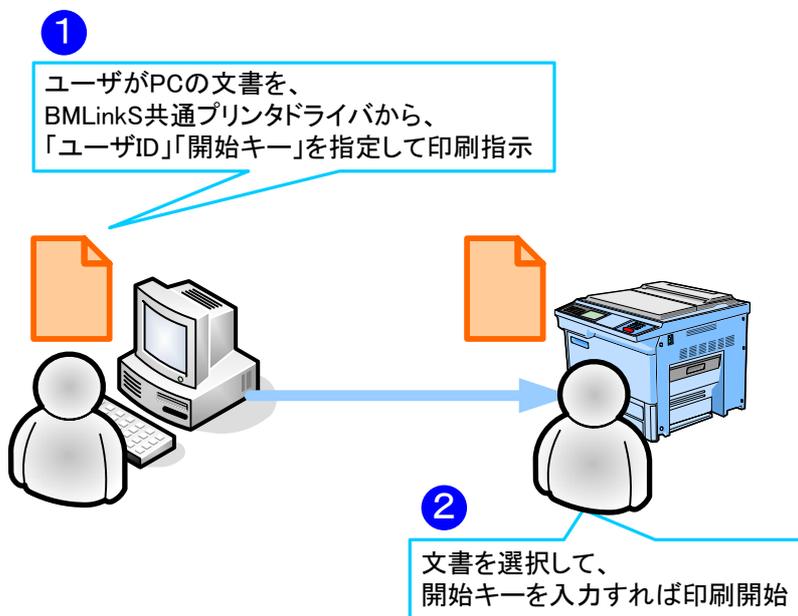
[SSL を使用する]

出力先の BMLinkS 機器が SSL 通信に対応している場合、この画面左下にある「SSL を使用する」をチェックして印刷を行うと、印刷クライアントと出力先の BMLinkS 機器の間の通信が暗号化され、第三者がネットワークを盗聴して印刷文書の内容を不正に入手する脅威から印刷文書を守ることができます。



[機密印刷を行う]

「SSL を使用する」と同様に、「機密印刷を行う」をチェックして印刷を行うと、印刷データがいったん BMLinkS 機器に保存され、BMLinkS 機器の操作パネルから開始キーを入力して実際の印刷が開始されるようになります。これにより、印刷結果が不正に第三者に持ち去られることを防止することができます。

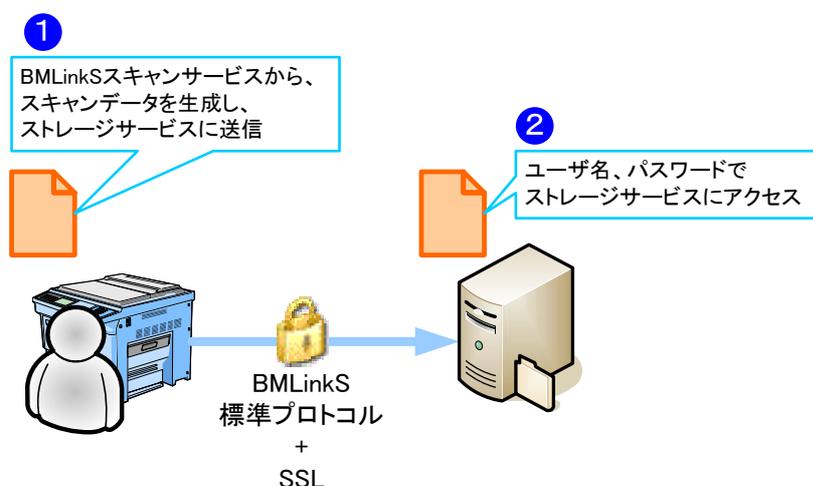


なお、機密印刷および SSL 対応はオプションです。対応する BMLinkS 機器につきましては各メーカーにお問い合わせください。

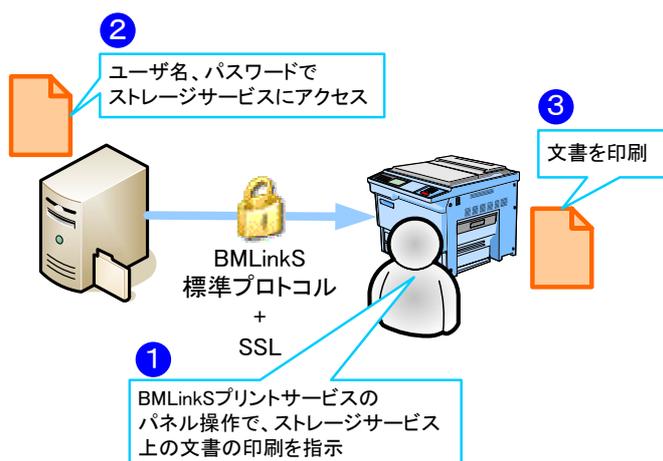
4.2. ストレージサービスへの格納における経路暗号化について

ストレージサービスは、各ユーザの PC 上で BMLinkS ストレージサービスを提供するソフトウェアです。PC 上でストレージサービスを動作させることにより、以下のようなことが可能になります。

1. BMLinkS スキャンサービスから、スキャンデータを PC のハードディスクに保存することができます。(ネットワーク保存)



2. PC のハードディスクに保存したお客様の文書データを、BMLinkS 機器のパネル操作で、印刷することができます。(保存文書印刷)



なお、ストレージサービスでの SSL 対応はオプションです。対応する BMLinkS 機器につきましては各メーカーにお問い合わせください。

5. BMLinkS セキュリティ機能の運用

BMLinkS で飛躍的に向上したネットワーク上でのオフィス機器間の接続性・データ交換性を安全に確保するために、BMLinkS 機器だけでなく、その周りのオフィス環境も含めたセキュリティ面の運用をきちんと行う必要があります。

[前提環境について]

BMLinkS 機器は、基本的なセキュリティ機能を備えていますが、利用される環境により守られている事を前提としている部分もあります。BMLinkS 機器を使用される場合には、以下の点に関してもご考慮下さい。

BMLinkS 機器は、BMLinkS 機器が接続されるネットワークや環境が管理されている事を前提にセキュリティ機能を定義しています。(この様な前提を置かないで、セキュリティ機能を設計しますと、多くのセキュリティ機能を BMLinkS 機器に実装しなければならなくなり、より多くのコンピュータリソースや物理的機材が必要となります。この場合、機器本体の価格上昇や、機器本来の機能の低下を招く事が懸念されるため、BMLinkS ではこの様な選択を行っていません。)

ネットワークに接続する機器については、どのような機器が接続されているか、どのような機器を接続するか、把握してください。ネットワーク管理者が許可した機器のみを接続するというルールを決めることも重要です。

BMLinkS ストレージサービスをインストールするサーバに関しては、設置する部屋の入退室管理を行い、ハードディスク等の盗難が発生しないように管理して下さい。場合によっては、ハードディスク等の暗号化を実施することも検討して下さい。

[サーバ証明書の運用について]

クライアントと BMLinkS 機器との通信、また、BMLinkS 機器同士で通信を行う際には、SSL/TLS を用いて通信路を暗号化することを推奨します。

SSL/TLS 通信を行う場合には、BMLinkS 機器にインストールされたサーバ証明書を利用します。サーバ証明書は、利用する環境において信頼できるものをご利用下さい。BMLinkS 機器が生成する自己証明書などをサーバ証明書として利用する事も可能ですが、その場合には、クライアントの「信頼する証明書リスト」にサーバ証明書を追加して下さい。

[ユーザ認証の推奨について]

BMLinkS 機器の機能の中にはユーザの認証が拡張仕様として規定されており、必ずしもユーザの認証が必要ではないように設定できるものもあります(例: BMLinkS ストレージサービス)が、セキュリティの観点からはユーザを認証する様にして利用される事を推奨します。

また、BMLinkS が提供するサービスにおいては、利便性を優先するため、認証されたユーザが

サービスの全ての機能を利用できるようになっているものがあります。このようなサービスを利用される場合には、同じサービスを複数個起動させ、それぞれのサービスを個々のユーザだけがアクセスするように設定することを推奨します。

これらの設定により、ユーザが他のユーザの文書データにアクセスすることを不可とする運用が可能となります。

[パスワードの管理について]

ユーザを認証する場合には、認証のパスワードの管理にもお気をつけ下さい。他のユーザにユーザ自身のパスワードを教えたり、紙に書いて誰でも見える所に置いておく様な事をしないのはもちろんの事、容易に推測できるパスワードや、短いパスワードも危険です。英数字や記号等も交えた8文字以上のパスワードを利用される事を推奨します。また複雑なパスワードでも、総当たり攻撃などにより発見されてしまう危険がありますので、定期的に変更される事を推奨します。

パスワードは入力操作が伴うため、盗み見されてしまう危険性があります。パスワードを入力する際には、まわりを確認するようにしてください。

[セキュリティ教育について]

BMLinkS 機器を利用する場合に限らず、ご利用の環境を安全に保つためにも、利用者や管理者に対してセキュリティの基本的な教育を行うことは有効です。いままで述べて来たことと重なる部分もありますが、BMLinkS 機器の利用者や管理者に対して、以下の様な内容を指導して頂く事を推奨します。

一般の利用者に対して、

- ・ パスワードは、英数字・記号交えて少なくとも8文字以上を用い、他人に推測されにくい内容にしましょう。
- ・ パスワードは、定期的に変更しましょう。
- ・ 重要な文書のプリントには機密印刷機能を使いましょう。

管理者に対して、

- ・ パスワードは、英数字・記号交えて少なくとも8文字以上を用い、他人に推測されにくい内容にしましょう。
- ・ パスワードは、定期的に変更しましょう。
- ・ BMLinkS 機器をセキュアに保つために、正しく設定を行いましょう。
- ・ BMLinkS 機器の設定を定期的を確認しましょう。

[機密印刷機能の使用推奨について]

BMLinkS プリントサービスをご利用になる際には、機密印刷機能を利用する事を推奨します。機密印刷機能により、ユーザが開始キーを入力しなければ BMLinkS 機器における印刷動作が開始しませんので、印刷文書の盗難や、置き忘れといった情報漏えいの危険を回避する事ができます。

6. おわりに

本文書では BMLinkS におけるセキュリティへの取り組み、セキュリティ機能の使用方法、運用に関しまして説明をいたしました。

BMLinkS では、3 章で説明したようにセキュリティに関する基準を定め、この基準に基づいて仕様に関してセキュリティ面からのアセスメントを実施した結果、現在の仕様が規定されたセキュリティ基準を満たしていることを確認しております。さらに今後新規追加される機能、仕様に関しても定期的な見直しを図ります。

また、セキュリティ基準そのものに関しても、暗号化アルゴリズム／暗号化方式をはじめとする最新の技術動向やセキュリティ標準など世の中の動向を踏まえ、セキュリティ基準となる「資産」「脅威」「対策」の定期的な見直しを図っていきます。

7. 参考文献・関連リンク

- T. Dierks and E. Rescorla. RFC 4346: The Transport Layer Security (TLS) Protocol Version 1.1
<http://www.ietf.org/rfc/rfc4346.txt>, April 2006.

BMLinkS ホワイトペーパー Version 1.0.0

2008.05.20

発行社団法人ビジネス機械・情報システム産業協会

BMLinkS プロジェクト委員会

〒105 - 0003 東京都港区西新橋 3 丁目 25 番 33 号

NP 御成門ビル

<http://www.jbmia.or.jp/bmlinks/>

無断転載禁止© 2008 Japan Business Machine and Information System Industries Association



BMLinks セキュリティ ホワイトペーパー Version 1.0.0

